

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Administración y Economía

Economic Analysis of Cryptocurrency

Proyecto de Investigación

Artem Kazakov

Economía

Trabajo de titulación presentado como requisito

para la obtención del título de

Economista

Quito, 6 de diciembre de 2018

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ
COLEGIO DE ADMINISTRACIÓN Y ECONOMÍA

**HOJA DE CALIFICACIÓN
DE TRABAJO DE TITULACIÓN**

Economic Analysis of Cryptocurrency

Artem Kazakov

Calificación:

Nombre del profesor, Título académico: Jaime Maya, MBA.

Firma del profesor:

Quito, 6 de diciembre de 2018

Derechos de Autor

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante:

Nombres y Apellidos: Artem Kazakov

Código: 00117969

Cédula de Identidad : 1719840819

Lugar y fecha: Quito, 6 de diciembre de 2018

RESUMEN

El presente trabajo tiene como objetivo proveer un análisis económico general de las cryptomonedas. Este análisis se refiere de manera general a todas las cryptomonedas pero principalmente se enfoca en el bitcoin debido a que es la moneda de mayor uso y aceptación a nivel mundial. Dado que el tema es relativamente nuevo, este trabajo comienza resumiendo la historia y definiciones importantes del ecosistema de las cryptomonedas. Después se explica la formación del precio del bitcoin y a qué se debe su gran volatilidad mediante un estudio reciente de Kancs et al. (2015). Además se analizan los principales riesgos y problemas que surgen con el uso libre del bitcoin y se plantean posibles soluciones que podrían mitigar estos obstáculos. Finalmente, se concluyen los principales riesgos que se deberían tomar en cuenta al invertir o utilizar cryptomonedas como bitcoin y cómo ésta se podría utilizar para la diversificación de un portafolio.

Palabras clave: Bitcoin, Historia, Problemas, Cryptomonedas, Volatilidad, Formación de precio, Diversificación de portafolio, Riesgo

ABSTRACT

The present work aims to provide a general economic analysis of cryptocurrencies. This analysis refers in a general way to all cryptocurrencies but will mainly focus on bitcoin since it is the currency with the highest usage and worldwide acceptance. Because the subject is relatively new, this work begins by summarizing the history and important definitions of the cryptocurrency ecosystem. Afterwards, the formation of the bitcoin price and its great volatility is explained through a recent study by Kancs et al. (2015). Then, the main risks and problems that arise with the free use of bitcoin will be analyzed and possible solutions are proposed that could mitigate these obstacles. This research project ends by going over the main risks that should be taken into account when investing or using cryptocurrencies and how bitcoin could be used as a great portfolio diversifier.

Keywords: Bitcoin, History, Problems, Cryptocurrencies, Volatility, Price formation, Portfolio diversification, Risks.

TABLA DE CONTENIDO

Contents

1	Introduction	9
2	History and Background	9
2.1	Before bitcoin	9
2.2	Background	10
3	Definitions and Specifications	15
3.1	Definition	15
3.2	Centralization and Decentralization	16
3.3	Bitcoin evolution	17
3.3.1	Currency Exchanges	17
3.3.2	Digital Wallets	18
3.3.3	Mixers or Anonymizers	19
3.3.4	Mining pools	20
3.4	Bitcoin network and its characteristics	20
4	Price Formation	22
4.1	The Model	24
4.2	Testable Hypotheses	25
4.2.1	Hypothesis 1: Market forces of bitcoin supply and demand	26
4.2.2	Hypothesis 2: Investment attractiveness	27
4.2.3	Hypothesis 3: Global macroeconomic and financial developments	28
4.3	Results	29

5	Analysis	31
6	Risks	38
7	Regulation	43
7.1	Consumer protection	43
7.2	Money laundering, bribing and tax evasion	44
7.3	Regulatory options	44
8	Bitcoin as a Financial Asset	45
9	Conclusion	49
10	References	53

ÍNDICE DE FIGURAS

1	Top 10 Cryptocurrencies by Market Capitalization	14
2	Distribution amongst the largest mining pools	36
3	Weekly price history	38
4	Weekly volume history	39
5	Reported DDoS attacks on bitcoin services over time	42
6	Bitcoin correlation matrix with major assets and currencies	46
7	Optimum portfolio analysis	47

1 Introduction

The rise of cryptocurrency in the past decade is more than just a technological innovation or feature. It can be seen as a real world incarnation of a monetary system, which lacks some characteristics of fiat currencies like USD, EUR, Yen, and others; but features other advantages like no central issuer, no monetary regulations and other characteristics. Some people go as far as to affirm that cryptocurrency or bitcoin may supplant the current international regime of fiat currency issued by the respective central banks. The purpose of this paper is to explain how cryptocurrencies work, what are their differences, limitations, problems, advantages and usability in our modern world. What are the key factors that affect its price formation and whether bitcoin can be treated as a currency or as a speculative asset. Although my research is about cryptocurrencies in general, it will frequently refer to bitcoin because it is the most relevant in the topic and is considered the benchmark cryptocurrency. This work will also briefly analyze the problems bitcoin has to face along with some possible solutions and to conclude, I will go over some of the key risks that should be considered when using cryptocurrency and provide a short analysis of how bitcoin can be used as a potent portfolio diversifier.

2 History and Background

2.1 Before bitcoin

Before the emergence and popularity of cryptocurrencies like bitcoin, there have been some examples of digital currencies that also managed to attract a great deal of

attention. These currencies usually behave in a closed environment like in the case of online games and are designed to be a payment opportunity for the players within this environment. One of the oldest examples of this type of currency is the Linden Dollar, which emerged in the virtual world of an online video game called Second Life. This currency made it possible for players to purchase Linden dollars with real fiat money (EUR, USD, YEN, etc) and then use these linden dollars to purchase in game goods and services. Ernstberger (2009) analyzed the policies of Linden Dollar and found out that this currency is used as money equivalent. He found that users in Second Life spend Linden Dollars the same way as people spend real money in the real life.

Another example of a very successful virtual currency is the virtual gold that is used in the massively multiplayer online role-playing game (MMORPG) called World of Warcraft. This currency was very successful inside its environment, and even though it had a closed design that limited its use to the game, multiple websites started offering World of Warcraft gold to be delivered in-game in exchange for real money payments. Of course, this method of obtaining gold in the game violated its terms of service, but today the game is still so popular that there are still a variety of websites offering gold and even in game content to players willing to spend the money.

In contrast to these examples, bitcoin allows us to analyze the emergence of a global digital currency in a new and much more open way than the currencies that are environment-limited.

2.2 Background

The origin of bitcoin began when in 2008, when Satoshi Nakamoto published a white paper proposing a peer-to-peer electronic cash system. His purpose was to

provide an easier way for online payments to be sent directly from one party to another without the need to go through a financial institution (Nakamoto, 2008). In 2009, the first cryptocurrency called bitcoin was created based on Nakamoto's white paper. In the following years, many other cryptocurrencies were introduced. All of these currencies are considered decentralized systems, i.e., they have no central authority and cannot be ruled or influenced by any common monetary laws. Cryptocurrencies use cryptography to control transactions, prevent fraud and manage the supply. Once a transaction has been confirmed, it is digitally recorded into a "blockchain", which can be described as an accounting system. All payments and transactions are validated by a decentralized network. I will further explain this functionality in the next section.

Although bitcoin has implemented a very effective safeguard against counterfeiting and fraud, the system is still vulnerable to theft. Given that bitcoin is a digital currency, it must be stored in a digital wallet or an exchange. Exchanges are websites that facilitate trade between cryptocurrencies and fiat currencies and therefore, allow people to store cryptocurrencies as well. To access this wallet or storage, a user must remember its unique key and a password. If either one is lost, specially the unique wallet key, there is no way to recover the cryptocurrencies that were stored in that wallet. On the other hand, theft is also a problem. In February 2014, \$350 million worth of bitcoins were stolen from an exchange site called Mt.Gox, which led to the shutdown of the exchange (Gandal & Halaburda, 2016). Even though bitcoin has made sure that it is impossible to counterfeit or fabricate more bitcoins outside the system, its protocol was not a hundred percent secure and probably still isn't.

On august 15, 2010 it was discovered that a certain block in the network authorized a transaction that created 184 billion bitcoins for three specific addresses. This was possible because at that time, the code did not account for outputs so large that

they overflowed when summed, allowing the hackers to proceed with the transaction. However, this was fixed in a matter of hours by a revised protocol. The illegally created bitcoins were made obsolete by network consensus and the supply of bitcoins came back to normal (Coindesk.com, 2018).

Bitcoin mining requires a huge amount of processing power, which has made it impossible for a single individual to successfully mine a block in a reasonable amount of time. Because of this, many companies have started investing in large amounts of hardware and began to offer their mining services to any person who wants to buy a mining contract. Basically, you can purchase the hashing power you want and everything that you get to mine with that power is yours, minus a small fee. This way users have the possibility to invest in a good mining contract, instead of buying a supercomputer that would also make them incur in massive electricity costs. Given that bitcoin price has been on the rise, more and more mining pools started to appear on the web. The problem is, however, that these companies are not regulated by any anti monopoly law and theoretically, could get consolidated into two or three large mining pools. This makes us think of another latent vulnerability of bitcoin.

