Funktionsweise einer Blockchain am Beispiel von Bitcoin

Elias Wachmann

8 C

Betreuer: Mag. Joachim Maderer

BG/BRG Fürstenfeld

Realschulstraße 6

8280 Fürstenfeld

26. Februar 2019

Abstract

Die Blockchain, eine dezentrale Datenbank mit kryptografischer Verschlüsselung, ist Basis von digitalen Währungen (Kryptowährungen) und weiterer Anwendungen. Die Arbeit beantwortet die Fragen, wie eine Blockchain funktioniert, welche Probleme auftreten können und wie diese gelöst werden. Der theoretische Teil behandelt reproduktiv die Technik der Blockchain, sowie wirtschaftliche Themen im Bezug auf die Kryptowährungen. Anschließend stellt die Dokumentation des Baues eines Kryptowährungs-Mining-Computers die Praxis dar. Durch Berechnungen zur Rentabilität eines Miners konnte der Strompreis als größter Faktor bei der Profitabilität des Minings ausgemacht werden. Eine Neuberechnung des CO_2-Ausstoßes pro Transaktion ergab einen höheren Wert als der bestehende Literaturwert, was auf den Anstieg der Berechnungsschwierigkeit zurückzuführen ist.

Inhaltsverzeichnis

1 Einleitung

Blockchain und Bitcoin waren vor einem Jahr kaum jemanden ein Begriff. Heute, nach zahlreichen Berichten über die Blockchain und öffentlichem Interesse an den Kryptowährungen, kennt sie beinahe jeder. Doch wie genau die dahinterliegenden Techniken funktionieren, ist oft unklar. Hier setzt die Arbeit an und klärt die Kernfrage: „Was ist eine Blockchain und wie funktioniert sie?“

Ziel ist es, durch die Vernetzung mit dem Anwendungsbeispiel Bitcoin die Techniken zu schildern. Die Arbeit vermittelt einen grundlegenden Überblick der technischen Konzepte hinter Blockchain-Anwendungen und dem Handel von Kryptowährungen. Der reproduktive Teil der Arbeit vernetzt dabei das Wissen aus dem technischen Teil mit dem Wirtschaftssegment. Der produktive Teil beschäftigt sich, für das tiefere Verständnis der Funktionsweise einer Blockchain, mit dem Bau zweier Kryptowährungs-Miner. Außerdem wird die theoretische Rentabilität eines Miners und auch die Umweltauswirkungen der selbstgebauten Miner mittels Rechnungen analysiert. Somit verfügt die Arbeit auch über einen produktiven theoretischen Teil. Die Methodik des praktischen Abschnittes beruht hingegen auf der Dokumentation des Baues der beiden Miner.

Zuerst gibt die Arbeit einen Überblick der Konzepte und Techniken einer Blockchain, verdeutlicht Probleme anhand der Bitcoin Blockchain und zählt Anwendungsgebiete auf. Was ein Miner ist, welche Arten es gibt und wie rentabel er ist, wird theoretisch sowie anhand von zwei selbst gebauten Mining-Computern dargestellt. Eine Analyse der Umweltauswirkungen des Minings rundet den produktiven Teil ab. Im letzten Kapitel wird geklärt, wie man Kryptowährungen handelt und aufbewahrt.

Aus Gründen der leichteren Lesbarkeit wird in dieser Arbeit die geschlechtsspezifische Differenzierung nicht berücksichtigt. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für beide Geschlechter.

2 Konzepte einer Blockchain

Die Blockchain, eine Art dezentralisierte Datenbank, dient als wichtiger Baustein für die dezentralisierten und kryptografisch gesicherten Kryptowährungen (Franco, 2014). In den folgenden Unterkapiteln werden die grundlegenden Konzepte einer Blockchain mit Hilfe des Beispiels Bitcoin erklärt.

Bitcoin ist eine sogenannte Kryptowährung, eine digitale durch kryptografische Methoden gesicherte Währung. Obwohl der Bitcoin die höchste Marktkapitalisierung aufweist, entgeht er nicht den (teils) starken Kursschwankungen (CoinMarketCap, 2018). Jedoch sind einige Parameter festgelegt, so beispielsweise die maximale Anzahl an Währungseinheiten, welche auf 21 Millionen Bitcoins limitiert ist (Franco, 2014, S. 23). Die folgenden drei Unterpunkte sind nicht nur für Bitcoin, sondern auch für einen Großteil der anderen Kryptowährungen gültig.

2.1 Open Source

Übersetzt man „Open Source“ wortwörtlich, erhält man „offene Quelle“, was zu bedeuten hat, dass das Produkt, beim Bitcoin das Protokoll oder der Code, öffentlich verfügbar ist. Open Source Code bietet, im Vergleich zum nicht öffentlichen Code, den Vorteil, dass er leicht von jeder beliebigen Person angesehen und modifiziert werden kann. Somit kann jeder Interessent, der im Fall von Bitcoin C++ lesen kann, das Programm auf Fehler überprüfen und es eventuell selbst weiterentwickeln. Verglichen mit anderen digitalen Währungssystemen bieten solche, die auf Open Source Code beruhen den Vorteil, transparenter zu sein. Aus diesem Grund kann der Endnutzer selbst den Code auf die Richtigkeit überprüfen. (Franco, 2014, S. 5)

2.2 Dezentralisierung

Bitcoin verzichtet auf zentrale Rechenzentren, wie Banken sie betreiben. Stattdessen wird auf ein *„Peer-to-Peer“* (kurz *„P2P“*) Netzwerk aufgebaut, in welchem die teilnehmenden *„nodes“* (=Rechner) sich direkt untereinander austauschen. Dies wird dezentralisiert genannt, da es keinen zentralen Server gibt, der eine zentrale Datenbank verwaltet. Die Daten (u.a. Transaktionsadressen und Geldmengen), die durch die Verwendung von Bitcoin erzeugt werden, sind in der Blockchain gespeichert. Anstelle des zentralen Servers gibt es

sogenannte *„full-nodes“*. Das sind jene Rechner, die eine Kopie einer gesamten Blockchain gespeichert haben. Durch diesen dezentralen Aufbau würde eine Manipulation an einer Transaktion sofort auffallen, weil der Betrüger in seiner Kopie der Blockchain andere Daten und somit eine Diskrepanz vorliegen hat. Dadurch kann, im Gegensatz zum zentralen System, ein erfolgreicher Angriff auf einen der Server leicht identifiziert und abgewehrt werden. (Tapscott & Tapscott, 2016, S. 53)

Trotz des dezentralen Aufbaus meinen viele Kritiker, wegen vieler Betrügereien im Kryptowährungs-Raum, dass Bitcoin eine Betrugsmasche ist. *„Some critics have argued that Bitcoin is a Ponzi scheme. It is not.”* (Franco, 2014, S. 4) Wie Franco erklärt, ist Bitcoin kein Ponzi-Schema (auch Schneeballsystem genannt). Ein Schneeballsystem basiert auf einer zentralen Person oder Gruppe, welche die hohen versprochenen Investitionsgewinne der alten Investoren mit den Einnahmen der neuen Anleger deckt. Wegen der dezentralen Natur von Bitcoin, kann keine einzelne Person die Währung steuern; Ergo ist kein Schneeballsystem möglich. Das Verwalten der eigenen Bitcoins, sowie deren Transaktionen wird vom Benutzer selbst kontrolliert und kann nicht durch Dritte oder die Software geändert oder manipuliert werden. Aus diesem Grund kann eine Transaktion jedoch auch nicht wieder rückgängig gemacht werden.
(Franco, 2014, S. 9)

2.3 Public Asset Ledger

„Public Asset Ledger“, im deutschen auch öffentliches Vermögensbuch, beschreibt die Art in der Vermögenswerte und Transaktionen der Bitcoin-Nutzer gehandhabt werden. Jeder Nutzer kann durch eine eindeutig zugewiesene Bitcoin-Adresse (z.B.: *'15vM9wd9goyK8gSnxmtPDCdUQnbnJrqaji'*) klar identifiziert werden. Der Public Asset *Ledger* legt alle Adressen und auch den Kontostand der Adressen offen.

Aufgrund dieses Aufbaus kann man theoretisch nur das Vermögen und die Transaktionen einer gewissen Adresse sehen, nicht aber den Namen der dahinterstehenden Person. Es ist jedoch möglich, mit Hilfe von Mustern in den Transaktionen Rückschlüsse auf die Person zu machen. Somit könnte beispielsweise ein Kollege einem anderen Kollegen Bitcoins überweisen und anschließend, nachdem er die Adresse kennt, dessen Transaktionen nachverfolgen. Diese Transparenz kann aber auch genutzt werden, um Betrügerei aufzuspüren. So können Börsen, die Kryptowährungen handeln, dazu aufgefordert werden

Daten nach dem KYC-Verfahren (siehe 7.3.2) von Kunden freizugeben, wenn ein Verdacht auf Steuerhinterziehung besteht. (Franco, 2014, S. 8-9)

Eine der größten Kontrollen dieses *Ledgers* durch eine öffentliche Behörde, der IRS (Internal Revenue Service), erfolgte Ende November 2017. Hierbei mussten von 14.355 Konten Daten per Gerichtsbeschluss von der US-Amerikanischen Kryptowährungs-Börse Coinbase an die IRS übergeben werden. (Oberhaus, 2017)

3 Funktionsweise und Grundprinzipien einer Blockchain

Damit eine Blockchain funktionieren kann, benötigt diese sogenanntes *Time-Stamping* und eine Technik, welche die Blockchain verifiziert. *Time-Stamping* ordnet den Transaktionen gewisse Daten zu, welche als *Hash* bezeichnet werden. Diese ermöglichen die zeitliche Ordnung der Daten. *Proof-of-Work*, wie im Unterkapitel erklärt, hingegen verifiziert die Daten in der Blockchain und trägt somit zur Sicherheit der Datenbank bei.

3.1 Time-Stamping

Time-Stamping bezeichnet das Markieren von Transaktionen mittels eines *Hashs*, welcher bezeugt, dass eine Transaktion zu einem bestimmten Zeitpunkt stattgefunden hat. Ein *Hash* ist das auf eine bestimmte Länge begrenzte Ergebnis eines Algorithmus, welcher für eine bestimmte Eingabe stets dieselbe Ausgabe generiert. Bei Bitcoin werden mehrere Transaktionen und somit deren *Hashes*, welche eben diese *Time-Stamps* enthalten, in Blöcken zusammengefasst. Die *Hashes* dieser Transaktionen bilden schließlich zusammen einen sogenannten „*Root Hash*“, indem sie miteinander verknüpft werden. Diese Verknüpfung erfolgt bei Bitcoin mithilfe von „*Merkle Trees*“ (auch „*Hash Tree*“ genannt). Der *Root Hash* wird im dazugehörigen Block, im sogenannten „*Block Header*“ gespeichert. Ein Block ist dabei eine Einheit der Blockchain, welche eine gewisse Anzahl an Transaktionen enthält und in der Blockchain gespeichert ist. Wie man in Abbildung 1 erkennen kann, ist im *Block Header* der *Hash* des letzten Blockes sowie eine *Nonce* (zufällige Zeichenfolge; Parameter zur Berechnung), welche die Gültigkeit des Blockes verifiziert, enthalten. Auf die *Nonce* wird im nächsten Kapitel näher eingegangen.
(Franco, 2014, S. 99-101)

