

Initial Coin Offering

Studie zu Kryptowährungen und der Blockchain-Technologie

Prof. Dr. Michaela Hönig
Frankfurt University of Applied Sciences

Frankfurt am Main
Stand Mai 2018



Der Studiengang International Finance Bachelor of Science hat im Wintersemester 2017/2018 in fünf Projektgruppen unter Leitung von Frau Prof. Dr. Hönig das Thema ICOs, Bitcoin und Blockchain über mehrere Wochen analysiert, diskutiert und über 30 Befragungen mit Kreditinstituten und aufsichtlichen Institutionen durchgeführt. Das Ergebnis ist diese Studie mit dem Ziel Aufklärung des Themas in einem Dokument zu vermitteln.

Management Summary

Initial Coin Offering (ICO) und Kryptowährungen sind Innovationen, die eine virtuelle, unregulierte und grenzüberschreitende Welt darstellen. Demgegenüber steht die reale Welt mit 194 Staaten und ihren Wirtschaftsräumen, in denen eigene Gesetze, Regeln und Normen gelten. Diese beiden Welten sind noch nicht miteinander kompatibel – das wird die Herausforderung der kommenden Jahre für die Entscheidungsträger in Politik, Wirtschaft und Gesellschaft werden. Von daher sollten die Entwicklungen und Folgewirkungen dieser virtuellen Neuerungen genau beobachtet werden. Darüber hinaus sollten Wege gefunden werden, wie die Vorteile dieser neuen Technologie in die bestehenden Finanzsysteme integriert werden können.

Bitcoin ist der bekannteste Vertreter unter den Kryptowährungen und hat vor allem aufgrund des immensen Kursanstieges und den nachfolgenden starken Kursschwankungen große Aufmerksamkeit in den Medien gefunden. Aufsichtsbehörden und Notenbanken warnen, dass sich in dem Segment eine Blase bilden könnte mit hohen Risiken für Anleger und daraus folgend für die Marktstabilität. Kryptowährungen werden von den Aufsichtsbehörden als digitale Recheneinheiten angesehen. Sie sind kein gesetzliches Zahlungsmittel und weder Währungen, Devisen oder Sorten. Sie zählen nicht zum elektronischen Geld im Sinne des Zahlungsdienstenaufsichtsgesetzes.

Im Zeitraum vom Oktober 2017 bis Februar 2018 haben wir in einer Projektgruppe das Thema ICO untersucht. Zentrale Fragestellungen zu ICO's waren dabei: Die rechtliche/aufsichtsrechtliche Einordnung, die Funktionsweise, der Markt sowie die dahinter liegende Blockchain-Technologie. Handel und Börsen von Kryptowährungen wurden analysiert und Aspekte einer Blasenbildung bei Bitcoin untersucht.

Die wesentlichen Ergebnisse unserer Untersuchung sind:

- Dass Kryptowährungen bestehende Währungen ablösen könnten, halten wir für nicht realistisch. Gründe dafür sind die komplizierte, technische Aufbewahrung der Wallets (digitaler Briefbörse/Aufbewahrungsort), die aufwendigen und teuren Transaktionen, der fehlende intrinsische Wert, hohe Deflation, fehlendes Vertrauen, geringe Akzeptanz als Zahlungsmittel und der fehlende Rechtsrahmen.
- Eine Blasenbildung bei Bitcoin ist möglich. Die Gefahren ansteckender Effekte auf die Realwirtschaft und den Finanzsektor sind jedoch gering. Adresskonzentration, Marktkapitalisierung und derivativer Anteil von Bitcoin wurden in der Studie untersucht. Die Adressen, die 95% der Bitcoins im Bestand haben sind zu 2,2% public keys (Miner Fabriken in Asien). Die restlichen Adressen (97%) halten in der Regel jeweils nur 0,1 bis 1 Bitcoin. Die Granularität der Adresskonzentration ist somit sehr breit und stellt daher kein Risiko oder Übertragungseffekt auf die reale Wirtschaft dar, da anzunehmen ist, dass die geringen Bestände der Anleger nicht kreditfinanziert sind.
- Der Anteil des derivativen Handels als auch die Marktkapitalisierung von ICO's in Relation bspw. zur Geldmenge ist zu gering, um von einer Gefährdung der Finanzstabilität zu sprechen. Die Blase ist daher als nicht invasiv bzw. infiltrierend anzusehen.
- Das Thema ICOs ist grenzüberschreitend und kann daher nur global reguliert werden.
- Wir betrachten Bitcoin als Recheneinheiten, da beim Mining der Nummernkreis eines Codes um 12,5 Bitcoins fortgeschrieben wird. Das ist nichts anderes als ein Hinzuaddieren von Zahlen. Aus unserer Sicht sind digitale Recheneinheiten weder aus ökonomischer noch aus ökologischer Sicht effizient. Die ökologische Ineffizienz richtet sich auf den hohen Stromverbrauch der Hash-Berechnung, der bei der Verwendung nicht erneuerbarer Energien zu erheblichen Umweltbelastungen führt.

- Kryptowährungen erfüllen die Kernfunktionen von Geld – Wertspeicher, Zahlungsmittel und Recheneinheiten – nur sehr bedingt.
- Viele Kreditinstitute und Industrieunternehmen haben Projekte mit dem Ziel gestartet, die Blockchain-Technologie auf mögliche Elemente zur Nutzung in den Unternehmen zu untersuchen. Die ursprüngliche Blockchain-Technologie, von Bitcoin-Erfinder Satoshi Nakamoto, eignet sich aus heutiger Sicht nicht zur Übernahme in die Kreditwirtschaft oder Industriebetriebe.

Spekulationsblasen wie die Dotcom-Blase im Jahr 2000 oder die Finanzkrise ab 2007 haben immer auch zu Veränderungen in der Wirtschaft und der Gesellschaft geführt. Spannend wird, welche Veränderungen durch die Blockchain-Technologie in Geschäftsprozessen und Wertschöpfungsketten entstehen können.

Schlussendlich wird sich auch der ICO-Markt konsolidieren, entweder durch Vorgaben von außen oder durch die natürlichen Kräfte von Angebot und Nachfrage.

Beim letzten G20 Gipfel im März erklärten die Finanzminister, dass sie Kryptowährungen wie den Bitcoin aufmerksam beobachten werden. Konkrete Maßnahmen zur Regulierung wurden auf dem Treffen aber nicht beschlossen.

Inhaltsverzeichnis

1.	Was ist Initial Coin Offering?	7
1.1.	Definition	8
1.2.	Rechtliche Grundlagen	9
1.3.	Einordnung durch die ESMA	10
1.4.	Einordnung durch die EBA	10
1.5.	Einordnung durch die EZB	11
1.6.	Einordnung durch die Bundesbank	11
1.7.	Einordnung durch die BaFin	12
1.8.	Steuerrechtliche Behandlung in Deutschland	17
1.9.	Regulierungen im asiatischen Raum	18
1.9.1.	China	18
1.9.2.	Japan	19
1.9.3.	Südkorea	19
2.	Handel und Marktplätze	20
2.1.	Kryptobörsen	20
2.2.	Kauf auf Handelsplattformen	23
2.3.	Risiken für Anleger	23
2.4.	Spekulationsblase Bitcoin	25
2.4.1.	Adressenkonzentration	26
2.4.2.	Marktkapitalisierung	27
2.4.3.	Derivatehandel	29
2.5.	Illegale Verwendungen im Darknet	30
2.6.	Energieverbrauch & technische Restriktionen des Handels	31
2.7.	Übersicht der Mining Pools	33
3.	Die Blockchain-Technologie	34
3.1.	Ursprung und Begriffe	34
3.2.	Wie funktioniert die Blockchain-Technologie?	35
3.3.	Smart Contracts	38
3.4.	Sicherheit der Blockchain	39
3.5.	Distributed Ledger Technologie (DLT)	40
3.6.	Einsatzmöglichkeiten in Banken	41
3.7.	Einsatzmöglichkeiten in der Industrie	42
3.7.1.	Einzelhandel – Lebensmittelsicherheit	42
3.7.2.	Transport – E-Mobilität	43
3.7.3.	Energiewirtschaft	43
3.8.	Einsatzmöglichkeiten in anderen Bereichen	44
3.8.1.	Non Profit Organisationen	44
3.8.2.	Gesundheitswesen	44
3.8.3.	Demokratie 2.0	45
4.	Kernaussagen unserer Untersuchungen	47
5.	Abbildungsverzeichnis	49

1. Was ist Initial Coin Offering?

Initial Coin Offering (ICO) ist eine nicht regulierte Methode des Crowdfundings und auch als sogenannte Schwarm- oder Gruppenfinanzierung bekannt. Es ist ein neues Mittel zur Kapitalaufnahme von Firmen, deren Geschäftsmodell auf Kryptowährungen basiert und keinen einheitlichen globalen Gesetzen oder Vorschriften unterliegt. Mit dieser neuen, digitalen Form der Kapitalbeschaffung umgehen Firmen den bekannten, streng regulierten Vorgang eines Börsengangs (Initial Public Offering, IPO). In einem Initial Coin Offering wird ein Anteil einer neu emittierten Kryptowährung an Anleger verkauft im Austausch gegen staatlich emittierte Währungen oder gegen andere Kryptowährungen wie beispielsweise Bitcoin (Schueffel, 2017).

<p>IPO:</p> <p>Börsenzulassung</p>	<p>Aktien werden über die Börse Anlegern zum Kauf angeboten. Eigenkapitalbeschaffung durch Ausgabe von Aktien. Zeit- und kostenintensiver Prozess. Bestehende Regulierung, Prospektpflicht. 12 IPO's in 2017 in Deutschland.</p>	
<p>ICO:</p> <p>Nicht regulierte Methode des Crowdfundings.</p> <p>Finanzierung eines Projektes</p> <p>Coins und Tokens um Kapital einzusammeln</p>	<p>Coins sind <u>digitale Münzen</u>, die für <u>Bezahlungen</u> geeignet sind. Das System basiert auf einer von den Teilnehmern <u>gemeinsam verwalteten dezentralen Datenbank</u>, in welcher alle Transaktionen in einer Blockchain aufgezeichnet werden. Neue Einheiten werden durch Mining erzeugt.</p> <p>Tokens englischer Begriff Wertmarke oder Jeton, <u>keine eigene Blockchain</u>, laufen meist über Ethereum-Blockchain - können unabhängig von dieser nicht existieren.</p> <p>Einfach zu generieren, keine neue Infrastruktur mit eigenen Nodes und Minern notwendig. Utility Tokens / App Token gewähren Zugang zu einem Service oder Dienstleistung.</p>	

Abbildung 1: Unterschiede ICO versus IPO

Bitcoin ist die bekannteste Kryptowährung. Unter dem Pseudonym Satoshi Nakamoto wurde im November 2008 auf 8 Seiten die technische Grundlage für Bitcoin, Kryptowährungen und die Blockchain-Technologie in einem „Whitepaper“ beschrieben. Welche Person oder Personengruppe sich hinter diesem Pseudonym verbirgt, ist bis heute unbekannt.

Die wesentlichen Unterschiede zwischen Initial Coin Offering (ICO) und einem Börsengang (IPO) sind nachfolgend dargestellt.

	Initial Public Offering (IPO)	Initial Coin Offering (ICO)
Ziel und Zweck	Börsengang eines Unternehmens. 12 IPO's im Jahr 2017 in Deutschland.	Digitale Form der Kapitalbeschaffung. Stand 3. April 1599 „Kryptowährungen“ nach CoinMarketCap davon 918 Coins und 681 Tokens.
Gesetze & Regulierung	Ja, eine Vielzahl von Gesetzen und Vorschriften die bei einem Börsengang zu beachten sind wie beispielsweise Wertpapierprospektgesetz, Aktiengesetz, Börsengesetz.	Komplett rechtsfreier Raum. Keine Regulierung. Keine Anwendung des Aktienrechts. Tokens weder Mitgliedschafts- noch Informations-, Kontroll- und Stimmrechte. Keine Vorschriften für den ICO. Der Anbieter schildert sein Vorhaben in einem sogenannten Whitepaper. Durchschnitt vier Seiten.
Gefahren	Kursverluste, Insolvenz des Institutes entsprechende Ansprüche des Anlegers	Höhere Volatilität wie bei Aktien bis zum Totalverlust, Hacken der Online Börsen, Unseriöse, illegale ICO's (Geldwäsche, Betrug, etc.), Datenmissbrauch, Anleger hat keinerlei Ansprüche.

Abbildung 2: Regulatorische Unterschiede IPO zu ICO

1.1. Definition

Anstatt beispielsweise Aktien im Gegenzug zum eingezahlten Geld, verteilen die Firmen bei ICOs Einheiten einer Digitalwährung in Form von sogenannten „Tokens“, welche die Investoren dann als Zahlungsmittel oder als Wertanlage nutzen können. Das Konzept ähnelt stark dem eines IPO (Initial Public Offering). Beide Begriffe referenzieren eine Finanzierungsmöglichkeit, bei der Investoren Zugang zu einem künftigen Feature des finanzierten Projektes bekommen sollen. Bei ICO startet das Projekt aber erst in der Zukunft.

Es gibt keine Vorschriften zu einer bestimmten Unternehmensform bei Durchführung eines ICOs, auch ein tatsächlicher Geschäftsbetrieb ist nicht erforderlich. Theoretisch können Einzelpersonen, die kein Geschäft betreiben, Tokens technisch anbieten oder beauftragen. (BaFin, Journal Initial Coin Offering, 2017).

In den USA existiert bereits ein funktionierender Markt für ICOs. Einschlägige Übersichtsseiten listen Dutzende laufende Transaktionen auf. In China haben die Behörden ICOs verboten und ließen den Bitcoin-Preis dadurch kurzzeitig um beinahe 40 % einbrechen.

Im Juli 2017 deutete die US-amerikanische Börsenaufsicht Securities and Exchange Commissions (SEC) an, dass sie die amerikanische Wertpapiergesetzgebung auf ICOs anwendbar sein könnte (SEC, 2017). Die SEC äußerte sich allerdings nicht dazu, ob alle auf basierende Tokens und Kryptowährungen tatsächliche Wertpapiere im zu regulierenden Sinne darstellen, vielmehr werde diese Entscheidung von Fall zu Fall getroffen. Das Statement der SEC könnte aber mehr Vertrauen der breiten Öffentlichkeit in ICOs schaffen und damit eine höhere Investitionsbereitschaft in diese Finanzinstrumente.

Europäische und deutsche Aufsichtsgremien haben das Thema erfasst, stehen miteinander in Kontakt und beobachten die Entwicklungen genau. Alle haben Verbraucherwarnungen ausgesprochen und sehen die Token Ausgabe nicht als Währung, sondern als digitale Recheneinheiten an (BaFin, Journal Initial Coin Offering, 2017).

Der erste bekannte ICO in Deutschland ist der Verkauf von Wys-Token ab Oktober 2017. (Wystoken, 2017). Wysker hat seinen Sitz in Berlin und arbeitet an einer gleichnamigen Shopping-App, bei der Nutzer ihre persönlichen Daten für Werbetreibenden zugänglich machen können und dafür mit Rabatten auf ihren Einkauf belohnt werden. Werber und Einzelhändler erhalten dagegen Zugang zu potenziellen Kunden und deren Daten. Die Technologie dahinter basiert auf der Ethereum-Blockchain. Das nötige Kapital für die Umsetzung sammelte Wysker bei einem ICO der Kryptowährung Ether (ETH) ein. Die Investoren erhalten im Gegenzug Wys-Tokens, ein ETH entspricht aktuell 18.123 WYS. Diese Wys sollen auch später als Zahlungsmittel in der App zum Einsatz kommen. Die Nutzer werden damit entlohnt, wenn sie ihre Daten mit Werbetreibenden teilen und können ihre gesammelten oder im Zuge des ICOs erworbenen Token beim Shoppen über die App zum Bezahlen oder für Rabattaktionen nutzen. Darüber hinaus sollen „Wys“ später auch an Krypto Börsen handelbar sein. Die Wysker App ist seit dem 31. Januar 2018 erhältlich. Eine gute Übersicht der weltweit bekanntesten ICOs, Themen und Konferenzen online verfügbar bietet die Plattform Coinschedule. Dort sind aktuell 235 ICO beschrieben und mit dem Stand des eingesammelten Kapitals dargestellt (Coinschedule, 2017).

1.2. Rechtliche Grundlagen

Da das Aktienrecht auf ICOs keine Anwendung findet, müssen Tokens weder Mitgliedschafts- noch Informations-, Kontroll- und Stimmrechte enthalten. Der Anbieter kann also völlig frei entscheiden, welche Rechte oder Ansprüche er den Anlegern durch die Tokens einräumt. Der Begriff der „Rechnungseinheiten“ ist in Deutschland nur im KWG erfasst. Die deutsche Finanzaufsichtsbehörde stuft den Bitcoin, sowie andere Kryptowährungen, als Finanzinstrumente gemäß §1 Absatz 11 Satz 7 KWG ein (KWG, 2018). Der Bitcoin fällt dabei nicht unter eine Digitalwährung, da dieser nicht die dafür notwendige Wertstabilität einer Währung aufweist (vgl. finanzen.net, 2017a). Vielmehr ist dieser eine „digitale Abbildung von Wert, die nicht von einer Zentralbank oder Behörde geschaffen wird und auch keine Verbindung zu gesetzlichen Zahlungsmitteln haben muss“ (BaFin, 2014).

Meist schildern Anbieter ihr Vorhaben und die Funktionsweise der angebotenen Tokens in einem sogenannten Whitepaper, in dem die Vertragsbedingungen veröffentlicht werden. Die Inhalte dieser Unterlagen sind weder gesetzlich vorgegeben noch von einer Aufsichtsbehörde auf Vollständigkeit geprüft. Zur Durchführung eines ICO ist weder eine bestimmte Unternehmensform noch ein tatsächlicher Geschäftsbetrieb erforderlich. Es können also auch Einzelpersonen, Tokens anbieten, die gar kein Geschäft betreiben, sie müssten nur über die relevanten Programmierkenntnisse verfügen.

Geld muss nach der Definition der Bundesbank drei Eigenschaften erfüllen:

- Tausch / Zahlungsmittel
- Recheneinheit
- Wertaufbewahrungsmittel (Bundesbank, Begriff und Aufgabe des Geldes, 2018)

Kryptowährungen erfüllen aus unserer Sicht zwei dieser drei Kernfunktionen in keinem relevanten Maße. Die Kursschwankungen beim Bitcoins liegen einzig in der Hoffnung auf eine hohe Rendite begründet und nicht in sei-

nem fairen, intrinsischen Wert. Bitcoin ist eine digitale Recheneinheit unter Betrachtung des Bitcoin Schürfens. Ausführliche Argumente dazu unter Punkt 1.6 und 1.7.

1.3. Einordnung durch die ESMA

Die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) ist eine unabhängige EU-Behörde, die den Anlegerschutz verbessert und für stabile, ordnungsgemäß funktionierende Finanzmärkte sorgen soll (ESMA, 2018). Die ESMA warnt Anleger auf ihrer Homepage vor Risiken im Zusammenhang mit Initial Coin Offering (ESMA, Highlights ICO risks for investors and firms, 2018).

Investitionen in ICOs seien sehr riskante und hochspekulative Investments. Ein Totalverlust des investierten Vermögens sei möglich, ebenso könne es betrügerische Absichten der Emittenten geben. Einige ICOs seien als Betrug identifiziert worden, und die ESMA könne auch nicht ausschließen, dass einige ICOs zur Geldwäsche benutzt würden. Die Technik sei in vielen Fällen noch nicht ausgereift, warnt die ESMA: Fehler in Codes oder Programmen könnten bewirken, dass Anleger keinen Zugriff auf ihre Tokens hätten oder sie ihnen gestohlen werden könnten. ICOs sind aufgrund ihrer Anonymität und der Möglichkeit, mit ihnen in kurzer Zeit hohe Geldbeträge aufzunehmen, anfällig für Betrug und unerlaubte Tätigkeiten.

Sofern ICOs sich als Finanzinstrumente qualifizieren, sei es wahrscheinlich, dass die daran beteiligten Firmen regulierte Investmentaktivitäten betreiben. Dann müssten sie laut ESMA entsprechende Vorgaben erfüllen. Genannt werden die EU-Prospektrichtlinie, die Finanzmarktrichtlinie MiFID, die Richtlinie für Verwalter alternativer Investmentfonds (AIFMD) sowie die vierte Geldwäscherichtlinie.

