An Analysis of the Cryptocurrency Industry
by Ryan Farell

INTRODUCTION

The cryptocurrency market has evolved erratically and at unprecedented speed over the course of its short lifespan. Since the release of the pioneer anarchic cryptocurrency, Bitcoin, to the public in January 2009, more than 550 cryptocurrencies have been developed, the majority with only a modicum of success [1]. Research on the industry is still scarce. The majority of it is singularly focused on Bitcoin rather than a more diverse spread of cryptocurrencies and is steadily being outpaced by fluid industry developments, including new coins, technological progression, and increasing government regulation of the markets. Though the fluidity of the industry does, admittedly, present a challenge to research, a thorough evaluation of the cryptocurrency industry writ large is necessary. This paper seeks to provide a concise yet comprehensive analysis of the cryptocurrency industry with particular analysis of Bitcoin, the first decentralized cryptocurrency. Particular attention will be given to examining theoretical economic differences between existing coins.

Section 1 of this paper provides an overview of the industry. Section 1.1 provides a brief history of digital currencies, which segues into a discussion of Bitcoin in section 1.2. Section 2 of this paper provides an in-depth analysis of coin economics, partitioning the major currencies by their network security protocol mechanisms, and discussing the long-term theoretical implications that these classes entail. Section 2.1 will discuss network security protocol. The mechanisms will be discussed in the order that follows. Section 2.2 will discuss the proof-of-work (PoW) mechanism used in the Bitcoin protocol and various altcoins. Section 2.3 will discuss the proof-of-stake (PoS) protocol scheme first introduced by Peercoin in 2011, which relies on a less energy intensive security mechanism than PoW. Section 2.4 will discuss a hybrid PoW/PoS mechanism. Section 2.5 will discuss the Byzantine Consensus mechanism. Section 2.6 presents the results of a systematic review of 21 cryptocurrencies. Section 3 provides an overview of factors affecting industry growth, focusing heavily on the regulatory environment in section 3.1. Section 3.2 discusses public perception and acceptance of cryptocurrency as a payment system in the current retail environment. Section 4 concludes the analysis.

A note on sources: Because the cryptocurrency industry is still young and factors that impact it are changing on a daily basis, few comprehensive or fully updated academic sources exist on the topic. While academic work was of course consulted for this project, the majority of the information that informs this paper was derived from White Papers or synthesized using raw data.

A note on terminology: When used in its conceptual or possessive sense, “Bitcoin” will be capitalized, but when used in its unit sense, it will not be (i.e., “Bitcoin protocol” versus “2,000 bitcoins”). The abbreviation “BTC” will also be used to refer to Bitcoin units. All other altcoins will be referenced by their capitalized names.

SECTION 1: INDUSTRY OVERVIEW

1.1 A BRIEF HISTORY

Although the concept of electronic currency dates back to the late 1980s, Bitcoin, launched in 2009 by pseudonymous (and still unidentified) developer Satoshi Nakamoto, is the first successful decentralized cryptocurrency [2]. In short, a cryptocurrency is a virtual coinage system that functions much like a standard currency, enabling users to provide virtual payment for goods and services free of a central trusted authority. Cryptocurrencies rely on the transmission of digital information, utilizing cryptographic methods to ensure legitimate, unique transactions. Bitcoin took the digital coin market one step further, decentralizing the currency and freeing it from hierarchical power structures. Instead, individuals and businesses transact with the coin electronically on a peer-to-peer network. It caught wide attention beginning in 2011, and various altcoins – a general name for all other cryptocurrencies post-Bitcoin – soon appeared.

Litecoin was released in the fall of 2011, gaining modest success and enjoying the highest cryptocurrency market cap after Bitcoin until it was overtaken by Ripple on October 4th, 2014. Litecoin modified Bitcoin's protocol, increasing transaction speed with the idea that it would be more appropriate for day-to-day transactions. Ripple, launched in 2013, introduced an entirely unique model to that used by Bitcoin and currently maintains the second highest market capitalization of approximately $255 million (April 22) [1] [3]. Another notable coin in the evolutionary chain of cryptocurrency, Peercoin, employs a revolutionary technological development to secure and sustain its coinage [4]. Peercoin merges the PoW technology used by Bitcoin and Litecoin along with its own mechanism, proof-of-stake (PoS), to employ a hybrid network security mechanism. More recently NuShares/NuBits have emerged, introduced in August 2014, which rely on a dual currency model almost entirely divorced from the single currency model used by previous coins [5].

At the time this paper was written, the cryptocurrency industry consisted of over 550 coins with varying user bases and trade volumes [1]. Because of high volatility, the market capitalization of the cryptocurrency industry changes dramatically, but is estimated at the time of this paper to be just over $3.5 billion, with Bitcoin representing approximately 88% of the market cap [1].

1.2 IN THE BEGINNING WAS BITCOIN

Bitcoin is an open source, peer-to-peer digital currency first proposed in a 2008 white paper published under the name of Satoshi Nakamoto. Nakamoto begins his paper by stating that "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 weakness of the trust based model" [2]. Further, the existence of a trusted intermediary increases transaction costs, "cutting off the possibility for small casual transactions." Additionally, the trusted intermediaries are pressured to gather as much information about the parties as possible in order to control transaction costs. Hence, Nakamoto sought to create a coin that completely removed any trusted central authority and replace

trust with cryptographic proof. This system would have the added benefits of having low transaction fees, low latency (time to make transactions), and pseudo-anonymity.

A bitcoin, and every subsequent cryptocurrency, is merely "a chain of digital signatures" where "Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin" so that ownership can dynamically be programmed into the coin [2]. Further, these lines of computer code are stored in a program called a "wallet" on personal hard drives and/or via online wallets like Coinbase. Like cash or commodities, bitcoins can be lost, stolen or destroyed. One British man became famous for throwing out his hard drive, and with it his wallet containing over 7,000 BTC, which had a market value of approximately $7 million at the time [6]. The prominent Bitcoin exchange, Mt. Gox, had nearly $350 million worth of bitcoin stolen in February 2014, forcing the exchange to declare bankruptcy and highlighting security issues within the cryptocurrency world [7].

Bitcoins can only be sent or received by logging the transaction on the public ledger, also known as the "blockchain." Bitcoins lack intrinsic value; rather, Bitcoin's value is purely a function of supply and demand [8]. Unlike paper "fiat currency" that derives value from a government, Bitcoin is neither created by, nor backed by, any government. Bitcoin protocol seeks to solve the double-spending problem (essentially, spending the same coin more than once) inherent in non-cash payment systems resulting in the need for a trusted third party (such as a bank or credit card company) to verify the integrity of the transaction. Double-spending occurs when an asset is duplicated, and thus can be spent multiple times. This problem does not exist in physical currencies, since transactions involve changing possession of property. However, a digital file has the potential to be copied. The security of cryptocurrency, however, and its ability to safeguard against such digital copying, is inherent in its blockchain or public ledger systems. These systems keep records of ownership and transaction timestamps, eliminating the possibility of digital copying and, thus, double-spending. The mechanism used to secure the network is discussed deeply in section 2. In the case of Bitcoin, a transaction is only complete and added to the blockchain once a required amount of computational power is used so as to satisfy the proof-of-work (discussed in section 2.1). The transaction at this point is considered complete, and ownership of the coin has been absolutely transferred, without fear of double-spending, because the entire network becomes informed of which wallet the coin currently resides in.

Bitcoin was introduced to the public on January 3rd, 2009, but traded for less than a dollar until February 2011 [1]. Bitcoin reached an all-time high of $1151/coin on December 4th, 2013, and has since steadily declined (see figure 8). Despite this decline, it is apparent that daily trading volume has held steady for the past year (see figure 5). Further, the number of unique transactions, including (see figure 1) and excluding popular addresses (see figure 2), is increasing steadily, despite a sliding price [9].

