Tulip-Mania 2.0?

A Closer Look Into Crypto-Currencies

Christoher Campos [*]

Abstract

Interest in cryptocurrencies has increased quite recently, but there is still much uncertainty about the stability of such unconventional and decentralized systems. Moreover, numerous episodes of rapid appreciation in value only to experience fast and sudden crashes shortly after contribute to the fog of uncertainty behind the value of such currencies. I then analyze the backbone of such cryptocurrency networks— the mining environment—and find a self sustaining equilibrium but several components of cryptocurrency networks raise some concerns. This is followed by look into the growing competitive market for cryptocurrencies which finds that although interest in Bitcoin is increasing, most individuals are hoarding their digital wealth. Finally, the hypothesized primary factor driving the value of Bitcoin—the computing power—turns out to not Granger cause changes in price, but changes in price Granger cause changes in the computing power of the Bitcoin network.

[*] The author thanks Dr. Jelena Bradic for her assistance and guidance with the econometric portion of the paper. Also, I would like to thank Dr. Ross Starr for his guidance and advise throughout the course of this project.

1 Introduction

The discovery of money is one of the most significant discoveries humankind has made, and is in line with the discovery of the wheel and the development of a writing system. It arises in the necessity to prevent the double coincidence of wants problem that arises in a pure barter economy. In doing so, the predominant currency becomes pervasive and essential in conducting trade. Since its introduction, money has evolved and taken many forms as civilizations rose and fell. Now, in the twenty-first century a new type of money has been introduced, the cryptocurrency. Introduced at a time of financial insecurity with the global financial crisis well under way, the creator of Bitcoin hoped to create a decentralized system where individuals could store their wealth without needing to trust government or anyone in particular to insure its value. He did so in an eight page paper which laid the foundation for what would inspire most, if not all, cryptocurrencies that exist today. For most of their early existence, cryptocurrencies were ignored by most, but idolized by computer programmers and tech enthusiasts. Very recently, with sudden increases in value have cryptocurrencies come to the attention of not just computer programmers, but businesses and entrepreneurs as well. The sudden increased interest in cryptocurrencies leads one to question the validity and use of such an unconventional approach to money.

Money should serve three primary functions. It should serve as a medium of exchange, a unit of account, and more importantly, a store of value. Cryptocurrencies have proven to be able to serve as a medium of exchange as more and more businesses are adopting cryptocurrencies. As for being a store of value or unit of account, dismal performance at best is what a cryptocurrency can offer its holder thus far. Mostly driven by speculative interest, the price of the most prominent cryptocurrency, Bitcoin, has soared several times to only experience drastic depreciation in value shortly after. If treated as a recently introduced innovation, it is hard to say whether cryptocurrencies are truly diffusing or just Tulip-Mania 2.0.

The aim of this paper is to give an introduction into the nature of cryptocurrencies and the dynamics that govern their existence. A decentralized system depends on the collective participation of its users to ensure its proper function. This motivates the analysis of the individual nodes in the network—the miners—who ensure the network operates as intended to. If their incentives are not properly aligned with the direction of the network in the long run, then one cannot expect cryptocurrencies to be around by then. Indeed, a lacking participation rate means no trade within the network, and thus rendering the proposed currency useless. This is to be followed by a look into the growing market for cryptocurrencies which might come as a surprise since the only cryptocurrency that seems to make headlines is Bitcoin. The growing number of cryptocurrencies is surely generating a competitive environment in which the advantages of alternative cryptocurrencies highlight weaknesses of Bitcoin. Finally, using the freely available data the Bitcoin network prides itself on providing, we attempt to isolate factors that may be driving the value of Bitcoin, and see if the price follows a random walk or not.

2 Literature Review

Since it was expected that there would be scant economic research related to cryptocurrencies, the literature that was scanned is differentiated into two categories. First, a look into differing schools of thought pertaining to the role, creation, and characteristics of money was considered. This was done to see if the introduction of cryptocurrencies was aligned with any already existing theories. This was followed by a review of the vast amount of research conducted by computer scientists studying the cryptographic properties and implications introduced by earlier digital currencies. The motivation behind this was to see if the system proposed by cryptocurrencies incorporates any of the ideas proposed in the well established literature.

2.1 What Makes Good Money?

Theories on the necessity and use of money can be traced back to times of Plato and Aristotle who held distinct views on money. The two had distinct views on the origins of money but nevertheless, their thought had significant impact on the contributions of subsequent theories. Friedrich Hayek and George Knapp provided two distinct perspectives pertaining to the creation of money. The two distinct theories are incompatible with one another as one argues the state is essential for a sound currency, and the other renders the state as an impediment into attaining a sound currency.

2.1.1 The Chartalist and Free Market Approach to Money

The basis for the Chartalist approach is intuitively simple. “Money is a creature of the state,” stated Abba Lerner and similarly Knapp stated“ money is a creature of law.” These two statements complement each other in developing the basis for the Chartalist approach to money. The meaning behind these statements lies in the fact that fiat currencies of today derive their value from the state and its laws. The government creates the dollar and expects its citizens to use the currency, but the assumption that the nation as a collective whole will utilize the dollar as their currency of choice is an assumption that holds no substance without proper law. Accompanied with the creation of the dollar, the state then must proclaim their created currency as the only means of payment it shall accept in receiving tax payments from its citizenry. This essentially relaxes the need for the original assumption, and with simple laws governing the acceptance of tax payments, the state creates an effective demand for its currency. As the people are now enticed into demanding this currency, it becomes a mere convenience to use it as their primary currency. Considering the decentralized nature cryptocurrencies propose, it is immediately obvious that they would not fit with Knapp’s vision. Hayek's approach to money, however, provides a system in which cryptocurrencies might work.

Naturally, an argument made proclaiming the need of the state is followed by an argument proclaiming free markets are indeed the better alternative. Hayek accepts the notion that historically, there has been a need for the state in monetary affairs. Metallic currencies were at one point valued by their size and weight, and the state became a valuable asset to merchants when it began stamping coins asserting their value. Furthermore, the existence of a single monetary unit of exchange was crucial in effectively teaching the uneducated man accounting techniques, and to effectively price goods in a market. The issues introduced with having differing currencies throughout a region would have been insurmountable during those primitive times. Moving ahead to the time of Hayek, the mere convenience of the state's monopolistic powers over currency were no longer needed.

He proposed that financial institutions and private firms enter the market as primary suppliers of currency. To remain in the market of supplying currency these entities must remain competitive, and the competitive nature of the market enforces the production of a sound currency. Any currency that is not seen as stable or reliable will be promptly abandoned under this market structure. Under this rhetoric the need for the state is completely abolished and the market decides which currencies will be most widely adopted. This does not mean that national currencies are abolished immediately, but it means that they must remain competitive to remain in the market. These ideas seem to be rooted in the motivation behind creating a decentralized currency such as Bitcoin, and many early adopters turned to it due to a lack of trust in their government. Furthermore, when looking at the competitive nature in the cryptocurrency markets one can see how Hayek's vision lives on in the digital realm. One key aspect that is missing from his approach in the implementation of cryptocurrencies is that of the private entity ensuring the currency remains stable. Indeed, the fact that cryptocurrencies serve as a poor store of value is surely one of the primary impediments behind user adoption.

2.1.2 Properties of a Good Currency

Besides the three main functions of money—a medium of exchange, a store of value, and a unit of account—William Jevons developed a list of properties that make a good currency. Using his exact terminology, Jevons stated the following as elements in a good currency.

1. Utility and Value
2. Portability
3. Indestructibility
4. Homogeneity

5. Divisibility
6. Stability of Value
7. Cognizability

Of these seven properties, cryptocurrencies satisfy all except the most important—stability of value. If individuals are transacting and trading in cryptocurrencies, then it must be they place some positive value on their digital assets. Moreover, the cryptocurrency contributes another property not originally proposed by Jevons, which is a layer of anonymity. If individuals value the extra layer of anonymity and the freedom from government, then this could explain the why some are turning to cryptocurrencies.

2.2 Cryptography as a Means to Generate Currency

Before the internet became as pervasive as it has become today, cryptographers were exploring possible applications of cryptography in the exchange of money. In 1982, David Chaum introduced the concept of the *blind signature* which proposed an automated payment system that provided a layer of anonymity and security to the user.[1] Chaum essentially paved the way for three decades of cryptographic research in possible *e-cash* schemes. One might think the cryptographers read some Jevons as they focused on almost all of the properties Jevons proposed which they could control. Okamoto (1995) proposed a method to make e-cash properly divisible. Camenisch et al. (2005) also proposed methods to improve portability and homogeneity. However, most research conducted focused on privately controlled networks in which the possibility of one double spending their funds was not possible. These privately owned digital currencies or payment systems were the first incarnation of digital money in the late twentieth century.

Unfortunately for cryptographically based digital currencies, alternative payment mechanisms that facilitated trade using existing government issued fiat currencies arose at around the same time. Consumers sided with alternative payment mechanisms that let them use their existing currency. Cryptocurrencies of today are a twenty-first century attempt to digitize money. However, Bitcoin and other cryptocurrencies alike have not implemented much of the research that was conducted over the past 30 years. Moreover, it is the first attempt to create a decentralized system which prevents the issue of double spending by implementing what is known as the *blockchain.* The concept of the blockchain is new way to safely and securely transmit data over the internet and is the truly innovative idea behind cryptocurrencies.

[1] Chaum is sometimes referred to as the individual who invented electronic cash (Camenisch et al. 2005).