There is one type of attack that bitcoin is still vulnerable to, and that is the 51 percent attack. This attack is considered as bitcoin's, and many other cryptocurrencies that follow a similar protocol, greatest inherent flaw. Given that the coin is decentralized, it can be compromised if one player gains 51% control of the computing power of all miners. This could allow the player to implement any change to the currency's system and give the power to control the (as of this writing) almost \$65 billion dollars worth of bitcoin across the globe. To date, the only mining pool that has come close to obtaining 50% is Ghash.io. However, despite widespread concern, bitcoin has become a widely used cryptocurrency all over the world, and every year dozens of mining pools

join the network to seek profitability. This ensures that the mining power keeps being spread into many different mining pools, keeping the biggest miners away from the verge.

The supply of most cryptocurrencies increases by a predetermined rate and cannot be changed by any central authority. It can be thought of as the most democratic money supply rule ever. The only way to create more coins is to get more than 50% of the network to agree on the change and proceed to implement the protocol. There are about 17.4 million bitcoins in circulation, with the final maximum supply reaching 21 million in the year 2150. Some other coins like Litecoin (LTC) have a higher maximum supply of 89 million. (Coindesk, 2017) This has generated concerns about the deflationary aspect of the currencies due to its limited supply, which will be further analyzed in this paper.

Bitcoin was initially popular because of its anonymity, which enabled many underground websites to trade illegal goods and accept bitcoins as a way of payment. On October 2012, the US government shut down the biggest site that was involved in illegal activities called SilkRoad (Forbes, 2017). Despite this, bitcoin price continued to climb over a few months afterwards. Overall, bitcoin has experienced massive fluctuations in value, mainly because of speculation, coin hoarding, massive deflation and general uncertainty as to how this industry would develop.

By the end of 2013, almost all cryptocurrencies were based on the bitcoin protocol, which is open source. However, each cryptocurrency had implemented its own set of changes into its protocol. For example, Litecoin was based on the bitcoin protocol too, but implemented a faster payment authorization code, which allowed it to confirm transactions in 1/4th of the time it took for bitcoin. Some other coins like Ethereum removed their maximum supply cap, allowing the miners to “fabricate” as many coins

as their processing power allowed them to do so.

By 2014 there were hundreds of alt-coins in the market. Most of them did not provide a significant improvement over bitcoin. This surge in entry into the cryptocurrency market was mostly because it was relatively cost less to develop a coin based on the open source protocol of bitcoin, and because every coin founder has made millions doing so. As of February 2014, the 34th largest alt coin in the market had a capitalization of one million dollars. Today, the same position has a capitalization of \$687 million and the 100th altcoin has a value of \$157 million. The top 5 cryptocurrencies by market capitalization are bitcoin, with \$65.6 Billion, XRP with \$13.7 billion, Ethereum with \$10.7 billion, Stellar with \$2.6 Billion and bitcoin Cash with \$2.3 billion. The total cryptocurrency capitalization now sits at \$121 billion (CoinMarketCap.com, 2018).


















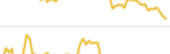


#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$65,686,500,285	\$3,773.20	\$5,331,454,007	17,408,712 BTC	-4.41%	
2	 XRP	\$13,696,635,649	\$0.339636	\$402,757,397	40,327,341,704 XRP *	-3.58%	
3	 Ethereum	\$10,724,978,525	\$103.50	\$2,030,680,074	103,622,536 ETH	-6.07%	
4	 Stellar	\$2,619,486,357	\$0.136682	\$67,549,395	19,164,799,106 XLM *	-7.56%	
5	 Bitcoin Cash	\$2,312,028,425	\$132.16	\$94,602,327	17,494,663 BCH	-11.98%	
6	 EOS	\$2,015,607,471	\$2.22	\$843,422,775	906,245,118 EOS *	-9.34%	
7	 Tether	\$1,843,469,845	\$0.993023	\$3,101,780,974	1,856,421,736 USDT *	-0.70%	
8	 Litecoin	\$1,750,606,896	\$29.45	\$392,897,765	59,448,038 LTC	-5.52%	
9	 Bitcoin SV	\$1,517,053,652	\$86.80	\$75,327,376	17,477,861 BSV	-3.92%	
10	 TRON	\$930,586,625	\$0.014069	\$69,827,418	66,145,018,619 TRX *	-2.11%	

Figure 1: Top 10 Cryptocurrencies by Market Capitalization

Despite the improvements introduced by hundreds of other currencies and slow transaction problems with bitcoin, it managed to hold its position on the top. This is very interesting because while it is easy to create another coin with a similar protocol, once the coin is created and in circulation, it is difficult to change the protocol. The only way would be by consensus among loosely connected developers. It is extremely difficult for bitcoin to do so, but it does not mean it never happened before. On August 1st, 2017 bitcoin had implemented a revised protocol which allowed bitcoin to have a much faster transaction time. However, a great part of the network wanted to stay with the previous protocol because of many different reasons, and therefore refused to implement the new code. Developers later agreed to “fork” the revised protocol into a new currency called “bitcoin cash” (BCH)(Verge, 2017). Basically what happened was the bitcoin network separated into two: bitcoin and bitcoin cash. Those that wanted to stay with the older protocol stuck with bitcoin, and those who wanted the new system went on to bitcoin cash. This is a very common process for cryptocurrencies, given that they are decentralized, only majority decisions can implement huge changes. And when those changes are not approved by the totality of the network peers, those peers are free to separate from the network and create a whole new currency.

3 Definitions and Specifications

3.1 Definition

To begin, it is important to define what exactly a cryptocurrency is. A cryptocurrency is a method of constituting a virtual coin and guaranteeing a secure ownership and transaction using a cryptographic problem. This problem is designed to be easy to

verify, but difficult to solve. Most cryptocurrencies use a hash target method for this purpose. The hash target or difficulty of the problem is adjusted periodically, every 2 weeks in the case of bitcoin, based on the total computing power on the network. This makes it so the time between solutions is almost constant.

Unlike traditional currencies that are issued through central banks, bitcoin has no central monetary authority. It is underpinned by a peer-to-peer computer network, similar to the network of BitTorrent and Skype. bitcoins are mathematically generated by computer intensive tasks, a procedure called as bitcoin "mining". (Harwick, 2015). The mathematical function of the bitcoin system was set up in a way that it becomes progressively more difficult to mine more bitcoins over time, at the end there can be a maximum supply of 21 million coins, therefore there is no way to create more and devalue those that are already in circulation without a major change in the code (which would be subject to a vote).

3.2 Centralization and Decentralization

One of the most important innovative characteristics in bitcoin, compared to other digital currencies issued by governments or corporations, is that it is completely decentralized. That means that there is no central authority that can could manipulate transactions, impose fees or regulate it in any way like Banks usually can with fiat money. Decentralization offers certain advantages. First of all, it avoids concentrations of power that could let a single government or organization take control. By its nature, it helps to avoid any central point of failure. For the system to collapse it would be necessary to physically shut down every computer in every node around the world. It also offers greater privacy for users than any other centralized digital currency

and a faster and more cost-effective way to make payments around the world.

3.3 Bitcoin evolution

I will briefly review the most important categories that have helped bitcoin evolve into what it now. These categories include currency exchanges, mining pools, wallet services and mixers.

3.3.1 Currency Exchanges

Currency exchanges are a very important part for any cryptocurrency ecosystem. They allow users to trade their fiat currencies (U.S Dollars, Euros, Sterling Pounds, etc) for cryptocurrencies like bitcoin, Litecoin, Ethereum, and many others. Just like a traditional financial market, they provide users with ask and bid prices and some also allow to post more complex orders like limit, stop-loss, fill-or-kill, etc. By doing so they charge a small commission which is rarely higher than 1%

Every transaction regarding a cryptocurrency like bitcoin is usually accompanied by a conversion to a conventional fiat currency. However, some exchanges allow cryptocurrencies to be traded directly for other cryptocurrencies without needing to convert. Every price quote is calculated in real time for each cryptocurrency mostly by supply and demand. Given that it is a decentralized system and its code is open source, it is easy for intermediaries to join the system. However, since cryptocurrencies became so popular, there was a number of regulatory changes and requirements imposed by governments regarding the use and trade of these currencies. For example, China has banned financial institutions from trading cryptocurrencies. United States has imposed harder regulatory requirements for currency exchanges in order to protect users and

limit its effects on the financial markets. In other countries like Germany, exchange houses are considered as deposit banks and require a large minimum capital requirement.

Most importantly, intermediaries that wish to trade cryptocurrencies must have a strong online infrastructure that can resist all kinds of cybernetic attacks without compromising the electronic assets. Any intermediary can be a potential target for hackers and, like I mentioned above, some have managed to get away with the electronic assets and caused some exchange houses to shut down. Given the irreversible and hard to trace nature of these assets, crypto exchanges' biggest investment should be its cyber security and strong infrastructure capable of processing thousands of transactions per second while withstanding possible DDoS attacks.

3.3.2 Digital Wallets

Cryptocurrency wallets are necessary when users need to store their digital currencies. There is a number of ways to do so and each cryptocurrency has a slightly different way to generate a wallet. The most common way is to install a program on your computer that will generate you a personal address and a private key (which you will need in order to transfer the assets). However, some users find this method unsecure and unappealing (imagine someone storing millions worth of bitcoin on their pc). A crash or some physical damage to the pc could render the electronic assets inaccessible very easily. Given these problems and the general tendency to store everything of value "in the cloud", many users rely on a digital wallet service.

