Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorthesis

Vor-und Zuname [redacted] [redacted] [redacted]
Lennart Back [redacted] [redacted] [redacted]

Titel: Cryptocurrencies - a future form of money?
An analysis of the functionality of Bitcoin as a means of exchange and payment

Abgabedatum: 16.07.2019

Betreuender Professor: Prof. Dr. Stephan Boll

Zweite Prüfende: Prof. Dr. Natalia Ribberink

Fakultät für Wirtschaft und Soziales
Department Wirtschaft
Studiengang Außenwirtschaft/Internationales Management, B.Sc.

Faculty of Business and Social Sciences
Department of Business
Major Foreign Trade/International Management B.Sc.

HOCHSCHULE FÜR ANGEWANDTE
WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Cryptocurrencies - a future form of money?

An analysis of the functionality of Bitcoin as a means of exchange and payment

Bachelor Thesis submitted by
Lennart Back

Abstract

With the rise of market capitalisation of cryptocurrencies in 2018, Bitcoin in particular and to lesser extent also its offspring, commonly referred to as Altcoins, have gained significant interest by governments, institutions and investors. The future of these new forms of currency remains a topic that is debated heavily. While some enthusiasts believe that the status of cryptocurrencies will rise up to the point where they are equivalent or even replacing traditional currencies in some departments of online commerce, sceptics usually evaluate them as a dubious new form of assets with no intrinsic value. The latter thereby often point at the large sell-off of cryptocurrencies in the first quarter of 2018 as the beginning of the end of the crypto era. This work aims at elaborating the characteristics of the cryptocurrency Bitcoin by applying monetary theory to answer the research question whether Bitcoin is actually feasible to serve as a future means of payment and exchange and which consequences result of this feasibility for the cryptocurrency in the future. While Bitcoin provides reasonable advantages to individuals involved in monetary online transactions and from a theoretical perspective also fulfils the criteria for a means of exchange, the cryptocurrency will likely face difficulties to attract more users due to issues regarding its scalability, price volatility and many more. Alongside with other technical restrictions, the author concludes that - considering all facts presented in this work – Bitcoin in its current state will be unable to achieve a transaction volume comparable to PayPal, Visa or Mastercard and will therefore only play a niche-role in certain environments as a future means of payment.

Keywords: cryptocurrencies, digital cash, currency competition, monetary theory

JEL Classification: E39, E40, E42, E49, F24, G10, G29

I. Outline

II. List of Figure, Tables and Formulas

Figures:

Tables:

Formulas:

1 Introduction

1.1 Research problem

In November 2008, the pseudonymous developer Satoshi Nakamoto published a white paper called “Bitcoin: A Peer-to-Peer Electronic Cash System”. He describes a peer-to-peer network approach of a virtual currency based on a cryptographic protocol called proof-of-work-system, which allows participants to carry out transaction directly without the necessity of an intermediary. By requiring all transactions to be listed in a shared public transaction log called blockchain, Nakamoto also presented a solution to the double spending issue, which previous virtual currencies struggled to overcome. Although enthusiasts often describe Nakamoto’s work as revolutionary, his payment system is from a more factual perspective rather to be seen as a combination of concepts that have all previously existed. It emerged in a time when the bankruptcy of Lehman Brother’s induced a spiral of global economic downturn. The underlying ideas of Nakamoto’s work reflect a mindset of a small but growing group of people who criticised the existing monetary system predominantly for its centralised nature. Nakamoto envisioned a new decentralised approach with a fixed supply of coins in which all members have equal rights and obligations towards each other. At the time this paper is written, the internet community celebrates the ten-year anniversary of the so called “Genesis block” which was the first block created by Nakamoto on the blockchain of Bitcoin. In these past ten years, Bitcoin and cryptocurrencies as a whole have become a fixture in world financial media coverage experiencing a tremendous increase of both market capitalisation and daily transaction volumes. From its initial price in the range of less than 10 USD cents back in 2009, Bitcoin’s price to this day averages at around 11,000 USD per Bitcoin unit after reaching a peak of almost 20,000 USD per coin in the first quarter of 2018. Many other cryptocurrencies like Ethereum or Ripple have experienced a similar growth in recent years. While the remarkable development of these new forms of digital currencies cannot be denied, a fundamental question is still debated vigorously: What are cryptocurrencies? A new form of currency or just a speculative asset that is deemed to fail? A means of payment or a store of value? Or both? Many experts and enthusiasts describe Bitcoin as the first global currency in history while others describe it as a mere investment hype, a gimmick or even fraud. One of the most famous sceptics is the American economist Paul Krugman who published an article named “Bitcoin is evil” on the website of the New York Times

in which he expresses his view on the cryptocurrency as an asset with no intrinsic value that would ultimately be deemed to fail (Krugman, 2013). However, the adoption and the attention that Bitcoin has received prove that indeed many people believe in Bitcoin as a future worldwide currency. The topic of currency and monetary theory is a widely covered subject of academic work. Throughout history, currencies have occurred in all kinds of shapes and forms providing for a more efficient system of exchange than a system solely based on bartering. Monetary theory describes among other properties a triad of three functions that an asset has to deliver to be considered as a currency: It has to function as a means of exchange, as a store of value and as a unit of account. The aim of this thesis is to analyse in how far the intrinsic function and its consequential properties of a currency as a means of exchange and payment as laid out by monetary theory is applicable to the cryptocurrency of Bitcoin. For this analysis, the cryptocurrency of Bitcoin is selected because it was on the one hand the first project that utilised blockchain technology in combination with cryptography to become what is now known as a cryptocurrency. Moreover, it has ever since its emergence been the cryptocurrency with the highest market capitalisation. In popular media and in the general public, the name of Bitcoin is therefore often used synonymously with the entirety of cryptocurrencies. Due to its capitalisation as well as its awareness, Bitcoin is also the cryptocurrency project that enjoys the widest coverage of academic publications.

1.2 Research method

This written paper is based on philosophical research, i.e. literature-based research. Thereby, a selection of relevant sources has been analysed and considered collectively to condense findings that resemble a consensus of the literature provided. The following types of academic literature have been considered:

- Monographs
- Working papers
- Conference papers
- White papers
- Articles in academic journals

These sources have been gathered by carrying out a profound research using web search engines, library catalogues, journal databases and subject specific professional websites. In a second step, the sources have been carefully reviewed and included in this work based on their relevance to the topic, the design of studies and the age the material. For the explanation of the technical functioning of Bitcoin, all sources published after its emergence in 2008 were considered since the underlying features have since the cryptocurrency's initial publication largely remained the same. At the same time, all information retrieved from these sources have in a second step been reviewed on their actuality and relevance for present day discussions. While this paper is predominantly based on an analytical review of academic literature and reports of major financial institutions, the author also refers to data provided by coinmarketcap.com and blockchain.info which are online platforms created to track the market capitalisation of all major cryptocurrencies, the amount of trade within each cryptocurrency's market and the most current price of cryptocurrencies converted into fiat currencies. Furthermore, data provided by Google Trends is addressed to supplement the illustration of trends on the field of cryptocurrencies. To raise more current issues and subjects of debate in the field of cryptocurrencies, the author has also included information gathered from cryptocurrency-news providers as long as the given content has been assessed as being coherent with academic literature. All information provided by referred sources has been obtained lawfully and reported accurately.

1.3 Course of investigation

Based on the research question as stated in chapter 1.1, chapter 2 will be dedicated to explaining the definition of currency (chapter 2.1) and the functions and properties of currency in modern society (chapter 2.2). This chapter will serve as a basis for later evaluation of cryptocurrencies. In chapter 3, character and functionalities of virtual currencies will be introduced (chapter 3.1). In a second step, the subgroup of cryptocurrencies will be differentiated (chapter 3.2) and then elucidated by the example of Bitcoin which is at the time this work was written the most dominant cryptocurrency in the world (chapter 3.3). Thereby, a short introduction and explanation of the background of Bitcoin will be given (chapter 3.3.1) before the following subchapters will elaborate on the recent development of the cryptocurrency (chapter 3.3.2) and its technical features (chapter 3.3.3). In the following chapter 4, the findings of chapter 2

and chapter 3 will be condensed by applying monetary theory on Bitcoin in order to assess whether it may actually be considered as means of exchange and payment with regard to the previously explained three major functions of currencies. Alongside the sole theoretical feasibility of Bitcoin as a means of exchange and payment (chapter 4.1), the role of Bitcoin as such will also be reviewed from a transactional, a market and a conceptual perspective (chapter 4.2 - 4.4). Chapter 5 will then summarise the previous chapters and be followed by a conclusion regarding the underlying research question of this work (chapter 5.1). Finally, an outlook will be provided (chapter 5.2) as well as a critical acclaim (chapter 5.3).

2 Monetary theory and currency

2.1 Definition of currency

In his famous work, the founder of modern economic theory Adam Smith established the idea that in societies that had existed before the invention of money, barter was used to exchange goods and services (Strauss, 2016). Although Strauss explains in her essay that Smith's idea of a society solely based on barter cannot be proven by any historic accounts, barter has always existed and still does to this day (ibid.; Ammous, 2018, p.1). However, this direct exchange of goods and services is impractical due to an issue that is described by Jevons (1898, p.3f.) as a double coincidence of wants. Thereby, in the absence of a single medium of exchange a situation in which goods and services are exchanged requires that the two participants are seeking to possess the exact goods of the other person (Kasper, 2017, p.17). Additionally, issues regarding the measurement of value as well as the divisibility of exchanged goods arise that will be explained in the following subchapters (Jevons, 1898, p.5f.). Hence, such a system without currency is only imaginable in comparably primitive economies (Issing, 2011, p.1). In larger economies, there is more space for specialisation and exchange, but at the same time the issue of coincidence of wants is also bigger (Ammous, 2018, p.2). Issing (2011, p.1) claims that the presence of money as a means of exchange only enables the modern form of specialised economies.

From a macroeconomic perspective, an asset is typically considered as a form of currency or money if it fulfils three separate functions: First, it must function as a standard unit of account, meaning that the value of other goods is expressed as units of that currency. Second, the asset must be a store of value to be considered a currency. Third, an asset must represent a generally accepted means of payment and exchange with the highest degree of liquidity (Sixt, 2017, p.47). In the following, these three functions shall be further examined.

2.2 Functions and properties of money

2.2.1 Unit of account

According to Kasper (2017, p.17), a major issue in an economy without a generally recognised means of payment is that it becomes increasingly difficult to measure the value of a commodity or product. Since prices in the absence of a generally accepted currency may only be measured in units of the good that is intended for an exchange,

a standardisation of prices in such circumstances is highly impractical if not impossible (Jevons, 1898, p.5). In a barter economy the number of prices grows exponentially with the number of products (Mishkin, 2010, p.55f.).

Formula 1: The number of exchange pairs in absence of a currency

$$t = \frac{n(n-1)}{2}$$

(Source: Issing, 2011, p.2)

Formula 1 describes the number of exchange pairs *t* in a barter economy with *n* goods. An increasing number of goods *n* thereby leads to an exponentially larger number of exchange pairs *t*. In a theoretical simple economy that only has access to a set of 100 products, the number of prices would already account for 4950 exchange ratios (Jevons, 1898, p.5). The relatively complicated determination of prices for a given exchange would significantly increase general transaction costs (ibid.). In an economy based on the division of labour, money functions as a unit of account to break down goods and services to a common denominator and hence allows for all kinds of comparisons among them (Kasper, 2017, p.19). It allows for the value of goods being stipulated as absolute prices of the respective currency (Issing, 2011, p.2). By introducing a generally accepted means of exchange as a numeraire, the number of prices as shown in Formula 1 is significantly reduced to $t = n - 1$ (Borchert, 2001, p.29). It is a fundamental function of money to measure value and consequently allow exchanging parties to interpret and compare prices (Vandezande, 2017, p.139). Additionally, significantly less resources must be spent for the procurement of price information which can instead be spent to generate other income, leading to an increase of real incomes in an economy (Borchert, 2001, p.30).

The unit of account function of money enables all forms of commercial accounting in our modern-day economy, such as profit and loss statements, balance sheets, calculation of wages, etc. (Kasper, 2017, p.19). To function as a unit of account, currencies have to possess a certain degree of divisibility to be able to express prices of even the least valuable goods and services (Kerscher, 2014, p.25). Issing (2011, p.3) compares the use of currency as a common denominator of value to the role of units of measurement for length, weight or power. A currency may be used as a unit

of account, even if it is not used as a means of exchange as the example of the Guinea shows, which was likewise used in 19th-century-England (Jarchow, 2010, p.2).

2.2.2 Means of exchange and payment

Almost all kinds of transactions in modern economies are denominated in a currency that acts as a medium of exchange and payment (Mishkin, 2010, p.54). Kasper (2017, p.18) describes this specific function of currency as probably being the most important one. Money is defined as a medium of exchange due to being an asset that is acquired not to be consumed, nor to be used as a means of producing other goods (Ammous, 2018, p.3). The presence of currencies enables a division of an exchange transaction into two separate steps: On the one hand, individuals are able to sell goods for money. On the other hand, they can use money to purchase goods (Issing, 2011, p.1). By introducing a single medium that is valuable for everyone in the same way, the earlier mentioned issue of double coincidence of wants can be replaced by a single coincidence (Kasper, 2017, p.18). Hence, it is far easier to find suitable exchange partners because usually everyone will accept legal tender (Kasper, 2017, p. 17). The time spent to arrange transactions is far less and therefore a higher level of economic efficiency can be achieved (Mishkin, 2010, p.54).

According to Menger (1892, pp. 248f.), the key determinant of a good being adopted as a generally accepted means of exchange is its saleability, i.e. the relative ease with which it can be sold on the market. He described the issue of coincidence from a different perspective in identifying three dimensions that are problematic in exchanges within a barter economy, namely scales, time and space (ibid., p.245-247). The saleability of a good and consequently its usefulness as a currency is determined by its ability to address issues regarding these three dimensions (ibid.). Being saleable across scales means that a good is easy to convert into smaller pieces or grouped into larger units (Ammous, 2018, p.4). Furthermore, if a good is easy to transport, it possesses saleability across space (ibid.). An indicator to measure this ability is the value per unit of weight (ibid.). The third aspect – a goods saleability across time – refers to its ability to preserve value over time (ibid.). This function is linked to the function of money as a store of value (see chapter 2.2.3).

Freedom of exchange is another precondition for the functioning of currency as a means of exchange. If there is no such freedom, goods may not be freely exchanged with money and therefor excess demand, increased delivery times and queues may

occur. Currency may in such an environment partially lose its function as a means of exchange, especially if black markets occur where other commodities assume this role (Borchert, 2001, p.28).

2.2.3 Store of value

A third important intrinsic function of currency is its role as a store of value (Mankiw, 2011, p.103). Thereby, owners of currency do not have to spend received funds right away but can instead opt to hold them and exchange them for goods and services at any future time. An underlying condition of this concept is that when the currency is spent, owners expect to receive more or less the same economic value that their funds were worth upon receival (Yermack, 2013, p.11). A store of value hence enables individuals to store their purchasing power until the need or desire to spend it arises (Jarchow, 2010, p.3).

Apart from money, there are a variety of other options to store value over time, e.g. stocks, bonds, land, property and so on (Mishkin, 2010, p.56). Holding money does not provide the owner with gains from interest payments, price appreciation or any other services. However, money enables its holders with a relative ease to convert it into other assets, i.e. liquidity (ibid.). In fact, money is commonly referred to as the most liquid asset, since it does not have to be converted before purchasing other assets (ibid.).

