HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

DIPLOMARBEIT

Herr Ing.

Klaus Froschauer

Matrikel-Nr.: 41490

Seminargruppe: KW13wVA-F

Blockchain – neue Chancen neue Möglichkeiten

Haid, 2017

Fakultät Wirtschaftsingenieurwesen

DIPLOMARBEIT

Blockchain – neue Chancen neue Möglichkeiten

Autor:
Herr Ing.

Klaus Froschauer

Studiengang:
Wirtschaftsingenieurwesen

Seminargruppe:
KW13wVA-F

Erstprüfer:
Prof. Dr. rer. pol. Andreas Hollidt

Zweitprüfer:
Prof. Dr. rer. pol. Andreas Piel

Einreichung:
Mittweida, 07.07.2017

Verteidigung/Bewertung:
Salzburg, 15.09.2017

Faculty Industrial Engineering

DIPLOMA THESIS

Blockchain – new opportunities new possibilities

author:
Mr. Ing.

Klaus Froschauer

course of studies:
Industrial Engineering

seminar group:
KW13wVA-F

first examiner:
Prof. Dr. rer. pol. Andreas Hollidt

second examiner:
Prof. Dr. rer. pol. Andreas Piel

submission:
Mittweida, 07.07.2017

defence/ evaluation:
Salzburg, 15.09.2017

Bibliografische Beschreibung:

Froschauer, Klaus:

Blockchain – neue Chancen neue Möglichkeiten - 2017. - 8, 58, 1S.

Mittweida, Hochschule Mittweida, Fakultät Wirtschaftsingenieurwesen, Diplomarbeit, 2017

Referat:

Die vorliegende Arbeit befasst sich mit dem Thema der Blockchain. Dazu wird zuerst auf die Entstehung als Dokumentationswerkzeug für Überweisungen von Bitcoins geblickt. Der dezentrale Aufbau der Blockchain wird genauer beschrieben und es wird erläutert warum dieser als fälschungssicher gilt. Anschließend wird Ethereum behandelt – eine Blockchain mit der Möglichkeit, programmierbare Verträge darin zu betreiben, um dadurch eine Anwendung in beinahe allen Bereichen des täglichen Lebens zu finden. Zuletzt werden noch Projekte erläutert, welche das enorme Potential der Blockchain verdeutlichen sollen.

I. Inhaltsverzeichnis

II. Abbildungsverzeichnis

1. Einleitung

1.1. Motivation

Im Jahr 1989 wurden die Grundlagen des World Wide Web entwickelt und etwa zwei Jahre später war es öffentlich und weltweit verfügbar. Damit war das Zeitalter des Internets angebrochen, auch wenn zum damaligen Zeitpunkt vermutlich nur wenige mit einer derartigen Erfolgsstory dieser Entwicklung rechneten. Heute, etwa 30 Jahre später, ist eine Welt ohne diesen virtuellen Raum mit seinen scheinbar unendlichen Möglichkeiten nicht mehr denkbar. Der tägliche Einkauf, eine Shopping-Tour, das Buchen einer Reise, das Knüpfen sozialer Kontakte sowie die Verbreitung von Nachrichten sind nur einige weniger Beispiele der vielen Aktivitäten, die heutzutage bereits online durchgeführt werden können.

Auch in der Finanzwelt wird die Nachfrage nach online abzuwickelnden Geschäften immer größer. Über das Internet bezahlbare Waren, wie etwa Kleidung, Reisen oder andere Alltagsartikel, ist lange nichts mehr Neues. Auch die Banken folgen dem Trend und bieten bereits seit längerem den Dienst des Online-Bankings an. Es scheint, als könnte kein Bereich der heutigen Gesellschaft dem Internet entgehen. Die beinahe orts-unabhängige Verwendungsmöglichkeit, die riesige Auswahl und die scheinbare Anonymität sind wohl einige Gründe unter vielen weiteren, die zum großen Erfolg des Internets führten.

Als nächster Schritt werden nun erstmals Systeme entwickelt, welche tatsächlich ausschließlich im Internet und somit online existieren und ablaufen. Vor allem im Bereich der Finanzwelt wird diese Entwicklung forciert. Eine der jüngsten Neuerungen in diesem Bereich ist die Kryptowährung, eine Währung, die nur im Internet existiert und dort als Zahlungsmittel eingesetzt werden kann.

Eine dieser Währungen rückt derzeit durch ihren medienwirksamen Wechselkurs immer mehr ins Blickfeld von AnwenderInnen – Bitcoin. Damit verbunden wird der Begriff der Blockchain, ein System zur lückenlosen Dokumentation der Transaktionen, ebenfalls immer aktueller. Fast täglich hört man von neuen Blockchain-Anwendungen und dass diese auf Grund ihres Aufbaus sicher wären. Doch kann dieses System ohne einer vertrauensgebenden Instanz wirklich die Zukunft der Finanzwelt oder sogar ganz anderer Bereiche bedeuten?

Im Laufe dieser Arbeit möchte ich dieser Frage auf den Grund gehen.

1.2. Problemstellung

Diese Arbeit versucht den detaillierten Aufbau und den zugrundeliegenden Ablauf einer Blockchain zu erläutern. Vor allem soll dabei geklärt werden, wodurch die Vertrauenswürdigkeit entstehen kann und die Sicherheit für die NutzerInnen gewährleistet wird. Im Anschluss daran wird der Frage nachgegangen, welche anderen Bereiche davon profitieren können und welche Vorteile sich daraus ergeben würden.

1.3. Methodisches Vorgehen

Die vorliegende Arbeit lässt beabsichtigt die spekulativen Investitionsmöglichkeiten in Kryptowährungen außen vor und beschäftigt sich mit dem Thema der Blockchain wie folgt:
Im ersten Teil wird der Einstieg zum Thema Blockchain über die wohl bekannteste und vor allem erste Anwendung getätigt – Bitcoin. Dazu wird mit einem kurzen Ablauf der noch jungen Geschichte gestartet. Anschließend wird der Frage auf den Grund gegangen, wer den Grundstein dafür gelegt hat und wie die Wertentwicklung in den letzten Jahren ausgesehen hat. Danach wird beschrieben, wie eine Transaktion im Bitcoin-Netzwerk abläuft und was für die Umsetzung getan werden muss. Dies bietet dann den Übergang dazu, welche Vorgänge direkt in der Blockchain passieren.
Darauf wird etwas genauer eingegangen, denn darin steckt das Detail, welches die Blockchain zu dem macht was es ist – eine lückenlose Dokumentation von zeitlich hintereinander folgenden Zuständen und Aktionen. Danach wird auf den Prozess zur Generierung neuer Bitcoin-Einheiten eingegangen, ein Vorgang, der als Proof of Work bezeichnet und auch Mining genannt wird. Anschließend wird die Entwicklung dieses Minings beschrieben und wie es sich mit der Zeit verändert hat.

Nun folgen die Ausführungen zu Ethereum, einer eigenen Blockchain, die im Vergleich zu Bitcoin einige Erweiterungen enthält. Es wird auf die ebenfalls junge Entstehungsgeschichte geblickt und auf ihren größten Vorteil, die Smart Contracts, genauer eingegangen. Danach werden die unterschiedlichen Accounts, die Kryptowährung Ether und der Unterschied zwischen einer Nachricht und einer Transaktion im

Ethereum-Netzwerk beschrieben. Es wird der Frage nachgegangen, was der Gas-Price und das Gas-Limit ist und ob es Einschränkungen bei den programmierbaren Smart Contracts und Transaktionen gibt. Im Anschluss werden die vier großen Entwicklungsschritte beschrieben und darauf eingegangen in welcher Entwicklungsstufe sich die Ethereum-Blockchain zurzeit befindet. Eine Vorschau auf die noch kommenden Schritte soll die größte Veränderung der zukünftigen Ethereum-Blockchain zeigen – den Proof of Stake. Dieser wird den vorerst letzten Meilenstein in Ethereum einleiten, bei dem vom herkömmlichen, energieaufwändigen Mining, auf eine alternative Validierung der Transaktionen umgestiegen wird. Dabei wird vor allem beschrieben, wie dieser Schritt mit einer sogenannten „Difficulty Bomb“ umgesetzt wird. Danach wird noch kurz auf die Risiken von Kryptowährungen eingegangen.

Im letzten Teil wird ein Überblick zu vergangenen und laufenden Projekten gegeben. Dies zeigt am besten, welches Potential in der Technologie der Blockchain steckt und dass einem findigen Entwicklergeist beinahe keine Grenzen gesetzt sind.

Den Abschluss bildet eine Zusammenfassung zur vorliegenden Arbeit, welche noch einmal die wichtigsten Punkte enthält.

2. Bitcoin

2.1. Entstehung

Bitcoin ist die als erste eingeführte und zurzeit am weitesten verbreitete Kryptowährung, die es gibt. Eine Kryptowährung wird sehr häufig als virtuelle Währung oder digitales Geld beschrieben. Als der Erfinder dieser Währung gilt ein gewisser Satoshi Nakamoto, der im Jahr 2008 ein Werk publizierte, das den Namen „Bitcoin: A Peer-to-Peer Electronic Cash System" trug. Darin wird unter anderem die Möglichkeit beschrieben, elektronische Transaktionen durchzuführen, ohne dass für die Validierung neben der/dem VerkäuferIn und der/dem KäuferIn eine dritte Partei – wie zum Beispiel eine Bank – notwendig ist. Die Sicherheits- und Servicefunktion, welche bei herkömmlichen Überweisungen von einer Bank übernommen werden würde, ist hier einzig und allein durch das dezentral aufgebaute Netzwerk gegeben, in welchem die Überweisungen getätigt werden. Darüber hinaus wurde die dazugehörige Referenz-Software als Open-Source – also für jede/jeden NutzerIn frei zugänglich und einsehbar – veröffentlicht.[1]

Bitcoin beruht, so wie alle anderen Kryptowährungen auch, auf dem Vertrauen der beteiligten NutzerInnen in die Unbestechlichkeit des zu Grunde liegenden Computersystems. Dabei wird die Glaubwürdigkeit einer Notenbank durch ein dezentral aufgebautes System ersetzt. Das bedeutet, dass die getätigten Transaktionen nicht zentral auf einem Rechner oder Server gespeichert und verwaltet, sondern auf jedem im Netzwerk beteiligten Rechner abgelegt werden. Alle im Bitcoin-Netzwerk vorgenommenen Transaktionen werden in dieser dezentral gespeicherten Datenbank so abgelegt, dass eine lückenlos nachvollziehbare und vor allem fälschungssichere Abfolge von Transaktionen dargestellt werden kann. Einzelne Transaktionen werden dabei zu Blöcken zusammengefasst und in einer Kette nacheinander folgend abgebildet. Deshalb spricht man von einer Block-Kette – also einer „Blockchain". Diese Blockchain ist für jede/jeden NutzerIn frei zugänglich und es können alle darin enthaltenen Transaktionen, jedoch ohne personenbezogene Details, angesehen werden – bis hin zur ersten Transaktion im Jänner 2009. Überweisungen, die einmal getätigt wurden, können nicht mehr rückgängig gemacht werden. Sie sind also irreversibel.[2]

[1] Vgl. Weiss/Moutafis (2013), S.1, abgerufen am 01.04.2017
[2] Vgl. Brühl (2017), S.135-142

Neue Bitcoins werden nicht wie herkömmliches Geld durch eine Notenbank generiert, sondern durch ein Anreizsystem ausgeschüttet. Dabei werden NutzerInnen dafür belohnt, Rechenleistung zur Validierung von im Netzwerk getätigten Transaktionen zur Verfügung zu stellen. Mit Anfang Mai 2017 waren in etwa 16,3 Millionen Bitcoins im Umlauf.[3] Die maximal mögliche Anzahl dieser ist begrenzt und die Generierung der Bitcoins wird durch den so genannten Mining-Prozess gesteuert. Mining ist die englische Übersetzung für den im Bergbau verwendeten Begriff „schürfen". Dieses Mining bezeichnet den Vorgang, der zur Verarbeitung der getätigten Transaktionen im Bitcoin-Netzwerk benötigt wird. Alle TeilnehmerInnen, die sich aktiv an dem Mining beteiligen, lassen ihre Rechner eine mathematische Aufgabe lösen. Der Rechner, welcher als erstes das Ergebnis (den so genannten Hash-Wert) berechnet hat, darf einen Datenblock in die Kette von Informationen eintragen. Als Belohnung für die aufgewendete Rechenleistung erhält der/die TeilnehmerIn eine bestimmte Anzahl an Bitcoins.[4]

Die Zahl der durch diesen Mining-Prozess herausgegebenen Bitcoins wird etwa alle vier Jahre halbiert. Seit Beginn im Jänner 2009, bis zum November 2012 wurden 10.500.000 Bitcoins generiert. Pro Datenblock, welcher in diesem Zeitraum freigegeben wurde, wurden 50 Bitcoins ausgegeben. Dabei wurden 210.000 solcher Datenblöcke erzeugt. In den vier darauf folgenden Jahren (bis Juli 2016) halbierte sich die Zahl der neu generierten Bitcoins auf 5.250.000, was einer Summe von insgesamt 15.750.000 Bitcoins entsprach. Dabei wurden ebenfalls 210.000 Datenblöcke erzeugt, jedoch nur eine Belohnung von 25 Bitcoins pro errechnetem Hash-Wert ausbezahlt. Im Juli 2016 wurde nach insgesamt 420.000 Datenblöcken die Belohnung auf 12,5 Bitcoins halbiert. Die nächste Halbierung der Belohnung für das Mining wird im Jahr 2020 erwartet. Die Exponentialfunktion, welche die summierte Ausgabemenge beschreibt, hat einen Endwert dem sich die Summe der ausgegebenen Bitcoins immer langsamer nähert. Dies hat zur Folge, dass sich die maximal mögliche Anzahl der Bitcoins auf 21 Millionen begrenzt. Diese Obergrenze wird voraussichtlich im Jahr 2032 erreicht werden.[5]

[3] Statistik abgerufen online im Internet: https://blockchain.info/de/charts/total-bitcoins, am 07.05.2017
[4] Vgl. Kannenberg (2016), abgerufen am 07.05.2017
[5] Vgl. Weiss/Moutafis (2013), S. 2, abgerufen am 07.05.2017

2.2. Satoshi Nakamoto

Um die Identität des Verfassers des 2008 veröffentlichten Bitcoin-Werkes, also den Erfinder der Kryptowährung Bitcoin – Satoshi Nakamoto – herrschte lange Zeit keine Klarheit. Dass es sich bei dem Namen um ein Pseudonym handeln muss, war jedoch bereits sehr rasch bekannt. Die Veröffentlichung des 2008 publizierten Werkes und das Bitcoin-Protokoll waren sehr lange die einzigen Lebenszeichen dieser (fiktiven) Person. Es wurde schnell vermutet, dass es sich entweder um eine Einzelperson, oder eine Entwicklergruppe handeln muss, welche anonym unter diesem Pseudonym ihre Arbeit publiziert. Die Suche nach der richtigen Identität entbrannte rasch und die Liste der Namen der Personen, welche bereits fälschlicherweise als Satoshi Nakamoto identifiziert wurden, ist dementsprechend lang. Einige Fachmagazine und Online-Portale unternahmen Versuche das große Geheimnis um Satoshi Nakamoto zu lüften. Dies gelang jedoch nicht, ohne dass berechtigte Zweifel bestehen blieben, oder die ausgewählte Person das Ergebnis der Suche dementierte.[6]

Anfang Mai 2016 trat der australische Unternehmer Craig Wright an die Öffentlichkeit und erklärte im Rahmen von 3 Interviews mit BBC, GQ und dem Economist, dass er hinter dem Pseudonym Satoshi Nakamoto stecke und damit der Erfinder von Bitcoin sei. Hinweise hierfür gab es bereits im Dezember 2015. Damals wurde er unter anderem von JournalistInnen von Wired – einem amerikanischen Online-Magazin – als der Ursprung von Bitcoin ausgeforscht. Die Beweise, mit welchen diese Entdeckung begründet wurde, bestanden zum Großteil aus alten E-Mails und Blogeinträgen von Wright und einigen seiner MitarbeiterInnen. Viele ExpertInnen zweifelten damals jedoch an der Stichhaltigkeit dieser Beweise und deshalb auch an der geklärten Identität von Satoshi Nakamoto.[7]

In den oben genannten Interviews im Jahr 2016 bestätigte Wright die Wahrheit seiner Behauptung mit einem kryptografischen Schlüssel. Jede Überweisung in dem Bitcoin-Netzwerk wird durch den/die AbsenderIn mit einem privaten Schlüssel bestätigt, den nur der/die rechtmäßige BesitzerIn kennt. Anhand eines öffentlichen Schlüssels, welcher allen TeilnehmerInnen zur Verfügung steht und ebenfalls fest mit dieser Überweisung verbunden ist, kann dann die Rechtmäßigkeit der Transaktion verifiziert werden. Der kryptografische Schlüssel, welcher von Wright benutzt wurde, gehörte

[6] Vgl. Kühl (2016), abgerufen am 20.04.2017
[7] Vgl. Kühl (2016), abgerufen am 05.05.2017

zu dem am 09.01.2009 erstellten Block mit der Nummer 9. Also der neunten Transaktion, welche im Bitcoin-Netzwerk getätigt wurde. Der Entwickler Hal Finney bestätigte vor seinem Tod, dass er durch diese Transaktion damals zehn Bitcoins von Satoshi Nakamoto überwiesen bekommen hat. Durch den Block 9 wird zwar nicht zweifelsfrei Wright als Erfinder von Bitcoin bestätigt, vielmehr bedeutet es aber dass er ganz zu Beginn von Bitcoin zumindest daran teilgenommen hat. Ein Vergleich anderer Veröffentlichungen von Wright mit dem 2008 publizierten Werk über Bitcoin zeigte keine, oder nur sehr geringe, Übereinstimmungen. Dies erklärte er damit, dass er das ursprüngliche Konzept mit dem Amerikaner Dave Kleinman erstellt hat. Dieser ist jedoch bereits im Jahr 2013 verstorben und konnte deshalb zur Enthüllung der Identität von Satoshi Nakamoto nicht mehr befragt werden. Ein als sehr sicher angesehener Beweis dafür, dass Wright der Erfinder von Bitcoin ist, wäre der private Schlüssel zum ersten Block, also der ersten Transaktion im gesamten Netzwerk. Der Auftraggeber für diese erste Überweisung muss die überwiesenen Bitcoins selbst generiert haben. Dies wiederum konnte nur der Erfinder selbst getan haben. Wright behauptet zwar, auch für diesen Block den Schlüssel zu besitzen, hat dies jedoch nie öffentlich zur Schau gestellt und damit bewiesen.[8]

Ein großer Teil der allerersten Bitcoins wurde nie zum Bezahlen genutzt. Diese Bitcoins wurden in den Anfängen generiert und seitdem nicht mehr bewegt. Durch den Besitz dieser Bitcoins würde Wright beweisen können, dass er der Erfinder sein muss. Es wird angenommen, dass es zu Beginn nur dem/der ErfinderIn selbst möglich war, eine so große Summe an Bitcoins – es dürfte sich dabei um ca. 1,1 Millionen Bitcoins handeln – zu generieren. Wright behauptet zwar, dass er diese Bitcoins besitzt, könnte dies jedoch nicht beweisen, da er sie einem Treuhandfond übergeben habe und zurzeit keinen Zugriff darauf habe. Wright sagt weiter, dass es für ihn, abgesehen vom Block Nummer 9, keiner weiteren Begründung notwendig sei, um sicherzustellen, dass er Satoshi Nakamoto sei.[9]

Eine Person, die von Beginn an bei der Entwicklung von Bitcoin involviert war, ist Gavin Andresen. Der Software-Entwickler hatte in der Anfangszeit Kontakt mit Satoshi Nakamoto – ausschließlich über E-Mail. Als sich der Bitcoin-Erfinder zurückzog, übernahm Andresen das Projekt von ihm und führte es weiter. Andresen überzeugte sich selbst in einem persönlichen Gespräch mit Wright davon, ob dieser dieselbe

[8] Vgl. Schönleben (2016), abgerufen am 12.05.2017
[9] Vgl. Schönleben (2016), abgerufen am 12.05.2017

Person ist, mit der er seit 2009 unter dem Namen Satoshi Nakamoto Kontakt hatte. Nach diesem Treffen stand für ihn fest, dass Craig Wright diese Person ist.[10]

Es wirkt fast so als ob für jeden Beweis, dass Satoshi Nakamoto in Wirklichkeit Craig Wright ist, der dies im Jahr 2016 selbst öffentlich machte, ein Gegenbeweis auftaucht, der zumindest begründete Zweifel daran entstehen lässt. Ob es wirklich Craig Wright alleine zuzuschreiben ist, sich als Satoshi Nakamoto zu bezeichnen, oder ob es im Grunde mehreren Menschen zustehen würde, ist meiner Meinung nach eines der größten Rätsel, welches die Online(-Finanz)-Welt in den letzten Jahren beschäftigt. Vermutlich würde es auf die Onlinewährung Bitcoin – insbesondere den Wechselkurs zu anderen Währungen – einen Einfluss haben, wenn der/die ErfinderIn mit Sicherheit feststehen würde und die Identität von Satoshi Nakamoto geklärt wäre. Was es für die Person(en) bedeuten würde, ist zum jetzigen Zeitpunkt relativ schwer zu beurteilen.

