Norwegian School of Economics
Bergen, Spring 2018

Exploration of bubble properties in cryptocurrencies

A hybrid-study with quantitative models for crash estimation supplemented with industry experts

Eirik R. Hollekim and Jonathan Raa

Supervisor: Associate Professor Tommy Stamland

Master of Science in Economics and Business Administration, Financial Economics

NORWEGIAN SCHOOL OF ECONOMICS

Abstract

We employ Supremum Augmented Dickey-Fuller (SADF), the General Supremum Augmented Dickey-Fuller (GSADF) tests and a Log Periodic Power Law (LPPL) test to Cryptocurrency Index (CRIX) price data to evaluate cryptocurrencies as a financial bubble. The tests display bubble tendencies during 2017 and into 2018. Current research within bubble analysis has not been successfully implemented for cryptocurrency price data. Our hybrid-approach with interviews supplementing the quantitative analysis reflects better the factors that determine whether or not cryptocurrencies can be labeled a bubble. The greatest challenge to determining if cryptocurrencies are in a bubble relates to the fundamental value and the, currently, inadequate estimation method for fundamental value. After assessing cryptocurrencies as money, we see that this analysis does not align cryptocurrencies as a large scale payment system. The definition and characteristics of money are complementary, and it is likely that cryptocurrencies can satisfy these terms better in the future and make up a bigger part of the financial world in the long term. However, anonymity and limited acceptability make cryptocurrencies more likely to function as a niche payment system in the near future. Furthermore, while some cryptocurrencies are superior to fiat money with respect to aspects such as transaction speed and cost, other areas seem underdeveloped. We present arguments for and against a bubble and while the arguments against a bubble are stronger and easier to defend, the arguments for a bubble prevents such a conclusion. The future development of cryptocurrencies is uncertain, resulting in predictions being proportionally inaccurate. Despite, we present our conclusion as an addition to the debate regarding cryptocurrencies being in a bubble or not.

Acknowledgements

This thesis concludes our studies at the Norwegian School of Economics (NHH). The project has been first of all interesting, but also challenging and comprehensive. The deeper understanding of cryptocurrencies in relation to financial bubbles, gained through this master thesis, has been very insightful and allowed us to view the debate from a different perspective.

We would like to thank all our interviewees for their contributions. Their expertise and insights have helped us to better understand the topic that made this thesis possible. We would also like to thank Laura Olesk for proof-reading and help in the most crucial period, at the absence of Jonathan Raa.

Finally, we would like to thank our supervisor Tommy Stamland for valuable feedback and academical advice in the research process.

Contents

List of Figures

List of Tables

1 Introduction

Having a monetary system that works efficiently is crucial, and with a fast developing society, it warrants a close look into digital money that has emerged. There have been debates about a financial bubble in the digital currency market, more specifically cryptocurrencies. Financial bubbles are complex phenomena which can be affected as well as affect other parts of society and the economy. In addition, even though this is a thesis in financial economics, its application extends to other fields as well. Financial bubbles are of interest not only to economists, but also to the political and business sector.

Trading is assumed to have happened as long as humans have lived, but ways of exchanging and the complexity has developed over the years. Today, technology facilitates payments faster than before, but such improvements also involve a certain complexity. The improved technology is not always successful and a relatively new concept, cryptocurrencies, is a topic of discussion today. The first draft of a cryptocurrency appeared in 1985, when David Chaum published the document "Security without Identification: Card Computers to make Big Brother Obsolete", outlining how a transaction system could function. Before this, International Business Machine (IBM) developed Data Encryption standard (DES) in early 1970s (Tuchman, 1997) which was the foundation for what later came to be cryptocurrencies.

Cryptocurrencies came under the spotlight on an even larger scale in 2017 as we saw major price increases for many cryptocurrencies. A label often used to describe these price increases is a "bubble". We will attempt to analyze to what extent we can label cryptocurrencies as being in a bubble, or even exhibiting bubble characteristics. To understand what a financial bubble could encompass, the latest financial crisis we experienced began in 2007 and originated from what we commonly know as the housing bubble. The housing bubble led to a banking crisis with sub-prime lending causing non-performing loans (NPL) to default and the banks unable to recoup their losses (Brueckner, Calem and Nakamura, 2012). From the banking sector, the rest of the economy was affected as banks act as financial intermediaries to various parts of the economy. In other words, a potential cryptocurrency bubble could lead to a crisis which then spreads to other parts of the economy. Therefore, this analysis extends to an audience wider than that of cryptocurrency enthusiasts.

As we will see through this master thesis, there is a lot more to financial bubbles than a steep price increase and uncertainty around fundamental value contributes to the difficulty of drawing a conclusion. Our interest in the subject comes from a curiosity of the technology that drives cryptocurrencies in an ever digitizing society. The lack of peer-reviewed articles in the field of cryptocurrencies and financial bubbles leaves us with an impression that the media attention is a based on claims rather than facts. In order to examine this, we have chosen this thesis with intention to answer our research question:

> *"To what extent can we identify cryptocurrencies as being in a bubble, historically or currently?"*

According to Sørensen and Whitta-Jacobsen (2010), the business cycle period after World War II was 57 months or a little less than 5 years. If we keep in mind the last crisis in 2008/2009, this analysis is relevant and interesting in terms of a probable future crash. The last time we saw technology increasing in value similar to what cryptocurrencies have was in 2001 when we experienced yet another crisis - an overvaluation of Internet-based companies. This led to what is commonly referred to as the Dot-com bubble. The NASDAQ-100 index high point during the Dot-com bubble was around the 4,700 level, while the low in 2002 was below the 1,200 level - a total drop of approximately 75% (Finance.yahoo.com, 2018). The total value loss after the Dot-com bubble in US dollars was 1.755 trillion (Kleinbard, 2000).

In the world of financial intermediaries, cryptocurrencies provide a global payment system not previously seen before. We will mention the details of cryptocurrencies' ability to function as a payment system later in this paper, but cryptocurrencies have developed from the existing payment system of fiat money as a proposed superior alternative. Consequentially, in order to evaluate this new proposed payment system, we must compare it to the existing system of fiat money. With regard to this, Alvseike and Iversen (2017) master thesis has provided insight related to the topic of our thesis.

After discussing fiat money, we will elaborate on the methodology of this master thesis, as well as frameworks and quantitative models. Subsequently, we take a broad approach to some of the important areas of cryptocurrencies, such as criminality and regulation, to supplement our quantitative analysis of whether or not we can identify cryptocurrencies as a financial bubble. In the discussion section towards the end of this thesis we will reflect on previous sections as well as make predictions of what to expect of cryptocurrencies in the future. Finally, we will present concluding arguments to answer our research question.

2 Money

"Loved by many, hated by more" - money is a social-economic entity that controls most of humans actions, directly or indirectly. That is why it is crucial to use money that is accepted by people and that stabilizes a society. Therefore, money has a great impact on politics and is influenced by the government distribution of its resources.

However, if we are going to evaluate cryptocurrencies as a means of payment, it warrants a look into the origin of money. The first part of this section we will shortly present how money has historically worked and the two most common methods of transacting. Lastly, we will introduce cryptocurrencies, blockchain technology and the three most popular cryptocurrencies.

2.1 Origin of Money

Before the emergence of money, individuals used to trade by barter which is defined as "Exchange (goods or services) for other goods or services without using money" by Oxford dictionary[1]. As trading goods for mutual advantage is intrinsic to the symbiotic relationship between plants, insects and animals, it would not be surprising if trading by barter is as old as humans itself. As trades became more complex, the various systems of barter developed to accommodate these demands. Eventually, the demands exceeded the role a barter could fulfill and commodities became the preferred barter item. Compared to other tradable goods, commodities were convenient and easy to store, had high value, higher durability and could easier be transported. The more of these characteristics the commodity had, the more preferred the commodity was, which eventually led to money. Money offered considerable advantages and progressively took over the role of the barter which gradually diminished. However, the barter re-emerged in extraordinary occasions because the money system was less robust and subject to breakdowns. To maintain a stable value of money, the government made sure people could exchange the money into a valuable resource, most commonly gold. Finally, the way of exchanging commodity money had some imperfections which led to fiat money, a type of money not backed by any physical quantity (Davies, 2010).

2.1.1 Commodity Money

Commodity money refers to a medium of exchange to a commodity, meaning it is backed by a physical good and is used to facilitate further trade (Kiyotaki and Wright, 1989). As the

[1] Available at: https://en.oxforddictionaries.com/definition/barter

currency is backed by a physical good such as gold, silver, and copper, it is said to have an intrinsic value equal to the value of the underlying asset. The currency has, therefore, two types of usages: it can be used for trading goods, or an alternative of trading the commodity. Historically, people have had more trust in money when there is an underlying value in the currency (Dobeck and Elliott, 2007). The main problem with commodity currency is that fluctuations in the underlying value will make the currency unstable over time and will not have the characteristic of stability, which we present in section 2.4 Characteristics of Money. Furthermore, increasing the money supply can only be done by also raising the quantity of the underlying commodity. For precious metals, this becomes a limitation. In addition, commodity money works as a break on inflation (Davies, 2010). Controversially, a stable and low inflation enhances sustainable growth and a consistent economy, which resulted in fiat money we use today (Bheemaiah, 2017).

2.1.2 Fiat Money

Fiat money is a currency used as medium of exchange but not backed by any physical good and, therefore, is without intrinsic value (Kiyotaki and Wright, 1989). Fiat money is not redeemable in any physical quantity. The value of fiat money is supported by the confidence people have in the monetary system: trust, that will be further explained in section 6.7.3 Trust. As long as everyone accepts what the currency is worth, which is influenced by the government, the monetary system will work. This means, if the government becomes unstable due to, for instance, political reasons, war or high inflation, the currency exhibits instability. Therefore, the government plays an important role in determining the value of the currency and its actions can either enhance or damage the value of the currency. Throughout history, there have been many instances of hyperinflation, which is the worst kind of inflation, when the currency can increase thousands of percentages in a matter of days or even hours. Because fiat money is sensitive to inflation, it is crucial for the government to maintain low and stable inflation. This is where inflation targeting becomes important to which we will get back to in section 6.7.2 Inflation Targeting (Dobeck and Elliott, 2007).

2.2 Money in Modern Times

This section gives a brief overview of the history of modern money. Note that the most crucial changes in the history will be mentioned, without going in dept to various countries. To begin with, most economies have utilized commodity money for a long time, mainly gold and silver (Bheemaiah, 2017). In 1870 there was a shift from bimetallism where both silver and gold were equivalent to certain quantities to only gold Oppers (1996). The British Sterling used to be the strongest currency, but in the twentieth century, more specifically after the great depression, the American Dollar took over the Sterling's place as the leading currency. This led to America creating the Bretton Woods system in 1944, where the American Dollar was convertible into gold. Most developed countries joined the system which was idealistic in regards to convertible currencies, fixed exchange rates and free trade. After a period with instability of international rates of exchange, Bretton Woods resulted in a breakdown in 1971 (Davies, 2002). The collapse from the gold standard to a currency floating freely triggered the following years to be filled with high inflation and recession. Through crisis, the world economy has adopted various ways of controlling the inflation and to influence the economic cycles (Mellor, 2010)

This system is called fiat money that we use today. The government has laws in place to make sure that the currency is a forced method of payment, ensuring that taxes are paid with the currency and that businesses accept the currency as a means of payment. This leads to demand of the currency, which helps to maintain its circulation. Each central bank has monetary instruments such as setting rates and regulating the money supply to keep the currency stable.

2.3 Definition of Money

In *The Wealth of Nations*, Adam Smith defines money by the role it plays in society and in particular how well it serves as: (Ali, Barrdear, Clews and Southgate, 2014; Bheemaiah, 2017; Halaburda, 2016*b*)

1. A medium of exchange
2. A store of value
3. A unit of account

These three functions of money make it possible to facilitate a currency and if one is missing, individuals would not accept the currency. The first function is medium of exchange, meaning that a currency needs to be a trade intermediary. In other words, in a trade, people are willing to accept the money because they trust the money will be accepted elsewhere. The second function is store of value, which essentially means that money needs to keep its value over time. The third function of money is unit of account. "It is possible to define the monetary unit [the unit of account] as one unit of a resource called currency, but this is only one of many different definitions." (White, 1984). For a currency to function as a unit of account, it must be able to be used as a medium of exchange by several people, in a variety of transactions, over time[2]. However, Halaburda (2016*b*) is critical towards the functions of unit of account and claims that it only describes an equilibrium. Furthermore, the book writes that Smith's definition is too simple and that it does not hold because a medium of exchange cannot work in *all* transactions and store of value cannot remain *forever*. Although these counterarguments point out that the definition put forward by Adam Smith is relatively broad, the roles specified by Smith should not be seen as yes or no questions as argued by Halaburda (2016*b*). Rather they should be seen as three dimensions in which, for instance, a specific currency could satisfy each one of them to a better or worse degree. Regardless, we consider Smith's definition to be valuable and, thus, we will utilize it later in this master thesis.

2.4 Characteristics of Money

Adam Smith, and other neoclassical economists, argued that medium of exchange was the primary account of the origin of money. As a barter economy relies on "double coincidence of wants", where person A had to want something from person B and vice versa, the need for a medium of exchange became apparent. To construct these trades on a large scale, some characteristics were needed (Smith, 2000; Federal Reserve Bank of St. Louis, 2018). The six characteristics of money are listed below:

1. Durability: Can be used over and over again and can survive in long periods.
2. Portability: People can easily take money with them.
3. Divisibility: Money can be divided into smaller denominations or units of value.
4. Stability: Money must be stable in value.
5. Scarcity: Money must be available only in limited quantities.
6. Acceptability: Everyone must be able to exchange the money for goods and services.

2.5 Cryptocurrencies

The emergence of cryptocurrencies started in the aftermath of financial crisis 2007-2008. This crisis caused a debate about the conventional view of money and its capitalistic system, in particular the roles of banks and financial institutions. The result was a new way of conducting transactions, challenging the profit-driven market economy, while being socially

[2]Further explanation of the three functions of money available at: https://ssrn.com/abstract=2499418

administered for the benefit of the rest of society as a public resource. The timing of Bitcoin surfacing in 2009 was not a coincidence, but rather a consequence of the financial crisis (Halaburda, 2016*a*). It was a modest beginning for Bitcoin where a small group of enthusiasts of the financial world discussed the new technology. In 2014, Bitcoin documentaries surfaced and in 2015 blockchain conferences emerged. The following year 2016, books about blockchain were published and, thus, the popularity around Bitcoin and blockchain increased together with the Bitcoin price (Bheemaiah, 2017). However, the success of Bitcoin gave rise to a variety of new digital currencies and today 1640 cryptocurrencies are listed on CoinMarketCap, a website tracking the price data of these cryptocurrencies (CoinMarketCap, 2018).

Cryptocurrencies is a broad topic with many categories. Although we attempt to address cryptocurrencies collectively, we recognize there are differences between cryptocurrencies which limits such an analysis. In terms of classification of the types of cryptocurrencies, we separate cryptocurrencies into the following three categories, as suggested by an article posted on the NASDAQ homepage to show the variety within the cryptocurrency market: (Goodboy, 2018)

1. Transactional cryptocurrencies
2. Platform cryptocurrencies
3. Utility cryptocurrencies

Transactional cryptocurrencies are Bitcoin, mentioned below in section 2.7.1 Bitcoin, and all alternative cryptocurrencies, such as Litecoin, offering improvements to the Bitcoin protocols. These transactional cryptocurrencies are also called altcoins as they are alternative coins to Bitcoin. Platform cryptocurrencies are cryptocurrencies operating on a platform for application development and can include features such as smart contracting. Ethereum is an example of a platform cryptocurrency, discussed below in section 2.7.3 Ethereum. Lastly, utility cryptocurrencies are cryptocurrencies designed for a certain task. Ripple is the best example of a utility cryptocurrency as its task is to facilitate fiat money transfer as an efficient and low-cost option (Schwartz et al., 2012). Other examples of utility cryptocurrencies are crypto tokens such as TRON, which can be used to exchange for information on TRON, an information storage system based on the Ethereum platform (TRON.NETWORK, 2018)

According to the European Central Bank (ECB), cryptocurrencies do not have a legal status because it is not widely used to exchange value and hence cryptocurrencies do not have legal tender. Cryptocurrencies can, therefore, not be considered as money. However, when there is an agreement between buyer and seller in order to accept a given virtual currency as a means of payment, cryptocurrencies can be used as contractual money (ECB, 2015 as cited in Bheemaiah, 2017).

Cryptocurrencies with its blockchain technology contain features which are new to the economy. When analyzing cryptocurrencies, the scalability and transaction speed are normally emphasized as areas where some cryptocurrencies have shown limitations. Furthermore, the volatility and the correlation between cryptocurrencies are essential topics, in addition to initial coin offerings (ICOs). ICOs are a way of raising funds, where the investors receive cryptocurrencies or crypto tokens for their investment. The regulatory framework around ICOs has received criticism (Jackson, 2018*b*). All of this will be discussed later in section 6 A New Payment System.

The following Figure 1 from the International Monetary Fund (IMF) (He et al., 2016) illustrates the scope of cryptocurrencies as opposed to digital currency and virtual currencies, which are labels often confused by the general public.

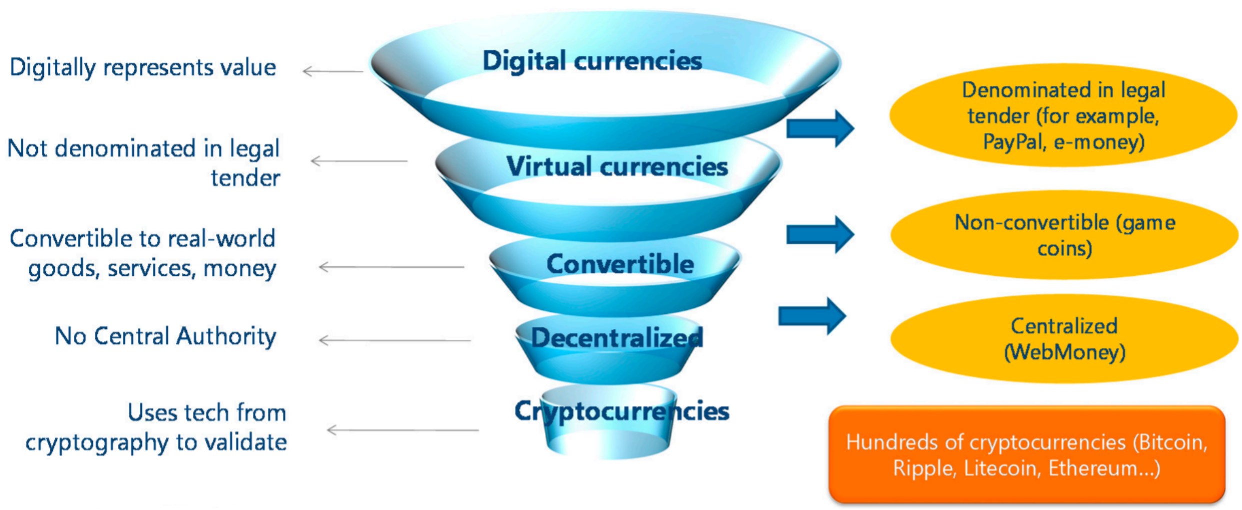


Figure 1: Scope of Digital Currency Classification (He et al., 2016)

2.6 Blockchain

Most cryptocurrencies are based on a technology called Blockchain, while other cryptocurrencies have other adoptions of a Distributed Ledger Technology (DLT) system. The name Blockchain stems from its assumed shape of being a line of connected blocks of information as shown in Figure 2 below. In this structure, each block contains records. For cryptocurrencies, this list of records are transaction records showing all transactions made with the given cryptocurrency. The green block is what is known as the genesis block. It is the first block in any Blockchain and after being programmed, its properties will define the following blocks.

The blue blocks in Figure 2 are the normal blocks that follow as the records increase and time goes by. Normally, a block can only be succeeded by one other block, but in the case of when two blocks are added at the same time, a split may occur as shown in Figure 2 with the red block. Blockchain will then discontinue one of the new chains based a criterion known as difficulty, a concept we will explain below in section 2.6.1 Block Structure (Pilkington, 2016).

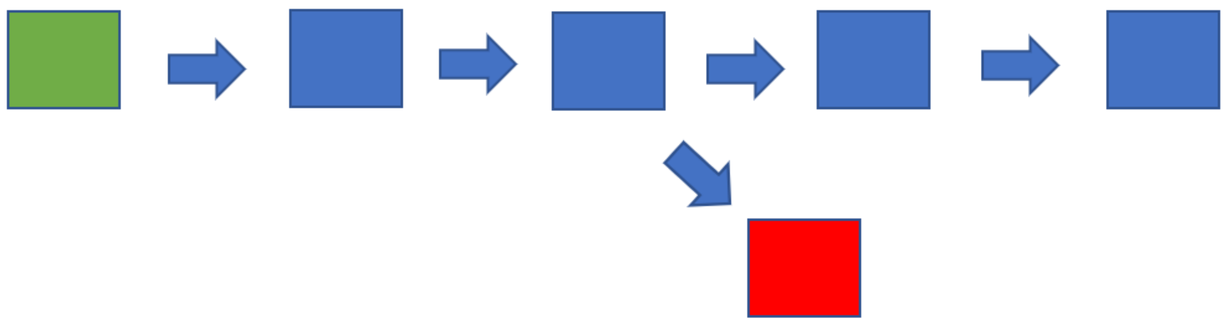


Figure 2: Blockchain Structure (Own Illustration)

Blockchain consists of several different parties. When a transaction with cryptocurrencies occur, the transaction is recorded in a public ledger. Transactions are encrypted, meaning that people cannot visibly see who are conducting the transaction, but the amounts transferred and the unique addresses of these two unknown accounts are recorded (Peters and Panayi, 2015). For this payment to be made directly, miners verify the transaction. Miners are individuals who verify transactions awaiting confirmation and add blocks to the blockchain. Miners ensure, for example, that the sender has the funds he is trying to send. In return, miners are paid in cryptocurrencies. For Bitcoin, this reward was 50 Bitcoin (BTC) per block added to the blockchain when it first launched, but every 210,000 blocks the reward is halved. In April 2018, the reward is at 12.5 BTC and this asymptotic behavior limits the total supply of Bitcoin to 21 millions. In 2040, there will be no more blocks to mine (Nakamoto, 2008).

2.6.1 Block Structure

In terms of block structure, it varies in size and composition between cryptocurrencies. Bitcoin, the most common cryptocurrency by market capitalization, has a block size cap of 1 megabyte. An illustrative figure of Bitcoin block structure can be seen in Figure 3 below. The magic number for Bitcoin blocks is an arbitrary number which is always 0xD9B4BEF9. The blocksize is the bytes number which is added at the end of the block. The transaction counter is a positive integer. The blockheader is split into six components: version, time, target, nonce, hash of previous block, and Merkle root. The version component is the block version number and is updated when the software upgrades. The time component sets a timestamp which updates every few seconds. The target component regulates the difficulty which is adjusted to keep the verification time of one block to 10 minutes. The hash of the previous block contains a 256-bit hash based on the header of the previous block, linking this block to the previous block. The Merkle root is a 256-bit hash based on all the transactions in the current block, giving this block a unique signature. The nonce is some 32-bit arbitrary number which miners are trying to guess. Once this number is correctly guessed and it fits the difficulty requirements set by the target, the block is added to the blockchain. As more miners join the network and the computing time for the difficulty level goes down, the difficulty is adjusted to make the computing time for one block close to 10 minutes. This difficulty adjusting makes mining very energy intensive as more people join the network (O'Dwyer and Malone, 2014). If two miners guess two numbers at the same time, it can result in the blockchain in two blocks as shown above in Figure 2. In this case, the blockchain will discontinue the chain with the lowest cumulative difficulty level and not necessarily the shorter chain. This ensures there is only one chain at a given point.