SECTION 2: COMPETING CRYPTOCURRENCIES

According to coinmarketcap.com, there are just over 550 distinct cryptocurrencies at the time this paper is written [1]. Thus, the cryptocurrency industry includes much more than just Bitcoin, although Bitcoin has a market capitalization of approximately 3.3 billion compared to the total market capitalization of the cryptocurrency industry of 3.8 billion (86%) [1]. This section seeks to analyze how competition in the cryptocurrency industry has evolved since the inception of Bitcoin in 2009. Specifically, it explores the evolution of network security protocols and changing trends in coin economics.

2.1 NETWORK SECURITY PROTOCOL

Perhaps Bitcoin's greatest technological achievement (and the sine qua non of every altcoin) is building a peer-to-peer transaction system that relies on "cryptographic proof rather than trust" [2]. However, replacing a central authority presents a unique problem with a solution that is not obvious. First, the coin needs to be able to change ownership. Transactions are recorded by combining the digital signatures of each party and a timestamp, so that the transaction date is recorded. This new code represents the coin and its path through the network. This code is then broadcasted to all nodes (computers connected to and running the cryptocurrency network software) on the network. However, it is necessary that the majority of the nodes agree on transactions that have occurred, otherwise double-spending and denial-of-service (DoS) attacks can occur. The mechanism used to reach consensus among nodes puts integrity in the system by verifying that the transaction is indeed legitimate. Hence, transactions are verified, and the system made secure, by implementing certain mechanisms that make it too costly to violate the integrity of the system. Larry Ren, developer of Reddcoin, notes, "The underlying principle of such a mechanism is the necessity of expending resources when confirming transactions" [10]. Various cryptocurrencies have developed novel resources to use as a means of network security. The resource can be a combination of electricity, time, or temporary surrender of coinage, and represents the cost to secure the network. Miners - those who own the underlying resource, and thus expend it - secure the network, and are compensated for their work in the form of either transaction fees or newly minted coins. The mechanism used to secure the network determines the resource chosen and the method used to pay the miners. Thus, the underlying network security mechanism of each coin has a significant impact on the underlying economics of the coin. Sections 2.2 through 2.5 explain the most widely used mechanisms in the industry. Section 2.6 presents the results of a systematic literature review of 21 coin white papers and resulting conclusions.

2.2 PROOF-OF-WORK

First proposed by Cynthia Dwork and Moni Naor in 1993, "A Proof-of-Work (PoW) is a piece of data which is costly to produce so as to satisfy certain requirements but is trivial to verify" [11]. That is, PoW adds an economic cost to perform a given function. In the case of cryptocurrencies, transactions are not considered verified until a certain amount of energy has been expended. Most altcoins that use the PoW mechanism are direct copies of, or are very similar to, Bitcoin's protocol. The following section will focus on how the mechanism is implemented by Bitcoin.

2.2.1 BITCOIN

Under the Bitcoin protocol, all transactions during a certain time period are collected into something called a block. This block is then broadcasted to all the nodes currently connected to the Bitcoin network. Bitcoin uses the Hashcash PoW mechanism, first proposed by Adam Back in 1997 [12]. Under this mechanism, in order to agree upon a set of broadcasted transactions, each node essentially takes the block and begins adding a piece of data to the block called a nonce, such that the (block+nonce), when put into a hashing algorithm, has a hash that meets certain requirements - in this case, it begins with a certain number of zeros. Thus, each node attempts to solve a complex mathematical computation, the result of which can be easily verified by computing a single hash. The Bitcoin protocol requires that nodes use the SHA-256 hashing function [2]. Once a node finds a solution to the problem, the PoW requirements are considered satisfied, and the new (block+nonce+hash) is added to the blockchain and broadcasted to all nodes. Because only one block can be verified at a time, the probability a node will solve for the correct hash increases proportionally with the amount of CPU power expended. Hence, the resources consumed in this instance are electricity and time, which are indeed scarce.

2.2.2 BITCOIN MINING

The entire process undergone by each node is called mining, because in each block that is verified, the node (now the miner) receives a payment for his service. Miners are rational profit seekers, so in order to incentivize individuals to mine, the Bitcoin protocol offers rewards in two forms: transaction fees and newly minted coins, called mined coins [2]. Each block that gets verified under the Bitcoin protocol introduces new coins to the market, which are given to the miner as payment for the energy and time expended [2]. This number decreases with time so that there will never be over 21 million BTC in existence [2]. In this way, Bitcoin functions similarly to commodities like gold: “The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation” [2]. Hence, in the long run, transaction fees will likely have to increase to compensate miners appropriately. A major criticism of the PoW mechanism is the massive amounts of energy it consumes, with no other benefit than to verify transactions. Thus, as the mint rate slows in the Bitcoin network, “eventually it could put pressure on raising transaction fees to sustain a preferred level of security” [13]. It is already evident that miners’ revenue has been declining dramatically (see figure 6).

2.2.3 HASHING ALGORITHMS

In addition to the network security mechanism, hashing algorithms also affect the coin. For PoW mechanisms, the hashing algorithm and the target difficulty of the hash dictate how many hashes - how much energy - is expected to be spent. Because miners are incentivized to find ever more powerful computing equipment, this has created a mining arms race. For instance, mining originally was carried out by CPU (Central Processing Unit); however, the same functions could be carried out by GPU (Graphics Processing Unit) at a much faster rate. GPUs then gave way to Application Specific Integrated Circuits (ASICs), designed to carry out PoW mining at incredible speeds - magnitudes higher than could be done through GPUs. The SHA-256 algorithm used in Bitcoin and various altcoins felt the brunt of this arms race, and many coins have introduced

alternative hashing algorithms that are often praised as being ASIC-resistant [10]. However, this is not the case, as ASICs can be designed to carry out any hashing algorithm. It is expensive to do so, so until miners receive enough incentive to build ASICs for a particular hashing algorithm other than SHA-256, like Scrypt, they will likely not. There has been a dramatic increase in the number of giga hashes per second expent on the Bitcoin network (see figure 7).

Another problem with this is that economies of scale are created. In order to be decentralized, coins need to have the security distributed among many users. However, small-scale investors no longer see it as profitable to connect their home computers to the coin network, as they would then be forced to compete with much faster ASICs. Hence, this arms race has had the side effect of essentially centralizing network authority into the hands of the largest miners.

2.3 PROOF OF STAKE

An alternative to the PoW mechanism is the Proof-of-Stake (PoS) mechanism. Instead of relying on computational power as its "scarce resource," the resource that the network security depends on is ownership of the coin itself – "proof-of-stake means a form of proof-of-ownership" [4] – which is also scarce. Hence, in order to verify a transaction and receive the coin reward (whether new coins or transaction fees), a miner must own some coin himself. Further, the probability that he succeeds in creating a new block is a function of the amount of coin he owns, not of computational power. Hence, there are very little energy costs in this transaction. Further, in order to undermine the integrity of the system, one would have to own more than 50% of the coin currently being staked, in which case violating the coin security would be very costly [4]. Generally, payment takes the form of an "interest" on the amount of coin staked to verify the transaction [4]. Hence, most PoS coins do not have a capped money supply, and are thus inflationary. However, PoS systems are faced with the challenge of how to initially distribute the coin. Whereas PoW distributes the coins to the miners who add value to the network, a coin that relies purely on PoS must decide whom to distribute the coins to. This can create a host of problems. In fact, most pure PoS coins have turned out to be fraudulent, as the creator often gives himself the majority of the coins [10].

2.4 HYBRID POW/POS

A hybrid PoW/PoS system uses the PoW mechanism for initial coin minting and distribution. That is, PoW allows the network to distribute new coins to miners. However, over time, the PoS mechanism phases out the PoW mechanism, creating a long-term energy efficient cryptocurrency. Sunny King and Scott Nadal, in their white paper "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," are the first to propose and then implement such a hybrid PoW/PoS system. In this hybrid-design, block generation, instead of relying on one CPU per vote, relies on a concept of "coinage" [4]. Coinage is roughly the amount of coin owned multiplied by the life of ownership by the current owner of the coin. Block generation thus goes to the block with the most coinage. Further, coins are minted according to one percent per coin-year consumed, which functions as an interest rate for staking coin [4]. The main advantage, however, is that this system does not rely on high-energy consumption in the long run. Hence, the design

is cost-competitive to that which relies on PoW and avoids the distribution problem inherent in PoS.

