Kryptowährungen

Gefährliche Spekulation oder digitale Revolution?

D i p l o m a r b e i t

an der Fachhochschule für öffentliche Verwaltung und Rechtspflege
Meißen,
Fortbildungszentrum des Freistaates Sachsen

vorgelegt von
Kevin Günther
aus Sangerhausen

Meißen, 18.03.2019

Inhaltsverzeichnis

Abkürzungsverzeichnis IV
Abbildungsverzeichnis V
1 Einleitung 1
2 Die Geldtheorie 3
2.1 Geldfunktionen 3
2.1.1 Tausch- bzw. Zahlungsmittel 3
2.1.2 Wertaufbewahrungsmittel 4
2.1.3 Rechnungseinheit 4
2.2 Eigenschaften des Geldes 5
3 Das zweistufige Bankensystem 7
3.1 Geldmenge 7
3.2 Geldschöpfung 8
3.2.1 Wie neues Buchgeld entsteht 8
3.2.2 Grenzen der Buchgeldschöpfung 9
3.3 Geldpolitik 10
4 Die Kryptowährung Bitcoin 12
4.1 Dezentralisierung versus Zentralisierung 12
4.2 Technische Grundlagen 14
4.2.1 Double-spending 14
4.2.2 Das Kontensystem des Bitcoins 15
4.2.3 Die Blockchain 16
4.2.4 Mining 18
4.2.4.1 Der Arbeitsbeweis bzw. proof-of-work 19
4.2.4.2 Anreize für die Miner 19
4.2.4.3 Schöpfung neuer Bitcoins 20
4.3 Sicherheit 21
4.3.1 Sicherheit des Kontensystems 22
4.3.2 Sicherheit der Blockchain 23
4.4 Anonymität 24
4.5 Probleme 26
4.5.1 Energieverbrauch des Konsensmechanismus 26
4.5.2 Volatilität 27
4.5.3 Quantencomputer 28
4.5.4 Skalierung 29
5 Bitcoin als Währung 30
5.1 Bitcoin und die Geldtheorie 30
5.1.1 Geldeigenschaften 30
5.1.2 Geldfunktionen 33

5.1.2.1 Eignung als Tausch- bzw. Zahlungsmittel 33
5.1.2.2 Eignung als Wertaufbewahrungsmittel 34
5.1.2.3 Eignung als Recheneinheit 35
5.2 Gefahren und Risiken 35
5.2.1 Bitcoin versus Zentralbanken 35
5.2.2 Bitcoin versus Geschäftsbank 36
5.2.3 Risiko für die Wirtschaftsstabilität 38
6 Chancen der Bitcoin Technologie 40
6.1 Chancen für Banken und Unternehmen 40
6.2 Weitere Anwendungen der Blockchain Technologie 42
6.2.1 Dezentrale Nachweise und Datenbanken 42
6.2.2 Smart contracts 43
7 Schluss und Ausblick 45
Anlagenverzeichnis IV
Anlage 1: Geldpolitik der EZB V
Anlage 2: Blöcke einer Blockchain VI
Anlage 3: Eine *Bitcoin-Farm* VII
Anlage 4: Teilbarkeit des Bitcoins VIII
Literaturverzeichnis IX
Rechtsquellenverzeichnis XV
Eidesstattliche Versicherung XVI

Abkürzungsverzeichnis

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Aufl.	Auflage
BBankG	Gesetz über die Deutsche Bundesbank
bzw.	beziehungsweise
ca.	circa
d. Verf.	des Verfassers
DLT	Distributed-Ledger-Technologie
EZB	Europäische Zentralbank
sog.	sogenannte
z. B.	zum Beispiel

Abbildungsverzeichnis

Abbildung 1: Bilanz einer Geschäftsbank bei einer Kreditvergabe...……....S. 9

Abbildung 2: Volatilitätsindex des Bitcoins…….……..…….S. 27

1 Einleitung

Es ist Montag, der 15. September 2008. Dieser Tag ist wohl einer der Höhepunkte, der bis heute anhaltenden Finanzkrise. Die amerikanische Investmentbank *Lehman Brothers* meldete an diesem Tag Insolvenz an. Diese spekulierte mit *toxischen*[1] Paketen aus Immobilienkrediten, welche sich als wertlos erwiesen und der Bank milliardenschwere Verluste einbrachten. Die toxischen Wertpapiere verbargen sich jedoch auch in den Bilanzen unzähliger anderer Banken, welche sich aufgrund der immer weiter steigenden Immobilienpreise hohe Renditen erhofften und dafür hohe Risiken eingingen. Als die Preise auf dem Immobilienmarkt wieder sanken, kollabierten die Finanzmärkte, da sich die gehandelten Immobilienkredite als wertlos herausstellten. Die Kreditnehmer konnten die Raten ihres Immobilienkredits nicht mehr bezahlen und das Haus musste zwangsversteigert werden. Das Vertrauen in die gesamte Banken- und Finanzwelt war erschüttert.

Diese Situation stellte eine gute Ausgangslage für ein Geldsystem dar, welches vollkommen auf die Notwendigkeit einer Bank verzichten könnte. Mit einem solchen System müsse man keiner Bank oder einer sonstigen zentralen Institution mehr vertrauen. Am 1. November 2008 stellte ein anonymer Herausgeber, unter dem Pseudonym *Satoshi Nakamoto,* in einer E-Mail ein Konzept vor, welches genau dies ermöglichen solle. Diese E-Mail trug den Titel „Bitcoin: Ein elektronisches Peer-to-Peer[2] Bezahlsystem".[3] Da dieses Konzept auf kryptographischen Verschlüsselungsmethoden basiert, wird der Bitcoin umgangssprachlich als Kryptowährung bezeichnet. Seitdem wurden immer mehr Kryptowährungen entwickelt, welche jedoch alle auf dem Grundkonzept des Bitcoins basieren.

[1] Wertpapiere werden als toxisch bezeichnet, wenn damit eine Forderung verbunden ist, welche ein hohes Ausfallrisiko besitzt. Im Fall Lehman Brothers handelte es sich um Immobilienkredite, welche vom Kreditnehmer nicht mehr beglichen werden konnten.
[2] Peer-to-Peer bedeutet, dass der Vorgang direkt von einem Mitglied zu einem anderen Mitglied stattfindet.
[3] Satoshi Nakamoto 2008, S.1, aus dem Englischen übersetzt, Original: „Bitcoin: A Peer-to-Peer Electronic Cash System".

Ziel dieser Arbeit ist es, die Funktionsweise unseres konventionellen Geldsystems mit der von Kryptowährungen, am Beispiel des Bitcoins zu vergleichen. Durch diese Gegenüberstellung soll einerseits untersucht werden, inwiefern Kryptowährungen unser Bankensystem ersetzen können und andererseits geschlussfolgert werden, welche Risiken und Chancen von Kryptowährungen ausgehen.

Dazu soll in Kapitel 2 erörtert werden, was Geld überhaupt ist und welche Voraussetzungen dieses erfüllen muss. In Kapitel 3 werden die wesentlichen Funktionsweisen und Eigenschaften unseres konventionellen Bankensystems und in Kapitel 4, die des Bitcoins beschrieben. In Kapitel 5 soll untersucht werden, ob der Bitcoin als Geld angesehen werden kann. Weiterhin sollen durch eine Gegenüberstellung des Bitcoins mit dem Bankensystem die ökonomischen Risiken und Gefahren untersucht werden, welche sich ergeben könnten, wenn der Bitcoin konventionelle Währungen verdrängen würde. Im letzten Kapitel werden Chancen und Möglichkeiten der Bitcoin Technologie aufgeführt, um schlussendlich ein Fazit und einen Ausblick auf die Zukunft der Kryptowährungen formulieren zu können.

2 Die Geldtheorie

Bevor wir uns die Frage stellen, ob eine Kryptowährung, insbesondere der Bitcoin, als Geld betrachtet werden kann oder sogar den Platz einer Währung einnehmen kann, muss man sich die Frage stellen, was Geld eigentlich ist. In diesem Kapitel sollen die Eigenschaften und die Funktionen des Geldes erörtert werden.

2.1 Geldfunktionen

In der Nationalökonomie wird der Begriff Geld üblicherweise indirekt definiert. Geld ist alles, was Geldfunktionen erfüllt.[4] Es wird zwischen drei Grundfunktionen unterschieden, nämlich der Funktion als Tauschmittel, als Recheneinheit sowie als Wertaufbewahrungsmittel.[5] Der britische Ökonom Sir John Richard Hicks bezeichnete diese Funktionen auch als Triade des Geldes.[6]

2.1.1 Tausch- bzw. Zahlungsmittel

Seit Jahrtausenden menschlicher Geschichte stand von jeher der Tausch im Mittelpunkt, sowohl von niedrigen als auch hochentwickelten Kulturen. Während beim Naturalhandel reale Güter direkt gegen andere reale Güter getauscht wurden, teilt der Handel mit Geld den Tauschakt in zwei Teilakte.[7] Getauscht wird also Ware gegen Geld und dieses Geld wiederum gegen die eigentlich gewünschte Ware.[8] Dies löst ein wesentliches Grundproblem des Naturalhandels, nämlich das der doppelten *Koinzidenz*[9] der Wünsche.[10] Jenes impliziert, dass der direkte Austausch von Gütern voraussetzt, dass zwei Handelsparteien genau das jeweils andere Gut zum gleichen Zeitpunkt benötigen. Der Einsatz von Geld ist also ein Zwischenschritt, welcher den Handel erheblich vereinfacht.[11]

---

[4] Vgl. Engelkamp, Paul ; Sell, Friedrich L. 2017, S. 166.
[5] Vgl. Gerdesmeier, Dieter 2004, S. 1.
[6] Vgl. Engelkamp, Paul ; Sell, Friedrich L. 2017, S. 166.
[7] Vgl. Issing, Otmar 2011, S. 1.
[8] Vgl. Deutsche Bundesbank 2017, S. 9.
[9] Koinzidenz beschreibt das zeitliche Zusammenfallen zweier Ereignisse.
[10] Vgl. Neubäumer, Renate ; Hewel, Brigitte ; Lenk, Thomas 2017, S. 502.
[11] Vgl. Deutsche Bundesbank 2017, S. 9.

2.1.2 Wertaufbewahrungsmittel

Wenn Geld, welches wir als Wertaufbewahrungsmittel bezeichnen wollen, über die Zeit hinweg wertbeständig ist[12], können die nunmehr zwei getrennten Schritte eines Tausches (Kauf und Verkauf) zeitlich weit auseinander liegen. Wirtschaftssubjekten ist es somit möglich, den Erwerb von Gütern und Dienstleistungen bis auf einen passenden Zeitpunkt aufzuschieben[13] und ihr Geld zu sparen.[14]

2.1.3 Rechnungseinheit

Geld muss als Rechnungseinheit fungieren. Dadurch lassen sich Güterwerte in einer allgemeinen Bezugsgröße ausdrücken und vergleichen.[15] Folgendes Rechenbeispiel verdeutlicht die Tragweite dieser Funktion. Angenommen, auf einem Markt existieren n Güter, wobei n die Anzahl aller Güter beschreibt. Mithilfe der folgenden Formel kann man berechnen, wie viele Preisrelationen ein Käufer, **ohne den Einsatz von Geld**, kennen müsste, um die einzelnen Güter im Vergleich zu anderen Angeboten beurteilen zu können:[16]

$$\frac{\boldsymbol{n} * (\boldsymbol{n} - \mathbf{1})}{\mathbf{2}}$$

Bei 100 verschiedenen Gütern (n = 100) müsste der Käufer nach dieser Formel 4.950 Preisrelationen kennen, um die einzelnen Güter im Vergleich zu anderen Angeboten beurteilen zu können.

Der Einsatz von Geld bietet hier eine erhebliche Vereinfachung. „Geld fungiert als Wertmaßstab.“[17] Somit lassen sich Güterwerte in Preisen ausdrücken, was ihre Vergleichbarkeit erheblich vereinfacht.[18] In Bezug auf das oben genannte Beispiel, in dem 100 Güter (n = 100) auf einem Markt existieren, müsste der Käufer durch den Einsatz von Geld, nur noch 100 Preise anstatt 4.950 Relationen kennen.

[12] Vgl. Gerdesmeier, Dieter 2004, S. 2.
[13] Vgl. Neubäumer, Renate ; Hewel, Brigitte ; Lenk, Thomas 2017, S. 504.
[14] Vgl. Deutsche Bundesbank 2017, S. 10.
[15] Vgl. Deutsche Bundesbank 2017, S. 11.
[16] Formel vgl. Gerdesmeier, Dieter 2004, S. 2.
[17] Deutsche Bundesbank 2017, S. 10.
[18] Vgl. Deutsche Bundesbank 2017, S. 11.

2.2 Eigenschaften des Geldes

Um die vorgenannten Funktionen erfüllen zu können, muss Geld in unserem Idealmodell bestimmte Eigenschaften besitzen. Hier findet man in der Literatur uneinheitliche Ausführungen. Im Folgenden wurden sechs Eigenschaften zusammengetragen, welche Geld besitzen sollte: Es muss allgemein akzeptiert, homogen, haltbar und teilbar sein.[19] Weiterhin muss Geld wertbeständig sein.[20] Es soll noch hinzugefügt werden, dass Geld auch gut transportierbar sein muss.[21]

Akzeptanz: Die deutsche Bundesbank schreibt: „Geld wird nur akzeptiert, wenn alle Besitzer von Geld darauf vertrauen können, dass es seinen Wert behält.“[22] Dieser Wert, von dem die Bundesbank hier spricht, ist lediglich das Vertrauen in das Geld und in die Zentralbank. Das bedeutet, dass die Akzeptanz auf dem bloßen Vertrauen beruht, von anderen als Tauschmittel akzeptiert zu werden.

Homogenität: Damit Geld seine Funktion als Recheneinheit erfüllen kann, muss es gleich beschaffen sein. Es muss in homogene Untereinheiten teilbar sein.[23]

Haltbarkeit: Voraussetzung für die Wertaufbewahrungsfunktion ist, dass das Material des Geldes beständig ist.[24] Im Gegensatz zu verderblichen Handelsgütern, wie zum Beispiel Fleisch oder andere Naturalgüter, muss Geld unverderblich und haltbar sein.

Teilbarkeit: Damit Geld als Tauschmittel fungieren kann, muss es gegen verschiedene Güter und Dienstleistungen zu jeweils unterschiedlichen Preisen gehandelt werden können. Dazu muss Geld entweder physisch teilbar sein oder in entsprechend kleinen Stückelungen zur Verfügung stehen.[25]

---

[19] Vgl. Engelkamp, Paul ; Sell, Friedrich L. 2017, S. 166.
[20] Vgl. Deutsche Bundesbank 2017, S. 10.
[21] Vgl. Gerdesmeier, Dieter 2004, S. 3.
[22] Deutsche Bundesbank 2017, S. 19.
[23] Vgl. Bontrup, Heinz - Josef 2004, S. 437.
[24] Vgl. Deutsche Bundesbank 2017, S. 11.
[25] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 16.

Werterhaltend: Damit die Kaufkraft des Geldes auch zu einem beliebigen späteren Zeitpunkt eingesetzt werden kann, muss es relativ wertbeständig sein.[26] Absolute Wertbeständigkeit kann jedoch aufgrund inflationärer Prozesse nicht möglich sein.[27]

Kompakt: Je kompakter das Geld ist, umso leichter kann es für Transaktionen genutzt werden. Der Transport von Geld darf nicht mit großen Hürden und Kosten verbunden sein, da dies die Funktion als Tauschmittel einschränken würde.[28]

[26] Vgl. Bontrup, Heinz - Josef 2004, S. 437.
[27] Vgl. Bontrup, Heinz - Josef 2004, S. 437.
[28] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 16.

3 Das zweistufige Bankensystem

Um einerseits beurteilen zu können, ob ein dezentrales Zahlungssystem wie der Bitcoin wirklich ohne Banken bestehen kann und andererseits abschätzen zu können, was das für Folgen haben könnte, müssen wesentliche Merkmale und Funktionsweisen unseres konventionellen Bankensystems bekannt sein. In diesem Kapitel soll es deshalb um die Funktionsweise und die Eigenschaften unseres derzeitigen Bankensystems gehen, welches von Zentralbanken gesteuert und beeinflusst wird.

3.1 Geldmenge

Als Erstes sollte die Frage aufkommen, wie sich das aktuell in Umlauf befindliche Geld eigentlich zusammensetzt. In der Eurozone gibt es ein sogenanntes zweistufiges Bankensystem mit den Zentralbanken[29] an der Spitze sowie den normalen Geschäftsbanken[30] auf der nächsten Ebene.[31] Aufgrund dieser Zweiteilung wird zwischen dem Zentralbankgeld und dem Geschäftsbankengeld unterschieden.[32]

Zentralbankgeld ist Geld, welches nur von den Zentralbanken geschaffen werden kann.[33] Es besteht aus dem umlaufenden Bargeld sowie den Sichtguthaben der Geschäftsbanken bei der Zentralbank.[34] Wenn eine Geschäftsbank Sichteinlagen (also Guthaben) bei einer Zentralbank unterhält, bedeutet das, dass diese einen Kredit bei der Zentralbank aufgenommen hat, um sich Zentralbankgeld zu beschaffen. Geschäftsbanken benötigen Zentralbankgeld zum einen zur Abwicklung des Zahlungsverkehrs, zum anderen zur Einhaltung der sogenannten Mindestreservepflicht bei der Zentralbank.[35] Außerdem benötigen Geschäftsbanken Zentralbankgeld zur Befriedigung des Bargeldbedarfs ihrer Kunden.[36] Diese Beschaffung von Zentralbankgeld wird auch als Refinanzierung bezeichnet. Man

[29] Das Zentralbankensystem besteht aus der EZB und den nationalen Geschäftsbanken.
[30] z.B. Sparkasse, Volksbank oder Commerzbank.
[31] Vgl. Engelkamp, Paul ; Sell, Friedrich L. 2017, S. 169.
[32] Vgl. Engelkamp, Paul ; Sell, Friedrich L. 2017, S. 169.
[33] Vgl. Deutsche Bundesbank 2017 S. 74.
[34] Vgl. Naser, Rainer, Dr.: Wie kommt das Geld in die Welt? In: Wochenschau, Politik und Wirtschaft im Unterricht. August 2018, S. 18.
[35] Vgl. Deutsche Bundesbank 2017, S. 74.
[36] Vgl. Deutsche Bundesbank 2017, S. 78.

kann somit sagen, dass die Zentralbanken den Geschäftsbanken Liquidität geben bzw. entziehen.[37] Das Zentralbankgeld wird auch als Basisgeld bezeichnet.[38]

Unter Geschäftsbankgeld versteht man das von den Geschäftsbanken geschaffene Geld, welches auch als Buchgeld beziehungsweise Giralgeld bezeichnet wird.[39] Dieses Buchgeld bildet mit Abstand den größten Anteil der im Umlauf befindlichen Geldmenge.[40]

3.2 Geldschöpfung

Wie im vorherigen Punkt erwähnt, können Geschäftsbanken Geld schaffen. Doch nicht nur diese, sondern auch Zentralbanken können dies tun und damit die jeweilige Geldmenge erhöhen. Die Schöpfung des Zentralbankgeldes erfolgt analog zur Schöpfung des Geschäftsbankgeldes.[41] Der Prozess der Geldschöpfung ist essenziell, um die Funktionsweise unseres Finanzsystems zu verstehen. Dieser Punkt ist weiterhin wichtig, da Kryptowährungen einen vollkommen anderen Ansatz verfolgen.