3 What Are Cryptocurrencies?

From what we have seen in the past and present as currency—physical objects—cryptocurrencies attempt to leave the physical world to exist only in a digital realm. A bitcoin is not a claim on a physical object or any other currency, but rather an attempt to replace physical currency for a bit of data which holds positive digital value. Like government issued fiat currencies, cryptocurrencies hold no intrinsic value to the beholder, and strictly depend on one believing they attain positive value to be used in trade. Similarities with government issue fiat end there, and the departure from conventional money is what seems to entice the early adopters. Unlike government issued currencies, cryptocurrencies are lacking a central authority or central bank. Instead, it turns to mutually distrustful parties, known as *miners*, to ensure a properly functioning system. The supply of each cryptocurrency is predetermined at its launch and cannot be changed or manipulated by any one entity. Furthermore, changes made to the software that governs these cryptocurrencies usually need the approval of 70% of the community, making it quite difficult for one single party, or a single party with large influence to cause any harm. Thus, Nakamoto developed a system that combined components of peer-to-peer networks to create a distributed cryptocurrency whose network is not as complex as one would expect.

3.1 How They Work

Trade and exchange in a cryptocurrency is transmitted through the Internet making many issues pertaining to authenticity, validation and fraud quickly come to mind. If one has been conditioned to trust no one on the internet, then why would the idea of storing wealth in such an unsafe location be worthy of any consideration? With this in mind, the creator of the Bitcoin protocol created a system dependent on absolutely no trust, and protected it with the cryptography integrated into its software. In doing so, it not only created a new currency, but a way to securely transmit information through the internet. However, one can easily question the claim that there exists a system dependent on the participation of strangers in different regions of the world, but not dependent on their trust. Identifying the issues of trust that arise in the transferring and creation of wealth online helps better understand how Bitcoin deals with these issues. Barber et al. (2012) state a few fundamental problems that arise in the attempt to create a digital currency:

1. Authenticity
2. Control over creation
3. Double Spending

Since data can be easily duplicated, how can one be sure their claim of digital value is authentic and know the amount being transacted has not already been spent? Bitcoin's protocol solves all of these issues simultaneously. It does so by creating a public ledger known as the *blockchain* that is validated in a recursive manner; one in which the validity of the current state is dependent on a cryptographic link to the previous state, that state is dependent on a cryptographic link to the previous state, and so on. Moreover, it makes additions to this cryptographic chain costly, meaning any addition to the *blockchain* takes immense amounts of computing power, electricity, and time. A simple example helps clarify some of the inner workings inherent in the Bitcoin ecosystem[2], but before, let's define some terms that will be freely used.

Definition 1. The *blockchain* is a transaction history of a network. There is only one blockchain, and every validated transaction gets added to this blockchain.

Definition 2. A *node* is a user connected to the network. For the purposes of this paper, it shall be analogous to a miner.

Definition 3. A *miner* is an individual who supplies the network computational resources. In doing so, they maintain the protocol and generate newly created bitcoins every time they *mine* a block.

Definition 4. A *hash rate* is the number of valid computational guesses a computer makes per second. The *network hashing rate* is the collective computing power of a network.

Definition 5. In the context of cryptocurrencies, a *private key* is a secret number that allows funds to be spent. Every address has a private key which is stored in the user's digital wallet file.

Suppose Alice wants to send Bob some bitcoins.[3] She must then access her *digital wallet* and broadcast a message to the network stating her intent. The message she broadcasts is a function with the sender's *private key* and message as inputs. To ensure Amy has the appropriate funds, the message associated with the transaction references *outputs* to their proof of ownership from a set of *inputs*. All this information is contained within the *blockchain*. The system then allows those set of outputs to be reallocated correctly only if the proof of ownership is validated, meaning account balances are calculated at the time the message is broadcast. In doing so, this prevents the possibility of a malicious user modifying account balances. This also leads to one of the first issues that arises when depending on the participation of distributed nodes in a network—differing information sets. Although the issue pertaining to funds availability was solved in providing proof of ownership in the transaction message, it is not enough to ensure nodes in the network agree at all times.

[2] Since most cryptocurrencies adopt a similar, if not identical protocol, an explanation of how Bitcoin works should generalize to other cryptocurrencies.

[3] Capitalizing the word *Bitcoin* refers to the network. A lack of capitalization refers to it as a currency.

It is crucial for all nodes in the network have consensus on the state of the network for the Bitcoin economy to function properly, which means the dissemination of information must be controlled in such a way that distributed nodes have nearly identical information sets. Regional distances make it possible that a node in the network receives Amy's message before the messages that validated her proof of ownership. Likewise, it is possible that there may exist multiple transactions that are attempting to spend those coins simultaneously—known as *double spending.* Herein comes the implementation and necessity of the *blockchain.* To ensure agreement among the distributed nodes in the network, the Bitcoin protocol requires that transactions be validated in *blocks*, with new blocks being mined every 10 minutes, on average. A block contains a set of transactions that are valid up to that point. Once a block has been mined, it then has to be validated by the entire network to ensure its authenticity. Thus, the blockchain contains a transaction history that has been validated and confirmed by the entire network; this avoids the possibility of *double spending* and incorrect input-output referencing. This is a consequence of making the entire network reference the same blockchain and thus, every node in the network agrees on the state of the network at all times. We have mentioned how the blockchain is implemented in the Bitcoin network and that additions are costly, but a more technical description of blockchain additions help clarify why this novel idea proves to be of such significance.

A hash function maps an arbitrary string of letters or text to a number of fixed length.[4] The hash function *miners* solve is one which considers the set of previous states $B = \{b_0, b_1, ..., b_{n-1}\}$, the next block b_n, and an additional number n. A miner finds n such that $f(B, b_n, n) \leq \alpha$ where α denotes the network difficulty. The difficulty α is controlled exogenously by the pre-programmed software. An increase in α makes solutions easier to find and conversely, a decrease in α implies an increase in difficulty. The difficulty is adjusted with changes in the network hashing rate, so that a new block is mined every ten minutes on average. As for the hash function, it is so complex that it is nearly impossible to guess n, so a miner focuses on guessing as many times as they can. This generates the necessity of computing power since more computing power generates more guesses every second. It takes the entire Bitcoin network 10 minutes on average to mine a new block. Upon finding a solution to such a hash function a miner then confirms all the transactions that were waiting to be validated, places them in block b_n, and then broadcasts a message indicating they mined the block. Once their message is validated, a reward of X bitcoins is received.[5] The reward of newly created coins provides an incentive to validate transactions and thus, maintain the network's accounts.

In summary, the Bitcoin network creates a system independent of trust, but dependent on the participation of miners. It deals with the issue of funds availability by referencing a transaction

[4] The specific hash function used for bitcoin mining is SHA256 applied twice.

[5] The reward is decreasing geometrically with time. Initially, 50 BTC was the reward for mining a block, it currently is 25 BTC, and expected to decrease to 12.5BTC in two years.

history—the blockchain—to validate every outgoing transaction. It then implements the blockchain to deal with the issue of differing information sets among the distributed nodes in the network. Additions to the block chain are costly to make, but as long as the individuals contributing their resources get rewarded for their contribution, their incentives remain aligned with that of the network. Furthermore, the computational power required to alter the blockchain is costly, and in probabilistic terms, the probability of cheating is near zero.

3.2 Difficulty of Malicious Behavior

The blockchain is a public ledger containing the entire transaction history of the Bitcoin network. By design, any attempts to alter account balances, double spend funds or any attempts to cause harm to the network require one to make alterations to the blockchain or in other words, change the history of the network. In its infancy, the Bitcoin network was rather small and the computational power required to cause such harm was relatively small. [6] The exponential growth of the network makes it costly to be successful in altering the blockchain.

To alter the blockchain an individual would need to first generate a fork in the portion of the chain that contains the information they would like to change. From this point, they would have to mine enough blocks on their fork to become the longest ongoing chain in the network. The reasoning for this is that the longest portion of the chain serves as proof of work to the network that the required resources were expended in generating those blocks. To successfully make their fork the longest portion of the chain, a malicious user would have to mine the required number of blocks to make their fork equate in length to the original chain(basically, rewrite the history of the network), and then simultaneously outpace the entire network in mining the subsequent block. Figure 1 provides a visual description of such an attempt. Given that it takes a the entire network's computational power to mine a new block, it becomes unlikely that an individual or a group of individuals to be successful in making any alterations to the blockchain.