Die ESMA betont, dass an ICOs beteiligte Firmen sorgfältig prüfen sollten, ob ihre Vorhaben eine von den EU-Gesetzen regulatorisch erfasste Aktivität darstellten. Sei dies der Fall, würde jede Nichterfüllung der entsprechenden Regularien einem Verstoß gleichkommen. Es liegt laut ESMA in der Verantwortung der an ICOs beteiligten Firmen, entsprechende rechtliche Rahmenbedingungen zu prüfen, die notwendigen Genehmigungen einzuholen und alle anwendbaren Anforderungen zu erfüllen (Börsen-Zeitung, Börsen-Zeitung, 2017). Die Investoren könnten sich nicht auf den Schutz von EU-Gesetzen verlassen, wenn die virtuellen Börsengänge sich außerhalb des Rechtsraums der 28 EU-Mitgliedsstaatenbewegen.

1.4. Einordnung durch die EBA

Die Europäische Bankenaufsichtsbehörde (EBA) ist eine unabhängige EU-Behörde. Ihre Aufgabe ist es, gemeinsam mit den nationalen Aufsichtsbehörden der EU-Mitgliedsstaaten ein wirksames und stimmiges Maß an Regulierung und Beaufsichtigung im europäischen Bankensektor zu gewährleisten. Somit spielt sie auch bei der Einstufung von Kryptowährungen, wie Bitcoin, eine entscheidene Rolle (EBA, 2017).

Im Juli 2014 nahm die Aufsichtsbehörde in ihrem Paper „EBA Opinion on virtual currencies“ Stellung zu den so bezeichneten virtuellen Währungen und zeigte Risiken auf:

Nutzer von Bitcoin-Handelsplattformen und digitalen Wallets seien nicht durch Regularien vor Insolvenzen, Aufgabe der Geschäftstätigkeit oder Fehlern der jeweiligen Plattform geschützt. So drohe im Extremfall der Totalverlust für den Anleger, da die digitalen Wallets keiner Einlagensicherung, wie etwa Konten bei einer Bank, unterlä-

gen. Die digitalen Wallets sind zudem nicht vor Hackern sicher und keine zentrale Stelle speichert Passwörter oder stellt diese wieder her (EBA, 2014).

Ein Käufer, der mit Bitcoin zahlt, hat keine Rückerstattungsansprüche. Der Kurs der Kryptowährungen ist sehr volatil: Bei steigender Popularität einer anderen Währung wäre der Kurs des Bitcoins nicht gesichert vor einem vollständigen Verfall, da dieser keine realen Werte wie Gold als Grundlage hat. Da zwar Transaktionen öffentlich sind, aber Sender und Empfänger nicht, sei das System gegenüber Geldwäsche und Terrorismusfinanzierung sehr anfällig (EBA, 2017).

1.5. Einordnung durch die EZB

Die wesentlichen Aufgaben der Europäischen Zentralbank (EZB) sind die Preisniveaustabilität im Euroraum sicherzustellen, die Aufsicht über die systemrelevanten Banken im Euro-Raum und die Festlegung und Durchführung der Geldpolitik (ECB, 2017). Die EZB hat als eine der ersten Institutionen bereits im Oktober 2012 in einem 55-seitigen Bericht das Thema virtuelle Währungen und Bitcoin beschrieben (ECB, 2012). In einer weiteren Studie „Virtual currencies Schemes – a further Analysis“ vom Februar 2015 wurde eine klare Einordnung vorgenommen. Die EZB betrachte virtuelle Währungen nicht als Form von Geld oder Währung. Es handele sich um digitale Recheneinheiten, die nicht von Zentralbanken, Kreditinstituten oder e-money Institutionen als alternative Währung ausgegeben werden (ECB, 2015).

In den letzten Monaten hat die EZB über ihre Pressestelle folgende Aussagen zu Kryptowährungen abgegeben (Finanznachrichten, 2017); (European Central Bank, Digital Transformation of the retail payments ecosystem, 2017).

- Der Einfluss von Kryptowährungen erscheint bislang zu gering, um diese regulieren zu müssen. Die Regulierung von Kryptowährungen liegt nicht im Zuständigkeitsbereich der Zentralbank.
- Digitale Kryptowährungen stellen keine Bedrohung für den Euro dar und würden somit keiner Kontrolle durch die EZB bedürfen.
- Die Auswirkungen der Kryptowährungen würden nur einen geringen Einfluss auf die Wirtschaft haben. Somit sei das Monopol der Zentralbanken für Geld nicht gefährdet.
- Kein Land der Europäischen Union sei befugt neben dem Euro seine eigene Währung einzuführen.

EZB, Bundesbank, BaFin sowie weltweite aufsichtsrechtliche Institutionen und Zentralbanken stehen in einem permanenten Austausch zu diesem Thema. Sie sind sich der Chancen und Risiken bewusst, die sich durch ein verstärktes Investment der Bevölkerung in Kryptowährungen ergeben. Für die EZB stehe dabei die Frage der Cyber-Sicherheit an oberster Stelle. Präsident Draghi führte in den letzten Aussagen (Stand Januar 2018) aus, dass man aus den Finanzkrisen in der Vergangenheit gelernt habe und solche finanziellen Innovationen und deren Risiken mit großer Aufmerksamkeit beobachtet werden müsse (Finanzen, Finanzen, 2017).

1.6. Einordnung durch die Bundesbank

Der Präsident der Deutschen Bundesbank, Jens Weidmann, deklarierte die Bezeichnung der „Digitalwährung“ für den Bitcoin erst kürzlich als irreführend. Er begründete dies damit, dass ein Zahlungsmittel eine Wertstabilität aufweisen sollte. Dies sei jedoch beim Bitcoin nicht der Fall (Handelsblatt, 2017). Der hohe Kurs des Bitcoins liegt

für ihn einzig in der Hoffnung auf eine hohe Rendite begründet und nicht in seinem fairen Wert (Finanzen.net, 2017).

Der Anleger könne nur an der Kursentwicklung partizipieren. Es könnten keine Erträge in Form von Zinsen gezahlt werden und der Bitcoin weise auch keine Korrelation zu anderen Assets auf (Börsen-Zeitung, 2017); (Hanke, 2017).

Für Spezialisten der Deutschen Bundesbank ist der Bitcoin als Währung nicht vorstellbar. Eine Währung beruht auf Vertrauen. Zu dieser Währung sollte kein Vertrauensverlust entstehen können. Ebenso schließen sich die Begriffe staatlich und kryptographisch gegenseitig aus, da diese im Charakter gegensätzlich seien.

Der Bitcoin ist eine „deflationäre Währung“. Da die Geldmenge auf eine bestimmte Anzahl begrenzt ist, sinkt diese auf lange Frist immer weiter. Somit werden technische Änderungen durch den Einigungsprozess sehr schwierig sein und das generelle Handling aus Verbrauchersicht kompliziert. Das Eurosystem sei derzeit dabei, digitales Zentralbankgeld für Nichtbanken zu erforschen. Jedoch überwiege hier allgemein die Skepsis, da bisher keine Abwicklungsvorteile gesehen werden. Die Deutsche Bundesbank sieht ebenfalls keine Notwendigkeit für ein digitales Zentralbankgeld. Ein großer Kritikpunkt werde bei einem möglichen Insiderhandel, begünstigt durch die Anonymität der Marktteilnehmer gesehen (Bundesbank I., 2017).

Die Deutsche Bundesbank warnte im Januar 2018 Privatanleger vor einem Investment in digitale Währungen. Bislang erachtet sie jedoch kein Verbot der Kryptowährungen für notwendig.

1.7. Einordnung durch die BaFin

Die BaFin verwendet den Begriff VC für „Virtual currencies“. Kryptowährungen, wie beispielsweise Bitcoin, Ethereum, Ripple und Litecoin werden als „digitale Abbildung von Wert, der nicht von einer Zentralbank oder Behörde geschaffen wird und auch keine Verbindung zu gesetzlichen Zahlungsmitteln haben muss“ definiert. Sie werden von natürlichen und juristischen Personen als Zahlungs-/ und Tauschmittel verwendet, und können digital verwahrt, gehandelt, oder übertragen werden.

Anders als bei Zentralbankgeld, das Notenbanken theoretisch unbegrenzt ausgeben können, und bei dem Buchgeld, das von Geschäftsbanken geschaffen wird, erfolgt die Generierung neuer Werteinheiten über ein mathematisches Verfahren innerhalb eines Computernetzwerks. Diese Generierung wird als „Mining“ bezeichnet (BaFin, Virtuelle Währungen/Virtual Currency, 2016).

Die BaFin hat Bitcoins gemäß §1 Absatz 11 Satz 1 Kreditwesengesetz (KWG) rechtlich verbindlich als Finanzinstrumente qualifiziert. Jedoch ist die bloße Nutzung von VC als Ersatz für Bar- oder Buchgeld zur Teilnahme am Wirtschaftskreislauf im Austauschgeschäft keine erlaubnispflichtige Tätigkeit. (BaFin, Virtuelle Währungen/Virtual Currency (VC), 2016). Rechnungseinheiten lauten nicht auf gesetzliche Zahlungsmittel. Hierunter fallen auch Werteinheiten, die die Funktion von privaten Zahlungsmitteln bei Ringtauschgeschäften haben, sowie jede andere Ersatzwährung, die aufgrund privatrechtlicher Vereinbarungen als Zahlungsmittel in multilateralen Verrechnungskreisen eingesetzt wird. Diese rechtliche Einordnung gilt grundsätzlich für alle VC. Auf die zugrundeliegende Software oder Verschlüsselungstechnik kommt es hierbei nicht an.

VC sind dagegen kein gesetzliches Zahlungsmittel und daher weder Devisen noch Sorten. Sie sind auch kein E-Geld im Sinne des Zahlungsdienstleistungsgesetzes (ZAG), da es keinen Emittenten gibt, der sie, unter Begründung einer Forderung gegen sich, ausgibt.

Die bloße Nutzung von VC als Ersatz für Bar- oder Buchgeld zur Teilnahme am Wirtschaftskreislauf im Austauschgeschäft ist keine erlaubnispflichtige Tätigkeit. Der Dienstleister oder Lieferant kann seine Leistungen mit VC bezahlen lassen, ohne dass er dadurch Bankgeschäfte oder Finanzdienstleistungen erbringt. Gleiches gilt für den Kunden. Ebenso stellt das Mining von VC an sich kein erlaubnispflichtiges Geschäft dar, da der „Miner“ die VC nicht selbst emittiert oder platziert. Auch der Verkauf selbst geschürfter oder erworbener VC oder deren Ankauf sind grundsätzlich nicht erlaubnispflichtig.

Erlaubnispflichten für Plattformen und Börsen

Der gewerbliche Handel mit VC erfolgt meist über Plattformen, die häufig auch als Börsen bezeichnet werden. Unter diesen Begriff werden viele verschiedene Geschäftsmodelle zusammengefasst. Geht es um die Frage der Erlaubnispflicht, muss aber nach der technischen Umsetzung und der jeweiligen Ausgestaltung der Geschäfte differenziert werden. Derjenige, der im eigenen Namen gewerbsmäßig VC für fremde Rechnung an- und verkauft, betreibt das erlaubnispflichtige Finanzkommissionsgeschäft. Die Anschaffung oder Veräußerung der VC erfolgt für fremde Rechnung, wenn die wirtschaftlichen Vor- und Nachteile aus diesem Geschäft den Auftraggeber treffen. Des Weiteren muss die Tätigkeit dem Kommissionsgeschäft nach dem Handelsgesetzbuch hinreichend ähnlich sein, wobei einzelne Rechte und Pflichten vom typischen Kommissionsgeschäft abweichen können.

Bei VC-Plattformen ist daher das erlaubnispflichtige Finanzkommissionengeschäft erfüllt, wenn:

- 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 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 VC auf deren Adressen übertragen.
- Die Plattform verpflichtet ist, den Teilnehmern über die Ausführung der Geschäfte Rechenschaft abzulegen und angeschaffte VC zu übertragen.

Liegt bei Plattformen kein Finanzkommissionengeschäft vor, kann es sich um den Betrieb eines multilateralen Handelssystems handeln. Dieses bringt die Interessen einer Vielzahl von Personen am Kauf und Verkauf von Finanzinstrumenten innerhalb des Systems nach festgelegten Bestimmungen in einer Weise zusammen, die zu einem Vertrag über diese Finanzinstrumente führt. Dies bedeutet, dass ein Regelwerk über die Mitgliedschaft, den VC-Handel zwischen den Mitgliedern und Meldungen über abgeschlossene Geschäfte vorliegt. Eine Handelsplattform im technischen Sinne ist nicht erforderlich.

Multilateral bedeutet, dass der Betreiber nur die Parteien eines potenziellen Geschäfts über VC zusammenbringt. Als Interesse am Kauf und Verkauf zählen auch Interessenbekundungen, Aufträge und Kursofferten. Eine Vielzahl von Personen bedeutet vor allem, dass es keinem Auftrag zur Vermittlung im Einzelfall bedarf. Die Interessen müssen nach dem Regelwerk durch Software oder Protokolle zum Vertragsabschluss zusammengeführt werden, ohne dass die Parteien im Einzelfall entscheiden können, ob sie ein VC-Geschäft mit einem bestimmten Vertragspartner eingehen wollen. Ob der Vertrag anschließend innerhalb des Systems abgewickelt wird, ist ohne Belang.

Multilaterale Handelssysteme sind daher insbesondere bei Plattformen naheliegend, bei denen Anbieter VC einstellen und eine Preisschwelle festlegen, ab der ein Handel abgewickelt werden soll, oder bei denen Anbieter Transaktionen durch eine Hinterlegung absichern, indem sie der Plattform VC übertragen und diese erst freigegeben werden, wenn der Anbieter die Zahlung bestätigt.

Bei Plattformen mit dem Angebot regional gegliederter entgeltlicher Verzeichnisse von Personen oder Unternehmen, die VC zum Kauf oder Verkauf anbieten, handelt es sich regelmäßig um die Anlage- und Abschlussvermittlung.

Erlaubnispflichten beim Mining

Anbieter, die als „Wechselstuben“ gesetzliche Währungen in VC oder VC in gesetzliche Währungen umtauschen, erfüllen den Tatbestand des Eigenhandels. Dieser liegt dann vor, wenn VC nicht nur geschürft, gekauft oder verkauft werden, um damit an einem bestehenden Markt zu partizipieren, sondern ein besonderer Beitrag geleistet wird, um diesen Markt zu schaffen oder zu erhalten. Aufgrund des zusätzlichen Dienstleistungselements handelt es sich dann um erlaubnispflichtigen Eigenhandel. Dies ist etwa der Fall, wenn eine Person öffentlich damit wirbt, dass sie regelmäßig VC an- oder verkauft.

Zwar stellt das Mining von VC an sich kein erlaubnispflichtiges Geschäft dar, bieten jedoch Mining-Pools gewerblich Erlösanteile aus geschürften und veräußerten VC z. B. gegen die Überlassung von Rechnerleistung durch den Nutzer an, sind sie i. d. R. erlaubnispflichtig tätig.

Die BaFin hat am 29. Januar 2018 eine umgehende Einstellung des Finanzkommissionsgeschäfts der Crypto.exchange GmbH in Berlin angeordnet. Das Geschäft sei entgegen der Eigenwerbung ohne Erlaubnis der BaFin betrieben worden.

Keine Einordnung als Geld oder Währung

Kryptowährungen haben keinen intrinsischen Wert. Durch ihren dezentralen Charakter besteht keine Rücknahmepflicht durch einen Emittenten und auch kein Pfand, der als Sicherheit dient. Ebenso gibt es keine vorgegebene Steigerungsrate, wodurch die Zahl der Kryptowährungen schnell steigt. Die volatilen Wertschwankungen des Bitcoins sind auf das Fehlen des intrinsischen Wertes sowie der fehlenden Verantwortlichkeit eines Emittenten zurückzuführen. Somit ist der Bitcoin kein Geld sondern ein Spekulationsobjekt, da der Preis beliebig bis zum Totalverlust variieren kann (Thiele, 2017).

Da bisher in keinem Land weltweit Kryptowährungen als gesetzliches Zahlungsmittel anerkannt wurden, handelt es sich um Währungssurrogate beziehungsweise um Komplementärwährungen (Sixt, 2016).

Bei Kryptowährungen ist die Zahlungsmittelfunktion durch die geringe Anzahl der Akzeptanzstellen stark eingeschränkt. Ebenso fallen für eine Transaktion hohe Gebühren an (Bundesbank I., 2017).

Im Vergleich zu Bargeld kann bei einem Verlust des privaten Schlüssels als Zugang zum „Wallet“ oder bei einem Festplattendefekt ein Totalverlust drohen. Zudem sind durch die geringe Verbreitung der Kryptowährungen und das Fehlen der Verantwortung einer Emissionsbehörde Bitcoins unter Umständen nicht jederzeit wieder veräußerbar und in eine offizielle Währung tauschbar (Bundesbank, Kryptowährungen, 2017).

Bei elektronischem Geld handelt es sich nach der E-Geld-Richtlinie um einen elektronisch oder auch magnetisch gespeicherten monetären Wert. Dieser wird in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird, um damit Zahlungsvorgänge durchzuführen, definiert. Ebenso muss er auch von anderen natürlichen oder juristischen Personen als dem E-Geld-Emittenten akzeptiert werden. Somit ist der Bitcoin dem E-Geld nicht zuzuordnen, da zwar die elektronische Speicherung und Akzeptanz zutreffen, aber keine Forderung gegenüber einem Emittenten vorliegt (Sixt, 2016).

Ein Emittent ist für die Aufsichtsbehörden nicht greifbar und es wird auch kein Dritter für die Durchführung der Zahlungsvorgänge mit einbezogen, da die Bitcoin-Überweisungen von Rechner zu Rechner (Peer-to-Peer) erfolgen (Hussein, 2017).

Der Kursanstieg von Kryptowährungen sei reine Spekulation. Nach Ansicht der Deutschen Bundesbank ist der hohe Kurs des Bitcoins allein in der Hoffnung der Anleger/Spekulanten auf eine hohe Rendite begründet. Der Kurs spiegelt somit keinen fairen Wert wieder (dpa-AFX, 2018).

Aus unserer Untersuchungssicht handelt es sich um digitale Recheneinheiten.

ESMA	EBA	EZB	Bundesbank	BaFin
<p>Warnung Anleger (12/2017)</p> <ul style="list-style-type: none"> Investitionen in ICOs seien sehr riskante und hochspekulative Investments. Ein Totalverlust des investierten Vermögens sei möglich, ebenso könne es betrügerische Absichten der Geldeinwerber geben. Keine Aussage zu Tokens / Wallets 	<p>Warnung Anleger (7/2014)</p> <ul style="list-style-type: none"> Risiken zu virtuellen Währungen und Wallets Hohe Volatilität Vollständiger Verfall Transaktionen sind öffentlich, daher ist das System auch anfällig gegenüber Geldwäsche und Terrorismus 	<p>Warnungen Anleger über Studien und Presse (seit 2011)</p> <ul style="list-style-type: none"> Es handelt sich um digitale Recheneinheiten und keine Währung Erste Studie im Jahr 2012, weitere 2015 Virtuelle Währungen sind nicht Geld oder Währung. Keine Kontrolle durch die EZB Jedoch kein Verbot von Kryptowährungen Projekt zur DLT mit Bank of Japan 	<p>Warnung Anleger in 2018, Presse & Studien seit 2017</p> <ul style="list-style-type: none"> Bezeichnung Digitalwährung ist irreführend Keine offizielle Währung und keine Notwendigkeit Sehen Bitcoin als deflationäre Währung Kompliziertes System Möglicher Insiderhandel durch Anonymität Jedoch kein Verbot von Kryptowährungen Internes Projekt zur DLT mit Deutscher Börse 	<p>Warnung Anleger (11/2017)</p> <ul style="list-style-type: none"> Digitale Abbildung von Wert, Einstufung als Finanzinstrument in Form von Recheneinheiten Einstufung als kein gesetzliches Zahlungsmittel und daher weder Devisen noch Sorten. Kein E-Geld Aussagen zu erlaubnispflichtigen Tätigkeiten für Privatanleger, Plattformen, Börsen und Minern

Abbildung 3: Übersicht Kernaussagen der Aufsichten zu ICO

Beim Mining wird ein Nummernkreis eines Codes um 12,5 Bitcoins fortgeschrieben. Das ist nichts anderes als ein Hinzuaddieren von Zahlen. Diese Zahl (derzeit 12,5) halbiert sich alle 210.000 Blocks (vgl. bitcoinmining.com, 2017). Somit ist mathematisch ein Maximum bzw. eine Asymptote logisch. Dies ist bei dem aktuell akzeptierten Protokoll 21 Millionen. Das Generieren von Bitcoins ist rechnerisch im Jahr 2130 erreicht (Dörken, 2018).