3.2.1 Wie neues Buchgeld entsteht

Der hierbei interessanteste Punkt ist die Schöpfung des Buchgeldes der Geschäftsbanken. Buchgeld existiert nur in den Geschäftsbüchern der Banken.[42] Jeder Euro eines Bankkunden auf seinem Konto bei zum Beispiel der Sparkasse ist Buchgeld. Der einfachste Weg, wie dieses Buchgeld entsteht, besteht darin, dass ein Bankkunde Bargeld auf sein Konto einzahlt.[43] Bei diesem Vorgang, wird jedoch kein neues Geld geschaffen, da das Geld des Kunden lediglich in eine andere Form umgewandelt wird.[44] Es existiert also nicht mehr in Form von Banknoten bzw. Münzen, sondern lediglich als Sichteinlage bei der Bank. Die Bank kann dieses Geld auch quasi aus dem Nichts entstehen lassen.[45] Dies geschieht

[37] Vgl. Deutsche Bundesbank 2017, S. 75.
[38] Vgl. Issing, Otmar 2011, S. 6.
[39] Vgl. Issing, Otmar 2011, S. 6.
[40] Vgl. Deutsche Bundesbank 2017, S. 71.
[41] Vgl. Engelkamp, Paul ; Sell, Friedrich L. 2017, S. 172.
[42] Vgl. Deutsche Bundesbank 2017, S. 56.
[43] Vgl. Engelkamp, Paul ; Sell, Friedrich L. 2017, S. 172.
[44] Vgl. Deutsche Bundesbank 2017, S. 57.
[45] Vgl. Müller, Dirk 2010, S. 68.

durch Kreditvergabe der Banken beziehungsweise durch den Ankauf von Vermögensaktiva.[46]

Das folgende Beispiel soll diesen Prozess veranschaulichen. Die Bank X räumt einem Kunden einen Kredit in Höhe von 10.000 Euro ein. Betrachtet man nun die Bilanz der Bank stellt man fest, dass sich auf der Aktivseite eine Kreditforderung an den Kunden in Höhe von 10.000 Euro und auf der Passivseite eine Verbindlichkeit in Höhe von 10.000 Euro gegenüber dem Kunden. Diese Verbindlichkeit der Bank stellt die Sichteinlage des Kunden dar. Dieser verfügt nun über 10.000 Euro, mit welchen er Transaktionen tätigen kann. Die folgende Abbildung veranschaulicht diesen Buchungsprozess:[47]

Aktiva	**Bank X**		Passiva
10.000 €	Kreditforderung an Kunde 1	Sichteinlage Kunde 1 (Verbindlichkeit)	10.000 €

Abbildung 1

Buchgeld entsteht also in einem reinen Buchungsakt.[48]

3.2.2 Grenzen der Buchgeldschöpfung

Die gerade beschriebene Buchgeldschöpfung ist jedoch nicht vollkommen frei von Grenzen. Hierbei anzumerken ist, dass die Geschäftsbanken, wie bereits an vorheriger Stelle erwähnt, Bedarf an Zentralbankgeld haben. Dieser Bedarf an Zentralbankgeld bildet die Grundlage für die Zentralbanken, durch Geldpolitik die Währungsstabilität zu sichern.[49] Anders formuliert trifft folgende Aussage zu: „Geldpolitik und bankenaufsichtliche Regeln begrenzen die Geldschöpfung.“[50]

Zum einen sind die Geschäftsbanken dazu verpflichtet, „einen bestimmten Prozentsatz ihrer Kundeneinlagen als sog. Mindestreserve auf ihrem Zentralbankkonto und somit in Form von Zentralbankgeld bei ihr [(der Zentralbank), d. Verf.]

[46] Vgl. Naser, Rainer, Dr.: Wie kommt das Geld in die Welt? In: Wochenschau, Politik und Wirtschaft im Unterricht. August 2018, S. 22.
[47] Abbildung in Anlehnung an Deutsche Bundesbank 2017, S. 77.
[48] Vgl. Naser, Rainer, Dr.: Wie kommt das Geld in die Welt? In: Wochenschau, Politik und Wirtschaft im Unterricht. August 2018, S. 22.
[49] Vgl. Deutsche Bundesbank 2017, S. 18, 85.
[50] Deutsche Bundesbank 2017, S. 78.

zu halten."[51] Dieser Prozentsatz wurde letztmals von der Europäischen Zentralbank mit Wirkung vom 18.01.2012 auf 1 % festgelegt.[52] Zum anderen benötigen Banken Zentralbankgeld für die Abwicklung des bargeldlosen Zahlungsverkehrs untereinander, da Zentralbankguthaben das Zahlungsmittel der Geschäftsbanken untereinander ist.[53] Das ist zum Beispiel der Fall, wenn Kunde A bei der Bank A einen Betrag an Kunde B bei der Bank B überweisen möchte.

Wie bereits an vorheriger Stelle erwähnt, stellt Bargeld einen Teil des Zentralbankgeldes dar. Somit benötigt eine Geschäftsbank Zentralbankgeld in Form von Bargeld, um schließlich den Bargeldbedarf ihrer Kunden befriedigen zu können, welche Bargeld benötigen.

Wie es den Zentralbanken möglich ist, diese Abhängigkeit der Geschäftsbanken von Zentralbankgeld zu nutzen, um durch Geldpolitik die Geldmenge zu beeinflussen und dadurch auch die Preisstabilität des Geldes zu sichern, wird im nächsten Abschnitt beschrieben.

3.3 Geldpolitik

„Vorrangige Aufgabe der Zentralbanken ist, den Wert des Geldes zu schützen."[54] In diesem Abschnitt soll es darum gehen, wie sich die Zentralbanken den Zentralbankgeldbedarf der Geschäftsbanken zunutze machen, um dadurch Geldpolitik betreiben zu können und um den Wert des Geldes aufrecht zu erhalten. Hierbei soll es um das wichtigste Instrument der Geldpolitik, den sogenannten Leitzins gehen.

Wie man im Folgenden feststellen wird, gehen die Mechanismen der Geldpolitik mit einer Erhöhung beziehungsweise Verringerung der im Umlauf befindlichen Geldmenge einher. Um genauer zu sein, reguliert die EZB indirekt die

[51] Naser, Rainer, Dr.: Wie kommt das Geld in die Welt? In: Wochenschau, Politik und Wirtschaft im Unterricht. August 2018, S. 23.
[52] Vgl. Deutsche Bundesbank (Hrsg.): Mindestreserven. URL: *https://www.bundesbank.de/de/aufgaben/geldpolitik/mindestreserven* , abgerufen am 19.01.2019, 16:10 Uhr.
[53] Vgl. Naser, Rainer, Dr.: Wie kommt das Geld in die Welt? In: Wochenschau, Politik und Wirtschaft im Unterricht. August 2018, S. 23.
[54] Deutsche Bundesbank 2017, S. 2 Vorwort.

Geldschöpfung der Geschäftsbanken, wie im vorherigen Punkt der Geldschöpfung beschrieben. „Entscheidendes Instrument, um die Kreditvergabe [und somit die Schöpfung von Buchgeld, d. Verf.] der Geschäftsbanken zu beeinflussen, ist der Leitzinssatz.“[55]

Wie in Abschnitt 3.2.2 beschrieben, haben Geschäftsbanken zwangsläufig einen Bedarf an Zentralbankgeld. Dieses müssen sich Geschäftsbanken über sogenannte Refinanzierungsgeschäfte bei der Zentralbank beschaffen, indem sie einen Kredit bei dieser aufnehmen.[56] Durch den aufgenommenen Kredit bei der Zentralbank erhöht sich das Zentralbankguthaben einer Geschäftsbank.[57] Diese Refinanzierung ist notwendig für die Betreibung der Geldpolitik. „Die Geschäftsbanken sollten über ihren Refinanzierungsbedarf an die Notenbank [(Zentralbank wird auch Notenbank genannt), d. Verf.] gebunden sein, damit das Kreditvolumen beeinflusst werden kann.“[58] Auf diesen aufgenommenen Zentralbankkredit muss die Geschäftsbank im Regelfall Zinsen bezahlen, den sogenannten Leitzins, welcher von der EZB festgelegt wird.[59] Durch den Anstieg des Leitzins, erhöhen die Banken in der Regel ihrerseits den Zins, zu dem sie Kredite vergeben, was die Kreditnachfrage von Unternehmen und Haushalten dämpft.[60] Dadurch, dass weniger Kredite vergeben werden, wird weniger Buchgeld geschaffen und die Geldmenge sinkt. Da die Kreditaufnahme teurer wird, kommt es in der Regel zu einer Dämpfung der Konjunktur.[61] Unternehmen und private Haushalte verlagern Investitionen lieber in die Zukunft und sparen ihr Geld, was zu deflationären Tendenzen führt.[62] Wenn der Leitzins gesenkt wird, passiert im Regelfall das Gegenteil. Dieser Mechanismus ist in der Anlage 1 schematisch verdeutlicht. Zusammengefasst kann die Zentralbank durch geldpolitische Maßnahmen Einfluss auf die Geldmenge nehmen und somit zur Preisstabilität beitragen.

---

[55] Naser, Rainer, Dr.: Wie kommt das Geld in die Welt? In: Wochenschau, Politik und Wirtschaft im Unterricht. August 2018, S. 26.
[56] Vgl. Deutsche Bundesbank 2017, S. 78.
[57] Vgl. Deutsche Bundesbank 2017, S. 75.
[58] Spahn, Heinz - Peter 2009, S. 90.
[59] Vgl. Deutsche Bundesbank 2017, S. 78.
[60] Vgl. Deutsche Bundesbank 2017, S. 78.
[61] Vgl. Gerginov, David: Geldpolitik: Definition, Wirkung und Ziel. Verlag für die Deutsche Wirtschaft AG. URL: *https://www.gevestor.de/details/geldpolitik-definition-wirkung-und-ziel-652473.html* , abgerufen am 20.01.2019, 14:45 Uhr.
[62] Vgl. Deutsche Bundesbank 2017, S. 161.

4 Die Kryptowährung Bitcoin

Im Oktober des Jahres 2008, inmitten der Finanzkrise, veröffentliche eine bis dahin vollkommen unbekannte Person bzw. eine Gruppe unter dem Pseudonym *Satoshi Nakamoto*[63] ein Konzept, welches es ermöglichen soll, ein elektronisches Zahlungsverfahren zu erschaffen, das Online-Zahlungen von einer Partei direkt an eine andere senden kann, ohne dabei ein Finanzinstitut zu benötigen.[64] Dieses Konzept setzte *Satoshi Nakamoto* Anfang 2009 in die Tat um und implementierte einen kryptographischen Code, welcher die ersten Bitcoins emittierte. Daraufhin wurden immer mehr Kryptowährungen erschaffen und veröffentlicht. Obwohl nahezu alle Kryptowährungen unterschiedlich funktionieren, so basieren doch alle auf dem gleichen Grundkonzept, welches im Folgenden am Beispiel des Bitcoins erläutert werden soll.

4.1 Dezentralisierung versus Zentralisierung

Der Buchautor und Mitgründer der Firma *TenX*[65], Dr. Julian Hosp, sieht drei wesentliche Punkte, welche in einem Geldsystem geregelt sein müssen, damit dieses funktionieren könne:[66]

1. Zugang zum Geld (Wann kann auf das Geld zugegriffen und in welchem Umfang über es verfügt werden)
2. Senden und Empfangen von Geld (Transaktionen)
3. Menge des in Umlauf befindlichen Geldes (geregelte Geldmenge)

In unserem zweistufigen Bankensystem werden diese Aufgaben von zentralen Institutionen (Geschäftsbanken und Zentralbanken) übernommen. Im Gegensatz dazu ist die wesentlichste Eigenschaft des Bitcoins, welche Satoshi Nakamoto in einem *white-paper*[67] hervorhob, dass Vermögensübertragungen ohne ein Finanzinstitut oder einer sonstigen Kontrollinstanz möglich sind.[68] Dieses Konzept ist dezentral, da es keine Instanz gibt, welche die oben genannten drei Funktionen regelt. Um die Frage der Notwendigkeit eines solchen dezentralen Systems beantworten zu können, muss bekannt sein, weshalb ein solches

---

[63] Die wahre Identität hinter *Satoshi Nakamoto* konnte bis heute nicht aufgedeckt werden
[64] Vgl. Satoshi Nakamoto 2008, S. 1.
[65] TenX ist ein Unternehmen, welches sich mit der Weiterentwicklung und Nutzung von Kryptowährungen und Blockchainanwendungen beschäftigt.
[66] Vgl. Hosp, Julian 2017, S. 26.
[67] Ein white-paper ist eine Sammlung von Ratschlägen und Empfehlungen zu einem bestimmten Sachverhalt (in diesem Kontext wird Satoshi Nakamotos E-Mail, in der er das Bitcoin Konzept vorstellte, als white-paper bezeichnet).
[68] Vgl. Satoshi Nakamoto 2008, S. 1.

System überhaupt entwickelt wurde. In erster Linie geht es dabei um das beschädigte Vertrauen in das Bankensystem. Als Satoshi Nakamoto das gerade beschriebene Konzept veröffentlichte, befand sich die Weltwirtschaftskrise auf ihrem vorläufigen Höhepunkt. Auslöser war das Platzen einer Immobilienblase in den USA.[69] Ausgangssituation dafür bildete der niedrige Leitzins der amerikanischen Zentralbank, welcher eine günstigere Kreditvergabe an Geschäftsbankkunden ermöglichte.[70] Weiterhin spielten die stetig steigenden Immobilienpreise eine entscheidende Rolle. „Die seit Anfang der 90er Jahre steigenden Immobilienpreise boten eine attraktive Alternative für die Anleger, zumal ein Ende des Preisanstiegs nicht abzusehen war."[71] Die Banken sahen in den steigenden Immobilienpreisen sowie in der günstigen Kreditvergabe lukrative Geschäfte. Sie fingen an, nahezu jeden Kunden mit Krediten für den Hauskauf zu versorgen. Dies geschah teilweise sogar unabhängig davon, ob der Kreditnehmer überhaupt über ein Einkommen oder wenigstens über entsprechende Rücklagen zur Tilgung dieser Kredite verfügte.[72] Die Banken stellten die *Hypotheken*[73] zu Wertpapierpaketen zusammen und verkauften diese an andere Banken.[74] Als dann die amerikanische Zentralbank den Leitzins erhöhte, stiegen auch die Zinsen für die Immobilienkredite. Die Kreditnehmer konnten ihre Raten nicht mehr begleichen, und die Immobilienpreise stürzten in die Tiefe.[75] Die Immobilien mussten zwangsversteigert werden und bescherten den Banken aufgrund des Wertverlustes Abschreibungen in Milliardenhöhe.[76] Die Banken begannen sich untereinander nicht mehr zu vertrauen und sich kein Geld mehr zu leihen, was zu einem Stocken der weltweiten Finanzströme und zu einer globalen Finanzkrise führte.[77]

---

[69] Vgl. Rosenberger, Patrick 2008, S. 114.
[70] Vgl. Badek, Bianca ; Nguyen, Tristan: Ursachen der Immobilienkrise in den USA. In: Schriften der Wissenschaftlichen Hochschule Lahr. 2010, S. 25.
[71] Badek, Bianca ; Nguyen, Tristan: Ursachen der Immobilienkrise in den USA. In: Schriften der Wissenschaftlichen Hochschule Lahr. 2010, S. 9.
[72] Vgl. Rosenberger, Patrick 2008, S. 114.
[73] Die Hypothek ist der Eigentumsvorbehalt der Bank an der Immobilie im Falle des Zahlungsausfalls.
[74] Vgl. Rosenberger, Patrick 2008, S. 114.
[75] Vgl. Bude, Matthias ; Kaufmann, Sabine: Finanzkrise 2008. URL: *https://www.planet-wissen.de/gesellschaft/wirtschaft/boerse/pwiefinanzkrise100.html* , abgerufen am 22.02.2019, 19:04 Uhr.
[76] Vgl. Bude, Matthias ; Kaufmann, Sabine: Finanzkrise 2008. URL: *https://www.planet-wissen.de/gesellschaft/wirtschaft/boerse/pwiefinanzkrise100.html* , abgerufen am 22.02.2019, 19:21 Uhr.
[77] Vgl. Bude, Matthias ; Kaufmann, Sabine: Finanzkrise 2008. URL: *https://www.planet-wissen.de/gesellschaft/wirtschaft/boerse/pwiefinanzkrise100.html* , abgerufen am 22.02.2019, 19:28 Uhr.

Diese Geschehnisse beschädigten wohl das Vertrauen der Bevölkerung in die Finanzwelt erheblich.[78] Nakamoto schrieb in seinem white-paper Folgendes: „Notwendig ist ein elektronisches Zahlsystem, das auf kryptographischem Nachweis an Stelle von Vertrauen basiert und es zwei bereitwilligen Parteien ermöglicht, Transaktionen direkt untereinander durchzuführen, ohne dass eine vertrauenswürdige dritte Partei benötigt wird.“[79]

4.2 Technische Grundlagen

Um verstehen zu können wie ein Zahlungssystem ohne Banken funktionieren kann, werden in diesem Abschnitt die technischen Grundlagen der Kryptowährungen am Beispiel des Bitcoins beschrieben.

