An empirical study of how Bitcoin related incidents impact its price volatility

Piotr Pryzmont

Master of Business Administration

National College of Ireland

Submitted to the National College of Ireland, August 2016

Piotr Pryzmont

"An empirical study of how Bitcoin related incidents impact its price volatility"

Abstract

Bitcoin, a fascinating phenomenon of crypto-technology, has emerged in financial markets as a potential alternative to standard fiat currencies. It represents unique socio-technical ecosystem working outside of any traditional markets, and its economy is still not well understood. Dynamics of Bitcoin price proves to be quite a controversial subject, but there is a strong indication that social factors mainly influence its economy.

Technical flaws and lack of any central authority issuing and controlling this digital currency make it vulnerable to abuse. It has been associated with controversy due to frequent incidents, namely hacks, theft, scam, and illicit use, which affected its ecosystem ever since it gained popularity.

This thesis adds to the discussion about social aspects of Bitcoin economy by analysing the changes in its price volatility in the context of incidents occurring in its ecosystem. As empirically proven, those negative events have no impact on the fluctuations of Bitcoin price.

Submission of Thesis and Dissertation

National College of Ireland
Research Students Declaration Form
(Thesis/Author Declaration Form)

Name: Piotr Pryzmont

Student Number: x14115026

Degree for which thesis is submitted: Master of Business Administration

Material submitted for award

(a) I declare that the work has been composed by myself.

(b) I declare that all verbatim extracts contained in the thesis have been distinguished by quotation marks and the sources of information specifically acknowledged.

(c) My thesis will be included in electronic format in the College Institutional Repository TRAP (thesis reports and projects)

(d) I declare that no material contained in the thesis has been used in any other submission for an academic award.

Signature of research student: ______Piotr Pryzmont______

Date: _____29th August 2016_____

Acknowledgments

I would like to thank my supervisor Deirdre Bane for her support, guidance and feedback.

I would also like to thank Jonathan Lambert who helped me with the analysis of research data.

The most important thank you goes to my darling wife, Anita. Without your support, patience and love during this adventure I would not have been successful.

Table of Contents

List of Tables

List of Figures

List of Appendices

INTRODUCTION

“The relative success of the Bitcoin proves that money first and foremost depends on trust.” – Arnon Grunberg, Writer.

Background

Throughout the history, people have used many different methods of payment to facilitate trade. They quickly found that exchanging symbolic forms of value, whether being rare jewels, coins forged from precious metals or simply printed paper banknotes, is far more practical than bartering with raw goods. Until the middle of last century, the currency has always been represented by something material, that had to be either collected or produced and then physically exchanged. However with the recent development of computer systems and networks this traditional paper money, when used as a form of payment, started to be replaced by simple electronic transaction records (Reed Edge, 2014). In today's world, people find it more compelling to pay for goods using a credit card, shop on the Internet (online/virtual stores) or send money via electronic services (like PayPal). In effect, the currency lost the very physical aspect, and its intrinsic value is no longer apparent. This noticeable change in which money is being perceived eventually led to the creation of a true 'virtual currency', which many economists view as the natural evolution of money (Castronova, 2014).

The main idea behind the virtual currency is the ability to exchange value, which is embedded feature of traditional money, without direct control of a bank or financial institution. Many businesses use electronic currency either as a form of distributing perks to their customers (loyalty points, air miles, etc.) or as a method of payment for their services (coupons). However, in most cases, the use of such 'money' is contained within a specific environment (dedicated service/product), usually controlled by a specific company, and can rarely be transferred into real currency (Maftei, 2014). That is until 2009, when anonymous programmer (or group of developers) known under pseudonym Satoshi Nakamoto (2009) published an article in which he integrated several different ideas related to conceptual 'cryptocurrency' and managed to implement his concept in a dedicated computer software, shortly after, thus creating a new form of trade network – Bitcoin.

Bitcoin represents virtual currency which principles are based on cryptographic technology to store, spend and validate transactions (in which it was used) through the adoption of public and private crypto keys. The name Bitcoin also refers to software designed to use this currency as well as to a distributed network which stores the information about every bitcoin transaction. Since the main concept of Bitcoin is a peer-to-peer exchange, this digital currency does not require any central trusted clearing party to verify the transaction, nor there is any central issuer associated with it. It is available for everyone to use, its design ensures that each and every bitcoin can only be spent by the owner, and only once. Its operating principle also protects from hyperinflation by controlling the amount of new 'coins' put into circulation (number halves every four years). The protocol allows only 21 million bitcoins to be ever created (in total) and therefore its 'mining' process will cease in 2140 (Neguriaa, 2014).

Since May 2010, when first bitcoin payment took place (someone bought 25$ worth pizza for 10.000 BTC), the public interest in Bitcoin ecosystem started to gain momentum. Only a few months later first Bitcoin Exchange ('Mt.Gox') emerged and recorded bitcoin's first exchange rate set to 0.0769 USD. By April 2013 its price raised to nearly 200 USD and total Bitcoin's market capitalisation passed the 1B dollar mark. In late 2013, Bitcoin was subject to United States Senate hearing on which policymakers, regulators and subject experts made a positive opinion regarding its usefulness and, which is more import, legitimacy (Lee, Long and McRae, 2015). This decision boosted the price of bitcoin to (all-time high) 1120 USD and made it the most discussed topic in the financial news all around the world. It is quite evident that interest in Bitcoin, both public and regulatory, continue to grow as this digital currency can now be easily exchanged for other currencies or used directly to pay at many different online shops. At the time of writing, there is more than 15.7M bitcoins in circulation and its market capitalisation is estimated at 10.2B USD (Blockchain.info, 2016).

However, the success of Bitcoin also drew the public attention to certain issues related to its ecosystem. Many different incidents have repeatedly been reported as the Bitcoin system is frequently targeted by hackers and fraudsters (Moore and Christin, 2013). For instance, over 1M USD worth of bitcoins were stolen from the MyBitcoin electronic wallet service in July 2011, 3M USD of users' investments were lost in Bitcoin's biggest Ponzi scheme ('Bitcoin Savings and Trust') which operated until August 2012, and over 3.4M USD investors funds were plundered in GBL Scam in November 2013 (Wolfson, 2015). The biggest incident, so far, was the collapse of

Mt.Gox in February 2014, the Bitcoin's largest exchange at the time, where alleged system hack lead to the loss of over 400M USD worth of bitcoins (Decker and Wattenhofer, 2014). Interestingly, it seems that Bitcoin ecosystem is uniquely resilient to such issues and failures as they do not necessarily affect its growth nor trigger a drop of its popularity (Morisse and Ingram, 2016).

Research Motivation and Objective

While technical aspects of Bitcoin system are well documented and described in the literature, it seems that the internal economy of this phenomena is still not well understood. According to Polasik, Piotrowska, Wisniewski, Kotkowski and Lighfoot (2015), main difficulties arising during attempts to characterise Bitcoin come the fact that it operates in two separate dimensions – technical and economical.

From one perspective, Bitcoin offers tangible utility delivered through its innovative and revolutionary technology. Its design allows performing fast and secure transactions which make it a viable alternative to current international payment systems (Papadopoulos, 2015). It is also considered to become a standard for micropayments (Ly, 2014) as well as a payment platform for retail business (Cascarilla, 2015) and e-commerce (Jaag and Bach, 2015). Going further, Bitcoin's open ledger system – blockchain – offers unique functionality which found its use beyond crypto-currency, for example in voting systems, domain name registries, financial exchanges, crowdfunding platforms, company governance, smart contracts, and much more (Forte, Romano and Schmid, 2015).

From the other side, Bitcoin denotes virtual currency which is used as a medium of exchange, has its own value and represents a unit of account, thus satisfies the economic definition of money (Pacy, 2014). However, unlike traditional fiat currencies, Bitcoin is not tied to the economy of any particular country, is independent of central banks and free of standard capital control mechanisms (Polasik et al., 2015). As such, Bitcoin operates outside the real economy (Dowd and Hutchinson, 2015) and lack of central administration indicates that its internal market is based primarily on the collective trust (Sapuric and Kokkinaki, 2014).

It seems that the fundamental interdependence between those two dimensions, technical and economical, allowed Bitcoin to form unique socio-technical ecosystem capable of sustaining and driving its own growth (Morisse and Ingram, 2016). It is also evident that this ecosystem is characterised by complex internal dynamics that have a direct effect on Bitcoin price (Polasik et al., 2015). However, what factors are influencing it the most?

So far, the extent of empirical research related to Bitcoin ecosystem is quite limited. The notable exceptions are studies carried out by Garcia, Tessone, Mavrodiev and Perony (2014) as well as Kristoufek (2013; 2015) who used certain indicators, such as Google search statistics, to examine how the general public interest in Bitcoin influences its price. However, those studies did not take into consideration the sentiment of the information, as to whether negative or positive developments drove the publicity and the impact it could have on Bitcoin price. Additionally, the hypothesis of the interaction between technical and social dimensions of Bitcoin has also not been considered empirically.

This study aims to add to the current literature by providing empirical event driven analysis of Bitcoin price relative to social issues and technical vulnerabilities of its ecosystem. The main objective of this research is to identify whether the major incidents, which have already affected Bitcoin's ecosystem on numerous occasions, have any direct effect on the volatility of its price.

To frame the research in proper context, the first part of this thesis presents a review of the available literature that holds the theoretical study of relevant concepts. It explains how Bitcoin is situated within existing financial system, discusses its price dynamics as well as focuses on the main issues related to Bitco4in. The second chapter declares the main research question and explains the aims and objectives of the investigation. The third chapter concentrates on research methodology and explains how the research is constructed and relevant data collected. The fourth chapter presents the research findings. Last part of this thesis discusses the results and presents final conclusions about the research topic.

CHAPTER I

LITERATURE REVIEW

The purpose of this chapter is to elaborate on some specific aspects of Bitcoin social and technical system to clarify the purpose of the research. It aims to form the theoretical perspective for this study and to frame the main research question in a proper context. Firstly, it will describe the general concept of Bitcoin and explain how it is positioned in the current financial system and economic market. Secondly, it will identify and discuss the main drivers of Bitcoin price, sources of its volatility, and catalysts of its growth. Lastly, this chapter will pinpoint and characterise certain issues related to Bitcoin that enhances the social factors influencing its ecosystem, namely hacks, thefts, frauds, scams, and susceptibility to crime.

1.1 Bitcoin

The common definition of Bitcoin is not yet forged, and therefore it is often referred to as crypto-currency, virtual money, digital money, e-currency or e-money (Ly, 2014). Satoshi Nakamoto (2009), the inventor of Bitcoin himself, referred to it as "electronic cash". Bitcoin is however not only the name of the currency but also the name of the open-source software and peer-to-peer network that forms its architecture and facilitates transactions (Böhme et al., 2015). The technical principles of Bitcoin, the production of coins, executing transactions and general development of crypto-currency market is a subject that goes beyond the scope of this study. However, it is important to describe some of its selected characteristics to set the proper context for this work.

According to Kauffman and Walden (2001), Bitcoin shares the theoretical assumptions of software money presented in early 90's by Chaum as well as Camp, Sirbu, and Tigar. It is simply a digital code that cannot be directly converted to any physical commodity (like gold or raw material), and the idea of its operation is based exclusively on users' trust (Sapuric and Kokkinaki, 2014). However, in a contrast to software money which is issued and controlled by a specific institution, such as Liberty Reserve (offered by Costa Rica-based money transfer service) or Linden Dollars (used in the social game – 'Second Life'), Bitcoin does not substitute any existing legal tender and has its own value (Polasik et al., 2015).

Bitcoin is characterised by a decentralised mechanism of creation and operation. It is not controlled by any particular institution but rather jointly managed by the users themselves through the peer-to-peer network (Tu and Meredith, 2015). However, unlike earlier software money, Bitcoin virtual currency does not depend on user's trust but is rather build upon cryptographic proof (Pacy, 2014).

Generation of new coins (recognised as "mining" or "digging") consists of processing very specific, random-based numerical calculations that require significant computing power (Garcia et al., 2014). In this respect, a certain amount of bitcoins is obtained as proof that the work has been done to solve a computational problem, so-called "Proof of Work" (Nakamoto, 2009, p. 3). The size of this reward, set initially to 50 bitcoins, is halving every four years and currently amounts to 12 bitcoins (Coinbase, 2016). Due to Bitcoin's specific and unique design, this virtual currency cannot be forged outside of the standard creation mechanism, and any attempt to falsify bitcoin or its transaction is ineffective (Sapuric and Kokkinaki, 2014).

Carrying out a Bitcoin transaction requires the use of digital signatures (public and private keys) which allow authenticating transfer of bitcoin ownership between two different user addresses in the network (Neguriaa, 2014). Each such transaction is recorded in a public ledger, so-called "blockchain" (Nakamoto, 2009, p. 2) and distributed among all nodes of the network (Bradbury, 2013). Also, on the contrary to traditional payment systems, Bitcoin protocol defines that each and every transaction is final and irreversible (Böhme et al., 2015).

Bitcoin status and classification within the current financial system is actively discussed and opinions whether Bitcoin can be considered a real currency are still split (Maftei, 2014). According to Yermack (2015) and Bal (2015), Bitcoin is primarily used to facilitate trade and as such it satisfies one essential function of money – being a 'medium of exchange'. However, authors explain that Bitcoin does not meet the remaining criteria, notably a 'store of value' and 'unit of account', due to its limited adoption and highly volatile price. Nonetheless, Pacy (2014) argues that, since Bitcoin represents its own unit of measure and that its volatility is progressively diminishing it should, in fact, be considered as true money.

Currently, it seems that increasing interest in Bitcoin, from both media and the market, is primarily caused by its ever-growing value. However, the real utility of Bitcoin is the ability to perform fast and low-cost transactions, with global reach, that are available to anyone, and are virtually anonymous (Little, 2014). Those features, however, open a possibility to use Bitcoin for money laundering, trade of prohibited goods, supporting terrorist groups or other criminal activity, which depreciates its functionality from the viewpoint of maintaining the legal order (Raibornand and Sivitanides, 2015). Also, exchange rate instability and high susceptibility to speculation means that many countries do not accept Bitcoin as means of payment and find its development as a threat to the maintenance of price stability in financial and payment systems (ECB, 2012).

1.2 Bitcoin Price

1.2.1 Bitcoin Price Drivers

Dynamics of Bitcoin's price proves to be quite a controversial subject since this digital currency became popular and accessible to the wider public in late 2010 (Kristoufek, 2015). While it is hard to recognise direct factors driving its value, there is a strong indication that its economy is mainly influenced by social factors (Garcia et al., 2014). Early work of Kristoufek (2013) indeed shows a positive bi-directional correlation between search queries on Google Search Engine and the price of the digital currency. This indicates that Bitcoin price may be directly affected by information available in media or by general public opinion, but also suggests that amount of publicity around Bitcoin is directly linked to this cryptocurrency's price changes during its rapid appreciations or depreciations. Kristoufek's (2015) later study shows that this relationship between Bitcoin price and the level of attention coming from internet users is not only directional (increased interest drives prices up during the formation of price bubbles as well as pushes it further down during their bursts) but also asymmetric (effect is more rapid during price deflation comparing to its inflation). The author also suggests that Bitcoin price is mostly driven by the growing public interest in this crypto-currency. According to Glaser, Zimmermann, Haferkorn, Weber and Siering (2014) such observable relationship reflects the fact that majority of new users joining Bitcoin community uses this crypto-currency primarily as an asset for purely speculative investments. Nonetheless, Buchholz, Delaney, Warren and Parker (2012) argue that Bitcoin price is mainly driven by supply (number of coins in circulation) and demand (number of transactions on exchanges) but may also be prone to speculation, like any other emerging market's fiat currency, due to visible characteristics of price bubbles.

Looking from a different perspective, Little (2014) explains that the value of Bitcoin comes from the fact that users are willing to exchange it for services and products of real value. According to the author, price in this respect is not driven by Bitcoin's internal economics, at least from the e-commerce perspective, because the majority of payments made in bitcoins are converted instantly to traditional currencies. The author indicates that Bitcoin should be considered as a bridge between currency payments and barter but not a true currency itself. To the contrary, Kondor, Posfai, Csabai and Vattay (2014) are of the opinion that while the initial phase of Bitcoin evolution was characterised by significant fluctuation in the properties of its network, transaction volumes and price, there is an evidence that Bitcoin network, in its current "trading" stage, reached the necessary stability and can be characterised by a coherent exponential distribution and disassortative degree correlations, thus indicating that Bitcoin system started to behave like a real currency. While Kristoufek (2015) agrees that standard and fundamental economic factors, like price level, volume of trades and currency supply indeed seem to influence Bitcoin economy, the author concludes that this effect is weak and can only be observed in the long term.

1.2.2 Bitcoin Price Volatility and Growth

Turpin (2014) indicates that there are many factors that impact the volatility of Bitcoin price, from which the most significant one seems to be its limited adoption in the global consumer's market. The author continues that this situation may change as there is a strong indication that growth of the electronic and Internet-based commerce will most likely influence the growth of the digital currencies, and Bitcoin in particular, due to their lower transaction cost, the anonymity of use, robustness and speed of operation. Grinberg (2011) argues that Bitcoin success in that field is still questionable as existing payment systems (PayPal, credit cards) can effectively compete against virtual currencies by simply lowering their transaction fees. Nonetheless, Bitcoin still has a potential to grow as a standard for micropayments since the cost of processing such transaction will always be significantly lower than in traditional systems (Ly, 2014). Besides, there is also strong evidence that certain social factors continuously influence the expansion of Bitcoin network (Garcia et al., 2014).