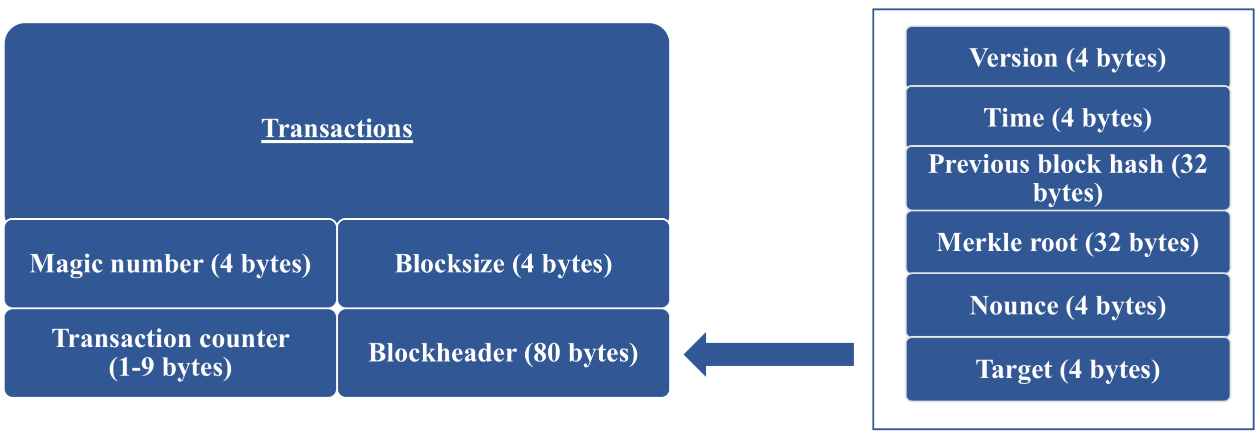


Figure 3: Block Structure (Own Illustration)

2.7 Prominent Cryptocurrencies

Because the cryptocurrency market is so vast and varied, we cannot hope to include all of them. Below are the three biggest cryptocurrencies by market cap, each with their own purpose. In many ways, these three will also represent the three areas mentioned in 2.5 Cryptocurrencies.

2.7.1 Bitcoin

Bitcoin is the largest cryptocurrency, measured by a market capitalization of $144,348,790 as of 24^{th} 2018. The price of Bitcoin has increased significantly over the past year, from

\$997.69 on 1st January 2017 to \$13,412.44 on 1st January 2018 (CoinMarketCap, 2018). Bitcoin is used as a means of payment and is said to be pseudo-anonymous (Nakamoto, 2008). The estimated transaction speed with Bitcoin is 3-7 transactions per second (Seigneur et al., 2017). The characteristics of volatility and price increase, with daily price fluctuations up to 30% during the past year (CoinDesk, 2018), have caused significant media coverage. The consensus function in Bitcoin requires 51% of the network to be in agreement for the transaction to be recorded in the Blockchain. The minimum transaction possible is one-hundredth million of a Bitcoin, or to the eight decimal place. One would require a public and a private keys to transfer Bitcoin encryption and decryption information. The public key is used for encrypting the message or transaction, and the paired private key can be used to decrypt the sent message, as shown in Figure 4 (Nakamoto, 2008). The encryption happens in the form of hashing, and as explained in section 6.6 Improvements, ensures that the information cannot be falsified.

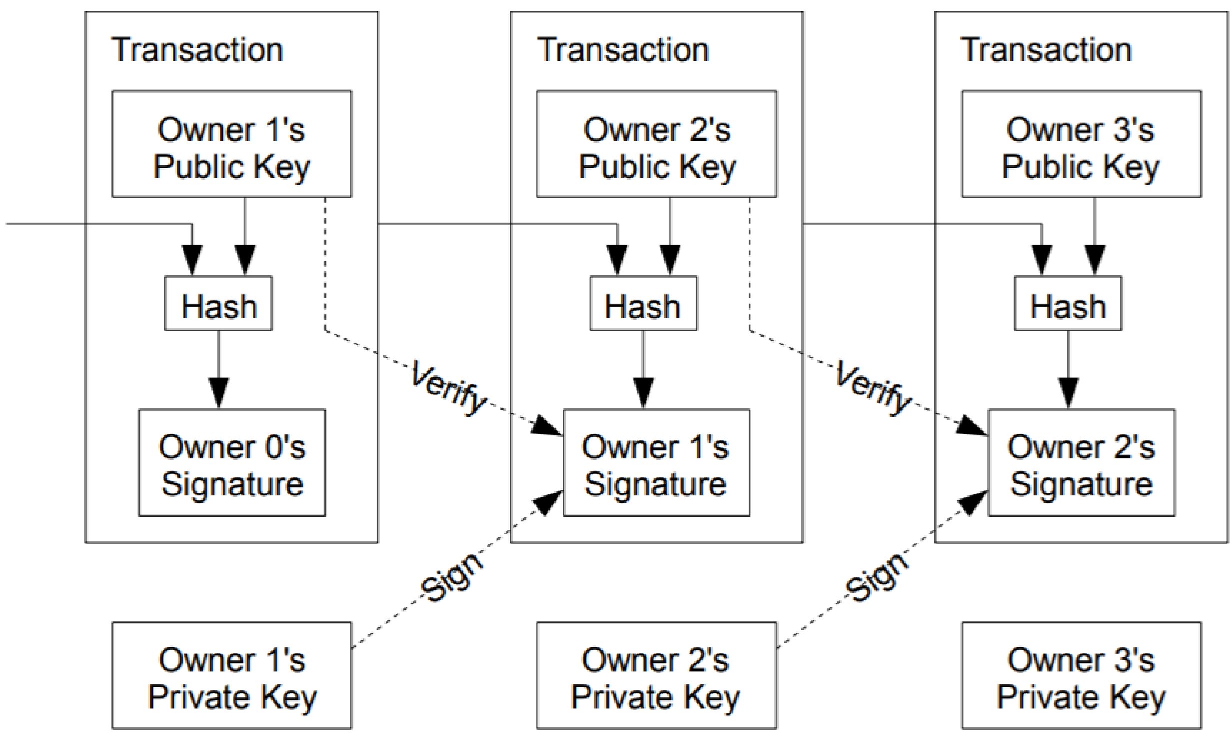


Figure 4: Bitcoin Transaction Process (Nakamoto, 2008)

2.7.2 Ripple

Ripple is a payment system that works different from Bitcoin in the way transactions are approved. The characteristics of the technology behind Bitcoin transactions is inferior to the Ripple system in terms of transaction speed and costs (Schwartz, Youngs and Britto, 2012). The price of Ripple has increased from $0.0064 per coin to $2.26 during the course of 2017 (CoinMarketCap, 2018). Ripple is divisible up to six decimal places. The consensus function in Ripple requires 80% of the network to be in agreement for the transaction to be added to the network. Figure 5 shows the relationship of traditional payments with Ripple payments and the potential of lower transaction costs. According to the Ripple website, the theoretical transaction speed is 1,500 transactions per second and can scale towards 50,000 transactions per second - significantly higher than Bitcoin and Ethereum (Larsen and McCaleb, 2018). In addition, Ripple cannot be mined and, thus, does not consume as much electricity and, therefore, provides a big improvement to Bitcoin's resource issue (Schwartz et al., 2012).

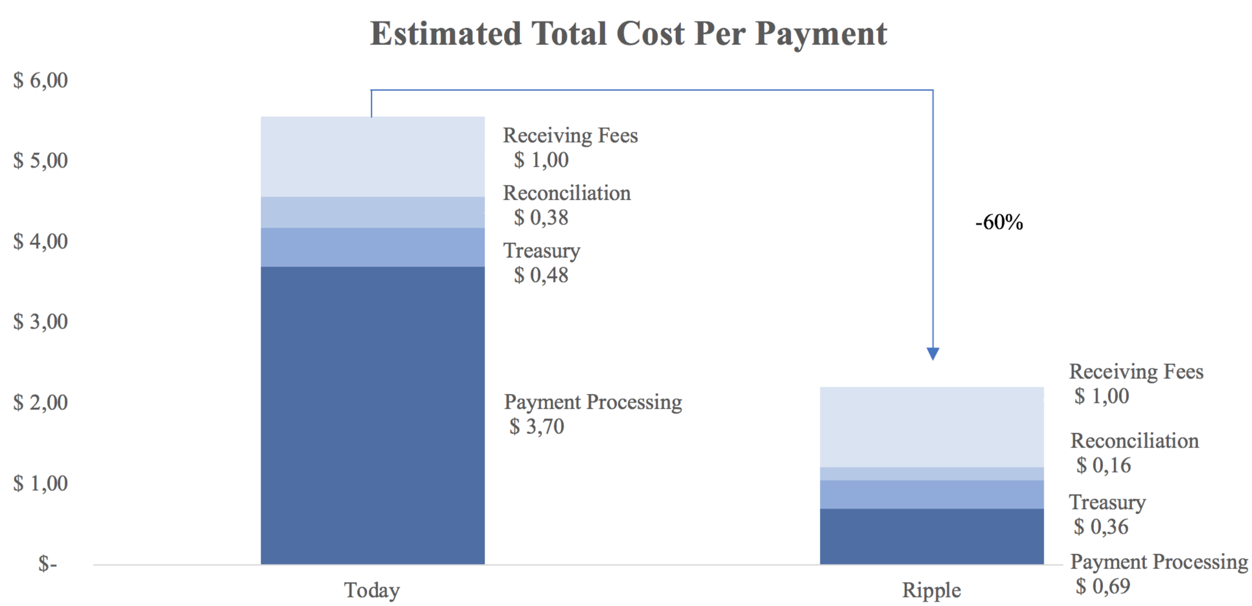


Figure 5: Ripple Transaction Cost Relative to Normal Transaction Costs (Ripple.com, 2018)

2.7.3 Ethereum

Ethereum is the blockchain platform which can be applied to virtually any transaction involving a governing or economic aspect. In other words, Ethereum works well with what is commonly known as smart contracts (Buterin, 2015). The cryptocurrency based on the Ethereum platform is known as Ether and is the second-largest cryptocurrency after Bitcoin. Ether was worth \$ 8.15 on January 1^{st}, 2017. A year later, that price amounted to \$772.33 (CoinMarketCap, 2018). Hence, the price exuberance of Ether exceed even that of Bitcoin. Ether can also be divided into one eighteenth decimal place. The popularity behind Ethereum comes from its possibilities as a smart contract platform and not Ether's utility as a cryptocurrency. It is, therefore, not correct to say that Ethereum is a pure cryptocurrency. Due to the hardcoded limitations of Ethereum, the transaction speed is limited to 10-15 transactions per second (Buterin, 2015). Ethereum uses the Proof-of-Work (PoW) consensus system, but Ethereum is in the process of converting to the Proof-of-Stake (PoS) consensus system. The PoW consensus system is the energy-consuming system Bitcoin is currently using (Buterin, 2015), which we will get back to later in section 6.6 Improvements.

3 Methodology

In this section we explain our approach to answer our research question. As a thought through methodology is a key to a good analysis, we will also outline the risks, ethical considerations as well as potential limitations and how we have dealt with these challenges in our work.

3.1 Research Design

In order to answer our research question, we have chosen a hybrid-approach. This means that the research design is mixed methods in which "the use of quantitative and qualitative data collection techniques and analytical procedures" are combined (Saunders, Lewis and Thornhill, 2015). The quantitative approach consists of a set of bubble tests, while the qualitative part encompasses mainly interviews to support our qualitative analysis. Our quantitative analysis comes first, supplemented with the qualitative interviews. This is consistent with the concurrent research design, but the data collection is separate of each other (Saunders et al., 2015). The tests used for the quantitative part are a set of the Log-Periodic Power Law (LPPL) model and different variations of the Dickey-Fuller test to test the CRIX dataset for explosive price behavior. The CRIX data will be discussed in more detail in the next section, 3.2.1 Quantitative Data. In the qualitative part of this thesis, we have chosen to conduct semi-structured interviews. This choice of semi-structured approach in interviews was made because qualitative interviews help to give the interviewees the possibility to speak freely, as well as enable the interviewer to understand the connections between attributes and ask in-depth questions if there are unclear statements (Mayring, 2016). Our analysis of bubble tests will concentrate on the price movement and estimating crash windows with a focus on historical performance in terms of CRIX data. The qualitative part will attempt to enrich the bubble analysis by looking at aspects of cryptocurrencies which can contribute for or against a bubble. The combined purpose of the study is, therefore, both exploratory for the methods of analysis. Exploratory studies are considered to be particularly useful if one wishes to clarify understanding of an issue, problem or phenomenon and if its precise nature is uncertain (Saunders et al., 2015). This seems particularly fitting for cryptocurrencies.

3.2 Data

3.2.1 Quantitative Data

For data analysis we have decided to use the CRypto-currency IndeX (CRIX) computed by the Ladislaus von Bortkiewicz Chair of Statistics at Humboldt University of Berlin, Germany. The development of this index was in joint work with SKBI at Singapore Management University. CoinGecko, a cryptocurrency data company, provides data for the computation. There are 20 index members as of February 27^{th}, 2018. All index members are weighed by market capitalization, shown in Table 1[3]. The dataset features daily prices dating back to July 31^{st}, 2014, which is the first computation day for the CRIX and the data is indexed to 1000. This constitutes a part of the secondary data used in this master thesis. Furthermore, the quantitative part of this master thesis is a longitudinal study in the sense that we follow the data over a specific time window, attempting to explore bubble properties for the test window July 31^{st}, 2014 to April 26^{th}, 2018. CRIX is checked every three months to see if the constituents in the index represents the market well. The index also includes a liquidity rule to include cryptocurrencies that are actively traded with sufficient market capitalization to effectively represent the market. CRIX does, however, only include successful cryptocurrencies and could give a distorted view of the crypto market.

Table 1 CRIX Constituents as of 24^{th} May, 2018

#	Name	Price (in $)	Market Cap (in $)	Volume (in $K)
1	Bitcoin	8473.35	144,348,790	2,586,241
2	Ethereum	703.16	69,935,482	1,318,045
3	Ripple	0.70	27,323,878	401,164
4	Bitcoin Cash	1344.61	23,032,962	727,056
5	EOS	12.93	11,101,836	1,309,939
6	Litecoin	138.83	7,850,604	330,038
7	Cardano	0.26	6,719,529	98,957
8	Stellar	0.35	6,417,881	32,750
9	TRON	0.07	4,490,948	286,447
10	NEO	63.16	4,105,271	94,806
11	Dash	428.95	3,462,824	158,759
12	Monero	203.71	3,266,499	53,514
13	NEM	0.34	3,022,826	19,294
14	VeChain	4.71	2,476,825	43,758
15	Tether	1.00	2,204,161	1,587
16	Ethereum Classic	18.11	1,841,819	237,936
17	ICON	4.01	1,550,960	102,877
18	QTUM	16.74	1,483,190	153,015
19	Binance Coin	12.56	1,432,426	35,452
20	OmiseGO	13.54	1,381,313	25,766

[3] Available at: http://crix.hu-berlin.de

3.2.2 Qualitative Data

To supplement the price analysis we have done, we have decided to collect and analyze primary data, gathered via semi-structured interviews. Prior to conducting interviews, an interview guide was carefully prepared which can be found in Appendix B: Interview Guide. As outlined by Saunders et al. (2015), semi-structured interviews encompass "a list of themes and possibly some questions to be covered, although their use may vary from interview to interview." Each interview question has been tailored to the respondent, while attempting to keep the themes and intentions of each question the same for each respondent. This means, for instance, that we ask the superintendent and the cryptographer if the price increase can be explained by criminality and increase in cryptographic protocols, respectively. Furthermore, the qualitative part of this master thesis is a cross-sectional study as we only reflect the responses of the interviewees at one particular point in time. Baker, Edwards and Doidge (2012) found that the number of appropriate interviews depends on the study. If we are aiming to find similarities among the interviewees, we should continue sampling past the saturation point (Saunders et al., 2015). If the study is to gather in new information, sampling should stop when we experience data saturation, or no new information or themes are gathered from the data sampling. Moreover, we decided to keep the interviewees anonymous to eliminate stakeholders' effect on interviewees' responses. In addition, the anonymization was used at an argument to attract more interviewees. With regards to sampling, we decided to use non-probability purposive sampling as this is the best way to select an expert sample (Tongco, 2007). Our sample of interviewees are from around the world and, thus, will be conducted using electronic communications tools as this is the most efficient way of reaching out to experts across national borders. The interviews will be transcribed as soon as possible to prevent data loss. Table 2 provides an overview of the conducted interviews, chronologically. The interviews were conducted in spring 2018.

Table 2 Overview of Interviewees

#	Title	Industry/Sector	Place	Length	Language
1	Executive	Central bank/infrastructure	Phone call	35 min	Norwegian
2	Managing director	Financial services	Phone call	45 min	English
3	Head content manager	Financial services	Call, Skype	35 min	English
4	Founder and CEO	Financial services	Call, Skype	30 min	English
5	Consultant	Financial services	Video, Skype	30 min	English
6	Professor	Academia, IT	Video, Skype	30 min	English
7	Superintendent	Law enforcement	Video, Skype	40 min	Norwegian

3.3 Statistics

In the following section, we explain the statistical steps taken in the bubble tests conducted for this master thesis. Before starting the bubble tests, we converted the data to time-series, performed analyses to test the lag, in addition to test the stationarity. Our results, in addition to Phillips, Shi and Yu (2015) showed that using the logarithmic scale was crucial to get reliable results for the ADF bubble tests. Furthermore, correlogram test displayed a lot of correlation between the days, but as stated in Pedersen and Schütte (2017) including more lag than 1 or 3 days will result in less power in the tests. Finally, after discussing what models to include, we ended up incorporating Log Periodic Power Law (LPPL) and a recursive moving window Augmented Dickey Fuller test called PWY/PSY. All of these models will be discussed in more detail in section 4 Bubble Tests. Furthermore, these models are integral to the discussion about analyzing cryptocurrencies, in addition to the suitability with the exponential data.

3.4 Research Quality

According to Saunders et al. (2015), in order to establish quality of a research project, two factors need to be in place. These factors are reliability and validity. Reliability refers to whether the results are replicable using the same procedures again. Validity is concerned with "the appropriateness of the measures used, accuracy of the analysis of the results and generalisability of the findings (Saunders et al., 2015)." In terms of reliability, by using CRIX dataset that is readily available, we make sure the study can be easily replicated. However, there are a number of threats to both reliability and validity. We acknowledge that there is selection bias present in the CRIX dataset as it only includes largest cryptocurrencies in terms of market capitalization. Selection bias may appear when a subset of the population is excluded from the sample due to the sampling process (Keller and Gaciu, 2012). Thus, as we aim to analyze cryptocurrencies collectively, the characteristics of cryptocurrencies in the CRIX dataset sample may vary from other cryptocurrencies in the crypto market. Although this threatens the validity of the results, CRIX dataset is used in this master thesis as it is the only well-documented cryptocurrency index. However, we take into account the selection bias when interpreting the results obtained via bubble tests.

In terms of reliability in the qualitative part, we attempt to minimize researcher bias or influence by formulating open-ended questions, as opposed to questions with an intent towards a certain response, so-called loaded questions (Leech, 2002). In addition, we have followed the guidelines proposed by Lincoln Yvonna and Guba (1985). This study suggests there are four criteria of trustworthiness: credibility, transferability, dependability, and confirmability.

Credibility refers to the confidence that the researcher has arrived at the truth of the finding. We attempt to take a closer look at cryptocurrencies in relation to financial bubbles, but we do not rely entirely on the models to draw definite conclusions and we are confident that there is the truth in the findings. Transferability shows that the findings can be generalized to other areas. Looking at when a bubble occurs is not just a topic for financial economics, but also other fields, such as policymaking. Dependability measures whether the findings are consistent and can be replicated. While replicating an interview is very difficult, the interviewees clearly stated their stance to the research question. To replicate the respondents general knowledge and opinion on the subject should not be an obstacle for dependability. We also utilized participant validation for the qualitative part, which allows the participants to confirm the accuracy of the data. Lastly, confirmability means the level of which the findings are based on respondents and not researcher bias, motivation, or interest. We attempt to have an objective mind about the topic of cryptocurrencies and bubbles and, therefore, believe the findings are not based on researcher bias, motivation, or interest. Our objective is to be open, truthful and promote accuracy throughout our master thesis.

3.5 Research Ethics

It is critical to take into consideration potential ethical issues when designing a research in order to take measures to avoid unethical harm. This master thesis has followed the ethical principles outlined by Saunders et al. (2015)[4]. In terms of researchers' integrity and objectivity, we have collected the CRIX data from a public site, open to everyone and transparent in where the data originates. In addition, we report the results obtained from the bubbles tests and the interviewees openly, truthfully, and accurately. In terms of interviews, we are communicating clearly to our interviewees what the purpose of the study is and what we wish for them contribute with. Furthermore, we ask for oral permission to record the interview before the interview start so that the interviewees are aware that their words will be recorded. This is to ensure integrity when we are transcribing the interviews and to prevent data loss. The interviews contain input from individuals and organizations for privately-issued cryptocurrencies, as well as government officials and regulators, to make sure we capture various sides of the topic we are discussing. We have informed the participants about the purpose of the interviews prior to conducting them and participation has been completely voluntary. Moreover, our goal is to protect the privacy of all the participants and, thus, we have censored personal data and our data collection contains no indirectly identifiable data. By censoring the data, we also hope to attract more interview participants. In addition, we have conducted online searches to a certain extent prior to the interviews to

[4] More information about the ethical principles is available: Saunders et al. (2015, pp. 243-245).

ensure that the participants have the assumed knowledge we are looking for in our study.

3.6 Potential Limitations

We are both master students in financial economics, however part of our quantitative analysis is based on physics. We recognize that our competence in this area may prove to be a weakness to the study. In addition, because we are working with general models meant for bubble analysis in the financial markets, we have taken care to not draw conclusions based on the analysis which may be inaccurate. What is more, the data used from the CRIX contains only 20 constituents, leaving a large part of the crypto market unexplored. This could be considered as a clear limitation of this master thesis since the aim is to explore cryptocurrencies collectively. Even though CRIX is the only available cryptocurrency index, the quality of CRIX is extensively documented. However, as a consequence, we have chosen to supplement our thesis with interviews from industry experts while relying on advice from academia professionals. Moreover, the literature on cryptocurrencies is limited at the time and there is little existing research. We have, therefore, acquired an understanding about the industry as well as used existing theory to perform a thorough analysis. Lastly, since not all interviews are held in English, this may cause some linguistic problems, but we try to not lose contextual meaning in the translation process.

4 Bubble Tests

When attempting to identify if cryptocurrencies recently have been in a financial bubble, it is a natural starting point to look at the prices. Using CRIX as mentioned in section 3.2 Data, we are conducting bubble analysis to see if we can determine whether cryptocurrencies are in a bubble. First, to get a strategic overview of the price boom and bust, we will explain and perform a seven steps taxonomy.

4.1 Seven Steps Taxonomy

Grytten and Hunnes (2016) developed a theory from Kindlberger and O'Keefe (2001), and Minsky (1975): a seven step taxonomy that explains the various phases of a bubble as shown in Table 3. A bubble does not necessarily need to follow the phases from start to end and a bubble does not need to contain all the phases. Furthermore, this is a framework in which it is important to apply the potential bubble to the framework and not apply the framework to the bubble.

Table 3 Seven Steps Taxonomy

#	Phases	Actions	Signs
1	Disruption	The economy/financial markets are subject to a significant change which boosts money supply and substantially improves the growth outlook.	• New push in the economy • Optimism • Increased demand
2	Overheating	Expectations about positive shift are permanent. Supply and demand for credit increases and pushes the economy forward. Financial speculation becomes attractive	• Money and credit expansion • Supply and demand grows • Prices of asset classes are increasing • Economic growth
3	Bubble economy	Debt and speculation growth, no real economic growth.	• Money and credit expansion • Economic growth slowing down • Bubble tendencies
4	Nervousness	The market realizes potential overheating. Uncertainty when and if the economy/financial markets will start falling	• Markets are restless • Big price fluctuations in asset markets • Tightening of credit
5	Turning point	Markets start falling	• Optimism turns into pessimism • Asset prices fall (crash)

#	Phases	Actions	Signs
6	Crisis	Falling profits and asset prices. Financial markets are not contributing capital.	• Stop in money and credit growth • Negative bubble tendencies (crash) • Bankruptcies • Bank crisis
7	Spreading	Financial crisis spreads to other markets and the real economy	• Economic value creation stagnates • Unemployment increases

4.1.1 Application of the Framework

1. Disruption

As written in section 2.5 Cryptocurrencies, after Nakomoto's issuance of Bitcoin, the interest in Bitcoin and the blockhain technology gradually increased. Although one could say that the financial crisis in 2007-08 was a disruption that caused the rise of Bitcoin, however this was not a disruption to the bubble phases of cryptocurrencies. Furthermore, when looking at GDP growth worldwide, the growth has been increasing in most countries since the end of the financial crisis in 2009 (United Nations, 2014, 2012). However, the recent price boom in cryptocurrencies was during 2017, indicating that there has been no disruption in the real economy to explain the recent price boom.