2.3. Wechselkurs

Zu Beginn hatten Bitcoins weder einen eigenen Wert, noch einen Wechselkurs nach dem in andere Währungen umgerechnet werden konnte. Die ersten Wechselkurse, mit denen dies möglich war, wurden erst im Jahr 2010 eingeführt. Dies geschah damals jedoch nur zwischen Einzelpersonen, welche in Internetforen miteinander kommunizierten und selbst die Höhe der Wechselkurse festlegten. Auch heute ist es noch so, dass die Wechselkurse weder von Zentralbanken, noch von der Regierung oder ähnlichen Behörden festgelegt oder kontrolliert werden – dies bedeutet, dass die Währung dezentral verwaltet wird. Der Wert eines Bitcoins wird im Grunde rein von Angebot und Nachfrage auf den vorhandenen Tauschbörsen bestimmt.[11]
Abbildung 1 zeigt die Kursentwicklung des Bitcoin im Vergleich zum Euro mit Stand 25.06.2017 um 16:07 Uhr.

[10] Vgl. Schönleben (2016), abgerufen am 12.05.2017
[11] Vgl. Bosk (2015), abgerufen am 14.04.2017

Abbildung 1 Bitcoin-Euro Chart[12]

In der Abbildung 1 kann man erkennen, dass die Aufzeichnung dieses Wechselkurses im ersten Halbjahr 2013 beginnt. Damals startete der Kurs bei etwa 125€ pro Bitcoin. Gegen Ende des Jahres 2013 erlebte der Bitcoin einen sehr starken Aufschwung. Kurzzeitig stieg der Wert auf über 800€ pro Bitcoin an. Dieser Aufschwung hielt jedoch nicht lange an. Noch vor dem Jahreswechsel auf 2014 sank der Kurs wieder unter 500€, um dann nach einem kurzen Hoch erneut zu sinken.

Im Jahr 2014 pendelte der Kurs zwischen 500€ und 250€ pro Bitcoin.

Zu Beginn des Jahres 2015 bewegte sich der Wechselkurs um 250€, um dann gegen Ende auf ca. 350€ zu steigen. Seit dem Jahr 2016 steigt der Kurs des Bitcoins relativ stetig und teilweise sehr stark an. Anfang 2017 wurde die 1.000€ Marke das erste Mal überschritten. Nach einem kleineren Tiefpunkt bei ca. 750€ im Jänner 2017 stieg der Kurs Anfang März auf seinen damaligen Höchststand bei 1.210,77€. Dies sorgte zu dieser Zeit für besondere Schlagzeilen, da damit auch der Wert je Feinunze Gold übertroffen wurde – dieser befand sich damals bei ca. 1.160€.

Ende März 2017 fiel der Wechselkurs erneut unter die 1.000€ Marke, um danach eine wahrliche Bergauffahrt zu bestreiten. Ab Anfang April bis ca. Mitte Juni stieg der Wechselkurs auf unfassbare 2.500€ je Bitcoin an. Das entspricht einer Steigerung von 1.500€ innerhalb von nur zweieinhalb Monaten. In den darauffolgenden Tagen

[12] Bitcoin-Euro Chart, online im Internet: http://www.finanzen.net/devisen/bitcoin-euro/chart, abgerufen am 25.06.2017 um 16:07 Uhr

bewegte sich der Wechselkurs gegen 2.200€, um sich mit Stand 25.06.2017 bei 2.338,1€ zu befinden.
Zusammengefasst kann gesagt werden, dass der Wechselkurs des Bitcoin nach einem Hoch gegen Ende 2013, einem kleineren Tief in 2015 nun seit Anfang 2017 einen wahren Höhenflug bestreitet. Wie sich der Preis jedoch weiterentwickeln wird, bleibt zum jetzigen Zeitpunkt abzuwarten.
Die Einheit Bitcoin wird mit BTC abgekürzt. Um auch kleinere Beträge überweisen zu können, ist ein Bitcoin auch teilbar. Der kleinste mögliche Betrag wird zu Ehren des Erfinders 1 Satoshi genannt.[13]

2.4. Transaktionsgebühren

Im Bitcoin-Netzwerk gibt es grundsätzlich keine zwingenden Transaktions-Gebühren. Diese können jedoch von der/dem AuftraggeberIn der Überweisung in ihrer Höhe frei festgelegt werden. Die Tatsache, dass die/der AuftraggeberIn der Transaktion die von ihr/ihm zu bezahlende Gebühr für diese Transaktion selber festlegen kann, lässt sehr schnell die Frage aufkommen, warum solch eine Transaktions-Gebühr überhaupt festgelegt werden sollte. Die Gebühren, welche für die Transaktionen bezahlt werden, kommen der/dem MinerIn zu Gute – also der Person, welche einen Block verifiziert und die Transaktionen darin für korrekt erklärt. Dazu jedoch später mehr. Wenn nun eine Transaktion verifiziert wird, die Gebühren enthält, geht ein Teil dieser Gebühr an die/den MinerIn über. Den MinerInnen steht es grundsätzlich frei, sich die Transaktionen auszusuchen, welche in ihren Block aufgenommen werden. Folglich wird er/sie eher Transaktionen auswählen, welche einen Profit bringen. Dies kann bedeuten, dass eine Transaktion, die keine Gebühren enthält, zum Teil verhältnismäßig lange auf eine Bestätigung warten muss.[14]
Daraus könnte man schließen, wenn einer Person die getätigte Transaktion, oder besser gesagt die Geschwindigkeit, mit der diese Transaktion bearbeitet wird, etwas wert ist, zahlt diese Person auch gerne einen (verhältnismäßig kleinen) Betrag an Gebühren. Ich denke, dass dies durchaus legitim ist, da bei so ziemlich allen Geldgeschäften, eine Gebühr zu zahlen ist. Außer natürlich bei der persönlichen, physi-

[13] Vgl. Miller (2017), online abgerufen am 20.06.2017
[14] Vgl. Scheurer (2017), online abgerufen am 15.06.2017

schen Übergabe von Bargeld. Das ist auch nicht weiter verwunderlich, da dort das Risiko und der Aufwand der Geldübergabe, für welches eine solche Gebühr im Normalfall eingehoben wird, direkt bei den beteiligten Personen liegt und von keinem Dritten übernommen wird.

2.5. Ablauf einer Bitcoin Transaktion

Um aktiv am Bitcoin-Netzwerk teilnehmen zu können, wird eine Software benötigt, welche Wallet (englisch für Geldbörse) genannt wird. Diese Software kann – wie der Name bereits sagt – sehr gut mit einer echten Geldbörse verglichen werden. Mit Hilfe der Wallet Software können die eigenen Bitcoins verwaltet, und Transaktionen umgesetzt werden. Des Weiteren sind sie durch ein Passwort geschützt und sollen so auch den Diebstahl der Bitcoins unterbinden. Wallets sind anonym und es werden bei den meisten AnbieterInnen keine persönlichen Daten gespeichert. Mittlerweile gibt es bereits viele solcher Wallet-Lösungen. Sehr gängig sind zum Beispiel „Bitcoin Knots“, „MultiBit HD“ und „Armory“ – um nur einige davon zu nennen. Grundsätzlich bauen sie jedoch alle auf der Bitcoin-Referenz-Software auf, welche die Transaktionen im Bitcoin-Netzwerk ermöglicht. Um die Sicherheit der eigenen Bitcoins zu erhöhen und missbräuchliche Zugriffe zu erschweren, ist es sehr ratsam, sein Bitcoin-Vermögen nicht in einem einzigen Wallet zu speichern, sondern in mehrere unterschiedliche aufzuteilen. In „Abbildung 2“ ist der grundsätzliche Ablauf einer Bitcoin-Transaktion abgebildet. Die drei Schritte, welche für eine Bitcoin-Transaktion notwendig sind, werden nachfolgend beschrieben.[15]

[15] Vgl. Keßler (2015), abgerufen am 26.05.2017

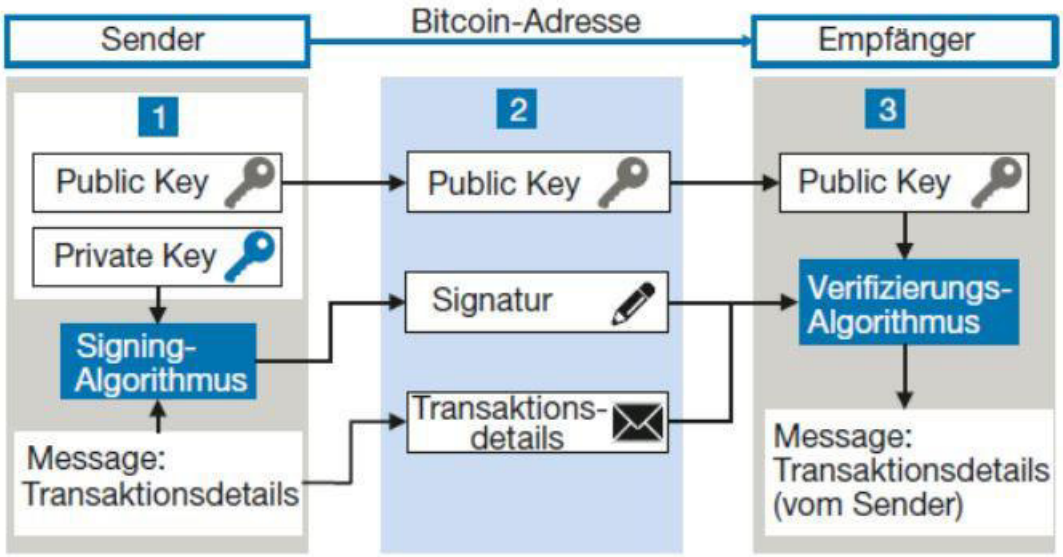

Abbildung 2 Ablauf einer Bitcoin Transaktion[16]

1. Im ersten Schritt wird von der/dem SenderIn der Transaktion ein so genanntes Schlüsselpaar erstellt. Dieses Schlüsselpaar ist nur für genau diese eine Überweisung gültig und besteht aus einem privaten (Private Key) und einem öffentlichen Schlüssel (Public Key). Ein Schlüssel ist eine Abfolge von Nummern und Buchstaben und jeder Schlüssel ist im Netzwerk einzigartig. Mit Hilfe des Private Keys kann der/die SenderIn eine verschlüsselte Signatur für die Transaktion erstellen. Der Public Key dient der/dem EmpfängerIn und dem gesamten Bitcoin-Netzwerk dazu, die Rechtmäßigkeit der durch die/den SenderIn eingeleiteten Transaktion bestätigen zu können. Anders formuliert ob die/der SenderIn die Bitcoins, welche sie/er überweisen möchte, auch tatsächlich besitzt. Um Bitcoins übertragen zu können, braucht man neben dem Wallet auch die Bitcoin-Adresse der Empfängerin/des Empfängers. Dies ist eine bis zu 34-stellige Reihenfolge aus Zahlen und Buchstaben, welche mit Hilfe eines kryptographischen Verfahrens erstellt wird. Eine Bitcoin-Adresse kann zum Beispiel so aussehen: 12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX[17]. Um die Überweisungen im Bitcoin-Netzwerk noch sicherer zu gestalten, wird jede Bitcoin-Adresse normalerweise für nur eine einzige Transaktion verwendet und danach wieder verworfen.[18] [19]

[16] Ablauf einer Bitcoin Transaktion, Brühl (2017), S.136
[17] An diese Adresse wurden unter anderem am 09.01.2009 50 Bitcoins überwiesen – die Transaktion des Blocks mit der Nummer 1
[18] Speziell in der Anfangszeit wurde dies noch nicht so praktiziert und eine Adresse für mehrere Transaktionen verwendet.
[19] Vgl. Brühl (2017), S.135f

2. Danach wird von der/dem SenderIn eine Transaktion erstellt, welche die Informationen in einer festgelegten Reihenfolge enthält. Darin sind zum Beispiel die Zieladresse und der Betrag der Überweisung enthalten. Darüber hinaus werden Transaktionsreferenzen gesendet, welche die genauen Informationen über die enthaltenen Bitcoins wiedergeben. Damit kann also zweifelsfrei geklärt werden, ob die versendeten Bitcoins auch wirklich rechtmäßig im Besitz der Senderin/des Senders waren. Aus den vorhandenen Daten wird mittels des Private Keys und unter Verwendung eines Signaturalgorithmus die oben erwähnte Signatur erstellt. Diese wird anschließend zusammen mit dem Public Key an die/den EmpfängerIn der Transaktion – und an das gesamte Netzwerk – gesendet. [20]

3. Im letzten Schritt wird durch die/den EmpfängerIn unter Zuhilfenahme des eingegangenen Public Keys die Transaktion verifiziert. Das bedeutet sie/er kann damit prüfen, ob der vereinbarte Betrag in ihrem/seinem Wallet angekommen ist. Diese Verifizierung kann nur dann erfolgen, wenn das Schlüsselpaar aus Private Key und Public Key zueinander gehören und die Signatur durch die/den SenderIn verschlüsselt wurde. Die/Der EmpfängerIn ist nach dieser Prüfung darüber im Klaren, ob sie/er nun die/der rechtmäßige BesitzerIn der Bitcoins ist. [21]

2.6. Bitcoin Transaktion – Vorgänge in der Blockchain

Die zuvor beschriebene Transaktion, wird wie erwähnt von der/dem SenderIn nicht nur an die/den EmpfängerIn übermittelt, sondern an alle TeilnehmerInnen, welche sich im Bitcoin-Netzwerk befinden. Es hat zwar den Anschein, dass diese in erster Linie keinen Nutzen aus dieser Information ziehen, jedoch ist dies für die Funktionalität des Systems unumgänglich.

[20] Vgl. Brühl (2017), S.135f
[21] Vgl. Brühl (2017), S.135f

Die Blockchain baut darauf auf, dass alle TeilnehmerInnen versuchen, getätigte Transaktionen dezentral – das heißt auf ihrem eigenen Rechner – zu überprüfen und diese anschließend zu einem neuen Block zusammenzufassen, an das gesamte Netzwerk zu versenden und in die Blockchain einzugliedern. Die Aufgabe der Blockchain, alle Transaktionen zu dokumentieren, ist mit einem Hauptbuch von Banktransaktionen vergleichbar. Deshalb spricht man bei dieser dezentralen Speicherung der Daten auch von einem Distributed Ledger. Frei übersetzt bedeutet das ein „verteiltes Hauptbuch“. Durch diese stetige Verifizierung und Bildung neuer Blöcke wird sichergestellt, dass alle TeilnehmerInnen in der Blockchain auf demselben Stand sind und dadurch keine Unklarheit bezüglich der getätigten Überweisungen herrscht. Um dies zu erreichen, beinhaltet die Blockchain hinter dem Bitcoin-Netzwerk eine Art Anreizsystem, welches NutzerInnen belohnt, die einen neuen Block erstellen, verifizieren und chronologisch in die Kette eingliedern. Dieses Anreizsystem ist das Mining. Damit ein neuer Block erstellt werden kann, muss im Zuge des Mining-Prozesses der Hash-Wert berechnet werden. Dies ist ein Wert, der einen bestimmten Zielwert abbildet, welcher im Zuge der Berechnung unterschritten werden muss.[22]

Der Hash-Wert eines Blocks ergibt sich zum einen aus den Verschlüsselungswerten der in dem Block enthaltenen Transaktionen und zum anderen aus einer Referenz zu dem vorangegangenen Block. So ergibt sich aus den chronologisch folgenden Blöcken, welche auch immer zu ihren vorhergehenden eine direkte Verbindung haben, die lineare Kette der Blockchain. Die Hash-Werte werden im Falle der Kryptowährung Bitcoin mit der Funktion SHA 256 erstellt. Dies ist eine von vielen Hash-Funktionen, die für solche Anwendungen sehr beliebt ist. Damit werden beliebige Zeichenfolgen nach einem genau vordefinierten Ablauf so miteinander verknüpft und zusammengeführt, dass am Ende wieder eine Zeichenfolge mit festgelegter Länge entsteht. Wird nur ein einziger Input-Wert dieser Funktion verändert – zum Beispiel die Zieladresse oder der Betrag einer Transaktion – ändert sich der ausgegebene Hash-Wert so sehr, dass dieser nicht vorhergesagt werden kann. Dadurch wird eine unbemerkte Änderung einer Transaktion praktisch unmöglich gemacht. Wird nur ein kleiner Teil eines Blocks verändert, verändert sich damit die gesamte nachfolgende Blockchain.[23]

[22] Vgl. Brühl (2017), S.136f
[23] Vgl. Brühl (2017), S.137

Die in der Blockchain abgespeicherten Blöcke enthalten unterschiedliche Bereiche, welche fest definiert sind. In einem dieser Bereiche – dem Transaktionsteil – werden die Transaktionen abgespeichert. Es ist nicht genau festgelegt, wie viele Transaktionen in einem Block abgelegt werden. Das kommt allein auf die Anzahl der von den NutzerInnen in dieser Zeit getätigten Transaktionen an. Von den gespeicherten Transaktionen werden zuerst Kopien erstellt. Diese Kopien werden dann mit der zuvor beschriebenen Funktion so lange paarweise verschlüsselt – also „gehasht" – bis nur mehr ein einziger Hash-Wert übrig bleibt. Dieser Wert bildet dann über die Funktion alle Transaktionen ab, welche in dem Block gespeichert sind. Dieser Hash-Wert der gesamten Überweisungen wird auch „Merkle Root" genannt. Die Merkle Root wird dann im Blockheader abgelegt und gespeichert. Den Blockheader kann man sich als definierten Bereich im Block vorstellen, in dem die wichtigsten Informationen separat abgelegt werden. Zu diesen Informationen zählt auch der Hash-Wert des vorhergehenden Blocks. Dieser Wert ist wie bereits erwähnt einzigartig und verknüpft den aktuellen Block mit dem chronologisch zuvorkommenden. Abgesehen von der Merkle Root und dem Hash-Wert des vorhergehenden Blocks, enthält der Blockheader auch noch ein Feld das mit NONCE (Number Only Used Once) bezeichnet wird. Aus diesen drei Werten wird nochmals mit Hilfe der Hash-Funktion der Hash-Wert des aktuellen Blocks generiert.[24]

[24] Vgl. Brühl (2017), S.137

In der nachfolgenden Abbildung ist der vereinfachte Aufbau einer solchen Blockchain dargestellt.

