2017

Can Bitcoin Become a Viable Alternative to Fiat Currencies? An Empirical Analysis of Bitcoin's Volatility Based on a GARCH Model

Vavrinec Cermak
Skidmore College

Can Bitcoin Become a Viable Alternative to Fiat Currencies? An empirical analysis of Bitcoin's volatility based on a GARCH model

Vavrinec Cermak

Skidmore College, Saratoga Springs, NY

Abstract

This study examines whether Bitcoin, a digital decentralized currency, can become a viable alternative to fiat currencies. Bitcoin currently does not fulfill the criteria of being a currency because it does not function as a medium of exchange, a unit of account, and a store of value. Bitcoin's biggest obstacle from fulfilling these functions is the price volatility. A GARCH(1,1) model is used to analyze Bitcoin's volatility in respect to the macroeconomic variables of countries where Bitcoin is being traded the most. Bitcoin already behaves similarly to fiat currencies in China, the U.S. and the European Union but not in Japan. There is also evidence that Bitcoin acts as a safe-haven asset in China. The volatility of Bitcoin has been steadily decreasing throughout its lifetime. If it follows the trend of its six years of existence, it will reach the volatility levels of fiat currencies in 2019-2020 and become a functioning alternative to fiat currencies.

Keywords: Bitcoin, volatility, cryptocurrency, GARCH

Preprint submitted to Skidmore College *May 2, 2017*

Contents

List of Figures

List of Tables

Abbreviations

ARCH Autoregressive Conditional Heteroskedasticity

BTC bitcoin (unit of currency)

CNY Chinese Yuan

EIA U.S. Energy Information Administration

ETF Exchange-Traded Fund

EUR Euro

FinCEN Financial Crimes Enforcement Network

GARCH Generalized AutoRegressive Conditional Heteroskedasticity

GH/s Gigahash per second - primary measure of a Bitcoin "miner's" performance

IRS Internal Revenue Service

JPY Japanese Yen

MSB Money Service Business

PBoC People's Bank of China

SEC U.S. Securities and Exchange Commission

USD U.S. dollar

W watt (unit of power)

1. Theoretical part

1.1. Origin of Bitcoin

Bitcoin[1] was first mentioned in 2008 in a self-published white paper written by an anonymous person (or people) who went by the pseudonym of Satoshi Nakamoto [1]. In the paper, Nakamoto described Bitcoin as a payment system, which uses a decentralized peer-to-peer cryptocurrency with a finite monetary supply. There is a theory that Nakamoto created Bitcoin as a response to the global financial crisis in 2008 [2]. Before the introduction of Bitcoin, online payments relied exclusively on financial institutions that act as trusted third parties to facilitate electronic payments [1]. Nakamoto was the first developer who solved the problem of replacing the trust model with cryptographic proof, which ultimately eliminated the need of an intermediary and replaced it with a peer-to-peer network. Nakamoto also solved the problem of double spending by recording all transactions on a public time-stamped ledger called the blockchain [1]. All transactions that happen on Bitcoin are verified by network nodes, which are essentially computers that are connected to the Bitcoin network. These network nodes are called the "miners" because they are compensated in bitcoin for verifying transactions. Bitcoin compensation is an incentive that keeps the Bitcoin network running. Therefore, the nodes are theoretically "mining" bitcoin in exchange for their computing power. One year after publishing the white paper, Nakamoto released Bitcoin as an open-source software and made it available for anyone to use[2].

1.2. Brief History

Even before Bitcoin, the idea of a digital currency was nothing new. David Chaum, a pioneer for cryptographic protocols, wrote the first paper that outlined an anonymous payment system by using blind signatures [3]. Since then, cryptographers published several academic papers attempting to improve the security and efficiency of the hypothetical digital currencies [4]. Some of these ideas came to life in forms of independent digital currencies - Digicash, E-Gold, Flooz and Beenz. However, the lack of decentralization,

[1]For the remainder of this paper, I will use Bitcoin with a capital "B" when talking about the protocol and payment system. I will use lower-case "b" when talking about the denomination of the currency

[2]www.github.com/bitcoin/bitcoin

transparency and security ultimately led to the extinction of all of these attempts.

After the release of the open-source code of Bitcoin, the first 50 BTC were "mined" by Nakamoto himself in order to demonstrate the method to online observers [5]. The first Bitcoin real world transaction took place in May of 2010 when Laszlo Hanyecz, a programmer living in Florida, sent 10,000 BTC to a volunteer in the United Kingdom, who then ordered two pizzas for Hanyecz, which cost him 25 USD [5]. Today, 10,000 BTC have value of over 10 million USD. The interest in Bitcoin, especially among computer enthusiasts, led to the creation of Mt. Gox, the first bitcoin exchange. Prior to the creation of Mt. Gox, users could only "mine" their own bitcoins. However, the introduction of a bitcoin exchange meant that the users could now buy bitcoins in exchange for fiat currencies [4]. On the first day of trading, Mt. Gox sold 20 BTC and offered one BTC for the rate of 4.96 cents [5].

The first and only vulnerability was discovered in the Bitcoin verification mechanism in 2010, which allowed hackers to extract large amounts of bitcoin. However, the code was quickly patched and the falsely "mined" bitcoins were deleted from the blockchain. Ever since then, there has not been a single vulnerability in the Bitcoin verifying mechanism or Bitcoin blockchain. Moreover, the Bitcoin blockchain has never been hacked according to a former White House communicator Jamie Smith [6] and it is thought to be virtually unhackable.

In 2011, Bitcoin started to become more widely utilized. Its popularity was sparked because Bitcoin is global, anonymous, has low transaction costs, accounts cannot be frozen, and there are no prerequisites or arbitrary limits [7]. Controversial organizations such as Wikileaks started accepting bitcoins as anonymous donations [7]. Financial institutions such as PayPal, Visa, Mastercard, which were susceptible to government pressure, cut off their services to Wikileaks because of its controversial political affiliations. As a result, this made Bitcoin a perfect option to use as a donation system. However, its anonymity also started attracting illegal activities including black markets that sold illegal goods online. The operation of a darknet marketplace called "Silk Road" was discovered, which created a nightmare for the FBI because it was virtually impossible to track the illegal transactions. Even though "Silk Road" was shut down by the FBI in 2014, there are now several replacements, which still use Bitcoin as a payment system [8]. On February 9, 2011, Bitcoin briefly reached parity with USD on Mt. Gox [9].

The interest in Bitcoin skyrocketed after the Time magazine wrote one of the first mainstream articles describing the digital currency in April of 2011 [10]. Later in 2011, the first conferences about Bitcoin took place in New York City and the first European conference was held in Prague, Czech Republic [9].

In 2012, several Bitcoin startups such as Coinbase began to form. They were aimed at assisting nontechnical users in becoming familiarized with using Bitcoin [11]. Coinbase created an online, technologically friendly Bitcoin wallet, which let users purchase bitcoins in exchange for USD and then store the bitcoins online. Moreover, by the end of 2012, a French company called Bitcoin-Central became the first bitcoin exchange to be licensed to operate as a bank [12]. Bitcoin-Central also functioned within the framework of the European Union, which meant that customers' funds were held under their name rather than that of the exchange.

In 2013, FinCEN established regulatory guidelines for "decentralized virtual currencies", which classified Bitcoin "miners" and exchanges in the U.S. as MSB [9]. All MSBs are required to be registered and are subject to legal requirements such as disclosing large transactions or suspicious activities. As a result, Mt. Gox started dealing with serious legal issues. In May of 2013, the U.S. Department of Homeland Security seized more than 5 million USD from Mt. Gox's U.S. accounts because Mt. Gox had not registered as a MSB with FinCEN [9]. Mt. Gox received an MSB license in June of 2013 but ever since then, its users started experiencing long delays of their USD withdrawals [9]. Mt. Gox, was handling 70% of all Bitcoin trading [13], which means that even a slight issue with Mt. Gox resulted in significant price fluctuations of bitcoin. When difficulties with Mt. Gox became apparent, more and more people tried to withdraw their funds. Nearly one million customers lost trust in Mt. Gox resulting in a digital bank run. There were speculations that these issues were caused by a system of fractional reserves and that Mt. Gox simply did not have enough reserves to satisfy all withdrawals [14]. Towards the end of February, Mt. Gox announced that the company filed for bankruptcy protection. The company claimed that an error allowed hackers to steal more than 850,000 BTC, worth around 480 million USD [15]. Mt. Gox had 127,000 creditors, a debt of 6.5 billion CNY ($\approx$63.7 million USD), and assets of 3.84 billion CNY [16]. Because Mt. Gox was located in Tokyo where bitcoin exchanges were unregulated, customers had no legal protection. Moreover, digital currencies are not backed by the central banks. This event had crippled faith in Bitcoin for many investors and the price plummeted.

On a more positive note, the first Bitcoin ATM was launched in Vancouver in 2013 [17]. The ATM let customers withdraw their bitcoins in Canadian dollars and it also let them deposit Canadian dollars, which were quickly converted to their Bitcoin wallets. Currently, there are 956 Bitcoin ATMs in 55 countries[3]. Additionally, several retailers began accepting Bitcoin as a means of payment; notably Overstock.com, Reddit, OKCupid, Wordpress, Microsoft, Expedia and Virgin Atlantic [18]. By the end of 2014, the IRS announced that it would be treating Bitcoin as an asset rather than a currency meaning that any capital gains from selling or "mining" bitcoin are treated the same way as selling shares[4].

1.3. Bitcoin's Supply

In a centralized economy, fiat currency has, theoretically, an unlimited supply. It is at a central bank's discretion to inject money into or withdraw money from the banking system in order to match the growth of the economy. The central banks have distinct instruments of monetary policy, by which they control the monetary base. The most common methods are the open market operations, quantitative easing, modifying the reserve requirements and changing the federal discount rate.

In a decentralized monetary system, no central authority can regulate the monetary base; therefore, monetary policy would be ineffective. Bitcoins are created by the "miners" around the world as opposed to the central bank. The Bitcoin's algorithm defines, in advance, at what rate the currency will be created [1]. A new bitcoin is created when a "miner" discovers a block. A block is a file where transaction data is permanently recorded. Therefore, a blockchain is a perpetual store of records. New blocks are discovered when 'miners" solve cryptographic mathematical problems, by which they also verify the transactions. Every year[5], the number of blocks discovered is constant at 52,500. However, the number of bitcoins generated per one block halves every 210,000 blocks (roughly four years). This decreasing-supply algorithm is supposed to replicate the rate at which commodities such as gold are mined. Because of the reward halving every four years, the maximum

[3] www.coinatmradar.com

[4] https://www.irs.gov/pub/irs-drop/n-14-21.pdf

[5] On average 343 days. The length varies depending on the mining power and network difficulty. In the future, it could take significantly less time.

amount of bitcoins that can ever exist is 21,000,000. At the time of writing, there were approximately 16,250,000 bitcoins in existence. The final amount of Bitcoin can be calculated by Equation 1.

$$\frac{\sum_{i=0}^{32} 210000 \cdot (\frac{50 \cdot 10^8}{2^i})}{10^8} \tag{1}$$

Table 1 shows the number of bitcoins in existence in the short term. However, it is more difficult to estimate the amount of bitcoins in circulation, which are the bitcoins that are physically used to conduct transactions rather than stored somewhere. In 2012, Ron and Shamir analyzed the full available history of Bitcoin transactions and found that 78% of all bitcoins were stored in accounts that never made a transaction. That implies that only 22% of existing bitcoins were in active circulation [19]. In 2014, Swanson conducted a similar blockchain analysis and found that 70% of all bitcoins had not moved in six or more months implying that about 30% of bitcoins were in active circulation [20].

Year	**Date**	**Blocks**	**BTC/Block**	**BTC added**	**BTC in circ.**
1	1/2009	0	50	2,625,000	2,625,000
2	4/2010	52,500	50	2,625,000	5,250,000
3	1/2011	105,000	50	2,625,000	7,875,000
4	12/2011	157,500	50	2,625,000	10,500,000
5	11/2012	210,000	25	1,312,500	11,812,500
6	10/2013	262,500	25	1,312,500	13,125,000
7	8/2014	315,000	25	1,312,500	14,437,500
8	7/2015	367,500	25	1,312,500	15,750,000
9	7/2016	420,000	12.5	656,250	16,406,250

Table 1: Amount of bitcoins in existence in the short term

Currently, it is estimated that 99% of all bitcoins will be "mined" by 2040 and the remaining 1% will be "mined" in the next 80-100 years [5]. Figure 1 shows the rate, at which the remaining bitcoins will be added.

