Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Industriell økonomi/lnvestering og finans	Vårsemesteret, 2018 Åpen
Forfattere: Einar Berg Kvammen og Andreas Lie Askeland	…………………………………… (signatur forfatter) …………………………………… (signatur forfatter)
Fagansvarlig: Atle Øglend Veileder(e): Atle Øglend	
Tittel: A comparative volatility analysis and an enquiry into the future of Bitcoin	
Studiepoeng: 30	
Emneord: Cryptocurrency, Bitcoin, GARCH, eGARCH, financial time series, volatility, efficient market hypothesis.	Sidetall: 58 + vedlegg/annet: 7 Stavanger, 06.06.2018

i. Abstract

The main object of this thesis is to investigate if Bitcoin has matured as a financial asset. We intend to do this by comparing the volatility of Bitcoin to the volatility of gold and S&P500 using the best fitting GARCH models. By doing this we can examine whether the volatility is decreasing, suggesting a maturing market. We will also look at the correlation between these assets.

As part of this thesis we will provide a clear picture of what Bitcoin is, and how it functions. We are also going to uncover some of the opportunities and limitations that faces Bitcoin. This will be done by giving a thorough explanation of the technical aspects of Bitcoin to get a clear image of the security and reliability of Bitcoin and the blockchain-technology.

To answer the questions presented in this thesis we used a variety of GARCH models to model the volatility of Bitcoin and other assets. This revealed that Bitcoin exhibits an extreme volatility, which does not seem to be decreasing or stabilizing. This lead to the conclusion that Bitcoin is not yet maturing as a financial asset.

ii. Preface

The work presented in this thesis is written in cooperation between Andreas Lie Askeland and Einar Berg Kvammen. The workload has been shared equally between the two authors. This thesis concludes our master within the field of Industrial Economy. Through our education we have acquired a balanced set of knowledge within the fields of economics and technology. This combination of knowledge has been useful throughout this thesis as we got to combine technology and economy into one subject. The subject is of great interest to us as we both are interested in technological advances, valuation, and the subject of privacy in a digitalized world.

We would like to thank Atle Øglend as our mentor and supervisor. His good advice and quick response to our questions and requests has been of great help through the writing process. We would also like to thank our family and friends for all the support through the writing of this thesis and through our entire education.

Andreas Lie Askeland and Einar Berg Kvammen

Dato: 06.06.2018

iii. Terminology

ACF – Autocorrelation function

AIC – Akaike information criteria

AR – Autoregressive

ARCH – Autoregressive conditional heteroskedasticity

ARIMA – Autoregressive integrated moving average

ARMA – Autoregressive Moving Average

BIC – Bayesian information criteria

BTC – Bitcoin

DCF – Discounted cash flow

eGARCH – Exponential generalized autoregressive conditional heteroskedasticity

EMH – Efficient market hypothesis

GARCH – Generalized autoregressive conditional heteroskedasticity

HQIC – Hannah Quinn information criteria

IID – Independent and identically distributed

MA – Moving Average

PACF – Partial autocorrelation function

SHA-256 – Secure Hash function 256-bits

SIC – Shibata information criteria

S&P500 – Standard & Poor 500

WACC – Weighted average cost of capital

Table of Contents

1. Introduction

In 2007 the USA housing market collapsed, causing a global financial crisis. The stock market crashed, and a lot of people lost their investments and life savings. This caused big banks and financial institutions to declare bankruptcy. The problem when large financial institutions and banks declare bankruptcy is that it does not simply affect the workers of the bank, but everyone involved with the bank. This has been popularized as “too big to fail”, implying that we simply can’t allow these banks to go bankrupt because of the impact it will have on the economy (Goodman, 2008). To save the banks and the economy, the government had to step in and bail out the banks, which meant spending taxpayers’ money to save the banks. Given that the financial crisis initially started with banks giving out risky loans to reap huge profits, many people found it provoking that they had to suffer the consequences of the banks misbehavior, while the consequences for the banks were minor (Amadeo, 2017).

In 2008 a person or a group with the pseudonym Satoshi Nakamoto released a paper called "Bitcoin: A peer-to-peer electronic cash system" where the idea of a digital currency was explained. In a world moving away from cash, meaning that two free individuals would be unable to exchange any money without the intermediation of a bank, Satoshi argued that a new and digital global currency was necessary. A digital currency without the need of an external third party to verify transactions is not a new concept, however. It has been experimented with many times in the past, but they all seem to have had one problem in common. Namely the “double-spending” problem. In Satoshi’s paper he explained the concept behind a new type of technology he called blockchain that allegedly solved this problem. The new digital currency called Bitcoin would work, as the title would suggest, as a peer-to-peer electronic cash system removing the need of a trusted third party to verify all transactions (Nakamoto, 2008). Since the launch of Bitcoin, it has been a disputed subject in the world of finance. Some claim Bitcoin to be a revolutionary payment system, while others consider it a bubble exhibiting many traits similar to a Ponzi-scheme (Reid, 2018).

In this thesis we intend to answer the following questions:

- What are cryptocurrencies and what advantages do they bring to the table compared to traditional fiat currencies?
- Is Bitcoins volatility decreasing, indicating that Bitcoin is maturing as a financial asset?

A technical introduction to Bitcoin will be presented followed by some financial framework to understand how Bitcoin should be classified. Methodology regarding the analysis of financial time series is presented for the reader to understand how we have chosen to examine the maturity of Bitcoin through its volatility. Further, our data and findings will be presented and interpreted, and this will be used to draw a conclusion about the future of Bitcoin.

2. Bitcoin

Bitcoin was first introduced to the world through a white paper titled "Bitcoin: A peer-to-peer electronic cash system". The paper was published in 2008 by the pseudonym Satoshi Nakamoto (Marr, 2018). The paper described the concept of a digital currency called Bitcoin, and the program sustaining Bitcoin was launched in 2009. Since then, the volatility of Bitcoin and the massive profit collected by early investors has brought Bitcoin to the spotlight of the media, and most people with an interest in finance or technology has an opinion on it. In this section of the thesis the authors will give a simple and a technical introduction to Bitcoin with the intent of giving the reader an idea of how Bitcoin works, why Bitcoin has gained value, and what limitations and possibilities that faces Bitcoin.

2.1. A technical introduction to Bitcoin

The technology that enables Bitcoin and other cryptocurrencies is called a blockchain. A blockchain is a publicly distributed ledger. This ledger enables transactions to take place in a peer-to-peer[1] network, without a third party to verify transactions. For this system to work, everyone in the network has a copy of the public ledger. If anyone wish to conduct a transaction, they must announce this to the rest of the network. Each participant in the network will then investigate if there are sufficient funds to complete the transaction and confirm the transaction if it is deemed possible. This is to avoid someone spending their funds several times. When the transaction is confirmed by the network, every participant updates their ledger with the new transaction. All transactions that are confirmed will later be encrypted with other transactions in a *block*. Each block on the blockchain contains information about the previous block, ensuring that one cannot alter a single block without altering all the following blocks. Because of this it is impractical and very demanding to alter the information that is stored on the blockchain, which is paramount for the blockchains security.

[1] A peer-to-peer network is a network without a centralized authority that must approve of actions taken in the network

In the next section the simplified explanation given above will be elaborated on, and some important functions of the Bitcoin system will be examined.

2.1.1. Double-spending

Blockchain technology solves a challenging issue regarding cryptocurrencies, namely the issue of *double-spending* (Lasn, 2017). Most digital files on a computer can be duplicated or falsified. This poses a threat to the concept of a decentralized cryptocurrency, as the opportunity for anyone to counterfeit a digital currency would render it useless. Usually when conducting a transaction there is an exchange of physical items, or in the case of paying with a credit card, there is a third party that will make sure that the transaction is genuine. This system with centralized authority gives a lot of power to the banks and credit card companies that keep track of the transactions, and it also has transaction costs.

With a decentralized currency exchanges are conducted directly between buyers and sellers. In place of relying on a third party to track and keep record of the transaction on a ledger closed off to the public, Bitcoin uses a blockchain as a public ledger. Anyone can access this ledger, and the balances of every user can be viewed by anyone. Actually, it's more precise to say that every user can view every transaction ever registered on the blockchain, and the balances are kept by adding all the transactions together. As soon as a transaction is transmitted to the network, the active participants will check the balances of the parties in the transaction and confirm the transaction if it is feasible. After the transaction is confirmed, the funds in question will move from buyer to seller. Because any transaction on the blockchain is checked and must be accepted by the peer-to-peer network it is practically impossible to confirm a transaction that is not valid, and so the only way to fool the blockchain is to go back in time to delete transactions, and thus be able to spend the money several times. This is known as double-spending.

The active participants in the network that confirm or reject the transactions are called *miners*. The miners receive a reward of Bitcoins if they confirm a block of transactions to the blockchain. To decide which of the miners will be allowed to add and confirm transactions to the blockchain, the public ledger is operated as a democracy based on computing power. This will be explained further in chapter 2.1.4.

2.1.2. Cryptographic hash function

To understand the mining prosses and how the miners confirms and reject transactions, it is necessary to be introduced to some cryptography. A hash function is a mathematical algorithm that converts an input of any size to an unrecognizable output of a fixed size (Fisher, 2018). The hash function used when creating Bitcoin addresses is the SHA-256 function developed by the NSA. The output of the SHA-256 function consists in every case of 64 digits, consisting of numbers and small letters from the English alphabet. (Pacia, 2013) The input can vary from an empty space to a long story, or in the case of Bitcoin, a ledger of every transaction made in the last 10 minutes on the blockchain. A characteristic of a hash function is that it is easy to calculate the output given the input, while it is extremely demanding to calculate the input given the output. The only way a computer can do this is to run random guesses to the input to find a match for the output. Given the 36^{64} different combinations that may be the correct output, this is extremely time consuming.

2.1.3. Merkel trees

A Merkle tree is a binary tree where the outermost branches are hashes of original data, and each parent node is a hash of the combination of its children nodes. Each transaction (Tx) is used as the input of a hash function and the outputs are then combined two and two, before the result is hashed again. This is repeated until one ends up with a single hash output called the *Merkel root*. The Merkel root is then hashed, resulting in the *root hash,* which is placed in the *block header* along with the hash of the previous block and the *nonce.* The entire block header is then hashed with SHA-256 and the output serves as the block identifier. The hashed block header is then sent out to the miners of the network whom proceeds with verifying the block as explained in the next section.

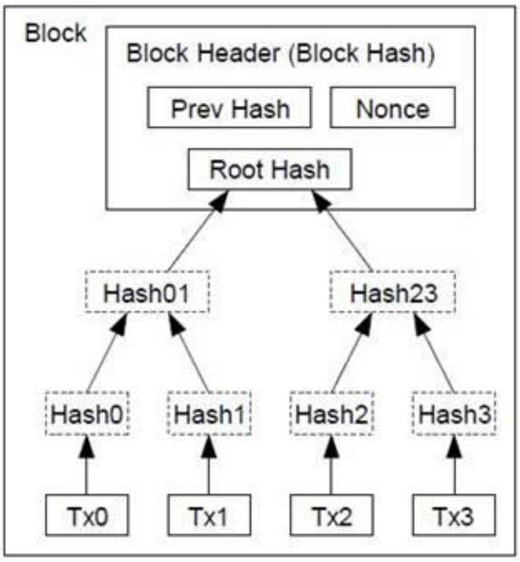

Figure 2.1: Graphical representation of the root hash, or Merkel Root (Nakamoto, 2008)

2.1.4. Miners

For a peer-to-peer cryptocurrency network to function properly, the network requires people with computer power whom are willing to contribute to the system. Every person with a strong enough computer and a stable internet connection can sign up and "rent" their computer power to the network. In the early days of Bitcoin, every user of the system was also a miner, but due to the increase in popularity of Bitcoin, mining now requires specialized hardware and software. (Pacia (1), 2013) When you download the *mining program* and connect to the system, your computer becomes part of the infrastructure that sustains the cryptocurrency. All the computers in the system receives all the transactions on the blockchain and arrange them into blocks. The blocks in the Bitcoin protocol is limited to 1 MB of data to prevent big blocks from clogging the system. The list of the recent transactions in the system is then passed through a cryptographic hash function together with a number called a "nonce". Nonce is an abbreviation for "number used once" and is in the case of Bitcoin an integer between 0 and 4 294 967 296 (Acheson, 2018). The nonce, the hash of the previous block, and the transaction list is set as the input in the cryptographic hash function and produces a corresponding output. The miners in the system each receive an individual copy of the transaction list and is given control of the nonce. To verify the transactions and accept them as changes to the public global ledger, the miners must solve a task. Solving this task and submitting the answer is called *Proof of work.* The task consists of creating an output of the hash function that meets certain criteria. In the example of Bitcoin, the criteria are that the output must start with a predetermined number of zeros. The miners then proceed to changing the nonce in the block, resulting in a random output for each new number.

Once a miner manages to guess a number that results in an output of the hash function, starting with the predetermined number of zeros, the block and all the transactions in it is considered verified and the result is broadcasted to the rest of the network. The miner that first solves the puzzle is rewarded with a predetermined number of Bitcoins, in addition to transaction fees payed by the users of the blockchain. The number of Bitcoins rewarded to the miner who is first to solve the task is halved every 210 000 blocks. The number of zeros required in solving the puzzle determines the difficulty level of solving the blocks. The difficulty level is calibrated every two weeks to ensure that the average block confirmation time is 10 minutes. In the start of 2009 the reward for solving a Bitcoin block was 50 Bitcoins. Because one block takes on average 10 minutes to solve, it takes approximately four years for the reward to be halved. After the reward for bitcoin mining has been halved 64 times, the reward is programed to be zero, since this is approximately where the function converges. This makes the finite number of bitcoins ever to be created equal to $21*10^6$ as shown in equation 2.1. (Skvorc, 2017)

$$\sum_{n=0}^{\infty} \frac{50*210\ 000}{2^n} \approx 21*10^6 \qquad (2.1)$$

The block reward at the time of writing is 12,5 Bitcoins.

As an example of the mining process, one can look at a hash function with the input "Hello world!", and a nonce that the computer of a miner would be in control of in figure 2.2. In the case of Bitcoin-mining, the input would be 1 MB of transaction history instead of the sentence "Hello world!". In this example, the predetermined number of zeros the miner must find to confirm the transactions is 4. One can see that by changing the nonce from 0 to 1 the output changes completely. It is impossible to know the output, so the only way to find an output that matches the criteria given is by systematically changing the nonce until one achieve a correct answer. In figure 2.2, the nonce 4250 resulted in an output that matched the criteria. The more zeros required in the beginning of the hash. The harder the task becomes (Pacia, 2013).

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Figure 2.2: An example of the large changes in output from a small change to the input of a hash function (Pacia, 2013).

2.1.5. Blockchain

Once a miner has broadcasted a valid hash to the network by using the correct nonce, the miners will start working on the next block. The block header of the new block contains the Merkel root of the latest transaction, the nonce that the miners can edit, a time stamp, and the solved hash output of the previous block. The hash output of the previous block links the blocks together, hence the name "blockchain". In the case of multiple blocks being solved by different miners simultaneously, the individual miners will work on the longest blockchain, resulting in multiple chains. This split lasts until someone solves the next block. When this happens, all miners will start working on the longest chain. This process is the root of the security in the blockchain. In the case of an attacker wishing to edit the ledger to increase his own balance, the hash output of the edited block will change. As shown in figure 2.2, this will result in a completely different output. This in turn will lead to a change in the next block, because the header of the previous block is included in all blocks. The domino-effect of this initial change will change every following block on the blockchain, but these blocks will not be validated by the community, leaving the change with no impact. The only way an attacker would be able to permanently edit their balance would be to calculate the new hash for the next block. The intruder would in addition have to do this for every following block. Because all the honest miners in the system always works on the longest publicly known blockchain, the attacker would have to solve blocks faster than the entire network to get the compromised blockchain validated. The only way to successfully attack the network in this way is called a 51% attack and is explained in the next section.

