

Charles University in Prague
Faculty of Social Sciences

Institute of Economic Studies



Master's Thesis

Exploring the Price Determinants of Bitcoin with Vector Autoregression

Author: Bc. Hugo Vozak

Program: International Economic and Political Studies

Supervisor: Ing. Oldřich Dědek CSc.


Academic Year: 2014/2015

Date of Submission: May 15th 2015

Declaration of Authorship

I, Hugo Vozak, hereby declare that this thesis is my own work, based on the sources and literature listed in the appended bibliography. The thesis as submitted is 127,507 keystrokes long including spaces, i.e. 54 manuscript pages excluding the initial pages, the list of references and appendices.

Prague, Czech Republic, 15.05.2015



Bc. Hugo Vozak

Acknowledgements

Foremost, I would like to express my sincere gratitude to Ing. Oldřich Dědek CSc. for accepting to undertake the adventure into uncharted territory that Bitcoin represents. I am truly thankful to PhDr. Ladislav Křištofuk Ph.D. for his insight on Bitcoin and most notably for the help and advice with the econometric analysis. Furthermore, I would like to thank Le Club Laval-sur-le-Lac for their indefectible moral and financial support during my Master's studies. Finally, I would like to salute Mr. Joseph C. Wang for his macroeconomic model, which influenced the course of this thesis.

Abstract

This thesis explores the price determinants of Bitcoin using a macroeconomic model based on the economic equation of exchange presented by Joseph Wang (2014). The thesis provides a concise and structured introduction to Bitcoin and a comprehensive literature review on Bitcoin. The analysis begins with the application of the functions of money to Bitcoin, arguing that while Bitcoin does fulfill the three classical functions of money to a certain extent, its use remains mainly as a speculative instrument. Wang's model is criticized and amended to reflect the realities of empirically analyzing the Bitcoin market. Using the daily number of transactions and Bitcoin days destroyed as proxies for economic activity and inactivity – to measure Bitcoin's velocity on the block chain – vector autoregression modelling is used to determine if there is Granger causality between the price of bitcoin and the two proxies. The results demonstrate that there is a bidirectional Granger-causal relationship between Bitcoin days destroyed and the price of bitcoin and that there is none between the daily number of transactions and the price of bitcoin; proving Wang's two main assumptions. Impulse-response functions are provided to illustrate and discuss this bidirectional relationship. The results are in line with the theoretical reasoning provided within the thesis. The main finding is that saving does have an impact on the price of bitcoin.

Keywords:

Bitcoin, price determinants, valuation, economic equation of exchange, classical functions of money, velocity of Bitcoin, Bitcoin days destroyed, Granger Causality, impulse-response functions

Master Thesis Proposal

Institute of Political Studies
Faculty of Social Sciences
Charles University in Prague

Date: 13.01.2014



Author:	Hugo Vozak	Supervisor:	Prof. Ing. Oldřich Dědek CSc.
E-mail:	hugo.vozak@mail.mcgill.ca	E-mail:	dedek@mbox.fsv.cuni.cz
Phone:	+0420 776 550 272	Phone:	
Specialisation:	IEPS	Defense Planned:	

Proposed Topic:

Bitcoin: Pyramid-scheme Wildfire, New Online Payment Medium or Future Alternative Currency?

Registered in SIS: YES

Date of registration: 16.01.2014

Topic Characteristics:

My thesis will focus on the Bitcoin, an online cryptocurrency that has gained increasing attention since its creation in 2008. This new form of virtual currency relies on a proof of work algorithmic system to 'mine' its bitcoins into existence. Designed to replicate the characteristics of gold (intrinsic value aside), bitcoins are not pegged to any real-world currency with their value determined through supply and demand mechanisms on Bitcoin exchanges. Unlike modern fiat-based currencies emitted through fractional-banking systems, the Bitcoin is not controlled by any central authority and remains an open-source system structured on decentralized peer-to-peer networking.

This topic is of particular interest to me given its contemporary, evolutionary nature, and the challenge that working on such a topic presents. My main aim is to present the Bitcoin in a comprehensive way, by shedding light on this emerging monetary scheme, and provide answers to the main inquiries people have on the Bitcoin.

I believe this research will be of significant importance to the field of alternative currencies primarily through its comprehensive assessment and application of monetary theory. Individuals in and outside of the field of economics will benefit from the concise explanations and analyses within my thesis as a foundation for potential future research developments in the field or simply obtaining an intelligible outline of the Bitcoin and its relation to monetary theory.

Hypotheses:

1. The Bitcoin will eventually replace fiat-based currencies in the long run while short run adoption will face recognition hurdles.
2. The Bitcoin can act as an alternative, parallel form of currency.
3. The Bitcoin is not a pyramid scheme, while early users will benefit immensely from early adoption (Bitcoin millionaires).
4. The Bitcoin will eventually become the main form of online payment methods (vs. PayPal, prepaid credit cards & other digital forms of payment).
5. The Bitcoin experiment is unlikely to fail when faced with the uncertain threat posed by regulatory bodies (unlike E-Gold and Liberty dollars), while its ever-changing, emerging issues with security puts its future in peril.

Methodology:

To further my aim and seek answers to my hypothesis(es), several steps will have to be undertaken. First, I will take on a theoretical approach based on Austrian Economics inspired primarily on the works of Eugen von Böhm-Bawerk, Ludwig von Mises and Friedrich A. Hayek, while taking into consideration accounts from contemporary critics such as Jon Matonis. I will also consider Modern Monetary Theory, the Cantillon Effect, and the Misesian Regression Theorem in relation to the Bitcoin. Through these theoretical applications, I hope to determine the Bitcoin's viability or non-viability as a currency for states (e.g. micronations) and whether it can be a form of alternative currency, running parallel to mainstream fiat currencies. I will expose the dangers and weaknesses of the Bitcoin, particularly its volatile and deflationary nature.

Furthermore, in providing a detailed and comprehensive assessment of the Bitcoin's functioning, I hope to establish how the Bitcoin is not a pyramid scheme and is a feasible transaction method for goods and services both virtual and real. It's structure could also reveal how it could become a new online payment medium stripped of the main hurdles current mediums impose on users.

Outline:

1. Introduction
2. Theoretical background, Austrian Economics and review of main literature and contemporary Bitcoin assessments
3. The Bitcoin
 - a. Functioning: algorithms, proof of work, mining, and wallets
 - b. Transactions: proof of work, exchanges
 - c. Control: Decentralized control, exchanges
 - d. Monetary aspects: supply, deflationary nature, anonymity
4. Applying Theory, Empirical Models
 - a. Austrian Economics (applicability)
 - b. Cantillon Effect
 - c. Misesian Regression Theorem
 - d. Inflation v. Deflation
 - e. Endogenous Money Theory
 - f. Macroeconomic model?
5. Content Analysis
 - a. TBD (Possibility of Macroeconomic model – waiting on confirmation from scholar).
 - b. Quantitative Analysis?
 - c. Discussion of the Results: linking the hypothesis(es) with the data
6. Conclusions
7. References / Bibliography

References / Bibliography:

- Friedman, M. (1994). *Money Mischief: Episodes in Monetary History*. San Diego: Harcourt Brace & Co.
- Hayek, F. A. von. (1994). *The Road to Serfdom* (50th anniversary edition). Chicago: University of Chicago Press.
- Hayek, F. A. von (1978). *Denationalisation of Money — The Argument Refined*. London: Institute of Economic Affairs.

Mises, L. von (1990). The Position of Money among Economic Goods. Alfred Zlabinger, trans. In idem, Money, Method, and the Market Process. Richard M. Ebeling, ed. Norwell, Mass.: Kluwer Academic Publishers.

Rossi, S. Rochon, L. (2003). Modern Theories of Money: The Nature and Role of Money in Capitalist Economies. Front Cover.

Table of Contents

1	Introduction	1
2	Bitcoin	4
2.1	Terminology and Usage.....	4
2.2	The Origins of Bitcoin.....	5
2.3	The Mechanics of Bitcoin.....	5
2.3.1	Decentralized Networking.....	6
2.3.2	Data Broadcasts: Transactions and Blocks	7
2.3.3	Mining: Bitcoin’s Money Supply.....	8
2.4	Bitcoin Usage	10
2.4.1	Acquiring and Storing Bitcoin	11
2.4.2	Bitcoin Exchanges and Buying Bitcoins	12
2.4.3	How are bitcoins priced?.....	12
2.4.4	Bitcoin’s Acceptance in Real-World Markets	13
3	Literature Review	14
3.1	Literature Review on Bitcoin	14
3.1.1	On Bitcoin’s Precursors	14
3.1.2	On the Mechanics of Bitcoin and Bitcoin Usage	16
3.1.3	On Bitcoin Regulation.....	19
3.1.4	On Bitcoin and Economics.....	20
3.1.5	On Other Graduate and Undergraduate Works	21
3.1.6	On Bitcoin and Econometrics	22
3.2	Relevant Theory	23
3.2.1	On the Functions of Money.....	23
3.2.2	On the Economic Equation of Exchange	26
3.2.3	Wang’s Macroeconomic Model for the Valuation of Bitcoin.....	27
4	Methodology.....	30
4.1	Hypotheses.....	30
4.2	Bitcoin and the Functions of Money	31
4.3	Macroeconomic Model for the Valuation of Bitcoin	31
4.4	Econometric Analysis.....	31
4.4.1	Data Selection and Collection	31
4.4.2	Software	36
4.4.3	Econometric Models	37

5	Analysis.....	39
5.1	Bitcoin and the Functions of Money	39
5.1.1	Bitcoin as a Medium of Exchange	39
5.1.2	Bitcoin as a Unit of Account.....	40
5.1.3	Bitcoin as a Store of Value.....	41
5.1.4	Is Bitcoin Money?	42
5.2	Amending Wang’s Macroeconomic Model	42
5.3	Econometric Analysis.....	44
5.3.1	Augmented Dickey-Fuller Test.....	45
5.3.2	VAR Lag Selection	46
5.3.3	VAR Results and Granger Causality.....	46
5.3.1	Impulse-Response Function: BPI to a shock in BDDC	48
5.3.2	Other Interesting Findings.....	50
6	Conclusion	52
7	References.....	55
8	Appendices	62
	Appendix 1: Elements of a Bitcoin Transaction	63
	Appendix 2: More on the BPI.....	64
	Appendix 3: Table of Exogenous Shocks	65
	Appendix 4: VAR Lag Selection Test Results	67
	Appendix 5: Other Impulse-Response Functions	68
	Appendix 6: Material Included on the CD.....	71

List of Tables

Table 1: Summarized ADF Test Results	45
Table 2: Summarized VAR Results.....	47
Table 3: Exogenous Shocks.....	65

List of Figures

Figure 1: Impulse-Response Function of BPI to BDDC	49
Figure 2: Impulse-Response Function of BDDC to BPI	50
Figure 3: VAR Lag Selection Test Results	67
Figure 4: Impulse-Response Function of TexR to BPI	68
Figure 5: Impulse-Response Function of TexR to MrkC	69
Figure 6: Impulse-Response Function of TexR to GT	70

List of Abbreviations and Acronyms

ADF	Augmented Dickey-Fuller (test)
AIC	Akaike information criterion
API	Application programming interface
BDDC	Bitcoin days destroyed cumulative
BPI	Bitcoin Price Index
BTC	A bitcoin
CPU	Central processing unit
DN _o T	Daily number of transactions
ExSh	Exogenous shocks
FPGA	Field programmable gate array
GPU	Graphics processing unit
GT	Google Trends
HashR	Hash rate
MrkC	Market capitalization of Bitcoin
P2P	Peer-to-peer
TexR	Trade-exchange ratio
TNBTC	Total number of bitcoins
USD	United States dollar

1 Introduction

Bitcoin is a nascent, virtual open-source currency system structured on a decentralized peer-to-peer network and operated under cryptographic rules and principles. Introduced in 2008, this new digital monetary scheme has recently gained substantial attention, which has resulted in increased usage and notable price volatility. Bitcoin has also garnered its share of negative media attention with its use on the online, illegal drug marketplace Silk Road and with the controversial closure of Mt. Gox, once Bitcoin's largest exchange. Academic interest has increased in recent years, yielding a plethora of novel studies and articles in a field that had previously been marginally explored since Bitcoin's inception. Scholarly interest helps to further people's understanding on Bitcoin's functioning and provides answers to queries about the future of virtual cryptocurrencies.

In February 2014, Joseph Wang (2014) proposed a new macroeconomic model for the valuation of Bitcoin. Modifying the economic equation of exchange to take into account the unique aspects of Bitcoin, Wang claims that "the value of bitcoin is determined largely by the willingness of bitcoin holders to save bitcoin and not by its transactional use." Therefore, the value of bitcoin should not increase with the spread of its use and acceptance, but rather increase with users' willingness to remove it from circulation by saving bitcoins. In other words, the "increased usage of Bitcoin should manifest itself in larger volumes rather than increased prices." Hence, in the long run, changes in the price of bitcoin will be influenced by external factors affecting the likelihood that a bitcoin is saved rather than by changes in the transactional use of Bitcoin, which should be reflected by changes in transaction volumes.

This thesis undertakes Wang's proposal and seeks to determine the validity of its claims by furthering and amending the proposed assumptions. Wang's model asserts that through empirical observation of the Bitcoin market, under a certain set of parameters, the price of bitcoin is determined by the likelihood that a given bitcoin will be saved. This thesis takes on the empirical observation of the Bitcoin market through readily available data and renders an econometric analysis based on two hypotheses:

H₁: The price of bitcoin is not influenced by changes in the trade volume.

H₂: The price of bitcoin is determined by the likelihood that a bitcoin will be saved.

To assess both of the hypotheses, an econometric analysis of the Bitcoin market is required. The validity of H_1 will be determined by using vector autoregression analysis and Granger causality to ascertain if the daily number of transactions (trade volume) has an effect on the price of bitcoin. Using the same analysis, the validity of H_2 will be ascertained by determining if Bitcoin days destroyed (saving) has an effect on the price of bitcoin.

The contributions made in this thesis are manifold. A comprehensive assessment of Bitcoin will benefit all seeking to get acquainted to Bitcoin, or simply deepen their understanding. The detailed overview of the academic literature on Bitcoin shall provide a basis for future research extending beyond Bitcoin itself to the field of cryptocurrencies, econometrics, and macroeconomics. Applying the functions of money to Bitcoin and discussing the economic equation of money in relation to Bitcoin will complement and expand on previous research; this will address a gap in the macroeconomic literature at this time. The econometric analysis will provide valuable insight on the price determinants of bitcoin from a previously unexplored perspective derived from Wang's model.

Once a new model is proposed, it is up to researchers to establish its validity by proving or disproving the assumptions the model makes. It therefore warrants a stringent methodology to determine whether or not the proposed macroeconomic model can be proved using empirical observations of the Bitcoin market.

Given that Bitcoin is a nascent, unconventional monetary scheme, special attention must be given to introducing it in a concise but illustrative manner. The second chapter is devoted entirely to Bitcoin to familiarize readers with the mechanics of Bitcoin: Bitcoin mining, Bitcoin storage, Bitcoin trading, and Bitcoin purchases. This comprehensive assessment of Bitcoin will allow readers to understand the theories presented and explored as well as the reasoning behind the analytical tools chosen and used.

The third chapter is devoted to the theoretical background relevant to the hypothesis. It is divided in two sections. The first section is devoted to the literature review, consisting of an overview of the literature on Bitcoin and the main authors in the field. While a nascent area of study, online cryptocurrencies have garnered their share of academic interest across numerous fields. The second section presents the relevant theory. The pertinent literature is presented in conjunction with the models explored in the thesis. The classical functions of money are introduced to familiarize readers with relevant literature on money and its role. The final two sections of the third chapter present the economic equation of exchange and

Wang's macroeconomic model respectively. It is essential to note that this chapter is focused solely on setting forth the germane models and their respective literature to provide insight on the proposed model evolving from the economic equation of exchange. Applicability to Bitcoin and future developments are reserved for the fifth chapter.

The fourth chapter provides the foundation for the analytical section of the thesis. The methodology chapter presents a detailed overview of what the analytical section undertakes. It presents the two hypotheses and provides the reasoning as to why and how they are processed, highlighting the relevant issues and the reasons behind the use of each variable in the analysis. It describes how and why the data was collected, why some data and variables are omitted, and why the analytical software Gretl is used to carry out the analysis. It also delves into the econometric models used to set the stage for the fifth chapter.

The fifth chapter is devoted to the analysis. It provides the core value added of the thesis. The first section applies the classical functions of money to Bitcoin to determine the extent and validity of Bitcoin as a form of money, a crucial stage to clarify both the breadth of Bitcoin as a currency and the applicability of the proposed macroeconomic model. This provides insight for Bitcoin's potential regulatory framework. It is established that while Bitcoin fulfills the functions of money, it currently remains a speculative instrument. The second part of the chapter amends Wang's model. It provides additional assumptions to adapt the model to the realities of empirically analyzing the Bitcoin market; this establishes the framework for the analysis. The third part of the chapter provides the results of the econometric analysis and uses them to determine the validity of the two hypotheses. The results establish that both hypotheses, H_1 and H_2 , cannot be rejected and are therefore valid; the empirical evidence supports the model. To conclude the chapter, other interesting findings are briefly discussed.

Henceforth, the final chapter provides an overview of the claims undertaken and recapitulates the results and findings. The concluding remarks caution on the interpretation of the results and their limited scope and on the assumptions made in building the model. Future research and potential developments with regards to Bitcoin are also addressed in light of the research's outcomes, setting a foundation for its future applicability.

2 Bitcoin

Bitcoin is a virtual open-source currency system structured on decentralized peer-to-peer (P2P) networking and operated under the rules of cryptography. This chapter serves as a platform to introduce Bitcoin and familiarize readers on the mechanics of Bitcoin: Bitcoin mining, Bitcoin storage, Bitcoin trading, and Bitcoin purchases. This sets the scope under which Bitcoin will be analyzed in the following chapters. It presents an objective account of Bitcoin and reserves criticisms and praises for the analytical section of the thesis.

The first subsection clarifies terminology and usage of the term Bitcoin. The subsequent subsection develops on the origins of Bitcoin, its creator(s), and the legacy left forth by Bitcoin. The third subsection describes how Bitcoin functions; it is divided into three parts: (1) how Bitcoin relies on decentralized networking to function, (2) what and how data is broadcasted on the network, and (3) how Bitcoin's money supply functions, which is also known as *mining*. The fourth subsection delves into Bitcoin usage. It covers acquiring and storing bitcoins, Bitcoin exchanges, how bitcoins are priced, and lastly, its acceptance in real-world markets.

Providing a comprehensive assessment of Bitcoin is paramount to undertaking further developments in the analytical section.

2.1 Terminology and Usage

In order to delve into Bitcoin's intricacies, it is important to clarify terminology. The following subsection outlines the different terminological uses of Bitcoin.

The primary online reference for Bitcoin is www.bitcoin.org, the original domain name used by Satoshi Nakamoto in his working paper and the original idea behind Bitcoin. The Bitcoin Foundation (2014) sponsors this website, whose three primary objectives are: standardizing, protecting, and promoting Bitcoin. Terminology usage is therefore based on those used by the Bitcoin foundation in an attempt to standardize the discussion and understanding around Bitcoin.

Capitalized, *Bitcoin* refers to the concept of Bitcoin and the Bitcoin network in its entirety. Without capitalization, a *bitcoin* refers to the unit of account and can be pluralized as *bitcoins*; it is often abbreviated to BTC, similar to how one Canadian dollar is abbreviated as one CAD. When this distinction is unclear, Bitcoin is used. Subsequently, technical

terms will be addressed in their respective sections and explained therein. Now that the usage of the term has been established, it is time to look into what is Bitcoin.

2.2 The Origins of Bitcoin

Bitcoin is a novel online peer-to-peer electronic cash system, which was first introduced by Nakamoto (2008), an alleged pseudonym, in *Bitcoin: A Peer-to-Peer Electronic Cash System*. Nakamoto's work proposed a solution to the double-spending problem faced by electronic cash systems, which had, up to then, required a trusted third party to mitigate any double spending.

