

AMERICAN UNIVERSITY OF BEIRUT

POSSIBILITY OF USING BITCOIN AS A STORE OF VALUE
AND A MEANS OF EXCHANGE, AND THUS REPLACING
FIAT MONEY

by

ELIAS RAYMOND CHOUCAIR

A project
submitted in partial fulfillment of the requirements
for the degree of Master of Arts in Financial Economics
to the Department of Economics
of the Faculty of Arts and Sciences
at the American University of Beirut

Beirut, Lebanon
May 2018

AMERICAN UNIVERSITY OF BEIRUT

POSSIBILITY OF USING BITCOIN AS A STORE OF VALUE
AND A MEANS OF EXCHANGE, AND THUS REPLACING FIAT
MONEY


by
ELIAS RAYMOND CHOUCAIR

Approved by:

Dr. Leila Dagher, Associate Professor
Economics


First Reader

Dr. Casto Martin Montero Kuscevic, Assistant Professor
Economics


Second Reader

Date of project presentation: May 2, 2018

AMERICAN UNIVERSITY OF BEIRUT

THESIS, DISSERTATION, PROJECT RELEASE FORM

Student Name: Choucair Elias Raymond
Last First Middle

Master's Thesis Master's Project Doctoral Dissertation

I authorize the American University of Beirut to: (a) reproduce hard or electronic copies of my thesis, dissertation, or project; (b) include such copies in the archives and digital repositories of the University; and (c) make freely available such copies to third parties for research or educational purposes.

I authorize the American University of Beirut, to: (a) reproduce hard or electronic copies of it; (b) include such copies in the archives and digital repositories of the University; and (c) make freely available such copies to third parties for research or educational purposes

after : **One ---- year from the date of submission of my thesis, dissertation, or project.**

Two ---- years from the date of submission of my thesis, dissertation, or project.

Three ---- years from the date of submission of my thesis, dissertation, or project.


Signature

16/5/2018
Date

ACKNOWLEDGMENTS

Special thanks are for Dr. Leila Dagher, Dr. Casto Martin Montero Kusevic for sharing their valuable knowledge in the studied field and their assistance in my research paper.

AN ABSTRACT OF THE PROJECT OF

Elias Raymond Choucair for Master of Arts in Financial economics
Major: Financial Economics

Title: Possibility of using bitcoin as a store of value and a means of exchange, and thus replacing fiat money

Bitcoin, a decentralized digital currency introduced in 2009, has become a major product invading the global market. Bitcoin differs from many commodity currencies by its nature and function. Using a GARCH/ARCH model I will try to elaborate a model in order to identify the possibility of bitcoin to become a viable alternative to commodity currencies and a new means of exchange across the world.

CONTENTS

	Page
ACKNOWLEDGEMENTS	v
ABSTRACT	vi
Chapter	
1. INTRODUCTION	1
2. DEFINITION OF BITCOIN AND BLOCKCHAIN TECHNOLOGY	4
2.1. The Evolution of Mining.....	6
2.2. Understanding Bitcoin Mining Profit	7
3. LITERATURE REVIEW	9
4. BITCOIN'S FUNCTIONALITY AS A CURRENCY.....	11
4.1. Store of Value	11
4.2. Unit of Account.....	12
4.3. Proof of Security	12
4.4. Medium of Exchange	14

5. DISADVANTAGES OF ADOPTING BITCOINS	15
5.1. Bitcoins Aren't Accepted Widely	15
5.2. Wallets Can Be Lost	15
5.3. Bitcoin Valuation Fluctuates.....	15
5.4. No Buyer Protection.....	16
5.5. Built In Deflation	16
5.6. No Physical Form.....	16
5.7. No Valuation Guarantees	16
6. EMPIRICAL STUDY	17
6.1. Data	17
6.2. Methodology	18
6.2.1. Clustering Volatility	20
6.2.2. Arch Effect	21
7. CONCLUSION	24
Appendix	
A. FIGURES AND TABLES.....	26
REFERENCES	32

CHAPTER 1

INTRODUCTION

With the speedy growth of technology, the world has witnessed, people are looking deeper into every new arising aspect. One of the most common topics turning heads nowadays is “money”. Individuals who are interested in investments are constantly asking “What is the future of money?”. While little is known about how money originated, paper money was first introduced in China in 740 B.C. by the Tang Dynasty (Dumas 2015). Moving forward in time, and with the invention of credit and debit cards, and the online banking system, money’s sole purpose remains to make trades easier. Although the presence of the internet has erased the borders between the countries, currencies are still bound to the physical limits of their respective countries.

In order to achieve the decentralization of the transactions’ monitoring, a new notion has been studied by a person or group known as Satoshi Nakamoto. The latter introduced a study on Bitcoin which is a network-encrypted virtual currency with no dominant power. A year after the publication of the paper, in 2009, Nakamoto launched the first units of bitcoin. The bitcoin falls under a broad category, known as cryptocurrencies. By definition, a cryptocurrency is a currency that uses cryptography for security making it difficult to fake and resistant to government interference. The Bitcoin has attracted the attention of many investors ever since it was launched. As of September 2015, the total market value of the former was equivalent to 3.4 Billion US Dollars. Its success has led to the creation of a number of competing cryptocurrencies, such as Litecoin, Namecoin and PPCoin.

Since digital currencies have made the headlines on several occasions and have become important in our world today, it is crucial to understand how they work in order

to deduce their effects on our future. Authorities are going deeper in their studies to see how this invention may affect their tax and monetary policies. Not only are governments interested in the functioning of cryptocurrencies, but also investors are eager to learn more about them and how to use them. This is so because the virtual coins allow an easier process of funds' transfers with minimal fees and zero government manipulation.

This thesis targets to study the world of cryptocurrencies. Since bitcoin was the first digital currency to make surface having the highest trading volume and market capital, it will be used as a basis for this study. This way it will be easier to comprehend how all virtual currencies function. Bitcoins are virtual coins intended to be contained independently from banks. Thus, they provide a method to interchange tokens of value online. With the lack of centralization, the records are kept in a "blockchain". Similar to the books in a bank, the latter is a ledger that holds the transaction history of all bitcoin on the network that is exclusive to every individual. Since there is no central authority, mining is used to add the trades on the blockchain and turn them into a mathematical puzzle. People who perform this procedure later receive new Bitcoins as a way of motivating them to prevent fraud. At this level, it is important to observe the differences between Bitcoins and the real currencies.

