Cryptocurrency: An economic review of its current and potential benefits

Authors:
Jesper Haar Jakobsen & Simon Kristensen
cand.oecon - Group 12

AALBORG UNIVERSITET
STUDENTERRAPPORT

Date 30-05-2018

Faculty of Social Sciences
Economics
Fibigerstraede 5

Title:

Cryptocurrency: An economic review of its current and potential benefits

Project period:

10. semester, spring semester 2018

Project group:

12

Authoring:

Jesper Haar Jakobsen

Simon Kristensen

Counselor:

Hamid Raza

Copies: 4

Pages: 57

Completed: 30-05-2018

Abstract

This project evolves around the nature of cryptocurrencies and some of the benefits that investors and consumers can exploit or potentially gain from. In order to examine the nature of cryptocurrencies and decide which kind of commodity it is some knowledge on money and monetary theory is established. This is done in order to decide what kind of commodity we are dealing with. It is found out that cryptocurrencies have a lot of attributes worthy of being a money commodity but one of the most important one — price stability — is not one of those. This means that in order to converge towards the mandatory attributes of a money commodity, some changes needs to happen.

The reason for the lack of price stability is its current nature which is highly speculative, due to the fact that it is a relatively unknown 'commodity'. An asset analysis is put forth in order to determine what asset class it belongs to but it is learned that it does not remind of any of the classical assets. This fact and its current nature of high returns and high risk and the predominantly independence from other classical assets makes it an asset that can be included in portfolio for riskier but higher returns. It is a very current theme, and the nature of cryptocurrencies can vary relatively much in the matter of not much time.

The next topic involves a possible way to obtain price stability in cryptocurrencies. This possibility is put forth by Ametrano who sought inspiration in Hayek's denationalisation of money and consists of a rebasing solution which involves a method where your wallet is automatically rebased to keep the purchasing power constant.

The final section considers how an implementation would look in the critical juncture framework and the benefits that consumers receive after this theoretical implementation. There are some elements from cryptocurrencies that draw parallels with that of the critical juncture framework, and it can be argued that a critical juncture is needed in order to see an adaption of cryptocurrencies. Regarding how the consumers can benefits from this, with the help from various litterature, some attributes outside of the classic three (medium of exchange, store of value, unit of account) like transaction costs, protection against credit card fraud as well as monetary fairness are considered. It is learned that a eventual adoption of cryptocurrency has the possibility to benefit the consumers of different levels.

Contents

1 Introduction **2**
1.1 Critical Juncture 6

2 Introduction to the cryptocurrency technology **8**
2.1 Digital signatures and addresses 8
2.2 Transactions and the Blockchain 9
2.3 Security 12

3 Money **14**
3.1 Origin of money 14
3.2 Theory on money 15
3.3 Cryptocurrency - Is it a currency? 20

4 Classifying Cryptocurrencies **22**
4.1 National approaches 22
4.2 What asset class does cryptocurrencies belong to? 24
4.3 Data 25
4.4 Methodology 25
4.5 Empirical Analysis 33
4.6 Concluding remarks 37

5 Hayek Money - Price Stability **42**
5.1 Rebasing 45

6 An implementation of cryptocurrencies **50**
6.1 Defining the financial crisis in the critical juncture framework 51
6.2 Effects on the consumer post implementation 53

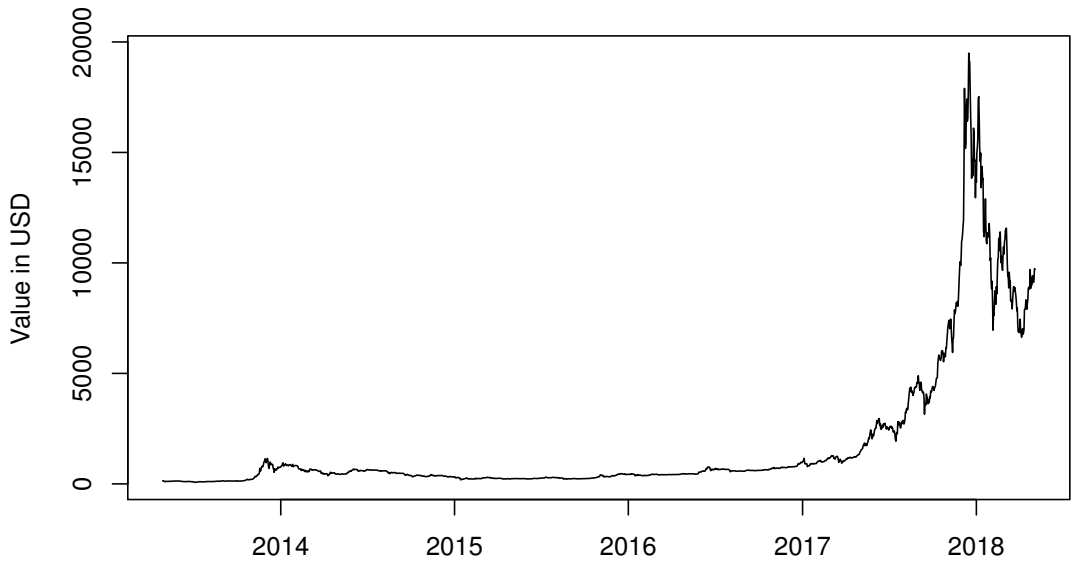
7 Conclusion **57**

Bibliography **58**

1 Introduction

In the recent year cryptocurrencies have made a serious impact in the economic and especially the financial world[1]. Bitcoin protocol was introduced in the wake of the global financial crisis in 2008, but it was not until the spring of 2017 where it began to receive broad attention. Since then, the price of bitcoin has skyrocketed as can be seen on figure 1.

Figure 1: Historic development for Bitcoin



But why did the price on bitcoin suddenly just begin to rise? Japan accepted the bitcoin as a legal tender on the first of April 2017[2], and as can be seen on above-mentioned figure, it is also around this time that bitcoin started to rise. This can be a sign that good news leads to a rise in the price, which leads to more good news. It is a positive spiral and a reinforcing effect, as long as people "trust" in the bitcoin. Trust and expectation are very important in this case, given that Bitcoin and other cryptocurrencies have no inherent value. Some research has already been made and Cheah and Fry (2015) actually

[1] https://www.bloomberg.com/view/articles/2017-12-18/cryptocurrencies-are-starting-to-affect-the-real-economy

[2] `https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow/`

finds that the fundamental value of bitcoin is zero. The main reason being that a huge share of it is price is based upon speculation.

Motivation

But what is it, this bitcoin? And what is a cryptocurrency, and what can its benefits and/or disadvantages be for the especially the consumer but also other institutions in the economy? This project will evolve around this question, and some close nearby issues. The reason that this is interesting, is the whole nature of cryptocurrencies. It is a whole new subject and a lot of different people have shown their different thoughts on these new currencies, and as Noble Prize winner Robert Shiller says:

> *Practically no one, outside of computer science departments, can explain how cryptocurrencies work, and that mystery creates an aura of exclusivity, gives the new money glamour, and fills devotees with revolutionary zeal* (Shiller, 2018).

It can be argued that the initial thought from Satoshi was to create a decentralized cash system, maybe or maybe not to threaten the current fiat based commodity money. The introduction of Bitcoin came right after an international financial crisis and if we take starting point in some institutionalist thoughts, a thing called a *critical juncture* can take place (Collier and Collier, 2002). A critical juncture means, that the whole of the economic landscape and equilibrium has been shaken up, often by an economic crisis like we saw in 2008. This makes way for changes, like an introduction to a whole new way to handle money. The release of the bitcoin white paper were therefore perfectly timed in a critical juncture framework and it could even be argued to be the cleavage point, which means that the financial crisis really doesn't matter. This will be discussed in later sections. But as an interested economist (we're guessing he/she/they is/are), what better timing for introducing a whole new way to handle money, than that of an international crisis starting with Lehmann Brothers collaps in september '08? However, bitcoin didn't exactly break through as the new money commodity. It has however gained popularity, not so much as a currency but more as an speculative asset, which some people have profited heavily from. Meanwhile, over 1500 other altcoins[3] has been introduced, some of them trying to perfect the system in their own way. Some of these other altcoins will be briefly examined later in this section. In this project we would like to investigate how the consumer and investor is affected on different levels by the introduction of bitcoin and cryptocurrencies in general. The way this is done is by developing a section on assets and portfolio theory to investigate how investors can take advantages of this new form of asset. As for the consumer, we would argue that if cryptocurrencies is destined to have a future as a money commodity, we would have to experience a critical juncture, that would pave the way for an introduction of a new money commodity. If this should happen, what would the advantages and disadvantages be for the consumer?

Structure

In order to understand this topic fully, the first sections will contain a shortened but adequate examination of the blockchain technology behind cryptocurrencies. Following

[3] Altcoins is another name for other cryptocurrencies besides bitcoin

this some of the benefits of this blockchain technology will be mentioned, together with a short walkthrough of some of the most known altcoins.
Following this section, a more economic approach will take place with a review of two economic schools theory on money — these schools being the Post-Keynesian/institutionalist and the Austrian School. This is done in order to describe the functionality of cryptocurrency as money.
A thorough examination will hereafter be carried out of a close-linked question; should cryptocurrencies be considered as a new asset class? This question arises from the fact that different cryptocurrencies are experiencing extreme degrees of volatility[4], which is normally linked with highly speculative assets and not a money commodity. To investigate this question, an examination of all the traditional assets together with cryptocurrencies will take place, these classical assets being; currency, stocks, bonds, commodities and real estates. Empirical data will be used to compare liqudity of cryptocurrencies to well known stocks and to calculate the correlation between returns of cryptocurrencies an returns of traditional assets. To edge this section out, an examination on the impact of cryptocurrencies on optimal portfolio structures will take place to hopefully give investors an idea on how to handle cryptocurrency. After this section, we'll take a look at Hayek Money and a price stability solution and the last section will contain a discussion regarding cryptocurrencies possibility to function as money with the help from different litterature. Together with this, a discussion will take place which goal is to investigate how and in what way an implementation of cryptocurrency might affect the consumers on the market. This will be a complete theoretical discussion.

Bitcoin

Bitcoin is the first protocol to use a decentralized system, which means that it is being run by individuals without the need for a bank or government. This network is peer-to-peer which means that money, bitcoins, is being sent directly between the users, with the only fee being collected by the individuals that "runs" the network. These individuals called miners verify the transactions using cryptography and a proof-of-work concept and are being rewarded if they solve it first. All the transactions are being recorded on a public ledger (Nakamoto, 2008). It was invented by a person or group called Satoshi, and the conspiracy theories on who this person or group might be are many. The average transaction time is ten minutes and the supply of bitcoins is finite, set at a limit at 21,000,000 coins. At the current rate of block creation at ten minutes per block, the last bitcoin will be mined in 2140, which means the supply limit will be reached [5].

Ethereum

Ethereum is like bitcoin based on a blockchain system, while they also have implemented smart contracts. A smart contract is an online protocol that gives the possibility to enforce the contents of a contract without a third party. Ethereum have a coin called Ether which like bitcoin can be transferred around between users with an average transactions time between 14-15 seconds. The supply is finite, but unlike some other cryptocurrencies they haven't put a number on the max supply. There is however a maximum of 18,000,000 new

[4] https://btcmanager.com/u-s-federal-governor-calls-out-cryptocurrencies-terms-it-extremely-volatile/
[5] https://en.bitcoin.it/wiki/Controlled_supply

Ether entering the market per year. According to their own website they will theoretically reach a point where the new coins will amount to the destroyed ones, thereby creating an equilibrium[6]. As well as bitcoin, miners are using a proof-of-work concept and are being rewarded for doing it first with five Ether, which is how the supply is growing.

Ripple

Ripple is a payment protocol and unlike the two above-mentioned not based on the blockchain system. Ripple has a finite supply having released all 100 billion coins at their inception, with a current supply of about 39 billion coins, but as of 2017 the company has put 55 billions coins in escrow planning to release one billion coins each month. But not all the coins are necessary going to be demanded, which means the left overs are put back in escrow, being released at another time. They are currently expecting the supply limit to be reached by 2047[7]. They boast themselves as on of the fastest networks handling transactions in a matter of 3-5 seconds[8].

Dash

Dash is running on the same blockchain system as bitcoin and Ether, but differs in the way of mining. Where bitcoin have a single-tier network where the miners handles it all, Dash has a two-tier network. Miners is doing the same but they have masternodes, which concentrates on PrivateSend and InstandSend. These two options being a part of their way to be one of the most user friendly payment system there is[9]. PrivatSend giving the users anonymity, while InstandSend can handle a transaction within one second. The average block time is however about 2,5 minute. The supply of Dash is a little bit more complicated, but it has a theoretical limit of 22 million coins[10].

To sum it up, a table containing the above-mentioned cryptocurrencies have been designed to give a good overview to the reader.

	bitcoin	Ethereum	Ripple	Dash
Block time	10 minutes	14-15 seconds	3-5 seconds	2.5 minutes
System	Blockchain	Blockchain	Ripple Protocol	Blockchain
Current supply	$\sim$ 17 million	$\sim$ 100 million	$\sim$ 39 billion	$\sim$ 8 million
Supply limit	$\sim$ 21 million	18 million per year	$\sim$ 94 billion	$\sim$ 22 million

[6] https://www.ethereum.org/ether
[7] https://ripple.com/insights/ripple-to-place-55-billion-xrp-in-escrow-to-ensure-certainty-into-total-xr
[8] https://www.weusecoins.com/what-is-ethereum-classic/
[9] https://www.weusecoins.com/what-is-dash/
[10] https://www.youtube.com/watch?v=2vZDclyqh5Y

1.1 Critical Juncture

> *A critical juncture may be defined as a period of significant change, which typically occurs in distinct ways in different countries (or in other units of analysis) and which is hypothesized to produce distinct legacies* (Collier and Collier, 2002, pp. 29).

That is one of the definitions of a critical juncture. The term critical juncture introduced by Collier and Collier (2002) emanated from the well known term path dependence (North, 1989). Path dependence is one way to explain why the world looks the way it do. Every choice made in past has formed a path in which the economy is heading. That way, people today is limited in their choices because of the choices that were made in the past. Imagine that Hoover made the right choices as a president back in the 1930's and managed to turn the economy around and in that way being able to beat Roosevelt for president in 1932. In that case, it is possible that we would never see Roosevelts politics which leaned heavily towards Keynesian economy. That would have meant that the Keynesian thoughts on government spending would not have been adapted in the 1930's but instead later or maybe never. That we will never know, and that is partly because of path dependency.
In Colliers framework, the great depression have the characteristics to be defined as a cleavage or crisis able to trigger a critical juncture in both the political and economical landscape. These terms belong in the Colliers framework, which we now will take a look at. The way a critical juncture can take place varies greatly and is dependent on the current context. Colliers talks of three components and five elements, that can help to define and detect these critical junctures (Collier and Collier, 2002).

- Significant change occurred within every case
- Change took place in different ways within every case
- The explanatory hypothesis about consequences

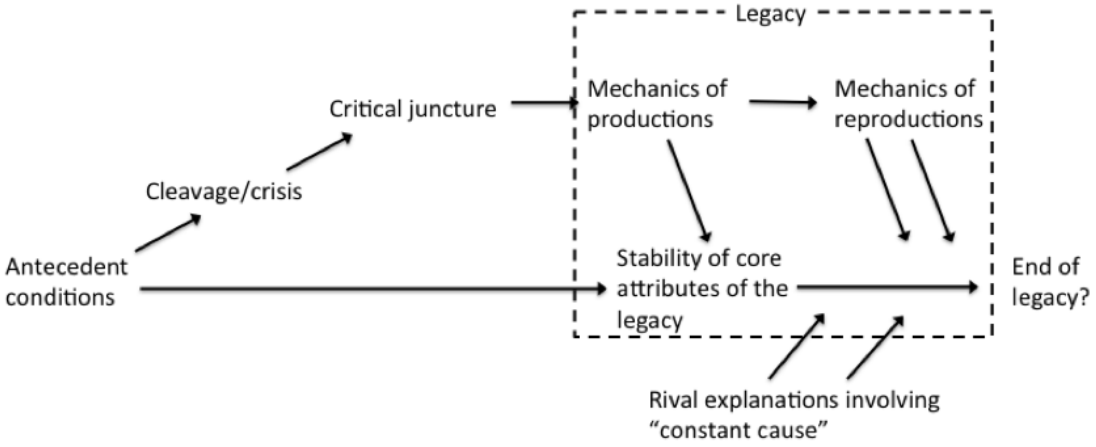
The last one means that if the critical juncture did not produce a legacy, then it cannot be defined as a critical juncture.

1. The conditions prior to the critical juncture make a baseline, so that the critical juncture and legacy can be assessed.
2. The crisis or cleavage which emanates from the antecedent landscape which triggers the critical juncture.
3. Three components of the legacy:
    - *Mechanisms of production of the legacy.* The legacy will not be present immediately, but will have to be nursed in order to be shaped.
    - *Mechanisms of reproduction of the legacy.* Stability is not guaranteed, but reached through institutional and political processes.
    - *The stability of the core attributes of the legacy.* Some basic attributes is produced as an outcome of the critical juncture. As an example you could consider the Roosevelt-presidency, which could have been caused by the change in the political landscape.**bob bob**

4. Rival explanations, which will not be looked at further
5. End of the legacy. If this is not the case, then there never was a critical juncture.

Colliers figurized these steps, which lead to figure 2.

Figure 2: Building block of the Critical Juncture framework (Collier and Collier, 2002, pp. 30)



This is a distinct framework that tries to take a look at how the institutions on the market can be changed and what needs to happen in order for this to be true. From Veblen we know that institutions tend to show rigidity and conservatism — because why change something that works? (Rutherford, 1984)
This can be one of the reasons why such a term as critical juncture is needed, in order to change the economic institutions. The project will take a further look at this term in the analysis, where the crisis in '08 seeks to be put in the above-mentioned framework.

2 Introduction to the cryptocurrency technology

In 2008 an unknown person or group published the white paper *Bitcoin: A Peer-to-Peer Electronic Cash System* under the alias Satoshi Nakamoto. The paper introduced a clever way of using cryptographic constructions to establish a completely decentralized electronic cash system that does not rely on a trusted third party issuing money and managing transactions. In the following year 2009 the software facilitating the Bitcoin protocol was released as open-source and the first cryptocurrency was introduced to the world.
The fact that the software behind Bitcoin is open-source also means that it is possible to re-parametrize the source code and thereby creating a new cryptocurrency fairly easy and at the time of writing there exists 1563 different cryptocurrencies[11]. This chapter aims to provide a basic understanding of the technology that makes it possible for a decentralized system to overcome challenges such as;

- Consensus in a distributed network.
- Doublespending behaviour.
- Proper transaction validation.

We will refer to the Bitcoin protocol for examples, but emphasise will be put on components of the system that are design decisions.

The construction of a cryptocurrency system requires two fundamental cryptographic technologies; Cryptographic validation of function and public-private key cryptography for storing and spending money. This chapter is based on Narayanan et al. (2016).

2.1 Digital signatures and addresses

To create a digital equivalent to wallets and handwritten signatures for approval of transactions public-private key cryptography is used. To be able to trade in a cryptocurrency system one needs to create a pair of keys, one of which should be made known to the public and one which should be kept private and only known by oneself. The public key serves as a wallet address from which transactions can be made to and from, while the private key is used to make sure that the only one that is able to make transactions from the public key address is the one holding the private key. This is made possible by using the private key to create *digital signatures*.

[11] `https://coinmarketcap.com/all/views/all/`

To illustrate how digital signature are constructed in practice using cryptography, we construct a digital signature scheme that consists of the following algorithms:

- (sk, pk) := generate_keys($keysize$) This algorithm generates a key pair, consisting of a privately kept secret key, sk, and a key made publicly available, pk, using a randomized algorithm, generate_keys .

