

Bitcoin – Hype oder Währung?

Eine Random-Walk-Analyse anhand von Renditezeitreihen

Bachelorarbeit

Institutsdirektor: Prof. Dr. Claudio Loderer

Betreuender Assistent: Oliver Dichter, M Sc Ec

Verfasser: Ozan Harman

Zürich

E-Mail on.harman@gmail.com

Bern, 12. September 2014

Disclaimer:

Die in der vorliegenden Arbeit vertretenen Ansichten sind diejenigen des Verfassers und nicht notwendigerweise die Ansichten des Instituts für Finanzmanagement. Das Institut für Finanzmanagement übernimmt keine Verantwortung für allfällige Fehler.

I. Executive Summary

Diese Arbeit hat zum Ziel, die Funktionsweise der Kryptowährung Bitcoin zu analysieren, damit verbundene Chancen und Gefahren aufzuzeigen sowie zu untersuchen, inwiefern Bitcoin als Währung geeignet ist. Des Weiteren wird im Rahmen der Effizienzmarkthypothese empirisch überprüft, ob Bitcoin-Renditen einem Random-Walk folgen. Anhand des Testergebnisses wird überprüft, ob der Bitcoin-Markt schwach informationseffizient ist.

Eines der ersten Themen, die Robert Shiller am Weltwirtschaftsforum 2014 in Davos aufgeworfen hat, war Bitcoin. Er erklärte, dass Bitcoin ein verblüffendes Beispiel einer Spekulationsblase ist [vgl. Weisenthal (2014)]. Als Verfechter des Behavioral-Finance ist Shiller der Auffassung, dass Marktpreise von psychologischen Attributen geprägt werden. Wirtschaftlich irrationales Verhalten übt dabei massgeblichen Einfluss aus. Eugene Fama, der die Effizienzmarkthypothese aufgestellt hat, bezweifelt, dass Spekulationsblasen auf effizienten Märkten existieren. Fama begründet unter Annahme der Effizienzmarkthypothese, dass weder Preise, noch Spekulationsblasen vorhersehbar sind. Unter Annahme eines effizienten Marktes sind Spekulationsblasen lediglich zufällige Abweichungen vom tatsächlichen Preis [vgl. Cassidy (2010)].

Ferner ist durch das Wachstum von Kryptowährungen und insbesondere Bitcoins, nicht auszuschliessen, dass Kryptowährungen Teil internationaler Finanzmärkte werden könnten. Bereits jetzt hat Bloomberg, einer der grössten Anbieter für Finanzinformationen, Bitcoins in die Bloomberg Professional Datenbank aufgenommen [vgl. Van (2014)]. Es ist jedoch auch zu erwähnen, dass Kryptowährungen ein Risiko für Fiat-Währungen darstellen könnten, falls die Benutzung von Kryptowährungen stark ansteigen sollte [vgl. Europäische Zentralbank (2012)].

Die Analyse zeigt, dass sich Bitcoin zurzeit nicht als Währung im konventionellen Sinn eignet, da Bitcoin zu unsicher ist und hohe Kursschwankungen, Wertstabilität verhindern. Auch wird im Rahmen der empirischen Analyse gezeigt, dass Bitcoin-Renditezeitreihen bisher einem Random-Walk gefolgt sind und nicht prognostizierbar sind. Die Ergebnisse stehen nicht im Widerspruch zu Shillers oder Famas Aussagen. Spekulationsblasen können im Zusammenhang mit Bitcoin nicht ausgeschlossen werden, es können jedoch auch keine Prognosen anhand von Renditezeitreihen gemacht werden.

Für die zukünftige Forschung eignet sich Bitcoin aufgrund der Datenfülle sehr gut zur Untersuchung der Markteffizienz und bietet Raum für Erkenntnisse im Hinblick auf elektronisches Geld.

II. Inhaltsverzeichnis

I.	Executive Summary	I
II.	Inhaltsverzeichnis	III
III.	Tabellenverzeichnis	V
IV.	Abbildungsverzeichnis	V
V.	Abkürzungsverzeichnis	V
1.	Einleitung.....	6
1.1	Ausgangslage	6
1.2	Zielsetzung und Relevanz	7
1.3	Methodik und Aufbau	8
2.	Theorie.....	9
2.1	Was sind Kryptowährungen?.....	9
2.2	Was ist Bitcoin?	10
2.2.1	Byzantinische Generäle und Bitcoins	11
2.2.2	Entstehung von Bitcoins.....	12
2.2.3	Aneignung von Bitcoins.....	13
2.2.4	Kritische Einordnung	13
2.2.5	Ist Bitcoin eine Währung?	15
2.3	Märkte.....	17
2.3.1	Markt für Kryptowährungen	18
2.3.2	Markt für Bitcoins	21
2.4	Finanzmarkttheorie	26
2.4.1	Einführung.....	26
2.4.2	Bitcoin und die Finanzmarkttheorie	29
2.4.3	Die Effizienzmarkthypothese	31
2.4.4	Random-Walk-Hypothese	33
2.4.5	Random-Walk ₁ -Tests	34

3.	Empirischer Teil	35
3.1	Folgen Renditen von Bitcoins einem Random-Walk?	35
3.2	Daten	35
3.3	Methoden	37
3.3.1	Regressionsanalyse	38
3.3.2	Run-Test	38
3.4	Ergebnisse	39
3.4.1	Regressionsanalyse	39
3.4.2	Run-Test	39
4.	Schluss	40
5.	Anhang.....	41
6.	Literaturverzeichnis	44
	Selbständigkeitserklärung	50

III. Tabellenverzeichnis

Tabelle 1: Geldmatrix [eigene Tabelle in Anlehnung an Europäische Zentralbank (2012)]	9
Tabelle 2: Einordnung verschiedener Wertträger [eigene Tabelle in Anlehnung an Ametrano (2014)] ...	15

IV. Abbildungsverzeichnis

Abbildung 1: Volatilität verschiedener Wertträger im Vergleich [eigene Abbildung in Anlehnung an Ametrano (2014)]	17
Abbildung 2: Marktkapitalisierung von Kryptowährungen [eigene Abbildung]	20
Abbildung 3: Die Blockchain als Informationszentrale [eigene Abbildung]	21
Abbildung 4: Marktkapitalisierung von BTC [eigene Abbildung]	22
Abbildung 5: Historische Volatilität BTC [eigene Abbildung]	23
Abbildung 6: Theorie rationaler Erwartungen [eigene Abbildung in Anlehnung an Muth (1961)]	27
Abbildung 7: Preisreaktion auf neue Information [eigene Abbildung in Anlehnung an Ross et al. (2002), S. 344]	31
Abbildung 8: Grade der Markteffizienz [eigene Abbildung in Anlehnung an Fama und Malkiel (1970)] ..	32

V. Abkürzungsverzeichnis

<i>BF:</i>	Behavioral-Finance
<i>BIC:</i>	Bayessches-Informationskriterium
<i>BPI:</i>	Bitcoin-Preis-Index
<i>BTC:</i>	Bitcoin
<i>EMH:</i>	Effizienzmarkthypothese
<i>logRendite:</i>	logarithmierte Rendite
<i>RW:</i>	Random-Walk
<i>RWH:</i>	Random-Walk-Hypothese
<i>USD:</i>	United States Dollar

1. Einleitung

1.1 Ausgangslage

Als Milton Friedman in einem Interview mit der National Taxpayers Union die Entstehung von E-Cash, auch sogenannten Kryptowährungen, prognostiziert hat, ahnte wohl kaum jemand, dass sich diese Prognose bewahrheiten würde [vgl. Berthoud und Friedman (1999)]. Friedman (1999) beschrieb eine Währung, die es den Akteuren erlaubt, Überweisungen anonym über das Internet zu tätigen. Diese Beschreibung trifft weitgehend auf sogenannte Kryptowährungen zu. Die populärste Kryptowährung nennt sich Bitcoin (BTC), wurde 2009 geschaffen und erweckt seither das Interesse verschiedenster Wirtschaftsakteure. In diversen Industriestaaten wird darüber diskutiert, wie BTC rechtlich gehandhabt werden soll [vgl. Europäische Zentralbank (2012)]. Experten wie etwa Paul Krugman (2014) warnen davor, dass BTC, aufgrund der Anonymität der Transaktionspartner, für illegale Aktivitäten förderlich sei und die hohe Volatilität zu grossen Verlustrisiken führe.

In naher Vergangenheit häuften sich Medienmitteilungen über Hackerangriffe und Sicherheitslücken im Zusammenhang mit der grössten BTC-Wechselstube Mt.Gox. Am 7. Februar 2014 blockierte Mt.Gox Transaktionen in und aus der Wechselstube. Noch im selben Monat wurde die Internetseite des Dienstleisters gelöscht. Im Vorfeld waren die Handelsblockade auf Mt.Gox und die Unsicherheit bei den Nutzern Grund für Kursunterschiede von bis zu 400 Prozent zwischen dem Bitcoin-Preis-Index (BPI)¹ und dem auf Mt.Gox notierten Kurs.

Durch das wachsende Volumen von Kryptowährungen sowie deren Ähnlichkeit zu traditioneller Währung ist nicht auszuschliessen, dass in naher Zukunft Kryptowährungen Teil internationaler Finanzmärkte werden könnten [vgl. Europäische Zentralbank (2012)]. Bloomberg, einer der grössten Anbieter für Finanzinformationen, nahm am 30. April 2014 BTC in die Bloomberg Professional Datenbank auf [vgl. Van (2014)]. Dennoch scheuen sich grössere Finanzinstitutionen davor, in BTC zu investieren. Als Gründe dafür werden mangelnde Liquidität, strukturelle Instabilität, Unsicherheit und fehlende Gesetzesgrundlagen genannt [vgl. Mataro (2014)]. Die geringe Liquidität², hohe Volatilität³ und der spekulative Charakter⁴ des BTC-Marktes könnten das Resultat von Marktineffizienz sein. Nach Shiller (2014) war es

¹ Siehe Kapitel 3.2

² Vgl. Chung und Hrazdil (2010)

³ Vgl. Shiller (1981)

⁴ Vgl. Weisenthal (2014)

bereits vor dem Zusammenbruch von Mt.Gox klar, dass BTC eine Spekulationsblase ist. Dem ist anzufügen, dass nach Fama, ein Verfechter der Effizienzmarkthypothese (EMH), die Existenz von Spekulationsblasen auf effizienten Märkten grundsätzlich zu hinterfragen ist, da diese nicht prognostizierbar sind [vgl. Cassidy (2010)]. Selbst wenn BTC eine Spekulationsblase sein sollte, stellt sich die Frage, zu welchem Grad der BTC-Markt die Bedingungen der EMH erfüllt.

1.2 Zielsetzung und Relevanz

Das Ziel dieser Arbeit ist, die Funktionsweise von BTC zu analysieren, Chancen und Gefahren aufzuzeigen und zu untersuchen inwiefern BTC als Währung geeignet ist. Des Weiteren wird im Rahmen der EMH empirisch überprüft, ob BTC-Renditen einem Random-Walk (RW) folgen. Das Testergebnis ermöglicht die Beurteilung der schwachen Informationseffizienz des BTC-Marktes.

virtuelle Währungen haben das Wirtschaftsgeschehen bislang nur marginal beeinflusst. Der Handel mit diesen neuartigen Wertträgern hat sich bisher auf die Währungen des Typs Eins und Zwei¹ beschränkt. Somit beschränkte sich deren Geltungsbereich nur auf von Onlinespielen und die virtuelle Realität [vgl. Bartle (2004)]. Mit der Entstehung von Bitcoin und damit des Währungstyps Drei wurden diese Grenzen aufgehoben. Heute wird auf diversen Handelsplattformen mit Kryptowährungen gehandelt. Der Markt für Kryptowährungen wächst täglich, gewinnt neue Teilnehmer und ist Treffpunkt für Spekulanten, Kriminelle, Technikbegeisterte und Freidenker.

BTC hat mit 93 Prozent den grössten Anteil am Markt für Kryptowährungen und konnte sich erfolgreich gegen andere Kryptowährungen durchsetzen. Es ist jedoch anzufügen, dass auch BTC von einer hohen Volatilität geprägt ist und Chancen und Gefahren existieren, wie sie bei bewährten Fiat-Währungen nicht vorkommen. Das Abtauchen der grössten BTC-Wechselstube Mt.Gox und der damit verbundene Preiszusammensturz ist ein weiteres Beispiel dafür, wie instabil BTC ist. Sollte die Benutzung von Kryptowährungen signifikant ansteigen, so könnte dies, laut einem Bericht der Europäischen Zentralbank (2012), ein Risiko für Fiat-Währungen darstellen.

¹ siehe Kapitel 2.1

1.3 Methodik und Aufbau

Die vorliegende Arbeit ist in einen theoretischen und einen empirischen Teil gegliedert. Im Theorieteil wird zunächst (Kapitel 2.1) analysiert, inwiefern Kryptowährungen sich von gängigen elektronischen Zahlungsmitteln unterscheiden und wie diese einzuordnen sind. Dies ist wichtig, um ein allgemeines Verständnis im Zusammenhang mit Kryptowährungen zu ermöglichen. Im Kapitel 2.2 wird die Funktionsweise von BTC analysiert und Chancen und Gefahren kritisch eingeordnet, um anschliessend zu untersuchen, inwiefern BTC die Funktionen einer Währung – als Zahlungsmittel, Wertaufbewahrungsmittel und Recheneinheit – erfüllt [vgl. Krugman (1984)]. Kapitel 2.3 bietet einen Ausblick auf BTC im Zusammenhang mit Finanzmärkten, einen Überblick des Marktes für Kryptowährungen und eine deskriptiv-konzeptionelle Analyse des BTC-Marktes. Kapitel 2.4 widmet sich der Finanzmarkttheorie im Allgemeinen und im Hinblick auf BTC. Ferner dient dieses Kapitel als theoretische Basis für den Empirischen Teil. Die Random-Walk-Hypothese (RWH) und der Run-Test sind weitere Bestandteile des Kapitels 2.4.

Der empirische Teil beginnt mit einer Einleitung, in welcher die Relevanz der empirischen Untersuchung aufgezeigt wird (Kapitel 3.1). Im Kapitel 3.2 wird überprüft, welche Preisdaten zur Analyse geeignet sind. Dabei wird der BPI ausgewählt, weil dieser die Rahmenbedingungen der Datenqualität bezüglich Verfügbarkeit, Interpretierbarkeit, Relevanz und Zuverlässigkeit erfüllt [vgl. Wang et al. (1995)]. Im Kapitel 3.3 werden das methodische Vorgehen und die statistischen Analyseverfahren beschrieben. Als Analyseverfahren wurden die robuste Regressionsanalyse (parametrisch) und der Run-Test (nichtparametrisch) verwendet. Danach werden im Kapitel 3.4 die Ergebnisse vorgestellt. Im Schlussteil werden die Ergebnisse bewertet und interpretiert, um die Frage zu beantworten, ob BTC-Renditen einem Random-Walk folgen und ob von einer schwachen Informationseffizienz ausgegangen werden kann. Zudem werden im Frageb für die zukünftige Forschung aufgeworfen.

Im empirischen Teil wurde getestet, ob BTC-Renditezeitreihen einem Random-Walk folgen. Anhand der robusten Regressionsanalyse wird überprüft ob Renditezeitreihen seriell korreliert sind. Der Run-Test dient dazu zu überprüfen ob Sequenzen positiver/negativer Renditen zufällig sind.

2. Theorie

2.1 Was sind Kryptowährungen?

Kryptowährungen sind eine Untergruppe der virtuellen Währungen. Sie sind im Allgemeinen unabhängig von Zentralbanken und unterliegen keiner gesetzlichen Regulierung. Ausserdem erfolgen Transaktionsverifizierung und Mengenregulierung auf Basis verschiedener digitaler Verschlüsselungsalgorithmen [vgl. Stevenson und Lindberg (2010)].

