F A C H H O C H S C H U L E W E D E L

Seminararbeit

In der Fachrichtung Wirtschaftsingenieurwesen

Thema:

Digitales Geld, die Blockchain und Bitcoin

Eingereicht von:	Bünyamin Kilic (B_Wing101997) Kampstr.36 20357 Hamburg Tel. (040) 43 99 256, 017648320369 E-Mail: kilic.buenyamin@web.de
Erarbeitet im:	6. Semester
Abgegeben am:	16.07.2018
Referent (Fh-Wedel):	Prof. Dr. Michael Anders Fachhochschule Wedel Feldstr. 143 22880 Wedel Tel. (04103) 8048-13 E-Mail: an@fh-wedel.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
Art.	Artikel
Abs.	Absatz
BTC	Bitcoin
bzgl.	bezüglich
ca.	circa
d.h.	das heisst
DLT	distributed ledger Technology
E-Geld	elektronisches Geld
etc.	et cetera
H/s	hash pro Sekunde
KH/s	Kilo hash pro Sekunde
PoS	Proof of Stake
PoW	Proof of Work
P2P	peer to peer
SPV	Simplified Payment Verification
TH/s	Terra hash pro Sekunde
u.a.	unter anderem
vgl.	vergleiche
z.B.	zum Beispiel

1 Einleitung

1.1 Problemstellung

„Bargeld ist nach wie vor das beliebteste Zahlungsmittel in Deutschland und wird es auf absehbarer Zeit wohl auch bleiben“.[1] In der Bevölkerung werden Münzen und Banknoten aufgrund Ihrer allgemeinen Akzeptanz und der kostengünstigen Verwendung nach wie vor als beliebteste Währung gesehen. Im Jahr 2017 wurden 74% der Transaktionen mit Münzen oder Banknoten getätigt. Jedoch werden gängige Zahlungsvorgänge in privaten Haushalten, wie zum Beispiel Versicherungen, Mieten, Strom- und Gasrechnungen über automatische Kontoabbuchungen abgewickelt. Der Umsatz, welcher mit Debitkarten (hauptsächlich girocard) erreicht wurde, ist im Vergleich zu 2014 um 6% gestiegen. Kreditkarten haben ebenfalls an Popularität gewonnen und machen einen Anteil von 5 % des Gesamtumsatzes aus. Kontaktloses Zahlen, wie zum Beispiel mit dem eigenen Handy bekommen immer mehr an Bedeutung, während Bezahlverfahren übers Internet bereits den Durchbruch im Onlinehandel geschafft haben.[2]

Virtuelle Währungen, wie zum Beispiel Bitcoin, gehören zu der Kategorie der jüngsten Internet-Innovationen, welche Konsumenten von der Abhängigkeit des Finanzsystems befreien können. Im Kontext der Finanzkrise 2008 und des damit einhergehenden Vertrauensverlustes der Konsumenten in staatliche und privatwirtschaftliche Institutionen, hat der Bitcoin eine einmalige Entwicklung durchgemacht und sich seither als Referenz auf dem Gebiet der virtuellen Währungen etabliert.[3]

Die Technologie, auf welcher die virtuelle Währung Bitcoin basiert, existiert bereits seit 2008 und hat laut Experten das Potenzial etliche Bereiche der Gesellschaft, die weit über das Gebiet digitaler Währungen hinausgehen, zu verändern. Aufgrund ihrer vielseitigen Einsetzungsmöglichkeit, werden immer mehr Menschen aufmerksam auf die Blockchain-Technologie.

Im Oktober 2009 entstand der erste Wechselkurs auf Dollar-Basis. Dieser wurde mit 1309,03 BTC für 1 US-Dollar festgelegt. Der Wert des Bitcoins betrug also 0,08 Cent.

[1] Vgl.Horstmann(2015, S.66)

[2] https://www.bundesbank.de/Redaktion/DE

[3] dievolkswirtschaft.ch/de/2014/09/sansonetti-3

Anfang 2013 hatte der Bitcoin einen Wert von ca.25 US-Dollar. Ende 2017 hat der Bitcoin sein absolutes Maximum von 19.950 Dollar erreicht.[4]

1.2 Zielsetzung und Aufbau der Arbeit

Das Ziel dieser Arbeit soll sein, ein Verständnis für die technische Funktionsweise der innovativen Technologie hinter dem Bitcoin und die älteste Währung, welche auf dieser Technologie basiert zu vermitteln.

Der erste Teil der Arbeit bietet einen Einblick in elektronische Währungen und ihrer Zahlungssysteme. Im zweiten Teil der Arbeit wird die Blockchain-Technologie analysiert. Zunächst einmal werden theoretische Grundlagen sowie die Rolle der Kryptographie in der Blockchain erörtert. Anschließend wird die Funktionsweise der Blockchain und mögliche Anwendungsfälle der Technologie beschrieben. Der dritte Teil der Arbeit beschäftigt sich damit, einen Überblick über die virtuelle Währung Bitcoin zu vermitteln. Hierfür wird zunächst einmal auf die Geschichte des Bitcoins eingegangen. Im Anschluss werden theoretische Aspekte sowie Entwicklungen des Bitcoins beleuchtet. Im letzten Teil der Arbeit werden Bitcoin Transaktionen und wie man in den Besitz von Bitcoins kommt vorgestellt.

1.3 Methodisches Vorgehen

Aufgrund der Tatsache, dass virtuelle Währungen erst in den letzten Jahren stark an Popularität zugelegt haben, werden sie erst seit einiger Zeit in wissenschaftlichen Arbeiten beschrieben. Veröffentlichungen in Buchform haben erst seit Ende 2016 an Bedeutung gewonnen.

Für eine entsprechende Vielfältigkeit, werden nicht nur vergangene und aktuelle Artikel aus Internetblogs und Artikel aus Fachzeitschriften berücksichtigt, sondern auch einige Bücher aus dem aktuell begrenzten Sortiment. Da Bitcoins dezentral organisiert sind und keinen Bezug zu Währungen, die durch die Regierung selbst reguliert werden haben, werden auch Webseiten von Regierungen zum Thema Dezentralität und Transparenz als Informationsquelle betrachtet.

[4] www.blockchain.com/de/explorer

2 Digitales Geld

2.1 Definition Geld

Elektronisches Geld (E-Geld, digitales Geld, Cybergeld, früher auch Computer Geld) wurde in Europa erstmals durch die E-Geld Richtlinie 2000/46 EG durch das Europäische Parlament definiert. Diese Richtlinie befasste sich mit der Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten. Darüber hinaus handelt es sich nach dieser Richtlinie (Art. 1 Abs.3) bei elektronischem Geld um einen monetären Wert, welches durch eine Forderung gegen die ausgebende Stelle gekennzeichnet ist. Dieser ausgegebene Wert ist niemals geringer als der Wert, der monetär ausgegeben werden kann. Außerdem muss dieser Wert durch andere Unternehmen als Zahlungsmittel akzeptiert werden.[5]

Die EU- Kommission definiert E-Geld zur Vereinfachung als digitales Bargeld, welches auf einem elektronischen Gerät („Elektronische Geldbörse“) oder einem räumlich entfernten Server gespeichert ist. Als mögliche physikalische Speichermedien dienen nicht nur Chipkarten auf die der Anwender den aktuellen Wert (bis zu 200 Euro) direkt auf den Chip oder auf dem Magnetstreifen von Kunststoffkarten abspeichert, sondern auch Mobiltelefone, USB-Sticks und Fitness-Armbänder. Zusätzlich zur „Elektronischen Geldbörse“ kann auch das softwarebasierte Netz Geld zum Speichern und übertragen von E-Geld dienen. Hier wird zunächst Buchgeld an die herausgebende Bank oder das E-Geld-Institut überwiesen. Anschließend wird durch den Herausgeber ein gleichwertiger Betrag in Form von E-Geld an den Kunden übertragen. E-Geld-Institute stehen in der Pflicht die vorgegebenen Richtlinien einzuhalten. So muss z.B. jeder neue Kunde eine Legitimationsprüfung durchlaufen. E-Geld wird durch E-Geld-Institute ausgegeben.[6]

2.2 Anforderungen an E-Geld-Zahlungssysteme

Bargeld als physikalisches Zahlungsmittel wird nach wie vor in Deutschland als bevorzugte Zahlungsmöglichkeit gesehen.[7] Viele Menschen empfinden das bargeldlose Zahlen als unsicher. Die Gefahr mit Betrugsversuchen konfrontiert zu werden ist viel zu groß. Darüber hinaus besteht die Möglichkeit mehr Geld auszugeben, als man tatsächlich besitzt. Aufgrund

[5] www.bundesgerichtshof.de/DE/Bibliothek

[6] eur-lex.europa.eu

[7] www.bundesbank.de/Redaktion/DE/Themen/2018

dieser Tatsachen werden verschiedene Anforderungen an elektronische Zahlungssysteme gestellt. Um eine möglichst breite Masse für Transaktionen mit elektronischem Geld zu gewinnen ist die Erfüllung dieser Anforderungen von immenser Bedeutung.

Eine fundamentale Anforderung an elektronische Zahlungsmittel ist die Sicherheit. Das System muss eine sichere Transaktionsabwicklung gewährleisten. Die übertragenen Daten (Transaktionspreis, Transaktionsinhalt, Identität) müssen vertraulich behandelt und gegenüber dritten geheim gehalten werden. Eine mindestens gleichermaßen bedeutsame Anforderung stellt die Authentizität dar. Bei jeder Transaktionsabwicklung muss die Identität der Person auf Echtheit überprüft werden. Eine der gängigsten Möglichkeiten für die Authentifizierung ist die Authentifizierung durch Wissen. Bei dieser Methode wird überprüft ob die Person, notwendige Informationen wie z.B. ein Kennwort, eine PIN (Persönliche Identifikationsnummer) oder eine TAN (Transaktionsnummer) kennt. Eine Absicherung im Schadensfall sowohl für Händler als auch für Kunden spielt eine ebenso wichtige Rolle. Der Kunde muss gegenüber Missbrauch seiner Daten geschützt werden. Sowohl bei Zahlungen durch die Verschlüsselung mit SSL (Secure Sockets Layer) als auch beim Lastschriftverfahren ist der Händler der Träger des Missbrauchsrisikos, weshalb der Kunde hier auf der sicheren Seite ist und die Möglichkeit hat ohne die spezifische Angabe von Gründen die Zahlung zu stornieren. Anders ist es aus Sicht des Händlers, welcher sich gegen die hohen Zahlungsausfälle schützen möchte und auf Maßnahmen wie Bonitäts- und Adressprüfungen zurückgreift.[8]

Bei der Auswahl des jeweils richtigen Zahlungssystems aus Sicht des Kunden, ist die Betrachtung der Transaktionsgebühren, welche bei diversen Zahlungssystemen anfallen enorm wichtig. Forderungen, welche nicht zwingend notwendig, aber dennoch aus Sicht des Kunden erwünscht werden sind u.a. Benutzerfreundlichkeit, Bedienbarkeit, Verbreitung der Bezahlmöglichkeit und Akzeptanz durch Kunden.