In his General Theory of Employment, Interest and Money, Keynes (1937, p.202 f.) describes the fundamental characteristics of money as to be seen in its zero or relatively low elasticity of production in conjunction with an elasticity of substitution that is equal to or very close to zero which is sometimes interpreted as an emphasis of the importance of the store of value function of money (e.g. Sardoni, 2015, p.1). Furthermore, Keynes (1937, S.172 f.) describes holding idle money as means of defence against uncertainty. His opinion on money as a store of value is however not undisputed. Hicks (1967, p.17 f.) for example argues that the role of currency as a means of payment in conjunction with its function as a unit of account are necessary criteria, while being a store of value is in itself not a sufficient property to define an asset as a currency. For a good to be able to preserve value over time, it must be durable, i.e. immune to corrosion (Ammous, 2018, p.4).

Apart from durability, historic accounts indicate that for most currencies there has been a mechanism or policy to restrain the production of the monetary good (ibid., p.5).

According to Ammous (2018, p.5), the relative difficulty of expanding the total supply of monetary units allows for a distinction between two groups of currencies: On the one hand, there is so called easy money whose supply can easily be increased. On the other hand, a currency is considered as hard money if its supply is only increasable under large efforts. Ammous (ibid.) further explains that only hard money provides for a functioning store of value. Consequently, a major threat to the usefulness of money as a store of value is inflation (Vandezande, 2017, p.140). In a scenario where the value of a currency significantly decreases, the willingness of others to accept payments with that respective currency will also be negatively impaired and thereby eliminate its store of value function (Kasper, 2017, p.18).

During the hyperinflation in Germany that peaked in 1923, the currency lost its value so quickly that workers had to be paid several times a day to spend their wage right away before it became worthless (Mishkin, 2010, p.56). The amount of money that was required to purchase even the most basic items became immoderate and simultaneously the attractiveness of holding and using money declined with an increasing number of transactions being carried out in barter (ibid.). A second threat to the functioning of currency as a store of value is high volatility (Jevons, 1898, p.37f.). If the value of a currency fluctuates too strongly, its holders lose certainty about the ability of their funds to deliver the expected economic value in the event of a purchase (Jarchow, 2010, p.4).

2.2.4 Properties of money

Alongside the explained intrinsic functions, currencies must also possess a set of properties that enable them to function as a means of exchange, a store of value and as a unit of account (Kasper, 2017, p.31). According to Niehans (1980, p.14), whether a commodity is commonly used as a currency or not is determined by its transactional costs and storage costs, which should be as low as possible. With regard to these properties, a set of technical features as well as features regarding a commodity's ability to store purchase power over time can be identified as intrinsic to currency (Jarchow, 2010, p.3). These features involve a commodity's portability, permanency, homogeneity, divisibility and scarcity (ibid.; Kasper, 2017, p.20f.). Thereby, portability means that only small and light-weighted quantities of monetary units must be carried to buy larger assets (Kasper, 2017, p.20). The properties of homogeneity and divisibility are achieved if all monetary units are of the same kind and quality and can

also be divided into smaller units, as well as scaled to larger amounts without any costs of division (Jarchow, 2010, p.3). Permanency and scarcity define the ability of a commodity to store value and follow the concepts that are laid out in subchapter 2.2.3. Acceptance means that holders of monetary units are able to pay all of their obligations unconditionally within the realm of the respective currency, usually enforced by law (Kasper, 2017, p.21).

3 Virtual currencies and cryptocurrencies

3.1 Characteristics of virtual currencies

With the emergence of the internet in the late 20th century, a new medium for the sale and marketing of goods has been introduced. Alongside the rise of internet-based ecommerce and the spread of mobile devices, several innovative technologies have also come up on the field of online payment systems (He et al., 2016, p.5). While networks like PayPal provide a platform for secure online transactions denoted in fiat currency, some other networks went one step further in introducing an own currency-like unit that is traded on their platform. In the following, these virtual currency schemes and cryptocurrencies by example of Bitcoin shall be examined.

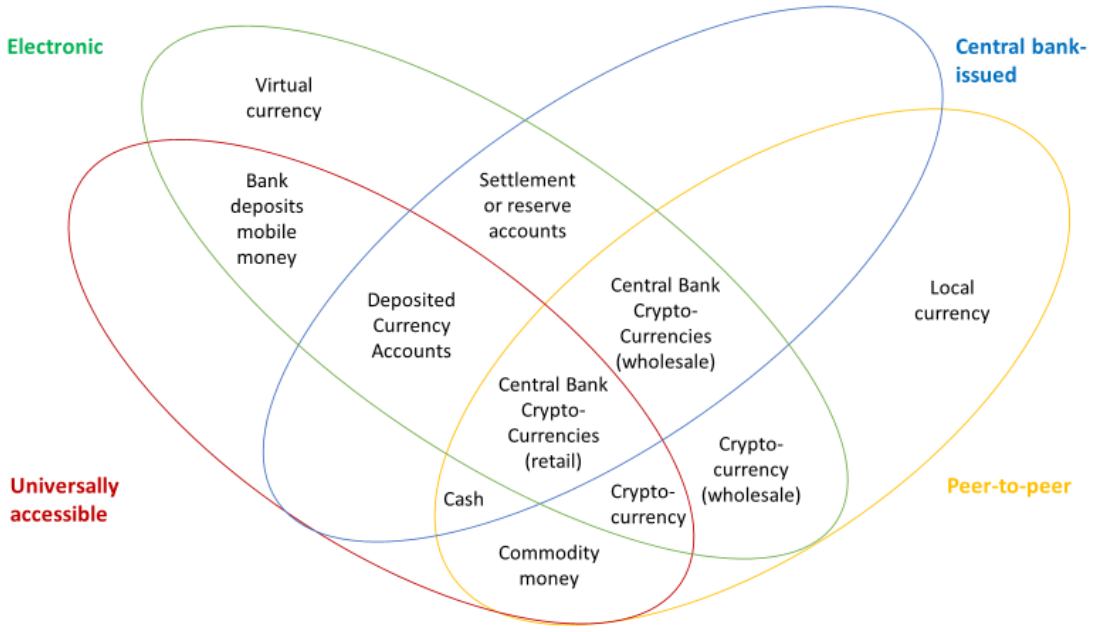
Virtual currencies are defined as digital representations of value that have been issued by private developers (He et al., 2016, p.7). Their supply usually circulates internationally across borders with little to no restrictions (Dabrowski & Janikowski, 2018, p.4). The general function of a virtual currency is to serve as a means of payment in a specific virtual community, e.g. a website or a computer game. Within this community, all participants voluntarily agree to use the respective virtual currency to carry out transactions (Segendorf, 2014, p.72). Virtual currency schemes can be distinguished by their degree of convertibility to other assets, e.g. goods, services, national currencies or other Virtual Currencies (He et al., 2016, p.8). Closed currency schemes comprise those virtual currencies that can only earned and used on a certain platform without the possibility to purchase or sell them for fiat currency (Segendorf, 2014, p.72). On the other hand, convertible virtual currencies enable holders to exchange virtual currency units with other assets (He et al. 2016, p.8). Thereby, some virtual currency schemes allow for bidirectional flows, meaning that both purchasing the currency with fiat currency as well as selling it for fiat currency is possible (Segendorf, 2014, p.72). Moreover, there are currency schemes that only allow for unidirectional flows, i.e. the purchase of virtual currency tokens for fiat currency. In such schemes, there is no channel for a re-exchange of virtual currency into fiat currency provided (ibid.). Another feature that can be used to categorise virtual currency schemes is the distinction between centralised and decentralised systems. Whenever payments are made, the ownership of virtual currency units must be adjusted accordingly (ibid.). In this case, traditional currency schemes make use of a centralised system in which a single centralised entity is responsible to verify and execute transactions. On the contrary, decentralised systems shift the task of

verification and execution of transactions to the entire decentralised network (Segendorf, 2014, p.72). Alongside the settlement of transactions, He et al. (2016, p.8) describe the issuance and redeemability as well as the establishment and enforcement of rules of the currency system as key tasks of any virtual currency scheme. Again, each of these functions can be performed by a trusted central third-party or in a decentralised manner by the entirety of participants (ibid.).

3.2 Characteristics of cryptocurrencies

Electronic currencies that are based on a decentralised ledger, blockchain technology and cryptography are commonly referred to as cryptocurrencies (Pielke, 2018, p.2). As illustrated in Figure 1, which shows the taxonomy of money in terms of the four criteria "electronic", "central-bank-issued", "universally accessible" and "peer-to-peer". Cryptocurrencies are thereby not a subcategory of virtual currency but are instead distinct from them due to their peer-to-peer architecture and their accessibility. They are characterised by being an electronic peer-to-peer network that is universally accessible and not governed by a central authority (Bech & Garrat, 2017, p.60). In the following, the background and the technical features of the most widely spread cryptocurrency Bitcoin will be further examined.

Figure 1: The Taxonomy of money



(own creation based on Bech & Garrat, 2017, p.60)

3.3 The case of Bitcoin

3.3.1 Introduction

Starting from the thoughts gathered in the previous subchapter, Bitcoin may be described as a decentralised cryptocurrency scheme with bidirectional flows, which is designed to be independent of banks, governments and other institutions (Segendorf, 2014). The famous white-paper “Bitcoin: A Peer-to-Peer Electronic Cash System” written by the anonymous Satoshi Nakamoto was firstly introduced to a mailing list on the topic of cryptography (Küfner, 2018, p.30).

In his paper, Nakamoto (2008, p.1) criticises the reliance on trusted third parties to process electronic payments in e-commerce. Due to non-reversibility of transactions being practically impossible in these traditional platforms, third parties would have to be involved as a source of trust and to mediate disputes on the network whenever users do not agree with the outcome of a transaction. In online payment systems like PayPal or VISA, financial institutions act as a trustworthy supervisor and in turn are being paid for their services by collected transaction fees (Kasper, 2017, p.23). Hence, the presence of intermediaries in payment systems would raise transaction costs and thereby also the minimum practical transaction size (Nakamoto, 2008, p.1).

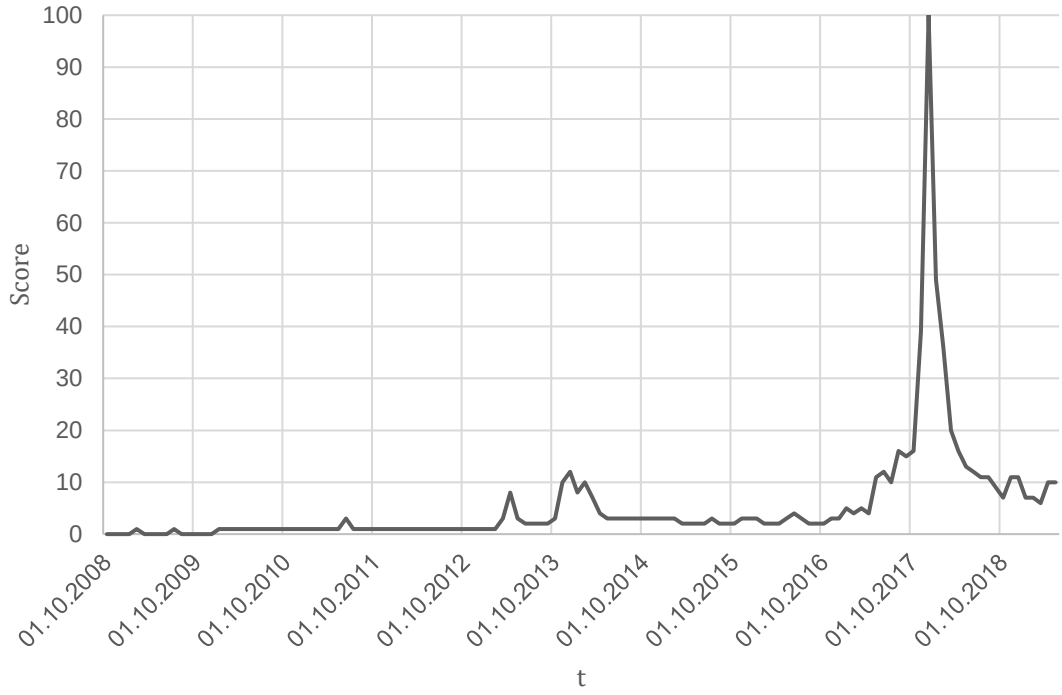
In his paper, Nakamoto describes Bitcoin as a peer-to-peer version of electronic cash which would provide users with the ability to make online payments directly from one party to another without an intermediary (Nakamoto, 2008, p.1). The cryptocurrency makes use of an innovative method of storing transactions called blockchain, which enables Bitcoin to function similarly to traditional online payment systems, but in a decentralised manner (Huberman, Leshno & Moallemi, 2017, p.2). It is an electronic payment system that is to be trusted as a whole, although none of the system’s servers is individually to be trusted (ibid.). Bitcoin’s transaction system is formed by a network of participants having equal rights which run the Bitcoin-Client on their hardware, thereby interconnecting with one another (Sixt, 2017, p.29). In the following, the recent past of Bitcoin as well as some of the system’s major technical aspects will be further explained.

3.3.2 Recent History of Bitcoin

After Nakamoto’s publications on the Bitcoin network in autumn 2008, the interest on his system initially remained within the reach of the mailing list that he originally published his paper to. As underlined by the data shown in Figure 2 provided by Google

Trends, the search term of Bitcoin only in 2011 did not achieve a considerable popularity until 2011 (Sixt, 2017, p.17).

Figure 2: Google Trends analysis of the search term Bitcoin



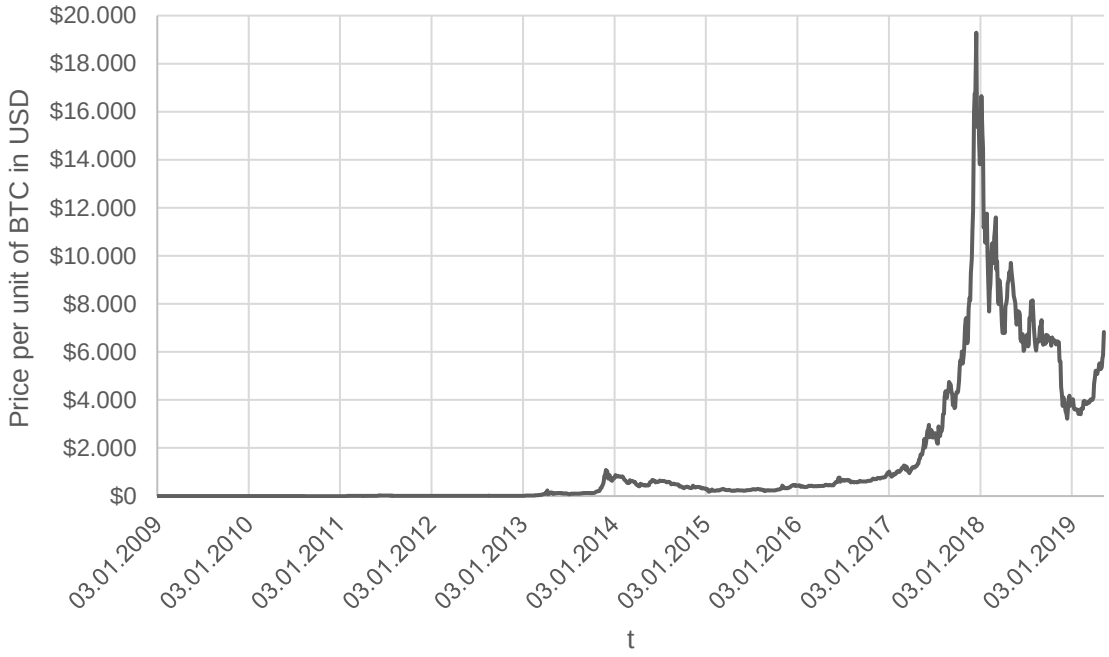
(Source: own creation based on data provided by Google Trends, n.d.)