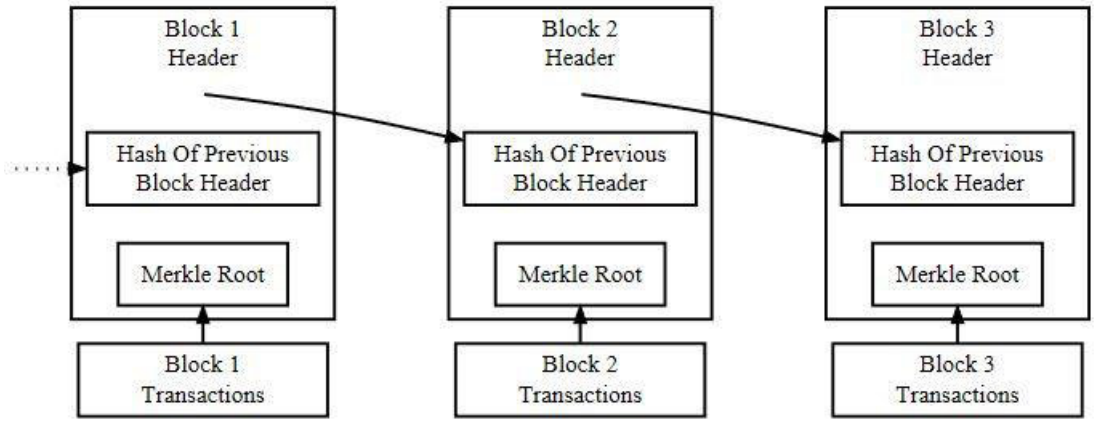

Abbildung 3 Aufbau der Bitcoin-Blockchain[25]

Mit dem NONCE-Feld beschäftigt sich der eigentliche Aufwand des Mining-Prozesses. Es ist die Aufgabe der MinerInnen, für das Feld eine Zahl zu finden, welche die nachfolgende Hash-Funktion eine Zeichenfolge generieren lässt, die den geforderten Hash-Wert unterschreitet – darin liegt die Schwierigkeit. Dazu bedienen sie sich verschiedener Suchalgorithmen, welche ihnen Zufallszahlen für das NONCE-Feld generieren. Es ist nicht gesagt, dass eine möglichst niedrige Zahl für das NONCE-Feld auch einen ebenso geringen Hash-Wert generieren wird. Dies macht den Mining-Prozess so schwierig und erfordert eine hohe Rechenleistung, um diese Zahl möglichst schnell finden zu können. Wie der Name bereits sagt, können NONCE nur einmal verwendet werden. Dies ist eine weitere Maßnahme, um das Bitcoin-Netzwerk fälschungssicherer zu machen. Über den geforderten Hash-Wert, welcher unterschritten werden muss, kann die Schwierigkeit und damit auch die Zeit festgelegt werden, die benötigt wird, um einen neuen Block zu generieren. Dieser Schwierigkeitsgrad wird durch die Bitcoin-Software und den zu Grunde liegenden Algorithmus immer wieder angepasst und so festgelegt, dass in etwa alle zehn Minuten ein neuer Block generiert wird. Die Zeit in der ein neuer Block erzeugt wird hängt einzig und allein von der Rechenleistung des gesamten Netzwerks ab. Wird sehr viel Mi-

[25] Aufbau der Bitcoin-Blockchain, online im Internet: https://bitcoin.org/en/developer-guide#block-chain, abgerufen am 25.06.2017

ning mit jeweils einer sehr hohen Rechenleistung betrieben, wird die Zeit, bis ein passender Hash-Wert gefunden wird, eher geringer ausfallen. Dann wird die Schwierigkeit Schritt für Schritt ein wenig erhöht. Würden nun einige MinerInnen ihre Arbeit beenden und den anderen diese Aufgabe überlassen, würde die im Netzwerk vorhandene Rechenleistung sinken und die Zeit bis zur nächsten Generierung eines Blocks würde steigen. Falls diese Situation eintreten würde, wäre eine Verminderung der Schwierigkeit die Folge.[26]

Wird nun von einer/einem MinerIn ein Hash-Wert für den aktuellen Block gefunden, welcher den Anforderungen entspricht, muss dies noch allen anderen TeilnehmerInnen mitgeteilt werden. Zuerst wird der Block in die Kette der Minerin/des Miners eingetragen, die/der ihn generiert hat. Danach wird dieser neu generierte Block, welcher auch alle zu verifizierenden Transaktionen beinhaltet, an das gesamte Netzwerk versendet. Jede/r TeilnehmerIn, die/der solch einen neuen Block erhält, prüft und verifiziert ebenfalls sofort mit Hilfe der empfangenen Public Keys, ob die enthaltenen Transaktionen in Ordnung sind, der geforderte Hash-Wert unterschritten wurde und somit der empfangene Block als rechtmäßig angesehen werden kann und wiederum in die dezentral gespeicherte Blockchain gespeichert wird. Dieser Ablauf, dass ein neuer Block zuerst durch das gesamte Netzwerk gesendet werden muss, um dann verifiziert zu werden, benötigt etwas Zeit. Falls es nun dazu kommen sollte, dass eine/ein konkurrierende/r MinerIn fast zur selben Zeit ebenfalls einen gültigen Block generiert hat, kann die Situation entstehen, dass zwei gültige Blöcke im Umlauf sind. Bildlich gesehen würde dann bei der Blockchain eine Gabelung entstehen. Da dieser Zustand aber per Definition der Blockchain nicht möglich sein darf, beseitigt sich diese Gabelung sehr schnell selbst. Das Netzwerk einigt sich nämlich stets auf den längsten Block. Wird ein Block von der Mehrheit der TeilnehmerInnen im Netzwerk bestätigt, wird er fix in die Blockchain integriert und der Mining-Prozess für den nächsten Block beginnt. Durch diesen Ablauf entsteht mit der Blockchain ein lückenloses und unveränderbares Protokoll der getätigten Transaktionen im Bitcoin-Netzwerk. Es stellt eine Auflistung von Eigentums- und Übertragungsbeziehungen der Bitcoins dar. Das bedeutet, dass man jeden erhaltenen Bitcoin bis zu seinem Ursprung zurückverfolgen kann. Jeder Block und damit auch jede Transaktion ist öffentlich zugänglich. Einige enthaltene, verschlüsselte Transaktionsdetails sind jedoch ohne dem passenden Private Key nicht einsehbar und ermöglichen deshalb ein ge-

[26] Vgl. Brühl (2017), S.137

wisses Maß an Privatsphäre beziehungsweise eine Vertraulichkeit zwischen den beteiligten Parteien.[27]

Wie bereits oben erwähnt, wirkt sich die Verkettung beginnend bei den einzelnen Transaktionen bis hin zu jedem nachfolgenden Block sehr positiv auf die Sicherheit des gesamten Systems aus. Eine Änderung eines noch so kleinen Details einer Transaktion führt zu einer Änderung des gesamten Blocks und dahingehend auch zu einer Änderung aller nachfolgenden Blöcke und des gesamten nachfolgenden Netzwerks. Dies macht eine missbräuchliche Veränderung, die im Nachhinein geschieht, sehr schnell und einfach erkennbar. Wie oben beschrieben wird ein Block als gültig angesehen, wenn mehr als die Hälfte der im Netzwerk befindlichen TeilnehmerInnen bestätigen, dass dieser Block korrekt ist. Daraus lässt sich schließen, dass ein/e HackerIn über mehr als 50% der im Netzwerk vorhandenen Rechenleistung verfügen müsste. Nur so wäre es möglich, einen eigenen, veränderten Block einzubringen und diesen für alle NutzerInnen bereits zuvor als gültig zu erklären. Eine so hohe Rechenleistung ist zwar mit extremen Aufwand und auch mit sehr hohen Kosten verbunden, wäre theoretisch jedoch möglich.[28]

2.7. Die Entwicklung des Minings

Als die ersten Bitcoin-Transaktionen Anfang 2009 getätigt wurden, war es noch relativ einfach, mit einem handelsüblichen Rechner Mining zu betreiben. Zum einen waren im gesamten Netzwerk noch wenige Personen beteiligt und zum anderen war die Schwierigkeit der Berechnung des Hash-Wertes auch noch dementsprechend niedrig. Die Möglichkeit für einzelne Personen sich aktiv in dieser Form am Mining zu beteiligen war noch einige Monate gegeben. Je bekannter Bitcoin wurde, desto mehr Personen waren mit ihren Rechnern in dem Netzwerk vertreten. Dadurch stieg die gesamt vorhandene Rechenleistung und der Schwierigkeitsgrad nahm dementsprechend zu. Daraus, und aus der Tatsache, dass immer mehr Personen Mining betrieben, resultierte, dass es für Einzelpersonen immer schwieriger wurde, einen Block zu

[27] Vgl. Brühl (2017), S.137
[28] Vgl. Brühl (2017), S.137

erstellen, diesen in die Blockchain einzugliedern und dafür eine Belohnung in Form von Bitcoins zu erhalten. Es wurde mit der Zeit immer geläufiger, dass eigens für das Mining spezialisierte Hardware – sei es durch Aufrüsten eines Rechners, oder durch die Anschaffung eines so genannten Miners – einzelne Personen sich selbst einen Vorteil gegenüber anderen im Bitcoin-Netzwerk verschafften. Ein Miner ist eine speziell für das Mining entwickelte Hardware. Diese wird meist über eine serielle Schnittstelle mit dem Rechner verbunden. Die hohe Rechenleistung, welche beim Mining notwendig ist, wird nachfolgend von diesem Miner übernommen. Dafür ist meist eine externe Stromversorgung notwendig, um den Energiebedarf zu decken. Dieser Energiebedarf ist es auch, der die zum Teil hohen Kosten des Minings entstehen lässt. Mit der Zeit wurde es aber auch für die Personen mit spezialisierter Hardware immer schwieriger und dadurch seltener, einen neuen Block zu erzeugen und damit neu generierte Bitcoins zu bekommen.[29]

Allmählich bewegte sich das Bitcoin-Netzwerk in eine neue Richtung. Da es bereits für eine große Anzahl an TeilnehmerInnen beinahe unmöglich wurde, selbst durch Mining Bitcoins zu erhalten, entstand eine Zentralisierung der Rechenleistungen. Dies resultierte aus Zusammenschlüssen, welche die MinerInnen eingingen, um sich dadurch einen Vorteil im gesamten System zu verschaffen. Die Rechenleistungen wurden gebündelt und so versuchten sie gemeinsam, neue Blöcke zu generieren und dadurch als eine große Einheit am Mining-Prozess teilzunehmen. Solche Zusammenschlüsse werden Mining-Pools genannt. Diese Pools erhöhen für die/den Einzelnen die Chance an einem erfolgreichen Mining-Prozess teilzunehmen und so zumindest einen kleinen Teil der Belohnung zu erhalten. Mit dieser zunehmenden Zentralisierung und stetigen Erhöhung der Rechenleistung wird es immer schwieriger neu in den Mining-Prozess einzusteigen. Die bereits im Bitcoin-Netzwerk etablierten MinerInnen haben oftmals die Kosten für ihre Hardware durch die erhaltenen Bitcoins amortisiert. Von den nun erhaltenen Bitcoins müssen also rein die Stromkosten bezahlt werden. Dadurch bleibt es für diese MinerInnen meist noch rentabel, auch wenn sie im Laufe der Zeit weniger oft Bitcoins erhalten oder die für einen Block ausgeschüttete Menge an Bitcoins sinkt.[30]

Wenn sich neue MinerInnen nur sehr schwer im Netzwerk platzieren können, kann dies zur Folge haben, dass die eingesessenen und vor allem größeren MinerInnen

[29] Vgl. Obermeier (2017), online abgerufen am 27.05.2017
[30] Vgl. Obermeier (2017), online abgerufen am 27.05.2017

immer mehr Einfluss auf das gesamte Netzwerk bekommen, da ihre anteilige Rechenleistung steigt. Dies könnte in weiterer Folge dazu führen, dass die Gefahr einer missbräuchlichen Verwendung steigt.[31]

3. Ethereum

3.1. Entstehung

Die im Jahr 2008 veröffentlichte, von Satoshi Nakamoto beschriebene Funktionsweise von Bitcoin, beinhaltet zwei Konzepte, welche zum damaligen Zeitpunkt völlig neu waren. Zum einen die Onlinewährung Bitcoin. Sie ist, wie bereits im Kapitel 2 beschrieben, eine Kryptowährung, welche bei ihrer Einführung im Jahr 2009 keinen realen Wert hatte und auch von keiner zwischengeschalteten, zentralen Instanz wie einer Bank herausgegeben oder verwaltet wird. Ihr Wechselkurs wird allein von Angebot und Nachfrage gesteuert und auf dafür vorgesehenen Online-Plattformen gehandelt. Das zweite, neue Konzept, welches veröffentlicht wurde, steckt hinter den Bitcoins – die bereits im Kapitel 2.6 erläuterte Funktionsweise der Blockchain. Durch ihren festgelegten Ablauf, bei dem Transaktionen im Bitcoin Netzwerk erstellt, verifiziert und abgespeichert werden, war es erstmals möglich mit Sicherheit festzustellen, welche Transaktion zuerst und damit gültig war, wodurch das Problem einer mehrfachen Verwendung derselben Geldeinheiten gelöst wurde. Des Weiteren war (und ist) es auch nicht möglich, diese Kryptowährung aus dem Nichts selbst zu erzeugen, da die Bitcoins nur über den Mining-Prozess generiert und nachvollziehbar – und vor allem dokumentiert – ausgegeben werden. Darüber hinaus war durch die lückenlose Dokumentation in diesem so genannten Distributed Ledger – frei übersetzt dem „verteilten Hauptbuch“ – eine Verifizierung des Eigentums der überwiesenen Bitcoins möglich. In diesem Hauptbuch sind, wie bereits erwähnt, alle Transaktionen bis hin zur ersten Überweisung im Jänner 2009 gespeichert. Bis zu diesem Zeitpunkt war solch eine Lösung zwar intensiv gesucht, aber nicht gefunden worden. Vitalik Buterin erkannte zu Beginn des Jahres 2014 immer mehr die große Errungenschaft in der Unverfälschbarkeit der dezentral aufgebauten Blockchain. Eine im Jahr 2014 bereits

[31] Vgl. Valfells/Egilsson (2016), S.1674-1678

existierende, alternative Verwendung der Bitcoin-Blockchain, war das sogenannte Konzept der Colored Coins. Dabei handelte es sich zuerst jedoch ebenfalls um ein reines Finanzinstrument, welches benutzerdefinierte Währungen und ihre Zugehörigkeit zu Adressen der Blockchain – und damit in weiterer Folge zu Personen – dokumentierte. Diese Colored Coins wurden als digitale Wertanlagen verwendet und erlaubten im Gegensatz zu den reinen Transaktionen der Bitcoins bereits eine weit höhere Möglichkeit der benutzerdefinierten Gestaltung. Durch diese Möglichkeit entstand aus den Colored Coins nach kurzer Zeit auch die Anwendung, das Eigentumsrecht verschiedener Dinge wie etwa Fahrzeuge oder sogar den Identitätsnachweis zur eigenen Person über die Bitcoin-Blockchain zu erbringen. Damit wäre es zum Beispiel einem Unternehmen, welches Auto-Vermietung betreibt, möglich gewesen, jedem Auto, das sie besitzen, einen eigenen Colored Coin zuzuweisen. Bei der Anmietung eines solchen Fahrzeugs durch einen Kunden, könnte dieser den zu diesem speziellen Wagen zugehörigen Colored Coin in seine Wallet-Software überwiesen und durch den Private Key des Vermieters die Erlaubnis erteilt bekommen, das Fahrzeug zu benutzen. Die genannten Anwendungen basierten jedoch bis zu diesem Zeitpunkt allein auf der Bitcoin-Technologie. Dies war auch weiter nicht verwunderlich. Wenn eine neue Anwendung kreiert wird, wird zuerst versucht die gewünschten Aufgaben mit vorhandenen Mitteln umzusetzen. Es besteht keine Notwendigkeit für die Entwicklung einer neuen Technologie oder eines neuen Protokolls, wenn alles was gefordert wird, mit bestehenden Protokollen und dergleichen abgearbeitet werden kann. Als die Nachfrage nach immer komplexeren Möglichkeiten immer stärker wurde, erkannte Vitalik Buterin, dass die Grenzen der Bitcoin-Blockchain für weitere Anwendungen bald erreicht waren. Buterin sah das Potential, welches in der Blockchain steckte und wusste, dass er es weiter nutzen konnte. [32]

Sein veröffentlichtes Konzept beinhaltete die Möglichkeit alle nur erdenklichen Sachverhalte, welche bisher eine übergeordnete Instanz erforderten, in einer Blockchain abzubilden und dadurch für alle Beteiligten sicher und vertrauenswürdig zu machen. Er beabsichtigte die durch die Blockchain entstandenen Innovationen zu nutzen, seine Ideen einzubringen und daraus ein System zu erschaffen, das praktisch keine Grenzen setzen würde. Diese Uneingeschränktheit der NutzerInnen sollte dadurch möglich gemacht werden, dass sie beliebig komplexe Verträge, Beziehungen und

[32] Vgl. Buterin (2014), online abgerufen am 04.06.2017

Anweisungen selbst programmieren konnten und alles über die Blockchain abgehandelt werden würde.[33]

Gleichzeitig zum ersten Artikel über Ethereum, der von Vitalik Buterin veröffentlicht wurde, publizierte er ein umfangreicheres White Paper, in welchem er die Funktionsweise der Ethereum Blockchain etwas präziser beschrieben hat. Darin fand sich unter anderem ein noch junger geschichtlicher Rückblick zum Thema Bitcoin und Blockchain. Es wurde das Mining, Merkle Roots und auch bereits bestehende, alternative Blockchain Anwendungen dargestellt. Alle jedoch, wie bereits erwähnt, noch mit der Bitcoin-Blockchain umgesetzt. Im nächsten Abschnitt dieses White Papers wurde Ethereum vorgestellt. Das Ziel von Ethereum sei es, den vielen vorhandenen Konzepten von Blockchain-Anwendungen eine gemeinsame Bühne zu geben. Dabei soll es EntwicklerInnen ermöglicht werden, eigene dezentrale Anwendungen zu erstellen, welche den Konsens-Grundsatz der Blockchain verfolgen. Das Hauptaugenmerk sollte dabei auf der Skalierbarkeit, der Standardisierung und der umfangreichen Möglichkeit, Erweiterungen zu erstellen, liegen. Diese Vorgaben würden ermöglicht werden, indem eine eigene Programmiersprache zur Verfügung gestellt werden würde. Diese Programmiersprache sollte möglichst einfach gestaltet sein. Darüber hinaus sollte mit Hilfe eines eigenen Compilers die Möglichkeit bestehen, Programmzeilen aus anderen Programmiersprachen in einen Ethereum-Code umzuwandeln. Der Compiler hat dabei, einfach betrachtet, die Aufgabe eines Übersetzers. Die ProgrammiererInnen haben so die Möglichkeit, ihre dezentralen Anwendungen selbst zu gestalten und in der Ethereum-Blockchain laufen zu lassen.[34]

3.2. Accounts in Ethereum

Um im Ethereum-Netzwerk auftreten zu können, benötigt man einen Account. Es werden zwei Arten von Accounts unterschieden. Zum einen gibt es externe Accounts. Diese Accounts werden von Personen betreut sowie gesteuert und besitzen einen Private Key. Sie haben keinen Code hinterlegt und können nur mit dem Private

[33] Vgl. Buterin (2014), online abgerufen am 04.06.2017
[34] Vgl. Buterin (2014), S. 13, White Paper online abgerufen am 04.06.2017

Key bedient werden. Mit so einem externen Account ist es im Ethereum-Netzwerk möglich, Nachrichten zu senden. Eine Nachricht kann gesendet werden, indem sie von einem externen Account erstellt und mit Hilfe des dazugehörigen Private Keys unterzeichnet wird. Die zweite Art von Accounts sind die „Contract Accounts“. Frei übersetzt bedeutet das Vertragskonto. Bei so einem Vertragskonto ist in einem definierten Bereich des Accounts ein Programmcode hinterlegt. In gewisser Weise also ein Vertrag. Dieser Code wird immer dann ausgeführt, wenn das Vertragskonto eine Nachricht erhält. Ein Ethereum-Account besteht immer aus einer 20 Byte großen Adresse und beinhaltet folgende vier Felder. Ein nonce Feld. Dieses ist vergleichbar mit dem NONCE Feld eines Bitcoin-Blocks. Es beinhaltet ebenfalls eine Nummer, welche nur einmal verwendet werden kann und garantiert, dass ein Account einzigartig bleibt. Das nächste Feld stellt den Speicher dar. Darin können Informationen abgelegt werden. Dieser Speicher ist beim Erstellen des Accounts standardmäßig leer. Das nächste Feld kann einen Contract-Code, also einen Vertrags-Code, enthalten. Dieser Code ist nicht zwingend erforderlich. Sein Dasein hängt wie oben erwähnt davon ab, um welche Art von Account es sich handelt. Gemeint ist dabei ein Programmcode, mit welchem zum Beispiel Transaktionen oder Nachrichten freigegeben oder andere Aktionen eingeleitet werden. Das letzte Feld beinhaltet den aktuellen Kontostand des Accounts. Es gibt an wie viel Ether – die Währung des Ethereum Netzwerks – sich gerade auf dem Konto des Accounts befinden. [35]

3.3. Der Treibstoff Ether

Ether ist wie Bitcoin ebenfalls eine Kryptowährung. Der Ausgabe der ersten Einheiten dieser Währung ist ein Crowdfunding-Prozess vorangegangen. Dieser Crowdfunding-Prozess ermöglichte es allen Personen, die sich für dieses neue Projekt interessierten, durch die Finanzierung des Projekts mit einem Bitcoin eine bestimmte Anzahl an Ether zu bekommen. Die Anzahl an Ether war von dem Zeitpunkt der Investition abhängig. So wurden zum Beispiel am Beginn des Crowdfunding-Prozesses 2.000 Ether pro investiertem Bitcoin zugesichert. Die Anzahl an Ether, welche aus-

[35] Vgl. Buterin (2014), S. 13, White Paper online abgerufen am 04.06.2017

gegeben wurde, verringerte sich nach dem Start jeden Tag um genau 20 Ether. Das Minimum an Ether, das während des Crowdfundings für einen Bitcoin zu bekommen war, wurde auf 1.000 begrenzt. Dieses Minimum wurde nach 50 Tagen erreicht. Auf diese Weise konnten innerhalb der 60 Tage 60.102.216 Ether an die InvestorInnen verteilt werden. Dabei wurden 31.591 Bitcoins für die Entwicklung der Ethereum-Blockchain gesammelt. Die Belohnung für den durch das Mining entstandenen Aufwand beträgt pro generiertem Block 5 Ether. Dazu kommen noch die durch die/den SenderIn bezahlten Transaktionsgebühren, die ebenfalls der/dem MinerIn zugehen. Diese gleichbleibende Belohnung der Block-Generierung hat zur Folge, dass Ether eine inflationäre Kryptowährung ist. Das bedeutet, dass der Wert dieser Währung im Laufe der Zeit tendenziell ständig abnimmt. Dies lässt sich darauf zurückführen, dass auf lange Sicht immer mehr Ether in Umlauf gebracht werden und so die gesamte Menge an verfügbaren Ether ständig steigt. Die Höhe der Inflation nimmt dabei jedoch jedes Jahr ab, da das Verhältnis der neu ausgegebenen Ether zu der Gesamtzahl immer kleiner wird. Die Inflation geht also gegen Null, erreicht diesen Wert theoretisch jedoch niemals. Eine Tatsache, welche dieser Inflation teilweise entgegenwirkt und bei anderen Währungen genauso auftritt, ist der sorglose Umgang mit Ether. Das bedeutet, dass Ether auf Konten einfach „vergessen“ wird und somit nicht mehr im Umlauf ist. Darüber hinaus ist es auch möglich, dass durch das Ableben der/des Kontoinhaberin/s, Ether auf dem Konto „eingefroren“ ist und nicht mehr verwendet werden kann. Dies ist vor allem der Fall, wenn der Nachlass der/des Kontoinhaberin/s – bis hin zu seinem Ethereum-Konto – nicht geregelt ist und die Passwörter sowie der Private Key nicht bekannt sind.[36]

Zum jetzigen Zeitpunkt beträgt die durchschnittliche Zeit zwischen zwei Blöcken in etwa 12-15 Sekunden.[37] Das bedeutet, dass alle 12-15 Sekunden ein neuer Block generiert und in die Ethereum-Blockchain eingegliedert wird. Alle 12-15 Sekunden werden also 5 Ether generiert und an eine/einen MinerIn ausgeschüttet. Das entspricht einer Jahresmenge zwischen 2,1 und 2,6 Millionen neu generierter Ether.

