The ₿itcoin Revolution

An Internet of Money

ĐIGINOMICS

Travis Patron

The Bitcoin Revolution

An Internet of Money

Travis Patron

ÐIGINOMICS

RESOURCES WITHOUT BOUNDARIES

www.diginomics.com

Diginomics is a concept which describes the all-encompassing transition to a cultural, financial, and political genre governed by digital law.

For the purposes of education, this publication is best served by providing links to the hosting page at https:// diginomics.com/the-bitcoin-revolution/ rather than sending copies of the PDF file itself. This is because the file may be updated to provide the most accurate content, although both methods are acceptable.

Dedication

Satoshi Nakamoto

Ask not how to acquire more money, but how to acquire more bitcoin.

Table of Contents

Foreword

Money … that old fashioned, hold-it-in-your-hand medium of exchange called "legal tender," is on its way out. Soon (sooner than most are prepared and fewer still are aware of), it will totally disappear. Even now – 2014 – "one in ten US dollars in circulation today is a physical note -- the kind you can hold in your hand or put in your wallet," reports McKinsey & Company. "The other nine are virtual."

Bitcoin researcher, Travis Patron, has captured the essence of this global trend toward total cashlessness by tracking the development and evolution of the "cryptocurrency" world, especially as it pertains to ***bitcoin*** -- that strange algorithmic creation sweeping the nations in its bid to become the new official digital replacement for "fiat" cash, coins, checks and cards.

When I first coined the word "diginomics" in 1998, it was intended to depict a fully digitized economy and the culture surrounding it in the forthcoming century. Now, that Diginomic World embeds everything we purchase. As *bitcoin* evolves in becoming the king of "megabyte money" (Kurtzman, 1993: *The Death of Money*), the hemorrhaging world economy awaits its salvation in something dramatically new.

"The economy for the Age of Networked Intelligence is a *digital economy*," Don Tapscott wrote in THE DIGITAL ECONOMY (1998). "In this new economy, information in all its forms becomes digital – reduced to bits stored in computers racing at the speed of light across networks. The world, the economy, and all the rules of business are changing."

Indeed, *the change* has happened! We are there. "Money's destiny is to become digital," cites a 2002 report by the United Nations. David Wolman, writing in WIRED (June 2009), noted: "In an era when books, movies, music, and newsprint are transmuting from atoms to bits, money remains irritatingly analog. Let's dump it!"

What Patron has done here is to brilliantly reveal to us how the new era of digitized money is evolving. It's the next important link in understanding the future … *now!* Others have said, "It's coming." Patron says: "It's here!"

- Wallace Wood

www.diginomicsdefined.com

Introduction: Monetary Evolution, Ready or Not

> *All the forces in the world are not so powerful as an idea whose time has come.*
>
> *- Victor Hugo*

An idea with the potential to change the world may only start with one man or woman, but can demonstrate that no individual is powerless to make a profound impact on society in a way that alters the course of human history into a daringly new direction.

An idea which disrupts the most basic fundaments of our sprawling economies arrives when eroding trust of financial institutions call for not more regulatory oversight, but a set of rules provided by the very laws of science – a paradigm shift in the way we approach an emerging problem of centralization. Too many are now dependent on too few. Our societies have been built with a degree of efficiency where if our systems are not capable of reproducing the results of recent history, catastrophe looms. Is *this time truly different*? Have we finally learned the lessons of the past and engineered the infrastructure of our society to withstand dramatic change? Can we continue our current trajectory with no unforeseen circumstances?

These instances of centralization always, inevitably lead to abuse. Onlookers have become desensitized to the mistrust so prevalent in industries' ranging from national politics to currency management, central banking to mortgage-backed securities and the individuals whom these institutions exist to serve are now seeking a way to liberate their financial livelihoods in a way which does not jeopardize personal well0being – that is, they wish for a vehicle which can alleviate them from under the heel of political and economic consolidation of power.

People are anxious for an alternative to our system which has fallen prey to common occurrences of corruption and fraud. Man's greatest weakness has always been himself, and humans succumb to the whim of greed and fear. Who can blame them? When opportunity exists for gain without consequence, what rational man would not take the deal?

Herein lies the problem. The systems we have engineered are inherently vulnerable to corruption because they require a high degree of **trust**. Complex systems, as our global economies have become over the last 100 years, cannot operate at efficiency with this requirement of trust, for there is too much to lose for too many and those many are at the whim of the very few. If humanity is to prosper into a **type 1 civilization** (one which is able to harness the full potential of an entire planet), it must operate from a paradigm which requires no trust and attributes no dominant ownership. It must be one which allows the individual to act upon their own accord, while simultaneously presenting the opportunity to contribute to the *whole*.

A solution may lie in the adherence to an intelligence based on the very laws of science and universal in scope.

Rise Above Primal

When faced with the problem of systemic inefficiencies, one must look at the very root problem to devise a solution. When we come to understand the current economic system, we see that the currency of any financial system is its lifeblood. Our economies are animals, much the way a consumer would have animal spirits based on instincts of emotion, national economies absorb their lifeblood by way of the citizens' which comply with their governing jurisdictions. Their issued currency, and the trust imbued within it, *is* the lifeblood flowing through the veins of the nation state.

When a currency loses its trust, it loses its value. When people do not trust something, it inherently loses its perceived value from that person and indirectly, the value attributed to everyone else. Therefore when people come to mistrust a currency, the financial system which it gives life to, is in risk of collapse. When the citizens of any nation no longer have reason to trust the issuing authority the animal spirit dies.

Trust is the backbone of any traditional economy, and once it is misplaced, the current regime topples under shifting circumstances. Unable to keep pace with disruptive change, sometimes these regimes fall for the greater good and the fall can also precipitate a period of utter economic stagnation.

What then causes a breach of trust? If you ask an unfaithful partner or spouse, they may say it's because they've found something better. Only just recently realizing there was an unmet need. Something more compatible and interesting grabs their attention, and they jump ship.

While this may be a loose comparison to the concept of our current trust in national politics, the premise remains true: something more compatible to our increasingly digitized lives has been conceived and people are severing their dependency of government issued currencies and stepping into something bold and new - **bitcoin**. Fiat currency is just now entering denial mode, fighting to stay above water, clawing in a desperate attempt to hold onto what it already knows it's losing – people's trust.

Many are beginning to believe digital currencies to be the rival to fiat currencies economic pundits have been predicting for years. When the smoke of battle clears something far more complex, yet orderly in nature will be left standing.

The Bitcoin Payment System

Digital currencies which are built upon decades of cumulative research in cryptography and network computing, use mathematical algorithms to prove ownership and rely on a massively distributed database known as the *blockchain*. We call these digital currencies, which are built upon techniques for secure communication, *cryptocurrencies*. Although they share many economic characteristics of assets which have come before them, cryptocurrencies open up an entirely new class of financial asset.

What we are seeing with cryptocurrency is an evolutionary process of our money supply. In this evolution of money we can clearly see three distinct stages:

1. commodity based currency (precious metals as money)
2. debt based currency (national governments printing money)
3. math based currency (computer networks which determine the issuance of money)

Cryptocurrencies are no fad or passing novelty, they are positioned to be the new standard in the 21st century. Bitcoin, and cryptocurrency, cannot be *uninvented*.

Differentiating Factor

As we discussed previously, all currency relies on trust, and in order to establish trust, a consumer must have knowledge that there is no breach in the functioning or management of the money supply. They must rely on a government agency to ensure the proper oversight is applied so that the stock of their money supply is not overblown, and their holdings retain value.

Bitcoin requires no such trust from a third party. Outside the control of any centralized institution and owned by no one party in particular, bitcoin sets the stage for something bold and new. Operating by way of cryptography, bitcoin creates a database of all transactions which have ever occurred within the payment system, storing them as a plain text file freely available to any computer to verify the integrity of the network, all via an entirely open-source software protocol. This network, the bitcoin payment system, has quickly become the largest computing project in history, as thousands of computers have joined their hashing power to confirm transactions sent over this protocol, and in doing so, vie for compensation on behalf of predetermined money issuance algorithms. Essentially, the computers which are able to add the most value to the network in the way of verification and compensated most generously via issuance of new bitcoin. We call this process *mining*. This application of cryptography to money makes bitcoin a secure and distributed channel of verifying payments without requiring the administration of humans.

The bitcoin payment system excludes no one from participation, as the use of requires nothing more than an internet connection. Bitcoin gives users the ability to be their own bank, by providing a private key which is used to verify holdings on the payment network, all of this done without recognizing physical geography and with virtually no fees.

With bitcoin technology, a brave new digital economy is beginning to emerge, one governed by daringly new laws that not only subvert, but fail to recognize man-made law in any sense. This emergence of a digital economy represents the blueprints of a system which operates outside the control of human intervention absolutely.

The ability to store and access financial information on a global network, without it hinging on political judgment or central points of failure is the dawning of a new era in human civilization. When individuals have access to these resources of information, they become empowered by their capacity to conduct decisions without permission from an external authority. When this decision making ability separates itself from the confines of third party management, money will reach escape velocity and our societies will have advanced unimaginably.

Not only does this type of trustless computing have implications for the management and movement of money, blockchain networks will redner conventional industries which rely on centralized institutions to manageme information and resources on behalf of another party irrelvant. Instead, we will come to work for, and invest our energy into massive computing networks which are essentially owned by no one. As Ray Kurzweil puts it in his *Age of Spiritual Machines*, "The purposeful destruction of information is the essence of intelligent work" (Kurzweil, 2000), and this adequately describes the revolution bitcoin technology will spark, uprooting traditional ways of business which characterize consolidation and trustworthiness of assets. Fantastic opportunities lie ahead for those able to appreciate the implications blockchain networks will bring.

We are privileged to have a front row seat in this transition towards a very different age of cultural, economic, and social growth. To live in the greatest paradigm shift in human history, one should yearn to find others who truly appreciate this awakening and participate in the discoveries which will ensue.

It is my hope that the readers of this book come to a higher understanding of the potential benefits and challenges behind bitcoin as we work through the growing pains, as all phases of adoption must. When cryptocurrencies reach their fullest potential, we will have entered a new era of prosperity, one where the dimensions of intelligence, imagination, and possibility are boundless.

Chapter 1: Bitcoin Basics

Cryptography represents the future of privacy [and] by implication [it] also represents the future of money and the future of banking and finance. (1995)

– Orlin Grabbe, Economist, Prolific Writer

What is Money?

The need for money comes from the idea that we live in a world with finite resources. Human desire is not limited, yet resources vary by scarcity and availability. Therefore, it is necessary to have a medium to exchange those resources which are finite. A unit of exchange is necessary to allocate the ability to own these resources among a population with theoretically limitless desire. Money itself is neither good nor evil, rather a necessary tool in a properly functioning economy.

Would we need money in a world where there is perfect abundance? The answer is quite simply no, because there would be no need to earn in order to afford. All resources would be immediately within the reach of the individual.

Currency is a legal term which describes the attribution of purchasing power on behalf of a state authority (whether it be through coercion or persuasion). Currency is something which is attributed general acceptance for food, shelter, and other basic necessities because of the trust its userbase has in the state authority (persuasion). These same users might also use a currency because the state would impose punishable actions if they were to conduct transactions outside the approval of the authority (coercion). Traditionally, both these methods of governance characterize our political institutions today. Currency could then be described as a legally-imposed construct. Money, on the other hand, is a collective agreement among it userbase. Often these terms overlap.

When there are enough people who settle on what holds their trust, that which they agree upon becomes secondary. The userbase needs no state authority to tell them what they should use as their money supply. History has provided us of countless examples of this being true. Whether it

be cigarettes, animals, precious metals, artifacts, and now computer code, money remains a collective agreement established by its user base.

Aristotle, the Greek philosopher, defined the characteristics of sound money comprising of four core aspects:

- *Durability*

Money must remain in the same state it was originally created in. It cannot change or be destroyed by the forces which use it. In relation to bitcoin, they are almost perfectly durable. Bitcoin cannot be changed as each coin is based off computer source code. However, bitcoin can be lost quite easily in the event of a forgotten password or mishandled storage.

- *Portability*

Since bitcoin is a digital currency, it has no physical cumbrance and, therefore, is portable to anyone with a wallet address capable of receiving payment. There is no burden in sending bitcoin across borders because in cyberspace, no such borders exist. You can cross a border with $1 billion in bitcoin using a brainwallet and no number of patrol agents or cash-sniffing dogs would be the wiser.

- *Divisibility*

Bitcoin is made to be infinitely divisible by design. Currently, we use 8 decimal places to represent smaller fractions of an entire bitcoin. The unit of account down to the last of the 8 decimal places is known as a *satoshi,* in reference to the mysterious founder. If there is ever a need to extend the amount of decimal places, the developers and community can come to an agreement and make necessary changes. Bitcoin is perfectly divisible.

- *Intrinsic Value*

The argument most commonly heard against bitcoin is that it lacks intrinsic value. That is, the currency has no desirable features and no value in and of itself. Outside of the acceptance trust, currency usually holds little or no intrinsic value; there is no value inert to the unit when it is presented simply for what it is. Anything other than trust would be considered a bonus to intrinsic value. The industrial uses of precious metals, however limited, are intrinsically valuable.

Investors are correct in asserting that the bitcoin unit of currency itself has no intrinsic value outside of trust. To make the claim of intrinsic value with bitcoin, we must make the distinction between bitcoin the payment network and bitcoin the unit of account capable of being spent. Both are known as bitcoin, but to not recognize the difference would be a hazardous miscalculation.

The reason bitcoin has "perceived" intrinsic value is because of the technological capabilities of the network which acts to send payments. The intrinsic value comes from the idea that, with bitcoin, we can now do things with money we never previously were able to do.

As more people take time to understand the technological advantage of bitcoin, more people will come to accept it as payment. In doing so, the value will grow as trust is engrained. Considering bitcoin is a payment system which is made open to a scarce number of coins, the bitcoin unit of account commands a market price. Because bitcoin is both useful and scarce, it is valuable.

The Fiat Emperor Has No Clothes

Fiat currency gains its intrinsic value from government's laws and regulation. The compliance on these laws rests with the credibility and authority of the governance which issues them. The term "fiat" is a revealing description as well, this time of paper currency. In Latin it literally means *"let it be."* -- government-created currency which sounds as though the only thing holding it in place is confidence in the authority issuing. Such a currency, which sounds as though it has been buckling under the weight of illusion, is waiting for something more real to come along and relieve it of its temporary purpose. No fiat currency has ever stood the test of time, nor has it been designed to.

Bitcoin gains its credibility because it is a cryptographic form of money based on mathematical approaches to the laws of science. Or as the unofficial maxim of the bitcoin community goes, *'in cryptography we trust'*.

The term "bit", as in bitcoin, is a basic unit of information relating to digital communications. This unit of information (a bitcoin) resides on the blockchain and has its ownership assigned to a wallet address. What bitcoin as a system truly represents is a global database of financial information. To use the name "bitcoin" is nothing more than clever branding tactics and a proverbial play on words describing numismatic information.

In this sense, the concept of decentralization of power also gives bitcoin value. The idea of money being owned and supported by only the people who use it instead of a central authority makes the currency viable and at the will of those it exists to serve. In a world where circumstances and events are becoming increasingly interdependent, consolidation of power is unfavorable to dispersal of such power. If the currency fails to serve these needs, the people have the power of choice to use a different money system, and bitcoin will debase. It is no longer necessary to have the state manage, manipulate, and control money.

