Critical Success Factors for Bitcoin Economics

by

Alejandro D. Santiago Boothby

A thesis submitted in partial fulfillment of the requirements for the degree of

MASTER IN BUSINESS ADMINISTRATION

in

Finance

UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS
2015

Approved by:

_____	_____
Darik Cruz-Martínez, Esq., LL.M. Member, Graduate Committee	Date
_____	_____
Mario Córdova-Claudio, Ph.D., J.D. Member, Graduate Committee	Date
_____	_____
María Amador-Dumois, Ph.D. President, Graduate Committee	Date
_____	_____
Jorge Schmidt-Nieto, Ph.D. Representative of Graduate Studies	Date
_____	_____
Roberto Seijo-Vidal, Ph.D. Acting Associate Dean for Research and Graduate Affairs	Date

Abstract

Bitcoin is a relatively new topic with limited research into its economic and financial implications. While originally described as a peer-to-peer electronic cash system, Bitcoin has popularly come to be known as the world's first cryptocurrency – an assertion that has generated controversy, yet has received little academic scrutiny. To better understand Bitcoin economics, this thesis led exploratory research identifying Critical Success Factors driving Bitcoin growth and adoption as currency by businesses and individuals. The Critical Success Factors identified were transaction costs, technical efficiency, governance, payment security, distribution, quantity and velocity. Although Bitcoin successfully serves as a fungible medium of exchange, it lacks enough widespread adoption and trading volume to achieve price stabilization – a shortfall significantly diminishing its function as a reliable storage of value. In practice, many merchants also choose to convert bitcoins at the point of sale into other traditional currencies, effectively leveraging Bitcoin as a payment system, rather than a currency on its own accord. In light of these findings, we conclude that Bitcoin is best described as a cryptocommodity rather than a cryptocurrency.

Resumen

Bitcoin es un tema relativamente nuevo cuya investigación sobre sus implicaciones económicas y financieras es relativamente limitada. Aunque originalmente fue descrito como un sistema de pago "peer-to-peer", Bitcoin es popularmente conocido como la primera criptomoneda del mundo – una aseveración que ha generado controversia, pero poco escrutinio académico. Para mejor entender la economía de Bitcoin, esta tésis llevó a cabo una investigación exploratoria para identificar los Factores Críticos de Éxito llevando el crecimiento y adopción de Bitcoin como moneda por negocios e individuos. Los Factores Críticos de Éxito identificados fueron costos de transacción, eficiencia técnica, gobernanza, seguridad de pago, distribución, cantidad y velocidad. Aunque Bitcoin exitosamente sirve como un medio de intercambio homogéneo, carece de suficiente adopción y volumen de uso para alcanzar estabilidad de precio – una carencia que significativamente reduce su habilidad de funcionar confiablemente como reservorio de valor. En práctica, muchos comerciantes también escogen intercambiar sus bitcoins a otras monedas en el momento de venta, efectivamente aprovechando Bitcoin como un sistema de pago en lugar de usarlo como una moneda por su cuenta. A partir de estos resultados, concluimos que Bitcoin es mejor descrito como una "criptomateria prima" en lugar de una "criptomoneda".

Acknowledgements

I would like to extend my gratitude to family and friends who consistently encouraged my research and cheered me on from beginning to end.

- To my fiancée, Sonia, from whom I learned how to stand on my own.
- To my father, Aladino, from whom I learned the power of questions.
- To my mother, Frances, from whom I learned organization.
- To my sister, Daniela, from whom I learned determination.

I would also like to extend my gratitude to my Graduate Committee who served as the guiding force driving the quality of my research.

- Dr. Maria Amador-Dumois
- Dr. Mario Córdova-Claudio
- Prof. Darik Cruz-Martínez

Terminology / Acronyms

- 51 attack – a theoretical vulnerability allowing an attacker controlling the majority of the network's computing power to influence the processing of certain transactions
- ACH – Automated Cleaning House
- BEP – Bureau of Engraving and Printing
- Bitcoin – (singular, upper case B) refers to the protocol, software, and community
- bitcoins – (lower case b) refers to the units of the currency
- BSA – Bank Secrecy Act
- BTC – common unit abbreviation for bitcoins
- CSF – Critical Success Factor
- DGM – Double Geometric Method
- ECDSA – Elliptic Curve Digital Signature Algorithm
- ESMPPS – Equalized Shared Maximum Pay Per Share
- EU – European Union
- INTERPOL – International Criminal Police Organization
- IRS – Internal Revenue Service
- M1 – a measure of the money stock which includes funds that are readily accessible for spending
- M2 – a broader measure of the money stock which includes M1 plus savings deposits, retail money market mutual funds, and small-denomination time deposits
- mBTC – millibitcoin (0.001 BTC)
- NRC – National Research Council

- POS – Point of Sale
- PPLN – Pay Per Last N Shares
- PPS – Pay Per Share
- PROP – Proportional
- SEC – Securities Exchange Commission
- SHA-256 – Secure Hash Algorithm
- SMPPS – Shared Maximum Pay Per Share
- U.S.C. – United States Code
- US – United States
- USD – United States Dollar

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

Bitcoin is popularly known as the world's first completely decentralized cryptocurrency. "Bitcoin solves two challenges of digital money – controlling its creation and avoiding its duplication – at once." (Velde, 2013, p. 2) Its design effectively manages to solve the "double-spending" problem of money being copied online. It represents a new type of asset that is generated and exchanged without the need of a centralized organization. However, the validity of Bitcoin as a currency is doubted by many due to its current level of usage and economic volatility (Ali, Barrdear, Clews, & Southgate, 2014) (Badev & Chen, 2014). This disruptive technology has stimulated conversation across media and motivated entrepreneurs to explore novel ways of approaching payment transactions (Casey & Vigna, 2015). Although its technical design is surprisingly innovative, it remains an open question whether it may reliably serve as a store value (Ali, Barrdear, Clews, & Southgate, Innovations in payment technologies, 2014).

1.1 Bitcoin

Bitcoins are not physical items. Bitcoin are amounts recorded in a file that is publicly shared across the Internet. This file contains all the accounts and transactions that have ever occurred since Bitcoin started – an electronic ledger filled with all debits and credits between accounts. Using network computer science, Bitcoin is able to maintain a single version of this file across the Internet. This consensus prevents counterfeiting and allows the creation of new bitcoins in a controlled, yet decentralized manner.

Although all account balances are publicly visible, account transactions are secured using a special type of password-like system. This way, only its owner controls each account, and third parties are blocked from tampering with the ledger.

All transactions are processed by a decentralized network of computers that run the electronic ledger. Each network node must bundle the data using a special kind of math problem that is difficult to solve, but easy to verify – a statistically random process that is achievable only via constant trial and error. By adjusting the difficulty level of this bundling process, the network is able to regulate the rate at which transactions are added to the ledger and shared across the Internet. Every 10 minutes, only one computer node in the network will find an acceptable solution. To incentivize participation in this process, the network rewards successful nodes with new bitcoins, effectively representing the mechanism by which new bitcoins are created and distributed into the Bitcoin network.

Bitcoin's original whitepaper was published in 2008 under the pseudonym Satoshi Nakamoto. The seminal paper highlights, "Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model" (Nakamoto, 2008). The paper highlights how financial institutions function as mediators, creating an extra level of cost that requires parties to pay fees for processing payments. Faced with the aforementioned limitations of conducting business over the Internet, the paper proposes an electronic payment system that effectively removes dependence on any single trusted third party and instead uses a decentralized network running cryptographic proofs to verify and conduct secure transactions. The cryptographic method proposed in the paper not only laid the foundation for how Bitcoin works, but also what it allows to achieve – electronic peer-to-peer transactions (Brito & Castillo, 2013).

1.2 Justification

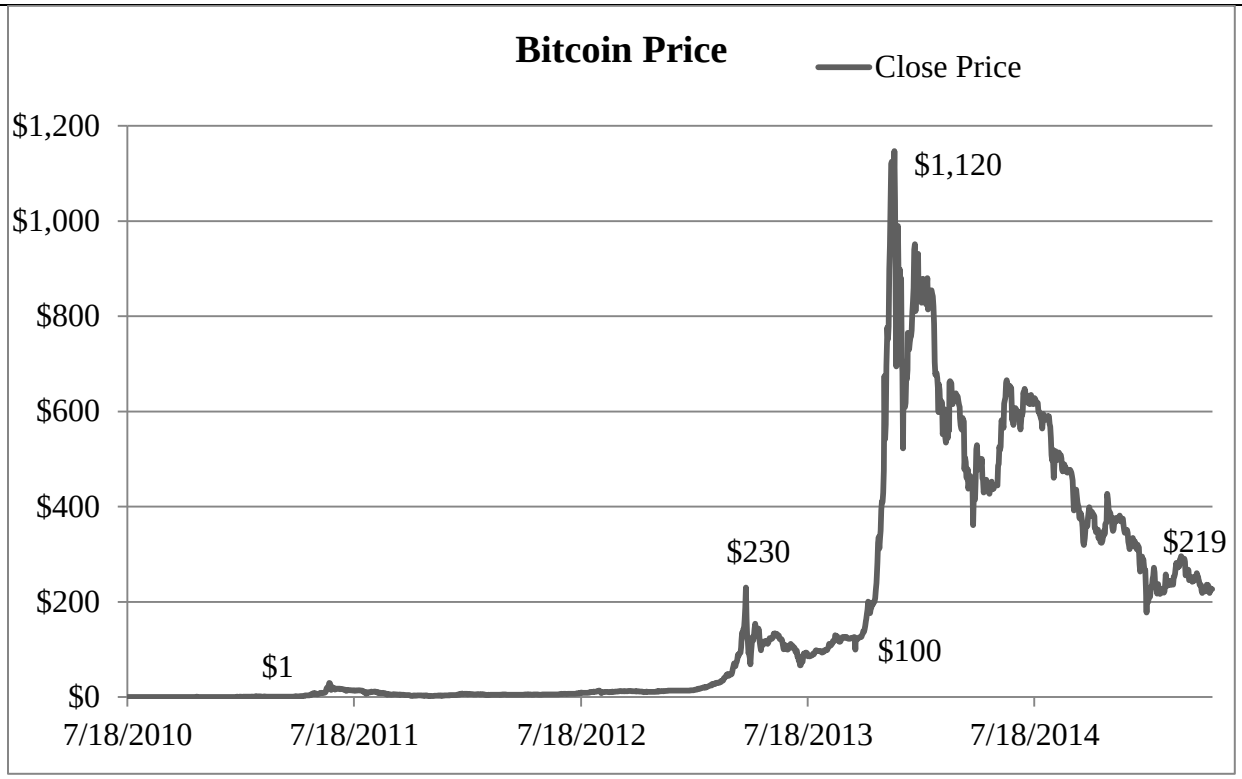
Bitcoin lies at the intersection of several important academic research areas, including cryptography, distributed computing, finance, political science, law, and economics. The combination of these fields is so unique, that widespread academic discourse over the properties of Bitcoin has proved limited. Given the underlying complexity of Bitcoin technology, academic conversations have typically revolved around what it is and how it works. "Even though Bitcoin has been frequently discussed on various financial blogs and even mainstream financial media, the research community is still mainly focused on the currency's technical, safety and legal issues, while discussion about the economic and financial aspects remains relatively sparse" (Kristoufek, 2014, p. 2).

The most controversial aspect concerning Bitcoin appears to be the explanation of why it holds value; the description of which requires not only a deep understanding of Bitcoin, but of traditional money itself. Currency is defined by its three major functions: medium of exchange, unit of account, and store of value (Mankiw, 2014). These characteristics underline the importance of money, not as a valued asset in its own accord, but as a means to allow trade between people. From ancient sea shells and gold coins to modern day fiat currencies, money has evolved throughout history to accommodate ever changing needs and influences. With the arrival of the Internet, people were able to communicate directly with anyone in the world, but were still unable to conduct business as usual without relying on a trusted third party to mediate transactions. Just as money has evolved in the past, it will continue to do into the future.

However Bitcoin does not come without its risks. "Bitcoin potentially allows any user – legitimate or criminal – to transfer money at near instantaneous speed at little or no cost, with very low barriers to entry, while remaining virtually anonymous without what could otherwise

require a public paper trail" (Bryans, 2014, p. 447). This was indeed the case presented by the now defunct Silk Road online marketplace, shut down by the FBI in 2013 (Southern District of New York, 2013). US senators Schumer and Manchin (2011) noted this issue in a public letter to the Attorney General, "The only method of payment for these illegal purchases is an untraceable peer-to-peer currency known as Bitcoins" (Schumer & Manchin, 2011, p. 1). Considering these risks, the FBI (2012) drafted a report on Bitcoin noting it "will likely continue to attract cyber criminals" and that "since Bitcoin does not have a centralized authority, law enforcement faces difficulties detecting suspicious activity, identifying users, and obtaining transaction records" (Federal Bureau of Investigation, 2012, p. 2).

Regardless of these legal risks, Bitcoin has become a notable development in computer science and financial economics. Figure 1 presents the drastic changes in Bitcoin since its introduction in 2009, fueling the motivation of several stakeholders into further studying the potential of Bitcoin and how it may shape the marketplace moving forward. As noted in a Wall Street Journal article, "For all bitcoin's growing pains, it represents the future of money and global finance" (Casey & Vigna, 2015, p. 1).



- 2008 Satoshi Nakamoto published first Bitcoin whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System"
- 2009 Bitcoin protocol was released
- 2010 First Bitcoin exchange, Mt. Gox, was founded
- 2011 Online black-market, Silk Road, was founded and began using bitcoins as means of payment
- 2011 Additional Bitcoin exchanges were founded including BTC China, BTCE and Bitstamp
- 2011 Cryptographic payment system, Litecoin, was released using a modified protocol based of the original Bitcoin code

- 2012 Online gambling website, Satoshi Dice, was founded and began using bitcoins as means of payment
- 2012 Online Bitcoin wallet service, Coinbase, is founded
- 2013 FinCEN issued consumer advisory regarding virtual currencies
- 2013 FBI shut down Silk Road
- 2013 China prohibited banks and payment institutions from using bitcoins
- 2014 Mt Gox filed for bankruptcy after loss of 850,000 BTC (approximately $500M USD)
- 2014 IRS issued guidance on virtual currencies
- 2014 Coinbase launched first US based Bitcoin exchange
- 2014 Bitcoin ETF, Winklevoss Bitcoin Trust, filed prospectus to SEC

Figure 1. Timeline of Bitcoin price. Source: Price calculated from historical data obtained via http://www.coindesk.com/price/. Timeline from (Badev & Chen, 2014)

Bitcoin introduces a new area of study that requires a different set of knowledge beyond the traditional financial economics and law to include technical areas of cryptography and distributed computing, and political science. As such, thoughtful academic research is needed to properly tie these fields together and address how Bitcoin might influence commerce going forward. Considering the need for further clarity on Bitcoin economics, this study adds value by identifying the Critical Success Factors affecting the growth and adoption of Bitcoin as a currency, and analysis on how well these are currently being met. In essence, we seek to identify

and analyze “the limited number of areas in which results, if they are satisfactory, will ensure successful competitive performance for the organization” (Rockart, 1979, p. 3).

