Das Potenzial von Kryptowährungen

Maturaarbeit

Marco Gabriel
Kollegium St. Fidelis
Stans, 18.10.2018

Inhaltsverzeichnis

Vorwort 4

Motivation 4

Danksagung 4

Abstract 5

1 Einleitung 5

1.1 Ziele 5

1.2 Leitfragen 5

1.3 Methoden 6

2 Kryptowährungen 6

2.1 Was sind Kryptowährungen? 6

2.2 Funktionsweise 7

2.2.1 Blockchain 7

2.2.2 Kryptografie 8

2.2.3 Hash 8

2.2.4 Asymmetrische Verschlüsselung 9

2.2.5 Netzwerk 11

2.2.6 Transaktionen 12

2.2.7 Entstehung und Eigenschaften der Blöcke 13

2.2.8 Verzweigte Blockchain 15

3 Eigenschaften von Kryptowährungen 16

3.1 Instabile Wechselkurse 16

3.2 Falschgeld 17

3.3 Varianten der Blockerstellung 17

3.4 Manipulation der Blockchain 17

3.5 Ressourcen Verbrauch 21

3.5.1 Strom ... 21
3.5.2 Hardware ... 22
3.5.3 Speicherplatz ... 23
3.6 Dezentrales Mining ... 23
3.7 Dezentral oder Zentral ... 24
3.8 Transaktionsgeschwindigkeit ... 24
3.9 Illegaler Handel und Geldwäsche ... 25
4 Wie werden Kryptowährungen gesetzlich geregelt? ... 26
4.1 Geldwäsche ... 27
4.2 Steuern in der Schweiz ... 27
5 Lohnt es sich für Unternehmen, Kryptowährungen zu akzeptieren? ... 29
6 Diskussion ... 31
7 Schlusswort ... 33
8 Anhang ... 34
8.1 Literaturverzeichnis ... 34
8.1.1 Abbildungen ... 38
8.1.2 Interviews ... 39
8.2 Eigenständigkeitserklärung ... 42

Vorwort

Motivation

Ich beschäftige mich schon seit Anfang 2017 mit Kryptowährungen und wie man mit ihnen umgeht. Was diese genau sind, werde ich in Kapitel 2 erklären. Ich kaufte am 1. Januar 2017 am Ticketautomaten des Stanser Bahnhofs für zwanzig Franken meine ersten Bitcoins zu einem Kurs von eintausend Franken pro Bitcoin, und begann, meinen Computer zur Gewinnung von Gridcoin einzusetzen. Im Dezember 2017 stieg der Wert eines Bitcoins auf fast 20‘000 Franken[1]. Genau zu dieser Zeit wählte ich das Thema für meine Maturaarbeit. Der Hype um Bitcoin machte dieses Thema für mich noch interessanter, aber mein Interesse galt schon damals nicht nur den Spekulationen mit Kryptowährungen, sondern auch der Blockchain-Technologie im Allgemeinen und der praktischen Anwendung von Kryptowährungen. Auch die Blockchain-Technologie werde ich im zweiten Kapitel erläutern. Ein weiterer Grund für meine Themenwahl war der Umstand, dass Kryptowährungen noch nicht von vielen Leuten genutzt werden, ich aber trotzdem an deren Potenzial glaube.

Danksagung

Ich möchte meinen Interviewpartnern, Christoph Schneeberger, Phillipp Röll und Rene Odermatt herzlich für ihre Offenheit danken. Meinem Mentor Urs Zellweger danke ich für das Vertrauen und die Freiheit die er mir gelassen hat. Mein Dank geht auch an die Balmer-Etienne AG, an deren Veranstaltung ich ein Referat von Dr. rer. pol. Fabian Schär anhören durfte. Meinen Eltern, Verwandten, Kollegen und Kolleginnen danke ich für ihre Unterstützung beim Verbessern meiner Dokumentation.

[1] Poloniex.com

Abstract

Kryptowährungen werden momentan meist nur für Spekulationen verwendet, obwohl sie als Zahlungsmittel gedacht sind. Die Technologie von Kryptowährungen besitzt das Potenzial, den Zahlungsverkehr zu modernisieren, aber auch zu dezentralisieren. Es würden keine Banken mehr für Online Zahlungen benötigt werden. Kryptowährungen existieren erst seit kurzer Zeit und haben bis jetzt noch einige Probleme. Jedoch können durch Weiterentwicklung und weiterer Verbreitung ihre Vorteile gegenüber dem traditionellen System überwiegen. Dadurch wären sie als digitalen Ersatz des Zahlungsverkehrs der Banken anwendbar.

1 Einleitung

1.1 Ziele

Mit meiner Maturaarbeit möchte ich nicht stark auf die Chancen und Wertentwicklungen einzelner Kryptowährungen eingehen. Mein Ziel ist es, zu analysieren, ob und wie Kryptowährungen im Alltag verwendet werden können. Aufgrund der grossen Anzahl von Kryptowährungen werde ich nur auf die verbreitetsten Arten eingehen. Begleitend möchte ich die Differenzen verschiedener Kryptowährungen und ihre Stärken und Schwächen darlegen. Den rechtlichen Aspekt will ich auch nicht ausser Acht lassen, denn dieser ist sehr zentral wenn es um die Verwendung von Kryptowährungen geht.

1.2 Leitfragen

Um diese Ziele zu erreichen, stelle ich drei Leitfragen auf. Zuerst möchte ich beantworten, welche Arten von Kryptowährungen es gibt, welche Eigenschaften sie jeweils haben und worin sie sich unterscheiden. Darauf aufbauend will ich mithilfe von Interviews mit Unternehmen herausfinden, ob sich Kryptowährungen als Zahlungsmittel eignen. Auch die konkreten Vor- und Nachteile im Vergleich zu herkömmlichen Zahlungsmitteln möchte ich herausfinden. Schlussendlich möchte ich mich auch damit auseinandersetzen, wie Kryptowährungen gesetzlich geregelt werden, vor allem wie man sie versteuern muss.

> Welche Eigenschaften besitzen verschiedene Kryptowährungen?
> Lohnt es sich für Unternehmen, Kryptowährungen als Zahlungsmittel zu akzeptieren?
> Wie werden Kryptowährungen gesetzlich geregelt?

1.3 Methoden

Ich habe mich schon vor dem Erarbeiten der Maturaarbeit gerne mit Kryptowährungen beschäftigt, und habe daher bereits Grundkenntnisse in den meisten Gebieten, mit denen ich mich auseinandersetzen wollte. Anfangs habe ich im Internet recherchiert, wie Kryptowährungen gesetzlich geregelt sind und wie man sie versteuern muss. Danach habe ich viele verschiedene Webseiten, Foren und Blogs durchgelesen, die das Blockchain System erklären und ein von der Balmer-Etienne AG organisiertes Referat von Dr. rer. pol. Fabian Schär besucht. Daraufhin befragte ich meine Interviewpartner, Unternehmen welche bereits Kryptowährungen akzeptieren, nach ihren Erfahrungen mit diesem Zahlungsmittel. Ich analysierte und verglich ihre Antworten miteinander und auch mit meinen bisherigen Erkenntnissen.

2 Kryptowährungen

In diesem Kapitel erkläre ich die Grundlagen von Kryptowährungen, also was sie sind und wie sie funktionieren. Dabei gehe ich auch auf die technischen Details ein, allerdings nicht exakt, es geht nur um das jeweilige Prinzip.

2.1 Was sind Kryptowährungen?

Kryptowährungen sind eine neue Art von Geld. Der offensichtlichste Unterschied ist, dass Kryptowährungen rein digital existieren. Das Ziel von Kryptowährungen ist, eine Alternative zum bisher stark zentralisierten Geldmarkt darzustellen, welcher auf Vertrauen in eine Zentralbank basiert[2]. Kryptowährungen werden dezentral organisiert und entziehen sich somit dem Einfluss von Regierungen und Banken. Es gibt sehr viele verschiedene Kryptowährungen, doch allgemein gilt[3], dass Transaktionen schneller abgewickelt werden als Banküberweisungen und die Transaktionsgebühren tief sind. Des Weiteren sind Kryptowährungen anonym und frei von Regulierungen.

Kryptowährungen basieren auf öffentlichen, kryptografischen Systemen. Diese Systeme werden nicht auf den Servern von Banken betrieben, sondern auf Computern auf der ganzen Welt. Die meisten Kryptowährungen, darunter Bitcoin und Ethereum, basieren auf der Blockchain-Technologie. Auf Alternativen zur Blockchain, wie „Tangle“, worauf die Kryptowährung IOTA basiert, wird in dieser Arbeit nicht eingegangen.

[2] Vgl. Nakamoto, Satoshi. Bitcoin open source implementation of P2P currency, 11.02.2009.
[3] Vgl. Cryptocurrencyarmy.com

2.2 Funktionsweise

2.2.1 Blockchain

Eine Blockchain ist, wie der Name schon erahnen lässt, eine Kette von Blöcken. Die Blockchain fungiert als manipulationssicheres Verzeichnis. In diesem Verzeichnis wird, im Fall von Kryptowährungen, festgehalten, wer wie viel Geld besitzt.[4] Damit diese Information stets aktuell ist, wird der Blockchain periodisch ein neuer Block angehängt. In diesem Block stehen jeweils die neusten Transaktionen. Die älteren Blöcke werden durch die neueren, oben aufliegenden Blöcke gefestigt, wodurch diese nicht mehr verändert werden können.

In Bezug auf das Besitzen von Kryptowährungen bedeutet dies, dass man Kryptowährungen nicht wie Bargeld im Portemonnaie aufbewahrt, sondern dass man in der Blockchain als Besitzer eines bestimmten Betrages eingetragen ist. Wenn man nun einen Teil seines Vermögens einer anderen Person überweisen will, muss man nur dafür sorgen, dass die entsprechende Transaktion in den nächsten Block geschrieben und an die Blockchain gehängt wird.

Ein System, ähnlich der Blockchain, wurde schon vor hunderten von Jahren auf den Yap-Inseln in Mikronesien verwendet. Die Bewohner der Inseln benutzten Steinscheiben mit einem Durchmesser von bis zu 4 Metern als Geld. Die Steinscheiben, Rai genannt, mussten mühsam von weit entfernten Inseln auf Flössen herangeschafft werden. Die Anzahl der Steinscheiben war somit stark begrenzt, deren Wert entsprechend hoch. Jeder Einwohner wusste, welcher Stein wem gehört, und Besitzerwechsel sprachen sich jeweils schnell herum. Weil sowieso jeder wusste, wem welcher Stein gehört, wurde auf den anstrengenden Transport der Rai verzichtet. So kam es, dass es genügte, dem Kollektiv als Besitzer bekannt zu sein, ohne sein Reichtum im eigenen Garten liegen zu haben. Diese Angewohnheit ging so weit, dass auch mit Steinscheiben gehandelt wurde, die während des Transportes vom Floss fielen und fortan auf dem Meeresgrund lagen.[5]

Das kollektive Gedächtnis der Inselbewohner ist vergleichbar mit einer Blockchain, denn darin wird festgehalten, wer wie viel besitzt. Die Steine wiederum sind vergleichbar mit einer Kryptowährung, welche man auch nicht physisch besitzt.

Die Basis einer Kryptowährung ist die Blockchain, auf der sie gehandelt wird. Die Blockchain ist öffentlich und wird oft, aber nicht immer, von einem dezentralen Netzwerk betrieben. Die Blockchain von Bitcoin ist zum Beispiel auf der Webseite *Blockchain.info* einsehbar. Auf einer

[4] Vgl. D'Aliessi, Michele. How Does the Blockchain Work?, 01.06.2016.
[5] Vgl. Postfinance.ch

Blockchain können mehrere Währungen gehandelt werden. Auf der Bitcoin-Blockchain gibt es beispielsweise nicht nur Bitcoin, sondern auch Tether, eine Währung deren Wert an den US-Dollars gebunden ist. Auf der Ethereum-Blockchain werden sogar über hundert Kryptowährungen gehandelt.

2.2.2 Kryptografie

In den bisherigen Erklärungen wurde der Aspekt der Sicherheit weggelassen. Sicherheit ist aber im Umgang mit Vermögen sehr wichtig. Herkömmliche Banken setzen dabei unter anderem auf Unterschriften, PIN-Codes und Identitätskontrollen. Bei Kryptowährungen sorgen kryptografische Funktionen für die Sicherheit. Grundlegend für Kryptowährungen ist einerseits eine Hashfunktion, andererseits eine asymmetrische Verschlüsselungsmethode. Beide Verfahren werden nachfolgend genauer erklärt.

2.2.3 Hash

Eine wichtige Eigenschaft von Hashfunktionen ist, dass es für Computer sehr leicht ist, den Hashwert eines Inputs auszurechnen, aber praktisch unmöglich ist, von einem Hashwert auf den Input zu schliessen. Eine Hashfunktion ist somit eine Einwegfunktion. Eine weitere Eigenschaft ist, dass bereits kleinste Änderungen am Input ein komplett anderes Ergebnis verursachen. Aufgrund dieser Eigenart werden Hashfunktionen benutzt, um effizient zu überprüfen, ob Dateien manipuliert oder beschädigt wurden. Man muss dafür nur die Hashwerte der beiden Dateien vergleichen, nicht deren ganzen Inhalt. Der Aufbau einer Hashfunktion ist relativ simpel. Sie verlangt als Input eine beliebig grosse Zahl oder einen beliebig langen Text und gibt als Ergebnis eine Zahl zurück. Dieses Ergebnis wird Hashwert genannt. Der Hashwert ist garantiert kleiner als ein bestimmter Maximalwert, deswegen ist die Länge des Inputs egal. Dieser Maximalwert ist allerdings eine sehr grosse Zahl, darum werden Hashwerte zur besseren Lesbarkeit oft nicht nur mit Ziffern, sondern auch mit Buchstaben dargestellt. Aufgrund der Einschränkung durch den Maximalwert, ist es möglich, dass mehrere Inputs denselben Hashwert ergeben, denn es gibt nur eine endliche Anzahl von möglichen Hashwerten.

