LEUPHANA
UNIVERSITÄT LÜNEBURG

Die Blockchain.

Ein Vergleich zwischen Bitcoin und Ethereum.

The Blockchain.

A comparison between Bitcoin and Ethereum.

Bachelorarbeit

zur Erlangung des Grades Bachelor of Arts (B.A.)

im Studiengang Betriebswirtschaftslehre

Leuphana Universität Lüneburg

Erstprüfer: Herr Thomas Slotos

Zweitprüfer: Herr Prof. Dr. Matthias Pelster

Eingereicht von: 30.01.2017

Schneekluth, Marco

Inhaltsverzeichnis

Inhaltsverzeichnis II
Abbildungsverzeichnis IV
Tabellenverzeichnis V
Abkürzungsverzeichnis VI
1. Einleitung 1
2. Übersicht 3
2.1. Bitcoin – Blockchain 1.0 3
2.2. Ethereum – Blockchain 2.0 7
2.3. Blockchain 10
2.4. Geld und Währung 11
3. Einführung Kryptografie 14
3.1. Asymmetrische Verschlüsselung 16
3.2. Hash-Funktionen 17
3.3. Funktionsweise bei Bitcoin 18
4. Technische Grundlagen der Blockchain 22
4.1. Netzwerk 22
4.2. Transaktionen 24
4.3. Bitcoin Blockchain 27
4.3.1. Blockstruktur 28
4.3.2. Mining 30
4.4. Ethereum Blockchain 33
4.4.1. Accounts, Nachrichten und Transaktionen 33
4.4.2. Blockstruktur 35
4.4.3. Mining 37
5. Vergleich Bitcoin und Ethereum 40
5.1. Blockchain 1.0. – Kryptowährung 40
5.1.1. Verteilung der Währung 40
5.1.2. Kryptowährung und traditionelle Währungen 43
5.1.3. Geschwindigkeit der Bestätigungen 45
5.2. Blockchain 2.0. – Verträge 45
5.3. Vergleich der Blockchain 48
5.3.1. Sicherheit 48

5.3.2. Skalierbarkeit 51
5.3.3. Dezentralität 52
5.3.4. Mining und ökologische Folgen 54
6. Fazit und Ausblick 56
Literaturverzeichnis 60
Eidesstattliche Erklärung 64

Abbildungsverzeichnis

ABBILDUNG 1: PRIVATER SCHLÜSSEL, ÖFFENTLICHER SCHLÜSSEL UND BITCOIN-ADRESSE 20
ABBILDUNG 2: MERKLE-BAUM 29
ABBILDUNG 3: BLOCKCHAIN 32

Tabellenverzeichnis

TABELLE 1: MEILENSTEINE VON ETHEREUM 9
TABELLE 2: EIGENSCHAFTEN VON HASH-FUNKTIONEN 18
TABELLE 3: DATENSTRUKTUR BITCOIN-TRANSAKTION 26
TABELLE 4: DATENSTRUKTUR BITCOIN-BLOCK 28
TABELLE 5: FELDER EINES ETHEREUM-ACCOUNTS 34
TABELLE 6: VORTEILE VON UTXO UND ACCOUNTS ALS ZUSTAND 35
TABELLE 7: DATENSTRUKTUR ETHEREUM-BLOCK 36
TABELLE 8: EINHEITEN IN ETHEREUM 38

Abkürzungsverzeichnis

ASIC ..... Application-specific integrated circuit
BTC..... Bitcoin
CPU.....Central Processing Unit
DAO..... Dezentrale, autonome Organisation
DApps.....Dezentralen Applikationen
ECDSA ..... Elliptic Curve Digital Signature Algorithm
Et al..... Und andere
EVM ..... Ethereum Virtual Machine
GPU ..... Graphics Processing Uni
HTTP .....Hypertext Transfer Protocol
ICO .....Initial Coin Offering
NIST ..... National Institute of Standards and Technology
NSA ..... National Security Agency
P2P..... Peer-to-Peer
PoS.....Proof-of-Stake
PoW .....Proof-of-Work
RIPEMD ..... RACE Integrity Primitives Evaluation Message Digest
SHA ..... Secure Hash Algorithm
SPV .....Simplified Payment Verification
TCP .....Transmission Control Protocol
TH/s .....Terrahash pro Sekunde
UDP ..... User Datagram Protocol
UTXO ..... Unspent Transaction Output

1. Einleitung

Der Begriff Blockchain tritt zum ersten Mal in Verbindung mit der Kryptowährung Bitcoin im 21. Jahrhundert auf. Bitcoin basiert auf einer dezentralen Open Source Software, welches Ende 2008 erstmals vorgestellt und kurz danach gestartet wird.[1]

Das anfänglich beschriebene Protokoll von Bitcoin hat sich mittlerweile zu einem Phänomen entwickelt, dass unter dem Begriff Kryptoökonomie zusammengefasst wird. Es ist ein Phänomen, dass eine Revolution in vielen Bereichen der Wirtschaftssysteme hervorrufen wird. Im Zentrum stehen dabei dezentrale und fälschungssichere Datenbanken, dessen Wertschöpfung auf kryptografischen Algorithmen basieren. [2]

Mittlerweile ist Bitcoin nicht mehr die einzige Kryptowährung, denn innerhalb der letzten sieben Jahre hat sich ein großes, vielseitiges Universum von Kryptowährungs- und Kryptotransaktionssystemen entwickelt. Am 11.10.2016 sind auf der Webseite coinmarketcap.com 711 verschiedene Kryptowährungen eingetragen, die einen Wechselkurs besitzen. Es kann davon auszugehen sein, dass noch eine Vielzahl weiterer Kryptowährungen existieren, welche keinen Wechselkurs ausweisen, unter privater Nutzung stehen oder sich noch in Entwicklung befinden. All diese Entwicklungen werden durch die Blockchain vereint. Auch Swan sieht in der Blockchain die größte technologische Innovation von Bitcoin. Sie vergleicht dabei die Blockchain-Technologie mit dem revolutionären Potential des Internets und ordnet Blockchain nach der mobilen und sozialen Vernetzung als fünftes, disruptives Computerparadigma ein. Sie untergliedert die zahlreichen Systeme in Bezug auf die Blockchain in drei Kategorien. [3]

Blockchain 1.0 stellt Währungen, den Einsatz von Kryptowährungen in Anwendung bezogen auf Bargeld, wie Währungstransfer, Überweisung und digitalen Zahlungssystemen, dar. Blockchain 2.0 sind Verträge, wirtschaftlicher Märkte und Finanzanwendungen, die die Blockchain umfangreicher als einfache Bargeldtransaktionen benutzen, beispielsweise für Smart Contracts, Smart Property, Aktien, Titel,

[1] Nakamoto (2008).
[2] Vgl. Sixt (2016), S. 1ff.
[3] Vgl. Swan (2015), S. ix.

etc. Blockchain 3.0. sind Blockchain-Anwendungen jenseits von Währungen, Finanzen und Märkten, beispielsweise in den Gebieten Administration, Gesundheit, Wissenschaft, Literatur, Kultur und Kunst.

Für den Vergleich in dieser Arbeit werden jeweils die beiden bekanntesten Kryptowährungen der ersten beiden Kategorien ausgewählt. In der ersten Kategorie handelt es sich um das vorher bereits erwähnte dezentrale Zahlungssystem Bitcoin. In der zweiten Kategorie wird Ethereum, eine Entwicklungsplattform für dezentrale Applikationen, vorgestellt. Beide Systeme können sowohl als digitale Währung in Blockchain 1.0., als auch als Verträge im Rahmen von Blockchain 2.0. betrachtet werden.

Die vorliegende Arbeit beinhaltet sechs Kapitel, die in mehrere Unterkapitel gegliedert sind. Zuerst wird ein allgemeiner und historischer Überblick über die relevanten Themengebiete gegeben. Die beiden Systeme, Bitcoin und Ethereum, die Blockchain und Geld und Währungsdefinition werden betrachtet. Im dritten Kapitel werden relevante Aspekte der Kryptografie vorgestellt, um später die Eigenschaften der Blockchain besser verstehen zu können. Besonderer Fokus liegt dabei auf asymmetrischen Algorithmen und Hash-Funktionen. Im vierten Kapitel werden in den ersten beiden Unterkapiteln weitere relevante Komponente beschrieben, mit der die Blockchain interagiert. Im weiteren Verlauf des vierten Kapitels wird die Bitcoin Blockchain und die Ethereum Blockchain gesondert und detaillierter beleuchtet. In diesem Kapitel werden sowohl die unterschiedlichen Ziele der Projekte, aber auch die Entwicklung der Blockchain an sich, deutlich. Anhand der Merkmale der jeweiligen Blockchain ergeben sich Schnittpunkte, die miteinander verglichen werden können. Im fünften Kapitel werden dann Bitcoin und Ethereum im Allgemeinen und die Blockchains jener im Speziellen miteinander verglichen. Die Vergleichspunkte orientieren sich sowohl an ökonomischen, als auch an technischen Gesichtspunkten. Im letzten Kapitel wird das Ergebnis des Vergleichs präsentiert und ein Fazit gezogen. Darüber hinaus soll ein Ausblick über zukünftige Entwicklungen der Blockchain-Technologie, Bitcoin und Ethereum gegeben werden.

2. Übersicht

2.1. Bitcoin – Blockchain 1.0

Der Begriff Bitcoin setzt sich aus den Wörtern *Bit* und *Coin* zusammen. Bit steht für die kleinste elektronische Speichereinheit in der Informatik und Coin ist das englische Wort für Münze. Beim Bitcoin handelt es sich demnach um eine digitale Münze. Grundsätzlich wird bei Bitcoin zwischen dem Protokoll und der Technik und der digitalen Währung Bitcoin (BTC) unterschieden. Am 29.01.2017 kostet ein BTC 860 Euro. Mit einer Marktkapitalisierung von 13,9 Milliarden Euro ist BTC auch die mit Abstand erfolgreichste Kryptowährung.

Im Oktober 2008 veröffentlichte Satoshi Nakamoto das Diskussionspaper *Bitcoin: A Peer-to-Peer Electronic Cash System*[4], der die Motivation und Funktionsweise von Bitcoin initial beschreibt und vorstellt. Nakamoto ist bis heute ein Pseudonym für den anonymen Erfinder von Bitcoin. Ob es sich bei ihm um eine Einzelperson oder eine Gruppe von Personen handelt ist nicht sicher.[5] Nakamoto hat Bitcoin primär als dezentrales, digitales Zahlungssystem konzipiert.[6]

Einige Wochen danach am 3. Januar 2009 startete Nakamoto die Bitcoin-Software manuell mit dem *Genesis-Block* und markiert somit den offiziellen Start von Bitcoin. Im Genesis-Block hinterlässt Nakamoto eine versteckte Nachricht mit dem Text "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." Dieser Text dient als Nachweis dafür, dass der Block auch an diesem Tag erstellt wurde, indem auf den damaligen Titel der britischen Zeitung *The Times* verwiesen wird.[7]

Nakamoto hat Bitcoin quelloffen gestaltet und andere interessierte Entwickler in die Weiterentwicklung eingebunden. 2011 hat sich Nakamoto aus dem Projekt Bitcoin zurückgezogen und die Weiterentwicklung einer Gruppe von Entwicklern übergeben. Trotzdem hat weder Nakamoto noch sonst jemand Kontrolle über das Bitcoin-System, was auf kompletttransparenten, mathematischen Prinzipien basiert.

---

[4] Nakamoto (2008).
[5] Vgl. Sixt (2016), S. 5.
[6] Vgl. Nakamoto (2008), S. 1.
[7] Vgl. Antonopoulos (2014), S. 163.

Nakamoto beschreibt in dem Diskussionspapier die Motivation hinter dem elektronischen Zahlungssystem. Bitcoin versucht die Notwendigkeit von Finanzinstitutionen im E-Commerce Bereich überflüssig zu machen. Diese Finanzinstitutionen treten bei elektronischen Zahlungen als vertrauenswürdige Drittinstanzen auf, um jene Zahlungen zwischen zwei Marktteilnehmern zu verifizieren.

Für diese auf Vertrauen basierende Methode nennt Nakamoto einige inhärente Schwachpunkte. Eine Hauptschwäche sind die aus der Vermittlungsdienstleistung hervorgehenden erhöhten Transaktionskosten, welche für Transaktionen mit niedriger Menge eine Belastung darstellen und die minimale praktische Transaktionsgröße limitiert. Des Weiteren erhöht die Möglichkeit Transaktionen zu stornieren, die Notwendigkeit von Vertrauen zwischen den Marktteilnehmern. Die Kosten und Unsicherheiten könnten vermieden werden, indem Bargeld benutzt wird. Allerdings existiert bisher kein Mechanismus für Zahlungen über einen Kommunikationskanal ohne vertrauenswürdige Dritte. Nakamoto schlägt ein elektronisches Zahlungssystem vor, welches auf kryptografischen Nachweis anstatt auf Vertrauen basiert, sodass zwei Marktteilnehmer direkt miteinander Geschäfte tätigen können, ohne die Notwendigkeit von einem vertrauenswürdigen Dritten.[8]

Diese initialen Gedanken Nakamotos stellen den Ursprung und den Lösungsansatz von Bitcoin dar. Sein Diskussionspapier beinhaltet die Funktionsweise des Systems, die im Folgenden kurz angerissen wird.

Bitcoin ist ein elektronisches Zahlungssystem, welches auf kryptografischen Nachweis basiert. In einem Peer-to-Peer-Netzwerk agieren ebenbürtige Netzwerkknoten untereinander und direkt ohne Mittelsmann. Knoten können das Netzwerk nach Belieben verlassen oder betreten. Die digitalen Einheiten BTC, welche als Währung benutzt werden, sind Adressen zugeordnet. Adressen werden über sogenannte digitale Brieftaschen (*Wallets*) verwaltet. Wallets enthalten einen öffentlichen und einen privaten kryptografischen Schlüssel, um Zahlungen zu genehmigen. Der öffentliche Schlüssel wird dabei durch die Adresse repräsentiert.[9] Vereinfacht ausgedrückt verfügt eine Wallet somit über öffentliche Konten und dazugehörige Passwörter. Durch diese Autorisierung können Einheiten von Adresse zu Adresse be-

[8] Nakamoto (2008), S. 1.
[9] Vgl. Antonopoulos (2014), S. 61.

wegt werden. Dieser Vorgang wird Transaktion genannt. Transaktionen werden sofort öffentlich ans Netzwerk übermittelt und in Datenblöcken zusammengefasst. Jeder Block wird an den vorigen Block angehängt, sodass die Blockchain, eine öffentlich einsehbare Datenbank der bisherigen Transaktionen, entsteht. Die Knoten müssen für das Erstellen eines Blocks ein kryptografisches Problem lösen, welches durch Anpassungsparameter im Durchschnitt immer zehn Minuten dauert. Dieser Vorgang wird *Mining* genannt und stellt die Verifizierung der in den Blöcken befindlichen Transaktionen dar. Die hierfür benötigte Computerrechenleistung wird mit dem Erhalt von neuen BTC und einer kleinen, freiwilligen Transaktionsgebühr entlohnt. Die Wahrscheinlichkeit das Problem zu lösen und somit einen neuen Block zu „finden" und die neugeschaffenen Einheiten als Belohnung zu erhalten, ist durch die Rechenleistung des Computers, die in Hashs pro Sekunde gemessen werden, definiert. Je höher die eigene Rechenleistung in Relation zu der gesamten Rechenleistung des Netzwerkes ist, desto höher ist die Wahrscheinlichkeit. War es am Anfang noch möglich mit dem eigenen Rechner nach BTC zu schürfen, ist es heute ohne den Betrieb von riesigen, hochspezialisierten Mining-Lagerhäusern oder im Zusammenschluss von Rechner in Gruppen praktisch nicht mehr möglich einen Block als Einzelner zu finden. Die Gesamtanzahl von BTC-Einheiten ist auf knapp 21 Millionen Stück festgesetzt, wobei ein BTC acht Nachkommstellen haben kann und somit die effektive Anzahl an digitalen Einheiten knapp 2,1 Billiarden (2.099.999.997.690.000) beträgt. Diese kleinste Einheit wird zu Ehren des Erfinders Satoshi genannt.

Bitcoin ist nicht der erste Versuch ein dezentrales Zahlungssystem zu erstellen. Es ist aber das erste was gut genug funktioniert, um eine gewisse Akzeptanz in der Öffentlichkeit zu erhalten. Bitcoin vereinigt viele seiner früheren Vorläufer, da bereits seit dem Aufstieg des Internets in der Kryptografie-Gemeinschaft ein Interesse an dezentralisierten Währungssystemen bestand.[10] Laut Sixt bindet Nakamoto dabei eine Reihe von Konzepten und Technologien in Bitcoin ein.[11]

Die Idee einer Datenbank, die alle gespeicherten Transaktionen chronologisch erfasst, stammt 1991 von Haber und Sornetta. Ein zentraler Server versah einen Block

[10] Vgl. Halaburda et al. (2016), S. 111.
[11] Vgl. Sixt (2016), S. 6-8.

mit einem Zeitstempel und einer Verlinkung zu einem anderen Block, sodass eine Kette von Blöcken gefüllt mit Daten entstand.

1997 beschreibt Adam Back in *hashcash*[12] ein *Proof-of-Work-System* (PoW), was als Grundlage für den in Bitcoin verwendeten Algorithmus verwendet wird und die Generierung der Blöcke steuert. In *hashcash* müssen Computer einen rechnerischen Arbeitsnachweis errichten, bevor sie eine Information versenden dürfen. *Hashcash* wurde entwickelt um E-Mail-Spam und Denial-of-Service-Angriffe zu begrenzen, indem die Überflutung eines Netzwerkes mit Nachrichten, mit Kosten verbunden wurde.

1998 wurde mit *b-money*[13] von Wei Dai eine dezentralisierte, digitale Währung entworfen, welche anonyme peer-to-peer Transaktionen ermöglicht. Alle Transaktionen würden in *b-money* in einem öffentlichen Register aufgenommen und an alle Teilnehmer verteilt werden. *B-money* war nur als Vorschlag vorgesehen und wurde daher nicht von Dai umgesetzt.

Alle Konzepte brauchten eine zentrale Instanz, um das *Double-spending-Problem* bei digitalen Währungen zu lösen. Das Double-spending-Problem beschreibt die Möglichkeit bei einer digitalen Währung ein digitales Gut beliebig oft zu kopieren bzw. auszugeben. Laut Sixt vermeidet Bitcoin das Double-spending-Problem, indem es das PoW-Konzept mit dem Konzept von Haber und Sornetta zur Bitcoin-Blockchain verbindet.[14]

In den obigen Ausführungen wird bereits deutlich, dass Bitcoin nicht nur eine digitale Einheit ist, die untereinander getauscht werden kann, sondern dass sie verschiedene kryptografische Ansätze in der Blockchain-Technologie vereint.