Even an attacker with a significant amount of computing power and resources (such as a government) still has bad odds at success in making any alterations to the blockchain. Since the entire network is continuously working to mine a block, the probability a malicious miner finds the next block is equal to their proportion of the network's computing power. The probability of a malicious miner outpacing the entire network and successfully altering the transaction history can be modeled like a random walk on $\mathbb{Z}$, where mining a block is analogous to moving right on the integer lattice. The probability of a miner making alterations to a block in the blockchain that is z blocks in the past, is analogous to the well known gambler's ruin problem. The notation P_x denotes the probability under the initial condition $X_0 = x$, and $T_y := \inf\{n \geq 0 : X_n = y\}$ denotes the hitting time of y. The probability of a malicious miner finding the next block is p_m, and the probability of an

[6] Figure 2 shows the increase in the network's computational power over time

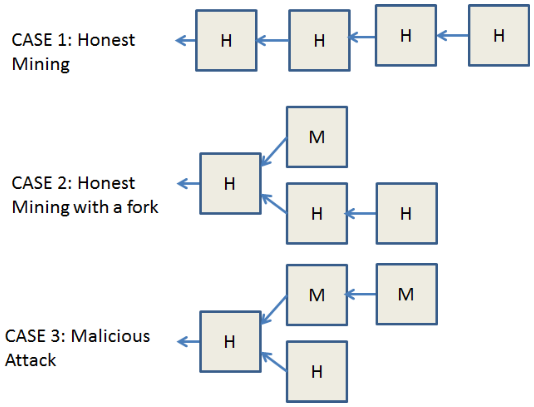


Figure 1: A block with an H denotes an honestly mined block, and M denotes a malicious block. Case 1 provides a visual description of the blockchain operating as supposed to. Case 2 shows the creation of a fork in the chain, and how honest miners respond to a malicious miner's attempt at creating a fork. Case 3 depicts a successful malicious attack in which the malicious miner outperformed the entire network and generated a longer fork in which subsequent blocks are added.

honest miner finding the next block is $p_h = 1 - p_m$. The transition probabilities are $p(i, i+1) = p_m$ and $p(i, i-1) = p_h$ for all $i \in \mathbb{Z}$. Then

$$P_0(T_z < \infty)^7 = \begin{cases} (p_m/p_h)^z & if \quad p_m < 1/2 \\ 1 & if \quad p_m \geq 1/2 \end{cases} \tag{1}$$

As long as a malicious user does not attain half the computing power of the network, $(p_m/p_h)^z < 1$ for all $z \geq 1$. It follows, $(p_m/p_h) \to 0$ as z increases.[8] Although malicious users exist, the way the protocol is designed makes their odds of success highly unfavorable if their proportion of computer is strictly less than that of honest miners. This implies there exists an incentive for miners to join a pool controlling half of the network's computational resources, but no pools have been successful thus far. A corollary to this is that for the network to remain secure there must remain interest in the network, so that the computational power exceeds a threshold at which malicious behavior is not economically feasible.

[7] See the Appendix A for a full proof

[8] Merchants that accept cryptocurrencies as a means of payment are advised to wait an hour before considering a received payment final. Given that a new block is mined every 10 minutes, z tends to equal six. This means a malicious miner must begin their attempt to outpace the network from six blocks behind.

4 Mining Cryptocurrencies

Thus far, an introductory explanation into the inner workings of the Bitcoin ecosystem has been given. We have provided novel solutions to problems that had plagued previously proposed types of digital currency, but these novel solutions have a strict dependence on the participation of *miners*. Nakamoto (2008) created an ecosystem in which he hoped the incentives of the *miners* were compatible with the success of the network. In creating an incentive compatible system, the protocol Nakamoto created does not depend on the trust of the *miners*. Although no trust is needed from individuals, the participation of a strictly positive quantity of miners is a necessity for the network to function correctly. Modeling the decision to *mine* bitcoins proves to be of significant importance to the internal stability of the currency in the long run. Furthermore, not only must there be a long run willingness to participate, but the economic behavior of these mutually distrustful parties must prove to be necessarily aligned with Nakamoto's propositions. First, we model the decision process in deciding to join the Bitcoin network as a *miner*.

4.1 The Decision To Mine: The First Troubling Result

Kroll et al. (2013) developed a model that relied on the consensus about three states simultaneously

1. Consensus about the rules: Having consensus about the rules enables distributed nodes in the network to agree on what transactions are valid.

2. Consensus about the state: The state at all times is transparent and visible to all nodes in the network through the blockchain. Miners must agree that the blockchain does in fact represent the state of the network at all times.

3. Consensus on positive value: Since a miner is rewarded newly created units of currency for providing time and resources to mine new blocks, there must be consensus that they have value.

Having consensus on these three states at all times then enables one to model the decision to enter the Bitcoin mining community. Extending Kroll et al. (2013) we create a simple model that captures every aspect an individual takes into account before mining bitcoins.

In terms of supply and demand, the Bitcoin network demands computing power and the miners are the suppliers of such a resource. As long as consensus of the three states remains upheld, then the demand for computing power is infinite, meaning the network will take all that is given. So an individual considering supplying the network with computing power must simply maximize the quantity they can produce given their costs. The computing power an individual provides the network is quantified in hashes per second, which we will denote as H. To generate H hashes per second, a potential miner must provide certain levels of capital and labor. Letting K denote the units of capital, and L represent the labor units a potential miner will provide, we propose the production function to take the form $f(K, L) = K^\alpha L^\beta$ where α and β denote corresponding output elasticities. Since labor inputs are only required to troubleshoot any downtime of equipment, and increases in capital more directly reflect gains in output, we assume $\beta < \alpha$. Furthermore, the assumption of a constant returns to scale function is assumed meaning $\alpha + \beta = 1$. The motivation for this is the fact that doubling units of capital and labor yields twice as much computing power. The costs that a miner incurs are $C = rk + wL$ where r denotes electrical costs and w denotes the opportunity costs a miner incurs from choosing to mine. A potential miner must then maximize the computing power they supply the network given subject to their cost constraint The Lagrangian for this maximization problem is

$$\max_{K,L,\lambda} \mathscr{L} = f(K, L) + \lambda(C - wL - rK),$$

so the optimal levels computing power a potential miner is to provide is where $\frac{w}{r} = \frac{\beta L}{\alpha K}$ and thus, the efficient allocations of K and L are where $K = \frac{\beta w}{\alpha r} L$. A potential miner maximizing their potential production does not necessarily imply they will begin mining. Assuming a miner is only interested in non-negative profits, they will begin mining if their marginal revenues are at least equal to their marginal costs.[9] This dynamic threshold is determined externally by the Bitcoin network. Since miners are solving cryptographic puzzles whose difficulty is an exogenous variable determined by the Bitcoin network, then their marginal revenue exceeding their marginal costs will depend on the network difficulty, which we will denote δ.

Suppose it takes $P = P(\delta)$ hashes per second to mine a block (on average) for a given level of difficulty. Additionally, suppose mining a block yields revenue $R = M + F$ and incurs costs C, where M denotes the mining reward and F denotes any fees collected by miners.[10] Then profit is given by $\pi = HR - CP(\delta)$. So an individual will mine only if $HR > CP(\delta)$, or equivalently,

$$\frac{HR}{C} > P(\delta). \tag{2}$$

This could be a troubling result considering the exponential growth in the network difficulty δ. Like mentioned earlier, an increase in the aggregate network hashing rate is followed by an increase in the network difficulty. Since it is one's best interests to increase their individual hashing rates to yield higher returns, then one can clearly see why mining might prove to not be profitable in the long run. The participation of miners is of vital importance since they process every transaction in the network. Their incentive to do so is correlated with the profit they make from doing so.

[9] There exists a plethora of individuals who choose to contribute their resources in the mining effort expecting absolutely zero profits. Our analysis does not consider these individuals.

[10] Currently, most revenue received from mining is through the fixed mining reward. In the long run, since most cryptocurrencies have fixed supplies, the mining reward will be zero and transaction fees will be the primary source of revenue.

If this profit is driven to zero, then a miner will not be willing to participate, and if all miners are not willing to participate, then the proposed currency fails. Figure 2 below shows the rapidly increasing network hashing rate over the past year, and figure 3 shows the accompanying increases in the Bitcoin network difficulty.

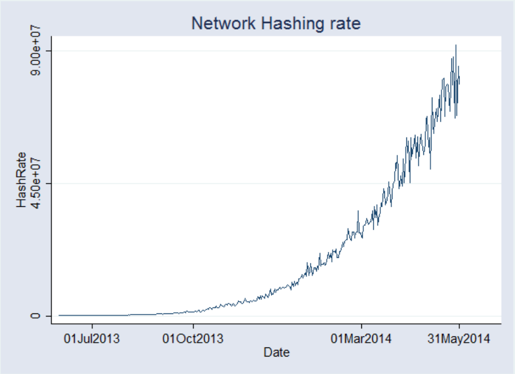


Figure 2: Bitcoin Network Hashing Rate

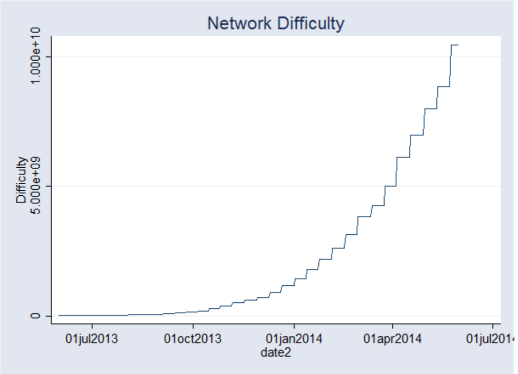


Figure 3: Bitcoin Network Difficulty

Once a miner takes into consideration increasing difficulty rate they can then make the decision to contribute their resources to a specific network or not. However, miners do no venture out alone. They join *mining pools*, which incorporates another element they must consider in their profitable venture—other miners. The Bitcoin protocol was devised in such a way so that trust is not needed between individuals transacting through the network. It was not, however, devised in a way that would strictly protect the interests of miners' from other miners. Nevertheless, the Bitcoin network and all cryptocurrencies have evolved in a way that mining is dependent on pools.

4.2 Mining Behavior

Thus far, we have shown under what conditions a profit seeking miner will proceed to begin mining. If there is consensus on the rules, the current state, and that coins have value, then one would consider mining. The motivation to mine collectively with others is to reduce the variance of one's earnings. This assumes miners are risk averse. Since mining is a random and risky process, revenue is given in expectation and has an accompanying variance. Furthermore, the time between mined blocks is also a random process, so it too has an expected value and variance. These components can be grouped together to explain why miners turn to mining pools as opposed to mining alone. To do so, we first define a Poisson process which will be used to model the disbursement of revenue and frequency miners actually mine blocks.