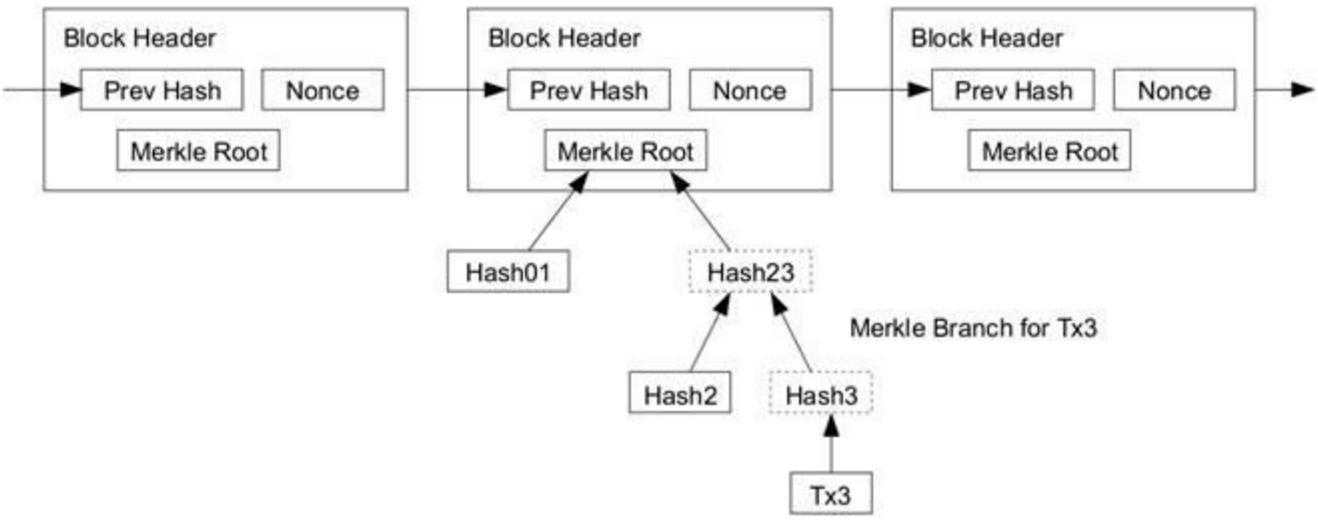

Figure 2.3: The figure shows what information the blocks on a blockchain contains (Nakamoto, 2008).

2.1.6. 51% attack

A successful attack on Bitcoins blockchain is usually referred to as practically impossible. This is because an attack is theoretically possible if one agent were to take control over more than 50% of the networks computing power. This scenario is commonly referred to as a 51% attack. As mentioned in section 2.1.4, the confirmation of new blocks on the blockchain is a race between the miners to solve a task before the rest of the network. The way the Proof of work system functions is that a miner's probability of solving the task is proportional to the miners relative computing power. In other words, a mining pool[2] that controls 10% of the networks computing power will have a 10% chance of solving the next block.

As we know from section 2.1.5, a change in a former block will also lead to a change in the following blocks. Because the network only accepts the longest blockchain as the true ledger, an attacker will have to create new blocks faster than the rest of the network to manipulate the ledger. If we examine the case of a mining pool operating 10% of the networks computing power, they would face a diminishing chance of beating the network for every block that is accepted, illustrated by equation 2.2.

$$P = 0{,}1^{n} \qquad (2.2)$$

[2] A mining pool is a group of miners who shares resources to solve blocks in cooperation. The mining pool share the rewards based on how much computer power one contributes, securing an even cash flow.

Where P is the probability of success, and n is the number of blocks solved by the community after the changed block. However, if the attacker is in possession of 51% of the networks computing power the game changes. In this case, the attacker could make alterations to transactions in an accepted block and find new solutions for the other accepted blocks without publishing the solutions to the rest of the network. Because the attacker controls more than 50% of the network, he would theoretically solve blocks in private faster than the rest of the network, and as soon as the hidden blockchain is longer than the public blockchain, the hidden chain would be published. This would lead to the honest miners starting to work on the previously hidden blockchain, validating the alterations made by the attacker. The attacker would not be able to transfer Bitcoins to himself from other users, but he could use his Bitcoins to buy goods, and delete the transactions as soon as he receives the goods, allowing him to spend money several times. Obviously, an attack like this would be devastating for the trust people put in Bitcoin and deem the coin useless. Fortunately, this is a highly unlikely scenario because of the high cost of obtaining this amount of computing power. In addition, it would probably be in the interest of any group holding such a large amount of the networks computing power to behave honestly to secure the integrity of the blockchain, and thus maximize future profits. In the original white-paper, Nakamoto calculated that an attacker with 10% of the computing power would have a 0,024% chance of beating the odds and confirm 6 blocks of transactions before the rest of the community (Nakamoto, 2008). This is one of the reasons why it is recommended for suppliers to wait 6 blocks, which is about an hour, after receiving Bitcoins before sending goods.

2.1.7. How to transfer Bitcoins

To understand how Bitcoins are transferred safely, it is necessary to possess some knowledge of data encryption. Cryptocurrencies are secured through key cryptography. There are mainly two types of key cryptography, symmetric key cryptography and asymmetric key cryptography. In the case of symmetric key cryptography, both the sender and the receiver of a message will have an identical cryptographic key. This key is used by the sender to encrypt the message, and by the receiver to decrypt it. This is comparable to applying password protection to a file.

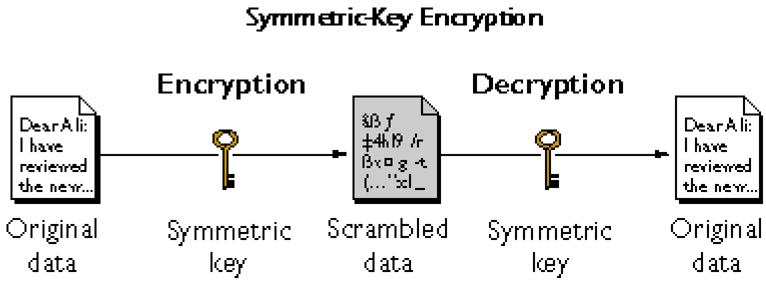

Figure 2.4: Data encryption/decryption using a symmetric key (IBM knowledge center, 2018).

This is a very effective and easy way of sending private information, but there are negative sides to this method. It is safe to exchange information as long as only the sender and the recipient has access to the encryption key. Thus, the drawback to the symmetric secret-key ciphers is the exchanging of the secret key. If one wishes to safely send a key to a recipient without a physical exchange, one must encrypt the key itself, meaning that the person must already own the key to decrypt the new key (IBM knowledge center, 2018). Symmetric key cryptography also works as a signature for the message. If you can decrypt a message, you know it has been encrypted by the matching key.

Bitcoin does not use symmetric key encryption. Instead Bitcoin uses asymmetric key cryptography. With this system two keys are used instead of one. This is a private key, and a public key. The public key is open for all to see, but the private key is kept secret. In more practical terms one can say that that the public key is a user's address or account. The pair of keys associated with an account are related, enabling the private key to decrypt messages encrypted by the public key. The hash chain relating the two keys makes it infeasible for an attacker to decrypt a message encrypted by a public key without knowing the private key. This ensures that each person holding a private key can receive and interpret messages from anyone with access to his public key. The combination of a private key and a message also works as a signature. Given that all public keys are accessible for anyone, it is possible to use the public key to see who has signed a transaction. If someone's public key can be used to decrypt a message, one can be positive that the person holding the corresponding private key has encrypted it. The key pair is automatically created when someone becomes part of the Bitcoin network. Joining the Bitcoin network does not require any form of identification, though most people will create their key pair through a third party that requires identification. It is nonetheless possible to participate in the Bitcoin network without revealing your identity to anyone.

When Bitcoins are transferred from one user to another, what happens is that the sender will publish a message to the network. This message will contain the address of the recipient, and the number of Bitcoins the sender wishes to transfer. The message is also signed by the sender using the private key. Once the nodes in the network receive the message they will check that the signature matches the public key, and if it does the network will also confirm that the sender is in possession of sufficient funds to complete the transaction. When this is done, the transaction will be pooled with the other confirmed transactions, and the miners will include it in the next block on the blockchain (Nakamoto, 2008).

2.2. Classification of Bitcoin

The classification of Bitcoin is a subject which there are some disagreement among economists. For the authors, and most people who hear of Bitcoin for the first time, it may be natural to think of Bitcoin as a currency because of its name and the fact that the creator of Bitcoin intended it to be a form of money (Nakamoto, 2008). However, to give a formal classification of Bitcoin it is necessary to look at Bitcoins properties.

According to the Merriam Webster dictionary, a currency is something that circulates as a medium of exchange. Although this is not limited to money, in our modern society, currency and money goes hand in hand. For something to be classified as money it should be generally accepted as a medium of exchange, it should store value, and be a unit of account. Examination of Bitcoins properties can rise doubts of whether Bitcoin can be classified as either money or a currency.

As will be shown in chapter 5, the volatility of Bitcoin is extreme, even compared to stocks. Traditional currencies like the Dollar and the Euro also experience volatility, but not anywhere near the levels exhibited by Bitcoin. With that being said, there are examples of currencies backed by national banks that has experienced extreme inflation, which has made them temporarily or permanently unable to function as money (Stoltz, 2018). It can non the less be argued that Bitcoin isn't a good store of value compared to other currencies considering how volatile the value of Bitcoin is at the time of writing.

Bitcoin does not provide a perfect unit of account either. Though Bitcoin provides a perfect record of all transactions ever conducted through the Blockchain, these transactions only represents the underlying economic transactions, and is thus not complete as a unit of account (Jenssen, 2014, p. 40).

Bitcoin has been used as a medium of exchange since its very beginning (Ytterstad, 2017). Since then Bitcoin has gained a reputation as a currency used by criminals to conduct untraceable transactions. Today there seems to be some problems facing Bitcoin as a medium of exchange. One of which has to do with circulation. Since Bitcoins beginning in 2009, the value has skyrocketed. There have also been periods of extreme reduction in value, but in general there has been an appreciation of Bitcoin. This has led to many people acquiring Bitcoin not to use it, but to accumulate it for future economic benefit, or to "HODL"[3]. The consequence of this strategy is that there are few Bitcoins in circulation, and that few people wish to trade Bitcoins for other goods in fear of missing out on the expected economic benefit from selling the Bitcoins at a higher price in the future. There is some evidence that the price of Bitcoin is correlated with news regarding Bitcoin. (Meland & Øyen, 2017, p. 18). This implies that not all investors follow the "HODL" philosophy.

There are also some concerns related to the transaction speed of Bitcoin. Blocks are confirmed every 10 minutes, and the maximum block size is 1 MB. This puts a constraint on the output of the network and may limit transaction speed. This may make Bitcoin impractical for daily use.

Another problem is that few businesses accept Bitcoin as a payment method, thus limiting the usage of Bitcoin as a medium of exchange.

2.3. Problems with Bitcoin

The problems mentioned so far are mostly connected to the technical properties of Bitcoin and the short amount of time that Bitcoin has been around. Perhaps the biggest problem for Bitcoin is that use of cryptocurrencies requires people to think different about money. With traditional fiat currencies your moneys value is guaranteed by the government. There are also sophisticated safety nets that to some degree can prevent scams and help recover lost funds or revoke mistakes made when transferring money.

---

[3] HODL is an intentional misspelling of the word hold and refers to the strategy of acquiring Bitcoins with the intent of holding on to the coins without regard for negative price shocks.

What keeps a currency valuable is mainly trust. People trust that when they trade a good or service for money today, they will be able to trade the same money for other goods or services tomorrow. Building trust in a system takes time and usually requires multiple positive experiences with the system. One example where trust has slowed down the implementation of a new type of payment method is the introduction of credit cards. The credit card has several advantages over cash as it is easier and safer to store, it can easily transfer large amounts of money, and it is possible to stop or revoke transactions. The popularity of credit cards exploded in the 1970s and it has become a common way of exchanging value for most people. Yet even today, almost 50 years later, after several successful years of proving its trustworthiness and reliability there are still people whom prefer to make payments using cash.

It can be argued that Bitcoin possesses advantages over traditional credit card and cash payments, some of them are mentioned earlier, but it also has several disadvantages. One of the advantages of Bitcoin is that it removes the need for an external third party to verify transactions. This of course also means that people will have to take responsibility for their own transactions. If one makes a mistake when transferring Bitcoin, the mistake is yours, and there is no one to correct it. This means that if you type in an address where you want to send funds and make a typing error and send the coins to a non-existing address these funds will be lost forever. This is due to the security of the blockchain, which does not allow revoking confirmed blocks/transactions. When we look at how long it took before credit cards were adopted by the mass majority, a system which is backed by governmental law and requires nothing of the user except memorizing a 4 digit code and putting the system to use, one can only try to imagine the time it will take before people start placing trust in a new system that offers no warranty that your values are safe, and that punishes you for making mistakes. This combined with high volatility and lack of user-friendliness can prove to be huge obstacles for the implementation of Bitcoin.

Hackers and cybercrime is also a big threat to the mass-adaption of Bitcoin. Cryptocurrencies are building on emerging technologies that may have unknown security-holes, and there has been several known cases of theft and security breaches like Mt. Gox[4] and the Ethereum hacking[5]. With the anonymity offered by cryptocurrencies it may be easier than ever to get away with large sums of money from crime, because cryptocurrencies often are untraceable.

2.4. Potential of Bitcoin

As an unregulated and independent money system, Bitcoin provides some advantages and opportunities under certain conditions. Bitcoin functions the same way independent of geography, and this can prove to be valuable when transferring funds across borders. Especially when sending remittances to third world countries, use of Bitcoin could be a way to reduce fees and allow people to transfer more money at a lower cost. This offers a way around international giants like Western Union and MoneyGram by enabling quick transactions with lower fees and would probably force these companies into harder competition (Seth, 2018). In addition, the Bitcoin market is never closed, so one does not have to limit transactions to certain days and times.

In Venezuela, Bitcoin and other cryptocurrencies are used by some people to maintain their purchasing power. Though Bitcoin has high volatility, it still more stable than the national currency of Venezuela, the Bolivar, which has experienced extreme inflation during the rule of president Maduro (Voge, 2018).

In Zimbabwe, a country that haven't had a national currency since 2009, Bitcoin has gained popularity as a mean to obtain foreign currencies. The country suffers from low currency reserves, and on the black-market Bitcoin can be traded for US dollars and other foreign currencies that are legal tender (Brand, Latham, Marawaniyka, 2017). Bitcoin is also very difficult to counterfeit because of the blockchain technology. This might give cryptocurrencies an upper hand versus cash.

In western society some policymakers wish to move toward a cashless society. This has several advantages when it comes to stopping crime and ensuring that people pay taxes, but it can also

---

[4] Mt. Gox was a large Bitcoin exchange platform until it unexpecdetly shut down in 2014 after an attacker had stolen a significant amount of Bitcoins without detection (Jeffries, 2018).
[5] In 2016 an attacker took advantage of a weakness in the cryptocurrency Ethereums code, allowing him to claim a large amount of Ether.

be used as a mean to surveil the people and put restrictions on civil liberties. The existence of Bitcoin and other cryptocurrencies ensures that it will always be possible for two individuals to exchange values anonymously without an external third party even as our society becomes more and more digitalized.

3. Financial theory

In this chapter we will give a brief overview of some of the theories that will be used when discussing Bitcoins properties as a financial asset, and how Bitcoin eventually may be made part of a modern portfolio.

3.1. The Efficient market hypothesis

Whether or not it is possible to predict stock prices has been a hot and disputed topic amongst economists for decades. Many people and businesses in the financial industry make a living from doing technical and fundamental analysis of assets to uncover possible arbitrages or profiting by selling information to investors. The efficient market hypothesis (EMH) was first formulated by Eugene Fama. His hypothesis was influenced by the work of physicist Louis Bachelier and economist Paul Samuelson whom both pioneered within financial mathematics (Read, 2013, p. 1-5). In general, the efficient market hypothesis argues that is not possible for an investor to "beat the market". This means that all available and relevant information regarding a stock or an asset is considered when the market price of the stock or asset is decided (Malkiel, 2003, p. 59-61). This implies that any form of arbitrage will be impossible, and the only way an investor can achieve a higher return than the market is by increasing risk in the portfolio. Burton Malkiel illustrates this by saying that a chimpanzee throwing dart at different stocks in the Wall Street journal to set up a portfolio would have a similar long-term return as that of a portfolio set up by experts. According to the efficient market hypothesis, the value of assets will be affected by news regarding the asset directly or indirectly, but news is unpredictable and therefore the value of the asset is also unpredictable. EMH is usually classified into 3 different versions, weak, semi-strong and strong. The weak EMH suggests that the current asset price reflects all previously publicly available information. This implies that analysis of historical data can’t predict the future asset price. The semi-strong EMH says that current asset prices reflect all historical information, and that any new information immediately will be reflected in the price. This means that news about an asset will lead to a new equilibrium price for the asset, removing all possibilities for an arbitrage unless one has information that is not publicly available. With a strong EMH, all information, both public and secret, is reflected in a price, and thus it is not possible to earn risk-adjusted return that is higher than the market (Maverick, 2015).

Critics of the efficient market hypothesis often points to financial crisis and bubbles, claiming that these are evidence that EMH is inaccurate and has flaws. Behavioral economists have in recent years shown that psychology is a major influence of stocks value, and that herd mentality can undermine the efficiency of a market (Nocera, 2009). If the market truly is effective, it does not make sense that the market in the past has dropped by 20% or more in a single day. The occurrence of bubbles in a market also implies that the efficient market hypothesis can be violated under certain conditions.

