Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Bachelor Thesis

Bitcoin. Money of the future or instrument for criminal activities?

Submission Date

May 10, 2019

Supervised by

Prof. Dr. Martina Metzger and Prof. Dr. Jennifer Pédussel Wu

Submitted by:

Harry Wiesner
Karlsbader Str. 12a
14193 Berlin
Tel: 01773422455
Matriculation number: 481483

Abstract

The Bitcoin phenomenon has attracted worldwide attention in the last decade. Some consider the new cryptocurrency to be the money of the future, while others see it as a promising new investment category. However, attention has recently been drawn to the serious risks arising from virtual currencies, especially with respect to financial integrity. Virtual currencies seem to be a powerful new tool for money laundering, terrorist financing, trading of illegal goods and services, and fraud. This has also been recognised by legislative institutions, which are working on regulatory approaches to control these risks in the future.

The central subject of this thesis is divided into two main parts. First, Bitcoin's potential as money is examined with the help of money theory and a comprehensive investigation of Bitcoin technology and development. Second, the focus shifts to the risks associated with virtual currencies. The aforementioned criminal activities are studied, and the use of virtual currencies as instruments for these purposes analysed. Furthermore, this thesis focuses on the difficulties regulators face, on recommendations of different regulatory approaches, and on the question of whether or not successful regulation is generally possible.

In order to cover this topic comprehensively, a quality review of literature from acknowledged experts and institutions is conducted. It is hoped that this thesis will provide detailed information about Bitcoin, its potential as money, the resulting risks, and how to manage these in order to secure the future financial integrity of global markets.

Tabel of Contens

List of Figures

List of Tables

List of Abbreviations

AMLD ..... *Anti-Money Laundering Directive*
CFTC ..... *US Commodity Futures Trading Commission*
CIA ..... *Central Intelligence Agency*
CPU ..... *Central Processing Unit*
FATF ..... *Financial Action Task Force*
FinCEN ..... *Financial Crimes Enforcement Network*
GDP ..... *Gross Domestic Product*
KWG ..... *German Banking Act*
RUSI ..... *Royal United Service Institute for Defence and Security Studies*
SEC ..... *US Securities and Exchange Commission*
UNODC ..... *United Nations Office on Drugs and Crime*
USD ..... *United States Dollar*

1 Introduction

The cryptocurrency concept originated in 1998 in the cypherpunk community. Technically versed members wanted to create a new type of money that would stand out from the conventional monetary system and avoid any financial intermediaries. In 2008, Satoshi Nakamoto provided the technical basis and created Bitcoin, which is basically a computer program based on cryptography. It allows users to save, send, and receive units called bitcoins. These units were soon able to be traded for fiat currency and exchanged for goods and services (bitcoin.org, n.d. (a)). Almost 10 years later, in December 2017, Bitcoin hit its record high with a value of $19,783.21 per unit and thus reached the peak of worldwide attention (blockchain.com, 2019). The first cryptocurrency, which today is the best known representative of the virtual currency era, is often discussed as the wave of the future for payment systems (FATF, 2014, p. 3), or even as the future of money (La Monica, 2018).

In addition to technical innovation and great potential for monetary transactions, serious risks for financial integrity have emerged from this new payment system. It is proving to be a powerful new tool for criminals, terrorist financiers, and other sanctions evaders to move and store illicit funds out of the reach of law enforcement and other authorities (FATF, 2014, p. 3). As Bitcoin continues to establish itself, risks and possible responses from jurisdictions are a highly relevant issue at the moment, and institutions around the world are working on regulatory concepts to address the dangers of virtual currencies or, more precisely, cryptocurrencies.

The goal of this thesis is therefore to examine Bitcoin's role under the heading 'Money of the future or instrument for criminal activities?' This thesis discusses Bitcoin in terms of the theory of money, investigates the related risks for financial integrity, and examines possible regulatory approaches to successfully controlling such risks. In order to provide comprehensive insight into the topic, the following key questions should be answered: What is Bitcoin and how can it be classified in monetary theory? What risks are emerging from Bitcoin and other cryptocurrencies? What is the status of regulation, and how can related dangers be controlled in the future?

First of all, to classify Bitcoin, Chapter 2 deals with the money theory and explains what money actually is, what functions and qualities money has, and in what forms it occurs. This is followed by a detailed analysis of Bitcoin, its technical functionality, and its uses in Chapter 3. This background is important for the analysis of risks to financial integrity and the specific difficulties of its regulation. Furthermore, it provides insight into why Bitcoin use is increasing so rapidly. Chapter 4 evaluates Bitcoin in terms of the money theory and answers the question of whether or not Bitcoin can be considered money. Chapter 5 contains a comprehensive risk analysis of cryptocurrencies in terms of financial integrity. For the risk analysis, the dangerous aspects of cryptocurrencies in general are considered and do not refer solely to Bitcoin. The main criminal areas inspected are money laundering, terrorist financing, cybercrimes, and fraud. This is followed by an overview of regulatory approaches. Chapter 6 explains the specific challenges regulators face when dealing with cryptocurrencies. Furthermore, recommendations from specialised institutions are examined and compared with the actual regulation systems of various jurisdictions, including an evaluation of their expected success. Finally, the main findings of the thesis are listed and evaluated in the conclusion to provide a final overview of the situation around Bitcoin and cryptocurrencies.

The thesis is based on a systematic review of the literature on money theory and virtual currencies, especially Bitcoin, as well as publications of institutions studying the risks of and working on regulatory approaches for virtual currencies. First, several library catalogues were searched for academic books and peer-reviewed journals providing information about money theory and virtual currencies. The range of keywords included money theory, Bitcoin, virtual currencies, cryptocurrencies, risks, and virtual currency laws. Second, subject-specific professional websites such as Bitcoin's official website and websites of renowned institutions related to the key topics of this thesis were searched for publications providing the current scientific status of research on virtual currencies, their risks, and regulation possibilities. Research papers on the aforementioned topics were also searched independently. Third, the reference sections of these publications were searched in order to find additional related articles.

2 The theory of money

Money is currently a circulating medium. The process of trading goods and services has greatly improved through the possibility of an intermediate step within the exchange. Money allows purchase and sale to be separated in time (Rosenberger, 2018, p. 6). It appears in the form of currency printed by central banks or deposits at commercial banks (McLeay, et al., 2014, p. 4). To answer the question of how money is defined, this chapter briefly examines the theory of money and explains the functions and basic qualities of money.

2.1 Functions of money

While goods and services could only be exchanged for other goods and services in what are called ‘natural economies’, trading is significantly improved in ‘monetised economies’. Goods and services can be exchanged for money, and vice versa (Anderegg, 2007, p. 19 f.). Although most people in the world use money on a daily basis, there is no agreement on what money is. One way to define money as such is through examining its essential functions. It must function as medium of exchange, a unit of account, and a store of value (McLeay, et al., 2014, p. 5).

Medium of exchange

A medium of exchange is absolutely necessary in a modern economy, because individuals specialise in a certain field and are therefore not usually able to produce all the goods and services that are required to live self-sufficiently. Specialising is only possible if other goods and services are available through bartering. Money simplifies the process of commodity exchange. Instead of finding another individual who exactly matches the supply and demand of commodities, every individual can now trade his/her goods for units of money and swap the money later for the goods required. Therefore, only one consensus must take place for a trade to occur. To make this improvement possible, a good that functions as money must to be accepted collectively within the economy. (Berentsen & Schär, 2017, p. 12 f.) Money is then something people hold to buy goods and services. Money itself requires no intrinsic value. The process of exchange from natural economies is basically still existent, just in a modernised way (McLeay, et al., 2014, p. 5).

Unit of account

Money also needs to be a unit of account, meaning that all goods and services can be priced in terms of money and compared to each other (ibid.). This reduces the information that is required to understand the overview of exchange rates in a natural economy. In this case, the exchange ratio is shown as $\frac{n(n-1)}{2}$, where n is the amount of goods. For an example of 1,000 goods (n=1000), are 499.500 exchange ratios or 'prices' existent. Money reduces this information to one price per good (Anderegg, 2007, p. 20). Another part of the unit of account function is money being the standard for deferred payments, meaning that it is the unit in which debts and payments are stated in long-term contracts (Rabin, 2004, p. 24).

Store of value

The possibility of storing value and saving money allows individuals to postpone any purchases. This smoothes individuals' consumption and makes it easier for them to secure themselves against unexpected costs. Saving money also makes larger investments possible that previously could not have been carried out by single individuals. A collectively accepted medium of exchange is always working as a store of value. On the other hand, there are a lot of potential ways to store value with non-liquid mediums of exchange. To function as a store of value, money needs to be stable in price to guarantee that it is not losing any value while being stored (Berentsen & Schär, 2017, p. 15 f.).

2.2 Qualities of money

To fulfil the functions listed in Section 2.1, money ideally needs to have certain qualities. Jevons (1876, p. 31 f.) has stated that utility and value, portability, indestructability, homogeneity, divisibility, stability of value, and cognisability are the essential qualities of money material. Today, the research literature agrees that utility and value besides its function as money is not necessary for the money material, because modern currencies do not require any intrinsic value. Cognisability is adjusted to verifiability. One important quality to add is limitation of availability (Berentsen & Schär, 2017, p. 16). The qualities of money are explained below.

Indestructability

Indestructability was already important in natural economies: since traded goods functioned as stores of value, any deteriorating objects could not be used. One of the first commodity monies that was established nationwide was the snail shell of the cowry. Cowry shells are comprised of a heavy material and are therefore almost indestructible. Cowry shells are considered one of the most successful means of payment in history (Rosenberger, 2018, p. 6).

Portability

Portability also enables transferability. Money must be easy to carry and exchange with no or relatively low transaction costs. Only if portability and transferability are present can money function as a store of value and medium of exchange (Berentsen & Schär, 2017, p. 16).

Homogeneity

Money needs to be homogeneous, meaning that any unit must contain the same value as other units of the same size and weight. If the material differs in mass or appearance, a certain process of recognition is necessary to determine the exact value. This process includes transaction costs. The material therefore cannot be used as a medium of exchange (Sykes, 1911, p. 7).

Divisibility

The requirement of divisibility is connected to that of homogeneity. Ideally, the material of which money is comprised must not lose any value when divided. Materials like skin or fur, for example, lose value when divided, and it is impossible to reunite the pieces after they are cut in half. Metals, on the other hand, can be melted again without a significant loss of value (Jevons, 1876, p. 38). Another solution for divisibility is that the material is available in such small pieces that dividing it further is not necessary for any exchange (Berentsen & Schär, 2017, p. 16).

Cognisability/verifiability

The medium of exchange must be of some substance that can be easily identified without expert knowledge, as mentioned in terms of homogeneity. The material must also be immune to forgery (Sykes, 1911, p. 7), which is difficult to ensure today. For instance, the

European Central Bank recently declared that it is no longer printing the €500 bill because it is susceptible to criminal activities and the most targeted unit of forgery (Europäische Zentralbank, 2016).

Limitation

Limited availability makes the use of money as a medium of exchange possible. There is no reason to trade a material that is available in unlimited amounts (Berentsen & Schär, 2017, p. 17).

2.3 Types of money

Different types of money have different monetary values. Berentsen and Schär (2007, p.17 f.) have determined that the monetary value of each type is based on different combinations of intrinsic value, promised payments, liquidity, and speculation premia.

The first type of money, commodity money, was previously mentioned in terms of natural economies and originated in the sixth millennium before Christ. It consisted of useful items such as shells, arrowheads, pearls, and animal skins. People were willing to take these items for barter without actually needing the items themselves (Rosenberger, 2018, p. 6). The monetary value of commodity money is characterised by high intrinsic value and holds an even higher value if a liquidity or speculation premia is added in case of an omnipresent trade component (Berentsen & Schär, 2017, p. 19).