Double spending occurs when an electronic coin is spent more than once, a form of counterfeit or fraud. The double-spending problem can be summarized as follows: "a representation of currency requires that it not be possible to create multiple copies and spend the same digital currency two or more times (Wanyer in Dwyer 2014). In economic terms, Dwyer (2014) states that "if the double-spending problem is not solved, the value of the bits is the same as the marginal cost of reproducing any particular set of bits: zero."

Other forms of online electronic currencies had previously been launched, but without much success given the issues related to double spending and the constant need for a central authority or mint; in other words, a trusted third party. Nakamoto's paper proposed to diffuse the trustee third party requirement through a decentralized peer-to-peer network based on a proof-of-work system with a public ledger of all transactions, hence voiding the need for a centralized authority. Bitcoin would act as "an electronic payment system based on cryptographic proof instead of trust, allowing [for] any two willing parties to transact directly with each other without the need for a trusted third party." Together, users on the network were to validate transactions, preventing double spending. In January 2009, Nakamoto officially released Bitcoin. From there on, a group of core developers, which included Nakamoto, worked on the Bitcoin software and development. However, Nakamoto's last communication was on 23 April 2011 and he has not been heard from ever since, further fueling the mystery around Bitcoin. Nonetheless, Bitcoin has continued to develop, with its market capitalization surpassing 8.5 billion USD in June 2014. One question remains: how does it all work?

2.3 The Mechanics of Bitcoin

As a peer-to-peer-based cryptocurrency, Bitcoin operates on a global decentralized network over the Internet. Bitcoin users running the necessary software fuel this P2P

decentralized network. The software is open-source, which means that the code used in Bitcoin's creation and operation is subject to public scrutiny. The creation of bitcoins and their transaction between users are bound by the cryptographic rules and enforcement mechanisms embedded in the software's computer code. A group of core developers updates the Bitcoin software, but not without consensus. Given Bitcoin's open-source nature, its software and protocol can be modified by anyone. However, it is not possible to dictate unilateral implementation of any changes because users are free to choose what software and version they use. This is essential because in order to function, the system must have users operating software bound by the same rules. Compatibility forces consensus amongst developers and users and is in itself a powerful incentive to abide by. Additionally, it removes the possibility of a single entity dictating the outcome of Bitcoin.

At first, Bitcoin appears to be complex to outsiders given its cryptographic nature. This can lead to several misconceptions and misunderstandings, but these are addressed once incrementally explained. The explanation is divided into three parts. First, the reasoning behind the decentralized networking Bitcoin operates under is explained. Second, the process of how data is broadcasted on the network through transactions and blocks is described, which then bridges to the third part on how Bitcoin's money supply functions.

2.3.1 Decentralized Networking

Contrary to most electronic-cash schemes, Bitcoin does not require a central authority for neither issuance of the currency nor transaction verification, but rather relies on its users to carryout these tasks. Users operating the Bitcoin client software have downloaded the totality or part of Bitcoin's public ledger containing all previous transactions. Once downloaded, users become *nodes*; they relay data broadcasts through the P2P network. Given that there is no central point of trust, Bitcoin relies on the majority of the nodes in its network to be honest. The nodes must relay the 'right' version of the public ledger, based on "a majority vote mechanism for double spending avoidance, and dispute resolution" (Barber *et al.* 2012). This perpetuates Bitcoin's decentralized nature and prevents any one entity from being tempted or coerced into unilaterally subverting it. However, unilateral group action is not unfeasible. The majority vote mechanism can be subjugated when users group together to form more than 50% of the nodes in the system and rely their 'right' version of the block chain as seen in subsection [2.3.3 Mining: Bitcoin's Money Supply](#). In short, Bitcoin's decentralized networking relies on data broadcasts amongst its users to operate.

2.3.2 Data Broadcasts: Transactions and Blocks

There are two types of data broadcasts between nodes on the network: transactions and blocks. Each data broadcast has a *hash* value. A hash algorithm turns any arbitrarily large quantity of data into what is known as a fixed-length hash. An identical hash will always result from the same data, but changing the data by a single bit will completely change the hash. It is impossible to predict the value of a hash given a specific set of data. The Bitcoin protocol requires that a hash value have a specific form, which can only be achieved using brute force, i.e. a proof-of-work mechanism. This makes any attempt at changing any block with a given set of transactions and all those after it very labor intensive. Barber *et al.* (2012) summarize Bitcoin transactions as “the operations whereby money is combined, divided, and remitted.”

Every Bitcoin transaction starts with a Bitcoin address. Each Bitcoin address has a cryptographic key pair: a public key and a private key. Both are alphanumeric strings, but while the public key is visible to all users (without automatically revealing the user’s identity), the private key is and should only be known by the owner of the address. Private keys are a safety mechanism that allows the owners to spend the bitcoins on their addresses much like a PIN code. A new address is normally created for every new Bitcoin transaction. Once a user decides to transfer some bitcoins to another address, a Bitcoin client will broadcast the request on the network for it to be validated. A Bitcoin client is the end-user software that facilitates private key generation and security as well as payment sending, much like an Internet banking application on a phone. Once broadcasted, transactions are ready to be vetted. Vetting a transaction occurs when its various components are validated (see [Appendix 1](#)) and checked against double spending, i.e. funds have not been spent before or spent by a wrongful user.

Once vetted by the miners, a transaction is incorporated into a *block*. A block is a record that contains the waiting transactions that have been vetted. A transaction is confirmed when the block it is incorporated in is appended to the *block chain*. Once appended, a transaction is confirmed. The block chain is the public ledger of Bitcoin; it serves as a public record of all vetted Bitcoin transactions in chronological order. Through the nodes of the network, the block chain is shared between all Bitcoin users and can be viewed by anyone. Permanently allowing the verification of all Bitcoin transactions prevents double spending. It is Nakamoto’s (2008) “solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological

order of transactions.” Furthermore, the creation of blocks and incorporating them in the block chain has two main incentives: (1) obtaining new bitcoins by mining them into existence, and (2) collecting fees for vetting transactions. In other words, mining receives the first types of data broadcast, transactions in order to generate the second type of data broadcast, blocks.

2.3.3 Mining: Bitcoin’s Money Supply

The process of bringing bitcoins into existence is referred to as *mining*. Bitcoin functions as an “algorithmic currency with a deterministic supply and growth rate tied to the rigor of mathematics” (Yermack 2013). Indeed, the supply of bitcoins is exogenously determined in its protocol. Bitcoins are *mined* into existence when transactions are verified and a block is appended to the block chain. To mine bitcoins, miners must operate software with specialized hardware. By devoting their computer power and the electricity required to run the necessary hardware, *miners* compete to obtain the bitcoin reward allotted when a new block is added to the block chain and the possible transaction fees associated with the transactions they successfully vet into a block. Nakamoto mined the first block of the block chain – the *genesis block* – on 3 January 2009.

Ever since the first block was mined, the rate of block creation has been limited by Bitcoin’s proof-of-work mechanism with adaptive difficulty. The level of difficulty sets how hard it is to solve a cryptographic hash function fulfilling the hash value of a specific form; in Bitcoin’s case, the specific form operates under SHA-256 cryptography. The level of difficulty fluctuates as competition varies, as Houy (2014) puts it: “the complexity of mining is made dependent on the total computational power of all miners.” The total computational power of all miners is known as the hash rate. Therefore, network difficulty is adjusted automatically by the Bitcoin protocol in light of the hash rate every 2016 blocks to maintain block creation at an average of once every ten minutes.

While network difficulty dictates the creation of new blocks, the reward for block creation is also engrained in the Bitcoin protocol. The block reward was initially set at 50 BTC per block and is programmed to halve every 210,000 blocks. It is currently at 25 BTC per block and will continue to halve until all 21,000,000 BTC are mined as set forth in the protocol. This way, the number of bitcoins mined is set to asymptotically end around the year 2140. Given the rate of block creation set by the difficulty and the preordained block reward for block creation, Bitcoin’s money supply is finite, asymptotically determined, and therefore predictable.

Although only 21 million bitcoins will ever be mined, a bitcoin is divisible down to eight decimal places, i.e. 0.00000001 or $1e^{-8}$. Currently, one bitcoin represents 100,000,000 *satoshis*. A satoshi is the name given to the smallest possible unit of bitcoin. The scale of divisibility gives Bitcoin a vast potential to expand and currently allows for micro transactions. However, this engenders much criticism over how early adopters could greatly benefit later as price per BTC increases.

The divisibility of bitcoins has several advantages for Bitcoin, particularly for mining. It allows miners to charge very small transaction fees to the senders for vetting transactions, which are only charged when the said transaction is added to a new block appended to the block chain. These fees are usually in-line with the number of bytes in the transaction, i.e. how computationally sizeable it is. The potential additional rewards serve several purposes. First, transaction fees prevent users from spamming the block chain with menial transactions. It also helps transactions to get included when miners decide which transactions to include in the block they are attempting to solve. Furthermore, a user can help prioritize their transaction by paying a higher transaction fee to fasten its addition to the block chain. Finally, by being adjustable, transaction fees can be adjusted over time as the reward for block bounties decrease and vetting costs increase, for as the block chain “grows over time, so does the demand on the computational hardware responsible to maintain and update the block chain” (Lawn 2014). Hence, the divisibility of bitcoins helps users and miners to adapt as Bitcoin evolves.

Mining has substantially changed and adapted since the genesis block. In its early beginning, bitcoins were mined using CPU power from personal computers. As Bitcoin’s popularity grew, the number of miners increased and the difficulty adjusted accordingly. A switch to Graphic Processing Units was inevitable as “a CPU [is] ideal for general computing, but [it is] inefficient for performing the same type of simple calculation repeatedly” (DuPont 2014). Next came Field Programmable Gate Array (FPGA) devices tailored to compute SHA-256 cryptographic puzzles. However, Application-Specific Integrated Circuit (ASIC) devices quickly replaced FPGAs. ASIC devices are custom-built, Bitcoin mining machines that eclipse other devices due to their remarkable speed and power efficiency. The rise in popularity of Bitcoin alienated individual, small-scale miners. With an exponentially growing hash rate, efficient Bitcoin mining is now “only possible using specially built software, tailored to take advantage of built-in hardware capabilities”

(DuPont 2014), which comes at a greater cost. To counter the increase in cost and difficulty, miners have formed collectives called *mining pools*.

The emergence of mining pools has challenged the idea of Bitcoin working in a decentralized manner. A mining pool is a collective of miners, who by pooling their computational power, seek to create a powerful mining platform and successfully solve a block before others. As mining becomes increasingly expensive and difficult, “mining pools have grown to allow individuals to collectively contribute effort to the transaction verification process in exchange for an interest in the proceeds from the mining activity” (Gordon *et al.* 2015). By pooling their mining efforts, mining pools have at times threatened to own more than 50% of the computing power of the entire network (Gervais *et al.* 2013). Potential solutions have been proposed and implemented, including self-regulation by miners through boycott (Buterin 2014). Nevertheless, the possibility that a collective could own over 50% of the computing power of the entire network remains a contentious issue for the future.

Mining embeds Bitcoin’s monetary base in its protocol. As the sole creator of bitcoins, it is a “distributed process in which the network processes and secures transactions” (Buterin 2014), creates and maintains the block chain and the integrity of the system as a whole. It is the launching pad to all other Bitcoin uses.

2.4 Bitcoin Usage

An extensive ecosystem composed of third-party intermediaries that support Bitcoin transactions is emerging as Bitcoin’s popularity grows. This ecosystem encompasses several intermediaries such as: mining pools, Bitcoin wallets, Bitcoin exchanges, Bitcoin ATMs, OTC (over-the-counter) exchanges, marketplace escrow services, investment services, mixing services, and gambling websites. Interestingly enough, “most of the risk Bitcoin holders face stems from interacting with these intermediaries, which operate as *de facto* centralized authorities” (Moore and Christin 2013).

This subsection expands on the uses of Bitcoin within its ecosystem starting from how Bitcoins are most commonly acquired, how they are stored, how the value of a bitcoin is determined in terms of fiat currency, and concludes on how bitcoins are used in purchasing goods and services.

2.4.1 Acquiring and Storing Bitcoin

There are three main ways to acquire bitcoins: mining, earning, and buying. As previously presented, mining was the only way to acquire bitcoins in the beginning. However, it has now evolved into a complex, highly competitive cryptographic puzzle-solving race compelling new potential Bitcoin users to earn or buy bitcoins rather than mining them. One can earn bitcoins through donations or tips, as income, from gambling, and by accepting them as a means of payment for goods and services. Details on buying bitcoins are reserved for subsection [2.4.2 Bitcoin Exchanges and Buying Bitcoins](#). With a Bitcoin address, a user can acquire bitcoins. It is recommended to use a Bitcoin wallet to store private keys, which grant them access to their funds.

A Bitcoin wallet answers the need for users to safely store private keys. The main types of Bitcoin wallets are: mobile, web, desktop, and hardware. A mobile wallet runs on a mobile device through an application; it is the most portable and fastest wallet, but sacrifices some security given that a mobile phone can be lost or hacked. A web wallet is an online wallet hosted on a server rather than a user's computer. While also accessible from anywhere in the world, hacking of the provider's servers and illicit behavior from a provider's personnel remain potential threats. Hybrid web wallets address this issue by encrypting the private keys on the user's browser before sending them to the server. A desktop wallet is a full-feature Bitcoin client with the most features and notable security, given that it is downloaded onto the user's computer. However, the desktop version has its shortcomings: owning a computer vulnerable to malware, requiring the download of the entire block chain (currently over 30 gigabytes), and its operation necessitates powerful hardware. The last main type of wallet is a hardware wallet, which is physical hardware on which private keys are stored. Immune to computer viruses, recently released hardware wallets store private keys and actively sign transactions without sending the user's private keys. This provides the highest degree of security, but functionality requires having the physical hardware on hand.

Private keys can be stored on encrypted USB keys or simply printed on paper; this is known as cold storage or offline storage. However, for security and practical reasons, it is better to have private keys stored onto some form of Bitcoin wallet. Furthermore, it is important to remember that a Bitcoin wallet does not store bitcoins – that is what the block chain does through public keys – but rather stores a user's private key(s) to their Bitcoin address(es). The importance of safeguarding private keys is quintessential given that

Bitcoin transactions are irreversible. This is why it is recommended that users spread their bitcoins over several addresses to mitigate the potential losses from a stolen private key, furthering the importance of wallets.

2.4.2 Bitcoin Exchanges and Buying Bitcoins

The most common method for buying bitcoins is to purchase them through Bitcoin exchanges. A Bitcoin exchange is an online platform where a user sets up an account to deposit fiat currency. Bitcoins are bought and sold between traders on the exchange through *bid* (buy) and *ask* (sell) offers. Once a buy offer meets a sell offer, a user's fiat currency is credited into bitcoins on their exchange account, which can then be sent to a user's Bitcoin address if they wish to do so. The exchange acts as the intermediary and manages the *order book*, taking a fee off every exchange transaction. In other words, "the exchanges are handling accounts of their customers in an internal accounting system, guaranteeing for keeping record of the on-exchange purchased and sold Bitcoins without actually transferring these Bitcoin through the Blockchain [*sic*]" (Glaser *et al.* 2014). The traded bitcoins are only appended to the block chain once a user sends their bitcoins from their exchange account to a Bitcoin address.

Bitcoin exchanges are the gateway through which bitcoins are purchased. Research demonstrates that "newly attracted users primarily limit their relation to Bitcoin to trading on exchanges" (Glaser *et al.* 2014). To meet the demand of customers from all over the world, different exchanges accept different currencies and have different trade volumes, with trade in USD far exceeding any other currency at nearly 80% as of March 2015 (Bitcoin Charts 2015). It is on these Bitcoin exchanges that the value of Bitcoin in terms of fiat-based currencies is established.

2.4.3 How are bitcoins priced?

Given that Bitcoin is a digital open-source currency system, data is readily available. This also applies to Bitcoin exchanges, which must divulge their financial and technical data through API (application program interface) requests to be considered as trust worthy in the community. Bitcoin Charts (www.bitcoincharts.com) provides real-time data on Bitcoin exchanges. The exchange rate for bitcoins in a certain currency is determined by supply and demand in the market on an exchange trading bitcoins in that particular currency. Since Bitcoin is decentralized, the value of bitcoins is not pegged to any real-world currency. Several exchanges trade in the same currency; 13 exchanges trade in USD

as of March 2015. With different order books for different exchanges, the price in terms of a certain fiat currency varies between exchanges. CoinDesk (CoinDesk 2015c) launched the CoinDesk Bitcoin Price Index (BPI) in September 2013. The BPI represents an average of bitcoin prices across leading global exchanges that meet criteria specified by CoinDesk. More information on the BPI is provided in the subsection 4.4.1 Data Selection and Collection. It is up to the Bitcoin user – whether a merchant, trader, or any other party – to use any of these valuation mechanisms in determining the value they wish to appraise bitcoins at, particularly when trying to determine the price they wish to charge or pay for a certain good or service.

2.4.4 Bitcoin’s Acceptance in Real-World Markets

Bitcoin’s acceptance in real-world markets has grown exponentially since the genesis block. Growing from a few dozen locations in September 2011 (Kapalov 2012) to over 100,000 businesses in February 2015, more businesses are accepting BTC as a means of payment including Overstock, Google, Dell, and PayPal (Cuthbertson 2015). To counter the high exchange rate volatility, merchants accepting BTC usually use a Bitcoin merchant solution such as Coinbase or BitPay to get instant conversion to the fiat-based currency of their choice, normally with no transaction fee.

This overview of the mechanics of Bitcoin provides readers with the necessary understanding of Bitcoin for the subsequent chapters. It will allow readers to understand the theories presented relevant to Bitcoin and the reasoning behind the analytical tools chosen and used to further the thesis’ hypotheses and serves as a gateway to the literature review.

3 Literature Review

This chapter explores the relevant theoretical background required to answer the hypotheses. The first section provides a comprehensive overview of the literature on Bitcoin. It forms part of the value added of the thesis by providing an extensive assessment of the literature on Bitcoin in conjunction with Bitcoin's presentation in the previous chapter to help future researchers narrow the scope of their study. The second section centers around the macroeconomic theories needed to pursue the hypotheses. This division ensures that the pertinent literature to both Bitcoin and the macroeconomic and econometric theories at hand are easily discernable, further facilitating the reader's understanding in the analysis chapter.

3.1 Literature Review on Bitcoin

In recent years, Bitcoin has sparked academic interest, leading the way to a plethora of novel studies and articles. The first subsection begins with a review of Bitcoin's precursors in terms of cryptography and digital currencies. It explains their influence on Bitcoin and discusses Nakamoto's work. The second subsection focuses on the relevant literature with regards to the mechanics of Bitcoin and Bitcoin's usage. The remaining subsections are divided as follows: On Bitcoin and Regulation, On Bitcoin and Economics, On Other Graduate and Undergraduate Work, concluding with On Bitcoin and Econometrics.

3.1.1 On Bitcoin's Precursors

Cryptography is core to Bitcoin's existence. Research on the science of secret communication long precedes the inception of Bitcoin. Public key cryptography, which is a core component to the Bitcoin protocol, was invented as early as the 1970s (DuPont 2014). Rivest *et al.* (1978) presented an encryption method in which publically revealing an encryption key (public key) did not automatically reveal the corresponding decryption key (private key). In 1981, David Chaum expanded on their work when he developed a technique for public key cryptography; this allowed for an electronic mail system to hide with whom a participant communicates with, as well as the contents of the communication, without the need for a universally trusted authority. This technique is essential to Bitcoin's decentralized networking.

In 1982, Ralph Merkle was granted a patent for Merkle trees, which are "a method of providing a digital signature for purposes of authentication of a message, which utilizes an

authentication tree function” (Merkle 1982). Hash trees are used to allow efficient and secure verification of Bitcoin transactions while saving disk space (Nakamoto 2008). Bitcoin’s proof-of-work element (the one-way hashcash function SHA-256) is based on Adam Back’s Hashcash, a proof-of-work algorithm that is “efficiently verifiable, but parameterisably [*sic*] expensive to compute” (Back 2002). In addition to Chaum, Merkle, and Back, DuPont (2014) asserts that Wei Dai’s b-money scheme (1998), Nick Szabo’s bit gold concept (1999), and Hal Finney’s reusable proofs of work (2004) were also some of the most significant and influential developments contributing to the creation of Bitcoin.