1.3 Main Objective and Research Questions

The main objective of this study is to determine whether Bitcoin is a currency. This thesis seeks to generate a cohesive explanation of how Bitcoin compares to traditional currencies and identify the Critical Success Factors driving its adoption and valuation. Our research questions include:

- How does Bitcoin function as a payment system?
- How do these relate to the function as money?
- How do these compare to traditional fiat currencies?
- What characteristics of Bitcoin influence its valuation and economic utility?
- What are the Critical Success Factors driving its adoption as currency?
- How well does Bitcoin satisfy each these Critical Success Factors?
- Is Bitcoin best described as a cryptocurrency or a cryptocommodity?

The purpose of the study is to determine Critical Success Factors to understand how Bitcoin will move forward as cryptocurrency, or otherwise lead to improving the definition of Bitcoin in an economic context. Due to the unique innovations of Bitcoin, few academic studies have been published addressing the economic and financial aspects of cryptocurrencies.

1.4 Limitations

This lack of research represents a limitation to the study in terms of readily available information. In response, information was consolidated from various academic disciplines, requiring a comprehensive study of each in the process. Major topics included cryptography,

distributed computing, and financial economics. It also includes legal issues. Although the scope does not include the areas of political science and negotiations, the results of the study are relevant for policymakers. This exploratory case study focuses only on Bitcoin which means that the findings cannot be generalized to the larger population of "cryptocurrencies". A final key limitation is our focus on non-quantitative design and methodology.

1.5 Research Outline

The research is divided as follows. The second chapter provides a discussion of existing literature including the evolution of traditional currencies and a technical explanation of Bitcoin. The third chapter presents the methodology designed to carry out the main objective of this study. The fourth chapter presents all findings organized into Critical Success Factors. The fifth chapter includes the conclusion and recommendations for future research.

Chapter 2: Literature Review

2.1 Functions and Characteristics of Money

Mankiw (2014), as well as Dieterle & Simmons (2014) describes the three basic functions of money as a medium of exchange, unit of account, and store of value. Medium of exchange constitutes a representation of value used for the trade of good and services. Unit of account allows for the value of dissimilar goods and services to be accounted for and expressed in like terms. Store of value describes the ability to reliably store and retrieve value over time.

Money also possesses six key qualitative characteristics that support how well it serves as medium of exchange in a given economy (Dieterle & Simmons, 2014, pp. 246-247):

- Durability – withstanding physical wear and tear from usage
- Portability – easily carried and transferred
- Divisibility – easily divided into smaller units
- Uniformity – all units are exactly the same and interchangeable
- Limited supply – represents a finite amount to hold value
- Acceptability – recognizable and able to be exchanged as payment

Taken together, these functions and characteristics allows money to be valued not by its own accord, but as a mediating tool to assist in transferring goods and services between agents (McLeay, Radia, & Thomas, Money in the modern economy: an introduction, 2014). It should be noted though that "changes in these properties affect the quality of money and thereby its purchasing power independent from money's quantity or expectation about money's quantity" (Bagus, 2009, p. 32). In practice, anti-counterfeiting measures reflect one of the efforts led by the government to maintain the quality of money. However, beyond these basic functions and

characteristics, money is also typically distinguished as being considered legal tender by a sovereign state. "In this approach, money is a creature of the state. The state defines money as that which it accepts at public pay offices, mainly in payment of taxes" (Wray, 2002, p. 86). However, it should be noted that state money by government decree does not by itself represent a requirement of money, but instead serves to reinforce the use of state money as legal tender to pay taxes. Under this economic and regulatory environment, "all other monies used domestically are denominated in the state money, with their liquidity and acceptability related to (although not strictly determined by) the ease with which they can be converted to state money" (Wray, 2002, p. 103).

Rothbard (2004) also identifies the importance of the purchasing power of money through the relation of its demand and supply. On one side, "the total demand for money on the market consists of two parts: the exchange demand for money (by sellers of all other goods that wish to purchase money) and the reservation demand for money (the demand for money to hold by those who already hold it)" (Rothbard, 2004, p. 756). This demand, at its core, remains tied to the basic utility of money as a medium of exchange, unit of account, and store of value; functions that are affected no only by the quantity of money, but also its quality.

Since money is subject to the market forces of demand and supply, its relationship to price can thus be described as "the intensity of the valuation of money in relation to the valuation of other goods and services on the part of potential buyers and sellers" (Bagus, 2009, p. 29). This description however is "determined at all times by subjective valuations, not by purely objective, quantitative, or mechanical relationships" (Hazlitt, 1983, p. 78). In other words, the value of money and its purchasing power is not equal in all places, at all times. As perceptions

change in relation to the quantity and quality money, so too will its purchasing power shift accordingly. The relationship between the value of money and the value of goods and services is constantly changing in relationship to the demand and supply of both elements concurrently and continuously.

In the context of this thesis we will focus on further describing the importance of money as a reliable store of wealth. Since real world transactions do not occur simultaneously, this would imply that the passing of time is fundamental to the utility of money. Money as a store of value must reliably preserve and retrieve the value for which it was exchanged for at a later time. There are several characteristics of a good store of value including (Bagus, 2009):

- Hoardability – the ability to add and remove small amounts of money from storage at minimal cost
- Expected market utility – subject to future supply and demand, subject to both quantitative and qualitative characteristics
- Integrity – the ability for representative money to be redeemed for an underlying commodity or to settle an underlying liability
- Governance – the risk of government and monetary policy changes

In summary, these characteristics of money are central to the function, value and utility of money in a modern economy. With the increasing use of electronic money within the banking industry, these characteristics have become increasingly subject to forces defined by information technology, rather than physical manifestations of money.

2.2 Bitcoin Core Design

2.2.1 Bitcoin Definition

Bitcoin is a peer-to-peer electronic cash system that allows for secure transactions over a decentralized network. It is the first payment system of its kind and is popularly called a type of cryptocurrency. The original creator(s), known only by the pseudonym Satoshi Nakamoto, published the original Bitcoin paper in November 2008 and officially launched the network in January 2009 using the first open-source Bitcoin client. (Olafsson, 2014)

The payment system is possible due to revolutionary advances in encryption and networking solutions based heavily on hash cryptography. These innovations allow for pseudo-anonymous transactions that protect against double spending and counterfeiting. The computational power required to encrypt these transactions is provided by decentralized contributors motivated by reward. Other similar cryptocurrencies have emerged with similar frameworks and are collectively referred to as altcoins.

2.2.2 Overview

Due to the novel use of networking and encryption solutions that make cryptocurrencies possible, it is important to establish a firm understanding of key concepts and terminology. The basic conceptual framework of operation is popularly presented as follows (Bitcoin.org, 2015):

- *Ledger - Block chain*

The block chain represents a shared public ledger where all bitcoin transactions are stored. This transaction database is shared by all nodes participating in the network and is encrypted via hash cryptography. This is the main innovation of Bitcoin and protects the network against double-spending.

- *Transactions – Public-key cryptography*

Bitcoin uses public-key cryptography to allow secure transactions. This method uses keypairs, a private key and public key, to authorize transactions as being authentic from respective Bitcoin wallets. Private keys must be kept secret since they constitute the unique code allowing bitcoins to be spent, even though all transactions stored in the block chain are publicly broadcasted.

- *Processing – Mining*

Mining is the process by which transactions are encrypted and included in the block chain. The block chain itself is an encrypted cryptographic hash that is obtained using computational brute force. This ensures chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system.

2.2.3 Block Chain

The big revolution of Bitcoin is solving the double spending problem, mitigating the risk that a user may spend an electronic coin more than once. This was a fundamental weakness of traditional digital cash since it would allow fraudulent transactions to take place. To address this issue, electronic cash has traditionally relied on online third parties, tamper-proof hardware, or client accounts at the bank, all three of which pose scalability challenges and single-point of failure risks (Osipkov, Vasserman, Hopper, & Kim, 2007). To address these weaknesses, Bitcoin was designed to use the block chain, a network solution using cryptography and computational power to produce a secure public ledger.

For the sake of illustration let's assume two users, Alice and Bob, intend to do business together online. In the physical world, Alice could walk up to Bob and exchange physical money for goods and services. This approach is commonplace and assumes effective bill forgery

protection is in place to deter counterfeiting. In the digital world however, information can be easily copied and there are no immediate measures preventing Alice from sending Bob an electronic coin, only to immediately turn around and re-spend the same coin in a second transaction without Bob's knowledge. There are now two copies of the same coin in circulation and no reliable way of verifying which coin originated from the first legitimate transaction. Alice has effectively double-spent a single coin and introduced a counterfeit into the network, effectively undermining trust in the system.

Businesses have traditionally addressed this risk by using centralized electronic payments systems offered by banks, credit cards companies, and other payment intermediaries. These central authorities are trusted in to accurately manage and vouch for the cash and credit limits of its members. Before the creation of the Bitcoin protocol, there was no way of conducting digital transactions without relying on a discrete third party to verify funds.

To prevent this, Bitcoin uses a payment system based of cryptographic proof instead of trust, allowing parties to complete transactions directly without the need for a third party. These transactions would be computationally impractical to reverse and allow users to verify the chronological order of transactions, termed the block chain (Nakamoto, 2008)

The system defines each electronic coin as a chain of digitally signed transactions. By publicly announcing all transaction to the network, anyone can track the chain of ownership and verify the electronic coin has not been spent before. Since there is no central authority, the majority of nodes must agree on a single history. A consensus is achieved via mining, a process by which a transaction and is coded into the block chain and broadcasted throughout the network.

The block chain is also unique for its application of SHA-256, an advanced cryptographic hash function, to encode transactions and add them to each generated block. At the fundamental level, hashing encrypts a variable-sized data input into a fixed-sized data output by applying a mathematical transformation. The resulting data output is known as a hash. By applying advanced techniques to the creation of the hashes contained in each block, the block chain can effectively pack large amounts of data into a small packet of information and almost instantaneously propagate the block through all connected nodes in the network (Badev & Chen, 2014).

To corroborate the chronology of the block chain, the bitcoin protocol adds a timestamp to each block as proof that the data must have existed when the block was generated. The timestamp is hashed along with current transactions and the previous block to create a new block. The process of each new block being generated including the previous block conceptually forms a chain. This chain is the basis for the term block chain, a chain of blocks within blocks. Since previous blocks are rehashed into new blocks, each additional timestamp and related transactions are reinforced. In practice - thanks to the design of the protocol and the distribution of the network - the block chain is effectively unchangeable, irreversible, invulnerable to counterfeits, and unobstructed by the efforts of any single node in the network (Nakamoto, 2008).

This approach characterizes how the public ledger is conceptually put into practice. It represents a solution through which all secure transactions are broadcasted through the network, encrypted into the block chain, and are publicly verifiable by everyone.

2.2.4 Secure Transactions

To ensure individual transactions are executed and within the control of each respective user, Bitcoin uses public key cryptography to transfer data securely. It is important to begin by understanding that each bitcoin does not represent a single packet of information. Bitcoins are represented as a series of transaction, encrypted into the block chain, and spent using digital signatures.

Key concepts underlying Bitcoin transactions are as follows:

- A wallet is a file that contains a collection of public/private keypairs
- An address is a 160-bit hash of the public portion of a keypair
- Output amounts are always received by an address
- Each output is locked to the receiving address and consequently termed an unspent transaction output
- Unspent transaction outputs can only be unlocked using the private key associated with the receiving address
- Addresses are intended to receive bitcoins only once as single discrete unspent transaction output
- An unspent transaction output cannot be split into small amounts
- Transaction inputs are attained by grouping the unspent transaction outputs tied to one or more addresses
- The difference between the input and output represents the change of a transaction and is sent as a separate output to an address owned by the sender
- Any amount not accounted for between the primary transaction and the change transaction is offered to the network as a transaction fee.

Let's consider an example where Alice sends 10 BTC to Bob. First, we are reminded that Alice does not technically send 10 BTC from an undifferentiated pool of 50 BTC in her wallet. Instead, she groups and three unspent transaction outputs of the following amounts: 3, 4, and 5 BTC. These unspent transaction outputs are "unlocked" using each address' corresponding private key and assigned as the input for the new 10 BTC transaction. The entire 12 BTC sum of the inputs is "spent" in the process; 10 BTC is sent to Bob and 2 BTC to Alice as change. From this transaction each party receives BTC as a single output to an address, forming the unspent transaction output of a future transaction. Optionally, Alice may have also offered a transaction fee to the network as a way to prioritize the transaction.

To keep each user's unspent transaction outputs secure, Bitcoin clients use cryptographic algorithms to ensure these funds can only be spent by their rightful owners. This approach is also used by banks, the NSA, and other information-sensitive organizations to ensure secure communications over the Internet. As a point of reference, Internet users may sometimes notice a small padlock icon in their browser window indicating the use of a cryptographic algorithm when using certain secured websites.

Public-key cryptography, also known as asymmetric cryptography, is used to encrypt and decrypt data using a pair of two different keys; one private and one public. This keypair is mathematically linked in such a way that it is infeasible to determine the private key from the public key, and any data encrypted using the public key can only be decrypted using the private key. This encapsulates the underlying concept of one-way trapdoor functions; easy to compute in one direction, yet difficult to compute in the opposite direction.

There are several modern cryptographic algorithms available to achieve this including the RSA encryption algorithm and the Diffie-Hellman key exchange protocol. However, Bitcoin primarily uses the Elliptic Curve Digital Signature Algorithm (ECDSA) which allows the same level of security as previous mentioned alternatives using a smaller key size. In short, ECDSA is a process that uses an elliptic curve and a finite field to "sign" data. Specifically, the parameters used in Bitcoin's elliptic curve and finite field are predefined under secp256k1. The mathematics behind describing elliptic curve cryptography is complex and beyond the scope of this thesis, however it is important to note that the selection of ECDSA is central to the reliability of Bitcoin's network security and no known methods exist that can break these keys other than infeasible computational brute force (Bos, Halderman, Heninger, Moore, Naehrig, & Wustrow, 2014).

2.2.5 Processing - Mining

In essence, mining describes how the block chain is created through the distributed computational effort of the network; a framework that balances cryptographic hash functions, probability, computing power, and networking, to allow for the decentralized generation and propagation of the block chain. The incentive to participate in this network process is driven by the opportunity to claim a bitcoin award every time the miner is able to generate the next accepted block in the block chain.

Central to the process of mining itself is Proof-Of-Work; a concept that combines cryptography, probability, and the collective processing power of the network. This combination ensures that the system remains decentralized and that ultimately only a single transaction history is acknowledged by everyone.

Proof-Of-Work operates thanks to cryptographic hash functions, a type of mathematical transformation that may be used to represent information of variable length as a fixed amount of characters. The transformation process occurs in such a way that hash are functions considered to be asymmetric – "easy to compute in one direction, yet believed to be difficult to compute in the opposite direction" (Myasnikov, Shpilrain, & Ushakov, 2011, p. 74). As hash functions have become more elaborate, it is possible to produce hashes that are also considered unique for any given input. Any change to the input would result in entirely different hash value. Therefore, sophisticated cryptographic hash functions not only allow obtaining fixed-size outputs, but also unique hashes that are practically undecipherable yet easily verifiable. These properties are central to the design of various information security applications including password privacy.

There are several mathematical variants of cryptographic hash functions; Bitcoin specifically adopted SHA-256. "SHA" stands for Secure Hash Algorithm, was developed by the NIST in association with the NSA and was first published in May 1993 as the Secure Hash Standard (Penard & van Werkhoven, 2008). There have been several developments since it was initially made public, including the release of SHA-256 along other modern variants in 2001. These most recent hash functions are valuable for their reliability at upholding the four main properties of an ideal cryptographic hash function:

- It is easy to compute the hash value for any given message
- It is infeasible to generate a message from its hash
- It is infeasible to modify a message without changing the hash
- It is infeasible to find two different messages with the same hash.