Vergleichbar mit der Teilbarkeit des amerikanischen Dollars in Cent oder den Bitcoins in Satoshi, ist dies auch bei Ether möglich. „Wei“ ist die ursprüngliche Bezeichnung für den kleinsten Teil der Währung Ether. Um nach dem Start von Ethereum einer nachträglichen Namensgebung kleinerer Einheiten durch die NutzerInnen ent-

[36] Vgl. Kryptocoinr (2016), online abgerufen am 16.06.2017
[37] Statistik abgerufen unter https://ethstats.net/, am 18.06.2017 um 18:29 Uhr

gegen zu wirken, wurden folgende Bezeichnungen bereits im 2014 veröffentlichten White Paper von Buterin niedergeschrieben. Der kleinste Teil heißt „Wei". 10^{12} Wei heißen „Szabo". 10^{15} Wei nennt man „Finney". 10^{18} Wei sind somit ein „Ether". Es sind auch weitere Abstufungen dieser Bezeichnungen mit den aus der Informatik und Physik bekannten Vorsilben wie Kilo (10^3), Mega (10^6) oder Giga (10^9) möglich. So wären zum Beispiel 10^9 Wei gleich einem Giga-Wei (oder kurz GWei).[38]

3.4. Nachrichten / Transaktionen

Im Ethereum-Netzwerk unterscheidet man zwischen Nachrichten und Transaktionen, die zwischen zwei Accounts gesendet werden können. Unter Nachrichten versteht man in etwa dasselbe, was in der Bitcoin-Blockchain Transaktionen sind. Nachrichten enthalten die Information, wie viel Ether von der/dem SenderIn an die/den EmpfängerIn übermittelt werden sollen. Es gibt jedoch zu den Bitcoin-Transaktionen einige Unterschiede. Nachrichten können entweder so wie Bitcoin-Transaktionen von einem externen Account (bei Bitcoin gibt es nur diese Art von Accounts), oder von einem Vertragskonto („contract account") ohne dem aktiven Zutun einer Person gesendet werden. Des Weiteren können Nachrichten im Ethereum-Netzwerk Daten enthalten. Die gesendeten Daten müssen ein bestimmtes Format haben und werden in der hexadezimalen Schreibweise versendet. Jeder Groß- oder Kleinbuchstabe, jede Zahl und jedes Sonderzeichen, das wir verwenden, hat einen eigenen hexadezimalen Wert. So entspricht zum Beispiel der Buchstabe „a" dem hexadezimalen Wert von 61. Der Buchstabe „b" entspricht dem hexadezimalen Wert von 62. Ein Text, der in seinen hexadezimalen Wert umgewandelt wurde, kann so in dem Bereich der Nachricht welche die Daten enthält, abgespeichert und versendet werden. Hexadezimale Werte bestehen sowohl aus Zahlen und Buchstaben und bei der Darstellung wird dem hexadezimalen Wert immer das Präfix „0x" vorangestellt. Da das gesamte Ethereum-Netzwerk diese hexadezimale Schreibweise verwendet, werden alle Adressen der Accounts, Hash-Werte der Transaktionen und auch die versendeten Daten/der Code mit diesem Präfix begonnen (siehe Abbildung 4, S. 29). Der dritte

[38] Vgl. Buterin (2014), S. 30, White Paper online abgerufen am 16.06.2017

Unterschied zwischen den Nachrichten in Ethereum und den Transaktionen in der Bitcoin-Blockchain liegt darin, dass die/der EmpfängerIn der Nachricht, wenn es sich dabei um ein Vertragskonto handelt, eine Antwort zurücksenden kann. Diese Vertragskonten werden wie erwähnt nicht von einer externen Person gesteuert, sondern besitzen einen ausführbaren Programmcode (den Vertrag) der durch eine eingehende Nachricht gestartet wird und eben wie hier eine Antwort an die/den SenderIn der Nachricht retournieren kann. Nachrichten im Ethereum-Netzwerk haben also nicht nur die Aufgabe eine Ether-Überweisung darzustellen, sondern können mehr. [39]

Unter einer Transaktion versteht man ein signiertes Datenpaket, welches in der Ethereum Blockchain abgelegt wird. Dieses Datenpaket kann, abgesehen vom zu überweisenden Ether, entweder eine Nachricht, oder einen neuen Smart Contract enthalten. Transaktionen können nur von einem externen Account versendet werden und müssen mit Hilfe des Private Keys der Senderin/des Senders signiert werden. Transaktionen enthalten mehrere Bestandteile. Darin sind die Sende- und Empfangs-Adressen sowie die Signatur zur Identifizierung der Senderin/des Senders enthalten. Darüber hinaus werden der Betrag an Ether, welcher überwiesen wird, und die zu sendenden Daten darin gespeichert. Eine Transaktion beinhaltet noch zwei Werte, welche von der/dem SenderIn vorgegeben werden. Dabei handelt es sich zum einen um den Gas-Price und zum anderen um das Gas-Limit. Des Weiteren wird aus den Transaktionsdetails der so genannte Hash der Transaktion erstellt. Mit diesem Hash ist jede Transaktion eindeutig identifizierbar.[40]

3.5. Gas-Price/Gas-Limit

Unter dem Gas-Price versteht man die Gebühr, welche für jedes Byte der Transaktion von der/dem SenderIn bezahlt werden muss. Das bedeutet eine Transaktion, die mehr Informationen, oder besser gesagt mehr Code enthält, kostet mehr, als eine Transaktion, die nur eine sehr kurze Nachricht enthält. Zu dieser Summe an verwendeten Gas wird nicht nur die ursprünglich in der Transaktion vorkommende Nachricht

[39] Vgl. Buterin (2014), S. 14, White Paper online abgerufen am 04.06.2017
[40] Vgl. Buterin (2014), S. 14ff, White Paper online abgerufen am 04.06.2017

gezählt, sondern auch alle anderen Nachrichten oder Contracts, welche durch diese Transaktion gestartet werden. Das Gas-Limit ist das Maximum des für eine Transaktion zur Verfügung stehenden Gas. Münzt man die beiden Begriffe auf ein Kraftfahrzeug um, ist bildlich gesprochen der Gas-Price der Preis für den Kraftstoff pro gefahrenem Kilometer und das Gas-Limit ist die Tankfüllung zu Beginn der Transaktion.[41]

Das Gas-Limit wird, so wie der Gas-Price, beim Erstellen der Transaktion festgelegt und kann im Nachhinein nicht mehr verändert werden. Man kann es sich wie eine reservierte Menge an Gas vorstellen, die zur Verfügung steht. Wird das gesamte Gas verbraucht, ist es verbraucht. Ist die Transaktion abgeschlossen und es wurde nicht das gesamte Gas benötigt, steht das restliche Gas der/dem SenderIn erneut zur Verfügung. Diese Limitierung der in der Transaktion ausführbaren Schritte hat einen sehr einfachen Grund. Zum einen soll verhindert werden, dass NutzerInnen, welche einen Contract in die Ethereum-Blockchain einfügen, diese mit programmierten, endlos ausgeführten Schleifen lahm legen. Zum anderen wird dadurch ein Anreiz geschaffen, die Contracts in der Blockchain möglichst effektiv zu programmieren und so die Geschwindigkeit des gesamten Systems hoch zu halten. [42]

Wird im Ethereum-Netzwerk zum Beispiel eine Transaktion erstellt, welche eine programmierte Schleife enthält, die endlos laufen würde, führt das Gas-Limit zu einer vorzeitigen Beendigung der Transaktion. Sobald das Limit erreicht wird und die Transaktion noch nicht beendet ist, werden alle Schritte, welche bis zu diesem Zeitpunkt von der Transaktion und den eventuell dahinter liegenden Codes ausgeführt worden sind, rückgängig gemacht. Das bedeutet, dass die Transaktion durch die Überschreitung des Gas-Limits keine Auswirkung in der Blockchain hat. Das bis zu diesem Punkt verwendete Gas wurde jedoch verbraucht und steht der/dem SenderIn der Transaktion nicht mehr zur Verfügung. Das heißt, dass ein falsch gesetztes Gas-Limit, oder eine solche endlos laufende Transaktion, der/dem SenderIn nur Kosten verursachen würde, und die Blockchain davon nicht betroffen wäre. Der/Dem SenderIn entstehen dadurch jedoch nicht nur Nachteile. Wird in der Transaktion ein Code gestartet, der unbeabsichtigt Fehler enthält, welche die Transaktion ungewollt ver-

[41] Vgl. Wood (2014), S.4, online abgerufen am 17.06.2017
[42] Vgl. Wood (2014), S.7f, online abgerufen am 17.06.2017

größern, kann dadurch verhindert werden, dass solch eine Transaktion der/dem SenderIn einen sehr hohen Betrag an Ether kostet.[43]

Die oben genannte Abhängigkeit der Gebühr von der Größe der getätigten Transaktion ist durchaus sinnvoll und nachvollziehbar. In der Ethereum-Blockchain werden ähnlich wie bei der Bitcoin-Blockchain, die in Blöcken zusammengefassten Transaktionen durch den Mining-Prozess verifiziert. Durch den Ablauf des Mining-Prozesses entstehen bei der/dem MinerIn Kosten. Diese Kosten sind zum überwiegenden Teil Stromkosten. Diese entstehen, weil die Transaktionen, welche in den nächsten Block aufgenommen werden sollen, auf jeden lokalen Rechner heruntergeladen werden müssen. So auch auf den der Minerin/des Miners. Ist nun eine Transaktion sehr umfangreich, dauert dieser Vorgang etwas länger und benötigt deshalb auch mehr Strom. Deshalb sind die entstandenen Kosten bei großen Transaktionen höher und die bezahlten Gebühren dafür ebenfalls. [44]

Grundsätzlich kann man das Gas also in Treibstoff und Gebühr unterteilen. Sieht man es als Treibstoff, spricht man von dem Gas-Limit. Wird das zu niedrig gewählt, wird die Transaktion niemals ausgeführt werden und kommt so auch nicht bei den MinerInnen an. Wird das Gas als Gebühr gesehen, spricht man vom Gas-Price der der/dem SenderIn für den Umfang der Transaktion berechnet wird und der/dem MinerIn als zusätzliche Vergütung bezahlt wird. Dieser Gas-Price kann, wie erwähnt, ebenfalls von der/dem SenderIn frei gewählt werden. Wird der Gas-Price zu gering gewählt, kann dies zur Folge haben, dass die Transaktion erst sehr spät, oder sogar überhaupt nicht von einer/einem MinerIn in einen Block integriert wird. Ein zu geringer Gas-Price hat also dieselbe Auswirkung wie eine zu niedrig gewählte Transaktionsgebühr im Bitcoin-Netzwerk. In den gängigen Wallet-Softwaren wird der zurzeit als standardmäßig gesehene Gas-Price angezeigt. Dieser richtet sich nach mehreren Faktoren des Ethereum-Netzwerks und wird durch den Ethereum-Algorithmus vorgegeben. Darin gehen unter anderem die gesamte Rechenleistung der MinerInnen und das zurzeit vorherrschende Transaktions-Aufkommen im Netzwerk ein. [45]

Die folgende Abbildung zeigt zur Veranschaulichung eine Transaktion im Ethereum-Netzwerk:

[43] Vgl. Wood (2014), S.7f, online abgerufen am 17.06.2017
[44] Vgl. Wood (2014), S.7f, online abgerufen am 17.06.2017
[45] Vgl. Wood (2014), S.7, online abgerufen am 25.06.2017

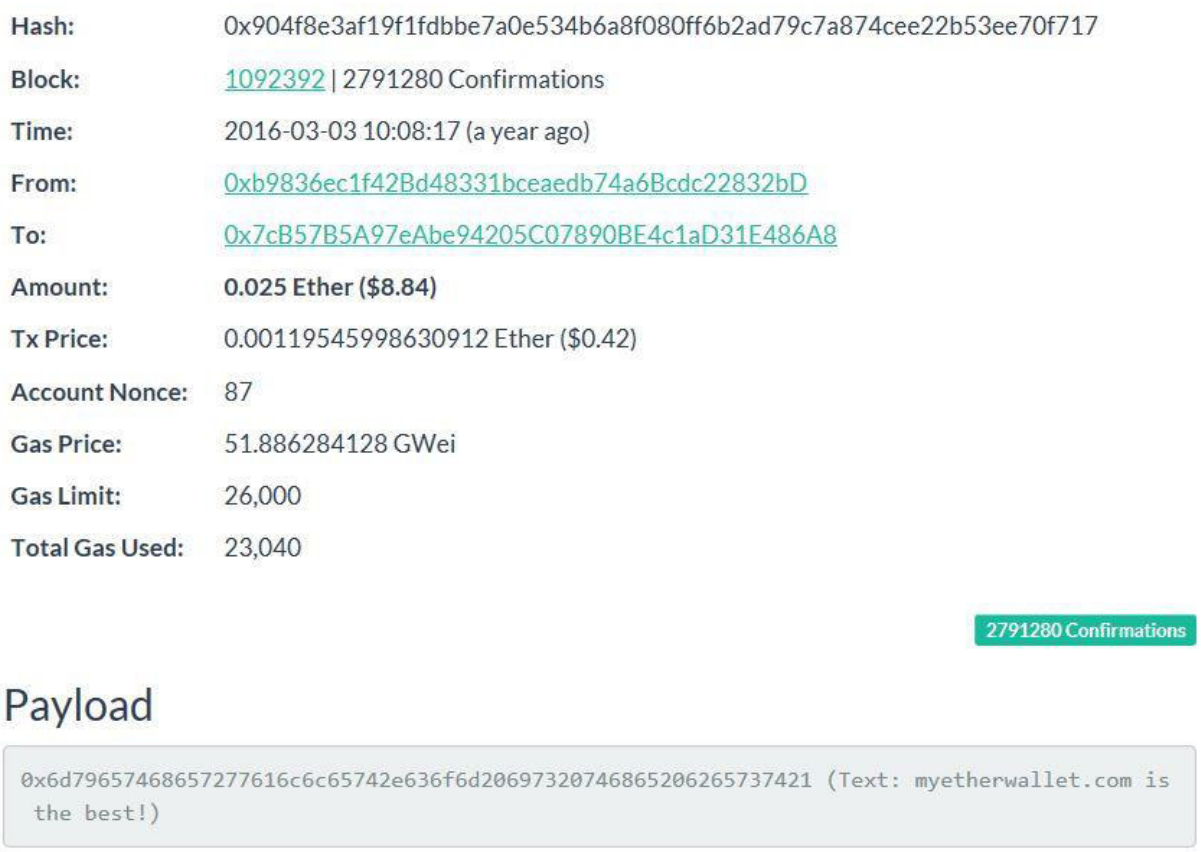

Abbildung 4 Beispiel Transaktion Ethereum[46]

Diese Transaktion ist unter dem Hash 0x904f8e3af19f1fdbbe7a0e534b6a8f080ff6b2-ad79c7a874cee22b53ee70f717 zu finden. Sie wurde am 03.03.2016 um 10:08:17 Uhr getätigt. Es sind die beiden Accounts zu sehen, die bei dieser Transaktion beteiligt waren und auch wie viele Ether (hier 0,025 Ether) versendet wurden. Darüber hinaus wird in der Abbildung unter „Payload“ dargestellt welche Daten – in diesem Fall eine Nachricht – zusätzlich übermittelt wurden. Zum einen wird die Nachricht in der hexadezimalen Schreibweise, beginnend mit „0x“ und zum anderen auch in der „herkömmlichen“ für uns lesbaren Schreibweise dargestellt. Die gezeigte Transaktion ist im Block 1092392[47] abgespeichert und wurde zum Zeitpunkt des Abrufens 2.791.280-mal verifiziert. Die Anzahl an Verifizierungen für diese Transaktion steigt ständig. Immer wenn nachfolgende Blöcke der Blockchain überprüft und freigegeben

[46] Beispiel Transaktion Ethereum, online im Internet: https://etherchain.org/tx/0x904f8e3af19f1fdbbe7a0e534b6a8f080ff6b2ad79c7a874cee22b53ee70f717, abgerufen am 17.06.2017 um 21:00 Uhr

[47] siehe dazu Block Nummer 1092392 unter https://etherchain.org/block/1092392

werden, werden wie bereits bei Bitcoin beschrieben, die „Vorgänger-Transaktionen“ verifiziert. Das Gas-Limit dieser Transaktion betrug 26.000, davon wurden 23.040 Gas verwendet. Der Gas-Price wurde beim Erstellen der Transaktion mit 51.886284128 GWei festgelegt. Das entspricht umgerechnet einem Wert von 0,000000051886284128 Ether. Dies mit dem für die Transaktion tatsächlich verwendeten Gas ergibt die Transaktionsgebühr („Tx Price“) von 0.00119545998630912 Ether. Die in der Abbildung 4 in Klammer angegebenen Dollar-Preise werden laufend mit dem aktuellen Ether-Dollar-Kurs aktualisiert.

3.6. Transaktions-Limit

Es macht den Anschein, dass die Größe einer Transaktion im Ethereum-Netzwerk nur von der/dem SenderIn selbst limitiert werden kann. Dies ist grundsätzlich auch richtig. Die/Der SenderIn legt das Gas-Limit für die Transaktion fest und hat dabei keine effektive Grenze nach oben. Die Transaktionen werden zu Blöcken zusammengefasst, um in die Blockchain aufgenommen zu werden. Diese Blöcke haben – durch den Ethereum-Algorithmus vorgegeben – ein festgelegtes Gas-Limit. Dieses Block-Gas-Limit kann sich jedoch durch die aktuellen Forderungen der NutzerInnen im Ethereum-Netzwerk verändern. Wird für die zusammenzufassenden Transaktionen, ein Gas-Limit gefordert, welches in den Blöcken summiert nahe an dem Block-Gas-Limit liegt, reagiert der Algorithmus darauf, indem er das Block-Gas-Limit um einen definierten Prozentsatz erhöht. Diese Änderung des Limits kann auch in die entgegengesetzte Richtung passieren. Wird von den NutzerInnen, ebenfalls über einen definierten Zeitraum gesehen, weniger Gas gefordert oder benötigt, kann sich das Block-Gas-Limit prozentuell verringern. Diese Erhöhung oder Verringerung des Block-Gas-Limits reagiert nur auf kurzzeitige Änderungen im Netzwerk. Auf längere Sicht wird über eine größere Anzahl an Blöcken ein Mittelwert gelegt, welcher ein Minimum für das Block-Gas-Limit setzt. Dieses Minimum kann in gewisser Weise als „Standard-Wert“ für das Limit verstanden werden, welches bei Bedarf durch den Algorithmus angepasst wird. Würde eine Transaktion erstellt werden, welche so viel Gas benötigt, dass dieses Block-Gas-Limit überschritten werden würde, könnte diese Transaktion nicht umgesetzt werden. Deshalb wird bereits bei der Erstellung einer

Transaktion automatisch überprüft, ob dieses Block-Gas-Limit von der Transaktion eingehalten wird. Ist dies nicht der Fall, so lässt sich diese Transaktion auch nicht freigeben.[48]

Durch die lückenlose Dokumentation aller Transaktionen in der Blockchain, lässt sich folgendes Beispiel für die Erhöhung des Block-Gas-Limits finden:

Die Transaktion, mit dem Hash-Wert von 0x25e54394ab4e5f17d6e1240c02c1a-6c4bb675ef9471f1105b006988f5fe5aec1, welche in nachfolgender „Abbildung 5“ zu sehen ist, hat ein durch die/den SenderIn festgelegtes Gas-Limit von 3.131.800.