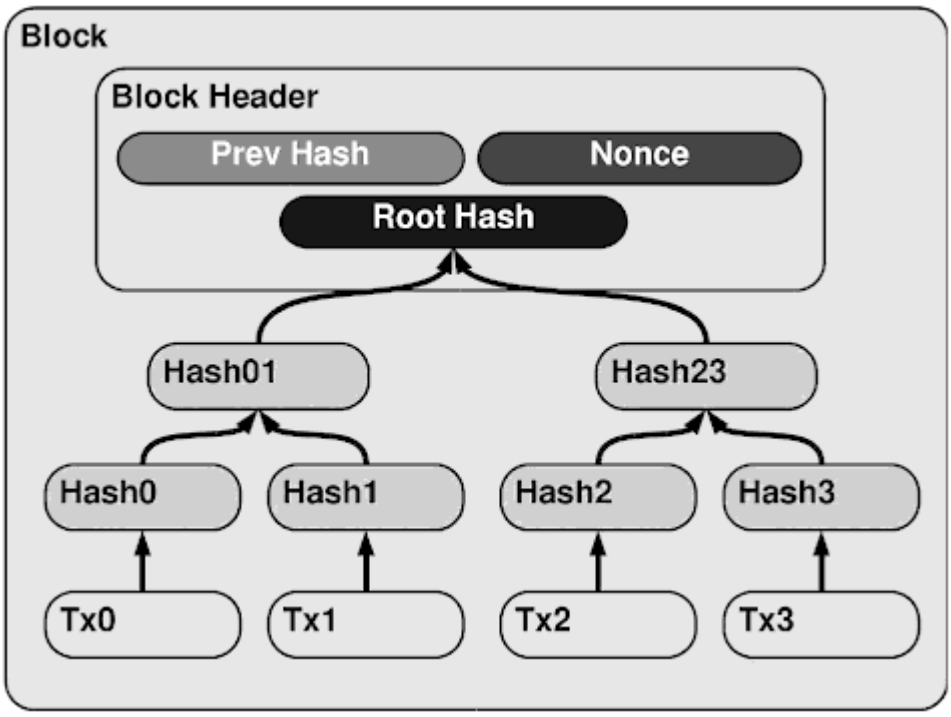

Abbildung 1: Aufbau eines Bitcoin-Blocks mit *Merkle Trees*

(Franco, 2014, S. 118)

Durch die Verwendung des *Time-Stampings* und das Beinhalten des jeweilig vorhergehenden *Hashes* in den Blöcken werden alle Blöcke vernetzt. Aufgrund dieser Vernetztung kann man von jedem beliebigen Block einer Blockchain auf den *Genesis-Block* (erster Block einer Blockchain) schließen. Wichtig ist zu wissen, dass eine Blockchain mit neuen Transaktionen nur länger werden kann, da alte Blöcke nie entfernt werden.
(Franco, 2014, S. 105)

Grundsätzlich würde eine Blockchain durch *Time-Stamping* funktionieren, diese hätte aber keinen Sicherheitsmechanismus; Deshalb ist in den meisten Blockchains ein *Proof-of-Work* implementiert.

3.2 Proof-of-Work

Proof-of-Work wird verwendet, um zu überprüfen, ob Arbeit von einem Netzwerkteilnehmer geleistet wurde. Durch die Implementation von *Proof-of-Work* können *DoS* und *DDoS* –(*Distributed*)-*Denial-of-Service*, eine Art einer Cyber-Attacke – Attacken verhindert werden. Ein bekanntes Beispiel ist die Anwendung dieses Konzeptes in Googles Captcha. (Franco, 2014, S. 103)

Im Bitcoin-Netzwerk wird mit Hilfe von *Proof-of-Work* ein Block und damit die darin enthaltenen Transaktionen verifiziert. Nachdem der *Root Hash* und der *Hash* des vorherigen Blockes im *Block Header* stehen, verbleibt die Berechnung der *Nonce* (Parameter für die Berechnung des Algorithmus). Um die *Nonce* zu erhalten, muss Arbeit geleistet werden. Diese Arbeit wird als Mining bezeichnet und meint das wiederholte Berechnen einer gewissen *Hash*-Funktion mit unterschiedlichen Parametern. Im Falle von Bitcoin wird eine „*Partial Hash Inversions*“ durch den „SHA-256^2“ Algorithmus berechnet. Dabei werden die Transaktionsdaten, welche mit *Merkle Trees* zum *Root Hash* verrechnet wurden, als Input benutzt und mit Hilfe des Parameters (*Nonce*) und des Algorithmus berechnet, bis ein Ergebnis gefunden ist. Ein valides Ergebnis beginnt, wie in Abbildung 2 dargestellt mit einer gewissen Anzahl an Nullen. Der Parameter für dieses richtige Ergebnis ist die *Nonce*, welche schließlich in den *Block Header* geschrieben wird. Wie Abbildung 2 auch verdeutlicht, ergibt nur der *Root Hash* mit einer bestimmten *Nonce* den gewünschten *Hash* mit 3 Nullen am Anfang. (Nakamoto, 2008)

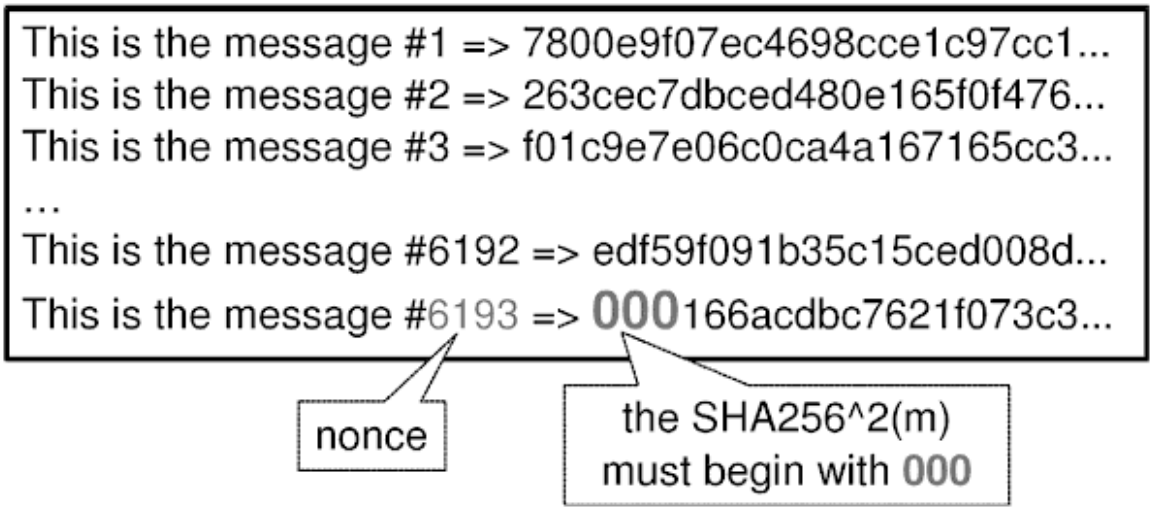

Abbildung 2: *Root Hashes* mit *Nonces* und deren Werte nach Berechnung der *Hash*-Funktion (Franco, 2014, S 19)

Die große Schwierigkeit dabei ist, dass eine Änderung der *Nonce* in einer komplett anderen Zeichenfolge des berechneten *Hashes* resultiert. Wegen der Architektur des SHA-256^2 Algorithmus ist es jedoch auch nicht möglich, vom gewünschten Ergebnis (z.B. 000166acdbc…) auf die *Nonce* zu schließen. (Nakamoto, 2008)

Als Input der *Hash*-Funktion verwenden die Miner den jeweiligen *Root Hash* des Blockes und zufällig generierte *Nonces*. Da der Algorithmus nicht vorhergesehen werden kann, wird

solange eine neue *Nonce* zur Berechnung verwendet, bis der *Root Hash* mit der richtigen *Nonce* das gewünschte Ergebnis (die gewünschte Anzahl an Nullen zu Beginn) ergibt. Tritt dieser Fall ein, so ist ein Block bestätigt und wird in die Blockchain eingegliedert. Sollte dieser Fall jedoch nicht eintreten, so werden Transaktionen im Block umgeschichtet, damit ihr *Merkle Tree* einen anderen *Root Hash* zur Folge hat. Moderne Mining Computer berechnen alle Möglichkeiten an *Nonces* (32-bit Feld → also 2^{32} Kombinationen) für einen bestimmten *Root Hash* in unter einer Millisekunde. Jedoch kann bei Weitem nicht aus jedem *Root Hash* ein *Hash* mit der richtigen Anzahl an Nullen zu Beginn errechnet werden. Folglich ist es nahezu unmöglich, dass der erste *Root Hash* ein Ergebnis liefert. Durch diese Schwierigkeit ergibt sich eine Durchschnittszeit, in welcher Blöcke bestätigt werden. Bei Bitcoin passiert dies ca. alle 10 Minuten. (Franco, 2014, S. 107)

Die Schwierigkeit der Berechnung hängt von der gesamten Rechenleistung des Netzwerks ab. Kommt mehr Rechenleistun hinzu steigt die Schwierigkeit, auch *Difficulty* genannt, an; Sinkt sie, nimmt auch die *Difficulty* ab. Dadurch wird die Zeit zwischen dem Bestätigen von Blöcken bei ca. 10 Minuten gehalten. Die Anpassung dieser *Difficulty* erfolgt, vereinfacht betrachtet, durch Änderung der benötigten Nullen, der *Partial Hash Inversion*, nach jeweils 2.016 berechneten Blöcken (ca. 14 Tagen). (Franco, 2014, S. 105)

Obwohl die Berechnung der richtigen *Nonce* sehr zeitintensiv ist, gestaltet sich das Überprüfen auf die Richtigkeit relativ simpel. Hierzu muss nur eine Berechnung getätigt werden, nämlich die mit dem *Root Hash* des Blocks und der zuvor von den Minern berechneten *Nonce*. Ist die *Nonce* richtig, ergibt sich ein *Hash* mit der gewünschten Anzahl an Nullen zu Beginn. (Franco, 2014, S. 103)

4 Blockchain-Anwendungen

Datenbanken werden heutzutage in den verschiedensten Sektoren benutzt. Dabei bleibt die Kernfunktion, das Speichern und Ändern von Datensätzen, immer gleich. Da eine Blockchain im Grunde eine Datenbank ist, sind Blockchain-Anwendungen in vielen Bereichen denkbar. In den folgenden Unterkapiteln wird zuerst auf die Bitcoin Blockchain eingegangen und danach weitere Anwendungsbereiche mit großem Wachstumspotenzial erwähnt.

4.1 Die Bitcoin Blockchain

Das Konzept der Bitcoin Blockchain wurde im November 2008 unter dem Pseudonym Satoshi Nakamoto in einem *Whitepaper* veröffentlicht. Die Blockchain, welche 2009 mit dem Programm *Bitcoin Core* veröffentlicht wurde, hat eine Größe von 192 GB (Stand 11/2018) (Smith, www.blockchain.com, 2018). Wie schon erläutert, ist diese eine dezentrale Datenbank, in welcher in regelmäßigen Abständen Blöcke mit Transaktionen gespeichert werden. Diese Blöcke haben eine limitierte Größe von 1 MB und sind immer mit dem davor kommenden Block verknüpft (*Hash* im *Block Header*). Durch diese Verknüpfung der Blöcke wird eine Rückverfolgungsmöglichkeit bis zum ersten Block, dem *Genesis-Block*, gewährleistet. *Full-Nodes*, Teilnehmer, welche eine Kopie der ganzen Blockchain speichern, sind weltweit verteilt und gewährleisten dadurch Sicherheit. Jedoch sind nicht immer alle Netzwerkteilnehmer gleicher Meinung; Einige haben sogar kriminelle Absichten, wie die nächsten beiden Unterkapitel zeigen werden.

4.1.1 Double-Spend Problem

Das *Double-Spend* Problem bezeichnet die doppelte Ausgabe eines Währungsanteils. Beispielsweise wird versucht, einen einzigen Bitcoin simultan auf zwei unterschiedliche Konten zu überweisen. Das Bitcoin-Netzwerk ist dagegen gerüstet, indem es eine eigene Datenbank, die *Unspend Transaction Outputs* (UTXO), neben der Blockchain führt, welche Vermögenswerte einzelner Konten enthält. Sollte es dennoch gelingen einen Bitcoin doppelt auszugeben, so ist lediglich die Transaktion gültig, die zuerst durchgeführt wurde. Andere Transaktionen werden nicht mit dem nächsten Block verrechnet und werden daher auch nicht anerkannt. (Franco, 2014, S. 113)

Durch die Dezentralität der Blockchain hilft die Manipulation der UTXO Datenbank nichts, da sie den anderen Netzwerkteilnehmern widersprechen würde. Um die Kontrolle über die Blockchain zu erhalten, muss man die absolute Mehrheit an Rechenleistung stellen. Ausgeführt nennt sich diese Attacke auf das Netzwerk „*51% Attack*“.