Legaler Status	Nicht reguliert	<i>Gewisse Arten von Regionalwährung</i>	<i>virtuelle Währung</i>	Typ 1	Geschlossene Gemeinschaft
				Typ 2	Unidirektionale Währung
				Typ 3	Bidirektional (Kryptowährung)
	Reguliert	<i>Banknoten und Münzen</i>	<i>-elektronisches Geld -Geschäftsbank Geld (Deposite)</i>		
		Physisch	Digital		
		Format			

Tabelle 1: Geldmatrix [eigene Tabelle in Anlehnung an Europäische Zentralbank (2012)]

Die obige Tabelle dient lediglich zur Übersicht der momentanen Situation, da es sich bei virtuellen Währungen um eine neuartige Form von Wertträgern handelt und grosse Veränderungen, beispielsweise in Bezug auf den legalen Status, zu erwarten sind. Zusätzlich ist klarzustellen, dass virtuelle Währungen die Eigenschaft teilen, keinen physischen Konterpart zu besitzen. elektronisches Geld hingegen ist an eine staatlich anerkannte Währung gebunden. Eine Klassifikation der verschiedenen virtuellen Währungen ist aufgrund der Heterogenität nur bedingt möglich. Eine Möglichkeit ist die Unterscheidung auf Basis des Transaktionsflusses. Dieser Ansatz betrachtet erstens transaktionsbezogene Möglichkeiten der Währung und zweitens deren Verwendungszweck. In Zusammenhang mit BTC werden Kryptowährungen dem Typ Drei zugeteilt, weil einerseits Wechselkurse zu offiziellen Währungen bestehen und andererseits kontextunabhängig Güter und Dienstleistungen erworben werden können.

2.2 Was ist Bitcoin?

BTC ist zurzeit mit einer Marktkapitalisierung von ungefähr acht Milliarden USD die grösste, prominenteste und älteste Kryptowährung [vgl. CoinMKTCap (2014)]. Als Schöpfer der Währung gilt der unter dem Pseudonym⁶ bekannte Programmierer Satoshi Nakamoto (2008). Dieser hat 2009 ein Paper veröffentlicht, in welchem er den Grundgedanken und die Funktionsweise von BTC beschreibt und somit die Entstehung der Währung ermöglichte.

Sein Gedanke war es, eine Währung zu kreieren, die auf einem Peer-to-Peer-Netzwerk basiert. Durch dieses Netzwerk können Transaktionen zwischen Akteuren getätigt werden, ohne auf eine finanzielle Institution angewiesen zu sein. Akteure erscheinen dabei als sogenannte Peers, die durch die frei zugängliche BTC-Software miteinander verbunden sind und zusammen das BTC-Netzwerk bilden. Mithilfe der BTC-Software können Nutzer – ähnlich eines Bankkontos – eine digitale Wallet erstellen und mit dieser BTCs empfangen und versenden. Alle verifizierten Transaktionen werden in einem öffentlich zugänglichen Buchungssystem, der Blockchain⁷, abgespeichert. Das ermöglicht die Berechnung der Kontostände der einzelnen Wallets. Die Echtheit und chronologische Reihenfolge der Blockchain wird mithilfe kryptographischer Algorithmen sichergestellt. Um BTCs von einer Wallet zu senden, muss der Nutzer die Transaktion mit einem geheimen Private-Key signieren – anschliessend versendet die BTC-Software einen zugehörigen Public-Key an alle Miner. Eine Transaktion erfolgt nur dann, wenn anhand eines mathematischen Beweises nachgewiesen werden kann, dass die Signatur vom Besitzer der Wallet stammt.⁸ Der mathematische Beweis wird von Nutzercomputern des Netzwerkes erbracht. Nutzer, die ihre Rechenleistung für diesen Prozess zur Verfügung stellen, erscheinen hierbei als Miner. Mining ist ein verteiltes Konsens-System, bei dem der durch einen Miner erbrachte Beweis bezüglich einer Transaktion, von der absoluten Mehrheit der Miner verifiziert werden muss. Nach der Verifikation speichert die BTC-Software die Transaktion in der Blockchain und berechnet die neuen Beträge in den Wallets. Dieser Sicherheitsmechanismus ist eine zentrale Eigenschaft, die es BTC ermöglicht, das Problem doppelter Transaktionen zu lösen. Der folgende Abschnitt analysiert das Problem von doppelten Ausgaben im Zusammenhang mit digitalen Transaktionen.

⁶ Die wahre Identität Nakamotos ist nicht bekannt.

⁷ Für mehr Informationen bezüglich der Blockchain wird auf Abschnitt 2.3.2 verwiesen.

⁸ Dieser Beweis wird von sogenannten Minern erbracht. Der Prozess basiert auf der Proof-Of-Work-Methode.

2.2.1 Byzantinische Generäle und Bitcoins

Bisher hat kein digitales Tauschformat existiert, das ohne einer dritten Instanz funktionierte. Diese Drittinanz half bei der Vermeidung von, doppelten Transaktionen. Anbieter wie Paypal verhindern, anhand zentraler Buchführung doppelte Transaktionen. Eine denkbare Methode, um Drittinanzen zu umgehen, ist ein System, bei dem Wirtschaftssubjekte Geldbeträge als Datenpakete auf ihren Rechnern ablegen und diese bei Bedarf versenden. Bei dieser Variante besteht jedoch das Problem, dass Daten sich beliebig duplizieren lassen. Dies resultiert im Problem von doppelten Ausgaben. Wirtschaftssubjekt A kann ein Datenpaket, das einen Geldbetrag widerspiegelt, an Wirtschaftssubjekte B und C versenden, indem das Datenpaket dupliziert wird. Je nachdem wer das Datenpaket zuerst verwendet, zerfällt die Gültigkeit des Datenpaketes und damit des Duplikates. BTC löst dieses Problem, indem Transaktionen dem ganzen Peer-to-Peer-Netzwerk mitgeteilt werden. Die Überprüfung der Buchführung wird somit, anstelle einer zentralen Instanz, durch die gesamte Nutzergemeinschaft durchgeführt. Dies mündet jedoch im Problem des Byzantinischen Fehlers.

Der Begriff Byzantinischer Fehler stammt aus der Informatikwissenschaft und beruht auf der abstrahierten Darstellung des Konsensfindungsprozesses innerhalb verteilter Systeme. Das Modell beschreibt eine Gruppe byzantinischer Generäle, welche ihre Truppen, räumlich voneinander getrennt um eine feindliche Stadt platziert haben. Die Kommunikation beschränkt sich auf die verbale Übermittlung eines Boten. Ziel ist die Konsensfindung über einen gemeinsamen Angriffsplan, welcher jedoch verhindert wird, da sich Verräter unter den Generälen befinden [vgl. Leslie et al. (1982)]. Im Rahmen der Transaktionsverifizierung sind Miner mit demselben Problem konfrontiert. Zu bestätigende Transaktionen werden an das BTC-Netzwerk versendet. Miner empfangen die Transaktionsanfrage und überprüfen individuell, ob es sich um eine doppelte Transaktion handelt. Dies geschieht, indem jeder Miner anhand seiner Blockchain überprüft, ob die Transaktion buchhalterisch konsistent ist. Simultan zu dieser Überprüfung stellen Miner die Rechenleistung ihrer Computer zur Verfügung, um ein mathematisches Problem zu lösen. Das Problem wird anhand der Blockchain generiert und besitzt die Eigenschaften, schwer lösbar und leicht überprüfbar zu sein und hat ausserdem eine Lösungsmenge, die grösser als Eins ist. Ein Miner, der eine Lösung gefunden hat, versendet seine Lösung und die um die neue Transaktion erweiterte Version der Blockchain. Zu diesem Zeitpunkt kann es vorkommen, dass zwei Versionen der Blockchain im Netzwerk kursieren. Dies ist vergleichbar mit der Situation, in welcher ein General zwei unterschiedliche Botschaften über einen Angriffsplan empfängt. Im BTC-System besteht die Lösung zum Problem darin, dass die Blockchain je nach Berechnungsaufwand in ihrer Länge variiert. Je

länger die Blockchain war, desto mehr Rechenleistung wurde zur Lösung des mathematischen Problems benötigt. Durch die Wahl der längsten Blockchain wird im BTC-System die Legitimität der Buchhaltung gewährleistet. Die einzige Möglichkeit eine illegitime Blockchain als legitim erscheinen zu lassen, besteht darin, einen Sybil-Angriff⁹ durchzuführen. Dieser Angriff basiert auf der Systemeigenschaft, dass eine neue Blockchain als gültig deklariert wird, falls eine Menge von Computern mit mehr als 51 Prozent der gesamten Rechnerkapazität, die Blockchain als legitim deklarieren.

Es herrscht Uneinigkeit über die Resistenz des BTC-Systems gegen einen 51-Prozent-Angriff. Einerseits würden die Kosten für den Erwerb einer solchen Rechenkapazität den Gewinn übersteigen und andererseits sind die Kosten eines 51-Prozent-Angriffes rein spekulativ und nicht als Sicherheitsargument verwendbar. Ein weiterer Kritikpunkt ist, dass auch mit tieferer Rechenkapazität ein Sybil-Angriff möglich ist. Die bezifferten 51 Prozent sind erforderlich, um den Misserfolg eines Angriffes auszuschliessen. Falls ein Angriff mit weniger Rechenleistung ausgeführt wird, sinkt die Wahrscheinlichkeit für einen erfolgreichen Angriff zwar drastisch, ist aber immer noch möglich [vgl. Kaskaloglu (2014)].

Trotz vieler technischer Unsicherheiten ist BTC ein Beispiel dafür, dass technologischer Fortschritt und elektronische Zahlungsmittel, Finanzsysteme revolutionieren könnten [vgl. Weisenthal (2014)]. Der folgende Abschnitt analysiert den Geldschöpfungsmechanismus des BTC-Systems.

2.2.2 Entstehung von Bitcoins

Nakamoto (2008) zufolge erfolgt Geldschöpfung im BTC-System nur durch das Mining und ist limitiert in der oberen Grenze von insgesamt 21 Millionen BTCs.

Miner erhalten BTCs, wenn sie den mathematischen Beweis für die Validierung einer Transaktion erbringen und dieser auch tatsächlich validiert wird. Durch diesen Prozess gelangen neue BTCs in den Umlauf. Je mehr BTCs gesamthaft im Umlauf sind, desto mehr Rechenleistung wird zur Validierung von Transaktionen benötigt. Dies hat zur Folge, dass der Geldschöpfungsmechanismus verlangsamt wird.¹⁰ Des Weiteren sind die Entschädigungsbeiträge für das Mining abnehmend. Bei Erreichung der Obergrenze kann eine Finanzierung der Mi-

⁹ Als Sybil-Angriff wird der Prozess bezeichnet, bei dem innerhalb eines verteilten Systems eine Interessengemeinschaft durch Übernahme grosser Anteile illegitime Forderungen durchzusetzen versucht [vgl. Douceur und Douceur (2002)].

¹⁰ Je mehr Transaktionen insgesamt getätigt beziehungsweise validiert wurden, desto mehr BTCs werden in das System eingespeist. Die Validierung einer Transaktion hat zur Folge, dass die Blockchain verlängert wird und somit der Schwierigkeitsgrad der darauf basierenden mathematischen Probleme erhöht wird.

ning-Aktivität mit einer Validierungsbelohnung erfolgen. Diese Belohnung wird von Handelspartnern im Rahmen einer Transaktion festgelegt. Höhere Beträge führen dabei zu einer rascheren Validierung der Transaktion.

2.2.3 Aneignung von Bitcoins

Zurzeit bestehen fünf Möglichkeiten, in den Besitz von BTC zu gelangen.

1. Innerhalb des BTC-Systems können Akteure als Miner agieren und werden dementsprechend dafür entschädigt.
2. BTC können als Zahlungsmittel für Güter und Dienstleistungen akzeptiert werden.
3. Kauf von BTCs mit traditioneller Währung bei virtuellen Wechselstuben.
4. Over-The-Counter-Tausch mit anderen Nutzern von BTCs: Es existieren verschiedene Online Plattformen, auf denen BTC-Nutzer miteinander Onlinehandel betreiben, Face-To-Face-Treffen vereinbaren oder Tauschevents organisieren.
5. Erwerb über BTC-Geldautomaten.

Trotz der Ähnlichkeit von BTC mit traditioneller Währung, kann sich der Erwerb von BTC sehr schwer gestalten. Finanzielle Institutionen sind derweil vorsichtig im Umgang mit der Währung, da rechtliche Grundlagen nur beschränkt vorhanden sind. Diese restriktive Haltung ist nicht nur seitens der Finanzinstitute beobachtbar sondern auch auf staatlicher Ebene [vgl. Bitlegal (2014)].

2.2.4 Kritische Einordnung

BTC ist geprägt von Unsicherheit und hohen Verlustrisiken. Der dezentrale Charakter der Währung bietet zwar Raum für fundamentale Neuerungen, wie zum Beispiel konkurrierende Kryptowährungen, im Sinne der österreichischen Schule [vgl. Ametrano (2014)], doch der Verzicht auf einen zentralen Kontrollapparat führt dazu, dass kriminelle Aktivitäten ein unkontrollierbares Ausmass annehmen können. BTC ermöglicht das Tätigen von globalen Transaktionen, ohne dabei persönliche Informationen freigeben zu müssen. Mithilfe von BTC können digitale Bankkonten in Form einer Wallet innert weniger Sekunden generiert werden. BTC-Nutzer sind nach Aussen nur durch einen Public-Key sichtbar.

Diese Charakteristika haben die Aufmerksamkeit von Aufsichts- und Steuerbehörden verschiedener Nationen erweckt und hatten meist regulatorische Massnahmen zur Folge.

In den Vereinigten Staaten von Amerika beispielsweise wird BTC generell nicht als Währung anerkannt, ist aber als Wertträger zu versteuern. Zahlungseingänge in Form von BTC seien zum Fair Market Value der virtuellen Währung zu versteuern. Bereits bei der Ermittlung des

Fair Market Value sind jedoch Ermessensspielräume möglich, da lediglich die Angabe gemacht wird, den Wechselkurs auf vernünftige Weise zu ermitteln [vgl. Fahey (2014)].

Unsicherheiten im Umgang mit der Währung äussern sich nicht zuletzt auch in Form von enormen Kursschwankungen und den damit verbundenen Risiken: Preisschwankungen des Faktors 1:10 innert eines Jahres sind keine Seltenheit [vgl. Barker (2014)].

Des Weiteren setzen sich Nutzer von BTC der Gefahr aus, Opfer von Hackerangriffen zu werden. Trotz grosser Sicherheitsmassnahmen besteht die Möglichkeit, dass sich Cyberkriminelle Zugriff auf die Wallet verschaffen, um BTCs zu stehlen. Transaktionen von BTC sind irreversibel und können in diesem Zusammenhang nicht wiederbeschafft werden. Nutzer von BTC müssen individuell Sicherheitsmassnahmen ergreifen, um sich vor Angreifern zu schützen. Zudem ist auch der Privatsphärenschutz nur bedingt gewährleistet. BTC-Nutzer mit kriminellem Hintergrund sind daran interessiert, ihre Identität zu verbergen und ergreifen dementsprechende Massnahmen. Private Nutzer, welche keine speziellen Massnahmen zur Anonymisierung ihrer Transaktionen ergreifen, setzen sich der Gefahr aus, ungewollt Informationen öffentlich zugänglich zu machen. Transaktionen werden in der Blockchain abgespeichert und sind als Public-Key öffentlich zugänglich. Androulaki et al. (2013) zufolge ist es in 40 Prozent der Fälle möglich, anhand der Blockchain Nutzer zu identifizieren. Die Identifizierung von Nutzern erfolgt, indem der Public-Key mit Informationen ausserhalb des BTC-Systems verknüpft wird. Externe Informationen können IP-Adressen, Email-Adressen, Blog-Einträge, Facebook-Profil oder weitere nutzerspezifische Daten sein [vgl. Reid und Harrigan (2011)]. Dementsprechend ist die propagierte und zugleich kritisierte Anonymität falsch, denn Public-Keys sind individuell und erlauben die Identifikation der Besitzer. Public-Keys sind folglich mit Nummernkontos vergleichbar und somit pseudo-anonym.

Neben einer privaten Wallet bietet sich Nutzern die Alternative in Form eines Benutzerkontos bei einer BTC-Wechselstube, um BTC zu halten. Diese Alternative setzt jedoch voraus, dass Wechselstuben genügend Massnahmen ergreifen, um gelagerte BTC vor Hackerangriffen zu schützen. Bislang mussten 18 von 40 bekannten Wechselstuben den Betrieb einstellen. Wechselstuben verschwanden dabei entweder ohne eine Erklärung oder sie begründeten den Verlust der gelagerten BTCs mit einem Hackerangriff. In den meisten Fällen bedeutete die Auflösung einer solchen Wechselstube für deren Nutzer den irreversiblen Verlust ihrer BTCs. Die bekannteste Wechselstube, die ihren Betrieb einstellte, ist Mt.Gox. Nutzer, welche BTCs bei Mt.Gox lagerten, verzeichneten insgesamt einen Verlust von 450 Millionen USD (Fair Market Value BTC) [vgl. Moore und Christin (2013)]. Die Nutzung solcher Wechselstuben stellt den dezentralen Charakter von Bitcoin in Frage, da diese als Vermittler für Transaktionen

erscheinen und somit die Rolle einer Drittinanz einnehmen. Im Rahmen der BTC-Gemeinschaft wird davon abgeraten, solche Wechselstuben zur Lagerung von BTCs zu benutzen, um die Dezentralität von BTC zu wahren [vgl. o.A. (2014b)].