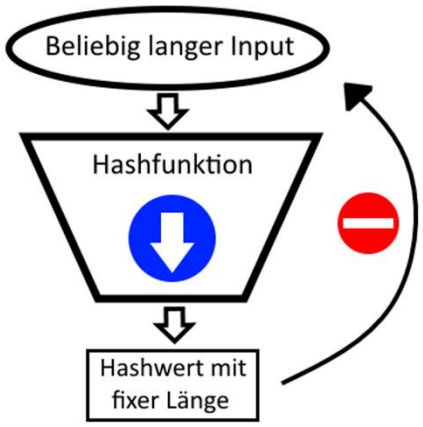

Abb. 1: Bildliche Darstellung einer Hashfunktion

Das Prinzip von Hashfunktionen lässt sich einfach anhand der MD5-Hashfunktion demonstrieren[6]. Der Hashwert der Hausordnung[7] des Kollegiums, welche zwei A4 Seiten umfasst, lautet *24ea5fc37099d8450ec6fa3fcb96566c*. Wenn nun ein Schüler deren Text manipuliert, zum Beispiel von „Die Mensa ist […] handyfrei“ zu „Die Mensa ist […] *nicht* handyfrei“, ändert sich der Hashwert zu *516d797b90285b748aa736377d131d8e.* Obwohl die Änderung am Input nur klein ist, ist der Hashwert komplett anders, man erkennt sofort, dass es sich nicht um die offizielle Hausordnung handelt. Auch bei kurzen Inputs sind die Hashwerte etwa gleich lang, der Hashwert von *Matura 19* ist *5982f7a5d71ec827017eb4b26efd2e08.*

2.2.4 Asymmetrische Verschlüsselung

Herkömmliche Verschlüsselungsverfahren benutzen denselben Schlüssel zum Verschlüsseln, wie auch zum Entschlüsseln einer gegebenen Information. Diese Verfahren werden als symmetrische Verfahren bezeichnet. Das Hauptproblem bei diesen Verfahren liegt darin, dass der Absender einer Nachricht dem Empfänger vorgängig den Schlüssel geben muss. Vor vergleichsweise kurzer Zeit, in den 70er Jahren des zwanzigsten Jahrhunderts, wurde eine neue Art der Verschlüsselung erfunden, die asymmetrische Verschlüsselung[8].

Das neue Verfahren verwendet zwei verschiedene Schlüssel. Einen für die Verschlüsselung und einen anderen für die Entschlüsselung. Um solch ein Schlüsselpaar zu erhalten, wählt man zuerst möglichst zufällig einen Schlüssel, aus welchem dann der zweite durch mathematische Funktionen errechnet wird. Die Eigenschaft dieses Schlüsselpaares ist, dass eine Nachricht, die mit einem der beiden Schlüssel verschlüsselt wurde, nur durch den jeweils anderen entschlüsselt werden kann[9].

[6] Lemats.net
[7] Kollegistans.ch
[8] Vgl. Burgess, Jed et al. Public Key Cryptography.
[9] Vgl. Pacia, Chris. Bitcoin Explained Like You’re Five: Part 3 – Cryptography, 07.09.2013.

In der Praxis ermöglicht diese Eigenschaft, auf simple Weise relativ sicher zu kommunizieren. Jede Partei generiert für sich ein solches Schlüsselpaar. Einer der Schlüssel wird geheim gehalten und als privaten Schlüssel bezeichnet. Der andere Schlüssel wird öffentlicher Schlüssel genannt und mit jedem geteilt, der danach fragt. Wenn man jemandem etwas verschlüsselt mitteilen möchte, kann man seine Nachricht ganz einfach mit dem öffentlichen Schlüssel des Empfängers verschlüsseln[10]. Eine Nachricht die mit dem öffentlichen Schlüssel verschlüsselt ist, kann mit diesem nicht mehr entschlüsselt werden. Diese Nachricht kann nur vom Empfänger gelesen werden, da er den entsprechenden privaten Schlüssel kennt. Ermöglicht wird das, weil es praktisch unmöglich ist, den privaten Schlüssel herauszufinden, auch wenn man den korrespondierenden öffentlichen Schlüssel kennt. Es ist aber wichtig, den privaten Schlüssel sicher aufzubewahren.

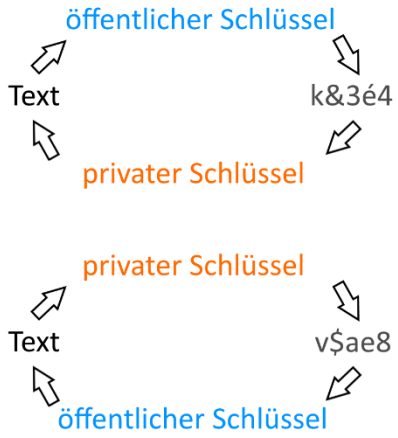

Abb. 2: Funktionsweise von asymmetrischer Verschlüsselung

Zusätzlich zum Verschlüsseln einer Nachricht mit dem öffentlichen Schlüssel des Empfängers, kann der Absender den Hashwert der Nachricht mit seinem eigenen privaten Schlüssel verschlüsseln und auch dem Empfänger zuschicken[11]. Dieser verschlüsselte Hashwert kann von jedem entschlüsselt werden, denn der dafür notwendige Schlüssel ist öffentlich. Der Umstand, dass der Hashwert mit dem öffentlichen Schlüssel decodierbar ist, beweist jedoch, dass wirklich der Absender diese exakte Nachricht verfasst hat, und nicht jemand, der sich als ihn ausgeben will. Denn nur der Absender besitzt seinen privaten Schlüssel, und damit die Fähigkeit, den Hashwert seiner Nachricht so zu verschlüsseln, dass er mit seinem öffentlichen Schlüssel entschlüsselbar ist. Wenn die Nachricht von einer Drittpartei manipuliert wird, stimmt der wirkliche Hashwert der Nachricht nicht mehr mit dem Hashwert überein, der mit dem privaten Schlüssel des Absenders codiert ist. Die Drittpartei kennt den privaten Schlüssel nicht, und kann somit den Hash der manipulierten Nachricht nicht richtig

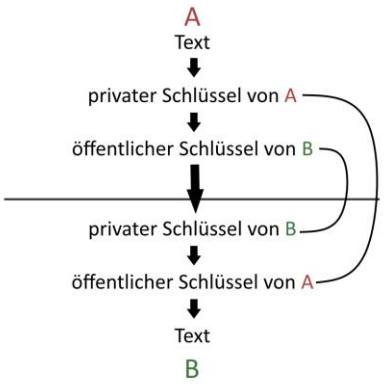

Abb. 3: Asymmetrisch verschlüsselte Kommunikation zwischen zwei Personen

[10] Vgl. IBM.com
[11] Vgl. Stackoverflow.com

verschlüsseln. Der Prozess des Verschlüsselns eines Hashwertes mit dem privaten Schlüssel wird „signieren“ genannt[12].

In folgender Abbildung stellt der Manipulator einen Schüler dar, der seine Note von einer 3 auf eine 6 ändern will. Sein Betrugsversuch fällt jedoch auf, weil er den privaten Schlüssel des wahren Absenders nicht kennt, und somit die Nachricht nicht korrekt signieren kann. Dadurch entsteht beim Empfänger eine Unstimmigkeit beim Vergleichen der Hashwerte.

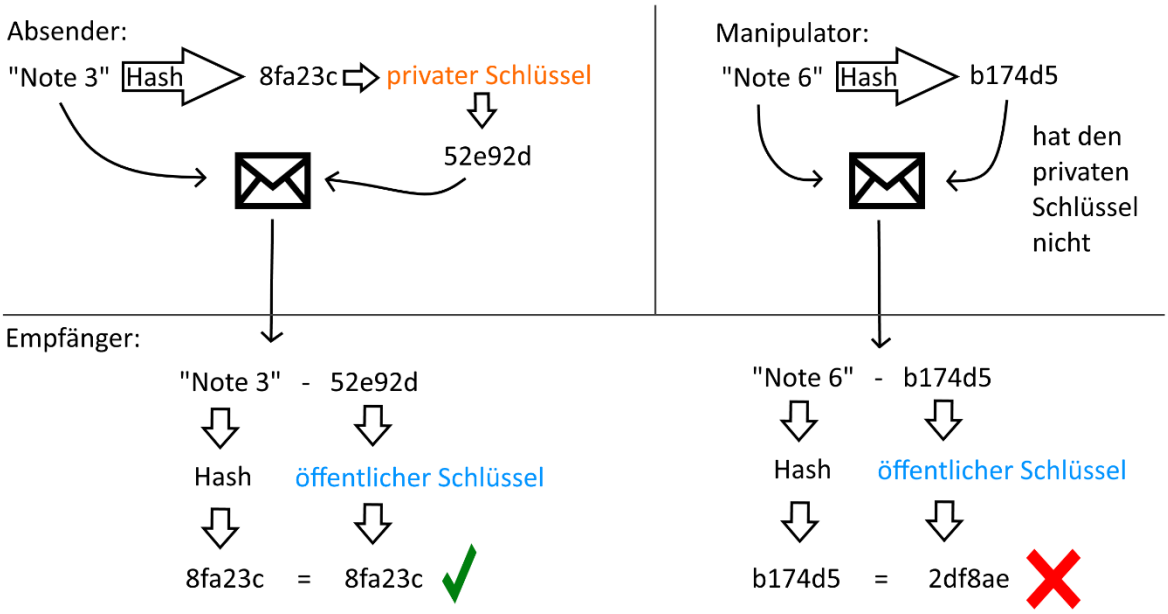

Abb. 4: Beispiel des Signierens einer Nachricht

2.2.5 Netzwerk

Das Netzwerk, welches eine Blockchain betreibt, besteht aus vielen einzelnen handelsüblichen Computern, manchmal auch auf eigens dafür entwickelten, und daher hocheffizienten Mikroprozessoren. Die Betreiber dieser Computer werden „Miner“, also Bergarbeiter oder Schürfer genannt, weil ihre Computer die Arbeit erledigen, die für die Sicherheit der Blockchain benötigt wird. Im Gegenzug werden sie mit Geld belohnt, welches sie sozusagen abbauen.

Wenn jemand eine neue Transaktion abwickeln möchte, wird die Information von einem Computer zum Nächsten verbreitet, bis das ganze Netzwerk davon weiss. Die Transaktion ist damit Teil einer grösseren Anzahl von Transaktionen, die darauf warten, bestätigt und in die Blockchain aufgenommen zu werden. Jede Transaktion beinhaltet eine kleine Gebühr,

[12] Vgl. Oracle.com

die derjenige Miner erhält, welcher die Transaktion in die Blockchain einbaut. Die Miner haben eine Auswahl von Transaktionen, von denen sie einige in den nächsten Block aufnehmen können. Jeder Miner kann selbst entscheiden, welche, oder ob er überhaupt Transaktionen in den nächsten Block aufnimmt. Die Miner müssen jede Transaktion verifizieren, das heisst sie müssen überprüfen, ob die Signatur mit der Nachricht übereinstimmt und der Auftraggeber über genügend Vermögen verfügt. Wenn ein Miner in seinem Block ungültige Transaktionen hat, wird der Block vom restlichen Netzwerk nicht akzeptiert, und seine Arbeit war umsonst. Die Miner nehmen also grösstenteils die Transaktionen auf, welche die höchsten Gebühren offerieren, denn sie handeln meistens gewinnorientiert.

2.2.6 Transaktionen

Eine Transaktion ist einer Verschlüsselung ähnlich. Vermögen welches Person A besitzt, lautet in der Blockchain auf die öffentliche Adresse von Person A. In der Blockchain steht zum Beispiel: *5 Bitcoins gehören 1NU2XcDRiJrgBckoxwxDCYXGXCi5mA4sUw*. Eine öffentliche Adresse kann als Synonym zu einem öffentlichen Schlüssel betrachtet werden. Das Vermögen von Person A ist sozusagen mit ihrem öffentlichen Schlüssel verschlüsselt. Um ihr Vermögen auszugeben[13], benötigt Person A ihren privaten Schlüssel, um ihr Vermögen zu entschlüsseln, oder genauer gesagt, die Transaktion zu signieren[14]. Das verschlüsselt sie dann mit dem öffentlichen Schlüssel von der Person, der sie das Geld überweisen möchte. Eine Transaktion kann man sich also auch als Pfeil von einer Adresse zur nächsten vorstellen. Wenn das Geld immer weitergegeben wird, entsteht aus den einzelnen Transaktionen eine Art Kette. Diese Erklärung ist etwas vereinfacht, aber sie erklärt das Prinzip und veranschaulicht, dass das, was als Vermögen bezeichnet wird, eigentlich nur das momentane Ende einer Transaktionskette ist. In der Abbildung 5 steht *pubK* für den öffentlichen Schlüssel, *privK* bedeutet privater Schlüssel und der nachfolgende Kleinbuchstabe zeigt an, zu wem der jeweilige Schlüssel gehört. In der Transaktion entschlüsselt Person A ihr Vermögen, das auf ihren öffentlichen Schlüssel lautet, mit ihrem privaten Schlüssel, und verschlüsselt es anschliessend mit Person Bs öffentlichem Schlüssel. Die Transaktion von Person A zu Person B stellt nun das Vermögen von Person B dar. Dieses könnte sie nun wiederum mit ihrem privaten Schlüssel an eine dritte Person weitersenden.

Abb. 5: Darstellung einer Transaktion von Person A an Person B

[13] Vgl. Coindesk.com
[14] Vgl. Stackexchange.com

Die Funktionsweise der Transaktionen bedeutet auch, dass einzig ein privater Schlüssel benötigt wird, um Bitcoins zu besitzen, die an die korrespondierende öffentliche Adresse gesendet wurden. Wenn es jemandem gelingt, den privaten Schlüssel zu stehlen, kann er die Bitcoins an seine eigene Adresse schicken. Deswegen muss der private Schlüssel immer sicher aufbewahrt werden. Zum Beispiel kann man ihn auf Papier ausdrucken. Wenn man auch die öffentliche Adresse ausdruckt, hat man eine sogenannte Paper-Wallet. Eine Paper-Wallet ist ein Portemonnaie in Papierform. Man kann Bitcoins auf die gedruckte Adresse einzahlen, und mit dem gedruckten privaten Schlüssel wieder vom Papier weg, auf eine andere Adresse senden. Ähnlich wie man Geld in ein Portemonnaie stecken, und wieder rausnehmen kann. Dabei darf man nicht vergessen, dass die Bitcoins zu keiner Zeit wörtlich auf dem Papier gespeichert sind. Sie bleiben immer auf der Blockchain, auf dem Papier ist lediglich der Zugangsschlüssel gespeichert.

2.2.7 Entstehung und Eigenschaften der Blöcke

Ein Block besteht im Fall von Bitcoin zum grössten Teil aus Transaktionen, aber auch aus einem sogenannten Blockheader. Im Header stehen diverse Informationen, wie der Zeitpunkt der Erstellung des Blockes, aber auch der Hashwert aller Transaktionen in diesem Block. Somit garantiert der Blockheader die Integrität seiner Transaktionen.

Da jeder Block den jeweils vorhergehenden Block gegen Manipulationen schützen muss, enthält der neue Block in seinem Header auch den Hashwert des vorherigen Blockheaders. Die neu generierten Blöcke sind somit essenziell für die Sicherheit der Blockchain. Falls ein alter Block manipuliert werden sollte, würde dessen Header-Hashwert nicht mehr mit dem Wert im nachfolgenden Block übereinstimmen. Die Erzeugung der neuen Blöcke ist somit ein Prozess, der sehr wichtig für das Funktionieren und die Sicherheit einer Kryptowährung ist. Es gibt verschiedenste Ansätze, die ein korrektes und effizientes Ablaufen dieses Prozesses ermöglichen sollen.