2.3 Abgrenzungen E-Geld

Immer mehr Konsumenten fühlen sich durch E-Geld-Emittenten wie PayPal oder Amazon Payments angezogen. E-Geld muss entsprechend seiner Definition nicht nur abgespeichert werden können, sondern der ausgegebene Wert darf niemals geringer sein als der Wert der monetär ausgegeben werden kann. Bevor E-Geld mit einem vorhandenen Wert ausgestellt

[8] https://de.wikipedia.org/wiki/Elektronisches_Geld

werden kann muss zunächst einmal mit „echtem“ Geld, welches dem erwünschten Wert entspricht gezahlt werden. Dabei spiel die Art der Zahlung (Bar, Rechnung, Lastschrift etc.) keine wichtige Rolle. Darüber hinaus muss eben dieses E-Geld bei anderen Unternehmen als Zahlungsmittel akzeptiert werden.

Gängige Gutscheinkarten für bekannte Unternehmen wie Zalando, H&M oder IKEA werden zwar abgespeichert und ihr Wert entspricht auch dem gezahlten Geldbetrag, jedoch erfüllen diese die Notwendigkeit, dass diese Gutscheinkarten auch von anderen Unternehmen akzeptiert werden müssen nicht. Dementsprechend kann man hier nicht von E-Geld sprechen. Nach der Definition können auch Tankkarten, Restaurantgutscheine und Reisegutscheine als E-Geld ausgeschlossen werden. Die im September 2000 erstmals durch das Unternehmen paysafecard Wertkarten GmbH eingeführte paysafecard findet nach wie vor sehr viel Zuspruch in der Gesellschaft. Über 2.5 Millionen Nutzer pro Monat verzeichnete das Unternehmen 2016.[9] Hier wird die sogenannte paysafecard mit einem bestimmten Betrag aufgeladen. Anschließend lässt sich die paysafecard bei vielen anderen Unternehmen als Zahlungsmittel einsetzen d.h. die Bedingung, dass das Geld von anderen Unternehmen als Zahlungsmittel akzeptiert werden muss wird erfüllt, weshalb man hier von E-Geld sprechen kann. Ein weiteres Beispiel für E-Geld sind Prepaid-Kreditkarten, welche immer mehr Zuspruch bekommen. Diese lassen sich ebenso benutzen wie andere Kreditkarten. Der zentrale Unterschied ist jedoch, dass die Prepaid Kreditkarte nur bis zu dem Limit, den man vorher aufgeladen hat verwendet werden können. Dementsprechend wird das Risiko sich zu verschulden aufgehoben.

Bitcoin und andere Kryptowährungen werden von einigen Experten als E-Geld angesehen. Wenn man sich jedoch der Definition von Kryptowährungen, welche auch „virtuelle“ Währungen genannt werden bewusst ist, wird einem schnell klar, dass dies nicht so einfach sagen kann. Nach der Definition muss E-Geld von einem Emittenten gegen eine Forderung ausgegeben werden, welches bei Kryptowährungen nicht der Fall ist.[10] Virtuelle Währungen wie z.B. Bitcoin werden von keiner höheren Instanz kontrolliert und haben auch keinen Bezug zu Zahlungsmitteln, die gesetzlich durch die Regierung vorgegeben sind.

[9] www.paysafecard.com/de/corporate/presse/pressemitteilungen

[10] www.ppro.com/de/blog-de/ist-eigentlich-e-geld

3 Grundprinzipien der Blockchain-Technologie

3.1 Begriffserklärung und theoretische Grundlagen

Der Begriff Blockchain stammt aus dem englischen und setzt sich aus zwei Begriffen zusammen. Unter „Block“ versteht man die zusammengefassten Transaktionsblöcke. Der Begriff „Chain“ (deutsch: Kette) beschreibt die Verkettung dieser Datenblöcke.[11]

Das Konzept der Blockchain-Technologie wurde von einer Person mit dem Pseudonym Satoshi Nakamoto 2008 erstmals unter Bitcoin beschrieben. Ein Jahr später kam es zur ersten Implementierung der Bitcoin Software. Die Voraussetzung für eine Transaktion ist eine Bestätigung durch sämtliche Teilnehmer. Diese Transaktion wird zur Gewährleistung der Sicherheit verschlüsselt.[12]

Eine der zentralen Säulen der Blockchain ist die Dezentralität. Unter Dezentralität versteht man, dass keine zentralen Instanzen, weder Personen noch Unternehmen oder Behörden Kontrolle über die Blockchain haben. Die einzelnen Transaktionsprotokolle zwischen zwei oder mehr Parteien liegen nicht nur auf einem Server, sondern verteilt auf unzähligen Rechnern. Eine jede noch so kleine Information zu einer Transaktion wird auf einem digitalen Kontoauszug protokolliert und ist für jeden beteiligten einsehbar. Dadurch wird die Transparenz zwischen den Transaktionspartnern gewährleistet. Informationen die auf mehreren Rechnern gleichzeitig administriert werden sind nahezu unmöglich zu verfälschen. Dadurch, dass bei Transaktionen kein Vermittler notwendig ist, kommt es zu einer schnelleren Transaktionsabwicklung.

3.2 Dir Rolle der Kryptographie

Der Begriff Kryptographie kommt ursprünglich aus dem griechischen und setzt sich zusammen aus κρυπτος´ (deutsch: verborgen) und γρ´αφειν (deutsch: schreiben).[13] Kryptographie konnte man aufgrund dieser Übersetzung als Wissenschaft der Verschlüsselung verstehen. Für ein leichteres Verständnis dieser Definition ist die Betrachtung der Kryptologie von immenser Bedeutung. Unter Kryptologie versteht man die wissenschaftliche Disziplin der Ver.- und Entschlüsselung von Informationen. Kryptographie ist eben der Teil der Kryptologie

[11] wirtschaftslexikon.gabler.de/definition

[12] www.allianzdeutschland.de/digitalisierung-was-steckt-hinter-der-blockchain-technologie-

[13] www.polyas.de/blog/de/online-wahlen/sicherheit/kryptographie-was-ist-das

der sich mit verschiedenen Methoden zur Verschlüsselung von Informationen befasst. Diese Disziplin verfolgt das Ziel der Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit von Informationen. Vertrauliche Daten wie Transaktionsinformationen sollen somit geschützt werden. Bei der Blockchain-Technologie werden hauptsächlich zum einen Hash-Funktionen zum anderen Digitale Signaturen zur Verschlüsslung von Informationen verwendet.

3.2.1 Hash-Funktionen

Der Begriff „Hash“ aus „Hashfunktion“ kommt ursprünglich aus dem englischen und lässt sich im deutschen als „zerhacken“ übersetzen. Die Übersetzung gibt einen Hinweis darauf, dass die Funktionen, Informationen eben zunächst „zerhacken“ um sie anschließend strukturieren zu können.[14]

Hashfunktionen werden in der Blockchain-Technologie eingesetzt um Informationen bzgl. der Transaktion wie z.B. Transaktionsbetrag zwischen zwei Parteien vor dritten zu schützen. Dabei werden die eingegebenen Zeichen variabler Länge auf Zeichen fixer Länge komprimiert.[15] Das Ergebnis der Hashfunktion ist der Hashwert. Diese Hashwerte haben alle dieselbe Länge. Eine zentrale Eigenschaft der Hashfunktionen ist, dass diese als Einwegfunktion zu verstehen sind. Es sollte unmöglich sein, aus dem Hashwert auf die Eingabe zu schließen. Darüber hinaus sollte die Kollisionssicherheit gewährleistet sein. Zwei Werte aus der Eingabemenge dürfen nicht auf einen Hashwert abgebildet werden. Einer der gängigsten Hash-Algorithmen ist der SHA256-Algorithmus. Dieser Algorithmus findet auch beim Bitcoin-Mining seine Verwendung mehr(vgl. 4.6).[16] Abbildung 3-1 veranschaulicht einige Hash-Funktionen.

[14] de.wikipedia.org/wiki/Elektronisches_Geld

[15] www.datenschutzbeauftragter-info.de/bitcoin-technische-grundlagen-der-kryptowaehrung

[16] blockchainwelt.de/kryptographie-innerhalb-der-blockchain-technologie/

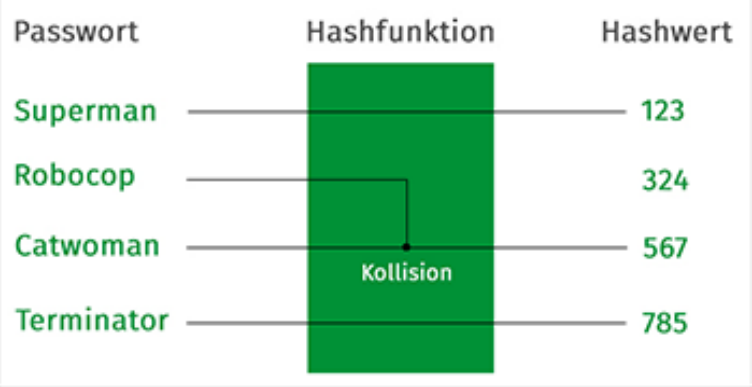

Abbildung 3-1: Darstellung einer Hash-Funktion[17]

3.2.2 Digitale Signatur

Digitale Signaturen gehören zu der Kategorie der asymmetrischen Verschlüsselungsverfahren und werden dazu verwendet um sicherzustellen ob Transaktionen durch rechtmäßige Parteien getätigt wurden. Unter „Asymmetrisch“ versteht man, dass zum Entschlüsseln einer Nachricht ein anderer Schlüssel verwendet wird als zum Verschlüsseln.[18] Digitale Signaturen sind als online Versionen von handschriftlichen Signaturen zu verstehen.[19]

Bei digitalen Signaturen werden vom Benutzer zwei verschiedene elektronische Schlüssel erzeugt. Zum einen ein privater Schlüssel (private key) zum anderen ein öffentlicher Schlüssel (public key). Zusammen bilden diese ein Signaturschlüsselpaar. Bestimmte Hashfunktionen wie z.B. der Algorithmus SHA-256 sorgen dafür, dass eine Prüfsumme (Hashwert) kreiert wird. Dieser Hashwert wird durch den private key, welcher nur dem Ersteller bekannt ist verschlüsselt. Es resultiert ein digital signiertes Dokument. Der Empfänger der Nachricht entschlüsselt das Dokument nun durch das übertragene Zertifikat, welches den public key enthält. Außerdem nimmt der Empfänger eine vom ursprünglich erstellten Hashwert unabhängige Berechnung des Hashwertes vor. Anschließend wird überprüft ob die Hashwerte identisch sind. Ist dies der Fall kann davon ausgegangen werden, dass die Nachricht nicht verfälscht wurde. Bei nicht identischen Hashwerten wurde die

[17] www.datenschutzbeauftragter-info.de/bitcoin-technische-grundlagen-der-kryptowaehrung
[18] www.schnatterente.net/software/was-ist-eine-digitale-signatur
[19] www.globalsign.com/de-de/digitale-signaturen/was-sind-digitale-signaturen/ abgerufen

Nachricht manipuliert.[20] Den Ablauf einer digitalen Signatur kann man in Abbildung 3-2 erkennen.

