Charles University in Prague

Faculty of Social Sciences
Institute of Economic Studies

MASTER'S THESIS

Does Bitcoin Have Potential to Co-Function with Fiat Money

Author: **Bc. Josef Kurka**

Supervisor: **prof. Ing. Oldřich Dědek, CsC.**

Academic Year: **2015/2016**

Declaration of Authorship

The author hereby declares that he compiled this thesis independently; using only the listed resources and literature, and the thesis has not been used to obtain a different or the same degree.

The author grants to Charles University permission to reproduce and to distribute copies of this thesis document in whole or in part.

Prague, May 13, 2016

Signature

Acknowledgments

The author is grateful to his family and friends for support and understanding through the course of his work.

Abstract

This paper examines the potential of Bitcoin, a decentralized digital currency, to pose competition to fiat currencies. To accomplish that, Bitcoin would have to become efficient as a store of value. Thus far, high volatility makes it inferior in that respect. We analyze the dynamics and drivers of Bitcoin volatility using GARCH and HAR models. Moreover, we test for presence of asymmetries displayed by stock, commodity and currency markets. That way we can conclude, whether volatility of Bitcoin behaves similarly to currencies, commodities or stocks. Lastly we reveal interconnections between these markets and market for Bitcoin. We find significant evidence for the leverage effect documented for stock market. Furthermore, the effect of trading volume, documented for currency markets, displays an opposite sign in our research. Results of spillover estimation suggest Bitcoin is the most interconnected with commodity market. Thus, we conclude Bitcoin does not behave similarly to currencies in terms of volatility; hence is not a good candidate to substitute them.

JEL Classification	E1, G1, G2, O3
Keywords	Bitcoin, volatility, GARCH, leverage effect

Author’s e-mail	24805288@fsv.cuni.cz
Supervisor’s e-mail	dedek@fsv.cuni.cz

Abstrakt

Tato práce zkoumá potenciál Bitcoinu, decentralizované digitální měny, konkurovat tradičním „papírovým“ měnám. Aby to bylo možné, musel by se Bitcoin stát efektivním uchovatelem hodnoty, v čemž mu zatím bránila jeho vysoká volatilita. Tato práce analyzuje dynamiku a spouštěče této volatility za použití modelů GARCH a HAR. Dále je testována přítomnost asymetrií, které jsou prokázány pro akciový, komoditní a peněžní trh. To nám napoví o podobnosti Bitcoin akciím, měnám nebo komoditám. V poslední řadě zkoumáme předávání volatility mezi těmito jednotlivými trhy a objevujeme tak propojenost mezi nimi. Výsledky nenaznačují podobnost mezi chováním volatility Bitcoin a měn. Volatilita vykazuje přítomnost pákového efektu, který je zdokumentován pro akciové trhy, naopak, co se týče efektu objemu obchodů, výsledky pro Bitcoin jsou opačné než pro měnové trhy a největší propojenost vykazuje trh s Bitcoiny s trhem komoditním.

Klasifikace	E4, G1, G2, O3
Klíčová slova	Bitcoin, volatilita, GARCH, pákový efekt

E-mail autora	24805288@fsv.cuni.cz
E-mail vedoucího práce	dedek@fsv.cuni.cz

Contents

List of Tables

List of Figures

Acronyms

ARFIMA	Auto-Regressive Fractionally Integrated Moving Average
ARMA	Auto-Regressive Moving Average
CNY	Chinese Yuan
CTFC	Commodity Futures Trading Commision
EGARCH	Exponential Generalized Auto-Regressive Conditional Heteroscedasticity
EWMA	Exponentially Weighted Moving Average
EUR	Euro
FATF	Financial Action Task Force
GARCH	Generalized Auto-Regressive Conditional Heteroscedasticity
HAR	Heterogeneous Auto-Regressive
IGARCH	Integrated Generalized Auto-Regressive Conditional Heteroscedasticity
SEC	Securities and Exchange Commission
TSA	Treasury Single Account
USD	US Dollar
VAR	Vector Auto-Regressive

Master's Thesis Proposal

Author:	Bc. Josef Kurka
Supervisor:	Prof. Ing. Oldřich Dědek, CSc.
Defense Planned:	June 2016

Proposed Topic:

Does Bitcoin Have Potential to Co-Function with Fiat Money?

Motivation:

Satoshi Nakamoto (2008) published a paper proposing new peer-to-peer electronic payment system, an alternative to payment system mediated by financial institutions. This system later came to life as "Bitcoin". After a period of negligible Bitcoin usage in sales of goods and services, as well as limited activity on Bitcoin exchanges, price of one Bitcoin has risen from friction of dollar to over 200 USD in present times. Not any more is Bitcoin only a tool of amusement for computer "geeks", thus voices calling for its regulation are emerging. If Bitcoin usage became more widespread, it could be potentially used for speculative attacks on fiat currencies (Plassaras, 2013).

My goal is to find out, if Bitcoin could fulfill the three basic functions of money. Nowadays it serves as medium of exchange on a small scale, but its usability as a store of value and unit of account is questionable. Šurda (2012) applies definitions of money as stated by Mises (1980) on Bitcoin, to see if Bitcoin theoretically classifies as money. Then he also does empirical tests to see, if Bitcoin could become a widespread currency. Lo & Wang (2014) argue that Bitcoin possesses the key characteristics of a currency from a classical point of view. I plan to elaborate, which of different definitions of money Bitcoin suffices and then empirically verify if relatively low liquidity and high price volatility prevent Bitcoin from being an effective store of value.

Hypotheses:

1. Hypothesis #1: Bitcoin fulfills necessary criteria to be a medium of exchange.
2. Hypothesis #2: Bitcoin is inferior as a unit of account due to a high price against dollar.
3. Hypothesis #3: There exist statistically significant volatility spillovers between Bitcoin and currency markets.

Methodology:

The data for empirical part will be taken from exchanges trading with Bitcoin, along with currency exchanges. Daily data about changes in Bitcoin price against USD will be collected and daily, weekly and monthly volatility computed. Different approaches as described in Hull (1997) will be used to measure volatility. Measured volatilities will be then compared to price volatilities of selected currencies with different levels of importance on international markets. This approach will give us information, whether any functioning currency is as volatile as Bitcoin. The same approach will be used also for liquidity measures, specifically bid-ask spreads.

Nature of Bitcoin can also be documented by measuring co-movements with other currencies. We will examine linkages in volatility between Bitcoin and currency markets. If presence of these spillovers is verified, we will conduct a research on different strength of this effect for different countries. Spillovers should be stronger for countries, whose currencies are most used for Bitcoin related transactions (CHY, USD, EUR).

Usefulness as a unit of account is impossible to measure precisely. Thomas and Morwitz (2009) conducted a research on comprehensibility of prices for costumers. According to their results prices lower than 1, with many decimal points are difficult for customers to cope with and compare. This would be the case for Bitcoin, e.g. a pizza worth 10 USD would cost 0.0437 BTC nowadays. A survey detecting how uncomfortable does it make people to compare prices expressed in tenths or hundredths of Bitcoin will help us evaluate usability of Bitcoin as a unit of account.

Expected Contribution:

It can be assumed that Bitcoin is presently not suitable as a unit of account due to its high volatility. I will verify this assumption by estimating past volatility and comparing it to that of fiat currencies and investment and speculation tools (stocks, precious metals). Moreover I plan to examine the dynamics of volatility and model its movement in future periods and conduct a research on spillovers form currency markets. That will allow me to make conclusions about Bitcoin’s potential to substitute fiat money to some extent in the future.

Outline:

1. Introduction. Papers that inspired me for this thesis and my contribution to their results.
2. Description of Bitcoin. How it works, why was it founded, at major pros and threats.
3. Theoretical part. Does Bitcoin fulfill definitions of money?
4. Empirical part. Applying measures of price volatility and liquidity, comparing with major currencies. Testing how quickly Bitcoins are spent, to see how big fraction is used for speculation purposes.
5. Conclusion. Summary of results and few remarks about possible future development, taking those results into account.

Core Bibliography:

Ali, R., Barrdear, J., Clews, R., Southgate, J., 2014. The Economics of Digital Currencies. Bank of England Quarterly Bulletin 2014 Q3.

Hull, J.C., 1997. Options, Futures, and Other Derivatives. Prentice Hall, Upper Saddle River, NJ

Lo, S., Wang, J., 2014. Bitcoin as Money? Current Policy and Perspectives. 14(4)

Luther, W.J., White, L.H., 2014. Can Bitcoin Become a Major Currency GMU Working Paper in Economics No. 14-17.

Mises, L. von, 1953. The Theory of Money and Credit. New Haven, Conn.: Yale University Press.

Šurda, P., 2012. Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold? Diploma Thesis, WU Vienna University of Economics and Business.

Thomas, M., Morwitz, V., 2009, Heuristics in Numerical Cognition: Implications for Pricing. In Vithala R. Rao ed., Handbook of Pricing Research in Marketing. Northampton, MA: Edward Elgar Publishing.

Yermack, D., 2013. Is Bitcoin a real Currency? NBER Working Paper Series, Working Paper 19747.
Available at: http://www.nber.org/papers/w19747

Author

Supervisor

1 Introduction

When a programmer under pseudonym Satoshi Nakamoto (2008) published a paper introducing an innovative virtual currency named Bitcoin, he could have not anticipated the amount of success and recognition it is going have 8 years later. In the early stages, it was believed Bitcoin has flaws that would prevent it to see wider adoption. Probably the largest concerns were anonymity supporting settlements of illegal transactions through Bitcoin (Grinberg, 2011; Kaplanov, 2012; Brezo & Bringas, 2012), or proneness to deflationary spirals due to limited money supply (Grinberg, 2011). Few years after its inception, Bitcoin has become quite successful, and is traded all over the world. One of reasons behind its rise could be its high volatility that makes it a great speculation tool (Bouoiyour, 2015; Gomez-Gonzalez & Parra-Polania, 2014; Yermack, 2013). Increased demand and recognition have made Bitcoin a hot topic not only in the economic circles.

Frequent discussions deal mainly with problems and possible disruptions Bitcoin could cause. We suppose more light should be shed on its usefulness for its primary purpose. It was designed as an alternative currency to traditional banks backed currencies. Need for a central institution to oversee all transactions, and protect them against double-spending, causes high transaction costs of the traditional banking system (Nakamoto, 2008). The essential idea of Bitcoin is increase of effectivity, if it was possible to eliminate the central institution. Decentralization is ensured via blockchain technology; a public ledger containing all previously made transactions, and peer-to-peer transaction processing. To pose competition to fiat currencies, Bitcoin would have to fulfill three basic functions of money: medium of exchange, unit of account and store of value.

Increasing willingness of merchants to denominate prices in Bitcoin, besides fiat currencies, confirms it can serve as a medium of exchange and unit of account to a certain extent. Efficiency of an instrument as a store of value lies in limiting its volatility as much as possible. Thus far, Bitcoin volatility supported its use for speculations, rather than as a store of value (Yermack, 2013). The goal of this paper is to examine the dynamics and drivers of Bitcoin volatility as the market matures, and make conclusions about its future as a currency. Our hypothesis is; volatility of Bitcoin displays a downward trend.

As already stated, Bitcoin has been severely more volatile than currencies in the past; hence, direct comparison of volatilities is not very informative. Instead, we can look for similarities and interconnections between markets for Bitcoin, currencies, stocks and commodities. Estimation of volatility spillovers reveals the interconnections. Stock market volatility is documented to be influenced by asymmetric reaction to positive and negative returns, the "leverage effect" (Corsi & Reno, 2012; Bouchaud et. al, 2001), and the same asymmetry is documented also for volatility of commodities (Du et. al., 2009; Cheong, 2009; Morana, 2011). Currency markets, on the other hand, display different type of irregularity, negative correlation between trading volume in the past period and present volatility (Fung & Patterson, 1998; Scott & Tucker, 1988). Presence of any of these phenomena in Bitcoin volatility will serve as evidence for similarity between Bitcoin and the respective market. We assume market for Bitcoin to be most similar and interconnected with currency markets.

It is well documented in the literature, that volatility of financial market returns contains autoregressive features (Fung & Patterson, 1998; Scott & Tucker, 1988; Choi & Hammoudeh, 2010). Therefore we employ different models from Generalized Auto-Regressive Conditional Heteroscedasticity (GARCH) family. Specifically simple GARCH(1,1), that was shown to be superior for currency volatility estimation (Hansen & Lunde, 2005), Integrated GARCH (IGARCH) to allow for non-stationarity and Exponential GARCH (EGARCH) that accounts for the leverage effect, and outperforms GARCH(1,1) in stock volatility estimation (Hansen & Lunde, 2005). GARCH family models are used very frequently, although their drawback is no utilization of high-frequency data and strong distributional assumptions. High-frequency data are the core of Realized Volatility concept, a non-parametric method of volatility estimation. Realized volatility is the cornerstone of Heterogeneous Auto-Regressive (HAR) model proposed by Corsi (2004). Using HAR model, we can test for leverage effect using Realized Positive and Negative Semivariance, and for effect of trading volume.

The dataset used consist of 48500 observations of high-frequency prices from Bitcoin exchanges in three major Bitcoin markets, China, Europe and USA. Moreover, we use 1200 returns computed from daily closing prices from the respective exchanges to construct GARCH models, and 800 daily low and high prices for S&P 500 index, Bloomberg commodity index, the New York Board of Trade US dollar index futures and BTC/USD on BitStamp exchange for purpose of spillover estimation. The data range from January 2013 to April 2016, because the price of Bitcoin and its trading volume were negligible before 2013, and drawing any conclusions from data before

2013 would make no sense. Our contribution lies in revealing the dynamics and asymmetries in volatility of Bitcoin and examining the scope of similarity to currencies and investment tools. Based on the results we can conclude about the potential of Bitcoin to serve as a currency in a wider scope.

Rest of the paper is structured as follows, chapter 2 describes Bitcoin and its role in finance from the theoretical perspective, chapter 3 elaborates on the blockchain technology, chapter 4 sums up the methodology, chapter 5 describes the data, results are presented in chapter 6 and chapter 7 concludes.

2 Bitcoin properties

Bitcoin is an innovative digital currency not backed up by any commodity or trusted central authority. Transactions are handled through a peer-to-peer network, and verified using cryptography (Grinberg, 2011). The concept of anonymous electronic money (e-cash) has been broadly discussed by many academic authors since early 1980s, yet none of e-cash schemes came into life (Barber et. al, 2012). Although Bitcoin does not directly build on years of research made on e-cash, it has already become a worldwide discussed phenomenon since its introduction in 2008, despite its numerous opponents who believe it has a disruptive potential. Need for a trusted central authority to verify every transaction against double-spending leads to high transaction costs in current payment system, which makes it largely inefficient (Nakamoto, 2008).

2.1 Origination

Growing importance and amount of electronic transactions since the end of 20th century has led to increasing interest in electronic payment systems. Satoshi Nakamoto (2008) published a paper, describing an alternative payment network working on peer-to-peer basis: Bitcoin, whose goal was to reduce transaction costs for e-payments. Transactions made in the Bitcoin network are grouped together into blocks, and those blocks are ordered to form a chronological chain. Such a chain of all previously made transaction is called “blockchain”. When users request to make new transactions; the requests are broadcasted to all nodes in the system, which group them into a block, and work on finding a proof-of-work. Proof-of-work is necessary for the transactions to be processed. Once it is found, the block is broadcasted to all nodes, and they accept it, only if none of the transactions has already been spent. Creating a public ledger containing all past transactions, and incentivizing users to oversee correctness of transactions, effectively solves the double-spending problem.

Function of nodes is served by “Bitcoin miners”, users who work on finding a proof-of-work, which is solution to a complex mathematical puzzle. Miners are incentivized by a reward granted for finding the proof-of-work; currently it is 25 BTC and the amount is decreased by 50% with every 210.000 blocks created. Thus opposed to traditional monetary systems, nodes only have the function of overseeing transaction validity. Central institution, in addition to that, also looks after the overall economic environment, and makes effort to keep it stable. Variety of tools is used to achieve this objective, very often money supply manipulation. Nothing like that is possible for Bitcoin, as the money supply evolves in a predetermined way. The total number of Bitcoins to be generated is 21.000.000, and as of now there is about 15.000.000 BTC in circulation. After the last Bitcoin is mined, payers will have to include transaction fees, to incentivize nodes. Hence, transaction costs will increase, but they should still be negligible compared to traditional monetary system.

