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

Seminararbeit

in der Fachrichtung
Wirtschaftsingenieurwesen
SS 2017

Thema:

Digitales Geld, die Blockchain und Bitcoin

Eingereicht von:	Johanna Pfeiffenberger (Mat.-Nr. 102538) Achterbruch 11 21335 Lüneburg Mobil: 0176-34974670 E-Mail: johanna.pfeiffenberger@web.de
Erarbeitet im:	2. Semester
Abgegeben am:	04.07.2017
Betreuerin (FH Wedel):	Prof. Dr. Michael Anders Fachhochschule Wedel Feldstraße 143 22880 Wedel Tel. (04103) 8048-24 E-Mail: an@fh-wedel.de

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Problemstellung

Die sogenannten virtuellen Währungen, insbesondere der 2009 kreierte Bitcoin, gehören zu den jüngsten Internet-Innovationen seit der Entwicklung des World Wide Web im Jahr 1989. Im Kontext der Finanzkrise und des damit einhergehenden Vertrauensverlustes der Konsumenten in staatliche und privatwirtschaftliche Institutionen hat der Bitcoin seit 2008 eine einmalige Entwicklung durchgemacht und sich seither als Referenz auf dem Gebiet der virtuellen Währungen etabliert.[1]

Zurzeit hat Bitcoin von allen heute existierenden virtuellen Währungen in Bezug auf Verbreitung und Kapitalisierung die größte Bedeutung.
So kann man Bitcoins an speziellen Börsen kaufen und verkaufen und sie werden auch bei diversen Online-Händlern als Zahlungsmittel akzeptiert.

Die dieser Entwicklung zugrunde liegende Technologie existiert in der Theorie bereits seit einem Jahrzehnt. Die Verfahren basieren auf asymmetrischer Verschlüsselung, interaktiven Systemen auf Grundlage von Zero-Knowledge-Beweisen und verschiedenen Software-Protokollen für Interaktion, Authentifizierung und Verifizierung. Die Blockchain ist dabei das zentrale Werkzeug die Bitcoin möglich macht und ohne die die dezentralisierte, verteilte Buchhaltung des Systems nicht möglich wäre.[2]

Die Erwartungen, die an den Erfolg der Kryptotransaktionssysteme gestellt werden, lassen sich gut anhand der Entwicklung des Wechselkurses zeigen.

---

[1] Vgl. Sansonetti (2014)
[2] Vgl. Platzer (2014, S.17)

Abbildung 1: Preisentwicklung für Bitcoins seit 2012(faz.net)

So betrug der Wert eines Bitcoins Anfang 2013 ungefähr 25 US-Dollar. Vier Jahre später durchbrach der Kurs die Marke von 2000 US-Dollar.

Gründe für den Anstieg sind derzeit bei Japan und der amerikanischen Börsenaufsicht zu finden. Die drittgrößte Volkswirtschaft der Welt hatte Bitcoins Anfang April zu einem offiziellen Zahlungsmittel erklärt. Zum Wochenauftakt wurde nun bekannt, dass mit Peach Aviation erstmals eine Fluggesellschaft Bitcoins als offizielles Zahlungsmittel für den Ticketkauf zulassen möchte.[3]

Die Risiken für einen Kursfall, wie es im Jahr 2013 der Fall war, sind auch heutzutage wieder ähnlich. Noch immer ist China der Haupthandelsort für die Bitcoin. Schon durch leichte politische Maßnahmen – sei es eine weitere Schwächung des Yuan zum Dollar oder wieder strengere Kapitalverkehrskontrollen – könnte es gigantische Schockwellen auf dem Bitcoin-Markt geben.

[3] Vgl. Nestler (2017)

Auch sind viele Handelsbörsen bis heute nicht sicherer als damals Mt. Gox. Immer wieder gibt es erfolgreiche Hackerangriffe. Dank mangelnder Regulierung ist auch keine Transparenz hergestellt.[4]

Ihre konzeptionellen Schwachstellen und die Unbeständigkeit ihres gehandelten Wertes lassen den Erfolg zweifelhaft erscheinen. Die Ideen der Entwickler neuer, alternativer Währungen sind wertvoll und tragen zu der Verbesserung des Gesamtkonzeptes dieser Form des elektronischen, dezentralen Geldes bei.[5]

1.2 Aufbau und Zielsetzung der Arbeit

Das Ziel dieser Arbeit soll sein, ein Verständnis für die wichtigsten technischen Aspekte dezentraler, elektronischer Währungen zu vermitteln.

Es soll die Technologie der Blockchain sowie die darauf zierkulierenden Bitcoins weitestgehend erläutert werden.

Dazu bietet der erste Teil der Arbeit zunächst einen Einblick in die Funktionsweise von der Blockchain als erste Umsetzung einer dezentralen, elektronischen Währung. Der zweite Teil schafft einen Überblick über den Bitcoin. Es werden die Entwicklung des Bitcoins und aktuelle Daten des Bitcoin erarbeitet. Zudem wird dargestellt wie Transaktionen durchgeführt und wie man in den Besitz von Bitcoins kommt.

1.3 Methodik und Vorgehensweise

Informationen zu dezentralen, elektronischen Währungen sind kurzlebig und werden erst relativ spät in wissenschaftlichen Arbeiten oder gar Veröffentlichungen in Buchform aufgegriffen. Um eine hohe Diversität bei den zugrundeliegenden Informationen zu gewährleisten, werden einige Beiträge aus Foren oder Artikel aus Blogs berücksichtigt. Auch Bücher und aktuelle Artikel aus Fachzeitschriften werden genutzt. Beleuchtet werden dabei Hintergrundinformationen und Einblicke bezogen auf die Technologie der elektronischen Währung.

---

[4] Vgl. Klemm (2017)
[5] Vgl. Nestler (2017)

2 Blockchain Allgemein

2.1 Distributed Ledger

Ein Distributed Ledger (wörtlich „verteiltes Kontobuch“) ist ein öffentliches, dezentral geführtes Kontobuch. Es verfügt über einen Mechanismus, dass es auf alle teilnehmenden Parteien verteilt.

Es ist die technologische Grundlage virtueller Währungen und dient dazu, im digitalen Zahlungs- und Geschäftsverkehr Transaktionen von Nutzer zu Nutzer aufzuzeichnen, ohne dass es einer zentralen Stelle bedarf, die jede einzelne Transaktion legitimiert. Blockchain ist der Distributed Ledger, welcher der virtuellen Währung Bitcoins zugrunde liegt.[6]

2.2 Blockchain, Protokoll, Währung

Eine Blockchain ist eine kryptographisch geschützte, globale und irreversible peer-to-peer verteilte Datenbank, in der atomare Veränderungen des Systemzustands blockweise in einer immer länger werdenden Kette gespeichert werden.

Diese Systemupdates werden in vielen Anwendungen, jedoch nicht notwendigerweise bei allen, in Form von Transaktionen verbucht, weswegen die Blockchain auch den Namen „Ledger“ (Transaktionsbuch) trägt. Solche Transaktionen werden dann wie bei Bitcoin, der ersten Blockchain-Anwendung, mit den Einheiten von sog. Kryptowährungen, d.h kryptographische Verrechnungseinheiten, beziffert. [7]

Weiterhin besteht die Datenbank aus einer Verkettung von „Blöcken“, die die Datenbank in regelmäßigen Abständen um die jeweils neusten Transaktionen blockweise erweitern. Hierbei werden die Transaktionen geprüft und mit einem Hash-Algorithmus vor Veränderungen geschützt und dabei mit dem Hash-Wert des vorherigen Blocks verbunden. So entsteht eine Kette, die

[6] Vgl. Hurr (2016, S. 4)
[7] Vgl. Garzik (2015, S.8)

namensgebende Blockchain, bei der Blöcke nicht mehr verändert werden können.[8]

Die Blockchain speichert somit die gesamte Historie der Transaktionen in chronologischer Reihenfolge. Folglich ist der aktuelle Systemzustand nicht direkt ablesbar, sondern muss durch die Transaktionshistorie rekonstruiert werden.

Technologisch gesehen bildet die Blockchain die unterste und fundamentale Schicht von insgesamt drei Schichten, wie in der Abbildung 1 dargestellt. Das Protokoll liegt dabei auf der mittleren Ebene über der Blockchain. Es legt das gesamte Regelsystem, wie Transaktionen auf der Blockchain ablaufen, sowie die Programmiersprache fest.[9]

Darüber liegt die Kryptowährung, die mittels der Software bzw. des Protokolls auf der Blockchain zirkuliert. In der Regel verwendet jede Währung ein gleichnamiges Protokoll, kann jedoch auch auf einer eigenen Blockchain oder einer fremden, d.h. zusammen mit einer anderen Währung funktionieren.

