

Hochschule Anhalt
Standort: Bernburg (Saale)

Funktionsweise, rechtliche Einordnung und
ökonomische Auswirkungen der Kryptowährung
Bitcoin

Sebastian Neumann

Matrikelnummer: 4058463
Erstgutachter: Prof. Dr. Carsten Sonnenberg
Zweitgutachter: Prof. Dr. Sebastian Volkmann
Studiengang: Wirtschaftsrecht
Abgabedatum: 23.11.2017

A. EINLEITUNG	3
B. BITCOIN ALS DIGITALE WÄHRUNG	4
I. SATOSHI NAKAMOTO	4
II. DIE ANFÄNGE VON BITCOIN.....	5
III. FUNKTIONSWEISE VON BITCOINS	6
a) <i>Mining</i>	8
b) <i>Tausch und Handel</i>	10
c) <i>Ablauf einer Transaktion</i>	11
IV. VOR- UND NACHTEILE VON KRYPTOWÄHRUNGEN NACH DER EZB	12
B. RECHTLICHE EINORDNUNG VON BITCOINS	14
I. BITCOINS ALS GELD	14
II. BITCOINS ALS WÄHRUNG	15
III. MÖGLICHE ZIVILRECHTLICHE AUSRICHTUNG VON BITCOINS	15
a) <i>Bitcoin – Sache oder Recht</i>	15
b) <i>Möglicher Vertragstyp beim Erwerb von Bitcoin</i>	16
IV. STRAFRECHTLICHE ASPEKTE VON BITCOIN.....	17
V. DER HANDEL MIT BITCOIN.....	18
a) <i>Bitcoin bei Finanzkommissionsgeschäfte</i>	19
b) <i>Bitcoin in multilateralen Handelssystemen</i>	19
c) <i>Bitcoin bei der Vermittlung und dem Eigenhandel</i>	20
d) <i>Die Steuerpflicht bei Bitcoin</i>	20
VI. MEHRWERTSTEUERPFLICHT BEIM TAUSCH ZWISCHEN KONVENTIONELLEN WÄHRUNGEN UND BITCOIN	21
a) <i>Sachverhalt</i>	21
b) <i>Die Entscheidung und Entscheidungsgründe des EuGH sowie dessen Bedeutung für den Bitcoin</i>	22
D. DER BITCOIN IM WIRTSCHAFTLICHEN GESCHÄFTSLEBEN	23
I. KURSENTWICKLUNG	23
II. RISIKEN VON BITCOIN	25
a) <i>Die 51% Attacke</i>	25
c) <i>Silk Road</i>	26
d) <i>Kriminelle Programmentwicklung</i>	28
e) <i>Verlustrisiko</i>	28
f) <i>Verbotsrisiko</i>	29
g) <i>Nischenrisiko</i>	29
h) <i>Kontrollrisiko</i>	30
i) <i>Spekulationsrisiko</i>	30
j) <i>Deflationsrisiko</i>	31
k) <i>Regulierungsrisiko</i>	31
III. CHANCEN VON BITCOIN	33
a) <i>Innovationschance</i>	33
aa) <i>Multisignatur-Transaktionen</i>	33
bb) <i>Bitpay</i>	34
cc) <i>Hardware Wallets</i>	35
b) <i>Kostenchance</i>	36
c) <i>Dezentralisierungschance</i>	36
d) <i>Wertsteigerungschance</i>	36
e) <i>Marktchance</i>	37
IV. DER BITCOIN ALS OFFIZIELLES ZAHLUNGSMITTEL IN JAPAN	37
V. DIE BLOCKCHAIN – EINE REVOLUTIONÄRE TECHNOLOGIE.....	38
E. SCHLUSSBETRACHTUNG	40

ABBILDUNGSVERZEICHNIS.....	45
ABKÜRZUNGSVERZEICHNIS	46
SELBSTSTÄNDIGKEITSERKLÄRUNG.....	48

A. Einleitung

Seit der Einführung des Internets in den 90er Jahren hat es im Laufe der Zeit immer mehr an Bedeutung im Leben der Menschen gewonnen. Das World Wide Web besitzt die Fähigkeit eine Menge von Informationen zu speichern und für alle seine Nutzer zugänglich zu machen. Dank dem damit verbundenem, enormem Wachstumspotenzial fand eine große Weiterentwicklung insbesondere in den Bereichen der Technik, Wissenschaft und Wirtschaft statt. So ist es durch das World Wide Web ermöglicht wurden eine globale Handelsplattform unter den Nutzern zu generieren. Dementsprechend bildeten sich mit der Zeit diverse Onlineshops, die es den Kunden ermöglichten Güter und Waren aus der ganzen Welt zu erwerben. Allerdings stellen die weltweit unterschiedlichen Währungen für diese Handelsmethode noch immer ein Problem dar, da es keinen einheitlichen Zahlungsverkehr ermöglicht.¹

Im Jahre 2009 wurde zur Behebung dieses Problems die Idee einer einheitlichen digitalen Währung publiziert. Dabei handelte es sich um ein globales, dezentrales Zahlungsmittel was ausschließlich im Internet gehandelt werden konnte und keinen physikalischen Wert in der realen Welt durch etwa Münzen oder Scheine wie Fiatgeld besaß. Diese im Internet vorgestellte Währung trug den Namen „Bitcoin“².

Bitcoins schufen mit ihrer Einführung den Beginn einer sogenannten Krypto-Ökonomie. Diese junge Ökonomie besitzt das Potenzial, ähnlich wie das Internet 20 Jahre zuvor, eine ökonomische Evolution einzuleiten. Aber gleichzeitig muss man sich auch vor den Gefahren hüten, die diese neuartige Ökonomie für die Gesellschaft mitbringen kann.³

Mit der Krypto-Ökonomie traten noch andere digitale Währungen im Internet auf, die über eine ähnliche Funktionsweise wie Bitcoins verfügten. Allerdings blieb der Bitcoin bis heute der populärste Vertreter.

¹ Vgl. (Sander, 2016) S.5,7

² Vgl. (Sander, 2016) S.6

³ Vgl. (Platzer, 2014) S. 14-15



Abbildung 1: Bitcoin und andere Kryptowährungen

In der folgenden Arbeit werden die Funktionsweise und wirtschaftliche Bedeutung der Bitcoins genauer behandelt. Weiterhin wird der Versuch einer rechtlichen Einordnung in das deutsche Rechtssystem vorgenommen.

B. Bitcoin als digitale Währung

Bei Bitcoins handelt es sich um eine virtuelle Zahlungseinheit. Die Währung besitzt keine Scheine oder Münzen und kann damit nur in digitaler Form im Internet gehandelt werden. Bitcoins sind dezentral, was bedeutet dass weder der Handel oder die Ausgabe von einem Staat oder von einer Bank abgewickelt wird. Der Handel mit Bitcoins findet also ausschließlich im Internet unter den Nutzern statt.⁴

Der Bitcoin wurde dementsprechend auch nicht wie eine gewöhnliche Währung von einem Staat eingeführt. Die Idee und das Konzept des Bitcoins wurde von einem unabhängigen Entwickler unter dem Internetpseudonym Satoshi Nakamoto entwickelt.

I. Satoshi Nakamoto

Man ist bis heute sich nicht wirklich sicher, ob sich hinter dem Pseudonym eine Gruppe oder eine einzelne Person verbirgt. Obwohl die Spekulationen eher zu einer Gruppe von Programmierern tendieren, da es für Entwicklung eines so großen und aufwendigen Projektes wie Bitcoins eine Menge an unterschiedlichen Kompetenzen braucht. Alle verfügbaren Informationen über das Pseudonym sind dessen eigenen Angaben bei der p2p-foundation, einer Organisation welche sich mit den verschiedenen Anwendungen des Peer-Peer Netzwerks auseinandersetzt. Dort gab er an, dass er männlich, am 05.04.1975 geboren und sein Heimatland Japan sei. Es ist für viele ein Rätsel warum das wahre

⁴ Vgl. (Sander, 2016) S.6

Gesicht hinter Satoshi Nakamoto nicht in Erscheinung tritt. Es wird aber dem Wissen geschuldet sein, dass seine Erfindung das Potenzial besitzt die finanziellen, wirtschaftlichen und politischen Machtgefüge in der Welt zu verändern. Daher könnte er als Entwickler in Gefahr laufen politisch verfolgt zu werden.⁵

Am 31.10.2008 wurde von ihm der Aufsatz „Bitcoin: A peer to peer electronic cash system“ sowie einen Tag später am 01.11.2008 das Whitepaper „A distributed time stamping system for contracts“ in der Cryptographies Mailingliste veröffentlicht. Darin beschreibt er die Hauptprobleme derzeitiger Währungen und wie man mit dem Open Source Prinzip und der Algorithmus Verschlüsselung des Bitcoins diese umgehen kann. Der offizielle Launch der Bitcoins war am 03.01.2009. Satoshi Nakamoto arbeitete danach noch 9 Monate an der Weiterentwicklung mit. Danach zog er sich langsam zurück, beantwortete keine E-Mails mehr und war auch nicht mehr in den Foren online.⁶

II. Die Anfänge von Bitcoin

Zum Launchdatum (03.01.2009) wurde von Satoshi Nakamoto über einen herkömmlichen PC der erste Genesisblock erzeugt. Damit wurden die ersten 50 Bitcoins ausgeschüttet. Die Funktionsweise dazu wird in darauffolgenden Kapiteln beschrieben. Durch die Neuartigkeit der Bitcoins gab es für sie keinen Referenzwert. Deshalb wurde der Preis in einem nur sehr kleinen Personenkreis ausgehandelt. Am 12.01.2009 fand die erste Transaktion in Höhe von 10 Bitcoin von Satoshi Nakamoto an Hal Dinney statt. Einige Monate später am 05.10.2009 wurde im New Liberty Standard der erste offizielle Wechselkurs veröffentlicht. Demnach entsprach 1 Dollar = 1392,33 Bitcoin. Zum 30.12.2009 wurde das erste Mal eine Hürde für das Minen eingebaut. Auch die Funktionsweise dazu wird in den folgenden Kapiteln erläutert. Eines der bedeutendsten Ereignisse in der Geschichte von Bitcoin trug sich am 22.05.2010 zu. An diesem Tag kaufte ein Mitglied der Bitcointalk-Community mit dem Username „lazlo“ zwei Pizzen für 10.000 Bitcoin. Der damalige Gegenwert dafür betrug um die 25 Dollar. Einige Jahre später hätte er zum Höchstkurs diese Menge für über 12 Millionen Dollar verkaufen können. Am 17.07.2017 wurde durch die Online Plattform Mt.Gox der Handel mit Bitcoins eröffnet. Gleichzeitig bot die Plattform auch die Möglichkeit den Bitcoin in andere Währungen wie etwa den Dollar, Euro, oder Yen umzutauschen. Damit gab es nun auch eine zentrale, leicht zugängliche Möglichkeit um Bitcoin auch

⁵ Vgl. (Strutzenberger, 2016) S.10-11

⁶ Vgl. (Strutzenberger, 2016) S.11

ohne Mining Bitcoins zu erlangen. Zum 18.07.2010 begann die Ära des GPU-Minings, da der erste Block mithilfe einer Grafikkarte erzeugt wurde. Vorher wurden Blocks nur mithilfe des Prozessors des PC's erzeugt. Grafikkarten werden von Hackern gern benutzt um sich Zugriff auf das System von Bitcoin zu verschaffen. Möglicherweise kam es deshalb am 15.08.2010 zur ersten Sicherheitslücke im System. Die allgemeinen Protokollregeln wurden gebrochen und es wurden 184 Milliarden Bitcoins erzeugt. Glücklicherweise bemerkte das Core Developer Team innerhalb weniger Stunden diesen Eingriff und konnte die fälschlich erzeugten Bitcoins ungültig machen. Im Laufe der nächsten Jahre sollten auch noch weitere Hackangriffe folgen. Am 09.02.2011 gelang Bitcoin eine Preisgleichheit mit dem Dollar.⁷

III. Funktionsweise von Bitcoins

Hinter dem technischen Grundkonzept der Bitcoins verbirgt sich ein Peer-to-Peer Netzwerk.

„Peer-to-Peer-Netze (P2P) sind Rechnernetze bei denen alle Rechner im Netz gleichberechtigt zusammen arbeiten. Das bedeutet, dass jeder Rechner anderen Rechnern Funktionen und Dienstleistungen anbietet und andererseits von anderen Rechnern angebotene Funktionen, Ressourcen, Dienstleistungen und Dateien nutzen kann. Die Daten sind auf viele Rechner, in der Regel auf die der Nutzer, verteilt. Das Peer-to-Peer-Konzept ist ein dezentrales Konzept, ohne zentrale Server, wie das Internet. Jeder Rechner eines solchen Netzes kann mit mehreren anderen Rechnern verbunden sein.“⁸

Durch dieses Netzwerk werden alle Nutzer gleichberechtigt untereinander behandelt und es ist keine übergeordnete Instanz notwendig. Außerdem besitzt ein solches Netzwerk nie eine feste Struktur. Dadurch ist es möglich das sich Nutzer aus dem System komplett zu entfernen oder integrieren können, ohne die Funktionstätigkeit des gesamten Systems zu beeinträchtigen.⁹

⁷ Vgl. (Strutzenberger, 2016) S.12-13

⁸ (ITWissen.info Technologiewissen online, 2014)

⁹ Vgl. (Strutzenberger, 2016) S.6

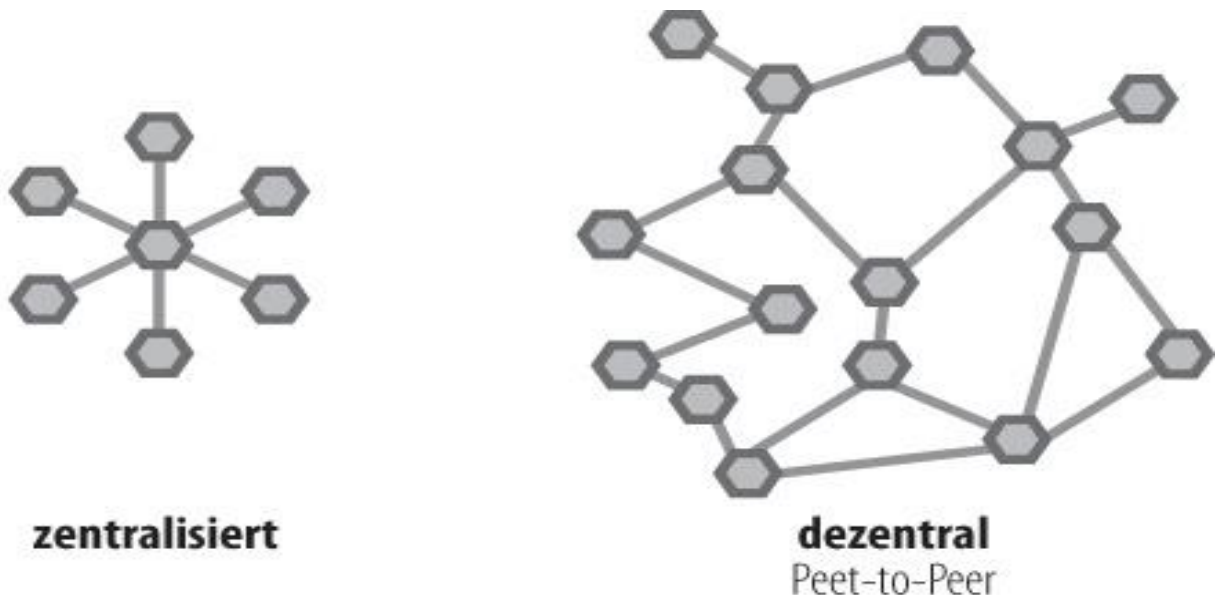


Abbildung 2: Struktur von Netzwerken

Dabei basiert das Peer-to-Peer Netzwerk von Bitcoin auf einer von allen Nutzern gemeinsam genutzten und verwalteten Datenbank. Innerhalb dieser Datenbank werden alle Transaktionen zwischen den Nutzern in der Blockchain gespeichert. Das Netzwerk fungiert dabei wie ein globales, kollektives Buchführungssystem wodurch es unmöglich ist Bitcoins zu verdoppeln oder zu fälschen.¹⁰