- sig := sign(sk, msg) The sign algorithm provides a signature from the user with the private key, sk, to be put on a message, msg.

- is_valid := verify(pk, msg, sig) Given the public key, the message and the signature, the verify algorithm will return the value true, if sig is a valid signature on msg from the user behind the public key, pk, otherwise false is returned.

From the digital signature scheme it can be seen, that the signature not only depends on the private key but also on the message or transactions that is put on. A digital signature therefore changes with every new transaction. To get around the fact that identical transactions would have the same signature, so that it would be possible to broadcast an already signed transaction one more time to the network, a unique id representing the coins being spend is included in every transaction. As it can also be seen, the public key is not only being used as a wallet address but also for the confirmation of transaction validity. Whenever someone hear of a transaction they can use the public key of the address from which some coins are being transferred from to confirm that it is indeed the one owning the coins, who has broadcast the transaction.
An important requirement for a digital signature scheme like this, is that signatures can not be forged, meaning that people who are sending signed messages will not be able to uncover the secret key, sk. We wont go into more details on how the algorithms used in a digital signature works, but just note that algorithms exist, so that a digital signature scheme can be set up.

2.2 Transactions and the Blockchain

In a cryptocurrency system every transaction ever made is being kept on a public ledger, which is being maintained in a peer-to-peer network. In fact the currency itself is the history of all transaction, as no one holds coins in a cryptocurrency. They instead hold the private key that gives them the right to spend coins that, in the last transaction that they were in, were send to the associated public key. To make a transaction one would broadcast a signed message telling which coins (by referring to the transaction where the coins were received) should be send to another address. Everyone in the network running the cryptocurrency protocol, called nodes, can confirm that the transaction is valid by checking that the public key and signature matches with the transaction and by checking that the coin has been transferred to the public key at some point.
For a system like this to work it is necessary that *distributed consensus* can be achieved, which mean that everyone has the same ledger and agrees upon that this is the correct record of transactions, which is quite a challenge in a decentralized network. In cryptocurrencies distributed consensus is achieved by having a competition for the right to update the ledger with new transactions. Such a competition is known as a mining puzzle.

Mining Puzzles

The main idea in mining puzzles is to use a resource that can not be monopolized and let the chance of getting to update the ledger be proportional to the proportion held of this resource. Bitcoin and most other cryptocurrencies uses computing power as the resource, this type of mining puzzle is known as *proof of work*. A little fun fact is that mining is using extremely much power and an investigation from 2017 showed that bitcoin mining consumers more electricity than Ireland on a year[12]. Another possibility is to use *proof of stake*, which depends on the proportion to ownership of the currency.
Only proof of work is described in this chapter, as this is the most widely used mining puzzle. To understand proof of work, a basic understanding of cryptographic *hash functions* is needed.

Cryptographic hash functions

For a hash function $H()$ to be cryptographically secure and useful for cryptocurrencies, it is required that it has all of the following six properties:

- Takes any string as input.
- Produces a fixed size output. SHA-256, which is used in Bitcoin, produces a 256 bit output.
- Efficiently computable: For any input it should be possible to figure out the output in a reasonable amount of time.
- Collision-free: Nobody can find two values, x and y, where $x \neq y$ and $H(x) = H(y)$.
- Hiding: If a secret value r is chosen from a probability distribution with a high *min-entropy*, then it is infeasible to find x given $H(r \parallel x)$. A distribution with a high min-entropy is essentially a distribution that is very spread out and therefore there is no value that is particular likely to occur.
- Puzzle friendliness: for every y, if k is drawn from a high min-entropy distribution, it is infeasible to find x such that $H(k \parallel x) = y$.

The output of a hash function is called the *hash* which, because of the collision-free property, serves as an unambiguous summary of the input. The hiding property means that given a hash, it is infeasible to compute its associated input and the optimal way to do so is to try every possibility uniformly randomly. The puzzle friendliness property is very much alike the hiding property, but it differs in the way that if a part of the input is given along with the hash, the optimal way to find the rest of the input is still to try every possibility randomly. In fact no hash function exists which has been proved to be inverse infeasible, but a lot have tried to solve the problem with no luck, so the properties are assumed to hold.
A function with these properties can be used to prove that a particular list of transactions is associated with a lot of computational work.

[12] `https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland`

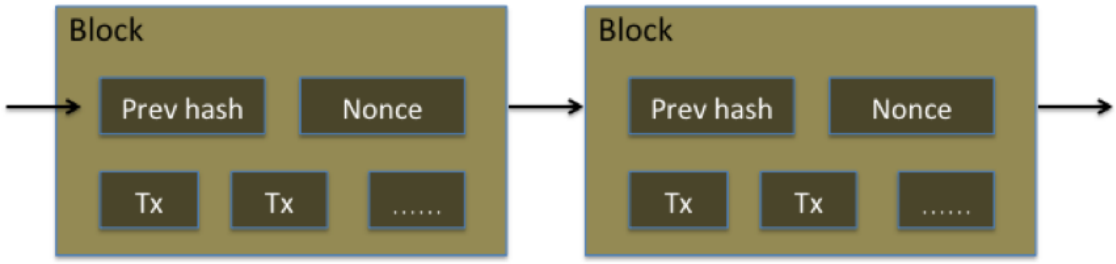
Proof of work

Cryptocurrencies using proof of work as a mining puzzle require that to update the ledger with a new block of transactions, the node proposing the new block has to find a number that concatenated with the information in the block gives a hash under a specific target value. If the requirement for example is for the hash to start with 40 zeroes the chance of finding such a number would be $\frac{1}{2^{40}} \approx \frac{1}{1{,}000{,}000{,}000{,}000}$. Because of the puzzle friendliness property of the hash function, the best way to find such a number is just to try random numbers. When someone succeed in finding such a number, they can broadcast it to the rest of the network and everyone can easily check that the hash indeed starts with at least 40 zeroes, thereby verifying that a lot of work has been put into finding this number.
The proof-of-work mining puzzle relies on the idea that if the ledger with the most computational work put into it is trusted as the correct one, faulty and malicious behaviour is made computational infeasible. This becomes the case, when the public ledger is stored as a *blockchain*.

The blockchain

Instead of just keeping the public ledger as one long list of transactions, the public ledger is divided into blocks and each of these blocks consist of a list of transactions and a proof of work. Like a digital signature is needed for a transaction to be considered valid, a proof of work is needed for a block to be considered valid. Furthermore each block contains the hash of the previous block to implement a standard ordering of the blocks and therefore the transactions in them. Figure 3 shows an illustration of a blockchain. When the hash of

Figure 3: A Block chain (Nakamoto, 2008, pp. 3)



the previous block is included in each block anyone who tries to alter some information in a block will have to do a lot of work. If an adversary alters the data in block k, he would first have to find a new proof of work for block k, while the new hash would be different from the hash in block $k+1$, so a new proof of work would have to be done for that block as well and so on.

Updating the Blockchain

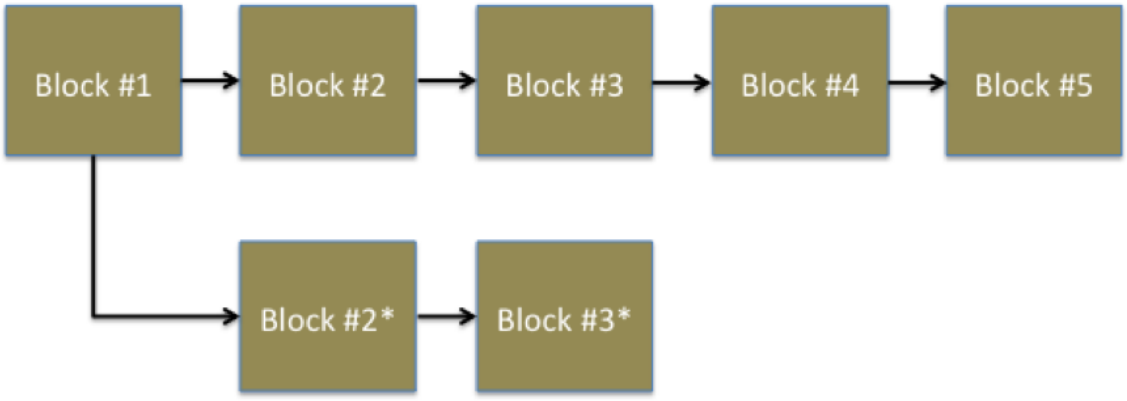
In cryptocurrencies the ones maintaining the bookkeeping system are called miners. Miners keep a personal copy of the blockchain on their computers and can therefore easily verify if a transaction that are being broadcasted to the network are valid or not. Putting transactions that they have heard about together in a block, miners then compete to find a proof of work. Since it takes a lot of work to find a proof of work, miners receive a *block reward* as each new block contains a transaction of new coins to an address owned by the

miner. This is how new money are created in a lot of cryptocurrency systems. In Bitcoin the block reward started out being 50 bitcoins, however the block reward is halved every four years and in 2140 it will reach zero and no more bitcoins will be created. Another way to compensate the miners for their work is by including a transaction fee. The mining process is like a lottery for the miners, since no one has a better way of finding a proof of work than just trying random numbers and the only way to increase ones chances of winning the lottery is to increase ones proportion of the overall mining computational power.
Anyone using the system for making transactions will therefore, instead of listening for transaction being broadcast, be listening for blocks with a valid proof of work. If for example Frank is buying a beer keg from Mitch for ten digital coins, Mitch would wait for a block with the transaction of ten digital coins from Frank to Mitch in it. However it might be that Frank wants to hustle Mitch by mining a block himself with the transaction in it and broadcasting it to Mitch, but not to the rest of the network. Leaving Frank with both the digital coins and the beer keg, this is called a *double spending attack*. Fortunately there is a way for Mitch to make sure that he will receive the coins.

2.3 Security

The key component of the protocol in a cryptocurrency is that it is the blockchain with the most work put into it, that is trusted as the correct one and all honest miners mine on this chain. This simple rule makes the system secure. Going back to the scenario where Frank is trying to hustle Mitch and Frank has broadcast a fake block to Mitch. Mitch however also receive new blocks from the other miners in the network, thereby creating a *blockhain fork*, which can be seen in Figure 4 Since everyone else is working to find blocks to extend

Figure 4: A blockchain fork



a different chain than the one Frank is working on, it becomes increasingly unlikely that Frank will be able to find blocks at the same speed that the rest of the network is finding blocks. Mitch will therefore eventually, as the blockchain that is being broadcast to him from Frank has become shorter than the other one he is hearing about, disregard the Blockchain from Frank and accept the other one as the correct one, thereby realising that he have not received any transaction from Frank and he will keep the beer keg. As this example shows one should never trust a block immediately after it has been broadcast to the network, instead the convention in Bitcoin is to wait for six blocks to be mined before

trusting the transactions in the first one of these blocks.
There does not need to be a deliberately attempt of cheating for a blockchain fork to be created. It might happened that two miners find a new block at approximately the same time and they will both broadcast their blocks to the network. Due to network latency it will be different for the rest of the miners in the network which of the blocks they receive first and it will therefore be different which block they continue to mine upon. However when a new block is found in one of these chains, all the miners that were working on the other chain realizes that there now is a longer chain with more computational work put into it, and they therefore switch to work on this chain.

The 51 percent Attack

As noted in the Frank and Mitch example, Franks problem is that he does not hold more than half of the computing power. If Frank was holding 51 percent of the computing power he could have launched what is known as a 51 percent attack. Instead of broadcasting blocks to only Mitch to try to convince him that he can believe the transaction, Frank will broadcast the transaction to the whole network and as soon at it has been included in a block he will secretly create a deliberate fork in which the transaction is not included. As Frank holds 51 percent of the computing power he is able to keep up with the rest of the network in producing blocks and when Frank has received the keg from Mitch and his own chain is the longest in the network, he will broadcast his chain to the network and every honest node will switch to this chain, leaving Frank with both the keg and his coins.
This attack however does not enable the theft of coins or counterfeit production, it only allows an attacker to succeed in double spending of already owned coins. However a successful attack might destroy the confidence in the security of a cryptocurrency, leading the value of the currency to plummet. Considering the amount of investment, however, an adversary would have to make to achieve a 51 percent majority of the computing power, such an attack does not really make sense from a financial point of view.

3 Money

Money drives the world. That is a quote you have heard before and most people would probably nod their head in agreement. It is, however, a bit funny how a piece of worthless paper can drive people mad. As Shiller have said in a very recent post:

> *As the medium of exchange throughout the world, money, in its various embodiments, is rich in mystique. We tend to measure people is value by it. It sums things up like nothing else. And yet it may consist of nothing more than pieces of paper that just go round and round in circles of spending. So its value depends on belief and trust in those pieces of paper. One might call it faith* (Shiller, 2018).

Money in itself has no value whatsoever, the reason it has is because we as people, costumers, owners, workers believe and trust in the the little green note with Abraham Lincoln on it. Nonetheless, it is with good reason that we trust in that little note. When have it ever failed you? For the Average Joe, money is important. It is not important to know what money is but rather what their ability is and how to utilize this particular ability. We are talking new clothes, food on the table, paying rent etc. In this chapter we take a look on the origin of money and how we got to where we are today.

3.1 Origin of money

The division of labour was one of the main reasons that the world were in need of a mean-of-exchange. Before the existence of money, people used to barter with each other. To barter, also called direct exchange, is to change goods directly with each other - this could be the farmer and the butcher. The farmer has loads of wheat, but he does not have any meat to go along with it. For the butcher it is the opposite. These two workers could therefore with good reason barter with each other so that the farmer could grill a good steak, and the butcher could get some carbohydrates to go along with all the protein. This is what we call the coincidence of wants (Rothbard, 1963). For this trade to be possible, two attributes should apply: B wants exactly the goods that A is offering, and B has precisely the goods that A wants. Clearly, this is not going to work in the long term. Imagine if that was the way we did it today. Is Maggie the school teacher supposed to teach the McDonalds family about neutrons, while they make dinner for her? The only way barter can be effective is if the coincidence of wants can be present at all times, but this is clearly impossible (Rothbard, 1963).
So what did the clever man do? He figured that there must be some good that almost everybody is in need of. So from that point of, the farmer trades his good A for B, and after that he trades good B for C. The butcher trades the other way around. Good C for

B, and the good B for A, and as you might have thought, indirect exchange is born. It really does not matter whether this good is salt or metal, just as long it is something that all people is accepting as a mean-of-exchange. However, it should be noted that this good most likely would be a marketable good, that does not have problems with indivisibility which means that butter are more likely to become this good B, than a cow (Rothbard, 1963). As more and more people are starting to use a specific good as a media, it becomes more marketable, which in turn means that even more people are likely to use this good as a media, which then again makes it even more marketable. It is a reinforcing effect (Rothbard, 1963). Many different goods have been used as a media throughout history, some of these being tobacco, sugar, grain, salt, beads and copper.
After a lot of different medias were in use, the free market, as Rothbard says, chose silver and gold as their new money. The introduction of a money-commodity is a huge leap forward for the economy as a whole (Rothbard, 1963). With a general medium-of-exchange, the economy can continue to expand and evolve in a fast pace. Suddenly, instead of working for a kilo of wheat you work for money, which you then can use how- and wherever you like. Furthermore, you can start to compare prices and it is easier when you only have one commodity which you can use to buy all other commodities. Instead of having to pay two bags of wheat and your daughter for three cows, you can save up money to buy some cows instead and let your daughter make her own decisions.

3.2 Theory on money

The bartering and the birth of money is something most economists agree on. The theory on money is however not something they always agree on. The main focus in this project is to determine how the consumer benefits form cryptocurrency both pre- and post-implementation. This section will therefore primarily focus on the behaviour of money from different perspectives and through this knowledge hopefully be more able to derive a conclusion on some of the benefits to the consumers. For now, we will look at two different theories on money. The next sections will include an examination on the post-Keynesian theory on money and the Austrian theory on money.

Post-Keynesian/institutionalist Theory on Money

In order to examine the PK and institutionalist view on monetary theory, a paper from Philip Arestis & Alfred Eichner has been studied. Money is an important part of the economic system, and is closely connected to the system as whole. It is already easy to conclude that money definitely is not neutral in this framework. Arestis calls his approach *The Monetary Theory of Production* with inspiration from Keynes and Veblen (Arestis and Eichner, 1988). The endogenous nature of money is quickly established together with the thought of a credit based economy, where credit, not money, is the main driving power in economic growth. Arestis states the following:

> *Money, in this view, is an output of the system, with the endogenous response by the financial sector governed by the borrowing needs of firms, households, and the government. Once it is recognized that money is credit-driven and therefore endogenously determined, any money creation emanating from fiscal or debt management operations initiated by the authorities or from a favorable balance*

> *of payments, can be neutralized through an equivalent reduction in commercial bank credit brought about by the actions of private economic agent* (Arestis and Eichner, 1988, pp. 1004).

So, government can not inject money directly in the economy, but it is however possible to redistribute money with one premise:

> *To the extent that the latter groups are different from those initially receiving/destroying money following the government's initiatives, redistribution of money between those groups takes place* (Arestis and Eichner, 1988, pp. 1004).

Given that this theory relies heavily on the fact that it is a credit-based system, a lot of the assumptions and thoughts arises from this. An industrialized economy must necessarily have a credit based system to help advance this. As Arestis say:

> *The financial problem inherent in any market regulated system of production is that goods cannot be produced until the necessary labor and material inputs have first been obtained, and those inputs cannot be purchased except out of the proceeds from the sale of the output produced by them* (Arestis and Eichner, 1988, pp. 1005).

In an evolving economy, there is a need for capital in order to launch new production strategies. A credit-based system makes it possible for business firms to lend capital against a small price. The funds floating around is created by the commercial banks, who is imposed by the government to hold a reserve of a predetermined size. For example the Fed has divided their requirements compared to how *big* the bank is. Big meaning how much money they are transacting. From $0 - $16 million there is no requirement. From $16 - $122.3 million a reserve requirement of three percent is set and for holdings above $122.3 million a reserve of at least ten percent is required.[13] It is quite obvious in this framework that for every loan the bank provide, the money supply will grow, especially with the establishment of the fiat currency that was made possible because of the governments interest and willingness to support this new currency and to act as a "lender of last resort" (Arestis and Eichner, 1988). In fact, Arestis postulates that if the monetary authorities, i.e. the central bank, does not accommodate the commercial banks when needed, a series of effects can take place. We can see a financial crisis, a recession or a rise to interest rates. You probably will not see neither a crisis or a downturn before something happens to the interest rate, which according to Arestis is the most likely to happen. If this happens, it can lead to a series of negative events, ending out with a financial crisis if the monetary authorities do not step in (Arestis and Eichner, 1988). Turning back to the credit-based system, where credit is the crucial part. Arestis says:

> *When entrepreneurs expand production, and until the output is sold, there is a gap in working capital needs that is bridged by bank loans* (Arestis and Eichner, 1988, pp. 1009).

This leads us to one of the biggest differences between PK/institutionalist theory and neoclassic theory, where money is given exogenous and can be described with the well-known formula: $M = m * B$, where M is money stock, m the money multiplier and B the

[13] `https://www.federalreserve.gov/monetarypolicy/reservereq.htm`

monetary base. The PK and institutional theory reverse the causality and says that the monetary base is given by the money stock; $B = (1/m) * M$. From the previous quote, it is quite obvious to see that that the firm expanding is the reason for the rise in the money stock. It is not an increase in the money supply that forces the entrepreneur to loan money, it is the other way around according to Arestis:

> *Thus, variations in the supply of money are caused by fluctuations in the level of economic activity instead of the reverse* (Arestis and Eichner, 1988, pp. 1009).