First and foremost, Bitcoins are not issued by governments and central banks such as the Fed. Therefore, they are not bound to the physical borders of any country. However, they are supported by an international network. As a result, the forex rate can be obliterated. This will make it easier for international companies to be secure against currency conversion risk.

Moreover, the virtual currency in question has an unchanging, foreseeable supply in contrast to other currencies like EUR. This is due to the fact that as the

number of miners (Bitcoin providers) increases, the supply of Bitcoins rises at a constant level.

CHAPTER 2

DEFINITION OF BITCOIN AND BLOCKCHAIN TECHNOLOGY

Bitcoin is a digital crypto currency. It is the first decentralized currency (is not generated by a government), and it was created in 2009. It uses encryption techniques to balance the production of units. Since bitcoin is used to manage the transfer of funds between two parties without the interference of a central bank, it is difficult to integrate it in the economy. As a result, the basis of this virtual currency should be studied thoroughly. The technicalities in the creation of the bitcoin will be therefore explained. For a bitcoin transaction to take place, two number sequences should exist and belong to the owner. The first sequence is known as the private key and the second is the public verification key. The former is only known to the owner and is used to make a payment. On the other hand, the second key is recognized by the whole network of users, and it is used to receive the payment and confirm the trades. Both sequences, being indispensable to the users, form what is known as a bitcoin wallet.

Consequently, when a payment is being made, three factors must be taken into account. They are recognized as: the amount to be paid, the change and the tips. To begin with, we consider the Buyer “A”, the Seller “B” and the miner (the one who verifies the transaction and adds it to the public ledger). When “A” wants to execute a transaction, it will have to precise how much tips and change it will receive after the operation is carried on. After all the above is agreed on, “A” will use its private key to sign and make the payment to “B” using its public key. This verified deal will then be announced to all users on the network who can verify the validity of the transaction

using “A’s” public key. Afterwards, the miners will add this specific operation into the block. Hence, the transaction of “A” is complete and “B” collects the payment.

The miner is crucial to the bitcoin community. This is so because its job is to verify the transactions made and gather information to create blocks. The latter are used to make up a blockchain. By definition, a blockchain is an assembly of blocks that records every transaction made. It is denoted as the public ledger. As its name indicates, the blockchain gives every user on the network the opportunity to see the transaction of every wallet. Thus, the miners are rewarded for their work. The remunerations they receive come from two different sources. The first one is the tips indicated at the beginning of the operation by the buyer. There are no fixed rates for tips; it is up to the buyers to pay as much as they want. The second compensation received by miners is known as the coin-based income. This means that whenever these people finish a block they earn 25 bitcoins. This way, new units of this crypto currency enter the flow. Unlike the tips, the coin-based income is fixed. Once the records are collected into the block, the most complicated procedure of bitcoin mining begins. It is known as “proof of work”.

Proof of work is intended to be complicated for miners to decipher; however, it is easy for the network to validate once a solution is obtained. It is meant to be difficult to solve so that miners spend some amount of time in making the blocks. Subsequently, the bitcoin supply is limited through the control of coin-based income. This will increase the value of the digital currency and make it harder to acquire. Since the rate of coin production needs to remain constant, the production time of new blocks has to be 10 minutes per block. With the technological advances, the complexity of the “proof of work” is adjusted every two weeks. Hence, when blocks take less than ten minutes to be created, the level of intensity increases and the mining slows down.

Moving on with the process, proof of work is obtained by a procedure called hashing. The second is a bunch of functions that generate outputs given certain inputs. The yield of this formula is referred to as the digest. The digest is a random result, and therefore it cannot be forecasted given the input. When miners solve the proof of work, they need to obtain a result, the digest, which is below the target number. This number belongs to the interval of 1 and $1.1579209e+77$. Since every input results in a random output, miners cannot predict which digest is below the target. When the target is smaller, the probability of obtaining a digest less than the former decreases, and the difficulty increases. This means that the miners will have to use billions of inputs.

Finally, the rapidity required to get the correct result is known as the hashrate. When the miners' speed "hashrate" is higher, the precise proof of work is attained faster. Once the right proof of work is found, miners have the right to ask for their bitcoin and add one block to the blockchain.

2.1 The Evolution of Mining

The mining process has been growing at a persistent rate. From 2013 and on, the bitcoin price has drastically augmented leading to the high value of the digital currency. Therefore, many firms and miners joined the bitcoin production procedure. The level of difficulty of the process has been consequently rising, and mining has become more and more challenging. Mining a bitcoin three years ago would have taken a new Mac Pro desktop computer 269 years¹.

In addition to the above, the basis of bitcoin mining has changed. It has become more specialized. Thus, the personal computers once used in the process are no longer efficient. This is so because they do not have enough computational power to participate in the mining process. As a result, Application-Specific Integrated Circuits (ASICs)

were created for the purpose of mining. These circuits decreased the use of energy of the mining process and improved the hashrate (Morrow 2014). This led to the advancement of a mere hobby in becoming a profitable industry.

It is vital to understand the importance of mining in the bitcoin system. During the process, miners aid in the circulation of the bitcoin through helping with the transactions. Moreover, as the number of miners increases, this particular network becomes more protected. Subsequently, hacking the bitcoin network is quite impossible.

2.2. Understanding Bitcoin Mining Profit

In order to understand how the profits resulting from the mining process are calculated, one must look at several factors. First and foremost, it is important to mention that the previously mentioned procedure is extremely demanding on the system. Therefore, the ASICs need to be used constantly, resulting in their drainage. The price of the circuits used varies from hundreds to several thousand dollars. In addition to the expense of the ASICs (which is the fixed cost), electricity bills are a factor to look at. This is so because, electric energy is needed for the ASICs to run and for the cooling devices required by the circuits. Moreover, the profit is also affected by the speed at which a unit of bitcoin is mined and added to the blockchain. Finally, the profitability of mining is affected by the price of the bitcoin itself.

Since the price of bitcoin fluctuates rather quickly, the profit awarded to the miners is bound by economic risks. In January 2015, for instance, the price of bitcoin started off as 317.00 – USD and plunged to reach 183.00 – USD on the 14th of January which was the lowest (Coinmarketcap 2015). Due to this drop in the bitcoin's price, several mining operations were obliged to stop.