Die Konten der einzelnen Nutzer werden als Clients bezeichnet. Jeder Client besitzt ein sogenanntes Wallet. Die Clientsoftware inklusive den Wallets werden durch verschiedene Anbieter im Internet vertrieben. In dem Wallet werden aber nicht die eigentlichen Bitcoins aufbewahrt, sondern die Schlüssel zur eigenen Bitcoin - Adresse und damit seinem eigentlichen Kontostand welcher in der Blockchain gespeichert ist. So erhält man einen öffentlichen und einen privaten Schlüssel die mathematisch miteinander zusammenpassen. Durch den öffentlichen Schlüssel ist die eigene Bitcoin - Adresse für alle Clients im Netzwerk sichtbar. Dadurch können sich die Clients untereinander identifizieren und Bitcoins aneinander versenden. Durch den privaten Schlüssel erhalten die Clients Zugriff auf ihren eigenen Kontostand und auf Bitcoins welche ihnen von anderen Clients übertragen wurden.¹¹

Die Clientsoftware kann außerdem auf mehrere Datenträger gleichzeitig installiert werden, wie zum Beispiel am PC, Handy oder Laptop. Darüber hinaus kann jeder Client auch mehrere Wallets haben.¹²

¹⁰ Vgl. (Strutzenberger, 2016) S.6

¹¹ Vgl. (Strutzenberger, 2016) S.6

¹² Vgl. (Bank, February 2015) S.13

a) Mining

Jeden Tag werden unzählige Transaktionen mit Bitcoins über das Netzwerk getätigt. All diese Transaktionen werden aufgezeichnet und gespeichert. Einem Nutzer ist es allerdings nicht möglich einzusehen, wer welchen Betrag an welchen Nutzer gesendet hat. Diese Transaktionsdaten werden in die sogenannte Blockchain gespeichert. Die Blockchain besteht aus mehreren Blocks, welche die Transaktionsdaten von einem bestimmten Zeitraum beinhalten. Dadurch fungiert die Blockchain als eine Art Kontobuch für das System von Bitcoin. Ein Miner hat dabei die Aufgabe, die einzelnen Transaktionen zu bestätigen und in der Blockchain einzutragen. Dafür erhält er eine Belohnung in Bitcoins von dem System.¹³

Entsteht ein neuer Block durch Transaktionen wird von den Minern ein standardisierter Prozess verwendet. Sie entnehmen die Daten des Blocks und wandeln sie mit Hilfe einer mathematischen Formel in kürzere Datenstränge um. Dadurch bestehen die Informationen der Transaktionen aus einer Aneinanderreihung von Zahlen und Buchstaben. Diese Anreihung bezeichnet man als einen Hash. Der Hash wird im Block aufbewahrt und am Ende der Blockchain gespeichert.¹⁴

Jeder Hash ist dabei einzigartig. Wenn man nur ein Zeichen im Block verändert, verändert sich auch gleichzeitig der Hash. Dabei ist weiterhin zu beachten, dass die Miner zur Entstehung eines neuen Hashs nicht nur die Daten der Transaktionen benutzen, sondern auch zusätzliche Daten hinzuziehen. Dazu gehören die Daten des Hashs des letzten Blocks in der Blockchain. Damit besitzt jeder neue Hash also Daten der vorherigen Hashs. Dementsprechend kann der neue Hash den alten Hash bestätigen und bringt damit eine zusätzliche Sicherheit für das System. Würde jemand versuchen eine Transaktion zu manipulieren, indem er den Block verändert der bereits Teil der Blockchain ist, würde er damit auch den zugehörigen Hash verändern. Somit kann die Echtheit des Blockes mit der Hashingfunktion überprüft werden. Es würde dann festgestellt werden, dass dieser nicht identisch mit dem eigentlichen Eintrag in der Blockchain ist. Der Block kann dies dann als Fälschung erkennen.¹⁵

Miner suchen also daher im Netzwerk ständig nach neuen Blocks. Dabei konkurrieren die Miner stets untereinander und nutzen spezielle Software um möglichst schnell neue Blocks im Netzwerk ausfindig zu machen. Erzeugt ein Miner einen neuen Hash enthält er dafür eine Belohnung von momentan 12,5 Bitcoin. Zusätzlich erhält die Blockchain

¹³ Vgl. (Sander, 2016) S.38

¹⁴ Vgl. (Sander, 2016) S.38

¹⁵ Vgl. (Sander, 2016) S.38

ein Update und alle Nutzer erhalten Informationen darüber. Diese Belohnung stellt den Anreiz für die Miner dar und bewirkt die Aufrechterhaltung des Systems von Bitcoin. Dabei entsteht aber das Problem, dass es für unsere Computer sehr einfach ist aus einer bestehenden Datensammlung einen Hash zu erzeugen. Dementsprechend wurde im Bitcoin Netzwerk eine stetig wachsende Hürde integriert, wodurch verhindert werden soll, dass die Nutzer innerhalb kürzester Zeit hunderte Blocks hashen. Hinzu kommt, dass alle Bitcoins innerhalb weniger Stunden geschürft wären.¹⁶

Diese ständig wachsende Hürde ist der sogenannte Arbeitsnachweis. Dieser macht das Mining mit der Zeit immer schwieriger und damit auch zeitaufwendiger. Das System von Bitcoin wurde so aufgebaut, dass es nicht einfach die alten Hashs akzeptiert. Der neue Hash muss nach einem bestimmten Muster aufgebaut sein. Am Anfang besteht dieser immer aus einer bestimmten Anzahl von Nullen. Aber die darauf folgenden Zahlen und Buchstaben kann man nicht vorher wissen, da mit der Integration der Datensätze vergangener Hashs ein völlig neuer einzigartiger Hash entsteht. Dabei werden aber nur bestimmte Datensätze von den alten Hashs für den neuen Hash benötigt. Die Miner muss das passende Format finden damit der neue Hash entstehen kann und sie ihre Belohnung erhalten. Diese komplizierte Prozedur wird auch als „None“ bezeichnet und soll verhindern, dass Miner sich nicht in die Blockchain Einträge einmischen.¹⁷

Es gibt generell zwei Arten von Mining: ASIC Mining und das Cloud-Mining. Unter „Application-specific integrated circuit (ASIC)“ Miners versteht man Nutzer, die spezielle Mininghardware auf ihrem PC zuhause nutzen um damit Bitcoins zu schürfen.¹⁸

Da aber eine ständig höhere Rechenleistung benötigt wird, schließen sich solche Miner oft in sogenannten Miningpools zusammen. Dazu stellt jeder Nutzer seine Rechenleistung mit zur Verfügung und erhält dementsprechend einen Anteil an der Belohnung. Beim Cloud-Mining bietet ein Anbieter seine Server zum Minen an. Gegen Entgelt können andere Nutzer seine Server nutzen.¹⁹

Außer dem Schürfen von neuen Bitcoin-Blocks erhalten Miner noch eine zusätzliche Belohnung für die Verwaltung des Bitcoinnetzwerkes. Sie bekommen alle Transaktionsgebühren. Oftmals wird von vielen Quellen berichtet, dass bei

¹⁶ Vgl. (Sander, 2016) S.39-40

¹⁷ Vgl. (Sander, 2016) S.40

¹⁸ Vgl. (bitcoinmining.com, 2011-2017) ASIC Bitcoin Mining Hardware

¹⁹ Vgl. (Bank, February 2015) S.12

Transaktionen mit Bitcoin keine Gebühren anfallen. Das ist aber nicht vollständig die Wahrheit. Eigentlich hat Bitcoin flexible Gebühren, die im von nicht vorhanden bis sehr gering liegen. Häufig haben Bitcoin-Wallets eine standardmäßig voreingestellte Überweisungsgebühr, die abhängig vom jeweiligen Anbieter ist. Es ist allerdings für den Nutzer des Wallets möglich die Gebühren selbst festzulegen oder komplett wegzulassen. Wenn der Nutzer das tut kann dies jedoch auf die Geschwindigkeit auswirken, mit der die Transaktion vom Netzwerk bestätigt wird.²⁰

b) Tausch und Handel

Bitcoins können über verschiedene Onlinebörsen oder Bitcoinbesitzern für eine andere Währung eingetauscht werden. Dabei besteht auch die Möglichkeit Bitcoin über Paysafecards zu erwerben. Wenn Bitcoins durch Tauschbörsen oder Paysafecards erworben werden, so geschieht es in der Regel das Gebühren anfallen. Diese Gebühren können je nach Handelsplatz unterschiedlich hoch ausfallen. Im Regelfall betragen sie meist 0,2-1 Prozent vom Tauschbetrag.²¹

Die Online-Tauschbörsen werden dabei nicht von irgendeiner Behörde reguliert. Dennoch unterlegen sie diversen Regeln. Diese Regeln wurden von der Bitcoin Community weitgehend akzeptiert und dienen als Maßnahme gegen kriminelle Absichten, z.B. Geldwäsche. Eine Regel sieht etwa ein Auszahlungslimit vor. Bei dem Handel mit größeren Beträgen wird ein Identifikationsnachweis benötigt.²²

Ein- und Auszahlungen gehen direkt über das Wallet per Überweisung verzeichnet. Dabei will die Wahl des Walletanbieters wohlüberlegt sein. Wer als Nutzer einen schlechten Walletsoftware besitzt, riskiert durch einen Hackerangriff seinen gesamten Bitcoins zu verlieren. Mögliche Indikatoren für die Zuverlässigkeit von Walletanbietern sind dabei die Erfahrungsberichte von Nutzer oder Sicherheitszertifikate. Manche Tauschbörsen bieten dabei auch teilweise Haftung bei Hackerangriffen an, sodass der Nutzer ein Teil seiner Bitcoins erstattet bekommen kann. Die Höhe des erstatteten Anteils, richtet sich dabei nach den AGB des Walletanbieters.²³

Für den Handel mit Bitcoinbesitzern gibt es zusätzlich virtuelle Handelsplätze wo man, ähnlich wie bei Ebay, Kauf- und Verkaufsangebote abgeben kann.²⁴

²⁰ Vgl. (Platzer, 2014) S. 121

²¹ Vgl. (Sander, 2016) S. 53

²² Vgl. (Sander, 2016) S. 53

²³ Vgl. (Sander, 2016) S 54

²⁴ Vgl. (Sander, 2016) S 54

c) Ablauf einer Transaktion

In einer Transaktion zwischen den Nutzern A (Sender) und Nutzer B (Empfänger) sind folgende Informationen in der Transaktion enthalten:

1. Der Input

Der Input beinhaltet Informationen über die Vorgängeradresse. Das bedeutet er enthält die Information über den Nutzer, der Nutzer A diesen Bitcoin zunächst übersendet hat.

2. Die Menge

Diese Information beinhaltet die tatsächliche Menge an Bitcoins, die Nutzer A an Nutzer B zusenden möchte.

3. Der Output

Der Output enthält Information über die Empfängeradresse. Wenn Nutzer A also Bitcoins an Nutzer B übersenden möchte, enthält es die Information von Nutzer B.²⁵

Zum Versenden von Bitcoins werden zwei Dinge benötigt, eine gültige Bitcoin – Adresse und ein dazu passenden privaten Schlüssel. Die Bitcoin – Adresse wird mithilfe der Clientsoftware zufällig generiert. Sie besteht dabei aus einer zufälligen Reihenfolge von Buchstaben und Zahlen. Der private Schlüssel besteht gleichzeitig auch aus einer zufälligen Reihenfolge aus Zahlen und Buchstaben. Dabei ist zu beachten, dass der private Schlüssel niemals preisgegeben werden darf, da man sonst die Transaktion des Nutzers manipulieren kann.²⁶

Will Nutzer A also eine Transaktion an Nutzer B ausführen, muss er mithilfe seines privaten Schlüssels eine Nachricht signieren. Diese Nachricht beinhaltet dann die oben genannten Informationen des Inputs, der Menge und des Outputs.²⁷

²⁵ Vgl. (Altinpicak & Völkel, 2016)

²⁶ Vgl. (Altinpicak & Völkel, 2016)

²⁷ Vgl. (Altinpicak & Völkel, 2016)

Das Bitcoin-Prinzip

Vereinfacht dargestellt ist eine elektronische Münze eine Kette digitaler Signaturen mit dem Besitzer am Ende. Der Besitzer gibt die Münze weiter, indem er ans Ende der Kette eine Transaktion anfügt und mit seinem geheimen Schlüssel unterschreibt. Mit dem öffentlichen Schlüssel lässt sie sich überprüfen.