To conclude this section, it is noted that this theory relies heavily on the credit-ability that the fiat-based currency and current banking regimes allow. The Austrians is eyeing this topic from a more singular view.

Austrian Theory on Money

In the year 1912 Ludvig von Mises published his work of art called *Theory of Money and Credit*, which laid the groundwork for the Austrian School's theory of money. In short, Mises took the theory of marginal utility and used this to explain the demand and price of money (Rothbard, 2011).
The Austrian School of economy are focused on the aspect of free market, but done through the framework of human action axiom which is their cornerstone and where all their economic theories come from. This action axiom simply means that human take actions to fulfill their wants, which in part can explain the rise of a medium-of-exchange (Rothbard, 1963, pp. 1-4). Mises' goal was to put money in the same box as every other good. In doing this, he used the so called *Wicksteedian concept*, which says following:

> *Supply is the total stock of a commodity at any given time; and demand is the total market demand to gain and hold cash balances, built up out of the marginal-utility rankings of units of money on the value scales of individuals on the market* (Rothbard, 2011, pp. 2).

This concept proved useful for Mises for several reasons, but the main reason being that money, unlike every other commodity, is acquired for later use and not immediate consumption.

> *(...) Mises pointed out that the currency unit serves as unit of account and as a common denominator of all other prices, but that the money commodity itself is still in a state of barter with all other goods and services* (Rothbard, 2011, pp. 4).

Another view that is quite different than that of the mainstream economist, is the way that the Austrians see an increase in the money supply. In what Rothbard calls the Angel Gabriel model, he shows how the best possible solution (To increase every single citizen account of money by ten percent), does not lead to an all around price increase of ten percent. This is because every human being has a unique scale of value[14] with a different

[14]Scale of value, is a scale that every person has, and which is highly dependant on time, scarcity, uncertainty and context. It can and will continuously change. For example, if I am sitting outside in -10 degrees i would probably not value an ice cream as much as I would value a cup of hot cocoa. However, if I am lying on the beach in 30 degrees, that ice cream would not sound so bad.

ordinal ranking of utilities. Remember that the ranking is ordinal, which means that you can not say how much utility you get from buying a car, you can only know that buying a car gives you more utility than buying a motorcycle. Let us turn back to the increase of the money supply. Everyone finds out that they have become ten percent richer. The monetarist would call for a ten percent increase in all prices, but given the different scale of values, ordinal rankings as well as the relative marginal utility, people will *use* this increase in their money stock differently. This means that the demand for different goods will not react the same way. This situation can be described as part of the Cantillon-effect[15]. This effect being that an increase in the monetary supply will affect relative prices and cause a change to this. The reason being that the money does not behave like the Angel Gabriel example above, but instead the money is available for some agents and people on the market before it floats out in the rest of the economy. This means that some people can use their increase in money before any prices have risen. And as Rothbard says this increase will cause a permanent shift in wealth and income — especially for those on fixed income (Rothbard, 2011).
This leads us to the fallacy of measurement. For the economists who worships the Quantity Theory, a ten percent increase in the money supply, will, like we have previously mentioned result in a ten percent price increase in all goods. This however, is not the case according to Mises. Prices will not rise uniformly and that is partly because of different scale of values for the economic agents. The goods that are being demanded in the beginning of the process will experience a higher price increase than most other goods, as Mises state in the following:

> *(...) the increase of prices continues, having a diminishing effect, until all commodities, some to a greater and some to a lesser extent, are reached by it* (von Mises, 1912, pp. 139).

According to the above-mentioned and Mises, you simply can not index the price increase uniformly, because of the wide ranges of different scale of values. This section of this short introduction to Austrian Monetary theory, deals with the purchasing power of money. According to Mises and Rothbard, the purchasing power of a currency tends to be not just alike, but the same throughout the area where the same currency is used. The obvious problem here is, that by the looks of it, this is not true. An apartment in Aalborg is definitely more expensive than one in the small town called Arden. Even though the good theoretically could be exactly the same, the important part is not the apartment, but how the consumers value the apartment. Aalborg is a bigger and obviuosly more exciting town, which is why consumers are willing to pay more, even though it is the *same* good. Rothbard sums it up:

> *At all times, a homogeneous good must be defined in terms of its usefulness to the consumer rather than by its technological properties*(Rothbard, 1963, pp. 302).

To understand this fully, another example can be given about the sun bed in Alaska and Miami. Even though it is the exact same model of the sun bed, a consumer in Alaska would not put much value into it - however in Miami it is much more useful. To conclude

[15] `https://wiki.mises.org/wiki/Richard_Cantillon`

this paragraph, the value of money in one nation is the same, but a nation is but a complex collection of different individuals who has a vast array of different wants. The last point is very important in Mises' development of his *purchasing-power-parity* theory. This probably reminds you of something, but this theory slighty differs from the one which Cassel put forth. The main objective still being that the exchange ratio between two currencies - does not matter whether it is silver/gold or euro/dollars - equals the ratio between their respective purchasing power. The main difference being that Cassel's theory does not take into account the locational differences in wants and needs as mentioned above.

Mises developed a regression theorem[16] in 1912 (Rothbard, 2011), to solve the 'austrian circle' problem which circled around the problem that money is demanded because of its pre-existing purchasing power. As Rothbard states:

> *(...) money is not useful in itself but because it has a prior exchange value, because it has been and therefore presumably will be exchangeable in terms of other goods. In short, money is demanded because it has a pre-existing purchasing power; its demand not only is not independent of its existing price on the market but is precisely due to its already having a price in terms of other goods and services* (Rothbard, 2011, pp. 305).

Rothbard states that Mises's theorem is able to fully explain the demand for money as well as integrating the theory of marginal utility with his monetary theory — and furthermore it brings evidence that money did indeed originate from barter (Rothbard, 2011). Regarding the supply of money, Mises position is very clear. As mentioned in this whole section, money is a commodity, a good. Not a good you can consume directly, but a good you can use in exchange for almost every other directly consumable good. The biggest difference between money and these other commodities is the fact that an increase in consumer goods would mean a bigger supply to consume and therefore a lower price. So an increase would benefit the consumer. However, an increase in the money supply will not, as we have discussed above, make you more rich. As Rothbard states:

> *An increase in the supply of money causes no increase whatever in the exchange service of money; all that happens is that the purchasing power of each unit of money is diluted by the increased supply of units* (Rothbard, 2011, pp. 310-311).

This is not meant to say that money is neutral - because they definitely are not. An increase in the money supply will have an effect on real side of the economy, but unlike an increase in consumer goods, not everyone will benefit from it. To imagine a constant money supply would for most governments seem terrifying. However, Rothbard has a positive view of it:

> *A world of constant money supply would be one similar to that of much of the eighteenth and nineteenth centuries, marked by the successful flowering of the Industrial Revolution with increased capital investment increasing the supply of goods and with falling prices for those goods as well as falling costs of production. As demonstrated by the notable Austrian theory of the business cycle, even an inflationary expansion of money and credit merely offsetting the*

[16] See (Rothbard, 2011, pp. 305-306) for an explanation

> *secular fall in prices will create the distortions of production that bring about the business cycle* (Rothbard, 2011, pp. 311-312).

This is hard to imagine, but it could be the case if cryptocurrency gets implemented. In the next section we will examine whether or not cryptocurrency can be defined as a currency.

3.3 Cryptocurrency - Is it a currency?

In the field of economics, there is a common way to decide if a good can be said to be a currency. The good should excel at three things; working as a medium of exchange, as a unit of account and finally as a store of value. In this section, we will go through these three attributes to decide whether or not cryptocurrencies can be defined as a currency.
As of this moment there is 1,563 registered cryptocurrencies and even though a lot of them have some similarities, it is still the Bitcoin, which is worth the most. Unlike gold and other precious metals, and more like the fiat currency, cryptocurrencies has no intrinsic value and because of this, it can be argued that its fundamental value is zero (Cheah and Fry, 2015). Therefore, its worth is *decided* by the consumers' demand of the coin, which normally is an attribute assets have. So is the bitcoin an asset or a currency? David Yermack finds that the daily volume of transactions is about 70,000 and of these 70,000 Fred Ehrsam estimates that about 80 percent of that is speculation (Chuen et al., 2015, ch. 2). As of today, using the same reference, we find that the daily volume ranges from 135,000 to 210,000. However, in early january, when the bitcoin was still peaking in terms of value, sitting at around $17,000, the daily volume of transactions reached 425,000[17]. These rises in transactions are most likely caused by the enormous speculations in bitcoins during the end of 2017 and the beginning of 2018. But taking Ehrsams estimations without touching it, 80 percent of the transactions is speculative, only 85,000 is involving the purchase of a product or service, which in a world with +7.5 billion people is not much.

Medium of exchange

That brings us to the first attribute a currency should have. It shall work as a medium-of-exchange. Obviously, there is definitely ground for cryptocurrencies to work as a medium. One of the biggest problems is that not all retailers accepts these currencies yet. This is one of the obstacles that has to be torn down. Furthermore, some critique of the transaction time of bitcoin has been noted, for example Roger Aitken in an article from Forbes, where he mentions that bitcoin only can handle 7 transactions per second, whereas the good, old Visa can handle 65,000[18]. However, other cryptocurrencies, like Dash for example have introduced an *InstantSend*-option, where confirmation happens in seconds[19]. This means, that there is definitely a possibility for cryptocurrencies to be used as a medium, but there is still one big problem. These currencies have to be recognised around the world as a proper payment method.

[17] https://blockchain.info/charts/n-transactions?timespan=all
[18] https://www.forbes.com/sites/rogeraitken/2018/03/02/cryptocurrencies-slammed-as-speculative-mania-by-cent
[19] https://cointelegraph.com/news/top-10-altcoins-all-you-wanted-to-know-about-bitcoins-contenders

Unit of account

To be a unit of account is a bit more complicated. Imagine you are back in the barter economy. As before mentioned you would very much like a steak to go a long with your bread, but how much steak can you get for one bread? This is impossible to know without having a medium of exchange. With a medium you know that one bread costs a dollar, while a steak is ten dollars. It is pretty easy to see that the steak costs ten times more. That way you know that you have to produce eleven pieces of bread. One for you, and ten for the steak. In the modern day life it is a bit easier to handle, given that you can work to gain money, which you can freely choose to spend on whichever good you would like. As of now, it can be argued that it is just as difficult to recognise the price difference with Bitcoin as it was with the bread. Given that the one bitcoin is approximately worth \$10,000[20], means that a Big Mac on McDonald's costs around 0,00053 BTC while a bike for kids costs 0,0074 BTC. For the economists and math teacher, you would say the price is around 10 times higher, a little bit more actually, but for the Average Joe in the shopping mall, the difference is far from crystal clear. But as Yermack says in the big handbook (Chuen et al., 2015), this is not a difficult obstacle to overcome. Previously it was the other way around due to inflational tendencies in the economy, such as in Italy where an ice-cream costed 5000 lira. In the bitcoin case, it should be possible to turn it the other way around, so that 0,0001 BTC can be represented as 1 microBTC. In the above-mentioned example, the Big Mac would now cost 5,3 microBTC while the bike would cost 74 microBTC. Chuen et al. (2015)
However, in order to be a stable unit of account, the price needs to be stable as well. This is obviously not the case as we saw in figure 1. This is the most important attribute, and is the problem for both the unit of account and the next section store of value.

Store of value

The third property a currency should meet to be recognised as a currency, is to be a store of value. To be a store of value, means that you should be able to hold on to your money, without being afraid that it could lose its value. That is something the commodity money, like gold and silver excels at, given that its value does not depreciate and the fact that metal is eternal. A good like bread and butter does not last forever, which therefore makes these goods impossible to implement as a currency, as you would have to use the money before a certain date. For a cryptocurrency, it certainly is not a problem that it eventually would melt or mold away. However, for cryptocurrency the biggest problem is its volatility. The price of especially bitcoin has been extreme volatile during the last year, experiencing a sixfold rise in its price. As Yermack says, this behaviour does not seem anything near that of a trusted currency:

> *The excessive volatility (...) is more consistent with the behavior of a speculative investment than a currency* (Chuen et al., 2015, ch. 2).

So, the real question to be asked here is how and whether cryptocurrency can be compared to other speculative assets. The next section will take a look at this.

[20] `coinmarketcap.com`

4 Classifying Cryptocurrencies

The term cryptocurrency can be quite misleading as it leads one to believe that cryptocurrencies are a part of the currency asset class. However, as argued in Chapter 3 the most popular cryptocurrencies of today do not really have the basic properties that a currency is expected to have. Therefore another name might be more suitable, but what exactly is a cryptocurrency, if it is not a currency? Should it be seen as being a new asset class or does it belong to one of the already existing classes such as precious metals or equities? These questions are highly relevant as the popularity and awareness of cryptocurrencies keep increasing and governments around the world are taking their stand on cryptocurrencies by introducing varying degrees of regulation. Furthermore, if cryptocurrencies can be seen as their own asset class, it is interesting for investors to investigate what effect cryptocurrencies can have on optimal portfolio structures.
The first section takes a look on how various countries are taking different approaches to the regulation and taxation of cryptocurrencies. Section two offers an empirical investigation into if cryptocurrencies should be considered their own asset class.

4.1 National approaches

The rules governing cryptocurrencies varies wildly by country as there is no global coordination concerning the topic and for a lot of countries the whole cryptocurrency community is operating in a grey area both with the matter of what rules applies to cryptocurrency exchanges and which tax rules apply to cryptocurrencies. A quick but very comprehensive overlook, in the sense of the stand of countries, can be found on the Bloomberg website[21]. In this section we present the standpoint of the U.S Japan, China and Germany.

In the U.S.A the Internal Revenue Service(IRS) has stated that virtual currency and thereby cryptocurrencies is treated as property for U.S. federal tax purposes[22], this puts cryptocurrencies along assets such as gold and real estate, which is also considered as property by the IRS. The Foreign Account Tax Compliance Act (FATCA), however, which requires foreign financial institutions to provide the IRS with information about accounts held by U.S. taxpayers or foreign entities controlled by U.S. taxpayers, [23] are considering cryptocurrency exchanges to be financial institutions, thereby in some sense treating cryptocurrency as money.
Another U.S governmental institution, the U.S. Commodity Futures Trading Commission (CTFC), has a different stand on cryptocurrency, as a 2015 press release stated that

[21] https://www.bloomberg.com/news/articles/2018-03-26/what-the-world-s-governments-are-saying-about-cryptocu
[22] https://www.irs.gov/newsroom/irs-virtual-currency-guidance
[23] http://www.cpapracticeadvisor.com/news/12380583/the-classification-of-bitcoin-and-cryptocurrency-by-the-i

"CFTC Holds that Bitcoin and Other Virtual Currencies Are a Commodity Covered by the Commodity Exchange Act."[24] Thereby contradicting the view of the IRS.
A third approach is taken by the U.S. Securities and Exchange Commission (SEC), who are handling the issue of cryptocurrencies on a case to case basis. In a public statement in 2017 the SEC Chairman Jay Clayton announced that

> *It has been asserted that cryptocurrencies are not securities and that the offer and sale of cryptocurrencies are beyond the SEC's jurisdiction. Whether that assertion proves correct with respect to any digital asset that is labeled as a cryptocurrency will depend on the characteristics and use of that particular asset.*[25]

On the 1st of December, 2017, Japan's National Tax Agency(NTA)released a statement classifying capital gains from cryptocurrency as miscellaneous income, which mean that any income earned on an individual level obtained from virtual currency is subject to tax on aggregate income. For tax purposes gains and losses from foreign currency transaction are treated exactly the same way in Japan.[26] Since the gains from virtual currencies are taxed through aggregate income the percentages that should be payed run from 15 to 55 percent[27]. To comparison capital gains from investing in stocks are taxed around 20 percent. As was the case in Canada the purchase of goods using cryptocurrency is also a taxable event.

Recently China has taken a lot of measures to stop its citizens from trading in cryptocurrencies, by banning crypto exchanges and *initial coin offerings*(ICOs), which is the equivalent to initial public offerings for new virtual currencies and by making the great firewall of China block access to overseas trading platforms and cutting of power to mining pools. However in December 2013 the People's Bank of China along with five other government ministries published an official notice stating that Bitcoin was being classified as a virtual commodity and therefore should not be seen as a currency. A similar notice was issued in Jan 2017, emphasizing that the classification of Bitcoin and other cryptocurrencies as a virtual commodity has not changed.[28]

The Federal Ministry of Finance in Germany issued a notice on February 27, 2018, regarding taxation of cryptocurrency.[29] It is made clear that cryptocurrencies will be treated as legal tender, when it is used for purchases. This means that even though the coins used for the purchase has appreciated since they were acquired, the buyer does not need to pay any taxes. Furthermore Germany considers cryptocurrencies as private money, which give cryptocurrencies cconsiderable tax benefits compared to stocks. Private sales that do not exceed 600 euros are tax exempted and if a cryptocurrency is held for more than a year

[24] https://www.cftc.gov/PressRoom/PressReleases/pr7231-15
[25] https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11
[26] https://medium.com/@norbert.gehrke/japan-income-tax-on-virtual-currencies-8e8c170195a2
[27] https://www.bloomberg.com/news/articles/2018-02-08/crypto-investors-in-japan-face-tax-of-up-to-55-on-t
[28] https://intpolicydigest.org/2018/02/23/the-future-of-cryptocurrency-in-china/
[29] https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/2018-02-27-umsatzsteuerliche-behandlung-von-bitcoin-und-anderen-sog-virtuellen-waehrungen.html

no tax has to be paid no matter how much it has appreciated.

As it can be seen from the very different standpoints of some of the biggest economies in the world, cryptocurrencies have not been around long enough to be uniquely described and defined. In the U.S.A alone some of the major governmental institutions do not even agree on, what this thing called cryptocurrencies should be defined. The sector has gotten massive attention in the last years but it is still unsure how the huge potential of cryptocurrencies will unfold and it what way they will end being used by people. Will it be as a means of payments or will the speculating part keep playing a huge role?
The next section aims to provide insight into the apparent state of cryptocurrencies as and investigate if the group of cryptocurrencies can be considered as their own asset class.

4.2 What asset class does cryptocurrencies belong to?

What is an asset class?

In order to investigate if cryptocurrencies should be classified as it own asset class or if it belongs to an already existing asset class, a proper description of what is considered an asset class is needed.
So what is an asset class? Lustig (2014) looks to the dictionary for the definition of asset and class, which leads him to the following definition:

> *An asset class is a category of valuable things that share common attributes and can be differentiated from other asset classes.*

Also Greer (1997) offers his view of a definition as,

> *An asset class is a set of assets that bear some fundamental economic similarities to each other, and that have characteristics that make them distinct from other assets that are not part of the class.*

Greer argues that most assets can be put in one of the following three super classes of assets,

- Capital assets are assets such as equities, bonds and real estate, that provide an ongoing source of value and their value are measured by calculating the present value of the expected returns.
- Consumable/transformable assets such as commodities, they do not yield an ongoing stream of value in contrast to capital assets, instead they can be transformed into another asset or they can give utility through consumption.
- Store of value assets such as currency and art can neither be consumed nor do they generate an ongoing stream of value. Nevertheless they have monetary value.

The borders separating the super asset classes may, however, sometimes be blurry as precious metals fulfil both the properties of consumable/transformable assets and store of value assets. The super classes are quite extensive in their definition and each of them therefore contains more than one of what is thought of as traditional asset classes. Capital assets includes for example both equities and bonds, but they differ quite substantially in

their basis of value, as equities provides a claim on a company's future cash flows, while bonds provides a claim to a fixed amount of payments over a finite period of time.
The aim of this analysis is to see if cryptocurrencies should be considered their own asset class and the super classes become for that purpose to extensive in their definitions, instead we will focus on their layer of classification that separates traditional asset classes. Both Lustig (2014) and Burniske and White (2017) puts up characteristic that a group of investments need to satisfy for them to be considered their own asset class. Building upon that work we set up five criterias that cryptocurrencies need to fulfil for them to be considered their own asset class.