2.5 BYZANTINE CONSENSUS

Ripple and Stellar offer an alternative security mechanism entirely, which are both implementations of the Byzantine Consensus Protocol [13] [3]. The infrastructure of the coins is that of a distributed network, where each server in the network is faced with the problem of deciding whether other servers in the network are sending accurate messages. The messages in this case are transactions. This system is tolerant of a class of failures known as the Byzantine Generals problem and is thus deemed Byzantine fault tolerant [14]. In the Byzantine Generals problem, the Byzantine army is divided among multiple lieutenants who receive an order of attack or retreat from a commanding general. However, there are a number of traitors - potentially the commanding general himself - yet all loyal generals need to reach consensus despite a small number of traitors working to foil this plan. The problem is that the loyal lieutenants need to reach consensus on which order to obey by sending each other signed messages. Various algorithms have been proposed that provide solutions to the above problem.

The distributed networks created by Ripple and Stellar face a problem analogous to the Byzantine Generals problem. First, individuals engaging with one of these coins would have to join a server. Each server in the network is faced with the problem of deciding whether other servers in the network are sending accurate "messages," which in this case are transactions. Ripple's protocol requires that entities join a server. Each server maintains a Unique Node List (UNL), whereby the server only communicates with the nodes on its UNL. This allows servers to be in contact with only trusted servers. Any server can broadcast transactions, and the servers then vote on the transactions. However, servers vote only on transactions that came from other nodes on its UNL. Every few seconds, the servers all send messages back and forth, until the algorithm terminates with consensus or failure to reach consensus. The specific algorithm used in Ripple requires that a transaction be accepted by 80 percent of the servers in order for consensus to be reached. This security mechanism is both much more energy efficient than the PoW mechanism, requires at least an 80% attack on the network in order for the network security to be violated (the algorithm terminates without consensus if there is not 80% agreement), allows for flexible trust, and offers faster transaction times [3].

The main features of each mechanism are summarized below:

Mechanism	Decentralized control	Low latency	Flexible trust	Long-run Low Energy Cost
PoW	✔			
PoS	✔	maybe		✔
Byzantine consensus	✔	✔	✔	✔
PoS/PoW	✔	maybe		✔

Table 1: Information Derived/ Reproduced From [13]

2.6 RESULTS

This section presents the results of a systematic review of coins which meet two criteria: they have a market capitalization, as measured by coinmarketcap.com, of at least $1 million as of April 2015, and they were released prior to January 1st, 2015, so as to allow a maturity time. There were 21 coins that met these parameters. The primary method of review was through their white papers, although several coins did not have white papers, in which case the material was gathered from the coins' websites. Answers to the question "how has network security mechanisms in the cryptocurrency industry evolved since the inception of Bitcoin in 2009?" can now be drawn from the information that follows. The table below summarizes the major characteristics of each coin, listed in descending order of market capitalization numbers.

Release	Currency	Market Cap (April 23rd)	Hash Algorithm	Mechanism	Supply	Deflationary	Theoretical Long Term Inflation	Source
Jan-09	Bitcoin	$3,312,281,631	SHA-256	POW	21,000,000	yes		[2]
Sep-13	Ripple	$255,536,445	ECDSA	Byzantine Consensus	100,000,000,000	yes		[3]
Oct-11	Litecoin	$55,662,783	Scrypt	POW	84,000,000	yes		[15]
Jan-14	Dashcoin	$19,482,137	X11	POW & POS	22,000,000	yes		[16]
Aug-14	Stellar	$13,115,557	Undefined	Byzantine Consensus	Unlimited	no	1%	[13]
Jul-14	Bitshares	$11,688,038	Undefined	Undefined				[17]
Dec-13	Dogecoin	$10,841,501	Scrypt	POW	Unlimited	no	0%	[18]
Nov-13	Nxt	$9,606,282	Curve25519 and SHA-256	POS	1,000,000,000	yes		[19]
Aug-12	Peercoin	$5,073,573	SHA-256	POW & POS	Unlimited	no	1%	[4]
May-14	Monero	$4,433,105	CryptoNight	POW	18,400,000	yes		[20]
Jul-12	Bytecoin	$4,199,290	CryptoNight	POW	184,470,000,000	yes		[21]
Apr-11	Namecoin	$3,845,575	SHA-256	POW	21,000,000	yes		[22]
Jun-13	Ybcoin	$2,991,777	Scrypt	POW & POS	3,000,000	yes		[23]
Jan-14	Counterparty	$2,402,854	SHA-256	POB	2,650,000	yes		[24]
Aug-14	NuShares/NuBits	$3,901,430	Undefined	POS	1,000,000,000	yes		[5]
Dec-14	Paycoin	$2,294,250	SHA-256	POW & POS	12,500,000	yes		[25]
Sep-14	ARCHcoin	$2,228,501	Scrypt	POS	16,200,000	yes		[26]
Mar-14	Monacoin	$1,798,198	Scrypt	POW	105,120,000	yes		[27]
Nov-14	Faircoin	$1,201,450	Undefined	POS	Unlimited	no	1.50%	[28]
Jul-14	BitcoinDark	$1,133,283	SHA- 256	POW & POS	22,000,000	yes		[29]
Feb-14	Blackcoin	$1,113,916	SHA- 256	POS	Unlimited	no	1%	[30]

Table 2: Breakdown of 21 coins

	2009	2010	2011	2012	2013	2014	Total
POS					1	4	**5**
POW/POS				1	1	3	**5**
POW	1		2	1	1	2	**7**
Byzantine Consensus					1	1	**2**
Other						2	**2**

Table 3: Evolution of Network Security Mechanisms

Mechanism	Combined Market Capitalization
POS	$18,051,579
POW/POS	$30,975,020
POW	$3,393,062,083
Byzantine Consensus	$268,652,002

Table 4: Market Capitalizations by Mechanism (Data from April 23, 2015 [1])

The final results of the systematic review of each coin suggest that a standalone PoW or PoS system is not feasible by itself. The PoW system is not feasible long-term as it is energy intensive, typically deflationary, and tends to create economies of scale within the mining community. Similarly, PoS can be feasible in the long run, but it faces the logistical issue of how to initially distribute the coins. A hybrid system, however, is much more flexible regarding inflationary and deflationary tendencies, is energy efficient long-term, and relies on the successful PoW distribution system for initially distributing coins. The trend in the industry appears to be growing consensus of the hybrid mechanism among the cryptocurrency community, as measured by the number of successful coins introduced recently. However, alternative methods have also been proposed with noteworthy success. Ripple and Stellar are two such examples. However, the value of a coin today is largely a function of acceptance and network size, so even if Bitcoin's current characteristics render it functionally suboptimal, it will likely take time for an alternative coin to outpace it in terms of user base and trading volume.

SECTION 3: FACTORS THAT AFFECT GROWTH

Despite the traction that cryptocurrency has gained over the last half decade, its path has been turbulent. Many argue that the performance of anarchic cryptocurrency has been underwhelming in comparison to the hype it stirred when it publicly emerged in 2009 [31]. This section will address two of the main factors that have affected the growth of the cryptocurrency industry and will continue to influence its development and integration into the broader financial scheme well into the future: international government regulatory attempts, and ambivalent public perception in moving toward its wider adoption.

3.1 GOVERNMENT REGULATIONS

While the expanding cryptocurrency market has the potential to revolutionize the way money is exchanged, its introduction into global venues is fraught with challenges and potential pitfalls. Because virtual currencies are not universally recognized as official means of paying for goods and services, developing standardized systems for their use is critical. For the currencies to be sustainable, their legal status must be established.