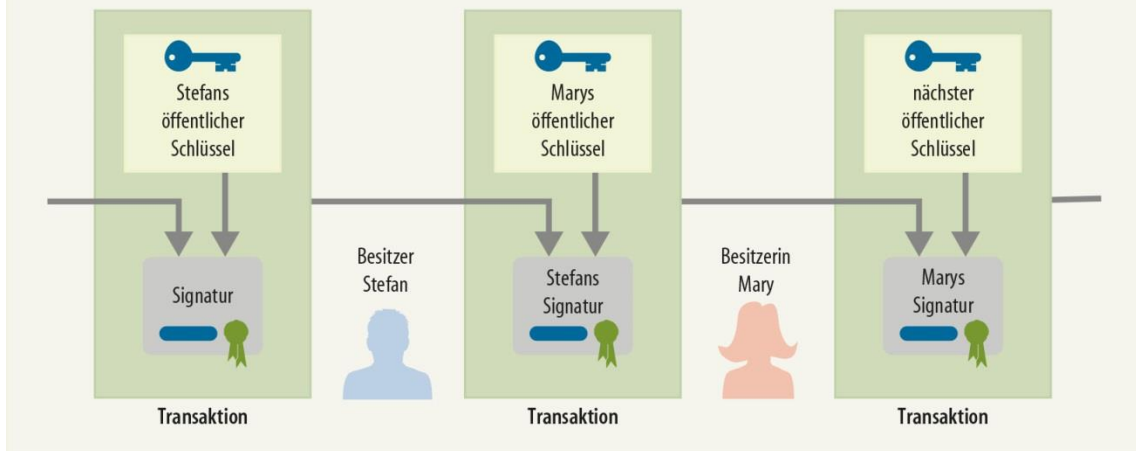


Abbildung 3: Transaktionsprinzip von Bitcoin

Nachdem dies geschehen ist, wird die Information über Transaktion an alle Nutzer verbreitet und dann von den Minern verifiziert. Sobald die Miner die Transaktion im Bitcoin Netzwerk verifiziert haben, wird sie als Block dem öffentlichen Transaktionsprotokoll, besser bekannt als Blockchain, zugefügt.²⁸

IV. Vor- und Nachteile von Kryptowährungen nach der EZB

Nach dem Bericht der EZB können durch virtuelle Währungen viele Vorteile für den Verbraucher entstehen. So kann zunächst einmal in sehr kurzer Zeit die Identifikation des Käufers dank seiner öffentlichen Bitcoinadresse schnell bestätigt werden und eine sofortige Transaktion bei einem Kaufgeschäft ist garantiert. Dank der Schnelligkeit der Transaktion können Waren damit sofort und ohne Verzögerungen versendet werden.²⁹

Ein weiterer großer Vorteil digitaler Währungen wie etwa Bitcoins ist die Anonymität. Bei Transaktionen sind für den Käufer und Verkäufer nur die dazugehörigen öffentlichen Adressen sichtbar. Private Daten der Geschäftsteilnehmer werden dabei nicht preisgegeben. Vielen Kunden gefällt das, da es für sie somit sichergestellt ist, dass ihre persönlichen Daten weder gespeichert noch weitergegeben werden könnten. Allerdings findet gerade die Anonymität der Bitcoins eine große Beliebtheit bei den Kriminellen für ihre Geschäfte.³⁰

²⁸ Vgl. (Altinpicak & Völkel, 2016)

²⁹ Vgl. (Bank, February 2015) S.18

³⁰ Vgl. (Bank, February 2015) S.19

Dabei kann allerdings als weiterer Vorteil angesehen werden, dass Bitcoins dank der Blockchain Technologie und dem Peer-to-Peer Netzwerk es für Hacker nahezu unmöglich ist Bitcoins zu ergaunern und diese für diverse andere Geschäfte einzusetzen. Des Weiteren hat man durch Bitcoins eine Kostenersparnis bei grenzüberschreitenden Zahlungen, da man weder mit Zöllen oder Kursunterschiede verschiedener Währungen zu tun hat.³¹

Ein Vorteil für die Händler ist außerdem der geringe Kostenaufwand zur Akzeptanz von Bitcoins. Ein Händler muss dazu nur eine Wallet von einem Internetanbieter herunterladen, um künftig Zahlungen in Bitcoin zu akzeptieren. Es könnten nur weitere Kosten durch das Involvieren von Payment – Provider entstehen. Allerdings wären selbst dann die Kosten nicht höher als die anderen Zahlungsmöglichkeiten, z.B. Zahlung per Karte.³²

Weiterhin vorteilhaft ist, dass die Software hinter den Bitcoins nach dem „open source“-Prinzip aufgebaut ist. Dadurch kann die Software von den Nutzern selbst ständig gewartet und weiterentwickelt werden. Daher können Systemupdates von der Community selbst entwickelt und an alle anderen Nutzer weitergeleitet werden ohne von einer zentralisierten dritten Partei autorisieren zu werden. Dabei können allerdings manchmal auch Probleme bei einigen Nutzern auftreten, die in Bugs oder allgemeinen Performance – Schwankungen resultieren.³³

Ein weiterer großer Vorteil für die Händler und Kunden ist die globale Verfügbarkeit von Bitcoins. Damit ist es den Händlern möglich ihre Produkte weltweit zu verkaufen und für Kunden diese weltweit zu erwerben. Damit schaffen virtuelle Währungen wie Bitcoin eine Harmonisierung des Marktes.³⁴

Allerdings besitzen Bitcoins wie jedes Zahlungsmittel gewisse Nachteile. Zunächst ergibt sich eine fehlende Transparenz durch das dezentrale Wesen der Bitcoins. Da die meisten Informationen über Bitcoins im Internet zu finden sind, kann es schnell vorkommen dass man durch Fehlinformationen falsche Entscheidungen trifft. Demnach können speziell neue Nutzer schnell betrogen werden durch falsche Investitionsmöglichkeiten oder dem Herunterladen und Installieren gehackter Clientsoftware mit Wallet.³⁵

³¹ Vgl. (Bank, February 2015) S.19

³² Vgl. (Bank, February 2015) S.19

³³ Vgl. (Bank, February 2015) S.20

³⁴ Vgl. (Bank, February 2015) S.19

³⁵ Vgl. (Bank, February 2015) S.20-21

Durch die Neuartigkeit der Bitcoins besteht ein allgemeiner unklarer Rechtstatus. Dem verbunden ist auch keine Regulierungsbehörde für Bitcoins zuständig. Nutzer von Bitcoins bei Kauf- und Dienstverträgen müssen beachten, dass sie keinen allgemeinen Verbraucherschutz haben. Des Weiteren besitzen Bitcoin-Nutzer auch keine Einlagensicherung.³⁶

Einer der größten Risiken für die Nutzer von Bitcoins ist das allgemeine Verlustrisiko durch Börsenpleite. Dies kann bei virtuellen Währungen wie Bitcoin schnell passieren, wenn etwa viele internationale Händler diese nicht akzeptieren oder die Investitionen der Unternehmer ausfallen wegen schlechter Prognosen. Am Ende können die Nutzer dadurch mit einem Haufen von Bitcoins enden die auf den Markt aber nun wertlos sind.³⁷

Ein weiteres allgemeines Problem von Kryptowährungen ist, dass sie von Betrügern leicht missbraucht werden könnten. Diese könnten mit etwas Fachwissen eine eigene Kryptowährung anfangen zu entwickeln um dann urplötzlich das Projekt verlassen. Die Nutzer die bereits in die neue Währung investiert haben, würden dann mit wertlosen Einheiten enden.³⁸

B. Rechtliche Einordnung von Bitcoins

I. Bitcoins als Geld

Bei der rechtlichen Einordnung von Bitcoins muss man zunächst fragen ob es sich bei Bitcoins um Geld handelt. Nach dem allgemeinen Geldbegriff handelt es sich bei Geld um jedes anerkannte Zahlungs- oder Tauschmittel. Daher können Bitcoins zunächst als Geld angesehen werden. Allerdings ist danach zu fragen um welche Art Geld es sich dabei handelt. Bitcoins sind zunächst einmal kein Naturalgeld(z.B. Muscheln, Edelsteine oder Tierprodukte) oder Gewichtsgeld wie z.B. Gold. Bei Bitcoins kann es sich auch nicht um Bargeld handeln, da sie außerhalb ihrer digitalen Präsenz im Internet keine physische Form durch anfassbare Münzen oder Banknoten besitzt. Bei Bitcoins handelt es sich auch nicht um Buchgeld oder E-Geld (z.B. PayPal-Geld). Denn beide Geldarten setzen voraus, dass dessen Inhaber eine Forderung auf Auszahlung in Bargeld hat. Diese Forderung wird beim E-Geld auch digital verzeichnet. Bitcoins sind in ihrem Wesen aber dezentral, wodurch sie nicht von einer dritten Partei ausgegeben werden

³⁶ Vgl. (Bank, February 2015) S.21

³⁷ Vgl. (Bank, February 2015) S.22

³⁸ Vgl. (Bank, February 2015) S.22

können und damit auch kein Forderungsanspruch entsteht. Letztendlich stellen Bitcoins eine neue Geldform dar. Sie werden aufgrund ihrer Entstehung und ihres Ursprungs auch als Kryptogeld oder digitales Geld bezeichnet.³⁹

II. Bitcoins als Währung

Von einer Währung spricht man wenn sie in einem Staat als offizielles Zahlungsmittel anerkannt ist. Allerdings wurden Bitcoins von keinem Land als Zahlungsmittel anerkannt, wodurch sie noch nicht als offizielle Währung gilt.⁴⁰

Bitcoins sind aber als eine Privatwährung (Komplementärwährung) anerkannt.⁴¹ Sie wurden von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) als Rechnungseinheiten gemäß § 1 Absatz 11 Satz 1 Kreditwesengesetz (KWG) rechtlich verbindlich eingeordnet. Damit fallen Bitcoins unter Werteinheiten, die eine Funktion von privaten Zahlungsmitteln bei Ringtauschgeschäften haben und dabei, wie jede andere Komplementärwährung, aufgrund von privatrechtlicher Vereinbarungen als Zahlungsmittel in multilateralen Verrechnungskreisen eingesetzt wird. Demzufolge kommt es auf einen zentralen Emittenten nicht an.⁴²

Dabei zählen Bitcoins nicht unter E-Geld gemäß des Zahlungsdienstleistungsaufsichtsgesetzes (ZAG) da es, wie bereits oben erwähnt, durch den fehlenden Emittenten kein Forderungsanspruch entsteht.⁴³

III. Mögliche zivilrechtliche Ausrichtung von Bitcoins

a) Bitcoin – Sache oder Recht

Bei einer zivilrechtlichen Einordnung muss man zunächst die Frage stellen, ob es sich bei Bitcoins um Sachen oder Rechte handeln könnte. Nach § 90 BGB können nur körperliche Gegenstände als Sachen bezeichnet werden. Bei Bitcoins gibt es keine körperliche Manifestation, wodurch sie nicht als Sachen gemäß § 90 BGB gelten.⁴⁴

³⁹ Vgl. (Schwenke, 2014)

⁴⁰ Vgl. (Schwenke, 2014)

⁴¹ Vgl. (Schwenke, 2014)

⁴² Vgl. (Münzer, 19.12.2013)

⁴³ Vgl. (Münzer, 19.12.2013)

⁴⁴ Vgl. (Schwenke, 2014)

Bei einem Recht erlangt man den Anspruch von jemandem ein Tun oder Lassen zu fordern. Dabei können Rechte vertraglich begründet werden, wie etwa bei Geldforderungen, oder sie werden vom Gesetzgeber als Immaterialgüterrechte festgelegt, wie zum Beispiel Urheberrechte oder Markenrechte.⁴⁵

Dazu ist zu sagen, dass es sich bei Bitcoin um kein Recht und auch nicht um ein gesetzliches Immaterialgüterrecht handelt, da Bitcoins keine Forderung gegenüber jemandem darstellt. Es ist natürlich möglich von jemandem einen Bitcoin erwerben, woraus eine Forderung entsteht. Aber diese Forderung ist dann durch einen Vertrag vereinbart worden und ergibt sich dementsprechend nicht aus dem Bitcoin selbst.⁴⁶

Demnach sind Bitcoins zivilrechtlich weder als Sachen oder Recht anzusehen.

b) Möglicher Vertragstyp beim Erwerb von Bitcoin

Entsprechend der Erkenntnisse des vorangegangenen Kapitels, muss man sich nun die Frage welche zivilrechtliche Vertragsform bei dem Erwerb von Bitcoins vorliegen kann.

Ein typischer Kaufvertrag nach § 433 BGB ist auszuschließen, da es nur möglich ist, das Eigentum an einer Sache zu erwerben. Bitcoins sind allerdings keine Sachen.⁴⁷

Ein Rechtskauf nach § 453 BGB ist dabei unter ähnlichen Gesichtspunkten auszuschließen, da Bitcoins auch keine Rechte sind.⁴⁸

Ein Tausch nach § 480 BGB könnte für den Erwerb von Bitcoin ebenfalls annehmbar sein. Dabei wird bei einem Tausch der Umsatz eines individuellen Wertes gegen einen anderen individuellen Wert gerichtet. Der Tausch zeichnet sich also dadurch aus, dass er zum Austausch zweier Werte führt, die keiner individueller, also konkretisierter Natur bedarfen, sondern auch Gattungsgegenstände sein können. Damit stellt sich aber die Frage, ob es sich bei Bitcoins um ein solches tauschfähiges Wirtschaftsgut handelt. Dabei kann man dieser Vermutung entgegenbringen, dass in der klassischen Terminologie mögliche Objekte des Tausches nur Sachen und Rechte seien. Durch die Erläuterung vom vorangegangenen Kapitel zählen Bitcoins nicht unter Sachen oder Rechten. Jedoch kam es beim Tausch nie durch eine rechtliche Kategorisierung dieses Umstandes, weder durch Wortlaut, noch durch eine historische, systematische oder teleologische Auslegung. Man könnte dementsprechend zum Tausch Wirtschaftsgüter

⁴⁵ Vgl. (Schwenke, 2014)

⁴⁶ Vgl. (Schwenke, 2014)

⁴⁷ Vgl. (Schwenke, 2014)

⁴⁸ Vgl. (Schwenke, 2014)

beliebiger Art einsetzen. Wenn man davon ausgeht, könnten Gegenstände eines Tauschvertrages Sachen, Rechte und Sachinbegriffe sein, aber gleichzeitig auch alle anderen vermögenswerten Positionen, sofern sie natürlich in einer von der Rechtsordnung gebilligten Weise übertragen werden können. Bitcoins können als ein solches Wirtschaftsgut angesehen werden, da sie als Daten unter eine vermögenswerte Position fallen. Dafür wäre die konkrete Rechtsnatur nicht relevant. Dem steht natürlich das eigentliche Wesen des Tausches entgegen, dass die vermögenswerten Positionen ohne Entgelt umgesetzt werden. Beim Erwerb von Bitcoin gegen Fiatgeld ist dies aber nicht der Fall, da dabei eine einseitige Geldleistung stattfindet.⁴⁹

Ein möglicher Vertragstyp für den Erwerb von Bitcoins stellt der Werkvertrag nach § 631 BGB dar. Bei einem Werkvertrag wird immer ein Erfolg geschuldet. Dieser Erfolg ist dabei immer das Ergebnis einer vorangegangenen Leistung, einem sogenannten Werk.⁵⁰ Bei Bitcoins wäre die zu erwartende Leistung der digitale Transfer von Daten die in eine gültige Transaktion resultieren. Demnach würde die Transaktion als der geschuldete Erfolg gelten. Diese Auslegung würde aber einen atypischen Werkvertrag beschreiben, da nicht um eine „schöpferische Leistung“ des Veräußerers ankommt, sondern um die einfache Übertragung eines vorbestehenden Gutes.⁵¹

Durch die noch rechtliche unklare Definition von Bitcoin ist es nicht möglich einen spezifischen Vertragstyp für deren Erwerb zu finden. Nach meinem eigenen Verständnis würde ein atypischer Werkvertrag für den Erwerb von Bitcoin in Frage kommen.