Nakamoto’s original intent in the publication of *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) and the launch of Bitcoin in 2009 was to introduce a potentially revolutionary electronic cash system. The author’s famed anonymity is subject to a lot of speculation. It is interesting to highlight that with an anonymous author, attention can truly be focused onto Bitcoin itself rather than on its creator, particularly because Bitcoin’s software is open-source and available for everyone to scrutinize. By introducing “a solution to the double-spending problem using a peer-to-peer network” in the realm of cryptography, Nakamoto (2008) simultaneously launched “an electronic payment system based on cryptographic proof instead of trust.” There is no evidence to whether or not the original intent behind Bitcoin was for it to replace fiat-based currencies or to take on such a magnitude. Nevertheless, it did revolutionize electronic money.

Since the 1990s, the Internet and Web-based commerce have grown exponentially, generating the need for online electronic payments systems. With digitization came the creation of a digital currency. Peter Tucker (2009) provides a detailed overview and analysis of digital currencies that preceded Bitcoin, such as DigiCash, Pecunix, Webmoney, and Liberty Reserve. He also addresses the legal implications behind those digital currencies and their run-ins with the law. Within the framework of Bitcoin literature, Grinberg (2011) addresses gold-backed currencies and virtual world and game-related commerce, such as Linden dollars in the virtual online world Second Life, Facebook credits, and World of Warcraft Gold. Grinberg (2011) states that “Bitcoin competes with at least two classes of products: (1) products that facilitate internet-based commerce, and (2) gold-backed currencies.”

With Bitcoin, Nakamoto addressed several issues inherent to digital currencies and online payments systems: fraud (reversible transactions), the requirement for a trusted third party, and centralized operations. Through a peer-to-peer distributed electronic payment system

based on cryptography, transactions are irreversible, there is no need for a trusted third party as users can directly transact with one another across borders, and there is no need for centralized operations because transactions are broadcasted on a P2P network with a decentralized block chain. Together, these improvements addressed the most challenging issue for both digital currencies and online payment systems: double spending. Nakamoto's proposal was "a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power."

However, double spending is still possible. Karame and Androulaki (2012) "focus on double-spending attacks on fast payments and demonstrate that these attacks can be mounted at low cost on currently deployed versions of Bitcoin." Furthermore, Rosenfeld (2012) demonstrates how the ways in which the block chain provides protection against double spending can be undermined and discusses the conditions in which a double-spending attack can be economical. While double spending is possible on fast payments, double-spent funds become void as new blocks are appended. However, it is then sometimes too late for the defrauded party. Since Bitcoin's inception, many other scholars have studied the mechanics of Bitcoin and its use, which are the focus of the subsequent subsection.

3.1.2 On the Mechanics of Bitcoin and Bitcoin Usage

The review of the literature in this subsection is structured to reflect sections [2.3 The Mechanics of Bitcoin](#) and [2.4 Bitcoin Usage](#). The subsection headers are ordered in accordance with the way they were introduced in the second chapter to ease comprehension of how authors from different fields and with different scopes approach Bitcoin.

3.1.2.1 On Decentralized Networking

Bitcoin's decentralized networking has come under academic scrutiny. Gervais *et al.* (2013) address the true limits of decentralization in the Bitcoin system, showing "that a limited set of entities currently control the services, decision making, mining, and the incident resolution processes in Bitcoin." Barber *et al.* (2012) provide a detailed study of Bitcoin mechanics and potential solutions to the issues and eventual attacks Bitcoin may face; they conclude that "while the instantiation is impaired by its poor parameters, the core design could support a robust decentralized currency if done right." Their comparative

study on Bitcoin provides a detailed overview of Bitcoin’s functioning, which is essential in structuring the chapter on Bitcoin.

3.1.2.2 On Data Broadcasts

In regards to data broadcasts, Nakamoto (2008) did caution that it is possible to link public keys to users with multi-input transactions (e.g. using multiple addresses for one payment), which jeopardizes a user’s anonymity. Reid and Harrigan (2011) address the anonymity of Bitcoin using passive analysis mapping to demonstrate that “it is possible to associate many public-keys [*sic*] with each other, and with external identifying information” and that the activity of known users can be observed in detail by the usage of centralized services, such as Bitcoin exchanges and online wallets. Ober *et al.* (2013) analyze the topology of the Bitcoin transaction graph using network dynamics to assess its structure and anonymity. Koshy *et al.* (2014) analyze the anonymity of Bitcoin, but use P2P network traffic, demonstrating that “addresses can be mapped to their likely owner IPs [*sic*] by leveraging anomalous relaying behavior.” Ron and Shamir (2012) quantitatively analyze the full Bitcoin transaction graph, which provides insight into the “typical behavior of users, how they acquire and how they spend their bitcoins, the balance of bitcoins they keep in their accounts, and how they move bitcoins between their various accounts in order to better protect their privacy.” Their work is crucial in determining what variables to use in the analysis. Meiklejohn *et al.* (2013) focus on the growing gap “between the potential anonymity available in the Bitcoin protocol design and the actual anonymity that is currently achieved by users.”

3.1.2.3 On Mining: Bitcoin’s Money Supply

Babaioff *et al.* (2012) demonstrate the lack of incentives for Bitcoin miners to include recently announced transactions in a block and propose a modification to the Bitcoin protocol; this modification eliminates the problem by rewarding information propagation. Furthermore, Eyal and Sirer (2013) argue that the Bitcoin mining protocol is not incentive-compatible and is vulnerable to attacks by colluding miners (mining pools) below the assumed $\frac{1}{2}$ bound (known as the 51% attack); they propose “a practical modification to the Bitcoin protocol that protects Bitcoin in the general case.” Houy (2014) explores incentives for miners through the Nash equilibrium, showing that “miners do not play a Nash equilibrium in the current Bitcoin mining environment; instead, they should not process any transactions at all.”

3.1.2.4 On Acquiring and Storing Bitcoin

As some of the first to address Bitcoin wallets, Omar and Aamir Syed (2011) propose the introduction of a “peer-to-peer network for storing bitcoin wallet and mapping email addresses to bitcoin addresses [...] to provide features similar to centralized online payment systems, such as PayPal, while maintaining the decentralized goal of bitcoin.” Goldfeder *et al.* (2014) argue that “due to the irreversibility, automation, and pseudonymity [*sic*] of transactions, Bitcoin currently lacks support for the sophisticated internal control systems deployed by modern businesses to deter fraud.” They continue, stating that a threshold-signature scheme compatible with Bitcoin’s ECDSA signatures can be used for enhancing the security for: “(1) shared control of a wallet, (2) secure bookkeeping, a Bitcoin-specific form of accountability, (3) secure delegation of authority, and (4) two-factor security for personal wallets.”

3.1.2.5 On Bitcoin Exchanges and Buying Bitcoins

Moore and Christin (2013) study the risk an investor faces from Bitcoin exchanges and employ a proportional hazards model to “find that an exchange’s transaction volume indicated whether or not it is likely to close.” Androulaki *et al.* (2013) evaluate user privacy in Bitcoin in a university setting; they demonstrate that considerable information is leaked about the profiles of users when using Bitcoin and add that reliance on third-party trusted entities “emerges as one of the few workable solutions to increase the privacy of Bitcoin clients.”

3.1.2.6 On Bitcoin Pricing

Academic interest in Bitcoin prices and the factors influencing it is considerable. Author contributions in this subsection provide the foundation for the thesis’ analysis. Yermack (2013) studies correlations between Bitcoin prices and various currencies and the price of gold demonstrating that Bitcoin’s excessive volatility is more consistent with the behavior of a speculative investment than a currency. Dwyer (2014) compares the monthly standard deviations of log returns of gold as well as Bitcoin prices claiming that gold is likely to be a less volatile investment than Bitcoin. Grondwald (2014) also provides a comparison between Bitcoin and gold analyzing Bitcoin prices with results “suggesting that Bitcoin price are particularly marked by extreme price movements; a behavior generally observed in immature markets.”

Bucholz *et al.* (2012), Kristoufek (2013, 2014), Bouoiyour and Selmi (2014), Garcia *et al.* (2014), Glaser *et al.* (2014), and Ciaian *et al.* (2014) provide empirical insights on the different variables affecting Bitcoin's price and on how the price of bitcoin is determined. A more in-depth overview of their work is provided in subsection 3.1.6 On Bitcoin and Econometrics.

3.1.3 On Bitcoin Regulation

As the first decentralized digital cryptocurrency, Bitcoin has garnered significant attention from academia and regulatory bodies in regards to its regulation. Author contributions in this subsection are key to the thesis in addressing Bitcoin's future. Elias (2011) is one of the first to investigate the legal aspects of Bitcoin. Stokes (2012) analyzes the money laundering risks of the Linden dollar and Bitcoin demonstrating that "although these virtual currencies have money laundering utility, they are currently unsuitable for laundering on a large scale." Kapitalov (2012) maintains that cash-like transactions and miners "fall outside of the regulatory provisions under federal banking, money transmission, and securities laws" and that bitcoin should be treated as a community currency under the law. More recently, Gordon *et al.* (2015) argue to the contrary that mining pools should be regulated under the existing federal securities regulation regime.

On a global scale, Plassaras (2013) posits that the International Monetary Fund is unable to handle the widespread use of Bitcoin into foreign exchange markets and proposes a certain interpretation of its Articles of Agreement that would allow it to intervene. He judiciously argues that law enforcement should become familiar with the technology in order to investigate and prosecute illegal activity. Bollen (2013) addresses Bitcoin regulation in different countries through three groups of issues: general financial services regulation, specific banking regulation, and currency regulation and legal tender. He demonstrates that regulation of virtual currencies is still at a very early stage. Trautman (2014) provides an overview of virtual currencies, how regulators define them, how they are regulated, and their potential illicit use. He explores Bitcoin's recent run-ins with the law with the closure of Silk Road and the Mt. Gox debacle. Christin (2013) provides an empirical analysis of Silk Road discussing the economic, ethical, and policy implications for future research.

3.1.3.1 Official Publications

The following subsection provides examples of official publications from governments, banking authorities, and financial entities that attend to Bitcoin to illustrate the growing attention given to Bitcoin and virtual currencies and how their regulation is approached.

The European Central Bank (2012) released an official publication on virtual currency schemes, their definition and categorization, providing case studies (namely, Bitcoin and the Second Life), and addressing their relevance. The ECB acknowledges that virtual currency schemes can have positive aspects in terms of financial innovation and the provision of additional payment alternatives for consumers, but warns that they clearly entail risk. The Financial Crimes Enforcement Network (2013, 2014) addressed the regulation of administrators and exchangers of both centralized and decentralized convertible virtual currencies, as well as virtual currency trading platforms. The Law Library of Congress (2014) published a survey of forty foreign jurisdictions plus the European Union, “reporting on any regulations or statements from central banks or government offices on the handling of bitcoins as well as any significant use of bitcoins in business transactions.” The publication discusses “whether bitcoins are recognized as legal tender, the possibility of negative impacts on the national currency, concerns about fraud, and how transactions using the Bitcoin system are viewed by tax authorities.”

Badev and Chen (2014), members of the Board of Governors of the Federal Reserve System, seek to “provide the necessary technical background to understand basic Bitcoin operations and document a set of empirical regularities related to Bitcoin usage.” Lo and Wang (2014) of the Federal Bank of Boston discuss how some Bitcoin features have hampered its ability to perform the functions of money; a work essential to the application of the functions of money to Bitcoin in the analysis. In an official publication from J.P. Morgan, John Normand (2014) addresses Bitcoin with regards to the functions of money and as a potential investment tool, arguing that it is vastly inferior to fiat currencies.

3.1.4 On Bitcoin and Economics

The economic literature on Bitcoin covers many fields of economics. The author contributions summarized in this subsection are vital to discussing Bitcoin in light of the classical functions of money; this will assist in determining the extent and validity of Bitcoin as a form of money and furthering the hypotheses on Wang’s (2014) proposed macroeconomic model.

In monetary economics, Luther and Olson (2013) apply Bitcoin to the concept of ‘memory,’ arguing that, like memory, Bitcoin functions as a public record-keeping device. They provide evidence that Bitcoin use has soared as the expected cost of storing traditional money increased. Furthermore, Luther (2013) argues that network effects and switching costs are responsible for the failure of cryptocurrencies to gain widespread acceptance and that “cryptocurrencies like Bitcoin are unlikely to generate widespread acceptance in the absence of either significant monetary instability or government support.”

Gans and Halaburda (2013) study the economics of private digital currencies including Bitcoin and find that “it will not likely be profitable for such currencies to expand to become fully convertible competitors to state-sponsored currencies.” Yermack (2013) examines whether or not Bitcoin should be considered as a currency. He argues that Bitcoin behaves more like a speculative investment rather than an established currency, citing BTC’s high exchange rate volatility. Luther and White (2014) research Bitcoin in terms of a medium of exchange, store of value, and unit of account, arguing that the price volatility of Bitcoin will not preclude its spread as a medium of exchange. In a similar vein, Evans (2014) studies the economic aspects of Bitcoin and other decentralized public-ledger currency platforms. He claims the economic efficiency and the potential viability of public-ledger platforms depend on the design of incentives and governance systems.

On a more theoretical front, Selgin (2013) addresses what he calls synthetic commodity money: “money that lacks nonmonetary value but is nevertheless reproducible only at a positive and rising marginal production cost, if indeed it can be reproduced at any cost at all.” Bitcoin is at the forefront of his analysis of synthetic commodity money. Graduate and undergraduate works also explore the Bitcoin and economics, complementing is the economic literature on Bitcoin.

3.1.5 On Other Graduate and Undergraduate Works

While most academic work on Bitcoin take on the form of working papers, articles, and publications, one must not neglect student input. The following subsection delves into the theses of other graduate and undergraduate students.

Ísak Andri Ólafsson’s (2014) Master of Science thesis argues that from an Austrian perspective, Bitcoin is not money, but should be considered synthetic commodity money. He provides an in-depth analysis on the functions of money from the same perspective. An

in-depth analysis of Bitcoin as a medium of exchange is provided by Peter Šurda's Master thesis (2012) that analyzes Bitcoin from a Libertarian perspective through the Austrian school of economics.

Jiří Šafka's Master thesis (2014) *Virtual currencies in real economy: Bitcoin* examines the relationship between virtual currencies, Bitcoin, and the real economy and inspects the volatility of Bitcoin price through Autoregressive heteroskedasticity models. His work influences the econometric basis in the analysis of this thesis. Martin Janota's bachelor thesis analyzes Bitcoin demand. Janota (2013) argues that the "quantity theory of money is well applicable on transaction-based data, which Bitcoin provides;" he uses the economic equation of exchange, fitted to the dynamics of Bitcoin, to estimate money velocity and output index. However, a different methodology is presented and used in this thesis. Davies' (2014) Honors Bachelor (2014) *The Curious Case of Bitcoin: Is Bitcoin volatility driven by online search?*, carries out an econometric analysis just like the one in this thesis, but looks at online searches from Twitter and Google as price determinants. The methodology is very similar in that his work uses vector autoregression modeling, Granger causality, and impulse-response functions; methods developed on in the fourth chapter.

3.1.6 On Bitcoin and Econometrics

The econometric analysis that is carried out in the Analysis chapter refers in many aspects to that of previous econometric work on Bitcoin. The main authors and their contributions are presented below.

Buchholz *et al.* (2012) use vector autoregression (VAR) models to study the relationships between transactions volumes, Google hits, and Bitcoin prices; they find that Google hits Granger cause transaction volumes. Bouoiyour and Selmi (2014) also use VAR models and find that investor attractiveness, which they measure using Google views, is an important driver of Bitcoin prices. They highlight the speculative nature of Bitcoin claiming that "Bitcoin behaves heavily as a speculative bubble" (2014). Kristoufek (2013) uses Google Trends and Wikipedia to study their relationship to Bitcoin price; he finds "a very strong correlation between [the] price level of the digital currency and both the Internet engines" and a strong causal relationship between prices and searched terms. In a similar line, Garcia *et al.* (2014) address the role of social interactions in the creation of price bubbles with regards to Bitcoin by quantifying four socio-economic signals about Bitcoin: price on online exchanges, volume of word-of-mouth communication in online social media sites, volume of information search, and user base growth. They use VAR to

“identify two positive feedback loops that lead to price bubbles in the absence of exogenous stimuli: one driven by word of mouth, and the other by new Bitcoin adopters” (2014).

Glaser *et al.* (2014) give empirical insights on whether users’ interest regarding digital currencies is driven by its appeal as an asset or as a currency. They find “strong indications that especially uninformed users approaching digital currencies are not primarily interested in an alternative transaction system but seek to participate in an alternative investment vehicle.”

Kristoufek (2014) examines potential drivers of Bitcoin prices through wavelet coherence analysis; he finds that “standard fundamental factors – usage in trade, money supply and price level – play a role in Bitcoin prices in the long term.” Gronwald (2014) deepens the understanding of Bitcoin price behavior by using a univariate time series model. He applies the autoregressive jump-intensity GARCH model; his results suggest that extreme price movements particularly mark Bitcoin price, a behavior generally observed in immature markets. More recently, Ciaian *et al.* (2014) also use VAR modeling to estimate four econometric models of Bitcoin price, finding that to a large extent, “the formation of BitCoin [*sic*] price can be explained in a standard economic model of currency price formation.”

With the literature review on Bitcoin completed, it is time to explore the relevant theory.

3.2 Relevant Theory

This section is devoted to the relevant theory required to pursue the hypotheses. It contains both the pertinent literature and models that will be explored in the fifth chapter. The first subsection presents the traditional functions of money. The second subsection presents the economic equation of exchange, first introduced by Irving Fisher. The third subsection introduces Wang’s (2014) proposed macroeconomic model for the valuation of Bitcoin, which is derived from the economic equation of exchange. The reasoning behind the econometric models used to carry out the empirical analysis of the Bitcoin market and their relevant literature is reserved for the methodology chapter.

3.2.1 On the Functions of Money

While different schools of economics have differently defined money, the definition of money in this thesis will be approached from a classical perspective. Numerous economic textbooks have covered what are known as the ‘traditional functions of money.’

Contemporary authors such as Parkin (2012) and Abel and Bernanke (2001) have developed concise renderings on what money is and what are its classical functions. Parkin (2012) describes money as “any commodity or token that is generally acceptable as a means of payment” and that a means of payment is a way to settle a debt. Abel and Bernanke (2001) argue that in economics money refers specifically to assets that are widely used and accepted as payment. Classical economists (Krugman 1984) argue that there are three main functions of money: medium of exchange, unit of account, and store of value. Each function is developed below.

3.2.1.1 Medium of Exchange

A medium of exchange solves barter’s double coincidence of wants problem. A user accepts the medium of exchange as payment for the good or service provided to the extent that he or she is confident that enough other users will accept it from them for another good or service. The users themselves determine the value of the medium of exchange by determining what and how much of it they will accept. While there have been many mediums of exchange throughout history, the most notable ones have been precious metals such as gold and silver. Economists refer to money that takes the form of a commodity with intrinsic value as commodity money (Mankiw 2011). In other words, commodity money has non-monetary use value and is naturally or inevitably scarce. On the other hand, fiat money has no non-monetary use value (Kyotaki and Wright 1989) and is scarce only by design.

Frederic Mishkin (2004) defines money as “anything that is generally accepted in payment for goods or services or in the repayment of debts.” In today’s modern economy, most money is fiat based; these act as the principal medium of exchange. Fiat money consists of coins, paper notes, and deposit credits issued by central banks. Legal tender is fiat money recognized and enforced by law through governments and the judiciary. The value assigned to fiat money far exceeds the near-zero marginal cost of production, with perhaps the exception of coins in certain cases (e.g. the U.S. penny). Fiat currency acquires its value from the confidence people have in the money’s future ability to “exchange such money for other financial assets and for real goods and services” (Federal Reserve Bank of Chicago 1994). Scarcity in fiat-based currencies is artificially designed because supply must be contrived to prevent hyperinflation and increase its legitimacy, which is why numerous counterfeiting measures are implemented.