2.2 Brief history

First block, so-called “genesis block”, was mined in January 3, 2009. About two months earlier, a programmer or group of programmers under pseudonym Satoshi Nakamoto[1] published a paper introducing Bitcoin. For a couple of months Bitcoin’s development has been completely separated from the real economic world. First connection with actual economics took place in October 2009, when Bitcoin was assigned an exchange rate with US Dollar (1 USD = 1309 BTC)[2]. Next step in bringing Bitcoin closer to the real world was creating a Bitcoin/fiat currencies exchange. Dwdollar established such an exchange in February 2010. Convergence to the real world went further in May 2010, when the first real-world transaction settled with Bitcoins took place. A pizza was bought for 10.000 BTC, equivalent of around 25 USD back then. In terms of today’s exchange rate, the pizza would cost around 4.000.000 USD[3].

Bitcoin was still believed to be a short-lived entertainment of geeks. Value against USD was still negligible, although it increased tenfold during a single week in July 2010. Increasing number of new users resulted in emergence of new Bitcoin exchanges, amongst them MtGox Bitcoin currency exchange, scene of unfortunate events in the future. Period of rising trust was interrupted by a successful hacking attempt. A loophole in the system was discovered and 180 billion were Bitcoins

[1] Identity of Satoshi Nakamoto has never been revealed. In May 2016 Australian businessman Craig Steven Wright published an article claiming he can prove he is Mr. Nakamoto. Proofs were already presented, however IT, Bitcoin and other specialists have not reached consensus on whether Mr. Wright and Mr. Nakamoto are a single person (Economist, 2015)

[2] The exchange rate was result of a mathematical formula expressing expensiveness of Bitcoin mining (electricity, computing power, etc.)

[3] http://thenextweb.com/insider/2015/03/29/a-brief-history-of-bitcoin-and-where-its-going-next/#gref

fraudulently generated. All previously gained trust was lost and exchange rate dropped sharply[4]. Not much later Bitcoin also gained attention of national governments. The Financial Action Task Force (FATF) published a report, stating that anonymity of Bitcoin makes it an ideal currency for illegal trades or money laundering, which started pursuit for its regulation.

Legitimacy of this report was later confirmed, when operations of Silk Road were discovered. Established in 2011, the site served as a marketplace for drugs, and used Bitcoin as an untraceable means of payment. Emergence of Silk Road might have helped the development of Bitcoin, as it increased volume of transactions. Therefore on February 9, 2011, Bitcoin reached parity with USD for the first time. Rapid value growth caused by wider recognition of Bitcoin, along with increasing demand for alternative currencies after global financial crisis, led to an inevitable creation of first bubble, that burst in mid 2011.

Rising price has motivated hackers to steal Bitcoins; an admin account at MtGox exchange was attacked in June 2011, which left the hackers with the user table containing personal details and password hashes to 60.000 accounts. Hackers used these data to make fraudulent transaction, forcing MtGox to shut down for a week, and causing a major breakdown of exchange rate (back to 0.01 USD). Users of MyBitcoin exchange using same usernames as on MtGox had their Bitcoins attacked too. Other Bitcoin exchanges, although they were not attacked, postponed trading until security was restored.

MtGox eventually filed for bankruptcy in 2014 and was liquidated later that year[5]. Representatives of MtGox claimed Bitcoins disappeared due to a bug in Bitcoin system, but there have also been rumors of misappropriation. Either way, only part of missing Bitcoins was returned to customers of MtGox. Despite frequent events of thefts and frauds, Bitcoin is still heavily demanded by the end of 2015, currently trading around 420 USD (December 29, 2015). It is not any more used only for speculation purposes; nowadays it is applicable also as a medium of exchange. Many legal *offline* businesses adopted Bitcoin as an official means of payment. It is presently accepted in hotels, restaurants, bars, etc. However it still remains a handy speculation tool, as it is subject to enormous bubbles. Largest bubble peaked in

[4] http://historyofbitcoin.org/

[5] https://en.bitcoin.it/wiki/Mtgox

November 2013 with price of 1242 USD per BTC, almost 10 times the price of October.

2.3 Classification

So far, we have described Bitcoin as a type of currency; however, its true nature is a subject to an ongoing debate. Plenty of academics have elaborated on this topic, but there is no consensus yet. Some see Bitcoin as a currency, others as a security, commodity, or just a good. Classification of Bitcoin is not only important for purposes of our research itself; it also determines how it will be approached with respect to regulation and taxation. Grinberg (2011) examines this question from the legal perspective. He argues Bitcoin does not fulfill definition of security in a narrow sense; nevertheless, it may satisfy a broader definition of security[6].

Profits gained by holding Bitcoins are derived in other way than usual for securities. Securities derive profit based on gains made by another entity, while Bitcoin based on its appreciation against denominated currency. Hence, it may be argued Bitcoin is rather a commodity. However Bitcoin lacks features that are usually said to differentiate a commodity from security; it is not tangible, nor has inherent value. More precise definition is, that Bitcoin is a money-like informational commodity (Bergstra & Weijland, 2014). It is argued there, Bitcoin cannot be classified as a currency (either as cryptocurrency, digital currency, informational money, etc.), because it lacks wider acceptance. When Bitcoin gets a wider recognition, it may be defined as a cryptocurrency, it is admitted.

Economic analysis of Bitcoin in Mittal (2012) concludes Bitcoin hardly fulfills "conventional or constitutional" definition of money. Bitcoin's speculative nature prevents it from functioning as a medium of exchange; high value against USD makes it difficult to use Bitcoin as a unit of account, and high volatility makes it more of a speculative commodity (Mittal, 2012). Currency-like features are also denied in Yermack (2013), who claims Bitcoin must overcome high volatility and difficulty to be hedged against currency risk, in order to classify as currency. Novelty of Mittal's paper lies in a proposition, that definitions of money are only conventions established after money was created. By this logic Bitcoin might be a currency, just one economics does not have a classification for yet.

[6] "The Supreme court has interpreted something to be … a security, if it is a "contract, transaction or scheme, whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party"

Some automatically assumed Bitcoin to be a currency, and tried to sort it into some class of monies (Selgin, 2013). Then it is clearly not a fiat currency, as it value is not "created by oversight of trusted central institution", but it cannot be either a commodity currency in a classical point of view, because it has no intrinsic value. Like commodities, Bitcoin is scarce; hence, Selgin (2013) categorizes Bitcoin as a synthetic commodity currency. Doguet (2013) even finds a legal definition of currency suitable for Bitcoin, stated in The Stamp Payment Act of 1962[7].

Apparently, academics have not found a consensus, as to whether Bitcoin is a security, commodity or a currency. Courts possess the deciding power in this matter anyway. European Court of Justice (ECJ) has been deciding if proceedings from Bitcoin exchanges should be subject to VAT, based on a request made by Sweden in 2014[8]. ECJ ruled Bitcoin should be exempt from VAT; hence, saw Bitcoin as a medium of exchange and not a commodity.

One of the biggest markets for Bitcoins is the USA. Therefore, the stance of its courts and politicians is very important for future of digital currencies. The largest Bitcoin related trial was Securities and Exchange Commission (SEC) versus Trendon Shavers[9]. Shavers was accused of running a Bitcoin based Ponzi Scheme, and fraudulently acquiring 700.000 BTC. He defended himself by claiming Bitcoin is not money; thus, he cannot be prosecuted under existing laws. The court did not find Bitcoin to be "currency under the Bank Secrecy Act, as it is not a legal tender", but stated Bitcoin is a form of money from legal point of view, as it is used as a means of payment. Nevertheless, in 2015 the Commodity Futures Trading Commission (CTFC) decided Bitcoin is a commodity, and ordered to shut down a page offering options with Bitcoin as an underlying asset[10].

Somewhat more curious was the approach Thailand selected. Their courts ruled Bitcoin is not a currency, and after Bitcoin Co. Ltd tried to legitimize Bitcoin,

[7]" Whoever makes, issues, circulates, or pays out any note, check, memorandum, token, or other obligation for a less sum than $1, intended to circulate as money or to be received or used in lieu of lawful money of the United States, shall be fined under this title or imprisoned not more than six months, or both"

[8] http://www.coindesk.com/europe-inches-towards-decision-Bitcoin-vat/

[9]http://www.coindesk.com/sec-charges-texan-man-for-defrauding-investors-in-Bitcoin-ponzi-scheme/

[10] http://www.coindesk.com/cftc-ruling-defines-Bitcoin-and-digital-currencies-as-commodities/

Thailand decided to ban it entirely due to lack of existing laws and capital controls[11]. Apparently various approaches exist to asses trading with Bitcoin. There are extreme approaches, where countries prosecute traders exchanging Bitcoin for foreign currency or merchants denominating their prices in BTC (Thailand, Russia), while other countries apply strict regulation (Brasil). Friendlier approaches are more common, many countries have not imposed any regulation yet (Belgium, Greece), some only released statements that trading with Bitcoin is not backed by the state, and might be risky (India, Cyprus). In Germany Bitcoin was recognized as a unit of account in a similar manner as foreign currencies, some countries see it as an alternative form of money (Canada, Estonia), lastly there is a group of countries that recognize Bitcoin as a good for legal and taxation purposes (Australia, Argentina, Singapore)[12].

Countries will want to figure out what Bitcoin means for their economies, and how to treat it in the future. When most of them do so, there will probably be an effort to harmonize regulations imposed on Bitcoin. With many different approaches, it will not be an easy task for governments to find a mutual approach. At present time it is hard to tell, if Bitcoin will profit from or be harmed by the process of unification.

2.4 Relevant literature

Mainly flaws and possible problems are pointed out during the beginning period of Bitcoin life, the period of little awareness and acceptance. Many implied Bitcoin’s anonymity would be a considerable threat (Grinberg, 2011; Kaplanov, 2012; Brezo & Bringas, 2012), as it makes Bitcoin a great tool to settle illegal transactions.

Slowly increasing acceptance and importance of Bitcoin is admitted by Brezo & Bringas (2012). They also pointed out Bitcoin was only in the beginning stage; thus, it should happen to be a more important economic phenomenon in the future. Main problems of Bitcoin are seen in its speculative nature, but more importantly in its high suitability for illicit transactions. Besides above mentioned anonymity that promotes money laundering and illegal trades, Bitcoin economy is claimed to

[11] http://www.theverge.com/2013/7/29/4569126/Bitcoin-tries-to-become-legal-currency-in-thailand-gets-outlawed

[12] An overview of regulations and laws imposed on Bitcoin by individual countries can be found at:

http://www.loc.gov/law/help/Bitcoin-survey/

“behave as a barter economy” (Brezo & Bringas,2012). Therefore it might be difficult to determine precise prices of transactions, which might lead to cases of tax evasion and frauds. Moreover, Bitcoin could suffer by traceability of transactions to some extent, or proneness to get caught in a deflationary spiral due to limited money supply (Grinberg, 2011).

Others questioned functioning of the whole system, and proposed improvements (Barber et. al, 2012). There was not much faith, Bitcoin should be widely used in the future, Gürring & Grigg (2011) did not find it useful even for speculation purposes, and there were even voices Bitcoin is just another Ponzi scheme (Ou, 2011). Sceptic voices carried on into the period of rising awareness and acceptance. As they stated, Bitcoin was a hastily created attempt of electronic money deemed to collapse at a certain point, or even a return to medieval forms of trade (Hanley, 2013). Quote of an experienced banker is added to support this claim: “ *[Bitcoin is]…a very clever practical joke by someone who is having enormous fun exposing in the most sophisticated way imaginable the naivety of clever mathematicians, economists and/or rich speculators. ... or ... The cleverest con trick ever conceived, and probably one of the most rewarding.”* (Gardiner in Hanley, 2013)

On the contrary, Šurda (2012) suggested Bitcoin satisfies Austrian definition of money, and empirically verified it serves as a medium of exchange, while others assumed it could become a significant player in e-commerce (Martins & Yang, 2011), or specifically in computer game commerce (Grinberg, 2011). In accordance to that, Krištoufek (2015) made an argument against a purely speculative nature of Bitcoin, stated by Bouoiyour (2015), or Gomez-Gonzalez & Parra-Polania (2014). He analysed the process of Bitcoin price determination, and found price is driven by usage in trade, price level and money supply. This is in line with monetary theories about currency price formation.

Schlichter (2012) claims contemporary paper money system is not sustainable, and banks are deemed to collapse on a large scale. Place for a whole new system will arise when that happens. Schlichter (2012) suggested Bitcoin would be one of the candidates to take over the function of fiat money, along with precious metals. A little more modest evaluation is provided by Jansen (2012). He evaluates the nature of Bitcoin, and reveals its functional similarity with cash and money. He concludes Bitcoin does have attributes of “identifier to money - cash - rather than contemporary money itself”. From this point of view, Bitcoin should be seen as evidence; it is possible to create currencies functioning without the oversight of banks. Similar belief is expressed in Economist[13]. It is stressed there that the truly revolutionary element brought by Bitcoin is blockchain, and it could alter the way current economy works.

Doguet (2013) believes Bitcoin could become an important means of payment for certain parts of the economy, if it was to overcome certain shortcomings. Specifically loss of trust caused by infrequent thefts or misappropriation, but more importantly severe price volatility dissuading merchants from accepting it, and users from holding it. Possibility of Bitcoin being widely accepted is admitted by Yermack (2013), but at the time his paper was written, enormous volatility and impossibility to hedge against currency risk were preventing it. Bitcoin could fail, even if widespread faith in cryptocurrencies is established. Bornholdt & Sneppen (2014) developed an empirical model studying cryptocurrencies, and point out possible domination of Bitcoin by another cryptocurrency, as it holds no advantage over them according to their model.

Bitcoin's life has still been quite short, so the literature is rather scarce. But overall, there are papers assessing the future of Bitcoin mostly from the theoretical point of view. Apart of the majority of critical and skeptical voices, there exist some authors seeing usefulness of Bitcoin and its longer-term survival, even as a currency (Schlichter, 2012) or at least smaller scale medium of exchange (Grinberg, 2011; Martins & Yang, 2011).

2.5 Threats

The fact that Bitcoin still exists; is used as a means of payment; held by the users, and accepted by merchants by the end of 2015 can be deemed a success. Especially, when we take into account numerous problems it had to overcome. Firstly distrust of society due to novel and peculiar design of the whole Bitcoin project. Timing was perfect in this matter, as people were willing to try payment systems alternative to the current one, after it was roughly hit by global financial crisis. Bitcoin has already gained attention (and trust to some extent) of the public; thus, it is relevant to elaborate on drawbacks that could threaten its role as a currency in the future. Monetary systems, where money has no intrinsic value, are based solely on trust. Trust that money obtained today will also be accepted tomorrow. Banks promote this kind of trust in traditional monetary system, along with ensuring all parties "play by

[13] http://www.economist.com/news/leaders/21677198-technology-behind-Bitcoin-could-transform-how-economy-works-trust-machine

the rules”. Bitcoin system has no such central authority; hence, trust is an extremely fragile commodity there.

Events that undermine trust in Bitcoin are threatening its functioning as a currency, and functioning of the system as a whole. Loss of trust naturally damages the market value of any good or commodity, but with currency, the collapse happens as a self-fulfilling prophecy, and can be very rapid, even after a seemingly insignificant incident. During its life Bitcoin has already experienced events with disruptive potential for a new and unverified currency. Mainly they were flaws in the software. Users having their money generated, managed, and transactions processed by a software, do not like to see there are loopholes in it. Such a loophole was discovered in August 2010, and 180 billion Bitcoins were falsely generated[14]. Bigger problem than these software errors is the doubt they put in heads of Bitcoin users. After this event in August 2010 Bitcoin’s price against USD dropped sharply and the network lost a lot of current users. That time Bitcoin was still in early stages of its life with small number of users; thus, the damage was not fatal.