Swan untergliedert den Terminus Bitcoin dabei in drei Ebenen. Erstens, Bitcoin beschreibt die darunterliegende Blockchain-Technologieplattform. Zweitens, Bitcoin wird dazu verwendet das über der Blockchain liegende Protokoll zu benennen, welches bestimmt wie Vermögenswerte auf der Blockchain transferiert werden. Drittens, Bitcoin beschreibt die digitale Kryptowährung. Diese drei Ebenen, Block-

[12] Back (2002).
[13] Dai (1998).
[14] Vgl. Sixt (2016), S. 8.

chain, Protokoll und Währung sind generelle Struktur jeder modernen Kryptowährung. Einige weitere bekannte Kryptowährungen. sind Litecoin, Ripple, NXT, Peercoin, Ethereum und Counterparty. Jede Kryptowährung ist typischerweise eine Währung, hat ein Protokoll und seine eigene Blockchain oder läuft auf der Bitcoin-Blockchain. Litecoin ist beispielsweise nur leicht von Bitcoin angepasst wurden, um einige Eigenschaften zu verbessern. Die Litecoin-Währung läuft auf dem Litecoin-Protokoll, welches auf der Litecoin-Blockchain läuft. Counterparty dagegen läuft auf der Bitcoin-Blockchain, während es seine eigene Währung und Protokoll hat. Bitcoin ist in die erste Generation der Blockchain-Technologie eingeordnet.[15]

2.2. Ethereum – Blockchain 2.0

Von Anfang an wurde die Komplexität jenseits von Währung und Zahlungen für Bitcoin in Betracht gezogen. Bei seiner Erfindung wurden die Möglichkeiten für programmierbares Geld und Verträge im Protokoll hinterlegt.[16] Die Open-Source Plattform Ethereum ist eine solche Weiterführung der Idee von Bitcoin, indem es das Konzept der Blockchain aufgreift und die Benutzung auf andere Anwendungsfälle als nur Geld ausweitet.[17] Ethereum besitzt eine eigene Blockchain, ein eigenes Protokoll und eine eigene Währung. Die Software-Entwicklungsplattform von Ethereum und die eigene Blockchain wurden speziell für das Erstellen von dezentralen Applikationen (DApps) konzipiert.[18]

DApps sind Open-Source-Anwendungen, die autonom und ohne zentrale Autorität arbeiten. Die Daten und Aufzeichnungen der Anwendung müssen dezentral auf der Blockchain gespeichert werden. Jegliche Änderung an der Anwendung muss per Übereinstimmung gemäß dem definierten Anwendungsprotokoll stattfinden. Mit den DApps können Entwickler Projekte entwickeln, die weit über das Konzipieren von digitalen Währungen hinausgehen. [19]

Eine Untergruppe von DApps sind die sogenannten *Smart Contracts*. Das Konzept der Smart Contracts wurde bereits 1994 von Nick Szabo geprägt.[20] Mit Smart

[15] Vgl. Swan (2015), S. 1f.
[16] Ebd., S. 9.
[17] Vgl. Buterin (2013), S. 1.
[18] Vgl. Sixt (2016), S. 189.
[19] Vgl. ebd., S. 9f.
[20] Vgl. ebd., S. 14.

Contracts, also intelligenten, programmierbaren Verträgen, lassen sich Vertragslogiken und Regeln für Vermögensgegenstände technisch über Programmcodes abbilden. Die Verträge sind auf der Blockchain öffentlich gespeichert und führen sich durch die vorher definierte Logik automatisch selbst aus bzw. nicht aus. Langfristig angelegte Smart Contracts können untereinander agieren und so in einem Komplex ganze Organisationen abbilden.[21]

Ethereum geht davon aus, dass jede Organisation ein Zusammenspiel von Verträgen, Menschen und anderen Beziehungen ist. Wenn solche Organisationen auf Basis ihres Programmcodes größtenteils autonom agieren, werden sie dezentrale, autonome Organisation (DAO) genannt.[22] Ethereum bildet die algorithmische Durchsetzung von Vereinbarungen ab und kann als Implementierung eines „Kryptorechtssystems“ gesehen werden.[23]

Ethereum wurde von einem jungen russischstämmigen, kanadischen Programmierer und Blogger namens Vitalik Buterin gestartet. Buterin kommt 2011 zum ersten Mal mit Bitcoin in Berührung und betreute ab September 2011 als Mitgründer und Chefautor das *Bitcoin Magazine*. Ethereum wurde Ende 2013 von Buterin erstmalig im sogenannten *Ethereum White Paper*[24] beschrieben. Zusammen mit Gavin Wood und Jeffrey Wilcke wird Ethereum Anfang 2014 angekündigt und mit der in der Schweiz gelegenen gemeinnützigen Stiftung Ethereum Foundation gegründet. Das Ziel der Ethereum Foundation ist es „Forschung, Entwicklung und Bildung zu fördern und zu unterstützen, um dezentralisierte Protokolle und Werkzeuge der Welt näher zu bringen.“[25] Zum Zweck der Lizenzierung und Entwicklung der Software gründete die Stiftung die Ethereum Switzerland GmbH. Im April 2014 veröffentlichte Gavin Wood das *Ethereum Yellow Paper*[26], was Ethereum formal beschreibt und unter anderem eine detaillierte, technische Vorgabe für die Ethereum Virtual Machine (EVM) gibt. Die EVM ist das Herz von Ethereum und führt Programmcode arbiträrer, algorithmischer Komplexität aus.

[21] Vgl. Buterin (2013), S. 1.
[22] Vgl. Sixt (2016), S. 190.
[23] Vgl. Wood (2014), S. 2.
[24] Buterin (2013).
[25] Vgl. Ethereum Foundation (2016).
[26] Wood (2014).

Ethereum basiert auf einen vorher skizzierten Fahrplan für die Umsetzung des Projektes. Der Fahrplan wurde bevor Ethereum gestartet wurde in einzelne Meilensteine untergliedert, die in Tabelle 1 zu sehen sind.

Version	Bezeichnung	Startdatum
Vorabversion 0	Olympic testnet	Mai 2015
1	Frontier	30.07.2015
2	Homestead	14.03.2016
3	Metropolis	noch nicht veröffentlicht
4	Serenity	noch nicht veröffentlicht

Tabelle 1: Meilensteine von Ethereum (Ethereum Foundation, 2016)

Die erste Version von Ethereum, Frontier, war im Wesentlichen eine Beta-Version, die es Entwicklern erlaubte über Ethereum zu lernen, damit zu experimentieren und mit dem Aufbau von dezentralisierten Applikationen und Werkzeugen zu beginnen. Die zweite Version Homestead markiert den Eintritt in eine stabile Version von Ethereum. Viele Fehler wurden erkannt und repariert, sodass Ethereum sicherer geworden ist. Metropolis soll Ethereum für Endanwender öffnen und attraktiver machen, indem es die Benutzeroberfläche für nicht-technische Benutzer verbessert und anwendungsfreundlicher gestaltet. Serenity soll den noch auf PoW-basierende Algorithmus von Ethereum beenden und zu einem alternativen Konzept wechseln. Zurzeit wird über das sogenannte *Proof-of-stake-Konzept* (PoS) nachgedacht, das den Arbeitsnachweis durch Besitz anstatt von Rechnerleistung darstellt.

Die zu Ethereum gehörende Kryptowährung Ether hat am 29.01.2017 auf Coinmarketcap.com eine Marktkapitalisierung von 866 Tausend Euro. Die zu diesem Zeitpunkt vorhandenen gut 88,3 Millionen Ether haben einen Marktpreis von 9,80€ je Stück. Somit ist Ethereum zu diesem Zeitpunkt die zweitgrößte Kryptowährung nach der Marktkapitalisierung.

Bereits vor dem offiziellen Start wurde eine große Anzahl Ether durch die Ethereum Foundation in einer Schwarmfinanzierung ausgegeben, um ein großes Netzwerk für Entwickler, Miner, Investoren und andere Akteure anzukurbeln. Durch den öffentlichen 42 tägigen Vorverkauf, beginnend am 22. Juli 2014, wurden 31.591 BTC von der Ethereum Switzerland GmbH eingesammelt. Zum damaligen Zeitpunkt

stellte dies ein Volumen von knapp 18,5 Millionen USD dar.[27] In den vorher vereinbarten Geschäftsbedingungen wurde unter anderem festgehalten, wie viele Ether initial und fortlaufend geschöpft werden. 60.102.216 Ether wurden initial geschöpft und an die 9007 teilnehmenden Investoren ausgegeben. Weitere knapp 12 Millionen Ether bzw. 19,8% der Vorverkaufssumme gingen an frühe Beteiligte, Entwickler und Mitarbeiter.[28] Ethereum steht durch seine erweiterbaren Funktionalitäten für die zweite Generation der Blockchain-Technologie.

2.3. Blockchain

Eine Blockchain, im Deutschen auch weniger häufig Blockkette genannt, ist eine öffentlich zugänglich, verteilte Datenbank. Die Blockchain erlaubt es anonymen Teilnehmern sicher, ohne Intermediäre, untereinander Transaktionen in einem Peer-to-Peer-Netzwerk durchzuführen.[29]

Die Teilnehmer des Netzwerkes sind durch Kontoadressen repräsentiert. Die Adressen können sich, mit Hilfe von kryptografischen Algorithmen, gegenseitig digitale Güter zu senden. Diese Transaktionen werden dann über einen gemeinsamen Netzwerkkonsens durch die Netzwerkkonten validiert. Für Swan ist „die Blockchain ein öffentliches Register von allen … Transaktionen, die jemals ausgeführt wurden."[30] Die Transaktionen werden dann in Datenblöcken zusammengefasst und chronologisch nacheinander gespeichert. Die Reihe von Datenblöcken vom ersten bis zum letzten, aktuellsten Block wird Blockchain genannt. Besonders Public-Key-Kryptografie, digitale Signaturen und Hash-Funktionen sorgen hierbei für die Integrität der Daten.[31]

[27] Ether.Fund (2016).
[28] Ethereum Switzerland GmbH (2014), S. 8-10.
[29] Vgl. UCL (2016).
[30] Swan (2015), S. x.
[31] Vgl. ebd., S. xf.

2.4. Geld und Währung

Im Kontext von Kryptowährungen sind die Begriffe Geld und Währung als Hintergrund relevant. Weltweit wird Bitcoin von Regulatoren unterschiedlich eingeordnet. Von der Bundesregierung wurde die Währung 2013 als „privates Geld" eingestuft.[32]

Ein erster Anlaufpunkt für Informationen über Geld und Währung gibt die Deutsche Bundesbank in ihrer Veröffentlichung *Geld und Geldpolitik*[33]. Die Verwendung des Begriffes Geld ist unterschiedlich und bringt die universale Rolle, die Geld im Wirtschaftsleben spielt, zum Ausdruck. Geld trat in der Geschichte in unterschiedlichen Formen auf. In der Geschichte traten fünf verschiedene Formen von Geld auf. Das Warengeld, Münzgeld, Papierne Geldzeichen (Papiergeld), Banknoten und das Buchgeld.[34]

Das Warengeld ist eine einfache Form von Geld. Es handelt sich um Gegenstände, die als Geld verwendet werden. Beispiele sind Salzbarren oder Felle. Dem Münzgeld liegen auch Waren, meistens Edelmetalle wie Gold und Silber, zugrunde. Die Gold- und Silberklumpen wurden aber zu einheitlichen, genormten Stücken geprägt und in Umlauf gebracht. Die ältesten Münzen stammen aus dem 7. Jahrhundert vor Christi und Münzgeld wird auch heute noch benutzt. Papiergeld besitzt im Gegensatz zu Münzgeld aus Gold und Silber kaum einen Warenwert. Erst durch eine herrschende oder akzeptierte Instanz, wie beispielsweise einen Monarchen, erhält das Papiergeld seinen Wert. Es hat den Vorteil gegenüber Münzgeld, dass Geldbeträge sehr viel leichter, sicherer und damit billiger und schneller weitergegeben werden können. Das Prinzip der Banknoten funktioniert ähnlich wie Papiergeld. Banknoten werden von privaten oder staatlichen Banken herausgegeben. Der Gegenwert der Banknote, meist Edelmetalle wie Gold, wird in der Bank gelagert und kann jederzeit in der Bank eingetauscht werden. Banknoten sind daher eine Art Hybrid aus Münz- und Papiergeld. Mitte des 20. Jahrhunderts sind die meisten Volkswirtschaften allerdings losgelöst vom goldgedeckten Gegenwert. Den Banknoten steht kein innerer Wert gegenüber, sondern nur ein Versprechen des Staates über den Wert

[32] Vgl. Bundesministerium der Finanzen (2013), S. 1 vgl. dazu auch alle Anfragen des ehemaligen Bundestagsabgeordneten Frank Schäffler unter: http://www.frank-schaeffler.de/bitcoin-alle-anfragen-und-antworten-im-volltext.
[33] Deutsche Bundesbank (2015).
[34] Vgl. ebd., S. 12-17.

der Banknote. Der Begriff *Fiatgeld* beschreibt diesen Zustand, wo allein durch Beschluss der gesetzgebenden Organe eines Staates das Geld entsteht und dieses Geld dann als gesetzliches Zahlungsmittel bestimmt. Das Buchgeld bzw. Giralgeld bezeichnet Geld, was nur in den Kontobüchern der Banken verzeichnet ist. Das Guthaben wird zwischen den Konten verschoben. Früher geschah das durch Zu- und Abschreiben in echte Kontobücher, heute geschieht dies über Computer oder elektronische Medien.

Die Geschichte des Geldes zeigt, dass Geld unterschiedliche Formen aufweisen kann. Die Deutsche Bundesbank ist sich einig darüber, dass Geld für die heutige arbeitsteilige Wirtschaft von großer Bedeutung ist, Geld drei wichtige Funktionen hat und Geld nur akzeptiert wird, wenn alle Besitzer von Geld darauf vertrauen können, dass es seinen Wert behält.[35] In dieser Hinsicht scheint eine Definition des Begriffes Geld nicht homogen zu sein, weshalb ein Blick auf die Funktionen des Geldes gerichtet werden kann. Geld wird drei wesentliche Funktionen zugesprochen, um seine Vorteile auszuspielen.[36]

Geld als Tausch- und Zahlungsmittel, Geld als Recheneinheit, Geld als Wertaufbewahrungsmittel. Geld als Tauschmittel vereinfacht den Austausch von Gütern, während Geld als Zahlungsmittel die Möglichkeit bietet Kredite zu gewähren und Schulden zu begleichen. Geld als Recheneinheit bedeutet, dass Geld in einer allgemeinen Bezugsgröße ausgedrückt ist und mit Güter- und Vermögenswerten vergleichbar ist. Geld als Wertaufbewahrungsmittel lässt Geld einen gewissen Wert „speichern“ und zu einem späteren Zeitpunkt wieder eintauschen.

Auch für Issing gibt einen unmittelbaren Zusammenhang zwischen Geldfunktion und Geldbegriff. „In der Nationalökonomie wird der Geldbegriff heute allgemein von Geldfunktionen her bestimmt: Alles, was Geldfunktion ausübt, ist Geld.“[37] Issing klassifiziert die Geldfunktionen in die oben genannten drei Funktionen, sodass angenommen werden kann, dass der Geldbegriff alles einschließt, was diese drei Funktionen erfüllt.

[35] Vgl. Deutsche Bundesbank (2015), S. 19.
[36] Vgl. ebd., S. 10f.
[37] Issing (2014), S. 1.

Trotzdem sollte diese Definition nur als grober Annäherungspunkt verstanden werden. Beispielsweise beantwortet sie nicht die Frage, ob ein Tausch- und Zahlungsmittel gegen alle Waren weltweit getauscht werden kann oder nur gegen bestimmte. Außerdem ist nicht genau definiert wie lange Geld den Wert eines Gegenstandes aufbewahrt. Ob Geld 50 Jahre, 500 Jahre oder gar unendlich wertstabil bleibt, macht einen Unterschied und würde entsprechend viele Gelder von der Gelddefinition aus- oder einschließen.[38]

Den Begriff der Währung bringt die Deutsche Bundesbank kürzer auf den Punkt. „Der Begriff Währung bezeichnet in einem weit gefassten Sinne die Verfassung und Ordnung des gesamten Geldwesens eines Staates, zumeist wird darunter aber die Geldeinheit eines Staates oder Gebietes verstanden. Nach wie vor haben die meisten Länder eine eigene nationale Währung.“[39] Die Definition macht deutlich, dass Währung in Verbindung mit der Geldeinheit eines Staates steht.

[38] Vgl. Halaburda et al. (2016), S. 23f.
[39] Deutsche Bundesbank (2015), S. 218.

3. Einführung Kryptografie

Die Kryptografie eröffnet Bitcoin und somit auch der Blockchain-Technologie erst ihren Durchbruch. Sie ermöglicht es digitale Güter ohne vertrauenswürdige Drittinstanz eindeutig zuordenbar zu machen. Um zu verstehen, was Kryptowährungen und die Blockchain mit Kryptografie zu tun haben, ist ein grundlegendes Verständnis von Kryptografie von Vorteil.

Kryptografie wird schon seit vielen Jahrtausenden genutzt, um Nachrichten zu verschlüsseln und Informationen innerhalb einer bestimmten Personengruppe geheim zu halten. Gerade in der sicheren Übermittlung von Nachrichten über große Distanzen per Bote oder per Brief gab es einen Bedarf, um Vertrauen zwischen den Nachrichtenteilnehmern herzustellen. Es ist nicht verwunderlich, dass in der Literatur mit der Cäsar-Chiffre im antiken Römischen Reich ein erstes, prominentes Beispiel für die Übermittlung von Militärinformationen zu finden ist. Militärinformationen waren von immenser strategischer Bedeutung und so ist es nicht verwunderlich, dass das Militär eine Vorreiterrolle bei der Entwicklung übernimmt und übernommen hat. [40]

Die Cäsar-Chiffre benutzt einen Algorithmus, um den Text einer Nachricht unkenntlich zu machen. Der Algorithmus funktioniert mit Buchstabenverschiebung innerhalb des Alphabets. Empfänger und Adressat legen anfangs fest, welcher Buchstabe durch welchen Chiffratsbuchstaben ersetzt wird. Dies kann beispielsweise in einer Tabelle übersichtlich festgehalten werden. Die Wahl dieser Tabelle kann dabei völlig willkürlich sein, was das Entschlüsseln für einen potenziellen Angreifer erschwert. Die Cäsar-Chiffre verschiebt nun die Buchstaben um eine bestimmte, feste Anzahl von Positionen im Alphabet (Beispiel: Um einen Buchstaben nach rechts):

A→B
D→E
Z→A

Aus dem Wort BLOCKCHAIN entsteht das verschlüsselte Wort CMPDLDIBJO. Es lässt sich erkennen, dass diese Methode nicht sehr sicher ist, da durch einfaches

[40] Vgl. Paar et al. (2016), S. 1.