A central bank's prime objective can be summarized as acting "for the economic interests of the nation, consistent with government economic policy" (Bank of International Settlements 2009). It does so primarily through three main methods: (1) maintaining price stability, subject to the money regime in operation, (2) maintaining financial stability and financial development, and (3) support the State's financing needs (Goodhart 2011). At the macroeconomic level, this encompasses the central banks' ability to control the money supply to regulate inflation and price stability; this is known as monetary policy. Central banks can also influence their currency's value on foreign exchange markets through market interventions. At the microeconomic level, central banks can act as lender of last resort.

Critics of fiat-based currencies argue that money should not be subject to financial controls such as restriction on convertibility, changes in interest rates, and changes to the money supply to help stabilize inflation and foreign exchange markets.

However, money functions as a medium of exchange and a device for carrying out transactions. It allows people to trade goods and services with fewer costs in time and effort, which allows for increased productivity and specialization (Bernanke 2012). Discussion now revolves on specifically what type of medium of exchange should be used. The function of medium of exchange is closely related to that of unit of account.

3.2.1.2 Unit of Account

A unit of account is an agreed measure that states the prices of goods and services. Money functions as the basic unit for measuring economic value in modern economics (Bernanke 2012). Doepke and Schneider (2013) highlight that "historically, units of account and media of exchange often used to be distinct, but became unified in modern economies characterized by the widespread use of government-issued nominal bonds" with the emergence of fiat-based currencies. Today, the medium-of-exchange and unit-of-account functions of money are closely linked. As a unit of account, money must be fungible (all units are viewed as having equal value), divisible (component parts are worth the same as a complete unit, e.g. $\$1.00 = 100 * \0.01), and countable (easily measured and calculated). Money's function as a unit of account is crucial in modern economics as a form of measurement for a plethora of economic variables and is usually stable in value relative to other goods traded in the economy.

3.2.1.3 Store of Value

Classical economists view money's function as a store of value as a way of holding wealth (Bernanke 2012). Money acts as a store of value in that it can be held and later exchanged for goods and services. However, future usage and value rely on money's acceptance in the future and that its value will remain stable or increase. This is not always the case as fiat-based currencies are subject to changes in inflation and volatility in foreign exchange market. Money as a store of value must be scarce, divisible, portable, and easy to store. Therefore, a store of value can take on many forms, such as: stocks, bonds, and real estate.

3.2.2 On the Economic Equation of Exchange

Wang (2014) bases his model on the economic equation of exchange from the quantity theory of money. Wang uses Fisher's (1911) economic equation of exchange in its simplest form.

$$M \cdot V = P \cdot T$$

where

M is the nominal amount of money; the money supply

V is the velocity of money

P is the price level

Q is the total volume of transactions of goods and services

There is much debate as to the validity of this equation and those inspired by it (Tao 2001; Hillinger and Süssmuth 2008; Agassi 1971). Classical economists, monetarists, and New Keynesians alike dispute the different interpretations of the equation. In this analysis, the equation is viewed as a tautology (Agassi 1971). The empirical study of economics is far from that of physics or chemistry. Given that the random variables gathered for the empirical econometric analysis are a result of a time series process, each realization is observed once and cannot be recreated (Woolridge 2006). In this analysis, Fisher's equation is used as in other studies, as a method to structure the interpretation of stochastic observations under a set of assumptions. Wang interprets the equation of exchange by adapting it to the dynamics of Bitcoin. The following subsection presents Wang's model; discussion of the model and how it is used in the analysis are reserved for the analysis chapter in section [5.2 Amending Wang's Macroeconomic Model](#).

3.2.3 Wang's Macroeconomic Model for the Valuation of Bitcoin

The price volatility on Bitcoin exchanges is a contentious issue and a main source of criticism from the media and academics alike. This volatility can be attributed to a plethora of factors. The macroeconomic model explored in this thesis seeks to determine whether the price of bitcoin is determined by the likelihood that a bitcoin will be saved.

Joseph Wang (2014) proposed a new macroeconomic model using Irving Fisher's economic equation of exchange to establish that "the main determinant of the price of bitcoin is the interaction between the level of bitcoin usage and the velocity of bitcoin." In this model, he adapts the equation to encompass the unique aspects of Bitcoin. This subsection presents the model, as described by Wang (2014) and solely summarizes this assumptions and claims. Interpretation and possible use of the model is covered in the fifth chapter.

The model begins with Fisher's (1911) economic equation of exchange:

$$M \cdot V = P \cdot Q$$

where

M is the nominal amount of money

V is the velocity of money

P is the price level

Q is the index of real expenditures

Subsequently, the economic equation of exchange is modified to allow for the particular aspects of Bitcoin. First, all quantities are expressed in units of fiat currency, which makes the price level P equal to 1 because Bitcoins are valued in terms of fiat currency. Given that all quantities are expressed in fiat currency, the value for M is now the value of bitcoin as measured in fiat currency units. The next assumption is that the quantity M is expanded to the number of bitcoin in circulation n_b and the price of a single bitcoin p_b expressed in fiat currency units.

$$(n_b \cdot p_b) \cdot V = Q$$

As seen in the second chapter, the number of bitcoin in circulation, n_b , is determined externally in a slow, predictable way. On the other hand, the price of a single bitcoin will fluctuate according to market demand and supply on Bitcoin exchanges. Rearranging the equation to isolate price yields:

$$p_b = \frac{Q}{n_b V}$$

Hence, the assumption is that the main determinant of the price of bitcoin is the interaction between the level of bitcoin usage and the velocity of bitcoin. Thus far, the model has not yet made any assumptions concerning the dynamics of Bitcoin.

The following equation contains assumptions on the dynamics of Bitcoin, particularly the relationship between the number of bitcoin expended, Q and the velocity of an individual bitcoin, V . The model then assumes that the velocity of bitcoin is two-fold: the velocity of a bitcoin that is saved and the velocity of a bitcoin that is transacted. The likelihood that an individual bitcoin is saved is denoted by l_s while the likelihood that a bitcoin is transacted is denoted by l_t . These two probabilities sum up to 1.

$$\sum_{k \leq 1} (l_s, l_t) = 1$$

Both l_s and l_t have corresponding velocities represented by v_s for the velocity of a saved bitcoin and v_t for the velocity of a transacted bitcoin.

$$p_b = \frac{Q}{n_b \cdot [(l_s \cdot v_s) + (l_t \cdot v_t)]}$$

The next assumption is that the velocity of a transacted bitcoin is much more than of a saved bitcoin, represented by the following assumption:

$$v_t \gg v_s$$

Wang then sets the velocity of saved bitcoins, v_s to zero, as a saved bitcoin has no velocity. The model assumes that “the velocity of transacted bitcoins can be modeled as a linear function of Q .” Therefore the total velocity of bitcoin is:

$$V = l_t \cdot \alpha_t \cdot Q$$

Once substituted back into the original equation for p_b :

$$p_b = \frac{1}{l_t \cdot \alpha_t}$$

The model then assumes that α_t “will remain roughly constant over time.” This leaves only one term that can influence the price of bitcoin, l_t . The model claims “the price of bitcoin is determined almost solely by the likelihood that a given bitcoin will be saved.” The

implications are two-fold. First, if bitcoin is used for transaction purposes, then this has no impact on the value of bitcoin. Second, if it is saved, then this has an influence on the value of bitcoin. The model also assumes that in the long run, shocks will not change the long-run price level of bitcoin if they do not change how likely a bitcoin is to be saved or transacted.

Furthermore, the model predicts that an “increased usage of bitcoin should manifest itself in larger volumes rather than increased prices.” In chapter 5, section [5.2 Amending Wang’s Macroeconomic Model](#) argues why some assumptions made in this model are wrong and amends the model to allow for empirical analysis of the Bitcoin market. The new model will help determine whether the price of bitcoin is determined by the likelihood that a bitcoin will be saved, with a method congruent with other econometric analyses in the field.

4 Methodology

This chapter establishes the foundation for the analytical section. First, the two hypotheses are presented, including the reasoning behind their inclusion. Next, the methods used in each section of the analysis to further the hypotheses are presented. This begins with answering why the functions of money are applied to Bitcoin arguing that while Bitcoin currently does fulfill the classical functions of money, its usage mainly remains as a speculative instrument. The reasoning behind the use of Wang's model as a basis for the analysis is provided along with how it is used therein. Finally, information on the econometric analysis is provided in the last section of the methodology chapter. The data and variables that were selected for the analysis are detailed, including how they were gathered and why they are important. Omitted variables and Gretl, the software used for the analysis, are briefly discussed as well. The chapter concludes with the employed econometric models.

4.1 Hypotheses

This analysis undertakes two different hypotheses in an attempt to assess the claims made by Wang (2014) on the valuation of Bitcoin. Wang's first claim is that the value of bitcoin (dependent variable) is not determined by its transactional use (independent variable). The independent variable that must be analyzed to assess this claim is the daily number of transactions, i.e. the transactional volume on the block chain. The dependent variable, the value of bitcoin, is the price of bitcoin in terms of fiat currency. The first claim is assessed by hypothesis H_1 .

H_1 : The price of bitcoin is not influenced by changes in the trade volume.

Wang's second claim is that "the value of bitcoin is determined largely by the willingness of bitcoin holders to save bitcoin" (2014). The independent variable that must be analyzed to assess this claim is Bitcoin days destroyed and the dependent variable is the price of bitcoin in terms of fiat currency. This second claim is assessed by hypothesis H_2 .

H_2 : The price of bitcoin is determined by the likelihood that a bitcoin will be saved.

The fourth subsection of this chapter presents the variables used in the analysis and provides an in-depth discussion as to their inclusion and relevance for addressing the two hypotheses. Section [5.2 Amending Wang's Macroeconomic Model](#) explains how Wang's model is changed to empirically analyze the Bitcoin market.

4.2 Bitcoin and the Functions of Money

As presented in the third chapter, the classical functions of money are applied to Bitcoin to determine the following: the extent and validity of Bitcoin as a form of money, if its behavior reflects that of a speculative investment, or both. This is a crucial stage to clarify both the breadth of Bitcoin as a currency and the applicability of the proposed macroeconomic model. Moreover, it helps to set forth the potential regulatory framework for Bitcoin, which will be addressed in the conclusion in hopes of stimulating future research in the fields of economics, law, and regulation.

4.3 Macroeconomic Model for the Valuation of Bitcoin

Prior to the econometric analysis, Wang's model is criticized and its assumptions are amended to narrow the scope of the analysis and strengthen the robustness of the results. It also addresses the limitations of the analysis and the interpretation of the results. This takes shape in section [5.2 Amending Wang's Macroeconomic Model](#).

4.4 Econometric Analysis

Econometric models and theories are used to complete the empirical analysis to assess the two hypotheses. While theoretically conferring over an economic model is the first step in establishing its validity, empirical evidence serves to assess the robustness of the assumptions made. Econometrics, the branch of economics concerned with the use of mathematical methods (especially statistics) in describing economic systems, is therefore befitting.

4.4.1 Data Selection and Collection

It is imperative to collect data prior to any analysis. Bitcoin's open-source software and the Bitcoin ecosystem provide an unmatched abundance of data. Blockchain.info (Blockchain.info 2015), CoinDesk.com (CoinDesk 2014; 2015a,b,c) and Bitcoincharts.com offer free API access to their Bitcoin data. Quandl.com (Quandl 2015) is a search engine for numerical data that freely provides data through API requests as well, but notably provides data downloadable in CSV, Excel, JSON, and XML formats. This subsection explores the reasons behind data selection and explains how and where it was collected. All variables used in the econometric analysis are described below:

Bitcoin Price Index

As the dependent variable in this analysis, the Bitcoin Price Index (BPI) published by CoinDesk (CoinDesk 2015c), represents the average of bitcoin prices across leading global exchanges; it is intended to serve as a standard retail price reference. To be included in the BPI, global exchanges are required to meet criteria specified by CoinDesk. For more detailed information on which exchanges are included in the BPI and how the BPI is calculated, please refer to [Appendix 2](#). The BPI acts as a substitute for price in the analysis, which is core to exploring Wang's Bitcoin valuation proposal. It is logical to use the BPI not only because it is a reliable reference, but also because it is expressed in USD, which is representative of the currency used in nearly 80% of exchange transactions. The BPI is currently the closest price rendering of Bitcoin in USD and has been used in many recent analyses (Bouoiyour and Selmi 2014; Kristoufek 2014). Daily data on the BPI's closing price was collected through CoinDesk's public access API in CSV format.

As the dependent variable in this analysis, the BPI sets the range of the time series. Therefore, the range for all variables was set between 14/09/2011 and 14/03/2015. While price data is available prior to September 2011, data is more reliable from then onward as seen in Kristoufek (2014). The end date is selected to include as many observations as possible prior to completing the analysis. (Note: the BPI is abbreviated in equations, figures and tables as **BPI**.)

Daily Number of Transactions

The first independent variable is the daily number of transactions; this represents the total number of unique bitcoin transactions appended to the block chain per day. It does not differentiate the types of transactions carried out on the block chain and does not include the number of transactions carried out off the block chain. Therefore, it is not a fully accurate representation of bitcoin usage, given that users can easily send bitcoins between their own addresses at will, which overstates the amount of economic activity on the block chain. In this analysis, the daily number of transactions is considered as the upper threshold of Bitcoin economic activity on the block chain, i.e. transactional use. While there has been research attempting to identify and calculate Bitcoin users (Ron and Shamir 2012) to narrow down economic activity, the daily number of transactions variable is currently the most reliable estimate of on-chain Bitcoin economic activity; several authors employ this estimate in their work (Buchholz *et al.* 2012; Glaser *et al.* 2014; Kristoufek 2014; Ciaian *et al.* 2014).

This variable is crucial to the analysis in assessing Wang's claim that the price of bitcoin is not determined by its transactional use; this is addressed in the first hypothesis, H₁. Daily data on the total number of transactions was collected through Quandl's public API in CSV format, which provides user-friendly access to the data provided by Blockchain.info. (Note: the daily number of transactions is abbreviated in equations, figures, and tables as **DNoT**.)

Bitcoin Days Destroyed Cumulative

The second independent variable is the daily cumulative number of Bitcoin days destroyed. Bitcoin days destroyed are calculated by multiplying the daily amount of Bitcoin in each transaction by the number of days since they were last spent, giving more weight to coins that have not been spent for a longer amounts of time. Ciaian *et al.* (2014) use Bitcoin days destroyed as a proxy for the monetary velocity of bitcoin. It is argued that it provides a better indication of how much real economic activity is occurring compared to the number of transactions. However, this analysis argues that when used as a measure of economic activity, Bitcoin days destroyed will always overstate the actual economic activity in the Bitcoin market because users can simply send bitcoins to themselves, reducing the amount of Bitcoin days destroyed.

Since Bitcoin days destroyed will always overstate the amount of economic and understate the amount of actual saving, Bitcoin days destroyed are used as an indication of economic inactivity or saving. This is congruent with the use of the daily number of transactions as an indicator of economic activity. The variables selected to represent the level of economic activity (transactions; DNoT) and inactivity (saving; BDDC) are currently the best available measurements to assess Wang's claims, and hence, the two hypotheses. The total number of bitcoins was collected through Quandl's public API in CSV format. (Note: the cumulative number of Bitcoin days destroyed is abbreviated in equations, figures, and tables as **BDDC**.)

Trade-Exchange Ratio

The third independent variable is the trade-exchange ratio; this represents the ratio between the volume of trades (i.e. daily number of on-chain transactions) and exchange transactions (i.e. off-chain transactions on Bitcoin exchanges). The trade-exchange ratio can be seen as a measure of transactional usage, in that "the lower the ratio, the more frequently Bitcoin is used for 'real world' transactions" (Kristoufek 2014). This variable provides

complementary insight when assessing Wang's claim that the value of bitcoin is largely determined largely by users willingness to save bitcoin; this is addressed in the second hypothesis, H₂. It is the ratio of Bitcoin usage in real-world transactions versus its potential use as a speculative instrument, although not all exchange transactions are carried out for speculative aims. Again, the reason behind each transaction is skewed by the fact that the intention behind each transaction is unknown.

Similar to the DNoT, daily data on the trade-exchange ratio was collected through Quandl's public API in CSV format. (Note: the trade-exchange ratio is abbreviated in equations, figures, and tables as **TexR**.)

Market Capitalization of Bitcoin

The fourth independent variable is the daily market capitalization of Bitcoin measured in USD. It is calculated by multiplying the value of a bitcoin times the number of bitcoins in circulation. The market capitalization variable influences the price of bitcoin because it is a popular figure cited both in the media and in academic writing. Such publicity might influence current and potential Bitcoin users alike, a type of 'investor attractiveness' measure. Glaser *et al.* (2014) posit that "the interest of new users has an influence on Bitcoin volume traded at the exchange, but not on the volume within the Bitcoin system;" they add that most new users trade Bitcoin as a speculative investment, which affects its price. It can therefore be argued that market capitalization can have an effect on the price of bitcoin with new users entering and leaving the Bitcoin ecosystem. The daily market capitalization of Bitcoin was collected through Quandl's public API in CSV format. (Note: the market capitalization of Bitcoin is abbreviated in equations, figures, and tables as **MrkC**.)

Total Number of Bitcoins

The fifth independent variable is the daily total number of bitcoins; this represents the sum of bitcoins in circulation. Given that the supply of bitcoins is fixed, this variable accounts for the total stock of bitcoins in circulation (Ciaian *et al.* 2014). It is important to include this variable in the analysis as it takes into account changes in the number of bitcoins available in the Bitcoin ecosystem for both trade in exchanges and the purchase of goods and services. In this analysis, the total number of bitcoins is viewed as an exogenous variable because the supply of bitcoins is asymptotically determined in a predictable way by the protocol and cannot be influenced by other variables. The total number of

bitcoins was collected through Quandl's public API in CSV format. (Note: the total number of bitcoins is abbreviated in equations, figures, and tables as **TNBTC**.)

Google Trends

The sixth independent variable, Google Trends, refers to the frequency of searches for the term 'bitcoin' regardless of capitalization. Powered by Google, Google Trends results are normalized so that the maximum value of the series is equal to 100. The relevance of search query variables is ample in the literature; it is used in the analysis based on Kristoufek's (2013) findings that there is a strong correlation between price level of the digital currency and search queries, which therefore makes it a good measure of potential investor interest. Both Wikipedia page views (Kristoufek 2013; Glaser *et al.* 2014; Ciaian *et al.* 2014) and Google Trends (Buchholz 2012; Kristoufek 2013, 2014; Bouoiyour and Selmi 2014; Garcia *et al.* 2014) have been used as crucial variables in econometric analyses of the Bitcoin market. Therefore, daily data from Google, the world's leading search engine, is a proper fit.

The Google Trends data was collected on the Google Trends webpage (Google Trends 2015). Once logged in, the daily global data for 'bitcoin' was downloaded in CSV format in three-month increments (the maximum range allowing daily data) and manually chained into a full time series. One drawback is that the reason behind search queries is unknown. (Note: the normalized Google Trends search queries are abbreviated in equations, figures, and tables as **GT**.)

Hash Rate

The seventh independent variable is the hash rate; this represents the measure of the Bitcoin network's processing power. This analysis uses hash rate as an indicator for network participation. As seen in the second chapter, the network difficulty is mirrored by hash rate, which can influence the price of bitcoin; a falling hash rate could signify a decreasing amount of miners and be an indicator of a loss of interest in Bitcoin. The hash rate was collected through Quandl's public API in CSV format. (Note: the hash rate is abbreviated in equations, figures, and tables as **HashR**.)

Exogenous Shocks

The eighth and final independent variable is a dummy variable for exogenous shocks; it represents significant events that may have affected the Bitcoin ecosystem. Building on Glaser *et al.* (2014), a set of 39 exogenous variables (1 for an exogenous shock, 0

otherwise) was manually compiled in CSV format using information from two websites (History of Bitcoin 2015; I Got Bitcoin 2015) and from CoinDesk's *State of Bitcoin* (2014, 2015a,b). Together, they provide a comprehensive listing of major Bitcoin events. The selection process was carried out to include as many significant events as possible while ignoring the less significant ones. Since there are no fixed numerical criteria for their inclusion, more details are provided on the events and their selection in [Appendix 3](#). (Note: the exogenous shocks variable is abbreviated in equations, figures, and tables as **ExSh**.)