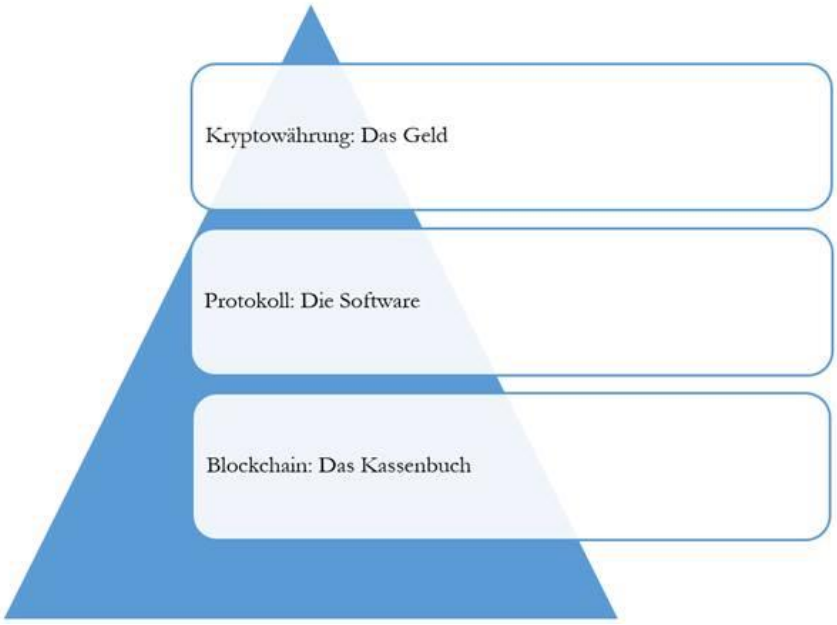

Abbildung 2:Schichtenmodell der Blockchain-Technologie (nttdata.com)

[8] Vgl. Garzik (2015, S.9ff)
[9] Vgl. Liesenjohann (2016, S. 23)

Blockchain-Technologien haben Anwendungspotenziale in einer Vielzahl von Branchen. Sie ermöglichen neue Formen der Abwicklung von Geschäften, indem sie die Rolle zentraler Clearingstellen als Mittler ersetzen oder verändern können. Da die Technologie und deren Anwendungen noch jung und zum Teil erst im Entstehen sind, gibt es noch wenige Erfahrungswerte.

Auf Blockchain basierende Smart Contracts, dezentralisierte Anwendungen (dApps) und Dezentral Autonome Organisationen (DAOs) können herkömmliche „Trusted 3rd Parties“ ersetzen, sowie wirtschaftliche und bürokratische Transaktionen unterschiedlichster Natur um ein vielfaches billiger, schneller und sicherer als herkömmliche zentralisierte Client-Server-basierte Informationssysteme machen.[10]

2.3 Technologie hinter Blockchain

Die Blockchain ist eine Kombination aus drei Konzepten bzw. Technologien. Dem Peer-to-Peer Netzwerk, der Kryptografie und der Spieltheorie.[11]

2.3.1 Peer-to-Peer Netzwerkarchitektur - Dezentralität und Digitalität des Systems

Eines der wichtigsten Eigenschaft der Blockchain ist die Dezentralität. Die Systemarchitektur kennt keine zentrale Autorität mit einer Steuerungs- oder Kontrollkompetenz. Die Verifizierung und Validierung der Transaktionen erfolgt dezentral. Die Dezentralität beruht hier auf der Umsetzung des Systems als Peer-to-Peer Netzwerk.

Peer-to-Peer-Netze (P2P) sind Rechnernetze bei denen alle Rechner im Netz gleichberechtigt zusammen arbeiten. Das bedeutet, dass jeder Rechner anderen Rechnern Funktionen und Dienstleistungen anbieten und andererseits von anderen Rechnern angebotene Funktionen, Ressourcen, Dienstleistungen und Dateien nutzen kann. Die Daten sind auf viele Rechner, in der Regel auf die der Nutzer, verteilt.[12]

---

[10] Vgl. Voshmgir (2016, S. 10)
[11] Vgl. Voshmgir (2016, S. 11)
[12] Vgl. Voshmgir (2016, S. 13)

Das Peer-to-Peer-Konzept ist ein dezentrales Konzept, ohne zentrale Server, wie das Internet. Jeder Rechner eines solchen Netzes kann mit mehreren anderen Rechnern verbunden sein.[13]

Einfache Peer-to-Peer-Netze organisieren sich selbst, als Self Organized Networks (SON). In einem solchen dezentralen Peer-to-Peer-Netzwerk stellen sich die Workgroup-Mitarbeiter gegenseitig Betriebsmittel und Ressourcen zur Verfügung. Jeder Nutzer legt fest, welche Dateien er freigeben möchte, welches Passwort benötigt wird und schon können die jeweiligen Peers des Netzwerks gegenseitig Daten oder Ressourcen austauschen.[14]

In einer Blockchain sind alle Teilnehmer über ein Peer-to-Peer Netzwerk verteilt und Transaktionen sind für jeden Teilnehmer einsehbar. Damit können alle Transaktionen bis zu ihrem Ursprung zurückverfolgt werden und sind somit transparent. Alle jemals durchgeführten Transaktionen werden in einem Register gespeichert.

Davon ist auch ihre Bezeichnung als „Distributed Ledger“ abgeleitet. Hierbei verfügt jeder Knoten, d.h. Teilnehmer im P2P-Netz, über die gesamte Kette von Blöcken und gleichzeitig über dieselben Rechte, neue Blöcke zu erzeugen. Die gleichen Informationen zu besitzen, bedeutet im gegebenen Kontext, dass jeder Knoten eine Kopie des kompletten Ledgers besitzt (siehe Abbildung 3). [15]

[13] Vgl. One Page Wiki Lexikon (2017)
[14] Vgl. One Page Wiki Lexikon (2017)
[15] Vgl. IT Kompetenzzentrum (2017)

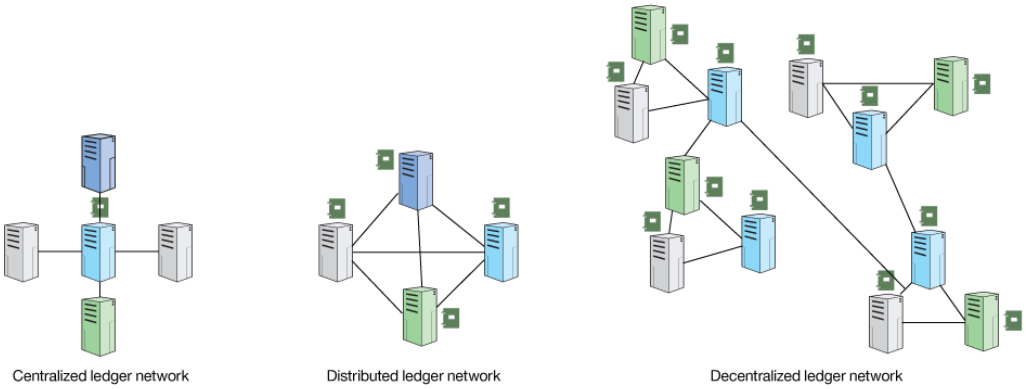

Abbildung 3:Darstellung unterschiedlicher Netzwerkstrukturen (blockchain.net)

In diesem Fall bestünde ein Basisschutz des Netzes vor Manipulationen, da diese auf der Mehrzahl der Knoten durchgeführt werden müssten, um wirksam zu sein. Diese Funktionsfähigkeit des Netzes selbst bliebe auch dann erhalten, wenn einzelne Knoten oder Knotensegmente ausfallen würden. Gleiches gilt auch für das hinzufügen oder Entfernen von Knoten. [16]

Die durch die Verteilung des Ledgers bewirkte vollständige Redundanz ist somit ein Mittel gegen einseitige Macht, Manipulation und Ausfall, womit allein durch die Architektur des Systems bereits Schutzmechanismen existieren.

Eine zentrale Fehlerquelle sowie Zensur durch eine zentrale Institution sind somit abgeschafft. Man vertraut nicht einer Person oder Institution, sondern dem Protokoll und den Netzwerkteilnehmern.[17]

2.3.2 Das Problem des Double-Spending

Derartige Systemansätze scheitern im Finanzberiech in der Vergangenheit immer an dem sog. Double-Spending-Problem.
Bei digitalen Währungen kann es zu Problemen kommen, wenn nicht verhindert wird, dass Einheiten der Währung beliebig kopiert und ausgegeben werden können, was zwangsläufig zur Entwertung der Währung führen würde.

[16] Vgl. IT Kompetenzzentrum (2017)
[17] Vgl. Liesenjohann (2016, S. 16)

Wie bei klassischem Papiergeld wachte auch bei digitalem Geld bisher stets eine zentrale Instanz darüber, dass eine Einheit nur transferieren kann, wer diese auch wirklich besitzt und im Zuge dessen von seinem Konto wieder streicht. Da es solche Intermediäre bei einem dezentralen System der Blockchain nicht gibt, wird die Integrität der Transaktionen auf andere Weise gewährleistet.[18]

2.3.3 Bedeutung des Distributed Consensus

Eine große Herausforderung dezentraler und digitalen Netzwerke besteht im Erreichen eines dezentralen Konsens, denn nur wenn Konsens zwischen den einzelnen Teilnehmern eines Systems darüber erreicht wird, wem welche Werte zu welchem Zeitpunkt zuzuordnen sind, kann ein digitales dezentrales Zahlungssystem funktionieren.

Der sog. „Distributed Consensus“ ist ein bestimmter Konsens zwischen den anonymen und sich einander nicht vertrauenden Knoten im P2P-Netz über die Validität von Transaktionen in Bezug auf ihre zeitliche Reihenfolge.[19]

Dabei einigen sich die Nutzer auf die Chronologie der Transaktionen. Beispielhaft bedeutet dies, dass bei gleichzeitigem Auftreten zweier Transaktionen über denselben digitalen Wert sichergestellt sein muss, dass in die öffentliche Datenbank nur die erste der beiden Transaktionen aufgenommen wird und dass von allen Nutzern dieselbe Transaktion als die valide und nicht reversible Transaktion betrachtet wird.