Another type of money is credit money. Credit money is basically a promise to pay a person or institution at some point in the future, also known as an 'I owe you' (IOU). Modern currencies including bills, coins, and scriptural money belong to this category. Credit money has no intrinsic value; the promised payment linked to the credit money makes it valuable, and an added liquidity and speculation premia is also possible (ibid. 19 f.). Credit money is exposed to a certain risk of failure; therefore, the credibility of the promise is a component of the value. Modern currencies solve this problem since the IOU is widely trusted as a result of guarantees by central banks, governments, and jurisdictions (McLeay, et al., 2014, p. 7). The other component of credit money is scriptural money. Scriptural money is a non-haptic, written amount of money. It was introduced in the 14th

century when banks established the possibility of making deposits into bank accounts. Interest was developed for these accounts to make deposits more valuable for individuals, since increasing deposits enables banks to work with more money (Rosenberger, 2018, p. 8). Scriptural money arises either through deposits or through the lending of commercial banks. The overall amount of scriptural money is only limited by a minimum reserve requirement, which is a central bank regulation for commercial banks. It implies that commercial banks need to hold a certain percentage of their lendings as reserves. Every functional currency that is not guaranteed to be exchanged to either another currency or certain goods on a fixed exchange rate is called fiat money. The acceptance of fiat money is based on legal regulations and general trust in central banks, governments, and jurisdictions (Sixt, 2017, p. 52). Fiat money has neither intrinsic value nor a promised payment linked to it. The liquidity and speculation premia are the only value components. Since future expectations determine the value, fiat money can be completely worthless if it loses its monetary function (Berentsen & Schär, 2017, p. 21).

In the 20th century, digitisation ultimately led to electronic money. Transactions that were previously handwritten became almost completely electronic. Credit and debit cards issued by financial institutions are an essential part of today's economy. With the internet prevailing, e-payments and online banking became common. Electronic money, along with widespread internet usage, prepared the ground for cryptocurrencies (Rosenberger, 2018, p. 8 f.).

3 Cryptocurrency and Bitcoin

> *Virtual Currencies are a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a Fiat Currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically. The main actors are users, exchanges, trade platforms, inventors, and e-wallet providers.* (European Banking Authority, 2014, p. 5)

To classify cryptocurrencies and Bitcoin, a clear distinction between electronic money and cryptocurrencies is indispensable. Electronic money represents fiat money, which is guaranteed by jurisdictions and the government. Cryptocurrencies, on the other hand, are a

digital representation of value. This value is only based on the agreement within the community of its users (FATF, 2014, p. 4). Most characteristics for cryptocurrencies are that monetary control is no longer the responsibility of the central bank. Instead, computing processes and algorithms are responsible. Thus, no trust in an intermediary confidant (banks, etc.) is required to confirm transactions (Meisner, 2018, p. 92).

This chapter provides comprehensive insight into Bitcoin since it is a pioneer in the field of virtual currencies and is still the leading cryptocurrency to date. To understand Bitcoin and cryptocurrencies in general, Bitcoin's history and the motives behind it, as well as its technical background and different aspects of its usage, are discussed.

3.1 The history of Bitcoin

The idea of cryptocurrencies originated in cypherpunk communities in the early 1990s. Cypherpunks can be described as groups of data security activists that represent the idea of securing privacy in the upcoming digital age. Cypherpunks have also worked on alternative currency systems to limit the power of central financial institutions (Sixt, 2017, p. 6). The idea was to create new type of money isolated from the existing conventional monetary system (bitcoin.org, n.d. (a)). This idea was realised when Satoshi Nakamoto, a mysterious and anonymous cypherpunk, published his paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' in November 2008 via a personal email distributor (Nakamoto, 2008, p. 1). In this paper, Nakamoto describes his philosophy and provides a detailed technical solution for a decentralised electronic payment system. Since payment systems are completely based on trust in financial institutions as intermediaries, trasactions are susceptible to several weaknesses. Intermediaries are not free and increase the costs of transactions; therefore, the smallest transactions are not worth being realised. Nakamoto emphasises the problem of the possibility of reversing transactions, because without this option, less trust would be required. Overall, a certain percentage of fraud is generally accepted and viewed as unavoidable. Furthermore, the paper states that transaction costs and payment uncertainties could be avoided if a physical currency is used, presuming that there is a general trust in the currency. As soon as payments are made through a communication channel, there are no mechanisms to avoid parties of trust (Nakamoto, 2008, p. 1).

Soon after the dissemination of Nakamoto's paper, the platform for bitcoin transactions was created when the first open-source Bitcoin client was launched. Nakamoto himself created the first data block of bitcoins through mining (which is explained further in Section 3.2); this block is referred to as a 'genesis block'. The first transaction occurred between Nakamoto and Hal Finney, an early supporter of Bitcoin, and involved 10 bitcoins (Chohan, 2017, p. 3). The first known real purchase made indirectly with bitcoin was made through a post on a Bitcoin forum in 2010. The famous purchase was of two large pizzas for 10,000 bitcoins, making it the most expensive pizza order in history for about $40 million measured in today's bitcoin value (as of February 2019) (Laszlo, 2010). In 2010, bitcoins were traded on an exchange for the first time. The market price was $0.06 per bitcoin. Since then, the price of bitcoins has fluctuated massively (Sixt, 2017, p. 2).

It did not take long for the dark side of Bitcoin to emerge. The global black market cyber bazaar Silk Road went online and quickly became the largest online shop for drugs and several other unlawful products and services (FATF, 2014, p. 11). Silk Road enabled every individuum to by and sell, every kind of good, anonymously. The page itself was only accessible through a special internet browser, the 'Tor-Browser', which guarantees complete anonymity. The only payment method that was accepted on Silk Road was bitcoin. The Tor-Browser combined with Bitcoin made it almost impossible for state authorities to intervene. Transactions were completely anonymously and hidden (Rosenberger, 2018, p. 37). Silk Road generated sales of approximately $1.2 billion until the webpage was finally seized in September 2013, and with it approximately 173,991 bitcoins. An individuum who was held responsible for running the site was arrested and charged with drug trafficking, money laundering, and formation of a criminal organisation. Since Silk Road's payment system was completely based on bitcoin, this has greatly damaged Bitcoin's reputation (FATF, 2014, p. 11).

In 2010, Mt. Gox was founded and became the largest Bitcoin exchange for the following years. For the first time the new currency became more present and accessible in the non-digital world. Bitcoin was growing rapidly and people wanted an easy, trustworthy platform for buying and selling bitcoins. Between April and June 2010, over 60,000 accounts were registered on Mt. Gox. In mid-2011, the turn occurred when customers realised that bitcoins disappeared from their accounts. Several customers reported this problem to forums and realised that hackers had stolen huge amounts of bitcoins. Some of

the stolen bitcoins were traded suddenly on Mt. Gox for $0.01 per unit, resulting in a dramatic fall of the bitcoin market price. The owner of Mt. Gox, Mark Karpelès, tried several times to stabilise the exchange without success. In 2014 the disaster came to a climax when Karpelès admitted that more than 850,000 bitcoins were lost, more than 750,000 of which were from customer accounts. In 2017, Karpelès was convicted of fraud, manipulation, and embezzlement. It is believed that 643,000 bitcoins were withheld by Karpelès, 7,000 were actually stolen by hackers, and 100,000 reappeared on customer accounts. Overall, Bitcoin's reputation suffered massively because of these affairs, and bitcoin market prices fell drastically (Rosenberger, 2018, p. 42 ff.).

Repeating high rising notoriety of promising chances as profitable investment resulted in several comebacks of value; however, hacker attacks, negative headlines, and political statements against Bitcoin repeatedly led to drastic decreases in the history of bitcoin's value (Sixt 2017, 2 f.). Figure 1 shows the average United States Dollar (USD) market price across major bitcoin exchanges beginning in 2010 until the present, also demonstrating the massive increase in value in 2017 followed by a continuing decrease. Bitcoin reached an all-time high of almost $20,000 in December 2017, and is currently at about $4,000 per unit (as of February 2019).

Figure 1: Market price in USD for one bitcoin unit
Source: (blockchain.com, 2019)

3.2 Bitcoin technology

The Bitcoin programme is based on a peer-to-peer network that connects all Bitcoin users in a decentralised manner and enables communication as well as transactions between users. The revolutionary aspect in peer-to-peer networks is the equal status of all participants. Figure 2 illustrates the difference between a conventional server-based network with one server as the intermediary and decentralised peer-to-peer networks (Berentsen & Schär, 2017, p. 95).

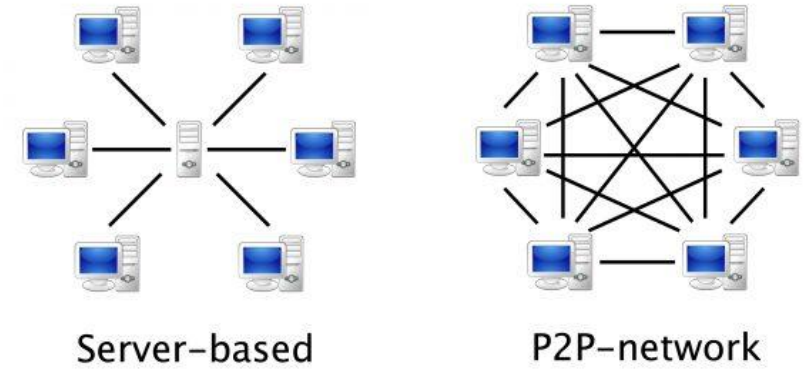

Figure 2: Server-based networks and peer-to-peer networks
Source: (insurelab, 2017)

Nakamoto (2008, p. 1) has stated that one of the main problems when it comes to online transactions is the double spending problem. Bitcoin units are defined as chains of digital signatures. These units can be transferred within users by digitally signing a hash of all previous transactions combined with a public key (address) of the payee and extending the chain with this information. These are the contents of every single bitcoin. The next owner then verifies the chain of digital signatures and the chain of previous ownerships. However, the payee cannot verify whether or not the previous owner copied the coin and also paid it to a third user (Nakamoto, 2008, p. 1 f.). This double spending can be prevented in a server-based network since the intermediary would notice doubled coins and stop the transaction. If an intermediary were introduced, however, transaction costs would reappear, and the ideology of Bitcoin would have failed.

Nakamoto's paper suggests solving the double spending problem via a timestamp server. The timestamp server adds the information of time to a hash when a transaction is made. It proves that the data existed when the transaction was made, and it includes all of the

previous time information, forming a chain and adding the time information to previous information of any transaction before. The timestamp server also publishes the hash to all other participants of the peer-to-peer network for ever user to verify (Nakamoto, 2008, p. 2). In addition to the timestamp server, a proof-of-work is added to prevent the risk of attacking a chain by someone who allocates many IP addresses, using the majority needed in decision-making, for the system to decide which chain is reliable. Proof-of-work is a one central processing unit (CPU), one vote system. It takes the transaction information including the timestamp information and summarises this information into a block, then increments a nonce with a certain amount of zero bits. When a block is hashed, a certain amount of CPU effort is necessary to find the right amount of bits by trial and error. When the right number sequence is found, the block is extended and cannot be changed by any CPU without redoing the work. Every transaction adding another block results in more and more CPU effort for redoing all previous blocks. The system considers the longest chain of blocks to be the real one since it is outpacing every other chain, which might be build by attackers. Since the real chain is continuously growing, it is almost impossible for hackers to attack the Bitcoin transaction system in a peer-to-peer network (ibid., p. 3). The only possibility for attacking the system would be to have more than half of the participating CPUs working on a 'fake' chain to outpace the original chain. If the continuously growing peer-to-peer network starts with real CPUs, attacks by hackers are nearly impossible. This revolutionary system is known as block chain.

To further secure the system and ensure synchronisation, it is possible for participants to provide their CPU computing power to the system to generate new blocks. In doing so, the participant is rewarded with a small amount of bitcoins. This process is called 'mining'. Since miners are spread all over the world, no individual can gain control over the network. (bitcoin.org, n.d. (b)) Mining creates new bitcoins through rewards; however, the amount issued as a reward decreases with the increase of participating miners. The Bitcoin algorithm is designed for a maximum of 21 million bitcoins. The number of bitcoins increases steadily through mining, and the total amount is expected to be accomplished around the year 2130. (bitcoin.org, n.d. (b)). Since more and more participants have provided their CPU computing power to benefit from rising bitcoin prices, it has become much more difficult to create new blocks. Today, specialised hardware is required to compete against other miners. The amount of energy used to keep the Bitcoin network running is often seen as very controversial. The study 'Bitcoin's Growing Energy Problem'

published by ScienceDirect in May 2018 indicates that '[t]he Bitcoin network is consuming an estimated of 2.55 gigawatts of electricity at the moment, and potentially 7.67 gigawatts in the future, making it comparable with countries such as Ireland (3.1 gigawatts) and Austria (8.2 gigawatts)' (de Vries, 2018). Bitcoin.org argues that energy that is used for mining can be transferred into heat, and miners who can use this heat profitably are not wasting any energy and are therefore perfectly efficient (bitcoin.org, n.d. (b)). However, this ideal scenario is a rare exception, leading to the question of whether or not Bitcoin can be environmentally sustainable in the future.