According to Perez and Urbaniak (2013), Bitcoin's intrinsically limited supply, considered by many authors as an ultimate protection against hyperinflation and distinctive advantage over fiat currencies, as well as its constantly increasing demand, stimulated by the public interest in this novel concept, are strongly influencing Bitcoin's further growth. Authors continue that this increasing demand in crypto-currencies is a result of general public distrust in global financial systems fuelled by a recent economic crisis. In fact, the conceptual work on Bitcoin itself was driven by the very same reason (Nakamoto, 2009) and this decentralised currency was created to address some issues pinned to central banks and discretionary monetary policies, for example: manipulation of interest rates, quantitative easing or political pressure (Dowd and Hutchinson, 2015). However Perez and Urabaniak (2015) add that Bitcoin is also not free from similar concerns since risks associated with the use of digital money are quite high, especially for inexperienced users. Authors predict that growing demand may not protect Bitcoin from radical price fluctuations in case of major break of public trust for this currency. Bad publicity resulting from major incidents, namely security breaches, providers bankruptcy or fraud, which already affected Bitcoin's ecosystem on numerous occasions, may lead to its sudden price drops and eventual collapse. Other authors provide more extreme opinion suggesting that “the underlying economics of Bitcoin mean that it is unsustainable and in all likelihood will be remembered as failed experiment” (Dowd and Hutchinson, 2015, p. 358).

Despite some strongly negative opinions and apparent risks or issues related to Bitcoin system, there is a visible evidence of an actual increase in confidence in this crypto-currency as more and more merchants start to accept Bitcoin as a valid form of payment for their products or services (Turpin, 2014). While this list is continuously expanding, some of the most prominent ones are Microsoft, Dell, WordPress, OverStock, Google, Wikipedia or even PayPal (Mishkin, 2014). Empirical analysis of the Bitcoin system presented by Kondor et al. (2014) indeed shows a stable and consistent growth of its network as well as increasing distribution of nodes and end-user addresses. Turpin (2014) indicates that such expansion of the Bitcoin network will most likely decrease the price volatility in the long term and reduce its reliance on pure speculation. However, the author is also not overoptimistic about Bitcoin's future and explains that other factors like regulatory and legal uncertainties or frequently reported system issues related to Bitcoin security, namely hacking, thefts and illicit use, may negatively impact users' trust in this crypto-currency which can in turn directly affect its value. Kroll, Davey and Felten (2013) warn that loss of confidence in Bitcoin can lead to so-called “death spiral” which can occur if its price drops below certain threshold rendering bitcoin mining uneconomical. “Loss of confidence in Bitcoin could cause the Bitcoin price to go down, a falling price lowers the incentive to mine and the equilibrium mining rate, lower mining rate leads to the currency being easier to subvert, and this leads to a further loss of confidence in the currency. Such a death spiral reflects the perceived loss of consensus in the potential value game” (Kroll et al., 2013, p.8).

1.3 Bitcoin Vulnerabilities

While Bitcoin economy continues to grow, some question about system integrity and security appear persistently within its community as well as in the academic world. Böhme et al. (2015) raised some concerns regarding decentralised nature of Bitcoin. Authors suggest that without central governance structure, which is found in conventional financial systems, this virtual currency may be vulnerable to cybersecurity threats as it solely relays on the function of underlying software and the global computer network. While the community of Bitcoin enthusiasts and evangelists is only growing stronger (Pagliery, 2014), the amount of reports about system abuse is also increasing hand-to-hand (Tu and Meredith, 2015), thus opinion that "Bitcoin is deeply flawed" (Guadamuz and Marsden, 2014) is not without an account.

1.3.1 Exploits

Like with any cryptographic software solution, design vulnerabilities may be found in Bitcoin own core protocol allowing for the system to be exploited, or a breakthrough in the crypto analysis could compromise its integrity (Böhme et al., 2015). While cryptographic security that forms a backbone of this digital currency is still considered to be safe for any foreseeable future, the implementation of the Bitcoin protocol itself, unfortunately, is not without flaws (Tschorsch and Scheuermann, 2015). Among few different software bugs, which users and programmers maintaining the code were able to identify so far, the one mostly known to the public is Transaction Malleability, allegedly linked to the collapse of MtGox in 2014 – the largest Bitcoin exchange at that time (Decker and Wattenhofer, 2014). While, in general, malleability is viewed as a specific feature of cryptographic systems, it proved to be profoundly problematic for the Bitcoin transaction protocol (Andrychowicz, Dziembowski, Malinowski and Mazurek, 2015). In certain cases, due to inadequate implementation of the protocol, this bug allowed modifying details of Bitcoin transaction so that payment system was not able to confirm successful transfers. The dishonest actor could, therefore, request the same withdrawal multiple times, draining additional bitcoins from exchange's account (Tschorsch and Scheuermann, 2015).

After filing bankruptcy in early 2014, Mt.Gox claimed that transaction malleability solely caused their loss of more than 600,000 bitcoins (worth more than 400 million USD at the time). Although security experts claim that this bug could not lead to such substantial losses (Decker and Wattenhofer, 2014), the very incident was a “major shock for the emergent sociotechnical field” and “made many question the security of both the Protocol and Bitcoin” (Ingram, Morisse and Teigland, 2015, p. 4). While many different implementation issues were discovered, analysed, and corrections to the underlying protocol put forward, the complexity of Bitcoin architecture makes it difficult or sometimes even impossible to apply those software patches without a risk of disruption of an entire system (Andrychowicz et al., 2015). For this reason, Bitcoin is considered quite vulnerable to software hacks and network-based attacks (Böhme et al., 2015).

Exceptionally prominent type of attack, which can disrupt Bitcoin operations, is so called 'Denial-Of-Service' attack (Vasek, Thornton, and Moore, 2014). In such attack, target service is overwhelmed by countless meaningless requests coming from multiple network sources ultimately rendering the service unusable or unable to communicate with the external network to perform its nominal function (Johnson, Laszka and Moore, 2014). There are two most common reasons behind DoS attacks. In the first scenario, a dishonest party is being paid for launching such attack for reasons only known to the requesting party (Karami and McCoy, 2013). The second motivation is simply extortion, where an adversary is requesting a direct payment from the affected company to stop the attack (Pappalardo and Messmer, 2005). However, Beekman (2016) indicates that certain DoS attacks in Bitcoin network, used to exploit some weaknesses of multi-party computation schemes, may, in fact, generate direct profit for the attacker at the cost of the deposits made by honest users. This, unfortunately, may open entirely new opportunities for exploiters of Bitcoin system.

Regardless of the motives, analysis provided by Johnson et al. (2014) as well as Vasek et al. (2014) indicate that DoS attacks are quite common in Bitcoin's ecosystem. Vasek et al. (2014) report that more than 7% of all services related to Bitcoin were targeted by DoS attacks, mostly affecting the Currency Exchanges. During one of such attacks, in late 2012, hackers were able to extract 24,000 bitcoins from “Bitfloor”, one of the popular exchanges operating at the time (Brito and Castillo, 2012). Recent reports suggest that amount of such incidents is on the rise, and major Bitcoin Exchanges are frequently targeted for extortion (Oconnel, 2016). Interestingly, escalation of denial-of-service attacks can be correlated not only with peaks in Bitcoin transaction volumes but also with sudden downfalls of its exchange rate. This suggests that the primary motives behind those attacks were linked to economic benefits of traders who were able to block other users' transactions from taking place (Vasek et al., 2014). Analysis conducted by Moore and Christin (2013) also highlights that many of the smaller Exchanges, who were victims of such attacks, had to close down their operations as a result of funds being stolen from its customers in the attack process. In the majority of such events, funds were never paid back, leaving a wave of unrest in the Bitcoin users community.

1.3.2 Thefts

In the Bitcoin system the entire history of each and every bitcoin transaction is stored in 'blockchain' – a public ledger which is distributed throughout the entire network and continuously verified by all its users. This unique technology enables the possibility to securely validate transactions directly between buyer and seller, protects against duplicates and also assures that all transactions are final so that they can never be reversed (Neguriaa, 2014). According to Mas and LEE Kuo Chuen (2015), most advocates of Bitcoin system claim that transaction irreversibility is one of the biggest advantages of the system, as it greatly reduces the possibility of fraud. It is argued that conventional payment systems are open to abuse as transactions can be disputed long after they were authorised, thus creating a high level of uncertainty for merchants. Bitcoin technology addressed that issue by eliminating the charge-back process entirely, thus operating “strictly under a buyer beware policy.” (Mas and LEE Kuo Chuen, 2015, p. 435).

However, Böhme et al. (2015), as well as Moore and Christin (2013), strongly argue that this feature of the Bitcoin system is, in fact, one of its major disadvantages. Lack of a built-in mechanism to reverse transactions makes it impossible to correct errors without the full cooperation of both parties (buyer and seller), nor it allows for a forceful retake of the funds lost due to theft (Moore and Christin, 2013). Although the illegal transaction is clearly visible on the public blockchain, FBI has determined that identification of the individuals executing such transaction is virtually impossible (Young and Natsios, 2012). For this very reason Bitcoin is especially susceptible to theft and thus very popular among cyber criminals (Brito and Castillo, 2013).

The scale of the problem can be quite distressing. Tu and Meredith (2015) explain that Bitcoin community forums are full of reports about alleged thefts since the early days of its advancement. It is estimated that more than 800,000 bitcoins, (currently worth approximately $500M USD) have been stolen between late 2010 and early 2014 in a series of bigger and smaller incidents. According to Amores and Paganini (2013), the most common method applied in persisting attempts to steal bitcoins from their owners is a malware-based attack. This is consistent with early findings of Barber et al. (2012) who reported that increasing value of Bitcoin mostly attracted community from cyber-underground who quickly recognised it as a new way of realising easy profits. Sophisticated malware software, designed to search for users digital wallets and their private keys, allows hackers to instantly take ownership of any bitcoins found on the infected computer. Just a single massive malware attack on the customers of MyBitcoin (online wallet service), in July 2011, resulted in a total loss of 1.3M USD worth of users' bitcoins (Amores and Paganini, 2013).

Major concern around theft in Bitcoin ecosystem is not only limited to issues related to security of individual users' computers since businesses offering Bitcoin services face similar problems (Grant and Hogan, 2014). Those companies operate under constant fear of malicious attack (Tu and Meredith, 2015) as reports of successful bitcoin heists appear in media quite regularly (Trautman, 2014). While the scale of attacks is increasing, hackers also employ more and more sophisticated techniques to gain access to large deposits of bitcoins (Paganini, 2013). Attacks on large companies are planned very carefully and “social engineering” techniques are often used to compromise even most secure networks and systems by focusing on the weakest chain – people (Hadnagy, 2011). The effectiveness of such attack was well proven in the case of Bitstamp, one of the largest Bitcoin exchanges, where a week's long phishing campaign focused on six employees of the company resulted in a theft of bitcoins worth almost 5M USD in January 2015 (Coindesk, 2015).

In any such incident, the loss for the company is unrecoverable thus often leads to bankruptcy. For that reason, many authors find Bitcoin to be a risky business to be in because “without Federal Deposit Insurance Corporation (FDIC) protection or other similar regulatory oversight or insurance, digital theft of bitcoins leaves the company with little recourse.” (Grant and Hogan, 2015, p. 32). Guadamuz and Marsden (2014) also highlight the fact that current situation within Bitcoin community, where theft and hacker attacks are very common, created somehow alarming "blame the victim mentality” (Guadamuz and Marsden, 2014, p. 10). This may be driven by the fact that many Bitcoin users are careless when it comes to security (Krombholz, Judmayer, Gusenbauer and Weipp, 2016). Especially that, from end-user perspective, Bitcoin's security assumptions require all participants to actively protect themselves from generic cyber-threats (malware, social engineering, negligence, data corruption) as anyone who has access to bitcoin's 'private keys' has the ability to control them (Raskin, 2015; Böhme et al., 2015).

1.3.3 Fraud, Scam and Illicit use

A major concern related to Bitcoin is its technical complexity which often exposes inexperienced users to many different risks (Moore and Christin's, 2013), and specifically scam. In contrast to hacking, scam does not use brute-force methods to override security and steal users bitcoins, but rather feeds on people's trust by tricking them to give their funds away willingly (Turpin, 2014). According to DeMartino (2016), there are two main types of scam that can be recognised in Bitcoin ecosystem: service scams and Ponzi schemes.

Bitcoin service scams were especially notorious in the early days when Bitcoin only started to gain its popularity (Turpin, 2014). Due to constantly increasing interest in this novel technology more and more websites started to appear on the Internet offering a broad spectrum of Bitcoin-related services, namely shops, auctions, casinos, online wallets or exchanges. Increasing demand for such services allowed some nefarious individuals to take advantage of innocent Bitcoin users by offering bogus websites disguised as reputable Bitcoin services. Undoubtedly, the most prominent type of service scam is fraudulent Bitcoin Exchanges. While those are usually relatively short-lived, they can attract many victims and so generate proceeds worth hundreds of thousands of dollars like in the infamous cases of *Ubitex, BTC Promo, CoinOpened* or *btcQuick* (Vasek and Moore, 2015). Any person depositing bitcoins to such fake service have no chance to recover the funds due to Bitcoin transaction irreversibility (DeMartino, 2016). This situation creates a real challenge for Bitcoin users who alone need to make a difficult decision of selecting the most appropriate service provider or exchange that could support their activities (Cofnas, 2015).

More sophisticated and complex type of scam in Bitcoin ecosystem are so-called Ponzi schemes (DeMartino, 2016). As described by Moore, Han and Clayton (2012), those High-Yield Investment Programs (HYIPs) are simply electronic versions of traditional financial scams (named after Charles Ponzi who first started using those techniques in 1920 in Boston) in which people are promised remarkably high returns on their deposits, with interest rates often exceeding 1% per day. Bitcoin proves to be especially fertile ground for investments scams due to the lack of proper legal classification (Ly, 2014) and de-centralised nature of the operation (Moore et al., 2012) thus making HYIPs impervious to existing legislative countermeasures. However, recent scandals related to Bitcoin already forced the authorities to take proper enforcement actions regarding investment scams (Ly, 2014). The one that gained most publicity was an investment firm “Bitcoin Savings and Trust” (former “First Pirate Savings and Trust”) run by Trendon Shavers, which was accused of defrauding large portion of clients funds estimated at around 700,000 bitcoins. The court charged Bitcoin Savings and Trust with a $40.7M fine while The Securities and Exchange Commission (“SEC”) issued an 'investor alert' warning about potential fraudulent or fabricated investments, namely Ponzi schemes, related to virtual currencies and Bitcoin in particular (Lee et al., 2015).

Despite the warnings, it seems that new investment services with clear properties of potential scam are still appearing in Bitcoin ecosystem and can successfully lure innocent users on the back of the promise of quick and substantial returns. According to Vasek and Moore (2015), nine such Ponzi schemes that entered into Bitcoin space between September 2013 and September 2014 (the biggest of which were “Leancy” and “Cryptory”) were able to raise more than 6.5M USD from bitcoin deposits alone. According to authors, more than half of the funds were never returned to the naive investors. Tu and Meredith (2015) underpin that victims of abuse in Bitcoin ecosystem have very few means of seeking retribution and can only express their frustration on public community forums. However, Moore et al. (2012) argue that many investors of Ponzi schemes are acutely aware of the fraudulent nature of that business. Those opportunists aim to participate in a scam at very early stage and help to promote it, to simply exit at the right time at the cost of other innocent investors.

Another problem that is often emphasised in media, and has a significant influence on public trust in Bitcoin, is its potential to facilitate criminal activities (Brito and Castillo, 2013). There is a prevailing opinion that Bitcoin is actively used to traffic illegal goods or finance terrorist activities as well as for money laundering and tax evasion (Tropina, 2014; Ron and Shamir, 2014). Criminal underground has exploited Bitcoin ecosystem primarily due to speed and security of its transactions as well as high level of anonymity of users comparing to traditional payment methods (Trautman, 2014). The most prominent example of such illicit use was the infamous *Silk Road*, an online marketplace operating in a hidden network, so-called *TOR* (Christin, 2013). This service, launched in January 2011, was used by thousands of drug dealers and other nefarious merchants to distribute illegal merchandise to hundreds of thousand customers from all over the world. Silk Road acted as a broker service, charging a commission for each transaction, and used bitcoins as the exclusive form of payment. It is estimated that this service facilitated sales revenues exceeding 1.2 billion USD and generated almost 80 million USD commission for its owners (FATF, 2014).