The figure displays the interest over time on the search term “Bitcoin”, which is measured by a relative score that ranges from 0 to 100. Thereby, the scores of 0 and 100 mark the bottom and the peak of interest and all other scores are attributed in relation to these two. In fact, the analysis of Figure 2 in conjunction with Figure 3 which shows the price development of 1 Bitcoin indicates that the interest on the topic of Bitcoin unsurprisingly highly correlates with the price development. Since there are price differences across the variety of exchanges that offer a platform for trading Bitcoins, blockchain.info (n.d.) created a daily average of prices across all major exchanges which is used as a database for Figure 3.

The interest on the search term has thereby always risen when the Bitcoin price witnessed a stark increase in a relatively short period of time. In 2011, it was the first ten days of June when the Bitcoin price on the Bitcoin exchange Mt.Gox reached a temporary high of 10 USD per Bitcoin on 2 June and then peaked at 31.91 USD six days later (Giese et al., 2016, p. 42). The data provided by Google Trends shows that in these first ten days of June 2011, the interest on the search term of Bitcoin increased

in a correlated manner to the price development. After the first Bitcoin bubble (also called “The Great Bubble of 2011”) burst on 12 June, not only prices, but also the interest in Bitcoin collapsed (Küfner, 2018, p.67f.; Google Trends, n.d.). This pattern has continued to occur throughout Bitcoins relatively short history.

Figure 3: The price development of Bitcoin



(Source: own creation based on data provided by blockchain.info website, n.d.)

While Bitcoin’s rise established its name on the internet, the idea of decentralised and encrypted currencies simultaneously continued to unfold with the emergence of the first alternative cryptocurrencies. On 13 October 2011, Litecoin launched as an attempt to improve the original design of Bitcoin with some alterations regarding the maximum of coins and the hash algorithm for mining (Küfner, 2018, p.71). In the following years, new cryptocurrency projects that emerged alongside Bitcoin were commonly referred to as Altcoins. Ahamad et al. (2013, p.43) describe the term Altcoin as a slang term that evolved in the cryptocurrency development community as a catch-all term for a steadily increasing number of cryptocurrency projects.

The events of the following year 2012 – although not having led to price fluctuations as dramatic as in the previous year – demonstrated the limitations of Bitcoin’s concept of decentralisation (see chapter 3.3.3.2). Hackers continued their efforts to exploit loopholes in the security of Bitcoin-exchanges. These exchanges controlled sales

transactions in a centralised manner and held hundreds of thousands of Bitcoins which were stored by users on these platforms with relatively little cyber security (Küfner, 2018, p.76). The first major crime occurred in March 2012 when a security violation of the webhosting company Linode led to the theft of 46,000 Bitcoins (ibid.). Similar hacks of the exchanges Bitcoinica and Bitfloor followed (ibid.).

In 2013, the Bitcoin price dramatically increased from 30 USD in February to an all-time high of 266 USD per Bitcoin in early April (Giese et. al., 2016, p.43). A delay of handling transactions on the Mt.Gox exchange led to yet another stark price decrease to 76 USD, but unlike after the collapse in 2011, Bitcoin proved its price resistance in the following weeks and months and stabilised (Küfner, 2018, p.92). On 2 October 2013, the FBI shut down the online marketplace Silk Road and arrested its operator Ross Ulbricht (Rhodes, 2018). Until that point in time, Silk Road had been a marketplace in the darknet for illegal drugs and by that time accounted for an estimated 50 percent of all transaction of Bitcoin, which was the means of payment on the website (Küfner, 2018, p.95). Although the seizure of the online drug market meant that the by that time predominant use case of Bitcoin vanished, the impact on the Bitcoin price was rather small which was seen as a turning point for the credibility of the cryptocurrency (ibid.). With an increasing credibility and the market entrance of two major venture-capital companies of the Silicon Valley (Andreesen Horowitz and Union Square Ventures), the Bitcoin price continued to rapidly increase, reaching a peak of 1242 USD at the end of November, topping the 1000 USD mark for the first time (Giese et al., 2016, p.44). After the Chinese Central Bank officially announced to consider a complete ban of Bitcoin, the price soon plummeted back to a level of around 500 USD (ibid.). These rumours were especially impactful to the market price of Bitcoin because China used to be a core marketplace for Bitcoin with more than 80 percent of global transactions being made in the People's Republic (Küfner, 2018, p.98).

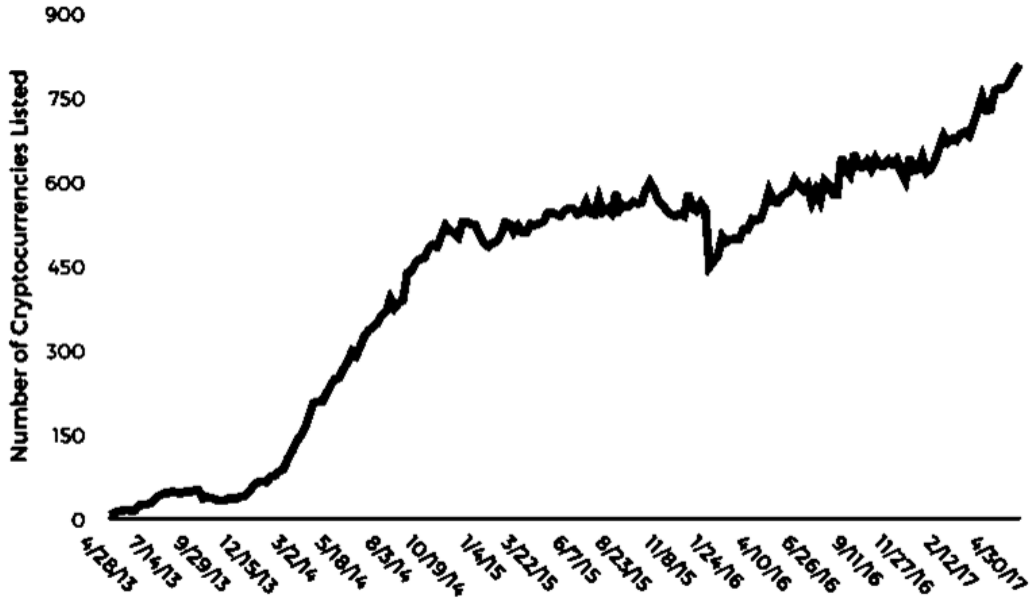
In 2014, negative headlines of government regulations and interventions continued. Although the British government decided to classify Bitcoin as a form of private money and not as an asset, a guideline paper of the Internal Revenue Service stated that Bitcoin would be subject to capital gains tax and thereby introduced complicated tax calculations to users (Rizzo, 2014; Internal Revenue Service, 2014, pp.2-4). Soon after, China continued to apply its sanctions to Chinese cryptocurrency exchanges by forcing them to close their Chinese bank accounts (Giese et al., 2016, p.45). Bitcoin's rapid growth in the previous year posed an obstacle for governments in terms of

consumer protection and also due to the threat of Bitcoin to destabilise national currencies (Küfner, 2018, p.106f.).

2015 was the year that marked the beginning of a new era in the history of cryptocurrency. While in previous years the Bitcoin network's intended use was to provide a network for payments and transactions (Blockchain 1.0), the emergence of the altcoin Ethereum introduced the idea to use decentralised transaction systems as a platform for contracts over various kinds of assets (e.g. stocks, bonds, credits, smart property, smart contracts, etc.) (Sixt, 2017, p.9). Ethereum is therefore commonly referred to as the first Cryptocurrency 2.0 (also Blockchain 2.0) (Leys, 2014, p.157; Küfner, 2018, p.118).

In 2016, the enthusiasm around the Ethereum network continued to grow and with it so called initial coin offerings (also ICO's) emerged (Marr, 2017). ICO's are commonly described as fundraising platforms through which start-up ventures procure capital from investors who speculate on a future price increase of proprietary tokens offered by the respective company (Ver, Kanemoto & Matsuda, 2018, pp.16-19).

Figure 4: The number of cryptocurrencies as listed on coinmarketcap.com



(Source: Rowley, 2017)

Figure 4 shows the number of cryptocurrencies that were listed on the website coinmarketcap.com over time. After a reduction of projects between November 2015 and January 2016, the number continued to grow in the following months due to the

relative ease by which start-up projects were able to generate capital influxes by using the Ethereum platform.

In 2017, a set of positive influence factors, predominantly rising acceptance, but also acts by governments (Japan, Russia, etc.) and technical innovations (e.g. Lightning Network, SegWit) led to a continuous growth of cryptocurrency prices throughout the year (Marr, 2017; Küfner, 2018, pp.143-156). As indicated in Figure 3, the Bitcoin price and alongside with it the price of most other major cryptocurrencies rose almost in an exponential manner from July 2017 until December 2017 (see also Heun, 2018, p.28). This unprecedented growth of cryptocurrency capitalisation sparked debates on the issue of cryptocurrency investment bubbles. Numerous celebrities on the field of finance and investment criticised Bitcoin, comparing it to earlier speculation bubbles, such as the Dutch tulip mania in the 1630's (Küfner, 2018, p.153). Others outright described the entirety of cryptocurrencies as "fraud" or "index of money laundering" (ibid.). These remarks were however unable to stop Bitcoin's price surge which peaked at around 19500 USD in December 2017 (Rhodes, 2018).

However, a series of negative headlines would introduce a downtrend in the beginning of 2018. Alongside a wave of sanctions imposed by the governments of Egypt, South Korea, China and India, the search engine Google and the social network service Twitter announced an upcoming ban of all kinds of advertisement for cryptocurrencies on their websites (Küfner, 2018, p.160). In their review of the developments of cryptocurrencies in 2018, Hays & Valek (2019, p.7) state that "as far as prices were concerned, 2018 was virtually the opposite of 2017. After the euphoria came disillusionment. After the boom came the bust." At the day this work is written, the Bitcoin price is set at a level of 11000 USD after a recovery of a low of 3000 USD at the beginning of 2019.

3.3.3 Technical features of Bitcoin

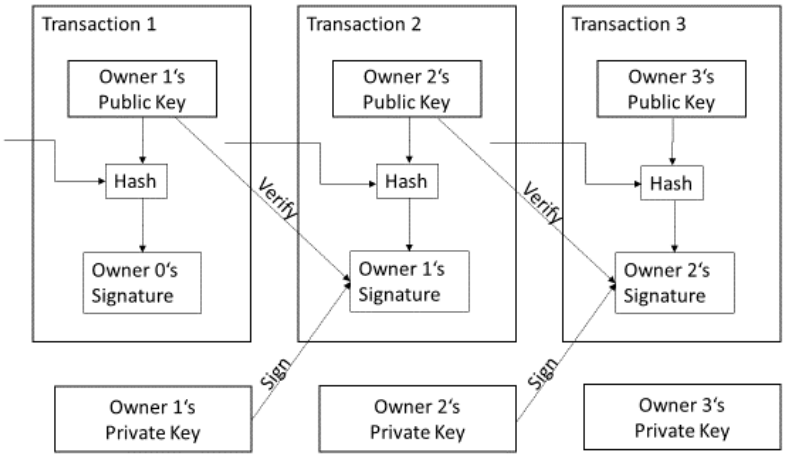
3.3.3.1 Asymmetric Encryption and Hash function

The Bitcoin network that Satoshi Nakamoto designed did not introduce any new technologies that were previously unknown. Instead, he combined a set of technologies that had already been published in separate projects, such as proof-of-work, peer-to-peer networks and cryptography to create a new product (Küfner, 2018, p.38). In the following, a set of these technical features shall be explained.

Subject of transactions carried out on the Bitcoin network are Bitcoins which represent a digital value within the network and consist of a digital string of characters (Sixt, 2017, p.30). Miller (2014, p.34) illustrates the nature of a unit of Bitcoin by pointing at its non-physicality and the fact that it is not represented by any bills or coins. He claims that Bitcoins would neither be stored on computers nor hard drives, but instead simply represent a record of previous individual transactions (ibid.). These records of transactions result in balances on so called wallets that are held by users. Wallets have been given their name by their wallet-alike role within the Bitcoin Network (Franco, 2015, p.123). A wallet is an encrypted computer file, which communicates with other wallets in the network through a technology called public key cryptography (Pagliery, 2014, p.35). Whenever a new wallet is created, a pair of cryptographic keys containing a public and a private key is generated (Miller, 2014, p.35). Users hold and securely store private keys in their wallets (Franco, 2015, p.17). A public key is - as its name suggests - publicly shared and acts as the address to which transactions can be sent, similarly to a bank account number (DuPont, 2019, p.60; Franco, 2015, p.124). On the other hand, a private key can be described as a secret piece of data that proves a user's right to conduct transactions from a respective wallet by means of a cryptographic signature (Guttmann, 2013, p.20).

Wallets are not to be understood as a standard software, but instead occure in a variety of forms (Heun, 2018, p.91). In general, wallets face a trade-off between flexibility and security. Hot wallets are predominantly used for day-to-day operations since they are always conncected to the internet and thus a potential subject to hacks and other sorts of fraud (Franco, 2015, p.126). On the other hand, cold storages provide for an offline alternative to securely store long-term holdings of Bitcoin to avoid the previously mentioned risks (Giese et al., 2016, p.104). Next to hardware wallets, users may also write down (Paper Wallet) or simply remember their private key strings (Brain Wallet) as a means of storing them securely (Heun, 2018, p.95; Franco, 2015, p.132). In the Bitcoin Network, the initiator of a transaction, i.e. the sender, encodes the transaction with the public key of the receiver, which has been shared between the two parties prior to the transaction.