Over and above the volatility of the bitcoin's price, the recompense received at the end of mining is not constant. The reward which was set at 25 bitcoins in 2015 is automated to be divided by two every four years. Since July 2016, the reward received became 12.50 bitcoins. Halving the reward of the block, *ceteris paribus*, will lead to doubling the price of the bitcoin.

CHAPTER 3

LITERATURE REVIEW

Bitcoin significantly rose since its creation, and been treated in many research as its rise has implications for four different fields. The first field treated was the technological one, including cryptography technology, system security and blockchain concept itself. (1) Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015) presented the platform design principles and stress on its past, present and future uses by pointing out risks and main issues as bitcoin interact with the traditional financial system. (2) SebastianFeld MircoSchönfeld MartinWerner (2014) explained the ecosystem of bitcoin and how transaction blocks are built and integrated in the blockchain. (3) Elli Androulaki , Ghassan O. Karame, Marc Roeschlin (2013) investigated the privacy provision in bitcoin when it is used by consumers as a currency for their daily transactions. (4) Dorit Ron, Adi Shamir (2013) analyzed for the first time how users behave with their bitcoin in their wallet in order to better protect their privacy. The second field treated looks at legalization and public issues, checking on how bitcoin is treated in the legal jurisdictions, along with the treatment of taxes arising from bitcoin trading operations and anti-money laundering regulations. (5) Bryans (2014) focused on the impact of virtual currencies on anti-money laundering, (6) Christopher (2014) described first the US antimony Laundering laws, then discussed the use of bitcoin as a tool for money laundering, and he conclude that cryptocurrency exchangers should be treated as partner in protecting the financial system from these type of crimes. (7) Tropina (2014) stressed on the issues of cyber-laundering by studying the challenges that tackled online money laundering. The third area related to political and ethical

implications concerning the integration of bitcoin. Especially libertarians found an opportunity in the fact that this technology relies on decentralization so it get out of governments control and financial institutions manipulation. (8) Karlstrom (2014) mentioned the possibility of taxation of an untraceable money, (9) Angel and McCabe (2014) stated that payment tools like cryptocurrency are ethically neutral since it could be used in both ethical and unethical way.

The last and most important area of research involves economic issues on the global scale. This includes questioning first whether bitcoin performs functionally as money (10) Evans (2014) (11) Wang (2014) presented a model where bitcoin value depends on the willingness of its holder to save and not transactional use, in other term bitcoin won't fall in a liquidity trap. Second, its investment potential, (12) Yermack (2013) found that bitcoin look like a speculative investment close to the internet stocks of the late 1990s. (13) Polasik (2015) ran an empirical study but couldn't find out a way to fairly price bitcoin since it yields no dividends, cash flows or earnings.

CHAPTER 4

BITCOIN'S FUNCTIONALITY AS A CURRENCY

Satoshi defined bitcoin as “A peer-to-peer version of electronic cash”, by that he meant that bitcoin is an electronic currency. Economically speaking, currency is defined to function as: Medium of exchange, store of value and a unit of account. Even the presence of these three characteristics doesn't necessarily make a currency successful and not eligible to Fraud problems for example, fraud lowers the credibility of a currency. Since every currency is pegged and secure by the government we assume it security for most of the times. From a personal perspective I do believe that a successful functioning of a currency is related to its evidence of storage of value, unit of account, proof of security and a medium of exchange.

4.1. Store Of Value

Currency first should persevere its value for the long run in order to have a current value. Traditional (national) currencies have a maintained value because of the intervention of central banks which control its fluctuation based on some criteria as inflation and level of unemployment. For example one of the tools for a reduction in inflation is by lowering the money supply. In a period where deflation governs central bank push the economy by increasing the money supply to surpass this deflation (devaluation its currency. Conversely, Bitcoin is not controlled by a central bank and the range of its prices fluctuation is too wide.

In Figure 1, I illustrated the absolute value of daily fluctuation in the prices of BTC, Euro and US dollar during 2017. We can directly notice that BTC has a significant higher fluctuation in price compared to Euro and USD. On average BTC

daily fluctuation in absolute value is 4.66%, while Euro has a 0.72%, and USD has a 0.67%.

Bitcoin's price fluctuation compared to other government issued currency is too volatile. Concerning storage of value, bitcoin is poor at least in the short run due to this high instability in its price. For risk-averse consumer, the instability and high fluctuation in bitcoin price turned to be in favor of the government issued currencies, and this is one of the major obstacles for BTC to become a mainstream currency used by a large portion of the market.

4.2. Unit Of Account

Unit of account means, divisible, verifiable, and fungible.

In our case bitcoin is divisible to eight digits after the decimal point and each transaction is verifiable since it is recorded in the blockchain and available to all the nodes (interested parties in the blockchain). Here is the most important part of this section. Is Bitcoin fungible? The answer is yes, if one bitcoin is interchangeable with another bitcoin. Each bitcoin in circulation is represented in the same way in the Bitcoin protocol. There is no difference between all the Bitcoins in the blockchain and this is what makes Bitcoin Fungible.

4.3. Proof of Security

Bitcoin security is through cryptographic technology and an incentive structure of hashes and blocks that discourages cheating. When creating Bitcoin the biggest challenge was to create a structure to prevent double spending (when the same digital currency is spent twice). For example, A bought X product with one Bitcoin. If A then used the same bitcoin to buy another X, he would be double spending that Bitcoin. By

recording all the Bitcoin transactions and maintaining the network blockchain, no transaction could be doubled and this is what makes the blockchain network secure.

To avoid uncertainty, Bitcoin network only accepts the longest blockchain as a reference for transactions and accounting information. For more security, the Bitcoin protocol states that only the longest blockchain is accepted as the legitimate chain because the longest one must have the larger number of miners working on it then it's more likely to be the most trustful chain. In case of attacking the Bitcoin network, the hacker must change the information in the blockchain. For instance, let's assume "A" wants to double spend his Bitcoin. When the transaction is confirmed first and accepted by the network, his Bitcoin is already delivered to the merchants. In order to be able to spend the same bitcoin again, "A" has to modify the transaction history starting with the moment he spent his bitcoin. In this scenario, "A" should start creating an alternative chain that doesn't include or record his payment to the merchant. We already stated that the network only accepts the longest chain. In other word, "A" has to make sure that his alternative chain is the longest in order to alter the record of his Bitcoin and get it back.