Mit der Schaffung des Bitcoins ging es Nakamoto vielmehr um die Schaffung eines modernen bargeldähnlichen Zahlungsinstruments, um sich dem digitalen Zeitalter anzupassen. Da keine Banken oder Zahlungsdienstleister mit eingebunden sind und somit ein direkter Übertrag stattfindet, wurde eine Wertheinheit kreiert, die nicht auf dem Vertrauen in eine bestimmte Institution, eine Notenbank, basiert (Thiele, 2017).

Kryptowährungen basieren auf einem dezentralisierten Peer-to-Peer System (Nakamoto, 2008). Somit gibt es keinen zentralen Server und dementsprechend auch keine Möglichkeit zu einer zentralen Aufsichtsinstitution, da diese Aufgabe auf alle Teilnehmer des Netzwerks verteilt ist. Ein wichtiger Bestandteil dieses Systems sind die Miner. Sie sind das Prüforgang oder Sinnbildlich auch die Buchhalter eines Blockchain-Systems. Ein Miner verifiziert jede Transaktion und teilt diese über das Netzwerk. Andere Teilnehmer prüfen diese Verifizierung und bestätigen diese auf Richtigkeit (Klotz, 2018).

1.8. Steuerrechtliche Behandlung in Deutschland

Die steuerliche Behandlung von Geschäften mit Kryptowährungen ist in Deutschland noch nicht geregelt. Das zuständige Bundesministerium für Finanzen hat hierzu noch keine Stellungnahme abgegeben. Somit ist die Besteuerung aus den Einordnungen und Einstufungen der Kryptowährungen zu erschließen.

Das Mining stellt eine selbständige, nachhaltige, mit Gewinnerzielungsabsicht verbundene Tätigkeit dar. Dabei nimmt der Miner am allgemeinen wirtschaftlichen Verkehr teil. Die Einkünfte, die dabei erzielt werden, sind den Einkünften aus einem Gewerbebetrieb zuzuordnen und somit zu versteuern. Alle mit dem Mining verbundenen Ausgaben können steuerlich geltend gemacht werden. Ab einem Gewinn von 24.500 Euro fällt das Mining schließlich unter die Gewerbesteuerpflicht (Roland, Besteuerung von Kryptowährungen, 2017 a).

Kryptowährungen sind im Privatvermögen als immaterielle Wirtschaftsgüter einzuordnen. Damit fallen Verkäufe unter das private Veräußerungsgeschäft nach §23 EStG. Folglich gilt bei diesen die Spekulationsfrist von einem Jahr (Roland, Besteuerung von Kryptowährungen, 2017 a). Der §20 EStG, nach dem Kapitalertragsteuer auf Veräußerungsgeschäfte anfällt, greift nicht. Dabei ist bei Veräußerung nach weniger als einem Jahr der persönliche Steuersatz (bis maximal 45%) anzuwenden (Roland, Bitcoin Kapitalertragsteuer: Vorsicht vor Fakenews, 2017 b). Bei der Bewertung gilt „First in first out“.

Gewinne bleiben steuerfrei, wenn der aus den privaten Veräußerungsgeschäften erzielte Gesamtgewinn im Kalenderjahr weniger als 600 Euro betragen hat (Einkommensteuergesetz, 2017, §23, Absatz 3). Wird diese Grenze überschritten, ist der gesamte Gewinn steuerpflichtig. Erfolge aus der Veräußerung sind in der Steuererklärung in der Anlage SO (Sonstige Einkünfte) unter Angabe von Kauf- und Verkaufskurs, abzüglich der Gebühren, zu erfassen (VLH, 2017). Die bei Kapitalerträgen anzuwendende Kapitalertragssteuer erhält nur Bedeutung, wenn Zinsen aus der Leihe von Bitcoins in Bitcoins bezahlt werden würden. Dann sind die gezahlten Bitcoin Zinsen mit der Kapitalertragssteuer zu besteuern (Roland, Besteuerung von Kryptowährungen, 2017 a).

Der Tausch von Bitcoin in eine andere Währung ist nach Aussage des EuGHs umsatzsteuerfrei, da Gebühren, die beim Tausch anfallen, lediglich die Kosten des Arbeitsaufwandes, der beim Wechsel anfällt, decken. Demnach ist dieses Geschäft mit dem normalen Devisengeschäft zu vergleichen (Haufe, 2015).

1.9. Regulierungen im asiatischen Raum

Die nachfolgenden Erläuterungen basieren auf dem Stand vom Januar 2018. Da im asiatischen Raum insbesondere China, Japan und Südkorea zu den wichtigsten Bitcoin Nationen zählen und dort rund 80% der Miner sitzen wurde hier eine ausführlichere Erläuterung vorgenommen.

1.9.1. China

In keinem anderen Land werden so viele Minen der Kryptowährung betrieben wie in China. Zudem gibt es dort die meisten Privatanleger und Investoren, welche Geld in Bitcoins angelegt haben. Trotz des großen Vertrauens vieler Anleger in Bitcoin ist der chinesische Staat skeptisch. Folglich haben die Regulierungsbehörden in Peking im September 2017 ICOs für illegal erklärt. Kurze Zeit danach schlossen die Regulierungsbehörden zudem die Handelsplattformen des Landes.

Diese durch die Behörden erlassenen Regulierungen bedeuten jedoch nicht, dass der Besitz einer Kryptowährung in China verboten sei. Wer Bitcoins in seinem Wallet hält, darf diese behalten oder auch mit anderen Besitzern handeln und tauschen. Lediglich der organisierte Handel von Kryptowährungen auf Internetplattformen ist in China nicht mehr erlaubt.

Anlass zu den Regulierungen gaben missbräuchliche Verwendungen des Bitcoins durch Umgehen der Kapitalverkehrskontrollen der Volksrepublik China. Hierbei wurde Vermögen mithilfe von Kryptowährungen außer Landes geschafft, wodurch die Zentralbank dies zukünftig mit neuen Regulierungsmaßnahmen zu verhindern versuche (Handelsblatt, Globaler Hype um Bitcoin und Co., 2017).

Im Januar 2018 gaben die Regulierungsbehörden in China Maßnahmen zur Reduzierung des Minings aus. So können die lokalen Behörden in China Einfluss auf die Miningfabriken nehmen. Dies erfolge über die Bestimmung der Strompreise, die Landnutzung der Mining-Farmen sowie mit steuerlichen Maßnahmen oder Umwelt-Vorschriften. Infolge dessen werde der Strom für einige Miner zu teuer, was diese zu einer Abwanderung in ein anderes Land bewege. So soll die größte Mining-Farm Chinas bereits Fuß in Singapur, USA und Kanada gefasst haben. Anlass zur Erhöhung der Strompreise ergaben Schätzungen von Experten, dass 70 % des weltweiten Minings in China betrieben werde und zu einem extrem hohen Energieverbrauch führe. Daher drohe in China die Gefahr, dass zukünftig ein generelles Verbot für Mining-Rechenzentren verhängt werde könne (Schürmann, 2018). Die lokalen Behörden erhielten bereits am 10. Januar 2018 die Anweisung, einen Ausstieg einzuleiten. So soll die Umsetzung in der westlichen Region Xinjiang bereits begonnen haben und das Bitcoin-Mining verboten werden (Finanzen, 2018).

1.9.2. Japan

Japan ist in den letzten Jahren als eines der Zentren des Bitcoins immer bekannter geworden. Bevor die japanische Börse Mt. Gox mit dem Boom der Kryptowährungen kollabierte, hatte Japan den größten Krypto-Handelsplatz der Welt. Ebenso wurden die Finanzaufsichter mit dem Zusammenbruch von Mt. Gox früh dazu gezwungen, sich mit der Regulierung der Kryptowährungen zu beschäftigen. Um zu einem digitalen Vorreiter im Bereich dieser zu werden, entschieden sich die Aufsichter und Banken Japans, kein Verbot gegen diese auszusprechen.

Mit der Zulassung von Kryptowährungen als Zahlungsmittel können japanische Kunden seit April in einer Vielzahl von Geschäften und großen Einzelhandelsketten mit dem neuen Zahlungsmittel bezahlen. Im Oktober 2017 hat die japanische Finanzaufsicht eine Regelung erlassen, wodurch Krypto-Börsen Mindestbedingungen einhalten müssen, die auch von jener kontrolliert werden. Mit dieser Maßnahme soll eine finanzielle und technische Stabilität aufgebaut und neues Vertrauen geschaffen werden, indem betrügerische Aktivitäten verringert werden können.

Aufgrund der staatlichen Unterstützung und der somit vorherrschenden Sicherheit, würden einige Banken in Finanz-Startups verschiedener Arten in Japan investieren. (Handelsblatt, Globaler Hype um Bitcoin und Co., 2017).

Die japanische Finanzaufsicht FSA hat Coincheck, einen der größten Händler für Kryptowährungen Ende Januar 2018 gemahnt, nicht ausreichend auf Hackerangriffe vorbereitet zu sein. Auch die japanische Polizei nahm Ermittlungen gegen Coincheck auf. Am 26. Januar 2018 hatte Coincheck den Verlust von 523 Millionen Einheiten der Kryptowährung NEM im Wert von 58. Mrd. Yen (430 Mill. €) gemeldet. Der Handel mit allen Kryptowährungen außer Bitcoin wurde daraufhin eingestellt. Durch eine strenge Regulierung wolle die FSA verhindern, dass sich ein weiterer schwerer Diebstahl wie bei der Bitcoin Börse Mt. Gox im Februar 2014 ereigne (Börsenzeitung, 2018).

1.9.3. Südkorea

Die Regierung in Südkorea plant, dass Konten für Kryptowährungen zukünftig nicht mehr anonym und somit unter Angabe des realen Namens der Kunden geführt werden müssen. Ebenso sollen ab Januar 2018 alle anonym genutzten Konten geschlossen werden (Manager-Magazin, 2017). Mit dieser Maßnahme soll die Spekulation mit Kryptowährungen verringert und die Maßnahmen zur Bekämpfung der Geldwäsche verschärft werden.

Zudem soll ein neues Gesetz eingeführt werden, dass die Aufsichtsbehörden ermächtigt wird, Börsen, an denen Kryptowährungen gehandelt werden, schließen zu dürfen, wenn sie den neuen Regelungen nicht nachkommen. Eine weitere Neuerung wird eine Reform zur Besteuerung von Kapitalerträgen aus diesen Handelsgeschäften sein.

Seit dem Handelsverbot von Kryptowährungen in China ist Südkorea zum wichtigsten Handelsplatz für Bitcoins in Asien gewachsen. Durch den gestiegenen Einfluss Südkoreas wirken sich die geplanten Regulierungsmaßnahmen stark auf den Kurs des Bitcoins aus. So fiel der Kurs am 28. Dezember 2017 durch Bekanntgabe der geplanten Regulierungsmaßnahmen auf unter 14.000 USD und verlor somit um 11%.

Der Hintergrund für die geplante Regulierung sei das Risiko des starken Kursanstiegs, da viele Bürger Südkoreas in Bitcoin investiert haben. So sollen zwei Millionen der 51 Millionen Bevölkerung bereits mit durchschnittlich 5000 Euro in Kryptowährungen investiert haben. Daher fühlt sich die Regierung Südkoreas verantwortlich, in die Spekulationen um die zukünftigen Kurserwartungen einzugreifen (Kölling, 2017).

Des Weiteren kam es am 11. Januar 2018 zu erneuten Kurseinbrüchen der Kryptowährungen. Der Bitcoin fiel hierbei um 10% auf 13.100 Dollar, erholte sich aber anschließend wieder (Kessler, 2018). Diese Turbulenzen wurden durch Einleiten der Maßnahmen eines Handelsverbots für Kryptowährungen im Land ausgelöst. An neuen Gesetzen solle derzeit gearbeitet werden (SPIEGEL, 2018).

2. Handel und Marktplätze

Stand Anfang Februar 2018 wurden weltweit 1514 Virtual Currency auf über 8655 Online-Marktplätzen gehandelt. Es gibt verschiedene Möglichkeiten Kryptowährungen zu erwerben. Sie können nicht nur gekauft werden, sondern dienen auch zum Tausch von Gütern und Dienstleistungen. Möglichkeiten zum Erwerb bestehen durch:

- 1) Kauf an Kryptobörsen,
- 2) Kauf auf Handelsplattformen, direkt von privaten Anbietern.

2.1. Kryptobörsen

Stand April/2018 gab es 10.654 Online Marktplätze an denen über 1580 Kryptowährungen angeboten werden. (Coinmarketcap, 2018). Bevor die Kryptowährungen über die Börsen gekauft und verkauft werden benötigt der Anleger ein Wallet – einen digitalen Aufbewahrungsort. Der Anleger kann sich durch Eingabe einer E-Mail-Adresse, eines Passworts und eines Benutzernamens bei einer Börse registrieren und ein Konto eröffnen. Unterhalb eines bestimmten Handelsvolumens ist es möglich, anonym zu bleiben. Jedoch verlangen die meisten Börsen ab einem bestimmten Handelsvolumen aus Sicherheitsgründen und der Vorschriften des Geldwäschegesetzes die Identifizierung der Benutzer. Das maximal handelbare Volumen variiert je nach Börse. Die Handelsplattformen entscheiden, welche Kryptowährungen zur Verfügung stehen und mit welchen anderen Währungen diese gehandelt werden können (Weiprecht, 2018). Alle Online-Börsen bieten 24-Stunden Handelsmöglichkeiten. Englisch ist die Hauptsprache neben der Landsprache des Börsenanbieters. Der Handel an den Börsen erfolgt automatisiert, während die Trades auf einem Marktplatz manuell abgewickelt werden (Finanzen, Bitcoin kaufen – diese Möglichkeiten gibt es, 2017). Benutzer können die Kryptowährungen außerdem untereinander handeln, zum Beispiel Bitcoins gegen Ethereum, Ripple oder Ähnlichen. Selbstverständlich können Bitcoins auch gegen herkömmliche Währungen, zum Beispiel USD, Euro oder Yuan gewechselt werden. Findet die Börse ein passendes Angebot, so kauft sie im Kundenauftrag die Bitcoins und schreibt diese dem Kunden anschließend gut (Finanzen, 2018).

Im Folgenden werden die fünf wichtigsten Börsen mit ihren Merkmalen kurz erläutert:

Poloniex ist die volumenmäßig größte Tauschbörse für Kryptowährungen mit Sitz in den USA (kryptocoins.net; Tuwiner, 2017). Die Hauptwährung dieser Börse ist in der Regel Monero – eine dezentrale Blockchain-basierte Kryptowährung – und Bitcoin (Kryptocoins.net, 2017).

Bittrex gehört ebenso zu den größten Tauschbörsen für Digitalwährungen (kryptocoins.net). Seit April 2014 ist die Börse aktiv und hat ihren Sitz in den USA. Neben der wichtigsten digitalen Währung Bitcoin können auf dieser Tauschbörse über 200 verschiedene Kryptowährungen gehandelt werden, wie beispielsweise Dash, Litecoin und Ethter (aktienrunde, 2017). Die Bitcoin-Börse Bittrex wird vor allem von vielen erfahrenen Tradern genutzt (kryptocoins.net).

Kraken ist einer der weltweit größten Bitcoin-Börsen mit Sitz in den USA. Nach eigenen Angaben verzeichnet die Kryptobörse das weltweit größte Handelsvolumen zwischen Digitalwährungen und Euro. Zudem zeichnet sich die Börse durch die Kooperation mit der Fidor-Bank aus, wodurch ein zuverlässiger und schneller Handel gewährleistet werden kann. Um das Angebot aufzubessern, arbeitet die Kryptobörse kontinuierlich an Sicherheitsstandards. Die Nutzung von Kraken ist kostenfrei. Es fallen lediglich Gebühren für den Kauf beziehungsweise Tausch von Kryptowährungen an (Bitcoinmag.de, 2017).

Bitfinex ist nach eigenen Angaben zufolge die größte und fortschrittlichste Bitcoin-Börse weltweit (Broker-Bewertungen.de, 2017), welche sich auf den Kryptowährungshandel und Fiat-Währungen spezialisiert (aktienrunde, 2017). Die Börse hat ihren Hauptsitz in Hongkong (broker-bewertungen.de, 2017). Bitfinex bietet den Nutzern die Möglichkeit virtuelle Währungen, wie beispielsweise Bitcoins in echtes Geld einzutauschen. Allerdings ist der Tausch von Kryptowährungen untereinander hierbei nicht möglich (aktienrunde, 2017).

Bitstamp gehört zu den bekanntesten und führenden Bitcoin Börsen weltweit (Broker-Bewertungen.de, 2017). Diese Börse ist die erste staatlich lizenzierte Plattform (aktienrunde, 2017). Sie hat ihren Sitz nach der Lizenzierung von Slowenien nach Luxemburg verlegt. Bitstamp ist die erste Bitcoin Börse, die im Juli 2016 eine EU-Lizenz als Zahlungsinstitut erhielt. Damit bekam die Börse eine Zulassung für ihren Handel und kann somit ihre Dienste rechtssicher EU-weit anbieten. Es ist die erste derartige Zulassung, die von einem EU-Land an einen Bitcoin-Dienstleister vergeben wurde (Kannenberg, 2017). Die Börse besitzt das zweitgrößte Handelsvolumen (Broker-Bewertungen.de, 2017).

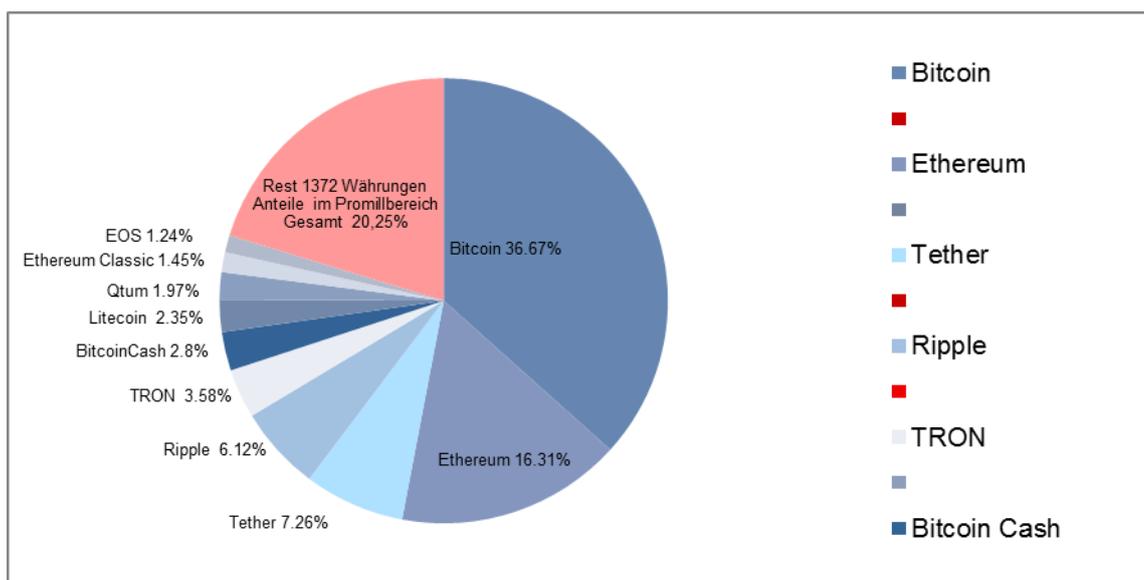
Die folgende Tabelle vergleicht die wesentlichen Handelsplattformen hinsichtlich des Angebots der Kryptowährungen und der anfallenden Gebühr je ausgeführte Transaktion.

Börse	Angebot	Gebühr	Sitz
Poloniex	BTC, ETH, BCH, XRP, LTC, NEM, DASH, ETC, XMR, STRAT, ZEC, (+60 Coins)	0,15%	USA
Bittrex	BTC, ETC, BCH, XRP, LTC, NEO, XEM, ETC, DASH, XMR, LSK, STRAT, UBO, KMD, MLN, WAVES, GAME, STEEM, SYS, MAID, GNT, SC (+190 Coins)	0,25%	USA
Kraken	EUR, USD, BTC, ETH, BCH, XRP, LTC, DASH, ETC, XMR, EOS, MLN, (+17 Coins)	0,16%	USA
Bitfinex	EUR, USD, BTC, ETH, BCH, XRP, IOTA, LTC, DASH, ETC, NEO, BCC, OMG, XMR, EOS, ZEC, QTM, AVT, EDO, BTG (+14 Coins)	0,10%	Hongkong
Bitstamp	EUR, USD, BTC, ETH, XRP, LTC	0,25%	Luxemburg

Abbildung 4: Kryptobörsen im Vergleich

Das nachfolgende Schaubild verdeutlicht den Anteil der zehn umsatzstärksten Kryptowährungen im Q4/2017 (Coinmarketcap, 2018). Bitcoin und Ethereum führen zusammen mit über 50% Umsatz die Handelsliste an. Im Mittelfeld bewegen sich im einstelligen Prozentbereich sechs bis acht teils bekannte Namen. Der größte Teil der über 1.300 gelisteten Kryptowährungen liegen im Umsatz unter 1%, teils auch nur im Promillebereich.