- *Originative*

I would like to build off Aristotle's concept of a valid currency by considering a fifth characteristic: originative. Bitcoin comprises nothing more than computer software, and therefore it is easy to see how a copycat currency could come along at any time and tweak minor aspects of technical specification in order to make it superior. This we have seen to be a common practice among alternative cryptocurrencies, but very few currently have the infrastructure and competitive advantage necessary to co-exist with bitcoin. Is this infrastructure built around bitcoin enough to give it a lengthy first mover advantage?

For a currency to establish itself, it must have the necessary time and exposure to its user base to establish collective agreement of its acceptance. In order to do so, the currency must be originative, and refrain from being carbon copied in a way that would introduce a similar money supply with slightly altered characteristics.

Much like we see programming languages being created very frequently, yet the ones who catch on are far and few between, only a select few cryptocurrencies which appeal to a large demographic of users and provide solutions to difficult technical and economic problems will garner the largest market capitalizations. The ability for programming languages to be created is accessible to any developer with the ability to do so, and much the same will be said for cryptocurrencies. However, there will be industry standards in cryptocurrency much the same way Python, C++ and other languages are standards for software engineering, standards for cryptocurrency will be bestowed upon a select few, likely the ones with the largest input from community development behind them.

Unless a new money supply is created that has a unique, sustainable use case for the cryptocurrency in circulation, it represents nothing more than a speculative investment. With current competing cryptocurrencies, only those which serve a definite purpose and those with a dedicated community behind them will have long-term outlook. It would make for an interesting argument for which tweaks in bitcoin's technology make it viable, and which are nothing more than marketing fluff. There is only need for projects being built which introduce a new use-case scenario for a supply of cryptocurrency being circulated. Whichever emerging cryptocurrencies this describes is up to the investor to determine.

Fiat currency does not need to concern itself with being originative because its value is tied to the political, economic, and social decisions the issuing authority makes. A fiat currency's dominance ends where its borders no longer reach. Government issued currency can survive and prosper along with almost identical other supplies of currency because it represents an already established and centralized economy. Digital currencies on the other hand however, have no boundaries which to assess its value against. Fiat currency is tied to a centralized force, bitcoin is without geographical or physical limitation. Therefore any digital currency designed for monetary uses will survive only if it can establish itself as a solution to a unique problem. Cryptocurrencies which do not fill a unique use case will be nothing more than collectables.

The cryptocurrency which establishes itself as the benchmark of the digital domain will be the one with the highest degree of trust and the most innovative technological features. However, as we have seen in the past, the most brilliant technology alone cannot guarantee market success.

There exist large implications for the right mix of marketing, community, and experimentation for a new entrant to reach its potential.

The infrastructure and first mover position give bitcoin a temporary but sizable advantage. In the way currency relies on trust, this makes bitcoin king. It can be seen in price movements that when bitcoin makes a move, the other cryptocurrencies make a similar, exaggerated move. When bitcoin sneezes, the others catch a cold.

What is Bitcoin?

In order to understand bitcoin, we must first determine the type of financial instrument it represents. Bitcoin is a peer-to-peer digital payment system. As Satoshi Nakamoto, the creator of bitcoin puts it – "*an electronic cash system".* Not simply a currency or asset, it is an electronic way of exchanging value across a new economy, one which operates entirely independent of human intervention and 20th century financial infrastructure. For the sake of explanation, we must establish the fact that the way bitcoin works and the way the payment system operate, are one in the same. We are dealing with one payment system known as the bitcoin blockchain, and one unit of account for said system known as a bitcoin.

Bitcoin is a digital, cryptographic form of money. By this, we mean the cryptocurrency exists as a computer software solution supported by techniques of cryptography to ensure the integrity of the peer-to-peer network structure. Cryptography describes a form of data transmission which serves the needs of information security and confidentiality. Many applications of online communication, banking, and ATMs already use an array of cryptographic techniques to ensure user information is not tampered with or intercepted by a third party.

Credit cards, which were conceived in a time when internet technology was nonexistent, do not have the ability to perform the functions bitcoin is designed to carry out. The use of credit cards originated in the United States during the year 1958, when firms such as the Bank of America began issuing them to customers who made purchases based on credit at partnered institutions. In 1983, long after the advent of credit cards, the TCP/IP protocol was standardized into

ARPANET and is still the primary technology we use today for the internet. (Computer Hope, 2014)

Bitcoin was designed for the internet, although it has far reaching implications for the physical realm, it will come to dominate our online lives because it was specifically made to capitalize on payment functionality only internet technology makes possible. We will discuss these functionalities later in this book. Combined with the reality that our lives are becoming progressively intertwined with the internet and computers, bitcoin will increasingly be seen as the standard way to make transactions worldwide.

As a digital form of money, bitcoin is not physical in any sense and exists solely as recorded information on the shared bitcoin blockchain. Because this form of money is entirely digital, it has the innovative attribute of being native to the online realm. When we talk about existing as recorded information on a shared ledger, we mean residing on a network supported by an interconnected linkage of computing power. These computers which agree to the information recorded in the blockchain ledger, are known as miners, a concept of supporting the network as a *node*, something we will discuss later.

This network of interconnected computing power is created when computers running software (the bitcoin client) link up to record and handle transactions. Every time a transaction is made, the amount is recorded in the network payment system, adding to the public ledger (the blockchain) and making available for anyone to view. For this reason, it is said that the bitcoin payment system is a fully transparent network - anyone can view any payment and the time it was made since the inception of bitcoin. When a payment occurs, ownership of the amount that was transacted is now passed onto a new party.

Because the blockchain ledger is completely transparent, as in completely visible and accessible, it creates a situation where the user can remain anonymous or have their identity tied to their bitcoin holdings depending on how they handle the transaction. In order to control a set amount of bitcoin, a user must first create a wallet (a bitcoin bank account) which will serve as the point from which funds are sent and received by other wallets in the bitcoin ecosystem. A typical wallet is identified by a string of characters called a public address which is generated by the network. If

you do not tie your real-world identity to this string of numbers and letters, it is possible to remain anonymous and have full privacy with your payments.

Mining Bitcoin

The distributed ledger bitcoin operates on, which is freely accessible and growing in size as more transactions are made, is known as the bitcoin blockchain and it's what makes the idea of cryptocurrency so astoundingly powerful. When a transaction is made, computers running the software and supporting the network (known as miners) timestamp the transactions, preventing a double spend situation of the money. A double spend would describe identical bitcoin being in multiple places at once, something which would compromise the entire integrity of the bitcoin payment system. Because the blockchain serves as an authoritative body to display and confirm transactions, double spending is not possible as long as there is a sufficient distribution of the network power. Therefore, payments are verified by the blockchain, which is maintained by a collection of nodes running the bitcoin client worldwide, and the bitcoin in circulation are then not capable of being double spent.

The computers running this type of software, the bitcoin client, are known as miners because, other than verifying transactions on the network with their computing power, they are also compensated with bitcoin for supporting the network. Miners running the bitcoin client solve what are known as blocks (a collection of transactions waiting to be verified and confirmed). When a block is solved, a predetermined amount of bitcoin is then rewarded to the miner and the total money supply of bitcoin grows. This is the only way to introduce new bitcoin into the money supply (the total amount of money units available in the economy at a specific time). The miners act as the participants who increase the supply of money as they figuratively "mint" new blocks and confirm transactions which are recorded on the blockchain. Therefore, if you want to increase the total number of bitcoin in circulation, the only method of doing so is by mining them.

The total amount of bitcoin that will ever be in circulation is hard capped by a constant value in the source code. There will never be more than 21 million bitcoin available, a striking contrast to our current fiat system which could hypothetically create an infinite number of dollars, euros, etc. Currently there are about 13 million in circulation and the money supply continues to grow as miners verify more blocks of transactions. One of the reasons bitcoin is considered a deflationary currency rather than an inflationary currency, is because there is a finite limit on the amount that will ever exist.

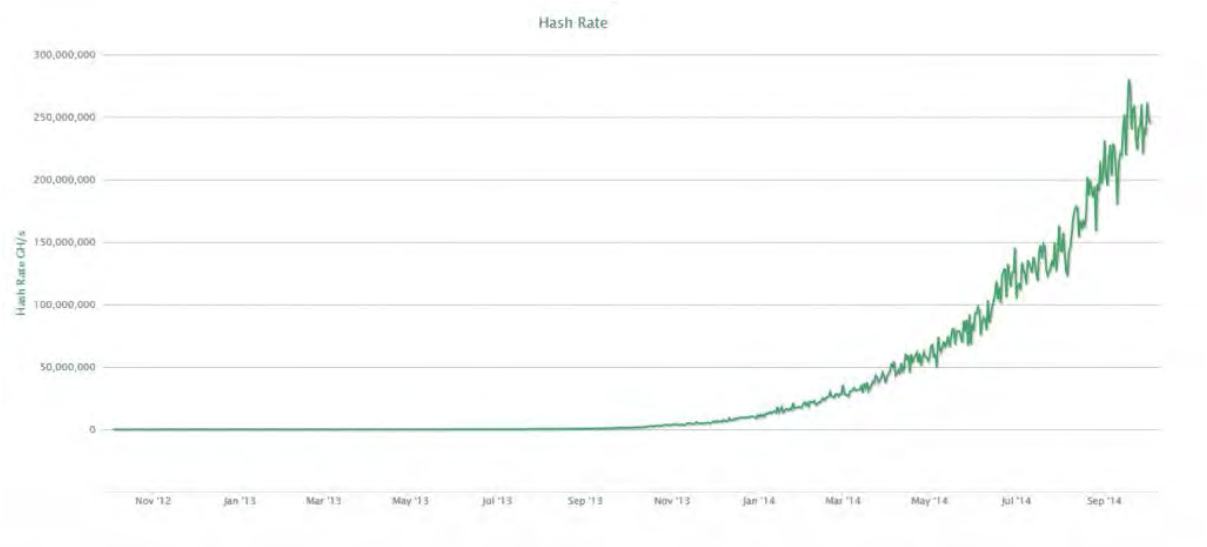
Because these miners are computers around the world running the bitcoin client, the money supply is said to be decentralized, or having no single point of issuance. In today's fiat system, money is created at will through a central bank and through private commercial banks, giving the people who have power over the central banking institutions monopoly of the nation's money supply power. This is something that is met with great criticism in the cryptocurrency industry among many others, and one of the many pitfalls of 20th century economies which bitcoin aims to solve.

The blocks which are being mined contain a predetermined amount of bitcoin to be released into the total money supply once they are solved by miners. As the bitcoin economy grows, mining these blocks also requires more computing power and a smaller amount of bitcoin are rewarded. Note this does not necessarily mean less total value of the reward, only a smaller number of units. Mining does not necessarily become progressively less profitable, only gradually more difficult, given that bitcoin continues to see adoption at pace with increased mining difficulty. The increase in difficulty of mining new blocks is designed to regulate the average time it takes to solve a new block of transactions to *10 minutes*. The greater number of users on the network, the greater the demands for processing power will become. In a situation where mining is too difficult to incentivize miners to compete for block rewards, the difficulty required is programmed to automatically adjust accordingly.

In the current landscape of cryptocurrency mining, competition has become so fierce that only specialized, high-performance computers have a chance to influence the network and earn block rewards. We call these specialized computers application-specific integrated circuit computers (ASIC). The type of computations these computers perform are functionally different from

mainstream computers, as they run only particular applications programmed into the circuitry of the chip. The ASIC computers involved in bitcoin mining, are custom built to run only the SHA-256 hash function required in finding new blocks.

To get an idea of the combined computing power of the bitcoin network, we use a unit of measurement called the hash rate. The hash rate is the measurement unit of blockchain processing power. These networks require this kind of processing power to conduct intensive mathematical security operations. When a network reaches a hash rate of 10 Th/s for example, it would be making 10 trillion calculations per second. The following graph illustrates the increasing hash rate of the bitcoin network.



The concept of a network with many different miners decentralized across the world gives it the potent characteristic of having no central point of failure. In a peer-to-peer network, tasks are shared amongst multiple interconnected nodes (a communication endpoint, in this case the miners) who each devote their resources (in this case computing processing power) and make it available to an entire network (in this case the blockchain). Similar types of peer-to-peer technologies are often seen in file-sharing software (Napster, Limewire, The Pirate Bay), and also make it extremely resilient to attacks because there is no single point which would destroy the network. However, unlike previous peer-to-peer technologies, bitcoin is not a company or single organization, it is a technology for the decentralization of resources waiting to be used by anyone. The code bitcoin is built upon is open source, meaning anyone can look-up the algorithms which give it functionality and build a better implementation of the technology.

Coinbase Transaction

In the mining process of bitcoin, a special input called the coinbase occurs when a newly minted block is attributed to the miner. Because newly mined bitcoin have no inputs, and every transaction displays its inputs as its parent's transaction output, a coinbase transaction describes the inputs of a newly minted block with no prior history.

Any arbitrary data can then be used as the coinbase input of a newly minted block of bitcoin. For example, the very first block of bitcoin mined, the genesis block, has its coinbase input as:

```
The Times 03/Jan/2009 Chancellor on brink of second bailout for bank
```

Transacting With Bitcoin

There are many ways to obtain bitcoin. The first is to mine them with a computer and support the growing bitcoin network. In the early days this was possible to do with an average household computer because at the time the difficultly to mine new blocks and be compensated for contributing computing power was much lower. Now, mining bitcoin has become the specialized domain of a few dedicated operations with sophisticated hardware. Demands of mining difficulty have required hardware designed precisely for mining operations. If your intention is to make large profits off mining today, you'd be best served by joining an already established operation using custom designed hardware which delivers serious performance. We won't get into the technicalities of mining bitcoin in this book because it is an entirely new industry which deserves a manuscript of its own.

The second way of obtaining bitcoin is by being paid in it. This method is a fantastic way to support and help grow the youthful bitcoin economy and help it gain acceptance worldwide. Sell your goods and services for bitcoin and ask your employer if they would consider paying your salary in bitcoin (and be prepared for a bewildered reaction). The merchants and individuals who

began accepting bitcoin as payment early on, and held onto it, are reaping incredible profits as they have witnessed the value of their bitcoin revenues increase exponentially.

The third and most common way of obtaining bitcoin is by buying it outright. You can do this in a number of different ways, the most common being in person or through an online exchange service and you can also find an increasing number of bitcoin ATMs available (BTMs).

In person trades operate on a reputation basis, so if someone has a glowing reputation on a site you operate through, then they are most likely trustworthy. It is in the seller's interest to give you a fair deal, or else you can give them negative feedback and their reputation will take a hit, hampering their ability to do future business. If anonymity is your goal, buying bitcoin in person is the best way to achieve it, although you will have to take the necessary precautions to hide your identity.