1. The group must be investable, providing sufficient liquidity and opportunity for investments.
2. Reliable data for the group of investments need to be available.
3. The investments in the group must share similar attributes in basis of value, governance and use cases.
4. There needs to be a high degree of correlation between returns within the group of investments.
5. The group should be exclusive from other asset classes.

If the first four criterias are fulfilled cryptocurrencies are a potential asset class. Furthermore if they do not share attributes with other traditional assets classes and their market value fluctuates relatively independently of the traditional asset classes, we argue that it should be considered its own asset class. This is what is meant by criteria five.

4.3 Data

The cryptocurrency data used in the analysis have been obtained from `coinmarketcap.com`, which collects data from all the exchanges that the respective cryptocurrencies are listed on and reports the daily volume weighted average prices and total volume. The data are collected, recorded, and reported in UTC time.
Cryptocurrencies can be divided into cryptographic *coins* and cryptographic *tokens*. A coin operates its own proprietary blockchain, protocol and currency, while a token does not use its own blockchain and might follow another cryptocurrency's protocol as well. For the analysis the top 10 coins with respect to market cap as of May 4th, 2018 and with a price history of more than 600 days have been chosen as representatives for the potential cryptocurrency asset class. they can be seen in Table 1.
Financial market data of daily prices representing traditional market classes have been obtained from the Federal Reserve Bank of St. Louis, except for the Bond data and the data on Apple, Amazon, Alphabet, Facebook and Microsoft, which has been obtained from `finance.yahoo.com`. The obtained data can be seen in Table 2.

4.4 Methodology

The aim of our methodology is two-fold. First we wish to analyse if the group of cryptocurrencies fulfil the properties that are required to be considered a separate asset class.

Cryptocurrency	**Market Cap**
Bitcoin (BTC)	164,956,000,000
Ethereum	77,066,200,000
Ripple	34,537,000,000
Litecoin	9,045,430,000
Stellar	8,138,850,000
Neo	5,700,730,000
Dash	4,047,060,000
Monero	3,945,670,000
Nem	3,906,870,000
Ethereum Classic	2,306,220,000

Table 1: Top 10 cryptocurrencies with respect to market cap and a price history longer than 600 days.

Asset Class	**Representatives**	**Description**
Stock Index	S&P500	Includes 500 leading companies in leading industries of the U.S. economy, which are publicly held on either the NYSE or NASDAQ.
	Nikkei 225	Comprising 225 highly liquid stocks of the Tokyo Stock Exchange.
Commodities	Oil	West Texas Intermediate crude oil prices.
	Gold	The London Bullion Market Association Gold Price.
Bonds	Bond Index	Seeks to track the investment results of the Bloomberg Barclays U.S. Aggregate Bond Index.
Currencies	Major/USD	Major currencies index includes the Euro Area, Canada, Japan, United Kingdom, Switzerland, Australia, and Sweden.
	USD/EUR	The price of 1 EUR in USD.
	JPY/USD	The price of 1 USD in JPY.
	CNY/USD	The price of 1 USD in CNY.
Real Estate	Wilshire Index	Measures U.S. publicly-traded real estate securities. Designed to offer a market-based index that is reflective of real estate held by pension funds.

Table 2: Traditional asset classes included in the empirical analysis.

The group is therefore evaluated with regard to its liquidity, politico-economic profile and correlation both with other asset classes and within the group of cryptocurrencies. No real theory is employed in the analysis of the politico-economic profile, therefore this will just be presented in the empirical analysis part.
Secondly we wish to analyse if cryptocurrencies have a positive impact on optimal portfolio structures by conducting an analysis in a mean-risk framework.

Liquidity

To measure how the group of cryptocurrencies perform with respect to the investability criterion the exchange traded volumes of the cryptocurrencies is used as a measure of liquidity. The trading volumes of the top five cryptocurrencies with respect to market cap and an equally weighted crypto index of the top ten cryptocurrencies are compared to the trading volumes of Apple, Alphabet, Amazon, Facebook and Microsoft and a basket of these five stocks to put them into perspective.
Furthermore we construct the turnover rate which gives an indication of times the outstanding volume of the asset changes hands. The turnover rate is defined as $T = V/M$, where V is traded volumes and M is the market capitalization. The market capitalization of Apple, Alphabet, Amazon, Facebook and Microsoft are calculated using the quoted number of outstanding share in the most recently filed quarterly or annual report. As we are interested in the market of today only data from 2018 is used in this part.

Correlation

To measure the degree of return correlation within the group of cryptocurrencies and between cryptocurrencies and traditional assets, daily log returns for every asset in the analysis are computed. All log return time series are tested for normality using the Jarque-Bera test, which have been shown to be superior in power to its competitors for symmetric distributions with medium up to long tails and for slightly skewed distributions with long tails.[30] The Jarque Bera test is given by

$$JB = n\left(\frac{S^2}{6} + \frac{(C-3)^2}{24}\right),$$

where n is the number of observations, S is the sample skewness coefficient and C is the sample kurtosis coefficient. JB is asymptotically chi-squared distributed with two degrees of freedom.
For the estimation of correlation Spearman's correlation coefficient is chosen, as it does not require the data to be normally distributed. To calculate the coefficient between a variable X and a variable Y a rank is assigned to each observation. To determine the rank of an observation the absolute deviations from the sample mean μ_0, given by

$$|X_1 - \mu_0|, \ldots, |X_n - \mu_0|,$$

is considered and ordered by size, from smallest to largest. Each observation is then given a rank R_k such that $R_k = j$ if X_k has the jth smallest absolute deviation from μ_0. Assuming

[30] Thadewald and Buning (2007)

that there is no ties in terms of rank in the data, Spearman's correlation coefficient is given by

$$\rho = 1 - \frac{6}{n(n^2-1)} \sum_{k=1}^{n} (r_k - s_k)^2,$$

where r_k is the rank of X_k among $X_1, \ldots, X_n$ and s_k is rank of Y_k among $Y_1, \ldots, Y_n$. To test the hypothesis $H_0 : \rho = 0$ the test statistic

$$T = \rho \sqrt{\frac{n-2}{1-\rho^2}}$$

can be used. The test statistic T approximately follows a t distribution with $n-2$ degrees of freedom for large n.

Portfolio Optimization

To perform an analysis of the group of cruptocurrencies effect on optimal portfolio structures we addopt the framework introduced by Markowitz (1952) which has become known as modern portfolio theory (MPT). The theory suggest that portfolio choice must be made with respect to the expected portfolio return and the variance of the return, which is used as a measure of risk. Markowitz emphasises that if two portfolio offers the same expected return, the one which has less risk should be preferred. The optimization problem can therefore either be formulated as allocating assets so that expected return is maximized for a given risk level or to minimize risk for a given level of expected return. This section is based on Svetlozar T. Rachev and Fabozzi (2008).
The framework for optimal portfolio choice, which Markowitz introduced, is known as mean-variance analysis, it can be mathematically presented as follows. Considering n different financial assets, the asset returns are denoted by the vector $\mathbf{r} = (R_1, R_2, \ldots, R_n)^T$, where R_i is the return of the i-th asset. The expected returns are denoted by

$$\mathrm{E}(\mathbf{r}) = (\mathrm{E}(R_1), \mathrm{E}(R_2), \ldots, \mathrm{E}(R_n))^T.$$

To construct a portfolio a weight vector $\mathbf{w} = (w_1, w_2, \ldots, w_n)^T$ is designed in which w_i is the portfolio weight of the i-th asset. Our analysis only considers long positions and therefore all weights should be nonnegative, $w_i \geq 0$, and they should sum to one, $\sum_1^n w_i = 1$. The expected portfolio return can then be calculated as

$$\mathrm{E}(P_r) = \mathbf{w}^T \mathrm{E}(\mathbf{r}) = \sum_{i=1}^{n} w_i \mathrm{E}(R_i).$$

Assuming that the portfolio risk V is a function of $\mathbf{w}$ and $\mathbf{r}$ and letting $\mathbf{e} = (1, 1, \ldots, 1)^T$ the optimal portfolio in the MPT is given by the solution to the optimization problem

$$\begin{aligned} \min_{w} \quad & V(\mathbf{w}, \mathbf{r}) \\ \text{subject to} \quad & \mathbf{w}^T \mathbf{e} = 1, \\ & \mathbf{w}^T \mathrm{E}(\mathbf{r}) \geq t_r, \\ & w_i \geq 0, \end{aligned} \tag{4.1}$$

where t_r is the target return rate.
The solution to 4.1 depends on the target return rate, t_r, if the target rate is set to zero the most diversified portfolio with minimum risk will be the optimal portfolio, while the portfolio only containing the asset with the highest expected return also will be an optimal portfolio, as no other combination will yield higher expected return. Adjusting the target return rate therefore yields a set of optimal portfolio known as *efficient portfolios*. If the efficient portfolios are known it is easy to determine the trade-off between risk and expected return, this trade-off is known as the *efficient frontier*.
In the optimization problem 4.1 the risk measure is not defined. When MPT was introduced the variance/standard deviation was used as a measure hence the name mean-variance analysis, however the standard deviation is not a true risk measure but a measure of dispersion. Risk is only concerned with losses and therefore the standard deviation, which penalizes symmetrically both positive and negative deviations from the mean, is a not a good choice. Instead we adopt the *conditional value-at-risk* (CVaR) for the empirical analysis.

CVaR

The CVaR is defined using the *value at risk* (VaR), which is a measure for the minimum level of loss at a given confidence level for a predetermined time period. If for example the loss of an asset is greater than 1$ million with probability 1 percent over the next month, the one month $\text{VaR}_0.01$ is equal to 1$ million. Formally the VaR is defined as

$$\text{VaR}_\epsilon(R) = -\inf_r\{r \mid \text{P}(R \leq r) \geq \epsilon\}, \tag{4.2}$$

where $\epsilon \in (0, 1)$ and P() is the distribution function.
The CVar is defined as the average of the VaRs that are larger than the VaR at probability ϵ, thereby taking the magnitude of the losses that are larger than the VaR level under consideration, which the VaR does not. The CVaR is defined as

$$\text{CVaR}_\epsilon(R) = \frac{1}{\epsilon}\int_0^\epsilon \text{VaR}_p(R)dp. \tag{4.3}$$

An illustration of the VaR and CVaR can be seen in Figure 5.
If the return distribution is a continuous function, the CVaR can be represented in a more intuitive form in terms of a conditional expectation,

$$\text{CVaR}_\epsilon(R) = -\text{E}\left(R \mid R < -\text{VaR}_\epsilon(R)\right), \tag{4.4}$$

which is known as *expected shortfall* (ES) denoted by $ES_\epsilon(R)$. The ES shows that the CVaR is equal to the average loss if the loss is larger than the VaR level.

CVaR Estimation

One method of estimating the CVaR for a return series is to use historical data. Ordering the observed sample portfolio returns $r_{p1}, r_{p2}, \ldots, r_{pn}$ at times $t_1, t_2, \ldots, t_n$ after magnitude, such that $r_{p(1)}$ denotes the smallest observed return and $r_{p(1)}, r_{p(2)}, \ldots, r_{p(n)}$, the CVaR can be estimated using the formula

$$\widehat{\text{CVaR}}_\epsilon(\mathbf{r}) = -\frac{1}{\epsilon}\left(\frac{1}{n}\sum_{k=1}^{\lceil n\epsilon\rceil-1} r_{p(k)} + \left(\epsilon - \frac{\lceil n\epsilon\rceil - 1}{n}\right) r_{p(\lceil n\epsilon\rceil)}\right) \tag{4.5}$$

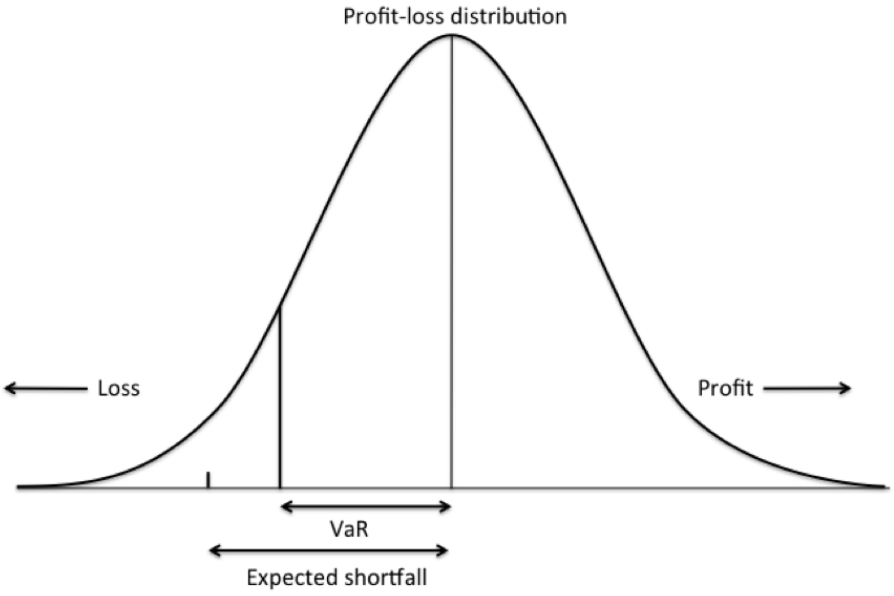


Figure 5: VaR and CVaR in a return distribution.

where the notation $\lceil x \rceil$ denotes the smallest integer larger than x. This method however has some major drawbacks, as the estimate will be very inaccurate for low probabilities where only very few data points are used for the estimation. Furthermore the used data points are the ones with the smallest value and they will therefore change substantially from sample to sample.
An alternative is the *Monte Carlo method*, which consists of the following steps:

1. *Selection of model.* The selected model should be able to explain observed characteristics of the sample data such as heavy tails, skewness and volatility clustering that might effect portfolio risk.

2. *Estimation of model parameters.* Sample of returns is used to estimate the parameters of the model.

3. *Simulations from fitted model.* Independent stock returns scenarios are drawn from the fitted model over a given period. Thereby creating different scenarios of time series of portfolio returns.

4. *Calculating portfolio risk.* The portfolio risk is calculated for each scenario simulated in step 3.

The performance of the Monte Carlo depends on the selected model and the number of scenarios simulated. One could for example generate a sample of 5000 portfolio returns using the specified model and then use equation (4.5) to calculate the CVaR for this sample. Doing this for example 100 times and then calculate the mean of the 100 estimated CVaR's gives a pretty accurate estimate if the selected model describes the data well. The more scenarios simulated the better the approximation of the portfolio risk. This method is therefore quite time consuming compared to the historical method, however it gives better approximations as it incorporates both historical observations and future expectation.

When a portfolio is considered the selected model needs to be capable of capture the behaviour of the stock returns on a stand alone basis and the dependence between them. If, for example, it is assumed that the joint stock return distribution is a multivariate normal distribution the behaviour of individual stocks are captured by the normal distribution while the covariance matrix of the multivariate normal distribution describes their dependence. However return data rarely follows normal distributions and therefore a more flexible statistical model will provide better approximations.
Generalized hyperbolic distributions (GH) introduced by Barndorff-Nielsen and Halgreen (1997) are more flexible than normal distributions and can therefore provide better fits to return data.

Generalized Hyperbolic Distribution

In the univariate case the density function of the GH distribution of $X \in \mathbb{R}$ can be represented as

$$GH(X;\lambda,\alpha,\beta,\lambda,\mu) = a(\lambda,\alpha,\beta,\delta,\mu)\frac{K_{\lambda-1/2}\left(\alpha\sqrt{\delta^2+(X-\mu)^2}\right)}{\left(\sqrt{\delta^2+(X-\mu)^2}\right)^{\frac{1}{2}-\lambda}}\exp^{\beta(X-\mu)} \tag{4.6}$$

where

$$a(\lambda,\alpha,\beta,\delta,\mu) = \frac{(\alpha^2-\beta^2)^{\lambda/2}}{\sqrt{2\pi}\alpha^{\lambda-1/2}\delta^{\lambda}K_{\lambda}\left(\delta\sqrt{\alpha^2-\beta^2}\right)}$$

and K_λ denotes the modified Bessel function of the third kind with order λ defined as

$$K_\lambda(X) = \frac{1}{2}\int_0^\infty y^{\lambda-1}\exp^{-\frac{X}{2}(y+y^{-1})}\,\mathrm{d}y, \quad X>0. \tag{4.7}$$

The parameters μ, δ, β and α describes location, scale, skewness and shape respectively. The distribution is symmetric if β is equal to zero and otherwise the value of β determines if the skewness is positive or negative. The shape is changed with the value of α as the kurtosis of the distribution increases when α increases.
Figure 6 displays the quantile-quantile plots of observed bitcoin log returns and the theoretically hyperbolic and normal distribution respectively. It is evident from the plots that the hyperbolic distribution is better at describing the distribution of bitcoin log returns than the normal. Using the generalized hyperbolic distribution to specify the distribution of the one-dimensional distributions require the use of a copula function to describe their dependence.

Copula

The distribution of a multivariate random variable $\mathbf{X}$ such as portfolio returns can be factored into two separate components, one representing the purely univariate features of $\mathbf{X}$ in the form of marginal distributions and one repesenting the purely joint features in the form of a copula, C. Copulas therefore links multivariate distribution functions to their marginal distributions such that

$$F(X_1,X_2,\ldots,X_n) = C\left(F_1(X_1,X_2,\ldots,X_n)\right., \tag{4.8}$$

where F denotes the joint distribution and F_i denotes the marginal distribution of X_i. From (4.8) it can be seen that a copula function needs to satisfy the following properties

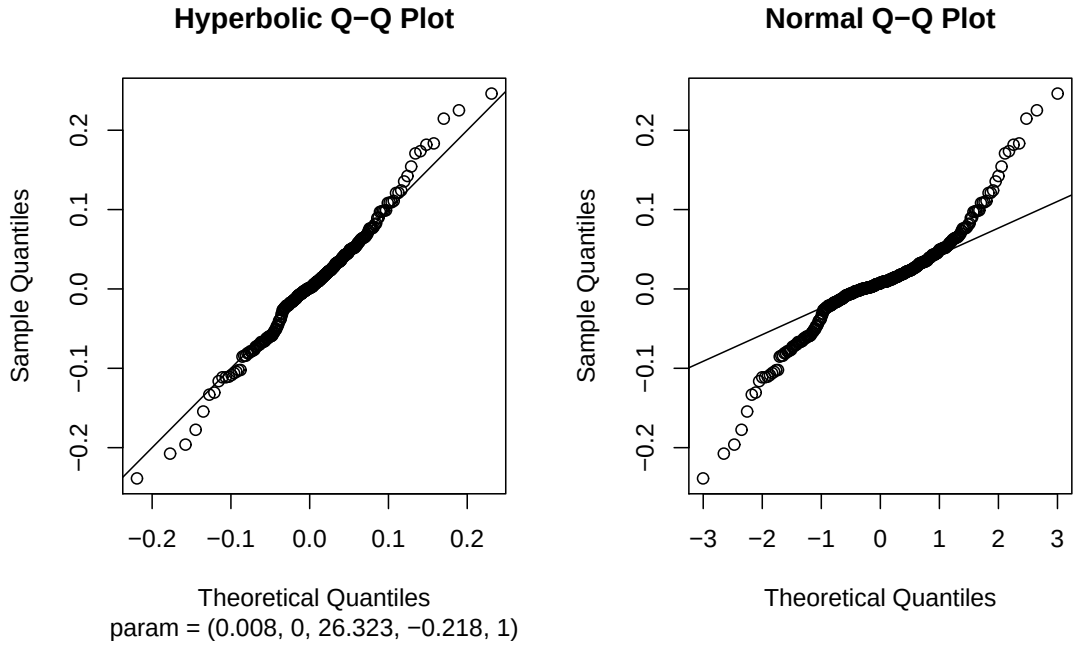


Figure 6: Q-Q plots of bitcoin log returns.

