UNIVERSITY OF LJUBLJANA
SCHOOL OF ECONOMICS AND BUSINESS

MASTER'S THESIS

AN ANALYSIS OF CRYPTOCURRENCIES FROM A MONETARY POLICY PERSPECTIVE

Ljubljana, December 2020

BENJAMIN ZAJC

AUTHORSHIP STATEMENT

The undersigned Benjamin Zajc, a student at the University of Ljubljana, School of Economics and Business, (hereafter: SEB LU), author of this written final work of studies with the title An analysis of cryptocurrencies from monetary policy perspective, prepared under supervision of Vasja Rant PhD

D E C L A R E

1. this written final work of studies to be based on the results of my own research;
2. the printed form of this written final work of studies to be identical to its electronic form;
3. the text of this written final work of studies to be language-edited and technically in adherence with the SEB LU's Technical Guidelines for Written Works, which means that I cited and / or quoted works and opinions of other authors in this written final work of studies in accordance with the SEB LU's Technical Guidelines for Written Works;
4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offence and can be prosecuted in accordance with the Criminal Code of the Republic of Slovenia;
5. to be aware of the consequences a proven plagiarism charge based on the this written final work could have for my status at the SEB LU in accordance with the relevant SEB LU Rules;
6. to have obtained all the necessary permits to use the data and works of other authors which are (in written or graphical form) referred to in this written final work of studies and to have clearly marked them;
7. to have acted in accordance with ethical principles during the preparation of this written final work of studies and to have, where necessary, obtained permission of the Ethics Committee;
8. my consent to use the electronic form of this written final work of studies for the detection of content similarity with other written works, using similarity detection software that is connected with the SEB LU Study Information System;
9. to transfer to the University of Ljubljana free of charge, non-exclusively, geographically and time-wise unlimited the right of saving this written final work of studies in the electronic form, the right of its reproduction, as well as the right of making this written final work of studies available to the public on the World Wide Web via the Repository of the University of Ljubljana;
10. my consent to publication of my personal data that are included in this written final work of studies and in this declaration, when this written final work of studies is published.

Ljubljana, December 31th 2020 Author's signature: _________________________

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AML	anti-money laundering
BIS	Bank for International Settlements
BoE	Bank of England
CBDC	central bank digital currency
DCEP	Digital Currency Electronic Payment is a CBDC issued by the People's Bank of China
DLT	distributed ledger technology
ECB	European Central Bank
ECDSA	Elliptic Curve Digital Signature Algorithm
EONIA	euro overnight index average
EU	European Union
FED	Federal Reserve
FTOs	fine-tuning operations
GDP	gross domestic product
GSM	Global System for Mobile Communications
IT	information technology
KYC	know-your-customer
LTROs	longer-term refinancing operations
MPC	Monetary Policy Committee
MROs	main refinancing operations
PBoC	People's Bank of China
PIN	personal identification number
RTGS	real-time gross settlement
SEPA	Single Euro Payments Area
TDNS	time-designated net system

USA	United States of America
USD	United States dollar
USSD	Unstructured Supplementary Service Data
XRP	Ripple currency
ZLB	zero lower bound

INTRODUCTION

Cryptocurrencies still represent only a small fraction of the value of fiat currencies in circulation in 2020. According to CoinMarketCap (n.d. b), cryptocurrencies in a combined value of 393 billion USD circulate over the globe. For comparison, the Board of Governors of the Federal Reserve System (n.d.) states that the value of the broad M2 money supply stands at over 18 trillion USD. Cryptocurrency adoption follows a pattern different to the adoption pattern of fiat currencies. Whereas governments can prescribe a fiat currency as the legal tender in a particular jurisdiction, a cryptocurrency's user base grows organically. Cryptocurrency adoption grows with the successful competition of cryptocurrencies with other forms of money.

Fiat money is issued by the central banks at their own discretion. By using this discretion, central banks pursue monetary policy goals. To achieve them, central banks adjust the money supply to the economic and financial conditions. On the other hand, there is no central authority controlling the issuance of cryptocurrencies. Instead, the pace of issuance is predetermined by the programming of the cryptocurrency, which makes their supply unable to react to the economic and financial conditions.

Cryptocurrencies can act as a medium of exchange for their users. Many less risk averse users also hold cryptocurrencies as investment, which could imply a store of value function (at a future point). Cryptocurrencies may even work as a unit of account in some specific cases. A distributed ledger technology called blockchain is used for record-keeping by cryptocurrencies. This technology enables cryptocurrencies to perform transactions without intermediaries and without a central authority. The technology is still evolving and could in the future bring additional efficiencies to the benefit of cryptocurrencies. However, not all cryptocurrency developments will come from technological improvement. Growth in the adoption and the maturing of the cryptocurrency landscape could also change the way cryptocurrencies perform the functions of money.

Further adoption and use of cryptocurrencies could, therefore, represent a challenge to monetary policy implementation in the future. In 2012, the European Central Bank (ECB) published a report titled Virtual currency schemes. In the report, the ECB identified three sources of risk to its main monetary policy goal that could emerge from different virtual currency schemes, including Bitcoin (ECB, 2012, pp. 33–34). Virtual currency schemes could pose a risk to price stability if (1) they substantially modify the quantity of money, (2) they have an impact on the velocity of money, the use of cash, and/or influence the measurement of monetary aggregates, or (3) there is an interaction between virtual currencies and the real economy. The ECB (2012, p. 47) concludes that virtual currency schemes do not pose a risk for price stability in the present, but there is a need to re-examine and reassess these risks periodically. In the follow-up report, the ECB (2015, p. 26) came to the same conclusion regarding price stability as in the 2012 report. The Bank of England

(BoE) also examined cryptocurrencies and pointed out the problem of their predetermined supply due to the inability to respond to variation in demand, causing welfare-destroying volatility in economic activity (Ali, Barrdear, Clews & Southgate, 2014b, p. 8). Furthermore, the BoE identified a potential risk to monetary stability in the form of the erosion of the ability of the Monetary Policy Committee (MPC) to influence aggregate demand through the transmission mechanism if digital currencies substituted the sterling (Ali et al., 2014b, p. 9). The Bank for International Settlements' (BIS) research showed that the substitution of banknotes for digital currencies would result in the reduction of the central banks' seigniorage revenue and that a significant increase in digital currency adoption could affect the demand for existing monetary aggregates and bank reserves and could, therefore, cause a decline in the efficiency of monetary policy (Committee on Payments and Market Infrastructures, 2015, p. 16).

These and other reports show that monetary authorities and financial regulators are monitoring cryptocurrency developments and that they see them as potentially significant. In 2019, they were taken by surprise with the announcement of Facebook's cryptocurrency project, the Libra, which takes the challenge of virtual currency schemes to a whole new level. As cryptocurrencies enter the realm of social media and the mainstream with potentially far-reaching implications, a closer look at the monetary implications of the cryptocurrency landscape is again warranted. Responses to the cryptocurrency challenge have also been proposed. In the Bank of Canada's Staff Discussion Paper, Engert and Fung (2017, p. ii) examine central bank digital currency (CBDC) as a possible answer to the potential impacts of cryptocurrencies. On the other hand, the deputy governor of the Sveriges Riksbank, Skingsley (2016, p. 1) sees CBDC as a complement for the declining cash use in Sweden. One of the first economists to propose a contemporary form of CBDC, Koning (2014) sees CBDC simply as an improvement upon Bitcoin.

The purpose of this thesis is to show the benefits and risks of cryptocurrencies in comparison with fiat currencies and why it is necessary to explore the effect of cryptocurrencies on the economy. This thesis also aims to explore the cryptocurrencies' effect on the monetary system in order to understand how significantly the adoption of cryptocurrencies and cryptocurrency substitution of fiat could affect the central banks' ability to implement monetary policy. Further, this thesis also aims to explore CBDC as an alternative to cryptocurrencies.

The first objective of the thesis is to analyse the ability of cryptocurrencies to perform the basic functions of money and to substitute fiat money. The second objective is to derive the implications of this substitution for monetary authorities in terms of performing monetary policy, including the development of the central banks' own digital currencies.

Given the purpose and objectives described above, this thesis is focused on answering the following research questions:

Q1: Can cryptocurrencies perform the functions of money better than fiat currency?
Q2: Can cryptocurrencies influence the monetary authorities' ability to conduct monetary policy?
Q3: Can central bank (public) digital currencies be used as an efficient alternative to private cryptocurrencies?

Descriptive methods will be used for describing the properties of cryptocurrencies. At the same time, a comparative method will be used to compare cryptocurrencies and CBDC to fiat money. Furthermore, a theoretical and analytical review of the theoretical sources will be conducted, as well as of the scientific papers from the fields of cryptology, banking, currency substitution, and monetary policy implementation. Finally, an attempt will be made to adapt and apply the reviewed theories to the fields of cryptocurrency and CBDC.

In the first part of the thesis, the properties of cryptocurrencies will be defined, and the comparison between cryptocurrencies and fiat currency will be presented. Next, the broader landscape surrounding cryptocurrencies will be described. In the second part of the thesis, the extent to which cryptocurrencies perform the different functions of money in comparison to fiat currency will be examined. In the third part of the thesis, the cryptocurrencies' effect on the monetary system will be examined. First, the examination of the current monetary system will be provided. Next, the potential implications of the growing cryptocurrency adoption for monetary policy will be predicted. Finally, the proposals for CBDC will be examined and compared to cryptocurrencies and the current fiat system.

1 DEFINING ELEMENTS OF CRYPTOCURRENCIES

According to the Merriam-Webster Dictionary (n.d.), cryptocurrency is "any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions".

The above definition does formally define cryptocurrencies, but it lacks the description of all the implications of the basic properties mentioned in the definition. Cryptocurrencies are also assets that people can transact between themselves without any intermediaries. Cryptocurrencies can be exchanged for fiat currencies or products and services. Cryptocurrency users can manage and store their cryptocurrency balances with the help of electronic devices that are connected to the internet. Cryptocurrencies can be transferred to users and devices regardless of their location. New cryptocurrency units enter circulation through a process called mining. Cryptocurrency units are called coins.

To summarise, the cryptocurrencies' main properties are:

1. they are digital,
2. they are decentralised,
3. they have a predetermined supply, and
4. they are assets and a payment protocol at the same time.

The first property of cryptocurrencies is that they are digital. This means that the data about balances, accounts and transactions is stored in digital form. This data is stored in the form of a database called blockchain. Blockchain is stored on many computers; from servers, personal computers, laptops, smartphones to computers especially dedicated to only storing blockchain data. Since blockchain is stored on many devices, it forms what is called a distributed database. Transactions between accounts can be made and balances can be examined by using an electronic device connected to the internet. There is some distinction between digital and virtual currencies, even though the ECB (2012) called Bitcoin a virtual currency scheme. Virtual tokens used in virtual worlds (e.g. video games) are usually classified as virtual currencies. Cryptocurrencies are usually classified as digital currencies. This is similar to bank deposits in commercial bank accounts that also exist in digital form. In Table 1, we can see that, like virtual currencies, cryptocurrencies are also a subcategory of digital currencies. Also, virtual currencies are, unlike cryptocurrencies, not decentralised and are not based on cryptography. Cryptocurrencies, on the other hand, get their name from the use of cryptography. Cryptography is used in order to secure the ownership of cryptocurrency assets and the workings of the cryptocurrency itself.

Table 1: Money matrix

<table>
<tr><td colspan="3" rowspan="3"></td><td colspan="3">Money format</td></tr>
<tr><td rowspan="2">Physical</td><td colspan="2">Digital</td></tr>
<tr><td>Not based on cryptography</td><td>Based on cryptography</td></tr>
<tr><td rowspan="5">Legal status</td><td rowspan="3">Unregulated</td><td rowspan="2">Centralised</td><td>Coupon</td><td>Internet coupon</td><td rowspan="2"></td></tr>
<tr><td>Local currencies</td><td>Centralised virtual currencies</td></tr>
<tr><td>Decentralised</td><td>Physical commodity money</td><td></td><td>Decentralised cryptocurrencies</td></tr>
<tr><td colspan="2" rowspan="2">Regulated</td><td rowspan="2">Cash</td><td>E-money</td><td rowspan="2">Central bank digital currencies (CBDCs)</td></tr>
<tr><td>Commercial bank money (deposits)</td></tr>
</table>

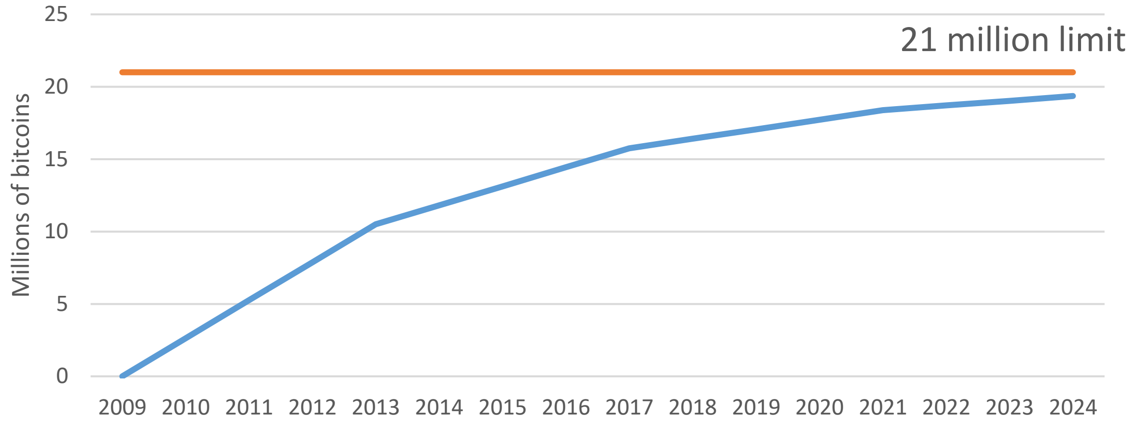
Source: Wikipedia (n.d. b); European Central Bank (2012, p. 11); Martinez (2015); Craig (2015).

The second distinctive property of cryptocurrencies is decentralisation. Besides being decentralised, blockchain data is also distributed. This means that blockchain data is stored on many computers, called nodes, which are distributed all around the world. This makes blockchain the type of database belonging to distributed ledger technology (DLT). Ledger in this context means a database that stores data about balances and transactions. There are two different types of DLT databases. The first type is a permissioned distributed ledger which is managed by a central authority and is, therefore, not decentralised. In a permissioned DLT, the central authority appoints trusted nodes that can store, view and change data in the ledger. The other type of DLT is a permissionless distributed ledger. A permissionless ledger is open to anyone and has no central authority that controls access. The integrity of the data in a permissionless ledger is ensured through cryptography and incentives for its users. Only permissionless ledgers are, therefore, truly decentralised. So far, cryptocurrencies have used the permissionless form of the DLT database.

Cryptocurrencies are not decentralised only in record keeping, but also in transaction processing. The processing of new cryptocurrency transactions is performed by miners through their competition for newly issued cryptocurrency coins. Competition between miners is only possible if mining operations are not centralised. The beneficial consequence of competition between miners is the integrity of new transaction data. Decentralisation, therefore, means that no single authority can control transactions or alter balances. Decentralisation also means that there is no single point of failure from a technical security standpoint.

The third property of cryptocurrencies is that they have a predetermined supply. Fiat currency supply is determined by the monetary authority at its discretion. Cryptocurrency has no central authority that would be able to regulate supply according to its policy. This is why cryptocurrency monetary policy has to be programmed into the cryptocurrency protocol itself. Different cryptocurrencies have different monetary policies incorporated. Most have a deflationary supply that gradually reduces the volume of newly issued coins. For example, the Bitcoin protocol is programmed in such a manner that the number of newly issued bitcoins halves approximately every four years. This event is called halving. As shown in Figure 1, the total number of bitcoins through time is a limit function that approaches 21 million. Other cryptocurrencies, like Ether, do not have halving events and have a linear function of newly issued coins through time.

Figure 1: Predicted Bitcoin supply through time



Source: Bitcoin Wiki (n.d. b).

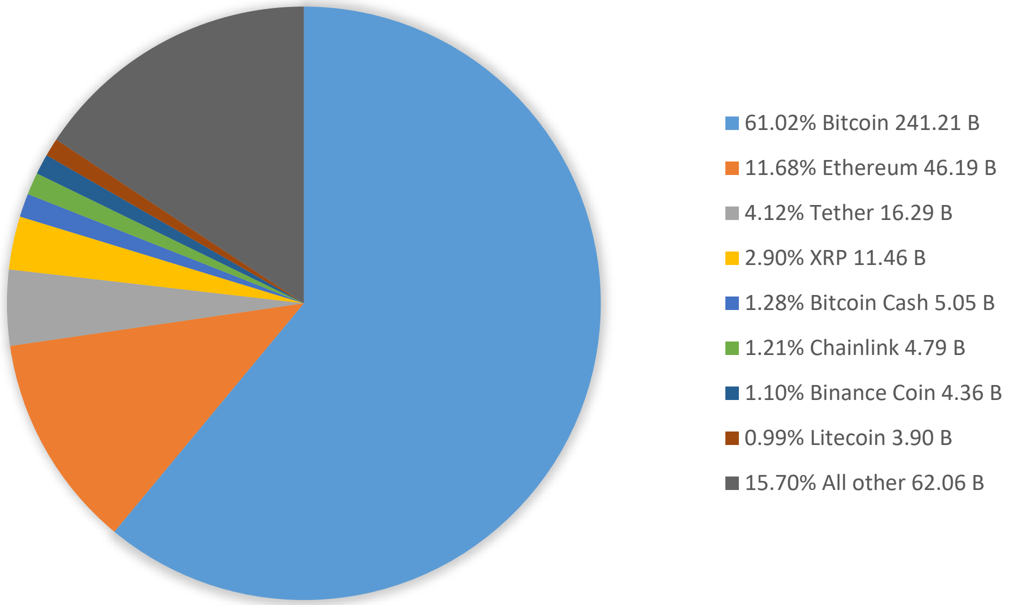
Since cryptocurrencies are digital, there is no intrinsic value in cryptocurrency coins (units). Demand is, therefore, driven by cryptocurrency utility and speculation. The market value on the exchanges is discovered between this demand and the predetermined supply. The newest addition to the cryptocurrency family are stablecoins. Stablecoins are programmed in a way which regulates supply in order to keep the stablecoin exchange rate constant. Stablecoin supply, therefore, reacts to stablecoin demand, but the algorithm that regulates this reaction is predetermined. Stablecoins are cryptocurrency analogues of fiat currency peg regimes. A predetermined supply has another consequence; if cryptocurrencies substituted fiat money, monetary authorities would have to deal with money, over which they do not have control.

The fourth property of cryptocurrencies is their duality of being an asset and a payment protocol at the same time. Cryptocurrency coins are an asset that can be owned, transferred and traded with. On the other hand, cryptocurrency is also a protocol and a network of computers, which enables its users to make transactions without any intermediaries. Because of cryptocurrency duality, there is a need for differentiation between the names for an asset and a protocol. In this thesis, lower case names will be used for coins (e.g. 5 bitcoins) and upper case names for a protocol (e.g. Bitcoin network).

1.1 Cryptocurrency landscape

According to CoinMarketCap (n.d. b), Bitcoin is the biggest cryptocurrency by market capitalisation value out of more than two thousand known cryptocurrencies. As can be seen from Figure 2, Bitcoin market capitalisation represents the majority share of the market capitalisation value of all cryptocurrencies. Bitcoin was also the first cryptocurrency to appear. However, the high number of cryptocurrencies in existence demands a broader look. Bitcoin may be surpassed by another cryptocurrency in the future. New cryptocurrencies with better properties are emerging through innovation. The cryptocurrency field is still in its infancy both from a technical and socio-economic perspective.

Figure 2: Share of different cryptocurrencies in billions of USD, October 2020



Source: CoinMarketCap (n.d. a).

There are several reasons for the proliferation of new cryptocurrencies. One reason is the need for different properties of cryptocurrencies. Another is that it is easier to create new cryptocurrencies than agreeing on the changes to the existing ones. Cryptocurrencies intended for special groups of users and cryptocurrencies intended for use with special services or products are yet another reason to create new cryptocurrencies. Also, many cryptocurrencies were created in order to extract money from naïve investors. The low cost of creating a new cryptocurrency and the low switching cost between cryptocurrencies for users also means that entry barriers are relatively low.

Bitcoin was the first cryptocurrency. Its inventor, Nakamoto (2008, p. 1), states that Bitcoin answers the need for a trustless electronic payment system, which means that Bitcoin enables electronic transactions without a central trusted party. New bitcoins are issued approximately every 10 minutes. Bitcoin's total issuance is limited to 21 million bitcoins. The number of newly issued bitcoins is programmed in such a way that it halves approximately every 4 years and will, therefore, never reach 21 million. Bitcoin has, through the network effect, retained the biggest share in market capitalisation of all cryptocurrencies. It is the most widely used of all cryptocurrencies.

Litecoin was one of the first cryptocurrencies that copied the Bitcoin design. Bitcoin code is open source and, therefore, available for copying. Litecoin showed how easy it is to create another cryptocurrency. At Litecoin's creation, Litecoin and Bitcoin were identical in all but a few properties. According to Litecoin Wiki (n.d.), new litecoins are created approximately every 2.5 minutes and the supply is limited to 84 million. Litecoin is still one of the most used cryptocurrencies.

Dogecoin was a cryptocurrency not much different than Bitcoin. The main difference was the users of both cryptocurrencies. Dogecoin was created as a novelty currency that was not intended for serious use. Because of its fun-oriented and positive community, it was used in charity fundraising and for entertainment. Dogecoin creation also reflected the simplicity of creating new currency.

According to the Ethereum Foundation (n.d. b), Ethereum is a cryptocurrency that is, unlike Bitcoin, programmable. This means that computer developers can use the Ethereum blockchain to build decentralised applications on it. When decentralised applications are uploaded to the blockchain, they will run on the network autonomously. Blockchain and ether are then used as support systems for this application platform. These applications can be cryptocurrency wallets and financial applications for borrowing, lending and investing digital assets. It is also possible to build decentralised markets, games and other kinds of applications on the Ethereum blockchain.

Ethereum Classic is a cryptocurrency that was created when the community around the original Ethereum split over an issue about cryptocurrency governance. It is important because it shows that, with an open-source cryptocurrency, part of a community can democratically choose to pursue its own version of cryptocurrency without being locked in an ecosystem. Ethereum Classic is also an important case study for cryptocurrency value. When the original Ethereum split into new Ethereum and Ethereum Classic, new cryptocurrencies had a very different exchange rate on cryptocurrency exchanges.

Ripple is a currency that is used as the final settlement in a Ripple global settlement protocol. The Ripple global settlement protocol is intended for transactions between financial institutions over the internet. Ripple currency unit (XRP) is meant as a backup when a settlement in all other assets is not possible. Ripple is not a true cryptocurrency in the sense that it is not decentralised and is, to some extent, controlled by a private company – Ripple Labs. Ripple currency is mentioned here because of its significance and its relatively high market share. Because it is not decentralised, it will not be included in the cryptocurrency analysis in the following chapters.

Tether is a relatively new kind of cryptocurrency called stablecoin. Stablecoins are cryptocurrencies that are supposed to have a stable value and are usually pegged to fiat currencies. According to Tether Operations Limited (n.d.), Tether is a blockchain-enabled platform enabling fiat currency use in a digital manner. Tether is meant to provide digital currency experience without the volatility associated with cryptocurrencies. The Tether exchange rate is fixed against the dollar at 1:1. Stablecoins have gained in prominence as a safe asset, especially after the 2018 cryptocurrency market crash.