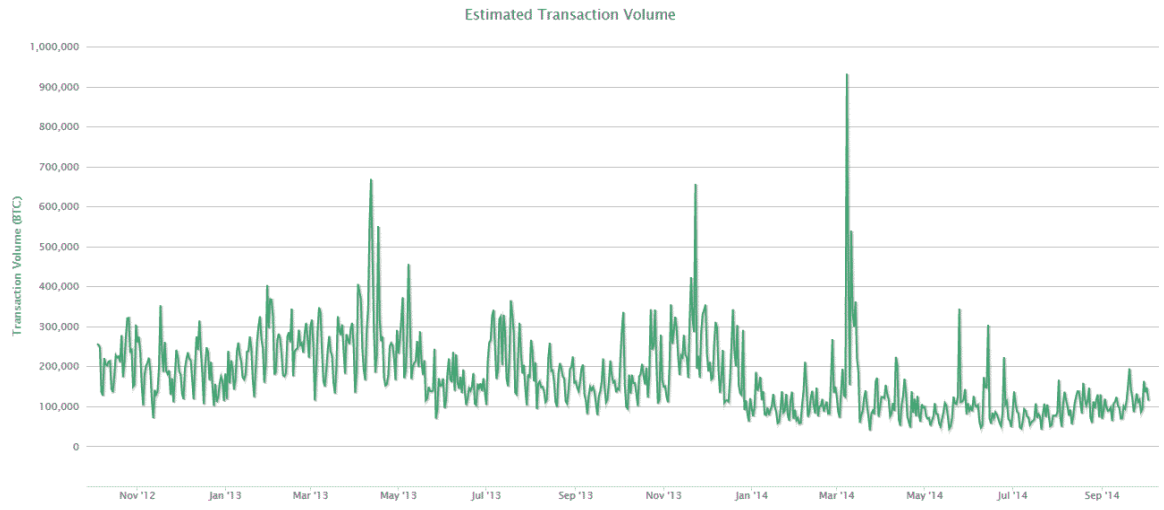
If you prefer to operate through an exchange, you are essentially trading your government issued currency for bitcoin through an online brokerage. Exchanges work well for larger volumes of transactions but require verification and submitting government identification to process trades and transfers from a bank account. These verifications are required by national law and can sometimes take days or weeks to complete. Once your account is setup and verified, you can transfer funds from your bank account to an exchange using a wire transfer or payment processor.

Note that because the exchange verified your identity, the bitcoin wallet the exchange provides you with will have your identity tied to it and any wallet you transfer your funds to from that one has an element of traceability and therefore is not anonymous.

The final way to earn bitcoin is to accept them as donations. This has become an increasingly popular form of keeping community desired operations afloat, even when traditional payment processors and banks have built a barrier around them. In order to begin accepting donations, you must make your wallet address (the character string of numbers and letters) available to the party which will be doing the donating. All the payer needs to do from here is transfer their funds to the address you present them.

So how does one actually go about spending bitcoin and what can it buy? Since bitcoin is a new form of money, you can hypothetically buy anything as long as the other party is willing to accept bitcoin as payment. As more and more parties begin accepting bitcoin as payment, it will rise in value because the main determinant of a currency's value is acceptance.

One of the best ways to support the bitcoin economy is to begin accepting it and convincing others to consider it for their own business. The following graph displays the total estimated transaction volume of bitcoin.



While the bitcoin economy is growing in the number of individuals and merchants accepting it, the trust and value of this new digital ecosystem will take on a life of its own, independent of 20th century currency markets. To begin accepting bitcoin, all that is needed is a wallet capable of receiving payments. In order to spend bitcoin, you can just as easily transfer your money to the wallet of a merchant when they present their address.

Storing Bitcoin

As one of the most important topics on cryptocurrency, learning to store your money securely is absolutely essential if you are to use digital payments systems with the peace of mind that your money will still be available when you return. If you make a mistake in the area of storing your bitcoin or another cryptocurrency, there is a chance they will come under the control of someone else, so take heed when we say this is the most important aspect of being a holder. Storing bitcoin

securely is a topic cryptocurrency holders must appreciate. Without the necessary understanding, your money is susceptible to theft and hacking attempts.

Wallets

When someone says that you hold bitcoin in a wallet, it is not entirely true. Think of a wallet as a key which unlocks a certain amount of bitcoin in circulation. There are never any bitcoin being transferred from wallet to wallet, but rather the ownership of the bitcoin is what's being transferred. In fact, there is no such thing as bitcoin as a "currency" in the first place. There is no computer file or data to represent the unit of account itself. The only file associated is a wallet data file which acts as your representation on the blockchain ledger. Instead, when you buy bitcoin, you are essentially increasing the percentage of the blockchain which you claim ownership to. Your wallet is your key to that amount of ownership. In this sense, Satoshi was correct in labeling it as an "*electronic cash system*" and not a digital currency, because it is a payment system which was built and not simply a unit of currency. For the sake of simplicity, everyone still views bitcoin as a type of currency, when in truth the ownership of the blockchain ledger entry is what is being transferred.

A wallet address functions much the same way an email address might function. Payments are capable of being sent from and received at a wallet address. These are the primary purposes of a cryptocurrency wallet. Each wallet is randomly assigned a string of characters which designate its address. For example, if you create a new wallet address you may have a string of 34 characters such as:

16C4QXWNFZ9K94RMAD1NUMJWN15AIJBMGR

This would be the address shown in the blockchain ledger when you send and receive payments. As we have discussed, keeping your real-world identity separate from this string of characters is crucial if you wish to have your cryptocurrency holdings remain private.

Public Key Cryptography

There are two parts to a bitcoin address. The first is the public key, which is the 34 character string wallet address we just displayed, and the second is the private key. We must always keep

our private key unknown to other parties, else the contents in our wallet are not truly controlled by the person using the wallet. Whoever holds the private key to a wallet, controls the ownership associated with the wallet on the blockchain. These two keys in combination are known as public key cryptography and they are the reason why using and transacting with bitcoin is secure.

In order to transfer bitcoin from one address to another, a request is broadcast to the network that a certain amount of bitcoin now belongs to the receiver's address. This transfer is authorized by the sender's private key and the miner's verify the transaction through a hashing algorithm. Once the transfer is fully verified, they are added to the next block in the chain of transactions.

Bitcoin addresses are created by first picking a random number and creating an ECDSA (Elliptic Curve Digital Signature Algorithm) public/private key pair with them. This operation alone generates the private key – but bitcoin addresses are not simply public keys, but rather modified versions of them. The generated public key is then put through several SHA-256 and RIPEMD-160 operations, until eventually being converted into a format called Base-58. Base 58 is an encoding that removes the possibility of similar looking characters, such as lowercase L and uppercase I, as well as 0 and O. Finally an identifying number is added to the beginning of the address – for most bitcoin addresses, this is 1, indicating it is a public bitcoin network address. (Learn Cryptography)

Operating Systems

The first recommendation in regards to using bitcoin securely, is only managing your funds on a computer that has a clean operating system. By this we mean free of malware, viruses, and other hidden key logging programs you may have no idea lurk in shadows on your computer. These programs will crawl your computer hard drive for wallet files and passwords, sending sensitive information to the attacker. Some programs even have the ability to take control of your webcam, microphone, and files without you being aware of it. If you suspect your computer is infected, use another one or reformat your computer in order to erase your hard drive and install a fresh copy of your operating system.

Not all operating systems are created equal. The most inviting operating system for hacking attempts is Windows. Although it is user friendly and compatible with most programs, it is

relatively vulnerable by design. In contrast, the safest operating system you could use is a Linux system which runs 98% of the world's supercomputers and comes in a variety of distributions. Linux can come with a steep learning curve and is not your operating system for typical mainstream needs, but when the essentials of security and performance arise, none best it. Take as many security precautions as you can, and remember that there is no such thing as a computer system which is impossible to hack. Because Linux provides the most resilient and reliable operating system, it is your safest bet, but not guaranteed to prevent hacking attempts to steal your holdings.

Dangerous hacking programs can get onto your system by opening email attachments, transferring files from media storage devices, and browsing unscrupulous corners of the web. The most common way hackers infect your computer is through email attachments. Therefore it is imperative that you never open an email attachment or download a file when you are unsure of the implications it will bring. Always obtain as much information about the properties of the file before you transfer it to the same device as your bitcoin wallet.

Passwords

When you are confident in the security of the computer you are using, the next biggest threat is that of handling your wallet information with complete confidentiality. When settling upon a password to access your bitcoin wallet, it is imperative that you tattoo the phrase into your mind in a way that you will surely never forget.

A brainwallet refers to the concept of storing bitcoin in one's own mind by memorization of a passphrase. As long as the passphrase is not recorded anywhere, the bitcoin can be thought of as existing nowhere except in the mind of the holder. If a brainwallet is forgotten or the person dies or is permanently incapacitated, the bitcoin are lost forever. (Bitcoin Wiki, 2012) The importance of remembering your password cannot be stressed enough. If you forget your password and do not have your private key, your money will be impossible to ever be reclaimed. Writing down your password somewhere private is a helpful deterrent in the event you forget your password, but it makes it accessible to someone who may come across it.

It is very important when creating a brainwallet to use a passphrase that would be not be susceptible to a dictionary attack or brute force attack. If this is not done, theft is an eventual certainty if a hacker uses a high level of computing power. In the event of a brute force attack, an attacker will unleash a machine to continuously attempt passwords until they are locked out. Another method, a dictionary attack, will figuratively throw the dictionary at your login system, using word combinations found in the dictionary.

"The simple fact of the matter is that hacking a brainwallet password is a mathematical exercise that requires no internet access, no communication, and leaves no trace, so hackers can collectively try multiple trillions of passwords every second in the privacy of their own homes with the very same equipment they use for mining bitcoin." (Bitcoin Wiki, 2012)

Backing Up Your Wallet

You may also want to consider making a copy of your wallet file and storing it with a cloud computing service (Google Drive, Dropbox, Microsoft OneDrive). In the case where you lose access to your wallet, you can restore it by opening your saved wallet file and using your password. Access to your wallet file alone will not give the user the ability to move your bitcoin unless you have not encrypted it with a password.

As well as storing an electronic copy of your wallet file, you can also print out what is known as a paper wallet. Bitcoin storage does not entirely require the use of computers, and using a paper wallet is one of the safest methods of storing your bitcoin holdings. This method of storage works because the private key to your bitcoin wallet is printed on the paper, making it easy to enter the information when you want to access your wallet file. If you use a paper wallet, realize that it represents the key to accessing your bitcoin and should be kept in a safe location.

A final method to storing your bitcoin is keeping your wallet file on a hard drive belonging to a computer which has never connected to the internet. To achieve this, many large bitcoin holders have purchased an old computer, wiped the hard drive clean, and transferred their wallet onto this system. This gives you the most security because you know the operating system is clean. Without an internet connection, an outside attacker cannot make changes to your wallet file.

You can also put your wallet file on an external media device such as a USB stick. Many large holders of bitcoin put their wallet file on a USB and then lock that device in the safe at their bank. That's about the highest security for your bitcoin you could come across. This is known as cold storage and is the most effective way of storing bitcoin safely.

Additional Security Measures

A further step in securing your bitcoin if you must use online services, and one that is highly recommended, is using 2-factor authentication to gain access to your wallet. Online exchanges offer 2-factor authentication which involves an outside source to verify the request before granting access, even if they know the password. Typically this is done by sending a text message to a smartphone or by inputting a code sent to the email associated with the wallet. Always enable 2-factor authentication on your bitcoin wallet and always associate a secure email address with an exchange account.

Generally, the safest way to store your bitcoin is to do so offline or with a paper wallet. One sure way of putting your bitcoin holdings in jeopardy is by keeping them on an exchange. In a world filled with tech-savvy criminals, even businesses which promise to practice security procedures and guarantee the safety of your money are susceptible to hacks. These exchanges are targets for some of the most skilled hackers in the world and leaving your money on the exchange means when that service goes down, your bitcoin sinks with it. Already many times exchanges have been on the receiving end of a calculated hacking attempt or an unanticipated technical glitch, causing users who kept their holding on that exchange's server to lose everything.

Don't let this happen to you.

Move your money off the exchange if you do not plan on actively trading it. Furthermore, be wary of phishing attempts (hacking attempts which attempt to imitate trusted services and ask you to submit sensitive information) on your wallet information and passwords. Always check the URL an email or webpage is being broadcast from and use common sense when dealing with customer inquiries. You will never be asked for your password from any legitimate business because it would be easier to simply reset the password.

Remember, the magnificence of bitcoin is that it is a financial obligation between you and your money, no third party need be involved. Never should you give anyone access to your private key.

Advantages and Disadvantages of Bitcoin

Now that we have covered the basics of how bitcoin works, where we can obtain it, and how to keep it outside the clutches of hackers, we need to discuss the advantages and disadvantages that come with this new type of money. As you will see, the benefits of using a cryptographic ledger for payments far outweighs the costs, and is a drastic improvement upon our current arrangement of financial payment systems using government sponsored currency.

Advantages

1. **Trustless Payments**. Bitcoin does not require a central party to facilitate transactions or confirm account balances. This, as we described earlier, is the peer-to-peer functionality of cryptographic money which makes bitcoin so useful. When payments are made they go directly from one account to another, in a completely secure and direct manner which is confirmed by the network.

   Eliminating the need for third party trust was one of the objectives of bitcoin in the first place, and it accomplished this unlike any financial instrument before. Typically, people trust banks to store their money, they trust central banks to retain the value of their money, and they trust governments to manage debt problems in a responsible manner. Bitcoin divorces the reliance on these institutions by putting trust in cryptographic technology rather than human judgment.

2. **Free and Open Payment System**. The bitcoin payment system is free to use and open for anyone to use it. It does not require paying monthly fees or deny access to people who are not in a position to be serviced by a traditional banking institution. Your account is never in jeopardy of being locked because there is no institution needed to manage your

funds and no way of blocking payments unless the network agrees it to be necessary. Previously, organizations such as WikiLeaks have had payment barriers set up around their accounts which prevented them from receiving necessary funding for their operations. With bitcoin, they were able to bypass these barriers and accept donations needed to keep whistleblower journalism alive. With bitcoin technology, advocacy groups are able to accept and spend their money as they like, without requiring approval from government payment processing services.

3. **Personal Information Privacy**. Under the current system, unless you are using cash, you are identified before you can make a purchase. With bitcoin money, this is no longer necessary, but it comes as a double edged sword. In one sense, bitcoin can be obtained and used in an anonymous manner. It does not require the personal information that traditional financial institutions would, such as government identification and contact information among a host of other data. Because the bitcoin payment system does not require these inputs, it need not put a citizen's personal information at risk. However, just as easily as it can be used for stealth can bitcoin be used transparently, giving the entire world first-hand viewing ability into your financial standings. Being a distributed ledger, the blockchain will be making your wallet viewable but will only be tied to your identification if you forego taking the necessary steps to mask traceability. Wallets are also usually capable of housing multiple bitcoin addresses and make it simple to create more.

   Every person has an inalienable right to privacy, and that includes financial privacy as well as privacy from surveillance. Bitcoin promises to provide that financial privacy while eliminating the potential for identification fraud and theft of personal information.

   Many people will argue that providing the ability to transact anonymously opens the flood gates for money laundering, illicit purchases, and all kinds of criminal activity. This may be true to a certain degree, but bitcoin technology does not aggravate this more than paper cash does today. Indeed, using cash is still the most effective and popular way to

conduct money laundering and other illegal activities. There are risks associated with an anonymous form of transaction that financial enforcement agencies are well aware of. Even more so are they aware that paper cash is still the best medium for laundering money.

4. **Simplicity & Security.** The cryptographic technology behind bitcoin is the most advanced of its kind, making the system impractical to hacking attempts. Rather, the hacking attempts to steal funds have been successful due to poor storage practices and faults with exchanges. Security experts around the world have been attempting to attack the bitcoin network only to admit sound defeat. When used correctly, the bitcoin blockchain is an elegant and airtight solution to sending money cheaply and efficiently.

5. **Internet Functionality.** The innovation the bitcoin payment network brings is one of the primary reasons people are so interested in it. The payment system features include:
    - Worldwide accessibility outside the grasp of financial institutions
    - Zero or low processing fees
    - Open-source, public design (the computer source code bitcoin is built upon can be viewed and improved at any time)
    - Fraud control (the network provides protection against most prevalent frauds like chargebacks or unwanted charges, and is impossible to counterfeit)
    - Donation solutions (bitcoin donations could contribute to a faster international response)
    - Multi-signature accounts (allow a transaction to be accepted only if a group of parties agree to sign)
    - Peer-to-peer resiliency (With no central point of failure such as a data center, attacking the network is a burdensome and difficult undertaking)
    - Public transparent private transactions (all transactions are time-stamped, verified, and attributed the withdrawal and deposit addresses)

Disadvantages

1. **Technical Understanding.** In order to properly store and use bitcoin, it requires a certain degree of technical understanding. The more you understand about vulnerabilities to storing your money, the safer you will be. As we discussed earlier, storing your bitcoin is one of the biggest challenges and being protected from hackers takes some computer competency.