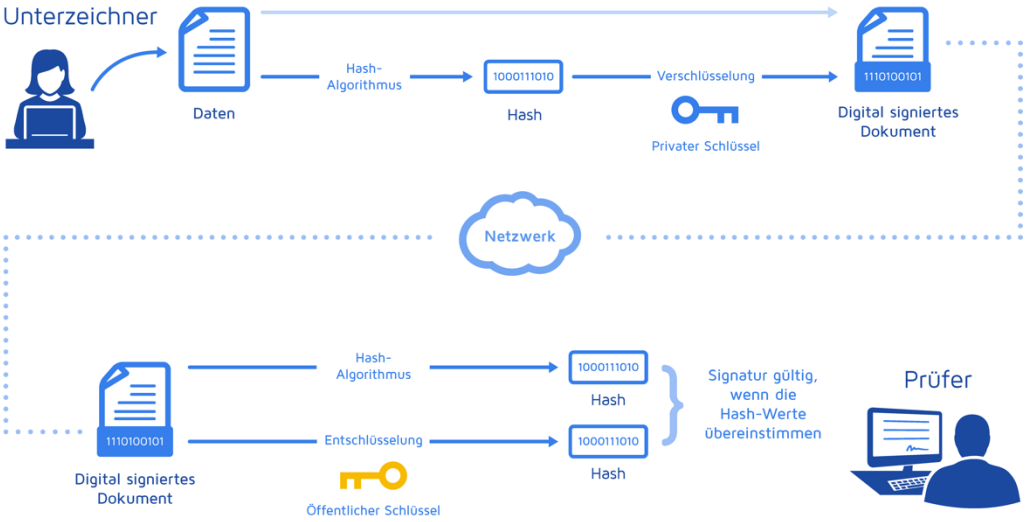

Abbildung 3-2: Darstellung einer digitalen Signatur[21]

3.3 Funktionsweise der Blockchain

3.3.1 Distributed Ledger Technology

Distributed Ledger bedeutet aus dem Englischen übersetzt etwa so viel wie dezentralisiertes Konto. Diese Beschreibung kommt daher, dass die DLT ein Netzwerk ist, bei dem die Daten verteilt (distributed) organisiert sind. Anders ist es bei gewöhnlichen Datenbanken, bei denen Daten auf zentralen Servern gespeichert werden und von einer administrativen Instanz verwaltet werden. Das besondere Merkmal der DLT ist das Fehlen einer zentralen Instanz, welche die Daten administriert. Die Aufgabe der Instanz, Informationen über Daten und deren Transfer wird hier von der Technologie selbst geregelt. Blockchain ist die DLT, welcher der Kryptowährung Bitcoin zugrunde liegt.[22] In Abbildung 3-3 kann man sowohl ein distributed Network, als auch ein centralized- und decentralized Network erkennen.

[20] www.schnatterente.net/software/was-ist-eine-digitale-signatur
[21] www.docusign.de/wie-es-funktioniert/elektronische-signatur/digitale-signatur/digitale-signatur-faq
[22] www.btc-echo.de/tutorial/was-ist-proof-of-stake/

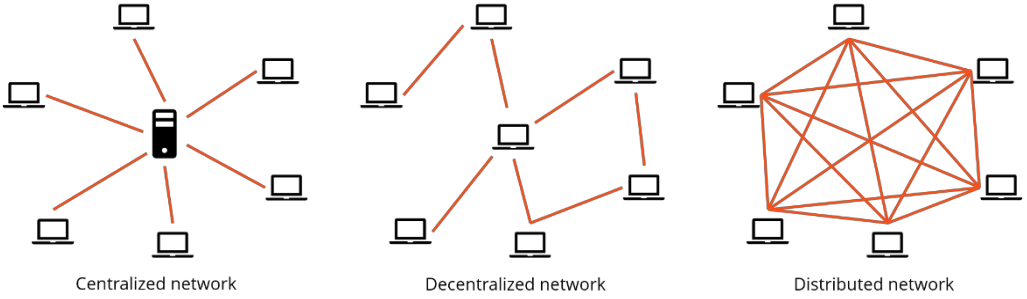

Abbildung 3-3: Darstellung unterschiedlicher Netzwerkstrukturen[23]

3.3.2 Peer to Peer (Dezentrales Netzwerk) Netzwerkarchitektur

Die Blockchain- Technologie zeichnet sich u.a. durch ihre Dezentralität aus, welche durch eine P2P Netzwerkarchitektur gewährleistet werden soll. P2P ist ein System das zur Kommunikation zwischen gleichberechtigten Netzwerkteilnehmern dient. Dieses System ist selbstorganisierend und bedarf an keiner zentralen Kontroll- oder Steuerinstanz, weshalb es auch dezentrales Netzwerk genannt wird. Ressourcen und Daten können zwischen allen Teilnehmern getauscht werden ohne, dass diese zunächst über einen Server umgeleitet werden. Jeder Teilnehmer kann Daten und Ressourcen sowohl senden als auch empfangen. Aufgrund dessen, dass es keinen Administrator oder Netzwerkverwalter gibt, muss jeder Netzwerkteilnehmer selbst entscheiden welche Daten und Ressourcen er freigeben möchte. Transaktionen werden nicht auf zentralen Datenbanken, sondern auf den Rechnern von allen Teilnehmern des Netzwerkes, welche auch als Nodes bezeichnet werden gespeichert. Ein wichtiges Merkmal der Blockchain ist, dass die Transaktionen die über ein P2P Netzwerk getätigt werden, von allen Teilnehmern dieses Netzwerkes einsehbar und zurück verfolgbar sind.[24] Abbildung 3-4 zeigt eine P2P Netzwerkarchitektur.

[23] ethereum-base.com/blockchain

[24] bitcoin-live.de/was-ist-bitcoin/

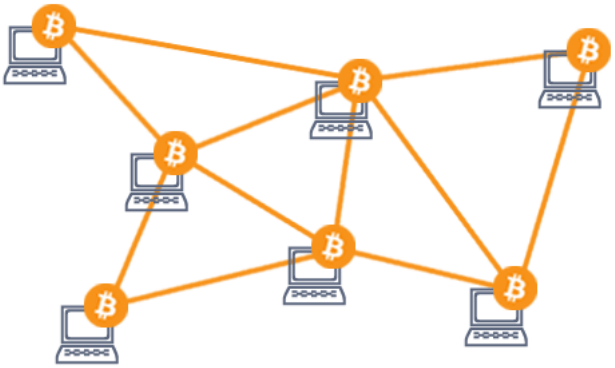

Abbildung 3-4: P2P Netzwerkarchitektur[25]

Je mehr Teilnehmer das P2P Netzwerk hat, desto widerstandsfähiger ist es gegenüber Ausfällen einzelner Systeme. Jeder zusätzliche Teilnehmer bringt mehr Ressourcen und Daten in das Gesamtsystem ein, weswegen eine höhere Leistungsfähigkeit zugrunde liegt. Dadurch das jeder Teilnehmer des P2P Netzwerkes dieselben Informationen vorliegen hat, ist das System vor Manipulationen geschützt, weil diese bei allen Teilnehmern durchgeführt werden müssten um erfolgreich zu sein. Jeglicher Versuch der Zensur durch zentrale Institutionen kann die Speicherung und Verbreitung der Daten nicht aufhalten.[26]

3.3.3 Konsensmechanismen

Alle Vorgänge im Netzwerk, wie z.B. Zahlungen, werden von allen Teilnehmern des Netzwerkes bestätigt. Aus diesem Grund gibt es keine zentrale kontrollierende Instanz welche die Ereignisse bestätigen muss. Soll z.B. eine Zahlung validiert werden, liegt die Entscheidung bei der Mehrheit der Teilnehmer. Es gibt mehrere Mechanismen um einen Konsens zu gestalten. Jede Blockchain muss einen Mechanismus wählen, der die Übereinstimmung aller Teilnehmer mit einer Wahrheit über ihre Daten sicherstellt.[27]

Der PoW Mechanismus beschreibt die Notwendigkeit, dass ein Teilnehmer im Netzwerk ehrliche und beweisbare Arbeit verrichtet haben muss um eine Anzahl von Transaktionen bestätigen zu können. Für diese Arbeit wird er anschließend

[25] www.finanziator.de/geldanlagen/bitcoin-einfach-erklaert

[26] blog.frankfurt-school.de/wp-content/

[27] blog.codecentric.de/2017/10/konsens-mechanismen-blockchain

angemessen belohnt. Proof of Work ist vor allem bei Kryptowährungen das gängigste Verfahren. Der Nachteil von PoW ist, dass die benötigte elektrische Energie die Umwelt extrem belastet. Der Energieverbrauch in Deutschland könnte über 3 % der benötigten Energie beim Bitcoin Mining gedeckt werden.[28]

Der zweite populäre Mechanismus ist der PoS Mechanismus. Dieser basiert nach der Grundidee auf einer stark verteilten Rechenleistung über viele Teilnehmer im gesamten System. Der Hintergrund hierbei ist, die Sicherheit und Stabilität des Netzwerkes zu gewährleisten. Die Validierung der Transaktion auf der Blockchain durch einen einzelnen Teilnehmer basiert auf seinem wertmäßigen Anteil am Netzwerk. Wenn ein Teilnehmer zum Beispiel 0,1% aller Einheiten einer Kryptowährung besitzt bedeutet es, dass dieser dann auch 0,1% aller Transaktionen validieren kann. PoS benötigt aufgrund der verteilten Rechenleistung weniger Strom als der PoW Mechanismus, weshalb der PoS Mechanismus auch umweltfreundlicher ist. Der Nachteil bei diesem Mechanismus liegt darin, dass es zu einer 51% Attacke kommen könnte. Im Detail bedeutet dies, dass wenn jemand über die Hälfte des Gesamtvermögens der jeweiligen Coins besitzt, kann die Blockchain und somit auch vergangene Transaktionen manipulieren.[29]

3.3.4 Das Double spending Problem

Der überwiegende Teil der Kryptowährungen sind dezentral organisiert. Diese Eigenschaft ermöglicht Räume für Manipulationen, insbesondere für das Double Spending. Ein Angreifer versucht hierbei einen Coin mehrfach auszugeben. Angenommen Bob möchte von Alice einen PC für 200 Euro kaufen. Bob initiiert die Transaktion T1, welche Alice 200 Euro senden soll. Sobald die Transaktion zu Alices Knotenpunkt weitergeleitet wurde, versendet er die Ware. Bob initiiert daraufhin eine zweite Transaktion T2, welche 200 Euro an sein eigenes, zweites Konto sendet. Nun besteht die Möglichkeit, dass T2 im Netzwerk schneller weitergeleitet und somit noch vor T1 vom Netzwerk akzeptiert wird. Soll T1 jetzt verifiziert werden, ist das Konto von Bob wegen T2 nicht gedeckt und T1 wird zurückgewiesen. Das Ergebnis ist, dass Alice die Ware bereits verschickt bevor T1 zurückgewiesen wurde. Bob bekommt die

[28] blog.codecentric.de/2017/10/konsens-mechanismen-blockchain

[29] coin-hero.de/proof-of-work-vs-proof-of-stake/

Ware, hat aber nicht dafür gezahlt.[30] Abbildung 3-5 stellt das Double Spending Problem dar.