Figure 5: Technical aspects of a transaction on the Bitcoin network



(Source: own creation based on Nakamoto, 2008, p.2)

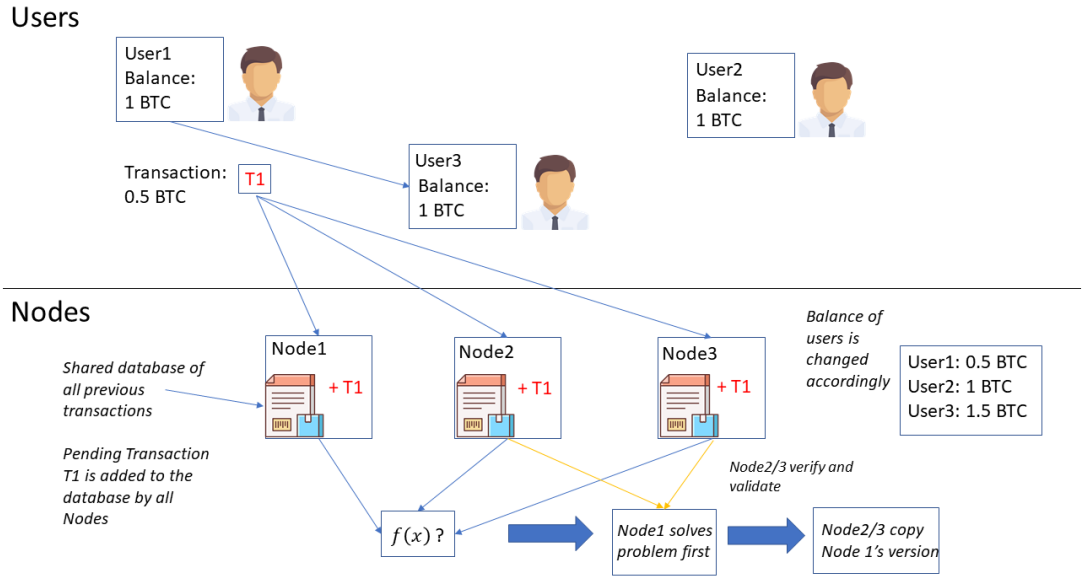
The information can then only be decoded with the private key of the receiver who thereby identifies as the rightful owner of the receiving address (Sixt, 2017, p.37). Figure 5 illustrates the usage of cryptography in transactions on the Bitcoin network according to its inventor Satoshi Nakamoto (2008, p.2). To conduct a transaction, the sender refers to the set of previous transactions that resulted in his possession of the respective bitcoin units (Sorge & Krohn-Grimberghe, 2012, p.1). This information includes all public keys that the Bitcoin units were previously assigned to. By using his private key to create a digital signature that contains an order to send the transaction to the receiver, the sender proves that he is the rightful owner of the sending public key. In a transaction, the sender is to create a data package that contains the public key of the receiver, a hash value about the data of previous transactions and a signature created by the sender (ibid.). The Bitcoin network makes use of the hashing algorithm SHA256 in conjunction with the so called Merkle-Damgård construction to project inputs of any length to a smaller collision resistant hash value (Sixt, 2017, p.38). The encryption of information by means of cryptography prevents interruptions of transactions as well as other means of fraud such as double spending (ibid.). Sorge & Krohn-Grimberghe (2012, p.2) demonstrate that an attempt to manipulate a transaction is practically impossible with our current technology as it would require a recalculation of the hash values of all previous transactions on the entire blockchain.

3.3.3.2 Decentralisation through Blockchain

According to Kerscher (2014, p.37), traditional payment systems usually rely on an intermediary (e.g. banks or companies like PayPal), who provides a platform for transactions or carries out transactions in a centralised manner. Giese et al. (2017, p.6f.) emphasise that the key feature of Bitcoin and its underlying blockchain technology lies in its decentralised structure (Giese et al., 2017, p.6f.). Cryptocurrencies forgo such an intermediation and thereby enable users to directly interact with each other. The decentralisation within the Bitcoin network is achieved through its peer-to-peer-architecture (Sixt, 2017, p.31). A peer-to-peer network is a system where all participants enjoy equality of privileges. Simultaneously, they also bear equal obligations towards one another (Ammous, 2018, p.192). For the case of Bitcoin, the privilege of its network participants lies in the removal of the need for trust in a third party while the obligation is to record every transaction within the system (ibid., p.171). In principle, every simple personal computer can become a part of the Bitcoin network and thereby maintain Bitcoin's shared database, i.e. the blockchain, by recording transactions (Giese et al., 2017, p.7).

Such a computer or client that actively participates in the maintenance is generally referred to as a node (Leys, 2014, p.46f.). Nodes must be distinguished from normal users, who do not provide computational power, but just hold units of Bitcoin in digital wallets and trade them between each other. In Figure 6, a theoretical transaction of 1 Bitcoin (BTC) from User1 to User3 is illustrated. Here, a transaction is initialised by User1 as a pending request, which is recorded by all nodes. Every Bitcoin transaction thereby contains three pieces of information: First, an input which is the Bitcoin address that was used to send the Bitcoins. Second, the amount, which is the number of Bitcoins exchanged. Third, an output, which is the address where the Bitcoins are sent (Miller, 2014, p.35). The blockchain is a public record that is shared among all network participants and contains all Bitcoin transactions in a chronological order. Blocks of pending transactions are created by all nodes individually and are then - after verification and validation - added to the public database roughly every ten minutes, creating a chain of these blocks (Guttmann, 2013, p.17).

Figure 6: The blockchain from the perspective of users and nodes



(Source: own creation based on Sixt, 2017, pp.39-42)

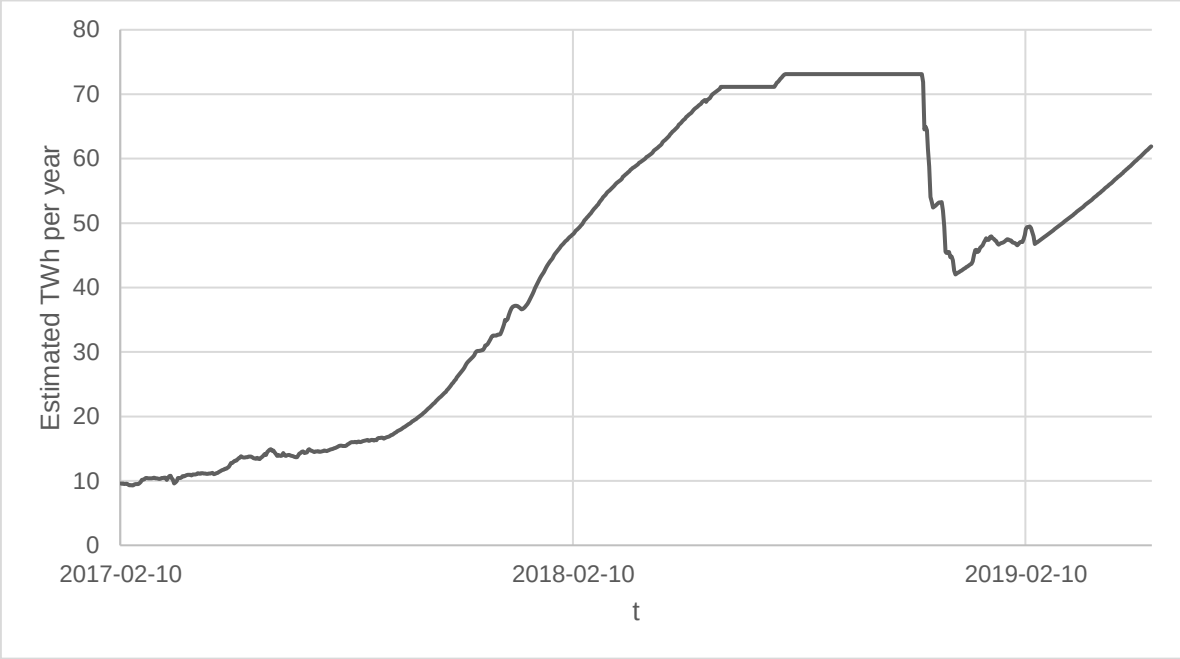
To determine, which node is allowed to add its block to the blockchain, nodes must use computational power to solve mathematical tasks (Kerscher, 2014, pp.81-85). It is then the node that solves this task first that is empowered to add its block to the blockchain (Heun, 2018, p.13). Finally, all other nodes copy this new version of the blockchain, and all balances of users are updated accordingly (Miller, 2014, p.43f.). In the exemplary transaction displayed in Figure 6, Node1 is able to solve the problem first and thus Node2 and Node3 verify and validate Node1's version of the blockchain, which is then taken as a basis to update all balances accordingly. Contrary to intermediated payment systems where a third party keeps track of all transactions in a centralised manner, the blockchain is maintained by all participants of the Bitcoin network that offer their computational power to the system (Franco, 2015, p.5). The process of creating blocks and appending them to the blockchain is commonly referred to as mining, which will be further explained in the following.

3.3.3.3 Mining by proof-of-work

The term mining describes the continuous process of using computer hardware to conduct mathematical calculations for the Bitcoin network (Guttmann, 2013, p.19). It is a metaphorical name, which hints at the similarities to gold mining (Giese et al., 2016, p.78). The calculations carried out by miners are needed to verify Bitcoin transactions, condense them into so called blocks and finally adding these to the

blockchain (Miller, 2014, p.124). This set of tasks is compulsory and existential for Bitcoin's ability to process new transactions (Giese et al., 2016, p.77). Hence, so called Miners, who offer their computational power, are rewarded with newly created Bitcoins and the total amount of transaction fees that were condensed in the added block (Franco, 2015, p.106f.). Thereby, the reward is not equally split among all miners within the network, but it is the miner who solves the mathematical problem first that is rewarded (Segendorf, 2014, p.75). In general, the term "calculate", which is commonly used to describe the process of mining is not precise. In fact, the Bitcoin algorithm does not provide problems which are possible to solve through calculations. Rather, these mathematical problems can only be solved by trial and error (Sixt, 2017, p.40). Consequently, miners who use the fastest hardware are not guaranteed to find every proof-of-work first but compared to miners with slower equipment their likelihood of finding one is higher (Miller, 2014, p.126f.). While in the early days of Bitcoin it was common to use personal computers to successfully solve proof-of-works, nowadays it is almost impossible to generate profits in that manner (Schredder, 2018, p.53). The competition on the field of mining has continuously increased in an arms-race of miners as Figure 7 illustrates which shows the estimated energy consumption of Bitcoin miners over time. In order to increase their likelihood of earning Bitcoin and also the predictability of their income, miners have formed larger mining pools by aggregating their computational power (Franco, 2015, p.150). In 2018, these pools have accounted for an energy consumption which is comparable to that of entire countries like Hungary or Switzerland (Babayan, 2019). Typically, mining pools operate their hardware in facilities located in countries where energy is relatively cheap (Franco, 2015, p.145). They receive funding from investors, who are in turn rewarded by mined Bitcoins, which are split among all investors according to their investment share (Miller, 2014, p.134). Critics argue that the presence of mining pools poses a threat to the idea of decentralisation since a small number of mining pools would be able to account for more than 50 percent of computational power (e.g. Gervais, Karame & Capkun, 2014, p.3). In such a scenario which is commonly referred to as a 51-percent-attack, a mining pool holding the majority of computational power would be able to decide which transactions will be validated and thereby conduct fraudulent double-spending (Sixt, 2017, p.105).

Figure 7: The estimated global energy consumption of Bitcoin mining



(Source: own creation based on data provided by Digiconomist.net website, n.d.)

The blockchain of Bitcoin is designed in a way that a new block is created every ten minutes (Nakamoto, 2008, p.4). A fixed difficulty of the mathematical problems to be solved by miners would imply that in a scenario of increasing computational power as it was present in recent years, the time needed to solve a problem and consequently create a block would decrease. Therefore, the difficulty of the respective proof-of-work's is determined by a moving average, precisely the average amount of blocks per hour (Sixt, 2017, p.41). In case the average time of ten minutes required for the creation of a block is fallen short of, the difficulty of mathematical problems will be adjusted biweekly (ibid.). The Bitcoin protocol specifies that the amount of newly created coins that miners are rewarded with will halve every four years (precisely every 210,000th block), eventually being removed entirely in 2140 (Miller, 2014, p.44). By that time, the total Bitcoin supply will have reached its maximum of around 21 million Bitcoin. Currently, a newly created block is rewarded with a newly created amount of 12.5 Bitcoin and in May 2020, this reward will be halved to 6.75 Bitcoin (Bitcoinblockhalf.com website, 2019).

4 Bitcoin as a means of exchange

4.1 A monetary theory perspective

The question whether Bitcoin is a feasible means of exchange is theoretically easy to answer, but from a practical perspective an underlying complexity unfolds as explained in the following subchapters. In chapter 2, the three basic functions of a currency as a means of exchange, as a store of value and as a unit of account have been examined. Although this paper aims at elaborating only one of these three functions, namely the means of exchange and payment function, all three functions must be considered at this stage of the analysis since there is an interdependence between these. For example, a commodity may only become a generally accepted means of exchange if it is also able to store value, since otherwise nobody would be willing to accept it (Ammous, 2018, p.4f.). Similarly, it is a logical consequence that money expresses the value of other goods and services in multiples of its units if it is used as a means of exchange (Vandezande, 2017, p.139). If we look at Bitcoin and its underlying concepts as laid out in chapter 3.3, it is arguable that the cryptocurrency from a mere theoretical point of view is capable of functioning as a means of exchange and payment (Giese et al., 2014, p.5). First, it is possible to exchange Bitcoin against other assets and to use it as a means of payment at a growing number of retailers, such as Microsoft, Dell or Expedia (Kasper, 2017, p.28; Madore, 2018).

Table 1: Bitcoin Denominations

Denomination	**Value**
Megabitcoin	1,000,000 BTC
Kilobitcoin	1,000 BTC
Hectobitcoin	100 BTC
Decabitcoin	10 BTC
Bitcoin	1 BTC
Decibitcoin	0.1 BTC
Milibitcoin	0.01 BTC
Microbitcoin	0.000001 BTC
Satoshi	0.00000001 BTC

(Source: own creation based on Miller, 2014, p.42 f.)

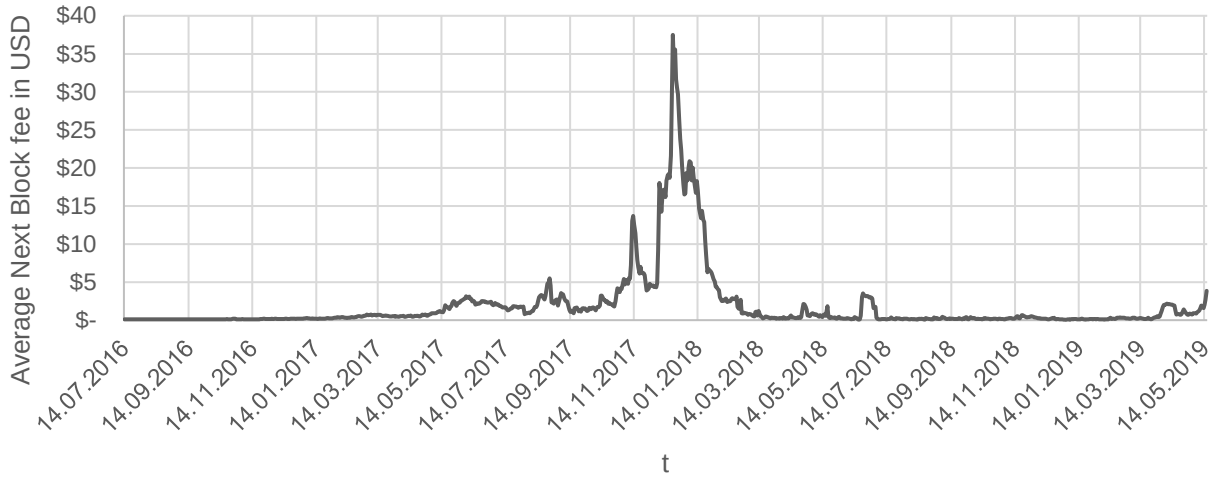
Second, Bitcoin's divisibility allows for prices to be expressed in its units as we can see in Table 1, which shows all commonly used denominations. Since Bitcoin is designed to increase in value over time, its source code allows transactions that are as granular as a hundredth of a millionth of 1 Bitcoin. This most granular unit on the Bitcoin network is called Satoshi (Miller, 2014, p.43). Hence, even if the price of one Bitcoin would reach a level of 1,000,000 USD, the current setting would still allow Bitcoin to display transactions in the 1 US Cent range, which would be the price of a Satoshi in such a scenario (Kenigsberg, 2013). Therefore, it can be argued that the underlying architecture allows for the use of Bitcoin as a unit of account. Third, Bitcoin may work as a suitable store of value. If a person purchases 1 Bitcoin, he or she may exchange it for other goods and services at any time as long as Bitcoin is accepted by other parties. Thereby, Bitcoin is able to preserve purchase power over time. While this purely theoretical examination is only answering the question whether it is possible to use Bitcoin as a means of exchange, it does not answer whether Bitcoin is actually used as such or whether it is likely to be used as such in the future. Therefore, the following subchapters shall further examine Bitcoin's usefulness as a means of exchange from a variety of perspectives.