Proof-of-Work leverages these cryptographic properties by partially combining the first two. Via network agreement, the bitcoin protocol requires that each new block contain a predetermined sequence of character at the beginning of its calculated hash value. Since each unique input will result in a unique output, this condition is unlikely to be met. If the condition is not met by the original input, then the only way to try again is to modify the input. However, since the outputs are unpredictable, the probably that the modified input will satisfy the condition remains equally unlikely no matter how the input is modified. There is no easy way to find an acceptable hash value. A solution can only be found via trial-and-error.

In practice, a computer will add a random piece of data to the end input - called a nonce -, to calculate the hash value, compare the output to the preset requirement, and repeat if the condition is not met. A single cycle of calculating a hash value with modern computer processors can occur almost instantaneously. However, depending on the probability of finding a solution, there might not be another alternative than to continue running trials until a solution is found. A sufficiently challenging requirement can be so computationally demanding that the probability of finding a solution through trial-and-error is very low.

However, in spite of the outcome being very unpredictable, calculating the probably of finding it is not. It is possible to statistically estimate the number of trials usually needed to find a desired output. By combining this measure of probability along with the number of trials conducted per second, it is possible to calculate how much time is expected for a solution to be found. In practice, this allows for the network to auto-calibrate and set a predetermined hash value requirement that can reliably be expected to be solved every 10 minutes. No matter how

much computer processing power is added to the network, the system can always recalibrate to adjust the difficult level and consistently maintain a 10 minute block generation rate.

In stark contrast, it is very easy to verify a solution as true when given the corresponding input. Thus Proof-Of-Work offers a cryptographic approach that is extremely hard to encode, yet very easy to validate. Only a genuine solution will be accepted by other nodes in the network, creating a competitive validation process that prevents untrue solutions.

The statistical random property of Proof-Of-Work also ensures that there is no bias in the network and supports a decentralized mining environment. In practice, nodes are successful depending on computer processing power. Moreover, it is also unlikely any one node can forcibly influence the network, since doing so would require controlling more that 50% of the collective network computing power. However, it is critical to point out, that the level of influence is very limited and unlikely produce any persistent negative effects on the security and reliability of the network.

To incentivize the participation of miners to generate new blocks, the bitcoin protocol rewards a set amount of bitcoins for each successful block generated – starting at 50 bitcoins in 2009 and halving the reward every 4 years. The term mining is inspired by parallels to gold mining, given the fact that this halving process mathematically implies only a set amount of bitcoins ever be introduced into the network; effectively meaning Bitcoin is a finite resource similar to common natural resources such as gold. There is no central authority that can "print" more bitcoins once the algorithm has run its course for several years. Miners will thus receive an incentive to continue operating solely on transaction fees offered by the system. Per the current

network protocol, a maximum of 21 million bitcoins will be produced by year 2140; however, the decreasing reward curve will have reached 99% of Bitcoins by the year 2032.

Bitcoin addresses many of these issues by creating near real-time double-spending detection. The Block Chain encrypts all transactions using hash cryptography and creates a secure public ledger where anyone can verify funds spent and received.

It is clear that the technical design of Bitcoin is well thought out, relying on novel cryptographic and network approaches. However, in light of Bitcoin's emergence as a noteworthy economic asset, research into its financial aspects is needed.

Krištoufek Ph.D. plainly points out, "Even though Bitcoin has been frequently discussed on various financial blogs and even mainstream financial media, the research community is still mainly focused on the currency's technical, safety and legal issues, while discussion about the economic and financial aspects remains relatively sparse" (Kristoufek, 2014, p. 2).

Chapter 3: Methodology

This study conducted exploratory research on the Critical Success Factors driving Bitcoin economic growth and development. Specifically, research drew comparisons to the US dollar as a point of reference, which ultimately warranted the design of a new comparative framework. To address the goals of this study, a qualitative case study method was employed in support of the exploratory nature of the research.

3.1 Research Strategy Selection

In support of encouraging qualitative research, Starr (2014) pointed out the commonly held misconception that quantitative research analyzes numerical data using statistical/econometric methods, while qualitative the latter uses data expressed in words and analyzed some other way." Information is not unambiguously separated into numerical and conceptual categories. The key distinction between the two lies in approach is thus; qualitative research gravitates towards an open-ended nature of data collection, and quantitative research gravitates towards information available in predetermined research instruments. Qualitative studies recognize the need for a relative flexibility in information gathering to gain complete insight into the phenomenon of interest. In contrast, quantitative studies assume *a priori* that the researcher knows the central variables. (Starr, 2014)

An open-ended approach to data collection in qualitative research typically yields more diverse information than close-ended approaches, and thus typically warrants a greater depth of complex analysis. Given this contrast, Starr (2014) defines several key circumstances that motivate and justify qualitative research:

- When very little is known about the topic, so that broad exploratory research is needed to identify its basic characteristics
- When there has already been a lot of quantitative research on the subject, but key questions remain unresolved
- When back-and-forth with an interviewer is thought to be needed to help elicit full and accurate information
- When the topic under investigation has some inherent complexities the researcher wants to be able to capture
- When the respondent's own views of their own situation are of inherent interest

Bitsch (2005) also defined the purpose of qualitative research approaches as being especially suited for studies addressing "the description and interpretation of new or not well-researched issues, theory generation, theory development, theory qualification, and theory correction, evaluation, policy advice, and action research, and research directed at future issues" (Bitsch, 2005, p. 2).

3.2 Study design

Keeping in mind research goals, a qualitative and model building approach was leveraged to allow greater insight into the underlying meaning behind our phenomena. Creswell (2013) reinforces this method, highlighting how an emerging qualitative approach to inquiry can meaningfully contribute to the literature. More precisely, our study design encapsulates Case Study research, as it takes into account the relevance of Bitcoin as a contemporary bounded system and the requirement of collecting multiple sources of information to achieve in-depth understanding.

Preliminary research revealed that Bitcoin economic theory remained underdeveloped, generating significant confusion in both the public and academic discourse. To address this inadequacy, exploratory research was conducted to produce a sound framework and effectively consolidate essential findings.

Key concepts for this approach included theoretical sensitivity and theoretical/purposeful sampling so that in-depth understanding is allowed to emerge from the research process. Specifically, theoretical sensitivity refers to the attribute of having insight and the capability to separate the pertinent from that which not. Correspondingly, theoretical sampling refers to sampling decisions that are grounded in the emerging concepts that become relevant to the research process (Baskarada, 2014); an approach consistent with Creswell's (2013) emphasis of purposeful sampling as showing different perspectives on the problem.

In line with the research principles set forth by Maxwell (2013) and Bitsch (2005), we pursued an interactive study design aimed at promoting constant conceptual review and refinement of theory development. The process of identifying and developing an adequate theoretical model consisted of the following main phases:

1) *Data collection phase*

A combination of academic databases, public resource directories, and institutional/government portals were used to carry out a thorough search of relevant articles.

Due to Bitcoin's relative novelty and scarcity of available research, indirect data collection was often required which resulted in capturing copious papers on related subject matter. Key academic articles were confirmed as being peer-reviewed, although select Bitcoin related information was mainly available on open content websites. Non peer-reviewed

information was validated through extensive scrutiny of developer documentation and key related forums.

2) *Data classification phase*

All articles were reviewed for relevance and grouped according to subject matter. Papers with common topics were organized in order of academic reliability depending on factors including: peer-review status, year of publication, institutional source, and number of citations in other papers. More than one classification may be attributed to individual articles.

3) *Data analysis phase*

Articles were systematically examined and questioned to achieve increasing levels of insight and implications. Key concepts not sufficiently explained in individual articles were marked for follow-up. In subsequent reexaminations, articles were prioritized for effectively unifying major concepts identified as critical success factors. Conducting several rounds of reexaminations helped prune redundant articles and reinforce influential papers.

4) *Data comparison phase*

Grouped articles were compared against each other to test the clarity of conceptual boundaries. Tightly bound conceptual clusters were consolidated and tested against multiple possible arrangements. Emergent relationships became apparent as primary clusters were reinforced through numerous rounds of reexamination.

5) *Theory development phase*

Concept clusters were compared against traditional currencies and generated preliminary critical success factors. Examining articles on traditional currencies played a central part in theory development. After thorough review, analogous concepts emerged between the two,

which further reinforced conceptual clusters. After an exhaustive reexamination of critical success factors, theory development was deemed complete.

We visualize the flow of our methodology as shown in the figure below, reiterating the importance of refining our analysis so we may confidently derive and analyze Critical Success Factors moving forward.

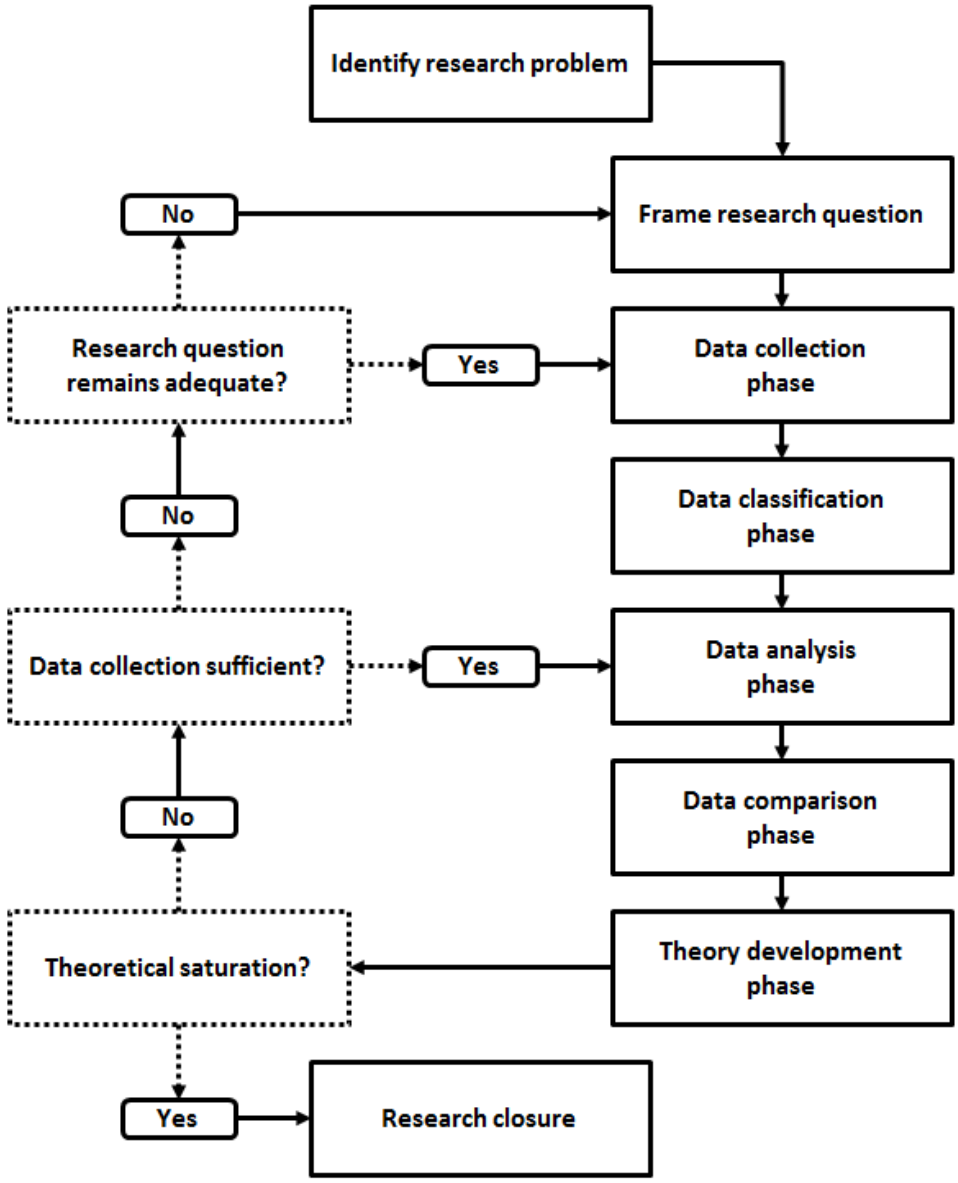


Figure 2. Methodology flowchart.

In summary, given the wide range of topics required for this study, the researcher concluded that a qualitative research approach oriented towards discovery, description, and interdisciplinary understanding of processes was a suitable point of departure. The Critical

Success Factors identified ultimately led to achieve a better understanding relevant economics considerations and the development of a more accurate conceptual framework. To ultimately answer our research question of how Bitcoin functions as a payment system, how it functions as a type of money, how it compares to current currencies, which are the Critical Success Factors to achieve its adoption, and how it may be best described as a cryptocurrency or a cryptocommodity.

Chapter 4: Findings

The Critical Success Factors identified were transaction costs, technical efficiency, governance, distribution, quantity and velocity, and payment security. This section divided the discussion of each Critical Success Factor into two segments: a description as applied to traditional currencies, and a description as applied to Bitcoin. This division allowed for an effective introduction of each CSF's significance within a traditional economic model, and what this ultimately translates into with regards to Bitcoin.

4.1 Critical Success Factors

Considering the changing landscape of money and payment technology, the scope of this thesis seeks to identify the Critical Success Factors (CSF) as a means of comparing the existing paradigm of money with the innovations presented by Bitcoin. The Critical Success Factor approach was first introduced by Daniel in 1961, and later popularized by Rockart in 1979, the latter of which broadly defined them as "the limited number of areas in which results, if they are satisfactory, will ensure successful competitive performance for the organization" (Rockart, 1979, p. 3). Rockart also noted the distinction between goals and CSFs: "Goals represent the end points that an organization hopes to reach. Critical success factors, however, are the areas in which good performance is necessary to ensure attainment of those goals" (Rockart, 1979, p. 3). Bullen and Rockart (1981) expanded the discussion to identify the four hierarchical levels of CSFs: industry, corporate, sub-organization, and individual. In this thesis, we focus on describing industry level CSFs addressing the principal factors that underlie Bitcoin vs traditional currencies. We note that Bitcoin, although inspiring the creation of similar

cryptocurrencies, remains the principal manifestation of this unique asset class, and as such, carries with it the weight of the industry.

Bullen and Rockart (1981) also identified five prime sources of CSFs that should be considered whenever research is being conducted: industry, competitive strategy, environmental, temporal, and managerial. Considering these sources, CSFs means to consider all possible elements that influence success and ultimately identify those that are most important. Caralli (2004) proposed a structured five step approach for analyzing collected data and deriving CSFs: defining scope, collecting data, analyzing data, deriving CSFs, and analyzing CSFs.

These basic activities ultimately lead to identifying, rather than creating, CSFs – a distinction that highlights the preexistence of factors, regardless of them being known or not. During the analyzing stage, raw data is transformed into CSFs by using a series of repeatable and consistent processes. Considering the data available, processes may include developing activity statements, performing affinity grouping, and developing supporting themes. Defined broadly, these activities enable "the categorization of data that share common characteristics, traits, or qualities so that a common description of the data can be developed" (Caralli, 2004, p. 72). During this analysis stage, groupings may merge and divide, contingent on the constant feedback of clarifying and organizing data.