2.2.5 Ist Bitcoin eine Währung?

Um beurteilen zu können, ob BTC als Währung geeignet ist, müssen drei Funktionen erfüllt sein. Eine Währung sollte als Zahlungsmittel, Wertaufbewahrungsmittel und Recheneinheit verwendet werden können [vgl. Krugman (1984)].

Damit eine Währung als Zahlungsmittel verwendet werden kann, muss diese transportierbar, fungibel und teilbar sein. Die Funktion als Wertaufbewahrungsmittel wird erfüllt, wenn eine Währung über einen beliebigen Zeithorizont gespart und aufbewahrt werden kann und dabei eine gewisse Sicherheit gewährleistet ist. Eine Währung sollte zudem benutzt werden können, um den relativen Wert von Gütern und Dienstleistungen zu ermitteln. Diese Messfunktion erfordert temporale Wertstabilität und Knappheit [vgl. Ametrano (2014)]. Auf Tabelle 2 werden vier Wertträger bezüglich der genannten Funktionen untersucht und bewertet.¹¹

Rangmatrix	Zahlungsmittel			Wertaufbewahrungsmittel		Recheneinheit		Summe
	Transportierbar	Teilbar	Fungibel	Sicher	Konservierbar	Wertstabil	Knapp	
Waren-geld	4	4	4	3	4	3	4	26
Gold	3	3	3	1	1	2	2	15
Fiat-Währung	2	2	1	2	2	1	3	13
BTC	1	1	2	4	3	4	1	16

Tabelle 2: Einordnung verschiedener Wertträger [eigene Tabelle in Anlehnung an Ametrano (2014)]

BTC wurde im Zusammenhang mit der Transportierbarkeit am höchsten platziert, da durch das BTC-Protokoll gewährleistet ist, BTCs ort- und zeitunabhängig in beliebiger Menge zu transferieren. Fiat-Währungen unterliegen gesetzlichen Regulatorien und können nicht belie-

¹¹ Rang Eins steht für den höchsten Erfüllungsgrad.

big transferiert werden. Die beiden Wertträger Gold und Warengeld sind durch deren physische Existenz nur begrenzt transportierbar. Dieselbe Rangfolge wurde in Bezug auf Teilbarkeit eruiert. BTC ist mit der kleinsten Einheit, des Satoshi (0.000 000 01 BTC), allen anderen Wertträgen überlegen. Warengeld ist letztplatziert, da in der Regel ein Wertverlust durch die Zerstückelung stattfindet – Diamanten etwa gewinnen überproportional an Wert, je grösser deren Einheit ist. Weniger klar ist die Bewertung der Wertträger bei Betrachtung der Fungibilität. Als fungibel gelten Sachen, die untereinander austauschbar sind und nur nach Zahl, Mass oder Gewicht bezeichnet werden [vgl. Honsell (2010)]. Dabei ist es nicht eindeutig, ob Fiat-Währung oder BTC höher platziert sind. Der Verfasser hat Fiat-Währung am höchsten eingestuft, da eine grössere Anzahl an erwerbbaaren Gütern verfügbar ist. Gold ist drittplatziert, da es neben quantitativen auch qualitative Attribute besitzt. Dies gilt auch für Warengeld – wobei weitere Attribute denkbar sind.

Geld muss sicher und konservierbar sein, um die Funktion als Wertaufbewahrungsmittel zu erfüllen. Der Verfasser dieser Arbeit bewertet Sicherheit, basierend auf der bestmöglichen Lagerungsweise. Gold wird beispielsweise in einem Hochsicherheitstresor aufbewahrt. Es ist für das Kriterium Sicherheit am höchsten platziert, da es unter Eigenverantwortung aufbewahrt werden kann, ohne dabei langfristig von inflationärer Entwertung betroffen zu sein [vgl. GHOSH et al. (2004)]. Fiat-Währung muss, um langfristig Wertstabil zu bleiben, zu einem bestimmten Zinssatz bei einer Bank angelegt werden. Diese Art der Lagerung ist jedoch von Finanzrisiken betroffen – die Insolvenz einer Bank ist nicht ausgeschlossen. Warengeld wurde vor BTC platziert, da in der Regel gesetzliche Bestimmungen vorliegen. Zum Verfassungszeitpunkt dieser Arbeit, existieren kaum gesetzliche Bestimmungen dazu, wie das Eigentum von virtuellen Währungen geregelt wird [vgl. FINMA (2014)]. Falls also BTC-Nutzer Opfer von Internetkriminalität werden, ist der Rechtsweg ausgeschlossen oder nur begrenzt möglich.

Die Konvertierbarkeit wurde aufgrund der physikalischen Haltbarkeit bewertet. Gold ist als Edelmetall am haltbarsten, gefolgt von Fiat-Währung. BTC existiert nur digital und ist an die physikalische Beständigkeit der Hardware Komponenten gebunden. Warengeld ist hier letztplatziert, da auch verderbliche Materialien unter diesen Wertträger fallen. Geld funktioniert nur als Recheneinheit, wenn die Kriterien der Wertstabilität und der Knappheit erfüllt sind.

Die Wertstabilität wurde aufgrund der Volatilität der verschiedenen Wertträger bemessen. Fiat-Währungen sind hier höchstplatziert, gefolgt von Gold [vgl. Conway (2014)]. BTC (notiert in USD) ist mit einer Volatilität von ungefähr 130 Prozent letztplatziert [vgl. Ametrano (2014)]. In der Rangordnung bezüglich der Knappheit ist BTC erstplatziert, da nach Protokoll 21 Millionen BTCs die obere Grenze sind. Gold ist zweitplatziert, da per Definition keine obere Grenze existiert.

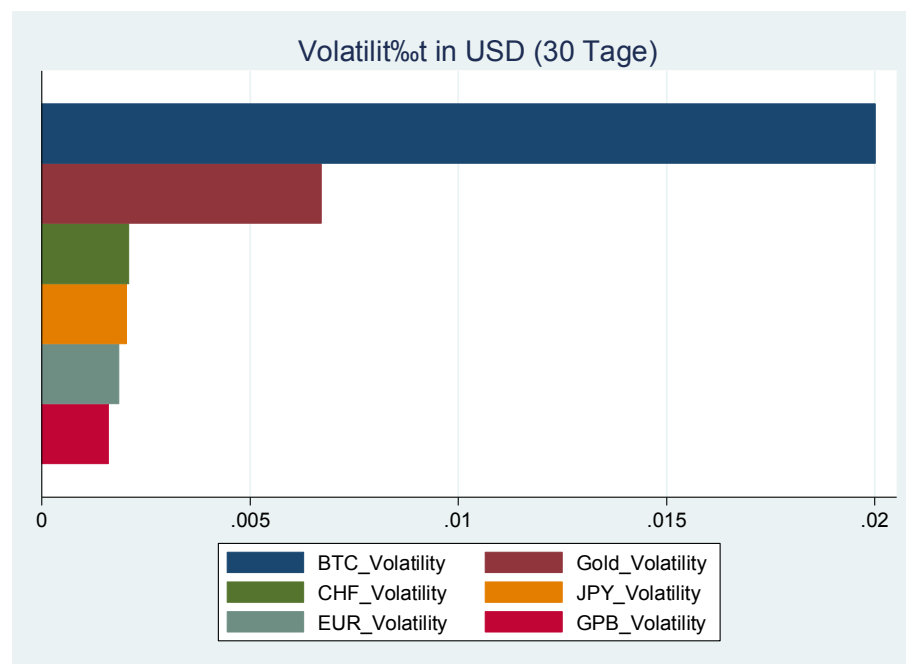


Abbildung 1: Volatilität verschiedener Wertträger im Vergleich [eigene Abbildung in Anlehnung an Ametrano (2014)]

Zusammenfassend kann also gesagt werden, dass sich BTC zurzeit nicht als Währung eignet und daran scheitert, dass vor allem Sicherheit und Wertstabilität nicht gewährleistet sind. Diese Faktoren sind jedoch stark von äusseren Einflüssen geprägt und es ist nicht auszuschliessen, dass BTC seine Stellung in dieser Rangfolge verbessert. Gesetzliche Bestimmungen und Marktstabilisierung könnten dazu führen.

2.3 Märkte

Die Finanzkrise ab 2007 und die europäische Schuldenkrise ab 2009, hatten zur Folge, dass die Effizienz der gegenwärtigen Wirtschaftsstruktur angezweifelt wurde [vgl. Brunetti (2012)]. Die Entstehung von BTC kann dementsprechend als Resultat des Vertrauensverlustes in zeitgenössische Währungssysteme angesehen werden [vgl. Kuster (2010)]. Dennoch kann BTC zu diesem Zeitpunkt nicht als Alternative zu bestehenden Währungen betrachtet werden. Trotz multipler Währungskrisen in der Vergangenheit konnten bestehende Währungssysteme eine funktionierende Wirtschaft gewährleisten [vgl. Sattler und Walter (2008)]. Ob BTC den gleichen Herausforderungen gerecht werden kann, ist aufgrund fehlender Erprobung anzu-

zweifeln. Die gestiegene Kapitalmobilität und die Globalisierung der Finanzmärkte stellen die Handlungsfähigkeit der Zentralbanken auf die Probe. Währungen sind vermehrt dem spekulativen Druck internationaler Finanzmärkte ausgesetzt. In diesem Zusammenhang ist es die Aufgabe der Zentralbanken, mithilfe geld- und währungspolitischer Massnahmen eine stabile Währung zu gewährleisten. In diesem Kontext würde bei einer Einführung des BTC, der Handlungsspielraum von Zentralbanken enorm eingeschränkt werden. Ob eine Währung frei von institutionellen Regulierungsmassnahmen funktionieren kann, ist zum jetzigen Zeitpunkt ungewiss. BTC ist geprägt von enormen Kursschwankungen spekulativen Ursprungs. Falls Währungsmärkte effizient sind, ist es Marktteilnehmern nicht möglich, dauerhaft überdurchschnittliche Gewinne zu erzielen, da alle Teilnehmer auf Basis gleicher Informationen agieren. Die Währungskurse widerspiegeln somit die Summe aller zugänglichen Informationen. Staatlich anerkannte Währungen besitzen diese Eigenschaft weitgehend [vgl. Fama (1991), Cornell, W. Bradford und Dietrich, J. Kimball (1978), Azad (2009), Al-Khazali und Koumanakos (2011)]. Ob der Markt für BTC gleichermassen effizient ist, wird im Teil Vier dieser Arbeit empirisch überprüft. Im folgenden Abschnitt wird der Markt für Kryptowährungen beschrieben, um ein tieferes Verständnis des BTC-Marktes zu ermöglichen.

2.3.1 Markt für Kryptowährungen

Der Markt für Kryptowährungen ist sehr heterogen und dadurch nur schwer definierbar. Ein gemeinsames Merkmal der Kryptowährungen ist, dass kein Währungsmonopol in Form einer Zentralbank existiert und somit die institutionelle Regulierung entfällt. Zum Verfassungszeitpunkt dieser Arbeit setzt sich der Markt aus 612 Kryptowährungen zusammen [vgl. Eisenberg (2014)].¹² Der Markt kann in drei Arten von Kryptowährungen gegliedert werden. Das Unterscheidungskriterium für diese Eingliederung ist der kryptologische Verschlüsselungsalgorithmus.¹³ BTC verwendet den SHA-256 und Litecoin (LTC) den Scrypt-Algorithmus. Diese beiden genannten Kryptowährungen bilden die technische Grundlage für Altcoins. Altcoin ist ein Überbegriff für Kryptowährungen, die als Derivate von BTC oder LTC gesehen werden können [vgl. Ahamad und Varghese (2013)]. Diese Marktzusammensetzung und die Möglichkeit sich frei für eine Währung entscheiden zu können, erlauben den Wettbewerb

¹² Es wird auf eine Auflistung verschiedener Währungen verzichtet, da im Rahmen dieser Arbeit vor allem der Pluralismus von Kryptowährungen von Bedeutung ist und der Fokus auf BTC gelegt wird.

¹³ Im Rahmen dieser Arbeit wird nicht auf die Funktionsweise des kryptologischen Verschlüsselungsalgorithmus eingegangen. Für weitere Informationen wird auf das Buch von Henk (2000) verwiesen.

unter den Währungen. Konkurrierende Währungen sind nach Hayek (1990), ein Verfechter der österreichischen Wirtschaftslehre, notwendig für die Entstehung einer stabilen Währung.¹⁴ Die Auffassung von Kryptowährungsanhängern geht diesbezüglich auseinander. Die Einen vermuten, dass sich die Diversifikation des Marktes positiv äussert, da die Marktdynamik erhöht wird und die Teilnehmerzahl ansteigt. Andere befürchten, dass durch die grosse Anzahl von Kryptowährungen, spekulativer Handel die Stabilisierung des Marktes verhindert und somit die Entwicklung zu einer konventionellen Währung verunmöglicht [vgl. Heid (2013)]. Grösstenteils wird der Wert von Kryptowährungen durch die Nachfrage gesteuert. Angebotsseitige Mengenregulierung im Sinne konventioneller Geldpolitik, ist nicht vorhanden.¹⁵ Marktteilnehmern ist das Angebot bekannt, da die Regulierung auf einem zuvor definierten Mechanismus basiert [vgl. Buchholz et al. (2012)]. In diesem Zusammenhang ist die Frage nach der Entstehung von Geld relevant. Nach Auffassung der neoklassischen Lehre wird die Geldmenge vorwiegend exogen determiniert. Geldschöpfung geschieht dabei ausserhalb des Finanzsystems und wird durch die Zentralbank reguliert. Die Zentralbank erhöht die Geldmenge, indem sie Wertschriften am Markt erwirbt und somit den Geschäftsbanken Geld zur Verfügung stellt. Im Gegensatz dazu geht die post-Keynesianische Lehre davon aus, dass die Geldmenge endogen determiniert wird – also innerhalb des Finanzsystems. Geschäftsbanken können dabei durch Kreditvergaben Geld schaffen [vgl. Söllner (1999)]. Die Grundidee hinter Kryptowährungen ist deren Unabhängigkeit. Es soll keiner einzelnen Partei oder Gruppe möglich sein, den Wert oder die Menge der Währung zu steuern. Zentralbanken und Geschäftsbanken haben demnach keine regulatorische Macht über Kryptowährungen. Die Regulierung geschieht durch einen im Voraus definierten Mechanismus der Protokolle verschiedener Kryptowährungen. Im Falle von BTC geschieht dies durch Mengenregulierung basierend auf der Mining-Aktivität. Andere Kryptowährungen verfügen ausserdem über Eigenschaften, wie etwa inflationäre Entwertung und Alterung von Währung [vgl. Stevenson (2013)]. Die Besonderheit, dass Kryptowährungen über keine definierbare Kontrollzentrale verfügen, sondern mathematische Algorithmen für das Funktionieren der Währung verantwortlich sind, ist neuartig und entspricht nicht der Vorstellung eines traditionellen Währungsmarktes. Ein Markt wird als Ort definiert, an dem Angebot und Nachfrage zusammentreffen und sich im Falle eines Tausches Preise bilden [vgl. Piekenbrock (2010)].

¹⁴ Trotz dieser Übereinstimmung mit der österreichischen Wirtschaftslehre, ist zurzeit keine Kryptowährung wertstabil. Eine ausführliche Arbeit hierzu wurde durch Šurda (2012) verfasst.

¹⁵ Diese Aussage bezieht sich auf die bekanntesten Kryptowährungen, wie beispielsweise BTC und LTC.

Um zu verstehen, weshalb sich Kryptowährungsmärkte grundsätzlich von Devisenmärkten unterscheiden, ist ein Vergleich sinnvoll. Das Wertmass für traditionelle Währung ist deren relativer Wert gegeneinander. Als Produzent, beziehungsweise Anbieter, erscheinen hierbei Staaten. Der Wert einer Währung hängt wesentlich von der Wahrnehmung über die Wirtschaftspolitik eines Landes ab [vgl. Conway (2011)]. Im Falle von Kryptowährungen existiert in engerem Sinne kein definierbarer Anbieter – Marktteilnehmer erscheinen als Anbieter wie auch als Käufer. Der Wert einer Kryptowährung hängt von der Wahrnehmung der Nutzer ab. Geldpolitische Regulierung, wie etwa durch Fixierung von Wechselkursen, ist nicht möglich. Trotz der diffusen Marktzusammensetzung und jungen Geschichte von Kryptowährungen ist der Markt sehr ausführlich dokumentiert, da alle Daten jederzeit frei zugänglich sind.

