Nick Maximilian Müller

Nickmd3@outlook.com  
Matrikelnummer: 429049

Exposee

In dieser Hausarbeit werde ich die Grundlagen von Kryptowährung erklären, welches Prinzip sich dahinter verbirgt und welche Aussichten diese neue   
Art des Geldes für die Gesellschaft haben könnte.

Kryptowährung

Grundlagen

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Formelverzeichnis

Listings

Abkürzungsverzeichnis

1. Einleitung

2. Grundlagen  
 2.1. Kryptowährung  
 2.2. Blockchain

3. Bitcoin  
 3.1. Geschichte  
 3.2. Eigenschaften von Bitcoin  
 3.2.1. Verteilung von Bitcoin  
 3.2.2. Dezentrales Netzwerk  
 3.2.3. Fälschungssicherheit  
 3.2.4. Transaktionsnachweis  
 3.2.5. Anonymität  
 3.2.6. Unumkehrbarkeit von Transaktionen  
 3.2.7. Sicherheit der Geldbörse  
 3.2.8. Transaktionsgebühren

4. Die Technik hinter Bitcoin  
 4.1. Das Peer-to-Peer-Netz  
 4.2. Der Block  
 4.3. Die Block-Chain  
 4.4. Die Transaktion  
 4.5. Die Wallet  
 4.6. Das Mining  
 4.6.1. Das Mining mit der CPU  
 4.6.2. Das Mining mit der GPU

5. Bitcoin in der Praxis  
 5.1. Wie erhält man Bitcoin  
 5.1.1. Bitcoin geschenkt  
 5.1.2. Bitcoin kaufen  
 5.1.3. Erzeugen von Bitcoin durch Mining  
 5.2. Bezug von Waren und Dienstleistungen mit Bitcoin

6. Bitcoin Heute und Zukünftig  
 6.1. Andere alternative Währungen  
 6.2. Bitcoin und das heutige Geldsystem  
 6.3. Verbesserungsmöglichkeiten von Bitcoin  
 6.4. Hat Bitcoin eine Zukunft?

Anhang

Quellenverzeichnis

Literaturverzeichnis

# Einleitung

Die erste praktische Umsetzung einer Kryptowährung, begann mit der Veröffentlichung des Whitepapers „Bitcoin: A Peer-to-Peer Electronic Cash System“ von Satoshi Nakamoto im Jahre 2009, besser bekannt als „Bitcoin“.   
Durch das Fundament der Kryptowährung Bitcoin, führten aufbauende Entwicklungen zu neuen Nutzungsmöglichkeiten der „Blockchain“ als eigenständige Technologie.   
Die vorliegende Ausarbeitung im Rahmen der Hausarbeit befasst sich mit den Grundlagen der Kryptowährung und seinem Zukunftspotential. Insbesondere wird dabei die Kryptowährung Bitcoin untersucht. Das Ziel der Ausarbeitung ist es, zunächst ein Verständnis für die zugrundeliegende Technologie zu gewinnen. Auf Basis dessen versuche ich darzustellen, wie diese neue Währung die Gesellschaft verändern kann. Die Herausforderungen liegen zum einen in der Verknüpfung der unterschiedlichen Disziplinen wie der verteilten Infrastruktur, der Kryptographie und der Anwendungsmöglichkeit in der Wirtschaft. In der vorliegenden Arbeit wird zunächst ein grundlegendes Verständnis von Kryptowährungen vermittelt. Anschließend wird die Funktionsweise der Blockchain-Technologie detailliert dargestellt. Darauf aufbauend versuche ich darzustellen, wie das Prinzip der Kryptowährung Bitcoin funktioniert und welche Techniken in Bezug dessen angewendet werden. Abschließend wird ein Fazit zur Thematik gezogen sowie ein mittelfristiger Ausblick gegeben.

# Grundlagen

Im nachfolgenden Kapitel werden zuerst die grundlegenden Eigenschaften von Kryptowährungen beschrieben, um eine Wissensbasis für die Ausarbeitung zu schaffen. Abschließend folgt eine Definition des begriffs „Blockchain“.

## 2.1 Kryptowährungen

Eine Kryptowährung ist ein Digitales Zahlungsmittel. Dieses Zahlungsmittel als Objekt hat keinen Warenwert, an den es geknüpft ist und klassifiziert sich somit als Fiatgeld (Swan, 2015, S. 10).   
Die Funktionsweise des digitalen Zahlungssystems wird über ein verteiltes dezentrales Netzwerk sowie ein Verfahren der Kryptografie sichergestellt.  
Der Inhaber einer Geldeinheit erhält Anstelle einer Münze oder eines bedruckten Geldscheins, einen kryptografischen Schlüssel. Der Tauschwert der Geldeinheit wird durch den Schlüssel repräsentiert. Die Akzeptanz durch die Handelspartner bestimmt den Wert der Geldeinheit. Das Besondere an dieser Form von Zahlungssystemen ist, dass keiner dritten Instanz (z.B. Bank) vertraut werden muss. Die zugrundeliegende Blockchain-Technologie ersetzt dadurch die dritte Instanz. Die Blockchain beinhaltet somit also die gemeinschaftlich erstellte und für jeden zugängliche Buchführung (Nakamoto, 2009, S. 1). Die Funktionsweise dieser Technologie wird in Kapitel 4 näher betrachtet.