Deriving and analyzing CSFs describes the process composing the fewest number of factors that still manages to comprehensively characterize the scope defined. Once these are identified, affinity analysis is applied to clarify relationships between CSFs and draw conclusion about their importance. By conducting a thorough study, the CSF process seeks to make factors

explicit, rather than merely implicit a process that exposes actual success factors from those that might have merely been initially perceived (Ellegard & Grunert, 1992).

To arrive at these conclusions, there is a variety of research methods available including: action research, case studies, Delphi technique, group interviewing, literature review, multivariate analysis, scenario analysis, and structure interviewing (Amberg, 2005). In this thesis, we explore CSFs of Bitcoin economics using the case study and literature review methods to collect and analyze data. To derive these factors, this study focused on collecting data from government, institutional, and academic sources to establish the foundation of our analysis moving forward. The following table presents a summary of our findings, which are described in more detail in subsequent sections.

Critical Success Factors	**Summarized findings**
Transaction Costs	– "All the costs which do not exist in a Robinson Crusoe economy" (Cheung, 1998, p. 515) – May be described in three categories: o Search and information costs o Trading and processing costs o Policing and enforcement costs – Bitcoin shifts macroeconomic costs away from government and central institutions by using a decentralized network – Bitcoin employs transaction fees, voluntary bitcoin payments to incentivized timely processing – These transaction fees are influenced by the size of transactions in terms of computer memory consumed – Payment using many small unspent outputs uses more computer memory vs one large unspent output
Technical Efficiency	– Describes the efficiency of a payment system infrastructure enabling transfer of monetary value between parties discharging mutual obligations (Bossone & Cirasino, 2001) – Must consider cost effectiveness and physical performance of payment system

	– Addresses how deposit money, credit, liquidity, and fraud risk is managed by a payment system, including timing delays in handling payments – With Bitcoin, every transaction requires computer memory to be digitally signed and executed, a process dependent on the total bytes being processed. – Bitcoin generates a block every 10 minutes on average – Consensus and block chain forking influences the integrity of transactions
Governance	– "One of the direct powers of Congress under the U.S. Constitution, grants the authority 'to coin Money' and 'regulate the Value thereof' " (Elwell, Murphy, & Seitzinger, 2015, p. 9) – IRS defines bitcoins as property rather than currency, thus requiring payment of taxes on trade – Consumer Financial Protection Bureau has issued consumer advisory – Securities and Exchange Commission has prosecuted businesses for offering publicly traded securities without proper registration, yet is currently evaluating a prospectus for a NASDAQ exchange-traded fund – Financial Crimes Enforcement Network requires Bitcoin exchanges/businesses to register as a money services business and comply with the Bank Secrecy Act – Board of Governors of the Federal Reserve System requires following Bank Secrecy Act / Anti-Money Laundering Examination Manual – Allowed in US, but restricted in China/Russia – Government control of Bitcoin governance is unlikely, except over businesses and exchanges ("off-ramp") – Bitcoin governance subject to Nash equilibrium of the network due to consensus and forking
Distribution, Quantity and Velocity	– The quantity of money is often referred to as money supply, which describes the total amount of monetary assets available in an economy at a specific time – Velocity of money is the frequency at which one unit of currency is used – May be influenced by changes in real interest rates, expectation of inflation, financial innovations that reduce the cost of transferring funds, and cyclical factors such as changes in real income and money growth – With Bitcoin, decentralized distribution occurs via mining – Depth of Bitcoin exchanges is limited – Analysis of addresses suggests bitcoins are largely held as a form of investment – High volatility and large swings in transaction volume correlated with price movements suggests Bitcoin is influenced by speculative bubbles and implies limited retail usage
Payment Security	– The US National Research Council's (NRC) Committee on Next-Generation Currency Design (Williams & Anderson, 2007) described the features of a "perfect" currency including difficulty to duplicate, recognizable, durable, machine-readable, easy to produce at low cost, and non-toxic. – With regards to traditional electronic payment systems, there are robust

	protections available to users of popular electronic payment systems, with Bitcoin all transaction are final – Traditional currencies shift burden of fraud usually falls on merchants and merchant banks – Studies by the Federal Reserve continue to raise concerns since current regulations of traditional electronic payment systems do not incentivize all parties involved to actively participate in fraud reduction – Bitcoins uses public-key cryptography, in which there no known methods to break the keys other than infeasible computational brute force – Bitcoin maintains limited risk of network attacks such as the 51 attack – Major source of fraud is theft of private keys, such as in the case of Mt Gox

Table 1. **Summarized findings per Critical Success Factor**

In our next section we identify Transaction Costs as a Critical Success Factor due to its relationship with both transactional and macroeconomics costs of doing business.

4.2 Transaction Costs

4.2.1 Description as applied to traditional currencies

Economics for the most part seeks to explain supply and demand, usually focused on operational costs of production and pure market demand. However, this approach largely omits costs associated with realizing transaction between sellers and buyers. We find that transaction costs in general may be described into three categories, described below (Dahlman, 1979). In this thesis, we broaden these categories to include macroeconomic costs incurred to support the production and circulation of traditional currencies. Broadening these categories is consistent with Cheung's (1998) wide definition of transaction costs as "all the costs which do not exist in a Robinson Crusoe economy" (Cheung, 1998, p. 515); in other words, any macroeconomic costs enabling the operation of a modern economy. "Variations cover the incomes of lawyers, financial institutions, policemen, middlemen, entrepreneurs, managers, clerks, civil servants, ... just about all the conceivable costs in society except those associated with the physical processes

of production and transportation." (Cheung, 1998, p. 516). For example, the government costs incurred in printing money, managing financial institutions, and maintain a secure interbank electronic exchange are paid for by levying fees/taxes over transactions – be these explicitly shown at the point of sale or implicitly included in the costs of goods and services. These transaction cost categories are broken out as follows:

Search and information costs associated with facilitating relevant information between agents. May be crudely thought of as, costs incurred before a transaction. A straightforward example is the costs required to maintain a stock exchange, an institution that facilitates agents coming together. A broader example may also include costs incurred to access Internet commerce, likewise a medium enabling buyers and sellers to come together, communicate, and compare prices. However, given the multiple payment methods available to facilitate online transactions, agents may also incur additional costs to find counterparts handling a common payment system and potentially suffer opportunity costs if transactions are prevented because of incompatible currencies or payment methods.

Trading and processing costs associated with achieving reasonable agreements between agents. May be crudely thought of as, costs incurred during a transaction. This category includes the direct costs incurred to draft contracts and handle payment processes, but also the indirect costs exerted by macroeconomic forces such as monetary policy decisions, institutional risk taking, and international currency markets. For example, the cost of printing of money and maintaining a secure interbank exchange system is ultimately paid through taxes and fees, while the ripple effect of interest rates are directly influenced by Wall Street and the Federal Reserve. Debt instruments such as mortgages and credit card transactions directly increase the ultimate

costs of transactions by requiring interest payment. Payment systems such as point-of-sale (POS) devices are financed by businesses. International purchases often incur currency conversion fees. Sending cash may entail shipping, handling, or escrow account fees. We point out that all these hidden bargaining costs stem from the need to execute transaction and are ultimately paid for by the collective contribution of agents in the market. (United States General Accounting Office, 2004)

Policing and enforcement costs associated with monitoring and controlling transactions from a legal standpoint. May be crudely thought of as, costs incurred after a transaction. This category includes direct costs such as legal actions taking to enforce a contract between two agents and the indirect costs of government anti-counterfeiting efforts. In the US, the Secret Service is currently responsible for leading investigations and seizures of fake money, while international organizations such as INTERPOL assist law enforcement between varying national jurisdictions to control counterfeiting abroad. Likewise, indirect costs are also incurred during the printing process to enhance paper money with multiple levels of protection, costing many countries around 10 cents per note on average (United States Treasury Department, 2006).

In summary, transaction costs are subject to varying levels of direct and indirect costs needed to sustain the reliability of money and the integrity of the transactions taking place. Valuable developments such as credit cards systems and currency anti-counterfeiting measures so far have enabled traditional currencies to remain the primary medium of economic transactions worldwide. In the next section, we compare how Bitcoin differs from traditional currencies within the scope of the previously defined categories, and reinforce our findings with detailed explanations of the transaction fees directly tied to completing Bitcoin transactions.

4.2.2 Description as applied to Bitcoin

Search and information costs associated with Bitcoin primarily involve the direct costs of setting up a device with a Bitcoin wallet and maintaining an Internet connection. However, it is important to note that these costs are shared with the additional functions of Internet-enabled devices and the wallet application itself is open-source.

Trading and processing costs associated with Bitcoin is the key category affecting transaction costs. There are two main drivers: the direct cost of transaction fees incurred during individual transactions, and the indirect cost of mining to process the block chain. Since mining requires computer processing power, miners will incur hardware, networking, space, and energy costs to continuously run their respective network nodes. These costs are scalable with the difficulty level of the Bitcoin network and are directly related to the profitability of each node. We will further explain how Bitcoin transaction fees – also known as miner fees – work in the subsequent segment below. With regards to other trading cost, the processing fees levied by financial institutions are avoided since Internet transactions via Bitcoin do not require third party intermediaries. There are also no government printing costs since Bitcoins are not physical objects. Likewise, there are no shipping costs associated to distributing physical money, nor the need to periodically replace notes when reissuing new versions.

Policing and enforcement costs associated with Bitcoin to deter counterfeiting is not needed since the Bitcoin protocol makes it computationally impossible to do so as long as there are enough independent nodes in the network. No law enforcement initiatives are required to investigate counterfeiting criminal organizations, and there is no need to invest in printing physical notes. However, since Bitcoin relies on the integrity of its cryptography, there will

always be costs associated in researching more secure encoding moving forward. In the following segment we will explain how miner fees work as mentioned under the trading and processing costs category:

Bitcoin transaction fees – also known as miner fees – are small voluntary payments on the part of the user to ensure transactions are processed and verified quickly. Miner fees are useful since Bitcoin miners are not obliged to include any particular transactions in a newly generated block; in other words, miners are free to intentionally exclude transactions during the mining process and prioritize only those offering payment. This incentive is not directly dependent on the value of the transaction taking place, but rather the size of the transaction in term of computer memory consumed. The larger the size of the information being processed, the more miner fees would be needed to effectively motivate miners to prioritize a transaction. (Kroll, Davey, & Felten, 2013)

The technical explanation considers how every transaction requires computer memory to be digitally signed and executed, a process dependent on the total bytes being processed. We recall that bitcoin are not physical units, but are in fact only represented as a record of transactions in the block chain – the shared Bitcoin ledger. Therefore, when a user received Bitcoins, these are not simply mixed into an undifferentiated pool of other Bitcoins, but rather stored as individual records of varying amounts. By convention, each of the most recent stored record is known as an "unspent output".

When a user sends a payment, unspent outputs are added up in value to an amount equal to or greater than the desired output. The receiver will in turn obtain a single unspent output, regardless of the number of inputs combined, while the difference between the aggregate input

and the desired output is returned to the sender as change in the form of a newly recorded unspent output. Any Bitcoin amount not accounted for between the unspent output, the output, and the change, is considered a transaction fee to be collected by the miner.

Hence, given the numerous combinations of unspent outputs adding to any given desired amount, not all transactions are created equal in terms of size; variations in size are proportional to the number of "unspent outputs" required to execute a transaction. To protect the integrity of the network, rules are set in place to regulate how transactions of varying sizes are prioritized. As of when this thesis is written, the popular bitcoin client Bitcoin Core currently defaults to 0.1 mBTC (0.0001 BTC) per thousand bytes. Other clients follow similar settings. There is no direct way to know the size of a transaction until after the transaction has taken place since digital signatures can vary in length (Moser & Bohme, 2015). Additional rules also offer exceptions to the client's minimum transaction fee setting when the certain requirements are met. These may include a small transaction size and prioritization due to age.

These common rules and restrictions are not only aimed at promoting transaction fees for miners, but also helps prevent malicious low-value transactions from flooding the system. Although transaction fees are not required by the network protocol, the size limit of each new block strongly supports its use since every transaction must compete for limited space.

Blockchain.info, a prominent bitcoin company, tracks daily transaction fees paid. As shown in the figure below, daily total fees have hovered slightly over 10 BTC for the last 12 months, supporting the common argument that bitcoin miners will eventually rely on these fees as their primary source of revenue as bitcoins awarded are decreased over time per the bitcoin protocol.

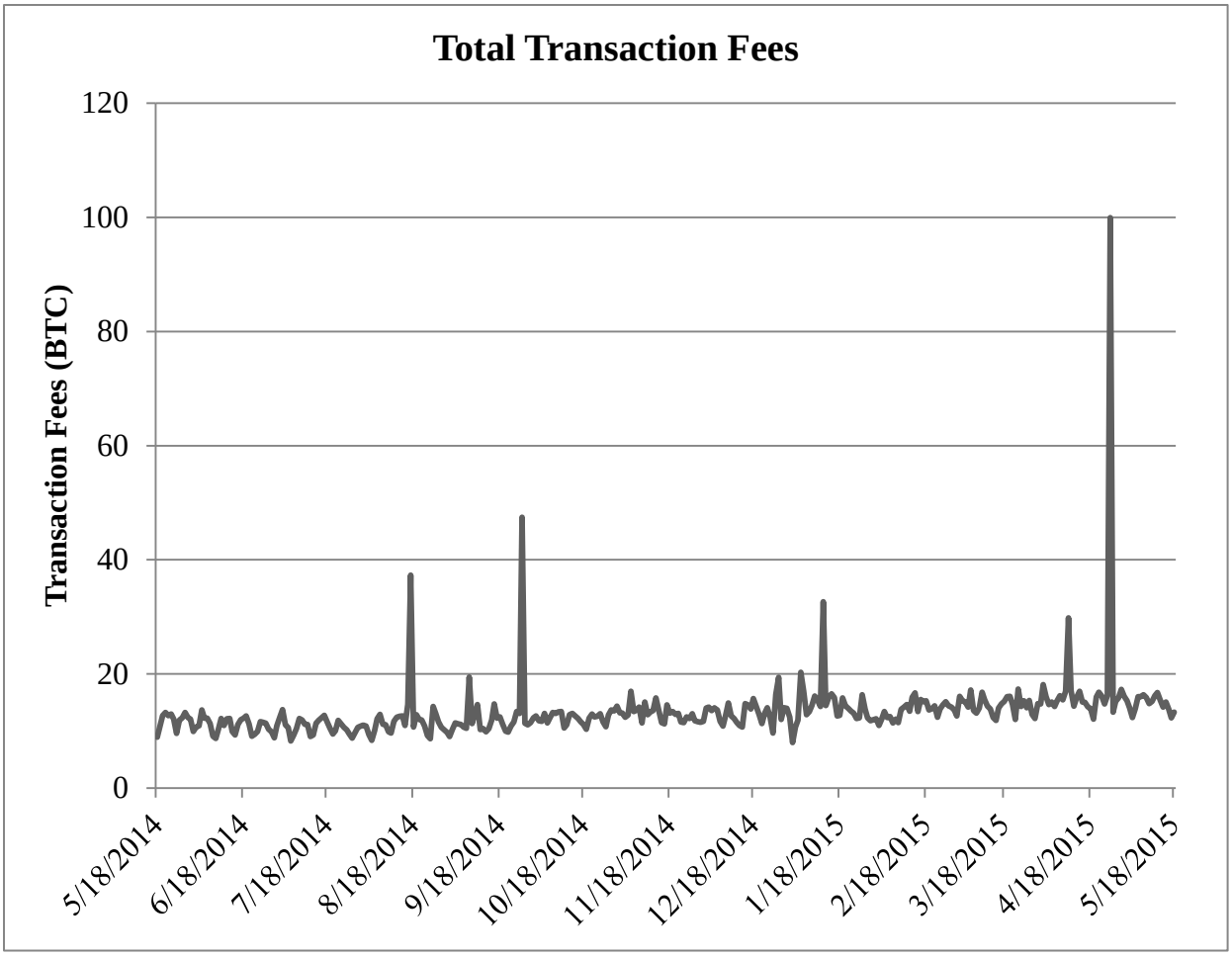


Figure 3. Total Transaction Fees. Source: Values calculated from historical data obtained via blockchain.info

In conclusion, the comparison between traditional currency and Bitcoin with regard to transaction cost demonstrates how traditional currency involve higher indirect costs in terms of producing/transporting physical notes, and the policing efforts required to avoid institutional fraud and counterfeiting. Overall, Bitcoin transaction fees are lower than 0.1% of the transmitted value, which is significantly below the fees charged by conventional payment

systems even if one accounts for the fact that some payments settle in two or more Bitcoin transactions (Moser & Bohme, 2015). In our next section we identify Technical Efficiency as a Critical Success Factor due to its relationship with handling and clearing payments.