While Silk Road website was eventually tracked down and closed by FBI in October 2013, along with its main operator, Ross Ulbricht arrested, Bitcoin association with this illegal activity has seriously damaged its reputation. Some senators requested immediate action to delegalize use of Bitcoin in general (Duskin, 2014). However, according to Tu and Meredith (2015), Silk Road incident was not properly addressed as authorities "have failed to effectively distinguish between the risk posed by the Silk Road site and the Bitcoin technology itself." (Tu and Meredith, 2015, p. 327). While some authors argue that anonymity of Bitcoin transaction give a criminal perfect tool to operate under-the-radar of legal authorities (Duskin, 2014), Ron and Shamir (2013) underpins that Bitcoin transaction transparency, in fact, allowed FBI to identify many Silk Road's unlawful vendors. Going further, some empirical study indicates that illegal transactions account only to a small percentage of total Bitcoin volumes (Brito and Castillo, 2013) and its susceptibility for mistreatment do not differ from regulated financial tenders or services (Tu and Meredith, 2015).

1.4 Summary of the Literature Review

Bitcoin represents a new category of digital money which uses cryptographic principles for issuing and transferring this currency (Böhme et al., 2015). Unlike any earlier software money, Bitcoin is not controlled by any particular institution (Tu and

Meredith, 2015) and represents its own unit of measure (Pacy, 2014). However, there is still an open argument whether Bitcoin can be considered a real currency (Maftei, 2014), and opinions are forging on both negative (Yermack, 2015; Bal, 2015) and positive (Pacy, 2014) fronts.

Dynamics of Bitcoin's price also proves to be quite a controversial subject (Kristoufek, 2015). While there is a strong indication that it is mainly driven by social factors (Garcia et al., 2014; Kristoufek, 2015), some authors argue that it is strongly influenced by speculative investment (Glaser et al., 2014) or solely driven by fundamental economical factors (Buchholz, 2012). Although the Bitcoin price volatility remains extremely high (Dowd and Hutchinson, 2015), there are opinions that further growth of this ecosystem will stabilise the price (Turpin, 2014), which is already evident in some empirical studies (Kondor, 2014).

However, while Bitcoin economy continues to grow, the amount of reports about system abuse is also increasing hand-to-hand (Tu and Meredith, 2015) as Bitcoin system is frequently targeted by hackers and fraudsters (Moore and Christin, 2013). Bitcoin underlying software is often compromised (Böhme et al., 2015; Decker and Wattenhofer, 2014; Tschorsch and Scheuermann, 2015; Ingram, Morisse and Teigland, 2015) since the complexity of Bitcoin architecture makes it difficult to implement necessary countermeasures (Andrychowicz et al., 2015).

In addition to technical vulnerabilities, Bitcoin is also not free from socially-driven issues (DeMartino, 2016). Bitcoin proves to be especially fertile ground for investments scams (Ly, 2014; Moore et al., 2012) and there is a prevailing opinion that Bitcoin is actively used to to facilitate criminal activities (Brito and Castillo, 2013; Tropina, 2014; Ron and Shamir, 2014). According to Kroll et al. (2013), all those issues affecting Bitcoin ecosystem may cause sudden loss of confidence in the system and lead to so-called “death spiral.”

This chapter has explained the general concept of Bitcoin and discussed its position in the current financial system. It identified and discussed the main drivers of Bitcoin price, sources of its volatility, and catalysts of its growth. It also outlined the main characteristics of different technical vulnerabilities and social issues that are affecting its ecosystem. This literature review forms the perspective for this research, for which the main question, aims and objectives are detailed in the next chapter.

CHAPTER II
RESEARCH QUESTION, AIMS AND OBJECTIVES

2.1 Research Question

The purpose of this study is to provide event driven analysis of Bitcoin price relative to social issues and technical vulnerabilities of its ecosystem.
The main question, which this study addresses, is as follows:
How do incidents related to Bitcoin ecosystem affect its price volatility?

2.2 Research Aims and Objectives

The research aim of this thesis is to identify whether the Bitcoin incidents have any direct effect on the volatility of its price.

As a result, the established objectives for this research are as follows:

- Identify and analyse major incidents (negative events) which occurred in Bitcoin ecosystem.
- Analyse changes in Bitcoin price relative to those incidents.
- Determine the difference in price volatility before and after negative events

2.3 Hypothesis

This study will test the following hypotheses:

- H_1 *– Negative events cause a change in price variance*

To test this hypothesis and reach the objectives of this study specific research methods will be used, which are described in next chapter of this paper.

CHAPTER III
RESEARCH METHODOLOGY

This thesis is an empirical study that uses a deductive approach to explain how Bitcoin economy responds to incidents occurring in its ecosystem. The context of this work is based on earlier studies of Bitcoin phenomena which essence formed the basis for the first chapter. To answer the main research question, this study adopts quantitative methods to collect and analyse data related to the subject. This chapter aims to explain how the research process for this thesis was formed and conducted. Firstly, it will discuss the research methodology applied by the author and provide a rationale for choosing a particular approach for this study. Secondly, it will explain the process of data collection, sampling and analysis. Lastly, it will describe the limitations of this study and explain ethical considerations related to this work.

3.1 Introduction

Yin (2014) describes research methodology as a logical plan that allows the researcher to pursue and reach the conclusion or provide an answer to initially defined question. In other words, it is "a strategy or architectural design by which the researcher maps out an approach to problem-finding or problem-solving" (Buckley, Buckley and Chiang, 1976, p.13). Research design consists of important decisions regarding the approach to the research problem and the nature of data being collected, as well as the methods used to analyse and interpret that data. The aim of the research design is to assure that the final conclusions of the research properly address the research problem or question (Yin, 2014). This process can be divided into four main aspects: research purpose, research approach, research strategy and research methods.

3.2 Research Purpose

The purpose of this thesis is to analyse the relationship between various types of incidents affecting Bitcoin ecosystem and the price of this virtual currency. According to Saunders et al. (2009) as well as Cooper and Schindler (2014), a study that focuses on casual relationships between different variables is recognised as an explanatory research. Authors underpin that this type of study needs to be based on earlier exploratory work (which has a relatively broad focus and aims to assess certain phenomena or clarify a problem) or, more often, descriptive research (which attempts to provide much more detailed view of the problem by focusing on its one specific aspect). Therefore, in the case of this thesis, the context of main research is formed on the earlier work of Kristoufek (2013; 2015) who provided an analysis of the social drivers of the Bitcoin economy. A number of different studies of Bitcoin ecosystem, and specifically those related to its security, formed the perspective of this research which is represented by the literature review.

3.3 Research Approach

According to Saunders, Lewis and Thornhill (2009), research approach depends on the researcher's initial understanding of the theory linked to the subject of his study and, as such, can be divided into two distinctive categories:

- *deductive* – where research aims to test the initially defined theory or hypothesis, or
- *inductive* – where theory is developed as a result of the research.

This study represents the deductive approach, in which researcher develops hypotheses from previously defined theory and employs a rigid methodology (scientific methods) to test them through the analysis of (primarily) quantitative data collected in the research process. Usually, the results of such analysis either confirms that the theory is correct or indicates that it needs to be modified (Collis and Hussey, 2003).

In contrast, studies using inductive approach attempt to understand not only the nature of a problem but also the context in which measured events are taking place. Inductive researchers often apply many different methods to collect data (primarily qualitative) so that they can establish different views of the phenomena. (Easterby-Smith, Thorpe, Jackson and Lowe, 2008).

Onwuegbuzie and Leech (2005) highlight the fact that advocates of those two paradigms “often view themselves as being in competition with each other” (Onwuegbuzie and Leech, 2005, p. 267). However, authors are of the opinion that both orientations have many similarities and share the same goal. Thus the decision what research approach to take shouldn't depend solely on the research question. This view is shared by Easterby-Smith et al. (2008) who explain that choice of a particular approach is often driven by many different factors, like research constraints (both practical and theoretical) or situational circumstances.

3.4 Research Strategy

The research strategy is a general plan which allows the researcher to meet the aims and objectives of his study and to provide a reliable answer to the research question (Cooper and Schindler, 2014). Saunders et al. (2009) explain that while there are many different strategies available for the researcher (experiment, case study, grounded theory, etc.), “no research strategy is inherently superior or inferior to any other” and “what is most important is not the label that is attached to a particular strategy, but whether it will enable you to answer your particular research question.” (Saunders et al., 2009, p. 141). In the context of this study, selected research strategy can be described by two key features: time dimension of the study and form of the research data.

3.4.1 Time Dimension of the Study

The purpose of this thesis, as described earlier in the chapter, is to determine whether there is a relationship between certain negative events occurring in Bitcoin ecosystem (social and technical incidents) and its price. To meet the established objectives, this study uses the cross-sectional research strategy.

While the lack of a time dimension doesn't allow this strategy to establish causal inferences between analysed variables (Saunders et al., 2009), this limitation does affect this particular study from reaching its objectives. According to Rindfleisch, Malter, Ganesan and Moorman (2008), the cross-sectional strategy can be effectively used to determine the correlation between different variables. Saunders et al. (2009) agree that such approach gives the researcher simple means to determine the difference between variables based on their existent characteristics. Authors underpin that cross-sectional research method is found to be particularly useful in business studies to measure a specific phenomenon in a time- and cost-effective manner.

While the data collected for the purpose of this research reflects measurements taken only at a single point in time, the availability of historical data allows performing analysis of relevant events retrospectively. As highlighted by Oler, Oler and Skousen

(2010) this approach is especially effective and therefore popular in financial research studies where access to archive information is relatively effortless.

3.4.2 Form of the Research Data

While the research strategy is independent of the method of data collection, the form of that data determines the type of the approach which can be categorised as either quantitative or qualitative (Yin, 2014). Since this study focuses strongly on financial, numerical data, it inherently requires the former approach. Although both strategies can be considered as complementary to each other (Saunders et al., 2009), many authors are of the opinion that differences between them go beyond the form of data or research techniques (Trochim and Donnelly, 2006).

Bryman (1984) points out that differences between those two traditions emerge from the epistemology of learning, thus have a philosophical rather than methodological background. Quantitative paradigm postulates that knowledge is found, as usually assumed in deductive approach (Bryman, 1984) and that reality can be accurately and reliably measured with the use of scientific methods (Onwuegbuzie and Leech, 2005). In contrast, qualitative tradition considers knowledge to be constructed, as usually assumed in inductive approach (Bryman, 1984), and believes that interpretation of the reality is often very subjective since different individuals may have different perception of events and the measure of reality is greatly influenced by researcher's values (Onwuegbuzie and Leech, 2005).

However, Trochim and Donnelly (2006) argue that generalising qualitative strategies as exploratory and inductive or quantitative strategies as explanatory and deductive is tendentious and misleading. Authors underpin that many quantitative studies can be classified as exploratory as much as qualitative methods can often be used to test deductive hypotheses. While the author of this thesis believes that both strategies could be effectively applied to provide answers for the main research question, decision to choose a particular strategy was dictated by technical rather than philosophical reasons.

Although this thesis applies statistical methods of analysis of numerical data, some elements of qualitative methods were used to collect and analyse the research samples. Creswell and Plano-Clark (2007) claim that no study is ever purely qualitative or quantitative. According to authors, both methods share the same structure and address the same elements of the study, and that the difference between them is only reflected in the method of how each step is implemented. Quantitative research relies strongly on the literature review which is used to identify the purpose of the study and to guide the main research question. It helps the researcher to narrow down the hypotheses and identify specific variables on which the study should focus (Creswell and Plano-Clark, 2007).

The intent of the quantitative research is to provide accurate measurement of research variables, their relationships or characteristics. Therefore it strongly relies on numerical data (Cooper and Schindler, 2014). The connection between theory and reality is usually formed through statistical analysis of collected data, for which conclusions are based on evidence, argument and logic (Trochim and Donnelly, 2006).

The interpretation of quantitative data follows specific guidelines which aim to assure the validity of tested instrument as well as help to evaluate the research findings (Creswell and Plano-Clark, 2007).

3.5 Research Methods

Research methods describe the techniques and procedures that researcher applies to collect and analyse research data (Saunders et al., 2009). Although research methods are fundamentally linked to the research strategy, which determines the type of data and techniques applied to analyse that data during the research process, it is considered that form of data is not limited by any particular strategy (Yin, 2014). Therefore, there are many different methods and tools available for the researcher to conduct any given study (Cooper and Schindler, 2014). This section of “Research Methodology” chapter will detail the techniques of data collection, sampling and analysis used for this particular study.

3.5.1 Data Collection

As described earlier in the chapter, this study employs a quantitative strategy to address the main research question. Since the objective of this research is to perform event-driven analysis of Bitcoin price, the archival method of collection of secondary data was determined to be the most effective for this type of study. According to Saunders et al. (2009), archival research is especially useful in explanatory studies as it allows to analyse past events and study changes that occurred over the extended period of time. Oler et al. (2009) emphasise that archival method of data collection is found to be the most common technique employed in financial studies. Authors explain that it is considered to be the most objective since it is unobtrusive, non-reactive and allows the research to be easily replicated.

Due to the specifics of the research topic and the requirements of the research design, this study is based purely on secondary data. According to Saunders et al. (2009), this approach is often used when the collection of primary data is uneconomical or simply impossible. In the context of research methods, secondary data refers to results of earlier studies that were performed by other authors for different purposes (Cooper and Schindler, 2014), variety of other written documents, including books, journals, articles, public records etc. (Bryman, 1989) as well as Internet-based electronic data (Benfield and Szlemko, 2006). Saunders et al. (2009) argue that secondary data can often offer better quality than data collected from primary sources and is much less expensive to acquire. However, authors underpin that researcher needs to take into consideration ethical issues related to the use of data originally collected for different purposes as well as the potential bias related to the nature of that data.

To fulfil the objectives of the study, two separate sets of data had to be collected for analysis. The first dataset consists of Bitcoin price information for the period between 1st of January 2011 and 17th of August 2016. Raw data containing daily Bitcoin Price Indices was exported from CoinDesk (www.coindex.com) – web portal providing news and price data for digital currencies.

The second dataset represents relevant events, notably security incidents, which occurred in Bitcoin ecosystem between 2011 and 2016. List of Bitcoin events was compiled from multiple sources including journal articles as well as internet-based news items and posts on Bitcoin community forums. A search conducted via Google Engine included phrases such as: “*Bitcoin incident*”, “*Bitcoin security breach*” and “*Bitcoin disaster*”. The minimum level of details required for any result to be considered valid included: date of occurrence, type of incident and incurred loss. The rationale for selecting particular events is provided in the section that follows.

3.5.2 Research Sample

Saunders et al.(2009), as well as Cooper and Schindler (2014), emphasise the importance of selecting correct sampling procedures for any given research project. As explained by Saunders et al. (2009), research sample represents a selected part of the population which is tested by the researcher in an attempt to provide the answer to certain research questions and to fulfil predefined research objectives. In such context, population describes a full set of cases that are being studied and therefore may not necessarily relate only to people, but also products or services.

In the context of this study, population describes negative events that ever affected the Bitcoin ecosystem. Due to practical limitations, this study focuses only on selected cases as the collection of the data from the entire population was not achievable due to a number of different constraints (limited funds, time and access restrictions). According to Saunders et al. (2009) examining small sample allows the researcher to generalise results and extrapolate them onto full set of cases. In fact, as indicated by authors, many researchers suggest that working with samples allow to perform much more detailed analysis of the problem and may, therefore, provide more accurate results than a study conducted on the entire population.

Due to the nature and requirements of this research project, non-probability sampling method was applied to select the study cases. As described by Cooper and Schindler (2014) such selection process is somehow subjective, usually relies on some specific pattern, and therefore limits the validity of the statistical study. In contrast, probability sampling method is based on a principle of 'random selection', where each element of the population has an equal chance of being selected, and therefore allows the researcher to perform statistical analysis of the population's characteristics. However, Saunders et al. (2009) argue, that non-probability method is often adequate for statistical analysis, specifically when research sample represents the studied problem.

The samples collected for this particular research represent incidents which occurred in Bitcoin ecosystem and lead to noticeable financial loss, set at a minimum of 10,000 USD. However, this study disclaimed any incidents resulting from personal loss of bitcoins where no third party was involved, like loss of private key, regardless of the loss associated.

Due to the context of this study, social factors were also taken into account in the selection process. The research considered only those events that were reported by media or were actively discussed on public Bitcoin community forums.

3.5.3 Data Analysis

This study is an event-driven analysis of Bitcoin price, and specifically its volatility, that applies the inferential statistical analysis of collected data to test the research hypothesis. The objective of this study is to determine whether the negative events occurring in Bitcoin ecosystem affect its price volatility.

Bitcoin price volatility is calculated from raw data consisting of daily open and close prices. It is represented by standard deviation of Bitcoin intraday returns for a given period, calculated as:

$$x=\frac{p_c-p_o}{p_o}, \quad \sigma=\sqrt{\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n-1}}$$

$$
\begin{aligned}
&, where:\\
&p_o - daily\, open\, price\\
&p_c - daily\, close\, price\\
&\sigma - Standard\ Deviation(variance)\\
&n - number\, of\, days\, for\, which\, variance\, is\, measured(period)\\
&x_i - each\, individual\, intraday\, return\\
&\bar{x} - mean\, of\, the\, intraday\, return\, values
\end{aligned}
$$

Variables used for this study represent Bitcoin price variance calculated for 7, 14 and 28 days before and after each negative event has occurred. According to Kirkpatrick and Dahlquist (2010), those three different time windows (1, 2 and 4 weeks) are often used in technical analysis of financial data.

To reach the objective set for this study, two main tests will be performed on the research data. First, the Pearson's product-moment correlation test will be used to determine the relationship between the variables. According to Myers, Well and Lorch (2010) this test generates a coefficient (called the Pearson correlation coefficient “r”) which measures the strength and direction of a linear relationship between two continuous variables.