Definition. *Let $X((s,t])$ be a random variable counting the number of events occurring in an* *interval* $(s,t]$. *Then* $X((s,t])$ *is a Poisson process with rate* $\lambda > 0$ *if*

1. *for* $m \in \mathbb{N}$, *and distinct time points* $t_0 = 0 < t_1 < t_2 < ... < t_m$, *the random variables* $X((t_0,t_1]), X((t_1,t_2]), ..., X((t_{m-1},t_m])$ *are independent.*

2. *for any times* $s < t$ *the random variable* $X((s,t])$ *has the Poisson distribution*

$$P(X((s,t] = k) = \frac{(\lambda(t-s))^k e^{-\lambda(t-s)}}{k!}$$

The following are a few properties of a Poisson process which will be used freely.

1. $E[X((s,t])] = \lambda(t-s)$

2. $\text{Var}(X((s,t])) = \lambda(t-s)$

3. A sojourn time S_n measures the duration that the Poisson process stays in state n. The sojourn times are independent random variables each having the exponential probability density function $f_{S_k}(t) = \lambda e^{-\lambda t} \quad t \geq 0$

Now that we have defined a Poisson process and a few of its properties, we can proceed. Since miners receive revenue every time they successfully mine a block, then the quantity of mined blocks accompanied by the frequency of their occurrence is important in determining a miner's expected revenue. Mining can be depicted as a Poisson process with a given rate $\lambda > 0$. For notational simplicity, let $X = X((0,t])$ denote the number of blocks mined between the time interval of length t. For a miner whose hash contribution is H, the rate at which blocks are mined is $\lambda = \frac{H}{2^{32}\delta}$. [11] Given this, it follows that the expected number of blocks mined over a time interval of length t is $E[X] = \frac{Ht}{2^{32}\delta}$. Letting r denote the reward one receives for mining a block we have $E[rX] = r \cdot E[X] = \frac{rHt}{2^{32}\delta}$ and $\text{Var}(rX) = \frac{r^2Ht}{2^{32}\cdot\delta}$.

Now suppose that this miner is risk averse in their preferences and is considering joining a mining pool. Without a loss of generality, suppose this mining pool will consist of n members upon this miner joining, and that each member's hash contribution is $H_i = H$ for $i = 1, 2, ..., n$. That is, each member is contributing an equivalent amount of computing power to the network and to the pool. Also, suppose the mining pool distributes earnings to each member proportional to their computing power contributed to the pool. It follows that the pools computing power $H^p = \sum_{i=1}^{n} H_i = nH$. Let X_p denote the number of blocks a pool mines over a time interval of length t. Then given H^p, the expected number of blocks a pool will mine is $E[X_p] = \frac{H^p t}{2^{32}\delta} = \frac{nHt}{2^{32}\delta}$. It follows that each individual miner should expect to receive $\frac{1}{n} \cdot \frac{rnHt}{2^{32}\delta} = \frac{rHt}{2^{32}\delta}$ in expected revenue over a time interval of length t, which is equivalent to their expected revenue if they mined alone. If a pool charges a fee

[11] Rosenfeld (2011) states the probability of mining a block is approximately $\frac{1}{2^{32}\delta}$.

f (which most do), then a miner would have expected revenue of $(1-f)\frac{rHt}{2^{32}\delta}$. This quantity is less than what they would have earned if mining alone, so if a miner was only worried about expected revenue, then they would not join a mining pool.

Although the expected revenue (excluding fees) is the same whether in a pool or alone, the variance of one's earnings is not the same. The variance of a miner's earnings from mining in a pool is $\text{Var}(\frac{r}{n}X_p) = \frac{\frac{r^2}{n^2}nHt}{2^{32}\delta} = \frac{r^2Ht}{n2^{32}\delta}$, which is less than the variance of their earnings from mining alone. Assuming miners are risk averse in their preferences, mining in a pool would be preferred over mining alone. The reduced variance in earnings might suffice for some, but another component that makes pooled mining a preferred option is the frequency of mined blocks.

Suppose a miner can mine alone at a rate λ_s, or join a pool that mines at a rate λ_p where $\lambda_p > \lambda_s$. For a solo miner, the sojourn times between mined blocks have density $f(t) = \lambda_s e^{-\lambda_s t}$ for $t \geq 0$ and 0 otherwise. The probability they mined a block over a time interval of length t is $1 - e^{-\lambda_s t}$. Similarly, the probability a pool of miners mine a block over time interval of length t is $1 - e^{-\lambda_p t}$. Since $\lambda_s < \lambda_p$, the probability of a pool mining a block is greater than an individual mining a block. This should make sense since the aggregate computing power of a pool is significantly larger than that of a solo miner, and thus increasing their odds of mining a block. Moreover, a property of the exponential distribution is that it adheres to the memoryless property. This means that if a miner should expect to wait x days to mine a block, and has already been waiting s days, then they should still expect to wait x days to mine a block. This holds even if $s > x$. It is reasonable to assume that one would like to see revenue streams happen more frequently as opposed to less frequently, so someone who may not necessarily be risk averse in their preferences might prefer joining a pool based solely on the fact that they would see more frequent revenue streams. Moreover, the volatility in the exchange value of cryptocurrencies adds a degree of uncertainty to the realized profits one makes after exchanging their mined coins. The following examples give a more realistic feel to the miner's decision to join a pool or not. The difficulty rate used in the following calculations is the most recent difficulty rate of the Bitcoin network.

Example 1 (Solo Mining)**.** Let's consider revenue over one day in the Bitcoin network. That is, $t = 86,400$ seconds. Let X_s denote the number of blocks mined alone over this time period with rate λ_s. Furthermore, suppose that a miner has maximized his hash contribution and is supplying the network $H = 1TH/s = 10^{12}$ hashes per second, which is a reasonable amount. Currently, a miner receives a reward $r = 25$ for mining a block and the current network difficulty is $\delta = 10,455,720,138$. It follows, $E[rX_s] = \lambda_s tB = \frac{10^{12} * 86,400}{2^{32} * 10,455,720,138} 25 \approx .048$BTC per day, where BTC denotes bitcoins. Now consider the variance of a miner's earnings. $\text{Var}(X_s B) = \frac{10^{12} * 86,400}{2^{32} * 10,455,720,138} 25^2 \approx 1.2$, and $\text{SD}(BX_s) = \sqrt{2.511} \approx 1.1$ BTC. The probability of mining one block is by $1 - e^{\lambda_s t} \approx 0.001$, so it would take approximately 520 days on average to mine one block, if one is solo mining.

Example 2 (Pooled Mining)**.** Let X_p denote the number of blocks a pool has mined with rate λ_p. Consider a mining pool containing $n = 1000$ miners with collective hashing rate $\sum_{i=1}^{1000} H_i = \bar{H}$, and suppose that earnings are distributed proportionally and earnings are distributed proportional to the provided computing power to the pool. We have $\lambda_p = \frac{1000*10^{12}}{2^{32}*10{,}455{,}720{,}138}$. It follows that the expected earnings for the pool over a given day is $E[rX_p] = \frac{1000*10^{12}*86{,}400}{2^{32}*10{,}455{,}720{,}138} 25 \approx 48.1$BTC. Assuming the pool does not charge a fee, a miner in such a pool should expect $100.44/1000 = 0.048$BTC in revenue per day. If a fee f is charged, then their expected revenue is $(1 - f) \cdot 0.048$ BTC. Also, $\text{Var}(X_pB) = \frac{(1000)(10^{12})(86{,}400)}{(2^{32})(10{,}455{,}720{,}138)} 25^2 \approx 1202$, and $\text{SD}(X_pB) = \sqrt{2511} \approx 34$BTC. Clearly, the relative variance and standard deviation of earnings from pooled mining is less than that of solo mining shown in Example 1. The probability that a pool mines *at least* one block is $1 - e^{\lambda_p t} \approx 0.85$ meaning that the pool mines at least every 1.17 days, on average.

The preceding examples showed that a miner receives the same in expectation whether mining in a pool or alone. In fact, their earnings might be slightly less if their pool charges a pool fee. The motivation behind joining a pool is not contained in expected earnings but in the sojourn times between mined blocks and the reduced variance in their earnings. The high degree of uncertainty due to the probabilistic nature of mining makes mining individually not a preferred option. Since all miners are profit seeking individuals, a continuous flow of revenue is preferred over stagnant periods of zero revenue. The reduction in the variance of ones earnings is enough for those individuals who are risk averse in their preferences, as both solo and pooled mining provide the same profits in expectation.

4.3 Network Equilibrium

The decentralized nature cryptocurrencies propose does not control the individual behavior that can be observed by individuals contributing to the network, but internal components of the system can ensure a proper functioning system. The notion that cryptocurrencies allow for a pre-determined rate of supply increases proves to be important in providing a network equilibrium. As stated earlier, new blocks are mined every ten minutes on average meaning the supply is increased at a predetermined rate every ten minutes. Suppose this translates into B new blocks per second, and it takes an individual miner $P(\delta)$ hashes to mine a block, on average. Suppose there are N miners and each is supplying H_i hashes per second to the network for $i = 1, 2..., N$. Since B blocks are generated (on average) regardless of the network hashing rate, we have

$$B = \sum_{i=1}^{N} \frac{H_i}{P(\delta)} \tag{3}$$

Let $\bar{H} = \sum_{i=1}^{N} H_i$ be the aggregate network hash rate and $\bar{C} = \sum_{i=1}^{N} C_i$ be the network aggregate costs. Rearranging (3) we have $P(\delta) = \frac{\bar{H}}{B}$. Recall from (2) that $P(\delta) < \frac{HR}{C}$ which implies $\frac{\bar{H}}{B} < \frac{\bar{H}R}{\bar{C}}$. Rearranging this inequality yields

$$\bar{C} < RB \longrightarrow \bar{C} = RB \tag{4}$$

This result was also proposed by Kroll et al. (2013) which they denote as the *global equilibrium* once $\bar{C} = RB$. That is, miners will collectively supply computing power to the network only if they are expected to attain non-negative returns from their contributions, and the equilibrium point is where network costs equate with network mining revenue. There are two components that affect the inequality proposed in (3)—the exchange value of a cryptocurrency, and the quantity of computing power contained in the network costs. Let us now consider two possible scenarios pertaining to the network equilibrium.