IV. Strafrechtliche Aspekte von Bitcoin

Durch die unklare Rechtsnatur von Bitcoin könnte eine Problematik bei der Strafverfolgung auftreten. Da Bitcoins keine Sachen nach § 90 BGB sind, kann es bei ihrer Wegnahme sich auch nicht um einen Diebstahl nach § 242 StGB handeln, da es das Entwenden einer Sache erfordert.⁵²

Jedoch sind Bitcoins eine Ansammlung von Daten die mit einer entsprechenden Sicherung in Form von Schlüsseln versehen sind. Wenn man verschlüsselte Daten von einem fremden Computer einsieht, verändert oder entwendet kann sich verschiedener Datendelikte nach dem StGB strafbar machen. Mögliche Deliktstatbestände die beim

⁴⁹ Vgl. (Schroeder, 2014) Abs. 48

⁵⁰ Vgl. (Schwenke, 2014)

⁵¹ Vgl. (Schwenke, 2014) Abs. 46

⁵² Vgl. (Schwenke, 2014)

Zugriff auf fremde Bitcoins erfüllt werden könnten sind das Ausspähen von Daten nach § 202a StGB, das Abfangen von Daten nach § 202b StGB, der Datenveränderung nach § 303a StGB und der Computersabotage gemäß §303a StGB.⁵³

Sollte ein Täter zusätzlich noch auf die Datenverarbeitungsvorgänge Einfluss nehmen um somit etwa eine Handelsplattform dazu zu bringen Bitcoins an die falsche Adresse zu senden, macht er sich zudem des Computerbetruges nach § 263a StGB strafbar.⁵⁴

V. Der Handel mit Bitcoin

Bitcoins können zum Ausgleich von schuldrechtlichen Verträgen verwendet werden, wenn sich die Parteien darauf einigen. Jedoch kann der gewerbliche Umgang mit Bitcoins eine Erlaubnispflicht nach dem Kreditwesengesetz(KWG) auslösen. Wenn diese Erlaubnis fehlt, kann es zu einer Erfüllung des Straftatsbestandes von § 54 KWG kommen.⁵⁵

Dabei ist zu beachten, dass der Kauf und Verkauf von Bitcoins nicht zulassungspflichtig ist. Genauso ist das Minen von Bitcoins nicht zulassungspflichtig. Wird das Mining aber gewerblich vertrieben, so kann durch die Vergabe von Schürfrechte in Miningpools eine Zulassungspflicht, gemäß § 1 Absatz 1a Nr. 4 KWG für den erlaubnispflichtigen Eigenhandel, entstehen.⁵⁶

Zulassungspflichtig sind dabei alle Dienstleistungen, die zur Vermarktung von Bitcoins benutzt werden oder den Bitcoin selbst zur Ware haben. Das schließt den Börsenbetrieb, Kommissionsgeschäfte und die Finanzberatung ein. Somit ergibt sich für ein Finanzkommissionsgeschäft ein Erlaubnistatbestand nach § 1 Absatz 1 Satz 2 Nr. 4 KWG. Für das multilaterale Handelssystem, die Anlage- und Abschlussvermittlung und den Eigenhandel ergibt sich daraus ebenfalls ein Erlaubnistatbestand(§ 1 Absatz 1 Satz 2 Nr.1-4 KWG).⁵⁷

⁵³ Vgl. (Schwenke, 2014)

⁵⁴ Vgl. (Schwenke, 2014)

⁵⁵ Vgl. (Münzer, 19.12.2013)

⁵⁶ Vgl. (Schwenke, 2014)

⁵⁷ Vgl. (Münzer, 19.12.2013)

a) Bitcoin bei Finanzkommissionsgeschäfte

Wer im eigenen Namen auf fremde Rechnung gewerbsmäßig Bitcoins an- und verkauft, betreibt damit ein erlaubnispflichtiges Finanzkommissionsgeschäft. Dabei gilt die Veräußerung oder Anschaffung von Bitcoins auf fremde Rechnung ab dem Moment, in dem die wirtschaftlichen Vor- und Nachteile aus dem Geschäft den Auftraggeber treffen. Zusätzlich muss die besagte wirtschaftliche Tätigkeit dem Kommissionsgeschäft entsprechend dem Handelsgesetzbuch hinreichend ähnlich sein. Dabei können einzelne Rechte und Pflichten vom typischen Kommissionsgeschäft abweichen. Ein erlaubnispflichtiges Finanzkommissionsgeschäft bei Bitcoin-Plattformen liegt demnach vor, wenn:⁵⁸

- „- die einzelnen Teilnehmer den Plattformen gegenüber bis zur Ausführung der Order weisungsbefugt sind, indem sie die Zahl und den Preis der Geschäfte vorgeben,
- den jeweiligen Teilnehmern ihre Handelspartner nicht bekannt sind und die BTC-Plattform nicht als Vertreter der Teilnehmer, sondern im eigenen Namen auftritt,
- die wirtschaftlichen Vor- und Nachteile der Geschäfte die Teilnehmer treffen, die Geld auf Plattform-Konten überweisen oder BTC auf deren Adressen übertragen, und
- die BTC-Plattform verpflichtet ist, den Teilnehmern über die Ausführung der Geschäfte Rechenschaft abzulegen und angeschaffte BTC zu übertragen.“⁵⁹

b) Bitcoin in multilateralen Handelssystemen

Wenn es bei der wirtschaftlichen Tätigkeit bei den Bitcoin-Handelsplattformen kein Finanzkommissionsgeschäft vorliegt, so handelt es mit größter Wahrscheinlichkeit um den Betrieb eines multilateralen Handelssystems. Bei einem multilateralen Handelssystem bringt man die Interessen von einer Vielzahl von Personen am Kauf und Verkauf von Finanzinstrumenten in einem System zusammen. Das System funktioniert dabei nach festgelegten Bestimmungen und in einer Art und Weise, dass zum Vertrag über diese Finanzinstrumente entstehen kann.⁶⁰

Bei Bitcoin-Plattformen muss dafür zunächst ein Regelwerk über die Mitgliedschaft, den Handel zwischen den Mitgliedern und entsprechende Meldungen über abgeschlossene Geschäfte vorliegen. Eine konkrete Handelsplattform ist dabei zwar nicht erforderlich, meistens aber der Fall. Der Begriff Multilateral bedeutet in diesem

⁵⁸ Vgl. (Münzer, 19.12.2013)

⁵⁹ (Münzer, 19.12.2013)

⁶⁰ Vgl. (Münzer, 19.12.2013)

Zusammenhang, dass der Betreiber nur Parteien eines potenziellen Geschäfts über Bitcoin zusammenführt. Interesse am Kauf sowie Verkauf suggeriert man dabei durch Interessensbekundungen, Aufträge und Kursofferten. Zusätzlich muss eine Annahme des Geschäfts über das System möglich sein. Es ist dabei jedoch nicht von Belang, ob die eigentliche Abwicklung des Vertrages außerhalb des Systems stattfindet.⁶¹

Nach der Sicht der BaFin sind Handelsplattformen, in denen die Anbieter Bitcoins mit einer Preisschwelle einstellen, mit dem Ziel einen Kauf zustande kommen zu lassen, ebenfalls ein multilaterales Handelssystem. Gleiches kann gilt dafür, wenn die Anbieter eine Transaktion durch Hinterlegung von Bitcoin bei dem Plattformbetreiber absichern kann. Sollte ein Plattformbetreiber so etwas erlauben, so benötigt er eine Zulassung als Finanzdienstleistungsinstitut entsprechend dem KWG.⁶²

c) Bitcoin bei der Vermittlung und dem Eigenhandel

Die BaFin bezieht damit vor allem an die Bitcoin-Wechselstuben. Diese handeln im eigenen Namen und damit auf eigene Rechnung. Dementsprechend ist es somit möglich, dass sie den Tatbestand des Eigenhandels erfüllen und somit eine Zulassung als Finanzdienstleistungsinstitut nach dem KWG benötigen. Außerdem muss es sich noch um eine gewerbliche Tätigkeit oder einer Tätigkeit größeren Ausmaßes handeln. Üblicherweise gab es eine dafür eine Bagatellschwelle von 25 Geschäften, jedoch nimmt die BaFin für jedes Geschäft nun eine Einzelbetrachtung vor.⁶³

d) Die Steuerpflicht bei Bitcoin

Auch wenn Bitcoins keine feste rechtliche Definition besitzen, so stellen sie dennoch werthaltige Güter dar. Dementsprechend kann an deren Entstehung oder deren Handel eine Steuerpflicht geknüpft sein.⁶⁴

Dabei ist zunächst zu sagen, dass das reine Halten von Bitcoin nicht steuerpflichtig ist. Da es in Deutschland keine Vermögenssteuer gibt kann auch nie der reine Vermögensbestand von Bitcoin selbst versteuert werden.⁶⁵

Beim Handel mit Bitcoin kann eine Steuerpflicht mit Bitcoin auftreten, wenn sich diese im Betriebsvermögen befinden, sprich durch ein Unternehmen erworben werden. Durch die Differenz zwischen dem Anschaffungs- und Veräußerungspreises entsteht dabei

⁶¹ Vgl. (Münzer, 19.12.2013)

⁶² Vgl. (Terlau, 2014)

⁶³ Vgl. (Terlau, 2014)

⁶⁴ Vgl. (Schwenke, 2014)

⁶⁵ Vgl. (Schwenke, 2014)

nach wie vor ein steuerpflichtiger Betriebsgewinn. Befinden sich Bitcoin allerdings im Privatvermögen, so zählen die Gewinne aus Bitcoin zu den sog. Spekulationsgeschäften welche der Einkommenssteuer gemäß §§ 22 Nr. 2, 23 EStG unterliegen. Voraussetzung dafür ist, dass die Bitcoin innerhalb eines Jahres erworben und wieder veräußert werden und die Gewinne aus diesen Spekulationsgeschäften im Jahr weniger als 600 EUR betragen. Werden die Bitcoin aber länger als ein Jahr gehalten, so ist der Gewinn steuerfrei.⁶⁶

VI. Mehrwertsteuerpflicht beim Tausch zwischen konventionellen Währungen und Bitcoin

Der Europäische Gerichtshof hat am 22.10.2015 zu diesem Sachverhalt ein Urteil erlassen. Nach dem Beschluss des EuGH fällt beim Umtausch von einer herkömmlichen Währung zu Bitcoin und umgekehrt keine Mehrwertsteuer an.

a) Sachverhalt

Der Beklagte David Hedqvist ist angehender Unternehmer. Seine Geschäftsidee ist die Erstellung einer Website, die den Tausch zwischen herkömmlicher Währung und Bitcoin ermöglicht. Da er sich nicht sicher war ob für den bloßen Umtausch mit Bitcoin eine Mehrwertsteuerpflicht anfällt, beantragte er bei dem Steuerrechtsausschuss einen Vorbescheid. Unter Vorlage des Urteils der First National Bank of Chicago (C-172/96, ECLI:EU:C:1998:354) wurde angenommen, der Beklagte bietet eine Umtauschdienstleistung gegen Entgelt an. Dabei ist der Beklagte der Meinung, dass eine solche Umtauschdienstleistung gemäß Kap. 3 §9 MWSTG unter einer Steuerbefreiung fällt. Die schwedische Steuerverwaltung (Kläger) hat gegen den Bescheid des Steuerrechtsausschusses beim obersten Verwaltungsgericht von Schweden Klage erhoben. Die Beklagte vertritt dabei die Meinung, dass die Umtauschleistung nicht unter einer Steuerbefreiung gemäß Kap. 3 §9 MWSTG fällt.⁶⁷

Das oberste Verwaltungsgericht war der Ansicht, dass das Urteil der First National Bank of Chicago anwendbar ist. Bei dieser Annahme stellte sich damit aber die Frage, ob sie unter einer der Art. 135 Abs. 1 der MwSt-RL Finanzdienstleistung fällt, die eine unter einer Steuerbefreiung fällt.⁶⁸

⁶⁶ Vgl. (Schwenke, 2014)

⁶⁷ Vgl. EuGH, 22.10.2015, C-264/14, Sachverhalt

⁶⁸ Vgl. EuGH, 22.10.2015, C-264/14, Sachverhalt

b) Die Entscheidung und Entscheidungsgründe des EuGH sowie dessen Bedeutung für den Bitcoin

Der EuGH bestätigt die Vermutung des Obersten Verwaltungsgerichts und entschied letztendlich, dass beim Umtausch mit Bitcoin gem. Art. 135 Abs. 1 MwSt-RL keine Umsatzsteuer anfällt.⁶⁹

In dem Verfahren war auch die deutsche Bundesregierung mit vertreten und argumentierte gegen die letztendliche Entscheidung des EuGH's. Nach der Argumentation der deutschen Regierung sei die nach der MwSt-RL und deren deutschen Umsetzung in § 4 Nr. 8 b) UStG eine Mehrwertsteuerbefreiung nur bei ausschließlich gesetzlichen Zahlungsmitteln besteht. Der Bitcoin war zu diesem Moment noch nirgendwo auf der Welt als gesetzliches Zahlungsmittel anerkannt und war nach Ansicht der Bundesregierung betrugsanfällig, unsicher und im allgemeinen ein Werkzeug der organisierten Kriminalität.⁷⁰

Die wörtliche Auslegung des deutschen Wortlauts von Art. 135 Abs. 1 MwSt-RL war zunächst korrekt. Allerdings tauchte das Wort „gesetzlich“ in den anderen Sprachfassungen der MwSt-RL nicht auf. So ist etwa in der englischen Fassung nur die Rede von „currency, bank notes and coins“. Jedoch sind alle Amtssprachen der EU maßgeblich. Da die Umsatzsteuer aber europaweit verbindlich gelten muss, kann auch nur eine einzige verbindliche Auslegung der Richtlinie geben.⁷¹

Da die wörtliche Auslegung widersprüchlich ist, ging der EuGH über auf die teleologische Auslegung der Richtlinie, also dem ursprünglichem Sinn und Zweck der Umsatzsteuerbefreiung.⁷²

Zunächst einmal soll die Konvertierbarkeit reiner Zahlungsmittel nicht durch eine Mehrwertsteuer bzw. Umsatzsteuer zu verteuern werden wodurch es zu Behinderungen im Zahlungsverkehr kommen kann. Außerdem sollen Schwierigkeiten bei der Ermittlung der steuerlichen Bemessungsgrundlage und der abzugsfähigen Umsatzsteuer vermieden werden. Deshalb werden nach Art. 135 Abs. 1 MwSt-RL sämtliche weltweiten Währungen erfasst und nicht nur die der europäischen Union.⁷³

⁶⁹ Vgl. EuGH, 22.10.2015, C-264/14, Rnd 22 - 57

⁷⁰ Vgl. (Klein, 2015) S. 1

⁷¹ Vgl. (Klein, 2015) S.1

⁷² Vgl. (Klein, 2015) S.1

⁷³ Vgl. (Klein, 2015) S.1

Wenn ein Medium in seiner Funktionsweise nur als reines Zahlungsmittel genutzt werden kann, so ist nach gemäß der steuerlichen Neutralität und Gleichbehandlung die Umsatzsteuerbefreiung zulässig. Nach der Ansicht des EuGH's ist diese ausschließlich reine Zahlungsfunktion bei den Bitcoin vorhanden. Andere "Tauschmedien" wie Zigaretten oder Gold besitzen einen über die bloße Zahlungswirkung hinausgehenden "eigenen" Wert und unterliegen damit nicht der Umsatzsteuer.⁷⁴

Nach der Entscheidung des EuGH wird der Bitcoin somit steuerrechtlich wie jedes andere herkömmliche Zahlungsmittel behandelt. Damit wird die Kryptowährung den gesetzlichen Zahlungsmitteln gegenüber teilweise gleichgestellt. Dieses Urteil ist somit für die Akzeptanz der Bitcoins im wirtschaftlichen Verkehr ein großer Meilenstein.