Omitted Variables

There are many other variables that could have been included in the analysis. Some were omitted due to potential redundancy (difficulty vs. hash rate, Bitcoin days destroyed cumulative vs. non-cumulative, total number of bitcoins vs. daily mined bitcoins, etc.). Others were omitted due to lack of data (number of Bitcoin users, number of businesses that accept bitcoin, off-chain transactions between users of a third party system). While it is hard to evaluate economic activity on the block chain (DNoT vs. BDDC), it is even more difficult and practically impossible to account for the total Bitcoin economic activity in the Bitcoin ecosystem. For example, a user with a Coinbase wallet purchasing goods from a merchant with a Coinbase account will result in the transaction being carried out off the block chain. Furthermore, Coinbase offers off-block chain micro-transactions between Coinbase accounts free of transaction fees (Coinbase 2013).

Variables outside of the Bitcoin ecosystem used in previous research (e.g. price of gold, price of crude oil, Financial Stress Index) were excluded to limit the scope of the analysis to factors within Bitcoin's ecosystem. More details are provided in section [5.2 Amending Wang's Macroeconomic Model](#). Taking these characteristics into consideration, this analysis posits that all relevant variables have been included in light of their contributions and drawbacks.

4.4.2 Software

Gretl is a cross-platform, open-source software package used for econometric analysis. This software is used since the targeted analysis does not require the creation of new functions. Moreover, Gretl's user interface is simple and easy to operate, which speeds up reproduction of the analysis and provides results standard to most econometrics students. The use of Gretl will also allow others to reproduce the results and 'play' with the data more easily (see [Appendix 6](#)).

4.4.3 Econometric Models

This subsection presents the econometric reasoning and models used in the analysis and simultaneously acts as the literature review for the theories and models used in the econometric analysis. While the methods are described, the results and discussion of the analysis are reserved for the fifth chapter.

Once data is acquired, it is important to determine its type. The data in this analysis is time series data consisting of observations of several variables over time issued from a stochastic process (Woolridge 2006). Since past events can influence future events and lags are prevalent, it is imperative to have a chronological ordering of the observations; this is why the range was set chronologically between 14/09/2011 and 14/03/2015 for all variables and the data frequency was set to daily. Taking into consideration the potential for a heteroskedastic time series and to allow for an easier interpretation of the results, all variables (except ExSh) were transformed to their natural logarithm (denoted $l_variable$). Using log-log modeling addresses the potential heteroskedasticity, simplifies the model, and allows for the interpretation of the respective elasticity of all variables.

The next step is to determine whether the time series data is stationary. Stationary data has the mean, variance, and autocorrelation structure constant over time. Plotting the variables exposes signs of a random walk (Woolridge 2006), a unit root process. Therefore, the assumption is that the time series is non-stationary and qualifies as an AR(1) model. The Augmented Dickey-Fuller (ADF) test is used to test for non-stationary. The ADF test is preferred over other autoregressive unit root tests because many financial time series “have a more complicated dynamic structure than is captured by a simple AR(1) model” (Zivot and Wang 2006); to correct for this, the ADF allows for a lag order. It augments the basic autoregressive unit root test to accommodate general ARMA(p, q) models with unknown orders (Said and Dickey in Zivot and Wang 2006). The maximum lag order, p_{max} , for the ADF test is based on Schwert’s (1989) suggested equation where T represents the number of observations:

$$p_{max} = \left[12 \cdot \left(\frac{T}{100} \right)^{1/4} \right]$$

To get an indication of whether the time series is non-stationary, the ADF test was carried out on the natural logarithm of the dependent variable BPI, l_BPI . More details on the selected criteria for the ADF test and the results are provided in the subsection [5.3.1](#)

Augmented Dickey-Fuller Test. The null hypothesis that there is a unit root was not rejected and therefore warrants further investigation in the time series' stationarity. Zivot and Wang (2006) posit that “pre-testing for unit roots is often [...] required to make sense of regression models and VAR models with I(1) data.” Two non-stationary series are cointegrated if they tend to move together through time.

In technical terms, time series data is cointegrated when two series are integrated to different orders and their linear combinations will be integrated to the higher of the two orders. Woolridge (2006) writes that “the notion of cointegration, which was given a formal treatment in Engle and Granger (1987), makes regressions involving I(1) variables potentially meaningful.” To further investigate, the ADF test was carried out on all variables. First differencing was carried out on the variables found to be a unit root. With the unit root variables differenced, VAR modeling can then be used because the variables are now of the same order with a similar level of integration. Vector auto-regression models are used to analyze the causality between endogenous time series. It is possible to determine Granger causality from the VAR results.

Granger causality is useful in that it allows for testing whether after controlling for the past of a variable, Y , the past variable X helps forecast Y_t (Wooldridge 2006; Zivot and Wang 2006). It is used to describe intertemporal relationships (Guo *et al.* 2010). Therefore, a variable X Granger-causes Y if Y can be better predicted using the histories of both X and Y than it can using the history of Y alone. The null hypothesis for the Granger causality test is: no Granger causality.

While providing p-values to establish the significance of Granger Causality between variables, Granger causality tests do not provide any information on the direction of the impact that the variable of interest has on another variable. Therefore, impulse response functions (IRF) are used to remedy this by tracking the responses of a system's variables to impulse of the system's shock. An IRF acts as an exogenous shock to the error term of the multivariate VAR in this analysis. The Cholesky ordering used to generate the IRFs is explained in the Analysis chapter. With the methods presented and established, it is time for the core value added of the thesis: the analysis.

5 Analysis

The analysis chapter constitutes the main value added of the thesis. The first part applies the functions of Bitcoin to money in order to assess if Bitcoin does in fact act as a form of money, a speculative instrument, or both. The following section discusses Wang's macroeconomic model, criticizing the model and amending it to create a more robust analysis. The final part of this chapter revolves around testing the two hypotheses undertaken in the thesis through econometric analysis using the methodology provided in the previous chapter. The chapter concludes with a discussion of the results and other interesting findings.

5.1 Bitcoin and the Functions of Money

Applying the functions of money to Bitcoin will reveal if Bitcoin does in fact act as a form of money, if it is merely a speculative instrument or both. Assessing if Bitcoin acts as a medium of exchange, unit of account, and store of value structures the analytical framework for the applicability of Wang's model and the econometric analysis.

5.1.1 Bitcoin as a Medium of Exchange

Bitcoin acts as a medium of exchange. The scope of its use as a medium of exchange is bound by the limits of Bitcoin's ecosystem. Bitcoin is an electronic token, "a container that carries value across the network" (Evans 2014). It is not pegged to an underlying commodity or sovereign currency. Owning and using bitcoins is limited to Bitcoin's ecosystem and solves the double coincidence of wants within its ecosystem. Bitcoin is fiat money, just like other modern fiat-based currencies (DuPont 2014). The difference is that bitcoins are backed by cryptography and proof-of-work rather than by governments and central banks; Bitcoin mining and the prevention of double spending provide the scarcity element. Both bitcoins and dollar bills have no intrinsic value. A Bitcoin user is willing to accept it as a form of payment for goods and services believing someone else will accept it in return at a later time. Unlike fiat-based currencies, no one can compel Bitcoin's acceptance. Therefore, Bitcoin's role as a medium of exchange is constrained by the extent of its ecosystem, which reflects users' acceptability of Bitcoin as a form of payment for goods and services.

Novel decentralized cryptographic currencies entice their share of skepticism and criticism, and Bitcoin is no different. Bitcoin's use as a medium of exchange is far from its potential.

Bitcoin evolves as the understanding of its functioning increases, issues are addressed, and solutions proposed and implemented. It is possible to witness Bitcoin's evolution as a medium of exchange by reviewing the literature. Expansion of its acceptance as a means of payment by major corporations such as PayPal and Overstock, easier and safer to use interfaces for Bitcoin wallets, market exchange pricing for customers, instantaneous exchange facilities for retailers, and FinCEN's (2013) recognition of Bitcoin as a medium of exchange are some of the numerous examples of Bitcoin's evolution in recent years.

However, this progress has come at high costs. Bitcoin's brief history is plagued with controversy. The controversial closure of Bitcoin exchanges (particularly Mt. Gox), the publicized thefts of bitcoins, hacked wallets, Bitcoin's use in illegal activities (e.g. Silk Road), and its price volatility are some of the numerous factors which make potential Bitcoin users wary. Their wariness is justified. However, not all controversies have gone unpunished: Mt. Gox users are now seeing their funds refunded (Kraken 2015), Silk Road's mastermind was trialed, condemned, and the seized bitcoins were sold at auction by US Marshals (CoinDesk 2015a).

Furthermore, participation in any nascent endeavor involves a plethora of risks. Whether customer, retailer, or speculator, it is a user's responsibility to assess the potential risks and benefits in venturing out into Bitcoin's ecosystem, just like it is to participate in the stock market. With high risks come high rewards or high losses. Bitcoin's value is established on Bitcoin exchanges where demand and supply of bitcoins is derived from a combination of the demand for its use as a medium of exchange and as a speculative investment. Bitcoin prices are "particularly marked by extreme price movements; a behavior generally observed in immature markets" (Gronwald 2014). Bitcoin's value is determined by "(a) the eagerness of speculators to hold bitcoin as an asset, and (b) the willingness of transactors [*sic*] to hold bitcoin as a medium of exchange" (Luther and White 2014). The inevitable conclusion is that Bitcoin acts both as a medium of exchange and a speculative instrument. The extent to which it acts as a medium of exchange and a speculative instrument is changing (Yermack 2014). Price volatility will decrease as Bitcoin is used more as a medium of exchange.

5.1.2 Bitcoin as a Unit of Account

Bitcoin's role as a unit of account is debatable. An early critic of Bitcoin as a unit of account, Yermack (2014) wrote that "perhaps the most serious obstacle to bitcoin becoming a widely used unit of account – and one often overlooked or trivialized by

bitcoin enthusiasts – occurs due to the relatively high cost of one bitcoin compared to most ordinary products and services.” Indeed, pricing in terms of bitcoins might influence consumer behavior, but developments in Bitcoin payment systems are making accepting bitcoins as a medium of exchange easier, and hence simpler to use as a unit of account. With growth of the Bitcoin ecosystem and advances in payment processing, merchants can now quote the prices of their retailed goods in both Bitcoin and fiat-based currencies. The rate at which the price in bitcoins is refreshed varies between merchants, but is usually around 10 to 15 minutes. Bitcoin has become easier to use as a unit of account with the introduction of market exchange pricing for customers and the provision of instantaneous exchange facilities for retailers who are not required to bear the effects of Bitcoin’s volatility. Bitcoin merchant solutions provide instant conversion of funds and are willing to take on the volatility risk of Bitcoin price.

The varying price between exchanges, a violation of the classical law of one price, is another issue faced by Bitcoin in becoming a unit of account. This is mitigated by the indices such as the BPI. Currently, Bitcoin’s use as a unit of account is fairly limited, which is congruent with its role as a medium of exchange. While bitcoins are fungible, divisible, and countable, their use as a unit of account is “so far entirely derived from, and hence secondary to, its medium-of-exchange function” (Lo and Wang 2015).

5.1.3 Bitcoin as a Store of Value

Currently, Bitcoin is not a reliable store of value. With a fixed supply, Bitcoin is not designed to accommodate shocks to its money demand. These shocks, which are often volatile, cause Bitcoin’s purchasing power to fluctuate with the demand for Bitcoin (Luther and Olson 2013). As a novel digital cryptocurrency, Bitcoin has been the subject of much speculation and volatility is a major source of criticism. Bitcoin’s use as a speculative instrument contributes to its price volatility. Early adopters have sought to cash in on the potential increase in value; hoarding bitcoins is pushing the price up. A very notable example of speculation occurred between 15/10/2013 to 16/12/2013. A price bubble formed, starting from Baidu – China’s largest search engine – accepting bitcoins and ending with the People’s Bank of China issuing a statement stating that China’s payment processors cannot deal with bitcoins. The price went from 139\$ on 15/10/2013, peaking at \$1068 on 02/10/2013 before dipping to \$522 on 18/12/2013.

As illustrated, the price volatility of Bitcoin does make it a poor store of value. Yermack (2014) states that “Bitcoin’s value is almost completely untethered to that of other

currencies, which makes its risk nearly impossible to hedge for businesses and customers and renders it more or less useless as a tool for risk management.” While the extent of Yermack’s claims might be refuted by some today given the growth in Bitcoin’s ecosystem, it remains that even as a temporary unit of account, Bitcoin does not fulfill this function of money adequately.

5.1.4 Is Bitcoin Money?

Applying the functions of money to Bitcoin reveals that it is still being used as a speculative instrument rather than a currency. This is congruent with most findings and particularly that of Yermack 2014. However, it is clear from the material presented in this thesis that Bitcoin was not designed to compete with mainstream fiat-based currencies and that its future lays in the digital cryptographic realm. This does not mitigate the fact that it fulfills the functions of money to a certain extent. Bitcoin’s closed ecosystem provides a plethora of data unlike many other financial markets. Even if it is used principally as a speculative instrument, the Bitcoin market can be analyzed and discussed. It is important to remember that: “payment and money are sociological and economic phenomena – certain things are accepted as money or payment by social consensus – and while this can change over time, trust in new forms of money takes time to develop” (Bollen 2013). Bitcoin’s fulfillment of the functions of money allows for it to be used in pursuing Wang’s model, while highlighting its notable use as a speculative instrument.

5.2 Amending Wang’s Macroeconomic Model

This subsection revisits Wang’s model. It starts by acknowledging the weaknesses in the model, criticizing the assumptions and amending them. It concludes by presenting the valuation model used to further the hypotheses, providing further explanations on why the variables discussed in the methodology section were included in the econometric analysis.

Wang (2014) uses the economic equation of exchange to explore the price determinants of Bitcoin. His model takes into consideration economic activity on the block chain. His assumptions on the dynamics of Bitcoin thereby exclude a significant portion of Bitcoin economic activity that occurs off the block chain. Wang’s model starts to falter when it assumes that “the velocity of transacted bitcoins can be modeled as a linear function of Q” in equation:

$$V = l_t \cdot \alpha_t \cdot Q$$

In reality, measuring the velocity of bitcoin is very difficult, if not impossible. One reason is embedded in Bitcoin's protocol: the inability to differentiate between the types of transactions and the users behind them. The velocity of bitcoin, in terms of the daily number of transactions, overstates the amount of economic activity on the block chain. For example, users can send bitcoins to themselves or use mixing services that make bitcoins harder to track to secure their funds, which adds transactions to the block chain without actually contributing to the velocity of Bitcoin. However, the daily number of transactions can still be used as a proxy for economic activity on the block chain and provide insight on its influence on the price of bitcoin and is used in this analysis to proxy the likelihood that a bitcoin will be transacted.

The complexity of calculating transactions off the block chain is another factor that makes measuring the velocity of bitcoin difficult. Calculating how frequently bitcoins are used in a given period of time for a specific purpose (e.g. purchasing goods and services) is made more inaccurate when transactions can be carried out off the block chain, such as micro-transactions between Coinbase accounts. Therefore, the velocity of transacted bitcoins cannot be modeled as a linear function of the total number of bitcoins Q , voiding the constant α_t .

With the daily number of transactions as a proxy for the velocity of bitcoin in terms of economic activity on the block chain (trade volume), a proxy is set for the amount of economic inactivity on the block chain (saving). Bitcoin days destroyed serves as a proxy for the likelihood that a bitcoin will be saved. Alike Wang's model, the amended model states that the velocity of a saved bitcoin is zero. Having a proxy for the velocity of a saved bitcoin provides a counterweight to the shortcomings of the daily number of transactions as a proxy for the velocity of a transacted bitcoin. As presented in the methodology chapter, Bitcoin days destroyed is a potential indication of economic inactivity, but it understates the amount of actual saving. Alike the daily number of transactions, the bias in measurement is caused by the inability to know the intent behind transactions recorded on the block chain. Bitcoin days destroyed will be fewer if users transact the money without actually contributing to the velocity of bitcoin (sending funds to themselves, using mixing services). In addition, the intent behind the destroyed days – whether the bitcoins are saved, lost, or moved off the block chain (e.g. to a Bitcoin exchange account) – is also unknown. Nevertheless, Bitcoin days destroyed provides an effective proxy to measure the

effects of saving on the price of bitcoin and has been used as a proxy for the velocity of bitcoin in other research (Ciaian *et al.* 2014).

Therefore, this analysis amends Wang's measurement of velocity to adapt it to the realities of empirically analyzing the velocity of bitcoin on the block chain. Rather than being a linear function of the amount of bitcoins in circulation, the velocity of bitcoin on the block chain is a combination of both economic activity and inactivity, represented by DNoT and BDDC respectively. It is important to highlight that the two proxies used for the analysis are variables that are measured on the block chain and that the velocity of bitcoin off the block chain is not included. Any potential finding with regards to the price of bitcoin is therefore limited to activity on the block chain. To take this into consideration, the variables used as potential price determinants of bitcoin in the analysis are closely related to activity on the block chain.

To determine if the proxies for velocity have an influence on the price of bitcoin, all other potential price determinants must be included in the econometric model. Developed in the methodology section, the potential price determinants of bitcoin were set as: DNoT, BDDC, TexR, MrkC, TNBTC, GT, HashR, and ExSh. The following variables are determined on the block chain: the daily number of transaction, Bitcoin days destroyed cumulative, the total number of bitcoins, and the hash rate. Economic activity off the block chain is presented in relation to economic activity on the block chain through the trade-exchange ratio. Google Trends and Exogenous shocks occur off the block chain but are assumed to have a direct impact on block chain activity. Market capitalization is a function of the bitcoin price and the total number of bitcoins.

With the model and its assumptions amended to add two proxies for the velocity of bitcoin and having taken into consideration all relevant potential price determinants, the econometric analysis can now be completed.

5.3 Econometric Analysis

The econometric analysis serves as an empirical analysis of the Bitcoin market to determine whether Wang's two main assumptions are indeed correct. This section is devoted to the discussion of the results and findings from the econometric analysis. The methodology chapter provides an overview of what variables, models, and tests are included in the analysis and why. Therefore, this section focuses on the results rather than reintroducing the theory behind each model. The analysis begins with Augmented Dickey-

Fuller tests on all the variables to determine if they contain a unit root. Once all variables are on a similar level of integration, the VAR lag selection test is completed. With the number of lags established, the VAR analysis is carried out. From the VAR results, Granger causality between the variables is discussed and impulse-response functions are provided. This section concludes with other interesting findings.

5.3.1 Augmented Dickey-Fuller Test

The ADF test is used to determine if variables in the equation contain a unit root and are therefore non-stationary. The null and alternative hypotheses are as follows:

H_0 : The variable contains a unit root.

H_a : The variable was generated by a stationary process.

An ADF test was carried out on all logged variables. Following Schwert's equation presented in the methodology, maximum lag order was set to 22. All ADF tests used the Akaike information criterion and tested down for maximum lag order with a constant. The results are summarized in the following table:

Table 1: Summarized ADF Test Results

<i>Variable</i>	<i>Asymptotic p-value</i>	<i>H₀</i>
<i>l_BPI</i>	0.7376	Cannot reject
<i>l_DNoT</i>	0.3845	Cannot reject
<i>l_BDDC</i>	0.006519	Reject at 1%
<i>l_TexR</i>	0.006726	Reject at 1%
<i>l_MrkC</i>	0.7375	Cannot reject
<i>l_TNBTC</i>	0.07443	Reject at 10%
<i>l_HashR</i>	0.9969	Cannot reject
<i>l_GT</i>	0.0009229	Reject at 1%
<i>d_l_BPI</i>	8.341e ⁻²⁸	Reject at 1%
<i>d_l_DNoT</i>	4.74e ⁻¹⁶	Reject at 1%
<i>d_l_MrkC</i>	1.066e ⁻²⁰	Reject at 1%
<i>d_l_TNBTC</i>	0.5802	Cannot reject
<i>d_l_HashR</i>	7.733e ⁻⁰⁵	Reject at 1%

Variables with a p-value > 0.05, in bold, are considered to contain a unit root because it is not possible to reject H_0 that the variable contains a unit root at the 5% significance level. As discussed in the methodology section, for all variables to be on a similar level of integration and thereby suitable for VAR, the first difference was taken for: *l_BPI*, *l_DNoT*, *l_MrkC* and *l_HashR*. All variables with a first difference were appended with a

d_1 prefix. Although it is not possible to reject H_0 at 5% for l_1 TNBTC, the first difference was not taken for two reasons: (1) taking the first difference and running the ADF test resulted in a p-value of 0.5802, worse than in its logged form (0.07443) and (2) it is used as an exogenous variable in the VAR model. The increase in the p-value of l_1 TNBTC after taking the first differences can be attributed to its asymptotic increase at a fixed rate that is determined in the Bitcoin protocol. Therefore, the null hypothesis was rejected at 10% for l_1 TNBTC. Based on econometric theory and from running the ADF test on d_1 BPI, d_1 DNoT, d_1 MrkC and d_1 HashR, it is possible to reject the null hypothesis at 1% and use them VAR modeling.