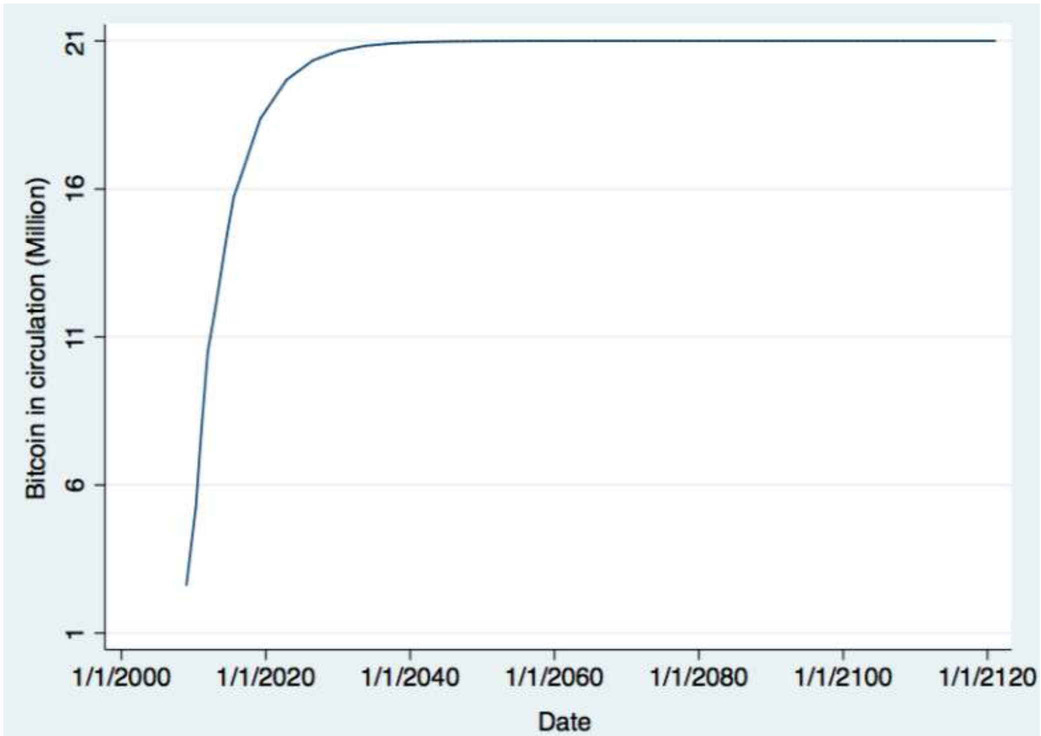

Figure 1: Amount of bitcoins in existence

However, it is impossible to predict the exact year without knowing future advances in mining power and network difficulty. The difficulty of solving the cryptographic problems increases when more "miners" are competing for a fixed amount of bitcoins. In 2009, an individual with a personal laptop could "mine" 200 BTC in a few days but in 2014, it would take about 98 years to "mine" just one bitcoin on a personal computer [21]. Thus, most of the mining right now happens in specialized mining pools with power efficient supercomputers situated in a place with cheap electricity. Because of these reasons, over 70% of Bitcoin mining pools are located in China [22]. The profitability of new "miners" entering the market decreases because of the reward halving and the lack of economies of scale, which creates a barrier to entry that could lead to a centralization of Bitcoin [23]. Bitcoin has a so-called positive feedback loop, which means that when the price of bitcoin decreases or the halving event occurs, "mining" becomes less profitable and some "miners" will be forced out of business. When there are less miners, the network automatically adjusts to decrease the difficulty of the cryptographic problems and therefore makes "mining" profitable again. In other words, Bitcoin is designed to make "mining" barely profitable on average. Valfells and Egilsson found a break-even point, at which it makes economic sense for independent "miners" to enter the market. For the current reward (12.5 BTC/block), which will be in effect for at least the next three years, the breakeven point is 600 USD/BTC [23]. In 2016, The New York Times reported that three Chinese mining companies processed over half of the Bitcoin's computing power, which technically gave them an ability to veto over any changes to the Bitcoin software and technology [22]. If the leading mining pools decided to cooperate[6], they could theoretically alter the original code and make macroeconomic decisions similar to the central banks. However, such cooperation is unlikely to be formed because Bitcoin's users would stop using the altered version of Bitcoin in favor of the older version and "miners" would lose all the profits. Any alteration of Bitcoin's code would result in a fork, which means that the network would split into two separate Bitcoin networks. At the time of writing this has yet to occur, but it is a possibility in the future.

Because bitcoins are added at a decreasing rate and there is a finite amount that will ever exist, rational people will expect the value to increase in the future. Therefore, they will tend to hold the bitcoins in the short term rather than spending it. Bitcoin is theoretically disinflationary, which means that the inflation rate is slowing down every four years until all the remaining bitcoins are "mined" and then it becomes deflationary. Deflation in fiat currencies causes economic activity to slow down because it encourages saving, and discourages consumption. Therefore, Bitcoin can act as an alternative to fiat currencies but it cannot fully replace fiat currencies because it would not be able to match the growth of the economy.

1.4. Schools of Economic Thought

In order to determine whether bitcoin can become a viable alternative to fiat currencies, I will look at two schools of economic thought - Austrian and Keynesian. I will analyze how these frameworks view Bitcoin in theory.

1.4.1. Austrian School of Economics

In 2012, the European Central Bank (ECB) published a study of the decentralized cryptographic money, in which they say: "*the theoretical roots*

[6] Assuming that they would have more than 51% of Bitcoin's mining power combined

of Bitcoin can be found in the Austrian school of economics" [24].

One of the cornerstones of the Austrian School is the Austrian business cycle theory, which originated from economists Friedrich Hayek and Ludwig von Mises. The theory suggests that the occurrence of business cycles in the economy is not a natural phenomenon but rather that it is caused by the central banks and fractional reserve banking. According to this theory, the business cycle is the consequence of the government's manipulation of the money supply and the interest rates. The idea behind it is that when the central banks keep the interest rates artificially below where the free market rate would have been, it sends a false signal to the productive segments of the economy. According to Ludwig von Mises, the false signals result in in badly allocated business investments - malinvestments [25]. According to Mises and Hayek, the only way the interest rates would decrease in a free economy is if there was an increase in savings [26]. This would cause businesses to have more money available to finance capital investments for long term purposes. Moreover, Mises and Hayek believed that if a central bank starts stimulating the economy and artificially lowers the interest rates, it creates an incentive for businesses to finance capital investments for long term purposes even if there was not an increase in savings. This causes malinvestment and overconsumption in the economy, which results in an economic boom, followed by a crisis, and the economy would ultimately try to correct itself.

In 19th and the beginning of the 20th century, the world's most successful currencies were easily exchangeable for a fixed amount of gold or a precious metal. Mises formulated an argument as "the regression theorem" of money, which says:

"*People will only accept a medium of exchange if they observe that it has value, and can actually be exchanged for things. The only way to observe that is by looking at whether it was so used in a preceding time period. Thus, this chain of observations can be followed back until the first instance in which a particular type of money was used as a medium of exchange, and in order for those first adopters to accept it, it must have had value independent of its use as a medium of exchange, or in other words, be a commodity. Paper money, especially that with no commodity backing, is only adopted when governments force it upon people.*" [27]

However, the gold standard collapsed in most economies between 1920's and 1970's because the economic growth outpaced the production of gold and the governments could not keep their promise to exchange the currency for the fixed amount of gold. Therefore, the vast majority of currencies in the world today are fiat, which means that they are not backed by a physical commodity. The value of fiat currencies relies directly on the public belief that the central bank will not increase the supply too rapidly and therefore overinflate the value of the currency to worthlessness [5]. The Austrian school claims that currency is only possible if governments monopolize the issuance of a fiat currency [28].

In 1976, Hayek published an essay, in which he described his vision of competition in currency markets; not just competition between the countries but also within the countries [29]. He believed people should be free to choose any currency they wish to use. Hayek argued that a free-market monetary system would provide a check against inflation. His reasoning was that the government would have to keep the inflation low, otherwise people would simply switch to a different currency.

In theory, the Austrian School of economic thought should find Bitcoin to be an intriguing currency because it introduces a possibility of disrupting the monopolization of the issuance of fiat currencies and because it has potential to weaken the power of central banks. If Bitcoin continues to attract more interest and if it becomes more widely used, it could introduce a viable alternative currency to people, who could switch to Bitcoin if the inflation of their domestic currency was too high. In fact, we already see this phenomenon, but on a much smaller scale. The predetermined issuance of new bitcoins and their finite monetary base is also attractive to Austrian economists because it presents certainty of the monetary supply, which they prefer over the uncertainty of central banks' manipulation of the interest rates.

However, even the bitcoin exchanges (e.g. Mt. Gox) could sell more bitcoins than they actually have and hope that there will not be a digital bank run. Fractional reserve banking could theoretically increase the Bitcoin money supply but not the amount of bitcoins on the blockchain. It is impossible to increase the bitcoin supply on the blockchain because it is predetermined and created by the "miners". It is important to note, however, that people would rather keep their bitcoins in private wallets rather than allowing fractional banking because of Bitcoin's disinflationary nature. The only reason why Mt. Gox was able to sell more bitcoins than they had is because their customers were not aware of it. All of the future efforts to create a transparent service of fractional lending with bitcoins failed because the Bitcoin community is skeptical of fractional reserve banking; especially without the oversight of an authority.

Despite these factors, the majority of economists supporting the Austrian school of economics are critical of Bitcoin and other cryptocurrencies [30][31][32]. The criticism stems from the belief that Bitcoin violates Mise's regression theorem of money because it is not backed by a commodity. However, there are some Austrian economists who are pro-Bitcoin such as Konrad Graf [33] and Peter Surda [34]. Surda and Graf have a different interpretation of the regression theorem. They believe that even though Bitcoin is not backed by a tangible commodity, it is a scarce intangible good, which satisfies the same requirements as a commodity. Therefore, according to Surda and Graf, Bitcoin satisfies the Austrian definition of a currency because it functions as a medium of exchange. I will examine whether Bitcoin satisfies the criteria of being a currency in the next chapter. It is interesting to note that most of the Bitcoin enthusiasts are supporters of Austrian economics, while the majority of Austrian economists are critical of Bitcoin.

1.4.2. Keynesian Economics

Central banks around the world use Keynesian models in order to set appropriate interest rates. Essentially, the Keynesian view of the business cycles is that the fluctuations are caused by the changes in the aggregate demand. When aggregate demand decreases, producers are not able to produce as much as previously and they must adjust in the short run. However, adjusting by cutting the production costs is difficult because wages are said to be sticky-down, which means that they can move up easily but it is harder to move them down. The producers are therefore forced to fire their workers rather than to decrease their wages, which translates to higher levels of unemployment. If less people are working, spending also decreases and aggregate demand is pushed down even further. The Keynesian model says that when the unemployment rate is higher than the natural unemployment rate, change in fiscal and monetary policies can help reduce the economic fluctuations. The natural unemployment rate is the lowest unemployment rate attainable in the economy. The relationship between unemployment and inflation in the short run is described by the Phillips curve, which indicates that there is an inverse relationship between unemployment rates and inflation.

In his book The General Theory of Employment, Interest and Money, John Maynard Keynes first developed the concept of liquidity preference. He argued that individuals value money for "*the transaction of current business and its use as a store of wealth*" [35]. Keynes also suggested that individuals give up their interest in order to spend money in the present, but also as a precautionary measure. Moreover, he saw interest as more of a reward for giving up liquidity rather than as a reward for saving. The three motives, which affect the demand for liquidity are: the transaction motive, the precautionary motive, and the speculative motive. Because of these motives, the demand for money fluctuates based on the current interest rate.

It is accepted by economists that the majority of users currently treat their bitcoins as a speculative asset rather than as a means of payment [36][19][37]. In a study that looked at blockchain data from 2009 to 2012, Ron and Shamir found that only about a half of bitcoins were spent during the first three months after being received. The same finding was accomplished by Baek and Elbeck who report strong evidence that Bitcoin volatility is internally (buyer and seller) driven, leading to the conclusion that the Bitcoin market is presently highly speculative. The interest rates are at historic lows, which incentivizes riskier investments that have higher potential returns. Therefore, we can assume that when the interest rates are lower, risk-tolerant investors will invest more in Bitcoin. When the value of Bitcoin starts to decrease, the speculative investors will try to minimize their losses and sell their Bitcoin, which causes the value to drop even lower. When the value is low, other speculative investors will enter the Bitcoin market, which snowballs the value back up. A large Bitcoin infrastructure is needed where more businesses will accept Bitcoin and individuals will use it as a payment system rather than just as an investment to hedge inflation. As I previously mentioned, Bitcoin is decentralized with a predetermined finite supply, which makes it impossible to be affected by a monetary policy and therefore, affect its inflation. Thus, we can assume that Bitcoin's demand for liquidity is largely driven by speculative motives.

Most of the modern Keynesian economists are skeptical of Bitcoin but there is not a unanimous opinion. Although Bitcoin is a relatively new concept, it has already garnered the attention of economists. Nobel memorial prize laureate Paul Krugman famously wrote a blog post titled "Bitcoin is Evil", in which he questioned Bitcoin's ability to be a reliable store of value [38]. Other economists such as DeLong and Cowen question whether Bitcoin can survive when the cost of producing a Bitcoin clone is virtually zero [39][40]. DeLong is also skeptical because Bitcoin is not backed by a "too-big-to-fail entity" that could buy it back if necessary. Cowen and other

Keynesian economists are concerned about the eventual deflationary nature of Bitcoin.

1.5. Currency Criteria

A currency is generally considered by economists to be an instrument that serves as a medium of exchange, a unit of account, and a store of value. In the next three subchapters, I will discuss whether Bitcoin satisfies these criteria.

1.5.1. Medium of Exchange

A medium of exchange is an instrument to facilitate sale, purchase, or trade of goods between multiple parties to avoid the inconvenience of a barter system. For a currency to function as a medium of exchange, it must represent a standard of value accepted by all parties. The most essential function of a medium of exchange is to measure value. A medium of exchange should have a constant intrinsic value and a stable purchasing power on average.

Bitcoin is definitely an instrument that achieves facilitating sale, purchase, or trade of goods between multiple parties. I would even argue that Bitcoin facilitates transactions more elegantly without an intermediary that often charges unreasonable fees. However, in order to become an effective medium of exchange, bitcoins would have to be accepted by a sufficient amount of merchants. Merchants have several reasons motivating them to accept bitcoin; the biggest reason being the avoidance of expensive, 2%-3%, credit card fees for each transaction. This has been especially useful for microtransactions that cost a minimum of 30 cents, which could end up being 30% on a 1 USD transaction [41]. However, the transaction fees of Bitcoin have recently been increasing because of the blocksize limit, which makes microtransactions completely unfeasible. Bohme et al. [42] found that because of the blocksize limit, the transactions could be delayed for up to an hour, which diminishes the liquidity possibilities and increases risk associated with accepting bitcoins. I will discuss the blocksize limit issue further in the "Bitcoin's Weaknesses and Altcoins" chapter.

Moreover, a big disadvantage of accepting Bitcoin payments is a minimum 10 minute waiting time until a confirmation is cleared. This means that a merchant is technically taking on a risk that in 10 minutes, the transaction will not clear. The customer can therefore double spend the same bitcoin again and the transaction would not clear before 10 minutes. However, there are now services such as BitGo instant and Coinbase, which allow merchants to basically insure every transaction for a 0.1% fee and get the payment instantly. Another disadvantage of accepting bitcoins is the extreme volatility of the bitcoin's price. Just in the 10 minutes that it takes to clear the transaction (without a service such as BitGo or Coinbase), the value of Bitcoin could potentially fall by more than the fee that is normally paid to the credit card companies. It is important to note that most of the merchants that accept bitcoins will only show prices at the register or checkout and exchange them for a fiat currency immediately after the transaction clears in order to minimize the volatility risk. Another difficulty that merchants have to deal with are the returns. Bitcoin transactions cannot be reversed and all of the revenue is immediately converted to USD. The merchants solve this by offering in-store credit denominated in USD. However, even with all of these disadvantages, some merchants offer a discount for paying with bitcoins, which indicates that transactions in bitcoin are on average more profitable than credit card transactions [43].