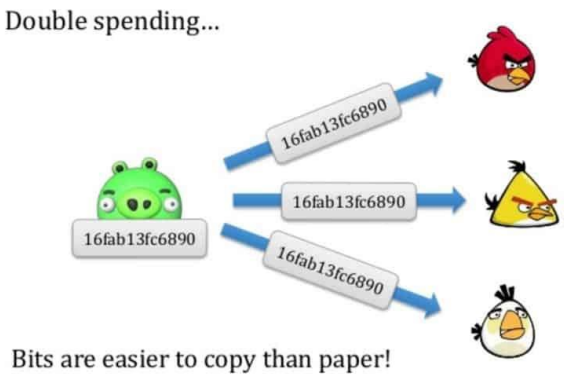

Abbildung 3-5: Darstellung des Double Spending Problems[31]

3.4 Mögliche Anwendungsfälle der Blockchain-Technologie

Die Blockchain Technologie hat aufgrund ihrer Vorteile der Integrität der Daten, Zuverlässigkeit, Geschwindigkeit und Transparenz enormes Potential, weshalb die Technologie auch viele Anwendungsmöglichkeiten aufweist.

Neben Kryptowährungen wie Bitcoin, Ethereum und viele mehr, wird die Blockchain Technologie auch in der Finanzwelt eingesetzt. Wenn es um Banktransaktionen geht, kann die Verschlüsselung dafür sorgen, dass die Daten sicher sind. Darüber hinaus kann die gegenseitige Verifizierung Fehler sowohl nach innen als auch nach außen minimieren. Es ist möglich Zahlungen international, ohne Beteiligung einer Instanz wie eine Bank, abzuwickeln und dadurch die Transaktionskosten verringern. Dementsprechend wird auch die Geschwindigkeit der Überweisungen erhöht. Eine weitere Möglichkeit ist der Schutz vor Geldwäsche. Abgeschlossene Verträge sind transparent und werden genauestens durch die Technologie aufgezeichnet. Welche Transaktion an welche Person getätigt wurde ist somit leicht identifizierbar. Versuche der Geldwäscherei können identifiziert und verifiziert werden, weshalb es zu einer aktiven Unterbindung kommen kann. Beim Immobilienkauf können Betrüger gestoppt

[30] thecoinscout.com/krypto-lexikon

[31] coinsutra.com/bitcoin-double-spending

und Verkaufsabwicklungen vereinfacht werden. Auch im Gesundheitswesen kann die Blockchain Technologie zur Speicherung von sensiblen Daten genutzt werden. Patientenakten, Berichte und vieles mehr können in der Blockchain gespeichert und an berechtigte Personen zur Einsicht freigeschaltet werden. Für die Energiewende kann die Blockchain Technologie eine entscheidende Rolle spielen. Durch die Transparenz und Nachverfolgbarkeit können z.B Solaranlagen effizienter abrechnen. Wenn genug Daten vorhanden ist, wäre es sogar möglich mit Informationen wie eines Geburtsdatums die Person zu identifizieren und zu verifizieren. Personalausweise oder Führerscheine wären immun gegenüber Fälschungen.[32]

[32] morethandigital.info/blockchain-moeglichkeiten-und-anwendungen-der-technologie/

4 Bitcoin Allgemein

4.1 Definition von Bitcoin

Der Begriff Bitcoin kommt ursprünglich aus dem englischen und bedeutet in der deutschen Übersetzung digitale Münze. Bei Bitcoin handelt es sich um eine dezentral organisierte virtuelle Währung. Die Währung Bitcoin kann sowohl gekauft als auch verkauft werden. Sein Wert lässt sich aus Angebot und Nachfrage ermitteln.[33] Bitcoin ist die älteste Digitalwährung welche auf der Blockchain- Technologie basiert. Diese Technologie ist eine Open-Source Software, weshalb es jedem möglich ist nachzuvollziehen was genau die Software macht. Eins der wichtigsten Charakteristika des Bitcoins ist seine Dezentralität. Das Bitcoin- Netzwerk wird von keiner zentralen Instanz kontrolliert. Keine Zentralbank und kein Staat hat die Möglichkeit die Geldmenge zu steuern oder zu beeinflussen. Nutzer der Bitcoin können mehrere Konten (Wallets) besitzen, welche keinen Namen, Wohnadressen oder anderen sensiblen Informationen zugeordnet sind. Dementsprechend ist Bitcoin als pseudoanonym zu betrachten. Jede einzelne Transaktion in der Blockchain wird im Netzwerk gespeichert, weshalb Bitcoin Zahlungen zu 100% transparent sind. Wenn man eine internationale Überweisung tätigen möchte kann es dazu kommen, dass Banken hohe Transaktionskosten erheben. Transaktionen über Bitcoin spielt die Entfernung keine Rolle. Es entfallen lediglich geringe Transaktionsgebühren. Darüber hinaus sind Zahlungen über Bitcoin aufgrund des fehlenden Mittelsmannes sehr schnell. Eine Überweisung erfolgt ohne Umwege von A nach B.[34]

4.2 Geschichte hinter Bitcoin

Im Jahr 2008, veröffentlichte eine Person oder eine Gruppe mit dem Pseudonym „Satoshi Nakamoto“ ein Whitepaper, welches das Konzept einer dezentral organisierten virtuellen Währung beinhaltete. Nakamoto schrieb: „Benötigt wird ein elektronisches Zahlungssystem, das auf einem kryptografischen Beweis anstelle von Vertrauen basiert, und es zwei Parteien erlaubt, direkt miteinander zu handeln“.[35]

[33] boerse.ard.de/boersenwissen/boersenlexikon/bitcoin138.html

[34] www.btc-echo.de/tutorial/was-ist-proof-of-stake/

[35] www.handelsblatt.com/finanzen/maerkte

Zunächst einmal bestand das Bitcoin- Netzwerk aus 50 Bitcoins, welches auch „Genesis Block“ genannt und am 2 Januar 2009 von Satoshi Nakamoto generiert wurde. Jedoch wurde die maximale Anzahl an allen verfügbaren Bitcoins auf 21 Millionen Einheiten begrenzt, wobei die Coins in kleinere Einheiten aufgeteilt werden können. Die kleinste Einheit beträgt ein Hundertmillionstel und wird Satoshi genannt.[36]

Im Anschluss an die Veröffentlichung des „Genesis Blocks“ entstand im Oktober 2009 der erste Wechselkurs auf Dollar-Basis. Der erste Wechselkurs wurde mit 1309,03 BTC für 1 US-Dollar festgelegt. Der Wert eines Bitcoins betrug also 0,08 Cent. 2009 betrug der Gesamtwert aller Bitcoins 277.000 US-Dollar.[37]

Die erste Transaktion mit Bitcoin wurde am 22.Mai 2010 von einer Person namens Laszlo Hanecyz, einem Softwareprogrammierer aus Florida durchgeführt. Laszlo erwarb für 10.000 Bitcoins zwei Pizzen.

Drei Jahre später erreichte die Marktkapitalisierung des Bitcoins umgerechnet 2.533 Milliarden Dollar.[38] Nachdem die Bitcoin- Börse Mt. Gox Anfang März 2014 Insolvenz ging und die Onlineplattform „Silk Road“, welche ein Portal für den Drogenhandel im Internet war und als Zahlungsmittel ausschließlich Bitcoin akzeptierte Zwangs geschlossen wurde hat der Bitcoin stark an Popularität in der Öffentlichkeit verloren. Darüber hinaus hatten auch externe, von der digitalen Welt unabhängige Entwicklungen den Kurs des Bitcoins beeinflusst. So haben Ereignisse wie die Zypernkrise im März 2013 und die Griechenlandkrise, welche eine seit 2010 laufende Krise meint, einen Einfluss auf den Wechselkurs. Trotz der sinkenden Nachfrage an Bitcoin im Anschluss an die Krisen, nahm die Anzahl an Bitcoin- Transaktionen pro Tag stetig zu, welches in der Abbildung 4-1 verdeutlicht wird.

[36] www.hotelier.de/lexikon/b/bitcoin-definition-geschichte
[37] itfconsult.wordpress.com/2013
[38] itfconsult.wordpress.com/2013

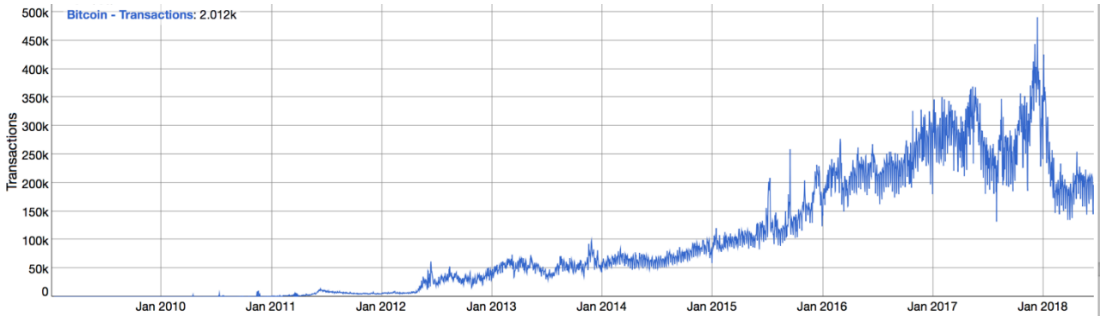

Abbildung 4-1: Anzahl der Bitcoin Transaktionen[39]

Anfang 2013 wurden ca. 31.000 Transaktionen täglich registriert. Während im Januar 2017 noch täglich ca. 320.000 Transaktionen pro Tag durchgeführt worden sind, beträgt die Anzahl der Transaktionen im Dezember desselben Jahres ca. 405.000 Transaktionen.[40] Das Transaktionsvolumen betrug Anfang 2013 lediglich ca. 270.000 US- Dollar. In den nächsten Jahren hat sich das Transaktionsvolumen jedoch relativ konstant gehalten, bis es gegen Ende 2017 rapide gewachsen ist und mit einem Volumen von 1.883.000.000 US-Dollar sein absolutes Maximum erreicht hat (vgl.Abb.4-2).