D. Der Bitcoin im wirtschaftlichen Geschäftsleben

I. Kursentwicklung

Seit der Einführung von Bitcoins im Jahre 2009 haben sie eine stetig wachsende Entwicklung erlebt. Zum Beginn verhielt sich der Wert von 1 Bitcoin zu 0.00076 Dollar. Im Juni 2010 belief sich nach der Online-Exchange Plattform der Wert eines Bitcoins bereits auf 0.07 Dollar. Dadurch konnten Bitcoins innerhalb eines Jahres bereits eine Wertsteigerung von über 9000% verzeichnen. Dieser Trend hielt über das Jahr 2011 weiterhin an. Zu Beginn des Jahres stieg der Preis eines Bitcoins bereits auf über 1 Dollar. Im Juni 2011 stieg der Wert dann weiter auf 20 Dollar pro Bitcoin. Allerdings sollte dieser rasche Aufstieg zum Erliegen kommen. Denn im selben Monat wurde der bisher größte Hackerangriff auf Bitcoin gestartet. Dies bewirkte dass der Kurs für eine sehr lange Zeit unterhalb der 10 Dollar Grenze verweilte. Die Anleger wurden daraufhin zunehmend unsicherer. Bis zum Frühjahr 2012 waren keine weiteren gravierenden Kursschwankungen aufgetreten und es stand nicht gut um die Entwicklung der Bitcoins. Dies änderte sich aber dann durch eine Bürgschaft in das Bankensystem auf Zypern. Diese Maßnahme sorgte bei den Einheimischen natürlich für Unsicherheit. Es bestand die Angst, ihre Sparanlagen auf ihre Banknoten zu verlieren. Sie versuchten daher einen Teil mithilfe von Bitcoins zu retten. Demzufolge resultierte einen enormer Kursanstieg. Spekulative Anleger sahen ihre Chance und schossen den Preis somit noch mehr in die Höhe. Danach brach der Preis der Bitcoins durch die Überlastung der Onlinebörse Mt. Gox erneut ein. Allerdings war dies nur von kurzer

⁷⁴ Vgl. (Klein, 2015) S.1

Dauer. Einer der größten Kursanstiege in der Geschichte der Bitcoins fand am gegen Ende 2013 statt. Zu diesem Zeitpunkt beriet der US-Senat über das Thema Bitcoin. Dabei waren viele Reporter von verschiedenen Medienportalen anwesend. Es folgte eine medienweite Diskussion über die Bitcoins. Daraufhin entschieden sich viele chinesische Spekulanten in diesen Markt zu investieren. Die Chinesen halten bis zum heutigen Tag einen großen Marktanteil der Bitcoins inne. Der Zuwachs der chinesischen Investoren bewirkte Anfang 2014 einen Wertanstieg von 1.242 Dollar pro Bitcoin auf der Mt.Gox. In den darauffolgenden Monaten kam ein Abwärtstrend zustande der bis Mitte 2015 anhielt.⁷⁵

Der Kurs erholte sich danach wieder und steigt bis zum heutigen Tag kontinuierlich an. Besonders 2017 machte der Bitcoin-Kurs einen großen Sprung nach oben. Ein wichtiger Faktor dafür war die Akzeptanz von Bitcoin als offizielles Zahlungsmittel in Japan am 01.04.2017. Zusätzlich versuchen die Zwillinge Cameron und Tyler Winklevoss erneut einen Bitcoin-Fonds zu bewilligen. Die US-Börsenaufsicht SEC hatte den bisherigen Antrag abgewiesen. Allerdings prüft momentan der Börsenbetreiber Bats diesen Antrag erneut. Allein die Möglichkeit, dass es zu dem Bitcoin-Fond „Winklevoss Bitcoin Trust ETF“ kommen könnte, bewirkt ein rapiden Anstieg des Kurses. Selbst durch die derzeitigen Hackerangriffe auf mehrere Unternehmen scheint der Bitcoin-Kurs auch weiterhin beständig nach oben zu steigen.⁷⁶



Abbildung 4: Wechselkurs von Bitcoin

⁷⁵ Vgl. (Sander, 2016) S. 72-73

⁷⁶ Vgl. (Neuhaus, 2017)

II. Risiken von Bitcoin

a) Die 51% Attacke

Dabei handelt es sich um das wahrscheinlich größte technische Risiko welches im System von Bitcoins vorhanden ist. Im Normalfall werden alle Transaktionen von Minern verifiziert und geprüft. Es ist für Hacker oder Betrüger damit eigentlich unmöglich Bitcoins zu verdoppeln oder zu fälschen, da diese Transaktionen von Minern verworfen werden. Erlangt aber jetzt eine Person oder Gruppierung über 50% der Rechenkapazität des Systems wird es problematisch. Sie hätten damit die Kontrolle über das ganze System. Es wäre ihnen damit möglich selbst zu bestimmen welche Transaktionen verworfen oder bestätigt werden. Zusätzlich wäre es ihnen möglich Transaktionen rückgängig zu machen oder Bitcoins doppelt auszugeben.⁷⁷

Um Bitcoins doppelt ausgeben muss man es mit dem Großteil der Rechenkapazität des Systems schaffen seine zweite Transaktion vor der ersten zu bestätigen. Damit man das erreicht muss man die erste Transaktion ohne Gebühren versehen und die zweite Transaktion mit. Das System wird dadurch die zweite Transaktion als gültig ansehen und die erste als ungültig, da die Bitcoins mit der Bestätigung von Transaktion 2 bereits als ausgegeben gelten. Unter dieser Masche ist nun folgendes Szenario möglich: Der Betrüger kauft eine Sache von einem Händler mit Bitcoins. Mit seiner 1. Transaktion bezahlt er diese Sache beim Händler. Gleichzeitig übersendet er mit einer 2. Transaktion Bitcoins auf einer seiner Adressen. Da aber nur die 2. Transaktion vom System anerkannt wird, erhält nur der Betrüger seine Bitcoins auf eine seiner eigenen Adressen, während der Händler zwar denkt das er das Geld erhalten hätte, jedoch leer ausgeht.⁷⁸

Die Wahrscheinlichkeit dass eine einzige Person so viel Rechenkapazität besitzt ist allerdings unwahrscheinlich, da die Hardwarekosten astronomisch hoch wären. Es wäre wahrscheinlicher dass ein Pool von Minern es schafft die 50% Grenze zu knacken.⁷⁹

⁷⁷ Vgl. (Strutzenberger, 2016) S.20

⁷⁸ Vgl. (Strutzenberger, 2016) S.20

⁷⁹ Vgl. (Strutzenberger, 2016) S.20

b) Die DDoS- Attacke

Bei der DDoS- Attacke (Distributed-Denail-of-Service) handelt es sich um eine Erpressungsmasche. Dabei werden vor allem Onlinehändler als Opfer solcher Angriffe. Zunächst erhält das Opfer eine E-Mail von den Erpressern, dass er einen gewissen Betrag Bitcoins an eine bestimmte Adresse zu senden. Wenn das Opfer nicht kooperiert, wird der tatsächliche DDoS Angriff gestartet. Es werden enorm große Datenpakete von Anfragen auf die Server des Opfers geladen. Dadurch wird der Server überlastet und kompromittiert. Es ist den Angreifern nun möglich in das Netzwerksystem des Opfers einzudringen und somit die Daten des Opfers auszuspionieren oder zu manipulieren. Es ist sehr schwer sich gegen diese Angriffe zu verteidigen, da die Website des Onlinehändlers es nur für einen Besucheransturm hält.⁸⁰

Diese Art von Angriffen sind im Internet bereits seit vielen Jahren bekannt und wurden auch bereits vor der Einführung von Bitcoins durchgeführt. Allerdings kommen treten sie seit Frühling 2017 immer häufiger bei Online Händlern auf, die Bitcoins akzeptieren. Die Täter wählen genau diese Plattformen aus, da es durch Vorteile die Bitcoins mit sich bringen (z.B. Anonymität und schneller Geldtransfer) eine höhere Erfolgchance garantiert.

c) Silk Road

Bei der Silk Road handelt es sich um eine digitale Schwarzmarktverkaufsplattform. Auf dieser Seite werden mehrere illegale Produkte verkauft. Das Angebot reicht dabei von Waffen und Drogen bis hin zu gestohlenen Identitäten. Zusätzlich sind auf der Seite auch Auftragsmorde ausgeschrieben. Dieser Online-Schwarzmarkt nutzt dabei als einziges Zahlungsmittel Bitcoin. Der Grund dafür ist der Anonymitätsvorteil der Nutzer. Damit ist es keiner Regierung möglich, die Käufer und Verkäufer zurückzuverfolgen.⁸¹

⁸⁰ Vgl. (Sander, 2016) S. 25

⁸¹ Vgl. (Graff, 2016)

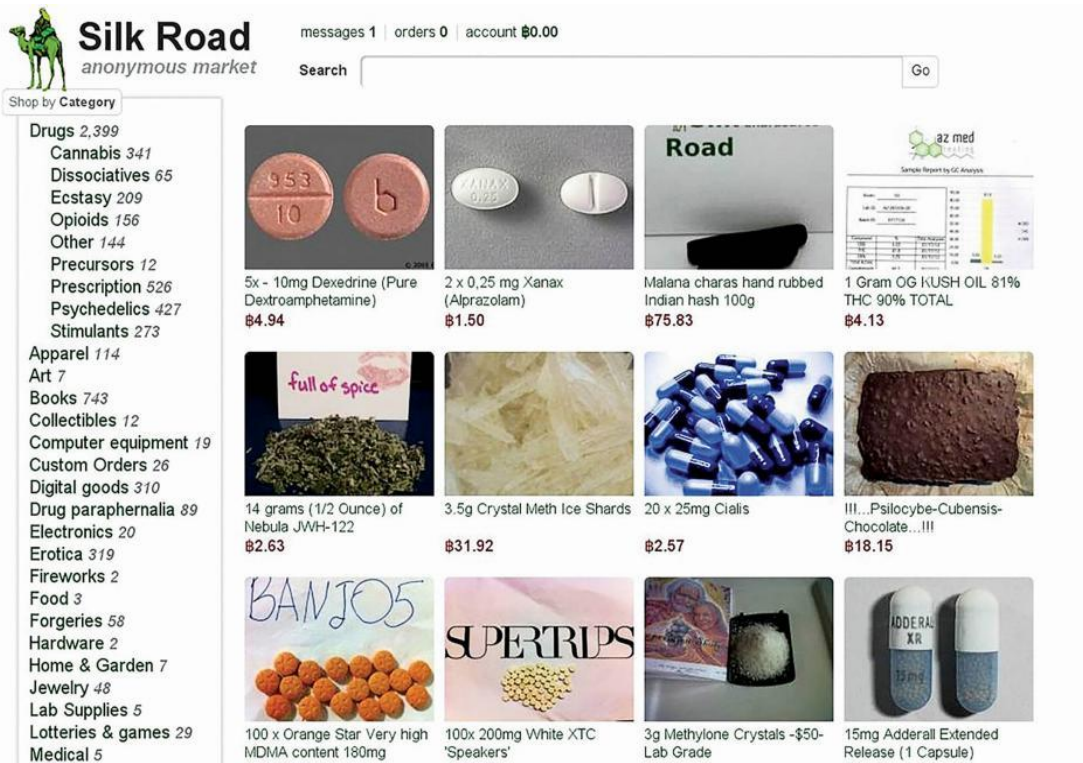


Abbildung 5: Schwarzmarktwebsite „Silk Road“

Die Aufmachung der Website ähnelt dabei anderen Verkaufsplattformen wie etwa Amazon oder Ebay. Es sogar möglich Produktbewertungen in Form von Sternen und Erfahrungsberichte abzugeben.

Als die Website das erste Mal 2011 in Erscheinung trat arbeiteten der FBI und die CIA auf Hochtouren um die Website zu entfernen und die Verantwortlichen festzunehmen. Sie nutzten dazu Cyber-Attacken wie etwa eingeschleuste Trojaner und Rechner-Attacken, welche normalerweise als kriminell angesehen werden. Der Gründer von Silk Road war im Dark-Net bekannt als „Dread Pirate Roberts“. Im Oktober 2013 nahm das FBI den US- Amerikaner Ross Ulbricht fest, dessen Vorstrafen von Handel mit Waffen und Drogen, Computereinbruch bis hin zur Geldwäsche reichte. Dem FBI gelang es nach der Festnahme von Ulrich auch die Entfernung der Website. Ulrich selbst behauptete dass er nicht „Dread Pirate Roberts“ sei und dass es sich dabei um eine ganze Gruppe handelt, die sich gegen die Regierung auflehnt. Kurze Zeit nach dem Verschwinden von Silk Road tauchte im Netz die Plattform Silk Road 2.0 auf.⁸²

Bis heute kamen tauchten wieder neue Varianten der Silk Road im Netz auf, kurz nachdem die alten Versionen vom FBI oder CIA entfernt wurden. Leider zeigt dieses Beispiel warum Bitcoins ihren schlechten Ruf als eine Währung für Kriminelle haben. Die Vorteile von Bitcoin geben den Verbrechern ein unglaublich sicheres und schnelles

⁸² Vgl. (Graff, 2016)

Zahlungssystem ohne direkten Kontakt. Natürlich gab es auch schon vorher Verkaufsplattformen mit illegalen Produkten wie Drogen und Waffen. Jedoch wird mit Bitcoin die Geldwäsche immens erleichtert, wodurch es für die Regierungen weniger Möglichkeiten gibt die tatsächlichen Handelspartner ausfindig zu machen.