Ausprobieren der passende Algorithmus herausgefunden werden kann. Dieses Ausprobieren wird vollständige Schlüsselsuche oder Brute-Force-Angriff genannt.[41]

Bei dem dargestellten Beispiel handelt es sich um eine Substitutionschiffre, welche im Bereich der symmetrischen Kryptografie einzuordnen ist. Bei der symmetrischen Verschlüsselung besitzen zwei Parteien, durch vorige geheime Absprache, eine Chiffre (geheimer Schlüssel) zum Ver- und Entschlüsseln einer Nachricht. Die gesamte Kryptografie von der Antike bis in das Jahr 1976 folgte diesem Ansatz, wobei die Algorithmen zur Generierung des geheimen Schlüssels durch den technologischen Fortschritt komplizierter wurden.[42]

Giese et al. nennt in diesem Zusammenhang drei Eigenschaften, die kryptografische Algorithmen besitzen müssen: Vertraulichkeit, Authentizität und Integrität.[43]

Vertraulichkeit wird durch die Generierung des Schlüssels im Geheimen erzeugt. Kann ein Angreifer bei dieser Absprache lauschen oder sichert einer der zwei Parteien den Schlüssel nicht hinreichend, ist die Nachricht leicht zu knacken. Vertraulichkeit kann durch geheime Absprache erfolgen.

Authentizität bezeichnet die Echtheit einer Nachricht. Authentizität beantwortet die Frage, ob eine Nachricht in der Originalform vorhanden ist oder ob es sich um eine veränderte Kopie handelt. Hat der Angreifer den Schlüssel, kann er die Nachricht entschlüsseln, zu seinen Gunsten verändern und wieder verschlüsseln. Ein Brief kann beispielsweise auf dem Weg der Zustellung abgefangen werden, mit gleicher Schrift neugeschrieben werden und entsprechend verschlüsselt werden. Der Empfänger würde dies nicht merken, da die Entschlüsselung der Nachricht reibungslos funktioniert. Authentizität kann durch Übermittlung der Nachricht durch eine Vertrauensperson, die beide Parteien kennen, hergestellt werden.

Integrität beschreibt die Vollständigkeit und Unversehrtheit der Nachricht. Im oben beschriebenen Beispiel kann ein Angreifer jetzt nicht mehr einfach einen Brief austauschen oder die Nachricht auf dem Blatt durchstreichen und eine neue Nachricht drauf schreiben – der Empfänger würde dies merken. Der Angreifer kann, nachdem

[41] Vgl. Paar et al. (2016), S. 7f.
[42] Vgl. ebd., S. 3.
[43] Vgl. Giese et al. (2016), S. 19-21.

der vertrauliche Bote unaufmerksam war, die Nachricht durch Hinzufügen einzelner Worte in ihrem ursprünglichen Sinn verändern. Aus „Schickt Verstärkung nach Rom“ kann so „Schickt keine Verstärkung nach Rom“ werden. Integrität wurde früher beispielsweise durch das Stempeln und Schließen des Briefes mit einem einheitlichen, königlichen Siegel erreicht.

Um diese drei Eigenschaften sicherzustellen benutzt die Blockchain-Technologie eine Mischung aus kryptografischen Algorithmen der symmetrischen und asymmetrischen Verschlüsselung, digitalen Signaturen und Hash-Funktionen. Die symmetrische Verschlüsselung wurde bereits oben vorgestellt. In den nächsten zwei Unterkapiteln wird asymmetrische Verschlüsselung zusammen mit digitalen Signaturen und Hash-Funktionen vorgestellt.

3.1. Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung ist eine von Whitfield Diffie, Martin Hellman und Ralph Merkle im Jahr 1976 gänzlich neue Art der Kryptografie. Bei der asymmetrischen Kryptografie besitzt ein Teilnehmer einen geheimen Schlüssel, ähnlich wie bei der symmetrischen Kryptografie, und einen öffentlichen Schlüssel, welcher allgemein bekannt ist. Durch den privaten Schlüssel lässt sich der öffentliche Schlüssel berechnen, umgekehrt funktioniert dieser Vorgang nicht. Es handelt sich dabei um ein Schlüsselpaar das miteinander verknüpft ist. Asymmetrische Kryptografie wird daher auch als Public-Key-Kryptografie bezeichnet.[44]

Mit asymmetrischer Kryptografie können digitale Signaturen von Dateien erstellt, der Austausch von geheimen Schlüsseln über unsichere Kanäle realisiert oder klassische Nachrichtenverschlüsselung eingesetzt werden. Möchte ein Absender dem Empfänger eine Nachricht zusenden, benötigt er hierfür den öffentlichen Schlüssel des Empfängers. Nur der dazugehörige private Schlüssel des Empfängers kann die Nachricht nun entschlüsseln. Paar et al. vergleicht dieses Vorgehen mit dem eines Briefkastens der Post. Jeder könne einen Brief einwerfen, d.h. verschlüsseln, aber

[44] Vgl. Paar et al. (2016), S. 3f.

nur der Postbote kann den Briefkasten mit dem passenden Schlüssel öffnen und entleeren, d.h. entschlüsseln.[45]

Die Blockchain setzt primär auf asymmetrische Kryptografie, um Vertrauen zwischen den einzelnen Teilnehmern des Netzwerkes zu gewährleisten. Das bedeutet, dass eine Nachricht von einem Netzwerkteilnehmer zu einem anderen Teilnehmer ohne das Überprüfen durch eine zentrale Instanz oder eines Drittens stattfinden kann. Dies wird unter anderem durch digitale Signaturen erreicht.

Digitale Signaturen sind wichtige Werkzeuge der asymmetrischen Kryptografie mit denen sichergestellt wird, „dass eine Nachricht tatsächlich von der Person stammt, die angibt, sie versendet zu haben."[46] Paar et al. führt in diesem Kontext weiter aus, dass digitale Signaturen mit konventionellen Signaturen, also auf Papier gezeichneten Unterschriften, vergleichbar sind. Eine eindeutige digitale Signatur wird an jede Transaktion angehängt und stellt die Authentizität einer Nachricht sicher.[47]

3.2. Hash-Funktionen

Als letzter wichtiger Baustein werden Hash-Funktionen verwendet, um die Integrität zu gewährleisten.[48] Hash-Funktionen berechnen aus einer Nachricht einen Hash, welcher als Repräsentant oder als Fingerabdruck der ursprünglichen Nachricht gesehen werden kann. Der so berechnete Hashwert hat eine verkleinerte und feste Bitlänge im Gegensatz zu der ursprünglichen Nachricht. In dieser Hinsicht kann auch von einem „Zerhacken" gesprochen werden. Im Gegensatz zu anderen kryptografischen Algorithmen besitzen Hash-Funktionen keinen Schlüssel, sie sind durch Sicherheitseigenschaften aber nur in eine Richtung abwärts berechenbar. Diese und weitere Eigenschaften von Hash-Funktionen sind in Tabelle 2 dargestellt.[49]

[45] Vgl. Paar et al. (2016), S. 176.
[46] Ebd., S. 297.
[47] Vgl. Giese et al. (2016), S. 29.
[48] Vgl. ebd., S. 25.
[49] Vgl. Paar et al. (2016), S. 335.

Eigenschaft	Beschreibung
Beliebige Nachrichtenlänge	Eine Hash-Funktion kann Nachrichten x-beliebiger Länge verarbeiten.
Feste Ausgangslänge	Eine Hash-Funktion erzeugt Hash-Werte z fester Länge.
Effizienz	Eine Hash-Funktion kann einfach berechnet werden.
Urbildresistenz	Es ist rechnerisch unmöglich, für einen gegebenen Ausgangswert z einen Eingangswert x zu finden, sodass h.(x) = z gilt, d.h. Hash-Funktionen sind Einwegfunktionen.
Zweite Urbildresistenz	Für einen gegebenen Eingangswert x1 ist es rechnerisch unmöglich, einen zweiten Wert x2 zu finden, sodass h(x1) =h(x) gilt.
Kollisionsresistenz	Es ist rechnerisch unmöglich, zwei Eingangswerte x1 ≠ x2 zu finden, sodass h(x1) = h(x2) gilt.

Tabelle 2: Eigenschaften von Hash-Funktionen (Vgl. Paar et al., 2013, S. 345)

Der *Secure Hash Algorithm* (SHA) ist eine solche weitverbreitete, sichere Hash-Funktion, die auch von Bitcoin und Ethereum verwendet wird. SHA wurde von dem *National Institute of Standards and Technology* (NIST) und der *National Security Agency* (NSA) entwickelt.

3.3. Funktionsweise bei Bitcoin

In diesem Unterkapitel soll verdeutlicht werden, wie in Bitcoin die kryptografischen Algorithmen verwendet werden. Eigentum von Bitcoins wird über drei Komponenten sichergestellt. [50] Es handelt sich dabei um:

- Kryptografische Schlüsselpaare,
- Bitcoin-Adressen und
- Wallets

Das kryptografische Schlüsselpaar besteht aus privatem und öffentlichem Schlüssel. Antonopoulos vergleicht in diesem Zusammenhang das Schlüsselpaar mit einem Bankkonto. Der öffentliche Schlüssel entspricht dabei der Bankkontonummer,

[50] Vgl. Antonopoulos (2014), S. 61-65.

während der private Schlüssel als der geheime PIN der EC-Karte gesehen werden kann. Die Schlüssel können völlig unabhängig von der Blockchain und dem Internet in einer Wallet-Anwendung oder separat erstellt werden.[51] Der private Schlüssel ist dabei eine zufällig gewählte 256-Bit Zahl.[52] Der folgende Schlüssel ist ein Beispiel für einen zufällig generierten privaten Schlüssel im Hexadezimalsystemformat:

BD8FB3463D29AB36D8CD62E6F581D6AF5D4C3D98D7D5F508C5C436E2DD9DE15C

Es lässt sich auch in anderen Formaten kodieren, um die Länge die Ziffernlänge zu verändern oder Schreibfehler zu vermeiden, der Wert bleibt aber immer der gleiche.

Mit dem privaten Schlüssel lassen sich digitale Signaturen erstellen mit denen BTC transferiert werden. Außerdem kann aus ihm der öffentliche Schlüssel berechnet werden. Für die Netzwerkteilnehmer ist der private Schlüssel somit das zentrale Element, um den Besitz von BTC zu verifizieren. Alle relevanten Informationen lassen sich aus dem privaten Schlüssel errechnen, sodass es ausreicht nur diesen privaten Schlüssel sicher aufzubewahren.

Der öffentliche Schlüssel entsteht durch Multiplikation des privaten Schlüssels mit einem Punkt, der auch Basispunkt genannt wird, auf einer elliptischen Kurve. Dabei wird der *Elliptic Curve Digital Signature Algorithm* (ECDSA) mit dem Standard der secp256k-Kurve verwendet. Dieser Standard wurde vom NIST eingeführt. Der Basispunkt besteht aus einem X- und Y-Wert und ist immer gleich.[53]

Durch die definierten Gruppenoperationen[54] einer elliptischen Kurve lassen sich X und Y addieren und der Basispunkt kann auch in einem Wert ausgedrückt werden.[55] Im Hex-Format dargestellt wird die große Länge des Basispunktes deutlich:

04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

[51] Vgl. Antonopoulos (2014), S. 61.
[52] Genaugenommen kann es sich um eine Zahl zwischen 1 und (1,158 * 10^77) - 1 handeln (etwas weniger als 2^256).
[53] Vgl. Antonopoulos (2014), S. 65f.
[54] Hier handelt es sich um die Punktverdoppelung.
[55] Vgl. Paar et al. (2016), S. 276f.

Die Multiplikation von privatem Schlüssel und Basispunkt ergibt den öffentlichen Schlüssel.[56] Auch dieser Hash-Algorithmus ist nur in eine Richtung und nicht rückwärts berechenbar. Der öffentliche Schlüssel taucht in der Wahrnehmung der Anwender häufig nicht auf, da BTC durch ihre Bitcoin-Adressen repräsentiert sind.

Bitcoin-Adressen sind die virtuellen Aufbewahrungskonten der Empfänger von Transaktionen. Sie sind an das jeweilige Schlüsselpaar geknüpft. Zur Umwandelung vom öffentlichen Schlüssel zur Bitcoin-Adresse werden Hash-Funktionen benutzt. Die Algorithmen dieser Hash-Funktionen heißen SHA 256 und RACE Integrity Primitives Evaluation Message Digest (RIPEMD), speziell RIPEMD160. Es handelt sich dabei wiederum um eine Einwegs-Funktion, sodass aus der Bitcoin-Adresse nicht der öffentliche Schlüssel berechnet werden kann.[57]

In Abbildung 1 sind Beziehungen zwischen privaten Schlüssel, öffentlichen Schlüssel und Bitcoin-Adresse dargestellt.

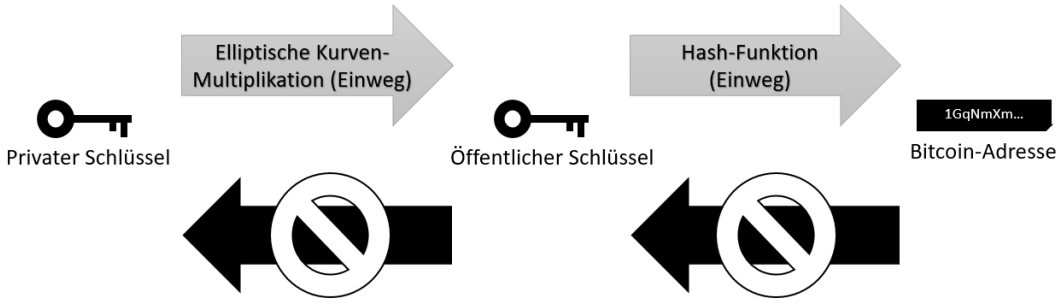

Abbildung 1: Privater Schlüssel, öffentlicher Schlüssel und Bitcoin-Adresse (Antonopoulos 2014, S. 63)

Häufig wird die Bitcoin-Adresse im *Base58Check*-Format kodiert und dargestellt, was die Länge der Adresse kleiner macht und Tippfehler versucht zu vermeiden. Base58Check benutzt alle lateinischen Klein- und Großbuchstaben sowie arabische Ziffern mit der Ausnahme von vier sich ähnelnden Zeichen (l, I, 0 und O) und fügt eine Prüfsumme am Ende und eine Identifizierungsnummer am Anfang hinzu (für die meisten Bitcoin-Adressen ist das eine 1, was aufzeigt, dass es sich um eine öffentliche Bitcoin-Netzwerkadresse handelt).[58] Beispielsweise sieht die Bitcoin-Adresse in diesem Format für den oben aufgeführten privaten Schlüssel wie folgt aus:

[56] Hier handelt es sich um die Punktaddition. S. Paar et al. (2016), S. 277.
[57] Vgl. Antonopoulos (2014), S. 70f.
[58] Vgl. Swan (2015), S. 98.

1GqNmXmqcw6sMG4zKcqNqp94CpfJsudtxa

Technisch ist es möglich, dass zwei verschiedene Individuen die gleiche Bitcoin-Adresse generieren, sodass beide in der Lage sind die BTC auf dieser Adresse zu transferieren. Swan betitelt diese Wahrscheinlichkeit als äußerst gering und mit 99,9999999999 prozentiger Wahrscheinlichkeit als fast unmöglich. Antonopoulos vergleicht in dieser Thematik dazu die Anzahl möglicher privaten Schlüssel (10^{77}) mit der geschätzten Anzahl der im sichtbaren Universum befindlichen Atome (10^{80}).[59]

Wallets enthalten die Schlüsselpaare, jedoch keine BTC an sich. Größtenteils handelt es sich dabei um ein Anwendungsprogramm für Endnutzer, Programmierer oder Miner. Mittlerweile gibt es eine große Anzahl an Wallet-Anwendungen für Desktop, mobile Endgeräte und Webbrowser mit unterschiedlichen Eigenschaften, wie erhöhte Anwenderfreundlichkeit, erhöhte Sicherheitsfunktionen, etc. Da der private Schlüssel benötigt wird um Transaktionen durchzuführen, ist die Wallet ein potenzielles Ziel von Angriffen. Um die Wallets zu schützen wird die symmetrische Verschlüsselung genutzt. Da die Sicherung sehr wichtig ist, ist die Verschlüsselung bei vielen Wallet-Anwendungen möglich und sogar verpflichtend.

[59] Vgl. Antonopoulos (2014), S. 64.

4. Technische Grundlagen der Blockchain

Aus den vorigen Kapiteln wurde deutlich, dass die Blockchain ein zentraler Baustein einer jeden Kryptowährung ist. Die Anzahl und Vielfalt von blockchain-basierten Kryptowährungen ist in den letzten Jahren ständig gewachsen. Ihr Potenzial hat der Blockchain-Technologie mittlerweile große Aufmerksamkeit in den Medien gebracht und auch Gesetzgeber, Banken und Zentralbanken beginnen damit, die Technologie näher zu untersuchen und eigene Anwendungen, wie etwa private Blockchains, in diesem Bereich zu entwickeln.

Die Blockchain ist nur ein Teil der vorgestellten Kryptowährungen. Wie Bitcoin als erfolgreichste Umsetzung der Blockchain zeigt, funktioniert die Blockchain in der Umgebung von Komponenten, die vor allem die Dezentralität, Offenheit und Sicherheit des Netzwerkes unterstützen.

Das Kapitel wird zunächst in den ersten beiden Unterkapiteln 4.1 Netzwerk und 4.2 Transaktionen zwei wesentliche Komponente der Blockchain anhand der Bitcoin Blockchain erklären und dann auf die Funktionen von der Bitcoin Blockchain und der Ethereum Blockchain eingehen.

4.1. Netzwerk

Die Blockchain ist als ein Peer-to-Peer-Netzwerk, im folgenden P2P-Netzwerk genannt, aufgebaut. Ein P2P-Netzwerk zeichnet sich durch die Gleichheit seiner Knoten aus. Es gibt keinen Server, keinen zentralisierten Service und keine Hierarchie im Netzwerk. Das Internet ist ein gutes Beispiel für ein P2P-Netzwerk, da für die verwendeten Protokolle wie Transmission Control Protocol (TCP), User Datagram Protocol (UDP) und Internet Protocol (IP) immer das Prinzip der Gleichheit für die Rechner gilt. Diese Gleichbehandlung geschieht allerdings nur in der Transportschicht, in der Anwendungsschicht treten zumeist Client-Server-Protokolle auf. Der Server stellt in dieser Client-Server-Architektur einen privilegierten Knoten gegen-

über dem Client dar. Ein P2P-Netzwerk ist daher im Grunde genommen eine Anwendung, die ohne Client-Server-Architektur auskommt, in dem alle Knoten gleich sind und das Internet als darunterliegende Transportschicht verwendet.[60]

Die Blockchain hat eine solche Netzwerkarchitektur. Die Knoten in einem P2P-Netzwerk können unterschiedliche Funktionen haben, um unterschiedlichen Zwecken zu dienen. Ein Basisknoten mit allen Funktionen (*Full Node*) hat beispielsweise andere Anforderungen als ein leichtgewichtiger Knoten, der speziell für mobile Endgeräte konzipiert wurde. Exemplarisch soll dies anhand von Bitcoin deutlich werden. Laut Antonopoulos gibt es vier Funktionen, die ein Knoten im Bitcoin-Netzwerk haben kann:[61]

1. Routing von Nachrichten, wie das Validieren und Verbreiten von Transaktionen und Blöcken.
2. Speichern und aktualisieren einer Kopie der kompletten Blockchain-Datenbank.
3. Mining, d.h. Berechnung von Blöcken und Sicherstellung des Netzwerkes.
4. Verwaltung von Wallets.