Bitcoin und viele andere Systeme verwenden das Proof of Work System. Damit ein von einem Miner neu erstellter Block vom ganzen Netzwerk anerkannt und somit der öffentlichen Blockchain angehängt wird, muss der Miner beweisen, dass er viel Arbeit dafür geleistet hat. Das Netzwerk akzeptiert nur Blöcke, deren Header einen Hashwert ergibt, der kleiner ist als ein bestimmter Wert. Bildlich betrachtet bedeutet das, dass der Hashwert des Headers mit einigen Nullen beginnen muss. Die Chance, dass der Hashwert mit einigen Nullen beginnt, ist sehr klein. Aber jede kleine Änderung am Inhalt des Blocks hat einen neuen Hashwert zur Folge. Der Miner hat die Möglichkeit, eine kleine Zahl in den Blockheader einzufügen, die sogenannte Nonce. Unter Nonce versteht man eine zufällige Zahl, die nur einmal verwendet

wird. Wenn der Hashwert nicht mit genug Nullen beginnt, kann eine andere Nonce gewählt werden, wodurch sich der Hashwert verändert und eventuell den Anforderungen entspricht. Die Nonce darf, im Fall von Bitcoin, jedoch nur 32 Bits des Speichers belegen, wodurch ihr Maximalwert bei 2^{32}, oder ca. vier Milliarden liegt. Es ist sehr gut möglich, dass auch nach dem Ausprobieren von allen vier Milliarden Möglichkeiten noch kein genug tiefer Hashwert entsteht. In diesem Fall muss ein anderer Teil des Blocks verändert werden. Entweder inkludiert man andere Transaktionen oder verändert deren Reihenfolge innerhalb des Blockes, oder man verändert die Zeitangabe des Blockes. Jeder Block enthält eine Zeitangabe. Diese ist jedoch nicht wirklich relevant und darf auch um eine Stunde daneben liegen. Dieses Ausprobieren von verschiedenen Werten und Ausrechnen der Hashwerte, bis der Hashwert klein genug ist, wird als „Mining“ bezeichnet.

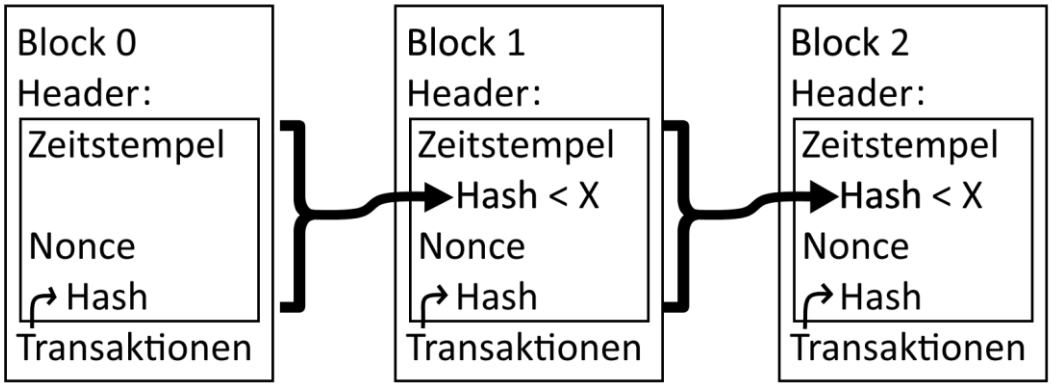

Abb. 6: Inhalt einer Blockchain

Weil Computer mit der Zeit immer schneller werden, aber auch nicht immer gleich viele Computer an der Berechnung teilnehmen, wird der maximale Hashwert eines Headers immer wieder angepasst. Dieser Wert wird als „Schwierigkeit“[15] der Blockchain bezeichnet. Wenn die Schwierigkeit nicht angepasst wird, würde das Zeitintervall zwischen zwei Blöcken nicht konstant bleiben. Wenn die Schwierigkeit viel zu hoch wäre, gäbe es tagelang keine neuen Blöcke. Die gesamte Hashleistung aller Computer des Netzwerkes wäre zu klein, um in vernünftiger Zeit genügend Werte auszuprobieren, bis ein akzeptabler Hashwert gefunden werden würde. Wäre die Schwierigkeit viel zu einfach, würde das Netzwerk mit hunderten von Blöcken geflutet werden, und es wäre unmöglich, daraus eine einzige, geordnete Kette zu bilden.

Die Bitcoin-Blockchain soll durchschnittlich alle zehn Minuten um einen Block wachsen. Im Jahr 2009, als der erste Block von Bitcoin entstand[16], erbrachte das gesamte Netzwerk eine

[15] Vgl. Blockchainwelt.de
[16] Vgl. Eklitzke.org

Leistung von fünf Megahashs pro Sekunde. Das Netzwerk bestand in diesem Jahr zur meisten Zeit vermutlich nur aus dem Computer des Erfinders von Bitcoin, welcher unter dem Pseudonym[17] „Satoshi Nakamoto“ bekannt ist. Die Hashwerte begannen zu dieser Zeit mit zehn Nullen[18]. Im Vergleich dazu, beginnen die Hashwerte im Jahr 2018 mit 18 Nullen, und die Hashrate des gesamten Netzwerkes beträgt ungefähr fünfzig Exahashs pro Sekunde, also zehn Billionen Mal mehr als noch vor zehn Jahren. Es werden somit durchschnittlich dreissig Trillionen Hashwerte ausgerechnet, bis ein gültiger Block entsteht.

Der erste Block einer Blockchain ist etwas Besonderes, er wird „Genesis-Block“ genannt. Er wird benötigt, damit die folgenden Blöcke darauf aufbauen können, denn ohne Startpunkt gibt es keine Blockchain. Der Genesis-Block ist eigentlich ein normaler Block, mit dem Unterschied, dass er keinen Vorgänger hat, dessen Hashwert er beinhalten könnte. Der Genesis-Block von Bitcoin wurde von Satoshi Nakamoto erstellt, und enthält die Schlagzeile *„Chancellor on brink of second bailout for banks“*[19] vom 3. Januar 2009 der Zeitung *The Times* als Beweis, dass der Block nicht schon Tage zuvor erstellt wurde, was dem Erfinder einen Vorteil gegenüber anderen Minern gegeben hätte. Die Schlagzeile ist gleichzeitig auch eine Anspielung auf den Erfolg von Bitcoin über das traditionelle Bankenwesen.

2.2.8 Verzweigte Blockchain

Wenn das Netzwerk keinen Konsens findet, welche Blockchain die richtige ist, weil zum Beispiel ein Teil der Mitglieder einen Block akzeptieren, den ein anderer Teil nicht akzeptiert, gibt es plötzlich mehrere Varianten derselben ursprünglichen Blockchain. Solch eine Verzweigung wird „Fork“ genannt. Entsteht ein Fork unabsichtlich, wird die kleinere Kette die daraus entsteht absterben. Die Teilnehmer eines Netzwerkes werden immer der längsten Blockchain, also der mit mehr Blöcken oder schnellerem Wachstum, folgen. Wenn das Blockchain System verändert werden soll, zum Beispiel um etwas zu verbessern, gibt es auch einen Fork. Die neue Variante geht als Zweig aus der alten Blockchain hervor und wird von allen Mitgliedern akzeptiert, die der Veränderung zustimmen. Die Mitglieder, welche die

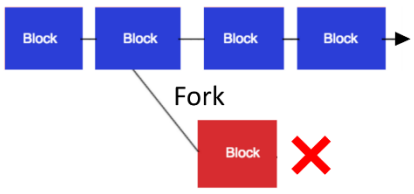

Abb. 7: Erfolgloser Fork einer Blockchain

[17] Vgl. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System, 31.10.2008.
[18] Vgl. Blockchain.com
[19] „Kanzlerin kurz vor dem zweiten Rettungspaket für Banken“. Vgl. Eliott, Francis und Duncan, Gary (2009).

Veränderung ablehnen, werden weiterhin die alte Blockchain weiterführen. Dies passierte im Jahr 2017 mit Bitcoin. Ein Teil der Community spaltete sich von der alten Variante ab, und es entstand Bitcoin-Cash, eine modernere Variante von Bitcoin. Weil Bitcoin-Cash aus derselben Blockchain hervorgeht wie Bitcoin, besitzt jeder, der vor der Abspaltung Bitcoin besass, auch Bitcoin-Cash.

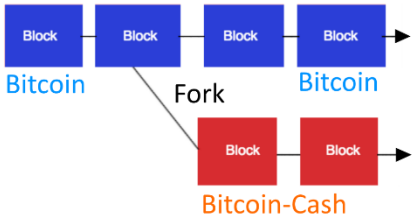

Abb. 8: Erfolgreicher Fork

3 Eigenschaften von Kryptowährungen

Aufbauend auf die Funktionsweise von Kryptowährungen gehe ich in diesem Kapitel auf die Eigenschaften ein, die aus der Funktionsweise resultieren. Diese Eigenschaften können positiv, aber auch negativ sein und Risiken enthalten. Ich vergleiche dabei Kryptowährungen mit konventionellem Geld, aber auch verschiedene Kryptowährungen untereinander.

3.1 Instabile Wechselkurse

Der Wert einer Kryptowährung stützt sich nicht indirekt auf die Wirtschaftsleistung eines Landes, wie bei konventionellen Währungen, sondern hängt rein von Angebot und Nachfrage ab. Dies hat zur Folge, dass die Wechselkurse von Kryptowährungen extremen Schwankungen[20] ausgesetzt sind, was momentan Spekulationen mit immensen Gewinnen, aber auch sehr hohen Verlusten erlaubt. Diese Eigenschaft erschwert die Verwendung von Kryptowährungen als Zahlungsmittel, denn niemand will aufgrund einer Kursschwankung plötzlich mit wertlosem Geld dastehen.

Der Wert kann allerdings theoretisch stabiler werden. Entweder durch eine Institution, welche aktiv für einen bestimmten Wechselkurs garantiert, wie es die Schweizerische Nationalbank[21] in den Jahren 2011 bis 2015 mit dem Franken zu Euro Kurs gemacht hat[22], oder passiv durch eine höhere Verbreitung. Denn der Kurs einer Währung bleibt eher stabil, wenn sie von vielen akzeptiert wird und es einfach ist, jemanden zu finden, der einem die Währung abkauft. Eine grosse Verbreitung reduziert auch die Wichtigkeit des Wechselkurses, denn wenn jeder die Kryptowährung akzeptiert, ist es nie nötig, sie gegen eine konventionelle Währung einzutauschen.

[20] Vgl. Poloniex.com
[21] Vgl. SNB.ch
[22] Vgl. Handelszeitung.ch

3.2 Falschgeld

Konventionelle Währungen, wie der Schweizerfranken oder der Dollar basieren auf mehr oder weniger fälschungssicheren Münzen und Noten. Kryptowährungen hingegen verwenden Kryptografie. Dadurch sind sie praktisch unfälschbar, was ein grosser Vorteil im Vergleich zu Bargeld ist. Denn im Jahr 2017 wurden alleine in der Schweiz[23] falsche Schweizerfranken im Wert von fast 400‘000 CHF konfisziert. Hinzu kommen über 300‘000 Euro, 25 Millionen Yen (entspricht 250‘000 CHF) und fast 400‘000 US-Dollar.

3.3 Varianten der Blockerstellung

Es gibt auch andere Wege zu entscheiden, wer Blöcke erstellen darf, statt der von Bitcoin verwendeten Variante. Bitcoin verwendet Proof of Work, also der Beweis von Arbeit. Die Arbeit ist das Herausfinden eines Hashwertes, der die Bedingungen des Netzwerks erfüllt. Es gibt aber auch andere Ansätze, wie Proof of Storage oder Proof of Stake.

Proof of Stake bedeutet, dass man, um einen Block zu erstellen und Geld zu verdienen, keine Rechenleistung benötigt, sondern Kapital. Die Belohnung ist ähnlich wie Zins auf einem Bankkonto. Je länger und je mehr Geld man auf der Blockchain besitzt, desto eher darf man einen neuen Block erstellen und die Belohnung einsacken.

Proof of Capacity hingegen ist sehr ähnlich zu Proof of Work. Die Hashwerte werden jedoch nicht immer neu berechnet, sondern einmal abgespeichert und später wieder hervorgesucht. Dieses Verfahren benötigt statt viel Rechenleistung viel Speicherplatz. Die Burst Plattform[24] verwendet dieses System und besteht aus ungefähr 250‘000 Terabyte. Dies entspricht grob der Datenmenge, die in einem Jahr auf die Videoplattform YouTube hochgeladen wird.

3.4 Manipulation der Blockchain

Das Netzwerk einer Blockchain folgt grundsätzlich der Mehrheit, also der längeren Blockchain. Es wäre somit eine Katastrophe, wenn es einem Angreifer gelingen würde, die Mehrheit alleine zu bilden. Dafür müsste der Angreifer bei einem Proof of Work System über 51% der Rechenleistung, oder bei einem Proof of Stake System über 51% des gesamten Vermögens verfügen. Wenn dies einem Angreifer gelingen würde, könnte er einen Block erstellen, in welchem er jemandem Geld gibt, zum Beispiel für ein Auto. Das Netzwerk akzeptiert den Block, der Verkäufer geht davon aus, dass er nun die Bitcoins besitzt und lässt

[23] Vgl. Fedpol.admin.ch
[24] Vgl. Cryptoguru.org

den Käufer mit dem Auto wegfahren. Der Angreifer kann nun einen alternativen Block zum vorherigen Block erstellen, in dem die Auto-Transaktion nicht enthalten ist[25]. Diesen alternativen Block kann der Angreifer mit weiteren Blöcken bestätigen. Weil der Angreifer über mehr als die Hälfte der gesamten Rechenleistung verfügt, wird seine Blockchain schneller wachsen als die des restlichen Netzwerkes, in der das Auto bezahlt wird. Die vom Angreifer erstellte Blockchain ist nach einer bestimmten Zeit länger als die, in der das Auto bezahlt wird. Somit wechselt das gesamte Netzwerk auf die Blockchain des Angreifers. Der Verkäufer des Autos wurde nie bezahlt, denn der Block in dem er die Bitcoins erhält, wird als ungültig angesehen. Diese Art von Manipulation wird „Double-Spending“ genannt, weil der Angreifer sein Vermögen theoretisch zweimal ausgeben kann.