2. Overheating

Michael Jackson, a partner at Mangrove Capital Partners, emphasizes that the changes in Bitcoin prices in 2013 started to get more widespread attention and the demand significantly increased (Barford, 2013). As written in section 2.5 Cryptocurrencies, cryptocurrencies have steadily increased since their issuance, but in 2017 cryptocurrencies grew more than ever. The latter could potentially be due to a lot of media attention, which continued the widespread awareness and fuelled demand as in 2013. A growth in demand supplemented with general optimism of economic growth can naturally lead to inflated trading volumes, which we identify as the second step in the framework (United Nations, 2018). Market participants selling cryptocurrencies with the belief that the buyer will buy at a higher price than what the seller paid is known as the Greater Fool Theory. In addition, Shaw (1996) finds that income growth is positively linked to risk taking. Thus, increasing wealth among the world population may have contributed to an overheating in the cryptocurrency market.

3. Bubble Economy

Looking at the price growth throughout the year 2017, CRIX rose from a price of \$1737 on 1^{st} of January to \$47588 on 31^{st} of December, which is a price increase of 2639%. Looking at the south sea bubble, the Mississippi bubble, the tulip crisis and the NASDAQ index under the Dot-com bubble: none of these crises come close to CRIX when looking at price increase in percentage during the same time period (Garber, 1990). In historically established bubbles, there are still some disagreement, where, for instance, Thompson (2007) argues that the tulip mania was not a bubble because "... bubbles require the existence of mutually-agreed-upon prices that exceed fundamental values. The "tulipmania" was simply a period during which the prices in futures contracts had been legally, albeit temporarily, converted into options exercise prices." Therefore, with cryptocurrencies we have to be careful to conclude that only large changes in price define a bubble. Moreover, the GDP growth has been positively increasing in the world since 2015, but the growth has not reflected the price boom in CRIX, meaning that there has to be another factor explaining the price increase of cryptocurrencies (United Nations, 2018). On the other hand, the rapid growth in cryptocurrencies and number of ICOs can be related to money expansion. To conclude, in step 3 of the framework we identify bubble tendencies and money expansion, but not an economy slowing down.

4. Nervousness

At the end of 2017, the prices in CRIX increased at an exponential rate, without a fundamental change in cryptocurrencies. However, there was a mass-adoption, justifying the exponential increase. Together with its high price fluctuations it is difficult to distinguish between a nervous phase and volatility. Still, with, for instance, a 15.5% decrease on 22^{nd} of December 2017, 15 days prior to the turning point, there are reasons to believe this is due to nervousness. On the other hand, as an unregulated market, major price fluctuations and manipulation can also stem from a major sales order or negative news event, either from nervousness, negative market outlook or general volatility.

5. Turning Point

Looking at CRIX, the all time high price and turning point is 6^{th} of January 2018, with a price of \$62 895. After the turning point, it seems like the market became more skeptical and individuals trading with cryptocurrencies were willing to sell their position for a significant lower price, resulting in falling prices, as the framework explains.

6. Crisis

The sixth phase tries to identify a crisis, but we cannot see such a crisis within the CRIX. One criterion the framework explains for a crisis is the negative bubble tendency (crash).

CRIX indicates that there have been negative bubble tendencies as the price hit \$18 694 7^{th} of April 2018, which is a 70% price drop from its turning point. At the end of the sample, as of 26^{th} of April the price is \$28 205 and much higher than the sample average of \$6 092. Even after the fall in prices, the CRIX is still upwards trending for the period, potentially indicating a price correction, and not a crash.

7. Spreading

There are no information about spreading of any crisis to the real economy as the real economy has steadily been increasing the past few years (United Nations, 2018).

Conclusion

The conclusion from using the seven step taxonomy is that some stages look almost identical to a bubble, especially the price boom in phase 1-3. In order to conclude that cryptocurrencies have been a bubble, the ending of the bubble phase must be identified. By using the last steps in the framework, the prices do not look significantly like the end of a bubble. Moreover, as seen in phase "6. Crisis", the trend has been continuously increasing and the price has been higher than average for the whole period, i.e August 2014 to April 2018. Furthermore, phase "7. Spreading" indicates no spread to the real economy. Although there are tendencies of bubble movements in the price, we cannot include the last phases of the framework mentioned above. Therefore, based on this framework we cannot establish that there has been a bubble, recently or present.

4.2 Financial Bubble Theory

There are various definitions of bubbles but there is no agreement regarding the most suitable one. A commonly used approach is the asset-pricing approach which proves evidence of a bubble as the part of the market price that is higher or lower than the fundamental value of an asset (West, 1987; Diba and Grossman, 1988; Van Norden, 1996). As this is the clearest and widely used definition of a bubble, the asset pricing model will be first explained and then applied to cryptocurrencies.

4.2.1 Asset Market Bubbles

When analyzing the stock market, Craine (1993) emphasizes the importance of a stock's fundamental value. In practice, the capital asset pricing model, the consumption capital asset pricing model and the arbitrage asset pricing model are models connecting expected returns to risk through equilibrium conditions. If the discount factor is endogenous and stochastic, the calculation of fundamental value is dependent and difficult.

However, in analysis of financial bubbles a common starting point of explaining a bubble would be the asset pricing equation (Phillips, Shi and Yu, 2015).

$$P_t = \sum_{i=0}^{\infty} \left(\frac{1}{1+r_f} \right)^i \mathbb{E}_t(D_{t+1} + U_{t+1}) + B_t, \tag{1}$$

Equation 1 is based on Craine (1993) and Campbell and Shiller (1988*b*) which helps to explain rational bubbles. In a rational expectations equilibrium to the stock price, P_t, equals the expected discounted value, r_f, of the price plus the dividend D_{t+1} next period. U_t represents the unobserved fundamentals and B_t is the bubble component.

Leone and de Medeiros (2015) argue that using the dividend-price information is the best alternative for analyzing the stock market. Furthermore, they claim that low dividend stocks can be seen as an indication of overpriced stocks, while high dividend stocks indicate underpriced stocks. Analyzing the time-series, a downward trending dividend-price ratio would be evidence of a stronger overpricing, or a bubble. A price rise would indicate increasing expectations of higher dividends at some point, and if the dividends are not realized, the price rise is, therefore, not due to fundamentals and, thus, there are indications of a deviation from the fundamentals. The price can, therefore, be seen as a composite of fundamentals plus a bubble component. As described e.g. by Craine (1993): "rational bubbles satisfy an equilibrium pricing restriction implying that agents expect them to grow fast enough to earn the expected rate of return. The explosive growth causes the stock's price to diverge from its fundamental value".

One could relate equation 1 to a housing bubble. An example of such a bubble is the housing bubble in the United States, where there is evidence of periodically collapsing rational bubbles in the post-2000 market. For the housing industry, we have the ability to fairly accurately measure the fundamental value, for instance, where Nneji, Brooks and Ward (2013) replaced dividends with rents.

$$P_t = P_t^{pv} + B_t, \qquad P_t^{pv} = \sum_{S=t}^{\infty} e_t^{-ir(s-t+1)} E_t(R_s)^5 \tag{2}$$

The latter equation is the fundamental value and if the market price equals to the fundamental

[5]"Where P_t^{pv} is the present value of the house price in period t, ir is the constant t interest rate, R is the gross rents value, and E is the expectation of the market given information at the start of period t [...] the actual price of a house is given by Pt while the bubble term, Bt, is the difference between the actual price and the fundamental value" (Nneji et al., 2013).

value, $P_t = P_t^{pv}$, it indicates that there is no bubble and $B_t = 0$. Controversially, if the market price does not equal to the fundamental value, $P_t \neq P_t^{pv}$, resulting in $B_t \neq 0$, the former equation derives the potential size of the bubble by solving $B_t = P_t - P_t^{pv}$ (Nneji et al., 2013).

4.2.2 Application of Asset Pricing Model

From Equation (1) in previous section, $P_t^f = \sum_{i=0}^{\infty} \left(\frac{1}{1+r_f}\right)^i \mathbb{E}_t(D_{t+1} + U_{t+1})$ is often called the market fundamental and B_t satisfies the submartingale property

$$\mathbb{E}_t(B_{t+1}) = (1 + r_f)B_t, \tag{3}$$

In the case of no bubbles ($B_t = 0$), the degree of nonstationarity of P_t is controlled by unobserved fundamentals, where P_t will be explosive in the presence of bubbles. Following the asset pricing model approach entails determining the fundamental value of an asset, which is often found by calculating the present value of the payoffs, taking into account all available relevant information (Campbell and Shiller, 1988*a*). However, as cryptocurrencies do not generate any cash flows, the fundamental value approaches used in stocks cannot be applied. This implies that cryptocurrencies cannot be an asset, so the question that remains is; how do we classify cryptocurrencies? Lo and Wang (2014) asks the same question, where they point out the unclear definition and whether cryptocurrencies are assets or currencies, or a mix. It warrants a look into how suitable cryptocurrencies are as a currency. Even if cryptocurrencies can be labeled a currency, it is still the essential question about its fundamental value. Therefore, before looking at the fundamental value of cryptocurrencies, it warrants a look into bubble tests that exclude using it.

4.3 A Recursive and Flexible Unit Root Test

Cheung, Roca and Su (2015) write about alternative approaches that avoid modeling the fundamental value, where they prefer to use a unit root test, similar to the one Phillips et al. (2015) explains. They discuss that a bubble expansion can be viewed as mildly explosive behavior (i.e. autoregressive root $\theta = 1 + gT^{-}m$ with $g > 0$ and $0 < m < 1$). Phillips, Wu and Yu (2011) explain the phases in a bubble as a stochastic process, where it starts from a martingale behavior, leads to sub-martingale behavior and ends the bubble in super-martingale behavior. Put differently, the conditional expectation of a price rise is sub-martingale behavior, whereas the conditional expectation of a price fall gives super-martingale behavior.

For the rest of the sub-sections below, we will explain the technicalities for the bubble tests used in this master thesis for determining whether cryptocurrenices are or have been in a bubble. The first test is called Supremum Augmented Dickey Fuller (SADF) based on Phillips, Wu and Yu (2011, PWY hereafter) and the extended version is named General Supremum Augmented Dickey Fuller (GSADF) based on Phillips et al. (2015, PSY hereafter). Furthermore, to more accurately date the origin and end of a bubble, Phillips et al. (2011) created the Backward SADF (BSADF), which is a part of PWY. Moreover, Phillips et al. (2015) also created Backward GSADF (BGSADF) as a part of PSY, for the same reasons as BSADF in terms of the origin and end of a bubble.

4.3.1 Introduction to the Recursive Augmented Dickey Fuller Tests

There have been several attempts to develop econometric tests to explain abnormal behavior, where Diba and Grossman (1988) were the first to propose a test that exploits the explosive characteristics of rational bubbles to look for exuberance in the stock market. Instead of testing the unit root against the stationary alternative, they looked at the right-tail of the distribution and tested it against the explosive alternative. Evans (1991) cited in Phillips et al. (2015) explains through simulations that a problem with this approach is that unit root tests have low power when trying to detect periodically collapsing bubbles.

4.3.2 The First Supremum Augmented Dickey Fuller - PWY Approach

Phillips et al. (2011) continued the research of Diba and Grossman (1988), where the former article found a solution to the low power problem. Instead of running a single test over the whole sample, they implemented right-tailed augmented Dickey-Fuller (ADF) test using subsets incremented by one observation each run in a forward expanding sequence, where the largest of these test statistics is used to test for explosiveness. The procedure to this method was named Supremum Augmented Dickey Fuller (SADF) test where they showed that it has much greater power, in addition to that they could pinpoint the start and ending date if the test showed bubble behavior (Pedersen and Schütte, 2017). Furthermore, Homm and Breitung (2012) consider different statistical methods that are similar in character to the SADF test, where they found in their simulations that the PWY test was most powerful in detecting bubbles. Thus, the SADF test is mainly used for detecting one single bubble.

4.3.3 The Generalized Supremum Augmented Dickey Fuller - PSY Approach

However, in Phillips et al. (2015) it is noted that the PWY procedure can exhibit reduced power and some inconsistency if the sample period contain multiple collapsing bubbles. To avoid this challenge in a quickly changing market data where there is more than one episode of abnormal behavior, Phillips et al. (2015) came up with a generalized SADF (GSADF) method. The same way as in PWY, they allowed for flexible window widths, but in the PSY procedure they allowed to change both the starting and ending point over a flexible range of windows.

Phillips et al. (2015) compare various tests, where it is shown that the PSY method outperforms the PWY approach and a related cumulative sum (CUSUM) test, as it covers more sub-samples and have greater window flexibility. Thus, as cryptocurrencies have been highly volatile, the PSY method is more suitable to time-stamp the bubble origination and termination dates.

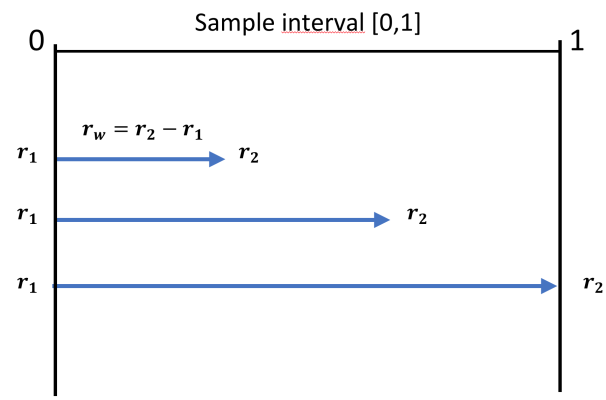
4.3.4 Technicalities to PSY and PWY

Unit root testing takes into account intercepts, deterministic trends, or trend breaks which are all factors impacting the limit theory developed by Phillips et al. (2015). The analysis conducted in Phillips and Shi (2014) tries to incorporate the small drift process for prices that can be realistically expected for long periods of time. This is done by adding an insignificant drift til the martingale null, meaning that they allow for a fundamental change over time. The prototypical model of this type has the following weak (local to zero) intercept form:

$$\Delta Y_t = dT^{-\eta} + \theta Y_{t-1} + \varepsilon_t, \qquad \varepsilon_t \sim^{iid} (0, \sigma^2),\ \theta = 1, \tag{4}$$

Where d is a constant, T is the sample size, and the parameter η is a localizing coefficient that controls the magnitude of the intercept and drift, as $T \to \infty$ and $\theta = 1$. Solving the equation gives $Y_t = d\frac{t}{t_\eta} + \sum_{j=1}^{t} \varepsilon_j + Y_0$ revealing the deterministic drift dt/T^η. When $\eta > 0$, the drift is small relative to a linear trend, when $\eta > \frac{1}{2}$, the drift is small relative to the martingale component of Y_t, and when $\eta < \frac{1}{2}$, the standardized output $T^{1/2\eta}$ behaves asymptotically like a Brownian motion with drift (Phillips et al., 2015). In Phillips et al. (2015), the focus is directed to $\eta > \frac{1}{2}$, where Y_t equals a random walk procedure, in essence what the null of PWY is. However, the procedure may be used to detect bubbles when $\eta > \frac{1}{2}$, as shown in Phillips and Shi (2014). The recursive approach involves a rolling window ADF style regression and the empirical regression; it is based on the Augmented Dickey Fuller model, and can be written as:

$$\Delta Y_t = \hat{\alpha}_{r1,r2} + \beta_{r1,r2} Y_{t-1} + \sum_{i=1}^{k} \hat{\psi}^i_{r1,r2} \Delta Y_{t-1} + \hat{\epsilon}_t \tag{5}$$



$$SADF(r_0) = \sup_{r_2 \epsilon [r_0,1]} \left\{ ADF_0^{r_2} \right\} \tag{6}$$

Figure 6: Illustration of SADF (Phillips et al., 2015)

Where k is the (transient) lag order and $r1, r2$ indicate the beginning and end of the regression window in the data sample. The first regression in the model will have a sample size of $T_w = \lfloor Tr_w \rfloor$, where $\lfloor . \rfloor$ is the floor function and extends one observation at a time until the time series reaches the end of the sample (i.e. $Tr_w = \lfloor T \rfloor$). The ADF statistic from the regression is non-standard and is denoted by ADF_{r1}^{r2}, which is obtained from the recursive regression by simulations together with the critical value, $CV_{r2}^{\beta_T}$ (Pedersen and Schütte, 2017). The null hypothesis of the models is that the time series follows a random walk with asymptotically negligible drift as we can see in expression (4) above.

Pedersen and Schütte (2017) are concerned that Phillips et al. (2015, 2011) sets lag-length k to zero and claim that the results are subject to severe size distortion. This may result in an incorrect rejection of the null hypotheses and the empirical results should be interpreted with caution. Pedersen and Schütte (2017) suggests setting the GSADF test with size $k = 1$, while the SADF should be set to $k = 1$ or $k = 3$, depending on the magnitude of θ together with the sample size.

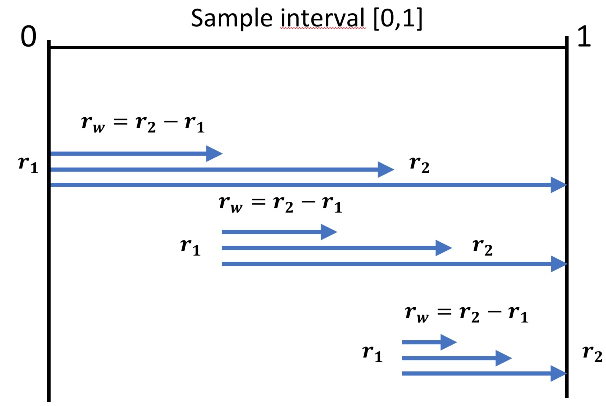
4.3.5 Illustration of the PWY and PSY Test

PWY

The starting point in the data set is always $R_1 = 0$ and the endpoint varies with R_w and ends up in $R_2 = 1$ in PWY. Figure 6 and Equation 6 illustrate the SADF testing procedure.

PSY

In contrast to the SADF test, Phillips et al. (2015) allowed for both the starting point R_1 and ending point R_2 in the sample window to vary as seen in Figure 7 and Equation 7.

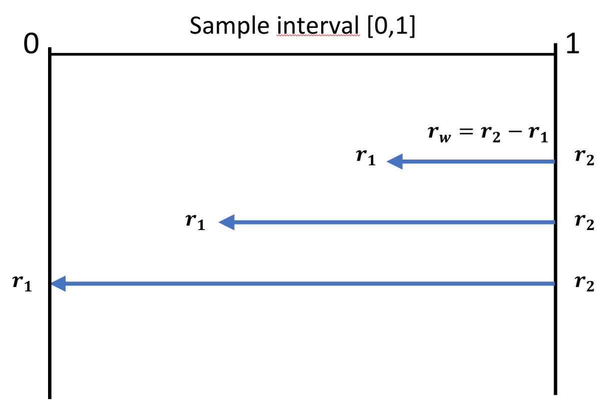


$$GSADF(r_0) = \sup_{\substack{r_2 \epsilon [r_0,1] \\ r_1 \epsilon [0, r_2 - r_0]}} \left\{ ADF_{r_1}^{r_2} \right\} \tag{7}$$

Figure 7: Illustration of GSADF (Phillips et al., 2015)

4.3.6 Date-stamping of Bubbles

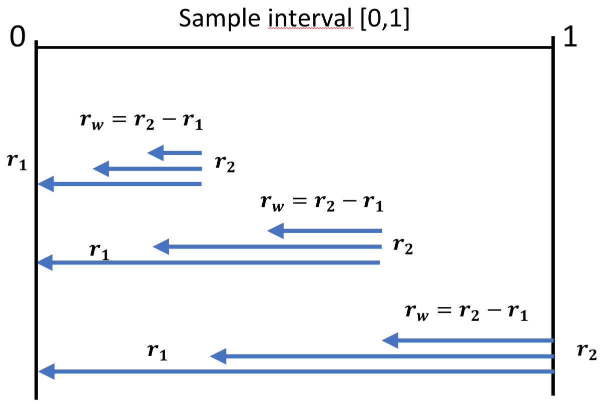
An addition to both of the models is that they allow identifying the origin and collapse of a bubble. The date-stamping is done by executing the tests backwards, resulting in Backward SADF (BSADF) and Backward GSADF (BGSADF). The date-stamping strategy is shown in Figure 8, 9 and Equation 8 and 9



$$BSADF_{r_2}(r_0) = \sup_{r_1 \epsilon [0, r_2 - r_0]} \left\{ ADF_{r_1}^{r_2} \right\} \tag{8}$$

Figure 8: Illustration of Backward SADF (Phillips et al., 2015)

We can deduce if observation r is part of the bubble by comparing the BSADF/BGSADF test statistic for the specific observation to its equivalent critical value (based on a sample size of Tr_2). Thus, by comparing the observations and critical values throughout the sample, we can infer the origination date of a bubble Tr_e as the first sequential observation where the ADF statistics exceeds the critical value. However, the termination date of a bubble Tr_f is the first sequential observation after $\lfloor T\hat{r}_e \rfloor + L_T$ where the ADF statistics goes below the critical value. For a bubble to exist, Phillips et al. (2015) argue that the bubble's duration must exceed a varying non-constant quantity. This requirement helps to control for smaller



$$GSADF(r_0) = \sup_{r_2 \epsilon [r_0, 1]} \left\{ BSADF_{r_2}(r_0) \right\} \quad (9)$$

Figure 9: Illustration of Backward GSADF (Phillips et al., 2015)

changes in the fitted autoregressive coefficient. Such a requirement is also adjustable and considers data frequency. The dating prediction are given by the crossing time formulas:

$$\hat{r}_e = \inf_{r_2 \epsilon [r_0, 1]} \left\{ r_2 : ADF_{r_2} > CV_{r_2}^{\beta_T} \right\} \quad and \quad \hat{r}_f = \inf_{r_2 \epsilon [\hat{r}_e + \delta log(T)/T, 1]} \left\{ r_2 : ADF_{r_2} < CV_{r_2}^{\beta_T} \right\}, \quad (10)$$

Where $CV_{r_2}^{\beta_T}$ is $100(1 - \beta_T)\%$ the critical value of the ADF statistic based on $\lfloor Tr_2 \rfloor$ observations. The significance level β_T rely upon the sample size T and an assumption is that $\beta_T \to \infty$ and thus, $CV^{\beta_T} \to \infty$, as $T \to \infty$. δ is a tuning parameter which determines the minimum duration for a bubble and is usually set to 1 (Fantazzini, Nigmatullin, Sukhanovskaya and Ivliev, 2016; Phillips, Shi and Yu, 2015).

The dating strategy for PSY are according to the following equations, 11 and 12.

$$\begin{aligned} \hat{r}_{1e} &= \inf_{r_2 \epsilon [r_0, 1]} \left\{ r_2 : BSADF_{r_2}(r_0) > SCV_{r_2}^{\beta_T} \right\} \quad and \\ \hat{r}_{1f} &= \inf_{r_2 \epsilon [\hat{r}_{1e} + \delta log(T)/T, 1]} \left\{ r_2 : BSADF_{r_2}(r_0) < SCV_{r_2}^{\beta_T} \right\}, \end{aligned} \quad (11)$$

$$\begin{aligned} \hat{r}_{2e} &= \inf_{r_2 \epsilon [\hat{r}_{1f}, 1]} \left\{ r_2 : BSADF_{r_2}(r_0) > SCV_{r_2}^{\beta_T} \right\} \quad and \\ \hat{r}_{2f} &= \inf_{r_2 \epsilon [\hat{r}_{1e} + \delta log(T)/T, 1]} \left\{ r_2 : BSADF_{r_2}(r_0) < SCV_{r_2}^{\beta_T} \right\}, \end{aligned} \quad (12)$$

Lastly, Phillips et al. (2015) recommend using a rule for choosing the window size, r_0, that is based on a lower bound of 1% of the full sample and has the functional form $r_0 = 0.01 + 1.8/\sqrt{T}$.