As Bitcoin's volatility decreases and more businesses realize that Bitcoin has smaller transaction costs when compared to the credit cards, the number of merchants accepting Bitcoin is increasing. In 2015, 160,000 merchants accepted bitcoins [44]. Several large companies such as Overstock.com, DISH, Microsoft, Dell, Expedia, Newegg, Zynga, TigerDirect and Virgin Galactic accept Bitcoin in 2017. Nonetheless, all of these companies do not accept bitcoins directly; instead they partner with a middleman (usually either BitPay or Coinbase), which takes the customers' bitcoin, immediately converts it to cash, and deposits the cash into the company's bank account [45].

Bitcoin can also be used for remittances especially because of the low fees associated with sending bitcoins across different countries. A report by Goldman Sachs from 2014 measured a cost of sending remittances using Bitcoin, which ended up being 1% on average. The average cost of sending remittances using traditional methods is notoriously high, 7.7% on average in 2015 [46].

Overall, Bitcoin works best as a medium of exchange when both parties are willing to negotiate in Bitcoin rather than just using Bitcoin as an intermediary to convert their fiat currencies from and then immediately afterwards. The reason why there are not more parties willing to do that is because of Bitcoin's volatility, which makes trading ineffective and risky. However, infrastructure has certainly been improving and this motivates more merchants to begin accepting bitcoins as a payment. When more merchants accept Bitcoin as an alternative payment, it has the potential to disrupt a very profitable monopoly on payments. Even if that means that payments in Bitcoin will be immediately converted to a fiat currency until Bitcoin's volatility stabilizes. Transactions in Bitcoin are cheap, reliable, and transparent, which makes it attractive for both the merchants and the customers. When Bitcoin becomes less volatile and the blocksize limit issue is solved, it could become a very effective medium of exchange.

1.5.2. Unit of Account

A unit of account is a numerical monetary unit of measurement of the market value of goods, services, and other transactions. In other words, it is something that can be used to value goods, services, and other transactions and make calculations. A unit of account must also be divisible, countable, and fungible.

Bitcoin's use as a unit of account is so far entirely dependent on its medium of exchange function. Bitcoin's biggest obstacle in becoming a useful unit of account is its high volatility. As previously discussed, merchants who accept bitcoin will either use a middleman or convert bitcoin to a fiat currency immediately after the transaction clears. Merchants will also post their prices in fiat currencies and only show the converted price in bitcoins at the register or checkout. These are clear indications that Bitcoin is not sufficient as a unit of account yet. However, that does not necessarily mean that it will never be. If Bitcoin's volatility ever reaches the levels of other fiat currencies, it would be entirely possible for countries to use bitcoin as a unit of account.

Bitcoin is perfectly divisible and countable. In fact, some refer to Bitcoin as having an "infinite" divisibility because the level, at which Bitcoin can be divided can be adjusted as time goes on. The current level selected in the code is 8 decimal places. The smallest unit is thus 0.00000001 BTC. However, one of the issues is that Bitcoin's price is relatively high when compared to goods and services. If I were to buy a Big Mac, which costs 3.99 USD, it would equal to 0.00379 BTC in today's prices. This creates a confusion for a consumer and makes price comparisons fairly complicated. One of the possible solutions in the future is to start using smaller units such as milli-bitcoins (mBTC) or micro-bitcoins (µBTC).

Moreover, bitcoins are not fully fungible. Any two bitcoins have the same exact value. But because all transactions are publicly available, it is common for bitcoin exchanges to discriminate between bitcoins based on the owner or their history. For example, some exchanges will attempt to block bitcoins, which have been confirmed as stolen or obtained illegally. This becomes an issue because when not every exchange accepts the so called "dirty" bitcoins, the "dirty" bitcoins become less valuable. Vorick, a Bitcoin Core developer, is worried that if "dirty" bitcoins become more common, the only way to know if bitcoins are clean is to go to a centralized service and ask for a background check. Suddenly the value of bitcoins would be decided by a centralized party, which would go directly against Bitcoin's core values [47].

Another aspect that is important to discuss is an occurrence of price fragmentation across different bitcoin exchanges. At the time of writing, the bitcoin price of two leading bitcoin exchanges BitStamp and BTC-E differed by 19 USD. The ask price at BitStamp 1048 USD and the bid price at BTC-E is 1029 USD. This creates a clear violation of the law of one price. The price disparities technically create an opportunity for arbitrage. However, because of slow bitcoin verification process and fees (exchange, deposit and withdraw), arbitrage is rarely profitable. The prices between exchanges vary greatly because of the reliability of exchanges, different fee policies, different cashout methods, and different standards of accepting "dirty" bitcoins. Since Bitcoin does not serve as a unit of account yet for the reasons above, most of the regular users will need to convert back and forth from a fiat currency. These price fragmentations and uncertainties also hinder Bitcoin as a store of value.

1.5.3. Store of Value

A store of value can be any asset that is not perishable or subject to depreciation over time. Essentially, a store of value must retain purchasing power into the future. The most liquid assets are the best store of value because they can easily be exchanged for other goods and services.

Bitcoin's utility as a store of value is dependent on its utility as a medium of exchange. That means that in order for Bitcoin to maintain its store of value, it has to rely on an expectation of others' willingness to accept it in the future. Bitcoin has no intrinsic value[7], which means that its value lies in people's willingness to keep using it. Similarly to gold, bitcoin is limited in quantity, easily transportable, easily divisible, impossible to counterfeit and people accept it as barter. However, if network effect gives bitcoin its

[7] Economists agree that bitcoin has no intrinsic value but Bitcoin enthusiasts claim that its intrinsic value is the invention of eliminating trust from the payment system.

only real value and the network is still relatively small, it remains a question whether a new cryptocurrency similar but better than Bitcoin could completely replace it. Bitcoin has a first mover advantage along with popularity, network effect, investment and trust; but so did Yahoo and MySpace. On the other hand, hundreds of alternative cryptocurrencies exist and none of them were successful at replacing or even threatening Bitcoin so far. I will talk about the largest alternative cryptocurrencies in more detail in the latter chapter. Bitcoin enthusiasts claim that Bitcoin's invention is comparable to the invention of the Internet and that if there was a cryptocurrency that was threatening Bitcoin with superior features, Bitcoin could possibly implement those features in its own protocol as well. However, this assumption has been very questionable lately as Bitcoin is being threatened by its block size limit and a solution has yet to be implemented.

Bitcoin serves as the best store of value for individuals who are looking for an unregulated and relatively anonymous store of wealth. However, if an individual is not necessarily looking for non-regulation and anonymity, he must be averse to possibility that a superior Bitcoin clone will emerge and diminish Bitcoin's biggest value maker, which is the network effect. To summarize, if an individual has a positive outlook for Bitcoin in the future, it could serve as a store of value. However, Bitcoin is currently not established enough to function as an effective store of value.

1.5.4. Overview of Bitcoin as a Currency

As of now, based on the reasons above, Bitcoin is not suitable as a currency. Currently, it could be categorized as a scarce digital commodity. Bitcoin acts more as a payment system to avoid high credit card fees rather than a medium of exchange. Businesses are not willing to hold bitcoins and, as a result, they immediately convert it to fiat currencies. This should change when volatility decreases. Bitcoin does not serve as a unit of account for many reasons but it is primarily a result of its volatility again. Cheah and Fry [48] argued that if Bitcoin were to function as a unit of account and a store of value, it would not display such volatility expressed by bubbles and crashes. Bitcoin is also not fully fungible and frequently violates the law of one price. Lastly, Bitcoin does not serve as store of value because of its volatility and uncertainty whether Bitcoin will be able to hold its value without having any intrinsic value.

The biggest obstacle that comes up while evaluating whether Bitcoin can act as a medium of exchange, unit of account, and store of value, is its volatility. If bitcoin's volatility reaches the levels of other fiat currencies, there will not be much stopping it from becoming a fully functional alternative to fiat currencies.

1.6. Bitcoin's volatility

As described in the previous chapter, price volatility is bitcoin's Achilles heel. As of the time of writing, there were roughly 16,250,000 BTC in existence with one valued at about 1,084 USD. That means that Bitcoin's market cap was currently approximately 17.6 billion USD, which is still relatively low when compared to fiat currencies. For example, even a small currency such as the New Zealand Dollar had an M1 money supply of 41.9 billion USD in February 2017. Due to Bitcoin's small market cap, it is easy to affect the price with large orders. Because Bitcoin is decentralized, its price is strictly determined by supply and demand. In combination with Bitcoin's speculative nature, its price volatility is mostly affected by external events. Investors react to these events either positively or negatively, which often causes a panic selling or panic buying. The large price fluctuations are caused mainly by the sudden government regulations, security breaches of the third party wallets or exchanges and depreciation of fiat currencies. There is one internal event that affects volatility, which is the reward halving that I discussed before.

Bitcoin's volatility has been trending downwards as the volume of bitcoins in existence and circulation increases. Another factor that helps limit bitcoin's volatility is an emergence of bitcoin derivatives exchanges[8] where customers can hedge or short sell their positions by using futures contracts. Bitfinex also offers peer-to-peer lending and marginal trading in Bitcoin, which technically allows customers to short sell. As the infrastructure improves and the volume increases, the volatility will decrease.

1.6.1. Government Regulations

In December of 2013, the People's Bank of China (PBoC) banned Chinese banks from handling Bitcoin transactions citing risks of money laundering and protecting financial stability [49]. The PBoC stated that individuals were free to buy and sell bitcoins at their own risk. This warning had triggered the bitcoin bubble to burst and introduced volatility levels of more than

[8] Deribit and BitMEX (BitMEX does not work in the United States at the time of writing)

13%. Nonetheless, these factors did not stop the existence of Chinese bitcoin exchanges. According to bitcoinity[9] and as displayed in Figure 2, in 2016, over 90% of Bitcoin's volume was traded in CNY. On top of that, over 70% of Bitcoin mining pools are located in China [22].

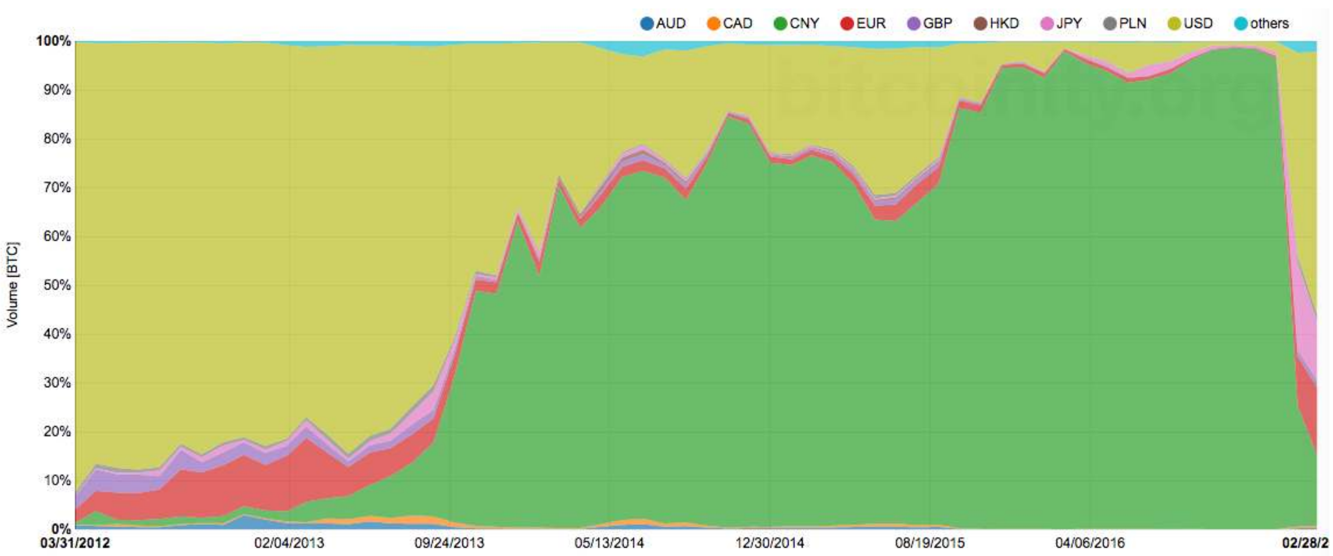

Figure 2: Bitcoin trading volume by currencies

One of the reasons why China has taken over Bitcoin is because it is not controlled and regulated by the PBoC. Therefore, we can assume that external events affecting trading in China will be the most detrimental to price fluctuations. Indeed, in January and February of 2017, Bitcoin has experienced the highest levels of volatility since February of 2015. This sudden spike has been attributed to the attempts of the Chinese government to limit the outflow of the CNY. In early January, the PBoC announced that all financial institutions will be required to notify the PBoC of any transactions over 50,000 CNY (≈7,250 USD), down from a ceiling of 200,000 CNY (≈29,000 USD) [50]. China's foreign exchange reserves have hit a 5-year low in early February of 2017 [51]. Later in February, China banned the users of the two largest bitcoin exchanges from withdrawing any bitcoins amid concerns that the cryptocurrency is being used to facilitate capital flight [52].

[9] https://data.bitcoinity.org/markets/volume/

In the following month, the PBoC will inspect the exchanges and if serious violations are discovered, the platforms will be shut down. The users of these two exchanges are still allowed to sell their bitcoins and withdraw CNY. These actions by the PBoC resulted in a huge selloff of Bitcoin, which increased the volatility greatly.

1.6.2. Security Concerns

Even though Bitcoin itself is unhackable according to security experts, third party wallets and exchanges are prone to hacks or even scams. Bitcoin platforms are attractive to hackers because of bitcoin's high price, anonymity, and lack of involvement from the government authorities. This has been an issue especially in early days of Bitcoin as these third party platforms were not as transparent and as secure as they are now. Security was a major concern in the early days and the perceived trust of investors reflected the price movements quite accurately. Whenever a security breach was announced and a large amount of bitcoins were stolen, the volatility increased. The most publicized scam was Bitcoin Savings and Trust, which ran a Ponzi scheme and achieved to steal 700,000 BTC from its investors. The most significant hack was Mt. Gox, which was handling over 70% of all bitcoin transactions at the time. It went bankrupt in 2014 and claimed that 850,000 BTC worth around 480 million USD were stolen by hackers. Mt. Gox customers lost their savings and were left with no recourse. Not only did people lose their savings, they lost their trust in Bitcoin and this drove the price down significantly. Since the insolvency of Mt. Gox in early 2014, there were two more hacks, resulting in thefts of over 19,000 BTC from Bitstamp in 2015 and 120,000 BTC from Bitfinex in 2016. The price has dropped by more than 10% in both of these instances but it has recovered fairly quickly. Nonetheless, these breaches resulted in spikes of volatility. Because it is so difficult to avoid getting hacked, most of the widely used exchanges store their virtual currency in offline storage and keep only a small percentage of funds online. The funds that are stored online are often insured, which means that the customers of these exchanges are not risking anything.