Damit es möglichst schwer ist, mehr als die Hälfte der Rechenleistung zu kontrollieren, sollte die gesamte Rechenleistung möglichst hoch sein. Dies wird erreicht, indem diejenigen,

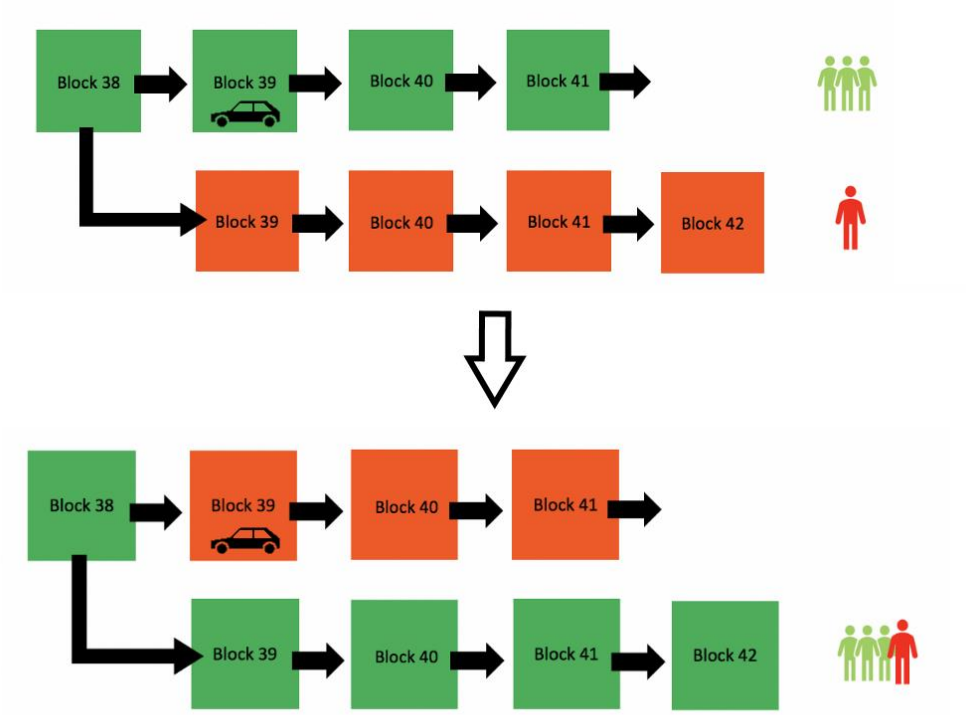

Abb. 9: Manipulation der Blockchain durch einen Miner, der schneller als die restlichen Miner Blöcke generieren kann

welche sie bereitstellen, belohnt werden. Die Belohnung besteht aus den Transaktionsgebühren und teilweise zusätzlich aus einem konstanten Block-Reward. Der Block-Reward ist Geld, welches aus dem Nichts erschaffen wird, wie wenn eine Nationalbank Geld druckt. Der Ersteller des Blocks darf sich dieses Geld überweisen. Dies führt zu einer konstanten Inflation, weil es immer mehr von der Kryptowährung gibt, sorgt aber auch dafür,

[25] Vgl. S., Jimi. Blockchain: how a 51% attack works (double spend attack), 05.05.2018.

dass es immer genügend Geld gibt, sollte die Nachfrage steigen. Im Fall von Bitcoin wird der Block-Reward alle vier Jahre halbiert, bis er Null erreicht. Momentan steht er bei 12.5 BTC pro Block.

Ein hoher Block-Reward sorgt dafür, dass die Einnahmen der Miner nicht stark von den Transaktionsgebühren abhängen. Das bedeutet, dass es sich für Miner auch dann lohnt die Blockchain weiterzuführen, wenn es gar keine, oder nur wenige neue Transaktionen gibt. Wenn das nicht so wäre, würde es sich für Miner nur lohnen ihre Computer anzuschalten, wenn es genügend Transaktionsgebühren zu verdienen gibt. Wenn es für ehrliche Miner unrentabel wäre ihre Computer anzuschalten, könnte ein unehrlicher Miner, dem die ungedeckten Stromkosten egal sind, weil er durch Manipulationen der Blockchain Geld verdient, sehr einfach 51% der gesamten Rechenleistung erreichen. Das ist ein Grund, weshalb der Block-Reward wichtig ist.

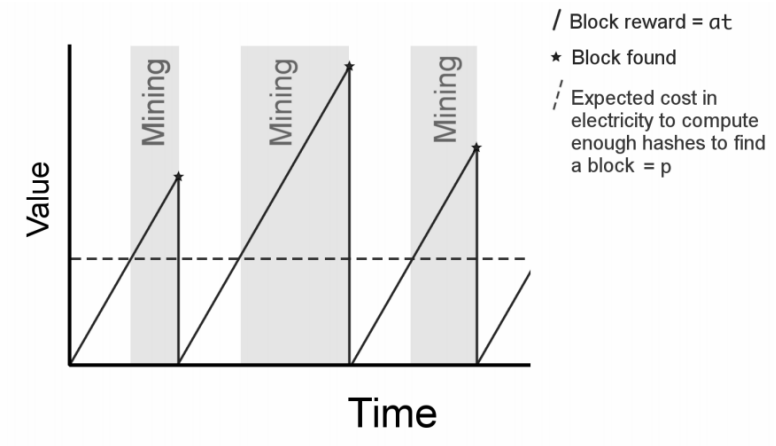

Abb. 10: Mining ohne Block-Reward ist nicht immer profitabel

Abbildung 10 veranschaulicht dieses Problem graphisch. Die horizontale Achse steht für die Zeit, die vertikale für einen Geldbetrag. Die gestrichelte Linie stellt die Stromkosten dar, um einen Block zu erstellen. Die durchgezogene Linie steht für die möglichen Einnahmen durch Transaktionsgebühren. Diese steigen konstant an, denn es kommen immer mehr neue Transaktionen hinzu, die ein Miner in einen neuen Block einbauen kann. Der kleine Stern an den Spitzen der durchgezogenen Linie markiert, dass ein Block erschaffen wurde. In diesen Block werden alle Transaktionen aufgenommen, es gibt also keine offenen mehr. Die grauen Flächen markieren, wo das Mining profitabel ist. Dies ist nur der Fall, wenn man mehr Geld durch die Transaktionsgebühren einnimmt, als man für den Strom ausgiebt.

Der Block-Reward führt jedoch auch dazu, dass es Miner gibt, die gar keine Transaktionen in ihre Blöcke aufnehmen, sondern diese leer lassen und nur den Reward einkassieren. Denn es kann sein, dass es profitabler ist einen leeren Block statt einen vollen zu erstellen[26], denn man muss nicht zuerst alle Transaktionen überprüfen. Während der Überprüfung suchen deshalb viele Miner schon nach einem leeren Block, um keine Zeit zu verschwenden.

[26] Vgl. Gauthier, Pascal. Why Do Some Bitcoin Mining Pools Mine Empty Blocks?, 12.07.2016.

Das Ganze gilt auch für Proof of Stake Systeme. Bei diesen könnte ein grosser Investor über 50% des Vermögens besitzen, und damit das Recht bekommen, über die Hälfte der Blöcke zu erstellen. Aber dank dem Block-Reward, der in diesem Fall mit Zinsen vergleichbar ist, lohnt es sich auch für kleine Investoren Geld zu investieren. Dadurch wird es erschwert, über 50% des gesamten Vermögens zu besitzen.

Wäre das Einkommen der Miner nur von den Transaktionsgebühren abhängig, wäre nicht mehr sichergestellt, dass die Mehrheit immer der längsten Blockchain folgt[27]. Ein Miner könnte einen Fork starten, der kürzer als die eigentliche Kette ist und deshalb nicht akzeptiert werden sollte. In diesem Fork verarbeitet er nur Transaktionen mit kleinen Gebühren. Transaktionen mit hohen Gebühren lässt er warten. Das bedeutet für alle anderen Miner, dass sie mehr Geld verdienen könnten, wenn sie der kürzeren, statt der längeren Blockchain folgten. Denn dadurch könnten sie Transaktionen mit hohen Gebühren in ihren Block schreiben, statt sich mit kleinen Gebühren zufrieden zu geben. Dies würde eine Manipulation der Blockchain, wie der Double-Spending-Angriff, erneut vereinfachen. In der folgenden Abbildung ist die Ausgangssituation eine Blockchain, in der bereits 100 Fr. Gebühren an frühere Miner ausbezahlt wurden. Die Transaktionen die noch nicht in der Blockchain stehen, bieten 5 Fr. Gebühren. Ein Miner hat also zwei Möglichkeiten. Er kann die offenen Transaktionen verarbeiten, der Blockchain anhängen und somit 5 Fr. verdienen. Den restlichen Minern lässt er somit kein Geld mehr übrig. Die zweite Möglichkeit wäre, eine Alternative zur momentanen Blockchain zu erschaffen, einen Fork. Dadurch werden die bereits ausbezahlten Gebühren von 100 Fr. wieder verfügbar, denn jener Block verliert seine Gültigkeit. In dieser Alternative kann der Miner 55 Fr. der Gebühren beanspruchen, was den anderen Minern 50 weitere Franken zur Verfügung stellen würde. Da die anderen Miner auf

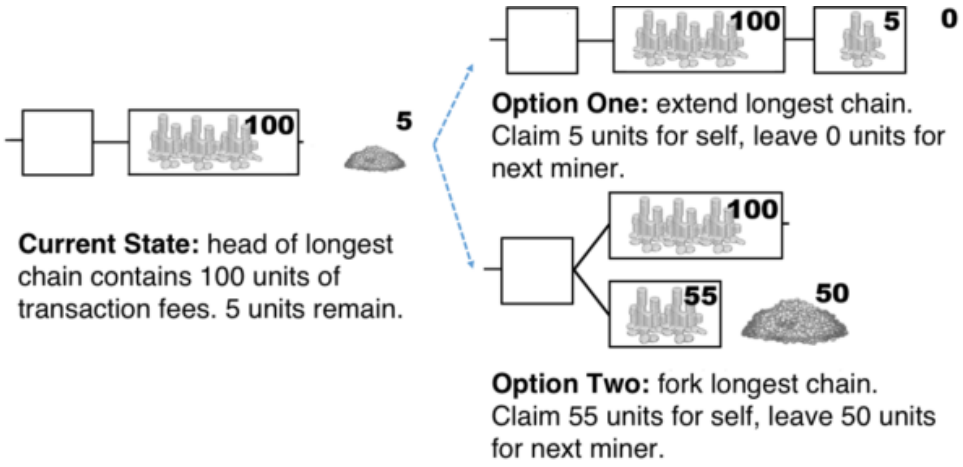

Abb. 11: Anlocken von anderen Minern durch höhere Einnahmen

[27] Vgl. Carlsten, Miles et al. On the Instability of Bitcoin Without the Block Reward.

Einnahmen angewiesen sind, werden sie dem Fork folgen, denn er verspricht ihnen mehr Einnahmen. Der erste Miner kann sich sozusagen die Zustimmung anderer Miner erkaufen.

3.5 Ressourcen Verbrauch

3.5.1 Strom

Ein bekannter Nachteil von Kryptowährungen ist deren enormer Stromverbrauch. Die effizienteste Bitcoin-Mining Hardware[28] im Jahr 2018 verbraucht etwa 90 Watt pro Terahash pro Sekunde. Wenn die gesamte Rechenleistung des Bitcoin-Netzwerkes mit diesem Effizienzgrad erbracht würde, beliefe sich der gesamte Stromverbrauch auf 4.5 Gigawatt[29]. Es ist zu beachten, dass dieser Wert einen unrealistischen Minimalwert darstellt. Der reale Wert ist sehr wahrscheinlich um den Faktor 1.5 höher, also ca. 7 Gigawatt. Die Schweiz[30] verbrauchte über das Jahr 2017 hinweg insgesamt 58'483 GWh Elektrizität, was umgerechnet 6.7 GW entspricht. Das Bitcoin-Netzwerk verbraucht somit ungefähr gleich viel Strom wie die gesamte Schweiz. Eine einzige Transaktion verbraucht dadurch über 300 kWh Strom, das ist über hunderttausend Mal mehr als eine Kreditkartentransaktion[31].

Es gibt jedoch viele andere Kryptowährungen, deren Stromverbrauch signifikant kleiner ist. Das liegt einerseits daran, dass der hohe Wert von Bitcoin es erlaubt, sehr viele Computer mit entsprechend hohem Stromverbrauch für das Mining einzusetzen. Wenn der Wert geringer wäre, wäre das Mining finanziell weniger attraktiv und die Miner wären gezwungen, den Stromverbrauch zu reduzieren, da der Gesamtgewinn konstant bleibt. Im Fall von Bitcoin beträgt dieser momentan circa eine halbe Million Franken pro Stunde. Erhöht ein Miner seine Rechenleistung, steigt damit einerseits sein Anteil am möglichen Gesamtgewinn, aber auch seine Stromkosten. Andererseits gibt es Alternativen zum Proof of Work System von Bitcoin, die massiv weniger Strom verbrauchen, wie zum Beispiel Proof of Stake[32] oder Proof of Capacity.

Es gibt einen weiteren Grund, der den Nachteil des riesigen Stromverbrauchs von Kryptowährungen relativiert. Nämlich, dass der verbrauchte Strom möglicherweise nicht aus fossilen Energieträgern produziert wurde, sondern aus erneuerbaren Quellen[33]. Denn grüner

[28] Vgl. Chi, Clifford. 7 of the Best Bitcoin Mining Hardware for 2018, 30.08.2018.
[29] $5*10^7$TH/s * 90 W = 4.5 GW Vgl. Blockchain.com
[30] Vgl. Bfe.admin.ch
[31] Vgl. Statista.com
[32] Vgl. Bolzli, Michael. Bitcoin verbraucht so viel Strom wie die Schweiz, 26.04.2018.
[33] Vgl. Bergmann, Christoph. Warum der hohe Stromverbrauch von Bitcoin vermutlich kein Problem für die Umwelt ist, 28.05.2018.

Strom ist oftmals auch günstiger Strom. Der wichtigste Faktor um mit dem Minen von Kryptowährungen Profit zu machen, ist günstiger Strom. Damit das Bitcoin-Netzwerk profitabel ist, dürfen die Stromkosten momentan nicht mehr als ca. 10 Rappen pro Kilowattstunde betragen[34]. Ein gutes Beispiel ist Island. Islands Strom wird zu 99% aus erneuerbaren Ressourcen[35] gewonnen, kostet aber trotzdem nur 4 Rappen[36] pro Kilowattstunde. In der Schweiz kostet der Strom[37] vergleichsweise viel, je nach Kanton und Verbrauch zwischen 10 und 30 Rappen pro kWh. In China ist der Strompreis mit 8 Rappen pro kWh im internationalen Vergleich auch sehr tief. Es wird deshalb angenommen, dass der Grossteil der Miner ihre Hardware in China und Island betreiben. China bezieht über die Hälfte seines Stromes aus Kohlekraftwerken[38]. Es gilt jedoch zu beachten, dass Strom aus Wasserkraft in China billiger ist, als Strom aus fossilen Rohstoffen[39]. Zusätzlich werden erneuerbare Energiequellen, wie die Photovoltaik und die Windenergie, durch neue Innovationen immer billiger, oder sind bereits schon billiger als Strom aus fossilen Rohstoffen[40].