Regardless of whether or not Bitcoin's philosophy of a future currency occurs, block chain technology has already been adopted by several other projects. So-called 'smart contracts' show great potential. Smart contracts are digitised contracts in a block chain network that execute certain orders when terms are fulfilled, such as salary payments or time-displaced bank transactions. Conditions set in the block chain are verified constantly until the conditions are confirmed. Miners are rewarded the same way as with Bitcoin. One successful example of the usage of smart contracts is Digix, a service that simplifies gold trading. Digix runs a physical bank vault in Singapore, and for each gram of physical gold, Digix creates a token in the so-called Ethereum block chain. These tokens can be traded against bitcoins, for example, without any physical exchange of gold. Since Digix cooperates with several exchanges for cryptocurrencies, tokens can also be exchanged against fiat currencies (Seitz, 2017, p. 58).

The complete Bitcoin code is aligned as an open source project, meaning that everyone can use the program or alter the code for other projects. This has led to over 400 similar projects and other applications (Sixt, 2017, p. 34). Some of the largest cryptocurrencies following Bitcoin include Ethereum, Ripple, and Litecoin (Hileman & Rauchs, 2017, p. 15).

3.3 Usage of Bitcoin

There are different ways for individuals to use Bitcoin. The first implemented access to the usage of Bitcoin is the Bitcoin Core client, which was published by Nakamoto himself. It is a free software with a MIT license available for Windows, Mac, Linux, and Ubuntu. The Core client provides all the features required to store, send, or receive transactions;

however, fast internet access and huge amounts of free disc space are needed for its installation (as of this writing, about 200 gigabytes) (bitcoin.org, 2018). The software downloads and saves the whole block chain. Every time the client operates, it adds the new blocks and keeps the block chain updated (if the client can operate fast enough, it also mines when used). Although it takes a lot of effort to run the Core client, it is still the most secure way to use Bitcoin (Sixt, 2017, p. 35).

Another way to use the Bitcoin network is through light clients, which basically provide the same features as the Core client but operate through the Simplified Payment Verification system. Light clients do not download and process the whole block chain but rather only the block header, which is the information about previous hash values that are connected to one's own transaction. This results in a much easier use of Bitcoin with significantly less time consumption. Compared to the fully anonymous Core client, light clients' origins are much easier to comprehend since they are connected to the Core client for validation (ibid., p. 36).

So-called 'mobile wallets' are most qualified for the everyday use of Bitcoin. Mobile wallets are applications for mobile phones that manage bitcoins directly in the software. Prepayments of bitcoins must be made into the wallet. This enables the user to send and receive transactions with the lowest effort possible. Scanning a quick response code (a square of black and white dots) is enough to recognise another wallet and confirm a transaction. The mobile wallet is only accessible through the mobile phone that is running the wallet; if the mobile phone is lost, there is no way to restore the bitcoins held in the wallet (Rosenberger, 2018, p. 23).

The last and very common way to use Bitcoin is through online exchanges. These exchange services offer all the features that are necessary to use Bitcoin in terms of storage, transactions, and, in most cases, trading in various categories like order-book exchanges and brokerage services (Hileman & Rauchs, 2017, p. 27). Web wallets can be accessed through every regular web browser, and interfaces are easily arranged and can be used without technical expertise (Sixt, 2017, p. 36 f.).

The 'Global Cryptocurrency Benchmarking Study' by Hileman and Rauchs (2017) investigates key cryptocurrency industry sectors and analyses the usage of Bitcoin. It

gathered data from nearly 150 cryptocurrency companies and individuals in 38 countries from five world regions. Estimating how many individuals are using cryptocurrencies is difficult even if reliable data about wallets is available. Users can either use multiple wallets from several providers at the same time or centralised wallets that pool several wallets or addresses (Hileman & Rauchs, 2017, p. 8). The aforementioned study only considers active users and excludes inactive wallets holding bitcoins without transactions. The results are provided in Figure 3.

Figure 3: Estimated active users of cryptocurrency wallets
Source: (Hileman & Rauchs, 2017, p. 25)

Figure 3 shows that the number of active users of cryptocurrencies has increased significantly since 2013. In 2017, there was an estimate of between 2.9 million and 5.8 million unique active users. Considering the excluded inactive wallets as well as usage through payment service providers or other platforms, the actual number of users could be higher than the estimate (ibid., p. 25). To calculate the share of users utilising Bitcoin, the market capitalisation of Bitcoin must be considered. Bitcoin is without doubt the most dominant cryptocurrency with a market capitalisation share of approximately 70% in 2017 (ibid., p. 16). This led to an estimated number of 2.1 to 4.2 million active Bitcoin users in 2017.

Bitcoins market capitalisation is currently at approximately $70 billion but is continuously decreasing in keeping with the falling price per unit (see Figure 1, as of March 2019) (CoinMarketCap, 2019).

3.4 Reasons for the increasing usage of Bitcoin

Apparently, the fascination with and usage of cryptocurrencies is continuously rising. Some of the main reasons might include the transparent coin creation process and the decentralised and distributed structure that was mentioned in terms of block chain technology. Bitcoin is only controlled by the users themselves and by algorithms written in the code. A lot of users are following the original philosophy of cypherpunks or are critical of national governments, commercial banks, or monetary authorities. This can be described as the 'political side' of cryptocurrencies. People are investing in cryptocurrencies to support alternative transaction technologies, to rebel against the monetary system, or to avoid strict capital controls of certain countries such as China. These aspects are further encouraged by the pseudonymity that Bitcoin provides. Transactions are made without the exchange of personal information and addresses and wallets are not necessarily tied to the identities of their users (Kiel Institute for the World Economy, 2018, p. 10 f.).

Another reason for the increase of Bitcoin usage is the unlimited possibilities of transactions with very low operational costs. Every Bitcoin user can send and receive money to other users anywhere in the world. Transactions cannot be controlled or prevented and coins cannot be faked, copied, or spent twice (Bunjaku, et al., 2017, p. 37). Considering these benefits combined with the fact that transaction fees only amount to approximately 0.1% of the transactions, it is very tempting to use Bitcoin instead of regular bank transactions. Especially when used as a medium for global money transfers, Bitcoin has a significant cost advantage over traditional currencies (Kiel Institute for the World Economy, 2018, p. 10) Since no financial intermediary is needed to confirm transactions, it takes only minutes until the Bitcoin network will process payments and create a new block in the block chain. Finally, using personal data for fraud, as is possible with credit card transactions, is not possible with Bitcoin (Bunjaku, et al., 2017, p. 37 f.)

In addition to ideological, practical, or economic reasons, Bitcoin could be a great opportunity for people in the developing world in the future. The Global Findex Database

states that more than 1.7 billion adults do not have a bank account at a financial institution or access through a mobile money provider. Not earning enough money to cover bank fees, unemployment, or simply the lack of a bank in the community are a few of the reasons for this lack (Demirguc-Kunt, et al., 2018, p. 4 f.). However, the expansion of information and telecommunication infrastructure is occurring rapidly in these developing countries (Sixt, 2017, p. 80). This means that people without bank accounts could be included in world trade through Bitcoin. The trend suggests that access to the internet will be less of a barrier. These circumstances could massively boost the usage of Bitcoin or other cryptocurrencies, and with it the prosperity of developing countries (ibid., p. 83).

4 Is bitcoin money?

Every now and then there is a discussion in the media or in scientific circles about whether or not cryptocurrencies might become the new money, or a currency of the future. Opinions are currently varied. While Bitcoin is often referred to as a 'typical speculation bubble' (Wendt, 2018) and the future of bitcoin as a real currency is denied (Kirsch, 2018), other opinions see potential in bitcoin being the future money (La Monica, 2018).

To discuss whether bitcoin and cryptocurrencies in general are money the following chapter examines bitcoin in terms of the functions of money described in Section 2.1 and in terms of the qualities of money listed in Section 2.2. Furthermore, bitcoin is compared to existing legal currencies. To facilitate a solid conclusion, the legal point of view is also considered.

4.1 Bitcoin and the functions of money

Medium of exchange

The general acceptance and usage of bitcoin is increasing. The main difference from legal currencies, however, is that bitcoin lacks legal tender status. There is no jurisdiction determining that bitcoin must be accepted to clear debts (Berentsen & Schär, 2017, p. 244). This implies that a payment can only take place when both parties agree to use bitcoin. As mentioned in Section 2.1, money must be accepted collectively within the economy to function as such. Comparing the number of only 5.8 million active Bitcoin users

worldwide in 2017 (Figure 3), the estimated 1.5 billion credit card users in the US alone (Resendiz, 2018) illustrates that Bitcoin is a long way from being a largely accepted or dominant medium of exchange.

Store of value

Since bitcoin is not a liability of a state or a private entity, the price per unit fluctuates greatly within short timeframes (see Figure 1). The price of bitcoin depends only on aggregate demand. In terms of legal currencies, central banks are adjusting the money supply in response to changes of aggregate demand in order to stabilise the price level. These mechanisms are absent for bitcoin, making prices highly volatile (Berentsen & Schär, 2018, p. 14). Prices and volatility also seem to be unrelated to economic or financial factors, making it very difficult to forecast any trends (He, et al., 2018, p. 17). The above factors limit bitcoin's function as a store of value significantly, because holders are exposed to the risk of bitcoins losing their value while they are stored.

Unit of account

Bitcoin's function as unit of account is also questionable. The first problematic aspect is the relatively high value of a single unit. Goods and services must therefore be displayed in small fractions of a unit. It is assumed that people have difficulty understanding decimals, especially in terms of denominations up to 0.00000001 bitcoins, which is the smallest bitcoin denomination called a satoshi (see Figure 4) (Berentsen & Schär, 2017, p. 272 f.). So far there is no evidence that bitcoin is used as an independent unit of account; goods and services are more commonly represented in the value of fiat currency. Bitcoin prices are then based on the exchange rate. Retailers often quote prices in fiat currency and accept bitcoin at the exchange rate of the point in time where the purchase is made. In most cases, bitcoins are then exchanged to fiat currency immediately because of the high exchange rate risk (He, et al., 2018, p. 17). The high price volatility of bitcoin also complicates users' understanding of real economic prices. If bitcoin's exchange rate varies, the prices must also be adjusted. This makes bitcoin a rather unsuitable unit of account, although the function as unit of an account is not necessarily indispensable for a currency (Berentsen & Schär, 2017, p. 274).

4.2 Bitcoin and the qualities of money

Although the previous section already suggests that bitcoin's functions as money are rather poor, an examination of its monetary qualities is nevertheless informative. The block chain technology Nakamoto created includes the quality of indestructability, meaning that no units can be deleted or damaged. Bitcoins are easily portable and transferable through wallets of various kinds. Homogeneity is also assured through the Bitcoin code, since units are exactly the same as other units. The divisibility is divided in the subunits shown in Figure 4, making bitcoins suitable for even the smallest transactions.

Subunit	In bitcoins
1 Bitcoin	1 Bitcoin
1 Deci-Bitcoin	0.1 Bitcoin
1 Centi-Bitcoin	0.01 Bitcoin
1 Milli-Bitcoin	0.001 Bitcoin
1 Bit (Microbitcoin)	0.000001 Bitcoin
1 Satoshi	0.00000001 Bitcoin

Table 1: Subunits of bitcoin
Source: cf. (Berentsen & Schär, 2017, p. 273)

Furthermore, the Bitcoin network verifies transactions and their authenticity. Forgery is therefor out of question. Finally, as mentioned in Section 3.2, Bitcoin is limited to a maximum number of 21 million units. In conclusion, this means that bitcoin fulfils all of the qualities listed in Section 2.2, though the lack of compliance of functions drastically limits the possibility of bitcoins working as money.