1. $\bar{C} < RB$

If the network costs are below the aggregate mining revenue, this means mining is a profitable venture. Profit seeking individuals are expected to enter the market if this is true. This in turn is accompanied with an increase in the network's costs. This is expected to continue until the network costs equate aggregate mining revenue.

2. $\bar{C} > RB$

If network costs exceed aggregate mining revenue, then there must exist a set of miners that are operating at a loss. Unprofitable miners will leave the network and continue leaving until an equilibrium is attained.

Thus, the network equilibrium proposed in (4) turns out be self sustaining. A decrease in the value of the currency (in dollars) is expected to be accompanied with a decrease in miner participation. Likewise, an increase in the exchange value of a cryptocurrency is expected to be accompanied with an increase in miner contribution. Although, this network equilibrium is self sustaining, it still is dependent on the exchange value of a given cryptocurrency. Moreover, as time progresses $R = M + F \rightarrow F$ meaning that in the future mining revenue will be solely dependent on transaction fees. Today, transaction fees are optional and not every individual must include them. This could be troublesome in the long run since mining revenue will be decrease, and the incentive to mine will decrease substantially. However, many alternative cryptocurrencies have already taken this issue into consideration and have begun competing with Bitcoin.

5 Competitive Cryptocurrencies and the Current State of the Bitcoin Economy

At the time of this writing approximately 300 cryptocurrencies exist with new ones coming into existence almost daily. The extensive publicity Bitcoin has drawn over the past year has led to a significant increase in interest and possibly value, but that has not been exempt from attracting extensive criticism as well. A combination of increases in value accompanied with possible solutions to some of the economic weaknesses that lie inherently in Bitcoin has led to the creation of hundreds of new cryptocurrencies. Other cryptocurrencies target specific subpopulations. For example, for the Lakota nation (a semi-autonomous North American Indian reservation in South Dakota), MazaCoin has been introduced as a possibility of being the tribe's official currency and is pending council approval. However, not all cryptocurrencies propose better alternatives to Bitcoin or target specific subpopulations, and it is also possible to attribute the sudden interest in the creation of new cryptocurrencies to that of bubble like behavior. Nevertheless, the creation of markets in which these new *alt-coins* are traded has generated a competitive atmosphere to become the dominant cryptocurrency. Table 1 lists ten cryptocurrencies ranked by their total market capitalization (in US dollars) along with their price and available supply. [12] A natural question arises from the existence of these such markets that allow these currencies to be traded—are these currencies legitimate alternatives to conventional currencies in circulation today?

Table 1: Cryptocurrencies Ranked by Market Capitalization

Name	Market Cap	Price	Available Supply
Bitcoin	$8,317,815,372	$647.83	12,839,525
Litecoin	$317,484,985	$11.00	28,875,985
Peercoin	$43,049,960	$2.01	21,443,189
Mastercoin	$47,183,317	$83.78	563,162
Ripple	$46,632,611	$0.006	7,579,478,083
Dogecoin	$44,676,511	$.0006	72,816,789,083
Nxt	$24,180,056	$0.024	999,997,096
Namecoin	$21,797,515	$2.54	8,875,982
BlackCoin	$15,549,220	$0.21	74,512,140
PrimeCoin	$5,087,807	$ 0.95	5,347,965

[12] These prices are as of May 31, 2014.

Dowd and Greenaway (1993) proposed a model to depict the adoption of new currencies. They claim adopting a new currency depends primarily on switching costs and a network effect, where the network effect is a reflection of the quantity of users adopting the new currency. Typical switching costs that arise in the act of switching ones unit of account involve changing records, adapting to new relative prices and any other exogenously determined costs. These switching costs must outweigh the net gains in utility one would incur from adopting a new currency. The model proposed by Dowd and Greenaway (1993) measures the utility an individual receives from adopting a currency from time T onwards. Their model considers an economy with $N+1$ agents. Each agent derives the following utility from using a given currency from time T onwards:

$$U(t) = (a + bn) \int_T^\infty e^{-r(t-T)} dt = \frac{a + bn}{r}.$$

The constant $a > 0$ captures utility gains that are network-independent, so for a currency that were tied to the gold standard, a would be equivalent to the currency's exchange value. The constant $b > 0$ along with $n := \ln N$ capture network related benefits that are increasing at a diminishing rate with N, and r represents the discount rate or equivalently, the interest rate. The implications of this model are straightforward. An individual derives utility based on the discounted direct value a given currency gives them, but is also positively affected by the number of individuals that have adopted the currency up by time T.

Suppose a new currency is introduced at time T, and the utility the new currency gives is

$$V(t) = (c + dn) \int_T^\infty e^{-r(t-T)} dt = \frac{c + dn}{r},$$

where the constants $c > 0$, $d > 0$, $n := \ln N$ and r are defined similarly. An individual will only switch currencies if their net gain in utility from switching outweighs their switching costs. That is,

$$U(t) \leq V(t) - s$$

or equivalently,

$$s \leq \frac{(c - a) + (dn - rn)}{r},$$

where s denotes the switching costs incurred from moving one's wealth to the new currency. This model reveals an intriguing fact—an alternative currency that yields significantly higher utility than the status quo may not be adopted if the net gain in utility cannot offset the switching costs. Furthermore, one can clearly see that significant gains in user adoption through the network effect are what ultimately determines whether one chooses to adopt a new currency or not.

In the case of Bitcoin, user adoption can be easily observed by analyzing the transaction activity contained in the blockchain.[13] As expected, there is a significant increase in Bitcoin's user base

[13] The author is thankful to John Ratcliff for the guidance with the required computer code needed to extract such data.

through time. This however, is not the complete story behind the currency's growth. A significant user base for Bitcoin does not necessarily mean individuals are using bitcoins to conduct trade, which is what should eventually determine user adoption. Although 2.5 million distinct addresses exist with positive balances, only roughly a fifth of them hold accounts with reasonable trading balances. The remaining addresses are those of the significantly wealthy individuals in the network, and those with meaningless balances. Figure 4 depicts the distribution of wealth in the Bitcoin network.

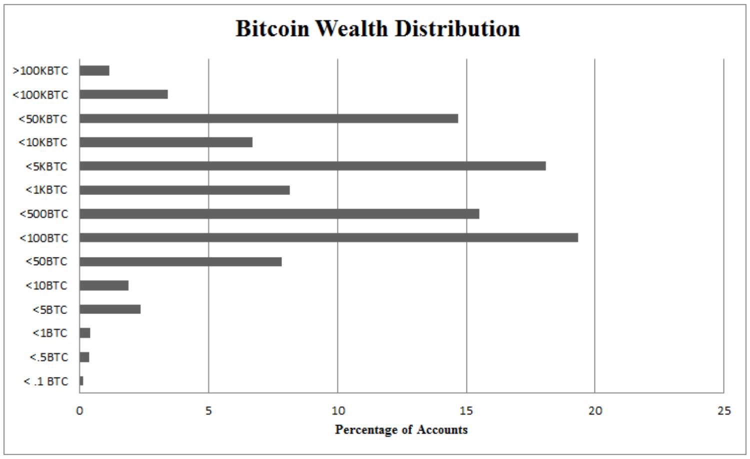


Figure 4: The figure $< x$ BTC represents the proportion of users that hold x but more than the previous amount.

Of these individuals that have stored portions of their wealth in Bitcoin, the entire transaction history of these individuals was then analyzed. The blockchain was analyzed from January 3, 2009 (Bitcoin's date of creation) to April 4, 2014, and Table 2 gives a summary of some statistics pertaining to the current state of the Bitcoin economy. There exist nearly 30 million addresses but only the ones with positive balances were considered. It is clear that most individuals in the Bitcoin network hold at least one bitcoin (roughly 98 %), but the question of interest is whether or not these individuals are transacting in Bitcoin. Since the Dowd and Greenaway model claims that currency adoption depends primarily on a network effect, the frequency individuals are using their Bitcoins is of vital importance.

Unfortunately for the Bitcoin network, its users are not too interested in transacting in bitcoins thus far. Table 3 shows the mean number of days since Bitcoin users last used their bitcoins. Even for individuals who hold less than 1 bitcoin (approximately $600), they are not using their Bitcoins for at least 9 months, on average. For the even wealthier individuals holding at least 25 bitcoins (approximately $15,000), they have not moved any of their Bitcoins for at least 2.5 years,

	Quantity	
Total BTC	12,613,964	
Active BTC	8,779,153	
Addresses With Balance	2,778,853	
< 0.001BTC	1,340,498	BTC Total: 158
> 0.001BTC and < 1BTC	1,136,932	BTC: Total 253,608
> 1BTC and < 1K BTC	301,423	BTC Total: 6,952642
> 1K BTC	1516	BTC Total: 5,407,556

Table 2: As of April 4, 2014

Number of BTC	Mean Number of Days Since Address Last Used
> 0 BTC and < 1 BTC	296
> 1 BTC and < 5 BTC	420
> 5 BTC and < 25 BTC	610
> 25 BTC	973

Table 3: As of April 4, 2014

on average. Although the Bitcoin network is growing rapidly, most users are not turning to Bitcoin in hopes of adopting a new currency, and see it as an investment instrument instead. The hoarding of bitcoins seems reasonable as most expect them to increase in value, specially since the exchange value of Bitcoin has increased by approximately 390% over the past year.