Die gültige Transaktionshistorie wird einerseits im dezentralen Netzwerk über einen Proof-of-Work-Mechanismus erreicht und andererseits dadurch das Konsens unter den „ehrlichen“ Minern besteht, dass immer die längste Kette die valide Blockchain ist.[20]

Darüber hinaus müssen für valide Transaktionen folgende Eigenschaften gelten:[11]

[18] Vgl. Roßbach (2016, S.4)
[19] Vgl. Roßbach (2016, S.6ff)
[20] Vgl. Sixt (2017S. 32)

- *Konformität:* Z.B. wenn jemand lediglich 100 BTC besitzt, kann er keine 1000 BTC versenden.
- *Autorisierung:* Es ist klar geregelt, wer zu Transaktionen berechtigt ist und wie diese Person sich dazu im System legitimiert.
- *Unveränderbarkeit:* Sobald eine Transaktion in die Blockchain integriert wurde, können keine ihrer Parameter mehr modifiziert werden.
- *Finalität:* Transaktionen sind irreversibel, d.h. können nicht gelöscht und damit nicht rückgängig gemacht werden.
- *Zensur-Resistenz:* Wenn eine Transaktion mit dem Protokoll übereinstimmt, muss sie in die Kette eingefügt werden, ohne dass dies aus anderen Gründen unterbunden werden könnte. Zu beachten ist hier jedoch, dass dieses Kriterium von Bitcoin und anderen Ansätzen theoretisch nicht erfüllt wird. Die zur Erzeugung eines Blocks berechtigten Knoten sowie die Überprüfer können selbständig erwägen, ob sie Transaktionen bewilligen oder nicht, ohne dass das Protokoll sie zur Einhaltung dieses Kriteriums zwingen würde. In der Praxis dürfte dieses Manko aber eine weniger große Rolle spielen, da eine etwaige Zensur von der Mehrheit der Teilnehmer bezweckt sein müsste.

Diese Eigenschaften werden mittels des Konsensus-Mechanismus durch die Netzwerkteilnehmer verifiziert.[21]

Es wird nicht über einzelne Transaktionen abgestimmt, sondern über die Blöcke, die mehrere Zahlungen beinhalten. Neue Transaktionen müssen also zunächst in einem temporären Speicher warten, bis sie in einen Block eingefügt und per Konsens anschließend zur Datenbank hinzugefügt werden.

Blockchain-Varianten unterscheiden sich im sog. Consensus-Mechanismus oder Hashing-Algorithmus, worunter man die Art und Weise versteht, wie unter den Teilnehmern des Netzwerks entschieden wird, mit welchen

[21] Vgl. Sixt (2017S. 34ff.)

Transaktionsblöcken die Blockchain aktualisiert und wie dieser Prozess im Netz organisiert wird.[22]

2.3.4 Kryptographie und Sicherheit

Kryptografie ist ein Teilgebiet der Kryptologie und befasst sich mit dem Verschlüsseln von Informationen. Es ist die Anwendung mathematischer Verfahren, um Techniken und Algorithmen zu entwickeln, welche die Sicherheit der Daten schützen.

Das Ziel der Sicherheit umfasst in diesem Zusammenhang Vertraulichkeit, Integrität, Verbindlichkeit und Authentifizierung, welches die Methoden zur Überprüfung der Identität des Senders übermittelter Daten, der z.B. an der Tätigkeit eines Zahlungssystems beteiligt ist, und zur Bestätigung, dass eine Nachricht bei der Übermittlung nicht verändert wurde, umfasst.[23]

Die Blockchain baut auf zwei fundamentalen Konzepten der Kryptographie auf: Public-Key-Kryptographie bzw. digitalen Signaturen und kryptographischen Hash-Funktionen.

Bei dem Konzept der Public-Key-Kryptographie wird durch einen Algorithmus ein mathematisch miteinander verbundenes Schlüsselpaar generiert, bestehend aus einem privaten und einem öffentlichen Schlüssel. Um Transaktionen durchführen zu können, erhält jeder Teilnehmer der Blockchain einen solchen privaten und einen öffentlichen Schlüssel. Die Nachricht kann durch die asymmetrische Verschlüsselung nicht unbemerkt verändert werden, wodurch ihre inhaltliche Integrität gewährleistet wird.[24]

Die weitere Ausführung von Transaktionen mittels der asymmetrischen Verschlüsselung wird in Kapitel xx näher erläutert. Die Blockchain erlaubt nicht nur Transparenz, sondern auch eine “relative Anonymität”. Das für die jeweiligen Anwendungen erwünsche Level von Transparenz und Anonymität kann durch entsprechende Programmierung der im Einzelfall verwendeten Blockchain und der zugehörigen Protokolle festgelegt werden und ist auch bei

[22] Vgl. Roßbach (2016, S. 8)
[23] Vgl. Kryptowissen.de (2017)
[24] Vgl. Voshmgir (2016, S. 24)

aktuell in Anwendung befindlichen unterschiedlichen Blockchains recht verschieden.[25]

Die Kryptographie kommt allerdings noch an anderer Stelle zum Einsatz: Um die Datenbank vor rückwirkender Manipulation zu schützen, werden Zahlungen einerseits nicht sequenziell, sondern blockweise verbucht, und andererseits enthält jeder Block neben allen seit dem letzten Block neuen Transaktionen eine kryptographische Signatur des vorangegangenen Blocks mittels eines Hash-Wertes sowie einen Zeitstempel.

Dadurch hängen die einzelnen Blöcke voneinander ab. Wenn man also versuchen würde, eine Transaktion aus einem älteren Block zu verändern, wären dadurch alle neueren Blöcke inkonsistent und müssten ebenso manipuliert werden. Zusätzlich müsste all dies an der absoluten Mehrheit der Knoten passieren und noch vor der nächsten Aktualisierung der Blockchain durch einen neuen Block. Hinzu kommt die vom Consensus Mechanismus abhängige Hürde bei der Blockerzeugung, die z.B. viel Rechenleistung verlangt. Alles in allem ist die Blockchain u.a. durch Kryptographie somit äußerst gut gegen jegliche Manipulation, systemextern und –intern, abgesichert, und dies als system-inhärente Eigenschaft.[26]

2.3.5 Spieltheoretische Incentivierung

Ökonomische Anreizsysteme sorgen dafür, dass die Teilnehmer im Netzwerk im eigenen Interesse für ein funktionierendes Gesamtsystem sorgen: Proof of Work (PoW), Proof of Stake (PoS), Proof of Burn (PoB), u.v.m. Einzelne Teilnehmer im System sind hierbei ökonomisch incentiviert, Transaktionen dem Protokoll entsprechend zu verifizieren. Proof of Work ist bisher am weitesten verbreitet und funktioniert folgendermaßen: Wenn ein Block von Transaktionen korrekt, d.h. dem Protokoll gemäß, verifiziert wird, bekommt der Teilnehmer im Netzwerk einen Block Reward.[27]

[25] Vgl. IT Kompetenzzentrum (2017)
[26] Vgl. Sixt (2017, S.39ff)
[27] Vgl. Roßbach (2016, S.25ff)

Incentivierung führt im Zusammenspiel mit dem P2P-Charakter der Blockchain dazu, dass der Aufwand für Manipulationen des Gesamtsystems dann enorm groß wird, wenn die Zahl der beteiligten Nutzer groß ist. Um bestehende Transaktionen, die in der Blockchain gemacht wurden, zu zensurieren oder zu fälschen, müsste man über die Mehrheit der Netzwerkteilnehmer verfügen und diese dazu bringen können, Transaktionen nicht dem Protokoll entsprechend zu verifizieren. Der ökonomische Aufwand steht in den allermeisten Fällen mit dem Nutzen nicht im Verhältnis. Fälschung oder Zensur wird dadurch ökonomisch unrentabel. Proof of Work macht eine Blockchain sicher, ist aber auch sehr langsam, d.h. zu wenige Transaktionen pro Sekunde können auf einer PoW-basierten Blockchain abgewickelt werden.[28]

Auch wenn sie noch in der Entwicklung sind, zeichnen sich viele unterschiedliche Ansätze ab, wie man diese Skalierungsprobleme bewältigen könnte. Hier besteht grundsätzlich noch viel Forschungs- und Entwicklungsbedarf. Im Laufe der nächsten Jahre könnte sich daher die Grundarchitektur von Blockchains unter anderem auch hinsichtlich der Anreizmechanismen ändern.[29]

2.4 Blockchain Anwendungen

Smart Contracts sind automatisch ausführbare Programme, die auf der Blockchain aufbauen und vordefinierte Transaktionsspielregeln im Programmcode abbilden. Eine Transaktion, die über einen Smart Contract läuft, wird automatisch ausgeführt, wenn alle beteiligten Parteien die zuvor definierten Konditionen erfüllen. Dadurch erübrigt sich die Notwendigkeit einer zentralen, zwischengelagerten Instanz, insbesondere wenn die beteiligten Parteien sich nicht kennen und somit auch nicht vertrauen, und senkt zudem die Transaktionskosten.

dApps (Decentralized Applications) sind dezentrale Anwendungen, vom Backend bis zum User Interface, die auf einer Blockchain laufen und einen oder mehrere Smart Contracts verwenden.

---

[28] Vgl. Roßbach (2016, S.28ff)
[29] Vgl. IT Kompetenzzentrum (2017)

DAOs (Decentralized Autonomous Organizations) sind eine neue Form der Organisation, deren Statuten, Geschäftsordnung, Gesellschaftsvertrag oder Satzung durch einen Smart Contract abgebildet und automatisch ausgeführt werden. Die Spielregeln der Organisation werden im Vorfeld definiert und in die Smart Contracts programmiert. DAOs brauchen kein zentral organisiertes Management des Tagesgeschäfts mehr. Die Rollen von Spezialisten werden durch gewählte Teilnehmer der DAO oder externe “Agenten” übernommen. DAOs sind die höchste und komplexeste Form eines Smart Contracts.[30]

[30] Vgl. Hurr (2016, S.9ff.)