3.2. Bubbles

Bubbles are commonly known as the phenomena where an asset is increasing in value to an extreme level above its intrinsic value. This is followed by a correctional drop, referred to as the bubble bursting, which returns the value of the asset to a more representative level. In some cases, the asset can also be undervalued after the bubble bursts. A bubble often occurs because of a boom in a specific market and is fueled by the investors hope that the boom will continue further into the future. Bubbles have occurred in financial time series many times and can be viewed as a violation of the efficient market hypothesis. What triggers a bubble is often new information about an assets intrinsic value and an extreme increase in an assets value compared to its historical value (Brunnermeier and Oehmke 2012, p. 12-14). Bubbles often occur within markets that investors know little about, and where they are in a hurry to invest to capture some of the extreme price increases often associated with bubbles. It can be difficult to detect a bubble, which is one of the reasons why they occur, but they are usually very clear after the bubble has burst. An example of a bubble is the dot-com bubble of the mid to late 90's. In the 20^{th} century investors' expectations of what the internet could offer businesses drove them to invest heavily in companies claiming to be the first to take practical advantage of this new phenomena. As a result, the stock value of companies who were early to adopt the internet in their business model skyrocketed until the start of the 2000's when investors realized the assets were overvalued. This resulted in a major drop in the stock prices of these companies leading to many people losing their investments (Smith, 2012). Though many companies filed for bankruptcy, and a lot of people lost money on internet-stocks, many of the most valuable companies today emerged from this era, showing that it was not all air. Examples of companies that recovered from the dot-com bubble is Amazon and Google (Misamore, 2018).

3.3. Asset valuation

Asset valuation is the process of determining an assets present value. There are many reasons for performing an asset valuation, it can for instance be necessary in the case of bankruptcy, but most commonly it is used to value an asset that one wishes to buy or sell (Simkovic, 2016). The correct price/value of an asset is supposed to reflect all available information about the assets future and present. There are different approaches to valuating assets, and the most used method is that of DCF. The following equation is used to determine an assets value by DCF.

$$V = \sum_{t=1}^{\infty} \frac{c}{(1+r)^t} \qquad (3.1)$$

Where V is the value of the asset, c is the expected cash flow, t is time, and r is the discount rate. This method is based on the time-value of money and use a discount rate in combination with the expected future cash flow of an asset to determine its present value. The discount rate can be established using WACC. The discount rate will also be affected by the riskiness of the asset. The future cash flow can be estimated by historical data, analysis of the asset, expert opinion, and all other public information about the asset. V's value is extremely sensitive to the expected value of c. DCF is focused on the intrinsic value of the asset, but the results hinges on good input to the model. Without good estimates for the expected cash flow, DCF will yield poor results.

4. Methodology

The theory presented in this chapter is inspired by the book "Analysis of Financial Time Series" by R. Tsay.

Analyses of time-series has gained popularity for decades. Some of the reason for this fields popularity is the potential to gain an upper hand in predicting the future movement of stocks. Evaluation of time series started with stochastic processes, and in the 1920s economists George. U. Yule and J. Walker first started applying autoregressive models. As an attempt to remove cyclical fluctuations in series due to seasonality and shocks the moving average model was introduced. The ARMA models were introduced during the same period by Swedish economists Herman Wold, but he was not able to determine a likelihood function to acquire a maximum likelihood estimation of the parameters. Much later, in 1970, G. E. P. Box and G. M. Jenkins authored the book "Time Series Analysis", introducing the full modelling method for individual time series in an applicable sense. One of the weaknesses of ARMA models were that most of them were only applicable to stationary time series. Non-stationarity from a rising trend and stochastic volatility is very common in financial time series, hence the field required models that were applicable to non-stationarity. This led to further research, and the development of ARMA models extended to modeling the variance of data, such as Engle's ARCH model, and the many different GARCH models. The new ARCH and GARCH models allowed for parameterization and forecasting of non-constant volatility, something that the existing Box-Jenkins models would not. These perks of the ARCH and GARCH models have made them very applicable to financial time series (Zuobir, 2017).

4.1. Lag-operators, lag-polynomials, and inverses

A lag-operator is often defined for models that are designed to forecast a result based on historical data. A lag-operator can be defined as $L^k x_t = x_{t-k}$ where k is number of lags. This equation is used to model the process moving forward. Lag-polynomials are defined as polynomials in the lag operator and can be defined as $\varphi(L)$ where:

$$\varphi(L) = \varphi_0 + \varphi_1 L^1 + \cdots + \varphi_{\mathrm{p}} L^p \qquad (4.1)$$

This again is defined as a lag-operator, giving the following equation

$$\varphi(L)x_t = \varphi_0 x_t + \varphi_1 x_{t-1} + \cdots + \varphi_{\mathrm{p}} x_{t-p} \quad (4.2)$$

An important feature of the lag-polynomials is that one can add and multiply polynomials in complex variables in the exact same way as one can add and multiply lag-polynomials. The lag-polynomial notation can be used to more easily determine stationarity in a time series process (Sørensen, 2012, p. 2-4)

4.2. Stationarity

Stationarity is the most important concept of time series analysis and says something about the series behavior with respect to time. If all the statistical properties of the series are independent of time, the series are stationary. The two main types of stationarity are *strictly stationary processes*, and *weakly stationary processes*. If, for all t, the joint distribution of $(x_{t_1}, \dots, x_{t_{\mathrm{k}}})$ is identical to that of $\left(x_{t_{1+\mathrm{t}}}, \dots, x_{t_{\mathrm{k+t}}}\right)$ the time series $\{x_t\}$ is strictly stationary. Here k is a positive integer, and t is positive integers. Simply put, a process is strictly stationary if the distribution of $\{x_t\}$ doesn't vary with time. This condition is challenging to verify based on empirical observations alone. A series $\{x_t\}$ that is weakly stationary possesses a mean and a covariance between x_t and x_{t-l} that is independent of time, l being an integer. If a time series $\{x_t\}$ is observed and it can be shown that for all $(t = 1, \dots, T)$ the T values is fluctuating with a constant variance revolving around a fixed level, the series is considered weakly stationary. The statistical moments of the series depend only on time difference and not upon time of occurrence. In other words, the covariance between one value of the series and another value at a different time, $\gamma_l = Cov(x_t, x_{t-l})$ called the lag-l autocovariance of x_t, will have two important properties; $\gamma_0 = Var(x_t)$ and $\gamma_{-l} = \gamma_l$. Weak stationarity can be used to make assumptions about a series future value. A normally distributed weak stationary series $\{x_t\}$ can be considered equal to a strictly stationary series. Stationarity is assumed to simplify the development of stochastic processes, and it is often required for models analyzing time series. (Tsay, 2010, p. 30)

To use time series models such as the ARMA variations, one must assume stationarity. In an ARMA(p,q) process consisting of a AR(p) and a MA(q) term, the MA(q) term is irrelevant when determining stationarity. A method for checking whether a timeline is stationary or not is to examine the roots of the characteristic equation. We can obtain this expression by presenting a AR(p) process in a lag-polynomial notation. If we for instance take a random AR(p) expression such as:

$$y_t = \phi_1 y_{t-1} + \phi_2 y_{t-2} + \cdots + \phi_{\mathrm{p}} y_{t-\mathrm{p}} + \varepsilon_t \qquad (4.3)$$

We can express this using lag-polynomial expression $\phi(L)$ and solving for ε_t such that:

$$\varepsilon_t = (1 - \phi_1 \mathrm{L} - \phi_2 \mathrm{L}^2 - \cdots - \phi_{\mathrm{p}} L^p) y_t \qquad (4.4)$$

By replacing the lag operator with a variable (z) and setting the resulting polynomial equal to zero we obtain the characteristic roots of the of the process. The roots will be the values of z that results in a solution to the equation:

$$\left(1 - \phi_1 z - \phi_2 z^2 - \cdots - \phi_{\mathrm{p}} z^p\right) = 0 \qquad (4.5)$$

The AR(p) process is stationary if all the values of z that solves this equation lie outside the unit circle. Should any of the solutions for z turn out to be a complex number, the process is experiencing non-stationarity. A root that is equal to one or minus one is called a *unit root*. To say that the AR(p) process is stationary all the absolute values of the roots in the process must be larger than one and be a *real* number (Magee, 2008)

4.3. Moving average models

A moving average model is a model used to determine the value of a dependent variable based on a weighted sample of the historical values of the variables error terms. The model was introduced in 1937 by E. Slutsky. A MA(q) process, where we examine observed values q periods back in time, can be written as

$$y_t = \mu + \sum_{j=0}^{q} \theta_{\mathrm{j}} \varepsilon_{t-\mathrm{j}} \; = \mu + \varepsilon_t - \theta_1 \varepsilon_{t-1} - \theta_2 \varepsilon_{t-2} - \cdots - \theta_q \varepsilon_{t-q} \qquad (4.6)$$

Where the ε_t term has a distribution of $\varepsilon_t \sim iid(0, \sigma^2)$ and is generated as "white noise". Conceptionally a MA model is a linear regression based on the current observations of the series against the random shocks of prior observations. Where θ_0 is fixed as 1. The μ represents the expected value of the series and is the intercept at $t = 0$. One of the assumptions for this model to be applicable is that the process is stationary. The label "Moving Average" can be somewhat misleading because the weights θ_{p} may be both positive and negative and does not necessarily sum to unity. The label is used by convention (Pankratz, 1983)

4.4. Autoregressive models

The AR(p) model was first introduced by Yule in 1926. In an AR(p) model an observed value at period t is weighted by the preceding observations p periods back in time and is assumed to be a linear combination of p, a random error term ε_t and a constant term. A pure AR(p) process can be written as

$$y_t = \delta + \varepsilon_t + \sum_{i=1}^{p} \phi_{\mathrm{i}} y_{t-\mathrm{i}} = \phi_1 y_{t-1} + \phi_2 y_{t-2} + \cdots + \phi_{\mathrm{p}} y_{t-\mathrm{p}} + \delta + \varepsilon_t \qquad (4.7)$$

Where the ϕ coefficients determines the weight given to the observation at period $t - p$. The error term ε_t is also in this model considered "white noise". If we reduce the AR(p) model to AR(1) with ε_t as "white noise" we end up with a simple random walk process. Autoregressive models attempt to forecast y_t by considering and weighting the predeciding observations and has proven to be useful in predicting economical time series with higher fit and accuracy than naive expectations which is one of the simplest forecasting techniques. The reason why the model is labeled autoregressive is because the parameters can be estimated using regression analysis where the independent variable is estimated by the weighting and sum of the preceding dependent variables (Sørensen, 2012, p. 4-6).

4.5. ACF and PACF

ACF and PACF are functions designed to analyze time series for autocorrelation and determine the terms for the AR and MA processes. As stated by Box & Jenkins ACF can be used to detect those lag orders of which there is significant correlation (Box & Jenkins, 1970). Autocovariance of a series, say x_t, is defined as

$$\gamma_k = \mathrm{cov}(x_t, x_{t-k}) \qquad (4.8)$$

These equations can be solved for ϕ_{ii} given that we know the value of ρ_{i}. The way this helps us to determine the lag term of an AR process is by setting different null hypotheses of $p = 1,2, \dots, k$ and analyzing which values that yield a statistically significant result. Since we normally don't possess or utilize the entire data set for time series, estimated values for ρ and ϕ will be presented. The PACF is a useful tool for determining the term of autoregressive processes. If the actuall term of the autoregressive process is equal to k we will observe that the PACF will aprox zero for any lags larger than $p = k$ (Brockwell, 2009)

4.6. ARMA models

The ARMA(p,q) time series model is a model used to determine heteroscedasticity. The model uses a combination of the autoregressive and moving average models. Including both these terms in the same model has proven to be a useful tool of analyzing time series data. The model can be written as

$$Y_t = \varsigma + \sum_{j=0}^{q} \beta_i E_{t-j} + \sum_{i=1}^{p} \alpha_i Y_{t-i} \qquad (4.9)$$

Where the $\sum_{i=1}^{p} \alpha_i Y_{t-i}$ is the AR part, and the $\sum_{j=1}^{q} \beta_i E_{t-j}$ is the MA part with β_0 fixed as 1, and $E_{t-j} \sim N(0, \gamma)$ where E_t is independent for all t. To benefit from this model, the parameters ς, $(\beta_1, \dots, \beta_q)$, $(\alpha_1, \dots, \alpha_p)$ and the variance must be estimated by maximizing the likeliehood equation for the model. For an estimated forecast of $\hat{Y}_t$ we put the initial value of $j = 1$ and derive the equation

$$\hat{Y}_t = \varsigma + \sum_{j=1}^{q} \beta_i E_{t-j} + \sum_{i=1}^{p} \alpha_i Y_{t-i} \qquad (4.10)$$

This exploits the fact that at every time t the error term in the ARMA model will be represented by the difference between the forcasted result and the actual result.

$$E_t = Y_t - \hat{Y}_t \qquad (4.11)$$

From the definition of ARMA models it is clear that the observable variables represent a deterministic variable and that the error terms represent arbitrary variables. When choosing the delay in the ARMA models (the p and q) we can use the BIC or the AIC to determine the best fit. By testing for different values and comparing the BIC or AIC output we can determine which p and q values that will result in a model closest to the true model. The ARMA model is only applicable to stationary processes (Thiesson, Chickering, Heckerman and Meek 2004).

4.7. ARIMA models

One of the main issues with the ARMA models is the lack of stationarity in time series. Time series models often assume the observed variables to be i.i.d following the normal distribution. However, time series more than often follows specific patterns over a long term such as seasonality and other cyclical behaviors. As a response to this, the ARIMA model was suggested. The ARIMA model solves the problem of non-stationarity by adding an additional parameter d to the ARMA model. The d in the ARIMA model represents the number of times we have to difference a series to achieve a stationary trend. A time series that need to be differenced to achieve stationarity is said to be an integrated version of a stationary series. The model is useful for series that experience non-stationarity and the fluctuations are non-seasonal. An ARIMA model for such a case is written as a ARIMA(p,d,q) model where p and q remains the same as for the ARMA model and d is the number of non-seasonal differences needed to achieve stationarity. Random walk models, autoregressive models and exponentially smoothing models are special cases of the ARIMA models. (Thiesson, 2004)

4.8. ARCH models

The ARIMA model and the different variations of it are based on the Box-Jenkins principle. These linear models have proven themselves useful for analyzing time series and have become quite popular due to their simplicity and ease of implementing. However, in time series, non-linearity is a quite common trait. There have been presented a variety of different models attempting to analyze time series constrained by non-linearity. Some of the most widely used are the models in the ARCH family such as GARCH and eGARCH. There exists several other models considering time series with conditional volatility, but they will not be discussed further in this thesis. One of the advantages of using a non-linear model to describe a time series is its ability to capture volatility clustering. An ARCH model could be used to describe an increase or decrease in volatility over time but is most often used to describe volatility in situations regarding shocks in a market or short periods with increased variation. An ARCH(p) model shows the variance at a given time that is conditional on predeceasing observations and their relationship. If we for instance consider an ARCH(1) model. We have the equation

$$V_{ar}(y_t|y_{t-I}) = \sigma_t^2 = \alpha_0 + \alpha_1 \varepsilon_{t-1}^2 \qquad (4.12)$$

In this equation y_t is a set of regressors that varies over $= \{1, \dots, p\}$ and ε_t is a shock or an inovation. ε_t in this example can be specified as $\varepsilon_t = \sigma_t z_t$. z_t we consider to be N~i.i.d.(0,1).

We also impose the constraints $\alpha_0 > 0$ and $\alpha_1 > 0$ to avoid negative variance. An ARCH model is useful for time series where there is an ARCH effect. The ARCH effect implies that the volatility of this period is correlated to the last period $-l$. This implies that the volatility of the series will be larger after a period of relatively large volatility and smaller after periods of relatively small volatilities. The ARCH model is designed to analyze the relationship between these volatilities, detect potential trends and try to forecast the volatility for time $t+1$. As shown in eq. 4.12 the ARCH model utilizes the values past squared observations to forecast volatility. For observations in the past the ARCH(m) relationship is

$$v_{ar}(y_t|y_{t-1},\dots,y_{t-m}) = \sigma_t^2 = \alpha_0 + \alpha_1 y_{t-1}^2 + \cdots + \alpha_m \varepsilon_{t-\mathrm{m}}^2 \qquad (4.13)$$

The term is determined by the result of either the Box-Ljung test or the Lagrang Multiplier test which examines the time series for an ARCH effect. The effect of not assuming the error term to have constant variance have proven several times to be useful in analyzing time series. The creation of the ARCH model spawned the foundation of modern day technical analysis. However, due to some complications in the model for instance the determining of the lag component and the assumption of $\alpha_0 > 0$ and $\alpha_1 > 0$, other models derived from the ARCH model have been more frequently used the last decades. Among them is the GARCH model.