2. **Limited Acceptance.** Bitcoin is only now gaining traction with merchants and the number of businesses accepting it is growing daily. More often than not, these are businesses that do transactions online while brick and mortar retailers are still just getting onboard with this new type of payment. Because you may find it difficult to pay your rent or buy food at the grocery store with bitcoin (for now), this limited acceptance can be a disadvantage. There are however, individuals who live entirely off bitcoin. This can prove to be very challenging, yet operating entirely in the bitcoin economy has the added bonuses of not requiring a banking institution.

3. **Uncertain Future.** No one can say with certainty what will come of bitcoin. As it remains today, bitcoin is very speculative as it is still an experimental type of technology. There are potential vulnerabilities which may bring about the downfall of bitcoin. However, the upside is so one-sided that the average consumer would be wise to research and understand this new type of technology, given that money factors into our lives essentially every day. In the long-run bitcoin technology will transform the distribution and access to information in a manner similar to internet and smartphone technology. We are truly on the cusp of a powerful disruption in business, economics, and daily life.

Potential Vulnerabilities

Although bitcoin represents a profound technological innovation, it is not without its flaws and vulnerabilities to failure. There are some limitations that come with the bitcoin network and it is still in early development. The following are potential hazards that may cause the adoption cycle of bitcoin to be irritated:

1. **Government imposes regulations on cryptocurrencies through exchange businesses**

If governments intend to repress bitcoin, they have a few available options for doing so. One of the few options they have is to put barriers around the money transmitters and exchange operations. State regulations on the movement, storage, and privacy of bitcoin will make it less useful in the short term for the masses of people. This would effectively queue the adoption of bitcoin and may cause increases in volatility and twisted market perception.

Regulation through exchanges is the most likely way government would control bitcoin. Many hearings have already been presented on the subject of cryptocurrencies and the nations which stand to gain the most from this technology recognize it as an opportunity. If a jurisdiction places severe limits on the use of cryptocurrencies, there will surely be neighboring countries eager to pick up the slack. Given the chance to understand the potential benefits and challenges of using a new technology such as bitcoin, state regulators will draw closer to adopting it and exploring its usability. Hopefully in doing so, they will not cripple their own opportunity by imposing crude regulations on exchange businesses.

2. **Mining power sees a consolidation of computing power, leading to a 51% attack**

The method in which the mining process is coordinated and set into algorithms is what makes the blockchain work. However, with increased difficulty and block sizes continually halving, operations will likely become the exclusive domain of dedicated mining operations, making the possibility of a 51% attack a distinct possibility. Indeed we have already had panicked situations where one group of miners has come near 51% of the network power, allowing the ability to take control of the system and effectively double spend their holdings.

A mining network which controls 51% or more of the hashing power would have an incentive to remain honest. That is, they would not want to compromise (and therefore devalue) the money system which they have made heavy investments in and come to dominate, thereby ruining maximum profit opportunity.

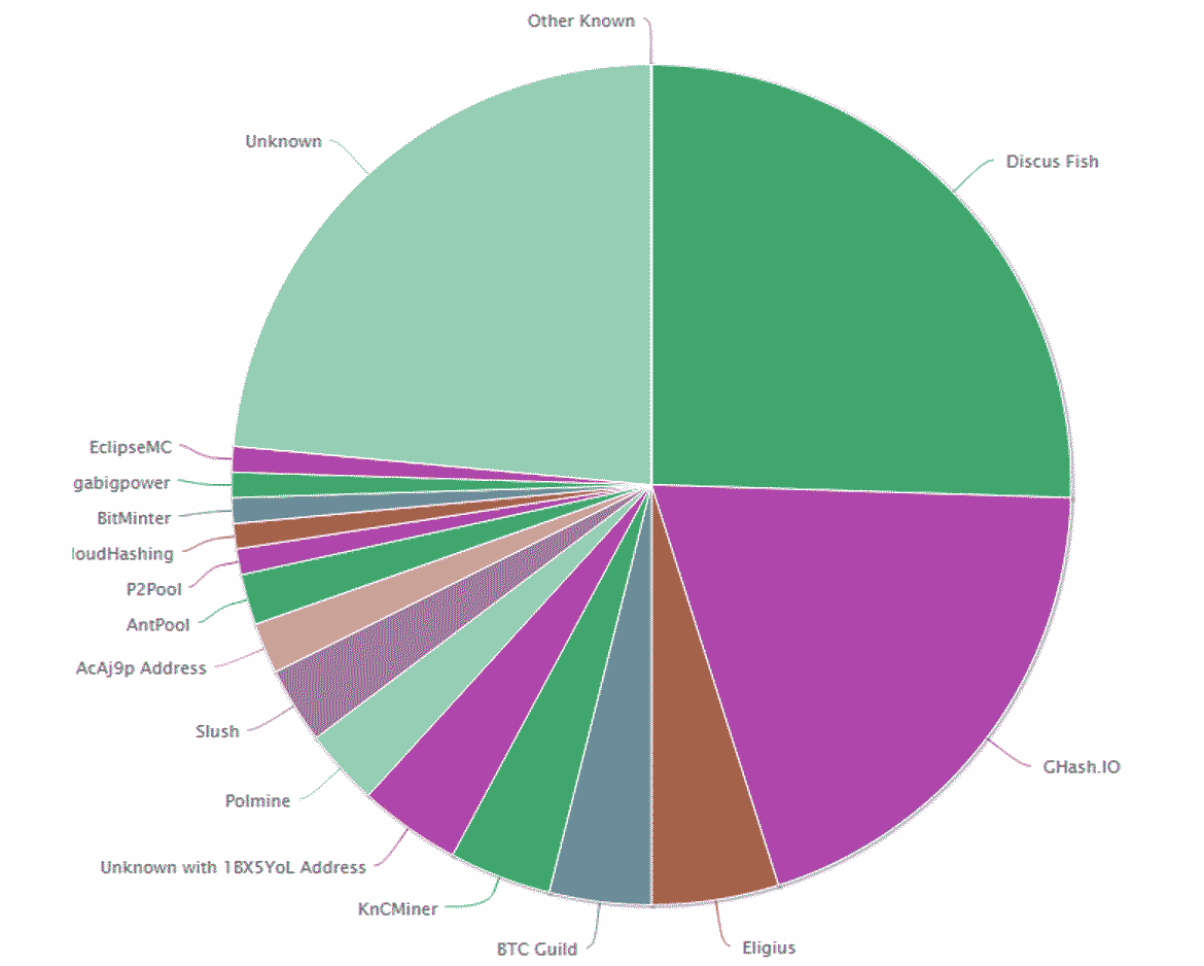


FIGURE 1: HASHRATE DISTRIBUTION (BLOCKCHAIN.INFO, 2014)

This pie graph shows the market share of various mining pools on the bitcoin network. In January of 2014, GHash.IO reached into the mid 40%, causing widespread panic among bitcoin

enthusiasts. GHash.IO themselves released a press statement and voluntarily denied new miners while taking precautions not to reach 51% of all hashing power.

There are a couple things someone with 51% of the network hash rate could do. They could prevent transactions of their choosing from gaining any confirmations, thus making them invalid, potentially preventing people from sending bitcoin between addresses. They could also reverse transactions they send during the time they are in control (allowing double spend transactions), and they could potentially prevent other miners from finding any blocks for a short period of time. (Learn Cryptography, 2013)

3. Government intervention in the blockchain

A handful of firms have expressed interest in tracking coins, which could make it easier to detect crimes such as theft and money laundering, but come at the dire cost of reduced fungibility (the acceptance of all currency in a market). A counter technique to this has been used called "tumbling" or "mixing". Tumbling involves the movement of bitcoin through multiple wallets and varying amounts, effectively scrambling the traceability of the coins. By reducing the usability of specific bitcoin, the utility of the payment system would be greatly diminished and would never be able to reach its full potential.

4. Transaction Bloating

Another option governments may opt to use is flooding the blockchain with transactions, effectively making the blockchain unusable for legitimate transactions due to the sheer volume of requests to move money. In terms of transaction scalability, the blockchain has a maximum frequency of 7 requests per second. The scenario would be similar to a distributed denial of service attack against a website where a huge number of requests are made artificially to overload the server and make the service unusable. If an attacker were to spam the network with requests to move bitcoin between wallets, it could reach this limit and drastically reduce its usability.

Who Is Satoshi Nakamoto?

The creator of bitcoin is one of the greatest disruptors in modern history, and this is reason enough not to want an identity attached to the source code.

So what then do we know about Satoshi Nakamoto? Information on their identity remains unknown. Bitcoin has since evolved without their input, put forth for anyone willing to experiment with the technology. Satoshi's last call was to deemphasize their unknown identity.

When Satoshi had the basic foundation of the bitcoin client built, they transitioned the responsibilities to a group of early enthusiasts and withdrew back into the shadowy depths of anonymity. Nothing tangible has been heard since, although they are widely regarded to still be alive.

Satoshi claimed to reside in Japan, although searches and inquiries into their true identity turn up few results. Facts that were uncovered seem to be contradictory and may purposefully lead followers on a false trail. In his early days working on the project, Satoshi was known for a business-like demeanor and very seldom revealed details about himself, instead dedicating himself feverishly to the bitcoin project.

If the work of the bitcoin client was produced by one man, and began in 2007 as Satoshi claimed, then it must have required serious commitment for several months before releasing it. At one point, when early adopters aimed at increasing its popularity, after users began lobbying for WikiLeaks to accepting bitcoin donations, Nakamoto intervened. Giving decisive orders to the team, they wrote: "No, don't bring it on. The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage." Then, as mysteriously as they had appeared, Satoshi Nakamoto vanished.

As it still remains today, the true identity of Satoshi Nakamoto is unknown and the alias is considered a pseudonym. Whoever the creator was, they wanted to remain invisible, and thus far they have achieved such.

Some researchers proposed that the name was derived from a combination of tech companies consisting of **Sa**msung, **Toshi**ba, **Naka**yama, and **Moto**rola, solidifying the notion that the name was a pseudonym and leading many to question if they were from Japan, given the paper had a distinctly English dialect to it. British formatting in their written work implies Nakamoto is of British origin. However, they also uses American spelling, which may indicate they were intentionally trying, somewhat unsuccessfully, to mask his writing style, or that they are more than one person. Many in the bitcoin space also believe Satoshi to be of American nationality, asserting that the time frames for code submission coincided neatly with someone living in an EST time zone.

Easter Eggs

Satoshi listed their date of birth as April 5th, 1975, and at first glance this appears to be insignificant. However, upon further analysis we find that On April 5th 1933 U.S. President Franklin D. Roosevelt signed two executive orders: 6101 of Civilian Conservation Corps, and 6102 which forbade the hoarding of gold coin, gold bullion, and gold certificates by U.S. citizens. We then find that in the year 1975 gold ownership was again legalized for citizens of the US. Quite clearly Satoshi Nakamoto was politically motivated and displayed such through easter eggs hidden within their work.

Technical Analysis

As for the code itself, it has been dubbed multi-disciplinary and of extremely high expertise in the area of cryptography and C++ programming language, causing many to believe Satoshi Nakamoto is a small group of computer programmers rather than a single individual. Nakamoto claimed to have begun work on the bitcoin project in 2007 and published their paper in the following year. Based on analysis from other programmers who worked on the source code, it does not appear to be written by someone who is well versed in professional programming but rather has a strong academic or theoretical knowledge of cryptography.

> *He was the oracle to which we would go for questions about the system, but he rarely followed standard engineering practices, like writing unit or stress tests or any of the standard*

qualitative analysis that we'd perform on software. Several things had to be disabled almost immediately upon public release of Bitcoin because they were obviously exploitable.

– Jeff Garzik, bitcoin developer

Linguistic Analysis

Adam Penenberg of FastCompany came to the conclusion that Satoshi Nakamoto may in fact be a trifecta of programmers, arguing through linguistic analysis that phrases from the whitepaper match in a very unique sense to a patent application for updating and distributing hashing functions, which was filed around a remarkably similar time frame as the bitcoin.org domain name was registered. The domain was listed as being registered in Finland, and one of the patent authors had travelled there months before the domain was registered (Penenberg, 2011). Regardless, all three programmers deny the claim to the Nakamoto throne. In any case, when bitcoin.org was registered on August 18 2008, the registrant actually used a Japanese anonymous registration service, and hosted it using a Japanese ISP. The registration for the site was only transferred to Finland in May 2011, which weakens the Finland theory (CoinDesk, 2013).

I exchanged some emails with whoever Satoshi supposedly is. I always got the impression it almost wasn't a real person. I'd get replies maybe every two weeks, as if someone would check it once in a while. Bitcoin seems awfully well designed for one person to crank out.

- Laszlo Hanyecz, bitcoin developer

Blockchain Analysis

Based on a blockchain analysis technique created by Sergio Lerner, an authority on bitcoin and cryptography, a dominant entity believed to be Satoshi has been mining the network since block 1, with identical performance as the genesis block. Lerner claims this miner is "the only entity that has shown complete trust in bitcoin, since it hasn't spent any coins," estimating that Satoshi holds around 1 million BTC. (Lerner, 2013).

NewsWeek Claims

Most recently in March 2014, Satoshi Nakamoto reemerged from the shadows of anonymity to clear his suspected identity to a man living in California. After several mainstream news sources claimed to have found the real Nakamoto, and in doing so displayed an astounding disregard for journalism ethics and privacy, Satoshi Nakamoto posted to the P2P foundation "I am not Dorian Nakamoto". (P2P Foundation, 2014) Donations to this Californian man ensue and he rests easy, still quite unsure what all the commotion was about. Dorian Nakamoto is almost certainly not the inventor of bitcoin.

Many in the early community wondered why Satoshi had forsaken them in a project they poured his energy into for so long. Perhaps it was the fact bitcoin was starting to gain traction, evolving without his direct counsel, and the decision to hand the reins of power over was necessary.

However, the question still lingers, have we seen the last of them?

Chapter 2: Blockchain Networks

A revolution is coming – a revolution which will be peaceful if we are wise enough; compassionate if we care enough; successful if we are fortunate enough – but a revolution which is coming whether we will it or not. We can affect its character; we cannot alter its inevitability.

– Robert F. Kennedy

Bitcoin Solves the Byzantine Generals Problem

The *byzantine generals problem* described abstractly as a situation in which components of a whole system are unable to achieve consensus across an untrustworthy network, thereby giving conflicting information to different parts of the system. The system can be expressed as an example in which groups of generals are camped around an enemy city. Only able to communicate by messenger, the generals must arrive at a consensus for their battle plan. However, one or more of the generals may be a traitor and give conflicting information to the other parties. The problem as it relates to bitcoin is to find an algorithm to ensure trustworthy nodes will reach consensus on the blockchain. With unforgeable messages, the mining verification mechanism built into bitcoin, the problem is solvable.

Applications of this solution to reliable computing systems are flexible and applicable to such a great number of use-cases, most of which we haven't even begun to comprehend yet and which will disrupt the very nature of peer-to-peer collaboration on a global scale. Custom currencies, financial derivatives, identification systems, autonomous organizations, and smart property are only a few applications capable of being built on top of the bitcoin protocol.