This service keeps your electronic wallet and the private keys on a internet connected server. A user is able to access their wallet by using an account just like you would by using online banking. Technically this method is safer for the average user, but it

also can be more dangerous. These types of services must bear with the same risks as an exchange house would. It needs to protect against cyber-attacks. Some digital wallets allow users to keep their private keys, meaning that the service itself is unable to spend your bitcoins even if it wanted to, nor hackers would be able to steal them without your private keys. This is how Blockchain.info, CoinPunk and StrongCoin operate. The only downside is that if a user somehow loses its private key, he would be unable to recover his electronic assets. In practice, this type of service tends to increase centralization as much as crypto exchanges.

3.3.3 Mixers or Anonymizers

So far, we have stated that a user can stay anonymous when trading cryptocurrencies by only providing his public address to his wallet. However, anyone who knows that this is your specific address will be able to see all your transactions ever since you first used that address (although he will not be able to know who you are sending to). Specially banks and exchange houses that require users to register with real ID and provide some documents may be able to link your identity to the wallet address you are working with. This is where mixers come into play. To preserve the user's privacy, mixers pool a set of transactions in unpredictable combinations, therefore making it impossible for someone to track who you sent the funds to specifically. This way, an observer will only see that you sent an amount to the mixer's address, but he will not be able to tell where those funds will end up. These types of intermediaries definitely help to improve the privacy of the crypto network, but it generates additional risks and costs. For example, a mixer that is not trustworthy enough might run off with your funds. A user that wants to guarantee his anonymity might have to incur in additional fees up to 3%, however, mixing algorithms are not public and therefore its efficiency

can be questioned.

3.3.4 Mining pools

Ever since bitcoin was created, it has become exponentially more difficult to mine than ever. Today it is impossible for a single user to mine bitcoin by their own without having very costly and expensive to operate hardware. That's why mining pools were created. What they basically do is they pool together all the computational power from every user that wishes to be part of the pool, and once a user solves the blockchain problem, the rewards are shared between all the users of the pool, proportionate to the processing power each user provides minus a small fee. Technically, a mining pool large enough could compromise bitcoin's trustworthiness. When a mining pool holds the majority of the computational power (more than 50%) it can modify the transaction records, double spend bitcoins and even revert transactions. Although this would be completely evident to the rest of the users, nevertheless it would generate massive price fluctuations because of fear and reduced trust and could possibly crash a cryptocurrency's value.

3.4 Bitcoin network and its characteristics

The entire bitcoin network serves to monitor and approve transactions by keeping a log or a ledger that is encrypted and sent to all the peers on the network. This log is collectively maintained by all the nodes in the network and every new transaction is broadcast and approved via the network. This process is computationally intensive, and therefore it is rewarded. All pending transactions are stuffed into a blockchain, which is heavily encrypted via complicated mathematical problem. Users around the

world can use their computing power to find a specific hash for that blockchain, and when they do, they are awarded bitcoins. This has prompted users to gather ever more powerful computers to use for bitcoin mining (Harwick, 2015).

The major characteristics of the bitcoin system that Iwamura, et al. (2014) summarize are:

- No authority is responsible for issuing or managing the bitcoin system. Its operational rules are open and transparent to everyone in the network. No malicious intervention can happen without the approval of all the peers in the network, therefore no discretionary intervention can be expected. This purely peer-to-peer system can allow online payments directly from one party to another without the use of a financial institution.
- All bitcoin transactions are organized in the log into blocks called blockchains, which have a sequence number, a timestamp, a cryptographic hash of the previous block, some metadata, a nonce and a set of valid bitcoin transactions. Every new block contains the hash of the previous block, allowing users to confirm and verify that no preceding block has been modified.
- Any player may choose to become a “miner”, which means they can use their computing power to attempt to rehash the new blocks containing new or pending transactions and add them into the log. This procedure is called proof of work and is rewarded by bitcoins. Essentially, this is the only way new bitcoins can be created, with ever-diminishing returns throughout the years.
- Nakamoto (2008), the creator of this system, argues that the proof of work solves the problem of determining representation in majority decision making.

Proof of work is essentially one CPU power – one vote. The majority decision is represented by the longest blockchain, which has the biggest effort invested in it. If honest nodes control the majority of CPU power, this chain will grow the fastest and render obsolete and invalid the other nodes.

- To compensate for Moore's law, which states that the number of transistors in a CPU will double every year, effectively increasing the computing power; the proof of work difficulty is determined by a moving average of a number of blocks per hour.
- Incentive is paid for proof of work. Every few years the reward for each blockchain is halved. It was 50 bitcoins in 2009-2012, 25 in 2013-2016, 12.5 in 2017-2020, 6.25 in 2020-2024 and so on to zero in 2140. After reaching the maximum number of bitcoins at 21 million, the incentive falls entirely on transaction fees (Iwamura et al., 2014).

4 Price Formation

An article made by Ciaian, Rajcaniova and Kancs in 2015 is the first in literature that studies bitcoin price formation by considering both traditional determinants of currency price, such as the common market forces of demand and supply, and cryptocurrency-specific factors like bitcoin attractiveness for investors (Kancs et al., 2015). In order to explain bitcoin price formation I will mostly refer to this article, but also other studies from Buchholz et al. (2012), Kristoufek (2013), Wijk (2013), Bouoiyour & Selmi (2015), and others.

Buchholz et al. (2012) find that a very important determinant for bitcoin price, or any other currency for that matter, is the interaction between bitcoin supply and demand. The supply determines the amount of coins in circulation and therefore its scarcity on the market. In the previous section I explained that the bitcoin supply is pretty much fixed and limited in a way that there can only be 21 million bitcoins. Therefore, it is safe to affirm that the demand of bitcoin is a key factor for its price formation.

According to Kristoufek (2013), bitcoin price formation can not be explained by current economic theories such as purchasing power parity, cash flows model or uncovered rate parity, because several features which usually form the basis of currency price are absent on bitcoin markets. Specifically, given that bitcoin is not issued by any central bank of government, it is detached from the real economy as there are no real macroeconomic fundamentals that would determine its price formation. Findings from Bouoiyour et al. (2014) provide a strong argument that bitcoin mostly behaves like a speculative bubble and therefore is detached from macroeconomic fundamentals. According to Bouoiyour, Selmi and Tiwari, the contribution of speculation to bitcoin price dominates other drivers such as market forces of supply and demand.

Wijk (2013) states the importance of the role of global macroeconomic development, captured by stock exchange rates and oil price measures, in determining bitcoin price. Van Wijk finds evidence supporting that the Dow Jones index, the euro-dollar exchange rate and the oil price have significant impact on the value of bitcoin in the long run.

An important shortcoming of previous studies is that they look separately at specific bitcoin price determinants without trying to consider possible interactions between them. Also, most studies do not account for potential structural breaks in bitcoin price

series, which can lead to biased results when performing econometric estimations. The article by Kancs et al. (2015) attempts to close this research gap by accounting for all three types of bitcoin price determinants identified in previous literature: market forces of supply and demand, indicators of attractiveness for investment and global macroeconomic and financial development, to explain the formation of bitcoin price and account for interactions between them too.

In order to identify and assess the determinants for bitcoin price formation, Kancs et al. (2015) derive an econometrically estimable model from the Barro (1979) model for gold standard. Second, based on previous studies on bitcoin price formation, they extend the canonical model to capture factors which are specific to digital currencies and formulate testable hypotheses. Finally, in order to test the bitcoin price formation hypotheses, time-series analytical mechanisms to daily data for the period 2009–2015 was applied.

4.1 The Model

Bitcoin price formation can be analyzed in an augmented version of Barro (1979) model for gold standard. For this model, it was important to denominate the stock of money base of bitcoins in a traditional government controlled currency such as the dollar. Similarly, the study also assumes that users need to convert bitcoins into dollars or other fiat currencies in order to operate in common economies using traditional currencies for purchasing goods and services.

Lets suppose that B represents the total stock of bitcoins in circulation and P^B denotes the exchange rate of bitcoin (dollar per unit of bitcoin). The total bitcoin money supply, M^S is then given by $P^B B$:

$$M^S = P^B B$$

The demand for circulating bitcoins in dollars, M^D , is assumed to depend on the general price level of goods and services, P , the size of bitcoin economy, G , and the velocity of bitcoin circulation, V . The velocity measures the frequency at which one bitcoin is used for purchasing goods or services.

$$M^D = \frac{PG}{V}$$

The equilibrium between bitcoin supply M^S and bitcoin demand M^D implies the following:

$$P^B = \frac{PG}{VB}$$

In a perfect market, the equilibrium price is given by this last equation, which implies that the price of bitcoin decreases with the velocity and stock, but increases with the size of bitcoin economy and the general price level. It is also important to note that some variables in the last equation such as P^B , P and G adjust simultaneously, which can cause endogeneity issues when estimating the price relationship econometrically. In order to avoid this issue, time series analytical mechanism will be applied.

4.2 Testable Hypotheses

Kancs et al. (2015) use the above outlined Barro's (1979) model for gold standard and insights from previous empirical studies mentioned to derive a testable hypotheses of bitcoin price formation:

1. Market forces of bitcoin supply and demand
2. bitcoin attractiveness for investors
3. Global macroeconomic and financial developments

4.2.1 Hypothesis 1: Market forces of bitcoin supply and demand

According to Buchholz et al. (2012) and Bouoiyour & Selmi (2015), one of the key drivers of bitcoin price is the interaction between bitcoin supply and demand on the bitcoin market. The demand for bitcoin is primarily driven by its value as a medium of exchange for goods and services, i.e., by its value in future exchange.