5.3.2 VAR Lag Selection

Vector autoregression modeling is sensitive to lag. Gretl provides a command to ease appropriate lag selection. The VAR lag selection test was completed to include a constant with a maximum lag order of 14, the equivalent of two weeks for daily data. The endogenous variables were: d_1 BPI, d_1 DNoT, l_1 BDDC, l_1 TexR, d_1 MrkC, d_1 HashR, and l_1 GT. The exogenous variables were: l_1 TNBTC and ExSh. The results of the VAR lag selection are provided in [Appendix 4](#). The optimal number of lags is 7 according to the AIC, which is equivalent to one week for daily data.

5.3.3 VAR Results and Granger Causality

Once all the variables are on a similar level of integration (not unit root) and the optimal number of lags is determined, it is time to carry out the VAR analysis. The choice of endogenous and exogenous variables is the same as in the VAR lag selection test, which is in accordance to the reasoning provided in the methodology chapter. To account for potential autocorrelation, HAC (Heteroskedasticity Autocorrelation Consistent) robust standard errors are selected. A constant is also included. The main results are summarized in Table 2.

The results of the F-tests provided by the VAR are used to determine Granger causality between variables. The null and alternative hypotheses for Granger causality are as follows:

H_0 : There is no Granger causality.

H_a : There is Granger causality.

Table 2: Summarized VAR Results

<i>Causality:</i> ↑	d_l_BP I	d_l_DNo T	l_BDDC	l_TexR	d_l_MrkC	d_l_HashR	l_GT
d_l_BPI	0.6096	0.0187	0.017	0.0274	0	0.0789	0.7285
d_l_DNoT	0.5548	0	0.2695	0.1609	0.4878	0.2015	0.0525
l_BDDC	0.0407	0.3144	0	0.9923	0.0963	0.0512	0.8089
l_TexR	0.9287	0.9348	0.3457	0	0.3386	0.2402	0.6832
d_l_MrkC	0.4032	0.3199	0.0079	0.0254	0	0.042	0.6457
d_l_HashR	0.5897	0.0023	0.5472	0.9143	0.6078	0	0.0359
l_GT	0.2802	0.0065	0.4853	0.0006	0.1217	0.0012	0

Note: The table summarizes the p-values of the F-tests. P-values < 0.05 are in bold.

Interpretation: a variable in the 1st column is said to Granger-cause a variable in the 1st row if the p-value < 0.05. The arrow in cell 1:1 indicates the direction of causality.

Granger causality is core in determining whether or not the potential price determinants of bitcoin have an effect on the dependent variable, BPI. The VAR results in Table 2 are used to assess the two hypotheses:

H₁: The price of bitcoin is not influenced by changes in the trade volume.

With a p-value of 0.5548, the null hypothesis cannot be rejected; there is no Granger-causation between the trade volume, denoted as d_l_DNoT , and Bitcoin price, denoted as d_l_BPI . With this result, it is possible to accept Wang's claim that the price of bitcoin is not influenced by changes in the trade volume under the assumptions made in section 5.2. In other words, block chain economic activity does not have a significant impact on the price of bitcoin. This conclusion is in line with two main factors addressed in the thesis with regards to activity off the block chain: (1) the price of bitcoin is determined on Bitcoin exchanges and (2) as established in section 5.1, Bitcoin is still used as a speculative instrument rather than a currency.

H₂: The price of bitcoin is determined by the likelihood that a bitcoin will be saved.

With a p-value of 0.0407, the null hypothesis can be rejected at a 5% significance level; there is Granger-causation between the number of saved bitcoins, denoted as l_BDDC , and Bitcoin price, denoted as d_l_BPI . With this result, it is possible to accept Wang's claim that the price of bitcoin is determined by the likelihood that a bitcoin will be saved. Therefore, economic activity on the block chain does have an impact on the price of bitcoin. This conclusion is in line with the mechanics of Bitcoin presented in the thesis: (1) inactive bitcoins on the block chain can be active off the block chain, (2) lost bitcoins decrease the total amount of bitcoins that can be used in its price determination on Bitcoin

exchanges, (3) saving decisions will affect the supply (e.g. more saving, fewer bitcoins for transactions) and demand (e.g. as a speculative instrument) on Bitcoin exchanges.

With Granger causality established for H_2 , it is possible to gather information on the direction of the impact that the variable of interest (BDDC) has on the dependent variable (BPI) with an impulse-response function. The IRF tracks the response of the Bitcoin Price Index to a shock in Bitcoin days destroyed.

5.3.1 Impulse-Response Function: BPI to a shock in BDDC

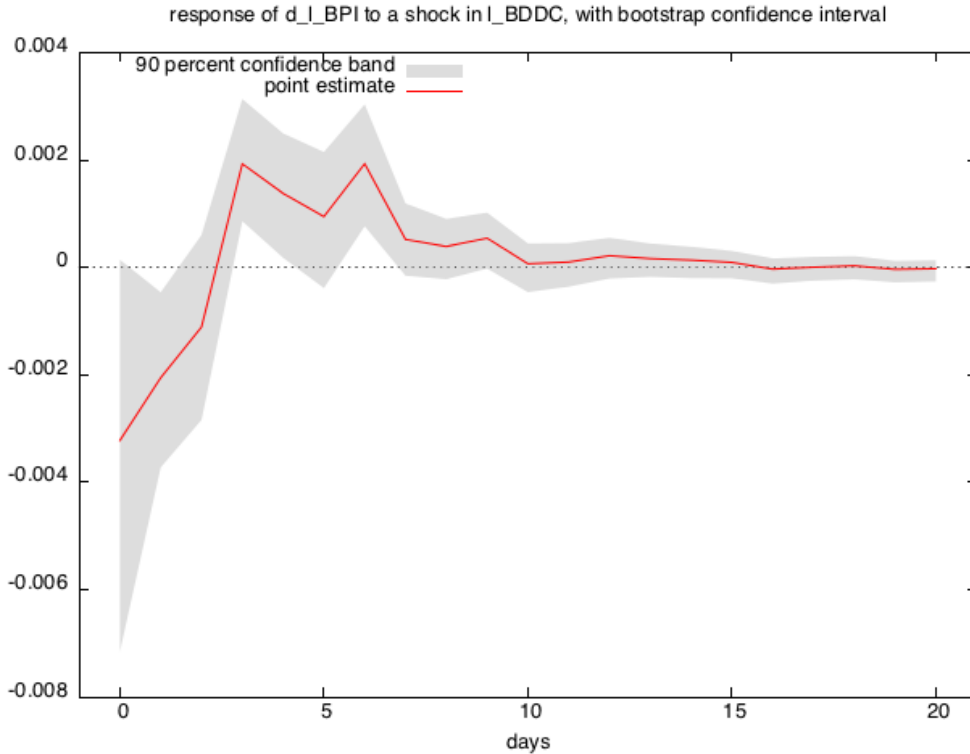
The most important element in carrying out an IRF is to determine the Cholesky ordering. The Cholesky ordering is used because residuals from a VAR model are generally correlated and applying the Cholesky decomposition is equivalent to assuming recursive causal ordering from the top variable to the bottom variable. It allows to adjust for temporal effects. The Cholesky ordering is based on theoretical arguments rather than from the VAR results given the complexity of the interaction between the variables and the debatable causal relations that can be interpreted from the VAR model.

The Cholesky ordering is determined by establishing (theoretically) the order in which the independent variables react to a shock in the dependent variable. While Gretl sets the last influenced variable first, it is presented here from first to last. A change in the Bitcoin Price Index has an immediate impact on market capitalization. Then, the daily number of transactions is influenced as bitcoins can be moved to and from exchanges, which immediately impacts the trade exchange ratio. This movement then influences Bitcoin days destroyed. Search queries on Google Trends are then affected as information propagates and interest in Bitcoin changes. The hash rate is the last variable to change, given that a lot of resources are involved in network participation, i.e. mining.

With the Cholesky ordering set, the IRF can then be generated, as illustrated in Figure 1. By using logarithmic differences, it is possible to interpret the shock in percentage terms. Figure 1 demonstrates that, in the short term, an increase in Bitcoin days destroyed (saving) causes Bitcoin price to fall. After the third day, there is a positive bounce back and price increases slightly, before converging to zero after approximately one week. In other words, a 10% increase in economic inactivity causes a 0.3% decrease in the price of bitcoin on the first day and by the third day, that negative effect is negated. On the fourth day, the price of bitcoin increases by 0.2% relative to its original price. After the 7th day, the shock converges back to around zero. It is possible to conclude from the IRF in Figure

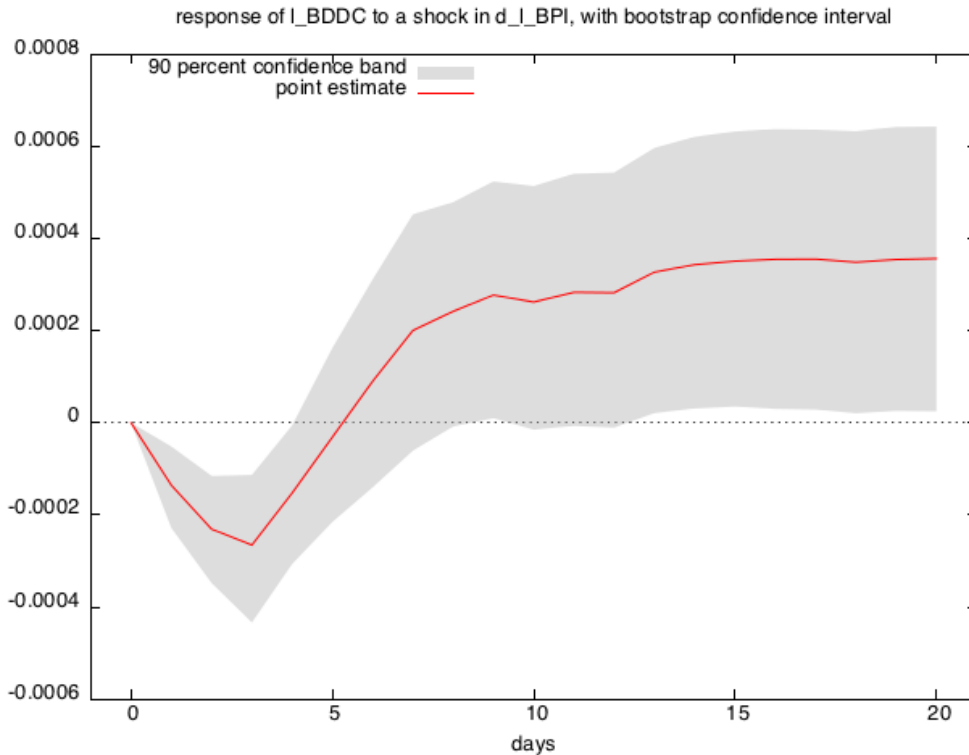
1 that the Granger-causal effect is quite weak. This can be attributed to Bitcoin’s extreme price volatility.

Figure 1: Impulse-Response Function of BPI to BDDC



From the VAR results, it can also be concluded that there is a bidirectional relationship between Bitcoin days destroyed and the Bitcoin Price Index: saving influences the price of bitcoin (H_2) and the price of bitcoin influences saving. In Table 2, with a p-value of 0.017, d_I_BPI Granger-causes I_BDDC . The IRF for this Granger-causal relationship is provided in Figure 2. An increase in the price of bitcoin causes a gradual decrease in Bitcoin days destroyed for the first three days as economic activity on the block chain increases. One example could be an increase in transactions from users more prone to pay in bitcoins, given the lower opportunity cost of using bitcoins rather than fiat currency. However, from the third day, Bitcoin days destroyed increases as illustrated in Figure 2. The results reflect the assumption that Bitcoin is used a speculative instrument, i.e. saving increases when price increases to increase potential returns. Given the volatility in the price of bitcoin, it is impressive that significant results (at 5%) can be obtained.

Figure 2: Impulse-Response Function of BDDC to BPI



5.3.2 Other Interesting Findings

One of the most interesting findings relates to Wang’s original proposal: “the price of bitcoin is determined almost *solely* by the likelihood that a given bitcoin will be saved” (emphasis added). The word *solely* was removed from H_2 to narrow the scope of the analysis. Surprisingly, under the assumptions made and the model amended, the VAR results show that savings (Bitcoin days destroyed) is the *only* variable for which it is possible to reject the null hypothesis that there is no Granger causality on BPI. This finding can be used in future research on the price determinants of Bitcoin for its original contribution to the field.

Another interesting finding is that there is a significant Granger causality between Google Trends and the daily number of transactions with a p-value of 0.0065. This is congruent with the findings of Buchholz *et al.* (2012). This means that economic activity on the block chain is influenced by the amount of search queries, which are a form of investor attractiveness.

Another very insightful finding is that BPI (0.0274), MrkC (0.0254), and GT (0.0006) all have a Granger-causal effect on the trade exchange ratio. This provides insight on the

relationship between on-chain and off-chain activity. Bitcoin price, its market capitalization, and Google Trends are all factors that can theoretically influence the ratio between the number of transactions on the block chain (trade volume) and off the block chain (exchange transactions). They are all factors that can influence whether bitcoins are being speculated or used as a medium of exchange. These findings are illustrated by the impulse-response functions in [Appendix 5](#), where an interpretation of each figure is provided.

As a final note, it is important to remember that Granger causality is only equivalent to causation under the restrictive assumption that there are no other potential causes. The analysis has encompassed variables deemed suitable in furthering the two hypotheses to mitigate this assumption. Moreover, it is important to reiterate that the results and their interpretation are subject to the assumptions and amendments made to Wang's model in section [5.2](#) and should only be interpreted in light of these assumptions.

6 Conclusion

Bitcoin is a nascent, virtual open-source currency system structured on a decentralized peer-to-peer network and operated under cryptographic rules and principles. Introduced by Nakamoto in 2008, its popularity exploded in 2011. Bitcoin is a revolutionary concept in the realm of digital currencies and has garnered its share of media attention. In an attempt to further people's understanding of Bitcoin, the second chapter introduced Bitcoin in an intricate and structured manner. This helped to structure the rest of the thesis in the hopes of stimulating future research on Bitcoin. The four main sections are devoted to terminology and usage, the origins of Bitcoin, the mechanics of Bitcoin, and Bitcoin usage.

Academic interest in the field has also grown since 2011 with a plethora of novel studies on Bitcoin from different fields. The third chapter, devoted to the literature review, provides an in-depth overview of the literature on Bitcoin. It encompasses the most important works on Bitcoin and is structured like the second chapter to facilitate future research. The second section of the third chapter introduces the relevant theory: the functions of money, the economic equation of exchange, and the model for the valuation of Bitcoin proposed by Wang (2014) as a basis for the analysis.

The methodology chapter established the foundation for the analysis. It presented the two hypotheses:

H₁: The price of bitcoin is not influenced by changes in the trade volume.

H₂: The price of bitcoin is determined by the likelihood that a bitcoin will be saved.

It explains that the two hypotheses were selected in light of Wang's assumptions and what methods and models were used in each section of the analysis.

The analysis chapter argued that Bitcoin does fulfill the classical functions of money, but that its usage mainly remains as a speculative instrument, which can be witnessed in Bitcoin's extreme price volatility. It is crucial to understand the elements behind Bitcoin's price formation to understand Bitcoin's ability to serve as a medium of exchange. Understanding the functioning of Bitcoin and its potential economic impact is important for regulatory bodies to better respond to Bitcoin and other cryptocurrencies.

The analysis goes on to argue that the economic equation of exchange can be applied to the dynamics of Bitcoin given that the equation can be viewed as a tautology. Wang's model is then amended to reflect the realities of empirically analyzing the Bitcoin market, where it

is argued that the velocity of Bitcoin is difficult to measure and that given the dynamics of Bitcoin, the velocity of Bitcoin is not a linear function of the total number of bitcoins in circulation. The analysis also demonstrated that Wang's model is limited to activity on the block chain, which limits the scope of the analysis and potential insight on the velocity of Bitcoin, given that theoretically, the velocity of Bitcoin should include off-chain activity. Two proxies were chosen to assess economic activity and inactivity on the block chain: the daily number of transactions and Bitcoin days destroyed.

This research was inspired by other econometric studies of Bitcoin price determinants that have encompassed a plethora of variables both in and out of the Bitcoin ecosystem. First of its kind, this econometric analysis focused on the variables directly related to the block chain. Rather than using financial instruments and measurements outside the Bitcoin ecosystem to determine its price, the variables selected were limited to those deemed to influence the price of bitcoin within its ecosystem.

The econometric analysis included a dependent variable as a proxy for Bitcoin price, the Bitcoin Price Index. Eight independent variables were selected: the daily number of transactions, the cumulative number of Bitcoin days destroyed, the trade-exchange ratio, Bitcoin's market capitalization, the total number of bitcoins, the hash rate, Google search queries, and a compilation of exogenous shocks. After getting the natural logarithm of all variables except the dummy variable exogenous shocks, Augmented Dickey-Fuller tests revealed that variables were not of the same order. To give the variables the same order of integration with a similar level of integration, the first difference of four variables was taken. After completing the VAR lag selection test and vector autoregression modeling, the results demonstrate that both hypotheses cannot be rejected. With the daily number of transactions not having a Granger-causal effect on the price of bitcoin, it was determined that indeed, the price of bitcoin is not influenced by changes in trade volume. The results also reveal that there is a bidirectional Granger-causal relationship between the price of bitcoin and saving. Impulse-response functions are used to graph and interpret the direction of the Granger causality in the analysis. The results confirm that the price of bitcoin is determined by the likelihood that a bitcoin will be saved.

Even though the two hypotheses were determined to be valid. It is nevertheless important to acknowledge that correlation does not imply causality and that it is always possible that a variable was omitted, which could affect the causal relationship, which was deemed weak. In addition, it is important to reiterate that the results and their interpretation are

subject to the assumptions and amendments made to Wang's model and should only be interpreted in light of these assumptions.

In closing, this thesis makes significant contributions to the study of Bitcoin in the fields of economics and econometrics. It has provided a comprehensive assessment of Bitcoin that will benefit all those seeking to get acquainted to Bitcoin, or simply deepen their understanding. The detailed overview of the academic literature on Bitcoin provides a basis for future research extending beyond Bitcoin itself to the field of cryptocurrencies, econometrics, macroeconomics, and financial regulation. Applying the functions of money to Bitcoin and discussing the economic equation of money in relation to Bitcoin complements and expands on previous research; this addresses a gap in the macroeconomic literature at this time. The econometric analysis builds on previous research and provides valuable insight on the price determinants of bitcoin from a previously unexplored perspective derived from Wang's model. Hopefully, this thesis can inspire future research on the price determinants of Bitcoin, which would encompass both economic activity on and off the block chain.