3 Die Grundlagen des Bitcoin-Systems

3.1 Aktuelle Daten und Entwicklung des Bitcoins

Das Konzept der dezentralen Währung, die weder von Banken noch von Regierungen kontrolliert und mit der anonym umgegangen werden kann, ist schon länger bekannt.

Bereits in den 1970ern wurde über verschlüsselte digitale Währungssysteme nachgedacht. 1990 gründete David Chaum das Unternehmen DigiCash, das ein elektronisches Zahlungssystem anbot und zusammen mit dem System eCash kleinere Zahlungen abwickelte.

Innovativ war auch hier schon die Verwendung kryptographischer Protokolle, die die Anonymität der Benutzer garantieren sollte. Das System konnte sich aufgrund der Frühzeit des Internets und den im Vergleich zur heutigen Zeit wesentlich geringeren Nutzerzahlen nicht durchsetzen.[31]

Das Konzept der Bitcoin-Währung wurde erstmals am 31. Oktober 2008 von Satoshi Nakamoto in einem Aufsatz vorgestellt.

Ob es sich bei Satoshi Nakamoto um eine reale Person oder das Pseudonym einer einzelnen Person oder einer Personengruppe handelt ist bis heute unklar, da er bis heute niemals öffentlich in Erscheinung getreten ist.

In diesem Aufsatz beschreibt er das Grundproblem jeder modernen Währung, als das Ausmaß des Vertrauens, das nötig ist, damit Währung funktioniert. Zudem versucht er gleichzeitig eine Lösung dafür anzubieten.[32]

Basierend auf seinem Konzept entstand das Bitcoin-Netzwerk mit der ersten Version des Bitcoin-Clients „bitcoind“, der die ersten Bitcoins auf einem normalen PC erzeugt.

Der sogenannte „Genesis Block“ mit den ersten 50 Bitcoins wurde am 3. Januar 2009 von Satoshi Nakamoto generiert. Die ersten Bitcoins hatten noch keinen Bezugspunkt, deshalb wurde ihr Wert unter den ersten Teilnehmern

[31] Vgl. Sansonetti (2014, S.49)
[32] Vgl. Sansonetti (2014, S.50)

des Netzwerks ausgehandelt. Sobald sich jemand fand, der den Preis eines Bitcoin in einer anderen Währung oder in Waren bzw. Dienstleistungen akzeptierte, war der Bitcoin-Markt entstanden.[33]

Im Oktober 2009 entstand der erste Wechselkurs auf Dollar-Basis für den Bitcoin (veröffentlicht von New Liberty Standard). Mithilfe einer Kalkulation, die auf den Stromkosten und Hardwarekosten für das Mining beruhte, wurde der erste Wechselkurs mit 1309,09 BTC für 1 US-Dollar festgelegt.

Das entsprach 0,08 Cent für 1 Bitcoin. Im Juli 2010 wurden Bitcoins erstmals über die Bitcoin-Börse Mt. Gox (gegründet von Jed McCaleb) zu einem Kurs von 0,06 US-Dollar pro Bitcoin gehandelt. Der Gesamtwert aller Bitcoins betrug damals 277.000 US-Dollar.

Ende Juli 2015 erreichte die Marktkapitalisierung umgerechnet 3,8 Mrd. US-Dollar (ausgegebene *bitcoins* * Tageskurs bitcoin/US-Dollar). Die bisher höchste Marktkapitalisierung weist der Bitcoin derzeit aus mit über 46,6 Mrd. US-Dollar (Juni 2017).[34]

Der Bitcoin-Umtauschkurs hat seit der Einführung des Bitcoin-Systems schon mehrere Hochphasen mit anschließendem Kursverfall erlebt. Bis zum aktuellen Zeitpunkt ist der Tauschkurs gegenüber gängigen Währungen jedoch tendenziell sehr stark gestiegen. In den ersten elf Monaten des Jahres 2013 schoss der Wechselkurs des Bitcoins um 8500% die Höhe, in den folgenden sechs Monaten verlor diese Währung zwei Drittel ihres Werts wieder.[35] Derzeit beträgt der Marktpreis um die 2,4 Tsd. US-Dollar mit einer Anzahl von rund 16,4 Millionen Bitcoins im Umlauf (Juni 2017). Die Kursschwankungen des Bitcoins reflektierten zum einen Ereignisse innerhalb der Bitcoin-Ökosphäre. [36]

So haben die Umstände rund um die medienwirksame Schließung des Online-Drogenhandelsplatzes Silk Road (ausschließliches Zahlungsmittel war der

[33]Vgl. Sansonetti (2014, S.52)
[34] Vgl. Blockchain.info (2017)
[35] Vgl. Giese (2016, S.36)
[36] Vgl. Blockchain.info (2017)

Bitcoin) Anfang September 2013 und die Ereignisse rund um die Insolvenz der Bitcoin-Börse Mt. Gox im März 2014 das Vertrauen in das neue elektronische Zahlungssystem in der Öffentlichkeit nachhaltig beschädigt. Die Kursentwicklung wird jedoch auch durch externe, außerhalb der digitalen Welt vor sich gehende Entwicklungen beeinflusst. So haben auch ständig steigendes Misstrauen in das herkömmliche Geld – und Politiksystem und Vorfälle wie die Zypernkrise (2013) und auch die Griechenlandkrise (GREXIT) 2015 Auswirkungen auf den Kurs des Bitcoins.[37]

Die erste reale Bitcoin-Transaktion wurde am 22. Mai 2010 von Laszlo Hanecyz, einem Softwareprogrammierer aus Florida, getätigt. Er erwarb zwei Pizzen für 10.000 Bitcoins.

2010 fanden nur sehr wenige Bitcoin-Transaktionen statt, selten wurde die Zahl von 100 pro Tag überschritten. [38]

Beginnend mit Januar 2011 stiegen die durchschnittlichen täglichen Transaktionen auf über 1000; innerhalb von weiteren 6 Monaten stiegen die Transaktionen auf 5000 bis 6000 pro Tag. 2011 akzeptierte auch Wikileaks die ersten Bitcoin-Spenden. Ab Mitte 2012 stiegen die Transaktionen auf mehr als 20.000 pro Tag. Zu dieser Zeit wurde die Nutzung von Bitcoin auch populär durch die ausschließliche Möglichkeit des Ankaufs illegaler Substanzen gegen Bitcoins auf der Silk Road, einem anonymen Marktplatz des DeepWeb.

Trotz der offensichtlichen Abnahme des öffentlichen Interesses im Jahre 2014 und des geringeren Kurses, erhöhte sich die Anzahl der Bitcoin-Transaktionen pro Tag kontinuierlich, wie aus der Abbildung 4 ersichtlich ist.[39]

[37] Vgl. Sixt (2017, S.21)
[38] Vgl. Sixt (2017, S.18)
[39] Vgl. Blockchain.info (2017)

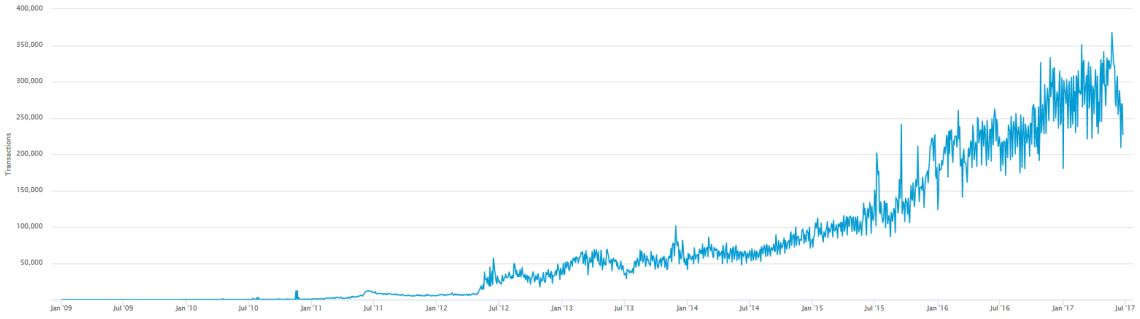

Abbildung 4:Transaktionen pro Tag (2009-2017) (blockchain.info)

Während vor einem Jahr noch täglich 170.000 bis 300.000 Transaktionen pro Tag durchgeführt worden sind, sind dies heute kontinuierlich 300.000 – 350.000 Transaktionen (Abbildung 4). Das Transaktionsvolumen betrug im Juli 2013 noch etwa 15 bis 30 Mio. US-Dollar am Tag und hat sich im Juli 2014 zwischen 30 und 100 Mio. US-Dollar bewegt. Ende Juni 2017 betrug das durchschnittliche Transaktionsvolumen pro Tag rd. 400 Mio. USD (Abbildung 5).[40]