4.3 Legal consideration

In general, there is no accepted legal definition of currency or money; however, certain aspects are defined in the law. To answer the question of whether or not bitcoin can be considered as money from a legal perspective, it is important to state that currencies are associated with the sovereign's power to provide a legal framework for issued banknotes and coins. Currencies only reach the status of legal tender under such legal framework, which is lacking for bitcoin and for cryptocurrencies in general. Furthermore, currency refers to money that is only issued by central authorities like a central bank (He, et al., 2018, p. 16). A domestic legal tender currency must be accepted to clear debts in the

respective country as cash but also in the form of bank transfers, checks, or direct debit. At present, bitcoin is not accepted as legal payment in any country except Japan;[1] therefore, bitcoin can only be described as complementary currency, missing to be accepted in economic transaction by majorities in other countries(Sixt, 2017, p. 120).

The value and credibility of a currency is linked to the ability of the state to support the currency, which is also part of the broader legal concept of money. This concept also includes certain types of assets or instruments that are convertible into legal tender currency. To count as such, assets or instruments must be expressed in currency, which must be generally accepted as a medium of exchange within the state (He, et al., 2018, p. 16). Bitcoin can be most accurately compared to e-money. E-money is every value saved electronically. However, this value must be in the form of a claim against an issuer. Since this claim against an issuer is missing in the case of bitcoin, it fails to meet the requirements to count as e-money (Sixt, 2017, p. 120).

Although the legal tender status may differ to some extent between jurisdictions, bitcoin is neither currency nor money from the legal point of view.

4.4 Bitcoin compared to existing legal currencies

Feature	Bitcoin	USD (home currency)
Economic demand factors		
Intrinsic value	None	None
Claim to issuers?	No	Yes
Legal tender	No	Yes
Used as a medium of exchange	Small, but rising especially in online retail	Yes
Used as unit of account	No	Yes
Used as store of value	Yes, subject to very high exchange rate risk and sudden confidence shock	Yes, subject to inflation risk

Table 2: Characteristics of currencies (extract)
Source: (He, et al., 2018, p. 14)

He et al. (2013, p. 13) have compared the characteristics of currencies as shown in Figure 5. This comparison provides a good overview of how the economic demand factors differ between a currency with legal tender status like the U.S. dollar and bitcoin. It reveals that bitcoin cannot conduct the functions of money, which legal tender currencies fulfil. Although neither has intrinsic value, one essential difference is the claim to the issuer. There are further substantial differences in the supply structures and the risks of macro-financial stability. While Bitcoin's supply is

[1] Japan's Bank Act is covering virtual currencies snce 2017, i.e. Bitcoin is officially accepted for payments of goods and services, making Bitcoin a legal tender within the country. The use and exchange of Bitcoin is highly regulated. (Reiff, 2017)

private and decentralised without the possibility of changing the quantity, U.S. dollars are issued flexibly by public financial institutions. This is the same for changes of the amount of units in circulation. The amount of bitcoins cannot be changed through monetary policy by central banks. A hyperinflation to oversupply can be denied for bitcoin because of the digressive supply of mining, which was explained in Section 3.2. This supply structure is characterised by the risk of long-term hyperdeflation because of the already set maximum amount of 21 million units. The U.S. dollar only faces a small risk of hyperinflation in the case of significant policy mismanagement, and long-term hyperdeflation is very unlikely (He, et al., 2018, p. 14 f.).

4.5 Conclusion

To answer the initial question of whether or not bitcoin can be considered future money, this chapter clearly shows the difficulties of bitcoin fulfilling the functions of money. Although bitcoin was originally designed to work as money and certainly has some monetary characteristics, it misses the initial ideology. Bitcoin is currently far from being a dominant medium of exchange because of a low adaption rate and technical limitations (Berentsen & Schär, 2017, p. 274). Bitcoin is neither suitable as a store of value because of strong fluctuations in the market price nor used independently as a unit of account. Berentsen and Schär (2017, p. 274) have concluded that bitcoin is not an optimal money unit, but a monetary use could be possible in the future. In general, jurisdictions do not accepting cryptocurrencies as money; therefore, laws concerning legal money are not applicable. Overall, this chapter demonstrates that bitcoin is not money.

Bitcoin and other cryptocurrencies must be considered assets. Their attractiveness as an investment class grew instantaneously when early investors made fortunes through bitcoin's rise over the years (Kiel Institute for the World Economy, 2018, p. 10). Today, people are not using bitcoin to be part of the original ideology of decentralised money, to pay with it, or out of interest in the technological progress. People more likely invest in bitcoin to generate profits (Rosenberger, 2018, p. 117). Bitcoin and other cryptocurrencies should therefore be considered crypto-assets.

Cryptocurrencies have a high potential for creating rapid changes in the financial industry even if they are not technically money. The absence of effective regulation has so far

contributed to their potential advantages, such as low transaction fees and processing times. On the downside, cryptocurrencies pose huge risks to the financial system in two different ways. One aspect is financial stability, and the other is financial integrity (He, et al., 2018, p. 24). As the analysis of bitcoin usage in Sections 3.3 and 3.4 demonstrated, bitcoin is comparatively insignificant compared to the worldwide financial markets. The risk of financial stability seems less immediate and is not examined further in this thesis.

The dimension of risk for financial integrity is highly relevant, however, including money laundering and the financing of terrorism, insecurity for consumers, tax evasion, and unregulated capital movements. These risks are much more contemporary and need to be addressed as soon as possible (ibid.) This is resulting in a challenge for financial regulators and supervisors, raising the question of what risks cryptocurrencies such as bitcoin bear for the integrity of the financial system and what actions policy response could take against them.

Since crypto-assets are commonly referred to as cryptocurrencies or by the generic term of virtual currencies, these terms are retained in the following chapters.

5 Risks to financial integrity

Virtual currencies appear to have certain characteristics that are very appealing to illicit actors. Overall, these characteristics can be summarised as ease of access and use, independence from controls of legitimate financial systems, increase of anonymity, and the possibility of use in the dark web (Jordan, et al., 2017, p. 10 f.). This chapter deals with common criminal activities and the reasons why virtual currencies, especially cryptocurrencies, are favourable for their implementation.

5.1 Money laundering

Money laundering is the process of disguising money of illegal origins to enable criminals to generate profits without attracting any attention to the criminal activities or persons involved. Organised crimes such as illegal arms sales, drug trafficking, and prostitution are just a few examples of the ways that criminals generate huge profits that then need to be

‘legitimised’ through money laundering. This happens by disguising the sources, changing the form, or moving the funds to inconspicuous places or businesses (FATF, n.d.). The goal of money laundering is therefore to create the illusion that the money originates from a legitimate source (Troeller, 2016, p. 163).

Since money laundering is an illegal activity, it is very difficult to estimate how much money is laundered; however, it is a fact that money laundering is happening worldwide to a large extent (ibid.). The United Nations Office on Drugs and Crime (UNODC) published a report on illicit funds in 2011 that estimates that the total amount of criminal proceeds generated in 2009 (tax evasion excluded) was approximately $2.1 trillion, or 3.6% of the global gross domestic product (GDP). The report estimates that 70% of these proceeds were laundered. In other words, approximately 2.7% of the global GDP, or $1.6 trillion, was successfully laundered by criminals worldwide in 2009 (UNODC, 2011, p. 10). These estimates are consistent with the International Money Fund’s previously established estimation that illicit money constitutes 2% to 5% of the global GDP (ibid., p. 19.).

The Financial Action Task Force (FATF) has emphasised how important the fight against money laundering is. Money laundering is a thread to the functioning of financial systems, affecting economic development, business, and even society. The integrity of the banking and financial services marketplace can only be maintained under a framework of high legal, professional, and ethical standards. When illicit money is processed through institutions, the integrity is in danger, which might result in significant macroeconomic consequences. Inexplicable changes in money demand, prudential risks to bank soundness, contamination effects on legal financial transactions, and increased volatility of international capital flows and exchange rates due to unanticipated cross-border asset transfers are examples provided by the FATF (FATF, n.d.). Furthermore, the whole economic development could be endangered. Like the damaged integrity of institutions, there can be negative effects on foreign direct investment when countries are associated with the influence of organised crime such as money laundering (ibid.).

Money laundering is very likely to be processed by professional money laundering individuals, organisations, or networks since ordinary private persons do not usually have the ability to launder large amounts of illicit proceeds (FATF, 2018, p. 12). An individual professional money launderer is someone who provides services or expertise in placing and

moving funds. The money laundering service might be performed under the guise of a legitimate occupation. Examples of services by individuals can include ‘accounting services, financial or legal advice, and the formation of companies and legal arrangements’ (ibid.). When two or more individuals act as a structured group to provide such services, the money launderers are considered a professional money laundering organisation. Finally, professional money laundering networks operate in the largest, most global dimensions and consist of associates or contacts facilitating money laundering schemes. These networks can include various organisations working together (ibid., p. 13).

5.1.1 Process of money laundering

To begin with, illegal goods and services are exchanged for money: usually cash, since cash allows anonymous and irrevocable transactions without the involvement of third parties. This ensures that no traces are left behind for investigative authorities (Brening , et al., 2015, p. 3 f.). Because of their design, virtual currencies appear to be a good alternative to cash considering the same possibility of anonymous and irrevocable transactions. Virtual currencies are especially suitable for internet transactions involving illicit stores, including dark web marketplaces. Although cash and virtual currencies are most suitable to be used for the money laundering process, bank transfers can also be used, especially for proceeds created through fraud, embezzlement, or tax crimes (FATF, 2018, p. 18).

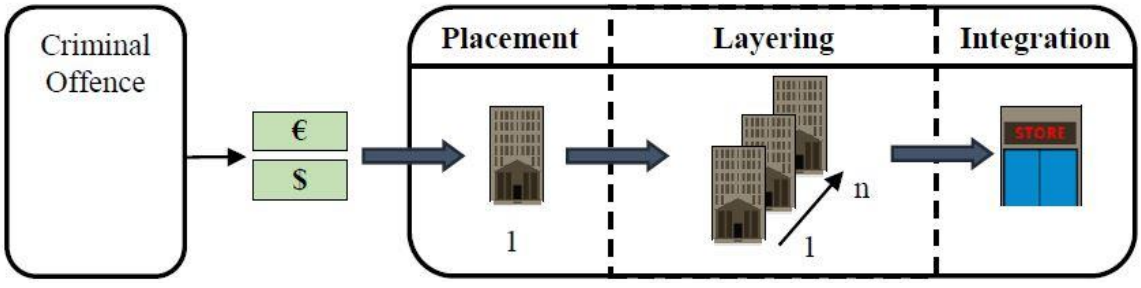

Figure 4: Money laundering process
Source: (Brening , et al., 2015, p. 4)

No matter the form in which illegal proceeds are created, the funds then run through three general stages of money laundering, as illustrated in Figure 6: placement, layering, and integration (Brening , et al., 2015, p. 4).

To begin with, the obtained funds are placed into the financial system in a form that will attract less suspicion from public authorities, making the funds more liquid to operate (Brening , et al., 2015, p. 4). The funds are introduced into the money laundering scheme depending on the form in which they were originally generated. In terms of cash, the funds are passed over to a cash collector who then introduces the money through cash-intensive businesses such as money value transfer services or casinos. In terms of virtual currencies, an e-wallet or address on a distributed ledger platform is required, which the funds can then easily be transferred to anonymously. Bank transfers are usually run through legal entities to then be transferred to the first layer of companies that are run by money launderers (FATF, 2018, p. 18).

Then the layering stage is initiated. The funds are passed through many layers such as institutions or jurisdictions in the form of various complex financial transactions to disguise the illicit origin. They can be channelled through investment instruments such as bonds, stocks, and cheques or simply transferred from accounts of various banks to other accounts, particularly into countries with loose anti-money laundering controls (Brening , et al., 2015, p. 4).