7 References

Primary Sources:

- Bitcoin Charts (2015): *Exchange volume distribution*. [online] Available at: <<http://bitcoincharts.com/charts/volumepie/>> [Accessed: 10 April 2015]
- Blockchain.info (2015): *Charts*. [online] Available at: <<https://blockchain.info/charts>> [Accessed: 5 April 2015]
- CoinDesk (2014): *State of Bitcoin 2014*. [online] Available at: <<http://media.coindesk.com/report/CoinDesk-State-of-Bitcoin-2014.pdf>> [Accessed: 10 April 2014]
- CoinDesk (2015a): *State of Bitcoin 2015*. [online] Available at: <<http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/>> [Accessed: 13 April 2015]
- CoinDesk (2015b): *State of Bitcoin Q1 2015*. [online] Available at: <<http://www.coindesk.com/state-of-bitcoin-q1-2015-record-investment-buoys-ecosystem/>> [Accessed: 13 April 2015]
- CoinDesk (2015c): *Bitcoin Price Index API*. [online] Available at: <<http://www.coindesk.com/api/>> [Accessed: 5 April 2015]
- Google Trends (2015): *Bitcoin*. [online] Powered by Google. Available at: <<https://www.google.com/trends/>> [Accessed: 10 April 2015]
- History of Bitcoin (2015): *History of Bitcoin*. [online] Available at: <<http://historyofbitcoin.org/>> [Accessed: 13 April 2015]
- I Got Bicoïn (2015): *Milestones*. [online] <<http://www.igotbitcoin.com/milestones/>> [Accessed: 13 April 2015]
- Quandl (2015): *Bitcoin Currency Data*. [online] Available at: <<https://www.quandl.com/collections/markets/bitcoin-data>> [Accessed: 5 April 2015]

Secondary Sources:

- Abel, A. & B. Bernanke (2001): *Macroeconomics*. Addison Wesley, 4th edition.
- Agassi, J. (1971): *Tautology and Testability in Economics*. [online] Philosophy of the Social Sciences 1, pp. 49-63. Available at: <<http://www.tau.ac.il/~agass/joseph-papers/tautology.pdf>> [Accessed: 27 April 2015]
- Androulaki, E., G. Karame, M. Roeschlin, T. Scherer & S. Capkun (2013): *Evaluating User Privacy in Bitcoin*. [online] In: Proceedings of Financial Cryptography and Data Security Conference (FC). Available at: <<http://eprint.iacr.org/2012/596.pdf>> [Accessed: 20 April 2015]
- Babaioff, M., S. Dobzinski, S. Oren & A. Zohar (2012): *On Bitcoin and red balloons*. [online] In: ACM Conference on Electronic Commerce, pp. 56-73. Available at: <<http://research.microsoft.com/pubs/156072/bitcoin.pdf>> [Accessed: 11 March 2014]

- Back, A. (2002): *Hashcash - a denial of service counter-measure*. [online] Available at: <<http://www.hashcash.org/papers/hashcash.pdf>> [Accessed: 14 April 2014]
- Badev, A. & M. Chen (2014): *Bitcoin: Technical Background and Data Analysis*. [online] FEDS Working Paper No. 2014-104. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544331> [Accessed: 22 February 2015]
- Bain, K. & P. Howells (2009): *Monetary Economics: Policy and its Theoretical Basis*. 2nd edition New York: Palgrave Macmillan.
- Barber, S., X. Boyen, E. Shi & E. Uzun (2012): *Bitter to Better - How to Make Bitcoin a Better Currency*. [online] Palo Alto Research Center, University of California, Berkeley. Available at: <<https://crypto.stanford.edu/~xb/fc12/bitcoin.pdf>> [Accessed: 14 November 2013]
- Bitcoin Foundation (2014): *About*. [online] Available at: <<https://bitcoinfoundation.org/about/>> [Accessed: 16 March 2014]
- Bitcoin Project (2014): *Home* [online] Available at: <<https://bitcoin.org/en/>> [Accessed: 10 January 2014]
- Bollen, R. (2013): *The Legal Status of Online Currencies: Are Bitcoins the Future?* [online] Journal of Banking and Finance Law and Practice. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285247> [Accessed: 24 March 2014]
- Bouoiyour, J. & R. Selmi (2014): *What Bitcoin looks like?* [online] Munich Personal RePEc Archive, Paper No 58091, 15 October. Available at: <http://mpra.ub.uni-muenchen.de/58133/1/MPRA_paper_58133.pdf> [Accessed: 20 April 2015]
- Buchholz, M., J. Delaney & J. Warren (2012): *Bits and Bets: Information, Price Volatility, and Demand for Bitcoin*. [online] Unpublished manuscript. Available at: <<http://www.bitcointrading.com/pdf/bitsandbets.pdf>> [Accessed: 20 April 2015]
- Buterin, V. (2014): *Mining Pool Centralization at Crisis Levels*. Bitcoin Magazine, January 2014, pp. 32-34.
- Chaum, D. (1981): *Untraceable electronic mail, return addresses, and digital pseudonyms*. [online] Communications of the ACM, February, vol. 24, no. 2, pp. 84-90. Available at: <http://www.cs.utexas.edu/~shmat/courses/cs395t_fall04/chaum81.pdf> [Accessed: 14 April 2015]
- Christin, N. (2013): *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*. [online] In: Proceedings of WWW 2013. Available at: <<https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf>> [Accessed: 20 April 2015]
- Ciaian, P., M. Rajcaniova & D. Kancs (2014): *The Economics of BitCoin Price Formation*. [online] Available at: <<http://arxiv.org/ftp/arxiv/papers/1405/1405.4498.pdf>> [Accessed: 10 March 2013]
- Coinbase (2013): *You Can Now Send Micro-Transactions With Zero Fees*. [online] Blogpost, 6 August 2013. Available at: <<https://blog.coinbase.com/2013/08/06/you-can-now-send-micro-transactions-with-zero-fees/>> [Accessed: 18 April 2015]

- CoinDesk (2015d): *About the Bitcoin Price Index*. [online] Available at: <<http://www.coindesk.com/price/bitcoin-price-index/>> [Accessed: 10 April 2015]
- Cryptocoins News (2015): *How a Bitcoin Transaction Works*. [online] Available at: <<https://www.cryptocoinsnews.com/bitcoin-transaction-really-works/>> [Accessed: 6 March 2015]
- Cuthbertson, A. (2015): *Bitcoin now accepted by 100,000 merchants worldwide*. [online] International Business Times, 4 February. Available at: <<http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613>> [Accessed: 10 April 2015]
- Dai, W. (1998): *b-money*. [online] Available at: <<http://www.weidai.com/bmoney.txt>> [Accessed 15 April 2014]
- Doepke, M. & M. Schneider (2013): *Money as a Unit of Account*. [online] CEPR Discussion Paper No. DP9700. Available at: <<http://ssrn.com/abstract=2346217>> [Accessed: 23 April 2015]
- DuPont, Q. (2014): *The Politics of Cryptography: Bitcoin and the Ordering Machines*. [online] Journal of Peer Production. Available at: <<http://peerproduction.net/>> [Accessed: 17 April 2014]
- Dwyer, G. (2014): *The Economics of Bitcoin and Similar Private Digital Currencies*. [online] Available at: <<http://ssrn.com/abstract=2434628>> [Accessed: 20 April 2015]
- Elias, M. (2011): *Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy*. [online] Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1937769> [Accessed: 20 April 2015]
- Evans, D. (2014): *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms*. [online] University of Chicago Coase-Sandor Institute for Law & Economics Research Paper, No. 685. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424516> [Accessed: 19 May 2014]
- Eyal I. & E.G. Sirer (2013): *Majority is not enough: Bitcoin mining is vulnerable*. [online] Available at: <<http://www.cs.cornell.edu/~ie53/publications/btcProcArXiv.pdf>> [Accessed: 23 March 2015]
- Finney, H. (2004): *RPOW – Reusable Proofs of Work*. [online] Cypherpunks. Available at: <<http://marc.info/?l=cypherpunks&m=109259877510186&w=2>> [Accessed: 17 April 2015]
- Fisher, I. (1911): *The Purchasing Power of Money*. New York: Macmillan.
- Garcia, D., C. Tessone, P. Mavrodiev & N. Perony (2014): *The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy*. [online] J. R. Soc. Interface 11: 20140623. Available at: <<http://dx.doi.org/10.1098/rsif.2014.0623>> [Accessed: 10 March 2015]
- Gervais, A., G. Karame, S. Capkun, V. Capkun (2013): *Is Bitcoin a Decentralized Currency?* [online] IACR. Available at: <<https://eprint.iacr.org/2013/829.pdf>> [Accessed 25 March 2014]

- Glaser, F., Z. Kai, M. Haferkorn, M. Weber & M. Sieiring (2014): *Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions* [online] Available at: <<http://ssrn.com/abstract=2425247>> [Accessed: 10 March 2015]
- Goldfeder, S., J. Bonneau, E. Felten, J. Kroll & A. Narayanan (2014): *Securing Bitcoin wallets via threshold signatures*. [online] Available at: <http://www.cs.princeton.edu/~stevenag/bitcoin_threshold_signatures.pdf> [Accessed: 28 November 2014]
- Goodhart, C. (2011): *The Changing Role of Central Banks*. Financial Markets Group, London School of Economics.
- Gordon, J., J. Chapman & B. Akins (2015): *The Case for the Regulation of Bitcoin Mining as a Security*. [online] Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2559769> [Accessed: 9 March 2015]
- Grinberg, R. (2011): *Bitcoin: An Innovative Alternative Digital Currency*. [online] Hastings Science & Technology Law Journal, Vol. 4, pp.160-208, December. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857> [Accessed: 24 March 2014]
- Grondwald, M. (2014): *The Economics of Bitcoins – Market Characteristics and Price Jumps*. [online] CESIFO Working Paper No. 5121. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2548999> [Accessed: 10 March 2015]
- Guo, S., C. Ladrone & J. Feng (2010): *Granger causality: theory and applications*. In: *Frontiers in Computational and Systems Biology*. Springer-Verlag, pp. 83-111.
- Houy, N. (2014a): *The Bitcoin Mining Game*. [online] Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407834> [Accessed: 12 March 2014]
- Houy, N. (2014b): *The economics of Bitcoin transaction fees*. [online] Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400519> [Accessed: 24 March 2014]
- Janota, M. (2013): *Digital currencies: Analysis of Bitcoin demand*. Bachelor thesis. Charles University, May 2013.
- Kapalov, N. (2012): *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*. [online] Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203> [Accessed: 24 March 2014]
- Karame, G., E. Androulaki & S. Capkun (2012): *Double-spending fast payments in bitcoin*. [online] Proceedings of the 2012 ACM conference on Computer and communications security. Available at: <<https://eprint.iacr.org/2012/248.pdf>> [Accessed: 17 April 2015]
- Kaşkaloğlu, K. (2014): *Near Zero Bitcoin Transaction Fees Cannot Last Forever*. [online] In: *The International Conference on Digital Security and Forensics*, pp. 91–99. Available at: <<http://goo.gl/E7dmxe>> [Accessed: 23 March 2015]
- Kiyotaki, N. & R. Wright (1989): *On Money as a Medium of Exchange*. *Journal of Political Economy*, vol. 97, No. 4, pp. 927-954.

- Koshy, P., D. Koshy & P. McDaniel (2014): *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*. [online] Available at: <<http://www.ecole.ensicaen.fr/~lacharme/article15.pdf>> [Accessed: 28 February 2014]
- Kraken (2015): *Mt Gox Creditor Claims*. [online] Available at: <<http://goo.gl/fY1RGM>> [Accessed: 21 April 2015]
- Kristoufek, L. (2013): *Bitcoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era*. [online] Scientific Reports 3 (3415): 1-7. Available at: <<http://goo.gl/WEYGe0>> [Accessed: 10 March 2015]
- Kristoufek, L. (2014): *What are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis*. [online] Available at: <<http://arxiv.org/pdf/1406.0268.pdf>> [Accessed: 3 January 2015]
- Kroll, J., I. Davey & E. Felten (2013): *The economics of Bitcoin mining, or Bitcoin in the presence of adversaries*. [online] Proceedings of WEIS. vol. 2013. Available at: <https://www.cs.princeton.edu/~kroll/papers/weis13_bitcoin.pdf> [Accessed: 18 April 2015]
- Krugman, P. (1984): *The International Role of the Dollar: Theory and Prospect*. In: *Exchange Rate Theory and Practice* by J. Bilson & R. Martson. University of Chicago Press, Ch. 8, pp. 261 – 278.
- Lawn, A. (2014): *What is Bitcoin mining?* *yBitcoin*, Summer 2014, p. 62.
- Lo, S. & Wang C. (2014): *Bitcoin as Money?* [online] Federal Reserve Bank of Boston, Current Policy Perspectives No 14-4. Available at: <<http://goo.gl/oET04G>> [Accessed: 23 April 2015]
- Luther, W. (2013): *Cryptocurrencies, Network Effects, and Switching Costs*. [online] Mercatus Center working paper no. 13-17. Available at: <<http://ssrn.com/abstract=2295134>> [Accessed: 14 April 2014]
- Luther, W. & J. Olson (2013): *Bitcoin is Memory*. [online] Available at: <<http://ssrn.com/abstract=2275730>> [Accessed: 24 March 2014]
- Luther, W. & L. White (2014): *Can Bitcoin Become a Major Currency?* [online] GMU Working Paper in Economics No. 14-17. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446604> [Accessed: 02 February 2015]
- Mankiw, G. (2011): *Principles of Microeconomics*. Cengage Learning, 6th edition.
- Meiklejohn, S. *et al.* (2013): *A fistful of bitcoins: characterizing payments among men with no names*. [online] Available at: <<https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>> [Accessed: 25 November 2013]
- Merkle, R. (1982): *Method of providing digital signatures*. U.S. Pat. 4,309,569.
- Mishkin, F. (2004): *The Economics of Money and Financial Markets*. 7 ed. Boston: Pearson.
- Moore, T. & N. Christin (2013): *Beware the middleman: Empirical Analysis of Bitcoin-Exchange risk*. [online] Proceedings of Financial Cryptography. Available at: <fc13.ifca.ai/proc/1-2.pdf> [Accessed: 10 April 2014]

- Nakamoto, S. (2008): *Bitcoin: A peer-to-peer electronic cash system*. [online] Available at: <<http://www.bitcoin.org>> [Accessed: 16 February 2014]
- Norman, J. (2014): *The audacity of bitcoin*. [online] Global FX Strategy, J.P. Morgan Securities plc. Available at: <<http://goo.gl/cl5DCH>> [Accessed 6 January 2015]
- Ober, M., S. Katzenbeisser, K. Hamacher (2013): *Structure and Anonymity of the Bitcoin Transaction Graph*. [online] Future Internet. 7 May, vol. 5, no. 2, pp. 237-250. Available at: <<http://www.mdpi.com/1999-5903/5/2/237>> [Accessed: 25 March 2015]
- Ólafsson, Í. (2014): *Is Bitcoin money? An analysis from the Austrian school of economic thought*. Master of Science thesis. University of Iceland, June 2014.
- Parkin, M. (2012): *Macroeconomics*. Pearson Series in Economics, 10th edition.
- Plassaras, N. (2013): *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*. [online] Chicago Journal of International Law 14 (1): 377–407. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2248419> [Accessed: 24 March 2014]
- Rivest, R., A. Shamir & L. Adleman (1978): *A method for obtaining digital signatures and public-key cryptosystems*. [online] Communication of the ACM 21, 2 February, pp. 120-126. Available at: <<http://people.csail.mit.edu/rivest/Rsapaper.pdf>> [Accessed: 14 April 2015]
- Ron, D. & A. Shamir (2012): *Quantitative Analysis of the Full Bitcoin Transaction Graph*. [online] The Weizmann Institute of Social Science. Available at: <<http://fc13.ifca.ai/proc/1-1.pdf>> [Accessed: 14 April 2014]
- Rosenfeld, M. (2012): *Analysis of hashrate-based double-spending*. [online] Available at: <<http://arxiv.org/abs/1402.2009>> [Accessed: 30 April 2014]
- Šafka, J. (2014): *Virtual currencies in real economy: Bitcoin*. Master thesis. Charles University, May 2014.
- Selgin, G. (2013). *Synthetic Commodity Money*. [online] Available at: <<http://ssrn.com/abstract=2000118>> [Accessed: 24 March 2014]
- Šurda, P. (2012): *Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?* Master thesis. Vienna University of Economics and Business, November 2012.
- Süssmuth, B. & C. Hillinger (2008): *The Quantity Theory of Money is Valid - The New Keynesians are Wrong!* [online] Available at: <<http://ssrn.com/abstract=1303456>> [Accessed: 23 April 2015]
- Syed, O. & A. Syed (2011): *Bitcoin Gateway, A Peer-to-peer Bitcoin Vault and Payment Network, 2011*. [online] Available at: <<http://arimaa.com/bitcoin/>> [Accessed: 25 March 2015]
- Szabo, N. (2008): *Bit gold*. Available at: <<http://unenumerated.blogspot.cz/2011/05/bitcoin-what-took-ye-so-long.html>> [Accessed: 17 April 2015]
- Tao, J. (2001): *The Mismatch of Fisher and His Equation of Exchange: A Proposal to the Federal Reserve System*. Available at <<http://ssrn.com/abstract=293439>> [Accessed: 23 April 2015]

- Trautman, L. (2014): *Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?* Richmond Journal of Law and Technology, Vol. 20, No. 4. Available at: <<http://ssrn.com/abstract=2393537>> [Accessed: 24 March 2015]
- Tucker, P. (2009): *The Digital Currency Doppelganger: Regulatory Challenge or Harbinger of the New Economy?* [online] Cardozo Journal of International and Comparative Law, Vol. 17, No. 3. Available at: <<http://ssrn.com/abstract=1525846>> [Accessed: 15 April 2015]
- Wang, J. (2014): *A Simple Macroeconomic Model of Bitcoin.* [online] Available at: <<http://ssrn.com/abstract=2394024>> [Accessed: 24 March 2014]
- Woolridge, J. (2006): *Introductory Econometrics: a Modern Approach.* Mason, OH, Thomson/South-Western.
- Yermack, D. (2014): *Is Bitcoin a Real Currency? An Economic Appraisal.* [online]. National Bureau of Economic Research working paper no. 19747. Cambridge, MA. Available at: <<http://www.nber.org/papers/w19747>> [Accessed: 12 April 2014]
- Zivot, E. & Wang, J. (2006): *Modeling financial time series with S-plus.* New York, NY, Springer.