4.1.2 51% Attacks

Die *51% Attack* bezeichnet die Übernahme von mehr als 50% der gesamten Rechenleistung des Netzwerks. Diese Attacke ist auch mit weniger Rechenleistung möglich, doch ist die Chance einer erfolgreichen Attacke nur bei Rechenleistungs-Prozentsätzen von über 50%

hundertprozentig. (Franco, 2014, S. 113-115) Im Falle dieser Attacke stellt der Angreifer einen immensen Teil der Rechenleistung. Dadurch ist er in der Lage, einen Angriff auf Miner zu starten und die Blöcke der Miner für ungültig zu erklären, da der Angreifer selbst die längste Kette der Blockchain kontrolliert. „Richtig“ ist nämlich immer die längste Kette (gemessen an der *Difficulty*), welche der Angreifer durch die überlegene Rechenleistung kontrolliert. Durch die Kontrolle des Kettenverlaufs kann der Angreifer einen *Double-Spend* ausführen. Jedoch kann er keine Transaktionen ändern, weil diese mit einer Signatur geschützt sind. (Franco, 2014, S. 113-115)

Die Kosten einer *51% Attack* sind relativ hoch. Bei einer gesamten *Hashrate* (Rechenleistung in *Hash*/Sekunden) des Netzwerkes von 35.000 bis 50.000 PH/s (*Petahash*; Stand: Juli 2018) benötigt man eine Unzahl an Minern, um eine erfolgreiche Attacke durchführen zu können. (Coinwarz.com, 2018) Moderne Bitcoin-Miner schaffen bis zu 14 TH/s; Bei Anschaffungskosten von 2.520 Euro pro Gerät (Amazon, 2018) kostet eine Attacke ca. 3,2 bis 4,5 Mrd. Euro. Hinzu kommen noch Stromkosten von 1,2 bis 1,7 Mio. Euro pro Tag (3 Cent pro KW/h). Je nach täglichem Handelsvolumen müsste man die Bitcoin Blockchain hypothetisch ca. 24 Stunden kontrollieren, um die Investition zurückzugewinnen.

4.1.3 Hardforks bzw. Softforks

Es kann dazu kommen, dass mehrere Ketten in einer Blockchain vorhanden sind, hierbei ist dann immer die längste, gemessen an der benötigten Rechenleistung, gültig. Teilweise kommt es aber aufgrund von verschiedenen Vorstellungen von Benutzern und entwickelnden Teams zur Auftrennung der Blockchain in zwei separate gültige Ketten. Diese Trennung bezeichnet man generell als *Fork*. Man unterscheidet weiter zwischen *Hard*- und *Softfork*, je nachdem wie gravierend die Eingriffe in die Technik sind. Eine *Fork* passiert dann, wenn sich ein Teil des Netzwerkes entschließt, etwas an der Technologie der Kryptowährung zu ändern. Ein prominentes Beispiel ist die Bitcoin-*Fork* von Bitcoin auf Bitcoin Cash, welche im August 2017 über die Bühne ging. Technische Änderungen waren unter anderem die Erhöhung der Block-Größe auf 8 MB im Vergleich zu Bitcoins 1 MB. (Bitcoin Wiki, 2018)

4.1.4 Skalierbarkeit

Die Skalierbarkeit der Bitcoin Blockchain ist eines der größten Probleme, wenn nicht das größte zurzeit. Durch die fixierte Block-Größe von 1 MB gibt es nur eine begrenzte Anzahl von Transaktionen, die in einen Block passen. Durch diese geringe Größe und den großen Abstand der Blöcke von 10 Minuten, schafft Bitcoin gerade einmal 7 Transaktionen in der Sekunde. Andere Anbieter wie VISA und auch andere Kryptowährungen schaffen Zehntausende, teils sogar Hunderttausend Transaktionen in der Sekunde. (Franco, 2014, S. 120-121)

Eine temporäre Lösung für die Bitcoin Blockchain wäre eine Erhöhung der Block-Größe auf 2 MB. Diese wird „SegWit2x“ genannt, würde jedoch nicht wesentlich mehr Transaktionen pro Sekunde schaffen. (Torpey, 2017) Ein besserer Lösungsansatz ist das Bündeln von Transaktionen mittels des *Lightning Networks*. Anwendung könnte dieses Netzwerk beispielsweise in einem Café finden. Die vielen kleinen Transaktionen der Kunden werden auf eine große Transaktion pro Tag gebündelt. Lediglich die einzelnen Konten werden bei den Microtransaktionen, ähnlich wie bei Kreditkartenzahlung, auf ihre Belastbarkeit überprüft. Die Bestätigung der kleinen Transaktionen läuft wesentlich schneller auf dem *Lightning Network* ab, als über die Bitcoin Blockchain. (Poon & Dryja, 2016)

4.2 Weitere Anwendungsbereiche einer Blockchain

Bis jetzt wurde in dieser Arbeit die Nutzung der Blockchain im Falle der Kryptowährung Bitcoin beschrieben. Jedoch ergibt sich ein wesentlich weitreichenderer Nutzen dieser Technologie. Neben den bekannten Kryptowährungen, welche als Funktion zumeist lediglich das Verwalten und Transferieren von Währung haben, gibt es auch noch eine Anzahl an Sparten, in denen man die Blockchain bereits einsetzt oder einsetzten könnte.

Die folgenden drei Beispiele illustrieren Anwendungsbereiche der Blockchain, welche jedoch größtenteils noch in den Kinderschuhen stecken. Durch die umfassenden Vorteile einer Blockchain in diesen Bereichen und großen Kapitaleinsatz von staatlicher-, aber auch privatwirtschaftlicher Seite, schreitet die Implementation schnell voran.

4.2.1 Supply-Chain-Managment

In der heutigen Industrie, welche Produkte in Millionenauflage produziert und nach der Online-Bestellung am nächsten Tag nach Hause liefert, ist es essenziell, dass alle Produktionsschritte nahtlos ineinandergreifen. *Supply-Chain-Managment* (Managment der Versorgungskette) befasst sich mit der Problematik, alle Komponenten, welche zur Produktion einer Ware benötigt werden, am richtigen Standort zur richtigen Zeit zu haben. Liefert ein Zulieferer zu spät oder gar nicht, ist oft die gesamte Produktion gezwungen anzuhalten.

Einige Unternehmen bieten auf Blockchain-Basis Lösungen an, welche es ermöglichen, Produkte und deren Bestandteile klar zu kennzeichnen. So können sie auch später an ihren Ursprung rückverfolgt werden. Eine Firma namens Vechain stellt eine Zukunft in Aussicht, in der Informationen über den gekauften Artikel für den Kunden zur Verfügung stehen. Dadurch wird auch eine Legitimationsüberprüfung, beispielsweise bei Markenkleidung, für den Kunden möglich. Außerdem kann ein Kunde, welcher im Supermarkt Joghurt kaufen will, nachverfolgen ob die Kühlkette des Joghurts während der Lieferung unterbrochen wurde. Dies benötigt natürlich Sensoren in den Verpackungen, welche uns schließlich zum Internet der Dinge oder „*Internet of Things*“ bringen. (Vechain, 2018)

4.2.2 Internet of Things (IoT)

Internet of Things beschreibt die Vernetzung von zahlreichen Dingen und Geräten im Alltag. So kann man in einen Supermarkt gehen und ein Produkt mithilfe der Daten von unzähligen Sensoren, welche über die Qualität Auskunft geben, auswählen. Man trifft eine Kaufentscheidung und verlässt das Geschäft, daraufhin wird der Kaufbetrag vom Konto automatisch abgebucht. Teilweise ist dies sogar schon in einem Amazon Go Markt in Seattle möglich. (Levy, 2018)

Ein weiterer Einsatz der Blockchain in Sachen *Internet of Things* wären rasche Abwicklungen von Microtransaktionen. Hiermit könnten Autos automatisch Kosten für Parkhäuser oder Mautstraßen bezahlen. Außerdem wird das *P2P* (*Peer-to-Peer*) Handeln von Strom möglich werden. (Orlov, 2017)

4.2.3 Sozial- & Gesundheitssystem

Im Bereich der Sozial- und Gesundheitssysteme kann eine Blockchain durch ihre Dezentralität wesentlich zum Datenschutz der Patienten oder Sozialleistungsbezieher beitragen. Dem gegenüber ermöglicht eine zentrale Blockchain, wie die einer Regierung, die Sozialleistungen und Gesundheitsleistungen effizient zu kontrollieren. Durch die Daten der Bürger, welche von Behörden oder Regierungen in einer Blockchain gesammelt werden, könnte beispielsweise Sozialleistungsbetrug, Steuerhinterziehung oder ähnliches vermindert werden.

China und Indien verwenden zum Teil bereits solche oder ähnliche Systeme. In China ist es möglich, durch gutes oder schlechtes Verhalten eine bessere oder eben schlechtere Punkteanzahl zu erhalten. Einfluss auf diese gesellschaftlichen Bonitätspunkte (Chinesisches Sozialkredit-System) nehmen zum Beispiel das Strafregister, Jahresberichte oder sogar das Überqueren der Straße bei roten Fußgängerampeln. Aufgrund eines niedrigen Rankings kann man durch eine Drosselung der Internetgeschwindigkeit oder sogar durch eine höhere Steuerlast bestraft werden. (Meissner, 2017)

5 Mining

Mining bezeichnet das Berechnen der *Hash*-Funktionen einer Kryptowährung (siehe: 3.2, Proof-of-Work). Die Computer, welche Mining betreiben, werden für ihre Arbeit, das Überprüfen von Transaktionen, belohnt.

Durch die Wertsteigerung verschiedenster Kryptowährungen kam es in den letzten Jahren zu einem Mining-Boom. Die Investitionen in das Mining-Equipment konnten in wenigen Monaten, manchmal sogar Wochen, mit den Einnahmen aus den geschürften Währungen wieder eingenommen werden.

5.1 Mining-Arten

Laut *Coinmarketcap.com*, einer Übersichtsseite für Kryptowährungen, gibt es über 2.000 verschiedene Kryptowährungen (CoinMarketCap, 2018). Die meisten Kryptowährungen benutzten, wie auch Bitcoin, *Proof-of-Work* (siehe 3.2) wodurch Mining möglich ist. Jedoch unterscheiden sich diese Krytowährungen zumindest marginal voneinander. Es werden verschiedene Algorithmen verwendet um Transaktionen sicher zu gestalten. Neben dem SHA-256^2 Algorithmus, welcher von Bitcoin benutzt wird, sind außerdem „Cryptonight“, „EquiHash“ und „ETHASH“ weit verbreitet. (Crocosource.com, 2019)

Während Bitcoins SHA-256^2 derzeit am effizientesten auf speziell dafür gefertigter Hardware zu schürfen ist, benötigt man für Cryptonight neueste Grafikkarten. Im folgenden Unterkapitel sind die wichtigsten Mining-Arten aufgelistet.

5.1.1 CPU

Der CPU („*Central Processing Unit*“) oder der Prozessor ist in einem Computer der Hauptchip. Dieser führt während des Mining Berechnungen durch, welche spezifisch für jeden Algorithmus sind.