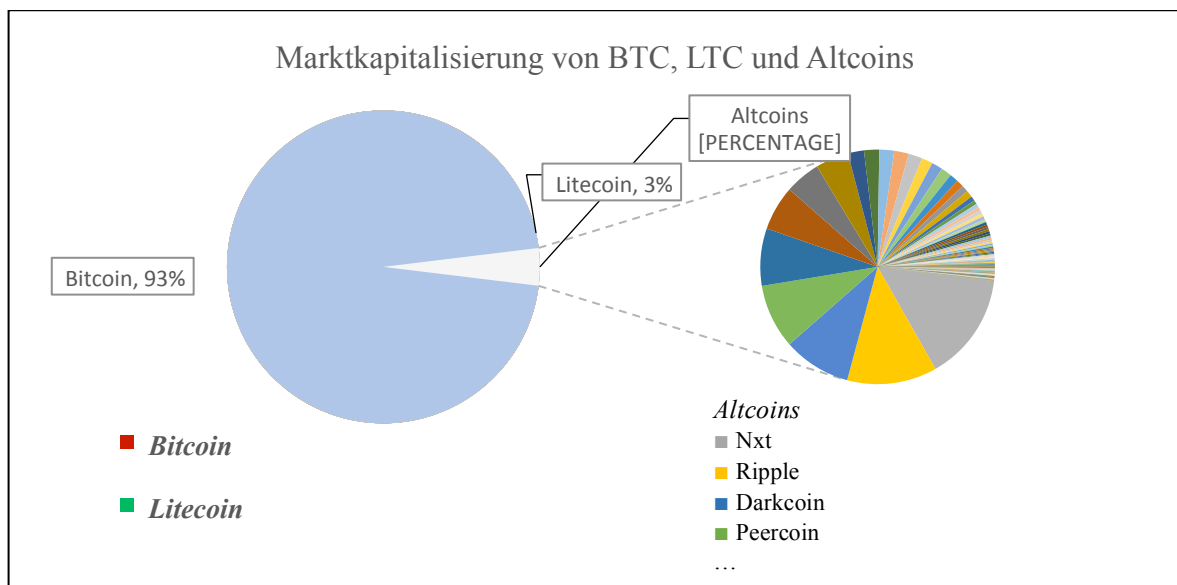


Abbildung 2: Marktkapitalisierung von Kryptowährungen [eigene Abbildung]

Mit einer Marktkapitalisierung von insgesamt 8.7 Milliarden USD setzt sich der Kryptowährungsmarkt wie in der Abbildung 2 dargestellt, zusammen.¹⁶ Dabei wurde die Marktkapitalisierung als Ordnungskriterium ausgewählt.^{17,18} Es ist ersichtlich, dass BTC mit 93 Prozent den Markt dominiert. Die verschiedenen Altcoins machen lediglich vier Prozent des Marktes aus. Die meisten Altcoins haben keinen Gegenwert in Fiat-Währung und existieren nur für kurze Zeit. Da das BTC-Protokoll frei zugänglich ist, können Internetnutzer ohne fundierte Fachkenntnisse ihre eigene Kryptowährung erschaffen [vgl. Grothaus (2014), Hern (2014), Kelly (2014)]. Seit der Entstehung von BTC, haben Miner immer effizientere Methoden gefunden,

¹⁶ Das Diagramm wurde auf Basis aller bekannten Kryptowährungen erstellt, welche einen Gegenwert in Fiat-Währung haben.

¹⁷ Denkbar wäre auch das tägliche Transaktionsvolumen als Ordnungskriterium.

¹⁸ Der Übersicht halber wurden nur die sechs grössten Kryptowährungen aufgelistet.

um Transaktionen zu verifizieren. Falls also eine neue Kryptowährung XY geschaffen wird, können Miner innert Kürze grosse Mengen an Transaktionen verifizieren und werden dafür mit der entsprechenden Kryptowährung entschädigt. Falls XY sich später am Markt behaupten kann und der Kurs für XY steigt, verzeichnen frühzeitige Miner hohe Gewinne [vgl. Robinson (2014)]. Diese Konstellation resultiert darin, dass stetig neue Kryptowährungen kreiert werden.

2.3.2 Markt für Bitcoins

Es ist sinnvoll, Informationsquellen genau zu beschreiben, bevor auf den BTC-Markt eingegangen wird. Berechnungsgrundlage für die Marktanalyse ist dabei die Blockchain, welche im übertragenen Sinne als Buchhaltung von BTC bezeichnet werden kann. Für ein besseres Verständnis bietet sich hier die graphische Darstellung der einzelnen Bestandteile der Blockchain.

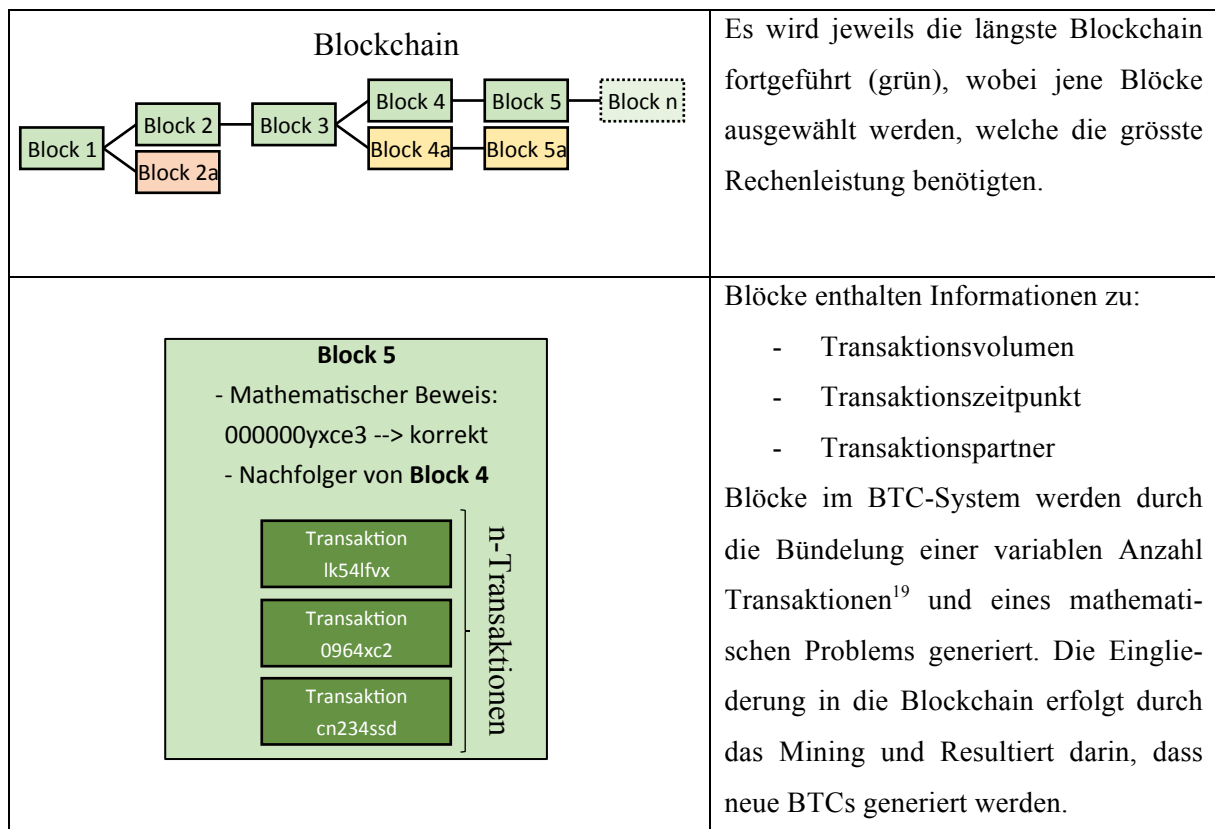


Abbildung 3: Die Blockchain als Informationszentrale [eigene Abbildung]

Mit einer Marktkapitalisierung von 8.1 Milliarden USD verkörpert BTC 93 Prozent des Kryptowährungsmarktes.²⁰ Die Marktkapitalisierung lässt sich über den BPI [vgl. o.A. (2014b)]

¹⁹ Ein Block kann maximal 1 Megabyte gross sein, diese Datengrösse limitiert die maximale Anzahl Transaktionen pro Block. Zurzeit reicht die Anzahl Transaktionen pro Block von einer bis 3861 Transaktionen [vgl. blockr.io (2014)].

²⁰ Stand 23. Juli 2014

und die Summe generierter BTCs berechnen. Die Gesamtzahl der BTCs im Umlauf erhält man, indem man die in der Blockchain enthaltenen Blöcke summiert und mit der Anzahl generierter BTCs je Block multipliziert. Die Länge der Blockchain determiniert demzufolge den Geldschöpfungsmechanismus. Bei einer Blockchain-Länge von $\leq 210\,000 \times x$ Blocks werden $50/x$ BTCs je Block generiert, wobei $x \in \mathbb{N}^+$ gilt. Danach wird zeitpunktabhängig die jeweilige Gesamtzahl BTCs mit dem BPI multipliziert. Da der Geldschöpfungsmechanismus des BTC-Systems weitgehend linear verläuft und prognostizierbar ist²¹, sind die enormen Schwankungen der Marktkapitalisierung hauptsächlich auf den BPI zurückzuführen. Auf den folgenden Grafiken sind Approximationen der Marktkapitalisierung und historischen Volatilität zu sehen.²² Die Trendlinie auf Abbildung 5 deutet auf einen Abwärtstrend der Volatilität hin.²³

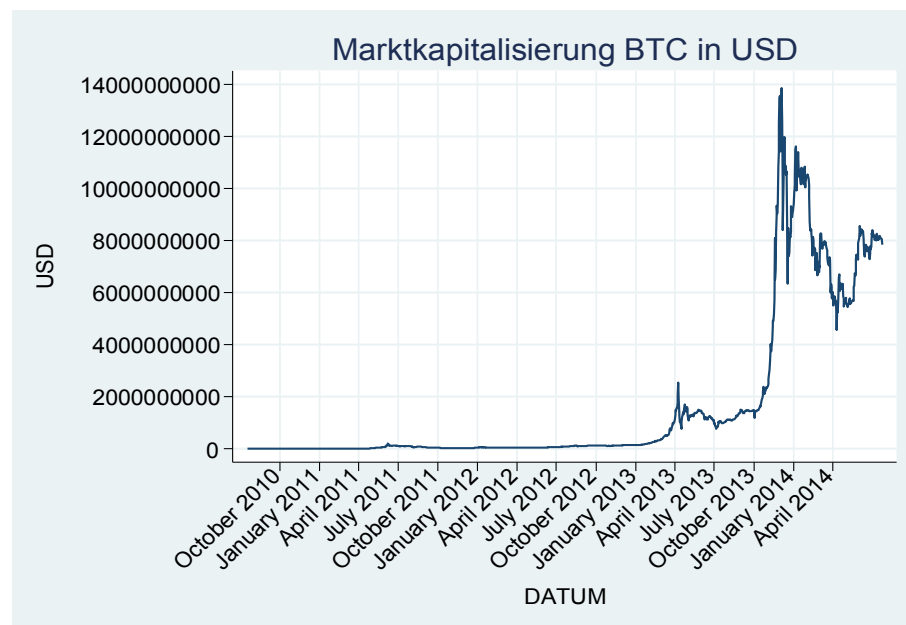


Abbildung 4: Marktkapitalisierung von BTC [eigene Abbildung]

²¹ Anhang: Regressionen Abschnitt 2.3.2 ($\beta = 6492.67$; $t = 265.87$; $P > |t| = 0.0$; $R^2 = 0.9797$).

²² Als Datensatz wurde der tägliche BPI verwendet.

²³ Anhang: Regressionen Abschnitt 2.3.2 ($\beta = -.0000261$; $t = -11.73$; $P > |t| = 0.0$; $R^2 = 0.0874$).

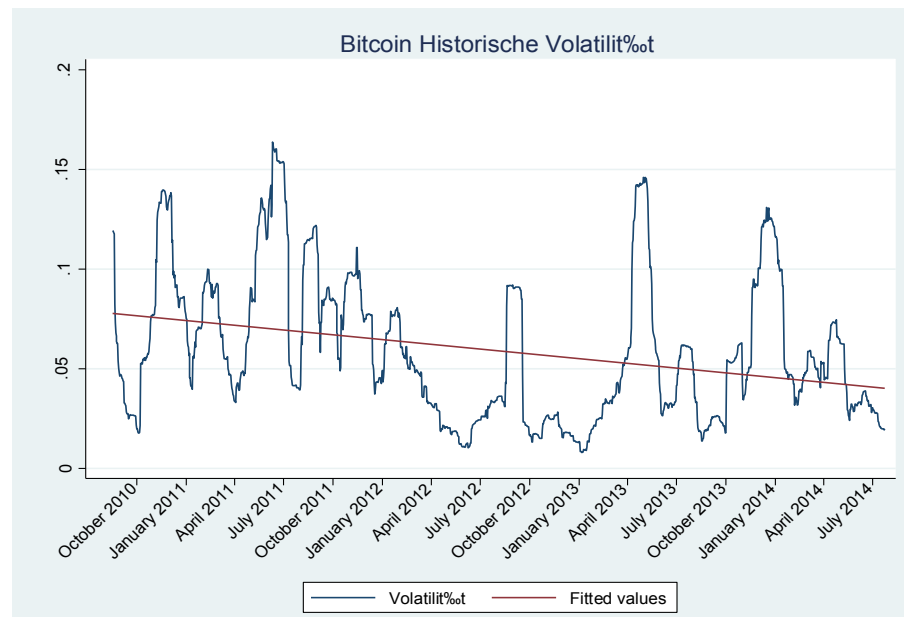


Abbildung 5: Historische Volatilität BTC [eigene Abbildung]

Die Preisbildung und die daraus resultierende Volatilität auf dem BTC-Markt erweckte das Interesse etlicher Wirtschaftswissenschaftler. Bisherige Literatur verweist auf mehrere Einflussfaktoren im Zusammenhang mit dem BTC-Preis. Buchholz et al. (2012) analysierten den BTC-Markt bezüglich des Angebots und der Nachfrage. Wijk (2013) untersuchte die Korrelation des BTC-Preises mit verschiedenen Finanzindikatoren, wie Beispielsweise – Ölpreis, Aktienmärkte oder Währungskurse. Kristoufek (2014), (2013) zufolge wird der Preis hauptsächlich durch die Erwartungen der Investoren determiniert. Zusätzlich besteht ein bidirektionaler Zusammenhang zwischen BTC-Preisen und der Nutzung von Suchmaschinen im Zusammenhang mit BTC.

Ciaian et al. (2014) untersuchen den BTC-Preis im Zusammenhang mit Nachfrage und Angebot, globaler Finanzindikatoren und der Attraktivität für Investoren.

Buchholz et al. (2012) zufolge ist das BTC-Angebot exogen gegeben und prognostizierbar. Deshalb wird der Preis hauptsächlich nachfrageseitig determiniert. Das Verhalten der Marktteilnehmer wird durch die Medienpräsenz von BTC beeinflusst. Je öfter die Suchmaschine Google im Zusammenhang mit BTC verwendet wurde, desto mehr Transaktionen haben stattgefunden. Ein Anstieg der Anzahl Transaktionen kann wiederum als ein Anstieg der Teilnehmerzahl gedeutet werden. Der Preis als Indikator der BTC-Nachfrage wird durch die Volatilität des BTC-Marktes positiv beeinflusst. Steigende Volatilität resultiert im Anstieg des BTC-Preises. Dies lässt vermuten, dass der Marktpreis stark vom spekulativen Verhalten der Teilnehmer geprägt ist. Des Weiteren ist die Volatilität nach negativen Preishocks geringer als nach positiven Preishocks. Dies weist nach Buchholz et al. (2012) auf die Existenz von Preisblasen auf dem BTC-Markt hin.

Wijk (2013) zufolge ist der BTC-Preis positiv mit dem USD-EUR Wechselkurs und dem Dow Jones korreliert. Der West-Texas-Intermediate Öl-Preis hingegen ist negativ korreliert. Wijk (2013) betont, dass die Resultate darauf deuten, dass der BTC-Preis stark von der US-Wirtschaft abhängt. Eine Stärkung der US-Wirtschaft hat zur Folge, dass der BTC-Preis ansteigt.