Thus far, it is clear that the growing Bitcoin network is not growing in a manner that would lead to individuals to adopt Bitcoin as a preferred currency. Moreover, if the most prominent cryptocurrency (Bitcoin) which is an accepted means of payment at certain locations is not being used by its adopters, then the same is probably true for others. The dominant network effects of the Dowd and Greenaway model require agents in an economy to use the currency and not just treat it as a commodity. Nevertheless, interest in Bitcoin and crypto-currencies is increasing and the driving force behind the value of Bitcoin is still unknown, but there exists some hopeful predictors.

6 The Exchange Value of Bitcoin

It is quite difficult to pinpoint what exactly is the driving force behind Bitcoin's rapid appreciation. It was created in early 2009 and went unnoticed for much of its early existence, but very recently has seen significant interest drawn to it. Although it has seen significant growth over the past year, the analysis of the blockchain revealed that individuals are not willing to utilize their bitcoins, so the appreciation of the price could be indicative of a bubble. However, the consistent increase in price could be due to the constant increases in the marginal costs of producing Bitcoins which can be observed with the increases in the network hashing rate.

6.1 Granger Causality Between Price and Hashing Rate

The hypothesis behind what should be the fundamental value of a Bitcoin and other crypto-currencies alike is

$$P_t = MC_t.$$

That is, the price or exchange value of a bitcoin at a given time t should equal the marginal cost of producing a Bitcoin at that given time. From the model provided in section 4, the primary factor affecting the cost of producing a bitcoin is the computational power of the network—the aggregate network hashing rate. Figure 6 shows a strong correlation between the logarithmic values of the Bitcoin price and the network hashing rate, and could be indicative of possible Granger causality between the two variables. A time series $X_t(t = 1, ..., T)$ is said to Granger cause a time series $Y_t(t = 1, ..., T)$ if the values of $X_t(t = 1, ..., T)$ provide statistically significant information about the future values of Y_t. However, Granger causality is not equivalent to true causality, and Granger causality tests yield predictive causality if there is enough statistical evidence. After running a sequence of tests, the optimal autoregressive models to then conduct a Granger causality test were chose to have three lags. [14]

$$\begin{aligned}\Delta\text{ln}P_t = \beta_{10} + \beta_{11}\Delta\text{ln}P_{t-1} + \beta_{12}\Delta\text{ln}P_{t-2} + \beta_{13}\Delta\text{ln}P_{t-3}\\ + \gamma_{11}\Delta\text{ln}Hash_{t-1} + \gamma_{12}\Delta\text{ln}Hash_{t-2} + \gamma_{13}\Delta\text{ln}Hash_{t-3} + u_{1t}\end{aligned} \tag{5}$$

$$\begin{aligned}\Delta\text{ln}Hash_t = \beta_{20} + \beta_{21}\Delta\text{ln}P_{t-1} + \beta_{22}\Delta\text{ln}P_{t-2} + \beta_{23}\Delta\text{ln}P_{t-3}\\ + \gamma_{21}\Delta\text{ln}Hash_{t-1} + \gamma_{22}\Delta\text{ln}Hash_{t-2} + \gamma_{23}\Delta\text{ln}Hash_{t-3} + u_{1t}\end{aligned} \tag{6}$$

Conducting a Granger-Causality test yielded results indicating that log changes of the exchange value of Bitcoin Granger cause the log changes in the hashing rate, but log changes in the hashing

[14] See Appendix for the sequence of steps taken to justify the chosen model.

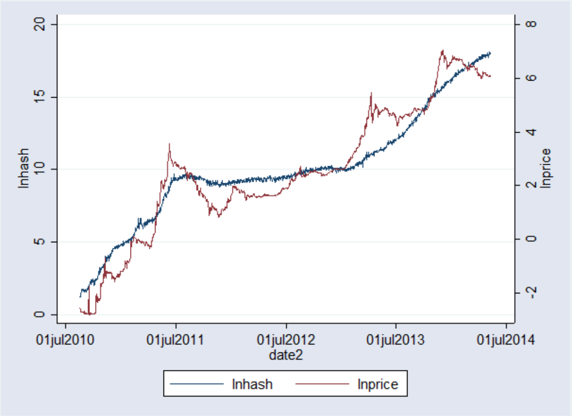
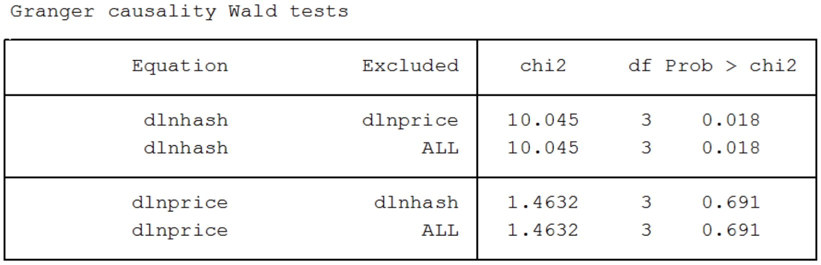


Figure 5

rate *do not* Granger cause log changes in the exchange value of a bitcoin. The null hypothesis in the test conducted on Figure 6 is that the "equation" variable does not Granger cause the "excluded" variable. With 5% significance we can conclude that previous values of the price are predictive factors for future hashing rates. This agrees with the the network equilibrium conditions provided in section 4. That is, increases in the exchange value of a bitcoin lead individuals to begin mining, and therefore increasing the computing power of the network, which subsequently increases network costs. However, it was surprising to see that log changes in hashing rate do not Granger cause log changes in price. Furthermore, the variation explained in this equation is near zero, so it is evident that there must be something else driving the value of Bitcoin other than the increases in marginal costs of production.



```
Granger causality Wald tests

          Equation           Excluded     chi2     df  Prob > chi2

           dlnhash           dlnprice    10.045     3     0.018
           dlnhash                ALL    10.045     3     0.018

          dlnprice            dlnhash    1.4632     3     0.691
          dlnprice                ALL    1.4632     3     0.691
```

Figure 6

6.2 Does Price Follow a Random Walk?

It is clear that the marginal cost of production is not the only factor affecting the exchange value of crypto-currencies. Figure 7a plots the exchange value of Bitcoin over time, and one can see that the value of Bitcoin has not seen smooth and gradual increases. Rather, there are three known periods in which the value of Bitcoin is said to have behaved like a bubble—once in 2011, another in March 2013 and a third in December 2013. Given that the exchange value of Bitcoin has been subject to three bubble periods, we form an alternative hypothesis for the exchange value of a bitcoin. The efficient market hypothesis states that information is incorporated into the market price, which should be at equilibrium and should not change unless new information is attained. Since the disbursement of information and events are unpredictable, then so should prices. In the case of Bitcoin, if this were the case then one would expect previous values of its price to not have a statistically significant effect on future prices.

We consider the the following model[15]:

$$\Delta \ln P_t = \beta_0 + \beta_1 \Delta \ln P_{t-1} + ... + \beta_k P_{t-k} + u_t.$$

If the price of a bitcoin follows a random walk, then one would expect the coefficients β_i for $k = 1, 2$ to not be statistically significantly different from zero. Moreover, a positive β_k coefficient would imply that market participants respond positively to recent changes and thus, inflate the price further. Since the price of Bitcoin has been subject to three bubble episodes in the past, we hypothesize that these coefficients will be positive and statistically significant.

The results for the regression with one lag have that $\hat{\beta_1} = 0.9986$ and is statistically significant at the 1% level. This means that if the price experienced a percent increase the previous day, then it should be expected to increase by approximately one percent. This confirms the hypothesis that the price of Bitcoin does not follow a random walk. Next, the same regression with two lagged values was considered. Again, $\hat{\beta_1}$ was positive and statistically significant at the 1% level, and $\hat{\beta_2}$ was positive and statistically significant at the 5% level. Specifically, $\hat{\beta_1} = 0.9392$ and $\hat{\beta_2} = 0.0594$. Although the effect of $\hat{\beta_2}$ was positive and statistically significant, it does not affect the current price as much.

[15] See Appendix for procedure followed to determine appropriate number of lags.

	(1) lnprice	(2) lnprice
L.lnprice (β_1)	0.9986^{***} (0.0009)	0.9392^{***} (0.0271)
L2.lnprice (β_2)		0.0594^{*} (0.0270)
_cons (β_0)	0.00991^{**} (0.0010)	0.0104^{**} (0.0032)
N	1362	1360
R^2	0.0035	0.0041

Standard errors in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

The fact that previous levels of price are affecting subsequent prices could be indicative of bubble like behavior. However, the R^2 for both regressions are near zero meaning not much of the variation in price can be explained by previous changes in price. Positive and statistically significant coefficients on logged values of previous prices are still alarming and contradictory to the efficient market hypothesis which implies previous price levels should have no effect on future price levels. There is clearly more work that needs to be done to pinpoint all factors affecting the Bitcoin price levels since the marginal costs of production and previous changes in price fail to capture everything that is affecting the price.