4.3.7 Critiques Towards PWY and PSY

Pedersen and Schütte (2017) express the following "a critical assumption behind the recursive right-tailed unit root test is that innovations to the relevant time series are homoscedastic and serially uncorrelated under the null hypothesis." Since the tests by Phillips et al. (2015) and Phillips et al. (2011) are repetitions of unit root tests, these tests are also subject to the pitfalls of such tests. Thus, this may be a drawback associated with sequenced unit root tests. Phillips et al. (2015) explore the presence of time-varying but stationary volatility in their tests and find that it does not lead to noticeable size distortions. Harvey, Leybourne, Sollis and Taylor (2016) on the other hand, do research on the PWY method and write as follows "their supremum-based test has a non-pivotal limit distribution under the unit root null, and can be quite severely over-sized, thereby giving rise to spurious indications of explosive behavior". In other words, recursive testing on many sub samples can lead to size problems in the smallest sample windows.

Through the simulation study by Pedersen and Schütte (2017), it is shown that the occurrence of serially correlated innovations can lead to large-size distortions for the PWY and the PSY test. The distortions decrease with the sample size, but could also be a problem for large samples and the tests could be critically oversized, especially the GSADF test. These distortions could lead to rejection of the null hypothesis of a random walk against the explosive alternative too often and risk concluding presence of a bubble when there is no bubble. Pedersen and Schütte (2017) suggest using a bootstrap procedure that is supposed to lead to almost perfectly sized tests and that the corrections of size come at a fairly low cost in terms of power. Upon starting to work with the models, we noticed the challenges with cryptocurrency prices, its volatility and how the results were likely to be inaccurate. This led us to limit drawing conclusions from the use of recursive bubble test based on Phillips et al. (2015) that is used in this thesis.

4.4 Results

Firstly, we explain how the simulation of the tests were conducted, following an interpretation of the graphs. As we have performed both bubble tests, PWY- and PSY test, the results are shown in this respective order. Furthermore, we perform the date-stamping of the bubble tests and, in the end, we conclude our discoveries.

Explanation of the results

When the ADF statistics (blue line) crosses the critical value (red line) it could be either Tr_e, signaling the start of a bubble and is upward sloping, or Tr_f, signaling the end of a bubble and is downward sloping. CRIX shows the index price in US dollars.

4.4.1 Simulation of the ADF Bubble Test

First of all, because of the exponential data set, to achieve some stationarity in sub samples, we made the data logarithmic. In our simulation of the right-tailed unit root tests, we start from the null hypothesis in equation 4. We use a Monte Carlo simulation to loop the Dickey Fuller tests on various sub samples. The results are collected from the ADF test statistics, together with the critical values.

We set the minimum window length to $r_0 = 0.01 + 1.8/\sqrt{T}$, which results in *80* observations. In terms of k we have done multiple simulations, where we see little difference. Therefore, we have decided to follow the advice of Pedersen and Schütte (2017) and, to be consistent, we have set all the tests to $k = 1$. The critical values are performed together with the ADF statistics so that the critical values that belong to the ADF statistics are compared.

4.4.2 PWY Method - One Bubble

As seen in Figure 10 below, the PWY method finds evidence of a bubble starting in the beginning of May 2017 and continuing throughout the sample period. Looking at the graph, the extreme growth seen during 2017 appears to have subsided. The graph also shows ADF statistical value close to the critical value, indicating a more normalized price. However, a still volatile price makes it hard to draw conclusions this close to the latest price exuberance during 2017.

There are some spikes earlier in the sample, one at the beginning of 2015, one around June 2016 and one at the beginning of 2017. As written in 4.3.1 Introduction to the Recursive Augmented Dickey Fuller Tests, earlier research has shown that in the SADF test, normally the most significant bubble shines through, as is this case (Phillips et al., 2015).

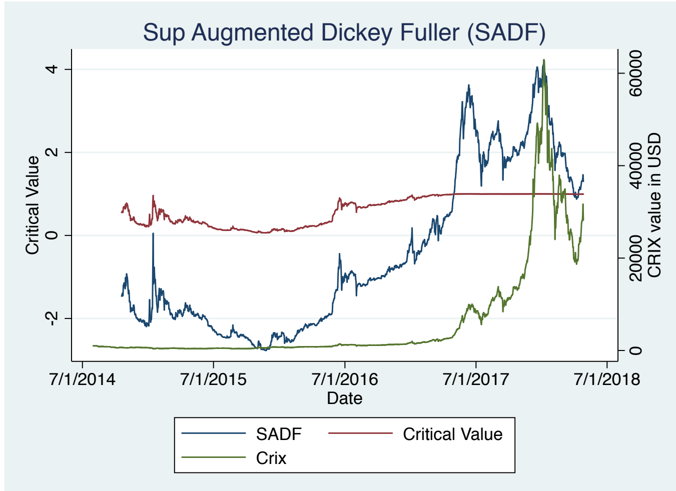


Figure 10: SADF Test of One Bubble

4.4.3 PSY Method - Multiple Bubbles

Figure 11 below shows more significant bubble tendencies than the SADF test, where the GSADF indicates that there is a bubble starting at the beginning of December 2014 and ends at the beginning of May 2015. The second bubble tendency start around mid June 2015 and continues throughout the sample period. The results are consistent with what was stated in section 4.3.1 Introduction to the Recursive Augmented Dickey Fuller Tests, that the GSADF test produce higher power results. However, as the ADF statistics are barely below critical value in 2015, we should not exclude that most of the sample could be one longer-lasting bubble, according to the test.

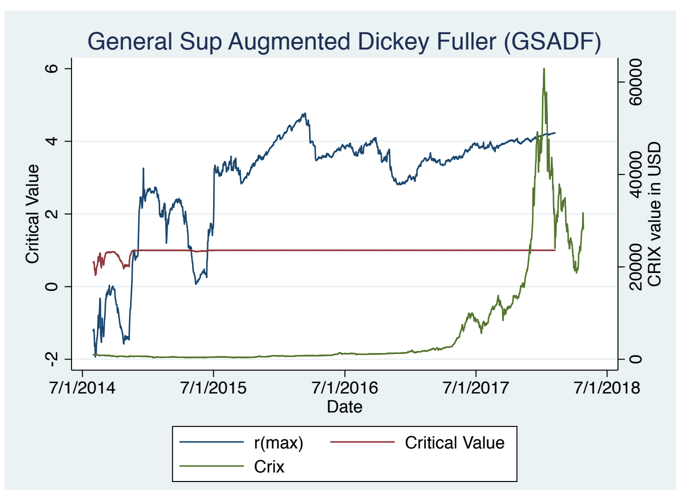


Figure 11: GSADF Test of Multiple Bubbles

4.5 Date-stamping the Bubble

When using the time-stamping strategy, BSADF test for the PWY approach and BGSADF test for the PSY method, displays conflicting results. As seen in Figure 12 below, the backward SADF date the bubble to 21^{st} of September 2017.

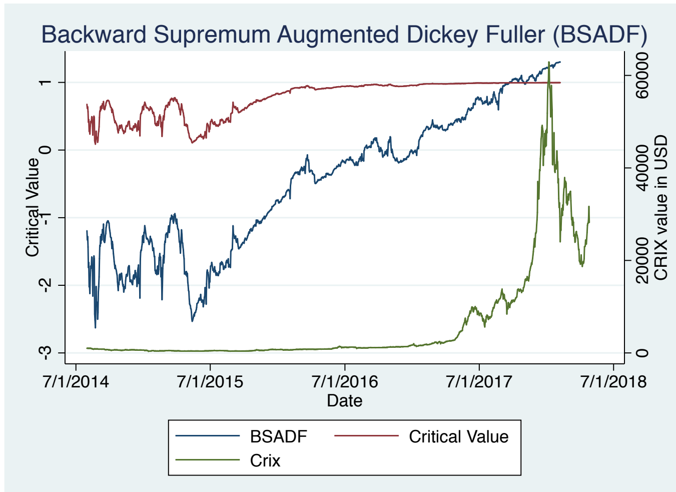


Figure 12: Backward SADF Test of One Bubble

Figure 13 below illustrates multiple bubble tendencies, but most of them are short lasting, making these bubble tendencies questionable. However, looking at the last bubble tendency, the ADF statistics seem to be slight upward trending and the dating of the beginning of the bubble is 27^{th} of April 2017.

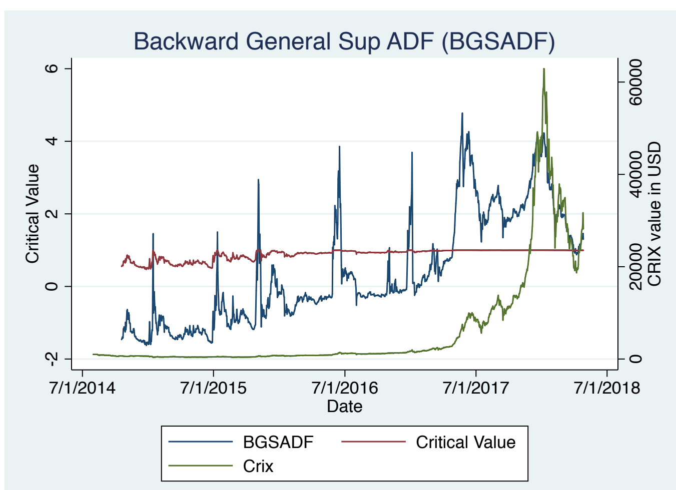


Figure 13: Backward GSADF Test of Multiple Bubbles

The spikes showed in 4.4.2 PWY Method - One Bubble is in Figure 13 displayed as bubbles tendencies, where the first, fourth and fifth spike are the most significant ones. Controversially, the fourth bubble tendency in Figure 13 can barely be seen in the PWY approach. As expected, when there are multiple bubble tendencies, the results before the bubble in the PWY approach are inconsistent. Lastly as in 4.4.2 PWY Method - One Bubble, there are five days at the end of the sample where it is not defined as a bubble according to the tests. This may be due to that the cryptocurrency prices are starting to stabilize.

To get an overview of the volatility in the data, a daily percentage change is presented in Figure 14 below. As Figure 14, the volatility in CRIX is significant, which means that the spikes in the bubble tests are not necessarily bubbles. However, the interpretation of these results depend on how a bubble is defined.

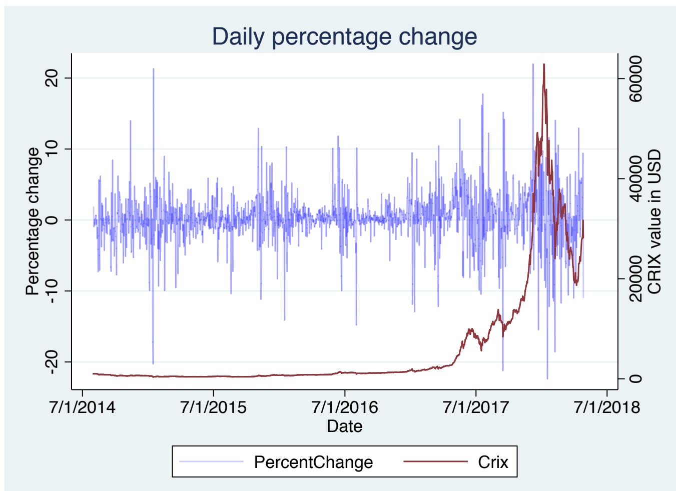


Figure 14: Daily Percentage Change of CRIX

4.5.1 Additional Comments

As this master thesis extends over the course of 6 months, we have conducted an updated analysis in the end of April 2018 to get updated results from the analysis conducted in February 2018. This inclusion of newer data led the ADF statistics in the SADF and BGSADF tests to fall below the critical value at the end of the sample period. According to theory, this signifies the end of a bubble and the subsequent rise above the critical value signifies the start of a new bubble. As seen in Figure 10 and Figure 13, we can see a momentary exit from the bubble values and back to bubble values. If we are to interpret these results, the momentary disparity from ADF statistics and critical value show the end of a bubble which continues into a new bubble a few days later. Results such leads us to further question the use of mechanical models for cryptocurrency price data.

4.5.2 Conclusion

To conclude, the spikes in the backward GSADF and SADF test could be due to high volatility. However, when the price increases or decreases up to 50 % in a week, there is some confusion in terms of the cause being either general volatility or indication of a bubble. This may be due to the fact that cryptocurrencies have emerged relatively newly and, therefore, experience adoption at an exponential rate, but it may also be part of cryptocurrencies' natural price volatility. The natural volatility seems more probable, but to conclude this is speculation.

Furthermore, both the GSADF and SADF test show bubble tendencies, but to different degrees. If we are to believe the SADF test, it shows bubble tendencies at the beginning of May 2017 and throughout the sample period. The GSADF test, on the other hand, shows bubble tendencies from beginning of December 2014 to beginning of May 2015 and mid-June 2015 to throughout the sample period. Thus, by being conservative towards the results of the GSADF and SADF tests, we conclude that there have been bubble tendencies from May 2017 and throughout the sample period.

When date-stamping the bubble, the PWY method using the BSADF test identifies the start date of a bubble as being approximately around 21^{st} of September 2017. The PSY method, using BGSADF test, finds the origin date of bubble tendencies starting in mid-June 2015. However, as written in 4.3.7 Critiques Towards PWY and PSY about size distortion and the fact that the results of the GSADF showing more bubble behavior than the rest of the tests, it is reason to believe the result could be contain incorrect rejections of the null hypotheses and can affect the accuracy of the results.

4.6 Log Periodic Power Law

The other method we used to evaluate the CRIX price data is the Log Periodic Power Law (LPPL) test. This model was first used in economics by Didier Sornette in 1996, when he attempted to identify the critical points to the October 1987 market crash. The model proposes a connection between crashes and critical points with identifiable patterns prior to the crash as well as characteristic oscillations of relaxation and aftershock signs (Sornette, Johansen and Bouchaud, 1996). Successful fitting of the oscillations to financial data has later been independently confirmed (Feigenbaum and Freund, 1998). Subsequently, the LPPL test has been developed into the Johansen-Ledoit-Sornette (JLS) model, which is the model we will be using (Johansen, Ledoit and Sornette, 2000). The model states that bubbles are not identified by an exponential increase in price, but rather a faster-than-exponential growth in price: a feature resonating well to the price movement of cryptocurrencies. Other studies have found that this model can be fitted to any type of financial data, even non-trading day based prices such as cryptocurrencies (Gazola et al., 2008).

The background for the model comes from a simplistic approach. In financial markets, we encounter several participants who hold roles as buyers and/or sellers. A crash is an instability where agents place sell orders of sufficient quantity and this magnitudes simultaneously to make market makers unable to absorb the order without lowering the price. A key point in terms of large markets is that the participants are largely strangers to each other. Johansen et al. (2000) aim to understand what can cause such coordinated behavior among strangers and propose a theory of micro-level imitation. According to their study, they believe all participants are trading in an organized way of networks among friends, colleagues and other groups, where they influence each other locally. In this network, there are two factors from which individuals form opinions. The first factor is through the opinion of the other participants and the second is through an individual, or idiosyncratic, signal that a participant alone receives. When the participants in financial markets are not coordinated, or in disorder, we experience roughly as many sell orders as buy orders and no crash is occurring. By disorder we mean no one-sided consensus about buying or selling because individuals perceive the available information differently. Herd behavior in financial markets have been researched empirically and we know participants tend to imitate others (Scharfstein and Stein, 1990). The cryptocurrency market is very accessible when it is not subject to security and trading laws and the easy access can lead to a larger herd behavior effect. Hong (2017) analyze Bitcoin momentum returns and find consistency with sentiment theories of initial under-pricing and delayed over-pricing; these sentiment theories play a part in the social side of investing in Bitcoin. As we will mention later, the technology behind cryptocurrencies is not fully understood and there are societies surrounding individual cryptocurrencies. Thus, the social network mentioned above appears to be strong for a cryptocurrency like Bitcoin, where investment professionals typically have limited knowledge and investors take matters more in their own hands, directly affecting their local network to a much higher degree. Calcagno and Monticone (2015) show that individuals with low financial literacy are less likely to visit a financial advisor for advice. This further reinforces the social side of a cryptocurrency like Bitcoin, where local influence plays a bigger part than professional advice on investing in Bitcoin. Such micro-level imitation is what ultimately leads to macro-level coordination. Thus, when we experience coordinated behavior in the form of sufficient sell orders, a crash may occur.

4.6.1 Technicalities

Sornette et al. (1996) proposed the phenomenon of log-periodic oscillation, with the frequencies of the oscillations increasing up until the most likely time of a crash occurring. This phenomenon is intended for describing endogenous crashes in financial markets. The function of the Log-Periodic Power Law (LPPL) model can be quantified as:

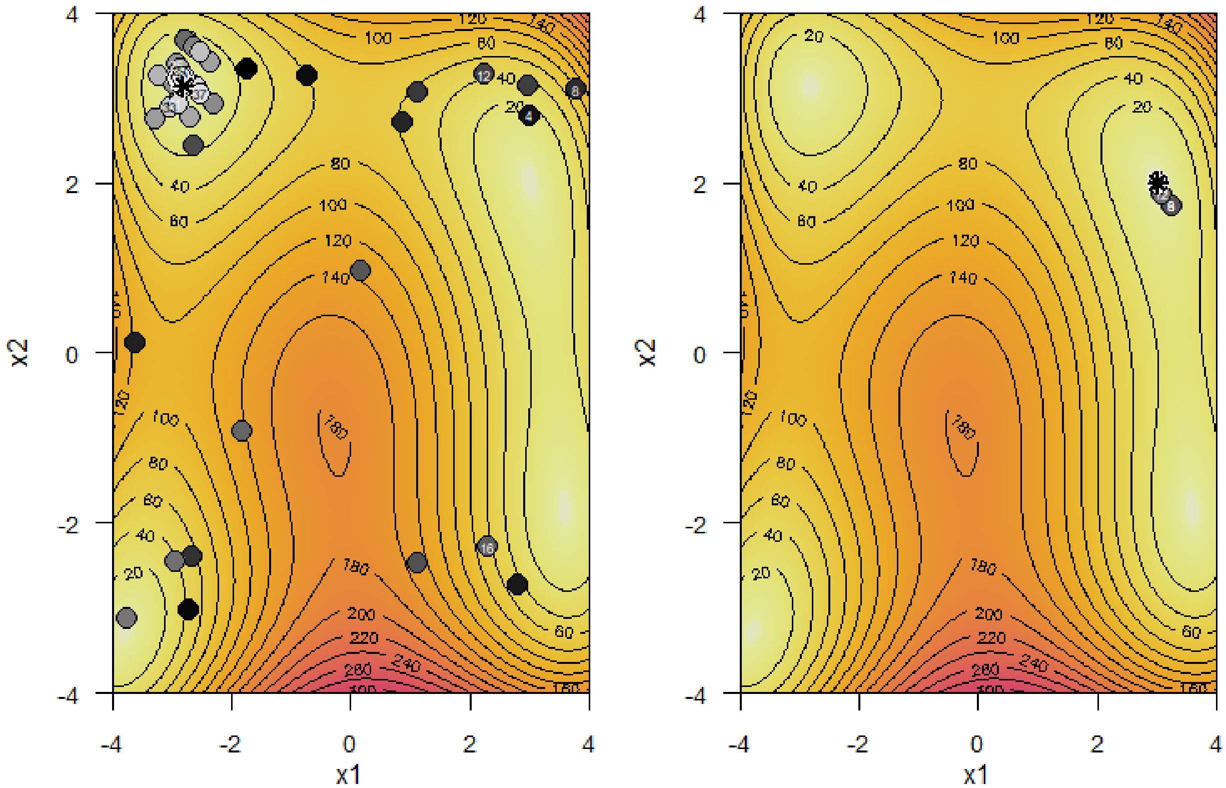
$$y(t) = A + B(t_c - t)^{\beta} + C(t_c - t)^{\beta} cos[\omega ln(t_c - t) + \phi] \tag{13}$$

The model contains three linear parameters - A, B, and C - and four non-linear parameters - t_c, β, ω, and ϕ. Thus, there are a total of seven parameters. t_c denotes the critical time for which a crash is most likely to occur. ω is the frequency of oscillations in the bubble, ϕ is the phase of oscillations, and β is the exponential growth. Estimating a model with seven parameters can be complicated, not just for the computational difficulty, but also the many pitfalls that surrounds such a process. We first express the three linear parameters as a function of the remaining four nonlinear parameters to reduce the number of parameters (Johansen et al., 2000). If we want to fit a function to data, it will be minimizing the residual sum of squares, SSE, given by the objective function:

$$\min_{\theta} F(\theta) = \sum_{i}^{N} y_{\theta}(t_i) - \hat{y}_{\theta}(t_i))^2, \quad where\ \theta = (t_c, \phi, \omega, \beta) \tag{14}$$

4.6.2 Critiques

The optimization problem leaves us with having to find the global minimum for the objective function. A function with several local minima may not give a reliable answer to this. Methods like the downhill simplex method and Quasi-Newton method are efficient, but they can only find the local minimum near where the initial starting point is set. Hence, we cannot effectively rely on the optimization with certainty that the minimum is global. The optimization process used to determine the global minimum is simulated annealing which is one of many optimization tests that can be used to determine the global minimum in the face of multiple minima (Bohachevsky, Johnson and Stein, 1986). Since the parameter space contain four non-linear parameters, we cannot hope to get an accurate picture of the characteristics of the objective function. To illustrate this optimization problem simplified, we use the Himmelblau function, as shown in Figure 15 below, which contains four local minima for two parameters. The difference between the two plots below is the method of estimation. The figure (a) to the left displays the optimization done by simulated annealing and figure (b) to the left only displays the downhill simplex method (Nelder-Mead). It is clear that the downhill simplex method ignores any other solutions other than where the starting point is set, whereas the simulated annealing does explore these minima as well.



(a) Optimization by Simulated Annealing (b) Downhill Simplex Optimization

Figure 15: Optimization Processes (Own Illustration)

4.6.3 Limitations

Although the LPPL model has previously been used to forecast financial bubbles and is suited to use in financial data (Johansen et al., 2000), it may not present reliable results for the cryptocurrency data we are working with. This is due to critics of the model in previous section, in addition to the high volatility of cryptocurrency price data. The model is designed to detect large changes in regimes and not necessarily crashes. Because cryptocurrencies are of such high volatility, this model becomes unpredictable as it may show a crash where there is instead simply abnormal volatility present. In addition, computing such an optimization problem requires large computational power. The LPPL computation is purely mechanical and ignores a lot of potential changes in the data. The critical point assumes the oscillating signature apply for the prices of cryptocurrencies as they do with traditional stock markets:

an assumption which has not yet been backed by research.

4.6.4 Results

As previously mentioned, the oscillations are fitted until they reach the critical value. Therefore, this test shows the most likely time for a regime change, which we denote as the most likely time of a crash in this test. The critical value we get is the most likely time of a crash, although a crash can happen at any time before that as well. Furthermore, a crash does not need to happen either. Based on the analysis we have done, we estimate the parameters for the LPPL model to be:

$$\beta = 2.9 \qquad \omega = 0.6 \qquad \phi = 0.9$$

If we are to believe this calculation, the most likely point of a regime change, defined as a crash in the model, is after 1406 days. This corresponds to 40 days after our sample of 1366 days, or on June 5^{th}, 2018. The R^2 of 0.9381 shows a good fit for the regression, but the standard deviation of 0.3045 shows how uncertain the result actually is. Therefore, albeit we get a plausible date for the regime change, the result is untrustworthy. The critical value is simply a most-likely estimation for when we can expect a regime change in the price, based on the oscillating signature of the historical price. We notice the standard deviation being fairly large, making the estimated crash window also large and unreliable.