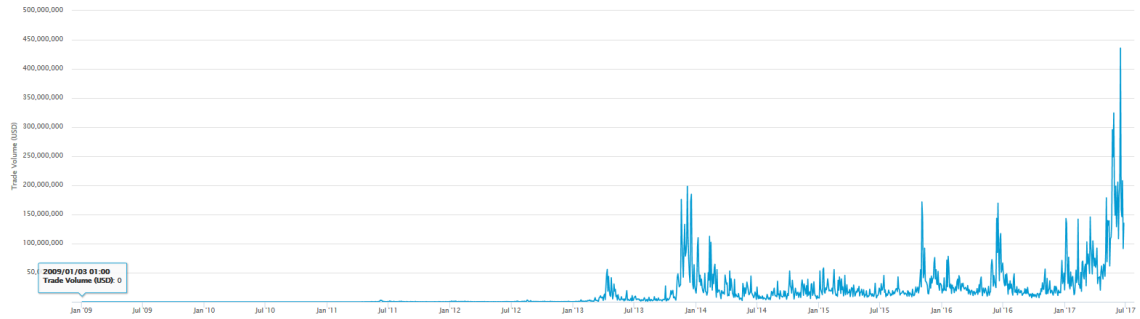

Abbildung 5: Transaktionsvolumen(2009-2017) (blockchain.info)

Eine Aufstellung von blockchain.info zum Juli 2017 zeigt den aktuellen Status der Bitcoin-Wallets bei 14,8 Mio. im Vergleich zu 7,1 Mio im Juli 2016 und damit mehr als eine Verdoppelung. Die Anzahl der aktiven Nutzer lag laut Juniper Research 2014 bei wenig mehr als 1,3 Mio. und soll 4,7 Mio. bis Ende 2019 erreichen.[41]

[40] Vgl. Blockchain.info (2017)
[41] Vgl. Blockchain.info (2017)

3.2 Bitcoin-Wallets und Clients

Ein Bitcoin-Wallet ist eine spezielle Software für das Bitcoin-System. Die Wallets unterscheiden sich vor allem hinsichtlich des Ausmaßes, in dem Transaktionen verifiziert werden und an andere Teilnehmer des Netzwerkes weitergeleitet werden, der Sicherheit der Wallets und dem Grad der Netzwerksicherheit. Die ersten Versionen ermöglichten auch eine Teilnahme am Mining. Mit zunehmender Größe des Bitcoin-Systems und damit wachsenden Anforderungen an den Mining-Client, wurden spezielle Mining-Clients entwickelt, die ausschließlich Mining-Funktionalitäten bereitstellen.[42]

Das Wallet (englisch für „Geldbeutel“ oder „Portemonnaie“) steht sinnbildlich für eine Art virtuellen Geldbeutel, der die Bitcoins eines Teilnehmers enthält. Da Bitcoins jedoch nur innerhalb der Blockchain existieren und transferiert werden können, ist das Wallet eher vergleichbar mit einer Kreditkarte, die bestimmte Daten enthält, mit denen der Kunde Zahlungen tätigen kann, selbst aber kein Geld enthält.

Das Wallet ist ein digitaler Schlüsselbund, mit dem ein Benutzer nachweist, dass ihm eine gewisse Menge Bitcoins gehören, und der es ihm erlaubt, diese zu überweisen. Die Adressen zum Empfang von Zahlungen werden aus den Schlüsseln erzeugt. Es können beliebig viele Schlüssel generiert werden. [43]

3.2.1 Bitcoin Core Client/ Full-Node Client

Der ursprüngliche von Nakamoto Satoshi im Januar 2009 als Open-Source veröffentlichte Bitcoin Core ist in der Programmiersprache C++ geschrieben.
Der Bitcoin Core bietet die höchste Netzwerksicherheit und besitzt alle grundlegenden Funktionen. Da er die gesamte Blockchain auf dem einzelnen Rechner speichert, braucht er viel Festplatten- und Arbeitsspeicher (mehr als 40GB Daten) und es dauert sehr lange bis er vollständig geladen ist. In der Folge 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.[44]

---

[42] Vgl. Sixt (2017, S.34)
[43] Vgl. Kerscher (2014, S.60)
[44] Vgl. Platzer (2014, S.20ff)

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 Sybil- bzw. Double Spending-Attacken. Durch diese erzeugte Kopie des Netzwerkes entsteht ein weiteres Backup, welches diese Manipulationsversuche erschwert.[45]

3.2.2 SPV Client

SPV bedeutet Simplified Payment Verification und beschreibt eine Art von Client, welcher nicht die gesamte Blockchain herunterlädt und aktualisiert, sondern mithilfe eines Algorithmus, welcher wie ein Filter wirkt, nur für die Verwaltung der eigenen Adressen relevante Einträge herausfiltert und speichert.[46]

3.2.3 Serverabhängige- (Thin/Light-) Clients

Serverabhängige Clients, oder auch Thin-Clients genannt, besitzen keine lokale Kopie der Blockchain, sondern verwenden eine von ihren Anbieter gespeicherte Blockchain. Dies ist meist nur der Blockheader der einzelnen Blöcke, der sich aus den Hashes aller in einem Block verarbeiteten Transaktion zusammensetzt. Bei der Nutzung von Thin-/Light-Clients kommt das Simplified-Payment-Verification (SPV)-Verfahren zur Anwendung. Light oder Thin bezieht sich dabei auf die Größe/Menge der auf dem lokalen Gerät abgespeicherten Blockchain-Informationen. Es gibt auch bei den Light/Thin-Clients inzwischen die unterschiedlichsten Ausprägungen: Die Ladezeit und der benötigte Speicherplatz für diese Bitcoin-Clients sind beträchtlich kürzer als beim Bitcoin Core, in Relation dazu sinkt aber auch die Netzwerksicherheit und die Sicherheit der verwendeten Wallets. Auch der Anonymisierungsgrad sinkt beträchtlich dadurch, dass ein SPV-Client bei der Validierung von Transaktionen immer auf mit ihm verbundene Full-Node-Clients zugreifen muss.[47]

---

[45] Vgl. Sixt (2017, S.34)
[46] Vgl. Platzer (2014, S.25ff)
[47] Vgl. Sixt (2017, S.34)

3.2.4 Webwallets

Parallel zu den plattformbasierten Clients existiert eine Vielzahl von Webdiensten, die Online-Wallets anbieten. Das Bitcoin-Guthaben wird dabei vollständig an eine Adresse innerhalb des eigenen Kontos beim Anbieter der Plattform übertragen.

Dies ist eine Möglichkeit, um Daten online zu speichern und von jedem PC weltweit darauf zugreifen zu können. Die Sicherheit der Guthaben hängt hier aber vollständig von der serverseitigen Sicherheit und der nicht immer gegebenen Vertrauenswürdigkeit der Betreiber ab. Die Speicherung von Bitcoins in Online-Wallets schützt vor dem Risiko eines Datenverlustes durch einen Hardwaredefekt des heimischen Computers und gleichzeitig sind die Bitcoins überall verfügbar, nicht nur auf dem Gerät, an das sie gesendet wurden. Aber der Betreiber der Online-Wallets erhält ebenfalls Zugriff auf die eigenen Bitcoins. Zudem besteht auch bei Online-Wallets die Gefahr eines Hackerangriffs und des Diebstahls der gespeicherten Bitcoins.[48]

3.2.5 In-Browser-Clients

In-Browser-Clients sind eine sehr neue Entwicklung, sie dienen zum schnellen online Bezahlen und machen dieses mit einem Browser-Plugin sehr effizient. Die Schlüssel werden lokal gespeichert und das System basiert auf dem Open Source Prinzip, dies bedeutet, dass der Quelltext öffentlich und frei verfügbar ist. Außerdem gibt es die Möglichkeit Schlüssel mit einem Backup zu sichern.[49]

3.2.6 Hardware Wallets

Eine andere neue Entwicklung ist eine Art von Wallet mit sehr hoher Sicherheit, hierbei speichert man die Schlüssel auf einem kleinen Single Purpose Computer, also Computer, die nur diesen einen Zweck erfüllen. Um Transaktionen zu signieren, welche man in einer Online- oder einer lokalen Wallet erstellt hat, verwendet man die Schlüssel auf dem Gerät. Diese verlassen es niemals, so ist eine hohe Sicherheit gewährleistet, auch wenn

[48] Vgl. Kerscher (2014, S.62)
[49] Vgl. Platzer (2014, S.25ff)

der PC von Viren befallen ist oder von Dritten überwacht wird, da ein Versenden von Bitcoins ohne eine Bestätigung mit USB Verbindung zum Gerät nicht möglich ist. Zusätzlich sind ein Passwort und ein PIN notwendig, wodurch das Guthaben bei Verlust oder Diebstahl geschützt ist. Falls dies passiert, kann man ein neues Gerät kaufen und mit einem Backup alte Daten wiederherstellen, das bekannteste derartige Gerät nennt sich Trezor.[50]

3.3 Transaktionen von Bitcoins im Bitcoin-Netzwerk

Bei einer Transaktion werden aus dem Wallet des Absenders Bitcoins in die elektronische Geldbörse des Empfängers transferiert.
Im Unterschied zu einer Banküberweisung erfolgt die Transaktion aber peer2peer, also ohne den Umweg über eine zentrale Instanz. Die Nachverfolgbarkeit und Autorisierung des Zahlungsvorgangs werden im Sinne der asymmetrischen Verschlüsselung durch den Einsatz zweier Schlüssel sichergestellt.