Regulatory systems are burgeoning, with myriad approaches being taken by various governments. Current regulatory measures are in their infancy and continue to evolve with the rapidly expanding industry.

Regulations will offer greater legitimacy to a currency struggling to gain mass acceptance. They will standardize elements of the market and minimize at least some of the volatility. While governments are testing an amalgam of regulatory steps, their end goal is the same: to limit fraud, protect consumers, respect economic sanctions, and institute viable taxation methods [32]. A brief detail of current cryptocurrency policy in various states will offer clarity and a broad overview of contemporary regulation attempts. Because of the infancy of virtual currency, available data is in flux and subject to frequent change.

The United States takes a permissive, slightly neutral stance on cryptocurrencies. The current challenge faced by regulators is expanding existing laws to allow for the unique aspects and challenges of the virtual currency world. For taxation purposes, virtual currencies are handled as property rather than as currency, and transactions are subject to the same taxation norms as other types of property.

At a federal level, the Financial Crimes Enforcement Network (FINCEN) has taken the forefront on implementing regulatory methods. The FINCEN's early attempts to clarify cryptocurrencies' place in the financial market came in 2013 with its announcement that while individual use of virtual currencies is not to be considered a money service business (MSB), exchanges and conversion of virtual currencies *do* fall under the definition of a money service business [33]. As such, virtual currency transmitters must follow the government requirements already established for MSBs, including reporting techniques, record-keeping and abiding by the Bank Secrecy Act of 1970. This is significant in that it demands a degree of accountability from virtual currency transmitters, as well as one more layer of security against fraud.

Individual U.S. states also have a large role in establishing regulations for the emerging currency. As of April 2015, 12 states and Puerto Rico have instituted licensing protocol for virtual coin operations [34]. Currently, California has more cryptocurrency activity than any other state, and has been proactive in incorporating digital currencies into existing financial frameworks [35]. In January of 2015, cryptocurrency gained legal status in California, leading to predictions that other states would follow suit [35]. New York has also taken note of the emerging market, currently in the final stages of instituting its own regulatory framework [36].

Australia, whose citizens account for roughly 7% of Bitcoin users, has not formally adopted regulations for virtual currency, but has established a system of taxation for the coinage [37]. Trading done in the form of cryptocurrency is subject to the country's pre-existing tax rules relating to goods and services. While the Australian government has been clear that "Bitcoin is not a legally recognized universal means of exchange and form of payment by the laws of Australia or the laws of any other country," it has provided space for the cryptocurrency to comfortably exist [38].

Canada perhaps has the most cohesive and developed system of regulation, being the first country in the world to establish a tax on virtual currencies. This taxation system seeks to minimize the risks most frequently associated with cryptocurrencies: money-laundering and terrorist-funding. The Bank of Canada has expressed a willingness to acknowledge the developing virtual currency market, but currently recognizes cryptocurrencies as investments rather than currency [33].

Russia has reacted less favorably to the emergence of cryptocurrencies. The Bank of Russia shared concerns that the currency could facilitate money-laundering attempts, as well as be convenient means to transport funds to terrorist organizations. Additionally, the bank argued that virtual currency violates federal law mandating one central bank and currency [39]. Last year, the Ministry of Finance announced its intent to restrict use of cryptocurrency as a means of payment. In February of 2015, Russia's Prosecutor General's Office claimed that Bitcoin "cannot be used by individuals or legal entities." And in April, Deputy Minister of Finance Alexei Moiseev reiterated that position, stating "The law, which provides measures for penalizing the usage of monetary surrogates, will finally be passed this year" [40]. Indeed, Russia's crackdown on the currency is already evident, with at least half a dozen cryptocurrency websites blocked at the beginning of 2015 [41].

This skepticism towards "money surrogates" is shared by China, which has also taken steps to restrict the use of virtual coinage. In December of 2013, China's Central Bank prohibited financial institutions from handling Bitcoin transactions, limiting legal trade of the coin to individuals and private parties [42]. Citizens are being encouraged to treat bitcoins and other cryptocurrencies as a good rather than a viable currency.

The trend towards restriction is mirrored in other countries. Vietnam has firmly cautioned its citizens on the use of cryptocurrencies. While there is no regulation specifically relating to virtual currency usage, the Bank of Vietnam has warned that Vietnam does not consider virtual currency to be a legitimate form of currency [33]. Transactions utilizing forms of cryptocurrency are not covered by legal protections.

The following chart summarizes attempts made by various governments to define legal parameters for cryptocurrency and to regulate its activity and usage:

Content/Scope	Country	Additional Information
Prohibition	China	December 5th, 2013, China's Central Bank prohibited financial institutions from handling Bitcoin transactions. Individuals and private parties can legally trade Bitcoin. [43]
	Russia	In February 2015, Russia's Prosecutor General's Office claimed that Bitcoin "cannot be used by individuals or legal entities." [44]
	Iceland	The Icelandic Central Bank said "it is prohibited to engage in foreign exchange trading with the electronic currency bitcoin, according to the Icelandic Foreign Exchange Act"[3]

Prohibition of ATM's	Taiwan	Approval for Bitcoin ATMs refused.
Protection from money laundering & illicit activities	Singapore	Financial intermediaries to verify the identities of their customers and report suspicious transactions.
	USA	Bitcoin exchanges and most miners obliged to collect information on potentially suspicious transactions and report these to the federal government
Taxing Bitcoin		The sale, exchange or use of Bitcoin for payment in a real-world economy transaction may result in tax liability.
	Japan	The tax will cover gains from trading bitcoins, purchases made with bitcoins and revenues from transactions. Banks and securities firms will be prohibited from Bitcoin trades.
	Finland	Rules on taxation of capital gains apply when profits are in Bitcoin after it was obtained as payment is also taxable.
	Germany	Profits from mining or trading subject to capital gains tax unless hoarded for at least one year
Unclear	Israel	The Bank of Israel, the Capital Market, Insurance and Savings Department, the Israel Tax Authority, the Israel Securities Authority, and the Israel Money Laundering and Terror Financing Prohibition Authority issued a joint statement warning of the risks cryptocurrencies posed to users. However, no regulation has been established.
	India	The Reserve Bank of India's Secretary General, Ajit Prasad, said "The creation, trading or usage of virtual currencies including bitcoins, as a medium for payment are not authorized by any central bank or monetary authority." However, cryptocurrencies are currently not regulated.

Table 5: Information Derived/Reproduced From [45] [33]

3.2 PUBLIC PERCEPTION

While retailers are starting to officially respond to the virtual currency market, the scope of the currency's success is ultimately contingent on gaining public acceptance. The intrinsic value of cryptocurrency is in its number of users; without public trust, the system of virtual currency as an alternative payment method is unsustainable. This road is complicated and will require massive amounts of education and assurance to assuage a skeptical public, particularly in light of recent events indicating the volatility of cryptocurrency. This section will highlight both positive and negative factors related to public perception that have and will likely continue to affect the growth of the cryptocurrency industry.

Slowly, through news stories and pioneering individuals championing its virtues, cryptocurrency is gaining a presence in the global market. However, despite the recent surge in media coverage, cryptocurrencies are still widely unknown by the general public. Coincenter.com has conducted a monthly survey for the past eight months, tracking American public sentiment towards Bitcoin. Since Bitcoin is by far the most prominent of the cryptocurrencies, much can be inferred about attitudes towards cryptocurrency as a whole. April's results indicate that the average person is still largely unaware of Bitcoin's

existence. Only 4.5% of those surveyed had ever used the currency [46]. This statistic, coupled with survey results indicating skepticism regarding Bitcoin's usefulness today, forms an underwhelming picture.

Users and Transactions

Gauging public perception of a nascent concept - particularly one that involves a certain level of risk and the potential to significantly alter the status quo - is typically difficult, as many factors contribute to shaping it. Quantifiable evidence of success or failure, however, plays a role in informing public opinion. In the cryptocurrency industry, the three largest indicators of success are the market capitalization, the estimated number of cryptocurrency users, and daily transaction volume. Market capitalization was introduced in the table in section 2.6. The estimated number of users and transaction volume will be discussed below. All three factors lend legitimacy to the system as they indicate the level of trust that has been placed in it. These numbers will serve as indicators of the extent to which cryptocurrency has already been accepted by the public, which is one metric for gauging public perception.