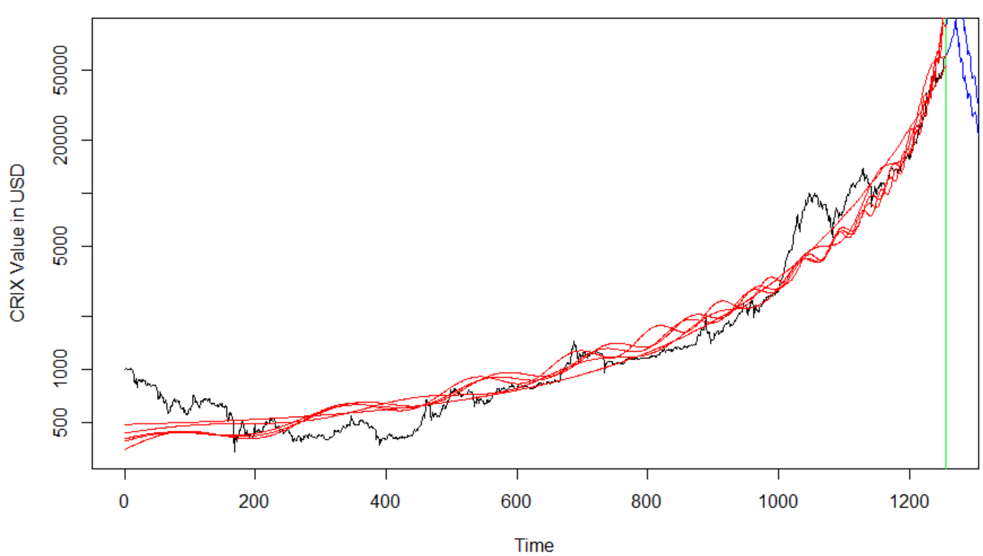


Figure 17: Illustrative Fitting of Oscillations

5 Decomposing Cryptocurrencies

Our thesis attempts to answer whether we can identify cryptocurrencies as being in a bubble, either in the past or present. In section 4 Bubble Tests, we wrote about the importance of finding the fundamental value in determining if an asset is in a bubble, e.g. an overvalued stock. As cryptocurrencies could not be labeled as an asset, we performed bubble tests to try to detect bubble behavior in cryptocurrencies by using CRIX data. However, we also established that the asset pricing model could be used to determine a bubble if we could calculate the fundamental value. Therefore, in this section we will present two of the most discussed approaches to finding the fundamental value for cryptocurrencies. Next, as cryptocurrencies are a part of the emerging business of financial technology (fintech), we will discuss fundamental value and its nature in terms of cryptocurrency. Lastly we will examine cryptocurrencies' suitability using the definition and characteristics of money, in addition to Central Bank Digital Currency (CBDC).

5.1 Fundamental Value

Fantazzini, Nigmatullin, Sukhanovskaya and Ivliev (2016) present two approaches for calculating fundamental value of Bitcoin: market sizing and the (marginal) cost of production based on electrical consumption.

5.1.1 Market Sizing

In terms of market sizing, there are various approaches, where Fantazzini et al. (2016) present three different procedures. These procedures are made by various assumptions in different degrees of complexity, where the value of Bitcoin according to the potential in the market is calculated. One of the procedures is presented in Woo, Gordon and Iaralov (2013), a Bank of America (BoA) Merrill Lynch report, and is the most complex procedure, potentially resulting in a more reliable valuation than the simpler approaches as the former includes more factors than the latter approaches. However, the complexity of cryptocurrencies may make the assumptions unreliable and the result imprecise. The report from BoA sets Bitcoin as an equivalent to e-commerce and calculates the fair market value of Bitcoin as a percentage of the total e-commerce market. The conclusion of the report was a fair value of US$1 300 per Bitcoin, but the valuation makes some opaque assumptions. Furthermore, as the report is from 2013, the assumptions may have been relevant to Bitcoin at the time. However, this valuation has not been applied in present days which alone can make the procedure doubtful. In addition, the valuation comes from a bank with financial interests in the payment industry.

In addition, the bank may have influenced the assumptions and data to get a valuation close to the actual price because they have to take into consideration their own reputation. It is, therefore, possible that the assumptions were molded to fit the price of the time, an attempt to suppress the price, and that these same assumptions no longer apply to the current price.

Thus, this procedure of calculating fair market value is inaccurate and a lot of assumptions are made. The other procedures consist of using the value of fiat money supply and calculate the value from probability of success where the chance is a self-picked number. This seems unreliable and may be a prediction equivalent to a wild guess without any analysis. At this point in time, it is unknown on what factors cryptocurrencies' value is based. If these factors would be known, they would probably vary among cryptocurrencies due to the individual differences between the plethora of cryptocurrencies, as well as the differences between cryptocurrencies in an early and mature stage of growth. For example, an anonymous cryptocurrency whereas a utility cryptocurrency.

5.1.2 Marginal Cost of Production

The second approach is based on the marginal cost of Bitcoin production to determine the lower bound and estimate the fundamental value of one Bitcoin. Garcia, Tessone, Mavrodiev and Perony (2014) introduced this approach where their main idea is that the Bitcoin price should be at least equal to the cost of the energy involved in mining. Hayes (2016) developed the marginal cost of Bitcoin production further and, in addition, he explained that a halving of a block reward will increase the Bitcoin price substantially. The valuation method is limited to the assumption that "A rational agent would not undertake production of Bitcoins if they incurred a real ongoing loss in doing so" (Hayes, 2015).

Furthermore, if costs exceed the price, agents will stop mining and the Bitcoin network will automatically adjust down the difficulty variable, making the hash function easier to solve and resulting in less power required and lower mining costs. This will be adjusted until the costs are lower than the price, which will profit the miner. These Bitcoin network protocols also work the other way; a high Bitcoin price will attract agents to mine, which will make the difficulty level higher and increase costs through higher required power. This approach is useful for the miners in order to know the break-even price of producing Bitcoin. There will be an equilibrium between the cost and the price for every Bitcoin that will always stabilize and attract, or discourage, mining. In addition, there are discussions about how to reward the miners and, especially after 2040, when Bitcoin has reached its capacity of total Bitcoin.

However, it seems unlikely that the Bitcoin price is driven by the cost of production, rather than the other way. Although as the cost is related to the price in a supply/demand equilibrium, it is unlikely that the costs are the main driver and, thus, the marginal cost of production cannot be a good valuation method.

5.1.3 Redefining Fundamental Value

As mentioned before, the definition for a bubble is arbitrary and media often misuses the term. However, as shown earlier, estimating the fundamental value of cryptocurrencies proves to be quite difficult. If we are going to estimate a fundamental value, we may have to come up with a new framework, as mentioned by interviewee #3:

> *"...we are kind of in the middle of redefining what fundamental value means. And what I mean by that is, there is kind of a social side to cryptocurrencies what we have not seen in traditional stocks."*

What this framework should include is still too early to determine, but as mentioned earlier, the fact remains that cryptocurrencies are vastly different from any currency and any other asset (Bank of England, 2018). The social side we see with a cryptocurrency like Bitcoin distinguishes it from that of traditional financial markets.

Interviewee #3 continues with an example of where there might be some kind of value within the cryptocurrency market:

> *"And we have projects like Neo, for instance, which you know, you could argue that foundational value is also in the ecosystem that surrounds it. So, there over 600 developers like very high-spec developers that contribute code for free to the project. So that kind of gives it foundational value as well because when the bubbles pop, and we are seeing a lot those projects that have no use to evaporate, and the ones that are going to remain and give success are the ones that, the ones that people have invested most in. I'm not talking about money, I'm talking about time, effort and kind of the whole ecosystem around it."*

Using resources may not necessarily give something value, but if the resources give a foundational value, it may contribute to establishing a fundamental value. Based on our understanding of foundational value from the interview, the definition is the fact that there are communities around the cryptocurrency, where societies are formed in order to create and support a specific cryptocurrency. These societies of people are working to improve cryptocurrencies and are truly enthusiastic about cryptocurrencies. The rise of these societies has proved to make authorities acknowledge them and, thus, can lead to a change in the monetary system. On the other hand, Dodd (2018) is skeptical towards Bitcoin and the characteristics of the communities that have emerged. He claims that the success of Bitcoin is because of the communities with the following characteristics: e.g. structure, leadership, hierarchy, friendship and community. The skepticism comes from these characteristics being embraced, rather than evaded. These characteristics reflect centralization, while Bitcoin initially was supposed to be decentralized. However, the centralization may not be a weakness or the main problem with neither the economy, nor the society. The fact that these communities exhibit these sociological characteristics is probably one of the reasons for cryptocurrencies' success and it is likely that a decentralized way of thinking has its foundation in democracy; the structure around cryptocurrencies has evolved and is still evolving into something not yet known. Another scenario, however, is that cryptocurrencies are and will be underdeveloped and eventually disappear. Still, the unresolved nature and the price exuberance does not necessarily make cryptocurrencies a bubble. It may simply be because cryptocurrencies have surpassed most expectations and as there is potential, the world should not exclude cryptocurrencies from being a part of a monetary system.

The societies above do not necessarily make cryptocurrencies work as money, but the blockchain may be developed to make cryptocurrenices to better suit as money and they can become more accepted by the government and society. However, we may also see other innovations such as Mastercoin and Ethereum with approaches to smart contracts being successful due to high potential value as a platform (Dodd, 2018). One rational expectation could also be the communities supporting the most functional blockchain project and that this foundational value is later translated into tangible value creation within the community. However, the effort one sees from these communities could be disproportionately high with the initial rewards, making rational predictions difficult. More importantly, if a project would fail, the pieces of the project, whether it is codes or something else, can be used in another project that will generate money in the future, even if there is no intrinsic value. A comparison can be made with constructing a building, where the material can be sold if the project would fail. Furthermore, when innovations are emerging and there are uncertainties, whether it will fail or be successful, the expected future cash flows are expressed as fundamental value in traditional valuation. Consequentially, with cryptocurrencies there are probably considerable more unresolved issues and risks related to the success rate and, therefore, issues relating to estimating the fundamental value of cryptocurrencies. These uncertainties in fundamental value can lead investors to potentially lose or gain a lot, depending on the real value of cryptocurrencies.

Interviewee #3 compares cryptocurrencies with the rise of technology firms:

> *"If you can take it from the perspective of the Dot-com bubble, where you know was a similar situation, where there were a lot of IPO's that started selling, basically, vapor products. And yes, that was kind of a bubble as well in the same sense as it is now,*

but it also gave birth to a lot of amazing companies like Amazon, Google and stuff like that."

The argument here is that even if projects around cryptocurrencies are uncertain, it does not necessarily mean that there is no value, even if the fundamental value in terms of cryptocurrencies is unresolved.

5.2 Application of Traditional Definition and Characteristics of Money

Recalling 2.3 Definition of Money and 2.4 Characteristics of Money, we will first analyze cryptocurrency with Adam Smith's definition of money and then the characteristics money should possess.

5.2.1 Smith's Definition of Money

Emerging cryptocurrencies are, as mentioned before, private and largely unregulated worldwide. Central banks around the world have had to recognize cryptocurrencies and the possibilities as well as the threats cryptocurrencies pose. However, in terms of the roles as money, The Bank of England (2018) noted in the report "The future of money" by Mark Carney, the Governor of Bank of England and Chairman of the G20's Financial Stability Board, how ill-suited cryptocurrencies are as money. The three functions of money mentioned in section 2.3 Definition of Money are broken down by Carney.

A medium of exchange

The first issue brought forward by The Bank of England is cryptocurrencies' use as a medium of exchange. Carney stresses that "...no major high street or online retailer accepts Bitcoin as payment in the UK, and only a handful of the top 500 US online retailers do." As Ripple has a smaller market capitalization, it can be assumed that its acceptance is lacking more than Bitcoin. Bitcoin also suffers from a lack of efficiency as the average confirmation time for transactions to be accepted into a mined block have been reported as slow as 1 week on January $23rd$, 2018 to as fast as 0 minutes on April $10th$, 2018 (Blockchain.info, 2018). Such unreliable transaction speed makes Bitcoin unsuitable as a medium of exchange. However, Ripple is shown to have superior features that makes it more reliable in terms of transacting. A report from Cambridge University shows that, while cryptocurrencies are growing in terms of acceptance from merchants, cryptocurrencies are still not being used as a primary medium of exchange for daily transactions (Hileman and Rauchs, 2017). Hence, it is safe to assume that cryptocurrencies lack the function medium of exchange, when the main issue is that they are not widely accepted as a means of payment. If this trend continues cryptocurrencies will remain as a peer-to-peer transactor.

A store of value

The second function of money is being a store of value. The standard deviation of 30-day BTC/USD exchange rate is almost five times that of the EUR/USD as of May 1^{st} 2018 (Buybitcoinworldwide, 2018*a*), showing Bitcoin is a poor store of value. This is with the caveat that Bitcoin is the largest cryptocurrency and one of the more stable non-backed cryptocurrencies CryptoCompare (2018*a*). A currency which deviates this much in value, relative to other currencies, is deemed a poor store of value(Bank of England, 2018). Long-term saving with such high volatility is dreadful because the expected return might not even be positive. Daily fluctuations that can reach up to 30% for Bitcoin, as mentioned in section 2.7.1 Bitcoin, show how unreliable Bitcoin is as a store of value. The exception to using cryptocurrencies as a store of value is if economic uncertainty is considerable high. A country suffering from hyperinflation or a country without basic infrastructure could be such examples. This is explained further in section 6.8.1 Cryptocurrencies Demographically.

A unit of account

The third function of money is unit of account. To begin with, prices in the store is not displayed in cryptocurrencies. This signals the notion that cryptocurrencies are not a unit of account. According to Ali et al. (2014), they are not aware of any businesses that accepts the most used cryptocurrency, Bitcoin as a payment who also maintains its accounts in Bitcoin. However, if goods and services would be denoted in cryptocurrencies, it could to some degree be unit of account. Nevertheless, for cryptocurrencies to function as a unit of account, they must be able to be used as a medium of exchange by several people, in a variety of transactions, over time. If we cannot establish cryptocurrencies as a medium of exchange, it cannot be a unit of account either. Therefore, we would argue that cryptocurrencies do not currently fulfill the role as a unit of account.

5.2.2 Characteristics of Money

Recalling the characteristics from section 2.4 Characteristics of Money and if we try to evaluate the cryptocurrencies with what has been established as criteria for money, we will get a better idea as to the suitability of cryptocurrencies as money. In terms of durability, cryptocurrencies are not in physical form and satisfy the need for durability. This reduces the cost of producing more money, but work the same way as money in bank accounts.

Portability is also a criterion cryptocurrencies fulfill as they are digital and can be moved around in large quantities relatively effortlessly. We also know from section 2.7.1 Bitcoin that one Bitcoin can be split into one hundred million of smaller pieces. This ratio of divisibility varies among the cryptocurrencies and, therefore, shows that cryptocurrencies exhibit the characteristic of divisibility. Stability of cryptocurrencies is, however, a problem due to the high volatility. It may look implausible for cryptocurrencies to exhibit the stability required of a large scale currency, due to the present small market capitalization, relative to the global money supply. It is shown that, for instance, banning cryptocurrency in a country creates volatility and instability. On the other side, a more mature cryptocurrency may have a larger market capitalization and can become more predictable which can lead to the required stability. With regard to the fifth characteristic of money, cryptocurrencies are scarce as there is a maximum number that may be issued. In terms of acceptability, cryptocurrencies are slightly lacking to meet this characteristic of money. As mentioned earlier in section 5.2.1 Smith's Definition of Money, cryptocurrencies are gaining acceptability among merchants, but at the same time, cryptocurrencies are not and perhaps will not be the preferred daily payment option. Based on these six criteria, cryptocurrencies partly work, but do not work sufficiently to get adopted as a large scale payment system. Naturally, this is a very simplistic way of evaluating cryptocurrencies and does not account for what cryptocurrencies may or may not develop into in the future. This list of characteristics is also not all-encompassing, meaning there are certainly aspects unaccounted for with these six characteristics. For instance, the immutability of the transaction records is not accounted for by the characteristics. Nonetheless, the framework provides a basis for evaluating some criteria of money.

In the interview with the representatives from financial infrastructure, they emphasized the criteria needed for a currency to be employed in large-scale payment system. The criteria are as follows:

1. Cost efficient
2. Cheap
3. Fast
4. Secure
5. User-friendly

Cost efficient in this context is from the issuers of the currency, i.e central banks. Cheap is in relation to the users of the payment system. A payment system that is either expensive to run for the issuers or expensive to use for the payees is not cost efficient or cheap. If we use these criteria proposed by the representatives from financial infrastructure to evaluate a cryptocurrency like Bitcoin, it is questionable if cryptocurrencies are suitable as a means of payment. Hence, Bitcoin is proven not to be cheap and cost-efficient. In addition, is is slow compared to the traditional fiat money system and other cryptocurrencies. Ripple however, features faster payment system and is more cost efficient compared to Bitcoin. The consensus function in Bitcoin of 51% can cause mining pool problem; the cryptocurrency might not even be secure in terms of majority consensus, which will be further explained in section 6.5 Transacting with Blockchain. Ripple however, is more secure with 80% consensus in the network. Controversially, in terms of counterfeiting or hacking, cryptocurrencies block structure cannot be altered, but their storage can which presented in section 6.4 Security. Although, cryptocurrencies are secure, the additional services such as storage has the potential to ameliorate. User friendliness can be debated, but cryptocurrencies require a certain amount of equipment and technological understanding in order to be used in transactions. Thus, not everyone can easily transact with cryptocurrencies. Bitcoin is the most-accepted cryptocurrency but the venues where one can use Bitcoin as a means of payment are limited. Therefore, from the standpoint of large-scale financial infrastructure, cryptocurrencies are questionable to be suitable as a payment system at this time.

The representatives from financial infrastructure note that, although we may not see a full-scale payment system based on cryptocurrencies, they may fulfill a role as a niche means of payment:

> *"...these are criteria set forth for a large-scale payment system. And if cryptocurrencies are to be used for such a purpose, these criteria must be met. Right now, cryptocurrencies are more suitable as, perhaps, niche means of payment where not all of the criteria is met... "*

An example of such a niche transaction could be a transaction to a country with weak banking system and high levels of corruption which we will discuss further in section 6.8.1 Cryptocurrencies Demographically. This is because the peer-to-peer system would effectively ignore the financial intermediaries.

5.3 Central Bank Digital Currency

There have been debates if a country will issue a Central Bank Digital Currency (CBDC), but there seems to be no country in the developed world who has done so. Interviewee #1, the representatives from financial infrastructure, described cryptocurrencies' role and what was important to ensure for central banks:

> *"... cryptocurrencies can potentially, while not currently, threaten financial stability if*

cryptocurrencies are being used a lot and end up on the banks' balance sheet, either directly or indirectly, e.g by individuals taking up a mortgage to buy a cryptocurrency or by finance institutions using cryptocurrencies as interbank payments."

Furthermore, the representatives from financial infrastructure explains that central banks are concerned about not surpressing the innovation, in addition to possible efficiency effects, by regulating too much, as will be further explained in section Regulation 6.3. The representatives from financial infrastructure continue:

"The central bank does not have an agenda for a cashless society. We think this should be a decision for the general population."

Thus, the central banks in the North of Europe are dedicated to maintaining the payment method the population prefers, and they do not have plans of removing cash in near future. However, it is maybe natural that central banks are conservative. This could also be due to them trying to represent a conservative population as most people do not like change.

In addition to what is written in section 5.2.2 Characteristics of Money, cryptocurrencies today are still not and are probably not going to satisfy the central banks' criteria in the near future. Yet, if cryptocurrencies would develop towards satisfying the government and population's needs, we may see cryptocurrencies playing a bigger role in the economy. For the short term, however, cryptocurrencies will probably mainly work as a minor currency in niche segments.

Contrary to the argument that cryptocurrencies do not fit the criteria for money, as mentioned in section 5.2.1 Smith's Definition of Money, people that live in countries with unstable governments and political turmoil, have reasons to adopt cryptocurrency. An example of a government based cryptocurrency is Venezuela, a country currently struggling with hyperinflation (Hanke, Bushnell et al., 2017). Venezuela has issued a cryptocurrency, the PETRO, which is backed and can be exchanged for reserves of oil, gold, or diamonds. As we have limited the thesis to the most popular and cryptocurrencies in general, we will not go into Venezuela's Petro. However, doing a Google search on 9^{th} of June 2018 about "petro venezuela" displays "Crypto Rating Sites Are Already Calling Venezuela's Petro a Scam" and "Crypto Investors Should Stay Away from Venezuela's Petro - CoinDesk" as the second and third post, after Wikipedia. As such, we see there is some public skepticism. The representatives from financial infrastructure were critical towards a government based cryptocurrency, yet, a government based DLT was plausible, but not in near future. Other central banks have displayed an interest in issuing digital money, but not necessarily based on cryptocurrencies. In interviews with representatives from financial infrastructure, they stress that digital assets issued by the Norwegian Central Bank may or may not have elements of DLT, and a digital system may be more aimed towards classical electronic money, rather than a currency based on Blockchain technology:

> *"It could contain elements of DLT, but it does not have to. I think most central banks considering DLT realize it is not feasible in the near future."*

After all, central banks do not control cryptocurrencies as they are private. This warrants a look as to how commercial banks are treating cryptocurrencies. Statements from bank executives like Jamie Dimon calling Bitcoin as a "fraud" (Son, Levitt and Louis, 2018), but that the underlying technology, Blockchain, has some apparent advantages they wish to investigate. Commercial banks, as well as other businesses, have adopted Blockchain projects and are looking into what benefits can come from this new technology. Several central banks have diminished cryptocurrencies as money and deem it not a currency, but a speculative investment.

6 A New Payment System

In the following section we aim to analyze features of cryptocurrencies. We begin with looking at the privacy and criminality surrounding the use of cryptocurrencies, following with regulation and security. We will then take a closer look at transactions with blockchain technology, its limitations and improvements. Next, we break down fiat money and analyze the assumptions. Finally, we look at cryptocurrencies in the future, by investigating the demography and potential usage for cryptocurrencies. The aim with this section is to analyze cryptocurrencies, its potential and if there is a place for cryptocurrencies in the future. This helps us to evaluate if the expectations about the price today reflect cryptocurrencies' features and in which way it is reasonable the price will develop further.

6.1 Privacy

The underlying technology which allowed for the first modern cryptocurrency, Bitcoin, to exist is blockchain technology, as mentioned earlier. Contrary to popular belief, Bitcoin is not completely anonymous (Halaburda, 2016*a*). Bitcoin is pseudo-anonymous, meaning that a user's identity can be tracked through a person's pseudonym (Buybitcoinworldwide, 2018*b*; Nakamoto, 2008). Article by Lab (2017) points out the disadvantage about the public ledger. After two individuals have transacted, both know each other's pseudonym and can see all historical transactions the other individual has done. If these pseudo-anonymous cryptocurrencies would be a large-scale payment system, there would be a challenge with privacy. For instance, there would always be someone that would find celebrities', or politicians pseudonym. On the one hand, this can be a preventative measure against corrupt politicians. On the other hand, it would violate a public individual's personal life. In addition, privacy is a fundamental human right (United Nations, 1948) and the large amounts of transactions data that is available risk the potential of being misused. This means that there is often a trade-off between anonymity and public information. There are other cryptocurrencies with strengthened focus on anonymity, such as Monero (Saberhagen, 2013), where it becomes more difficult to connect a person's pseudonym with actual identity. However, the way to transact is not well-understood and, thus, results in less privacy than most people think (Bheemaiah, 2017). Interviewee #7, a mathematician and cryptographer, explains the cryptography behind Bitcoin:

> *"Bitcoin, the most famous of the original modern cryptocurrency, [...] uses quite simple cryptography that we have known about for quite some time, but it is just the way it puts things together that is [...] think it is fair to say not still fully understood."*

Sedgwic (2018) criticize Monero and Zcash for not being that anonymous as promised. Zcash is by default not anonymous, where one needs to activate the anonymity, resulting in 85% of the transactions not being shielded and becoming easy to track. Monero has not received criticism about the anonymity problem until recently, where Möser, Soska, Heilman, Lee, Heffan, Srivastava et al. (2018) investigated the traceability in the Monero blockchain (Sedgwic, 2018). There are two weaknesses in Monero's mixin selection policy[6] which pose significant risks in traceability, especially for old transactions. Some suggests cryptocurrencies should merge with a centralized management system[7] in the future, while others continue to support decentralization (Bheemaiah, 2017).