Abbildung 5: Umsatzstärkste Kryptowährungen



2.2. Kauf auf Handelsplattformen

Auf verschiedenen Handelsplattformen können direkt von Privatpersonen Bitcoins erworben werden. Ähnlich wie bei Auktionsportalen oder Kleinanzeigen – wie beispielsweise Ebay – bieten Nutzer auf dieser Plattform ihre Bitcoins an. Findet der Käufer ein passendes Angebot, kann dieser direkt mit dem Verkäufer in Kontakt treten.

Zu den Online-Händlern gehören unter anderem coinmama.com und bitpanda.com. Die Zahlung kann über verschiedene Online-Zahlungsmöglichkeiten, beispielsweise über SEPA oder Giropay, erfolgen. Nach der Bezahlung können schließlich die erworbenen Bitcoins anhand eines bereitgestellten Codes kostenlos in ein Wallet, transferiert werden (Schillmann, 2017). Zu den bekanntesten Anbietern gehören Blockchain.info und Coinbase.com. Coinbase aus den USA stellt die größte Wechselstube weltweit für den Handel von Bitcoins und anderen Kryptowährungen dar (Niggemann, 2017).

2.3. Risiken für Anleger

Verlustrisiko

Aufgrund fehlender gesetzlicher Grundlagen, Vorgaben und Transparenzvorschriften für ICOs besteht für den Anleger entsprechend ein großes Risiko. Des Weiteren bestehen Verlustrisiken bis hin zu einem Totalverlust der eingebrachten Investition (BaFin, Journal Initial Coin Offering, 2017).

Volatilität

Ein weiteres Risiko sind die großen Schwankungen der Token-Preise, bei dem die Anbieter den Handel der Tokens auf möglicherweise unregulierten Zweitmarktplattformen versprechen. Die Anleger haben jedoch keinen Anspruch auf Verkauf ihrer vorhandenen Tokens und können diese eventuell nicht oder nur zu einem unter den Erwartungen liegenden Preis wieder veräußern. Um über die erworbenen Tokens verfügen zu können, ist der Anleger für die sichere Aufbewahrung des virtuellen Schlüssels (Private Key) verantwortlich. Ein Diebstahl oder Verlust des Private Keys bedeutet auch gleichzeitig ein Verlust aller Tokens (BaFin, Journal Initial Coin Offering, 2017).

Hacker-Angriffe

Seit der Erfindung von Bitcoin 2009 wurden ein Drittel der Handelsplattformen für Kryptowährungen gehackt. Bislang wurden insgesamt knapp eine Million Bitcoins gestohlen (Kölling, 2017). Die Sicherheitsinfrastruktur der Anbieter ist nicht ausreichend, um die Anleger vor solchen Angriffen zu schützen. Nach Angaben der Datenschutzorganisation Privacy Rights Clearinghouse lag die Quote bei US-Banken im gleichen Zeitraum bei 1% (Kölling, 2017). Am bekanntesten ist die Attacke auf die damals weltgrößte Bitcoin Börse Mt.Gox aus Japan im Februar 2014. Etwa 25.000 Kunden verloren rund 650.000 Bitcoins (Boerse-online, 2017). Daraufhin folgte für Mt.Gox offiziell der Konkurs. Das jüngste Hacker-Opfer ist die Kryptowährungsbörse Yobit am 19. Dezember 2017. Ihr wurden 17% der gesamten Krypto-Portfolios gestohlen. Daraufhin mussten auch sie später Konkurs anmelden (Boerse-online.de, 2017).

Frühphasenprojekte

ICO-Projekte befinden sich typischerweise meist in einer experimentellen Phase, in der weder ausreichende Kenntnisse über das Geschäftsmodell noch über die Entwicklung vorhanden sind (Müller, Palette der Bitcoin-Produkte wird breiter, 25.11.2017). Die Inhalte des Whitepapers werden durch den Anbieter festgelegt, in dem die Dokumentation meist schwer verständlich, verwirrend oder unvollkommen ist. Zusätzlich hat der Anbieter jederzeit die Möglichkeit, vor oder auch während des ICOs, das Whitepaper zu aktualisieren oder zu ändern (BaFin, Journal Initial Coin Offering, 2017).

Komplexität

Bei einer ausführlichen Beurteilung ist aufgrund der Komplexität ein weitreichendes technisches Verständnis erforderlich (BaFin, Journal Initial Coin Offering, 2017).

Betrugsrisiko

Ferner besteht bei ICO-Strukturen ein enormes Risiko für Betrug und Missbrauch. Nur Experten können anhand des zugrundeliegenden Programmiercodes (etwa des Smart Contracts) überprüfen, ob die im Whitepaper oder den Vertragsbedingungen angegebene Funktionsweise der jeweiligen Tokens zutrifft. Bei falschen Angaben der Anbieter trägt auch hier allein der Anleger das Risiko. Die systembedingte Anfälligkeit von ICOs für Betrug, Geldwäsche und Terrorismusfinanzierung erhöht zusätzlich das Risiko, dass Anleger ihr eingesetztes Kapital verlieren, auch aufgrund notwendiger Maßnahmen der Behörden gegen die Betreiber oder andere Personen, die in solche illegalen Geschäfte einbezogen werden (BaFin, Journal Initial Coin Offering, 2017).

Mining

Ein weiteres Risiko besteht in einem 51%-Angriff. Darunter wird ein Vorgang des Bitcoin-Minings verstanden, der die Kontrolle von über 50% der Blockchain beansprucht. Dabei kann eine Person oder eine Institution bei einer 50%igen Rechenleistung des Netzwerks möglicherweise Manipulationen durchführen und falsche Transaktionen bestätigen. Vergleichbar ist dieser Vorgang mit einer politischen Wahl, bei dem eine Person mehr als 50% der Stimmrechte besitzt. Bei Besitz dieser Stimmrechte könnte diese Person unabhängig von Entscheidungen der anderen Teilnehmer über den Beschluss entscheiden. Zu diesem Zeitpunkt könnte diese Person Transaktionen rückgängig machen, in der die Blockchain beeinträchtigt werden kann, da kein Vertrauen im Netzwerk mehr erhalten wäre. Bergbauaktivitäten werden zu diesem Zeitpunkt weltweit verteilt und das Netzwerk von Bitcoin komplett dezentralisiert. Bei einer Kontrolle von über 50% über die Blockchain durch einen Mining-Betrieb könnte zukünftig die Existenz Bitcoins gefährdet werden (Lielacher, 2017).

Regulatorisches Risiko

Die gesetzliche und regulatorische Einordnung ist für den zukünftigen Erfolg von Kryptowährungen wahrscheinlich das größte Risiko. Die Gründe für die Kursschwäche im Januar 2018 sind vermehrte Regulierungsschritte der Behörden. In Südkorea gibt es seit dem 30. Januar eine neue Vorschrift, die die Anonymität des Bitcoin Netzwerkes aushebelt. So muss künftig jedem Krypto-Konto ein Name zugeordnet werden, um Geldwäsche und Steuerflucht einzudämmen.

Die US-Börsenaufsicht SEC geht verstärkt gegen ICOs vor und die US-Aufsicht für Termingeschäfte CFTC hat Vorladungen an die Verantwortlichen der Handelsplattform Bitfinex und Tether zwecks Offenlegung der Geschäftsführungen verschickt.

Die BaFin hat am 29. Januar die umgehende Einstellung des Finanzkommissionsgeschäfts der Crypto.exchange GmbH in Berlin angeordnet. Das Geschäft sei entgegen der Eigenwerbung ohne Erlaubnis der BaFin betrieben worden. Wie schon erwähnt wird der G20-Gipfel im März 2018 sicherlich globale Regulierungsvorgaben hervorbringen.

2.4. Spekulationsblase Bitcoin

Bei Bitcoin, der bekanntesten Kryptowährung, war im Jahr 2017 ein Kursanstieg von über 1.500% zu verzeichnen. Somit stellen sich in der Makroökonomie Fragen nach der Bildung einer Spekulationsblase und möglichen Auswirkungen auf die Finanzmärkte und die Realwirtschaft. Zum Stichtag 13. Februar 2018 bestand eine Gesamtanzahl von 16,9 Millionen Bitcoin und eine Marktkapitalisierung des Bitcoins von rund 150 Mrd. USD. Das Marktvolumen aller Tokens betrug zu diesem Stichtag 403 Mrd. USD.

Die Markteffizienzhypothese von Fama besagt, dass die Preise, die in einem Markt erzielt werden, sämtliche Informationen reflektieren, die in diesem Markt verfügbar sind. Zur Definition eines effizienten Marktes gehören die Annahmen, dass die Teilnehmer zum großen Teil aus rationalen Marktteilnehmern bestehen und dass wichtige aktuelle Informationen für alle Teilnehmer nahezu frei verfügbar sind.

Die Anwendung der Markteffizienzhypothese bezieht sich in aller Regel nur auf Kapitalmärkte. Informationen zu Unternehmen, Staaten und Rohstoffen führen hier bereits Sekunden nach dem Bekanntwerden zu Konsequenzen in den Kursen, was ein Indiz dafür ist, dass die Preise sehr schnell den Informationsstand des Marktes repräsentieren (E.F.Fama, 1991).

ICO und Kryptobörsen sehen wir nach dieser Definition als nicht effizient an, da Käufer in der Regel ein erhebliches Informationsdefizit gegenüber dem Verkäufer/Anbieter haben und der Bitcoin Preis nicht den tatsächlichen Informationsstand des Marktes repräsentiert.

Zur Beurteilung eines möglichen negativen Übertragungseffektes auf die Realwirtschaft wurden nachfolgende Aspekte bei Bitcoin untersucht:

- Adressenkonzentration
- Marktkapitalisierung
- Derivatehandel

2.4.1. Adressenkonzentration

Untersuchte Fragestellungen: Wer hält Bitcoins? Wie ist die Adressenkonzentration von Bitcoins? Hierzu haben wir die Wallets ausgewertet, die Bitcoin halten. Leider ist durch die Anonymisierung keine Länderzuordnung möglich. 97,53% der Bitcoin Besitzer halten zwischen 0,001 und 1 Bitcoin. 1,93% der Adressen halten zwischen 1 und 10 Bitcoin. 0,51% halten zwischen 10 und 1.000 Bitcoin.

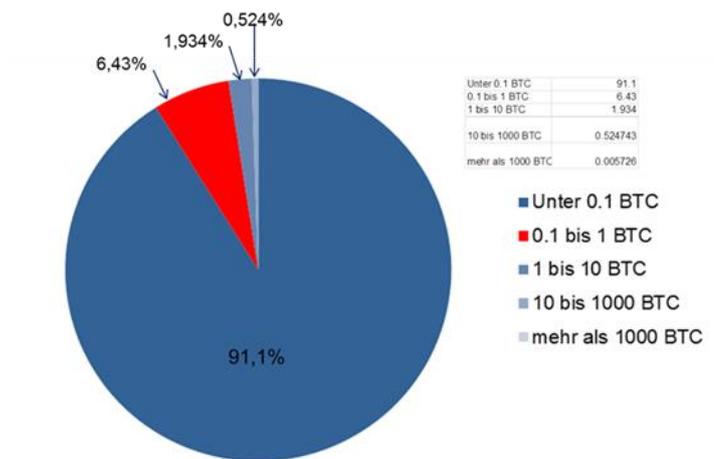


Abbildung 6: Adressenkonzentration Bitcoin

1.624 Adressen bzw. 0,005726% des Gesamtbestandes von 16.782.932 Bitcoins halten mehr als 1.000 Coins. Rund 100 Adressen halten mehr als 10.000 Bitcoins, diese sind bei den Mining-Farmen zu vermuten. Es gab 2017 etwa 20 Hauptmining Pools weltweit. Die chinesischen und japanischen Pools kontrollieren ca. 81% der gesamten Netzwerk-Hash-Rate weltweit. Damit befinden sich mit Abstand die meisten Mining Pools in Asien.

In unserer empirischen Untersuchung gaben lediglich 1% der Befragten an, Bitcoin als Zahlungsmittel verwendet zu haben bzw. ein Wallet zu besitzen. Übertragen auf die Einwohnerzahl in Deutschland wären das rund 820.000 Personen.

Die Granularität der Adressenkonzentration ist sehr breit und stellt somit kein Risiko oder Übertragungseffekt auf die reale Wirtschaft dar, da die Bestände nicht kreditfinanziert sind.

Nachfolgend die Übersichtstabelle und das Schaubild zur Visualisierung (bitinfocharts, 2018). Die Tabelle zeigt die Adressenverteilung in Bitcoins.

Bitcoin distribution					
Balance	Addresses	% Addresses (Total)	Coins BTC	\$USD	% Coins (Total)
0 - 0.001	15,229,206	53.69389	2,800	39,745,308 USD	0.02% (100%)
0.001 - 0.01	5,951,909	20.98476	25,760	365,668,147 USD	0.15% (99.98%)
0.01 - 0.1	4,659,349	16.42755	150,053	2,129,993,378 USD	0.89% (99.83%)
0.1 - 1	1,824,812	6.43377	569,365	8,082,096,201 USD	3.39% (98.94%)
1-10	548,790	1.934879	1,459,093	20,711,709,191 USD	8.69% (95.54%)
10 - 100	131,601	0.463988	4,359,276	61,879,563,488 USD	25.97% (86.85%)
100 - 1,000	15,722	0.055431	3,712,369	52,696,778,007 USD	22.12% (60.87%)
1,000 - 10,000	1,510	0.005324	3,307,252	46,946,170,537 USD	19.71% (38.75%)
10,000 - 100,000	111	0.000391	2,757,138	39,137,355,570 USD	16.43% (19.05%)
100,000 - 1,000,000	3	0.000011	439,826	6,243,290,091 USD	2.62% (2.62%)
Summe	28,363,013	100	16,782,932		

2.4.2. Marktkapitalisierung

Zur weiteren Prüfung, ob es sich aus dem Segment der ICO's negative Übertragungseffekte auf die Realwirtschaft und den Finanzsektor ergeben können, betrachten wir den rechnerischen Gesamtwert der ICOs weltweit und vergleichen diesen mit wirtschaftlichen Kennziffern. Die Marktkapitalisierung unterliegt ständigen Veränderungen.

Gemäß der Informationsplattform ICO Rating besteht Stand 14. Februar 2018 folgende Anzahl von ICOs (ICO-Rating, 2018):

Anzahl vergangene ICOs	283
Laufende ICOs seit 2017	123
Angekündigte ICOs	78

Die Marktkapitalisierung von Bitcoins betrug per 14. Februar 2018, rund 150 Mrd. USD. Die Anzahl der existierenden Bitcoins betrug 16.864.312. Die Website coinmarketcap.com listet Stand 9. Februar 2018 ca. 1514 Kryptowährungen mit einer Gesamtmarktkapitalisierung von ca. 403 Milliarden USD (Coinmarketcap, 2018). Diese Werte wurden ins Verhältnis gesetzt zu bekannten Kenngrößen, um eine Relation zu erhalten:

Den rechnerischen Wert von Bitcoin abgezogen, beläuft sich die Marktkapitalisierung der restlichen Kryptowährungen somit auf rund 255 Mrd. USD. Zur ersten Einordnung die Marktkapitalisierung von Apple (USA, 639 Mrd. USD), Microsoft (USA, 446 Mrd. USD) und Amazon.com (USA, 366 Mrd. USD).

In einem ersten Schritt wurde die Marktkapitalisierung von Bitcoin Kennzahl (a) ins Verhältnis gesetzt zu den Kennzahlen 1 – 6. Das Ergebnis sind die prozentualen Angaben in der Spalte Relation Bitcoin. Der Bitcoin in Relation zum Euro Stoxx 50 und Dow Jones beträgt 5,11% bzw. 2,20%. Gemessen an der Geldmenge der Euro Zone

liegen die Werte im 1% Bereich. Verglichen mit der weltweiten Geldmenge liegt der Anteil des Bitcoins unter 1% nämlich bei 0,41% und 0,17%.

Im zweiten Schritt wurden die Marktkapitalisierung aller ICOs Kennzahl (c) ins Verhältnis gesetzt zu den Kennzahlen 1 - 6. Der Vergleich mit dem DAX ist nicht adäquat, aber zur Vollständigkeit mit angegeben. In Vergleich zu Dow Jones, Geldmenge M1, M3 liegt der Anteil der ICO im einstelligen Prozentbereich.

Nr.	Segment	Kapital	Kapital umgerechnet in US Dollar (1 €=1,2325Dollar)	Relation Bitcoin	Relation ICO weltweit gesamt
a	Bitcoin	150 Mrd.USD	150	150	
b	Rest Kryptowährungen	253 Mrd. USD	253		
c	Gesamt	403 Mrd. USD	403		403
				Angaben in Prozent	
1	Marktkapitalisierung DAX gesamt	1.006 Mrd.€	1240	12.10	32.50
2	Marktkapitalisierung Euro Stoxx 50	2.384 Mrd. €	2938	5.11	13.72
3	Marktkapitalisierung Dow Jones 30 Industrial	5.521 Mrd. €	6805	2.20	5.92
4	Geldmenge M1 Eurozone	7.770 Mrd.€	9577	1.57	4.21
5	Geldmenge M3 Eurozone	11.870 Mrd.€	14630	1.03	2.75
6	Geldmenge weltweit Banknoten und Sichteinlagen	36.8 Trillionen USD	36800	0.41	1.10
7	Geldmenge weltweit	90.4 Trillionen USD	90400	0.17	0.45

(Statista, 2018), (Market, 2018), (Finanzen.net, 2018)

Die Marktkapitalisierung von ICOs bzw. Bitcoin ist als zu gering anzusehen, um einen negativen Übertragungseffekt auf den Finanzsektor oder die Realwirtschaft zu erzeugen.

ICOs werden überwiegend von kleineren meist nicht stark in der Wirtschaft gefestigten Unternehmen zur Finanzierung genutzt und stellen daher eine riskante Investition dar. Durch hohe Kursschwankungen kann es zu Marktkapitalisierungsverzerrungen kommen.

2.4.3. Derivatehandel

In der Sub prime-Krise war der ursprüngliche Häuserkreditmarkt der USA um das 20-fache in synthetischen Derivaten wie ABS und CDO-Produkten weiter verbrieft. Dies war neben weiteren Faktoren eine Ursache, die zu dem Ausmaß der Finanzmarktkrise 2007/2008 beigetragen hat. Somit wird in diesem Abschnitt der Future Handel und das Kursverhalten Derivat zur Kasse bzw. Relation zum DAX-Future um einen Vergleich zu ziehen, betrachtet.

Am 17. November wurden [erste Ankündigungen](#) von der CBOE und CME veröffentlicht, dass diese erstmalig Bitcoin-Futures anbieten werden. Wie dem nachfolgenden Candle-Chart der letzten drei Monate zu entnehmen ist, markierte diese Ankündigung quasi den Startschuss für eine volatile Kursbewegung des Bitcoins vom November 2017 bis Januar 2018.



Abbildung 7: Candle-Chart Bitcoin

Nach der offiziellen Ankündigung der Bitcoin-Futures war ein rasanter Anstieg des Bitcoin-Kurses von 7.000 auf 15.000 Euro zu beobachten. Der Anstieg wurde lediglich von dem Start der CBOE unterbrochen. Am 18.12.2017 sind dann die CME-Futures gestartet. Danach war ein massiver Kurssturz von Bitcoin von 16.300 Euro auf unter 12.000 Euro zu beobachten. Mit dieser Kursbewegung wurde auch die Unterstützungszone von 13.000 Euro durchbrochen, die bis dahin als Widerstand diente (coinhero, 2018).

Als die CBOE Futures am 17. Januar ausgelaufen sind, wies Bitcoin den bis dahin niedrigsten Preis für das Jahr 2018 aus: 9.366 Euro. Am 26. Januar lief der erste Bitcoin Futures der CME aus. Die CME ist die weltweit größte Terminbörse. Sie hat die Kontraktgröße auf 5 Bitcoins festgelegt. Im Vergleich hierzu verfügt der CBOE-Kontrakt mit der Kontraktgröße 1 Bitcoin über einen deutlich geringeren Handelsgegenwert. In den folgenden 7 Handelstagen danach (29.1.-6.2.) fand ein Kursabsturz um 38% auf 5.536 Euro statt.