4.2.1 Double-spending

Bevor man sich mit der technischen Funktionsweise des Bitcoins beschäftigt, muss man sich die Frage stellen, vor welchem Problem digitales dezentrales Geld grundsätzlich steht. Es handelt sich um das Problem des sogenannten *double-spending*, was übersetzt soviel wie doppelte bzw. mehrfache Ausgabe bedeutet. Das *double-spending* ist ein grundsätzliches Problem von digitalen Gütern. Es handelt sich um ein Problem, bei welchem digitale Güter kopiert und somit doppelt verwendet werden können.[80] Angenommen, man nimmt ein digitales Foto mit seiner Handykamera auf und möchte es einem Freund schicken, so sendet man das Foto zum Beispiel via Internetplattformen an die gewünschte Person. Man kann dieses digitale Foto jedoch auch an mehrere Freunde schicken, indem man einfach auf seinem Handy beliebig viele digitale Kopien anfertigt und es an eine beliebige Anzahl von Personen schickt. So wie das Foto ist grundsätzlich auch digitales Geld ein Gut, welches kopiert und mehrfach verschickt werden kann. Dieses Problem der Mehrfachausgabe muss im bargeldlosen Zahlungsverkehr gelöst sein. In unserem bestehenden Finanzsystem überwacht eine Bank jede bargeldlose Transaktion und verhindert somit, dass digitales Geld kopiert und mehrfach

[78] Vgl. Diehl, Martin ; Thiele, Carl-Ludwig: Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten? In: ifo Schnelldienst. 2017, S. 3.
[79] Satoshi Nakamoto 2008, S.1, aus dem Englischen übersetzt, Original: „What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”.
[80] Vgl. Drescher, Daniel 2017, S. 70.

ausgegeben wird.[81] Der Bitcoin ist jedoch dezentral und funktioniert ohne eine Bank. Bis 2008 gab es keinen Lösungsansatz für eine dezentrale digitale Währung, mit welchem Mehrfachausgaben verhindert werden konnten.[82] Als Nakamoto 2008 das Konzept des Bitcoins veröffentlichte, stellte er hierfür eine Lösung vor. Das Problem des *double-spending* soll durch die sogenannte Blockchain[83] gelöst werden.[84]

4.2.2 Das Kontensystem des Bitcoins

In einem Geldsystem muss der Zugang zum Geld geregelt sein.[85] Dazu benötigt der Anwender eine Art Konto. Für den Zugriff bzw. für die Verfügung über Bitcoin ist ein kryptographisches Schlüsselpaar erforderlich.[86] Dabei handelt es sich um den sogenannten *private key* **(privater Schlüssel)** sowie die *public address* **(öffentliche Adresse)**. Die public address kann mit einer öffentlichen Kontonummer verglichen werden. Der private key ist gleichzusetzen mit dem Passwort bzw. der PIN für ein Bankkonto, welcher geheim gehalten werden sollte, um einen fremden Zugriff zu verhindern. „Anhand der kryptographischen Signatur [(Eingabe des private key), d. Verf.] wird erkannt, dass auch tatsächlich die Berechtigung vorhanden ist, diesen [Bitcoin, d. Verf.] von dieser Adresse an eine andere zu transferieren.“[87] Aber wie genau passiert diese Kontenvergabe in einem dezentralen System ohne Bank als Kontrollinstanz? In einem zentralen System, beispielsweise bei einem E-Mail Anbieter erstellt man sich zuerst seine Wunsch-E-Mail-Adresse (analog dazu: public address). Der Mail Dienstleister stellt mithilfe von Datenbanken sicher, dass diese Adresse nicht bereits vergeben wurde. Im Anschluss daran legt man selbst das Passwort (analog: private key) fest. Da es in einem dezentralen System keine Datenbank gibt, die abgleicht, ob ein Konto bereits vergeben wurde oder nicht, erhält man bei einer Kontoerstellung zuerst ein geheimes Passwort (private key) nach dem Zufallsprinzip.[88] Im Falle von Bitcoin gibt es 2^{256} Möglichkeiten für einen private key.[89] Man erhält einen 256-stelligen Binärcode (Zahlenfolge aus 0 und 1). Nun ermittelt ein Computerprogramm,

[81] Vgl. Hosp, Julian 2017, S. 40.
[82] Vgl. Hosp, Julian 2017, S. 40.
[83] Die Blockchain wird in Abschnitt 4.2.3 erläutert.
[84] Vgl. Hosp, Julian 2017, S. 40.
[85] Siehe Abschnitt 4.1 – diese Voraussetzungen an ein Geldsystem nach Julian Hosp haben nichts mit dem in Kapitel 2 beschriebenen Geldbegriff zu tun.
[86] Vgl. Seiler, Benedikt ; Seiler, Daniel: Sind Kryptowährungen wie Bitcoin (BTC), Ethereum (ETH) und Ripple (XRP) als Sachen im Sinne des ZGB zu behandeln? In: sui generis. 2018, S. 153.
[87] Platzer, Joerg 2014, S. 24.
[88] Vgl. Hosp, Julian 2017, S. 46.
[89] Vgl. Hosp, Julian 2017, S. 46.

basierend auf diesem private key, mittels eines kryptographischen Algorithmus die public address. Wenn ein Netzwerkteilnehmer einem anderen Teilnehmer Bitcoins senden möchte, muss dieser seine public address kennen und die Transaktion mit seinem geheimen private key signieren.

Die Besonderheit an diesem Algorithmus ist, dass dies nur in eine Richtung funktioniert. „Es ist einfach, eine public address aus einem private key zu errechnen, aber es ist buchstäblich unmöglich, einen private key von einer public address zu erraten.“[90] Das Wort unmöglich bedeutet in diesem Kontext, dass der Zeitaufwand dafür, einen private key anhand einer dazugehörigen public address zu ermitteln, absurd hoch wäre. Mit einem hochmodernen Computer würde es über sieben Quadrilliarden[91] Jahre dauern, um mit einer einprozentigen Wahrscheinlichkeit den passenden privaten Schlüssel (private key) finden zu können.[92] Diese Aussage kann jedoch nur getroffen werden, wenn von herkömmlicher Computertechnologie ausgegangen wird.

4.2.3 Die Blockchain

Die wohl wesentlichste Technologie in der Welt der Kryptowährungen ist die sogenannte Blockchain. „Die Blockchain Technologie bietet die Grundlage zur Existenz einer dezentralen digitalen Währung.“[93] Diese Technologie wird auch als *Distributed-Ledger-Technologie* (DLT) bezeichnet, was übersetzt *verteiltes Kontenbuch* bedeutet. Wie sich im Folgenden herausstellen wird, kann durch diese Technologie das grundsätzliche *double-spending* Problem von digitalen Gütern gelöst werden.[94] Wörtlich aus dem Englischen übersetzt bedeutet Blockchain *Blockkette*. Die Blockchain ist also eine Kette, bestehend aus einer chronologischen Reihenfolge von Transaktionen. Die Blockchain kann mit einem Kontenbuch verglichen werden. Sie ist eine unveränderliche Transaktionshistorie.[95] Der Unterschied zu einem zentralisierten System ist, dass die Blockchain von jedem und jederzeit öffentlich eingesehen werden kann.[96] Die vollständige Blockchain

[90] Hosp, Julian 2017, S. 49.
[91] Eins mit 27 Nullen ($1*10^{27}$).
[92] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 136.
[93] Hosp, Julian 2017, S. 41.
[94] Zu double spending siehe Abschnitt 4.2.1.
[95] Vgl. Hosp, Julian 2017, S. 64.
[96] Vgl. Platzer, Joerg 2014, S. 20.

kann man z. B. auf der Seite *bitcoin.org* im Internet herunterladen.[97] Nakamoto schrieb in seinem white-paper übersetzt: „Um dies [(Transaktionen von einem Teilnehmer direkt zu einem anderen Teilnehmer durchzuführen), d. Verf.] ohne vertrauenswürdige Partei zu erreichen, müssen Transaktionen öffentlich gemacht werden, (…).“[98] Ein Teilnehmer muss nicht die ganze Transaktionshistorie speichern. Da dies sehr umständlich wäre, wird die Blockchain in einzelne Blöcke unterteilt.[99] In einem Block sind mehrere Transaktionen gesammelt und verkettet. Da ein neuer Block unwiderruflich auf dem vorherigen aufbaut, können ihn die Teilnehmer als Beweis darüber akzeptieren, was in den vorherigen Blöcken geschehen ist.[100] Ein solcher Block enthält nach Jörg Platzer folgende Informationen:[101]

1. Transaktionen, die im Netzwerk seit der Erstellung des letzten Blocks von den Teilnehmern gemeldet waren.
2. Sogenannter *proof-of-work* (Arbeitsbeweis), der das Ergebnis des *Bitcoin-Minings*[102] ist
3. Eine sogenannte *Nonce*[103] - das ist ein leicht überprüfbar mathematischer Bezug zum vorausgegangenen Block, um jedem anderen Netzwerkteilnehmer gegenüber zu beweisen, dass der neue Block auf dem bisherigen Stand der gemeinsamen Buchhaltung aufbaut.

Es ist von einer gemeinsamen Buchhaltung die Rede, da alle Teilnehmer das gleiche Kontenbuch als Wahrheit darüber akzeptieren, was seit der allerersten Transaktion geschehen ist. Durch diese Verkettung der Transaktionen wird auch deren zeitliche Reihenfolge unveränderlich festgehalten, da jede Transaktion, die in die Blockchain aufgenommen wird, mit einem Zeitstempel versehen ist.[104] Bezugnehmend auf das zuvor angesprochene double spending Problem ist es nicht möglich, einen Bitcoin doppelt auszugeben, da der Prozess der Überprüfung und Aneinanderreihung von Blöcken als Grundlage für weitere Blöcke eine Übereinkunft über die Authentizität der Transaktionen darstellt.[105] Das bedeutet, dass

[97] Vgl. o. V.: Download Bitcoin Core. URL: *https://bitcoin.org/de/download* , abgerufen am 25.12.2018, 16:00 Uhr.
[98] Satoshi Nakamoto 2008, S. 2, aus dem Englischen übersetzt, Original: „To accomplish this without a trusted party, transactions must be publicly announced (…).“.
[99] Vgl. Platzer, Joerg 2014, S. 20.
[100] Vgl. Hosp, Julian 2017, S. 64, 65.
[101] Alle 3 Punkte aus Platzer, Jörg 2014, S. 20, 21.
[102] Zu Bitcoin-Mining siehe Abschnitt 4.2.4.
[103] Siehe Abschnitt 4.2.4.1.
[104] Vgl. Platzer, Joerg 2014, S. 21.
[105] Vgl. Rosenberger, Patrick 2018, S. 19.

der Zahlungsempfänger jederzeit die aktuelle Version des Kontenbuches kennt und somit überprüfen kann, ob der erhaltene Bitcoin wirklich im Eigentum des Auftraggebers stand oder ob er diesen bereits zuvor ausgegeben hat. Ansonsten könnte die Transaktion nicht ausgeführt werden. Die Überwachung der Transaktionen übernehmen im Netzwerk sogenannte *Miner*.[106]

4.2.4 Mining

Die im vorherigen Abschnitt beschriebene Blockchain funktioniert nur, wenn Miner[107] am Netzwerk teilnehmen, welche das *Mining* betreiben. Die Miner legitimieren die Transaktionen im Netzwerk und überprüfen sie. „Dieses Legitimationsverfahren wird – in Anlehnung an die Goldgräberei – wegen der zu erlangenden Gegenleistung [(Miner erhalten Bitcoins als Gegenleistung), d. Verf.] auch „Mining" (…) genannt"[108] Dadurch generieren die Miner aus vielen Transaktionen neue Blöcke, welche sie der Blockchain hinzufügen.[109] Dafür müssen die Miner im gesamten Netzwerk Konsens[110] kreieren.[111] Konsens ist in einem dezentralen System notwendig, da sich alle Teilnehmer auf eine Version des Kontenbuchs einigen müssen, damit dies fortgeführt werden kann. Wenn eine Transaktion der Blockchain hinzugefügt wird, wird diese Information exponentiell innerhalb von wenigen Millisekunden dem ganzen Netzwerk bekannt gegeben.[112]

In Bezug auf die zuvor in Abschnitt 4.1 genannten Voraussetzungen eines Geldsystems[113], sind die Miner für die Überwachung von Transaktionen sowie deren Einmaligkeit zuständig und regeln somit das Senden und Empfangen der Bitcoins.[114]

---

[106] Vgl. Rosenberger, Patrick 2018, S. 19.
[107] Miner bedeutet sinngemäß übersetzt: *Schürfer* (in Anlehnung an einen Goldschürfer)
[108] Geiling, Luisa: Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain. In: Bafin Journal. 2016, S. 29.
[109] Vgl. Rosenberger, Patrick 2018, S. 19.
[110] Konsens bedeutet Übereinstimmung bzw. Einigkeit.
[111] Vgl. Hosp, Julian 2017, S. 54.
[112] Vgl. Hosp, Julian 2017, S. 56.
[113] Diese Voraussetzungen an ein Geldsystem nach Julian Hosp haben nichts mit dem in Kapitel 2 beschriebenen Geldbegriff zu tun.
[114] Vgl. Rosenberger, Patrick 2018, S. 19.

4.2.4.1 Der Arbeitsbeweis bzw. proof-of-work

Es gibt verschiedene Mechanismen, mit denen Konsens kreiert werden kann. Im Fall des Bitcoins wird der sogenannte *proof-of-work*[115] Mechanismus verwendet. Dabei müssen die Miner die Rechenleistung ihrer Computer bereitstellen, um eine Rechenaufgabe zu lösen.[116] Bei dieser Rechenaufgabe handelt es sich um einen komplexen kryptographischen Algorithmus.[117] Der Miner, der die Rechenaufgabe als Erster gelöst hat, kann einen neuen Block generieren, Transaktionen in diesem Block bestätigen und schließlich der Blockchain hinzufügen.[118] Diese Rechenarbeit ist für die Sicherheit der Blockchain notwendig. „Aus wirtschaftlicher Sicht muss es (…) etwas kosten, einen Block zu kreieren, ansonsten kann Information kostenlos kreiert, verändert oder gelöscht werden."[119] Diese Rechenaufgaben[120] sind einerseits sehr schwer und rechenintensiv zu lösen, andererseits jedoch auch von anderen Teilnehmern sehr einfach und schnell zu überprüfen.[121] Der Miner muss dabei die Lösung der Aufgabe durch Probieren von Millionen verschiedener Noncen[122] erraten.[123] Zur Vereinfachung kann man sich die Rechenaufgabe als Gleichung mit einer Variablen x vorstellen (z.B. $x + 100 = 110$). Der Miner muss nun versuchen, den Wert von x durch Probieren verschiedener Möglichkeiten herauszufinden. Dieses Probieren erfordert Zeit und Arbeit. Wenn die Lösung jedoch gefunden ist ($x = 10$), kann jeder Teilnehmer leicht prüfen ob die Lösung korrekt ist, indem er das Ergebnis ($x = 10$) einfach in die Gleichung einsetzt.

4.2.4.2 Anreize für die Miner

Da die Miner, wie zuvor dargestellt, für die Verkettung der Blockchain (für das Fortführen des Kontenbuchs) zuständig sind, kann das Netzwerk ohne sie nicht funktionieren. Damit dauerhaft gewährleistet werden kann, dass es Miner gibt, müssen bestimmte Anreize bestehen.

---

[115] Aus dem Englischen übersetzt bedeutet proof-of-work: Arbeitsbeweis.
[116] Vgl. Hosp, Julian 2018, S. 59.
[117] Vgl. Hosp, Julian 2017, S. 62.
[118] Vgl. Hosp, Julian 2017, S. 63.
[119] Hosp, Julian 2018, S. 59.
[120] Bei der Rechenaufgabe handelt es sich bei Bitcoin um den sogenannten SHA-256 Algorithmus
[121] Vgl. Platzer, Joerg 2004, S. 23.
[122] Die Noncen kann mit den Lösungsmöglichkeiten verglichen werden. Nur eine Nonce ist richtig. Der Miner muss so viele Noncen probieren bis er die richtige gefunden hat.
[123] Vgl. Hosp, Julian 2017, S. 62, 63.

Der Anreiz besteht darin, dass der Miner, der es geschafft hat einen neuen Block zu generieren, dafür einige Bitcoins als Belohnung erhält.[124] „Diese [Belohnung, d. Verf.] besteht aus (…) Transaktionsgebühren (…) plus zusätzliche Ausschüttungen (…).“[125] Diese zusätzlichen Ausschüttungen sind die **neu** in Umlauf gebrachten Bitcoins.[126]

4.2.4.3 Schöpfung neuer Bitcoins

In Abschnitt 3.2 ging es darum, wie neues Geld in unserem Bankensystem entsteht. Bei Bitcoin geschieht dies über die Mining Belohnung. Nakamoto schreibt in seinem white-paper übersetzt: „(…) die erste Transaktion in einem Block [ist, d. Verf.] eine spezielle Transaktion, die einen neuen *Coin*[127] schöpft, der dem Erzeuger des Blocks gehört.“[128] Aus dieser Aussage und der Tatsache, dass der Miner als Belohnung auch eine von anderen Teilnehmern gezahlte Transaktionsgebühr erhält, kann geschlussfolgert werden, dass sich diese Belohnung sowohl aus der Transaktionsgebühr (bereits existierende Bitcoins), als auch aus neuen Bitcoins zusammensetzt. „Dies gibt (…) einen Anreiz, das Netzwerk zu unterstützen und bietet einen Weg, Münzen erstmals in Umlauf zu bringen, da es keine zentrale Instanz gibt, die sie herausgibt.“[129] Derzeit kommen pro Block 12,5 neue Bitcoins in Umlauf.[130]

Dies ist jedoch nicht dauerhaft so, denn dieser Betrag halbiert sich jedes Mal, wenn 210.000 neue Bitcoins in Umlauf gebracht werden.[131] Die nächste Halbierung auf 6,25 Bitcoins wird voraussichtlich im Mai 2020 stattfinden.[132] Durch die Halbierung sinkt auch die Inflationsrate von Bitcoin. Pascal Thellman, Marketingchef einer Internetplattform für Kryptowährungen, schreibt in einem Gastbeitrag auf der Internetseite *Coindesk*, dass die Inflationsrate bei der nächsten Halbierung im Jahr

---

[124] Vgl. Geiling, Luisa: Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain. In: Bafin Journal. 2016, S. 29.
[125] Hosp, Julian 2017, S. 61.
[126] Siehe dazu Abschnitt 4.2.4.3.
[127] Coin steht im Folgenden für eine Bitcoin Einheit.
[128] Satoshi Nakamoto 2008, S. 4, aus dem Englischen übersetzt, Original: „ (…), the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block.”
[129] Satoshi Nakamoto 2008, S. 4, aus dem Englischen übersetzt, Original: „This adds an incentive (…) to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.”.
[130] Vgl. Hosp, Julian 2017, S. 63.
[131] Vgl. o. V.: Bitcoin Block Reward Halving Countdown. URL: *https://www.bitcoinblockhalf.com* , abgerufen am 23.01.2019, 19:34 Uhr.
[132] Vgl. Wagner, Niklas: Nächstes Bitcoin (BTC)-Halving könnte schon dieses Jahr für Preisanstieg sorgen. URL: *https://coinkurier.de/halving/* , abgerufen am 23.01.2019, 19:38 Uhr.