Kristoufek (2013) geht davon aus, dass es nicht möglich ist, den Preis von BTC mit konventioneller Finanztheorie²⁴ zu untersuchen. Fiat-Währungen können anhand makroökonomischer Modelle analysiert werden, da unter anderem, Informationen zu Bruttoinlandprodukt, Zinssätze, Inflation, Arbeitslosigkeitsrate und weiteren Aspekten vorhanden sind. Der BTC-Markt und insbesondere die Nachfrage, können nicht auf Basis einer zugrundeliegenden Wirtschaft analysiert werden.²⁵ Kristoufek (2013) behauptet, dass Teilnehmer des BTC-Marktes ausschliesslich, in der Erwartung, dass der BTC-Preis steigt in BTC investieren. Zudem setze sich der Markt aus Noise-Tradern²⁶, Spekulanten und Trend orientierten Teilnehmern zusammen und die Investorengruppe der Fundamentalisten sei inexistent. Um das Verhalten der Marktteilnehmer zu verstehen, untersuchte Kristoufek (2013) die Internetnutzung bezüglich BTC. Aus der Untersuchung des BTC-Preises und der Suchaktivität²⁷ auf Wikipedia und Google stellte sich heraus, dass ein bidirektionaler Zusammenhang besteht. Erhöhte Suchaktivität resultiert in grösserer Preisveränderung. Wenn sich der BTC-Preis über/unter der Trendgeraden des Preises befindet, steigt/sinkt der Preis. Der Zusammenhang ist bidirektional, da auch Preisveränderungen von einem Anstieg der Suchaktivität gefolgt werden.

Ferner analysierte Kristoufek (2014) verschiedene Faktoren²⁸ hinsichtlich deren Einfluss auf den BTC-Preis. Angesichts ökonomischer Werttreiber zeigte sich, dass BTC-Preise langfristig mit der Verwendung von BTC als Zahlungsmittel positiv korreliert sind. Kurzfristig werden die Preise hauptsächlich durch den BTC-Devisenhandel determiniert und die Verwendung von BTC als Zahlungsmittel ist kein massgebender Werttreiber. Als technische Werttreiber werden sämtliche Vorgänge im Zusammenhang mit der Mining Aktivität bezeichnet. Steigende BTC-Preise erhöhen den Anreiz, sich bei der Mining-Aktivität zu beteiligen. Das BTC-

²⁴ Beispielsweise: Future Cash Flow Modell, Kaufkraftparität, ungedeckte Zinsparität.

²⁵ Dem widerspricht Wijk (2013), da er einen positiven Zusammenhang des BTC-Preises mit der US-Wirtschaft postuliert.

²⁶ Noise Trader sind Marktteilnehmer, die bei Investitionsentscheidungen neben objektiven auch subjektive Informationen verwenden. Entscheidungen sind demzufolge beeinflusst durch Gerüchte, Expertenmeinungen und technischen Analysemethoden [vgl. Daske (2002)].

²⁷ Kristoufek (2013) untersuchte wie oft Suchbegriffe im Zusammenhang mit BTC verwendet wurden.

²⁸ Ökonomische Werttreiber, technische Werttreiber, Popularität, Safe Haven Funktion und der Einfluss des chinesischen BTC-Marktes

Protokoll gewährleistet, dass bei erhöhter Mining-Aktivität, die zu lösenden mathematischen Probleme komplexer werden und somit mehr Rechenleistung benötigen. Die benötigte Rechenleistung steigt und erfordert dadurch Investitionen in technische Ausrüstung. Folglich sind der BTC-Preis und die Komplexität der mathematischen Probleme positiv korreliert. Die Popularität von BTC hat die grösste Auswirkung auf BTC-Preise, sodass hauptsächlich Erwartungen der Marktteilnehmer den BTC-Preis bestimmen.

Ciaian et al. (2014) widersprechen Wijk (2013) bezüglich der Korrelation des BTC-Preises mit verschiedenen Finanzindikatoren, da sie diesbezüglich keinen signifikanten Zusammenhang feststellen konnten. Bei der Auswertung der Daten berücksichtigte Wijk (2013) den Effekt von Transaktionsvolumen und -anzahl, Umlaufgeschwindigkeit und Popularität von BTC nicht – sodass die Korrelation des BTC-Preises mit den betrachteten Finanzindikatoren überbewertet wurde. Ciaian et al. (2014) konnten feststellen, dass der BTC-Preis durch das Transaktionsvolumen/-anzahl und der Umlaufgeschwindigkeit beeinflusst wird. Den stärksten Einfluss auf den Preis hatte die BTC-Popularität.²⁹

Zusammenfassend kann auf Basis der vorgestellten Literatur davon ausgegangen werden, dass der BTC-Markt stark durch spekulative Investitionen beeinflusst wird. Der bisherige Wissensstand lässt vermuten, dass der BTC-Preis systematisch über und unterbewertet wird. Robert Shiller etwa bezeichnete BTC als ein ausserordentliches Beispiel einer spekulativen Preisblase [vgl. Weisenthal (2014)].

In diesem Zusammenhang wird im folgenden Kapitel auf theoretische Erklärungsansätze bezüglich der Erwartungsbildung und die Markteffizienztheorie eingegangen.

²⁹ Als Proxy für die Popularität dienten: wie oft Wikipedia im Zusammenhang mit BTC verwendet wurde und wie viele neue Einträge auf der Internetseite bitcointalk.com erstellt wurden.

2.4 Finanzmarkttheorie

2.4.1 Einführung

Die Verhaltensmotive von Akteuren auf Währungsmärkten ist seit rund 50 Jahren Bestandteil der Finanzmarkttheorie. Bis zum heutigen Zeitpunkt sind sich Wirtschaftswissenschaftler uneinig darüber, wie Erwartungsbildung und Investitionen auf Märkten zusammenhängen. Die ältesten zwei theoretischen Ansätze der Erwartungsbildung propagieren einerseits die rationale und andererseits die adaptive Erwartungsbildung auf Märkten [vgl. Heri (1982)]. Anhänger der Theorie rationaler Erwartungen gehen davon aus, dass rationale Marktteilnehmer bei ihrer subjektiven Erwartungsbildung bezüglich des Preises keine systematischen Fehler begehen. Abweichungen vom objektiven Preis sind zufällig und unterliegen somit einem RW.³⁰ Ferner basieren der objektive Preis und die subjektive Preiserwartung auf den gleichen Informationen, sodass der rationale Marktteilnehmer im Durchschnitt den Preis erwartet, der dem wahren Preis entspricht. Ausserdem sind frei zugängliche Informationen vollständig im aktuellen Preis enthalten [vgl. Muth (1961)]. Preisveränderungen sind dementsprechend nur aufgrund unvorhersehbarer Ereignisse möglich [vgl. Poppen (2010)]. Im Modell adaptiver Erwartungsbildung hingegen wird der Preis auf Basis von historischen Informationen determiniert [vgl. Dangl (1999)]. Beispielsweise korrigieren Akteure des BTC-Marktes ihre Erwartungen überproportional nach oben/unten, falls der BTC-Preis über/unter ihrer subjektiven Preiserwartung lag. Im Rahmen rationaler Erwartungen wäre dies ein Hinweis auf die Ineffizienz des BTC-Marktes, da der BTC-Preis in diesem Fall systematisch über-/unterbewertet würde.

³⁰ Siehe Kapitel 2.6

Folgende Abbildung verdeutlicht, weshalb keine der theoretischen Ansätze mit Sicherheit bestimmen kann, ob ein Markt effizient ist.

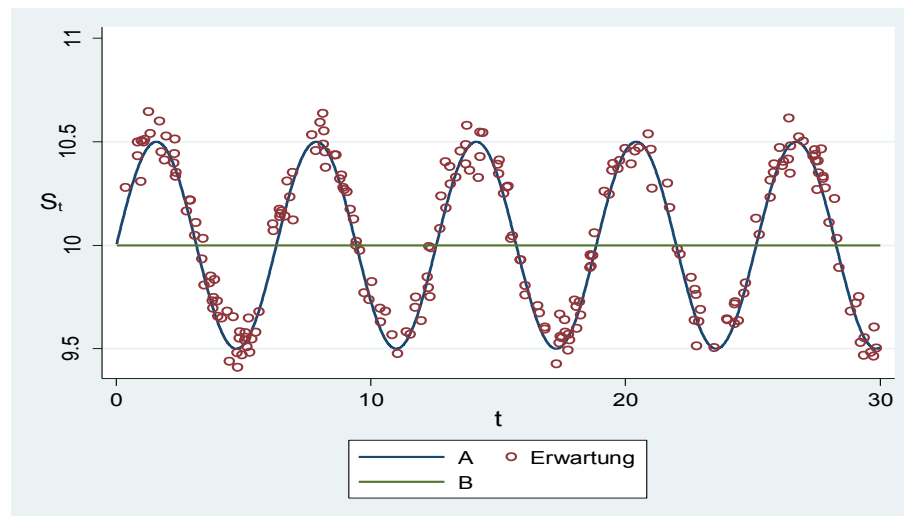


Abbildung 6: Theorie rationaler Erwartungen [eigene Abbildung in Anlehnung an Muth (1961)]³¹

Auf Abbildung 6 stellen A und B, Modelle zur Berechnung des objektiven Preises dar. Falls das Modell B als das richtige Modell angenommen wird, so begehen Akteure des Marktes einen systematischen Fehler.³² Dies bedeutet, dass die Markteffizienz abgelehnt wird. Falls jedoch das Modell A als das richtige Modell angenommen wird, sind Abweichungen vom objektiven Preis zufällig und dementsprechend ist der Markt effizient. Auch in diesem Fall kann aber nicht mit Sicherheit gesagt werden, ob das Modell korrekt gewählt wurde. Die EMH, welche die empirische Überprüfbarkeit ermöglichen soll, wurde durch Fama und Malkiel (1970) aufgestellt. Die EMH postuliert, dass Finanzmärkte sich aus Akteuren mit homogenen Erwartungen zusammensetzen und deren Verhalten stets rational ist. Akteure, die in ihrer Erwartungsbildung vom fundamentalen Wert abweichen, werden sofort durch den Marktmechanismus korrigiert. Diese Annahmen implizieren, dass der Markt fehlerfrei ist. Ein Jahrzehnt nach dem die EMH publiziert wurde, kamen erste Zweifel an dieser auf. Shiller (1981) zeigte unter Verwendung von Marktdaten, dass gewisse Aktienkurse zu volatil sind, als dass sie durch zufällige Abweichungen vom fundamentalen Preis erklärt werden könnten. Marktanomalien stellten die Robustheit der EMH etliche Male unter Probe [vgl. Shleifer (2000)]. 1991 gründeten Robert Shiller und Richard Thaler die Forschungsgruppe Behavioral-Finance (BF) am National Bureau of Economic Research in Massachusetts [vgl. Shiller

³¹ Muth (1961) verwendet lineare Modelle zur Analyse. Modell A wurde jedoch auf Basis der Sinuskurve erstellt, da nichtlineare, rationale Erwartungsmodelle der Theorie nicht widersprechen [vgl. Sewell (2012)].

³² Der subjektive Preis über-/unterschätzt den objektiven Preis systematisch.

(2003)]. Der BF lehnt den Grundgedanken der EMH, der Markt könne langfristig nur aus wirtschaftlich rationalen Teilnehmern bestehen, ab. Vertreter des BF gehen davon aus, dass Marktpreise von psychologischen Attributen geprägt sind und auch wirtschaftlich irrationales Verhalten massgeblichen Einfluss auf die Preisbildung am Markt hat. Preisveränderungen basieren daher nicht nur auf neu eintreffenden Informationen, sondern werden auch durch psychologische Faktoren beeinflusst. Enorme Marktanomalien in den letzten Jahren³³ führten dazu, dass neben Akademikern auch Praktiker die Konsistenz der EMH in Frage stellten. Unsicherheit bezüglich der EMH resultierte in zunehmender Popularität des BF und der Polarisierung der akademischen Diskussion [vgl. Ferber (2009)]. Trotz der Ansicht vieler Akademiker und Praktiker, dass der BF und die EMH sich stark unterscheiden oder sich sogar widersprechen, wurde 2013 der Wirtschaftsnobelpreis an Eugene Fama, Lars Peter und Robert Shiller vergeben. Die Preisvergabe wurde vielerorts als widersprüchlich bezeichnet und stark kritisiert [vgl. Bris und Cantale (2013), Meier (2013)]. In diesem Zusammenhang erläutert Amman (2013), dass die beiden Ansätze sich nicht grundsätzlich widersprechen, sondern den Markt von verschiedenen Standpunkten analysieren. Die Hauptaussage von Fama bezüglich der Informationseffizienz und der Unvorhersehbarkeit von Marktpreisen in der kurzen Frist wird weitgehend anerkannt [vgl. Fama (1965)]. In der langen Frist hingegen sind Preisentwicklungen durchaus vorhersehbar.

Shiller et al. (1984) zeigen, dass hohe Dividenden relativ zum Preis langfristig in einem Preisanstieg resultieren und auch der umgekehrte Mechanismus gilt. Dies impliziert, dass Investoren höhere Gewinne erzielen können, wenn sie Wertträger kaufen wenn das Dividende/Preis Verhältnis hoch ist und verkaufen, wenn dieser tief ist.

Das Economic Sciences Prize Committee (2013) erklärt in der Pressemitteilung der Wirtschaftsnobelpreisvergabe 2013, dass die langfristige Vorhersehbarkeit von Marktpreisen auf Basis beider Modelle interpretiert werden kann. Aus dem Blickwinkel der EMH, gelingt dies, indem man anstelle eines konstanten, einen variablen Diskontsatz annimmt. Diese Annahme erklärt die übermässige Varianz, die Shiller (1981) als Argument gegen die EMH verwendet hat. Aus Sicht der BF besteht der Markt nicht nur aus vollständig rationalen Teilnehmern – auch Irrationalität beeinflusst die Marktpreisbildung. Auf Basis des BF kann interpretiert werden, dass irrationale Teilnehmer nicht aus dem Markt verdrängt werden, da institutionelle Beschränkungen dies verhindern. Rationale Teilnehmer können beispielsweise, infolge finan-

³³ Finanzkrise ab 2007 – Der Dow Jones Industrial Average beispielsweise, fiel zwischen Oktober 2007 und März 2009 von 14164 auf 6547 Punkte.

zieller Hemmnisse, irrationale Teilnehmer nicht vollständig vom Markt verdrängen. Dies führt zu überhöhter Volatilität und langfristiger Vorhersehbarkeit der Preise.

Trotz wichtiger Erkenntnisse beider Modelle ist ersichtlich, dass der Momentane Forschungsstand der Finanzmarkttheorie über keine allgemein gültige Theorie verfügt. Finanzmärkte sind keine geschlossenen Systeme sondern dynamisch und offen. Auch wenn Märkte meistens zu funktionieren scheinen, treten ab und an grosse Anomalien auf. Beide Modelle enthalten Elemente, die zum einem besseren Verständnis von Zusammenhängen verhelfen, es ist jedoch keine der Theorien in der Lage, die vollständige Funktionsweise von Finanzmärkten zu erklären.

Im Anschluss an die Nobelpreisvergabe 2013 führte Bloomberg mit zwei Wirtschaftswissenschaftlern des Massachusetts Institute of Technology Interviews. Robert Solow sagte, die Preisvergabe sei ein Zeichen dafür, dass die Finanzwissenschaft keine beständige Doktrin hat. Andrew Lo bekräftigte die Relevanz der Entwicklung neuer analytischer Methoden um Märkte verstehen zu können [vgl. Miller et al. (2013)]

Im nächsten Abschnitt wird BTC im Zusammenhang mit der Finanzmarkttheorie analysiert.

2.4.2 Bitcoin und die Finanzmarkttheorie

BTC ist aufgrund seiner Geschichte besonders interessant im Zusammenhang mit der Finanzmarkttheorie. Die rasante Preisentwicklung und die exzessive Volatilität deuten auf Basis des BF auf eine Preisblase hin. Am World Economic Forum 2014 griff Shiller in der Diskussion über digitale Trends und Finanzmärkte das Thema BTC auf und bezeichnete BTC als ein ausgezeichnetes Beispiel einer Spekulationsblase [vgl. Weisenthal (2014)].

Fama erklärt in einem Interview mit THE NEW YORKER, dass es nicht möglich sei, Blasen im Vorfeld zu identifizieren. Aussagen über Preisentwicklungen und Blasen, seien zu 50 Prozent falsch. Unsicherheit über die Existenz von Blasen auf Märkten begründet er damit, dass Preisblasen im Vorfeld identifizierbar sein müssen und dass dies nicht der Fall sei [vgl. Cassidy (2010)].