The main difference between gold standard and bitcoin is that the demand for bitcoin is driven by its value in future exchange, whereas the demand for commodity currency is driven by its intrinsic value and its value in future exchange. The supply is given by the stock of circulating bitcoins which is known and predefined in the long run. Having said that, the supply of bitcoin is exogenous.

The empirically estimable model of bitcoin price can be rewritten as follows:

$$P_t^B = \beta_0 + \beta_1 p_t + \beta_2 g_t + \beta_3 v_t + \beta_4 b_t + \varepsilon_t$$

where ε_t is an error term. According to the underlying theoretical framework of Barro (1979), Kancs et al. (2015) expect β_1 and β_2 to be positive, whereas β_3 and β_4 would be negative. Also, the total stock of bitcoins in circulation, b , is a semi-exogenous variable because the supply is largely predefined. Therefore we can imply that impact of coefficient β_4 on bitcoin price should be small or statistically insignificant.

4.2.2 Hypothesis 2: Investment attractiveness

Bitcoin has been created relatively recently, compared to standard currencies like dollar or other investment goods such as gold. Because of that, there are many factors in addition to traditional currency price determinants that determine investment demand for bitcoin (Barber et al., 2012), (Buchholz et al., 2012), (Kristoufek, 2013).

Bitcoin price is affected by the risk and uncertainty of the whole cryptocurrency system. Because bitcoin is a fiat currency and thus intrinsically worthless, it does not have a derived value by itself or cannot be used in a production process (such as gold). The value of a fiat currency is based on trust that it will be valuable and accepted as a means of exchange in the future (Greco, 2001). Trustworthiness and acceptance are specially relevant for bitcoin as it is a very new currency and is in the phase of establishing its market share by building trust and credibility. The credibility of bitcoin is mostly connected to the security of the bitcoin system. Given that bitcoin is a digital currency and can only be used through the internet, cyber security is a very important matter.

Cyber attacks can and have destabilized the bitcoin system in the past. Barber et al. (2012) and Moore & Christin (2013) have examined 40 bitcoin exchanges and found out that 18 have been closed down after cyber attacks. One special example was Mt.Gox, once the world biggest exchange, which collapsed in 2014 due to a cyber attack that allowed the criminals to steal 850 thousand bitcoins, which led the exchange house to bankruptcy. Negative news such as these affect bitcoin's attractiveness for investors.

Given that the currency is so new, its attractiveness for investors and therefore bitcoin's price is determined by transaction costs for potential investors and users.

According to Gervais et al. (2001), Grullon et al. (2004) and Barber & Odean (2007), potential investors' and users' decisions can be affected by an increase or decrease of attention in the news media. Given that investment demand depends on the costs associated with searching for information for potential investment opportunities, like stock exchange, the investment opportunities that are under attention in the news media may be preferred by potential investors because they reduce search costs. Lee (2014) finds evidence that the alteration of positive and negative news generated high price cycles. It is possible to imply that the attention-driven behaviour from investors and users can affect bitcoin price positively or negatively, depending on whether the news is positive or negative.

In order to account for investment attractiveness in bitcoin price formation, Ciaian, Rajcaniova and Kancs extend the estimable model as follows:

$$P_t^B = \beta_0 + \beta_1 p_t + \beta_2 g_t + \beta_3 v_t + \beta_4 b_t + \beta_5 a_t + \varepsilon_t$$

where a_t captures investment attractiveness. β_5 can be either positive or negative as either type of news attracts attention.

4.2.3 Hypothesis 3: Global macroeconomic and financial developments

The role of macroeconomic and financial development is further stressed by Wijk (2013). This development can be captured by variables such as stock exchange indices, exchange rates, oil price measures, etc. The impact of macroeconomic indicators on bitcoin may happen through different channels. For example, stock prices may reflect general macroeconomic developments of the global economy. Positive macro and financial developments may stimulate the use of bitcoin and therefore strengthen its

demand, thus increasing its price.

Inflation and price indices are also important macroeconomic and financial development indicators. According to Krugman et al. (2018), oil price is one of the main sources of demand and cost pressures, and it may provide an early indication of inflationary development. Therefore, when oil price changes, there could be potential changes in the general price level, and this may lead to appreciation or depreciation of the traditional currencies. This variation in fiat currencies could stir demand for bitcoin as a means of temporary store of value to avoid losing money due to inflation.

Also, according to Dimitrova (2005), there could exist a negative relation between a currency's price and macro financial indicators. A decline in the stock market could induce foreign investors to sell their assets. This may lead to a depreciation of the respective currency, and therefore stimulate bitcoin demand and its price, for the same reasons stated above. In order to account for macroeconomic and financial developments, the econometric model gets extended as follows:

$$P_t^B = \beta_0 + \beta_1 p_t + \beta_2 g_t + \beta_3 v_t + \beta_4 b_t + \beta_5 a_t + \beta_6 m_t + \varepsilon_t$$

where m_t captures macro and financial indicators. β_6 is expected to be either positive or negative.

4.3 Results

Kancs et al. (2015) empirical results confirm that market forces of bitcoin supply and demand have an important impact on bitcoin price, implying that the formation of bitcoin price can be explained largely in a standard economic model of currency price formation. In particular, the demand side drivers such as the bitcoin economy

have a strong impact on its price. Given that supply is exogenous, it is likely that the development of the demand-side drivers will be key determinants of bitcoin's price in the future.

Second, it was found that the arrival of new information impacts bitcoin's price positively, which is probably a result of increasing trust among users. The results suggest that when bitcoin was little known, the online queries about bitcoin generated a stronger impact on bitcoin price than in later years when it became more mainstream. In the long run, the online information queries about bitcoin have no impact on bitcoin price (Kancs et al., 2015)

Third, the hypothesis that affirms investor speculations are also affecting bitcoin price could not be rejected. The statistically significant short-run impact of Wikipedia views and new posts on bitcoin price could be an indicator of speculative short-run behaviour of investors. Speculative trading of bitcoins is not necessarily an undesirable activity per se, as it may serve to generate benefits in terms of absorbing excess risk from risk adverse users and providing liquidity on the bitcoin market. On the other hand, a downside of the speculative investment is that it may increase price volatility and create price bubbles. Thus, the success of bitcoin hinges on its ability to reduce the potential negative implications of such speculations and expand the use of bitcoin in trade and commerce (Kancs et al., 2015)

Finally, the estimates do not support previous studies that the global macro-financial development may be driving bitcoin price. Ciaian, Rajcaniova and Kancs find that a significant impact of global macro-financial development captured by the Dow Jones index, exchange rate and oil price, affect bitcoin price only in the short run. In contrast, for the long run, they don't determine bitcoin price. Furthermore, the impact is not significant in all estimated models.

Understanding the bitcoin price formation is highly important from a general monetary policy point of view and from a bitcoin ability to serve as a medium of exchange for global economy point of view. Ciaian, Rajcaniova and Kancs's findings contribute to a better understanding of the determinants behind the enormous bitcoin price fluctuations experienced in recent years. A desirable property of any currency is that it holds its value over short to medium periods of time, as long as it does not create distortion when used as a medium of exchange in transactions. The results suggest that this may not hold for bitcoin. Large price movements alter the purchasing power potentially causing costs and risks to firms and consumers who use it as a means of exchange for goods and services.

5 Analysis

One of the problems that bitcoin experiences is its price instability, which is mostly caused by the weakness of regulations over the currency or fears of governments attempting to prohibit its use. It can also be attributed to the total issue limit of 21 million bitcoins. As people start to realize the terminal value or the value of the last bitcoin issue, the fever will grow, effectively driving the currency price to the skies. This in turn should attract miners, but by construction, rewards from mining have been declining over the years while the cost of technology has been going up because of competition for scarce resources. It looks like it is just a matter of time before bitcoin miners find the mining activity to no longer be profitable. As miners begin to leave, the market value of bitcoin can drop as transactions would take longer times to approve (because of fewer miners). Therefore, the profitability of mining would drop further and the transaction fees could rise or the immigration of miners to other alter-

native cryptocurrencies would accelerate. This is an important problem that bitcoin will have to face in the future, and also is a product of its own design.

There is a very interesting argument that Hayek (1999) wrote, and it states:

Once the system had fully established itself and competition had eliminated a number of unsuccessful ventures, there would remain in the free world several extensively used and very similar currencies. In various large regions, one or two of them would be dominant, but these regions would have no sharp or constant boundaries, and the use of the currencies dominant in them would overlap in broad and fluctuating border districts. Most of these currencies, based on similar collections of commodities, would in the short run fluctuate very little in terms of one another, probably much less than currencies of the most stable countries today, yet somewhat more than the currencies based on a true gold standard. If the composition of the commodity basket on which they are based were adapted to the conditions of the region in which they are mainly used, they might slowly drift apart. But most of them would thus concur, not only in the sense of running side by side, but also in the sense of agreeing with one another in the movements of their values (p.223).