- $C : [0,1]^n \to [0,1]$.
- $C(u_1, u_2, \ldots, u_n)$ is an increasing function of each u_i.
- $C(1, \ldots, 1, u_i, 1, \ldots, 1) = u_i$

The first property must be satisfied since the codomain of the copula needs to match that of the jointly distribution F. The same goes for the second property, as the copula needs to match this fundamental property of the distribution function. The third property comes from the fact that if $F_i(X_i) = 1$, then $X_i = \infty$, so $C(1, \ldots, 1, u_i, 1, \ldots, 1)$ corresponds to $F(\infty, \ldots, \infty, F_i^{-1}(u_i), \infty, \ldots, \infty)$ which is equivalent to $P\left(X_i \leq F_i^{-1}(u_i)\right)$.
The quite remarkable result in the following theorem about the existence of copulas was proved in 1959 by Abe Sklar.

4.1 Theorem (Sklar's theorem): If F is a multivariate cdf with marginals $F_1, F_2, \ldots, F_n$ then there exists a copula C such that

$$F(X_1, X_2, \ldots, X_n) = C\left(F_1(X_1, X_2, \ldots, X_n)\right)$$

The proof of Theorem 4.1 can be found in Lamberton and Lapeyre (2008). Sklar's theorem is very powerful in the sense that if we construct the univariate distributions of the stocks in a portfolio then we now that there exists a function, which can describe the dependence between the stocks, so that a full model can be estimated and used in the monte carlo method. The **copula** package in R can be used to find copulas for specific marginal distributions.

4.5 Empirical Analysis

Politico-Economic Features

The group of cryptocurrencies have unique features compared to traditional assets, when it comes to their basis of value and governance. Cryptocurrencies are purely digital and consensus based assets that have no intrinsic value but still can be used as a mean of payment. In this way cryptocurrencies differs from traditional asset class, as stocks have their basis of value in the form of fractional ownership of a company, bonds gives the right to future cash flows and gold have unique physical properties. In their basis of value cryptocurrencies have most in common with fiat currencies, which hold no intrinsic value as well. However fiat currencies are declared as legal tender by governments, whereas there is no legal entity that is accountable for the functioning of cryptocurrencies.
In terms of governance the cryptocurrency group also stands out from the rest of the asset classes. The cryptocurrencies are decentralized and depend on the network to maintain the ledger and verify transactions, a network which is accessible to everybody, as the software underlying the cryptocurrencies are open-source. Therefore the supply of cryptocurrencies are not left to decisions based on monetary policies as is the case for fiat currencies. Instead supply trajectory is known to everybody for example bitcoin and litecoin has a cap at 21 million and 84 million coins respectively with new ones being created with every block. Ethereum does not have a overall maximum cap but a yearly maximum cap of new created coins of 18 million and Ripple created 100 billion coins at inception with no more to ever be created. The predictable supply trajectory of cryptocurrencies is unlike any other asset.
The obvious applications of cryptocurrencies resemble the ones of fiat currencies and gold, as a store of value and a mean of payments, which is also the services that Bitcoin aim to provide. However cryptocurrencies are not limited to these two use cases, as different cryptocurrencies aim to provide different use cases. Ethereum provides decentralized application and smart contracts and Monero has been successful in making truly anonymous, private and fungible digital money.

Investability

The mean trading volumes in dollars of the cryptocurrencies and the stocks is displayed in Table 3, which shows that the mean dollar trading volume of bitcoin is on equal footing with the most traded of the five stocks, Amazon. Ethereum is approximately equal to the one of Microsoft and higher than Alphabet, the stock with the lowest trading volume, whereas Ripple, the third largest of the cryptocurrencies, fall short of all of the stocks. The mean trading volume of the crypto index is approximately equal to that of Ripple, which shows that bitcoin is still pulling the most attention from traders, in fact bitcoin accounts for approximately 57 percent of daily trading volume during the time period. The coefficient of variation is generally higher for the cryptocurrencies than for the stocks except for Facebook, especially Ripple and Stellar have really high CV's, which shows that there is a high sampling variation in daily trading volumes around their mean. This means that these cryptocurrencies are more likely to have been experiencing days with low trading volume, which is also seen from the minimum daily trading volumes. The CV of the crypto index, however, is not that high, as bitcoin is the only cryptocurrency with a lower CV. Again this points to the fact that bitcoin dominates the market, but also it

points to some averaging effect among the cryptocurrencies.

Considering the turnover rate, which is displayed in Table 4 the cryptocurrencies are dominating the stocks. Amazon, which has the highest liquidity if mean daily trading volume is used as a measure, has a turnover rate that is way lower than any of the cryptocurrencies. With respect to the coefficient of variation Ripple and Stellar are still high, but both bitcoin and ethereum are on equal footing with the stocks. Comparing the crypto index and the FAAMA group the crypto index is on average five times as liquid as the stock with approximately equal CV's.

These considerations points to a class of cryptocurrencies that can provide the liquidity that is necessary for investor that wants to enter or adjust investment positions. In absolute terms bitcoin and ethereum are on equal footing with some of the biggest firms in the stocks market and ripple is not far of. The group of cryptocurrencies as a whole still fall behind the FAAMA basket, which highlights the fact that the cryptocurrencies is very dominated by a couple of players and suggest relative weaker liquidity in the smaller coins. Even though the smaller coins might lack liquidity in absolute terms their turnover rate is impressive if this trend continuous as the sector grows in absolute terms, the cryptocurrencies will be a very liquid asset class.

Correlation

As it can be seen in Table 5 all of the presented log return series are non-normal according to the Jarque-Bera test. The same is true for the log return series of the rest of the cryptocurrencies and the rest of the traditional asset class representatives from Table 2. All of the series express positive excess kurtosis, which indicates fatter tails than a normal distribution. Mostly negative skewness is expressed for the traditional asset classes while the cryptocurrencies all have positive skewness, indicating the right tail to be longer than the left one.

The fact that the Jarque-Bera test points to non-normality makes Spearman's correlation coefficient seem like an appropriate choice of correlation measure. The estimated correlation between each pair of the ten cryptocurrencies can be seen in Table 6 ranging from 0.26 to 0.61. When testing for the null hypothesis that $\rho = 0$, the null hypothesis is rejected in every case, which shows that there exists strong return correlation within the

	Mean USD	**Min USD**	**St.Dev. USD**	**CV**
Crypto Index	1,497,725,296	519,502,430	804,640,786	53.7 %
Bitcoin (BTC)	8,628,739,274	3,652,500,000	3,933,964,457	45.6 %
Ethereum	3,021,252,734	948,488,000	1,821,668,517	60.3 %
Ripple	1,492,975,702	137,548,000	1,689,740,067	113.2 %
Litecoin	700,216,032	194,664,000	529,556,811	75.6 %
Stellar	176,639,936	18,973,800	215,731,450	122.1 %
FAAMA	5,150,878,423	2,330,832,992	1,691,094,187	32.8 %
Apple	6,307,061,736	3,259,193,668	2,141,844,254	34 %
Alphabet	2,072,073,495	1,001,233,522	820,947,021	39.6 %
Amazon	8,635,273,559	3,157,954,000	3,732,174,916	43.2 %
Facebook	5,708,691,865	1,806,492,182	3,904,854,835	68.4 %
Microsoft	3,031,291,461	1,569,498,304	980,392,180	32.3 %

Table 3: Descriptive statistics of daily trading volumes from 01-01-2018 to 04-05-2018.

	Mean %	**St.Dev. %**	**CV**
Crypto Index	4.44	1.42	32.1 %
Bitcoin (BTC)	5.02	1.46	29 %
Ethereum	3.85	1.50	39 %
Ripple	3.21	2.69	84 %
Litecoin	6.87	4.12	60 %
Stellar	2.20	2.16	98 %
FAAMA	0.84	0.28	33.7 %
Apple	0.75	0.27	36.1 %
Alphabet	0.55	0.22	40.4 %
Amazon	1.22	0.52	42.5 %
Facebook	1.38	1.00	72.2 %
Microsoft	0.43	0.14	32.8 %

Table 4: Descriptive statistics of turnover rates from 01-01-2018 to 04-05-2018.

group of cryptocurrencies. When estimating the correlation between cryptocurrencies and traditional asset classes the number of instances in which a cryptocurrency and one of the representatives of traditional assets experience significant correlation at the 5 percent level is presented in Table 7. The results show that cryptocurrencies returns moves relative independent of traditional asset returns, as only 15 out of 190 pairs express significant correlation.

	BTC	**S&P500**	**Oil**	**Gold**	**Bonds**	**USD/EUR**	**R. Estate**
Mean	0.0073	0.0006	0.0010	-0.00002	-0.0001	0.0002	-0.0002
St.Dev.	0.0576	0.0071	0.0176	0.0077	0.0020	0.0049	0.0089
Min	-0.2387	-0.0418	-0.0603	-0.0466	-0.0093	-0.0267	-0.0310
Max	0.2462	0.0268	0.0871	0.0279	0.0058	0.0156	0.0307
Skewness	0.0269	-1.0972	0.0642	-0.7519	-0.4003	-0.2833	-0.3217
Excess Kurtosis	3.4755	6.8032	1.8117	3.9751	1.0019	2.034	1.1948
J-B test	192(.000)	808(.000)	52(.0005)	286(.000)	26(.0005)	71(.000)	29(.000)

Table 5: Descriptive statistics of logreturn series for representatives of different asset classes over the time period from 12-09-2016 to 24-04-2018.

	BTC	ETH	XRP	LTC	XLM	NEO	DASH	XMR	XEM	ETC
BTC	1.00	0.43	0.32	0.57	0.35	0.35	0.46	0.37	0.39	0.40
ETH	0.43	1.00	0.37	0.52	0.38	0.43	0.55	0.60	0.60	0.44
XRP	0.32	0.37	1.00	0.39	0.61	0.26	0.38	0.35	0.33	0.46
LTC	0.57	0.52	0.39	1.00	0.37	0.33	0.45	0.47	0.43	0.42
XLM	0.35	0.38	0.61	0.37	1.00	0.32	0.48	0.39	0.36	0.47
NEO	0.35	0.43	0.26	0.33	0.32	1.00	0.32	0.42	0.33	0.41
XMR	0.46	0.55	0.38	0.45	0.48	0.32	1.00	0.45	0.55	0.47
ETC	0.37	0.60	0.35	0.47	0.39	0.42	0.45	1.00	0.54	0.42
DASH	0.39	0.60	0.33	0.43	0.36	0.33	0.55	0.54	1.00	0.45
XEM	0.40	0.44	0.46	0.42	0.47	0.41	0.47	0.42	0.45	1.00

Table 6: Spearman's correlation coefficient between the log return of cryptocurrencies.

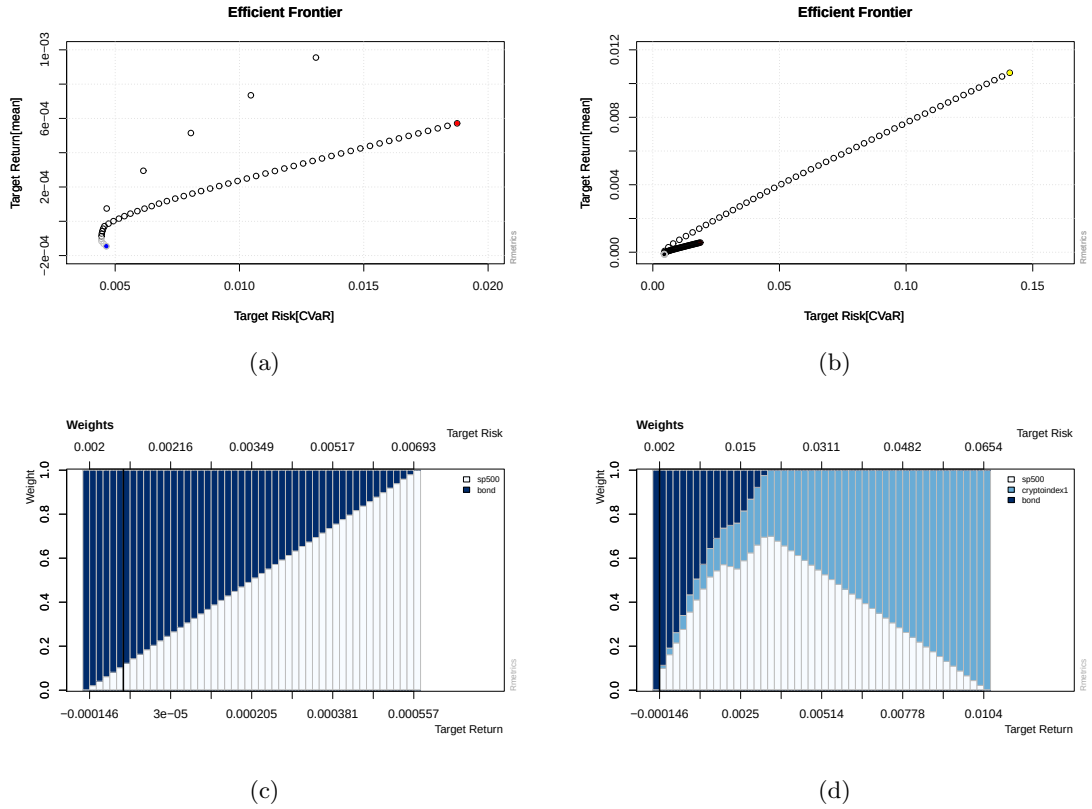
Asset Class	Significant Correlations	Of Total
Stock Indices	4	20
FAAMA	6	50
Bonds	2	10
Oil	0	10
Gold	2	10
Real Estate	0	10
FX	1	80
Total	15	190

Table 7: Number of instances of significant correlation at the 5 percent level between the 10 cryptocurrencies and the traditional asset class representatives.

Optimal portfolios

To evaluate the impact of including cryptocurrencies in portfolio structures we construct five portfolios composed of traditional asset representatives. The simplest portfolio (p1) consist of stocks represented by S&P500 and bonds. p1 is extended by adding gold (p2), gold and oil (p3), gold, oil and real estate (p4) and finally gold, oil, real estate and Euros. These five portfolios acts as benchmark portfolios to which cryptocurrencies are added to see the effect on efficient portfolios. The cryptocurrency asset class is added to each portfolio represented by an index that weigh each cryptocurrency according to its relative market size cap with the constrain that no weights can be higher than 0.3. The efficient frontiers for each portfolio when only long positions are considered are calculated using the R package **fPortfolio**[31]. How the estimation of CVaR is carried out in **fPortfolio** is not clear. The estimation is based on daily log returns over the time period from the 12th of September 2016 to the 4th of May 2018.
From Figure 7(a) and (c) it can be seen that even though the expected returns of the bondindex is negative, they are still positive for the portfolio structure if a lower risk than that of a portfolio consisting exclusively of S&P500 is wanted. It is also evident from Figure 7(b) that both the expected value and CVaR of the cryptoindex is very high if compared to the bondindex and S&P500. Furthermore the inclusion of the cryptoindex to the portfolio helps improve the portfolio structure, as can be seen both from the efficient frontiers and the weights depicted in 7(d). For given target risks, the inclusion of cryptocurrencies, even just a small proportional amount, will raise the expected return.
The efficient frontiers and optimal weight graphs for the p2 portfolio can be seen in Figure 8. Gold, just like bonds, has a negative expected return, but still it is beneficial for the portfolio structure in terms of diversifying. This can be seen in 8(d) where the weights of gold in some of the efficient portfolios with low risk is on level or even higher than the weights of the cryptoindex. The portfolios in which some portion consists of cryptocurrencies are again superior to the ones only including traditional assets, the efficient frontiers in 8(a) shows this very clearly.
The efficient frontier of the p3 portfolio in Figure 9(a) shows that oil has the highest expected return and risk of the traditional assets considered so far. It does not, however, come close to the characteristics of the cryptoindex. The addition of oil to the portfolio does not cancel out the positive effect of the cryptoindex, which still receive a small

[31] `https://cran.r-project.org/web/packages/fPortfolio/fPortfolio.pdf`



(a) (b)

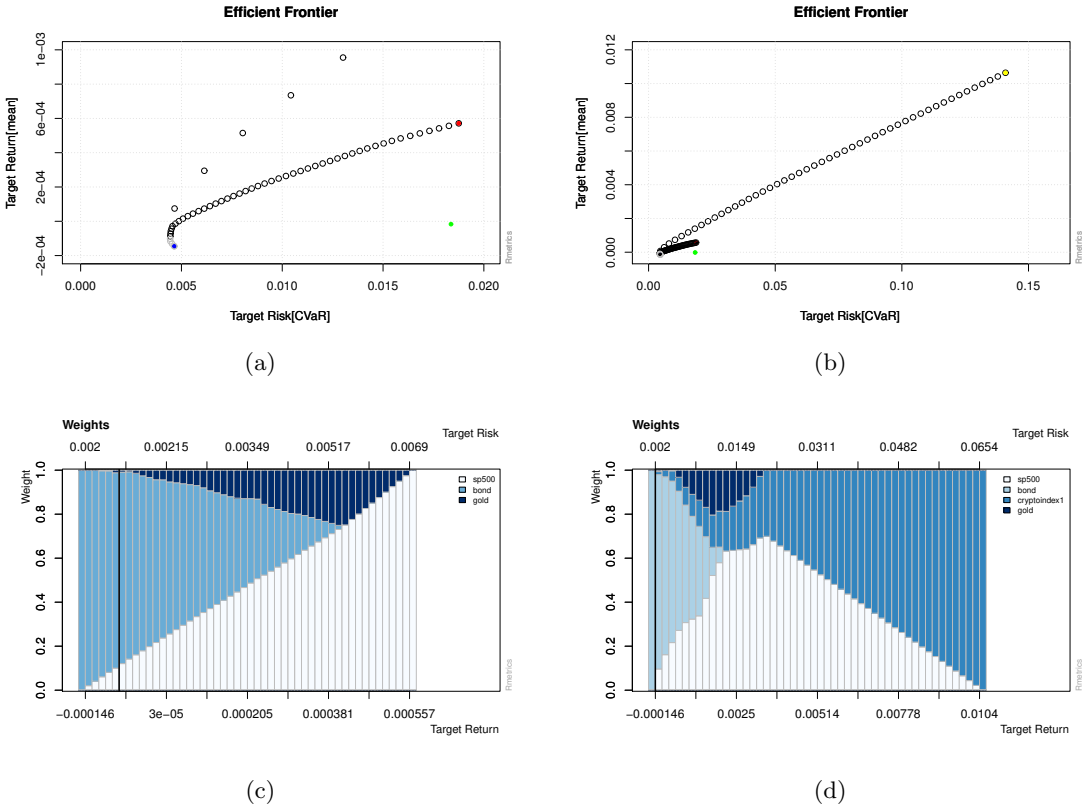
(c) (d)

Figure 7: Plots of portfolio 1: (a) shows the efficient frontier with an without the cryptoindex(blue = bonds, red = S&P500); (b) depicts (a) zoomed out(yellow = cryptoindex); (c) shows efficient portfolio weights; and, (d) shows efficient portfolio weights with cryptocurrencies added to the portfolio.

weighting in each efficient portfolio with positive expected return.
The addition of real estate to the investable assets sets does not improve the portfolio structure as real estate, as bonds and gold, has negative expected returns and relative high risk. From the weights graph 10(c) and (d) it is seen that it does not provide sufficient diversification to the portfolio structure to compensate for the negative expected return. Therefore no efficient portfolios with positive expected returns include real estate.
If Euros are added to the portfolio gold is removed from every efficient portfolio as seen in 11(c) and (d). The effect of including the cryptoindex, however, still shows a positive impact on the portfolio structure for every portfolio with positive expected return even with all of the traditional asset classes represented in the set of available assets.