Another vulnerability lies somewhat outside its network. Majority of users have their Bitcoins stored with Bitcoin exchanges. Quite frequently it has happened, that they disappeared, whether they got stolen by hackers or somehow misappropriated by managers. In a period from 2010 to 2013, there were 40 Bitcoin exchanges opened, and 18 of them “have subsequently closed”, with a median exchange life 381 days (Moore & Christin, 2013). Those figures give us a 45% failure rate. Usual businesses also get closed often, simply because they cannot compete with other market participants, but that is not the case here. Even some of the largest exchanges ceased their services. Most famous is the story of MtGox, which was hacked in 2011; personal data and passwords were stolen and used to make fraudulent transactions. After shutting down for a week, the exchange continued its service only to discover in 2013, that majority of Bitcoins stored on their exchange “went missing”.

Collapse of MtGox was eventually also caused by a flaw in Bitcoin protocol, known as “transaction malleability”. Due to transaction malleability an ID of a transaction can be changed without sender’s knowledge. No harm is made to the transaction, but it does not appear under the original ID in sender’s overview; hence, the sender may deem the transaction not completed and resend the funds[15]. Malleability should not be

[14] http://thenextweb.com/insider/2015/03/29/a-brief-history-of-bitcoin-and-where-its-going-next/#gref

[15] https://www.theguardian.com/technology/2014/feb/27/how-does-a-bug-in-bitcoin-lead-to-mtgoxs-collapse

a real problem for well-managed and secured exchanges. Sloppy management, especially from the CEO Mark Karpelles is believed to really have brought MtGox down.

Vague management is not the most serious of denunciations Karpelles faces; some believe he used Bitcoins of his customers to enrich himself, or to cover liabilities of his company. More important than how exactly those Bitcoins disappeared, is what the collapse meant for world of Bitcoin. When the shortage of funds in MtGox leaked out in February 2014, Bitcoin has already established decent reputation and popularity. If most Bitcoin holders would suddenly start questioning, whether their Bitcoins are safe on other exchanges, and start converting Bitcoin into dollars wildly; the price would drastically decrease, and the whole Bitcoin network could collapse. Surprisingly events did not follow this scenario. Price indeed decreased, by 22% from 581 USD to 437 USD in 24 hours, but it cannot be considered so drastic a movement, if we consider magnitude of the situation and Bitcoin’s usual volatility. Nevertheless, potential collapse of other significant Bitcoin exchanges could lead to loss of trust in Bitcoin network and eventually collapse of the whole system.

Equivalently dangerous as events that crush faith in the network, and drive the price down, might be an ongoing upward price movement, so-called deflationary spiral. When the price level drops in classical monetary system, and consumers expect further decreases of the price level; they lower consumption, because they know their money will have greater purchasing power in the future. Decreased demand causes lowering of prices, which makes consumers even less willing to spend. Thereby the deflationary spiral gets started, and it is very difficult to reverse. Deflationary pressures on Bitcoin are not coming from the demand side. Its appreciation would be driven by limited money supply. If it is to ever become a medium of exchange accepted in a large scope; it will have to appreciate significantly, so that it generates enough value for all intended transactions. Such period of appreciation could lead to start of above explained deflationary spiral, or as ongoing appreciation over the sustainable level is called in stock markets, a bubble. After the price skyrockets to unsustainable levels the bubble will burst. The price fall could potentially be hard enough to destroy faith in Bitcoin once for all.

Furthermore, Bitcoin is threatened by regulatory interventions, as some countries have already banned trading with it, and denominating prices in it. Another threat is, being dominated by a competing and possibly better designed cryptocurrency. It shall be noted, that most of the above described threats are dangerous also for the classical monetary system, starting with loss of trust, and self-fulfilling collapse of the system (e.g. bank runs), and ending with deflationary spirals (e.g. case of Japan).

3 Blockchain

Reviewing the literature assessing Bitcoin from various angles gives us a clear sign; its contribution lies beyond its currency-like features. Academics reach no consensus as to whether Bitcoin can be considered a currency, or even a sustainable financial scheme; however, majority of them would agree that blockchain is a technology that could change ways of information processing for many institutions. It basically brings a way to verify truthfulness of information without need for trusted central party.

3.1 How it works

The role of a central institution in financial system is to protect the payee against double-spending. If all transactions are publicly or semi-publicly recorded, and there is a heterogeneous group incentivized to verify new transactions, double-spending is improbable. Blockchain is effectively a ledger containing all transaction, since the genesis block was created. Anonymity is ensured via hashes that make information about a transaction publicly displayable, but encrypt identities of individual parties involved. Each Bitcoin holder possesses a public key and a private key to his account. Public keys of both payer and payee are displayed in the blockchain. That way it can be validated, if the sender of Bitcoins has a sufficient amount in his account. To complete a transaction one also needs to provide the private key, corresponding to the particular public key. Hash algorithm is extremely difficult to reverse, i.e. recreate the original data from the hash value, which is crucial to prevent frauds and preserve anonymity.

Blockchain would not work, if anyone could edit it at any time. Proof-of-work ensures blockchain is not editable by anyone, but the user who succeeds to solve it. Proof-of-work is a solution to a complex computational puzzle. These users who invest effort into finding the proof-of-work are called “miners”. Incentive for miners is a reward they get for finding the proof-of-work. Nowadays the reward is a certain amount of BTC, which will decrease with every 210.000 blocks until all Bitcoins are in circulation. After that, miners will be incentivized by transaction fees added by individual payees. Anyone is welcome to become a node in the Bitcoin blockchain; however, nowadays the probability of finding the proof-of-work when working alone is negligible. Miners work on finding the proof-of-work by the “trial and error” method, usually using powerful computers. Due to low probability of finding the proof-of-work individually, miners associate themselves into groups called mining pools.

Each transaction begins with a user of Bitcoin broadcasting his intention to complete a transaction to all nodes. From the received requests, nodes form cornerstones of the blockchain: transaction blocks. Once transactions have been broadcasted to nodes, they start searching for the proof-of-work, and one of them eventually finds it, whereby proof-of-work difficulty is adjusted to sustain constant Bitcoin generation pace[16]. When the proof-of-work is found, the block is broadcasted to all nodes, who examine, if none of transaction contained has already been spent. When nodes recognize all transactions as valid, they confirm authenticity of the block by adding its hash to the next block created. By iterative addition of blocks, the blockchain is formed.

Clearly, as all previously made transactions are contained in the blockchain, payees are protected against double spending. Problems could arise if a node or a group of nodes would be able to control the decision making, or alter already built parts of the blockchain. If the decision making was based on one-IP-address-one-vote, blockchain could be subject to attacks from anyone able to accommodate many IP addresses (Nakamoto, 2008). One-CPU-one-vote basis which proof-of-work is based on preserves honest decision making, as long as majority of nodes are honest. In case there exist conflicting chains, nodes always consider the longest one to be correct, and keep working on extending it. Hence, if an attacker wants to modify an already built-in block, he would have to redo its proof-of-work, then proof-of-work of all blocks after it, and then outpace the honest nodes in extending the chain. Such an event is not impossible; however, the probability of such an event happening is very tiny[17]. Since the probability is not in favor of an attacker, attack of such type would be very impractical, given the gains in case of success are limited. Successful attacker would not be able to fraudulently generate new coins; he could only erase transactions in the given block; hence, effectively get back Bitcoins he already spent.

[16] "Difficulty is determined by a moving average targeting average number of blocks per hour" (Nakamoto, 2008). The target xorresponds to roughly one block in 10 minutes.

[17] See appendix A for details.

Considering a very low probability of success and limited gain, such an attack is very unlikely even to be attempted[18].

3.2 Loopholes

Situation would be different, if a group of miners would be able to acquire more than 50 percent of Bitcoin network capacity. Then it would be possible for such a group to change past blocks, and probable it outpaces the honest nodes in creating the longest chain. Event of such a nature is called the “51% attack”. It may seem like acquiring 51 percent of hashing power is almost impossible; however, in June 2014 a mining pool GHash.IO reportedly exceeded the 51 percent mark. Although it has attracted attention of Bitcoin users, there has been no registered double spending incident. On the contrary, GHash.IO voluntarily declared it will try to keep its share of hashing power below 40 percent[19]. Even with 51 percent of the hashing power, incentives to attack the blockchain are conflicting. Changing blocks, to enable double-spending might bring excessive profits in the short run. But such fraudulent behavior would eventually be revealed, and would very likely destroy trust in Bitcoin, and crash down its price. For a mining pool possessing majority of hashing power, which means they also mine majority of Bitcoins, the long run loss from price breakdown surely exceeds the gain from short-term ability to double-spend.

More recent threat comes along with regular functioning of blockchain. There is a way to discourage Bitcoin users without necessarily stealing anyone’s funds, using so called “transaction malleability attack”. As already mentioned, the code behind Bitcoin is set up to adjust the difficulty of problems, so that a block is completed about every ten minutes, which results in creation of 144 blocks per day, while capacity of one block is limited to 1 Megabyte. Apparently number of transactions the network is able to cope with, is narrow in such a setting (about 4 per second, compared to 2500 VISA is able to make)[20]. Rapid rise in number of Bitcoin users could actually lead to breakdown of the system, because transaction processing would become too slow. Transaction malleability attacks are usually realized through a code transacting small amount of Bitcoins between two wallets over and over again;

[18] http://www.coindesk.com/51-attacks-real-threat-bitcoin/

[19] http://arstechnica.com/business/2014/07/bitcoin-pool-ghash-io-commits-to-40-hashrate-limit-after-its-51-breach/

[20] http://motherboard.vice.com/read/bitcoin-is-unsustainable

hence, flooding the blocks, and increasing time it takes for any transaction to be processed.

The obvious question here is why anyone makes an effort to attack anything, when he does not have a chance to profit from it. Transaction malleability attacks are probably organized by Bitcoins enemies with an intention to disrupt the system, or for demonstrative reasons. Such people could be bankers, politicians, ecologists, etc. In the days of heated debates about global warming, Bitcoin mining (hence, effectively also transactions completion) requires excessive amounts of electricity. According to Christopher Malmo, a single Bitcoin transaction consumes electricity equal to daily consumption of one and a half American households[21]. Such an amount is unsustainable, if Bitcoin shall become an alternative to fiat currencies, in which case the number of transactions would increase rapidly.

A natural way to decrease amount of electricity needed to complete a transaction is to increase maximum size of a block. As simple as this step may seem, it divided Bitcoin community like nothing has before. Opposition of block size increase fears, it could damage the most notable difference between Bitcoin and banking system – decentralization. They claim increase of block size would drive up amount of resources needed for mining; thus, force small mining pools out of the game. Therefore, block size increase would indirectly increase centralization of Bitcoin, and decrease egalitarianism[22]. Another problem for miners associated with block size increase is less incentive for users to attach transaction fees to intended transactions, as there will suddenly be lot of unused space in blocks.

Decentralization and libertarianism differentiating Bitcoin from other payment platforms, and standing behind its rise may now also lead to its fall. The reason is lack of decision making rules due to these attributes. In times, when decision on approach regarding block size increase must be made, disputes about decision making can be fatal. Success of malleability attacks and high demand on electricity per transaction show that a consensus on block size increase must be made, should Bitcoin see a considerable inflow of new users. Even the founder of Bitcoin, who set strict rules on total amount of Bitcoins generated or time between creation of new blocks, reportedly supported such a change in an e-mail sent to Mr. Hearn: "*A higher*

[21] http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020

[22] http://motherboard.vice.com/read/unless-everyone-using-bitcoin-makes-this-radical-change-the-currency-will-die

[block size] limit can be phased in once we have actual use closer to the limit and make sure it's working OK"[23]. Decentralization makes Bitcoin subject to political fights, and if their participants will not be able to find common approach, it can lead to its fall.

Before we move on to possible applications, it shall be noted blockchain used for Bitcoin is not flawless. Above mentioned flaws need not really pose problems for designs of blockchain adopted by individual institutions, but awareness of their presence is important.

3.3 Applications

We already know contribution of blockchain does not end with intermediation of financial payment systems. Blockchain could improve efficiency of all public ledgers, where verification of truthfulness is needed, or completion of contracts depends on certain conditions. It has overgrown its primary purpose, and now serves as a cornerstone of so called "smart contracts". Those are contracts, which are self-reinforced when certain conditions are met. They can be applied in a wide range of fields. Nowadays blockchain-based systems are being implemented by commercial banks, central banks, land registries or for purpose of crowdfunding. As already mentioned different uses require different specifications. Some distinctions are described in the following section.

Blockchain would not work without nodes serving as verifiers. Primary distinction of blockchain types is between permissionless and permissioned. Permissionless type presents the most liberal option, as anyone can serve as a node. On the other hand in the permissioned type, one must be allowed by a central authority to be able to serve as a node. Why would it sometimes be appropriate to have a tool for decentralization moderated by an authority which controls verifiers of contracts? The essential answer is scalability. The data are stored on every node's computer; hence, nodes with weaker computers start running out of computational power, when number of transactions increases. Such event leads to increase of centralization. For pre-selected nodes in permissioned type of blockchain, it is easier to accommodate sufficient computational power. Importantly the centralization taking place in permissioned blockchain is driven by a central authority, and does not occur according to "survival of the strongest".

[23] See 20.

Users may frequently not find partial traceability of information displayed in the blockchain not favorable[24]. When possible, users would pay the price of partial centralization for higher amount of privacy. Permissioned type of blockchain is usually built for private ledgers, where only a certain group of people or institutions can read and submit transactions (Peters & Panay, 2015). Cryptocurrencies like Bitcoin require to be run on a permissionless blockchain, because trust and transparency are essentially only drivers of its value. However, some applications by central banks or commercial banks would be served better by the permissioned type.

Efficiency in terms of government accounts management and timely availability of resources is one of the cornerstones for efficient functioning of a state. Pattanayak & Fainbom (2010) proposed “a unified structure of government bank accounts that gives a consolidated view of government cash resources”: a Treasury Single Account (TSA). TSA concept comprehensively unifies all government accounts, that way it is simple for an authorized ministry to oversee government cash inflows and outflows. Studies have shown potential of TSA to improve clarity of financing in emerging market countries, who suffer from government account fragmentation (Peters & Panay, 2015). An account allocating government incomes and expenditures is a perfect candidate to work efficiently under blockchain. Decentralization of TSA reduces the need for the trusted third party operating government accounts. Furthermore, in traditional TSA environment, commercial banks are often utilized for revenue collection and redistribution into TSA. Such a practice is both nontransparent and costly (Pessoa & Williams, 2013). Utilization of smart contracts would allow for government spending to simply and automatically follow transparent rules.

Accounting of commercial banks involves a complicated structure of different bills, and keeping track of such a complicated system naturally brings severe inefficiencies and costs. Implementing a blockchain, that could keep track of the whole complicated structure on its own, would be a breakthrough improvement for bank’s accounting. Engineering a blockchain like that is somewhat trickier than engineering one that records transactions chronologically and irreversably. After the global financial crisis in 2008 a new set of accounting rules (IFRS 9) was adopted, which adjusts accounting standards in terms of asset classification according to risk and loss provisioning. The complication here lies in possible missclassification of items in bank’s accounting. Irreversibility makes such mistakes difficult to correct.

[24] Information about tracing bitcoin transactions are available here:

http://time.com/3689359/bitcoins-track-anonymous/

Blockchain for commercial banks must be containing set of tests ensuring every item is classified properly.

Above mentioned irreversibility makes Bitcoin blockchain superior to other payment systems in terms of transaction fees, as there is no need for dispute mediation (Franco, 2014). Nevertheless it would be sometimes beneficial to modify blockchain, so that it can handle reverse modification of disputed transactions (Peters & Panay, 2015). Partial solution to this problem is a multisignature system, where an Escrow service acts as an intermidiary. Two of three signatures are then needed for the transaction to be completed. The whole process works as follows. Suppose agent B provides some good to agent A in exchange for a certain amount of funds, and agent M acts as an intermediary. Agent A deposits the funds at the multisignature adress, and three possible outcomes exist.

Agent A either receives the good; completes the transaction with his signature, and sends the funds to account of agent B, who adds his signature, and publishes the transaction. Secondly, in case agent B recognizes a problem preventing him from sending the good (either on his side or agent A’s side); he returns the funds to account of agent A providing his signature; agent A then adds his signature, and publishes the transaction on blockchain. The intermediating agent M comes into play in the last scenario. If there is a dispute between agents A and B, they pass their case to agent M, who decides whose position is rightful; passes the funds to whichever side he sees apropriate, providing his signature, and publishes the transaction on the blockchain. In the last case the intermediary agent would charge a percentage fee from the transaction (Peters & Panay, 2015; Buterin, 2014). Blockchain in this form loses its disintermediation feature, and transaction fees increase; however, it must be noted the intermediary party is not involved in the transaction, unless a dispute occurs.