In the last stage, the funds are integrated into the legal economy without any connection to the criminal activity from which they were earned. Professional money launderers often invest the funds on behalf of their clients in real estate, luxury goods, and businesses abroad. In rare cases, the funds are invested in their country of origin; alternatively, the funds can be spent on goods deliveries to the country (FATF, 2018, p. 19).

The Royal United Services Institute for Defence and Security Studies (RUSI, 2017) has published a paper on ‘Virtual Currencies and Financial Crime’, explaining two generic methods of how virtual currencies are used in the money laundering process. One involves the placement of fiat currency into a bank or similar financial institution, converting those funds to virtual currencies through exchanges and then disguising the criminal origin through a number of virtual currency-based transfers or purchases. The second method includes the acceptance of virtual currencies for illegal goods and services in the first place, then converting them to fiat currency and ‘subsequently fund transactions and purchases designed to conceal their illicit source’ (RUSI, 2017, p. 14).

5.1.2 Virtual currencies as money laundering instruments

An analysis of money laundering-related factors demonstrates why bitcoin and other cryptocurrencies are very suitable for money laundering. Brening et al. (2015, p. 7 ff.) have examined how certain features of bitcoin affect its potential for money laundering. The first essential aspect is the lack of intermediaries for transactions as well as the lack of a central oversight body authorised to control which individuals create accounts, and how many. Section 3.3 illustrated how easily individuals can use wallets and accounts. These wallets and accounts can only be accessed by the individual knowing the corresponding private key, making it impossible for financial institutions to have insight into wallets and transactions for investigative purposes. The lack of a central authority prevents the applicability of any anti-money laundering controls. There are basically no barriers for individuals in using cryptocurrencies and no possibilities for authorities to detect illicit funds. This makes cryptocurrencies a particularly suitable instrument for money laundering (ibid., p. 8). This aspect has also ben emphasised by Scheau and Pop Zaharie (2017, p. 307): any potential user is allowed to transfer money with high speed and low costs, no matter whether the transfer is legitimate or criminal.

In addition to the possibility of using various wallets and transferring illicit money quickly, inexpensively, and without any limitations, the money can also be transferred much more discreetly (ibid.). Anonymity is the therefore the second important factor that must be noted. Although every transaction made is written in the block chain, it is impossible for investigative authorities to link the pseudonyms (public keys) to individuals without identifying information from outside the system. The possible use of various wallets and accounts also amplifies these problems and hides the origins of illicit funds. The pseudonymous authentication within the Bitcoin system allows individuals to act anonymously and prevents any customer identification procedures, as long as individuals do not communicate any personal information outside the system (e.g., with exchanges or online retailers) (Brening , et al., 2015, p. 8).

As previously mentioned, bitcoin offers almost the same anonymity and irrevocability of transactions as cash does. Once a transaction is confirmed within the Bitcoin system, there is no possibility of demanding the transferred funds back unless the receiver opens a new transaction. Criminals profit from this aspect, since receiving transactions for illegal goods

and services is protected against payment fraud (criminals obviously cannot take any legal action against payment fraud). Law enforcement is unable to detect and assign transactions or to reverse transactions posteriori (ibid., p. 9). While cash is restricted to being handed over in a physical process, Section 3.4 clarifies how flexible and portable virtual currencies are, no matter what sums are involved in transactions. Furthermore, virtual currencies can be transferred worldwide without interruption. Compared to bank transfers, virtual currencies leave out several authorities. This enables criminals to move large amounts of money across borders easily, which clearly encourages laundering processes using virtual currencies.

Although virtual currencies seem to be perfectly conducive to money laundering, the high price volatility must be considered a significant problem. The layering stage of the money laundering process usually involves several transactions that take time (Brening , et al., 2015, p. 9). The exchange rates between fiat currency and virtual currencies can fluctuate highly while the illicit funds are in the layering process. If, for example, money is exchanged for bitcoin to be laundered, the price of bitcoin might decrease rapidly. The original funds would then decrease in overall value. Money launderers operating with virtual currencies have to monitor the market continuously to prevent losses. This monitoring, however, adds to the cost of the laundering. Volatility has a direct negative effect on money laundering, adding a certain difficulty of calculation and risks of losing the value of the funds (ibid.).

The analysis of virtual currencies as money laundering instruments shows how much potential they have for criminals and especially for money laundering. In theory, virtual currencies seem to be the ideal instrument for these illegal procedures. The decentralised matter, the quasi-anonymous system, and the ease of implementation make cryptocurrencies very likely to become a frequently used tool in money laundering around the world.

5.1.3 Evidence of the use of virtual currencies for money laundering

The National Crime Agency gives an annual 'National Strategic Assessment of Serious and Organised Crime' dealing with criminal activities and money laundering in the UK. The report warns about the increasing use of cryptocurrencies as a money laundering tool, though cash is still the most frequently used tool at present (NCA, 2018, p. 40). However, law enforcement is already dealing with cases of money laundering through virtual currencies.

Liberty Reserve was the largest online money laundering case in history. Taking place in May 2013, the U.S. Department of Justice charged Liberty Reserve, a money transmitter based in Costa Rica, with operating an unregistered money transmitter business and money laundering of more than $6 billion USD of illicit proceeds (FATF, 2015, p. 32). The centralised digital currency service allowed users to deposit fiat currency and convert it to digital currency that was bound to the value of the fiat currency. The deposited money could be transferred to other users without any limitation for just a small transaction fee. Personal information of users contained only a name, an email address, and a birthdate. (UNODC, 2015). However, Liberty Reserve did not validate identities, which meant that users could routinely establish accounts under false names and fake addresses. To extend the anonymity, deposits were primarily made through unlicensed money transmitting businesses in Russia, Malaysia, Nigeria and Vietnam. While making transactions, users could choose to pay an extra privacy fee of $0.75 USD per transaction to hide their Liberty Reserve account number, thus making the transfer completely untraceable (FATF, 2015, p. 33). Investigators are sure that Liberty Reserve was run mainly for money laundering purposes. The high degree of untraceability and the simple structure were perfect for storing and transferring proceeds of illegal activities. Investigators shut Liberty Reserve down in May 2013. Seven individuals were charged and sentenced for money laundering and operating an unlicensed money transmitting business (UNODC, 2015).

The cryptocurrency research group CipherTrace conducted an analysis of 45 million bitcoin transactions, estimating money laundering through unregulated cryptocurrency exchanges. The outcome identified 380,155 bitcoins received in cryptocurrency exchanges from criminal sources since Bitcoin was founded in 2009. This means that unregulated

bitcoin exchanges laundered an estimated $2.5 billion USD. The report states that criminals are laundering illicit funds mostly in countries with low anti-money laundering policies and that criminal activities and transactions can be reduced in the presence of strong anti-money laundering regulations, including warnings about virtual currencies (CipherTrace, 2018, p. 2 f.). Regulations and possible policy responses are examined in Chapter 6.

5.2 Terrorist financing

The financing of global terrorist organisations through virtual currencies is an emerging risk. Although third party reporting has suggested the use of anonymous virtual currencies like bitcoin, the use has not often been confirmed by law enforcement at this point (RUSI, 2017, p. 17). There is no concrete indication in the public record that terrorists are financed through cryptocurrencies on a regular basis (ibid., p. 19). The main question that needs to be answered is whether or not virtual currencies provide substantial benefits for a wide range of terrorist actors over other terrorist financing methods. To answer this question, it is necessary to define different structures of terrorist actors and subdivide the term ‘terrorists’, which is often used as a generic term. The range of terrorist actors include lone actors who act on their own and may lack connections to terrorist groups; small cells and facilitation networks, which might be connected to main groups; command and control organisations without an established base; and finally, territory controlling groups such as ISIS or Al-Shabaab (European Parliament, 2018, p. 27). The term ‘terrorist financing’ includes various methods of financing, particularly raising funds through donations or criminal activities. Mostly moving funds into countries near theatres of combat that can be later spent on attacks or military operations (ibid.).

A recent study on virtual currencies and terrorist financing by the European Parliament (2018, p. 28) investigated different financing methods for terrorist actors. For lone actors and small cells, relatively small funds are required to plan and commit attacks. Given the example of the 2016 Bastille Day attack in Nice, France, the only funds required were those to hire a truck. It is basically impossible for financial institutions to foresee that funds of this size will be used for terroristic actions. Virtual currencies provide no substantial advantages for actions that are already funded easily using conventional methods such as

cash through self-funding. The present opportunities for everyday use of virtual currencies are very limited and make no difference for terrorist actors in small structures.

The financing of larger groups, such as al-Qaeda and ISIS, is often accomplished through enforced taxation of individuals and businesses that are under the control of these groups (European Parliament, 2018, p. 28). The financing must be simple, straightforward, and reliable. ISIS members often rely on simple funding methods such as acquiring student loans (RUSI, 2017, p. 17 f.). The volatility and challenges of usability makes virtual currencies a rather unreliable method of transferring or moving funds as soon as they reach a meaningful size. However, bitcoin was discussed in an al-Qaeda online publication in terms of whether or not it is allowed by Sharia law. It concludes that there are very favourable aspects of cryptocurrencies for the purposes of these groups, but there are also obstacles that would have to be overcome for increased use (European Parliament, 2018, p. 28).

Virtual currencies are creating new possibilities for the financing of terrorism, even if there is no particularly need for a replacement of already established financing methods. It is important to bear in mind that terrorists are rapidly adapting to technological progress and virtual currencies are becoming an increasingly viable tool for financing, especially for certain areas (RUSI, 2017, p. 18). This is particularly true for a younger demographic of jihadis who are comfortable using new financial technologies, having grown up with the internet. Areas that clearly benefit from the use of virtual currencies are the procurement of illegal firearms or explosives on the dark web, as well as the purchase of travel documents or other items useful for terrorist operations (ibid.). Virtual currencies could also open a new dimension of online crowdfunding for terroristic groups. These crowdfunding efforts are often disguised under a pretext of donations for humanitarian activities. In 2015, a teenager in the US was convicted of supporting ISIS by providing advice on how bitcoin could be used to mask financial transactions to support ISIS. This illustrates how virtual currencies could be an essential new way of gathering funds in the future (European Parliament, 2018, p. 28).

5.2.1 Aspects favouring terrorist financing

The features of virtual currencies that bring advantages to terrorist financing methods are mostly the same ones that make virtual currencies favourable for money laundering. In the case of bitcoins, pseudonymity becomes somewhat problematic for criminals in terrorist financing. As previously mentioned, users are represented in the block chain with alphanumeric addresses of their wallets. Information such as dates, values, and sending and receiving addresses are recorded chronologically for all transactions (European Parliament, 2018, p. 30). In terms of money laundering, the pseudonymity could be considered as anonymity if no information from outside the system was provided and then linked to any information within the system. In the case of terrorist financing, such as a public crowdfunding effort in disguise, it is more likely to be detected outside the system and might be connected to at least one receiving address that was used to receive funds inside the system. At this point, an entity or person is known to be the owner of a certain Bitcoin address. Various private firms are specialising in de-anonymising these Bitcoin addresses through analysis of their transactions, connecting more addresses to illicit activities and then providing this information to law enforcement agencies or exchanges in order to scrutinise them for signs of suspicion. Terrorists who trusted Bitcoin's pseudonymity and posted an address to social media accounts and public channels could be traced through such an analysis, allowing security analysts to monitor the movement of jihadists' bitcoins in real time (ibid., p. 31).

This shows that the financing of terrorism is slightly more afflicted with risks than the procedure of money laundering, since intersection points are more easily exposed. However, there are several ways to add layers of anonymity. Services are offering ways to aggregate bitcoins from many users and redistribute them to disguise the origins. One example is DarkWallet, a service that integrates a mixing feature into a user's wallet. Alternative virtual currencies are even hiding information such as the date, the value, and sender and receiver information, making it impossible to comprehend transactions at all (ibid., p. 32).

The transferability and portability of bitcoin are very attractive for the financing of terrorism. International transfers avoiding any regulated intermediaries are very suitable for any criminal activity and reduce the risks of being detected by law enforcement.

Portability can also be seen as an advantage when funds need to be carried across borders without transactions. Carrying large amounts of physical cash is likely to raise suspicion at border controls, but the same amount of money in bitcoins can be carried as a piece of paper or in a wallet application in a mobile phone (ibid., p. 39).