2020 sogar geringer sein wird als die von Gold.[133] Dieser Halbierungsprozess hat jedoch eine Grenze und zwar, wenn die kleinstmögliche Einheit des Bitcoins, der sogenannte *Satoshi*[134] erreicht ist, was ungefähr im Jahr 2140 der Fall sein wird.[135] Das bedeutet, dass beim derzeitigen Bitcoin Algorithmus maximal knapp 21 Millionen[136] Bitcoins in Umlauf gebracht werden können.[137] Diese Begrenzung ist jedoch keine zwingende Eigenschaft von Kryptowährungen. Bei der Kryptowährung *Litecoin*[138] beispielsweise liegt die Begrenzung bei 84 Millionen Litecoins.[139]

In Bezug auf die zuvor genannten Voraussetzungen eines Geldsystems[140], kann festgestellt werden, dass der Bitcoin die Voraussetzung an eine geregelte Geldmenge nur partiell erfüllt. Die Entwicklung der Geldmenge ist zwar grundsätzlich durch den Blockchain Algorithmus bestimmt, sie kann jedoch nicht beeinflusst bzw. angepasst werden.

4.3 Sicherheit

Der Bitcoin-Algorithmus gilt aus Sicht der Sicherheit als sehr gelungen.[141] Trotzdem hört man regelmäßig in den Medien, dass große Mengen an Bitcoin bzw. andere Kryptowährungen von Hackern gestohlen wurden. Um die Sicherheit von Kryptowährungen beurteilen zu können, wird im Folgenden sowohl die Sicherheit des Kontensystems[142] als auch der Blockchain selbst untersucht.

---

[133] Vgl. Thellman, Pascal: Bitcoin's Next Halving Rally: Coming Soon in 2019. URL: *https://www.coindesk.com/bitcoins-next-halving-rally-coming-soon-in-2019* , abgerufen am 23.01.2019, 19:45 Uhr.
[134] Ein Satoshi entspricht 0,00000001 Bitcoin (siehe Abschnitt 5.1.1).
[135] Vgl. Hosp, Julian 2017, S. 85.
[136] Dabei handelt es sich um einen Grenzwert, durch die stetige Halbierung kann dieser Wert nie exakt erreicht werden.
[137] Vgl. Hosp, Julian 2017, S. 85.
[138] Litecoin ist eine im Jahr 2011 veröffentlichte Kryptowährung.
[139] Vgl. o. V.: Litecoin Details – Mehr über Litecoin erfahren. URL: *https://www.coinwelt.de/2014/12/litecoin-details/* , abgerufen am 23.01.2019, 18:50 Uhr.
[140] Siehe Abschnitt 4.1 - diese Voraussetzungen an ein Geldsystem nach Julian Hosp haben nichts mit dem in Kapitel 2 beschriebenen Geldbegriff zu tun.
[141] Vgl. Krohn-Grimberghe, Artus ; Sorge, Christoph: Bitcoin: das Zahlungsmittel der Zukunft? In: Wirtschaftsdienst. 2013, S. 721.
[142] Schlüsselpaar aus private key und public address.

4.3.1 Sicherheit des Kontensystems

Wie in Abschnitt 4.2.2 beschrieben, benötigt jemand, der am Bitcoin Netzwerk teilnehmen möchte, ein Schlüsselpaar, bestehend aus dem private key und dem public address. Da der private key, also das Passwort, nach dem Zufallsprinzip generiert wird und es dabei 2^{256} Möglichkeiten gibt, kann es als äußerst unwahrscheinlich angesehen werden, mit herkömmlicher Computertechnik einen private key (analog: Passwort) zu einer dazugehörigen public address (analog: öffentliche Kontonummer) zu erraten.[143]

Eine potenzielle Gefahr besteht jedoch in der Abspeicherung des private keys. Da der private key aus einer zufälligen Reihenfolge von 256 Binärziffern (Einsen und Nullen) besteht, kann man sich einen solchen Schlüssel theoretisch selber mit Stift, Papier und einer Münze generieren. Da dies ein sehr umständlicher Weg ist, können sowohl zur Generierung als auch zum Sichern solcher private keys sogenannte *Wallets*[144] verwendet werden.[145] Riskant ist dabei eine sogenannte Soft-Wallet. Dies ist ein Computerprogramm, welches den private key auf einem Computer speichert.[146] Hackern kann es somit gelingen, durch dieses Aufbewahrungsprogramm an den private key zu gelangen und somit Kontrolle über das Vermögen auszuüben, welches der dazugehörigen public address zugeordnet ist.

Noch riskanter, dafür aber am komfortabelsten, sind sogenannte *Exchanges*.[147] Bei diesen Exchanges, welche eine benutzerfreundliche und einfache Bedienung anbieten, kann der Nutzer mit Kryptowährungen handeln und muss sich dabei nicht um die Erstellung und Sicherung seines private keys kümmern, da dies automatisch von dem Exchange Anbieter übernommen wird.[148] Dies bedeutet auch, dass der Nutzer seinen private key nicht kennt und somit seinen Bestand an Kryptowährungen den Händen der Exchange anvertraut. Das Risiko hierbei ist die Angreifbarkeit solcher digitalen Dienste, denn diese selbst können durch unsichere Strukturen Angriffsfläche für Hacker bieten, welche die Kontrolle über die, von der

[143] Vgl. Hosp, Julian 2017, S. 49.
[144] Zu deutsch: Brieftasche. In diesem Kontext ist eine Wallet, eine Speichermethode des private key. Die Wallet speichert keine Bitcoins, sondern nur den private key, welcher den Zugriff auf die Bitcoins ermöglicht.
[145] Vgl. Hosp, Julian 2017, S. 89.
[146] Vgl. Hosp, Julian 2017, S. 93.
[147] Exchanges sind Online-Tauschbörsen, welche damit werben, bequem und einfach mit Kryptowährungen handeln zu können.
[148] Vgl. Hosp, Julian 2017, S. 94, 95.

Exchange verwalteten Konten übernehmen. Am 11. Juni 2018 berichtete der Spiegel in einem Online Artikel, dass eine solche südkoreanische Exchange namens *Coinrail beraubt*[149] *wurde* und dabei Kryptowährungen von umgerechnet 31 Millionen Euro gestohlen wurden.[150] Dabei knackte der Angreifer nicht etwa die Konten einzelner Bitcoin-Besitzer, sondern lediglich die von der Exchange gespeicherten und verwalteten private keys (Passwörter) ihrer Kunden.

4.3.2 Sicherheit der Blockchain

Die bisher beschriebenen Blockchain Funktionsweisen, insbesondere der proof-of-work Mechanismus[151], kann nur unter einer Bedingung als sicher gelten: „Kein Angreifer darf mehr Rechenleistung zur Verfügung haben als alle ehrlichen Teilnehmer zusammengenommen."[152] Solch ein theoretischer Angriff wird als *51-Prozent-Attacke* bezeichnet.[153] Das bedeutet, dass ein Angreifer bzw. eine zusammengeschlossene Gruppe von Angreifern mehr als 50 % der Rechenleistung im Netzwerk haben, um den Konsensmechanismus[154] zu kontrollieren. Die Angreifer könnten dadurch verschiedene Dinge erreichen. Sie könnten zum einen vergangene Transaktionen ungültig machen, indem sie eine alternative Blockkette generieren, welche an einem vorherigen Punkt der Blockchain anknüpft.[155] In dieser alternativen Blockkette wird die ungewünschte Transaktion dann absichtlich nicht aufgenommen.[156] Da die Angreifer über mehr Rechenleistung verfügen als der Rest der ehrlichen Teilnehmer, können die Angreifer diese alternative Blockkette im Netzwerk als Wahrheit verbreiten. Je weiter eine Transaktion jedoch in der Vergangenheit liegt, umso unwahrscheinlicher wird ein solcher Angriff auf diese Transaktion. Es gilt, dass ein Block ab sechs Bestätigungen[157] samt aller darin enthaltener Transaktionen, als unumkehrbar gilt.[158]

---

[149] Umgangssprachlich wird auch oft von *hacken* gesprochen.
[150] Vgl. Reuters (Hrsg.): Südkorea: Hacker greifen Krypto-Börse Coinrail an. URL: *http://www.spiegel.de/netzwelt/web/coinrail-aus-suedkorea-hacker-greifen-krypto-boerse-an-a-1212322.html* , abgerufen am 28.02.2019, 19:25 Uhr.
[151] Siehe Abschnitt 4.2.4.1.
[152] Krohn-Grimberghe, Artus ; Sorge, Christoph: Bitcoin: das Zahlungsmittel der Zukunft? In: Wirtschaftsdienst. 2013, S. 721.
[153] Vgl. Sixt, Elfriede 2017, S. 105.
[154] Der Konsensmechanismus ist im Falle des Bitcoins proof-of-work
[155] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 233.
[156] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 233.
[157] Das Bedeutet, dass der Block von mindestens sechs neueren generierten Blöcken gefolgt wird und somit unumkehrbar in die Blockchain integriert ist.
[158] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 233.

Des Weiteren könnte der Angreifer double-spending[159] (Mehrfachausgaben) durchführen, indem die gleichen Coins innerhalb von kurzer Zeit an unterschiedliche Empfänger verschickt werden. „Da diese Leute [(die Angreifer), d. Verf.] den Konsensus [(Konsens), d. Verf.] erschaffen, könnten sie zuerst die eine und dann die andere Transaktion als „Realität“ [für das restliche Netzwerk, d. Verf.] erscheinen lassen.“[160]

Dieses Problem sah bereits der Entwickler des Bitcoins, Satoshi Nakamoto und schrieb diesbezüglich in seinem white-paper: „Er [(der Angreifer), d. Verf.] sollte es profitabler finden, sich an die Regeln zu halten – Regeln, die ihn mit mehr neuen Münzen versorgen können als alle anderen zusammen – als dass er das System und damit die Gültigkeit seines eigenen Wohlstands untergräbt.“[161]

4.4 Anonymität

Die Blockchain ist mit einem öffentlich einsehbaren Kontenbuch vergleichbar. Wie bereits an vorheriger Stelle erwähnt, kann jede einzelne Transaktion, die jemals getätigt wurde, aus dem Internet heruntergeladen werden. Aktuell getätigte Transaktionen können sogar in Echtzeit verfolgt werden.[162] Dennoch wird es Kryptowährungen, insbesondere dem Bitcoin vorgeworfen, sich gut für illegale Aktivitäten wie Geldwäsche, Drogenhandel oder Lösegeldforderungen zu eignen, da Transaktionen angeblich vollkommen anonym seien sollen. In einem Bericht von Europol heißt es: „Bitcoin etabliert sich als einheitliche gemeinsame Währung für Cyberkriminelle (…).“[163] Weiterhin heißt es: „Darüber hinaus wurde eine (…) Migration von traditionellen Zahlungsmechanismen zu solchen mit einem höheren Grad an Anonymität beobachtet, insbesondere pseudonyme Zahlungssysteme wie Bitcoin.“[164]

---

[159] Siehe Abschnitt 4.2.1.
[160] Hosp, Julian 2017, S. 110.
[161] Satoshi Nakamoto 2008, S. 2, aus dem Englischen übersetzt, Original: „He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.”.
[162] Vgl. o. V.: Live aktualisierte Liste der aktuellen Bitcoin Transaktionen. URL: *https://www.blockchain.com/de/btc/unconfirmed-transactions* , abgerufen am 30.01.2019, 17:40 Uhr.
[163] Europol (Hrsg.) 2015, S. 11, aus dem Englischen übersetzt, Original: „Bitcoin is establishing itself as a single common currency for cybercriminals within the EU.”.
[164] Europol (Hrsg.) 2015, S. 30, aus dem Englischen übersetzt, Original: „Additionally, a continuation of migration from traditional payment mechanisms to those offering a greater degree of anonymity, particularly pseudonymous payment systems37 such as Bitcoin, has been observed.“.

Wie in Abschnitt 4.2.2 beschrieben, ist die öffentliche Adresse (public address) jedem Transaktionspartner bekannt (analog zur IBAN bzw. Kontonummer). Eine solche Bitcoin Adresse kann beispielsweise folgendermaßen aussehen: 1HFSx5TPYYuQZQmBXeJNvMhUDT6GNGN11e.[165] Obwohl jede Überweisung die jemals mit dieser Bitcoin Adresse vorgenommen wurde jederzeit im Internet nachvollzogen werden kann, da die Blockchain (die Transaktionshistorie) frei zugänglich ist, wirkt diese bloße Kombination aus Zahlen und Buchstaben auf den ersten Blick sehr anonym. Wenn es jedoch beispielsweise Strafverfolgungsbehörden gelingen würde einer public address die passende Identität des Bitcoin Nutzers zuzuordnen, wäre die Nutzung von Kryptowährungen keineswegs mehr anonym. Hierbei kommt es stark auf die technischen Fähigkeiten des Nutzers an. Aber auch ein technisch versierter Nutzer hinterlässt früher oder später digitale Spuren im Internet. In einem Artikel des *Spiegel Online* heißt es: „Es gibt Muster, Schnittstellen zu Börsen und Spuren auf anderen Plattformen [(z.B. Exchanges), d. Verf.], die sich zurückverfolgen lassen. Behörden und andere Akteure haben schon öfter Personen hinter Bitcoin-Transaktionen ausfindig gemacht. Spätestens beim Umtausch der Onlinewährung [(hiermit sind Kryptowährungen gemeint), d. Verf.] in bares Geld [(staatliche Währungen), d. Verf.] muss sich der Besitzer einer Kryptowährung zu erkennen geben.“[166]

Zusammengefasst kann es, abhängig vom technischen Kenntnisstand des Nutzers, bedeutend schwieriger sein, die Identität eines Nutzers seiner public address zuzuordnen, als dies in unserem Bankensystem der Fall ist. Jedoch können der Bitcoin und andere Kryptowährungen aber keineswegs als anonym sondern eher als *pseudonym* bezeichnet werden. Nutzer verwenden die public address lediglich als Pseudonym bei Transaktionen.[167]

---

[165] Die public address ist eine Kombination aus 34 Zahlen und Buchstaben, das Beispiel ist eine frei erfundene Adresse.
[166] Dittmer, Diana: Ist Cybergeld vor allem was für Kriminelle? Spiegel Online. URL: *https://www.n-tv.de/wirtschaft/Ist-Cybergeld-vor-allem-was-fuer-Kriminelle-article20143681.html* , abgerufen 01.02.2019, 18:20 Uhr.
[167] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 119.

4.5 Probleme

In diesem Abschnitt sollen verschiedene Probleme hervorgehoben werden, welche dem Bitcoin entgegenstehen.

4.5.1 Energieverbrauch des Konsensmechanismus

Aufgrund der Tatsache, dass für den Konsensmechanismus bei Bitcoin (proof-of-work) die Rechenleistung von Computern genutzt werden muss, wird bei diesem Prozess äußerst viel Energie verbraucht. Am 16. Mai 2018 erschien ein Artikel in der Zeitschrift *Joule,* in dem es um eine Studie zum Thema Energieverbrauch des Bitcoin-Mining ging. Darin schreibt der Ökonom Alex de Vries, dass der aktuelle Energieverbrauch des Bitcoin-Minings mindestens 2.55 Gigawatt beträgt, was fast dem Stromverbrauch ganz Irlands von 3,1 Gigawatt entspricht.[168] Alex de Vries rechnete in seiner Studie sogar mit einem Anstieg auf 7,67 Gigawatt, was fast dem Stromverbrauch ganz Österreichs von 8,2 Gigawatt entsprechen würde.[169] Wie im Abschnitt 4.2.4.2 beschrieben, besteht der Anreiz für die Miner darin, eine Belohnung in Form von neuen Bitcoins zu erhalten. Je höher der Wert[170] des Bitcoins ist, desto profitabler wird dementsprechend das Mining und dementsprechend erhöhen sich die Anreize für die Miner. „Je teurer der Bitcoin wird, je mehr es zu verdienen gibt, desto mehr Rechenleistung werden die Miner einsetzen. Wenn der Preis entsprechend hochschießt, kann man nicht ausschließen, dass sich der Energieverbrauch noch einmal verzehnfacht.“[171] Die Abbildung in Anlage 3 zeigt eine sogenannte *Bitcoin-Farm*. Dort wird in großem Stil Bitcoin-Mining betrieben. Die räumlichen Ausmaße solcher Einrichtungen sollen an dieser Stelle den benötigten Energiebedarf für den Konsensmechanismus veranschaulichen.

Hierbei muss erwähnt werden, dass dieses Problem nur Kryptowährungen betrifft, welche einen proof-of-work Konsensmechanismus verwenden. Dieser Mechanismus ist unter den Kryptowährungen allerdings der verbreitetste, da dieser am meisten getestet wurde und am widerstandsfähigsten ist.[172]

---

[168] Vgl. De Vries, Alex: Bitcoin's Growing Energy Problem. In: Joule. 2018, S. 801.
[169] Vgl. De Vries, Alex: Bitcoin's Growing Energy Problem. In: Joule. 2018, S. 801.
[170] Mit Wert ist in diesem Zusammenhang der Wechselkurs in konventionelle Währungen z.B. dem Euro gemeint.
[171] Hecking, Klaus Interview mit De Vries, Alex, veröffentlicht in einem Artikel des Spiegel Online. "Das Bitcoin-System verbraucht mehr Strom als die Schweizer Volkswirtschaft". URL: *http://www.spiegel.de/wirtschaft/unternehmen/bitcoin-energieverbrauch-fuer-produktion-und-verwaltung-a-1208635.html* , abgerufen am 04.02.2019, 18:50 Uhr.
[172] Vgl. Hosp, Julian 2017, S. 61.