Large number of parties involved disrupts also the process of financial assets trade settlement. Currently it takes 2 or 3 days to get purchase of financial assets settled, depending on a particular country of trade. Entrusting trade settlement into the hands of blockchain would automatize the whole process, which includes several steps connected to trade evaluation, risk management or payment confirmation. Transition to blockchain could shorten the lengthy process from days to minutes, and bring reduction in transaction costs by lowering the number of intermediaries necessary to complete the trade (Peters & Panay, 2015).

Financial sector is only one of many, whose processes are to be dramatically improved thanks to implementation of blockchain. It will take some time before proper modifications are found and engineered, in order to meet different needs of particular ledgers, but we already see occasional blockchain applications, and there will be more to come in the next years. Nasdaq uses blockchain for pre-IPO trading (Liebenau & Elaluf-Calderwood, 2016), Ripple developed a payment and exchange blockchain-based protocol for commercial banks (Allison, 2015), which 10 of 50 top banks are working with[25]. Ethereum[26], Hyperledger[27] or Balanc3[28] are other projects targeting widespread implementation of blockchain. Meanwhile VISA is developing a payment network running on blockchain (Liebenau & Elaluf-Calderwood, 2016), the health care industry also awaits blockchain implementation, as e.g. Phillips Healthcare confirmed, it is exploring its utilizability (Rizzo, 2015). All sumed up, the years to come will likely bring emergence of blockchain-based ledgers, that will change and simplify the way transaction and information are being processed, and contracts enforced.

[25] https://www.ripple.com/

[26] https://www.ethereum.org/

[27] https://www.hyperledger.org

[28] http://balanc3.net/

4 Methodology

Suitability as a store of value will be crucial for Bitcoin’s success among currencies, and consumers want their value stored in a stable instrument. We already mentioned, there were times of enormous bubbles and price drops in Bitcoin history. Periods of enormous volatility like that are not compatible with optimal store of value. But times are changing, and Bitcoin markets are getting more mature and competitive, as new users arrive, and flaws in the blockchain are being fixed. Hence, to examine potential of Bitcoin as an alternative to fiat currencies, we must look at the dynamics of volatility as the market evolves. Moreover, interconnection between Bitcoin and currency markets can be demonstrated by estimating volatility spillovers.

Estimation of volatility spillovers provides us information about similiraties between individual markets, we are interested in spillovers between currency and Bitcoin market, but it must also be accounted for influence of stock and commodity market. Diebold & Yilmaz (2009) propose a way to estimate volatility spillovers, which is based on Vector Auto-Regressive (VAR) model. The idea is based on ability to decompose VAR model forecast error variance to individual factors. Such a decomposition leaves us with own variance shares and cross-variance shares of error - spillovers. The methodology needed improvements, as it suffered from both methodological and functional drawbacks (Diebold & Yilmaz, 2010), namely influence of variable ordering or impossibility to measure directional spillovers.

Generalized VAR framework proposed by Koop et. al. (1996) and Pesaran & Shin (1998) is useful in this respect. The generalization allows shocks to be correlated, and uses historically observed errors distribution to account for them in a proper way, instead of using orthogonalized errors leading to dependence on ordering. Moreover, assets might not be responding the same way to extreme positive and extreme negative returns (volatility). According to the particular asset in question, there might be a stronger reaction to positive or negative volatility. To be able to measure such asymmetry, Baruník et al. (2015) used the concept of Realized Variance and Semivariance. For a period t containing n observations we have:

$$RV_t = \sum_{i=1}^{n} r_i^2$$

$$RS_t^- = \sum_{i=1}^{n} r_i^2 \, I_{r_i<0}$$

$$RS_t^+ = \sum_{i=1}^{n} r_i^2 \, I_{r_i>0}$$

where r_i is i-th realization of log return in day t.

Asymmetric spillovers are then measured by replacing the vector of realized variance by realized negative and then positive semivariance, and comparing magnitude of spillovers under each of them. If magnitudes are the same, then the response is symmetric. We cannot follow this method, because we do not possess high-frequency data for stock, currency and commodity markets.

As spillover estimation is only a side task of our research, we choose to employ the basic model developed by Diebold & Yilmaz (2008). We account for the possible influence of variable ordering by estimating the model for every possible order of variables and reporting the mean result for every i to j spillover. The cornerstone to the method developed by Diebold & Yilmaz (2008), is the 1-step ahead forecast error matrix $\varepsilon_{t+1,t} = A_0 u_{t+1} = \begin{pmatrix} a_{0,11} a_{0,12} \\ a_{0,21} a_{0,22} \end{pmatrix} \begin{pmatrix} u_{1,t+1} \\ u_{2,t+1} \end{pmatrix}$, the covariance matrix is $E\left(\varepsilon_{t+1,t} \grave{\varepsilon}_{t+1,t}\right) = A_0 \grave{A}_0$. Variance decomposition allows us to decompose the covariance matrix into parts attributable to individual shocks. Hence own variance shares can be defined as a_{ij}^2, where $i = j$, and cross variance shares – spillovers – where $i \neq j$.

Main task of this paper is examining the dynamics of Bitcoin volatility. In ideal econometric world, volatility of a time series is time invariant, and not a function of other variables. However, years of research have shown this is not the case for most financial assets. Volatility shocks persist for a certain amount of time for most of them. Hence, volatility at period t is dependent on lagged values of volatility at previous periods. Whether Bitcoin is considered a commodity, currency or simply an asset, volatility modelling should be based on models successful in predicting volatility of financial assets. Presence of heteroscedasticity and autoregressive features must be taken into account, when estimating and modelling volatility (Lamoureux & Lastrapes, 1990).

Volatility is subject to clustering, i.e. large volatility in a certain period drives large volatility in the subsequent periods. Length of such clusters determines if the process is deemed long-memory or short-memory. More accurately the speed at which autocorrelation function decays determines the classification. Pong et al. (2003) measured precision of long-memory and short-memory processes in forecasting exchange rate volatility, by performing out-of-sample forecasts. Their research shows no distinct difference between long and short memory models. Auto-Regressive Moving Average (ARMA, short-memory) and Auto-Regressive Fractionally Integrated Moving Average (ARFIMA, long-memory) models outperform GARCH forecasts, and also implied volatility forecasts using option prices. Best performing model always depends on the precise period and currency of interest (West & Cho, 1995)

Currencies are used as speculation tools less frequently than commodities or stocks; thus, the heteroscedastic effect should be weaker. Scott & Tucker (1988) still find evidence for time-varying variance in the data on currency options. It can be supposed also volatility of Bitcoin will display strong autoregressive features, similar to those shown by a more recent study for currencies (Fung & Patterson, 1998). Not only volatility is dependent on its lagged values; it is also negatively correlated with trading volume (Scott & Tucker, 1988; Fung & Patterson, 1998). The trading volume increases as the markets mature; hence, this relationship will also be tested in our research. Ex ante there is no reason to believe GARCH family models are a bad fit for volatility of Bitcoin returns, as heteroscedastic effects are found for both currencies and commodities (Choi & Hammoudeh, 2010).

Specificity of Bitcoin among other financial assets makes it harder to find the proper model for estimating volatility. Moreover, the literature does not reach a consensus regarding which model is the most efficient. Therefore, we will not rely on a single model; estimate different specifications of GARCH models; perform diagnostics, and elaborate on differences. The most popular model in financial applications is simple GARCH model. GARCH of order (1,1) is used the most often, it takes form:

$$a_t = \sigma_t \varepsilon_t$$

$$\sigma_t^2 = \omega + \alpha_1 a_{t-1}^2 + \beta_1 \sigma_{t-1}^2$$

Volatility often explores asymmetric response to positive and negative shocks that cannot captured by a simple GARCH model. EGARCH model, an extension to GARCH, enables to capture such asymmetry. It reads:

$$a_t = \sigma_t \varepsilon_t$$

$$\ln(\sigma_t^2) = \omega + \frac{1 + \alpha_1 L}{1 + \beta_1 L} g(\epsilon_{t-1})$$

$$g(\epsilon_t) = \theta \epsilon_t + \gamma(|\epsilon_t| - E|\epsilon_t|)$$

where ω>0, θ and γ are real constants and $E|\epsilon_t| = \sqrt{2/\pi}$ in case of standard Gaussian ϵ_t. The function $g(\epsilon_t)$ is a zero mean i.i.d. sequence and captures the asymmetric response of volatility to returns. It captures both sign and magnitude (Baruník, 2015).

A special case of a GARCH family model and a good starting point is an Exponentially Weighted Moving Average (EWMA).

$$\sigma_t^2 = (1 - \lambda)\, r_{t-1}^2 + \lambda\, \sigma_{t-1}^2$$

Recommended λ used in most financial applications is 0.94, however EWMA is a simplified IGARCH model with zero intercept; hence, λ can be easily estimated. Drawback of GARCH family models is they rely on a certain distribution of returns, usually standard Gaussian (Baruník, 2015). Heterogeneous Auto-Regressive (HAR) works with non-parametric estimate of variance, Realized Variance and Realized Positive and Negative Semivariance described earlier in this section. These estimates allow variance to be treated as observable, and are not based on distributional assumptions. HAR model assumes variance on a particular day to be driven by previous daily, weekly and monthly variance.

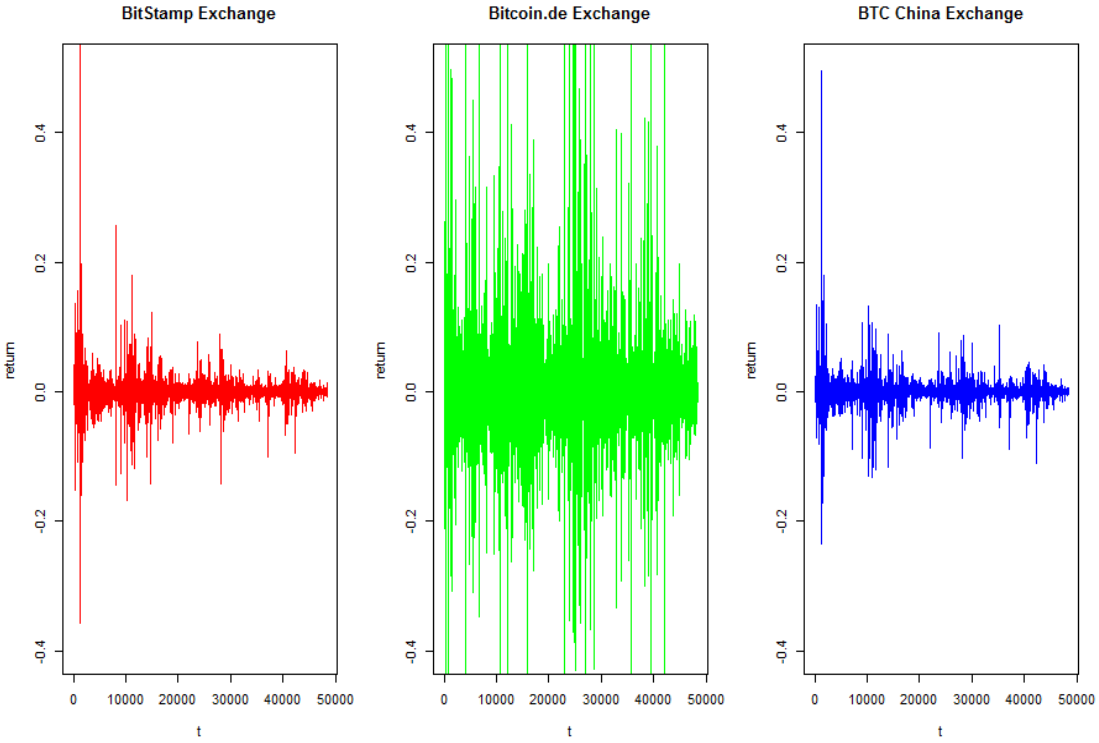
$$RV_t = \omega + \beta_1 RV_{t-1} + \beta_2 RV_{t-1}^{(7)} + \beta_3 RV_{t-1}^{(30)} + u_t$$

where $RV_{t-1}^{(7)}$ and $RV_{t-1}^{(30)}$ are weekly and monthly realized variances respectively. Normally 5 and 22 days are used to proxy a week and a month, but we can use 7 and 30 days, because unlike stock exchanges, Bitcoin exchanges do not close at the weekend, or on holidays. An error term u_t is supposed to be an independent identically distributed sequence. Another advantage of HAR model is that it lets us test for the leverage effect by inserting RS_{t-1}^{-} and RS_{t-1}^{+} instead of RV_{t-1}. Moreover, effect of trading volume can be easily tested by adding it to the model.

5 Data

Our dataset consist of two segments, the first is price (and returns) development on major Bitcoin exchanges, collected in high-frequency; the second daily returns from US currency, commodity and stock market. The examined period is quite short due to relatively short life of Bitcoin; moreover, at the early stages of its development it did not make sense to talk about price development of any kind, as trading volumes were extremely low. The dataset of high-frequency prices consists of Bitcoin prices against respective currencies from the most significant exchange (must have been operating through the whole period) in chosen markets (USA, Europe, China), recorded every 30 minutes. After deleting N/A observations, we ended up with 48 385 records of price and trading volume in BTC ranging over 1100 days from April 2013 until April 2016.

Figure 1: High-frequency returns from US (red), European (green) and Chinese (blue) Bitcoin exchanges



Returns are prioritized over prices for financial time series, as they mostly satisfy stationarity, and we do not need to care about accounting units. Difference in the graphs is obvious. Returns on the US and Chinese BTC exchange behave very similarly; they go through periods of moderate volatility and exhibit few clusters of higher volatility. Such volatility clustering is in line with econometric theories, according to which large (small) price changes drive (large) small price changes (Baruník, 2015). Behavior of returns on the European exchange is far less disciplined, the time series is extremely volatile. The reason follows in Figure 2.