The second test, the paired-samples t-test, will be used to analyse the difference between variables, notably Bitcoin price volatility measured before and after each negative event takes place. As explained by Myers et al. (2010), this test is used to determine whether the mean difference between paired observations is statistically significantly different from zero. From the specific perspective of this study, a result of the paired-samples t-test will indicate if negative events have any effect on Bitcoin price volatility.

It is also important to mention that both Pearson's correlation test and paired-samples t-test assume linearity and normality of the analysed data (Myers et al., 2010). Therefore, in that consideration, those two additional tests will be used as a prerequisite for further analysis.

3.6 Limitations

One of the limitations of this study is the sampling method applied in the research, as well as the size of the analysed sample. The author recognises that this limitation does not allow to generalise research results statistically as they may be biased.

Another limitation of this study is its relatively narrow focus on raw price volatility. The architecture of Bitcoin system opens an opportunity to study its price changes in much wider context, for example by taking into account trading volume or available liquidity. As a result, the author believes that the research findings will lack the deep understanding of the Bitcoin market dynamics and that there is scope for further research to be carried out on this topic.

3.7 Ethical Considerations

Business research, like any other aspect of business activities, requires that all involved parties follow strong moral and ethical norms. "Ethics are norms or standards of behaviour that guide moral choices about our behaviour and our relationships with others. The goal of ethics in research is to ensure that no one is harmed or suffers adverse consequences from research activities." (Cooper and Schindler,2014, p. 28). In the context of this work, research ethics relates to the data collection methods and subsequent write-up of research conclusions.

According to Saunders et al. (2009), the archival method of data collection, which is used for the purpose of this study, requires the researcher to take into account the original intent for which the information was acquired. This research was based solely on publically available data, and any personal information attached to collected study cases was removed from analysed dataset.

Ethical considerations have also been taken into account during the write-up of the final chapter. The author recognises that Bitcoin community is especially influenced by the publicity, as explained by Kristoufek (2013, 2015). Therefore it is important to underpin that this study drew the conclusions from objective analysis of available information.

3.8 Summary of the Research Methodology

The purpose of this thesis is to analyse the relationship between various types of incidents affecting Bitcoin ecosystem and the price of this virtual currency. It takes a deductive approach and uses rigid scientific methods to test the hypothesis developed through the review of the topic-specific literature.

This research uses quantitative, cross-sectional strategy to provide an answer to the main research question by analysing the characteristics of numerical financial data. This data, categorised as secondary data, represents Bitcoin price information and is acquired through the archival method of data collection.

The main analysis of the research data, selected via non-probability sampling method, uses Pearson's correlation test and paired-samples t-test to measure the correlation between tested variables and determine the difference between them. The result of this inferential statistical analysis will decide whether the research hypothesis is accepted or rejected.

This chapter has explained in details the methodological approach chosen for this study, provided the rationale for research methods applied, and outlined the design of the research. It also explained the limitations of this study and discussed its ethical considerations. The details the data analysis process and research results will be presented in next chapter.

CHAPTER IV

RESULTS AND ANALYSIS

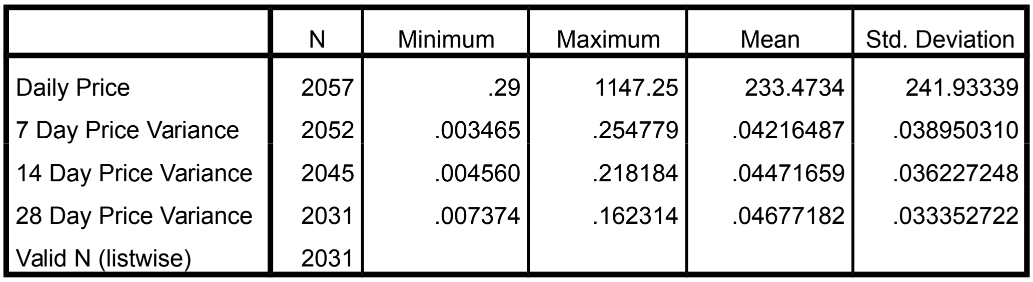
The objective of this research was to identify the correlation between tested variables, notably the calculated Bitcoin price variance before and after selected negative events, as well as to test the evidence of the difference between them. To provide reliable results, the variables were calculated for three different timeframes – short (7 days), medium (14 days) and long (28 days). This chapter will describe the process of data analysis and present the final results of this study. Firstly, it will provide an overview of the measured data, and secondly it will present results of relevant statistical tests, which were described in previous chapter.

4.1 General Characteristics of The Research Data

The data used for this research consists of two separate datasets – *Bitcoin Price Data* and *Bitcoin Negative Events List.* The first dataset was used to calculate relevant research variables, notably Bitcoin price volatility, while the second dataset represents relevant cases used to test the hypothesis stated in the second chapter. General characteristics of both datasets are presented below.

4.1.1 Bitcoin Price Data

The raw dataset of Bitcoin Price Indices used for this research includes 2057 consecutive samples representing Bitcoin daily close prices for the period between 1st of January 2011 and 17th of August 2016. Variables are calculated from raw price data resulting in 2031 valid measures. The data shows a significant difference in minimum and maximum values of Bitcoin daily prices as well as all corresponding calculated variables. While the maximum value of price volatility decreases with larger time ranges, their average values are in fact increasing, as presented in Table 1.



	N	Minimum	Maximum	Mean	Std. Deviation
Daily Price	2057	.29	1147.25	233.4734	241.93339
7 Day Price Variance	2052	.003465	.254779	.04216487	.038950310
14 Day Price Variance	2045	.004560	.218184	.04471659	.036227248
28 Day Price Variance	2031	.007374	.162314	.04677182	.033352722
Valid N (listwise)	2031				

Table 1: Descriptive Statistics of Bitcoin 5 year Price Data

High-level analysis of the Bitcoin data for the entire observed period shows the overall upward trend of daily prices, while the volatility displays strong tendency to decrease over time. This is clearly visible on below chart (Figure 1), which represents changes in Bitcoin daily price and its 7 days annualised volatility for the relevant period.

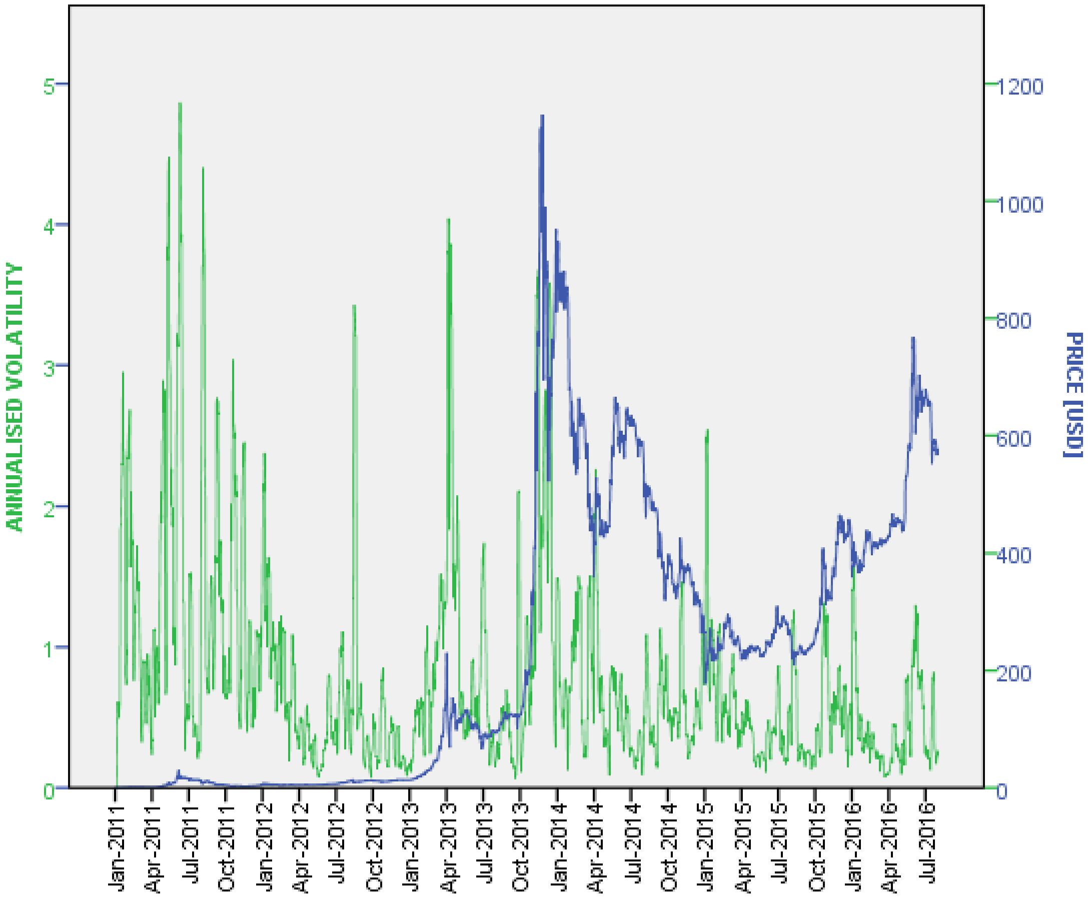


Figure 1: Bitcoin Daily Price and Volatility Chart

4.1.2 Bitcoin Negative Events

The second collected dataset represents negative events, namely incidents, which affected Bitcoin ecosystem in the observed period leading and resulted in a substantial direct financial loss for the users. Those incidents can be broadly categorised as (1) theft, (2) hack, (3) scam and (4) illicit use. A preliminary search was performed on Google Engine, and a total number of 6080 results were found. A detailed search was limited to documents that presented consolidated lists of Bitcoin incidents. From the overall search results, 42 different cases matched the criteria required for this study. Chronological list of relevant events is presented in Tables 2-4, while results of descriptive statistics is shown in Table 5.

Selected Events Between January 2011 and December 2012

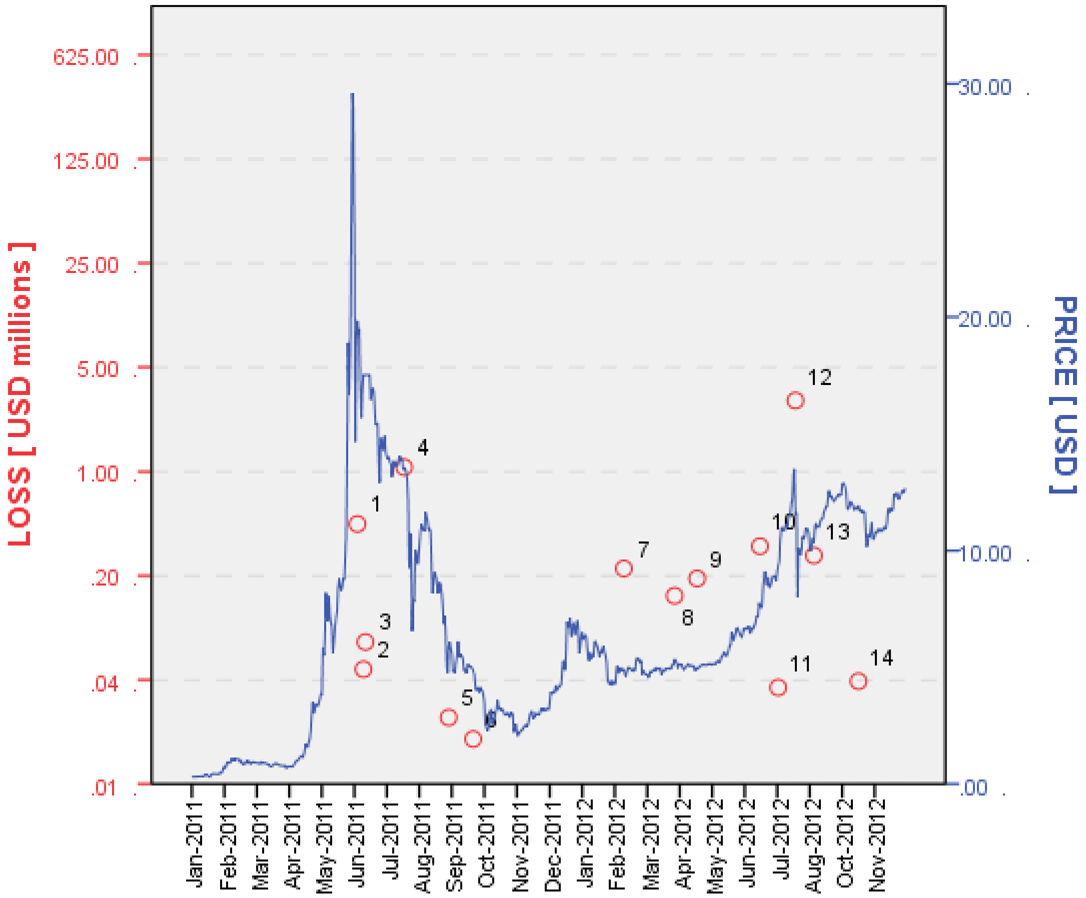


Figure 2: Bitcoin Price and Losses Chart (2011-2012)

Seq.	Date	*Type*	Name	Loss
1	2011-06-13	*Theft*	Allinvain Theft	$445,688
2	2011-06-19	*Hack*	Mt.Gox Incident	$47,123
3	2011-06-21	*Hack*	Mass MyBitcoin Thefts	$71,656
4	2011-07-29	*Theft*	MyBitcoin Theft	$1,072,570
5	2011-09-11	*Theft*	Mooncoin Theft	$22,346
6	2011-10-05	*Theft*	Bitcoin7 Incident	$15,980
7	2012-03-01	*Hack*	Linode Hacks	$223,278
8	2012-04-20	*Scam*	Tony Silk Road Scam	$146,944
9	2012-05-12	*Hack*	Bitcoinica Hack	$191,638
10	2012-07-13	*Hack*	Bitcoinica Theft	$315,133
11	2012-07-31	*Hack*	BTC-E Hack	$35,452
12	2012-08-17	*Scam*	Bitcoin Savings and Trust	$2,983,473
13	2012-09-04	*Theft*	Bitfloor Theft	$273,209
14	2012-10-18	*Hack*	Trojan	$39,146

Table 2: Selected Events 2011-2012

Selected Events Between January 2013 and December 2014

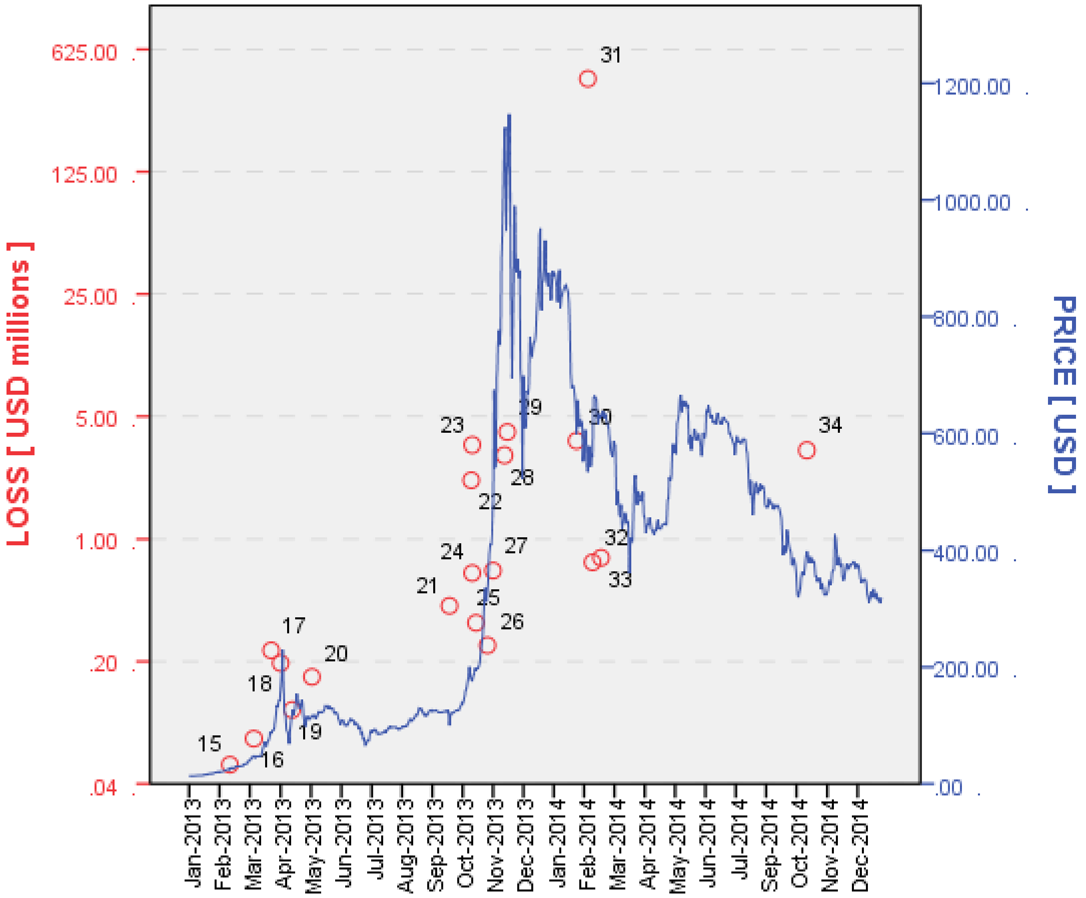


Figure 3: Bitcoin Price and Losses Chart (2013-2014)