4.9. GARCH

The GARCH model is an extension of the ARCH models introduced by Tim Bollerslev (1986). The GARCH model aims to increase the accuracy of its forecast by including a third term to the equation and thereby allowing the conditional variance to be dependent on its predeceasing values. Written in its most general form a GARCH(p,q) model may look like

$$(y_t|y_{t-1},\dots,y_{t-m} \cap \sigma_{t-1},\dots,\sigma_{t-\mathrm{n}}) = \sigma_t^2 = \gamma + \alpha \sum_{i=1}^{q} \varepsilon_{t-\mathrm{i}}^2 + \beta \sum_{i=1}^{p} \sigma_{t-\mathrm{i}}^2 \qquad (4.14)$$

$$\varepsilon_t = \sigma_t z_t \qquad (4.15)$$

Where the γ is the long-run average of the series while α and β terms are the weights of the previous error terms and volatilities. These parameters are determined by a maximum-likeliehood fucntion. The parameters reveal how the series reacts to market changes. For instance, a high β value tells that it will take long time for the volatility to stabilize after a market shock, and a relatively large α value is a sign that the volatility is sensetive to market events. The error term ε_t consists of two paramters σ_t and z_t, where z_t is strong white noise (i.i.d.(0,1)) and σ_t is a scaling. The advantages of adding the third volatility term are many. One of them is the fact that since last measure of volatility $(\sigma_{t-1,}\sigma_{t-2,} \dots, \sigma_{t-n})$ is included, the GARCH value at time t will be dependent on all its predeceasing values. A GARCH(1,1) model then becomes equal to an ARCH(∞) model. Other advantages that comes with the GARCH model is the ability to model phenomena's such as leptokurtosis which is very common in financial time series. Leptokurtosis is when the distribution of the time series has a fat tail with most of the observations close to the expected value. This distribution model indicates that there is a higher probability of observing both high and low extreme values then what we see in normal distributions. The data can be transformed to normality using a heavy tail Lambert W x F distribution and must be done if we intend to use a linear model. However, the GARCH model takes leptokurtosis into account, which eliminates the need for a transformation. Another useful feature of non-linear models is their ability to forecast a series in the presence of long-range dependence. Long-range dependence, also referred to as long-memory in a time series, refer to the time it takes for a market event to affect the values of future observations. This effect can be measured by the ACF to determine how much of a lag we need to accurately predict future values. However, in many cases, negative shocks have proven to be followed by higher volatility than periods with equally large positive shocks. This effect is called the "Leverage effect" and has been described several times in scientific studies, amongst them in the work of Black (1976). This is one of the disadvantages with the GARCH model as it only models the absolute value of the volatilities of past shocks. The eGARCH model, which is an extension to the standard GARCH mode, takes this leverage effect into account.

4.10. eGARCH

The eGARCH model is an exponential variation of the GARCH model presented by Nelson in 1991. Nelson argued that the nonnegative constraints on the GARCH model were too restrict and proposed the eGARCH model as a response. The eGARCH model has several advantages one of which is incorporating the leverage effect often experienced in financial time series. The model also has the advantage of removing the need for a positive parameter constriction as the parameters are put through a logarithmic function, allowing for asymmetries which is likely to occur in financial time series as many series often exhibit skewness and fat tails. The weighted innovation was considered as

$$g(\epsilon_t) = \theta\epsilon_t + \gamma[|\epsilon_t| - E(|\epsilon_t|)] \quad (4.16)$$

Where both θ and γ are constants, and both ϵ_t and $|\epsilon_t| - E(|\epsilon_t|)$ are i.i.d. variables with zero-mean and a continuous distribution. The innovation creates an asymmetry

$$g(\epsilon_t) = \begin{cases} (\theta + \gamma)\epsilon_t - \gamma E(|\epsilon_t|) & if\ \epsilon_t \geq 0 \\ (\theta - \gamma)\epsilon_t - \gamma E(|\epsilon_t|) & if\ \epsilon_t < 0 \end{cases} \quad (4.17)$$

This gives eGARCH the property of separating between positive and negative returns. An eGARCH(p,q) model can be written as

$$ln(\sigma_t^2) = \gamma + \frac{1+\beta(B)}{1-\alpha(B)} g(\epsilon_{t-1}) = \alpha_0 + \frac{1+\beta_1 B + \cdots + B_{\mathrm{q}-1} B^{q-1}}{1-\alpha_1 B - \cdots \alpha_p B^p} g(\epsilon_{t-1}) \quad (4.18)$$

Where α_0 is a constant and is the unconditional mean of $ln(\sigma_t^2)$, B is a lag operator such that $Bg(\epsilon_t) = g(\epsilon_{t-1})$ and the lag-polynomials $\beta(B)$ and $\alpha(B)$ contains zeros outside the unit circel without common factors. By using a logged conditional variance to remove the need for a positive parameter constraint and by incorporating $g(\epsilon_t)$ to allow the model to act asymetrically to positive and negative returns, the eGARCH model differs from the standard GARCH model in ways that have proven to be useful when modeling financial time series (Tsay, 2010, p. 143-145)

4.11. ARMA-GARCH

To achieve good results from the GARCH model, it is crucial that the inputs of the model are as accurate as possible. The simplest way of estimating the long run average of the time series is to simply assume the expected value to be independent of its previous values and calculate their mean. However, if a time series shows signs of autocorrelation being present then such an estimate might be too simple to achieve the most accurate results. A common way to estimate the long run average (γ) of the model is to apply the previously mentioned AR models. An ARMA model may be used to calculate the expected value of a time series where the order of the model is decided by a trial and error attempt. The expected value of a time series $E(y_t)$ given the information at time $t - 1$ can be decided using an ARMA(q,p) model

$$E(y_t|\Omega_{t-1}) = \varsigma + \sum_{j=0}^{q} \beta_i E_{t-j} + \sum_{i=1}^{p} \alpha_i y_{t-i} \qquad (4.19)$$

Where ς is the independent expected value of the observation, the Ω_{t-1} represents the information set at time $t-1$ and the AR and MA order of the model is estimated using a trial and error approach. Combining these two models is a commonly used method to forecast a time series, where the GARCH term in the model estimate the conditional volatility of the series and the ARMA term estimates the conditional mean. The goodness of the result is determined by reading the value of certain Information criteria. In this thesis we have chosen to use the Akaike Information Criteria (AIC) to determine the which of the models presented yields the most accurate results. The reason for this is because the AIC is a relatively good criteria that reveals how well the model fit compared to alternative models. It does so by dealing with a trade-off of goodness of fit and the simplicity of the model. Our reason for applying a model to a time series is to remove some of its complexity and explain it in a simpler manner. This makes the AIC the most suited criteria for our purpose. Other alternative Information criteria include the Bayes Information Criteria (BIC), the Hannah-Quinn Information Criteria (HQIC) and Shibata Information Criteria (SIC). These are commonly used when analyzing the result of an ARMA-GARCH model.

4.12. ARCH effect

To determine whether a GARCH model is suited to model a time series, we test for ARCH-effect. ARCH-effect, also known as conditional heteroskedasticity, are mainly discovered using two tests. The Box-Ljung test (1978) and the Lagrange multiplier test of Engel (1982). Both the tests are executed as a hypothesis test with null hypothesis H_0 that the data is independently distributed and an alternative hypothesis H_a that the dataset is experiencing serial correlation. The Box-Ljung test is conducted by applying the Box-Ljung statistics $Q(\mathrm{h})$ to the squared residuals of the series. The Box-Ljung statistics $Q(\mathrm{h})$ can be written as

$$Q = n(n+2) \sum_{k=1}^{\mathrm{h}} \frac{\rho_k^2}{n-k} \qquad (4.20)$$

Where ρ_k^2 is the squared result of the theoretical ACF of the series at lag k and h is the number of lags being tested. The n is the length of the sample of the series. The test statistic is under the null hypothesis asymptotically distributed as a chi-squared distribution $\chi^2_{1-\alpha,\mathrm{h}}$ with h degrees of freedom and α as the significance level. If the test statistic $Q(\mathrm{h}) > \chi^2_{1-\alpha,\mathrm{h}}$ or the p-value of $Q(\mathrm{h})$ is less than α then the null hypothesis will be rejected, and the series is experiencing an ARCH-effect. The Lagrange multiplier test is equivalent to the usual F-statistic and is similar to performing an F-test with a chi-squared distribution. The F-statistics is defined as

$$F = \frac{(SSR_0 - SSR_1)/\mathrm{h}}{SSR_1/(n-2\mathrm{h}-1)} \qquad (4.21)$$

Where SSR_0 is the sum of squared residuals for the sample period and the SSR_1 is the sum of the squared least-square residuals of the prior linear regression. Also, here n and h represents respectively the sample length and the number of lags being tested. If the F-value turns out higher than the $\chi^2_{1-\alpha,\mathrm{h}}$ or the p-value of F is lower than our chosen α, we reject the null hypothesis and conclude that conditional heteroskedasticity is present in the series (Tsay, 2010, p. 114-115).

5. Data and results

The data used in this thesis is chosen based on the authors understanding of what Bitcoin is, and what Bitcoin is meant to be. Bitcoin is a recent invention, and as a financial asset there has been conducted little research on Bitcoins properties and possibilities. This in turn implies that it is challenging to find other financial assets that has shown any significant relationship with Bitcoin. Facing these challenges, the focus of this chapter will be to compare the volatility of Bitcoin to that of the S&P500 index, and the spot price of gold. In addition, the rolling correlation between Bitcoin, S&P500 and gold will be examined.

5.1. Data collection

The historical data used in this thesis has been retrieved from various sources. S&P500 data comes from Yahoo finance[6], Bitcoin prices is retrieved from charts.bitcoin.com[7], gold prices are from the and LBMA[8] via Quandl[9]. All data is daily observations from all available trading days. The observations run from 1st of October 2010 until 20th of March 2018. The original dataset

[6] https://finance.yahoo.com/quote/%5EGSPC/history/?guccounter=1
[7] https://charts.bitcoin.com/chart/price
[8] London Bullion Market Association
[9] https://www.quandl.com/data/LBMA/GOLD-Gold-Price-London-Fixing

for Bitcoin contained 2728 observations, the S&P500 dataset contained 1879 observations, and for gold we have 1887 observations. All GARCH models has been created by using the rugarch[10] package in R, and price observations and correlation has been plotted in Excel.

Unlike traditional financial assets and products, Bitcoin is always trading, and so the market is never closed. The "closing price" of Bitcoin in this thesis is the price observed at midnight. With no closed days this gives 2728 daily observations. Seeing that the S&P500 is an American index, the observations used follows the American trading calendar, resulting in a total of 1879 observations over the observation period. The gold price on the other hand is from LBMA and therefore follows the British calendar, giving 1887 observations. It was the authors wish to have 3 datasets with an equal amount of observations, and to achieve this, all American and British closed days has been removed from the datasets, resulting in a total of 1845 daily observations.

The S&P500 is a popular indicator of the performance of the US economy. It has less exposure to tech-stocks than NASDAQ, and it captures about 80% of the total market capitalization of the stock market (Amadeo, 2018). It is considered by the authors to be a good asset to compare to Bitcoin because many people treat Bitcoin as an asset when they invest in it. In addition to the S&P500, Bitcoin will be compared to gold. As mentioned in chapter 2, Bitcoin has many of the same properties as gold, for that reason it is of interest to investigate how Bitcoins price move compared to gold.

[10] Author of the package is Alexios Ghalanos, 2014.

5.2. Descriptive statistics of Bitcoin

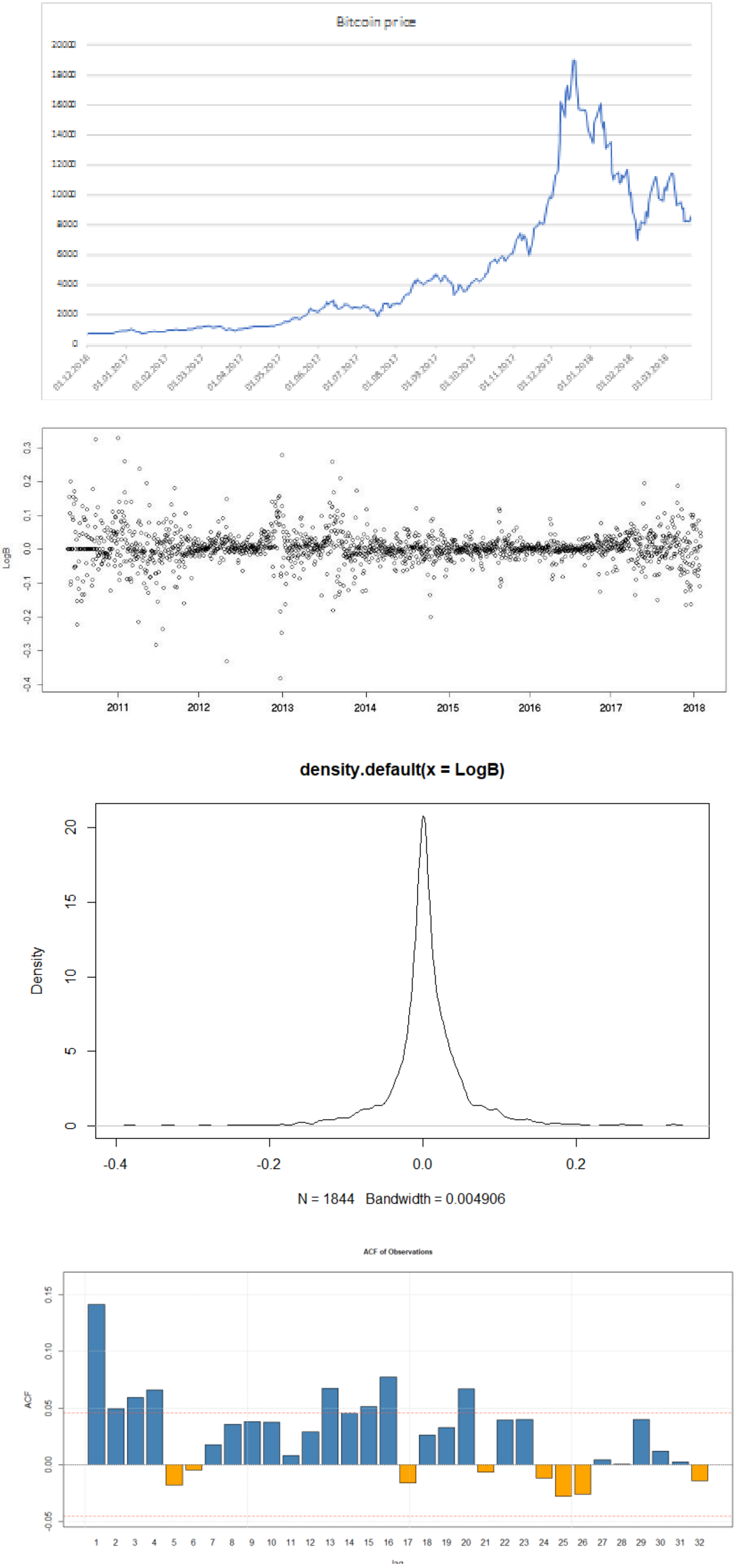

Figure 5.1: Descriptive statistics for Bitcoin. (Price, log daily return, density plot and ACF).

From the plotted daily return of Bitcoin, we can see from simple visual inspection that the price has been going through some dramatic changes during the sample period. From a minimum value at the beginning of the period of $0,06 and a peak value of $18 987 right before Christmas 2017. Though the price has since been falling, it is clear that Bitcoin has been appreciating heavily since its introduction to the public. It is worth noting that there has not been any major financial crisis in the sample period. If we look at the density distribution of the Bitcoin daily log-return we see that most of our observations are centered around the expected value of the return and the data set has heavy tails with a high probability of extreme values compared to the normal distribution. The daily log-return plot for Bitcoin also suggests that volatility clustering is present and gives us an idea that the series is exposed to an ARCH effect. We can also see from the daily log-return plot that bitcoin is an extremely volatile asset peaking with a daily log-return in the sample period of 32,89% and a loss of -38,25%. The volatility of Bitcoin also seems to be steadily decreasing from the beginning of the sample period, but it experiences a rising trend near the end of the sample period. The ACF plot gives us an idea that there is autocorrelation present in the series and that it is significant all the way back to lag $k = 20$.

When analyzing the data for an ARCH effect by applying the Lagrang multiplier test and the Box-Ljung test we obtain the results listed in tables 5.1 and 5.2. As we can see from table 5.1 and table 5.2 all the lags tested yields a test statistic value greater than the corresponding chi-squared values ($\chi^2_{1-\alpha,\mathrm{h}}$) with a significantly low p-value. Judging by the test results, it is safe to say that an ARCH-effect is present in the time-series.