3.5.2 Hardware

Durch die Lukrativität des Minings stieg die Nachfrage nach Grafikkarten in den Jahren 2017 und 2018 stark an. Die Kapazitäten der Hersteller reichten nicht aus, um die hohe Nachfrage zu stillen. Die Preise von Grafikkarten stiegen je nach Modell um 20 bis 50 Prozent, und es gab starke Lieferengpässe. Viele Händler, unter ihnen auch der Onlineshop digitec.ch, haben deswegen eine Beschränkung[41] eingeführt. Jeder Kunde darf nur noch zwei Grafikkarten einer Modellreihe erwerben. Momentan, im Herbst 2018, sinken die Preise jedoch wieder. Der Boom ist grösstenteils vorbei, die Kaufbeschränkung auf digitec.ch ist aber immer noch in Kraft, obwohl der Onlineshop wieder Grafikkarten an Lager hat. Die grosse Nachfrage sorgt zwar für hohe Gewinne bei den Herstellern, trägt aber auch Nachteile für die normalen Konsumenten und die Umwelt mit sich. Die Konsumenten leiden unter erhöhten Preisen und langen Lieferzeiten.

[34] 12.5 BTC pro Block * 6 Blöcke pro Stunde + Gebühren = 75 BTC ~ 500‘000 CHF pro Stunde geteilt durch den Verbrauch von ca. 5 GWh pro Stunde, ergibt 0.1 CHF pro KWh.
[35] Vgl. Mims, Christopher. One Hot Island: Iceland's Renewable Geothermal Power, 20.10.2008.
[36] Vgl. Årebo, Ingrid (2014).
[37] Vgl. Strompreis.elcom.admin.ch
[38] Vgl. Wikipedia.org
[39] Vgl. Irena.org
[40] Vgl. Wikipedia.org
[41] Vgl. Rüegg, Philipp. Grafikkarte nur fürs Crypto Mining kaufen: Lohnt sich das überhaupt (noch)?, 09.02.2018.

Der Herstellungsprozess von Hardware verbraucht viel Energie und Rohstoffe. Die Herstellung einer Komponente ist ungefähr gleich belastend für die Umwelt wie die Komponente ein Jahr zu betreiben[42]. Da ein Grossteil der Hardware nur wenige Jahre lang eingesetzt wird, weil neuentwickelte Produkte viel effizienter[43] sind, ist die Herstellung somit für einen sehr grossen Teil der Gesamtbelastung verantwortlich.

3.5.3 Speicherplatz

Die Haupteigenschaft der Blockchain, dass in ihr alle je getätigten Transaktionen gespeichert sind, führt zu einem Problem: der benötigte Speicherplatz. Die Blockchain wird immer länger, denn nichts kann daraus gelöscht werden. Die Bitcoin Blockchain ist im Herbst 2018 bereits über 180 Gigabyte gross, was momentan noch auf vielen Computern Platz hat. Die zunehmende Grösse könnte jedoch in Zukunft dazu führen, dass es weniger Leute gibt, welche die gesamte Blockchain speichern und damit Transaktionen verifizieren können. Dies ist der Dezentralisierung nicht förderlich, sollte aber nie zu einem grossen Problem werden. Wenn man auf seinem Handy Bitcoins hat und diese ausgeben möchte, muss man nicht die gesamte Blockchain auf seinem Handy haben, es reicht wenn auf dem Handy nur die Transaktionen gespeichert sind, die mit den eigenen Bitcoins in Verbindung stehen.

3.6 Dezentrales Mining

Damit Kryptowährungen wirklich Dezentral organisiert sind, muss möglichst jeder die Möglichkeit haben, daran mitzuarbeiten. Das ist jedoch nicht unbedingt der Fall, denn Mining mit dem Proof of Work System ist nicht immer profitabel. Ein grosser Faktor ist der Strompreis. Der hat zur Folge, dass ein Grossteil der Rechner in Island und China stehen, weil dort der Strom billig ist. Dazu kommt, dass es beispielsweise im Fall von BTC spezielle Mikroprozessoren für das Ausrechnen der Haschfunktion gibt. Diese Mikroprozessoren sind weitaus effizienter als handelsübliche Hardware. Solche spezialisierten Mikroprozessoren werden *application-specific integrated circuits*, also applikationsspezifische integrierte Schaltkreise, kurz ASICs, genannt. Die Entwicklung oder der Kauf von solchen ASICs verlangt hohe Investitionen. Dadurch ist Bitcoin nicht mehr wirklich dezentral, sondern wird von grossen Gruppen in Billigstrom-Ländern betrieben.

Es gibt aber Kryptowährungen, welche eine Hashfunktion einsetzen, für die keine ASICs gebaut werden können. Solche Hashfunktionen sind für handelsübliche Prozessoren und

[42] Vgl. Schischke, Karsten. Energie- und CO_2-Bilanz von PCs – Relevanz für ReUse-Strategien, 02.2005.
[43] Vgl. Bitcoin.it

Grafikkarten optimiert, und ermöglichen somit privates Mining im kleinen Rahmen. Eine dieser Kryptowährungen ist Monero.

3.7 Dezentral oder Zentral

Die meisten Kryptowährungen sind dezentral organisiert. Das entspricht auch der allgemeinen Philosophie hinter einer Blockchain und Kryptowährungen. Es gibt jedoch Firmen, die ihre eigene Art von Blockchain und Kryptowährung haben. Eine von ihnen ist Ripple mit der Währung XRP. Die Firma will mit ihrem System die alten Zahlungssysteme ersetzen, denn ihr System kann theoretisch bis zu 50‘000 Transaktionen pro Sekunde verarbeiten, jede Transaktion ist binnen weniger Sekunden abgewickelt[44]. Ripple ist jedoch noch sehr nah am jetzigen Bankensystem und möchte es effizienter gestalten, statt wie Bitcoin das Bankensystem komplett zu umgehen[45]. Ripple verwendet auch keine wirkliche Blockchain[46], sondern ein System mit ähnlichen Eigenschaften. Solch zentralisierte Systeme werden oft kritisiert, denn schlussendlich muss man der dahinterstehenden Firma vertrauen. Ein Vorteil von zentralisierten Kryptowährungen ist, dass die Firma alleine über die Transaktionen bestimmt, es muss also kein Konsens gefunden werden, und das System kann nicht von einem Aussenstehenden manipuliert werden. Zentralisierte Kryptowährungen sind vergleichbar mit konventionellen Banksystemen mit Geschwindigkeiten wie Visa oder Mastercard.

Weil bei dezentralen Kryptowährungen keine zentrale Institution die Kontrolle über die Blockchain hat, ist es sehr schwer etwas rückgängig zu machen. Eine falsche Transaktion und das Geld ist für immer verloren. Nur in Ausnahmefällen, wenn die Mehrheit des Netzwerkes dem zustimmt, kann etwas ungeschehen gemacht werden, sozusagen eine Art Fork. Für traditionelle Banken ist es hingegen kein Problem, Transaktionen rückgängig zu machen, und wenn die Kontonummer des Empfängers nicht stimmt, ist das Geld nicht verloren sondern wird wieder an den Absender überwiesen. Bei Kryptowährungen ist Geld verloren, wenn es an eine ungültige Adresse geschickt wird.

3.8 Transaktionsgeschwindigkeit

Die Geschwindigkeit einer Transaktion hängt vor allem von der Zeit ab die benötigt wird, um einen neuen Block der Blockchain anzuhängen. Vorausgesetzt die Transaktion enthält eine genug hohe Gebühr, wird sie sofort in den nächsten Block aufgenommen. Damit ist die

[44] Vgl. Wikipedia.org
[45] Vgl. Draglet.com
[46] Vgl. Gordon, Shawn. What is Ripple?.

Transaktion theoretisch fertig. Doch da der neuste Block noch durch keinen weiteren Block abgesichert wurde, könnte er relativ leicht durch einen anderen Block ersetzt werden. Je mehr Blöcke an einen Block angehängt werden, desto unwahrscheinlicher, respektive schwieriger ist es, diesen zu manipulieren. Aus diesem Grund wird in der Praxis[47] eine Transaktion erst akzeptiert[48], wenn sie durch mehrere Blöcke bestätigt wurde. Eine Bitcoin Transaktion zum Beispiel wird von vielen erst als bezahlt angesehen, wenn sie 6 Bestätigungen erhält. Das bedeutet, eine Transaktion dauert ca. 60 Minuten. 10 Minuten vergehen bis sie in der Blockchain steht, und 50 weitere Minuten bis genügend weitere Blöcke die Transaktion absichern.

Bei Blockchains mit kürzeren Blockintervallen, zum Beispiel Litecoin, erhalten Transaktionen schneller Bestätigungen. Weil dadurch aber die Sicherheit, die ein neuer Block verleiht, kleiner ist, werden mehr Bestätigungen verlangt. Bei zentralisierten Kryptowährungen - wie Ripple - muss man auf keine Bestätigungen warten, denn die Blockchain kann so oder so nicht manipuliert werden.

Ein weiterer limitierender Faktor ist die Kapazität des Netzwerkes. Bitcoin zum Beispiel erlaubt nur ein Megabyte an Transaktionen pro Block, was nur 7 Transaktionen pro Sekunde ermöglicht. Dieses Limit wurde im Dezember 2017 erreicht. Die Folgen waren lange Wartezeiten und hohe Transaktionsgebühren. Andere Systeme, wie Ripple oder Ethereum, besitzen aber viel höhere Kapazitäten, die den Systemen von Banken nicht mehr unterlegen sind.

3.9 Illegaler Handel und Geldwäsche

Auf einer Blockchain werden keine Namen, sondern nur Adressen gespeichert. Durch die Adressen ist es nicht einfach so möglich, auf den Besitzer zu schliessen. Es ist schliesslich nicht bekannt, wer den privaten Schlüssel einer bestimmten Adresse besitzt. Person A kann Person B beliebig viel Geld senden, und es ist praktisch unmöglich, herauszufinden wer sich hinter den jeweiligen Adressen verbirgt. Wegen dieser Anonymität sind Kryptowährungen sehr beliebt für Geldwäsche und den Handel mit illegalen Gütern.

Ein gutes Beispiel dafür ist die Webseite Silk Road[49]. Die Webseite existierte erstmals im Jahr 2011. Viele der Drahtzieher konnten jedoch einige Jahre später gefasst, und die Webseite abgeschaltet werden. Daraufhin erschienen mehrere Nachahmungen von Silk Road. Auf Silk Road wurde mit allerlei Drogen gehandelt und die Webseite galt als sichere

[47] Vgl. Kraken.com
[48] Vgl. Bitpay.com
[49] Vgl. Wikipedia.org

Alternative zum Strassenhandel. Einerseits, weil die verkauften Waren von höherer Qualität waren, als die, welche auf der Strasse verkauft werden. Dies ist so, weil Verkäufer bewertet[50] wurden, wie man heute Restaurants im Internet bewertet. Qualitativ hochwertige Produkte waren notwendig, damit man viele Abnehmer fand. Auf der Strasse ist die Angebotsauswahl viel kleiner, der Konsument muss das kaufen was er bekommt, denn oft gibt es keinen alternativen Anbieter. Andererseits kann im Onlinehandel keine physische Gewalt[51] auf den Kunden ausgeübt werden. Eine Bestellung über das Internet ist auch schlichtweg bequemer[52], denn sie wird per Post vor die Haustüre geliefert.

Die einzige Zahlungsmöglichkeit auf Silk Road war Bitcoin. Die Webseite galt als eine der sichersten illegalen Webseiten. Durch Fehler in ihrem System konnten die Betreiber jedoch gefasst werden. Es wurden aber noch fast keine Nutzer der Webseite festgenommen, was beweist, dass Kryptowährungen wirklich anonym sind, obwohl die Blockchain öffentlich ist.

Weil eine Blockchain, und damit alle Transaktionen, öffentlich ist, können theoretisch alle Geldflüsse überwacht und verfolgt werden. Man kann auch die Herkunft von Vermögen genau herausfinden. Das nützt jedoch nur etwas, wenn bekannt ist, wer sich hinter einer in der Blockchain auftauchenden Adresse verbirgt. Aber auch wenn man weiss, wem eine Adresse gehört, kann man die Person nicht daran hindern, ihr Geld an jemand anderen zu überweisen. Die dezentrale Zahlungsabwicklung durch die Miner verhindert das Einfrieren von Konten, denn mehr als die Hälfte der Miner müsste sich an den Entscheid des Einfrierens halten. Bei zentral organisierten Kryptowährungen wäre dies jedoch gut möglich.

4 Wie werden Kryptowährungen gesetzlich geregelt?

In diesem Kapitel erläutere ich die gesetzliche Lage rund um Kryptowährungen. Einerseits der Umgang mit Geldwäsche, aber auch wie man Kryptowährungen momentan versteuern muss. Ein zentraler Punkt ist, dass es praktisch noch keine Gesetze spezifisch für Kryptowährungen gibt. Bisher werden einfach bestehende Gesetze angewendet. Kryptowährungen gelten deswegen auch noch nicht als Geld, sondern als Wertschriften. Eine Ausnahme dazu stellt Japan dar. Dort gelten Kryptowährungen offiziell als Geld. Die offizielle Anerkennung führte dazu, dass viele Geschäfte und Personen begannen, Kryptowährungen als Zahlungsmittel zu verwenden[53].

[50] Vgl. Barrat, Monica et al. Use of Silk Road, the online drug marketplace, 25.12.2013.
[51] Vgl. Jeffries, Adrianne. Silk Road may have prevented drug violence, study says, 02.06.2014.
[52] Vgl. Cadwalladr, Carole. How I bought drugs from 'dark net' – it's just like Amazon run by cartels, (06.10.2013).
[53] Vgl. Mathew, Joel. Cryptocurrency: Japan’s Approach, 29.06.2018.

4.1 Geldwäsche

Weil Kryptowährungen ideal für Geldwäsche und illegalen Handel sind, müssen sich Handelsplattformen[54] an Vorschriften halten, wie auch Wechselbüros und Banken. Um den Anti-Geldwäsche Gesetzen zu folgen, müssen Handelsplattformen ihre Kunden identifizieren. Die meisten Onlineplattformen verlangen deshalb Namen, Adresse und Telefonnummer ihrer Kunden, teilweise auch eine Kopie der Identitätskarte oder des Passes. Um an den Ticketautomaten der SBB Bitcoins zu kaufen, reicht alleine die Angabe der Telefonnummer. Durch dieses Vorgehen sollen die Unterstützung von Terrorismus, Steuerhinterziehung und die Geldwäsche von illegal erwirtschaftetem Geld verhindert werden[55]. Banken und Handelsplattformen müssen allerdings eingezahltes Geld nicht auf seinen legalen Ursprung überprüfen Eine Ausnahme bilden Einzahlungen, die auf den ersten Blick suspekt erscheinen[56], wie zum Beispiel grosse Beträge in bar. Es reicht, wenn die Banken den Ermittlern die Identität des Kontoinhabers geben können[57].