1.2 Methods of issuance

Any discussion of cryptocurrencies from a monetary policy perspective requires knowing how new cryptocurrency coins enter circulation and why cryptocurrencies have to issue new coins constantly. To understand cryptocurrency issuance, transaction processing and incentives for miners have to be looked at in more detail.

Cryptocurrency transaction processing requires explaining the use of wallets and the public-private key encryption technology. According to Antonopoulos (2015, p. 61), the control of any cryptocurrency account is performed using digital keys. These keys come in pairs of public and private keys. A public key is similar to a bank account number and is sometimes called an address. A private (secret) key is used as a password or PIN in order to provide control over the account and to authorise the transactions made from this account. One or more addresses are stored in a wallet. A wallet is a device that stores both private and public keys. Usually, applications on smartphones or computers are used as wallets since they can interact directly with the blockchain through the internet in order to perform transactions.

To perform a transaction is to send coins from one address (public key) to another. Antonopoulos (2015, p. 18) explains that a transaction announces to the network that the owner of the funds at a particular address is transferring them to another address. In order to send coins from one address to another, the sender has to sign the transaction announcement with a private key and transmit the transaction data to the network. Miners on the network then pick up this transaction data, check the validity of the transaction and pack it in a block with other valid transactions. Afterwards, this block is added to the blockchain. At that time, the coins are effectively transferred from the sender's address to the receiver's address.

Cryptocurrency transaction data is called a blockchain because blocks of transaction data form a chain of transactions. Antonopoulos (2015, p. 159) states that "blockchain data structure is an ordered, back-linked list of blocks of transactions". This means that in order to see how many coins a certain address contains, we have to follow those coins from their issuance through all the past transactions until the present moment. Transactions with valid private key signatures (authorisation) are packed in blocks and added to the blockchain as part of the mining process.

Transactions are processed by miners. Miners compete with each other for a reward that comes in the form of newly issued coins. Every block of transactions that is added to the blockchain also contains an additional transaction that creates newly issued coins. These coins are distributed among miners after they add the transaction block to the blockchain. Bashir (2018, p. 167) explains that mining is a resource-intensive process where miners compete to solve mathematical puzzles. This is done in order to ensure that the required resources have been spent before a new block of transactions can be accepted. The spending of resources secures the system against frauds and double spending attacks. In order to be able to forge transactions, a malicious actor would have to invest more resources into mining than all the other miners at that point. It is necessary to mention that this explanation of the mining process is oversimplified from a technical point of view.

The number of newly issued coins, which will be distributed to miners with every block, is programmed into each cryptocurrency protocol. Since the time in which every new block is added to the blockchain is roughly constant, the issuance of new coins is highly predictable. Bashir (2018, p. 167) reports that a new Bitcoin block is created roughly every 10 minutes. In the beginning of 2020, every Bitcoin block miner reward equalled 12.5 bitcoins. A Bitcoin miner block reward was reduced to half of that in May 2020 and will further be halved approximately every four years. This halving of the reward is encoded into the Bitcoin protocol. Every other cryptocurrency has a predetermined supply, but uses its own parameters of issuance. The downside of predetermined issuance is that it cannot be used to respond to fluctuation in a macroeconomic environment. This also means that a monetary authority cannot have control over cryptocurrency supply.

1.3 Cryptocurrency use

Tasca, Liu and Hayes (2016, p. 2) analysed Bitcoin blockchain transactions from 2009 to 2015 and were able to allocate many of the transactions to specific business categories, namely exchange, mining pools, online gambling, black markets, or composite. The transactions done with specific business categories help us conclude what Bitcoin was used for at that time. Since Bitcoin is the biggest cryptocurrency by market capitalisation, we can extrapolate its use to other cryptocurrencies.

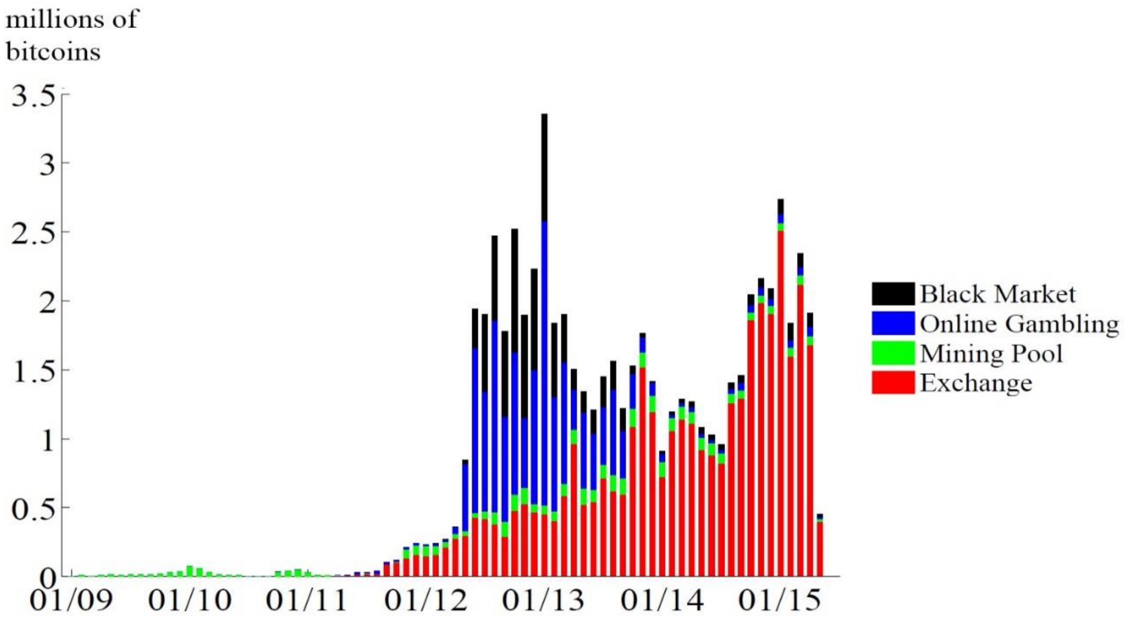
The most widespread use of cryptocurrencies is as an investment vehicle. The high volatility of cryptocurrency exchange rates makes them interesting for speculation. Interest rates in the economy have been relatively low since the start of the quantitative easing programmes. This is why investors search for alternative investment opportunities. The low trading cost and the accessibility of online exchanges attracted many private investors who do not have access to the stock market.

Many transactions were made by miners. They receive the newly mined coins and sell them on exchanges in order to cover their costs. Miners join their resources into pools to smooth out their income over time. On the one hand, mining is a necessary part of processing transactions, but on the other hand, mining is also a part of the cryptocurrency economy since they sell most of their mining rewards.

One of the first successful uses of cryptocurrency was online gambling. Since gambling is usually highly regulated, cryptocurrencies were used for transactions in illegal online gambling. Cryptocurrency transactions are public and can be seen on the blockchain, but the owners of the addresses are usually not known. This partial privacy was used in order to hide the profits made by illegal online gambling operators from tax authorities.

Online trade is another use for cryptocurrencies. The first adopters of cryptocurrencies for trading were marketplaces for illegal products and services on the dark web. The dark web is a part of the internet that is not accessible through regular means. Illegal marketplaces mostly use Tor anonymising technology in order to hide servers on which their webpages are hosted. A cryptocurrency's partial anonymity is complementary to their clandestine operation. Products offered on these marketplaces range from illegal drugs, prescription drugs, weapons, stolen credit card numbers as well as services like money laundering, but also legal products and services. Nowadays, it is possible to buy many legal products and services from different stores on the internet with cryptocurrencies. A cryptocurrency payment option in brick and mortar stores is still very rare.

Figure 3: Bitcoin income by category in millions of bitcoins



Source: Tasca et al. (2016, p. 34).

The most common uses of cryptocurrencies from 2009 to 2015 are shown in Figure 3. Tasca et al. (2016, pp. 34–36) identify three periods with distinguishable regimes in cryptocurrency use. From January 2009 through March 2012, transactions were conducted for testing and mining. There was barely any value associated with Bitcoin in the beginning. Value was first associated with bitcoins when they started trading on exchanges. According to Sedgwick (2018), the first exchange called Bitcoinmarket.com launched in March 2010. Caffyn (2014) reports that the first purchase with bitcoins was done on May 22, 2010, when Laszlo Hanyecz paid 10,000 bitcoins in exchange for two pizzas.

In the period from April 2012 through October 2013, gambling and illegal marketplaces dominated transaction activities, however, a growing trend of transactions from and to exchanges could also be seen. This trend is especially impressive since these income values are denominated in bitcoins. The bitcoin exchange rate and its real value have grown from nothing to more than 1000 USD for one bitcoin in the period shown in the figure.

Since November 2013, exchanges have assumed a central role in transaction activity. Exchanges are used for investing and speculation with cryptocurrencies as well as the exchange between fiat and cryptocurrency for legal and illegal trade. Black market and illegal gambling income transactions did not grow too much in real terms from late 2013 to 2015, but neither did they disappear. In Figure 3, we can also see that the income of miners stayed the same. This is expected in a cryptocurrency that has predetermined issuance. Figure 3 also only shows transactions researchers were able to attribute to one of four categories. Bitcoin income data is only available up to May 2015. This is the consequence of cryptocurrencies being decentralised. This means that any analysis of cryptocurrency use or its users is done by looking and examining every individual address and further searching information and connections about it.

Further cryptocurrency usage can only be speculated about based on anecdotal evidence. The continuation of the trend of using cryptocurrency exchanges in order to speculate about the further value of cryptocurrencies can be confirmed as long as cryptocurrencies go through boom and bust cycles. Diminishing volatility could be an indicator of a shift from speculation to using cryptocurrencies as a medium of exchange. Higher cryptocurrency exchange rates can also be explained by higher demand or even higher use.

1.4 Trust and security issues

Trust in money is fundamentally dependent on its technical safety and on the governance of the monetary system. If balances on bank accounts or in wallets were not safe, no one would use them for storing money. Trust in a currency also derives from currency governance, which encompasses regulation, monetary policy as well as stakeholders' actions.

In technical terms, cryptocurrencies are safeguarded by cryptography and decentralisation. Public and private key cryptography is used in order to control access to addresses and balances stored on them. Only the party possessing the correct private key can make transactions from a specific address. This means that users have to take care of their private keys in order to safeguard their coins. According to Böhme, Christin, Edelman and Moore (2015, p. 216), public and private key cryptography is widely used and is, therefore, a tried and trusted method of securing access. The decentralisation of mining ensures that miners compete with each other for mining rewards. When competing with one another, they also make sure to only process transactions that use the correct private keys. Decentralisation in record keeping is achieved through many copies of the blockchain, which ensures the integrity of the transaction data and, therefore, the integrity of the balances.

Even though cryptocurrency technology ensures the safety of balances, users still rightfully worry over security issues. A particular concern about safety arises from the fact that using some services, vital for the cryptocurrency economy, requires depositing cryptocurrency coins. Most cryptocurrency exchanges, online gambling and online marketplaces require their users to deposit cryptocurrency funds. Depositing cryptocurrencies means losing direct control over them. This is similar to when we deposit fiat money. The distinction between cryptocurrency and fiat deposits is that fiat deposit-taking institutions are highly regulated. On the other side, there is almost no regulation in place for cryptocurrency deposits at the moment. Cryptocurrency depositors can, therefore, be victims of the institutions that take their cryptocurrency deposits. This happens either because deposit-taking institutions steal the cryptocurrency for themselves or they themselves have been victims of theft by hackers, or just because of the underperformance of the deposit-taking institution. And because there is no cryptocurrency deposit insurance, the deposits can be lost in such cases. In the past, big cryptocurrency exchanges had their funds stolen. This caused distrust not only in a specific exchange, but also in the whole cryptocurrency ecosystem.

There is an important assumption about the technological safety of cryptocurrencies. It is assumed that miners are decentralised and that no miner represents more than half of the network in computing power. If any miner has more than half of the computing power of the network, that miner can spend the same cryptocurrency coins multiple times. This should not happen in normal circumstances because controlling more than half of the network's computing power is expensive and because miners generally do not want users to lose trust in the cryptocurrency they mine. Making double-spend transactions in such a way is called a 51% attack. According to Palmer (2020), a 51% attack did happen to the Bitcoin Gold cryptocurrency that had a relatively low network computing power at that moment. This is when a miner from outside entered and was able to make double-spend transactions.

The governance of a central monetary authority can greatly affect the trust in fiat currency. A central bank must perform a credible monetary policy in order to maintain trust. Regulation needs to safeguard the ownership of balances and provide for the smooth workings of the monetary system. Cryptocurrencies have their monetary policy and regulation encoded into the software code. Adherence to the code is ensured by the network that checks every transaction before it is added to the blockchain. Security and trust are, therefore, maintained by everyone adhering to the same protocol. This also means there are no permissions necessary to join the network as long as the rules of the protocol are adhered to.

Trust in the cryptocurrency also derives from the cryptocurrency community which consists of users, miners, code developers and other stakeholders. The community, especially developers with their past record and plans for the future cryptocurrency project credibility, can, therefore, make a cryptocurrency more or less trusted. The community can also express a lack of trust in a cryptocurrency by voting with their feet. If users lose confidence in a particular cryptocurrency, they will sell it and then use another one. Since the network effect is present in cryptocurrencies, any loss in the number of users can have a big effect on cryptocurrency utility and value. Any disagreement over the governance of the cryptocurrency code can also lead to a split of the blockchain. If the blockchain splits, we get two different cryptocurrencies and two communities. Each different cryptocurrency after a split is called a fork. A split usually also means a split in the user base and two smaller networks with a smaller network effect and a smaller value. This is why splits in cryptocurrency governance are extremely undesired.

Cryptocurrency transactions cannot be reversed after a few blocks are added to the blockchain. This makes transactions final in practice and removes any chargeback option that exists when transacting with fiat. Cryptocurrency transaction finality is probabilistic and not deterministic. This means that after a few blocks have passed, there is a very high degree of probability that the transaction encoded in the blockchain will always be valid. The additional time needed to make transactions final also represents a cost for cryptocurrency transactions. A reversal of a transaction is only possible if the original receiver of the transaction sends the funds back by making a new transaction. There was an exception to transaction finality on the Ethereum blockchain in the summer of 2016. An error in the code made a cryptocurrency amount worth 150 million USD available to a hacker. The hacker then transacted them into his or her own address. The majority of Ethereum stakeholders then voted to reverse that transaction. A minority of Ethereum stakeholders did not agree with that decision because they saw the blockchain as something that should be immutable. That is why the Ethereum blockchain split into two cryptocurrencies; Ethereum, which reversed the transaction in question, and Ethereum Classic, which let the transaction as it was (Hertig, 2016).

1.5 Summing up cryptocurrencies

Cryptocurrencies are digital and decentralised currencies that have their supply predetermined. While they share some characteristics with fiat currencies, they are in many ways different.

From a monetary policy point of view, a predetermined supply is the interesting property of cryptocurrencies since it is fundamentally different to fiat currency issuance. Most of the orthodox macroeconomics argue that money supply should be adjusted to the macroeconomic conditions, but cryptocurrencies use a predetermined supply as a technological condition for decentralisation.

Decentralised technology enables cryptocurrency protocol to work without legal contracts between users. Users only have to safeguard their private keys. However, cryptocurrency protocol does not provide sufficient safety for services where users have to deposit their coins. In practice, the theft of cryptocurrency coins is a relevant security threat. This is why regulation is needed to protect users when they deposit coins. Regulation is also needed in order to prevent illegal activities, terrorism and money laundering. Cryptocurrency adoption is dependent on balanced regulation. The legal status of cryptocurrencies will be determined by trial and error of the legislative process as it had been for fiat currencies in the past. Cryptocurrency trading, online gambling and selling illegal products and services were the most common uses of cryptocurrency up to this point. Cryptocurrency use has changed through the first eleven years of its existence. It is reasonable to conclude that it will also change in the future.

All this means that there is a benefit in analysing whether and how well cryptocurrencies can perform the functions of money.

2 COMPARISON OF CRYPTOCURRENCIES VS. FIAT CURRENCIES AS MONEY

People use money because it brings them utility when used for buying or selling goods, transfering purchasing power through time, and measuring the value of other goods. These are the most common uses underlying the three basic functions of money: medium of exchange, store of value and unit of account.

Jevons (1896, p. 31) further states that certain properties of money are important: utility and value, portability, indestructability, homogeneity, divisibility, stability of value, and cognisability.

Whereas money in the time of Jevons was certainty different from the current fiat money and cryptocurrencies, any money needs to perform the same basic functions. The examination of cryptocurrencies from a monetary policy perspective, therefore, first needs to have a look at how well cryptocurrencies perform the functions of money relative to fiat money.

2.1 Comparative performance of the medium of exchange function

Mishkin (2009, p. 54) states that medium of exchange is the function that distinguishes money from other assets. The performance of the medium of exchange function leans on the ability of an asset to lower transacting costs in an exchange. In a potential society with no money and no way to record debt, traders have to overcome a double coincidence of wants by searching for someone who has the goods or services that the trader wants, and will, at the same time, accept the goods or services the trader has to offer. This search can be very costly (Mishkin, 2009, pp. 54, 55).

Jevons (1896, pp. 32, 33) also states that money has to have utility and intrinsic value in order for people to be induced to receive it and pass it on freely at steady ratios of exchange for other objects. Nowadays, we use money without intrinsic value, but money still brings utility to its users. The point is that people have to be induced to receive money. This means that money has to be in demand and, therefore, accepted. Also, Menger (2009, p. 35, 36) already notes that the commodity which possesses superior saleableness relative to other commodities becomes a generally acceptable medium of exchange. Saleableness in Menger’s context means that there is demand for it. A good medium of exchange, therefore, has to be widely accepted. If everyone accepts their own type of specific asset as money, exchange would not be any more efficient than in a barter exchange. If more people accept and use the same medium of exchange, they lower the potential cost of exchange.

Jevons (1896, pp. 34, 35) also notes that a good medium of exchange has to be carried or transferred easily because this leads to lower transaction costs. In today's world of electronic money, transaction costs mostly depend on the efficiency of payment systems. On the other hand, the costs associated with physically moving money depend on the physical properties of money, security concerns, etc. The speed of the transaction also affects costs. The longer the transaction takes, the bigger the opportunity cost of the funds that are not available during the transaction.

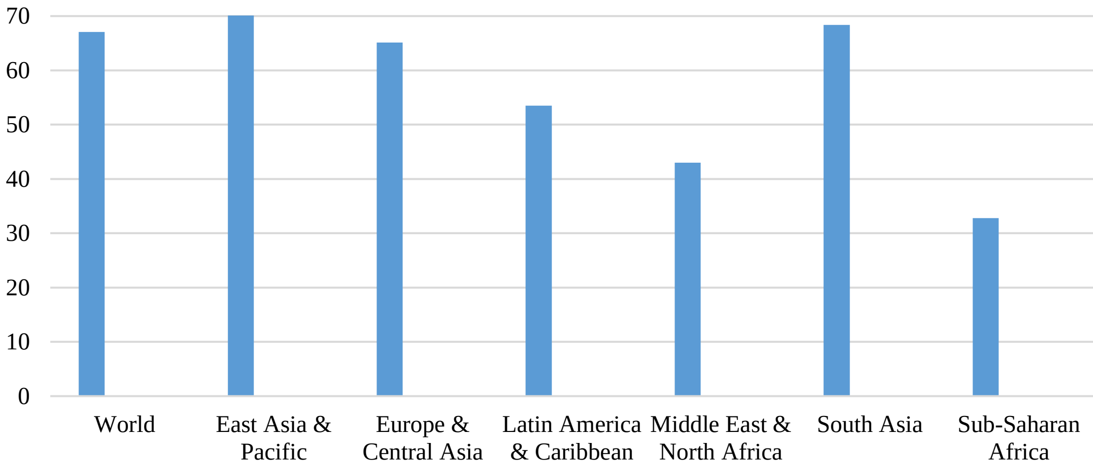
Acceptance is a precondition for the use of an asset as a medium of exchange. If this condition is fulfilled, the medium of exchange can perform its function of lowering transaction costs in an exchange. Fiat and cryptocurrencies will, therefore, be evaluated as media of exchange by comparing their acceptance and their ability to lower transaction costs and their speed of transactions.

2.1.1 Fiat currencies as a medium of exchange

Fiat money is typically enforced as a legal tender by the state and is usually widely accepted. Money being legal tender means that everyone is required by law to accept it for payments. Legal tender status is limited to the area of a country or a currency union. Some currencies are also used in international trade. According to the Bank for International Settlements (2019, p. 5), 88.3% of the foreign exchange market turnover in April 2019 was in US dollars, 32.3% in euros and 16.8% in Japanese yen. Two currencies are involved in each transaction which is why the sum of shares in individual currencies totals 200%. Foreign exchange turnover does not only tell us about the exchange between currencies, but can also be used as an indicator of currency use in international trade. According to this data, US dollars, euros and Japanese yen are present in more than two thirds of all foreign exchanges. But even these currencies are not generally accepted outside of their native areas, with the exception of countries where the domestic currency is substituted by another currency. According to Quispe-Agnoli (2002, p. 5), currency substitution happens in inflationary situations because of the cost of holding domestic currency. The acceptance of a particular fiat currency is, therefore, very high within the same monetary jurisdiction, but conversion is generally necessary for the use outside of this area.

The acceptance of fiat does not mean that each individual has to accept every payment instrument. For example, some individuals and businesses only accept cash, whereas others only accept electronic fund transfers. Obtaining cash and making cash payments is usually not problematic, even though it still incurs costs, but obtaining a bank account, as a prerequisite for electronic fund transfer, is not always trivial. Obtaining a bank account in developing countries can be so costly (in monetary or other costs) that significant parts of the population do not have one. In Figure 4, the percentages of the population over 15 years old that have an account at a financial institution are presented. We can see that many people, especially in developing countries, do not have access to a bank account and are not able to make electronic transactions.

Figure 4: Percentage of people over 15 with a financial institution account in 2017



Source: World Bank (2018, pp. 2–8).

Since the physical exchange of fiat in the form of cash is only possible in person and is cumbersome for large sums, many transactions are done through payment systems. According to Kokkola (2011, p. 25), any payment system comprises of: a) payment instruments, which are a means that initiate and authorise a payment, b) processing, which includes a bank's internal processing and interbank processing (clearing – exchange of payment information between banks), and c) settlement, which stands for the compensation of funds between involved banks. The most common payment instruments are credit transfers, direct debits, payment cards and, in some countries, cheques (Kokkola, 2011, pp. 31, 32). These payment instruments are different ways for a payer or a payee to inform and authorise a bank to initiate a transaction. Afterwards, the bank checks for sufficient balance on the paying account and prepares the transaction's information for interbank processing or clearing. Kokkola (2011, p. 41) describes the start of the clearing process with the submission of the transaction into the clearing system by the initiating bank. The transaction is then validated and further accepted for processing. After the acceptance, transactions can be matched, sorted, collected and aggregated before finally being sent to the receiving bank. After clearing, both banks proceed to settle the transaction in the order determined by the payment system and the type of transaction.

According to Kokkola (2011, p. 43), a settlement is the act of discharging obligations between two or more parties. In a payment system, this happens when a payer's bank transfers funds to a payee's bank. Banks can choose to perform a settlement with either a net or a gross method and can also choose to perform a settlement in real time or at a designated time.