Even as new technological hurdles are being identified, developers continue to introduce value-added features and alternative use-cases which capture the incredible potential of bitcoin. Currently, things such as receipts, messaging systems, refundable transactions, and increasing the scalability of the network are some of the focus points of the community behind bitcoin. As a

universal public ledger, the bitcoin protocol could help establish property ownership in disputed regions as well as establish rights to public resources in third world countries. Outside of financial applications; decentralized domain management, cloud internet services, law contracts, escrow, voting systems, and data storage are just some of the projects presently being developed.

The Internet as a protocol continues to expand and increase in complexity, as we've seen the introduction of larger IPv6 addresses, email evolving to include file attachments and sharing, and a number of programming languages making things like Facebook, YouTube, and LinkedIn possible.

As the rate of complexity in technological development continues to increase rapidly, we will see a transition to decentralized systems outside the grasp of individual or centralized control. If the systems are purposely set outside the reach of human control, at a point where computing power consensus sets the underlying rules, it will make the transition to an entirely information society. This will have vast implications for the way resources and money are managed. Rather than requiring bypassing human actors, protocols will act without the need of legislators or maintenance operators. These protocols will deliver an entirely different possibility of doing business, one where the network itself represents a *decentralized autonomous organization*.

Autonomous Organizations

Do corporations actually need people to survive? Over the course of the last 100 years the answer has been increasingly *no*. One of the most interesting aspects of bitcoin technology is that it brings with it the ability to create autonomous organizations, an entity which operates completely irrespective of human intervention. Autonomous corporations are described as entities which operate on the blockchain without any central control whatsoever, eschewing all dependence on legal contracts and organizational bylaws in favor of having resources and funds autonomously managed by a self-enforcing smart contract on a cryptographic blockchain. (Ethereum, 2014) The only method capable of creating such a system lies in decentralization of power, and more importantly, management of information which operates entirely on a

distributed network bitcoin now makes possible. Methods for allocating an autonomous corporation's funds could range from bounties and salaries, to even more exotic mechanisms such as an internal currency to reward work. This essentially replicates the legal trappings of a traditional company or nonprofit by using only cryptographic blockchain technology for enforcement. (Ethereum, 2014)

In this regard it is vital to recognize that bitcoin technology represents so much more than what first meets the eye. Developers rave about the network functionality because it opens up a daringly, even frightening range of possibilities. Autonomous corporations will be a new breed of business that acts and behaves, for all practical purposes, just like regular corporations. However, no one 'owns' them. Not the creator, not the customers, not the governments, no one really.

Internet of Things

If society is to take its next great leap forward, it demands a way to not only aggregate information about the things we use, but that the things we use *themselves* are capable of sharing information. Billions of ordinary things are being chipped and linked to an online network capable of delivering results in real-time, a technological trend that has some experts predicting the "Internet of Things" as the next great leap forward. This transformation will change every facet of business and life as we know it today, molding the earth's resources into a living, breathing ecosystem of shared instantaneous information.

Research firm IDC predicts the internet of things will generate nearly $9 trillion in annual sales by 2020. To put that into perspective, total annual sales of the Bay Area's 150 largest technology firms in 2012 was about $677 billion. (Johnson, 2014) Even more interesting as this "global brain of connectedness" evolves, a worldwide network is being conceptualized through internet technology in a way which connects information into a self-organizing system. As the accessibility and complexity of the internet increases, it will syndicate its users into a single information processing system, one which reflects the nervous system of a living organism. Similarly to the blockchain collecting data on the movement of money, timing of transactions,

and ownership of bitcoin, objects which are embedded with a microchip to gather and share information, from “sneakers to drill presses to lamp shades to cans of soda will contain a tiny sliver of embedded thought.” (Kelly, 1998)

Blockchain technology represents an integral component necessary to create an internet of things network where information can be accessed and shared anywhere on earth precisely because it is scalable and independent of ownership. The interactivity of these dynamic networks between data and its components is a characteristic resembling that of a complex adaptive system. Likewise, blockchain networks could form an entirely new kind of adaptable system, one where addresses communicate with one another to trigger scenarios when pre-established conditions are met. Beyond purely payment systems, blockchain networks would provide a means for the internet of things to collaborate and share data without having to rely on centralized systems and a single point of failure. This kind of global transformative change will lead to astoundingly powerful information systems in an economic expansion that dwarfs the industrial revolution.

Chapter 3: Adoption

A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up that is familiar with it.

– Max Planck

The Future of Bitcoin

A future where bitcoin is fully adopted and accepted is a future that looks very different from our world today. If you only consider the implications bitcoin will bring to the banking and financial services industry, you are only looking at bitcoin as a payment system.

Bitcoin technology will essentially allow a redesign of society where our infrastructure for sharing information and resources will not hinge on a central party. Our business models will become incredibly resilient and far more secure from the breach of hacking attempts, although emphasis on information security will increasingly become a top priority. Banking, both commercial and central, will feel disruption to the core and will be forced to align their business models to a type of currency which resides on a decentralized network. Many of our existing institutions will be uprooted, some will make the necessary changes in their business models to adapt to changing economic landscapes. Most will not.

As a still infant monetary experiment, bitcoin has seen explosive growth in acceptance and interest worldwide. As this experiment continues to unfold, bitcoin has the potential to usurp conventionally used currencies and become the standard in payments. Eventually, goods and services might be priced in bitcoin instead of being denominated in dollars, euros, or yen.

No longer will physical robberies exist, but rather thefts of the cyber domain will take center stage. Massive heists will be possible when hackers break the cracks in poorly developed software and the businesses which rely on them.

The need to use credit cards and divulging identification for online purchases might soon be on its way out as well. Not only will the security of storing financial information make a dramatic shift, but the security involved in completing a transaction will be hastened towards methods verified through biometric identification (a form of identification through physiological traits unique to the individual). Previously researched forms of biometric identification include fingerprint authentication, retina scanning, and voice tone activation. These methods of identification will be a more efficient way of verifying our identities. However, they will come at the cost of permanent identification through biological characteristics, something mainstream society will view with an amount of uncertainty, yet still partake in this transition.

Our current understanding of where bitcoin will carry society is still very convoluted. There are no definitive directions that tell us how technology will have changed our lives in a decade's time. No one could have predicted with perfect accuracy the types of applications we use today with the internet TCP/IP and DNS infrastructures built in the early days of development. Bitcoin is a reflection of this evolution in technology. As it now stands, the trend seems to be moving toward trustless networks where users are empowered and responsible for their own information. With more individual power, comes greater responsibility.

Bitcoin Based Society

If businesses and governments are able to take full advantage of the innovative features the bitcoin payment system makes possible, society will become a far more interconnected globalized culture while the speed of exchange between businesses and individuals will take a giant leap forward. In comparison to today's so-called global economy, the behavior of resources will operate on a frictionless, less authoritative system of wealth transfer. Because bitcoin transactions do not concern themselves with the agenda of governments, currency could become detached from political institutions and their related procedures. While bitcoin for the time being remains outside the realm of feasibility for citizens who are not computer competent, they may opt to trust external institutions to store and manage cryptocurrency on their behalf, be these institutions private or government establishments. Because of this, regulation will largely be

targeted at the exchange and money services businesses in order to control the identity and flow of cryptocurrency.

What about the poor? Can those living at poverty levels and on fixed incomes afford bitcoin? Will the rich get richer and the poor get poorer in a bitcoin-based economy? Seeing as the digital economy is one made available wherever internet connectivity is possible and no barriers or discrimination to entry exist for wealthy or poor citizens, it would seem cryptocurrency would raise the global tide of welfare, effectively lifting all boats. The poor would have just as much access and usability for the bitcoin network as the extremely wealthy and, unlike conventional capitalistic structures, money would not systemically flow toward those with the greatest financial abundance.

If you treat your bitcoin well (by storing them safely), and if you desire to increase your holdings of bitcoin (through adding value to the economy), then the rich will have no discriminate advantage over the poor in such a system given that all involved have necessary access to technological and financial services.

We have seen a similar trend of non-discriminatory technology before. As services based on information technology become refined and improved, they are also made available to a wider audience at lower costs. For example, in the 1980s a person carrying a cellphone was considered of high socioeconomic class. Today, smartphone technology is omnipresent in the developed world and growing rapidly in the developing nations. Software services such as conducting a Google search query are free and available to anyone. Technology starts out inefficient and progressively moves toward cheap and efficient access for everyone.

Payment transactions themselves will see possibilities brought to the table like never before. Users will have the ability to pay for WiFi by the kilobyte, pay for faster internet speeds, or pay for time spent with access to privileged sources of information. Although microtransactions were not the primary goal of bitcoin, these types of "nanopayments" are very possible and may only be a few short years away. One problem that has prevented the emergence of micropayment systems is a need to keep costs for individual transactions low, which is impractical when transacting such small sums even if the transaction fee is just a few cents. (W3C Technology and Science

Domain, 2001) Bitcoin solves the problem of impracticality due to costs, because the fees associated with moving cryptocurrency are negligible.

Balaji Srinivasan, an evangelist in the bitcoin space, postulated the following example as indicative of what a society which takes advantage of bitcoin's unique functionality may look like: Imagine it's a few years in the future, you are driving down the road. You are in a hurry, so you decide to accelerate and pass the other cars. Your vehicle could then interface with the other cars, and pay them a sliver of bitcoin to let you pass. You get where you are going faster, and everyone is happy. (Wilhelm, 2013)

What about money-motivated crime? Will bitcoin eliminate robberies? Will we be safer owning bitcoin over cash? In one thought experiment, consider yourself the victim of a holdup. The robber demands you give him your wallet and the cash inside. You tell him you have no cash, only bitcoin, and that it would be impossible to hand any over to you because in order to do so you would need access to your wallet file and to input the password. The only way the criminal will get your bitcoin from you is through sheer force by threatening you to transfer your wallet funds to his address. Furthermore, if the criminal was actually successful in forcing you to send bitcoin to his address, you would have complete transparency into following his transactions and if any of his associated wallets revealed personal identity, it would be possible to bring him to justice. For these reasons, in person thefts are largely unrealistic. Robberies of this nature become impractical. Bitcoin promises to drastically alter returns to violence, because it transcends locality.

In the digital realm, theft transitions to those possessing the ability to exploit weaknesses in information security and steal money via cybercrime. This is why it is so incredibly important to learn how to store cryptocurrency securely. People in the streets will no longer fear being robbed because there will be no real opportunity to take their money unless they relinquish their private keys. Physical muggings for money will disappear. But cyber thefts will cause massive breaches where users and businesses fail to understand best security practices.

Crossing the Chasm

Most early adopters will be quick to admit we are still in an infant stage of digital currency and blockchain technology itself. The price may have seen massive fluctuations and appreciation, however, the infrastructure, the community, and the price equilibrium of bitcoin have yet to be fully realized. The lands of cryptocurrency are still ripe with opportunity and it would be a mistake to wait for the perfect time to enter an emerging trend. At this point no choice is the worst choice of all. Cryptocurrency is a brand new industry, and it remains completely wide open.

Among the many opportunities is that of educating the general public who still hold a distorted outlook on bitcoin. Ask someone on the street if they have heard of bitcoin and if they have, ask them to explain to you what it is. Ask the merchant if they accept bitcoin next time you go to pay for something, and you will be able to judge where the adoption of cryptocurrencies lie within your community. This type of market research will give you a general sense of the adoption of bitcoin, and the research conducted since the very early days shows an undeniable, rapidly adoption and uptake in the understanding of bitcoin and digital currency. Especially among the younger generations, people seem to be able to bridge the gap between national currencies and non-political, cryptocurrencies.

Cryptocurrency is still just making the leap, vying to be known and widely used. Cryptocurrency is in the process of crossing the chasm, making the transition between the early adopters and the early majority of market adoption. The newcomers are still just getting their feet wet. The water is cold, but it has an inviting feel.

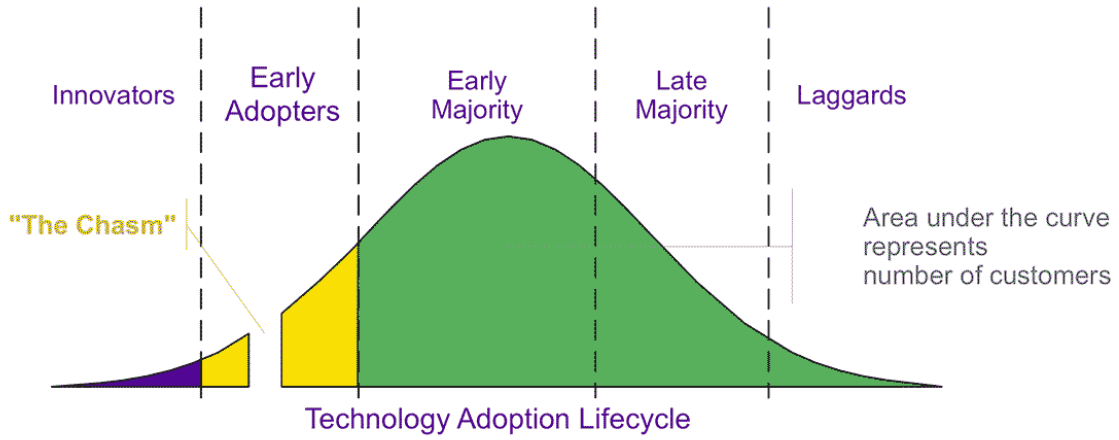


FIGURE 2: CROSSING THE CHASM (MOORE, 1999)

When technologies fail, it is when they attempt to cross the chasm of market adoption. This theory of market adoption usually applies to disruptive or discontinuous innovation, that which forces significant change in behavior by the consumer. Confusion between continuous and discontinuous innovation is a leading cause of failure for high-tech products. (High Tech Strategies, Inc., 2011)

Analyzing the various growth segments, cryptocurrencies are quite empirically not the domain of the majority in any way. The trend – as of 2014 – seems to lie somewhere at the midway point of early adoption. This estimate is made because of representation in media, changing public perception of the technology, and people meeting it with curiosity and self-directed learning. The people who are building the bridge to cross into the majority of adoption are the entrepreneurs, computer scientists, and most importantly the users which are spreading understanding among their peers and communities and helping grow the market.

An easy thought experiment to try with someone who is attempting to understand cryptocurrency is to make the relation between email for communication and bitcoin for money. You require an email address to send and receive messages, and with bitcoin you require a bitcoin address to send and receive payments. Bitcoin then, can be thought of as email for money. This relation makes it easy for a newcomer to understand because we can relate it to something they already use frequently, and understand enough to displace previous modes of communication (or money) such as those that are physical and use central controls.

A good example of changing market perception can be looked at when the Silk Road was closed in October 2013. It was thought of as an anchor on the adoption of bitcoin had been lifted and there was no longer such a link between the black market and cryptocurrency from holding it back and making waves in a big way. Because of the public's negative perception of Silk Road and its affiliation to bitcoin, people understood it mostly as a tool for criminals, absorbing propaganda from news sources and not bothering to consider the notion that the dollar or euro is used just as commonly in illicit activities. Once Silk Road's shadiness was detached from bitcoin, people saw that it could stand on its own, and that garnered massive credibility. Indeed, today most people will be quick to comment that bitcoin makes illicit activities easier, something which is a reoccurring pattern among market adoption with new technologies. The internet in its early days had conversations around its ability to empower criminal activity, and certainly it has made things easier for criminals on one hand, but it has also come with benefits that make comparable illicit activities an afterthought.