4.2 Steuern in der Schweiz

Kryptowährungen gelten in der Schweiz grundsätzlich als Wertschriften. Vermögen in Kryptowährungen muss in der Schweiz[58] wie normales Vermögen versteuert werden. Zu Jahresende veröffentlicht die eidgenössische Steuerverwaltung für die meisten Kryptowährungen einen einheitlichen[59] Wechselkurs, zu welchem die Kryptowährungen versteuert werden müssen. Kryptowährungen müssen in der Steuererklärung als übrige Guthaben im Wertschriftenverzeichnis deklariert werden.

Das Geld welches man durch Mining erhält, zählt als Einkommen und muss als solches versteuert werden.

Kapitalgewinn, also Gewinn den man durch das Kaufen und Verkaufen von Kryptowährungen zu unterschiedlichen Wechselkursen erreicht, ist steuerfrei. Nur wenn der Handel als gewerbsmässig angesehen wird, muss man den Gewinn als Einkommen versteuern, darf dadurch aber auch eventuelle Verluste von den Steuern abziehen. Auch privater Handel kann

[54] Vgl. Tassev, Lubomir. Europe Introduces Customer Verification on Cryptocurrency Exchanges, 20.04.2018.
[55] Vgl. Europa.eu
[56] Vgl. Admin.ch
[57] Vgl. Ross, Anderson. Stolen Bitcoin Tracing – Computerphile, 23.03.2018.
[58] Vgl. Steuern-nw.ch
[59] Vgl. ICTax.admin.ch

als gewerbsmässiger Handel eingestuft werden. Damit dies nicht passiert, muss man folgende Kriterien[60] einhalten:

- Die Anteile der Kryptowährung muss man für mindestens 6 Monate besitzen, bevor man sie verkauft. Dabei gilt das First In – First Out (FIFO) Prinzip.
- Das Transaktionsvolumen muss kleiner sein, als das Fünffache des gesamten eigenen Guthabens zu Beginn der Steuerperiode.
- Der Gewinn wird nicht für den Lebensunterhalt benötigt, das heisst, er macht höchstens die Hälfte des versteuerten Einkommens aus.
- Man investiert nur eigenes Vermögen, kein Fremdkapital.
- Optionen und Derivate dürfen nur zur Absicherung der eigenen Investitionen verwendet werden.

Diese Kriterien gelten nicht strikt, Steuerämter haben einen gewissen Ermessensspielraum. Wenn nicht alle Kriterien eingehalten werden, kann der Handel als gewerbsmässig eingestuft werden. Aber das Steueramt von Nidwalden nimmt einen gewerbsmässigen Wertschriftenhandel eher zurückhaltend und nach Beachtung sämtlicher Umstände des Einzelfalls an[61]. Wenn man also im Januar für 1‘000 Fr. und im Mai, weil der Kurs gestiegen ist, für weitere 2‘000 Fr. jeweils einen Bitcoin kauft, darf man durch das FIFO-Prinzip im Juli den Bitcoin vom Januar verkaufen. Weil der Wechselkurs inzwischen auf 5‘000 Fr. gestiegen ist, realisiert man damit einen Gewinn von 4‘000 Fr. Zu Jahresende liegt der Bitcoin Kurs bei 3‘000 Franken. Der im Mai gekaufte Bitcoin muss somit als 3‘000 Fr. Vermögen versteuert werden. Mit diesem erreichte man somit einen Gewinn von 1‘000 Fr. Der erste Gewinn von 4‘000 Fr. wie auch der zweite von 1‘000 Fr. gelten als steuerfreies Einkommen, sofern man über ein versteuertes Einkommen von mindestens 10‘000 Fr. verfügt und zum Anfang der Steuerperiode mehr als 1‘000 Fr. Vermögen besass.

[60] Vgl. EStv.admin.ch
[61] Vgl. Steuern-nw.ch

5 Lohnt es sich für Unternehmen, Kryptowährungen zu akzeptieren?

Kryptowährungen gelten momentan noch nicht als Geld, sondern mehr als eine Art von Wertschrift oder Aktie. Kryptowährungen werden auch meistens nicht als Zahlungsmittel, sondern nur zu Spekulationen verwendet[62]. Eine Ausnahme dazu bildet der Schwarzmarkt, auf welchem schon seit Jahren[63] vorzugsweise mit Kryptowährungen bezahlt wird. Von dieser neuen Zahlungsmethode können allerdings auch legale Unternehmen profitieren.

Ein Grund, Kryptowährungen als Zahlungsmethode zu akzeptieren, ist, dass damit auf eventuelle Erwartungen des Kunden eingegangen wird[64]. Viele Kunden erwarten, dass ein Unternehmen mit der Zeit geht und dem Kunden den bestmöglichen Service bietet. Ein sehr ähnlicher Anlass ist die Aufmerksamkeit, die ein Geschäft momentan noch erhält, wenn bekannt wird, dass dieses Kryptowährungen akzeptiert[65]. Unternehmen die bereits Kryptowährungen annehmen, haben sich meist nur für die verbreitetsten entschieden. Dazu gehört vor allem Bitcoin, aber auch Ethereum. Der Anteil an Kunden die mit Kryptowährungen bezahlen, ist allerdings bei allen von mir befragten Unternehmen sehr tief, je nach Wechselkurs zwischen 0.1% und 5%.

Ideal wäre, wenn möglichst viele Geschäfte Kryptowährungen akzeptieren, denn dann können Kryptowährungen weitergegeben werden. Für ein Unternehmen ist es von Vorteil, wenn es die Lieferanten mit derselben Währung bezahlen kann, die auch der Kunde verwendet. Das ist momentan noch nicht oft der Fall. Kryptowährungen umzutauschen ist oft mit Gebühren verbunden, aber nötig, wenn man sie nicht weiterverwenden kann.

Durch die Zahlungsmethode Kryptowährung kann das Geschäft tiefere Preise anbieten, als im Vergleich zu einigen anderen Zahlungsmöglichkeiten. Denn durch PayPal, Posteinzahlungen und Kreditkartenzahlungen können dem Verkäufer Gebühren von bis zu 3% anfallen. Diese Kosten werden im Fall von Kryptowährungen vollständig vom Käufer übernommen[66], denn dieser muss die Transaktionsgebühr für die Miner übernehmen.

Bei Kryptowährungen kommt es praktisch nie zu Unterbrechungen im System. Wegen der Dezentralität können einzelne Server ausfallen oder Opfer von Hackerangriffen werden, das Zahlungsnetzwerk funktioniert trotzdem einwandfrei. Die Transaktionen werden nicht durch

[62] Vgl. Kasper, Jan. Zahlungsmittel ohne Bank? Bitcoin als Währung der Zukunft, 2017, S.14.
[63] Vgl. Greenberg, Andy. Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market, 05.09.2013.
[64] Vgl. Schneeberger, Christoph; Interview mit Gabriel Marco. (25.6.2018) Siehe Interview im Anhang
[65] Vgl. Odermatt, Rene; Interview mit Gabriel Marco. (19.7.2018) Siehe Interview im Anhang
[66] Vgl. Schneeberger, Christoph; Interview mit Gabriel Marco. (25.6.2018) Siehe Interview im Anhang

eine Drittpartei bearbeitet. Das ist ein grosser Vorteil gegenüber bisherigen Zahlungsmethoden, denn es kann vorkommen, dass Zahlungsanbieter Blackouts haben, einzelne Konten einfrieren oder einfach lange brauchen um eine Zahlung abzuwickeln[67]. Beispiele hierfür sind ein einstündiger Ausfall von Postfinance[68] im Jahr 2016 und ein zweistündiger Ausfall der Migros Bank im Jahr 2017[69].

Obwohl die Instabilität des Wechselkurses grundsätzlich ein Nachteil gegenüber zu konventionellen Währungen darstellt, kann sie sich positiv auf den Verkauf auswirken. Denn wenn der Wert einer Währung sehr hoch liegt, sind Kunden die in dieser Währung bezahlen, sehr kauffreudig und kaufen Sachen, die sie ansonsten nicht gekauft hätten[70].

Die Unternehmen die ich befragt habe, profitieren alle nicht wirklich von den relativ schnellen Transaktionen. Für Situationen, in denen eine Transaktion innert Sekunden erledigt sein muss, sind auf einer Blockchain basierende Kryptowährungen schlicht nicht geeignet. An der Kasse[71] von Migros und Coop wird man wahrscheinlich nie mit der momentanen Version von Bitcoin zahlen. Nicht auszuschliessen sind jedoch zentralisierte Kryptowährungen wie Ripple.

Geschäftsseitig gibt es die Möglichkeit, einen Zahlungsprovider zu nutzen. Der grösste Zahlungsprovider für Bitcoin ist BitPay mit einem Volumen von einer Milliarde Dollar pro Jahr[72]. Ein Zahlungsprovider sorgt dafür, dass Kunden mit einer Kryptowährung bezahlen können. Der Provider übernimmt den gesamten Transaktionsablauf, und tauscht auf Wünsch die Kryptowährung in eine konventionelle Währung um. Das Geschäft hat somit kein Risiko von eventuellen Kursschwankungen, und praktisch keinen Mehraufwand. Die Kosten dafür belaufen sich auf 1%[73], und sind somit geringer als Zahlungen per Kreditkarte oder PayPal, welche ca. 1.5-3% des Betrages kosten[74]. Die anfallenden Transaktionskosten des Bitcoin-Netzwerkes werden vom Kunden übernommen.

Zuletzt muss aber immer noch der Kunde mit einer Kryptowährung bezahlen wollen. Damit dies passiert, müssen viele Voraussetzungen erfüllt sein. Die Währung muss einen relativ stabilen Wechselkurs haben[75]. Wenn dies nicht der Fall ist, trauen sich die Leute entweder nicht, Geld in dieser Währung zu besitzen, aus Angst vor einer Wertminderung, oder sie hoffen auf Gewinne und wollen ihr Geld nicht ausgeben. Damit dieser Fall eintritt, muss das

[67] Vgl. Ebenda
[68] Vgl. SRF.ch
[69] Vgl. 20min.ch
[70] Vgl. Schneeberger, Christoph; Interview mit Gabriel Marco. (25.6.2018) Siehe Interview ab Seite
[71] Vgl. Schär, Fabian (2018).
[72] Vgl. Blog.Bitpay.com
[73] Vgl. Bitpay.com
[74] Vgl. Boxtec.ch
[75] Vgl. Haran, Neil. What's keeping cryptocurrencies from mass adoption?, 2017.

Umfeld um Kryptowährungen stabiler werden. Das heisst, die Veränderungen und neuen Innovationen müssen langsamer werden, und es muss klare Gesetze für Kryptowährungen geben. Eine weitere Voraussetzung ist, dass die Kryptowährungen einen klaren Vorteil gegenüber herkömmlichen Systemen bietet. Dies ist teilweise jetzt schon so, denn Kryptowährungen sind schneller als Banken und günstiger als Kreditkarten-Systeme. Aber Kryptowährungen sind nicht unübertrefflich.

Ein subjektiver Faktor, der von allen anderen Faktoren abhängig ist, ist der Glaube an eine Währung. Dieser hängt vor allem von der Kursstabilität, den Gesetzen und der Verbreitung ab. Kryptowährungen gibt es noch nicht lange und es wird noch an vielen gearbeitet. Aufgrund dessen, und weil momentan vor allem junge Leute den Kryptowährungen vertrauen, ist anzunehmen, dass der Glaube an Kryptowährungen in der Zukunft stärker sein wird.

Die Akzeptanz von Kryptowährungen könnte auch das Resultat einer erneuten Finanzkrise sein. Bei Finanzkrisen verschwindet das Vertrauen in Banken, und Kryptowährungen stellen eine mögliche Alternative dar[76].

6 Diskussion

Zurzeit haben Kryptowährungen noch verschiedene Probleme, die eine weite Verbreitung verhindern. Unter diesen Problemen ist der enorme Stromverbrauch, aber auch die fehlenden Kapazitäten um viele Transaktionen zu verarbeiten. Diese Probleme können jedoch durch Veränderungen der Systeme behoben werden. Zum Beispiel durch einen Wechsel von Proof of Work auf Proof of Stake. Die Gemeinschaft von Ethereum wird diesen Wechsel vermutlich bald umsetzen[77]. Ein stabiler Kurs ist eine weitere Voraussetzung, die Kryptowährungen erfüllen müssen, um von vielen Leuten verwendet zu werden. Auch das ist theoretisch möglich, momentan sind die Wechselkurse aber noch sehr instabil.

Dank der höheren Geschwindigkeit und tiefen Gebühren haben Kryptowährungen das Potenzial, Banküberweisungen zu ersetzen. Auch Online Zahlungen, die momentan mit PayPal oder Kreditkarten bezahlt werden, können sehr gut mit Kryptowährungen erledigt werden. Zahlungen mit Bargeld, EC- oder Kreditkarten die nur wenige Sekunden dauern dürfen, können durch Kryptowährungen nicht effizient vollbracht werden. Eine Ausnahme stellt aber eine zentralisierte Kryptowährung wie Ripple dar. Es wird jedoch auch am sogenannten Lightning-Netzwerk gearbeitet. Dieses benutzt zwar eine Blockchain als

[76] Vgl. Leisin, Jonas. Haben Kryptowährungen das Potential, den US- Dollar als Leitwährung abzulösen? Bitcoin, Ripple und IOTA, 2018.
[77] Vgl. Tuwiner, Jacob. Ethereum's Switch to Proof of Stake – Better Than Proof of Work?, 30.012018.

Grundlage, soll aber blitzschnelle Transaktionen erlauben, indem die Transaktionen von der Blockchain losgelöst werden.

Die Akzeptanz von Kryptowährungen als Zahlungsmittel hat für Unternehmen folgende mögliche Auswirkungen.