4.2 A transactional perspective

4.2.1 Transaction costs

A major incentive of introducing Bitcoin as a means of payment is that transactions on its network are comparably cheap (Heun, 2018, p.138). Figure 7 shows the development of the average next-block transaction fee in USD over the last three years. Thereby, a next-block transaction fee is to be paid if a user wants his transaction to be confirmed by the blockchain within the next block, i.e. within the next ten minutes (Bitcoinfees website, n.d.). The fee peaked out in January 2018 at over 35 USD per transaction, but soon collapsed and remains at a price of less than 5 USD at present. When carrying out a transaction on the Bitcoin network, it does not matter whether the interacting parties are located in different countries or whether it is a domestic transaction; the transaction fee remains the same (Giese et al., 2016, p.141). Hence, Bitcoin provides for a universal world-wide means of payment. However, Berentsen & Schär (2017, p.245) emphasise that the fees directly paid by senders only account for a minor share of the total economic costs that each transaction involves.

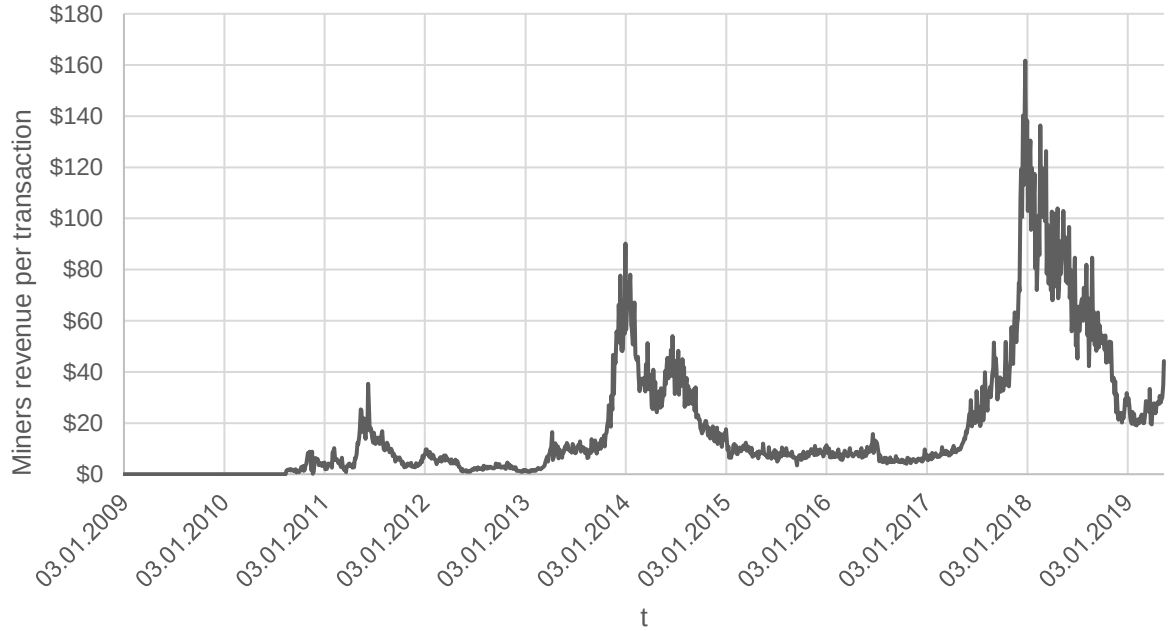
Figure 8: Average next-block transaction fee in USD



(Source: own creation based on data provided by bitcoinfees.info website, n.d.)

Since every block, which is mined ex-nihilo, creates new units of bitcoin as a compensation for the respective miner, the total supply is continuously extended. These newly minted Bitcoins represent additional costs, which are indirectly paid by the entirety of users on the network since the inflation of supply leads to a decreasing value of previously existing units (ibid., p.246).

Figure 9: The economic costs per Bitcoin-transaction



(Source: own creation based on data provided by blockchain.info website, n.d.)

Figure 9 illustrates the development of miners' revenue over time, which follows a similar trend as transaction fees, but is overall much higher. For instance, in January 2018, the network had to bear economic costs of over 160 USD per transaction, which were granted to miners as revenue. The effects of this inflation of Bitcoins is, however, difficult to detect predominantly due to the high level of volatility (Moos, 2019). Critics also raise concerns about the in chapter 3.3.3.3 mentioned waste of energy, which is caused by the energy consumption of miners (Thum, 2018, p.3). The Bitcoin Sustainability Report 2017 estimated the average energy consumption per transaction at 259 kWh, which is more than an average U.S. household needs per week (Digiconomist.net website, 2018).

4.2.2 Anonymity

Bitcoin transactions are by design not completely anonymous or secret, but rather public and pseudonymous. Whenever transactions are conducted on the Bitcoin network, users only identify each other by their addresses, i.e. public keys (Franco, 2015, p.14). The real identities behind public addresses remain hidden, thereby providing quasi anonymity or pseudonymity (ibid.). Kasper (2017, p.24) describes the degree of anonymity as incomplete, but nevertheless high. Users must not share their real identity and therefore remain anonymous, but by public keys they are provided with pseudo-identities that enable other users to trace back all transactions of their accounts (Sixt, 2016, p.33). Like cash in non-virtual commerce, Bitcoin is intended to allow its users to carry out anonymous transactions on the internet (Weber, 2013, p.80). Green (2013) describes the level of Bitcoin's anonymity as lying between cash and credit cards.

Wu (2017, p.4) notes that Bitcoin's anonymity provides people that have a relatively crucial demand for non-retraceable transactions, among others also criminals, with a solution. He further clarifies that the anonymity of Bitcoin is only a true advantage to individuals that have a reason to hide their identity, such as criminals (ibid.). Irwin & Milad (2016, p.410) reference a number of terrorist attacks that have evidently been financed with Bitcoins. Another notorious website that made use of Bitcoin's anonymity was the online black-market Silk Road, which operated in the dark web as a platform for selling illegal drugs (Wu, 2017, p.5). In October 2013, when the operator of Silk Road Ross Ulbricht was detained and the platform was shut down by the FBI, transactions on the website accounted for around 50 percent of Bitcoin's total

transactions (Küfner, 2018, p.95). Hence, despite the undisputed moral issues of these Bitcoin stakeholders, it remains evident that Bitcoin is used as a means of exchange by those who intend to remain hidden. Nonetheless, a variety of sources argue that due to the public ledger of all transactions it would be relatively easy to implement measures to trace back illicit transactions (e.g. Villasenor & Monk, 2011, p.18; Möser, Böhme & Breuker, 2013, p.1). Miller (2014, p.63f.) also identifies libertarians, cryptographers and privacy advocates as other possible user profiles with legal intentions of usage. In case the identity behind a public key is revealed, the anonymity of that specific user is diminished. According to Leys (2014, p.78), the blockchain represents both Bitcoin's biggest strength and its biggest weakness in terms of its anonymity.

4.2.3 Finality of transactions

Next to anonymity, another feature that is often referred when examining the potential of the Bitcoin network is the finality of transactions. This finality is a prerequisite of a decentralised payment system. In traditional centralised payment systems, funds, which are displayed on each user's account, are technically held by the system's operator and may thus be revoked in case of errors or fraud (Franco, 2015, p.15). Since such a party is absent in any decentralised payment scheme, moderation is not possible (ibid.). A Bitcoin transaction that has been verified, validated and then added to the blockchain is irreversible (Sixt, 2017, p.30). Therefore, if a hacker is able to unlawfully access other users' wallets and steals funds by sending them to his own wallet, there is no means to reverse the damage (Kasper, 2017, p.25). The same principle obviously applies for users that send their Bitcoins to a wrong wallet. Consequently, users are required to handle information regarding their accounts and transactions responsibly (Kerscher, 2014, p.37). In traditional payment schemes, a transaction usually imposes a risk of fraud on the side of the vendor. A buyer may try to spend his funds in excess of what he is actually eligible to and thereby receive goods or services of the seller without actually paying them. The underlying issue of this scenario is commonly referred to as the double spending issue (Asolo, 2018a). In his white paper, Nakamoto (2008, p.8) envisioned a network that would allow for electronic transactions without trust and consequently also without risk. However, according to Franco (2015, p.25), critics argue that in the Bitcoin network, the risk that traditionally lied at the side of the vendor is shifted to the buyer. Those buyers that experience

fraud, such as non-delivery of goods and hence look for a retraction of payments, will face difficulties if they are unaware of the vendors real identity (ibid.). However, Dourado (2015, p.33) explains that Bitcoin in fact provides for an opportunity to conduct reversible transactions or so-called multi-signature transactions. Thereby, a third party in form of an arbitrator is involved into a transaction whose presence improves the security of a transaction (Asolo, 2018b). The arbitrator ensures that transferred funds remain locked in an escrow account until the goods have been delivered and consequently prevents the buyer from being subject to scams (Buntinx, 2017). Such a set up obviously raises transaction costs due to costs of arbitration, but according to Dourado (2015, p.33) the total transaction costs is still lower than those of credit card systems. However, an analysis carried out by tradeblock.com (2015) shows that the relevance of multi-signature transactions is relatively low with a share of less than 1% of all transactions. In the absence of more recent data on this subject, it must be assumed that their relevance is still negligible at the present day. For Bitcoin's envisioned role to become a widely used means of payment, the aspect of finality of payments may pose a severe obstacle. The conjunction of irreversible transactions and little to no room for legal recourse in case of fraud may significantly hinder a mass market adoption of cryptocurrencies (Kasper, 2017, p.25; Franco, 2015, p.5).

4.2.4 Complexity

A third reason for the relatively slow adoption of Bitcoin as a means of exchange is its inherent complexity (Sixt, 2017, p.91). John McAfee - founder of an anti-virus program and a celebrity in the cryptocurrency community - stated that Bitcoin would be "too complex for the average individual" (Young, 2015). Especially in e-commerce, a relatively easy handling is of significant importance for payment solutions since most retailers usually provide a variety of payment methods. Hence, these methods are competing with each other (Heun, 2018, p.145). A situation in which this complexity unfolds is the acquisition of new Bitcoins. Yermack (2013, p.10) described that while in the first years of Bitcoin's presence, users were able to acquire units of Bitcoin through mining them with personal computers, this practice has nowadays practically vanished due to an increased mining difficulty, which came about with increased competition on the field of Bitcoin mining (see also Co, 2017). Instead, users have to set up a purchase on an online exchange by providing the exchange with their bank

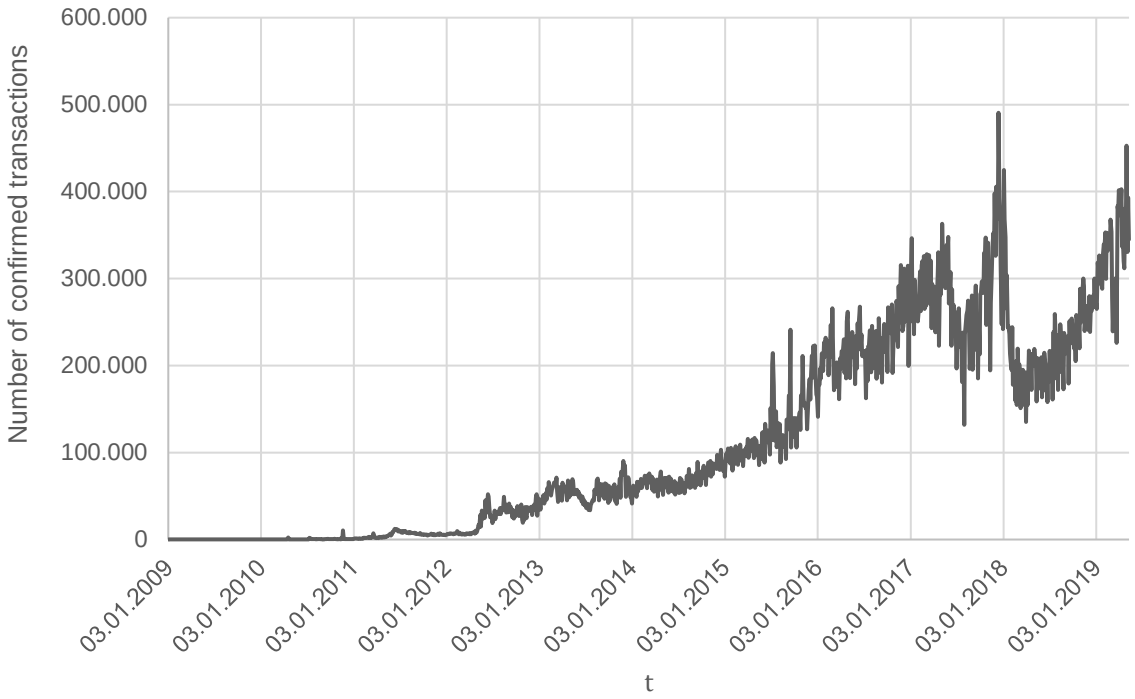
account information which implies a certain counter party risk due to low liquidity and other systematically intrinsic risks on the side of exchanges (ibid.).

4.3 A market perspective

4.3.1 Intended use of market participants

Among all cryptocurrencies, there is no doubt that Bitcoin to this day is the most widely adopted cryptocurrency with thousands of companies accepting it as a means of payment (Walton & Johnston, 2018, p.166; Franco, 2015, p.22). In addition, the number of daily transactions on the Bitcoin network experienced a rise from its inception until its peak price in early 2018 as Figure 7 indicates.

Figure 10: The number of confirmed daily transaction on the Bitcoin network



(Source: own creation based on data provided by blockchain.info website, n.d.)

The figure shows the development of the number of daily transactions that were confirmed on the blockchain of Bitcoin over time. In contrast to the market price which is still recovering from its collapse that unfolded throughout the year 2018, the number of transactions recovered relatively quickly and continues to rise to this day. However, this tendency does not provide evidence for the emergence of Bitcoin as a means of exchange since the majority of transaction is according to the U.S. Drug Enforcement Administration not devoted to the sale or purchase of goods, but to price speculation (Russo, 2018). Baur, Hong & Lee (2017, p.2) note that for Bitcoin to become a

generally accepted means of exchange, it would consequently have to be predominantly used to purchase and sell goods and services, competing with other fiat currencies. As pointed out, such a usage is currently the exception rather than the norm.