In a pure real-time gross settlement (RTGS) system, every transaction is settled as it enters the settlement system. The opposite of RTGS is a time-designated net system (TDNS), in which transactions are collected and settled in a net position at a predetermined point in time. The net position is the sum of all the received transactions minus all the sent transactions of a bank. Netting can be done between two banks (bilateral) or between all banks (multilateral) participating in the settlement system. A settlement system can also combine the elements of both variants (Leinonen & Soramaki, 2000, pp. 10, 11).

Most banks do not participate directly in payment systems outside their native country. This is why they need an intermediary to perform cross-border payments. A financial institution in the destination jurisdiction connects them to the local payment system and after the payment reaches the destination country, it also has to pass through the payee's domestic payment system. Besides that, cross-border payment can also involve currency conversions. Cross-border payments are also relatively less formalised than domestic ones. Sometimes cross-border payments even have to pass through multiple such loops of intermediaries and payment systems to reach their final destination. This is why cross-border payments add a complexity beyond the levels seen in domestic clearing and settlement systems (Kokkola, 2011, p. 61).

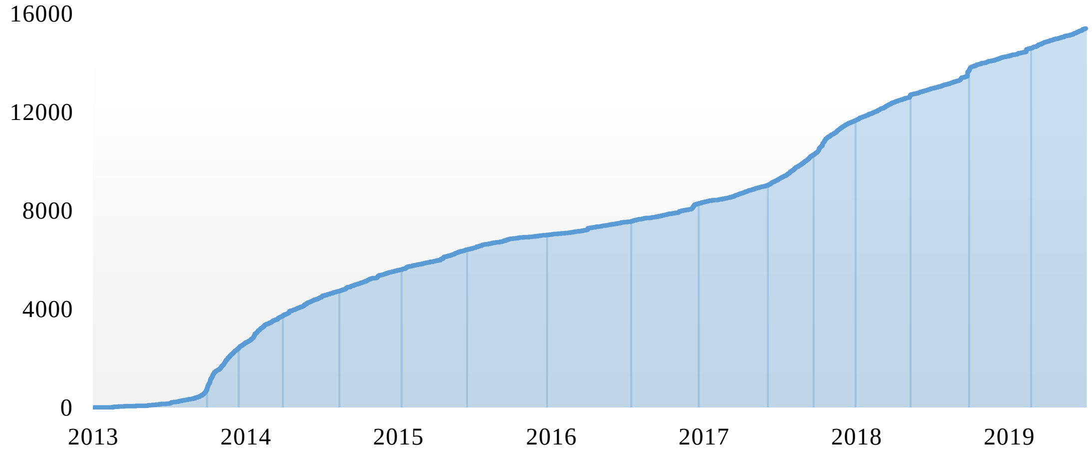
Because of the above-described processes that happens in payment systems, transferring money always incurs costs. The cost of transactions depends on the transaction type and the payment system used. In 2012, Schmiedel, Kostova and Ruttenberg (2012, p. 27) conducted a study of payment instrument costs in 13 EU countries. They examined the total social costs of the different kinds of transactions, reflecting all production costs involved in providing the payment service. The study found that the average social cost per transaction is 0.42€ for a cash payment, 0.70€ for a debit card transaction, 1.27€ for a direct debit transaction, 1.92€ for a credit transfer and 2.39€ for a credit card transaction. These payment costs represent the basis for estimating fiat transaction costs, but they only represent the costs for domestic payments. Cross-border payments are more complex, as described in the previous paragraph, and, therefore, more expensive. For example, the World Bank (2020, p. 2) reports the global average cost of international remittances at 6.79% for 200 USD transactions. Remittances are the transactions of money made by migrants to their home country. Also, McKinsey Financial Services Practice (2016, p. 16) finds that the operational costs per transaction for international payments continue to average well above 20 USD. It follows that the costs are usually proportional with the complexity of the transaction.

From the description of fiat payment systems above, it can be seen that transactions can take different amounts of time to complete. Transaction speed depends on the type of payment system used. The processing and clearing of a transaction is usually relatively fast compared to the settlement. Settlements in RTGS systems happen more or less in real time. On the other hand, it takes longer to process transactions in TDNS and hybrid systems of settlement because the settlement is conducted at a predetermined time and not right away as a transaction is being initiated. According to Kokkola (2011, p. 48), RTGS settlement systems are predominately part of wholesale payment systems used for large value and urgent payments between financial institutions. Users outside the financial sector usually use retail payment systems. Retail payment systems are designed to handle a large volume of relatively low-value payments and usually use TDNS or hybrid settlement systems. Kokkola (2011, p. 52) states that the netting of transactions considerably reduces the liquidity requirements for financial institutions participating in a net settlement system in comparison to a RTGS settlement system. In practice, this means different possible transaction speeds. Hartmann, Hernandez, Plooij and Vandeweyer (2019, pp. 28, 29) note that in the European Union, some countries offer a same-day completion of retail transactions while other credit retail payments take 1-3 business days. Rysman and Schuh (2016, p. 40) also find that payments through the Automated Clearing House payment system in the USA take several days to complete. Payments made with debit or credit cards may seem instant from the point of view of the user, but are, according to Bech and Hancock (2020, p. 25), generally settled on a net basis with a one- or two-day lag. Cross-border payments can take even longer because of their complexity. The Committee on Payments and Market Infrastructures (2018, p. 17) states that some payment service providers taking part in their survey reported a seven-day execution time for some cross-border payments.

2.1.2 Cryptocurrencies as a medium of exchange

The acceptance of cryptocurrencies for payment is at present much lower than the acceptance of fiat money. Cryptocurrencies are not legal tender in any jurisdiction. That means than no one is obliged to accept payment in cryptocurrency. On the other hand, cryptocurrencies are not bound to an area. The acceptance of cryptocurrencies is growing as can be seen in Figure 5 below, which shows the number of businesses accepting bitcoin that were added to the coinmap.org database.

Figure 5: Venues accepting Bitcoin as listed on coinmap.org



Source: OpenDataSoft. (n.d.).

Only a few of the most well-known cryptocurrencies are accepted in exchange as payment. Other cryptocurrencies have value on exchanges and can be converted into one of the accepted cryptocurrencies. That helps with their use, but also burdens users with the additional cost of conversion.

Since cryptocurrencies are still quite a new phenomenon for the general public, the biggest barrier for larger adoption is the lack of knowledge. Until the knowledge about safe and efficient cryptocurrency use becomes more widespread, there are significant costs associated with acquiring the skills necessary for the use of cryptocurrencies. Even though speculation with cryptocurrencies does not have a direct connection with using cryptocurrencies as a medium of exchange, speculators must learn at least the basic principles of cryptocurrency use. In that sense, speculation can be seen as a propagator of the use of cryptocurrency as a medium of exchange and, therefore, lowers the lack of knowledge barrier.

Unlike fiat, each cryptocurrency only uses one payment system. This payment system is incorporated into the cryptocurrency itself and is open to anyone. This means that cryptocurrency transactions are not negatively affected by the complexity that is present in fiat payment systems. Cryptocurrency transactions are processed and settled in real time and in gross terms. In this respect, cryptocurrency is comparable to a RTGS that is open to everyone.

The costs of cryptocurrency transactions vary depending on the demand for transactions and the free processing capacity in a specific cryptocurrency. In 2019, the median daily fee for a Bitcoin transaction was between 0.04 and 3.72 USD, and the median daily fee for an Ethereum transaction was between 0.02 and 0.27 USD (BitInfoCharts, n.d.). When the demand for transactions is higher than the cryptocurrency processing capacity, miners choose to process transactions that offer the biggest fees. In times of the biggest demand for Bitcoin transactions, the median daily fee went up to 34.09 USD on 23 December 2017 (BitInfoCharts, n.d.). Similarly, the median daily Ethereum transaction fee went up to 3.14 USD on 10 January 2018 (BitInfoCharts, n.d.). Such high fees were a consequence of the fact that in the beginning, cryptocurrencies were not designed with a high capacity of transactions in mind. This could act as a serious bottleneck to the scalability of cryptocurrencies in the case of higher adoption. More on transaction capacity and the scalability of cryptocurrencies will be presented in the following chapters.

It could be said that cryptocurrencies process transactions in real time, but the processing still takes a certain amount of time. When cryptocurrency transactions are initiated, they are gathered into a pool of transactions that get processed and added to a new blockchain block together. This means that every transaction must wait until the next new block. Different cryptocurrencies add new blocks to their blockchain at different rates. For example, the Bitcoin protocol ads a new block to the blockchain approximately every 10 minutes (Bitcoin Wiki, n.d. a). Litecoin adds a new block approximately every 2.5 minutes (Wikipedia, n.d. a). Ether is even faster at adding blocks, approximately every 12 seconds (EthHub, n.d.). In most cases, transactions can be considered final after they are added to the blockchain, but because double-spend transactions are temporarily possible, it is, in case of a large value transaction, prudent to wait for a few new blocks before we consider the transaction completed.

2.1.3 Key insights of comparison

By evaluating the medium of exchange function of both fiat money and cryptocurrencies, a few key insights can be extracted. Fiat money is generally accepted in its own respectable geographical area because of its legal tender status. Acceptability outside this area is usually low. Cryptocurrencies are not limited by geographical borders because of the global nature of the internet. On the other hand, the acceptance of cryptocurrencies is very low compared to fiat money.

The beginning of the use of fiat or cryptocurrencies poses different entry barriers. The entry barrier for using fiat money is the costs associated with obtaining access to a bank account or other financial services. This entry barrier can still be prohibitively high, especially in developing countries with less developed financial institutions and infrastructure. The biggest entry barrier for cryptocurrency use is the lack of knowledge about cryptocurrencies and their use.

Cryptocurrency payment systems are contained in the cryptocurrency itself. This means that they are strictly standardised in the cryptocurrency protocol. In this way, cryptocurrency transactions avoid the complexity that is present in fiat payment systems. Fiat transactions can be relatively inexpensive in their most basic form, but when they go cross-border, have to be urgently processed and settled, or in any other way become complex, their transaction costs rise. The costs of cryptocurrency transactions are the same regardless of the properties of the transaction and are usually cheaper than a fiat transaction. However, cryptocurrencies have a relatively low transaction capacity. If transaction demand exceeds this capacity, cryptocurrency transaction costs can become prohibitively expensive.

Cryptocurrency transactions are concluded in minutes or seconds. The speed of cryptocurrency transactions is, therefore, much faster than most fiat transactions, with the exception of transactions in a RTGS payment system. Sometimes, fiat transactions may look instant from the point of view of the consumer, but this does not take into account that the funds have to be settled before the transaction is truly completed.

Cryptocurrencies are a relatively poor medium of exchange in 2020 despite having some advantages in terms of speed and cost. The main obstacle for cryptocurrencies to perform the medium of exchange function is their low acceptability.

2.2 Comparative performance of the store of value function

People rarely receive money at the same moment they spend it. Because of this, money needs to be stored over shorter or longer periods of time. According to Mishkin (2009, p. 56), a store of value is used to save purchasing power from the time an income is received until the time that income is spent.

The first and main property of a good store of value is that it does not lose value through time. Since future values are not certain, there is always at least some risk involved. Individuals are usually risk averse and are only prepared to take a higher risk in exchange for a potential gain in value. Jevons (1896, pp. 38, 39) states that it is desirable for money not to be subject to fluctuations in value since this could change not only the future value of savings, but can also change all other contractual relations expressed in monetary units.

Einzig (1966, p. 325) notes that there is a property of good money that is missing in Jevons' list; money should conform to liquidity to a high degree. Mishkin (2009, p. 56) also counts liquidity as an important property of a good store of value. Liquidity is a relative property that makes it easy and fast to use an asset as a medium of exchange or to exchange it for a medium of exchange. Any additional exchange that has to be done bears an additional cost in exchange fees and in the additional time spent. Many different assets can perform the store of value function. The value of some assets can increase relative to the value of money, but these assets are usually less liquid. The performance of the store of value function, therefore, has to be evaluated against the change of the purchasing power of an asset through time, its stability and also against the asset's liquidity.

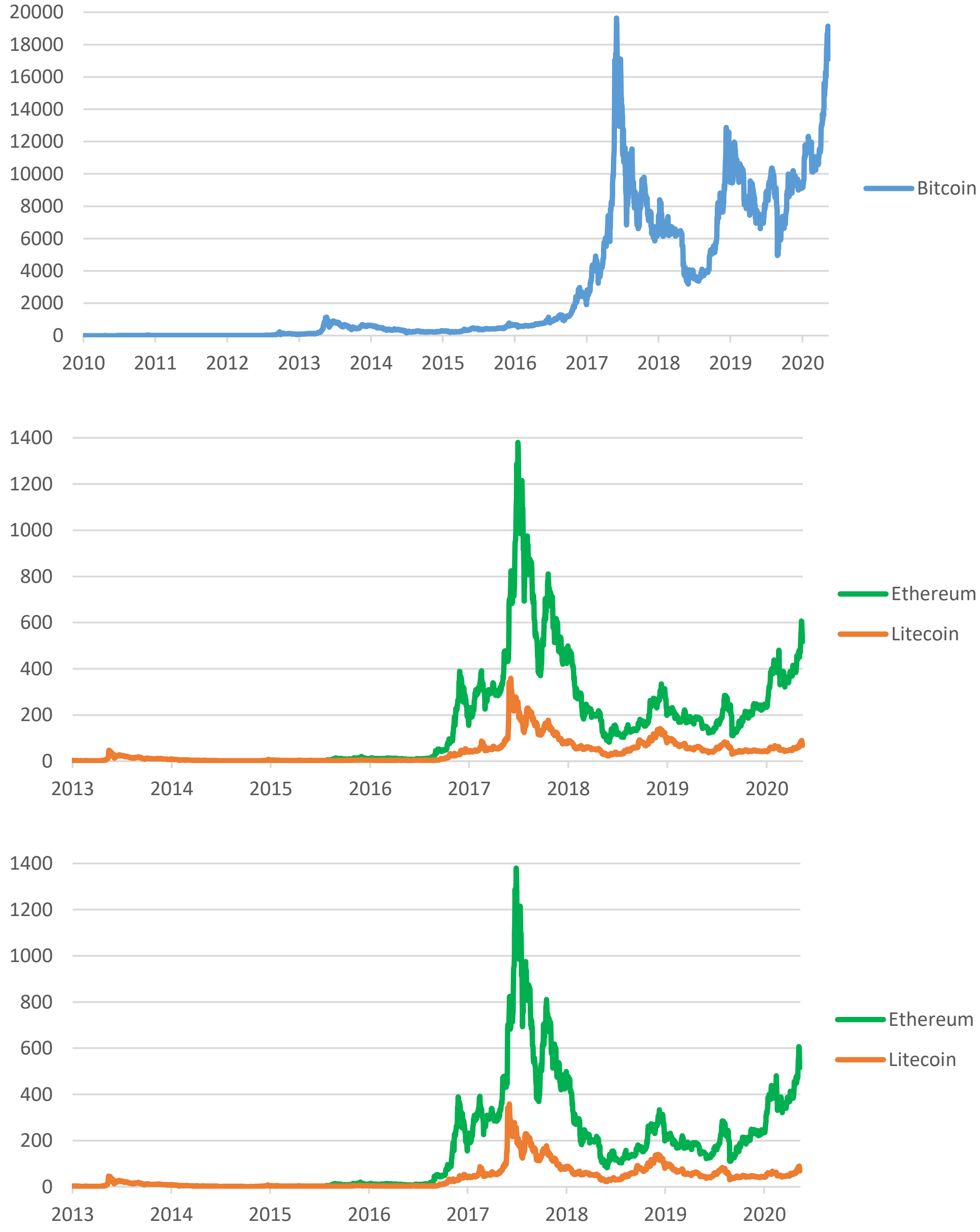
2.2.1 Fiat currencies as a store of value

Ideally, fiat money should have stable value. Fiat money value is determined by supply and demand, but supply is in the hands of the central bank. The central bank can regulate supply in sync with demand fluctuations in order to stabilise the value of fiat money. Different central banks have different goals, but they almost always include price stability among them. The inclusion of the price stability goal means that central banks try to maintain the value of the currency in terms of goods and services. This means that the price level stays the same and that there is no inflation. In reality, the central bank's goal is a low inflation instead of no inflation. The ECB (n.d. c) defines price stability as maintaining inflation below, but close to 2%. The Federal Reserve Board of Governors (n.d.) also states that a 2% inflation is consistent with their mandate. Other central banks have similar goals, but not every central bank is successful in keeping inflation low. The goal of low inflation means that fiat money loses around 2% of its value every year in the best case scenario. The loss of value can be much higher in countries with high inflation. On the other hand, there is very little risk associated with storing value in fiat money as even high inflation is usually anticipated. Despite inflation, people still choose to keep a portion of their wealth in fiat money. Fiat money is legal tender and it has to be accepted in exchange by law. That means that fiat is usually a good medium of exchange and also the ultimate liquid asset.

2.2.2 Cryptocurrencies as a store of value

Cryptocurrencies can also perform the store of value function, but since cryptocurrency exchange rates are very volatile, investing in them is more of a speculation than a storage of value. As shown in Figure 6, major cryptocurrencies like Bitcoin, Ethereum, Litecoin and Ripple have, like many others, increased in value tremendously in the long term. Further adoption could continue this trend.

Figure 6: Cryptocurrencies' exchange rates in USD through time



Source: Coin Metrics (n.d.).

Storing purchasing power in cryptocurrencies is also risky. Cryptocurrency exchange rates vis-à-vis fiat currencies are very volatile because cryptocurrency supply is predetermined and because cryptocurrency demand is volatile. That means that there is nobody trying to stabilise the exchange rate by managing supply like the central bank in the case of fiat money. Demand volatility can be partly explained with cryptocurrency adoption being in its early stages. According to Bolt and van Oordt (2016, p. 28), "more widespread use of virtual currencies by merchants and consumers lowers the impact of speculative behaviour and therefore stabilizes the exchange rate." This means that cryptocurrency investments could become less risky in the future.

Bariviera, Basgall, Hasperué and Naiouf (2017, p. 21) observe that Bitcoin volatility is trending downwards in relation to the higher volume of bitcoins in existence and in relation to increases in circulation. But Baur and Dimpfl (2017, p. 2) observed that bitcoin exchange rate volatility can still be up to 30 times higher than exchange rates between fiat currencies. This volatility can be clearly seen in Figure 6. Volatility in demand is so high because it stems mostly from the speculative (short term) part of demand. With an increased adoption of cryptocurrencies for commercial transactions, the source of demand should increasingly stem from the medium of exchange function, which will likely make the total demand smoother in the future.

There also exists a category of cryptocurrencies that have stable value – stablecoins. Their value is pegged to another asset, usually a fiat currency. For example, stablecoin called Tether can be seen in Figure 6. Tether value is pegged to 1 USD. This is why stablecoins are used as a safe asset in times of distress on cryptocurrency markets by cryptocurrency users.

As seen in Figure 6, investing in cryptocurrencies can be profitable even if it is risky, but a good store of value also has to be liquid. Marshall, Nguyen, and Visaltanachoti (2018, p. 4) use Bitcoin market spreads to assess Bitcoin liquidity. Lower spreads mean a higher liquidity of the assets. The authors observe that Bitcoin spreads are lower than the average stock spreads, but still higher than fiat currency spreads. Also, Wei (2018, p. 7) states that the established cryptocurrencies are improving in terms of market efficiency and liquidity, but on the other hand, new cryptocurrencies have limited liquidity. This means that cryptocurrency liquidity is lower than fiat liquidity. Until cryptocurrencies become a similarly good medium of exchange as fiat currency, they will be less liquid. Although, cryptocurrency liquidity already increased with the growing adoption. The exchange of cryptocurrencies for fiat money already became much easier than it was in the early years of cryptocurrencies. Cryptocurrencies may nowadays not be as liquid as required for a medium of exchange, but are relatively liquid as a store of value.

2.2.3 Key insights of comparison

Fiat currencies and cryptocurrencies perform very differently as a store of value. Fiat currencies are usually very stable and low risk, but are subject to low inflation. Cryptocurrencies, on the other hand, are volatile and risky, but can also be very profitable.

New developments in the form of stablecoins performs much better as a store of value than other cryptocurrencies.

Fiat currency liquidity is much greater than the liquidity of cryptocurrencies. If the adoption of cryptocurrencies keeps growing, it is reasonable to predict that the liquidity of cryptocurrencies will also grow. It has to be stated that until fiat currencies are the exclusive legal tender, they will always have the liquidity advantage over any other asset.

2.3 Comparative performance of the unit of account function

The unit of account function of money is performed when money is used for measuring and comparing the value of goods and services and for quantifying assets and liabilities. Jevons (1896, p. 14) was able to observe that when people frequently exchange things for money, they learn the value of those things expressed in it. A good unit of account must clearly and promptly convey information about the value of an item in question. As Jevons observed, money must first be used in exchange and, therefore, be a good medium of exchange before it can perform the unit of account function.

The unit of account function conveys information about values. The faster and more clearly this information is conveyed, the more utility it gives to an asset that performs this function. Jevons (1896, p. 40) states that money should possess cognisability. Cognisability means that money should be easily recognisable. Nowadays, this equates to the standardisation of money. A measuring unit of any kind has to be standardised in order to represent the same information to different people. It is the same with money. A unit of account has to be defined and standardised before it can represent the same value to different people. Additional effort, time and cost have to go into completing the exchange if the receiver of the payment has to determine the value of the money received. A poorly standardised unit of account can be misrepresented or just takes longer to convey value. Expressing value with unit of account is only practical if other people know and understand a specific unit of account. Jevons (1896, p. 37) also puts homogeneity down as a property that money should have. This means that all units of money representing the same amount should have the same value. Homogeneity of money also leads to fungibility. The fungibility of money means that units of money representing the same value are mutually interchangeable.

Goods or services can have any possible value and, therefore, money also has to be divisible in such a way that it can represent any possible value. Jevons (1896, p. 38) also noted the importance of divisibility. This means that good money has to be easily divided into the smallest units relevant to the expressed value. Money also has to be available in big enough units of value to be practical for high value payments. Any exchange for different units of money necessary for trade represents additional costs.

Fiat and cryptocurrencies will be further evaluated in their performance of the unit of account function. They will be compared by the level of standardisation and divisibility. The performance of the medium of exchange, as a prerequisite for performing the unit of account function, was already assessed in previous chapters. For the unit of account function, it is also beneficial if the values expressed in monetary units do not change too much through time since this would necessitate frequent and substantial changes in the valuations of goods, services, and assets.

2.3.1 Fiat currencies as a unit of account

A monetary authority is a central organisation that prescribes the standard for fiat money. This makes the standardisation of fiat money much easier. However, central banks only issue bank reserves and cash. Banknotes and coins are highly standardised to prevent forgery. Bank reserves are contained in accounts at the central bank and transferred between those accounts through a payment system at the central bank. Bank deposits, on the other hand, are stored at many different banks. These are internal bank systems that are connected through payment systems. Standardisation here is lower, but does not affect the unit of account function as long as parity between bank deposits, bank reserves and cash is preserved. In order to secure parity, commercial banks have to provide an interbank transfer possibility and the conversion of deposits to cash. This is how commercial banks "import" the unit of account function from central bank money to bank deposits.

As already stated, the stability of value of fiat currency is only threatened by inflation. The unit of account function first suffers from low and medium inflation in the form of the menu costs of inflation. According to Sheshinski and Weiss (1977, p. 287), there are costs associated with the transmission of price information to consumers. Inflation causes additional costs by constantly changing prices. In such a case, the costs associated with changing prices are called the menu costs of inflation. High inflation, on the other hand, causes people to lose track of the value represented by money and, therefore, prevents it from performing the unit of account function. According to Zijlstra (1975, p. 499), inflation higher than 10% fundamentally impairs the confidence in the unit of account function.