d) Kriminelle Programmentwicklung

Programmierer entwickeln die Systeme von Bitcoin immer weiter. Obwohl die meisten Verbesserungen im guten Glauben getätigt werden, so kann es jedoch vorkommen, dass sie für kriminelle Aktionen missbraucht werden. Der Informatiker Ari Juels von der Cornell University warnt vor der Erscheinung von kriminellen „smart contracts“. Diese Programme könnten dann etwa eine Belohnung für die Ermordung bestimmter Politiker oder anderer Personen aussetzen. Die Konzept würde wie folgt funktionieren: Der Programmierer stockt sein Programm mit Bitcoin auf. Danach legt er seine Bedingungen fest, z.B. an welchem Datum der Auftragsmord geschehen soll. Dann wartet er die gesetzte Frist ab. Führt ein Mörder den Auftrag aus, kann er das Programm wie eine normale Internetadresse aufrufen und seine Belohnung geltend machen. Ein Treffen von Auftraggeber und Auftragsmörder ist dabei nicht notwendig. Das Programm übernimmt die komplette Abwicklung des Verbrechens. Da der verbrecherische Code auf keinem Server gespeichert ist, sondern nur dezentral auf der Blockchain gespeichert wird, kann es nicht gestoppt werden.⁸³

e) Verlustrisiko

Wie es bereits unter dem Kapitel „Vor- und Nachteile von Kryptowährungen“ erwähnt wurde, besteht bei Bitcoins ein allgemeines Verlustrisiko durch Börsenpleite. Allerdings gibt es noch andere Umstände die zu einem großen Verlustrisiko von Bitcoins führen können. Zunächst muss man bei Bitcoins beachten, dass sie dezentral sind, wodurch die Nutzer gezwungen sind selbst verantwortlich zu handeln. Demnach besteht für den Nutzer das Problem, dass niemand die Haftung übernimmt bei Verlust oder Diebstahl. Dabei stellen mögliche Verlustgründe Hardwaredefekte, das Verlieren oder das Vergessen des privaten Schlüssels oder schädliche Umwelteinflüsse auf das Speichermedium wie Nässe dar. Zusätzlich kann es passieren, dass das Speichermedium des Nutzers gehackt oder ausspioniert wird, wodurch man Gefahr läuft Geld zu verlieren. Bei dieser Art von Hack müsste der Angreifer nur Zugriff auf die Daten des Speichermediums gelangen. Dies kann für einen Hacker mitunter bedeutend leichter

⁸³ Vgl. (Behrens, 2017) S.3

sein, als sich in das System von Bitcoin zu hacken. Zusätzlich kann es auch vorkommen, dass Hacker die Daten der Kundenkonten von Handelsplattformen, wie etwa durch die im vorherigen Kapitel beschriebenen DDoS – Attacke. Daher sollte man als Nutzer von Bitcoins darauf achten, dass sein Guthaben auf solchen Plattformen nur für die Dauer eines Kaufes und Verkaufes gespeichert bleibt.⁸⁴

f) Verbotsrisiko

Die Neuartigkeit von Bitcoin verschreckt viele Länder. Dadurch kann es passieren, dass in manchen Staaten vielleicht ein Verbot für Bitcoins ausgesprochen werden kann. Es könnte damit zwar nur sehr schwer kontrolliert werden, ob jemand tatsächlich Bitcoins auf seinem PC speichert aber es könnte dennoch gut möglich sein dein Handel mit ihnen zu verbieten. Im ersten Moment würde dies den Anlegern zunächst nicht schaden. Allerdings wurde über Zeit der Preis sinken, da es seine Funktion als Geld verloren hätte. Mögliche Gründe für ein Verbot wären dabei die Angst vor dem illegalen und anonymen Einkauf von Waffen und Drogen oder der mögliche Machtverlust der eigenen staatlichen Währung. Länder wie Ecuador und Bolivien verbieten bereits den Besitz von Bitcoins, da sie versuchen eine eigene digitale Währung einzuführen. In Russland ist der Besitz von Bitcoin ebenfalls untersagt, da dort der Rubel als einzige legale Währung zählt. In diesen Ländern war der Bitcoin aber auch von Beginn an nicht sehr verbreitet, wodurch auch ein großer Nachfrageeinbruch zu verzeichnen war. Sollten allerdings Länder wie die USA, Großbritannien oder Deutschland ein Verbot aussprechen, könnte dies einen vernichtenden Schlag für die Bitcoins bedeuten und damit auch einen herben Verlust für dessen Anleger bedeuten.⁸⁵

g) Nischenrisiko

Nachdem die Bitcoins erschienen waren, traten mit der Zeit auch leicht veränderte digitale Währungen auf der Bildfläche auf. Denn das Open-Source-Prinzip erlaubt die Softwarecodes zu kopieren und leicht zu verändern. Die erste, auf diese Weise erschaffene, alternative Währung hieß Litecoin. Mittlerweile gibt es zirka 600 alternative digitale Währungen, welche man allgemein unter den Begriff Altcoins zusammenfasst. All das birgt die Gefahr einer Nischenbildung. Damit könnte es passieren, dass sich für jede digitale Währung ein eigener kleiner Nutzerkreis bildet.

⁸⁴ Vgl. (Strutzenberger, 2016) S. 20-21

⁸⁵ Vgl. (Schwenke, 2014) S. 21

Das würde eine schnelle Verbreitung verhindern und eine globale Akzeptanz deutlich erschweren.⁸⁶

h) Kontrollrisiko

Das Open Source Prinzip gekoppelt mit dezentralem Wesen von Bitcoin macht Kontrollen unmöglich. Das momentane Entwicklerteam von Bitcoin hat nach dem Rücktritt von Satoshi Nakamoto weiter an der Verbesserung des Systems gearbeitet und bereits diverse Sicherheitslücken behoben. Jedoch gibt es nie die vollkommene Gewissheit, dass eben diese Entwickler sich irgendwann entgegen den Willen der Nutzer handeln oder Bitcoin aus eigenem Interesse manipulieren.⁸⁷

i) Spekulationsrisiko

Bitcoins besitzen eine enorm hohe Volatilität. Das bedeutet sie haben extrem schwankende Wechselkurse. Das ist auch der Grund warum es für Gewerbetreibende nur sehr ist in Bitcoins zu vertrauen und zu akzeptieren. Auch wenn momentan ein deutlicher Aufwärtstrend zu verzeichnen ist, gab es in der Vergangenheit regelmäßig Kurseinbrüche und Phasen, in denen der Bitcoinpreis langsam und stetig fiel. Dabei können Gewerbetreibende, welche es sich leisten können Bitcoins über längere Zeit halten, den deflationären Effekt von Bitcoins nutzen um einen Anstieg der Kaufkraft bei seinem eingenommenen Geld zu erreichen. Damit befindet man sich jedoch im absoluten Spekulationsrisiko und ist für die meisten Unternehmer kein wünschenswerter Geschäftsvorgang. Wenn ein Geschäft zum Beispiel 2,50 EUR für ein Bier berechnet, dann hat es diesen Wert dafür vorher kalkuliert um eine optimale Geschäftsführung zu gewährleisten. Das Bier dürfte dabei nicht für einen Tag plötzlich 2,00 EUR kosten und im nächsten Monat dann wieder auf einen Preis von 3,00 EUR steigen. Dies sorgt nicht nur bei einer Verwirrung bei den Kunden sondern macht es für das Geschäft unmöglich exakt zu kalkulieren.⁸⁸

Es kann nicht davon ausgegangen werden, dass Bitcoins in absehbarer Zeit diese Volatilität überwinden wird. Der Grund dafür ist, dass Bitcoins sich noch immer in der Preisfindungsphase befinden. Den meisten Menschen, für die Bitcoin als Zahlungsmittel in Frage kommt, haben davon noch nicht einmal etwas gehört. Erst ab dem Moment wo all diese Menschen sich über deren Existenz bewusst werden und sich dann für oder

⁸⁶ Vgl. (Strutzenberger, 2016) S.22

⁸⁷ Vgl. (Strutzenberger, 2016) S.22

⁸⁸ Vgl. (Platzer, 2014) S.108

gegen deren Gebrauch entscheiden, kann für den Markt möglich sein einen relativen stabilen Preis für einen Bitcoin zu finden.⁸⁹

j) Deflationsrisiko

Bitcoins sind auf eine Stückzahl von 21 Millionen begrenzt. Somit ist es nicht möglich, dass es zu einer Inflation kommt. Eine Deflation ist aber durchaus möglich. Nach den derzeitigen Berechnungen ist davon auszugehen, dass der Großteil der Bitcoins im Jahr 2040 erzeugt sein wird. Etwa ein Jahrhundert später wird im Jahr 2140 wahrscheinlich der letzte Bitcoin gefunden. Diese Stückzahl von 21 Millionen kann nicht angehoben werden. Allerdings ist dennoch eine ausreichende Menge vorhanden, da Bitcoins bis auf die achte Kommastelle teilbar sind. Damit wird es im Jahr 2140 insgesamt 2.100.000.000.000.000 Satoshis geben. Eine kleinere Stückelung im Nachhinein einzuführen ist dabei möglich. Normalerweise führt eine Deflation zu sinkenden Preisen. Zudem würde dadurch auch die Investitionsbereitschaft bei den Menschen zurückgehen, da sie erwarten, dass die Preise zukünftig noch weiter fallen. Dementsprechend geht die Ökonomie des Landes allmählich zugrunde. Die einzelnen Firmen und Konzerne entlassen immer häufiger Mitarbeiter, um die ständig zurückgehenden Verkäufe zu kompensieren. So würde die Lebensqualität im betroffenen Land stark zurückgehen. Jedoch sind Bitcoins global weitgehend vertreten, wodurch noch nicht klar ist, ob und wie sich eine Deflation auf die Weltwirtschaft auswirkt.⁹⁰

k) Regulierungsrisiko

Die Regulierungsbehörden eines jeden Landes stellen Kontrollorgane dar. Sie sollen sicherstellen dass die einzelnen Nutzer geschützt werden. Um dies zu gewährleisten, müssten sie eine möglich umfassende Kontrolle haben. Dazu muss man über jede Transaktion informiert sein. Die Identitäten von Sender und Empfänger müssen bekannt sein und es müsste Zugriff auf das Guthaben der einzelnen Nutzer haben. So eine Kontrolle ist bei unserem jetzigen Finanzsystem größtenteils möglich. Sollte man als einzelnes Land versuchen bei Bitcoins Regulierungen zu implementieren, würde man auf diverse Probleme stoßen. Das Hauptproblem wäre, dass man das Bitcoin-Protokoll des Systems ändern müsste. Dies würde wahrscheinlich das Black- und Whitelisting von Bitcoinadressen und die Reversibilität von Transaktionen zur Folge haben.⁹¹

⁸⁹ Vgl. (Platzer, 2014) S.108

⁹⁰ Vgl. (Strutzenberger, 2016) S. 22-23

⁹¹ Vgl. (Platzer, 2014) S.168

Von einem Blacklisting spricht man, wenn bestimmte Adressen innerhalb des Bitcoin-Netzwerkes nicht mehr benutzt werden darf und deren Benutzung technisch unterbunden wird. Beim Whitelisting werden Transaktionen nur zwischen bestimmten Adressen erlaubt wären. Beide Methoden hätten den gleichen Effekt und müssten auf eine ähnliche technische Methodik umgesetzt werden. Durch diese Maßnahmen könnten Regulierungsbehörden sicherstellen, dass nur Personen und Organisationen Geld benutzen könnten, die bei den Behörden bekannt und vertrauenswürdig sind.⁹²

Die Umkehrbarkeit von Transaktionen würden die Regulierungsbehörden die macht erlangen jegliches Geld jederzeit zu konfiszieren. Hauptsächlich würde dies also dem Zweck dienen, die Erträge von Kriminellen zu entwenden. Allerdings ist dabei auch durchaus möglich, dass ein Land diese Macht nutzt um einen politischen Gegner zu schädigen. Gleichzeitig könnte es zudem auch die Sparguthaben der einzelnen Bürger konfiszieren, um mit deren Geld die inländischen Banken zu retten.⁹³

Das Bitcoin-Netzwerk in seinem jetzigen Zustand wäre zunächst nicht in der Lage diese Art von Änderungen zu implementieren. Es würde letztendlich etwas vollkommen Neues entstehen. Generell lässt das Bitcoin-Protokoll solche grundlegenden Änderungen nicht zu. Um also Änderungen zu Regulierungszwecken zu integrieren, müsste man dies auf anderen Ebenen vornehmen.⁹⁴

Eine dieser Ebenen stellen die Tauschbörsen und Zahlungsdienstleister dar. Sie können, anders als das System selbst, mit den Jurisdiktionen der einzelnen Länder geregelt werden, da sie Schnittstellen zur bestehenden Finanzindustrie besitzen. Somit müssen diese Bitcoin-Unternehmen alle KYC- und AML- Vorschriften aus dem jeweiligen Land anwenden und umsetzen. KYC (Know Your Customer) - Regelungen besagen, dass ein Finanzunternehmen die Identität Ihrer Kunden feststellen muss. AML (Anti Money Laundering) - Regelungen zwingen die Finanzunternehmen zum Beispiel dazu, bei einem bestimmten Muster von finanziellen Aktivitäten eines Kunden, eine Mitteilung an die zuständige Behörde weitergibt. Diese muss dann entscheiden, ob es sich bei den finanziellen Aktivitäten um eine mögliche kriminelle Tat wie zum Beispiel Geldwäsche handelt.⁹⁵

⁹² Vgl. (Platzer, 2014) S.169

⁹³ Vgl. (Platzer, 2014) S.169

⁹⁴ (Platzer, 2014) S.170

⁹⁵ (Platzer, 2014) S.170

III. Chancen von Bitcoin

Bei Bitcoin handelt es sich nicht nur um eine einfache Internetwahrung. Es stellt vielmehr ein sich standig entwickelndes Finanzsystem dar. Dementsprechend besitzen Bitcoins die Moglichkeit neue Innovationen zu schaffen oder den vorhandenen Nachteilen im System entgegen zu wirken.

a) Innovationschance

Fur viele Handler und Nutzer sind Bitcoin relativ schwer als Zahlungsmittel zu akzeptieren. Das liegt vor allem an deren Neuartigkeit und den damit verbundenen Risiken. Aber anders als bei herkommlichen Wahrungen steht eine groe Community hinter ihnen, die eine standige Entwicklung der Wahrung. Dadurch konnten innerhalb weniger Jahre mehrere Verbesserungen bei der Software sowie Anwendungsmoglichkeiten der Hardware fur Bitcoin entwickelt werden. Diese standigen Updates bewirken eine nutzerfreundlichere Bedienung und Handhabung von Bitcoin. Auerdem wird damit probiert, die bestehenden Risiken von Bitcoin zu reduzieren oder im besten Fall komplett zu entfernen.

aa) Multisignatur-Transaktionen

Dabei handelt es sich um Transaktionen die, wie es der Name bereits impliziert, die Signatur von mehr als nur einer Partei braucht um ausgefuhrt zu werden. Diese zunachst simpel klingende Anwendung bringt groe Vorteile sowie eine Vielzahl von Anwendungsmoglichkeiten mit sich. So konnen etwa bei 2 aus 3 Multisignatur-Transaktionen beispielsweise dazu genutzt werden, dass ein Verkaufer erst dann Zugriff auf sein Geld erhalt wenn der Kunde und eine dritte Partei die Transaktion entsprechend absegnen. Die dritte Partei konnte dabei zum Beispiel ein Treuhand-Service oder ein Notar sein. Moglich ware aber auch der Postbote der uber die Unterschrift fur den Empfang des Paketes verfugt. Damit diese Art von Transaktion funktionieren kann, muss der Kaufer zunachst die Zahlung an den Verkaufer anweisen, dabei jedoch als Bedingung fur die Ausfuhrung der Transaktion integrieren, dass eine Signatur der dritten Partei notig ist. Dementsprechend entstehen Vorteile fur den Kaufer und Verkaufer. Der Verkaufer besitzt die Gewissheit uber die Zahlungswilligkeit und Zahlungsfahigkeit des Kaufers, da eine Transaktion an ihn bereits angewiesen wurde. Dem Kaufer kann damit eine vertragsgemae Lieferung vor der entsprechenden Entrichtung gewahrleistet werden.⁹⁶