Mögliche Erklärungen für den Kursabsturz Bitcoin Kasse:

- 1) Die Future-Investoren haben ihre Bitcoins verkauft und damit weitere Stop-Loss-Order ausgelöst um ihre Bitcoin Future Wetten zu gewinnen. Ob eine derartige Marktmanipulation tatsächlich stattfindet, kann nicht bewiesen werden. Jedoch zeigt der vorherige Chart einen engen zeitlichen Zusammenhang zwischen dem Bitcoin-Kassakurs und dem Bitcoin Futures. Die Unterstützungszone von 7.000 Euro (orangefarbene Linie) könnte dabei die Talsohle markieren. Mit dem Auslaufen des CME-Future-Kontraktes könnte damit eine Trendwende folgen (coinhero, 2018). Tatsächlich hat sich der Bitcoin Kurs dann um 20% wieder erholt und stand zum 16. Februar 2018 bei 9.839 USD.

2) Die Regierung in Südkorea gab am 30. Januar 2018 bekannt den Bitcoin stärker zu regulieren unter anderem die Anonymisierung der Wallets aufzuheben.

Vergleich des Bitcoin-Futures:

Im Januar bestanden durchschnittlich folgende Umsätze an den Future Börse CME:

Januar 2018	Börse	Kontraktgröße	Anzahl Kontrakte	Volumen 1 Kontrakt	Gesamt
	CME	5 Bitcoin	611	64.885 €	39.644.735 €
	CBOE	1 Bitcoin	328	12.977	4.256.456 €
	Summe				43.901.191
	Eurex	25€ Dax-Punkt	1.773.443	100.000	177.343.700.000€

Berechnung: Höhe CME: 5 Bitcoin * 12.977 EUR (durchschnittlicher Bitcoin Wert Januar) = 64.885 EUR = Eine Kontraktgröße

Gehandelt am 3. Januar wurden 611 Kontrakte. $611 * 5 = 3055$ Bitcoins * 12.977 = 39.644.735 EUR + 4.256.456 = 43.901.191 € Volumen eines Tages. Höhe EUREX: 1.773.437 Kontrakte * 100.000 = 177.343.700.000 Mrd.€

Verhältnis: Bitcoin Future Volumen 43,9 Mio. € versus 177 Mrd. € Dax Future Anteil beträgt 0,02475%. Der Bitcoin Future Handel ist somit unbedeutend.

Verhältnis Bitcoin Kasse zu Bitcoin Future: 43,9 Mio. € Future Handel versus 23 Mrd. Bitcoin Kasse am 3. Januar = sind 0,1908%. Es besteht keine derivative Spekulation da 99% über Kasse gehandelt werden.

2.5. Illegale Verwendungen im Darknet

Bitcoin wird bevorzugt als Zahlungsmittel im Darknet verwendet. Das Darknet wird überwiegend von jenen benutzt, die ihre Identität beim Benutzen des Internets wahren wollen oder müssen. Dies wird durch die spezielle Verschlüsselungstechnik gewährt (Handelsblatt, Treffpunkt für Kriminelle und Dissidenten, 2016).

Die bekannteste Webseite, auf der illegale Produkte gekauft werden konnten, war Silk Road. Silk Road wurde 2011 von Ross Ulbricht gegründet. Auf der Plattform wurden illegale Drogen, gefälschte Ausweisdokumente, Waffen, Kreditkarten und verschiedene digitale Güter verkauft. Die Größe und das Umsatzvolumen des virtuellen Schwarzmarktes waren unvorstellbar hoch. Nach Angaben des FBI verwendeten etwa eine Millionen Nutzer die Plattform, die einen Gesamtumsatz von über 1,2 Milliarden USD generierten. Der Inhaber der Webseite war für die meiste Zeit nur unter dem Decknamen Dread Pirate Roberts bekannt. Das FBI fahndete nach ihm, um den illegalen Drogenverkauf über seine Seite zu stoppen. Im Oktober 2013 wurde über ein Sicherheitsleck der Silk Road Server die wahre Identität Ulbrichts festgestellt. Im gleichen Monat wurde Silk Road durch das FBI geschlossen und Ulbricht verhaftet. Da sich die Plattform unter den Nutzern großer Beliebtheit erfreute, wurde im November 2013 die Webseite Silk Road 2.0 eröffnet. Diese war nur ein Jahr online und wurde ebenfalls vom FBI beschlagnahmt und geschlossen (Winter, 2015).

Bezahlt wurde auf Silk Road mit Bitcoins aus einem Wallet, welches ohne größere Identitätsprüfung eröffnet werden konnte, um die Identität des Käufers zu wahren. Dazu kommt noch, dass es Dienstleistungen gibt, die eine

Bitcoinwäsche anbieten, um den Ursprung des Coins zu verbergen. Coin-Mixing Dienste wie CleanCoin bieten dem Nutzer dadurch Sicherheit, dass die Bitcoins durch eine große Quelle ausgetauscht werden, wozu es laut der Seite nahezu unmöglich sei, den Ursprung zurückzuverfolgen (BTC-ECHO, 2016).

2.6. Energieverbrauch & technische Restriktionen des Handels

Der Bitcoin als Kryptowährung benötigt ein Netzwerk technischer Geräte, die das System stützen. Im Fall der Blockchain wird die Rechenleistung eines Computers dazu verwendet, Transaktionen zu kontrollieren und neue Blöcke zu generieren. Der Computer, der den Hash-Algorithmus am schnellsten berechnet, wird in Form von Bitcoins entlohnt (Nakamoto, 2008).

Stand Januar 2018 beträgt die Entlohnung für die schnellste Berechnung 12,5 BTC (Bitcoinbloghalf, 2018). Aufgrund des hohen Gegenwertes des Bitcoins versucht eine Vielzahl an Computern, den Hash am schnellsten zu berechnen.

Am 20. November 2017 lag der jährliche Stromverbrauch des Bitcoin-Netzwerks bei 29,05 Terrawattstunden (Powercompare.co.uk, 2017). Bitcoin würde sich heute auf der Weltrangliste der Länder hinsichtlich des Stromverbrauchs auf Platz 58 befinden (Dörken T. , 2018). Es wird erwartet, dass die Erhaltung des Bitcoin Netzwerks 2020 so viel Strom wie komplett Norwegen verbrauchen wird (Kaiser, 2017). Der zunehmende Stromverbrauch und die damit steigenden Kosten, werden fortlaufend auch durch eine steigende Relevanz von energieeffizienten Systemen, zu einem Hindernis.

Die Schwankungen des Bitcoin-Kurses decken einige technische Defizite der Handelsplattformen auf. So kam es am 22. Dezember 2017 aufgrund des Kursabsturzes zum Zusammenbruch einer der größten Handelsplattform Coinbase. Aufgrund eines hohen Nutzeransturms und somit hoher Zugriffszahlen war kein Handel mit Kryptowährungen mehr möglich. Die hohe Nachfrage scheint durch die starken Kursturbulenzen ausgelöst worden zu sein, wodurch die Server der Handelsplattform überlastet waren. Zudem wiesen die Betreiber kurz vorher erst darauf hin, dass sich Einzahlungen unter einem Betrag von 1000 Euro um bis zu zehn Tage verzögern könnten (Micijevic, 2017).

Die Bezahlung mit Bitcoins ist sehr langsam und bringt höhere Transaktionsgebühren mit sich. Bei einem Bezahlvorgang kann es immer wieder zu Verzögerungen kommen, da die Blockchain deutlich weniger Transaktionen verarbeiten kann als die Systeme der Banken, die zur Abwicklung des Zahlungsverkehrs eingesetzt werden (Deutsche Bundesbank , 2017).

Bei Vergleichen zwischen Kryptowährungen werden die Geschwindigkeit einer Transaktion und die Kosten als Hauptkriterien verwendet (ripple.com, 2018).

	Bitcoin	Ripple	Ethereum
Geschwindigkeit einer Transaktion	1+ Stunde	4 Sekunden	2+ Minuten
Transaktionskosten	Um 2USD	0,0004 USD	0,14 USD

(ripple.com, 2018), (Bitcoin, 2018)

Die nachstehende Statistik von 2016 macht sehr deutlich, dass die Verwendung der digitalen Wahrung Bitcoin als Zahlungsmittel zu anderen Zahlungsnetzwerken vergleichsweise gering ist.

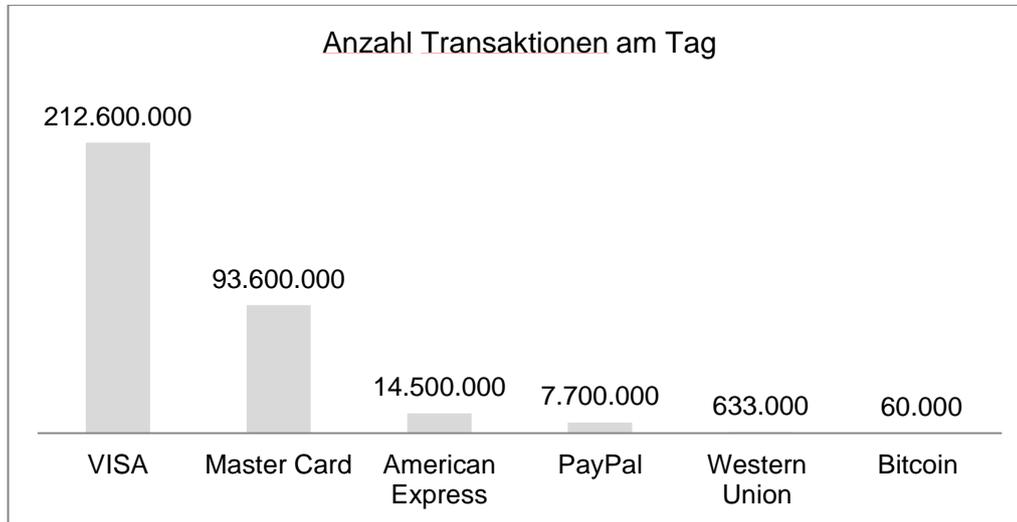


Abbildung 8: Anzahl Zahlungstransaktionen im Vergleich

Sie betragt gerade mal ein Zehntel der durch Western Union abgewickelten Transaktionen und noch nicht einmal 1% der Paypal-Transaktionen. Mit durchschnittlich 60.000 Transaktionen pro Tag liegt der Bitcoin noch weit hinten im Vergleich zu anderen bekannten Zahlungsmitteln.

Im Durchschnitt wird eine Bitcoin-Zahlung innerhalb von zehn Minuten gebucht. Auch die Anonymitat ist, gegenuber konventionellen uberweisungen bei Kreditinstituten, starker gegeben, da, zumindest theoretisch, niemand den aktuellen Kontostand oder auch Zahlungsstrome einsehen kann.

Nach derzeitigem Stand spielen Bitcoins jedoch eine untergeordnete Rolle. Die Deutsche Bundesbank wickelt taglich circa 24 Millionen uberweisungen und etwa 35 Millionen Lastschriften ab. Das gesamte Bitcoin-System, im Vergleich, weist circa 60 Tausend Transaktionen taglich aus.

Das Aufkommen an Transaktionen in Bitcoins ist, nach derzeitigem Stand, keine Gefahr fur konventionelle Kreditinstitute und weist keine signifikanten Steigerungen auf, aus denen sich eine zukunftig starkere Bedeutung des Bitcoin schließen liee. Zu bemerken ist jedoch, dass eine gleichbleibende Zahl an Transaktionen in Bitcoin bei steigenden Werten des Bitcoin im Gegenwert zu Euro oder US Dollar, zu groeren Volumina fuhrt. Fur die Beurteilung der Entwicklung des Bitcoin ist dies zu berucksichtigen (Elsner, 2018).

2.7. Übersicht der Mining Pools

Jordan Tuwiner (Tuwiner 2017) veröffentlichte 2017 einen Bericht über die Infrastruktur der Bitcoin Mining Pools. Als Bitcoin Mining Pools werden spezialisierte Computer bezeichnet, welche sich meistens in großen Lagerhallen, auch bekannt als Mining Farms, befinden. Es gibt etwa 20 Hauptmining Pools weltweit. Die chinesischen Pools kontrollieren ca. 81% der gesamten Netzwerk-Hash-Rate weltweit.

Damit befinden sich mit Abstand die meisten Mining Pools in China. Daran folgt Island mit 5%, Japan mit 3%, Tschechien mit 3%, Georgien mit 2% und Indien mit ebenfalls 2%.

Die unten aufgeführte Abbildung stellt eine Liste der wichtigsten Mining Pools dar. Abbildung 8: Abschätzung der Hashrate-Verteilung unter den größten Mining-Pools (blockchain.info, 2018)

Wie anhand der Graphik zu erkennen ist, sind die fünf größten Bitcoin Mining Unternehmen: AntPool, BTC.TOP, BTC.com, Bixin und BTCC Pool.

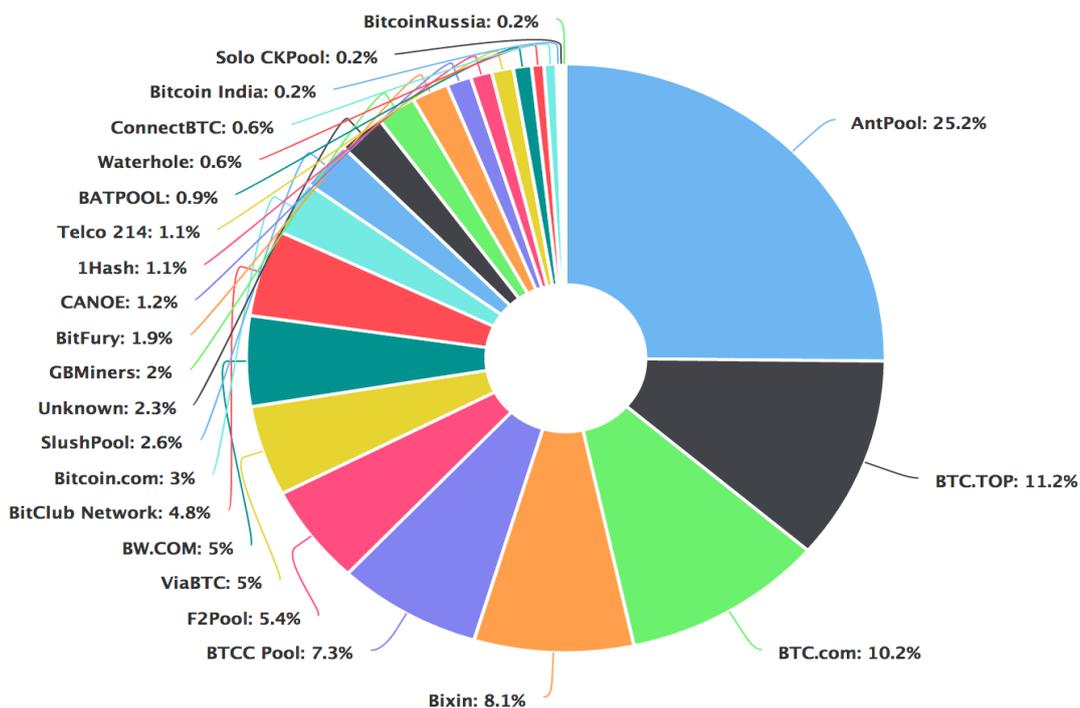


Abbildung 9: Übersicht Mining Pools weltweit

3. Die Blockchain-Technologie

3.1. Ursprung und Begriffe

Soweit öffentlich bekannt beginnt die Geschichte des Bitcoins und der Blockchain am 1. November 2008. Ein Pseudonym namens Satoshi Nakamoto veröffentlichte in einem Whitepaper mit dem Titel "Bitcoin: A Peer-to-Peer Electronic Cash System" das Konstrukt des Peer-to-Peer Electronic Cash System Bitcoin und sendet dieses an eine Kryptographie Mailing List. Die Identität von Satoshi Nakamoto bleibt bis heute ungeklärt.

Auf acht Seiten beschreibt Satoshi Nakamoto in diesem Whitepaper die technische Grundlage für Bitcoin, Kryptowährungen und die Blockchain-Technologie. Das Whitepaper gilt als Gründungsdokument der Kryptowährungen. Es verbindet mehrere kryptographische Konzepte - Hashes, Signaturen, Merkle Trees um erstmals ein dezentrales Transaktionssystem um digitales Bargeld zu schaffen (Bitcoin-Markplatz, 2017).

Blockchains sind fälschungssichere, verteilte Datenstrukturen, in denen Transaktionen in der Zeitfolge protokolliert, nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind. Mit der Blockchain-Technologie lassen sich Eigentumsverhältnisse direkter und effizienter als bislang sichern und regeln, da eine lückenlose und unveränderliche Datenaufzeichnung hierfür die Grundlage schafft (BaFin, Journal Initial Coin Offering, 2017).

Der Begriff Blockchain beschreibt eine dezentrale Datenbank, bei der jeder User, der Teil dieses Blockchain-Netzwerkes ist, die gesamte Datenbank mit sämtlichen Informationsketten „Chains“ (engl. für Kette) oder Ausschnitte davon besitzt. Die Blockchain funktioniert wie eine Art öffentliches Grundbuch oder ein digitaler Kontoauszug für Transaktionen zwischen Computern (Presse, 2017).

Um die Blockchain Technologie besser verstehen zu können, müssen einige Begrifflichkeiten vorerst erörtert werden:

Dezentral bedeutet, dass das Protokoll, also der „Block“, nicht auf einem einzigen zentralen Server liegt, sondern über mehrere Computer verteilt ist. Hier wird noch einmal unterschieden zwischen einer sogenannten öffentlich Blockchain und einer privaten Blockchain. Hierzu aber im Verlauf mehr. Dieses Protokoll oder dieser „Block“ ist öffentlich und für jeden innerhalb dieser Blockchain zugänglich. Es gibt also keinen Besitzer.

Transaktionen beschränken sich nicht auf finanzielle Transaktionen. Transaktionen beinhalten hier jegliche Art von Informationsübertragungen. Verfasst man zum beispielweise einen Satz auf Papier, kann dieser, einmal niedergeschrieben, nicht mehr geändert werden, zumal, wenn Zeugen anwesend waren. Angewendet auf die Blockchain, gibt es einen feinen Unterschied: Innerhalb der Blockchain kann eine Information jederzeit von jedem Teilnehmer nachvollzogen werden.

Um eine Transaktion durchführen zu können benötigt man einen sogenannten Wallet. Es handelt sich dabei um eine virtuelle „Geldbörse“ oder einen privaten Ordner. Ein Wallet besteht aus einem Public Key (engl. für öffentlicher Schlüssel) und einem Private Key (engl. für privater Schlüssel). Den Private Key sollte man ebenso wenig weitergeben wie seine Passwörter oder PINs. Mit ihm werden unsere Transaktionen autorisiert. Selbstverständlich wird dieser durch Kryptografie (siehe unter Kryptografie und Hash-Algorithmen) verschlüsselt, sodass es unmöglich ist diesen herauszufinden. Der Public Key ist unsere virtuelle „Kontonummer“. Über den Public Key können Transaktionen zu dem Wallet-Inhaber transferiert werden. Ein Wallet enthält keine privaten Informationen zum Inhaber. Dieser ist also anonym (Rueß, 2017).

Zwischen **öffentlichen und privaten Blockchains** gibt es nur einen simplen Unterschied und zwar die Teilnahme. Ein öffentliches Blockchain-Netzwerk ist für jeden zugänglich. Es steht jedem frei, Teil dieses Netzwerkes zu sein und damit zu arbeiten. Diese öffentlichen Netzwerke bieten meist einen Anreiz, also eine Art Belohnung umso ein möglichst breites Netzwerk zu bieten. Bitcoin ist zum Beispiel eines der größten öffentlichen Netzwerke heutzutage (Jayachandran, 2017).

Bei privaten Blockchains wird eine Einladung benötigt um Teil dieses Blockchain-Netzwerkes zu sein. Diese Netzwerke zielen meist darauf ab, das Datenmanagement innerhalb eines Unternehmens zu optimieren. Diese Lösung bietet eine höhere Transaktionssicherheit und das Protokoll ist im Gegensatz zur öffentlichen Blockchain nur für deren Teilnehmer einsehbar (Praveen Jayachandran, 2017).

Ein Peer-to-Peer (P2P) Netzwerk beschreibt ein Computernetzwerk/ Rechnernetzwerk bei denen alle Rechner miteinander verbunden sind und gleichberechtigt miteinander arbeiten. Es gibt keinen zentralen Server (Bryan, 2005).

Die **Kryptografie** sorgt für die Transparenz als auch für die Privatsphäre. Bei dem Prozess der Kryptographie im Zusammenhang mit der Blockchain wird ein geheimer Schlüssel in Form einer Zufallszahl generiert bzw. errechnet. Es werden somit alle Daten einer Transaktion verschlüsselt. Hierfür gibt es verschiedene Algorithmen auch *Hash-Algorithmen* genannt. Bitcoin benutzt die kryptologische Hashfunktion SHA-256 (Claudio Brecht, 2017).

Ein wichtiger Bestandteil dieses Systems sind die *Miner*. Sie bilden das Prüforgan oder sinnbildlich auch die Buchhalter eines Blockchain-Systems. Ein Miner verifiziert jede Transaktion und teilt diese über das Netzwerk. Andere Teilnehmer prüfen diese Verifizierung und bestätigen diese auf Richtigkeit (Maik Klotz, 2016).