## 2.2 Blockchain

In einem Block wird neben den kürzlich erfolgten Transaktionen auch auf den Vorgänger-block referenziert. Die sogenannte Blockchain entsteht (vgl. Eyal & Sirer, 2013, S. 1) durch, die Referenz Einzelner aneinander geketteter Blöcke. In der Blockchain sind dann alle Transaktionen gespeichert. Jeder Teilnehmer des Bitcoin Netzwerks kann dabei die Transaktionen überprüfen und gewährleistet, dass der Block gültig ist (vgl. Lehne, 2013, S. 2). Möglich macht dies, dass jeder Block zusätzlich eine schwer zu lösende mathematische Aufgabe enthält, und gleichzeitig die Lösung der vorherigen Aufgabe (vgl. bitcoin.it, 2014a). Das Ergebnis einer solchen Aufgabe wird als Hashwert bezeichnet.

Der Hashwert eines neuen Blocks kann von jedem Teilnehmer des Netzwerks durch einen sogenannten Proof-of-Work getestet werden. Der Vorteil liegt darin, dass die Berechnung der komplexen mathematischen Aufgabe, also des Hashwerts sehr zeitaufwendig ist, die Lösung allerdings schnell kontrolliert und verifiziert werden kann. Um dies plakativ zu verdeutlichen, kann folgendes Zahlenbeispiel zu Rate gezogen werden. Durch das Summieren zweier Zahlen soll das Ergebnis 180 erzielt werden. Ohne einen der beiden Summanden zu kennen ist das Lösen dieser Aufgabe deutlich schwieriger, als zu hinterfragen, welchen Wert 80 und 100 ergibt. So ähnlich verhält es sich bei den Berechnungen und Verifizierung der Hashwerte (vgl. Perry, 2012). Das Lösen einer solchen komplexen Aufgabe benötigt einen sehr hohen Rechenaufwand. Ist die Lösung allerdings einmal gefunden, kann das Ergebnis durch alle Teilnehmer leicht auf dessen Gültigkeit geprüft werden.

# Bitcoin

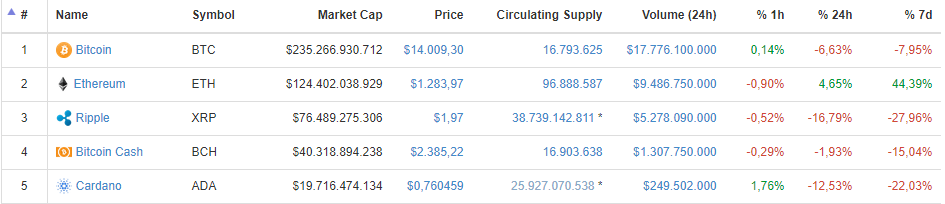
Die erste Kryptowährung mit dem Namen „Bitcoin“ wurde im Januar 2009 von Satoshi Nakamoto publiziert. Aus der durchgeführten Marktanalyse geht hervor, dass aktuell über 1300 alternative Kryptowährungen(Altcoin) existieren (siehe Anhang A).

Tabelle 1: Top 5 Kryptowährungen nach Marktkapitalisierung (Coinmarketcap)

In Tabelle 1 sind die fünf größten Kryptowährungen gemessen am Wert der Marktkapitalisierung aufgeführt. Die analysierten Kryptowährungen unterscheiden sich im Wesentlichen anhand der folgenden Kriterien:

- Art der verwendeten Kryptografieverfahren (SHA-2, SHA-3, Scrypt etc.)

- Verfahren zur Sicherung der Blockchain (z.B. Proof-of-Work, Proof-of-Stake etc.)

- maximalen Menge an Geldeinheiten (Coins)

- Zeitspanne, in der neue Blöcke generiert werden

Neue Einheiten einer Kryptowährung werden durch Mining erzeugt. Das Mining ersetzt die zentrale Institution (z.B. Zentralbank), die sonst neue Einheiten einer Währung ausgibt. Um in den Besitz einer Kryptowährungseinheit zu kommen, ist neben dem Mining auch der Erwerb über diverse Handelsplattformen (z.B. Bitstamp) möglich. In Kapitel 3.3.3 wird das Prinzip des Mining näher betrachtet. Anstelle eines Kontos tritt eine sogenannte Wallet Software. Diese Software speichert die für Transaktionen generierten Schlüsselpaare (ECDSA-Verfahren). Der öffentliche Schlüssel dient hierbei als „Kontonummer“, auf die ein anderer Teilnehmer Einheiten überweisen kann. Wer den passenden privaten Schlüssel hat kann über die erhaltenen Währungseinheiten verfügen. Die Wallet Software kann auf einem lokalen Rechner installiert sein oder über eine Börse als Online-Wallet angeboten werden. Es ist auch möglich sein „Guthaben“ in Form von Schlüsselwertpaaren auszudrucken und somit physisch rechnerunabhängig zu speichern (Nakamoto, 2009).