Im Folgenden wird die Interpretation des Economic Sciences Prize Committee (2013) der beiden Ansätze für die Analyse von BTC verwendet. Aus Sicht der EMH sind auf effizienten Märkten überhöhte Preisschwankungen mit der Variabilität des Diskontsatzes der Dividenden zu begründen. Da BTC über keine Dividenden verfügt und BTCs auch nicht verzinst werden, sollte dies darauf hindeuten, dass der BTC-Markt irrationale Investoren nicht erfolgreich verdrängen konnte. Alternativ kann es jedoch auch sein, dass der BTC-Markt effizient ist und keine prognostizierbaren Spekulationsblasen existieren. Aus Sicht des BF sollten institutionel-

le Beschränkungen die Existenz von irrationalen Teilnehmern am BTC-Markt erlauben. Sollte dies nicht der Fall sein, würden diese langfristig vom Markt verdrängt werden. Shiller (2014) beschreibt, dass BTC die Merkmale einer einfachen Spekulationsblase erfüllt. Denn er ist ein Wertträger, der gehalten wird, weil Investoren darauf hoffen, dass der Preis in der Zukunft steigen wird und Preisschwankungen verstärkt auftreten bei erhöhter Medienpräsenz des Wertträgers. In diesem Sinne besteht der BTC-Markt zu einem grossen Teil aus irrationalen Akteuren. Diese sollten jedoch langfristig vom Markt verdrängt werden, falls der BTC-Markt effizient sein sollte. Im Folgenden werden die theoretischen Grundlagen der EMH erörtert.

2.4.3 Die Effizienzmarkthypothese

Fama (1965) bezeichnet einen Markt als effizient, wenn dieser aus einer grossen Anzahl rationaler Teilnehmer besteht und relevante Informationen beinahe kostenlos verfügbar sind. Auf einem effizienten Markt versuchen Teilnehmer zukünftige Preise gewinnbringend zu prognostizieren. Aufgrund der rationalen Erwartungsbildung resultiert der Wettbewerb zwischen den Marktteilnehmern darin, dass Marktpreise zufällig – in Form eines RW – um den tatsächlichen intrinsischen Wert des Wertträgers fluktuieren. Diese Fluktuationen werden durch Unstimmigkeiten zwischen den Marktteilnehmern bezüglich des intrinsischen Wertes verursacht und entsprechen in ihrer Summe 0. Der intrinsische Wert ändert sich nur aufgrund neuer Informationen und Preisanpassungen erfolgen augenblicklich. Preisanpassungen aufgrund neuer Informationen sind ebenfalls nicht gefreit von Unstimmigkeiten zwischen Marktteilnehmern und können zeitlich wie auch in ihrer Amplitude vom intrinsischen Wert abweichen. Neue Informationen können dazu führen, dass Marktteilnehmer den intrinsischen Wert über oder unterschätzen. Ferner können Marktteilnehmer ihre Erwartungen auch verfrüht oder verspätet anpassen – was in der RW-Theorie als Lag bezeichnet wird. Diese Abweichungen vom intrinsischen Wert sind ebenfalls zufällig und in ihrer Summe 0.

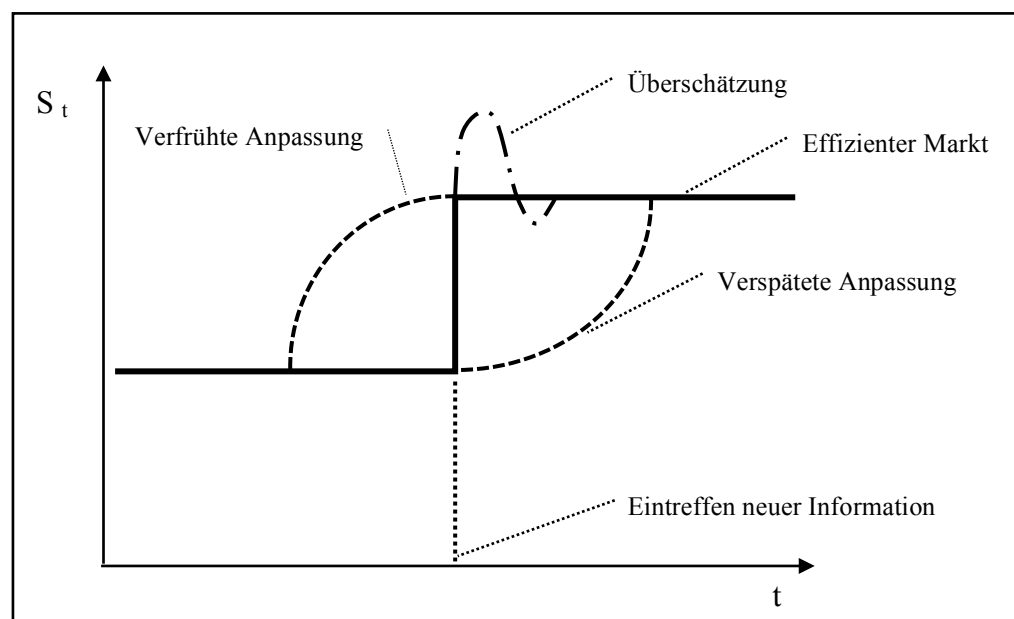


Abbildung 7: Preisreaktion auf neue Information [eigene Abbildung
in Anlehnung an Ross et al. (2002), S. 344]

Auf Abbildung 7 ist ersichtlich wie sich verschiedene Teilnehmerreaktionen auf den Marktpreis auswirken können. Diese Abweichungen vom Effizienten Markt finden regelmässig statt und können je nach Modellannahme über den untersuchten Markt zur Ablehnung der Markt-

effizienz führen. Fama (1998) postuliert dass die Markteffizienz in der langen Frist aufgrund methodischer Fehlannahmen möglich ist.

Es lassen sich drei Grade der Markteffizienz unterscheiden: die schwache, halbstrenge und strenge Form der Informationseffizienz. Die schwache Informationseffizienz statuiert, dass aktuelle Preise auf Basis historischer Preise stets alle preisrelevanten Informationen enthalten. Demzufolge sollte es unter Verwendung historischer Preise langfristig nicht möglich sein, höhere Gewinne zu erzielen als die Buy-And-Hold-Strategie³⁴. Falls Preise einem RW folgen, bedeutet dies auch, dass die schwache Form der EMH erfüllt ist. Die halbstrenge Informationseffizienz fügt die Bedingung hinzu, dass Preisanpassungen auch relevante öffentlich verfügbare Informationen enthalten. Folglich können unter Verwendung öffentlicher Informationen, wie beispielsweise Geschäftsberichten, langfristig keine Gewinne erzielt werden. Die strenge Form der Informationseffizienz erfordert, dass sämtliche relevanten Informationen im Preis enthalten sind, auch private Informationen, wie etwa Insiderinformationen. Demzufolge kann auch Insiderwissen nicht gewinnbringend verwendet werden, um Preise zu prognostizieren [vgl. Fama und Malkiel (1970)].

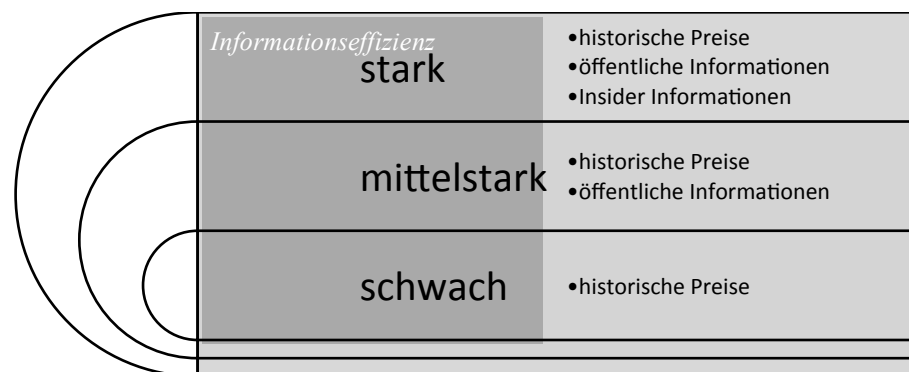


Abbildung 8: Grade der Markteffizienz [eigene Abbildung in Anlehnung an Fama und Malkiel (1970)]

Die direkte Überprüfung der Markteffizienz ist an und für sich nicht möglich. Es kann jedoch getestet werden, zu welchem Grad Informationen in Marktpreisen reflektiert werden, was wiederum Aufschluss über die Markteffizienz geben kann. Dem ist hinzuzufügen, dass Tests im Zusammenhang mit der Markteffizienz dem Problem der Verbundhypothese unterliegen. Falls die Nullhypothese eines effizienten Marktes abgelehnt wird, bedeutet dies entweder, dass der Markt ineffizient oder das unterstellte Bewertungsmodell falsch ist [vgl. Fama (1991)].³⁵

³⁴ Anlagestrategie bei der eine Geldanlage investiert und langfristig gehalten wird.

³⁵ Siehe Abbildung 6.

Die RWH, die als Basis für die EMH dient, bietet sich zum Test der schwachen Informationseffizienz der EMH an und wird in dieser Arbeit zur Analyse von BTC verwendet werden. Der folgende Abschnitt geht auf die theoretischen und methodischen Grundlagen der RWH ein.

2.4.4 Random-Walk-Hypothese

Gegenstand der RWH ist es, zu evaluieren ob aufeinanderfolgende Preisdaten seriell korreliert sind. Falls keine Korrelation besteht, kann die Annahme schwacher Informationseffizienz nicht abgelehnt werden.³⁶ Somit können historische Preise nicht zur Prognose verwendet werden und der aktuelle Preis ist der beste Schätzer für den zukünftigen Preis. Campbell et al. (1997) unterscheiden drei Versionen des RWs³⁷ wobei folgende Beziehung für alle drei Versionen gilt und strengere Versionen der RWH schwächere Versionen miteinschließen.

$$\text{Cov}[f(r_t), g(r_{t+k})] = 0$$

- $f(\cdot)$ und $g(\cdot)$ sind zwei beliebige Funktionen.
- r_t und r_{t+k} stellen Renditen zu zwei verschiedenen Zeitpunkten $t \in \mathbb{N}$ und $r \in \mathbb{N}^+$ dar.

Es wird zwischen den verschiedenen Versionen unterschieden, je nachdem welche Eigenschaften durch $f(\cdot)$ und $g(\cdot)$ erfüllt werden. Des Verständnisses halber wird zunächst das RW-Grundmodell vorgestellt, bevor auf die einzelnen Versionen eingegangen wird. Das Grundmodell des RW lässt sich wie folgt darstellen:

$$P_t = \mu + P_{t-1} + \epsilon_t$$

Der zukünftige Preis P_t formiert sich aus dem aktuellen Preis P_{t-1} , der erwarteten Preisänderung³⁸ μ und dem Zufallsterm ϵ_t .

Die RW₁H, welche die strengsten Anforderungen hat, besagt, dass der Zufallsterm unabhängig und gleichverteilt ist und dessen Erwartungswert Null beträgt. Unter der RW₂ H wird die Bedingung, dass der Zufallsterm gleichverteilt sein muss, gelockert. Campbell et al. (1997) erklären, dass die Annahme eines gleichverteilten Zufallsterms nicht plausibel sei für lange Zeithorizonte und nennen die 200-jährige Geschichte der New York Stock Exchange als Beispiel. In solch langen Zeithorizonten verändern sich Rahmenbedingungen des Marktes bezüglich ökonomischer, sozialer, institutioneller und regulatorischer Aspekte. Unter der RW₃H wird schliesslich auch die Unabhängigkeitsbedingung des Zufallsterms gelockert. Der RW₃

³⁶ Der Umkehrschluss gilt jedoch nicht: Schwache Informationseffizienz impliziert nicht, dass Preise einem RW folgen [vgl. Fama und Malkiel (1970)]

³⁷ RW₁, RW₂ und RW₃, wobei RW₃ die schwächste Form eines RWs darstellt.

³⁸ Wird in der Fachliteratur als *drift* bezeichnet.

erlaubt von Null verschiedene Kovarianzen zwischen den quadrierten Werten des Zufallsterms zu unterschiedlichen Zeitpunkten.

$$\text{Cov}[\epsilon_t^2, \epsilon_{t-k}^2] \neq 0$$

Zur Überprüfung der verschiedenen RW-Versionen existiert eine Vielzahl statistischer Tests. Im Rahmen dieser Arbeit werden BTC-Renditezeitreihen auf einen RW_1 getestet. Der BTC-Markt ist im Vergleich zu etablierten Finanzmärkten sehr jung. Deshalb wird angenommen, dass der Zufallsterm unabhängig und gleichverteilt ist. Im Abschnitt 2.6.1 wird auf Tests des RW_1 eingegangen.

2.4.5 Random-Walk₁-Tests

Die Bedingungen der RW_1H sind, dass der Zufallsterm unabhängig und gleichverteilt ist und dessen Erwartungswert Null beträgt. Zudem ist der RW_1 ein Prozess, der eine Einheitswurzel besitzt und somit nicht-stationär ist.

Es gibt eine Fülle von statistischen Tests zur Überprüfung des RW_1 , wobei in dieser Arbeit, in Anlehnung an Campbell et al. (1997), lediglich der Run-Test (Iterationstest) verwendet wird.

Eine erste theoretische Ausarbeitung des Run-Modells wurde durch Mood (1940) erstellt, wobei eine Stichprobe, bestehend aus einer fixen Anzahl Beobachtungen, deren Merkmal zwei oder mehr Ausprägungen haben kann. Die Population kann dabei binominal- oder multinominalverteilt sein. Campbell et al. (1997) verwenden zur Untersuchung von Preisdaten, die Rendite als Merkmal, das zwei Ausprägungen haben kann – positiv oder negativ. Die angenommene Population ist folglich binominalverteilt. Unter einem Run (Iteration) wird die Folge einer Ausprägung verstanden, welcher keine oder eine andere Ausprägung vorangeht oder folgt. Bei der Betrachtung von zehn Renditen beispielsweise, könnte die zu analysierende Sequenz wie folgt aussehen:

+ - - + + + - + - -

In diesem Fall existieren total sechs Runs, die sich zusammensetzen aus drei Runs von (+) mit der Länge Eins, Drei und Eins und drei Runs von (-) mit der Länge Zwei, Eins und Zwei. Die folgende Sequenz hingegen besteht aus zwei Runs, die sich aus einem Run von (+) und einem Run von (-) zusammensetzen, jeweils der Länge Fünf:

- - - - - + + + + + +

Um diese Reihen auf einen RW zu testen, werden sie mit der erwarteten Anzahl Runs eines RWs verglichen. Sollte tatsächlich ein RW bestehen, ist keine Regelmässigkeit erkennbar – es sind weder übermässig viele, noch sehr wenige Runs zu erkennen [vgl. Trenkler und Büning (1994)].

3. Empirischer Teil

3.1 Folgen Renditen von Bitcoins einem Random-Walk?

Wie bereits erwähnt, bezeichnet Shiller (2014) BTC als ein ausgezeichnetes Beispiel einer Spekulationsblase. Er begründet, dass BTC-Preise stark durch die Medienpräsenz von BTC beeinflusst und dass BTCs nur unter der Erwartung eines Preisanstieges gehalten werden.

Dass BTC-Preise mit der Medienpräsenz von BTC korrelieren, wurde auch durch Ciaian et al. (2014) bestätigt. Ferner konnte Kristoufek (2013) feststellen, dass BTC-Preise auch mit der Nutzung von Suchmaschinen zusammenhängen.

Diese Resultate deuten darauf, dass BTC die mittelstarke Informationsineffizienz nicht erfüllt. Hauptinteresse der vorliegenden Arbeit ist die Überprüfung der schwachen Informationseffizienz. Falls die schwache Informationseffizienz abgelehnt wird, könnten auch die höheren Grade der Informationseffizienz abgelehnt werden und bisherige Preiszusammenbrüche sind prognostizierbar gewesen.

Fama stellt die Existenz von Preisblasen deshalb in Frage weil diese auf effizienten Märkten nicht vorhergesagt werden können [vgl. Cassidy (2010)]. Damit also die Existenz von Preisblasen auf dem BTC-Markt bestätigt werden kann, sollten BTC-Preise vorhersehbar sein. Im Folgenden wird anhand einer Regressionsanalyse und des Run-Tests der RW_1 getestet. Die Nullhypothese lautet, dass ein RW_1 nicht abgelehnt werden kann. Falls der RW_1 nicht abgelehnt wird, kann auch die schwache Informationseffizienz nicht abgelehnt werden. Dies bedeutet, dass unter dem RW_1 Renditeprognosen anhand historischer Daten nicht möglich sind.