Bei einem **Hash** spricht man auch von einer Einwegfunktion. Man kann die Verschlüsselung nicht mehr umkehren beziehungsweise zu den Quelldaten decodieren. Der vom Hash-Algorithmus errechnete Code ist außerdem einzigartig und wird aufgrund dieser Eigenschaft auch als digitaler Fingerabdruck bezeichnet. Alle digitalen Medien, wie Dokumente und Musik, jeder beliebigen Größe können durch einen Hash-Algorithmus verschlüsselt werden. Dabei ist der einzigartige Hash bedeutend kleiner als die ursprüngliche Quelle. Jegliche Veränderung der Quelldatei würde den Hash verändern. Im Umkehrschluss würden die Quelldaten immer den gleichen Hash erzeugen (Chainthat, 2016).

Bei **SHA-256** wird der Datenblock mit Konstanten aus den ersten 32 Bits des Nachkommanteils der Quadratwurzeln der ersten acht Primzahlen 2 bis 19 initialisiert. Er wird in 64 Runden unter Verwendung von vier logischen Funktionen und je Runde einer anderen Konstanten verschlüsselt. Diese Konstanten werden aus den binären Nachkommastellen der Kubikwurzeln der ersten 64 Primzahlen gebildet.

Alle Teilnehmer in diesem **Nodes (Netzwerk)** sind für die Speicherung und Verifikation der gesendeten Transaktionen zuständig. Durch die dezentrale Ablage und dem Prozess namens Mining muss keine zentrale Autorität die Blockchain verwalten. Miner stellen die Rechenleistung zur Verfügung, um die einzelnen Blöcke zu verifizieren um dann den Block an die Kette zu hängen und zu versiegeln.

3.2. Wie funktioniert die Blockchain-Technologie?

Mit der Klärung der wichtigsten Begriffe wird folgend das System näher erläutert. Bei einer Blockchain werden Transaktionen in sogenannte Blöcke abgelegt. Wie bereits erwähnt ist die Datenquelle nicht auf Finanztransaktio-

nen beschränkt. Sie können ebenso Verträge, Musik, Filme oder sonstige Datenquellen sein. Visuell können wir uns einen Datenblock wie ein Blatt Papier vorstellen, auf dem alle benötigten Informationen enthalten sind um eine Transaktion korrekt auszuführen. In jedem neuen Block ist die Transaktionshistorie des vorherigen Blocks in Form einer Prüfsumme enthalten. Ebenso ist eine Prüfsumme der kompletten Blockkette enthalten. Es ist noch einmal wichtig sich dabei vorzustellen, dass dies alles mit Algorithmen errechnet wird.

Die Miner sammeln die Transaktionen und generieren einen neuen Block. Eine Übersicht über die neu generierten Bitcoin-Blöcke bietet die Webseite blockchain.info.

Ist ein Block einmal generiert, würden sich diese Daten nur ändern lassen, wenn jeder darauffolgende Block neu berechnet werden würde. Dies würde eine astronomische Höhe an Rechenleistung benötigen. Der Aufwand und die Kosten wären wesentlich höher als der Profit (Hajo Schulz, 2017).

Um dies erneut zu visualisieren, müsste man sich tausende Blätter Papier vorstellen, welche aneinandergeklebt sind. Diese müsste man wieder aufwendig voneinander trennen. Außerdem müsste auf jeder Seite eine Gleichung berechnet werden, auf der jedes Ergebnis notwendiger Bestandteil der darauffolgenden Gleichung wäre. Zusätzlich müsste man die Seiten wieder zusammenkleben.

Beispiel: Person A möchte an Person B 5 Bitcoin überweisen. Dazu benötigen beide Personen ihren persönlichen Wallet. Person A benötigt für eine Überweisung die Public Key Adresse von Person B. Diese gibt er, wie in der Abbildung, in das Feld „Pay To“ (engl. für Zahlung an): ein. Unter „Amount“ (engl. für Betrag): gibt er die Überweisungsmenge ein, 5 Bitcoin. Ist beides eingegeben, muss Person A nur noch auf „Send“ (engl. für senden) drücken und die Transaktion nimmt ihren Lauf (Satoshi Nakamoto, 2008).

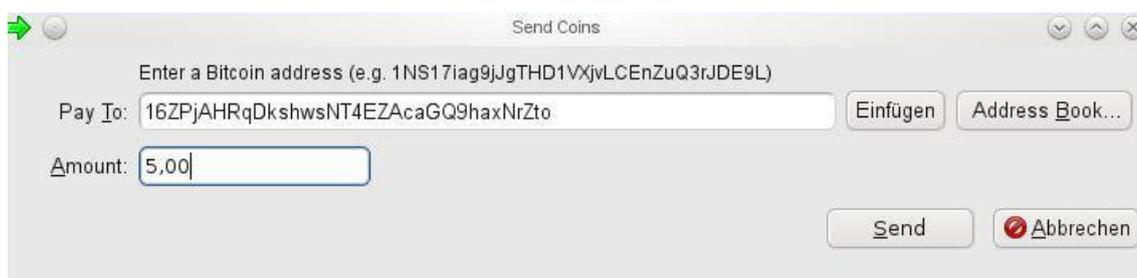


Abbildung 10: Bezahlung von Bitcoin von Wallet zu Wallet

Diese Transaktion wird als Block repräsentiert und an jeden Teilnehmer des P2P-Netzwerkes geschickt.

Über das P2P-Netzwerk wird die Transaktion auf Gültigkeit überprüft. Es wird geprüft ob Person A über die versendete Menge verfügt. Dies wird anhand der Blockchain geprüft, also den Hashes.

Ebenso werden der Public Key und die Signatur geprüft. Ist alles korrekt wird die Überweisung verifiziert, also für gültig erklärt. Dieser Block gehört nun zur gesamten Blockchain.

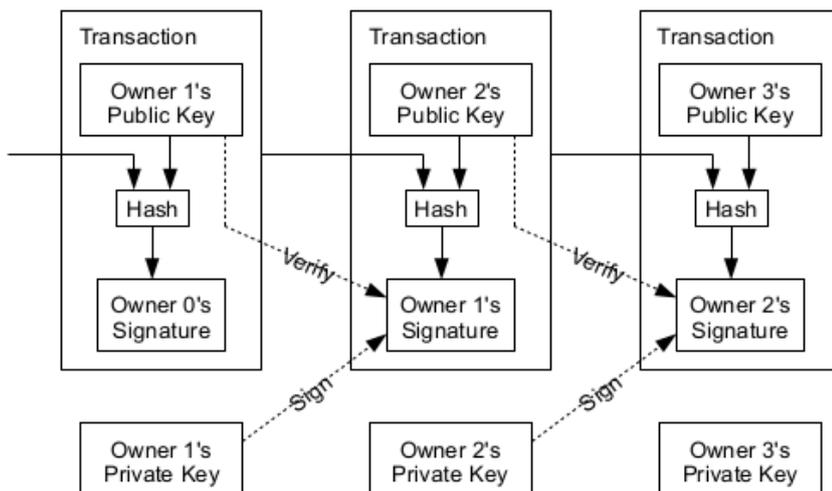


Abbildung 11: Hash-Transaktion

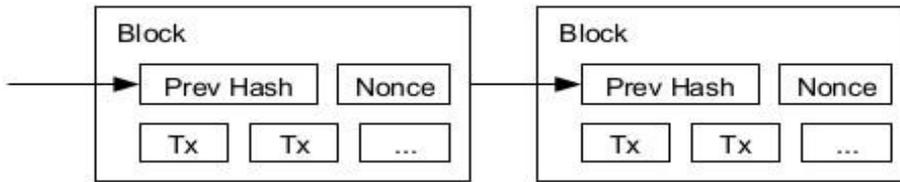
Die von uns vorgeschlagene Lösung beginnt mit einem Zeitstempel-Server. Ein Zeitstempel-Server funktioniert, indem er den Hash eines Blocks von mit Zeitstempel zu versendenden Datensätzen nimmt und den Hash weitläufig, etwa in einer Zeitung oder in einem Usenet-Post, veröffentlicht. Der Zeitstempel beweist, dass die Daten zu diesem Zeitpunkt existiert haben, offensichtlich, denn sonst gäbe es keinen Hash von ihnen. Jeder Zeitstempel beinhaltet in seinem Hash den vorhergegangenen Zeitstempel und bildet eine Kette, bei der jeder zusätzliche Zeitstempel die vorherigen verstärkt.

Proof-Of-Work

Um einen verteilten Zeitstempel-Server auf Peer-to-Peer-Basis zu implementieren, müssen wir ein Proof-of-Work-System, ähnlich des Hashcash-Systems von Adam Back [6], anstatt der Zeitungen oder Usenet-Posts verwenden. Der Proof-of-Work beinhaltet die Suche nach einem Wert, bei dem, wenn er gehasht wird, etwa durch SHA-256, der Hash mit einer Anzahl von Nullbits beginnt. Die durchschnittlich erforderliche Arbeit ist exponentiell zu der Anzahl der erforderlichen Nullbits und kann durch die Ausführung eines einzelnen Hashs verifiziert werden.

Für unser Zeitstempel-Netzwerk implementieren wir den Proof-of-Work, indem eine Nonce im Block solange ansteigt, bis ein Wert gefunden wird, der dem Hash des Blocks die erforderlichen Nullbits gibt. Nachdem die CPU genügend Arbeit aufgewendet hat, um den Proof-of-Work zu erfüllen, kann der Block nicht mehr geändert werden, ohne dass die Arbeit erneut ausgeführt wird.

Da spätere Blocks damit verkettet werden, würde die Arbeit zur Änderung des Blocks die Neuerstellung aller nachfolgenden Blocks beinhalten.



Der Proof-of-Work löst außerdem das Problem, bei Mehrheitsentscheidungen die Repräsentanten zu bestimmen. Wenn die Mehrheit auf einer Stimme je IP-Adresse basieren würde, könnte diese durch jeden unterwandert werden, der in der Lage ist, viele IPs zu reservieren. Proof-of-Work ist im Grunde eine Stimme pro CPU. Die Mehrheitsentscheidung wird durch die längste Kette repräsentiert, in die der größte Proof-of-Work Aufwand investiert wurde. Wenn eine Mehrheit der CPU-Leistung von ehrlichen Knoten kontrolliert wird, wird die ehrliche Kette am schnellsten wachsen und alle konkurrierenden Ketten abhängen. Um einen vergangenen Block zu ändern, müsste ein Angreifer den Proof-of-Work des Blocks sowie den aller nachfolgenden Blocks neu erzeugen, und dann die ehrlichen Nodes einholen und überholen. Wir werden später demonstrieren, dass die Möglichkeit, dass ein langsamerer Angreifer aufholt, sich exponentiell verringert, je mehr nachfolgende Blöcke hinzugefügt werden.

Die Schritte zum Betrieb des Netzwerks sind die Folgenden:

- 1) Neue Transaktionen werden an alle Knoten ausgestrahlt.
- 2) Jeder Knoten sammelt die neuen Transaktionen in einem Block.
- 3) Jeder Knoten arbeitet daran, einen schwierigen Proof-of-Work für seinen Block zu finden.
- 4) Wenn ein Knoten einen Proof-of-Work findet, strahlt er den Block an alle Knoten aus.
- 5) Die Knoten akzeptieren den Block nur, wenn alle Transaktionen darin gültig und nicht bereits ausgegeben sind.
- 6) Die Knoten drücken ihre Akzeptanz des Blocks aus, indem sie daran arbeiten, den nächsten Block in der Kette zu erzeugen, wofür sie die Hash des akzeptierten Blocks als vorhergegangene Hash verwenden.

Knoten gehen immer davon aus, dass die längste Kette die korrekte ist und arbeiten daran, diese zu verlängern. Wenn zwei Knoten gleichzeitig verschiedene Versionen des nächsten Blocks übertragen, könnten einige Nodes die eine oder die andere Version zuerst empfangen. In diesem Fall arbeiten sie an der ersten, die sie empfangen haben, speichern aber den anderen Zweig für den Fall, dass dieser länger wird. Der Gleichstand wird gebrochen, wenn der nächste Proof-of-Work gefunden wird und ein Zweig länger wird; die Nodes, die am anderen Zweig gearbeitet haben, werden dann auf den längeren umschalten.

3.3. Smart Contracts

Smart Contracts sind Programme, die zwischen den Vertragsparteien vertragliche Bedingungen und Vereinbarungen prüfen und durchsetzen können (Miller, 2003). Smart Contracts haben die Eigenschaft, dass sie nicht nur Be-

dingungen prüfen können, sondern auch definierte Aktionen im Quellcode, wie zum Beispiel finanzielle Transaktionen, ausführen können. Außerdem sind sie dezentral, das heißt sie werden von einem Betreiber nicht an einer zentralen Stelle als Dienst bereitgestellt, sondern werden von vielen unterschiedlichen Teilnehmern im Netzwerk ausgeführt. Dies ist mit der Nutzung der Blockchain-Technologie verbunden (Swan, 2015).

Vor Manipulationen sind Smart Contracts durch die Blockchain Technologie zwar geschützt, doch in der Blockchain sind jegliche vertraglichen Vereinbarungen und Details öffentlich vorhanden, sodass jeder Teilnehmer dieses Netzwerkes die Verträge betrachten kann (Kosba, 2015).

Rechtliche Aspekte der Blockchain

Zuerst muss festgestellt werden, ob Smart Contracts überhaupt Verträge im Sinne des BGB sind. Da Smart Contracts weder im BGB, noch in anderen Vorschriften der Rechtsordnung geregelt sind, ist die Rechtslage, ob diese Verträge darstellen oder nicht, aktuell unklar. Auf Grund der Vertragsfreiheit sind Verträge von den Vertragsparteien grundsätzlich frei gestaltbar. Die Tatsache, dass Smart Contracts Computercodes und nicht ohne Weiteres lesbar sind, erschwert vom rechtlichen Aspekt her die Beurteilung, ob ein Vertragsabschluss vorliegt. Per Gesetz kommt ein Vertragsabschluss durch Angebot und Annahme mit zwei übereinstimmenden Willenserklärungen zustande. Jedoch kann der Programmcode eines Smart Contracts die Willenserklärungen eines Vertrages inhaltlich nicht zum Ausdruck bringen.

Somit ist der Smart Contract im rechtlichen Sinne kein Vertrag, sondern nur eine computerbasierte Umsetzung eines Vertrages. Zwar steht im §311 Abs. 1 BGB Vertragsprinzip, dass es den Parteien grundsätzlich freisteht den Programmcode eines Smart Contracts als Vertragssprache zu wählen, doch bei gesetzlichen Formvorschriften (z. B. Schriftform) ist ein Vertragsabschluss unmöglich, da der Vertrag nicht die Formvorschrift einhält (Heckmann, 2016).

Im Einsatz von Smart Contracts stellt sich auch die Überwachung zur Einhaltung zivilrechtlicher Grundsätze als ein zentrales Problem dar. Eine Kontrollmöglichkeit seitens der Justiz auf Wirksamkeit der Verträge ist derzeit nicht möglich. Was passiert also mit Verträgen, die entweder von vorneherein oder nachträglich nichtig wegen Formfehlern oder anderen gesetzlichen Vertragsverstößen sind? Hinzu kommt die Tatsache, dass eine nachträgliche Korrektur eines abgeschlossenen Vertrages nicht mehr möglich ist (Heckmann, 2016).

3.4. Sicherheit der Blockchain

Der größte Sicherheitsfaktor in der Blockchain ist der Distributed Ledger, also die Dezentralität. Durch die an alle Teilnehmer verteilten Informationen sind alle auf dem gleichen Stand der Blockchain und somit sind auch alle Daten für jeden transparent einsehbar. Dies führt zu einer fast nicht möglichen Manipulation der Daten. Also möchte ein Teilnehmer Information nachträglich ändern, müsste er die Mehrheit über die Miner (51% Regel) besitzen um somit die Berechnung des alten Blockes abzuändern (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016). Sollte dies erfolgen, sind aber noch alle Teilnehmer im Netzwerk mit den alten Informationen vorhanden. Und diese lassen sich nicht ändern (Deloitte, 2017).

Mehr als 50% der Miner (= Full Nodes) müssen ehrlich sein, damit das System sicher gegenüber attackierenden Full Nodes ist (Nakamoto, 2008). Die „ehrliche Blockchain“ wird schneller wachsen als die betrügerische.

Um einen früheren Block zu modifizieren, müsste ein Angreifer den Proof-of-Work aller Blöcke, die auf jenen folgten, erneut leisten, um die ehrliche Blockchain zu überholen (Nakamoto, 2008). Dieser Rechenaufwand ist so hoch, dass er kaum zu bewältigen ist, beziehungsweise sich nicht lohnt.

Hoher Stromverbrauch

Aufgrund der hohen Rechenleistung zur Validierung der Blöcke und den damit verbundenen starken Energieverbrauch kann es im dezentralen Netzwerk zu einer zentralen Lokation der Server (Miner) kommen. Bei Bitcoin stehen die größten Miner schon heute in China. Rechnet man die Top 5 der größten Miner zusammen liegt man über dem Zwecks Manipulation relevanten Anteil von 51%. Dies ist die größte Schwäche der Blockchain-Technologie (Commerzbank, 2017).

3.5. Distributed Ledger Technologie (DLT)

Die DLT ist trivial gesagt eine Art Software, die Daten verarbeitet und speichert. Distributed Ledger (wörtlich übersetzt: Verteiltes Haupt-/Kontenbuch) ist eine Datenbank, die den Nutzern eines Netzwerks gemeinsame Berechtigungen erlaubt. Die gemeinsame Schreibberechtigung unterscheidet sich hierbei von der klassischen Datenverarbeitung, da in der Regel nur die jeweiligen Abteilungen großer Institutionen über die Berechtigungen verfügen, Datensätze zu ändern, da potenziell die Gefahr besteht, dass Unbefugte die Daten manipulieren könnten. In einem DL-Netzwerk sind solche Instanzen überflüssig, da jeder Teilnehmer des Netzwerkes über eine Kopie der Daten verfügt. Sobald eine neue Information in die Datenbank aufgenommen wird, wird sie jeder anderen Kopie im Netzwerk hinzugefügt, um Informationsasymmetrien zu vermeiden. (Baran, 1964).

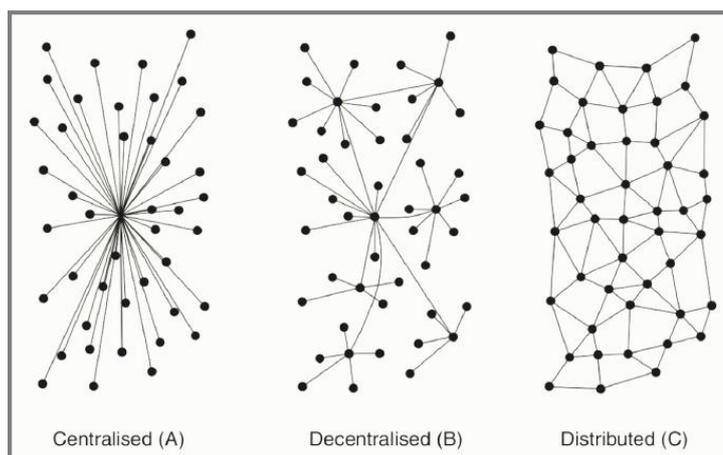


Abbildung 12: Zentrale, dezentrale und verteilte Netzwerke

Das Schaubild stellt drei verschiedene Netzwerkstrukturen dar. Deutlich zu erkennen ist, dass bei zentralen und dezentralen Netzwerken nur Administratoren eine unbeschränkte Autorisierung haben, während bei der Distributed Ledger jeder Teilnehmer über die gleichen Rechte verfügt.

Das Kontenbuch besteht aus einer Kette von chronologisch aufgeschichteten Blöcken, die mehrere Transaktionen beinhalten. Die Aktualisierung der Bücher erfolgt, indem die vorhandene Kette durch neu generierte Blöcke ergänzt wird. Um eine falsche Datenspeicherung zu vermeiden findet, ein Validierungs- und Konsensprozess statt (siehe Abbildung 2). Hierbei werden die übermittelten Daten (Information oder Transaktion) auf ihre Korrektheit und Zulässigkeit überprüft und die Entscheidung getroffen, ob und in welcher Reihenfolge sie angereicht werden.