Figure 2: Trading volumes on US (red), European (green) and Chinese (blue) Bitcoin exchanges

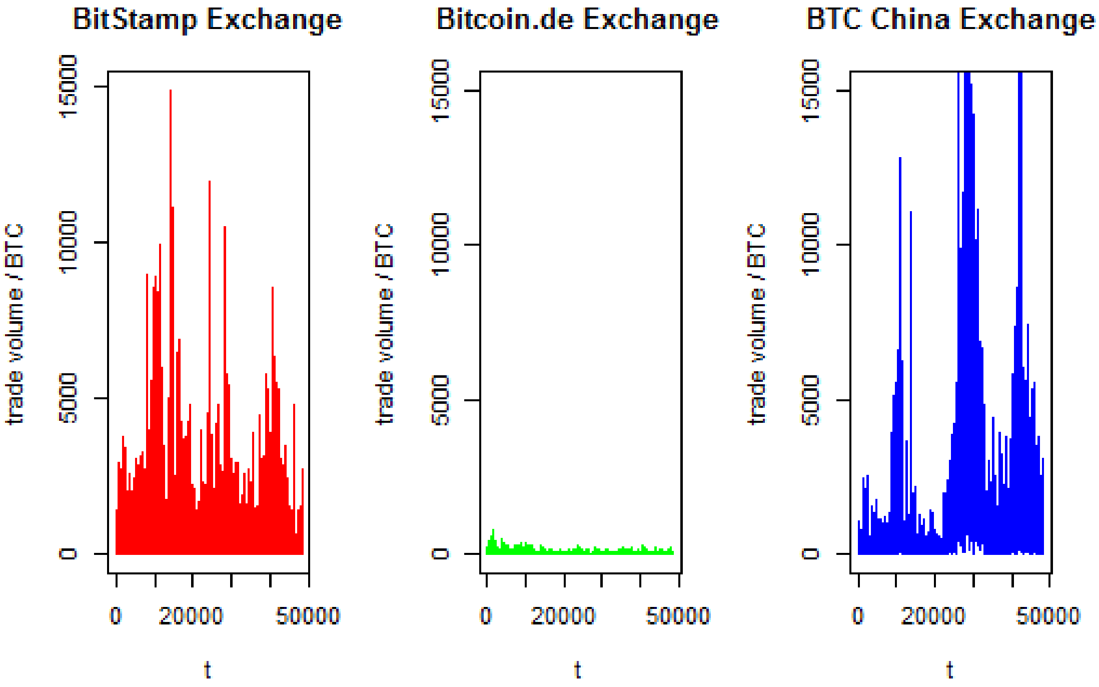
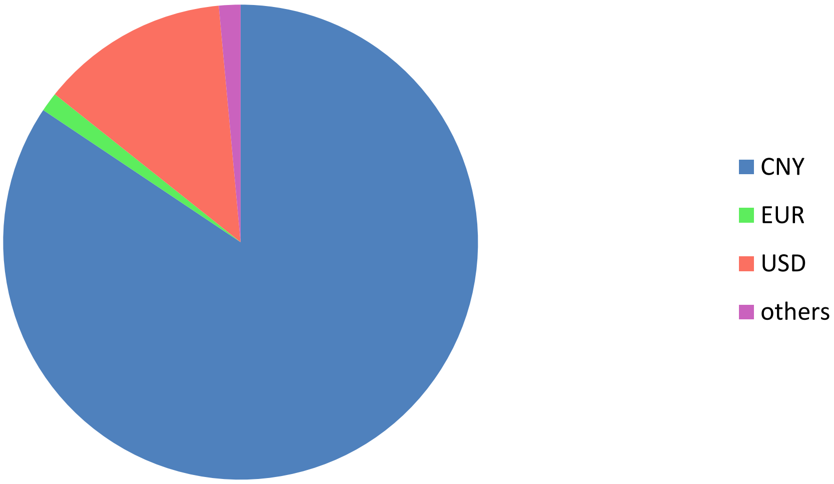


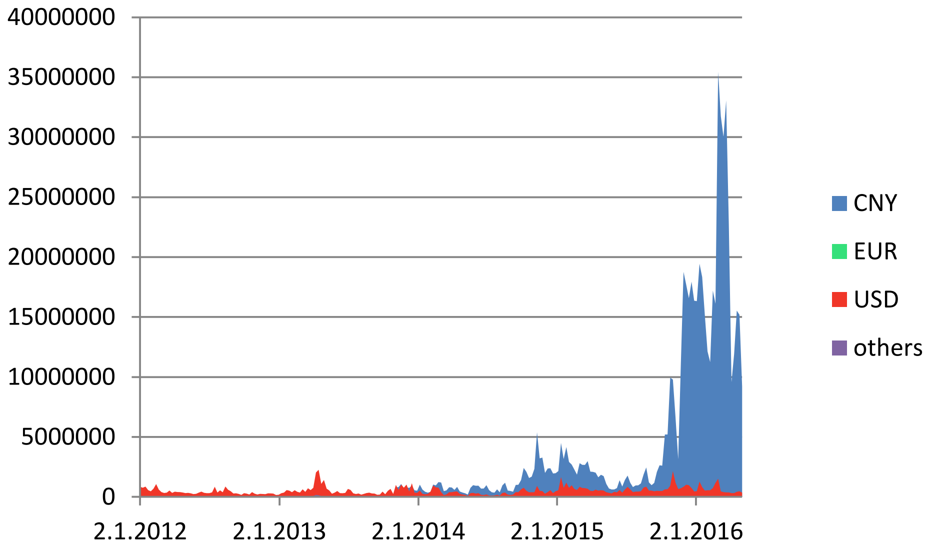
Figure 3: Trading volume according to currency of denomination



Source: http://data.bitcoinity.org/markets/volume/5y?c=c&r=week&t=a

Volume on the European market is negligible, and evidently not sufficient for the market to behave efficiently. This fact is not a result of wrong exchange being chosen, situation is similar on other exchanges. US Dollar (USD) and especially Chinese Yuan (CNY) denominated trades dominate Bitcoin markets, as shown in Figure 3. It depicts total trading volume since the start of 2013. Visibly EUR and other currencies have been inferior in Bitcoin trade, while only about 12% of trades were denominated int USD. It may seem examination of any other market, but Chinese, could be misleading. To make conclusions in that respect, we must first investigate what drives the domination of CNY denominated trades, and if it has been present for whole examinated period. Figure 4 presents the time evolution of trading volume in CNY, USD, EUR and other currencies.

Figure 4: Evolution of trade volume according to currency of denomination



Source: http://data.bitcoinity.org/markets/volume/5y?c=c&r=week&t=a

Clearly, we would make a mistake by excluding US market, as the phenomenon of CNY domination started shortly before the end of 2015. Until then, USD denominated trades displayed higher or comparable volume to CNY. There may be various reasons for such an odd behavior. Firstly, electricity in China is significantly cheaper than in USA, Japan or Europe[29], which makes it much more efficienct place for Bitcoin. The largest mining pools are indeed based in China[30]. This fact itself; however, does not explain the sudden jump since the end of 2015. The driver of the sudden jump might be depreciation of Chinese Yuan (Ranasinghe, 2015). After

[29] http://www.statista.com/statistics/477995/global-prices-of-electricity-by-select-country/

[30] https://en.bitcoin.it/wiki/Comparison_of_mining_pools

depreciation, and threat of other depreciation in early 2016; Chinese people started looking for another store of value, and switching to commodities. Besides gold and other tangible commodities, Chinese departed also to Bitcoin in a large scope[31]. This might be the first evidence of switching from currency to Bitcoin to maintain value.

Second branch of data are those needed to estimate volatility spillovers for US markets. We collected daily high and low prices from the start of 2013 till end of April 2016, for S&P 500 to proxy the stock market, Bloomberg Commodity Index for the commodity market, the New York Board of Trade US dollar index futures for foreign exchange market and BitStamp for US Bitcoin market. Daily variance is estimated as suggested by Parkinson (1980):

$$\tilde{\sigma}_{it}^2 = 0.361\left(ln(P_{it}^{max}) - \ln(P_{it}^{min})\right)^2$$

Annualized daily percent volatility is then estimated as follows:

$$\hat{\sigma}_{it} = 100\sqrt{365\tilde{\sigma}_{it}^2}$$

Summary of descriptive statistics is presented in *Table 17*, Appendix B. Most volatile is naturally the series of Bitcoin volatility. The first reason is Bitcoin’s volatility on its own, secondly proxies for the other 3 markets are already diversified indexes. Our interest is; however, which market contributes the most to Bitcoin volatility and which one gets the largest contribution from Bitcoin. Uncovering the interconnections between Bitcoin and the other markets will help us better understand similarities between stocks, currencies, commodities and Bitcoin. Notably, currency market volatility is also significantly positively skewed and leptokurtic compared to others, while commodity volatility is platykurtic.

Moreover, estimation of GARCH family models is based on daily returns from BitStamp, bitcoin.de and BTC China, constructed from daily closing prices for period January 1, 2013 to April 29, 2016. Descriptive statistics is presented in Table 16, Appendix B. Mean returns for every exchange are positive, most highly for BTC China. All exchanges are comparable in terms of standard deviation, and their return series are positively skewed. Furthermore, returns for all three exchanges are leptokurtic. Last two facts correspond to usually observed characteristics of financial series returns (Baruník, 2015).

[31] http://insidebitcoins.com/news/is-china-turning-to-bitcoin-as-yuan-devalues/35369

In addition we test for stationarity of BitStamp, bitcoin.de and BTC China daily returns using Augmented Dickey-Fuller test, and normality of returns using Jarque-Berra test. Non-stationar time series drives its own behavior, standard assumptions and testing are not valid, and they can be subject to spurious regression. The series contains a unit root under the null hypothesis. Non-stationarity is rejected for every exchange in the dataset. Normality is also rejected for all three exchanges, we must account for that when constructing GARCH models. Graphical depiction of annualized daily volatilies is presented in Figure 10. Commodity and foreign exchange volatilities behave very similarly according to the plot. On the other hand Bitcoin volatility displays resemblance to that of stock market; however, in much larger magnitude.

6 Results

6.1 EWMA model

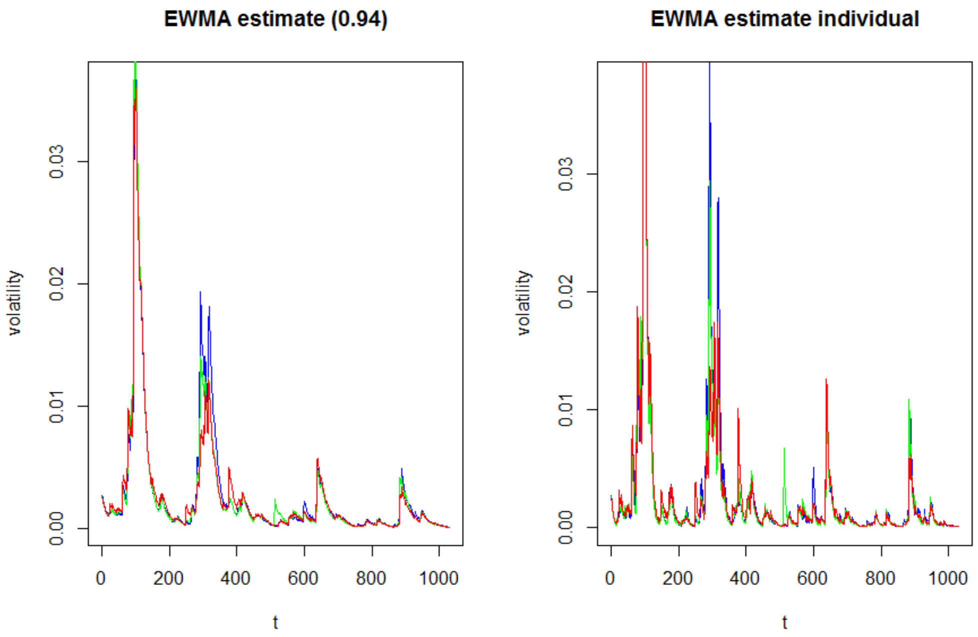
A first step in EWMA model estimation is determination of the λ parameter. There exist two ways of doing that, either estimating an IGARCH model without intercept, where β_1 corresponds to λ in EWMA, or taking an empirically verified λ. We will make the estimation using both approaches, and compare the results. For most financial applications $\lambda = 0.94$ is used.

Table 1: Estimates of λ produced by iGARCH

	Beta estimate
BitStamp	0.8395
Bitcoin.de	0.8150
BTC China	0.8149

Table 1 shows the amount of bias that would be caused by accepting the universal $\lambda = 0.94$. Graphical depiction of results is presented by Figure 5.

Figure 5: EWMA estimates of volatility, BTC China (blue), BitStamp (red), Bitcoin.de (green)



Magnitude of estimated volatility for all exchanges increases, along with frequency of fluctuations, if we use the estimated lambdas instead of the recommended 0.94. The trend of slightly decreasing and smoothing of volatility towards the end of examined period is; however, obvious on both graphs. Shortcomings of EWMA estimate are not taking into account the distribution of the data, and ignoring the long term unconditional volatility (Baruník, 2015).

6.2 GARCH family models

6.2.1 GARCH(1,1)

Modelling volatility using GARCH family models brings several advantages over EWMA. There are many different specifications allowing us to account for different characteristics of data. Secondly variance forecasts converge to unconditional variance as can be shown for GARCH(1,1) model.

$a_t = \sigma_t \epsilon_t$; hence, $a_t^2 = \sigma_t^2 \epsilon_t^2$ and, as $E(\epsilon_{t+1}|F_h) = 1$, the one step ahead forecast is:

$$\sigma_{h+1}^2 = \omega + (\alpha_1 + \beta_1)\sigma_h^2$$

$$\sigma_{h+2}^2 = \omega + (\alpha_1 + \beta_1)\sigma_{h+1}^2$$

$$\sigma_{h+l}^2 = \omega + (\alpha_1 + \beta_1)\sigma_{h+l}^2$$

$\sigma_{h+l}^2 = \frac{\omega}{1-\alpha_1-\beta_1}$, as l goes to infinity

As the null hypothesis of normality was rejected by the Jarque - Berra test, assuming normality of residuals seems susceptible. Usage of conditional Student's t-distribution of errors is discussed in Bolerslev (1985). Figure 6 shows Q-Q plots for conditionally normally and Student's t-distributed residuals. The results of estimating a GARCH(1,1) model as specified in the previous chapter, with conditional Student's t-distribution of errors, are presented in

Table ***2***. Notably sum of α_1 and β_1 is almost 1 for all exchanges. This implies the shocks die out only in a very slow pace, and persist in the process for a long time. GARCH model in the standard specification assumes stationarity of variance; however, the results suggest we should test the fit of IGARCH model allowing for unit roots in variance.

Figure 6: Q-Q plot of GARCH(1,1) residuals against quantiles of t-distribution and normal distribution, BitStamp exchange

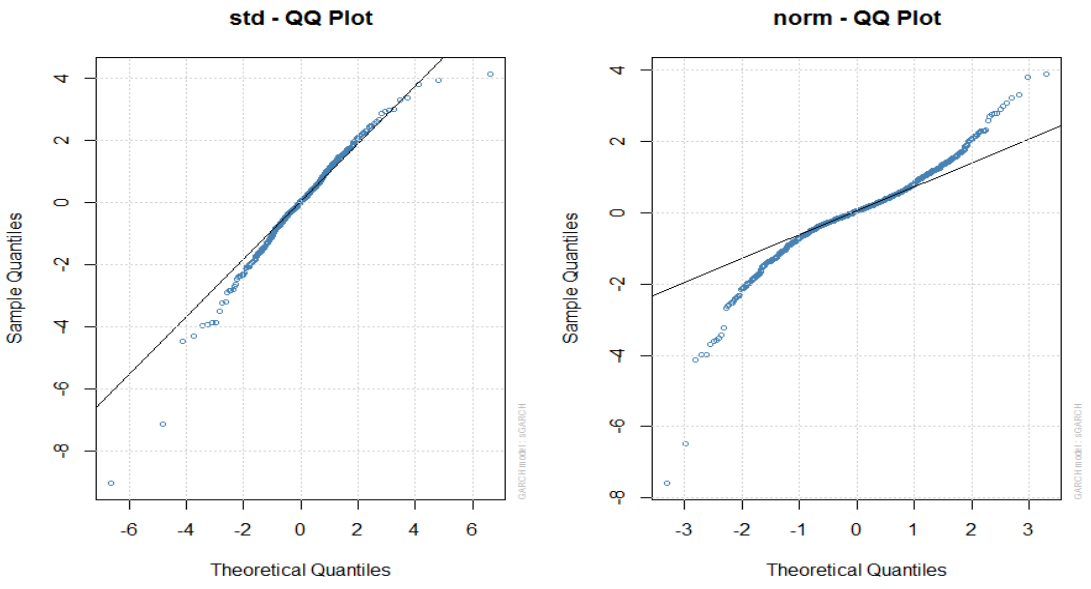


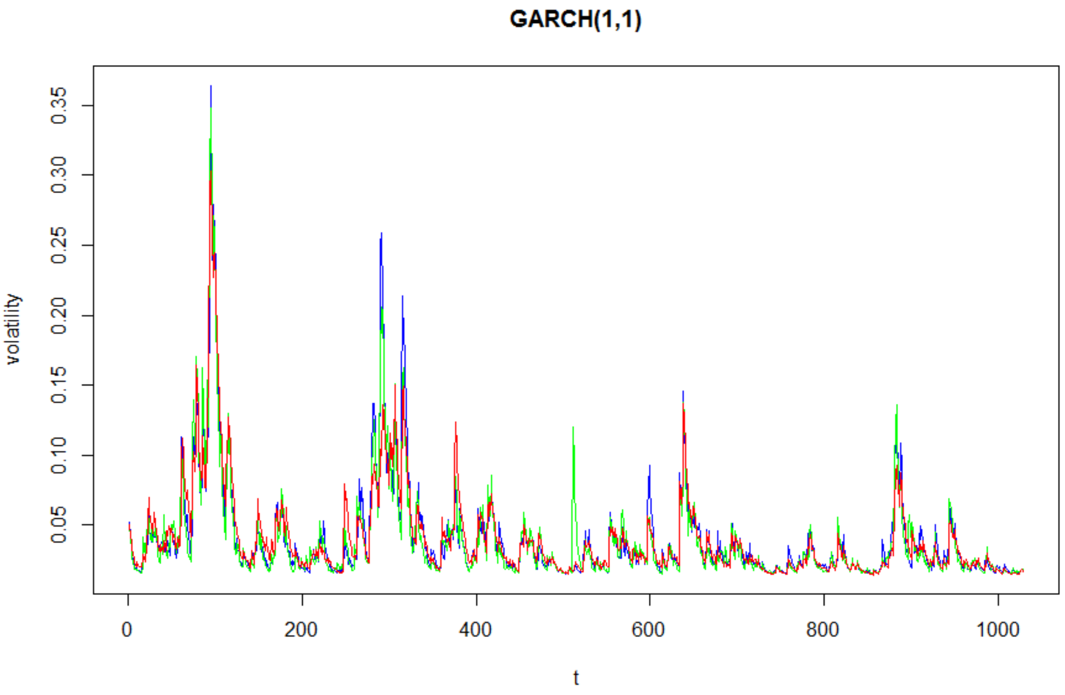
Table 2: GARCH(1,1) model coefficients

	ω	α_1	β_1	$\alpha_1 + \beta_1$	Log-likelihood
BitStamp	0.00005* (0.00004)	0.2681** (0.0432)	0.7308** (0.065)	0.999	2118.383
bitcoin.de	0.00009** (0.00004)	0.4004** (0.0538)	0.5985** (0.067)	0.999	2191.674
BTC China	0.00008* (0.00003)	0.3689** (0.0556)	0.63** (0.0508)	0.999	2140.071

** significance on 1%-level, * significance on 5%-level

Table 2 additionally shows big difference in decomposition between influence of recent (α_1) volatility and long-term rolling (β_1) volatility of the sample. While the Chinese and European Bitcoin exchanges react strongly to recent volatility, the US exchange shows much smaller sensitivity to recent volatility according to GARCH(1,1) model. Figure 7 depicts comparison of GARCH(1,1) conditional standard deviation fitted values for each of examined exchanges, which are in line with EWMA concerning both magnitude and dynamics. We cannot examine the unconditional variance, to which GARCH(1,1) process converge, because it is infinite when unit root is present. Summing up the results of GARCH volatility estimation it shows us the persistence of shocks, and indicates we should move to IGARCH model. As to the magnitude of volatility the results are in line with EWMA estimates.