4.5.2 Volatilität

Um prüfen zu können, ob der Bitcoin sowohl die Geldfunktionen als auch Geldeigenschaften erfüllt, muss vorab auf die Volatilität eingegangen werden. „Die Volatilität ist ein Risikomaß und zeigt die Schwankungsintensität des Preises eines Basiswertes innerhalb eines bestimmten Zeitraums.“[173] „Je höher die Volatilität, um so stärker schlägt der Kurs nach oben und unten aus und desto riskanter aber auch chancenreicher ist eine Investition in das Basisobjekt.“[174]

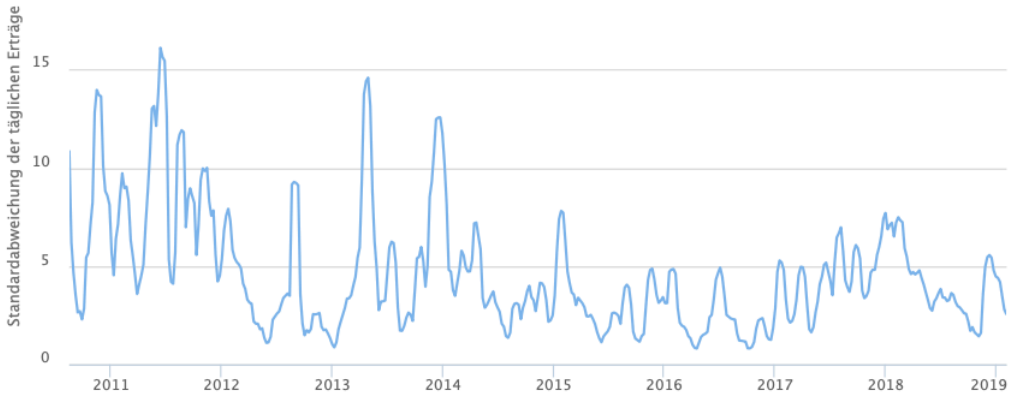


Abbildung 2

Die vorstehende Abbildung[175] zeigt den sogenannten Volatilitätsindex des Bitcoins. Die vertikale Achse zeigt die durchschnittlichen Preisschwankungen des Bitcoins, gemessen innerhalb eines Zeitraums von 30 Tagen, in Prozent an. Aus der Abbildung geht hervor, dass die Preisschwankung im Verlauf der Zeitachse abnimmt. Die aktuelle Volatilität von Bitcoin, gemessen anhand der Schlusskurse der letzten 30 Tage beträgt 2,92 %.[176] Obwohl dieser Wert auf den ersten Blick nicht sonderlich hoch erscheint, wäre es jedoch falsch zu behaupten, dass die kurzfristige Volatilität des Bitcoin das Niveau der traditionellen Währungen (z.B. Euro oder US-Dollar) erreicht.[177] „Gewisse Wertschwankungen werden aufgrund der starren und nicht durch exogene Einflüsse veränderbaren Geldmengenregel bestehen bleiben.“[178] Im Eurosystem sorgen Zentralbanken für Preisstabilität,

---

[173] Börse ARD (Hrsg.): Volatilität. URL: *https://boerse.ard.de/boersenwissen/boersenlexikon/volatilitaet-100.html* , abgerufen am 06.02.2019, 17:45 Uhr.
[174] Börse ARD (Hrsg.): Volatilität. URL: *https://boerse.ard.de/boersenwissen/boersenlexikon/volatilitaet-100.html* , abgerufen am 06.02.2019, 17:45 Uhr.
[175] Vgl. o. V.: Der Bitcoin-Volatilitätsindex. URL: *https://www.buybitcoinworldwide.com/de/volatilitatsindex/* , abgerufen am 09.03.2019, 16:25 Uhr.
[176] Vgl. o. V.: Der Bitcoin-Volatilitätsindex. URL: *https://www.buybitcoinworldwide.com/de/volatilitatsindex/* , abgerufen am 09.03.2019, 16:25 Uhr.
[177] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 261.
[178] Berentsen, Aleksander ; Schär, Fabian 2017, S. 261, 262.

indem diese Einfluss auf die in Umlauf befindliche Geldmenge nehmen können.[179] Im Gegensatz dazu folgt die Entwicklung der Geldmenge beim Bitcoin einem Algorithmus, welcher neue Münzen als Belohnung an die Miner ausschüttet.[180] Aufgrund der Tatsache, dass die im Umlauf befindliche Menge an Bitcoins nicht an zyklische Konjunktureffekte oder plötzlichen Veränderungen der Nachfrage angepasst werden kann, sind erhebliche Preisschwankungen möglich.[181] Auch wenn die kurzfristige 30 Tage Volatilität nicht sehr hoch erscheint, ist der Wechselkurs des Bitcoins trotz allem auf Jahresbasis von extremen Preissteigerungen und Preiseinbrüchen geprägt. Während ein Bitcoin noch Anfang März 2018 kurzzeitig über 9.000 Euro wert war beträgt der aktuelle Wert eines Bitcoins 3.179 Euro.[182]

4.5.3 Quantencomputer

Eine weitere potenzielle Gefahr für den aktuellen Blockchain Algorithmus sowohl des Bitcoins, als auch den der meisten Kryptowährungen, könnten sogenannte Quantencomputer werden. Quantencomputer basieren auf Grundlage der Quantenmechanik, also auf einem gänzlich anderen Funktionsprinzip als herkömmliche Computer und können theoretisch **millionenfach** leistungsfähiger als diese sein.[183] Schon ungefähr fünfundzwanzig Jahre lang verbringen Wissenschaftler bereits mit der Erforschung und Entwicklung solcher vielversprechenden Quantencomputersysteme.[184] Dem amerikanischen Großkonzern IBM ist es bereits eigenen Angaben zufolge erfolgreich gelungen, einen Quantencomputer zu testen, der die Rechenleistung von bisherigen Supercomputern bereits übertrifft.[185] Der Quantencomputer soll also zuvor nicht erreichte Grenzen der Rechenleistung von Computersystemen erreichen können. Dadurch ergeben sich gänzlich neue Möglichkeiten. Beispielsweise können Quantencomputer bestimmte

---

[179] Siehe Abschnitt 3.3.
[180] Siehe Abschnitt 4.2.4.3.
[181] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 262.
[182] Vgl. o. V.: Wechselkurs Bitcoin / Euro. Tagestief 13.02.2019. Finanzen.net. URL: *https://www.finanzen.net/devisen/bitcoin-euro-kurs/historisch* , abgerufen am 09.03.2019, 17:00 Uhr.
[183] Vgl. De Souza Soares, Philipp Alvares: Wettlauf um den Quantencomputer: Das nächste große Ding. Spiegel Online Artikel. URL: *http://www.spiegel.de/netzwelt/web/quantencomputer-die-naechste-dimension-der-it-a-1109142.html* , abgerufen am 08.02.2019, 19:25 Uhr.
[184] Vgl. Schlupeck, Bernd: Quantencomputer: Fortschritte in der Forschung. Deutsch-landfunk Online-Artikel. URL: *https://www.deutschlandfunk.de/quantencomputer-fortschritte-in-der-forschung.676.de.html?dram:article_id=417034* , abgerufen am 08.02.2019, 19:30 Uhr.
[185] Vgl. Filipp, Stefan: Quantencomputer: Der Beginn der kommerziellen Quanten-Ära. IBM Dach Blog Artikel. URL: *https://www.ibm.com/de-de/blogs/think/2018/02/23/quantencomputer/* , abgerufen am 08.02.2019, 19:40 Uhr.

Algorithmen aus dem Bereich der Kryptographie deutlich schneller und effizienter lösen.[186] In Abschnitt 4.2.2 wurde beschrieben, wie die public address mittels eines kryptographischen Algorithmus aus dem public address errechnet wird und dass dieser Prozess nicht umkehrbar mittels herkömmlicher Computertechnologie ist. Quantencomputer, die leistungsfähig genug sind, könnten eine Gefahr für diese Annahme sein, da die Rechenleistung noch nie zuvor da gewesene Möglichkeiten eröffnet. Ein solcher Quantencomputer, der genug Leistung erbringen könnte um den Algorithmus zurückzurechnen, konnte zumindest bis jetzt noch nicht gebaut werden. „Wer den ersten funktionsfähigen Computer mit einigen zehntausend *Qubits* [(Je mehr Qubits, umso leistungsfähiger ist der Quantencomputer), d. Verf.] besitzt, könnte damit als erstes die Verschlüsselung von Kryptowährungen hinterfragen.“[187]

Zusammengefasst stellen Quantencomputer bisher also nur eine theoretische Gefahr für den Bitcoin dar.

4.5.4 Skalierung

„Ein wichtiges Merkmal eines Finanzsystems ist, wie viele Transaktionen pro Sekunde verarbeitet werden können.“[188] Bei Bitcoin führen die maximale Speicherkapazität eines Blocks (ein Megabyte) sowie die durchschnittliche Zeitdauer für das Generieren eines neuen Blocks (fünf bis zehn Minuten) zu ein Maximum der möglichen Daten pro Zeiteinheit.[189] „Zur Zeit korrespondiert dieses Datenmaximum mit ungefähr sieben Transaktionen pro Sekunde. Mehr kann das Bitcoin Netzwerk in seiner jetzigen Form nicht bewältigen“[190] Ein weiteres Problem liegt in der Bestätigungsdauer von Transaktionen. Da es durchschnittlich fünf bis zehn Minuten dauert, bis es ein Miner schafft einen Block zu generieren, liegt die dazugehörige Bestätigungsdauer einer Transaktion auch in dieser Größenordnung.[191]

---

[186] Vgl. Hummel, Philipp: Quantencomputer: Kommt der Durchbruch in Deutschland? In: Spektrum der Wissenschaft – die Woche. 2018, S. 44.
[187] Fuest, Benedikt: Dieser Computerchip könnte Bitcoin und Co. wertlos machen. URL: *https://www.welt.de/wirtschaft/webwelt/article174393767/Quanten-Computer-Wie-Superchips-Bitcoin-und-Co-wertlos-machen-koennten.html* , abgerufen am 11.03.2019, 16:00 Uhr.
[188] Hosp, Julian 2017, S. 79.
[189] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 250.
[190] Berentsen, Aleksander ; Schär, Fabian 2017, S. 250.
[191] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 251.

5 Bitcoin als Währung

Um die Frage zu beantworten, ob die Möglichkeit besteht, dass der Bitcoin konventionelle Währungen verdrängen werde, soll in diesem Kapitel zum einen untersucht werden, ob der Bitcoin als Geld im Sinne der Geldtheorie angesehen werden kann. Zum anderen wird erörtert, inwiefern der Bitcoin, falls er sich eines Tages tatsächlich als Währung durchsetzt, das zweistufige Bankensystem ersetzen kann und welche Risiken sich daraus ergeben würden.

5.1 Bitcoin und die Geldtheorie

Im Folgenden soll untersucht werden, ob der Bitcoin als Geld im Sinne der in Kapitel 2 beschriebenen Geldtheorie angesehen werden kann. Dazu werden zuerst die Geldeigenschaften untersucht, um im Anschluss beurteilen zu können ob auch die Geldfunktionen erfüllt sind.

5.1.1 Geldeigenschaften

Generelle Akzeptanz: Derzeit gibt es weltweit knapp 5.000 registrierte Unternehmen[192], die den Bitcoin als Zahlungsmittel akzeptieren, darunter auch bekannte Firmen wie *Microsoft* oder *Dell.*[193] Die Attraktivität, vor allem für Onlineunternehmen ist durchaus begründbar. Hauptgründe dafür sind wohl die im Vergleich zu Kreditkartenzahlungen niedrigeren Transaktionsgebühren, welche im Regelfall vom Verkäufer zu tragen sind.[194] Weiterhin profitiert das Unternehmen von einem Marketingeffekt durch gegebenenfalls mediale Berichterstattung über die Akzeptanz von Kryptowährungen.[195] Unternehmen, die Bitcoin als Zahlungsmethode akzeptieren, leiden weiterhin nicht unter dem Volatilitätsrisiko. Aufgrund der logischen Konsequenz, dass der Preis eines Produkts an den aktuellen Umrechnungskurs[196] angepasst sein muss, könnte der Verkäufer die Kryptowährungen theoretisch unmittelbar nach Erhalt zu dem Euro Kurs verkaufen, zu welchem seine Preise angepasst waren. Aufgrund des kurzen Zeitabstandes würde der

[192] Shops, Läden, Gastronomiebetriebe und weitere Dienstleister.
[193] Vgl. o. V.: Bitcoin Akzeptanzstellen. Investoren Journal. URL: *https://www.investoren-journal.com/bitcoin-akzeptanzstellen/* , abgerufen am 11.02.2019, 18:50 Uhr.
[194] Vgl. Sixt, Elfriede 2017, S. 23.
[195] Vgl. Sixt, Elfriede 2017, S. 23.
[196] Umrechnungskurs des Bitcoins zu einer staatlichen Währung wie dem Euro.

Tausch der Kryptowährungen in eine konventionelle Währung entweder gar keinem oder einem nur sehr geringen Wertunterschied unterliegen.

Eine Online-Umfrage vom 28.08.2017 ergab, dass von 10.000 befragten Deutschen lediglich 1,7 % Kryptowährungen als Zahlungsmittel einsetzen.[197] Die Zahl der Bitcoin Nutzer ist weit unterhalb der kritischen Masse, deren Überspringen notwendig für die Verdrängung einer etablierten Währung wäre.[198] Nicht nur die Volatilität, sondern auch die Tatsache, dass die Bestätigungsdauer[199] einer Transaktion bis zu zehn Minuten betragen kann, bieten dem Konsumenten erhebliche Nachteile gegenüber konventionellen Bezahlverfahren.[200] Weiterhin spielt auch der geringe Kenntnisstand der Bevölkerung über die Funktionsweise von Kryptowährungen eine wichtige Rolle.[201] Die Eigenschaft der generellen Akzeptanz ist somit bisher nicht erfüllt.

Homogenität: Für diese Eigenschaft sind bestimmte physische Charakteristika wie Material, Form, Größe oder Aussehen ausschlaggebend. Da Bitcoin eine rein digitale Währung ist, kann diese Eigenschaft weder widerlegt noch bestätigt werden.

Haltbarkeit: Die Eigenschaft der Haltbarkeit im Sinne der Nichtverderblichkeit kann bestätigt werden, da der Bitcoin rein digitaler Natur ist und die Transaktionen in der Blockchain nicht reversibel sind.

---

[197] Vgl. Statista (Hrsg.): Umfrage in Deutschland zur Zahlungsbereitschaft mit Kryptowährungen (BitCoin) 2017. URL: *https://de.statista.com/statistik/daten/studie/742385/umfrage/umfrage-in-deutschland-zur-zahlungsbereitschaft-mit-kryptowaehrungen-bitcoin/* , abgerufen am 11.02.2019, 18:50 Uhr.
[198] Vgl. Michaelis, Jochen: Die Konkurrenz umarmen: Digitales Zentralbankgeld. In: ifo Schnelldienst. 2017, S. 17.
[199] Ein Block wird aller zehn Minuten erstellt, siehe Abschnitt 4.5.4.
[200] Vgl. Sixt, Elfriede 2017, S. 23.
[201] Vgl. Sixt, Elfriede 2017, S. 24.

Teilbarkeit: Wie aus Anlage 4 entnommen werden kann, ist eine Bitcoin Einheit bis auf die achte Nachkommastelle teilbar.[202] Zum Vergleich sind es beim Euro lediglich höchstens zwei Nachkommastellen. Aufgrund der Tatsache, dass ein Bitcoin nach dem aktuellen[203] Umrechnungskurs 3.179 Euro wert ist, würde man aktuell beispielsweise für eine Pizza mit einem Euro Wert von 5,50 Euro, einen Betrag in Bitcoin von 0,0017 Bitcoin bezahlen. „Die Problematik solcher Preise besteht in der Schwierigkeit der Informationserfassung. Verschiedene Marketing-Studien zeigen die Probleme von Konsumenten, Dezimalstellen korrekt zu interpretieren und zu vergleichen."[204] Trotz dieses Nachteiles kann die Teilbarkeit des Bitcoins nicht verneint werden.

Wertbeständigkeit: Wie in Abschnitt 4.5.2 beschrieben, ist der Bitcoin langfristig sehr volatil und erfüllt die Eigenschaft der Wertbeständigkeit daher keineswegs.

Kompaktheit: Um am Bitcoin Netzwerk teilzunehmen, benötigt man eine Internetverbindung.[205] Um diese Voraussetzung auch unterwegs erfüllen zu können, ist es am praktikabelsten, ein Smartphone oder ein sonstiges digitales Gerät dafür zu benutzen. Vorausgesetzt, der Nutzer ist technisch soweit versiert, dass er mit einem Smartphone umgehen kann und überhaupt ein solches besitzt, so erfüllt der Bitcoin diese Eigenschaft hinsichtlich seiner digitalen Präsenz hervorragend. Das Problem liegt jedoch darin, dass dieser Personenkreis begrenzt ist. Laut einer Umfrage nutzten im Jahr 2018 von ca. 83 Millionen rund 57 Millionen Personen in Deutschland ein Smartphone.[206] Die Eigenschaft der Kompaktheit ist bei Bitcoin zwar unzweifelhaft gegeben, erfordert jedoch einen gewissen technischen Wissensstand des Nutzers.

---

[202] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 273.
[203] Vgl. o. V.: Wechselkurs Bitcoin / Euro. Tagestief 13.02.2019. Finanzen.net. URL: *https://www.finanzen.net/devisen/bitcoin-euro-kurs/historisch* , abgerufen am 09.03.2019, 17:00 Uhr.
[204] Berentsen, Aleksander ; Schär, Fabian 2017, S. 273.
[205] Vgl. Hosp, Julian 2018, S. 50.
[206] Vgl. Statista (Hrsg.): Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2018 (in Millionen). URL: *https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/* , abgerufen am 11.02.2019, 19:50 Uhr.

5.1.2 Geldfunktionen

5.1.2.1 Eignung als Tausch- bzw. Zahlungsmittel

Der Bitcoin ist zwar kein gesetzliches Zahlungsmittel, was jedoch per se kein Ausschlusskriterium ist um als Zahlungsmittel fungieren zu können. Gemäß § 14 Abs. 1 Satz 2 des Gesetzes über die Deutsche Bundesbank, ist Bargeld das einzig gesetzliche Zahlungsmittel in Deutschland.[207] Im Umkehrschluss ist das in Abschnitt 3.1 beschriebene Buchgeld, also kein gesetzliches Zahlungsmittel. Das bedeutet, dass jede bargeldlose Euro Zahlung in Deutschland nur deshalb getätigt werden kann, weil das Buchgeld generell als Zahlungsmittel akzeptiert wird.

Wie an vorheriger Stelle erwähnt, ist eine generelle Akzeptanz des Bitcoins nicht gegeben, da es einerseits zu wenig Unternehmen gibt, die Bitcoin als Zahlungsmittel akzeptieren und andererseits zu wenige Personen, die Bitcoin als Zahlungsmittel verwenden. Gegen die Eignung als Tauschmittel spricht weiterhin die durchschnittlich bis zu zehnminütige Bestätigungsdauer einer Transaktion.[208] Dies kann vor allem bei Bezahlungen an der Ladenkasse unkomfortabel sein. Dagegen könnte man anbringen, dass Überweisungen und Kreditkartenzahlungen im Bankensystem einen oder mehrere Werktage andauern können.[209] Der Unterschied ist jedoch, dass bei der Bank im Zeitpunkt des Kaufes eine Zahlungsverbindlichkeit verbucht wird, welche später ausgeführt wird. Der Verkäufer hat hier die Sicherheit, dass seine Zahlungsforderung gegen den Käufer vollstreckt werden kann, falls das Konto des Käufers beispielsweise ungedeckt ist. Im Falle des Bitcoins stellt sich die Vollstreckung von Zahlungsversprechen als schwierig heraus, da es keine zentrale Instanz gibt und die Nutzung unter Pseudonymen erfolgt. Ein weiterer Aspekt, der für die Eignung als Tauschmittel eine wichtige Rolle spielt, ist die Komplexität, denn diese wirkt sich im Falle des Bitcoins negativ auf die derzeitige Akzeptanz durch Händler und Verbraucher aus.[210]

Zusammengefasst erfüllt der Bitcoin, vor allem aufgrund der aktuell noch zu niedrigen Akzeptanz nicht die Funktion eines Tausch- bzw. Zahlungsmittels.