Voraussetzungen für das Update sind ein Arbeits- (Proof-of-Work) und ein Anteilsnachweis (Proof-of-Stake) oder eine Mindestanzahl von Nutzern, die die Gültigkeit der Transaktion bestätigen (Practical Byzantine Fault Tolerance - PBFT). Sie dienen als eine Art „automatisierte Intermediäre“ zur Einigung auf Transaktionen sowie zur Verhinderung von Missbrauch oder Doppelbuchungen. Bevor Teilnehmer eine Transaktion durchführen können, müssen sie sich durch eine eigene digitale Unterschrift authentifizieren. Grundsätzlich kann man das Netzwerk offen (public) oder geschlossen (private) einrichten und darin beliebige Informationen verbreiten und speichern. In einem Private Ledger sind nur bestimmte Personen oder Institutionen autorisiert, auf die Daten zuzugreifen oder sie zu verändern.

Die Besonderheit an der DLT ist, dass sie eine direkte elektronische Wertübermittlung, ohne Involvierung Dritter, ermöglicht. Zurzeit ist dies im bestehenden Finanzmarkt unmöglich, da im Zahlungsverkehr mindestens ein Intermediär benötigt wird und je nach institutioneller Distanz zwischen Sender und Empfänger mehrere Intermediäre notwendig sind.

Im Vergleich zum Zahlungsverkehr ist die Anzahl der Intermediäre im Wertpapierhandel um einiges größer und komplizierter. Börsen, Zentralverwahrer, Handelsteilnehmer, Clearinghäuser, Banken sind in der Wertpapierabwicklung in Prozessen und Schnittstellen involviert.

3.6. Einsatzmöglichkeiten in Banken

Untersuchungen der EZB und der Bank of Japan zur DLT

Bereits im Dezember 2016 wurde von den beiden Zentralbanken das Projekt “Stella” ins Leben gerufen, um zu untersuchen, ob die DLT in der Lage ist, das gegenwärtige Real-Time-Gross-Settlement-System (RTGS) zu ersetzen. Als Impulsgeber zu dieser möglichen Systemerneuerung kann vor allem die Bank of England gesehen werden, die sehr aktiv eine Transformation gen Blockchain-Technologie forciert. Allerdings zielt die Tendenz der Bank of England auch eher auf eine DLT-Kompatibilität hin, anstatt zeitnah eine vollständige Umstellung vorzusehen.

Der Bericht der EZB und BoJ geht mit den Bestrebungen der Bank of England einher, indem der DLT zwar ein hohes Potential eingeräumt wird, diese allerdings noch nicht bereit sei, das Real-Time-Gross-Settlement-System zu ersetzen.

Vergleichende Untersuchungen zwischen RTGS und DLT haben ergeben, dass durchaus das Potential besteht, dass die DLT die Anforderungen an große Zahlungsabwicklungssysteme erfüllen kann. Allerdings bringt die Validierung von Transaktionen und das Erreichen eines Konsens eine deutliche Komplexitätssteigerung, verglichen mit zentralistischen Ansätzen, mit sich (Müller, 2017).

Die ursprüngliche Blockchain Technologie wurde für die Nutzung von Kryptowährungen geschaffen. Anonyme und direkte Übertragungen von Bitcoins sind eines der Hauptgründe für ihre Beliebtheit.

Die Nutzung im realen Finanzsystem ist nur durch Optimierungen vorstellbar, die zum Teil bei der DLT umgesetzt wurden. Zum Beispiel würden für die Anwendung im Finanzsektor nur Private Ledger auf Grund der Identifizierbarkeit in Frage kommen.

Eine weitere Herausforderung ist der Datenschutz. In der Blockchain ist jede Transaktion für jeden ersichtlich. Somit könnte jeder andere Netzwerkteilnehmer einsehen, wieviel Geld auf einem Konto verwaltet wird oder welche Zeitschriften-Abonnements von einer Person monatlich bezogen werden. Diese Herausforderung wäre nur durch eine Kombination von den heutigen Netzwerkstrukturen und der der DLT-Technologie zu meistern.

Lösungsansätze wären, nicht alle Daten dezentral zu speichern, sondern es wird ein Subnetzwerk mit beschränkter Einsicht erstellt. (Forward Security). Zudem stellt auch die Anzahl der Transaktionen eine Hürde dar. Während das Blockchain-Netzwerk global circa 350 000 Transaktionen täglich abwickelt, beträgt die Anzahl in Deutschland getätigter Transaktionen täglich mehr als 75 Millionen. Zusätzlich muss ein Bindeglied zwischen der realen und digitalen Welt geschaffen werden, da Kryptowährungen bisher keine realen Ansprüche darstellen, wie dies im Fall einer Aktie ist. Zwar wird der Handel eines Produktes erfasst und gespeichert, jedoch sind dadurch die Existenz und die Eigenschaft eines Gutes noch nicht bestätigt (Bundesbank I. , 2017).

Für den Einsatz im Alltag der Distributed-Ledger-Technology ist die weitere, intensive Forschung und Entwicklung notwendig.

Der Transfer als Technik hinter virtuellen Währungen im Zahlungsverkehr und Wertpapierabwicklung bekundet sich als eine komplexe Aufgabe, welche es zu meistern gilt, bevor diese alltagstauglich sein soll. Es sind diverse Anpassungen und Veränderungen notwendig.

Noch ist fraglich, ob tatsächlich Transaktionen ohne Intermediäre in der Finanzwelt der Zukunft verwirklicht werden kann. Auch die Tatsache, dass die gegenwärtigen Transaktionsvolumina zu unterschiedlich für ein qualifiziertes Fazit sind, lässt keine zuverlässige Einsatzprognose zu.

3.7. Einsatzmöglichkeiten in der Industrie

Durch Smart Contracts könnten in Zukunft stark arbeitsaufwendige und kostenintensive Arbeitsabläufe, insbesondere in der Industrie und Logistik, effizienter gestaltet werden. Im Bereich Immobilien hätten Eigentümer, durch die sichere und nicht veränderbare Blockchain, großen Nutzen ihre Rechte auf Dauer zu beweisen und durchzusetzen.

3.7.1. Einzelhandel – Lebensmittelsicherheit

Das US-amerikanische IT-Unternehmen IBM will mithilfe der Blockchain das globale Problem von verseuchter Nahrung, durch die jährlich 420 000 Menschen sterben, bekämpfen (WHO, 2017). In Kooperation mit dem Einzelhandel Konzern Walmart, arbeitet IBM derzeit an einem Projekt zur Lebensmittelsicherheit. Kunden sollen Sicherheit und Transparenz über die Produkte bekommen. Und das innerhalb von Sekunden. Wie das funktionieren soll?

Die Distributed-Ledger-Technologie bringt großes Potenzial zur Optimierung der Supply Chain mit. Über die Blockchain kann jedes Segment der Produktionskette dokumentieren werden. Was jeweils mit dem Produkt gemacht wurde, wer es bearbeitet hat und wo es überall war.

Somit kann der Kunde Schritt für Schritt die gesamte Reise des Produktes zurückverfolgen. Von welchem Hof stammt das Fleisch, mit welcher Temperatur wurde es gelagert und wurde alles richtig deklariert? Diese Fragen sollen in Zukunft sicher beantwortet werden können.

3.7.2. Transport – E-Mobilität

„Share&Charge“ heißt das Projekt des Startup Unternehmens slock.it in Zusammenarbeit mit Innogy, die Tochtergesellschaft des Energie-Unternehmen RWE. Die Idee ist es, grundlegende Probleme der E-Mobilität zu lösen. Der Auflade Vorgang ist bisher zahlungstechnisch zu kompliziert.

Mit der Blockchain-basierten „Share&Charge“-App wird ein einheitliches, flexibles und sicheres Bezahlungssystem geschaffen und zugleich das Problem von zu wenig öffentlichen Stromtankstellen beseitigt.

Private Haushalte können per App ihre Ladesäulen zu selbstgesetzten Tarifen der Öffentlichkeit zur Verfügung stellen. Der Zahlungsvorgang läuft komplett automatisiert.

Somit können sich E-Mobilisten untereinander vernetzen und dadurch die Ladeinfrastruktur und die Zukunft der e-Mobilität vorantreiben.

Eine Zukunftsvision, die an dieser Stelle nicht fehlen sollte:

Stellen Sie sich vor Ihr Elektroauto hat eine eigene Geldbörse, das sogenannte „Car eWallet“, beziehungsweise eine eigene Identität, mit der es sich ausweisen kann, natürlich auf Blockchain-Basis. Wenn man an einer Ladesäule auflädt, erfolgt der Zahlungsvorgang komplett autonom, Maschinen bezahlen praktisch Maschinen. Steht man an einer roten Ampel, kann das Auto sich ganz einfach für ein paar Minuten über eine Induktionsschleife aufladen und in Sekundenschnelle die Zahlung mit der Ampel abwickeln.

Klingt verrückt, könnte aber in naher Zukunft Realität sein.

3.7.3. Energiewirtschaft

Die „Enerchain-Initiative“ ist eine Kooperation von Ponton mit E.ON und 33 weiteren europäischen Energieunternehmen.

Der Ansatz ist, einen Blockchain-basierten Marktplatz für den Energiehandel zu schaffen und somit die Kosten der Strombeschaffung einzusparen.

Unternehmen können über die Enerchain Software anonym Aufträge an ein dezentralisiertes Orderbuch senden, welche dann von anderen Unternehmen durchgeführt werden können. Das Ganze läuft „peer-to-peer“ ab, also direkt zwischen den zwei Parteien ohne einen zentralen Mittelsmann.

Wie genau Blockchain für den Energiehandel funktioniert, erklärt Michael Merz, Managing Director bei Ponton, in einem Kapitel in „Blockchain technology. Introduction for business and IT managers.“ (Burgwinkel et al., 2016).

Vorgestellt wird ein Szenario für das Jahr 2020: die aktuellen Prozesse im Bereich des Energiehandels werden nicht abgelöst durch die Blockchain, sondern eher unterstützt. Das bedeutet die Blockchain könnte genutzt werden, um als eine Art „Kommunikationskanal“ zur Verbesserung des Datenaustauschs beizutragen.

Die Kommunikation ist einerseits zwischen den einzelnen Nodes (Knoten), welche jeweils von einem der wesentlichen Akteure betrieben werden, und andererseits zwischen Node und Teilnehmer gesichert.

Merz erklärt, dass hierbei der wohl wichtigste Effekt der Blockchain die Standardisierung ist. Man kann sich in diesem Fall die Blockchain wie einen riesigen Daten-Container vorstellen. Jeder Spieler kann Daten in diesen Container werfen, welche wiederum von jedem anderen Spieler gelesen werden können, da immer dieselbe Formierung genutzt wird (Ponton, 2017).

3.8. Einsatzmöglichkeiten in anderen Bereichen

3.8.1. Non Profit Organisationen

Auch für ein anderes Problem scheint Blockchain der Schlüssel zu sein. Das UN World Food Programme will den weltweiten Hunger bekämpfen und leistet aktuell Spenden und Hilfslieferungen in der Flüchtlingskrise. Am Standort München gab es die innovative Idee, Flüchtlingen ein virtuelles Konto auf Blockchain-Basis zu geben, um somit Transaktionen abwickeln zu können. Syrische Flüchtlinge gehen bereits Einkaufen und Bezahlen per Augenscan. Die Blockchain vergleicht die Netzhaut mit zuvor gespeicherten biometrischen Daten. Dadurch kann genau verfolgt werden wer wann etwas gekauft hat. Die Hilfsorganisation kann dann mit den jeweiligen Geschäften vor Ort wöchentlich die Zahlungen abwickeln.

Das macht zum einen die Abrechnung einfacher, zum anderen spart man enorm an Bankgebühren, die dann wiederum für mehr Essen verwendet werden können.

Bis zum Jahr 2030 soll durch diese neue Technologie das Hungerproblem der Welt gelöst werden.

3.8.2. Gesundheitswesen

Da auf der Blockchain Daten beinahe vollständig manipulationssicher dezentral gespeichert werden können, haben sowohl große Pharmakonzerne, sowie auch Gesundheitsbehörden ein Interesse daran. Patientendaten und Genanalysen könnten dadurch sicherer gespeichert und übermittelt werden. Klinische Tests könnten fehlersicher gestaltet werden.

Deloitte hat ein White Paper veröffentlicht, wie die Blockchain, nachdem es schon ein amerikanisches Forschungsprojekt („Precision Medicine Initiative, Patient Care and Outcomes Research“, kurz PCOR) dazu gab, auch im deutschen Gesundheitswesen eingesetzt werden könnte (Deloitte, 2017).

„Die Blockchain bietet ein vielversprechendes, neues, dezentrales Framework für eine verstärkte Integration von Patienten- und Gesundheitsinformationen über eine Reihe von Anwendungen und Akteuren“ heißt es. Der Begriff „Interoperabilität“ spielt hierbei eine wichtige Rolle.

Interoperabilität, also die „Fähigkeit eines Systems mit anderen gegenwärtigen oder zukünftigen Produkten oder Systemen ohne Einschränkungen hinsichtlich Zugriff oder Implementierung zusammenzuarbeiten bzw. zu intera-

gieren“ (<http://interoperability-definition.info/de/>) ist wohl das problematischste Thema im Gesundheitswesen. „Patienten haben ein Recht auf Standards. Interoperabilität ist eine ethische Verpflichtung“ betont auch Prof. Dr. Peter Haas, Fachhochschule Dortmund (Ärzteblatt, 2017).

Dem zu entnehmen, ist ein großes Problem im deutschen Gesundheitssystem der Datenaustausch. Schwachstellen sind hierbei beispielsweise die zu komplexen Regeln und Benutzerrechte, der limitierte Zugriff auf Gesundheitsdaten der Bevölkerung und die verschiedenen Datenstandards. Zur Verbesserung dieser und weiterer Schwachstelle muss eine „technische Infrastruktur“ geschaffen werden, um als Basis für eine sichere Kommunikation fungieren zu können. Blockchain könnte so ein System sein, welches die technischen Voraussetzungen für eine Standardisierung und Vernetzung erfüllt.

Durch den dezentralen und sicheren Zugriff auf Daten, der durch die Blockchain gewährleistet wird, könnten mehr Parteien einfacher am Gesundheitsmarkt teilnehmen. Probleme betreffend den Datenschutz würden über Smart Contracts geregelt und der gesamte Datenaustausch würde in standardisierter Form erfolgen.

Aufgrund von Vorteilen wie den Aufgeführten, wäre eine Nutzung der Blockchain-Technologie im deutschen Gesundheitswesen für einen sicheren Austausch von Patientendaten und eine gute Kooperation der einzelnen Gesundheitseinrichtungen, durchaus zu denken.

3.8.3. Demokratie 2.0

Werfen wir einen Blick auf eines der wichtigsten Systeme im deutschen Bundesstaat: das Wahlsystem. Noch gehen wir persönlich in Wahlbüros, setzen ein Kreuz auf Papier und geben somit unsere Stimme ab. Für viele mittlerweile zu kompliziert oder zu unwichtig, wie die sinkende Wahlbeteiligung der deutschen Bürger in den letzten Jahren zeigt. Eine einfache Lösung scheinen digitale Wahlen zu sein. „Handy raus, ein Klick auf den gewünschten Kandidaten und fertig“ heißt es in einem Artikel im Handelsblatt (Müller, 2017).

Die Idee Wahlen digital durchzuführen ist jedoch nicht neu. Auf den Gedanken eine höhere Wahlbeteiligung über das Internet zu erreichen hatten schon viele. Dennoch scheiterte es bisher an der Umsetzung. Woran es nämlich fehlt, ist Sicherheit.

Alle Systeme, die uns momentan zur Verfügung stehen, können gehackt werden.

Auch in der aktuellen Form des Wahlsystems gibt es einen Mangel, der mit einem neuen, ausgefeilten System zu beheben wäre: Vertrauen.

Was passiert nachdem wir unseren Stimmzettel eingeworfen haben?

Wir müssen darauf vertrauen, dass alles richtiggemacht wird, sowohl mit unserer Stimme, als auch mit allen anderen Stimmen. Wir müssen darauf vertrauen, dass die Wahlarbeiter ihren Job ordnungsgemäß machen, dass die Wahlaufsicht ihren Job macht und so weiter. Im Endeffekt besteht das Wahlsystem daraus vielen Personen und vielen Prozeduren zu vertrauen.

Was wäre aber, wenn jedem Wähler eine 100-%ige Sicherheit gewährleistet würde, dass seine Stimme korrekt gezählt wird, diese Stimme geheim bleibt und somit ein fälschungssicheres Wahlergebnis entsteht?

Ein Blockchain-basiertes System könnte genau das möglich machen. Ein einfacher Klick über eine App auf dem Smartphone und schon hat man seine Stimme abgegeben. Die Blockchain würde alle Stimmen direkt automatisch zählen und der gesamte Vorgang wäre transparent und nachvollziehbar für jeden.

4. Kernaussagen unserer Untersuchungen

1. Das Thema ICOs ist grenzüberschreitend und kann nur global reguliert und eingeordnet werden.
2. Aus unserer Sicht finden wir digitale Recheneinheiten aus ökonomischer und ökologischer Sicht nicht effizient. Die ökologische Ineffizienz richtet sich auf den hohen Stromverbrauch der Hash Berechnung und schädigt die Umwelt.
3. Als Ergebnis unserer Untersuchung betrachten wir den Bitcoin als eine Recheneinheit, da beim Mining der Nummernkreis eines Codes um 12,5 Bitcoins fortgeschrieben wird. Das ist nichts anderes als ein hinzuaddieren von Zahlen.
4. Die Blasenbildung bei Bitcoin ist aus unserer Sicht mit Ja zu beantworten. Die Gefahren ansteckender Effekte auf die reale Wirtschaft und den Finanzmarkt sind nach unseren Untersuchungen schwach bis bedeutungslos.
5. Tokens erfüllen die Kernfunktionen von Geld – Wertspeicher, Zahlungsmittel und Recheneinheiten – nur sehr bedingt.
6. Spekulationsblasen haben immer zu Veränderungen in der Wirtschaft und der Gesellschaft geführt. Spannend wird, welche Veränderungen durch die Blockchain-Technologie in Geschäftsprozessen und Wertschöpfungsketten entstehen.
7. Es besteht keine Gefahr für die Realwirtschaft oder den Finanzsektor allerdings sollte die Entwicklung von Kryptowährungen beobachtet werden.
8. Die Granularität der Adressenkonzentration im Bitcoin ist sehr breit und stellt somit kein Risiko oder Übertragungseffekt auf die reale Wirtschaft dar, da anzunehmen ist, dass die geringen Bestände der Anleger nicht kreditfinanziert sind.
9. Die Marktkapitalisierung von ICO's bzw. Bitcoin ist als zu gering anzusehen um einen negativen Übertragungseffekt auf den Finanzsektor oder die Realwirtschaft zu erzeugen.
10. Die Verwendung der digitalen Währung Bitcoin als Zahlungsmittel zu anderen Zahlungsnetzwerken ist vergleichsweise sehr gering. Sie beträgt nicht einmal 1 % der Paypal-Transaktionen. Mit durchschnittlich 60.000

Transaktionen pro Tag liegt der Bitcoin weit hinten im Vergleich zu anderen bekannten Zahlungsmitteln wie Visa oder Master Card.