I will take Figure 2, in order to illustrate a hacking process example. Let us assume that "A" bought a house using 200 Bitcoins in time period two. The seller will deliver the house when "A" s payment is confirmed. That means that "A" s transaction must be recorded in the second block. In order to retreat the transaction history, "A" has to produce a fake block, (block 4) that doesn't include the transaction between himself and the seller and here we are referring to alternative blockchain. Now in order for the network to approve his revision,"A" has to make sure that his alternative chain is the longest. It's very difficult for the hacker to proceed in his alternative "fake" chain because he has to obtain the correct proof of work quickly and he is basically racing against the sum of honest miners in creating blocks and to achieve the longest chain.

4.4. Medium of Exchange

Basically, this relies on whether businesses accept bitcoin as one of many forms of payment. The number of businesses accepting Bitcoin as a medium of exchange is relatively too small, so the main point here is to attract more firms to use it to improve this function. Coinmap is a famous website that tracks all the business around the world that take bitcoin as a form of payment. An individual can use this website in order to find local businesses near him to use his Bitcoin, as shown in Figure 3 Using Bitcoin as a payment system can reduce transaction fees and time and this is in favor of the firms who look for a better cost management (Credit card process fee is 2%, in the case of Bitcoin it is less than 1%). Payments using Bitcoin have a faster turnover than payments using credit cards (credit card payment process takes weeks for banks) and since small businesses rely on fast cashflow in order to financially cover their activities, a merchant using Cainbase wallets to process bitcoin payment will be paid in two days only.

CHAPTER 5

DISADVANTAGES OF ADOPTING BITCOINS

In this section, I will discuss the disadvantages of Bitcoin.

5.1. Bitcoins Aren't Accepted Widely

Just a small group of online merchants accept bitcoin, this makes bitcoin not reliable as a currency. Moreover, governments could also ban the use of bitcoins in order to track user's transactions.

5.2. Wallets Can Be Lost

Bitcoins are essentially "lost" if a hard drive crashes or data is corrupted by a virus. Nothing could be done to recover it. These coins will be forever lost in the system and no one can track it by then.

5.3. Bitcoin Valuation Fluctuates

The main factor of bitcoin price fluctuation is the market demand. This fluctuation will lead bitcoin accepting sites to continually modify prices and thus create confusion in case of a refund for example. If a car was originally bought for 3 bitcoins and returned after a week, should 3 bitcoins be returned even though its valuation has changed or should the new amount be sent? Which currency should bitcoin be tied to when measuring valuation?

5.4. No Buyer Protection

Transaction can't be reversed, that means if a product was bought using bitcoins and the seller didn't send the product nothing can be done for the buyer to recuperate his bitcoins. This issue could be solved by using a third party like "ClearCoin" , this will take us back to the main role of banks which lead back bitcoin to act like traditional currencies.

5.5. Built in Deflation

Total supply of bitcoins is determined primarily, at 21 million units, the fact that supply is limited will cause deflation on the long term since each bitcoin will be worth more as the total number of bitcoins mined increases. So far this system tends to reward early adopters.

5.6. No Physical Form

Experts proposed cards with bitcoin wallet information storage but there isn't consensus on a specific system.

5.7. No Valuation Guarantees

No one can guarantee bitcoin minimum valuation since there isn't a central authority manipulating bitcoins. With a simple supply/demand theory, if a potential group of investors decided to dump their bitcoins and leave the system, its valuation will decrease and that will affect other bitcoin investors in the system with no valuable excuse for that price movement.

CHAPTER 6

EMPIRICAL STUDY

6.1. Data

The daily bitcoin data is gathered from Coindesk. Coindesk relies on the Bitcoin Price Index known as BPI, that is the price of a bitcoin in USD and an average of the main global bitcoin exchanges. BPI is convenient when taking into consideration the price divergence between different exchanges. All existing price data is used in this following testing to avoid constructing a bias by picking a small sample. Our data sample ranges between July 20, 2010 until April 19, 2018, which is around eight and half years or exactly 2023 daily observations. In Figure 4, Bitcoin daily price chart of our timeframe could be seen.

Recent studies centered on forecasting the exchange rate levels instead of their volatility. Mostly exchange rate volatility is explained by macroeconomic variables as interest rates, money supply, exports and inflation. In our case, bitcoin is not related to any country since it is decentralized so its exchange rate volatility won't be interpreted by macroeconomics variables of a specific economy. For us to pick the appropriate variable, we must consider first where bitcoin is traded the most.

As we can notice in Figure 5, CNY has the most traded volume in the recent years, followed by USD, Euro and JPY. We can assume that external and macro factors related to China are significant in determining Bitcoin's volatility (same goes to the United States, EU and Japan). Therefore, I will use as explanatory macroeconomic variables the CNY (Chinese yuan renminbi) since most of the bitcoin are traded with this currency and two indices that reflect both economies where bitcoin is traded, S&P 500 (US) and Shanghai stock composite index (China). And since gold and bitcoin

share certain specifications as limited quantity and safe haven, I will add this precious metal to my empirical study. Note to mention, that explanatory variables aren't complete since financial markets are closed on weekends.

6.2. Methodology

Before testing or running any regression, we tested the stationarity of the variables by running a unit root test using “Augmented Dicky-Fuller” method, where the null hypothesis is the following: $H_0 = \text{variable has a unit root}$

From the following Figure 6 we can notice the existence of a unit root by rejecting the null (Probability less than 0.1). As a response to this issue, I will be using the log returns of the daily price of these variables to avoid having a unit root and get stationary variables:

$$R_t = \log(P_t) - \log(P_{t-1}) \quad \text{where: } R_t = \text{log returns at time } t$$

$$P_t = \text{price of the variable at time } t$$

After computing the log returns of all the variables Figure 6 we induce a Probability less than 0.1, which is a rejection of the null hypothesis, no unit root. Variables are stationary and could be used to run the regression.

No cointegration test is needed in this study since we are concerned with the short run relation and not the long run relation between the variables.