7 Conclusion

A closer look into the decentralized nature of cryptocurrencies has revealed some insight into the internal stability of such networks. Although there are many headlines proposing Bitcoin is not safe, the structure of its network makes it safe from malicious users by making malicious behavior economically unfeasible. Moreover, the proposed network equilibrium is self sustaining in the long run, if individuals are willing to participate. However, individuals who support such networks—the miners—do so only if they expect to attain positive returns on their investments. Due to the rapid increases in the network hashing rates the profitability of miners decreases rapidly they are not willing to constantly increase their levels of capital. This could be alarming in the long run when the maximum supply of a currency is reached, and the profitability of mining will rely solely on transaction fees. Nevertheless, such networks keep experiencing rapid growth with the Bitcoin network seeing a fourfold increase in computing power since January, and other networks such as the Litecoin network experiencing similar growth. The growth of such networks still has not been enough to convince most users to spend their holdings and many Bitcoins still remain unused. This is an impediment to any currency seeking to be a viable alternative to the dollar. It seems like individuals are not interested in cryptocurrencies as viable currencies just yet, but have turned to them because their increases in value making them profitable investments. However, the source of value still remains unknown. Although increases in computing power increase marginal costs of production it turns out that computing power does not Granger cause changes in price, but changes in price do Granger cause the network hashing rate. The fact that the marginal costs of production does not affect the price as hypothesized is alarming. Random walk tests on the price of Bitcoin revealed that it does not follow a random walk, which could be indicative of a bubble. With so much doubt and uncertainty in such cryptocurrencies, acceptability is becoming more widespread daily with more business accepting it as a means of payment. Bitcoin could be the future currency of the internet, or it could be another Tulip Mania 2.0.

A Malicious Miner's Problem

Since the malicious miner's problem proposed in (1) is analogous to a random walk on the integer lattice, we prove the following lemma which holds for asymmetric walks on the integer lattice.

Proposition: For an asymmetric random walk on $\mathbb{Z}$ with transition probabilities $p(i, i+1) = p$ and $p(i, i-1) = q \; \forall i \in \mathbb{Z}$ such that $q \neq p$, the probability of reaching state N before state 0 starting from i is

$$P_i(T_N < T_0) = \frac{1-(q/p)^i}{1-(q/p)^N}.$$

Proof. For $0 \leq i \leq N$, let $\phi(i) = P_i(T_N < T_0)$. Then of course, $\phi(0) = 0$ and $\phi(N) = 1$. First step conditioning for $1 \leq i \leq N-1$ we get,

$$\phi(i) = \phi(i-1)p(i, i-1) + \phi(i+1)p(i, i+1).$$

Equivalently,

$$\begin{aligned} &\phi(i) = \phi(i-1)q + \phi(i+1)p \\ \iff &(q)[\phi(i) - \phi(i-1)] = p[\phi(i+1) - \phi(i)] \\ \iff &\phi(i+1) - \phi(i) = \frac{q}{p}[\phi(i) - \phi(i-1)] \end{aligned}$$

To simplify notation, let $c = (\phi(1) - \phi(0))$. It follows that for $1 \leq i \leq N-1 \quad \phi(i+1) - \phi(i) = \frac{q}{p}c$. Thus,

$$\begin{aligned} 1 = \phi(N) - \phi(0) &= \sum_{i=0}^{N-1} [\phi(i+1) - \phi(i)] \\ &= \sum_{i=0}^{N-1} (q/p)^i c \\ &= c[(q/p) + (q/p)^2 + ... + (q/p)^{N-1}] \end{aligned}$$

Since $1 - x^n = (1-x)(1+x+x^2+...+x^{n-1})$, we have $1 = \frac{c(1-(q/p)^n}{1-(q/p)}$, so $\quad c = \frac{1-(q/p)}{1-(q/p)^N}$. It follows for $1 \leq i \leq N-1$, $\phi(i) = \phi(i) - \phi(0) = \sum\limits_{i=0}^{N-1} [\phi(i+1) - \phi(i)] = \frac{c(1-(q/p)^i}{1-(q/p)} = \frac{1-(q/p)^i}{1-(q/p)^N}$. □

Malicious Miner's Problem

Let a network's computing power be $\sum H_i = \bar{H}$, and the computing power of malicious and honest miners be h_m and h_h, respectively. The probability of a malicious miner finding the next block is $p_m = \frac{h_m}{\bar{H}}$, and the probability of honest miners finding the next block $p_h = \frac{h_h}{\bar{H}}$. Then the probability of a gambler with infinite wealth and resources reaching wealth z starting from 0 is analogous to a malicious user with infinite time and resources outpacing the network beginning z blocks behind. The probability is given by

$$P_0(T_z < \infty) = \begin{cases} \frac{(p_m/p_h)^z}{,} & if \quad p_m < 1/2 \\ 1 & if \quad p_m \geq 1/2 \end{cases} \tag{5}$$

Proof. Let r denote what one is willing to lose and z the the goal. Using our proposition, the probability of one reaching state z when one is willing to expend r in resources is given by $\frac{1-(p_h/p_m)^r}{1-(p_h/p_m)^{r+z}}$.
If $(p_h/pO_m) < 1$, then $(p_h/p_m)^r \to 0$ as $r \to \infty$, so $P_0(T_z < \infty) = 1$.
If $(p_h/p_m) > 1$, then $\frac{1-(p_h/p_m)^r}{1-(p_h/p_m)^{r+z}} = \frac{(p_h/p_m)^r((p_h/p_m)^{r-1})}{(p_h/p_m)^r((p_h/p_m)^{-r}-(p_h/p_m)^z} = \frac{(p_h/p_m)^{-r} \; -1}{(p_h/p_m)^{-r}-(p_m/p_m)^z} \to (p_m/p_h)^z$, as $r \to \infty$. Thus, a malicious miner's probability of outpacing the network given by (4). □

B Granger Causality

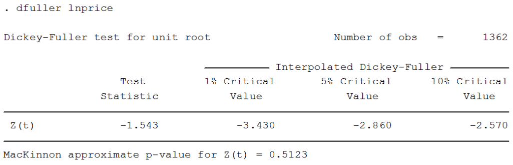
The following variables were defined in the STATA environment:

Table 4: Summary statistics

Variable	**Mean**	**Std. Dev.**	**Min.**	**Max.**	**N**
hash	2960998.802	10943805.377	0	80539344	1965
price	79.647	196.252	0	1151	1955
lnprice	2.543	2.456	-2.799	7.048	1364
dlnprice	0.006	0.083	-1.039	1.004	1362
lnhash	5.781	7.42	-9.909	18.204	1960
dlnhash	0.013	0.236	-3.076	2.89	1956

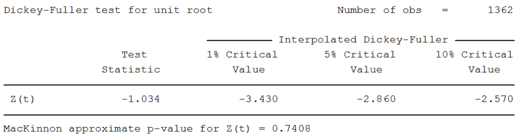
Since the model that was to be tested was an autoregressive model, the first thing that had to be done was to check for stationarity in the variables. Augmented Dickey-Fuller tests revealed that logged values of price and hashing rate were not stationary. This is a requirement for any time series regression. Thus, first differences were taken and the tests were run again. The first differenced variables were stationary.

Finally, the optimal number of lags was to be determined. We estimate to optimal number of lags by using information criterion by conducting a varsoc test in STATA. The starred cells are what STATA determines to be the optimal number of lags. It determines 3 lags are optimal using Schwartz information criterion and 10 are optimal using Akaike information criterion. The most parsimonious model is preferred so three lags is chosen.



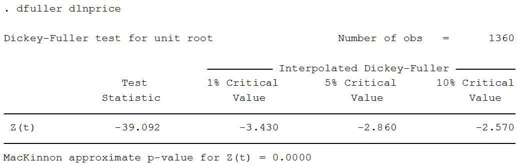
```
. dfuller lnprice

Dickey-Fuller test for unit root                   Number of obs   =      1362

                               ---------- Interpolated Dickey-Fuller ---------
                  Test         1% Critical       5% Critical      10% Critical
               Statistic           Value             Value             Value
------------------------------------------------------------------------------
 Z(t)             -1.543            -3.430            -2.860            -2.570
------------------------------------------------------------------------------
MacKinnon approximate p-value for Z(t) = 0.5123
```

Figure 7: Non-stationary price



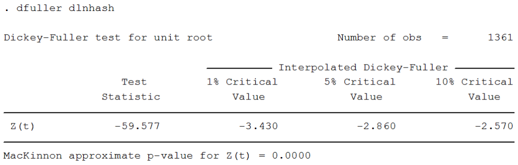
```
Dickey-Fuller test for unit root                   Number of obs   =      1362

                               ---------- Interpolated Dickey-Fuller ---------
                  Test         1% Critical       5% Critical      10% Critical
               Statistic           Value             Value             Value
------------------------------------------------------------------------------
 Z(t)             -1.034            -3.430            -2.860            -2.570
------------------------------------------------------------------------------
MacKinnon approximate p-value for Z(t) = 0.7408
```