An exact number of cryptocurrency users is impossible to obtain. Even estimates are difficult to determine with strong confidence, as one of the key characteristics of the cryptocurrency industry is the degree of anonymity afforded to its users; though transaction history is transparent, personal identity remains difficult to trace. Arguably the most accurate way to estimate the number of users is to examine the number of wallets created. As of May 2015, the number of Bitcoin wallets in created in My Wallet, a large online wallet, is approximately 3.3 million [9]. The number of wallets increases by approximately 5,000 wallets per day in April 2015 (see figure 4) [9]. Though this provides some indication of the number of users, it is also important to bear in mind that it is possible for a single user to own multiple wallets or to open a wallet without necessarily having Bitcoin in it. Data on altcoin users is even more difficult to obtain.

While the user count is unclear, there are exact figures relating daily transaction volume. With a market cap currently at $3.3 billion, the transaction volume of Bitcoin on a monthly basis has held steady over the past year (see figure 5), and has averaged just under $50 million USD [9] [1].

Retailers

Within the six years since Bitcoin and altcoins emerged in the public sphere, several large retailers have begun to accept cryptocurrency as a valid form of payment. Major retailers that accept Bitcoin, for example, include TigerDirect, Overstock.com, and Zanga [47]. Considering that cryptocurrency is still in its infancy, this can be perceived as a positive development.

But many more are reluctant to do so barring a significant increase in the estimated user base. In their 2013 paper "Bitcoin is Memory," William J. Luther and Josiah Olson write, "Few retailers accept Bitcoin as a form of payment due to the small user base; and many consumers will not consider using Bitcoin until a significant number of retailers accept

Bitcoin payments. Simply put: network effects favor the status quo.... Bitcoin may fail to gain widespread acceptance even if it were superior to existing monies" [48].

Fear has driven many companies, including banks, to thus far reject the embedding of cryptocurrency into their systems. While Bitcoin was founded as an anarchic alternative to the stiff policies and inhibitive regulatory nature of centralized currency schemes, this is ironically one of the main factors causing concern among financiers. The system operates on proof rather than trust, but overcoming a dependence on the latter seems to have proven difficult. Other concerns include the possibility of fraud, the sharp price volatility of Bitcoin, settlement risk, the potential for tax evasion, speculation over security, and recent instances of bankruptcy (see Mt. Gox below).

Aswath Damodoran, a finance professor at New York University, writes "While it may conflict with the vision of some Bitcoin revolutionaries, the Bitcoin economy may need a banking system of its own that is regulated and perhaps even insured by a centralized entity" [49]. This, however, would not only challenge the vision of "some" Bitcoin pioneers, but the grand purpose of Bitcoin to begin with. This would reintroduce the concept of "trust" into the system, which is exactly what Bitcoin's founders aimed to eliminate by substituting cryptographic proof mechanisms.

Mt. Gox

The highly publicized Mt. Gox theft has likely not furthered public trust in the currency. This breach in security resulted in massive losses for legitimate coin owners, and further paints virtual currency as a volatile and insecure "other" rather than a currency for everyday use. Much of these concerns could be mitigated with the right regulations. Guidelines and rules lend a degree of security and standardization to a volatile market; having federally mandated frameworks for cryptocurrency use strengthens the appeal to the average consumer, bringing the currency to the forefront of the market rather than a fringe hobby of eclectic Silicon Valley programmers.

SECTION 4: CONCLUSION

The cryptocurrency industry is rapidly moving forward. It has shown itself to be resilient in the face of major thefts, including Mt. Gox, and government shutdowns. Further, the industry has expanded dramatically in the number of coins currently in circulation. The industry has also shown its creativity in implementing workable solutions to deficiencies in the development of new coins. Bitcoin may not dominate the industry in the long run, but the industry owes its existence to the pioneering anarchic coin.

INDEX

Data for figures 1 to 8 was gathered from the website blockchain.info [9]. Figure 9 was gathered from the website Bitnodes [50].