Official publications:

- Bank for International Settlements (2009): *Issues in the Governance of Central Banks.* Chapter 2: Roles and objectives of modern central banks, pp. 17-55.
- Federal Reserve Bank of Chicago (1994): *Modern Money Mechanics.* Public Information Center.
- Financial Crimes Enforcement Network (2013): *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.* [online] Guidance: FIN-2013-G001. Available at: <http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html> [Accessed: 14 November 2013]
- Financial Crimes Enforcement Network (2014): Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform. [online] Ruling: FIN-2014-R011. Available at: <http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf> [Accessed: 21 April 2015]
- European Central Bank (2012): *Virtual Currency Schemes.* [online] ISBN: 978-92-899-0862-7. Available at: <<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>> [Accessed: 13 November 2013]
- The Law Library of Congress (2014): *Regulation of Bitcoin in Selected Jurisdictions.* [online] Report for Congress, LL File No. 2014-010233. Available at: <<http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf>> [Accessed: 10 April 2015]

8 Appendices

Appendix 1: Elements of a Bitcoin Transaction

Appendix 2: More on the BPI

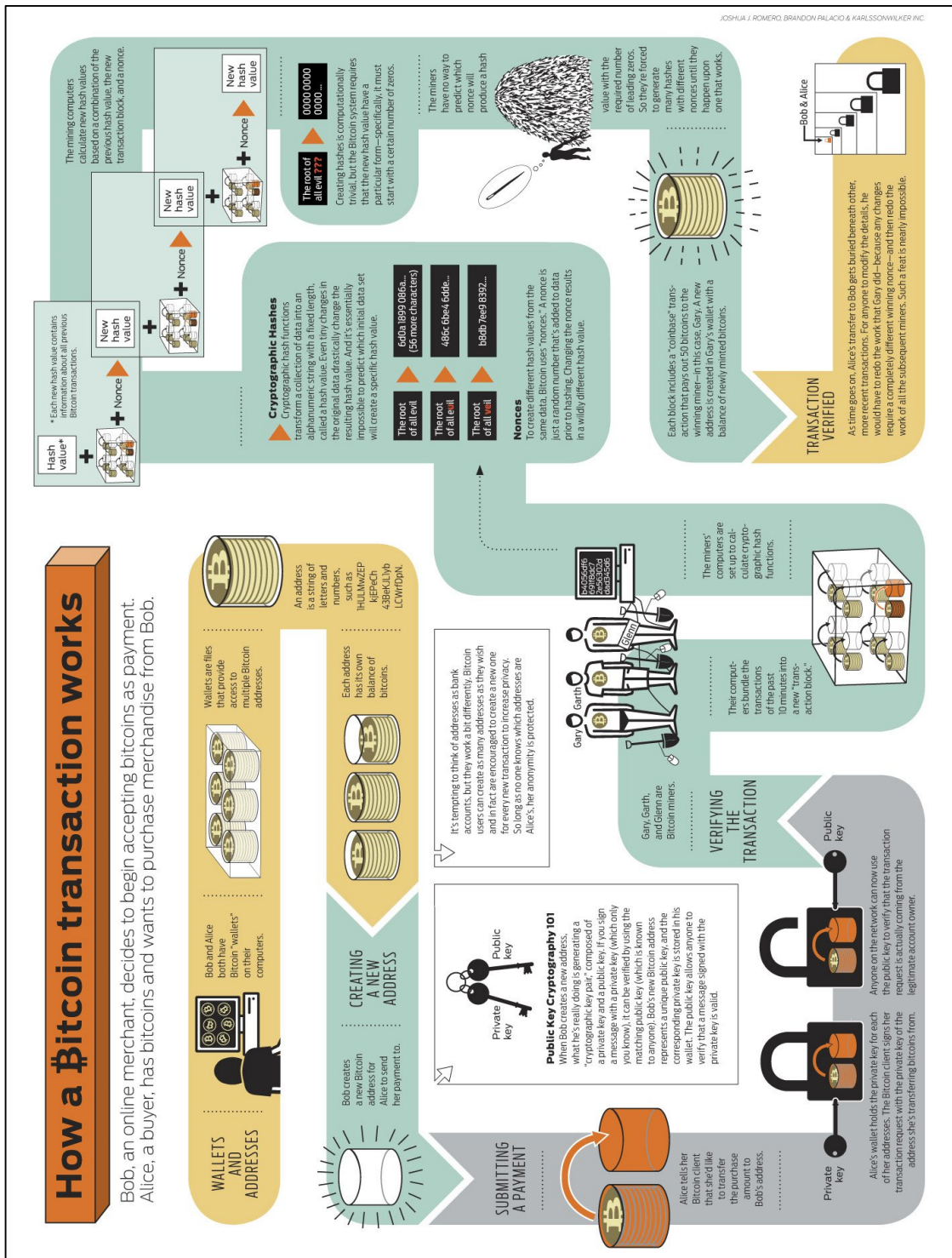
Appendix 3: Table of Exogenous Shocks

Appendix 4: VAR Lag Selection Test Results

Appendix 5: Other Impulse-Response Functions

Appendix 6: Material Included on the CD

Appendix 1: Elements of a Bitcoin Transaction



Source: Cryptocoins News 2015

Appendix 2: More on the BPI

“Which bitcoin exchanges does the BPI include?”

1. USD exchanges must serve an international customer base.
2. Exchange must provide a bid-offer spread for an immediate sale (offer) and an immediate purchase (bid).
3. Minimum trade size must be less than 1,500 USD (9,000 CNY) or equivalent.
4. Daily trading volume must meet minimum acceptable levels as determined by CoinDesk.
5. Exchange must represent at least 2% of the total 30-day cumulative volume for all of the exchanges included in the BPI.
6. Fiat currency and bitcoin transfers (whether deposits or withdrawals) must be completed by the exchange within seven and two business days, respectively.

How exactly is the BPI calculated?

1. The CoinDesk BPI is a simple average of leading XBT/USD and XBT/CNY exchange prices.
2. The BPI is expressed as the midpoint of bid/ask spread.
3. The BPI is updated every 60 seconds.
4. If an exchange does not update its price for more than 30 minutes, it is omitted from the live BPI calculation until it is updated again.
5. New index historical data commences on 1 July 2013.
6. Prior index historical data is obtained via Mt. Gox.
7. End-of-day high, low, and closing BPI is based on Coordinated Universal Time (UTC). As trades occur continuously, a day opens at 00:00:00 and closes at the end of 23:59:59, ie 00:00:00 of the next day.
8. Non-USD and non-CNY BPI prices are implied based on rates obtained via openexchangerates.org.
9. Any updates to the BPI criteria and formula shall occur as necessary.”

Source: CoinDesk (2015d)

Appendix 3: Table of Exogenous Shocks

Table 3: Exogenous Shocks

<i>Date</i>	<i>Event</i>	<i>Source</i>
12-03-01	Linode hacked, 46,000 BTC stolen.	History of Bitcoin (2015)
12-09-27	Bitcoin Foundation begins.	History of Bitcoin (2015)
12-11-28	BTC block reward is halved (now 25BTC/block).	History of Bitcoin (2015)
13-01-31	First ASICs delivered.	I got bitcoin (2015)
13-03-11	Glitch causes halt in transactions; massive sell-off.	History of Bitcoin (2015)
13-03-12	Block chain forked; rollback.	I got bitcoin (2015)
13-03-16	10% tax on Cyprus depositors	Coindesk (2014)
13-03-18	US Treasury FinCEN issues virtual currency guidance.	Coindesk (2014)
13-04-10	Bitcoin crashes due to hacks; exchanges crash.	Coindesk (2014)
13-04-11	Mt. Gox closed for nearly a day.	I got bitcoin (2015)
13-04-18	Attack on Mt. Gox and Blockchain.info.	I got bitcoin (2015)
13-05-07	Coinbase raises \$5m from Union Square Ventures.	Coindesk (2014)
13-06-08	Bitcoin ruled a currency in US court.	I got bitcoin (2015)
13-08-09	Bloomberg gets a BTC ticker.	History of Bitcoin
13-10-02	Silk Road shut down. FBI seize BTCs.	Coindesk (2014)
13-10-15	China's Baidu announces it will accept bitcoin.	Coindesk (2014)
13-10-17	Congressional hearings on Bitcoin strike positive tone.	Coindesk (2014)
13-10-18	Congressional hearings on Bitcoin strike positive tone.	Coindesk (2014)
13-12-05	People's Bank of China issues statement, Baidu and China Telecom stop accepting bitcoin	Coindesk (2014)
13-12-16	China's payment processors told not to deal with Bitcoin.	Coindesk (2014)
14-02-11	Massive DDoS attack exploits transaction malleability bug.	Coindesk (2015a)
14-02-25	Mt. Gox closes, announces 744,408 BTC missing.	Coindesk (2015a)

14-02-28	Mt. files for bankruptcy.	I got bitcoin (2015)
14-04-11	People's Bank of China official says China will not ban Bitcoin.	Coindesk (2015a)
14-04-30	Bloomberg provides BTC pricing to its 320,000 subscribers.	I got bitcoin (2015)
14-06-12	\$18m in Silk Road bitcoins sold by US Government.	Coindesk (2015a)
14-06-18	US Marshals leak list of possible Silk Road bitcoin bidders.	Coindesk (2015a)
14-07-02	VC Tim Draper revealed as Silk Road bitcoin auction winner.	Coindesk (2015a)
14-07-18	Dell announces it will accept bitcoin.	Coindesk (2015a)
14-09-23	PayPal announces bitcoin partnerships.	Coindesk (2014a)
14-12-11	Microsoft adds BTC payments for Xbox games, mobile content	Coindesk (2015a)
14-12-18	Favorable revisions made to proposed NY BitLicense.	Coindesk (2015a)
15-01-05	Bitstamp suffers \$5m hot wallet hack.	CoinDesk (2015b)
15-01-14	Bitcoin's price plunges, breaks 200\$ mark.	CoinDesk (2015b)
15-01-20	Coinbase funding round, a record of 75\$m.	CoinDesk (2015b)
15-01-25	Coinbase launches US bitcoin exchange.	CoinDesk (2015b)
15-02-04	Ross Ulbricht found guilty in NY court of operating Silk Road; Ben Lawsky releases revised NY BitLicense.	CoinDesk (2015b)
15-02-09	Hong Kong's MyCoin disappears with up to \$387m.	CoinDesk (2015b)
15-03-10	Bitcoin startup 21 Inc. announces \$116m raised.	CoinDesk (2015b)

Source: Author's compilation, primary sources cited within

Appendix 4: VAR Lag Selection Test Results

Figure 3: VAR Lag Selection Test Results

gretl output for Hugo Vozak 2015-04-28 14:08 page 1 of 1

VAR system, maximum lag order 14

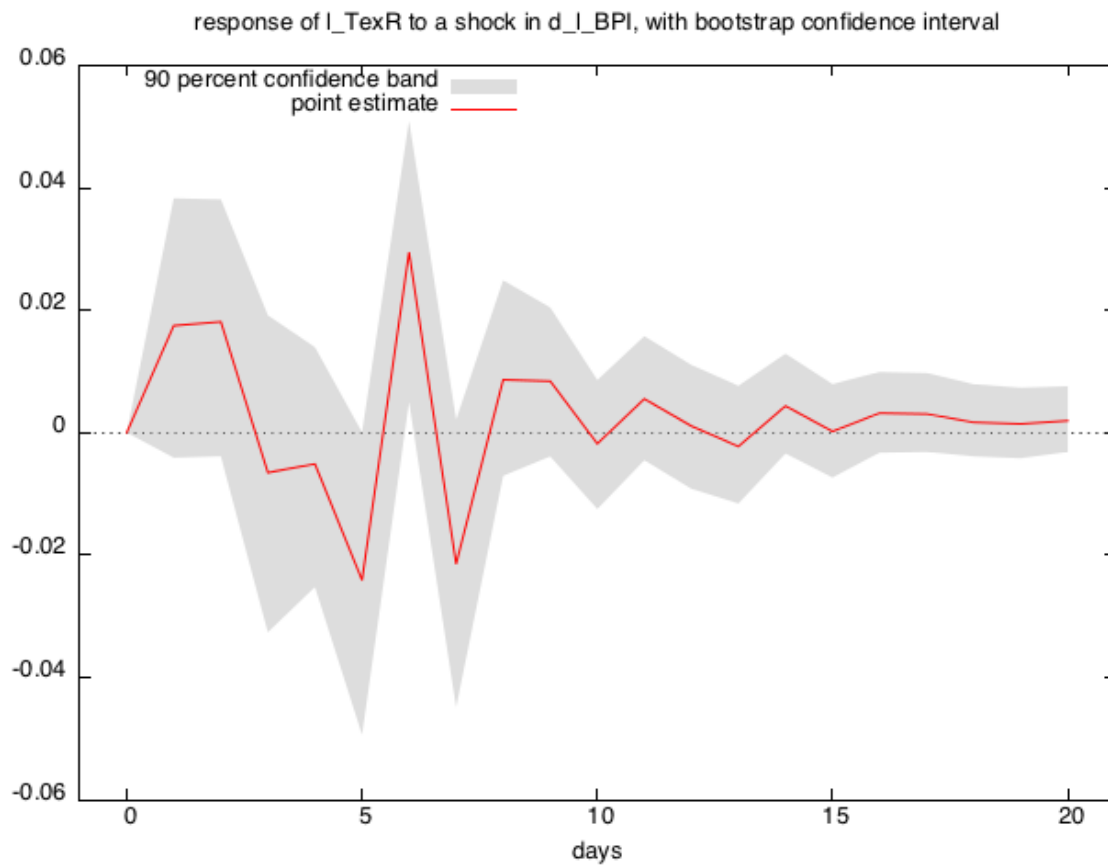
The asterisks below indicate the best (that is, minimized) values of the respective information criteria, AIC = Akaike criterion, BIC = Schwarz Bayesian criterion and HQC = Hannan-Quinn criterion.

lags	loglik	p(LR)	AIC	BIC	HQC
1	11101.26944		-17.468360	-17.183414	-17.361294
2	11347.51963	0.00000	-17.780712	-17.296303*	-17.598700
3	11481.87418	0.00000	-17.915874	-17.232003	-17.658916
4	11597.04612	0.00000	-18.020659	-17.137325	-17.688755
5	11712.46063	0.00000	-18.125828	-17.043033	-17.718978*
6	11778.03280	0.00000	-18.152071	-16.869813	-17.670274
7	11838.51407	0.00000	-18.170252*	-16.688531	-17.613509
8	11876.63701	0.00761	-18.153028	-16.471845	-17.521339
9	11903.42218	0.30329	-18.117850	-16.237204	-17.411215
10	11930.34213	0.29441	-18.082885	-16.002778	-17.301305
11	11972.21409	0.00146	-18.071598	-15.792028	-17.215071
12	12009.56116	0.01047	-18.053145	-15.574112	-17.121672
13	12044.36649	0.02800	-18.030667	-15.352172	-17.024248
14	12079.34231	0.02629	-18.008460	-15.130502	-16.927094

Source: Author's work using Gretl

Appendix 5: Other Impulse-Response Functions

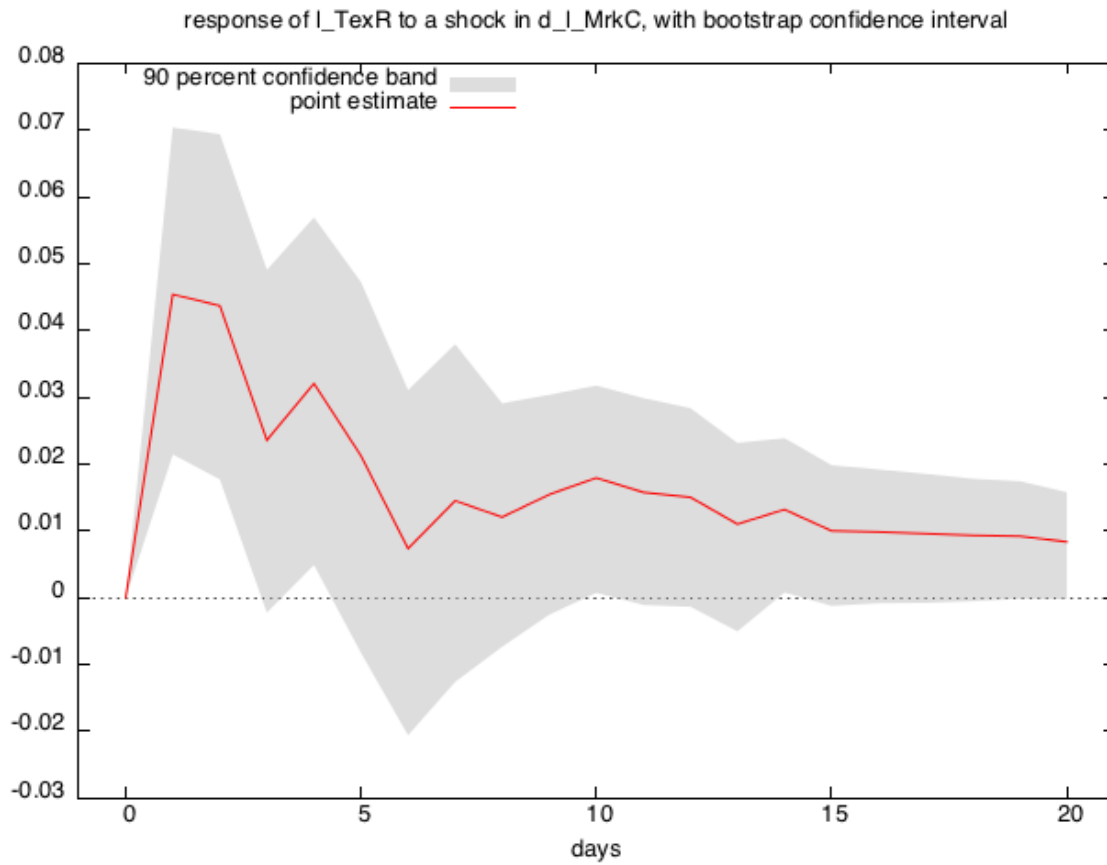
Figure 4: Impulse-Response Function of TexR to BPI



Source: Author's work using Gretl

The volatility illustrated in Figure 4 makes it difficult to interpret the effects. This can be attributed to the effect that both the daily number of transactions on the block chain and transactions on Bitcoin exchanges can have an impact on the BPI simultaneously.

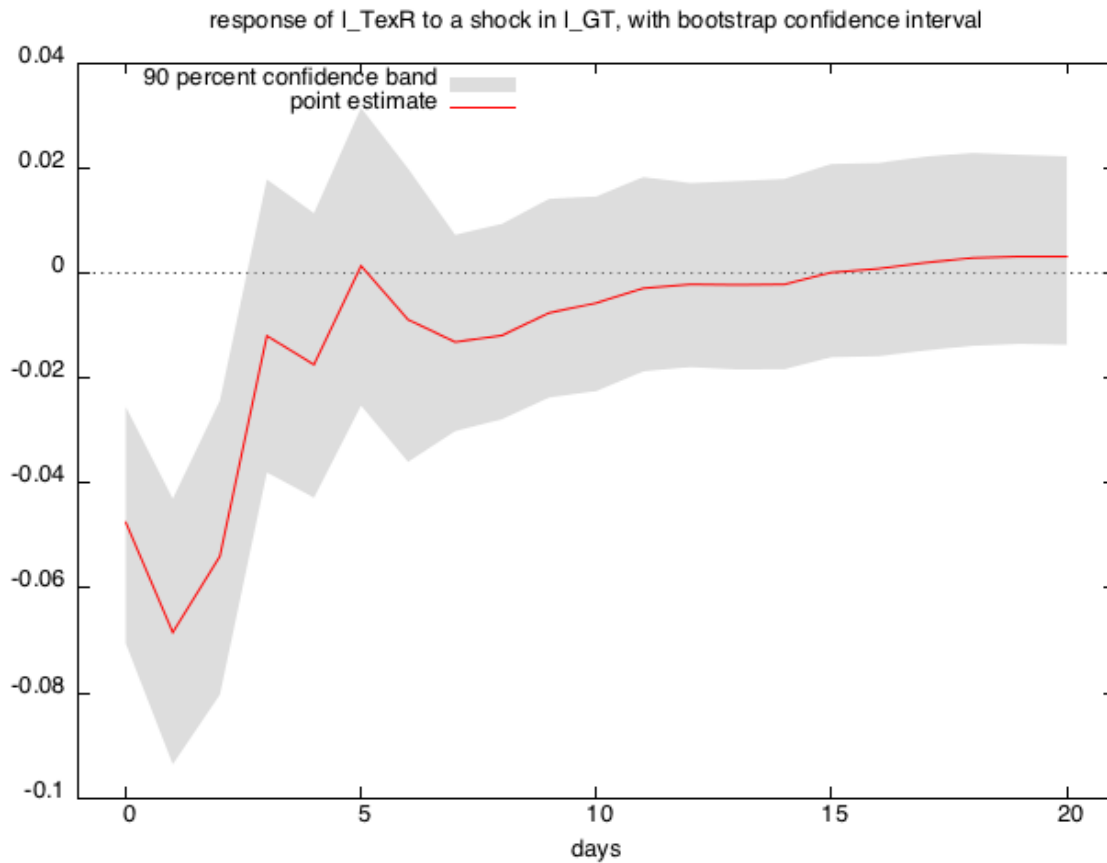
Figure 5: Impulse-Response Function of TexR to MrkC



Source: Author's work using Gretl

If the trade-exchange ratio increases – Bitcoin is transacted more on Bitcoin exchanges – then the market capitalization of Bitcoin will increase, fall and rise with the impact remaining positive. This is in line with the finding that Bitcoin is used as a speculative instrument.

Figure 6: Impulse-Response Function of TexR to GT



Source: Author's work using Gretl

If the trade-exchange ratio increases – Bitcoin is transacted more on Bitcoin exchanges – then the number of search queries will go down before converging back to around zero. This is in line with the finding that new users use Bitcoin mainly as a speculative instrument (Glaser *et al.* 2014); search queries would drop after new investors meet their search needs and decide to invest in Bitcoin.

Appendix 6: Material Included on the CD

Bitcoin time series data *Bitcoin Time Series Data.csv*

Complete VAR output *Complete VAR Results.pdf*

Gretl data file *Gretl Data File.gdt*

Gretl script file *Gretl Script File.inp*