4.6 Concluding remarks

The thought that the group of cryptocurrencies have the necessary attributes to be considered their own asset class have been supported of the findings in this chapter. The group has it own politico-economic profile and when trading volume is used as a measure of liquidity the group shows promising results that makes it possible for investors to enter and adjust positions. Furthermore the analysis of correlation between the cryptocurrencies and traditional assets shows that the returns of the cryptocurrencies are independent of



(a) (b)

(c) (d)

Figure 8: Plots of portfolio 2: (a) shows the efficient frontier with an without the cryptoindex(blue = bonds, red = S&P500, green = gold); (b) depicts (a) zoomed out(yellow = cryptoindex); (c) shows efficient portfolio weights; and, (d) shows efficient portfolio weights with cryptocurrencies added to the portfolio.

the returns of traditional asset according to this measure, thereby indicating that the addition of cryptocurrencies to portfolio might increase diversification and thereby risk. The analysis of optimal portfolio construction for long term investors based on the performance of the considered assets over the last 20 months shows that adding cryptocurrencies to portfolio increase expected returns for given risk targets even for inclusion of very small proportions of cryptocurrency. The group of cryptocurrencies should therefore attract attention from the risk-averse investor. Close intention, however, should be payed to the development of the market of cryptocurrencies, which is still in the early stages and considerable changes of significant market features might very well changes in the nearby feature, thereby altering the findings in this chapter.

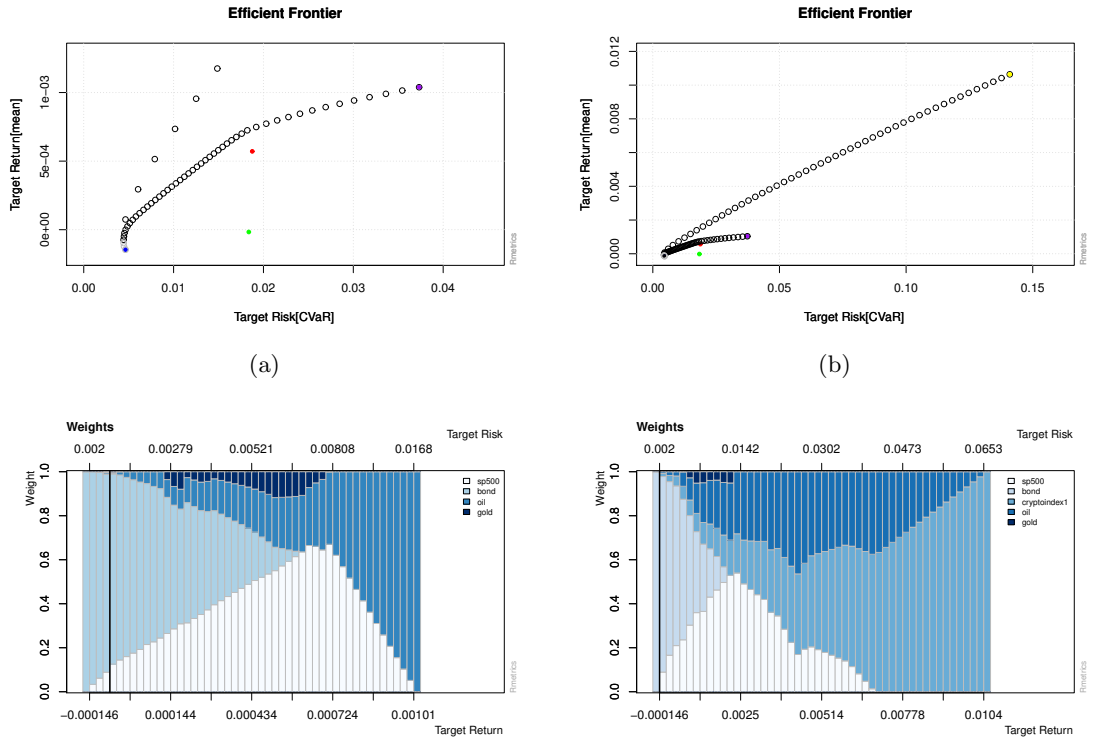
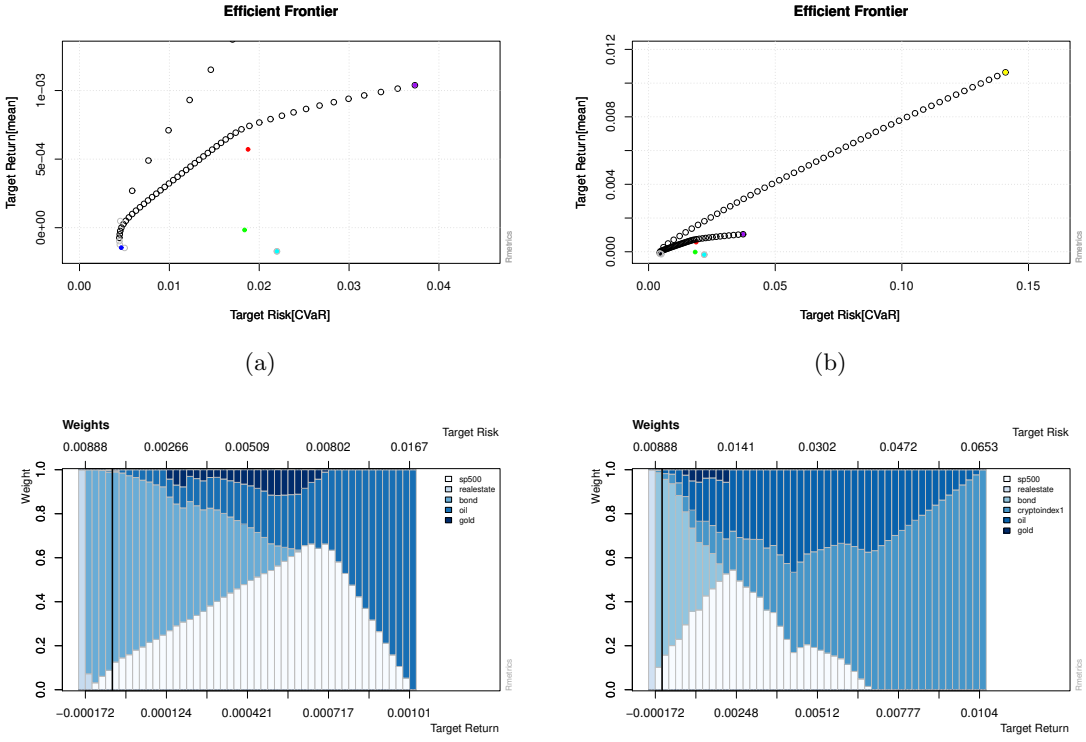


Figure 9: Plots of portfolio 3: (a) shows the efficient frontier with an without the cryptoindex(blue = bonds, red = S&P500, green = gold, purple = oil); (b) depicts (a) zoomed out(yellow = cryptoindex); (c) shows efficient portfolio weights; and, (d) shows efficient portfolio weights with cryptocurrencies added to the portfolio.



(a) (b)

(c) (d)

Figure 10: Plots of portfolio 4: (a) shows the efficient frontier with an without the cryptoindex(blue = bonds, red = S&P500, green = gold, purple = oil, cyan = real estate); (b) depicts (a) zoomed out(yellow = cryptoindex); (c) shows efficient portfolio weights; and, (d) shows efficient portfolio weights with cryptocurrencies added to the portfolio.

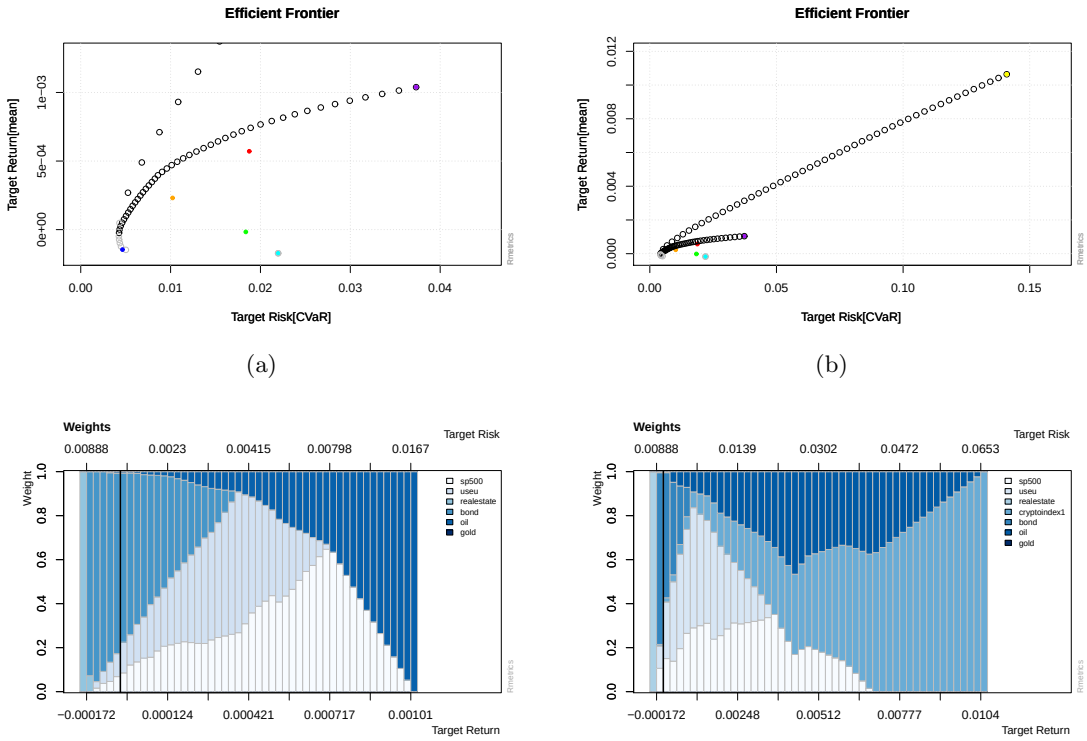


Figure 11: Plots of portfolio 5: (a) shows the efficient frontier with an without the cryptoindex(blue = bonds, red = S&P500, green = gold, purple = oil, cyan = real estate, orange = Euro); (b) depicts (a) zoomed out(yellow = cryptoindex); (c) shows efficient portfolio weights; and, (d) shows efficient portfolio weights with cryptocurrencies added to the portfolio.

5 Hayek Money - Price Stability

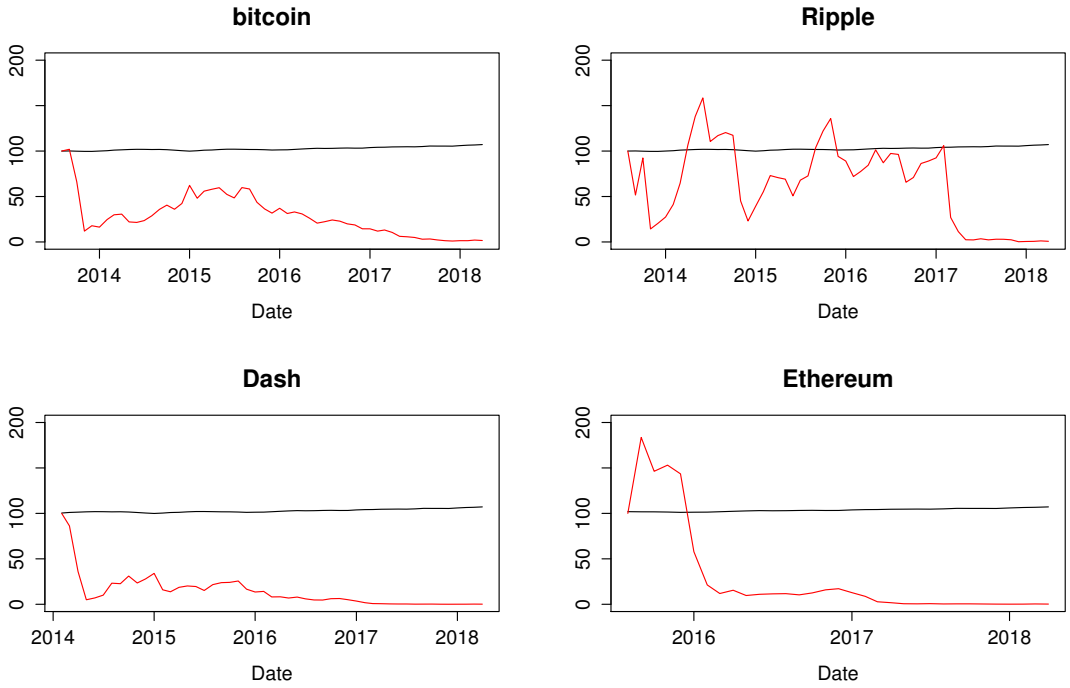
So far, this project has wandered between the zones on whether cryptocurrencies can be defined as a real currency or a speculative asset. Clearly, it is not yet to be defined as a currency. It is not fulfilling the three properties of money with the main issue being its price stability. This section will try to attack this issue with some help from Ametrano (2014) and Hayek (1990). Ametrano sought inspiration in Hayek's *Denationalisation of Money*, where Hayek argues for the destruction of the governments monopoly over creation of fiat money. The main reason being to avoid price instability which fits perfectly in the current situation with cryptocurrencies. In Hayek's perspective he argued for the banks to be the private issuers of the currencies in the market and due to market mechanisms the only currencies that would survive would be those that could deliver a currency that had stable price. However, it is definitely not the banks issuing the current stream of cryptocurrencies, on the contrary it is mostly private firms, but the first banks have begun the preparations for launching a cryptocurrency[32,33]. Furthermore there has been a lot of talk of some Japanese banks working together, in order to issue their own coin[34,35,36].
We have established that the biggest problem for cryptocurrencies is the price stability. Figure 12 shows the American CPI held up against respectively Ripple, bitcoin, Dash and Ethereum. They all share the attribute of having a finite supply of coins. Ametrano says in his paper, basic economics can explain the drastic increases in the cryptocurrencies. You have a supply, which after the initial period is basically constant and a rising demand. A rising demand for something with a constant supply calls for a price increase. The biggest problem for the consumer with this cryptocurrency is that they cannot know what their money is worth in one week. When bitcoin was experiencing the massive price increase, sure it would have been perfect getting paid in bitcoin. But when it is the other was around and the price of bitcoin is falling, you suddenly have lesser purchasing power than before. A currency with that kind of price volatility is impossible to implement, as the consumers would be in a constant state of choosing between using your money now or wait till tomorrow where we could see either a price rise or fall.

Advantages of government money supply

Before we are sold on the idea of private issuers of money, let us take a look at how the government's monopoly of money benefit the consumer. Hayek says the following:

[32] https://cryptoslate.com/bank-of-tokyo-mitsubishi-testing-prepares-to-launch-first-bank-issued-crypto/
[33] https://www.ccn.com/bank-of-korea-hints-at-issuing-a-central-bank-digital-currency/
[34] https://bitcoinexchangeguide.com/j-coin-ico/
[35] https://www.cnbc.com/2017/09/27/japanese-banks-cryptocurrency-j-coin.html
[36] http://nordic.businessinsider.com/japan-plans-new-digital-currency-j-coin-2017-9?r=US&IR=T

Figure 12: CPI in dollars held against an indexation of respectively CPI/Ripple, CPI/bitcoin, CPI/Dash and CPI/Ethereum in dollars

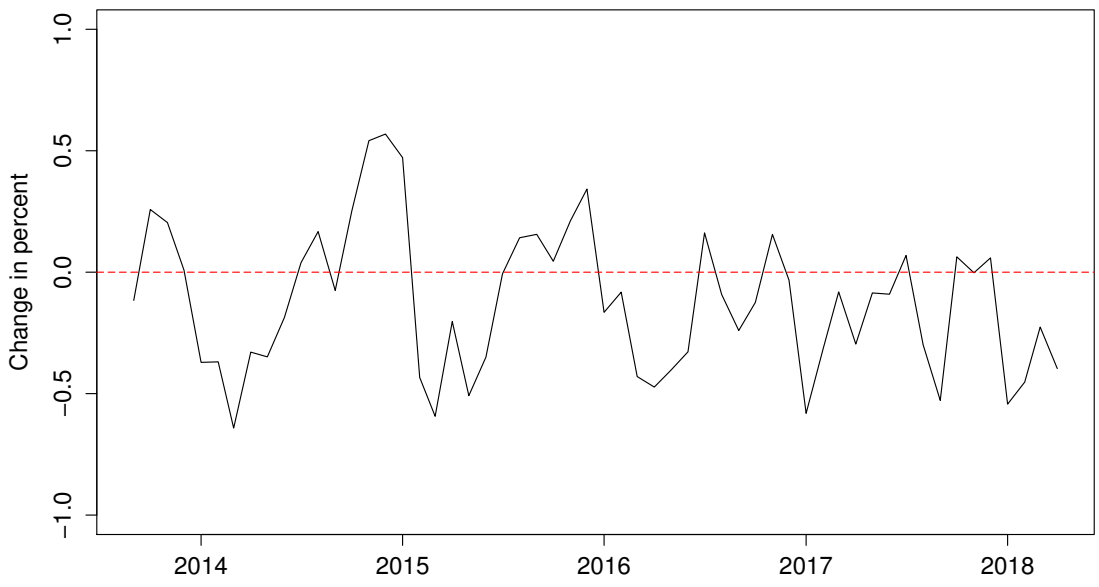


> *Perhaps when the money economy was only slowly spreading into the remoter regions, and one of the main problems was to teach large numbers the art of calculating in money (and that was not so very long ago), a single easily recognisable kind of money may have been of considerable assistance. And it may be argued that the exclusive use of such a single uniform sort of money greatly assisted comparison of prices and there- fore the growth of competition and the market* (Hayek, 1990).