I have to agree with Hayek, because the rise of cryptocurrency can already be seen as a new global currency that Hayek talks about. Competition is beginning to eliminate a number of unsuccessful ventures (other currencies), and eventually might be left with the most trustworthy, solid and secure currencies which have evolved and progressed far beyond all the hundreds of currencies that we currently have. Certainly,

it is too soon to make predictions at this time. However, it is safe to say that eventually all the currencies that are currently in use in the global market will collapse to a few strong and trustworthy ones. We might even stick to a currency that is unregulated by central authorities. The reason behind my beliefs is that this would make transactions easier, prevent intervention by central authorities, which in turn might prevent crises. It can help eliminate price distortions between countries and reduce the exchange rate volatility overall. Having a few powerful currencies around the world would definitely improve international commerce and lead to a more open market policies which, in turn, will lead to better price communication and resource distribution *à la* Hayek.

Another common problem that bitcoin or any other cryptocurrency faces is that it lacks an interest rate. Normally, when you deposit fiat currencies into financial institutions, you get a specific interest rate depending on the longevity of the deposit and other factors. Bitcoin and other cryptocurrencies refuse to have any relationship with banks and financial institutions. Furthermore, the price of the bitcoin has not been determined yet and is highly volatile, as it was explained above. Therefore, the interest rate cannot be determined either. We could calculate an implicit interest rate for bitcoin, but it would also be too volatile and practically useless. However, in theory, any money or currency, including cryptocurrency can earn interest income in exchange of lending or deposit. McCandless & Wallace (1991) have demonstrated this. Eventually, when bitcoin's price volatility fades, someone might create a way to represent the rate of return for lending cryptocurrencies to a third party (Iwamura et al., 2014).

There is one thing academics have been asking and that is why did Nakamoto, the creator of bitcoin, set a limit of total bitcoin issues. Apparently, he seemed to believe that a decreasing supply of money would prevent the currency from having inflation.

Even though his paper does not say that, he might have been influenced by the writing of Milton Friedman on his money supply rule Iwamura et al. (2014). While it is true that a geometrical reduction of the money supply will avoid inflation, it can cause deflation. Many researchers predict deflation in the long run for bitcoin because of a deflationary spiral caused by people hoarding bitcoin, waiting for a higher purchasing power in the future. Unfortunately, Nakamoto did not foresee the full effects of his limited supply rule. At this time very little can be affirmed about the future deflationary problems because it mostly depends on its user's behaviour, demand and regulation. Following what I have analyzed so far, it's important to provide some recommendations for an Ideal Cryptocurrency.

- First of all, there should be no supply limit, to eliminate the possibility of a deflationary spiral.
- The price of the ideal bitcoin should reflect the marginal cost of its production. In other words, it should reflect the cost of electricity, computer hardware, security, networking costs, etc.
- Once the bitcoin reflects its marginal cost, it can be properly evaluated by market competition. The pricing will become easier and more transparent. Bubble effects would be rendered obsolete (Iwamura et al., 2014).
- Given that the marginal costs becomes stable, it will be possible to obtain the implicit interest rate by arbitrage between the price of bitcoin today and tomorrow.
- The marginal cost of bitcoin production should be discounted by the technological

growth. Assuming a marginal cost such that

$$P_t = MC_t/TC_t$$

inflation can be defined as

$$P_{t+1} = (1 + \pi_t)P_t$$

Assuming that the marginal cost of production grows at the rate of β and technology grows at the rate of α . In the two periods, inflation can be expressed as

$$1 + \pi_t = (1 + \beta)/(1 + \alpha)$$

rearranging yields

$$\pi_t = (\beta - \alpha)/(1 + \alpha)$$

If the technological change rate (α) is higher than the marginal cost growth rate (β), then deflation might happen and *vice versa* (Iwamura et al., 2014).

One final problem, and one that is purely theoretical as of today, is the risk of 51% that I mentioned before. Theoretically, when a mining pool reaches the majority of the mining power of the currency's network, it is able to stop, reverse and double spend transactions however it pleases, without risking network disapproval. In other words, it can give the power to manage billions of dollars worth of transactions. Once a mining pool, a company or a group of individuals reaches this dangerous level, this could cause instability and generate damaging price fluctuations in the currency's value. Major investors are always on top of what is happening with their currencies, and when they begin to realize that the mining power is being consolidated into fewer groups,

they will begin to worry and probably shift their investments into other safer assets. This could generate massive price fluctuations and trigger millions of stop-loss trades that could devastate the currency's price and eventually lead the major mining pools into bankruptcy.

However, this scenario at the moment is very unlikely. Currently the top 3 mining pools that have the biggest share of the mining power of bitcoin are Unknown with 22%, BTC.com with 15.4% and SlushPool with 13.3% (Blockchain.info, 2018). To clarify, the "Unknown" pool means that its origin has not been determined. These shares are not likely to grow because there is plenty of competition in the market, and it is not so easy to consolidate power in a short period of time, specially when the total number of miners and pools is growing.

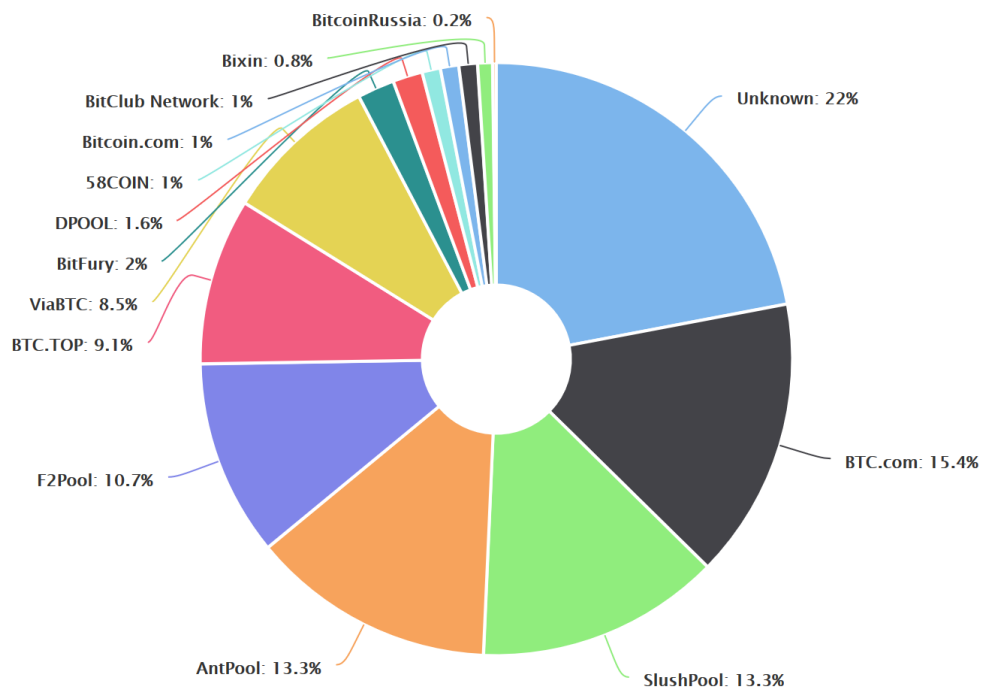


Figure 2: Distribution amongst the largest mining pools

This makes us think of a common situation that most other companies experience: Corporate consolidation. Currently there are no laws that regulate all the mining pools that have been appearing year over year. In addition, it would be practically impossible to regulate them effectively given that they can be located anywhere in the world (usually where electricity is cheaper). It would be impossible for a certain authority to try to impose anti-monopoly laws for these mining pools without some kind of global consensus. Given this lack of regulations, there is nothing that can stop these mining pools from merging or colluding with each other. Theoretically mining pools probably realize the power that they could amass by colluding or merging with other mining pools, but this scenario is unlikely because it would trigger red flags for most people invested in these assets, the price would drop significantly because of fear and uncertainty, therefore the mining profits would drop too. So overall there is no incentive to actually try and amass most of the power because such an attack would be fairly evident.

However, we can conclude that at least some kind of regulation is needed to restrict the possibility of something like that happening. Maybe there is a way to do this without the help from a central authority. Maybe the developers will think of this problem in the future and begin analyzing changes of protocols or ideas that could limit the hashing power consolidation. At this point in history, we cannot be sure. All is left for now is to expect more and better economic involvement into the whole cryptocurrency topic. Developers should keep contact with numerous economists that would be willing to advise and provide feedback for the cryptocurrency's protocols and rule sets. That way, we can at least avoid making the same mistakes that we have made in the past and eventually come up with the perfect cryptocurrency.

6 Risks

Because of bitcoin's nature, it faces risks that differ from other common payment methods and stores of value. In this section I will review the market risk, the shallow market problem, transaction risk, counter-party risk, operational risk, privacy related risks and regulatory and legal risks.

The most common of all is the market risk. Any user that chooses to hold bitcoins faces market risk because of fluctuation in the exchange rate price of bitcoin and fiat currencies like USD. Figure 3 shows the weekly price history of bitcoin in USD for the last 2 years along with the trading volume. The evident volatility that this graph shows us that it is a source of concern for all users and investors that try to use it as a currency, financial asset or storage of value.