Historisch betrachtet waren CPUs von großer Bedeutung, auch wenn sie heute fast immer von GPUs (Grafikkarten) und ASICs (Anwendungsspezialisierter Computer) in den Schatten gestellt werden. Die ersten „Bitcoin-Miner“ liefen nämlich meist auf den Computern einiger Technikenthusiasten. Zwischen der Veröffentlichung von „Bitcoin-Core“ (Bitcoin Wallet mit Netzwerkfunktionen) im Jänner 2009 und Sommer 2010 wurde ausschließlich mit Hilfe von Prozessoren geschürft. Die „*Hashrate*“, also die Berechnungen pro Sekunde lagen unter 20

MH (1 MH = 1.000.000 Hashes). Zum Vergleich, heute gibt es ASIC Miner mit Hashraten von bis zu 18 TH/s (18 TH = 18.000.000 MH). (Franco, 2014, S. 147)

Der große Vorteil von CPUs ist jedoch, dass sie im Vergleich zu speziellen ASIC Minern in jedem Computer verbaut sind. Dieser Vorteil war aufgrund des möglichen GPU-Minings bei Bitcoin Ende 2010 nichtig, da eine Grafikkarte einen wesentlichen Vorteil gegenüber dem Prozessor hat. Aktuell gibt es kaum noch Kryptowährungen, welche rentabel mit Prozessoren geschürft werden können. (Franco, 2014, S. 148)

5.1.2 GPU

Als Ende 2010 die *Hashrate* des gesamten Netzwerkes aus hardwarebasierten Gründen stagnierte, kamen Grafikkarten ins Spiel. Diese schafften mehr als 30 Mal so viele Berechnungen in der Sekunde. Nach Start des GPU-Minings stieg die *Hashrate* des Bitcoin-Netzwerks innerhalb eines Jahres auf das Hunderttausendfache (Franco, 2014, S. 146). Im Vergleich zu einem CPU hat eine Grafikarte wesentlich mehr Rechenkerne. Diese Rechenkerne sind bei Grafikarten in ihren Berechnungen, im Vergleich zu den Prozessorkernen, limitiert. Sie sind jedoch geeignet einfache Berechnungen, wie die des SHA-256^2, durchzuführen. Die ursprüngliche Funktion einer Grafikkarte, nämlich die Beschleunigung der Grafikberechnung eines Computers, ist sehr ähnlich, weshalb Grafikkarten bis heute häufiger als andere Techniken zum Schürfen von Kryptowährungen benutzt werden.

Neben Grafikkarten kamen Mitte 2011 sogenannte FPGAs („*Field-Programmable Gate Arrays*“) auf. Diese können je nach Anwendungsbereich programmiert werden und sind etwas besser im Hinblick auf die *Hashrate* als Grafikkarten. Dennoch sind Grafikkarten benutzerfreundlicher, haben eine höhere *Hashrate* bezogen auf die Kosten und einen höheren Wiederverkaufswert. Schlussendlich wurden jedoch die Grafikkarten und FPGAs aus dem Bitcoin Mining-Geschäft von ASICs verdrängt. (Franco, 2014, S. 147)

5.1.3 ASIC

„*Application-Specific Integrated Circuit*“ (ASIC) meint anwendungsspezifische, integrierte Schaltungen. (Franco, 2014, S. 147) Im Gegensatz zu normalen Prozessoren oder Grafikkarten gibt es ASIC-Schaltungen, welche nur darauf ausgelegt sind, den SHA-256^2 *Hash* so schnell wie möglich zu berechnen.

Dadurch, dass die Schaltung speziell auf einen Algorithmus (SHA-256) ausgelegt ist, kann man mit einem solchen ASIC-Miner nur Kryptowährungen, welche SHA-256^2 als Algorithmus verwenden, schürfen. Ein ASIC-Miner hat gegenüber einer Grafikkarte einen ähnlichen Vorteil, wie diese gegenüber einem Prozessor hat. Dadurch können ASIC-Miner, welche das Bitcoin Mining-Geschäft seit 2014 dominieren, weitaus höhere Leistungen von bis zu 18 TH (18 TH = 18.000.000 MH) pro Sekunde und Gerät erreichen.

Durch Verbesserungen in der Technik hat die Rechenleistung enorm zugenommen, und die Kosten pro errechneten *Hash* sind stark gesunken, wie in Abbildung 3 zu sehen ist.

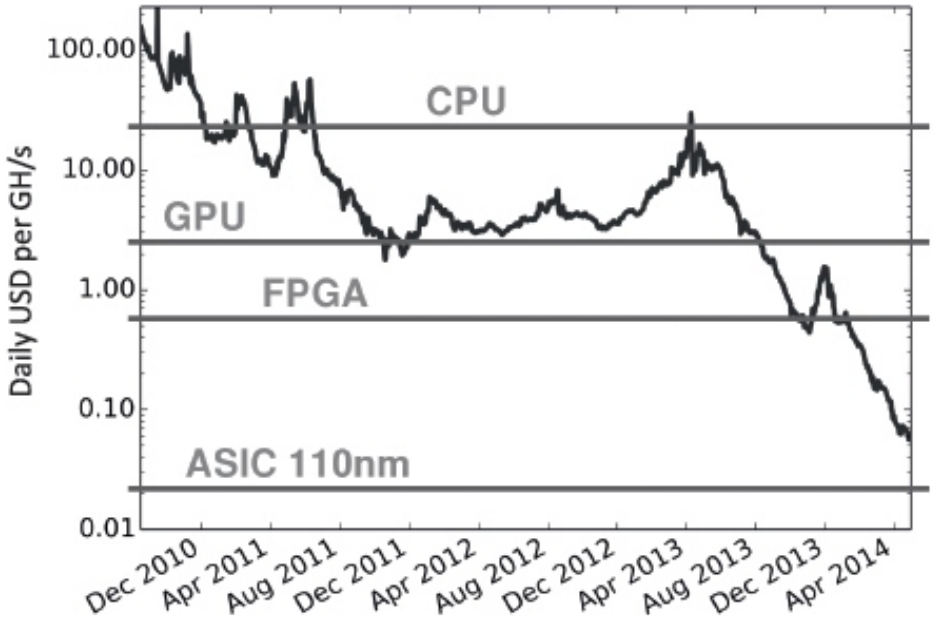

Abbildung 3: Elektrizitätskosten verschiedener Mining-Technologien (Franco, 2014, S. 64)

Der Großteil der Betriebskosten eines Miners hängt von seinem Stromverbrauch ab. Zurzeit sind die Stromkosten für einen effizienten Bitcoin-Mining-Computer, welcher 14 TH in der Sekunde liefert und 1300 Watt Strom (Strompreis: 20 Cent/KW) benötigt, 45 Cent pro TH/s und Tag.

5.2 Miningpool

Wie oben zu sehen war, wurde die Hardware um mehrere Potenzen effizienter. Die gesamte Miningleistung stieg von wenigen Hundert *Petahash* im Jahre 2015 auf über 45.000 *Petahash* 2018 (Coinwarz.com, 2018). Hauptgrund für diesen Anstieg ist die Belohnung für den Rechner, der den jeweils richtigen *Root Hash* (bzw. *Nonce*) für einen

Block findet. Zudem gibt es auch noch Belohnungen für das Bearbeiten von Transaktionen, jedoch ist die derzeitige Belohnung für einen Block mit 12,5 Bitcoin pro Block wesentlich höher. Da zirka alle 10 Minuten ein neuer Block entsteht, ist es bei der großen Anzahl von Teilnehmern im Netzwerk unwahrscheinlich, einen sogenannten „*Block-Reward*“ (die Belohnung von 12,5 Bitcoins) zu erhalten. Aus diesem Grund schließen sich Besitzer von Mining-Equipment und große Mining-Firmen in sogenannten „Miningpools“ zusammen. (Franco, 2014, S. 149-153) Ein Miningpool ist also ein Zusammenschluss, in welchem die Teilnehmer ihre Leistung vereinen, um leichter einen *Block-Reward* zu erhalten. Je größer der Miningpool ist, desto wahrscheinlicher ist es, dass ein Teilnehmer einen richtigen *Hash* für einen Block errechnet und der Pool einen *Block-Reward* erhält. (Franco, 2014, S. 151) Die Auszahlung erfolgt bei den meisten Miningpools nach Abzug einer gewissen Benützungsgebühr auf eine Adresse der geschürften Kryptowährung. Bezahlt wird nach Mining Leistung. Trägt man beispielsweise 0,5% der *Hashrate* des Pools bei, so bekommt man 0,5% des Gewinnes abzüglich der Gebühr ausbezahlt.

Somit bringen Pools für die Netzteilnehmer einen großen Vorteil, welcher aber zum Nachteil werden könnte. Denn wenn ein Pool mehr als 50% der Rechenleistung des Netzwerkes kontrolliert, könnten die Teilnehmer damit die gesamte Blockchain kontrollieren.

6 Aufbau und Wirtschaftlichkeit eines eigenen Miners

Dieses Kapitel beschäftigt sich mit dem Bau meines eigenen Mining-Computers. Zuerst werden die Komponenten meines Miners aufgelistet und es wird kurz auf die benötigte Software eingegangen. Anschließend erfolgt eine Analyse der Rentabilität, sowie eine Diskussion über den hohen Energieverbrauch des Minings.

6.1 Aufbau eines Miners

Wie in Kapitel 5 dargelegt, gibt es verschiedene Arten von Minern, welche sich jeweils auf verschiedene Hard- und Software konzentrieren, damit sie möglichst effizient bestimmte Algorithmen verarbeiten können. Das Konzept für den Miner entwickelte ich Anfang 2018. Die Wahl fiel auf einen Miner, welcher die Kryptowährung „Ethereum“ schürfen sollte und einen weiteren, der auf „Z-Cash“ ausgelegt war. Beide Miner nutzen Grafikkarten (GPU-Mining) und starteten im März 2018.

6.1.1 Hardware

Wie der Name GPU-Mining vermuten lässt, trägt hier die GPU (*Graphics Processing Unit*), zu Deutsch Grafikkarte, die Rechenlast des jeweilig verwendeten Algorithmus. In Abbildung 4 ist eine „msi RX-Vega 56“ zu sehen. Diese Karte wird für das Ethereum Mining-Rig benutzt.

Abbildung 4: msi RX-Vega 56 (eigene Darstellung)

Neben der Grafikkarte war für mich auch wichtig, dass das Motherboard möglichst viele Schnittstellen für Grafikkarten hat. Weniger wichtig waren der Prozessor, der Arbeitsspeicher und die Festplatte. Schlussendlich montierte ich den günstigsten Intel Prozessor, der auf den LGA 1151-Sockel passt. Wenn der Miner auch mit 2 GB RAM funktionieren sollte, entschied ich mich der Sicherheit halber für 4 GB. Das Betriebssystem für den Miner (Windows 10 Pro) speicherte ich vorab auf einer SSD-Festplatte ab.

Bei den oben genannten Bestandteilen war der Preis wichtiger als die Qualität. Jedoch nicht beim Netzteil, dieses sollte schließlich zuverlässig Strom liefern und nicht durch Spannungsschwankungen die teuren Grafikkarten ruinieren.