In our empirical work, to understand the mechanism of the GARCH model we must first elaborate the ARCH model. ARCH model (Autoregressive Conditional Heteroskedasticity) was introduced first by Engle in 1982 to estimate time varying volatility. The main idea of this model is that we can get a more accurate volatility estimation by taking into consideration previous periods data. In other word, that means that the current volatility is directly related to the information of the previous period.

Before setting this model, econometricians used to test their time series data by the ordinary least squares (OLS) method which is useful when the variance of residuals is constant. But if the variance of the residuals varies with time, what we call heteroskedasticity, which is the case of bitcoin in our study, we must set another method which is the weighted least squares (WLS) for the estimation of the regression. Ordinary least squares residuals are transformed into an endogenous process through the ARCH model.

In the case of bitcoin, Gauss Markov assumptions of the OLS fails since the data is heteroskedastic and the variance equal to a certain constant won't hold.

ARCH and GARCH are composed of two equations, a conditional mean equation and a conditional variance equation. These two equations should be estimated at the same time since the variance is a function of the mean.

Engel presented the first equation (conditional variance) of the ARCH (1) model as the following.

$$\sigma_t^2 = \omega + \alpha \varepsilon_{t-1}^2 \quad \text{With} \quad \omega > 0, \alpha \geq 0$$

The forecast of the current conditional volatility relies on the residual return in the previous period. "P" stands for the number of lags, ARCH (p) means how many lags of the squared residual return should be present to forecast. ARCH (P) is represented in the following equation:

$$\sigma_t^2 = \omega + \alpha_1 \varepsilon_{t-1}^2 + \dots + \alpha_q \varepsilon_{t-q}^2 \quad \text{With} \quad \omega > 0, \alpha_1 \geq 0, \dots, \alpha_q \geq 0$$

Bollerslev developed an extension of the ARCH model and named it GARCH which stands for Generalized Autoregressive Conditional Heteroskedasticity. This generalized version of the GARCH was created since crisis with large residuals aren't captured, as large residual crisis won't have the same persistence as it is detected during a current crisis.

GARCH (p,q) is composed of two parts; 'P' for the number of lags of the squared residual return, "q" for the number of the present lags of variances.

$$\sigma_t^2 = \omega + \sum_{i=1}^q \alpha_i \varepsilon_{t-i}^2 + \sum_{j=1}^p \beta_j \sigma_{t-j}^2,$$

GARCH (1,1) is the most widely used, it means that forecast of the volatility at time t, is a function of the weighted average long-term variance, squared residual return and volatility at previous periods.

To start with GARCH (1,1) model we should set a conditional mean equation, conditional mean and variance equation must be estimated simultaneously.

With a stationary time series, AR model is widely used when the volatility of a return is questioned.

Before testing the GARCH model, statistical properties of the mean equation should be examined. The two conditions are the following:

6.2.1. Clustering Volatility

Figure 7 stresses on this condition since periods of low volatility of the error term precede the periods of low volatility and those of high volatility of the error term precede those of high volatility. That means that high returns are followed by high returns and vice versa. That phenomena shows conditional heteroskedasticity of the residuals.

6.2.2. ARCH Effect

ARCH is used to prove the existence of serial correlation of the heteroskedasticity, the existence of ARCH effect is tested by an LM ARCH test, where the null hypothesis is the following:

H0 = No ARCH effect

The results shown in Figure 8 showed that the null hypothesis is rejected, meaning a strong evidence of an ARCH effect in the equation of the mean. Moreover, Figure 9, by doing a Breusch Pagan test and adding lags we could accept the null of no serial correlation, since p is above 0.1

Both criteria are valid to run a GARCH (1,1) model; Note to mention the presence of multicollinearity between the exogenous variables, although multicollinearity is not an issue in this paper since it treats macroeconomics on a global scale rather than on a national scale.

Regarding variance equation, Figure 10, ARCH (α) and GARCH (β) are statistically significant:

ARCH: Today's volatility of bitcoin is affected by the previous day's return of bitcoin.

And the mean equation is;

$$\text{BTC} = (0.065551) \text{XAU} + (0.895552) \text{CNY} + (0.788213) \text{Shanghai_index} - (0.002216) \text{SP500} + 0.052544 + 0.038522$$

GARCH: Today's volatility of bitcoin is affected by previous day's volatility.

The Variance equation is;

$$\text{GARCH} = (0.126255) \text{RESID} (-1)^2 + (0.601254) \text{GARCH} (-1) + 5.38\text{E-}05$$

Notice that $(0.126255 + 0.90254 = 1.03, \text{ around } 1)$ it is an indication of persistent and frequent shock on the bitcoin.

Moreover we notice that bitcoins volatility depends most on the China, since the CNY coefficient is around 0.9 (figure 10) which means a 1% change in CNY volatility incur 0.9% change in bitcoins volatility. Same goes to Chinese market, where a 1% change in the volatility of the shanghai composite index induce a 0.79% change in the volatility of bitcoin.

A negative coefficient for the s&p 500, -0.002216, which means that everytime the US economy performs well, people intend to go for the traditional investments of the stock market rather than investing in bitcoin.

TGARCH: This test is used to show Asymmetric volatility.

“A situation in which the [volatility](#) of a [security](#) is higher when the broader [market](#) is performing poorly than when it is performing well. Experts disagree on what causes asymmetric volatility, but factors such as [leverage](#) and [panic](#) are often cited. The fact that asymmetric volatility exists is important to [hedging](#) strategies and [option pricing models](#).”

Farlex Financial Dictionary. © 2012 Farlex, Inc.

Through Figure 11 (prob 0000) asymmetry exists

Moreover past volatility effects are more remarkable than past stock effect, and to forecast bitcoin volatility, past volatility effects must be taken into consideration. Explanatory variables are significant in showing the volatility of bitcoin.

Macroeconomic explanatory variables of China and the US are significant in forecasting the volatility of bitcoin. Unfortunately that means that bitcoin is in the beginning phase of reacting to the same variables as its fiat currency counterparts in the US and China. So for bitcoin to act as an alternative global currency, it should behave independently and more widely (not concentrated in certain countries), in that way intervention events and macro shocks will be diluted and won't affect bitcoin as much as it is affecting now.