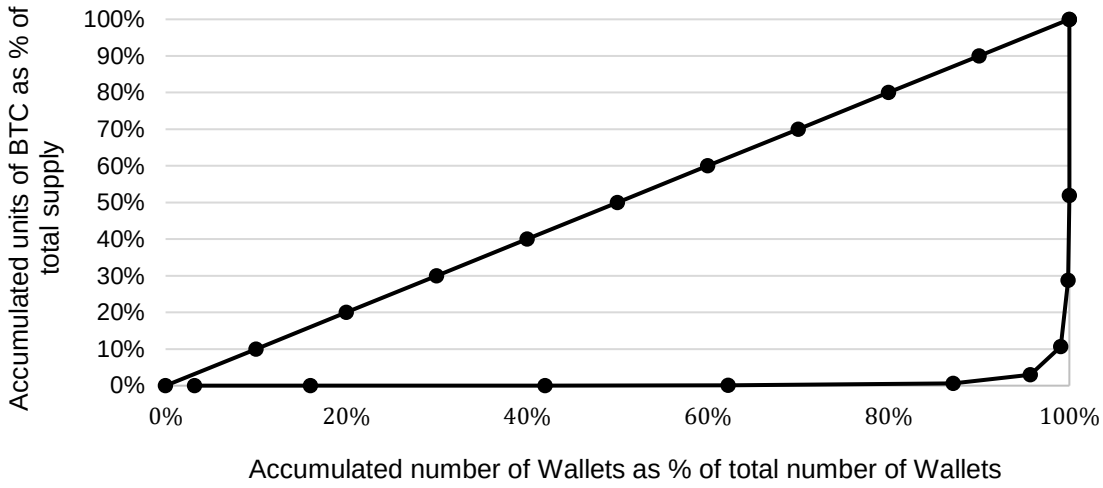
Furthermore, a recent study carried out by Bitwise Asset Management (2019, pp.20-62) presents evidence that the total volume of Bitcoin transactions is actually much lower than it is presented on widely accepted websites such as coinmarketcap.com, because most exchanges would artificially inflate these volumes to benefit from appearing as more widely used than they actually are. Thereby, the reported daily Bitcoin trade volume of around 6 billion USD which represents a daily turnover of 8.6 percent, shrinks to an actual figure of 273 million USD and a turnover of 0.39 percent if only the volume of those exchanges is considered that were deemed legitimate by the study (ibid., p.61f.). The relatively low turnover of Bitcoin might again be caused by its primary use as a speculative investment. Most of Bitcoin's users simply hoard their bitcoins on inactive accounts, hoping to achieve gains from a future Bitcoin price increase (Franco, 2015, p.27). Kerscher (2014, p.125) described the phenomenon of hoarding as a consequence of deflation caused by the inherent scarcity of circulating Bitcoins. In times of increasing demand for Bitcoins, holders have a lower incentive to spend their funds since they expect their Bitcoins to be more valuable in the future, meaning that the prices of goods and services in Bitcoin will decrease. In such a scenario, prices of goods would however not really decrease for Bitcoin holders since the acceptance of Bitcoin as a means of payment is still relatively low and thus most goods or services cannot be acquired using Bitcoins (ibid., p.127f.). Much rather, Bitcoin would fail to establish itself as a means of payment and exchange (ibid.).

4.3.2 Market concentration

Alongside the phenomenon of hoarding, Bitcoin's supply is spread very unevenly amongst its wallets as Figure 8 indicates. Here, the concentration of Bitcoin units on relatively few wallets is illustrated in comparison with a straight line which represents a theoretical equal distribution of Bitcoin across all wallets. In fact, 3 percent of Bitcoin wallets hold a combined share of more than 95 percent of the total supply of Bitcoins. Wallets are thereby held by a person or a legal entity, but there is no way to draw a precise conclusion for the distribution of Bitcoins among its users since one user may

hold multiple wallets or conversely, a group of users may share a single wallet (Leys, 2014, p.124f.).

Figure 11: The distribution of Bitcoin units on registered wallets



(Source: own creation based on data provided by bitinfocharts.com website, 2019)

Courtois (2014, p.31) notes that the large inequality of wealth distribution on the Bitcoin network may lead to late adopters leaving the cryptocurrency aside, seeking for a new one that offers more equality.

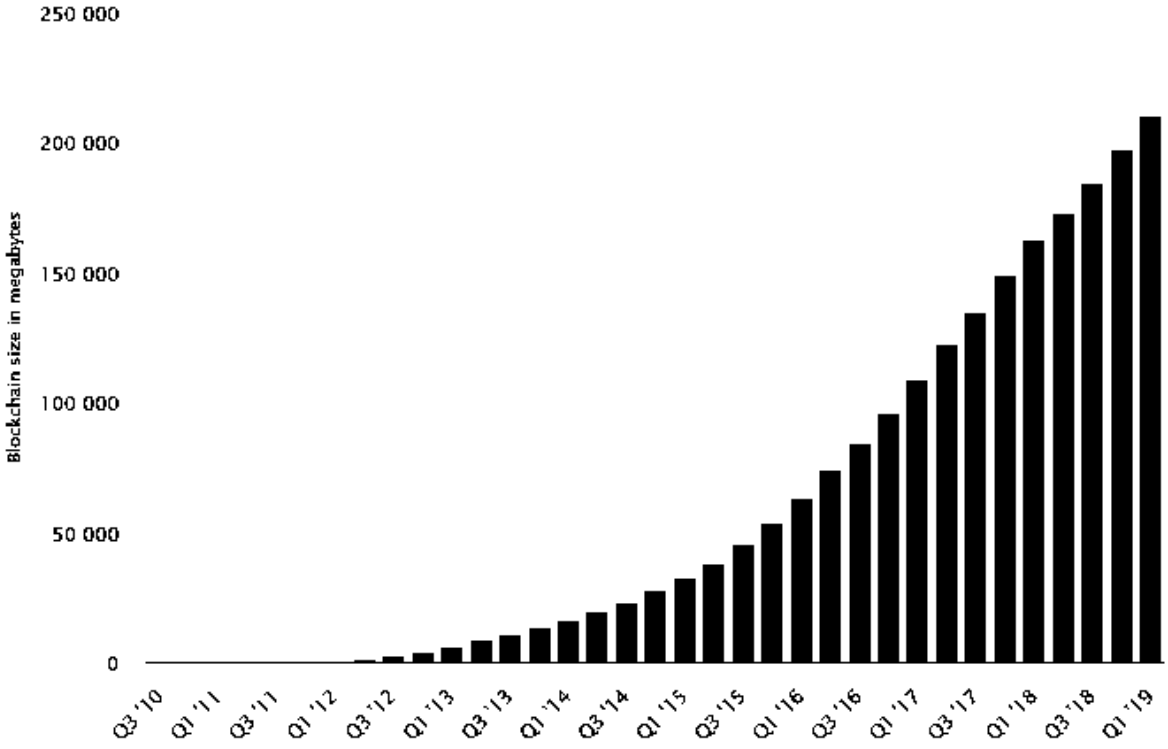
4.4 A conceptual perspective

4.4.1 Scalability

A conceptual weakness that could potentially hinder Bitcoin from becoming the world's most widely used means of exchange is the so-called scalability issue (Berentsen & Schär, 2017, p.251). Thereby, the issue unfolds in two different ways. First, to avoid the number of transactions from becoming large enough to overexert the network, Bitcoin is designed in a way that there is a hard cap of transactional throughput, which cannot be exceeded (Gurguc & Knottenbelt, 2018, p.19). This conceptual limit is enforced by the maximum size of each block as well as the average confirmation time of ten minutes per block, which is as already mentioned in chapter 3.3.3.3 maintained by adjusting the mining difficulty in accordance to the computational power of nodes (Berentsen & Schär, 2017, p.250). If the number of transactions is higher than the maximum of transactions that can be processed under these restrictions, the blockchain congests (Bank of International Settlements, 2018, p.100). Currently, the number of transactions is taxed at around 400,000 per day with a rising trend as

previously shown in Figure 7 (see chapter 4.3.1). A second dimension of the scalability issue is linked to the growing size of the blockchain. As a consequence of the requirement to represent an accurate account of all historic transactions, the blockchain's size has continuously increased as shown in Figure 10. The current size of the blockchain accounts for around 210 GB and the curvature of the graph indicates an exponential growth in upcoming years. At the present day, these two dimensions of the scalability issue only partly affect both miners and users, since neither the maximum storage capacity of miners has been exceeded nor the maximum number of transactions. The theoretical transactional capacity of the Bitcoin network lies at 27 transactions per second, which equates to 972,000 transactions per day and is therefore still relatively far from being reached with a historic peak of daily transactions that occurred in December 2017 with around 405,000 transactions (Georgiadis, 2019, p.1; blockchain.info website, n.d.). However, the implications of these two tendencies for the future role of Bitcoin only become clear if we compare its capacities with those of its competitors.

Figure 12: Bitcoin's blockchain size over time



(Source: Statista, 2019)

At the time of writing, VISA processes an average of 150 million transactions per day or 1736 transactions per second, which is more than 150 times higher than the capacity of Bitcoin (VISA USA website, n.d., Georgiadis, 2019, p.1). According to Moos (2019), the current limit of 2 MB per block on the Bitcoin network allows for 3500 transactions per block with each transaction accounting for an average of 570 bytes. In a theoretical scenario where we project the number of VISA transactions onto Bitcoin's blockchain, its incapability of representing any kind of competition in its current state becomes obvious. For example, the block creation time would have to be shortened from currently ten minutes to just two seconds per block to process the number of transactions that are currently processed on the VISA network. Similarly, if we assume the ten minute average time frame of block creation to remain, each block's size would have to be increased to 600 MB and hence the size of the blockchain would increase in a way that it would soon be impractical to store its whole version on most computational devices (Bank of International Settlements, 2018, p.99).

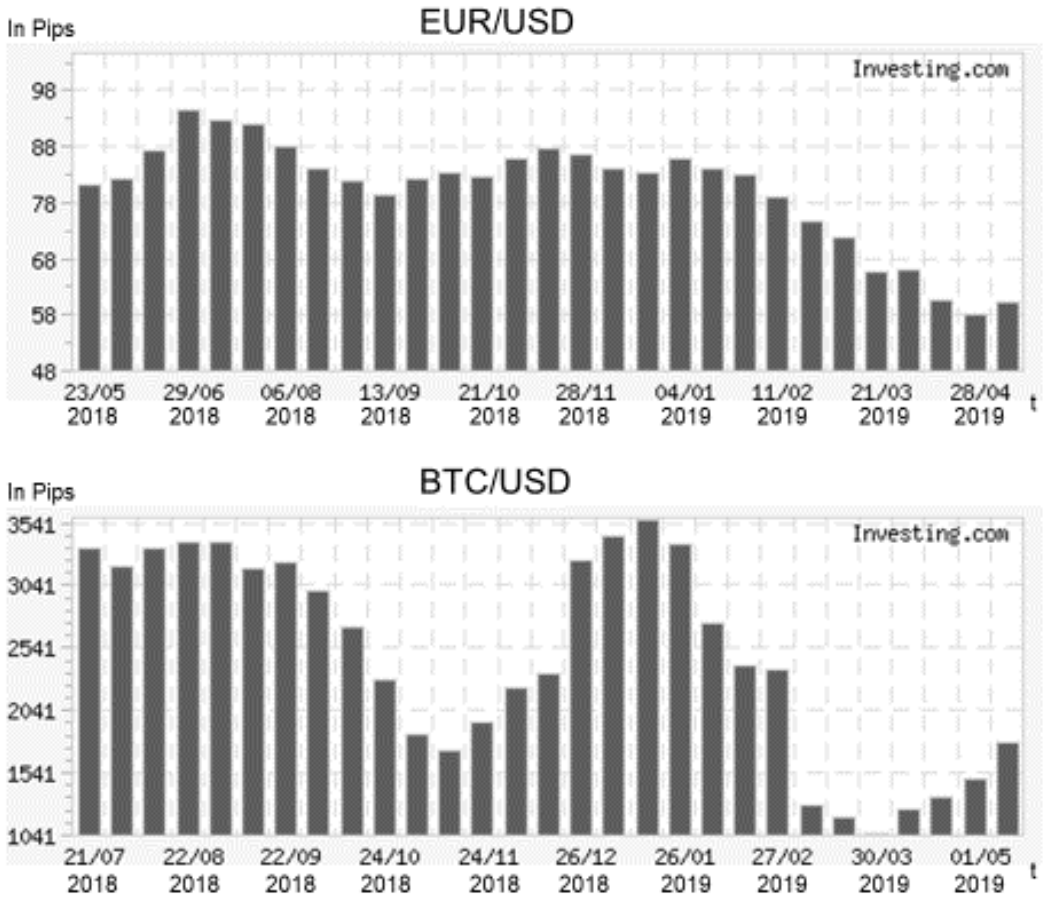
4.4.2 Volatility

Volatility describes an asset's fluctuation in price over a period of time (Wirtschaftslexikon Gabler, n.d.). From a currency perspective, low volatility can be identified a characteristic feature that unites all major established currencies in today's global economy (Miller, 2014, p.155; Sixt, 2017, S.107). Thereby, central banks hold a monopoly on the issuance of new bank notes which allows these centralised entities to determine the currency supply (Godschalk & Krüger, 2000, p.4). By either contracting or extending this supply of monetary units, central banks anticipate fluctuations on the demand side of currencies following a monetary policy that is among other motives oriented on securing monetary stability (Borchert, 2001, p.275; Jarchow, 2010, p.11ff.).

In contrast to government currencies, Bitcoin's volatility is significantly higher as Figure 11 indicates. The data provided by investing.com (n.d.), which displays the development of standard deviations of the exchange pairs of EUR/USD in comparison with BTC/USD illustrates the fact that the degree of volatility that Bitcoin experiences is in fact significantly higher than the volatility of the two most widely used currencies in the present-day economy. While the standard deviation of the Euro price in units of USD fluctuated between 60 and 90 pips in the period from July 2018 to May 2019, the standard deviation for the Bitcoin price in units of USD amounted to significantly higher

figures ranging from 1000 to 3500 pips. According to Leys (2014, p.84), Bitcoin's relatively high price volatility might pose the most severe obstacle for the cryptocurrency's adoption. If a retailer introduces an option for customers to make payments with Bitcoin, he introduces a certain exchange rate risk to his operations (Giese et al., 2017, p.142).

Figure 13: Volatility of EUR/USD and BTC/USD in Pips



(Source: investing.com website, n.d.)

Since Bitcoin's exchange rate to government-currencies like Euro or USD constantly fluctuates, the usage of Bitcoin implies great uncertainty for both customers and retailers: Customers might be worried that the units of Bitcoin that they are holding will be more valuable in the future and therefore refrain from spending them. Similarly, retailers might be afraid that those units of Bitcoin that they accept as payments might lose their value in the future (Sixt, 2017, S.107). The reasons for this phenomenon of volatile exchange rates that does not only affect Bitcoin but very much the entirety of cryptocurrencies apart from stable coins are manifold. As already pointed out in chapter 3.3.3.2, the Bitcoin network forgoes the installation of a centralised entity that

governs over the supply of Bitcoin units. Instead, the supply is fixed by the networks source code that sets the limit of coins to around 21 million, which are gradually being issued until the year 2140 (Miller, 2014, p.44). Consequently, in times of fluctuations of demand for Bitcoin, there is no entity that may alter the supply in an anticipating manner as it is the case in governmental monetary schemes. This conceptual issue is paired with a set of other issues that create an environment governed by uncertainty. First, although the market capitalisation of Bitcoin has experienced a remarkable growth in recent years, it still remains a comparably small market (Franco, 2015, p.33). On the day of writing, the market capitalisation of cryptocurrencies listed by coinmarketcap.com (n.d.) accounts for a little over 300 billion USD with Bitcoin resembling a share of 65% or 208 billion USD. In comparison, the global stock market reached a capitalisation of 76.3 trillion USD in 2017 (FXCM website, n.d.). Therefore, even a comparably small amount of transactions can lead to stark fluctuations of Bitcoin's market price (Vejačka, 2014, p.77). If this tendency is viewed in conjunction with the aforementioned high concentration of units of Bitcoin on a small number of wallets, it becomes evident that a small number of individuals are able to greatly influence the market price as news headlines of price drops that followed large scale transactions further indicate (e.g. Recksiek, 2019; Akhtar, 2019).