The divisibility of fiat money is not an issue with electronic payment systems, but it can be a problem when we transact in cash. Banknotes and coins are usually designed in denominations that allow us to represent any practical value. Finding exact cash can be a small inconvenience for a customer in a shop. On the other hand, businesses are expected to have enough cash in the right denominations available to return the exact change for the whole day. Managing cash and exchanging different denominations causes additional costs for a businesses. In the study performed by Schmiedel et al. (2012, p. 27), the average social costs of cash transactions were calculated as 0.42€ per transaction.

2.3.2 Cryptocurrencies as a unit of account

Cryptocurrencies are standardised by the computer protocol that defines them. This protocol decides whether a transaction is to be confirmed and added to the blockchain. If a transaction does not conform to the protocol, it is not going to be added to the blockchain and will be rejected by everyone that follows the protocol. This is how a cryptocurrency is able to ensure that all transactions obey the standard. There are more than two thousand cryptocurrencies in existence (CoinMarketCap, n.d. a). The sheer number of cryptocurrency protocols in existence could cause some confusion and, therefore, hurt the unit of account function of cryptocurrencies.

A unit of account has to be relatively stable in order for people to memorise its value. As can be seen in Figure 6 in the chapter about the store of value function, cryptocurrency exchange rates are very variable, with the exception of stablecoins. For example, Tether in Figure 6 is pegged to the value of 1 USD.

Divisibility is not an issue for cryptocurrency transactions. Bitcoin, for example, is divisable into smaller units called satoshis that represent 1×10^{-8} of one bitcoin (Bitcoin Wiki n.d. c). Ethereum is even more divisable. The smallest unit of ether is called a wei and represents 1×10^{-18} of one ether (Ethereum Foundation, n.d. a). Another problem is the high value of some cryptocurrencies. An example is the value of a cup of coffee expressed in bitcoin with four or five decimal places. The value of coffee could be expressed in satoshis, but this is another unit that people would have to learn to understand, even if it is directly related to one bitcoin.

2.3.3 Key insights of comparison

Cryptocurrencies do not perform well as a unit of account and can hardly compare to fiat in this regard. Cryptocurrencies came into existence 10 years ago, but are still in the very early stages of their evolution. Performing the medium of exchange function is a prerequisite for a currency to perform the unit of account function and cryptocurrencies are still too weak at preforming the former. The instability of exchange rates also works against cryptocurrencies being able to perform the unit of account function. On the other hand, the standardisation and divisibility of cryptocurrencies matches that of fiat money.

2.4 Overall assessment of cryptocurrencies' performance as money

At present, cryptocurrencies perform the more risky part of the store of value function. Speculative investments are a big part of it. In very limited terms, cryptocurrencies also perform the medium of exchange function. Bitcoin especially is performing the medium of exchange function in the purchase and sale of other cryptocurrencies. The unit of account function is not performed at all by cryptocurrencies. Cryptocurrencies cannot be considered money at this point in time. Since fiat currency is the benchmark for the performance of the functions of money, cryptocurrencies are assessed through their differences with fiat. The main differences between fiat and cryptocurrencies with respect to the functions of money are listed in Table 2 below.

Table 2: Main differences between fiat and cryptocurrency

Properties	Fiat	Cryptocurrency
Acceptance	High in specific geographical areas	Low, but global reach
Cost of transactions	Cost of transactions rises with the complexity of the transaction	Low as long as the number of transactions does not exceed the capacity
Speed of transactions	Speed can vary depending on the complexity of the transaction	Fast
Volatility	Low or at least predictable	High
Profitability as store of value	Low and low risk	Potentially high and high risk
Liquidity	Ultimate liquidity means	Lower than fiat money
Divisibility	Cash change is not always available	High
Standardisation	Electronic payments have to be standardised for every payment network	Standardised protocol for electronic payments

Source: Own work.

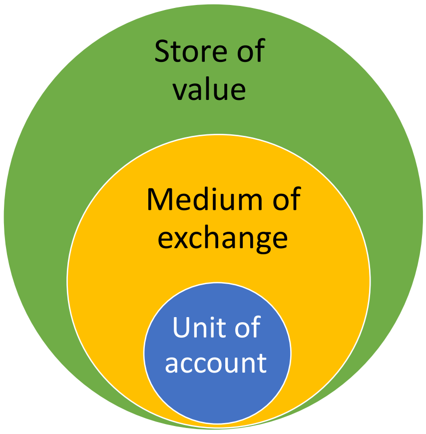
The low acceptance of cryptocurrencies is the first and most important benchmark that tells us that they are not performing very well as money. Cryptocurrencies also have a high exchange rate volatility, are relatively less liquid compared to fiat currency, and carry a high risk as a store of value. The advantages of cryptocurrencies over fiat currency are the speed of transactions and potential profitability. The low cost of transactions is also a potential advantage of cryptocurrencies provided that the cryptocurrencies' capacity of transaction processing is scaled up.

2.5 Future prospects of cryptocurrency as money

Since cryptocurrencies are a new technology, which has only been evolving for 10 years, it is possible that further evolution could improve cryptocurrencies' performance as money, which could lead them to challenging fiat money. If the current trend continues, cryptocurrency acceptability could rise and volatility could diminish further. With higher acceptance, liquidity would also improve and with lower volatility, risk would also diminish.

There are some mitigating circumstances that are favourable for cryptocurrency adoption. The first is the nature of the functions of money. According to Ali et al., (2014a, p. 3), different assets may, at various times, play some or all of the roles, and the functions of money may be considered to operate in a hierarchy, as depicted in Figure 7. Bitcoin, for instance, performs a limited medium of exchange function, but, at the same time, does not perform the unit of account function at all. Laughlin (1903, p. 2) already noted that "it is possible that some form of what everyone recognizes as money may serve only in one, and not in all, the functions of money; while another form may perform all of these functions." This means that the functions of money are separable and a specific cryptocurrency does not have to perform all the functions of money at the same time. Even cryptocurrencies will probably have to adhere to the hierarchy of the functions of money. Because of its IT nature, a cryptocurrency's functions of money could be even more easily separated from one another than the functions of fiat money. For example, prices could be denominated in fiat and only be converted into cryptocurrencies for payment with cryptocurrency.

Figure 7: Hierarchy of the functions of money



Source: Ali et al., (2014, p. 4).

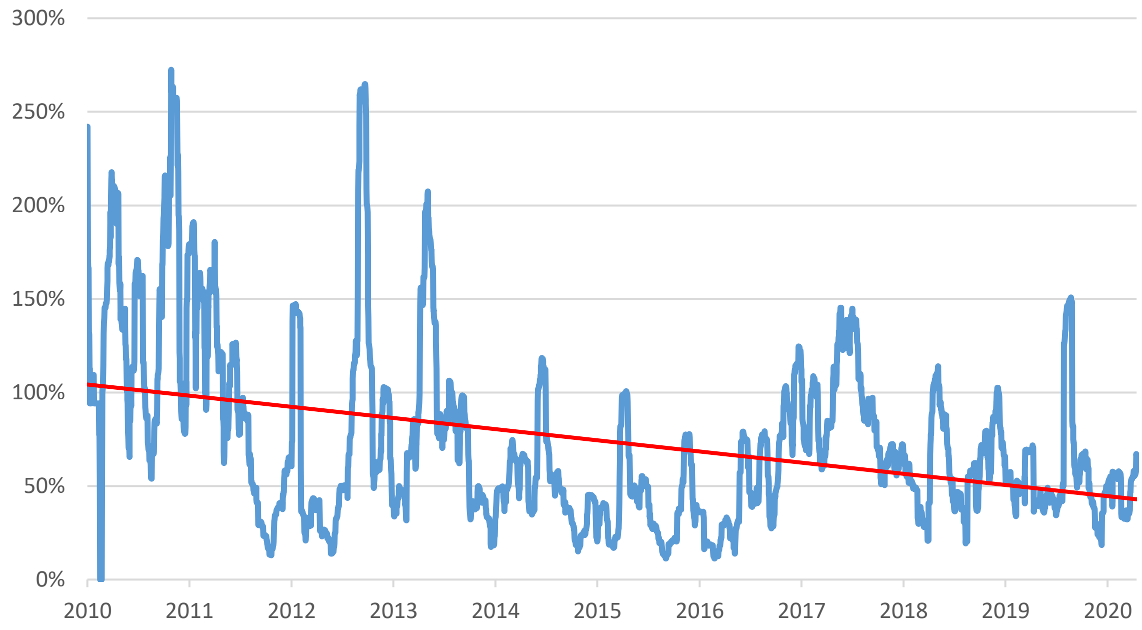
Functions other than the functions of money are also performed by cryptocurrencies. These are also beneficial for cryptocurrency adoption. Different platforms and services that are enabled by cryptocurrencies can increase the demand and, therefore, increase adoption. Cryptocurrencies are, as a protocol, computer-friendly even without intermediaries. This could make cryptocurrencies favourable for machine-to-machine payments in the Internet-of-Things world.

All this means that cryptocurrencies could gradually perform one function after another and it is possible that cryptocurrencies would someday perform all the functions of money and be used as parallel money. Cryptocurrencies could, therefore, become more competitive to fiat currencies in the future. Furthermore, this also means that it is necessary to evaluate the implications of increasing the adoption of cryptocurrencies from a monetary policy perspective. This evaluation will be done in the third part of this thesis.

2.5.1 Open issues for the wider adoption of cryptocurrencies

Before cryptocurrencies could be adopted further and have any effect on monetary policy implementation, some issues have to be resolved. The low cost and high speed of transactions could cause more people to use and accept them in the future. Even nowadays, potential profits in cryptocurrency speculation drive the growth in the use of cryptocurrencies. The higher acceptance and adoption would further benefit liquidity. Exchange rate volatility and the risk connected with it could also be diminished by the growing adoption. For example, Bariviera et al. (2017, p. 24) note that Bitcoin volatility is decreasing. They also note that the evolution of financial infrastructure, especially the emergence of bitcoin derivative exchanges, helped limit Bitcoin's volatility. In Figure 8, it can also be observed that the trend line (in red) for the annualised one-month volatility of the price changes of Bitcoin has a downward slope. Bariviera et al. (2017, p. 21) also add that this trend should continue as infrastructure further improves and the volume of transactions further increases.

Figure 8: The annualised one-month volatility of the price changes of Bitcoin



Source: Bitcoin.com (n.d.).

As shown in Figure 8, Bitcoin volatility is decreasing. This could be further extrapolated to all cryptocurrencies that would grow in user base and adoption similar to Bitcoin. However, the growing transaction volume could exceed a specific cryptocurrency's transaction capacity. In the past, this caused transaction costs to become prohibitively expensive and transactions having to wait for free processing capacity. Therefore, cryptocurrencies have to be able to scale their transaction capacity in order to keep the advantage of low transaction costs.

2.5.2 Scalability solutions

In order for cryptocurrencies to be used by many people, the cryptocurrency protocol has to be able to facilitate all the transactions its users make. Scalability is the property of a payment system, describing the ability to facilitate the transaction demand of a growing user base. Transaction throughput is measured in transactions per second (tps).

In Table 3 below, different payment systems' throughputs are compared with the throughputs of some cryptocurrencies. SEPA (Single Euro Payments Area) is a retail payment system used for transactions between bank accounts in the European Union. The Visa payment system is used for Visa card transactions. In comparison to SEPA and Visa, Bitcoin and Ethereum have much smaller throughputs. Ripple can process a number of transactions in the same order of magnitude as SEPA and Visa by sacrificing decentralisation. Cryptocurrencies will have to improve their throughput if they can ever hope to function as money. This fact is known in the cryptocurrency community and there are many solutions in development. Bitcoin Cash and Zilliqa use some of these solutions that are also reflected in an increased throughput.

Table 3: Transaction throughput in different payment systems

	SEPA In 2016	Visa	Bitcoin	Ethereum	Ripple	Bitcoin Cash	Zilliqa
Transactions per second	more than 3513 tps	Average 1736 tps, capable of 56000 tps	Capable of 7-8 tps	Capable of 15 tps	Capable of 1500 tps	Capable of 204 tps	2828 tps tested

Source: ECB (2017, p. 6); European Payments Council (2018); Visa (n.d.); Visa (2015); Kwaasteniet (2018); Ripple (n.d.); Hertig (n.d.); Zilliqa (n.d.).

The maximum throughput of cryptocurrencies is also important because it limits the supply of transactions, and when demand outstrips supply, the price of transactions goes up because transactions have to compete against each other. Transactions compete by increasing the fee they are willing to pay to miners. Miners always prefer transactions with higher fees. The maximum throughput of a cryptocurrency is determined by block time, block size and transaction size. Block time is the average time in which a new block with new transactions is added to the blockchain, block size is the maximum size of a block, and transaction size is the average space that a transaction takes in a block. Block size and transaction size determine how many new transactions can be added per block and block time determines how long one block is receiving new transactions. The following paragraphs will explain how the cryptocurrency community is trying to relax these limitations and increase the throughput.

Lowering the transaction size is the first parameter that has already improved the throughput of cryptocurrencies. By lowering the transaction size, it is possible to place more transactions into one block. An already successful solution for lowering transactions size is called SegWit, short for segregated witness. By implementing SegWit, Bitcoin was able to approximately halve the average transaction size and increase throughput from 4 tps to 7-8 tps (Kwaasteniet, 2018). According to Acheson (2018), SegWit was initially intended to fix a bug in the bitcoin code. SegWit implementation splits the digital signature part of the transaction from the main part of the transaction and stores it separately in the block. Block size, for the main part of the transaction without the signature, is still limited as before, but more transactions can be packed into one block. The signature part of the transaction is still there, but does not count into the block size cap.

Another way to lower transaction size is to implement Schnorr signatures instead of Elliptic Curve Digital Signature Algorithm (ECDSA) signatures that are nowadays used by most cryptocurrencies. Most ECDSA signatures come in lengths of 72 or 71 bytes. The more efficient Schnorr signatures have a maximum length of 64 bytes. Schnorr signature implementation also allows multi-signature transactions to be smaller by combining multiple signatures into one. There are estimations that Schnorr signature implementation would lower the size of an average transaction by 25 to 30% (Erhardt, 2018). Schnorr signature algorithms were already described by Schnorr (1990), but are only now started being adapted to be used with cryptocurrencies.

Another potential solution for improving cryptocurrency throughput is raising the maximum size of the block, which would then be able to accommodate more transactions. It has not been conclusively determined why Satoshi Nakamoto introduced a 1 MB limit for Bitcoin blocks and there are still debates going on Bitcoin Forum (n.d. b) about his intentions. Raising block size seems like a simple solution, but has proven to be difficult to implement in existing cryptocurrencies. For example, there have been proposals to raise Bitcoins block size since 2010 (Bitcoin Forum, n.d. a). Because there are a lot of stakeholders in decentralised systems and because there is a desire for a broad consensus between them before making changes, the implementation of any scaling solutions can take years. A high consensus between stakeholders is necessary in order to prevent splits in the blockchain. A split of the blockchain creates two different cryptocurrencies and also splits a cryptocurrency community. Because of the slow speed of change in existing cryptocurrencies, some stakeholders became frustrated and purposely created new cryptocurrencies. The most notable new cryptocurrency was Bitcoin Cash that came into existence as a fork of Bitcoin and raised the block size to 8 MB.

There is an argument against increasing the block size. A larger block would also mean a larger blockchain. In order for a node to independently verify address balances in a trustless manner, it has to download and store the whole blockchain, i.e. all transaction history. That is a problem due to bandwidth and storage costs; especially for devices that are very limited in both, such as mobile phones and Internet-of-Things devices. Increasing the blockchain size would, therefore, increase the costs of running a node and decrease the number of nodes. There is a potential solution for this in running a light node instead of a full node. A light node does not download and store the whole blockchain, but instead references a state from a trusted full node and only downloads the blockchain from this point onwards. This requires a light node to trust another node and lowers decentralisation. This is why not everybody sees light nodes as a solution. In practice, almost all mobile phones use light node software because storing a whole blockchain on a mobile phone is not practical. According to

Blockchain.com (n.d.), the Bitcoin blockchain measured more than 300 GB in November 2020.

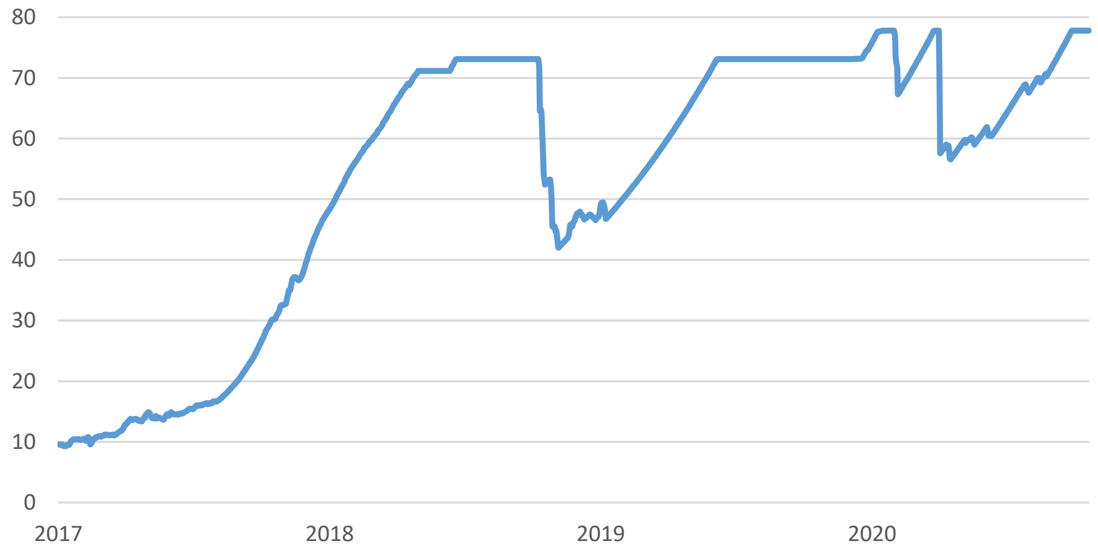
Another proposed solution is Sharding. Sharding is a technology used for scaling centralised databases and is now being considered or is already implemented in some cryptocurrencies. Sharding is a way of dividing a database into many shards that act as individual databases, but together form an aggregated original database. In cryptocurrency, this means grouping nodes that process transactions specific to that shard. This means that many shards can process transactions in parallel rather than all transactions being processed by all nodes. This increases the transaction throughput. Sharding is being most notably pursued by Ethereum developers and is already implemented in the Zilliqa cryptocurrency (Curran, 2018b).

Another group of scaling solutions is called Layer 2 scaling or off-chain scaling. In this group, there exist different solutions that are implemented by building another layer on top of the original blockchain, which is in such circumstances called the main chain. In Layer 2 scaling solutions, transactions are conducted on the layer above the main chain and only the results of these transactions are afterwards settled on the main chain. Layer 2 scaling does not require any change on the main chain. Therefore, there is no consensus needed for Layer 2 scaling to be implemented and anyone can try to invent the best scaling solution. Layer 2 solutions are built on the main chain using main chain smart contracts. Layer 2 scaling makes use of the safety provided by the main chain to process transactions, which do not burden the main chain. This is how Layer 2 solutions provide increased throughput. Layer 2 solutions enable cryptocurrency scaling in a similar manner as broad money enables scaling of narrow money in fiat. There are many ways Layer 2 scaling can be implemented and there are also competing solutions for the same cryptocurrency. A few examples of Layer 2 scaling solutions are the Lightning network for Bitcoin and Bitcoin-derived cryptocurrencies, the Raiden network, the Plasma network, and Truebit on Ethereum. There are also other solutions which are supposed to work on any cryptocurrency, such as the Celer Network (Stark, 2018). Most of these solutions are still being developed, but, according to statistics by 1ML.com (n.d.), the Lightning network was already being used by almost 15.000 nodes in December 2020, even though it is still being tested.

There is another metric that can be used for payment system throughput; this is the number of transactions per unit of energy used by the network. When looking at tps, we only try to increase the number in transactions in the numerator because time (second) in the denominator cannot be changed. But if we look at transaction per watt, we can also try to lower the energy consumption of the network. Most cryptocurrencies use a Proof-of-Work mechanism to secure the blockchain. In Proof-of-Work, miners solve a puzzle that is difficult to solve, but has a solution that is easy to confirm. The work of the miners is done by computer chips that require electricity, which is measured in watts. Miners are incentivised to use more efficient mining computers in order to lower their electricity costs. But since miners also compete with each other, they will all input more work and this is why no significant decrease in the energy consumption of miners is achieved with the use of more efficient mining computers. How much electricity all miners use depends on the mining rewards and fees received from the network and the exchange rate of a specific cryptocurrency. Miners will not use more electricity than they are able to pay for with the mining rewards and fees they earn. If mining rewards are decreasing through time, like with Bitcoin, miners receive less and are able to spend less on electricity. Ethereum, on the other hand, has constant miner rewards. As previously stated, fees are dependent on transaction demand and supply (maximum transaction throughput). The value of rewards and fees is determined by the exchange rate. The higher the exchange rate, the more miners can spend on electricity.

Figure 9 shows the estimated energy consumption of Bitcoin per year. The estimated energy consumption of more than 75 TWh per year in December of 2020 can be compared with the energy consumption of a small country. The fall in the estimated energy consumption seen at the end of 2018 is the consequence of the lower Bitcoin exchange rate that determines the value of the rewards paid out to miners. If the Bitcoin exchange rate decreases, then the value of the rewards also decreases proportionally. If rewards are low enough, less energy-efficient mining computers stop being profitable and are turned off and the network as a whole uses less electricity. In the same manner, there was a dip in the estimated energy consumption in May 2020 when the halving of the miner reward took place.

Figure 9: Estimated Bitcoin energy consumption per year in TWh



Source: Digiconomist (n.d.).

The solution to high cryptocurrency energy consumption is the switch to different systems of securing the blockchain. The most notable contender for the Proof-of-Work alternative is the Proof-of-Stake. In Proof-of-Stake, nodes secure the blockchain not by imputing work, but by staking their cryptocurrency assets against the right to process transactions. If the node performs its job honestly, it keeps its stake and gains a reward. If a node behaves maliciously, it loses its stake. Since there is no need for the input of work in the Proof-of-Stake protocol, energy consumption could be much lower. According to Buterin (2014), Proof-of-Stake for Ethereum has been in development since 2014, but the implementation is still not ready. Zilliqa, on the other hand, uses a combination of Proof-of-Work and another mechanism called the Practical Byzantine Fault Tolerance. Proof-of-Work is used approximately every 100 blocks; otherwise, the more energy efficient Practical Byzantine Fault Tolerance is used (Curran, 2018a).

In this chapter, only a few most prominent scalability solutions have been presented. There are more solutions in development. Some of the presented solutions have already been implemented, some are being tested and others are still in development. Most cryptocurrencies have yet to come close to their throughput limits, but are already developing and implementing scaling solutions. The scalability problem is recognised in the cryptocurrency community and is being dealt with. This is how cryptocurrencies will be able to facilitate a large enough transaction throughput and, as a result, scalability should not be an obstacle for cryptocurrencies to act as a medium of exchange and money.