Hash:	0x25e54394ab4e5f17d6e1240c02c1a6c4bb675ef9471f1105b006988f5fe5aec1
Block:	967163 | 2921164 Confirmations
Time:	2016-02-07 11:48:53 (a year ago)
From:	0x00006314Ee6Ba5a9421e4aa6A47C6867A882BD92
To:	0xfCAe7970392f510a985A7EacCD3820B7759d65D9
Amount:	**0.06 Ether ($21.31)**
Tx Price:	0.15159 Ether ($53.83)
Account Nonce:	1
Gas Price:	50 GWei
Gas Limit:	3,131,800
Total Gas Used:	3,031,800

Abbildung 5 Beispiel Gas-Limit Transaktion[49]

Das tatsächlich für diese Transaktion verwendete Gas liegt bei 3.031.800. Der Gas-Price liegt bei 50 GWei, was einer Transaktionsgebühr von 0.15159 Ether entspricht. Die Transaktion wurde während des Mining-Vorgangs von der/dem MinerIn „nano-pool" dem Block 967163 zugeordnet. Dieser Block ist in nachfolgender „Abbildung 6“ zu sehen.

[48] Vgl. Wood (2014), S.6, online abgerufen am 17.06.2017
[49] Beispiel Gas-Limit Transaktion, online im Internet: https://etherchain.org/tx/0x25e54394ab4e5f17d6e1240c02c1a6c4bb675ef9471f1105b006988f5fe5aec1, abgerufen am 17.06.2017 um 23:52 Uhr

Zu dem Zeitpunkt der Transaktion, lag das Block-Gas-Limit bei 3.141.592. Durch die Inanspruchnahme von mehr als 96 Prozent des Block-Gas-Limits (durch die getätigte und in den Block aufgenommene Transaktion), wurde dieses Block-Gas-Limit durch den Ethereum-Algorithmus für den nächsten Block erhöht. Der generierte Block enthält auf Grund der bereits sehr hohen Verwendung von Gas nur diese eine genannte Transaktion. Die Größe dieses Blocks beträgt 45.103 Bytes, was zum überwiegenden Teil durch die enthaltene Transaktion hervorgerufen wird. Die restlichen Informationen des Blocks gehen ebenfalls in dessen Größe ein.

Hash:	0x8da0f2ccff1565c1546210159b396f9d270f909e0c3b685a73e773c644bb9034
Difficulty:	10,929,786,153,749
Difficulty Bomb factor:	128 (0.000 %)
Miner:	nanopool
Gas Limit:	3,141,592
Gas Usage:	96.5% (3,031,800 of 3,141,592)
Minimum gas price:	50 GWei
Time:	2016-02-07 11:48:53 (a year ago)
Uncle Hash:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
Root:	0xfd3e7e848dfce1393b7cf4e0cc466ed8ebcb8fd9b31e479ac271b78046e5a2a1
Tx Hash:	0x280a5a19dd0fac0451b4b0257632bcc8d36fcad8f0a8ec23327eac0c76fc74c9
Size:	45103 bytes
Extra:	Geth v1.3.3 (Raw: 0xd783010303844765746887676f312e342e32856c696e7578)
Nonce:	0x88bd9cfa2d452453a3
Reward:	5.15159 Ether ($1,880.69)

Abbildung 6 Ethereum Block Nummer 967163[50]

Der nachfolgende Block ist in „Abbildung 7“ zu sehen und trägt die Nummer 967164. Wie oben erwähnt, wurde durch den der Blockchain zugrunde liegenden Ethereum-Algorithmus, das Gas-Limit für diesen Block erhöht. In diesem Fall auf 3.142.967. Dies entspricht einer Erhöhung um etwa 0,00044 Prozent.

[50] Ethereum Block Nummer 967163, online im Internet: https://etherchain.org/block/967163, abgerufen am 18.06.2017 um 00:08 Uhr

Im nächsten Schritt wurde der erzeugte Block in „Abbildung 7“ und die darin vorkommende sehr geringe Block-Gas-Limit-Ausnutzung wiederum wie oben beschrieben von dem Ethereum-Algorithmus wahr genommen.

Hash:	0x3bd3a5e4e293c65d1172adeeb65ed0311745e9ddab18bfd24e8879dec9f3fcdf
Difficulty:	10,924,449,344,232
Difficulty Bomb factor:	128 (0.000 %)
Miner:	nanopool
Gas Limit:	3,142,967
Gas Usage:	5.3% (165,094 of 3,142,967)
Minimum gas price:	52 GWei
Time:	2016-02-07 11:49:41 (a year ago)
Uncle Hash:	0x83acd4223c402f23f3c4db5608f44fdc0a6407e63ecef05c16bf092b5e22a14c
Root:	0xc633900b38dd09e548ec9b5ca545585701604f4036850d0352387772256069a9
Tx Hash:	0x96d84ce775385ef27ea156d9de0954d8a5453e557dd97982b38b38d611735f5c
Size:	1743 bytes
Extra:	Geth v1.3.3 (Raw: 0xd783010303844765746887676f312e342e32856c696e7578)
Nonce:	0x88cb77b4d0eb13731c
Reward:	5.164834888 Ether ($1,891.00)

Abbildung 7 Ethereum Block Nummer 967164[51]

Dieser nurmehr gut 5-prozentige Gas-Verbrauch führte dazu, dass im Block mit der Nummer 967165 das Block-Gas-Limit wiederum auf 3.141.592 gesenkt wurde – der zu diesem Zeitpunkt vorherrschende Standard-Wert.

Im Ethereum-Netzwerk gibt es zwar eine Größenbeschränkung der auszuführenden Programme, diese passt sich jedoch an das zurzeit benötigte Transaktions-Volumen der NutzerInnen an. Dieses Block-Gas-Limit kann auch nicht umgangen werden, indem man ein zu umfangreiches Programm in unterschiedliche Transaktionen aufteilt, welche sich nacheinander selbst aktivieren. Das Gas-Limit wird ja, wie bereits beschrieben, dahingehend berechnet, dass alle auszuführenden Schritte der Transakti-

[51] Ethereum Block Nummer 967164, online im Internet: https://etherchain.org/block/967164, abgerufen am 18.06.2017 um 01:22 Uhr

on – und auch alle dadurch aufgerufenen Transaktionen – zusammengezählt werden und daraus das verbrauchte Gas berechnet wird, welches durch das Gas-Limit abgedeckt sein muss. [52]

3.7. Ethereum Launch-Prozess

Ethereum, wie es heute existiert, und vor allem wie es einmal in Zukunft aussehen wird, ist kein „Ding“, das einfach am Tag „X“ eingeschaltet wurde. Natürlich gibt es wie in jeder Entwicklung besondere Ereignisse, die die Geschichte und Entwicklung von Ethereum bedeutend vorantrieben.

Zu Beginn standen das White Paper und die erste Veröffentlichung von Vitalik Buterin. Danach, im April 2014, veröffentlichte Gavin Wood das Ethereum Yellow Paper unter dem Titel „Ethereum: A Secure Decentralised Generalised Transaction Ledger“. Darin waren alle von Buterin vordefinierten Details, und darüber hinaus noch weitere Informationen und Spezifikationen, welche Ethereum betrafen, genauer definiert. Diese Veröffentlichung gilt bis heute als die technische Bibel von Ethereum. Diese genaue Definition aller Details hatte für den gesamten Entwicklungsprozess einen sehr großen Vorteil gebracht. Es blieben für die EntwicklerInnen nur sehr wenige Freiheiten für die grundlegende Gestaltung des Systems übrig. Dadurch wurde Ethereum zu genau dem, was es werden sollte. Es mussten lediglich die niedergeschriebenen Worte von Wood in einen programmierten Code umgewandelt werden. [53]

Abgesehen von der technischen Entwicklung der Blockchain, wurden auch sehr viele Vorkehrungen gesetzlicher Natur getroffen. So kam es dazu, dass alle in 2014 bekannten Rahmenbedingungen und Vereinbarungen vertraglich genau geregelt und niedergeschrieben wurden. Aus dieser vertraglichen Regelung entstand so im Juni 2014 die Stiftung Ethereum in Zug in der Schweiz. Dort hat die Stiftung bis heute ihren Hauptsitz. Nachdem der Grundstein für Ethereum durch diese Stiftung gelegt wurde, konnte der bereits oben erwähnte Crowdfunding-Prozess im Sommer 2014

[52] Vgl. Wood (2014), S.6, online abgerufen am 17.06.2017
[53] Vgl. Gerring (2016), online abgerufen am 05.06.2017

gestartet werden. Dieses Crowdfunding wurde in der Bitcoin-Blockchain durchgeführt, in welchem die Stiftung Ethereum als Bitcoin-Adresse zu finden war. Die Entscheidung, den Grundstein der neuen Blockchain durch Bitcoin – dem damaligen Aushängeschild der Blockchain-Technologie – zu legen, hatte einen demonstrativen Charakter. Man wollte zeigen, dass die Zeit für eine Weiterentwicklung der Blockchain gekommen war. Ethereum sollte bereits in etwas Großem seinen Anfang nehmen.[54]

Nach Ende des Crowdfunding hatte die Stiftung Ethereum endlich eigenes Kapital zur Verfügung. Damit wurden zuerst die Kredite beglichen, welche für den Start notwendig waren. Auch die EntwicklerInnen, welche bereits seit knapp einem halben Jahr an Ethereum gearbeitet hatten, bekamen ihre erste Entlohnung. Einige von ihnen hatten für diese Vision ihren Job gekündigt. Ohne sicheres Einkommen bedurfte es natürlich einem starken Glauben an das in Entstehung befindliche Projekt. Dies förderte den Zusammenhalt unter den EntwicklernInnen ungemein. Nachdem etwa im September 2014 der Großteil des Kapitals zur Verfügung stand, konnten die ersten Löhne bezahlt werden und es begann eine sehr umfangreiche Akquirierung neuer Arbeitskräfte. Die Gesamtheit der Team-Mitglieder war über beinahe den gesamten Globus verteilt wodurch sie vorerst nur per Telefon und Internet-Konferenzen in Kontakt traten. Ihr erstes ganzheitliches Treffen fand im November 2014 auf der so genannten „DEVCON0“ in Berlin statt. Dies war die erste Ethereum-Konferenz, die abgehalten wurde.[55]

Im Jänner 2015 waren bereits einige Teile des Ethereum-Algorithmus und der Software so weit fertig, dass mit den ersten Tests begonnen werden konnte. Aus diesem Grund wurde das sogenannte „Olympic testnet“ erstellt. Eine nur für die EntwicklerInnen zugängliche Ur-Version der Ethereum-Blockchain. Dieses Olympic testnet wurde im Mai 2015 gestartet. Natürlich gab es wie in jeder Entwicklung einige Fehler in der Software, die so gefunden werden konnten. Es war im Sinne der EntwicklerInnen, dass möglichst alle Eventualitäten und Vorkommnisse getestet werden konnten, wodurch die Software Schritt für Schritt stabiler und zuverlässiger wurde. Dadurch wuchs die Zuversicht bei den EntwicklernInnen und die Spekulationen über einen ersten Release für die Öffentlichkeit wurden lauter. Da man bei Ethereum jedoch ein

[54] Vgl. Gerring (2016), online abgerufen am 05.06.2017
[55] Vgl. Gerring (2016), online abgerufen am 05.06.2017

stabil laufendes Netzwerk einem baldigen Release vorzog, musste sich die wachsende Community noch ein wenig gedulden.[56]

Die Veröffentlichungen von Ethereum können grundsätzlich in vier größere Meilensteine unterteilt werden, die in den folgenden Kapiteln näher erläutert werden.

3.7.1. Frontier-Release

Im Juli 2015, kaum ein Jahr nachdem sich das Entwicklungs-Team das erste Mal getroffen hatte, war es dann so weit. Die erste Veröffentlichung wurde mit dem ersten Block am 30.07.2015 eingeläutet und trägt den Namen „Frontier". Dieses Frontier-Release war bereits eine Blockchain mit dem Namen Ethereum. Diese war der Bitcoin-Blockchain sehr ähnlich und stellte das Ethereum-Netzwerk in seiner ursprünglichsten Form dar. Darin war bereits der Mining-Prozess ausführbar um Ether zu generieren. Des Weiteren konnten schon die ersten Programme in Form von (Smart) Contracts in das Netzwerk geladen und ausgeführt werden. Der Hauptgrund für die Frontier-Veröffentlichung war, das gesamte System um die Ether-Generierung und den Tauschhandel der Währung über die Ethereum-Blockchain ins Laufen zu bringen. Die bereits in dieser frühen Phase aktiven Personen sollten sich an die Währung an sich und den Umgang damit gewöhnen. Die Notwendigkeit für diesen Schritt ist verständlich, da es zuvor nur den Crowdfunding-Prozess und einige öffentliche Auftritte rund um Vitalik Buterin gab. Es war wichtig, dass die NutzerInnen ebenfalls damit begannen, selbst Ether durch das Mining zu generieren, da sie nur so zeitnah an die Möglichkeit gelangten, selbst geschriebene Software in die Blockchain aufzunehmen und gemeinsam ein erstes Netzwerk aus Transaktionen und Smart Contracts zu erstellen.[57]

Das Benutzen der ersten Version der Ethereum-Blockchain war noch nicht ganz mit dem der heute existierenden Blockchain vergleichbar. Das Arbeiten mit der Blockchain war zu diesem Zeitpunkt nur über eine Kommandozeile möglich. Das bedeutet, dass jeder Befehl in einer extra für die Blockchain entwickelten Computer-Sprache geschrieben werden musste. Dies setzte bei den NutzerInnen natürlich ein grundle-

[56] Vgl. Gerring (2016), online abgerufen am 05.06.2017
[57] Vgl. Gupta (2015), online abgerufen am 18.06.207

gendes und vor allem umfangreiches Wissen über die Ethereum-Blockchain und das Programmieren mit vorhandenen Werkzeugen voraus. Dieses Wissen musste erst verbreitet und durch die TeilnehmerInnen während der Verwendung gefestigt und stetig weiterentwickelt werden.[58]

Um den Gedanken der EntwicklerInnen und erster EnthusiastInnen weiter in die Welt zu tragen und mehr Menschen die Vorteile von Ethereum aufzuzeigen, wurde im November 2015 die Veranstaltung „DEVCON1" in London abgehalten. Dabei wurde eine Woche lang über Ethereum gesprochen und im Zuge von 80 Vorträgen das gesamte System beschrieben. Unter knapp 400 Interessierten bei dieser Veranstaltung waren unter anderem auch MitarbeiterInnen von IBM und Microsoft, die das Potential von Ethereum für ihr Unternehmen beurteilen sollten. Bei dieser Veranstaltung ging es weniger um den Wert oder mögliche Spekulationen rund um die Kryptowährung, sondern viel mehr um die Entwicklung von Standards, Ideen für neue Möglichkeiten und die Zusammenführung von technischen und wirtschaftlichen Interessen. [59]

3.7.2. Homestead-Release

Das Homestead-Release ist der zweite Abschnitt des Ethereum-Fahrplans. Der Umstieg von Frontier zu Homestead wurde am 14.03.2016, genauer gesagt beim Block 1.150.000 der Ethereum-Blockchain durch einen Hard Fork durchgeführt. Unter einem Hard Fork versteht man eine erzwungene Gabelung in der Blockchain – siehe dazu „Abbildung 8". Diese entsteht, wenn grundlegende Änderungen an den vorherrschenden Regeln umgesetzt werden. Dabei verfolgt die bisherige Blockchain die alten Regeln und die neu entstandene die neuen Regeln. Normalerweise wird die „alte" Blockchain dann noch für ein paar Blöcke weiter existieren, da nicht alle NutzerInnen im selben Moment auf die neuen Regeln umsteigen. Dieser Umstieg erfordert meist ein Software-Update, welches von jeder/jedem NutzerIn auf ihrem/seinem eigenen Rechner durchgeführt werden muss. Bei einem Hard Fork kann es auch passieren, dass eine Vielzahl von NutzerInnen weiterhin die alten Regeln befolgen wollen und aus diesem Grund das Update nicht durchführen. Dies hätte zur Folge, dass beide Ketten parallel existieren würden. Ein Vorteil eines Updates durch einen Hard Fork ist, dass die EntwicklerInnen sofort ein Feedback von den NutzerInnen erhalten. Je

[58] Vgl. Gupta (2015), online abgerufen am 18.06.207
[59] Vgl. Gerring (2016), online abgerufen am 05.06.2017

nachdem wie viele NutzerInnen updaten und vor allem wie schnell sie das tun, zeigt dem Entwicklerteam wie gut das Update ankommt und ob die Mehrzahl der NutzerInnen der Weiterentwicklung zustimmen.[60]

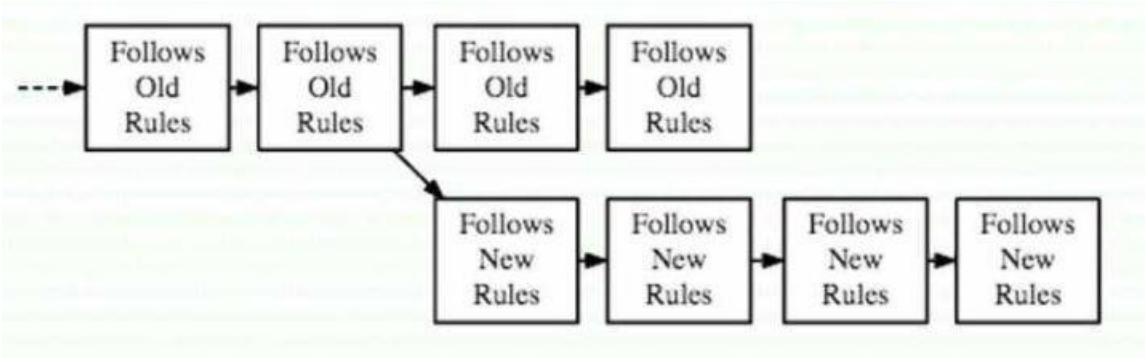

Abbildung 8 Hard Fork[61]

Die Gründe für den Hard Fork im Ethereum Netzwerk beim Umstieg von Frontier auf Homestead waren unter anderem eine Anpassung der Kosten für die Erstellung neuer Smart Contracts und einer Änderung der Auswirkungen bei Erreichen des Gas-Limits. Darüber hinaus wurde in diesem Release der Algorithmus für die Veränderung des Schwierigkeitsgrades weiter angepasst. Die Belohnung von 5 Ether pro erzeugtem Block blieb gleich und der Mining-Prozess wurde ebenfalls nicht verändert. [62]

Von Seiten Ethereum wurde allen NutzerInnen versichert, dass sofern sie ihre Private Keys nicht verlieren würden, durch den Umstieg auf Homestead kein einziger ihrer gekauften, gespeicherten oder empfangenen Ether verschwinden würde. Diese würden nach dem Update noch genauso zur Verfügung stehen, wie davor. Mit heutigem Wissen kann gesagt werden, dass dies korrekt war und kein einziger Bericht über verlorene Ether öffentlich gemacht wurde. Das Update von Frontier auf Homestead war freiwillig. Wollte man jedoch weiterhin das Ethereum-Netzwerk nutzen, musste man auf Homestead updaten, dies wurde von Ethereum so vorgeschrieben. Ein gewisser Anreiz war sicherlich die Zusage von Ethereum, dass mit

[60] Vgl. Donnelly (2016), online abgerufen am 25.06.2017
[61] Hard Fork, online im Internet: https://github.com/ethereum/homestead-guide/blob/master/source/introduction/the-homestead-release.rst, abgerufen am 25.06.2017 um 18:56 Uhr
[62] Vgl. Donnelly (2016), online abgerufen am 25.06.2017

dem Homestead-Release, die gesamte Blockchain als sicher galt. So wurden während der Frontier-Phase noch zahlreiche Warnhinweise auf der Homepage angezeigt, die darauf hinweisen sollten, dass Frontier zwar eine freigegebene Version sei, jedoch immer noch in einer Entwicklungs- und Testphase stehen würde. Mit dem Homestead-Release wurden diese Warnhinweise zur Gänze entfernt. Der Zeitpunkt für das Homestead-Release wurde also von den NutzerInnen bereits herbeigesehnt. Die erstellten Smart Contracts mussten zwar erneut in die Blockchain integriert werden, es konnte jedoch davon ausgegangen werden, dass diese dort bleiben würden und somit einen Platz in etwas Großem haben würden. Durch die Zusage der EntwicklerInnen, dass die Blockchain nun eine erhebliche Sicherheit besaß, wurde sie auch für Banken und öffentliche Stellen zunehmend interessanter.[63]