Figure 7: GARCH(1,1) estimates of volatility



6.2.2 IGARCH(1,1)

IGARCH model follows directly from GARCH model, but assumes presence of unit root in the variance. IGARCH(1,1) is specified as follows.

$$a_t = \sigma_t \varepsilon_t$$

$$\sigma_t^2 = \omega + \beta_1 a_{t-1}^2 + (1 - \beta_1)\sigma_{t-1}^2$$

That way shocks do not die out, but persist in the process.

Table 3 presents the results of IGARCH(1,1) model, which are naturally very similar to those of GARCH(1,1). We conduct a likelihood ratio test for the restriction of unit root in variance. The presence of unit roots biases results of tests towards rejection of unit roots (Dickey & Fuller, 1979); however, Hong (1988) shows this problem does not hold for IGARCH testing; hence, all testing is valid (Chou, 1988).

Table 4 shows the test results. The restrictions are not rejected for either exchange.

Table 3: Coefficients of IGARCH(1,1) model

	ω	β_1	Log-likelihood
BitStamp	0.00005** (0.00001)	0.2686** (0.0585)	2118.458
bitcoin.de	0.00009** (0.000024)	0.4011** (0.0507)	2191.732
BTC China	0.00008** (0.00002)	0.3695** (0.0486)	2140.13

** significance on 1%-level, * significance on 5%-level

Table 4: Likelihood ratio test for unit root restrictions

	Log-likelihood unrestricted	Log-likelihood restricted	LR	p-value
BitStamp	2118.383	2118.458	0.15	0.7
bitcoin.de	2191.674	2191.732	0.116	0.73
BTC China	2140.071	2140.13	0.059	0.81

$LR = 2(LL_R - LL_{UR})$

6.2.3 EGARCH(1,1)

Thus far we assumed the influence of volatility is the same for both positive and negative shocks, and that the effect is not magnified by larger shocks. Estimating volatility in this way ignores the “leverage effect”, interpreted as a negative correlation between lagged negative returns and volatility (Corsi & Reno, 2012). A GARCH family model created to account for such asymmetries is EGARCH. R estimates the model as specified by Nelson (1991).

$$\log(\sigma_t^2) = \omega + \left(\alpha_1 z_{t-1} + \gamma_1(|z_{t-1}| - E|z_{t-1}|)\right) + \beta_1 log(\sigma_{t-1}^2)$$

where z_t are standardized innovations, with expected value,

$$E|z_t| = \int_{-\infty}^{\infty} |z| f(z\,,0\,,1\,,\dots)\,dz$$

coefficient α_1 captures the magnitude effect, while coefficient γ_1 captures the sign effect[32].

Table 5: EGARCH(1,1) estimation results

	ω	α_1	β_1	γ_1	Log-likelihood
BitStamp	-0.4127* (0.0944)	0.02124 (0.02101)	0.9320** (0.0143)	0.4154** (0.0455)	2011.578
Bitcoin.de	-0.8398** (0.1358)	0.0394 (0.0266)	0.8649** (0.0207)	0.5415** (0.0578)	2028.047
BTC China	-0.3378** (0.0807)	0.0367 (0.0212)	0.944** (0.0119)	0.4952** (0.0411)	2066.268

The magnitude coefficient α_1 is not statistically significant, which suggests volatility of Bitcoin does not respond strongly to magnitude of shocks. Statistically significant and positive coefficients γ_1 suggest volatility responds more strongly to negative shocks. Under risk aversion of investors, γ_1 should be positive, as it means volatility increases after a negative shock. The results therefore show evidence for presence of the leverage effect. EGARCH models volatility, while accounting for asymmetric reaction assumed by theories of financial markets, and we should prefer it in this respect, nevertheless information criteria need to be employed in order find the superior model.

Table 6: Information criteria for IGARCH(1,1) and EGARCH(1,1)

	BitStamp		Bitcoin.de		BTC China	
	IGARCH	EGARCH	IGARCH	EGARCH	IGARCH	EGARCH
AIC	-4.2501	-3.9001	-4.2522	-3.9321	-4.1519	-4.0064
SIC	-4.2501	-3.9001	-4.2522	-3.9321	-4.1519	-4.0064
HQIC	-4.2410	-3.8910	-4.2449	-3.9230	-4.1446	-3.9972

GARCH(1,1) model is not included in the comparison, because it was rejected by likelihood ratio test to IGARCH(1,1). Table 6 clearly shows IGARCH minimizes the information loss function irrespective of the Information criterion employed.

[32] https://cran.r-project.org/web/packages/rugarch/vignettes/Introduction_to_the_rugarch_package.pdf

6.2.4 Comparison to GARCH models of stock, commodity and currency volatilities

Modelling Bitcoin volatility using GARCH models gave us information about its behavior through time. These information are useful for understanding how exactly the volatility is driven; however, they are not informative regarding the similarities to currencies, commodities or stocks. Therefore, we compare GARCH models of Bitcoin, stock, commodity and currency volatility. We use closing prices for the same time window as for volatility spillovers and compute daily returns of S&P 500, Bloomberg commodity index and the New York Board of Trade US dollar index futures, BitStamp is used to stand for Bitcoin. It has been shown standard GARCH(1,1) model is not outperformed by other GARCH family models for currency volatility estimation; however, EGARCH is superior for stock volatility, because it accounts for the leverage effect (Hansen & Lunde, 2005). Coefficients of GARCH and EGARCH are not directly comparable; thus, we present results from both models.

Table 7: Coefficient comparison for standard GARCH(1,1) specification

	ω	α_1	β_1	$\alpha_1 + \beta_1$	Log-likelihood
BitStamp	0.000051* (0.000039)	0.2681** (0.0432)	0.7308** (0.0656)	0.999	2118.383
Stocks	0.000003 (0.000003)	0.2015** (0.0399)	0.7420** (0.0517)	0.944	3127.047
Commodity	0	0.0461** (0.0078)	0.9523** (0.0077)	0.998	3097.866
Currency	0	0.0402** (0.0109)	0.9577** (0.0096)	0.998	3558.085

Table 8: Coefficient comparison for standard EGARCH(1,1) specification

	ω	α_1	β_1	γ_1	Log-likelihood
BitStamp	-0.4127** (0.0944)	0.0212 (0.0210)	0.9320** (0.0143)	0.4154** (0.0455)	2011.578
Stocks	-0.6204** (0.0169)	-0.2225** (0.0192)	0.0192** (0.0023)	0.1281** (0.0187)	3156.425
Commodity	-0.0318** (0.0016)	-0.0233** (0.0085)	0.9968** (0.0000)	0.0589** (0.0066)	3101.366
Currency	-0.0002 (0.0012)	0.0512** (0.0032)	1.000** (0.00003)	-0.0047 (0.0031)	3565.334

In the standard GARCH model (Table 7) the evidence is twofold. Individually, α_1 and β_1 coefficients of BitStamp are closer to those of the stock index; however, their sum describing the persistence of shocks is almost the same for commodity, currency and Bitcoin. Put differently Bitcoin corresponds more closely to stocks considering the effect of recent and long-term volatility, and to commodities and currencies in terms of shock absorption. Overall, volatility of Bitcoin is shown to be more similar to that of stocks based on GARCH(1,1) estimates, although the persistence of shocks is somewhat larger for Bitcoin.

The EGARCH model (Table 8) provides evidence for the presence of leverage effect in stocks and commodities volatility, as γ_1 is statistically significant. Same evidence is provided for volatility of Bitcoin. Nevertheless, in the EGARCH model, dynamics of Bitcoin volatility is estimated to correspond more closely to commodities, as $\beta_1$coefficients are close to each other.

Our hypothesis was autoregressive structure of Bitcoin and currency volatility is similar; however, no evidence was found to support this claim. Volatility of Bitcoin was found to correspond to stock or commodity exchange volatility due to strong significance of leverage effect for all three series, and similarity of other coefficients based on a particular model. It shall be noted coefficients for BTC China in standard GARCH estimation are different; however, the conclusions here would be the same as for BitStamp.

6.3 Realized volatility and HAR models

Traditional parametric models for volatility estimation are very difficult to be estimated precisely. Frequently they rely on assumption of returns being distributed according to standard Gaussian distribution; moreover, they do not utilize high-frequency data (Andersen et. al., 2003). Realized Variance is a concept of non-parametric estimation of variance, which uses high-frequency data. It is specified as:

$$RV_t = \sum_{i=1}^{n} r_i^2$$

$$RS_t^- = \sum_{i=1}^{n} r_i^2 \, I_{r_i<0}$$

$$RS_t^+ = \sum_{i=1}^{n} r_i^2 \, I_{r_i>0}$$

Realized Variance becomes consistent as the frequency of observations increases; however continuous sampling causes bias to the estimator due to bid-ask spreads. We specify realized volatility as square root of realized variance.

Figure 8: Realized volatilities through the high-frequency sample

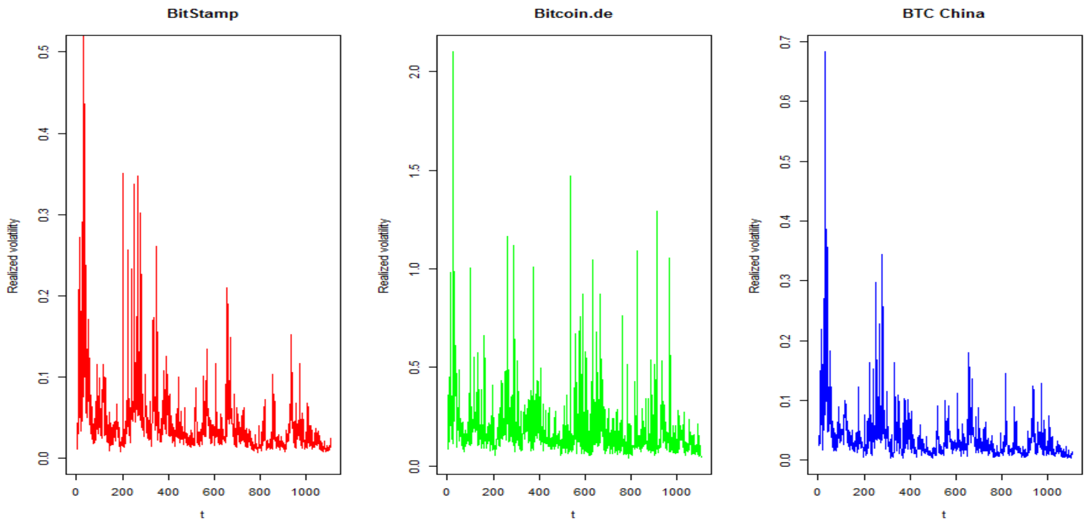


Figure 9: Positive and negative(plotted with negative sign) semivariances

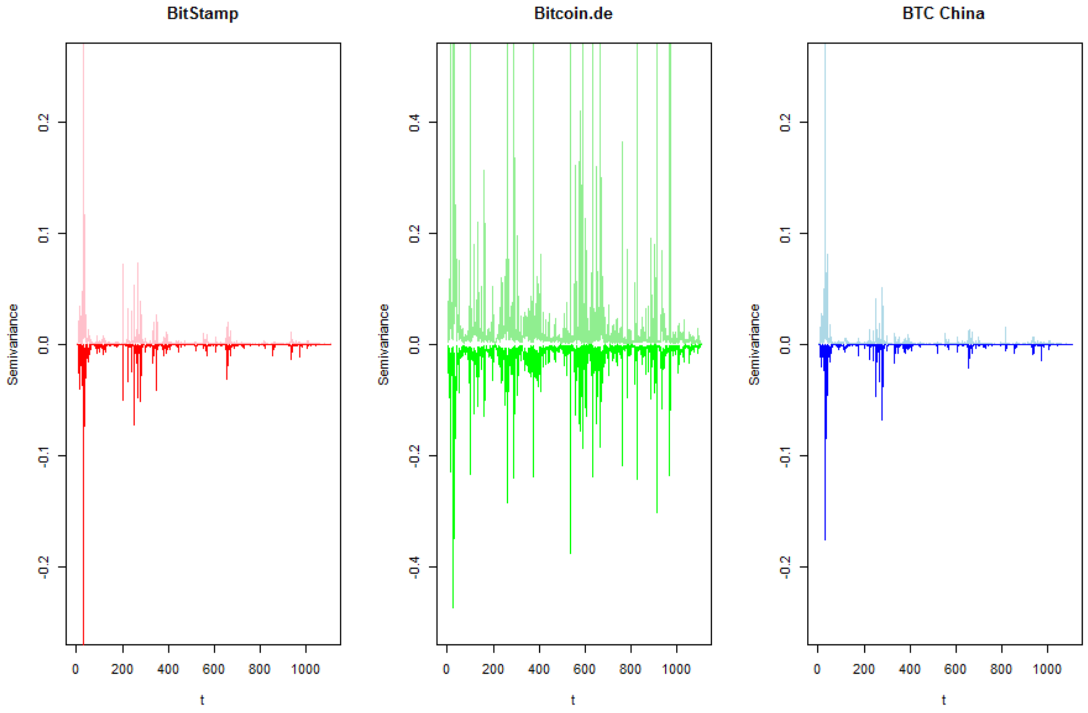


Figure 8 shows volatility measured on Bitcoin.de exchange cannot be involved in this section of estimations, because low trading volumes make its volatility incomparable to the other two series, when high-frequency data are used. Asymmetry between volatility connected to positive and negative returns is displayed in Figure 9. Positive and negative semivariance follow the same pattern; however, negative variance has greater magnitude for larger shocks.

Table 9: Estimates from the HAR1 model with following specification:

$$\sqrt{\boldsymbol{RV_t}} = \boldsymbol{\omega} + \boldsymbol{\beta_1}\sqrt{\boldsymbol{RV_{t-1}}} + \boldsymbol{\beta_2}\sqrt{\boldsymbol{RV^{(7)}_{t-1}}} + \boldsymbol{\beta_3}\sqrt{\boldsymbol{RV^{(30)}_{t-1}}} + \boldsymbol{u_t}$$

	ω	β_1	β_2	β_3	R-squared RMSE
BitStamp	0.0577** (0.0022)	0.4848** (0.0776)	0.0075 (0.0192)	-0.0313** (0.0077)	0.4526 0.0335
BTC China	0.0078** (0.0014)	0.3734** (0.1025)	0.0708* (0.0307)	0.0255** (0.0092)	0.4701 0.0274

**significance on 1%-level, *significance on 5%-level

Figure 8 shows volatility measured on Bitcoin.de exchange cannot be involved in this section of estimations, because low trading volumes make its volatility incomparable to the other two series, when high-frequency data are used. Asymmetry between volatility connected to positive and negative returns is displayed in Figure 9. Positive and negative semivariance follow the same pattern; however, negative variance has greater magnitude for larger shocks.