The technical solutions that are in development in regards to scalability imply that the cryptocurrency throughput limit will be resolved before it could throttle further adoption. As long as there is high enough throughput available, transactions do not have to compete for processing capacity by offering additional fees. This means that total network costs should not rise with the number of transactions as long as there is enough throughput available. If total network costs stay the same, a higher number of transactions will lead to a lower average cost.

By providing the efficiencies of the cryptocurrency protocol and network, cryptocurrencies could offer cheaper and faster transactions. With further adoption potentially leading to lower volatility and stablecoins providing a more stable environment, cryptocurrencies could begin to perform all three monetary functions in the future.

3 MONETARY POLICY IMPLICATIONS OF CRYPTOCURRENCIES

Monetary and fiscal policy are tools with which an economy is managed. Both are used for the propagation of economic growth and the smoothing of business and financial cycles. Fiscal policy makes use of the government's ability to manage its budget and taxes. Monetary policy uses the central bank's monopoly over the issuance of money to control money supply. By controlling money supply, the central bank is able to affect the economy. In the previous chapter, I concluded that cryptocurrencies have properties that could allow them to better perform the functions of money in the future, even though there are still several issues to be resolved before that happens. However, the central bank cannot control the issuance and supply of cryptocurrencies. The increased use of cryptocurrencies could have detrimental implications for monetary policy. On the other hand, a central bank could offer cryptocurrency users an alternative to cryptocurrency in the form of central bank digital currency (CBDC).

This chapter will explore the possible further cryptocurrency adoption in the future and its effect on the effectiveness of monetary policy. Furthermore, CBDC will be explored as a competing alternative to cryptocurrencies. Firstly, the role of a central bank and the banking system in a fiat currency system will be examined. Secondly, the implications of a significant cryptocurrency adoption will be examined. Monetary policy effectiveness in such a case will also be evaluated. Finally, CBDC proposals will be explored. The comparison of CBDC, cryptocurrency and fiat will also be performed in order to evaluate CBDC's ability to compete with cryptocurrency.

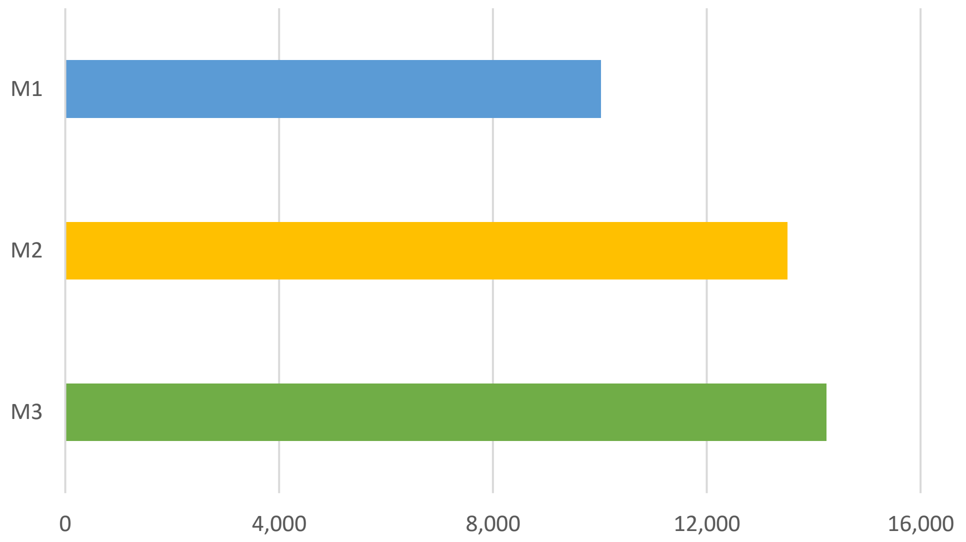
3.1 Traditional monetary and banking system

The monetary system that is in use in modern societies is called a fractional reserve banking system because of the reserves which commercial banks have to keep when they take deposits. Commercial banks do not have to hold all the deposits in reserve. Instead, they only keep a small fraction in reserve and use the rest to make loans.

In a fractional reserve system, there is a central bank at the top that manages and regulates the system. The central bank issues base money and lends that money to commercial banks. The central bank does not deal with businesses and individuals. Only commercial banks have accounts at the central bank. The central bank is also responsible for monetary policy. Commercial banks take deposits from the public and make loans. Commercial banks enable their clients to make transactions and allow them to withdraw their money when they need it.

Money in a fractional reserve banking system is issued by the central bank and the commercial banks. Money that is issued by the central bank is called base money and is denoted with M0. Base money consists of cash and bank reserves. Commercial banks issue money when they make new loans to the public. New loans are credited to the bank accounts in the form of deposits. This is how commercial banks are able to create new money. Demand deposits and cash in circulation are included in the M1 money aggregate. M1 plus deposits that are not available for immediate withdrawal are a part of a wider M2 money aggregate. M2 plus less liquid deposits and assets are denominated in the M3 aggregate. The M4 aggregate includes M3 and other assets that are even less liquid than M3. M1, M2, M3 and M4 are all part of broad money (Ryan-Collins, Goodhart, Greenham, Werner, & Jackson, 2012, ch. 4.1, par. 5). The proportions between monetary aggregates in the euro area can be seen in Figure 10.

Figure 10: Monetary aggregates in the euro area in October 2020 in billions of euros



Source: ECB (n.d. b).

3.1.1 Traditional role of the central bank in a fiat currency system

The role of the central bank in a fiat currency system is to regulate commercial banks and conduct monetary policy. By regulating commercial banks, the central bank ensures that the liabilities of commercial banks do not exceed their assets and that commercial banks have enough money to meet their maturing obligations, i.e. that they remain liquid. The central bank ensures that commercial banks are liquid by intervening on the interbank market where commercial banks lend bank reserves to each other. Intervening on the interbank market is possible because the central bank has a monopoly over issuing bank reserves and cash. The central bank injects reserves to commercial banks through its lending operations. On the other hand, the central bank can also absorb or buy back (repurchase) bank reserves at maturity of the central bank's lending operations. Since the general public does not have access to the central bank, cash has to be provided to them through commercial banks. Commercial banks obtain cash by exchanging bank reserves for cash with the central bank. This is how the central bank is able to manage the level of bank reserves on the interbank market.

To affect the level of bank reserves, the central bank conducts open market operations. When the central bank wants to permanently increase bank reserves on the interbank market, it usually makes outright purchases of government bonds from the banks. If the central bank wants to lower bank reserves on the interbank market, it buys bank reserves from commercial banks and pays for them with government bonds (Ryan-Collins et al., 2012, ch. 4.7, par. 4). The central bank can also temporarily increase the level of bank reserves on the interbank market by conducting collateralised repurchase agreements. The collateral for repurchase agreement loans are usually government bonds. When the central bank wants to maintain the same level of bank reserves, it just renews the expiring repurchasing agreements. Finally, if the central bank wishes to lower the level of bank reserves, it leaves repurchase agreements to expire, receives back bank reserves, and returns the collateral. The central bank can also use reverse repurchasing agreements for absorbing excess bank reserves from commercial banks (Ryan-Collins et al., 2012, ch. 4.7.1, par. 1). The central bank also provides standing facilities where commercial banks can deposit or borrow bank reserves in the case of an emergency. If interest rates on the interbank market are too high (to borrow) or too low (to deposit) relative to the policy rate, commercial banks can go to the standing facility. At standing facilities, commercial banks can borrow bank reserves at a penalty borrowing interest rate that is a little higher than the policy rate. Commercial banks can also deposit bank reserves at the standing facility at a penalty deposit interest rate slightly lower than the policy rate. Typically, the standing facility's penalty interest rates are 1% higher or lower than the policy rate (Ryan-Collins et al., 2012, ch. 4.7.2, par. 1).

With open market operations, repurchase agreements and standing facilities, the central bank ensures that commercial banks stay liquid. Another tool at the central bank's disposal is a reserve ratio requirement. The central bank can prescribe the minimum ratio of bank reserves to bank deposits. The central bank also has to ensure that a commercial bank's assets exceed its liabilities, i.e. that they remain solvent. Bad loans can lower a commercial bank's assets and turn it into an insolvent bank. Insolvent banks do not have enough assets to cover their liabilities and have to go bankrupt or have to be recapitalised. The central bank targets the solvency of commercial banks by imposing capital requirements. Capital requirements require commercial banks to hold additional capital that can be converted into assets in the case of non-performing loans (Ryan-Collins et al., 2012, ch. 4.8, par. 4).

Central banks can also manage foreign exchange rates, however, not all central banks do so. That depends on the exchange rate regime. Central banks have to hold foreign exchange reserves to be able to manage the exchange rate or for precautionary reasons (Ryan-Collins et al., 2012, ch. A2.5, par. 1).

3.1.2 Traditional role of the banking system in a fiat currency system

Since the general public does not have access to central bank accounts, people and businesses have to turn to the banking system to access money. Commercial banks provide access to bank accounts, issue bank deposits and hold cash. Cash is actually issued by the central bank and distributed to the public via commercial banks. Commercial banks get cash by exchanging bank reserves for it. Bank account holders can get cash by exchanging bank deposits for it (Ryan-Collins et al., 2012, ch. 4.4.1, par. 2, 3). Bank deposits are also issued by commercial banks through making loans. When a client of a commercial bank requests a loan, the commercial bank estimates if the client is creditworthy. If the commercial bank determines that the client will be able to repay the loan, it then issues the loan. The loan is issued by crediting the client's (deposit) bank account. When loans are issued, the money supply increases accordingly. On the other hand, the money supply shrinks accordingly when loans are repaid.

If people have bank deposits on their bank accounts, they will eventually want to use these deposits. This can be done by exchanging deposits for cash and using cash for payment, or by making payments by transferring deposits from one account to another. If the receiving account is located at the same bank as the sending account, the process is simply completed by reducing the sending account and increasing the receiving account by the corresponding amount. If the accounts are located at different banks, there are two options. Besides decreasing the amount in the sending account and increasing it in the receiving account, the amount also has to be transferred between the two banks. The first option is for the sending bank to have an account with the receiving bank and for the sending bank to make the transaction to the receiving bank from this account. Another option is for the banks to settle in bank reserves. All commercial banks have a bank reserves account at the central bank. The sender bank can make a transfer of bank reserves from its account at the central bank to the receiving bank's account at the central bank. In order to minimise the number of transactions between banks and the quantity of bank reserves needed, banks cancel out all the transactions between them and only settle the net difference (Ryan-Collins et al., 2012, ch. 4.3, par. 4, 5).

After settling for the day, banks either have too much or too little bank reserves for the next day. If a commercial bank is lacking bank reserves, it can always borrow bank reserves on the interbank market. Since bank reserves are only transferred between commercial banks, there should always be enough bank reserves in the system. Commercial banks can also borrow bank reserves from the central bank (Ryan-Collins et al., 2012, ch. 4.3.1, par. 4).

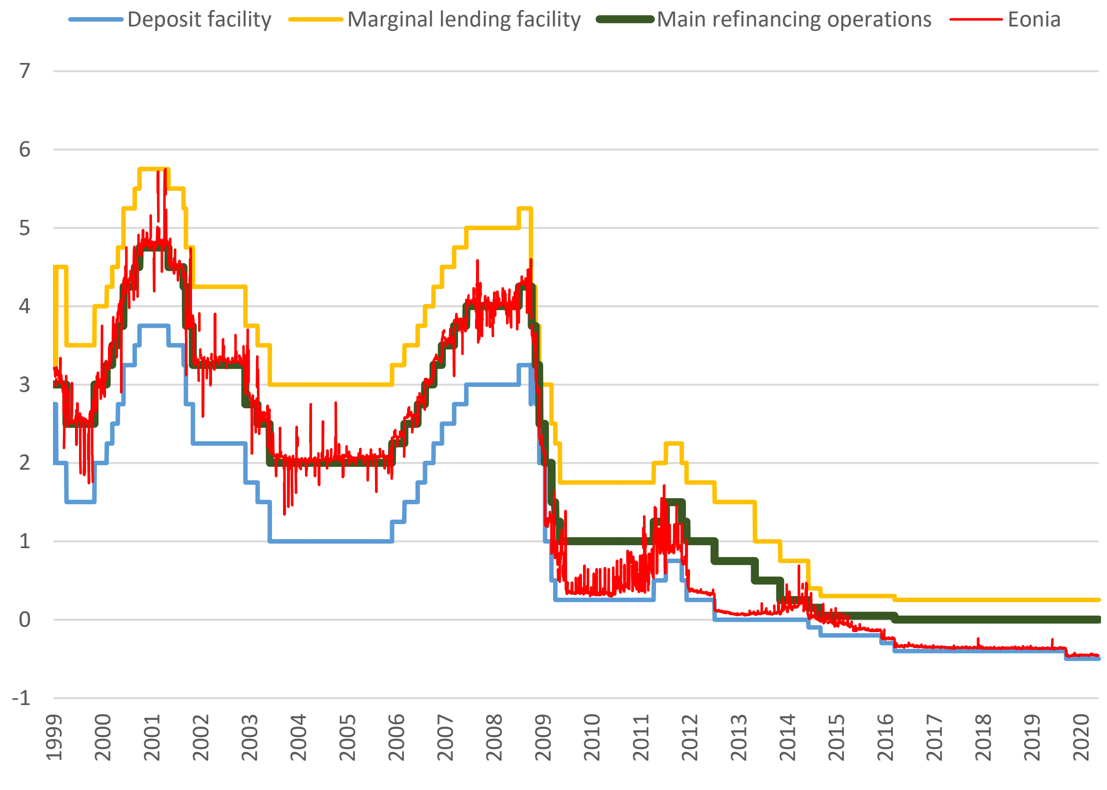
3.1.3 Monetary policy and its implementation

Central banks implement monetary policy towards specific goals, which are usually determined in legislation. Price stability is increasingly viewed as the most important goal of monetary policy. Price stability is defined as stable and low inflation. Price stability is important because inflation and instability can hamper economic growth (Mishkin, 2009, p. 315). High employment and growth of output are also the goals of monetary policy. The last two goals are hard to define. A high employment goal should not press onto the employment level beyond the natural rate of unemployment. But the natural rate of unemployment is subject to much uncertainty and disagreements. There is also an active debate about the efficiency of output growth as a monetary policy target. The other goals of monetary policy also include the stability of financial markets, interest rate stability and foreign exchange stability (Mishkin, 2009, pp. 317–319). Since price stability promotes economic growth, central bankers concluded that it should be the primary goal of monetary policy (Mishkin, 2009, p. 320).

3.1.3.1 Monetary policy tools

In order to achieve price stability or other monetary policy goals, central banks usually intervene on the money market. At the core of the money market stands the interbank market (Moenjak, 2014, pp. 118–120). In order to influence the conditions on the interbank market, central banks use the policy rate, open market operations, standing facilities and reserve requirements. These tools are not only useful for regulating commercial banks, as described in the previous chapters, but also for implementing monetary policy. When a central bank announces a policy rate, it signals what it deems is an appropriate interest rate on the interbank market and also sets the expectations about its further actions. Open market operations are then used to inject or absorb bank reserves from the interbank market. By injecting or absorbing bank reserves, the central bank can regulate their supply in such a way that the actual interbank rate comes as close as possible to the announced policy rate. Standing facilities are used by the central bank in order to limit volatility on the interbank market, which can be seen in Figure 11 for ECB rates and the EONIA (euro overnight index average) interbank rate. By lending at an interest rate higher than the policy rate, the central bank places a ceiling for the interbank rate because nobody would borrow at higher interest rates than can be obtained at the central bank. In the same way, by taking deposits at interest rates lower than the policy rate, the central bank places a floor for the interbank rate (Moenjak, 2014, pp. 123, 127).

Figure 11: ECB interest rates in percentages



Source: ECB (n.d. a); ECB (2020).

In the eurozone, the most important operations are open market operations. Liquidity to the banking system is provided by lending funds. Lending usually takes place in the form of reverse repurchasing agreements or in the form of a loan against assets pledged as collateral. Open market operations include main refinancing operations (MROs), longer-term refinancing operations (LTROs), fine-tuning operations (FTOs) and structural operations. These operations play an important role in steering interest rates, signalling the stance of monetary policy and managing the liquidity conditions for the euro area banking sector. MROs provide the bulk of liquidity to the banking system and generally have a maturity of one week. LTROs are aimed at providing longer-term liquidity to the banking system. LTROs have a three-month maturity. In the last financial crisis, LTROs have expanded substantially and have become one of the key policy tools of the ECB in addressing the crisis. FTOs are ad hoc open market operations aimed at managing the liquidity situation in the money market and steering interest rates, particularly in order to smooth the effects of unexpected liquidity fluctuations in the market on interest rates. The Eurosystem also offers two standing facilities to its counterparties: the marginal lending facility and the deposit facility. Both facilities have an overnight maturity (ECB, 2011, pp. 96–110).

The central bank can also use reserve requirements to affect bank reserves demand. By raising reserve requirements, the central bank forces commercial banks to acquire more bank reserves in order to comply with the requirements. This raises the demand and also the interest rates on the interbank market. With these tools, the central bank can effectively control the interbank market interest rate in order to make it as close as possible to the policy rate (Moenjak, 2014, p. 129).

In order for the interbank interest rate to affect real economic activity and price levels, the interbank interest rate must first affect interest rates in other segments of the financial markets. The interbank interest rate affects other interest rates through the overnight yield on government bonds. In an efficient financial market, overnight yields on government bonds will be very close to the interbank rate and, therefore, also close to the policy rate (Moenjak, 2014, p. 130). Commercial banks and other financial institutions use government bond yields as a benchmark for a risk-free interest rate since loans to the government are considered risk-free. Commercial banks and other financial institutions further translate a risk-free interest rate into an interest rate for their borrowers by adding a risk premium for a specific borrower (Moenjak, 2014, p. 131).

Until the fall of 2008, the ECB estimated the liquidity needs in the banking system that arise from autonomous factors plus reserve requirements and provided the system with this amount on a weekly basis, through open market operation, at the interest rate set by the ECB – the MRO rate. Commercial banks bid for the bank reserves at a rate very close to the rate set by the ECB and this rate smoothly transmitted to the whole yield curve. The interbank rate (EONIA) fluctuated between the marginal lending facility rate (upper limit) and the deposit rate (lower limit). The difference between the marginal lending facility rate and the deposit rate is the interest rate corridor (Rodríguez & Carrasco, 2014, p. 8). The corridor system can be observed in Figure 11 up to 2008. After 2008, the ECB adjusted its operations in response to the crisis by incorporating unconventional monetary policy tools.

3.1.3.2 Unconventional monetary policy

Unconventional monetary policy was the response to the conditions that have arisen from 2008 onwards. The impaired financial system prevented the conventional interest rate policy from supporting economic growth, and lowering the target interest rate to zero was not sufficient to stimulate the economy. Central banks then employed forward guidance. Central banks started to express publicly their commitment to achieving specific targets in the future. This target can, for example, be a low policy rate for a certain period. By doing this, a central bank can affect expectations. Expectations further affect developments on financial markets if market participants believe that forward guidance is credible (Cecchetti & Schoenholtz, 2015, pp. 506, 508).

Quantitative easing is a balance sheet policy used to relax the monetary stance when the policy target rate is close to zero when a central bank expands the supply of aggregate bank reserves beyond the level needed to maintain its policy rate target. With these new bank reserves, the central bank buys assets in order to inject additional liquidity into the money market, affecting the interbank market rate which is already close to zero (Cecchetti & Schoenholtz, 2015, p. 509).

In 2008, the ECB introduced fixed-rate full-allotment procedures for all refinancing operations. In other words, the ECB accommodated all bids from commercial banks at a specified fixed rate in full. This was done to mitigate the adverse effects that dysfunctional money markets were having on the liquidity situation of solvent banks in the euro area and to support the flow of credit to firms and households. The ECB also extended the maturity of LTRO from 3 months to 12 months and longer (up to 48 months) maturities in order to encourage banks to continue providing credit to the economy and to contribute to keeping money market interest rates at low levels. The Eurosystem purchased euro-denominated covered bonds issued in the euro area in order to revive the covered bond market through the covered Bond Purchase Programme. The covered bond market is a very important financial market in Europe and a primary source of financing for banks (ECB, 2011, pp. 105, 106, 127).

Asset purchase programmes are another part of unconventional monetary policy. They boost the relative price of these assets and stimulate economic activity. In order to limit interest rates on the sovereign debt of countries on the periphery of the euro area, the ECB introduced the Securities Market Programme. Through it, the ECB acquired more than 200 billion EUR of this debt. The ECB also offered to purchase, without limit, the debt of any country which accepted the stringent fiscal conditions on the secondary market through its Outright Monetary Transactions Programme. The ECB also introduced the Extended Asset Purchase Programme (quantitative easing) in which it widened the range of acceptable collateral in order to boost the relative prices of troubled assets and to make funds available to periphery banks lacking better collateral (Cecchetti & Schoenholtz, 2015, pp. 511, 512).

During the response to the conditions in 2008 and later on as well, many central banks migrated from the interest rate corridor system to the floor system. The floor system is not necessarily unconventional, but several central banks have moved from the corridor to the floor system during the financial crisis. In a floor system, the central bank supplies much more liquidity than in the corridor system. In order not to push the rate in the interbank market below the policy rate, the central bank offers a deposit rate equal to the policy rate at the deposit facility. This shift was also made by the ECB and can be seen in Figure 11. This is how it is possible for the central bank to increase the supply of liquidity to the banking system without pushing short-term money market rates below the key rate. The central bank can, therefore, use the policy rate and the amount of the liquidity supplied as two separate instruments (Bernhardsen & Kloster, 2010, p. 1).

3.1.3.3 Transmission mechanism

After interest rates pass through the financial sector, they reach the real economy and affect households and firms through the transmission mechanism. When interest rates fall, households tend to substitute future consumption for present consumption. This happens because the opportunity costs of present consumption in the form of returns on their savings are now lower. Lower interest rates also redistribute income from savers to borrowers. Because borrowers have a higher marginal propensity to consume, this also causes consumption to rise. The lowering of interest rates also causes a higher valuation of financial assets and, through the lower cost of financing, sparks demand for housing and, therefore, increases the value of housing. Because of the higher value of their financial assets and houses, households have more wealth and are able to consume more. For firms, lower interest rates mean a lower cost of funding and, therefore, higher spending and investment. Lower interest rates also mean a lower discount factor and, therefore, a higher net present value of firms. If firms are worth more, they will also be able to offer better collateral when applying for credit and it is also easier for them to issue new shares to finance their investments. Lower interest rates also lower the exchange rate, which in turn shifts consumption from imported to domestic goods and lowers the domestic costs of production relative to foreign production and, therefore, increase export. Monetary policy also effects households and firms through their expectations. When the central bank announces a new, lower policy rate, households and firms will take this announcement as a signal of future effects through the financial sector and immediately change their behaviour to consume and invest more (Moenjak, 2014, pp. 146–152; ECB, 2011, pp. 58–61).

Through the above-mentioned transmission mechanism, interest rates are able to affect aggregate demand and the price level through consumption, investment and net export (Moenjak, 2014, p. 143). This is how the central bank can affect the price level in order to achieve its goals of price stability, employment and output growth.

3.2 Cryptocurrency financial intermediation

In order to explore the implications of cryptocurrency adoption for monetary policy, the issue of cryptocurrency financial intermediation has to be examined first. Financial intermediation (lending and deposit taking) is important for monetary policy transmission and economic growth. This is why it has to be determined whether and how cryptocurrencies could be used for lending. The way cryptocurrencies are lent is especially important from a monetary policy perspective because new money can be issued through credit.