Darüber hinaus wurden mit dem Homestead-Release weitere Verbesserungen an einem Programm namens „Mist“ getätigt. Mist ist eine Entwicklung des Ethereum-Teams und befindet sich nicht in der Blockchain. Damit war es zum Teil bereits in der Frontier-Phase möglich, ein Wallet zu erstellen. Mist sollte sich zu einer Art Ethereum-Browser entwickeln. Die Wallet-Funktion wurde beibehalten und es sollte die Möglichkeit gegeben werden, Smart Contracts direkt über Mist aufzurufen. Es sollte eine Art App-Store für dezentrale Apps – sogenannte DApps – werden. Da in der Homestead-Phase immer mehr von diesen DApps erstellt wurden, war eine solche Sammlung der unterschiedlichen Smart Contracts sehr hilfreich. Mist ist nicht direkt von den Release-Schritten der Blockchain abhängig, musste aber zum Beispiel bei dem Homestead-Release ebenfalls upgedatet werden.[64]

3.7.3. Metropolis-Release

Zurzeit befindet sich die Ethereum-Blockchain noch in der Homestead-Phase. Der dritte Entwicklungsschritt wird den Namen Metropolis tragen. Dieses nächste Release liegt jedoch noch in der Zukunft und ein voraussichtlicher Termin dafür ist noch nicht offiziell. [65]

Die derzeit letzte Äußerung von Vitalik Buterin bezüglich des Termins war gegen Ende Mai dieses Jahres. Darin sagte er, dass der Termin noch nicht fest steht, jedoch

[63] Vgl. Donnelly (2016), online abgerufen am 25.06.2017
[64] Vgl. Donnelly (2016), online abgerufen am 25.06.2017
[65] Vgl. Gupta (2015), online abgerufen am 18.06.207

mit Hochdruck an dem Metropolis-Release gearbeitet wird. Die generelle Meinung unter den EntwicklernInnen sei jene, dass sie noch umfangreiche Tests und einige Weiterentwicklungen abwarten wollen, bevor der nächste große Schritt getan wird.[66]

Für Metropolis wurden bisher bereits einige Neuerungen angekündigt, welche in diesem Schritt umgesetzt werden sollen. Die Umstellung auf Metropolis soll, wie bereits bei dem Update von Frontier auf Homestead, über einen Hard Fork erfolgen. Die wohl wichtigste Neuerung unter Metropolis wird die Vereinfachung der Zugänglichkeit zur Ethereum-Blockchain sein. Durch eine neue Schnittstelle soll es auch für laienhafte BenutzerInnen möglich sein, die Funktionen und Möglichkeiten der Blockchain zu verwenden. Bisher musste sich zuvor ein umfangreiches Grundwissen angeeignet werden. Mit dem nächsten Release-Schritt soll dies teilweise der Vergangenheit angehören. Damit macht Ethereum einen sehr großen Schritt in Richtung Massentauglichkeit. Mit Metropolis wird sich also zeigen, ob Ethereum für eine hohe Anzahl an Menschen nutzbar gemacht werden kann. Deshalb ist es nur zu verständlich, wenn sich die EntwicklerInnen mit den Tests und Vorbereitungen für dieses Release ein wenig Zeit lassen. Wenn der Umstieg auf Metropolis gut funktioniert und dadurch bei mehr NutzerInnen das Interesse an Ethereum geweckt wird, kann sich das ebenfalls sehr positiv auf die Kryptowährung Ether auswirken. Deshalb wird das Release auch von Personen herbeigesehnt, die finanziell einen spekulativen Aufschwung darin sehen.[67]

Es kursieren bereits sehr viele Gerüchte über eventuelle Neuerungen bei dem nächsten Release. Einige davon werden immer wieder von dem Entwicklerteam bestätigt, indem sie selbst Auskünfte über kleinere Entwicklungsschritte geben. So sollen zum Beispiel mit Metropolis einige Updates kommen, welche die Verbesserung der Sicherheit und der Privatsphäre der einzelnen NutzerInnen betreffen sollen. Dies sind generell zwei Kernelemente, welche sehr häufig von Verbesserungen betroffen sind. Des Weiteren soll es eine Änderung betreffend der Bezahlung der Transaktionsgebühren geben. Diese Änderung soll es in Zukunft ermöglichen, dass die Gebühr – also das Gas – ebenfalls von der/dem EmpfängerIn bezahlt werden kann. Bis jetzt war es nur möglich, dass die/der SenderIn das verwendete Gas bezahlen musste. Um diese Änderung umzusetzen, benötigt es wie bereits oben erwähnt einen Hard Fork. Es muss Ethereum dazu möglich sein, vor Freigabe der Transaktion, den

[66] Vgl. Buterin (2017), online abgerufen am 28.06.2017
[67] Vgl. Buntinx (2017), online abgerufen am 25.06.2017

Kontostand der/des Empfängerin/s zu kontrollieren, und festzustellen, ob dort genügend Ether für die Bezahlung des verwendeten Gas zur Verfügung steht. Dies ist natürlich ein Eingriff in die Privatsphäre der NutzerInnen und benötigt deren Zustimmung durch ein Update, dem ein Hard Fork voraus geht. Darüber hinaus soll es noch weitere Änderungen und Verbesserungen geben. Grundsätzlich werden zurzeit jedoch jene priorisiert, welche einen Hard Fork bei deren Umsetzung benötigen. Kleinere Änderungen oder Updates können ohne diesen erfolgen und somit auch zu einem späteren Zeitpunkt nachgeholt werden.[68]

Meines Erachtens nach wird Metropolis der nächste Große Schritt in der Geschichte von Ethereum sein. Die Massentauglichkeit ist bei solch einer Technik wohl die größte Hürde. Wenn Massen dafür begeistert werden können, einen Nutzen darin sehen und die Verwendung auch kein Hindernis darstellt, denke ich, dass Ethereum das Potential besitzt, eine große Veränderung in vielen Bereichen zu bewirken.

3.7.4. Serenity-Release

Serenity wird die vierte und zurzeit letzte, geplante große Neuerung im Ethereum-Netzwerk sein. Wie bei den drei voran gegangenen Meilensteinen, wird es auch hier wieder einen Hard Fork geben. Kleinere Updates sollen teilweise die Benutzerfreundlichkeit weiter steigern. So soll es zukünftig zum Beispiel möglich sein, nur einen gewissen Teil der Blockchain, nämlich den, der für einen selbst von Bedeutung ist, zu verwenden. Dieser kleinere Teil benötigt am Computer der NutzerInnen weniger Speicherplatz und lässt sich schneller bearbeiten. Durch definierte Schnittstellen zur gesamten Blockchain soll jedoch immer noch der Konsensgrundsatz – also die Nachvollziehbarkeit des gesamten Netzwerks – gegeben sein. Smart Contracts sollen die Möglichkeit bekommen, autonomer handeln zu können. Weiters soll die Notwendigkeit der Aktivierung durch einen externen Account etwas gemindert, oder gar zum Teil aufgehoben werden. Zwei wesentliche Verbesserungen sollen die Zeiten und Geschwindigkeiten der Blockchain betreffen. Zum einen soll die Blocktime, also die Zeit, welche zur Erstellung eines neuen Blocks notwendig ist, gesenkt und zum anderen die Transaktionsgeschwindigkeit erhöht werden. Dies wird dann erneut das

[68] Vgl. Buntinx (2017), online abgerufen am 25.06.2017

Interesse von Banken und anderen Instituten wecken, bei denen eine schnelle Bearbeitung von Transaktionen wichtig ist.[69]

3.7.4.1. Proof of Stake

Die größte und bedeutendste Neuerung, welche das Serenity-Release beinhalten soll, betrifft das Mining. Bisher wurde die Validierung, also die Überprüfung der getätigten Transaktionen auf ihre Richtigkeit, durch den Mining-Prozess abgewickelt. Dabei musste, wie bereits beschrieben, eine Rechenaufgabe durch die MinerInnen gelöst werden. Dies bedurfte bisher einem hohen Maß an Rechenleistung und damit einhergehend einem hohen Stromverbrauch. Durch den Aufwand, den die MinerInnen mit der Überprüfung der Transaktionen haben, wird dieses Verfahren auch „Proof of Work“ genannt. Dieser hohe Stromverbrauch ist den EntwicklerInnen seit Beginn an ein Dorn im Auge. Aus diesem Grund wird für das letzte Release der Umstieg auf einen anderen Ansatz zur dezentralen Konsensbildung verfolgt – der „Proof of Stake“. Dabei wird versucht, allein durch die Zustimmung der Mehrheit der NutzerInnen, welche sich daran beteiligen, die Wahrheit der Transaktionen zu bestätigen. Es gibt zwar bereits Kryptowährungen, die eine Art Proof of Stake nutzen, doch noch nie wurde der Umstieg darauf von Proof of Work in einer bestehenden Blockchain vollzogen. In Ethereum wird dieses Proof of Stake unter dem Namen „Casper“ laufen.[70]

Casper soll, wie bereits oben erwähnt, ebenfalls die Validierung der Transaktionen im Ethereum-Netzwerk ermöglichen und das alles mit verhältnismäßig sehr geringem Energieaufwand. Die ersten Testversionen gibt es bereits seit einiger Zeit und ein Entwicklerteam rund um Buterin arbeitet fieberhaft an der Verbesserung und Finalisierung von Casper. Es trat jedoch relativ bald im Entwicklungsprozess ein Problem auf. Stakeholder, also am Validierungsprozess beteiligte Personen, konnten mehrere Versionen der vergangenen Blöcke bestätigen, ohne dass dies negative Auswirkungen für sie hatte. Deshalb konnte das Test-Netzwerk nicht zweifelsfrei feststellen, welche Transaktionen nun korrekt waren und welche nicht. Bei Casper soll dies anders laufen. Stakeholder, die sich nicht korrekt verhalten und die vorgegebene Regeln ignorieren, sollen bestraft werden. Um den gesamten Prozess zu veranschauli-

[69] Vgl. Silva (2017), online abgerufen am 29.06.207
[70] Vgl. Giese (2017), online abgerufen am 29.06.2017

chen, hier ein Beispiel: Es versammelt sich eine gewisse Anzahl von Personen (die Stakeholder) um einen Tisch. Nun wird ein Stapel mit Zetteln gebracht. Auf jedem Zettel ist ein anderer Transaktionsverlauf abgebildet. Es beginnt die/der erste StakeholderIn mit dem Unterzeichnen eines dieser Zettel und drückt damit seine Zustimmung zu dem abgebildeten Transaktionsablauf aus. Die/Der nächste StakeholderIn kann nun entweder denselben Zettel unterschreiben, oder aber einen anderen. Jede/Jeder StakeholderIn bekommt eine Belohnung dafür, wenn sie/er den Zettel, der am Ende die meisten Zustimmungen hat, ebenfalls unterschrieben hat. Daraus ergibt sich, dass es augenscheinlich am besten ist, die Transaktionen zu bestätigen, welche auch offensichtlich die richtigen sind. Sollte jedoch jemand zuerst einen Zettel unterschrieben haben, dann jedoch seine Meinung geändert haben und einen anderen ebenfalls unterschreiben, wird eine Strafzahlung fällig, welche die Belohnung übersteigt. Die StakeholderInnen sehen während diesem Vorgang selbstverständlich nicht, wer welche Transaktionsgeschichte unterzeichnet hat. Wird ein offensichtlich falscher Block als korrekt unterzeichnet, führt dies ebenfalls zu einer Strafzahlung. Dieser gesamte Proof of Stake Vorgang beruht darauf, dass die Mehrzahl an StakeholderInnen ihr Handeln dahingehend auslegen, den eigenen Gewinn zu erhöhen und nicht anderen möglichst keinen Gewinn zuzugestehen. Bis es dann tatsächlich zu dieser Änderung kommen kann und ein Algorithmus generiert wird, der alle Eventualitäten absichert und die nötigen Grenzen setzt, wird vermutlich noch einiges an Entwicklungs- und vor allem Test-Zeit vergehen.[71]

Grundsätzlich ist es bei einem auf Proof of Stake basierenden System so, dass nicht jede/jeder TeilnehmerIn sofort aktiv an der Validierung teilnimmt. Entscheidet sich eine Person dazu, benötigt diese zuerst die Kryptowährung, welche in der Blockchain verwendet wird. In diesem Fall Ether. Durch eine spezielle Transaktion, die getätigt werden muss, wird die gesamte Summe an Ether gesperrt. Das heißt die/der TeilnehmerIn kann mit ihrem/seinem Ether keine anderen Überweisungen mehr tätigen. Der Prozess der Generierung von neuen Blöcken wird dann mittels eines Algorithmus ausgeführt. Durch die Validierung eines Blocks, der dann in die Blockchain gereiht wird, erhält jede/jeder StakeholderIn wie oben beschrieben eine Belohnung. Diese wird voraussichtlich ein Prozentsatz des bereits in Besitz befindlichen Ethers ausmachen. Das bedeutet, dass StakekholderInnen, die mehr Ether besitzen, auch mehr Ether als Belohnung bekommen. Es ist noch nicht sicher, ob diese Belohnung

[71] Vgl. Giese (2017), online abgerufen am 29.06.2017

dann periodisch ausgeschüttet, oder dem gesperrten Betrag an Ether zugerechnet wird. Bei letzterem erhält die/der StakeholderIn zwar keine laufenden Auszahlungen, kann aber über längere Sicht ihr/sein Vermögen erheblich steigern. Der (vielleicht) gleich bleibende Prozentsatz für die Belohnung, wird dann von einem immer größer werdenden Ausgangsbetrag berechnet, was eine immer höher werdende Belohnung bedeuten würde. Das setzt natürlich voraus, dass die Kryptowährung ihren Wert beibehält, oder sogar steigert. Wie dieser Casper-Algorithmus letztendlich genau aussehen wird, steht jedoch noch nicht fest.[72]

3.7.4.2. Difficulty Bomb

Wie bereits erwähnt, wird es bei dem Update auf Serenity wieder einen Hard Fork geben. Vermutlich wird es nicht sehr schwierig sein, den Großteil der NutzerInnen dazu zu bewegen, das Update auf die neue Blockchain, welche Casper verwendet, durchzuführen. Schließlich bringen Neuerungen wie verkürtzte Blockzeiten, erhöhte Transaktionsgeschwindigkeiten und ein geringerer Energieverbrauch große Vorteile für die NutzerInnen. Für den Großteil der NutzerInnen scheint es also fast so, als ob Serenity und der darin enthaltene Casper-Algorithmus, das Ziel ihrer Reise wäre und sie das Update fast nicht mehr erwarten könnten. Das trifft natürlich auf eine Gruppe der NutzerInnen keinesfalls zu – die MinerInnen. Darin liegt auch der Handlungsbedarf bei den EntwicklerInnen, um auch diese Personen zum Umstieg zu bewegen. Denn sie sind es, die die alte Blockchain noch weiter am Leben erhalten könnten, indem sie weiterhin mit den alten Regeln und dem Proof of Work neue Blöcke generieren würden.[73]

Bei dem letzten Release und der damit einhergehenden Einführung von Casper könnten zwei Dinge nicht wie geplant funktionieren. Zum einen wäre es möglich, dass der Casper-Algorithmus zum vereinbarten Termin einfach noch nicht fertig ist. Das hieße, dass es den EntwicklernInnen nicht schnell genug möglich gewesen ist, eine funktionierende und bis ins Detail getestete Version von Casper zu erstellen. Wenn dies der Fall ist, könnte das Release einfach nach hinten verschoben werden und so dem Entwicklerteam mehr Zeit gegeben werden. Zum anderen könnte es wie erwähnt sein, dass die alte Blockchain nicht aufgegeben wird und die MinerInnen

[72] Vgl. Edwards (2017), online abgerufen am 29.06.2017
[73] Vgl. Castor (2017), online abgerufen am 24.06.2017

immer noch neue Blöcke generieren. Ethereum hatte dafür jedoch von Beginn an einen Plan. Aus diesem Grund wurde mit dem Frontier-Release bereits ein Grundstein gelegt. Ab einem bestimmten Block soll die so genannte „Difficulty Bomb" gestartet werden. Diese hat ein Ziel: Nach einer gewissen Anzahl von generierten Blöcken soll dieser Algorithmus die Schwierigkeit der Blöcke – also den Rechenaufwand für die MinerInnen – erhöhen. Diese Erhöhung soll zuerst relativ unscheinbar vor sich gehen und sich ab einem gewissen Punkt exponentiell steigern. Diese Steigerung sollte gegen Ende des Jahres 2016 ihren Höhepunkt erreichen und den Mining-Prozess so sehr erschwert haben, dass es nicht mehr wirtschaftlich ist, oder die Blockchain auf Grund von dermaßen langen Zeiten bei der Generierung von neuen Blöcken schlichtweg nicht mehr zu verwenden ist. Da man bildlich gesprochen von einem Einfrieren der Blockchain sprechen kann, würde dieser Zustand auch Eiszeit genannt werden. Die Veränderung der Schwierigkeit der Difficulty Bomb wurde in mehreren Updates immer wieder verändert. Dies ist auch der Grund warum die Eiszeit bis heute noch nicht eingetreten ist und sich die Zeit für die Generierung neuer Blöcke zurzeit (Stand Juni 2017) bei etwa 18 Sekunden aufhält. Die langsame Erhöhung der Blockzeit lässt darauf schließen, dass die Difficulty Bomb bereits jetzt Auswirkungen auf die Blockchain hat, diese aber noch überschaubar sind. Die im Netzwerk zur Verfügung stehende, gesamte Rechenleistung hat darauf ebenfalls einen Einfluss. Erhöht sich diese nicht wie vorhergesagt mit der Steigerung der Schwierigkeit für das Mining, erhöht sich der Zeitaufwand für die Generierung von neuen Blöcken ebenfalls. Buterin hat berechnet, dass bis Mitte August 2017 die Blockzeit auf ungefähr 30 Sekunden ansteigen wird. Eine Zeit von 30 Sekunden scheint im Vergleich zu den ungefähr 10 Minuten, die es bei Bitcoin dauern kann, nicht viel zu sein. Man muss jedoch beachten, dass die beiden Blockchains unterschiedliche Verwendungen abbilden. Bei Bitcoin werden ausschließlich Überweisungen dokumentiert und verifiziert. Diese Vorgänge stehen meist nicht derart unter Zeitdruck, sodass 10 Minuten kein Problem darstellen. In Ethereum hingegen laufen unter anderem Smart Contracts. Dabei kann eine Verzögerung von 30 Sekunden schon einen großen Unterschied in der Benutzerfreundlichkeit bedeuten.[74]

Vermutlich wird die Erhöhung der Blockzeiten, wie sie momentan vorkommt, in manchen Fällen für kleinere Probleme sorgen. Jedoch denke ich, dass dies von einer überwiegenden Anzahl an NutzerInnen in Kauf genommen wird, da die Lösung be-

[74] Vgl. Castor (2017), online abgerufen am 24.06.2017

reits in Sicht ist. Es muss lediglich abgewartet werden. Wie lange noch darauf gewartet werden kann, hängt von unterschiedlichen Faktoren ab, die von jeder/jedem NutzerIn selbst abgewogen werden müssen.

Eine Befürchtung der NutzerInnen ist jedoch begründet. Wenn der Mining-Prozess noch vor Einführung von Casper so schwierig werden würde, dass die zu erwartende Belohnung für die MinerInnen nicht mehr rentabel ist, werden viele von ihnen Ethereum verlassen. Andere Kryptowährungen, welche zwar nicht denselben, hohen finanziellen Wert besitzen wie Ethereum, würden zunehmend interessanter werden, da dort das Mining noch mit verhältnismäßig wenig Aufwand betrieben werden kann. Für Ethereum würde das bedeuten, dass die Sicherheit des Netzwerks mit der darin befindlichen Anzahl an MinerInnen sinken würde. [75]

Durch die Tatsache, dass Ethereum ständig weiterentwickelt und verbessert wird und immer wieder neue Erkenntnisse gemacht werden, ist es sehr schwierig vorherzusagen, welche Neuerungen und Veränderungen in den einzelnen, kommenden Release-Schritten vorgenommen werden. Der grundlegende Fahrplan ist zwar vorgegeben, wie die Details dazu aussehen, bleibt jedoch bis zum Tag X abzuwarten.