Although there are only a few known cases of terrorist financing through virtual currencies and no concrete indication in the public record (RUSI, 2017, p. 19), experts have assumed that the likelihood of terrorist actors using these methods is continuously increasing (European Parliament, 2018, p. 39). As the analysis of money laundering-related factors of virtual currencies illustrated, these features are also favourable for terrorists in various ways. Therefore, terrorists will adapt to new technologies.

5.2.2 The use of virtual currencies for terrorist financing

Only a few cases of terrorist financing have been confirmed so far, but since virtual currencies are reducing the ability of law enforcement to detect those transactions, real use with terroristic background could be more frequent than estimated.

One of the first cases of low-value bitcoin fundraising by a Palestinian terror organisation was detected by Yaya Fanusie, a former counterterrorism analyst for the Central Intelligence Agency (CIA). Fanusie discovered that the Ibn Taymiyya Media Center is linked to a jihadist propaganda unit based in the Gaza Strip. The media group ran an online campaign calling for Muslims worldwide to donate funds under religious obligations to fight for Islam. In late June 2016, the campaign added the option to pay in bitcoins, posting QR codes linked to the Bitcoin address on Twitter and social media (Fanusie, 2016). Fanusie has stated that this is the first publicly verifiable instance of a terrorist group using bitcoin. As previously mentioned, this revelation of a connection between a Bitcoin address and a terror group created an opportunity for law enforcement to detect further Bitcoin addresses that are connected through transactions. The Blockchain Alliance, a public-private partnership, engages and publishes this information to firms and exchanges to prevent further illicit activities. However, such efforts to prevent criminal activities have been few and rarely successful (Fanusie, 2016).

In 2017, the Indonesian government announced that Indonesian operatives of ISIS had used bitcoins in transactions with several other jihadis. The government confirmed that the terror group could be connected with a 2016 terrorist attack in Jakarta. Information on whether or not the Bitcoin transactions were instrumental in any attacks could not be confirmed (RUSI, 2017, p. 18). In the same year, a 27-year-old woman named Shahnaz pleaded guilty to using bitcoins and other virtual currencies to support ISIS. Shahnaz admitted to sending about $62,000 USD in bitcoins to ISIS (Mangan, 2018).

Some incidents of fundraising could be detected on Twitter and social media. Some actions were posted publicly without any effort to disguise them. One example was fundraising for Al-Sadaqah, an organisation that openly asked for funds to 'provide the Islamic rebels in Syria with financial aid.' The post requested donations 'anonymously with Bitcoin and Monero'. Monero is a highly anonymised private virtual currency. Al-Sadaqah is still calling followers to support terrorists in Syria with 100% anonymous and completely untraceable transactions (European Parliament, 2018, p. 34).

What is believed to occur more often than direct transactions supporting terrorism is the use of virtual currencies on the dark web to buy and sell illegal goods to support terroristic operations. Obtaining stolen credit card details or engaging in the sale of drugs to raise funds are some examples of many possible strategies. Even documents like registered German passports can be bought, as investigations have revealed (European Parliament, 2018, p. 37). Since only minimal amounts of funds are necessary to obtain illicit items for executing attacks, these activities often go undetected by law enforcement. Former technological barriers to using the dark web and Bitcoin to obtain such items are eroding, because guides on how to use these sites and disguise any traces can easily be found online. This indicates the increased likelihood that terrorist actors will use these methods for terrorist financing and the financing of goods and services to support their ideology (ibid.).

5.3 Fraud and cybercrime

The block chain's immutability guarantees that transactions cannot be reversed or terminated like credit card transactions; no intermediary can cancel or reverse a transaction. What seems to be secure can also expose users to a huge risk. Because the

transaction is irreversible, purchasers are not protected against failure to deliver goods. If the customer receives faulty products or counterfeits, there is no way to get the money back unless the seller agrees to a new transaction. This aspect also allows fraudsters to operate under false identities and carry out frauds much more easily since victims have no chance to make the fraudster accountable (RUSI, 2017, p. 19).

Another major fraud or, more specifically, cybercrime opportunity originates directly from virtual currency exchanges (ibid.). The Mt. Gox case discussed in Section 3.1 shows that even renowned and widely established Bitcoin exchanges are susceptible to attacks. Several cases of exchanges simply disappearing, shutting down, and stealing their customers' deposits have occurred (ibid.). When customers deposit in exchanges or online wallets, it is like holding an IOU; the website or exchange company holds the private key information and therefore the Bitcoin asset. These exchanges are major targets for fraudsters and hackers. If hackers successfully enter the internal system of online wallet providers or exchanges, they can easily transfer funds and disappear (Mansfield, 2018). The block chain's immutability prevents any chance of getting the stolen funds back. The amount of 750,000 bitcoins disappearing from users' accounts on Mt. Gox in 2011 provides a warning about how endangered exchanges and wallets are, or in Mt. Gox's case, how prone they are to internal criminal activities. A report by the block chain and virtual currency forensics firm CipherTrace estimates that more than $927 million USD in the form of virtual currency was stolen in 2018 alone. Attackers hacked into the Japanese Bitcoin wallet and exchange service Coincheck and stole approximately 500 million in NEM tokens, a cryptocurrency like Bitcoin. The estimated value of the stolen coins amounted to $530 million USD, making it one of the largest cryptocurrency heists in history (CipherTrace, 2018, p. 9).

The other main target for fraudsters is personal wallet information. Once hackers are able to receive login data or information to access a personal wallet by, for example, hacking a user's cloud information, funds can be stolen. Although the address of the receiving wallet is displayed in the block chain, there is no way to either sue users or reverse the transaction (Mansfield, 2018).

Virtual currencies have become the favoured tool of hackers and online thieves in recent years. A common cybercrime is the so-called 'ransomware' attack. These programmes

encrypt data on the targeted servers, computers, or mobile devices and will only encrypt the data when a ransom is paid. These attacks are not a new phenomenon, but since attackers demand virtual currencies for the ransom payment, it is more difficult to capture the criminals (RUSI, 2017, p. 20).

6 Regulatory approach

Taking the financial integrity risks proceeding from virtual currencies into consideration, the need for regulation becomes obvious. Suggested approaches differ from simple public warnings to regulation of certain market participants and even to complete prohibition. Taking a closer look at the problematic aspects of regulation, a coherent international approach seems to be necessary for successful control of risks (Read & Gräslund, 2018, p. 509). The Bank for International Settlements (2015, p. 13) has published a classification of the main types of regulatory actions that could be implemented in case of virtual currencies. The main options are listed below.

Information/moral suasion

For example, public warnings and publications on dangers and risks in the form of research papers.

Specific stakeholder regulation

For example, regulation of digital currency administrators or exchanges as well as consumer protection measures.

Interpretation of existing regulations

Existing frameworks such as tax law treatments are applied to digital currencies.

Overall regulation

An approach covering all the aspects of consumer protection, organised rules for stakeholders, and specific operation rules as payment systems.

Prohibition

A ban on transactions in general, digital currency acceptance, digital currency-based financial instruments, and digital currency exchangers.

Virtual currencies combine properties of currencies, commodities, and payment systems. Depending on which classification is used, different approaches to implications for legal treatments result. Even within the same jurisdiction, it can be difficult to determine the authority in charge, since different authorities classify virtual currencies according to their own policy priorities (He, et al., 2018, p. 24). In terms of regulation of virtual currencies, regulators are also facing unique new challenges. These challenges, recommendations for future implementations, and the current state of regulatory approaches with a focus on fighting criminal activities are discussed in the following section.

6.1 Challenges

The features of bitcoin and other cryptocurrencies that are favourable for criminal activities are the same features that create special challenges for authorities in charge of regulation. The pseudonymity/anonymity contains the first problematic aspect. As previously mentioned, it is impossible to collect any useful information such as statistical data, user information, or transaction processes. Although the data is visible in Bitcoin's case, it cannot be linked to users and is therefore not usable for authorities. Further aggravating the process of regulation is the transnationality of virtual currencies. Jurisdictions with national competence are facing transactions and market participants or schemes of a technology that is easily used across borders worldwide. National authorities lack the capability to enforce laws and regulations in a 'virtual' environment (He, et al., 2018, p. 25). Nevertheless, traditional regulatory models are usually applied at the central intermediary like issuers or payment processors. Since cryptocurrencies proceed without these intermediaries, one of the main challenges for regulation is to decide whom to regulate (ibid.). For example, Danton Bryans (2014, p. 469) has stated that it is more effective to analyse each Bitcoin transaction entity individually and decide which is the best to regulate based on a cost-benefit analysis.

6.2 Recommendations

Different recommendations on how to regulate virtual currencies in order to fight criminal activities have been published by various institutions. One of the most important guides was established by the FATF. The FATF guidance for a risk-based approach to virtual currencies (2015, p. 8 ff.) focuses on assisting countries in managing the money laundering and terrorist financing risks of virtual currencies. It advises countries to extensively assess the risks before taking any measures. The risk assessment resulted mainly in the advice that countries should focus on the exchange of virtual currencies. A solid cooperation between public and private sectors to assist competent authorities in the regulation of exchange platforms is therefore an important basis for regulation. Countries must consider inter-agency working groups to enable policy-makers, regulators, supervisors, financial intelligence units, and law enforcement authorities to cooperate in the process of employing effective polices and measurements to address money laundering and terrorist financing. Another recommendation by the report is to license or register any providers of money value transfer services and ensure their compliance with relevant anti-money laundering and counter-terrorist financing measures. Since these providers transfer values digitally via the internet, exchangers are most likely not present in the country in which they offer transfer value services. The more important is a clear oversight by home jurisdiction and their cooperation and information exchange to other jurisdiction the services are provided in. This is significant for any exchange activities from virtual currencies to fiat money. Exchanges should be subject to legal frameworks including the possibility of keeping records of customer identification. Further recommendations suggest targeting wire transfers in general. Countries should ensure that they obtain valid information about originators and beneficiaries. In this regard, countries may adopt a de minimis threshold for cross-border transfers no higher than $1,000. Financial institutions should monitor transfers of virtual currencies and intervene in cases of missing or alarming information (FATF, 2015, p. 10 f.). Overall, international cooperation is suggested in order to help other jurisdictions combat money laundering and terrorist financing (European Parliament, 2018, p. 47).

The FATF is currently reviewing its recommendations in light of the rapid developments of range and financial functions served by virtual currencies and considering whether further updates are necessary to ensure that FATF standards stay up-to-date (FATF, 2019).

The Royal United Services Institute for Defence and Security Studies (RUSI) (2017, p. 36) supports the FATF guidelines and has stated that international organisations should facilitate collaborations between governments on appropriate regulatory and law enforcement responses. Additionally, governments should ensure that staff have adequate knowledge and training regarding how to manage virtual currency risks. In general, an adaptive regulation is advised and new technologies should face new strategies of regulation since out-dated regulatory frameworks might not be suitable for countering emerging risks. Banning highly anonymised cryptocurrencies is considered impractical and counterproductive for promoting the useful innovation side of virtual currencies. RUSI has also emphasised that industry participants should aim for an appropriate balance between data privacy and transparency in dealing with virtual currency transactions in order to explore potential tools and applications for managing financial crime risks. Intra-industry working groups need to be established to ensure that participants can exchange information on best risk management solutions to tackle the new challenges as well (RUSI, 2017, p. 40). Finally, the RUSI report suggests that banks and other established financial sector participants build sufficient knowledge and awareness for related risks. Cross-sector partnerships with the virtual currency industry including networking arrangements, working groups, or associations should build a strong financial crime risk management practice to deal with virtual currency-related risks (ibid., p. 44).

6.3 Current state of regulation

At present, the regulatory approaches vary greatly in different jurisdictions. Some regulators prohibit the use of virtual currencies entirely out of fear that bitcoin and other virtual currencies allow free capital flows without any supervision to prevent criminal activities. Other regulators have attempted to design new, specific laws and regulations tailored to virtual currencies. Still other regulators have attempted to apply legacy regulatory systems to virtual currencies. This includes regulating virtual currencies in the same matter as money, securities, or commodities (Sackheim & Howell, 2018, p. viii). The publishers of *The Virtual Currency Review* (2018, p. viii) have collected information on regulation of virtual currencies of various jurisdictions and have emphasised that the lack of global standards has led to a great deal of regulatory arbitrage. So far there is no central authority over virtual currencies within or across jurisdictions. Furthermore, these

publishers have stated that optimal regulatory structures can only emerge and converge over time.