Seq.	Date	*Type*	Name	Loss
15	2013-02-13	*Theft*	Bit LC Theft	$51,480
16	2013-03-10	*Theft*	BTCGuild Incident	$72,556
17	2013-03-28	*Scam*	Bitcoin Rain	$231,440
18	2013-04-07	*Scam*	ZigGap	$195,490
19	2013-04-19	*Hack*	Ozcoin Theft	$105,600
20	2013-05-10	*Theft*	Vircurex Theft	$163,351
21	2013-10-02	*Illicit*	1st Silk Road Seizure	$415,592
22	2013-10-25	*Illicit*	2nd Silk Road Seizure	$2,171,967
23	2013-10-26	*Scam*	GBL Scam	$3,437,446
24	2013-10-26	*Hack*	Inputs.io Incident	$640,615
25	2013-10-30	*Theft*	BASIC-MINING	$332,963
26	2013-11-11	*Hack*	Bitcash.cz Hack	$247,422
27	2013-11-17	*Hack*	BIPS Hack	$660,959
28	2013-11-29	*Hack*	PicoStocks Hack	$3,009,397
29	2013-12-02	*Theft*	Sheep Marketplace Incident	$4,070,923

Table 3: Selected Events 2013-2014

Selected Events Between January 2015 and August 2016

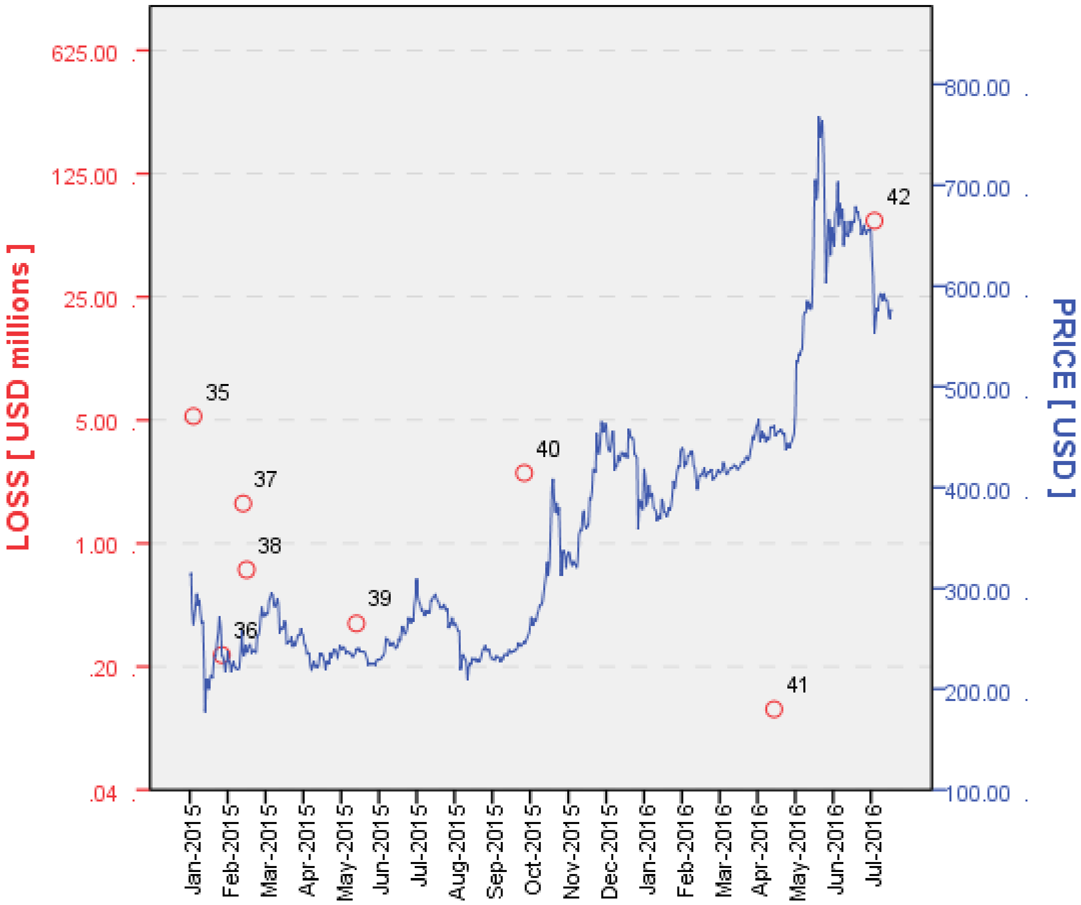


Figure 4: Bitcoin Price and Losses Chart (2015-2016)

Seq.	Date	*Type*	Name	Loss
30	2014-02-13	*Hack*	Silk Road 2 Incident	$3,624,866
31	2014-02-25	*Hack*	Mt.GOX Collapse	$405,000,000
32	2014-03-02	*Hack*	Flexcoin Theft	$738,240
33	2014-03-11	*Hack*	CryptoRush Theft	$782,641
34	2014-10-14	*Theft*	MintPal Incident	$3,208,412
35	2015-01-04	*Hack*	Bitstamp Hack	$5,263,614
36	2015-01-28	*Hack*	796 Hack	$233,210
37	2015-02-15	*Hack*	BTER Hack	$1,677,780
38	2015-02-18	*Hack*	KipCoin Hack	$708,630
39	2015-05-22	*Hack*	Bitfinex Hack	$350,918
40	2015-10-11	*Hack*	Purse.io	$2,507,575
41	2016-05-09	*Hack*	Gatecoin Incident	$114,675
42	2016-08-02	*Hack*	Bitfinex Theft	$67,662,140

Table 4: Selected Events 2015-2016

Incident Type	N	Minimum	Maximum	Median	Mean	Std. Deviation
Theft	11	15980	4070923	273209.00	884498.00	1408208.87
Hack	24	35452	405000000	495766.50	20593821.17	83010372.46
Scam	5	146944	3437446	231440.00	1398958.60	1661707.98
Illicit Use	2	415592	2171967	1293779.50	1293779.50	1241944.67
Overall (total)	42	15980	405000000	341940.50	12227703.29	62943953.03

Table 5: Descriptive Statistics of Selected Bitcoin Incidents

The complete list of all collected samples along with the detailed description of each event is included in Appendix A.

4.2 Detailed Analysis of The Research Data

This section outlines the research process and presents the results of the inferential statistical analysis of collected data. The primary objective of this study is to establish whether there is an observable difference in Bitcoin price volatility measured before and after the negative event takes place.

4.2.1 Test for Linearity

For each of 42 valid cases, reflecting Bitcoin negative events (incidents), three pairs of variables were calculated from raw price data. Those variables represent Bitcoin price volatility for 7, 14 and 28 day period before and after each event.

Analysis of linear relationship between variables, for each relevant pair, highlights some significant outliers present in measured samples (as shown in Figures 5-7).

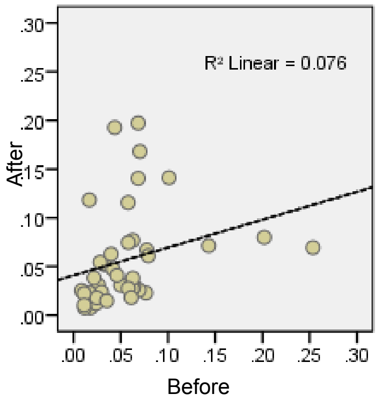


Figure 5: Scatter Chart
7 Day Price Variance Before and After Event

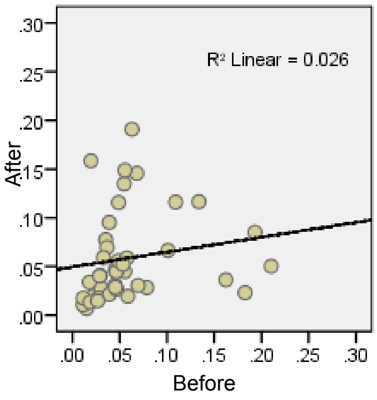


Figure 6: Scatter Chart
14 Day Price Variance Before and After Event

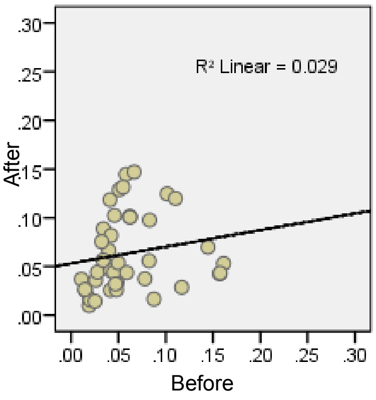


Figure 7: Scatter Chart
28 Day Price Variance Before and After Event

One of the assumptions of Pearson's correlation test is the linearity of the relationship between two continuous variables (Myers et al., 2010). To provide more reliable analysis of sample cases, as a measure of dealing with significant outliers, research data was extended to include a set of variables transformed by logarithmic function. According to Kirkpatrick and Dahlquist (2010) researchers often use such transformation for analysis of financial data.

Subsequent analysis of the data shows a linear relationship between transformed variables and lack of significant outliers (as presented in Figures 8-10).

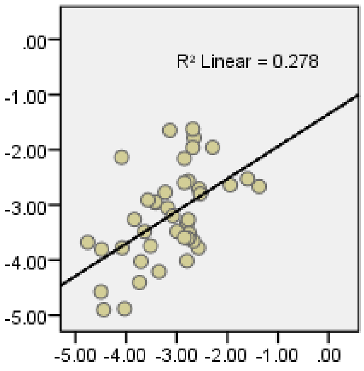


Figure 8: Scatter Chart
7 Day Price Ln(Variance) Before and After Event

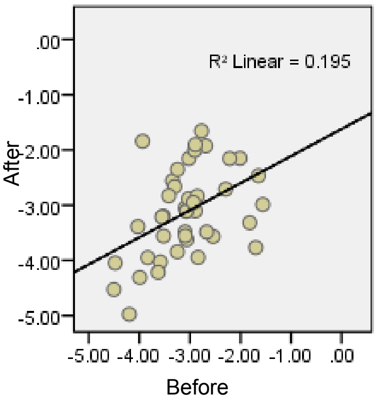


Figure 9: Scatter Chart
14 Day Price Ln(Variance) Before and After Event

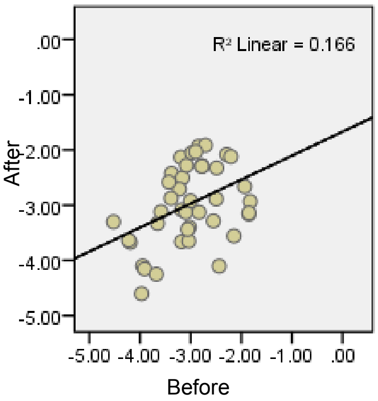


Figure 10: Scatter Chart
28 Day Price Ln(Variance) Before and After Event

The complete list of all variables and their values, calculated for each sample case, is included in Appendix B.

4.2.2 Test for Normality

The results of Shapiro-Wilk test of normality are listed in Table 6 (for non-transformed variables), and Table 7 (for transformed variables). The null hypothesis associated with this test assumes normality of the measured sample.

Price Variance		Kolmogorov-Smirnov			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Before Event	7 Day	0.225	42	0.000	0.738	42	0.000
	14 Day	0.249	42	0.000	0.767	42	0.000
	28 Day	0.193	42	0.000	0.863	42	0.000
After Event	7 Day	0.177	42	0.002	0.812	42	0.000
	14 Day	0.187	42	0.001	0.856	42	0.000
	28 Day	0.169	41	0.005	0.913	41	0.004

Table 6: Test of Normality Results for Price Variance

Price Ln(Variance)		Kolmogorov-Smirnov			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Before Event	7 Day	0.148	42	0.021	0.964	42	0.201
	14 Day	0.109	42	0.200	0.970	42	0.332
	28 Day	0.094	42	0.200	0.978	42	0.584
After Event	7 Day	0.086	42	0.200	0.979	42	0.615
	14 Day	0.079	42	0.200	0.984	42	0.811
	28 Day	0.109	41	0.200	0.960	41	0.156

Table 7: Test of Normality Results for Price Ln(Variance)

Test results indicate significant deviation from normality for all ranges of price variance (0.000<p<0.004). However, all transformed variables shows normal distribution (0.156>p>0.811). Detailed frequency histograms for each test are presented on Figures 11-18, listed in Appendix C.

It is important to mention that Pearson's correlation and paired-samples t-test assume a normal distribution of tested variables. However, according to Myers et al. (2010), both tests are considered to be fairly robust to deviation from normality and are often used even if not all variables are normally distributed, or when comparing tests performed on transformed and non-transformed variables. Results of those tests are presented below.

4.2.3 Pearson's Correlation Test

The null hypothesis of Pearson's test specifies that correlation coefficient is equal to zero (H_0: r=0). Test results of non-transformed variables, as shown in Table 8, indicate that there is no relationship between Bitcoin price variance for any of the measured periods before and after negative events (p>.078), thus the null hypothesis stands.

		7 Day Price Variance After Event	14 Day Price Variance After Event	28 Day Price Variance After Event
7 Day Price Variance Before Event	Pearson Correlation	.275	.229	.188
	Sig. (2-tailed)	.078	.145	.240
	N	42	42	41
14 Day Price Variance Before Event	Pearson Correlation	.201	.162	.140
	Sig. (2-tailed)	.202	.307	'.382
	N	42	42	41
28 Day Price Variance Before Event	Pearson Correlation	.154	.134	.148
	Sig. (2-tailed)	.331	.397	.355
	N	42	42	41

Table 8: Pearson's Correlation Test Results for Price Variance

However, test results of transformed variables, presented in Table 9, show a statistically significant relationship between them (.0005<p<.013) therefore we can reject the null hypothesis and accept the alternative hypothesis.

		7 Day Price Ln(Variance) After Event	14 Day Price Ln(Variance) After Event	28 Day Price Ln(Variance) After Event
7 Day Price Ln(Variance) Before Event	Pearson Correlation	.527	.512	.463
	Sig. (2-tailed)	.000	.001	.002
	N	42	42	41
14 Day Price Ln(Variance) Before Event	Pearson Correlation	.451	.442	.408
	Sig. (2-tailed)	.003	.003	.008
	N	42	42	41
28 Day Price Ln(Variance) Before Event	Pearson Correlation	.388	.399	.383
	Sig. (2-tailed)	.011	.009	.013
	N	42	42	41

Table 9: Pearson's Correlation Test Results for Price Ln(Variance)

The value of Pearson's correlation coefficient "r" indicates the strength of the association between transformed variables. Based on Ferguson's (2009) interpretation of the effect related to Pearson's coefficient, test results indicate a moderate relationship between transformed price variance measured on 7 day period before and after the negative event (r=.527). However, it is evident that this effect decreases for variances measured for longer periods (.512>r>.383).

4.2.4 Paired-Samples T-Test

The null hypothesis of paired-samples t-test specifies that the mean difference between two related variables is equal to zero (H_0: $\mu_{diff}=0$). Test results, presented in Table 10, indicate that there is no statistically significant evidence of a difference for any measured pair of variables, both non-transformed and transformed (.982>p>.618) and null hypothesis can not be rejected.

			Price Variance			**Price Ln(Variance)**		
			Pair 1	Pair 2	Pair 3	Pair 1	Pair 2	Pair 3
			7 Day After Event | 7 Day Before Event	14 Day After Event | 14 Day Before Event	28 Day After Event | 28 Day Before Event	7 Day After Event | 7 Day Before Event	14 Day After Event | 14 Day Before Event	28 Day After Event | 28 Day Before Event
Paired Differences	Mean		.00020400	-.00123520	.00365166	-.06015693	-.05511909	.05375240
	Std. Deviation		.05841688	.06167291	.05222648	.77674606	.80164289	.75255535
	Std. Error Mean		.00901392	.00951634	.00815641	.11985452	.12369618	.11752940
	95% Confidence Interval of the Difference	Lower	-.01799999	-.02045383	-.01283305	-.30220804	-.30492861	-.18378338
		Upper	.01840798	.01798344	.02013637	.18189419	.19469042	.29128818
		t	.02300000	-.13000000	.44800000	-.50200000	-.44600000	.45700000
		df	41	41	40	41	41	40
		Sig. (2-tailed)	.982	.897	.657	.618	.658	.650

Table 10: Paired T-Test Results

4.3 Summary of Data Analysis

Pearson's correlation test was used to determine whether there is a correlation between Bitcoin price volatility measured before and after the occurrence of certain negative events in its ecosystem. Price volatility was represented by variance in daily closing prices measured for three different periods. Also, a paired-samples t-test was used to determine whether those incidents had any effect on the observed volatility.

The relationship of measured variables was determined to be non-linear, and significant outliers were detected in samples. Therefore, a logarithmic transformation of variables was performed to assure reliability of data analysis. While the assumption of normality was not violated for transformed variables, as assessed by Shapiro-Wilk's test (p>.156), the non-transformed data was found to be significantly deviating from normality (p<.004).