Die in der Wallet gespeicherten Adressen beinhalten einen öffentlichen Schlüssel (Public Key) und einen privaten Schlüssel (Private Key). Während der öffentliche Schlüssel zum Empfangen von Beträgen weitergegeben werden kann, muss der private Schlüssel streng vertraulich behandelt werden, denn er ermöglicht die Bestätigung sämtlicher Transaktionen innerhalb einer Wallet, also auch die Übertragung des gesamten Bitcoin-Guthabens an andere Adressen.[51]

Bei der Generierung neuer Adressen wird zuerst ein privater Schlüssel erzeugt, auf dessen Basis durch den ECDSA (Elliptic Curve Digital Signature Algorithm) ein öffentlicher Schlüssel erzeugt wird. Aufgrund der Komplexität des Algorithmus kann durch den öffentlichen Schlüssel kein Bezug auf den privaten Schlüssel genommen werden. Durch die Berechnung mit den Verschlüsselungsmethoden SHA256 und RIPEMD-160 wird aus dem öffentlichen Schlüssel die Adresse generiert, die beispielsweise folgendermaßen aussieht: 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

[50] Vgl. Platzer (2014, S.25ff)
[51] Vgl. Kerscher (2014, S.72)

Adressen sind zwischen 27 und 34 Zeichen lang und bestehen nur aus Zahlen und Ziffern. Sie beginnen immer mit 1 oder 3. Die Adressen können auch nicht nur als Zahelen und Ziffern dargestellt werden, sondern auch als Barcode und in Form von QR-Codes. Die dazugehörigen öffentlichen und privaten Schlüssel werden in der wallet.dat-Datei der Clientsoftware gespeichert. Derartige Adressen können von der Software beliebig oft erzeugt werden. Die Adressen werden nicht zentral registriert oder gespeichert, sondern nur für die Transaktionen erzeugt und genutzt.[52]

Eine Bitcoin-Transaktion ist eine Fortführung vorangegangener Transaktionen. Durch Transaktionen werden einer oder mehreren Adressen Bitcoins gutgeschrieben, die selbst wiederum von einer oder mehreren Adressen aus dem Netzwerk stammen. Sie besteht daher aus einem oder mehreren Outputs (siehe Abbildung 6).

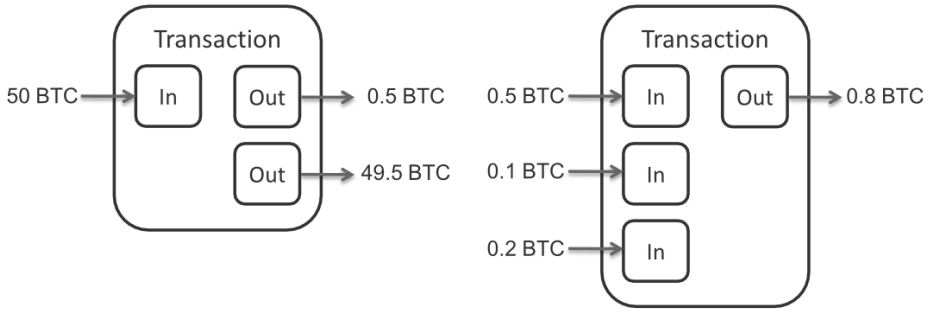

Abbildung 6: Inputs und Outputs von Transaktionen (Buch Bitcoin Blockchain Security)

Die Inputs verweisen dabei auf die Outputs vergangener Transaktionen, die dem Aussteller der aktuellen Transaktion geschickt wurde. Sie werden zusammengerechnet und bilden die Gesamtmenge an Bitcoins, die auf die Outputs verteilt werden kann. Bei einer Transaktion wird diese Menge durch mindestens einen Output an einen neuen Besitzer verschickt. Es ist zudem möglich, mit einer Transaktion Bitcoins an mehrere Empfänger zu versenden.[53]

Besteht eine Different zwischen der Summe an Bitcoins bei den Inputs und der Summe bei den Outputs, so wird sie als Transaktionsgebühr verstanden

[52] Vgl. Sixt (2017, S.37)
[53] Vgl. Karame (2016, S.36)

und geht an diejenigen, die die Transaktion bestätigt. Um eine Transaktion zu starten, muss der Empfänger der Bitcoin-Transaktion dem Sender seinen öffentlichen Schlüssel mitteilen. Der Sender schickt daraufhin den Bitcoin-Betrag durch die digitale Signatur des Hashwertes der vorherigen Transaktion und des ihm zugesandten öffentlichen Schlüssels an den Empfänger.

Wie in Abbildung 7 dargestellt beinhaltet eine Transaktion somit die Signatur des Übertragenden mit der Anweisung an die öffentliche Adresse des Empfängers zu zahlen und einen Hash mit dem Hinweis auf die vorhergehende Transaktion (bereits in der Blockchain als bestätigte Transaktionen enthalten). [54]

Der generierte Hashwert sagt nichts über den Inhalt aus und wird in der Folge verschlüsselt als digitale Signatur der jeweiligen Transaktion verschickt. Diesen Hash signiert der nächste Nutzer mit seinem privaten Schlüssel und bestätigt somit die Übertragung bzw. er entschlüsselt den Hashwert der Signatur und berechnet außerdem selbst den Hash der Transaktion, die Übereinstimmung der Hashes bestätigt die Senderidentität und die Originalität der Transaktion.[55]

[54] Vgl. Kersche (2014, S.75ff)
[55] Vgl. Karame (2016, S.41)

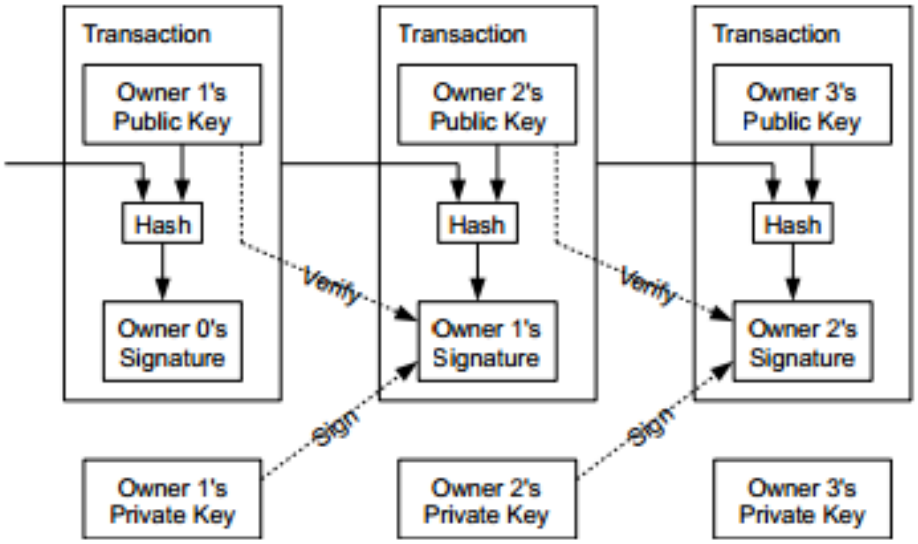

Abbildung 7: Darstellung von Transaktionen mit asymmetrischer Verschlüsselung (Buch)

Die asymmetrische Verschlüsselung, gemeinsam mit den digitalen Signaturen der Transaktionspartner sowie die Überprüfung der Transaktionscodes durch den Blockchain machen den Bitcoin praktisch fälschungssicher.

Das Bitcoin-Protokoll sieht vor, dass eine Transaktion mit sechs Bestätigungen, also sechs Blöcken in denen sie enthalten ist, als ausgeführt und nicht umkehrbar gilt. Um doppelte Ausgaben d.h. das wiederholte Versenden derselben Bitcoins, zu verhindern wird das Konzept des „Zeitstempels“ benutzt. Der Hashwert wird hier mit dem Zeitwert seines Vorgängers versehen. Dadurch können mehrfache Ausgaben derselben Bitcoins verhindert werden.

Wenn eine Adresse versucht, einen Bitcoin Betrag mehrfach zu versenden, wird im Netzwerk geprüft, welche Transaktion die älteste ist. Diese Transaktion bleibt bestehen, während alle danach erfolgten für ungültig erklärt und verworfen werden.[56]

[56] Vgl. Sixt (2017, S.39)

3.3.1 Validierung von Transaktionen im Bitcoin-Netzwerk

Die Übermittlung der Zahlung wird durch mehrere im Netzwerk generierte Bestätigungen festgestellt. Um zu verhindern, dass ein Teilnehmer seine Bitcoins mehrfach ausgibt (Double Spending), werden die Transaktionen im Netzwerk durch einen Flooding-Algorithmus verteilt. Mit Hilfe dieses Algorithmus gibt die Client-Software an jeden anderen erreichbaren Client, der noch nicht informiert wurde, Informationen weiter, d.h, wenn eine Transaktion gesendet wird, sendet der Client die Transaktion an alle anderen Clients, die mit dem Block zusammenhängen.

Diese Clients prüfen in der Folge in der bei ihnen gespeicherten Blockchain, in der alle vorhergegangenen Transaktionen gespeichert sind, ob diese Transaktion gültig ist (Prüfung der Besitzverhältnisse des zu übertragenden Tokens). Bereits zu diesem Zeitpunkt wird die Transaktion mit einem Zeitstempel versehen. Wird die Transaktion als valide eingestuft, schicken diese Clients sie wiederum an die Clients, mit denen sie verbunden sind, weiter.[57]

Dieser Prozess geht solange, bis eine Transaktion alle momentan aktiven Cleints im Netzwerk erreicht hat. Die Transaktion gilt jedoch erst als bestätigt, wenn sie in einem Block aufgenommen wurde. Der Bitcoin-Algorithmus sieht vor, dass die Generierung eines Blocks und damit die endgültige Bestätigung einer Transaktion etwa zehn Minuten erfordern. In diesen zehn Minuten verarbeitet das Netzwerk die durchgeführten Transaktionen auf eine irreversible Art und Weise.