To provide an overview of different strategic approaches to face arising virtual currencies, some exemplary regulatory approaches are examined below. The taxation of cryptocurrencies is not taken into account.

Germany and European Union member states

So far, Germany has no specific regulatory framework designed for virtual currencies. Instead, the general financial regulatory regime applies. This means that different laws concerning capital markets, banking, financial services, and anti-money laundering needs are validated on a case-by-case analysis. Numerous overlapping sources of German and European Union (EU) law must be considered for this purpose (Berberich & Wohlfarth, 2018, p. 118) The Federal Financial Supervisory Authority, which is subject to the legal and technical supervision of the Federal Ministry of Finance, has qualified bitcoin as legally binding as a financial instrument, and virtual currencies are categorised as a type of accounting unit but not as legal tender. According to the Federal Financial Supervisory Authority regulations, the general use of virtual currencies for participating in trade and exchange transactions (including private mining) is allowed without explicit permission. However, commercial handling of virtual currencies might require permission under the German Banking Act (Kreditwesengesetz) (BaFin, 2016). Operating exchanges and trading platforms in the finance commission business require a Kreditwesengesetz licence and are subject to financial supervision. In terms of anti-money laundering measures, virtual currencies are included in the Anti-Money Laundering Act (Geldwäschegesetz), which transposes the fourth EU Anti-Money Laundering Directive (AMLD4) into current German laws. This directive will soon be replaced by AMLD5, which was adopted in April 2018 by the European Parliament and must be transposed into the law of EU member states within 18 months (Berberich & Wohlfarth, 2018, p. 130). The fifth EU Anti-Money Laundering Directive introduces cryptocurrency regulation to the member states since it extends the anti-money laundering scope to virtual currency platforms, wallet providers, and tax-related services. It grants financial intelligence units more access to information and allows them to collect data and customer information and connect individuals to wallets and virtual currency addresses. Finally, business relationships or transactions involving high-risk third countries are limited by law (European Parliament, Council of the

EU, 2018). In general, AMLD5 prescribes monitoring virtual currency transactions and applying enhanced due diligence to high-risk companies and customers (European Parliament, 2018, p. 50). Entities subject to German Money Laundering Act and AMLD4/AMLD5 must also comply with various responsibilities such as establishing an adequate risk management system including analysis of activity-related risks and customer and business-related internal security measures. A nomination of a sufficient anti-money laundering officer at management level responsible for anti-money laundering compliance as well as know-your-customer principles that identify and verify customers and beneficial owners is advised. Finally, entities are obligated to report any sort of suspicious transaction to the Central Financial Transaction Investigation Unit (Berberich & Wohlfarth, 2018, p. 132).

In terms of the stage of regulation, EU member states are regarded as relatively advanced due to constantly developing EU mechanisms (Thomson Reuters, 2017).

The United States

Like in the EU, cryptocurrencies are legal in the United States but are also not legal tender. The U.S. Commodity Futures Trading Commission (CFTC) interprets cryptocurrencies as commodities. While tax laws and fine details vary among the states, U.S. regulations can be considered cryptocurrency-friendly. Using cryptocurrencies for transactions involving legal goods and services is free from regulation; commercial use, however, such as mining on a large scale, trading, or the operation of exchanges is defined as money transmitting and is subject to regulations. The main institutions of the U.S. regulatory regime for virtual currencies are the U.S. Securities and Exchange Commission (SEC), which is responsible for regulating transactions if they are offered or traded as securities or investment contracts, and the Financial Crimes Enforcement Network (FinCEN), which regulates money services transmitters and publishes the guidance for virtual currency exchanges in the U.S. (Austin, 2018, p. 330). The Bank Secrecy Act comes into effect in terms of money laundering. FinCEN issues and enforces anti-money laundering regulations under Bank Secrecy Act authority (ibid., p. 351). Any business acting as a money service business must be registered with FinCEN and is encouraged to implement a special risk-based, anti-money laundering programme. To prevent money laundering and terrorist financing, the programme must contain the following minimum requirements: any regulated business must establish policies, procedures, and internal controls to verify customer identification,

file reports, create and retain records of customers or business partners, and respond to law enforcement requests. Anti-money laundering compliance procedures must be set up with automated data processing systems to the extent applicable. Businesses must further maintain a list of agents, designate an anti-money laundering compliance officer, and provide anti-money laundering training for relevant personnel. Programmes are periodically reviewed to ensure adequacy (Austin, 2018, p. 355).

The CFTC and SEC are in charge of civil enforcement. The CFTC intervenes in any fraudulent, deceptive, or manipulative activity involving virtual currencies as well as violations of registration and executes enforcement actions in case misbehaving is detected. Several incidents of money laundering, fraud, or suspicious transactions from trading platforms and companies were reported and settled by courts through the work of the CFTC (ibid., p. 362). The SEC's scope of action is more limited than the CFTC's since the SEC can only execute legal actions involving incidents within the definition of securities. Rule violations involving registration, business conduct, trading, hacker attacks, fraud, and manipulation are targeted by the SEC's Cyber Unit (ibid., p. 364).

The US is considered very cryptocurrency-friendly and a global leader in terms of virtual currency regulation (Thomson Reuters, 2017).

Other countries

Other countries try to prevent criminal activities through general prohibitions. Jurisdictions such as Algeria, Saudi Arabia, Pakistan, and China forbid any commercial or private use of cryptocurrencies. Violations result in harsh penalties. To enforce laws, measures such as internet filters that block all virtual currency-related websites are implemented, and public warnings state that virtual currencies are extremely dangerous. Egypt has even declared Bitcoin haram, which means that Bitcoin is forbidden under Islamic law (ibid.). Still others have yet to undertake any concrete regulation approaches or risk-based policies at all, which creates an escape route for criminals (European Parliament, 2018, p. 47).

6.4 Evaluation

The examination of regulation of cryptocurrencies shows a clear link between the risks listed in this thesis and the recommended regulatory approaches. The German Anti-Money Laundering Act directly includes cryptocurrencies, as do the AMLD4/AMLD5 directives of the EU. The same connections between risks and regulation are observed in the US. Any commercial use of cryptocurrencies, both in the EU and the US, must comply with certain policies that are mainly designed to prevent money laundering and terrorist financing. If these policies are compared to the recommendations given by the FATF, a clear tendency of consistency is apparent. This becomes clear through the emphasis on risk-based approaches by the FATF and is executed with consideration of new emerging technologies and products related to cryptocurrencies. Both example jurisdictions follow the recommendations to register or license legal persons providing money value transfer services and implement regulation and supervision of cryptocurrency exchanges. This also includes customer identification and recordkeeping of information as well as monitoring transactions. Interagency cooperation can easily be realised through the transparency advised between authorities. Some countries are intensively adapting to the risks emerging from cryptocurrencies; however, the greatest challenge to a successful regulation of cryptocurrencies seems to be their cross-border portability and transferability, which makes it very difficult to enforce laws and regulations without a highly complex network of international cooperation. This has also been recognised by Joachim Wuermeling (Deutsche Bundesbank, 2018), a member of the board of Germany's Bundesbank, who has emphasised that an effective regulation of virtual currencies is possible through international cooperation. The regulatory power of national jurisdiction would not be sufficient to face global networks of illicit actors, which can easily escape regulation if other countries still allow unsupervised use (ibid.).

This clearly demonstrates how difficult the task of effective regulation actually is. The technological possibilities of dark net access or the use of proxy servers allow untraceable use of cryptocurrencies, even in jurisdictions with strict prohibitions. A prohibition can therefore only be considered conditionally effective. Considering the regulation possibilities presented by the International Bank for Settlements as well as recommendations by the FATF, an overall international regulation system including consumer protection, organised rules for stakeholders, specific operation rules as payment

systems, and a transparent cooperation between responsible institution seems to be the only way to deal with cryptocurrencies. Leading regulators like the US and Europe serve as an example; however, their regulatory approaches will only be effective in the long run if other countries follow and participate in the regulatory system.

7 Conclusion

To answer the initial question of whether or not bitcoins can be considered money, the detailed examination of Bitcoin based on the theory of money allows a clear classification. Bitcoins' functions in relation to state-supplied money show clearly that bitcoins cannot be considered money and is not regarded as such. This is due to bitcoins' failure to fulfil the essential functions of money. Bitcoin has no legal tender status and is far away from being a dominant medium of exchange. The prices for bitcoin are highly volatile, which prevents it from being an adequate store of value, and there is no evidence that it is used as an independent unit of account. Although a monetary use would technically be possible, from an economic and legal point of view, bitcoins are not classified as money. Bitcoin and other cryptocurrencies must therefore be classified as assets and are considered by many as an investment category. However, the great potential of the technology behind Bitcoin is widely noted and might be adopted by financial intermediaries processing fiat currency in the near future.

The analysis of the usage of Bitcoin indicates that Bitcoin's impact on financial stability is currently insignificant and is at this stage no danger to financial systems and state money monopolies. On the other hand, the sections that followed demonstrate what serious risks have arisen in terms of financial integrity and point out the risks emerging from bitcoin and other cryptocurrencies. As the thesis indicates, bitcoin and other cryptocurrencies are providing a powerful new tool to criminal actors in several ways. Money laundering, terrorist financing, fraud, and cybercrime are executed significantly more efficiently with cryptocurrencies. The examination of Bitcoin's outstanding characteristics such as ease of access, cross-border transactions, independence from controls of legitimate financial systems, increase of anonymity, and the possibility of disguise through the dark web also clearly indicate that the use of Bitcoin contributes to criminal activities. Although cryptocurrencies may not be widely established among criminals at this point, the early exemplary cases show that cryptocurrencies will become more and more popular for illicit

actors in the future. Institutions such as the FATF and the United Nations Office on Drugs and Crime have provided express warnings about this and have emphasised that extensive and risk-oriented regulation is absolutely necessary to secure financial integrity.

The same characteristics that are beneficial for the illegal use of cryptocurrencies have turned out to be those that challenge regulators most. Jurisdictions have to deal with anonymous actors who cannot be connected to any information about the user, although every transaction is listed in the block chain. This means that information such as statistical data, personal information, and transaction processes is hidden from authorities. While traditional regulatory models are applied at intermediaries such as issuers or payment processors, this is impossible with cryptocurrencies because they proceed without intermediaries. This contributes significantly to the problem of how to regulate cryptocurrencies. The FATF guidelines therefore suggest a regulatory system around licensed and registered exchange services (cryptocurrency to fiat money) and money value transfer services. This seems to be the only reasonable solution since it is by now the only approach that allows authorities to intervene and gather user information. Another main component of successful regulation is data transparency. Data collection from any interfaces is necessary, and any data should be available for responsible authorities. This enables cooperation, which is absolutely required.

The examination of the regulatory concept by the FATF shows a clear connection to the risks this thesis demonstrates. The risk-based regulation approach targets exactly those risks. This relation is also reflected in the analysis of the current state of regulation in Europe and the US. Several laws include cryptocurrencies in anti-money laundering and anti-terrorist finance directives. The examples show that pioneer countries, if open to cryptocurrencies, are for the most part following the guidelines. However, one of the greatest difficulties identified is transnationality. All regulatory approaches rely on international cooperation between jurisdictions; otherwise, users could simply avoid regulated exchanges or money value service providers if other countries still allow unsupervised services and/or do not regulate at all.

In conclusion, it must be noted that new cryptocurrencies like bitcoin have lots of technical potential for the financial world. This potential is accompanied by major risks for financial integrity, which need to be targeted intensively as soon as possible. This thesis

demonstrates that regulators are well aware of and on a promising path to control these risks. If regulatory approaches are implemented with international coherence, the chances of success are good. Even if criminals find new ways to technically avoid even well-organised regulation structures, the illegal use will at least be reduced and more difficult for criminals to execute. Whether or not cryptocurrencies will continue to assert their position in society is highly questionable. Latest tendencies of the price developments speak rather against it (blockchain.com, 2019), and everyday use remains a rarity. In conclusion, cryptocurrencies should be regarded as volatile assets and a highly speculative sector in which investments should be well thought out.