Although no evidence of a relationship between non-transformed variables was found, as assessed by Pearson's test (p>.078), the transformed variables demonstrated weak to moderate association between them (.527>r>.383, p<.013). However, the paired-samples t-test did not provide any statistically significant evidence of a mean difference between tested variables, both non-transformed and transformed (.982>p>.618). Research results indicate that there is no observable change in Bitcoin price volatility before and after the negative event takes place. Therefore, the research hypothesis (H_1), which states that *negative events cause a change in price variance*, has to be rejected.

This chapter has provided an overview of the research data and described the process of data analysis. It also presented the final results of relevant statistical tests which will be discussed in a chapter that follows.

CHAPTER V

DISCUSSION AND CONCLUSIONS

The results of data analysis, provided in the previous chapter, rejected the hypothesis established in this study. This chapter will firstly discuss the research findings and offer a possible explanation of the results. Secondly, it will provide final conclusions of this study.

5.1 Discussion

The context of this research was formed on the earlier work of Kristoufek (2013; 2015) which suggests that social drivers have a strong effect on Bitcoin economy, and specifically its price and growth. It can be therefore assumed, that incidents occurring in Bitcoin ecosystem may directly affect its price volatility.

The review of the topic-specific literature, as presented in the first chapter of this thesis, shows that the nature of those incidents is heterogeneous and reflect different aspects of Bitcoin environment. Issues originate from both the technical vulnerabilities of the system (exploits, hacks, thefts) as well as from regulatory side (scam, fraud, illicit use). However, it can be argued that those different incidents share common social dimension due to the fact that Bitcoin ecosystem is formed primarily on the collective trust of the community (Sapuric and Kokkinaki, 2014). The purpose of this study was to provide an event driven analysis of Bitcoin price in relation to the negative events that affect its ecosystem.

The research findings indicate that there is a statistically significant directional relationship between price volatility measured before and after the negative event takes place. This seems to be in line with the findings of Kristoufek (2015) which suggest that the increase in the level of public attention towards Bitcoin, in this context caused by publicity around negative events, enhances the effects of its price appreciation or depreciation.

However, results of the analysis of Bitcoin price data indicate that there is no observable difference in price volatility measured before and after the incidents occur. As a consequence, the hypothesis that *negative events cause a change in price variance* has to be rejected. The author offers few possible explanations.

First, the opinion that Bitcoin economy is primarily influenced by social factors (Garcia et al., 2014; Kristoufek, 2015) is often argued by other authors. Glaser et al. (2014) suggest that majority of Bitcoin users consider it primarily as an asset for pure speculation. This type of investment may create specific pressure or resistance in price that is not influenced by social factors. According to authors, those investors often hold their assets to look for substantial returns and are not influenced by publicity related to Bitcoin ecosystem.

Also, Buchholz et al. (2012) are of the opinion that Bitcoin is mainly driven by supply and demand. As explained by Urbaniak (2013), Bitcoin's intrinsically limited supply and constantly increasing demand are strongly stimulating its price. As a result, Bitcoin overall price volatility is continuously decreasing, regardless of other external factors, including incidents and bad publicity. A high-level overview of research data, which included analysis of Bitcoin price volatility changes over 5 years period, indeed show strong tendency to decrease over time, as presented in Chapter 4 (Figure 1).

Second possible explanation relates to the fact that Bitcoin represents more than just a digital currency. Its unique underlying technology delivers tangible utility, allowing users to perform fast and secure peer-to-peer transactions, without the need for any third party (Papadopoulos, 2015). This stimulates Bitcoin organic growth which is evident through constantly increasing distribution of nodes and end-user addresses (Kondor et al., 2014). This growth is also strongly enhanced by Bitcoin potential in global e-commerce market (Turpin, 2014) in which it is also progressively adopted (Mishkin, 2014). As a result, Bitcoin formed exceptionally resilient socio-technical ecosystem (Morisse and Ingram, 2016), which may be able to resist effects of negative events.

Lastly, lack of an observable change in Bitcoin price volatility may be explained by the efficient-market hypothesis. This theory states that, at any time, the price of an asset reflect all available information. As the unique structure of Bitcoin system is based solely on the information instantly and transparently exchanged throughout the network, it could, therefore, be argued that the interests of all members of Bitcoin ecosystem, including both honest and dishonest users, are instantly reflected in its price. In this respect, Bitcoin value would preemptively adjust even before incidents are made public.

While the author of this thesis is not aware of any research done in the field, he strongly believes that this is an interesting area worth exploring.

5.2 Conclusions

Many authors argue that Bitcoin value is derived from public trust in this novel concept. It is, therefore, certain that frauds, scams or illicit use are not doing Bitcoin any favours. The lack of proper legislation for cryptocurrencies makes it vulnerable to misuse and does not offer enough comfort or protection for new Bitcoin users to adopt it (Turpin, 2014). Bad publicity around it may lead to its sudden price drops and eventual collapse (Perez and Urabaniak, 2015).

However, as proven empirically in this research, incidents occurring in Bitcoin ecosystem have little or no effect on Bitcoin price volatility. This could indicate that public trust in this system is growing regardless of its flaws. Whether this will allow it to succeed remains to be seen.

REFERENCES

Adams, G. and Schvaneveldt, J. (1991) *Understanding Research Methods*. 2Nd ed. New York: Longman.

Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014) 'Innovations in payment technologies and the emergence of digital currencies'. *Bank of England Quarterly Bulletin*, 54(3): pp. 262–275.

Amores, R. and Paganini, P. (2013) *Digital Virtual Currency and Bitcoins: The Dark Webs Financial Market -- Exchange & Secrets*. Sitz, North Charleston: CreateSpace Independent Publishing Platform.

Andrychowicz, M., Dziembowski, S., Malinowski, D., Mazurek, Ł. (2015) 'On the malleability of bitcoin transactions'. In: Brenner, M., Christin, N., Johnson, B. and Rohloff, K. (eds.). *Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable*. San Juan, Puerto Rico. January 30, 2015, pp. 1-18.

Bal, A. (2015) 'How to Tax Bitcoin?'. In: LEE Kuo Chuen, D. (ed.) *HANDBOOK OF DIGITAL CURRENCY : Bitcoin, Innovation, Financial Instruments, and Big Data.* London: Elsevier, pp. 267-282.

Barber, S., Boyen, X. and Shi, E. (2012) 'Bitter to Better—How to Make Bitcoin a Better Currency'. In: Keromytis, A. (ed.) *Financial Cryptography and Data Security.* London: Springer, pp. 399–414.

Beekman, J. G. (2016) 'A Denial of Service attack against fair computations using Bitcoin deposits'. *Information Processing Letters*, 116(2): pp. 144-146.

Benfield, J. A. and Szlemko, W. J. (2006) 'Internet-based data collection: Promises and realities'. *Journal of Research Practice*, 2(2): 1-1. [Online] Available at: http://jrp.icaap.org/index.php/jrp/article/view/30/51 [Accessed 9th August 2016]

BitcoinTalk (2014) *List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses* [Online] Available at: https://bitcointalk.org/index.php?topic=576337.0;all [Accessed 22nd July 2016].

BitcoinWiki (2016) *MyBitcoin* [Online] Available at: https://en.bitcoin.it/wiki/MyBitcoin [Accessed 12th August 2016].

Blockchain.info (2016) *Bitcoin Charts* [Online] Available at: https://blockchain.info/charts [Accessed 17th July 2016].

Böhme, R., Christin, N. and Edelman, B. (2015) 'Bitcoin: Economics, Technology, and Governance'. *Journal Of Economic Perspectives*, 29(2): pp. 213-238.

Bradbury, D. (2013) 'The problem with Bitcoin'. *Computer Fraud & Security*, 2013(11): pp. 5-8.

Bregas, F. and Bringas, P. (2012) 'Issues and risks associated with crypto currencies such as Bitcoin'. In: Berntzen, L. (ed.). *Second International Conference on Social Ecoinformatics 2012 (SOTICS 2012).* New York, USA. 2012, pp. 20–26

Brito, J., and Castillo, A. (2013) 'A primer for policymakers'. *Policy*, 29(4): pp. 3–12.

Bryman, A. (1989) *Research Methods and Organisation Studies*. London: Unwin Hyman.

Bryman, A. (1984) 'The Debate about Quantitative and Qualitative Research: A Question of Method or Epistemology?'. *The British Journal of Sociology*, 35(1): pp. 75-92.

Buchholz, M., Delaney, J., Warren, J. and Parker, J. (2012) *Bits and Bets Information, Price Volatility, and Demand for Bitcoin* [Online] Available at: http://www.bitcointrading.com/pdf/bitsandbets.pdf [Accessed 20th July 2016].

Buckley J.W., Buckley, M.H. and Chiang, H. (1976) *Research Methodology and Business Decisions*. New York: National Association of Accountants.

Cascarilla, C.G (2015) 'Bitcoin, Blockchain, and the Future of Financial Transactions'. *CFA Institute Conference Proceedings Quarterly*, 32(3): pp. 18-24.

Castronova, E. (2014) *Wildcat Currency: How the Virtual Money Revolution Is Transforming the Economy.* London: Yale University Press.

Christin, N. (2013) 'Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace'. In: Schwabe, D., Almeida, V., Glaser, H., Baeza-Yates, R. and Moon, S. (eds.). *Proceedings of the IW3C2 WWW 2013 Conference.* Rio de Janeiro, Brazil. May 13–17, 2013, pp. 213–224.

Cofnas, A. (2015) *The Forex Trading Course: A Self-Study Guide to Becoming a Successful Currency Trader.* New Jersey: John Wiley & Sons.

Coinbase (2016) *Bitcoin Price - Bitcoin Charts* [Online] Available at: https://www.coinbase.com/charts [Accessed 18th July 2016].

Coindesk (2015) *Details of $5 Million Bitstamp Hack Revealed* [Online] Available at: http://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/ [Accessed 22nd July 2016].

Coindesk (2016) *Gatecoin Claims $2 Million in Bitcoins and Ethers Lost in Security Breach* [Online] Available at: http://www.coindesk.com/gatecoin-2-million-bitcoin-ether-security-breach/ [Accessed 22nd July 2016].

Coinfox (2015) *Purse.io users' accounts compromised, hackers stole more than 10 BTC* [Online] Available at: http://www.coinfox.info/news/3348-purse-io-users-accounts-compromised-hackers-stole-10-235-btc [Accessed 22nd July 2016].

Coinfox (2015) *BTER exchange's cold wallet hacked, $1.75 mln in bitcoin stolen* [Online] Available at: http://www.coinfox.info/news/company/1426-birzha-bter-poteryala-1-75-mln-v-rezultate-vzloma-kholodnogo-koshelka-2 [Accessed 22nd July 2016].

Coinfox (2016) *Bitfinex hacked and put offline* [Online] Available at: http://www.coinfox.info/news/6088-bitfinex-is-hacked-and-put-offline [Accessed 2nd August 2016].

Cointelegraph (2015) *Chinese Exchange Gets 'Goxed' for 1,000 bitcoins (UPDATE: Company Responds)* [Online] Available at: https://cointelegraph.com/news/chinese-exchange-suffers-1000-btc-loss-in-uncertain-service-compromise [Accessed 22nd July 2016].

Collis, J. and Hussey, R. (2003) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students.* 2Nd ed. Basingstoke: Palgrave Macmillan.

Cooper, D. and Schindler, P. (2014) *Business research methods.* 12Th ed. New York: McGraw-Hill

Creswell, J.W. (2013) *Qualitative inquiry and research design: Choosing among five traditions.* London: Sage.

Creswell, J.W. and Plano-Clark, V.L. (2007) *Designing and conducting mixed methods research*. London: Sage.

Decker, C. and Wattenhofer, R. (2014) *Bitcoin transaction malleability and MtGox*. In: Kutylowski, M. and Vaidya, J. (eds.). *Proceedings of the 19th European Symposium on Research in Computer Security.* Wroclaw, Poland, September 7-11, 2014, pp. 313-326.

DeMartino, I. (2016) *The Bitcoin Guidebook: How to Obtain, Invest, and Spend the World's First Decentralised Cryptocurrency*. New York: Skyhorse Publishing.

Dowd, K. and Hutchinson, M. (2015) 'Bitcoin will bite the dust”, *Cato Journal,* 35(2): pp. 357-382.

Duskin, V. (ed.) (2014) *Virtual Currency and the Bitcoin Revolution: Perspectives and Considerations from Congressional Hearings*. New York: Nova.

ECB (2012) *Virtual Currency Schemes* [Online] Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [Accessed 15th January 2016].

Easterby- Smith, M., Thorpe, R. Jackson, P. and Lowe, A. (2008) *Management Research*. 3Rd ed. Sage: London.

FATF (2014) *Virtual Currencies Key Definitions and Potential AML/CFT Risks* [Online] Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf [Accessed 29th July 2016].

Ferguson, C.J. (2009) 'An Effect Size Primer: A Guide for Clinicians and Researchers'. *Professional Psychology: Research and Practice*, 2009, 40(5): pp. 532–538.

Garcia, D., Tessone, C.J., Mavrodiev, P. and Perony, N. (2014) 'The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy'. *Journal of the Royal Society Interface*. 11(99): pp. 1-8.

Garret, G. (2000) 'The causes of Globalisation'. *Comparative Political Studies*, 33(6/7): pp. 941-991.

Glaser F, Zimmermann K, Haferkorn M, Weber MC, Siering M. (2014) 'Bitcoin—Asset or currency? Revealing users’ hidden intentions', *Proceedings of the Twenty Second European Conference on Information Systems*, Tel Aviv, 15th April 2014, pp. 1-14.

Grant, G. and Hogan, R. (2014) 'Bitcoin: Risks and Controls'. *Journal Of Corporate Accounting & Finance,* 26(5): pp. 29-35.

Grinberg, R. (2011) 'Bitcoin: An innovative alternative digital currency'. *Hastings Science and Technology Law Journal*, 4(1): pp. 160–207.

Guadamuz, A. and Marsden, C. (2014) 'Bitcoin: The Wrong Implementation of the Right Idea at the Right Time'. [Online]. *SSRN*. Available at: http://dx.doi.org/10.2139/ssrn.2526736 [Accesed 22nd July 2016]

Hadnagy, C. (2011) *Social Engineering: The Art of Human Hacking*. Indianapolis: Wiley.

Ho, S.J. and Mallick, S.K. (2010) 'The impact of information technology on the banking industry'. *The Journal of the Operational Research Society*, 61(2): pp. 211-221.

Hurlburt, G. and Bojanova, I. (2014) 'Bitcoin: Benefit or Curse?'. *IT Professional*, 16(3): pp. 10-15.

Ingram, C., Morisse, M. and Teigland, R. (2015) '”A Bad Apple Went Away”: Exploring Resilience Among Bitcoin Entrepreneurs'. Research-in-Progress Papers, Münster: ECIS.

Jaag, C. and Bach, C. (2015) 'The Effect of Payment Reversibility on E-commerce and Postal Quality'. In: LEE Kuo Chuen, D. (ed.) *HANDBOOK OF DIGITAL CURRENCY : Bitcoin, Innovation, Financial Instruments, and Big Data.* London: Elsevier, pp. 139-152.

Johnson, B., Laszka, A. and Moore, T. (2014) ' Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools'. In: Böhme, R. Brenner, M. and Moore, T. (eds.) *Financial Cryptography and Data Security.* London: Springer, pp. 72-86.

Karame, G.O., Androulaki, E. and Roeschlin, M. (2015) 'Misbehaviour in Bitcoin: A Study of Double-Spending and Accountability'. *ACM Transactions on Information and System Security*, 18(1): pp. 1-40

Karami, M. and McCoy, D. (2013) *Understanding the emerging threat of ddos-as-a-service* [Online] Available at: https://www.usenix.org/conference/leet13/workshop-program/presentation/karami [Accessed 27th July 2016]

Kauffman, R. J. and Walden, E. A. (2001) 'Economics and electronic commerce: Survey and directions for research'. *International Journal of Electronic Commerce*, 5(4): pp. 5-116.

Kirkpatrick, C.D., and Dahlquist, J.A. (2010) *Technical Analysis: The Complete Resource for Financial Market Technicians*. London: Pearson.

Kondor, D., Posfai, M., Csabai I. and Vattay, G. (2014) 'Do the rich get richer? An empirical analysis of the Bitcoin transaction network'. *PloS one*, 9(2), pp. e86197.

Kristoufek, L. (2013) *BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era* [Online] Available at: http://dx.doi.org/10.1038/srep03415 [Accessed 19th July 2016].

Kristoufek, L. (2015) 'What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis'. *PLoS One*, 10(4): pp. 1-19.

Kroll, J.A., Davey, I.C. and Felten, E.W. (2013) *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries* [Online] Available at: http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf [Accessed 16th July 2016].

Krombholz, K., Judmayer, A., Gusenbauer, M. and Weippl, E. (2016) 'The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy?'. Pre-conference working paper., Vienna, Austria: SBA Research.

Lee, J., Long, A. and McRae, M. (2015) 'Bitcoin Basics: a Primer on Virtual Currencies'. *Business Law International*, 16(1): pp. 21-48,1-2.

Little, E.M. (2014) 'Bitcoin'. *The Investment Lawyer*, 21(5): pp. 22-26.

Ly, M. KM. (2014) 'Coining Bitcoin's "legal-bits": Examining the regulatory framework for Bitcoin and virtual currencies'. *Harvard Journal of Law and Technology*, 27(2): pp. 587–608.