Positive Auswirkungen:

- Die Akzeptanz sorgt für Aufsehen
- Es fallen weniger Gebühren an als mit andere Zahlungsmethoden
- Die Zahlungsabwicklung funktioniert zu jeder Zeit

Negative Auswirkungen:

- Wegen fehlender Akzeptanz der Lieferanten nicht weiterverwendbar
- Nur von wenigen Kunden benutzt
- Instabilität des Wechselkurses

Die befragten Unternehmen sprachen jedoch vorwiegend von positiven Effekten. Daraus folgt, dass es sich für Unternehmen grundsätzlich lohnt, Kryptowährungen als Zahlungsmittel zu akzeptieren. Die Vorteile überwiegen die Nachteile. Es ist aber zu beachten, dass je nach Unternehmen die Umstände anders sind. Zum Beispiel, ob die Kryptowährung an die Lieferanten weitergegeben werden kann oder nicht. Der wichtigste Faktor ist natürlich, ob die Kunden überhaupt mit einer Kryptowährung zahlen möchten. Da ich mich nur für die Erfahrungen von Unternehmen interessierte, habe ich nur solche interviewt, die bereits Kryptowährungen annehmen. Unternehmen, die noch keine Kryptowährungen akzeptieren, haben eventuell andere Ansichten.

Steuerrechtlich gelten Kryptowährungen als Wertschriften. Das heisst, dass durch Kursveränderungen erzielter Gewinn steuerfrei ist. Ausser, man handelt damit geschäftlich. Dann muss der Gewinn als Einkommen versteuert werden, man darf dafür aber auch Verluste von den Steuern abziehen.

Das Geldwäschereigesetz[78] gilt auch für Kryptowährungen. Deswegen muss man seine Identität angeben, um welche zu kaufen. Die Herkunft von Vermögen in Kryptowährungen muss jedoch noch nicht überprüft werden. Die Gesetzeslage könnte sich aber noch verändern, denn Transaktionen von Kryptowährungen sind dank der öffentlichen Blockchain sehr einfach verfolgbar. Momentan ist das noch nutzlos, denn man weiss nicht, wer sich hinter einer Adresse in der Blockchain verbirgt. Doch das könnte sich ändern. Falls einmal bekannt ist, dass eine Adresse Schwarzgeld besitzt, könnte man verbieten, dieses Geld

[78] Vgl. Admin.ch

anzunehmen. Der Geldwäscher könnte sein Vermögen nicht mehr bei einer legalen Tauschbörse gegen eine Landeswährung eintauschen. Doch das funktioniert bisher nur theoretisch.

7 Schlusswort

Das Erarbeiten der Maturaarbeit empfand ich als sehr lehrreichen Prozess. Ich lernte viele neue Dinge über Kryptowährungen und bin gespannt, wie sich diese Technologie weiterentwickeln wird. Zusätzlich habe ich erfahren, wie es ist, selbstständig eine grosse Arbeit zu verfassen. Ab und zu bereute ich meine Entscheidung, eine rein theoretische Maturaarbeit zu verfassen. Ich hätte lieber noch ein Produkt erschaffen, was zu diesem Thema leider nicht wirklich möglich ist. Auch bereue ich, das Thema nicht enger eingegrenzt zu haben. Dadurch hätte ich viel stärker auf Details eingehen können, was ich sehr interessant gefunden hätte. Schlussendlich hätte ich früher anfangen sollen, die Dokumentation zu schreiben. Das Schreiben von dieser dauerte länger als ich erwartet habe.

8 Anhang

8.1 Literaturverzeichnis

20min.ch (13.03.2017). „Grössere IT-Panne bei Migros-Bank“. [https://www.20min.ch/finance/news/story/Groessere-IT-Panne-bei-Migros-Bank-11844237]. (15.10.2018).

Admin.ch. „Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung“. [https://www.admin.ch/opc/de/classified-compilation/19970427/index.html]. (14.10.2018).

Årebo, Ingrid (2014). „Island profiliert sich als grünes Datenzentrum“. In: NZZ, 23. Mai 2014. [https://www.nzz.ch/wirtschaft/island-profiliert-sich-als-gruenes-datenzentrum-1.18308011]. (14.10.2018).

Baratt, Monica et al. „Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States“. [https://onlinelibrary.wiley.com/doi/abs/10.1111/add.12470]. (14.10.2018).

Bergmann, Christoph (28.05.2018). „Warum der hohe Stromverbrauch von Bitcoin vermutlich kein Problem für die Umwelt ist“. [https://bitcoinblog.de/2018/05/28/warum-der-hohe-stromverbrauch-von-bitcoin-vermutlich-kein-problem-fuer-die-umwelt-ist/]. (14.10.2018).

Bfe.admin.ch (06.2018). „Überblick über den Energieverbrauch der Schweiz im Jahr 2017“. [http://www.bfe.admin.ch/php/modules/publikationen/stream.php?extlang=de&name=de_481063357.pdf]. (14.10.2018).

Bitcoin.it. List of Bitcoin mining ASICs. [https://en.bitcoin.it/wiki/List_of_Bitcoin_mining_ASICs]. (14.10.2018).

Bitpay.com. „How do bitcoin block confirmations work?“. [https://support.bitpay.com/hc/en-us/articles/115004832203-How-do-bitcoin-block-confirmations-work-]. (14.10.2018).

Bitpay.com. Pricing. [https://bitpay.com/pricing]. (15.10.2018).

Blockchain.com. Block #0. [https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f]. (14.10.2018).

Blockchain.com. Hash Rate. [https://www.blockchain.com/de/charts/hash-rate]. (14.10.2018).

Blockchainwelt.de (02.03.2018). „Bitcoin Difficulty | Einfach erklärt“. [https://blockchainwelt.de/bitcoin-difficulty-einfach-erklaert/]. (14.10.2018).

Blog.Bitpay.com (02.10.2017). „BitPay’s Bitcoin Payments Volume Grows by 328%, On Pace for $1 Billion Yearly“. [https://blog.bitpay.com/bitpay-growth-2017/]. (15.10.2018).

Bolzli, Michael (26.04.2018). „Bitcoin verbraucht so viel Strom wie die Schweiz“. [https://www.nau.ch/politik/wirtschaft/bitcoin-verbraucht-so-viel-strom-wie-die-schweiz-65329343]. (14.10.2018).

Boxtec.ch. Liefer- und Versandkosten. „Zahlungsarten“. [https://shop.boxtec.ch/shipping.php#payment]. (15.10.2018).

Burgess, Jed et al. „Public Key Cryptography“. [https://cs.stanford.edu/people/eroberts/courses/soco/projects/public-key-cryptography/main.html]. (14.10.2018).

Cadwalladr, Carole (06.10.2018). „How I bought drugs from 'dark net' – it's just like Amazon run by cartels“. [https://www.theguardian.com/society/2013/oct/06/dark-net-drugs]. (14.10.2018).

Carlsten, Miles et al. „On the Instability of Bitcoin Without the Block Reward“. [http://randomwalker.info/publications/mining_CCS.pdf]. (14.10.2018).

Chi, Clifford (30.08.2018). „7 of the Best Bitcoin Mining Hardware for 2018“. [https://blog.hubspot.com/marketing/bitcoin-mining-hardware]. (14.10.2018).

Coindesk.com (29.01.2018). „How do Bitcoin Transactions Work?“. [https://www.coindesk.com/information/how-do-bitcoin-transactions-work/]. (14.10.2018).

Cryptocurrencyarmy.com. „Properties Of Cryptocurrencies“. [https://www.cryptocurrencyarmy.com/properties-of-cryptocurrencies/]. (14.10.18).

Cryptoguru.org. Burst Explorer. Estimated Network Size. [https://explore.burst.cryptoguru.org/chart/supply/network_size]. (14.10.2018).

D’Aliessi, Michele (01.06.2016). „How Does the Blockchain Work?“. [https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae]. (14.10.18).

Draglet.com. „What is Ripple? The Ultimate Beginner’s Guide“. [https://www.draglet.com/what-is-ripple/]. (14.10.2018).

Eklitzke.org (07.12.2017). „How Many Bitcoins Did Satoshi Nakamoto Mine?“. [https://eklitzke.org/how-many-bitcoins-did-satoshi-nakamoto-mine]. (14.10.2018).

Eliott, Francis und Duncan, Gary (2009). „Chancellor Alistair Darling on brink of second bailout for banks“. In: The Times, 3. Januar 2009.

EStv.admin.ch (27.07.2012). Kreisschreiben Nr. 36. „Gewerbsmässiger Wertschriftenhandel“. [https://www.estv.admin.ch/dam/estv/de/dokumente/bundessteuer/kreisschreiben/2004/1-036-D-2012.pdf.download.pdf/1-036-D-2012-d.pdf]. (14.10.2018).

Europa.eu (25.11.2005). „RICHTLINIE 2005/60/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung“. [https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=uriserv:OJ.L_.2005.309.01.0015.01.DEU]. (14.10.2018).

Fedpol.admin.ch. „Falschgeldstatistik 2017“. [https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/falschgeld/statistik/stat-2017-d.pdf]. (14.10.2018).

Gauthier, Pascal (12.07.2016). „Why Do Some Bitcoin Mining Pools Mine Empty Blocks?“. [https://bitcoinmagazine.com/articles/why-do-some-bitcoin-mining-pools-mine-empty-blocks-1468337739/]. (14.10.2018).

Gordon, Shawn. „What is Ripple?“. [https://bitcoinmagazine.com/guides/what-ripple/]. (14.10.2018).

Greenberg, Andy (05.09.2013). „Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market“. [https://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-

we-got-busted-buying-drugs-on-silk-roads-black-market/#1b52f397adf7]. (15.10.2018).

Handelszeitung.ch (15.01.2015). „Nationalbank hebt Mindestkurs auf - Euro stürzt ab“. [https://www.handelszeitung.ch/konjunktur/schweiz/nationalbank-hebt-mindestkurs-auf-euro-stuerzt-ab-724798]. (14.10.2018).

Haran, Neil (2017). „What’s keeping cryptocurrencies from mass adoption?“. [https://techcrunch.com/2017/04/20/whats-keeping-cryptocurrencies-from-mass-adoption/]. (15.10.2018).

IBM.com. „Characteristics of public key pairs“. [https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.12/gtps7/s7char1.html]. (14.10.2018).

ICTax.admin.ch. Kurslisten Direkte Bundessteuer 2018. [https://www.ictax.admin.ch/extern/de.html#/ratelist/2018]. (14.10.2018).

Irena.org. „Renewable Power Generation Costs in 2017“. [https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2018/Jan/IRENA_2017_Power_Costs_2018.pdf#page=40]. (14.10.2018).

Jeffries, Adrianne (02.06.2014). „Silk Road may have prevented drug violence, study says“. [https://www.theverge.com/2014/6/2/5772572]. (14.10.2018).

Kasper, Jan. Zahlungsmittel ohne Bank? Bitcoin als Währung der Zukunft. Norderstedt: GRIN Verlag, 2017.

Kollegistans.ch. „HAUSORDNUNG KOLLEGIUM ST. FIDELIS FÜR DAS SCHULJAHR 2018/19“. [https://portal.kollegistans.ch/rf/Reglemente/Hausordnung_2018_19.docx.pdf]. (14.10.2018).

Kraken.com. „How long do digital assets/cryptocurrency deposits take?“. [https://support.kraken.com/hc/en-us/articles/203325283-How-long-do-digital-assets-cryptocurrency-deposits-take-]. (14.10.2018).

Leisin, Jonas. Haben Kryptowährungen das Potential, den US- Dollar als Leitwährung abzulösen? Bitcoin, Ripple und IOTA. GRIN Verlag, 2018.

Lemats.net. MD5-Hash erzeugen. [https://lemats.net/tech/tools/md5-hash-erzeugen/]. (14.10.2018).

Mathew, Joel (29.06.2018). „Cryptocurrency: Japan’s Approach“. [https://blog.ipleaders.in/cryptocurrency-japan-approach/]. (14.10.2018).

Mims, Christopher (20.10.2008). „One Hot Island: Iceland's Renewable Geothermal Power“. [https://www.scientificamerican.com/article/iceland-geothermal-power/]. (14.10.2018).

Nakamoto, Satoshi (11.02.2009). „Bitcoin open source implementation of P2P currency“. [http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source]. (14.10.2018).

Nakamoto, Satoshi (31.10.2008). „Bitcoin: A Peer-to-Peer Electronic Cash System“. [https://bitcoin.org/bitcoin.pdf]. (14.10.2018).

Oracle.com. Signature Algorithms. [https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html#Signature]. (14.10.2018).

Pacia, Chris (07.09.2013). „Bitcoin Explained Like You’re Five: Part 3 – Cryptography“. [https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/]. (14.10.2018).

Poloniex.com. Bitcoin Exchange. [https://www.poloniex.com/exchange#usdt_btc]. (14.10.2018).

Postfinance.ch. „Steinreiche Menschen“. [https://young.postfinance.ch/steinreiche-menschen]. (14.10.2018).

Ross, Anderson (Professor am Computer Laboratory, Universität von Cambridge) (23.03.2018) Im Video „Stolen Bitcoin Tracing“ von Computerphile, Sean Riley. TC:07:30. [https://www.youtube.com/watch?v=UlLN0QERWBs&feature=youtu.be&t=450]. (14.10.2018).

Rüegg, Philipp (09.02.2018). „Grafikkarte nur fürs Crypto Mining kaufen: Lohnt sich das überhaupt (noch)?“. [https://www.digitec.ch/de/page/grafikkarte-nur-fuers-crypto-mining-kaufen-lohnt-sich-das-ueberhaupt-noch-6897]. (14.10.2018).

S., Jimi (5.5.2018). „Blockchain: how a 51% attack works (double spend attack)“. [https://hackernoon.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474]. (14.10.2018).

Schär, Fabian (Geschäftsleiter für das Center for Innovative Finance der Universität Basel) (24.05.2018) Referat „Bitcoin, Blockchain und Kryptoassets“ an der Veranstaltung „Investieren in die Zukunft“ von Balmer-Etienne. [http://balmer-etienne.ch/wp-content/uploads/2018/02/Einladung_VAG_mit-Crowdhouse_Finanzplanung_23.-24.-Mai-2018.pdf]. (15.10.2018).

Schischke, Karsten (02.2005). „Energie- und CO2-Bilanz von PCs – Relevanz für ReUse-Strategien“. [http://www.reuse-computer.org/fileadmin/user_upload/documents/wissArbeiten/CO2-BilanzSchischke.pdf]. (14.10.2018).

SNB.ch (06.09.2011). „Nationalbank legt Mindestkurs von 1.20 Franken pro Euro fest „. [https://snb.ch/de/mmr/reference/pre_20110906/source/]. (14.10.2018).

SRF.ch (12.03.2016). „Störung bei Postfinance: Blackout mitten in der Einkaufszeit“. [https://www.srf.ch/news/schweiz/stoerung-bei-postfinance-blackout-mitten-in-der-einkaufszeit]. (15.10.2018).

Stackexchange.com (23.05.2017). „What happens to Private Key on Payment“. [https://bitcoin.stackexchange.com/questions/53649/what-happens-to-private-key-on-payment]. (14.10.2018).