1.6.3. Depreciations of Fiat Currencies

The price of Bitcoin grew by 130% in 2016 (435 USD to 998 USD) and outperformed all of the fiat currencies and commodities. Drastic booms and crashes have become a standard for bitcoin but what is interesting is that it grew relatively organically for the first time in its history with volatility levels of under 5%. This steady growth is largely attributed to the economic uncertainties in the world such as devaluation of CNY, hyperinflation in Venezuela, Indian banknote demonetization, depreciation of the GBP caused by the BREXIT, and other events. Investors rely on Bitcoin when they want to minimize the effects of inflation and economic uncertainty, which indicates that Bitcoin could qualify as a safe-haven asset. However, even though Bitcoin is often referred to as "digital gold", there is actually very little correlation between the two when geopolitical events are factored out [53]. Gold is a much larger and more mature asset - the demand needed to boost the gold prices is much larger than the demand needed to boost bitcoin.

As mentioned before, China has the largest effect on driving the bitcoin prices. In fact, there was an apparent inverse correlation in 2016 between CNY and USD as seen in Figure 3 [54].

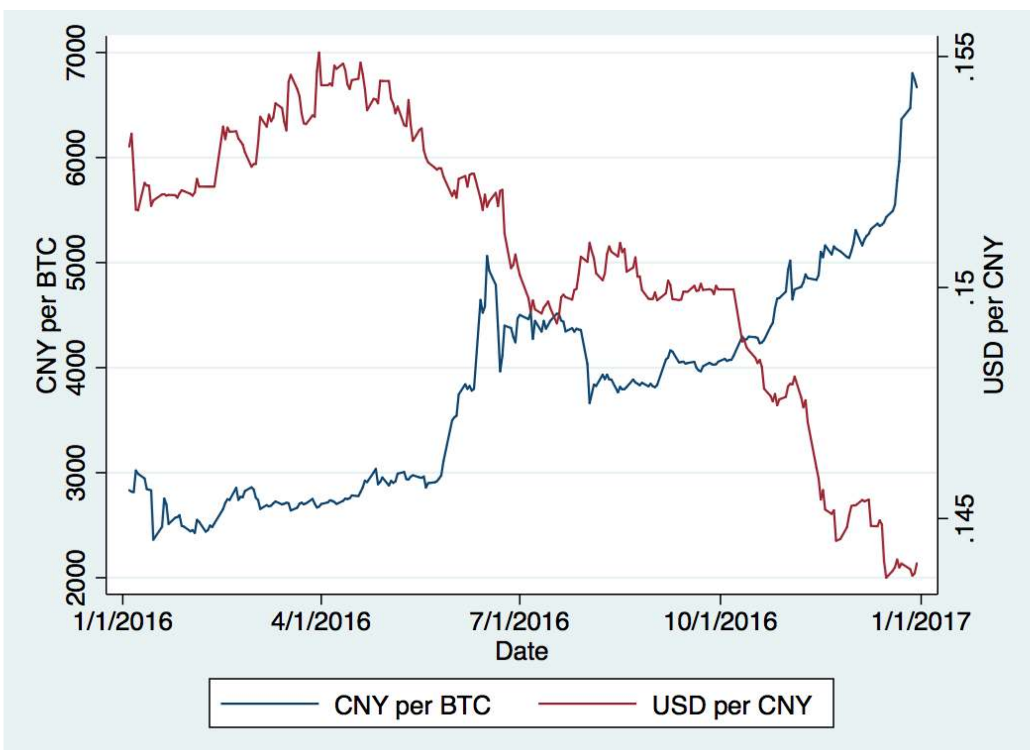

Figure 3: BTC surges when CNY falls

1.7. Bitcoin's Weaknesses and Altcoins

It is relevant to talk about Bitcoin's weaknesses because with the lack of intrinsic value, its sole value is based on trust and people's willingness to keep using it. There are currently hundreds of alternative cryptocurrencies (called Altcoins in the Bitcoin community), which try to capitalize on Bitcoin's weaknesses as well as innovate by adding new functions. Bitcoin's shortcomings currently include long verification times, relatively high fees, power inefficiency, non-fungibility and centralization. Nonetheless, the majority of these Altcoins are rarely used on a regular basis. At the time of writing, there were two cryptocurrencies that had a market capitalization larger than 1 billion USD - Bitcoin and Ethereum. Ethereum is an application platform with a cryptocurrency built-in called Ether. Ether already has confirmation times of 12 seconds instead of 10 minutes and it does not have a block size limit, which means that it could theoretically process an unlimited amount of transactions per second. Moreover, there are seven more cryptocurrencies with a market cap of over 100,000 USD. The Table 2 shows all the cryptocurrencies with a market cap of over 100,000 USD at the time of writing.

Name	**Available Supply**	**Price (USD)**	**Market Cap (USD)**
Bitcoin	16,248,737	1,084	17,610,868,623
Ethereum	90,306,627	49.348	4,456,144,390
Ripple	37,388,960,792	0.021562	806,173,295
Dash	7,199,514	68.23	491,227,135
Litecoin	50,439,682	6.50	327,616,834
Monero	14,217,500	20.24	287,743,710
Ethereum Classic	90,261,50	2.79	251,598,527
NEM	8,999,999,999	0.017586	158,271,300
Augur	11,000,000	12.82	141,002,400

Table 2: Cryptocurrency Market Capitalizations over $100k

Bitcoin's biggest asset over Altcoins is its network effect. At the time of writing, the total number of unique addresses used on the Bitcoin blockchain was 450,000[10] and the number of confirmed Bitcoin transactions per day was 300,000[11]. In fact, Bitcoin's market cap appears to be obeying Metcalfe's

[10]https://blockchain.info/charts/n-unique-addresses
[11]https://blockchain.info/charts/n-transactions

Law, which states that the value of a network is proportional to the square of the number of connected users of the system. Because the number of users in the Bitcoin network is not measured, a proxy of unique addresses used daily can be utilized. The result of the correlation can be seen in Figure 4.

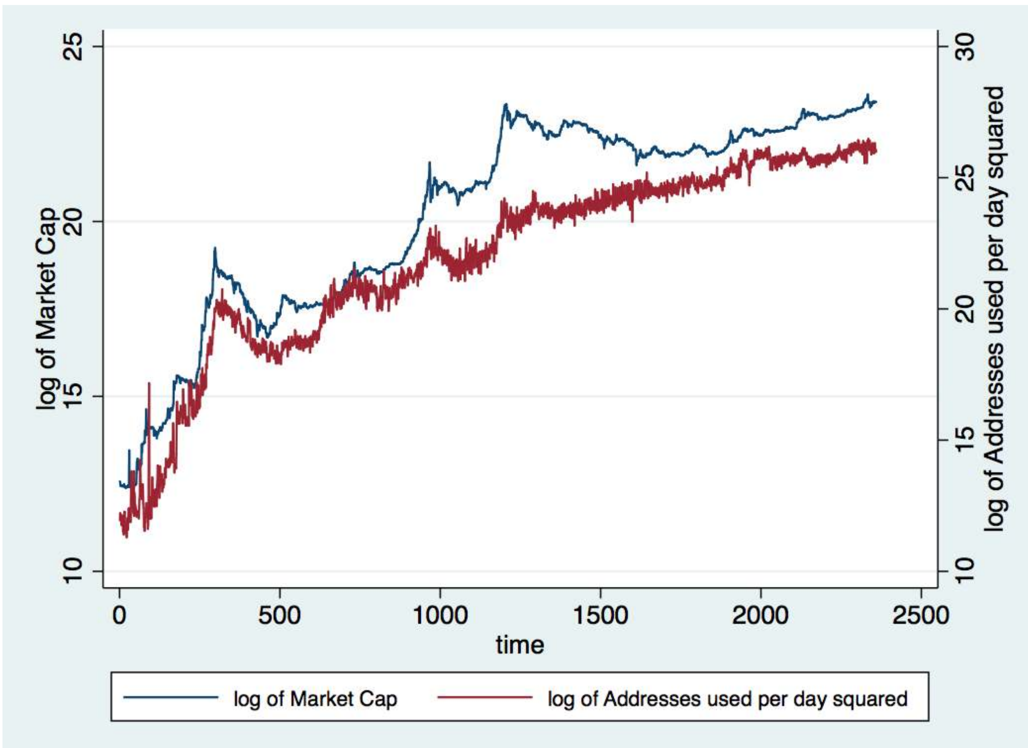

Figure 4: Metcalfe's Law of Bitcoin

Currently, Bitcoin is threatened mainly by the imperfections in its code, which was written nine years ago and is becoming outdated. Since then, Bitcoin has evolved into a widely-used network, which now requires different approaches to some problems. Currently, the biggest constraint is the block size limit of 1MB. The block size limit was designed in 2009 in order to protect the network from attacks. This means that Bitcoin can only tolerate 7 transactions per second [55], which is a drop in the ocean when compared to payment processors such as Visa. Visa handles 1,750 transactions per second on average but is capable of processing up to 24,000 transactions per second[12]. Bitcoin users have the freedom to decide if they want to pay a fee and how much, meaning that whoever pays the highest fee gets prioritized in the verification process. Because there are currently more than 7 transactions per second at any given time, transactions become delayed and this causes the average transaction fee to increase. Before the network was as widely used, most of the transactions were verified for free. However, the current average fee in order to avoid delays is 0.37 USD[13], which hinders one of the key attributes of Bitcoin. Even the most prominent Bitcoin developers are convinced that scalability is an urgent problem that is threatening the existence of the platform because of the inconvenience of waiting times and larger fees [56]. In order to overcome a scaling problem like this, the code needs to be modified, which has been the source of controversy in the Bitcoin community. As I have mentioned before, any alteration in Bitcoin's code results in a fork and Bitcoin "miners" are hesitant about this potentially risky step. Opponents of increasing the block size argue that it could damage decentralization by drive up the amount of resources needed for mining. They suggest to implement the so-called off-chain transactions, which means that the smaller transactions would happen outside of the blockchain. No matter which solution is implemented, if the scalability is not figured out soon, users will migrate to other Altcoins such as Ethereum with lower fees and shorter verification times.

Another critical issue is Bitcoin's power inefficiency. At the time of writing, the "miners" were performing approximately 3,286,700,000 GH/s[14]. On average, mining companies use 0.352W for every GH/s of computing power[15]. Following that assumption, the Bitcoin network runs at 1,156,918,400W or roughly 1,156MW. According to EIA, that's enough to power 930,000 average American households' daily electricity usage. With about 345,000 Bitcoin transactions per day at the time of writing, that works out to 2.7 households' daily usage of electricity per one Bitcoin transaction. The power inefficiency is caused by the extremely demanding cryptographic calculations that the "miners" have to compute on top of verifying transactions. The transaction costs are thus subsidized by the Bitcoin rewards in exchange for Bitcoin's inflation. As the bitcoin rewards get smaller, the power consumption will de-

[12]https://usa.visa.com/run-your-business/small-business-tools/retail.html
[13]https://bitcoinfees.info/
[14]https://blockchain.info/charts/hash-rate
[15]http://digiconomist.net/beci

crease. Another, more immediate, solution would be solving the scalability issue as discussed in the previous paragraph. This would result in increasing the amount of transactions per second and therefore, result in a more energy efficient system. On top of long verification times, relatively high fees, and power inefficiency, Bitcoin is also not fully fungible and not as decentralized as before.

1.8. Literature Review

In addition to the technical issues such as scalability, power inefficiency and non-fungibility, which could hinder Bitcoin's value alone, economists remain skeptical of Bitcoin because of its lack of attributes of a useful currency [5][38], operation in a legally gray area [7], threat of a superior Bitcoin clone [39][40], lack of government backing and oversight [7][57][39][58], eventual deflationary nature [7][40] and vulnerability to speculation [57][37].

The focus of this study is to determine whether Bitcoin can become a viable alternative to fiat currencies. I will evaluate the economic feasibility of Bitcoin without considering the risks of the technical issues as described in the previous chapter. From my research and analysis, I have found that Bitcoin's biggest obstacle from fulfilling the functions of a currency is its price volatility. In the past decade, Bitcoin has proven that it can effectively operate in the legally gray area, that it can function efficiently without government backing and that the currently disinflationary nature has not affected its functioning. The conventional models of measuring volatility such as standard deviation and moving average deviation, among others, do not take into account that the variance-covariance of returns may be volatile during crises. These methods only account for constant volatility, whereas a GARCH model accounts for time-varying volatility, which is much more common.

Gronwald [59] used an autoregressive jump-intensity GARCH model and concluded that Bitcoin prices are strongly characterized by extreme price movements, which is an indication of an immature market. Dyhrberg [60] explored the financial asset capabilities of bitcoin using GARCH models. By using the asymmetric GARCH model, she found evidence that bitcoin may be useful in risk management and ideal for risk averse investors in anticipation of negative shocks to the market. Bouri et al. found that Bitcoin can serve as an effective diversifier but it does not function as a hedging instrument [61]. Urquhart [62] examined Bitcoin's volatility and the forecasting ability of GARCH and HAR models in the Bitcoin market. He found that the realized volatility is quite high in the first half of the sample but has decreased in the recent years. He also concluded that there is no evidence of the leverage effect. In the following practical part, I will examine the dynamics and driving factors of Bitcoin's volatility by using a GARCH(1,1) model.

2. Practical part

2.1. Data

The daily Bitcoin data is collected from Coindesk[16]. Coindesk uses Bitcoin Price Index (BPI), which is the price of one BTC in USD and uses an average from the world's leading bitcoin exchanges. This index is particularly useful when we consider the price disparities amongst different exchanges. Moreover, many exchanges went bankrupt in Bitcoin's relatively short lifetime. All available data at the time of writing is used in order to avoid creating a bias by choosing a smaller sample. The data available ranges from August 18, 2010 to March 17, 2017, which is approximately six and half years or exactly 2404 observations. The Bitcoin price chart during this timeframe can be seen in Figure 5.