4.3 Technical Efficiency

4.3.1 Description as applied to traditional currencies

A study, conducted for the World Bank, Bossone and Cirasino (2001) describes a payment system as the infrastructure held to enable the transfer of monetary value between parties discharging mutual obligations. In support of a strong payment system, the study highlights the importance of technical efficiency – a descriptor of how efficiently the transaction money is used in the economy, and the risks associated with its use. A strong payment system would reduce effectively the cost of exchanging goods and services, and is indispensable to the functioning of the interbank, money, and capital markets. In contrast, reliance on a weak payment system would place the economy at risk of inefficient use of financial resources, inequitable risk-sharing among agents, actual losses for participants, loss of confidence in the financial system, and loss of faith in the very use of money. (Bossone & Cirasino, 2001)

In conjunction with the International Monetary Fund, Summers (1994) reinforced the description of technical efficiency as the cost effectiveness and physical performance characteristics influencing how the stock of deposit money balances in banks is used and how credit, liquidity, and fraud risk is managed by a particular payment system. Central to this principle, a strong payment system must address timing delays in handling payments, both considering the costs of operations and the exposure to risk. These considerations can contribute considerably to the overall monetary efficiency of a payment system (Summers, The payment

system: Design, management, and supervision, 1994). Summers (1994) reinforces the importance of payment innovations, restating the desire to achieve a "ubiquitous electronic solution for making retail payments … that does not require the sender to know the bank account number of the recipient" (Summers, Comments on Payment System Improvement – Public Consultation Paper, 2013, p. 5).

Credit card payment systems attempt to address the need for technical efficiency by offering a means to purchase items without physical cash. They are easy to use, usually agree to protect buyers from fraud, and ultimately reimburses merchants within a few days. However, the timing delay between the submission, clearing and settlement of credit card transaction still presents significant risk. Many credit card contracts generally place the burden of fraud reimbursement upon merchants and merchant banks (Board of Governors of the Federal Reserve System, 2013).

In a Federal Reserve Bulletin, Durkin (2000) highlights the importance of credit cards in modern commerce, representing an important payment device used in lieu of cash or checks for millions of routine purchases, including e-commerce. However, his finding indicated that although consumers enjoy the convenience of its use, they also express concerns such as how the interest rates of revolving credit are often seen as unreasonably high.

The Federal Reserve also conducts studies into the current affair of non-cash payment systems in general to assess aggregate trends (Gerdes, et al., 2014). The study reinforces the increasing use of card-based systems and decline of paper checks, although these too are processed electronically for interbank transactions. Largely driven by card fraud, the estimated annual number of unauthorized transactions stood at 31.1 million, with a value of $6.1 billion, in

2012 (Gerdes, et al., 2014). These figures are significant, but constitute just a portion of the estimated 122.8 billion noncash payments, valued of $79.0 trillion, in 2012 (Gerdes, et al., 2014). Considering the rising popularity of electronic payment systems, Bitcoin represents an alternative to the payment systems currently available.

4.3.2 Description as applied to Bitcoin

Developed as an electronic payment system, Bitcoin processes transactions by employing the block chain. This innovative approach effectively allows Bitcoin a means to replace the conventional process of clearing/settlement of credit card transactions. Once recorded into the block chain, transactions are computationally impractical to reverse and allow users to verify the chronological order of transactions. The generation of every block in the block chain is adjusted by the network to occur approximately every 10 minutes, as shown in the figure below. However, given the network effect of block generation and propagation, the network may sometimes produce forks in the block chain. These forks are mutually exclusive and cannot be merged back into single block chain continuity; only one fork will ultimately be considered part of the block chain. The block chain itself contains no forks, since any competing chains would ultimately be completely orphaned by the network. This consensus for linearity protects the integrity of the block chain and solves for the double spending problem (Kroll, Davey, & Felten, 2013).

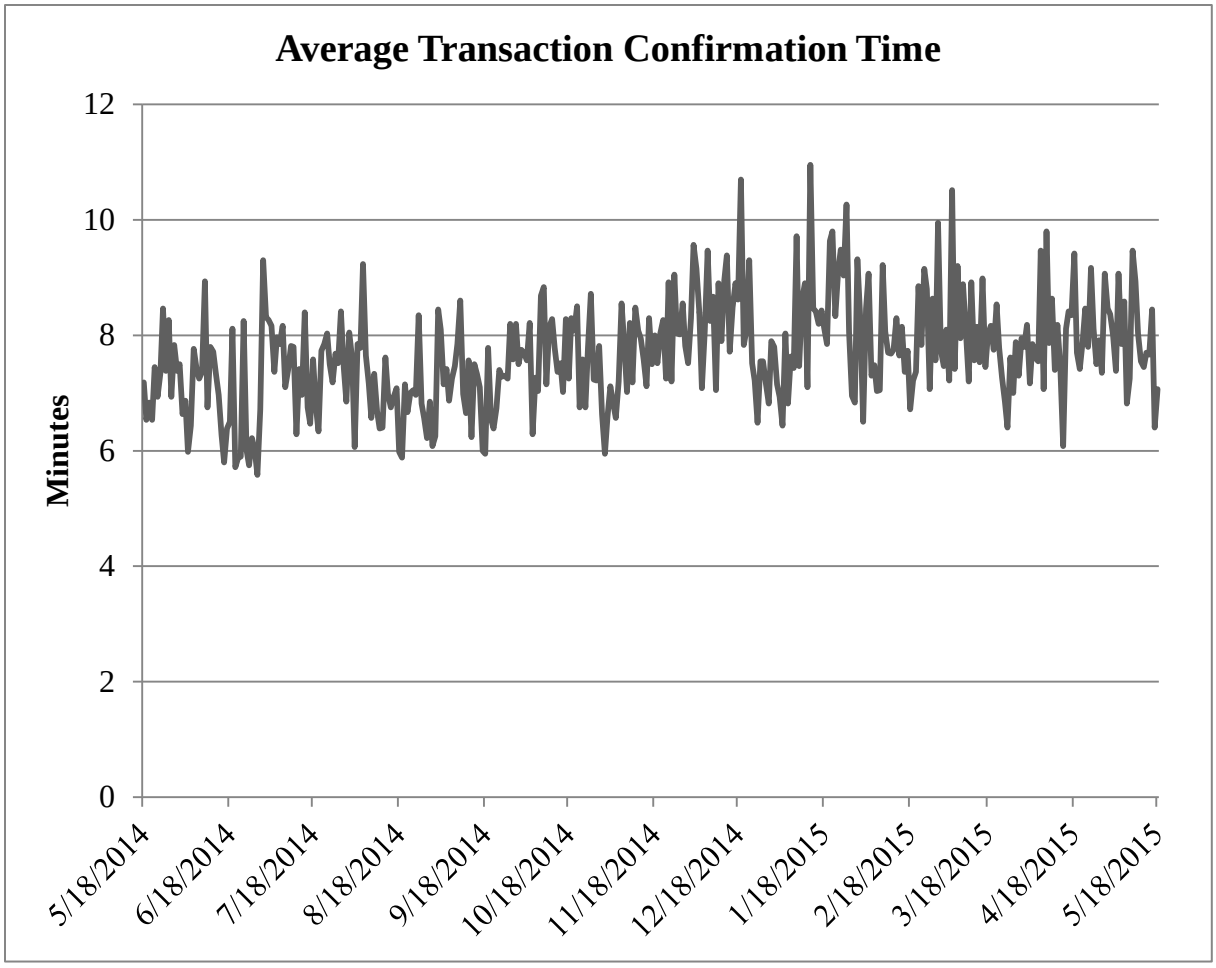


Figure 4. Average Transaction Confirmation Time. Source: Values calculated from historical data obtained via blockchain.info

To attain consensus, each node in the network independently assesses forks it receives against each other to find the longest chain. The longest chain is accepted, while competing forks are discarded. This process occurs continually throughout the network until all forks at a given block level are discarded and consensus is attained. As such, some chains will become orphaned, overruled by longest chain.

Each block generated constitutes a confirmation for the transactions it contains. Since all historical transactions are contained in block chain, each confirmation further reinforces the consensus of the network. Since the network may produce forks that last several generations, a common rule of thumb has become to wait for 6 confirmations – around an hour – before decisively acknowledging a confirmed transaction. The choice of six (6) blocks is arbitrary, originating from the reference client and is not based on any analysis of the probability of deep forks (Bonneau, Miller, Clark, Narayanan, Kroll, & Felten, 2015). Each confirmation reinforces the consensus of the network and reinforces transaction as unchangeable and irreversible (Nakamoto, 2008). This time delay is a marked improvement over credit card settlement times of up to several business days.

Bitcoin's cryptography based payment system allows parties to complete transactions directly without the need for a trusted third party. This also protects against payments being vulnerable to a single point of failure. Technical efficiency is enhanced by shifting the operational costs of processing payments from centralized institutions to a decentralized network of Bitcoin miners. Processing costs are scalable along with the market value of bitcoins since unprofitable mining operations would seek operational efficiencies or otherwise abandon their operations. A reduction in Bitcoin mining operations would in turn reduce the overall difficulty level of the network to which point the costs of mining operations achieve balance against revenues generated. This equilibrium would prove stable if not for the fluctuating exchange rate of bitcoins to other traditional currencies, with which mining costs are paid with. Thus if the Bitcoin price falls substantially, so too would the incentive to mine. This lowered mining rate may prove significant if it leads to loss of confidence in the integrity of the network (Kroll,

Davey, & Felten, 2013). In our next section we identify Governance as a Critical Success Factor due to its relationship with regulatory institutions and its relationship with merchants and taxation.

4.4 Governance

4.4.1 Description as applied to traditional currencies

"One of the direct powers of Congress under the US Constitution, grants the authority 'to coin Money' and 'regulate the Value thereof,' " (Elwell, Murphy, & Seitzinger, 2015, p. 9). In the US, these powers appoint the government as responsible for producing billions of coins and currency notes each year. Specifically, currency notes are produced by the Bureau of Engraving and Printing (BEP), a bureau of the Department of the Treasury, and issued by the Federal Reserve banks. Coins on the other hand are manufactured by US Mint, but follow a similar process. The Federal Reserve then releases them as required by the commercial banking system. US law requires that each Federal Reserve Bank hold collateral that equals at least 100 percent of the value of the currency it issues, usually in the form of US Government securities and gold certificates (United States General Accounting Office, 2004). Other central banks around the world follow similar collateral practices to provide liquidity to the financial system. These varying styles of collateral frameworks have continued to evolve over the years, but they all share common characteristics such as transparency of eligibility criteria and centrality of risk management measures (Bank for International Settlements, 2013).

To influence the money supply, the Federal Reserve sets a target for the federal funds rate. This target is achieved by conducting open market operations, imposing reserve requirements, permitting depository institutions to hold contractual clearing balances, and

extending credit through its discount window facility. Taken together, these operations allow the Federal Reserve to exercise considerable control over the demand and supply of Federal Reserve balances and the federal funds rate (Board of Governors of the Federal Reserve System, 2005). Flowing from this framework, commercial banks contribute to the money supply by issue commercial loans and recording deposit accounts as liabilities on their books. In other words, rather than the bank lending out deposits that are placed with them, the act of lending creates deposits (McLeay, Radia, & Thomas, Money creation in the modern economy, 2014). Together, these controls and processes constitute the basic mechanics that influence the distribution and supply of money and credit.

In the US, the Federal Reserve undertakes duties within four general areas:

- Conducting the nation's monetary policy by influencing money and credit conditions in the economy in pursuit of full employment and stable prices.
- Supervising and regulating banks and other important financial institutions to ensure the safety and soundness of the nation's banking and financial system and to protect the credit rights of consumers.
- Maintaining the stability of the financial system and containing systemic risk that may arise in financial markets.
- Providing certain financial services to the US government, US financial institutions, and foreign official institutions, and playing a major role in operating and overseeing the nation's payments systems (Board of Governors of the Federal Reserve System, 2005).

It is worth noting that the purpose of the Federal Reserve does not include addressing income inequality, regardless of its influence over national economic growth and stability. Yellen (2006), president of the Federal Reserve Bank of San Francisco, addressed economic inequality during a speech to the Center of the Study of Democracy. She remarked, "Inequality has risen to the point that it seems to me worthwhile for the US to seriously consider taking the risk of making our economy more rewarding for more of the people" (Yellen, 2006, p. 20). Bullard (2014), president of the Federal Reserve Bank of St. Louis, also address these concerns by discussing whether quantitative easing affects income inequality, the impact a higher inflation target on the poor, and whether current monetary policy hurts savers. However, regardless of the continued concerns over wealth inequality expressed by noteworthy figures, it remains unclear what role, if any, does the Federal Reserve hold in directly addressing these issues going forward (Bullard, Income inequality and monetary policy: A framework with answers to three questions, 2014).

4.4.2 Description as applied to Bitcoin

Before focusing on current regulation pertaining to Bitcoin, we first address the United States Code pertaining to counterfeiting and forgery under Title 18 U.S.C. Chapter 25; it is currently not clear the level of applicability these statutes hold over the issuance of digital currency, even if it is designed to attack the value of US legal tender (Elwell, Murphy, & Seitzinger, 2015). Thus, it may stand that until such language is amended to directly address digital currencies, Bitcoin will continue to circulate in the US. The same cannot be said of other countries: China has prohibited banks and payment systems from handling bitcoin, although individuals are free to trade; while Russia has banned Bitcoins outright (Szczepański, 2014).

Most countries and unions however, including the European Union (EU), have not adopted any specific regulation on Bitcoin.

With regards to active US government regulation, the most significant includes Internal Revenue Service (IRS) Notice 2014-21 which addressed the issue of Bitcoin taxation by defining it as property rather than a currency. This fundamental definition has created significant complexities regarding taxation and reporting. The IRS explicitly recognizes its purpose but unequivocally limits its recognition: "Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In some environments, it operates like "real" currency -- i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance -- but it does not have legal tender status in any jurisdiction" (Internal Revenue Bulletin: 2014-16, 2014). The IRS defined Bitcoin and other virtual currencies as "convertible" virtual currencies in reference to how these are regularly used to substitute real currencies such as the dollar and euro, and are readily exchanged for these in the open market (Internal Revenue Bulletin: 2014-16, 2014).