⁹⁶ Vgl. (Platzer, 2014) S.182

Außerdem wären dank dieser Anwendung auch zeitlich definierte Transaktionen möglich. Denkbar wäre zum Beispiel, dass ein Schüler zu seinem 18. Geburtstag Geld für sein erstes Auto auf seine Bitcoin-Adresse überwiesen bekommt. Der eigentliche Geldbetrag wurde ihm aber schon zum 16. Geburtstag geschenkt. Die eigentliche Anwendung hat auch hier die Transaktion bereits gespeichert und der Schüler kann sich sicher sein den geschenkten Geldbetrag an seinem 18. Geburtstag zu erhalten.⁹⁷

Diese Funktionen brauchen allerdings bis zu ihrer Ausreifung noch eine gewisse Entwicklungszeit um sie in die Blockchain zu integrieren.⁹⁸

bb) Bitpay

Bei Bitpay handelt es sich um einen der beliebtesten Bitcoin-Zahlungsdienstleister. Durch diese Zahlungsdienstleister ist es für ein Unternehmen möglich Bitcoins zu akzeptieren und diese dann am Ende des Tages gegen den exakten Rechnungsbetrag der Währung seiner Wahl umzutauschen. Der Rechnungsbetrag wird dabei auf das Bankkonto des Unternehmens gutgeschrieben. Auf Wunsch des Kunden ist es auch möglich zu bestimmen, ob alle eingegangenen Zahlungen in die entsprechende Wunschwährung gutgeschrieben werden oder ob nach einem selbstbestimmten Prozentsatz ein Teil der Einnahmen in Bitcoin verbleibt. Gleichzeitig unterstützt Bitpay das Unternehmen mit zusätzlichen Programmen und Ideen, welche etwa beim E-Commerce-Handel nützlich ist.⁹⁹

Durch Unternehmen wie Bitpay ist es möglich, dem Volatilitätsproblem durch Annahme von Bitcoin zu entgehen. Allerdings muss man dafür eine Gebühr an den Zahlungsdienstleister entrichten. Bei Bitpay beträgt bis zu einem Prozent, wobei es aber möglich ist bessere Konditionen zu erzielen.¹⁰⁰

Will ein Unternehmen mit Bitpay zusammenarbeiten, so muss es sich zunächst einer Prüfung unterziehen. Bei dieser Prüfung wird die Legitimität des Unternehmens kontrolliert. Damit soll bestätigt werden, dass die durch den Service des Unternehmens kein Geld aus illegalen Einnahmequellen gewaschen werden kann. Dabei ist auch zu bemerken, dass Bitcoin nicht mit Unternehmen zusammenarbeitet, die in den Bereichen Glücksspiel, Pornographie oder Drogenhandel tätig sind. Das gilt auch wenn im Heimatland des Unternehmens diese Aktivitäten legal sind.¹⁰¹

⁹⁷ Vgl. (Platzer, 2014) S.182

⁹⁸ Vgl. (Platzer, 2014) S.182

⁹⁹ Vgl. (Platzer, 2014) S.108-109

¹⁰⁰ Vgl. (Platzer, 2014) S.108-109

¹⁰¹ Vgl. (Platzer, 2014) S.108-109

Solche Unternehmen gibt es bereits in vielen Ländern unter jeweils anderen Namen. Durch ihre Dienstleistungen helfen sie anderen Firmen dabei, Bitcoins als Zahlungsalternative anzunehmen. Leider entfernen sie bei Bitcoins damit seiner wichtigsten Eigenschaft: Dezentralität. So übernimmt Bitpay die Rolle als Bank und es können wieder die gleichen Probleme entstehen wie bei den herkömmlichen Währungen. Da dies der ursprünglichen Grundidee von Bitcoin widerspricht sind einige Mitglieder der Bitcoin-Community gegen solche Unternehmen.

cc) Hardware Wallets

Hardware Wallets stellen die sicherste Form von Bitcoin-Wallets dar. Sie sind kleine Single-Purpose-Computer von der ungefähren Größe eines mp3-Players. Dieser Computer generiert die privaten Schlüssel des Nutzers und lässt damit die Transaktionen auf einem separaten Gerät signieren. Dabei arbeitet die Hardware Wallet mit der Software Wallet auf dem PC zusammen. Die generierten privaten Schlüssel verlassen dabei nie in irgendeiner elektronischen Form das Gerät. Damit ist es Dritten nicht möglich diese Abzufangen und die dazugehörigen Bitcoin zu stehlen. Es spielt außerdem keine Rolle ob der mit dem Hardware Wallet verbundene PC von Trojanern oder Keyloggern befallen ist. Denn ein überwachter Rechner kann keinen Zugriff auf diese Bitcoins erlangen oder in irgendeiner Form die signierte Transaktion manipulieren. Zudem kann das Hardware Wallet selbst nicht von Schadprogrammen angegriffen werden.¹⁰²

Dieses Wallet setzt ein bisschen technisches Know-how des Nutzers voraus. Um Bitcoins aus diesem Wallet auszugeben muss man zunächst seinen PC per USB mit es verbinden. Dann benötigt das Wallet eine Identifikationsbestätigung des Nutzers. Diese Sicherung ist meist in Form eines Passwortes oder eines PIN's, um der Gefahr von Verlust oder Diebstahl entgegenzuwirken. Wenn das Hardware Wallet zerstört wird oder verloren geht, ist es möglich mit Hilfe eines Backups jederzeit auf das darauf gespeicherte Guthaben Zugriff zu nehmen.¹⁰³

¹⁰² Vgl. (Platzer, 2014) S.31-32

¹⁰³ Vgl. (Platzer, 2014) S.32

b) Kostenchance

Transaktionen mit Bitcoin sind extrem günstig bis kostenlos. Seit 2012 haben die meisten Bitcoin-Wallets eine standardmäßig voreingestellte Überweisungsgebühr von 0,0001 Bitcoin, was umgerechnet ca. 5 Eurocent entspricht. Es ist allerdings dem Nutzer möglich die Gebühr für jede Transaktion selbst festzulegen oder ganz wegzulassen. Wenn man als entscheidet die Gebühren komplett wegzulassen, kann sich das auf die Verarbeitungsgeschwindigkeit der Transaktion auswirken, also der Zeit mit der die Transaktion von dem Netzwerk bestätigt wird.¹⁰⁴

Aber dennoch können alternative Zahlungsmethoden wie SEPA-Überweisungen und Kreditkartenzahlungen weder von den Kosten der Gebühren noch bei der Geschwindigkeit mithalten. Sogar Dienste wie Paypal sind teurer als Überweisungen per Bitcoin. Demnach kann es für Firmen und Privatpersonen von Vorteil sein bei größeren oder internationalen Überweisungen auf Bitcoins zurückzugreifen, da man erwarten kann, dass sie sicher, schnell und kostengünstig sind.¹⁰⁵

c) Dezentralisierungschance

Ein großer genereller Vorteil der Bitcoins ist ihre Dezentralität. Damit gibt es keine Zentralbanken welche oftmals andere Ziele angehen die im Wesentlichen sich der Verbesserung der Wirtschaftslage widmen. Zusätzlich bewirkt die Dezentralität einen guten Schutz gegenüber Manipulationsversuchen. Ein weiterer großer Vorteil daraus ist die Anonymität, die bereits bei den allgemeinen Vorteilen von Kryptowährungen eine Erwähnung fand.¹⁰⁶

d) Wertsteigerungschance

Über die letzten Jahre hat sich gezeigt, dass Bitcoin als Investitionsmedium immer mehr an Bedeutung gewinnt. Während der Eurokrise flüchteten viele Menschen in andere Währungen. Zu diesem Zweck investierte einige von ihnen in Bitcoin, da dies ein Wertspeicher darstellte der keine staatlichen Zugriffe zuließ. Diese Vorteile sind weiterhin geblieben und haben zusammen mit der steigenden Beliebtheit von Bitcoin eine anhaltende Wertsteigerung erzeugt.¹⁰⁷

¹⁰⁴ Vgl. (Platzer, 2014) S.122

¹⁰⁵ Vgl. (Strutzenberger, 2016) S.24

¹⁰⁶ Vgl. (Strutzenberger, 2016) S.24

¹⁰⁷ Vgl. (Strutzenberger, 2016) S.23

e) Marktchance

Der Markt um Bitcoin und um Kryptowährungen wächst ständig. Der Grund dafür ist das immer größer werdende Vertrauen der Gesellschaft in die digitale Währung. Jüngste Ereignisse, wie zum Beispiel das Akzeptieren von Bitcoin als legales Zahlungsmittel in Japan beweist, dass sich bereits ein starker Markt entwickelt hat. Zu den Anfängen von Bitcoin waren nur wenige Produkte per Bitcoin käuflich, wie etwa Pizza und Alpakasocken. Nun sind ein breites Spektrum von Produkten und Dienstleistungen über das Internet per Bitcoin erwerblich. Dadurch schaffen es die Kryptowährungen immer mehr den Ruf eines Nischenproduktes zu entkommen.¹⁰⁸

IV. Der Bitcoin als offizielles Zahlungsmittel in Japan

Zu Beginn der Bitcoins entstand in Japan die damals einst größte Bitcoin-Börse der Welt, Mt. Gox. Diesen Umstand ist es geschuldet, dass die japanische Finanzaufsicht gezwungen war sich schnellstmöglich neue Regeln für die damals noch neue Währung zu überlegen. Durch die frühzeitigen Regelungsüberlegungen der Japaner war es ihnen daher auch schneller möglich Bitcoins in ihre Ökonomie zu integrieren. Seit dem 01.04.2017 ist der Bitcoin in Japan nun auch als offizielles Zahlungsmittel anerkannt worden. Er steht dabei auf einer Stufe mit anderen alternativen japanischen Währungen wie elektronischem Geld oder Einkaufs- und Geschenkgutscheinen.¹⁰⁹

Durch Japan kann damit nun die Massentauglichkeit der Bitcoins getestet werden. Gleichzeitig entwickelt Japans Regierung auch weiterhin neue Regelungskonzepte für Unternehmen die sich für den Handel mit Bitcoins spezialisieren. So müssen sich zum Beispiel Bitcoin-Börsen nun lizensieren lassen. Durch solche Maßnahmen generiert man für Unternehmen, Banken und Konsumenten eine zusätzliche Sicherheit.¹¹⁰

Nach aktuellem Stand scheint der frühe Markteinstieg der Japaner in Kryptowährungen ein Erfolg zu sein. Es gibt bis heute schon eine Menge von großen und kleinen Firmen die in ihren Geschäften eine Bitcoin-Kasse installiert haben. Gleichzeitig werden weiterhin neue Bezahlsysteme in Verbindung mit den Bitcoins entwickelt um dessen volles Potenzial nutzen zu können. So entwickelt etwa der Billigflieger Peach Aviation als erste japanische Fluglinie zusammen mit der Bitcoin-Börse Bitpoint ein Bezahlsystem, womit es den Kunden möglich ist Flugtickets mithilfe von Bitcoins zu erwerben. Allerdings muss die Fluglinie zunächst eine zuverlässige

¹⁰⁸ Vgl. (Strutzenberger, 2016) S.24

¹⁰⁹ Vgl. (Holtermann, 2017)

¹¹⁰ Vgl. (Holtermann, 2017)

Abrechnungsmethode für die Kryptowährung entwickeln. Durch die hohe Volatilität ist diesbezüglich natürlich vorsichtig vorzugehen. Ob solche Systeme sich in der Zukunft nun als praktisch und durchsetzbar erweisen muss sich erst noch herausstellen.¹¹¹

Das größte Technikhaus Japans Bic Camera hat bereits seit April 2017 für die Bitcoin-Kassen im Geschäft einen Weg um hohe Volatilität der Bitcoins gefunden. Sie arbeiten dazu mit japanischen Unternehmen Bitflyer zusammen, welches nach einem ähnlichen System funktioniert wie die Firma Bitpay funktioniert. Wie bereits vor einigen Kapiteln erwähnt wurde, schaffen es solche Unternehmen dem Volatilitätsrisiko entgegen zu wirken, indem sie als Zahlungsabwickler dem Kunden den Kaufpreis von seinem Bitcoin-Konto abzieht und diesen Betrag dann in Yen an Bic Camera überweist. So wird auch hier Einer der heimischen Erstanwender hat da schon eine Lösung: Bei Japans größtem Technikkauflhaus Bic Camera kann man bereits seit April in zwei Filialen mit Bitcoins an der Kasse bezahlen. Bic Camera arbeitet nicht mit US-Firma Bitpay, sondern mit Bitflyer aus Tokio zusammen. Das Prinzip ist das gleiche: Der Zahlungsabwickler zieht den Kunden das Geld vom Bitcoin-Konto ein und der Kooperationspartner Bic Camera erhält den Betrag in Yen ausgezahlt. Wie bereits im vorangegangenen Kapitel festgestellt, entfällt damit das allgemeine Volatilitätsrisiko bei Bitcoin.¹¹²

V. Die Blockchain – eine revolutionäre Technologie

Der Ruf von Bitcoins ist bis heute bei vielen Banken und Unternehmen fragwürdig. Allerdings hat die Technologie hinter dessen Konzept über die Jahre bewiesen, dass sie sicher und transparent ist. Die Blockchain hat als digitales Buchungssystem großes Interesse bei Banken und Großkonzernen gefunden. Die allgemeinen Vorteile die sich aus dieser Technologie ergeben werden in verschiedenen Start-up-Unternehmen zu neuen Nutzungsmöglichkeiten und Geschäftsideen weiterentwickelt.¹¹³

So wird etwa an einer Möglichkeit von Verträgen in der Art einer Blockchain gearbeitet. Diese „smart contracts“ werden mit bestimmten Vorgaben programmiert, dies es von Vertragspartei zu erfüllen gilt. Das würde in der Theorie etwa folgendermaßen aussehen: Jemand versäumt die Rate nach einem Autokauf zum Stichtag zu überweisen. Durch die sofortige Verifikation des dezentralen Systems werden die Türen des Autos dauerhaft verriegelt. Eine andere mögliche

¹¹¹ Vgl. (Holtermann, 2017)

¹¹² Vgl. (Holtermann, 2017)

¹¹³ Vgl. (Boie, 2016) S.1-2

Beispielkonstellation wurde bereits in dem Kapitel „kriminelle Programmentwicklung“ vorgestellt.¹¹⁴



Abbildung 6: Funktionsweise von Smart Contracts

Eine andere Vision gibt es bereits in der Musikbranche. Programmierer arbeiten daran, mithilfe einer sich ständig aktualisierbaren Blockchain eine einheitliche Rechtslage unter den Musikern zu schaffen, ohne das es später zu gerichtlichen Auseinandersetzungen kommt. So soll es dann etwa für die Musiker möglich sein über das Startup „Peertracks“ ihre Songs für iTunes oder Spotify bereitzustellen. Die Blockchain würde dann über ein bestimmtes System dafür sorgen, dass alle Rechteinhaber ihren Anteil bekommen.¹¹⁵

Länder wie Griechenland oder Honduras überlegen währenddessen bereits über die Reorganisation ihres Staatwesens, indem sie die Grundbücher der Katasterämter in eine Blockchain umbauen.¹¹⁶

Ein weiteres Start-up-Unternehmen versucht mithilfe der Blockchain ein soziales Netzwerk aufzubauen. Die Zielsetzung dahinter ist es, ein soziales Netzwerk aufzubauen welches keinem Konzern ermöglicht die Daten von Nutzern abzugreifen. Der Prototyp dazu heißt Akasha und funktioniert komplett ohne Server. Der gesamte Programmcode ist vollständig auf einer Blockchain, zusammen mit den verknüpften

¹¹⁴ Vgl. (Boie, 2016) S.2

¹¹⁵ Vgl (Boie, 2016) S.2

¹¹⁶ Vgl (Boie, 2016) S.2

Informationscontainern gespeichert. Die Informationen sind dabei für alle sichtbar und werden nicht wie z.B. bei Facebook geheim gehalten.¹¹⁷

Auch wenn viele Ideen erst in der Entwicklung sind, so hat ein Großteil der Finanzbranche das Potenzial dieser Technologie bereits erkannt. Dazu gehören auch die Deutsche Bank und die Commerzbank. Diese Banken interessieren sich zunächst für die hohe Geschwindigkeit, mit der eine Blockchain arbeitet. Diese Eigenschaft ist dabei besonders nützlich bei grenzüberschreitenden Überweisungen oder Wertpapiergeschäften.¹¹⁸

Selbstverständlich treten auch bei der Weiterentwicklung der Blockchain-Technologie ständige Sicherheits- und Rechtsfragen auf, was für viele der oben genannten Projekte eine noch lange Testphase bedeutet.