Growing pains of the bitcoin economy can be seen in other areas as well, such as the 2014 demise of the Mt. Gox exchange where people who were widely using bitcoin in a way which undermined its ability to function as independent bank account, had their money vanish in a display of poor technology and poor corporate management. In such an event we are seeing weak players in the bitcoin industry being weeded out by market forces, infrastructure continually improving, and users demanding the highest standards of service quality and security from

businesses.

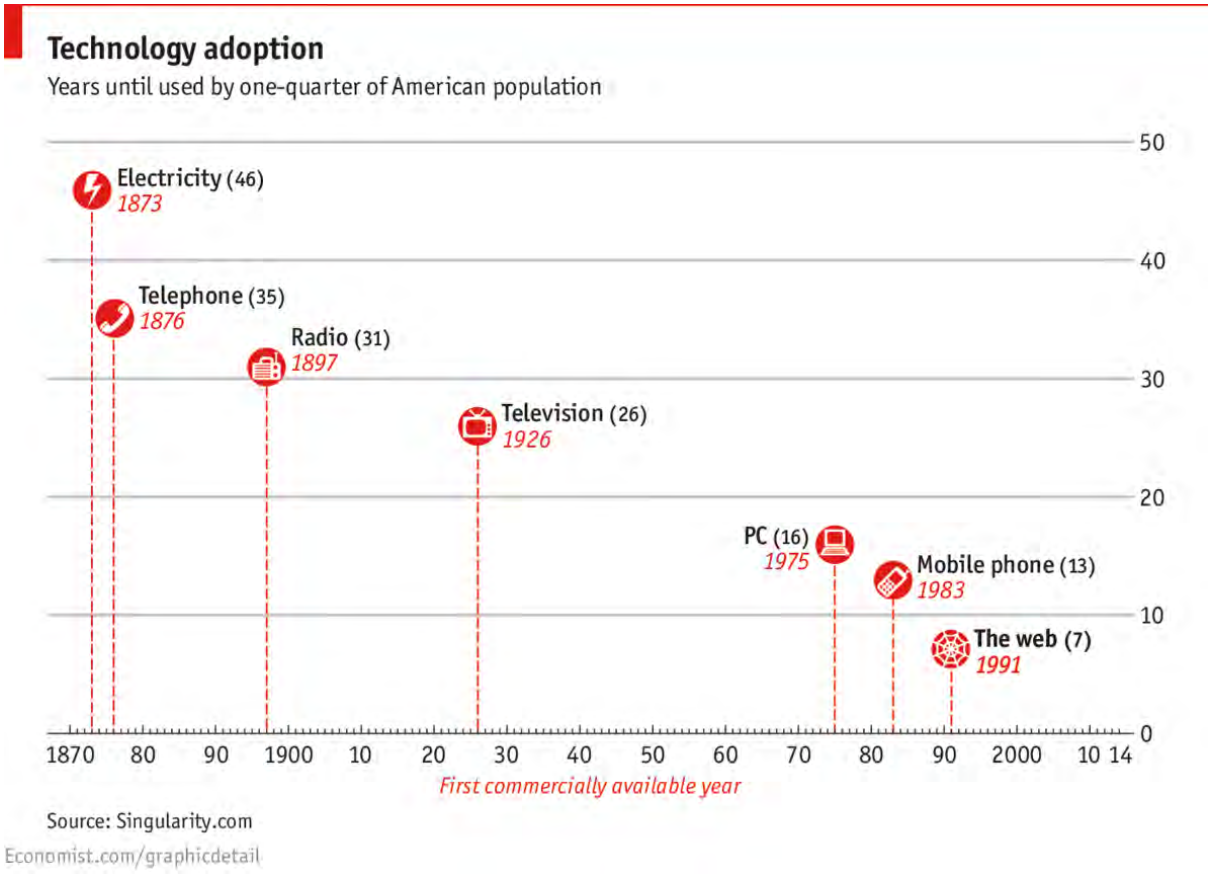


FIGURE 3: ADOPTION OF TECHNOLOGY SINCE 1870 (THE ECONOMIST, 2014)

Adoption of new technologies has seen a reliable increase in the rate of commercial use in the last 100 years. It took only seven years from the first web pages in 1991 for the web to be used by a quarter of the American population. That compares with 46 years for electricity, 35 years for the phone and 26 years for television. (The Economist, 2014) Bitcoin, which can be seen as a system built on top of the internet, has been displaying patterns of adoption which make the internet pale in comparison to the speed at which people are experimenting and using digital money. As a study done by the Federal Reserve Board of Washington, D.C. shows, the number of daily users has grown exponentially in the past few years. In particular, coarse calculations suggest that the user base has doubled every 8 months for the last 3 years. (Federal Reserve Board, 2014) Much in the same way people now refer to physical mail as "snail mail", will we soon be referring to physical and state-controlled currency as "snail money"?

From an adoption perspective, bitcoin has a great momentum in that it conveys the whole product concept. When you get down to the finer details, bitcoin clearly is more than just a lone

financial instrument. It's a framework to decentralize traditional business models whose power has been pinned to the centralized monopolies. Libertarians love it, and rightfully so; a creation that breaks the shackles of dependence like never previously in man's history has the potential to reduce international economic friction and lubricate the cogs of financial markets, not to mention transition away from national economies which operate from toxic debt-based systems.

Network Effects

Network effects describe the increase in value a service provides when additional users join the system. As the network of bitcoin users expands, so too will the benefit involved for everyone involved as the system becomes increasingly valuable and more users join the fold. The network effects of bitcoin allow everyone to benefit as more people begin accepting and exchange in digital currencies.

Online social services operate in a similar way. Twitter, Facebook, and LinkedIn are more useful as more people join their ranks. Facebook would hardly be valuable if there were only a few hundred who used it. Facebook is valuable because it now offers the ability to reach out to most of the people you have ever met in the developed world. Bitcoin operates in a similar way. The more merchants and individuals that are willing to accept bitcoin as payment, the higher people will value it as a medium of exchange, incentivizing new entrants to the market and increasing demand. Over time, this creates a momentum effect as more users join the positive feedback loop. Indeed, this is already what we are beginning to see with bitcoin. Systems that are open and allow all people to operate will defeat systems that close their doors or require extensive verification upon application to join, due to the network effect. Bitcoin requires no verification and is made open to anyone with an internet connection which is why it will become the most powerful network of financial information in the early 21st century.

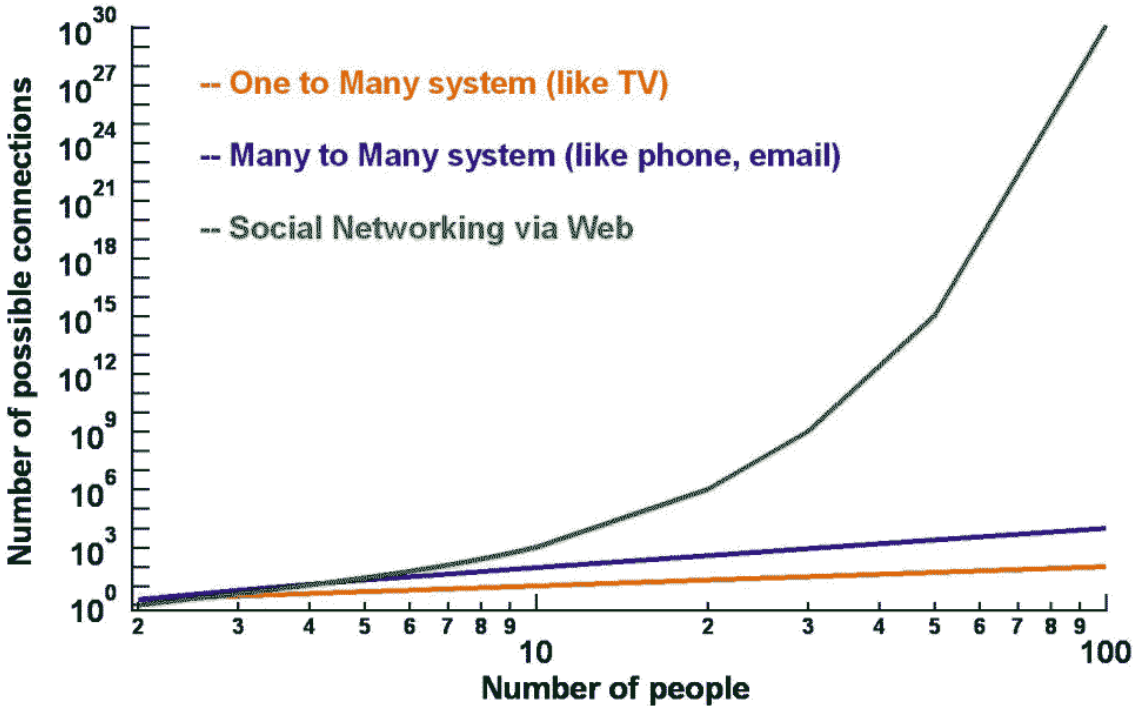


FIGURE 4: NETWORK EFFECTS GROWTH (TRIVIA, 2011)

Networking capacity scales as a function of *N*, where *N* is the number of users (Sarnoff's Law). Many-to-many networks such as email allow connections between the users which function scales as *N(N-1)/2* (Metcalfe's Law). Social networking on the other hand, grows exponentially with the number of users in the network (2^N)-N-1 (Reed's Law). These social connections allow the formation of an incredibly powerful network effect where the impact of the network is directly attributable to the number of active participants.

So when can we expect bitcoin to be more adoptable by the mainstream consumer?

Consider the falling costs and increasing usability of computer technology as the tools and understanding have become much more readily available. In the 1960's, an IBM computer would have filled an entire room and cost millions of dollars to own. This made it impractical for the common person and well out of budget for the average household. However, computers today are marvelously more powerful than they were in the past and consumers are able to access vast amounts of computing power for decreasing costs. More importantly, consumers are able to use these technologies without an intricate understanding of the underlying infrastructure which powers these systems.

Content management software such as WordPress have made publishing content to the web easier than ever and available to people with limited understandings of programming, web development, and computer competency. These types of applications serve to simplify otherwise difficult tasks and take the grunt work out of difficult frameworks which would otherwise be outside the grasp of mainstream audiences. We can expect a simplification in the use of cryptocurrencies where mainstream consumers will enter the market for the first time due to a transition toward user-friendliness, which is a primary ingredient when technologies move into a disruptive phase. In this phase, we will begin to see large institutional players acknowledge the legitimacy of digital currency as a financial asset and begin trading in it, investing in it, and creating infrastructure around it.

Economies of scale combined with Moore's Law allow the common person to now enjoy the benefits of computing which would have previously been unaffordable and far too complex. When this phenomenon is applied to bitcoin it is clear to see it will also become more user-friendly to the average consumer. Interestingly, the network will remain open and accessible to all, and as networks of trust built around currency go, bitcoin will become increasing valuable as the trend in adoption will drive merchants to accept and exchange in it. Bitcoin will get easier to use, but will become increasingly scarce and therefore more valuable.

Many observers have noted that this network effect benefits early adopters tremendously and that newly acquainted investors are only contributing to the appreciation in bitcoin value. Often times, someone who does not fully understand this process will label it a ponzi scheme and claim only the first investors benefit. This is a flawed understanding of bitcoin, essentially dismissing it as a nefarious scheme without providing valid reasons for it qualifying as such a scheme.

The early investors benefit and more so than someone entering the market today, but it comes at no cost to the new investor as they also benefit from the technological and political superiority of bitcoin. The bitcoin payment system requires no new investors to make it serve its purpose. It has demonstrated its utility for sending financial information across a universal network, and has proven to be an eloquent solution to many shortcomings of 20th century payment systems. The early adopters benefit because, as always, the people with strong ties to resources of information

and (more importantly) the ability to recognize patterns within that information, reap immense rewards.

Retail Incentives

In a typical retail environment, merchants deal with a razor-thin profit margin when making sales. Bitcoin offers a considerable incentive to consider as a payment method because it eliminates the processing fees associated with conducting sales which are plagued by a 2-3% credit card fee. Online retailers could commendably cushion their profit margins by offering a discount to customers paying with bitcoin in a bid to reduce their total processing fees.

This scenario, which is often advocated by enthusiasts, is becoming more apparent in the retail space. Overstock.com recently began accepting bitcoin as a form of payment on January 9th, 2014, garnering $130,000 in total first-day spending and totaling $1M in sales made with bitcoin in the months of January and February cumulatively. (Rizzo, 2014) In addition to accepting bitcoin as a payment option, Overstock is now launching a special rewards program that gives bitcoin buyers 1% back in the form of retail in-house loyalty points, installing a bitcoin ATM in their office, and giving employees the option of receiving their salary in bitcoin.

Clearly this approach to payments is working for Overstock. Can other retailers duplicate their success and make the leap to accept bitcoin as a payment method? If there are significant cost cuts in processing fees to be had, most retail businesses could increase their profit margins by adopting alternative payment methods such as bitcoin.

The barriers to accepting bitcoin as a payment option are almost entirely psychological. Most people would believe there to be some sort of expensive physical infrastructure required, but in truth nothing more than an app download needed for receiving payment. All smartphones today have this functionality and anyone which a phone in their pocket is capable of receiving and sending payments in the physical domain. The merchant's largest hurdle is understanding how the network functions and learning to trust in the validity of the payment and currency.

Not only are retailers incentivized by increased profit margins when using bitcoin, but the risk of chargebacks is eliminated. Ask a retailer what the most cumbersome aspects of running such a business are, and they will commonly answer chargebacks and processing fees associated with credit cards and the banking system. Bitcoin can provide a solution to both of these issues and merchants who have adopted this payment option early have become strong advocates for a system which solves their largest challenges when operating a successful business.

Is Bitcoin a Cult?

In society today, when we hear the word *cult*, the hair on the back of our neck stands up and our ears cringe. We quickly want to change the subject because of how negative a connotation the word cult carries with it. Why is this so? How can a word in and of itself be so detested and shunned from our lexicon? Let us explore the word *cult*.

The word *culture* comes from the root word *cult*, and describes a collection of human capacity in the pursuit of betterment for the individual and the whole. Culture is central to the way we view, experience, and engage with all aspects of our lives and the world around us. Thus, even our definitions of culture are shaped by the historical, political, social, and cultural contexts in which we live. (Sorrells, 2013)

More narrowly, the word *cult* describes a social order which carries deviant beliefs, that is, a group of individuals who operate from a set of practices which violate the conventionally dominant mindset of the surrounding culture. A cult establishes new social norms and practices to operate from, and therefore is seen as deviant until these new social norms are adopted as the dominant belief system. Once this saturation occurs, anything which violates these beliefs is then seen as the new cult. A cult in and of itself is neither good nor evil, but a social order that defies conventionally accepted social order.

Let us begin our analysis with three basic assumptions of a cult:

1. Holds socially deviant beliefs
2. Holds regular, frequent ritual practices
3. Holds their founder as the ideological realization of their socially deviant beliefs

Let us apply this framework to an existing culture: The United States of America.

Do the American people abide by socially deviant beliefs? At the time of its founding, America was based on the idea that if you're willing to work hard, success is available -- life, liberty, and the pursuit of happiness above all things. Americans subscribe religiously to the notion that it represents the "Land of Opportunity" and that anyone can realize the "American Dream". This is clearly seen when America is the most overworked culture is the world. At a time when the dominantly held belief was to serve the greater good of the British Empire, these ideas in the 18th century were indeed deviant.