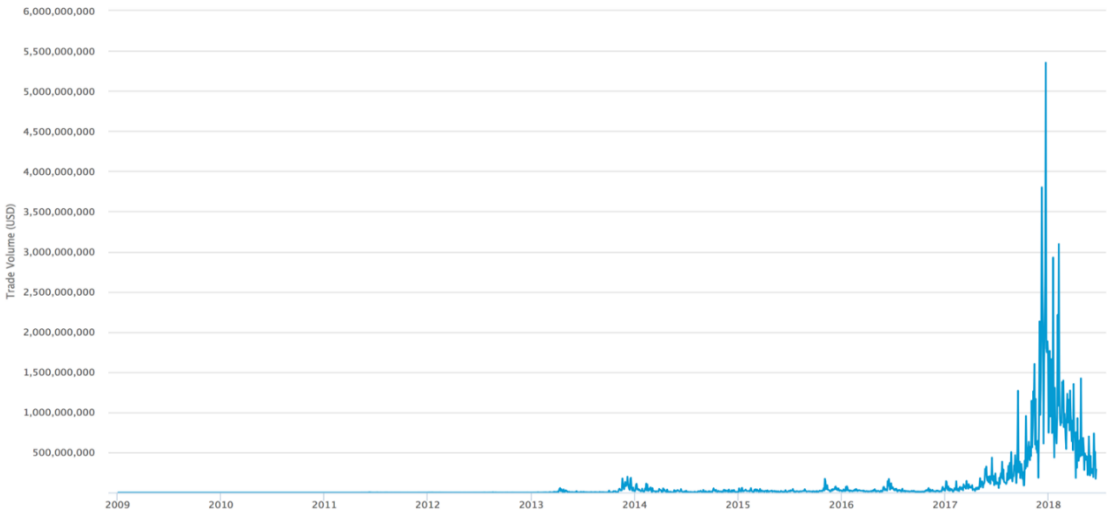

Abbildung 4-2: Transaktionsvolumen vom Bitcoin[41]

[39] bitinfocharts.com/de/bitcoin

[40] bitinfocharts.com/comparison

[41] www.blockchain.com/de/charts

Laut einem Bericht der Juniper Research Gruppe lag die Anzahl der aktiven Nutzer von Bitcoin schätzungsweise bei lediglich 1.3 Mio.[42] Aktuell schätzen Wissenschaftler die Zahl der Bitcoin-Nutzer zwischen 2.9 und 5.8 Millionen. Die genaue Anzahl ist aufgrund der Tatsache, dass viele Nutzer eine VPN- Verbindung nutzen schwierig zu ermitteln.[43]

4.3 Bitcoin-Adressen und Wallets

Der Begriff „Wallet“ kommt aus dem englischen und bedeutet im deutschen „Geldbörse“ oder „Portemonnaie“. Unter einem Wallet versteht man ein Programm, welches als virtuelle Geldbörse dient und Bitcoins bzw. die entsprechenden privaten Schlüssel aufbewahrt und verwaltet. Die primäre Aufgabe eines Wallets ist es, Bitcoins zu senden und zu empfangen. Darüber hinaus hat der Nutzer die Möglichkeit seinen virtuellen Kontostand zu überprüfen und seine Schlüssel zu verwalten. Im Prinzip ist ein Wallet als Client, wie z.B. Gmail oder Outlook, welche zum Versenden von Mails genutzt werden zu verstehen. Mittlerweile gibt es ein Angebot von über 20 verschiedenen Bitcoin- Wallets. Es wird zwischen Clients, welche man unterwegs (iOS, Android) nutzen und Clients, welche für den Desktop (Windows, Mac, Linux) entwickelt wurden unterschieden. Mittlerweile gibt es auch Hardware- Wallets oder aber auch Webseiten, welche als Wallet dienen können.[44]

Jede Wallet- Art hat verschiedene Vor- und Nachteile. Jedoch gibt es 5 Grundfunktionen die alle Wallets beinhalten. Alle Wallets müssen Bitcoins an eine Adresse senden und Adressen als Zeichenfolge oder QR- Code anzeigen können. Darüber hinaus müssen sie Nachrichten signieren können, um zu beweisen, dass man der Besitzer einer Adresse ist. Die Sicherung des privaten Schlüssels und die Verschlüsselung des Wallets mit einem Passwort sind ebenfalls Bestandteil dieser 5 Grundfunktionen. Natürlich muss jede Wallet- Art auch Adressen in einem Adressbuch speichern können. Jeder Nutzer muss individuell, je nachdem was er mit den Bitcoins vorhat entscheiden, welche Wallet- Art für ihn in Frage kommt.[45]

[42] www.juniperresearch.com/press/press-releases
[43] www.btc-echo.de/tutorial/was-ist-proof-of-stake/
[44] www.gevestor.de/details
[45] en.bitcoin.it/wiki/Anonymity

Im Rahmen dieser Arbeit werden lediglich die gängigsten Wallet- Arten vorgestellt, da das Eingehen auf über 20 Wallet- Arten den Rahmet sprengen würde.

4.3.1 Bitcoin- Adresse

Eine Bitcoin- Adresse kann von der Grundfunktion her mit einer E-Mail-Adresse verglichen werden. Ihr Aufgabe ist es Bitcoins zu senden und zu empfangen. Eine Adresse ist eine Kette aus 27-34 alphanumerischen Zeichen, die mit einer 1 oder 3 beginnen. Die Erzeugung einer Adresse ist beliebig und kostenlos. Ein Beispiel für eine Bitcoin- Adresse ist 1P82rBjJMDFSay2Rqkx1bydDRVh5QnGKkZ. Dabei bietet es sich für die Anonymität an, für jede Transaktion eine neue Adresse zu verwenden. Die Adressen können auch offline erzeugt werden.[46]

4.3.2 Hardware- Wallets

Unter einem Hardware- Wallet versteht man ein Gerät, welches für die Lagerung von Kryptowährungen wie Bitcoin, Ethereum, Litecoin oder Dash verwendet wird. Diese Wallet- Art wird als besonders sicher eingestuft, da die Wahrscheinlichkeit für einen Hackangriff nahezu 0% beträgt. Dies wird dadurch gewährleistet, dass der private Schlüssel zu den jeweiligen Währungen durch die Verbindung mit einem Computer oder einem Smartphone auf das Hardware- Wallet gespeichert werden und diese auch niemals verlassen. Die privaten Schlüssel, welche in den meisten Fällen aus einer Folge von 24 Wörtern (Seed) besteht, werden beim Speichern auf das Gerät zufällig generiert. Damit eine Transaktion reibungslos ausgeführt werden kann, muss durch digitale Signaturen sichergestellt werden, dass es sich auch tatsächlich um die digitale Währung des Versenders handelt. Ein Hardware- Wallet bekommt alle Informationen zur Transaktion von dem Computer oder dem Smartphone zugeschickt. Der Versender kann die Transaktion anschließend durch physisches Betätigen von Tasten, welches als digitale Signatur zu verstehen ist, zurück an den Computer senden. Der Computer versteht diese Aktion als eine Bestätigung und führt die Transaktion aus. Gängige Hardware- Wallets sind der Ledger Nano S, Trezor One und Ledger Blue.

[46] help.wirexapp.com/hc/de/articles

4.3.3 Web- und Mobile Wallets

Eine weitere Wallet- Art sind die sogenannten Web- Wallets, welche sich dadurch kennzeichnen, dass sie den privaten Schlüssel online auf einem Server speichern. Diese Server werden von externen Anbietern verwaltet. Sobald ein Nutzer eine Internetverbindung besitzt, kann er auf der ganzen Welt auf seine Bitcoins zugreifen und verwalten. Eine globale Verfügbarkeit wird also gewährleistet. Ob eine ausreichende Sicherheit auf dem jeweiligen Server vorhanden ist, kann der Nutzer nicht überprüfen und muss sein Vertrauen in die Hände externe Anbieter legen, da diese die privaten Schlüssel der Nutzer verwalten. Darüber hinaus haben eben diese Anbieter auch einen vollständigen Zugriff auf die Bitcoin- Bestände der Nutzer. Jedoch hat man bei Web- Wallets, das Risiko eines Hardwaredefektes wie bei Hardware- Wallets ausschließen. Zwei der bekanntesten Web- Wallets sind zum einen die Bitcoin- Börse Coinbase, welche auch als Wallet genutzt werden kann und zum anderen Circle. In Europa können Bitcoin Nutzer auch ihre Kreditkarte verwenden um Bitcoins zu erwerben.[47] Nicht wenige Bitcoin- Nutzer wollen unterwegs Bitcoin- Überweisungen tätigen. Egal ob beim Shoppen oder in der Mittagspause, die praktischste Möglichkeit bieten hier die Mobile- Wallets. Mobile- Wallets werden direkt als Applikation auf dem Smartphone installiert. Der private Schlüssel befindet sich beim Mobile- Wallet direkt auf dem Smartphone. Transaktionen werden innerhalb von wenigen Sekunden durchgeführt. Hierbei kann man Mobile- Wallets nicht gleichrangig mit vollwertigen Bitcoin- Clients betrachten, da die mehrere Gigabyte große Blockchain gedownloadet werden müsste. Um dieses Problem zu umgehen, verwenden so gut wie alle Mobile- Wallets die SPV. Es wird lediglich ein kleiner Teil der Blockchain, welches für eine sichere Transaktion vollkommen ausreichend ist runtergeladen. Gängige Mobile- Wallets sind Jaxx, Bread Wallet, Bitcoin Wallet und Blockchain.[48]

[47] www.btc-echo.de/tutorial/was-ist-proof-of-stake/

[48] www.btc-echo.de/tutorial/was-ist-proof-of-stake/

4.4 Bitcoin Clients

4.4.1 Bitcoin Core Client/ Full- Node Client

Der Bitcoin Core Client wurde von Satosohi Nakamoto Anfang 2009 als Open- Source Software veröffentlicht. Dieser wurde vollständig in der Programmiersprache C++ geschrieben. Er ist für die Betriebssysteme Windows, Mac, Ubunutu und andere Linux- Betriebssysteme verfügbar. Der Bitcoin Core bietet die höchste Netzwerksicherheit und besitzt alle grundlegenden Funktionen. Aufgrund dessen, dass die gesamte Blockchain auf dem einzelnen Rechner gespeichert wird, benötigt der Client viel Festplatten- und Arbeitsspeicher (mehr als 40 GB). Der Ladevorgang kann dementsprechend sehr lange dauern. In der Regel werden, wenn der Client regelmäßig in Betrieb genommen wird, nur mehr die fehlenden Blöcke runtergeladen. Damit entsteht ein vollwertiger Netzknoten (Full-Node) im Bitcoin- Netzwerk. Dadurch, dass jeder Full-Node lokal immer eine komplette und ständig aktualisierte Kopie der Blockchain speichert, wird das Bitcoin-Netzwerk durch jeden zusätzlichen Full-Node stabiler gegen Double-Spending-Probleme.[49]