---

[207] Gesetz über die Deutsche Bundesbank (BBankG) in der Fassung der Bekanntmachung vom 22. Oktober 1992 (BGBl. I S. 1782), zuletzt geändert durch Artikel 23 des Gesetzes vom 4. Juli 2013 (BGBl. I S. 1981).
[208] Siehe Abschnitt 4.5.4.
[209] Vgl. Deutsche Bundesbank 2017, S. 64.
[210] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 244.

5.1.2.2 Eignung als Wertaufbewahrungsmittel

Für diese Geldfunktion spielen vor allem die vorherbestimmte und begrenzte Geldschöpfung sowie die Volatilität eine Rolle. Wie in Abschnitt 4.2.4.3 beschrieben, ist die maximale Geldmenge des Bitcoins auf 21 Millionen Einheiten begrenzt. Die Wachstumsrate der Geldmenge nimmt durch den Halbierungsprozess[211] der neu in Umlauf gebrachten Bitcoin Einheiten stetig ab und nähert sich asymptotisch einem Nullwert an, was eine Seltenheit der Bitcoin Einheiten impliziert.[212] Diese Tatsache könnte den Bitcoin durchaus als Wertanlage interessant machen. „Bleibt die Nachfrage an Bitcoin Einheiten bestehen, wird ein positives Wirtschaftswachstum dazu führen, dass eines Tages eine konstante Anzahl an Bitcoin Einheiten einem wachsenden Güter- und Dienstleistungspool gegenübersteht.“[213] Diese Aussage prognostiziert eine potenzielle hohe Wertsteigerung des Bitcoins unter der Prämisse, dass die Nachfrage nicht abnimmt. Im Umkehrschluss ist ebenso möglich, dass der Preis eines Bitcoins auf null stürzt, falls die Nachfrage zurückgeht oder sogar verschwindet und die Anleger das Vertrauen in die Etablierung der Technologie völlig verlieren. Wenn man versucht aufgrund der begrenzten Geldschöpfung einen sicheren Preisanstieg zu begründen, befindet man sich im Bereich der Spekulation, da die moderne Geldtheorie keinen festen Zusammenhang zwischen Geldmenge und Preisentwicklung postuliert.[214] Erhebliche Preisanstiege mit attraktiven Renditen sind ebenso schädlich für die Geldfunktionen, wie hohe Wertverluste. Vielmehr sollte der Wert einer Geldeinheit möglichst konstant bleiben. „Fällt der Wert einer Geldeinheit zu schnell, versagt die Wertspeicher-Funktion (…). Ist eine Geldeinheit hingegen ein attraktives Investment und wirft hohe Renditen ab, kann dies eine hemmende Wirkung auf die Tauschmittelfunktion haben.“[215]

Zusammengefasst erfüllt der Bitcoin die Wertaufbewahrungsfunktion nicht, da die Wertschwankungen zu hoch sind und im Gegensatz zu konventionellen Währungen nicht von einer zentralen Instanz abgedämpft werden können.[216]

---

[211] Regelmäßige Halbierung der neu in Umlauf gebrachten Einheiten, siehe Abschnitt 4.2.4.3.
[212] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 255.
[213] Berentsen, Aleksander ; Schär, Fabian 2017, S. 255.
[214] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 256.
[215] Berentsen, Aleksander ; Schär, Fabian 2017, S. 270.
[216] Siehe Abschnitt 4.5.2.

5.1.2.3 Eignung als Recheneinheit

Aufgrund der Tatsache, dass der Bitcoin teilbar[217] ist, lassen sich Güterwerte in einer Bezugsgröße ausdrücken und es können sich verschiedene Preise abbilden. Der Zweck dieser Funktion liegt jedoch darin, den Handel durch die Vergleichbarkeit von Gütern zu vereinfachen.[218] Zwar sind Preisbildungen in Bitcoin-Einheiten möglich, man muss jedoch folgende zwei Kritikpunkte hinzufügen. Zum einen, die an vorheriger Stelle angesprochene Schwierigkeit der Menschen, Dezimalstellen zu erfassen und korrekt interpretieren zu können, da die Preisdarstellung in Dezimalzahlen erfolgen würde. Zum anderen kann aus der Volatilität des Bitcoins logisch geschlussfolgert werden, dass Preise ständig angepasst werden müssten, was eine Vergleichbarkeit von Gütern auf lange Sicht erheblich erschweren würde.

Zusammengefasst kann man sagen, dass der Bitcoin die Funktion als Recheneinheit grundsätzlich erfüllt, jedoch bei weitem nicht in dem Umfang wie konventionelle und kursstabilere Währungen.

5.2 Gefahren und Risiken

In diesem Abschnitt soll darauf eingegangen werden, inwieweit der Bitcoin die Funktionen und Aufgaben der Zentralbanken und Geschäftsbanken ersetzen kann. Wenn dem so wäre, könnten die Banken Gefahr laufen, entbehrlich zu werden. Außerdem sollen potenzielle Risiken und Gefahren erörtert werden, welche sich ergeben könnten, wenn den Banken die Kontrolle über die Geldmenge verloren ginge.

5.2.1 Bitcoin versus Zentralbanken

Wie die folgende Ausführung zeigen wird, stellen Kryptowährungen eine theoretische Gefahr für die Existenz von Zentralbanken dar. Falls es Kryptowährungen schaffen, den Euro oder andere konventionelle Währungen, welche auf einem Zentralbankensystem basieren zu verdrängen, würden die Zentralbanken überflüssig.

---

[217] Siehe Abschnitt 5.1.1.
[218] Siehe Rechenbeispiel in Abschnitt 2.1.3.

Zentralbanken besitzen das sogenannte Notenmonopol. Nur die Zentralbanken besitzen das Recht, Banknoten als gesetzliches Zahlungsmittel in Umlauf zu bringen.[219] Da die Geldschöpfung von Kryptowährungen dezentral durch einen festgelegten Algorithmus erfolgt[220], würden die Zentralbanken in der Konsequenz einerseits ihr Notenmonopol und andererseits ihren Einfluss auf die Geldmenge verlieren.

Wie im Abschnitt 3.2.2. beschrieben, kommt das Bargeld der Zentralbanken über die Geschäftsbanken in Umlauf, welche sich das Bargeld gegen einen Kredit von der Zentralbank leihen. Auf diesen Kredit erhebt die Zentralbank Zinsen und erwirtschaftet somit einen Zinsertrag, solange die Banknoten in Umlauf sind.[221] Diese Erträge werden auch als Seigniorage-Einkünfte bezeichnet.[222] Diese Gewinne werden typischerweise an den Staat abgeführt.[223] Kryptowährungen als dominante Währung, würden den Zentralbanken das Notenmonopol entziehen, wodurch dem Staat und den Zentralbanken die Seigniorage-Einkünfte verloren gehen würden.

5.2.2 Bitcoin versus Geschäftsbank

Der Zahlungsverkehr mit Kryptowährung ermöglicht eine Transaktion zwischen zwei Teilnehmern ohne eine zentrale Instanz, welche die Transaktion verifizieren muss.[224] Somit könnten Kryptowährungen die Geschäftsbanken als Drehscheibe für den bargeldlosen Zahlungsverkehr eliminieren, da Transaktionen von den Minern verifiziert werden.[225]

Kryptowährungen würden jedoch nicht zwangsläufig die Geschäftsbanken als solche eliminieren, sondern würden nur ihre Funktion in der Abwicklung des bargeldlosen Zahlungsverkehrs überflüssig machen. Falls es eine Kryptowährung

---

[219] Vgl. Deutsche Bundesbank 2017, S. 22.
[220] Siehe Abschnitt 4.2.4.3.
[221] Vgl. Deutsche Bundesbank 2017, S. 79.
[222] Vgl. Europäische Zentralbank (Hrsg.): Was ist Seigniorage? URL: *https://www.ecb.europa.eu/explainers/tell-me/html/seigniorage.de.html* , abgerufen am 18.02.2019, 16:45 Uhr.
[223] Vgl. Deutsche Bundesbank 2017, S. 79.
[224] Siehe Abschnitt 4.2.4.
[225] Vgl. Mayer, Thomas: Die Evolution des Geldes. In: ifo Schnelldienst. 2017, S. 8.

schafft, sich als dominante Währung zu etablieren, könnten Geschäftsbanken trotzdem theoretisch zumindest im Kreditbereich tätig bleiben. Im Unterschied zum konventionellen Bankensystem, könnten die Geschäftsbanken jedoch durch die Kreditvergabe kein neues Buchgeld schaffen, sondern lediglich zwischen Sparern und Kreditnehmern vermitteln.[226] Es kann die Hypothese gewagt werden, dass der an den Kreditgeber zu zahlende Zins zum Teil der Bank für die Vermittlungsleistung zufließen könnte. Ebenso kann nicht ausgeschlossen werden, dass die Banken ihren Kunden eine Anlegung und Verzinsung ihrer Bitcoins anbieten könnten.

Mit dem Wegfall einer Bank als zentrale Instanz fallen allerdings auch die damit verbundenen Vorteile für den Nutzer weg. An dieser Stelle soll folgendes Risiko hervorgehoben werden, welches sich als eines der größten Probleme im Umgang mit Kryptowährungen etablieren könnte. Bei dezentralen Systemen wie dem Bitcoin gibt es keine Datenbank, welche alle Konten und Passwörter speichert.[227] Wenn ein Bitcoin-Nutzer den Zugang zu seinem private key verliert, verliert er ebenso den Zugriff auf das gesamte unter dieser Adresse verwaltete Vermögen.[228] „Mit heutigen kryptographischen Verfahren ist eine Wiederherstellung praktisch nicht möglich.“[229] Im Gegensatz dazu kann ein Bankkunde einfach einen neuen PIN beantragen, sobald die Bank die Legitimität des Kunden überprüfen konnte. Nur durch die Lösung dieses Problems könnten Kryptowährungen massentauglich werden.[230]

[226] Vgl. Mayer, Thomas: Die Evolution des Geldes. In: ifo Schnelldienst. 2017, S. 8.
[227] Vgl. Hosp, Julian 2017, S. 50.
[228] Vgl. Elsner, Dirk ; Pecksen, Gerrit: Kryptowährungen sind noch nicht reif für eine weitreichende Umsetzung. In: ifo Schnelldienst. 2017, S. 10.
[229] Elsner, Dirk ; Pecksen, Gerrit: Kryptowährungen sind noch nicht reif für eine weitreichende Umsetzung. In: ifo Schnelldienst. 2017, S. 10.
[230] Vgl. Hosp, Julian 2017, S. 97.

5.2.3 Risiko für die Wirtschaftsstabilität

Das Ziel des europäischen Zentralbanksystems ist im Artikel 127 Absatz 1 Satz 1 des Vertrages über die Arbeitsweise der Europäischen Union geregelt. „Das vorrangige Ziel des Europäischen Systems der Zentralbanken (…) ist es, die Preisstabilität [durch Maßnahmen der Geldpolitik, d. Verf.] zu gewährleisten.“[231] Preisstabilität ist nach Definition der EZB gegeben, wenn die jährliche Preissteigerungsrate unter, aber nahe 2 % liegt, sodass nach dieser Definition der Inflation im Sinne eines unerwünschten wirtschaftlichen Prozesses eigentlich erst dann herrscht, wenn die jährliche Preissteigerungsrate für einen längeren Zeitraum deutlich über 2 % liegt.[232] Grundsätzlich gilt jedoch, dass sowohl Inflation (Erhöhung des Preisniveaus), als auch Deflation (Rückgang des Preisniveaus) schädlich für die Stabilität einer Volkswirtschaft sind und die Aussagekraft von Preisen zerstören.[233]

Wenn sich Kryptowährungen gegen konventionelle Währungen durchsetzen würden, könnte die Zentralbank keinen Einfluss mehr auf deren Geldmenge nehmen, da die Geldschöpfung bei Kryptowährungen einem festen vorherbestimmten Algorithmus folgt.[234] Dadurch entfällt die Geldpolitik als Anpassungs- und Stabilitätsinstrument, wodurch sich Schocks jeder Art stärker auf die reale Ökonomie durchschlagen würden.[235] „Da sich, vereinfacht dargestellt, die Nachfrage des Geldes [(also der Nachfrage nach Krediten), d. Verf.] durch reales Wirtschaftswachstum und veränderte Umlaufgeschwindigkeit ändern kann, muss auch das Angebot [(die Geldmenge), d. Verf.] angepasst werden, damit der Wert des Geldes stabil bleibt.“[236] Das bedeutet, dass die Nachfrage nach Geld[237] an die jeweilige Wirtschaftslage angepasst werden muss, um somit Preisstabilität zu gewährleisten. Dies kann nur durch eine flexible Steuerung der Geldmenge gewährleistet

[231] Vertrag über die Arbeitsweise der Europäischen Union (AEUV) in der Fassung aufgrund des am 1.12.2009 in Kraft getretenen Vertrages von Lissabon, zuletzt geändert durch die Akte über die Bedingungen des Beitritts der Republik Kroatien und die Anpassungen des Vertrags über die Europäische Union, des Vertrags über die Arbeitsweise der Europäischen Union und des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. EU L 112/21 vom 24.4.2012) m. W. v. 1.7.2013.
[232] Vgl. Deutsche Bundesbank 2017, S. 152.
[233] Vgl. Deutsche Bundesbank 2017, S. 160, 161.
[234] Siehe Abschnitt 4.2.4.3.
[235] Vgl. Michaelis, Jochen: Die Konkurrenz umarmen: Digitales Zentralbankgeld. In: ifo Schnelldienst. 2017, S. 17.
[236] Diehl, Martin ; Thiele, Carl-Ludwig: Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten? In: ifo Schnelldienst. 2017, S. 5.
[237] Nachfrage nach Geld bedeutet in diesem Kontext Nachfrage nach Krediten.

sein, was der derzeitige Blockchain-Algorithmus aufgrund des starren Geldschöpfungsprozesses und der fehlenden Anpassungsmechanismen nicht bieten kann.

Die unflexible Geldmenge führt zu einem weiteren Problem. Aufgrund der vorherbestimmten Limitierung des Bitcoins auf 21 Millionen Einheiten[238], neigt der Bitcoin zu deflationären Tendenzen. Deflation hat einen Rückgang des allgemeinen Preisniveaus zur Folge, was vereinfacht bedeutet, dass die Preise für Güter sinken.[239] Für den Verbraucher erscheint dies zunächst profitabel, jedoch ist Deflation schädlich für die Stabilität des Wirtschaftssystems. Dies liegt daran, dass die Verbraucher weiter auf sinkende Preise hoffen und somit Konsumausgaben eher in die Zukunft verlagern.[240] Diese Konsumstagnation kann Unternehmen dazu veranlassen ihre Produktion einzuschränken, eigene Investitionen zu stoppen und Arbeitnehmer zu entlassen.[241]

Ein weiteres erhebliches Wirtschaftsrisiko könnte sich ergeben, wenn der Bitcoin mehrere Währungen verschiedener Währungsräume verdrängt, wodurch das Wechselkursinstrument entfallen würde.[242] Dies könnte vor allem für wirtschaftlich schwächere Länder zu einem wirtschaftlichen Kollaps beitragen, denn freie Wechselkurse können wirtschaftliche Unterschiede effizient ausgleichen.[243] Mit unterschiedlichen Währungen und freien Wechselkursen könnten wirtschaftlich schwächere Länder leichter konkurrenzfähig auf internationalen Märkten bleiben, indem die eigene Währung entwertet wird. Diese Entwertung führt dazu, dass in diesem Land die Exporte wieder zunehmen (da das Ausland durch den günstigeren Wechselkurs billiger einkaufen kann) und im Umkehrschluss dazu die Importe sinken.[244]

---

[238] Siehe Abschnitt 4.2.4.3.
[239] Vgl. Deutsche Bundesbank 2017, S. 161.
[240] Vgl. Deutsche Bundesbank 2017, S. 161.
[241] Vgl. Deutsche Bundesbank 2017, S. 161.
[242] Vgl. Michaelis, Jochen: Die Konkurrenz umarmen: Digitales Zentralbankgeld. In: ifo Schnelldienst. 2017, S. 17.
[243] Vgl. Günter Hannich: Wechselkurse: Darum sind sie so wichtig. URL: *https://crash-investor.de/wechselkurse-darum-sind-sie-so-wichtig/* , abgerufen am 20.02.2019, 20:40 Uhr.
[244] Vgl. Günter Hannich: Wechselkurse: Darum sind sie so wichtig. URL: *https://crash-investor.de/wechselkurse-darum-sind-sie-so-wichtig/* , abgerufen am 20.02.2019, 20:40 Uhr.

6 Chancen der Bitcoin Technologie

In diesem Kapitel soll es um die Chancen und Möglichkeiten der Technologie gehen, welche sich hinter dem Bitcoin verbirgt. Diese Technologie wird als Distributed-Ledger-Technologie (DLT)[245] bezeichnet. Sie ermöglicht es, durch ein öffentliches, dezentral geführtes Kontobuch, Vermögenswerte direkt von Nutzer zu Nutzer zu übertragen, ohne den Einsatz einer zentralen Instanz vorauszusetzen. Sie bietet die essentielle Grundlage für die Existenz aller Kryptowährungen.[246] Die Distributed-Ledger-Technologie, welche dem Bitcoin zugrunde liegt, wird als Blockchain bezeichnet.

6.1 Chancen für Banken und Unternehmen

Vor allem Zentralbanken sehen die Entwicklung von Kryptowährungen mehrheitlich kritisch an, nicht zuletzt auch deshalb, weil diese potenziell die Effektivität ihrer Geldpolitik beeinträchtigen könnten.[247] Allerdings wird der dahinterstehenden DLT sehr viel Potenzial zugemessen, unter anderem um Prozesse im Bereich des Zahlungsverkehrs und des Wertpapierhandels effizienter zu gestalten. Die DLT der Bitcoin-Blockchain ist laut der Deutschen Bundesbank in seiner derzeitigen Form dafür jedoch noch zu unausgereift und benötigt weitere Anpassungen und Entwicklungen.[248] Im Folgenden wird auf potenzielle Vorteile sowohl für Banken als auch für Unternehmen eingegangen, welche die DLT bieten könnte.