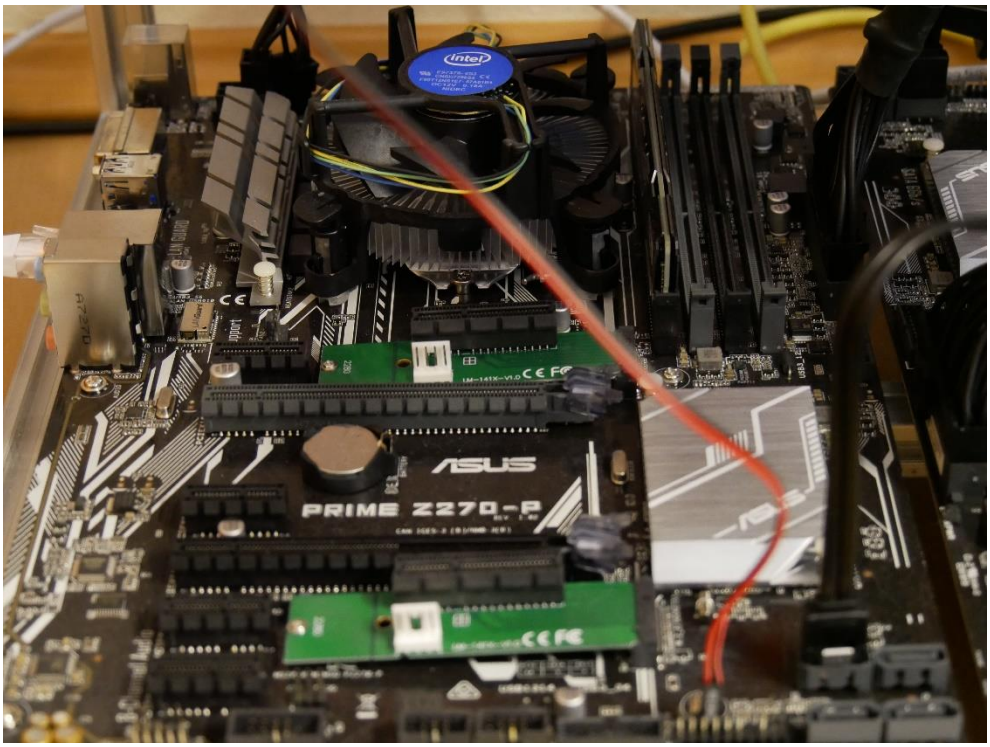

Abbildung 5: Motherboard mit RAM und CPU (eigene Darstellung)

Nach der Bestückung und Verkabelung des Motherboards, wie in Abbildung 5 erkennbar, wurden die Komponenten getestet. Bevor ich die ersten Karten auf das Mining-Rig montierten konnte, optimierte ich Hardware-Einstellungen und die Einstellungen des Betriebssystems für das Mining. Unter anderem ist der Computer so konfiguriert, dass er sich nach Stromausfällen selbst wieder einschaltet und nie in den Energiesparmodus wechselt.

Schließlich war es Zeit für die ersten Testläufe, welche nur mit einer Grafikkarte absolviert wurden. Um mehr als 2 Grafikkarten auf dem Motherboard installieren zu können, gibt es

sogenannte Riser. Diese steckt man auf der einen Seite in einen *PCI-E 1x Slot* und auf der anderen Seite sitzt ein *PCI-E 16x Slot*, in den auch eine Grafikkarte passt. Die Übertragungsgeschwindigkeit spielt dabei eine untergeordnete Rolle, da für die Berechnungen nur wenige Daten zwischen Prozessor und Grafikkarten ausgetauscht werden. Deshalb reicht auch ein *PCI-E 1x Slot* mit geringerer Bandbreite aus. Als alle *PCI-E Slots* besetzt waren, nutzte ich noch einen der beiden *M2*-Anschlüsse, um die 7. Grafikkarte anschließen zu können. In der Abbildung 6 sieht man die *PCI-E 1x* Enden der *Riser*, welche in die Slots am Motherboard gesteckt sind. Dahinter liegen die beiden grünen *M2-PCI-E 1x* Adapter.

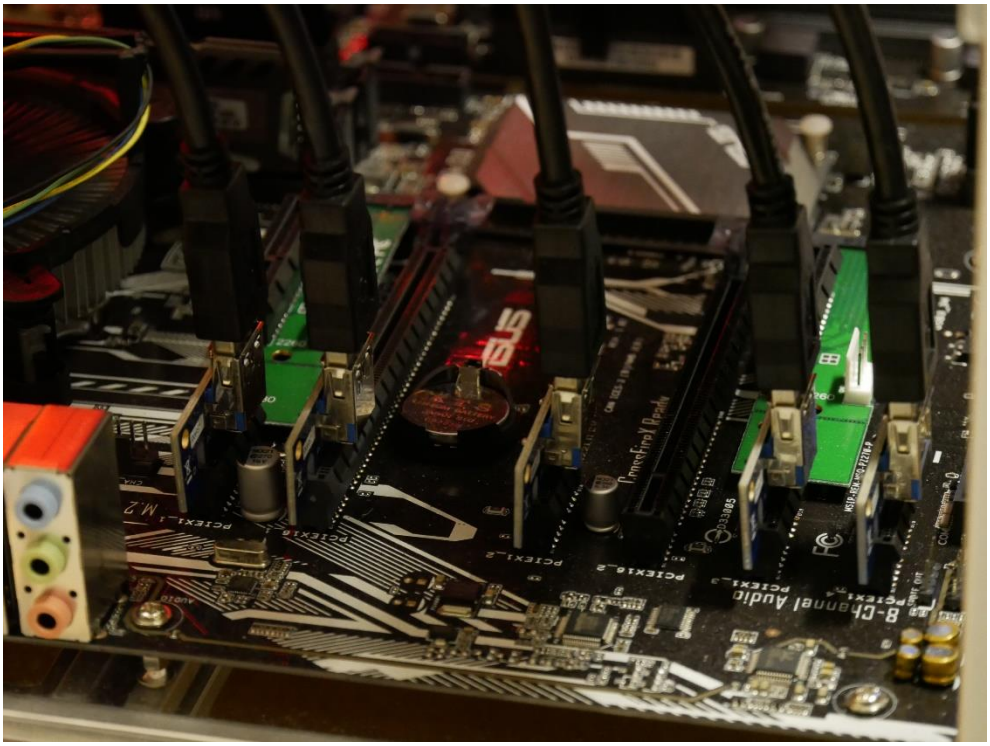

Abbildung 6: USB-*Riser* (eigene Darstellung)

Selbst die *Riser* brauchen wie alle anderen Komponenten auch Strom, weshalb jeder Miner mit zwei 850 Watt Netzteilen betrieben wird. Ein Netzteil ist für die Stromversorgung des Motherboards, des Prozessors, 3 Grafikkarten und der SSD zuständig. Das andere versorgt die restlichen 4 Grafikkarten und die Ventilatoren. Zusammen ergibt sich so eine theoretische Maximalleistung der Netzteile von 1.700 Watt. Der Ethereum Miner benötigt, je nach Konfiguration und Einstellung, zwischen 1.100 und 1.500 Watt, der Z-Cash Miner ca. 1.000 Watt. Somit bleiben stets mindestens 10% an Leistungsreserve übrig. Trotz dieser Reserve kam es in der Testphase des Öfteren zum Ausfall eines Netzteiles, weil zu viel Leistung beim Starten des Systems gebraucht wurde.

Die beiden Mining-Computer (Z-Cash und Ethereum) sind praktisch baugleich und unterscheiden sich nur im Komponentenpunkt Grafikkarten. Hier verwendet der Z-Cash Miner nämlich „Geforce GTX 1080“ mit Nvidia Chipset, im Gegensatz zum Ethereum Miner, welcher mehrere „RX-Vega 56“ mit AMD Chipset nutzt.

Nachdem der Miner fertiggestellt war, stationierte ich ihn in der Garage, in welcher die Temperaturen auch während der Sommermonate nicht allzu hoch waren. Damit die Grafikkarten nicht überhitzen, muss die entstandene Wärme ständig abgeführt werden. Dazu ist das gesamte Mining-Rig mit 12 Ventilatoren bestückt, wie man in Abbildung 7 sieht.

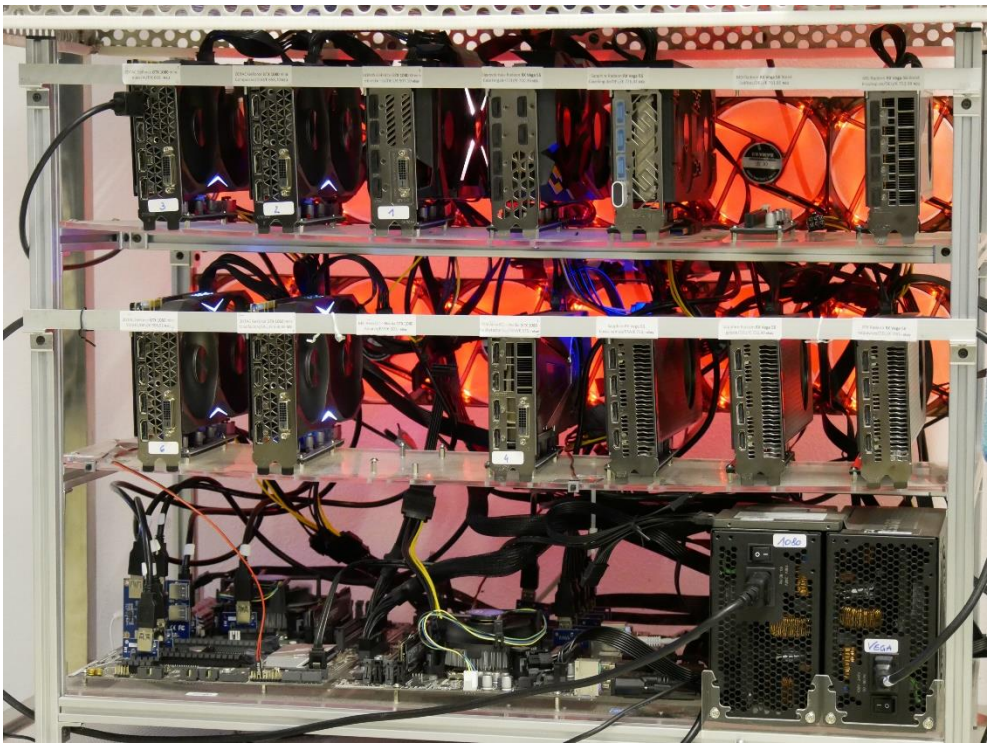

Abbildung 7: Die beiden Mining-Rigs im Betrieb (eigene Darstellung)

Trotz der vielen Parallelen zwischen den beiden Mining-Rigs in der Hardware, ergeben sich in der Software einige Unterschiede; Diese werden im nächsten Unterkapitel angeführt.

6.1.2 Software

Damit ein Miner arbeiten kann, benötigt er spezielle Software, welche den Computer mit dem Netzwerk verbindet und nach Arbeit sucht. Im Fall meines Aufbaus wird „CUDA-Miner“ mit den Nvidia GTX 1080 Karten zum Schürfen von Z-Cash benutzt. Die Software „Claymore“ wird mit den RX-Vega 56 Karten zum Schürfen von Ethereum verwendet. Beide

Computer laufen mit Windows 10 Pro als Betriebssystem, weshalb ich in diesem Kapitel keine auf Linux basierte Mining-Software erwähnen werde.

Um das Maximum aus der Hardware herauszuholen, müssen einige Einstellungen geändert werden. Klarerweise sollte man verhindern, dass sich der Computer nach einer gewissen Zeit in den Ruhezustand versetzt. Außerdem müssen spezielle Driver für die Grafikkarten installieren werden, welche den Betrieb von mehreren Grafikkarten in einem Computer erlauben. *Vega.Miningguides.com* erwies sich beim Einrichten der umfassenden Einstellungen meiner Mining-Rigs als große Hilfe. (@CircusDad, 2018)

Weil die Grafikkarten allein nicht ihr maximales Potenzial ausnutzen, gibt es sogenanntes „Overclocking“. Hierbei werden die Taktfrequenzen des Grafikspeichers und des Kerns soweit erhöht, dass die Grafikkarte noch stabil läuft, jedoch eine erhöhte Leistung zeigt. Wie in Abbildung 8 zu sehen ist, wird die Taktfrequenz und das sogenannte „Power Limit“, welches die Stromzufuhr steuert, mithilfe von „msi Afterburner“ geregelt. Außerdem sieht man im Hintergrund den CUDA-Miner mit 6 GTX 1080 laufen. Afterburner kontrolliert auch die Geschwindigkeit der Kühlventilatoren anhand der Temperaturen der Grafikkarten.