Lending that involves cryptocurrency already exists. There are some fiat loan providers that offer to take cryptocurrencies as collateral when making fiat loans like Bitbond, SALT Lending, Nexo, BlockFi and Unchained Capital. These are similar to loans that use securities as collateral. Some of these providers even offer cryptocurrency deposit accounts that pay interest. More integrated into the cryptocurrency ecosystem are peer-to-peer cryptocurrency lending platforms like LendaBit, Poloniex, Credible Friends, xCoins, ETHLend and BTCPOP. These platforms provide financial intermediation and cryptocurrency asset transformation. This means that borrowers can borrow in cryptocurrencies. Borrowing in cryptocurrencies could be even more interesting in stablecoins that are pegged to fiat currencies because this reduces exchange rate risk.

Fiat loans are made by two types of financial institutions. The first one are banks. Banks differ from other types of financial institutions by being able to make loans under a fractional reserve banking system. Since banks only hold a fraction of the value of their deposit liabilities in reserve, everyone cannot withdraw their money at the same time. In order to prevent a run on bank reserves, fractional reserve banking is highly regulated. If a bank run happens despite the regulation, a central bank has to step in as the lender of last resort. This can happen through the central bank’s standing facilities or through open market operations. The central bank also acts as the lender of last resort when there is a shortage of bank reserves on the interbank market. In extraordinary crises, central banks can even use unconventional monetary policy as described in previous chapters. Central banks are in a good position to act as the lender of last resort because of their ability to issue new money. The other type of financial institutions are non-bank financial institutions. These are all other financial institutions, such as investment and pension funds, insurance companies, and lease and microcredit firms that are not allowed to make loans or investments on a fractional reserve basis, but only based on collected funds. Non-bank financial institutions represent a smaller risk for their savers than banks and are, therefore, less strictly regulated. Consequently, the important question regarding cryptocurrencies is whether they could be lent on a fractional reserve or a fully collateralised basis.

The fractional reserve system benefits from the lender of last resort function and regulation. The same benefit would be favourable in the case of cryptocurrency fractional reserve banking. If the public lost confidence in a cryptocurrency financial institution, which operates under a cryptocurrency fractional reserve banking system, the cryptocurrency financial institution would experience a run on its digital currency reserves. The lender of last resort could then purchase the needed cryptocurrency in the open market and lend the cryptocurrency to the cryptocurrency financial institution. This lender of last resort could be the central bank. However, while the central bank could play the role of the lender of last resort for a single cryptocurrency financial institution, it would not be able to curb a widespread run on the cryptocurrency banking system because it cannot create cryptocurrency on demand (Nelson, 2018, p. 2). A central bank or any other state regulator would, therefore, not be able to efficiently perform the lender of last resort function to the whole cryptocurrency banking system at once, as needed in times of financial crises.

The lack of proper regulation and the lack of an efficient lender of last resort makes cryptocurrency fractional reserve banking unsustainable in the long run. There may be attempts from loan providers to lend under cryptocurrency fractional reserve banking in order to gain additional profit, but these attempts would lead to problems at the point of the next financial instability, much like the unregulated lending of banks in the past frequently ended in bank runs and financial crises before the advent of central banking and bank regulation. A bank run in a cryptocurrency fractional reserve banking system would result in defaults because there would not be anybody able to provide additional cryptocurrency liquidity into the system.

3.3 Implications of a wider adoption of cryptocurrencies

In the second part of this thesis, it was shown that cryptocurrencies could grow in adoption and, in time, perform all the functions of money. In such a case, cryptocurrencies could substitute a portion of cash. Since central banks earn seigniorage revenue from issuing money, including cash, the central bank would see diminished revenue relative to the current monetary system. Seigniorage is revenue that is earned on assets that a central bank receives from banks in return for newly issued money. This could also hurt central bank independence.

One of the roles of a central bank is to prevent financial instability that could damage economic growth. In the case where a cryptocurrency would be used alongside fiat, the central bank would have to regulate the financial institutions that take cryptocurrency deposits in order to facilitate financial stability. Any instability or panic in the cryptocurrency sector could spread to the whole banking system. Cryptocurrency markets are more transparent because all transactions are seen on a public ledger. A panic on the market, a speculative attack or an attack on the deposits held by a financial institution would be even more obvious because of this aggregate transparency. This is why regulation would need to be adopted in order to facilitate financial stability. The most urgent is the protection of deposits in order to protect the depositors and lower the potential panic.

Price stability is the main goal of traditional monetary policy because it represents the preferred state in the relation between fiat supply and the economy. When monetary policy effects pass through the interbank market, they affect the real economy through the transmission mechanism. The transmission mechanism is currently not affected by the presence of cryptocurrencies. The transmission mechanism mostly works through channels that affect credit creation. Cryptocurrencies, on the other hand, are presently not used for credit creation. The monetary authority's ability to conduct monetary policy is, therefore, not significantly influenced.

In the case of further cryptocurrency adoption, fiat and cryptocurrencies would exist in parallel. This would mean that cryptocurrency supply could also affect the economy. The relationship between cryptocurrency money supply and the economy has yet to be discovered. Cryptocurrencies fundamentally differ from fiat money in their interaction with the financial system. There is no analogue to cryptocurrencies that exists in the current monetary system. This is the reason for the uncertainty about the relationship between cryptocurrency supply and the economy.

In the case of a high enough adoption, cryptocurrency supply could affect the economy through a wealth effect channel. An increase in the value of cryptocurrencies would imply an increase in the wealth of cryptocurrency holders and, as a result, a rise in the consumer confidence of cryptocurrency holders. They could, therefore, consume and invest more. This wealth effect is similar to the wealth effect caused by the increase in prices on the stock market. The evidence of the stock market wealth effect on consumption is mixed. Case, Quigley and Shiller (2013, p. 29) found, at best, weak evidence of a link between stock market wealth and consumption. Cho (2006, p. 406) presents evidence for a statistically significant stock market wealth effect using the household level data of urban households in Korea. In Korea, the evidence of the stock market wealth effect was present in the highest income bracket households which typically hold a large share of corporate stock, while the effect for the rest of the income bracket turned out to be insignificant. Mankiw and Zeldes (1991, p. 110) find that the aggregate consumptions between stockholders and non-stockholders differ substantially. Furthermore, they find that stockholder consumption covaries more strongly with excess equity returns in comparison with total consumption. The estimations of the effect imply that a $1 capital gain raises the level of consumption by between 1 and 15 cents (Dynan & Maki, 2001, pp. 25, 26; Poterba, 2000, p. 107; Boone, Giorno, & Richardson, 1998, p. 14).

The stock market wealth effect may be an existing phenomenon that is the closest to the potential cryptocurrency wealth effect, but there are important differences between stock market assets and cryptocurrencies and between their respective holders. Stock market assets mostly perform the investment (store of value) function whereas cryptocurrencies represent savings and investment as well as means of payment. While holding stock market assets is limited to those that can afford to invest part of their income, cryptocurrencies could be used by people in every income bracket. The change in wealth should result in the biggest change in consumption in lower income households, which usually do not own stock market assets because of their relatively higher propensity to consume. Hence, if cryptocurrencies are someday used as money, the cryptocurrency wealth effect could be stronger than the stock market wealth effect is nowadays. The cryptocurrency wealth effect could, therefore, affect consumption and the economy.

If the cryptocurrency wealth effect could affect the economy, the central bank would ideally want to manage the cryptocurrency exchange rate. The question is: Is that possible? The central bank cannot issue cryptocurrencies as it can fiat and is, therefore, limited in its ability to affect the cryptocurrency exchange rate. The central bank could, therefore, try to manage the cryptocurrency exchange rate in the same way that it manages the exchange rates against other fiat currencies. According to Ryan-Collins et al. (2012, ch. 6.4.2., pr. 3), "the central bank sets the price of the domestic currency in terms of a foreign currency. To maintain this peg, sufficient foreign exchange reserves are required, and sufficient access to the securities in which the foreign exchange reserves are held." Likewise, the central bank would require sufficient reserves of cryptocurrency to be able to maintain the cryptocurrency exchange rate at the desired level. There are potential problems with maintaining the foreign exchange rate peg. It is not possible to simultaneously maintain free capital flows, a fixed exchange rate and a sovereign monetary policy, i.e. to use monetary policy as a policy tool to fulfil particular national requirements. This is known as the Impossible Trinity (Ryan-Collins et al. 2012, ch. 6.4.3., pr. 2). The same problem would arise if the central bank tried to maintain a fixed cryptocurrency exchange rate. If fiat and cryptocurrency are used as money in the same country, the capital flows of cryptocurrency are free. This means that, according to the Impossible Trinity, the central bank would have to choose between a sovereign monetary policy (i.e. fiat price stability) and managing the cryptocurrency exchange rate.

Apart from some efficiencies, the use of cryptocurrency as money alongside fiat also brings a few issues for the financial system and monetary policy. Reduced seigniorage is certainly an undesired effect for the central bank. Higher transparency over the aggregate financial system could even accelerate a potential panic in the system. Even though monetary policy tools and transmission mechanisms are not significantly affected by the use of cryptocurrency, the central bank's reduced ability to affect the exchange rate between cryptocurrency and fiat also makes the central bank less able to mitigate the shocks coming through a possible cryptocurrency wealth effect. All these issues make the further adoption of cryptocurrency undesirable for the central bank. If central banks could prevent the rise of cryptocurrencies, they would not have to deal with these issues. One proposal to do so is for the central bank to issue central bank digital currency (CBDC) in order to compete with and prevail over cryptocurrencies.

3.4 Central bank digital currency

In response to the growing popularity of cryptocurrencies, there were two initial propositions for a central bank cryptocurrency in 2014. Motamedi (2014) proposed for the central bank to fork the Bitcoin protocol and create BitDollar. BitDollar would be the same as Bitcoin in every way except for the size of the mining rewards that would be determined by the central bank. By managing the size of newly mined bitdollars, the central bank could conduct monetary policy. BitDollar would serve as legal tender and the central bank would also act as the lender of last resort by being able to access an unlimited amount of bitdollars in such a case.

Koning (2014) proposed a similar solution in the form of Fedcoin. The Fedcoin proposition would additionally feature an anchored value of fedcoins to dollars with a 1:1 convertibility at the central bank. In this proposal, Koning (2014) already notes that Fedcoin would, along with some other institutions, also make Bitcoin obsolete. Both propositions would mean that the public could access central bank money directly, without being limited to cash.

The idea of offering central bank accounts to the general public is not new. Tobin (1985, p. 25) described deposited currency as full reserve deposit accounts held by individuals at the central bank in order to protect society's payment systems from interruptions and breakdowns due to bank failures. Even the proposed concept of CBDC is not new. It only recently gained prominence in central bankers' circles. Cryptocurrencies and their potential competition with fiat money encouraged the otherwise conservative central banks to research the topic and propose potential candidates for CBDC. These proposals will be examined, analysed and compared with cryptocurrencies and fiat money in the following chapters.

3.4.1 Review of CBDC proposals

There have been quite a few central bank projects inspired by cryptocurrencies and their underlying blockchain technology, but not all were meant to compete with cryptocurrencies as money. Central banks have explored and proposed some candidates for payment systems. The Bank of Canada, TMX Group, Payments Canada, Accenture and R3 (2018, p. 5) conducted project Jasper in which they evaluated the potential role of distributed ledger technology (DLT) in Canadian financial market infrastructures and any material benefits that could result from its adoption as wholesale payments and securities settlement for equities. The Monetary Authority of Singapore (2017) and The Association of Banks in Singapore developed software prototypes of three different models for decentralised interbank payment and settlement systems with liquidity savings mechanisms. These CBDCs are of the wholesale variety and would not be a true competition to cryptocurrencies. According to the survey of central banks performed by Barontini and Holden (2019, p. 7), some 70% of respondents are currently (or will soon be) engaged in CBDC work. An eighth of these are focusing on wholesale CBDCs while the rest will focus either on retail or will combine retail and wholesale CBDCs. Since only retail and combined CBDCs can compete with cryptocurrencies, wholesale CBDCs will be excluded from further analysis in this thesis and only the research in retail and combined CBDC developments will be presented.

The Riksbank's e-krona is one of most advanced propositions for a CBDC. According to the Sveriges Riksbank (2018, p. 14), "…the e-krona would be Swedish currency, in an account with the Riksbank, or a value that can be stored locally on, for instance, a card or in an app on a mobile phone. The e-krona would quite simply be a krona, the Swedish national currency and would have the same value as the krona in the form of cash or in an account with a private bank. Like cash, the e-krona would be issued by the Riksbank and have no credit or liquidity risk. The Riksbank would offer the volume of e-krona demanded by the general public in the same way that we issue the volume of cash in demand."

Within the foreseeable future, Sweden could become a practically cashless society. The general public's access to cash, which is risk-free assets in the form of central bank money, could almost entirely cease. An e-krona could constitute a government-guaranteed means of payment without credit risk and be available for the general public in digital form as a complement to cash. The Executive Board of the Riksbank sees a need to introduce digital central bank money made available to the general public (Sveriges Riksbank, 2017, pp. 5, 13).

On the technological side, the e-krona platform contains the central register for the holders of e-krona and the regulatory framework and conditions to be applied. It is, therefore, not decentralised. It combines an open access value-based e-krona for transactions below 250 EUR and an account-based e-krona for higher value transactions. The value-based e-krona also would not, as a rule, incur any interest which is possible for the account-based e-krona. The Riksbank proposes opening up its infrastructure where payment services can be built and offered to the general public. There is still a possibility for the Riksbank to offer a basic range of services (Sveriges Riksbank, 2018, pp. 16–20).

According to the Sveriges Riksbank (n.d.), no decisions have yet been taken on issuing an e-krona, but the Riksbank has started working on developing the solutions for a possible future e-krona and is now running a pilot project in order to develop a proposal for a technical solution for a CBDC (Sveriges Riksbank, 2020).

The Central Bank of Uruguay had issued and put in circulation Uruguayan peso notes in digital form. The e-peso was legal tender and, at the same time, an electronic platform. The pilot project was conducted from November 2017 to April 2018 by issuing 20,000,000 Uruguayan pesos in e-peso form. The e-pesos were used through a mobile application that acted as a digital wallet and provided instantaneous settlement. The e-peso worked on Unstructured Supplementary Service Data (USSD) that is part of the G2/GSM mobile network standard and does not require internet access (Bergara & Ponce, 2018, pp. 84, 86, 89).

According to Bergara and Ponce (2018, p. 90), a monetary policy analysis will dispose of granular information in real time with the e-peso, which is not available with physical cash. This should improve the efficiency of day-to-day monetary operations. On the other hand, the e-peso could introduce extra volatility to the velocity of the circulation of cash and the money multiplier, making day-to-day operations harder.

The Central Bank of The Bahamas is already implementing Project Sand Dollar. In the project, a CBDC is to be developed as a general purpose, digital version of the Bahamian dollar. A blockchain infrastructure has been proposed for the digital currency's technical underpinnings. The digital version of the Bahamian dollar is not supposed to be anonymous and user accounts should rely on national identity infrastructure (Rolle, 2019, p. 4). In October 2020, the Central Bank of The Bahamas announced they will gradually release a digital version of the Bahamian dollar through the existing financial intermediaries starting immediately (Central Bank of the Bahamas, n.d.).

The Bank of England was one of the first central banks publishing papers on CBDC. There has yet to be a concrete proposition on the issuance of CBDC by the Bank of England. The Bank of England analysed different design principles and balance sheet implications (Kumhof & Noone, 2018), the potential impact on the monetary transmission mechanism (Meaning, Dyson, Barker & Clayton, 2018), and constructed a model of CBDC as the basis for further research and discussion (Bank of England, 2020).

In April 2020, the People's Bank of China (PBoC) introduced a pilot CBDC in four large cities (Shenzhen, Suzhou, Chengdu and Xiong'an). The project is known internally as Digital Currency Electronic Payment or DCEP (Cheng, 2020). In August, the pilot was expanded to Beijing, Hong Kong, Macau, the Yangtze River Delta and the provinces of Guangdong, Tianjin and Hebei (Xiao, 2020). According to the deputy governor of PBoC Fan Yifei, China's DCEP is distributed through the existing financial intermediaries. It is intended to substitute only cash and not bank deposits. DCEP is supposed to be limited to small retail transactions by setting maximum daily and yearly limits. Like cash, DCEP also does not pay interest (Fan, 2020).

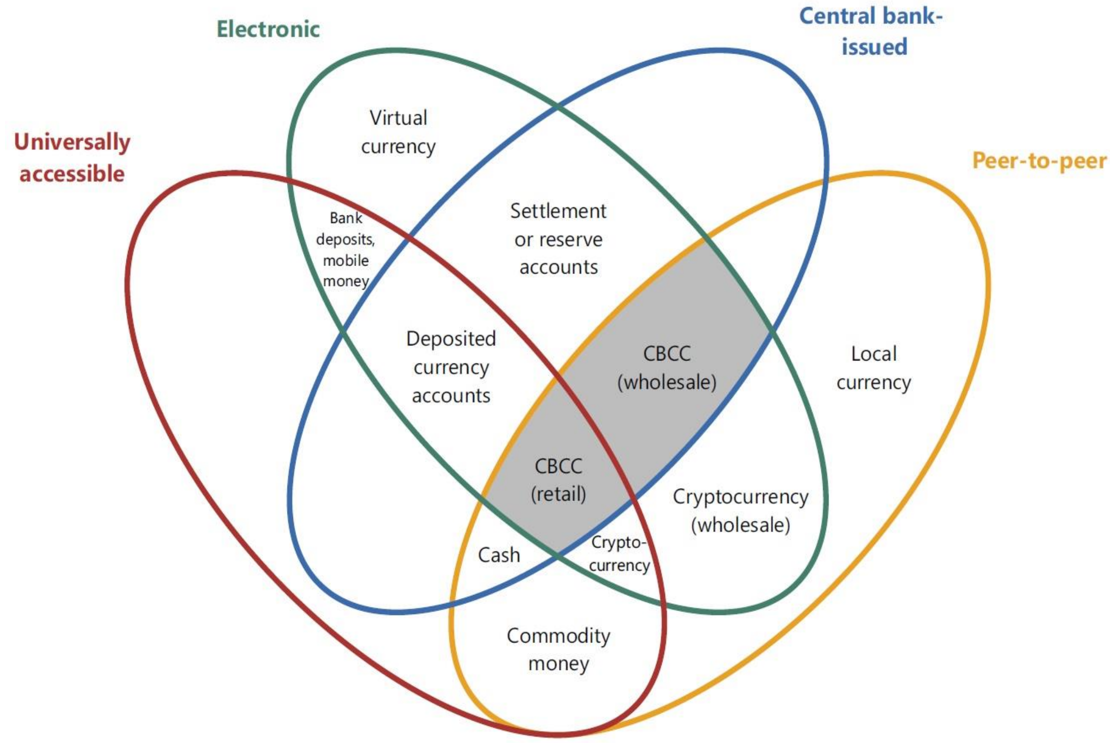
The Eastern Caribbean Central Bank is about to launch a CBDC version of the Eastern Caribbean dollar called DCash in four of the eight ECCB member countries, namely Antigua and Barbuda, Grenada, Saint Christopher (St. Kitts) and Nevis, and Saint Lucia. DCash is being distributed by the existing financial intermediaries (Eastern Caribbean Central Bank, n.d. a) (Eastern Caribbean Central Bank, n.d. b).

The ECB has issued a research report on the digital euro in October 2020. The decision on launching the digital euro is supposed to happen in the middle of 2021 (ECB, 2020b).

Other central banks and the International Monetary Fund have also conducted initial research into CBDCs. According to Barontini and Holden (2019, p. 12, 13), most central banks are conducting research into CBDCs, but are doing so with different speeds. Their survey also shows that central banks are proceeding cautiously, but also collaborating and sharing their work. In the next chapter, the CBDC model will be more comprehensively defined in order to compare it to cryptocurrencies.

Meaning et al. (2018, p. 4) define CBDC as "an electronic, fiat liability of a central bank that can be used to settle payments or as a store of value." In Figure 12, a Venn diagram can be clearly seen that shows the position of CBDC according to this definition and relative to other forms of money. CBDC tries to combine properties of fiat and cryptocurrency in order to offer the advantages of both. CBDC combines the stability of fiat and the efficiencies of cryptocurrencies. In order to harness the efficiencies from both, a different CBDC design needs to be thoroughly examined.

Figure 12: The money flower: a taxonomy of money



Source: Bech and Garratt (2017, p. 55).

The Sveriges Riksbank proposes two types of CBDC design; a value-based e-krona and a register-based e-krona. A register- or account-based e-krona is a variant of CBDC where the amount of e-kronas is attributed to an account and stored in a register. Value- or token-based e-kronas are stored on a physical medium (Sveriges Riksbank, 2017, pp. 19–21). An example of such a medium is a stored-value card used as a telephone calling card or public transport card. The advantage of a value-based e-krona is that it can make offline payments, but the disadvantage is that it requires closed-source hardware or software in order to prevent the copying of digital tokens. Preventing the forgeries of digital tokens in a value-based e-krona system could, from a technological point of view, become too complicated and costly to facilitate digital transactions which could successfully compete with cryptocurrencies. Like cryptocurrencies, account-based e-krona users only need a connection to the register and a way to authenticate themselves. After users are authenticated, they can perform transactions, and new balances arising from these transactions are written in the register. A register-based e-krona is, in fact, a system of deposit accounts at the Sveriges Riksbank. Other research makes a similar distinction between a value-based and account-based CBDC. Value-based CBDCs are not competitive compared to cryptocurrencies because they are too closed to enable the desired use. Besides this, it is already possible to make offline transactions using cash.

An account-based CBDC can have different levels of openness to its users. Wholesale CBDCs are accessible only to a closed circle of financial institutions or even only to commercial banks. Retail-based CBDCs are also meant to be used by households and businesses. There can be different ways of obtaining CBDC accounts. An account can be obtained just by generating a new account number and a private key as with cryptocurrencies. On the other hand, a central bank could authenticate every user before issuing them an account. A combination of both methods is also possible. Anonymous accounts could be generated by the users themselves, but would have limitations on storage and transaction values. Authenticated accounts would comply with know-your-customer (KYC) and anti-money laundering (AML) regulations and would enable their users to transact and store unlimited amounts. Anonymous accounts could be practical in replacing cash, but since CBDC is digital, numerous anonymous accounts could in principle be created without much effort. This could enable users to circumvent the limitations imposed on anonymous accounts and facilitate illicit transactions, the funding of terrorism, corruption and money laundering. Anonymous CBDC accounts are, therefore, not desired.

A CBDC can be denominated in a fiat unit or in a totally new unit. Most of CBDC propositions use the fiat unit. This is done in order to import the unit of account functionality and monetary policy from fiat to CBDC. This also means that CBDC has a stable exchange rate to fiat. It is only sensible for CBDC to use a new unit if the unit of account functionality and monetary policy are not successfully implemented in fiat, e.g. in a high inflation environment. By using the fiat unit, a CBDC has a de facto fixed exchange rate to fiat at 1:1. Since the central bank issues both fiat and CBDC, it is easy to regulate supply in order to maintain the fixed exchange rate.

Another design possibility is whether to pay interest on CBDC. Paying interest on CBDC could have an effect on monetary policy and bank deposits. CBDC can be implemented in a way which pays interest to all accounts at a 0% rate in the beginning. If there is a need for paying positive or negative interest, they can be implemented just by changing the parameter of the interest rate at a later date.