Furthermore, central banks play an important role in minimizing the systematic risk(volatility) of a currency using a variety of tools in the monetary policy (exchange rate, interest rate etc...)and since bitcoin is not guided by any central bank the ability to make macroeconomic adjustments to stabilize it exchange rate could not be reach. Therefore on the short term bitcoin is not able to reach the volatility levels of a stable fiat currency.

CHAPTER 7

CONCLUSION

To conclude, bitcoin doesn't fill the criteria of a currency, by not acting as a unit of account, store of value or effective unit of account. Bitcoin is acting as a demanded commodity with a finite supply; which makes it too speculative.

Volatility is the main factor for not letting bitcoin become an alternative to fiat currencies.

Since its creation, China was the main hub for this innovation, where bitcoin was mostly traded. This justify why bitcoins volatility is mostly influenced by events targeting China.

Unfortunately, bitcoin and fiat currencies of the countries mentioned in this paper reacts to the same factors, those which are significant in forecasting next day volatility of bitcoin.

So far for bitcoin to truly act as a decentralized alternative currency it must become less dependent on the economy of these countries.

Theoretically bitcoins volatility can't reach the volatility levels of stable fiat currencies for the fact that there is no entity as central banks to manage its stability.

APPENDICES

APPENDIX

FIGURES AND TABLES

Figure 1: BTC, EURO, USD daily price (2017) (source: Bloomberg)



Figure 2: Bitcoin Alternative Blockchains (source: Hennig 2015)

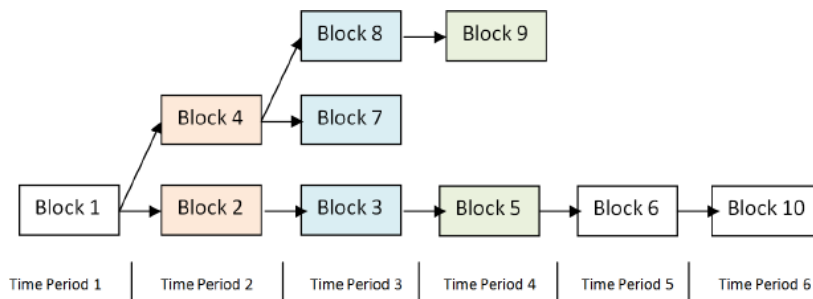


Figure 3: Homestead on Coinmap (source: OpenStreetMap 2015)

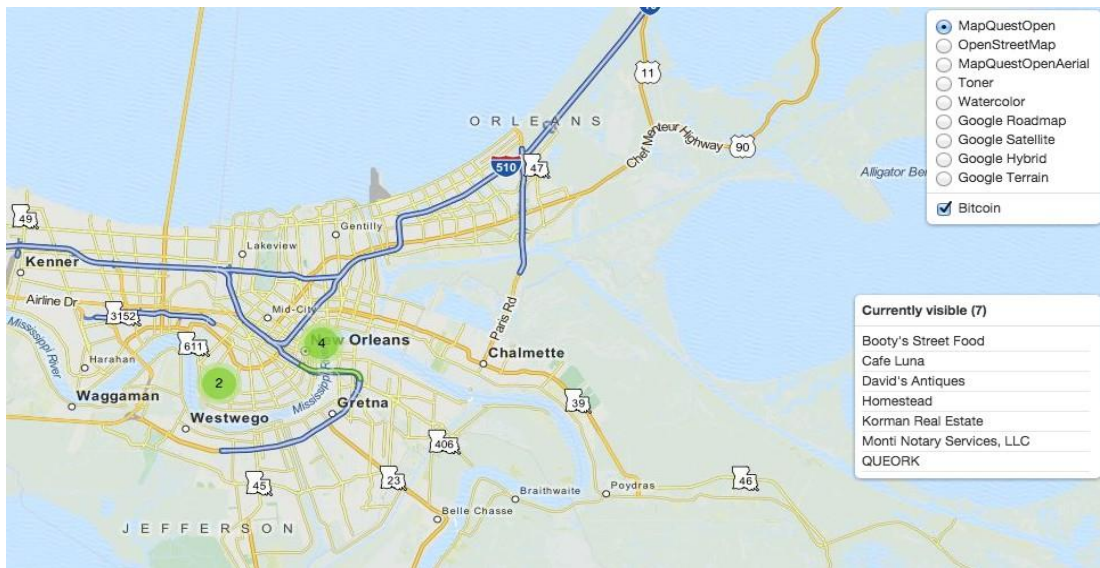


Figure 4: Bitcoin Price Index (source: Coindesk)

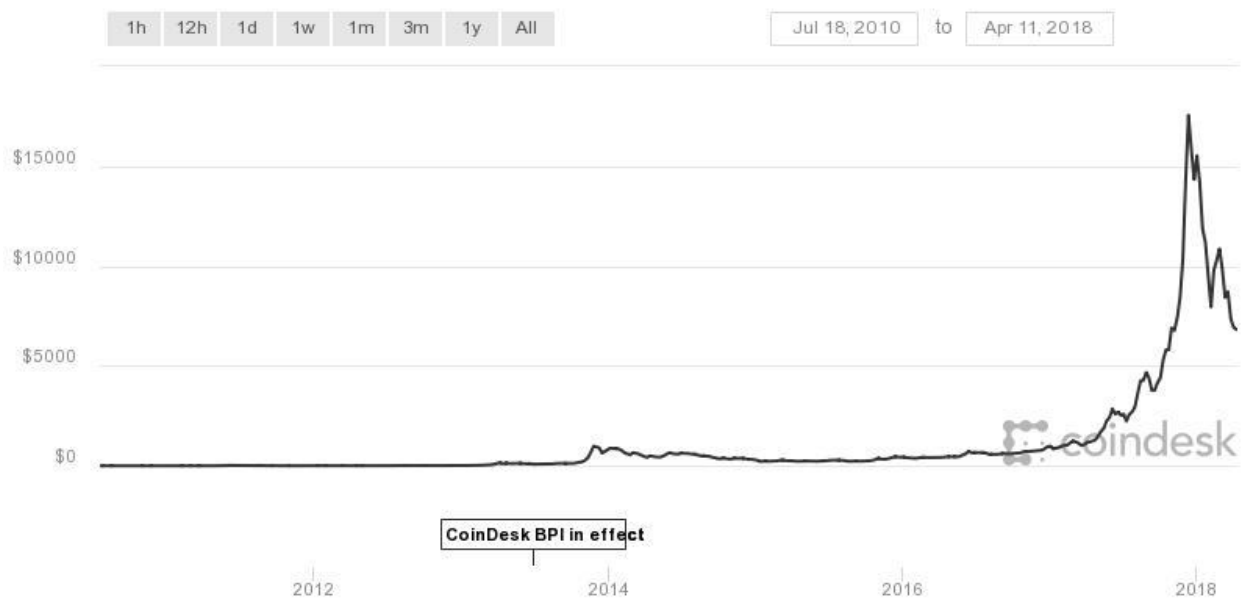


Figure 5: Bitcoin trading volume by the most traded currencies (source: Bitcoinity)