Miner generieren Blöcke, und sollte es gelingen einen Proof-of-Work zu erbringen, fügen sie unbestätigte Transaktionen in einen Block ein und senden diesen an die anderen Clients im Netzwerk. Es dauert zwischen einer und zehn Sekunden, bis ein Block 1000 andere Clients erreicht hat. Sobald ein Client einen Block erhält, fügt er ihn an seine Blockchain an und nutzt ihn, um künftige Transaktionen zu verifizieren. Der auf diese Weise neu informierte

[57] Vgl. Sixt (2017, S.34ff)

Client schickt keine Antwort, sondern sendet die Information an alle ihm bekannten Teilnehmer außer dem Sender der Information weiter.
Da informierte Teilnehmer keine weiteren Nachrichten aussenden, endet der Algorithmus automatisch, wenn alle erreichbaren Teilnehmer informiert wurden. Die erste Bestätigung der auf diesem Weg verbreiteten Transaktion dauert durchschnittlich 10 Minuten.[58]

Das Bitcoin-Protokoll sieht vor, dass Transaktionen nach 6 Bestätigungen als umkehrbar gelten. Meist geschieht dies sehr schnell, je nach Auslastung des Netzwerkes kann es bis zur Bestätigung aber auch mehrere Stunden dauern. Um den Vorgang zu beschleunigen, kann jeder Nutzer eine Gebühr entrichten, damit die Transaktion bevorzugt wird.

3.3.2 (Pseudo)- Anonymität

Grundsätzlich gibt es kein Erfordernis für den einzelnen Nutzer, sich bei Teilnahme am Bitcoin-System zu legitimieren. Eine Transaktion kann ohne Angabe persönlicher Daten durchgeführt werden. Der Nutzer muss seinen realen Namen nicht angeben, das System ist anonym. Durch die Nutzung einer Bitcoin-Adresse bekommt jedoch jeder Nutzer eine Pseudoidentität zugewiesen. Für das Einrichten des Wallets ist lediglich die Installation einer Software auf dem eigenen Rechner nötig. Die zur Anmeldung erforderliche E-Mail-Adresse kann man vorher als „Wegwerfadresse“ bei einem Dienst generieren, der die Identität des Inhabers verschleiert. [59]

Grundsätzlich kann jeder Nutzer beliebig viele Schlüsselpaare bzw. Bitcoin-Adressen haben. Er kann für jede Transaktion eine andere, neue Adresse verwenden und somit Pseudonymen haben. Analog hat ausschließlich der Nutzer auch volle Kontrolle über seine Bitcoins. Die angewandte Kryptografie erlaubt es den Benutzern, ihr Passwort einzugeben und einander direkt digitales Geld zu schicken, ohne das Passwort irgendeiner Person oder Institution anvertrauen zu müssen.[60]

---

[58] Vgl. Karame (2016, S.43ff)
[59] Vgl. Sixt (2017, S.33)
[60] Vgl. Paulsen (2014, S.26ff)

Die Blöcke in der Blockchain beinhalten die gesamte Historie der Bitcoin-Adressen, an die ein Bitcoin gesendet wurde. Damit werden alle Transaktionen öffentlich, nachvollziehbar und einzelnen Bitcoin-Adressen zuordenbar erfasst. Wenn die realen Identitäten der Nutzer dieser Bitcoin-Adressen nicht bekannt sind und jede Adresse nur einmal genutzt wird, dann verrät diese Information nur, dass eine unbekannte Person Bitcoins an eine andere Bitcoin-Adresse gesendet hat. Die Chance, anonym oder pseudonym zu bleiben, hängt somit davon ab, dass man keine Identitätsinformationen in Zusammenhang mit der Bitcoin-Adresse, die man benutzt, offenbart.[61]

Wenn eine reale Identität jedoch eindeutig mit einer Bitcoin-Adresse verknüpft ist, dann geht jegliche Privatsphäre für alle vergangenen und zukünftigen Transaktionen, die dieser Adresse zugeordnet werden können, verloren. Da die Blockkette öffentlich verfügbar ist, kann buchstäblich jedermann diese Art von Deanonymisierung durchführen, ohne sich selbst identifizieren zu müssen. Die Privatsphäre der Bitcoin-Transaktionen ist damit potenziell sogar weit schlechter geschützt als bei Nutzung des traditionellen Finanzsystems.[62]

3.3.3 Transaktionsgebühren

Nutzer können bei einer Transaktion auch eine Transaktionsgebühr angeben. Diese Gebühr darf sich der erfolgreiche Miner gutschreiben. Die Gebühr ist allerdings nicht zwingend im Bitcoin-Protokoll vorgeschrieben. Da ein Miner jedoch frei entscheiden kann, welche Transaktionen er in einen Block aufnimmt, erhöht eine Transaktionsgebühr die Wahrscheinlichkeit der raschen Aufnahme der Transaktion in einen Block. Mit der Skalierbarkeitsthematik der Bitcoin-Blockchain nimmt die Transaktionskostenthematik an Brisanz zu. Seit dem 10. Juni 2012 lauten die minimalen Transaktionsgebühren im Original Bitcoin Client wie folgt: Für das Einbetten einer Transaktion in einem neuen Block werden 0.0005 BTC akzeptiert. Für das Weiterleiten von Transaktion an andere Bitcoin Clients sind es 0.0001 BTC.

[61] Vgl. Paulsen (2014, S.28ff)
[62] Vgl. Sixt (2017, S.33)

Eine Transaktion kann ohne Gebühren versendet werden wenn zum einen die Transaktion kleiner ist als 10 (SI) Kilobytes (10.000 Bytes) und zum anderen alle Transaktionsausgänge 0.01 BTC oder mehr betragen.[63]

[63] Vgl. Bitcoin Wiki (2017)

4 Erstellung von Bitcoins – Bitcoin Mining

4.1 Der Block

Blöcke sind das zentrale Objekt im Bitcoin System. Mit der Erzeugung von Blöcken, dem Mining, werden Bitcoins erzeugt. In den Blöcken werden die Transaktionen gespeichert und bestätigt. Der erste Teil eines Blocks ist der Hash-Wert des Blocks. Es handelt sich dabei um einen doppelten SHA-256-Hash-Wert, wie in Abbildung 8 dargestellt. Es folgt die Versionsnummer des Blocks. Darauf folgt der Hash des vorherigen Blocks.

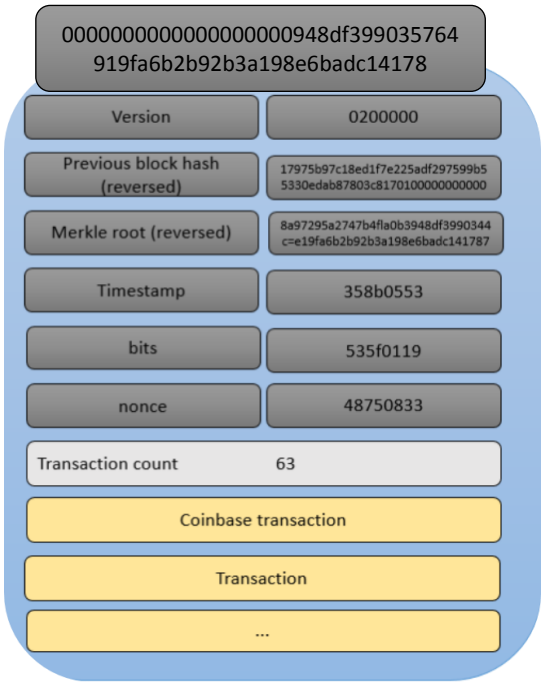

Abbildung 8: Darstellung Block aus Blockchain (eigene Darstellung)

Der Genesis-Block hat hier einen 0-Wert. Als nächstes wird die Merkle root dargestellt. Hier handelt es sich um einen binären Merkle tree, der mit einem doppelten SHA-256-Hash-Wert dargestellt wird. (doppelter SHA-256-Hash-Wert aller vorherigen Transaktionen). Der darauffolgende Timestamp protokolliert die Erstellungszeit des Blocks. Der nachfolgende Wert Bits wird als Target zur Zeit der Erstellung des Blocks gespeichert. Der anschließende Nonce ist der Anfangswert zur

Berechnung des nächsten Hash-Wertes und wird nach erfolgloser Berechnung inkrementiert. Der Wert size gibt die gesamte Größe des Blocks an.[64]

4.2 Proof-of-Work

Die ursprüngliche und seit Bitcoin gebräuchlichste Variante ist der Proof-of-Work-Mechanismus, bei dem die Nutzer des Bitcoin-Netzwerks darum konkurrieren, der Datenbank neue Transaktionen hinzufügen zu können. Satoshi Nakamoto beschrieb den Prozess des Proof of Work (PoW) im ursprünglichen Bitcoin Whitepaper wie folgt: Neue Transaktionen werden an alle Knoten geschickt. Jeder Knoten sammelt die neuen Transaktionen in einem Block. Jeder Knoten versucht, die Proof-of-Work-Aufgabe für seinen Block zu lösen, d.h. ein mathematisches Rätsel, dessen Lösung nur durch Testen gefunden werden kann.[65]

Zu diesem Zweck enthält bei dieser Variante jeder Block eine sog. „Nonce“, d.h. denjenigen Parameter, der im Rahmen des Proof of Work testweise verändert wird, um schließlich den richtigen Hash-Wertebereich zu erhalten.[66]

4.3 Bitcoin Mining

Die Bezeichnung Mining entstand, weil das Errechnen der Bitcoins mit dem Schürfen von Rohstoffen wie beispielsweise Gold vergleichbar ist, d.h. unter hohem Aufwand werden kleine Bitcoin-Mengen gewonnen.