E. Schlussbetrachtung

Bitcoin und Kryptowährungen im Allgemeinen stellen eine Technologie dar, welche das Potenzial hat unsere Gesellschaft deutlich zu verändern. Seit der Einführung des Internets hat eine stetig steigende Digitalisierung in nahezu allen Lebensbereichen des Menschen stattgefunden. Dementsprechend ist es auch nicht verwunderlich, dass auch für das Finanzsystem eine digitale Entwicklung unumgänglich ist. Die wahrscheinlich größte Errungenschaft dieser Entwicklung war das Online-Banking.

Ein System was in der heutigen Zeit eigentlich gar nicht mehr wegzudenken ist und ständig von Millionen von Nutzern auf der ganzen Welt genutzt wird. Selbstverständlich liegt das vor allem an seinen Vorteilen gegenüber herkömmlichen Bankgeschäften, da es schneller, übersichtlicher und ständig erreichbar ist. Aber mit den Vorteilen solcher Systeme sind oft auch Nachteile verbunden. So sind durch Einführung digitaler Systeme die Gefahren der Datenspionage und Datenmanipulation ständig präsent. Ein Grund warum viele technologisch unerfahrene Menschen von solchen Systemen die Finger lassen und bei ihren vertrauten Geschäftsabläufen bleiben. Damit ist ersichtlich, dass der Erfolg eines digitalen Systems heutzutage von Funktionalität und Vertrauen abhängig ist.

¹¹⁷ Vgl. (Behrens, 2017) S.1

¹¹⁸ Vgl. (Boie, 2016) S.2

Kryptowährungen wie Bitcoin müssen sich dieses Vertrauen noch erarbeiten. Die Funktionalität, die wirtschaftliche Bedeutung und die allgemeinen Vorteile gegenüber anderen Finanzkonzepten und Finanzsystemen wurde in den vorangegangenen Kapiteln bereits ausführlich dargestellt. Allerdings stehen den großen Ambitionen dieser neuen Währung immer noch große Stolpersteine im Weg, welche sich in den meisten Fällen auf das fehlende Vertrauen der Menschen zurückführen lassen können. Es zeigten sich bereits nach einigen Monaten der Einführung von Bitcoins die Anwendungsmöglichkeiten für kriminelle Aktivitäten, speziell für den Schwarzhandel. Damit hatte der Bitcoin schnell einen schlechten Status bei der Öffentlichkeit und den Regierungen.

Zusätzlich sind die eigentlichen Nutzungsmöglichkeiten in den meisten Ländern noch nicht weit genug ausgereift um den Bitcoin in seiner Grundfunktion als Zahlungsmittel nutzen zu können. So gibt es bis heute nicht viele Geschäfte die den Bitcoin akzeptieren. Und auch Bitcoin Automaten sind wenig bis gar keine in vielen Ländern vorhanden. So ist es deshalb auch nicht verwunderlich dass Kryptowährungen von vielen bisher als Anlagemöglichkeit wie Aktien oder Wertpapiere angesehen werden.

Auch wenn Bitcoin noch einen langen Entwicklungsweg vor sich hat, so hat die ursprüngliche Technologie dahinter bereits einen bleibenden Eindruck in der Finanzwelt hinterlassen. So haben selbst Kritiker von Bitcoin erkannt, dass die Blockchain als digitales Buchführungssystem eine große Innovation in der Branche darstellt. Verschiedene Banken und Unternehmen arbeiten an diversen Projekten mit der Hilfe dieses Systems. Also selbst wenn die Bitcoins vielleicht eines Tages scheitern, so haben sie dennoch einen Weg für neue Konzepte und Technologien in der Wirtschaft geebnet.

Eine Einordnung in unser derzeitiges Rechtssystem gestaltet sich durch die Neuartigkeit von Kryptowährungen entsprechend schwierig. Da sich Bitcoins und die anderen Vertreter ständig weiterentwickeln muss auch darauf entsprechend Rücksicht genommen werden. Es muss eine konkrete rechtliche Definition über den Begriff einer Kryptowährung erarbeitet werden. Auf dessen Grundlage hin müssten dann allgemeine Regelungen, bezüglich der grundlegenden Funktionen im Zusammenhang mit den Nutzungsmöglichkeiten erstellt werden. Die bisherige Rechtsdefinition und Einordnung ist unvollständig.

Viele Experten aus der Finanz- und Internetbranche sehen den Bitcoin schon jetzt als Erfolg an und glauben an dessen Überlegenheit gegenüber Fiatgeld. Auch der momentane Börsenkurs von Bitcoin steigt beständig an. Es ist anzunehmen, dass sich dieser Trend für die folgenden Monate fortführen wird.



Abbildung 7: Aussagen über Bitcoin

Letztendlich war die Intention des ursprünglichen Entwicklers Satoshi Nakamoto nach der Finanzkrise 2008 eine Alternative zum derzeitigen Finanzsystem aufzuzeigen. Viele Wirtschaftsakteure teilten diese Grundgedanken und halfen ihm dementsprechend bei der Entwicklung. Auch wenn Bitcoin vielleicht eines Tages verschwindet, so hat es Satoshi Nakamoto geschafft, dass eine funktioniere Alternative möglich ist.

Literaturverzeichnis

- Altinpicak, Ö., & Völkel, S. (2016). *Einsatz von Bitcoin im Online Handel*. Düsseldorf.
- Bank, E. C. (February 2015). *Virtual currency schemes - a further analysis*.
- Behrens, C. (10. Juni 2017). *Süddeutsche Zeitung*. Abgerufen am 16. August 2017 von [sueddeutsche.de: http://www.sueddeutsche.de/digital/bitcoin-neues-geld-fuer-eine-neue-welt-1.3539556](http://www.sueddeutsche.de/digital/bitcoin-neues-geld-fuer-eine-neue-welt-1.3539556)
- bitcoinmining.com*. (2011-2017). Abgerufen am 17. Juni 2017 von Bitcoin Mining Hardware Guide: www.bitcoinmining.com/bitcoin-mining-hardware/
- Boie, J. (8. Januar 2016). *Süddeutsche Zeitung*. Abgerufen am 13. August 2017 von [sueddeutsche.de: http://www.sueddeutsche.de/digital/blockchains-diese-technologie-wird-die-digitale-welt-veraendern-1.2808259](http://www.sueddeutsche.de/digital/blockchains-diese-technologie-wird-die-digitale-welt-veraendern-1.2808259)
- Burleigh, N. (19. Februar 2015). *Newsweek.com*. Abgerufen am 2017. August 15 von Newsweek: <http://www.newsweek.com/2015/02/27/silk-road-hell-307732.html>
- Cap, C. M. (7. März 2017). *Frankfurter Allgemeine*. Abgerufen am 13. Juli 2017 von faz.net: <http://www.faz.net/aktuell/wirtschaft/wirtschaft-in-zahlen/grafik-des-tages-die-einsame-herrschaft-der-bitcoins-14913188.html>
- Deutsche Welle. (5. Januar 2017). *Deutsche Welle*. Abgerufen am 23. Juli 2017 von dw.com: <http://www.dw.com/de/digitalw%C3%A4hrung-bitcoin-auf-rekordkurs/a-37017737>
- gechecked.de. (2017). *gechecked.de*. Abgerufen am 12. August 2017 von [gechecked.de: https://www.gechecked.de/bitcoin/](https://www.gechecked.de/bitcoin/)
- Graff, B. (25. April 2016). *sueddeutsche.de*. Abgerufen am 11. August 2017 von Süddeutsche Zeitung: <http://www.sueddeutsche.de/digital/media-player-digitale-schattengewachse-1.2964140>
- Holtermann, F. (16. Juni 2017). *Handelsblatt*. Abgerufen am 17. Juli 2017 von Handelsblatt.com: <http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/zockergeld-und-zahlungsmittel-bitcoin-boomland-japan/19932084-4.html>
- ITWissen.info Technologiewissen online*. (17. Januar 2014). Abgerufen am 25. Mai 2017 von <http://www.itwissen.info/Peer-to-Peer-Netz-peer-to-peer-network-P2P.html>
- Klein, P. D. (23. Oktober 2015). *Legal Tribune Online*. Abgerufen am 12. September 2017 von LTO Legal Tribune Online: <https://www.lto.de/recht/hintergruende/h/eugh-urteil-c26414-keine-umsatzsteuer-bitcoins-umtausch/>
- kreditkarte.net. (2016). *kreditkarte.net*. Abgerufen am 7. August 2017 von [kreditkarte.net: https://www.kreditkarte.net/wissenswertes/smart-contracts/](https://www.kreditkarte.net/wissenswertes/smart-contracts/)
- Münzer, J. (19.12.2013). *Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer*. BaFin.
- Neuhaus, C. (2017). Was hinter dem Kursanstieg der Bitcoins steckt. *Zeit online*.
- Platzer, J. (2014). *Bitcoin kurz & gut Banking ohne Banken*. Heidelberg: O'Reilly Verlag GmbH & Co. KG.

- Sander, P. (2016). *Bitcoins für Anfänger: Alles was Sie zum Thema Bitcoin wissen müssen. Eine Einführung in die Welt der Kryptowährung*. Wroclaw: Amazon Fulfillment.
- Scherschel, F. A., & Bögeholz, H. (14. Juni 2017). *c't magazin für Computertechnik*. Abgerufen am 24. Juli 2017 von heise.de: <https://www.heise.de/ct/artikel/So-funktioniert-die-Kryptowaehrung-Bitcoin-3742304.html>
- Schroeder, M. (24. Juni 2014). Bitcoin: Virtuelle Währung – reelle Problemstellungen. Bochum, Nordrhein-Westfalen, Deutschland.
- Schwenke, T. (14. April 2014). *Rechtsbelehrung.com*. Abgerufen am 17. Juni 2017 von Bitcoins - Rechtsbelehrung Folge 13 (Jura-Podcast mit FAQ in Shownotes): <https://rechtsbelehrung.com/bitcoins-rechtsbelehrung-folge-13-jura-podcast-faq-in-shownotes/>
- Strutzenberger. (2016). *Die Kryptowährung Bitcoin. Geschichte, Funktionsweise, Sicherheit und Wirtschaftliche Aspekte*. Norderstedt: GRIN Verlag.
- Terlau, D. M. (10. Januar 2014). Aktuelle Stellungnahme der BaFin zu Bitcoin. Köln, Nordrhein-Westfalen, Deutschland.
- Umtausch der virtuellen Währung „Bitcoin“ in konventionelle Währungen, C-264/14 (EuGH 22. Oktober 2015).

Abbildungsverzeichnis

Abbildung 1: Bitcoin und andere Kryptowährungen.....	2
(Cap, 2017)	
Abbildung 2: Struktur von Netzwerken.....	5
(Platzer, 2014) S.18	
Abbildung 3: Transaktionsprinzip von Bitcoin.....	10
(Scherschel & Bögeholz, 2017)	
Abbildung 4: Wechselkurs von Bitcoin.....	23
(Deutsche Welle, 2017)	
Abbildung 5: Schwarzmarktwebsite „Silk Road“	25
(Burleigh, 2015)	
Abbildung 6: Funktionsweise von Smart Contracts.....	37
(kreditkarte.net, 2016)	
Abbildung 7: Aussagen über Bitcoin.....	40
(gechecked.de, 2017)	

Abkürzungsverzeichnis

BGB –	Bürgerliches Gesetzbuch
ZAG –	Zahlungsdiensteaufsichtsgesetz
KWG -	Kreditwesengesetz
StGB -	Strafgesetzbuch
EStG -	Einkommenssteuergesetz
MWSTG -	Mehrwertsteuergesetz
MwSt. –RL -	Mehrwertsteuerrichtlinie
AGB -	Allgemeine Geschäftsbedingungen
BaFin -	Bundesanstalt für Finanzdienstleistungsaufsicht
EuGH -	Europäischer Gerichtshof
GPU –	Englisch: graphics processing unit; Deutsch: Grafikkarte
p2p –	Peer-to-Peer Netzwerk
PC –	Personal Computer
USB -	Universal Serial Bus
PIN -	Persönliche Identifikationsnummer
ASIC –	Englisch: Application-specific integrated circuit; Deutsch: anwendungsspezifische integrierte Schaltung
z.B. -	zum Beispiel
SEPA -	Englisch: Single Euro Payments Area; Deutsch: Einheitlicher Euro-Zahlungsverkehrsraum
ETF -	Englisch: Exchange Traded Fund Deutsch: börsengehandelter Indexfonds

KYC -	Know Your Costumer
AML -	Anti Money Laundering
mp3 -	Properietäres, verlustbehaftetes Kompressionsformat für Audiodaten
EUR -	Euro
DDoS -	Distrubed-Denial-of-Service
SEC -	Securities and Exchange Commision
FBI -	Federal Bureau of Investigation
CIA -	Central Intelligence Agency
USA -	Englisch: United States of America; Deutsch: Vereinigte Staaten von Amerika

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Die Stellen der Hausarbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Sebastian Neumann

Bernburg, den 30.09.2017