Maftei, L. (2014) 'Bitcoin - Between Legal And Informal'. *CES Working Papers*, 6(3): pp. 53-60.

Mas, I. and LEE Kuo Chuen, D. (2015) 'Bitcoin-Like Protocols and Innovations'. In: LEE Kuo Chuen, D. (ed.) *HANDBOOK OF DIGITAL CURRENCY : Bitcoin, Innovation, Financial Instruments, and Big Data*. London: Elsevier, pp. 419-451.

McCallum, B.T. (2015) 'The Bitcoin Revolution'. *Cato Journal*, 35(2): pp. 347-356.

Myers, J. L., Well, A. D. and Lorch, R. F. (2010) *Research design and statistical analysis.* 3Rd ed. New York: Routledge.

Mishkin, S. (2014) *Small step for PayPal, one giant leap for magic internet money* [Online] Available at: http://blogs.ft.com/tech-blog/2014/09/small-step-for-paypal-one-giant-leap-for-magic-internet-money/ [Accessed 22nd July 2016].

Moore, T. and Christin, N. (2013) 'Beware the Middleman. Empirical Analysis of Bitcoin-Exchange Risk'. In: Sadeghi, A. (ed.) *Financial Cryptography and Data Security.* London: Springer, pp. 25-33.

Moore, T., Han, J. and Clayton, R. (2012) 'The postmodern ponzi scheme: empirical analysis of high-yield investment programs'. In: Keromytis, A.D. (ed.) *Financial Cryptography and Data Security.* Berlin: Springer, pp. 41-56.

Morisse, M. and Ingram, C. (2016) 'A Mixed Blessing: Resilience In The Entrepreneurial Socio-Technical System Of Bitcoin'. *Journal of Information Systems and Technology Management*, 13(1): pp. 3-26.

Nakamoto, S. (2009) *Bitcoin: A Peer-to-Peer Electronic Cash System* [Online] Available at: https://bitcoin.org/bitcoin.pdf [Accessed 17th January 2016].

Neguriaa, O. (2014) 'Bitcoin – Between Legal And Financial Performance'. *Contemporary Readings in Law & Social Justice*, 6(1): pp. 242-248.

NewsBTC (2015) *Chinese Bitcoin Exchange Kipcoin On Hold After Claims of Losing 3000 BTC to Hackers* [Online] Available at: http://www.newsbtc.com/2015/02/19/chinese-bitcoin-exchange-kipcoin-shuts-claims-losing-3000-btc-hackers/ [Accessed 22nd July 2016].

Oconnel, J. (2016) *Are Bitcoin Businesses Targets for Online Extortion?* [Online] Available at: https://www.cryptocoinsnews.com/are-bitcoin-businesses-targets-for-online-extortion/ [Accesed 24th July 2016].

Oler, D.K., Oler, M.J. and Skousen, C.J. (2010) 'Characterizing accounting research'. *Accounting Horizons*, 24(4): pp. 635-670.

Pacy, E.P. (2014) 'Tales from the Cryptocurrency: On Bitcoin, Square Pegs, and Round Holes'. New Englad Law Review, 49(1): pp. 121-144.

Paganini, P. (2013) *How to Profit Illegally from Bitcoin... Cybercrime and Much More* [Online] Available at: http://resources.infosecinstitute.com/how-toprofit-illegally-from-bitcoin-cybercrime-and-much-more/ [Accessed 21st July 2016].

Pagliery, J. (2014) *Bitcoin: And the Future of Money*. Chicago: Triumph Books LLC.

Pak Niam, L. and LEE Kuo Chuen, D. (2015) 'A Light Touch of Regulation for Virtual Currencies'. In: LEE Kuo Chuen, D. (ed.) *HANDBOOK OF DIGITAL CURRENCY : Bitcoin, Innovation, Financial Instruments, and Big Data.* London: Elsevier, pp. 309-326.

Papadopoulos, G. (2015) 'Blockchain and Digital Payments: An Institutionalist Analysis of Cryptocurrencies'. In: LEE Kuo Chuen, D. (ed.) *HANDBOOK OF DIGITAL CURRENCY : Bitcoin, Innovation, Financial Instruments, and Big Data.* London: Elsevier, pp. 153-172.

Pappalardo, D. and Messmer, E. (2005) *Extortion via DDoS on the rise* [Online] Available at: http://www.networkworld.com/article/2320986 [Accessed 23rd July 2016].

Perez, K. and Urbaniak, M. (2013) 'Bitcoin – Wirtualny Experyment czy Waluta Przyszlosci?'. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 2013(4): pp. 163-180.

Polasik, M., Piotrowska, A.I., Wisniewski, T.P., Kotkowski, R. and Lightfoot, G. (2015) 'Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry'. *International Journal Of Electronic Commerce*, 20(1): pp. 9-49.

Raibornand, C. and Sivitanides, M. (2015) 'Accounting Issues Related to Bitcoins '. *Journal of Corporate Accounting & Finance*, 26(2): pp. 25-34.

Raskin, M. (2015) 'Realm of the Coin: Bitcoin and Civil Procedure'. *Journal of Corporate & Financial Law*, 20(4): pp. 696-1011.

Reed Edge, K. (2014) 'The History of Money: From Cows to Bitcoin', *Tennessee Bar Journal*, 50(8): pp. 25-27.

Rindfleisch, A., Malter, A.J., Ganesan, S. and Moorman, C. (2008) 'Cross-Sectional versus Longitudinal Survey Research: Concepts, Findings, and Guidelines'. *Journal of Marketing Research*, 45(3): pp. 261-279
Ron, D. and Shamir, A. (2013) Quantitative analysis of the full Bitcoin transaction graph [Online] Available at: https://eprint.iacr.org/2012/584.pdf [Accessed 25th July 2016].

Ron, D. and Shamir, A. (2014) *How did Dread Pirate Roberts acquire and protect his Bitcoin wealth?* [Online] Available at: http://link.springer.com/content/pdf/10.1007%2F978-3-662-44774-1.pdf [Accessed 12th July 2016].

Sapuric, S. and Kokkinaki, A. (2014) 'Bitcoin is volatile! Isn’t that right?'. In: Abramowicz, W. and Kokkinaki, A. (eds.). *Business Information Systems Workshops, Lecture Notes in Business Information Processing*. Larnaca, Cyprus. May 22-23 2014, pp. 255–265.

Saunders, M., Lewis, P. and Thornhill, A. (2009) *Research Methods for Business Students.* 5th ed. Harlow: Pearson

SiliconAngle (2015) *Bitfinex Bitcoin exchange hot wallet hacked, estimated 1474 BTC stolen* [Online] Available at: http://siliconangle.com/blog/2015/05/24/bitfinex-bitcoin-exchange-hot-wallet-hacked-estimated-1474-btc-stolen/ [Accessed 22nd July 2016].

Taran, E.M., Salmanova, I.P. and Dokukina, E.V. (2015) 'Features of Using the Cryptocurrency'. *Asian Social Science*, 11(14): pp. 330-336.

Trautman, L. (2014) 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox'. *Richmond Journal of Law & Technology*, 20(4): pp. 1-108.

Trochim, W.M. and Donnelly, J.P. (2002) *Research methods knowledge base* [Online] Available at: http://www.anatomyfacts.com/research/researchmethodsknowledgebase.pdf [Accessed 4th August 2016].

Tropina, T. (2014) 'Fighting money laundering in the age of online banking, virtual currencies and internet gambling'. *ERA Forum*, 15(1), pp. 69–84.

Tschorsch, F. and Scheuermann, B. (2015) 'Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies'. *Cryptology ePrint Archive*, 2015(464): pp. 1-1.

Tu, K.V. and Meredith, M.W. (2015) 'Rethinking Virtual Currency Regulation In The Bitcoin Age'. *Washington Law Review,* 90(1): pp. 271-347.

Turpin, J.B. (2014) 'Bitcoin: The economic Case for a Global Virtual Currency Operating in an Unexplored Legal Framework'. *Indiana Journal of Global Legal Studies*, 21(1): pp.335-368.

Vasek, M. and Moore, T. (2015) 'There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams'. In: Böhme, R. and Okamoto, T. (eds.). *Financial Cryptography and Data Security: 19th International Conference.* San Juan, Puerto Rico. January 26-30, 2015, pp. 44-61.

Vasek, M., Thornton, M. and Moore, T. (2014) ' Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem'. In: Böhme, R. Brenner, M. and Moore, T. (eds.) *Financial Cryptography and Data Security.* London: Springer, pp. 57-71.

Wolfson, S.N. (2015) 'Bitcoin: The Early Market'. *Journal of Business & Economics Research*, 13(4): pp. 201-214.

Yermack, D. (2015|) 'Is Bitcoin a Real Currency? An Economic Appraisal'. In: LEE Kuo Chuen, D. (ed.) *Handbook Of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data.* London: Elsevier, pp. 31-43.

Yin, R.K. (2014) *Case study research: design and methods*. 5Th ed. London: Sage.

Young, J. and Natsios, D. (2012) *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity* [Online] Available at: http://cryptome.org/2012/05/fbi-bitcoin.pdf [Accessed 22nd July 2016].

Appendix A: List of Bitcoin Incidents

No	Source	Details	Description
1	BitcoinTalk (2014)	Allinvain Theft 2011-06-13 Theft $445,688	A polarizing theft, its authenticity has undergone much dispute. The victim was an early adopter who mined many coins at a low cost, so there is little reason for him to sabotage Bitcoin's image.
2	BitcoinTalk (2014)	Mt.Gox Incident 2011-06-19 Hack $47,123	Mt. Gox, then the leading BTC/USD exchange service, suffered a severe breach as a consequence of an ownership change. The sale conditions involved a share of revenue to be remitted to the seller. To audit this revenue, the seller was permitted an account with administrator access
3	BitcoinTalk (2014)	Mass MyBitcoin Thefts 2011-06-21 Hack $71,656	Users with weak passwords on MyBitcoin who used the same password on Mt. Gox were in for a surprise after the June 2011 Mt. Gox Incident allowed weakly-salted hashes of all Mt. Gox user passwords to be leaked. These passwords were then hacked on MyBitcoin and a significant amount of money lost.
4	BitcoinWiki (2016)	MyBitcoin Theft 2011-07-29 Theft $1,072,570	In terms of both dollars and bitcoins, this was by far the largest theft, however, it is possible it was simply a scam. The theft resulted in the closure of MyBitcoin, which was once a successful Bitcoin company in Bitcoin's early days.
5	BitcoinTalk (2014)	Mooncoin Theft 2011-09-11 Theft $22,346	During the waning months of 2011, numerous alternative cryptocurrencies boomed, in part fuelled by Bitcoin's poor performance following the 2011 bubble. Exchanges such as Moonco.in were set up to capitalize on this alternative cryptocurrency boom. Suddenly, Mr. Moon disappeared. It is not known where the funds went.
6	BitcoinTalk (2014)	Bitcoin7 Incident 2011-10-05 Theft $15,980	An upstart exchange at the time, Bitcoin7, rapidly grew to the third-largest USD exchange (behind then-leaders Mt. Gox and Tradehill) but then suffered a major debilitating hack, or so the official story goes. It is widely suspected that there was no hack and Bitcoin7's operators simply ran away with the funds.
7	BitcoinTalk (2014)	Linode Hacks 2012-03-01 Hack $223,278	In early March 2012, the New Jersey-based web and cloud hosting company Linode was suspected of robbing many popular Bitcoin services. A vulnerability in the customer support system was used to obtain administrator access to the servers. Once the Linode servers were compromised, eight accounts dealing with bitcoins were targeted. The hardest hit was the bitcoin trading platform, Bitcoinica.
8	BitcoinTalk (2014)	Tony Silk Road Scam 2012-04-20 Scam $146,944	Users of Silk Road, an underground drug market using Bitcoin as the default currency, bought significant quantities of illicit drugs from trusted vendor “Tony76”. Although Silk Road has an escrow system, trusted vendors are allowed to bypass the system and request that the buyers pay first. On April 20, which is a popular day for drug sales in American culture, Tony76 offered drugs at a significant discount. However, none of the products made it to the customers, revealing the sale as an elaborate sham.
9	BitcoinTalk (2014)	Bitcoinica Hack 2012-05-12 Hack $191,638	Zhou Tong, former founder of Bitcoinica, discovered an entry into Bitcoinica's Rackspace server through an excessively privileged compromised email address. This caused the theft of the entire “hot wallet”, funds stored on-site, as well as the loss of the main database. No backups were kept. Bitcoinica shut down because of this incident.
10	BitcoinTalk (2014)	Bitcoinica Theft 2012-07-13 Hack $315,133	Thief compromised the Bitcoinica Mt. Gox account. The thief made off with around 30% of Bitcoinica's bitcoin assets, which are likely to cost claimants of Bitcoinica debt. Additionally, 40000 USD was also reported to be stolen. The thief is still unknown at this point, but the theft has supposedly been entirely returned.

No	Source	Details	Description
11	BitcoinTalk (2014)	BTC-E Hack 2012-07-31 Hack $35,452	BTC-E Liberty Reserve API secret key was broken. This key was shorter than it needed to be at only 16 characters long. The attacker initiated many Liberty Reserve deposits and injected large amounts of USD into the system, which were quickly sold for BTC.
12	BitcoinTalk (2014)	Bitcoin Savings and Trust 2012-08-17 Scam $2,983,473	Bitcoin Savings & Trust, a virtual hedge fund that promised to pay high rewards to investors who parked their Bitcoins there
13	BitcoinTalk (2014)	Bitfloor Theft 2012-09-04 Theft $273,209	Although the keys to the hot wallet of Bitfloor was secured, an unencrypted backup was mistakenly stored on some of the servers. After a hacker gained entry, most of not only the hot wallet but also the cold wallet was stolen.
14	BitcoinTalk (2014)	Trojan 2012-10-18 Hack $39,146	A trojan horse stole thousands of BTC between September and November of 2012
15	BitcoinTalk (2014)	Bit LC Theft 2013-02-13 Theft $51,480	This alleged theft was unique in that coins held in the hot wallet were safe, but coins held in a cold wallet compromised. The thief is not expected to have access to the coins regardless, so there was little financial gain from this theft. Erick, allegedly the only one with physical access to Bit LC Inc.'s cold wallet, has failed to communicate and withdraw coins. Bit LC Inc. therefore was required to declare bankruptcy. There is no proof that Erick intentionally stole the coins; indeed, some evidence asserts that he or she may simply have disappeared in some manner.
16	BitcoinTalk (2014)	BTCGuild Incident 1899-12-30 0 $0	When BTCGuild was upgrading the Bitcoind client to 0.8, the mining pool used its original upgrade plan. However, 0.8 is unique in that it reindexes the blockchain. This prompted a temporary state in which the pool was paying out for difficulty-1 shares, as that was the extent of the blockchain parsed. Sixteen separate thieves subsequently emptied the hot wallet. 47 BTC have been returned to the pool. The pool would on the following day lose even more money thanks to a bug causing its recent upgrade to 0.8 to differ from nodes running 0.7 or lower.
17	BitcoinTalk (2014)	Bitcoin Rain 2013-03-28 Scam $231,440	A suspected long-running con likened to the infamous Bitcoin Savings and Trust, Bitcoin Rain finally defaulted on March 28, 2013. Leandro César claimed there was a security breach on his exchange website Mercado Bitcoin.[52] As Bitcoin Rain's funds were stored there, investors in Bitcoin Rain as well as account holders on Mercado Bitcoin lost money.
18	BitcoinTalk (2014)	ZigGap 2013-04-07 Scam $195,490	User aethero, who was originally a reputable Bitcoiner, founded ZigGap after two previously succesful ventures, including BitPantry. Purporting to offer easy ways to purchase BTC, ZigGap saw little business.
19	BitcoinTalk (2014)	Ozcoin Theft 2013-04-19 Hack $105,600	A hacker managed to infilterate Ozcoin's payout script, such that all money was paid out to the hacker's address. Luckily, a day later Strongcoin seized most of the stolen funds and promptly returned them to Ozcoin.
20	BitcoinTalk (2014)	Vircurex Theft 2013-05-10 Theft $163,351	The hot wallet and “warm” wallet of Bitcoin to alternative cryptocurrency exchange service Vircurex was emptied in May 2013, resulting in a significant loss of three currencies: Bitcoin, Terracoin, and Litecoin.[57] Initially, Vircurex operated normally despite the loss, though it no longer paid dividends to shareholders. In March 2014, due to strain caused by large withdrawals (in addition to a default by AurumXChange, a fiat processor Vircurex used), Vircurex froze large quantities of many currencies