Box-Ljung test results (Bitcoin)						
Lag	1	5	10	15	20	30
X-squared	36,953	56,594	64,927	83,701	106,91	119,14
P-value	1,21E-09	6,13E-11	4,19E-10	1,46E-11	7,17E-14	1,42E-12

Table 5.1: Box-Ljung test results (Bitcoin)

Lagrange multiplier test results (Bitcoin)						
Lag	1	5	10	15	20	30
X-squared	96,816	257,44	328,08	379,11	444,7	484,62
P-value	2,20E-16	2,20E-16	2,20E-16	2,20E-16	2,20E-16	2,20E-16

Table 5.2: Lagrange multiplier test results (Bitcoin)

As seen in table 5.3, the Bitcoin series has a kurtosis value of 9,0165 which indicates a leptokurtotic distribution relative to the normal distribution which has a kurtosis of 3. This complies well with our suspicions from visual inspection of the density plot and this indicates that a student-t distribution would be of better fit than a normal distribution. The distribution also has a skewness of -0,07011 which is well within the range of being considered symmetrical {-0,5 , 0,5}.

	Number of observations	**Mean**	**Standard deviation**	**Kurtosis**	**Skewness**
BTC	1844	0,004673	0,050305	9,016505	-0,07011

Table 5.3 Descriptive statistics of Bitcoin

5.3. Descriptive statistics of S&P500

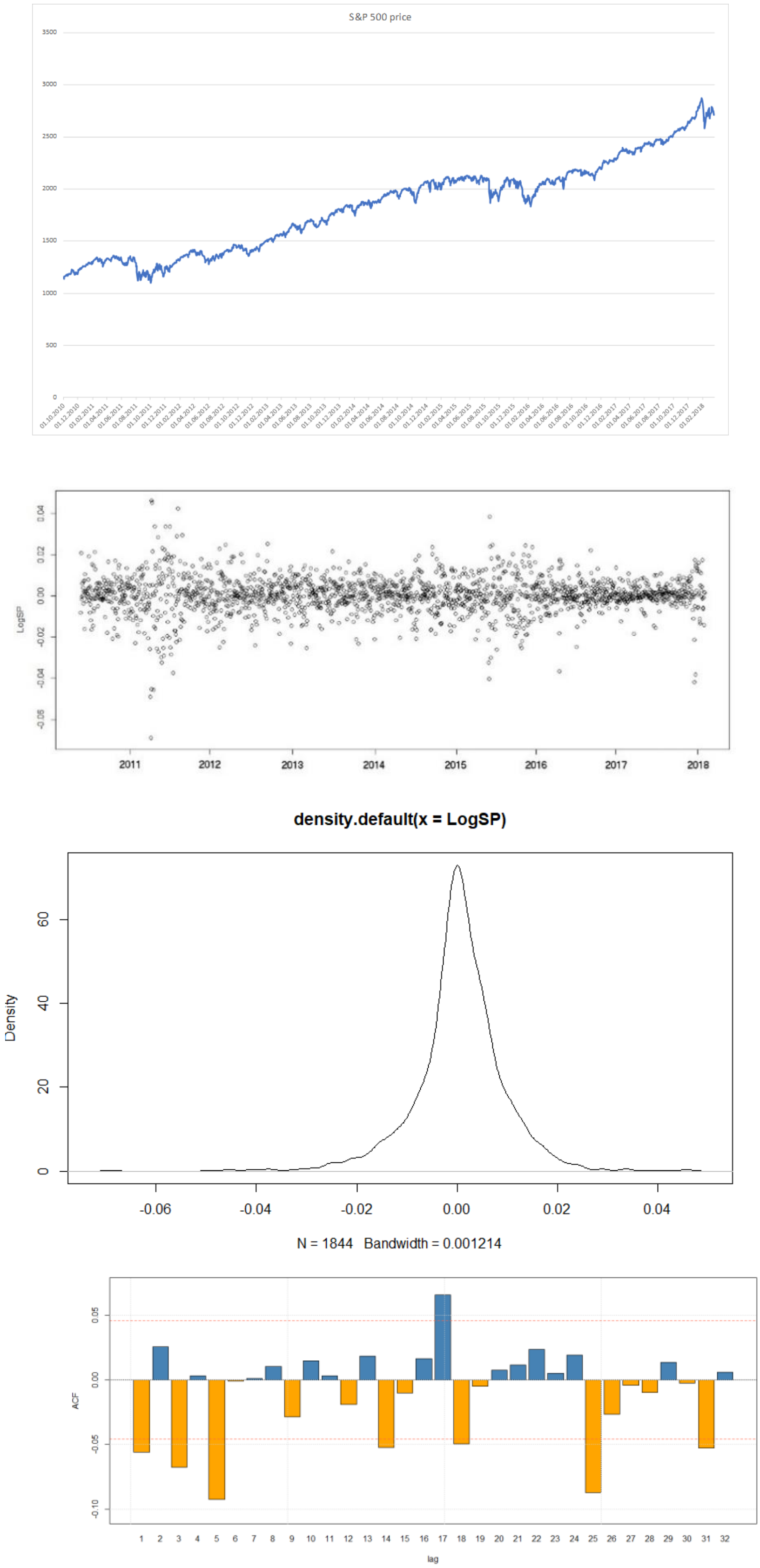

Figure 5.2: Descriptive statistics for S&P500. (Price, log daily return, density plot and ACF).

From the plotted stock price of S&P500 we can see that the index has increased in a stable manner during the sample period. The price of the S&P500 has gone from a bottom value of $1099 to a peak value of $2873 with small deviations from the trend. We can also see from the daily log-return plot that the price is quite stable with a maximum daily log-return value of 4,63% and a maximum daily loss of -6,9%. The plot also indicates that there is some volatility clustering in the series. The ACF graph indicates that we may have significant autocorrelation present in the series all the way back to lag $k = 31$.

When analyzing for ARCH-effect in the series, similarly as for Bitcoin, we apply the Lagrang Multiplier test and the Box-Ljung test and obtain the results presented in table 5.4 and 5.5. As shown in the tables, both tests indicate that ARCH-effect is present in the series.

Box-Ljung test results (S&P500)						
Lag	1	5	10	15	20	30
X-squared	5,75	31,199	33,332	39,876	53,06	71,127
P-value	0,01648	8,56E-06	0,0002395	0,000474	7,97E-05	3,43E-05

Table 5.4: Box-Ljung test results S&P500

Lagrange multiplier test results (S&P500)						
Lag	1	5	10	15	20	30
X-squared	155,63	809,78	1067	1162,5	1264,9	1443,6
P-value	2,20E-16	2,20E-16	2,20E-16	2,20E-16	2,20E-16	2,20E-16

Table 5.5: Lagrange multiplier test results (S&P500)

Furthermore, the S&P500 series has a skewness of -0,59376 and kurtosis of 5,4201. This shows that the series has a leptokurtotic distribution with a moderate negative skew. A negative skew in a financial time series indicates that there is a higher probability of getting extreme negative returns than the probability of getting extreme positive returns based on the sample period.

	Number of observations	**Mean**	**Standard deviation**	**Kurtosis**	**Skewness**
S&P500	1844	0,000433	0,009037	5,420099	-0,59376

Table 5.6: Descriptive statistics S&P500

5.4. Descriptive statistics Gold

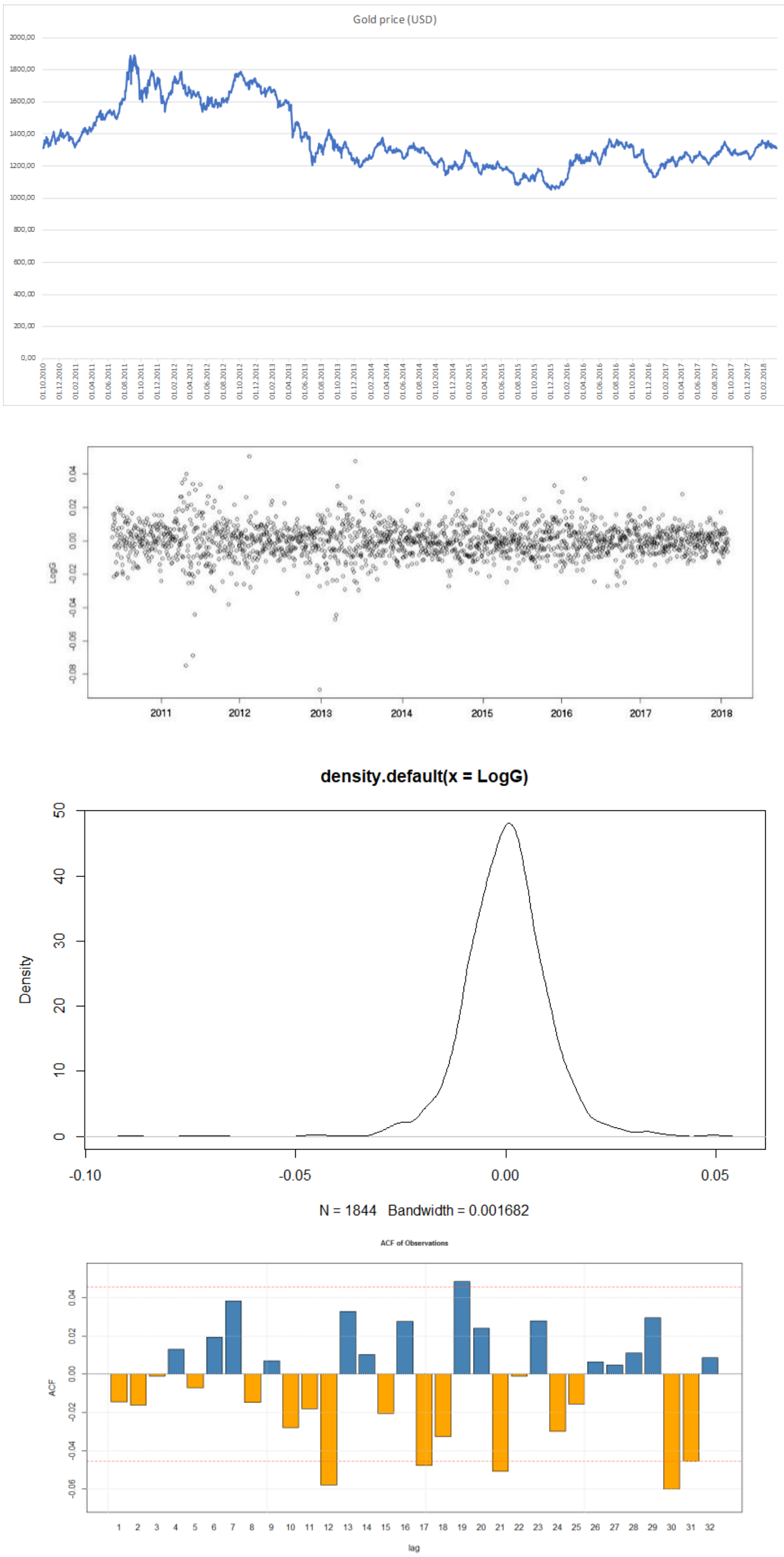

Figure 5.3: Descriptive statistics for gold. (Price, log daily return, density plot and ACF).

The plotted spot price of gold tells us that gold is the least performing asset in our evaluation portfolio. Through the sample period the price of Gold has been swinging within the range of a maximum value of $1891 and a minimum value of $1050. The spot price at the start of the sample period seems to be close to the spot price at the end of the sample period. The asset has been somewhat volatile during the sample period with a maximum daily log-return of 5,07% and a maximum loss of -8,91%. Even though the daily log-return plot shows signs of volatility clustering, visual inspection alone is not sufficient to draw this conclusion. The density plot gives us an idea of the skewness and kurtosis of the daily log-return distribution, while the ACF plot indicates that we have significant autocorrelation present in the series.

When applying the Box-Ljung test and the Lagrang Multiplier test to the data we achieve the results presented in table 5.7 and table 5.8. The results show that there appears to be a dispute between the test of whether an ARCH-effect is present or not. The Lagrange multiplier test shows clear signs of an ARCH-effect while the Box-Ljung test indicates that no conditional heteroskedasticity is present in the series.

Box-Ljung test results (Gold)						
Lag	1	5	10	15	20	30
X-squared	0,38147	1,2682	6,6387	16,461	29,575	46,706
P-value	0,5368	0,9382	0,7591	0,3521	0,07705	0,02568

Table 5.7: Box-Ljung test results (Gold)

Lagrange multiplier test results (Gold)						
Lag	1	5	10	15	20	30
X-squared	33,93	66,207	122,56	140,62	207,61	265,17
P-value	5,71E-09	6,30E-13	2,20E-16	2,20E-16	2,20E-16	2,20E-16

Table 5.8: Lagrange multiplier test results (Gold)

The daily log-return distribution of the spot price of Gold has a leptokurtotic distribution with a kurtosis of 7,38 and is moderately skewed to the left with a negative skewness of -0,64.

	Number of observations	Mean	Standard deviation	Kurtosis	Skewness
Gold	1844	4,8E-05	0,010119	7,384554	-0,64898

Table 5.9 Descriptive statistics Gold

5.5. GARCH and eGARCH results

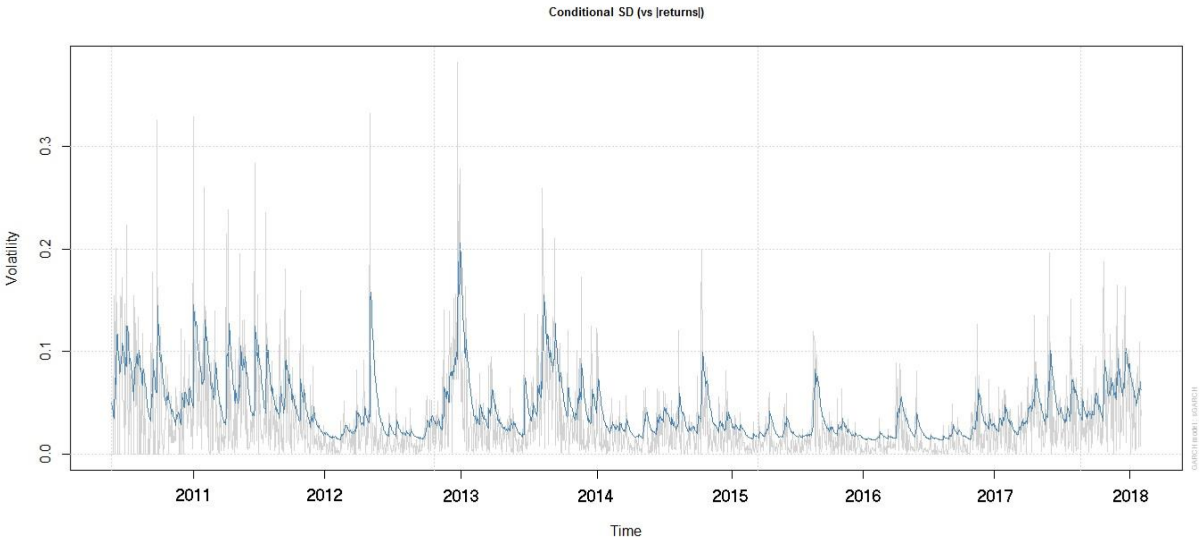

Figure 5.4: Standard GARCH, normal error distribution (Bitcoin)

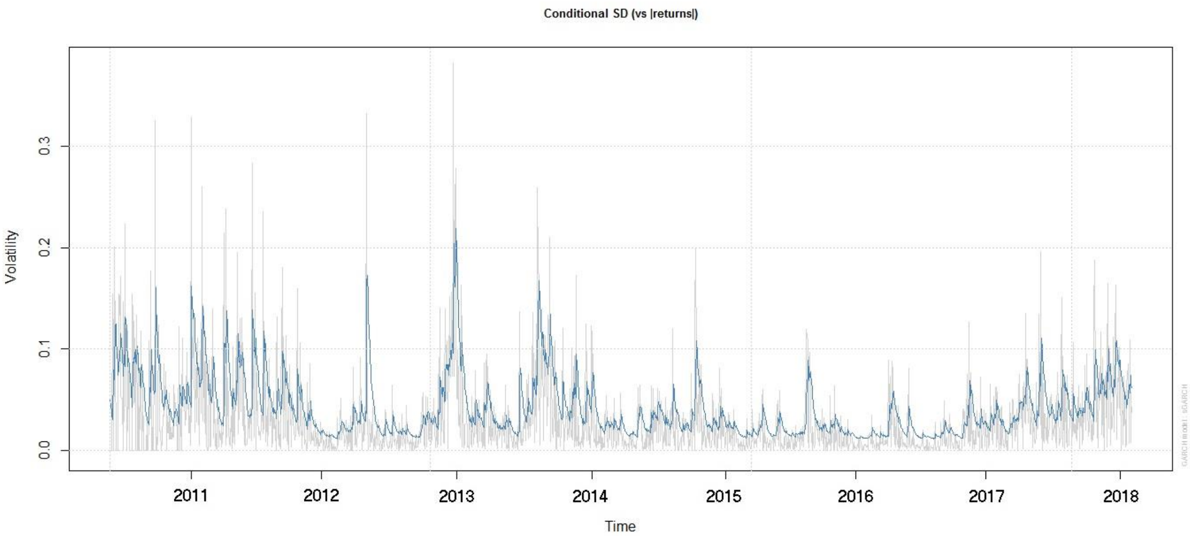

Figure 5.5: Standard GARCH, student-t error distribution (Bitcoin)