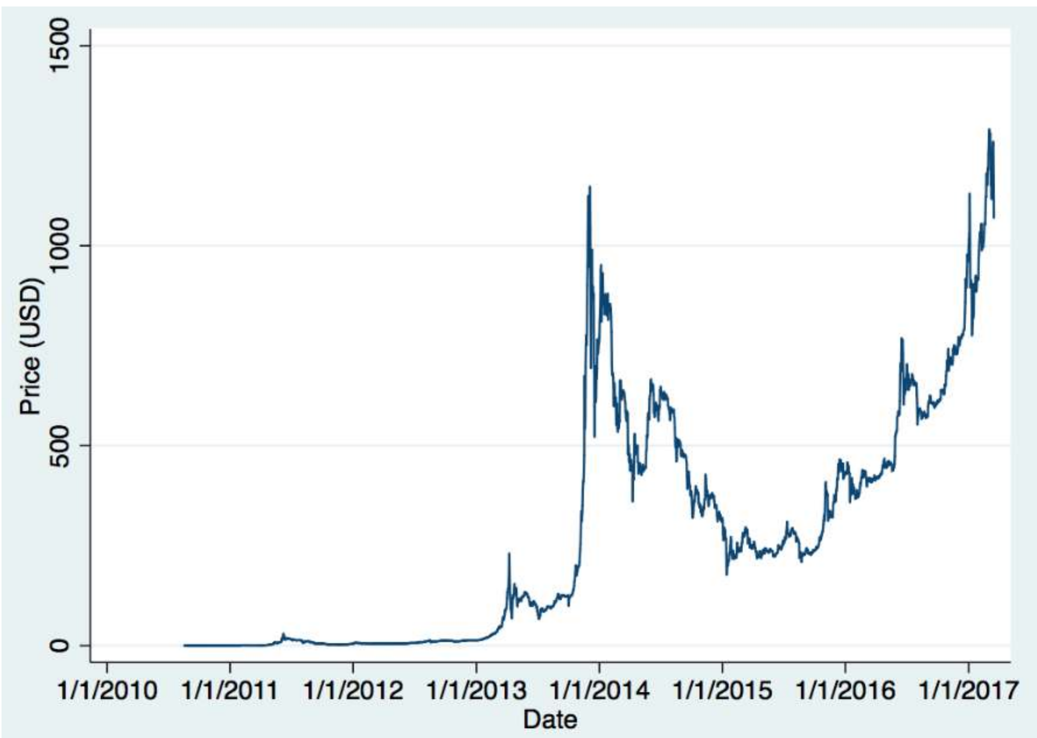

Figure 5: Bitcoin Price Index

[16]http://www.coindesk.com/price/

As a response variable, I am using the log returns of the daily Bitcoin price. The usage of the log returns is well documented by the empirical finance literature because prices are believed to be nonstationary. The advantage of using log returns is that the data is normalized and normally distributed. The log returns are defined as the first difference of the natural logarithm of the prices as seen in Equation 2.

$$r_t = \ln(P_t) - \ln(P_{t-1}) \tag{2}$$

where:

r_t = log returns at time t
P_t = price of BTC in USD at time t

The daily log returns of Bitcoin prices can be seen in Figure 6.

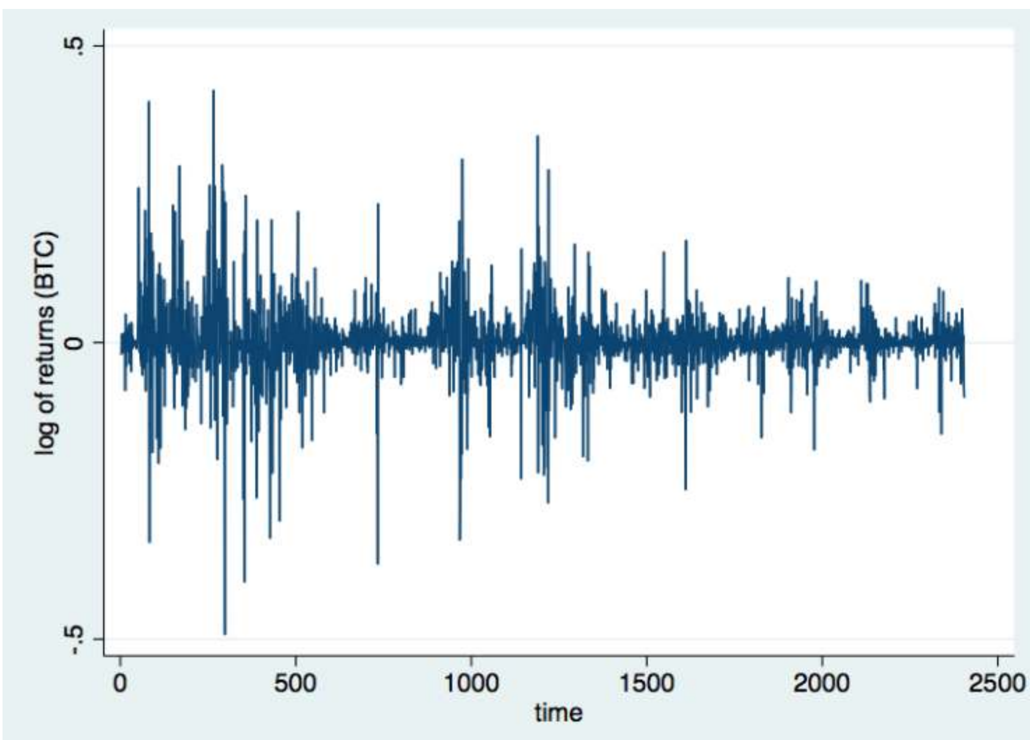

Figure 6: Daily log returns of Bitcoin prices

Most of the previous studies had focused on forecasting the exchange rate levels rather than their volatility. There is no consensus in the literature on exactly which factors affect exchange rate volatility of fiat currencies, but most studies agree that exchange rate volatility can generally be explained by macroeconomic variables such as inflation, interest rates, money supply, exports and GDP [63][64][65][66]. Because Bitcoin is decentralized and could technically be considered an international currency, its exchange rate volatility cannot be explained by macroeconomic variables of just one country. In order to determine which variables to use, we have to consider the countries in which Bitcoin is traded the most. To determine these countries, we can use a proxy statistic that tracks the currencies in which Bitcoin is traded the most. The data was taken from Bitcoinity[17] and the results of the traded volume can be seen in Figure 7.

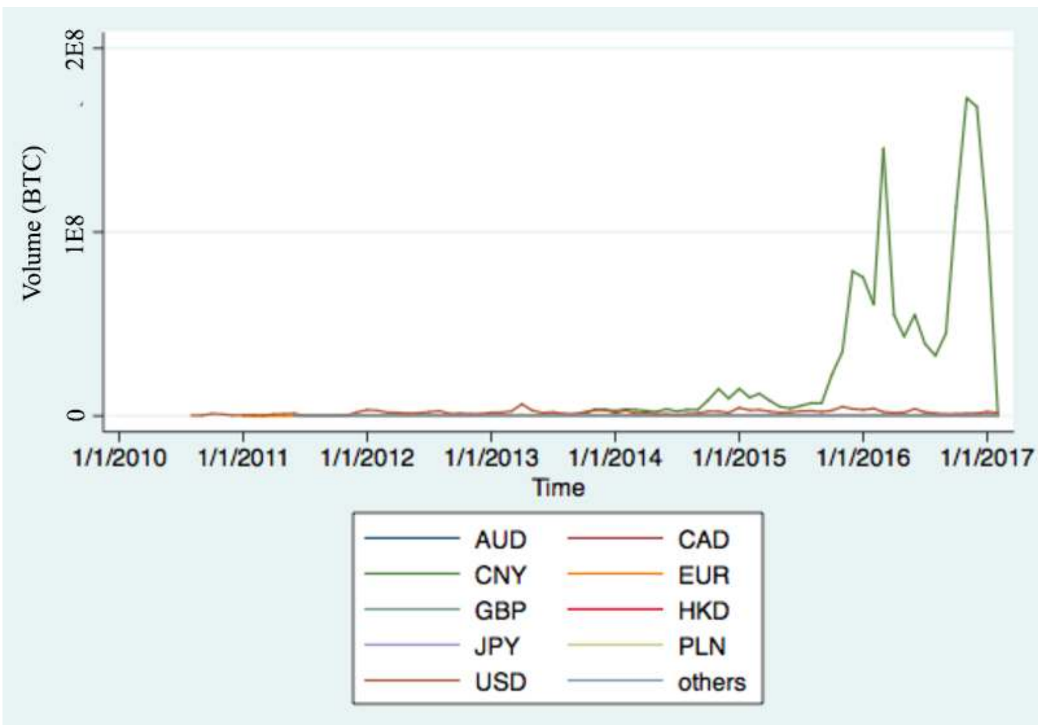

Figure 7: Bitcoin trading volume by the most traded currencies

[17]https://data.bitcoinity.org/markets/volume/

As expected from the research in the theoretical section, CNY has dominated the traded volume in the past two years. The same chart is generated without CNY (Figure 8) to determine other most traded currencies. From Figure 8, it is apparent that the second most traded currency in Bitcoin is USD, which is then followed by EUR and JPY most recently. Other currencies do not have a significant presence. As a result, it can be assumed that China is the most significant external factor that influences Bitcoin's volatility, followed by the United States, and then the European Union and Japan. Therefore, I will be using macroeconomic indicators from these three countries and the EU to explain the exchange rate volatility of Bitcoin. On top of these macroeconomic variables, I will also use the price of gold because of the shared qualities with bitcoin such as limited quantity, easy transportation, easily division, the inability to counterfeit, and acceptance as barter.

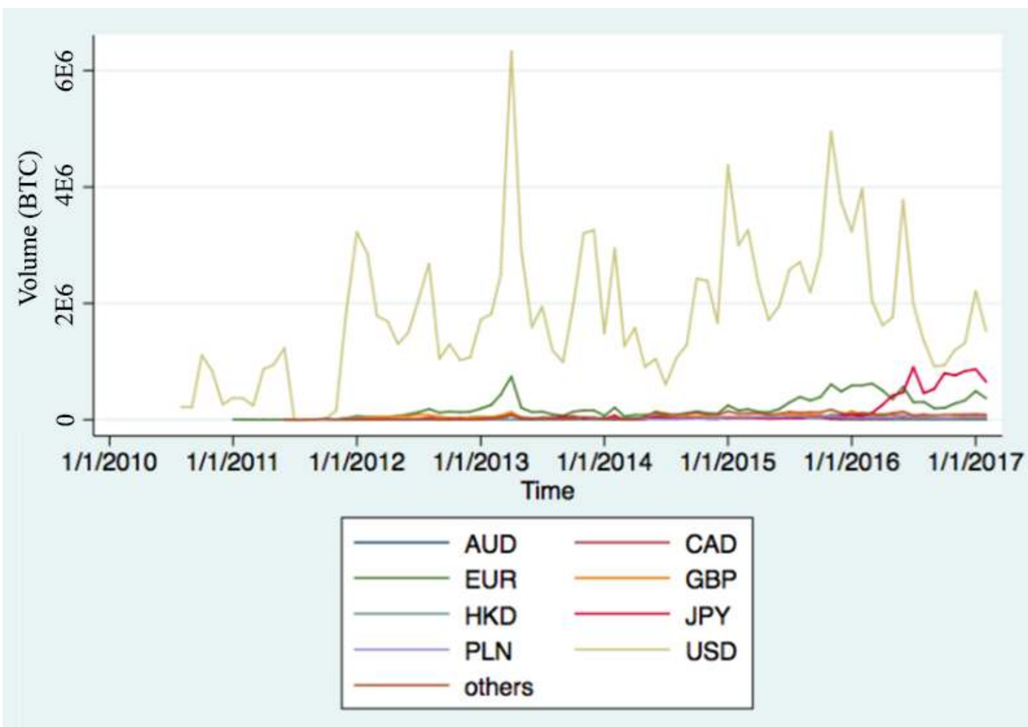

Figure 8: Bitcoin trading volume by currencies without CNY

The macroeconomic indicators with daily observations recommended by the literature are the currency exchange rate, the stock market index, 10-year government bond yield, and a three month interbank rate. The exchange rate represents the maroeconomic strength of a country, the stock market index represents the stock market, the government bond yield represents the bond market and the three month interbank rate represents the bank sector. The explanatory exogenous variables will therefore be: CNY/USD, EUR/USD, JPY/USD, Gold Price per Ounce, Shanghai Composite Stock Market Index, S&P 500, Euro Stoxx 50, Japan NIKKEI 225 Stock Market Index, China Government Bond 10Y, United States Government Bond 10Y, Germany Government Bond 10Y (as a proxy for a 10Y bond of the European Union), Japan Government Bond 10Y, China Three Month Interbank Rate, US Dollar LIBOR Three Month Rate, Euro LIBOR Three Month Rate and Japanese Yen LIBOR Three Month Rate. All the explanatory macroeconomic variables can be seen in Table 3.

	China	**U.S.**	**EU**	**Japan**
Exchange rate	$\Delta \ln CNY_{t-1}$		$\Delta \ln EUR_{t-1}$	$\Delta \ln JPY_{t-1}$
Stock market index	$\Delta \ln Shanghai\ Stock\ Index_{t-1}$	$\Delta \ln S\&P\ 500_{t-1}$	$\Delta \ln Euro\ Stoxx_{t-1}$	$\Delta \ln NIKKEI\ 225_{t-1}$
10Y gov't bond yield	$China\ 10YR\ Govt\ Bondt_{t-1}$	$U.S.\ 10YR\ Govt\ Bondt_{t-1}$	$Germany\ 10YR\ GovtBond_{t-1}$	$Japan\ 10YR\ Govt\ Bondt_{t-1}$
3M interbank rate	$China\ 3M\ Interbank\ Ratet_{t-1}$	$U.S.\ 3M\ Interbank\ Ratet_{t-1}$	$EU\ 3M\ Interbank\ Ratet_{t-1}$	$Japan\ 3M\ Interbank\ Ratet_{t-1}$

Table 3: Explanatory macroeconomic variables

All the data is taken from the Federal Reserve Economic Data (FRED) and Trading Economics. All the explanatory variables are missing observations because financial markets are closed over the weekend and holidays. Summary statistics can be observed in Table 4. A comparison of log returns of BTC/USD, CNY/USD, EUR/USD and JPY/USD can be seen in Figure 9 and Figure 10.