In addition to this issue, while Bitcoin enthusiasts often tend to use the term of fiat money in a derogatory manner to point at the lack of intrinsic value of governmental currencies, Bitcoin suffers from the same issue to an even larger degree. The network's coins are not backed by any assets and furthermore, laws that enforce the acceptance of the currency – as present for governmental currencies – are missing (Kerscher, 2018, p.16; Franco, 2015, p.31). Consequently, the only factor that determines the market price of Bitcoin is the market participants' perception of their future value (Ciaian, Rajcaniova & Kancs, 2014, p.6). A statistical model developed by Kinderis, Bezbradica & Crane (2018, p.11) to predict the price development of Bitcoin empirically backs this observation by suggesting that the most dominant influence factor on the Bitcoin price is the sentiment of market participants that was observed on social media platforms. Real time events on cryptocurrency markets and news headlines would thereby lead to price shifts that could be explained and foreseen by their model (ibid.).

An issue that is a staple in those headlines is the regulatory uncertainty of Bitcoin, which provides for another potential factor contributing to the cryptocurrency's intense

volatility (Kerscher, 2014, p.109). Although Franco (2015, p.30) notes that confiscation of Bitcoins is technically impossible, which distinguishes the cryptocurrency from governmental currencies or precious metals, governments might still introduce significant burdens or even ban the use of cryptocurrencies by shutting down exchanges and payment processors, which handle a major share of transactions (Franco, 2015, p.32; Weber, 2013, p.11). On the other hand, government regulation must not necessarily have negative implications. While an over-regulation in a solely restrictive manner would severely impair the usefulness of Bitcoin as a means of exchange, a more moderate regulatory policy could change the fraudulent and illicit image of the cryptocurrency and simultaneously relieve market participants from present regulatory uncertainty (Kerscher, 2014, p. 113).

5 Conclusion

5.1 Summary

Considering all facts presented in this work, it must be concluded that Bitcoin in its current state will likely not assume an important role as a means of payment and exchange.

In chapter 2, a review of monetary theory and an explanation of the role of currencies in modern economies has been provided. The triad of intrinsic functions of currency as a unit of account, a store of value and a means of exchange and payment greatly enhance an economy's efficiency. Absolute prices measured in units of a respective currency significantly reduce the resources that parties must spent on the procurement of price information and additionally enable all kinds of commercial accounting. By being utilised as a generally accepted means of exchange and payment, the presence of currencies also introduces a means to divide transactions into sales and purchases, replacing the double coincidence of wants as present in barter economies by a single coincidence. The third intrinsic function of currency as a store of value empowers its holders to preserve their purchase power over time and spend funds whenever a need arises. Here, the stability of value of a currency is of great importance and consequently, currency schemes must overcome issues of inflation and volatility to provide their holders with a sufficient degree of certainty to properly function as a store of value. If a currency shall function in the aforementioned ways, academic literature additionally suggests that a currency should have a set of properties, which are described by the five features of portability, permanency, homogeneity, divisibility and scarcity.

In chapter 3, both virtual currencies and cryptocurrencies have been defined and distinguished before examining the technical underlying of the cryptocurrency of Bitcoin. While virtual currencies usually serve as a means of payment within a specific community to carry out transactions, cryptocurrencies differ from them by their universal accessibility and their decentralised design. The latter emerged in 2008 when the white paper of Bitcoin was published, being the first currency scheme that combined the technologies of decentralised ledgers, blockchain and cryptography. Throughout the relatively short history of cryptocurrencies, Bitcoin has always remained the most dominant player on its market, although countless other cryptocurrency projects have emerged. Thereby, its market capitalisation has over the course of numerous investment bubbles continuously risen. Within the Bitcoin network,

transactions are carried out between public addresses that use cryptographic private keys to verify their rightful ownership, thereby preventing users from fraudulent transactions, such as double spending. Instead of making use of a centralised entity that monitors transactions, Bitcoin shifts the responsibility of maintenance to the entirety of its network. So called miners offer their computational power to keep track of all transactions and create a blockchain that resembles a record of all transactions. In turn, miners are rewarded with newly minted units of Bitcoin as well as collected transaction fees whenever they have been able to create and add a new block to the blockchain.

In chapter 4, the feasibility of Bitcoin as a means of exchange has been examined by pooling the results of the previous two chapters as well as showing additional practical implications that arise from different perspectives. The cryptocurrency is arguably able to theoretically fulfil all three functions of currencies. However, when looking at the feasibility of Bitcoin as a means of exchange and payment from a more practical perspective, several obstacles seem to hinder its usefulness. First, although the fees per transaction appear to be comparably low, the overall costs per transaction that shall be borne by the entire network are significantly higher. Moreover, the combination of quasi-anonymity and finality of transactions are only truly beneficial to people involved in criminal activities and instead introduce additional risks to those, who purchase goods and services with Bitcoin. Thirdly, the inherent complexity represents another obstacle to mass market adoption. From a market-perspective, the rising number of transactions does not indicate that the acceptance of Bitcoin is growing because most of these transactions are devoted to speculation. Additionally, studies suggest that the overall transaction volume might in fact be much lower than the figures that are displayed by major data providers. Instead of using Bitcoin as a means of payment, most holders simply hoard the cryptocurrency on cold storage accounts, hoping to benefit from potential future price appreciation. The tendency of hoarding is furthermore combined with the issue that Bitcoin’s supply is very unevenly spread amongst its wallets which might deter late adopters from using Bitcoin when other cryptocurrencies offer more equality. Alongside transactional and market-related issues, Bitcoin also suffers from conceptual weaknesses that unfold in its restricted scalability and high levels of volatility. Although the scale of the Bitcoin network has not reached a level where its functionality is negatively impaired, the cryptocurrency has a hard cap of transactional throughput and also the size of the blockchain is

continuously increasing, which both provide for obstacles assuming continuous growth of transactional volume. A major reason for the volatile nature of Bitcoin are the absence of a central entity that governs over the supply of Bitcoin. Since the supply of coins is fixed, shifts on the demand side lead to price fluctuations that are far greater than those of governmental currencies.

The entirety of presented findings in this work lead to the conclusion that the intrinsic function of currency as a means of exchange and payment can theoretically be fulfilled by Bitcoin, but when looking at the cryptocurrency from a more practical perspective, the aforementioned restrictions and weaknesses seem to significantly impair its potential to assume such a role in the future. While the technicality and the economic costs of transactions may be seen as minor obstacles to the usefulness of Bitcoin in present day commerce, the characteristics of the Bitcoin market as well as its conceptual design indicate that the project is not only not used as means of exchange and payment, but also not designed in a way that allows for broad acceptance. In fact, low turnover rates, hoarding of Bitcoins and predominantly speculative transactions show that most users interpret the cryptocurrency as a means of storing value that has a potential to generate gains from future price appreciation. Apart from this tendency, the conceptual analysis provided by this work additionally shows that Bitcoin suffers from severe scalability issues, which unfold in its comparably low capacity to process transactions and in the growing size of the blockchain. It has been demonstrated that these two conceptual restrictions will lead to issues that will under the assumption of a continuous growth of transactional volume significantly impair the functionality of the network.

5.2 Critical acclaim

Both Bitcoin and cryptocurrencies in general are still in an infancy-stage of development. The coverage of Bitcoin in macroeconomic literature is consequently relatively low and often shallow. On top of that, the sources that were reviewed in the course of this work tend to focus either at the pros or the cons of Bitcoin’s usefulness as a means of exchange. This tendency reflects continuous discussions of Bitcoin critics and enthusiasts, which might partly also be detached from mere facts due to the conflict of interest of governmental institutions and Bitcoin investors. The findings of presented in this work are also not to be projected on other cryptocurrency projects that have emerged either as improved versions of Bitcoin or as entirely new forms of

cryptocurrencies. Throughout this work, the role of Bitcoin as a means of exchange is evaluated from a global perspective. More specific research might draw different conclusions on the feasibility of the cryptocurrency as a means of exchange and payment, e.g. for distinct economies that suffer from dysfunctional currency schemes with high levels of inflation.

5.3 Outlook

The findings of this work indicate that Bitcoin is unlikely to assume a role of a generally accepted and widely adopted means of exchange and payment. Although the currency would thereby ultimately fail to fulfil its initially intended purpose, its systematically inherent and unique scarcity might lead to Bitcoin becoming a useful store of value for investors. It is also likely that Bitcoin will remain a useful means of exchange and payment in smaller online communities, e.g. in online black markets where the advantages of quasi-anonymity and finality of transactions outweigh the disadvantages of volatility, low scalability and complexity. Additionally, although Bitcoin's protocol itself cannot be altered, developers and users might fork the currency to create an improved version of the cryptocurrency as it has happened in the past. It is therefore possible that a future version of Bitcoin is introduced by a fork that is able to overcome the issues that the current Bitcoin network suffers from. In such a case the usefulness of Bitcoin as a means of exchange and payment would have to be reconsidered in the course of future academic work.

III. Glossary

Dutch Tulip Mania	An excessive trend of purchasing and growing tulips that was prevalent in Holland about 1634 and led to high levels of speculation (Merriam Webster, n.d.).
Guinea	An old British unit of currency that is still occasionally used in auctions (Collins Dictionary, n.d.).
Lightning Network	A new protocol that aims at achieving a higher transactional throughput of the Bitcoin network and lower transaction costs (Blockstream website, n.d.).
Merkle-Damgård construction	A method of building collision-resistant cryptographic hash functions (Sixt, 2017, p.38).
Peer-to-Peer	A network in which users are able to share information directly with each other without depending on a central server (Merriam Webster, n.d.).
SegWit	A process that separates transactional signatures from Bitcoin transaction, thereby raising the maximum number of transactions within one block (Binance.vision website, n.d.).
SHA 256	A hash algorithm that generates a 256 Bit random sequence of characters out of any given input to protect digital information (Decryptionary website, n.d.).

IV. List of References

Ahamad, Shaik Shakeel; Nair, Madhusoodhan; Varghese, Biju (2013): A survey on Crypto Currencies. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.428.7952&rep=rep1&type=pdf>
[Accessed at 28 June 2019].

Akhtar, Tanzeel (2019): Ten Mysterious Crypto Whales Influence Bitcoin Prices. Retrieved from <https://www.kitco.com/commentaries/2019-05-06/Ten-Mysterious-Crypto-Whales-Influence-Bitcoin-Prices.html>
[Accessed at 3 July 2019].

Ammous, Saifedean (2018): The Bitcoin Standard. New Jersey: John Wiley & Sons.

Asolo, Bisade (2018a): Double-Spending explained. Retrieved from <https://www.mycryptopedia.com/double-spending-explained/>
[Accessed at 28 June 2019].

Asolo, Bisade (2018b): Multisignature Technology explained. Retrieved from <https://www.mycryptopedia.com/multisignature-technology-explained/>
[Accessed at 28 June 2019].

Babayan, Davit (2019): Bitcoin's Energy Consumption Equalled That of Hungary in 2018. Retrieved from <https://www.newsbtc.com/2019/03/14/bitcoins-energy-consumption-equalled-that-of-hungary-in-2018/>
[Accessed at 7 June 2019].

Bank of International Settlements (2018): Annual Economic Report. Retrieved from <https://www.bis.org/publ/arpdf/ar2018e.pdf>
[Accessed at 4 June 2019].

Baur, Dirk; Hong, KiHoon; Lee, Adrian (2017): Bitcoin: Medium of Exchange or Speculative Assets?. Retrieved from <https://www.researchgate.net/publication/321988034_Bitcoin_Medium_of_Exchange_or_Speculative_Assets>
[Accessed at 5 June 2019].

Bech, Morten; Garratt, Rodney (2017): Central Bank Cryptocurrencies. Retrieved from <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041906>
[Accessed at 1 June 2019].

Berentsen, Aleksander; Schär, Fabian (2017): Bitcoin, Blockchain und Kryptoassets – Eine umfassende Einführung. Basel: BoD Books on Demand.

[Binance.vision website] (n.d.): Segregated Witness (SegWit). Retrieved from <https://www.binance.vision/glossary/segregated-witness>
[Accessed at 25 June 2019].

[Bitcoinblockhalf.com website] (2019). Retrieved from <https://www.bitcoinblockhalf.com/>
[Accessed at 31 May 2019].

[Bitcoinfees.info website] (n.d.). Retrieved from <https://bitcoinfees.info/>
[Accessed at 04 June 2019].

[Bitinfocharts.com website] (2019): Bitcoin distribution. Retrieved from <https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html>
[Accessed at 29 June 2019].

Bitwise Asset Management (2019): Presentation to the U.S. Securities and Exchange Commission. Retrieved from <https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf> Accessed at [28 May 2019].

[Blockchain.info website] (n.d.): Average USD market price across major bitcoin exchanges. Retrieved from <https://www.blockchain.com/charts/market-price?timespan=all>
[Accessed at 29 June 2019].

[Blockchain.info website] (n.d.): Average USD market price across major bitcoin exchanges. Retrieved from <https://www.blockchain.com/charts/market-price?timespan=all>
[Accessed at 23 June 2019].

[Blockchain.info website] (n.d.): Confirmed Transactions Per Day. The number of daily confirmed Bitcoin transactions. Retrieved from <https://www.blockchain.com/de/charts/n-transactions?timespan=all>
[Accessed at 1 July 2019].

[Blockstream website] (n.d.): Was ist das Lightning-Netzwerk?. Retrieved from <https://blockstream.com/lightning/>
[Accessed at 22 June 2019].

Borchert, Manfred (2001): Geld und Kredit. München: Oldenbourg Wissenschaftsverlag.

Buntinx, J.P. (2017): What is a Multisignature Escrow Wallet?. Retrieved from <https://themerkle.com/what-is-a-multisignature-escrow-wallet/>
[Accessed at 28 June 2019].

Ciaian, Pavel; Rajcaniova, Miroslava; Kancs, d'Artis (2014): The Economics of BitCoin Price Formation. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1405/1405.4498.pdf>
[Accessed at 30 June 2019].

Co, Mike (2017): Mine for Bitcoin with any Computer. Retrieved from <https://hackernoon.com/mine-for-bitcoin-with-any-computer-9a30337843e7> [Accessed at 23 June 2019].

[Coinmarketcap.com website] (n.d.): Top 100 Cryptocurrencies by Market Capitalization. Retrieved from <https://coinmarketcap.com/> [Accessed at 11 July 2019].

[Collins Dictionary] (n.d.): Guinea. Retrieved from <https://www.collinsdictionary.com/dictionary/english/guinea> [Accessed at 23 June 2019].

Courtois, Nicolas T. (2014): On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies. Retrieved from <https://www.researchgate.net/publication/262071868_On_The_Longest_Chain_Rule_and_Programmed_Self-Destruction_of_Crypto_Currencies> [Accessed at 29 June 2019].

Dabrowski, Marek; Janikowski, Lukasz (2018): Virtual currencies and central banks' monetary policy: challenges ahead. Monetary dialogue July 2018. European Parliament. Retrieved from <http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf> [Accessed at 23 June 2019].