Do the American people engage in regular ritual practices? Every February of the year, Americans drop whatever it was they were doing and gather around to watch the SuperBowl. Not necessarily because of their love for the sport of football, but because it is the *American* thing to do. Do not get in the way of an American and their SuperBowl time. The SuperBowl is one of the largest ritual practices of a culture on the planet, and it reinforces the beliefs that the social order was founded upon. It draws in an audience from around the world and sensationalizes commercialism and competitiveness. The SuperBowl does indeed represent an American ritual tradition.

Do the American people hold their founders as the ideological realization of their cultural beliefs? The founding fathers of America -- John Adams, Benjamin Franklin, Alexander Hamilton, John Jay, Thomas Jefferson, James Madison, and George Washington – are held as the epiphany of the belief system which the entire culture is founded upon.

Is America then a cult?

Consider a group of 100 people. 99 of those people are involved with the cult while one person has a different set of beliefs entirely. Would the 99 people of the cult describe themselves as cultists? Or would they view the outsider as having something fundamentally wrong with them and an inferior set of beliefs?

The only criteria to effectively judge a cult by then, is if their belief systems help improve the lives of individuals and the whole. A cult in itself is neither good nor evil, but a social order with deviant beliefs.

The United States of America indeed started as a sort of cult. It still holds deviant beliefs, has ritual traditions, and has the ideology of their 'father figures'. Only now, it is one which has reached a critical mass where its belief system has become the new social norm. Its belief system is no longer deviant and therefore, everything which violates its norms is the *new* cult.

So then is bitcoin a cult?

Does the bitcoin community hold deviant beliefs? Anyone in the bitcoin community knows this to be plainly true. There is an underlying, religiously abided to belief that we can create a system using the decentralization potential of bitcoin to build a better world. There also seems to be a deep loathing of the current banking system.

Does the bitcoin community engage in ritual practices? Regularly, and as a scheduled event, the bitcoin community braces itself for a readjustment in the difficulty of the mining reward. The block reward halving represents a ritual tradition within the bitcoin community. Every time the compensation per block of bitcoin is halved, the beliefs of the culture (that of scientific innovation and disruptive competition) are reinforced upon the subscribers.

Does the bitcoin community hold their founder as a sort of religiously actualized father figure? Without a doubt Satoshi Nakamoto is held as the realization of the underlying principles engrained into the bitcoin culture. Satoshi Nakamoto is the oracle upon which the concept of bitcoin was created. It is most interesting to note, that Satoshi has no personal identification and therefore, indirectly upholds the cultural belief of anonymity.

This brings us back to our original question: is bitcoin a cult? To which, the answer is a resounding, **yes**!

The only question which remains is when it will reach a critical mass and its socially deviant beliefs become the new norm. The bitcoin industry attracts some of the most intelligent and ambitious people in the world. It has the potential to improve the lives of, not just millions, but **billions** of people!

And that is indeed a worthwhile pursuit.

Chapter 4: Cyber-economics

There are 3 eras of currency: commodity based, politically based, and now, math based.

– Chris Dixon, Technology Investor

Advantage Africa: Why Developing Nations Stand to Gain Most

When you consider traditional forms of money -- US dollars, the Euro, Chinese Yuan – you realize these currencies are not backed by anything more than a promise that they will be worth something. Only recently has our money discontinued being backed by gold and other physical assets that could be audited for. People using these forms of money with nothing backing them but debt know that they can purchase food or shelter with them and, thus, it holds their trust. Similarly, once people begin to realize that bitcoin is accepted as a form of payment, it will see a rise in value and increasingly be seen as a legitimate currency. Under this pretense, it is clear that currency is dependent upon a network of institutions that are willing to accept it and investors confident enough to hold it as a medium of exchange.

If bitcoin acceptance reaches a critical mass where necessities of food, shelter, and clothing can be bought with it, it will likely have reached a tipping point where it displaces national currencies. In this scenario, many areas of the world would be leapfrogging banking infrastructure and traditional money wire transfers. Most notably this would describe the financial landscape in developing economies such as the nations of Africa.

Leapfrogging is described as a theory of economic development which skips inferior or obsolete technologies in order to move directly to advanced ones. Take, for example, phone coverage in African countries. Landlines and grids for household use were never fully developed because, by the time Africa came into market view, mobile phones were the new paradigm of telecommunications and hence, the entire infrastructure for household landlines was leapfrogged by cellular technology. Similarly, bitcoin technology could leapfrog the banking infrastructure of western economies and go directly to a new financial paradigm and serve the needs of the vast

number of the unbanked in these regions. All that would be required on behalf of the citizens is a mobile device with internet connectivity.

FIGURE 5: PERCENTAGE OF UNDERBANKED POPULATION (ALBERTO CHAIA, 2010)

Worldwide, approximately 2.5 billion people do not have a formal account at a financial institution. Access to affordable financial services is linked to overcoming poverty, reducing income disparities, and increasing economic growth. If one third of adults don't use formal banking systems, can you imagine what a bank account stored in cyberspace will allow them? Bitcoin will benefit Africa more than any other area in the world once it is properly accessible and accepted. In doing so, it will have a considerable effect on pulling struggling African economies out of the dark and into the developed and modernized world.

> *The combination of ubiquitous Internet-connected mobile devices and digital currency presents a tremendous opportunity to radically expand access to financial services on a worldwide basis,*
>
> - *Jeremy Allaire, Circle Internet Financial, 2013 US hearing on digital currencies.*

The potential to provide financial services worldwide is echoed by the adoption of mobile payment technologies such as M-Pesa, a mobile-phone based money transfer and microfinancing service for Safaricom and Vodacom. M-Pesa is estimated to have a near 70% market share in regions such as Kenya and is becoming more accepted in surrounding countries. (World Bank, 2012)

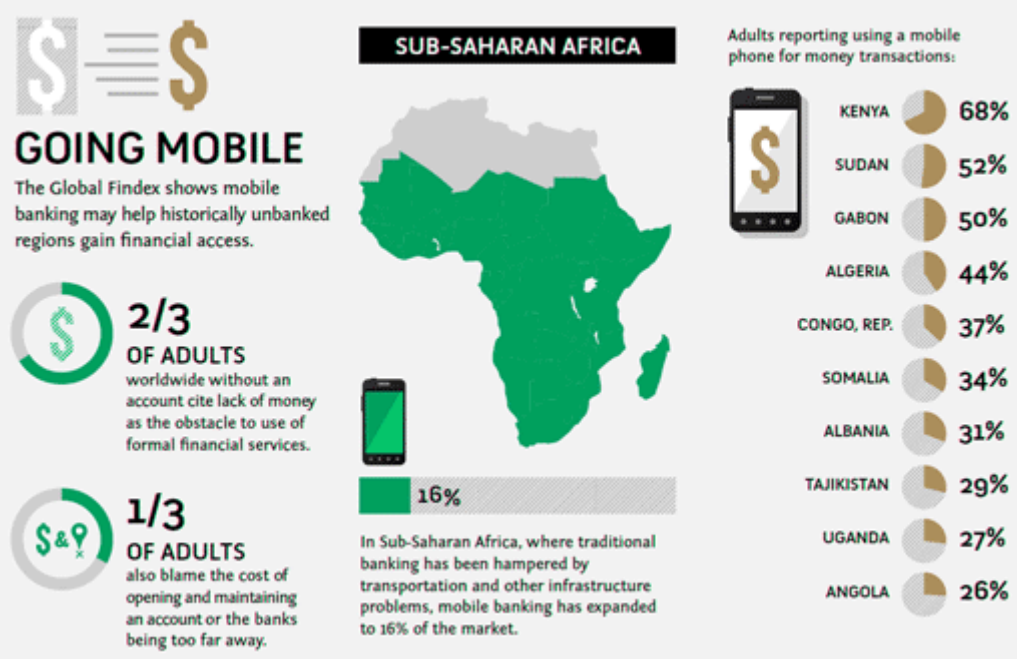


FIGURE 6: SUB SAHARA MOBILE PAYMENTS (WORLD BANK, 2012)

Admittedly, there remain many social barriers needed to bridge the unbanked to the rest of the financial world. Bitcoin does not help the illiterate learn to read instructions, nor does it guarantee someone with a mobile phone will want to do banking through it. Traditional customs of African countries also show that their citizens more often rely on societal traditions of borrowing money from friends and family rather than a third party.

Beyond just mobile payments and access to banking infrastructure, several African economies are the product of mismanaged currency policy. Zimbabwe's legacy of collapsed currency, with inflation reaching a nauseating 231,000,000% in mid-2008, is a prime example of such disastrous government intervention. (The Economist, 2013) Because of the devastating effects of hyperinflation, Zimbabwe has since adopted the US dollar as the main currency, a position it still holds today. The hyperinflation that crippled Zimbabwe was largely caused by currency being

too liberally printed, a swollen stock of money chasing a diminished supply of goods. The economy since has been recovering but only slowly making ground.

Africa is in prime position to benefit from a financial network built around bitcoin. Since the money supply of bitcoin is hard capped, and money printing is impossible, currency manipulation becomes much less of a concern. Governments in Africa will have fewer options of instituting thoughtless policies once bitcoin is adopted by the populous.

Bitcoin may not be the definitive answer for the masses that remain unbanked, but it is at least a step in the right direction. The hotspots for adoption will be most apparent in geographies which have a very unreliable currency and financial infrastructure to back it. Therefore, it is reasonable to assume that out of all the nations of earth, African countries will stand to benefit the most from financial technology such as bitcoin.

Deflationary Characteristics

Keynesian economists have stated that a deflationary currency, one which increases in purchasing power relative to other goods over time, is inherently negative for an economy because it creates a financial ecosystem which entices individuals and businesses to save money rather than using it to create jobs and invest in companies. They claim that a deflationary currency incentivizes the individual to adopt a buy and hold strategy because they know it will be worth more tomorrow than it is today. This is often referred to as hoarding and it can lead to lower interest rates and increase long term investments. In doing so, this decreases the velocity of money in the economy, or the speed at which units of money change hands. In a healthy economy, a high velocity of money is a very good thing, so a decrease in velocity would be unfavorable. Because the monetary base of bitcoin cannot be expanded, the currency would be subject to severe deflation, and this is something which we have seen to be true thus far.

The Austrian school of thought counters the idea that deflation is inherently negative, claiming that as deflation occurs in all stages of production, entrepreneurs who invest benefit from it. As a result, profit ratios tend to stay the same and only their magnitudes change. In other words, in a deflationary environment, goods and services decrease in price, but at the same time the cost for

the production of these goods and services tend to decrease proportionally, effectively not affecting profits. (Bitcoin Wiki, 2014)

A deflationary currency may incentivize a buy and hold strategy but it also creates a delayed gratification effect. Do the work now, and you'll reap the rewards later. Unlike an inflationary currency which incentivizes the individual to go out and use the money to create capital or spend it immediately, a deflationary currency would also incentivize the individual to work hard today so that their money is naturally working for them. Given all else equal, your purchasing power would increase because you've already put in your labor. The earlier and harder you work, the more you gain. With inflationary currencies, I'm not too worried about gaining money today because I know that it will have decreased in worth tomorrow, continuously thereafter, and after a 20-year span will have lost roughly half its value (given the typical US inflation rate).

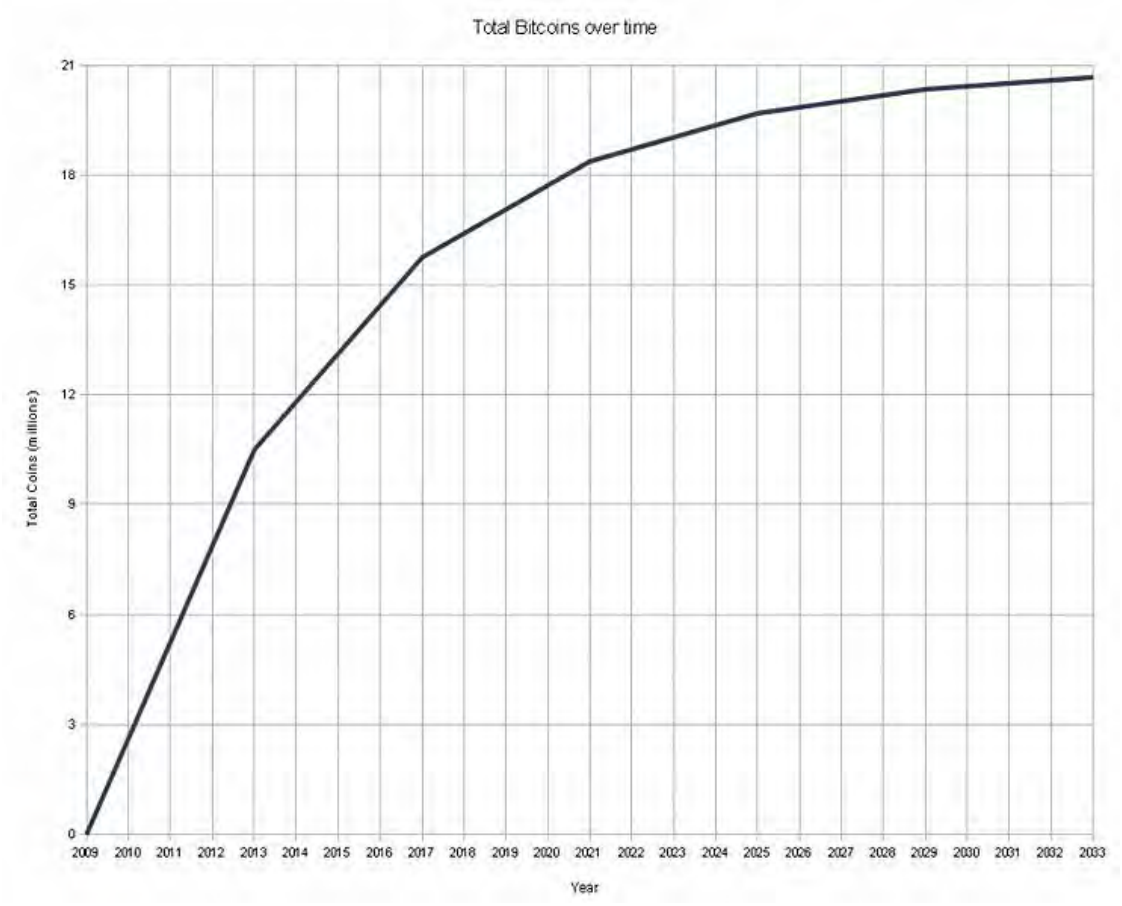


FIGURE 7: TOTAL BITCOIN OVER TIME

Even if bitcoin users know their money is increasing in purchasing power, they will still opt to spend their money on needs for food, housing, and other goods to ensure their survival. No person will have the willingness to put capital gains on bitcoin ahead of their own basic, compulsory needs. "Elaborate controls to make sure that currency is not produced in greater numbers is not something any other currency, like the dollar or the euro, has," says Russ Roberts, professor of economics at George Mason University. The consequence will likely be slow and steady deflation, as the growth in circulating bitcoin declines and their value rises. "That is considered very destructive in today's economies, mostly because when it occurs, it is unexpected," says Roberts, but he thinks that won't apply in an economy where deflation is expected. "In a Bitcoin world, everyone would anticipate that, and they know what they got paid would buy more than it would now." (Simontie, 2011)

Deflationary currencies don't dominantly exist because they would increase the real value of debt by design, and this is one of the reasons why a money supply backed by debt will not be sustainable in the long run. Runaway deflation, commonly referred to as a deflationary spiral, would lead to the collapse of an economy under certain conditions in a fractional reserve banking system. In the bitcoin system, money is not debt but an asset.