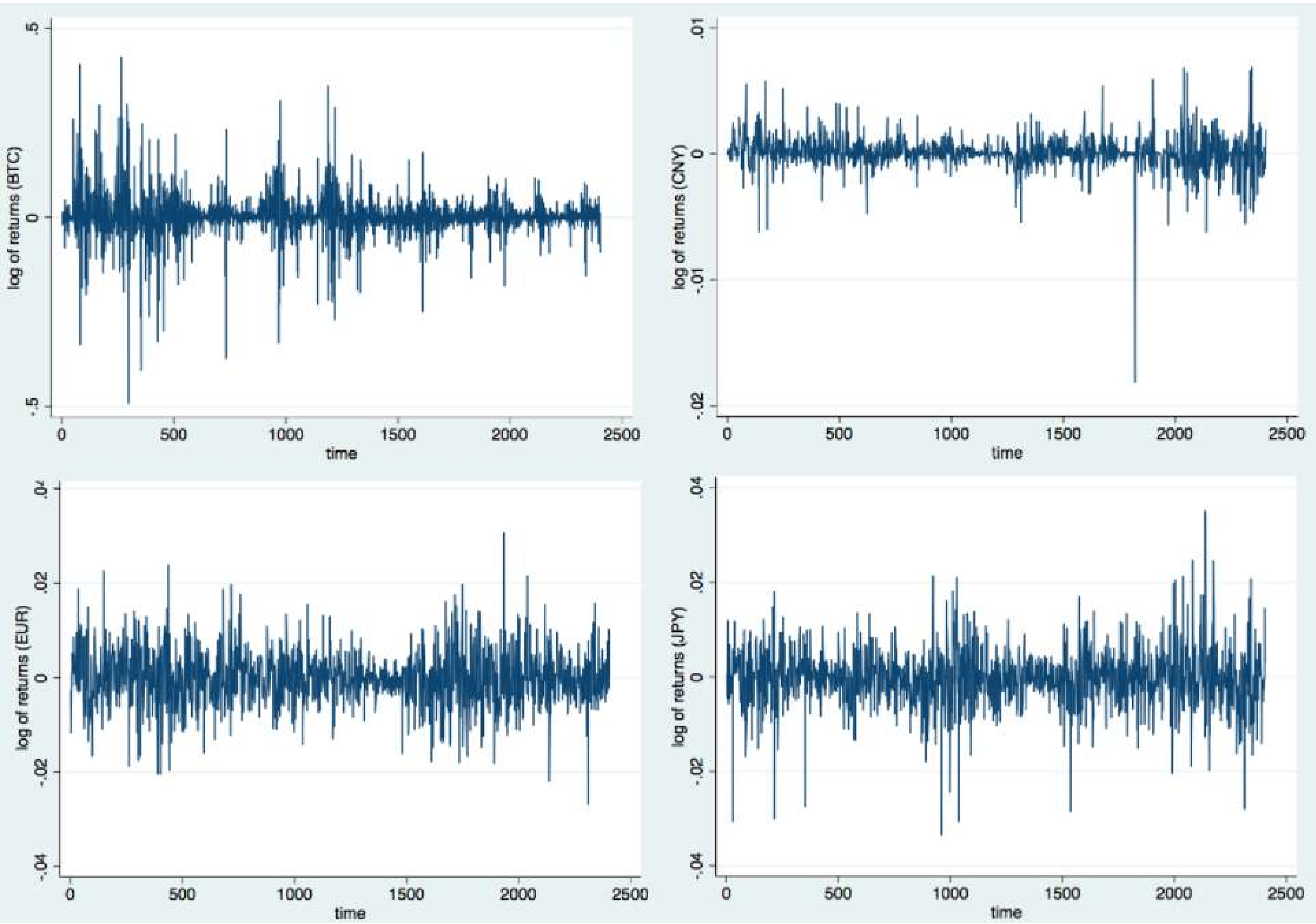

Figure 9: A comparison of log returns of BTC, CNY, EUR and JPY

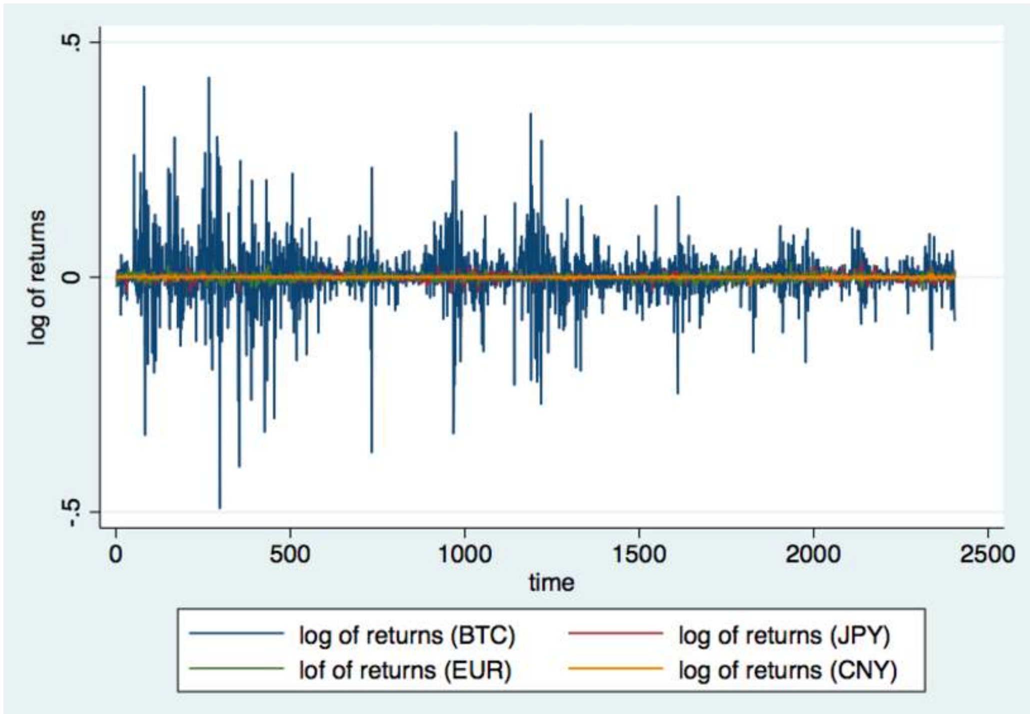

Figure 10: A comparison of log returns of BTC, CNY, EUR and JPY on the same scale

2.2. Methodology

In order to understand how the GARCH model functions, it is important to introduce the ARCH model first. The ARCH model, which stands for Autoregressive Conditional Heteroskedasticity, was first developed by Robert Engle [67] as a method of estimation that allows for time varying volatility. The concept of the ARCH model is that the volatility estimation will be more precise when the data from the previous periods is taken into account; this means that this period's volatility is conditional on information previous period. When the variance of residuals is constant (homoscedastic), we can use the method of the ordinary least squares (OLS). However, if the variance of residuals fluctuates (heteroskedastic), which is the case with Bitcoin, we must use the method of the weighted least squares (WLS) to estimate the regression. The ARCH model transforms the OLS residuals into an endogenous process. When the data is heteroskedastic, the standard OLS regression would fail the Gauss Markov assumptions because $Var(\varepsilon_t) = \sigma^2$ would not

Variable	**N**	**Mean**	**SD**	**Min**	**Max**
Time	2404	1202.5	694.1	1	2404
Bitcoin Price Index	2404	271.3	291.3	0.059	1290.8
CNY/USD	1648	0.1571	0.00531	0.1437	0.1656
EUR/USD	1648	1.257	0.1189	1.038	1.488
JPY/USD	1648	0.01043	0.001676	0.007963	0.013207
Gold OZ (USD)	1731	1377.7	201.3	1051.7	1898.3
Shanghai Stock Index	1602	2702.2	602.9	1950	5166.4
S&P 500	1657	1716.6	360	1047.2	2396
Euro Stoxx 50	1675	2905.8	382.1	1995	3838.8
NIKKEI 225	1629	13887.9	3923.5	8160	20868
China 10YR Govt Bond (%)	1706	3.61	0.48	2.62	4.85
U.S 10YR Govt Bond (%)	1732	2.26	0.5	1.36	3.72
Germany 10YR Govt Bond (%)	1708	1.33	0.9	-0.19	3.49
Japan 10YR Govt Bond (%)	1614	0.6	0.39	-0.3	1.35
China 3M Interbank Rate (%)	1718	4.43	1.14	2	9.89
U.S. 3M Interbank Rate (%)	1718	0.4	0.22	0.22	1.15
EU 3M Interbank Rate (%)	1718	0.32	0.55	-0.36	1.56
Japan 3M Interbank Rate (%)	1718	0.12	0.08	-0.08	0.24

Table 4: Summary Statistics

hold: Both ARCH or GARCH models consist of two equations; a conditional mean equation and a conditional variance equation. Both equations must be estimated simultaneously since the variance is a function of the mean. The conditional variance equation of an ARCH(1) model presented by Engle is seen in Equation 3.

$$\sigma_t^2 = \alpha_0 + \alpha_1 \varepsilon_{t-1}^2 \tag{3}$$

where:

σ_t^2 = conditional variance this period
α_0 = constant
ε_{t-1}^2 = squared residual return in the previous period (ARCH term)

$\alpha_0 > 0$ and $\alpha_1 \geq 0$ to ensure positive variance and $\alpha_1 < 1$ for stationarity

If the residual return in the previous period is large, the forecast for this period's conditional volatility will also be large. The ARCH process of order "p" or ARCH(p) signifies how many lags (noted as "p") of the squared residual return is present. When “p” is 1 such as in ARCH(1), it means that it lags on previous period’s squared residual return. The conditional variance equation for ARCH(p) is seen in Equation 4.

$$\sigma_t^2 = \alpha_0 + \alpha_1 \varepsilon_{t-1}^2 + ... + \alpha_p \varepsilon_{t-p}^2 \tag{4}$$

However, in the ARCH model, this period’s conditional volatility only depends on the square of the residual return in the previous period, which means that a crisis with a large residual would not have the same persistence as is usually observed during an actual crisis. In order to correct this and capture crises with large residuals, an extension of the ARCH model was developed by Bollerslev [68]. Bollerslev called this extension the Generalized Autoregressive Conditional Heteroskedasticity or GARCH. The most commonly used model in the literature is the symmetric GARCH(1,1), which is seen in Equation 5.

$$\sigma_t^2 = \alpha_0 + \alpha_1 \varepsilon_{t-1}^2 + \beta_1 \sigma_{t-1}^2 \tag{5}$$

where:

σ_t^2 = conditional variance this period
α_0 = weighted long run average variance
ε_{t-1}^2 = squared residual return in the previous period (ARCH term)
σ_{t-1}^2 = variance in the previous period (GARCH term)

$\alpha_1 + \beta_1 < 1$ is the stationary condition; $\alpha_0 > 0$, $\alpha_1 > 0$, $\beta_1 > 0$ must hold

According to GARCH(1,1), this period’s forecast of volatility is a function of the weighted average long-term variance, previous period’s squared residual return, and previous period’s volatility. The GARCH process of order “p” and “q” or GARCH(p,q) signifies how many lags of the squared residual return (noted as “p”) and how many lags of variances (noted as “q”) are present. When both “p” and “q” is 1 such as in GARCH(1,1), it means that it lags on previous period’s squared residual return and previous period’s variance. The conditional variance equation for GARCH(p,q) is seen in Equation 6.

$$\sigma_t^2 = \alpha_0 + \alpha_1 \varepsilon_{t-1}^2 + ... + \alpha_p \varepsilon_{t-p}^2 + \beta_1 \sigma_{t-1}^2 + ... + \beta_q \sigma_{t-q}^2 \tag{6}$$

The key statistic in a GARCH model is the sum of α and β. This gives us a parameter of persistence, which tells us how fast large volatilities decay after a shock. In the literature, GARCH models are used to exhibit time-varying volatility clustering, which is when time series data show continuous periods of high volatility and continuous periods of low volatility. GARCH models are not only used for modeling the historical process of volatility but also in forecasting multi-period volatility. GARCH models are mostly used to analyze and forecast the volatility of stock returns, interest rates and foreign exchange data, which is helpful in portfolio allocation, dynamic optimization and option pricing [69]. In my study, I will use a GARCH model precisely because of its ability to analyze and forecast volatility. Moreover, GARCH(1,1) model has been continuously proven to be a superior model for currency volatility estimation [70][71][72].

The first step in using a GARCH(1,1) model is to set a conditional mean equation. As stated before, the conditional mean equation is estimated simultaneously with the conditional variance equation because variance is a function of the mean. In stationary time series, the conditional mean equation must always be an AR, ARMA, or an MA model. The AR model is the most used in the literature when analyzing the volatility of financial returns. I decided to use the first order autoregression, written as AR(1), which means that the returns in the previous period will be used to predict the returns of the current period. The conditional mean equation while using the AR(1) model is seen in Equation 7.

$$r_t = \beta_0 + \beta_1 r_{t-1} + \varepsilon_t \quad \text{with} \quad \varepsilon_t \approx i.i.d.(0, \sigma^2) \quad \text{and} \quad |\theta| < 1 \tag{7}$$

In order to find whether the explanatory variables have an effect on Bitcoin's volatility, both AR(1) and GARCH(1,1) models can be modified by adding the explanatory variables to both the conditional mean and conditional variance equation as described by Vlastakis and Markellos [73].