[Decryptionary website] (n.d.): Secure Hash Algorithm 256 [SHA 256]. Retrieved from <https://decryptionary.com/dictionary/secure-hash-algorithm-256/> [Accessed at 4 July 2019].

[Digiconimist.net website] (n.d.): Bitcoin Energy Consumption Index. Retrieved from <https://digiconomist.net/bitcoin-energy-consumption> [Accessed at 1 July 2019].

Dourado, Eli (2015): Bitcoin Transactions Are Reversible. In: Berlatsky, Noah (Ed.): Bitcoin. Farmington Hills: Greenhaven Press.

DuPont, Quinn (2019): Cryptocurrencies and Blockchains. Cambridge: Polity Press.

Franco, Pedro (2015): Understanding Bitcoin. Cryptography, engineering, and economics. West Sussex: John Wiley & Sons.

[FXCM website] (n.d.): What causes Volatility in Bitcoin?. Retrieved from <https://www.fxcm.com/uk/insights/what-causes-volatility-in-bitcoin/> [Accessed at 3 June 2019].

Gabler Wirtschaftslexikon (n.d.): Volatilität. Retrieved from <https://wirtschaftslexikon.gabler.de/definition/volatilitaet-48641> [Accessed at 28 June 2019].

Gervais, Arthur; Karame, Ghassan; Capkun, Srdjan (2014): Is Bitcoin a Decentralised Currency?. Retrieved from <https://www.researchgate.net/publication/270802537_Is_Bitcoin_a_Decentralized_Currency?enrichId=rgreq0b44d5b910596ed9ce202366772ecd2fXXX&enrichSource=Y292ZXJQYWdlOzI3MDgwMjUzNztBUzo0NDIwMzg4MTU1OTY1NDRAMTQ4MjQwMTY3NDA5NQ%3D%3D&el=1_x_3&_esc=publicationCoverPdf>
[Accessed at 22 June 2019].

Georgiadis, Evangelos (2019): How many transactions per second can bitcoin really handle?. Retrieved from <https://eprint.iacr.org/2019/416.pdf>
[Accessed at 12 June 2019].

Giese, Philipp; Preus, Max; Kops, Maximilian; Wagenknecht, Sven; de Boer, Danny (2016): Die Bitcoin-Bibel. Das Buch zur digitalen Währung. Kleve: BTC-ECHO.

Godschalk, Hugo; Krüger, Malte (2000): Why e-money still fails – chances of e-money within a competitive payment instrument market. Retrieved from <https://www.researchgate.net/publication/244136842_Why_e-money_still_fails_-_chances_of_e-money_within_a_competitive_payment_instrument_market>
[Accessed at 14 June 2019].

Google Trends (n.d.): Search term: bitcoin. Retrieved from <https://trends.google.de/trends/explore?date=2008-08-01%202019-07-11&q=bitcoin>
[Accessed at 11 July 2019].

Green, Matthew (2013): Zerocoin: making Bitcoin anonymous. Retrieved from <https://blog.cryptographyengineering.com/2013/04/11/zerocoin-making-bitcoin-anonymous/>
[Accessed at 10 June 2019].

Gurguc, Zeynep; Knottenbelt, William (2018): Cryptocurrencies: Overcoming Barriers to Trust and Adoption. Retrieved from <https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/ic3re/CRYPTOCURRENCIES--OVERCOMING-BARRIERS-TO-TRUST-AND-ADOPTION.pdf>
[Accessed at 29 June 2019].

Guttmann, Benjamin (2013): The Bitcoin Bible. All you need to know about bitcoins. Norderstedt: Books on Demand.

He, Dong; Habermeier, Karl; Leckow, Ross; Haksar, Vikram; Almeida, Yasmin; Kashima, Mikari; Kyriakos-Saad, Nadim; Oura, Hiroko; Saadi Sedik, Tahsin; Stetsenko, Natalia; Verdugo-Yepes, Concepcion (2016): Virtual Currencies and Beyond: Initial Considerations. Retrieved from <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>
[Accessed at 23 June 2019].

Heun, Volker (2018): Bitcoin & Co. Eine neue Weltwährung. Chancen und Risiken für Investoren. Norderstedt: Books on Demand.

Hicks, John (1967): Critical Essays in Monetary Theory. Oxford: Oxford University Press.

Huberman, Gur; Leshno, Jacob; Moallemi, Ciamac (2017): Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System. Retrieved from <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032375>
[Accessed at 25 June 2019].

Internal Revenue Service (2014): Notice 2014-21. Retrieved from <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>
[Accessed at 4 June 2019].

[Investing.com website] (n.d.): Forex Volatility Calculator. Retrieved from <https://www.investing.com/tools/forex-volatility-calculator>
[Accessed at 23 June 2019].

Irwin, Angela; Milad, George (2016): The use of crypto-currencies in funding violent jihad. Journal of Money Laundering Control. Vol. 19. Retrieved from <https://www.emeraldinsight.com/doi/abs/10.1108/JMLC-01-2016-0003>
[Accessed at 23 June 2019].

Issing, Ottmar (2011): Einführung in die Geldtheorie. München: Franz Vahlen Verlag.

Jarchow, Hans-Joachim (2010): Grundriss der Geldtheorie. Stuttgart: Lucius & Lucius.

Jevons, W. Stanley (1898): Money and the Mechanism of Exchange. Retrieved from <https://archive.org/details/moneymechanism00jevo/page/2>
[Accessed at 1 June 2019].

Kasper, Jochen (2017): Bitcoin as Legal Tender. An Evaluation from an Economic Perspective. Hamburg: Verlag Dr. Kovac.

Kenigsberg, Marc (2013): BTC vs mBTC vs uBTC. Retrieved from <https://bitcoinchaser.com/bitcoin-units-and-denominations>
[Accessed at 27 June 2019].

Kerscher, Daniel (2014): Bitcoin. Funktionsweise, Risiken und Chancen der digitalen Währung. Dingolfing: Kemacon.

Kerscher, Daniel (2018): Handbuch der digitalen Währungen: Bitcoin, Litecoin und 150 weitere Kryptowährungen im Überblick. Dingolfing: Kemacon.

Keynes, John Maynard (1937): The General Theory Of Employment, Interest and Money. Cambridge: Palgrave Macmillan.

Kinderis, Marius; Bezbradica, Marija; Crane, Martin (2018): Bitcoin Currency Fluctuation. Retrieved from <https://www.researchgate.net/publication/324049612_Bitcoin_Currency_Fluctuation>
[Accessed at 23 June 2019].

Krugmann, Paul (2013): Bitcoin Is Evil. Retrieved from <https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/>
[Accessed at 31 May 2019].

Küfner, Robert (2018): Das Kryptojahrzehnt – Was seit dem ersten Bitcoin alles geschehen ist und wie digitales Geld die Welt verändern wird. Kulmbach: Börsenbuch Verlag.

Leys, Lukas (2014): Bitcoin and Cryptographic Finance. Technology, Shortcomings and Alternative Cryptocurrencies. Norderstedt: Books on Demand.

Madore, P. H. (2018): Companies that accept Bitcoin – List updated for 2019. Retrieved from <https://www.ccn.com/companies-that-accept-bitcoin>
[Accessed at 14 June 2019].

Mankiw, Nicholas G. (2011): Makroöknomik: mit vielen Fallstudien. Stuttgart: Schäffer-Poeschel.

Marr, Bernard (2017): A Short History of Bitcoin and Crypto Currency Everyone Should Read. Retrieved from <https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#15627c203f27>
[Accessed at 6 June 2019].

Menger, Karl (1892): On the Origin of Money. Vol.2, No.6, Retrieved from <https://www.jstor.org/stable/2956146?seq=1#page_scan_tab_contents>
[Accessed at 4 June 2019].

[Merriam Webster Dictionary] (n.d.): Tulipomania. Retrieved from <https://www.merriam-webster.com/dictionary/tulipomania>
[Accessed at 5 July 2019].

[Merriam Webster Dictionary] (n.d.): peer-to-peer. Retrieved from <https://www.merriam-webster.com/dictionary/peer-to-peer>
[Accessed at 5 July 2019].

Miller, Michael (2014): The Ultimate Guide to bitcoin. Indianapolis: Pearson Education.

Mishkin, Frederic (2010): The Economics of Money, Banking and Financial Markets. Harlow: Pearson Education.

Moos, Mitchell (2019): Each Transaction Costs the Bitcoin Network $45, Large Improvements Needed to Beat VISA. Retrieved from <https://cryptoslate.com/each-transaction-costs-the-bitcoin-network-45-large-improvements-needed-to-beat-visa/>
[Accessed at 24 June 2019].

Möser, Malte; Böhme, Rainer; Breuker, Dominic (2013): An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. Retrieved from <https://maltemoeser.de/paper/money-laundering.pdf>
[Accessed at 2 June 2019].

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from <https://bitcoin.org/bitcoin.pdf>
[Accessed at 31 May 2019].

Niehans, Jürg (1980): Theorie des Geldes. Synthese der monetären Mikro- und Makroökonomik. Stuttgart: Haupt.

Pagliery, Jose (2014): Bitcoin and the Future of Money. Chicago:Triumph Books.

Pielke, Walther (2018): Besteuerung von Kryptowährungen: ein Überblick über die verschiedenen Steuerarten. Wiesbaden: Springer Fachmedien.

Recksiek, Mirco (2019): Bitcoin Whale Alarm: Bitcoin Wal verschickt 48.000 BTC & „Mini“ Wal sendet 4.000 BTC an Bitfinex – folgt der Dump?. Retrieved from <https://cryptomonday.de/bitcoin-whale-alarm-bitcoin-wal-verschickt-48-000-btc-mini-wal-sendet-4-000-btc-an-bitfinex-folgt-der-dump/>
[Accessed at 30 June 2019].

Rhodes, Delton (2018): A Complete History of Bitcoin (2008 - 2019 Timeline). Retrieved from <https://blockexplorer.com/news/bitcoin-history-timeline/>
[Accessed at 3 June 2019].

Rizzo, Pete (2014): UK Eliminates Tax on Bitcoin Trading, Publishes Official Guidance. Retrieved from <https://www.coindesk.com/top-uk-tax-agency-eliminate-20-levy-bitcoin-trading>
[Accessed at 5 June 2019].

Rowley, Jason (2017): How Ethereum became the platform of choice for ICO'd digital assets. Retrieved from <https://techcrunch.com/2017/06/08/how-ethereum-became-the-platform-of-choice-for-icod-digital-assets/>
[Accessed at 27 June 2019].

Russo, Camilla (2018): Bitcoin Speculators, not Drug Dealers, dominate Crypto use now. Retrieved from <https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now>
[Accessed at 31 May 2019].

Sardoni, Claudio (2015): The functions of money and the demand for liquidity. Retrieved from <http://www.diss.uniroma1.it/sites/default/files/allegati/Sardoni_wp DISSE_3_15.pdf>
[Accessed at 6 June 2019].

Schredder, Tim (2018): Das neue Geld – Bitcoin, Kryptowährungen und Blockchain verständlich erklärt. Munich: Piper Verlag.

Segendorf, Björn (2014): What is Bitcoin?. Sveriges Riskbank Economic Review. Retrieved from <http://archive.riksbank.se/Documents/Rapporter/POV/2014/2014_2/rap_pov_artikel_4_1400918_eng.pdf>
[Accessed at 3 June 2019].

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

Sorge, Christoph; Krohn-Grimberghe, Artus (2012): Bitcoin: Eine erste Einordnung. Retrieved from <https://link.springer.com/article/10.1007/s11623-012-0164-9>
[Accessed at 17 June 2019].

Statista (2019): Size of the Bitcoin blockchain from 2010 to 2019, by quarter (in megabytes). Retrieved from <https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>
[Accessed at 2 June 2019].

Strauss, Ilana (2016): The Myth of the Barter Economy. Retrieved from <https://www.theatlantic.com/business/archive/2016/02/barter-society-myth/471051/>
[Accessed at 24 June 2019].

Thum, Marcel (2018): The Economic Cost of Bitcoin Mining. Retrieved from <https://www.cesifo-group.de/DocDL/CESifo-Forum-2018-1-thum-bitcoin-march.pdf>
[Accessed at 17 June 2019].

[Tradeblock.com website] (2015): Analysis of Bitcoin Transaction Size Trends. Retrieved from <https://tradeblock.com/blog/analysis-of-bitcoin-transaction-size-trends> [Accessed at 24 June 2019].

Vandezande, Niels (2017): Virtual Currencies: A Legal Framework. Vol. 1. KU Leuven Centre for IT & IP Law Series. Cambridge: Intersentia.

Vejačka, Martin (2014): Basic Aspects of Cryptocurrencies. Retrieved from <https://www.researchgate.net/publication/292586903_Basic_Aspects_of_Cryptocurrencies> [Accessed at 5 July 2019].

Ver, Roger; Kanemoto, Kaneto; Matsuda, Gen (2018): Reversal of Fortune – Changing the World with ICO Crypto Currency Services. Tokyo: Sougeisha.

Villasenor, John; Monk, Cody (2011): Shadowy Figures: Tracking Illicit Financial Transactions in the murky World of Digital Currencies, Peer-to-Peer Network and Mobile Device Payments. Retrieved from <https://www.brookings.edu/research/shadowy-figures-tracking-illicit-financial-transactions-in-the-murky-world-of-digital-currencies-peer-to-peer-networks-and-mobile-device-payments/> [Accessed at 15 June 2019].

[VISA USA website] (n.d.): Small Business Retail. Retrieved from <https://usa.visa.com/run-your-business/small-business-tools/retail.html> [Accessed at 1 June 2019].

Walton, Aiden; Johnston, Kevin (2018): Exploring Perceptions Of Bitcoin Adoption: The South African Virtual Community Perspective. Retrieved from <http://www.ijikm.org/Volume13/IJIKMv13p165-182Walton4724.pdf> [Accessed at 1 July 2019].

Weber, Beat (2013): Ordoliberale Geldreform als Antwort auf die Krise? Bitcoin und Vollgeld im Vergleich. Retrieved from <https://www.researchgate.net/publication/262198512_Ordoliberale_Geldreform_als_Antwort_auf_die_Krise_Bitcoin_und_Vollgeld_im_Vergleich_Responding_to_the_crisis_by_ordoliberal_monetary_reform_Comparing_Bitcoin_and_the_positive_money_proposal> [Accessed at 29 June 2019].

Wu, William (2017): Why Bitcoin Is Not a Viable Currency Option. Retrieved from <https://kw.wharton.upenn.edu/kwfellows/files/2018/06/2018-08-30-Bitcoin-Student-Series.pdf> [Accessed 26 June 2019].

Yermack, David (2013): Is Bitcoin a real currency? An economic appraisal. National Bureau of Economic Research. Retrieved from <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2361599>
[Accessed at 28 June 2019].

Young, Joseph (2015): McAfee: Bitcoin is “too complex” for the average individual. Retrieved from <https://www.newsbtc.com/2016/01/02/mcafee-bitcoin-is-too-complex-for-the-average-individual/>
[Accessed at 11 June 2019].

Declaration of Originality

I hereby declare that this Bachelor Thesis and the work reported herein was composed by and originated entirely from me. Information derived from published and unpublished work of others has been acknowledged in the text and references are given in the list of references. I declare my consent that a written copy of my Bachelor Thesis will be added to the library of the department of business; rights of any third party will thereby not be violated.

Hamburg, 15 July 2019 .