6.2 Criminality

The dimension cryptocurrencies offer to the crime world is entirely new, where individuals can sit at home and have illegal goods delivered at their doorstep and pay using cryptocurrencies, never seeing the other person. This shift towards digital drug crypto-markets, as opposed to physical trade, decrease the likelihood of violent outcomes (Morselli et al., 2017; Heaven, 2018). In other words, digital drug trade leads to less violence than physical drug trade. However, a market, where the transactions are being exchanged without a third-party like a bank are more difficult to regulate difficulties. This is akin to cash transactions which are also anonymous by themselves (i.e law enforcement will not know when cash exchanges hands.) Being able to make remote cash transactions, so to speak, is the new side of financing criminal transactions that cryptocurrencies has brought about with their peer-to-peer characteristics. Due to cryptocurrencies' superior anonymity to digital payment methods influenced by the government, cryptocurrencies work well to avoid authorities. The anonymity and decentralization make some cryptocurrencies especially attractive to criminals (Brown, 2016). Some cryptocurrencies focusing on privacy and anonymity claim to be absolutely untraceable, making crimes related to these cryptocurrencies particularly troublesome (Saberhagen, 2013). However, as seen before, cryptocurrencies with special focus on privacy have successfully been traced. Foley et al. (2018) estimate that one quarter of Bitcoin transactions, half of its users are connected to criminal activity and that illegal activity is a driver for the value of Bitcoin. If we are to trust the rough estimation made by Foley et al. (2018), and we assume cryptocurrencies with a higher focus on anonymity are more prevalent in criminal transactions, we get a rough idea of how widespread the use of cryptocurrencies is in criminal transactions. Having cryptocurrencies that are heavily influenced by illegal trade is prob-

[6]Javascript defines mixin "mixin provides methods that implement a certain behavior, but we do not use it alone, we use it to add the behavior to other classes." Available at: https://javascript.info/mixins

[7]Bheemaiah (2017) provides a list of private companies that provide services to blockchain, in addition to a brief explanation of their business.

lematic at several levels. The first aspect is the ethical considerations that might discourage investors who are concerned about their investment value not being derived from illegal activity. The second aspect to consider is the emergence of more anonymous cryptocurrencies negatively affecting the value of the more transparent cryptocurrencies, as a substitute effect, if illegal activity is a strong driver of value. Moreover, the article by Foley et al. (2018) find that the price growth prior to the paper being released in January 2018, does not reflect the increase in illegal use of cryptocurrencies. Our interviewee #7 presented the following about the illegal usage of cryptocurrencies:

> *"There has been an increase in criminals using cryptocurrencies, but this share has, as a total, been decreasing due to so many others joining the market."*

Thus, anonymous or pseudo-anonymous payments are not necessarily synonymous with criminal activity. However, tracking transactions becomes more difficult as the cryptocurrencies become more developed, and according to Europol, they notice a shift toward the cryptocurrencies with more focus on anonymity (Europol, 2017). We can assume that as long as the probability of being caught does not approach zero, the illegal use of cryptocurrencies will not outgrow law enforcement capabilities. In other words, as long as law enforcement of the illegal use of cryptocurrencies is effective, that in itself is a deterrent. Interviewee #7 claims that tracing illegal transactions has helped a lot by the fact that the transactors make poor attempts at hiding their tracks.

> *"And we see individuals who do not understand that in order to transact anonymously with cryptocurrencies, one has to anonymize all the transactions - it is not enough to anonymize almost all transactions due to how the technology works."*

On top of law enforcement capabilities is a debate of whether law enforcement wants users to conduct their transactions using cryptocurrencies, as opposed to cash. With effective countermeasures, it is likely that law enforcement will continue to keep relative control of the economic crime resulting from the use of cryptocurrencies. In terms of law enforcement and regulation, an important factor is which direction lawmakers want the use of cryptocurrencies to take. One option is to make attempts to suppress the use of cryptocurrencies altogether, or law enforcement can focus more on combating these digital transactions with digital monitoring themselves. With digital monitoring, there is an opportunity to track a larger volume of transaction with more effective use of resources.

6.3 Regulation

For a financial system to be fair and stable, it is crucial to enhance regulation and legislation. Few countries have taken a stance towards cryptocurrency regulation where some of them are outlined below. Work of getting new anti-money laundering (AML) laws in place are under work in the European Union. The newest addition to AML legislation is the fifth EU Anti-Money Laundering directive (European Commission, 2018). This directive is for EU countries, but as interviewee #7 pointed out, these types of directives typically translate into laws for non-EU countries as well. However, as cryptocurrencies are developing rapidly, the regulation and regulators are largely retroactive in their work. A regulation that is too extensive might also hinder innovation and growth. The interview object #1, the representatives from financial infrastructure, made the following statement about such regulations:

> *"This is a technology under development and it is important not to stifle innovation, and effectively killing any potential cryptocurrencies or what the underlying technology can provide. So, one needs to be careful with regulation"*

While encouraging innovation, it is also important that regulations help law enforcement in their work. It is, therefore, difficult to determine what should be an appropriate regulation, and this line will most likely be drawn differently from country to country. For instance, countries currently struggling with monetary policies, like Venezuela, are likely to have a different stance on cryptocurrency regulation than more stable nations like the US. There are some countries which are in favor of cryptocurrencies, like Switzerland, to countries like China which oppose cryptocurrencies altogether (Glotov and Mihailov, 2018). China has earlier clamped down on cryptocurrencies, banned ICOs, halted exchanges, and forced miners abroad. In March 2018, Yi Gang was appointed the new governor for the People's Bank of China (PBoC), the central bank of China. Yi Gang has reaffirmed the PBoC's previous statement about maintaining strict overview of cryptocurrencies as capital control intensifies (Mitchell and Clover, 2017), but that China is exploring options for using digital currencies to support the real economy and wishes to remain globally competitive within blockchain innovation and adoption. McMillan LLP, a Canadian business law firm, published a report outlining the regulatory stances of Canada, USA, and China. The report shows that the US is taking stricter stances to regulation, by defining cryptocurrencies as securities and, thereby, applying its regulatory framework to cryptocurrencies (Kent and Sasa, 2018). There does not seem to be a clear consensus as to where the regulatory line should be drawn. Therefore, there might be a transition period where cryptocurrency companies and transactors move to countries with more favorable regulations.

Cryptocurrencies also emerge in a period where large legal changes are currently taking place.

The General Data Protection Regulation (GDPR) and Revised Payment Services Directive (PSD2) are both introduced and expected to be fully implemented in 2018: PSD2 in January and GDPR in May. PSD2 is a EU-directive said to "disrupt payments in Europe". When PSD1 came out, it allowed for non-bank entities to perform pure payment services. Under PSD2, these institutions can perform these services on behalf of the customer. Payment services can also be performed without cards or online banking under PSD2. Therefore, this is particularly a directive where cryptocurrencies may gain some traction. GDPR relates to privacy and puts pressure on companies and how they collect and store consumer data (Jackson, 2018*a*). GDPR is a regulation and not a directive, meaning it will go in effect in its entirety and does not have to be translated into legislation in countries like the United Kingdom. This means that there will be a uniform GDPR compliance framework. However, PSD2 is a directive or a goal and will, therefore, be translated into law for all EU member countries for how to reach those goals, meaning that the laws will be different between countries (European Union, 2018). Companies who do not comply with GDPR could face fines up to 20,000,000 euros or 4% of global annual turnover, whichever is higher. However, PSD2 was passed in November 2015 and was likely not intended for cryptocurrency providers at the time when the total market cap of all cryptocurrencies was approximately 5 billion US dollars, compared to the market capitalization of over 400 billion US dollars as of May 1^{st}, 2018 (CoinMarketCap, 2018).

Regulations are central when it comes to price stability. A regulation, depending on the scope, can damage the cryptocurrency price short term and investors suffer losses. It is unlikely that cryptocurrency will be affected long term, as long as there is no collective ban. It is assumed there will not be such a ban because innovations are a central part of the economic growth. Furthermore, it is reasonable to believe that regulating cryptocurrencies can enhance their stability, which can improve their suitability to the money definition and characteristics mention earlier.

6.3.1 Initial Coin Offerings

One area that can be expected to see more regulation in the near future is within the Initial Coin Offerings (ICOs). TokenData is one of the more comprehensive ICO trackers, and shows that 59% of all 902 crowdsales in 2017 were either failures or semi-failures (Tokendata.io, 2018). ICOs are unregulated, and although an effective way of raising capital, they have proven to possess fatal flaws at times, costing the investors a lot. One example of this is Pincoin, which in April 2018 raised more than $660 million US dollars from 32,000 investors and then disappeared with the money (Tech Crunch, 2018). Such an example shows that the lack of regulations is overdue. Due to significant differences between countries and how cryptocurrencies are being treated, it is expected that the legislation will vary until cryptocurrencies are better understood. Countries will have a challenging task creating regulation that encourage innovation while also protecting individuals and companies. However, we conclude that ICOs should be more regulated than they are today, as the ICO regulation today allows for little documentation of the coin offering, along with a lot of regulatory gaps (Jackson, 2018*b*). Retrospective regulation in response to major flaws like Pincoin might not be optimal as the technology is developing at a rapid pace and one cannot effectively cover the regulatory gaps that exists within the cryptocurrency market by being retroactive. Regulating the ICO industry more may affect the emergence of new cryptocurrencies, but regulation will also limit the amount of fraudulent actors in the industry. In addition, an ICO regulation will reduce the downgrading reputation that ICO scams have caused in relation to cryptocurrencies in general. Therefore, while proactive regulation must be used with caution, such proactive regulation should be implemented towards ICOs. This type of regulation would decrease scam, protect the serious innovators and established cryptocurrencies.

6.4 Security

One security element required for transacting is a digital signature as shown in Figure 4 in section 2.7.1 Bitcoin. In addition to digital signatures, blockchain may use hash chains. Hash chains are pieces of information, where each piece is a product, or hash, of the previous piece. This makes it connected to the hash before, forming a chain (Bicakci and Baykal, 2002). Blockchain is a data structure which is immutable through these hash chains. To change the information added last to the chain, one would have to alter the previous piece of information and the one before. Such alterations can be done to a hash chain that is stored at a centralized location, but the decentralization of blockchain is what ultimately makes blockchain immutable. An alteration would have to be done to 51% of the network, which is spread throughout the world at thousands of devices. In section 6.5 Transacting with Blockchain, we will explain this in more detail. To conduct a simultaneous hacking attempt to 51% of the network is eminently unrealistic to that point that information stored in the Blockchain is considered immutable. Therefore, although cryptocurrencies cannot be hacked, cryptocurrency storage can be a central point of attack. For instance, the digital wallets where cryptocurrencies are stored have been reported to have 'been hacked at multiple occasions (Carmona, 2015). Besides wallets, hackers can attack other central store points like exchanges or companies storing cryptocurrencies. Therefore, similarly to bank accounts, Bitcoin wallets are subject to hacking attempts. In addition, losing the key to a wallet would cause a permanent loss of the coins and the coins can never be found. However, banks typically have deposit insurance where losses up to a certain limit are guaranteed by the bank (Diamond and Dybvig, 1983). Due to the lack of regulatory framework, such insurance does not exist for cryptocurrencies and one faces the risk of losing the invested value with no chance of redeeming one's loss (Coinbase, 2018)

6.5 Transacting with Blockchain

Upon conducting the interviews, we present the respondents with cryptocurrencies' suitability as a method of payment by asking what would have to be improved for cryptocurrencies to be a fully-fledged currency. Two factors are surfacing: the transaction time and the cost of transacting. To illustrate, we use the most accepted cryptocurrency Bitcoin. Intended as a method of payment, Bitcoin cannot process a lot of transactions, as mentioned in section 2.7.1 Bitcoin. VISA, on the other hand, process an average of 1,700 transactions per second and PayPal 115 transactions per second (Seigneur et al., 2017). This is one of the drawbacks of Bitcoin which does not make it suitable as a medium of exchange. Some transactions have been reported to have exceeded 11 000 minutes, or almost 8 days, and the transaction time is fluctuating as shown in Figure 18 (Blockchain.info, 2018). There are other cryptocurrencies with improvements to the transaction speed such as Ripple, which is mentioned in section 2.7.2 Ripple since it processes 1500 transactions per second. However, Bitcoin is the most used cryptocurrency and, therefore, a central point of discussion.

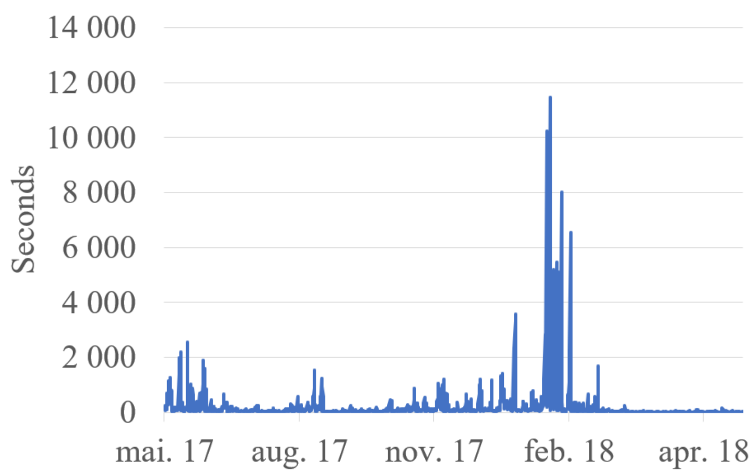
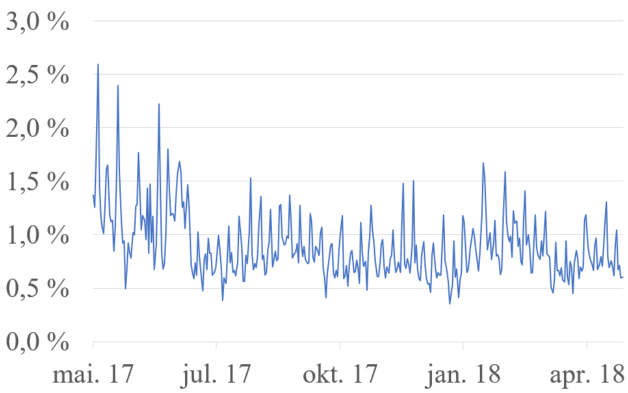


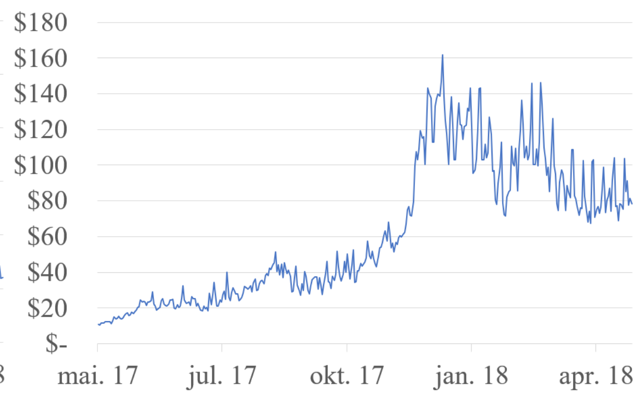
Figure 18: Average Confirmation Time at Specific Dates

The method of verifying transactions made in Bitcoin is also demanding in terms of resources. According to the Bitcoin Energy Consumption Index (BECI), the electricity cost for mining Bitcoins is estimated to be in the excess of 64 Terawatt-hour (TWh) as of May 1*st*, 2018 (Digiconomist, 2018). This electricity consumption is above to that of Switzerland, according to the electricity consumption report made by the Swiss Federal Office of Energy (SFOE)

(Admin.ch, 2018). By the end of 2018, the electricity cost could reach that of Austria, equal to 0.5% of the world's electricity consumption (de Vries, 2018). This may be unsustainably high. The high electricity cost of verifying transaction means that if one wishes for their transaction to be prioritized, fees must be offered. This fee structure has been increasing, both in absolute values and as a percentage of the transaction value, as shown in Figure 19 below (Blockchain.info, 2018).



(a) Cost as a Percentage of Transaction



(b) Transaction Cost in USD

Figure 19: Historical Costs of Transacting with Bitcoin

Interviewee #7 also noted that high transaction fees has become a topic even within the criminal environment, which law enforcement monitors to keep track of criminal trends:

> *"What has happened the last year is that the fee for each transaction has become so high that even criminals react to the disproportionately high transaction fees."*

As a result of high fees, micropayments are not attractive to be made with cryptocurrencies due to their abnormal size of the total transaction. The costs of transactions bring about a plethora of other challenges. The most significant issue is that mining of blocks today is done by large mining pools, which essentially means that the distributed network is becoming centralized and the validation of transaction can be falsified by someone who controls 51% of the network. An example of such centralization has happened before, the mining pool GHash.io voluntary reducing its pool size upon consisting of more than 51% of the Bitcoin mining pool (Bastiaan, 2015). Therefore, the whole notion of decentralization is endangered as a result of the computational pooling and could be an indicator cryptocurrencies no longer being able to perform its intended purpose. If one can no longer be certain that cryptocurrency transactions are secure, the currency stands to potentially lose a lot of value. Table 4 demonstrates the mining pool distribution on June 10*th* 2018. This table shows the top three mining pools potentially achieving the consensus majority discussed earlier. Therefore, there is the possibility of majority pooling.

Table 4 Five Largest Bitcoin Mining Pools as of 10^{th} June, 2018

#	Name	Market share of mining pool
1	BTC.com	27.1%
2	AntPool	14.9%
3	SlushPool	9.5%
4	BTC.TOP	9%
5	F2Pool	9%

6.6 Improvements

The previous arguments are the most commonly used against Bitcoin as a method of payment, but solutions are in the process of developing. Interviewee #5 noted that one solution to the transaction speed is by implementing Lightning Network which is a payment protocol added on top of a blockchain (Poon and Dryja, 2016). This lightning network will limit the transactions that get validated on, for example, the Bitcoin blockchain and, thus, increase the transaction speed. By using lightning network, a side channel will be created where settlements between two parties will be done. When the side channel is closed, the final balance of the two parties will be what is recorded in the blockchain ledger. Therefore, two parties can make as many transactions as they like and the final balance will be recorded, effectively making many transactions into two: one transaction to open the channel and one to close it.

Secondly, the high electricity costs come from the current consensus system, called proof-of-work. One proposed improvement to PoW is proof-of-stake (PoS). Interviewee #6 noted that under the current proof-of-work (PoW) consensus system, the entire network of miners works on verifying transactions and adding blocks to the network. Under PoW, the entire network is essentially competing against one another, wasting enormous resources. Instead, the proof-of-stake model will select a random validator in the network who will perform the validation (Kiayias et al., 2017). Each validator in the network will have to place a certain amount of money, a stake, in the network as a security deposit. The size of the stake determines the chance for the validator to be selected. This would make certain that the validator would not wrongly validate a transaction as that validator has a financial stake in correctly validating the transactions and adding the block to the blockchain. If the validator wrongly verifies a transaction, the stake is forfeited. There is a wait time for when the system accepts the validation so that a participant cannot utilize a momentary split in the chain, which is possible as shown in Figure 2 in section 2.6 Blockchain above. Arguably, the chances of being picked under PoS favors the resourceful, but this is no different from the PoW, where the resourceful data centers are the ones who capture the most of the mining rewards (King and Nadal, 2012). Therefore, this is not an argument against the PoS consensus system.

6.7 Assumptions of Fiat Money

Cheung, Roca and Su (2015) claim that cryptocurrencies have no intrinsic value and that the price mainly depends on its speculative value. It is also argued that the speculative value is based on the blockchain technology and it is claimed to be a Ponzi-scheme (Vasek and Moore, 2015). Similarly to cryptocurrencies, fiat money have no intrinsic value, but maintains its value due to a few aspects mentioned below. We will focus on these aspects to separate fiat money from cryptocurrencies: centralization, inflation targeting, and trust.

6.7.1 Centralization

One of the advantages cryptocurrencies were designed to offer was decentralization. Although decentralization is not an innovative disruption, it has not gained such popularity in modern times until Bitcoin was introduced and became a widespread digital alternative to the traditional intermediary transactions (Kaushal, 2016). Banks have existed as financial intermediaries since around the third millennium BC; a system that has been in place for a long time, with transactions between Babylonians, Assyrians, and other nations of Asia Minor on record (Davies, 2002). Changing the fundamental centralization of a system that has such strong roots, and financial interests, to a decentralized system can understandably be met with a certain level of resistance. This resistance can also have its roots in those who profit from the current system and are not eager to see more competition. However, a centralized top-down system with its new tools of data management can increase polarization and conflict, and more specifically corruption, hackers and extremists, among others (Helbing and Pournaras, 2015). The technology behind cryptocurrencies today can support decentralization of payments in, supposedly, a superior way. The advantage of decentralization is also the removal of a third-party or intermediary, but the drawback is that the responsibility for the system does not lie with one person or entity. In other words, a centralized structure also leaves a central point of authority in case of the system not working.

Whether the popularity cryptocurrencies display comes from its proposed superiority as a payment system, or from a dissatisfaction with the stricter nature of the traditional payment systems, is not yet certain and could be mix of both. Interviewee #2 note that the decentralized aspect of cryptocurrencies was not the most attractive aspect of cryptocurrencies upon first-glance:

> *"... being free from government control etc. was not at all attractive. In fact, it struck*

me as more than a bit idealistic and I think that is still the case."

There is little research indicating that a decentralized monetary system works better than the current system in place, or the other way around. Based on the statement of ideology, we do not know whether it is feasible to implement a decentralized system the way we are currently transacting: with centralized financial intermediaries being such a central point in the economy. However, it is likely that the challenges of centralization mentioned above from article Helbing and Pournaras (2015) can be improved by decentralizing the fiat system, thereby making a more democratic society as mentioned earlier. This would more likely prevent those challenges. The centralization of the money system might be faced with a certain degree of decentralization in similar way as PSD2 with its breakdown of banks information monopoly system. This way of a decentralization system requires a long transition period, but the sudden popularity can be a sign that the population wants some change to the centralized system. As written in 5.1.3 Redefining Fundamental Value, cryptocurrencies exhibit characteristics of centralization which is probably one of the reasons for the popularity of Bitcoin. Thus, there are no clear answer to the question of the degree of centralization/decentralization there should be, but it is certain that the system cannot be fully one or the other. It is therefore reasonable to say that the decentralization of cryptocurrencies should not be the main argument for cryptocurrencies taking up a larger role as a payment system.

6.7.2 Inflation Targeting

As written in section 2.1.2 Fiat Money, a great risk to fiat money is high inflation. At the end of the twentieth century, after a long period of unstable economy, regulations were loosened up, creating private enterprises and free markets. Thus, the government plays an important role in creating the conditions that give the power of the market free reign. Monetary policy with inflation targeting is one of the essential features of the government, where the goal is to maintain a low and stable inflation to enhance market driven growth (Bernanke, 2001). Inflation targeting refers to making sure a consistently low inflation results in economic growth and higher employment rate. However, setting the market free has given rise to dominant corporations where the rich get even more rich. As such, it is a shown tendency that the capitalistic system is in favor of the rich, where they nourish on the poor (Facchini and Couvreur, 2015).

Looking back at history may not provide suggestions for a better alternative, with high unemployment, slow and stagnating economies. Even though the capitalistic system is the best-known alternative for economic growth (Bheemaiah, 2017), it is not necessarily the optimal one. As many cryptocurrencies issue a fixed number of new coins, cryptocurrencies constantly increase in size, similar to fiat money with its inflation. Predicting how the economy functions with cryptocurrencies as the primary payment method will be mainly speculations, but as long as it continues being a free market, it seems unlikely that it will dramatically change the capitalistic system. Moreover, a central bank can adjust its monetary policy using a mixture of contractionary and expansionary tools. It is crucial to prevent large cycles and to bring the economy back on track, thereby avoiding even larger recessions. However, cryptocurrencies cannot adjust economic cycles via similar tools as with fiat money. This would be a weakness in the case of cryptocurrencies constituting the majority of the payment system. However, monetary policy can be altered by political and personal gain under the fiat monetary system, but not for cryptocurrencies. As one cannot influence cryptocurrencies the same way, cryptocurrencies can be an advantage as a niche payment. While cryptocurrencies are not regulated through monetary policy in the same way as fiat money is managed, the features of cryptocurrencies such as money supply are coded into the blockchain and leave cryptocurrencies largely immune to hyperinflation (Darlington III, 2014). As mentioned earlier, there are no constraints on the money supply with fiat money and, thus, hyperinflation could be a valid concern. Unconstrained money supply is the main strength and weakness of fiat money. However, having cryptocurrencies as an additional currency becomes attractive as they are largely immune towards hyperinflation. Hyperinflation was not an issue for commodity money where the supply of the pegged resource was limited, but this would also not allow for the money supply to grow (Hoppe, 1994). Similarly to commodity money, Bitcoin might cause a stagnating economy as well, when no more coins can be mined after 2040.