Alle Knoten müssen die erste Funktion aufweisen, um im Netzwerk teilnehmen zu können. Wenn ein Knoten die komplette Blockchain heruntergeladen hat spricht man von einem Full Node. Der Referenzclient *Bitcoin Core* ist ein solcher Full Node und verfügt des Weiteren auch über die anderen vier Funktionalitäten. Die Bitcoin Blockchain hat am 14.12.2016 bereits eine Größe von 94,02 GB erreicht, was einen tagelangen Download voraussetzt.[62] Nach dem Blockchain-Explorer 21.co läuft das Bitcoin-Netzwerk am 19.12.2016 auf 5439 solcher Knoten. Dieser Umstand zeigt die Dezentralität des Netzwerkes. Im Gegensatz zu einem Server, wo die Daten zumeist nur auf ebenjenen Computer gespeichert werden, verfügt jeder dieser Computer im Bitcoin-Netzwerk über eine Kopie der Daten.

Leichtgewichtige Knoten wie die Simplified Payment Verification (SPV) erlauben es nur eine Teilmenge der Blockchain herunterzuladen, was für mobile Endgeräte, wie Smartphones oder Tablets, als Knoten sinnvoll ist. Für den Großteil der Nutzer mit Wallet-Funktion ist sie mittlerweile der gängigste Knotentyp. SPV sind um den

[60] Vgl. Mahlmann et al. (2007), S. 7f.
[61] Vgl. Antonopoulos (2014), S. 138.
[62] Blockchain (2016).

Faktor 1000 kleiner als Full Nodes, weil sie die Transaktionen an sich nicht speichern, sondern nur die „Blocknummer“, die allgemein als *Block Header* bekannt sind, aller Blöcke der Blockchain.[63] Im Gegensatz zu einem Full Node fehlt SPV die Möglichkeit Transaktionen über die komplette Blockchain zu verifizieren. Wie später in Kapitel 4.3 beschrieben ist, ist die Sammlung der Block Header ausreichend, um den Nachweis über bestätigte Transaktionen zu erbringen.

4.2. Transaktionen

Antonopoulos beschreibt Transaktionen als den wichtigsten Teil im Bitcoin-System. Jede Transaktion ist dabei ein öffentlicher Eintrag in der Blockchain. Eine Transaktion hat den Zweck einen digitalen Wert vom Absender zum Empfänger zu übermitteln. Dazu durchläuft eine Transaktion drei Status: Erzeugung, Übertragung und Verifizierung. Eine Transaktion kann online oder offline erzeugt werden. Wenn sie erzeugt ist wird sie vom Besitzer mit der digitalen Signatur signiert. Hierbei stellt der Hash-Wert des öffentlichen Schlüssels den Absender dar. Die digitale Signatur des Absenders ist speziell an die jeweilige Transaktion gekoppelt und durch den dazugehörigen öffentlichen Schlüssel nachprüfbar. Dann kann es an einen Knoten übertragen werden. Der erste Knoten dient dabei als Eingang zum Bitcoin-Netzwerk. Sobald dieser erste Knoten erreicht ist, verbreitet jener, nach einer Prüfung auf Gültigkeit, die Transaktion im gesamten Netzwerk an sämtliche Knoten. Die initiale Prüfung der Gültigkeit einer Transaktion ist dabei an feste Kriterien gebunden und verhindert Spam und Denial-of-Service-Attacken gegen das Netzwerk. Schlussendlich wird die Transaktion von einem Mining-Knoten in einen Block aufgenommen und durch den Mining-Prozess verifiziert.[64] Jeder Mining-Knoten hat so einen Transaktionspool von unbestätigten Transaktionen. Der Mining-Prozess wird gesondert im Kapitel 4.3.2 bzw. 4.4.3 erläutert.

Eine weitere Komponente von Transaktionen ist die Transaktionsgebühr. Die Transaktionsgebühr ist eine Belohnung für die Miner für das Validieren der Transaktionen. Die Gebühr ist das Ergebnis der Subtraktion zwischen Transaktionseingängen und Transaktionsausgängen. Die Gebühr ist freiwillig, besitzt aber eine

[63] Vgl. Antonopoulos (2014), S. 147-149.
[64] Vgl. ebd., S. 109-111.

wichtige Funktion. Die Gebühr fungiert als Anreiz für die Miner, Transaktionen in die Blöcke aufzunehmen.[65]

Transaktionsgebühren werden anhand der Datengröße und nicht anhand des BTC-Wertes berechnet. Antonopoulos nennt als minimale Transaktionsgebühr 0,0001 BTC pro Kilobyte. Die meisten Transaktionen sind kleiner als ein Kilobyte, Transaktionen mit vielen Inputs und Outputs können diese Größe aber auch übersteigen. Da die Gebühr nicht verpflichtend ist, sind auch Transaktionen ohne Gebühr möglich. Die Wahrscheinlichkeit, dass eine Transaktion sofort in einen Block aufgenommen wird, steigt mit steigender Gebühr. Transaktionen mit keiner oder nur sehr geringen Gebühr verweilen mit höherer Wahrscheinlichkeit in einer Art Warteschlange, bis sie in den nächsten Block aufgenommen werden.[66] Der tatsächliche Preis der Gebühr für die sofortige Übernahme in einen Block bestimmt sich durch Angebot und Nachfrage. Am 27.12.2016 beträgt die Gebühr um sicher in den nächsten Block aufgenommen zu werden 0,0009 BTC je Kilobyte. Eine durchschnittliche Transaktion hat 250 Bytes Datenmenge.[67]

Bei Annahme von einer Blockzeit von 10 Minuten und Ausnutzung der maximalen Blockgröße von einem Megabyte sind so theoretisch bis zu 4000 Transaktionen je Block bzw. 6,6 Transaktionen pro Sekunde möglich.

Die Datenstruktur einer Bitcoin-Transaktion ist in Tabelle 3 dargestellt. Sie besteht im Kern aus Transaktionseingängen (Inputs) und Transaktionsausgängen (Outputs).

[65] Vgl. Nakamoto (2008), S. 4.
[66] Vgl. Antonopoulos (2014), S. 119.
[67] Vgl. 21.co (2016).

Größe	Feld	Beschreibung
4 Bytes	Version	Spezifiziert Regeln der Transaktion.
1-9 Bytes	Eingangszähler	Zähler der Eingangswerte.
x Bytes	Eingänge	Eine oder mehrere Eingangswerte.
1-9 Bytes	Ausgangszähler	Zähler der Ausgangswerte.
x Bytes	Ausgänge	Eine oder mehrere Ausgangswerte.
4 Bytes	Sperrzeit	Unix Zeitstempel oder Blocknummer.

Tabelle 3: Datenstruktur Bitcoin-Transaktion (Antonopoulos, 2014, S. 111)

Die zentrale Verrechnungseinheit von Inputs und Outputs heißt *Unspent Transaction Output* (UTXO). Antonopoulos vergleicht UTXO mit einem „Bitcoin-Brocken", welcher nur von dem Besitzer bewegt werden kann. Immer wenn ein Benutzer BTC erhält, ist es nichts Anderes als ein UTXO. Diese BTC können in vielen verschiedenen Transaktionen und Blöcken als UTXO verstreut sein. Daraus folgt, dass es keinen übersichtlichen Saldo über den Kontostand einer Bitcoin-Adresse gibt, sondern es sich um eine Sammlung von in der Blockchain gespeicherten UTXO handelt. Die Idee eines übersichtlichen Saldos wird von Wallet-Anwendungen angeboten, indem sie die gesamte Blockchain scannen und entsprechende UTXO zusammenaddieren. Der Wert von UTXO ist in der kleinstmöglichen Einheit Satoshi angegeben. UTXO sind unteilbar, sie verhalten sich dabei genau wie EURO Münzen, die auch nicht durch Schneiden halbiert werden können. Wenn der Wert von einer UTXO größer als der zu versendeten Wert ist, muss die gesamte UTXO verrechnet werden und es entsteht eine Art Wechselgeld, welches zurück an den Absender gesendet wird. Der Empfänger erhält dann die Differenz als neue UTXO. Wenn eine UTXO über 5 BTC vorhanden ist und ein Wert von 1 BTC an den Empfänger gesendet werden soll, beträgt das Wechselgeld, welches auch eine UTXO ist, 4 BTC.[68]

Transaktionen werden von *Script* ausgeführt, das in einer Forth-ähnlichen Skriptsprache geschrieben ist. Sowohl das Sperrskript, das auf der UTXO platziert ist, als

[68] Vgl. Antonopoulos (2014), S. 111f.

auch das Entsperrskript, dass gewöhnlich die digitale Signatur beinhaltet, ist in dieser Skriptsprache geschrieben. Die Skriptsprache ist sehr simpel gehalten, benötigt minimale Verarbeitungszeiten und ist, im Gegensatz zu heutigen Programmiersprachen, limitiert in seiner Nutzung. Die Programmierbarkeit der Skripte in Bitcoin ist eingeschränkt und nicht Turing-vollständig.[69] Mit ausgegeben (spend) oder nicht ausgegeben (unspend) kennt Script nur zwei Zustände für Bitcoins.[70]

Mit Script lassen sich zusätzliche, transaktionsspezifische Details individuell festlegen. So können beispielsweise Bedingungen erstellt werden, nach derer die Auszahlungen durchgeführt werden. Diese Skripte unterstützen eine Vielzahl möglicher Transaktionstypen, wie Treuhandtransaktionen, Multi-Signatur-Transaktionen, etc. Sie sind aber trotzdem durch die zwei Zustände der UTXO, *spend* und *unspend*, in den Einsatzmöglichkeiten begrenzt. Diese Fähigkeit mit Transaktionen gewisse Regeln und Bedingungen an Geld zu knüpfen führt zu der Begriffsbezeichnung des programmierbaren Geldes und zu den Überlegungen das Bitcoin-Protokoll für u.a. Smart Contracts zu verwenden.[71]

4.3. Bitcoin Blockchain

Die Möglichkeit eine beliebige Anzahl von Kopien eines digitalen Gutes zu erstellen ist in vielen Bereichen nützlich, bei digitalen Geld ist dieser Umstand aber kritisch. Normalerweise verwaltet eine zentrale Autorität in einem Register alle Transaktionen und prüft, dass digitale Münzen nicht zweimal ausgegeben werden und verhindert somit das Double-spending-Problem. Die Blockchain löst das Double-spending-Problem indem sie P2P-Technologie und Public-Key-Kryptografie kombiniert.[72]

Um sich den technischen Grundlagen der Blockchain zu nähern wird zuerst die Datenstruktur eines Blocks betrachtet. Anschließend wird dann der Prozess erklärt, der für die Generierung von Blöcken zuständig ist und Mining genannt wird.

[69] Vgl. Sixt (2016), S. 44.
[70] Vgl. Giese et al. (2016), S. 53.
[71] Vgl. Sixt (2016), S. 44.
[72] Vgl. Swan (2015), S. 2.

4.3.1. Blockstruktur

Ein Block kann eine maximale Größe von einem Megabyte haben. Der Hauptteil dieser Datenmenge sind die in ihr gespeicherten Transaktionen. Ein Block verfügt aber noch über weitere Felder, wie in Tabelle 4 zu sehen ist.

Größe	Feld	Beschreibung
4 Bytes	Blockgröße	Die Blockgröße in Bytes
80 Bytes	Block Header	Block-Metadatenfelder
4 Bytes	Version	Eine Versionsnummer
32 Bytes	Vorheriger Block Header	Verlinkung des Hashes des vorigen Blocks (Parent Block)
32 Bytes	Merkle Root	Ein Hash des Stammes des Merkle-Baumes
4 Bytes	Zeitstempel	Ungefähre Erstellungszeit des Blocks
4 Bytes	Schwierigkeit	Schwierigkeitsziel dieses Blocks
4 Bytes	Nonce	Ein Zähler des Proof-of-work-Algorithmus
1-9 Bytes	Transaktionszähler	Anzahl von folgenden Transaktionen
x Bytes	Transaktionen	Eingetragenen Transaktionen des Blocks

Tabelle 4: Datenstruktur Bitcoin-Block (Antonopoulos (2014), S. 160f.)

Die Größe des Block Headers, welcher von den bereits vorgestellten SPV-Knoten verwendet wird, ist im Vergleich zu einem kompletten Block, der im Durchschnitt mehr als 500 Transaktionen enthält, gering.

Die wesentlichen Felder des Blocks sind Block Header und die eingetragenen Transaktionen. Der Block Header enthält alle relevanten Metadaten, die in drei Felder aufgeteilt werden können. Das erste Feld ist der Block-Hash des vorangegangenen Blocks, sodass eine Verlinkung innerhalb der Blockchain entsteht. Dieser Block wird auch Elternblock genannt. Das zweite Feld enthält mit Zeitstempel, Schwierigkeit und Nonce drei Informationen für das Mining. Das dritte Feld ist ein *Merkle Tree Root*. Ein Merkle-Baum, auch als binärer Hash-Baum bekannt, ist eine Datenstruktur die für das effiziente Zusammenfassen und Verifizieren der Integrität großer Datensätze genutzt wird. Der Baum ist dabei verkehrt herum aufgebaut, mit

dem Root (Stamm) oben. Die untersten „Blätter“ sind Hash-Werte der einzelnen Transaktionen mit je 32 Byte. Je zwei dieser Hash-Werte, die auch als Werte-Paare angesehen werden können, werden durch den Hash-Vorgang zu einem neuen Hash-Wert gebildet, der als Elternknoten die Hash-Werte beider Kinderknoten vereint. Dieser Vorgang wiederholt sich bis am Ende nur noch ein Root Hashwert mit 32 Byte übrigbleibt. Sollte es sich um eine ungerade Anzahl von Blättern bzw. Transaktionen handeln wird die letzte Transaktion dupliziert. So konfiguriert sich der Merkle-Baum immer wieder selbst, bis am Ende wirklich nur noch ein Root Hashwert die Daten repräsentiert. So können beliebig viele Transaktionen durch einen viel kleineren 32 Byte Hashwert repräsentiert werden.[73] Abbildung zeigt die Bildung eines Merkle Root mit vier Transaktionen (Tx) und den jeweiligen Hash-Werten (H).

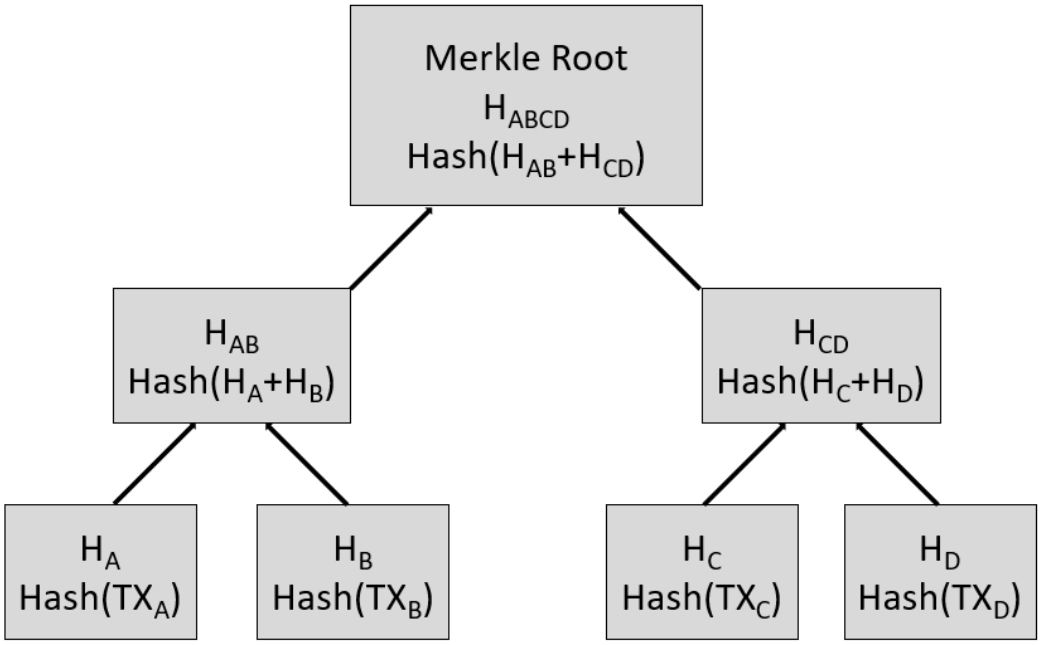

Abbildung 2: Merkle-Baum (Eigene Abbildung. Vgl. Antonopoulos, 2014, S. 166)

Diese Eigenschaft des Merkle-Baumes erlaubt es SPV-Knoten nur die Block Header herunterzuladen und trotzdem über eine Verifikation der Transaktion zu verfügen.

[73] Vgl. Antonopoulos (2014), S. 164-166.

4.3.2. Mining

Mining dient zwei zentralen Aspekten im Bitcoin-System. Zum einen ist es der einzige Weg um BTC neu zu schöpfen und dem System hinzuzufügen. Zum anderen fungiert der Prozess als Validierung der Transaktionen und verhindert so das Double-Spending-Problem. Das Mining ist dafür als Zeitstempel-Server organisiert, der die zeitliche Abfolge der Transaktionen aufzeichnet und richtig einordnet.

Mining hat mit dem klassischen Bergbau nichts zu tun. Um den Begriff des Mining greifbar und in den Kontext richtig einzuordnen, vergleicht Antonopoulos den Prozess mit dem Fördern von Edelmetallen oder dem Drucken von Banknoten der Zentralbanken. Im Deutschen kann von dem Schürfen bzw. dem Finden eines Blocks gesprochen werden.

Laut Antonopoulos beträgt die Geldschöpfung pro Block anfangs 50 BTC, wird aber alle vier Jahre bzw. alle 210.000 Blöcke halbiert, sodass im Jahre 2140 alle BTC gefunden sein sollten. Die Inflationierung ist dementsprechend in den ersten Jahren sehr hoch, während sie zum Ende hin gegen null tendiert und ab dem Jahr 2140 null ist.

Seit dem 09.07.2016 bzw. Block 420.000 ist die Blockvergütung für das Schürfen eines Blocks von 25 BTC auf 12,5 BTC gefallen. Zu diesem Zeitpunkt sind bereits 15.750.000 von 21.000.000 BTC im Umlauf, was dreiviertel aller BTC ausmacht. Der jährliche Zufluss von BTC ist für die nächsten vier Jahre 656.250 BTC, was einer Inflationsrate von 4,17 bis 3,7 Prozent der nächsten Jahre entspricht. Bei Block 630.000 wird die Blockvergütung dann auf 6,25 BTC halbiert.