4.4.2 Thin-/ Light- Clients

Möchte der Nutzer nicht die gesamte Bitcoin Core installieren, hat er die Möglichkeit eine abgemagerte Form, die sogenannten Thin-/ Light Clients auf seinem Rechner zu installieren. Thin-/ Light bezieht sich dabei auf die Größe/Menge der auf dem Computer abgespeicherten Blockchain. Diese Clients speichern nicht die gesamte Blockchain, sondern eigentlich nur die Block-Header (darin befinden sich Hashes aller in einem Block verarbeiteten Transaktionen) der einzelnen Blöcke und die Transaktionsdaten der eigenen Adressen. Aufgrund der abgemagerten Form, ist die benötigte Ladezeit und der benötigte Speicherplatz weit geringer als beim gesamten Bitcoin Core. Ein Nachteil von Thin-/ Light Clients ist, dass diese über eine geringere Netzwerksicherheit verfügen.[50]

[49] Vgl. Sixt, E. (2016, S. 35)
[50] Vgl. Sixt, E. (2016, S. 36)

4.5 Transaktion von Bitcoin

4.5.1 Bitcoin Transaktion

Unter Bitcoin- Transaktion versteht man den Transfer eines Betrags zwischen Bitcoin-Wallets. Die gesamte Transaktion geschieht in einer P2P Netzwerkarchitektur. Es gibt keine zentrale Kontroll- und Steuerinstanz. Alle jemals getätigten Transaktionen im Bitcoin- Netzwerk können von allen Nutzern über die Blockchain eingesehen werden. Abbildung 4-3 veranschaulicht den Ablauf einer Bitcoin- Transaktion.

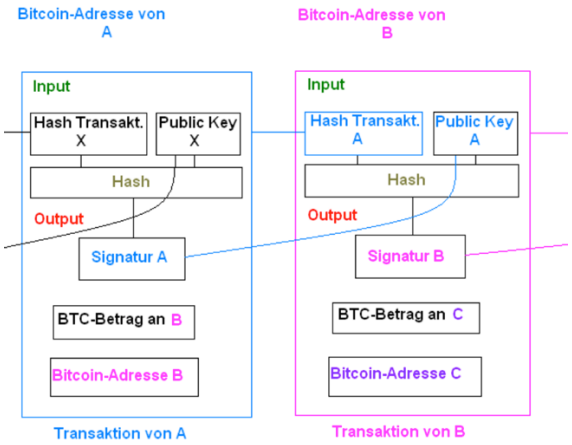

Abbildung 4-3: Darstellung einer Bitcoin-Transaktion[51]

Wenn Alice(A) Bitcoins an Bob(B) versendet, dann enthält diese Transaktion drei Informationen. Zunächst einmal den Input, das eine Aufzeichnung darüber ist, welche Sender-Adresse zuvor Alice diese Bitcoins geschickt hat. Darüber hinaus eine Menge, welche die Menge an Bitcoins, die Alice an Bob schicken möchte beinhaltet und anschließend einen Output, welches die Bitcoin-Adresse von Bob also die Empfängeradresse ist.

Soll eine neue Bitcoin- Adresse angelegt werden, generiert der Bitcoin- Client unter Nutzung des auf elliptischen Kurven beruhenden ECDSA-Algorithmus ein Schlüsselpaar im Sinne der asymmetrischen Verschlüsselung. Dieses Schlüsselpaar

[51] menshelp.cc/dokuwiki/doku.php?id=bitcoin

besteht aus dem öffentlichen Schlüssel (Public Key) und dem geheimen Schlüssel (Private Key).[52]

Eine Bitcoin-Transaktion ist also eine Fortführung vorangegangener Transaktionen. Durch Transaktionen werden einer oder mehreren Adressen Bitcoins gutgeschrieben, die selbst wiederum von einer oder mehrerer Adressen aus dem Bitcoin-Netzwerk stammen. Sie kann also aus entweder einem oder mehreren Outputs bestehen. (vgl. Abb. 4-4)

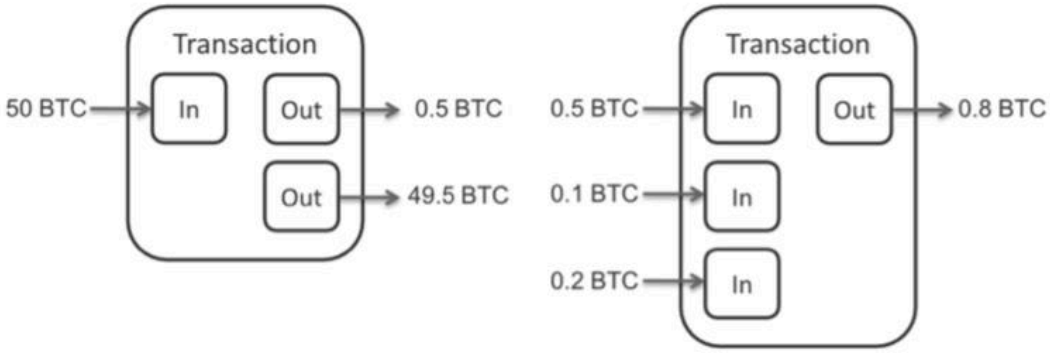

Abbildung 4-4: Darstellung der Mehrfachausgabe von Bitcoin[53]

Die Inputs verweisen dabei auf die Outputs vergangener Transaktionen, welche dem Aussteller der aktuellen Transaktion geschickt wurde. Diese werden zusammengerechnet und bilden die Gesamtmenge an Bitcoins, die auf die Outputs verteilt werden kann. Wie man in der Abbildung 4-4 erkennen kann, können Bitcoins an mehrere Empfänger versendet werden.[54]

Es kann jedoch vorkommen, dass die Summe an Bitcoins bei den Inputs sich von der Summe bei den Outputs unterscheidet. In diesem Fall wird die Differenz als Transaktionsgebühr interpretiert und denjenigen zugeschickt der die Transaktion bestätigt.

[52] Vgl. Sixt, E. (2016, S. 37)
[53] www.heikofrieberg.com/Das-Bitcoin-Buch.pdf
[54] Vgl. Karame (2016, S. 36)

Damit ein Nutzer nun Bitcoins an jemanden senden kann, nutzt dieser seinen privaten Schlüssel, um eine Nachricht mit dem Input, der Menge und dem Output zu signieren. Anschließend versendet er seine Bitcoins von seinem jeweiligen Wallet an das Bitcoin- Netzwerk.

4.5.2 Verifizierung von Transaktionen

Im Netzwerk wird die Transaktion durch Bitcoin- Miner verifiziert. Ein Bitcoin-Miner kann als Schürfer von „digitalem Geld“ beschrieben werden. Die Miner übernehmen im Bitcoin-Netzwerk bestimmte Aufgaben und werden dafür mit neu erzeugten Bitcoins belohnt. Um erfolgreich schürfen zu können benötigen Miner optimierte Hochleistungscomputer. Erst dann können sie neue Bitcoin-Transaktionen validieren und sequenzieren. Eine vollständige Validierung beinhaltet 18 technische Einzelprüfungen. Die Prüfung von Signatur und Saldo sind der eigentliche Kern dieser Prüfungen. Um die Signatur zu prüfen benötigen die Miner lediglich den Öffentlich verfügbaren Public Key. Mit diesem können sie überprüfen, ob die Transaktion tatsächlich vom Sender ausgelöst wurde. Der Sender kann zum gleichen Zeitpunkt mit seinem Private Key die Transaktionen signieren. Bitcoin-Konten können nicht überzogen werden, weshalb bei jeder Transaktion geprüft werden muss, ob der Sender über den notwendigen Betrag auf seinem Public Key verfügt. Diese Prüfung geschieht dadurch, dass jeder Zahlung die Transaktionshistorie mitgegeben wird, welche den Kontosaldo begründen. Vereinfacht lässt sich sagen, dass mit jeder Transaktion ein Kontoauszug des Senders mitgeschickt wird. Abbildung 4-5 zeigt einen Bitcoin-Kontoauszug.

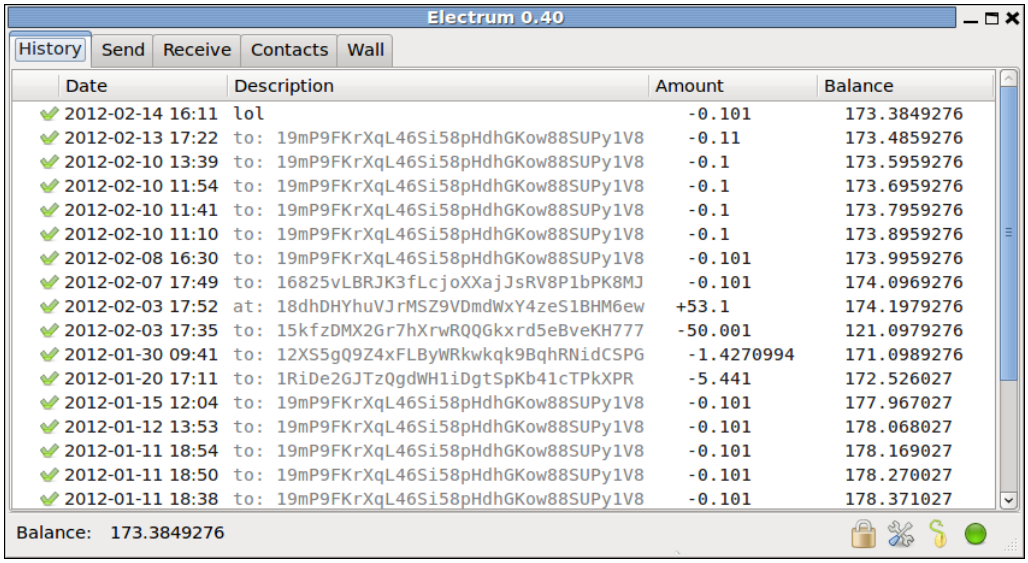

Abbildung 4-5: Darstellung eines Bitcoin-Kontoauszugs[55]

Wenn eine Transaktion die Validierung bestanden hat, wird sie von Minern einem noch unbestätigten Block zugewiesen. Die eigentliche Herausforderung liegt darin, den unbestätigten Block zu bestätigen und der Blockkette hinzuzufügen. Es kommt zu einer Transaktionssequenz, dessen Einhaltung von enormer Wichtigkeit ist. Dadurch wird gewährleistet, dass der gleiche Bitcoin nicht mehrfach ausgegeben werden kann (Double-Spending-Problem).