Table 9 presents the results from HAR model in the basic specification, with lagged daily, weekly and monthly volatility. Evaluation of statistical significance is made based on Newey-West standard errors as suggested by Corsi & Reno (2012). As is common, coefficients for lagged realized volatilities are all significant. Interestingly, monthly volatility coefficient for BitStamp is negative, which is susceptible. Model is fine in terms of R-squared, although it is not impressive. It can be improved by accounting for asymmetric response to sign of shocks and effect of trading volume. To get an idea about asymmetric response of variance, we substitute $\sqrt{RV_{t-1}}$ by $\sqrt{RS^{+}_{t-1}}$ and $\sqrt{RS^{-}_{t-1}}$.

Table 10: Estimates from the HAR2 model with following specification:

$$\sqrt{\boldsymbol{RV_t}} = \boldsymbol{\omega} + \boldsymbol{\beta_{1a}}\sqrt{\boldsymbol{RS^{+}_{t-1}}} + \boldsymbol{\beta_{1b}}\sqrt{\boldsymbol{RS^{-}_{t-1}}} + \boldsymbol{\beta_2}\sqrt{\boldsymbol{RV^{(7)}_{t-1}}} + \boldsymbol{\beta_3}\sqrt{\boldsymbol{RV^{(30)}_{t-1}}} + \boldsymbol{u_t}$$

	ω	$\boldsymbol{\beta_{1a}}$	$\boldsymbol{\beta_{1b}}$	β_2	β_3	R-squared RMSE
BitStamp	0.0089** (0.0016)	-0.0401° (0.1547)	0.6946** (0.1298)	0.0695* (0.0287)	0.0158* (0.0071)	0.4824 0.0331
BTC China	0.0080** (0.0013)	0.2712 (0.1916)	0.2530° (0.1433)	0.0732* (0.0310)	0.0250** (0.0093)	0.4681 0.0275

**significance on 1%-level, *significance on 5%-level, ° significance on 10%-level

Predictive power of the HAR2 model is comparable to HAR1 in terms of R-squared and Root Mean Square Error (RMSE). Neither model HAR3 (Table 11) does bring a dramatic improvement in terms of R-squared or RMSE. Economical interpretation of HAR2 and HAR3 is; however, interesting. Negative semivariance is found more significant than positive semivariance, which again suggests presence of leverage effect. Excess volume from the previous period is also found to be a significant predictor of volatility; however, with opposite sign than usual.

$$Excess\_volume_t = \frac{volume_t}{\frac{1}{29}\sum_{i=1}^{29} volume_{t-1}}$$

Table 11: Estimates of HAR3 model, specified as:

$$\sqrt{\boldsymbol{RV_t}} = \boldsymbol{\omega} + \boldsymbol{\beta_1}\sqrt{\boldsymbol{RV_{t-1}}} + \boldsymbol{\beta_2}\sqrt{\boldsymbol{RV^{(7)}_{t-1}}} + \boldsymbol{\beta_3}\sqrt{\boldsymbol{RV^{(30)}_{t-1}}} + \boldsymbol{\beta_4 excess\_volume_{t-1}} + \boldsymbol{u_t}$$

	ω	β_1	β_2	β_3	β_4	R-squared RMSE
BitStamp	0.0044* (0.0019)	0.3498** (0.0942)	0.0692** (0.0182)	0.0244** (0.0078)	0.0061** (0.0023)	0.4767 0.0333
BTC China	0.0043** (0.0017)	0.3409** (0.1046)	0.0677* (0.0299)	0.0310** (0.0102)	0.0033* (0.0013)	0.4754 0.0273

**significance on 1%-level, *significance on 5%-level

In attempt to improve our model we will estimate Bipower Variation (BPV), an estimate of Realized Variance robust to jumps in the series, and test its predictive power.

$$\boldsymbol{BPV_t} = \frac{\frac{m}{m-2}}{\left(\frac{\pi}{2}\right)} \sum_{j=3}^{m} \left|r_{t-1+(j-2)n}\right| \left|r_{t-1+jn}\right|$$

Jumps are essentially the difference between Realized Variance constructed according to the classical formula and Bipower Variation. Not all differences can be considered jumps, as majority of them is caused by sampling noise. Significance of jumps is tested by comparing Z statistic to quantiles of standard normal distribution.

$$Z_t = \frac{\frac{RV_t - BPV_t}{RV_t}}{\sqrt{\frac{\left(\frac{\pi}{2}\right)^2 + \pi - 5}{m} * max\left(1, \frac{TQ_t}{BPV_t^2}\right)}}$$

where TQ_t is an estimate of the fourth moment:

$$TQ_t = \frac{\frac{m^2}{m-4}}{0.8313^3} \sum_{j=5}^{m} \left|r_{t-1+(j-4)n}\right|^{\frac{4}{3}} * \left|r_{t-1+(j-3)n}\right|^{\frac{4}{3}} * \left|r_{t-1+(j-2)n}\right|^{\frac{4}{3}}$$

and $max\left(1, \frac{TQ_t}{BPV_t^2}\right)$ its small sample refinement (Baruník, 2015).

Corsi & Reno (2012) propose a model accounting for presence of jumps and leverage effect; we estimate its simplified version, whereas $Jump_t = RV_t - BPV_t$, if significant on 99.9%-level and 0 otherwise. HAR4 model reads as follows:

$$\sqrt{RV_t} = \omega + \beta_1\sqrt{BPV_{t-1}} + \beta_2\sqrt{BPV_{t-1}^{(7)}} + \beta_3\sqrt{BPV_{t-1}^{(30)}} \\ + \beta_4 Jump_{t-1} + \beta_5 r_{t-1}^{-} + \beta_6 r_{t-1}^{(7),-} + r_{t-1}^{(30),-} + u_t$$

where $r_{t-1}^{-} = \min(0, r_{t-1})$, $r_{t-1}^{(7),-}$ and $r_{t-1}^{(30),-}$ is the same principle applied on weekly and monthly returns.

Estimates resulting from the jump robust model are summarized in Table 12. Difference between jump robust model and models HAR1 – HAR3 is not very significant. In fact, it is not the best model in terms of R-Squared and RMSE. Jump robust estimates of realized volatility are significant with positive coefficients, as is common for HAR type models. Only other significant variable in the model are weekly negative returns. Negative sign for weekly negative returns provides another evidence for leverage effect and is in line with Corsi & Reno (2012).

Table 12: Estimates from HAR4 model

	BitStamp	BTC China
ω	0.0083** (0.0016)	0.0078** (0.0016)
β_1	0.5913** (0.127)	0.5363** (0.1638)
β_2	0.1391** (0.0364)	0.0772* (0.0328)
β_3	0.0319* (0.0126)	0.0663** (0.0201)
β_4	0.5848 (1.3381)	0.3937 (1.1419)
β_5	0.0156 (0.0759)	0.0696 (0.0927)
β_6	-0.0840** (0.0277)	-0.0939** (0.0319)
β_7	-0.0060 (0.0112)	0.0065 (0.0139)
R-Squared RMSE	0.4603 0.0337	0.4596 0.0276

**significance on 1%-level, *significance on 5%-level, ° significance on 10% - level.

6.4 Volatility spillovers

As anticipated the largest own volatility contributor is Bitcoin; however, the share is not significantly larger than for the stock exchange. We are basically only interested in results for Bitcoin. Largest contributor to the Bitcoin volatility is the commodity market, followed by the stock market. In addition Bitcoin contributes the most to the commodity market. The results are robust to variable ordering, as the mean spillovers for all orderings (*Table 20*) are not very different from those in Table 13. From Table 13 it can be concluded Bitcoin is most interconnected with commodity market. Regarding volatility spillovers there is not much evidence for Bitcoin connection to currencies.

The last row and last column display the contribution of the individual market to others and from others respectively. Bitcoin market contributes the least due to large contribution to own volatility. On the other hand the largest contributor to other markets is the stock market. Commodity and foreign exchange markets get contributed the most by others. Bitcoin again gets contributed the least, especially due to large own share. All summed up, Bitcoin displays largest interconnection with commodity market. Thus in this regard, there is no evidence for similarity with currencies.

Table 13: Volatility spillovers between stock market, currency market, commodity market and Bitcoin market in the USA

	Stock	Foreign Exchange	Commodity	Bitcoin	From others
Stock	0.96663	0.004553	0.0279	0.000904	0.0033
Foreign	0.120078	0.84684	0.0314	0.00165	0.1527
Commodity	0.10933	0.05224	0.82997	0.0084	0.17
Bitcoin	0.00816	0.00371	0.01554	0.9728	0.0274
To others	0.2376	0.06	0.0748	0.011	

6.5 Summary

We estimated different specifications of GARCH and HAR models to examine the pattern and drivers of volatility. Estimation of GARCH(1,1) model led to an evidence of unit root presence in variance. Hence, IGARCH(1,1) model was estimated and supported by likelihood ratio test over GARCH(1,1). To examine presence of asymmetric response to positive and negative volatility, leverage effect, EGARCH(1,1) model was also estimated; however, comparison according to Akaike Information Criterion (AIC), Schwarz Information Criterion (SIC) and Hannan-Quinn Information Criterion (HQIC) led to choice of IGARCH over EGARCH. GARCH models showed us a decreasing trend of volatility over the examined period and high persistence of volatility shocks.

Leverage effect was found to be significant phenomenon especially for volatility of stock indexes (Corsi & Reno, 2012; Bouchaud et. al, 2001) and commodities (Du et. al., 2009; Cheong, 2009; Morana, 2011). In HAR models, evidence for the leverage effect was found for both BitStamp (model with positive and negative semivariance included was the best performing one) and BTC China. The evidence was further supported by significance of negative returns in the jump robust HAR model. We also tested for negative correlation between trading volume and volatility documented by Scott & Tucker (1988) or Fung & Patterson (1998). Volume was found to be a significant predictor; however, the correlation was positive; hence, the effect was opposite than documented in literature for currency markets.

Estimation of volatility spillovers has also not brought any evidence of interconnections between currency and Bitcoin market. The largest interconnection was displayed with the commodity market. This is in line with steep rise in volume of CNY denominated Bitcoin transaction, after departure to commodities, when Chinese currency started depreciating. It must be; however, noted the estimation of volatility spillovers was not conducted for the market in China. Although results are in line with that phenomenon, they are not caused by it.

7 Conclusion

Bitcoin has come a long way from an instrument serving as “entertainment” for computer enthusiasts to a phenomenon discussed by the most important financial institutions, sold for 450 USD per Bitcoin. Nevertheless, it has not proven to fulfill its primary purpose of being an alternative to fiat currencies so far. High volatility makes it an inferior store of value relative to fiat currencies, and promotes its usefulness as a tool for speculation. In this paper we were examining the potential of Bitcoin to become competition to fiat currencies in the future. Dynamics of volatility was examined, looking for a downward trend, and also the drivers of volatility were compared to those of stocks, commodities and currencies. Lastly, we investigated the interconnections between Bitcoin market, currency market, stock market and commodity market by estimating volatility spillovers.

For purposes of volatility estimation we used GARCH family models, as returns volatility is documented to have autoregressive heteroscedastic features (Fung & Patterson, 1998; Scott & Tucker, 1988; Choi & Hammoudeh, 2010), and GARCH models are documented to display satisfactory performance in capturing the relationship between volatility and lagged volatility (Hansen & Lunde, 2005). Estimating also the EGARCH specification allows us to conclude about presence of leverage effect, which is present for stock markets (Corsi & Reno, 2012; Bouchaud et. al, 2001) and commodity markets (Cheong, 2009; Du et. al., 2009; Morana, 2011).

In addition we estimate HAR model developed by Corsi (2004), which also considers the effect of lagged values on volatility, but takes advantage of high-frequency data and is based on a non-parametric variance measure - Realized Variance. HAR model also lets us examine the relationship between volatility and trading volume documented for currency markets (Fung & Patterson, 1998; Scott & Tucker, 1988). Our dataset contains BTC/local currency returns from three markets with highest trading volume: USA, China and Europe, and returns of S&P 500, Bloomberg Commodity Index and the New York Board of Trade US dollar index futures for period between January 2013 and April 2016.

Results of GARCH(1,1) suggest presence of unit root in variance, as the sum of α_1 and β_1 coefficients is almost 1. We; therefore, moved to estimation of IGARCH(1,1) model which accounts for unit root. Likelihood ratio test supported IGARCH over GARCH. Then we tested for presence of leverage effect by estimating EGARCH model, which allows for asymmetric reaction to positive and negative shocks. Coefficient γ_1 standing for the asymmetric effect was significant; however, IGARCH was preferred over EGARCH using minimalization of Information Criteria. Overall, results of GARCH models show a trend of decreasing volatility; nevertheless, the pace of decrease is rather slow.

Moreover, there is evidence for presence of the leverage effect, as γ_1 is significant in EGARCH model. Nevertheless IGARCH is supported over both EGARCH and GARCH. Indication of IGARCH as best performing model suggests persistence of shocks in volatility of Bitcoin. Comparison of GARCH and EGARCH model estimates for stocks, currencies, commodities and Bitcoin shows similarities of Bitcoin volatility to stock and commodity volatility. The distribution of recent and rolling long-term volatility influence of Bitcoin is more closely matched by stock market. Furthermore, EGARCH model suggests presence of leverage effect for both stock market and Bitcoin, and also the commodity market.

Presence of leverage effect in Bitcoin volatility is supported by HAR models. Specifically, the one with positive and negative realized semivariance plugged in. Negative semivariance is more significant in terms of magnitude and statistical significance, which again points out to the presence of leverage effect. This hypothesis is additionally supported by a version of jump robust model suggested by Corsi & Reno (2013). We also tested for effect of trading volume, but we found opposite (positive) effect on volatility for Bitcoin, than previously found for currencies (Scott & Tucker, 1988; Fung & Patterson, 1998). Estimation of volatility spillovers showed market for Bitcoin is most closely interconnected with commodity market; however, the proportion of volatility added to Bitcoin market is still small, as it “causes” almost all volatility itself.

The results suggest volatility of Bitcoin decreases over time; however, to be useful as a store value this trend would have to continue for a considerable amount of time. Such a scenario naturally cannot be ruled out, but Bitcoin does not behave as a store of value comparable to fiat currencies for now. More importantly, the asymmetries we found in Bitcoin volatility do not corresponds to these usually displayed by currencies, but rather to these displayed by stocks or commodities; hence, Bitcoin is not even similar to currencies in terms of volatility drivers. Furthermore, no intrinsic value of Bitcoin and no central institution to “guarantee” its value make its price extremely vulnerable to sudden loss of trust. This threat will presume, even if its volatility should ever decrease to a level compatible with a stable store of value.

All in all our research suggests it is likely Bitcoin will stay an investment, or speculation, tool than compete with fiat currencies. Although the evolution on Chinese market suggests, we already saw departure from currency to Bitcoin as an alternative store of value. This itself cannot be taken as evidence, such a substitution is likely for other markets, since Chinese market is still developing and heavily controlled by state; hence, the circumstances cannot be deemed normal. In addition our results suggest current incomparability to currencies. Most importantly, even if Bitcoin ceased to exist at some point, blockchain has potential to revolutionize and improve the way of information processing and contracts reinforcing for a large variety of institutions worldwide. Possible extension to our research is testing, what the sudden jump in CNY denominated trades in the second half of 2015 is really attributable to.

Bibliography

Allison, I. (2015). Ripple’s Chris Larsen Adds Up Savings for Banks Using Distributed Ledgers. IB Times, http://www.ibtimes.co.uk/ripples-chris-larsen-adds-savings-banks-using-distributed-ledgers-1513866, Accesed at: March 6, 2016.