Following this definition of virtual currencies as property, the IRS goes on to point out that "In general, the sale or exchange of convertible virtual currency, or the use of convertible virtual currency to pay for goods or services in a real-world economy transaction, has tax consequences that may result in a tax liability" […] "General tax principles applicable to property transactions apply to transactions using virtual currency" (Internal Revenue Bulletin: 2014-16, 2014). Monitoring Bitcoin transactions is required by law to comply with the tax code. Transaction must be measured in equivalent US dollars at fair market value as of the date of

payment or receipt. Operations resulting from these activities are also seen as self-employment when done by individuals.

With regards to other regulatory agencies, the Consumer Financial Protection Bureau recently issued a consumer advisory regarding the risks and characteristics of virtual currencies and have begun accepting consumer complaints, although has largely limited further involvement through informal exchanges with federal, state, and international regulators (Elwell, Murphy, & Seitzinger, 2015).

The Security Exchange Commission released a notice alerting investors about potential scams and fraud surrounding virtual currencies (US Securities and Exchange Commission, 2014) Although the SEC has prosecuted Bitcoin businesses who were ultimately charged with offering publicly traded securities without proper registration, it is nonetheless currently considering a 2014 proposal for a NASDAQ public exchange-traded fund for Bitcoins submitted by Winklevoss Bitcoin Trust (Winklevoss Bitcoin Trust, 2014). This poses the possibility that the SEC may allow Bitcoin activity under certain regulatory frameworks going forward.

The Financial Crimes Enforcement Network, under the US Treasury, issued an interpretative guidance requiring exchanges of virtual currencies, such as Bitcoin, to register with the Treasury as a money services business and comply with the Bank Secrecy Act (Financial Crimes Enforcement Network (FinCEN), 2013). This would include all businesses handling currency conversions. Considering the risk for money laundering by financial institutions in general, the Currency and Foreign Transaction Reporting Act component of the BSA, requires money services businesses to: file reports of cash transactions exceeding certain amounts, file suspicious activity reports for transactions potentially seeking to evade reporting requirements,

and develop anti-money laundering / customer identification programs (Federal Financial Institutions Examination Council, 2010). These efforts seek to regulate Bitcoin at the exchange level, since regulation of the Bitcoin network itself would be infeasible.

The Board of Governors of the Federal Reserve System's only validation over Bitcoin is upholding the Bank Secrecy Act / Anti-Money Laundering Examination Manual. This limited involvement was noted by Federal Reserve Chair Janet Yellen (2014) to the Senate Banking Committee, "Bitcoin is a payment innovation that's taking place outside the banking industry. To the best of my knowledge there's no intersection at all, in any way, between Bitcoin and banks that the Federal Reserve has the ability to supervise and regulate" (Yellen, 2006, p. 1). Although the Federal Reserve has conducted research and discussion regarding Bitcoin and digital currencies in general, no regulation has currently been put in place (Elwell, Murphy, & Seitzinger, 2015).

In spite of limited external regulation, Bitcoins internal regulation simply appeals to the process of network consensus regarding the Bitcoin protocol. The Bitcoin community effectively results in a Nash equilibrium in which all players behave consistently with Bitcoin's reference implementation (Kroll, Davey, & Felten, 2013). This would imply that even if regulators are able to influence developers into incorporating changes into the next version release of the protocol, the rest of the Bitcoin community may collectively fork the block chain, disregard the changes, and carry on as usual. Thus, Bitcoin is not immune to regulation, but it is unlikely to internally adopt governance arising from outside the consensus of its development community. These regulatory pressures influence the core economic value of Bitcoin, directly affecting the overall distribution, quantity, and velocity characteristics covered in the following

section. In our next section we identify Distribution, Quantity and Velocity as a Critical Success Factor due to its importance describing and accounting for the level of use Bitcoin is receiving.

4.5 Distribution, Quantity and Velocity

4.5.1 Description as applied to traditional currencies

The quantity of money is often referred to as money supply as describes the total amount of monetary assets available in an economy at a specific time. To measure the money supply, the Federal Reserve employs several components arranged on a spectrum of narrowest to broadest, including the frequent use of M1 and M2 (Anderson & Kavajecz, 1994). M1 is narrowest and comprises funds that are readily accessible for spending, including: circulating currency, traveler's checks of nonbank issuers, demand deposits, and checkable deposits. M2 is slightly broader considering financial assets held principally by households, including: M1, savings deposits, small-denomination time deposits (less than $100,000), and retail money market mutual funds (Federal Reserve Bank of St. Louis, 2015).

Correspondingly, the velocity of money is the frequency at which one unit of currency is used to purchase domestically- produced goods and services within a given time period. The nature of these exchanges may be generally categorized as the income velocity of money, which covers the purchase of common goods and services, and broader transactions velocity of money, which covers any kind of transaction, includes financial assets. We will focus on metrics more closely related to income velocity of money as a better proxy to understanding the impact on the mainstream economy (Santoni, 1987).

The Federal Reserve also employs aforementioned components M1 and M2 to measure velocity of money. For example, a decreasing velocity of M1 might indicate fewer short- term

consumption transactions are taking place; usually representative of everyday consumption. By extension, M2 can provide additional insight into how quickly the economy is spending and how quickly it is saving (Federal Reserve Bank of St. Louis)

Fisher's Equation of Exchange conveys a simplistic conceptual relationship between the quantity and velocity of money (Thornton, 1983). It is expressed as MV = PX, whereas:

M: supply of money
V: velocity of money
P: average level of prices
X: real GNP

This relationship is useful in the long-run to conceptualize how production and price level are affected by both the supply and velocity of money. There are a number of factors that can cause velocity to change including changes in real interest rates and expectation of inflation, financial innovations that reduce the cost of transferring funds, and cyclical factors such as changes in real income and money growth (Thornton, 1983).

4.5.2 Description as applied to Bitcoin

Thanks to the nature of the block chain, all Bitcoin transactions are publicly available; this greatly increases the ease of collecting data over time. Transaction-level trade data is self-reported by the exchanges and aggregated through sites such as Bitcoincharts.com (Badev & Chen, 2014) and Blockchain.info (Lo & Wang, 2014). These provide statistics on volume, value, and exchange rate of trades that passed through each of the exchanges.

Badev and Chen (2014) found that since 2009, Bitcoin unique users have grown exponentially, albeit from a low user base, reaching close to 100,000 BTC by early 2014. Furthermore, transactions have steadily increased over time to around 80 thousand transactions per day, but remain negligible when compared to other electronic payment methods (Badev &

Chen, 2014). However, fluctuations in the USD exchange rate have driven large swings in its value. This is largely the opposite of what we would expect if BTC were a mainstream currency. With no intrinsic value, it has suffered significant price swings since its launch in 2009; peaking at $1,200 per Bitcoin in December 2013 and recently dropping to under $250 as of spring 2015 (Ember, 2015). We also find evidence of limited liquidity in the Bitcoin market as compared to other currencies, at some points reaching a spread of 20% between major Bitcoin exchanges, which suggests a lack of depth of the exchange markets for bitcoins (Badev & Chen, 2014). Less than 50% of all bitcoins in circulation are used in transactions, of which half are under $100 and largely associated with online gambling services (Badev & Chen, 2014). Taken together, the high volatility and large swings in transaction volume correlated with price movements suggests Bitcoin is influenced by speculative bubbles (Lo & Wang, 2014) and implies limited retail usage (Badev & Chen, 2014).

As derived from the figure below, as of the 4th quarter 2014, the top 100 addresses in the network owned 20% of all bitcoins in existence, while the bottom 95% of addresses hold less than 0.01%. Less than 1% of accounts have more than 1 BTC. We are reminded that addresses are not the same as wallets, and do not categorically represent individual persons. An address simply represents the public key of an asymmetric key pair. As of the 1st quarter 2015, the current market price of 1 BTC remained around $250. Since a unique address is generated each time payment is received, it seems unlikely that most bitcoins are being received and held as payment for retail transactions. Most all bitcoin addresses are held in addresses valued in the thousands USD, suggesting bitcoin are largely held as a form of investment.

Bitcoin Distribution by address at block 320,000				
Bitcoin Balance	**# of Addresses**	**% of Addresses**	**# of Bitcoins Owned**	**% of all Bitcoins**
0 - 0.001	44,917,388	96.47%	288.600	0.00%
0.001 - 0.01	468,390	1.01%	1,815.552	0.01%
0.01 - 0.1	545,136	1.17%	16,415.880	0.12%
0.1 - 1	300,665	0.65%	104,450.810	0.79%
1 – 10	214,170	0.46%	605,575.673	4.57%
10 - 100	99,925	0.21%	3,557,378.156	26.85%
100 - 1,000	13,813	0.03%	3,145,684.530	23.75%
1,000 - 10,000	1,445	0.00%	3,210,486.390	24.23%
10,000 – 100K	95	0.00%	2,178,395.722	16.44%
100K – 21M	3	0.00%	426,872.355	3.22%
Total	46,561,030	100%	13,247,363.668	100%

Table 2. Bitcoin Distribution by address at block 320,000. Source: Values calculated from historical data obtained via http://bitcoinrichlist.com

Distribution of currency is central to a fair, equitable economic system. It has both the independence of currency distribution from political pressure and the accessibility to capital affect how economies grow. Bitcoin attempts to addresses this issue by design – a decentralized network governed by a distributed protocol. It is key however to point out however that nodes do not have equal probabilities of obtaining bitcoins through mining. Bitcoin mining is dependent on computer hashing power, which in turn is affected by variable costs such as hardware, energy, space, and Internet access. These costs also must consider the cost of labor since setting up and maintaining a mining operation is a specialized field. Therefore, although the distribution of bitcoins is indeed decentralized from institutional control, it is not evenly spread across the economy. Its distribution is also unpredictable at the individual mining level over the short run due to the inherent probabilistic nature of Proof-Of-Work. While bitcoin production is stable at the network level, individual miners might endure long periods of time without realizing any bitcoin returns.

Also, since bitcoins have historically suffered considerable price volatility in the open market, mining operations are unable to reliably estimate future operational income. As shown in the figure below, technological innovations in mining hardware have produced marked increases in Bitcoin difficulty levels, eroding the overall profitability achieved by older mining operations. This uncertainty contributes to an uneven spread of bitcoins across nodes and the high barriers for entry by potential miners.

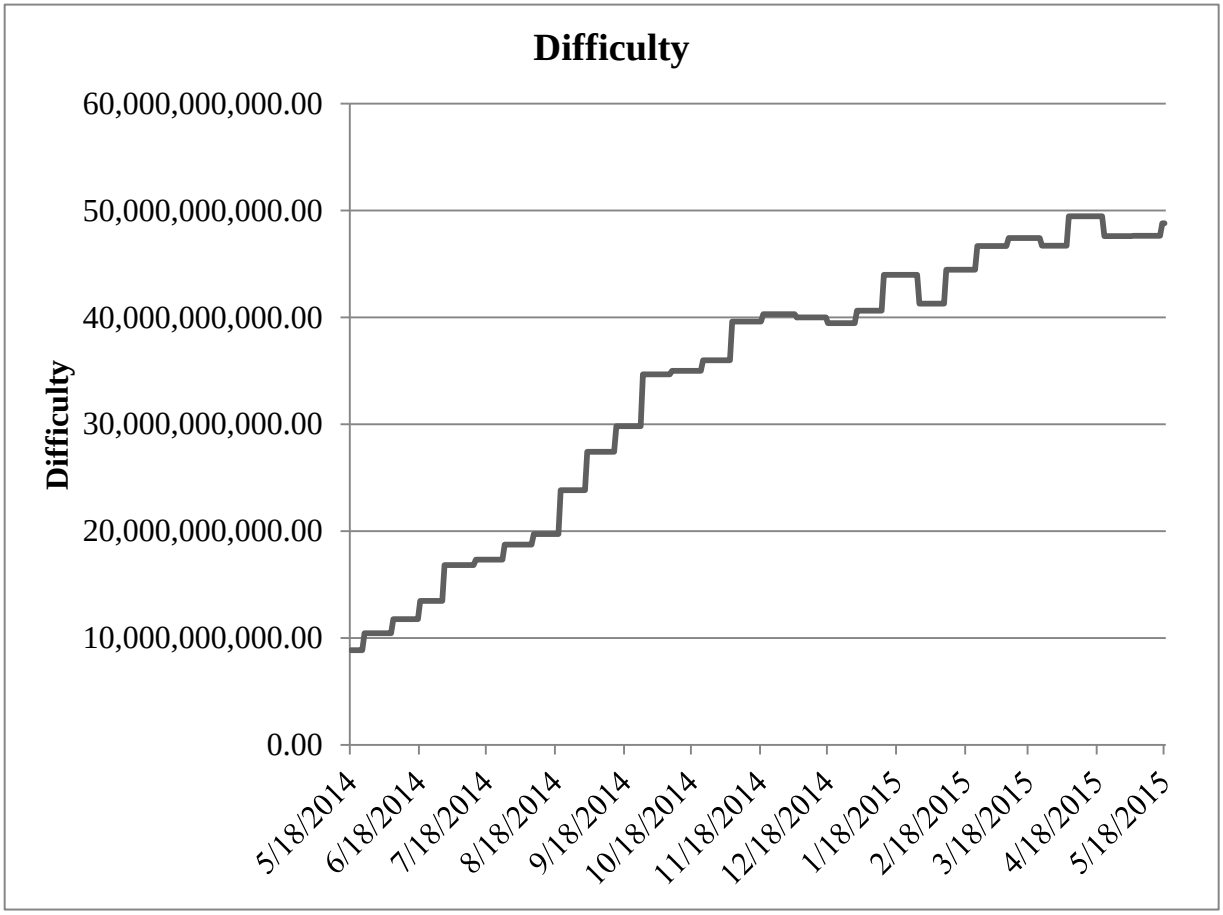


Figure 5. Bitcoin Difficulty Level. Source: (Values calculated from historical data obtained via blockchain.info)

In light of these challenges, mining pools were developed to address the unpredictability of bitcoin production. Mining pools offer miners a way to share the risks of bitcoin production and stabilize operational returns. There are several models used to calculate the distribution of bitcoins mined by the pool. The share of bitcoins each miner is entitled to is dependent on a number of factors including, but no limited to: hashing power, tenure, participation rate, and

origin. The most basic model for calculating mining pool shares include Pay Per Share (PPS) where individuals receive payment regardless if the mining pool successfully produces bitcoins; effectively shifting the entire mining risk to the pool. However, if the mining pool suffers a long enough period of non-production, it is possible that the payout reserve held by the pool will be completely expended and the model collapses (Rosenfeld, 2011).

Various models have been designed including, but not limited to, Proportional (PROP), Pay Per Last N Shares (PPLN), Double Geometric Method (DGM), Shared Maximum Pay Per Share (SMPPS), and Equalizes Shared Maximum Pay Per Share (ESMPPS) (Rosenfeld, 2011). PROP offers a proportional distribution of reward from each block generated based on the number of shares held each round. PPLN approach is similar to the proportional method, but instead of counting the number of shares in the round, it uses the last N shares, regardless of the boundaries of the round. DGM is a hybrid approach that enables the operator to absorb some of the risk. The operator receives a portion of payouts during short rounds and returns it during longer rounds to normalize payments. SMPPS has an similar approach to PPS, but never pays more than the pool has earned. Finally, ESMPPS approach is similar to SMPPS, but distributes payments equally among all miners.