Der Kern des Bestätigungsprozesses ist die Hash-Funktion. Das Bitcoin-Protokoll verwendet den Algorithmus SHA-256. Diese Funktion gibt aus beliebig vielen Input-Werten einen komplett zufälligen alphanumerischen String von 64 Zeichen zurück. Es ist nahezu unmöglich, aus einem gegebenen Hast-Wert auf den Input zurückzuschließen. Sobald der Inputwert minimal geändert wird, ergibt sich ein vollkommen anderer Hash-Wert.

Wollen Miner jetzt neue Transaktionen sequenzieren, müssen sie alle Transaktionen in einem unbestätigten Pool paarweise zu einem neuen Input für die Hash-Funktion kombinieren. Am Ende diese Kette steht ein eindeutiger Hash-Wert, für den ganzen unbestätigten Block. Dieser nennt sich Root-Hash. Dieser wird wiederum mit dem Block-Hash des letzten bestätigten Blockes in der Kette verhaschte. Es entsteht ein

[55] en.bitcoin.it/wiki/Anonymity

neuer Hash-Wert. Welcher Challenge genannt wird. Der Challenge ist die Grundlage für den Arbeitsnachweis (PoW) der Miner.[56]

4.5.3 Anonymität im Bitcoin-Netzwerk

Die Bitcoin-Technologie kann Anonymität stark unterstützen. Dennoch kann die aktuelle Umsetzung der Technologie nicht als stark anonym betrachtet werden. Das Hauptproblem liegt darin, dass jede Transaktion öffentlich protokolliert wird. Jeder kann den Fluss von Bitcoins, welche von Adresse zu Adresse fließen einsehen. Die Blöcke der Blockchain protokollieren die gesamte Historie der Bitcoin-Adressen, an die ein Bitcoin gesendet wurde. Aufgrund der Tatsache, dass die Adressen lediglich eine Aneinanderreihung von Zufallszahlen sind, ist es nahezu unmöglich mit dieser Information einen Nutzer ausfindig zu machen. Wenn jedoch eine der Adressen in der Vergangenheit oder in der Zukunft einer Transaktion an eine tatsächliche Identität gebunden werden kann, besteht die Möglichkeit, von diesem Punkt aus anzusetzen und abzuschätzen wer alle anderen Adressen besitzen darf. Somit ist jegliche Privatsphäre verloren. Einige Angriffsmöglichkeiten wären z.B. Netzwerkanalysen, Überwachung oder aber auch das einfache googeln der Adresse. Um sich vor derartigen Angriffen zu schützen wird empfohlen für jede Transaktion eine neue Adresse zu verwenden. Um den Sachverhalt in die Praxis übertragen zu können, nehmen wir an, dass Bob sowohl eine Website zum Verkauf von Kosmetikartikeln als auch eine Website, die Menschen in die Falle locken soll betreibt. Wenn Alice nun von der Website für Kosmetikartikel einkauft und nun die gleichen Bitcoins verwendet um von der „Fallen-Website“ einzukaufen, kann der Angreifer durch die Historie beweisen, dass diese beiden Transaktionen von derselben Person getätigt wurden.[57]

4.5.4 Transaktionsgebühren

Aufgrund der rechenintensiven Prozesse bei Bestätigungen von Transaktionen, welche die Miner ausführen müssen, gibt es als eine Art von Entschädigung unterschiedliche Transaktionsgebühren. Diese sollen die hohen Strom- und Hardwarekosten decken. Miner erhalten aber auch einen garantierten festen Bitcoin Betrag, wenn sie das Minen erfolgreich abgeschlossen haben. Ein weiterer Grund für das Einführen von Transaktionsgebühren ist, dass es „theoretisch“ möglich wäre das

[56] finalix.ch/wp-content/

[57] en.bitcoin.it/wiki/Anonymity

Bitcoin-Netzwerk mit Teilnehmern zu überfluten. Durch eine Mindestgebühr wird verhindert, dass Millionen von Transaktionen versendet werden. Aktuell gibt es keine Regelung darüber, welche Mindestgebühr eine Transaktion beinhalten muss. Transaktionen ohne Gebühr werden seit spätestens 2016 nicht mehr von Minern verarbeitet und bestätigt. Wie hoch die Gebühr ist, hängt zum einen vom aktuellen Bitcoin-Kurs ab und zum anderen von der Größe der Bitcoin-Transaktion in Kilobyte. Je größer die Transaktion umso höher ist die Mindestgebühr. Die (relative) Mindestgebühr beträgt 0,00001BTC pro Kilobyte, wobei eine Transaktion im Schnitt eine Größe von 0,25 Kilobyte besitzt. Auch das Bitcoin-Netzwerk kann an seine Grenzen stoßen. Miner können nur eine bestimmte Anzahl von Transaktionen pro Zeitraum verarbeiten. Die Anzahl der Transaktionen nimmt mit der Zeit zu, weshalb Miner sich gezwungen fühlen, Transaktionen mit höheren Gebühren schneller zu verarbeiten und zu bestätigen. Es kommt wie im Jahr 2017 zu mehr Transaktionen als verarbeitet werden können. Dies wird in der Abbildung 4-6 verdeutlicht.[58]

Abbildung 4-6: Transaktionsgebühren im Bitcoin-Netzwerk[59]

Einige Zahlungsabwickler wie z-B. BitPay bieten ihren Nutzern Transaktionsbelege und Kaufbestätigungen von Webseiten an, die man mit einer normalen Bitcoin-Transaktion nicht erhalten würde. Hierfür legt der Kunde einen Artikel in den Warenkorb und geht anschließend zur Kasse. Wenn der Kunde nun Bitcoin als Zahlungsmittel auswählt, wird er auf die Seite von BitPay weitergeleitet. Nun loggt sich der Kunde mit seinem Benutzerkonto auf BitPay ein und tätigt die Zahlung. Nach

[58] bitcoin-für-anfänger.de/infos-und-anleitungen

[59] bitcoin-für-anfänger.de/infos-und-anleitungen/bitcoin-im-detail

der abgeschlossenen Zahlung wird der Kunde zurück auf die ursprüngliche Seite geleitet. Der Verkäufer bekommt von BitPay eine E-Mail mit der Bestätigung der Transaktion.[60]

4.6 Geldausschöpfung (Mining) von Bitcoin

Unter Mining versteht man „Erzeugen“ oder auch „Schürfen“ von Bitcoins. Bei diesem Prozess steht die Rechenleistung des jeweiligen Rechners im Vordergrund, welche für das Bitcoin-Netzwerk zur Verfügung gestellt wird. Die Miner werden für ihre Arbeit und den Aufwand des Minings mit einer Transaktionsgebühr belohnt. Aufgrund der Dezentralität des Bitcoin-Netzwerks, können sich Nutzer aus der ganzen Welt am Mining beteiligen. Jedoch gibt es eine begrenzte Anzahl an Bitcoins, um genau zu sein sind es 21 Millionen. Im Juli 2017 wurden bereits 16,43 Millionen Bitcoins geschürft. Aus diesem Grund stehen alle Miner miteinander in Konkurrenz.[61]

Technisch gesehen führt der Rechner eine kryptografische Hashfunktion beim Mining aus. Dieser wird Block-Header genannt. Für jeden neuen Hash benutzt die Mining-Software eine andere zufällig generierte Zahl für den Block-Header. Diese wird Nonce genannt. Anschließend wird basierend auf die Nonce eine Hashfunktion erstellt. Ein Beispiel für solch eine Hashfunktion wäre: 93ef6f358fbb998c60802496863052290d4c63735b7fe5bdaac821de96a53a9a.

Es handelt sich um eine sehr lange Hexadezimalzahl. Das bedeutet, dass die Buchstaben A-F die Nummer 10-15 verkörpern. Damit das Mining nicht ganz so einfach ist, gibt es noch eine Ziel-Schwierigkeit. Damit ein gültiger Block erstellt werden kann, müssen Miner einen Hash finden, der kleiner als ist als die Ziel-Schwierigkeit. Eine Zielschwierigkeit ist z.B.: 10000000000000000000000000000000000000000000000000000000000000000

Jede Zahl die, die mit einer 0 anfängt, wäre somit kleiner als die Ziel-Schwierigkeit z.B.: 0787a6fd6e0782f7f8058fbef45f5c17fe89086ad4e78a1520d06505acb4522f

[60] www.plentymarkets.eu

[61] www.krypto-magazin.de/wie-funktioniert-bitcoin-mining

Wenn jetzt die Ziel-Schwierigkeit auf: 0100000000000000000000000000000000000000000000000000000000000000 reduziert wird, werden zwei Nullen am Anfang benötigt: 00db27957bd0ba06a5af9e6c81226d74312a7028cf9a08fa125e49f15cae4979

Somit ist der Hash kleiner als die Ziel-Funktion.

Wenn diese Prozedur (generieren von Hashes) erfolgreich vom Miner abgeschlossen und in einem Block zusammengefasst wird, schließt sich dieser Block an die Blockchain(Block-Kette).[62]

Grundsätzlich wird zwischen zwei Arten vom Minen unterschieden. Entweder alleine, oder als Mitglied eines Pools. Um alleine Minen zu können, reicht die Installation der Bitcoin-Software mit der anschließenden Konfiguration vollkommen aus. Mining-Pools basieren auf der Idee des kollektiven Minings. Eine Person die alleine schürft braucht länger, um neue Blöcke zu finden und zu Minen, als eine Gruppe von Minern. Die Rechenkapazität eines jeden Mitglieds wird gebündelt, weswegen das Finden neuer Blöcke viel schneller geschieht. Je nach der geleisteten Rechenkapazität, wird die Belohnung auf die einzelnen Miner aufgeteilt.[63]

Im Durchschnitt werden alle zehn Minuten ein Block fertiggestellt. Ein Block entspricht seit Sommer 2013 genau 25 Bitcoins. Aufgrund der immer steigenden Rechenleistung die Miner aufwenden müssen, halbiert sich der Wert von generierten Bitcoins. Die Rechenkapazität des Netzwerks lässt sich in Hashes pro Sekunde messen.[64]

1.000 H/s = 1KH/s

1.000.000.000.000 H/s = 1TH/s

Das Bitcoin-Netzwerk hat aktuell eine Rechenkapazität von 15.000.000 TH/s. Damit eine „51% Attacke“ von einer Person durchgeführt werden kann, muss diese Person eine Hashleistung von mehr als 15.000.000 TH/s aufbringen.[65]

[62] www.weusecoins.com/de/mining-anleitung
[63] www.weusecoins.com/de/mining-anleitung
[64] www.weusecoins.com/de/mining-anleitung
[65] www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe

Da es eine begrenzte Menge von 21 Millionen Blöcken gibt, wird es im Jahr 2140 keine zu generierenden Blöcke mehr geben. Bitcoins können ab 2140 also nur noch transferiert werden.[66]

[66] Vgl. Kerscher (2014, S. 89)

5 Fazit und Ausblick

Im Rahmen der Arbeit wurde eine umfangreiche Analyse der aktuellen Literatur zum Thema Blockchain und Bitcoin durchgeführt. Die Strukturen der Blockchain-Technologie ermöglichen sichere, effiziente und manipulationssichere Interaktionen zwischen Parteien. Diese Technologie weist nicht nur in der Finanzbranche ein enormes Entwicklungspotenzial auf, sondern auch in Bereichen der Wirtschaft und des öffentlichen Sektors.