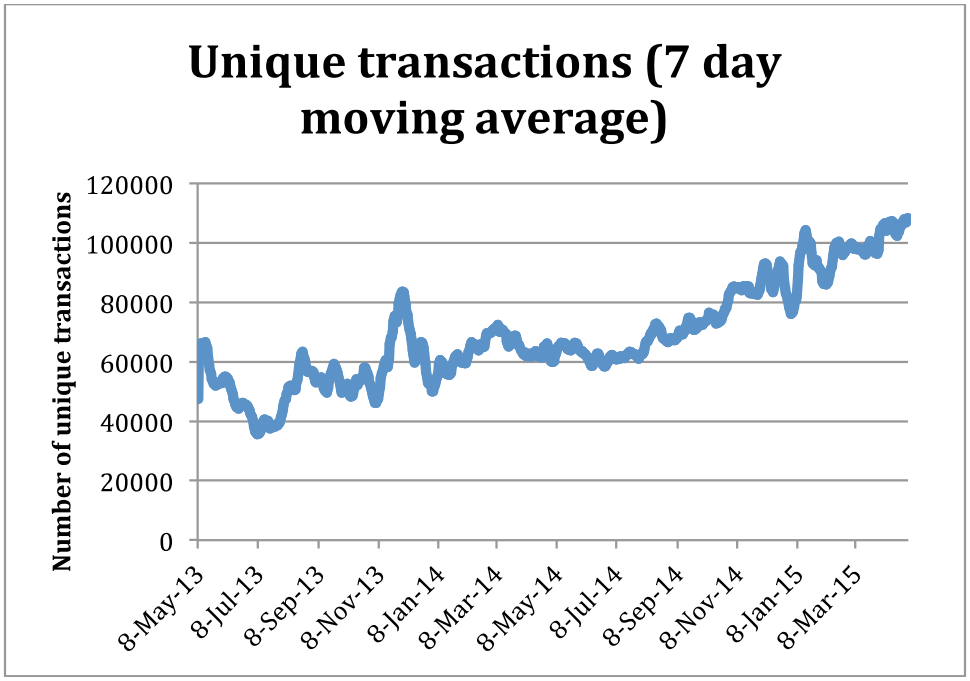

Figure 1: Number of unique transactions

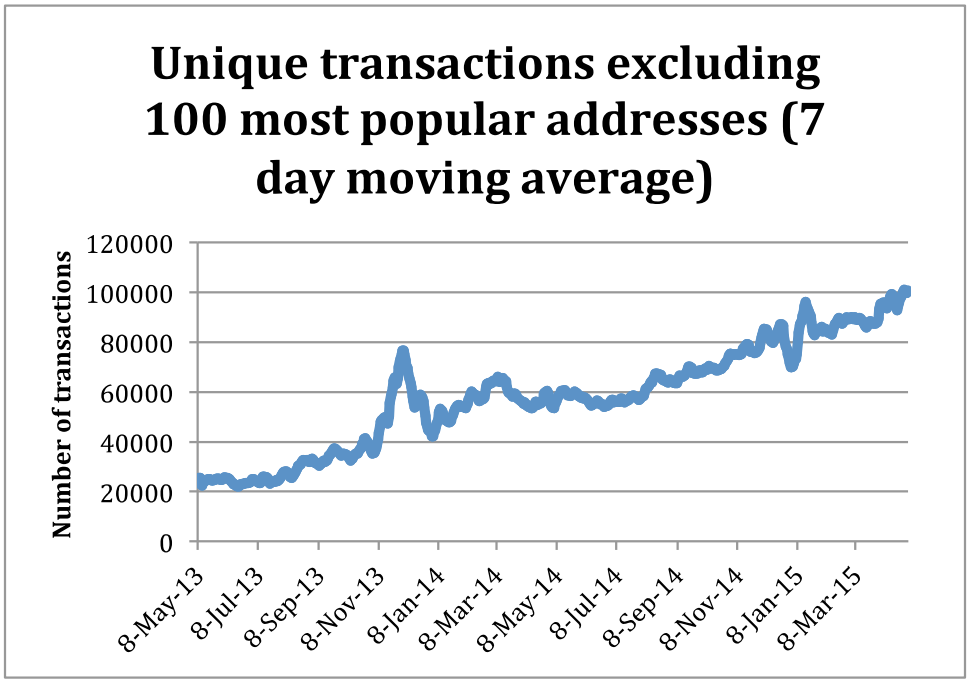

Figure 2: Number of unique transactions excluding popular addresses

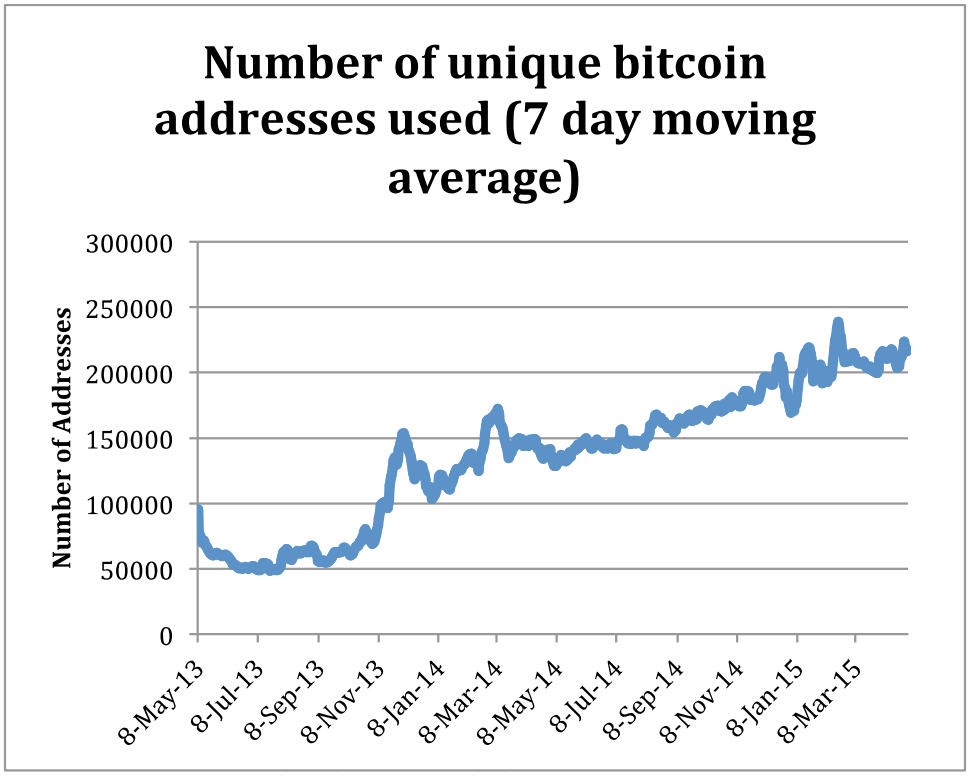

Figure 3: Number of unique addresses used

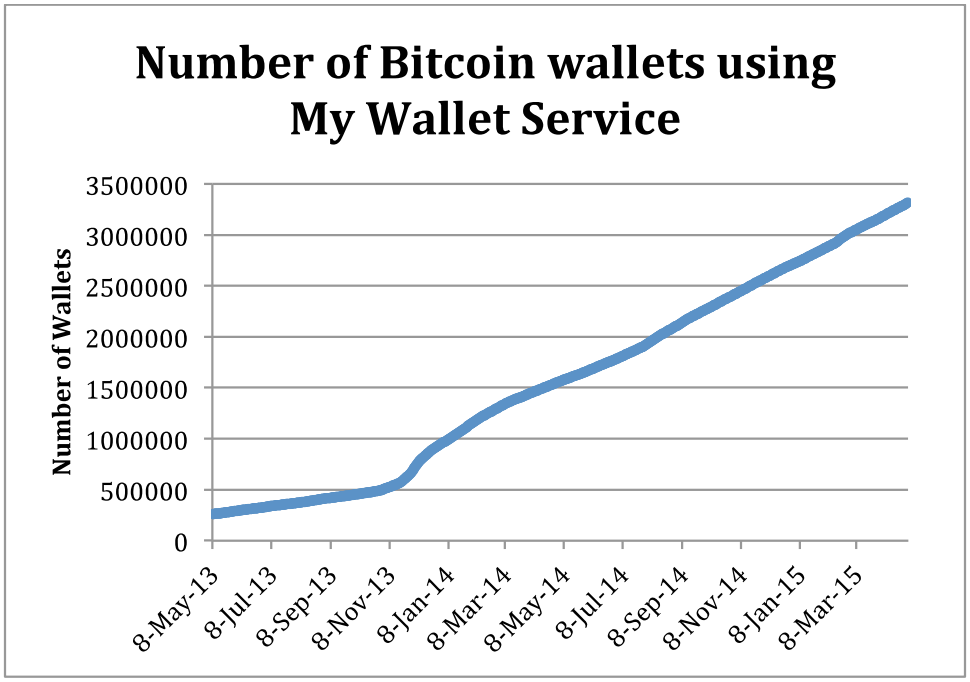

Figure 4: Number of wallets on My Wallet

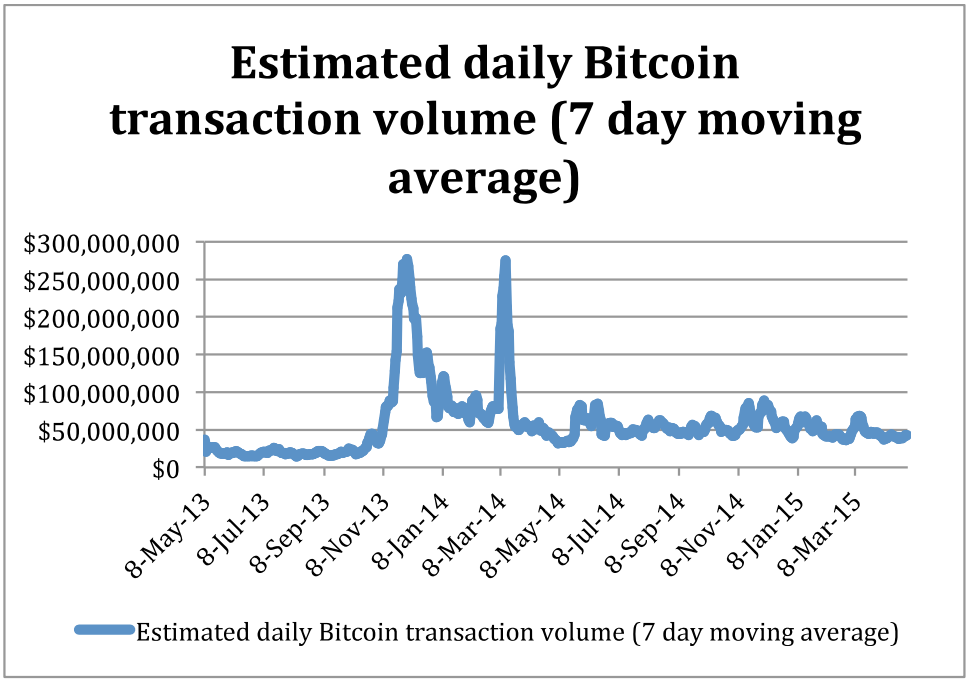

Figure 5: Transaction Volume USD

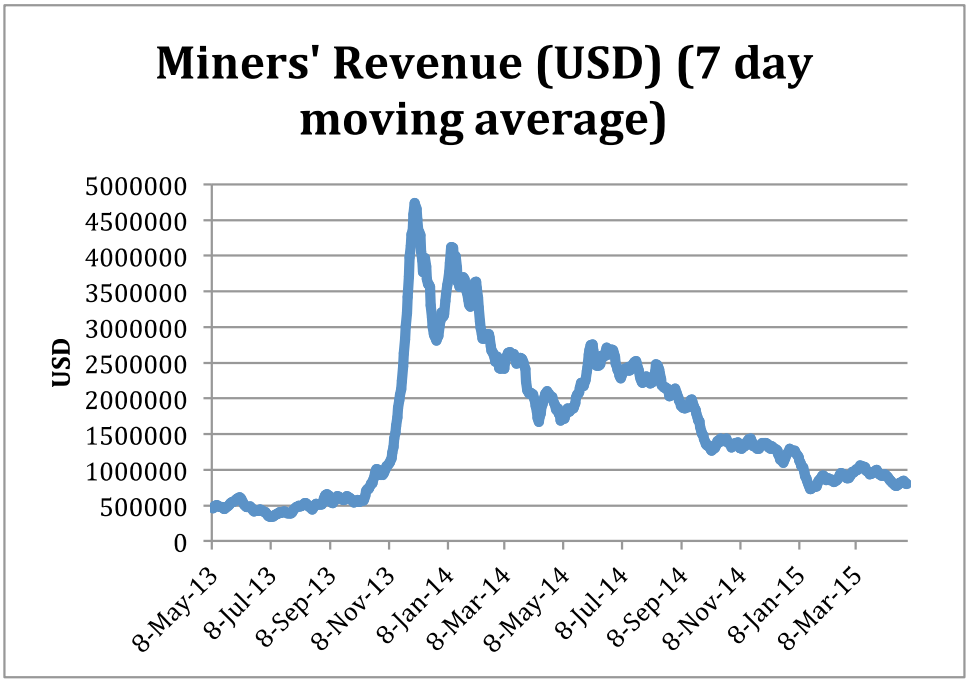

Figure 6: Bitcoin miners' total revenue (USD)

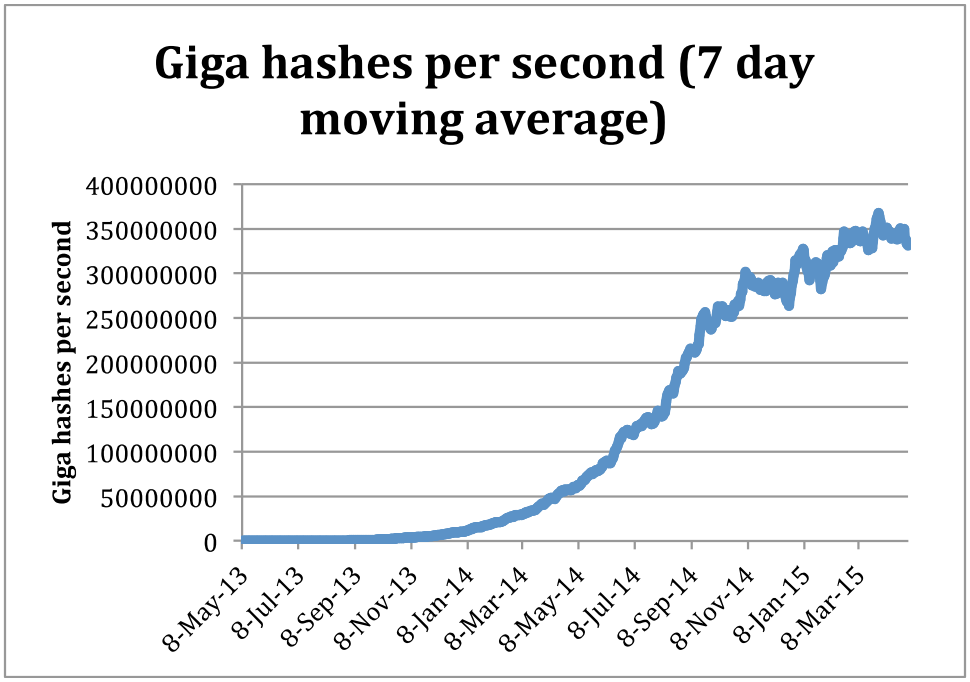