Transparenz und Unveränderlichkeit:

Die Aufbewahrung und der Austausch von Informationen kann fälschungssicher erfolgen, da das gesamte Netzwerk auf die gleiche unveränderliche Datenhistorie zurückgreifen kann.[249] „Dies ermöglicht das manipulationssichere Speichern von

[245] Zu deutsch: Technologie des verteilten Kontenbuchs.
[246] Vgl. Geiling, Luisa: Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain. In: Bafin Journal. 2016, S. 29.
[247] Vgl. Elsner, Dirk ; Pecksen, Gerrit: Kryptowährungen sind noch nicht reif für eine weitreichende Umsetzung. In: ifo Schnelldienst. 2017, S. 11.
[248] Vgl. Deutsche Bundesbank (Hrsg.): Monatsbericht September 2017. In: Monatsbericht September. 2017, S. 41.
[249] Vgl. Deutsche Bundesbank (Hrsg.): Monatsbericht September 2017. In: Monatsbericht September. 2017, S. 40.

Transaktionen, ohne dass gegenseitiges Vertrauen zwischen den Netzwerkteilnehmern erforderlich ist."[250]

Automatische Vertragsabwicklung:

Banken könnte es durch sogenannte *smart contracts*[251] möglich werden, Verträge automatisch von der DLT abwickeln zu lassen und somit Prozesse zu optimieren. „DLT könnte zum Beispiel zur automatisierten Auszahlung von Zinsen oder Dividenden im Wertpapiergeschäft genutzt werden."[252]

Effizienz bei komplexen Finanzmarktgeschäften:

Die DLT könnte komplexe Arbeitsprozesse von Finanzmarktgeschäften, vor allem solche mit hohem Abstimmungsbedarf[253] zwischen den Teilnehmern, erheblich optimieren. Die DLT ermöglicht einen direkten Abstimmungsprozess zwischen den Teilnehmern und eine automatische Dokumentation mehrerer prozessaufwendiger Zwischenschritte.[254] Dies kann die Transferzeit erheblich verkürzen und die Abwicklungskosten solcher komplexen Finanzgeschäfte senken.[255]

Niedrige Transaktionskosten:

Da die DLT die Übertragung von Vermögenswerten direkt von einem Teilnehmer zu einem anderen ermöglicht, sind Transaktionen mit niedrigeren Kosten als herkömmliche bargeldlose Übertragungen verbunden, da ein zentraler Intermediär, welcher Transaktionen überprüfen und zwischen den Teilnehmern abstimmen muss, entfällt.[256] Vor allem für Unternehmen sind die niedrigen Transaktionskosten sehr attraktiv, weil sich die Transaktionsgebühren bei herkömmlichen Zahlungen mit Kredit- oder Debitkarte auf 1 % bis 3 % belaufen.[257] Weiterhin sind

---

[250] Deutsche Bundesbank (Hrsg.): Monatsbericht September 2017. In: Monatsbericht September. 2017, S. 40.
[251] Smart contracts werden in Abschnitt 6.2.2 näher erklärt.
[252] Deutsche Bundesbank (Hrsg.): Monatsbericht September 2017. In: Monatsbericht September. 2017, S. 41.
[253] Zu solchen Geschäften zählen insbesondere Händel mit Wertpapieren.
[254] Vgl. Deutsche Bundesbank (Hrsg.): Monatsbericht September 2017. In: Monatsbericht September. 2017, S. 41.
[255] Vgl. Deutsche Bundesbank (Hrsg.): Monatsbericht September 2017. In: Monatsbericht September. 2017, S. 41.
[256] Vgl. Deutsche Bundesbank (Hrsg.): Monatsbericht September 2017. In: Monatsbericht September. 2017, S. 44.
[257] Vgl. Sixt, Elfriede 2017, S. 23.

aufgrund der niedrigen Transaktionskosten sogenannte *Mircopayments*, also die bargeldlose Bezahlung von Kleinstbeträgen, zu annehmbaren Kosten möglich.[258]

Des Weiteren sind währungsübergreifende Transaktionen mit den etablierten Währungen sehr kostspielig und zeitintensiv. Beispielsweise kostet eine Überweisung der Commerzbank von einem deutschen Konto auf ein ausländisches Konto einer anderen Währung ab einem Betrag von 250 Euro 1,5 % des Überweisungsbetrages, zuzüglich 2,50 Euro Standardabwicklungsentgelt.[259] Bei globalen Transaktionen mit Kryptowährungen entstehen jedoch keinerlei Mehrkosten im Vergleich zu inländischen Überweisungen.

6.2 Weitere Anwendungen der Blockchain Technologie

In diesem Abschnitt geht es um beispielhafte Anwendungsmöglichkeiten der Blockchain außerhalb des monetären Bereichs. Es soll gezeigt werden, wie vielfältig die Einsatzmöglichkeiten einer dezentralen Blockchain sind.

6.2.1 Dezentrale Nachweise und Datenbanken

Außer Transaktionsdaten können auch Informationen anderer Art auf der Blockchain gespeichert werden. „Die (…) Blockchain ist im Grunde genommen nichts anderes, als ein eindeutiges und dezentral geführtes Register [(bzw. Datenbank), d. Verf.].“[260] Daraus lassen sich vielfältige Einsatzgebiete schlussfolgern.

Beispielsweise können dezentrale Grundbücher zum sicheren Eigentumsnachweis von Grundstücken und Immobilien genutzt werden. Dies könnte vor allem in Ländern Südamerikas, Afrikas oder Asiens eine Rolle spielen, in denen Enteignungen zu befürchten sind und in denen ein bloßer Eintrag in das Grundbuch keine wirkliche Garantie für den Besitz darstellt.[261] Es herrscht eine Verunsicherung über tatsächliche Besitzverhältnisse. Dies schreckt auch ausländische Investoren davon ab, notwendige Investitionen in solchen Ländern zu tätigen, da bestehende

[258] Vgl. Sixt, Elfriede 2017, S. 23.
[259] Vgl. Commerzbank (Hrsg.): Preis- und Leistungsvergleich. Frankfurt am Main : Commerzbank. Stand 1. März 2019, S. 9.
[260] Berentsen, Aleksander ; Schär, Fabian 2017, S. 278.
[261] Vgl. Hosp, Julian 2018, S. 104.

Grundbucheintragungen plötzlich für nichtig erklärt und bestehende Besitzer enteignet werden könnten.[262] Durch die Implementierung der Grundbucheinträge in eine Blockchain würde eine fälschungssichere und unumkehrbare Chronologie von Eigentums- und Besitzrechten entstehen.[263] Durch die Eigenschaft der Blockchain öffentlich eingesehen werden zu können, würde dies ein erhebliches Maß an vertrauensschaffender Transparenz für beispielsweise potenzielle Investoren schaffen.

Dieses Prinzip einer transparenten, dezentralen und fälschungssicheren Datenbank auf Blockchain Basis könnte beispielsweise auch Patentanmeldungen erleichtern und dabei Kosten für einen Patentanwalt sparen bzw. verringern. Implementiert man die Informationen eines angemeldeten Patents zusammen mit einem Zeitstempel auf eine Blockchain, so könnte dies jedem ermöglichen zu prüfen ob ein Patent schon vergeben wurde, wodurch keine kostenverursachende Instanz mehr benötigt wird, die dies übernimmt.[264]

6.2.2 Smart contracts

Ein weiteres umfangreiches Anwendungsgebiet erschließt sich aus sogenannten *smart contracts.* Übersetzt bedeutet dies soviel wie *intelligente Verträge*. Die 2013 entwickelte Kryptowährung *Ethereum* bietet, neben der bisherigen monetären Funktion, auch erstmals die Möglichkeit solcher smart contracts.[265] Ethereum ist ausgereifter als Bitcoin und basiert auf einer neuen Blockchain, welche auch *Blockchain der zweiten Generation* genannt wird.[266] Dabei geht es darum, digitale Verträge auf eine Blockchain zu implementieren. Die Vertragsparteien müssen vorher die Vertragsbedingungen[267] vereinbaren und diese dem Netzwerk bekannt geben. Die Blockchain stellt sicher, dass diese Verträge auch tatsächlich ausgeführt bzw. erfüllt werden und übernimmt dabei die Funktion einer neutralen dritten Partei.[268] Durch diese Funktionsübernahme könnten sich die Vertragsparteien Kosten für bisherige dritte Parteien wie zum Beispiel Notare oder Anwälte sparen.

---

[262] Vgl. Hosp, Julian 2018, S. 104.
[263] Vgl. Berentsen, Aleksander ; Schär, Fabian 2017, S. 281.
[264] Vgl. Hosp, Julian 2018, S. 110.
[265] Vgl. Hosp, Julian 2017, S. 134.
[266] Vgl. Hosp, Julian 2017, S. 134.
[267] Eine oder mehrere Konsequenzen, welche automatisch ausgeführt werden, wenn ein oder mehrere Ereignisse eintreten. Beispielsweise: Eigentum an Immobilie wird automatisch auf den Käufer übertragen (Konsequenz), sobald dieser den vereinbarten Kaufpreis gezahlt hat (Ereignis).
[268] Vgl. Hosp, Julian 2018, S. 122.

Weiterhin wäre es nicht mehr nötig, solchen dritten Parteien vertrauen zu müssen. Eine Versicherung beispielsweise könnte ihre Verträge mit einem Kunden in eine Blockchain implementieren, wobei der Kunde darauf vertrauen kann, dass die Blockchain automatisch für eine vertragskonforme Umsetzung sorgt. Es ist möglich, vollkommen automatisiert sicherzustellen, dass Verträge eingehalten werden.[269] Auch die Deutsche Bundesbank sieht in den smart contracts viel Potenzial, Prozesse im Bankwesen zu optimieren und die Erfüllung von vertraglichen Ansprüchen zu automatisieren.[270]

[269] Vgl. Brühl, Volker: Bitcoin und andere Kryptowährungen – konsequente Regulierung und Aufsicht sind dringend geboten. In: ifo Schnelldienst. 2017, S. 15.
[270] Vgl. Deutsche Bundesbank (Hrsg.): Monatsbericht September 2017. In: Monatsbericht September. 2017, S. 41.

7 Schluss und Ausblick

Im Folgenden werden die Untersuchungsergebnisse zusammengefasst und ein Ausblick auf die Zukunft der Kryptowährungen gegeben.

Bitcoin ist kein Geld im Sinne der konventionellen Geldtheorie. Die hohen langfristigen Wertschwankungen machen den Bitcoin als Wertanlage bzw. Spekulationsobjekt interessant, jedoch nicht als Zahlungsmittel. Die Akzeptanz des Bitcoins hat zwar in den letzten Jahren stetig zugenommen, ist jedoch bei weitem nicht ausreichend, um der Funktion als Zahlungsmittel gerecht zu werden, geschweige denn konventionelle Währungen verdrängen zu können. Die eher unpraktische Darstellung von Preisen mit bis zu 8 Dezimalstellen sowie die Komplexität der Funktionsweise wirken sich besonders negativ auf die Akzeptanz des Bitcoins aus.

Obwohl der Bitcoin dem Geldbegriff nicht entspricht, ist es dennoch möglich, Vermögenswerte direkt von Nutzer zu Nutzer zu übertragen, ohne dafür einer zentralen Institution wie einer Bank vertrauen zu müssen. Satoshi Nakamoto konnte demzufolge das umsetzen, was er in seinem white-paper beschrieben hatte, und zwar ein **funktionierendes dezentrales Bezahlsystem** zu entwickeln.

Der **Bitcoin macht Geschäftsbanken als Drehscheibe für den Zahlungsverkehr überflüssig**. Die Überprüfungen der Transaktionen übernehmen die Miner. Die Blockchain kann erstmals das Problem des double-spending lösen, ohne eine zentrale Institution zu verwenden.

Der **Bitcoin kann nicht die Funktionen der Zentralbanken übernehmen**. Der unflexible Algorithmus, der die in Umlauf befindliche Menge an Bitcoins bestimmt, ist nicht in der Lage, auf konjunkturelle Veränderungen zu reagieren. Die Menge an Bitcoins kann nicht flexibel gesteuert werden, wodurch keine Preisstabilität gewährleistet werden kann, was ein großes Risiko für Wirtschaft und private Haushalte darstellen würde. Die deflationäre Tendenz würde sich negativ auf die Konjunktur auswirken, da Verbraucher ihre Ausgaben möglichst auf die Zukunft verlagern würden.

Dennoch kann durchaus von einer **revolutionären Technologie** die Rede sein. Satoshi Nakamoto hat mit dem Bitcoin eine Technologie präsentiert, welche das Vertrauen in zentrale Institutionen dem Grunde nach infrage stellt. Aufbauend auf dieser Technologie können in Zukunft Systeme entwickelt werden, welche zentrale Einrichtungen entbehrlich machen und deren Macht quasi auf alle Nutzer verteilen können.

Dezentrale Technologien stellen die Daseinsberechtigung von zentralen Institutionen infrage. Allerdings sprechen der Blockchain-Technologie auch Banken, Unternehmen und sogar öffentliche Institutionen **großes Potenzial** zu. Diese sehen in der Blockchain Chancen, um eigene Prozesse effizienter zu gestalten, Kosten zu sparen und Arbeitsschritte zu automatisieren. Gerade in einer zunehmend digitalisierten Welt wird die Blockchain Technologie in unzähligen Einsatzgebieten Anwendung finden.

Der derzeitige Entwicklungsstand von Kryptowährungen lässt eine **Verdrängung** von konventionellen Währungen nach aktuellem Stand **unwahrscheinlich** erscheinen. Die Technologie ist noch zu unausgereift und ermöglicht es derzeit nicht, die Funktionen einer Zentralbank ersetzen zu können. Mittlerweile gibt es jedoch viele Kryptowährungen, die innovative Lösungsansätze für vereinzelte Probleme des Bitcoins vorstellen. Bei stetiger Forschung und Weiterentwicklung könnte es in Zukunft durchaus eine Kryptowährung geben, welche sich zumindest als **Parallelwährung** neben den herkömmlichen Währungen etablieren könnte. Bei ausreichender Akzeptanz könnte dann jeder selbst entscheiden, ob er dem Ideal dezentraler Systeme folgen möchte oder weiterhin einer zentralen Institution vertrauen will. Inwiefern dies Realität werden kann, wird allein die Zukunft zeigen.

Anlagenverzeichnis

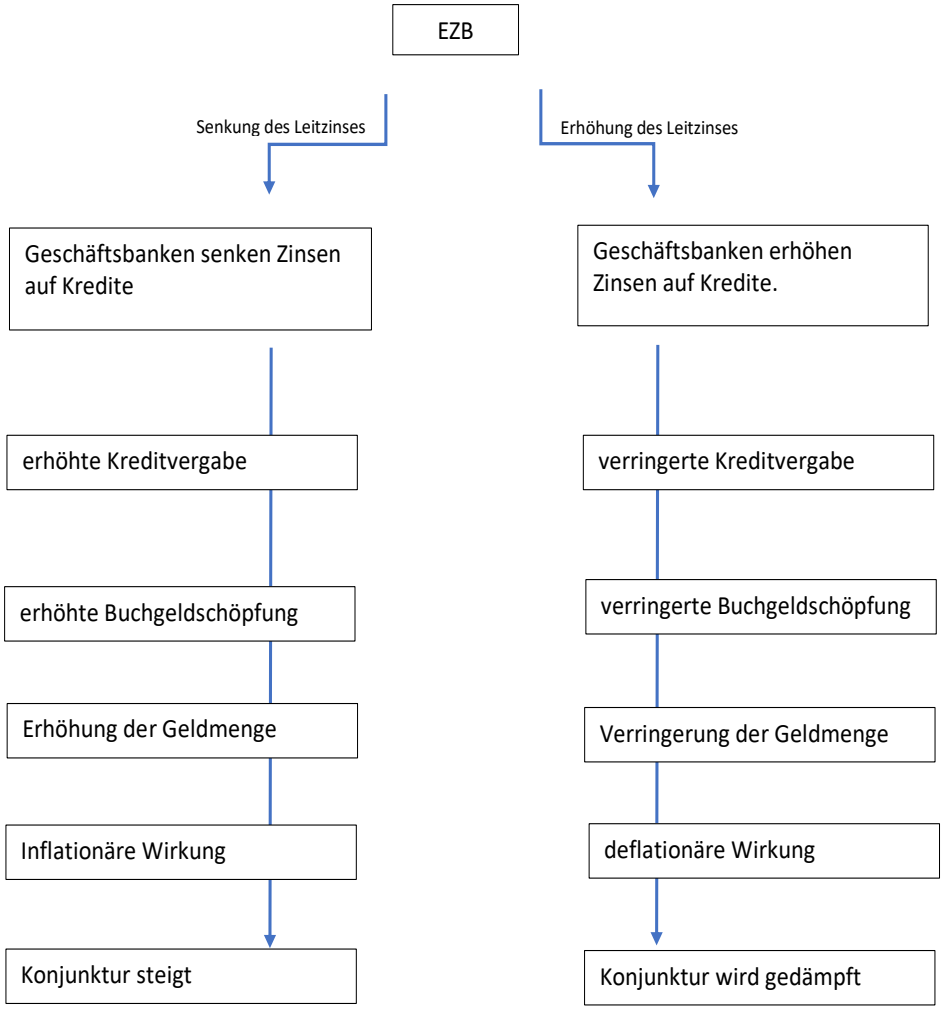
Anlage 1: Geldpolitik der EZB

Anlage 2: Blöcke in einer Blockchain

Anlage 3: Eine „Bitcoin-Farm“

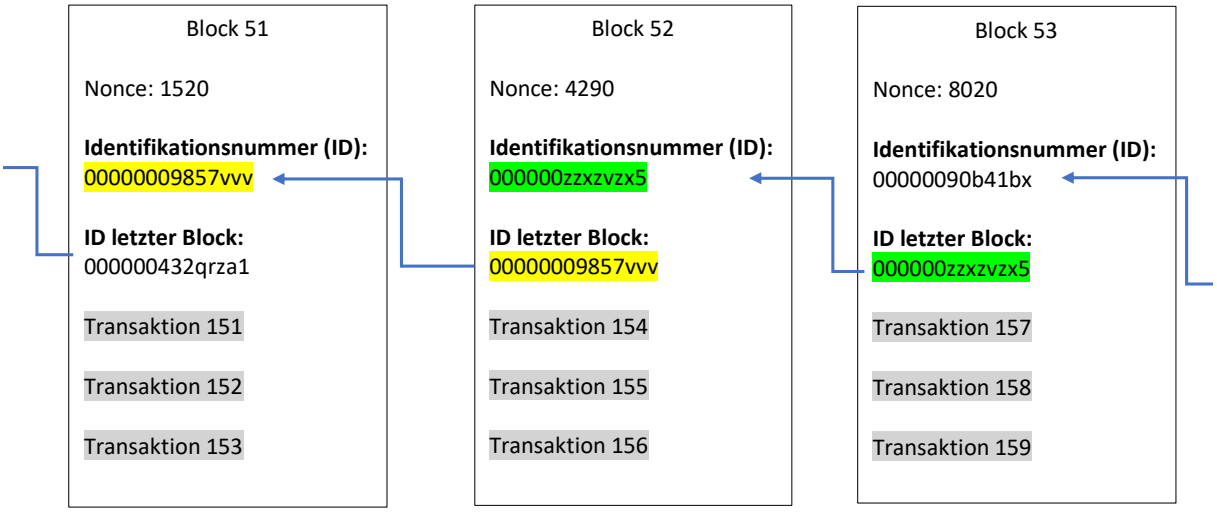
Anlage 4: Teilbarkeit des Bitcoins

Anlage 1: Geldpolitik der EZB[271]



[271] Selbst erstelltes Schema, vereinfachte Darstellung der Mechanismen der Geldpolitik, basierend auf dem Inhalt eines Lehrvideos der Europäischen Zentralbank zur Geldpolitik URL: *https://www.youtube.com/watch?v=WAlccQvkni8* , abgerufen am 20.01.2019, 15:40 Uhr.