Figure 8: Non-stationary hash



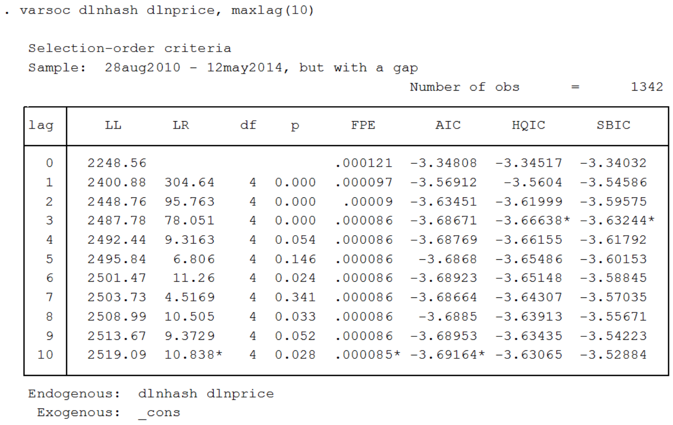
```
. dfuller dlnprice

Dickey-Fuller test for unit root                   Number of obs   =      1360

                               ---------- Interpolated Dickey-Fuller ---------
                  Test         1% Critical       5% Critical      10% Critical
               Statistic           Value             Value             Value
------------------------------------------------------------------------------
 Z(t)            -39.092            -3.430            -2.860            -2.570
------------------------------------------------------------------------------
MacKinnon approximate p-value for Z(t) = 0.0000
```

Figure 9: Stationary price



```
. dfuller dlnhash

Dickey-Fuller test for unit root                   Number of obs   =      1361

                               ---------- Interpolated Dickey-Fuller ---------
                  Test         1% Critical       5% Critical      10% Critical
               Statistic           Value             Value             Value
------------------------------------------------------------------------------
 Z(t)            -59.577            -3.430            -2.860            -2.570
------------------------------------------------------------------------------
MacKinnon approximate p-value for Z(t) = 0.0000
```

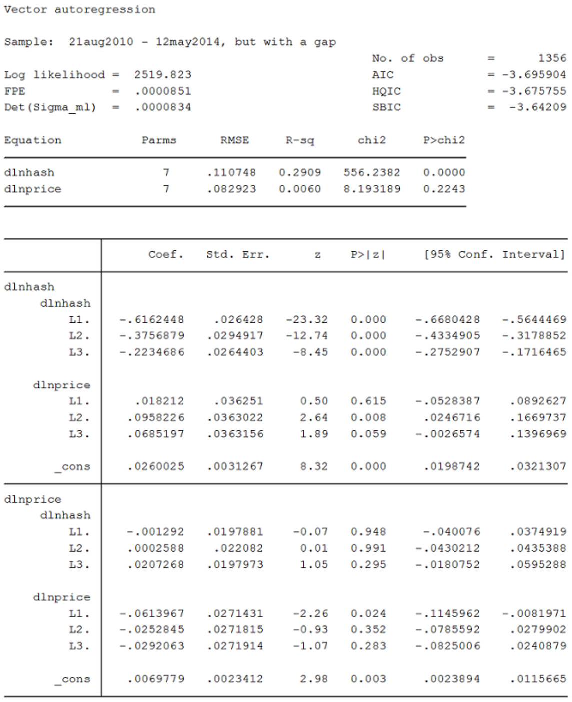
Figure 10: Stationary hash



```
. varsoc dlnhash dlnprice, maxlag(10)

   Selection-order criteria
   Sample:  28aug2010 - 12may2014, but with a gap
                                                Number of obs      =      1342
  +---------------------------------------------------------------------------+
  |lag |    LL      LR      df    p      FPE       AIC      HQIC      SBIC    |
  |----+----------------------------------------------------------------------|
  |  0 |  2248.56                      .000121  -3.34808  -3.34517  -3.34032  |
  |  1 |  2400.88  304.64    4  0.000  .000097  -3.56912   -3.5604  -3.54586  |
  |  2 |  2448.76  95.763    4  0.000   .00009  -3.63451  -3.61999  -3.59575  |
  |  3 |  2487.78  78.051    4  0.000  .000086  -3.68671  -3.66638* -3.63244* |
  |  4 |  2492.44  9.3163    4  0.054  .000086  -3.68769  -3.66155  -3.61792  |
  |  5 |  2495.84   6.806    4  0.146  .000086   -3.6868  -3.65486  -3.60153  |
  |  6 |  2501.47   11.26    4  0.024  .000086  -3.68923  -3.65148  -3.58845  |
  |  7 |  2503.73  4.5169    4  0.341  .000086  -3.68664  -3.64307  -3.57035  |
  |  8 |  2508.99  10.505    4  0.033  .000086   -3.6885  -3.63913  -3.55671  |
  |  9 |  2513.67  9.3729    4  0.052  .000086  -3.68953  -3.63435  -3.54223  |
  | 10 |  2519.09  10.838*   4  0.028  .000085* -3.69164* -3.63065  -3.52884  |
  +---------------------------------------------------------------------------+
   Endogenous:  dlnhash dlnprice
    Exogenous:  _cons
```

Figure 11: Optimal number of lags

The autoregression was then conducted using three lagged values of dlnhash and dlnprice. Clearly, the variation captured in the model for price is minimal and thus it is clear why the Granger causality tests yielded the results it did. The Granger causality test was then conducted and the results are in its appropriate section.

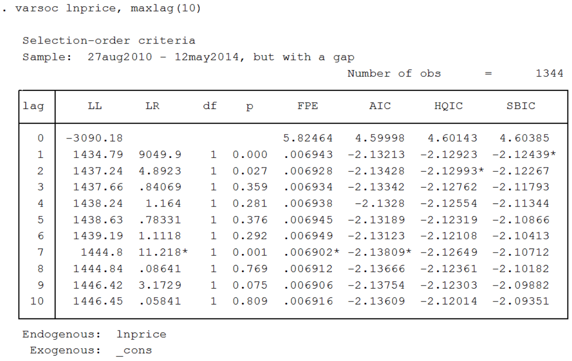


```
Vector autoregression

Sample:  21aug2010 - 12may2014, but with a gap
                                                   No. of obs      =      1356
Log likelihood =  2519.823                         AIC             = -3.695904
FPE            =  .0000851                         HQIC            = -3.675755
Det(Sigma_ml)  =  .0000834                         SBIC            =  -3.64209

Equation           Parms      RMSE     R-sq      chi2     P>chi2
----------------------------------------------------------------
dlnhash               7     .110748   0.2909   556.2382   0.0000
dlnprice              7     .082923   0.0060   8.193189   0.2243
----------------------------------------------------------------

------------------------------------------------------------------------------
             |      Coef.   Std. Err.      z    P>|z|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
dlnhash      |
     dlnhash |
         L1. |  -.6162448    .026428   -23.32   0.000    -.6680428   -.5644469
         L2. |  -.3756879   .0294917   -12.74   0.000    -.4334905   -.3178852
         L3. |  -.2234686   .0264403    -8.45   0.000    -.2752907   -.1716465
             |
    dlnprice |
         L1. |    .018212    .036251     0.50   0.615    -.0528387    .0892627
         L2. |   .0958226   .0363022     2.64   0.008     .0246716    .1669737
         L3. |   .0685197   .0363156     1.89   0.059    -.0026574    .1396969
             |
       _cons |   .0260025   .0031267     8.32   0.000     .0198742    .0321307
-------------+----------------------------------------------------------------
dlnprice     |
     dlnhash |
         L1. |   -.001292   .0197881    -0.07   0.948     -.040076    .0374919
         L2. |   .0002588    .022082     0.01   0.991    -.0430212    .0435388
         L3. |   .0207268   .0197973     1.05   0.295    -.0180752    .0595288
             |
    dlnprice |
         L1. |  -.0613967   .0271431    -2.26   0.024    -.1145962   -.0081971
         L2. |  -.0252845   .0271815    -0.93   0.352    -.0785592    .0279902
         L3. |  -.0292063   .0271914    -1.07   0.283    -.0825006    .0240879
             |
       _cons |   .0069779   .0023412     2.98   0.003     .0023894    .0115665
------------------------------------------------------------------------------
```

Figure 12: Optimal number of lags

C Random Walk Test

To test what would be the ideal optimal number of lags in this regression a varsoc test was run in STATA. The suggestion was 1 and 2 lags, if we were to choose the most parsimonious model.



```
. varsoc lnprice, maxlag(10)

   Selection-order criteria
   Sample:  27aug2010 - 12may2014, but with a gap
                                                Number of obs      =      1344
  +---------------------------------------------------------------------------+
  |lag |    LL      LR      df    p      FPE       AIC      HQIC      SBIC    |
  |----+----------------------------------------------------------------------|
  |  0 | -3090.18                      5.82464   4.59998   4.60143   4.60385  |
  |  1 |  1434.79  9049.9    1  0.000  .006943  -2.13213  -2.12923  -2.12439* |
  |  2 |  1437.24  4.8923    1  0.027  .006928  -2.13428  -2.12993* -2.12267  |
  |  3 |  1437.66  .84069    1  0.359  .006934  -2.13342  -2.12762  -2.11793  |
  |  4 |  1438.24   1.164    1  0.281  .006938   -2.1328  -2.12554  -2.11344  |
  |  5 |  1438.63  .78331    1  0.376  .006945  -2.13189  -2.12319  -2.10866  |
  |  6 |  1439.19  1.1118    1  0.292  .006949  -2.13123  -2.12108  -2.10413  |
  |  7 |   1444.8  11.218*   1  0.001  .006902* -2.13809* -2.12649  -2.10712  |
  |  8 |  1444.84  .08641    1  0.769  .006912  -2.13666  -2.12361  -2.10182  |
  |  9 |  1446.42  3.1729    1  0.075  .006906  -2.13754  -2.12303  -2.09882  |
  | 10 |  1446.45  .05841    1  0.809  .006916  -2.13609  -2.12014  -2.09351  |
  +---------------------------------------------------------------------------+
   Endogenous:  lnprice
    Exogenous:  _cons
```

Figure 13: Optimal number of lags