6.7.3 Trust

The fiat currency's value depends on peoples' trust, but trust is not constant over time. As the saying goes, trust takes years to build, seconds to break and forever to repair. There has been growth stagnation in the past, when the development has been slower, less volatile and hence more predictable due to fewer disruptions. Therefore, with the rapid development today, introduction of new technology may cause a greater risk of instability in the economy than we have seen earlier (Jacobs and Mazzucato, 2016). Instability in the government or economy can lead to reduced trust in the monetary system, directly affecting the value of fiat money. With cryptocurrencies, however, the system is slightly different as the government cannot endanger the trust in cryptocurrencies to the same extent as with fiat money. Contrary to fiat money, the technology behind cryptocurrencies is secure and immutable, making the system more robust and, therefore, people could potentially have more trust in the system. These abilities looks similar to commodity money in the sense that there are actually something "physical" to believe in. Regardless, the trust comes down to peoples' trust in being able to use the money elsewhere, which essentially boils down to the definition and characteristics of money. At this time, cryptocurrencies to a large degree do not satisfy such conditions, which results in less trust in cryptocurrencies. This lack of trust will be the foundation of high volatility, that makes cryptocurrencies less suitable as money, resulting in a vicious circle.

Having a fiat currency "backed" by trust seems to work for some countries in the world at the present time. In other developing countries such as Venezuela, people struggle to trust the fiat currency. So, this may not be the optimal long term solution, as it is likely more crises can become reality which can damage the trust also in developed countries and worsen the situation in developing countries. Cryptocurrency technology may help to enhance a better and more long term stability in the world economy overall as the technology is reliable. However, with the historically high volatility, cryptocurrencies does not contribute to the stabilization today, but with the rapidly changing technology, cryptocurrencies might optimize some parts of the world economy in the future. Controversially, as one of the likely reasons for cryptocurrencies lately success is economic growth (United Nations, 2018) and as long as trust is lacking, cryptocurrencies may risk a substantial setback if the economy goes into a recession.

6.8 Cryptocurrency in the Future

A totally new and not yet established intangible financial entity cannot easily be forecast. Interviewee #2 explained that when he first became interested in cryptocurrencies in 2012, he thought the technology would move in other directions than it has. He believed that international transactions would be cryptocurrencies' main usage, but its popularity and ambitions have developed beyond only international trading. As stated earlier, cryptocurrencies has been steadily increasing in popularity since 2012 and it show signs of being in early market stages (Reed, Sathyanarayan, Ruan and Collins, 2018). Early stage technologies are particularly difficult to forecast (Parr, 2018). However, several of the interviewees are confident that cryptocurrencies have come to stay in the future at which we will have a look in this section. First, we start by analyzing how cryptocurrencies are traded around the globe. Finally, we present where cryptocurrencies are likely to be adopted in the financial market.

6.8.1 Cryptocurrencies Demographically

The development in first world societies strives towards more digital products and services. With the declining trend of cash in developed countries, it is possible that physical cash eventually will cease to exist. However, in third world countries, cash is still used by the majority (Demirgüç-Kunt et al., 2018). As money in large parts of developed countries is already digitized, it is likely that the trend will continue to spread to the rest of the world. Moreover, cryptocurrencies have an advantage as digitized products are continuing to emerge, hence the survival of cryptocurrencies depends mostly on its characteristics and the further development (Stevis-Gridneff and Kantchev, 2018).

Some developing countries face unstable currencies, political and economic turmoil. These countries are looking for other places to deposit their value, and Bitcoin is often viewed as a haven for people living in countries with unstable governments. Thus, Bitcoin has been an alternative when the currency in frontier markets fails (Stevis-Gridneff and Kantchev, 2018). On of the arguments is if people do not have trust in their fiat currency, cryptocurrency may prove to be a better alternative. Nonetheless, there are reasons to be critical towards the source as the arguments presented seem shallow. These arguments do not explain the emergence of Bitcoin in developed countries, in addition to the fact that there might be other factors to why there has been a sudden increase in Bitcoin usage during 2017 and not only the turmoil in developing courntires.

The popularity in developed countries can, for instance, be due to speculations and media, among other factors. This may also be the case in developing countries. Although the critisism, cryptcurrencies may still be a better alternative when the fiat money faces instability. When looking at conversions into cryptocurrencies by countries, the majority of transactions come from developed countries (CryptoCompare, 2018*b*). Thus, there are parts of the world that have not adopted cryptocurrencies yet. Meaning there are potentials for cryptocurrencies in developing countries with economic turmoil, and especially if cryptocurrencies would become more stable.

6.8.2 Potential Areas of Usage

The interviewees seemed to agree that cryptocurrencies will still exist in the future, but that the number of cryptocurrencies enduring will be limited to a handful. Barry Silbert, the CEO of the cryptocurrency holding company Digital Currency Group (DCG), shares the same belief. He states that most of the tokens do not have utility and will probably disappear in the future. The ones that do survive will be in the most needed niche segments. Examples of such niche segments are privacy-based tokens, a token for gold and a smart contract platform. However, this may be done on one single platform, but at this time, the relative complexity of different technologies behind tokens makes it extremely difficult and time-consuming to combine such tokens on one single platform. Furthermore, it is questionable if it is even possible in reality. The development of cryptocurrencies can be described by the network effects, where it is easier for consumers to use the same platform if others use it as well, making it unnecessary for several almost identical cryptocurrencies to exist (Halaburda, 2016*b*; Shy, 2001). These network effects tend to favor the first-movers (Gandal and Halaburda, 2016) and we see that the first mainstream adopted cryptocurrency is Bitcoin which is also the largest cryptocurrency. However, there could be ways of easily converting between cryptocurrencies, which would cause the network effects to diminish; this point is made by interviewee #3. Yet, there would be currency risks when transferring between different coins, and if one always had to convert into the most-used coins, individuals would probably only hold these coins, making others obsolete.

Loyalty Points

Interviewee #3 explains three potential places of usage, where the first is the following:

> *"...so that is kind of the future I see for tokens, that they are going to replace kind of loyalty points."*

The interviewee further explains a possible scenario with loyal points, where a cryptocurrency will have its own platform and customers would pay to use that platform. In practice, this explains a more accepted society towards cryptocurrencies. For instance, if a shop uses a specific platform, the shop would be connected to the cryptocurrency the platform holds, and the customers can transact with the shop by using that cryptocurrency. In the back-end when something gets bought, a conversion between any cryptocurrency or fiat money will happen with a small fee, making the fiat money the mediator of exchange. This payment system would first of all lower costs payed to third party companies, but also have the possibility to excluding them. It would also enable more decentralization and everybody would have the same public information about transactions. This would enhance competition and perhaps technological advancements could integrate a non-profit system ran by computers or low cost system of miners. However, making a mechanism that can convert hundreds of cryptocurrencies, may seem superficial, but with the network effects, a simple conversion mechanism will probably be sufficient.

Replacement of Cash and International Transactions

Interviewee #3 continues with the second place of usage:

> *"So it is going to replace cash transactions and it is going to replace a lot of international transactions between companies that currently happen in kind of digital cash because it takes so long to transfer money from one point to the next."*

As digitized smart-phones are taking over more of peoples' everyday tasks, it is reasonable to believe that cryptocurrencies could work partially as a substitute to cash transactions in the near future. In spite of this, bank chips are getting easier to use and there are debates about making transactions even easier with, for instance, operating a chip in your hand or having it in the phone. This is evident in the new Applepay (Apple, 2018) and Facebook's payment platform (Facebook.com, 2018), in addition to many others, resulting in high competition. However, with cryptocurrencies, the transaction happens instantly, giving it a competitive advantage. Consumers in developed countries would maybe be indifferent to the technology the systems use and any of the systems may become adopted. Consequently, how user-friendly the transaction system is will probably decide what the majority of users will chose, a so called dominant design. As there are a lot of competition in the area of cash replacement, it is highly uncertain that cryptocurrencies can replace cash in the future. Which system that will get adapted will probably be decided by how good the system fits the requirements set forth in section 2.3 Definition of Money and section 2.4 Characteristics of Money.

In terms of peer-to-peer transactions internationally, we may expect to see an increase in these, as opposed to traditional international transactions. As shown earlier in Figure 5, Ripple is estimated to reduce costs of transaction by up to 60% and would allow for secure and fast transactions across the globe (Schwartz et al., 2012).

Incorporating blockchain technology in other arenas

Lastly, the third place of usage suggested by interviewee #3 is as follows:

> *"And I also see it replacing stuff like Google drive and let's say Microsoft and stuff like that because decentralized storages are one of the things that we are probably going see being the first and the most impact used case for it."*

Using the blockchain technology behind cryptocurrencies to facilitate storage of information is perhaps a segment with huge potential. Looking at Estonia, one of the leading countries in the world when it comes to blockchain technology, we have examples within their Electronic Coordination System for Draft Legislation, where the immutability and efficiency of storing draft laws is superior to the traditional systems. There are, however, still some challenges when it comes to the security, which Estonia also has invested a lot of money in (e-Estonia, 2018). However, despite today's challenges, it is likely that cryptocurrencies will continue to develop by improvements to the technology, resulting in them being implemented in more places of the society.

7 Are Cryptocurrencies in a Bubble?

In this section we will include arguments discussed in previous sections. The aim is to discuss arguments for and against a bubble. The collection of arguments in this section will be the basis for our conclusion. The first aspect we discuss is the bubble analysis, methods, framework, and valuation before we return to the characteristics of cryptocurrencies in order to assess whether these contribute to a financial bubble.

According to Bessembinder (2017), only 4% of the stocks in the CRSP database from 1926 to 2015 provide accumulated returns greater than a value-weighted index, Standard & Poor 500, and only 27.58% of the stocks in the CRSP database provide returns greater than US 1 month treasury bills. In other words, relatively few stocks have outperformed US 1 month treasury bills. If we relate this to cryptocurrencies, we cannot conclude that cryptocurrencies are in a bubble only because some cryptocurrencies are outperforming other investments like stocks, or other cryptocurrencies in terms of returns. With this in mind, we will continue to analyze the sudden boom and bust in cryptocurrencies.

7.1 Analysis of a Cryptocurrency Bubble

As mentioned in section 3.2 Data, the constituents of CRIX data are the largest and most successful cryptocurrencies. Cryptocurrencies should not necessarily be labeled a bubble if the cryptocurrencies in CRIX make up the most of the positive return of the cryptocurrency market. As shown, many ICOs turn out to be failures or semi-failures, leading only to a minority of successful cryptocurrencies. We cannot label Bitcoin a bubble because is part of a market that performs better than the rest; similarly to where a relatively small amount of stocks make up the accumulated return greater than the Standard & Poor 500. The point made here is where the bubble term creates confusion - whether all, the majority or individual cryptocurrencies constitute a bubble. Interviewee #3 compares the Dot-Com bubble with cryptocurrencies. He explains it is likely that few projects will survive and will be highly successful in the future, while the rest of the projects will disappear.

Comparing the market capitalization of cryptocurrencies and the total fiat money circulation, we see that cryptocurrencies are still low in value in comparison. As of May 20^{th} 2018, Bitcoin and the largest altcoins have $382 billions in terms of market capitalization. According to the Committee on Payments and Market Infrastructures (CPMI) statistics on payment[8], clearing and settlement systems in the CPMI countries, the value, albeit not total, of coins and banknotes in circulation was $4,686 billions in 2016. As discussed, it is likely that cryp-

[8]Available on page 422: https://www.bis.org/cpmi/publ/d172.pdf

tocurrencies will improve in the future which would increase their total market capitalization. However, such a growth in the form of value transfer between cryptocurrencies may still allow for explosive growth in individual cryptocurrencies and does not indicate a bubble. If the total market capitalization of cryptocurrencies remains the same, but the value of disappearing cryptocurrencies is transferred to the surviving cryptocurrencies there is no basis for labeling the surviving cryptocurrencies as a bubble, unless a bubble is already present. Although cryptocurrencies vary, we have chosen to look at cryptocurrencies collectively and we, therefore, will try to determine if a bubble exists collectively in cryptocurrencies.

7.2 Reflection on Frameworks and Methods Used

The framework and methods are all from section 4 Bubble Tests. After getting an overview by looking at the seven steps taxonomy, the cryptocurrency price boom seems similar to other bubbles. However, as there was no crisis nor spreading to the real economy, it is questionable whether cryptocurrencies can be called a bubble. To analyze the cryptocurrency price a step further, the PWY, PSY and LPPL tests were carried out . All the tests showed bubble tendencies. In both the PWY and PSY method, the results displayed bubble tendencies during 2017 to April 2018 which is the end of the sample. Similarly, LPPL showed an exponential regression function that anticipates a crash early June 2018. However, there are debates of the correct definition of a bubble. The most established theory is the asset-pricing approach in which a bubble is defined as the market price higher than the fundamental value of the financial entity.

As this is not possible with cryptocurrencies, we have looked at alternative approaches. Considering the limitations of the models, in addition to the high volatility and exponential growth in CRIX, we have interpreted these results with a critical eye. Supplementing these quantitative results with a qualitative methodology is, therefore, crucial. The relatively old frameworks and theories should be updated to better capture the essence of modern advances in finance. Due to lack of new established theories and frameworks, we need to use different theories while also being aware of the limitations in order to value cryptocurrencies and reach the same goal as with the asset pricing model. In trying to figure out if there is a more extensive bubble developing over the past years, we have analyzed cryptocurrencies and its place in the financial market in the future. Thus, the following section we will analyze the arguments made in sections 5 Decomposing Cryptocurrencies and 6 A New Payment System.

7.3 Valuing Cryptocurrency

We look into the two most used fundamental value approaches to value cryptocurrencies in section 5.1.1 Market Sizing and section 5.1.2 Marginal Cost of Production. We conclude that these methods are not satisfactory in determining a fundamental value of cryptocurrencies. These approaches show signs that there are no approaches for calculating a fundamental value at this time and cannot support the question about a bubble.

We have analyzed fundamentals around cryptocurrencies in section 5.1.3 Redefining Fundamental Value, in an attempt to define the underlying drivers. The unresolved nature of cryptocurrencies does not necessarily constitute a bubble. The argument against a bubble is that societies and people working on improving cryptocurrencies may be the key for cryptocurrencies' future survival and thus, is an argument against a bubble.

7.4 Cryptocurrency as Money

To summarize the previous section, we cannot set a fundamental value on cryptocurrency. Therefore, we have to evaluate cryptocurrencies by traditional definition and characteristics of money as done in section 5.2 Application of Traditional Definition and Characteristics of Money.

Application of Adam Smith's definition to cryptocurrencies shows that cryptocurrencies are not satisfying the functions to a large extent. Going forward, if cryptocurrencies do not improve so that it fits the definition better, it is likely that cryptocurrencies will continue to only work as peer-to-peer system or disappear when investors do not see any improvements and stop believing in them. Therefore, if cryptocurrencies do not fulfill its intended role as payment system, we may rationally expect a price decrease and a likely bubble. If cryptocurrencies would become less volatile or get more accepted by merchants and used more by the population, it is likely that cryptocurrencies can continue having a position in the economy where a crash and a bubble does not happen.

When fitting cryptocurrencies into Adam Smith's characteristics of money, cryptocurrencies exhibits some improvements when compared to the fiat system. The improvements of durability and divisibility are superior to fiat money, while portability and scarcity are satisfied to the same degree as fiat money. Stability and acceptability, however, are characteristics cryptocurrency are lacking at the present time. Durability and divisibility in fiat money serve their purpose, making the argument of superior characteristics superficial. More importantly, the lack of stability and acceptability is what essentially makes cryptocurrencies' characteristics not fully suitable as money. Looking forward, it is likely that these lacking characteristics can change for the better which strengthen the argument against a bubble.

When it comes to the criteria emphasized by the representatives from financial infrastructure, cryptocurrencies is to a degree lacking. In short, some cryptocurrencies have the required features of cost efficiency, cheap and fast, respectively. Cryptocurrencies are secure, but where you store the coins is not entirely. With the rapid technological advancements, it is reasonable to believe that cryptocurrency storage will become more secure in the future. As of today, cryptocurrencies lack some user-friendliness, making it less suitable for the general population.

From a bubble perspective, this part of the thesis shows contradicting indications. On one hand, cryptocurrencies do not satisfy the definition of money. On the other hand, the characteristics and criteria show additional potential for cryptocurrencies, leading to a contradiction of a bubble and potential for future growth.

After looking into assumptions of money, characteristics and criteria, we continue with a look into how cryptocurrencies as a large scale payment system could get adopted in the world economy in practice. However, there are a lack of examples with reliable sources in terms of government-based cryptocurrencies, which does not allow us to add arguments to our research question.

7.5 Features of Cryptocurrencies

We have further analyzed the features of cryptocurrency, where we might find out why cryptocurrencies have achieved such popularity and if the price is sustainable in the future, in order to establish a bubble.

7.5.1 Privacy and Criminality

We will first present the main arguments from sections 6.1 Privacy and 6.2 Criminality to get a better understanding of how these features will affect the price. Comparing the pseudonymous and anonymous cryptocurrencies, it is likely that the pseudonym only will continue as a niche payment system, while the anonymous have more potential, assuming they will be totally anonymous. Controversially, as it is likely that these anonymous cryptocurrencies will be used by criminals, law enforcement will always try to trace them. Furthermore, having a public ledger may not be that advantageous, especially as a large scale payment system. This results in an uncertainty if the anonymous cryptocurrencies can become more than a small scale payment system. However, connecting this to the bubble question, it is reasonable to say that this is an argument against a bubble, as these arguments predict more potential in cryptocurrencies than destruction of their value.

7.5.2 Regulation and Security

In the following sub-section, encompassing sections 6.3 Regulation and 6.4 Security, is an overview of the challenges in regulations of cryptocurrencies in the world, in addition to how safe cryptocurrencies are. As there are few regulations that capture cryptocurrencies today, there are few barriers. However, it is likely that there will be more regulations eventually, especially for ICOs. Regulation of ICOs will protect the existing cryptocurrencies and a regulation of cryptocurrencies could indirectly prove that it has its place in the economy, as long as it does not involve a total ban. Hence, regardless of the regulations, it is likely that cryptocurrencies will have a place in the world economy and, therefore, not exhibit bubble characteristics.

Cryptocurrencies' blockchain technology is secure, but the wallet or storage facilities are not. The blockchain technology has a superior security, but in order to be practically used the third-party technology surrounding cryptocurrencies is lacking. An example of this is when the Bitcoin price has met some turbulence after hackers have stolen coins from these third-party providers Huang (2018). These limitations have potential to become improved, but are also not crucial for the future existence of cryptocurrencies. Therefore, this argument cannot be used in explaining a bubble in cryptocurrencies.

7.5.3 Cost and Time Efficiency

In section 6.5 Transacting with Blockchain, it is shown that parts of Bitcoin's blockchain technology is inferior to Ripple. In section 6.6 Improvements, these flaws with Bitcoin's technology can be improved in the future. Furthermore, the transitioning from PoW to PoS is said to make cryptocurrencies cheaper. There is, however, a lot uncertainty connected to these improvements.

On the other hand, as Ripple already possesses technology which is fast and cost efficient, it is likely that other cryptocurrencies also do. To conclude, making a general statement for all cryptocurrencies is difficult on this topic as there are large variations in the technology. However, cryptocurrencies that exhibit cheap and fast technologies meet these two criteria discussed earlier and have the potential to make a place in the world economy. Therefore, it is likely that the cost and time consuming characteristics may become improved in Bitcoin as well or that users will transfer their value to another cryptocurrency that acquires these characteristics. In both cases, the argument does not indicate that cryptocurrencies are in a bubble.

7.6 Arguments based on Fiat Money

We evaluate the underlying constructs of fiat money in order to determine whether or not these also apply to cryptocurrencies. Trust is an assumption from which the price of fiat money is derived, which could to a certain degree also apply to cryptocurrencies. If this same underlying assumption applies to fiat money and cryptocurrencies, all else equal, we cannot conclude that cryptocurrencies are in a bubble, unless fiat money is also a bubble. Inflation targeting helps to maintain a low and stable inflation, but it is also a system which can be manipulated for political and personal gain. This can be done by short term manipulation or worse, such as causing instability from, for instance, war and corruption. The lack of a monetary policy for cryptocurrency leaves it vulnerable in the case of cryptocurrencies as a large-scale payment system, but a strength as a niche payment system. Furthermore, decentralization has no proven value over centralization and cannot explain the volatility or price growth that surrounds cryptocurrencies. However, high volatility can cause uncertainty among investors. This can result in a setback if the economic growth changes into a recession. Historically, recessions come in cycles, that may result in a collapse and a bubble formation. This being the case, the bubble would not have started off in cryptocurrencies and could not said to be caused by cryptocurrencies. To summarize, there are no indications that these arguments would cause a bubble as cryptocurrencies can function well as a small scale payment system.

7.7 Future of Cryptocurrencies

It is likely that only few cryptocurrencies and platforms will continue to exist, one for the most needed niche segments. Even if loyalty points would not be implemented the way discussed, there will be a need of a conversion mechanism if cryptocurrencies are incorporated into the payment system.

Developed countries in the long run are likely to become fully digitized, where physical cash eventually ceases to exist. However, in developing countries cash is more frequently used. As the trend towards digitization continues, the need for a digital payment system emerges. Whether the society will adopt cryptocurrencies as a payment system remains to be seen. The chances of an adoption of cryptocurrencies depend to a degree on how good the method of payment will meet the consumers' requirements. Thus, the future potential of cryptocurrencies in a digital world will depend on how good cryptocurrencies fit the characteristics and functions of money. This concludes in that cryptocurrencies may not be in a bubble as there are multiple potential areas for adoption of cryptocurrencies.

8 Conclusion

To begin with, predictions made in this thesis are based on rational investors. In other words, rationality underpins the entirety of the discussion and analysis. When looking into how we can determine if a bubble exist, as an established theory we find that the asset pricing model is considered the most reliable one. Firstly, one of the essential criterion in this model is that it needs to be an cash generating entity in order to find the fundamental value. Secondly, the asset pricing model defines a bubble where the market price deviates from this fundamental value. However, cryptocurrencies do not fit the above criteria. In trying to circumvent the asset pricing model, we looked at other methods for finding the fundamental value. We did not find a satisfying method and we, therefore, discussed whether fundamental value should be redefined to capture the nature of cryptocurrencies. In addition, we performed bubble tests in which the results indicated bubble behavior, but the tests alone could not provide definite conclusions. This led us to analyzing cryptocurrencies' characteristics and them as a means of payment. Below are summarized arguments against and for a bubble.

Arguments against a Bubble

- Growing societies with structure, leadership, hierarchy, friendship and community.
- Characteristics and criteria of money is suitable to a degree and have potential to improve.
- Privacy and criminality are arguments that prevent a cryptocurrency to become a large scale payment system, but these arguments also do not lead to a bubble via cryptocurrencies disappearing.
- Regulation: There are few regulations today and future regulations can expect to increase the reputation and competitive advantage of cryptocurrencies.
- Security: Superior technology in terms of security. However, the infrastructure surrounding cryptocurrencies lacks security, but can be expected to be improved in the future.
- Assumptions of fiat money do not indicate that cryptocurrencies will have a price bust.
- Multiple areas of usage.

Arguments for a Bubble

- The bubble tests showed bubble tendencies in CRIX dataset.
- Cryptocurrencies today do not satisfy the definition of money.

- Large scale regulation involving a ban.
- If the high volatility continues, it is likely that cryptocurrencies will continue to not function well as money, eventually resulting in decreasing their popularity as the usage is limited.