5. **Abbildungsverzeichnis**

Abbildung 1: Unterschiede ICO versus IPO	7
Abbildung 2: Regulatorische Unterschiede IPO zu ICO	8
Abbildung 3: Übersicht Kernaussagen der Aufsichtsinstanzen zu ICO	16
Abbildung 4: Kryptobörsen im Vergleich	22
Abbildung 5: Umsatzstärkste Kryptowährungen	22
Abbildung 6: Adressenkonzentration Bitcoin	26
Abbildung 7: Candle-Chart Bitcoin	29
Abbildung 8: Anzahl Zahlungstransaktionen im Vergleich	32
Abbildung 9: Übersicht Mining Pools weltweit	33
Abbildung 10: Bezahlung von Bitcoin von Wallet zu Wallet	36
Abbildung 11: Hash-Transaktion	37
Abbildung 12: Zentrale, dezentrale und verteilte Netzwerke	40

Literaturverzeichnis

- aktienrunde. (2017). *Bitcoin Trading - So funktioniert der erfolgreiche Handel mit Kryptowährungen*. Abgerufen am 23. 12 2017 von <https://www.aktienrunde.de/bitcoin-trading/>
- BaFin. (2016). *Virtuelle Währungen/Virtual Currency*. Von https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html abgerufen
- BaFin. (2017). Journal Initial Coin Offering. Frankfurt: BaFin.
- BaFin. (2018). *Virtuelle Währungen/Virtual Currency (VC)*. Abgerufen am 2018 von https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html
- Baran, P. (1964). *Paul Baran and the Origins of the Internet*. Abgerufen am 10. 1 2018 von <https://www.rand.org/about/history/baran.html>
- Bitcoin Deutschland AG. (2017). Abgerufen am 30. 12 2017 von <https://www.bitcoin.de/de/faq/welche-gebuehren-fallen-beim-kaufen-und-verkaufen-von-bitcoins-auf-bitcoinde-an/17.html>
- Bitcoin, M. (25. 1 2018). *Bitcoin Masons*. Abgerufen am 25. 1 2018 von <https://www.bitcoinmasons.com/>
- Bitcoinbloghalf. (2018). *Bitcoin Block Reward Halving Countdown*. Abgerufen am 13. 01 2018 von <http://www.bitcoinblockhalf.com>
- Bitcoinmag.de. (26. 12 2017). *Bitcoin Handel*. Von <https://www.bitcoinmag.de/bitcoin-handel/erfahrung-test-kryptoexchange-kraken/a-103> abgerufen
- Bitcoin-Markplatz. (2017). *Das Bitcoin Whitepaper von Satoshi Nakamoto*. Abgerufen am 19. 11 2017 von <https://www.bitcoin.de/de/bitcoin-whitepaper-deutsch>
- bitinfocharts. (2018). *bitcoin adresses*. Abgerufen am 30. 1 2018 von <https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html>
- boerse.ARD.de. (2017). <https://boerse.ard.de/anlageformen/kryptowaehrungen/fed-und-ezb-warnen-vor-bitcoin100.html>. Von FED und EZB warnen vor Bitcoin: <https://boerse.ard.de/anlageformen/kryptowaehrungen/fed-und-ezb-warnen-vor-bitcoin100.html> abgerufen
- Boerse-online.de. (25. 12 2017). *Bitcoin auf Höhenflug: Die wichtigsten Fragen und Antworten rund um die Kryptowährung*. . Von <http://www.boerse-online.de/nachrichten/aktien/Bitcoin-auf-Hoehenflug-Die-wichtigsten-Fragen-und-Antworten-rund-um-die-Kryptowae> abgerufen
- Börsen-Zeitung. (14. November 2017 Nr. 218). ESMA kreist Krypto-Finanzierungen ein. *Börsen-zeitung* , Seite 5.
- Börsen-Zeitung. (2017). *Börsen-Zeitung*. Von Warnungen vor Bitcoin werden lauter: Fed: Eine großflächige Ausbreitung könnte die Finanzstabilität gefährden: www.boersenzeitung.de abgerufen
- Börsenzeitung. (30. 1 2018). Krypto Nation unter Schock. *Börsenzeitung*, S.3, Nr. 20.
- Broker-Bewertungen.de. (27. 12 2017). *Bitfinex Erfahrungen und Test*. Von <https://broker-bewertungen.de/erfahrungsberichte/bitfinex> abgerufen
- Bryan, F. e. (7. 1 2005). *Peer-to-Peer Communication Across Network Address Translators*. Abgerufen am 2018 von <http://www.bford.info/pub/net/p2pnat/> [07.01.2018].
- BTC-ECHO. (2016). *Bitcoin bleibt beliebteste Währung im Darknet*. Abgerufen am 30. 12 2017 von <https://www.btc-echo.de/bitcoin-beleibtbeste-waehrung-im-darknet/>
- Bundesbank. (2017). Kryptowährungen. Frankfurt am Main.
- Bundesbank. (2018). *Begriff und Aufgabe des Geldes*. Abgerufen am 8. 2 2018 von https://www.bundesbank.de/Redaktion/DE/Dossier/Service/schule_und_bildung_kapitel_1.html?notFirst=true&docId=153022#chap
- Bundesbank, I. (13. 12 2017). Bitcoin und Blockchain Technologie. (S. F. uas, Interviewer)
- Chainthat. (2016). *Blockchain Basics Explained - Hashes with Mining and Merkle trees*. Abgerufen am 26. 12 2017 von <https://www.youtube.com/watch?v=lik9aaFisI4>

- coinhero. (16. 2 2018). *CME Bitcoin Futures*. Von <https://coin-hero.de/erste-cme-bitcoin-futures-laufen-am-26-01-kehrtwende-fuer-den-kryptomarkt/> abgerufen
- Coinmarketcap. (2018). *Coinmarketcap*. Von <https://coinmarketcap.com/currencies/volume/24-hour/> abgerufen
- Coinschedule. (2017). *coinschedule.com*. Von <https://www.coinschedule.com/stats.html> abgerufen
- Cointelegraph. (2017). *Karmacoin Becomes First Cryptocurrency to Issue Shares*. Abgerufen am Dezember 2017 von Cointelegraph.com.
- Commerzbank. (2017). *Blockchain: Mehr als Bitcoin*. Von <https://research.commerzbank.com/delegate/publication?params=2m7%2BDQO2CMQNGR2L0PoBvLF9I3Hf2b6yTTLDSi%2BvIrG9dLM6sGJ1smz5YSY6etBo> abgerufen
- Deloitte. (2017). *Vorstellung der Blockchain Technologie*. Von <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Vorstellung%20der%20Blockchain-Technologie.pdf> abgerufen
- Deutsche Bundesbank . (2017). *Aufgaben*. Abgerufen am 25. 12 2017 von <https://www.bundesbank.de/Navigation/DE/Aufgaben/aufgaben.html>
- Dörken. (13. 1 2018). *Regierung will gegen Miner vorgehen*. Abgerufen am 13. 1 2018 von China schränkt Bitcoin ein - wegen eines Problems, das auch Deutschland droht: https://www.focus.de/finanzen/boerse/kryptowaehrungen/regierung-will-gegen-miner-vorgehen-china-schraenkt-bitcoin-ein-wegen-eines-problems-das-auch-deutschland-droht_id_8277323.html
- Dörken, T. (2018). *FOCUS Online: China schränkt Bitcoin ein - wegen eines Problems, das auch Deutschland droht*. Abgerufen am 13. 01 2018 von https://www.focus.de/finanzen/boerse/kryptowaehrungen/regierung-will-gegen-miner-vorgehen-china-schraenkt-bitcoin-ein-wegen-eines-problems-das-auch-deutschland-droht_id_8277323.html
- dpa-AFX, C. (1. 1 2018). *Venezuela stemmt sich mit Gehaltserhöhung gegen Hyperinflation*. Abgerufen am 2018. 1 5 von <https://www.finanzen.net/nachricht/aktien/mindestlohn-angehoben-venezuela-stemmt-sich-mit-gehaltserhoehung-gegen-hyperinflation-5891619>
- E.F.Fama. (1991). *Efficient Capital Markets II*. Journal of Finance. Band 46, Nr. 5 .
- EBA. (2014). *Opinion on virtual currencies*. Von <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> abgerufen
- EBA. (2017). *Von Warning to consumers on virtual currencies*: <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> abgerufen
- EBA. (2017). *Von* <http://www.eba.europa.eu/about-us> abgerufen
- ECB. (Oktober 2012). *Virtual Currency Schemes*. Von <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> abgerufen
- ECB, E. C. (2015). *Virtual currency schemes - a further analysis*. Von <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> abgerufen
- ECB, E. C. (2017). Abgerufen am 22.. 12. 2017 von <https://www.ecb.europa.eu/ecb/html/>
- Elsner, D. (2. 2 2018). *Virtuelle Währungen am Beispiel des Bitcoin – Eine reale Herausforderung für den Zahlungsverkehr* . Von http://www.blicklog.com/2015/02/05/virtuelle-whrungen-am-beispiel-des-bitcoin-eine-reale-herausforderung-fr-den-zahlungsverkehr-teil-2/?ak_action=reject_mobile abgerufen
- ESMA. (2017). *ESMA The Distribute Ledger Technologie Applied to Securities Markets*. Von https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt_0.pdf abgerufen
- ESMA. (2018). Abgerufen am 10.. 1 2018 von <https://www.esma.europa.eu/>
- ESMA. (2018). *Highlights ICO risks for investors and firms*. Abgerufen am 10. 1 2017 von <https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms>
- European Central Bank, E. (2017). *Digital transformation of the retail payments ecosystem*. Abgerufen am 2017 von Yves Mersch, Member of the Executive Board of the ECB, at the Joint ECB and Banca d'Italia

- conference, Rome, 30 November 2017:
<https://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp171130.en.html>
- European Central Bank, E. (kein Datum). *Digital transformation of the retail payments ecosystem*. Von Yves Mersch ECB and Banca d'Italia conference, Rome, 30 November 2017:
<https://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp171130.en.html> abgerufen
- Finanzen. (24. 12 2017). *Bitcoin kaufen – diese Möglichkeiten gibt es*. Von
<https://www.finanzen.net/ratgeber/kryptowaehrung/bitcoin-kaufen> abgerufen
- Finanzen. (2017). *Finanzen*. Von Diese drei Voraussetzungen muss der Bitcoin erfüllen, um eine echte Währung zu sein: <http://www.businessinsider.de/diese-voraussetzungen-muss-bitcoin-erfullen-um-eine-waehrung-zu-werden-2017-11>> abgerufen
- Finanzen*. (8. 1 2018). Von Das sagen die Notenbanken zu Bitcoin, Ripple und Co:
<https://www.finanzen.net/nachricht/devisen-von-warnung-bis-akzeptanz-das-sagen-die-notenbanken-zu-bitcoin-ripple-und-co-5900560Y> abgerufen
- Finanzen.net. (25. 2 2018). *Euro Stoxx 50*. Von https://www.finanzen.net/index/Euro_Stoxx_50 abgerufen
- Finanznachrichten. (2017). *Draghis Aussagen über Bitcoin vor Europäischen Parlament*. Von
<http://www.finanznachrichten.de/nachrichten-2017-09/41808228-bitcoin-steigt-nach-draghis-aussagen-ueber-kryptowaehrungen-380.htm> abgerufen
- Handelsblatt. (2016). *Treffpunkt für Kriminelle und Dissidenten*. Abgerufen am 30. 12 2017 von
<http://www.handelsblatt.com/technik/it-internet/digitale-parallelwelt-darknet-treffpunkt-fuer-kriminelle-und-dissidenten/13659094.html>
- Handelsblatt. (27. 12 2017). *Bitcoin Kurs erholt sich* . Von
<http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/kryptowaehrung-bitcoin-kurs-erholt-sich/20792568.html> abgerufen
- Handelsblatt. (11 2017). *Globaler Hype um Bitcoin und Co*. Abgerufen am 2017. 11 16 von Die Aufsicht greift ein – von Tokio bis New York: <http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/globaler-hype-um-bitcoin-und-co-china-hartes-vorgehen-im-wichtigsten-markt/20482592-3.html>
- Hanke, S. F. (2017). *Forbes, Maduro's 'Petro' Cryptocurrency Will Join Chavez's Bolivar Fuerte*. Von In the Graveyard: <http://www.forbes.com/sited/stevehanke> abgerufen
- Haufe. (10. 12 2015). *EuGH Kommentierung: Steuerbefreiung von Umsätzen mit Bitcoins*. Abgerufen am 2017 von
<https://www.haufe.de/steuern/rechtsprechung/steuerbefreiung-von-umsaetzen-mit-bitcoins.html>
- Heckmann, J. &. (1. 9 2016). *Smart Contracts – Anwendungen der Blockchain-Technologie*. *Computer und Recht* , S. Band 32, Heft 9.
- Hussein, M. (2017). *legal corner*. Abgerufen am 30. 12 2017 von Bitcoins als E-Geld im Sinne des E-GeldG?:
<http://www.fwp.at/legal-corner/bitcoins-als-e-geld-im-sinne-des-e-geldg/>
- ICO-Rating. (2018). Von <https://icorating.com/> abgerufen
- J.P.Morgan. (2017). *J.P.Morgan, Volatility: keep calm and carry on*. Von www.jpmorganmarkets.com abgerufen
- J.P.Morgan. (16.. Dezember 2017). *Volatility:keep calm and carry on*.
- Jayachandran, P. (11. 11 2017). *Blockchain Explained: The difference between public and private blockchain, Blockchain Unleashed: IBM Blockchain Blog*. Abgerufen am 2017 von
<https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/>
- Kaiser, A. (2017). *Spiegel: Warum der Bitcoin-Boom die globale Energiewende bedroht* . Abgerufen am 30. 12 2017 von <http://www.spiegel.de/wirtschaft/unternehmen/bitcoin-stromverbrauch-bedroht-globale-energiewende-a-1182234.html>
- Kannenberg, A. (10. 1 2017). *Kryptogeld-Wallet Parity: Bug friert Ether-Einheiten im Wert von Millionen ein* . . Abgerufen am 2018 von <https://www.heise.de/newsticker/meldung/Kryptogeld-Wallet-Parity-Bug-friert-Ether-Einheiten-im-Wert-von-Millionen-ein-38829>
- Karma. (2017). *Give Karma* . Von <http://www.givekarma.net/> abgerufen

- Kessler, N. (2018). *Der Aktionär: Bitcoin-Verbot in Südkorea! Das müssen Sie wissen*. Abgerufen am 11. 01 2018 von <http://www.deraktionaer.de/aktie/bitcoin-verbot-in-suedkorea--das-muessen-sie-wissen-353970.htm>
- Klotz, M. (27. 2 2018). *Gar kein Mysterium: Blockchain verständlich erklärt*. Von <https://www.it-finanzmagazin.de/gar-kein-mysterium-blockchain-verstaendlich-erklaert-27960/> abgerufen
- Kölling, M. &. (2017). *Bitcoin fällt, weil Südkorea ihn regulieren will*. Abgerufen am 30. 12 2017 von <http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/kryptowaehrung-bitcoin-faellt-weil-suedkorea-ihn-regulieren-will/20795162.html>
- Kosba, A. M. (2015). *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*. University of Maryland and Cornell University.
- Kryptocoins.net. (26. 12 2017). *Tauschbörsen*. Von <http://kryptocoins.net/tauschboersen/> abgerufen
- Krypto-Magazin. (2017). *Krypto-Magazin*. Von <https://www.krypto-magazin.de/bitcoin-mining-anbietervergleich/> abgerufen
- KWG. (2018). *Gesetz über das Kreditwesen KWG*. Von <https://www.gesetze-im-internet.de/kredwg/BJNR008810961.html> abgerufen
- L.M., K. (2017). *Bitcoin fällt, weil Südkorea ihn regulieren will*. Von <http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/> abgerufen
- Ley, A. (2017). *EZB-Präsident Draghi: Der Einfluss von Krypto-Währungen ist gering*. Von <https://www.btc-echo.de/ezb-praesident-draghi-der-einfluss-von-kryptowaehrungen-ist-gering> abgerufen
- Lielacher, A. (24. 12 2017). *Bitcoin Magazin*. Von <https://bitcoinmagazine.com/authors/alex-lielacher/> abgerufen
- Manager-Magazin. (2017). *Bitcoin-Handel mit anonymen Konten verboten: Südkorea will "anormale Spekulation nicht länger dulden"*. Abgerufen am 30. 12 2017 von <http://www.manager-magazin.de/finanzen/boerse/bitcoin-suedkorea-verlangt-klarnamen-von-boersen-a-1185286.html>
- Market, W. M. (9. 2 2018). *All of the World's Money and Markets in One Visualization*. Von <http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/> abgerufen
- Micijevic, A. (2017). *Handelsblatt: Handelsplattform Coinbase bricht unter Nutzeransturm zusammen*. Abgerufen am 22. 12 2017 von <http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/bitcoin-kursturbulenzen-handelsplattform-coinbase-bricht-unter-nutzeransturm-zusammen/20787930.html>
- Miller, S. &. (2003). *The Digital Path: smart Contracts and the Third World*. Abgerufen am 10. 1 2017 von <http://www.erights.org/talks/pisa/paper>
- Momoh, O. (2017). *Initial Coin Offering (ICO)*. In: *Investopedia*. 20. Dezember 2016 (investopedia.com [abgerufen am 27. Juli 2017]). Abgerufen am 27. Juli 2017 von Investopedia. 20. Dezember 2016 (investopedia.com).
- Müller, D. (4. . Oktober 2017). *EZB vorsichtig optimistisch für Blockchain*. *Börsenzeitung*, S. S.3.
- Müller, D. (25.11.2017). *Palette der Bitcoin-Produkte wird breiter*. *Börsen-Zeitung*. 25.11.2017, Nr. 227, S. 14., Nr. 227, S. 14.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Abgerufen am 09. 01 2018 von <https://bitcoin.org/bitcoin.pdf>
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press , S.48.
- Niggemann, O. (20. 12 2017). *Die besten Bitcoin Anbieter – Bitcoins schnell und günstig kaufen*. V. Von <http://olaf-niggemann.com/die-besten-bitcoin-anbieter-bitcoins-schnell-und-guenstig-kaufen/> abgerufen
- Platzer. (2014). *Bicoïn – kurz & gut*. In J. Platzer, *Banking ohne Banken* (S. 20-21). O'Reilly.
- Powercompare.co.uk. (2017). *Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa*. Abgerufen am 03. 01 2018 von <https://powercompare.co.uk/bitcoin/>
- Presse, A. D. (30. 10 2017). *Viel Sicherheitspotenzial in Blockchain*. Von <http://www.zeit.de/politik/deutschland/2017-12/regierungsbildung-spd-cdu-bundestag-vereidigung-rekord> abgerufen

- ripple.com. (10. 1 2018). *The world's only enterprise blockchain solution for global payments*. Von https://www.ripple.com/?gclid=EAlalQobChMIhsHCtYrG2QIVT54bCh38SwChEAAAYAiAAEgKSpPD_BwE abgerufen
- Roland. (10. 12 2017 a). *Besteuerung von Kryptowährungen*. Von <https://www.finanzgefluester.de/besteuerung-von-kryptowaehrungen/> abgerufen
- Roland. (10. 12 2017 b). Abgerufen am 2017 von Bitcoin Kapitalertragsteuer: Vorsicht vor Fakenews: <https://www.finanzgefluester.de/bitcoin-kapitalertragsteuer>
- Rueß, S. (17. 12 2017). *So funktioniert Blockchain*. Von <https://www.computerwoche.de/a/so-funktioniert-blockchain,3331391> abgerufen
- Schillmann. (2017). *Die 36 besten Bitcoin Seiten zum Bitcoins handeln und verwalten im Test und Vergleich*. Von www.schillmann.com/top-bitcoin-seiten-bitcoins-handeln/ abgerufen
- Schueffel, P. (2017). *The Concise Fintech Compendium*. Freiburg, Schweiz: Institut für Finanzen, Hochschule für Wirtschaft Freiburg.
- Schürmann, L. (9. 1 2018). *Dreht Peking den Strom ab?* Abgerufen am 10. 1 2018 von China plant "geordnetes Ende" von Bitcoin-Mining: www.manager-magazin.de/finanzen/geldanlage/bitcoin-mining-in-china-peking-plant-geordnetes-ende-a-1186821.html
- SEC. (2017). *SEC: US Securities Laws 'May Apply' to Token Sales*. Von www.coindesk.com abgerufen
- Sixt, E. (2016). *Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie*. Wien, Österreich: Springer-Gabler.
- SPIEGEL. (2018). *Südkorea erwägt Verbot von Bitcoin-Handel*. Von <http://www.spiegel.de/wirtschaft/unternehmen/bitcoins-suedkorea-will-handel-verbieten-a-1187288.html> [Zugriff am 11.01.2018]. abgerufen
- Statista. (9. 2 2018). *Geldmenge der Eurozone*. Von <https://de.statista.com/statistik/daten/studie/241800/umfrage/entwicklung-der-geldmenge-m1-in-der-euro-zone/> abgerufen
- Swan, M. (2015). *Blockchain - Blueprint for a New Economy*. O'Reilly Media verlag.
- Thiele, C. -L. (23. 11 2017). *Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt?*. Abgerufen am 25. 12 2017 von Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten?: <https://www.cesifo-group.de/DocDL/sd-2017-22-thiele-diehl-et-al-bitcoin-2017-11-23.pdf>
- VLH. (10. 12 2017). Von Bitcoin, Ethereum & Co: So versteuern Sie Kryptowährungen: <https://www.vlh.de/kaufen-investieren/geldanlage/bitcoin-ethereum-co-so-versteuern-sie-kryptowaehrungen.html> abgerufen
- Weiprecht. (2. 27 2018). *CryptoDeal*. Von <http://alexander-weiprecht.de/> abgerufen
- Winter, A. (Regisseur). (2015). *Deep Web, BOND/360* [Kinofilm].
- Wystoken. (2017). *Wys Token Sale, Definiere E-Commerce neu*. Von <https://www.wystoken.org/de/index.html> abgerufen

Falls Sie Fragen und Anmerkungen zu dem Thema haben, stehe ich Ihnen gerne zur Verfügung.



Frankfurt University of Applied Sciences
Fachbereich 3: Wirtschaft und Recht
Nibelungenplatz 1
60318 Frankfurt
www.frankfurt-university.de

Prof. Dr. Michaela Hönig
Allgemeine Betriebswirtschaftslehre, Finanzwirtschaft und Asset Management
E-Mail: hoenig@fb3.fra-uas.de