Die theoretisch verfügbare Menge an BTC darf nicht mit der tatsächlichen verfügbaren Menge verwechselt werden. BTC können durch Verlust des privaten Schlüssels unbenutzbar werden. Eine Wiederherstellung des privaten Schlüssels ist nicht möglich, sodass eine sichere und verantwortungsbewusste Lagerung jenes wichtig ist. Diese Verluste von BTC werden durch eine Verlustrate beschrieben, die durch die Dezentralität nicht erfassbar ist. Die Verlustrate sorgt dafür, dass Bitcoin einen deflationären Charakter aufweist, der spätestens mit dem Ende der BTC-Schöpfung im Jahre 2140 ansetzt.[74]

[74] Vgl. Antonopoulos (2014), S. 173-176.

Die Betreiber von Mining-Knoten werden Miner genannt. Miner sorgen für die Sicherheit des Systems und erhalten als Anreiz dafür neu geschöpfte BTC und die freiwillige Transaktionsgebühr. Bitcoin benutzt die SHA256 Hash-Funktion und den PoW-Algorithmus für das Mining. Die Miner treten dabei in einem Wettkampf gegeneinander an, um als Erster die Lösung zu einem mathematischen Problem zu finden. Der Miner berechnet den Hash-Wert des Block Headers, indem er die sechs Felder des Block Header, Version, voriger Block Header, Merkle Root, Zeitstempel, Schwierigkeit und Nonce zusammenrechnet. Um das Problem erfolgreich zu lösen, muss der Hash-Wert des Block Headers unterhalb eines vorgegebenen Zielwertes (Difficulty target) liegen. Der Zielwert wird dabei über die Schwierigkeit gesteuert. Steigt die Schwierigkeit, sinkt der Zielwert, sodass es schwieriger wird einen passenden Block Header Hash zu berechnen. Die Schwierigkeit wird alle 2016 Blöcke angepasst, sodass die Blockzeit auch bei steigender oder fallender Gesamthashleistung gleich bleibt. Der Miner kann über das Verändern der Nonce den Hash-Wert anpassen. Die Nonce ist eine zufällige Zahl und standardmäßig null. Durch die Eigenschaften einer Hash-Funktion bewirkt eine kleine Änderung an der Nonce eine beliebige Änderung beim Hash-Wert. Das Hash-Ergebnis kann weder im Voraus bestimmt, noch kann ein Muster erstellt werden, dass einen speziellen Hash-Wert produziert. Nur über Probieren kann die Lösung erzwungen werden und somit der rechnerische Arbeitsnachweis erbracht werden. [75]

Nachdem ein Miner für einen Block das passende Hash-Ergebnis „gefunden“ hat, wird ein neuer gültiger Block an den vorigen angehängt und die Nachricht im Netzwerk verteilt. Erhält ein Miner eine solche Nachricht, bevor er selbst einen Block gefunden hat, verwirft er seine aktuellen Berechnungen, erkennt den gefunden Block als gültig an und startet sofort das Mining nach dem nächsten Block. Dieser Vorgang wiederholt sich und beginnt immer wieder von neuem. Nach Decker et al. benötigt ein Knoten im Durchschnitt 6,5 Sekunden (arithmetische Mittel 12,6 Sekunden), um die Information über das Finden eines Blocks im Netzwerk zu erhalten. Nach 40 Sekunden haben 95% der Knoten diese Information erhalten.[76]

[75] Vgl. Antonopoulos (2014), S. 187f.
[76] Vgl. Decker et al. (2013), S. 5.

Durch die dezentrale Datenstruktur der Blockchain kann es passieren, dass mehrere Miner gleichzeitig einen Block gefunden haben bevor die Nachricht über das Finden des jeweils ersten Blocks über das Netzwerk sie erreicht hat. Die Folge sind sogenannte Blockchain-Gabeln. Eine Gabel, im Folgenden mit dem englischen Begriff Fork beschrieben, ist eine Aufteilung der Blockchain in zwei oder mehrere parallel laufende Ketten. Die Miner schließen sich nun jener Kette an, von der sie als erstes den Block erhalten haben und beginnen den Wettkampf für den nächsten Block. Der Mining-Konsens stellt sicher, dass die Kette mit der höheren Hash-Rate sich gegen die Kette mit der niedrigeren Hash-Rate in der Folgezeit durchsetzt, da sie schneller den nächsten Block finden wird. Die Wahrscheinlichkeit, dass eine solche Aufteilung fortbesteht, wird mit jedem zurückliegenden Block in der Blockchain geringer, wie in Abbildung 3 zu sehen ist. Laut Antonopoulos geschieht das Fortbestehen einer Fork nach einem Block jede Woche, während sie nach zwei Blöcken bereits außerordentlich selten ist. Nach sechs Blöcken bzw. einer Stunde gilt eine Transaktion in Bitcoin als unwiderruflich. [77]

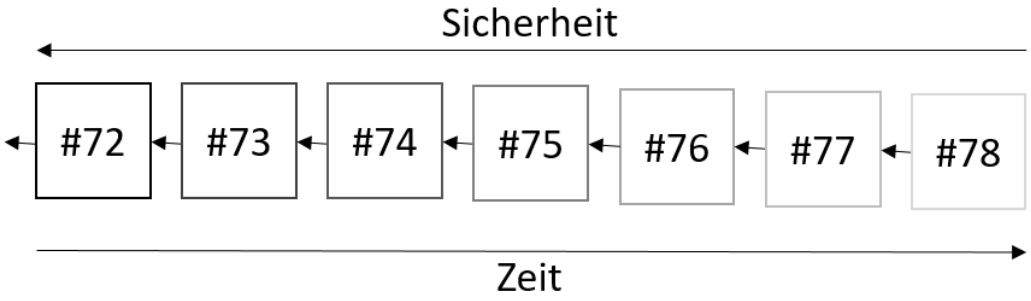

Abbildung 3: Blockchain (Eigene Abbildung)

Neben den natürlichen Forks gibt es auch künstliche Forks. Diesen Arten von Forks können eine Änderung des Protokolls erwirken, indem die Knoten einen Software-Update durchführen. Künstliche Forks untergliedern sich in *Soft Fork* und *Hard Fork*. Eine Soft Fork erfordert nicht, dass alle Knoten der Änderung durch Aktualisieren zustimmen müssen. Trotz Änderung wird an der gleichen Blockchain weitergearbeitet. Eine Hard Fork erfordert dagegen, dass alle Knoten ein Update durchführen, da sonst eine alte und eine neue Blockchain entsteht.[78]

[77] Vgl. Antonopoulos (2014), S. 204.
[78] Vgl. Sixt (2016), S. 11-15.

Die gesamte Hash-Rate des Netzwerkes hat sich seit der Einführung enorm gesteigert, sodass die Wahrscheinlichkeit einen Block zu schürfen für Privatpersonen ohne riesige Investitionssummen mittlerweile nahe Null ist. Viele Miner haben sich in sogenannten Mining-Pools zusammengeschlossen. Ein Mining-Pool stellt einen einzelnen Full Node dar, welcher die Mining-Rechenleistung vieler einzelner Miner bündelt, um die Wahrscheinlichkeit einen Block zu finden zu erhöhen. Wenn ein Block gefunden wird, wird die Belohnung an alle teilnehmenden Miner entsprechend ihres Rechenanteils ausgeschüttet.

4.4. Ethereum Blockchain

Ethereum besitzt, im Gegensatz zu Bitcoin, eine eigene Blockchain, ein eigenes Protokoll und eine eigene Kryptowährung. Die Blockchain ist in den meisten Aspekten ähnlich der Bitcoin Blockchain. In Bezug auf die Blockchain ist der größte Unterschied zu Bitcoin, dass die Ethereum Blöcke eine Kopie der Transaktionsliste und der letzten Zustände enthält.[79] Das Konzept der Zustände ist ein wichtiger Aspekt von Ethereum und wird im Laufe des Kapitels erklärt. Bevor die Blockstruktur genauer betrachtet werden kann, ist es für das Verständnis von Ethereum sinnvoll die ergänzenden Komponenten von Ethereum kurz vorzustellen.

4.4.1. Accounts, Nachrichten und Transaktionen

Ethereum besteht aus Objekten die Accounts genannt werden. Accounts sind ähnlich wie Bitcoin-Adressen eine Art Konto. Sie gehen in ihrer Funktionalität aber noch viel weiter.[80] In Tabelle 5 sind die vier Eigenschaften eines Ethereum-Accounts beschrieben.

[79] Vgl. Buterin (2013), S. 18.
[80] Vgl. ebd., S. 13.

Feld	Beschreibung
Nonce	Ein Zähler, der sicherstellt, dass eine Transaktion nur einmal ausgeführt wird
Ether-Saldo	Ein Saldo des Accounts.
Programmcode	Ein Programmcode für Verträge.
Internem Speicher des Accounts	Ein Speicher der beschrieben, geändert und gelöscht werden kann. Ist standardmäßig leer.

Tabelle 5: Felder eines Ethereum-Accounts (Buterin, 2013, S. 13)

Ethereum besitzt zwei Arten von Accounts. *Externe Accounts*, nachfolgend Accounts genannt, die ähnlich wie bei Bitcoin über die jeweiligen Privaten Schlüssel gesteuert werden, und *Contract Accounts*, die über ihren Programmcode kontrolliert werden und autonom agieren. Ein Account verfügt über keinen Programmcode und Nachrichten von Accounts können über signierte Transaktionen versendet werden. Contract Accounts führen ihren Programmcode jedes Mal aus, wenn sie eine Nachricht erhalten. Das erlaubt es ihnen den internen Speicher zu lesen und zu beschreiben und weitere Nachrichten zu senden oder im Gegenzug Contract Accounts zu kreieren. Die Verträge werden in der Blockchain über das Ethereum spezifischen binäre Format, EVM Bytecode, gespeichert.

Nachrichten sind in Ethereum ähnlich zu sehen wie Transaktionen in Bitcoin, mit einigen Unterschieden. Nachrichten können von beiden Account-Arten erstellt werden. Es gibt eine Option für Nachrichten Daten zu enthalten. Indem Contract Accounts auf Nachrichten antworten, umfassen Nachrichten in Ethereum auch das Konzept von Funktionen. Eine Transaktion bezieht sich im Zusammenhang mit Ethereum auf ein signiertes Datenpaket das von einem Account gesendet wird und eine Nachricht beinhaltet. Der Übergang von einem Zustand in den Folgezustand wird über Transaktionen durchgeführt.

Ethereum verwirft das Schema der UTXO aus Bitcoin für das Konzept der Accounts, durch die mehrstufige Zustände abgebildet werden können. Der simplere Ansatz der Accounts kann den Saldo eines Accounts über den Zustand speichern. Bei gültiger Transaktion wird vom Konto des Absenders der entsprechende Betrag,

wenn vorhanden, belastet und dem Empfänger gutgeschrieben.[81] Vorteile von UTXO und Accounts sind in Tabelle 6 gegenübergestellt.

Vorteile UTXO	Vorteile Accounts
Höheres Maß an Privatsphäre durch das Verwenden von neuen Adressen bei jeder Transaktion.	**Große Speicherersparnisse** da jede Transaktion nur eine Referenz, eine Signatur und einen Output produziert.
Potentielles Skalierbarkeitsmodell da nur der Besitzer von Münzen einen Besitznachweis des Merkle Tree behält.	**Große Übertragbarkeit** weil es kein Blockchain-Konzept für die Herkunft von speziellen Münzen gibt.
	Einfachheit da gerade bei komplexeren Skripten es einfacher ist den Programmcode zu schreiben und zu verstehen.
	Konstanter Referenz aller Daten Leichtgewichtige Knoten können an jedem Punkt alle relevanten Daten eines Accounts im Zustandsbaum prüfen.

Tabelle 6: Vorteile von UTXO und Accounts als Zustand (Ethereum Wiki, 2016)

Da das Hauptaugenmerk bei Ethereum auf DApps mit arbiträren Zuständen und Programmcodes liegt, wurde das Konzept von Accounts gewählt. Im folgenden Unterkapitel 4.4.2 wird deutlich, wo die Zustände gespeichert werden.

4.4.2. Blockstruktur

In Ethereum besteht ein Block aus einer Kollektionen von relevanten Informationen (Block Header), Informationen aus den entsprechenden enthaltenen Transaktionen und einer Reihe anderer Block Header, die in Tabelle 7 aufgelistet sind.

[81] Vgl. Ethereum Wiki (2016).

Größe	Feld	Beschreibung
32 Byte	parentHash	Block Header des vorigen Blocks
32 Byte	ommersHash	Hash einer Liste weiterer Block Header des Blocks
20 Byte	beneciary	Adresse für Gebühr des Miners
32 Byte	stateRoot	Hash des Root Knoten des Merkle Patricia Baumes mit dem Zustand
32 Byte	transactions-Root	Hash des Root Knoten des Merkle Patricia Baumes mit den Transaktionen
32 Byte	receiptsRoot	Hash des Root Knoten des Merkle Patricia Baumes mit den Transaktionenbestätigungen
x Byte	logsBloom	Bloom Filter mit indexierten Informationen aus Logeinträgen und Transaktionsbestätigungen
x Byte	difficulty	Schwierigkeitslevel des Blocks
x Byte	number	Fortlaufende Blocknummer
x Byte	gasLimit	Derzeitiges Gas-Limit des Blocks
x Byte	gasUsed	Gesamtes benutztes Gas des Blocks
x Byte	timestamp	Ungefähre Erstellungszeit des Blocks
<= 32 Byte	extraData	Weitere relevante Blockdaten
32 Byte	mixHash	Hash für Arbeitsnachweis (PoW) zusammen mit Feld „nonce“
8 Byte	nonce	Hash für Arbeitsnachweis (PoW) zusammen mit Feld „mixHash“

Tabelle 7: Datenstruktur Ethereum-Block (Wood, 2014, S. 4f.)

In einem Ethereum-Block sind ergänzend zu der vorgestellten Blockstruktur von Bitcoin drei Aspekte zu nennen. Der *Merkle Patricia Tree*, die Gebühren und Ommer-Hash.

Der Merkle Patricia Tree ist die primäre Datenstruktur Ethereums und wird benutzt um alle Account-Zustände, Transaktionen und Transaktionsbetätigungen in einem Block zu speichern. Der Merkle Patricia Tree ist eine Kombination aus Merkle-Baum und Patricia-Baum. Die Eigenschaft aus dem Merkle-Baum wurde in Kapitel 4.3.1 beschrieben und sagt aus, dass jeder eindeutige Satz von Werte-Paaren eindeutig einen Root Hash abbilden, sodass ganz oben ein einzelner Hash gebildet wird. Mit der zweiten Eigenschaft des Patricia-Baumes ist es möglich Werte-Paare in logarithmischer Zeit zu ändern, hinzuzufügen oder zu löschen. Ein Umstand der

entsteht um die Möglichkeit sich verändernder Zustände in der Blockchain abzubilden.[82]

Die Gebühren in Ethereum werden *Gas* genannt. Jede programmierbare Berechnung in Ethereum, das können Vertragserstellung, Nachrichten, Verwendung und Zugriff des Account-Speichers oder das Ausführen von Operationen in der virtuellen Maschine sein, kostet eine allgemein vereinbarte Menge Gas (gasPrice). Es vermeidet gleichzeitig den Missbrauch des Netzwerkes durch Überlastung und belohnt das Schreiben von effizienten Programmcode. Gas existiert nur in dieser Art von Transaktion zwischen Transaktion-Auftraggeber und Miner. In diesem Vorgang wird der entsprechende Wert Ether vom Kontosaldo in Gas zum gasPrice umgewandelt und dem Miner gutgeschrieben, welcher zum gleichen gasPrice Ether erhält. Eine Gebühr ist nicht zwingend, allerdings sind Miner auch nicht verpflichtet Transaktionen mit keiner Gebühr anzunehmen. Der Preismechanismus funktioniert dabei genau wie in Bitcoin über Angebot und Nachfrage.[83]

Die maximale Blockgröße wird in Ethereum über das gasLimit-Feld im Block definiert. Zurzeit haben die Miner über ein Wahlsystem die Möglichkeit das Limit des nächsten Blocks um 0,0975% an- oder abzuheben, wobei dieses Konzept in Zukunft noch Veränderungen durch die Entwickler erfahren könnte.[84]

Ein Ommer-Block ist ein verwaister Block, der auf einer Ebene mit dem in der Blockchain eingebunden Elternblock ist. Durch den Ommer-Hash wird ein oder mehrere Ommers in den aktuellen Block mit eingebunden.

4.4.3. Mining

Die Belohnung für das Finden eines Blocks setzt sich in Ethereum größtenteils aus der statistischen Blockbelohnung von fünf Ether und den variablen Gebühren des Blocks zusammen. Darüber hinaus geht 1/32-Anteil für das Einbinden von Ommer-

[82] Vgl. Ethereum Wiki (2016).
[83] Wood (2014), S. 7.
[84] Ethereum Wiki (2016).

Blöcken an den Miner.[85] Die angestrebte Blockzeit von Buterin sind zwölf Sekunden.[86] Da Ethereum sich noch nicht in der finalen Version befindet wird die Blockzeit getestet, sodass eine Abweichung von wenigen Sekunden möglich ist. Durch die kürzere Blockzeit entstehen natürliche Forks[87] viel häufiger als bei Bitcoin. Die daraus entstehenden verwaisten Blöcke sind nicht wie bei Bitcoin einfach ungültig. Da Miner belohnt werden, wenn sie Ommer-Blöcke einbinden, werden dann auch die ursprünglichen Ersteller der Ommer-Blöcke belohnt.

Ether ist ähnlich wie der BTC nicht die kleinste Einheit. Die kleinste Stückelung wird, zu Ehren des Computertechnikers und Autors von B-money Wei Dai, Wei genannt und entspricht ein Trillionstel von einem Ether. Weitere markante Stückelungen sind nach wichtigen Ideengebern und Persönlichkeiten der Kryptowährung-Szene benannt. In Tabelle 8 wird dieser Umstand veranschaulicht.

Einheit	**Wei-Wert**	**Wei**
Wei	1 Wei	1
Microether (Szabo)	1e12 Wei	1.000.000.000.000
Milliether (Finney)	1e15 Wei	1.000.000.000.000.000
Ether	1e18 Wei	1.000.000.000.000.000.000

Tabelle 8: Einheiten in Ethereum (Ethereum community, 2016, S. 47)

Die geplante, jährliche Ether-Schöpfung beträgt 26% der im Vorverkauf herausgegebenen Ether, was zirka 15,6 Millionen Ether (15.626.576) sind.[88] In den Geschäftsbedingungen des Vorverkaufes von Ethereum wird aber auch deutlich gemacht, dass dieser Wert durch die Ethereum Switzerland GmbH im Laufe der Entwicklung noch verändert werden kann, aber nicht beabsichtigt ist.[89]

Ethereum benutzt genau wie Bitcoin PoW für das Mining, mit dem Unterschied, dass Ethereum nicht die SHA256 Hash-Funktion benutzt, sondern mit *Ethash* einen eignen PoW-Algorithmus. Laut Wood ist die Intention dabei Mining wieder für normale Computer statt hochspezialisierten Rechnern zu ermöglichen und somit

[85] Wood (2014), S. 12.
[86] Buterin (2014).
[87] An dieser Stelle sei auf die ausführlichere Erklärung von *Forks* in Kapitel 4.3.2 verwiesen.
[88] Vgl. Buterin (2013), S. 30f.
[89] Ethereum Switzerland GmbH (2014), S. 10.

den Gedanken der Dezentralisierung zu verstärken. Ethash soll dabei im Algorithmus mehr Speicher und Bandbreite konsumieren, sodass die Berechnung auf Prozessoren von Grafikkarten dafür sehr geeignet ist.[90]

Durch die Elektrizitäts- und Umweltkosten für das Betreiben des Netzwerkes durch das PoW-Mining plant Ethereum in der finalen Phase auf Proof-of-Stake (PoS) zu wechseln. Dadurch, dass PoS nur den Besitz von Ether voraussetzt und keine (hochspezialisierte) Hardware benötigt wird, wird es auch als „virtuelles Mining" bezeichnet.