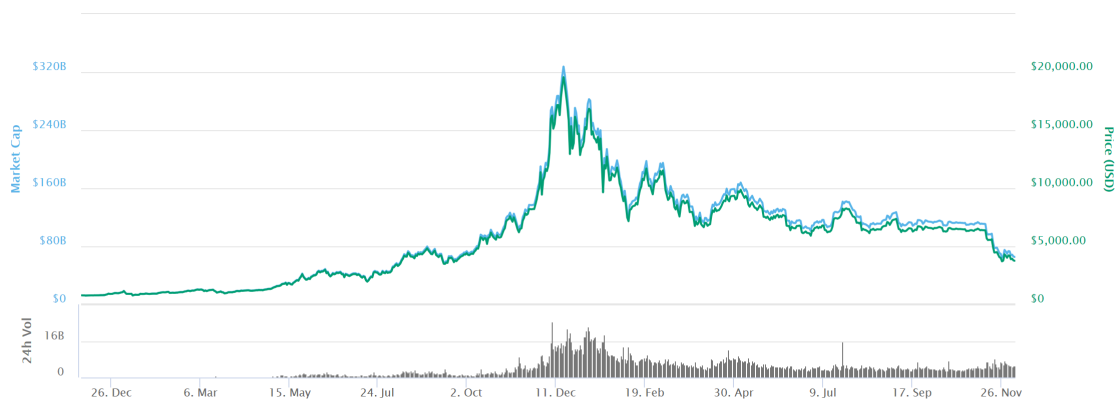


Figure 3: Weekly price history

Figure 4 shows the weekly volume of bitcoin across all exchanges for the same period of time. We can see that there is a consistent minimum of 200,000 bitcoins traded every week since 2016, and in the later years this value skyrockets to an average of 400,000 in 2017 and 600,000 for the beginning of 2018. Therefore, it is safe to

say that there is not enough proof to suggest that there might be a shallow market problem. If a person is willing to purchase or sell a large amount of bitcoin, he can do so on one of the biggest exchanges without a problem.

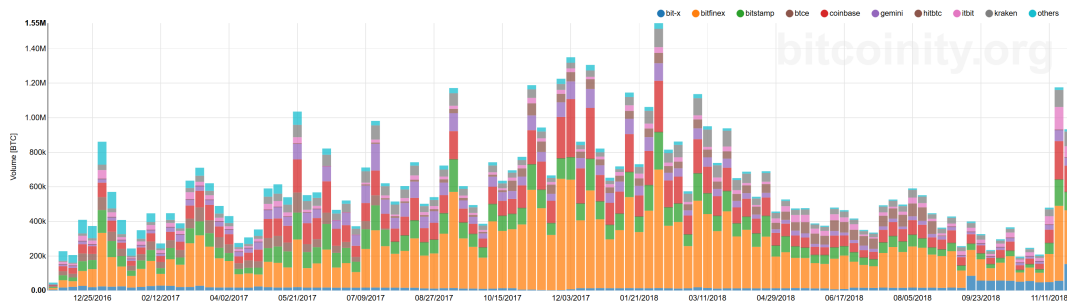


Figure 4: Weekly volume history

The counterparty risk has become even more substantial over the years. When users convert currency to bitcoin and leave their bitcoin funds in the exchanges, these exchanges act as de facto banks. According to a study by Moore & Christin (2013) 45 percent of bitcoin currency exchanges ceased operation. Most high volume exchanges that closed had to do so because they were hacked or had a security breach that resulted in large amounts of bitcoins being stolen. On the other hand, some small exchanges just disappeared without explanation. According to the study, 46 percent of the closed exchanges did not reimburse their customers after shutting down. One might think this issue can be avoided by holding the digital assets in a digital wallet service. However, other risks arise as these firms become a lucrative target for hackers and cybercriminals. The best way to avoid a counterparty risk is to avoid any counterparty and choose to hold the digital assets in an offline wallet on a secure computer without internet connection.

Transaction risks arises when sending and receiving payments. Due to the bitcoin's

blockchain technology discussed at the beginning of this paper, transactions do not clear instantly when they are executed. They clear only when they have been added to the authoritative block chain. These transaction batches happen every 10 minutes and one of two things could happen: first, there is a risk that the current authoritative block chain might be corrupted or cast aside by the majority of participants by whatever reason, causing the transactions recorded in that block chain to be rendered ineffective. This scenario is highly unlikely but worth mentioning. Second, participants could double-spend bitcoin through rapid transactions before the block chain got updated. Fortunately, this issue has already been mitigated.

Another transaction risk derives from the use of blacklisted bitcoins. These type of bitcoins are mostly obtained by theft, and some exchanges or arbiters would publicly announce the hash number (much like the serial number of paper currency) of these bitcoins to ask the community to reject them. There are two main problems that arise from the use of these blacklists. First, a new or uninformed user might unknowingly accept one of these blacklisted bitcoins and then might find it difficult to make a transaction with. Second, blacklists create the possibility to reject a transaction, allowing big and ill-motivated players to use this strategy for personal gain. Lastly, a widespread use of blacklists could alter the price of these bitcoins creating more confusion in an already not so clear topic and undermining bitcoin's fungibility at the same time.

There are other risks that compromise bitcoin's technical infrastructure and its security, this is encompassed by operational risk. A user might do everything he can to protect his digital assets. However, digital vulnerabilities, operator error, security flaws and malware generate operational risk for both users and intermediaries. Also, another operational risk is the so called "51 percent attack" that I mentioned earlier. These types of attacks are popular with new cryptocurrencies that have a small base

of users in the network. However, this is far from being a concern for bitcoin, because the sheer number of players in the network makes it almost impossible to somehow gather 51% of the power, even through the use of mining pools.

DDoS or distributed denial of service attacks are another form of operational risk very common within all types of digital information systems, specially in cryptocurrency. This type of attack are often done by a group of people or sometimes even by one single person by using a large amount of “bots” or malware infected computers across the internet that make a series of frequent requests to a specific server at the same time, clogging its resources and halting its service and usability altogether. This can be used to attack a mining pool and prevent its participants from solving the current puzzle, giving the advantage to other mining pools that are trying to do the same task. News of a DDoS attack on a specific exchange could undermine its trustworthiness and scare its users away to other exchanges. Attackers could even demand ransom from vulnerable exchanges to stop the attacks. Figure 5 shows the number of DDoS attacks reported by users on bitcointalk.org from 2011 to 2013, showing a clear growing trend through the years.

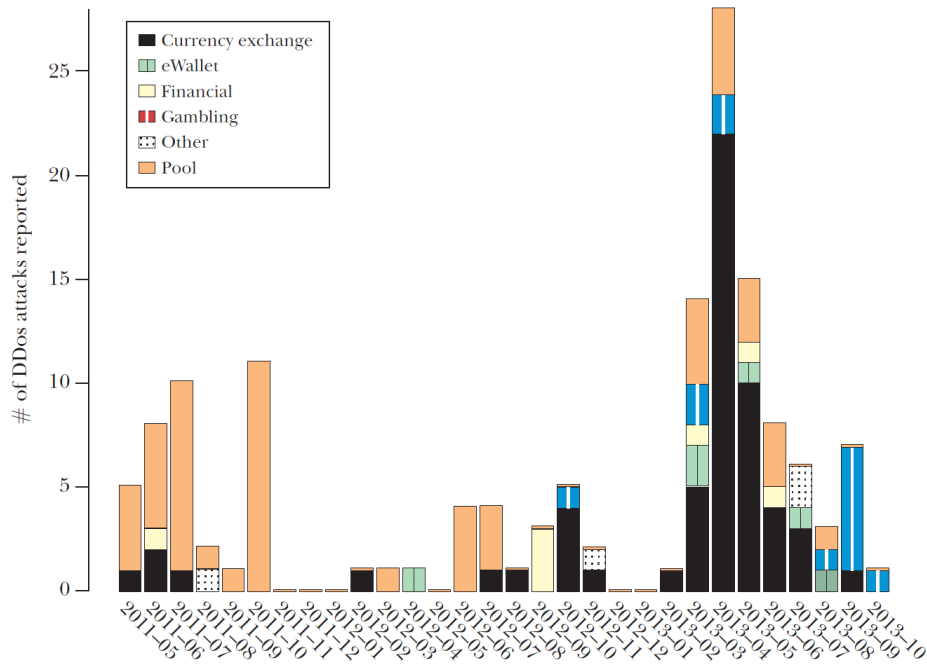


Figure 5: Reported DDoS attacks on bitcoin services over time

Finally, one last topic of concern over bitcoin is its privacy. Supposedly by design every transaction in the block chain is anonymous and is not linked to any name or personal information. However, transactions can be linked back to their origin – the people that made them. This means that transactions are not actually anonymous but pseudonymous that specify a user’s public key. If one is decided to track a user’s spending behavior, he can do so just by knowing the user’s public address. Furthermore, a bank or a financial institution could link a user’s information to his public key. This can be easily done when funds are converted to or from currencies in traditional banks. This privacy problem can be avoided by intermediaries that offer anonymizing services. They offer to randomly mix your funds with others and send them across a random number of accounts throughout the network at different times and finally to a user’s

specified address in order to make the funds untraceable to their origin. However, this can also be seen as a way of sacrificing privacy risk for extra operational risk due to the possibility of losing the funds throughout the process by a number of reasons.

7 Regulation

Originally, the vision of bitcoin has not been broadly in tension with regulation and government in its early years. However, after its exponentially increasing popularity and growth there now appears to be many possibilities of regulatory oversight that could be useful and not necessarily lead to undermine bitcoin's line of cyber-libertarianism. Before proceeding to suggest useful regulations it is necessary to review the reason to begin regulating this new digital asset.