3.2 Daten

Nach Wang et al. (1995) ist die Datenqualität essentiell, um ein repräsentatives Bild des Untersuchungsgegenstandes zu gewinnen. Im Zusammenhang mit BTC ist zwar eine Fülle von Preisdaten verfügbar, deren Datenqualität ist jedoch nicht in jedem Fall sichergestellt. Deshalb wurde bei der Wahl der Datenquelle darauf geachtet, dass konzeptionelle Rahmenbedingungen im Bezug zur Datenqualität erfüllt werden. Daten müssen verfügbar, interpretierbar, relevant und zuverlässig sein. Auf folgender Seite werden die Rahmenbedingungen in Bezug auf BTC analysiert.

- Verfügbarkeit BTC-Preisdaten sind auf verschiedenen BTC-Wechselstuben frei verfügbar. Problematisch ist jedoch, dass Wechselstuben nicht gleichzeitig in Betrieb genommen wurden und auch viele den Betrieb bereits eingestellt haben.
- Interpretierbarkeit Hierbei wurden Daten auf Verständlichkeit, Konsistenz und Prägnanz geprüft. Daten sind auf allen grösseren Wechselstuben leicht verständlich und übersichtlich. Kursdaten sind verfügbar als Geld-/Briefkurs und sind notiert in verschiedenen Fiat-Währungen.
- Relevanz Im Rahmen dieser Arbeit ist es wichtig, Preisdaten zu verwenden, die für den gesamten BTC-Markt repräsentativ sind. Es ist fraglich, ob Preisdaten einer einzigen Wechselstube geeignet sind, um globale Zusammenhänge zu verstehen. Durchschnittspreise machen in diesem Zusammenhang mehr Sinn.
- Zuverlässigkeit Da BTC-Preise nur sehr beschränkt gesetzlicher Kontrolle unterliegen, ist es wichtig, dass Preisdaten von Anbietern stammen, deren Reputation hoch ist. Somit kann davon ausgegangen werden, dass Preisdaten nicht manipuliert wurden.

Die verwendeten Preisdaten zur Analyse stammen aus der Online-Datenbank von CoinDesk³⁹ und wurden als .CSV heruntergeladen [vgl. o.A. (2014a)]. Der Datensatz zur Analyse besteht aus täglichen Schlusskursen in USD und reicht vom 18. Juli 2010 bis zum 24. Juli 2014.⁴⁰ Dies sichert die Interpretierbarkeit und Verfügbarkeit der Daten. Des Weiteren sind Preise in Form des BPI notiert, welcher als Durchschnitt des Mittelpunktes der Geld-/ Briefspanne führender BTC-Wechselstuben berechnet wird. Folgende Kriterien müssen erfüllt werden, damit Preisdaten einer Wechselstube in die Berechnung des BPI miteinbezogen werden. Anbieter müssen über eine internationale Nutzergemeinschaft verfügen, Angaben zu Geld-/Briefkursen machen, Transaktionsvolumina unter 1 500 USD erlauben, ein ausreichend grosses Handels-

³⁹ CoinDesk ist der grösste Datenanbieter für BTC-Marktinformationen [vgl. Popper (2014)].

⁴⁰ Der Datensatz besteht aus 1468 Beobachtungen und Preise sind auf vier Nachkommastellen genau angegeben.

volumen haben und Transaktionen innert höchstens sieben Werktagen abwickeln. Diese Kriterien sichern die Zuverlässigkeit der Preisdaten. Da der Markt global betrachtet wird – Kriterium einer internationalen Nutzergemeinschaft – ist auch die Rahmenbedingung der Relevanz gewährleistet.

3.3 Methoden

Der empirische Teil dieser Arbeit hat zum Ziel, herauszufinden, ob abgelehnt werden kann, dass BTC-Renditen einem RW_1 folgen und ob dementsprechend auch die schwache Informationseffizienz abgelehnt werden kann. Um dies zu analysieren, wird anhand einer robusten Regressionsanalyse⁴¹ der lineare Zusammenhang aufeinanderfolgender Renditen untersucht. Anschliessend wird der Run-Test durchgeführt um zu prüfen, ob die Nullhypothese – Renditen folgen einem RW_1 – verworfen werden kann. Sämtliche Analysen werden mit der Statistiksoftware STATA13 durchgeführt. Die Preisdaten werden zunächst in STATA13 importiert und entsprechend angepasst. Anschliessend wird die Variable *lnPreis* generiert, indem die Variable *Preis* logarithmiert wird. Aus den logarithmierten Preisen wird anschliessend die Variable *lnRendite* berechnet. Die Verwendung der logarithmierten Rendite⁴² (*logRendite*) hat im Zusammenhang mit der RW_1 -Analyse mehrere Vorteile gegenüber der diskreten Rendite. Die *logRendite* ist im Gegensatz zur diskreten Rendite symmetrisch. Daraus resultiert, dass unter der Annahme log-normalverteilter Preise auch deren *logRendite* log-normalverteilt sind. Ferner sind auch Renditen für längere Zeithorizonte log-normalverteilt [vgl. Agrawal und Thankachan (2013)].

$$Rendite_t = \frac{Preis_t}{Preis_{t-1}} - 1$$

$$\ln Rendite_t = \ln(Rendite_t + 1) = \ln Preis_t - \ln Preis_{t-1} = \ln \left(\frac{Preis_t}{Preis_{t-1}} \right)$$

Um die Regressionsanalyse und den Run-Test über verschiedene Zeithorizonte auszuführen, werden mit folgender Formel wöchentliche und monatliche Renditen berechnet [vgl. Zivot (2011)].

$$\ln Rendite_{Zeithorizont=n} = \frac{1}{n} \sum_{t=1}^{t=n} \ln Rendite_t$$

⁴¹ Es wird die robuste Regressionsanalyse verwendet, um Schwächen der klassischen Regression gegen Ausreisser und Heteroskedastizität zu umgehen [vgl. Draper und Smith (1981)]

⁴² Wird auch geometrische oder stetige Rendite genannt.

Bei der Berechnung der wöchentlichen Rendite wurde der Wochenanfang jeweils auf Mittwoch gesetzt, um Effekte der Marktmikrostruktur zu verringern [vgl. Topalov (2013)].

3.3.1 Regressionsanalyse

Im Rahmen der robusten Regressionsanalyse wurden die Zielvariable $\ln Rendite_t$ und die Einflussvariable $\ln Rendite_{t-Lag}$ gewählt.

$$\ln Rendite_t = \beta_0 + \beta_1 \ln Rendite_{t-1} + \beta_2 \ln Rendite_{t-2} + \dots + \beta_{Lag} \ln Rendite_{t-Lag} + \epsilon_t$$

Nachdem die robuste Regression mit STATA13 durchgeführt wurde, kann anhand der Nullhypothese, $H_0 =$ Regressionskoeffizient $\beta_{...}$ ist gleich Null, überprüft werden, ob $\ln Rendite_t$ und $\ln Rendite_{t-Lag}$ seriell korreliert sind. Damit die Nullhypothese auf dem Signifikanzniveau von fünf Prozent abgelehnt werden kann, muss der p-Wert kleiner sein als 0.05. Ferner werden jeweils Eins bis n - Lags⁴³ untersucht.

3.3.2 Run-Test

Die Variable $\ln Rendite_t$ wird anhand des Run-Tests nach Swed und Eisenhart (1943)⁴⁴ auf einen RW_1 überprüft. Wobei folgende Ausprägungen unterschieden werden und die Sequenz auf Basis der Zeit gebildet wird.

$$\mathcal{N}_{negativ} := \{\ln Rendite_t \leq 0\}$$

$$\mathcal{N}_{positiv} := \{\ln Rendite_t > 0\}$$

Falls $\ln Rendite_t$ den Wert 0 annimmt, wird diese Beobachtung bei der Analyse ignoriert. Dies ist sinnvoll, da sonst die Sequenz $+ 0 + 0$ als zwei Runs und die Sequenz $- 0 - 0$ als ein Run interpretiert würde. Die Nullhypothese – Rendite Zeitreihen sind zufällig und folgen einem RW_1 – wird überprüft, indem die Anzahl beobachteter und erwarteter Runs verglichen wird. Die Nullhypothese wird abgelehnt, falls sich diese signifikant unterscheiden. Die Nullhypothese wird auf dem Signifikanzniveau von fünf Prozent abgelehnt, falls der p-Wert kleiner ist als 0.05. Der Run-Test wird durchgeführt für auf täglichen, wöchentlichen und monatlichen Renditen basierenden Sequenzen.

⁴³ Die Wahl von n wird anhand des Bayesschen-Informationskriteriums (BIC) determiniert. Im Rahmen dieser Arbeit wird nicht weiter auf die Funktionsweise dieses Verfahrens eingegangen. Für weitere Informationen wird auf Gideon Schwarz (1978) verwiesen.

⁴⁴ Der Run-Test nach Swed und Eisenhart (1943) basiert auf jenem von Wald und Wolfowitz (1943), wobei einige Verbesserungen, bezüglich Kontinuität und kritischer Werte, angefügt wurden.

3.4 Ergebnisse

3.4.1 Regressionsanalyse

Für tägliche, wöchentliche und monatliche logRenditen wurde die Analyse für bis zu zwei Lags durchgeführt, da das BIC ab einem Lag für alle Zeitfenster anstieg. Die Nullhypothese kann auf dem Signifikanzniveau von fünf Prozent für keinen der Lags abgelehnt werden. Für tägliche, wöchentliche und monatliche Renditedaten ist der p-Wert grösser als das α -Niveau von 0.05. Demnach mit der Regressionsanalyse keine serielle Korrelation zwischen $Rendite_t$ und $Rendite_{t-1,2}$ nachgewiesen werden. Dem ist hinzuzufügen, dass das BIC bei der Analyse wöchentlicher Renditen nur schwache Evidenz aufweist [vgl. Burnham und Anderson (2002)]. Das BIC ist um 1.45 angestiegen, wohingegen bei täglichen und monatlichen Renditen ein Anstieg von ungefähr fünf zu verzeichnen war. Eine detaillierte Ansicht der Ergebnisse ist im Anhang unter dem Titel Regressionsanalyse zu sehen.

3.4.2 Run-Test

Für tägliche logRenditen wurden 699 Runs ermittelt. Auf dem Signifikanzniveau von fünf Prozent ist die ermittelte Anzahl Runs nicht von der erwarteten Anzahl Runs (715.36) verschieden. Der p-Wert beträgt 0.384 und ist grösser als das α -Niveau von 0.05.

Für wöchentliche logRenditen wurden 87 Runs ermittelt. Auf dem Signifikanzniveau von fünf Prozent ist die ermittelte Anzahl Runs nicht von der erwarteten Anzahl Runs (100.50) verschieden. Der p-Wert beträgt 0.501 und ist grösser als das α -Niveau von 0.05.

Für monatliche logRenditen wurden 19 Runs ermittelt. Auf dem Signifikanzniveau von fünf Prozent ist die ermittelte Anzahl Runs nicht von der erwarteten Anzahl Runs (23.78) verschieden. Der p-Wert beträgt 0.137 und ist grösser als das α -Niveau von 0.05.

Für alle untersuchten logarithmierten Renditedaten kann die Nullhypothese nicht verworfen werden.

4. Schluss

Dieser Arbeit legt dar, weshalb BTC zurzeit nicht als Währung geeignet ist. Ferner konnte mittels einer empirischen Analyse von BTC-Renditen gezeigt werden, dass diese einem RW_1 folgen. Im Zuge des empirischen Teils wurden tägliche, wöchentliche und monatliche BTC-Renditen anhand einer Regressionsanalyse und des Run-Tests analysiert.

Die Regressionsanalyse hat ergeben, dass die Regressionskoeffizienten auf einem α -Niveau von 0.05 weder für einen noch für zwei Lags von Null verschieden sind. Daraus ergibt sich, dass nicht abgelehnt werden kann, dass BTC-Renditen einem RW_1 folgen.

Konsistent mit diesem Ergebnis hat auch der Run-Test ergeben, dass auf einem α -Niveau von 0.05 kein Unterschied zwischen der beobachteten Anzahl Runs und der erwarteten Anzahl Runs unter einem RW_1 besteht. Folglich kann auch hier nicht abgelehnt werden, dass BTC-Renditen einem RW_1 folgen.

Im Rahmen der angewandten Tests war es Marktteilnehmern bisher nicht möglich, Renditen aufgrund historischer Preisdaten gewinnbringend zu prognostizieren, da diese zufällig um Null fluktuieren. Dementsprechend kann im Zusammenhang mit der EMH von schwacher Informationseffizienz ausgegangen werden.

Diese Arbeit kann nicht beantworten ob BTC-Marktpreise durch spekulative Investitionen dominiert werden oder welches die Motive der Investoren sind. Nach Shiller (2014) ist BTC ein ausserordentliches Beispiel einer Spekulationsblase, wohingegen Fama die Existenz von Spekulationsblasen in Frage stellt, da diese nicht prognostizierbar seien [vgl. Cassidy (2010)]. Aufbauend auf diesen Ansichten, zeigt die Annahme der schwachen Informationseffizienz auf dem BTC-Markt, dass Spekulationsblasen – falls BTC eine Spekulationsblase ist – nicht zwingendermassen Markteffizienz ausschliessen. Auch Timmermann und Granger (2004) zeigen, dass die Analyse von Renditen im Zusammenhang mit der EMH keinen Widerspruch zu Spekulationsblasen bilden. Der Zusammenhang zwischen dem intrinsischen Wert und dem Preis eines Gutes ist nicht unabdingbar.

Für die zukünftige Forschung ist BTC ein gehaltvolles Thema zur Untersuchung der EMH. Diese Arbeit beschränkte sich dabei auf zwei Tests des RW_1 , wobei weitere Tests Raum für Erkenntnisse bieten würden. Ferner wäre auch die empirische Analyse der mittelstarken Informationseffizienz wichtig, da bestehende Literatur zeigt, dass BTC-Preise stark mit öffentlichen Informationen korrelieren [vgl. Buchholz et al. (2012), Kristoufek (2013)]. Bislang wurde jedoch nicht untersucht, ob diese Korrelation im Widerspruch zur Markteffizienz steht.