[90] Wood (2014), S. 13.

5. Vergleich Bitcoin und Ethereum

Im nächsten Kapitel wird auf Basis der herausgearbeiteten Erkenntnisse Bitcoin und Ethereum verglichen. Es wird dabei ein Fokus auf die größten Unterschiede gelegt. Das Hauptziel von Bitcoin ist es eine dezentrale, digitale Währung zu sein, während Ethereum das Hauptziel verfolgt, als Plattform für das Erstellen von DApps und Smart Contracts zu fungieren. Diese unterschiedlichen Hauptziele von Bitcoin und Ethereum müssen beim Vergleich berücksichtigt werden. Trotz dieser Unterschiede bilden sich Schnittpunkte, die einen Vergleich in beiden Bereichen zulässig macht. Erstens, der Vergleich von BTC und Ether als digitale Kryptowährung. Zweitens, der Vergleich im Rahmen von Blockchain 2.0. als Verträge bzw. Smart Contracts. Dieser Schnittpunkt wird bei Bitcoin über die verwendete Skriptsprache hergestellt, die im Kapitel 4.2 kurz beschrieben wurde. Diese beiden Bereiche sind analog zu den von Swan beschrieben Blockchain-Kategorien Blockchain 1.0. und Blockchain 2.0. gewählt. Ein weiterer Vergleichspunkt ist der Vergleich der Blockchain von Bitcoin und Ethereum. Die Vergleichspunkte sind an die Eigenschaften angelehnt und größtenteils unabhängig von den unterschiedlichen Hauptzielen von Bitcoin und Ethereum.

5.1. Blockchain 1.0. – Kryptowährung

5.1.1. Verteilung der Währung

Bitcoin und Ethereum verfolgten auf dem ersten Blick eine unterschiedliche Strategie sowohl bei der initialen Verteilung, als auch bei der weiteren Ausgabe ihrer digitalen Münzen.

Bitcoin hat eine im Protokoll fest definierte, planbare Verteilungsrate. Die Ausgabe begann mit dem Genesis-Block und endet im Jahre 2140. Die Gesamtausgabemenge ist dabei auf 21 Millionen BTC fixiert. Die Vergabe geschieht ausschließlich durch Mining und keine Münzen wurden vor dem Genesis-Block verteilt. Die Ausgabe halbiert sich alle vier Jahre, sodass frühe gegenüber späteren Teilnehmern begünstigt werden. Nach bereits vier Jahren ist die Hälfte aller Münzen verteilt. Die steigende Anzahl der Mining-Gesamtrechenleistung verstärkt diese Benachteiligung der späteren Teilnehmer an neu ausgegebene Münzen zu kommen. Das Geld

weist dabei einen deflationären Charakter auf, der spätestens mit dem Ende der Geldausgabe erreicht wird.

Ethereum verfolgt einen anderen Ansatz. Die Höhe der in der *Initial Coin Offering* (ICO)[91] eingesammelten Summe ist die Grundlage für die initiale Verteilung der Ether-Münzen. Die Ethereum Foundation legte die prozentuale Verteilung der initialen Geldmenge an die Akteure fest, wobei mit 83,5% der größte Teil an die Investoren der ICO zurückgezahlt wurde. Die jährliche, angestrebte Inflation wurde durch die initiale Geldmenge festlegt und beträgt 26% davon. Sie ist im ersten Jahr mit 26% der Menge signifikant hoch, fällt im zweiten Jahr auf 22,4%, im zehnten auf 7% und im 64. Jahr wird eine Rate von 1% erreicht. Die Ether-Menge hat daher keinen deflationären Charakter, da es immer eine konstante Geldmengenerweiterung gibt, auch wenn diese in jedem Jahr prozentual geringer wird. Die Idee dahinter ist dadurch die jährliche Verlustrate auszugleichen und eine ungefähre gleichbleibende, tatsächlich verfügbare Geldmenge sicherzustellen. In Kontrast zu Bitcoin sollen Individuen in der Vergangenheit und in der Zukunft eine vergleichbare Möglichkeit erhalten in den Besitz von Ether zu gelangen.[92]

Es kann argumentiert werden, dass bei Bitcoin eine ungerechte Verteilung zugunsten frühzeitiger Anwender, im englischen *Early Adopter*, stattgefunden hat. In den ersten Jahren konnten Miner mit einem herkömmlichen Computer regelmäßig Blöcke finden und somit die 50-BTC Belohnung erhalten, die heute mehrere tausend Euro wert sind. Eine Konzentration einer großen Menge BTC in einer im Vergleich zu heute relativen kleinen Gruppe von Individuen. Dem ist entgegenzuhalten, dass diese frühzeitigen Anwender durch verschiedene Maßnahmen zur Bekanntheit und Sicherheit des Netzwerkes beigetragen haben. Hinzu kommt, dass auch immer das Risiko eines Scheiterns anfänglich höher war.

Bei Ethereum ist das Argument der Verteilung zugunsten der frühzeitigen Anwender ein wenig zu relativieren. Die Verteilung in einer offen zugänglichen ICO an über 9000 Investoren, hat die initiale Verteilung verteilter als bei Bitcoin gestaltet. Hinzu kommt, dass sich zum Zeitpunkt der ICO im Jahr 2014 die Szene um Kryp-

[91] Der Begriff Initial Coin Offering ist an den englischen Begriff Initial Public Offering (IPO) angelehnt, der einen Börsengang von Unternehmen beschreibt.
[92] Vgl. Buterin (2013), S. 30f.

towährungen sich bereits deutlich vergrößert hat. Begriffe wie Bitcoin oder Kryptowährungen sind in den Jahren zuvor durch den rasanten Wertaufstieg und Wertabstieg der Währung und die Hacking-Angriffen auf große Kryptowährungsbörsen immer wieder in der öffentlichen Wahrnehmung aufgetreten. Die initiale Verteilung war aus diesen Gründen daher bei Ethereum insgesamt zugänglicher als bei Bitcoin.

Ein weiterer Punkt ist die fortlaufende Zufuhr von neuen Einheiten in die Währung. Der deflationäre Charakter von Bitcoin ermutigt die frühzeitigen Anwender ihre Bitcoins zu halten, sodass sie im Wert steigen. Die Eintrittsbarriere für Neueinsteiger wird somit auch durch die steigende Verbreitung immer höher. Die kleinste Einheit Satoshi ist noch weit unter einem Euro-Cent zu erwerben. Trotzdem können für Geringverdiener in den Entwicklungsländern die höheren Eintrittsbarrieren in der Zukunft zum Problem werden, sodass Bitcoin eher den Anspruch eines digitalen Wertlagers, statt des eines digitalen Zahlungssystem hat. Ethereum mit einem leicht inflationären Charakter belohnt nicht das Halten von Ether, da damit ein Kaufkraftverlust einhergeht. Sollte Ethereum das angestrebte Ziel schaffen, dass sich Verlustrate und laufende Ether-Zufuhr decken, kann sogar von einer wertstabilen Währung gesprochen werden. Somit sind hier die Eintrittsbarrieren für Neueinsteiger deutlich geringer. Des Weiteren ist die kleinste Ether-Einheit, der Wei, die achtzehnte Nachkommastelle von einem Ether, sodass eine ausreichende Stückelung der Währungseinheiten vorhanden ist. Diese Gründe sprechen dafür, dass Ether Neueinsteigern geringere Eintrittsbarrieren bietet.

Der EZB-Rat bevorzugt eine leicht inflationäre Währung gegenüber einer leicht deflationären Währung.[93] Während Bitcoin das Halten und Sparen belohnt, ermutigt Ether zum schnelleren Ausgeben und hat geringere Eintrittsbarrieren für Neueinsteiger. Der geplante Umstieg auf PoS in Ethereum kann auch bei Ethereum das Halten von Ether für das Mining in Zukunft belohnen, sodass ein Anreiz für das Halten dann auch bei Ethereum vorhanden sein kann.

[93] Deutsche Bundesbank (2015), S. 153f.

5.1.2. Kryptowährung und traditionelle Währungen

Durch die steigende Anwendung von Kryptowährungen beschäftigen sich die Regierungen weltweit zunehmend mit der regulatorischen Bewertung jener. Die Einstufung der Staaten von der digitalen Währung BTC ist unterschiedlich und reicht von toleranten Begrenzungen (z.B. Deutschland: Privates Geld) bis zu sehr restriktiven Maßnahmen (z.B. Vietnam: Illegale Währung).[94] Die Einstufung Ethereums ist noch nicht soweit fortgeschritten. Restriktive Maßnahmen gegen Kryptowährungen verwundern, wenn bedacht wird, dass sie die drei Geldfunktionen erfüllen und mit heutigen, traditionellen Geld vergleichbar sind.[95]

Kryptowährungen können durch diese Eigenschaften auch in Konkurrenz zu den traditionellen Währungen stehen. Interessant sind hierbei die Unterschiede der Verteilung. Moderne Geldverfassungen der entwickelten Länder haben zwei prägnante Charakteristiken. Erstens, die Geldverteilung ist durch ein Monopol zentral gesteuert. Zweitens, diese zentralen Behörden (meist Zentralbanken) sind durch keine Deckungsvorschriften an irgendwelche Substanzwerte gebunden.[96]

Kryptowährungen stehen als dezentrale Online-Währungen ohne zentralen Herausgeber in Kontrast zu den modernen Geldfassungen. Die Herausgabe geschieht nach mathematischen, algorithmischen Prinzipien. BTC, als erste Kryptowährung, hat die öffentliche Wahrnehmung in Hinsicht politischer Aspekte als Währung ohne Zentralbank gesteigert.

Dieser Umstand mag auch ein Grund für die Idee Nakamotos gewesen sein. Dazu sind zwei Aspekte relevant. Erstens, die verdeckte Nachricht im Genesis-Block lässt eine Vermutung zu, dass Bitcoin auch als Antwort auf ein marodes Bankensystem gedacht ist, welches sich in 2009 in einer Finanzkrise befand. Eine Finanzkrise, die durch massives Eingreifen von geldpolitischen Maßnahmen begleitet wurde. Zweitens, lassen Nakamotos weitere Äußerungen auf eine Nähe zum klassischen Liberalismus schließen. Die Anhänger des klassischen Liberalismus sprechen sich gleichermaßen für gesellschaftliche und wirtschaftliche Rechte aller Menschen aus.[97] In diesem Zusammenhang unterstreicht Friedrich August von Hayek,

[94] Vgl. Halaburda et al. (2016), S. 99.
[95] Vgl. ebd., S. 156-159.
[96] Vgl. Sixt (2016), S. 59.
[97] Vgl. ebd., S. 147-149.

ein Ökonom des klassischen Liberalismus und der davon abzweigenden Österreichischen Schule der Nationalökonomie, in seinem Buch *Entnationalisierung des Geldes* die Hindernisse eines gesetzlichen Zahlungsmittels für die Anwendenden durch den Zwang es als Geld zu benutzen.[98] Hayek plädiert für ein wertstabiles Geld ohne große Inflation und Deflation. Als Lösung spricht sich Hayek für den freien Wettbewerb zwischen staatlichem und privaten Geld aus.[99]

Kryptowährungen können in diesem Zusammenhang als privates Geld interpretiert werden. Viele Akteure im Online-Bereich akzeptieren bereits jetzt Kryptowährungen, da sie schneller, sicherer und günstiger als traditionelle Währungen sind. Eine Auslandsüberweisung über 0,01 USD von den USA nach Indonesien kann Tage oder Woche dauern und Kosten zwischen 0,50 und 50 USD verursachen.[100] Kryptowährungen brauchen nur Sekunden zum Transferieren und nur Minuten zur Bestätigung. Die Kosten betragen dabei umgerechnet meist nur wenige Cents. Ein technologischer Rückstand, wenn man bedenkt, dass Kommunikation über das Internet heute normalerweise schnell, sicher und günstig ist. Kryptowährungen treten daher bei Online-Zahlungen in Konkurrenz zu traditionellen Währungen.

Kryptowährungen und traditionelle Währungen haben unterschiedliche Ansätze, um die Wertigkeit des Geldes sicherzustellen. Bei Kryptowährungen sichert das manipulationssichere Protokoll den Wert der Währung, dagegen ist es ist bei traditionellen Währungen meist der Staat bzw. eine zentrale Stelle.

Mit Kryptowährungen lassen sich viele verschiedene Konzepte verwirklichen. Eine Abschaltung ist technisch durch die globale, dezentrale Struktur schwierig, sodass ein Verbot eines einzelnen Staates vergleichbar mit dem Verbot oder der Restriktion des Internets ist. Diese Schwierigkeiten Kryptowährungen komplett zu verbieten, lassen sie und traditionelle Währungen weiterhin im Wettbewerb zu einander stehen.

[98] Hayek (1976), S. 22.
[99] Vgl. ebd., S. 126f.
[100] Vgl. Sixt (2016), S. 75.

5.1.3. Geschwindigkeit der Bestätigungen

Für die Benutzer von Kryptowährungen ist die Zeit, die für das Bestätigen von Blöcken benötigt wird die relevante Kennziffer für die Dauer einer Transaktion im Netzwerk. Laut Antonopoulos ist das Blockintervall ein Kompromiss zwischen schnelleren Bestätigungszeiten und die Wahrscheinlichkeit einer Fork in der Blockchain. Erst durch eine gewisse Mindestanzahl von zurückliegenden Blöcken gilt eine Transaktion als ausreichend bestätigt und unwiderruflich.[101] Die Verbreitung einer Transaktion über das Netzwerk kann nicht herangezogen werden, da erst der Mining-Prozess den ausreichenden Schutz vor dem Double-spending-Problem gibt.

Nach sechs Bestätigungen bzw. einer Stunde gilt ein Block in Bitcoin als unwiderruflich. Bei Ethereum sind es unter ähnlichen Sicherheitsaspekten zirka drei Minuten.[102] Ethereum hat im Vergleich zu Bitcoin deutlich kürzere Bestätigungszeiten und Wartezeiten für unwiderrufliche Transaktionen, woraus sich ein Vorteil für Ethereum ergibt. In zahlreichen Bereichen ist eine zehnminütige bzw. stündliche Wartezeit von Nachteil. Ist diese Wartezeit bei einem Online-Händler bei Erwerb eines physischen Gutes noch problemlos, ist die Wartezeit bei Erwerb eines digitalen Gutes, das heutzutage direkt nach Zahlungseingang ausgeliefert wird, problematisch. Für Bitcoin mit Ziel als Online-Währung zu agieren, stellt sich dies als nicht optimal heraus. Bei Betrachtung von Transaktionen mit ausreichend Bestätigungen ist Ethereum deutlich schneller und somit im Vorteil. Allgemein lässt dadurch die kürzere Blockzeit bei Ethereum eine flexiblere Gestaltung zu.

5.2. Blockchain 2.0. – Verträge

Transaktionen im Blockchain-Netzwerk dienen dem Transfer eines digitalen Wertes. Dieser digitale Wert muss aber nicht unbedingt eine Geldfunktion, wie bei Bitcoin, besitzen. Die Möglichkeit dem digitalen Wert komplexe Daten anzuhängen hat sich mit der Idee von programmierbaren Geld oder Verträgen immens gesteigert. Durch die Ethereum-Plattform können solche Verträge und Smart Contracts durch Programmierer umgesetzt werden und die meisten Einsatzmöglichkeiten

[101] Vgl. Antonopoulos (2014), S. 204.
[102] Vgl. Buterin (2015), Buterins Grundlage ist eine 17-Sekunden-Blockzeit. Es handelt sich dann um zehn Bestätigungen.

dürften bisher noch unbekannt sein. Die Fähigkeit die dynamischen Datenstrukturen solcher Smart Contracts abzubilden, stößt bei Bitcoin an seine Grenzen. Grund dafür ist vor allem die simple Skriptsprache bei Bitcoin, die bewusst für Bitcoin gewählt wurde und hier auch ihre Stärken, besonders in Sicherheitsaspekten, ausspielen kann.

Einige Projekte versuchen die Bitcoin Blockchain auf derartige Einsatzmöglichkeiten zu erweitern. Laut Sixt wird das Bitcoin-Transaktionssystem für derartige alternative Zwecke zu verwenden in zwei Kategorien eingeteilt:[103]

- Funktionen, die mit dem im Bitcoin-Protokoll vorhandenen Script umgesetzt werden können (z.B. Multi-Signatur-Transaktionen oder Treuhandkonstrukte).

- Aufgesetzte Anwendungen (*Overlays*), die auf dem Bitcoin-Transaktionssystem liegen.

Ein Overlay ist eine aufgesetzte Schicht, die vergleichbar mit dem Verhältnis von Internet zu World Wide Web ist. Das Internetprotokoll TCP/IP ist dabei vergleichbar mit dem Bitcoin-Protokoll und das World Wide Web Protokoll HTTP mit einem Overlay.

Overlay-Anwendungen folgen dem Ansatz die Blockchain für andere vertrauensunabhängige Formen des wirtschaftlichen Ausgleichs zu nutzen. Die verschiedenen Projekte der Overlay-Anwendungen greifen das Prinzip der Smart Contracts auf. Ein Beispiel für ein solches Projekt das Smart Contracts verwendet ist Counterparty.[104] Eine weitere Idee wurde mit *Colored Coins*[105] von Meni Rosenfeld vorgestellt, die das Einfärben von BTC-Münzen beschreibt. „Der Begriff Farbige Münzen beschreibt dabei eine bestimmte Methode zur Darstellung und Verwaltung von realen Vermögenswerten im Bitcoin-Transaktionssystem.“[106] Generell werden Overlay-Anwendungen über eine Soft Fork eingeführt, sodass nicht alle Knoten der Protokolländerung zustimmen müssen.

[103] Vgl. Sixt (2016), S. 163-166.
[104] Vgl. ebd., S. 168.
[105] Rosenfeld (2012).
[106] Sixt (2016), S. 167.

Mit den verschiedenen Anwendungen lassen sich die Funktionalitäten erweitern. In Kapitel 5.3.2 werden weitere Projekte vorgestellt, die die Limitationen der Bitcoin Blockchain zu lösen versuchen. Die Anwendungsschichten werden auch als Bitcoin 2.0. Anwendungen bezeichnet, da sie Funktionalitäten der Blockchain 2.0. Kategorie repräsentieren.