The modified mean equation is seen in Equation 8.

$$
\begin{aligned}
r_t = \beta_0 + \beta_1 r_{t-1} + \beta_2 \Delta lnCNY_{t-1} + \beta_3 \Delta lnEUR_{t-1} + \beta_4 \Delta lnJPY_{t-1} \\
+\beta_5 \Delta lnGold_{t-1} + \beta_6 \Delta lnSSI_{t-1} + \beta_7 \Delta lnSP500_{t-1} + \beta_8 \Delta lnStoxx_{t-1} \\
+\beta_9 \Delta lnNIKKEI_{t-1} + \beta_{10} \Delta ChinaB_{t-1} + \beta_{11} \Delta USB_{t-1} \\
+\beta_{12} \Delta GerB_{t-1} + \beta_{13} \Delta JapB_{t-1} + \beta_{14} \Delta ChinaI_{t-1} \\
+\beta_{15} \Delta USI_{t-1} + \beta_{16} \Delta GerI_{t-1} + \beta_{17} \Delta JapI_{t-1} + \varepsilon_t
\end{aligned}
\tag{8}
$$

The modified variance equation is seen in Equation 9.

$$
\begin{aligned}
\sigma_t^2 = \exp(\lambda_0 + \lambda_1 \Delta lnCNY_{t-1} + \lambda_2 \Delta lnEUR_{t-1} + \lambda_3 \Delta lnJPY_{t-1} \\
+\lambda_4 \Delta lnGold_{t-1} + \lambda_5 \Delta lnSSI_{t-1} + \lambda_6 \Delta lnSP500_{t-1} + \lambda_7 \Delta lnStoxx_{t-1} \\
+\lambda_8 \Delta lnNIKKEI_{t-1} + \lambda_9 ChinaB_{t-1} + \lambda_{10} USB_{t-1} + \lambda_{11} GerB_{t-1} \\
+\lambda_{12} JapB_{t-1} + \lambda_{13} ChinaI_{t-1} + \lambda_{14} USI_{t-1} + \lambda_{15} GerI_{t-1} \\
+\lambda_{16} JapI_{t-1}) + \alpha_1 \varepsilon_{t-1}^2 + \beta_1 \sigma_{t-1}^2 + \varepsilon_t
\end{aligned}
\tag{9}
$$

It is recommended by the literature to modify the mean equation with internal explanatory variables and the variance equation with exogenous explanatory variables. However, Bitcoin does not have any internal variables other than the intervention events such as the bitcoin exchange hacks, depreciation of fiat currencies, governmental regulations, and halving periods; which cannot be used as a function of returns. This is because Bitcoin's value is driven by market forces and has no intrinsic value. There are two possible solutions to this problem - either use the unmodified AR(1) mean equation or modify the mean equation by exogenous explanatory variables. Dyhrberg [60] recommends to modify the mean equation by exogenous explanatory variables and my study follows that recommendation.

Before estimating the GARCH(1,1) model, the statistical properties of the mean equation are investigated. The two preconditions that must be met in order to estimate GARCH(1,1) model are clustering volatility and ARCH effect in the residual. The results of the test of clustering volatility in the residuals can be seen in Figure 11. Figure 11 shows that the periods of low volatility of the error term are followed by the periods of low volatility and vice versa. This indicates that large returns are followed by large returns and small returns are followed by small returns. This phenomenon is called clustering volatility, which means that the residual is conditionally heteroskedastic. Therefore, the first precondition is met and we can move to the second precondition: whether there is an ARCH effect in the residual.

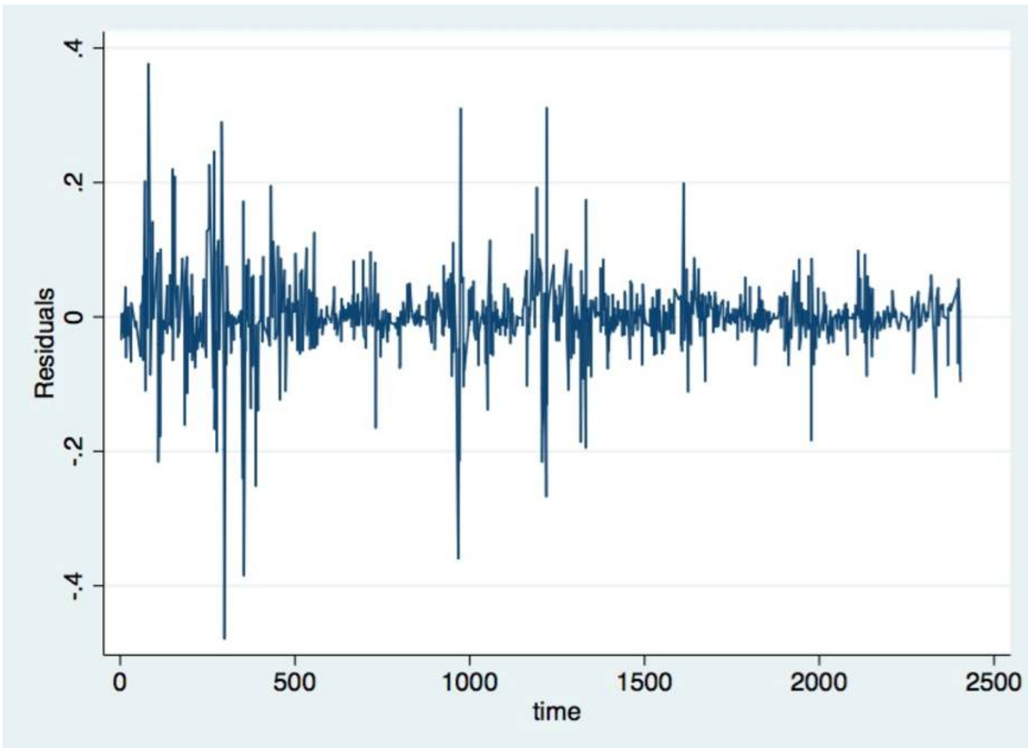

Figure 11: A test of clustering volatility in the residuals

An ARCH effect determines whether there is serial correlation of the heteroskedasticity. In order to determine whether there is an ARCH effect, we have to conduct an LM ARCH test. The null hypothesis in this test is that there is no ARCH effect and the alternative hypothesis is the opposite. The results of the test can be seen in Table 5. The LM test for ARCH provides strong evidence that there is an ARCH effect in the mean equation because we can reject the null hypothesis (0%<5%). Therefore, the mean model satisfies both of the criteria and we have the validity to run the GARCH(1,1) model.

It is also important to note that there is multicollinearity between the individual macroeconomic variables of Japan and the European Union. There is no multicollinearity between the individual macroeconomic variables of

lags(p)	chi2	df	Prob > chi2
1	105.484	1	0.0000

H0: no ARCH effects vs. H1: ARCH(p) disturbance

Table 5: ALM test for ARCH

the U.S. and China. However, the presence of multicollinearity between the macroeconomic variable is an expected outcome since macroeconomic variables often correlate based on economic developments of such country. In this study, multicollinearity does not present a problem since it is analyzing the larger macroeconomic picture of a country rather than the individual macroeconomic variables.

2.3. Expectations

Based on the previous literature, it is expected that both the previous day's return information and the previous day's volatility will be significant in explaining today's volatility [59][60][61][62]. Moreover, because China has the largest effect on driving the bitcoin prices, it is expected that it will be the most significant variable in predicting next day's volatility of Bitcoin. Furthermore, CNY has an inverse relationship to BTC [54], which indicates that the relationship between BTC's volatility and CNY's volatility should be negative.

There has been no previous literature that looked at the relationship between macroeconomic variables and Bitcoin's volatility to determine whether Bitcoin is starting to behave similarly to fiat currencies. If the macroeconomic variables of countries, where Bitcoin is being traded the most, have a significant relationship with Bitcoin's volatility, it would indicate that Bitcoin is starting to react to the same variables as its fiat currency counterparts. Moreover, the results will also show which countries are the most significant in predicting next day's volatility of Bitcoin.

2.4. Results

The results are shown in Table 6. GARCH(1,1) was also estimated with an unmodified AR(1) mean equation to verify the accuracy of the GARCH(1,1) estimation while using a modified mean equation. The same statistically significant variables and the same signs for these variables verified the validity of the modified mean equation.

Variable	Mean Equation	Variance Equation
$\Delta \ln CNY_{t-1}$	-.6109801 (.856853)	-199.9299 (69.57488)***
$\Delta \ln EUR_{t-1}$	-.7133233 (.2609827)***	61.09854 (13.86623)***
$\Delta \ln JPY_{t-1}$	.2073412 (.2561578)	3.604117 (19.09725)
$\Delta \ln Gold_{t-1}$	.1737769 (.129766)	-21.24307 (7.515253)***
$\Delta \ln Shanghai\ Stock\ Index_{t-1}$	.0820254 (.0738187)	39.90785 (9.025129)***
$\Delta \ln S\&P\ 500_{t-1}$	.0801723 (.1970611)	36.0822 (8.322125)***
$\Delta \ln Euro\ Stoxx_{t-1}$	.1361042 (.1368653)	-38.94776 (8.221662)***
$\Delta \ln NIKKEI\ 225_{t-1}$	-.1217739 (.1025617)	-7.737607 (7.615126)
$China\ 10YR\ Govt\ Bondt_{t-1}$	-.00446 (.0056461)	1.159014 (.3773523)***
$U.S.\ 10YR\ Govt\ Bondt_{t-1}$	-.0029994 (.0057765)	-2.100576 (.4388985)***
$Germany\ 10YR\ GovtBond_{t-1}$	.0106237 (.0067866)	4.549737 (.5396294)***
$Japan\ 10YR\ Govt\ Bondt_{t-1}$	-.009015 (.0221015)	-9.660189 (1.227745)***
$China\ 3M\ Interbank\ Ratet_{t-1}$	-.0015031 (.0014874)	-.2687734 (.1006237)***
$U.S.\ 3M\ Interbank\ Ratet_{t-1}$	-.0094399 (.0088782)	-1.725574 (1.009195)*
$EU\ 3M\ Interbank\ Ratet_{t-1}$	-.0011845 (.0065199)	2.041789 (.2874844)***
$Japan\ 3M\ Interbank\ Ratet_{t-1}$	-.0302514 (.0848204)	3.605629 (4.809523)
L.ar	.0195859 (.0271997)	
L.arch α		.1924326 (.034369)***
L.arch β		.3662459 (.0298018)***
Constant	.0309313 (.0178738)**	-6.789791 (1.334359)***
Observations	1041	1041

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$

Table 6: GARCH(1,1), dependent variable return on bitcoin.

In the mean equation, most of the explanatory variables are statistically insignificant, which is an expected outcome. All of the explanatory variables are lagged by one period, which indicates that if the variables were statistically significant, it could present an opportunity for arbitrage. The only statistically significant variable is the log returns of EUR/USD, which indicates that when the log returns of EUR/USD increase, the log returns of BTC/USD decrease in the following period. However, a separate regression was run to verify or refute this relationship and it showed that the relationship is no longer significant. Therefore, we can conclude that none of the explanatory variables in the previous period are significant in forecasting the current period's log returns of Bitcoin. In other words, Bitcoin's returns are independent from the influence of all of analyzed explanatory variables and there is no arbitrage opportunity.

In the variance equation, both ARCH (α) and GARCH (β) terms are statistically significant, which means that the previous day's return information of Bitcoin does affect today's volatility of Bitcoin (ARCH) and also that the previous day's volatility of Bitcoin does influence today's volatility of Bitcoin (GARCH). It is also important to note that because $\beta > \alpha$, we can conclude that past volatility effects are superior to past shock effects and that past volatility effects should be used when forecasting Bitcoin's volatility. In contrast with the mean equation, most of the explanatory variables are significant in explaining the volatility of Bitcoin, which is a favorable outcome.

The most significant finding is that macroeconomic explanatory variables of China, U.S. and European Union are all significant to forecast next day's volatility of Bitcoin. This indicates that Bitcoin is starting to react to the same variables as its fiat currency counterparts in China, U.S. and European Union. Moreover, it shows that Bitcoin is maturing to become an alternative currency especially in these countries and the EU. However, it also points to the centralization of Bitcoin, which is not a favorable outcome because macroeconomic shocks from China, the U.S. and the EU affect Bitcoin disproportionately more than shocks from other countries. If Bitcoin were to act as an alternative international currency, it must become independent from large countries and become more widely used worldwide. Therefore, the macroeconomic shocks and intervention events would spread out and not affect Bitcoin as greatly as now. For example, when China suspended the users from withdrawing bitcoins in early 2017 amid concerns that the cryptocurrency is being used to facilitate capital flight, the price of bitcoin dropped by over 30% in just a week. Since then, the price has recovered and continued to increase to the highest levels in Bitcoin's lifetime. But right after it hit its peak, the SEC has denied the application for the Bitcoin Trust ETF and the price crashed by 24% again. These are just two examples of how external shocks coming from either China or the United States greatly affect Bitcoin's volatility.

On the other hand, macroeconomic variables from Japan are not suitable to forecast next day's volatility. This is an expected outcome because Japan has just recently seen a growth of Bitcoin adoption and media coverage. If we only looked at the last year of Bitcoin's price development, it is possible that Japan's macroeconomic variables would be more significant in predicting Bitcoin's volatility.

The coefficients on the returns of exchange rates suggest that Bitcoin's volatility is the most sensitive to the price changes in CNY. This is also an expected outcome because the vast majority of Bitcoin was traded in CNY in the last two years. The returns of gold are significant in forecasting Bitcoin's volatility but the relatively small coefficient means that Bitcoin's volatility is not very sensitive to its price changes. Another significant finding is that a positive volatility shock to CNY decreases the volatility of bitcoin. The possible explanation could be that Bitcoin acts as a safe-haven asset in China. When there is an increased risk in holding CNY, more people convert their fiat currency to bitcoin and therefore increase the traded volume, which decreases Bitcoin's volatility. Estimated conditional variance of daily Bitcoin log-returns can be seen in Figure 12.