8 References

Anderegg, R., 2007. *Grundzüge der Geldtheorie und Geldpolitik.* München: Oldenbourg Wissenschaftsverlag GmbH.

Austin, S., 2018. United States. In: M. Sackhein & N. Howell, eds. *The Virtual Currency Regulation Review.* London: Law Business Research Ltd, pp. 330-380.

BaFin, 2016. *Virtuelle Währungen/Virtual Currency (VC).* [Online]
Available at:
https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html
[Accessed 23 March 2019].

Bank for International Settlements, 2015. *Digital Currencies.* [Online]
Available at: https://www.bis.org/cpmi/publ/d137.pdf
[Accessed 20 March 2019].

Berberich, M. & Wohlfarth, T., 2018. Germany. In: T. Barnes, ed. *The Virtual Currency Regulation Review.* London: Law Business Research Ltd, pp. 118-136.

Berentsen, A. & Schär, F., 2017. *Bitcoin, Blockchain und Kryptoassets - Eine umfassende Einführung.* Norderstedt: BoD - Books on Demand.

Berentsen, A. & Schär, F., 2018. A Short Introduction to the World of Cryptocurrencies. *Federal Reserve Bank of St. Louis Review,*, 10 January, Issue 100 No.1, pp. 1-16.

Berentsen, A. & Schär, F., 2018. The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies. *Federal Reserve Bank of St. Louis Review*, 16 April, pp. 97-106.

bitcoin.org, 2018. *Download Bitcoin Core.* [Online]
Available at: https://bitcoin.org/de/download
[Accessed 28 February 2019].

bitcoin.org, n.d. (a). *FAQ Bitcoin - Allgemein.* [Online]
Available at: https://bitcoin.org/de/faq#allgemein
[Accessed 20 February 2019].

bitcoin.org, n.d. (b). *FAQ Bitcoin - Mining.* [Online]
Available at: https://bitcoin.org/de/faq#mining
[Accessed 26 February 2019].

blockchain.com, 2019. *Average USD market price across major bitcoin exchanges..* [Online] Available at: https://www.blockchain.com/explorer
[Accessed 22 February 2019].

Brening , C., Accorsi, R. & Müller, G., 2015. Economics of Cryptocurrency Backed ML. In: *Twenty-Third European Conference on Information Systems (ECIS).* Münster: s.n.

Bryans, D., 2014. Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal: Vol. 89 : Iss. 1 , Article 13*.

Bunjaku, F., Gjorgieva-Trajkovska, O. & Miteva-Kacarski, E., 2017. CRYPTOCURRENCIES – ADVANTAGES AND DISADVANTAGES. *Journal of Economics*, 5 December, Issue Vol 2, pp. 31-39.

Chohan, U. W., 2017. *A History of Bitcoin.* [Online]
Available at: https://ssrn.com/abstract=3047875
[Accessed 22 February 2019].

CipherTrace, 2018. *Cryptocurrency Anti-Money Laundering Report.* [Online]
Available at: https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf
[Accessed 16 March 2019].

CoinMarketCap, 2019. *Bitcoin market capitalisation.* [Online]
Available at: https://coinmarketcap.com/de/currencies/bitcoin/
[Accessed 3 March 2019].

de Vries, A., 2018. *ScienceDirect - Bitcoin's Growing Energy Problem.* [Online]
Available at: https://doi.org/10.1016/j.joule.2018.04.016
[Accessed 26 February 2019].

Demirguc-Kunt, A. et al., 2018. *Global Findex Database 2017 - Measuring Financial Inclusion and the Fintech Revolution,* Washington: World Bank.

Deutsche Bundesbank, 2018. *Auswirkungen virtueller Währungen auf die Finanzmärkte.* [Online]
Available at: https://www.bundesbank.de/de/presse/reden/auswirkungen-virtueller-waehrungen-auf-die-finanzmaerkte-711074#tar-8
[Accessed 25 March 2019].

Europäische Zentralbank, 2016. *Pressemitteilung - EZB stellt Produktion und Ausgabe der 500-€-Banknote ein.* [Online]
Available at: https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.de.html
[Accessed 17 February 2019].

European Banking Authority, 2014. *EBA Opinion on 'virtual currencies'.* [Online]
Available at: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf
[Accessed 20 February 2019].

European Parliament, Council of the EU, 2018. *DIRECTIVE (EU) 2018/843.* [Online]
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843
[Accessed 23 March 2019].

European Parliament, 2018. *Virtual currencies and terrorist financing: assessing the risks and evaluating responses.* [Online]
Available at:
http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf
[Accessed 16 March 2019].

Fanusie, Y., 2016. *The New Frontier in Terror Fundraising: Bitcoin.* [Online]
Available at: https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin
[Accessed 18 March 2019].

FATF, 2014. *Virtual Currency - Key Definitions and Potential AML/CFT Risks*, Paris: FATF. [Online] Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf [Accessed 20 February 2019].

FATF, 2015. *Guidance for a Risk-Based Approach to Virtual Currencies.* [Online]
Available at: http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html
[Accessed 28 March 2019].

FATF, 2018. *FATF Report - Professional Money Laundering.* [Online]
Available at: http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf
[Accessed 12 March 2019].

FATF, 2019. *Regulation of virtual assets.* [Online]
Available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html
[Accessed 22 March 2019].

FATF, n.d. *Money Laundering.* [Online]
Available at: http://www.fatf-gafi.org/faq/moneylaundering/
[Accessed 10 March 2019].

He, D. et al., 2018. *Virtual Currencies and Beyond : Initial Considerations - IMF Staff Discussion Notes 16/3.* [Online]
Available at: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Virtual-Currencies-and-Beyond-Initial-Considerations-43618
[Accessed 5 March 2019].

Hileman, G. & Rauchs, M., 2017. *Global Cryptocurrency Benchmark Study.* [Online]
Available at:
https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf
[Accessed 26 February 2019].

insurelab, 2017. *Peer-to-Peer: Wie funktioniert Teilen in der Versicherungswirtschaft?.* [Online]
Available at: http://insurelab.de/peer-to-peer-wie-funktioniert-teilen-in-der-versicherungswirtschaft/
[Accessed 21 November 2018].

Jevons, W. S., 1876. *Money and the Mechanism of Exchange.* New York: D.Appleton and Co. [Online] Available at: http://lf-oll.s3.amazonaws.com/titles/318/0191_Bk.pdf
[Accessed 17 February 2019].

Jordan, E. et al., 2017. *Risks and Vulnerabilities of Virtual Currency - Cryptocurrency as Payment Method.* [Online]
Available at: https://www.dni.gov/files/PE/Documents/9---2017-AEP_Risks-and-Vulnerabilities-of-Virtual-Currency.pdf
[Accessed 9 March 2019].

Kiel Institute for the World Economy, 2018. *Virtual Currencies - Monetary Dialogue July 2018.* [Online]
Available at: https://docplayer.net/82389137-In-depth-analysis-requested-by-the-econ-committee-virtual-currencies-monetary-dialogue-july-2018.html
[Accesed 3 March 2019].

Kirsch, S., 2018. *Bitcoin ist nicht die Währung der Zukunft.* [Online]
Available at: https://www.wiwo.de/finanzen/geldanlage/invest-2018-bitcoin-ist-nicht-die-waehrung-der-zukunft/21179298.html
[Accessed 4 March 2019].

La Monica, P. R., 2018. *Bitcoin is down 66%. But it still may be the future of money.* [Online]
Available at: https://money.cnn.com/2018/07/10/investing/bitcoin-prices-bubble/index.html
[Accessed 4 March 2019].

Laszlo, 2010. *Pizza for bitcoins.* [Online]
Available at: https://bitcointalk.org/index.php?topic=137.0
[Accessed 22 February 2019].

Mangan, D., 2018. *New York woman pleads guilty to using bitcoin to launder money for terror group ISIS.* [Online]
Available at: https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html
[Accessed 18 March 2019].

Mansfield, I., 2018. *Bitcoin Fraud – What is it and How Do I Protect it from Fraud?.* [Online]
Available at: https://www.applegrowth.com/bitcoin-fraud/
[Accessed 20 March 2019].

McLeay, M., Radia, A. & Thomas, R., 2014. Money in the Modern Economy: An Introduction. *Bank of England Quarterly Bulletin 2014 Q1*, 14 March, pp. 4-13.

Meisner, H., 2018. Bitcoin als Herausforderung in der Finanzsphäre. In: J. Lempp, T. Pitz & J. Sickmann, eds. *Die Zukunft des Bargelds.* Wiesbaden: Springer Gabler, pp. 89-102.

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* [Online]
Available at: https://bitcoin.org/bitcoin.pdf
[Accessed 20 February 2019].

NCA, 2018. *National Strategic Assessment of Serious and Organised Crime.* [Online]
Available at: http://www.nationalcrimeagency.gov.uk/publications/905-national-strategic-assessment-for-soc-2018/file
[Accessed 15 March 2019].

Rabin, A. A., 2004. *Monetary Theory.* Cheltenham, UK: Edward Elgar Publishing Limited.

Read, O. & Gräslund, K., 2018. EU-Regulierung von Bitcoin und anderen virtuellen Währungen: erste Schritte. *Wirtschaftsdienst*, 98(7), pp. 504-511.

Reiff, N., 2017. *Japan Finally Recognizes Bitcoin After Long Battle.* [Online]
Available at: https://www.investopedia.com/news/japan-finally-recognizes-bitcoin-after-long-battle/
[Accessed 7 March 2019].

Resendiz, J., 2018. *Credit Card Usage and Ownership Statistics.* [Online]
Available at: https://www.valuepenguin.com/credit-cards/statistics/usage-and-ownership
[Accessed 5 March 2019].

Rosenberger, P., 2018. *Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik.* Münster: Springer-Verlag GmbH Deutschland.

RUSI, 2017. *Virtual Currencies and Financial Crime - Challenges and Opportunities.* [Online]
Available at:
https://rusi.org/sites/default/files/rusi_op_virtual_currencies_and_financial_crime.pdf
[Accessed 14 March 2019].

Sackheim, M. & Howell, N., 2018. *The Virtual Currency Regulation Review.* London: Law Business Research Ltd.

Scheau, M. C. & Pop Zaharie, S., 2017. Methods of Laundering Money resulted from Cyber-Crime. *Economic Computation & Economic Cybernetics Studies & Research*, Issue 3/2017, Vol. 51, pp. 299-314.

Seitz, S., 2017. Blockchain – genial und revolutionär. *die bank - Zeitschrift für Bankpolitik und Praxis*, 24 January, Issue 01/2017, pp. 54-59.

Sixt, E., 2017. *Bitcoins und andere dezentrale Transaktionssysteme.* Wiesbaden: Springer Gabler.

Sykes, E., 1911. *Banking and currency.* Fourth Edition ed. London: Butterworth. [Online] Available at: https://dds.crl.edu/item/233613 [Accessed 17 February 2019].

Thomson Reuters, 2017. *A World of Cryptocurrencies.* [Online]
Available at: https://blogs.thomsonreuters.com/answerson/wp-content/uploads/sites/3/2017/10/World-of-Cryptocurrencies-graphic.pdf
[Zugriff am 3 March 2019].

Troeller, L., 2016. Bitcoin and Money Laundering. *Review of Banking & Financial Law*, Issue 1, pp. 159-174.

UNODC, 2011. *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes.* [Online]
Available at: http://www.unodc.org/documents/data-and-

analysis/Studies/Illicit_financial_flows_2011_web.pdf
[Accessed 10 March 2019].

UNODC, 2015. *US v Liberty Reserve et al.*. [Online]
Available at: https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2014/us_v_liberty_reserve_et_al..html
[Accessed 15 March 2019].

Wendt, A., 2018. *Führt der Bitcoin-Hype zu einer neuen Finanzkrise?*. [Online]
Available at: https://www.focus.de/finanzen/boerse/kryptowaehrungen/wirtschaft-fuehrt-der-bitcoin-hype-zu-einer-neuen-finanzkrise_id_8364721.html
[Accessed 4 March 2019].

Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

May 10, 2019 

....

Date Signature