It can be argued that the public still prefer a single currency to make their daily transactions. Since Hayek's time we have fortunately invented something called the smart-phone which can tell you what your currency is worth in whatever currency you wish to know in a matter of second. So, even though the public still prefer one single currency, the option for implementing other currencies, whilst maybe keeping the recognisable currency as the one the prices is shown. So, the advantage of having one currency issued by a government is still there, but this advantage can easily be replicated due to technology so that the consumers still only considers one currency.
The other advantage is of course the governments ability to secure stable prices, which opens a world of possibilities for consumers and other economic agents. It opens up to economic calculations, budgeting, planning for the future etc. etc. Imagine that you had seen a hell of a smart car just for you. This car cost \$40,000 with all the extra equipment. You currently have \$20,000 in your bank account, whilst having a monthly income of \$3,000 after all necessary expenses. So, if you do not want to loan money in order to buy the car, you know that you have to save up money for seven months. $(7 \times 3,000 = 21,000 + 20,000$ in savings $= \$41,000)$ With a max inflation of 2 percent, the car can cost \$40,800. So, you

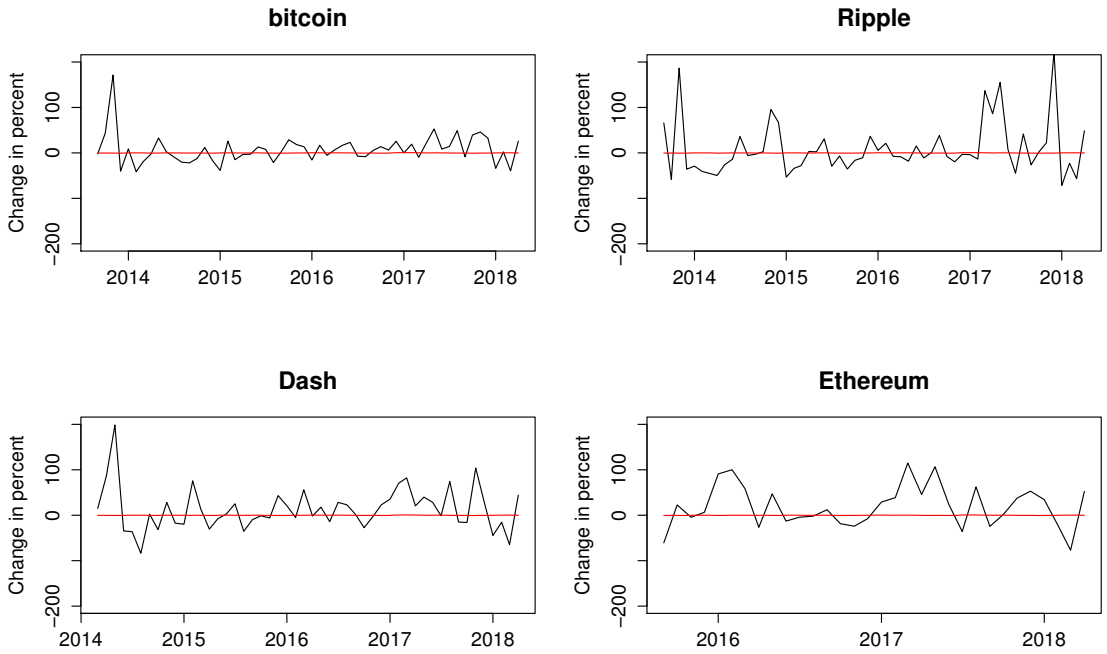
know that everything else alike you would be able to buy the car after seven months. This is one of the goodies of stable prices.
Now, let us imagine a scenario like this with unstable prices. You have still found your dream car for the same price as before, and you gotta have it. After five months you have $35,000 dollars in your savings, and you are now close to being able to buy the car. Let us assume that there is five different currencies in your country and you would prefer to use C1, because that is the custom in your region. However, a news channel brought a disastrous news on your currency, C1, whilst C3 are being praised for its new action which could be literally anything. Before you can do anything, the price of your currency has depreciated, which means that the car you had been looking for suddenly cost $55,000. Then, after five months of saving up you are looking at saving up again for another six months. The point being that it is impossible to make economic calculations with the price being that unstable. On figure 13 you can see the volatility of the American consumer price index since 2013. It should be quite clear to see that the prices are not moving that much. The biggest monthly change in the CPI is about 0.5 percent, which corresponds to the car getting $200 dollars more expensive, and that is only if the salesman changes his price that fast — which is highly unlikely. Instead we take a look at figure 14, where you can see the crazy volatility that these currencies are experiencing. The red line in the middle which seems pretty horizontal to both you and me is the volatility from figure 13 which pretty much says it all. Through the money supply control the government is able to secure these stable prices, in order for you to be able to plan ahead.

Figure 13: The volatility of the American consumer price index since late 2013



So, the government's monopoly of money printing makes sense, especially with their ability to secure price stability. However, having one currency for the sake of convenience is a bit of a stretch, so if there was a way to secure price stability without government control, we could look at a much more different situation. The next section will contain Ametrano's

Figure 14: Volatility of four cryptocurrencies



suggestion for handling price stability.

5.1 Rebasing

Ametrano argues for the introduction of a designed cryptocurrency:

> *At this point the line of reasoning should hopefully be self-evident: in order to target purchasing power stability, a cryptocurrency should be designed with outstanding amount elastically rebased in a fully automatic algorithmic non-discretionary way. A cryptocurrency adopting such an elastic supply is defined here as Hayek Money* (Ametrano, 2014).

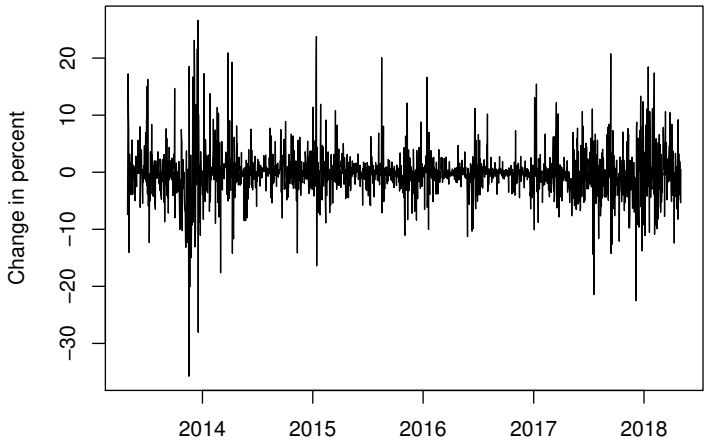
So, what Ametrano is arguing for is the birth of a new cryptocurrency with some distinct attributes. For the sake of the overview it is put up in bullet form:

- An elastic supply
- Algorithmic
- Non-discretionary

What Ametrano is suggesting is a whole new way to handle the money supply. Instead of the government controlling the money supply a fully automatic algorithm will decide when to shrink or increase the money supply. And instead of the classical way, where some agents on the market benefits from the money supply increase before others as per section 3, the money will now be evenly distributed in everyone's wallet — that is called a non-discretionary distribution of money. This method secures a constant purchasing

power through the rebasing. In Ametranos example, he uses a simplified way to explain the mechanics, which we will try to as well. Imaging that the CPI is made up by one dollar. In 2013 Frank would be able to buy 1 USD for 1 BTC. In december 2018 the price of 1 BTC is \$20,000. That means that Frank would be able to buy 1 USD for $\frac{1}{20{,}000}$ BTC. In this scenario Frank's wealth is 20,000-doubled. Ametranos suggestion rebases the money supply. Instead of letting it being fixed, the contents of Frank's wallet will be adjusted by the same amount of the change in the CPI (which is 1 USD). After rebasing his wallet would have the sum of 20,000 BTC worth \$20,000. In this way, his wealth and purchasing power remains the same. Rebasing does not change the value, but are merely adjusting in regard to the demand for the bitcoin relative to the dollar. In figure 15 the daily percentage change of the supply of RBTC is shown and thereby the percentage change of coins in everyones wallets. From the figure it can be seen that if this monetary policy had been implemented in the bitcoin protocol considerable changes to the amount of coins in each users wallet would happen regularly. These big changes would of course be confusing for the consumer, but really it is just another way of thinking of appreciation and depreciation when the wallet content rises and decreases respectively, so it is just a matter of habituation. The next section will take a quick glance at how a commodity price

Figure 15: USD/RBTC



index can be set up.

A Commodity Price Index

So far, the rebased cryptocurrency are being rebased against the consumer price index which currently consists of one dollar. This fixed exchange rate system, which have and are still being used in the world economy eg. in the Euro area, where some countries which held on to their own currencies have pegged this to the Euro. This fixed system brings along some advantages and disadvantages in some economists eyes. When the cryptocurrency is bound to the dollar, the inflational and deflational tendencies will follow that of the dollar i.e. the Fed is still able to run with monetary policies. The benefits of

this being that the Fed has done a decent job in the past of keeping price stability. Taking a look back at the monetary theories from section 3, one of the problems with having the government controlling the money supply, was the fact of uneven distribution of money when the supply was adjusted. In the rebasing perspective, the Fed and the government are still keeping their ability to regulate the economy through their control of the money supply, whilst getting rid of the uneven distribution of the money which leads to shifts in wealth of different society classes. One of the disadvantages with this peg from an Austrian perspective definitely still being the fact that the fiat money commodity has no intrinsic value. With the new cryptocurrency being pegged to dollar the benefits of price stability vanishes with the threat of a massive depreciation should another more demanded cryptocurrency be introduced.
This leads to the creation (or recreation) of a commodity price index, p1, consisting of gold and oil weighted equally. Figure 16 shows the price of the price index in both USD and BTC as well as the prices of gold and oil. If the monetary policy was to keep the price of this basket of goods constant to for example 600 RBTC, rebasing after this target would achieve a perfectly stable price of the basket as can be seen in Figure 17. It can also be seen that the prices of oil and gold are not perfectly stable but float freely as all other the goods will as well, the monetary policy only achieves perfectly stable prices for the basket, which hopefully leads to relative stable prices for other goods. This setup for monetary policy is possible for any type of basket and the one considered here could certainly be improved by including more commodities in the basket.

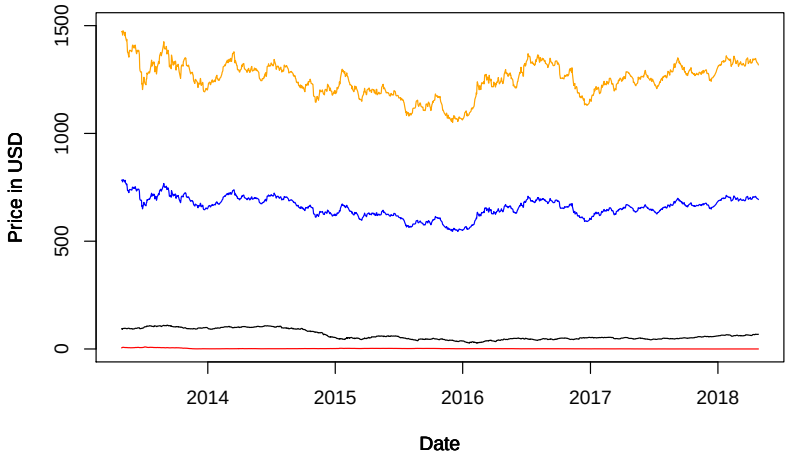


Figure 16: The price in USD of gold (orange), oil (black) and the commodity basket b1 consisting of 50 percent gold and 50 percent oil (blue) and the price of b1 in btc (red).

To evaluate the volatility of the RBTC that targets price stability for p1, the exchange rates of USD/RBTC and USD/EUR are plottet together in Figure 18. From the Figure it can be seen that the volatility of RBTC is not remarkable different from the Euro and RBTC could therefore be considered a currency.

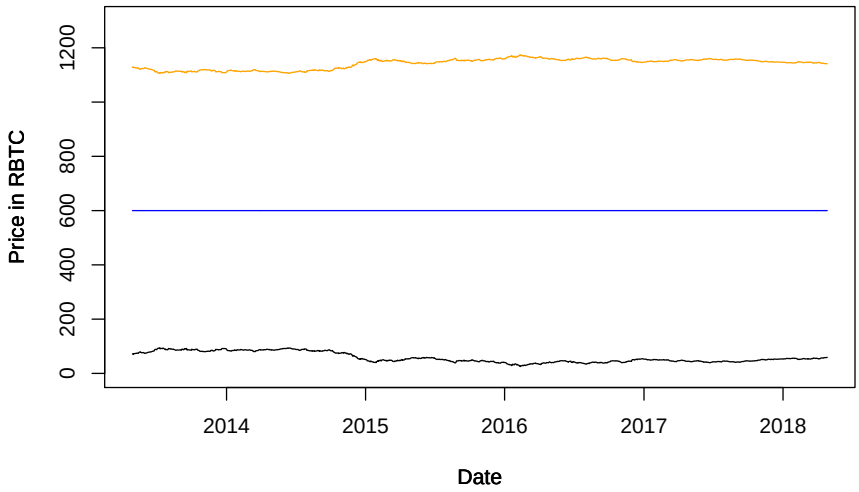


Figure 17: The price in RBTC of gold (orange), oil (black) and the commodity basket b1 consisting of 50 percent gold and 50 percent oil (blue).

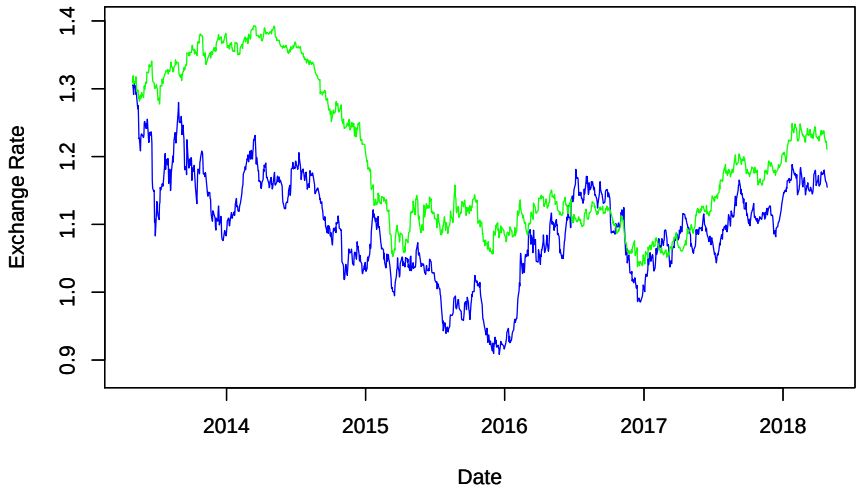


Figure 18: The exchange rates USD/EUR (green) and USD/RBTC (blue).

Introducing Tether

After this examination of a possible way to create a more stable cryptocurrency, we will take a look at another cryptocurrency called tether, which can remind a lot of the previous sections proposal. Tether is a cryptocurrency that works on the Omni Protocol which interacts with blockchain in order to issue their tokens. The reason that tether is closely linked to this section is that it has an exchange-rate of 1 to 1 with the US Dollar, which are being kept constant in order to secure price stability. This means that the purchasing power will follow that of the dollar. The users of this token can rely on this cryptocurrency

like they would with the dollar in regard to its function as a unit of account and store of value (Tether, 2016).
The way they keep it constant is quite simple. The supply of these tokens is elastic, so when I, as a user decide to buy tethers, the company automatically issues the corresponding tether to my dollar deposit. They keep this in check by a simple "Solvency Equation" which is $TUSD = DUSD$, where TUSD is the total supply of the tether token and DUSD is the daily bank account balance. This means that all circulating Tethers is 100 percent backed by fiat currencies according to the company behind (Tether, 2016). However, some people have begun to worry about whether or not it is actually 100 percent backed[37]. The reason this token is exciting, is because of its approach as simply a dollar token, but build on a blockchain. This way you get all the benefits of the blockchain technology and you simultaneously keep the benefits of the fiat currency and its price stability.

[37] https://arstechnica.com/tech-policy/2018/02/tether-says-its-cryptocurrency-is-worth-2-billion-but-its-

6 An implementation of cryptocurrencies

This chapter will mainly contain an examination of the theoretical effects on the consumers if an implementation of cryptocurrencies were to happen but also a section containing the critical juncture framework. Trace Mayer, one of the first "fans" of bitcoin and Blockchain has a very positive view towards cryptocurrencies:

> *Instant transactions, no waiting for checks to clear, no chargebacks (merchants will like this), no account freezes (look out Paypal), no international wire transfer fee, no fees of any kind, no minimum balance, no maximum balance, worldwide access, always open, no waiting for business hours to make transactions, no waiting for an account to be approved before transacting, open an account in a few seconds, as easy as email, no bank account needed, extremely poor people can use it, extremely wealthy people can use it, no printing press, no hyper-inflation, no debt limit votes, no bank bailouts, completely voluntary. This sounds like the best payment system in the world!*[38]

Not everyone is as optimistic as Trace, but several well-known people have expressed their opinion on the current wave of new information on cryptocurrency. IMF's CEO Christina Lagarde mentions the obvious problem in the cryptocurrencies state which are the volatility, but also the intensive need for energy and that the technology is not yet scalable but says that:

> *(...) these are technological challenges that could be addressed over time. Not so long ago, some experts argued that personal computers would never be adopted, and that tablets would only be used as expensive coffee trays. So I think it may not be wise to dismiss virtual currencies* (Lagarde, 2017).

She also mentions that it makes sense that *"countries with weak institutions and unstable national currencies"* adopts a virtual currency instead of that currency of another country (Lagarde, 2017). In the same context, Bill Gates sees a possibility that this digital currency can help people who lives in poverty[39], and has helped Ripple and other companies in their start up of Mojaloop, which is a software that helps connect digital, financial services[40,41]

[38] `https://bitcoinchaser.com/fun/best-bitcoin-quotes`

[39] `https://www.youtube.com/watch?v=4Xb8CKc7qOo`

[40] `http://mojaloop.io/`

[41] They optimize in the following ways:

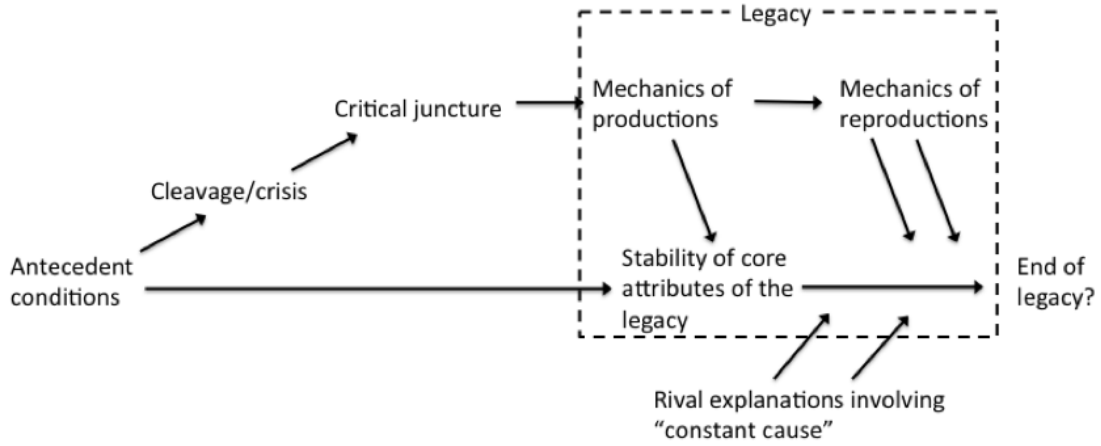
1. **Interoperability:** Connects different payment options
2. **Directory service:** Making sure the money ends up in the right places
3. **Transaction settlement:** Making sure that all transactions are being recorded on ledgers.

To start the chapter off, we will quickly take a look at the critical juncture-framework once again, in order to try and identify the cleavage/crisis point.