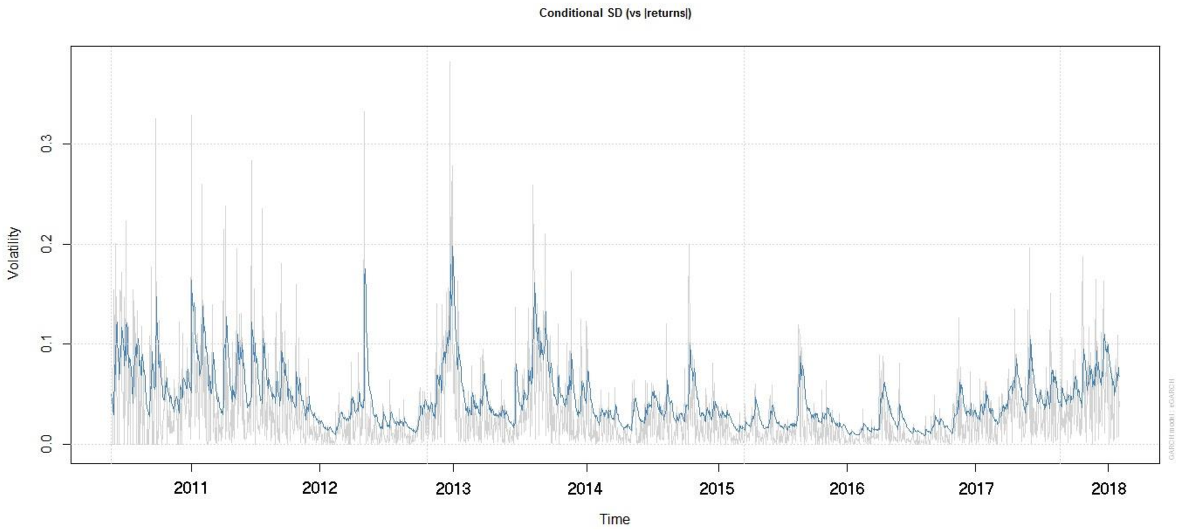

Figure 5.6: eGARCH, normal error distribution (Bitcoin)

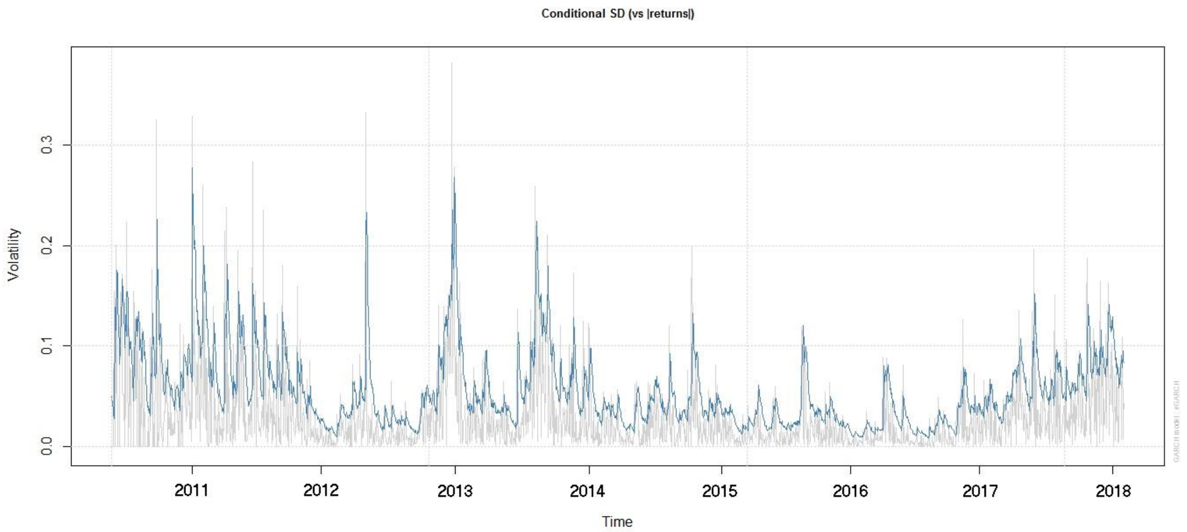

Figure 5.7: eGARCH, student-t error distribution (Bitcoin)

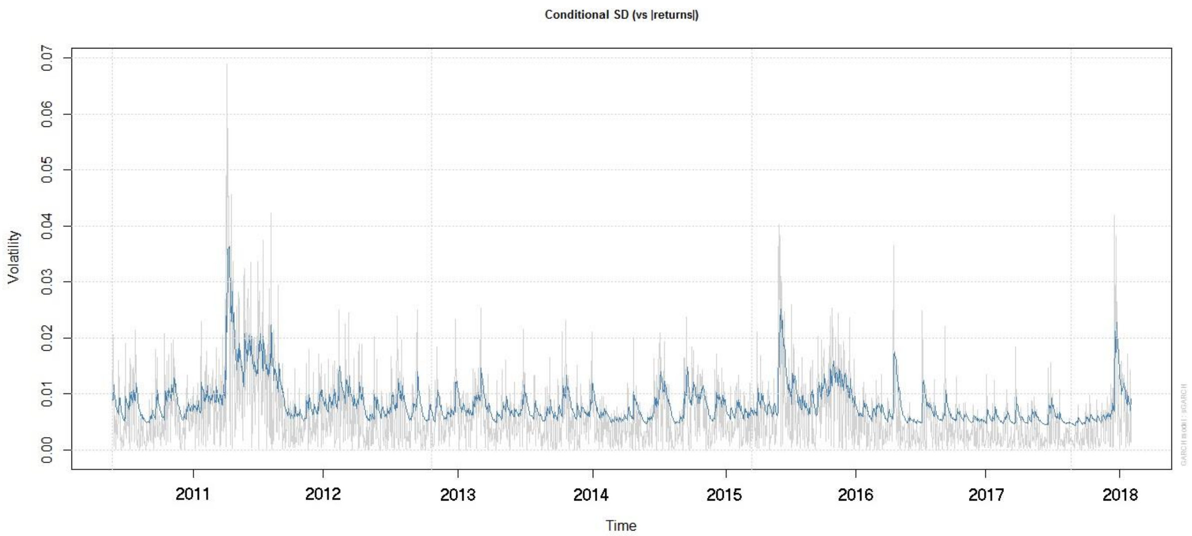

Figure 5.8: Standard GARCH, normal error distribution (S&P500)

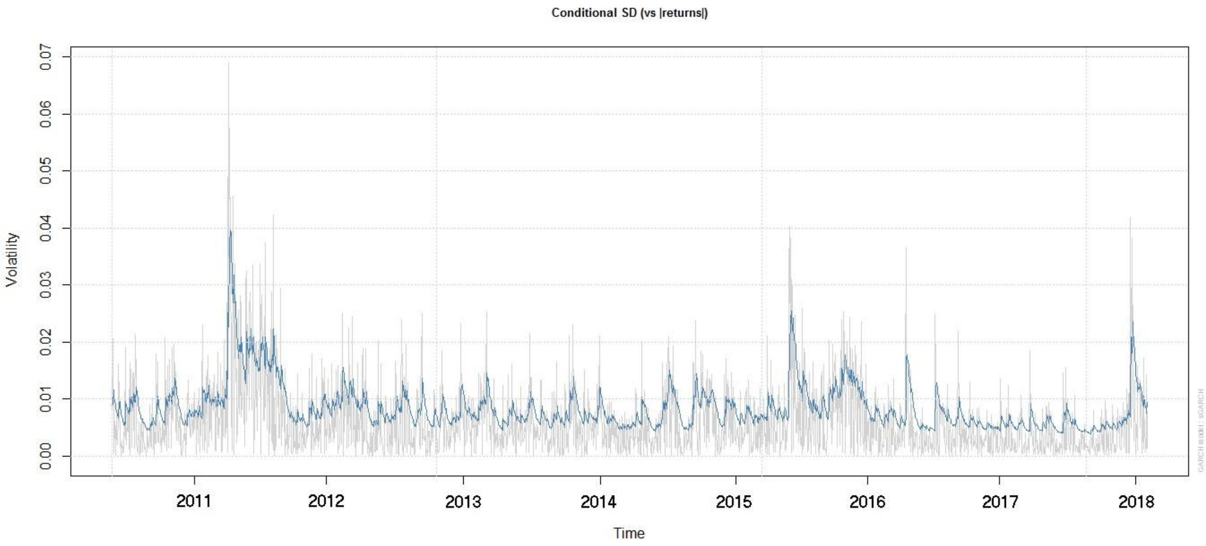

Figure 5.9: Standard GARCH, student-t error distribution (S&P500)

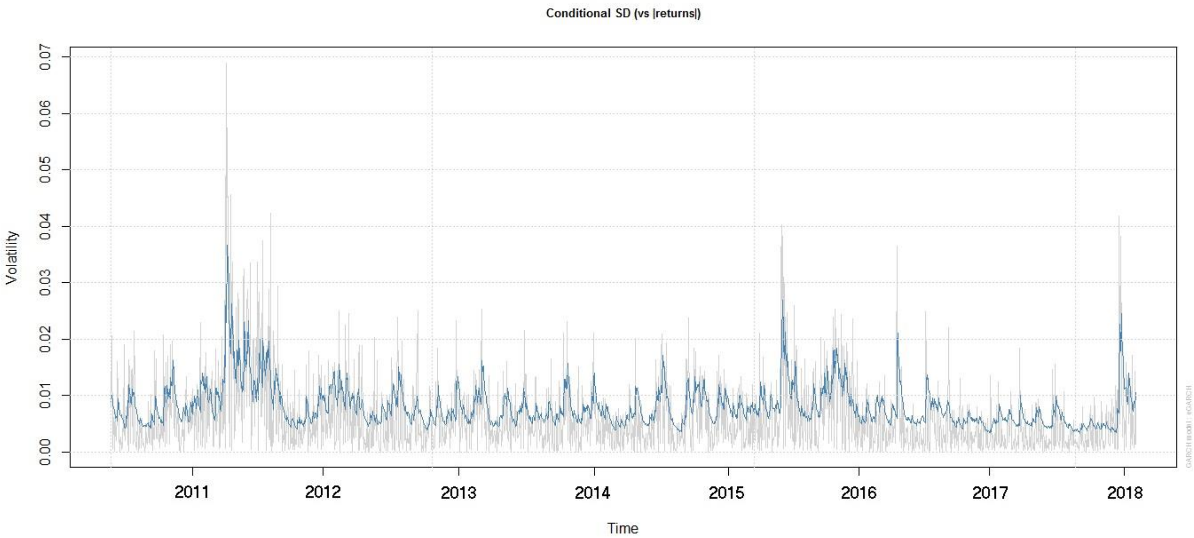

Figure 5.10: eGARCH, normal error distribution (S&P500)

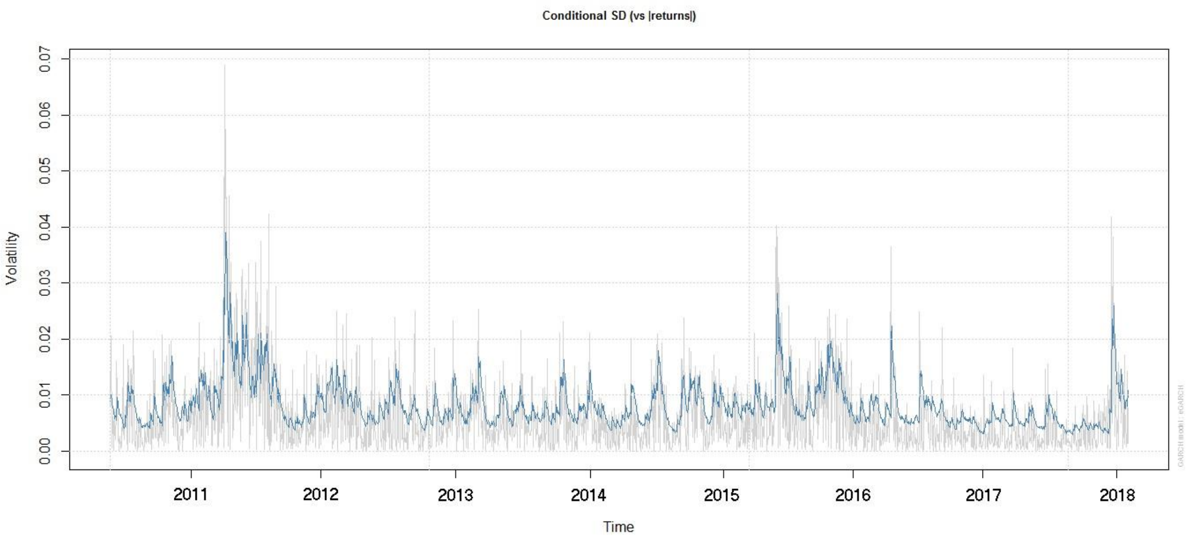

Figure 5.11: eGARCH, student-t error distribution (S&P500)

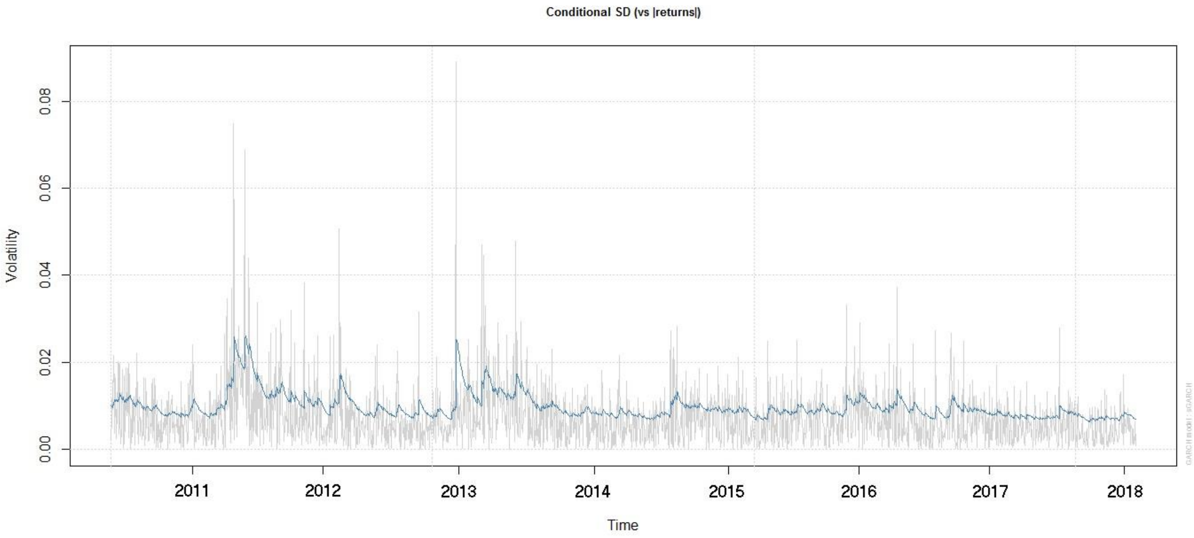

Figure 5.12: Standard GARCH, normal error distribution (Gold)

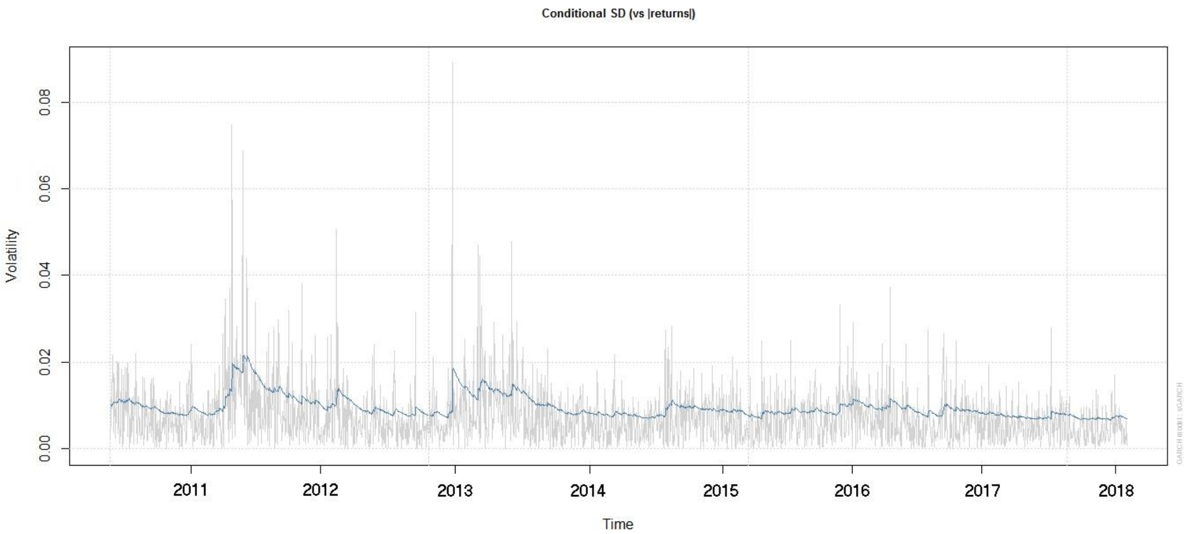

Figure 5.13: Standard GARCH, student-t error distributions (Gold)