Ethereum, als Blockchain 2.0. Anwendung, hat ein Protokoll, das wesentlich auf die Generierung von Smart Contracts und DApps ausgerichtet ist. Ein Hauptunterschied zwischen Bitcoin und Ethereum liegt in der vollständigen Programmierbarkeit der Ethereum-Blockchain, durch die Turing-vollständige Programmiersprache. Mit der Turing-Vollständigkeit wird die universelle Programmierbarkeit eines Systems beschrieben. „Eine turing-vollständige Programmiersprache kann verwendet werden, um jede andere Computersprache (nicht nur seine eigene) zu simulieren - es ist ein Satz von Anweisungen, die Bedingungen enthalten, Schleifen und Schreib- und Lesespeicher.“[107]

In Ethereum werden die Smart Contracts innerhalb der EVM ausgeführt. Die EVM ähnelt dabei den Script von Bitcoin, die in einer maschinenorientierten Programmiersprache geschrieben ist. Für Ethereum wurden zur besseren Programmierbarkeit verschiedene höhersprachige Programmiersprachen entwickelt, die dann in die für die EVM lesbaren Bytecode kompiliert wird. Die aktuellste und favorisierte Sprache ist zurzeit Solidity, die von der Struktur an Java ähnelt.[108]

Interessante Anwendungsfelder für Smart Contracts sind dezentrale Applikationen (DApps) und dezentrale autonome Organisationen (DAO). Ein DApp ist gewissermaßen eine auf der Blockchain gespeicherte Applikation. Eine DApp ist dabei zu jeder Zeit vollständig einsehbar. Es ist eine Weiterführung des Open-Source-Gedanken, bei dem der Programmcode häufig manuell abgelegt wird und somit den Zustand eines bestimmten Zeitpunktes repräsentiert. Giese et al. spricht in diesem Zusammenhang von *Open Execution*. DApps profitieren auch von einer weiteren Eigenschaft der Blockchain. Erst durch eine Hard Fork ist eine DApp zwangsmäßig aus der Blockchain zu entfernen. Solange es eine kleine Anzahl von Minern und Knoten gibt, kann eine DApp ewig laufen. Auf der Webseite dapps.ethercasts.com

[107] Vgl. Sixt (2016), S. 15.
[108] Vgl. Giese et al. (2016), S. 56.

können DApp-Projekte eingetragen werden. Am 26.01.2017 sind 328 DApps gelistet, wobei die meisten der Projekte in Entwicklungs- oder Konzeptstatus sind.[109]

Bei einer DAO haben die Mitglieder und Anteilseigner das Recht den Fond der Entität und dessen Algorithmen, nach vereinbarten Prinzipien, zu modifizieren. Ein Beispiel einer solchen DAO ist Bitcoin, dass sich nach definierten Konsens verhält und dabei ebenfalls ohne menschliche Führung agiert.[110]

Mit einer DAO sind bereits administrative, nicht-finanzielle Konstrukte denkbar, die im Rahmen von Blockchain 3.0. einzuordnen sind. Wie der Hack von *The DAO* im Sommer 2016 zeigt, sind solche Konstrukte mit besonderer Sorgfalt zu kreieren. Allgemein muss die Öffentlichkeit über diese neue Form von Organisationen informiert werden und es sind etliche Fragen, wie die Frage nach der Haftbarkeit ohne menschliche Führung, zu klären. Das DAO-Konstrukt ist bisher noch wenig etabliert und steht noch am Anfang der Entwicklung.

Diese Möglichkeiten zeigen auf, welchen Vorteil Ethereum gegenüber Bitcoin im Sinne der Vielfalt der Programmierbarkeit besitzt. Ethereum ermöglicht es ganze Kryptowährungen über Smart Contracts und DApps abzubilden. Umgekehrt schafft es Bitcoin nur über Umwege Smart Contracts zu ermöglichen, die zurzeit aber noch an den Limitationen des Bitcoin-Protokolls hängen. Nochmals sollte darauf hingewiesen werden, dass Bitcoin speziell für den Einsatz als digitales Zahlungssystem konzipiert wurde. Dieser Vorteil für Ethereum bedeutet daher nicht unbedingt einen Nachteil für Bitcoin.

5.3. Vergleich der Blockchain

5.3.1. Sicherheit

Beide Systeme zeigen Sicherheitsrisiken. Ein gemeinsames Risiko ist die Selbstbestimmtheit der Nutzer über die Kryptowährung. Durch die Eigenschaft, dass Transaktionen irreversibel sind, sind einmal getätigte Transaktionen nicht rückgängig zu machen. Was auf der einen Seite für Online-Händler eine nützliche Eigenschaft für Zahlungssicherheit im Internet darstellt, kann für unerfahrene Nutzer bedeuten,

[109] Vgl. Hitchcott (2017).
[110] Vgl. Buterin (2013), S. 23.

dass bei Unachtsamkeit Fehltransaktionen entstehen können, die bei einer herkömmlichen Banküberweisung noch nachträglich storniert werden können. Es gibt Prüfsummen in den Adressformaten und nutzerfreundliche Wallet-Software, die so etwas versuchen zu verhindern, allerdings resultiert daraus eine erhöhte Selbstbestimmtheit und Auseinandersetzung der Nutzer mit den Kryptowährungen gegenüber herkömmlichen Währungssystemen. Transaktionen der Kryptowährungen sind vergleichbar mit Bargeldüberweisung, nur das an die Stelle von zwei Menschen je zwei scheinbar anonyme, gesichtslose Adressen rücken.

Ein viel gravierendes Risiko stellt der Verlust des privaten Schlüssels dar. Auch hier erfordert die neue Technologie mehr Selbstbestimmtheit vom Nutzer als bei herkömmlichen Währungssystemen, wo beispielsweise der Verlust des geheimen PIN der EC-Karte nicht zum Verlust des mit dem Konto verknüpften Guthabens führt. Die Bank als zentrale Datenstelle kann über die Identität des Kunden den PIN wiederherstellen, was bei Bitcoin und Ethereum nicht möglich ist. An dieser Stelle ist zu erwähnen, dass gerade die Erfolgsgeschichte von Bitcoin auch mit einer Reihe von Negativereignissen gespickt ist. Neben verlorengegangenen privaten Schlüssel, die vor allem durch fehlende Sicherheitskopien oder Unfälle passieren, sind gerade die Diebstähle bei großen Börsen bzw. Tauschplattformen beachtenswert. Bei einer Vielzahl von Tauschplattformen ereigneten sich Hackerangriffe, die zu dem damaligen Zeitpunkt den BTC-Preis mehr oder weniger beeinflusst und das Vertrauen verringert haben. Nennenswert ist hier der bisher größte Bitcoin-Hack an der zu diesem Zeitpunkt her größten japanischen Tauschbörse MT. Gox über 744 408 BTC mit dem damaligen Wert von 590 Mio. Euro.[111]

Bei Ethereum fehlt durch die relative Neuheit des Systems und die geringe Marktkapitalisierung der Kryptowährung Ether vergleichbare Ereignisse. Trotzdem sind Hackerangriffe auf unsichere Tauschbörsen, die Ether handeln, technisch genauso möglich wie bei Bitcoin. Dieses Phänomen ist allerdings kein Sicherheitsmerkmal der Kryptowährungssysteme an sich, sondern vielmehr der unsicheren Tauschbörsen, die häufig die privaten Schlüssel auf Servern lagern, die direkt mit dem Internet verbunden sind. Ein für Ethereum vergleichbarer Vorfall ereignete sich im Sommer 2016 bei der Finanzierung des an Ethereum gekoppelten Projektes von Slock.it, genannt The DAO. In einer ICO sammelte die deutsche Firma Slock.it

[111] Vgl. Sixt (2016), S. 92f.

zwölf Mio. Ether, zu dem Zeitpunkt ungefähr 150 Mio. USD, über einen Smart Contract ein.[112] The DAO ist eine DAO, die sich über den Programmcode selbst verwalten sollte. Ein Hacker konnte eine Sicherheitslücke des Smart Contracts ausnutzen und entzog The DAO einen Teil (3,5 Mio. Ether) des investierten Ethers. Über eine Hard Fork konnten die gestohlen Ether schlussendlich zurückgeholt werden. Es handelte sich also um einen Programmierfehler eines Smart Contracts und nicht um ein generelles Problem von Ethereum. Nachdem der Wechselkurs der Kryptowährung Ether um mehr als 50% zusammenbrach, bleiben weitere Fragen offen, wie beispielsweise in Zukunft mit ähnlichen Fällen umzugehen ist. Bei weiterem Eingreifen kann die Ethereum-Plattform unter anderem den dezentralen und autonomen Anspruch verlieren, welchen sie konträr zu dem zentralisierten Gegensatz darstellen möchte.

Ein oft diskutiertes Angriffsszenario gegen die Blockchain ist die sogenannte „51%-Attacke". Bei einer solchen Attacke wird 51% bzw. mehr als die Hälfte der Gesamtrechenleistung durch einen Angreifer kontrolliert. Technisch bedeutet eine 51%-Attacke, dass ein Angreifer eine höhere Wahrscheinlichkeit gegenüber dem restlichen, ehrlichen Netzwerk hat, das Rennen um den nächsten Block zu gewinnen. Der Angreifer kann so durch die Eigenschaften der Blockchain die folgenden Transaktionen zu seinen Gunsten manipulieren, sodass die Münzen doppelt ausgegeben werden können. Theoretisch ist eine solche Attacke bereits mit 30% der Gesamtrechenleistung möglich. Die Möglichkeit einer solchen Attacke wurde von Anfang an berücksichtigt. Neben einer hohen Anfangsinvestition in die Hardware, soll das Blockbelohnungssystem potenziellen, profitorientierten Angreifern einen Anreiz dazu geben, ehrlich zu bleiben. Die Idee dahinter ist, dass es für Miner viel profitabler ist die Blöcke ehrlich zu validieren und die Einnahmen zu verkaufen, anstatt double-spending zu betreiben und durch den dann eingetretenen Vertrauensverlust in das System einen drastischen Kurseinsturz in Kauf nehmen zu müssen. Attacken durch nicht profitorientierte Akteure könnten nach Antonopoulos am Wahrscheinlichsten staatlich-finanzierter Natur sein.[113]

Aus diesen Erkenntnissen folgt, dass die Robustheit gegenüber einer solchen Attacke von der Gesamtrechenleistung des Netzwerkes abhängt, denn je größer diese

[112] Vgl. Jentzsch (2016).
[113] Vgl. Antonopoulos (2014), S. 210-213.

ist, desto höhere Anfangsinvestitionen muss ein Angreifer für die Hardware aufbringen. Am 16.01.2017 hat Bitcoin eine in der Hash-Rate gemessene Gesamtrechenleistung von 2.763.318 Terrahash pro Sekunde (TH/s) während die von Ethereum bei 7,25 TH/s liegt. Das Bitcoin-Netzwerk ist in dieser Hinsicht deutlich robuster und sicherer gegenüber Angriffen als das Ethereum-Netzwerk.

5.3.2. Skalierbarkeit

Das Bitcoin-System stößt durch sein rasantes Wachstum langsam an seine Grenzen. Nicht nur die rasant steigende Größe der Blockchain stellt ein Problem dar, auch die Begrenzung der Blockgröße auf ein Megabyte wird zunehmend erreicht. In Stoßzeiten sorgt dieses Problem für einen regelrechten „Stau" der Transaktion im unbestätigten Transaktionspool der Miner. Des Weiteren sorgt es dafür, dass für Transaktionen mit zu geringen Gebühren die Wartezeit ansteigt bzw. die Gebühr für schnelle Transaktionen ansteigt, sodass das System für Kleinstüberweisungen zunehmend ungeeigneter wird. Eine Protokolländerung ist möglich, erfordert aber eine Konsensbildung zwischen den Netzwerkteilnehmern, um die Zukunftsfähigkeit zu sichern. Es gibt verschiedene Lösungsansätze für kurz- und langfristige Verbesserung. Eine Anhebung der Blockgröße ist eine Möglichkeit, um kurzfristig eine Lösung zu finden. Die Blockchain prozessiert pro Sekunde, je nach Betrachtungsweise, drei bis sieben Transaktionen. Um mit dem VISA Netzwerk, welches bis zu 47000 Transaktionen in der Sekunde abwickelt, einigermaßen konkurrenzfähig zu werden, müsste die Blockgröße erheblich angehoben werden, was die Blockchain-Größe immens erhöhen würde und weitere Probleme in der Dezentralität des Netzwerkes mit sich ziehen würde (Siehe dazu Kapitel 5.3.3). Weiterhin schließt die jetzige Blockgröße aus, dass Smart Contracts im Bitcoin-Protokoll durch Script genutzt werden können, da auch davon die Blockgröße belastet wird.[114]

Das *Lightning Network*[115] und *Sidechains* sind mögliche Lösungskonzepte für das Skalierungsproblem, die als Overlay-Anwendungen konzipiert sind. Das Lightning Network soll ein angegliedertes, dezentrales, direktes (off-blockchain) Zahlungssystem für die zahlreichen Kleinstüberweisungen sein. Der Lösungsansatz würde

[114] Vgl. Sixt (2016), S. 96f.
[115] Vgl. Poon et al. (2016), S. 1.

durch eine Soft Fork implementiert werden, d.h. dass die Mehrheit der Full Nodes dieser Lösung zustimmen müsste, damit es durch die Unterstützung einigermaßen sicher läuft.[116] Sidechains wurden von *hashcash* Autor Adam Back und weiteren Autoren in dem White Paper *Enabling Blockchain Innovations with Pegged Sidechains*[117] vorgestellt. Sidechains sind parallel zur Bitcoin laufende alternative Blockchains, die mit der Bitcoin Blockchain interagieren. Durch das Ausgliedern auf verschiedene Sidechains, könnte Bitcoin so entlastet und besser skalierbar werden. Durch das Verwenden von alternativen Blockchains mit unterschiedlichen Eigenschaften könnten damit auch weitere Begrenzungen von Bitcoin verbessert werden. Sidechains stehen noch am Anfang des Entwicklungsprozesses und viele Fragen sind noch unbeantwortet.[118]

Ethereum besitzt keine Blockbegrenzung. Die Datengröße des Blocks wird über dessen maximalen Gas-Betrag gesteuert. Durch die nur geringen Anpassungsmöglichkeiten von unter 0,1% pro Block durch die Miner, könnte ein sprunghafter Anstieg auch hier kurzfristig einen Stau an Transaktionen nach sich ziehen. Zum jetzigen Zeitpunkt ist Ethereum skalierbar, Bitcoin ist dies nicht.

Die steigende Größe der Blockchain ist auch für Ethereum ein Problem. Vitalik stellt fest, dass es für Ethereum in dieser Hinsicht keine fundamentalen Verbesserungen über das in Bitcoin verwendete Prinzip gibt.[119]

5.3.3. Dezentralität

Dezentralität ist eine Kerneigenschaft der Kryptowährungssysteme. Es muss sich damit auseinandergesetzt werden, wie die Dezentralität bei weiterhin steigendem Interesse für Kryptowährungssysteme gewährt werden kann. Ein guter Gradmesser für die Beantwortung der Frage sind die Anzahl der Full Nodes im Netzwerk, denn simpel ausgedrückt, je mehr Full Nodes es gibt, desto dezentraler ist das Netzwerk organisiert.

---

[116] Vgl. Sixt (2016), S. 117.
[117] Back et al. (2014).
[118] Vgl. Sixt (2016), S. 115-117.
[119] Vgl. Buterin, Vitalik (2014a).

Wie bereits in Kapitel 4.1 beschrieben ist für die einfachen Anwender mit Wallet-Funktion das Herunterladen der Blockchain nicht notwendig. Durch die wachsende Größe der Blockchain wird das Benutzen von leichtgewichtigen Knoten zunehmend attraktiver. Auch müssen nicht mehrere Tage mit dem Herunterladen der Blockchain gewartet werden.

Eine andere Gruppe von Full Nodes ist bei den Minern zu finden. Die Anzahl der Miner ist im Wesentlichen durch die Rentabilität jener definiert. Die Rentabilität wird durch unterschiedliche Faktoren wie dem Verhältnis zu der Gesamtnetzrechenleistung, den Marktpreis der Kryptowährung, der Blockbelohnung, den Anschaffungspreis der Hardware, den aktuellen Strompreis und weiteren kleineren Faktoren beeinflusst und kann daher je nach Standort variieren. Da Bitcoin und Ethereum beide (noch) den rechenintensiven PoW-Algorithmus verwenden, spielt der Strompreis eine wichtige Rolle. Um die Einnahmen des Mining planbarer zu machen, gruppieren sich viele Miner in sogenannten Mining-Pools zusammen. Ein Mining-Pool bündelt die Rechenleistung seiner Mitglieder und schürft somit mit einer höheren Rechenleistung nach Blöcken. Bei Erfolg wird die Blockbelohnung an die Mitglieder entsprechend ihrer eingespeisten Rechenleistung ausgeschüttet. Ein weiterer Aspekt ist, dass Miner das Herunterladen einer kompletten Kopie der Blockchain auf den Mining-Pool Betreiberknoten auslagern können. Sowohl bei Bitcoin, als auch bei Ethereum sind die größten Miner Mining-Pools.

Trotz der höheren Marktkapitalisierung und Gesamtnetzwerkrechenleistung Bitcoins ist die Anzahl der Full Nodes bei Ethereum (6025)[120] größer als bei Bitcoin (5574)[121]. Die kürzere Blockzeit sowie der eigene Algorithmus Ethash begünstigt bei Ethereum den Neueinstieg und den Betrieb beim Mining. Zum einen werden keinen hochspezialisierten Computer benötigt, da bereits bestehende Hardware benutzt werden kann. Zum anderen sorgt das Einbinden und Belohnen der Ommer-Blöcke für einen Anreiz zum einzelnen Mining.

In diesem Sinne kann von Ethereum behauptet werden, dass es dezentraler als Bitcoin ist. Der Wechsel auf PoS kann zudem die Dezentralität in Zukunft weiter verstärken.

[120] Ethereum Nodes Explorer (2016).
[121] 21.co (2017).