To return to our research question, our quantitative findings predict a future crash date to be on June 4^{th}, 2018 in the CRIX dataset with data until May 25^{th} 2018. Furthermore, our quantitative findings also indicate bubble tendencies in the CRIX dataset that start at the end of September 2017, lasting into the end of the sample period, May 2018. Despite obtaining these results, the accuracy of the models used leaves the results doubtful. However, in the discussion section of this master thesis, we saw that cryptocurrencies look like an underdeveloped entity with a lot of potential to become a currency. Therefore, after analyzing cryptocurrencies, we believe there is a high probability that cryptocurrencies will continue to exist. Moreover, as the nature of cryptocurrencies is not yet determined, in addition to unusually high volatility, such a bubble conclusion cannot be proven at this time. The discussion part of this thesis revealed strong arguments on both sides of the bubble debate. However, they are incline towards the existence of cryptocurrencies, leading to no bubble being present, but no concrete single bubble conclusion can be drawn from the analysis. We, therefore, conclude that the media's use of the term "bubble" is inaccurate and we have seen that there are conclusions drawn from too shallow arguments as there is no theory backing up these statements.

References

Admin.ch (2018), 'Electricity consumption up 0.4% in 2017. [online]'. Available at: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-70489.html [Accessed 20 June 2018].

Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014), 'The economics of digital currencies'.

Alvseike, R. and Iversen, G. (2017), Blockchain and the future of money and finance, Master thesis in finance, Norwegian School of Economics. Available at: https://brage.bibsys.no/xmlui/handle/11250/2453330 [Accessed 21 May 2018].

Apple (2018), 'Applepay: Cashless made effortless. [online]'. Available at: https://www.apple.com/apple-pay/ [Accessed 20 June 2018].

Baker, S. E., Edwards, R. and Doidge, M. (2012), 'How many qualitative interviews is enough?: Expert voices and early career reflections on sampling and cases in qualitative research'.

Bank of England (2018), 'The Future of Money - speech by Mark Carney — Bank of England. [online]'. Available at: https://www.bankofengland.co.uk/speech/2018/mark-carney-speech-to-the-inaugural-scottish-economics-conference [Accessed 3 June 2018].

Barford, V. (2013), 'Bitcoin: Price v hype'.

Bastiaan, M. (2015), *Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin*. Available at: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack%20-a-stochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf.

Bernanke, B. S. (2001), *Inflation targeting: lessons from the international experience*, Princeton University Press.

Bessembinder, H. (2017), 'Do stocks outperform treasury bills?'.

Bheemaiah, K. (2017), *The Blockchain Alternative: Rethinking Macroeconomic Policy and Economic Theory*, Apress.

Bicakci, K. and Baykal, N. (2002), Infinite length hash chains and their applications, *in* 'Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on', IEEE, pp. 57–61.

Blockchain.info (2018), 'Bitcoin block explorer - blockchain. [online]'. Available at: http://blockchain.info/ [Accessed 25 May 2018].

Bohachevsky, I. O., Johnson, M. E. and Stein, M. L. (1986), 'Generalized simulated annealing for function optimization', *Technometrics* **28**(3), 209–217.

Brown, S. D. (2016), 'Cryptocurrency and criminality: The bitcoin opportunity', *The Police Journal* **89**(4), 327–339.

Brueckner, J. K., Calem, P. S. and Nakamura, L. I. (2012), 'Subprime mortgages and the housing bubble', *Journal of Urban Economics* **71**(2), 230–243.

Buterin, V. (2015), 'Ethereum white paper'. Available at: https://github.com/ethereum/wiki/wiki/White-Paper [Accessed 3 June 2018].

Buybitcoinworldwide (2018*a*), 'The bitcoin volatility index [online]'. Available at: https://www.buybitcoinworldwide.com/volatility-index/ [Accessed 19 June 2018].

Buybitcoinworldwide (2018*b*), 'Is bitcoin anonymous? no! it's pseudonymous. [online]'. Available at: https://www.buybitcoinworldwide.com/anonymity/ [Accessed 25 May 2018].

Calcagno, R. and Monticone, C. (2015), 'Financial literacy and the demand for financial advice', *Journal of Banking & Finance* **50**, 363–380.

Campbell, J. Y. and Shiller, R. J. (1988*a*), 'The dividend-price ratio and expectations of future dividends and discount factors', *The Review of Financial Studies* **1**(3), 195–228.

Campbell, J. Y. and Shiller, R. J. (1988*b*), 'Stock prices, earnings, and expected dividends', *The Journal of Finance* **43**(3), 661–676.

Carmona, A. (2015), The bitcoin: The currency of the future, fuel of terror, *in* 'Evolution of Cyber Technologies and Operations to 2035', Springer, pp. 127–135.

Cheung, A., Roca, E. and Su, J.-J. (2015), 'Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices', *Applied Economics* .

Coinbase (2018), 'How is coinbase insured?. [online]'. Available at: https://support.coinbase.com/customer/portal/articles/1662379- how-is-coinbase-insured- [Accessed 19 June 2018].

CoinDesk (2018), 'Bitcoin price movement. [online]'. Available at: https://www.coindesk.com/price/].

CoinMarketCap (2018), 'Bitcoin price movement. [online]'. Available at: https://coinmarketcap.com/currencies/bitcoin/.

Craine, R. (1993), 'Rational bubbles: A test', *Journal of Economic Dynamics and Control* **17**(5-6), 829–846.

CryptoCompare (2018*a*), '5 things you need to know about bitcoin volatility [online]'. Available at: https://www.cryptocompare.com/ [Accessed 22 May 2018].

CryptoCompare (2018*b*), 'Cryptocompare.com - live cryptocurrency prices, trades, volumes, forums, wallets, mining equipment and reviews [online]'. Available at: https://www.cryptocompare.com/ [Accessed 22 May 2018].

Darlington III, J. K. (2014), 'The future of bitcoin: Mapping the global adoption of world's largest cryptocurrency through benefit analysis'.

Davies, G. (2002), *History of Money:From Ancient Times to the Present Day*, University of Wales Press.

Davies, G. (2010), *History of Money*, University of Wales Press.

de Vries, A. (2018), 'Bitcoin's growing energy problem', *Joule* **2**(5), 801–805. Available at: http://dx.doi.org/10.1016/j.joule.2018.04.016.

Demirgüç-Kunt, Asli, Klapper, L., Singer, D., Ansar, S. and Hess, J. (2018), 'The global findex database 2017: Measuring financial inclusion and the fintech revolution'. Available at: https://globalfindex.worldbank.org/sites/globalfindex/files/2018-04/2017%20Findex%20overview%20English.pdf.

Diamond, D. W. and Dybvig, P. H. (1983), 'Bank runs, deposit insurance, and liquidity', *Journal of political economy* **91**(3), 401–419.

Diba, B. T. and Grossman, H. I. (1988), 'Explosive rational bubbles in stock prices?', *The American Economic Review* **78**(3), 520–530.

Digiconomist (2018), 'Bitcoin energy consumption index - digiconomist. [online]', *Online* . Available at: https://digiconomist.net/bitcoin-energy-consumption [Accessed 20 June 2018].

Dobeck, M. F. and Elliott, E. (2007), *Greenwood guides to business and economics - Money*, Vol. 1 of *1*, Greenwood Press, Westport, Conn.

Dodd, N. (2018), 'The social life of bitcoin', *Theory, culture & society* **35**(3), 35–56.

e-Estonia (2018), 'Ksi blockchain — e-estonia [online]'. Available at: https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/ [Accessed 1 June 2018].

European Commission (2018), 'European Commission - PRESS RELEASES - Press release - StatementBy First Vice-President Timmermans, Vice-President Dombrovskis and Commissioner Jourovà on the adoption by the European Parliament of the 5th Anti-

Money Laundering Directive. [online]'. Available at: http://europa.eu/rapid/press-release_STATEMENT-18-3429_en.htm [Accessed 19 June 2018].

European Union (2018), 'Regulations, Directives and other acts - European Union - European Commission. [online]'. Available at: https://europa.eu/european-union/eu-law/legal-acts_en [Accessed 19 June 2018].

Europol (2017), 'Internet organised crime threat assessment'. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017.

Facchini, F. and Couvreur, S. (2015), 'Inequality: The original economic sin of capitalism? An Evaluation of Thomas Piketty's" Capital in the twenty-first century"', *European Journal of Political Economy* **39**, 281–287.

Facebook.com (2018), 'Community payments terms. [online]'. Available at: https://www.facebook.com/payments_terms [Accessed 20 June 2018].

Fantazzini, D., Nigmatullin, E., Sukhanovskaya, V. and Ivliev, S. (2016), 'Everything you always wanted to know about bitcoin modelling but were afraid to ask'.

Federal Reserve Bank of St. Louis (2018), 'Functions of money, economic lowdown podcasts — education resources — st. louis fed. [online]'. Available at: https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-9-functions-of-money [Accessed 5 June 2018].

Feigenbaum, J. A. and Freund, P. G. (1998), 'Discrete scale invariance and the" second black monday"', *Modern physics letters B* **12**(02n03), 57–60.

Finance.yahoo.com (2018), 'Nasdaq composite (ixic). [online]'. Available at: https://finance.yahoo.com/quote/$^IXIC?p =^I XIC[Accessed 20 June 2018]$.

Foley, S., Karlsen, J. and Putniņš, T. J. (2018), 'Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?', *SSRN Electronic Journal* .

Gandal, N. and Halaburda, H. (2016), 'Can we predict the winner in a market with network effects? competition in cryptocurrency market', *Games* **7**(3), 16.

Garber, P. M. (1990), 'Famous first bubbles', *Journal of Economic perspectives* **4**(2), 35–54.

Garcia, D., Tessone, C. J., Mavrodiev, P. and Perony, N. (2014), 'The digital traces of bubbles: feedback cycles between socio-economic signals in the bitcoin economy', *Journal of the Royal Society Interface* **11**(99), 20140623.

Gazola, L., Fernandes, C., Pizzinga, A. and Riera, R. (2008), 'The log-periodic-ar (1)-garch (1, 1) model for financial crashes', *The European Physical Journal B* **61**(3), 355–362.

Glotov, V. and Mihailov, D. (2018), 'What are the technical means the state prepare for the regulation of the cryptocurrencies?', *KnE Social Sciences & Humanities* **3**(2), 583–592.

Goodboy, D. (2018), '3 types of cryptocurrencies you need to know'. Available at: https://www.nasdaq.com/article/3-types-of-cryptocurrencies-you-need-to-know-cm905488 [Accessed 19 Jun. 2018].

Grytten, O. H. and Hunnes, A. (2016), *Krakk og kriser i et historisk perspektiv*, Vol. 1 of *1*, 1 edn, Cappelen Damm Akademisk, Bergen/Kristiansand.

Halaburda, H. (2016*a*), 'Digital currencies: Beyond bitcoin', *DigiWorld Economic Journal* **103**, 77–92,213.

Halaburda, H., . S. M. (2016*b*), *Beyond bitcoin: the economics of digital currencies*, New York City, NY: Palgrave Macmillan.

Hanke, S. H., Bushnell, C. et al. (2017), 'On measuring hyperinflation', *World Economics* **18**(3), 1–18.

Harvey, D. I., Leybourne, S. J., Sollis, R. and Taylor, A. R. (2016), 'Tests for explosive financial bubbles in the presence of non-stationary volatility', *Journal of Empirical Finance* **38**, 548–574.

Hayes, A. (2015), 'A cost of production model for bitcoin'.

Hayes, A. (2016), 'Cryptocurrency value formation: an empirical analysis leading to a cost of production model for valuing bitcoin'.

He, D., Habermeier, K. F., Leckow, R. B., Haksar, V., Almeida, Y. and Kashima (2016), Virtual currencies and beyond: initial considerations, Technical report, International Monetary Fund.

Heaven, D. (2018), 'Sitting with the cyber-sleuths who track cryptocurrency criminals. [online] mit technology review.'. Available at: https://www.technologyreview.com/s/610807/sitting-with-the-cyber-sleuths-who-track-cryptocurrency-criminals/ [Accessed 14 June 2018].

Helbing, D. and Pournaras, E. (2015), 'Society: Build digital democracy', *Nature News* .

Hileman, G. and Rauchs, M. (2017), 'Global cryptocurrency benchmarking study', *Cambridge Centre for Alternative Finance* .

Homm, U. and Breitung, J. (2012), 'Testing for speculative bubbles in stock markets: a comparison of alternative methods', *Journal of Financial Econometrics* **10**(1), 198–231.

Hong, K. (2017), 'Bitcoin as an alternative investment vehicle', *Information Technology and Management* **18**(4), 265–275.

Hoppe, H.-H. (1994), 'How is fiat money possible?—or, the devolution of money and credit', *The Review of Austrian Economics* **7**(2), 49–74.

Huang, Z. (2018), 'Bitcoin crashed after another crypto exchange got hacked. [online] quartz'. Available at: https://qz.com/1301699/bitcoin-crashed-after-south-korean-exchange-coinrail-was-hacked/ [Accessed 20 June 2018].

Jackson, O. (2018*a*), 'PSD2 gives banks chance to evolve', *International Financial Law Review* .

Jackson, O. (2018*b*), 'US or Swiss approach for EU crypto regulation?', *International Financial Law Review* .

Jacobs, M. and Mazzucato, M. (2016), *Rethinking capitalism: economics and policy for sustainable and inclusive growth*, John Wiley & Sons.

Johansen, A., Ledoit, O. and Sornette, D. (2000), 'Crashes as critical points', *International Journal of Theoretical and Applied Finance* **3**(02), 219–255.

Kaushal, R. (2016), 'Bitcoin: First decentralized payment system', *International Journal Of Engineering And Computer Science* **5**(5).

Keller, G. and Gaciu, N. (2012), *Managerial statistics*, South-Western Cengage Learning.

Kent, C. and Sasa, J. (2018), 'Divergent regulatory approaches to cryptocurrency offerings: Developments in canada, the united states, and china'. Available at: https://mcmillan.ca/Divergent-Regulatory-Approaches-to-Cryptocurrency-Offerings-Developments-in-Canada-the-United-States-and-China.

Kiayias, A., Russell, A., David, B. and Oliynykov, R. (2017), Ouroboros: A provably secure proof-of-stake blockchain protocol, *in* 'Annual International Cryptology Conference', Springer, pp. 357–388.

King, S. and Nadal, S. (2012), 'Ppcoin: Peer-to-peer crypto-currency with proof-of-stake', *self-published paper, August* **19**.

Kiyotaki, N. and Wright, R. (1989), 'On money as a medium of exchange', *Journal of political Economy* **97**(4), 927–954.

Kleinbard, D. (2000), 'The $1.7 trillion dot.com lesson'. Available at: http://money.cnn.com/2000/11/09/technology/overview/.

Lab, K. (2017), 'Six main disadvantages of bitcoin and the blockchain. [online]'. Available at: https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/ [Accessed 12 June 2018].

Larsen, C. and McCaleb, J. (2018), 'XRP — Ripple'. Available at: https://ripple.com/xrp/ [Accessed 5 June 2018].

Leech, B. L. (2002), 'Asking questions: Techniques for semistructured interviews', *PS: Political Science & Politics* **35**(4), 665–668.

Leone, V. and de Medeiros, O. R. (2015), 'Signalling the dotcom bubble: A multiple changes in persistence approach', *The Quarterly Review of Economics and Finance* **55**, 77–86.

Lincoln Yvonna, S. and Guba, E. G. (1985), 'Naturalistic inquiry', *Beverly Hills: Sage Publications* .

Lo, S. and Wang, J. C. (2014), 'Bitcoin as money? current policy perspectives'.

Mayring, P. (2016), *Einführung in die qualitative Sozialforschung*, Vol. 5, Beltz Weinheim.

Mellor, M. (2010), *The future of money: from financial crisis to public resource*, Pluto Press.

Mitchell, T. and Clover, C. (2017), 'China steps up capital controls with overseas withdrawal cap'. Available at: https://www.ft.com/content/b69166fa-ee01-11e7-b220-857e26d1aca4.

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M. and Aldridge, J. (2017), 'Conflict management in illicit drug cryptomarkets', *International Criminal Justice Review* **27**(4), 237–254.

Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S. et al. (2018), 'An empirical analysis of traceability in the monero blockchain', *Proceedings on Privacy Enhancing Technologies* **2018**(3), 143–163. Available at: https://arxiv.org/pdf/1704.04299/.

Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system'. Available at: http://bitcoin.org/bitcoin.pdf.

Nneji, O., Brooks, C. and Ward, C. (2013), 'Intrinsic and rational speculative bubbles in the us housing market: 1960-2011', *Journal of Real Estate Research* **35**(2), 121–151.

O'Dwyer, K. J. and Malone, D. (2014), 'Bitcoin mining and its energy footprint'.

Oppers, S. E. (1996), 'Was the worldwide shift to gold inevitable? an analysis of the end of bimetallism', *Journal of Monetary Economics* **37**(1), 143–162.

Parr, R. L. (2018), *Intellectual property: valuation, exploitation, and infringement damages*, John Wiley & Sons.

Pedersen, T. Q. and Schütte, E. C. M. (2017), 'Testing for explosive bubbles in the presence of autocorrelated innovations'.

Peters, G. W. and Panayi, E. (2015), Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money, *in* 'Banking Beyond Banks and Money', Springer, pp. 239–278.

Phillips, P. C., Shi, S. and Yu, J. (2015), 'Testing for multiple bubbles: Historical episodes of exuberance and collapse in the s&p 500', *International Economic Review* **56**(4), 1043–1078.

Phillips, P. C., Wu, Y. and Yu, J. (2011), 'Explosive behavior in the 1990s nasdaq: When did exuberance escalate asset values?', *International economic review* **52**(1), 201–226.

Phillips, P. and Shi, S. (2014), 'Financial bubble implosion'.

Pilkington, M. (2016), '11 blockchain technology: principles and applications', *Research handbook on digital transformations* p. 225.

Poon, J. and Dryja, T. (2016), 'The bitcoin lightning network: Scalable off-chain instant payments', *draft version 0.5* **9**, 14.

Reed, C., Sathyanarayan, U. M., Ruan, S. and Collins, J. (2018), 'Beyond bitcoin—legal impurities and off-chain assets', *International Journal of Law and Information Technology* **26**(2), 160–182.

Ripple.com (2018), 'Solution overview - ripple. [online]'. Available at: https://ripple.com/files/ripple$_{s}olutions_{g}uide.pdf[Accessed20June2018]$.

Saberhagen, N. v. (2013), 'Cryptonote v 2.0'. Available at: https://cryptonote.org/whitepaper.pdf.

Saunders, M., Lewis, P. and Thornhill, A. (2015), *Research Methods for Business Students, Seventh edition*, Pearson, New York.

Scharfstein, D. S. and Stein, J. C. (1990), 'Herd behavior and investment', *The American Economic Review* pp. 465–479.

Schwartz, D., Youngs, N. and Britto, A. (2012), 'Ripple white paper'. Available at: https://ripple.com/files/ripple_consensus_whitepaper.pdf.

Sedgwic, K. (2018), 'Most privacy coins aren't that private - bitcoin news. [online]'. Available at: https://news.bitcoin.com/most-privacy-coins-arent-that-private/ [Accessed 5 Jun. 2018].

Seigneur, J.-M., D'Hautefort, H. and Ballocchi, G. (2017), Use case of linking a managed basket of fiat currencies to crypto-tokens, *in* 'First Meeting of the ITU Focus Group on Digital Currency including Digital Fiat Currency'.

Shaw, K. L. (1996), 'An empirical analysis of risk aversion and income growth', *Journal of Labor Economics* **14**(4), 626–653.

Shy, O. (2001), *The economics of network industries*, Cambridge University Press.

Smith, A. (2000), *Wealth of Nations*.

Son, H., Levitt, H. and Louis, B. (2018), 'Jamie dimon slams bitcoin as a fraud', *Bloomberg* .

Sørensen, P. and Whitta-Jacobsen, H. (2010), 'Introducing advanced macroeconomics: Growth and business cycles. harlow, england'.

Sornette, D., Johansen, A. and Bouchaud, J.-P. (1996), 'Stock market crashes, precursors and replicas', *Journal de Physique I* **6**(1), 167–175.

Stevis-Gridneff, M. and Kantchev, G. (2018), 'Bitcoin is a hit in countries where locals face currency troubles [online] wsj.'. Available at: https://www.wsj.com/articles/bitcoin-is-a-hit-in-countries-where-locals-face-currency-troubles-1515067201 [Accessed 22 May 2018].

Tech Crunch (2018), 'Exit scammers run off with $660 million in ico earnings'. Available at: https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/?guccounter=1[Accessed 7 May 2018].

Thompson, E. A. (2007), 'The tulipmania: Fact or artifact?', *Public Choice* **130**(1-2), 99–114.

Tokendata.io (2018), 'Token data — news, data and analytics for all ico's and tokens. [online]'. Available at: https://www.tokendata.io/ [Accessed 19 June 2018].

Tongco, M. D. C. (2007), 'Purposive sampling as a tool for informant selection', *Ethnobotany Research and applications* **5**, 147–158.

TRON.NETWORK (2018), 'Tron whitepaper'. Available at: https://o836fhe91.qnssl.com/tron/whitebook/TronWhitepaper_en.pdf [Accessed 19 June 2018].

Tuchman, W. (1997), A brief history of the data encryption standard, *in* 'Internet besieged', ACM Press/Addison-Wesley Publishing Co., pp. 275–280.

United Nations (1948), 'Universal declaration of human rights [online]'. Available at: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf [Accessed 17 June 2018].

United Nations (2012), 'World economic situation and prospects 2012', *New York* .

United Nations (2014), 'World economic situation and prospects 2014', *New York* .

United Nations (2018), 'World economic situation and prospects 2018', *New York* .

Van Norden, S. (1996), 'Regime switching as a test for exchange rate bubbles', *Journal of Applied Econometrics* pp. 219–251.

Vasek, M. and Moore, T. (2015), There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams, *in* 'International conference on financial cryptography and data security', Springer, pp. 44–61.

West, K. D. (1987), 'A specification test for speculative bubbles', *The quarterly journal of economics* **102**(3), 553–580.

White, L. H. (1984), 'Competitive payments systems and the unit of account', *The American Economic Review* **74**(4), 699–712.

Woo, D., Gordon, I. and Iaralov, V. (2013), 'Bitcoin: a first assessment'.

Appendix A: Interview Request

Dear Mr./Ms[9],

I am currently writing my master thesis along with a fellow student from the Norwegian School of Economics (NHH). We saw your articles about cryptocurrency and thought they were interesting.

Our thesis is about evaluating cryptocurrencies as a bubble. We are looking to combine our quantitative findings with interviews from experts within different areas of the industry. Therefore, it would be interesting to talk to you about cryptocurrencies in general, its usage, regulations and what to expect in the future.

We are wondering if someone from your organization would be interested in answering some questions to support our thesis?

We would like to thank you for your time and look forward to hearing from you!

Greetings, Jonathan Raa and Eirik Hollekim

[9]The inquiries were performed through email and were sent to various people with expertise within the cryptospace. The following email is an example to a person that had written an article about cryptocurrencies. After a potential interviewee showed interest, we continued with the formalities presented in our methodology part and booked an appointment.

Appendix B: Interview Guide

Research question: To what extent can we identify cryptocurrencies as being in a bubble, historically or currently?

Introduction

Motivation: Starting the interview by introducing ourselves, asking a permission for recording and explaining other formalities. Get an overview of the interviewee's knowledge and experience.

Discussion topics:

- Presentation of ourselves and the master thesis
- When he/she became involved/interested in cryptocurrencies and how the development has been since then

Main part: Characteristics of cryptocurrencies

Motivation: Get insights into the interviewee's standpoint towards cryptocurrencies and discuss the following topics.

Discussion topics:

- Potential
- Area of usages
- Immediate threats
- Fundamental value

Main part: Cryptocurrency as a bubble

Motivation: Get insights into the price development.

Discussion topics:

- Zero intrinsic value
- Fundamental value
- The recent boom in prices - Are cryptocurrencies in a bubble?
- Government and cryptocurrency

Ending: Cryptocurrency in the future

Motivation: Get insights into the future development of cryptocurrencies.

Discussion topics:

- Regulations and legislation
- Decentralization
- Cryptocurrencies in the future