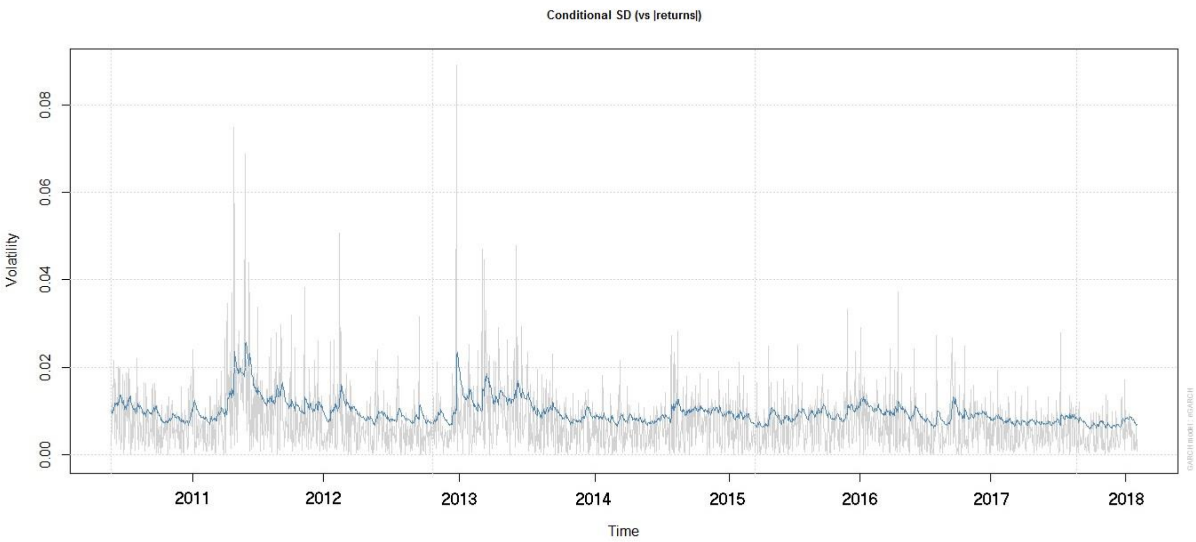

Figure 5.14. eGARCH, normal error distribution (Gold)

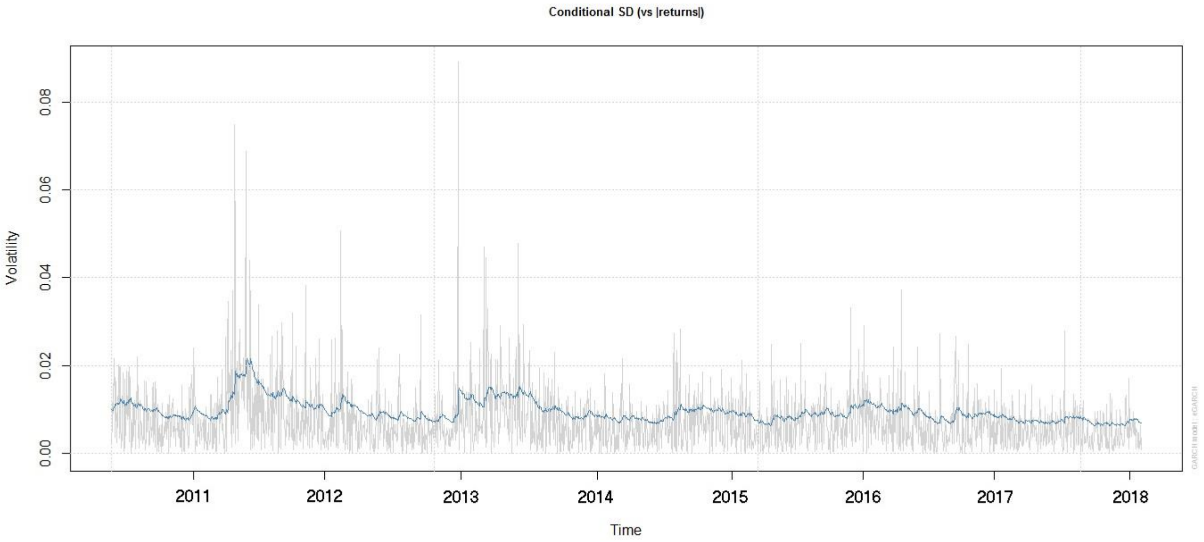

Figure 5.15: eGARCH, student-t error distribution (Gold)

Type of model	Bitcoin	S&P500	Gold
Standard GARCH with normally distributed errors	-3,6706	-6,8892	-6,475
Standard GARCH with student-t distributed errors	-3,9431	-6,9518	**-6,5545**
eGARCH model with normally distributed errors	-3,7141	-6,944	-6,478
eGARCH model with student-t distributed errors	**-3,9697**	**-6,9949**	-6,5522

Table 5.10: Akaike information criteria (AIC) for different models/assets

Figure 5.4-5.15 display the results from the standard GARCH and the eGARCH models both with the normal distribution and with the distribution. In table 5.10 the Akaike Information Criteria results reveal which of the models are best suited to describe the volatility present in each of the assets. The best fitted result is written in bold text. As we see in table 5.10 the best fitted model for both Bitcoin and S&P500 is the eGARCH model with a student-t distribution. This makes the eGARCH models ability to capture the nature of both Bitcoin and S&P500 weighted on its simplicity the most suited model for our purpose. The fact that the student-t distribution has a higher fit than the normal distribution is as expected when observing the kurtosis of the series. The eGARCH also outperforms the GARCH model, implying that a leverage effect is likely present in the series. In the case of Gold, the student-t distributed GARCH model has the lowest AIC value, indicating that in the time series of gold the leverage effect is lower or non-existing.

5.6. Correlation

To investigate if it is possible to reduce risk or improve returns in a portfolio using Bitcoin we examine the correlation between our three assets. We have used a rolling correlation window of one year and plotted the result. As one can see in figure 5.16 the correlation between Bitcoin and gold and Bitcoin and S&P500 does not seem any less stable than that of S&P500 and gold. All three combinations yield a fairly low correlation mostly in the range of -0,2 to 0,2.

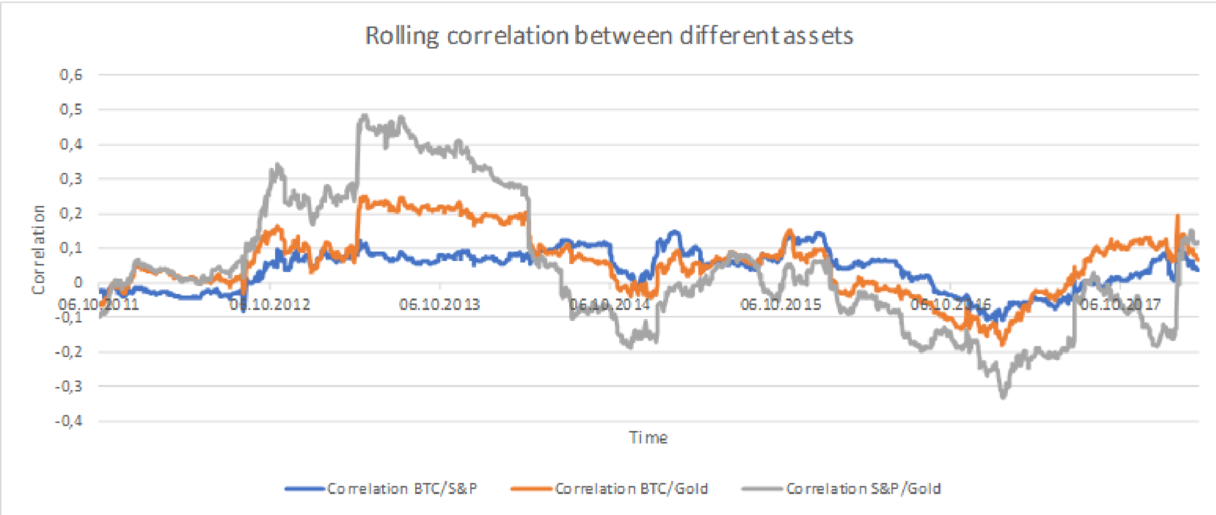

Figure 5.16: Correlation between the examined assets.

6. Discussion

In this section we intend to summarize our results and key findings and interpret them in an effort to answer the questions presented in the thesis. This will both be questions about the classification and future of Bitcoin, and an attempt to uncover the possibilities of Bitcoin as a financial asset.

6.1. Properties and value of Bitcoin

When we first started reading about Bitcoin, we started asking ourselves why Bitcoin gained a positive value in the first place. This was a hard question to answer, because it is difficult to find unbiased information and research about Bitcoin. Bitcoin is a new concept, and there are serious obstacles standing in the way of Bitcoin as a currency for daily use. The lack of user-friendliness makes it difficult for regular people to get involved in Bitcoin transactions, and the lack of a safety net can make mistakes costly. There are also currently very few establishments that accepts Bitcoin as payment. This combined with the extreme volatility of Bitcoin currently makes Bitcoin unsuitable for storing value and use on a day-to-day basis.

Though there obviously are big downsides with cryptocurrencies there are some aspects of Bitcoin that makes it a viable option for some groups of people, and we believe this justifies Bitcoin gaining a positive value. Perhaps the most important property of Bitcoin is that the use of cryptocurrencies lowers transaction costs when transferring money across international borders, as argued by Jenssen, (2014).

Some of the properties of Bitcoin mentioned in chapter 2 makes Bitcoin a revolutionary mean of payment. It is the first currency that is digital and completely independent of any third party, something that makes Bitcoin a very viable option for people living in countries without functional central banking. The security and safety offered by Bitcoin is similar to that of cash, and the anonymity of the currency is a possible way to maintain privacy in societies that are moving away from cash, in addition to being nearly impossible to counterfeit. Bitcoin also offers reduced costs when transferring funds across borders, seeing that there are no geographical limitations to Bitcoin. Without the need of an external third part in the transaction Bitcoin can be transferred across international borders independent of the regulations and transfer fees between the countries and it can be done independently of the working hours of the people who traditionally conduct monetary transactions. This allows for a more efficient value exchanging system than what exists today. Another feature of Bitcoin that separates it from traditional currencies is the privacy offered. This may be both a positive and a negative aspect of Bitcoin. In a digital society with enhanced opportunities of intense surveillance, privacy is a privilege that many people strive to achieve. A downside of the privacy incorporated in Bitcoin is the illegal activities it may support. Criminal activities are of no desire in a community and represents a cost to society. The fact that Bitcoin may be, and has been, used to finance criminal activities without leaving a digital trail is a downside of Bitcoin. However, this negative aspect of the currency may contribute to stabilizing the price of Bitcoin as it makes it, for better or worse, a desirable asset in certain communities.

Valuating Bitcoin in the traditional way of using DCF would be a very challenging task. As mentioned in chapter 3.3, while discussing equation 3.1, the value V of an asset is extremely sensitive to the expected cash flow, c. In the case of Bitcoin, the extreme volatility imposes a big challenge when finding an expected value for c. News regarding the future of Bitcoin will influence investors expectations, and thus change the value V. This may be the cause of much of the volatility. Determining the expected growth rate is probably equally difficult, and investors should be using a high discount rate to compensate for the immense risk of investing in Bitcoin.

The result from the ACF analysis (Figure 5.1) of Bitcoin implies that the Bitcoin market is not very efficient. According to EMH, it should not be possible to forecast future prices based on historical data. The number of significant lags showed by not only Bitcoin, but also S&P500 and gold is in violation with this principle. Though all three assets show conflict with EMH, judging by the Box-Ljung and Lagrange multiplier test results (Table 5.1 – 5.8), which shows very low p-values for Bitcoin, Bitcoin may be the least efficient asset.

6.2. Digital commodity money

It can be argued that Bitcoin is a digital commodity money (Jenssen, 2014, p. 51). Bitcoin share some properties with other commodity money like gold, and like other commodities, its price is set by supply and demand. One of the advantages that gold possesses over other commodity money is that it is relatively easy to store large amounts of it because of its dense value. Bitcoin is even easier to store because any amount of Bitcoin can be stored on a piece of paper by writing down the public/private key pair. It is also nearly impossible for a third party or an attacker to destabilize the supply of Bitcoin, and it should thus theoretically be able to keep its value.

6.3. Volatility analysis

As discussed in chapter 5, Bitcoin exhibits an extreme volatility compared to the other assets. This is not surprising, but also interesting. Bitcoin is a relatively new concept and is built on the emerging blockchain technology. Previous research on the volatility of Bitcoin is very scarce, but as argued by Meland and Øyen (2017), there seems to be a significant relationship between price shocks and news regarding Bitcoin. This research also found a significant negative relationship between the volume of Bitcoin traded and the price. This is consistent with the results from our eGARCH analysis of Bitcoin which shows that leverage effect is present in the dataset. When examining the historical price of Bitcoin and comparing the traits of Bitcoin with that of previously experienced bubbles we see some clear similarities. Bubbles are as mentioned often based on speculation about future prices which lead to extreme volatility measures. The downward trend exhibited towards the end of 2017 in our data set may explain some of the increased volatility in the same period due to the leverage effect. When prices go down, people become more impulsive in their buying and selling habits. This again increases volatility. EMH states that all relevant information about an asset will be reflected in the asset price. Given that Bitcoin is a new concept surrounded by a lot of speculations regarding regulations and legality, the extreme volatility can be explained by the market constantly trying to adjust the price of Bitcoin to the expected future price based on todays information. When new information is released everyday alternating between predicting the death and the mass adoption of Bitcoin, one can understand why Bitcoin appears to be so volatile.

6.4. Comparison of volatility

The three different assets we have examined in this thesis are different by nature. S&P500 is a well-known market index, and gold is often used by investors as a safe haven during financial crisis. In contrast, Bitcoin is viewed by some people as an asset that can generate cash flow, while the creator of Bitcoin created it, at least partly, as a response to the financial crisis and bank bailouts of 2008. Among investors there are both speculators and idealists, and on the sideline a lot of experts are skeptical. The volatility of the three assets in many ways reflect these differences. Gold shows the most stable volatility, but also has the lowest daily return. S&P500 has a higher daily return, but the volatility fluctuates more than gold. Bitcoin has an average daily return that is ten times higher than S&P500, but the volatility is also off the charts compared to both gold and S&P500. It is difficult to pinpoint the exact reasons why this is the case, but there are numerous factors that probably contributes to Bitcoins extreme volatility. One may be the uncertainty of Bitcoins future. If Bitcoin were to be adopted as a day-to-day currency it is not unlikely that the value of a Bitcoin would be significantly higher than todays value, given that the finite number of Bitcoins to ever be in circulation is 21 million coins. This means that any positive news regarding the legality of Bitcoin or signs of mass-adaption probably will generate positive price shocks. This may also be part of the reason why Bitcoin exhibits signs of being a bubble. One can for example look at the price rally before Christmas 2017 where the price increased by nearly 400% in about a month. This dramatic price increase resulted in a lot of media coverage of Bitcoin and may have resulted in people investing because they feared to miss out on a good opportunity to earn easy money. This is similar to what happened during the dot-com bubble of the late 90s, although this took place over a much longer time-span. In figure 5.7 one can see that the volatility of Bitcoin has been increasing the last year, and this may very well be related to the media coverage and huge price increase in this period.

In our data sets, S&P500 has a positive trend for the whole observation period, while Bitcoin fluctuates with both booms and busts. It is common knowledge that the stock market also has undergone periods of high volatility, especially during financial crisis. It would therefore be interesting to examine and compare how Bitcoin would behave in comparison to the S&P500 during a financial crisis. So far nobody has found any evidence of Bitcoin being able to act like a safe haven during financial crisis, which is one of the things Satoshi Nakamoto intended on when creating Bitcoin.

6.5. Correlation

As one can see in chapter 5.5, Bitcoins has a quite stable correlation with both gold and S&P500 compared to the correlation between S&P500 and gold. The relatively low correlation implies that people holding Bitcoin could reduce their risk by including stocks or commodities in their portfolio while still capturing some of the high returns from holding Bitcoin. This should come as no surprise given the results from the GARCH models, which portrays Bitcoin as an extremely risky asset.