Since the CBDC debate was spurred by the onset of cryptocurrencies, it is sometimes proposed for CBDC to use blockchain or distributed ledger technology. Blockchain is a specific form of distributed ledger and is only necessary for consensus in trustless decentralised systems. In CBDC, central banks are the trusted party in a centralised system. The use of blockchain technology is, therefore, not necessary in a CBDC. This is especially important since blockchain technology requires a consensus mechanism, e.g. Proof-of-Work, which incurs some costs. This is why blockchain is not an appropriate technology for CBDC, which should, therefore, use either a centralised database register or a permissioned distributed ledger for storing transactions and account data.

3.5 Assessment of CBDC with regards to monetary policy and the financial environment

By implementing CBDC, central banks would also inevitably initiate a change in the financial environment. The CBDC would compete with and, up to a point, substitute cryptocurrencies, cash and deposits. From the point of view of the conclusions in the previous chapters in this thesis, the competition with cryptocurrencies is especially significant. Besides competing as money, a CBDC will also compete with private payment systems like credit and debit cards, PayPal and even interbank transfers. By introducing CBDC, which is a very liquid and risk-free asset, in a relatively significant volume, the positions in the financial industry would inevitably shift and that could have an effect on financial stability. The introduction of CBDC would, besides impacting the financial system, also change the monetary policy tools and the transmission mechanism. All of this will be examined in this chapter.

The CBDC substitution of cash and deposits would be even greater than the substitution by cryptocurrencies. This is a consequence of the benefits that stem from an active monetary policy used with CBDC. Cash would be substituted by CBDC mostly because of the digital efficiencies of CBDC over physical cash. CBDCs are, just like cash, issued by the state and use the same unit. This contributes to additional trust towards CBDC over cryptocurrencies and, therefore, makes CBDC more competitive than cryptocurrencies. One argument for introducing CBDC is providing access to the accounts at central banks and central bank money for everyone. This argument stems from the desire to provide equal and fair access to basic financial services for all businesses and residents. Financial access could be regarded as one of the basic human rights, like internet access is in some countries. Nowadays, access to accounts at central banks is usually limited to commercial banks and this gives banks a monopoly over digital transactions. The introduction of CBDC would in fact offer accounts at central banks to everyone and would break this monopoly. This would also increase financial inclusion. According to the World Bank (n.d.), 5% of the population in the euro area over 15 years old does not own a bank account. The share of the unbanked population is much higher in less developed countries. CBDC may be especially beneficial in increasing the financial inclusion for residents in places where commercial banks are closing their brick and mortar branch offices. According to Mancini-Griffoli et al. (2018, p. 16), CBDC could provide equal access to the means of payment for all citizens, including the ones living in areas underserved by banks. In some countries, cash use is diminishing. This is most notable in Sweden, where cash use is diminishing up to a point where the Riksbank fears that Swedish residents could lose access to any central bank liability. This is why the Riksbank is researching CBDC as a central bank liability that could replace cash. By substituting cash, CBDC could also facilitate phasing out the issuance of large-denomination paper currency bills, as argued by Rogoff (2016), in order to inhibit criminal activity, money laundering and tax evasion. Providing access to cash is also associated with significant costs. According to Mancini-Griffoli et al. (2018, p. 16), the costs of 0.5 percent of the GDP are associated with providing cash. By adopting CBDC and lowering the costs associated with providing cash, financial institutions could offer their services at lower fees and in less profitable customer segments and less profitable areas.

CBDC would also substitute bank deposits. The reason for that is CBDC's higher liquidity and the lack of risk compared to bank deposits. The degree of substitution is dependent on CBDC design, the existing environment and the response of commercial banks. The introduction of CBDC would break the monopoly of commercial banks which are usually the only group able to access bank reserves and use them for final settlement. According to Dyson and Hodgson (2016, p. 9), by issuing CBDC, the central bank would enable new entrants to offer payment accounts and payment services that would not be dependent on the access to the balance sheets of incumbent commercial banks. This would free such potential competitors from the cost and usage constraints imposed by the incumbent banks, allowing new entrants to provide competition to the banks in the form of technical innovation and customer service. Besides providing additional competition, CBDC would also diminish the need for intermediaries since CBDC holders could make transactions without them. The reduced need for intermediaries would lead to lower costs and shorter times needed to complete transactions. A shorter CBDC transaction time in comparison to bank transfer transaction time is also a consequence of the banks' use of netting when they settle in bank reserves. The longer banks wait to settle, the more transactions are collected and more transactions can be netted between two banks. This enables commercial banks to use less bank reserves to complete transactions. Because CBDC transactions are instant and, therefore, do not use settlement netting, CBDC transactions need the full amount of funds to perform a transaction. This means that there will be additional CBDC assets needed in order to enable the same volume of transactions as would be done through bank transfers. According to Dyson and Hodgson (2016, p. 34), this could drain the bank reserves of commercial banks in the beginning of the issuance of CBDC. If clients would want to convert deposits into CBDC and withdraw them from their accounts, commercial banks would have to convert their bank reserves at the central bank in order to gain enough CBDC. To mitigate this drain on bank reserves, CBDC should be introduced gradually and with consideration for the concurrent financial environment. The central bank should also provide additional liquidity as a lender of last resort if needed. The Committee on Payments and Market Infrastructures and Markets Committee (2018, p. 26) also note that the introduction of CBDC would have an effect on seigniorage. The issuance of CBDC may be less costly than the issuance of banknotes and coins, but the central bank could incur costs by paying interest on CBDC, which is not the case in the case of cash. The net effect of CBDC substituting cash on seigniorage would depend on the specific cost of issuance and the interest rate paid on CBDC. CBDC substituting bank deposits would increase seigniorage. The Committee on Payments and Market Infrastructures and Markets Committee (2018, p. 26) note that "any asset that the central bank may buy from, lend to, or accept as collateral from its monetary counterparties should have an expected yield above the expected risk-free rate over the investment horizon." CBDC would pay an interest rate appropriate to its risk-free nature which would, therefore, mean a positive effect of CBDC substitution of bank deposits on seigniorage.

Dyson and Hodgson (2016, pp. 29, 30) state that the introduction of CBDC may make banks less willing or able to lend because a loan that was made by a commercial bank can now be converted to CBDC and withdrawn. As stated above, this could drains the banks' reserves. Banks will, therefore, need to try to persuade its customers to hold their money with them in either CBDC or bank deposit form. Commercial banks could also try to attract investors with better services, security and higher interest rates. According to Mancini-Griffoli et al. (2018, p. 21), the lack of deposits would lead to a higher deposit interest rate aimed at attracting deposits and, depending on the market power of the bank, a further increase in the lending interest rate to preserve the bank's profits. Andolfatto's (2018, p. 24) model and analysis suggest that CBDC would increase the financial inclusion and raise the interest rates. The analysis also concludes that CBDC needs not have any impact on bank intermediation and that only bank monopoly profits would lower.

3.5.1 CBDC's effect on financial stability

Any major change in the financial environment has the potential to affect financial stability. According to Dyson and Hodgson (2016, p. 9), the introduction of CBDC as a risk-free substitute for bank deposits would make possible the elimination of a degree of liquidity and credit risk within the financial sector as a whole. This, in fact, enables the separation of credit risk and the payment system. The state is also liberated of providing deposit guarantees on CBDC, which substitute bank deposits. This would also diminish the potential source of moral hazard stemming from the deposit guarantee. Bordo and Levin (2017, p. 20) also argue that payment networks typically exhibit substantial externalities and increasing returns to scale. Such payment systems might well become quasi-monopolistic and any significant operational problem within the payment network could pose a substantial risks to the entire financial system and to the macroeconomy. CBDCs represent a welcome competition that would prevent such a scenario from unfolding. In the case of potential disturbances on the financial market, CBDCs enable the central bank to see the financial flows in real time and without the netting effects of settling that could obscure actual flows. The overview of the flows of CBDC would bring a lot of additional information about the economy that could be used in determining future monetary policy.

Besides all of the above-mentioned effects, the issuance of CBDC would also introduce a very liquid digital asset. Some express fears that CBDC could be used as a very capable flight-to-safety vehicle. The Committee on Payments and Market Infrastructures and Markets Committee (2018, p. 16) count the flight away from private financial institutions and markets towards the central bank as the most significant and plausible financial stability risk of introducing CBDC. Further, the Committee on Payments and Market Infrastructures and Markets Committee argue that unlike cash, CBDC would enable "digital runs" towards the central bank with unprecedented speed and scale. Kumhof and Noone (2018, pp. 8, 9) argue that a solution for this is to have a distinction between CBDC and bank reserves and for them not to be convertible on demand into each other. Another solution presented by Kumhof and Noone (2018, pp. 15, 16) is not to guarantee convertibility between bank deposits and CBDC. These solutions, on the other hand, require additional measures to maintain the parity between bank deposits and central bank money. However, Meaning et al. (2018, p. 14) argue that depositors that are the most sensitive to credit risk would substitute deposits with CBDC over a period of time after CBDC had first been introduced and thus the probability of a run, for a given level of risk, may be lower when a safe outside option such as CBDC had already been provided. One could also argue that the gradual flow of deposits towards CBDC and the possibility of bank runs would bring tighter discipline in the banking sector and, as such, even increase financial stability.

3.5.2 CBDC's effect on monetary policy

CBDC would also significantly change the workings of monetary policy. Since CBDC shares the same unit of account and has the same issuer as bank reserves, it could also share the same monetary policy. This, of course, means that CBDC is pegged to bank reserves and is as stable in value as regular fiat money. If the central bank chooses to pay an interest rate to CBDC holders, the CBDC interest rate could become a significant monetary policy tool. Questions arising from this are: How should the CBDC rate be set? Should the CBDC rate be zero? Should the CBDC rate be the same as or different than the policy rate? According to Engert and Fung (2017, p. 19), since CBDC and bank reserves are substitutes, both being riskless and very similar in functionality, any spread between interest rates on reserves and a CBDC interest rate would provide an arbitrage opportunity for the banks. The Committee on Payments and Market Infrastructures and Markets Committee (2018, p. 13), on the other hand, warn that, depending on the degree of substitution, a larger balance sheet may be needed to implement monetary policy as agents substitute physical cash, commercial bank deposits and other safe assets for CBDC.

According to Dyson and Hodgson (2016, p. 31), the rate paid on CBDC would set the floor for the rates paid by banks on bank deposits. This means that the setting of the CBDC interest rate could directly affect a much bigger part of the money supply than the policy rate can. Since the central bank could directly set an effective rate on CBDC, forward guidance could be much more credible than by using a policy rate that has to be further translated to the interbank market through the transmission mechanism. Mancini-Griffoli et al. (2018, p. 25) state that the transmission mechanism would strengthen because the introduction of CBDC would increase the financial inclusion and expose more households and firms to interest-sensitive borrowing and saving instruments. They also state that the transmission mechanism would strengthen if the lack of bank deposits, induced by the introduction of CBDC, would force commercial banks to increase the share of the banks' wholesale funding. Meaning et al. (2018, p. 17) note that introducing CBDC would cause a fundamental change in the interbank market. The interbank market would become open to anyone and commercial banks could borrow and lend CBDC from and to the general public. Further, Meaning et al. (2018, p. 18) argue that an open interbank market would make it more likely for CBDC to be lent at longer terms than traditional reserves. These CBDC loans would give rise to a term structure on central bank money that was based on the expectations of the overnight rate over the term of the loan. All this would straighten the transmission mechanism.

One of most prominent benefits of introducing CBDC is that it could help with overcoming the zero lower bound (ZLB) constraint for the policy rate imposed by the availability of cash. Because cash is remunerated at 0%, any significant dip of the interest rate below 0% is supposed to encourage flows from bank deposits towards cash. Cash, therefore, makes interest rates below ZLB inefficient as a monetary policy tool. CBDC could help to eliminate cash from circulation by substituting it. Masciandaro (2018, p. 546) states that if individuals are sensible to the technological properties of electronic currencies, then the demand for electronic currencies will completely replace the demand for paper currencies. The higher utility of CBDC relative to cash alone would probably not suffice for CBDC to substitute cash in its entirety. Bordo and Levin (2017, p. 12) argue that the flight from deposits' negative rates to cash could be made unprofitable by imposing substantial fees on relatively large or frequent transfers to and from cash. Bordo and Levin (2017, p. 13) also argue that by being able to overcome ZLB, there would be no need for the inflationary buffer of 2% that currently represents the target of a 2% inflation for major central banks. CBDC can overcome the ZLB constraint if the CBDC interest rate is not equal to 0% like it is for cash. This is another argument in favour for CBDC to be remunerated. If the CBDC interest rate would equal 0%, CBDC would even exacerbate the ZLB constraint.

CBDC could help monetary policy around ZLB even before cash is significantly substituted. Dyson and Hodgson (2016, p. 8) propose to use CBDC as a distribution channel for a form of quantitative easing called helicopter money. Friedman (1969, pp. 4, 5) proposes helicopter money as a one-time transfer of money directly to the general public in equal amounts. Members of the public are supposed to spend this money and, therefore, create additional demand that would eventually stimulate growth.

The introduction of CBDC would provide equal access to digital central bank money for everyone. This would break the monopoly over digital central bank money held by commercial banks and increase competitiveness in the banking sector. The introduction of CBDC would also cause an increase in financial inclusion and the efficiency of transfers. The consequences stemming from the introduction of CBDC are also the relatively higher interest rates and the strengthening of the transmission mechanism. CBDC should be introduced gradually. A properly implemented CBDC would also eliminate the ZLB constraint. The potentially most disruptive and unpredictable issue is the possibility of the increased strength of digital bank runs caused by the implementation of CBDC. Depending on the view of the author, there are also different solutions prescribed for the issue. In any case, there should be additional care taken when implementing CBDC to preserve financial stability. What is still to be determined is whether the CBDC interest rate and the policy rate should be the same, and if there is a need for the separation of the bank reserves and CBDC.

3.6 Comparison of fiat, cryptocurrency and CBDC

CBDC represents a possible upgrade of the current fiat system, but it also stands as an alternative to the possible adoption of cryptocurrencies. In the near future, monetary authorities need to decide if they want to introduce CBDC or stick with the current system and allow for the possibility of cryptocurrencies assuming the position of digital cash.

Table 4: Main differences between fiat, cryptocurrency and CBDC

Properties	Fiat	Cryptocurrency	CBDC
Efficiency of transactions	Dependent on the complexity of the transaction	Fast and cheaper, especially when fiat needs many intermediaries.	Can be even more efficient than cryptocurrencies
Risk	Low	High	Even lower risk than bank deposits
Competitiveness of banking sector	Low	Could increase	Increased by a significant amount
Effect on Financial inclusion	Stays the same	Increased	Increased
Change in seigniorage relative to current system	None	Lower seigniorage	Positive effect relative to the amount of substituted bank deposits
Effect on financial stability	Potentially negative if cash use diminishes	Potential negative effects due to cryptocurrency deposits and higher transparency	Potential positive and negative effects
Change in monetary policy effectiveness	None	Negative due to the cryptocurrency wealth effect	Positive due to the strengthened transmission mechanism and the elimination of ZLB

Source: Own work.

In Table 4, the advantages and disadvantages of the current fiat system, cryptocurrency adoption and CBDC are shown. Cryptocurrencies would, compared to the current fiat system, offer more economical transactions and an increase in financial inclusion. On the other hand, cryptocurrencies involve high risk, would lower seigniorage, could negatively affect financial stability, and make the implementation of monetary policy more difficult. Monetary authorities can let cryptocurrencies grow slowly and risk their adoption. Another possibility is to take a proactive approach and introduce CBDC. CBDC is favourably compared to cryptocurrencies in all examined areas. Even without the threat of cryptocurrencies, CBDCs are favourable to the current fiat system. The only issue for CBDC implementation is the potential digital bank runs. These can be prevented, especially if sufficient care is taken in the design of CBDC and with gradual implementation.

4 CONCLUSION

With the invention of Bitcoin and subsequent cryptocurrencies, a new technology, which could potentially redefine the world of money, was born. The technological innovation behind these decentralised digital currencies involves the use of a distributed database, cryptography and Proof-of-Work, with the aim of making a new form of money. Because cryptocurrencies are open source, technological innovations are not limited to Bitcoin, but are used in many different cryptocurrencies. Since technological and social progress is inevitable and Bitcoin is only one example of cryptocurrencies, it is important to define cryptocurrencies as a group and analyse their properties as a whole. The most important and disruptive distinction of cryptocurrencies compared to the established forms of money is their independence from the existing financial intermediaries and closed payment system networks. This independence gives cryptocurrencies the possibility of being more efficient in performing transactions. At the same time, this also makes cryptocurrencies independent from the government and, consequently, from the central bank. As of 2020, this independence does not yet pose any problems for central banks due to the low levels of adoption of cryptocurrencies.

It is clear to anyone making payments nowadays that cryptocurrencies do not yet pose a true competition to fiat currencies. Cryptocurrencies have a poor performance of the functions of money when compared to the performance of fiat currencies. The main causes for this poor performance are the low acceptance, the high volatility of cryptocurrency exchange rates, the lower liquidity and the knowledge gap. These properties have been slowly improving since cryptocurrencies were first established and they could improve even further in the future. There is, however, one substantial obstacle that may prevent existing cryptocurrencies from ever achieving as low a volatility as a well-managed fiat currency has. The supply of existing cryptocurrencies is predetermined and cannot react to the fluctuations in demand. Additional (but potentially technically solvable) obstacles are also the scalability and the energy consumption of cryptocurrencies in the case of higher adoption. Cryptocurrencies also have some advantages over fiat money, in particular their independence from intermediaries and their digital (IT) nature. Even though cryptocurrencies cannot compete with fiat currency in the performance of the functions of money right now, the current obstacles may be technically solvable, which means that cryptocurrencies could perform the functions of money better than fiat money in the future. This is not certain by any means, but it is a possibility that makes cryptocurrencies interesting for analyses.

The significant adoption of cryptocurrencies could have an effect on the monetary system and monetary policy. When monetary policy effects pass through the interbank market, they affect the real economy through the transmission mechanism. The transmission mechanism is, at the present, not affected by the presence of cryptocurrencies. The transmission mechanism mostly works through channels that affect credit creation and cryptocurrencies are currently not used for credit creation. The monetary authority's ability to conduct monetary policy is, therefore, not significantly affected. However, in the case of significant cryptocurrency adoption, the implications for monetary policy could be different. In the case of higher adoption, there is a new part of the money supply present in the form of cryptocurrency that is used by households and companies. The central bank has no direct control over cryptocurrency supply and also cannot control the exchange rate between cryptocurrency and fiat and conduct independent monetary policy at the same time. Any shock to cryptocurrency demand would, therefore, have an effect on the cryptocurrency exchange rate and on the economy through a cryptocurrency wealth effect. Cryptocurrencies could, therefore, have a negative influence on the monetary authorities' ability to conduct monetary policy and achieve its price stability objective in the future.

Central bank digital currencies (CBDCs) are a potential competitor to cryptocurrencies that could prevent cryptocurrencies from achieving significant adoption. Not only would CBDCs compete with cryptocurrencies, but they would also bring with them additional benefits in the form of an increased competitiveness of the banking sector, payment systems, financial inclusion and a higher efficiency of transactions. In the case of CBDC adoption, monetary policy would also benefit from a stronger transmission mechanism and the elimination of the zero lower bound constraint. There is still an open question of the possibility of stronger bank runs enabled by the implementation of CBDC. Different authors argue whether this is a potential problem or not, but also offer solutions for it. CBDC could, therefore, be used as an efficient competition to cryptocurrencies.

REFERENCE LIST

1. 1ML.com. (n.d.). *Lightning Network Statistics*. Retrieved May 12, 2020, from https://1ml.com/statistics
2. Acheson, N. (2018, February 22). *What is SegWit?* Retrieved August 3, 2019, from https://www.coindesk.com/information/what-is-segwit
3. Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014a). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, Q3.
4. Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014b). The economics of digital currencies. *Bank of England Quarterly Bulletin*, Q3.
5. Andolfatto, D. (2018). Assessing the Impact of Central Bank Digital Currency on Private Banks. *Federal Reserve Bank of St. Louis, Working Papers, 2018*(026). https://doi.org/10.20955/wp.2018.026
6. Antonopoulos, A. M. (2015). *Mastering bitcoin* (First edition). O'Reilly.

7. Bank for International Settlements. (2019). *Triennial Central Bank Survey—Foreign exchange turnover in April 2019* (Triennial Central Bank Survey, p. 23). Bank for International Settlements.

8. Bank of Canada, TMX Group, Payments Canada, Accenture, & R3. (2018). *Jasper phase iii: Securities settlement using distributed ledger technology*. Retrieved July 10, 2019, from: https://www.payments.ca/sites/default/files/jasper_phase_iii_whitepaper_final_0.pdf

9. Bank of England. (2020). *Central Bank Digital Currency: Opportunities, challenges and design*. Retrieved December 5, 2019, from: https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593

10. Bariviera, A. F., Basgall, M. J., Hasperué, W., & Naiouf, M. (2017). Some stylized facts of the Bitcoin market. *Physica A: Statistical Mechanics and Its Applications*, *484*, 82–90. https://doi.org/10.1016/j.physa.2017.04.159

11. Barontini, C., & Holden, H. (2019). *Proceeding with caution: A survey on central bank digital currency*. Bank for International Settlements & Monetary and Economic Department, Eds.

12. Bashir, I. (2018). *Mastering blockchain: Distributed ledgers, decentralization, and smart contracts explained* (2. edition, fully revised and updated). Packt Publishing.

13. Baur, D. G., & Dimpfl, T. (2017). *Realized Bitcoin Volatility*. SSRN. https://doi.org/10.2139/ssrn.2949754

14. Bech, M., & Garratt, R. (2017). Central bank cryptocurrencies. *BIS Quarterly Review September, 2017*.

15. Bech, M., & Hancock, J. (2020). Innovations in payments. *BIS Quarterly Review March 2020*.

16. Bergara, M., & Ponce, J. (2018). Central bank digital currency: The Uruguayan e-peso case. *Do We Need Central Bank Digital Currency? Economics, Technology and Institutions*. SUERF, Viena

17. Bernhardsen, T., & Kloster, A. (2010). *Liquidity management system: Floor or corridor?* Retrieved September 2, 2019, from: http://www.norges-bank.no/upload/publikasjoner/staff%20memo/2010/staff_memo_0410.pdf

18. Bitcoin Forum. (n.d. a). *[PATCH] increase block size limit*. Retrieved March 11, 2019, from https://bitcointalk.org/index.php?topic=1347.msg15139#msg15139

19. Bitcoin Forum. (n.d. b). *Why the fuck did Satoshi implement the 1 MB blocksize limit?* Retrieved March 11, 2019, from https://bitcointalk.org/index.php?topic=2786690.0

20. Bitcoin Wiki (n.d. a). *Block.* Retrieved May 14, 2020, from https://en.bitcoin.it/wiki/Block

21. Bitcoin Wiki (n.d. c) *Satoshi (unit)*. Retrieved February 9, 2018, from https://en.bitcoin.it/wiki/Satoshi_(unit)

22. Bitcoin Wiki. (n.d. b). *Controlled supply*. Retrieved October 8, 2015, from https://en.bitcoin.it/wiki/Controlled_supply

23. Bitcoin.com. (n.d.). *Price volatility*. Retrieved November 29, 2020, from https://charts.bitcoin.com/btc/chart/price-volatility#5m9s

24. BitInfoCharts. (n.d.). *Bitcoin, Ethereum Avg. Transaction Fee chart*. Retrieved December 6, 2018, from https://bitinfocharts.com/

25. Blockchain.com. (n.d.). *Blockchain Size*. Retrieved September 7, 2019, from https://www.blockchain.com/charts/blocks-size

26. Board of Governors of the Federal Reserve System. (n.d.). *M2 Money Stock*. Retrieved October 25, 2020, from https://fred.stlouisfed.org/series/M2

27. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, *29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

28. Bolt, W., & van Oordt, M. R. C. (2016). On the Value of Virtual Currencies. *Staff Working Paper 2016-42*. Bank of Canada.