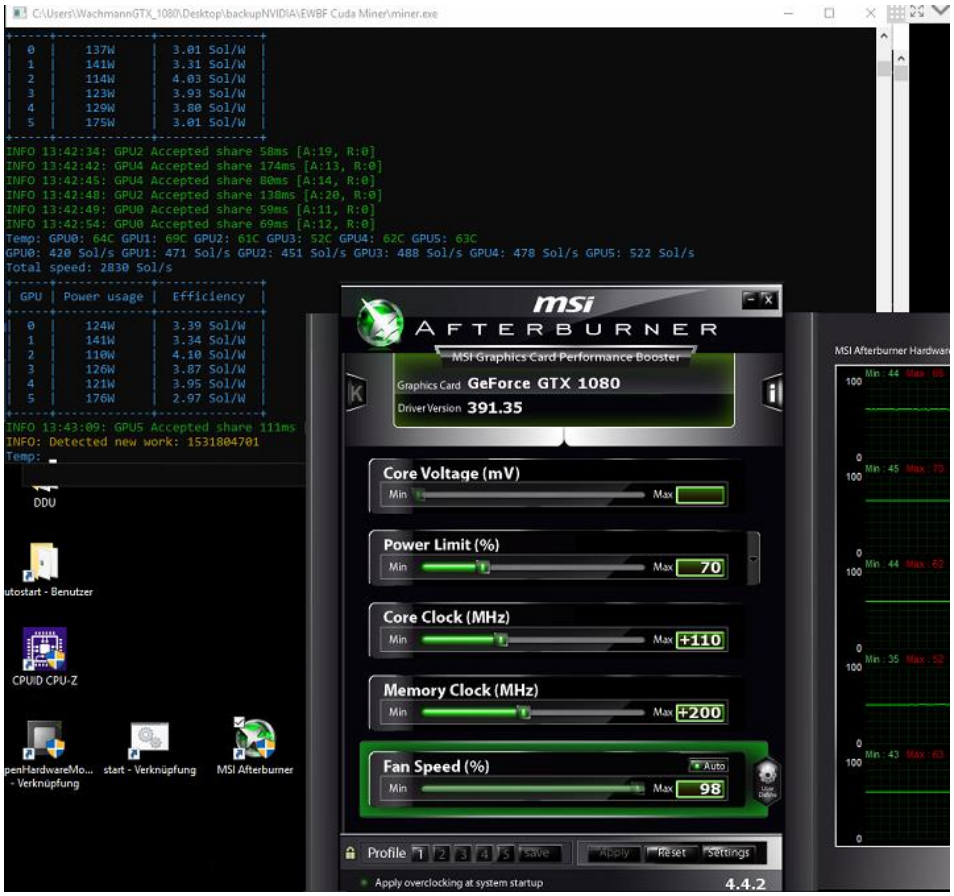

Abbildung 8: Afterburner und CUDA-Miner (eigene Darstellung)

Verglichen zum Z-Cash Mining-Rig, welches mit Afterburner und CUDA-Miner läuft, benutze ich für das Ethereum Mining-Rig den Claymore-Miner und OverdriveNtool zum Steuern der Frequenzen, Ventilatoren und des Power Limits.

Im Gegensatz zum Z-Cash-Rig ist das Einstellen eines großen virtuellen Speichers (V-RAM) bei Ethereum-Mining wichtig. Für das gleichzeitige Betreiben von 6 Grafikkarten empfiehlt sich eine Speichergröße dieses virtuellen Speichers von 16 GB.

Auch die Taktfrequenz der RX-Vega 56 Karten erhöhte ich mit Hilfe von „Overclocking“ von der normalen „Base Clock“ von 1.156 Mhz auf 1.407 Mhz („Boost Clock“). Dies ist auch in Abbildung 9 rechts oben zu erkennen. Außerdem sieht man, dass einige RX-Vega 56 mit diesen Einstellungen in der Lage sind, über 40 Mh/s zu berechnen.

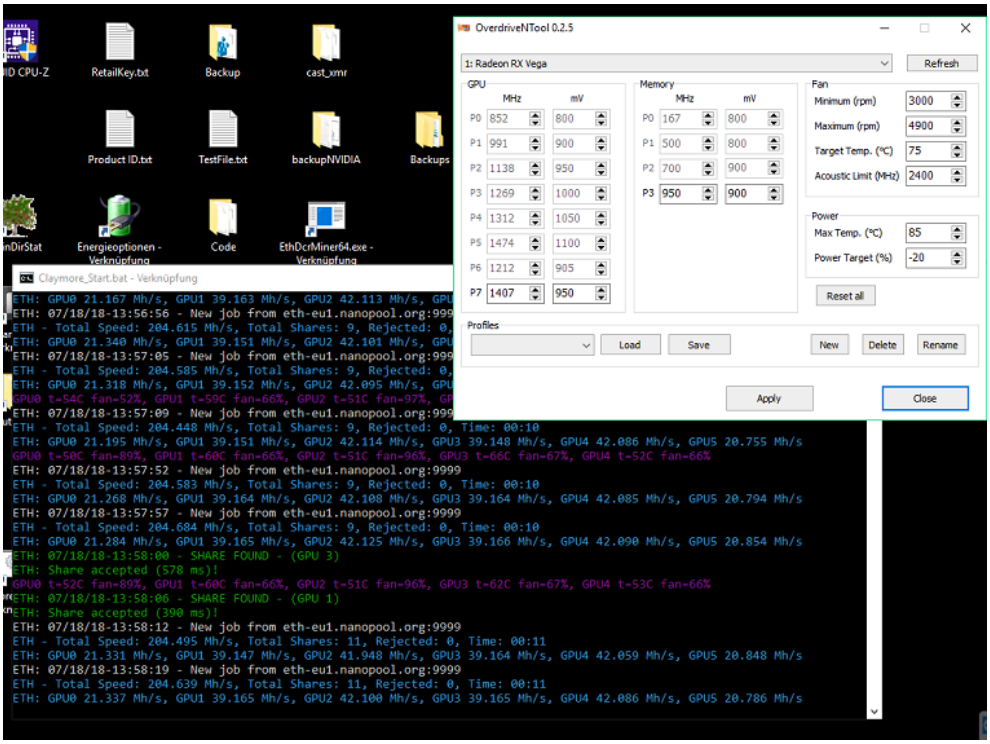

Abbildung 9: Claymore Miner und OverdriveNtool (eigene Darstellung)

Andere hingegen liefern wegen einer ungleichmäßigen Stromversorgung nur um die 20 Mh/s. Im Durchschnitt ergibt sich ein Wert von 34 Mh/s, welcher deutlich über dem von 30 Mh/s ohne Overclocking liegt. Der Wert könnte durch das Gewähren einer noch größeren Stromzufuhr höher sein, jedoch ist der Strompreis der höchste Kostenfaktor beim Betreiben eines Mining-Rigs. Das große Ziel ist somit, die Software bestmöglich zu optimieren, sodass die Karten auch bei höheren Taktfrequenzen mit nahezu gleich viel Strom stabil laufen.

6.2 Rentabilität eines Miners

Neben den Anschaffungskosten eines Mining-Rigs sind auch die Stromkosten für die Rentabilität des Rigs entscheidend. Der Preis für einen KW Strom kann je nach Bezieher, Standort und Tageszeit stark schwanken. Nicht nur für große Mining-Betreiber, welche auf Grund der niedrigen Stromkosten (< 3 Cent/KW für Industriekunden) zumeist in Island, Kanada oder China angesiedelt sind, stellt Strom die größte Kostenquelle dar. Weiters spielt der Preis der Kryptowährung, sowie die Belohnung, welche man für das Mining bekommt, eine große Rolle. Als die Preise vieler Kryptowährungen im 3. und 4. Quartal 2017 rasant anstiegen, war die Rentabilität eines Miners so hoch, dass man seine Investitionen in Equipment und Strom schon nach wenigen Wochen decken konnte. Zu den hohen Kurssteigerungen war die „*Difficulty*" damals, im Vergleich zu heute, noch gering. Zu sehen ist, dass die Rentabilität von Kryptowährungs-Mining stark vom Standort und den Betriebskosten abhängig ist. Eine große Mining-Firma in Island kann tausende Grafikkarten zu Sonderpreisen erwerben und Strom an der Börse wesentlich billiger als ein privater Betreiber einkaufen.

Folgende Tabelle vergleicht die Rentabilität von Bitcoin-Mining im zeitlichen Verlauf in Bezug auf die Stromkosten. Als Beispiel dient ein Antminer S9 (14 TH/s bei einem Verbrauch von 1.320 W/h) (Bitmain, 2018). Der Antminer S9 ist einer der effizientesten Bitcoin-Miner. Die Wahl der Kostenaufstellung fiel auf einen Bitcoin-Miner, da die Stromkostenaufstellung meines eigenen GPU-Miners den Rahmen dieser Arbeit sprengen würde. Anzumerken ist, dass sich das GPU-Mining etwas rentabler erweist, als das in der Tabelle analysierte ASIC-Mining.

Antminer S9 (14TH/s, 1320 W/h)		Monate					
Poolfee: 1%		Dez 17	Feb 18	Apr 18	Jun 18	Aug 18	Okt 18
Stromkosten	0,25 €	745,50 €	126,50 €	-46,50 €	-117,50 €	-136,50 €	-157,35 €
	0,20 €	793,80 €	174,80 €	1,80 €	-69,20 €	-88,20 €	-109,05 €
	0,15 €	842,10 €	223,10 €	50,10 €	-20,90 €	-39,90 €	-60,75 €
	0,10 €	890,40 €	271,40 €	98,40 €	27,40 €	8,40 €	-12,45 €
	0,05 €	938,70 €	319,70 €	146,70 €	75,70 €	56,70 €	35,85 €

Tabelle 1: Erwarteter Gewinn eines Antminers S9 in einem Monat (eigene Darstellung)

Die Tabelle stellt den erwarteten Umsatz des Miners bei gegebenen Stromkosten für das nächste Monat dar (bei gleichbleibender *Difficulty* und Preis). Für die Berechnung wurden die Auszahlungen am gegebenen Tag theoretisch anhand der *Difficulty* laut *Coinwarz.com* berechnet (Coinwarz.com, 2018) und anschließend mittels des Tagesdurchschnittskurses nach *CoinMarketCap* in Euro umgerechnet. (CoinMarketCap, 2018) Schlussendlich wurde noch die Pool Fee von 1% und die Stromkosten für 1.320W/h (also ca. 31,7 KW/h pro Tag) abgezogen. Die errechneten Werte sind theoretische Werte und weichen vermutlich etwas vom realen Wert ab.

6.3 Umweltauswirkungen des Minings

> *„[…] The carbon footprint per transaction of bitcoin is estimated to be 117.63 kg of CO_2, or about the same as the footprint of someone flying economy class from Amsterdam to Frankfurt."* (Hernández, 2017)

Wie Hernández darlegt, verbraucht das ganze Bitcoin-Netzwerk eine enorm hohe Menge an Strom, welche indirekt einen riesigen CO_2-Ausstoß mit sich bringt. Erst der Vergleich mit anderen gängigen Zahlungssystemen verdeutlicht das Ausmaß. Vergleicht man beispielsweise die benötigen Kilowatt-Stunden von einer Bitcoin-Transaktion mit einer Visa Transaktion ergibt sich, dass Visa über 400.000 Mal energiesparender ist. Anders ausgedrückt: Eine Bitcoin-Transaktion benötigt gleich viel Strom wie über 400.000 Visa Transaktionen. (Digiconomist, 2018)

Rechnet man beispielhaft den Tagesenergieverbauch vom Bitcoin-Mining für 1.11.2018 kommt man auf folgendes Ergebnis: Es ergibt sich eine durchschnittliche Block-Dauer von 9 Minuten, was 160 Blöcke a 12,5 Bitcoins am Tag zur Folge hat. Der Kurswert von Bitcoin war ca. 5.600 Euro am 1.11.2018 – daraus folgt ein Gesamtwert von ca. 11,2 Mio. Euro. Angenommen wird, dass die durchschnittlichen Kosten pro KW/h ca. 5 Cent entsprechen (anhand der durchschnittlichen Kosten pro KW/h der Leipziger Strombörse). (Bricklebrit Lastgangbepreisung, 2018) Zudem lassen sich mit ca. 50% des Mining Umsatzes die Stromkosten decken; d.h. es werden ca. 5,6 Mio. Euro für Strom ausgegeben, was umgerechnet 112 Mio. KW/h entspricht. Auf das Jahr gerechnet sind das ca. 40 Mrd. KW/h oder 40 TW/h. Zu beachten ist, dass diese Berechnung den Anstieg der *Difficulty* nicht berücksichtig.