Taken together, we find that although miners have developed several models to address uncertainty, the current level of exchange rate volatility continues to pose a challenge. This is cause for concern since the breadth of the Bitcoin network as a whole is central to the integrity of Bitcoin itself. In the following section, we explore how the network addresses payment security and enables reliable transactions. In our next section we identify Payment Security as a Critical

Success Factor due to its relationship with reliably conducting business, handling account balances and executing transactions.

4.6 Payment Security

4.6.1 Description as applied to traditional currencies

The US National Research Council's (NRC) Committee on Next-Generation Currency Design (Williams & Anderson, 2007) described the features of a "perfect" currency. These include that currency be extremely difficult to duplicate, easily recognized by the general public, durable, machine-readable, easy to produce at low cost, aesthetically pleasing, and non-toxic.

Although the committee drafted several key points regarding currency design, we clearly see that the first and foremost entry highlights the importance of deterring counterfeiting. However, technological innovations in color copying, scanning and printing pose a challenge for paper currency. Continuous advances in technology make this goal endlessly difficult to achieve. Ever improving performance and decreasing cost of information technology have reduced "barriers to entry". NRC's most recent technical report (NRC, 2007) concludes that this race eventually will be lost for the current generation of paper-based banknotes. Only ongoing design innovation and currency replacement can sustain a low frequency of counterfeit notes in circulation (Williams & Anderson, 2007).

Currently the US $100 banknotes contain a large number of security features to deter counterfeiting. These include security threads which glow under UV light, holographic security ribbons, watermarks, color-shifting ink, serial numbers, and microprinting (US Currency Education Program, 2013).

Additionally, the production process itself is closely monitored, with the paper itself being supplied by a single US firm under close security. NRC reports found that low-quality counterfeit notes are commonly identified by low optical image quality, lack of magnetic/infrared ink, or incorrect paper fluorescence. Other detection methods include sensing magnetic, infrared, or UV signatures.

These anti-counterfeiting measures come through the continued efforts of the US Treasury Department. However nearly 60 percent of all US banknotes in circulation, or about $450 billion of the $760 billion, is held abroad (United States Treasury Department, 2006).

With regards to electronic payment systems, there are robust protections available to users of popular electronic payment systems such as credit cards, debit cards, prepaid cards, and automated clearing house (ACH) e-checks. However, studies by the Federal Reserve continue to raise concerns since current regulations do not incentivize all parties involved to actively participate in fraud reduction. In the case of ecommerce, Internet merchant bear most all the liability of Internet fraud; as such, consumers and issuers have little incentive to adopt any measures to avoid it. In this regard, current protection mechanisms make it more difficult to encourage the adoption of fraud-reduction schemes which lead to a significant cost to banks, merchants, processors, and consumers (Furletti, 2005). In this thesis we recognize the immutable importance of anti-counterfeiting measures and will evaluate how these are applied to digital currencies.

4.6.2 Description as applied to Bitcoin

Bitcoin cannot be fraudulently minted and introduced into the network. These are made possible by the public-key cryptography that underpins the transaction process between users.

There are no known methods that can break these keys other than infeasible computational brute force (Bos, Halderman, Heninger, Moore, Naehrig, & Wustrow, 2014). This level of security enables Bitcoin to reliably maintain the integrity of the Bitcoin transaction and free from external manipulation.

With regards to the network as a whole however, some forms of fraud may come about from the accumulation of the network computing power being dedicated to the block chain; this is commonly called a 51 attack. The effects however would be limited. Transaction occurring in real time may be prevented from being written into the block chain and making them invalid, thus reducing bitcoin volume. Current transactions may also be reversed, thus allowing double spending. The network itself is unlikely to suffer long-term effects, but confidence in the currency might falter thus dropping in price in exchange markets. It is important to point out that a 51 attack would not be able to reverse a transaction having occurred several block chain generations ago, and would not be able to forge new coins than by regular mining, nor could other people's bitcoins be stolen.

The other major source of fraud is theft of bitcoins. If hackers obtain a bitcoin wallet's password, be it having been stored in an email or file, then bitcoins may potentially be transferred out of the account. Although the transaction can theoretically be traced eventually to a receiving account, bitcoins will have likely been forward to additional wallets in an effort to avoid detection. The Mt. Gox crisis is a prime example of bitcoin theft, where close to 744,00 bitcoins were stolen from Mt. Gox servers, accounting for around 7% of all bitcoins, and worth around $473 million near the time of the filing (Popper & Abrams, 2014). Around 100,000 bitcoins were recovered from Mt. Gox servers a few months later that had apparently been

misplaced. Concerns of bitcoin security and bitcoins exchanges soared after the incident and dialogue concerning new regulation began to take traction (Popper & Abrams, 2014).

In the next chapter we will take into account the Critical Success Factors identified in chapter 4, analyze the implications, and derive conclusions regarding the current state of Bitcoin and clarify areas of improvement moving forward.

Chapter 5: Analysis and Conclusion

How does Bitcoin function as a payment system? Bitcoin exhibits properties associated with both commodities and currencies. Although in practice it is used primarily as a means of payment, a utility ultimately associated with the purpose of money, it has not yet been adopted for widespread use nor commonly held by businesses for recirculation. Businesses often sign up to use a *Bitcoin merchant solution* to accept Bitcoins, which often supports automatic conversion to other traditional national currencies. Gallippi, chairman of BitPay, confirmed to *Time Money* during a 2015 interview that the majority of its major clients ask for Bitcoins received as payment be instantly converted to cash – "I would say as a general trend most of our larger business do choose a settlement in 100% US dollars because that's how they do their accounting and finance" (Davidson, 2015, p. 1). Bitcoins are not chiefly held by businesses as an alternative currency, but rather as a payment system at the point of sale. In this sense, Bitcoin ultimately behave more closely as a *complimentary currency* which compliments rather than substitute traditional currencies.

Since Bitcoin is used by merchants primarily as a means of payment rather than a currency, we find that the term "Bitcoin" itself ultimately invokes ambiguous meanings. "Bitcoin" may both refer to its unit as a currency, as well as a term distinguishing its protocol, software, and community. These separate meanings affect how Bitcoin is recognized and valued.

How do these relate to the function as money and traditional currencies? Bitcoin described as a unit of money fails to reliably satisfy all three functions of money. Since Bitcoin emerged independently, it lacks a marked regional presence supporting its value – it does not

serve as legal tender in any country. This lack of economic integration serves as the primary weakness to its function as a store of value. Since it has not been adopted for widespread use, it is inadequately exposed to the forces of mainstream demand and supply to stabilize value. This lack of local economic circulation or substantial use as money makes Bitcoin vulnerable to sudden price volatility. There is little incentive for the pricing of goods and services to change from traditional currencies, unless these currencies were to suffer from a wholesale collapse in confidence (Ali, Barrdear, Clews, & Southgate, The economics of digital currencies, 2014).

What are the Critical Success Factors driving its adoption as currency and how well does Bitcoin satisfy each? We identified five CSFs that are central to Bitcoin success as a currency. These included transaction costs, technical efficiency, governance, distribution, quantity and velocity, and payment security. Our findings indicate that Bitcoins performance as a whole is inadequate. In favor of Bitcoin, the implementation of the block chain technology provides significant innovations that drive a positive impact for transaction costs, technical efficiency and payment security. When compared to traditional currencies, Bitcoin succeeds is providing a novel approach to handling transactions that is secure, timely, cost-effective and reliable. In contrast, Bitcoin current shortcomings are driven by inadequate performance in governance as well as distribution, quantity and velocity. Driven by an evolving regulatory environment, Bitcoin is faced with several questions regarding its legitimacy as a currency. In the US, ambiguity remains regarding its proper classification and handling for tax and legal purposes, creating uncertainty around the future of Bitcoin moving forward. Ultimately, Bitcoin's most significant challenge is posed by inadequacies in its distribution, quantity and velocity. We find that high volatility and large swings in transaction volume correlated with price movements

suggests Bitcoin is influenced by speculative bubbles. In this regard, Bitcoin is unable to outperform traditional currencies when considering year over year price stability,

This brings to question whether Bitcoin can be indeed considered a currency, given that it cannot reliably be used to retrieve value over time. In the long run, Bitcoin only partially fulfills the functions of money. We find that the value of money is emergent in nature and requires a large enough system to achieve stabilization. The economic forces of demand and supply presiding over money are key determinants for its store of value. As it stands, Bitcoin is only able to reliably serve as a fungible medium of exchange.

What characteristics of Bitcoin influence its valuation and economic utility? Considering Bitcoin's insufficient description as a currency, it may potentially be more broadly described as a commodity possessing several unique characteristics. It is scarce because supply is limited, durable because it is imperishable and indestructible, portable since it may be easily transported electronically, divisible since it may be split into smaller units without losing its material identity, verifiable since it may be tested for authenticity and distinguishable from counterfeits, and fungible since individual units are capable of mutual substitution

However, these characteristics do not hold true of Bitcoin in a vacuum; not only is it impossible to physically hold a single bitcoin on its own accord, but its aforementioned characteristics are entirely emergent from its existence in a network.

In the open market, Bitcoin behaves similarly to precious metals such as gold, whose value is determined more by the marketplace than by its intrinsic value. Vulnerable to financial market forces pressures such as speculation, Bitcoin's value is highly volatile and unpredictable.

In this sense, we may draw parallels to the volatility of precious metals such as gold, which are subject to both monetary and financial market variables (Batten, Ciner, & Lucey, 2010).

Is Bitcoin best described as a cryptocurrency or a cryptocommodity? In light of this market behavior, we conclude that Bitcoin may be best described as a cryptocommodity rather than a cryptocurrency; a unique asset class than more closely resembles a digital commodity rather than a digital currency. This would be consistent with the IRS ruling of Bitcoin as property rather than currency and could potentially lead to Bitcoin falling under the jurisdiction of the Commodity Futures Trading Commission (CFTC). This remains to be seen however, since Bitcoin legal status and definition continue to mature within the US regulatory environment.

5.1 Future studies

After having derived the Critical Success Factors in this paper, we suggest future areas of research within the scope for these key areas. Considering the rapid evolution of Bitcoin, it is imperative to understand how this payment system will adapt to the changing regulatory landscape. We also find important to monitor for merchant adoption and the institutional use of the underlying Bitcoin protocol. As the Bank of England's Quarterly Bulletin 2014 Q3 very well observed, "the key innovation of digital currencies is the 'distributed ledger' which allows a payment system to operate in an entirely decentralized way, without intermediaries such as banks." (Ali, Barrdear, Clews, & Southgate, 2014, p. 1)

References

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). *Innovations in payment technologies.* Bank of England.

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). *The economics of digital currencies.* Bank of England.

Alston, L. J., & Gillespie, W. (1989). Resource coordination and transaction costs. *Journal of Economic Behavior and Organization*, 191-212.

Amberg, M. (2005). *Background of critical success factor research.* Nurnberg: Friedrich-Alexander-Universitat Erlangen-Nurnberg Working Paper No 2/2005.

Anderson, R. G., & Kavajecz, K. A. (1994). *A historical perspective on the Federal Reserve's monetary aggregates: definition, construction and targeting.* Federal Reserve Bank of St. Louis.

Anderson, R. G., & Rasche, R. H. (2001). *The remarkable stability of monetary base velocity in the United States.* St. Louis: Federal Reserve bank of St. Louis.

Andreessen, M. (2014, January 21). *Why Bitcoin matters*. Retrieved from The New York Times: http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1

Badev, A., & Chen, M. (2014). *Bitcoin: technical background and data analysis.* Finance and Economics Discussion Series.

Bagus, P. (2009). The quality of money. *The Quarterly Journal of Austrian Economics*, 22-45.

Bahmani, M. O., & Bahmani, S. (2014). Monetary uncertainty and demand for money in korea. *Asian Economic and Financial Review*, 317-324.

Bamert, T., Christian, D., Elsen, L., Wattenhofer, R., & Welten, S. (2013). Have a snack, pay with bitcoins. *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on* (pp. 1-5). IEEE.

Bank for International Settlements. (2013). *Central bank collateral frameworks and practices.* Markets Committee Publications No 6.

Barnett, E. R. (2014). Virtual currencies: Safe for business and consumers or just for criminals? *13th European Security Conference & Exhibition.* The Hague.

Baskarada, S. (2014). Qualitative case study guidelines. *The Qualitative Report*, 1-25.

Batten, J. A., Ciner, C., & Lucey, B. M. (2010). The macroeconomic determinants of volatility in precious metals markets. *Resources Policy*, 65-71.

Bitcoin Foundation. (2014). *Removing impediments to Bitcoin's success: A risk management study.* Retrieved from Bitcoin Foundation: https://bitcoinfoundation.org/wp-content/uploads/2014/04/Bitcoin-Risk-Management-Study-Spring-2014.pd

Bitcoin.org. (2015). *How it works*. Retrieved March 14, 2015, from Bitcoin.org: https://bitcoin.org/en/how-it-works

Bitsch, V. (2005). Qualitative research: A grounded theory example and evaluation criteria. *Journal of Agribusiness*, 75-91.

Blockchain.info. (2014). *Bitcoin charts*. Retrieved from Blockchain: https://blockchain.info/charts

Board of Governors of the Federal Reserve System. (2005). *The Federal Reserve system: Purposes and functions.* Washington, D.C.: Board of Governors of the Federal Reserve System.

Board of Governors of the Federal Reserve System. (2013). *2013 interchange fee revenue, covered issuer costs, and covered issuer and merchant fraud losses related to debit card transactions.* Retrieved from Federal Reserve: http://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2013.pdf

Board of Governors of the Federal Reserve System. (2014, September 18). *Interest on required balances and excess balances*. Retrieved from Federal Reserve: http://www.federalreserve.gov/monetarypolicy/reqresbalances.htm

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., & Felten, E. (2015). *Research perspectives and challenges for Bitcoin and cryptocurrencies.* IEEE Security and Privacy.

Bos, J., Halderman, J., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014). Elliptic curve cryptography in practice. *Financial Cryptography and Data Security*, 157-175.

Bossone, B., & Cirasino, M. (2001). *The oversight of the payments systems: a framework for the development and governance of payment systems in emerging economies.* CEMLA: The World Bank.

Brito, J., & Castillo, A. (2013). *Bitcoin: a primer for policymakers.* Arlington: Mercatus Center at George Mason University.

Bryans, D. (2014). Bitcoin and money laundering: Mining for an effective solution. *Indiana Law Journal*, 441-472.

Bullard, J. B. (1994). *Measures of money and the quantity theory.* Federal Reserve Bank of St. Louis Review.

Bullard, J. B. (2014). *Income inequality and monetary policy: A framework with answers to three questions.* Federal Reserve Bank of St. Louis.

Buterin, V. (2013, August 26). *What proof of stake is and why it matters*. Retrieved March 3, 2015, from Bitcoin Magazine: http://bitcoinmagazine.com/6528/

Camera, G., & Chien, Y. (2014). Understanding the distributional impact of long-run inflation. *Journal of Money, Credit and Banking*, 1137-1170.

Caralli, R. A. (2004). *The critical success factor method: Establishing a foundation for enterprise security management.* Carnegie Mellon University.