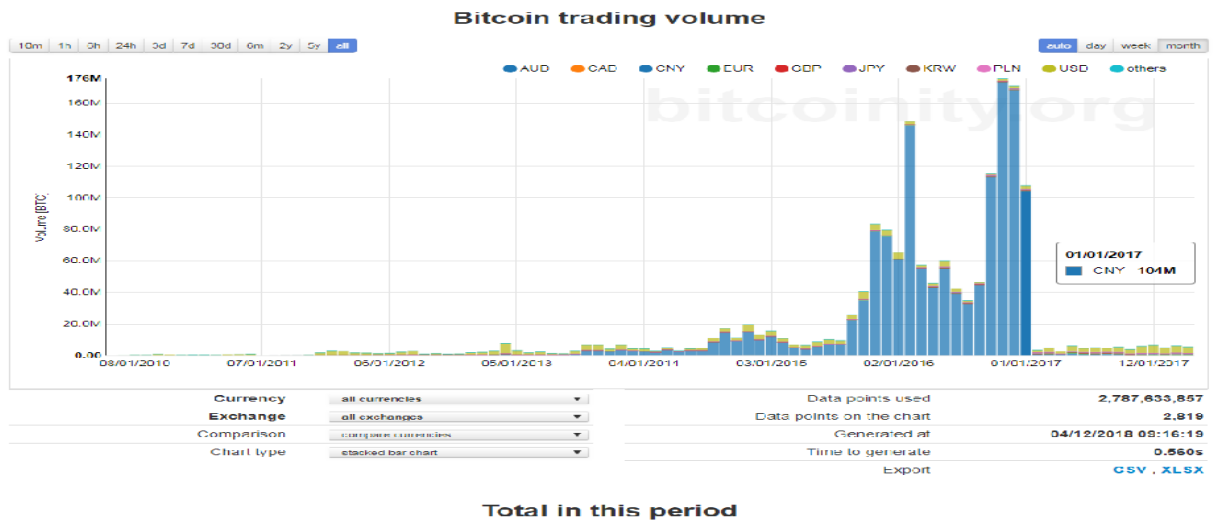


Figure 6: Results of unit root test by ADF (source: Eviews)

Variables	Prob (closing price)	Prob (log returns)
BTC	0.2440	0.000
Gold	0.2466	0.000
S&p 500	0.0551	0.000
CNY	0.6963	0.000
Shanghai composite index	0.4028	0.000

Figure 7: Bitcoin volatility (source: eviews)

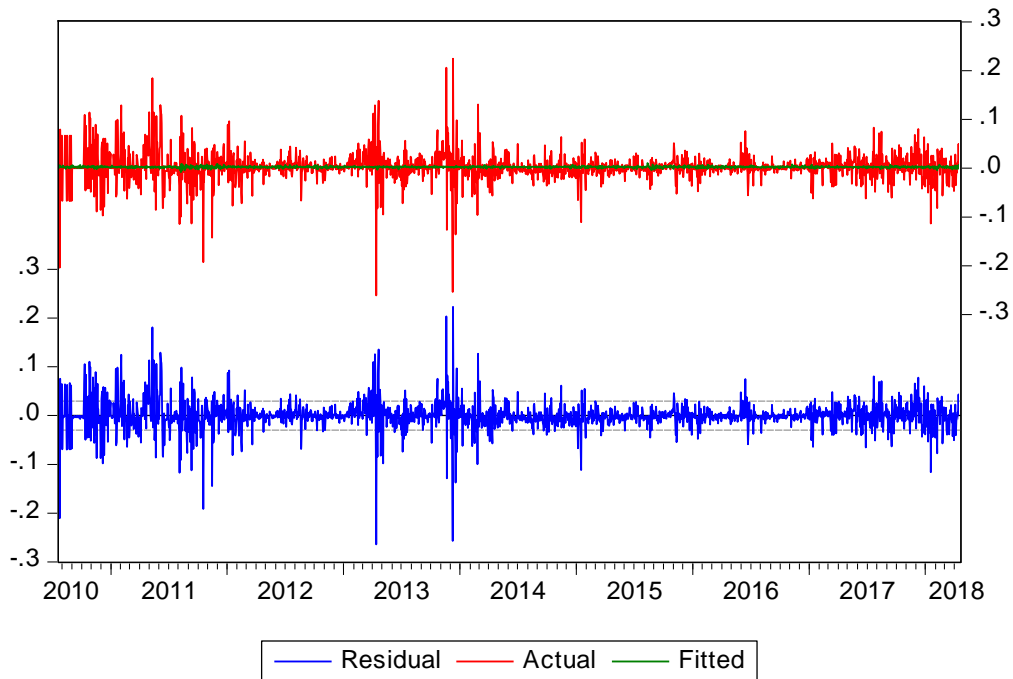


Figure 8: ARCH EFFECT (source: Eviews)

Heteroskedasticity Test: ARCH				
F-statistic	204.9120	Prob. F(1,2019)	0.0000	
Obs*R-squared	186.2156	Prob. Chi-Square(1)	0.0000	
Test Equation:				
Dependent Variable: RESID^2				
Method: Least Squares				
Date: 04/24/18 Time: 20:13				
Sample (adjusted): 7/22/2010 4/19/2018				
Included observations: 2021 after adjustments				
Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.000610	7.63E-05	7.997760	0.0000
RESID^2(-1)	0.303491	0.021201	14.31475	0.0000
R-squared	0.092140	Mean dependent var	0.000877	
Adjusted R-squared	0.091691	S.D. dependent var	0.003491	
S.E. of regression	0.003327	Akaike info criterion	-8.572343	
Sum squared resid	0.022352	Schwarz criterion	-8.566790	
Log likelihood	8664.353	Hannan-Quinn criter.	-8.570305	
F-statistic	204.9120	Durbin-Watson stat	2.016534	
Prob(F-statistic)	0.000000			