Aus dem Jahresenergieverbrauch kann man nun auf die Emissionen pro Transaktion schließen. Für die Berechnung des CO_2-Ausstoßes wurden Daten von *The Engineering ToolBox* verwendet. Zur vereinfachten Berechnung wurden nur die CO_2 Ausstöße für Kohle und Gas in die Berechnung miteinbezogen. Diese beiden Brennstoffe sind zu ca. 2/3 in der weltweiten elektrischen Energieproduktion vertreten. Das restliche Drittel besteht aus erneuerbaren Energien sowie Atomenergie und hat einen wesentlich geringeren Einfluss auf die Emissionen als Kohle und Gas. (The Engineering ToolBox, 2009) Ein Wert von 0,35 kg/KW/h wurde so berechnet. Bei ca. 260.000 Bitcoin-Transaktionen täglich (Smith, Blockchain.com, 2017), ergibt sich daraus schließlich der Wert von 161 kg CO_2 pro Transaktion. Die signifikante Differenz zum Literaturwert kann durch die Änderung der Schwierigkeit des Minigs begründet werden.

Die selbst gebauten Miner weisen somit theoretisch einen CO_2-Ausstoß von 0,875 kg/h (bei 2,5 KW/h) auf. Da der Großteil des Stroms direkt aus der hauseigenen Photovoltaikanlage kommt, ist der tatsächliche Ausstoß weitaus niedriger.

Zuletzt muss explizit darauf hinweisen werden, dass diese Berrechnungen nur den jetzigen Stand der Technik widerspiegeln. Wie in Kapitel 4.1.4 erwähnt, wird sich die Technik im Sinne einer leichteren Skalierbarkeit weiterentwickeln. Testweise wird bei Bitcoin auch schon das *Lightning Network* eingebunden, welches ebenfalls in Kapitel 4.1.4 erwähnt wurde und die Anzahl der tatsächlichen Transaktionen in der Bitcoin Blockchain drastisch reduzieren wird.

7 Kryptowährungshandel

Nachdem die Technik hinter den Kryptowährungen in den vorhergehenden Kapiteln beschrieben wurde, ist dieses den Kryptowährungen und deren Handel gewidmet. Zuerst geht es um das Verwalten von Kryptowährungen in „Wallets“. Das zweite Unterkapitel beschäftigt sich mit dem *Initial Coin Offering* (ICO), welches zum Teil dem *Initial Product Offering* (IPO), der Erstplatzierung von Aktien an einer Börse, nahesteht. Die Handelsplätze und Börsen an denen mit Kryptowährungen gehandelt werden, werden anschließend erwähnt.

7.1 Identifizierung – Keys und Wallets

Zum sicheren Verwalten von Kryptowährungen werden sogenannte Wallets benutzt. Diese Wallets sind mit Wertpapier- oder Devisendepots vergleichbar. Man kann Währungen halten oder an andere transferieren. Im Gegensatz zu Girokonten können Wallets jedoch nicht überzogen werden, d.h. man kann nie mehr ausgeben als man hat. Wie in den folgenden Unterkapiteln klar wird, gibt es unterschiedlichste Formen von Wallets, welche Stärken und Schwächen aufweisen.

7.1.1 Hardwallets – Paperwallets

Hardwallets und Paperwallets sind sich vom Konzept her sehr ähnlich. Man versucht, seine Kryptowährungen hiermit offline zu speichern. Ein Paperwallet ist die einfachste Form eines Wallets, denn für ein Paperwallet wird nur ein Ausdruck eines *Private Keys* und eines *Public Keys* benötigt. Wobei der *Public Key*, vergleichbar mit einem IBAN, die öffentliche Adresse ist. Der *Private Key* dient als Passwort für den *Public Key*, weshalb er nicht an andere weitergegeben werden sollte. Zudem ist der *Private Key* nötig, um Transaktionen vom entsprechenden Konto durchzuführen. Somit ist es jedem, der sich den *Private Key* und den *Public Key* aneignet möglich, Transaktionen in Auftrag zu geben. Dadurch stellt das Paperwallet wohl die unsicherste Aufbewahrungsmöglichkeit von Kryptowährungen dar. (Franco, 2014, S. 127)

Im Gegensatz zu einem Zettel Papier erweist sich ein sogenanntes Hardwallet oder auch Hardwarewallet wesentlich sicherer. Als Hardwarewallets werden meist kleine Computer bezeichnet, welche *Keys* durch Passwörter sichern. Außerdem werden sie oft zur zwei-Faktor-Authentifizierung bei Überweisungen mit dazugehöriger Software verwendet. In Abbildung 10 ist ein Hardwarewallet namens „Ledger Nano S“ zu sehen.

Abbildung 10: Ledger Nano S (eigene Darstellung)

Der Anschluss erfolgt mittels USB-Kabel am Computer. Zum erstmaligen Einrichten und zum Eingeben des Passwortes werden zwei Tasten, sowie das Display benutzt. Mit Hilfe der Software, die ebenfalls von der Firma Ledger bereitgestellt wird, kann der Stick bis zu 18 verschiedene Kryptowährungs-Konten speichern. Laut Angaben der Firma ist er mit über 1,3 Mio. verkauften Stück das meistverkaufte Hardwallet weltweit. (www.ledger.com, 2018)

Die Verwendung solcher Hardwarewallets ist recht zeitintensiv, um Transaktionen schneller in Auftrag geben zu können, bieten sich Softwallets und Web basierte Wallets an.

7.1.2 Softwallets – Webwallets

Wie der Name vermuten lässt, liegen Soft- und Webwallets in Softwareform vor. Wie bei einer auf Hardware basierten Wallet muss auch bei einer auf Software basierenden die Sicherheit der Kryptowährungen im Wallet gewährleistet sein. Dies erfolgt in beiden Fällen hauptsächlich durch kryptografische Verschlüsselungen. Gegensätzlich zu externen Hardwallets, welche nicht direkt mit den jeweiligen Kryptowährungs-Netzwerken verbunden sind, ergibt sich ein erhöhtes Sicherheitsrisiko. (Franco, 2014 S. 131)

Bei Einrichtung eines neuen Wallets wird eine sogenannte „*Back-up-Phrase*“ erstellt. Diese *Back-up-Phrase* dient zum Wiederherstellen oder Synchronisieren des Wallets und ersetzt praktisch den *Private Key*. Die meisten Anwendungen verwenden weitere Sicherheitsmaßnahmen, wie zusätzliche Pins vor Überweisungsfreigabe oder die Authentifizierung über den Fingerabdruck bei Apps. (Franco, 2014, S. 131)

Webwallets bieten den Vorteil, dass sie mittels Browser-Plugin oder Internetseite durch jeden beliebigen Computer erreicht werden können und nicht wie Apps zuerst installiert werden müssen. Börsen bieten außerdem Webwallets an, um das Handeln zu erleichtern. Doch damit das Handeln einer Kryptowährung erst einmal möglich wird, muss diese Währung entwickelt werden. Die dafür nötigen finanziellen Mittel werden in einem sogenannten ICO aufgetrieben.

7.2 ICO (Initial Coin Offering)

Wie bei einem IPO (Initial Product Offering), bei dem Aktien von (Haupt-)Aktionären verkauft werden, wird bei einem ICO (Initial Coin Offering) ein gewisser Bestand an „Coins“ (=Währungseinheiten) verkauft. Die Preise der Währungen bleiben während dieser Phase entweder gleich oder steigen bis zum Enddatum. Manchmal gibt es auch ein sogenanntes Pre-Mining, bei dem Coins errechnet werden können. In gewisser Weise sind ICOs dem „Crowdfunding“ sehr ähnlich. Eine Parallele ist beispielsweise die größtenteils unregulierte Natur. Dazu ist das Risiko eines hohen Verlustes oder eines Totalverlustes hoch. (Hecht, 2018)

Die rechtliche Behandlung in vielen Ländern ist noch nicht geklärt. Während in Österreich derzeit noch keine Regulierungen in Bezug auf ICOs in Kraft getreten sind, gibt es in China und Südkorea seit 2017 ein ICO-Verbot. Singapur und die Schweiz haben sehr liberale Gesetzte, welche viele ICOs in beiden Ländern zur Folge haben. Trotz dem hohen Risiko gibt es jedoch genügend Anleger, welche in ICOs investieren. (Hecht, 2018)

7.3 Handelsplätze – Kryptowährungs-Börse

Die gängigsten Methoden um Kryptowährungen zu erwerben sind Kryptowährungs-Börsen und „Bitcoin-Automaten“. Der Automat nimmt Fiat-Geld (Geld in Form von gängigen Währungen, wie Euro oder US-Dollar) entgegen und druckt einen entsprechenden Bon mit einem Code aus, welcher Online eingelöst werden kann. Der Kurs wird mit dem Zeitpunkt des Kaufes angenommen, die Anbieter verlangen dazu oft hohe Spesen.

7.3.1 Börsen

Kryptowährungs-Börsen, meist online betrieben, verlangen im Gegensatz zu Automaten wesentlich geringere oder gar keine Gebühren. Während sich einige Börsen nur auf Kryptowährungen mit sehr hoher Marktkapitalisierung spezialisieren, gibt es einige mit einer Vielzahl an Währungen. Die Preise der verschiedenen Währungen werden oft zum Bitcoin oder dem „*Tether*“ (USDT) bemessen, wobei der *Tether* einen zum US-Dollar äquivalenten Wert hat. Vorteil von *Tether* ist, dass er die gleiche Wertstabilität des US-Dollars aufweist und man dadurch bei hoher Volatilität des Marktes schnell auf eine stabile Kryptowährung wie *Tether* wechseln kann. (CryptoCurrencyFacts, 2019)

Neben den für Börsen typischen Werkzeugen wie Auftragsbuch und Übersichten zu Kursen sowie Kauf- und Verkaufspreisen, gibt es auch die Möglichkeit, die Währungen untereinander umzuwechseln. Für den Tausch wird gewöhnlich eine Flatrate oder ein prozentueller Anteil an Spesen fällig. (www.hitbtc.com, 2018)

Zu den bekanntesten und größten Kryptowährungs-Börsen zählen: Binance, Bitfinex, HitBTC, Bittrex und Kraken. In Abbildung 11 sieht man den Bitcoin-*Tether* Kursverlauf links; rechts sind verschiedenste andere Währungen mit jeweiligen Werten gelistet. (CryptoCoinCharts, 2018)

Abbildung 11: Frontpage HitBTC (www.hitbtc.com, 2018)

Ab Sommer 2017 wird von vielen Börsen ein Mindestalter von 18 Jahren und eine Kopie eines Ausweises zur Identifikation eingefordert, um den „*Know your customer*“ Richtlinien Folge zu leisten. (www.hitbtc.com, 2018)

7.3.2 Know your customer (KYC) und Anti money laundering (AML)

Da sich der unbeschränkte und relativ anonyme Zugang zu Kryptowährungs-Börsen als problematisch erwies, wurden in den meisten Ländern Gesetzte geschaffen oder erweitert. Diese Gesetzte hatten nach dem Prinzip „*Know your customer*“ (KYC) zum Ziel, Geldwäscherei, Betrügerei und Terrorismusfinanzierung zu verhindern. Daraus lässt sich auch die zweite Abkürzung erschließen, welche für „*Anti money laundering*“ (AML) steht. (Comben, 2018)