Figure 7: Increased Bitcoin mining competition (giga hashes per second)

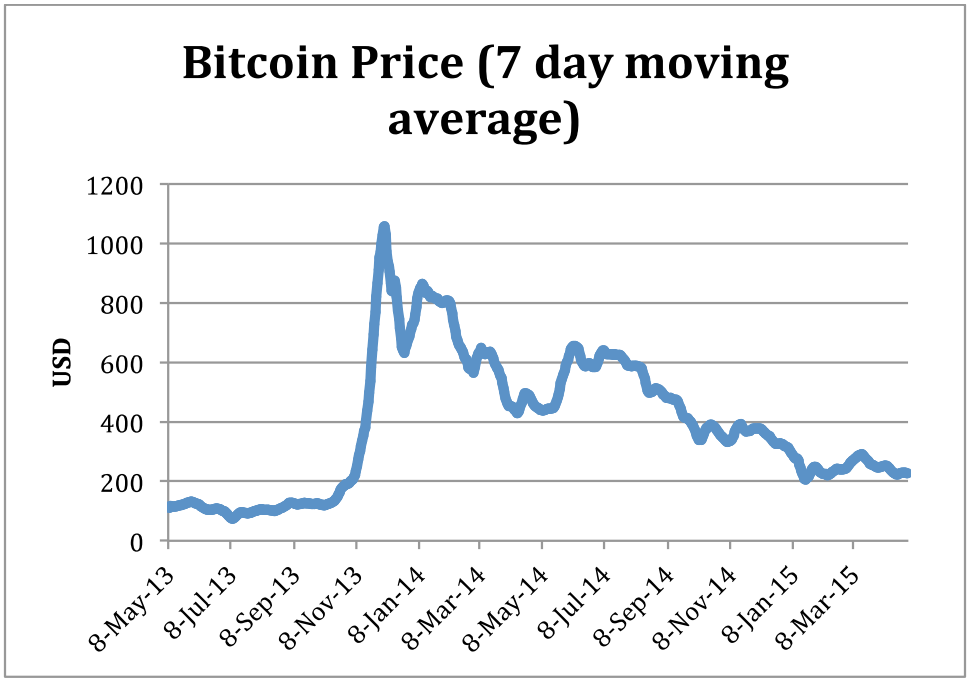

Figure 8: Bitcoin price in USD

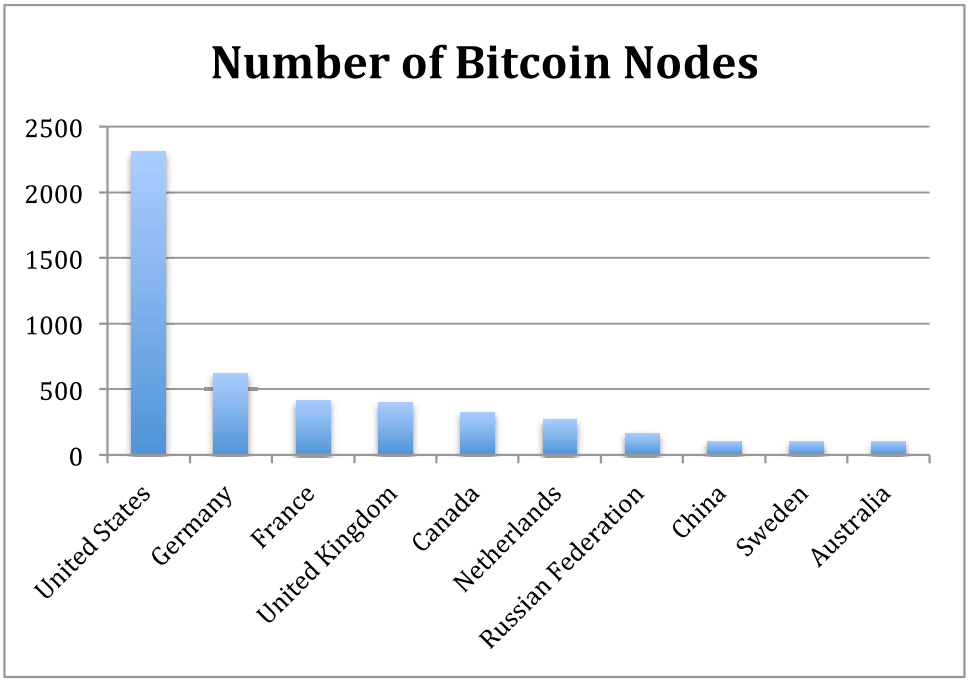

Figure 9: Number of Bitcoin nodes by country

Works Cited

[1] Crypto-Currency Market Capitalizations. [Online]. http://coinmarketcap.com/

[2] Satoshi Nakamoto. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. https://bitcoin.org/bitcoin.pdf

[3] David Schwartz, Noah Youngs, and Arthur Britto, "The Ripple Protocol Consensus Algorithm," Ripple Labs Inc,.