4. Risiken für NutzerInnen

Kryptowährungen wie Bitcoin oder Ether bergen Gefahren, welche zum Teil nicht neu sind und bei herkömmlichen Währungen ebenfalls vorkommen können. So zum Beispiel ist es möglich, dass diese verloren oder gestohlen werden. Durch die ausschließliche Verwaltung der eigenen Coins über eine Wallet Software, ist es möglich, dass diese aufgrund einer Fehlfunktion des Computers oder eines bösartigen Angriffs über das Internet unbrauchbar gemacht oder entwendet werden. Verliert jemand den Private Key eines Accounts – in welcher Art und Weise auch immer - kann die/der NutzerIn nicht mehr über die darin gespeicherten Einheiten der Kryptowäh-

[75] Vgl. Castor (2017), online abgerufen am 24.06.2017

rung verfügen. Die meisten Wallet Softwaren beinhalten eine Vielzahl von Schutzfunktionen, die die eigenen Konten sicher machen sollen. Je länger so eine Schutzfunktion bereits existiert, desto wahrscheinlicher wird es, dass jemand versucht, diese zu umgehen. Aus diesem Grund werden diese Schutzfunktionen ständig weiter entwickelt und an vorherrschende Sicherheitsstandards angepasst.[76]
Bei all den Sicherheits- und Schutzfunktionen gibt es jedoch meines Erachtens keine vollkommene Sicherheit. Vor allem nicht in einem System, das von eher laienhaften NutzerInnen ebenfalls bedient und nicht bis ins Detail verstanden werden kann. Diese Funktionen und Aufgaben müssen dann von den AnbieternInnen der Software übernommen werden. Ob in einem Verlust- oder Schadensfall dafür jedoch eine Haftung übernommen wird, ist fraglich und wird vermutlich durch eine Zustimmung der allgemeinen Geschäftsbedingungen ausgeschlossen.

Ähnlich wie bei Aktien ergibt sich eine weitere Gefahr durch die Möglichkeit der Kursschwankung. Der Wert von Bitcoin, Ether und anderen wird allein durch Angebot und Nachfrage der TeilnehmerInnen dieser Netzwerke bestimmt. Wie unter Kapitel 2.3 dargestellt, hat beispielsweise Bitcoin in den letzten Monaten eine Steigerung des Wertes erlebt, die nur mit einem wahren Höhenflug beschrieben werden kann. Es ist selbstverständlich auch denkbar, dass diese Entwicklung in die Gegenrichtung gehen kann und dadurch ein Wertverlust auftritt, welcher in kürzester Zeit sehr viel an Kapital zu Nichte machen kann. Eine Garantie für einen minimalen Wechselkurs, oder eine dauerhafte Stabilität gibt es nicht. Darüber hinaus ist auch keine Instanz vorhanden, welche einer negativen Entwicklung gegebenenfalls aktiv entgegen wirken könnte. Außerdem besteht die Gefahr, dass die zu bezahlenden Transaktionsgebühren eine Höhe erreichen, welche die Kryptowährung für die NutzerInnen schlichtweg uninteressant macht. Falls eine solche Erhöhung der Gebühren nur eine einzelne Währung betrifft, könnte es dazu führen, dass viele NutzerInnen auf eine andere Kryptowährung umsteigen. Natürlich ist die Gefahr der Abwanderung der TeilnehmerInnen bei einem am Markt der Kryptowährungen fest verankerten Größen wie Bitcoin oder auch bald Ether, eher unwahrscheinlich, jedoch nicht zwingend ausgeschlossen. Des Weiteren könnte eine solche Erhöhung der Transaktionsgebühren ebenfalls die Akzeptanz einer Kryptowährung durch Unternehmen beeinträchtigen.[77]

[76] Vgl. Münzer (2013), online abgerufen am 30.06.2017
[77] Vgl. Münzer (2013), online abgerufen am 30.06.2017

5. Neue Chancen/Möglichkeiten

Bitcoin an sich hat bereits einen hohen Stellenwert in der Welt der Kryptowährungen. Nicht zuletzt, weil es den Grundstein für alle nachfolgenden gelegt hat. Es bietet für Überweisungen und andere (Krypto-)Geldgeschäfte erhebliches Potential, wenn man zum Beispiel die Sicherheit und die zurzeit niedrigen Transaktionsgebühren betrachtet. Ethereum hingegen bietet mit der Möglichkeit, nicht nur Überweisungen zu tätigen, sondern eben auch Smart Contracts über die Blockchain abzubilden und laufen zu lassen, weitläufige Chancen für vielerlei Bereiche.

Smart Contracts können wie bereits erwähnt, je nachdem wie gut und umfangreich sie programmiert werden, nicht nur Bedingungen prüfen, sondern auch selbst vordefinierte Aktionen, wie etwa Überweisungen, tätigen. Grundsätzlich kann gesagt werden, dass alle Bestimmungen und Vereinbarungen, welche in Worte gefasst werden können, auch in einen Programmcode geschrieben werden können. Des Weiteren bieten sie, durch die Dezentralität und der damit verbundenen Sicherheit der Blockchain, einen sehr geeigneten Rahmen für unterschiedlichste Verwendungen. Verwendungen bei denen auf eine dritte Partei verzichtet werden möchte oder kann, die dabei rein die Kontroll- und Durchführungsfunktion innehat. Also anders ausgedrückt, um Vertrauen zwischen Parteien zu schaffen, wo es benötigt wird.[78]

5.1. Die DAO

Die beiden Brüder Christoph und Simon Jentzsch aus Mittweida gründeten zusammen mit ihrem Londoner Partner Stephan Tual, das Startup-Unternehmen Slock.it. Dieses Unternehmen sollte sich der Vernetzung aller möglichen alltäglichen Dinge, die vermietet werden können, über das Internet of Things widmen. Was dabei neuartig war, dass der gesamte Vorgang über die Ethereum-Blockchain laufen sollte. Also als Smart Contract. Slock.it sollte eine Online-Plattform werden, die einen Zugang für alle zu vermietenden, ungenutzten Ressourcen, wie zum Beispiel Parkplätze, unbenutzte Fahrzeuge oder leerstehende Wohnungen, bieten kann. Die Bezahlung und die darauffolgende Freigabe zur Nutzung sollte über die Blockchain abgehandelt und

[78] Vgl. Swan (2015), S. 16ff

so nachvollziehbar dokumentiert werden. Um diese Firma aufzubauen, benötigten sie jedoch Kapital. Sie wollten nicht von einer/einem InvestorIn abhängig sein, deshalb kreierten sie einen neuen Weg an Geld zu kommen.[79]

So gründeten sie das Unternehmen DAO. Ausgeschrieben bedeutet das „Decentralized Atonomous Organisation“ und heißt frei übersetzt: „dezentrale, selbstständige Organisation“. Es war jedoch keine Firmengründung im herkömmlichen Sinne. Sie wurde nirgends angemeldet und hat auch offiziell keinen Firmensitz. Die DAO existiert einzig und allein in der Ethereum Blockchain unter der in folgender „Abbildung 9“ zu sehenden Adresse: [80]

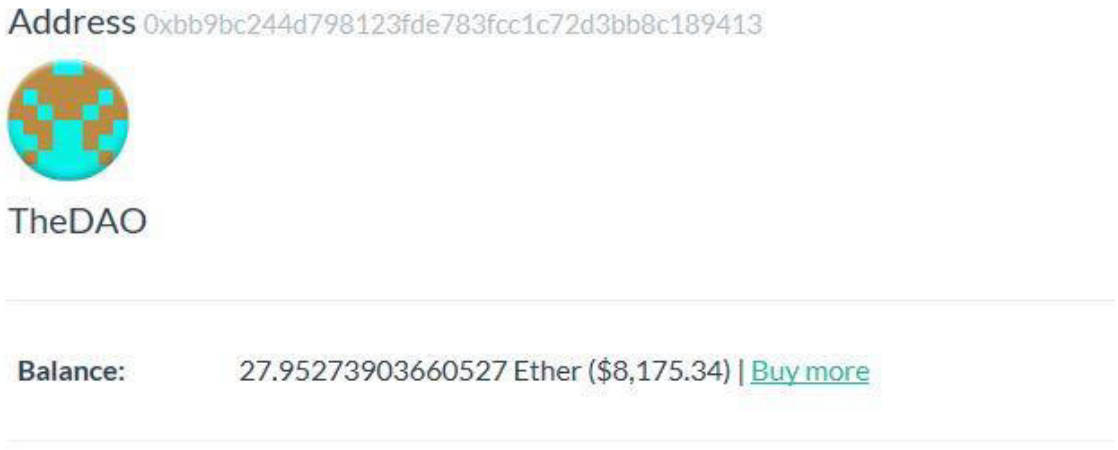

Abbildung 9 Die DAO in Ethereum[81]

Mit Stand 30.06.2017 befand sich in der DAO ein Kapital von nicht ganz 28 Ether. Dies ist im Vergleich zur anfänglichen Summe sehr gering, dazu später jedoch mehr. Die DAO wurde als Smart Contract programmiert und in die Blockchain geladen. Ihre Programmierer gaben ihr, durch den dahinterliegenden Code, die Aufgabe einer Investmentfirma. Die Idee hinter der Gründung DAO war es, dass eine real existierende Firma grundsätzlich nichts anderes als Verträge sind, die beachtet und ausgeführt werden. MitarbeiterInnen arbeiten auf Basis ihrer Arbeitsverträge und führen weitestgehend die darin niedergeschriebenen Anweisungen aus. Deshalb entwarfen sie den Code so, dass Ziele, Befugnisse und Zeiträume, in denen Schritte abgearbeitet wer-

[79] Vgl. Grassegger (2016), online abgerufen am 30.06.2017
[80] Vgl. Grassegger (2016), online abgerufen am 30.06.2017
[81] Die DAO in Ethereum, online im Internet: https://etherchain.org/account/0xbb9bc244d798123fde783fcc1c72d3bb8c189413#code, abgerufen am 30.06.2017 um 20:55 Uhr

den, genau vorgegeben sind. Dies war im Programmcode Großteils eine Abfolge von relativ einfachen Wenn-Dann-Entscheidungen. Der erste, klare Vorteil der DAO gegenüber einer realen Firma ist die Objektivität des Codes. Dieser hängt nicht von der Tagesverfassung oder dem Gemütszustand einer Managerin oder eines Managers ab und lässt sich auch, wenn dieser dahingehend programmiert wird, nicht bestechen. Über diese vertraglichen Grundregeln hinaus, welche im Code fest verankert sind, verfügt die DAO über ein virtuelles Abstimmungs-System, mit deren Hilfe die Personen, die an der DAO beteiligt sind, über die nächsten Schritte abstimmen können. Die Stimmrechte werden über so genannte DAO-Token verteilt. Jeder ausgeschüttete Token repräsentiert eine Stimme. Diese Token konnten – ähnlich wie bei der Gründung von Ethereum – über einen Crowdfunding-Prozess erstanden werden. Dabei konnten Interessierte in einem Zeitraum von vier Wochen durch die Überweisung von Ether an die DAO-Adresse Token kaufen. Der Betrag an Ether, welcher für 100 Token bezahlt werden musste, erhöhte sich in diesen vier Wochen. Der Verlauf ist in nachfolgender „Abbildung 10“ zu sehen.[82]

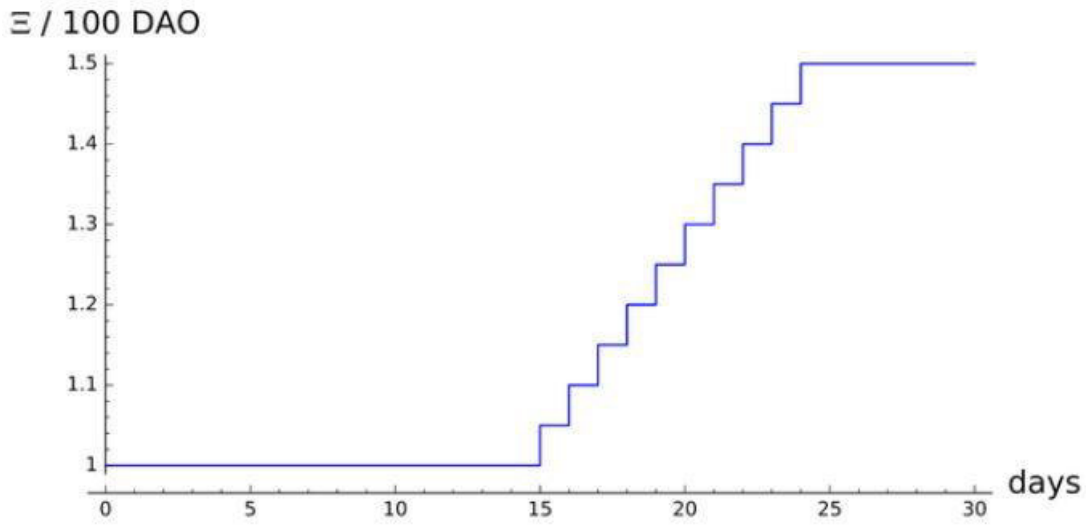

Abbildung 10 Verlauf Ether pro 100 DAO-Token[83]

Zu Beginn musste man für 100 Token einen Ether bezahlen. Ab dem 15. Tag erhöhte sich der Preis schrittweise bis ab dem 24. Tag 1,5 Ether zu bezahlen waren. Start dieses Crowdfundings war der 30.04.2016 und es konnte bis einschließlich

[82] Vgl. Grassegger (2016), online abgerufen am 30.06.2017
[83] Verlauf Ether pro 100 DAO-Token, online im Internet: https://altcoinspekulant.com/2016/05/18/der-ethereum-dao-das-200-millionen-dollar-ding/, abgerufen am 30.06.2017 um 21:36 Uhr

28.05.2016 investiert werden. Dabei kamen mehr als 144 Millionen Dollar zusammen.[84]

Nach dem Crowdfunding wurde die DAO gestartet. Ab diesem Zeitpunkt war es nicht einmal für die Entwickler selbst möglich, die DAO zu stoppen oder abzuschalten. Die einzige Möglichkeit wäre der einstimmige Beschluss aller Stimmberechtigten zur Auflösung der DAO. Bei größeren Unstimmigkeiten bezüglich der Weiterentwicklung wäre es auch denkbar gewesen, dass sich Tochterfirmen aus der DAO bilden würden, die eigenständig mit dem Kapital ihrer Interessenten investieren könnten. Die gut 144 Millionen Dollar, die eingenommen wurden, befanden sich also in Form von Ether sozusagen in der Firmenkassa des Unternehmens – also auf dem in „Abbildung 9“ zu sehenden Ethereum-Account. Da es sich um eine Investmentfirma handelt, konnte ab diesem Zeitpunkt durch die Stimmberechtigten entschieden werden, welchen (Startup-) Unternehmen das Geld zur Verfügung gestellt werden soll, welche Produkte gekauft oder welche Agentur mit einer Aufgabe beauftragt wird. Es konnte auf elektronischem Weg ein neuer Vorschlag eingebracht werden. Dieser wurde dann durch reale Personen, darunter einige Ethereum-EntwicklerInnen, auf formale Korrektheit geprüft und der DAO zwölf Wochen lang zur Abstimmung vorgelegt. In dieser Zeit konnten die InvestorInnen mit ihren Stimmrechten entweder dem Vorschlag zustimmen, oder diesen ablehnen. Als ersten Investitionsvorschlag wurde Slock.it durch die Entwickler selbst eingebracht und sollte so die erst Investition aus der DAO erhalten. Im Gegenzug dafür würde die DAO entweder eine Gewinnbeteiligung erhalten, oder selbst Kunde von Slock.it werden. Die Möglichkeiten schienen grenzenlos. Es war zu diesem Zeitpunkt jedoch nicht geklärt, ob und vor allem wer zur Verantwortung gezogen werden kann, wenn die DAO in etwas Illegales wie zum Beispiel eine Drogenfarm oder ein Zwangsarbeitslager investieren würde. Die DAO selbst existiert ja nur in der Blockchain und diese hat durch ihre Dezentralität keinen festen Standort. Es könnte auch bei den Abstimmenden angesetzt werden. Zur Gänze wurde diese Frage jedoch nicht geklärt.[85]

Soweit sollte es jedoch nicht kommen. Im Juni 2016 ereignete sich ein heute als „DAO-Hack“ bekannter Vorfall. Dabei verwendete eine/ein NutzerIn ein Sicherheitsfeature, welches eigentlich die eigenen Token schützen sollte um sich selbst zu bereichern. Dieses Sicherheitsfeature funktionierte folgendermaßen. Wenn die DAO

[84] Vgl. Fiedler (2016), online abgerufen am 30.06.2017
[85] Vgl. Grassegger (2016), online abgerufen am 30.06.2017

per Mehrheitsbeschluss eine Investition getätigt hat, mit der eine/ein NutzerIn nicht einverstanden war, konnte diese Person die eigenen Token auf eine Art „Unterkonto“ verschieben und so aus der DAO nehmen. Die/Der HackerIn machte sich einen kleinen Fehler im Programmcode der DAO zu Nutze und so gelang es die Anzahl der eigenen Token sehr oft auf ein solches Unterkonto zu verschieben. Auf diesem Weg war es ihr/ihm möglich, Token im damaligen Wert von 53 Millionen Dollar zu „parken“. Diese Token waren jedoch noch nicht ganz verloren. Eine zweite Sicherheitsfunktion sah vor, dass die Token auf diesem Unterkonto für 28 Tage eingefroren sind. Diese 28 Tage mussten vergehen, bevor sie dann wieder in Ether getauscht werden konnten und so wirklich aus der DAO gezogen werden konnten. So lange war also Zeit, um zu reagieren. Doch wie sollte oder konnte reagiert werden? Die DAO lief dezentral und autonom – also selbstständig. Ein Eingreifen der Entwickler war also nicht möglich. Dies konnte nur eine übergeordnete Instanz machen. In diesem Fall war das nur das Entwicklerteam von Ethereum. In einer ersten Stellungnahme von Vitalik Buterin hieß es, dass sich Ethereum nicht einmischen werden, da es sich rein um einen Programmfehler, und nicht um das Verschulden der Blockchain an sich handeln würde. In der darauffolgenden Zeit häuften sich hitzige Diskussionen und Schuldzuweisungen in den Ethereum- und DAO-Foren, bis dadurch ein Handlungsbedarf für Ethereum entstand. So entschied man sich knapp vor Ablauf dieser 28-Tage-Frist dazu, mittels eines Hard Forks einzugreifen. Dabei wurde den BesitzerInnen der DAO-Token ermöglicht, diese mit einem definierten Wechselkurs wieder in Ether zu tauschen und so gefahrlos aus der DAO zu ziehen. Mit dieser Hard Fork spaltete sich die Ethereum-Welt jedoch in zwei Teile. Der Großteil der NutzerInnen stimmte durch das damit verbundene Update der Änderung zu. Einige sahen darin jedoch eine Verletzung der Ideale von Ethereum. Sie verweigerten das Update. So konnte die DAO – mit den verbleibenden NutzerInnen auf der alten Blockchain weiter existieren. Darunter war auch die/der HackerIn mit den erbeuteten Token.[86]

Diese Token wurden genau genommen niemandem gestohlen. Ihre Erschaffung war durch den Programmfehler möglich und die/der HackerIn fand nur einen Weg, um sie zu generieren. Die alte Ethereum Blockchain wurde von einigen NutzerInnen weiter verwendet und es entstand daraus sehr bald eine Parallelwährung – Ethereum Classic. Durch das Interesse einiger Leute an dieser Währung entstand eine Nachfrage und daraus sogar ein Wechselkurs zu anderen Kryptowährungen. So war es der/dem

[86] Vgl. Biederbeck (2016), online abgerufen am 30.06.2017

HackerIn nach einiger Zeit durch mehrere, verschachtelte Transaktionen möglich, einen Teil der Token in Bitcoin zu tauschen. Ein Großteil der Token ist jedoch bis heute auf der Ethereum-Classic-Blockchain „geparkt".[87] Mit Stand vom 01.07.2017 waren es Ether im Wert von ungefähr 58 Millionen Dollar und die letzten abgehenden Transaktionen waren im Dezember 2016. Ob und vor allem wie die/der HackerIn an diese Einheiten kommt, bleibt abzuwarten. [88]

5.2. Energiemarkt

Von vielen Energieversorgern wurde oder wird die Technologie der Blockchain – allen voran Ethereum – als komfortable und auch kostengünstige Alternative für den Bezahlvorgang von Strom oder Gas gesehen. Die mehr oder weniger gleichbleibende Nutzung der Energie könnte über so genannte Smart-Meter, also intelligente Verbrauchszähler, den Energieversorgern über die Blockchain mitgeteilt werden. Anschließend könnte der Bezahlvorgang ebenfalls über die Blockchain abgehandelt werden. Smart-Meter sind keine Zukunftsmusik. Diese sind bereits in vielen Haushalten installiert. Würde die Blockchain-Technologie jedoch als reine Erfassungs- und Bezahl-Plattform angesehen werden, würde dies den umfangreichen Möglichkeiten derselben nicht gerecht werden. Sie würde schlichtweg unterschätzt werden.[89]
Durch den Grundsatz der Blockchain, Vertrauen dort zu schaffen, wo und wozu auch immer es benötigt wird, ergeben sich auch für den Energiemarkt viele Neuerungen. Für die großen Energieversorger, die konventionell für dieses Vertrauen gestanden sind, könnte sich so zum Teil die eigene Marktposition verschlechtern und ihre Dienste könnten immer weniger gefragt sein.