Andersen, T.G., Bollerslev, T., Diebold, F.X., Labys, P. (2003). Modeling and forecasting realized volatility. Econometrica 71: 579–625.

Barber, S., Boyen, X., Shi, E., Uzun, E. (2012).“Bitter to better – how to make bitcoin a better currency,” in Financial Cryptography, vol. 7397 of LNCS, 2012, pp. 399–414.

Baruník, J. (2015). Quantitative Finance I, Lecture Notes. Institute of Economic Studies, Faculty of Social Sciences, Charles University in Prague. Available at: http://staff.utia.cas.cz/barunik/quantitative_finance.htm

Baruník, J., Kočenda, E., Vácha, L. (2015). Volatility spillovers across petroleum markets. The Energy Journal, 36, 309-330.

Bergstra, J.A. Weijland, B.P. (2014). Bitcoin: A Money-like Informational Commodity. ArXiv: 1402.4778

Bolerslev, T. (1985). A Conditionally Heteroscedastic Time Series Model for Security Prices and Rates of Return data. Ucsd, Department of Economics, Discussion Paper No. 85-32

Bornholdt, S., Sneppen, K. (2014). Do Bitcoins make the world go round? On the dynamics of competing crypto-currencies. arXiv, 1403.6378.

Bouchaud, J.P., Matacz, A., Potters, M. (2001). Leverage Effect in Financial Markets: The Retarded Volatility Model. Physical Review Letters 87, 228701

Bouoiyour, J., Selmi, R. (2015). What Does Bitcoin Look Like?. Annals of Economics and Finance 16, (Forthcoming).

Brezo, F., Bringas., P.G. (2012). Issues and risks associated with crypto currencies such as Bitcoin. In: SOTICS 2012, Second Int. Conf. on Social-Eco-Informatics, 20–26

Buterin, V. (2014). Bitcoin Multisig Wallet: The Future of Bitcoin. Bitcoin Magazine, https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504, Accesed at: March 2, 2016

Cheong, C.W. (2009). Modeling and Forecasting Crude Oil Markets Using ARCH-Type Models. Energy Policy 37:2346-2355.

Choi, K., Hammoudeh, S. (2010). Volatility behavior of oil, industrial commodity and stock markets in a regime-switching environment. Energy Policy 38 (8), 4388–4399.

Chou, R.Y. (1988). Volatility Persistence and Stock Valuations: Some Empirical Evidence using GARCH. Journal of Econometrics 3: 279-294.

Corsi, F. (2014) A Simple Long Memory Model of Realized Volatility. Available at SSRN: http://ssrn.com/abstract=626064

Corsi, F., Reno, R. (2012). Discrete-time volatility forecasting with persistent leverage effect and the link with continuous-time volatility modeling. Journal of Business and Economic Statistics, 30(3), pp. 368-380. doi: 10.1080/07350015.2012.663261

Dickey, D.A., Fuller, W.A. (1979). Distribution of estimators for autoregressive time series with a unit root. Journal of the American Statistical Association, 77, 427-431

Diebold, F. X., Yilmaz, K. (2009). Measuring Financial Asset Return and Volatility Spillovers, with Application to Global Equity Markets. The Economic Journal, 119: 158–171. doi: 10.1111/j.1468-0297.2008.02208.x

Diebold, F.X., Yilmaz, K., (2011). Better to give than to receive: predictive directional measurement of volatility spillovers. International Journal of Forecasting, 28: 57-66. doi:10.1016/j.ijforecast.2011.02.006

Doguet, J.J. (2013). The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System. 73 LA. Literature Review, 1119, 1125-28.

Du, X., Yu, C.L., Hayes, D.J. (2009). Speculation and Volatility Spillover in the Crude Oil and Agricultural Commodity Markets: A Bayesian Analysis. Working Paper 09-WP 491, Center for Agricultural and Rural Development, Iowa State University.

Fung, H-G., Patterson, G.A. (1999). The dynamic relationship of volatility, volume, and market depth in currency futures markets. Journal of International Financial Markets, Institutions and Money, 9, 33-59.

Gomez-Gonzalez, J.E., Parra-Polania, J.A. (2014). Bitcoin: something seems to be "fundamentally" wrong. Borradores de Economía. Banco de la Republica Colombia. No. 819.

Grinberg, R. (2011). BitCoin: An Innovative Alternative Digital Currency. Hastings Science & Technology Law Journal 4: 159-208.

Güring, Philipp and Ian Grigg (2011): Bitcoin & Gresham's Law - the economic inevitability of Collapse. http://iang.org/papers/BitcoinBreachesGreshamsLaw.pdf.

Hanley, B. P. (2013). The false premises and promises of bitcoin. arXiv preprint arXiv:1312.2048.

Hansen, P. R., Lunde, A. (2005). A forecast comparison of volatility models: does anything beat a GARCH(1,1)?. J. Appl. Econ., 20: 873–889. doi: 10.1002/jae.800

Hong, C.H. (1987). The IGARCH model – the process, estimation and some Monte Carlo experiments. UCSD Discussion Paper, 87-32.

Jansen, M.A. (2012). The Political 'Virtual' of an Intangible Material Currency. MA Thesis, Department of New Media and Design, Utrecht University.

Kaplanov, N.M. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. Temple University Legal Studies Research Paper http://ssrn.com/abstract=2115203

Koop, G., Pesaran, M.H., Potter, S.M. (1996). Impulse response analysis in nonlinear multivariate models, Journal of Econometrics 74, 119-47.

Kristoufek, L. (2014). What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis. http://arxiv.org/pdf/1406.0268.pdf

Lamoureux, C.G., Lastrapes, W.D. (1990). Heteroskedasticity in Stock Return Data: Volume versus GARCH Effects. Journal of Finance, 45, 221-229.

Liebenau, J., Elaluf-Calderwood, S.M. (2016). Blockchain Innovation Beyond Bitcoin and Banking. Available at SSRN: http://ssrn.com/abstract=2749890

Martins, S., Yang, Y. (2011). Introduction to Bitcoins: A Pseudo-anonymous Electronic Currency System. CASCON '11 Proceedings of the 2011 Conference of the Center for Advanced Studies on Collaborative Research, 349–350.

Mittal, S. (2012). Is Bitcoin Money? Bitcoin and Alternate Theories of Money. Available at SSRN:http://ssrn.com/abstract=2434194

Moore, T., Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. Financial Cryptography - Lecture Notes in Computer Science. vol. 7859, A.-R. Sadeghi, Ed., ed: Springer, pp. 25- 33.

Morana, C. (2001). A Semiparametric Approach to Short-Term Oil Price Forecasting. Energy Economics 23:325-338.

Nelson, D.B. (1991). Conditional heteroskedasticity in asset returns: A new approach. Econometrica, 59(2):347–70.

Ou, G. (2011). Bitcoin. A Crypto-Geek Ponzi Scheme, High Tech Forum, http://hightechforum.org/bitcoins-a-crypto-geek-ponzi-scheme/, Accesed at: December 28, 2015.

Parkinson, M. (1980). The extreme value method for estimating the variance of the rate of return. Journal of Business, 53, pp. 61–65

Pattanayak, S., Fainboim, I. (2010). Treasury Single Account: Concept, Design and Implementation Issues. IMF Working Paper 10/143

Pesaran, M.H., Shin, Y. (1998). Generalized Impulse Response Analysis in Linear Multivariate Models. Economics Letters, Vol.58, 17-29.

Peters, G. Wi., Panayi, E. (2015). Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. Available at SSRN: http://ssrn.com/abstract=2692487

Pong, S., Shackleton, M.B., Taylor, S. J., Xu, X. (2004). Forecasting Currency Volatility: A Comparison of Implied Volatilities and AR(FI)MA Models, Journal of Banking and Finance 28, 2541–2563.

Ranasinghe, D. (2015). Why China’s Yuan May Be Set for 15% Devaluation. CNBC, World Economy, http://www.cnbc.com/2015/09/16/why-chinas-yuan-may-be-set-for-15-devaluation.html, Accesed at: May 12, 2016.

Rizzo, P. (2015). Health Care Giant Philips Exploring Blockchain Applications, CoinDesk, http://www.coindesk.com/health-care-giant-philips-exploring-blockchain-applications/, Accesed at: March 6, 2016.

Schlichter, D. (2012). The Death of Banks And the Future of Money, Gold Made Simple, http://www.goldmadesimplenews.com/gold/the-death-of-banks-%E2%80%93-and-the-future-of-money-7177/, Accesed at: February 14, 2016.

Scott, E., Tucker, A.L. (1989). Predicting currency return volatility. J. Banking Finance 13:6, pp. 839–51.

Selgin, G. (2013) Synthetic Commodity Money. University of Georgia Economics, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118

Šurda, P. (2012). Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold? MA Thesis, WU Vienna University of Economics and Business.

West, K.D., Cho, D. (1995), The Predictive Ability of Several Models of Exchange Rate Volatility, Journal of Econometrics, 69, 367-391.

Yermack, D. (2013) Is Bitcoin a real Currency? NBER Working Paper Series, Working Paper 19747. http://www.nber.org/papers/w19747

Web Sources:

The Next Web: *http://thenextweb.com*

History of Bitcoin: *http://historyofbitcoin.org*

Bitcoin Wiki: *http://en.bitcoin.it/wiki*

CoinDesk: *http://www.coindesk.com*

The Verge: *http://www.theverge.com*

LOC: *http://www.loc.gov*

Economist: *http://www.economist.com*

The Guardian: *http://www.theguardian.com*

Ars Technika: *http://arstechnika.com*

Mother Board: *http://motherboard.vice.com*

Time: *http://time.com*

Ripple: *http://www.ripple.com*

Ethereum: *http://www.ethereum.org*

Hyperledger: *http://hyperledger.org*

Balanc3: *http://www.balanc3.net*

Bitcoin Charts: *http://bitcoincharts.com*

Bitcoinity: *http://data.bitcoinity.org*

Statista: *http://www.statista.com*

Appendix A: Probability of Attack

Here we present the probabilities of an attacker outpacing honest nodes in extending the chain, given the starting deficit z[33] and probability of attacker extending the chain by one block q. The process can be characterized as a Binomial Random Walk; hence, probability of honest nodes extending the chain by one block is: p=1-q, and q corresponds to share of total computing power on the system held by the attacker (Nakamoto, 2008). The probabilities given corresponding values of q and z are:

Table 14: Probabilities of successful attack

z		p
	q=0.1	
0		1
2		0.050978
4		0.003455
6		0.000242
8		0.000017
10		0.000001
	q=0.3	
0		1
10		0.0416605
20		0.0024804
30		0.0001522
40		0.0000095
50		0.0000006

[33] z…number of blocks atacker is behind at the beginning

Table 15: Blocks behind sufficient to limit probability of success below 0.001 for given q.

q	z
	p < 0.001
0.1	5
0.2	11
0.3	24
0.4	89
0.45	340

The probability drops exponentially with number of blocks behind; therefore, the attack is virtually impossible for q below, say 0.45.

Appendix B: Additional Tables and Figures

Figure 10: Annualized daily volatilities of Bitcoin and foreign exchange market

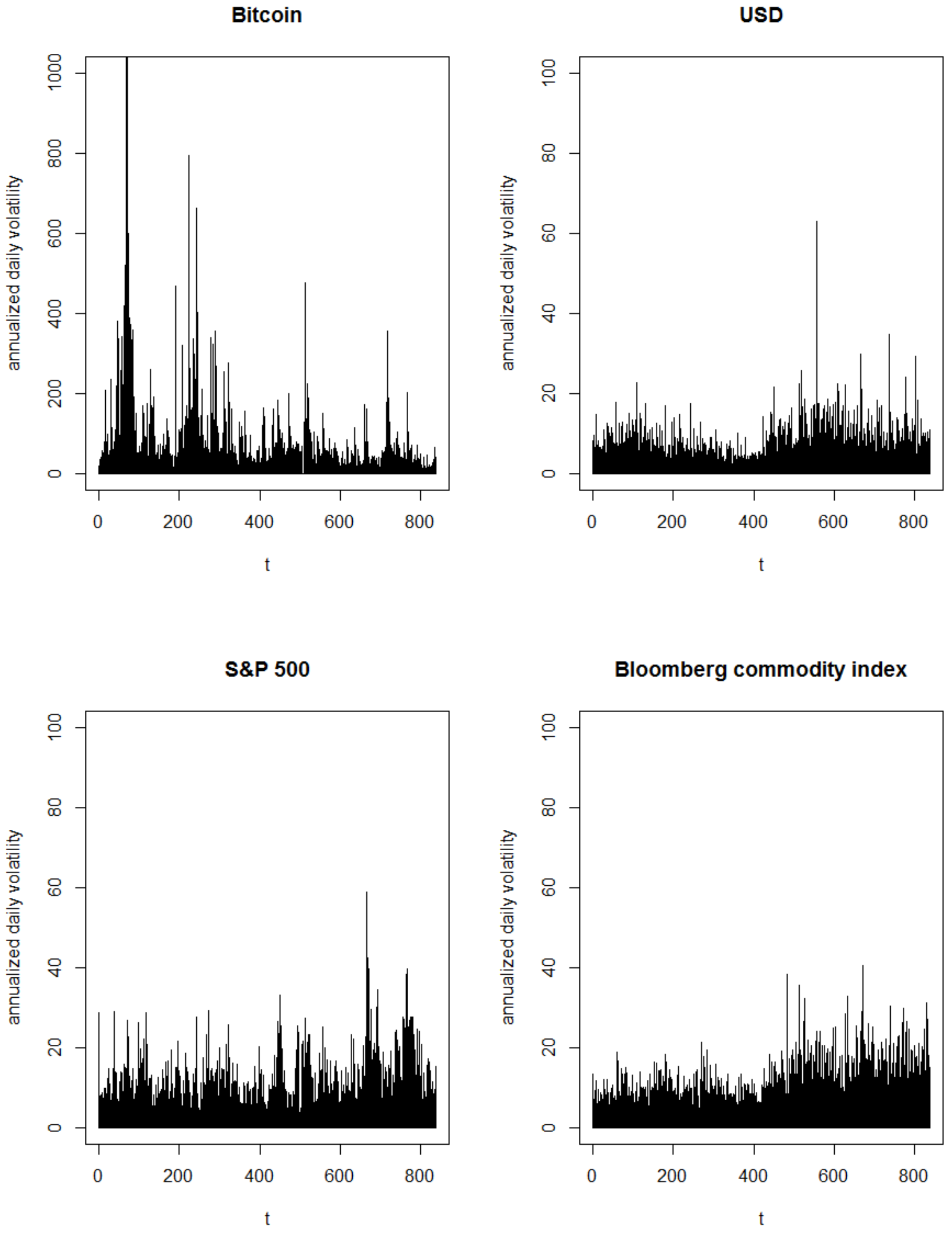


Table 16: Descriptive statistics of daily Bitcoin exchange returns

	mean	median	s.d.	Skewness	Kurtosis
BitStamp	0.00369	0.00192	0.0493	0.0483	12.543
bitcoin.de	0.00367	0.00097	0.0501	0.5476	15.311
BTC China	0.00403	0.00155	0.0512	0.1976	14.869

Table 17: Descriptive statistics of annualized daily volatility

	Stock market	Exchange	Commodity market	Bitcoin
Min	2.307	1.127	0.000	0.00
1st quantile	6.655	4.779	7.239	30.02
Median	9.701	6.809	10.136	49.59
Mean	11.249	7.813	11.382	82.33
3rd quantile	13.934	9.707	14.283	90.76
Max	58.807	63.038	40.452	1503.33
Standard deviation	6.519	4.640	5.694	115.4
Skewness	1.926	3.242	1.251	6.314
kurtosis	6.431	26.231	2.255	60.286

Table 18: Jarque-Berra p- values

	p-value
BitStamp	0.0000
bitcoin.de	0.0000
BTC China	0.0000

Table 19: Augmented Dickey-Fuller test p- values

	p-value
BitStamp	0.01
bitcoin.de	0.01
BTC China	0.01

Table 20: Robustness check, mean spillovers for different orderings

	Stock	Foreign	Commodity	Bitcoin
Stock	0.9603	0.0089	0.0494	0.004
Foreign	0.0781	0.8684	0.029	0.0016
Commodity	0.0978	0.0568	0.8412	0.0041
Bitcoin	0.0006	0.0038	0.0151	0.9803