6.1 Defining the financial crisis in the critical juncture framework

The financial crisis in '08 came to many as a shock while some people claims to have predicted it. The one thing that we can say for a fact is the aftershocks of this crisis. A huge focus was turned at the financial sector where the new talking point between economists and politicians were how to regulate the financial sector better, thus hoping to brace this particular sector for another crisis. An example is Basel lll[42], which aimed to increase supervision of banks whilst strengthening the banks liquidity. These institutional changes came because of this crisis, and would not had happened if not because of the crisis. The need for these regulation was a direct effect of the crisis, but the perspective of cryptocurrencies is anothers discussion. Taking a look at figure 19, we see the first block

Figure 19: Building block of the Critical Juncture framework (Collier and Collier, 2002, pp. 30)



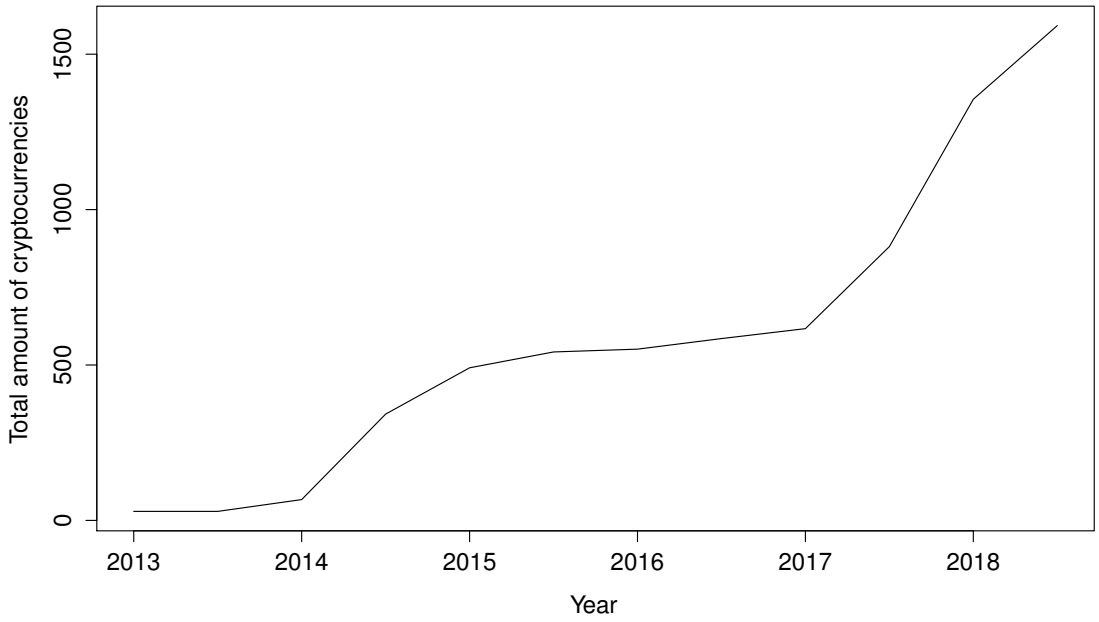
which is antecedent condition which describes how the scenario of the economy/institution dependent on which context, was before the critical juncture. This makes it possible to evaluate how the critical juncture affected the institutions. Our base scenario is an economy without blockchain technology and with a very small fraction of digital currencies. Attempts have been made to invent a cryptocurrency, but no one succeeded. Some web-based money gained traction, such as PayPal which perhaps is the most well-known "web-currency". From this block we have two arrows — one going to the cleavage/crisis which initially was thought to be the financial crisis. The important part here is to distinguish between cleavage and crisis. A crisis is swift and immediate and requires actions like the financial austerity after the financial crisis. On the other hand, a cleavage can last much longer and affects the political landscape in another way. As we saw in an earlier section, different countries are tackling cryptocurrencies in very different ways which is another talking point in this framework (Collier and Collier, 2002). Collier says:

[42]https://www.bis.org/bcbs/basel3.htm

> *First, the cleavage may be important because the activation or exacerbation of the cleavage creates new actors or groups and the critical juncture consists of their emergence. An example would be the emergence of the urban class and the organization of labor unions within the working class* (Collier and Collier, 2002, pp. 33).

In this case, there is a probability that the cleavage was not the financial crisis, but rather the moment began when Satoshi published his paper in October 2008. This paved the way for new actors on the market and given that Satoshi made all his work public, everyone had the same conditions. In this way it can be argued that the antecedent conditions was indeed an economy without blockchain technology and Bitcoin protocol. It can be argued the financial crisis is a part of this antecedent conditions, and that the crisis helped boost the interest for blockchain technology and Bitcoin. However, it has not been a constant growth in cryptocurrencies we have seen. If we take a look at figure 20, the development in the total amount of cryptocurrencies have taken some remarkable jumps, especially in the first part of 2014 and since the beginning 2017. That brings us to the next point, which are

Figure 20: The development of cryptocurrencies



how long critical junctures last. As we saw with the financial regulations imposed on banks after the financial crisis, this was a short juncture. But as Colliers mention, the length of a critical juncture is not defined. It can take whatever range it wants, and Colliers argues that a period of 23 years was the length of a juncture in Latin America (Collier and Collier, 2002). That should mean that the period of ”incorporation” of cryptocurrencies can take as long as necessary. This also connects with the way that nations react to the cryptocurrency introduction. As Collier says:

> *If the critical juncture is an immediate response to an external shock — such as the depression of the 1930s, the debt crisis of the 1980s, an international*

> *wave of social protest, or a war — it may occur more or less simultaneously across a number of countries(...)*(Collier and Collier, 2002, pp. 31)

... or the financial crisis in 2008. This categorizes as an immediate response from a lot of countries but on the other side we have the introduction of the Bitcoin protocol, which did not force the political authorities to react in the same manner, but is rather gaining more and more traction which can be seen on figure 20. This however means that we have yet to see the critical juncture. If we are still in a phase of cleavage, the juncture needs to happen in order for the economy to change and for the institution to embrace it. But it can indeed be argued that in order for the implementation of cryptocurrency to happen, some kind of a critical juncture is needed. In the next section we will make some concluding remarks about our portfolio analysis and how the investors can benefit from this. After that we will examine some of the theoretical effects an implementation can have on the consumers.

6.2 Effects on the consumer post implementation

This section will contain some attributes of money which can be argued to change if cryptocurrency were to be implemented. The first attribute being the transactions costs.

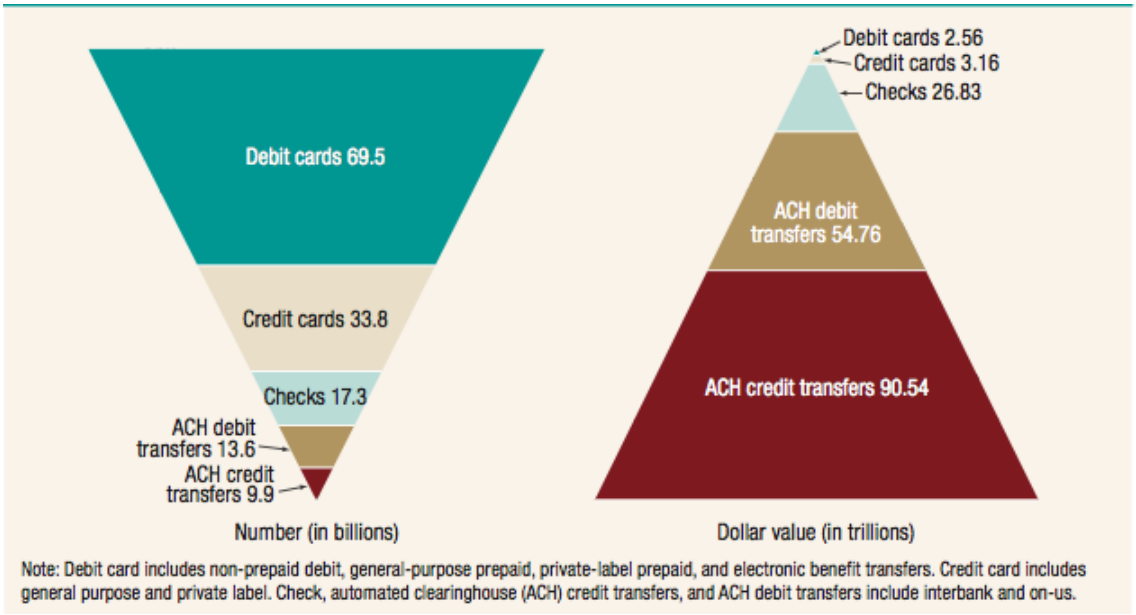
Transaction costs

What does the transaction time really mean for the consumer? As of today, I can pay with my VISA in under two seconds in almost every occasion and if it is physical, even faster with paper money. So what can for example Dash's transaction time do for me and you as a consumer? Well, nothing particular. The reason why cryptocurrencies are competing to have the fastest transaction time, is because it is one of the factors that can be adjusted. The one thing they all have in common is their transaction security. Instead of having to put in billing address etc. you simply need the public key of the person you are sending money to and input your private key. This all else equals lower the rising credit fraud which will be discussed in next section. The next attribute is the fact that there is no third party involved in money transfers. Instead of you paying a percentage to the bank, you can pay a fee in either bitcoin, Ether, Ripple or Dash at respectively $1.08, $0.606, $0.0015 or $0.116[43]. Bitcoin has not however been the best example of low transaction cost because of the extreme price increase together with a very low transaction volume which only made the fees higher. This also meant that in order to get your transaction through relatively fast you had to pay high fees to the miners. The peak transaction fee was about $35, but it has fallen again to the above-mentioned. Karl Kreder has investigated into the real costs of money transactions, and we would like to take a look at some of his findings (Kreder, 2017). He notices that from all the money spent in 2015, $2.35 trillion of these were cash and $178 trillion were checks, credit/debit cards and ACH transfers[44]. That means that cash use only corresponds to about 1.3 percent of the total. These non-cash transaction's distribution is showed in figure 21.

[43] `https://bitinfocharts.com/`

[44] ACH transfer is another form of wire transfer handled by another middleman than the bank. It has lower costs but takes on the other side 2-3 days to process

Figure 21: Distribution of core noncash payments by type, number, and value, 2015(System, 2016, pp. 3)



Card payments are by far the most used but does on the other side not cover a big share of the total dollar amount. Kreder tries to find the true transaction cost for different kinds of payment option and through an explanation how there is actually five parties involved in a standard credit card payment; the buyer → issuer of buyers credit card → switch[45] → The merchants bank → The merchant. He finds that there is a fee on \$0.25 + 2-3 percent. He examines all other non-cash transactions and comes up with a table that shows the costs for each payment method. For convenience, a table with his numbers have been made to show the reader, together with the costs of the four above-mentioned cryptocurrencies (Kreder, 2017). See table 8.

Table 8: Time and costs for different non-cash payment methods

Method	Time	Cost
Checks	3-7 days	$\$15 - 20$
Credit/Debit Card	2-3 days	$\$0.25 + 2\%$
ACH	2-3 days	\$1.96
Wire transfer	1-5 days	$\$35 - 75$
bitcoin	60 minutes	1.08
Ripple	4 seconds	\$0.0015
Ethereum	12,5 minutes	\$0.606
Dash	15 minutes	\$0.116

With cryptos, you have to wait an amount on time for block confirmation. For bitcoin it is 6 block, ethereum about 50 and dash 6 blocks. So the numbers here are multiplied from number of blocks and how long it takes for one block to be created. Ripple is more unclear, but it seems that the confirmation time is indeed 4 seconds[46]

Obviously cash is faster than all of these with almost zero transactions cost. The only cost of holding cash is inflation, but as we saw only 1.3 percent of all money being used is cash. Already without an implementation of cryptocurrency, the society is moving to a

[45] Handles the transfer from one bank to another

digital world where less and less people are holding cash and more people are using credit/debit cards or mobile payment method such as the danish Mobile-pay (Nationalbanken, 2017). As it is now, people have started using digital payment options, so why not make it cheaper by cutting out all the third parties?

Credit card fraud

Credit card fraud has been on the rise in the recent years[47,48,49], with especially the term "Card-not-present" being in focus. Card-not-present fraud occurs when it is possible for a criminal to obtain a cardholder's name, billing address, account number, security code and card expiration date. In order to do this with blockchain, you need the wallet-holders private key.
Achieving some other persons private key makes it possible to use all of this person's keys without him/her knowing. Like with card-not-present fraud, the hacker does not need anything physical from the person he is stealing from which is one of the reason it is hard to protect yourself against (Narayanan et al., 2016, ch. 4). A lot of the 'normal' consumers do not have the proper tools to protect themselves against a solid hack, but there is however a couple of ways to avoid it. Some of these ways are cold storage or a paper wallet. A cold storage is an offline wallet that is impossible to access without the physical device but it is however possible to send coins to this cold storage. This leaves an opportunity to transfer coins to the cold storage if you feel that you currently have to to much money in you 'hot' wallet. This kinda works like a wallet and a bank box with one exception being the possibility to transfer coins to the bank box while not being present (Narayanan et al., 2016, ch. 4).
Another way of protecting your wallet is with a paper wallet that includes printing a paper wallet where it is possible to include the important key contents in order to access your wallet. The typical way to do it, as Arvind says:

> *Typical paper wallets encode both the public and private keys in two ways: as a two-dimensional barcode and in base-58 notation* (Narayanan et al., 2016, ch. 4, pp. 125).

Unfairness

As we saw in Chapter 3, Mises and Rothbard have a strong opinion on the money supply and the way that it can affect the economy in different ways. Adjustments to the money supply causes a redistribution of money that is unfair. The reason for this being that the money is not available to all agents at the same time which means that those who receives the money latest does not benefit from the the increase of money. Furhtermore, due to their scale of value prices do not rise uniformly, which not necessarily is a bad thing.
But if we take starting point in the rebasing theory put forward in the previous chapter and the way that tether issues their tokens together with Lagarde's "proposal",

> *For instance, they could be issued one-for-one for dollars, or a stable basket of currencies. Issuance could be fully transparent, governed by a credible, pre-*

[47] http://nyheder.tv2.dk/krimi/2017-09-02-misbrug-af-dankort-er-tredoblet-pa-seks-ar
[48] https://www.statista.com/statistics/419628/payment-card-fraud-losses-usa-by-type/
[49] https://www.uspaymentsforum.org/wp-content/uploads/2017/03/CNP-Fraud-Around-the-World-WP-FINAL-Mar-2017.pdf

> *defined rule, an algorithm that can be monitored... or even a "smart rule" that might reflect changing macroeconomic circumstances* (Lagarde, 2017).

there is a way to enforce the so called Angel Gabriel model, mentioned in the Austrian theory in chapter 3, so that all people have their wealth adjusted evenly. Keeping the Austrian theory in mind, this must be a improvement from the current state. Furthermore, Rothbard do not see a constant money supply being a problem, which if a cryptocurrency like bitcoin, ripple or dash were to get implemented would be a fact. The bigger problem being that Austrians still do not put a lot of value into commodities that has no intrinsic value.

A collective evaluation

The previous sections have discussed how an implementation of cryptocurrency will benefit the consumer in different ways. To get a clear picture, a table has been put forth which ranks respectively gold, fiat money and cryptocurrencies after their ability to function as money on different levels.

	Gold	Fiat Money	Cryptocurrencies
Medium of exchange	● ●	● ● ●	● ● ● ○
Store of Value	● ● ● ●	● ● ●	● ● ● ● ○
Unit of Account	● ● ●	● ● ● ●	● ● ○ ○ ○
Transaction cost	●	● ● ●	● ● ● ●
Fraud-protection	● ● ● ●	● ●	● ● ●
Monetary fairness	N/A	●	● ● ●

Some concluding remarks about the above-mentioned table should be that the white circles represents how it would be ranked if it were to get implemented. This is only important for the three basic attributes money should have. The three white circles at unit of account can be achieved through a price stability progress, and the reason it is three circles is because of the big challenge it is and the present volatility cryptocurrencies show. The other three attributes would not change because of an implementation, which is why there is not any white circles her.

7 Conclusion

This project has evolved around cryptocurrency and how the society might benefit from it — both at the current moment but also if it were to get implemented. Through the development of what money is as well as what attributes it should have, it was concluded that at its current form, cryptocurrency cannot be defined as a money commodity, even though it calls itself a currency. An asset investigation involving not every but a lot of the different assets the economy can currently offer helped to understand what we are dealing with. Cryptocurrency behaves like a highly speculative asset with the possibility of huge returns while also being very risky. On top of that the data showed only small signs of dependency between the development in cryptocurrency and the traditional assets. Therefore, it can be concluded that cryptocurrency predominantly is independent from the entrained assets in this project.
A portfolio analysis confirmed the extreme volatility of cryptocurrencies where it is shown that including cryptocurrencies in your portfolio makes it riskier but also raises the returns. This is consistent with the previous observations of it is highly volatile nature. It is obviously an observation that is incredibly fluctuating and has to potential to vary relatively much under the right circumstances. This is however hard to speculate in, which is why the conclusion is not definite.
Last but not least a discussion of the conditions that need to be present in order for an implementation to happen in the critical juncture took place. In this section it was argued that we might as well be an a cleavage period, where the underlying structures of the economy is able to change. Given that the critical juncture framework is but a theory, it is not possible to conclude that it is indeed what needs to happen, but it can be argued from learned history that a critical juncture might be the drop that causes the cup to flow over. How the consumers can benefit from this was briefly looked at and according to our project and the inspiration that was found in different litterature, it is concluded that an implementation of cryptocurrency should benefit the consumers to a certain degree. How and how much they benefit will certainly depend on how the cryptocurrency is implemented and to what degree the government *lets go* of its current monopoly.

Bibliography

Ferdinando M. Ametrano. Hayek money: the cryptocurrency price stability solution. 2014.

Philip Arestis and Alfred S. Eichner. The post-keynesian and institutionalists theory of money and credit. *Journal of Economic Issues, Vol. 22, No. 4*, 1988.

Ole Eiler Barndorff-Nielsen and PO. Halgreen. Infinite divisibility of the hyperbolic and generalized inverse gaussian distributions. *Zeitschrift fÃijr Wahrscheinlichkeitstheorie und verwandte Gebiete 38*, 1997.

Chris Burniske and Adam White. Bitcoin: Ringing the bell for a new asset class. 2017.

Eng-Tuck Cheah and John Fry. Speculative bubbles in bitcoin markets? an empirical investigation into the fundamental value of bitcoin. *Economic Letters*, 2015.

David L. K. Chuen et al. *Handbook of Digital Currency*. Elsevier Inc., first edition, 2015.

Ruth Berins Collier and David Collier. *Shaping The Political Arena*. University of Notre Dame Press, second edition, 2002.

Robert J. Greer. What is an asset class, anyway? *The Journal of Portfolio Management*, 1997.

Frederich A. Hayek. *Denationalisation of Money - The Argument Refined*. The Institute of Economic Affairs, third edition, 1990.

Karl Kreder. Money vs. cryptocurrency, the real costs. 2017.

Christina Lagarde. Central banking and fintech - a brave new world? *Speech at Bank of England Conference*, 2017.

Damien Lamberton and Bernard Lapeyre. *Introduction to Stochastic Claculus Applied to Finance*. Chapman & Hall/CRC, second edition, 2008.

Yoram Lustig. *The Investment Assets Handbook: A definitive practical guide to asset classes*. Harriman, 2014.

Harry Markowitz. Portfolio selection. *Journal of Finance*, 7(1):77–91, 1952.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

Arvind Narayanan et al. *Bitcoin and Cryptocurrency technologies*. Princeton University Press, 2016.

Nationalbanken. Danskerne er mestre i at betale elektronisk. (6), 2017.

Douglass C. North. Final remarks-institutional change and economic history. *Journal of Institutional and Theoretical Economics*, 145(1):238–245, 1989.

Murray N. Rothbard. *What Has Government Done to Our Money.* Ludwig von Mises Institute, fifth edition, 1963.

Murray N. Rothbard. The austrian theory of money. *Economic Controversies*, 2011.

Malcolm Rutherford. Thorstein veblen and the processes of institutional change. *History of Political Economy*, 16(3):331–348, 1984.

Robert J. Shiller. The old allure of new money. *Project Syndicate*, 2018.

Stoyan V. Stoyanov Svetlozar T. Rachev and Frank J. Fabozzi. *Advanced Stochastic Model, Risk Assessment and Portfolio Optimization.* John Wiley & Sons, 2008.

Federal Reserve System. The federal reserve payments study 2016. 2016.

Tether. Tether: Fiat currencies on the bitcoin blockchain. 2016.

Thorsten Thadewald and Herbert Buning. Jarque-bera test and its competitors for testing normality - a power comparison. *Journal of Applied Statistics*, 34(1):87–105, 2007.

Ludwig von Mises. *The Theory of Money and Credit.* Ludwig von Mises Institute, english edition, 1912.