Casey, M. J., & Vigna, P. (2015, January 23). *Bitcoin and the digital-currency revolution*. Retrieved January 21, 2015, from The Wall Street Journal: http://www.wsj.com/articles/the-revolutionary-power-of-digital-currency-1422035061

Chambers, J. (2013). *Digital currency forensics.* Auckland University of Technology.

Cheung, S. N. (1998). The transaction costs paradigm 1998 presidential address Western Economic Association. *Economic Inquiry, 36(4)*, 514-521.

Coase, R. H. (1937). The nature of the firm. *Economica, 4(16)*, 386-405.

Counterfeiting and Forgery, Title 18 U.S.C., Chapter 25, Sections 470 to 514. (n.d.).

Creswell, J. W. (2012). *Qualitative inquiry and research design: Choosing among five approaches.* Sage.

Dahlman, C. J. (1979). The problem of externality. *Journal of Law and Economics*, 141-162.

Davidson, J. (2015, January 9). *No, big companies aren't really accepting bitcoin*. Retrieved March 10, 2015, from Time Money: http://time.com/money/3658361/dell-microsoft-expedia-bitcoin/

de Sousa, J. M. (2004). *Definition and analysis of critical success factors for ERP implementation projects.* Barcelona: Universitat Politècnica de Catalunya.

DeLeo, M. J., & Stull, W. (2014). *Does the velocity of bitcoins effect the price level of Bitcoin?* Temple University.

Dieterle, D. A., & Simmons, K. C. (2014). *Government and the economy: An encyclopedia.* ABC-CLIO.

Durkin, T. A. (2000). Credit cards: use and consumer attitudes, 1970-2000. *Federal Reserve Bulletin 86*, 623.

Dwyer, G. P. (2014). *The economics of private digital currency.* Clemson University and the University of Carlos III, Madrid.

Ellegard, C., & Grunert, K. (1992). *The concept of key success factors: theory and method.* MAPP.

Elwell, C. K., Murphy, M. M., & Seitzinger, M. V. (2015). *Bitcoin: Questions, answers, and analysis of legal issues.* Congressional Research Service.

Ember, S. (2015, January 13). *As Bitcoin's price slides, signs of a squeeze*. Retrieved April 21, 2015, from The New York Times: http://dealbook.nytimes.com/2015/01/13/as-bitcoins-price-slides-signs-of-a-squeeze/?_r=1

Eyal, I. (2014). *The miner's dilemma.* Cornell University.

Federal Bureau of Investigation. (2012). *Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity.* Retrieved from Cryptome: http://cryptome.org/2012/05/fbi-bitcoin.pdf

Federal Financial Institutions Examination Council. (2010). *Bank secrecy act anti-money laundering examination manual.* Federal Financial Institutions Examination Council.

Federal Reserve Bank of St. Louis. (2015). *Monetary trends.* Research Division of the Federal Reserve Bank of St. Louis.

Federal Reserve Bank of St. Louis. (n.d.). *Velocity of M1 money stock*. Retrieved April 19, 2015, from Federal Reserve Bank of St. Louis: https://research.stlouisfed.org/fred2/series/M1V/

Financial Crimes Enforcement Network (FinCEN). (2013, March 18). *Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies*. Retrieved from United States Department of the Treasury: http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

Financial Crimes Enforcement Network (FinCEN). (2013, March 18). *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* . Retrieved from United States Department of the Treasury: http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

Furletti, M. J. (2005). *The laws, regulations, and industry practices that protect consumers who use electronic payment systems: policy considerations.* Federal Reserve Bank of Philadelphia.

Garrison, R. W. (2007). *Hayek and Friedman: head to head.* New Orleans: Auburn University.

Gates, L. P. (2010). *Strategic planning with critical success factors and future scenarios: An integrated strategic planning framework.* Carnegie Mellon University.

Gerdes, G. R., Liu, M. X., Berkenpas, J. P., Chen, M. C., Hayward, M. C., McKee, J. M., et al. (2014). *The 2013 Federal Reserve payments study.* Federal Reserve System.

Gould, E. (2014, September 5). *Wages are growing far below the Fed's target*. Retrieved from The Economic Policy Institue: http://www.epi.org/blog/wages-growing-feds-target/

Greco, T. (2001). *Money: Understanding and creating alternatives to legal tender.* Chelsea Green Publishing.

Harvey, J. T. (2011, May 30). *What actually causes inflation (and who gains from it)*. Retrieved from Forbes: http://www.forbes.com/sites/johntharvey/2011/05/30/what-actually-causes-inflation/

Hazlitt, H. (1983). *The inflation crisis, and how to resolve it.* Ludwig von Mises Institute.

Heid, A. (2013). *Analysis of the cryptocurrency marketplace.* HackMiami.

Howells, P., & Mariscal, I. B. (1992). An explanation for the recent behavior of income and transaction velocities in the United Kingdom. *Journal of Post Keynesian Economics*, 367-388.

Huber, J., & Robertson, J. (2000). *Creating new money: A monetary reform for the information age.* London: New Economics Foundation.

Internal Revenue Bulletin: 2014-16. (2014). *Notice 2014–21: IRS virtual currency guidance.* IRS.

INTERPOL. (n.d.). *Counterfeit currency and security documents*. Retrieved April 19, 2015, from INTERPOL: http://www.interpol.int/Crime-areas/Financial-crime/Counterfeit-currency-and-security-documents/Counterfeit-currency

Jeffries, A. (2013, December 31). *Why don't economists like Bitcoin?* Retrieved from The Verge: http://www.theverge.com/2013/12/31/5260534/krugman-bitcoin-evil-economists

Keister, T., & McAndrews, J. (2009). *Why are banks holding so many excess reserves?* Current Issues in Economics and Finance 15(8).

Kharif, O. (2014, December 15). *Bitcoin bears say told-you-so as digital currency falls*. Retrieved April 21, 2015, from Bloomberg Business: http://www.bloomberg.com/news/articles/2014-12-15/bitcoin-bears-say-told-you-so-as-digital-currency-falls

King, S., & Nadal, S. (2012). *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake.*

Kostakis, V., & Giotitsas, C. (2014). The (a) political economy of Bitcoin. *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society, 12(2),* 431-440.

Kristoufek, L. (2014). *What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis.* arXiv preprint arXiv:1406.0268.

Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. *Proceedings of WEIS (Vol. 2013).*

Lee, T. B. (2013, April 17). *Four reasons Bitcoin is worth studying*. Retrieved from Forbes: http://www.forbes.com/sites/timothylee/2013/04/07/four-reasons-bitcoin-is-worth-studying/

Leonhardt, D., & Quealy, K. (2014, April 22). *The american middle class is no longer the world's richest*. Retrieved from The New York Times: http://www.nytimes.com/2014/04/23/upshot/the-american-middle-class-is-no-longer-the-worlds-richest.html?_r=0&abt=0002&abg=1

Lo, S., & Wang, J. C. (2014). *Bitcoin as money?* Federal Reserve Bank of Boston.

Lu, Y. (2013). Quantitative easing: Reflections on practice and theory. *World Review of Political Economy,* 341-356.

Mankiw, G. N. (2014). *Principles of Macroeconomics 7e.* Stamford: Cengage Learning.

Martin, F. M. (2013). Government policy in monetary economies. *International Economic Review, 54(1),* 185-217.

Maxwell, J. A. (2012). *Qualitative research design: An interactive approach (Vol. 41).* Sage.

McLeay, M., Radia, A., & Thomas, R. (2014). Money creation in the modern economy. *Bank of England Quarterly Bulletin, Q1*.

McLeay, M., Radia, A., & Thomas, R. (2014). *Money in the modern economy: an introduction.* Bank of England Quarterly Bulletin, Q1.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., et al. (2013). A fistful of bitcoins: characterizing payments among men with no names. *Proceedings of the 2013 conference on Internet measurement conference* (pp. 127-140). San Diego, California: ACM.

Moser, M., & Bohme, R. (2015). Trends, tips, tolls: A longitudinal study of Bitcoin transaction fees. *2nd Workshop on Bitcoin Research, affiliated with the19th International Conference on Financial Cryptography and Data Security.* San Juan.

Myasnikov, A. G., Shpilrain, V., & Ushakov, A. (2011). *Non-commutative cryptography and complexity of group-theoretic problems.* American Mathematical Society.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.*

Nowobilski, A. J. (2012). *The Financial Sector in Macroeconomics.* Northwestern University.

Olafsson, I. A. (2014). *Is Bitcoin money?: An analysis from the Austrian school of economic thought.* University of Iceland.

Osipkov, I., Vasserman, E. Y., Hopper, N., & Kim, Y. (2007). Combating double-spending using cooperative p2p systems. *Distributed Computing Systems, 2007. ICDCS'07. 27th International Conference on* (p. 41). IEEE.

Ott, M. (1982). *Money, credit and velocity.* Federal Reserve Bank of St. Louis Review.

Parguez, A., & Seccareccia, M. (2000). The credit theory of money: The monetary circuit approach. In J. Smithin, *What is money* (pp. 101-123). New York: Routledge.

Penard, W., & van Werkhoven, T. (2008). On the secure hash algorithm family. In G. Tel, *Cryptography in Context* (pp. 1-17). Utrecht: Utrecht University.

Plassaras, N. A. (2013). Regulating digital currencies: Bringing Bitcoin within the reach of IMF. *Chicago Journal of International Law, 14*, 377-407.

Popper, N., & Abrams, R. (2014, February 25). Apparent theft at Mt. Gox shakes Bitcoin world. *The New York Times*, p. B1.

Ro, S. (2014, February 17). *The Bitcoin economy*. Retrieved from Business Insider: http://www.businessinsider.com.au/bitcoin-economy-infographic-2014-2

Roach, S. S. (2013, September 25). *How quantitative easing exacerbates inequality*. Retrieved from Project Syndicate: http://www.project-syndicate.org/commentary/how-quantitative-easing-exacerbates-inequality-by-stephen-s--roach

Rochard, P. (2013, December 15). *The Bitcoin central bank's perfect monetary policy*. Retrieved from The Mises Circle: http://themisescircle.org/blog/2013/12/15/the-bitcoin-central-banks-perfect-monetary-policy/

Rockart, J. (1979). Chief executives define their own information needs. *Harvard Business Review*, 81-92.

Rockart, J., & van Bullen, V. (1986). A primer on critical success factors. In *The rise of management computing.* Homewood: Irwin.

Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. *Financial Cryptography and Data Security*, 6-24.

Rosenfeld, M. (2011). *Analysis of bitcoin pooled mining reward systems.* Cornell University.

Rothbard, M. N. (2004). *Man, economy, and state with power and market.* Ludwig von Mises Institute.

Salmon, F. (2014). *The Bitcoin bubble and the future of currency*. Retrieved February 3, 2015, from Genius.com: http://news.rapgenius.com/Felix-salmon-the-bitcoin-bubble-and-the-future-of-currency-annotated

Santoni, G. J. (1987). Changes in wealth and the velocity of money. *Federal Reserve Bank of St. Louis Review*.

Schumer, C. E., & Manchin, J. (2011, June 6). *Letter from Charles E. Schumer & Joe Manchin, U.S. Senators, to Eric Holder, Att'y Gen. of the United States.* Retrieved from Joe Manchin: http://www.manchin.senate.gov/public/index.cfm/2011/6/manchin-urges-federal-law-enforcement-to-shut-down-online-black-market-for-illegal-drugs

Schwartz, N. D. (2014, February 2). *The middle class is steadily eroding. Just ask the business world.* Retrieved from The New York Times: http://www.nytimes.com/2014/02/03/business/the-middle-class-is-steadily-eroding-just-ask-the-business-world.html

Selgin, G. (2014). Synthetic commodity money. *Journal of Financial Stability*.

Selorm, R., & Kodjo, E. (2013). *Mobile money security.* Lulea University of Technology.

Sheard, P. (2013). *Repeat after me: Banks cannot and do not "lend out" reserves.* New York: Standard and Poor's.

Silinskyte, J. (2014). *Understanding Bitcoin adoption: Unified theory of acceptance and use of technology.* Leiden University.

Southern District of New York. (2013). *Sealed complaint 13 MAG 2328: United States of America v. Ross William Ulbricht.* New York: Southern District of New York.

Sowell, T. (2012). *Tricke down theory and tax cuts for the rich.* Hoover Press.

Spenkelink, H. F. (2014). *The adoption process of cryptocurrencies: Identifying factors that influence the adoption of cryptocurrencies from a multiple stakeholder perspective.* University of Twente.

Starr, M. (2014). Qualitative and mixed-methods research in economics: Surprising growth, promising future. *Journal of Economic Surveys, 28(2),* 238-264.

Summers, B. J. (1994). *The payment system: Design, management, and supervision.* Washington, DC: International Monetary Fund.

Summers, B. J. (2013). *Comments on Payment System Improvement – Public Consultation Paper.* Federal Reserve Banks.

Szczepański, M. (2014). *Bitcoin: Market, economics and regulation.* European Parliamentary Research Service.

Thornton, D. L. (1983). *Why does velocity matter?* ederal Reserve Bank of St. Louis Review.

Tucker, P. (2004). Managing the central bank's balance sheet: where monetary policy meets financial stability. *Bank of England Quarterly Bulletin, Q3,* 359-382.

Tunali, D. (2012). *Essays on monetary economics.* Rutgers University.

United States General Accounting Office. (2004). *Coins and currency: How the costs and earnings associated with producing coins and currency are budgeted and accounted for.* Washington, DC: United States General Accounting Office.

United States Treasury Department. (2006). *The use and counterfeiting of United States currency abroad, part 3.* United States Treasury Department.

US Currency Education Program. (2013). *The redesigned $100 note*. Retrieved April 18, 2015, from Newmoney.gov: http://www.newmoney.gov/uscurrency/redesigned100.htm

US Securities and Exchange Commission. (2014, May 7). *Investor alert: Bitcoin and other virtual currency-related investments.* Retrieved from US Securities and Exchange Commission: http://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html

Velde, F. R. (2013). *Bitcoin: A primer.* The Federal Reserve Bank of Chicago.

Vulture, R. (2014, April 3). *How cryptocurrency is changing the world economy*. Retrieved from Socialsteak: http://socialsteak.com/2014/04/03/how-cryptocurrency-is-changing-the-world-economy/

Wen, Y. (2014). *Money, liquidity and welfare.* Federal Reserve Banks of St. Louis.

Wen, Y., & Arias, M. A. (2014, September 1). *What does money velocity tell us about low inflation in the US?* Retrieved from Federal Reserve Bank of St. Louis: https://www.stlouisfed.org/On-The-Economy/2014/September/What-Does-Money-Velocity-Tell-Us-about-Low-Inflation-in-the-US

Williams, M. M., & Anderson, R. G. (2007). *Currency design in the United States and abroad: Counterfeit deterrence and visual accessibility.* Federal Reserve Bank of St. Louis Review, 89.

Winklevoss Bitcoin Trust. (2014). *SEC Registration No. 333-189752.* Washington D.C.: Securities and Exchange Commission.

Wray, L. R. (2002). Modern money. In J. Smithin, *What is money?* (pp. 78-115). New York: Routledge.

Yellen, J. L. (2006, November 6). *Economic inequality in the United States.* Retrieved April 24, 2015, from Federal Reserve Bank of San Francisco: http://www.frbsf.org/news/speeches/2006/061106.pdf