Figure 9: Breusch-Godfrey serial correlation test (source: Eviews)

Breusch-Godfrey Serial Correlation LM Test:

F-statistic	2.02285	Prob. F(2,2012)	0.8521
Obs*R-squared	47.66546	Prob. Chi-Square(2)	0.8354

Figure 10: GARCH (source: Eviews)

Dependent Variable: BTC
 Method: ML - ARCH (Marquardt) - Normal distribution
 Date: 04/30/18 Time: 19:35
 Sample (adjusted): 7/22/2010 4/19/2018
 Included observations: 2021 after adjustments
 Convergence achieved after 64 iterations
 Presample variance: backcast (parameter = 0.7)
 GARCH = C(7) + C(8)*RESID(-1)^2 + C(9)*GARCH(-1)

Variable	Coefficient	Std. Error	z-Statistic	Prob.
C	0.052544	0.002104	2.581547	0.0010
XAU	0.065551	0.236621	0.985874	0.0458
CNY	0.895552	0.501255	1.623548	0.0008
SHANGHAI_INDEX	0.788123	0.125544	2.658441	0.0000
SP500	-0.002216	0.852544	-0.528188	0.0087
AR(1)	0.038522	0.020765	1.855170	0.0636
Variance Equation				
C	5.38E-05	5.18E-07	7.789500	0.0000
RESID(-1)^2	0.126255	0.011841	22.53206	0.0000
GARCH(-1)	0.901254	0.015894	289.0265	0.0000
R-squared	-0.003014	Mean dependent var		0.025185
Adjusted R-squared	-0.004932	S.D. dependent var		0.035611
S.E. of regression	0.925452	Akaike info criterion		-4.215644
Sum squared resid	2.352148	Schwarz criterion		-4.235487
Log likelihood	4254.687	Hannan-Quinn criter.		-4.235154
Durbin-Watson stat	1.945196			
Inverted AR Roots	.04			

Figure 11: TGARCH (source: Eviews)

Dependent Variable: BTC
Method: ML - ARCH (Marquardt) - Normal distribution
Date: 04/30/18 Time: 19:39
Sample (adjusted): 7/22/2010 4/19/2018
Included observations: 2021 after adjustments
Convergence achieved after 76 iterations
Presample variance: backcast (parameter = 0.7)
GARCH = C(7) + C(8)*RESID(-1)^2 + C(9)*RESID(-1)^2*(RESID(-1)<0) + C(10)*GARCH(-1)

Variable	Coefficient	Std. Error	z-Statistic	Prob.
C	0.059517	0.002685	1.058554	0.0026
XAU	0.063557	0.410257	1.535448	0.0000
CNY	0.785112	0.525441	1.782875	0.0011
SHANGHAI_INDEX	0.795244	0.084274	2.156510	0.0000
SP500	0.335773	0.035547	-0.518497	0.0087
AR(1)	0.027612	0.021290	1.296942	0.0001

Variance Equation				
C	2.87E-05	3.74E-06	3.111120	0.0000
RESID(-1)^2	0.015254	0.025541	16.65217	0.0000
RESID(-1)^2*(RESID(-1)<0)	-0.158987	0.006123	-3.254825	0.0000
GARCH(-1)	0.985474	0.005874	224.3526	0.0000

R-squared	0.008891	Mean dependent var	0.05225
Adjusted R-squared	0.005110	S.D. dependent var	0.000565
S.E. of regression	0.009256	Akaike info criterion	-4.268949
Sum squared resid	0.952214	Schwarz criterion	-4.285674
Log likelihood	6154.222	Hannan-Quinn criter.	-4.287156
Durbin-Watson stat	1.935196		

Inverted AR Roots	.03
-------------------	-----

REFERENCES

- Böhme, R., Christin, N., Edelman, B. & Moore, T. 2015, "Bitcoin: Economics, Technology, and Governance", *The Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213-238.
- Feld, S., Schönfeld, M. & Werner, M. 2014, "Analyzing the Deployment of Bitcoin's P2P Network under an AS-level Perspective", *Procedia Computer Science*, vol. 32, pp. 1121-1126.
- Karame, G.O. & Androulaki, E. 2016, *Bitcoin and Blockchain Security*, Artech House Inc, Norwood.
- Ron D., Shamir A. (2013) Quantitative Analysis of the Full Bitcoin Transaction Graph. In: Sadeghi AR. (eds) *Financial Cryptography and Data Security*. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg
- Bryans, D. 2014, "Bitcoin and money laundering: mining for an effective solution", *Indiana Law Journal*, vol. 89, no. 1, pp. 441.
- Christopher, C.M. 2014, "Whack-a-mole: why prosecuting digital currency exchanges won't stop online money laundering", *Lewis & Clark Law Review*, vol. 18, no. 1, pp. 1.
- Tropina, T. 2014, "Fighting money laundering in the age of online banking, virtual currencies and internet gambling", *ERA Forum*, vol. 15, no. 1, pp. 69-84.
- Karlstrøm, H. 2014, "Do libertarians dream of electric coins? The material embeddedness of Bitcoin", *Distinktion*, vol. 15, no. 1, pp. 23-36
- Angel, J.J. & McCabe, D. 2015, "The Ethics of Payments: Paper, Plastic, or Bitcoin?", *Journal of Business Ethics*, vol. 132, no. 3, pp. 603-611.
- Evans, David S., Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms (April 15, 2014). University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 685. Available at SSRN: <https://ssrn.com/abstract=2424516> or <http://dx.doi.org/10.2139/ssrn.2424516>
- Wang, Joseph Chen-Yu, A Simple Macroeconomic Model of Bitcoin (February 11, 2014). Available at SSRN: <https://ssrn.com/abstract=2394024> or <http://dx.doi.org/10.2139/ssrn.2394024>
- Polasik, M., Piotrowska, A.I., Wisniewski, T.P., Kotkowski, R. & Lightfoot, G. 2015, "Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry", *International Journal of Electronic Commerce*, vol. 20, no. 1, pp. 9-49.