Anlage 2: Blöcke einer Blockchain[272]



[272] Eigene Darstellung: Abbildung angelehnt aus: Platzer, Jörg 2014, S. 21, ergänzt um die *Nonce und die Transaktions ID.*

Anlage 3: Eine *Bitcoin-Farm*[273]

[273] Bildquelle: *https://www.slavorum.org/largest-bitcoin-farm-in-russia-earns-millions-of-dollars-each-month-on-a-secret-location/* , abgerufen am 04.01.2019, 17:00 Uhr.

Anlage 4: Teilbarkeit des Bitcoins[274]

Subeinheit	**In Bitcoin Einheiten**
1 Bitcoin	1 Bitcoin
1 Deci-Bitcoin	0,1 Bitcoin
1 Centi-Bitcoin	0,01 Bitcoin
1 Milli-Bitcoin	0,001 Bitcoin
1 Micro-Bitcoin (Bit)	0,000001 Bitcoin
1 Satoshi	0,00000001 Bitcoin

[274] Tabelle übernommen aus Berentsen, Aleksander ; Schär, Fabian 2017, S. 273.

Literaturverzeichnis

Bücher:

Berentsen, Aleksander ; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets. 1. Aufl. Norderstedt : Books on Demand, 2017

Bontrup, Heinz – Josef: Volkswirtschaftslehre: Grundlagen der Mikro- und Makroökonomie. 2., unwesentlich veränderte Aufl. München : Oldenbourg, 2004

Drescher, Daniel: Blockchain Grundlagen: Eine Einführung in die elementaren Konzepte in 25 Schritten. 1. Aufl. Frechen : mitp, 2017

Engelkamp, Paul ; Sell, L. Friedrich: Einführung in die Volkswirtschaftslehre. 7., ergänzte und aktualisierte Auflage. Berlin : Springer Gabler, 2017

Gerdesmeier, Dieter: Geldtheorie und Geldpolitik: Eine praxisorientierte Einführung. 1. Aufl. Frankfurt am Main : Bankakad, 2004

Hewel, Brigitte ; Lenk, Thomas ; Neubäumer, Renate: Volkswirtschaftslehre: Grundlagen der Volkswirtschaftstheorie und Volkswirtschaftspolitik. 6. Aufl. Wiesbaden : Springer Gabler, 2017

Hosp, Julian: Blockchain 2.0: einfach erklärt – mehr als nur Bitcoin. 1. Aufl. München : Finanzbuch Verlag, 2018

Hosp, Julian: Kryptowährungen: Bitcoin, Ethereum, Blockchain, ICO's & Co. einfach erklärt. 1. Aufl. Hongkong : Julian Hosp Coaching, 2017

Issing, Otmar: Einführung in die Geldtheorie. 15., wesentlich überarbeitete Aufl. München : Vahlen, 2011

Müller, Dirk: Crashkurs: Weltwirtschaftskrise oder Jahrhundertchance? Wie Sie das Beste aus Ihrem Geld machen. überarbeitete, aktualisierte und erweiterte Taschenbuchausgabe. München : Knaur, 2010

Platzer, Joerg: Bitcoin: kurz & gut: Banking ohne Banken. 1. Aufl. Köln : O'Reilly, 2014

Sixt, Elfriede: Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie. Wiesbaden : Springer Gabler, 2017

Spahn, Heinz – Peter: Geldpolitik: Finanzmärkte, neue Makroökonomie und zinspolitische Strategien. 2., überarbeitete Aufl. München : Vahlen, 2009

Digitale Literatur:

Badek, Bianca ; Nguyen, Tristan: Ursachen der Immobilienkrise in den USA. In: Schriften der Wissenschaftlichen Hochschule Lahr. Nr. 25, Jg. 8. Lahr : WHL Wissenschaftliche Hochschule Lahr. 2010. URL: *https://www.econstor.eu/bitstream/10419/175126/1/ifosd-v70-2017-i22-p03-20.pdf*

Brühl, Volker: Bitcoin und andere Kryptowährungen – konsequente Regulierung und Aufsicht sind dringend geboten. In: ifo Schnelldienst. Nr. 22, Jg. 70. München : ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München, vom 23. November 2017, S. 13 - 16. URL: *https://www.econstor.eu/bitstream/10419/175126/1/ifosd-v70-2017-i22-p03-20.pdf*

Commerzbank (Hrsg.): Preis- und Leistungsvergleich. Frankfurt am Main : Commerzbank. Stand 1. März 2019. URL: *https://www.commerzbank.de/portal/de/footer1/preisekonditionen/preisekonditionen.html*

De Vries, Alex: Bitcoin's Growing Energy Problem. In: Joule. Nr. 5, Jg. 2. Amsterdam : Elsevier, vom 16. Mai 2018, S. 801 – 804. URL: *https://clickonyx.co.uk/wp-content/uploads/2018/05/PIIS2542435118301776.pdf*

Deutsche Bundesbank (Hrsg.): Geld und Geldpolitik. Frankfurt am Main : Deutsche Bundesbank. Frühjahr 2017. URL: *https://www.bundesbank.de/resource/blob/606038/c0364dd6034eb7e0c9230b77ed995c06/mL/geld-und-geldpolitik-data.pdf*

Deutsche Bundesbank (Hrsg.): Monatsbericht September 2017. In: Monatsbericht September 2017. Nr. 9, Jg. 69. Frankfurt am Main : Deutsche Bundesbank, vom 15. September 2017. URL: *https://www.bundesbank.de/resource/blob/665470/02abccf09b7ebf3c9635b89405ead7e7/mL/2017-09-monatsbericht-data.pdf*

Diehl, Martin ; Thiele, Carl-Ludwig: Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten? In: ifo Schnelldienst. Nr. 22, Jg. 70. München : ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München, vom 23. November 2017, S. 3 - 6. URL: *https://www.econstor.eu/bitstream/10419/175126/1/ifosd-v70-2017-i22-p03-20.pdf*

Elsner, Dirk ; Pecksen, Gerrit: Kryptowährungen sind noch nicht reif für eine weitreichende Umsetzung. In: ifo Schnelldienst. Nr. 22, Jg. 70. München : ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München, vom 23. November 2017, S. 10 - 12. URL: *https://www.econstor.eu/bitstream/10419/175126/1/ifosd-v70-2017-i22-p03-20.pdf*

Europol (Hrsg.): The Internet Organised Crime Threat Assessment (IOCTA). Den Haag : European Law Enforcement Agency. 2015. URL: *https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2015.pdf*

Geiling, Luisa: Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain. In: Bafin Journal. Nr. 2, Jg. 10. Bonn, Frankfurt am Main : Mitteilungen der Bundesanstalt für Finanzdienstleitungsaufsicht, vom 15.02.2016, S. 28 – 32. URL: *http://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2016/bj_1602.pdf?__blob=publicationFile&v=3*

Hummel, Philipp: Quantencomputer: Kommt der Durchbruch in Deutschland? In: Spektrum der Wissenschaft – die Woche. Nr. 50, Jg. 41. Heidelberg : Spektrum der Wissenschaft, vom 13.12.2018, S. 43 – 48. URL: *https://shop.spektrum.de/index.php?cl=basket&anid=be475152c5a9028c1e9caba85b2e6536&listtype=list&*

Krohn-Grimberghe, Artus ; Sorge, Christoph: Bitcoin: das Zahlungsmittel der Zukunft? In: Wirtschaftsdienst, Nr. 10, Jg. 93. Berlin, Heidelberg : Springer Berlin Heidelberg, vom 15. Oktober 2013, S. 720 - 722. URL: *https://link.springer.com/article/10.1007/s10273-013-1589-y*

Mayer, Thomas: Die Evolution des Geldes. In: ifo Schnelldienst. Nr. 22, Jg. 70. München : ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München, vom 23. November 2017, S. 7 – 9. URL: *https://www.econstor.eu/bitstream/10419/175126/1/ifosd-v70-2017-i22-p03-20.pdf*

Michaelis, Jochen: Die Konkurrenz umarmen: Digitales Zentralbankgeld. In: ifo Schnelldienst. Nr. 22, Jg. 70. München : Ifo. ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München, vom 23. November 2017, S. 17 – 20. URL: *https://www.econstor.eu/bitstream/10419/175126/1/ifosd-v70-2017-i22-p03-20.pdf*

Naser, Rainer, Dr.: Wie kommt das Geld in die Welt? In: Wochenschau, Politik und Wirtschaft im Unterricht. Sonderausgabe, Jg. 69. Frankfurt am Main : Wochenschau Verlag. August 2018, S. 18 – 27. URL: *https://www.bundesbank.de/resource/blob/759192/ec39b74903cc68ef9d7743b6337ea453/mL/wochenschau-sonderausgabe-data.pdf*

Rosenberger, Patrick: Bitcoin und Blockchain: Vom Scheitern einer Ideologie und dem Erfolg einer Revolutionären Technik. Berlin, Heidelberg : Springer Berlin Heidelberg. 2018. URL: *https://link.springer.com/book/10.1007%2F978-3-662-56088-4*

Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. URL: *https://bitcoin.org/bitcoin.pdf*

Seiler, Benedikt ; Seiler, Daniel: Sind Kryptowährungen wie Bitcoin (BTC), Ethereum (ETH) und Ripple (XRP) als Sachen im Sinne des ZGB zu behandeln? In: sui generis. Nr.65, Jg. 5. Basel : sui generis. 2018. S. 149-163. URL: *https://edoc.unibas.ch/64047/1/20180508112949_5af16e0dd5198.pdf*

Internetquellen:

Börse ARD (Hrsg.): Volatilität. URL: *https://boerse.ard.de/boersenwissen/boersenlexikon/volatilitaet-100.html* , abgerufen am 06.02.2019, 17:45 Uhr

Bude, Matthias ; Kaufmann, Sabine: Finanzkrise 2008, URL: *https://www.planet-wissen.de/gesellschaft/wirtschaft/boerse/pwiefinanzkrise100.html* , abgerufen am 22.01.2019, 19:04 Uhr

De Souza Soares, Philipp Alvares: Wettlauf um den Quantencomputer: Das nächste große Ding. Spiegel Online Artikel. URL: *http://www.spiegel.de/netzwelt/web/quantencomputer-die-naechste-dimension-der-it-a-1109142.html* , abgerufen am 08.02.2019, 19:25 Uhr

Deutsche Bundesbank (Hrsg.): Mindestreserven. URL: *https://www.bundesbank.de/de/aufgaben/geldpolitik/mindestreserven* , abgerufen am 19.01.2019, 18:13 Uhr

Dittmer, Diana: Ist Cybergeld vor allem was für Kriminelle? Spiegel Online. URL: *https://www.n-tv.de/wirtschaft/Ist-Cybergeld-vor-allem-was-fuer-Kriminelle-article20143681.html* , abgerufen am 01.02.2019, 18:20 Uhr

Europäische Zentralbank (Hrsg.): Was ist Seigniorage? URL: *https://www.ecb.europa.eu/explainers/tell-me/html/seigniorage.de.html* , abgerufen am 18.02.2019, 16:45 Uhr

Filipp, Stefan: Quantencomputer: Der Beginn der kommerziellen Quanten-Ära. IBM Dach Blog Artikel. URL: *https://www.ibm.com/de-de/blogs/think/2018/02/23/quantencomputer/* , abgerufen am 08.02.2019, 19:40 Uhr

Fuest, Benedikt: Dieser Computerchip könnte Bitcoin und Co. wertlos machen. URL: *https://www.welt.de/wirtschaft/webwelt/article174393767/Quanten-Computer-Wie-Superchips-Bitcoin-und-Co-wertlos-machen-koennten.html* , abgerufen am 11.03.2019, 16:00 Uhr

Gerginov, David: Geldpolitik: Definition, Wirkung und Ziel. Verlag für die Deutsche Wirtschaft AG. URL: *https://www.gevestor.de/details/geldpolitik-definition-wirkung-und-ziel-652473.html* , abgerufen am 20.01.2019, 14:45 Uhr

Hannich, Günter: Wechselkurse: Darum sind sie so wichtig. Crash Investor Artikel. URL: *https://crash-investor.de/wechselkurse-darum-sind-sie-so-wichtig/* , abgerufen am 20.02.2019, 20:40 Uhr

Hecking, Claus: "Das Bitcoin-System verbraucht mehr Strom als die Schweizer Volkswirtschaft". Spiegel Online Interview, vom 22.05.2018. URL: *http://www.spiegel.de/wirtschaft/unternehmen/bitcoin-energieverbrauch-fuer-produktion-und-verwaltung-a-1208635.html* , abgerufen am 04.02.2019, 18:50 Uhr

o. V.: Bitcoin Akzeptanzstellen. Investoren Journal. URL: *https://www.investoren-journal.com/bitcoin-akzeptanzstellen/* , abgerufen am 11.02.2019, 18:50 Uhr

o. V.: Bitcoin Block Reward Halving Countdown. URL: *https://www.bitcoinblockhalf.com* , abgerufen am 23.01.2019, 19:34 Uhr

o. V.: Der Bitcoin-Volatilitätsindex. URL: *https://www.buybitcoinworldwide.com/de/volatilitatsindex/* , abgerufen am 09.03.2019, 16:25 Uhr

o. V.: Download Bitcoin Core. URL: *https://bitcoin.org/de/download* , abgerufen am 25.12.2018, 16:00 Uhr

o. V.: Largest Bitcoin Farm In Russia Earns Millions Of Dollars Each Month On A Secret Location. URL: *https://www.slavorum.org/largest-bitcoin-farm-in-russia-earns-millions-of-dollars-each-month-on-a-secret-location/* , abgerufen am 04.01.2019, 17:00 Uhr

o. V.: Litecoin Details – Mehr über Litecoin erfahren. URL: *https://www.coinwelt.de/2014/12/litecoin-details/* , abgerufen am 23.01.2019, 18:50 Uhr

o. V.: Live aktualisierte Liste der aktuellen Bitcoin Transaktionen. URL: *https://www.blockchain.com/de/btc/unconfirmed-transactions* , abgerufen am 30.01.2019, 17:40 Uhr

o. V.: Wechselkurs Bitcoin / Euro. Tagestief 13.02.2019. Finanzen.net. URL: *https://www.finanzen.net/devisen/bitcoin-euro-kurs/historisch* , abgerufen am 09.03.2019, 17:00 Uhr

Reuters (Hrsg.): Südkorea: Hacker greifen Krypto-Börse Coinrail an. Spiegel Online Artikel, vom 11.06.2018. URL: *http://www.spiegel.de/netzwelt/web/coinrail-aus-suedkorea-hacker-greifen-krypto-boerse-an-a-1212322.html* , abgerufen am 28.02.2019, 19:25 Uhr

Schlupeck, Bernd: Quantencomputer: Fortschritte in der Forschung. Deutschlandfunk Online-Artikel. URL: *https://www.deutschlandfunk.de/quantencomputer-fortschritte-in-der-forschung.676.de.html?dram:article_id=417034* , abgerufen am 08.02.2019, 19:30 Uhr

Statista (Hrsg.): Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2018 (in Millionen). URL: *https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/* , abgerufen am 11.02.2019, 19:50 Uhr

Statista (Hrsg.): Umfrage in Deutschland zur Zahlungsbereitschaft mit Kryptowährungen (BitCoin) 2017. URL: *https://de.statista.com/statistik/daten/studie/742385/umfrage/umfrage-in-deutschland-zur-zahlungsbereitschaft-mit-kryptowaehrungen-bitcoin/* , abgerufen am 11.02.2019, 18:50 Uhr

Thellman, Pascal: Bitcoin's Next Halving Rally: Coming Soon in 2019. URL: *https://www.coindesk.com/bitcoins-next-halving-rally-coming-soon-in-2019* , abgerufen am 23.01.2019, 19:45 Uhr

Wagner, Niklas: Nächstes Bitcoin (BTC)-Halving könnte schon dieses Jahr für Preisanstieg sorgen. URL: *https://coinkurier.de/halving/* , abgerufen am 23.01.2019, 19:38 Uhr

Audiovisuelle Informationsquellen:

Europäische Zentralbank (Urh.): Preisstabilität: Warum ist sie für dich wichtig? Video 8:17 Min. 2005. URL: *https://www.youtube.com/watch?v=WAlccQvkni8* , abgerufen am 20.01.2019, 15:40 Uhr

Rechtsquellenverzeichnis

Gesetz über die Deutsche Bundesbank (BBankG) in der Fassung der Bekanntmachung vom 22. Oktober 1992 (BGBl. I S. 1782), zuletzt geändert durch Artikel 23 des Gesetzes vom 4. Juli 2013 (BGBl. I S. 1981)

Vertrag über die Arbeitsweise der Europäischen Union (AEUV) in der Fassung aufgrund des am 1.12.2009 in Kraft getretenen Vertrages von Lissabon, zuletzt geändert durch die Akte über die Bedingungen des Beitritts der Republik Kroatien und die Anpassungen des Vertrags über die Europäische Union, des Vertrags über die Arbeitsweise der Europäischen Union und des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. EU L 112/21 vom 24.4.2012) mit Wirkung vom 1.7.2013

Eidesstattliche Versicherung

Ich versichere hiermit an Eides Statt, dass ich die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die gedruckte und digitalisierte Version der wissenschaftlichen Abschlussarbeit sind identisch.

Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Die gedruckte und die digitalisierte Form der Diplomarbeit sind identisch.

Sangerhausen,