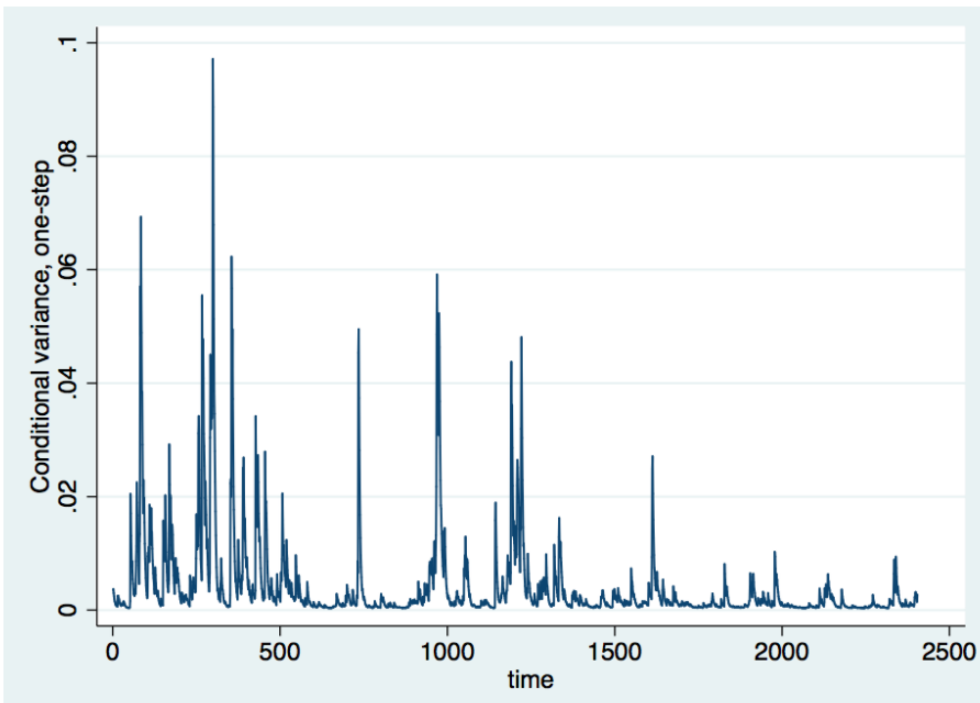

Figure 12: Conditional variance of daily Bitcoin log-returns

In Figure 13, the daily volatility of Bitcoin is shown with an average trendline and with a 30-day peak trendline. It is apparent that the volatility is trending downward but it is still far away from the volatility levels of other fiat currencies. However, an important takeaway from Figure 14 is that the economic properties for Bitcoin to become a viable alternative to fiat currencies are developing quickly. The dotted line indicates a continuation of the trendline as a prediction of volatility levels in the future. If the volatility levels follow the same trend as in the last six and a half years, Bitcoin will reach the fiat levels of volatility in 2019-2020. However, it is improbable that the volatility will continue to reduce at the current rate because of the absence of central banks and their ability to make macroeconomic adjustments to stabilize the exchange rate. An important task of the central bank is to minimize the systematic (undiversifiable) risks. Bitcoin does not have any way of minimizing the systematic risk and therefore, it is possible that Bitcoin will never reach the volatility levels of stable fiat currencies. Nonetheless, volatility will surely approach the fiat levels when the traded daily volume is sufficient.

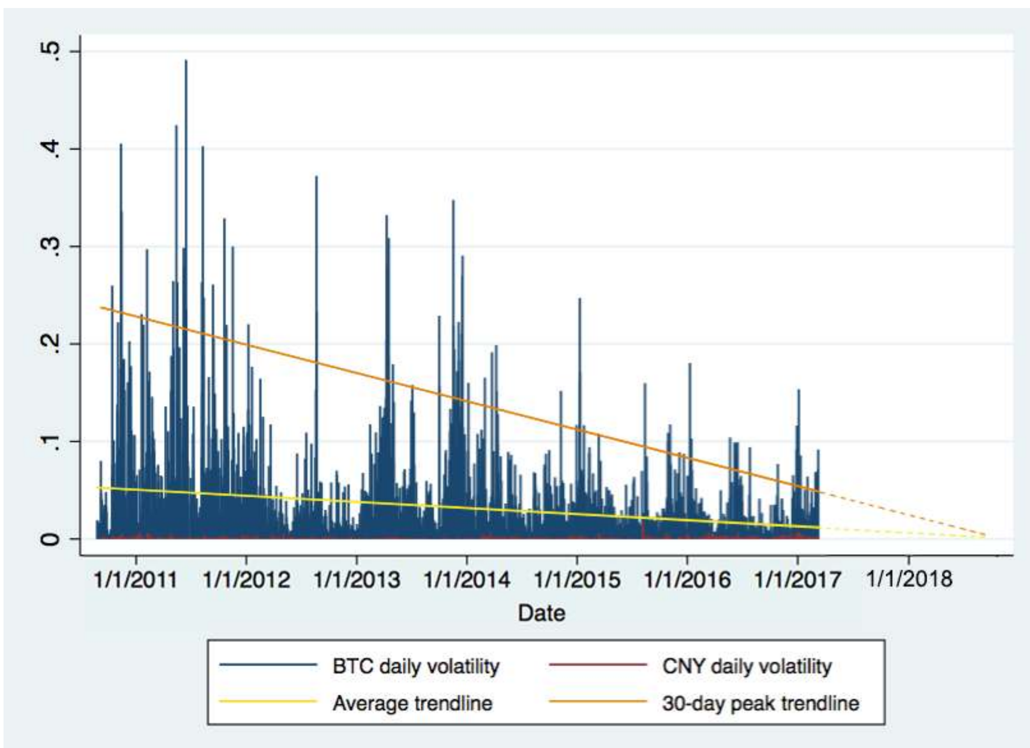

Figure 13: Daily volatility of Bitcoin

3. Conclusion

Currently, Bitcoin does not satisfy the criteria for being considered as a currency because it does not act as an effective medium of exchange, unit of account, or as a store of value. Bitcoin presently acts as a scarce digital commodity with a finite supply. The finite supply and deflationary pressures make Bitcoin highly speculative. When compared to other cryptocurrencies, which are also decentralized, anonymous and unregulated, Bitcoin's sole value lies in its network effect and a first mover advantage. This makes Bitcoin vulnerable to potentially superior alternatives. Apart from the technical issues such as the scalability, the biggest obstacle preventing Bitcoin from becoming an alternative to fiat currencies is its volatility. Bitcoin's volatility is far larger than even fiat currencies with a small supply.

Within the last two years, Bitcoin has mostly been traded in China. Historically, China is followed by the United States, the European Union, and Japan. Therefore, it is fair to assume that China is the most significant external factor that influences Bitcoin's volatility, followed by the United States, the European Union, and Japan. The macroeconomic explanatory variables of China, the United States, and the EU are all significant to forecast the next day's volatility of Bitcoin. This indicates that Bitcoin is starting to react to the same variables as the fiat currencies in these countries. Japan's macroeconomic variables are not significant, however.

Bitcoin's volatility is the most sensitive to the price changes in CNY, which further points to the centralization of Bitcoin. Currently, macroeconomic shocks from China, the United States, and the EU affect Bitcoin disproportionately more than shocks from other countries. In order for Bitcoin to truly become an international alternative to fiat currencies, it must become less dependent on larger countries.

However, the volatility levels have historically been trending downward and if Bitcoin were to follow the same trend as it has been for the previous six years, it would reach the volatility levels of fiat currencies approximately in 2019-2020. However, the absence of a central bank that acts as a minimizer of the systematic risk and a stabilizer of the exchange rate means that Bitcoin might never reach the volatility levels of stable fiat currencies. Nonetheless, volatility will surely approach the fiat levels when the traded daily volume is sufficient. If Bitcoin approaches the volatility levels of fiat currencies, it will satisfy the criteria of being a functioning currency and therefore, will be ready for mass adoption.

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008).

[2] M. Bustillos, The bitcoin boom, 2014.

[3] D. Chaum, Blind signatures for untraceable payments, in: Advances in cryptology, Springer, pp. 199–203.

[4] S. Barber, X. Boyen, E. Shi, E. Uzun, Bitter to betterhow to make bitcoin a better currency, in: International Conference on Financial Cryptography and Data Security, Springer, pp. 399–414.

[5] D. Yermack, Is Bitcoin a real currency? An economic appraisal, Technical Report, National Bureau of Economic Research, 2013.

[6] D. Golumbia, Trump, clinton, and the electoral politics of bitcoin, 2016.

[7] R. Grinberg, Bitcoin: An innovative alternative digital currency (2011).

[8] J. Redman, Openbazaar is here but darknet markets will remain, 2016.

[9] M. Miller, The ultimate guide to Bitcoin, Pearson Education, 2014.

[10] J. Brito, Online cash bitcoin could challenge governments, banks, 2011.

[11] R. Stross, What's coming out of silicon valley, 2012.

[12] A. Santos, Bitcoin-central becomes first bitcoin exchange licensed to operate like a bank, 2012.

[13] P. Vigna, 5 things about mt. goxs crisis, 2014.

[14] D. Howden, Bitcoin bank run, 2014.

[15] O. Williams-Grut, Mt.gox files for bankruptcy protection, 2014.

[16] R. Sidel, E. Warnock, T. Mochizuki, Almost half a billion worth of bitcoins vanish, 2014.

[17] P. Liljas, Worlds first bitcoin atm launched in canada, 2013.

[18] S. Acharya, J. Dunn, Overstock.com ventures into digital currencies, Journal of Business Cases and Applications 12 (2014) 1.

[19] D. Ron, A. Shamir, Quantitative analysis of the full bitcoin transaction graph, in: International Conference on Financial Cryptography and Data Security, Springer, pp. 6–24.

[20] T. Swanson, Approximately 70% of all bitcoins have not moved in 6 or more months, 2014.

[21] O. Beigel, Is bitcoin mining profitable in 2017?, 2016.

[22] N. Popper, How china took center stage in bitcoin's civil war, 2016.

[23] S. Valfells, J. H. Egilsson, Minting money with megawatts [point of view], Proceedings of the IEEE 104 (2016) 1674–1678.

[24] Virtual currency schemes, European Central Bank (2016).

[25] L. V. Mises, B. B. Greaves, Human action: A treatise on economics, Yale University Press New Haven, 1949.

[26] R. W. Garrison, Overconsumption and forced saving in mises-hayek theory of the business cycle, History of Political Economy 36 (2004) 323–349.

[27] L. v. Mises, The theory of money and credit, Indianapolis, IN: Liberty Fund, Inc., 1912.

[28] A. G. Clegg, Could bitcoin be a financial solution for developing economies, University of Birmingham (2014).

[29] F. Hayek, Choice in currency: a way to stop inflation, volume 48, Ludwig von Mises Institute, 1976.

[30] N. Gertchev, The money-ness of bitcoins, 2013.

[31] P. Korda, Bitcoin: Money of the future or old-fashioned bubble?, 2013.

[32] F. Shostak, The bitcoin money myth, 2013.

[33] K. Graf, On the origins of bitcoin: Stages of monetary evolution, Konrad S. Graf Investigations and Observations (2013).

[34] P. Surda, The origin, classification and utility of bitcoin (2014).

[35] J. M. Keynes, General theory of employment, interest and money, Atlantic Publishers & Dist, 2016.

[36] F. Glaser, K. Zimmermann, M. Haferkorn, M. C. Weber, M. Siering, Bitcoin-asset or currency? revealing users' hidden intentions (2014).

[37] C. Baek, M. Elbeck, Bitcoins as an investment or speculative vehicle? a first look, Applied Economics Letters 22 (2015) 30–34.

[38] P. Krugman, Bitcoin is evil, The New York Times 28 (2013).

[39] B. DeLong, Watching bitcoin, dogecoin, etc, 2013.

[40] T. Cowen, How and why bitcoin will plummet in price, 2013.

[41] G. Varriale, Bitcoin: how to regulate a virtual currency, International Financial Law Review 32 (2013) 43.

[42] R. Bohme, N. Christin, B. Edelman, T. Moore, Bitcoin: Economics, technology, and governance, The Journal of Economic Perspectives 29 (2015) 213–238.

[43] S. Lo, C. Wang, et al., Bitcoin as money?, 2015.

[44] C. Burniske, Bitcoin: A disruptive currency (2015).

[45] J. Davidson, Bitcoin not really being accepted by major companies, 2015.

[46] C. Burniske, All about bitcoin, Global Macro Research (2015).

[47] D. Vorick, Ensuring bitcoin fungibility in 2017 (and beyond), 2016.

[48] E.-T. Cheah, J. Fry, Speculative bubbles in bitcoin markets? an empirical investigation into the fundamental value of bitcoin, Economics Letters 130 (2015) 32–36.

[49] G. Mullany, China restricts banks use of bitcoin, 2013.

[50] G. Smith, Bitcoin is melting down as china cracks down on capital outflows, 2017.

[51] G. Wildau, China forex reserves dip under $3tn to touch 5-year low, 2017.

[52] G. Wildau, Major chinese bitcoin exchanges halt withdrawals after crackdown, 2017.

[53] C. Bovaird, Are bitcoin and gold prices correlated?, 2016.

[54] G. Wildau, China probes bitcoin exchanges amid capital flight fears, 2017.

[55] M. Vukolić, The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, in: International Workshop on Open Problems in Network Security, Springer, pp. 112–125.

[56] T. Simonite, The looming problem that could kill bitcoin, 2015.

[57] F. Brezo, P. G. Bringas, Issues and risks associated with cryptocurrencies such as bitcoin (2012).

[58] M. Van Alstyne, Why bitcoin has value, Communications of the ACM 57 (2014) 30–32.

[59] M. Gronwald, The economics of bitcoins–market characteristics and price jumps (2014).

[60] A. H. Dyhrberg, Bitcoin, gold and the dollar–a garch volatility analysis, Finance Research Letters 16 (2016) 85–92.

[61] E. Bouri, P. Molnar, G. Azzi, D. Roubaud, L. I. Hagfors, On the hedge and safe haven properties of bitcoin: Is it really more than a diversifier?, Finance Research Letters 20 (2017) 192–198.

[62] A. Urquhart, The volatility of bitcoin (2017).

[63] N. Antonakakis, J. Darby, Forecasting volatility in developing countries nominal exchange returns, Applied Financial Economics 23 (2013) 1675–1691.

[64] P. De Grauwe, Exchange rate variability and the slowdown in growth of international trade, Staff Papers 35 (1988) 63–84.

[65] T. G. Andersen, T. Bollerslev, Answering the skeptics: Yes, standard volatility models do provide accurate forecasts, International economic review (1998) 885–905.

[66] C. Engel, K. D. West, Exchange rates and fundamentals, Journal of political Economy 113 (2005) 485–517.

[67] R. F. Engle, Autoregressive conditional heteroscedasticity with estimates of the variance of united kingdom inflation, Econometrica: Journal of the Econometric Society (1982) 987–1007.

[68] T. Bollerslev, Generalized autoregressive conditional heteroskedasticity, Journal of econometrics 31 (1986) 307–327.

[69] T. Bollerslev, J. M. Wooldridge, Quasi-maximum likelihood estimation and inference in dynamic models with time-varying covariances, Econometric reviews 11 (1992) 143–172.

[70] S.-H. Poon, C. Granger, Practical issues in forecasting volatility, Financial Analysts Journal 61 (2005) 45–56.

[71] P. R. Hansen, A. Lunde, A forecast comparison of volatility models: does anything beat a garch (1, 1)?, Journal of applied econometrics 20 (2005) 873–889.

[72] C. T. Brownlees, R. F. Engle, B. T. Kelly, A practical guide to volatility forecasting through calm and storm (2011).

[73] N. Vlastakis, R. N. Markellos, Information demand and stock market volatility, Journal of Banking & Finance 36 (2012) 1808–1821.