5. Anhang

Regressionen Abschnitt 2.3.2

| <i>Zielvariable</i> | <i>Einflussvariable</i> | β | t | $P > t $ | R^2 |
|------------------------------|-------------------------|-----------|---------|-----------|--------|
| Kumulierte Anzahl
BTCs | Zeitpunkt | 6492.665 | 265.87 | 0.000 | 0.9797 |
| | (Konstante) | -1.16e+08 | -246.49 | 0.000 | |
| Historische Volati-
lität | Zeitpunkt | -.0000261 | -11.73 | 0.000 | 0.0868 |
| | (Konstante) | .55969 | 13.10 | 0.000 | |

Regressionsanalyse

| Zielvariable | | Einflussvariable | β | t | $P > t $ | R^2 | BIC |
|--------------|-----------------|---------------------|-----------|-------|-----------|--------|--------|
| täglich | $\ln Rendite_t$ | $\ln Rendite_{t-1}$ | .0466885 | 0.89 | 0.373 | 0.0022 | 4.090 |
| | | (Konstante) | .0057967 | 3.04 | 0.002 | | |
| täglich | $\ln Rendite_t$ | $\ln Rendite_{t-1}$ | .0473605 | 0.91 | 0.364 | 0.0030 | 10.156 |
| | | $\ln Rendite_{t-2}$ | -.0300291 | -0.68 | 0.497 | | |
| | | (Konstante) | .0060304 | 3.16 | 0.002 | | |
| wöchentlich | $\ln Rendite_t$ | $\ln Rendite_{t-1}$ | .0658413 | 0.40 | 0.691 | 0.0044 | 4.427 |
| | | (Konstante) | .005939 | 2.91 | 0.004 | | |
| wöchentlich | $\ln Rendite_t$ | $\ln Rendite_{t-1}$ | .0560021 | 0.35 | 0.723 | 0.0229 | 5.877 |
| | | $\ln Rendite_{t-2}$ | .1362905 | 1.38 | 0.169 | | |
| | | (Konstante) | .0051716 | 2.95 | 0.004 | | |
| monatlich | $\ln Rendite_t$ | $\ln Rendite_{t-1}$ | .2399516 | 1.39 | 0.172 | 0.0601 | 0.896 |
| | | (Konstante) | .0048034 | 2.21 | 0.032 | | |
| monatlich | $\ln Rendite_t$ | $\ln Rendite_{t-1}$ | .2265818 | 1.19 | 0.239 | 0.0534 | 5.120 |
| | | $\ln Rendite_{t-2}$ | .0151978 | 0.13 | 0.897 | | |
| | | (Konstante) | .004893 | 2.11 | 0.041 | | |

Run-Test*lnRendite_t* (täglich)

| | |
|---|--------|
| $ \mathcal{N}_{negativ} := \{lnRendite_t \leq 0\} $ | 654 |
| $ \mathcal{N}_{positiv} := \{lnRendite_t > 0\} $ | 787 |
| Stichprobenumfang | 1441 |
| Runs | 699 |
| Erwartete Anzahl Runs | 715.36 |
| z | -.87 |
| Prob> z | 0.384 |

lnRendite_t (wöchentlich)

| | |
|---|--------|
| $ \mathcal{N}_{negativ} := \{lnRendite_t \leq 0\} $ | 84 |
| $ \mathcal{N}_{positiv} := \{lnRendite_t > 0\} $ | 122 |
| Stichprobenumfang | 206 |
| Runs | 87 |
| Erwartete Anzahl Runs | 100.50 |
| z | -1.95 |
| Prob> z | 0.051 |

lnRendite_t (monatlich)

| | |
|---|-------|
| $ \mathcal{N}_{negativ} := \{lnRendite_t \leq 0\} $ | 18 |
| $ \mathcal{N}_{positiv} := \{lnRendite_t > 0\} $ | 31 |
| Stichprobenumfang | 49 |
| Runs | 19 |
| Erwartete Anzahl Runs | 23.78 |
| z | -1.49 |
| Prob> z | 0.137 |

6. Literaturverzeichnis

- Agrawal, C., Thankachan, D., 2013. Calculating Investment Returns, Texas.
- Ahamad, S., Varghese, M., 2013. A Survey on Crypto Currencies, Bangalore.
- Al-Khazali, O., Koumanakos, E., 2011. Empirical testing of random walk of Euro exchange rates. Evidence from the emerging markets. *Journal of Business & Economics Research (JBER)* 4 (4).
- Ametrano, F.M., 2014. Hayek Money: The Cryptocurrency Price Stability Solution. SSRN Electronic Journal.
- Amman, M., 2013. Wirtschaftsnobelpreis 2013: Effiziente Märkte und irrationale Investoren. <http://www.nzz.ch/aktuell/wirtschaft/wirtschaftsnachrichten/effiziente-maerkte-und-irrationale-investoren-1.18169309>, 7. August 2014.
- Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., 2013. Evaluating User Privacy in Bitcoin. In: *Financial Cryptography and Data Security*, Vol. 7859. Springer, S. 34ff.
- Azad, A.S., 2009. Random walk and efficiency tests in the Asia-Pacific foreign exchange markets: Evidence from the post-Asian currency crisis data. *Research in International Business and Finance* 23 (3), 322–338.
- Barker, J., 2014. Why Is Bitcoin's Value So Volatile? <http://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp>, 26. Mai 2014.
- Bartle, R., 2004. PITFALLS OF VIRTUAL PROPERTY, Noth Carolina.
- Berthoud, J., Friedman, M., 1999. Anti-Trust and the Internet. National Taxpayers Union, o.O.
- Bitlegal, 2014. Legal Status. <http://www.bitlegal.io/list.php>, 26. Mai 2014.
- blockr.io, 2014. Transaction Trivia. <https://btc.blockr.io/trivia/block>, 26. Juli 2014.
- Bris, A., Cantale, S., 2013. Efficient Market vs Behavioral Finance. <http://www.imd.org/news/Efficient-Market-vs-Behavioral-Finance.cfm>, 7. August 2014.
- Brunetti, A., 2012. Wirtschaftskrise ohne Ende? US-Immobilienkrise, Globale Finanzkrise, Europäische Schuldenkrise. hep Verlag, Bern.
- Buchholz, M., Delaney, J., Warren, J., 2012. Bits and Bets. Information, Price Volatility, and Demand for Bitcoin, Oregon.

- Burnham, K.P., Anderson, D.R., 2002. Model selection and multimodel inference. A practical information-theoretic approach. Springer, New York NY u.a.
- Campbell, J.Y., Lo, A.W., MacKinlay, A.C., 1997. The econometrics of financial markets. Princeton Univ. Press, Princeton NJ u.a.
- Cassidy, J., 2010. Interview with Eugene Fama. <http://www.newyorker.com/news/john-cassidy/interview-with-eugene-fama>, 11. August 2014.
- Chung, D., Hrazdil, K., 2010. Liquidity and market efficiency: A large sample study. *Journal of Banking & Finance* 34 (10), 2346–2357.
- Ciaian, P., Rajcaniova, M., Kancs, d., 2014. The Economics of BitCoin Price Formation. arXiv preprint arXiv:1405.4498.
- CoinMKTCap, 2014. Crypto-Currency Market Capitalizations. <https://coinmarketcap.com/>, 22. Mai 2014.
- Conway, B., 2014. Gold As a Currency? It's More Volatile Than the Peso - Focus on Funds. <http://blogs.barrons.com/focusonfunds/2013/02/28/gold-as-a-currency-its-more-volatile-than-the-peso/>, 28. Mai 2014.
- Conway, E., 2011. Währungen und Wechselkurse. In: Conway, E. (Ed.), 50 Schlüsselideen Wirtschaftswissenschaft. Spektrum Akademischer Verlag; Imprint: Spektrum Akademischer Verlag, Heidelberg, S. 94-97ff.
- Cornell, W. Bradford, Dietrich, J. Kimball, 1978. The Efficiency of the Market for Foreign Exchange Under Floating Exchange Rates. *The Review of Economics and Statistics* 60 (1), 111–120.
- Dangl, T., 1999. Adaptive Erwartungsbildung und Finanzmarktdynamik. Vienna University of Economics and Business Administration, Wien.
- Daske, S., 2002. Winner-Loser-Effekte am deutschen Aktienmarkt. <http://hdl.handle.net/10419/65290>.
- Douceur, J., Douceur, J.R., 2002. The Sybil Attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (Eds.), Peer-to-peer systems. First international workshop, Cambridge, MA, USA, March 7 - 8, 2002 ; revised papers, Vol. 2429. Springer Berlin Heidelberg; Springer, Berlin [u.a.], S. 251-260 // 251–260ff.
- Draper, N.R., Smith, H., 1981. Applied regression analysis. Wiley, New York NY u.a.
- Economic Sciences Prize Committee, 2013. Understanding Asset Prices. Scientific Background on the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2013. THE ROYAL SWEDISH ACADEMY OF SCIENCES, Stockholm.

- Eisenberg, C., 2014. Crypto Coins List. <https://www.cryptocoincharts.info/v2/coins/info>, 3. Juni 2014.
- Europäische Zentralbank, 2012. Virtual Currency Schemes. <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, 27. Februar 2014.
- Fahey, D., 2014. Notice 2014-21. Internal Revenue Service.
- Fama, E.F., 1965. Random Walks in Stock Market Prices. *Financial Analysts Journal* 21 (5), 55–59.
- Fama, E.F., 1991. Efficient Capital Markets: II. *The Journal of Finance* 46 (5), 1575–1617.
- Fama, E.F., 1998. Market efficiency, long-term returns, and behavioral. *Journal of Financial Economics* 49 (3), 283–306.
- Fama, E.F., Malkiel, B.G., 1970. EFFICIENT CAPITAL MARKETS: A REVIEW OF THEORY AND EMPIRICAL WORK*. *The Journal of Finance* 25 (2), 383–417.
- Ferber, M., 2009. Finanz-Blasen und der effiziente Markt. <http://www.nzz.ch/aktuell/wirtschaft/uebersicht/finanz-blasen-und-der-effiziente-markt-1.3190224>, 4. August 2014.
- FINMA, 2014. Wie sich Anleger gegen unerlaubt tätige Finanzmarktanbieter schützen können, Bern.
- GHOSH, D., LEVIN, E.J., MACMILLAN, P., WRIGHT, R.E., 2004. GOLD AS AN INFLATION HEDGE? *Studies in Economics and Finance* 22 (1), 1–25.
- Gideon Schwarz, 1978. Estimating the Dimension of a Model. *The Annals of Statistics* 6 (2), 461–464.
- Grothaus, M., 2014. How To Create Your Own Cryptocurrency. <http://www.fastcolabs.com/3025700/how-to-create-your-own-cryptocurrency>, 27. Juli 2014.
- Hayek, F.A., 1990. Denationalisation of money: the argument refined. Ludwig von Mises Institute, London.
- Heid, A., 2013. Analysis of the Cryptocurrency Marketplace, Florida.
- Heri, E.W., 1982. Bestimmungsgründe kurzfristiger Wechselkursfluktuationen. Eine empirische Analyse flexibler Wechselkurse unter besonderer Berücksichtigung der Theorie und Empirie effizienter Märkte. Diss. Staatswiss. Basel. (AB). s.n, S.l.

- Hern, A., 2014. Bitcoin me: How to make your own digital currency.
<http://www.theguardian.com/technology/2014/jan/07/bitcoin-me-how-to-make-your-own-digital-currency>, 27. Juli 2014.
- Honsell, H. (Ed.), 2010. Römisches Recht. Springer Berlin Heidelberg, Berlin.
- Kaskaloglu, K. (Ed.), 2014. Near Zero Bitcoin Transaction Fees Cannot Last Forever. The Society of Digital Information and Wireless Communication, Istanbul.
- Kelly, B., 2014. How I created my own bitcoin-like currency.
<http://www.cnn.com/id/101573131#>, 27. Juli 2014.
- Kristoufek, L., 2013. BitCoin meets Google Trends and Wikipedia: quantifying the relationship between phenomena of the Internet era. Scientific reports 3, 3415.
- Kristoufek, L., 2014. What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis, Prague.
- Krugman, P., 2014. Bitcoin is Evil.
http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_php=true&_type=blogs&_r=0, 22. Mai 2014.
- Krugman, P.R., 1984. The international role of the dollar: theory and prospect. In: Exchange rate theory and practice. University of Chicago press, S. 261ff.
- Kuster, P., 2010. Braucht es ein neues Geld- und Währungssystem? Impressionen von den Hayek-Tagen – Vertrauen in Europäische Zentralbank als Stabilitätshüter ist verdampft. Finanz und Wirtschaft 2010.
- Leslie, L., Robert, S., Marshall, P., 1982. The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 4 (3), 382–401.
- Mataro, E., 2014. Bitcoin trading needs bank liquidity, says Saxo chief.
<http://www.fxweek.com/fx-week/interview/2344056/bitcoin-trading-needs-bank-liquidity-says-saxo-chief>, 21. August 2014.
- Meier, M., 2013. Ein Nobelpreis für zwei Rivalen. Tages-Anzeiger.
- Miller, R., Zumburn, J., Magnusson, N., 2013. Fama, Shiller, Hansen Win Nobel Prize for Asset-Price Work. <http://www.bloomberg.com/news/2013-10-14/fama-hansen-shiller-share-nobel-economics-prize-academy-says.html>, 11. August 2014.
- Mood, A.M., 1940. The Distribution Theory of Runs. The Annals of Mathematical Statistics 11 (4), 367–392.
- Moore, T., Christin, N., 2013. Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In: Financial Cryptography and Data Security. Springer, S. 25ff.

- Muth, J.F., 1961. Rational Expectations and the Theory of Price Movements. *Econometrica* 29 (3), 315–335.
- Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Consulted 1, 2012.
- o.A., 2014a. About the Bitcoin Price Index. <http://www.coindesk.com/price/bitcoin-price-index/>, 30. August 2014.
- o.A., 2014b. How can I buy bitcoins? <http://www.coindesk.com/information/how-can-i-buy-bitcoins/>, 27. Mai 2014.
- Piekenbrock, D., 2010. Gabler Kompakt-Lexikon Wirtschaft. 4500 Begriffe nachschlagen, verstehen, anwenden. Gabler, Wiesbaden.
- Poppen, S., 2010. Makroökonomische Theorierichtungen nach Keynes, Münster.
- Popper, N., 2014. Winklevoss Brothers Offer an Index to Track Price of Bitcoin. <http://mobile.nytimes.com/blogs/dealbook/2014/02/19/before-a-bitcoin-fund-comes-a-price-index/>, 31. August 2014.
- Reid, F., Harrigan, M., 2011. An Analysis of Anonymity in the Bitcoin System. arXiv preprint arXiv:1107.4524.
- Robinson, M., 2014. Making Your Own Cryptocurrency Has Never Been Easier. <http://motherboard.vice.com/blog/making-your-own-cryptocurrency-has-never-been-easier>, 27. Juli 2014.
- Sattler, T., Walter, S., 2008. Wirtschaftspolitischer Handlungsspielraum im Zeitalter der Globalisierung. Eine empirische Untersuchung am Beispiel von Währungskrisen. *Politische Vierteljahresschrift* 49 (3), 464–490.
- Sewell, M.V., 2012. The Efficient Market Hypothesis: Empirical Evidence. *International Journal of Statistics and Probability* 1 (2).
- Shiller, R.J., 1981. The Use of Volatility Measures in Assessing Market Efficiency. *The Journal of Finance* 36 (2), 291.
- Shiller, R.J., 2003. From Efficient Markets Theory to Behavioral Finance. *The Journal of Economic Perspectives* 17 (1), 83–104.
- Shiller, R.J., 2014. In Search of a Stable Electronic Currency. *The New York Times*, 4.
- Shiller, R.J., Fischer, S., Friedman, B.M., 1984. Stock Prices and Social Dynamics. *Brookings Papers on Economic Activity* 1984 (2), 457.
- Shleifer, A., 2000. Inefficient markets. An introduction to behavioral finance. Oxford University Press, Oxford, New York.
- Söllner, F., 1999. Die Geschichte des ökonomischen Denkens. Springer, Berlin.

- Stevenson, A., Lindberg, C.A., 2010. New Oxford American dictionary. Oxford University Press, Oxford, New York.
- Stevenson, J., 2013. Bitcoins, litecoins, what coins?: A global phenomenon. John Stevenson, o.O.
- Šurda, P., 2012. Economics of Bitcoin: Is Bitcoin an alternative to fiat currencies and gold. WU Vienna University of Economics und Business: Wien.
- Swed, F.S., Eisenhart, C., 1943. Tables for Testing Randomness of Grouping in a Sequence of Alternatives. *The Annals of Mathematical Statistics* 14 (1), 66–87.
- Tilborg, Henk, 2000. Fundamentals of cryptology. A professional reference and interactive tutorial. Kluwer Academic Publishers, Boston.
- Timmermann, A., Granger, C.W., 2004. Efficient market hypothesis and forecasting. *International journal of forecasting* 20 (1), 15–27.
- Topalov, M., 2013. Die Wahrnehmung von Dividenden durch Finanzvorstände. Eine empirische Untersuchung zu den Determinanten der Dividendenpolitik in der Bundesrepublik Deutschland. Springer Fachmedien Wiesbaden, Wiesbaden.
- Trenkler, G., Büning, H., 1994. Nichtparametrische statistische Methoden. De Gruyter, Berlin.
- Van, T., 2014. Bitcoin Now on Bloomberg. <http://www.bloomberg.com/now/2014-04-30/bitcoin-now-bloomberg/>, 21. August 2014.
- Wald, A., Wolfowitz, J., 1943. An Exact Test for Randomness in the Non-Parametric Case Based on Serial Correlation. *The Annals of Mathematical Statistics* 14 (4), 378–388.
- Wang, Y.R., Strong, D.M., Guarascio, L.M., 1995. Beyond accuracy. What data quality means to data consumers. International Financial Services Research Center, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, Mass.
- Weisenthal, J., 2014. Bitcoin Is An Amazing Example Of A Bubble. <http://www.businessinsider.com/robert-shiller-bitcoin-2014-1>, 7. August 2014.
- Wijk, D., 2013. What can be expected from the Bitcoin?, Rotterdam.
- Zivot, E., 2011. Introduction to Computational Finance and Financial Econometrics [Selbstlernkurs]. <https://www.coursera.org/course/compfinance>.

Selbständigkeitserklärung

„Ich erkläre hiermit, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäss aus Quellen entnommen wurden, habe ich als solche gekennzeichnet. Mir ist bekannt, dass andernfalls der Senat gemäss Artikel 36 Absatz 1 Buchstabe o des Gesetzes vom 5. September 1996 über die Universität zum Entzug des aufgrund dieser Arbeit verliehenen Titels berechtigt ist.“

Ozan Harman