Eines der Unternehmen, welches diese neue Technologie bereits für sich entdeckt hat, ist die sonnen GmbH mit Sitz in Deutschland. Sie ist Anbieter für Batteriespeicher-Systeme – überwiegend im Privatbereich für Einfamilienhäuser oder Wohnungen. Die Speicher werden teilweise für die Nutzung mit einer Photovoltaik-Anlage

[87] Adresse in Bitcoin Classic online einsehbar mit aktuellem Ether-Stand: https://gastracker.io/addr/0x5e8f0e63e7614c47079a41ad4c37be7def06df5a
[88] Vgl. Giese (2016), online abgerufen am 30.06.2017
[89] Vgl. Erle (2017), online abgerufen am 01.07.2017

oder als privater Puffer gegen Ausfälle in der Energieversorgung vom Netz verwendet. Die Batteriespeicher gibt es in unterschiedlichen Größen, je nach Bedarf der KundInnen. Diese Batteriespeicher besitzen jeweils eine Adresse und sind über einen Smart Contract in der Ethereum-Blockchain miteinander verbunden. In der Blockchain werden Informationen über die einzelnen Speicher fälschungssicher dokumentiert und sind so für alle NutzerInnen einsehbar. Unter anderem werden Aufzeichnungen darüber gemacht, welcher Speicher wann und vor allem wie viel Energie vom Netz bezieht, durch eine eventuell vorhandene Photovoltaik-Anlage erhält oder selbst in das Netz zurückspeist. Diese Informationen werden als fest definiertes Protokoll in der Blockchain gespeichert. So werden die Details zu den privaten Stromspeichern für die sogenannte sonnenCommunity zur Verfügung gestellt. Diese sonnenCommunity ist eine Art Verzeichnis, in der alle Details zu den im Netz befindlichen Speichern abgebildet sind. Durch die Zusammenarbeit von sonnen mit TenneT, einem deutschen Netzbetreiber, und dem IT-Spezialisten IBM ist folgende Blockchain-Anwendung möglich. Redispatch-Maßnahmen sind Vorgänge die notwendig sind, um auftretende Energiespitzen, welche zum Beispiel durch starke Winde in Norddeutschland erzeugt werden, und aus Kapazitätsgründen nicht vom Netz zu den VerbraucheInnen transportiert werden können, abzuwenden. Das hohe Energievorkommen kann nicht durch das Netzt geleitet werden und würde so zu Problemen führen. Aus diesem Grund werden zum Schutz vor solchen Überangeboten an Energie zum Beispiel Windkraftanlagen gedrosselt, oder zur Gänze vom Netz genommen. Dabei spricht man von einer Redispatch-Maßnahme. Durch die sonnenCommunity ist es möglich, zumindest einen kleinen Teil dieses Überangebots trotzdem zu nutzen und in die Pufferspeicher der privaten Haushalte zu laden. Dadurch bleibt die Windenergie nicht ungenutzt und die Haushalte erhalten im Gegenzug sehr günstigen Strom. Dieses Überangebot im Norden hat häufig einen Gegenspieler im Süden. Dort kann teilweise der Bedarf an Energie nicht nur durch erneuerbare Energiequellen abgedeckt werden und muss weiterhin durch Kraftwerke, die mit fossilen Brennstoffen betrieben werden, aufgebracht werden. Dem kann ebenfalls die sonnenCommunity – im Moment zumindest im kleinen Rahmen – entgegenwirken. Durch die aus Photovoltaik-Anlagen zur Verfügung gestellte, in den Batterien gespeicherte Energie, kann dieser Bedarf zum Teil gedeckt werden. Die privaten Haushalte erhalten dafür, voll automatisch über den auf der Blockchain laufenden Smart Contract, eine Vergütung für diese bereitgestellte Energie. Diese Blockchain-

Anwendung macht es also möglich, dass „saubere“ Energie genutzt wird und weniger fossile Brennstoffe verbraucht werden. Mit nur ein paar Tausend Anlagen in Deutschland ist dies zwar noch keine endgültige Lösung, setzt jedoch bereits einen Schritt in die richtige Richtung. Darüber hinaus wird die Nutzung von nicht benötigter Photovoltaik-Energie für Haushalte immer interessanter, da ständig Förderungen für die Rückspeisung ins Netz auslaufen und so für den bereitgestellten Strom keine Einnahmen mehr zu erwarten sind.[90]

Eine weitere Anwendung der Blockchain auf dem Energiemarkt ist das Konzept der Grünstrom-Jetons, das der Stadtwerke Energie Verbund aus Nordrhein-Westfalen betreibt. Dieses Konzept spricht vor allem KundInnen an, die bei ihrem Verbrauch einen Wert auf einen möglichst hohen Anteil an Ökostrom legen. Wird bei einem anderen Anbieter ein herkömmlicher Tarif für Ökostrom gewählt, gibt es vom Energielieferanten nur die Zusicherung, dass ein gewisser Teil des von ihm eingespeisten Stroms aus erneuerbaren Energiequellen kommt. Im Netzt steht dann meistens eine nicht definierbare Mischung aus Öko- und herkömmlich produziertem Strom zur Verfügung. Die/Der VerbraucherIn weiß also nicht, ob die genutzte Energie nachhaltig produziert wurde, oder eben nicht. Genau dort setzen die Grünenergie-Jetons an. Durch einen Abgleich des Grünstrom-Index, der regionale Informationen zum aktuell zur Verfügung stehenden Strom enthält, mit dem in der Blockchain dokumentierten Verbrauch der Kundin/des Kunden, kann genau beurteilt werden, wie viel Ökostrom verwendet wurde. So sieht die/der VerbraucherIn genau, wie „grün“ ihr/sein verbrauchter Strom war. Darüber hinaus steckt auch eine Art Anreizsystem dahinter. Je höher der Anteil an verbrauchtem Ökostrom ist, desto mehr Grünstrom-Jetons werden auf das Blockchain-Konto des Haushaltes gutgeschrieben. Diese Jetons sollen zukünftig auch getauscht und gehandelt werden können. Wie und zu welchen Konditionen das genau ablaufen soll, ist zurzeit noch nicht bekannt.[91]
Im Fall der Grünstrom-Jetons besteht zurzeit der Anreiz für die VerbraucherInnen nur darin, dass sie über die Herkunft ihres verbrauchten Stroms relativ genau im Klaren sind. Um wirklich das Interesse der breiten Masse wecken zu können, bedarf es meiner Meinung nach einiger Neuerungen, die für die KundInnen einen gewissen Mehrwert versprechen und auch halten. Für den Stadtwerke Energie Verbund hat diese

[90] Vgl. Weimann (2017), online abgerufen am 01.07.2017
[91] Vgl. Erle (2017), online abgerufen am 01.07.2017

genaue Dokumentation über die Blockchain natürlich auch einen Vorteil. Es werden damit detaillierte Aufzeichnungen über den Energieverbrauch und somit über die Gewohnheiten einzelner Haushalte geführt. Wenn das jemand nicht möchte, wäre das für mich nur zu gut verständlich.

Bereits heute gibt es noch einige weitere Anwendungen auf dem Energiemarkt, welche über eine Blockchain abgewickelt werden. So zum Beispiel ein Zusammenschluss von einigen Haushalten in Brooklyn. Das so genannte Brooklyn Microgrid. Dabei stellen Personen, die bei ihrer Photovoltaik-Anlage überschüssig vorhandene Energie produzieren, diese anderen NutzerInnen in dem Microgrid direkt zur Verfügung. Diese Ethereum-basierende Anwendung macht den direkten Verkauf von Energie zwischen den einzelnen Parteien möglich und kann so Angebot und Nachfrage regeln, noch bevor überhaupt in das öffentliche Netz eingespeist oder daraus bezogen wird.[92]

[92] Vgl. Cardwell (2017), online abgerufen am 01.07.2017

6. Zusammenfassung und Zukunftsaussichten

Bitcoin zeigt im Moment, dass der Wert einer digitalen Währung, die nicht durch eine Noten- oder Zentralbank gesteuert wird, den einer Feinunze Gold weit hinter sich lassen kann. Eine Aussage darüber zu treffen, wie beständig dieser Wert ist und vor allem in Zukunft sein wird, wäre jedoch reine Spekulation.

In der heutigen Gesellschaft, in der dem Internet eine immer größere Bedeutung zukommt, ist die Sicherheit ein wichtiges Thema. Fast täglich hört man von neuen Hacker-Angriffen in beinahe allen Bereichen des täglichen Lebens. Dadurch wird das Vertrauen in Online-Plattformen immer öfter auf die Probe gestellt.

Die Blockchain bietet die Möglichkeit, Vertrauen online dort zu schaffen, wo es benötigt wird. Sei es in finanziellen, oder technischen Dingen. Das alles funktioniert durch ein dezentrales Netzwerk, welches aufgrund seines Aufbaus als überaus vertrauenswürdig und fälschungssicher gilt. Eine der wichtigsten und wohl schwierigsten Aufgaben der Zukunft wird es sein, die Sicherheit dieser Systeme langfristig und garantiert aufrecht zu erhalten. Aktuelle Vorkommnisse zeigen immer wieder, dass vermeintlich als sicher eingestufte Netzwerke dennoch gehackt und mit Schadsoftware infiziert werden können. Sehr oft ist zu beobachten, dass dadurch beinahe ein Wettrüsten zwischen EntwicklerInnen und HackerInnen entsteht. Häufig werden erst durch HackerInnen Sicherheitslücken entdeckt, welche den ProgrammiererInnen zuvor nicht bewusst waren.

Meiner Meinung nach muss zur Beurteilung der Sicherheit die Ethereum-Blockchain an sich und die darin ausgeführten Smart Contracts getrennt voneinander betrachtet werden. Nach intensiver Auseinandersetzung mit dem Aufbau und der Funktionsweise der Blockchain, ist es meiner Ansicht nach tatsächlich kaum vorstellbar, diese zu verfälschen. Es müsste mehr als 50% der gesamten Rechenleistung des Blockchain-Netzwerks aufgebracht werden, um eine Verfälschung erreichen zu können. Als Einzelperson ist das meiner Ansicht nach unmöglich, ob dies jedoch durch Zusammenschlüsse großer Rechenzentren theoretisch möglich wäre, lässt sich mit meinem Wissensstand nicht mit Sicherheit ausschließen.

Bei den Smart Contracts handelt es sich, wie in meiner Arbeit ausführlich behandelt, um Verträge, welche von NutzerInnen programmiert werden. Hierbei lässt sich nicht ausschließen, dass Programmierfehler oder Sicherheitslücken auftreten, welche von HackerInnen ausgenutzt werden können. Der im Kapitel 5.1 beschriebene Hacker-

angriff auf die Blockchain-Anwendung DAO, beruhte auf einem derartigen Programmierfehler. Somit lässt sich meiner Meinung nach feststellen, dass das eigentliche Sicherheitsrisiko in den meisten Fällen nicht die Blockchain an sich, sondern das darin enthaltene Programm darstellt.

Eine grundlegende Frage, welche noch viele Rechtswissenschaftler beschäftigen wird, ist wer in einem eventuellen Schadensfall die Haftung für entwendetes Kapital übernimmt. Die EntwicklerInnen der Blockchain könnten ausschließlich dann zur Verantwortung gezogen werden, wenn der Fehler in der Blockchain direkt liegen würde. Dieser Fall wird jedoch aus den oben genannten Gründen meiner Meinung nach kaum auftreten. Wenn der Schadensfall auf einem Fehler im Smart Contract beruht, könnte die/der ProgrammiererIn meines Erachtens sehr wohl zur Verantwortung gezogen werden. Dieser Gefahr sollte sich die/der ErstellerIn eines Smart Contracts bewusst sein und durch eine genaue Codeanalyse alle Eventualitäten betrachten. Um dieser Haftung für Schäden durch Fehler des erstellten Programms zu entgehen, wäre der Weg über einen Haftungsausschluss die für mich einzige Möglichkeit. Ob dies jedoch rechtlich überhaupt möglich ist, müsste genauer untersucht werden.

Schließlich bleibt als RisikoträgerIn einzig und allein die durch die Nutzung des Smart Contracts geschädigte Person. Würden sich Blockchain basierte Online-Systeme zukünftig tatsächlich ins alltägliche Leben integrieren, müsste jedes Gesellschaftsmitglied das Risiko durch die Verwendung der Smart Contracts selbst auf sich nehmen. Dadurch stellt sich für mich hier die Frage, ob sich eine derartige Technologie alltäglich verwenden lässt. Die gesellschaftliche Bereitschaft dieses Risiko selbst zu tragen ist für mich fraglich und daher bin ich mir nicht ganz sicher, ob sich diese Technik wirklich auch für die Allgemeinheit durchsetzen kann.

Abschließend komme ich zu der Ansicht, dass immer mehr Bereiche von dieser neuen Technologie profitieren können und werden. Jedoch gibt es vor allem in Rechtlichen und sicherheitsrelevanten Fragen Klärungsbedarf, welche vor allem für die Massentauglichkeit dieser Systeme von enormer Bedeutung sind.

Mit Spannung wird von mir verfolgt werden, wie sich der Wert einzelner Kryptowährungen zukünftig entwickelt und welche Neuerungen die nächsten Entwicklungsschritte der Blockchain-Anwendungen bringen.

III. Literaturverzeichnis

Biederbeck, M. (2016)
Der DAO-Hack: Ein Blockchain-Krimi aus Sachsen, online im Internet: https://www.wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde, veröffentlicht am 21.11.2016

Bosk, H. (2015)
Was ist Bitcoin?, online im Internet: http://www.novalnet.de/magazin/was-ist-bitcoin, veröffentlicht am 26.01.2015

Brühl, V. (2017)
Bitcoins, Blockchain und Distributed Ledgers, in: Wirtschaftsdienst (Volume 97, Issue 2), Hrsg. ZBW – Leibnitz-Informationszentrum Wirtschaft, Berlin Heidelberg: Springer, 2017

Buntinx, J.P. (2017)
What is Ethereum's Metropolis Hard Fork?, online im Internet: https://themerkle.com/what-is-ethereums-metropolis-hard-fork/, veröffentlicht am 17.03.2017

Buterin, V. (2014)
Ethereum White Paper – A Next Generation Smart Contract & Decentralized Application Platform, online im Internet: http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, veröffentlicht am 23.01.2014

Buterin, V. (2014)
Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform, online im Internet: https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/, veröffentlicht am 23.01.2014

Buterin, V. (2017)
Roundup Round III, online im Internet: https://blog.ethereum.org/2017/05/24/roundup-round-iii/, veröffentlicht am 24.05.2017

Cardwell, D. (2017)
Solar Experiment Lets Neighbors Trade Energy Among Themselves, online im Internet: https://www.nytimes.com/2017/03/13/business/energy-environment/brooklyn-solar-grid-energy-trading.html, veröffentlicht am 13.03.2017

Castor, A. (2017)
Ethereum's Difficulty Bomb: All Smoke, No Fire?, online im Internet: http://www.coindesk.com/ethereums-difficulty-bomb-smoke-no-fire/, veröffentlicht am 08.04.2017

Donnelly, J. (2016)
Ethereum Blockchain Project Launches First Production Release, online im Internet: http://www.coindesk.com/ethereum-blockchain-homestead/, veröffentlicht am 14.03.2016

Fiedler, L. (2016)
Der Ethereum DAO – Das 200 Millionen Dollar Ding!, online im Internet: https://altcoinspekulant.com/2016/05/18/der-ethereum-dao-das-200-millionen-dollar-ding/, veröffentlicht am 18.05.2017

Edwards, D. (2017)
Proof of Stake (Casper), Ether and Compund Interest gains, online im Internet: https://steemit.com/ethereum/@dana-edwards/proof-of-stake-casper-ether-and-compound-interest-gains, veröffentlicht am 05.05.2017

Erle, C. (2017)
Warum die Blockchain zur Disruption auf dem Energiemarkt führen kann, online im Internet: http://www.management-circle.de/blog/warum-die-blockchain-zur-disruption-auf-dem-energiemarkt-fuehren-kann/, veröffentlicht am 02.03.2017

Gerring, T. (2016)
Cut and try: building a dream, online im Internet: https://blog.ethereum.org/2016/02/09/cut-and-try-building-a-dream/, veröffentlicht am 09.02.2016

Giese, P. (2016)
DAO-Hacker tauscht ETC gegen Bitcoin, online im Internet: https://www.btc-echo.de/dao-hacker-tauscht-etc-gegen-bitcoin/, veröffentlicht am 29.110.2016

Giese, P. (2017)
Casper: Wie Ethereum seine Blockchain neu erfinden will, online im Internet: https://www.btc-echo.de/casper-wie-ethereum-seine-blockchain-neu-erfinden-will/, veröffentlicht am 21.01.2017

Grassegger, H. (2016)
Die erste Firma ohne Menschen, online im Internet: http://www.zeit.de/digital/internet/2016-05/blockchain-dao-crowdfunding-rekord-ethereum/komplettansicht, veröffentlicht am 26.05.2016

Gupta, V. (2015)
The Ethereum Launch Process, online im Internet: https://blog.ethereum.org/2015/03/03/ethereum-launch-process/, veröffentlicht am 03.03.2015

Kannenberg, A. (2016)
Bitcoin: Belohnung für Miner halbiert sich auf 12,5 Bitcoin, online im Internet: https://www.heise.de/newsticker/meldung/Bitcoin-Belohnung-fuer-Miner-halbiert-sich-auf-12-5-Bitcoin-3262822.html, veröffentlicht am 10.07.2016

Keßler, M. (2015)
Bitcoin Wallet – was ist das?, online im Internet: http://praxistipps.chip.de/bitcoin-wallet-was-ist-das_39912, veröffentlicht am 01.04.2015

Kühl, E. (2016)
Craig Wright erklärt sich zum Bitcoin-Erfinder, online im Internet: http://www.zeit.de/digital/internet/2016-05/bitcoin-erfinder-satoshi-craig-wright, veröffentlicht am 02.05.2016

Kryptocoinr (2016)
Ethereum: Entwicklung Anzahl der Ether-Einheiten, online im Internet: http://kryptocoins.net/2016/02/ethereum-entwicklung-anzahl-der-ether-einheiten/, veröffentlicht am 07.02.2016

Miller, M. (2017)
Vom Bitoin über den Bitcent zum Satoshi!, online im Internet: http://www.investor-verlag.de/devisen/bitcoin/vom-bitcoin-ueber-den-bitcent-zum-satoshi/, veröffentlicht am 12.01.2017

Münzer, J. (2013)
Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, online im Internet: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html, veröffentlicht am 19.12.2013

Obermeier, L. (2017)
So generieren Sie die Kryptowährung selbst, online im Internet: http://www.focus.de/digital/praxistipps/bitcoin-mining-so-generieren-sie-die-kryptowaehrung-selbst_id_6570065.html, veröffentlicht am 23.05.2017

Scheurer, B. (2017)
Bitcoin erhöht Transaktionsgebühren: Was bedeutet das für Startups?, online im Internet: https://www.btc-echo.de/bitcoin-erhoeht-transaktionsgebuehren-was-bedeutet-das-fuer-startups/, veröffentlicht am 13.06.2017

Schönleben, D. (2016)
Hat Craig Steven Wright wirklich Bitcoin erfunden?, online im Internet: https://www.wired.de/collection/life/craig-steven-wright-will-beweisen-dass-er-wirklich-bitcoin-erfunden-hat, veröffentlicht am 02.05.2016

Silva, C. (2017)
Ethereum's Road Map For 2017, online im Internet: https://www.ethnews.com/ethereums-road-map-for-2017, veröffentlicht am 25.02.2017

Swan, M. (2015)
Blockchain – Blueprint for a New Economy, First Release, O'Reilly Media, Inc., Kalifornien, 2015

Valfells, S. / Egilsson, J.H. (2016)
Minting Money With Megawatts, in: Proceedings of the IEEE (Volume: 104, Issue: 9), Hrsg. Institute of Electrical and Electronics Engineers, New York, 2016

Weimann, S. (2017)
Die Blockchain ist die nächste Evolutionsstufe der dezentralen Energieversorgung, online im Internet: https://www.sonnenbatterie.de/de/die-blockchain-ist-die-naechste-evolutionsstufe-der-dezentralen-energieversorgung, veröffentlicht am 02.05.2017

Weiss, H. / Moutafis, J. (2013)
Ist Bitcoin richtiges Geld?, online im Internet: http://www.chip.de/artikel/Bitcoin-So-funktioniert-die-virtuelle-Waehrung_64702069.html, veröffentlicht am 29.10.2013

Wood, G. (2014)
Ethereum: A Secure Decentralised Generalised Transaction Ledger, online im Internet: http://gavwood.com/paper.pdf, veröffentlicht am 06.04.2014

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Haid, den 07. Juli 2017

Klaus Froschauer