Ein beliebiger Rechner, der sich durch eine Software am Mining beteiligen kann, bekommt durch das Bitcoin-Netzwerk die Aufgabe zugewiesen, ein mathematisches Problem auf Basis der letzten verfügbaren Transaktionen zu lösen. Zur Lösung des Problems muss der Computer, unter Verwendung eines doppelten SHA256-Algorithmus, einen Schlüssel in Form eines Hashwertes finden, der mit der Liste der letzten Transaktionen und dem Hashwert des letzten abgeschlossenen Blocks in der Blockchain einen neuen Hash generiert.[67]

Jeder neue Hashwert muss eine vom Netzwerk geforderte Schwierigkeitsstufe, die als eine bestimmte Zahl von Nullen am Anfang des Hashwertes ausgedrückt wird, erfüllen.

---

[64] Vgl. Mölleken (2012, S.33)
[65] Vgl. Sixt (2017, S.40)
[66] Vgl. Mölleken (2012, S.35)
[67] Vgl. Mölleken (2012, S.33)

Der Computer kann den entsprechenden Wert nur durch die Versuch-und Irrtum-Methode ermitteln. Je mehr Nullen am Anfang des Hashwertes stehen, desto schwieriger ist die Berechnung, denn der Computer muss so viele Werte berechnen, bis sich ein Hashwert mit den vielen Nullen ergibt.[68]

Der Schwierigkeitsgrad für das Lösen der Blöcke wird alle 2.016 Blocke, was einem Zeitraum von zwei Wochen entspricht, angepasst, um zu gewährleisten, dass durchschnittlich alle zehn Minuten ein Block gelöst und neue Bitcoins generiert werden.

Der Schwierigkeitsgrad ist variabel, er lässt sich durch die Anzahl der Nullen am Beginn des Hashwertes regulieren. Je mehr Rechenkapazität zur Verfügung steht, desto höher fällt der Schwierigkeitsgrad in Form zusätzlicher Nullen am Anfang der Blöcke aus.[69]

Aufgrund der zunehmenden Nutzerzahl stieg auch der Schwierigkeitsgrad und 2011 war der Schwierigkeitsgrad so hoch, dass ein einzelner Rechner mehrere Jahre gebraucht hätte, um einzelne Bitcoin Blöcke zu lösen.

Sobald der Computer die Aufgabe lösen konnte, schickt er seinen Block an alle anderen. Der Block wird von den Anderen überprüft und wird nur akzeptiert, wenn die Kriterien der Transaktionen erfüllt sind. Die Akzeptanz drücken die anderen so aus, dass sie die digitale Signatur dieses Blocks (den Hash-Wert) verwenden, um ihn im nächsten Block als den vorangegangenen zu kennzeichnen. Wird ein passender Wert gefunden und der Block gelöst, wird als Erstes eine Transaktion generiert, die an die Adresse des Rechners geschickt werden, der den richtigen Hashwert errechnet hat. Dieser Rechner erhält den Bonus in Form von Bitcoins. [70]

Im Durchschnitt entsteht wie oben bereits erwähnt alle zehn Minuten ein Block. Um eine zu schnelle Ausschüttung aller Bitcoins zu verhindern, halbieren sich die in den Blöcken enthaltenen Einheiten alle 210.000 Blöcke, was einem Zeitraum von ungefähr vier Jahren entspricht. So erhalten seit dem Sommer 2013 die Miner pro Block nur mehr 25 Bitcoins und ab dem Sommer

[68] Vgl. Kerscher (2014, S.80ff)
[69] Vgl. Kerscher (2014, S.86)
[70] Vgl. Mölleken (2012, S.38)

2016 wird sich dieser Betrag nochmals halbieren auf 12,5 Bitcoins.[71] (1 Block alle 10 Minuten = 144 Blöcke am Tag = 4.320 Blöcke im Monat = 52.560 Blöcke im Jahr).

Die letzten der 21 Millionen Blöcke werden im Jahr 2140 erzeugt werden. Danach findet keine neue Generierung mehr statt, sondern nur noch ein Transfer der bestehenden Bitcoins.

Wichtiger als die Rechenoperationen an sich ist die zur Verfügung stehende Leistungsfähigkeit der Computer zur Berechnung der Aufgaben. Die Rechenkapazität des Netzwerkes wird in Hashes pro Sekunde gemessen.

Ein Hashwert ist ein Wert fester Länge, typischerweise codiert als hexadezimale Zeichenkette, der aus beliebigen Eingabedaten gewonnen wird. Da die Rechenleistung immer weiter ansteigt, ergeben sich auch ansteigende Messgrößen:

1.000 H/s = 1KH/s (Kilo hash pro Sekunde)

1.000.000.000.000 H/s = 1 TH/s (Tetra hash pro Sekunde)

Derzeit hat das Bitcoin-Netzwerk eine Rechenkapazität von ca. 110 bis 130 Terahashes in der Sekunde.[72]

[71] Vgl. Sixt (2017, S.40)
[72] Vgl. Kerscher (2014, S.89)

5 Schlussbetrachtung und Ausblick

Anhand der technischen Untersuchung und der Entwicklung dezentraler, elektronischer Währungen können einige Schlüsse gezogen werden.

Währungen, die ausschließlich digital existieren, sind neu und fanden über die vergangenen Jahre immer mehr Nutzer. Ohne Banken, Regulierungen, Steuern oder andere externe Einflüsse könnte diese Art der Währung sich in verschiedenen Ländern etablieren. In den vergangenen 3 Jahren hat sich allerdings gezeigt, dass ohne jeglichen Einfluss auf dezentrale
Währungen viele unglückliche Ereignisse wie Hackerattacken oder Diebstähle passieren. Auch illegale Geschäfte z.B. mit Drogen können kaum unterbunden werden.

Da Coin-Währungen allerdings global funktionieren und durch einzelne Regierungen kaum zu unterbinden sind, sollte es im Interesse von Regierungen sein, gemeinsam mit anderen Regierungen über die Existenz von Coin-Währungen zu diskutieren. Auch aus der Perspektive der Nutzer sollte es von Vorteil sein, wenn Regierungen dezentrale Währungen unter bestimmten Bedingungen anerkennen. Jederzeit können erhebliche Kursschwankungen durch Haltungswechsel einzelner Regierungen gegenüber den digitalen Währungen auftreten.

6 Literaturverzeichnis

Blockchain.info. (2017). *Blcockchain.info*. Abgerufen am 20. 06 2017 von www.blockchain.info

Dr. Philipp Giese, M. P. (2016). *Die Bitcoin Bibel: Das Buch zur digitalen Währung.* Kleve: BTC-ECHO.

Garzik, J. (2015). *Public versus Private Blockchains Part 1: Permissioned Blockchains.* Bitfury Group.

Hurr, E. (2016). *Smart Contracts und ihre Verwendungsmöglichkeiten im Finanzsektor.* Köln: Grin Verlag.

IT, K. ö. (2017). *Blockchain*. Abgerufen am 05. 05 2017 von Kompetenzzentrum öffentliche IT: http://www.oeffentliche-it.de/-/blockchain

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

Kerscher, D. (2014). *Bitcoin Funktionsweise, Chancen und Risiken der digitalen Währung.* (2. ü. 2014, Hrsg.) Dingolfing.

Klemm, T. (30. 05 2017). *Verrückte Währungswelt*. Abgerufen am 03. 06 2017 von Frankfurter Allgemeine: http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/bitcoin-wechselkurs-die-gruende-fuer-die-juengste-preisrally-15035648.html

Kryptowissen.de. (2017). *Kryptographie*. Abgerufen am 15. 05 2017 von http://www.kryptowissen.de/kryptographie.html

Lexikon, O. P. (2017). *One Page Wiki Digitales Marketing Lexikon*. Abgerufen am 05. 05 2017 von Peer-to-Peer: https://de.onpage.org/wiki/Peer-to-Peer

Liesenjohann, M. (2016). *Blockchain #Banking.* Berlin: Bitkom.

Mölleken, D. (2012). *Bitcoin Geld ohne Banken - Ist das möglich?* Hamburg: Diplomica Verlag.

Nestler, F. (01. 02 2017). *Bitcoin vor dem nächsten Sprung nach oben*. Abgerufen am 01. 06 2017 von Frankfurter Allgemeine: http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/bitcoin-kurs-errreicht-in-euro-neue-rekorde-14603376.html

Paulsen, C. (2014). *Sicherheit in vernetzten Systemen: 21. DFN Workshop.* Hamburg: DFN.

Platzer, G. (2014). *Bitcoin kurz&gut: Banking ohne Banken.* Köln: O'Reilly Verlag.

Roßbach, P. D. (2016). *Blockchain-Technologien und ihre Implikationen.* Frankfurt: Frankfurt School of Finance and Management.

Sansonetti, D. R. (01. 09 2014). *Bitcoin: Virtuelle Währung mit Chancen und Risiken*. Abgerufen am 01. 06 2017 von Die Volkswirtschaft: http://dievolkswirtschaft.ch/de/2014/09/sansonetti-3/

Sixt, E. (2017). *Bitcoins und andere dezentrale Transaktionssysteme:Blockchains auf Basis einer Kryptoökonomie.* Wiesbaden: Springer Gabler.

Voshmgir, S. (2016). *Blockchain Smart Contracts und das dezentrale Web.* Berlin: Technologiestiftung Berlin.

Wiki, B. (2017). *Transaktion*. Abgerufen am 06. 06 2017 von Bitcoin Wiki: https://de.bitcoin.it/wiki/Transaktion

.