7.1 Consumer protection

After the failure of the biggest exchange, Mt, Gox, which lost more than 300 million in bitcoin, regulatory action has been suggested by many victims and even managers of other exchange houses. Generally, it is desirable to have some type of process enforced by law that would guarantee a fair and equitable distribution of any remaining assets of a collapsed exchange among its users. This risk of collapse also calls for more transparency and disclosure to new users to help them understand the potential risk they might be getting into. Another consumer protection concern arises over the fact that transactions cannot be reversed. Most common electronic payments done with fiat currencies provide mechanisms that allow users to reverse an unauthorized or wrong transaction, such protections are often backed by law. However, due to bitcoin's design, it would be necessary to make some very important changes in its block chain

mechanism, a change that the users most likely will not welcome.

7.2 Money laundering, bribing and tax evasion

Bitcoin is often criticized for being a tool that facilitates crimes and illegal transactions due to its relative anonymity. Currently, the main concerns are money laundering, tax evasion and illegal transactions or bribes. Due to bitcoin's anonymous design, it is a safe haven for illegal operations regarding money laundering and tax evasion. Bitcoin transactions are already difficult (but possible) to trace. However, if one is willing to go through "mixers" or "anonymizers" that I have discussed in the previous topic, then it would be almost impossible for law enforcement to track the transactions. This greatly assists criminals in conducting their business without leaving a trail of evidence like would normally happen through the use of a fiat currency like the USD. Even tax evasion and bribes among corporations and high government officials can benefit from this digital asset if all the necessary steps are taken to completely anonymize the transactions. This opens new ways for corruption to arise, specially in underdeveloped countries where institutions are less developed than in first world nations.

7.3 Regulatory options

Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore (2015) analyze a series of regulatory options. A key challenge is where to impose constrains. They conclude that regulating each individual would be impossible due to their quantity, geographic distribution and privacy protections in the network. Instead, it would be more feasible to regulate through the key intermediaries like exchange houses. However, a person willing to commit crime will likely foresee this liability and avoid exchange

houses altogether.

The most important example that illustrates the challenges of regulation and their power was Silk Road. Silk Road was hosted as a website hidden under the Tor network (a network that is built for anonymity among its users). This website offered a range of illegal drugs, products and services, however, it was eventually seized by the FBI. The poor operational security led the FBI to large merchants that eventually led them to the website's operator, Ross Ulbricht. The whole case with Silk Road is evidence enough that certain control or regulation is needed in order to allow the law enforcement to fight crime.

Currently, most operations done through exchanges and large intermediaries can be audited by regulators. This is possible because of recent laws passed in the United States and some European countries that classify these intermediaries as money-service business, and therefore require them to perform registration, reporting and recordkeeping. This way regulators can trace transactions more easily, and effectively disincentivize crime (at least through these channels). To conclude, there are a number of possible regulations that could be applied to exchanges and intermediaries that can allow better control and transparency of transactions. Some might argue that this violates their privacy and right to anonymity or even that it undermines the whole bitcoin's anonymity vision. However, it all comes to the usual trade off of privacy for better security and vice-versa. It is just a matter of finding an optimum equilibrium.

8 Bitcoin as a Financial Asset

This section will briefly examine bitcoin's ability to serve as an investable financial asset by incorporating it in a portfolio that includes the top 10 world currencies, U.S.

bonds, U.S. Stocks, U.S. Real Estate and the VIX Volatility index. The objective of this section is to prove whether bitcoin enhances portfolio's efficiency. To assess the portfolio performance consisting of various asset classes it was necessary to find major indexes representing each asset class. Major world currencies were represented by the Bloomberg Dollar Spot Index (BBDXY). This index evaluates the U.S. Dollar against the top 10 most actively traded currencies. The S&P500 index was chosen to represent stocks. Bonds were represented by the Bloomberg composite bond index (BIG), the real estate market was represented by the FTSE NAREIT (FNARTR) total return index; and the commodities were represented by the S&P500 CME spot commodities index. The data for these indices was downloaded from the Bloomberg Terminal with a weekly frequency from 2010-07-10 until 2018-11-30. There was a total of 435 observations of returns for each asset class.

To measure the portfolio performance under the inclusion of bitcoin, first a correlation matrix was created. Figure 6 shows us the correlation matrix of bitcoin with the top five fiat currencies, five major asset classes, Gold and the SP500 volatility index.

	BTC	Gold	EUR	YEN	Pound	AUD	CAD	BBDXY	SPX	BIG	FNARTR	SPGSCI	VIX
BTC	1.000	-0.045	-0.033	-0.026	0.011	-0.009	-0.046	0.006	0.044	0.019	0.012	0.071	-0.059
Gold	-0.045	1.000	0.409	-0.478	0.336	0.388	-0.343	-0.553	-0.011	0.566	0.143	0.243	0.116
EUR	-0.033	0.409	1.000	-0.330	0.587	0.472	-0.435	-0.877	0.155	0.668	0.209	0.262	0.016
YEN	-0.026	-0.478	-0.330	1.000	-0.192	-0.233	0.158	0.537	0.235	-0.734	-0.018	0.012	-0.308
Pound	0.011	0.336	0.587	-0.192	1.000	0.431	-0.457	-0.673	0.235	0.466	0.207	0.296	-0.080
AUD	-0.009	0.388	0.472	-0.233	0.431	1.000	-0.680	-0.693	0.470	0.436	0.490	0.377	-0.295
CAD	-0.046	-0.343	-0.435	0.158	-0.457	-0.680	1.000	0.664	-0.470	-0.355	-0.427	-0.535	0.297
BBDXY	0.006	-0.553	-0.877	0.537	-0.673	-0.693	0.664	1.000	-0.253	-0.793	-0.351	-0.362	0.062
SPX	0.044	-0.011	0.155	0.235	0.235	0.470	-0.470	-0.253	1.000	-0.042	0.679	0.406	-0.797
BIG	0.019	0.566	0.668	-0.734	0.466	0.436	-0.355	-0.793	-0.042	1.000	0.268	0.103	0.154
FNARTR	0.012	0.143	0.209	-0.018	0.207	0.490	-0.427	-0.351	0.679	0.268	1.000	0.219	-0.494
SPGSCI	0.071	0.243	0.262	0.012	0.296	0.377	-0.535	-0.362	0.406	0.103	0.219	1.000	-0.295
VIX	-0.059	0.116	0.016	-0.308	-0.080	-0.295	0.297	0.062	-0.797	0.154	-0.494	-0.295	1.000

Figure 6: Bitcoin correlation matrix with major assets and currencies

From this figure it is safe to affirm that bitcoin has an extremely low correlation with all the assets, therefore it could be a potent diversifier in a investment portfolio. To measure the efficiency of bitcoin as part of a portfolio several optimal portfolios were created using the Excel Solver tool. The three main measures were Minimum variance, Maximum return and Maximum Sharpe Ratio. Restrictions of long-only positions were placed on all weights for all scenarios, so no short sales were allowed.

Optimal Portfolio Analysis						
	With Bitcoin			Without Bitcoin		
	Min Variance	Max Return	Max Sharpe	Min Variance	Max Return	Max Sharpe
Bitcoin	0.00%	100.00%	2.00%	-	-	-
Gold	0.83%	0.00%	3.03%	0.83%	0.00%	1.65%
Currencies	42.61%	0.00%	41.14%	42.61%	0.00%	41.01%
SP500	5.47%	0.00%	13.37%	5.47%	0.00%	14.24%
Bonds	48.24%	0.00%	38.90%	48.24%	0.00%	42.75%
Real Estate	0.00%	0.00%	1.57%	0.00%	100.00%	0.34%
Commodities	2.85%	0.00%	0.00%	2.85%	0.00%	0.00%
Portfolio Metrics						
Variance	0.039	326.917	0.208	0.039	4.508	0.064
Std. Deviation	0.197	18.081	0.456	0.197	2.123	0.253
Expected return	0.046	3.932	0.143	0.046	0.220	0.064
Sharpe Ratio	0.115	0.216	0.262	0.115	0.093	0.161

Figure 7: Optimum portfolio analysis

Figure 7 Shows the results of an optimal portfolio with and without bitcoin under the minimum variance, maximum expected return, and maximum sharpe scenarios. For the minimum variance scenario, we can see that bitcoin is not included into the portfolio. This makes sense because bitcoin has a huge variance relative to the other assets, therefore if one looks to minimize risk then bitcoin should not be included into the portfolio. For the scenario of maximum return, we can see that 100 percent of the weight goes to the asset with the highest expected return. This would maximize portfolio expected return, however, this kind of portfolio is not diversified and too

risky to be considered as an investment. When the Solver was used to maximize the Sharpe Ratio, interesting results were found. The Sharpe Ratio measures the excess return per unit of deviation in an investment asset or a trading strategy. Therefore, the bigger the ratio, the better return per unit of risk. The table shows that the highest possible Sharpe Ratio for a portfolio without bitcoin was 0.161. However, when bitcoin is incorporated into the portfolio, an optimum weight of 1.65% is assigned and the Sharpe Ratio improves to 0.262. Basically, when bitcoin is incorporated in to the portfolio, a higher excess return can be achieved per unit of risk, therefore portfolio's overall efficiency is improved.