29. Boone, L., Giorno, C., & Richardson, P. (1998). Stock Market Fluctuations and Consumption Behaviour: Some Recent Evidence. *OECD Economics Department Working Papers No. 208*. https://doi.org/10.1787/853414662323

30. Bordo, M., & Levin, A. (2017). *Central Bank Digital Currency and the Future of Monetary Policy* (No. w23711). National Bureau of Economic Research. https://doi.org/10.3386/w23711

31. Buterin, V. (2014, July 5). *On Stake*. Retrieved March 15, 2019, from https://blog.ethereum.org/2014/07/05/stake/

32. Caffyn, G. (2014, May 22). *Bitcoin Pizza Day: Celebrating the Pizzas Bought for 10,000 BTC*. Retrieved September 8, 2019, from https://www.coindesk.com/bitcoin-pizza-day-celebrating-pizza-bought-10000-btc

33. Case, K., Quigley, J., & Shiller, R. (2013). *Wealth Effects Revisited: 1975-2012* (No. w18667). National Bureau of Economic Research. https://doi.org/10.3386/w18667

34. Cecchetti, S. G., & Schoenholtz, K. L. (2015). *Money, banking, and financial markets* (Fourth Edition). McGraw-Hill Education.

35. Central Bank of the Bahamas. (n.d.). *The Sand Dollar is on Schedule for Gradual National Release to The Bahamas in mid-October 2020*. Retrieved December 5, 2020,

from https://www.centralbankbahamas.com/news/public-notices/the-sand-dollar-is-on-schedule-for-gradual-national-release-to-the-bahamas-in-mid-october-2020

36. Cheng, J. (2020, April 20). *China Rolls Out Pilot Test of Digital Currency*. Retrieved December 6, 2020, from https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339

37. Cho, S. (2006). Evidence of a stock market wealth effect using household level data. *Economics Letters*, *90*(3), 402–406. https://doi.org/10.1016/j.econlet.2005.09.006

38. Coin Metrics. (n.d.). *Tools*. Retrieved November 29, 2020, from https://coinmetrics.io/tools/

39. CoinMarketCap. (n.d. a). *All Cryptocurrencies*. Retrieved October 25, 2020, from https://coinmarketcap.com/all/views/all/

40. CoinMarketCap. (n.d. b). *Cryptocurrency Market Capitalizations*. Retrieved March 10, 2020, from https://coinmarketcap.com/

41. Committee on Payments and Market Infrastructures & Markets Committee. (2018). *Central bank digital currencies*. BIS. Retrieved July 6, 2019, from https://www.bis.org/cpmi/publ/d174.pdf

42. Committee on Payments and Market Infrastructures. (2015). *Digital currencies*. BSI. Retrieved July 19, 2016, from https://gla.news/wp-content/uploads/2015/11/Digital-Currencies.pdf

43. Committee on Payments and Market Infrastructures. (2018). *Cross-border retail payments*. BSI. Retrieved May 12, 2020, from https://www.bis.org/cpmi/publ/d173.htm

44. Craig, M. (2015, February 5). *The Race to Replace Bitcoin*. Retrieved June 7, 2015, from http://observer.com/2015/02/the-race-to-replace-bitcoin/

45. Curran, B. (2018a, May 11). *What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide*. Retrieved March 15, 2019, from https://blockonomi.com/practical-byzantine-fault-tolerance/

46. Curran, B. (2018b, July 13). *What is Sharding? Guide to this Ethereum Scaling Concept Explained*. Retrieved March 11, 2019, from https://blockonomi.com/sharding/

47. Digiconomist. (n.d.). *Bitcoin Energy Consumption Index*. Retrieved November 29, 2020, from https://digiconomist.net/bitcoin-energy-consumption

48. Dynan, K. E., & Maki, D. M. (2001). Does Stock Market Wealth Matter for Consumption? *Finance and Economics Discussion Series 23*(2001). https://doi.org/10.2139/ssrn.270190

49. Dyson, B., & Hodgson, G. (2016). *Why Central Banks Should Start Issuing Electronic Money*. Positive Money Retrieved July 5, 2019, from https://positivemoney.org/wp-content/uploads/2016/01/Digital_Cash_WebPrintReady_20160113.pdf

50. Eastern Caribbean Central Bank. (n.d. a). *About the Project*. Retrieved December 5, 2020, from https://www.eccb-centralbank.org/p/about-the-project

51. Eastern Caribbean Central Bank. (n.d. b). *ECCB Moves Closer to Launching Digital EC Currency (DCash).* Retrieved December 6, 2020, from https://www.eccb-centralbank.org/news/view/eccb-moves-closer-to-launching-digital-ec-currency-dcash

52. ECB. (2011). *The monetary policy of the ECB, 2011* (3rd ed.). ECB.

53. ECB. (2012). *Virtual currency schemes*. ECB.

54. ECB. (2015). *Virtual currency schemes a further analysis*. ECB.

55. ECB. (2017). *TARGET Annual Report 2017*. ECB.

56. ECB. (2020a, May 20). *Official interest rates*. Retrieved December 5, 2019, from https://www.ecb.europa.eu/stats/policy_and_exchange_rates/key_ecb_interest_rates/html/index.en.html

57. ECB. (2020b, November 6). *A digital euro*. Retrieved December 6, 2020, from https://www.ecb.europa.eu/euro/html/digitaleuro.en.html

58. ECB. (n.d. a). *As of 1 October 2019 EONIA is calculated with a reformed methodology tracking the euro short-term rate*. Retrieved May 20, 2020, from https://sdw.ecb.europa.eu/quickview.do?SERIES_KEY=198.EON.D.EONIA_TO.RATE&start=01-01-

59. ECB. (n.d. b). *Monetary aggregates*. Retrieved December 5, 2020, from http://sdw.ecb.europa.eu/reports.do?node=1000005717

60. ECB. (n.d. c). *Definition of price stability*. Retrieved February 20, 2018, from https://www.ecb.europa.eu/mopo/strategy/pricestab/html/index.en.html

61. Einzig, P. (1966). *Primitive money: In its ethnological, historical and economic aspects* (Second edition). Pergamon Press.

62. Engert, W., & Fung, B. S. C. (2017). Central Bank Digital Currency: Motivations and Implications. *Staff Discussion Paper 16*(2017)

63. Erhardt, M. (2018, February 3). *Excited for Schnorr signatures*. Retrieved March 8, 2019, from https://hackernoon.com/excited-for-schnorr-signatures-a00ee467fc5f

64. Ethereum Foundation. (n.d. a). *What is Ether*. Retrieved February 9, 2018, from https://www.ethereum.org/ether

65. Ethereum Foundation. (n.d. b). *What is Ethereum?* Retrieved March 24, 2020, from https://ethereum.org/what-is-ethereum/

66. EthHub. (n.d.). *Ethereum Mining*. Retrieved May 14, 2020, from https://docs.ethhub.io/using-ethereum/mining/#block-times

67. European Payments Council. (2018, January). *10 interesting facts about SEPA*. Retrieved March 7, 2019, from https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2018-01/EPC%20infographic_10%20SEPA%20facts.pdf

68. Fan, Y. (2020, April 1). *Some thoughts on CBDC operations in China*. Retrieved December 5, 2020, from https://www.centralbanking.com/node/7511376

69. Friedman, M. (1969). *The Optimum Quantity of Money and Other Essays*. Chicago: Aldine

70. Hartmann, M., Hernandez, L., Plooij, M., & Vandeweyer, Q. (2019). *Are instant retail payments becoming the new normal?* ECB.

71. Hertig, A. (2016, July 28). *Ethereum's Two Ethereums Explained*. Retrieved October 2, 2018, from https://www.coindesk.com/ethereum-classic-explained-blockchain/

72. Hertig, A. (n.d.). *How Will Ethereum Scale?* Retrieved March 7, 2019, from https://www.coindesk.com/information/will-ethereum-scale

73. Jevons, W. S. (1896). *Money and the Mechanism of Exchange*. D. Appleton and Company.

74. Kokkola, T. (2011). *The payment system payments, securities and derivatives, and the role of the Eurosystem*. ECB.

75. Koning, J. (2014, October 19). *Moneyness: Fedcoin*. Retrieved July 9, 2019, from http://jpkoning.blogspot.com/2014/10/fedcoin.html

76. Kumhof, M., & Noone, C. (2018). Central Bank Digital Currencies—Design Principles and Balance Sheet Implications. *Bank of England Working Paper No. 725*. https://doi.org/10.2139/ssrn.3180713

77. Kwaasteniet, A. de. (2018, November 30). *The nonsense of…. TPS (transactions per second)*. Retrieved March 7, 2019, from https://medium.com/@aat.de.kwaasteniet/the-nonsense-of-tps-transactions-per-second-2d7156df5e53

78. Laughlin, J. L. (1903). *The principles of money*. Charles Scribner's Sons.

79. Leinonen, H., & Soramaki, K. (2000). Optimizing Liquidity Usage and Settlement Speed in Payment Systems. *Bank of Finland Discussion Papers, 16*(99). https://doi.org/10.2139/ssrn.228249

80. Litecoin Wiki. (n.d.). *Comparison between Litecoin and Bitcoin.* Retrieved March 12, 2020, from https://litecoin.info/index.php/Comparison_between_Litecoin_and_Bitcoin

81. Mancini-Griffoli, T., Martinez, M. S., Agur, I., Ari, A., Kiff, J., Popescu, A., & Rochon, C. (2018). *Casting Light on Central Bank Digital Currency*. International Monetary Fund. doi: https://doi.org/10.5089/9781484384572.006

82. Mankiw, N. G., & Zeldes, S. P. (1991). The consumption of stockholders and nonstockholders. *Journal of Financial Economics, 29*(1), 97–112. https://doi.org/10.1016/0304-405X(91)90015-C

83. Marshall, B. R., Nguyen, N. H., & Visaltanachoti, N. (2018). *Bitcoin Liquidity*. SSRN. https://doi.org/10.2139/ssrn.3194869

84. Martinez, J. (2015, February 20). *Math-based Currency*. Retrieved June 7, 2015, from https://ripple.com/knowledge_center/math-based-currency/

85. Masciandaro, D. (2018). Central Bank Digital Cash and Cryptocurrencies: Insights from a New Baumol-Friedman Demand for Money: Central Bank Digital Cash and Cryptocurrencies. *Australian Economic Review, 51*(4), 540–550. https://doi.org/10.1111/1467-8462.12304

86. McKinsey Financial Services Practice. (2016). *Global payments 2016: Strong fundamentals despite uncertain times*. McKinsey & Company

87. Meaning, J., Dyson, B., Barker, J., & Clayton, E. (2018). Broadening Narrow Money: Monetary Policy with a Central Bank Digital Currency. *Bank of England Working Paper No. 724*. https://doi.org/10.2139/ssrn.3180720

88. Menger, C. (2009). *The Origins of Money*. Ludwig von Mises Institute.

89. Merriam-Webster Dictionary. (n.d.). *Definition of cryptocurrency*. Retrieved April 7, 2020, from https://www.merriam-webster.com/dictionary/cryptocurrency

90. Mishkin, F. S. (2009). *The economics of money, banking, and financial markets* (9th ed. (and the 2nd ed. of the business ed.)). Addison-Wesley.

91. Moenjak, T. (2014). *Central banking: Theory and practice in sustaining monetary and financial stability*. Wiley & Sons. http://site.ebrary.com/id/10891187

92. Monetary Authority of Singapore. (2017, October 5). *MAS and ABS lead consortium to harness blockchain technology for more efficient inter-bank payments*. Retrieved July 10, 2019, from https://www.mas.gov.sg/news/media-releases/2017/mas-and-abs-lead-consortium-to-harness-blockchain-technology

93. Motamedi, S. (2014, July 21). *Will Bitcoins Ever Become Money? A Path to Decentralized Central Banking.* Retrieved July 9, 2019, from https://tannutuva.org/2014/will-bitcoins-ever-become-money-a-path-to-decentralized-central-banking/

94. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved December 12, 2018, from https://bitcoin.org/bitcoin.pdf

95. Nelson, B. (2018). Financial stability and monetary policy issues associated with digital currencies. *Journal of Economics and Business, 100*, 76–78. https://doi.org/10.1016/j.jeconbus.2018.06.002

96. OpenDataSoft. (n.d.).*Coinmap - Venues accepting Bitcoin*. (n.d.). Retrieved September 5, 2019, from https://data.opendatasoft.com/explore/dataset/coinmap@public/export/?dataChart=eyJxdWVyaWVzIjpbeyJjaGFydHMiOlt7InR5cGUiOiJjb2x1bW4iLCJmdW5jIjoiQ09VTlQiLCJ5QXhpcyI6ImxvbiIsInNjaWVudGlmaWNEaXNwbGF5Ijp0cnVlLCJjb2xvciI6IiMyQzNGNTYifV0sInhBeGlzIjoiY3JlYXRlZF9vbiIsIm1heHBvaW50cyI6bnVsbCwic29ydCI6IiIsInRpbWVzY2FsZSI6Im1vbnRoIiwiY29uZmlnIjp7ImRhdGFzZXQiOiJjb2lubWFwQHB1YmxpYyIsIm9wdGlvbnMiOnt9fX1dLCJ0aW1lc2NhbGUiOiIiLCJzaW5nbGVBeGlzIjp0cnVlfQ%3D%3D&location=2,15.64847,0.00175&basemap=mapbox.light

97. Palmer, D. (2020, January 27). *Bad Actors Rent Hashing Power to Hit Bitcoin Gold With New 51% Attacks*. Retrieved February 4, 2020, from https://www.coindesk.com/attackers-rent-hashing-power-to-hit-bitcoin-gold-with-new-51-attacks

98. Poterba, J. M. (2000). Stock Market Wealth and Consumption. *Journal of Economic Perspectives, 14*(2), 99–118. https://doi.org/10.1257/jep.14.2.99

99. Quispe-Agnoli, M. (2002). Costs and Benefits of dollarization. *LACC Conference on Dollarization and Latin America,* Miami, Florida. https://www.frbatlanta.org/-/media/Documents/americascenter/ac_research/quispedollarizationrevised.pdf

100. Ripple. (n.d.). XRP. *Ripple*. Retrieved March 7, 2019, from https://ripple.com/xrp/

101. Rodríguez, C., & Carrasco, C. A. (2014). ECB Policy Responses between 2007 and 2014: a chronological analysis and a money quantity assessment of their effects. *FESSUD Working Paper Series No 65*.

102. Rogoff, K. (2016). *The curse of cash*. Princeton University Press.

103. Rolle, J. A. (2019). *The Bahamian Payment System Modernisation: Advancing Financial Inclusion Initiatives*. Retrieved July 20, 2019, from https://www.bis.org/review/r190321a.pdf

104. Ryan-Collins, J., Goodhart, C. A. E., & Greenham (Eds.). (2012). *Where does money come from? A guide to the UK monetary and banking system* (2nd ed.). New Economics Foundation.

105. Rysman, M., & Schuh, S. (2016). New Innovations in Payments. *Innovation Policy and the Economy 17*(2016), pp 27-48, NBER

106. Schmiedel, H., Kostova, G. L., & Ruttenberg, W. (2012). The social and private costs of retail payment instruments—An European perspective. *Occasional Paper No. 137*. ECB.

107. Schnorr, C. P. (1990). Efficient Identification and Signatures for Smart Cards. In G. Brassard (Ed.), *Advances in Cryptology—CRYPTO' 89 Proceedings, 435*, pp. 239–252. Springer New York. https://doi.org/10.1007/0-387-34805-0_22

108. Sedgwick, K. (2018, December 25). *Bitcoin History Part 6: The First Bitcoin Exchange*. Retrieved September 8, 2019, from https://news.bitcoin.com/bitcoin-history-part-6-the-first-bitcoin-exchange/

109. Sheshinski, E., & Weiss, Y. (1977). Inflation and Costs of Price Adjustment. *The Review of Economic Studies*, *44*(2), 287. https://doi.org/10.2307/2297067

110. Skingsley, C. (2016). *Should the Riksbank issue e-krona?* Sveriges Riksbank.

111. Stark, J. (2018, February 12). *Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit.* Retrieved March 14, 2019, from https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

112. Sveriges Riksbank. (2017). *The Riksbank's e-krona project; Report 1*. Sveriges Riksbank.

113. Sveriges Riksbank. (2018). *The Riksbank's e-krona project, Report 2*. Sveriges Riksbank.

114. Sveriges Riksbank. (2020, February 20). *Technical solution for the e-krona pilot*. Retrieved May 12, 2020, from https://www.riksbank.se/en-gb/payments--cash/e-krona/technical-solution-for-the-e-krona-pilot/

115. Sveriges Riksbank. (n.d.). *E-krona*. Retrieved July 10, 2019, from https://www.riksbank.se/en-gb/payments--cash/e-krona/

116. Tasca, P., Liu, S., & Hayes, A. (2016). *The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808762

117. Tether Operations Limited. (n.d.). *FAQs – Tether*. Retrieved March 24, 2020, from https://tether.to/faqs/

118. The Federal Reserve Board of Governors. (n.d.). *The Fed—What are the Federal Reserve's objectives in conducting monetary policy?* Retrieved February 20, 2018, from https://www.federalreserve.gov/faqs/money_12848.htm

119. The World Bank. (2020). *Remittance prices worldwide* (No. 33). Retrieved May 4, 2020, from https://remittanceprices.worldbank.org/sites/default/files/rpw_annex_q1_2020.pdf

120. The World Bank. (n.d.). *The Global Findex database 2017*. Retrieved August 27, 2019, from https://globalfindex.worldbank.org/

121. Tobin, J. (1985). Financial Innovation and Deregulation in Perspective. *Monetary and Economic Studies*, *3*(2).

122. Visa. (2015, June). *Visa Inc. At a Glance*. Retrieved July 7, 2019, from https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf

123. Visa. (n.d.). *Security and reliability*. Small Business Retail. Retrieved March 7, 2019, from http://usa.visa.com/content/VISA/usa/englishlanguagemaster/en_US/home/run-your-business/small-business-tools/retail.html>

124. Wei, W. C. (2018). Liquidity and market efficiency in cryptocurrencies. *Economics Letters*, *168*, 21–24. https://doi.org/10.1016/j.econlet.2018.04.003

125. Wikipedia. (n.d b). *Virtual currency*. Retrieved June 7, 2015, from http://en.wikipedia.org/w/index.php?title=Virtual_currency&oldid=662072446

126. Wikipedia. (n.d. a). *Litecoin*. Retrieved May 14, 2029, from https://en.wikipedia.org/w/index.php?title=Litecoin&oldid=951410373

127. World Bank. (2018). *The Little Data Book on Financial Inclusion 2018*. World Bank, Washington, DC

128. Xiao, E. (2020, August 14). *China to Expand Testing of a Digital Currency*. Retrieved December 6, 2020, from https://www.wsj.com/articles/china-to-expand-testing-of-a-digital-currency-11597385324

129. Zijlstra, J. (1975). Inflation and its impact on society. *De Economist*, *123*(4), 12.

130. Zilliqa. (n.d.). *About Zilliqa*. Retrieved March 7, 2019, from https://zilliqa.com/about-us.html

APPENDIX

Appendix 1: Povzetek (Summary in Slovene language)

Iznajdba Bitcoina in kasneje še ostalih kriptovalut je združila tehnologije distribuiranih baz podatkov, kriptografije in potrjevanje z delom (proof-of-work) z namenom stvaritve nove vrste denarja. Najpomembnejša lastnost kriptovalut v primerjavi z dosedanjimi oblikami denarja je neodvisnost od finančnih posrednikov in zaprtih plačilnih sistemov. Ta neodvisnost pomeni potencialno učinkovitejše transakcije. Hkrati pa so kriptovalute neodvisne tudi od države in centralnih bank. Ker je uporaba kriptovalut v letu 2020 relativno nizka, ta za delovanje centralnih bank ne predstavlja ovir.

Kriptovalute dandanes ne predstavljajo resne konkurence državnemu fiat denarju. Kriptovalute namreč v primerjavi z državnim fiat denarjem slabo opravljajo funkcije denarja. Pri tem jih omejuje nizka uporaba, visoka volatilnost menjalnega tečaja, nizka likvidnost in pomanjkanje znanja o kriptovalutah. Te lastnosti se sicer skozi čas izboljšujejo. Vseeno pa volatilnost menjalnega tečaja ne bo nikoli dosegla nizke volatilnosti tečaja primerno upravljane fiat valute, ker se ponudba kriptovalut ne more prilagajati povpraševanju. Prednost kriptovalut pred fiat denarjem je njihova neodvisnost od finančnih posrednikov ter njihova prilagojenost IT okoljem. Ker se lastnosti, ki zavirajo uporabo kriptovalut, izboljšujejo in ker bi bile tehnološke ovire za uporabo kriptovalut v prihodnosti lahko razrešene, bi lahko v prihodnosti kriptovalute funkcije denarja opravljale bolje kot državni fiat denar. Takšna prihodnost je vse prej kot zagotovljena, a naredi kriptovalute zanimive za nadaljnjo analizo.

Znaten delež uporabe kriptovalut bi lahko vplival na monetarni sistem in monetarno politiko. Transmisijski mehanizem monetarne politike deluje predvsem skozi kanale, ki vplivajo na ustvarjanje denarja prek posojil. Ker kriptovalute ne ustvarjajo denarja preko posojil, tudi ne vplivajo na transmisijski mehanizem in monetarno politiko. Bi pa znaten delež uporabe kriptovalut pomenil novo komponento ponudbe denarja, na katero centralna banka ne more direktno vplivati. Prav tako centralna banka ne more vplivati na menjalno razmerje med kiriptovaluto in državnim fiat denarjem, če želi izvajati monetarno politiko državnega fiat denarja. Šok v povpraševanju po kriptovaluti bi torej vplival na menjalno razmerje z državnim fiat denarjem in naprej na celotno ekonomijo preko vpliva premoženjskega učinka vrednosti kriptovalute. Na tak način bi lahko kriptovalute v prihodnosti negativno vplivale na zmožnost centralne banke za izvajanje monetarne politike in doseganje stabilnosti cen.

Digitalna oblika centralnobančnega denarja je potencialna konkurenca kirptovalutam, ki bi lahko preprečila znatno uporabo kriptovalut in na ta način centralnim bankam ohranila zmožnost izvajanja monetarne politike. Digitalna oblika centralnobančnega denarja bi poleg tega prinesla dodatne koristi v obliki povečane konkurence bančnega sektorja, plačilnih sistemov in povečano finančno vključenost. Za centralne banke bi uvedba digitalne oblike centralnobančnega denarja pomenila tudi ojačenje transmisijskega mehanizma in možnost uporabe negativnih obrestnih mer. Digitalna oblika centralnobančnega denarja po nekaterih napovedih omogoča močnejše navale na bančne vloge. Konsenza, ali je možnost navala na bančne vloge dejansko povečana, med različnimi avtorji še ni. Sicer pa bi bila digitalna oblika centralnobančnega denarja lahko uspešna v konkuriranju kriptovalutam.