Jedoch erkennt man anhand der vorliegenden Daten, dass das Bitcoin-Netzwerk aufgrund des Fehlens einer zentralen Instanz Räume für Hackangriffe bietet. Die südkoreanische Krypto-Börse Coinrail meldete, dass Mitte Juni 2018 Bitcoins mit einem Wert von rund 31 Millionen Eure geraubt wurden. Auch die japanische Krypto-Börse Coincheck geriet Anfang 2018 ins Visier der Hacker. Hier wurden Bitcoins im Wert von 534 Millionen Dollar erbeutet. Die Öffentlichkeit verliert immer mehr das Interesse an virtuellen Währungen, welches sich auch in der aktuellen Kursentwicklung des Bitcoins wiederspiegelt.[67]

Auch die immer strenger werdenden Regulierungen durch Regierungen spielen eine erhebliche Rolle beim aktuellen Wertverlust des Bitcoins. Der wohl bedeutendste Grund für den Kursverfall ist jedoch, dass viele Bitcoin Nutzer nicht mit der virtuellen Währung handeln. Der Wert einer Währung lässt sich aus Angebot und Nachfrage ermitteln. Der größte Teil der Bitcoin Nutzer spekuliert auf einen großen Kursanstieg des Bitcoins anstatt damit zu handeln.[68]

Auch wenn die Bitcoin-Blase geplatzt zu sein scheint, sollten sowohl Regierungen als auch die Gesellschaft, an der Idee der dezentral organisierten Währungen, aufgrund der vielseitigen Einsetzungsmöglichkeiten festhalten.

[67] www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe

[68] www.spiegel.de/wirtschaft/unternehmen

Literaturverzeichnis

BitcoinfürAnfänger. (03. Februar 2018). Von http://bitcoin-für-anfänger.de/infos-und-anleitungen/bitcoin-im-detail/bitcoin-gebühren

BitcoinLive. (20. Januar 2018). Von https://bitcoin-live.de/was-ist-bitcoin/

Bitinfocharts. (10. April 2018). *bitinfocharts*. Von https://bitinfocharts.com/de/bitcoin/

Bitinforcharts. (03. Februar 2018). Von https://bitinfocharts.com/comparison/bitcoin-transactions.html abgerufen

Blitzboom, & bitcoin-dev. (08. Februar 2018). *weusecoins*. Von https://www.weusecoins.com/de/mining-anleitung

Blockchain Luxembourg. (2. Juli 2018). *Blockchain Charts*. Von https://www.blockchain.com/de/charts

BoerseArd. (03. Februar 2018). Von https://boerse.ard.de/boersenwissen/boersenlexikon/bitcoin138.html

BTC-Echo. (17. Januar 2018). Von https://www.btc-echo.de/tutorial/was-ist-proof-of-stake/

Bundesgerichtshof. (1. März 2011). *Bundesgerichtshof*. Von http://www.bundesgerichtshof.de/DE/Bibliothek/GesMat/WP17/E/e_geld_rl.html

DeutscheBundesbank. (14. Februar 2018). *Deutsche Bundesbank*. Von https://www.bundesbank.de/Redaktion/DE/Themen/2018/2018_02_14_zahlungsverhalten.html

DociSign. (16. Januar 2018). Von https://www.docusign.de/wie-es-funktioniert/elektronische-signatur/digitale-signatur/digitale-signatur-faq

Donner, A. (01. Januar 2018). *Ip Insider*. Von https://www.ip-insider.de/was-ist-peer-to-peer-p2p-a-654713

Ethereumbase. (10. Januar 2018). *Ethereumbase*. Von https://ethereum-base.com/blockchain/

EurLexEuropa. (26. Februar 2009). *Eurlexeuropa*. Von https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32009L0110

Finanziator. (11. Januar 2017). *Finanziator*. Von http://www.finanziator.de/geldanlagen/bitcoin-einfach-erklaert

Frieberg, H. (07. Februar 2018). *Heiko Frieberg*. Von http://www.heikofrieberg.com/Das-Bitcoin-Buch.pdf

GlobalSign. (15. Januar 2018). *GMO Internet Group*. Von https://www.globalsign.com/de-de/digitale-signaturen/was-sind-digitale-signaturen/

Griesel, J. (03. Februar 2018). *Plentmarkets*. Von https://www.plentymarkets.eu/blog/Bitcoin-BitPay-als-neuer-Zahlungsanbieter-integriert/b-1267/

Herrmann, T. (16. November 2017). *Datenschutzbeauftragter-info.de*. Abgerufen am Januar 2018 von https://www.datenschutzbeauftragter-info.de/bitcoin-technische-grundlagen-der-kryptowaehrung/

Hotelier. (03. Februar 2018). Von https://www.hotelier.de/lexikon/b/bitcoin-definition-geschichte

Horstmann, U. (2015). *Bargeldverbot.* München: Münchener Verlagsgruppe GmbH.

ItfconsultWordpress. (02. Februar 2018). Von https://itfconsult.wordpress.com/2013/11/18/5-jahre-bitcoins-und-der-kurs-explodiert-gerade/

Jauernig, H. (11. Juni 2018). *spiegel*. Von http://www.spiegel.de/wirtschaft/unternehmen/bitcoin-was-hinter-dem-kursverfall-steckt-a-1212312.html

Karame, G. (2016). *Bitcoin and Blockchain Security.* Norwood, Massachusetts: Artech House Inc.

Kerscher, D. (2014). *Handbuch der digitalen Währungen.* Dingolfing: Kemacon UG.

Khatwani, S. (2. Februar 2018). *Coinsultra*. Von https://coinsutra.com/bitcoin-double-spending/

Klickdichschlau. (15. Januar 2018). Von http://www.klickdichschlau.at/ecdl_glossar.php?anzeigen=definition&begriff=Digitale%20Signatur&ref=7.5.2.4

Kölling, M. (03. Februar 2018). *handelsblatt*. Von https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/die-geschichte-des-bitcoin-1-akt-der-mythos-des-satoshi-nakamoto/20104424-2.html?ticket=ST-3264209-OrfFtocJLLg3mf62ZD9Q-ap6

Krapp, C. (11. Juni 2018). *Handelsblatt*. Von https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/kryptowaehrungen-bitcoin-kurs-bricht-nach-hackerangriff-auf-kryptoboerse-ein/22670236.html?ticket=ST-2654735-vETYoJG5Z9iNB7Utgb9I-ap2

KryptoInvest. (02. Februar 2018). Von http://kryptoinvest.de/bitcoin/

KryptoMagazin. (15. Februar 2018). Von https://www.krypto-magazin.de/wie-funktioniert-bitcoin-mining

Menshelpcc. (1. Juni 2018). *menshelpcc*. Von https://menshelp.cc/dokuwiki/doku.php?id=bitcoin

Misiak, M. (02. Februar 2018). *coin-hero*. Von https://coin-hero.de/proof-of-work-vs-proof-of-stake/

Mittermeier, A. (06. Februar 2018). *Gevestor*. Von https://www.gevestor.de/details/bitcoin-wallets-was-steckt-hinter-der-digitalen-bitcoin-geldboerse-800679.html

Nolte, A. (6. Februar 2017). *Allianzdeutschland*. Von https://www.allianzdeutschland.de/digitalisierung-was-steckt-hinter-der-blockchain-technologie-/id_79699698/index

OpenLimit. (15. Januar 2018). Von https://www.openlimit.com/de/wissen/elektronische-signatur/funktionsweise-elektronische-signatur.html

Paysafecard Group PLC. (12. April 2016). *Paysafecard*. Von https://www.paysafecard.com/de/corporate/presse/pressemitteilungen/de

tail/2015-ein-erfolgreiches-jahr-fuer-paysafecard-das-innovative-zahlungsmittel-erobert-neue-maerkte-und/

Prof.Dr. Andreas Mitschele. (19. Februar 2018). *Wirtschaftslexikon*. Von https://wirtschaftslexikon.gabler.de/definition/blockchain-54161

Renggli, R., Vassilev, Y., & Ullrich, C. (08. Februar 2018). *finalix* . Von https://finalix.ch/wp-content/uploads/2015/12/Finalix-Bitcoins-V01.00.pdf

Roßbach, P. (02. Januar 2018). *blogfrankfurtschool*. Von https://blog.frankfurt-school.de/wp-content/uploads/2016/01/Blockchain_FSBlog_part11.pdf

S.A.R.L, B. L. (02. Februar 2018). Von https://www.blockchain.com/de/explorer

Sansonetti, R. (1. September 2014). *Die Volkswirtschaft*. Von https://dievolkswirtschaft.ch/de/2014/09/sansonetti-3/

Schiller. (7. Februar 2018). *Blockchainwelt*. Abgerufen am März 2018 von https://blockchainwelt.de/kryptographie-innerhalb-der-blockchain-technologie/

Schreyer, T. (18. Januar 2017). *PPRO Financial Ltd*. Von https://www.ppro.com/de/blog-de/ist-eigentlich-e-geld/

Secrypt. (15. Januar 2018). *E.signature solutions*. Von https://www.secrypt.de/unternehmen/wissenswertes-und-rechtliches/

Sixt, E. (2016). *Bitcoins und andere dezentrale Transaktionssysteme.* Wiesbaden: Springer Gabler.

Smith, S. (6. Februar 2018). Von https://www.juniperresearch.com/press/press-releases/bitcoin-users-to-approach-5-million-by-2019

Talin, B. (03. Februar 2018). *morethandigital*. Von https://morethandigital.info/blockchain-moeglichkeiten-und-anwendungen-der-technologie/

Taras. (12. Februar 2018). *bitcoinWiki*. Von https://en.bitcoin.it/wiki/Anonymity

TheCoinscout. (02. Februar 2018). *coinscout*. Von https://thecoinscout.com/krypto-lexikon/was-ist-double-spending/ abgerufen

Verhoelen, J. (22. Januar 2018). *blog.codentric*. Von https://blog.codecentric.de/2017/10/konsens-mechanismen-blockchain/

Vetter, A. (3. Februar 2016). *Polyas*. Von https://www.polyas.de/blog/de/online-wahlen/sicherheit/kryptographie-was-ist-das

Weißbach, M. (30. März 2016). *Schnatterente*. Abgerufen am Januar 2018 von https://www.schnatterente.net/software/was-ist-eine-digitale-signatur

Wikipedia. (10. Januar 2018). *Wikipedia*. Von https://de.wikipedia.org/wiki/Elektronisches_Geld

Wirexapp. (06. Februar 2018). Von helpWirexApp: https://help.wirexapp.com/hc/de/articles/207869925-Was-ist-eine-Bitcoin-Adresse