[4] Scott Nadal Sunny King. (2012, August) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. [Online]. http://www.peercoin.net/assets/paper/peercoin-paper.pdf

[5] Jordan Lee. (2014, September) Nu. [Online]. https://nubits.com/sites/default/files/assets/nu-whitepaper-23_sept_2014-en.pdf

[6] Bill Chappell. (2013, November) npr. [Online]. http://www.npr.org/blogs/thetwo-way/2013/11/27/247577278/man-laments-loss-of-thousands-of-bitcoins-as-value-hits-1-000

[7] Pete Rizzo. (2014, February) CoinDesk. [Online]. http://www.coindesk.com/mt-gox-loses-340-million-bitcoin-rumoured-insolvent/

[8] MARC ANDREESSEN. (2014, January) The New York Times. [Online]. http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

[9] Blockchain info. [Online]. https://blockchain.info/

[10] Larry Ren, "Proof of Stake Velocity: Building the Social Currency of the Digital Age," 2014.

[11] Cynthia Dwork and Moni Naor ,., 1993.

[12] Adam Back, "A partial hash collision based postage scheme," 1997.

[13] David Mazières. (2015, April) The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus. [Online]. https://www.stellar.org/papers/stellar-consensus-protocol.pdf

[14] Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, pp. 382-401, December 1982.

[15] Litecoin. [Online]. https://litecoin.org/

[16] DashCoin. [Online]. http://dashcoin.net/

[17] BitShares Market Pegged Assets. [Online]. http://docs.bitshares.org/content/index.html

[18] Dogecoin. [Online]. http://dogecoin.com/

[19] Created by Nxt community. (2014, July) Nxt Whitepaper. [Online]. https://www.dropbox.com/s/cbuwrorf672c0yv/NxtWhitepaper_v122_rev4.pdf

[20] Monero. [Online]. https://downloads.getmonero.org/whitepaper_review.pdf

[21] Bytecoin. [Online]. http://bytecoin.org/

[22] Namecoin. [Online]. https://namecoin.info/

[23] Danny Deng. (2014, Nov.) New YBCoin White Paper. [Online]. http://www.ybcoin.com/wp-content/files/New_YBCoin_Whitepaper_V2.72_en.pdf

[24] Counterparty. [Online]. http://counterparty.io/docs/about_counterparty/

[25] Paycoin: A Cryptocurrency Fit for World Adoption. [Online]. https://c91475e716c8925e05c6-d2659d433205cf4410415f8dd63807af.ssl.cf5.rackcdn.com/paycoinwhitepaper.pdf

[26] Edgar Soares, "Designing Profit," White paper. [Online]. https://archcoin.co/pdf/whale_whitepaper.pdf

[27] Monacoin. [Online]. http://monacoin.org/en/

[28] Faircoin. [Online]. http://fair-coin.org/

[29] Captain James Lee. (2014, August) Teleport: anonymity through off-blockchain transaction information transfer. [Online]. http://www.flipgorilla.com/p/23023990364728535/show

[30] Pavel Vasin. BlackCoin's Proof-of-Stake Protocol v2. [Online]. http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[31] Raymaekers, "Cryptocurrency Bitcoin: distribution, challenges and opportunities," *Journal of Payments Strategy & Systems*, vol. 9, no. 1, pp. 30-40, Spring 2015.

[32] Gabi Stern. (2015, April) Bit post. [Online]. http://bit-post.com/players/bitcoin-regulation-around-the-world-the-current-state-5627

[33] Virtual Currency Today, "Regulation of Virtual Currencies: A Global Overview," Virtual Currency Today, 2015.

[34] Larry Greenemeier. (2015, April) Scientific American. [Online]. http://www.scientificamerican.com/article/cryptocurrency-exchanges-emerge-as-regulators-try-to-keep-up/

[35] Scott Fargo. (2015, May) Inside Bitcoin. [Online]. http://insidebitcoins.com/news/california-banking-and-finance-committee-oks-bitcoin-bill/32174

[36] Anthony Cuthbertson. (2015, January) International Business Times. [Online]. http://www.ibtimes.co.uk/cryptocurrency-round-new-york-considers-bitcoin-sustained-stability-mtgox-was-inside-job-1481630

[37] Evander Smart. (2015, April) Cryptocoins news. [Online]. https://www.cryptocoinsnews.com/australian-central-bank-rules-bitcoin-regulation-stance/

[38] (2015, January) Bitweb Magazine. [Online]. http://bitwebmagazine.com/australia-to-introduce-bitcoin-tax/

[39] Leon Pick. (2015, March) Finance Magnates. [Online]. http://www.financemagnates.com/cryptocurrency/news/russian-finance-

minister-bitcoin-ban-to-take-effect-this-year/

[40] Allen Scott. (2015, March) The Cointelegraph. [Online]. http://cointelegraph.com/news/113766/russian-ministry-of-finance-anti-bitcoin-law-will-finally-be-passed-this-year

[41] Caleb Chen. (2015, January) Cryptocoin News. [Online]. https://www.cryptocoinsnews.com/russia-blocked-several-bitcoin-sites-preperation-russian-bitcoin-ban/

[42] Sophie Song. (2014, March) The Rise And Fall Of Bitcoin In China: Central Bank Shuts Down All Chinese Bitcoin Exchanges. [Online]. http://www.ibtimes.com/rise-fall-bitcoin-china-central-bank-shuts-down-all-chinese-bitcoin-exchanges-1563826

[43] Steven Yang. Bloomberg. [Online]. http://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions

[44] Ellis Hamburger. (2014, February) The Verge. [Online]. http://www.theverge.com/2014/2/9/5395050/russia-bans-bitcoin

[45] Marcin Szczepański, "Bitcoin: Market, economics and regulation ," European Parliamentary Research Service , 2014.

[46] (2015, April) Coin Center. [Online]. https://coincenter.org/survey/

[47] Virtual Currency Today, "Virtual Currency 101 for Retailers," Virtual Currency Today, 2015.

[48] William J Luther and Josiah Olson , "Bitcoin is Memory," *Journal of Prices & Markets*, June 2013.

[49] Vincent Ryan. (2014, April) CFO. [Online]. http://ww2.cfo.com/cash-management/2014/04/corporations-resist-bitcoin-see-lack-of-regulation-as-a-negative-who-will-regulate/

[50] Bitnodes. [Online]. https://getaddr.bitnodes.io/

[51] Charles Lee. litecoin. [Online]. https://litecoin.org/

[52] Jae Kwon, "Tendermint: Consensus without Mining,".

[53] NEM. [Online]. http://www.ournem.com/

[54] Noah Youngs, Arthur Britto David Schwartz. (2014) The Ripple Protocol Consensus Algorithm. [Online]. https://ripple.com/consensus-whitepaper/

[55] Marcin Szczepański, "Bitcoin: Market, economics and regulation ," European Parliamentary Research Service , Briefing 2014.