No	Source	Details	Description
21	BitcoinTalk (2014)	1st Silk Road Seizure 2013-10-02 Illicit $415,592	Silk Road was a former underground marketplace that dealt primarily in Bitcoin. Run by Ross Ulbricht, it was once widely known for frequent narcotic sales. Although it operated under the jurisdiction of the United States, it made little attempt to comply with US law.However, clever use of the Tor technology allowed Silk Road to escape the authorities for years.
22	BitcoinTalk (2014)	2nd Silk Road Seizure 2013-10-25 Illicit $2,171,967	Finally, in October 2013, the FBI was able to produce conclusive evidence of Ross Ulbrict's culpability. Ulbricht was found in San Francisco and arrested.[69] In the days ensuing, it seized a large portion of Ulbricht's personal wealth in addition to stored balances by Silk Road users.
23	Wolfson (2015)	GBL Scam 2013-10-26 Scam $3,437,446	Beijing-based “GBL” was advertised as a Hong Kong-based exchange and shut down after attracting significant investment. At the time, there was a Bitcoin craze in China, which lasted for much of the latter half of 2013 and was credited as the leading cause of the November 2013 bubble.
24	Wolfson (2015)	Inputs.io Incident 2013-10-26 Hack $640,615	Web wallet service run by BitcoinTalk user TradeFortress, was supposedly “hacked” in October 2013 and was unable to repay user balances in full. There are many accusations of the hack being an inside job. TradeFortress had a contentious reputation and had supposedly scammed two separate people before this incident.
25	BitcoinTalk (2014)	BASIC-MINING 2013-10-30 Theft $332,963	Mining company BASIC-MINING took advantage of the ASIC boom to become a leading publically-traded mining company by early 2013. After the collapse of BTC-TC, the exchange on which it was traded, the founder disappeared with substantial assets.
26	BitcoinTalk (2014)	Bitcash.cz Hack 2013-11-11 Hack $247,422	A Czech Bitcoin exchange, bitcash.cz, reported a hack in mid-November 2013. The hack was relatively minor; however, Bitcoin prices were very high at the time relative to the preceding and succeeding months.
27	BitcoinTalk (2014)	BIPS Hack 2013-11-17 Hack $660,959	The then up-and-coming payment processor BIPS suffered a major breach in mid-November 2013, a month that saw numerous other companies shut down due to hacks. BIPS refused to refund creditors, justifying the loss as inevitable for a web wallet. BIPS made an attempt to continue business despite the hack.
28	BitcoinTalk (2014)	PicoStocks Hack 2013-11-29 Hack $3,009,397	PicoStocks, a stock exchange using a novel means of circumventing legal regulation, reported that someone that previously had access to PicoStocks keys used them to defund both hot and cold wallets. Creditors were reportedly unaffected as, despite the magnitude of the loss, PicoStocks covered it completely.
29	BitcoinTalk (2014)	Sheep Marketplace Incident 2013-12-02 Theft $4,070,923	Czech-based underground marketplace Sheep supposedly suffered a major breach causing the loss of 5400 BTC, which was passed down to its users. This official story is disputed, with many claiming the actual loss was far more severe. However, estimates of over 90000 BTC being stolen by the operator of Sheep were found to have accidentally tracked BTC-E internal wallet movements, thus discrediting this alternative explanation.
30	BitcoinTalk (2014)	Silk Road 2 Incident 2014-02-13 Hack $3,624,866	Defcon, an administrator at underground marketplace Silk Road 2 (not to be confused with Silk Road), noticed that funds held for the escrow service were stolen in February 2014. “Transaction malleability”, an issue with the Bitcoin protocol at the time that also affected some other services, was blamed for the theft.
31	Wolfson (2015)	Mt.GOX Collapse 2014-02-25 Hack $405,000,000	Mt. Gox goes offline without explanation. 850,000 bitcoins apparently stolen. (risk)

No	Source	Details	Description
32	BitcoinTalk (2014)	Flexcoin Theft 2014-03-02 Hack $738,240	Canadian-based Bitcoin "bank" Flexcoin reported a security breach causing the loss of most hot wallet funds, thanks to a race condition.
33	BitcoinTalk (2014)	CryptoRush Theft 2014-03-11 Hack $782,641	Cryptocurrency exchange cryptorush.in suffered a security breach leading the the loss of almost 1000 BTC and a significant amount of other cryptocurrencies such as Litecoin.
34	BitcoinTalk (2014)	MintPal Incident 2014-10-14 Theft $3,208,412	Cryptocurrency exchange MintPal was abruptly shut down by Moopay executive "Alex Green", which may be a pseudonym. The cold wallet was allegedly emptied by Green.
35	Coindesk (2015)	Bitstamp Hack 2015-01-04 Hack $5,263,614	Six employees of Bitstamp were targeted in a weeks-long phishing attempt leading up to the theft of roughly $5m in bitcoin in January, according to an unconfirmed incident report said to be drafted internally by the bitcoin exchange.
36	Cointelegraph (2015)	796 Hack 2015-01-28 Hack $233,210	According to the explanation, hackers had compromised areas of the exchange in the previous days, which had caused a user "to mention the current address has been tampered with, coupled with hackers deliberately [using] a similar address with the original withdrawals address to confuse users…"
37	Coinfox (2015)	BTER Hack 2015-02-15 Hack $1,677,780	The Chinese exchange BTAR also fell victim to cybercriminals in mid-February. The company suffered a loss of 7,170 BTC (roughly $1.75m) from its cold wallets as the result of a hacker attack. Clients' money was also compromised. However, BTER allowed reimbursing withdrawals in renminbi and virtual currencies other than bitcoin.
38	NewsBTC (2015)	KipCoin Hack 2015-02-18 Hack $708,630	KipCoin used to be a bitcoin exchange wallet service based in China. On February 18, the day of the Chinese Lunar New Year's Eve, a message was posted on their website stating that their wallet servers were hacked and that they had lost over 3000 BTC.
39	SiliconAngle (2015)	Bitfinex Hack 2015-05-22 Hack $350,918	Bitfinex, Hong Kong-based Bitcoin exchange operated by iFinex Inc. (Bvi), was hacked on Friday and has warned users to suspend bitcoin deposits until the potential compromise has been resolved. What's known so far back the hack is that hackers accessed the exchange's hot wallet and stole approximately 0.5% of the company's total held bitcoins.
40	Coinfox (2015)	Purse.io 2015-10-11 Hack $2,507,575	On 11 October 2015 several users of Purse.io, a P2P service provider that allows shopping on Amazon with bitcoin, suffered unauthorised withdrawal of funds from their accounts. The company admitted the fact of security breach, however, denying that any client funds were affected. Later the company published an update where it finally admitted that 11 user accounts were compromised and malefactors managed to steal 10,235 BTC. Purse.io claimed to have reimbursed all clients' funds.
41	Coindesk (2016)	Gatecoin Incident 2016-05-09 Hack $114,675	As reported on Friday, Gatecoin experienced a cyberattack on its hot wallets that resulted in the loss of funds. Gatecoin has claimed that it lost as much as 185,000 ethers and 250 bitcoins.
42	Coinfox (2016)	Bitfinex Theft 2016-08-02 Hack $67,662,140	The source of the vulnerability appears to lie in how Bitfinex structured its accounts and its use of bitcoin wallet provider BitGo as an additional layer of security on customer transactions.

Appendix B: Calculated Dataset

No	Date	Open Price	Close Price	Intraday Return	Annualised Volatility	7 Day Variance Before	14 Day Variance Before	28 Day Variance Before	7 Day Variance After	14 Day Variance After	28 Day Variance After
1	2011/06/13	18.55	19.84	0.069542	4.843116	0.253500	0.210319	0.161188	0.069373	0.050333	0.053103
2	2011/06/19	16.89	17.51	0.036708	1.462999	0.076577	0.182698	0.157062	0.022881	0.023126	0.042306
3	2011/06/21	17.51	17.51	0.000000	1.324626	0.069334	0.162314	0.157472	0.025846	0.036233	0.043263
4	2011/07/29	13.49	13.5	0.000741	0.320492	0.016775	0.019516	0.041092	0.118212	0.158369	0.118511
5	2011/09/11	4.77	5.86	0.228512	2.734820	0.143147	0.101111	0.082382	0.071298	0.066478	0.055730
6	2011/10/05	4.96	4.87	-0.018145	0.630215	0.032987	0.035321	0.082971	0.051861	0.077421	0.097539
7	2012/03/01	4.86	4.92	0.012346	0.505000	0.026433	0.045224	0.048652	0.030682	0.030649	0.033442
8	2012/04/20	5.14	5.35	0.040856	0.323924	0.016955	0.021646	0.019313	0.022855	0.019234	0.016540
9	2012/05/12	4.96	4.95	-0.002016	0.339758	0.017784	0.015002	0.018889	0.007561	0.006907	0.009998
10	2012/07/13	7.76	7.67	-0.011598	0.622877	0.032603	0.029344	0.025937	0.052634	0.040786	0.035851
11	2012/07/31	9.1	9.35	0.027473	0.412462	0.021589	0.029518	0.034099	0.038308	0.028523	0.088592
12	2012/08/17	13.5	11.58	-0.142222	1.343238	0.070308	0.048790	0.042259	0.168015	0.115665	0.081835
13	2012/09/04	10.53	10.38	-0.014245	0.565371	0.029593	0.027738	0.087513	0.023632	0.017806	0.016498
14	2012/10/18	11.81	11.94	0.011008	0.164154	0.008592	0.017810	0.015095	0.025254	0.033833	0.025365
15	2013/02/13	25.17	24.2	-0.038538	0.538924	0.028209	0.028635	0.027686	0.054427	0.040206	0.044205
16	2013/03/10	46.85	46	-0.018143	0.797495	0.041743	0.036704	0.039818	0.047238	0.069654	0.066573
17	2013/03/28	88.92	86.18	-0.030814	1.478883	0.077408	0.068011	0.058177	0.066891	0.145646	0.144667
18	2013/04/07	142.63	162.3	0.137909	1.306605	0.068391	0.062742	0.066573	0.197201	0.190754	0.147080
19	2013/04/19	109.01	118.48	0.086873	3.856550	0.201861	0.192950	0.144626	0.079812	0.085041	0.069698
20	2013/05/10	112.8	117.7	0.043440	1.173454	0.061421	0.078704	0.116920	0.035823	0.028246	0.028483
21	2013/10/02	125.49	99.81	-0.204638	1.512703	0.079178	0.055430	0.041705	0.060958	0.044858	0.045776
22	2013/10/25	183.15	178.12	-0.027464	1.217382	0.063721	0.045459	0.061980	0.029774	0.047451	0.101568
23	2013/10/26	178.12	175.9	-0.012464	1.190057	0.062290	0.046413	0.062194	0.027214	0.044611	0.100724
24	2013/10/26	178.12	175.9	-0.012464	1.190057	0.062290	0.046413	0.062194	0.027214	0.044611	0.100724
25	2013/10/30	198.19	194.55	-0.018366	0.955470	0.050012	0.048344	0.045776	0.030739	0.055833	0.102446
26	2013/11/11	311.9	332.63	0.066464	1.306393	0.068380	0.054714	0.050913	0.140493	0.134824	0.128866
27	2013/11/17	428.82	476.29	0.110699	0.833585	0.043632	0.055488	0.054991	0.192557	0.148743	0.131389
28	2013/11/29	1037.75	1120.4	0.079643	1.106662	0.057925	0.133799	0.101489	0.115607	0.116456	0.124674
29	2013/12/02	946.92	1038.35	0.096555	1.931912	0.101121	0.109155	0.110285	0.141027	0.115999	0.119747
30	2014/02/13	648.38	598.41	-0.077069	0.759158	0.039736	0.032753	0.033790	0.062693	0.059073	0.056408
31	2014/02/25	545.32	534.71	-0.019456	1.195106	0.062555	0.057605	0.045160	0.076731	0.058615	0.043852
32	2014/03/02	563.74	560.3	-0.006102	1.109899	0.058095	0.053350	0.049656	0.074504	0.052259	0.053742
33	2014/03/11	625.83	628.95	0.004985	0.457232	0.023933	0.058615	0.058721	0.012177	0.019354	0.043730
34	2014/10/14	388.38	398.71	0.026598	0.469481	0.024574	0.038856	0.041576	0.017862	0.021407	0.025676
35	2015/01/04	279.85	263.63	-0.057960	0.882208	0.046177	0.038974	0.032342	0.040824	0.095236	0.075509
36	2015/01/28	262.06	233.21	-0.110089	1.197890	0.062700	0.069320	0.077885	0.038054	0.030629	0.037361
37	2015/02/15	257.47	234.33	-0.089875	1.109280	0.058062	0.046797	0.048001	0.027564	0.026678	0.025991
38	2015/02/18	243.6	236.21	-0.030337	1.165813	0.061021	0.045405	0.046922	0.018021	0.028575	0.032126
39	2015/05/22	235.3	240.52	0.022184	0.225228	0.011789	0.011066	0.020013	0.007434	0.010801	0.015710
40	2015/10/11	245.33	247.53	0.008968	0.216197	0.011316	0.011369	0.010848	0.022202	0.017490	0.036846
41	2016/05/09	459.44	461.49	0.004462	0.213471	0.011174	0.018492	0.014632	0.010297	0.013463	0.026367
42	2016/08/02	607.37	552.82	-0.089813	0.671445	0.035145	0.026576	0.025301	0.014853	0.014733	

Appendix C: Variable Distribution Histograms

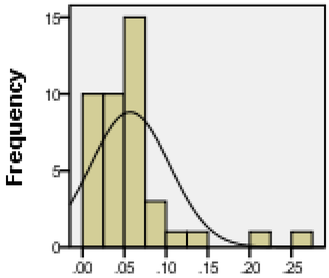


*Figure 11:Distribution Histogram
7 Day Variance Before Event*

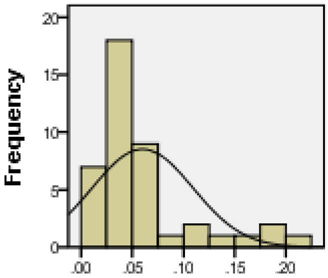


*Figure 12:Distribution Histogram
14 Day Variance Before Event*

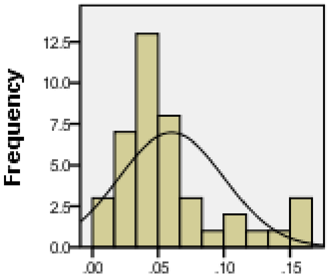


*Figure 13:Distribution Histogram
28 Day Variance Before Event*

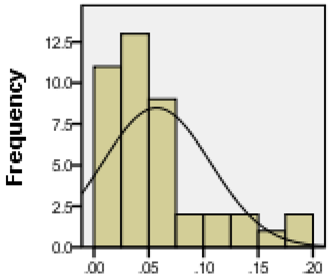


*Figure 14:Distribution Histogram
7 Day Variance After Event*

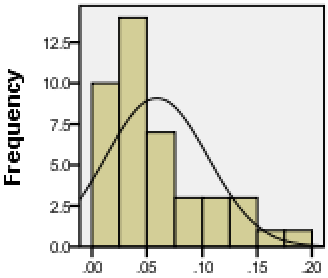


*Figure 15:Distribution Histogram
14 Day Variance After Event*

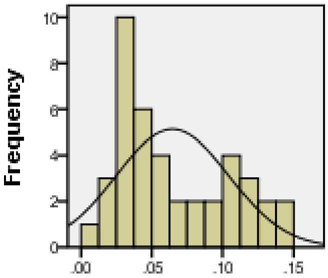


*Figure 16:Distribution Histogram
28 Day Variance After Event*

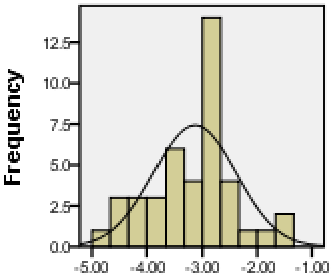


*Figure 17:Distribution Histogram
7 Day Ln(Variance) Before Event*

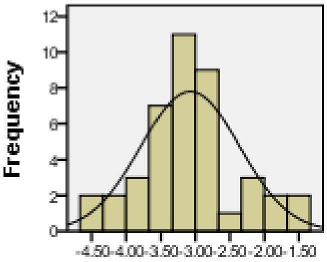


*Figure 18:Distribution Histogram
14 Day Ln(Variance) Before Event*

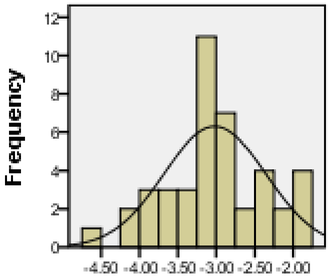


*Figure 19:Distribution Histogram
28 Day Ln(Variance) Before Event*

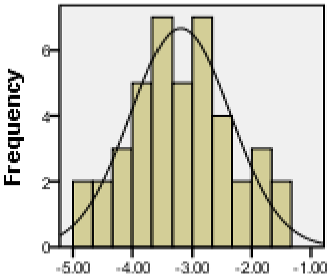


*Figure 20:Distribution Histogram
7 Day Ln(Variance) After Event*

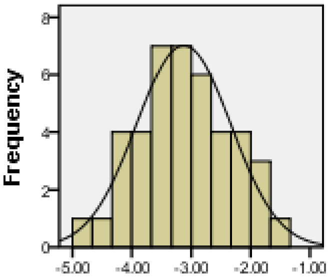


*Figure 21:Distribution Histogram
14 Day Ln(Variance) After Event*

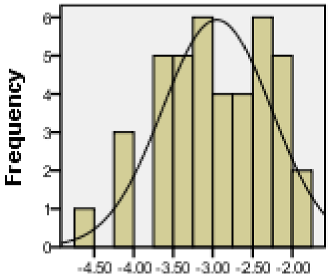


*Figure 22:Distribution Histogram
28 Day Ln(Variance) After Event*