Eine EU-Richtlinie war dazu bis Sommer 2017 umzusetzen, welche unter anderem beinhaltet, dass sich eine Person, die eine Geschäftsbeziehung mit einem Finanzinstitut eingeht, mit einem amtlichen Lichtbildausweis zu identifizieren hat. Außerdem erfolgt ein

solcher Nachweis bei Ein- und Auszahlungen von Spareinlagen ab einer Höhe von 15.000 Euro. (Bundesministerium für Finanzen, 2018)

Aus Angst vor Strafen rüsteten die meisten Börsen auf und verifizierten Konten erst nach einem gültigen Identitätsnachweis. Zusätzlich führten viele Anbieter die sogenannte 2-Faktor-Authentifizierung ein. Dabei muss der Nutzer beim Anmelden auf der Börsen-Website neben dem Passwort auch einen Code, welcher auf sein Handy gesendet wird, eingeben. (www.hitbtc.com, 2018)

8 Resümee

Zusammenfassend lässt sich sagen, dass eine Blockchain eine kontinuierlich wachsende, dezentrale Datenbank ist. Implementationen der Technik setzen auf öffentlichen Code, Dezentralität und Transparenz für die Netzwerkteilnehmer. *Time-Stamping* ermöglicht die grundsätzliche Funktion einer Blockchain. Zusammen mit den Minern, welche durch Berechnungen den *Proof-of-Work* liefern, mit wessen Hilfe die Sicherheit der Blockchain gewährleistet ist, stellen diese beiden Konzepte die Basis der Blockchain dar. Mit jeder Transaktion wächst die Blockchain, dies führt zwangsläufig zu einem Skalierungsproblem, welches durch SegWit2x oder durch das *Lightning Network* gelöst werden kann. Kryptowährungen werden auf Kryptowährungs-Börsen gehandelt. Aufbewahrt werden sie in Software- oder Hardwarewallets, welche durch Kryptografie gesichert sind. Dass die Wirtschaftlichkeit eines Miners stark vom Strompreis abhängt, wurde durch Berechnung gezeigt. Auch die Umweltauswirkungen der Transaktionen sind nicht zu unterschätzen.

Erkenntnisse der Arbeit gehen über die Leitfragen hinaus, so wurden beispielsweise die (potenziellen) Anwendungsgebiete der Blockchain genauer beleuchtet. Weiters konnte gezeigt werden, das ein Angriff auf die Bitcoin Blockchain ausgesprochen teuer und schwer zu bewerkstelligen ist. Außerdem ergibt sich ein umfassender Einblick in die Funktionsweise der Blockchain und Kryptowährungen sowie deren Handel.

Die gesammelten Erfahrungen aus dem praktischen Teil stellen einen Wissensgewinn im produktiven, wie auch im theoretischen Teil dar. So konnte im Experiment gezeigt werden, wie ein Miner aufgebaut ist und welche Software den Betrieb gewährleistet. Die Rentabilität wurde an Hand eines ASIC-Miners bestimmt, da die Berechnung für den selbst gebauten Miner den Rahmen dieser Arbeit sprengen würde. Neben der Analyse der Wirtschaftlichkeit ergab eine Neuberechnung, dass der CO_2-Ausstoß einer Bitcoin-Transaktion 161 kg beträgt. Umgelegt auf den selbst gebauten Miner ergibt sich ein hypothetischer CO_2-Ausstoß von 0,875 kg/h. Durch die Solarstromnutzung ist dieser Emissionswert in der Praxis jedoch geringer.

Trotz des limitierten Umfangs konnten die Stärken und Schwächen der Blockchain-Anwendungen aufgezeigt werden. Neben der hohen Umweltbelastung muss auch an der Skalierbarkeit der Bitcoin Blockchain gearbeitet werden. Hier wäre eine genauere Untersuchung der Umweltauswirkungen des Minigs interessant. Zudem bedarf es noch

einiges an Forschung im Hinblick auf die Skalierbarkeit der Blockchain. Zukünftig werden sich neue Anwendungsbereiche eröffnen. Neben den etablierten Kryptowährungen findet die Blockchain zukünftig Anwendung in den Bereichen wie: *Supply-Chain-Managment* und *Internet of Things*. Vorteile wie die Rückverfolgbarkeit und Sicherheit der Kryptografie bewähren sich in allen Anwendungsbereichen.

Gelingt es die bestehenden Probleme zu lösen, wird die Blockchain künftig herkömmliche Datenbanken ablösen. Somit ist es sehr naheliegend, dass die Blockchain zur Basis der Industrie 4.0 werden wird und die Digitalisierung maßgeblich vorantreibt.

Abbildungsverzeichnis

Literaturverzeichnis

@CircusDad. (10. 6. 2018). *Vegamininggguides.com*. Abgerufen am 18. 7. 2018 von http://vega.miningguides.com/

Amazon. (24. 1. 2018). Abgerufen am 23. 7. 2018 von https://www.amazon.de/dp/B0799HQZCN?linkCode=df0&creative=22398&smid=A3JWKAKR8XB7XF&tag=geizhals1-21

Bitcoin Wiki. (19. 9. 2018). Abgerufen am 31. 10. 2018 von https://en.bitcoin.it/wiki/Bitcoin

Bitmain. (2018). Abgerufen am 31. 10. 2018 von https://shop.bitmain.com/promote/antminer_s9i_asic_bitcoin_miner/

specification

Bricklebrit Lastgangbepreisung. (1. 11. 2018). Leipziger Strombörse (Spotmarkt D). Abgerufen am 1. 11. 2018 von http://www.bricklebrit.com/stromboerse_leipzig.html

Bundesministerium für Finanzen. (2018). *www.bmf.gv.at.* Abgerufen am 2. 8. 2018 von https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/geldwaesche.html

Buterin, V. (2013). Ethereum White Paper. *A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM*, 19-23. Abgerufen am 2. 8. 2018 von http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

CoinMarketCap. (16. 7. 2018). Abgerufen am 16. 7. 2018 von https://coinmarketcap.com/all/views/all/

Coinwarz.com. (16. 07. 2018). Abgerufen am 16. 7. 2018 von https://www.coinwarz.com/network-hashrate-charts/bitcoin-network-hashrate-chart

Comben, C. (26. 8. 2018). Have You Ever Wondered What Really Geos into KYC/AML? Abgerufen am 1. 11 2018 von https://coincentral.com/kyc-aml/

Crocosource.com. (2019). Abgerufen am 18. 01. 2019 von https://www.crocosource.com/coins/algo/

CryptoCoinCharts. (1. 11. 2018). Abgerufen am 1. 11. 2018 von https://cryptocoincharts.info/markets/info

CryptoCurrencyFacts. (2019). Abgerufen am 18. 1. 2019 von https://cryptocurrencyfacts.com/what-is-tether/

Deetman, S. (29. 3. 2016). Bitcoin Could Consume as Much Electricity as Denmark by 2020. Abgerufen am 1. 11. 2018 von https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020

Digiconomist. (31. 10. 2018). Bitcoin Energy Consumption Index. Abgerufen am 1. 11. 2018 von https://digiconomist.net/bitcoin-energy-consumption

Franco, P. (2014). *Understanding Bitcoin. Cryptography, Engineering and Economics [E-Book].* Hoboken, New Jersey: Wiley.

Hecht, J. (4. 7. 2018). *www.diepresse.com.* Abgerufen am 1. 8. 2018 von https://diepresse.com/home/wirtschaft/recht/5458730/ICO_Auf-der-Suche-nach-rechtlichen-Vorbildern

Hernández, S. G. (12. 2017). Bitcoin or the environment: you choose. Berlin. Abgerufen am 1. 11. 2018 von https://www.institut-fuer-sozialstrategie.de/wp-content/uploads/2014/10/nu_ifs_galeano_bitcoin.pdf

Hosp, J., & Mahrer, H. (2017). *Kryptowährungen. Bitcoin, Ethereum, Blockchain, ICO's & Co. einfach erklärt [E-Book].* Singapur.

Ismail, B. (7. 1. 2018). *quora*. Abgerufen am 12. 7. 2018 von https://www.quora.com/What-is-the-best-programming-language-to-learn-if-you-want-to-work-on-the-blockchain

Levy, N. (27. 8. 2018). Second Amazon Go store opens in Seattle with further expansion on the horizon. Abgerufen am 31. 10. 2018 von https://www.geekwire.com/2018/second-amazon-go-store-opens-seattle-expansion-horizon/

Meissner, M. (3. 8. 2017). *CHINAS GESELLSCHAFTLICHES BONITÄTSSYSTEM.* Abgerufen am 30. 7. 2018 von https://www.merics.org/sites/default/files/2017-09/China%20Monitor_39_SOCS_DE.pdf

Nakamoto, S. (31. 10. 2008). *www.bitcoin.org*. Abgerufen am 23. 7. 2018 von https://bitcoin.org/bitcoin.pdf

Oberhaus, D. (30. 11. 2017). *Motherboard.vice*. Abgerufen am 13. 7. 2018 von https://motherboard.vice.com/en_us/article/ywnmkk/coinbase-irs-14000-bitcoin-tax

Orlov, A. (2017). Blockchain in the Electricity Market: Identification and Analysis of Business Models. 48-51. Abgerufen am 31. 10. 2018 von https://brage.bibsys.no/xmlui/bitstream/handle/11250/2486421/masterthesis.PDF?sequence=1&isAllowed=y

Poon, J., & Dryja, T. (14. 1. 2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Abgerufen am 31. 10. 2018 von https://lightning.network/lightning-network-paper.pdf

Popov, S. (30. 4. 2018). The Tangle. *(Version 1.4.3)*. Abgerufen am 2. 8. 2018 von https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

ripple.com. (2018). Abgerufen am 2. 8. 2018 von https://ripple.com/company/

Smith, P. (2017). *Blockchain.com*. Abgerufen am 16. 7. 2018 von https://www.blockchain.com/de/pools

Smith, P. (21. 7. 2018). *www.blockchain.com*. Abgerufen am 23. 7. 2018 von https://www.blockchain.com/de/charts/blocks-size?timespan=all&scale=1

Sraders, A. (3. 8. 2018). Pay Attention to These 7 Bitcoin Scams in 2018. Abgerufen am 1. 11. 2018 von https://www.thestreet.com/investing/bitcoin/bitcoin-scams-14640202

Steem. (6. 2018). *An incentivized, blockchain-based, public content platform.* Abgerufen am 2. 8. 2018 von https://steem.io/steem-whitepaper.pdf

Tapscott, A., & Tapscott, D. (2016). *Die Blockchain Revolution* (4. Auflage 2018 Ausg.). (B. AG, Übers.) Kulmbach: Börenmedien AG.

The Engineering ToolBox. (2009). Abgerufen am 1. 11. 2018 von https://www.engineeringtoolbox.com/co2-emission-fuels-d_1085.html

Torpey, K. (31. 10. 2017). *Forbes.* Abgerufen am 31. 10. 2018 von https://www.forbes.com/sites/ktorpey/2017/10/31/is-bitcoin-facing-a-corporate-takeover-via-the-2x-fork-a-developer-and-a-business-leader-debate/#336690263bff

van Saberhagen, N. (17. 10. 2013). CryptoNote v 2.0. Abgerufen am 2. 8. 2018 von https://cryptonote.org/whitepaper.pdf

Vechain. (5. 2018). Development Plan and Whitepaper. Abgerufen am 31. 10. 2018 von https://cdn.vechain.com/vechainthor_development_plan_and_whitepaper_en_v1.0.pdf

www.hitbtc.com. (2. 8. 2018). Abgerufen am 2. 8. 2018 von https://hitbtc.com/exchange

www.ledger.com. (10. 7. 2018). Abgerufen am 1. 8. 2018 von https://www.ledger.com/products/ledger-nano-s

Selbstständigkeitserklärung

Ich erkläre, dass ich diese vorwissenschaftliche Arbeit eigenständig angefertigt und nur die im Literaturverzeichnis angeführten Quellen und Hilfsmittel benutzt habe.

Großhartmannsdorf, 26. 2. 2019 Unterschrift