7. Concluding remarks

If there is one thing that we have learned during this thesis, it is that the future of Bitcoin is very uncertain. The blockchain technology behind Bitcoin so far seems to be very secure and reliable, but as a currency there are still major obstacles to climb for Bitcoin. In the eyes of the authors Bitcoin should not be viewed as a potential substitute for the monetary systems in use today, but rather as a supplement, and be judged accordingly. Bitcoins very nature makes it a good transaction medium for exchanges over the internet and across borders, something that may prove to reduce the cost of transferring value. In countries that lack a functional banking system or suffer from major inflation like Venezuela and Zimbabwe, Bitcoin may offer a viable alternative for people who wants to keep their purchasing power. It is also in these countries we believe Bitcoin and other cryptocurrencies have the largest potential. In the western world Bitcoin must compete against a sophisticated and well-tried monetary system. As mentioned several times in this thesis there are many drawbacks to Bitcoin, the most important ones being a lack safety net, limited legislation and a lack of user-friendliness. The opinion of the authors is that Bitcoin is not yet able to compete with traditional fiat currencies when it comes to daily use.

The other aim of this thesis was to investigate whether Bitcoin had matured as a financial asset. Judging by the results from the GARCH models, Bitcoin has not yet matured. The volatility of Bitcoin was more extreme in the first years of our sample period, and showed a declining trend, but during 2017 the volatility increased, and this increase has continued until the end of our sample period. Bitcoin is still very volatile, implying an immature market.

Bitcoin exhibits signs of being a bubble, and much of the price rally seems to be fueled by speculation and hype, rather than the underlying value of Bitcoin. As seen before during the dot-com bubble of the late 90's investments based solemnly on speculations may cause extreme and irrational price increases. However, as shown by example of Google and Amazon, the fact that an asset is acting like a bubble does not mean that it doesn't have any value. Once the speculative period of Bitcoin ends and a clearer picture of what Bitcoin has to offer is brought to light, we may see a justified increase, or at least stability, in the value of Bitcoin.

Bitcoin shows a quite stable correlation with both S&P500 and gold. This could be used to research risk reduction for Bitcoin investors. This would require further research outside of the scope of this thesis.

The conclusion for this thesis is that Bitcoin has not yet matured as a financial asset.

8. Referals

Acheson, N. (2018). *How Bitcoin mining works*. Retrieved from https://www.coindesk.com/information/how-bitcoin-mining-works/

Amadeo, K. (2018, May 25th). The 2008 financial crisis. *The Balance*. Retrieved from https://www.thebalance.com/2008-financial-crisis-3305679

Black, F. (1976). *Studies of stock market changes. Proceedings of the American statistical association.* USA: American Statistical Association.

Brand, Latham, Marawanyika. (2017 November 15th). Zimbabwe doesn't have its own currency and Bitcoin is surging. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2017-11-15/bitcoin-surges-in-zimbabwe-after-military-moves-to-seize-power

Brockwell, P.J. & Davis, R.A. (2009) *Time series: Theory and Methods.*

Brunnermeier, M.K & Oehmke, M. (2012) *Handbook of the economics of Finance, volume 2.* USA

Coinpupil. (2017). *What's SHA-256?* Retrieved from https://coinpupil.com/altcoins/whats-sha-256/

Fisher, T. (2018). *Cryptographic hash function*. Retrieved from https://www.lifewire.com/cryptographic-hash-function-2625832

Goodman, P. (2008, July 20th). Too big to fail? *New York Times.* Retrieved from https://www.nytimes.com/2008/07/20/weekinreview/20goodman.html

Jeffries, A. (2018, March 22nd) Inside the bizarre upside-down bankruptcy of Mt. Gox. *The Verge.* Retrieved from https://www.theverge.com/2018/3/22/17151430/bankruptcy-mt-gox-liabilities-bitcoin

Jenssen, T.B. (2014). *Why Bitcoins have value, and why governments are skeptical.* (Master's thesis). Oslo | University of Oslo.

IBM knowledge center. (2018). *Symmetric cryptography.* Retrieved from https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7symm.html

Lasn, I. (2017). *The ultimate guide to understanding the basics of blockchain and cryptocurrencies*. Retrieved from https://hackernoon.com/the-ultimate-guide-to-understanding-blockchain-and-cryptocurrencies-f37cf4c0043

Liu, L.M. & Hudak, G.B. (1994) *Forecasting and time series analysis using the sca statistical system.* Chicago | Scientific Computing Associates Corp.

Malkiel, B.G. (2003). The Efficient Market Hypothesis and its critics. *Journal of Economic perspective, 2003(1).* Pages 59-82.

Marr, B. (2017, December 6th). A short story of Bitcoin and crypto currency everyone should read. *Forbes magazine*. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#43ccb80f3f27

Maverick, J.B. (2015) *What are the differences between weak, strong and semi-strong versions of the Efficient Market Hypothesis?* Retrieved from https://www.investopedia.com/ask/answers/032615/what-are-differences-between-weak-strong-and-semistrong-versions-efficient-market-hypothesis.asp

Meland, M. & Øyen, V. (2017). *Explaining Bitcoins Price Fluctations.* (Master's thesis). Trondheim | NTNU.

Misamore, B. (2018, April 3rd). How Amazon survived the Dot-com bubble [blog post]. Retrieved from https://hbx.hbs.edu/blog/post/how-amazon-survived-the-dot-com-bubble

Nocera, J. (2009, June 5th). Poking Holes in a Theory on Markets. *New York Times.* Retrieved from https://www.nytimes.com/2009/06/06/business/06nocera.html

Pacia, C. (2013) Bitcoin mining explained like you're five part 2 – Mechanics [blog]. Retrieved from https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/

Pacia, C. (2013) Bitcoin mining explained like you're five part 1 – incentives [blog]. Retrieved from https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-1-incentives/

Pankratz, A. (1983). *Forecasting with univariate Box-Jenkins Models: Concepts and cases.* John Wiley & Sons, Inc.

Read, C. (2013) *The Efficient Market Hypothesis.* United Kingdom | Palgrave Macmillan UK

Reid, D. (2018, February 6th). Bitcoin savaged by BIS as 'a bubble, Ponzi scheme and an environmental disaster'. *CNBC*. Retrieved from https://www.cnbc.com/2018/02/06/bitcoin-and-cryptocurrencies-are-ponzi-bubbles-says-bis.html

Seth, S. (2018). *Bitcoin's most profitable use: the $600 billion overseas remittance business?* Retrieved from https://www.investopedia.com/tech/bitcoins-best-use-isnt-currency-its-overseas-remittances/

Simkovic, M. (2016). *The evolution of valuation in bankruptcy.* Retrieved from https://www.valuewalk.com/2016/07/the-evolution-of-valuation-in-bankruptcy/

Skvorc, B. (2017). *Is Bitcoin finite or is it just a myth?* Retrieved from https://bitfalls.com/2017/09/17/bitcoin-finite-just-myth/

Smith, K. (2012) *History of the Dot-com bubble burst and how to avoid another.* Retrieved from https://www.moneycrashers.com/dot-com-bubble-burst/

Stoltz, G. (2018). Inflasjon. *Store Norske Leksikon.* Hentet fra https://snl.no/inflasjon

Sørensen, B. (2012). *Short introduction to time series*. Houston: University of Houston.

Thiesson, B., Chickering, M.D., Heckerman, D. & Meek, C. (2004). *ARMA Time-Series modeling with graphical models.* Retrieved from https://arxiv.org/ftp/arxiv/papers/1207/1207.4162.pdf

Tsay, R.S. (2002). *Analysis of Financial Time Series, 3rd edition*. USA | John Wiley & Sons inc.

Voge, C. (2018, March 22nd). Where could Bitcoin succeed as a currency? In a failed state. *Wired*. Retrieved from https://www.wired.com/story/where-could-bitcoin-succeed-as-a-currency-in-a-failed-state/

Ytterstad, M. (2017, May 22nd) "Bitcoin Pizza day". *Dagbladet.* Retrieved from https://www.dagbladet.no/nyheter/i-2010-kjopte-han-disse-to-pizzaene-i-dag-hadde-regninga-kommet-pa-182-millioner-kroner/67618949

Zuobir, L. (2017, October 31st). *A Brief history of times series.* Retrieved from https://www.statistics.su.se/english/research/time-series-analysis/a-brief-history-of-time-series-analysis-1.259451

Appendix

```
> setwd("C:/Users/Andreas/Documents/Masteroppgave")
> df<-read.csv("AlleTre.csv", header = TRUE)
> attach(df)
> library(rugarch)
Loading required package: parallel

Attaching package: 'rugarch'

The following object is masked from 'package:stats':

    sigma

> library(tseries)

    'tseries' version: 0.10-44

    'tseries' is a package for time series analysis and computational finance.

    See 'library(help="tseries")' for details.

> Box.test(LogB,type="Ljung",lag=5)

        Box-Ljung test

data:  LogB
X-squared = 56.594, df = 5, p-value = 6.131e-11

> Box.test(LogB,type="Ljung",lag=1)

        Box-Ljung test

data:  LogB
X-squared = 36.953, df = 1, p-value = 1.21e-09

> Box.test(LogB,type="Ljung",lag=10)

        Box-Ljung test

data:  LogB
X-squared = 64.927, df = 10, p-value = 4.187e-10

> Box.test(LogB,type="Ljung",lag=15)

        Box-Ljung test
```

```
data:  LogB
X-squared = 83.701, df = 15, p-value = 1.461e-11

> Box.test(LogB,type="Ljung",lag=20)

	Box-Ljung test

data:  LogB
X-squared = 106.91, df = 20, p-value = 7.172e-14

> Box.test(LogB,type="Ljung",lag=30)

	Box-Ljung test

data:  LogB
X-squared = 119.14, df = 30, p-value = 1.421e-12

> Box.test(LogSP,type="Ljung",lag=1)

	Box-Ljung test

data:  LogSP
X-squared = 5.7507, df = 1, p-value = 0.01648

> Box.test(LogSP,type="Ljung",lag=5)

	Box-Ljung test

data:  LogSP
X-squared = 31.199, df = 5, p-value = 8.559e-06

> Box.test(LogSP,type="Ljung",lag=10)

	Box-Ljung test

data:  LogSP
X-squared = 33.332, df = 10, p-value = 0.0002395

> Box.test(LogSP,type="Ljung",lag=15)

	Box-Ljung test

data:  LogSP
X-squared = 39.876, df = 15, p-value = 0.0004735

> Box.test(LogSP,type="Ljung",lag=20)

	Box-Ljung test
```

```
data:  LogSP
X-squared = 53.057, df = 20, p-value = 7.971e-05

> Box.test(LogSP,type="Ljung",lag=30)

	Box-Ljung test

data:  LogSP
X-squared = 71.127, df = 30, p-value = 3.425e-05

> Box.test(LogG,type="Ljung",lag=1)

	Box-Ljung test

data:  LogG
X-squared = 0.38147, df = 1, p-value = 0.5368

> Box.test(LogG,type="Ljung",lag=5)

	Box-Ljung test

data:  LogG
X-squared = 1.2682, df = 5, p-value = 0.9382

> Box.test(LogG,type="Ljung",lag=10)

	Box-Ljung test

data:  LogG
X-squared = 6.6387, df = 10, p-value = 0.7591

> Box.test(LogG,type="Ljung",lag=15)

	Box-Ljung test

data:  LogG
X-squared = 16.461, df = 15, p-value = 0.3521

> Box.test(LogG,type="Ljung",lag=20)

	Box-Ljung test

data:  LogG
X-squared = 29.575, df = 20, p-value = 0.07705

> Box.test(LogG,type="Ljung",lag=30)
```

```
	Box-Ljung test

data:  LogG
X-squared = 46.706, df = 30, p-value = 0.02658

> bt=LogB-mean(LogB)
> st=LogSP-mean(LogSP)
> gt=LogG-mean(LogG)
> Box.test(bt^2,type="Ljung",lag=1)

	Box-Ljung test

data:  bt^2
X-squared = 96.816, df = 1, p-value < 2.2e-16

> Box.test(bt^2,type="Ljung",lag=5)

	Box-Ljung test

data:  bt^2
X-squared = 257.44, df = 5, p-value < 2.2e-16

> Box.test(bt^2,type="Ljung",lag=10)

	Box-Ljung test

data:  bt^2
X-squared = 328.08, df = 10, p-value < 2.2e-16

> Box.test(bt^2,type="Ljung",lag=15)

	Box-Ljung test

data:  bt^2
X-squared = 379.11, df = 15, p-value < 2.2e-16

> Box.test(bt^2,type="Ljung",lag=20)

	Box-Ljung test

data:  bt^2
X-squared = 444.7, df = 20, p-value < 2.2e-16

> Box.test(bt^2,type="Ljung",lag=30)

	Box-Ljung test

data:  bt^2
```

```
X-squared = 484.62, df = 30, p-value < 2.2e-16

> Box.test(st^2,type="Ljung",lag=1)

        Box-Ljung test

data:  st^2
X-squared = 155.63, df = 1, p-value < 2.2e-16

> Box.test(st^2,type="Ljung",lag=5)

        Box-Ljung test

data:  st^2
X-squared = 809.78, df = 5, p-value < 2.2e-16

> Box.test(st^2,type="Ljung",lag=10)

        Box-Ljung test

data:  st^2
X-squared = 1067, df = 10, p-value < 2.2e-16

> Box.test(st^2,type="Ljung",lag=15)

        Box-Ljung test

data:  st^2
X-squared = 1162.5, df = 15, p-value < 2.2e-16

> Box.test(st^2,type="Ljung",lag=20)

        Box-Ljung test

data:  st^2
X-squared = 1264.9, df = 20, p-value < 2.2e-16

> Box.test(st^2,type="Ljung",lag=30)

        Box-Ljung test

data:  st^2
X-squared = 1443.6, df = 30, p-value < 2.2e-16

> Box.test(gt^2,type="Ljung",lag=1)

        Box-Ljung test
```

```
data:  gt^2
X-squared = 33.93, df = 1, p-value = 5.713e-09

> Box.test(gt^2,type="Ljung",lag=5)

	Box-Ljung test

data:  gt^2
X-squared = 66.207, df = 5, p-value = 6.295e-13

> Box.test(gt^2,type="Ljung",lag=10)

	Box-Ljung test

data:  gt^2
X-squared = 122.56, df = 10, p-value < 2.2e-16

> Box.test(gt^2,type="Ljung",lag=15)

	Box-Ljung test

data:  gt^2
X-squared = 140.62, df = 15, p-value < 2.2e-16

> Box.test(gt^2,type="Ljung",lag=20)

	Box-Ljung test

data:  gt^2
X-squared = 207.61, df = 20, p-value < 2.2e-16

> Box.test(gt^2,type="Ljung",lag=30)

	Box-Ljung test

data:  gt^2
X-squared = 265.17, df = 30, p-value < 2.2e-16

> b1<-
ugarchspec(variance.model=list(model="sGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="norm")
> bGarch1<-ugarchfit(spec=b1,data=LogB)
> b2<-
ugarchspec(variance.model=list(model="sGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="std")
> bGarch2<-ugarchfit(spec=b2,data=LogB)
```

```
> b3<-
ugarchspec(variance.model=list(model="eGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="norm")
> bGarch3<-ugarchfit(spec=b3,data=LogB)
> b4<-
ugarchspec(variance.model=list(model="eGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="std")
> bGarch4<-ugarchfit(spec=b4,data=LogB)
> plot(bGarch4)


> s1<-
ugarchspec(variance.model=list(model="sGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="norm")
> sGarch1<-ugarchfit(spec=s1,data=LogSP)
> s2<-
ugarchspec(variance.model=list(model="sGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="std")
> sGarch2<-ugarchfit(spec=s2,data=LogSP)
> s3<-
ugarchspec(variance.model=list(model="sGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="norm")
> s3<-
ugarchspec(variance.model=list(model="eGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="norm")
> sGarch3<-ugarchfit(spec=s3,data=LogSP)
> s4<-
ugarchspec(variance.model=list(model="eGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="std")
> sGarch4<-ugarchfit(spec=s4,data=LogSP)
> g1<-
ugarchspec(variance.model=list(model="sGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="norm")
> gGarch1<-ugarchfit(spec=g1,data=LogG)
> g2<-
ugarchspec(variance.model=list(model="sGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="std")
> gGarch2<-ugarchfit(spec=g2,data=LogG)
> g3<-
ugarchspec(variance.model=list(model="eGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="norm")
> gGarch3<-ugarchfit(spec=g3,data=LogG)
> g4<-
ugarchspec(variance.model=list(model="eGARCH",garchOrder=c(1,1)),mean.model=list(armaOrder=c(
1,1)),distribution.model="std")
```