Wu & Pandey (2014) have made a similar analysis regarding portfolio efficiency and bitcoin and found similar results. The results of Chen Y. Wu and Vivek K. Pandey show that first, this asset is not currently used as a medium of exchange for goods and services. Most merchants still price their goods in normal currencies and prefer fiat currencies over digital ones like bitcoin. Secondly, bitcoin's high price volatility suggests it is not a good store of value and way too risky. Under these definitions, it is concluded that bitcoin lacks the key attributes of a currency and instead looks more like a illiquid financial asset. The analysis shows that among the top 10 fiat currencies analyzed, bitcoin was the riskiest currency with the highest standard deviation. A correlation analysis was performed as well, and it shows that bitcoin return has very low or insignificant correlation with other fiat currencies, even gold. Whereas fiat currencies were all correlated between each other. This enforces the conclusion that bitcoin does not behave like a currency.

Wu & Pandey (2014) also concluded that bitcoin shows very low correlations with other assets such as bonds, real estate, stocks and commodities. This indicates that bitcoin could be used as an excellent portfolio diversifier. The optimal portfolios formed

with major asset classes including bitcoin show that it would be optimal to include a small weight of bitcoin into the portfolio, as it helps to maximize portfolio's return. Finally, when both portfolios (with and without bitcoin) were compared, the one that included bitcoin had higher returns per unit of standard deviation. Therefore, Chen Y. Wu and Vivek K. Pandey's analysis proves that adding bitcoin into a portfolio does indeed enhance its efficiency. Finally, the Black Litterman approach showed that even under pessimistic scenarios (bitcoin would lose 50% of its value) the weights for bitcoin were significantly reduced but stayed positive. This shows that when bitcoin is added into a portfolio with an optimum weight, its diversifying effects outweighs the potential losses even if a 50% loss of its value is to be expected.

9 Conclusion

Cryptocurrencies are relatively new, and still have many problems to overcome. The most important issue is price stability. Given a limited supply in the case of bitcoin, people are trying to speculate on its value in the future and are hoarding bitcoins, generating deflation in the process. On the other hand, the news can also create big price fluctuations in cryptocurrency value. For example, about a month ago people were afraid of the Chinese government trying to ban Cryptocurrencies as they were beginning to disrupt their strict monetary policy. That created massive selling orders of the main Cryptocurrencies like bitcoin, Litecoin and Ethereum. However, once the fear faded, the price of these coins rose back up and is trading now at levels higher than ever.

Understanding the bitcoin price formation is highly important from a general monetary policy point of view and to better understand bitcoin's ability to serve as a medium

of exchange for the global economy. Ciaian et al. (2016) findings contribute to a better understanding of the determinants behind the enormous bitcoin price fluctuations experienced in recent years. Kancs et al. (2015) provided a very interesting model to represent bitcoin's price formation and came to the conclusion that bitcoin's price is mostly determined by demand-side drivers. It was also found that the arrival of new information positively impacts bitcoin price and that speculative trading is not necessarily an undesirable activity per se. It benefits in terms of absorbing excess risk from risk adverse users and provides liquidity to the crypto market. A desirable property of any currency is that it holds its value over short to medium periods of time, as long as it does not create distortion when used as a medium of exchange in transactions. The results suggest that this may not hold for bitcoin. Large price movements alter the purchasing power potentially causing costs and risks to firms and consumers who try to use it as a means of exchange for goods and services.

One of the problems that bitcoin and most other cryptocurrencies face is its great price volatility. As it was analyzed, this volatility is driven mostly by speculative trading and hoarding. Due to the ease of access to this cryptocurrency, many people try to benefit from its volatility by making short term investments with hopes to earn quick money. Although these activities are not undesirable per se, the way bitcoin and many other cryptocurrencies are used at the moment show that they are not being utilized as a currency but rather as an investment asset.

From an investment point of view there are many risks that one should consider before beginning to use cryptocurrencies as an investment or transactional asset. First, due to its high volatility market risk is high and this asset's ability to be used as a storage of value is rendered obsolete by the price fluctuations. Second, the counterparty risk has become substantial over the years. As the cryptocurrency market keeps growing,

there is more incentive for hackers to attack exchanges, wallet services or even infect personal computers with malware in order to retrieve personal crypto-wallet keys. Third, one should be careful when purchasing cryptocurrencies directly from somebody, as they could be blacklisted and one may find it difficult to trade them on a large exchange. Finally, as with any other asset, it is important to stay sharp and read any new information that might come up in the internet that might affect the asset's price.

Even though bitcoin's volatility makes it a very bad storage of value and a very risky investment per se, it can bring benefits when it is combined with a diversified portfolio. My analysis and the findings of Wu & Pandey (2014) show that when bitcoin is incorporated into an optimum portfolio, it increases the portfolio's efficiency by increasing excess return per unit of risk. Therefore, I would recommend using a small proportion of bitcoin to further diversify a portfolio.

Given the uncertain scenario in which these currencies develop, it is not possible to predict exactly what will happen in the future. We can only analyze certain limited scenarios and predict some bubbles like the future deflationary spiral that bitcoin will have to solve. We can also predict potential consolidation issues with the cryptocurrency's hashing power. Eventually, bitcoin might be taken over by some other cryptocurrency with better security structures; or maybe it will get polished into the best cryptocurrency ever. What is needed the most for the cryptocurrency ecosystem to flourish at a stable pace is a proper design based on economic rationalities like the ones previously described. Unfortunately, such rationalities are not fully exhibited by the current cryptocurrency ecosystem. Developers themselves usually lack economic knowledge and therefore are likely to make mistakes that for economists are kind of obvious. Therefore, it is important that cryptocurrency's developers keep in contact

with economists who would be willing to give advise and feedback for new cryptocurrency protocols and rule sets, in order to avoid making the same economic disasters that we have been experiencing throughout history.

10 References

- Barber, B. M. & Odean, T. (2007). All that glitters: The effect of attention and news on the buying behavior of individual and institutional investors. *Oxford University Press*.
- Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better—how to make bitcoin a better currency. *Palo Alto Research Center*.
- Barro, R. J. (1979). Money and the price level under the gold standard. *The Economic Journal*.
- Blockchain.info (2018). Distribution amongst the largest mining pools,.
- Bouoiyour, J. & Selmi, R. (2015). What does bitcoin look like? *Annals of Economics and Finance*.
- Bouoiyour, J., Selmi, R., & Tiwarl, A. (2014). Is bitcoin business income or speculative bubble? unconditional vs. conditional frequency domain analysis. *Munich University Library*.
- Buchholz, M., Delaney, J., & Warren, J. (2012). Bits and bets - information, price volatility, and demand for bitcoin.
- Ciaian, P., Rajcaniova, M., & Kancs, D. (2016). The economics of bitcoin price formation.
- Coindesk.com (2018). The 9 biggest screwups in bitcoin history,.
- CoinMarketCap.com (2018). Cryptocurrency market capitalizations.

- Dimitrova, D. (2005). The relationship between exchange rates and stock prices: Studied in a multivariate model. *Issues in Political Economy*.
- Ernstberger, P. (2009). Linden dollar and virtual monetary policy. *University of Trier*.
- Forbes (2017). End of the silk road: Fbi says it's busted the web's biggest anonymous drug black market,. *Forbes Magazine*.
- Gandal, N. & Halaburda, H. (2016). Can we predict the winner in a market with network effects? competition in cryptocurrency market. *Tel Aviv University*.
- Gervais, S., Kaniel, R., & Mingelgrin, D. (2001). The high-volume return premium. *The Journal of Finance*.
- Greco, T. H. (2001). Money: Understanding and creating alternatives to legal tender. *White River Junction*.
- Grullon, G., Kanatas, G., & Weston, J. P. (2004). Advertising, breadth of ownership, and liquidity. *Rice University*.
- Harwick, C. (2015). Cryptocurrency and the problem of intermediation. *The College at Brockport SUNY*.
- Hayek, F. (1999). Good money, part 2.
- Iwamura, M., Kitamura, Y., & Matsumoto, T. (2014). Is bitcoin the only cryptocurrency in the town? economics of cryptocurrency and friedrich a.hayek.
- Kancs, D., Ciaian, P., & Miroslava, R. (2015). The digital agenda of virtual currencies. can bitcoin become a global currency? *Publications Office of the European Union*.

- Kristoufek, V. (2013). Bitcoin meets google trends and wikipedia: Quantifying the relationship between phenomena of the internet era. *Scientific Reports*.
- Krugman, P. R., Maurice Obstfeld, & Melitz, M. (2018). *International Economics: Theory and Policy*. Pearson, 11 edition.
- Lee, T. B. (2014). These four charts suggest that bitcoin will stabilize in the future. *Washington Post*.
- MCCandless, G. & Wallace, N. (1991). Introduction to dynamic macroeconomic theory: An overlapping generations approach. *Harvard University Press*.
- Moore, T. & Christin, N. (2013). Beware the middleman: Empirical analysis of bitcoin-exchange risk. *Financial Cryptography and Data Security*.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Verge, T. (2017). Bitcoin has split in two.
- Wijk, D. V. (2013). What can be expected from the bitcoin? *Erasmus Universiteit Rotterdam*.
- Wu, C. Y. & Pandey, V. K. (2014). The value of bitcoin in enhancing the efficiency of an investor's portfolio. *Journal of Financial Planning*.