5.3.4. Mining und ökologische Folgen

Im Zusammenhang mit Kryptowährungen steht immer wieder auch der stromintensive Mining-Prozess im Fokus. Bei Bitcoin ist das besonders zu beobachten. Auf Videoportalen wie YouTube werden teilweise riesige Lagerhallen voller Mining-Hardware präsentiert. Der Umstand zeigt deutlich das Problem beim Mining. Das PoW-Konzept, das die Sicherheit der Blockchain bereitstellt, ist durch ihren enorm hohen Stromverbrauch gleichzeitig ein allgemeiner Kritikpunkt. Da Hauptindikator für das schnelle Berechnen die Hash-Rate pro Sekunde ist, ist bei Bitcoin in Laufe der Jahre eine fortlaufende Hardwarespezialisierung aufgetreten. War es an am Anfang noch möglich mit der CPU bzw. der GPU seines Computers einen Block zu finden, reicht dies heute nicht mehr aus. Seit Juni 2013 werden ASIC Miner verwendet. ASIC Miner sind spezielle Computer, die ausschließlich SHA256 Hash-Berechnungen durchführen. Die Leistungsfähigkeit übersteigt die der leistungsfähigsten Grafikkarten um das 50- bis 500-fache. Eine regelrechte spezialisierte Mining-Hardware Branche hat sich gebildet, die jedes Jahr effizientere Spezialrechner auf den Markt bringt. Um beim globalen Wettrennen der steigenden Hash-Rate mithalten zu können, müssen Miner stetig neue ASICs kaufen oder ältere Modelle ersetzen. Die Entwicklung ist dabei so rasant, dass die Hardware nach wenigen Monaten nicht mehr rentabel ist. Durch seine hohe Spezialisierung ist ein ASIC-Computer nach seiner kurzen Laufzeit auch kaum weiter zu verwenden.[122]

Neben den Anschaffungskosten ist der weitaus größere Kostenblock die laufenden Kosten durch Energie- und Kühlkosten. Das Hamilton Institute hat 2014 herausgearbeitet, dass das Mining-Netzwerk von Bitcoin bereits damals einen Stromverbrauch hat, der vergleichbar mit dem von ganz Irland ist.[123] Der Strompreis spielt für die Standortwahl bei professionell agierende Mining-Farmen eine entscheidende Rolle. So werden unter anderem deshalb 70% des Bitcoin-Mining in China durchgeführt.[124] Ein weiterer Nachteil der ASIC Miner ist die hervorgerufene Zentralisierungstendenzen, was auch im Kapitel 5.3.3 angedeutet wurde.

Ethereum verfolgt mit Ethash einen ökologischeren Ansatz, auch wenn noch PoW genutzt. Ethash benötigt mehr Speicher und Bandbreite, sodass die spezialisierte

[122] Vgl. Sixt (2016), S. 103-105.
[123] O'Dwyer et al. (2014).
[124] Vgl. Sixt (2016), S. 105.

ASIC-Hardware keinen Vorteil gegenüber anderen Computern hat. Ethash führt den Mining-Gedanken zurück zu den Ursprünge Bitcoins, wo jeder Computer erfolgreich nach Münzen schürfen konnte. So kann bereits vorhandene Hardware für das Mining genutzt werden oder Mining-Hardware die nicht ausschließlich für das Mining verwendbar ist, sondern auch andere Einsatzmöglichkeiten hat.

Mit dem Wechsel auf PoS hat Ethereum einen weiteren Vorteil im Sinne einer ökologischeren Nutzung des Mining-Prozesses. Das virtuelle Mining würde Ethereum noch ressourcenschonenden machen. Bereits 2012 wurde PoS erstmals bei Peercoin eingesetzt, sodass es sich um kein komplett neues Konzept handelt.

6. Fazit und Ausblick

Die vorliegende Arbeit hat einen Einblick in die Funktionsweise der Blockchain-Technologie gegeben und einen Vergleich, bezogen auf die beiden bekanntesten Systeme Bitcoin und Ethereum, durchgeführt. Ursprünglich als Antwort auf die letzte Finanzkrise 2007 entworfen, wurde das Potential der Blockchain als sicheres, dezentrales Registerbuch aller Transaktionen in Bitcoin zunehmend erkannt und weiterentwickelt. Diese Entwicklung wird durch die drei Kategorien von Blockchain-Anwendungen von Swan beschrieben, wobei in dieser Arbeit Bitcoin und Ethereum sinnbildlich für die erste und zweite Kategorie stehen und miteinander verglichen worden.

In Hinblick auf den Vergleich in der ersten Kategorie weisen Bitcoin und Ethereum unterschiedliche Ansätze als Kryptowährung auf. Bitcoin tendiert zu einer Art digitalem Wertaufbewahrungsmittel, ähnlich wie Edelmetalle, zu werden. Zwei Ursachen sind dafür entscheidend. Zum einen der deflationäre Charakter, der aber durch die hohe, anfängliche Inflation zurzeit noch keinen großen Einfluss haben sollte. Zum anderen führt das Skalierungsproblem dazu, dass Transaktionen teuer werden und längere Bestätigungszeiten benötigen. Für Bitcoin mit dem Ziel als dezentrales, digitales Zahlungssystem, dass alltäglich benutzt werden soll, kann dieser Punkt kritisch sein, wenn sich das Netzwerk nicht für einen Lösungsansatz entscheidet. Ethereum als Kryptowährung ist besser für das ursprüngliche Ziel von Bitcoin ausgerichtet. Ethereum ist skalierbar, hat deutlich kürzere Blockzeiten und eine geeignetere Stückelung der Währung für den Einsatz als digitales Zahlungssystem. Trotzdem hat es den Nachteil, dass Bitcoin über eine weitaus größere Gemeinde und Infrastruktur zur Massenadaption verfügt. Die Bitcoin-Gemeinde muss sich grundlegend entscheiden, ob Bitcoin ein Wertaufbewahrungsmittel oder ein alltägliches, digitales Zahlungssystem sein soll.

In der zweiten Kategorie der Verträge ist Ethereum Bitcoin zurzeit überlegen. Hauptgrund dafür ist die komplett programmierbare Blockchain mit einer Turing-vollständigen Programmiersprache von der Ethereum-Plattform. Bitcoins Programmiersprache ist nicht Turing-vollständig, sodass nur eine beschränkte Nutzung für diesen Zweck möglich ist. Mit Overlay-Anwendungen verfügt Bitcoin aber über ein nützliches Werkzeug, um die Stärken von Bitcoin mit den Stärken anderer al-

ternativen Kryptotransaktionssysteme zu verbinden. Wie Counterparty zeigt, ist damit das Umsetzen von Smart Contracts möglich. Theoretisch ist auch das Anbinden eines „Ethereum-Klons“ an Bitcoin denkbar, um die Stärken von Bitcoin und Ethereum zu kombinieren. Die Entwicklungen rund um Sidechains können zukünftig von Bedeutung sein.

Beim Vergleich der Blockchain haben Ethereum und die Ethereum Blockchain in den meisten Vergleichspunkten einen Vorteil gegenüber Bitcoin und der Bitcoin Blockchain. Dies scheint nicht verwunderlich, wenn bedacht wird, dass Ethereum gerade deshalb angetreten ist, um Funktionalitäten zu erweitern und die Limitationen des Bitcoin-Systems aufzuheben. Besonders die Skalierbarkeit ist ein Vorteil, der hier besonders zu nennen ist. Durch die momentan fehlende Skalierbarkeit hat Bitcoin ein ernstzunehmendes Problem kurz- und mittelfristig. Auf der anderen Seite wird es für Ethereum schwer sein durch den zeitlichen Vorsprung von Bitcoin die Robustheit des Bitcoin-Netzwerkes gegenüber Angriffen zu erreichen, um im Bereich Sicherheit gleich zu ziehen. Als generelles Problem beider Systeme kann die totale Blockchain-Größe gesehen werden. Hier benötigt es in Zukunft Entwicklungsbedarf, um der Verfügbarkeit zu der kompletten Blockchain durch die steigende Größe nicht nur einen kleinen, elitären Kreis großer Unternehmen zugänglich zu machen, die über die notwendigen Speicherplatzressourcen verfügen. Ein weiterer allgemeiner Kritikpunkt sind die mit dem Mining verbundenen immensen Bereitstellungs- und Unterhaltungskosten. Der Ansatz von Ethereum geht sicherlich in die richtige Richtung, um ressourcenschonender zu agieren. Alternative Mining-Konzepte wie das geplante PoS bei Ethereum sollten getestet und weiterentwickelt werden. Hier ist sicherlich der Open-Source-Charakter der Kryptowährung- und Blockchain-Szene von Vorteil, um eine Lösung für diese Probleme in Zukunft zu finden.

Die Blockchain-Technologie ist dabei immer weitere Geschäfts- und Gesellschaftsfelder zu erschließen. Die Möglichkeiten, die sich aus ihr ergeben, machen die Blockchain zu einem ungemein hilfreichen Instrument. Viele der möglichen Anwendungsfälle sind heute noch unbekannt. Mehrere Wirtschaftsteilnehmer haben dies erkannt, sodass zahlreiche Investitionen in die Technologie oder mit der Technologie verbundene Unternehmen vorgenommen wurden. Auch die Banken als erste Betroffene erkennen nach anfänglicher Skepsis das Potential und versuchen

die Blockchain in ihre Geschäftsprozesse zu integrieren. Die große spanische Bank Santander hat als erste Bank im Mai 2015 eine Applikation für das Prozessieren von internationalen Zahlungen mit der Blockchain-Technologie vorgestellt.[125] Auch die Deutsche Bank stellt im gleichen Jahr fest, dass „die Blockchain-Technologie .. eine der ersten wirklich disruptiven Ideen aus dem Fintech-Bereich [ist]"[126] und Akteure aus dem Finanzsektor sich zunehmend damit beschäftigen.

Mit DApps aus Ethereum lassen sich unterschiedliche Eigentumsverhältnisse darstellen und über die Blockchain effizient prozessieren lassen. Bevor eine größere Adaption beginnen kann, sollte zuerst die weitere Entwicklung der Plattform durch die Ethereum Foundation abgewartet werden. Besonders ist zu beobachten, wie die beschriebenen, allgemeinen Herausforderungen gelöst werden und in Zukunft mit der Haftungsfrage bei autonom agierenden Organisationen umgegangen wird. Wie der Vorfall um The DAO zeigt, beeinflusst ein schlecht geschriebener Smart Contract die Reputation der Ethereum-Plattform als Ganzes. Für die positive Entwicklung von Ethereum ist die Beantwortung dieser Fragen von großer Bedeutung.

Mit Administration, Gesundheit, Wissenschaft, Literatur, Kultur und Kunst zielt Blockchain 3.0. bereits auf noch umfangreichere Gebiete für die Anwendung der Blockchain-Technologie. Die Blockchain-Technologie kann es hier schaffen nicht nur eine Anwendungsmöglichkeit für Transaktionen finanzieller Herkunft zu sein, sondern zu einer Art Massenadaption heranzuwachsen und somit ihre Flexibilität für verschiedene Einsatzmöglichkeiten zu zeigen. Auch hier muss für eine Einschätzung die nächsten Jahre abgewartet werden.

Wie das Internet ist die Blockchain-Technologie in den Trend hin zu mehr dezentralen Lösungen einzuordnen. Zentrale Lösungen können durch die Möglichkeiten der digitalen Revolution hinterfragt werden und durch effizientere, mehr dezentrale Lösungen ersetzt werden. Es gilt dabei die Blockchain-Technologie komplementär zu den bisherigen Lösungen zu verwenden und so eine Mischung aus den besten zentralisierten und dezentralisierten Konzepten zu erzeugen. Durch die ökonomischen Vorteile die sich durch den Einsatz von z.B. Smart Contracts ergeben, können kurzfristig Arbeitsplätze in der Gesellschaft obsolet werden. Die Funktion eines Notars der beispielsweise Grundbucheinträge beglaubigt, kann auch über Smart

[125] Vgl. Banco Santander (2015).
[126] Dapp et al. (2015).

Contracts auf der Blockchain abgebildet werden. Zurzeit wird in Schweden getestet das Katasteramt auf die Blockchain zu legen.[127] Wie so häufig bei technologischen Fortschritten würde dies bedeuten, dass dieser menschliche Arbeitsplatz durch die neue Technik ersetzt werden kann. Der technologische Fortschritt zeigt aber auch, dass langfristig ein neuer Arbeitsplatz an anderer Stelle dafür entsteht. Statt des Notars wird es in Zukunft Menschen brauchen, die Smart Contracts programmieren, interpretieren und administrieren können.

[127] Vgl. Chavez-Dreyfuss (2016)

Literaturverzeichnis

21.co (2016): Predicting Bitcoin Fees For Transactions. URL: https://bitcoin-fees.21.co/ [27.12.2016]

21.co (2017): Global Bitcoin Nodes Distribution. URL: https://bitnodes.21.co/ [16.01.2017]

Antonopoulos, Andreas M. (2014): Mastering Bitcoin. Unlocking Digital Cryptocurrencies. Sebastopol (O'Reilly Media, Inc.).

Back, Adam (2002): Hashcash - A Denial of Service Counter-Measure. URL: http://www.hashcash.org/papers/hashcash.pdf [02.12.2016]

Back, Adam / Corallo, Matt / Dashjr, Luke / Friedenbach, Mark / Maxwell, Gregory / Miller, Andrew / Poelstra, Andrew / Timón, Jorge / Wuille, Pieter (2014): Enabling Blockchain Innovations with Pegged Sidechains. URL: https://blockstream.com/sidechains.pdf [25.01.2017]

Banco Santander (2015): Santander becomes first UK bank to introduce blockchain technology for international payments with the launch of a new app. URL: http://www.santander.com/csgs/Satellite?appID=santander.wc.CFWCSancomQP01&c=GSNoticia&canal=CSCORP&cid=1278712674240&empr=CFWCSancomQP01&leng=en_GB&pagename=CFWCSancomQP01%2FGSNoticia%2FCFQP01_GSNoticiaDetalleMultimedia_PT18 [24.01.2017]

Blockchain Explorer (2016): Blockchain-Größe. URL: https://blockchain.info/de/charts/blocks-size [14.12.2016]

Bundesministerium der Finanzen (2013): Ihre schriftliche Frage Nr. 149 für den Monat Juni 2013. URL: http://wp1183395.server-he.de/FDP-Webseiten/FDP-www.frank-schaeffler.de/wp-content/uploads/2013/08/2013_06_20-Antwort-Bitcoin-Koschyk.pdf [19.10.2016]

Buterin, Vitalik (2013): Ethereum White Paper. A next generation smart contract & decentralized application platform. URL: http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [07.11.2016]

Buterin, Vitalik (2014): Toward a 12-second Block Time. URL: https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/ [05.01.2017]

Buterin, Vitalik (2014a): Ethereum Scalability and Decentralization Updates. URL: https://blog.ethereum.org/2014/02/18/ethereum-scalability-and-decentralization-updates/ [16.01.2017]

Buterin, Vitalik (2015): On Slow and Fast Block Times. URL: https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/ [22.01.2017]

Chavez-Dreyfuss, Gertrude (2016): Sweden tests blockchain technology for land registry. URL: http://www.reuters.com/article/us-sweden-blockchain-idUSKCN0Z22KV [28.01.2017]

Dai, Wei (1998): B-money. URL: http://www.weidai.com/bmoney.txt [28.11.2016]

Decker, Christian / Wattenhofer, Roger (2013): Information Propagation in the Bitcoin Network. URL: http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf [04.01.2017]

Dapp, Thomas / Karollus, Alexander (2015): Blockchain – Angriff ist wahrscheinlich die beste Verteidigung (Fintech #2). URL: http://www.dbresearch.de/servlet/reweb2.ReWEB?rwsite=DBR_INTERNET_DE-PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000358989 [25.01.2017]

Deutsche Bundesbank (2015): Geld und Geldpolitik. Frankfurt (Dt. Bundesbank).

Ethereum Wiki (2016): Design Rationale. URL: https://github.com/ethereum/wiki/wiki/Design-Rationale [04.01.2017]

Ethereum Wiki (2016a): Ethash Design Rationale. URL: https://github.com/ethereum/wiki/wiki/Ethash-Design-Rationale [04.01.2017]

Ethereum Wiki (2016b): Proof of Stake FAQ. URL: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ [04.01.2017]

Ethereum community (2016): Ethereum Homestead Documentation. URL: https://readthedocs.org/projects/ethereum-homestead/downloads/pdf/latest/ [28.11.2016]

Ethereum Foundation (2016): About the Ethereum Foundation. URL: https://www.ethereum.org/foundation [15.11.2016]

Ethereum Nodes Explorer (2016): The Ethereum Nodes Explorer. URL: https://www.ethernodes.org/network/1 [16.01.2017]

Ethereum Switzerland GmbH (2014): Terms and Conditions of the Ethereum Genesis Sale. URL: https://github.com/ethereum/www/blob/master-postsale/src/extras/pdfs/TermsAndConditionsOfTheEthereumGenesisSale-pre-view.pdf [23.11.2016]

Ether.Fund (2016): The Ethereum ether pre-sale results. URL: http://ether.fund/market [22.11.2016]

Giese, Philipp / Kops, Maximilian / Wagenknecht, Sven / De Boer, Danny / Preuss, Mark (2016): Die Blockchain Bibel. DNA einer revolutionären Technologie. Kleve (BTC-ECHO).

Halaburda, Hanna / Sarvary, Miklos (2016): Beyond Bitcoin. The Economics of Digital Currencies. Berlin, Heidelberg (Springer).

Hayek, F. A. v. (1976) Denationalisation of Money. An analysis of the theory and practice of concurrent currencies. London (Institute of economic affairs).

Hitchcott, Chris (2017) State of the Dapps. URL: http://dapps.ethercasts.com/ [26.01.2017]

Issing, Otmar (2014): Einführung in die Geldtheorie. München (Vahlen).

Jentzsch, Christoph (2016): The History of the DAO and Lessons Learned. URL: https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5#.beiy4swwt [09.01.2017]

Mahlmann, Peter / Schindelhauer, Christian (2007): Peer-to-Peer-Netzwerke. Algorithmen und Methoden. Berlin Heidelberg New York (Springer-Verlag).

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf [08.10.2016]

New Liberty Standard (2009): 2009 Exchange Rate. URL: http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate [12.10.2016]

O'Dwyer, Karl J. / Malone, David (2014): Bitcoin Mining and its Energy Footprint. URL: https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf [05.01.2017]

Paar, Christof / Pelzl, Jan (2016): Kryptografie verständlich. Ein Lehrbuch für Studierende und Anwender. Berlin Heidelberg New York (Springer).

Poon, Joseph / Dryja, Thaddeus (2016): The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. URL: https://lightning.network/lightning-network-paper.pdf [10.01.2017]

Rosenfeld, Meni (2012): Overview of Colored Coins. URL: https://bitcoil.co.il/BitcoinX.pdf [08.01.2017]

Sixt, Elfriede (2016): Bitcoins und andere dezentrale Transaktionssysteme. Blockchains als Basis einer Kryptoökonomie. Berlin Heidelberg New York (Springer-Verlag).

Swan, Melanie (2015): Blockchain. BLUEPRINT FOR A NEW ECONOMY. Sebastopol, CA (O'Reilly Media Inc.)

The Ethereum Blockchain Explorer (2016): Ethereum Network Stats. URL: https://www.etherchain.org/ [08.01.2017]

UCL (2016): UCL Research Center For Blockchain Technologies. URL: http://blockchain.cs.ucl.ac.uk [23.12.2016]

Wood, Gavin (2014): Ethereum: A secure decentralised generalised transaction ledger. URL: http://gavwood.com/paper.pdf [25.11.2016]

Eidesstattliche Erklärung

Ich versichere, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere, alle Stellen der Arbeit, die wortwörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht und die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt zu haben.

Lüneburg, 30.01.2017

Marco Schneekluth