Stackoverflow.com (25.07.2009). „Is it possible to encrypt with private key using .net RSACryptoServiceProvider?“. [https://stackoverflow.com/questions/1181421/is-it-possible-to-encrypt-with-private-key-using-net-rsacryptoserviceprovider]. (14.10.2018)

Statista.com. „Bitcoin network average energy consumption per transaction compared to VISA as of 2018 (in kilowatt-hours)“. [https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/]. (14.10.2018).

Steuern-nw.ch (15.01.2018). „Kryptowährungen (z.B. Bitcoin, Ethereum, Ripple, Litecoin)“. [http://www.steuern-nw.ch/fileadmin/steuern_nw2/content/documents/Merkblatt/StP-NW_44_MB_Kryptowaehrungen.pdf]. (14.10.2018).

Steuern-nw.ch. Natürliche Personen. „Wertschriftenhandel“. [http://www.steuern-nw.ch/natuerlichepersonen/einkommenssteuer/wertschriftenhandel/]. (14.10.2018).

Strompreis.elcom.admin.ch. Der kantonale Strompreis im Vergleich. [https://www.strompreis.elcom.admin.ch/Map/ShowSwissMap.aspx]. (14.10.2018).

Tassev, Lubomir (20.04.2018). „Europe Introduces Customer Verification on Cryptocurrency Exchanges“. [https://news.bitcoin.com/europe-introduces-customer-verification-on-cryptocurrency-exchanges/]. (14.10.2018).

Tuwiner, Jacob (30.01.2018). „Ethereum’s Switch to Proof of Stake – Better Than Proof of Work?“. [https://usethebitcoin.com/ethereums-switch-proof-work-proof-stake/]. (15.10.2018).

Wikipedia.org. Cost of electricity by source. [https://en.wikipedia.org/wiki/Cost_of_electricity_by_source]. (14.10.2018).

Wikipedia.org. Electricity sector in China. [https://en.wikipedia.org/wiki/Electricity_sector_in_China]. (14.10.2018).

Wikipedia.org. Ripple (Geldsystem). [https://de.wikipedia.org/wiki/Ripple_(Geldsystem)]. (14.10.2018).

Wikipedia.org. Silk Road. [https://de.wikipedia.org/wiki/Silk_Road]. (14.10.2018).

8.1.1 Abbildungen

Titelbild: Unhashed.com. „How to Buy Bitcoin and Ethereum“. [https://unhashed.com/how-to-buy-cryptocurrency/bitcoin-ethereum/]. (14.10.2018).

Abb. 1 Von mir erstellt

Abb. 2 Von mir erstellt

Abb. 3 Von mir erstellt

Abb. 4 Von mir erstellt

Abb. 5 Von mir erstellt

Abb. 6 Von mir erstellt

Abb. 7 Ray, Shaan (29.11.2017). „Blockchain Forks“. [https://hackernoon.com/blockchain-forks-b0dca84db0b0]. (14.10.2018). Von mir bearbeitet.

Abb. 8 Ray, Shaan (29.11.2017). „Blockchain Forks“. [https://hackernoon.com/blockchain-forks-b0dca84db0b0]. (14.10.2018). Von mir bearbeitet.

Abb. 9 S., Jimi (5.5.2018). „Blockchain: how a 51% attack works (double spend attack)“. [https://hackernoon.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474]. (14.10.2018). Von mir bearbeitet.

Abb. 10 Carlsten, Miles et al. „On the Instability of Bitcoin Without the Block Reward“. [http://randomwalker.info/publications/mining_CCS.pdf]. (14.10.2018).

Abb. 11 Ebenda

8.1.2 Interviews

Odermatt, Rene (Geschäftsinhaber der Stiller Hahn Haustechnik GmbH, Aawasserstr. 2, Dallenwil) (19.7.2018) E-Mail.

Weshalb hast Du beschlossen, Kryptowährungen zu akzeptieren?

Unsere Geschäftsphilosophie ist nicht nur Gutes Handwerk abzuliefern, sondern auch immer einen Schritt voraus zu sein. Sei es gegenüber der Konkurrenz oder der gesamten Geschäftswelt. Dadurch war der Entscheid Kryptowährung zu akzeptieren naheliegend.

Wie gross ist der Anteil der Kunden, die mit Kryptowährungen bezahlen?

Da sich die Kryptowährung noch am Anfang befindet und bloss ca 1% der Zahlungen Weltweit über Kryptowährungen gemacht werden, ist der Kundenstamm eher tief. Wir haben eine Mikrobrauerei aus Dallenwil, die unsere Arbeit mit Kryptowährung bezahlt hat. Es dürften gerne mehr sein. (schmunzeln)

Weshalb hast Du Dich dazu entschieden, genau Bitcoin und Ethereum, aber keine anderen Kryptowährungen zu akzeptieren?

Bitcoin haben wir aus Werbegründen gemacht. Die grosse Allgemeinheit kennt Bitcoin oder hat schon mal davon gehört. Ethereum ist aber für uns viel interessanter. Um dies zu verstehen braucht man einige Zeit. Einfach gesagt, viele Kryptowährungen laufen über die Blockchain von Ethereum. Dadurch ist sie für uns so spannend.

Tauschst Du die Kryptowährungen nach Erhalt in Franken um, wenn ja, weshalb?

Nein, nein, im Moment sind die Zahlungen und die Beträge noch überschaubar. Gerne würde ich mehr Zahlungen annehmen aber das braucht noch einige Jahre. Es würde vieles einfacher machen.

Hast Du Erfahrungen mit plötzlichen oder starken Kursschwankungen gemacht, wenn ja, welche?

Die Kursschwankungen sind meistens nur Momentaufnahmen. In letzter Zeit hat sich die Kryptowährung gut eingependelt. Natürlich ist es weiterhin ein Glückspiel, doch viel gefährlicher sind die neuen Kryptowährungen. Diese kommen auf den Markt, häufen Kapital an und danach verschwinden sie wieder.

Inwiefern profitierst Du durch das Akzeptieren von Kryptowährungen (z.B. mehr Kunden, weniger Unkosten als andere Zahlungsmöglichkeiten)?

In unserem Fall waren wir die ersten in Nidwalden und dadurch auch im Gespräch. Mehr Kunden haben wir nicht aber es wird darüber geredet und dies ist Gut für uns und die Kryptowährung. Es müssten viel mehr Firmen mitziehen, so würde die Kryptowährungen Saloon fähig.

Profitierst Du von der schnellen Transaktionsabwicklung im Gegensatz zu Banküberweisungen, die nur zu Bürozeiten ausgeführt werden?

Die Transaktionsgeschwindigkeit ist unglaublich. Auch die Überweisungsgebühren sind absolut spitze. Die Banken werden auf lange Sicht einige Schwierigkeiten beim Dailybusiness bekommen. Einfach, schnell, unkompliziert und sehr anonym. Leider profitieren wir aktuell noch gar nicht. Aber wenn unsere Lieferanten auf den Zug aufspringen, könnten wir in 10 – 15 Jahren so unsere Rechnungen bezahlen.

Röll, Phillipp (Geschäftsführer der TrafficPlex GmbH, Konsul-Smidt-Str. 90, DE-Bremen) (25.06.2018) E-Mail.

Weshalb hast Du beschlossen, Kryptowährungen zu akzeptieren?

Es wurde danach gefragt und es gab keinen Grund, es nicht als Zahlungsmethode zuzulassen. Der Aufwand für die Umsetzung war mit Bitpay gering.

Wie gross ist der Anteil der Kunden, die mit Bitcoin bezahlen?

2015: 0,55%

2016: 0,62%

2017: 0,64%

2018 (bis 25.6.): 0,09%

Weshalb hast Du dich für Bitcoin und keine andere Kryptowährung entschieden?

Die Kryptowährung ist mir grundsätzlich egal, wenn Kunden nach ETH fragen würden, würde ich ggf. auch das anbieten. Zudem bietet Bitpay meines Wissens nach nur BTC an, eine weitere Währung wäre also Aufwand.

Weshalb nutzt Du einen Zahlungsprovider (Bitpay)?

Deutlich geringerer Aufwand für die Einbindung des Zahlungssystems.

Tauschst Du die Bitcoins nach Erhalt in Euro um, wenn ja, weshalb?

Das macht Bitpay für uns. Für uns ist Bitcoin nur ein Werkzeug um Zahlungen zu erhalten, an den Bitcoins haben wir kein Interesse.

Hast Du Erfahrungen mit plötzlichen oder starken Kursschwankungen gemacht, wenn ja, welche?

Das ist nicht unser Problem, sondern das von Bitpay ;-)

Hattest Du jemals Probleme mit dem Blockchain-System, z.B. aufgrund eines Forks?

Nein.

Inwiefern profitierst Du durch das Akzeptieren von Bitcoin (z.B. mehr Kunden, weniger Unkosten als andere Zahlungsmöglichkeiten)?

Das haben wir nie untersucht. Bitcoin war für uns immer ein Nischen-Zahlungsmittel. Hätten wir größeren Zuspruch gesehen (im Bereich von 3-5% o.ä.) wäre das etwas anderes gewesen.

Profitierst Du von der schnellen Transaktionsabwicklung im Gegensatz zu Banküberweisungen, die nur zu Bürozeiten ausgeführt werden?

Banküberweisungen benutzen in der Praxis kaum Kunden. Die Kunden verwenden zum Großteil Zahlungsmittel, die sofort bestätigt werden (PayPal, Kreditkarte, SOFORT Überweisung, paysafecard, ...), Banküberweisung macht nur ca. 9,5% der Zahlungen aus. Da ist Bitcoin für den Kunden teilweise unbequemer, weil die Zahlung per Bitcoin langsamer bestätigt wird als per PayPal, etc.

Schneeberger, Christoph (Geschäftsinhaber der BOXTEC AG, Liestalerstrasse 47, Lupsingen) (25.6.2018) E-Mail.

Weshalb haben Sie beschlossen, Kryptowährungen zu akzeptieren?

Auf mehrfache Kundenanfragen hin haben wir uns dem bis dahin für uns fremden/unbekannten Thema Ende 2014 angenommen.

Wie gross ist der Anteil der Kunden, die mit Kryptowährungen bezahlen?

1-3 von 100 Bestellungen werden im mittelfristigen Durchschnitt mit LTC oder BTC bezahlt. Bei gutem Kurs der Währungen eher mal gegen 5+ von 100 bei schlechtem Kurs wie z.B. jetzt eher 1 pro 100.

Weshalb haben Sie sich dazu entschieden, genau Bitcoin und Litecoin, aber keine anderen Kryptowährungen zu akzeptieren?

Beide Projekte haben eine recht lange erfolgreiche Laufzeit und der Code des Core Wallets wurde von vielen Augen gesehen. Ethereum erfüllt diese Bedingungen zurzeit noch nicht, wenn es mal 5 Jahre Laufzeit hat und über 1-2 Jahre stabil vorangeht ziehen wir es auch in Betracht. Weitere Kryptos die als Zahlungsmittel tatsächlich geeignet sind und tatsächlich auch ein sicheres und stabiles Netzwerk mitbringen sehen wir zurzeit nicht. Bitcoin Cash und all die anderen Forks von Bitcoin betrachten wir als Manipulationsversuche einzelner (zu) starker Marktteilnehmer und ziehen es deshalb vor, diese als Opensource fokussiertes Unternehmen nicht zu unterstützen.

Tauschen Sie die Kryptowährungen nach Erhalt in Franken um, wenn ja, weshalb?

Nein. Wir kaufen damit bei unseren Lieferanten wieder Ware ein.

Haben Sie Erfahrungen mit plötzlichen oder starken Kursschwankungen gemacht, wenn ja, welche?

Ja, erfreuliche und nicht so erfreuliche :-) Genauso wie mit EUR(sic!) und USD.

Hatten Sie jemals Probleme mit dem Blockchain-System, z.B. aufgrund eines Forks?

Nein, während des Forks zu Bitcoin Cash haben wir für einige Tage BTC Zahlungen suspendiert wie fast alle Anbieter und ansonsten haben wir nie Probleme gehabt. Im Gegensatz zum Beispiel zu Zahlungsanbietern wie Paypal wo gelegentlich schon mal ein Konto gesperrt und Geld einbehalten wird.

Inwiefern profitieren Sie durch das Akzeptieren von Kryptowährungen (z.B. mehr Kunden, weniger Unkosten als andere Zahlungsmöglichkeiten)?

Einerseits gehört es zum Image eines Opensource Outfits, sich modernen und dezentralen Konzepten zu öffnen. Andererseits ist bei guten Kursen zu beobachten, dass der mit Kryptos zahlende Kunde sehr kauffreudig ist und vielleicht da und dort was in den Korb legt was per Rechnung oder Kreditkarte nicht gekauft würde. Und natürlich ist es im Vergleich zu allen anderen Zahlungsmöglichkeiten für uns die kostengünstigste (was auch dem Umstand geschuldet ist, dass der Käufer alle Gebühren übernimmt), dies ist der Grund, dass wir 3% Rabatt für Kryptozahlungen anbieten und diese Ersparnis dem Kunden weitergeben. Zahlungen via Kreditkarte, Paypal oder Einzahlung am Postschalter weisen zum Teil je nach Gesamtbetrag noch höhere Gebühren auf.

Profitieren Sie von der schnellen Transaktionsabwicklung im Gegensatz zu Banküberweisungen, die nur zu Bürozeiten ausgeführt werden?

Eher nicht, der Zeitfaktor ist bei uns eher zweitrangig, im schlimmsten Fall wenn die Bestellung kurz vor Versandschluss (13:30) kommt und nicht bestätigt hat wird sie bei einem Neukunden halt am nächsten Tag verschickt (bei bestehenden Kunden wird situativ entschieden ob wir auf 1 Bestätigung warten). Unser Betrieb ist diesbzgl. nicht mit einer Supermarktkasse vergleichbar wo das OK innnert Sekunden oder schneller kommen muss.

Speziell bei BTC muss man je nach Lage ja eh schon mit Stunden bis Tagen rechnen. Ein grosses Plus ist aber, dass wir uns nicht darum sorgen müssen dass ein Dritter sauber arbeitet oder überhaupt arbeitet (z.B. Bank oder Postfinance mit ihren fast schon legendären Blackouts). Das Geschäft findet wie bei einer Barzahlung im Restaurant direkt zwischen Kunden und Anbieter statt und ist nicht auf den Goodwill einer dritten Partei angewiesen. Bei Vorkassenzahlung ist dies ein Problem, da auch heute noch oft das Geld nach sofortigem Abgang auf dem Kundenkonto viele Stunden irgendwo in der Luft ist aber noch nicht auf unserem Konto eingegangen.

8.2 Eigenständigkeitserklärung

Ich, Marco Gabriel, erkläre hiermit,

- dass ich die vorliegende Arbeit selbständig und nur unter Benutzung der angegebenen

  Quellen verfasst habe,

- dass ich auf eine eventuelle Mithilfe Dritter in der Arbeit ausdrücklich hingewiesen habe.

Ort, Datum:

Unterschrift: