A Currency You Can't See: Bitcoin And Its Impacts On Our Society

by

Kehan Zhou
Class of 2015

A thesis submitted to the faculty of Wesleyan University in partial fulfillment of the requirements for the Degree of Bachelor of Arts with Departmental Honors from the College of Social Studies and with Departmental Honors in Economics

Middletown, Connecticut April, 2015
Acknowledgement

I want to take this opportunity to express my gratitude to all of the Economics Department faculty members for their help and support. As an Economics major, I am extremely lucky to have learned from and worked with many amazingly talented economists. I want to thank Professor Skillman for showing me the beauty of Economics during the intro class and constantly challenging me to grow as an economist since then. Professor Rayack, a mentor whom I highly respect, taught me to conduct empirical research and to use economics as a tool to challenge inequalities. From Professor Bonin, I learned the importance of attention to details in research and writing. I want to thank Professor Kuenzel for his feedbacks on my original Bitcoin paper. Last but certainly not least, I want to thank my thesis advisor and role model Professor Jacobsen for her continuous support and encouragement. Her positive attitude, passion for new knowledge, and abilities to analyze complex problems inspire me constantly.

I want to thank the CSS Co-Chairs and Mickie Dame for supporting my thesis research. The CSS department generously sponsored me to attend the Inside Bitcoin conference in Berlin, at which I learned so much on Bitcoin and cryptocurrencies. I also want to thank all the professors in CSS for teaching me how to analyze social problems from multiple angles and to think critically and productively.
I want to thank Professor Constantine for helping me understand the complex probability models involved in Bitcoin security. I am also grateful to have the opportunities to work with Professor Kaparakis whose humor, work ethic, and expertise in quantitative analysis never fail to impress me.

Certainly, I would not have been able to finish my thesis without the support from my family and friends. I want to thank my loving mother Wei Zhou for always believing in me and encouraging me to explore my passion. She taught me to follow my dreams and live everyday to the fullest. I also want to thank Andrew Lawson for his support and encouragement. I want to thank Nick Bender and John DiCandeloro for many stimulating conversations on Bitcoin, and Kerry, my writing mentor, for her help with my writing and her friendship.

Lastly, I want to express my appreciation to all, who directly or indirectly, have contributed to my thesis. Thank you!

Sincerely,

Kehan Zhou
An Investment Mishap Led to a Thesis Topic

Near the end of 2013, in the midst of Bitcoin’s historical rally, a friend who studies software engineering introduced me to the idea of cryptocurrency. I found the idea of creating a currency based on Internet connection and cryptography both futuristic and fascinating. At the same time, I was surprised by the high price of Bitcoin, which in December 2013 stood at 1000 dollars each. I decided to earn some extra spending money in cryptocurrencies, so I started “mining”, a process by which one obtains cryptocurrency using one’s computer. I decided to mine a less known and less valuable cryptocurrency, Dogecoin. Despite Dogecoin’s silly name and logo, which is the face of a dog, it had a lot of support in the first couple months of its creation in December 2013. Dogecoin supporters had their mantra “to the moon”, hoping that one day a Dogecoin would be as valuable as a Bitcoin. I spent hundreds of dollars on computer parts to help me mine Dogecoin faster, kept my computer running nights after nights, and managed to accumulated 10,000 Dogecoins by the end of January 2014.

Unfortunately, my dream of getting rich from Dogecoin never took off. Dogecoin soon ran out of steam and its value, which was worth a fraction of peanuts before, sank like a stone. At the point when I completed this thesis in April 2015, my vast ownership of Dogecoin was worth a little bit over a dollar.

However, in the process of tracking my investment in Dogecoin, I became more and more interested in the technology of cryptocurrency and its underlying economics. But there is a void of economic studies on Bitcoin and other cryptocurrencies. The information I could find online was mostly superficial in nature.
and most of it was about Bitcoin scandals. So I decided to analyze Bitcoin and cryptocurrencies more thoroughly and from the point of view of economics in order to provide more insights into this understudied topic.

Thus, while my investment never grew in value, the experience of mining Dogecoin paid off handsomely, as it opened my eyes to the topic of cryptocurrency.
Introduction

“What is the future of money?” many have asked, anxiously awaiting an answer. The origin of money is a mystery but the emergence of coin and paper money can be traced back to seventh century B.C. (Dumas 2015). Frankly, money has not evolved a lot since then. While nowadays we have credit cards and online banking, the essence of money is still to facilitate transactions. In addition, most of the time governments monopolize the issuance of new currencies. Citizens, thus, do not have a lot of choice in terms of what currency to use.

In 2008, a mysterious programmer, Satoshi Nakamoto, published the first paper on Bitcoin theory. In this paper Nakamoto articulated his idea of a network-encrypted virtual currency without a central authority to monitor the transactions. One year later, Nakamoto ceremonially mined the first block of Bitcoin and started this cryptocurrency revolution. A cryptocurrency is a digital currency that relies on cryptography to issue new units and verify transactions without a central authority. Since 2008, cryptocurrencies such as Bitcoin have drawn a lot of attention from the media and innovators, promising a new age of money.

As of early 2015, over two thousand different cryptocurrencies exist, sharing a billion-dollar market capitalization (Coinmarketcap 2015). It appears that they have become a disruptively innovative force that cannot be ignored. Big corporations such as Tesla and Paypal plan to incorporate cryptocurrencies into their businesses. Governments around the world are learning about how cryptocurrencies could affect their monetary policy and tax regulation. Given their apparent increasing importance,
understanding how cryptocurrencies function will help us predict the impact they will have on our world.

In my thesis, I will focus on a particular cryptocurrency - Bitcoin- to explore the cryptocurrencies world. Bitcoin was the first functioning cryptocurrency and it has the largest support base. It also has the highest trading volume and largest market capitalization. Additionally, most of the subsequent cryptocurrencies are based on the Bitcoin protocol and are variations on the same principle. Thus, studying Bitcoin will provide an accurate representation on the overall dynamics of cryptocurrencies.

How Bitcoin Works

As a currency without a central bank, the Bitcoin algorithm puts new currency into circulation through a process often referred to as mining. Bitcoin is mined by creating computational blocks containing information on new transactions. Miners who spend time and energy collecting transaction information and creating the blocks are awarded with new Bitcoins after finishing each block. Thus, much like gold mining, miners are compensated for providing liquidity to the market. Bitcoin miners, also known as nodes, maintain a chain of blocks that contains the full transaction history of Bitcoin. If attackers want to change the transaction history to steal Bitcoins, they need to create blocks in the blockchain at a faster pace than the sum of the speed that the honest nodes in the network can create new blocks. They need to outpace all honest nodes’ creation of new blocks. As long as the network is supported with honest miners, attacking cryptocurrency is an extremely demanding task. This is why cryptocurrencies have robust security measures against hacking.
Bitcoin is a virtual currency that is enabled by cryptography technologies. For example, a wallet in the Bitcoin system entails only two sequences of numbers. A hypothetical Bitcoin owner, say Alice, has two sequences of numbers that represent her Bitcoin ownership. The private key allows Alice to spend her Bitcoin, and the public key is Alice’s receiving address, helping the network to verify the authenticity of the transaction.

Bitcoin differs from traditional fiat currencies in four major ways beyond technical details. First, most currencies are issued by national governments as a way to unify currency within their territory (with the Euro as a notable exception). In contrast, Bitcoin is not mandated by a government, but is supported by the international Bitcoin network. As a product of cyberspace, Bitcoin is not bounded by geographical limitations and can facilitate international transactions more quickly.

Widespread adoption of Bitcoin could have significant implications for international trade. International companies vulnerable to foreign exchange risks pay premium to financial institutions to neutralize the currency risk. If cryptocurrency prevails, international trade could be carried out without the risk of currency conversion and dispute.

Second, in contact to currencies like the USD and Japanese Yen (JPY), Bitcoin has a stable supply that is predictable. Anyone with a computer can start mining Bitcoin and will be compensated for their service. However, the speed at which Bitcoin can be mined varies with the number of miners in the network. The level of mining difficulty is positively correlated with the number of miners at a given time. The built-in algorithm of Bitcoin is designed to keep supply Bitcoin increasing
at a constant rate regardless of its price volatility. As Figure 1 shows, Bitcoin supply has been increasing as a predictable rate while Bitcoin price fluctuates violently. According to Nakamoto, this characteristic is analogous to gold mining. Similar to the gold standard system, Bitcoin is not subject to monetary policies that operate to change the money supply.

Thirdly, transactions involving Bitcoins are in essence computer programs. Each transaction is a paragraph of computer codes that can be written to do much more than transferring money from one owner to another. Bitcoin transactions can be programmed to accomplish complicated payment arrangements that involve multiple dates, accounts, and conditional payments. This concept of “smart money” sets Bitcoin apart from any traditional currency.

Figure 1: Bitcoin Supply and Price from 2010 to 2014 (Data Source: Thomas 2015)
Lastly, Bitcoin does not require an authority to monitor online trades. Banks and ecommerce companies such as PayPal are crucial in traditional online transactions. These trusted third parties help prevent double-spending of online credit. Double spending is when the same credit is spent again after being used in a previous transaction. Having a third party to clear and validate each transaction is costly and inefficient. Nakamoto writes: “commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments” (2008, 1). Meanwhile, Bitcoin does not depend on a third party to facilitate transactions. This has two main implications. First, Bitcoin is a decentralized payment system. By using its decentralized network to verify transactions instead of using a third party, Bitcoin transactions are cheaper compared to traditional services. Second, privacy of the transactions is maximized, because security is guaranteed by the network and cryptography rather than proofs of identities from counterparties.

Since Bitcoin’s inception in 2008, the Bitcoin community has grown tremendously. This momentum pairs with the spike in Bitcoin’s monetary value. Over the course of five years, the price of Bitcoin has tripped from six cents to $255 per Bitcoin in April 2015 (Coinmarketcap 2015). During the early age of Bitcoin development, a Bitcoin supporter bought two large pizzas with 10,000 Bitcoins; that payment would now be worth 2.5 million dollars (Caffyn 2014). Its popularity and dramatic price movement have led more people to scrutinize cryptocurrencies and to understand whether this is the new technology that will have a significant impact on our lives like computers and the Internet. The goal of this thesis is to understand the
future of cryptocurrencies through Bitcoin and five different lenses: historical context, supply side, demand side, market dynamics, and technology applications in other fields. Each chapter analyzes Bitcoin through one perspective, together to answer the central question: are cryptocurrencies a new secular phenomenon that will change the world?

**Thesis Outline**

Chapter One situates Bitcoin in historical context. While cryptocurrency is a new phenomenon, the concept of alternative currency, free from the government or for a particular political goal, has been a historically recurring theme across different countries. A recent example is the Barter System in Argentina created during the ongoing financial crisis. Notably, most alternative currency movements have been short-lived and limited in their influence. Through analyzing the history of alternative currencies, I try to understand how various alternative currency movements came about and the common challenges they face. Then I compare and contrast Bitcoin with other movements to understand how Bitcoin is similar to these currencies and why it is also unique.

Chapter Two focuses on the production and technology of Bitcoin by analyzing the supply side. The implementation of Bitcoin relies heavily on cryptography and the advancement of computer science. It is crucial to comprehend the technology behind Bitcoin in order to appreciate its limits and potentials. This chapter explores this technical space with a focus on Bitcoin production, or mining. Miners facilitate Bitcoin transactions and help put new Bitcoin into the circulation.
The number of miners is crucial to the health of this currency. This chapter will provide a model to understand the cost-benefit analysis for mining and explore whether the current level of mining is sustainable.

Chapter Three explores the demand side of Bitcoin. The central question is who is using Bitcoin and why. This chapter first presents data on Bitcoin user’s demographics and what people use Bitcoins for. In particular, are they using it to buy illegal goods? Then I will analyze Bitcoin’s functionality as a form of currency through its store of value, medium of exchange, unit of account, and proof of security. After analyzing why consumers might use Bitcoin, I will look at the other side of transactions, businesses. More and more businesses have started accepting Bitcoin and I present some reasons to explain why there is an increasing incentive for merchants to adopt Bitcoins. Lastly, this chapter investigates the use of Bitcoin as a financial instrument in investment portfolios.

Subsequent to these discussions on the supply side and demand side of Bitcoin, Chapter Four explores the market dynamics for this currency. We will look at the efficiency of the Bitcoin market by looking at several indicators, such as money velocity and arbitrage opportunities. By analyzing the improvement in the Bitcoin market, we will be better able to understand the prospects of this cryptocurrency market.

Finally, in Chapter Five, we will enlarge the scope of analysis to not only Bitcoin but also other cryptocurrencies in order to understand their interrelated evolution. As of April 2015, there are more than two thousand cryptocurrencies and the number is still growing (Cryptocoins Chart 2015). In addition, Bitcoin has
inspired technological innovations in many other fields. I will explore how Bitcoin technology can be used and provide better solutions to many problems. Lastly, I will provide a prognosis of the future impact of cryptocurrencies on our society.
Chapter One: Historical Context for Bitcoin

Contrary to its everyday look and deceiving familiarity, money hides its complexity under colorful bills and shiny coins. We have a complicated relationship with money; some aspire to be rich in it while some despise it beyond necessity. Philosopher Georg Simmel argues in his book, *The Philosophy of Money*, that money promotes rationalization and freedom (Simmel 1978). The use of money helps dissolve bonds based on kinship, because it is impersonal. To others, money is the tool for the ruling class to achieve domination without visible coercion; it is the equivalent of weapons and shackles in a civilized world. However, money is in fact a flexible concept that can acquire different characteristics. Alternative currencies are the best examples of how the idea of money can still be surprising beyond its familiarity. Alternative currencies are various forms of money that operate along the side of traditional state-issued currencies. Bitcoin, for example, is an alternative currency. It is created by a programmer and maintained by the Internet. In this chapter, I trace back to noteworthy moments of alternative currencies in history and compare them to the on-going Bitcoin movement. By putting Bitcoin into its historical context, this analysis will further our understanding of Bitcoin and why it is revolutionary.

The evolution of money is driven by the dissatisfaction with the status quo. From the barter economy to using precious metal as a medium of exchange, money was created. From heavy gold ingots to paper currency, money became lighter and easier to carry. From cash to bank credits, money became more secure and invisible. Yet, modern currencies are still monopolized by the states. The founder of the
German Historical School, A. Muller, argued that money is an expression of the trust people have for the state and a form of the common will (Karimzadi 2013, 139). A country’s money, like its national flag, marks the national identity of its users and represents the control of the state. However, the monopoly can be limiting to citizens who disagree with a country’s monetary polices or ideology but have no other choice. That is when public trust in the state is low; people are looking for alternatives to replace the state currency. This dissatisfaction with national currency has driven many of the alternative currency movements in history. This is also why often these movements accompany economic distress when the “common will” departed from the will of the state. This chapter will look at examples of currency movements that attempted to escape the influence of the state in order to understand the challenges they faced. This will provide a historical context for Bitcoin’s creation.

**Robert Owen’s Labor Note**

One early example of alternative currency is the Labor Note. It was used as a way to wage an ideological war against the capitalist state during Britain’s Post-Napoleonic Depression. French socialists inspired the Labor Note. Robert Owen argued “that the source of all value was labor” and advocated for a currency that used labor hours as the basic unit. He explicated this idea in 1820 and by 1832 more than four hundred cooperatives that issued and accepted labor notes had sprouted like mushrooms in Britain (North 2007, 43).

Labor Note used labor hours as a unit of account. Producers were compensated for the hours they spent making a product and could use the note to purchase other goods. At their peak, Labor Note exchanges were exchanging over
fourteen thousand Labor Notes per week (North 2007, 44). The exchange’s doors often had to be closed due to the swarming crowds. Yet, the momentum of the movement dropped drastically; in 1834 the trading volume dropped more than sixty percent from the previous year. There were many reasons that the exchange lost its appeal to the public.

In hindsight, the Labor Note lacked the necessary level of support and its functionality as a currency suffered from serious flaws. The Labor Note failed to gain support from the poor. Because the movement operated mostly on Owen’s personal investment, the poorest were not given access to initial raw materials and could not begin to produce; they were excluded from the operation of the exchanges by default (North 2007, 49). In addition, the lack of food items in the exchanges further precluded the poor from supporting the exchanges. To the poor, food was a major expense and unfortunately the Labor Notes could not cover their needs. To make matters worse, the food vendors outside of the Labor Note exchanges took advantage of the situation by heavily discounting Labor Notes when selling the holder food. It was irrational and unrealistic for the poor and most disadvantaged to support the Labor Note since they could not survive on it.

One obvious flaw in the Labor Note was its method of denominated value in labor. Labor is by no means a homogenous input or product. It varies with many factors: physical strength, knowledge, skills, and intelligence. A skilled woodworker can make a beautifully polished table in two days, while it might take an apprentice months to do the same. The quality of labor spans such a great range that unifying it with respect to time is neither a sufficient nor fair representation. As a result, the
marketplace became the “lemons market” described by George Akerlof (1970). People with skills that produced good products had less incentive to participate in the exchange, as the indistinguihing Labor Note would undervalue their work. On the other hand, people with poor skills were more likely to join the Labor Note system and become the “lemons”. To make matters worse, the exchanges made inadequate effort in estimating how much time an item took to produce. Rather, they accepted the estimates by the workers themselves, which provided an incentive to cheat and left the currency vulnerable to moral hazard. North argues that the inefficient market valued items unevenly (North 2007, 48). While the undervalued items became scarce and hard to get, the overvalued items started to accumulate in the stores, reflecting the imbalance of supply and demand at the Labor Note exchanges.

Lastly, the Labor Note suffered from security issues. Because the exchanges were poorly organized, the markets attracted serious frauds (North 2007, 47). The currency itself was easy to counterfeit and ensuring security was a major challenge. The reputation of the Labor Note declined as the more fraudulent exchanges took advantage of the movement. Moreover, even within the genuine exchanges, trades were poorly regulated, which posed risks for the consumers. These risks only amplified for the poor people who could not afford to lose their grocery money.

Owen aimed to bring about a utopia through a new form of currency system that honored labor and honest work. However, reality rarely holds up to high expectations. The implementation and the design of the currency were not perfect. The Labor Note was not a good medium of exchange because it was limited to local exchange and the variety of product it could purchase was restrained by geography. It
also did not serve as a good unit of account. In fact, it is hard to value it because labor is heterogeneous. Lastly, the Labor Note failed the security measure. The prevalent fraud destroyed people’s trust for it.

**Manchester LETS**

While Owen’s Labor Note aimed to bring about a revolution to establish a utopia, the modern alternative currency movement Local Exchange Trading System (LETS) intended to serve more as a supplement to the existing currency instead of as a replacement. The Manchester LETS was founded in 1992 (North 2007, 79). At the point, Britain had been expelled from the European exchange rate mechanism and the U.K. economy fell into a deep recession (North 2007, 79). The LETS administration was careful to keep it a value-free system. It was built to be a value-neutral tool to facilitate local trading. LETS avoided alienating people with a fixed ideology to maximize its appeal and usage among the masses.

For example, the administration for Manchester LETS emphasized the system’s neutrality by calling the unit for LETS currency “bobbin”. In the local slang, bobbin means something that is of little worth and use. The name was chosen to demonstrate the idea that modern currency does not have any value by itself, but a symbol of value. Bobbin users determined both its monetary and ideological value. In every community that used LETS, a directory that contained services and goods provided by local members was available to all members. If a member wanted to purchase something from a buyer, the cost was negotiated between the two parties. When an agreement was reached, they submitted the trade to the administration who would credit the seller and debit the buyer. The central administration kept record of
each member’s balance and the records was available to all members to warn them about possible fraud. In case of a bankruptcy, the loss was distributed to all members in the community. LETS was a mutual credit exchange system, meaning that the currency was created simultaneous to the transaction (North 2007, 82).

Because LETS presented itself as a value-free tool for all, it attracted people with varying beliefs. Compared to the labor notes, LETS appealed to various organizations to support it. There were three major groups that supported the LETS movement: humanizers, greeners, and anarchists.

The humanizers actively promoted a higher participation from the mainstream economy. They believed that a large numbers of traders would help build an efficient network and simplify the monetary relationships between people in capitalism. They argued “that through their everyday interactions with others traders would be subjected to a number of social, market, and micro-political signals that would transform their outlook for the better” (North 2007, 87). North points out that some people joined this network because of their desire to be in an economy “that values people more than profit, need more than efficiency, and quality more than cheapness” (2007, 87). The humanizers envisioned a “throwback” economy to be achieved through LETS.

The greeners hoped to utilize LETS as a way to an economy favoring local products over imported ones. A localized economy, they argued, would be less polluting and more resilient. Their argument was ahead of its time and still exists in many local co-ops.
According to North, “the LETS anarchists fell into the nonviolent, Gandhian branch of Anarchism rather than the violent, Bakuninite class-struggle Anarchism” (2007, 91). These LETS supporters aim to live outside of the capitalism system. They tried to bring back a different set of values and they believed that LETS was tool for further resistance to capitalization and globalization.

These three schools of thoughts supported LETS because it was organized as an alternative to the capitalistic society and the value their government stood for. In contrast to the traditional system where money is issued by the government, LETS stood out in three major ways. First, it was a credit system. This reduced the chance of loss and theft that often happened to cash transitions. Second, LETS system was a mix of local issuance and central governance. Any individual could issue this currency by participating in one transaction. There was not a set value of the LETS currency as opposed to the centrally issued currency. “Members were free to decide how to value their work, how to value the bobbin, and how much sterling to charge, and individual members with different sets of values were left free to interact” (North 2007, 83). At the end of each day, all the transactions and balance were submitted to the central administration that kept the records and made it available to all members through a public directory.

Lastly, LETS operated in an interest-free scheme (North 2007). An interest-free scheme is counterintuitive to those in a system in which people are rewarded for their investment. In the interest-free LETS system, capital did not command as much force as in a capitalistic system where financiers could support themselves by moving funds around. Consequently, labor became the only source of value. LETS credits
were created and earned through transaction of services or products. Following the paramount position of labor was a more humanized economy in which relationship were valued over profit. This led to a more relaxed and relationship-driven trading environment where the connection between people would be more supportive than exploitive.

Unfortunately, the Manchester LETS shut down in 2005. The LETS system still lingers in some local communities, but its momentum and popularity has vanished out of sight. At this point, there are only several Internet applications of LETS. One of them is called Community Exchange System. They have around forty thousand active users around the globe who use it as a supplement to traditional monetary system. However, all these applications are small in scale and have no global implications.

LETS suffered from many drawbacks. One LETS member’s interview fully revealed LETS that did not function well as a medium of exchange. He said: “I’ve accumulated a great pile of bobbins in my bobbin account- which I haven’t as yet spent! I don’t know where to spend my bobbins” (North 2007, 100). Because of the low participation and small exchanges, people who owned bobbins often could not spend them. On the other hand, even when a bobbin was spent, it did not have good purchasing power. The Manchester LETS also suffered from a poor unit of account because it emphasized an individualized and personal valuation. There was no official statement or guidance as to how much a bobbin was worth in terms of the state-issued currency; users set prices and spent them based on their gut feelings and very
subjective notions of fairness. The amount one paid for a service might change drastically depending on the buyer’s relationship with the seller.

Thus, the relationship-based currency suffered from its very source of uniqueness: relationships. Simmel mentioned that money could be a way to clean up the complicated relationships people have to navigate in division of labor (North 2007, 20); it simplifies everything by applying a standard valuation system. LETS did exactly the opposite; it focused on the relationship between producers and consumers and consequently, relationship sometime got in the way of transactions. The users “found negotiation difficult, unsure about how much to ask people to do” and how much to pay (North 2007, 98). Some also found it difficult to make the first step of establishing connection with another member. Thus, the LETS economy made a simple transaction much more complicated in comparison to a quick cash payment.

LETS was designed not as a replacement but a supplement of the market economy. However it was overshadowed by the dominant economy; its benefits and meaning were lost in the dark. People often referred to the traditional money when making a trade. Many members found that “culture codes were not changed and the influence of structural forces in terms of common-sense value about money – that “debt is wrong,” that “it is good to have savings,” that “you can’t spend what you haven’t got” remain to govern the system” (North 2007, 99). At the end, the mainstream understanding of money dominated the innovative thoughts behind LETS, making the value of having a community-based trading system fade into the background. Combined with its inconvenience, the overshadowed and pale currency eventually lost its ground.
Argentine Barter

The LETS movement aimed to serve as an addition to the mainstream economy in a non-threatening way. In contrast, the Barter system in Argentina took up the burden of supporting millions of the poor during the crisis in the 1990s and early 2000s. In the 1990s, Argentina went through an economic deregulation. As a result of the policy changes, unemployment was high and GDP fell sharply. As a response to restrictive policy and mass unemployment, the Barter networks spouted in 1997, first in Bernal. These barters were facilitated with “currency generated by community groups, nongovernmental organizations, communities, and private businesspeople” (North 2007, 149). The development of the Barter networks was symbiotic with the crisis. The movement gained popularity as the crisis in Argentina worsened. According the organizers by 2001, “4,500 markets were used by a half a million people spending 600 million credits across Argentina” (North 2007, 153).

The mass usage of the Barter network was out of necessity. The harsh economic recession left many people in Argentina jobless and without food security. Many middleclass men were out of work and the women took up responsibilities to use Barter to provide food for their families. The people who used the network were called “prosumers”, who produced and consumed at the same time. They went to local barters to earn credits by selling products or services and then used it to purchase necessities. Some made pancakes to sell and used the credits to buy groceries and toilet paper for the family. One prosumer commented: “for me it was like a job… that year I could live off the trueque (Barter market), more of less”
(North 2007,158). To ensure fairness, market coordinators who facilitated transactions and monitored overly inflated price ran the markets. They cruised around the market to solve disputes and helped people get into and out of the market.

The Barter networks had a high degree of diversity and were organized according to different visions of the system. For example, the Red Global de Trueque (RGT) used a franchising model to promote their credits called arborlitos. The other major group, Red de Trueque Solidario (RTS) was active in most capital cities using locally diverse credits. RTS credits were created by the local exchanges and were not always convertible to other local RTS credits. RGT believed in a centrally managed and franchising approach while RTS was much localized and diverse. Their fundamentally contrasting concepts of how to organize the Barter system led to different responses when the crisis deepened in 2002.

The great depression of Argentina reached a height when the government decided to limit the amount of deposits one could withdraw each month, which is referred to as Coralito, in order to avoid defaulting on the IMF debt. People could not withdraw more than 300 pesos per month. This limit on withdrawing was joined by the devaluation of peso after the end of the peg. According to North, “the economy literally ground to a halt and million faced acute hardship, if not starvation” (North 2007, 154). The RGT responded by essentially increasing the money supply. They printed currency and sold barter start-up kits that included Barter credits paid by pesos. They argued that “the inflationary consequences should be disregarded in the short term in what was essentially a ‘Keynesianism from below’” (North 2007, 154).
In this regard, RGT credits resemble traditional currency in that they were centrally controlled, which made monetary policy possible.

On the other hand, RTS disagreed with RGT’s response to Coralito. They believed that the oversupply of currency would cause severe inflation and the key to help people overcome crisis was through community-based mechanisms. They insisted on the prosumer model where people contribute products before consuming. In addition, they also attacked RGT’s authoritarian nature and believed in a more democratic exchange system. This democratic decision-making dictated that RTS had to hold a monthly national meeting to discuss different decisions on exchange management.

History has proved that neither group was able to stop the deepening crisis in Argentina or to help millions of people who would do anything to survive. The “monetary expansion” by RGT was hugely inflationary. What made the matter worse was the franchising model. Some exchanges opened with bad management and convoluted the market. The bad exchanges also shook people’s faith in RGT. It was again like a lemons market, where the bad credits drove out the good. As an outcome of both, the value of RGT credit plummeted. As North documented, “a bolt of cloth selling for 40 credits in April went to 5,000 in November” (North 2007, 165).

The community-building model insisted on by the RTS, on the other hand, was overwhelmed by the number of people who wanted to earn their livelihood in the exchanges. The democratic approach was too slow to keep up with increasingly large number of participants. These new prosumers did not learn how to use the Barter network and often caused conflicts. As a result, the nodes were no longer supportive
communities where people survived the crisis together. They became a pessimistic state of nature where people competed and deceived each other. One participant commented that “people used to fight; they killed each other for a rag or for food” (North 2007, 164).

As a result of the horrific situation in Barter exchanges, in 2002 the exchanges lost more than sixty percent of their users. Even though the exchange system is still around in Argentina today, its popularity has decreased dramatically. Both RGT and RTS have changed their approaches to organize respective exchanges. RGT gave up the franchising model and switched to a more community-based system. In 2009, a leader from RGT commented that the exchange should not hold more than 100 people to ensure quality, which was greatly different from their old approach (Cerioli 2009). RTS insisted on its old method but retreated to smaller exchanges of 20 or 30 traders, a model that is much more like a LETS. The Barter system of Argentina did not disappear like people had predicted (North 2007, 168).

To many, the Barter system before the peak of the crisis represented a lifestyle that is becoming extinct in face of the capitalist expansion. The market environment was more cooperative than competitive. It was a place where people helped each other to survive hardship and a disastrous economic decline. To some, the market was not only a place to earn a livelihood, but also a place to make friends and find camaraderie. Before the economic condition worsened, people mostly traded fairly with each other and the participants were supportive for one another. The exchanges were often small and cozy. Going to an exchange was once a fashionable thing. North points out that on the weekends people often went to the barter market to get a cup of
coffee, sit around, and talk. The barter network brought people together in a local setting and generated solidarity to overcome economic hardship (North 2007, 159).

Yet, the Barter system as a currency is wildly insufficient and does not have global influence. First, the Barter system can only function well within small local communities but it is not scalable for larger applications. The barter exchange was a delicate ecosystem that required attention and honesty. Its low capacity dictated that when used by a large number of people the quality of transactions would go down. Once above its capacity, transactions in the exchanges became death-battles between the poor. Some smart business minds also went around exchanges to buy low and sell high. The system was overwhelmed.

The second major failure for the barter was the poor store of value of its currency. The hyperinflation created by the RGT’s franchising was an example of the instability in its value. Barter credits were created by non-state organizations. These credits were worthless by nature unlike gold or silver. If currency backed by the states can be unstable, this is even truer for the Barter credits.

The last reason for barter’s inability to become a major alternative currency system is its poor medium of exchange. Because the physical limits of an exchange and the efforts needed to maintain an orderly trading environment, the scale of the exchange is severely limited. The amount of participants is best limited to 100 as the crush has suggested. A small exchange cannot afford a wide variety of products that its participants need. The variety of product Barter can purchase is limited. With the Barter currency, people only have access to limited goods compared to the great
varieties of commodities in the global market. These plagues eventually disconnected the Barter system from its popularity.

**The Benefits of Alternative Currencies**

All of the three examples presented above demonstrated that innovations in currency are motivated by the need of an alternative when the trust in government currency is low. Some of them are more militant, such as the Labor Note; while some are less threatening, in the fashion of LETS. The dissatisfaction with state currency drove the alternative currency movements. In the case of the Labor Note, the dissatisfaction was ideological, while the dissatisfaction that motivated barter in Argentina was more out of the necessity to survive. Even though all of them failed to generate long-lasting influence, these movements demonstrated the possibility of money creation outside of the traditional government monopoly.

These examples are only some of many possible ways to create a new currency. Contrary to popular believes, the form of money is flexible and diverse. Money can be a state-issued currency backed by a strong government or any medium people are willing to accept. As we have seen, money has both local and systematic influence. Traditional currency issued by the government penetrates each layer of our everyday life in a systematic way. This kind of money often dominates what we conceive as currency. On the other hand, currency such as LETS created many communities where a different set of rules and values was practiced. These local exchanges are safe spaces one can escape to where one might find comforts and others alike. It is in these distinct spaces money exhibits its diverse nature and versatile properties. For example, money does not have to be a source of domination.
In the LETS system, one did not need to have money to start production, since anyone could issue credits. Even the poorest could start production in this system. Additionally, LETS currency operated in an interest-free system. Without the time value of money, capital did not serve as a servant for the rich to get richer. Creating an alternative currency scheme, LETS fundamentally changed the relationship people had with money from hostile to productive. Thus money, like any other tool invented by people, does not have a fixed nature and can change according to our will and our understanding of it.

While each alternative currency brings some different advantages to the monetary system, alternative currencies in general have several benefits. The proponents of LETS valued “diversity through a multiplicity of local currencies, [and] view[ed] the economy as a collection of interdependent actors connected to each other,” which “through its diversity is resilient” (North 2007, 91). Diversity in currency resembles diversity in an ecosystem; it helps reduce the risk of disasters. When government-issued currency suffers from hyperinflation, alternative currencies provide a functioning market that saves lives, such as in the case of Argentine Barter. Even though the Barter exchanges eventually caved in the face of the overwhelming numbers of jobless people, they cushioned the economic free fall.

Alternative currencies help increase the degree of informal employment. “By strengthening informal employment opportunities, many livelihoods can be generated quite quickly and cheaply to satisfy and stimulate local demand” (North 2007, 161). One might not have the time to attend a full-time or even a part-time job, but in a local exchange they can sell their cooking or homemade products according to a
flexible schedule to earn some extra for the household. This kind of informal employment bridges the gap between being employed and unemployed, by providing a more flexible option.

Alternative currencies also satisfy people’s need of money that represents different values. Viviana Zelizer argued that we mentally earmark money to represent different uses of it. She pointed out that “we react against the use of the ‘wrong’ sort of money or a ‘wrong’ use of money, such as giving money as a gift or as a declaration of love or paying for sex.” Money should be as diverse as the many ways we use it to embody different emotions and relationships. While traditional currency represents our duty to our national government, currency like LETS represents a neighborly love and solidarity.

Lastly, a competitive currency market holds all currencies accountable. Hayek believed that governments have incentives to print excessive amounts of money to finance their budget (Hayek 1976). As a result, inflations are common. Alternative currencies increase competition in the currency market. Governments then will have to minimize inflation. Alternative currency movements are in fact liberation movements for the currency market.

**The Challenges Alternative Currencies Face**

Alternative currencies contribute greatly to the resilience of the financial system and the diversity of our economic lives. While alternative currencies can benefit our societies in many ways, they also face many barriers when they try to survive in the mainstream economy. Traditionally, money is required to satisfy three criteria: medium of exchange, store of value, and unit of account. However, I argue
that these three criteria do not cover all the sufficient conditions for a successful currency. As demonstrated by the Labor Note and the Argentine Barter, the security of an alternative currency is crucial to its success. The importance of security is often overlooked because most of the currencies we use today are issued by the government and insured by the government. However, in the context of alternative currencies, the absence of government makes security a major hurdle for these currencies to overcome. Thus, the complete criteria for a successful currency should include, medium of exchange, store of value, unit of account, and proof of security. Without any one of these four, a currency cannot be fully functioning. Here I look at each criterion and understand the common challenges for alternative currencies.

Medium of exchange is a very important criterion and a good indicator of success. The amount of people buy into it affects the confidence and the authority the money commands. Additionally, if one decides to get off the standard monetary system and live fully on one alternative currency, it is important for the currency to be accepted by different producers and services to satisfy one’s diverse needs. Thus, the medium of exchange measures both the popularity of the new innovation and the potential commitment of its supporters. Yet, new currencies struggle to find vendors that accept them and costumers who believe in them. Matching the variety of product traditional currency can buy is difficult. To make matter worse, because most countries have their own currency as a legal tender, one has to pay taxes with legal tender even if one could live a life completely on alternative currencies.

Store of value is also a challenging criterion for alternative currencies. Many alternative currencies suffered from hyperinflation when people lost faith in the value
and prospect of the currency. In the case of the Argentine Barter, RGT’s arbitrary decision to flood the market with cheap credit created a major inflation that overwhelmed the Barter system. If the value of a currency is not kept stable, its supporters run major risks from the price volatility.

Unit of account is a fairly simple criterion to fulfill. In these examples we have seen, labor notes had trouble with it because it uses labor as the basic unit that is not a homogenous product. LETS also suffered from it near the end, because people were allowed to determine the value of their own currency. In general, as long as the currency uses some kind of quantifiable units, it will have a good unit of account.

Lastly, security holds the lifeline for the reputation of newly created currencies. Nothing disappoints more than getting a counterfeit bill from a trusted exchange. How to make sure a currency is secure is an important question alternative currencies have to find the answer to. As the examples show, the more successful the currency is becoming, the more exposed it is to security issues. Security is less of a risk to currencies that are centrally monitored. LETS had its credit registered to the organizers with a record. Thus it was harder to counterfeit LETS credit than the Labor Notes.

**How Bitcoin Compares and Contrasts to Other Alternative Currencies**

With appropriate understanding of the alternative currencies in history, we now turn our focus back to Bitcoin, the much more recent alternative currency. Financial distress in the mainstream economy often sparkles interests in alternative currencies. In the case of LETS and Argentina Barter, both currencies gained momentum when people lost faith in the mainstream economy and their government.
The financial crisis in 2008 was one of the most severe global financial crises in history. As a result, people were looking for other currencies as an alternative and envisioning new possibilities of money.

I collected Goggle search data from Google trend and plotted the amount of interests on alternative currency over time in Figure 2 (Google 2015). This is the data on how often people use Google to search the phrase “alternative currency” and it is normalized with respect to the highest search. The month when alternative currency was searched the most is set to be one hundred percent and all other months are normalized relative to this month. This data helps us understand how the interests on alternative currency change over time. As we can see, the number of Google search on alternative currency skyrocketed as the crisis hit and slowly declined as the global economy recovered. This shows that the popularity of alternative currencies is related to the economic outlook. In the mist of the financial meltdown, Bitcoin presented an alternative outside of the government currency. It soon gained popularity.

![Goolge Search Interest on Alternative Currency](image)

Figure 2: Percentage of Google Search on Alternative Currency (Data Source: Google Trends)
While Bitcoin, like other alternative currencies, was created during a financial meltdown, it stands out like no other. All those alternative currencies we studied were limited to small-scale applications. They functioned within local communities and often revolved around local exchanges. Bitcoin on the other hand is not bounded by the geographical limitation; it facilitates transactions across borders. As a digital currency, it transcends countries and continents and is able to generate support across the globe. Figure 3 shows the presence of Bitcoin users around the world. This kind of international influence is unheard of in alternative currency history.

![Figure 3: Bitcoin’s Global Presence (Data Source: The United Nations of Bitcoins 2015)](image)

Another major distinction Bitcoin has from other alternative currencies is that Bitcoin does not have a separate marketplace. Most alternative currencies such as the Labor Note or LETS had their own exchanges. These exchanges were the only places where the currency was accepted. The separated market can be a source of major
instability. It requires quality control and market regulation. Separated from the mainstream economy, the exchange has to build a strong market structure that can compete against the organic market that developed over centuries. These exchanges often suffer from problems that mainstream market does not because their small size and inefficiency. First, the pricing for a larger market is more efficient while smaller markets have more arbitrage opportunities. Second, the quality of products for the mainstream is monitored by the government, but for the local exchanges resources are rarely devoted to make sure that the products are safe and of good quality. In the case of the Labor Note and Barter, we have seen phenomena where bad products drove out the good products, similar to the lemons market.

Bitcoin, on the other hand, does not require a separate marketplace. Most of the vendors who accept Bitcoins are businesses within the mainstream economy. They are subjected to the market regulation and quality control by the government long before the creation of Bitcoin. Many businesses accept Bitcoin as a secondary payment. This duality helps Bitcoin avoided the frauds and lemons that often exist in the separated exchanges for other alternative currencies.

Lastly, many alternative currencies struggled with security. As a currency becomes successful, it attracts frauds. Bitcoin has excellent security because it is network-encrypted, which I will further explore in Chapter Three.

Alternative currencies in history play the role of defying government’s monopoly over money and the rigid concept of what constitutes money. Different currencies construct different societies and lifestyles. These currencies speak to the possibilities of a different world and a utopia. In the case of the Argentine Barter,
alternative currency and its organizers represented a way to survive an economic breakdown when the government failed to provide for its people. Alternative currencies are continuous efforts to liberate the state monopoly of currency. Bitcoin is in line with the unceasing efforts to serve as an alternative to the state currency. While it still faces many of the same challenges, its global application and security measures make it an improvement over its predecessors.
Chapter Two: the Supply Side of Bitcoin and Mining

Bitcoin is a complex phenomenon, and the technology behind it makes it stand out from other form of currencies. In this chapter, I will provide an overview of what Bitcoin is and how it is used. This chapter will focus on the production side of Bitcoin by understanding the mining process with greater details. Mining is the channel by which new Bitcoin join circulation. It is a difficult process that costs a lot of energy and is time-consuming. Thus, when miners decide to mine, they have to do a cost-benefit analysis and determine their potential profit. In this chapter, I will construct the profit function for mining Bitcoins and understand how Bitcoin price can affect the level of mining.

Bitcoin and Bitcoin Mining

Bitcoin is a digital currency encrypted by the network; its implementation is extremely technologically involved. In order to evaluate Bitcoin’s potential to fit into the mainstream economy, we have to understand how it is created and spent. While much of the media draws parallels between Bitcoin and traditional money, what makes Bitcoin special is the way it branches out from other currencies. I will provide the building blocks to understand Bitcoin within its rightful computer science context.

We begin with how Bitcoin transactions are carried out. A hypothetical Bitcoin owner, Alice, has two sequences of numbers that compose her ownership. The first, called the private key, is a sequence of numbers that allows Alice to add a digital signature to each Bitcoin transaction she makes. Encoded with her private key, the transaction information is now public and its authenticity can be verified by the
other number sequence: Alice’s public verification key. The public key allows the rest of the Bitcoin community to verify the transactions are actually signed by Alice with her private key. The public key also serves as the wallet address for transactions. Alice needs her public key if she wishes to receive a payment from someone else. These two sequences of numbers, shown in Figure 4, are together referred to as the Bitcoin “wallet.”

![Figure 4: Private and Public Key Comparison](image)

Now let us suppose Alice wishes to spend one of her fifty Bitcoins on a large pizza from a merchant Bob. In order to make a transaction, she will have to specify three parameters for the transaction: payment amount, change, and tips for the miners who will help record this transaction. Bitcoin requires the payer to specify the amount of tips and changes they will get back at the end of each transaction, which is
different from traditional currency. In this case, Alice assigns 1 Bitcoin to Bob, 48.5 Bitcoin to herself, and 0.5 Bitcoin as a tip to miners. The tip is similar to transaction fee but it is not a fixed amount and can be decided by the users. Then, the signing process will use Alice’s private key to generate a signed transaction containing Bob’s public key, his wallet address. The signed transaction will be broadcasted to the entire Bitcoin network, in which other users can use Alice’s public key to verify the authenticity of the transaction. Once it is verified, miners will record Alice’s transaction into a Bitcoin block along with other transactions in the network. Now, Alice’s transaction is complete and Bob receives his payment.

Bitcoin miners help verify transactions and collect information on transactions to create blocks that form the blockchain. The blockchain is a collection of blocks that contains all records of every completed Bitcoin transaction since the first ever Bitcoin block was created. Blockchain is public and anyone can check the transaction of a certain wallet. It is often referred to as the public ledger of Bitcoin. Everyone using Bitcoin will use the blockchain as the reference for balance and transaction history. Blockchain distributes information across the network and keeps everyone on the same page. This is why miners are extremely important to Bitcoin.

As a result, miners are compensated for their hard work. They receive compensations from two major sources. The first source is the tips that each Bitcoin user specifies before making a transaction. The amount of tips one pays is entirely determined by the payer and there is no minimum or maximum requirement. However, it is in the payers’ interest to pay a decent tip to make sure that miners are
motivated to help record their transactions. This tip is called the transaction-based Bitcoin income for the miners.

The other source of income for miners is called coin-based income. Every time the miners finish a block they are rewarded with 25 Bitcoins. This is how new Bitcoins are added to circulation, given that there is no central bank that controls the money supply. The coin-based income is predictable and scheduled to halve every four years. Both the transaction-based and coin-based income motivate the miner to collect the records into a block and perform what is called the “proof of work” operation which is the most time-consuming aspect of Bitcoin mining.

Proof of work is a computational challenge that is designed to be demanding for the miners to solve but easy for the network to verify once it is obtained. The idea is to make mining difficult and time-consuming to ensure that the miners spend sufficient time in creating the blocks. Difficult proof of work limits the supply of Bitcoin by controlling the coin-based income. Further, it also gives Bitcoin value by making it difficult to obtain. Bitcoin aims to maintain a constant rate of coin production. In order to do so, the amount of time the network spends on producing new blocks has to be constant, which is 10 minutes per block. However, as computers become more powerful, proof of work has to adjust its own difficulty to match faster computers. The difficulty of proof of work adjusts every two weeks according to the level of mining activities to account for the variance from expected block creation rate. When the blocks are mined faster than ten minutes per block, the difficulty will go up and slow down mining. This keeps the pace of Bitcoin creation constant.
Obtaining the proof of work involves a process called hashing. Hashing, a computer science concept, refers to functions that can generate random outputs with given inputs. The result of the hashing function is called the digest. Figure 5 shows the process of hashing. Because the hashing function returns random results, it is impossible to predict the digest given the input. Thus, hashing mimics drawing a lottery; and getting a certain digest is similar to winning a lottery. Bitcoin’s proof of work requires the miner to get a digest that is below a target number. The target number can be anything form $2^0$ to $2^{256}$. As the miners cannot predict which input will return a digest that is less than the target, obtaining the correct proof of work is purely probabilistic. The smaller the target, the less likely are miners to obtain a digest that is below the target. There is an inverse relationship between the target and difficulty. When the target gets smaller, the level of difficulty rises and miners need to make more attempts to get the correct proof of work.

![Figure 5: Hashing Process Illustrated](image)
In order to find a digest below the target, miners have to try billions of inputs. The speed at which miners can attempt to find the correct digest is called the hashrate, which measures a computer’s computational power. Miners with higher hashrates can obtain the correct proof of work faster. After finding the right proof of work, miners can claim their Bitcoin reward and add one block to the network blockchain.

The Evolution of Mining

Mining has been evolving constantly. Since 2013, the price of Bitcoin has risen dramatically. Bitcoin’s high value, as a result, attracted many companies and miners to join the production process. The difficulty level of mining has therefore been increasing, and mining Bitcoin is increasingly demanding. In April 2015, mining a single Bitcoin would have taken a new Mac Pro desktop computer 269 years\(^1\).

The nature of Bitcoin mining also has changed from recreational and amateur to profit-seeking and professional. Initially, computer programmers and tech-savvy college students mined Bitcoin with their personal computers and laptops. These miners were mostly curious about the currency and wanted to find out how it worked. When interviewed about why they mined Bitcoins, some of the earlier miners commented that they wanted to be part of something new and exiting (The First Miners 2015). The early miners’ equipment was slow and inefficient. As Bitcoin acquired more popularity, mining became much more difficult and the personal computers did not have enough hashrate to compete with professional equipment that

\(^1\) Calculated with data from (“Bitcoin Mining Rate MacBook Pro.” 2015)

\(^2\) Cloud mining is a way to pool computational resources from a cluster of computers to mine Bitcoins.
were designed for mining. Application-Specific Integrated Circuits (ASICs) were soon created for the sole purpose of Bitcoin mining. ASICs lowered the energy usage of mining and increased its computational power (Morrow 2014). The creation of Bitcoin-mining ASICs marked the birth of professional mining companies and the evolution of mining from a nonprofessional hobby to a profit-seeking industry.

Mining is crucial to the health of the Bitcoin network. First of all, miners assist transactions and facilitate the circulation of Bitcoin. Without the miners devoting their computers to mine Bitcoin, no transactions can be carried out. Second, the Bitcoin network is more secure when there are more miners. The network hashrate is the sum of all miners’ hashrates. To hack the Bitcoin system, the attackers have to be able to match the network hashrate. Thus, the more miners in the network, the safer Bitcoin is. Because miners are driven by profit, it is important to understand the cost-benefit analysis for miners in order to understand the prospect of Bitcoin.

Understanding Bitcoin Mining Profit

The profitability of mining depends on many factors. Mining is highly demanding on the hardware; ASICs wear out quickly due to constant usage. Further, ASICs are expensive; their price ranges from several hundred to tens of thousands of dollars. Besides the fixed cost, electricity is a major expense. Professional Bitcoin miners have thousands of ASICs running constantly that require cooling devices; both ASICs and cooling devices are powered by electricity. Figure 6 shows a professional Bitcoin mining operation with ASICs and cooling devices. Thus, electricity enters into the profit function as a variable cost. In addition, profitability also relies on how
fast one can mine Bitcoin and the reward one gets out from each block. Finally, the price of Bitcoin affects mining profitability.

Unfortunately, Bitcoin price has high market volatility, so miners are subject to economic risks as the price swings. For example, in January 2015, the price of Bitcoin took a major hit; it dropped from $317 at the beginning of the month to the lowest $183 on January 14th (Coinmarketcap 2015). Many mining operations around the world were forced to shut down due to unprofitability caused by the plummeting price. On January 12th, a major cloud mining company CEX. IO announced it would suspend its mining operations (CEX. IO 2015). This begs the question of how miners determine their profit and how miners decide to mine or not.

Figure 6: Professional Bitcoin Mining Production (Boden 2015)

---

2 Cloud mining is a way to pool computational resources from a cluster of computers to mine Bitcoins.
I constructed a Bitcoin mining profit function in terms of difficulty, reward, energy cost, and Bitcoin price. The profit function for Bitcoin miners is summarized as the following:

$$\pi = \left( \frac{\text{hashrate}/\text{seconds in a day}}{\text{difficulty} \cdot 2^{32}} \right) \cdot \text{reward} \cdot p - e.$$ 

In this function, $\pi$ represents the daily profit for Bitcoin miners. Profit depends on the number of Bitcoins mined daily, which is a function of the level of difficulty, the hash rate per second, and reward miners get after finishing each block (Theymos 2015). The product of difficulty and $2^{32}$ is the average number of attempts a miner must make to get the correct proof of work (Theymos 2015). Hashrate is the speed at which miners can attempt to obtain the correct proof of work. The higher the hashrate the faster one can solve the proof of work and claim a block. The reward is the number of Bitcoins a miner can get after solving a block. The first term in the function calculates the average amount of Bitcoin one can get in a day times the price for Bitcoin $p$.

The cost for mining has two parts. The first part is the sunk cost for purchasing ASIC units, which is often very high and the hardware wears off overtime. The second part is the variable cost of electricity. In this analysis, we ignore the sunk costs and focus on the variable cost. Additional sunk costs and administrative costs are not included in this model; sunk cost is not included because it does not affect the marginal profit, while administrative costs are difficult to
capture because they are proprietary data. Variable $e$ is a product of watts per/hour, hours, and the price for of electricity. It is the cost of powering the ASICs.

In order to stay in business, these professional miners have to make at least zero economic profit. The following equation solves for a price level $p$, at which the miners make zero profit.

$$p = e/\left(\frac{\text{hashrate/s*seconds in a day}}{\text{difficulty}*2^{32}} \times \text{reward}\right).$$

Using this model and data on 18 of the ASICs with the highest hashrate and cost-efficiency selected from various manufactures (Minr.info 2015), I calculated the target price each unit requires to reach zero profit. As Table 1 shows, these units vary in their cost-efficiency, which results in different target prices. The target price that can support zero profit mining ranges from $149 to $2133 per Bitcoin for different units; the discrepancy is caused by the varying degree of mining efficiency. Even for the most cost-efficient unit one can purchase, a minimum price of $149 was required to stay in the market in January 2015. Facing additional administrative costs, many miners went out of business when the Bitcoin price dropped to $183 in January 2015. This result is consistent with my model, which provides the lower bound of the price required for the miners to stay in the market.
<table>
<thead>
<tr>
<th>Mining Unit</th>
<th>Gh/s</th>
<th>Price</th>
<th>Watts</th>
<th>Coin/24</th>
<th>Reward</th>
<th>Energy Cost day</th>
<th>Target Price ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monarch BPU 600 C</td>
<td>600</td>
<td>$4,680</td>
<td>350</td>
<td>0.007</td>
<td>25</td>
<td>1.092</td>
<td>149.36</td>
</tr>
<tr>
<td>Monarch BPU 300 C</td>
<td>300</td>
<td>$2,800</td>
<td>175</td>
<td>0.003</td>
<td>25</td>
<td>0.546</td>
<td>149.36</td>
</tr>
<tr>
<td>TerraMiner IV (January Batch)</td>
<td>2,000</td>
<td>$5,999</td>
<td>1200</td>
<td>0.024</td>
<td>25</td>
<td>3.744</td>
<td>153.63</td>
</tr>
<tr>
<td>TerraMiner II (January Batch)</td>
<td>1,000</td>
<td>$3,499</td>
<td>600</td>
<td>0.012</td>
<td>25</td>
<td>1.872</td>
<td>153.63</td>
</tr>
<tr>
<td>Sierra Batch 2</td>
<td>1,200</td>
<td>$7,080</td>
<td>780</td>
<td>0.014</td>
<td>25</td>
<td>2.4336</td>
<td>166.43</td>
</tr>
<tr>
<td>Neptune</td>
<td>3,000</td>
<td>$9,995</td>
<td>2100</td>
<td>0.036</td>
<td>25</td>
<td>6.552</td>
<td>179.23</td>
</tr>
<tr>
<td>CoinCraft Rig</td>
<td>2,000</td>
<td>$14,999</td>
<td>1700</td>
<td>0.022</td>
<td>25</td>
<td>5.304</td>
<td>217.64</td>
</tr>
<tr>
<td>Baby Jet Batch 1</td>
<td>400</td>
<td>$5,600</td>
<td>350</td>
<td>0.004</td>
<td>25</td>
<td>1.092</td>
<td>224.04</td>
</tr>
<tr>
<td>Jupiter November Shipping</td>
<td>400</td>
<td>$4,995</td>
<td>640</td>
<td>0.004</td>
<td>25</td>
<td>1.9968</td>
<td>409.68</td>
</tr>
<tr>
<td>Saturn November Shipping</td>
<td>200</td>
<td>$2,995</td>
<td>320</td>
<td>0.002</td>
<td>25</td>
<td>0.9984</td>
<td>409.68</td>
</tr>
<tr>
<td>CoinCraft Desk</td>
<td>1,000</td>
<td>$7,099</td>
<td>1875</td>
<td>0.012</td>
<td>25</td>
<td>5.85</td>
<td>480.09</td>
</tr>
<tr>
<td>BitForce 500 GH/s Mini Rig SC</td>
<td>500</td>
<td>$22,484</td>
<td>3000</td>
<td>0.006</td>
<td>25</td>
<td>9.36</td>
<td>1536.30</td>
</tr>
<tr>
<td>BitForce 25 GH/s SC</td>
<td>25</td>
<td>$1,249</td>
<td>150</td>
<td>0.0003</td>
<td>25</td>
<td>0.468</td>
<td>1536.30</td>
</tr>
<tr>
<td>BitForce 50 GH/s Miner</td>
<td>50</td>
<td>$2,499</td>
<td>300</td>
<td>0.0006</td>
<td>25</td>
<td>0.936</td>
<td>1536.30</td>
</tr>
<tr>
<td>BitForce 5 GH/s SC</td>
<td>5</td>
<td>$274</td>
<td>30</td>
<td>6.093E-05</td>
<td>25</td>
<td>0.0936</td>
<td>1536.30</td>
</tr>
<tr>
<td>Block Erupter Blade</td>
<td>10</td>
<td>$4</td>
<td>75</td>
<td>0.0001</td>
<td>25</td>
<td>0.234</td>
<td>1920.37</td>
</tr>
<tr>
<td>Block Erupter USB</td>
<td>0.3</td>
<td>$25</td>
<td>2.5</td>
<td>3.656E-06</td>
<td>25</td>
<td>0.0078</td>
<td>2133.75</td>
</tr>
</tbody>
</table>

Table 1: Target Price for Various ASIC Units
Even during the price drop in January 2015, the price of Bitcoin was still above the lower bound of the target price. For many efficient mining operations, the price sway was not detrimental. However, if Bitcoin continues its downward price trend, the associated negative effect on profitability will force many miners out of business.

To complicate the mining decision, Bitcoin reward does not stay constant. In 2015, finishing one block rewards the miners 25 Bitcoins. However, this number is programmed to halve every four years. The next halving will happen on July 20\textsuperscript{th} 2016. By then, each block will only reward 12.5 Bitcoins. If we hold other factors constant, halving the reward will require the price of Bitcoin to double in order to keep the current miners in business: a minimum of $298 per Bitcoin will be necessary while the price for Bitcoin on April 9\textsuperscript{th} is $240 (Coinmarketcap 2015).

To visualize the relationship between target prices and Bitcoin price, I made a chart of the target price for Bitcoin mining for the current reward and the next reward in Figure 7. Although the price level is now above the current target price, it is below the required target price when halving happens next year.
Bitcoin reward halving is a supply shock. By lowering the payoff for mining, halving will push some miners out of business. Additionally, the lowered supply should push up price.

We can understand the dynamics by looking at the first ever halving in Bitcoin history. The Bitcoin reward was most recently halved in November 2012. In Figure 8, I plotted Bitcoin price and network hashrate that serves as a proxy of amount of miners, because a large number of miners is associated with a large network hashrate. The green vertical line indicates the occurrence of halving. Figure 8 shows that, following halving, the hashrate decreased. This decrease in hashrate was a result of some miners gone out of business. At the same time, Bitcoin price went up; the lowered supply accounted for the price increase.
The upward pressure on price will elevate some miners from bankruptcy. Additionally, when the network hashrate declines, difficulty will adjust downward, increasing the profitability of mining. As long as there is a sufficient demand for Bitcoin, the effect of halving should not be detrimental.

Yet the prospect for miners is not optimistic. The price volatility of Bitcoin is too high for the miners to be able to predict revenue accurately. Moreover, the price of Bitcoin is currently approaching the target price. The success of Bitcoin will ultimately depend on a reasonable price level that can sustain the amount of miners and the security miners provide.

In this chapter, we have explored the technical details of Bitcoin that make it stand out from previous alternative currencies. We further developed the tools to understand Bitcoin mining and the economic conditions that enable mining. Bitcoin mining has gone from a recreational hobby to a professional business. The economic
return of mining can be lucrative, but the risk of mining is also high. Additionally, the halving of Bitcoin reward can decrease the number of miners and drive up its price. The future of mining heavily relies on the demand for Bitcoin. Bitcoin can be used as a medium of exchange; it can also be used as a financial instrument. Bitcoin’s functionality and popularity influences the price, and then indirectly mining. In the next chapter, I will look at the demand side of Bitcoin by analyzing who are using Bitcoins and why they choose to use it.

Chapter Three: Bitcoin As a Currency and Investment

We have already explored the production side of Bitcoin and constructed the profit model for Bitcoin mining. While mining activities are crucial to the Bitcoin system, a high level of mining must be supported by a high target price. Further, with a predictable level of supply, the price level of Bitcoins is determined by demand. For traditional currencies issued by governments, the natural users are government subjects; almost all governments require their citizens to pay taxes in their own currencies and legislate the government currency as the legal tender. A currency issued by the government does not have to be competitive to acquire user base. However, using Bitcoin is a conscious choice, not a result of coercion. People use Bitcoin because they believe in what it stands for or think it is more convenient than traditional currencies.
There is a cost to start using Bitcoin. Adopting Bitcoin requires individuals to first understand how Bitcoin is used in everyday transactions. The owners have to download related software and create digital wallets. For businesses, setting price and reporting taxes can often be challenging. So for all Bitcoin users, switching to a Bitcoin dual payment system requires the users to overcome some initial adjustment and some serious research. What, then, encourages individuals’ and businesses’ entry into the Bitcoin network?

In this chapter, I move forward in my exploration of Bitcoin to its demand side. This chapter will first profile Bitcoin users. Bitcoin transactions can be anonymous. As a result of the anonymity, the demographics of Bitcoin users are poorly documented. Bitcoin has gained some reputation as the accomplice to the underground economy, partly due to the existence of websites such as the Silkroad, which provides illicit goods in exchange of Bitcoins. This left me wondering who these Bitcoin users are and what they actually use their Bitcoins for.

This chapter will also examine Bitcoin through the lens of the economic definition of money, whose characteristics include store of value, medium of exchange, and unit of account. However, these three standards do not in fact cover all the requirements for a successful currency. The forth criterion I add here is proof of security and I argue that it is extremely important to the vitality of the currency but is often assumed away because of the monotonicity of our currencies. Security is overlooked because almost all the currencies we use today are issued and protected by the government. However government-issued currency is only a subset of the
currency world and security is crucial to the success of an alternative currency, as we have seen in Chapter One.

Lastly, after examining Bitcoin’s functionality as a currency, I will analyze the use of Bitcoin as an investment. For example, Bitcoin can serve as a financial instrument that can diversify one’s portfolio due to its low correlation with other financial assets.

**Who Are the Invisible Average Bitcoin Users**

Unlike traditional online payment systems, Bitcoin does not require identity verification or personal information from the users, so one can remain anonymous when conducting a transaction. Bitcoin transactions can stay anonymous if the users are careful not to link their public keys to their identities. The users can also use an external mixing service to help reduce the risk of identification. The mixing service collects Bitcoin from multiple users and redistributes them to new wallets. One owner’s identity might be known before the mixing service, but after the mixing the new wallets are no longer associated with their owners in any predictable fashion. If careful, Bitcoin users can remain anonymous in their transactions, which no other online credit service can guarantee.

Figure 9 demonstrates how privacy is secured from being accessed by the public in two different models. In the traditional model, the users have to prove their identities first to the third party. The third party collects identity information and
keeps it private. For example, buying a product from eBay belongs to this category. The users have to prove their identities to eBay, but the public cannot access their order details. On the other hand, the Bitcoin model does not require any identification and all the transaction information is public. As long as one can provide the private key, one can make transactions without associating his or her identity to the private key. Nakamoto argued that this is similar to the stock exchange model where the size and time of transactions are announced but not the identities is associated with their buyers and sellers (2008, 6). Yet, in the stock exchange model the broker and the exchange are still aware of the identities of the buyers and sellers, while Bitcoin wallets do not need to have any association with their users. The Bitcoin privacy model allows the users to preserve their anonymity while still allowing transaction information to be available to the entire network.

![Diagram of Traditional and New Privacy Models](image)

**Figure 9: Comparison of Traditional and New Privacy Model (Nakamoto 2008, 6)**

However, some Bitcoin users take advantage of their anonymity to purchase illegal goods. The most famous example of such usage is the online black market,
Silk Road. Silk Road utilizes a technology, Tor hidden services, to hide users’ traffic. When the FBI shut down this online market in 2013, it seized 26,000 Bitcoins from the site owners and its users. The FBI later auctioned the Bitcoins to the public, but Silk Road’s buyers were not prosecuted (Hern 2013). Since Silk Road, many people believe that Bitcoin is mainly used for purchasing illicit goods online. Indeed, the media loves stories that relate to Bitcoin. Unfortunately, headlines such as “Cyber-money such as Bitcoin ‘makes crime easier’” (Martin 2015) and “Hackers use Cryptoware Against Police for Bitcoin Ransom” (Smart 2015) has led many to believe most Bitcoin users to be drug addicts or criminals.

However, according to an anonymous survey conducted by SIMULACRUM (Lui 2013) of over 1000 Bitcoin users, most Bitcoin users are neither criminals nor drug addicts. According to the survey, the average Bitcoin user is 32 years old; 95 percent of the users are male. Contrary to the belief that Bitcoin is used mostly in illegal activities, only 11 percent of the respondents reported using Bitcoins to purchase drugs and only 5 of respondents reported using Bitcoin for other illegal goods. The highest portion of usage is for gift/donation, at 55 percent. In fact, the gift and donation tradition of Bitcoin started early when the currency was worth very little. People used it to tip content creators on the Internet and support charities. One famous example was when users of Dogecoin, a less influential cryptocurrency, donated coins to send the Jamaican bobsled team to the Sochi Winter Olympics (Chappell 2015). Table 2 shows how the respondents used their Bitcoins.

<table>
<thead>
<tr>
<th>Usage</th>
<th>Number of Respondents</th>
<th>Percentage</th>
</tr>
</thead>
</table>

57
<table>
<thead>
<tr>
<th>Category</th>
<th>Usage</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Services</td>
<td>156</td>
<td>38</td>
</tr>
<tr>
<td>Computer Hardware</td>
<td>106</td>
<td>26</td>
</tr>
<tr>
<td>Other Legal Goods</td>
<td>190</td>
<td>47</td>
</tr>
<tr>
<td>Narcotics</td>
<td>46</td>
<td>11</td>
</tr>
<tr>
<td>Other Illegal Goods</td>
<td>20</td>
<td>5</td>
</tr>
<tr>
<td>Gambling Services</td>
<td>141</td>
<td>35</td>
</tr>
<tr>
<td>Gifts and Donation</td>
<td>223</td>
<td>55</td>
</tr>
</tbody>
</table>

Table 2: (Data Source: Lui 2013)

*People can select more than one usages thus the percentage does not add up to 100.

In additional, 36.7 percent of the Bitcoin users do not drink, smoke, or take drugs at all. To put this number in context, according to Weswell at Wesleyan University, 34.2 percent of Wesleyan students reported never using Marijuana, a number that is lower than the substance free population of Bitcoin users. This survey provides evidence on the demographics of Bitcoin users and showed that Bitcoin while can be used for illegal transactions, illegal transaction is not the dominant use of Bitcoin.

Bitcoin users’ demographics directly affect its prospects. If Bitcoin’s main usage is to purchase drugs, it is hard to imagine that Bitcoin will gain support from governments. Further, increasing regulation of the currency will make Bitcoin unappealing to people who use Bitcoin for illegal transactions. Yet, Bitcoin’s users are mostly young professionals and students and more than half of the transactions are over computer services. Moreover, the Bitcoin users base coincide with many technology firms’ target audience, which will be discussed later. This kind of user base can enable Bitcoin to integrate into the mainstream economy. It should also be
noted that there is a lack of female supporters in the Bitcoin demographics given that only 5 percent of Bitcoin users are women.

Besides the technocratic supporters, Libertarians also support Bitcoin and believe that Bitcoin embodies the spirit of their ideology. In the survey above, 30 percent of the respondents identify as libertarian. This is a large percentage considering that only 7 percent of the American population is consistent libertarians and another 15 percent can relate to its principle (Blake 2013).

Libertarians favor Bitcoin for three major reasons. First, the government cannot monitor Bitcoin transactions. Because the users of Bitcoin can stay anonymous when making a payment, a Bitcoin transaction is discrete. Staying away from government monitoring is appealing. Second, in his paper on a competitive framework of currencies, *Choice in Currency*, F.A. Hayek argued that the government has incentives to fund its own activities by flooding the market with newly minted currencies (1976). The oversupply of money creates unnecessary inflation. Contrary to that of traditional currencies, the Bitcoin algorithm adjusts its difficulty to keep Bitcoin supply increasing at a predictable rate. The algorithm that controls money supply removes the influence of arbitrary decisions. At the same time, the predetermined Bitcoin supply trajectory means that monetary policies are not available to Bitcoin. While for libertarians, the absence of monetary intervention is attractive; this might worry some believers of Keynesian economics. However, this would only be an issue if Bitcoin became the only currency. In addition, updating the Bitcoin protocol or creating a new cryptocurrencies that allow for monetary interventions is entirely possible.
Lastly, Bitcoin is consistent with the libertarian tenets because Bitcoin is an open source currency. Open source means that a code or algorithm is not patented, and anyone can use it for any lawful purpose. Since the creation of Bitcoin, its code has been open to the public. In fact, anyone can start a new cryptocurrency with the Bitcoin code. The implication of open source is that neither government nor Bitcoin has a monopoly over cryptocurrencies. Bitcoin provides an easy and safe way to create new currencies, which broke the governments’ monopoly over money and unlocked possibilities for innovation of currencies.

But in reality, Bitcoin’s independence from the government is limited. As I discussed in Chapter One, unlike LETS or the Labor Notes, Bitcoin does not have its own market. The absence of a private market is beneficial in that there is no need for Bitcoin to devote resources for market regulation as well as product quality control, because the government already regulates the businesses that adopt Bitcoins. However, this is the reason why Bitcoin is not independent from the government regardless of its libertarian appeal. Without the government providing quality control on the product in the market, Bitcoin will have the same problems that plagued other alternative currency exchanges: a lemons market in which bad products dominate and good products are driven out. The lemons market lowers people’s trust in a currency and disrupts the balance of supply and demand for higher quality goods. Thus, even though Bitcoin broke the monopoly of currency, it is still highly dependent on the other functions of the government. While it is possible to envision a world in which Bitcoin facilitates its own market and pays for its own infrastructure, in its current state Bitcoin cannot fully function without the government.
Now that I have examined the demographics of Bitcoin users, I turn to understanding what motivates these supporters to use Bitcoin. This question has to be answered from both consumers and merchants’ perspectives. The questions are whether Bitcoin is a good currency for the users, and whether the merchants benefit from adopting Bitcoins.

**Bitcoin’s Functionality As a Currency**

Bitcoin’s creator Satoshi Nakamoto defined it as “a purely peer-to-peer version of electronic cash” (2008, 1). In other words, Bitcoin is an electronic currency. From the economic point of view, currency is defined to function as a medium of exchange, store of value, and unit of account. Yet, these three criteria are not sufficient for a successful currency. From studying the alternative currencies in history, I realized that many of the currencies such as the Labor Note or LETS faced severe fraud problems. When these alternative currencies became successful, fake exchanges sprouted out to take advantage of their popularity with counterfeit credits. Fraud lowers a currency’s credibility. While counterfeit currency is an issue for government issued currency, the government’s ability to protect the integrity of its currency gives security to conventional money. Because the governments insure most of the currencies we use today, security of a currency is sometime assumed away. However, most alternative currencies do not enjoy this luxury and security is a serious problem the organizers have to solve. Consequently, I argue that for a currency to be fully functioning, it has to provide a good store of value, unit of account, medium of exchange, and proof of security.
Store of value

A currency’s value should be preserved for later use; the value of a currency should not fluctuate widely. For traditional currencies, the value is maintained by the central banks, which control inflation with consideration of the level of unemployment. Central banks can reduce inflation by lowering the money supply. In a deflationary environment, the central bank can increase the money supply to devalue its currency.

In contrast, Bitcoin does not have a central bank and its value fluctuates widely. I plotted Figure 10 to illustrate the absolute value of daily fluctuation in the prices of Bitcoin, the British Pound, and the Chinese Yuan in dollars from August 2010 to February 2015. As we can see, Bitcoin has a significantly higher fluctuation in price compared to other currencies. During the course of the most volatile day, the value of Bitcoin changed 45 percent. On average, Bitcoin’s value changes 3.6 percent a day while the Yuan has a 0.06 percent average daily fluctuation and the Pound has a 0.2 percent average daily change.
Bitcoin’s price fluctuation is extremely volatile compared to other government-issued currency. To provide a sufficient context, I calculated the daily fluctuation of the Standard and Poor 500 equity index for the same period, from 2010 to 2014. The S&P’s average movement per day is 0.66 percent which is only one sixth of Bitcoin’s price fluctuation. This instability of price shows that Bitcoin is a poor store of value, at least in the short run.

Being a poor store of value can deter a currency’s use. For risk-averse consumers, the large price fluctuation of Bitcoin is a potential source of loss and less preferable compared to currencies that are more stable such as the USD. Thus, price instability will be one of the major obstacles for Bitcoin to becoming a mainstream currency with widespread appeal to the public.

**Unit of account**

---

Figure 10: Bitcoin Price Fluctuation (Data Source: Thomas 2015)
The definition of unit of account includes, dividable, verifiable, and fungible. Bitcoin is divisible to eight digits after the decimal point. Bitcoin’s transaction is also verifiable because each transaction is recorded in the blockchain and available to all interested parties. The interesting question is whether Bitcoin is fungible, and further, whether any currency is truly fungible.

Bitcoin is fungible if one Bitcoin is interchangeable with another Bitcoin. All Bitcoin are represented in the same way in the Bitcoin protocol; there is no difference between your Bitcoin and my Bitcoin. Therefore, Bitcoin should be fungible. However, the complication comes in when we consider taxation on Bitcoin. IRS decided in March 2014 to define Bitcoin as a taxable property and introduced complications to Bitcoin fungibility. In his article “Why Bitcoin Can No Longer Work as a Virtual Currency,” Robinson Meyer argues that Bitcoin is no longer fungible and cannot function as a currency (2014). When one’s profit from holding Bitcoin is realized in any transaction, the owner’s gain is taxed. Thus, Meyer argues that the Bitcoin acquired at $10 and the Bitcoin acquired at $50 are different because each is subject to different taxation.

However, I argue that Meyer is incorrect, and Bitcoin can still be considered fungible, despite its status as a taxable property. First, this IRS policy implies that Bitcoin is only not fungible for people who hold Bitcoin for a period of time. However, at each point in time, all Bitcoin payments are in fact interchangeable because there is no price difference between Bitcoins. Thus, they are all taxed in the same way because they are acquired at the same price. This means that if one uses services offered by Coindesk that help convert Bitcoin to another currency in real
time, any Bitcoin payments at each point in time are interchangeable. Second, the only reason that Bitcoin is not fungible for the holders in the U.S. is because of the IRS’s definition of Bitcoin as a taxable property; Bitcoin is intrinsically fungible. For users outside of the U.S., Bitcoin is still as interchangeable as cash or any type of credits.

Absolute fungibility is not required for currencies; there are many functioning currencies that are not fungible. For example, gold coins are not fungible. The purity of gold varies and the degree of wear is also different. One gold coin is never truly interchangeable to another. But gold coin can serve as a currency. Government-issued currencies are not fungible under certain circumstances. For example, a currency trader can profit from holding JPY, but his or her gains will be taxed when this trader converts his or her JPY holding back to USD. It is obvious in this case JPY faces the same problem as Bitcoin does in terms of fungibility, because taxation depends on the magnitude of the capital gain. Lastly, even credits are not always fungible. The obvious counterexample would be money laundering. The reasoning behind money laundering is exactly that the source of the money matters, which is in fact the opposite of fungibility.

Consequently, while the IRS definition of Bitcoin limits its fungibility, it does not significantly affect Bitcoin’s prospect as a currency. Admittedly, it complicates users’ tax reporting but, as we have seen, many currencies are not fungible under certain circumstances. It unconvincing to argue that Bitcoin’s limited fungibility will prevent it from becoming a major currency.
**Proof of Security**

The security of Bitcoin is ensured by both cryptographic technology and an incentive structure that discourages cheating. Before Bitcoin, the idea of a decentralized digital currency never came to fruition. The biggest challenge was the prevention of double spending. Double spending is when the same digital currency is spent twice. For example, a user, Alice, just bought an ASIC miner with one Bitcoin. If she then used the same Bitcoin to buy another ASIC miner, she double spent that Bitcoin. Bitcoin solves this problem by maintaining the network blockchain, the records of all Bitcoin circulation.

To avoid ambiguity, the Bitcoin network only accepts the longest blockchain as a reference for transactions and accounting information. Any computer can start connecting blocks together to make an alternative blockchain. The chains that depart from the legitimate blockchain are called alternative chains. These alternative chains create confusion for the public in terms of which blockchain to trust. For example, in Figure 11, there are three blockchains in the picture. Let us assume that block 8, block 7, and block 3 contains conflicting information regarding one user’s account balance. In this case, the miners and users need to decide which one to believe; they cannot all be correct. The Bitcoin protocol dictates that only the longest blockchain will be accepted as the legitimate chain. This protocol helps everyone to stay on the same page. The reasoning is that the longest chain must have the most miners working on it; thus it is more likely to be an honest chain than alternative chains created by attackers. Additionally, the longest chain contains more blocks and more transaction information.
In order to attack the Bitcoin network, a hacker, Charlie, has to change the information in the blockchain. For instance, presume that Charlie wants to double-spend his Bitcoins. After the transaction is confirmed and accepted by the network, his Bitcoins are already sent to the merchants. In order to spend the same Bitcoins again, this hacker has to change the transaction history starting with when he spent his Bitcoins. The attacker has to start creating an alternative chain that does not contain the record of his payment to the merchant.

As we know, the network only accepts the longest chain. If the attacker Charlie wants to revise the transaction history, he has to make sure that the length of the alternative chain is longer than the network blockchain. If that is achieved, the attacker can successfully alter the record of his Bitcoins and get them back.

I will use Figure 11 again to illustrate the hacking process. Let us assume that Charlie bought a car with 100 Bitcoins in time period two. The merchant will deliver the car once Charlie’s payment is confirmed. Charlie’s transaction is recorded in block 2. In order to revise the transaction history, Charlie has to create a fake block, block 4, that does not contain the transaction between himself and the merchant. Now
there is an alternative blockchain. However, in order for the network to accept his revision, Charlie has to make sure that his chain is the longest.

Now the only obstacle between the attacker and double spending his previous Bitcoins is to create an alternative chain longer than the original chain. To creating the alternative chain, the attacker has to add blocks to the chain, like any other miner. The creation of blocks requires proof of work. However, as demonstrated in Chapter Two, obtaining the correct proof of work is very difficult, time-consuming, and demanding on the hardware. Thus, in order to create the alternative blockchain the attacker needs to be able to obtain the proof of work quickly.

How fast does the hacker need to solve the proof of work in order to fool the system by making the longest blockchain? At least as fast as the entirety of the Bitcoin network, excluding the hacker himself. While the attacker solves the proof of work and creates new blocks, the rest of the network is also doing the same. Thus, the attacker is actually racing against the sum of honest miners in creating blocks and to achieve the longest chain. The only difference between them is that the honest miners do not revise the transaction history in any particular way but the attacker tries to get back the coins he just spent.

It is very difficult for the attacker to win this race, because he is racing against the computational power of the entire network. Additionally, the attacker Charlie has another disadvantage. Because the attacker aims to revise his transaction history, he has to first recreate the block in which his previous transactions are recorded, before he creates the alternative blockchain. This means that the attacker has at least one more block to create compared to the rest of the network. Outpacing the network is
practically impossible, unless the number of miners and thus its computational power drop drastically.

Satoshi Nakamoto characterized the probability that an attacker ever catching up to the honest miners and achieving the longest blockchain by a Binomial Random Walk that is also known as a Gambler’s Ruin problem (2008, 6). He names the chance the attacker will get a block before the network can as \( q \), while \( p \) stands for the probability that the network finds the next block. Variables \( q \) and \( p \) are determined by the relative computational power of the attacker and the rest of the network. Because obtaining the correct proof of work is a probabilistic event, if one has a higher hashrate, computational power, there is a higher chance that miner will capture the next block. Variable \( q_z \) denotes the probability that the attacker can ever catch up from \( z \) blocks behind.

The conditional probability \( q_z = P(\text{attacker can ever catch up} \mid \text{attacker is z blocks behind}) \) is represented by:

\[
q_z = \begin{cases} 
1, & p \leq q \\
\left(\frac{q}{p}\right)^z, & p > q
\end{cases}
\]

I calculated the probabilities of the attacker ever catching up given various \( q \) values and plotted the probabilities in Figure 12. The Y-axis is the probability and the X-axis is the value for \( z \), number of blocks the attacker needs to catch up with. As we can see the probability drops exponentially as \( z \) gets larger for each level of \( q \). Every time the attacker fails to capture one block \( z \) increases by one. A larger \( z \) is associated with a lower probability that the attacker can ever catch to the honest miners. Moreover, the probability the attacker can capture the next block \( q \) directly influences the probability of catching up. As \( q \) approaches to 0.5, the chance of catching up
increases. When $q$ is 0.5, the probability is one. This means that when the attacker controls 50 percent of the computational power in the entire network, he or she can successfully attack the network.

![Probability of Attacker Catching Up](image)

**Figure 12: Probabilities of Attacker Catching Up to the Network**

In reality, control of even 10 percent of the computational power by any individual is extremely difficult. Figure 13 shows that the network hashrate of Bitcoin is at an all-time high which means that there are a large number of miners with large computational power. This then guarantees a safe Bitcoin network. Thus, as long as the network has a sufficient amount of honest miners and strong computational power, attacking Bitcoin is extremely difficult.
Moreover, attacks on the Bitcoin network can only take the form of revising previous transactions. The network will not allow for creation of Bitcoins from thin air by the attackers, because each Bitcoin is documented in the blockchain. Adding Bitcoins that did not previously exist is impossible and completely preventable.

Hacking the Bitcoin system requires an incredible amount of computational power that is practically impossible to gather. Even if someone controlled that amount of computational power, it does not mean that the system will be hacked. Hacking has high opportunity cost. Hacking takes away the computational power that one could have devoted to mining Bitcoins instead. If the hacker really has the power to outpace the entire network, it makes more sense for them use that power to mine Bitcoins; this means that the hacker could receive 25 Bitcoins every 10 minutes by mining, instead of revising some preciously spent coins. According to Nakamoto, the attackers “ought to find it more profitable to play by the rules, such rules that favor him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth” (2008, 4).
While hacking Bitcoin is nearly impossible, there are other ways that Bitcoins might be stolen, especially on the users’ end. Bitcoins can be stolen from the users when they leak their private keys or simply lost their keys. This is different from the security of the Bitcoin network. I define this kind of security as the “user end security”. Because Bitcoin is decentralized, when one loses the address of their wallet or their private keys, they will not be able to ask a third party to get the wallet back. There is no “forgot your password” service for Bitcoin and this is why many people make both physical and electronic copies of their wallets. If the Bitcoin users accidentally leaked information on their private keys, they will also lose their Bitcoins. For example, in 2013, a Japanese Bitcoin exchange Mt. Gox allegedly lost around 700,000 Bitcoins because the database containing private keys for their customers’ accounts was infiltrated. Bitcoin plummeted when the news of this hacking broke out. However, this type of hacking is preventable. The management of Mt. Gox was not responsible and its security measure in the company was not impressive. The chief executive of the exchange remarked “we had some cases where a stranger sneaked in and took things away. We also have at least one former employee stealing the company’s data” (Brustein 2014). These mistakes are avoidable and will improve as more responsible Bitcoin startups such as Coinbase emerge. Vitalik Buterin, writer at the Bitcoin Magazine, argued that there will be an “changing of the guard” moment for Bitcoin when more responsible Bitcoin enterprises dominate the Bitcoin market and badly managed business will die out (2014).
Additionally, the Bitcoin system is becoming safer with the new multiple signature technology. At the Inside Bitcoin Berlin conference in March 2015, I was introduced to multisig (multiple signatures). Many experts emphasized how this technology could largely improve Bitcoin security even more. The Bitcoin system in 2015 only allows one private key for each wallet. This uniqueness of the private key increases the likelihood of losing the wallet and theft. The multisig system developed by CryptoCorp allows people to use multiple private keys to sign transactions (Buterin 2014). For example, a 3-5 multisig wallet allows for five private keys. In order to validate the transactions, the owner has to sign it with at least three out of the five keys instead of one key in the original Bitcoin system. The owners can choose where to store their keys and often they can be stored in different medias. For example, one can be stored in a PC, one on a server, and one on a mobile phone. This means that now hackers cannot steal Bitcoins with a single private key. Instead, they need to hack into multiple mediums and steal several keys, which is much more difficult. If Mt.Gox had used multisig and only kept one private key from each of their costumers, the hacking would not have occurred. Multisig will strengthen the weakness of Bitcoin’s user end security and substantially increase the security of the entire system.

Medium of exchange

From a currency user’s perspective, one major concern is what one can purchase with Bitcoin. This all depends on whether businesses accept Bitcoins as a form of payment. On Aprile 10th, there are 6,439 businesses around the global that
accept Bitcoin (OpenStreetMap 2014). This is not an impressive number. However, if Bitcoin is able to attract more businesses to adopt it, this medium of exchange will improve. In this section we will look at which businesses already accept Bitcoin and whether Bitcoin will be able to attract more businesses to adopt it in the future.

In 2011, a programmer bought two large pizzas with Bitcoins and felt very proud to share the news with the entire Internet. Today, there are many businesses beyond pizzeria that accept Bitcoins. Many of them are major and well-known companies. Online retailers such as Overstock.com started to accept Bitcoin in January 2013. The famous blog platform Wordpress also accepts Bitcoin as a form of payment. Tesla accepts Bitcoin as a payment for their electricity-powered cars. In January 2015, eBay and PayPal announced that they are considering Bitcoin adoption and are waiting for regulatory clearance (Kar 2014). Many major corporations are considering how Bitcoin can fit into their business models and their acceptance can help push Bitcoin forward as a currency.

Bitcoin brings free publicity to big corporations. According to Nicholas Colas, chief market strategist at ConvergEx, “One thing that people haven't focused on with Bitcoin is that its users are a very attractive advertising demographic” (Brennan 2014). He pointed out that the average user is a “tech-savvy male, 25 to 40, with above-average income, commonly residing on one of the U.S. coasts” (Brennan 2014). Bitcoin’s demographics coincide with many technology firms’ target customers, who are young and passionate about technology. The publicity brought by Bitcoin adoption is positive to the company and a good medium of reaching their desired audience. As a result, Bitcoin adoption brings in new revenue. Gyft, an app that
allows users to send gift cards through their phones, welcomed millions of dollars of sales in Bitcoin after the first six months of accepting Bitcoins (Brennan 2014). Bitcoin adoption brings tangible benefits to major businesses both in terms of both publicity and new cash flow.

At the same time, small businesses may also benefit from accepting Bitcoin as part of their payment system. Adopting Bitcoin puts many small businesses on the map quite literally. Coinmap is a website that tracks businesses around the global that take Bitcoin as a form of payment. One can use Coinmap to find a local business near them to use their Bitcoins. The publicity of accepting Bitcoin brings new clients to the business. Robert Hohne is the owner of a general store in New Orleans called Homestead, whose store appears in the following Coinmap screenshot in Figure 14. He mentioned: “we’ve been fortunate to have met some great customers who only found us because we accept Bitcoin, and have also sparked the interest of customers who come in and ask us what this Bitcoin phenomenon is all about” (Renolds 2014). The early adaptation to Bitcoin can help small businesses attract new customers by offering free and substantial publicity.
Bitcoin adaptation brings more lasting benefits to small businesses than temporary fame. Using Bitcoin as a payment system can help business owners save transaction fees and time. Bitcoin transaction has the low transaction fee because miners are incentivized through both coin-based income and transaction based income, one from tips given by Bitcoin users and the other from the Bitcoin received after finishing each block. As a result, Bitcoin transactions cost very little or nothing at all. Compared to the credit card process fee that normally is around 2 percent, Bitcoin charges less than 1 percent. To small businesses that rely on every penny to stay put, Bitcoin adoption increases their bottom lines. Additionally, Bitcoin transaction is essentially both safe and nonreversible (Nakamoto 2008, 1). Once the coin is spent the information is locked in the block and cannot be changed. Credit card fraud often resulted in a credit card charge back and the fee falls on the merchants. Secure and nonreversible payment from Bitcoin can help merchants save
fees that are charged for credit card chargeback, which can cost five to 15 dollars per order.

A Bitcoin payment has a faster turnover than a traditional credit card payment. Credit card payment can take weeks for the banks to process. The slow process is a problem for small businesses in particular, which need every dollar to survive. For a merchant using Coinbase wallets to process payment in Bitcoin, it normally only takes one to two days to get paid (Shandrow 2014).

With the help of Bitcoin, merchants can also reach the international costumers, who previously were too expensive to serve due to the international transaction fee in addition currency conversion. According to the director of business development and strategy at Coinbase Adam White, now with Bitcoin small businesses can accept payment across the oceans at the speed of an email (Shandrow 2014). This accessibility will help merchants enlarge its market and further connect to the global market.

**Disadvantages of Adopting Bitcoins**

However, adoption of Bitcoins also has its disadvantages. Bitcoin price is often volatile, as demonstrated earlier in this chapter. For the merchants, receiving Bitcoin as a payment can be risky. The Bitcoin payment can drop sharply in value in the matter of days. Risk could thwart small businesses from adopting Bitcoins.

The solution to this problem is offered by Coinbase wallet, which provides a service to businesses that allows them to convert the Bitcoins they receive instantly to the currency of their choice at spot exchange rate (Coinbase 2015). This will mediate the currency risk of accepting Bitcoin. Yet, this means that merchants will have to
adjust the price for their products according to the Bitcoin price movement. Dynamic pricing is required, which could be troublesome for small business to set up.

The biggest disadvantage of adopting Bitcoin is the regulatory uncertainty. IRS treats Bitcoin as a property and the loss and gain from holding Bitcoin has to be reported to the IRS. In order to report it, the business has to keep track of the buying price and the selling price, which can be complicated and time-consuming. Additionally, the regulation of Bitcoin related businesses is not mature yet. In the case of the United States, the federal government and the state governments have different concerns. The federal government’s priority is to prevent money laundering. The state governments aim to protect the consumers. Each state has its own regulation and most of them do not have a clear policy. Coping with the developing policy is intimidating and often confusing for merchants. This uncertainty definitely prevents people from accepting Bitcoins in their shops.

However, the overarching outlook for Bitcoin is very positive. As more and more people will understand what Bitcoin is and how it works, it may gain more popularity. From the merchants’ perspective, the cost saved by adopting Bitcoin is attractive and the free publicity is also a nice addition. The main concern is regulation that is clarifying more and more as the regulators understand the benefits of adopting Bitcoins. Figure 15 is a screenshot of Coinmap of the continental United States. I believe that as the regulation becomes clearer we will see more businesses adopting Bitcoins to save money and time.
As a currency, Bitcoin is still immature but has potential to improve. It has good security as a form of money. The algorithm of Bitcoin makes hacking it technically impossible from the network’s perspective. The user-end security will improve over time as Bitcoin moves away from its initial trial and error phase. More responsible and mature companies are emerging to provide solutions to user end security. In addition, Bitcoin offers low transaction cost and positive publicity that can help businesses gain new revenue. Thus, as time moves forward, we will see more and more merchants start accepting Bitcoin.

On the negative side, Bitcoin’s store of value is unsatisfactory. It has very high volatility, which makes it very unattractive as a currency option. Additionally, regulation regarding Bitcoin related business is not clear and confusing. In order for
Bitcoin to become a mainstream currency, it has to be able to overcome its bad store of value and regulatory uncertainty.

**Bitcoin As an Investment**

Besides being used as a currency, Bitcoin also serves as a financial instrument for profit-seeking investors. Bitcoin’s price skyrocketed in 2013, at which time more and more people thought that Bitcoin investment could be a great way to reap a large amount of return in a short period of time. At the same time, the risk of such an investment is also very high. In this section, I examine the potential of Bitcoin as an investment. First I will explore the correlations between Bitcoin and other investment assets, such as stocks, commodity, and foreign exchange. Second, I will analyze the nature of Bitcoin as an investment and how it can help improve one’s portfolio.

Bitcoin as an investment has interesting properties. The Bitcoin price does not have strong correlations with other financial instruments. In order to understand how the changes in other assets can influence Bitcoin price, I first ran pairwise correlations between Bitcoin price and daily gold price, exchange rate from GBP to USD, JPY to USD, AUD to USD, CNY to USD, value of the S&P 500 index, and the value of NIKKEI Japanese equity index, WTI spot price, and U.S. ten year treasury bond yield.
The results in Table 3 show that Bitcoin has pretty strong covariance with most other investment assets. However, pairwise correlations are not sufficient to show that there are actual correlations between Bitcoin price and other assets, because these variables could have similar data generating process that is not taken into account by the simple correlation. Then, I ran a level regression using Bitcoin price as the dependent variable and the rest as the independent variables. The result is summarized in Table 4, where we can see that six out nine of the independent variables have coefficients that are significant at the 5 percent significance level. In addition, the R-square is 0.76.

The high R-square suggests that there might be a problem of autocorrelation. The Durbin-Watson statistic for this regression is 0.21 that suggests a high level of positive autocorrelation (When the Durbin-Watson statistic is equal to 2, there is no first-order autocorrelation). In order to correct for the autocorrelation, I decided to use ARIMA (Autoregressive Integrated Moving Average) modeling to account for the structure of the error term. I plotted the ACF and PACF for the residues from the level regression to figure out the structure for the error term.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Level Regression</th>
<th>ARIMA (1,0,0)</th>
<th>First Differencing Variables</th>
<th>ARIMA (1,1,0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold Price</td>
<td>-0.4976441*</td>
<td>0.0932349</td>
<td>D. Gold Price</td>
<td>0.1207555</td>
</tr>
<tr>
<td></td>
<td>(0.000)</td>
<td>(0.493)</td>
<td></td>
<td>(0.352)</td>
</tr>
<tr>
<td>Price of GBP</td>
<td>1728.555*</td>
<td>263.432</td>
<td>D. Price of GBP</td>
<td>248.7792</td>
</tr>
<tr>
<td></td>
<td>(0.000)</td>
<td>(0.487)</td>
<td></td>
<td>(0.480)</td>
</tr>
<tr>
<td>Price of JPY</td>
<td>91967.49*</td>
<td>8079.286</td>
<td>D. Price of JPY</td>
<td>19553.84</td>
</tr>
<tr>
<td></td>
<td>(0.002)</td>
<td>(0.807)</td>
<td></td>
<td>(0.508)</td>
</tr>
<tr>
<td>Price of AUD</td>
<td>-1241.753*</td>
<td>-475.4887</td>
<td>D. Price of AUD</td>
<td>-429.614</td>
</tr>
<tr>
<td></td>
<td>(0.000)</td>
<td>(0.112)</td>
<td></td>
<td>(0.131)</td>
</tr>
<tr>
<td>Price CNY</td>
<td>8652.025</td>
<td>4725.729</td>
<td>D. Price CNY</td>
<td>2022.493</td>
</tr>
<tr>
<td></td>
<td>(0.157)</td>
<td>(0.735)</td>
<td></td>
<td>(0.897)</td>
</tr>
<tr>
<td>S&amp;P Index Value</td>
<td>0.626791*</td>
<td>-0.0479656</td>
<td>D. S&amp;P Index Value</td>
<td>-0.106951</td>
</tr>
<tr>
<td></td>
<td>(0.000)</td>
<td>(0.803)</td>
<td></td>
<td>(0.579)</td>
</tr>
<tr>
<td>NIKKEI Index Value</td>
<td>.1920777</td>
<td>1.52098</td>
<td>D. NIKKEI Index Value</td>
<td>1.559461</td>
</tr>
<tr>
<td></td>
<td>(0.847)</td>
<td>(0.090)</td>
<td></td>
<td>(0.056)</td>
</tr>
<tr>
<td>WTI Spot Price</td>
<td>1.151404</td>
<td>-1.731126</td>
<td>D. WTI Spot Price</td>
<td>-1.984885</td>
</tr>
<tr>
<td></td>
<td>(0.298)</td>
<td>(0.162)</td>
<td></td>
<td>(0.076)</td>
</tr>
<tr>
<td>Ten Year Treasury Yield</td>
<td>-96.2067*</td>
<td>24.20865</td>
<td>D. Ten Year Treasury Yield</td>
<td>33.99086</td>
</tr>
<tr>
<td></td>
<td>(0.013)</td>
<td>(0.600)</td>
<td></td>
<td>(0.398)</td>
</tr>
<tr>
<td>R-Square</td>
<td>0.7626</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Number of Observations</td>
<td>247</td>
<td>247</td>
<td>NA</td>
<td>247</td>
</tr>
<tr>
<td>Durbin-Watson</td>
<td>0.2143206</td>
<td>1.500224</td>
<td>NA</td>
<td>1.959279</td>
</tr>
</tbody>
</table>

Table 4: Regression Results (Data Source: Thomas 2015) *denotes statistically significant at 0.05 significance level.

Figure 16 shows that the residual correlogram for the level regression declines after the first lag with a tail shaped curve. In Figure 17, the partial reside correlogram
has only one case of partial autocorrelation that is out of the confidence band.

Together, these graphs show that the error term has an autoregressive structure of order one. Thus, I ran an ARIMA (1,0,0) model that takes into account of the autoregressive error term. The result is shown in Table 4. After removing the influence of the autoregressive errors, all the coefficients fail to be significant at the 0.05 level. However, the Durbin-Watson test is 1.5, showing some minor positive autocorrelations.

Figure 16: Residual Correlogram
In order to better understand the nature of the data, I ran the Dickey-Fuller test on all the variables. The null hypothesis for Dickey-Fuller is that the variable is a unit root process. Thus, failing to reject the null means that the series is non-stationary.

Table 5 shows for all the variables, none of the p-values are below 0.05 thus we fail to reject the null. This means that the data is not stationary. Then, I ran Dickey-Fuller again on the variables after first differencing. This time, we are able to reject the unit root hypothesis at the 0.05 significance level. The results show that all these variables are in fact I(1) processes. Thus, I need to include this integration of order one in my ARIMA model.
<table>
<thead>
<tr>
<th>Variables</th>
<th>Dickey-Fuller P-value</th>
<th>Variables</th>
<th>Dickey-Fuller P-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin Price</td>
<td>0.5477</td>
<td>D.Bitcoin Price</td>
<td>0.0000*</td>
</tr>
<tr>
<td>Gold Price</td>
<td>0.5710</td>
<td>D.Gold Price</td>
<td>0.0000*</td>
</tr>
<tr>
<td>Price of GBP</td>
<td>0.9602</td>
<td>D.Price of GBP</td>
<td>0.0000*</td>
</tr>
<tr>
<td>Price of JPY</td>
<td>0.9863</td>
<td>D.Price of JPY</td>
<td>0.0000*</td>
</tr>
<tr>
<td>Price of AUD</td>
<td>0.9358</td>
<td>D.Price of AUD</td>
<td>0.0000*</td>
</tr>
<tr>
<td>Price CNY</td>
<td>0.1141</td>
<td>D.Price CNY</td>
<td>0.0000*</td>
</tr>
<tr>
<td>S&amp;P Index Value</td>
<td>0.8757</td>
<td>D.S&amp;P Index Value</td>
<td>0.0000*</td>
</tr>
<tr>
<td>NIKKEI Index Value</td>
<td>0.9860</td>
<td>D.NIKKEI Index Value</td>
<td>0.0000*</td>
</tr>
<tr>
<td>WTI Spot Price</td>
<td>0.8407</td>
<td>D.WTI Spot Price</td>
<td>0.0000*</td>
</tr>
<tr>
<td>Ten Year Treasury Yield</td>
<td>0.4136</td>
<td>D.Ten Year Treasury Yield</td>
<td>0.0000*</td>
</tr>
</tbody>
</table>

* denotes statistically significant at 0.05 significance level.

Table 5: Dickey-Fuller Statistics (Data Source: Thomas 2015)

The result from ARIMA (1,1,0) is documented in Table 4. None of the independent variables are significant at the 0.05 level. Moreover, the Durbin-Watson statistics for this regression is 1.96, which means that there is little autocorrelation of order one. Thus, ARIMA(1,1,0) is the best model out of the three. The ARIMA models show that Bitcoin price does not have strong correlation with the other financial instruments such as equity, foreign exchange, fixed income, and commodity. This characteristic makes Bitcoin a good financial instrument to hedge against risks and helps investors diversify their portfolios.
According to Professor Marie Briere and her colleagues at Paris Dauphine University, Bitcoin’s return possess a high positive skew that assemble sophisticated derivatives trading strategies that are used to hedge against financial crisis. This, Briere argues, “suggests that BTC could act as a partial hedge against crises” (Briere et. Al 2013). According to Briere, Bitcoin increases the Sharpe ratio in a portfolio when included. Sharpe ratio is used to measure return over risk. The higher the ratio, the more risk-return efficient the portfolio. That is, with the same level of risk, a portfolio with the higher Sharpe ratio portfolio will have a higher return than one with a lower ratio. Bitcoin can increase the Sharpe ratio of an investment portfolio. Figure 18 shows the returns of two portfolios at various level of risk tolerance. The blue line represents the return for a portfolio that contains three percent Bitcoin, while the pink line represents a portfolio with traditional assets. The performance of portfolios that includes three percent Bitcoin is significantly better than the portfolios at almost every risk level.
In addition to benefits from a risk-return perspective, Bitcoin can help investors respond to market events more promptly. The traditional financial market is open only on weekdays. Bitcoin’s market is 24/7. Investors can buy and sell Bitcoin anytime they want to. They can respond to market events by buying and selling Bitcoin at a more timely fashion than other financial instruments.

In this chapter, I have examined the demand side of Bitcoin. Contrary to popular belief, Bitcoin’s anonymity feature does not make it a default tool for criminals or drug dealers. I have also examined Bitcoin as a currency. To the consumers, Bitcoin presents a safe option to pay for transactions. However, its high price volatility prevents it from being adopted more widely. For businesses, adopting Bitcoin can bring positive publicity and reduce the cost and waiting time for transactions, but regulatory uncertainties make accepting Bitcoin complicated. Lastly,
I examined Bitcoin as a financial instrument. Bitcoin can help improve the risk-return of an investment portfolio with its low correlation with other financial assets.

The biggest challenges for Bitcoin are price instability and regulatory uncertainty. If Bitcoin can maintain a stable price level and the regulation can clarify, it will acquire a larger user base and more business partners. Now we have analyzed both the supply and demand side of Bitcoin. In the next chapter, I will analyze the dynamics and inefficiencies of the Bitcoin market.

**Chapter Four: Bitcoin Market Dynamics**

In this chapter, I demonstrate that the Bitcoin market is becoming more mature over time and its efficiency has improved since 2009. I show how the Bitcoin market has evolved over time from four different measures: Bitcoin velocity, bid ask spread, arbitrage opportunities, and regulation.

**Bitcoin Velocity**

Money velocity measures the speed at which money changes hand during a certain period (Federal Reserve Bank of St. Louis 2015). According to the quantity money theory, the product of money velocity and money supply has to equal the total domestic product (Heakal 2005). Thus, money velocity can measure the expansion of the economy and the economic outlook. Because Bitcoin supply is fixed and predictable, I am able to calculate the exact money velocity for Bitcoin from 2009 to
2015, which equals the annual transaction volume. I divide the annual transaction volume in Bitcoin with the total Bitcoin in the system to calculate the Bitcoin velocity.

![Bitcoin Velocity](image)

**Figure 19: Bitcoin Velocity (Date Source: Thomas 2015)**

Figure 19 shows that the money velocity of Bitcoin has been increasing since its creation. Increasing money velocity means that more transactions are conducted through Bitcoin and Bitcoin is circulating more actively than before. However, even with this upward trend, Bitcoin is still very slow compared to other currencies such as the U.S. dollars. Figure 20 shows the money velocity for dollar cash, also known as M2 velocity. This velocity has been in a downward spiral since the financial crisis in 2008, with the mean around 1.6. But still the M2 velocity is significantly higher than Bitcoin’s 0.025. What is promising is that Bitcoin’s velocity is picking up; Bitcoin is circulating more and more, like a mainstream currency.
Bid-Ask Spread

While Bitcoin is gradually working towards mainstream currency status in terms of its velocity, in the foreign exchange market Bitcoin already operates just like any other foreign currency. Owners of Bitcoin can exchange their Bitcoins to any major currencies in the world through Bitcoin exchanges. When users want to purchase Bitcoin, they will need to go to one of the online exchanges, similar to banks, convert Bitcoins to other currencies. Exchanges buy at a lower price and sell at a higher price. The ask price is the price at which one buys Bitcoin, and the bid price is the price at which exchanges will buy Bitcoins from individual users. The
difference between these two prices is the bid ask spread. The exchanges profit from taking the bid ask spread.

However, the spread is not a fixed quantity. The exchanges charge different spreads at different times. The magnitude of the spread varies according to the liquidity in the market. Liquidity represents the easiness to purchase or to sell a product in the market. A liquid asset is in demand and changes ownership often, while illiquid assets are hard to buy and sell. The bid ask spread has a negative relationship with the liquidity in the market. For a very liquid product, the spread will be thinner than illiquid products. I calculated the average daily bid ask spread in multiple Bitcoin exchanges and plotted the spreads in Figure 21.

![Bid Ask Spread In Dollars](image)

**Figure 21: Bitcoin Bid Ask Spread (Data Source: Thomas 2015)**

Figure 21 shows that the bid ask spread varies a lot day to day. Additionally, in this chart there is a discernable downward trend. In 2014, the spread often go
above 1.5 dollars. In 2015, the spread consistently stayed below one dollar. This trend shows that the Bitcoin market has become more liquid overtime, another sign that the Bitcoin market is becoming more active.

**Bitcoin Arbitrage**

As with any market, there are arbitrage opportunities in this “foreign exchange” market. Investopedia defines arbitrage as “buying in one market and simultaneously selling in another, profiting from a temporary difference [and] this is considered riskless profit for the investor” (Investopedia 2015). Arbitrage opportunities are abundant when there is inefficiency in the market. For example, if a car is sold for fifty thousand dollars in Middletown Connecticut but the same car is sold for only ten thousand dollars in New Haven, the car market is inefficient and there are arbitrage opportunities.

An arbitrage for the car market would be to buy cars in New Haven and sell them in Middletown. While arbitragers reap profit from the market inefficiency, they in fact help increase the efficiency through their profit driven activity. In the car example, arbitrage activity will increase demand in New Haven and drive up the price level. At the same time, they reduce the price in Middletown by providing more cars to buyers in Middletown. Eventually, the prices will be the same across these two locations and the inefficiency will be eliminated. When there is no efficiency, there is no arbitrage opportunity (Investopedia 2015).

Similar to the car arbitrage, an arbitrage strategy using Bitcoin could be taking advantage of the difference in exchange rates. For example, one investor could buy
Bitcoins for 300 dollars and sell them for 290 Euros. Assume the exchange rate between dollar and euro is 0.91. This trade means that the Bitcoin investor will be able to convert the 290 euros to 318 dollars. This trade will result in an 18-dollar profit for the investors.

There are two reasons that could explain the difference in Bitcoin price in euro and dollar. One reason could be that the Bitcoin market does not adjust to the change in the exchange rate between euro and dollar fast enough. For example, the exchange rate from dollar to euro could be 0.96 in the morning but in the afternoon it dropped to 0.91. Bitcoin exchange rate might not respond fast enough to reflect the change in the currency market and presents an arbitrage opportunity.

The other reason can be that the market for Bitcoin is more active in the U.S. that drives the price down, while the European market might be less active and less competitive. In this case, the inefficiency is due to the regional disparity.

As we have seen in the car example, an efficient market does not have a lot of arbitrage opportunities. In order to demonstrate that the Bitcoin market is maturing and become more efficient, I use arbitrage profit as a proxy for efficiency. While I cannot directly measure efficiency, I can explore the arbitrage opportunities in the Bitcoin market.

I simulated three arbitrage strategies with three different currencies: Euro, Chinese Yuan (CNY), and British Pound (GBP). In each case, I purchase one Bitcoin with dollars and then convert it to the three currencies respectively according to the conversion rates of that day. I then convert the three currencies back to dollars at the...
currency exchange rates and calculate the differences. In Figure 22, I plotted the arbitrage profit as a percentage of Bitcoin price from July 2013 to March 2015.

![Arbitrage Profit As % of Bitcoin Price](image)

Figure 22: Bitcoin Arbitrage Opportunities (Data Source: Thomas 2015)

This figure provides highly interesting information on the arbitrage opportunities in the Bitcoin market. The arbitrage profit for all three currencies has decreased over time. In 2013, the profit for GBP arbitrage averages around 15 percent of the Bitcoin price and in 2015 it is below 10 percent. The same holds true for the other currencies as well. This trend is even more pronounced for CNY arbitrage. The average profit went down to around 0 percent, showing a decrease in arbitrage opportunities between China and the U.S.

The decreasing arbitrage profit in the Bitcoin market marks the increasing efficiency in the market. An efficient market entails profit-maximizing investors who
are able to recognize the opportunities and use resources to beat the market and make it efficient (Damodaran). Thus, the increasing efficiency in Bitcoin foreign exchange market shows that the information of Bitcoin becomes more available to investors and there are more investors working on Bitcoin based arbitrage opportunities. This further shows that the Bitcoin market is maturing.

The Maturing of Bitcoin Exchanges and Regulation

Not only is the Bitcoin market evolving and becoming more efficient, the exchanges themselves are changing too. 2015 has witnessed a series of efforts by investors and startups to bring Bitcoin to the mainstream economy. In January 27th 2015, Coinbase, one of the most influential Bitcoin startups, announced that it had received licenses from more than a dozen states in the U.S. and will open the first regulated Bitcoin exchange that allows Bitcoin investors to trade Bitcoin in real time (Coinbase 2015). The legality of Bitcoin and Bitcoin businesses has always been a grey area as the government tries to figure out new regulations for them. The regulatory approvals for Coinbase help clarify the legality of Bitcoin enterprises in the United States.

In addition to having the support from the government, Coinbase exchange is supported by serious investors and abundant funding. The New York Stock Exchange, USAA, and Union Square Ventures all contributed to the opening of the first regulated Bitcoin exchange. The support has materialized into 75 million dollars of funding for Coinbase, which allows it to invest in infrastructures that highly improve the exchange security (Rizzo 2015). In addition, Coinbase has insurance that covers all Bitcoin loss from the exchanges including hacking and theft (Coinbase...
As a result, two weeks after its launch, Coinbase exceeded the trading volume of Bitstamp and BTC-e, two major biotin exchanges that are not regulated (Menezes 2015).

Coinbase is not the only exchange that aims to bring Bitcoin to more users by working with the government. After receiving a 65 million dollars settlement from Facebook, the Winklevoss twins also announced in January 2015 that they were going to start a fully compliant Bitcoin exchange called Gemini, Latin for twins (Shandrow 2015). The Winklevoss twins view Gemini as a way to raise consumer confidence on Bitcoin. In order to distinguish themselves, they hired “Michael Breu, former head of information security in the research department at hedge fund Bridgewater Associates” to be in charge of compliance for Gemini. The chief security officer will be Cem Paya who used to work for Airbnb in the same position. Gemini will also be fully insured once it receives the regulatory approval (Southurst 2015). All these efforts promise Gemini will be a safer and more secure exchange similar to Coinbase.

Another important development for Bitcoin is the first approved Bitcoin Exchange Traded Fund (EFT) is on its way to public on March 17th 2015 (Casey 2015). Bitcoin Investment Trust (BIT) received approval from the Financial Industry Regulatory Authority (FINRA) as an ETF. BIT will allow people to invest in Bitcoin without actually owning Bitcoin by investing in a fund that owns Bitcoin and tracks the movement of Bitcoin price. Bitcoin Investment Trust marks that Bitcoin is now officially a financial instrument that is accepted by the regulators and is further integrated into the mainstream economy.
During an international Bitcoin conference I attended in Berlin, a speaker polled the audience regarding whether we thought that Bitcoin should comply with the regulation in order to succeed. Half of the audience believed regulation will help Bitcoin while the other half thought it would ruin its integrity. I personally stand with the pro-regulation crowd. I believe that the creators of Coinbase, Gemini, and BIT share the same belief. As a cryptocurrency, Bitcoin does not have any physical backing for its value. Stocks have value because they represent shares of companies; dollars have value because it is the legal tender of the United States. Bitcoin’s value derives from purely faith in its technological strength and prospect.

Unfortunately, incidents such as the hacking of Mt. Gox and the shutdown of Silk Road have lowered Bitcoin’s public opinion. While most people still don’t understand what Bitcoin is (Vigna 2014), the negative news clouded their judgment and filled them with prejudice. This prejudice is combined with a natural instinct to resists change. I think the term disruptive innovation is fit Bitcoin the best. Disruptive innovation is a “product or service takes root initially in simple applications at the bottom of a market and then relentlessly moves up market, eventually displacing established competitors” (Christensen 2012). Bitcoin is revolutionary in that it decentralizes the currency market that we know and brings a whole new space for creativity and new solutions. However, this kind of disruption often fills people with fear of uncertainty especially when they are not sure where this technology can bring them. This fear then translates into the unwillingness to believe or learn about the new technology.
By complying with the regulations and integrating Bitcoin into the mainstream economy, the proponents of Bitcoin help the public learn about Bitcoin and its potential. By working with the legislators and insurance companies, companies such as Coinbase and BIT raise the consumer confidence in Bitcoin. It appears that we are entering a period where legislation and regulation can help Bitcoin regain trust from the public, a key ingredient to the success of a currency. Bitcoin investors who actively engage the regulatory authorities are in fact helping them to learn about how Bitcoin works and how it can benefit the businesses world. The success of BIT and Coinbase in term of engaging the regulators shows that the regulators are willing to learn about Bitcoin. This improvement in regulatory environment is a strong indicator of the maturity of the Bitcoin market.

In this chapter, I have presented four pieces of evidence to show that the Bitcoin market is maturing. First, to measure the activeness of the Bitcoin market, I calculated the Bitcoin velocity and showed that the velocity of Bitcoin has an upward trend since its creation. This means that the Bitcoin market is expanding and more transactions are conducted through Bitcoin. Second, I showed that the Bitcoin market is becoming more liquid by illustrating the decreasing bid ask spread in the market. Third, the market is also becoming more efficient as demonstrated by the decrease in arbitrage opportunities in the foreign exchange market for Bitcoin. The diminishing arbitrage profit means that more and more investors are investing in Bitcoins and the information on Bitcoin is more available. Lastly, I have discussed the most up-to-date developments in Bitcoin-related enterprises. The creation of regulated Bitcoin exchange and ETF is a significant improvement in the regulatory environment for
Bitcoins. It also indicates that the legislators are learning about Bitcoin and are working with Bitcoin startups to promote it. Regulated and insured Bitcoin exchange will help change Bitcoin’s public image and raise awareness and trust. Trust is crucial to the success of any currency, especially a decentralized digital currency.

The increasingly efficient and reliable Bitcoin market contributes positively to the popularity of Bitcoin and its influence as a currency. In the next chapter, I will summarize the potential of Bitcoin and explore the newest applications of Bitcoin technology to other fields.
Chapter Five: A Bitfuture

What is the future of money? This is the question that inspired this thesis and the research around Bitcoin. This is also the question that has inspired many to create new payment systems and currencies suitable to digital age in which we live. The years since Bitcoin’s creation have seen huge advancements in next-generation payment systems and cryptography. Many new digital currencies have been created. New payment systems have been invented. In fact, the technological breakthroughs brought by Bitcoin are not only limited to the financial sector. Bitcoin has precipitated a wave of decentralization in many fields that will challenge existing businesses and pose new solutions to old problems.

In this chapter, I will first explore the innovative payment systems that have been inspired by Bitcoin and decentralization. These include many cryptocurrencies based on the Bitcoin protocol, the rules of Bitcoin that allow electronic devices to communicate through networks. Further, I will present examples of how Bitcoin technology can influence fields beyond the financial sector. Lastly, I will summarize the findings of this thesis and its contributions to analyzing cryptocurrencies in general.

Cryptocurrencies Based on the Bitcoin Protocol

With its groundbreaking technology, Bitcoin has inspired a wave of cryptocurrency creation. Many companies created their own currencies based on the Bitcoin protocol. The Bitcoin protocol is totally open source and free for all to use.
As of April 8th 2015, there were 2972 cryptocurrencies in the market. Some of the most prominent ones include Litecoin and Dogecoin (CryptoCoin Chart, 2015).

Litecoin was created on October 13th, 2011 (Z 2015). The development team used Bitcoin protocol as the base for Litecoin, making minor changes on parameters including the specification of the proof of work, the average time in which a block can be created, and the total amount of Litecoin that can be mined. For example, the expected creation time required for each block of Litecoin is 2.5 minutes, rather than Bitcoin’s expected 10 minutes. One Litecoin was valuated at 1.53 dollars on April 9th, 2015. Compared to Bitcoin, it has less value. Nonetheless, Litecoin is still one of the major cryptocurrencies (Coinmarketcap 2015).

Dogecoin is another cryptocurrency based on the Bitcoin protocol. Doge is a dog that often appears in online memes. The creation of Dogecoin all started with a joke that Jackson Palmer, a marketing person, posted on Twitter; he asked people to invest in “Dogecoin” on November 27th 2013. His tweet caught the attention of Billy Markus, a software engineer, who then got in touch with Palmer. They worked together and created Dogecoin (Noyes 2014). Figure 23 is the logo for Dogecoin based on the Internet meme Doge.

Figure 23: Dogecoin Logo (Source: Dogecoin 2015)
Soon Dogecoin became a major phenomenon in the cryptocurrency market. The Dogecoin website had millions of visits within the first month. Furthermore, Dogecoin’s first month marks a large transaction volume that even exceeded Bitcoin’s transaction in terms of number of transactions, as demonstrated by Figure 24.

![Figure 24: Dogecoin Bitcoin Daily Transaction Volume (Source: Noyes 2014)](source: bitinfocharts.com)

However, Dogecoin’s popularity was short-lived. Dogecoin’ initial fame was due to both the popularity of the doge meme and the low difficulty of mining. While 95 percent of Bitcoin is to be mined in the first 20 years of its creation, 95 percent of Dogecoin was supposed to be mined in the first year. Miners gain profit from two
sources: coin-based income and transaction-based income. Bitcoin is scheduled to be mined slowly so that it can gain user base over time and increase the transaction-based income. Then after all the Bitcoin is mined, the tips from its users will still be significant enough to incentivize miners. However, Dogecoin’s mining incentive dropped drastically as fewer Dogecoins were available to be mined before it could gather a large number of supporters to ensure a sufficient transaction-based income. The limited number of miners leaves the Dogecoin network vulnerable to hacking. In order to solve this problem, Dogecoin’s creator Palmer announced in early 2014 that the supply for Dogecoin would not be fixed (Wile 2014). The removal of a cap increased the incentive for mining for there would be more Dogecoins to be mined.

In addition, in August 2014 Dogecoin merged mining with Litecoin. Merging mining means miners will get both Litecoin and Dogecoin as a reward for mining a block (DeMartino 2014). This essentially increases the award for mining and attracts more people to mine.

Even with these new incentives, Dogecoin and Litecoin still cannot compare to the influence of Bitcoin and no other cryptocurrency can currently compete against Bitcoin. Many of the cryptocurrencies on the market are based on Bitcoin protocol and have properties similar to Bitcoin. However, what they do not have is the Bitcoin’s first-comer’s advantage and its large community of miners. Figure 25 below shows the 24-hour trade volume on March 25th 2015 of all the cryptocurrencies denominated in Bitcoin. As we can clearly see, Bitcoin has a superior level of support that no other cryptocurrencies can match.
Compared to other cryptocurrencies, Bitcoin has the advantages of being the first cryptocurrency, the first to have its own legal exchange, its own exchange traded fund, and widespread public recognition. In order to compete against Bitcoin, a new cryptocurrency has to offer something Bitcoin cannot – it would have to be based on a technology different from the Bitcoin protocol.

**The Ripple Protocol**
There is another major protocol used in creating cryptocurrency called the Ripple protocol. The Ripple protocol is developed by the Ripple Lab as a digital currency and a payment system. Ripple is not based on the blockchain technology that supports Bitcoin. It has its own method of verifying transactions and providing security. This process is called “consensus”. Similar to Bitcoin, Ripple has a public ledger in which information on all account balances are public. When a transaction occurs, it is registered in one of the nodes in the Ripple network. This node later sends information to other nodes; when 80 percent of the nodes receive the updates on this transaction, the public ledger is updated. The consensus system allows the distribution of the transaction information across network in the fashion of a ripple. Evenly distributed information prevents the problem of double spending, as Bitcoin does through its blockchain technology (Ripple b. 2015).

The native currency of the Ripple network is called XRP (Ripple c. 2015). Any two parties can trade XRP. However, Ripple’s biggest achievement is not its currency but its currency-agnostic payment network. Ripple can directly facilitate transactions made in any currency. Ripple transactions in currencies other than XRP function similarly to Hawala, which means "money transfer without money movement" (Investopedia 2010). A simple example of Hawala is illustrated in Figure 26. A user Alex deposits money with an agent at one location with a password that is only known to another user Beth. Alex’s agent will inform Beth’s corresponding agent of the transfer and provide the password for Beth’s agent to verify. Beth, with the password, will be able to cash the deposit with her agent. Later, the two agents
will settle the trade. There is likely to be another transaction in which Beth sends money to Alex, canceling out this payment.

![Diagram of the Hawala System](source: Lewis 2014)

Figure 26: How the Hawala System Works (Source: Lewis 2014)

Without getting into the technical details, the Hawala model illustrates the basic concept of the Ripple network. Instead of having agents, Ripple has gateways. These gateways can be banks, business, or services that participate in the Ripple network where Alex and Beth can deposit and withdraw money. There are thousands of these gateways in the network that allow people to transfer money. In fact, the Ripple network allows you to send anything through the network as long as the gateway supports it; It can be gold, USD, Bitcoin, or XRP.

The biggest innovation of this system is that it also decentralizes exchanges. Figure 27 demonstrates a case in which one user wants to use USD to send another user JPY. User Alex only needs to send USD through his gateway. In the course of its
passage, the USD clears through a market maker who converts the USD to JPY. Beth, at the other gateway, is then able to withdraw JPY instead of the original USD. Anyone could be the market marker in the network. This essentially created a decentralized exchange system where money and goods can be easily converted in the network. The Ripple Network removes the hassle of currency conversion and leaves more room for people to choose the currency they want to use.

![Diagram of decentralized currency conversion in the Ripple Network](image)

**Figure 27: Decentralized Currency Conversion in the Ripple Network (Ripple a. 2015)**

Compared to the traditional banking systems in which currency conversion is monopolized, Ripple increases the level of competition in the market by allowing essentially any gateway to function as a market maker. More competitive markets will facilitate currency conversions by lowering their transaction costs. Ripple brings
the decentralization to a new level by decentralizing the relationship between different currencies.

**The Future of Money**

What, then, is the future of money? I believe that the development of smart money will one day dominate the way we use currency. Smart money is a new concept that refers to the fact that each transaction in Bitcoin is essentially some computer code. As a result, we are able to program it, just like we can program our phones to set up a timer or send a group text. Bitcoin transactions are fully programmable to the degree that they can be contingent upon the satisfaction of a condition or payment to multiple accounts at various dates (Bheemaiah 2015). The integrity of the blockchain guarantees the effectiveness and fulfillment of the instruction wrote for each transaction.

Programmable money has far-reaching implications; it can fundamentally change the way we use money. If current technologies are further adapted and adopted, we one day will be able to program Bitcoins to automatically pay our bills, invest for profit, save for retirement. Money will no longer be an object that simply facilitates transactions. Money will be able to interact with its owners and independently accomplish tasks that are specified by its users. Money one day will fully integrate into the Internet and transform from an object to an automated intelligence network. I believe this is the most far-reaching impact on money and payment system brought by Bitcoin. Traditional currency cannot compete against cryptocurrency in this regard at all.
There are four reasons cryptocurrencies will eventually join the mainstream economy. First, the potential for smart money is unlimited. Programmable money unlocks many new applications of money that were before unavailable such as various payment schemes. Second, decentralization means higher competition. If we look at Ripple’s model of decentralized market makers, it is possible for anyone – not only banks – to serve the function of market makers. As a result, decentralization breaks down the monopoly of financial institutions and governments over money and financial services. The effect of the increased competition will be lower costs and greater access to financial services. Third, cryptocurrencies will be more efficient. Traditional ecommerce with credit cards takes longer to process than cryptocurrency transactions. Cryptocurrencies can verify transactions faster and more efficiently, bypassing the complicated network of banking and identity verification. Lastly, Bitcoin can be private and public at the same time. Anyone can see the entire transaction history of Bitcoin but each transaction is not associated with a name. Bitcoin thus provide a high level of transparency that no other currency can achieve, because no other currency has a public ledger that records each and every transaction ever happened.

Admittedly, Bitcoin has its weaknesses as well. There are three major obstacles standing in way of its mainstream adoption. First, Bitcoin is a poor store of value. Its price volatility can prevent people from using it because of the high risk associated with price movement. Second, public awareness of Bitcoin and the benefits of this technology are currently lacking. According to the Wall Street Journal’s survey in 2014, 76 percent of the U.S. population had never heard about
Bitcoin; of those who had heard of it, even fewer understood how it could influence the future of technology. The knowledge gap prevents people from trying and trusting Bitcoin. Third, regulatory uncertainty has yet to be resolved. It takes time and effort for regulators to understand how Bitcoin can influence the government and the economy. It is still uncertain how the governments will adapt their policies for Bitcoin.

I strongly believe that the future of money has begun with Bitcoin, and that Bitcoin is not the end product. Like many technologies, the company that first invented it may not be the one that promotes its general usage. There are thousands of companies innovating around the blockchain technology provided by Bitcoin. It is very likely that a new product will arrive that has all Bitcoin can offer, plus a better store of value.

For example, the chair of St. Louis Fed argues that there might be a Fedcoin one day issued by the Fed that is pegged against USD (Andolfatto 2015). If this comes to fruition, pegging will resolve the Bitcoin’s issue with store of value. With time and constant research, the awareness of Bitcoin will increase in the general public and policymakers will figure out a way to integrate Bitcoin into the larger system.

What Bitcoin provides is its revolutionary technology and the successful experience with decentralization. Bitcoin’s recent success encourages developers and financial professionals to experiment with alternatives to our current monetary system. Regardless of which cryptocurrency becomes dominant in the future, the revolution over money has begun, and money as we know it will not remain the same.
Blockchain Technology in Other Fields

The ideas behind Bitcoin and the blockchain technology it entails are, in fact, so powerful that they have sparked innovations in many fields beyond finance. The Blockchain technology provides solutions to any problems that concern transparency, anonymity, decentralization, security, and efficiency. Voting is an example of such activities that requires both transparency and security. In 2014, the Liberal party in Denmark used blockchain for their internal voting (Parker 2014). Voters cast votes using their private key, and each vote could be verified using the public key that is available to all participants. All votes could be stored in the blockchain. While each vote was public, each voter’s identity is not associated with the vote. Thus, voters can stay anonymous. Additionally, voting members could participate anytime and from anywhere in the world. At the same time, the blockchain technology ensures that the security of the voting process.

A technology company, Bitcongress, is currently developing apps that apply Blockchain to voting (Rockwell 2014). One day, a citizen could cast a vote for the presidential election without waiting in line. The result would be an election that would be completely transparent and without the influence of human errors in vote-counting and bias in voter turnout.

Another application of Blockchain is on governance. With the transparency, government expenses will be visible to all citizens via the Internet and all transaction history will be public available in the blockchain. This transparency can immediately
expose corruptions and provide sufficient public supervision over government activities.

Blockchain can also be used as a record of ownership of properties. For example, with smart contract, a similar application to smart money, one can purchase fixed income products and the network will automatically distribute coupons to the debt owners without the need of custodians (Bheemaiah 2015).

The applications of Blockchain transcend Bitcoin itself. It can help improve upon other existing services and activities and fully realize the potential of the Internet. Blockchain technology is currently being applied to music download, file sharing, insurance, business ownership, governance, voting, and much more. The new innovations have implications that are far reaching and can potentially change the ways we interact with the world.

**The Access Issue of Cryptocurrencies and Blockchain Technologies**

While cryptocurrencies can provide many benefits to our monetary and economic systems, they have serious access issues. Bitcoin was invented due to dissatisfaction with government-controlled currencies. However, its emphasis on decentralization does not make it a democratic currency. In fact, its technocratic nature presents barriers for participants.

On the supply side, Bitcoin mining is extremely demanding on the hardware. ASICs are costly and wear out quickly in mining. Because the mining difficulty is extremely high and mining has become a competitive and profit-seeking industry, anyone who is serious about mining Bitcoin has to purchase ASICs in order to receive the coin-based income. However, the cost of ASICs makes mining Bitcoin not an
option for some potential participants; there are high and rising barriers to entry on the supply side.

On the demand side, Bitcoin is not very accessible either. In order to understand Bitcoin and how to use it, one needs knowledge of computer science and technology. Unlike cash, using Bitcoin involves working with a constantly evolving technology. Thus, lack of education in this area can prevent people from accessing Bitcoin.

In addition to education, Internet access also plays an important role in access to Bitcoin. Because Bitcoin relies on having a connection to the Internet, areas with low Internet penetration rates will have difficulty adopting it and enjoying the benefits of decentralized payment systems. Figure 28 shows the penetration rate of the Internet in different areas of the world. While eighty percent of the population in North America and Western Europe has access to the Internet, Africa and South Asia have access rates of only around twenty percent. For the developing world, the low Internet coverage also means that the population will be less prepared to compete in an era where blockchain technology is implemented widely. The opportunity cost is very high. This uneven access to Internet and cryptocurrencies will aggravate the technological gap between the developed world and the developing world.
If cryptocurrencies join the mainstream economy, they will increase the barriers for developing countries to participate and compete in the global market. Cryptocurrencies will also make the system even more favor people with a strong computer science background and good overall education. It is unfortunate that the decentralization of cryptocurrencies is thus likely limited to a population where power and wealth are concentrated.
Conclusion

The goal of this thesis is to set up the basic framework in which to analyze cryptocurrencies through presentation of original theoretical and empirical research on Bitcoin. As cryptocurrencies are still new and understudied, there is a lack of serious economic analysis on how they work and their impacts. More often than not, scandals rather than actual scholarly studies populate the media’s reporting of cryptocurrencies. Through studying cryptography and investigating in various aspects of Bitcoin, I have provided a systematic framework in which to situate cryptocurrencies.

In analyzing the supply side of Bitcoin, I constructed a mining profit function that can be used to estimate profit for cryptocurrency mining. The derivation of the profit function can then be used to estimate the target price for sustainable mining. Through studying the demand side of Bitcoin, I expanded the criteria for currency by adding proof of security to the original three measures, which were not sufficient to predict the success of alternative currencies, which often have more security concerns than government-issued currencies. I also proposed and implemented four ways in which to measure the maturity of cryptocurrency markets: money velocity, bid-ask spread, arbitrage opportunities, and regulatory. Lastly, I explored the potential impacts of cryptocurrencies on not only the financial system but also voting, governance, and contracts.

Who would have thought that a ten-page paper on the concept of a digital currency in 2008 would start a payment-system revolution and innovations in other
fields that we witness today? Millions of people work on the Bitcoin network as miners. Central Bankers try to understand it. The financial world is estimating its potential profit. The whole world is watching. We are fortunate to witness this new wave of technological innovation and I am anxious to see how it will change the human world as we know it. This is the Bitfuture. We begin as history embarks.