TABLE 1: MONEY SUPPLY SCHEDULE

Block	Reward Era	BTC/block	Year	Start BTC	BTC Added
0	1	50.00000000	2009.007	0.00000000	10500000.00000000
210000	2	25.00000000	2013.000	10500000.00000000	5250000.00000000
420000	3	12.50000000	2016.993	15750000.00000000	2625000.00000000
630000	4	6.25000000	2020.986	18375000.00000000	1312500.00000000
840000	5	3.12500000	2024.978	19687500.00000000	656250.00000000

1050000	6	1.56250000	2028.971	20343750.00000000	328125.00000000
1260000	7	0.78125000	2032.964	20671875.00000000	164062.50000000
1470000	8	0.39062500	2036.956	20835937.50000000	82031.25000000
1680000	9	0.19531250	2040.949	20917968.75000000	41015.62500000

While the supply is controlled, the issuance of bitcoin is predictable. As we discussed earlier, mining new blocks of bitcoin into circulation becomes increasingly difficult (see Table 1: Money Supply Schedule) while the quantity of bitcoin in each block is continually halved. This, along with a limit on the amount that will ever be available, is the primary driver for bitcoin deflation. By the year 2040, roughly 99% of all bitcoin available will have already been mined.

Money Velocity

Looking forward, when the bitcoin economy and technology is sufficiently used in society, we will see a velocity of money vastly superior to traditional forms of currency. Because bitcoin offers a very low-friction method of making payments, unlike paper money, it brings with it the possibility of a very high-velocity transaction rate. The beauty of making a frictionless form of payment is that it will eliminate the delay between when a payment is sent and when it is confirmed. No more 2-5 business days, locked accounts, and relentless fees with your money. With this increased velocity of money, struggling economies will be able to access a stronger pipeline with established economies which could serve to pull them out of stagnation. This pipeline for transactions will lead business to be conducted “at the speed of thought”. Bitcoin will accelerate the velocity of money using the ability to transfer directly over a digital, frictionless network.

The economic principles built into the bitcoin ecosystem are fundamentally game-changing. Bitcoin is an deflationary money supply by design, having a fixed total issuance of 21 million units. Furthermore, the supply rate is predictable and can be anticipated by market participants

more accurately than any 20th century money supply. Perhaps most importantly, bitcoin is a money supply which is not representative of debt, but an asset, something which is opposed to our current fiat system. These factors combine to make bitcoin a game-changing economic paradigm which will make the entirety of its adoption cycle a very wild ride.

Bitcoin vs. Gold

The bitcoin vs gold debate has raged on in investment circles since bitcoin has entered discussion circles among investors with increasing interest. Gold has been used as a form of currency and trade for thousands of years, but as we will show, bitcoin may be the kind of financial breakthrough to replace it.

Early on, seasoned investors began questioning the legitimacy of bitcoin value and wondering how such a commodity could have intrinsic value. What differentiates bitcoin from a mere collectible and what makes it similar to precious metal assets such as gold or silver? Among many circles, especially gold bugs and older-generation investors, bitcoin was not considered a valid investment up until very recently.

FIGURE 8: USD PER BITCOIN, GOLD OZ. 2011-2015

In order to properly analyze the value of bitcoin vs gold, we must clarify which attributes of gold are valuable and prop them up against the promise of bitcoin. When we measure the implications of today's economic environment, it is clear to see that bitcoin is gold for the 21st century, or as some pundits have advocated, a 'digital gold'.

Gold has perceived value because it is scarce, quasi-indestructible, and serves an industrial purpose. Bitcoin inherits all of these attributes and also adds the characteristics of portability and perfect divisibility. Both are also exceedingly durable and cannot be counterfeit. The main advantage for bitcoin over gold as a commodity is that bitcoin has perfect portability, while gold must be insured; physical stored and guarded, and verified that the integrity of the substance has remained intact and not mixed with other filler metals such as tungsten. If you are moving precious metals across borders, you must declare it. With bitcoin, no amount of border authorities can detect if you hold bitcoin as ownership can be distilled to memorizing the private key of your wallet. If you are attempting to buy something with gold, it usually needs to be exchanged for currency first. Bitcoin payments only need a smartphone to transact.

In terms of fungibility of a commodity, having one unit exactly similar to all others is important. With bitcoin, every unit of currency carries with it the entirety of its transaction history. This violates the idea of perfect fungibility as units of currency may be seen as more or less desirable if

it has previously been used in illegal activities. With gold, this is not so simple. Metals can carry dilutions and values estimates can differ depending on the mint which issued the coin or bar. We also know that the benchmark used by investors and central bankers to determine the value of precious metals has been, and continues to be, heavily manipulated. According to Bloomberg, authorities around the world, already investigating the manipulation of benchmarks from interest rates to foreign exchange, are examining the $20 trillion gold market for signs of wrongdoing. (Vaughan, 2014)

Bitcoin represents a form of gold which has transcended the physicality and operates within the cyber domain. It's very possible to send hundreds of millions USD worth of bitcoin within seconds and only the sender and receiver are aware of the identities involved. Physical actors cannot exert control over the portability of this commodity, and therefore, 'digital gold' represents bitcoin accurately.

Gold is a store of value which relies on tradition to support its value base along with a few minor industrial purposes. When you take away this perceived tradition of value you are left with a few manufacturing uses and nothing more. Tradition has built an idea in the consumers mind that gold and silver hold tremendous intrinsic value. This proposition is falsified, as precious metals clearly derive their intrinsic value from luxury and manufacturing applications, their price artificially high due to market perception which has vastly underestimated the quantity of these metals.

Despite what a merchant may tell you, we have no clear idea on the supply of gold. We have barely explored ocean depths let alone mined deeper than a scratch in the Earth's crust. Who is to say how much gold and precious minerals near-Earth asteroids contain?

One of the main reasons to add gold to an investor's portfolio today is as a hedge against economics disaster, that of collapse or hyperinflation. Outside the gold-bug crowd, and among the current generation, gold as a valid form of transaction is a stretch of the imagination. If such an event were to occur, would people be exchanging in pieces of gold if internet connectivity were still available? At the blurring rate of current technological advancements, who in their right mind would consider a shiny metal to be valuable?

Gold may have been reliable in the 20th century, but among a generation of digital natives, who are connected psychologically (and soon to be physically) to their mobile devices, bitcoin will increasingly be the method of choice for commerce. This is the information age, and information represents the most valuable form of commodity. Bitcoin is financial information stored on a collective, distributed computing network. The fact that bitcoin is instantly transferrable across the globe with no need to identify the parties involved, is why it will conquer precious metals. Bitcoin and other developments in cryptocurrency will make precious metals an afterthought as a store of wealth.

Antifragile Properties of Bitcoin

You would be hard pressed to find an investment that carries with it the antifragile properties of bitcoin. Antifragile is a term which here describes something which benefits from shock; it thrives and grows when exposed to volatility, randomness, disorder, stressors and risk. When things get uncertain, bitcoin thrives, and it gains on the mismanagement that is all too prevalent in our global economy. It can be used as a hedge for uncertainty in various markets, although the bitcoin market is very uncertain in itself. It's a place to look to when economic sanctions clamp down on the freedom of money, and it expands a portfolio's diversity if the investor is willing to absorb the risk. Bitcoin represents an antidote to conflict found in regions which do not have stable debt management and poor monetary policy.

> *Bitcoin is the beginning of something great: a currency without a government, something necessary and imperative.*
>
> - *Nassim Taleb, Anti-Fragile*

In his book *Anti-Fragile*, Taleb defines antifragility as having a larger upside than downside from disorder. Bitcoin encompasses this definition well. The potential downside of bitcoin is that a number of early adopters will lose their initial investments. The upside then? Lifting billions out

of poverty by bringing them onto the global stage of commerce, providing a bastion of liberty for decades to come, and curb corruption among governments.

The randomness of human error and conflict present a landscape which gives bitcoin a convincing draw for people looking to put their money in an asset which cannot be seized or manipulated. Consider the Cyprus financial crisis of 2013, where the country imposed capital controls leaving residents cash-restricted. Banks on the island nation of Cyprus temporary shut off access to customer deposits under losses on Greek government debt which put the nation on the fringe of bankruptcy and provided bitcoin a fertile opportunity in spite of these restrictions.

Bitcoin skyrocketed from $10 at the start of 2013 to $266 in early April, and although not all that investment/speculation can be attributed to the Cyprus crisis, the largest push happened as finance ministers publicly declared the seizure of citizen's capital. Investors and citizens in distress did not run to gold, they took a strong hold in a digital currency which was the remedy for the mistakes their government had made.

Systems which are artificially insulated from shock make the eventual threat more damaging but less frequent. Banking regulations and bail-outs, domestic industries which are protected from competition among imports, and others are all examples of insulated firms which are shielded from vulnerabilities which would otherwise make them stronger over the longer term. Bitcoin, on the other hand, has no such incubation. Regularly, the exchanges of bitcoin are hit with hacking attempts, negative media attention, and competition among a growing number of alternative cryptocurrencies. Each time, the antifragile properties of bitcoin allow it to become more resilient.

Antifragile systems are necessarily complex, and a degree of randomness is natural when it is functioning properly. These types of designs are resistant to top-down controls and interference, because they are too complex to be controlled externally. The only way that we can effectively work with complex systems is by working from the inside – by gearing our decisions and actions to act as minor tweaks (trial and error) on the system (just as evolution does). (Taleb, 2012)

Bitcoin is resistant to top-down controls by design due to the user base processing transactions. Developers of the source code could not suddenly make changes because the majority of the network would have to agree with said changes. No interference can take place where 51% of the

user base does not agree on a particular change. The mining power of the bitcoin network is what directs certain blocks of transactions to be included in the ledger or not. Moreover, an external actor cannot control the functionality of bitcoin. Therefore, as Taleb describes, the only way that the system can operate is from within – by implementing minor tweak into the system much in the same way evolution does on the flow of life and survival.

Price Stability

Many critics of bitcoin make the observation that it is a very volatile and fluctuating unit of value. Businesses aren't able to predict as accurately how much revenue they are making because they are not sure how the value of bitcoin may change from day to day. The price stability of bitcoin is seen as one of its greatest liabilities, as a wildly fluctuating unit of value makes a payment system much less usable.

As time goes on, the volatility of the price will subside as more users of the network enter. With more people holding and using bitcoin, more users need to take common action for there to be a significant price movement and it will make buys and sells based on emotion less common. In fact, we have seen such price stabilization of bitcoin over the course of 2014. Bitcoin is becoming increasingly resilient to market fluctuations and the confidence of investors seems to be holding strong. This is largely attributed to more people learning about, understanding, and most importantly, using bitcoin.

Consider a large holder selling his bitcoin insensitive to price. He gobbles up whatever he can take, sometimes causing panic, other times not causing much of a stir at all. Because that single seller now divided up his portion of bitcoin to many smaller holders, new users have entered the network and more people can say that they own bitcoin. As this process continues to unfold, we will see stability reflect a relationship with the number of people using bitcoin. Similarly, as bitcoin becomes more stable it also becomes more useful as a tool of commerce. At one point the price could be relatively stable, it all depends on market perception and while fiat currency is the benchmark, that perception will be skewed. As more people and businesses come to accept it as a

form of payment, this volatility will subside. When we take a look at past performance, we see a decline in the volatility of bitcoin's price, a pattern that will likely continue.

FIGURE 9: BITCOIN HISTORICAL VOLATILITY (DOURADO, 2014)

Eli Dourado, a PhD student at George Mason and research fellow at Mercatus Center, estimates that if the price stability of bitcoin volatility continues to subside at the current pace (halving ever 3.5 years), it could be as stable as the Euro in less than 15 years. Notably, Eli collected his price data from Mt. Gox, an exchange with relatively high volatility when compared to competitor businesses and one which has now ceased operations due to technical faults. The trend is statistically significant with a univariate OLS regression yielding a t-score on the date variable of 15. (Dourado, 2014)

What about the *daily* volatility of BTC/USD? Cryptonomics, a cryptocurrency technology and economics authority, estimated bitcoin daily volatility to hover around 5%. Comparing that to an S&P 500 index that fluctuates about 0.7% per day, and you see why bitcoin is considered erratic.

Regression analysis of bitcoin between price volatility and liquidity reveals a medium to strong negative correlation. This is consistent with a medium of exchange with an inelastic supply, as well as the economic features of competition between media of exchange. (Surda, 2011)

Bitcoin is increasingly a viable currency because of price stabilization and has the potential to be a widely used payment system when it is more widely accepted and speculators enable it to move closer to a price equilibrium. Although a price equilibrium will not truly be found, as the market perception of bitcoin will continue to deviate indefinitely, over time, and as new users enter the market, bitcoin will continue to stabilize and move closer to a permanent and accurate unit of account.

Price Trending

As the traditional generation of fiat currency continues to lose ground to digital currencies, those who first dismissed cryptocurrency as irrelevant will take the time to learn of and use its advantageous features. What most people fail to realize is that this is happening right now. The massive rises in bitcoin price do not merely represent an increase in its value, utility, or acceptance. Rather, it reveals a decline in the supremacy of the USD.

As we mentioned earlier, the value of bitcoin is derived from its supply and demand. Because supply is predetermined by source code, demand is the best factor for determining where the price will go. But how would one go about determining the demand for such a unique financial asset? Some believe following digital trends can provide insight, more specifically internet queries using Google and Wikipedia.

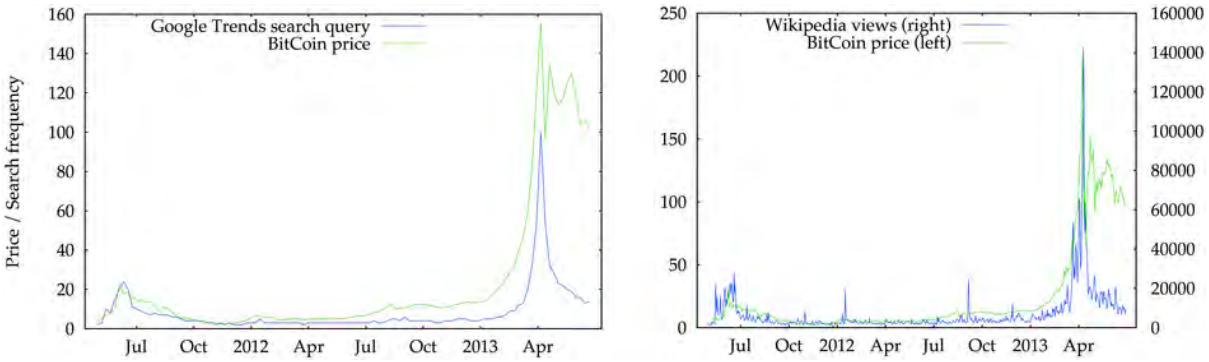


FIGURE 7: GOOGLE TRENDS & WIKIPEDIA QUERIES (BEREZOW, 2013)

As it is clear to see, there is a strong correlation between bitcoin price and search queries. However, the trend seems to display that internet traffic and media attention are a lagging indicator on the price of bitcoin. That is, increased interest is only a product of the rise in bitcoin appreciation, not the causation of it. The variables of search queries and price appreciation represent bidirectional causation, one where a rising price leads to higher media attention, which in turn leads to even faster rising prices. This positions us in a "virtuous cycle", one where good news drives bitcoin's price ever-higher. Similarly, in times when negative news of bitcoin heists, thefts, and hacks surfaces in the media, a "viscous cycle" occurs where the price spirals continuously downward. Both of these factors fuel volatility as they play a fitful balancing act in its public perception and therefore, its demand. There exists a strong correlation between the price of bitcoin and public visibility.

Greater Fools

The greater fool theory states that the price of an object is determined not by intrinsic value, but rather by the irrational beliefs and expectations of market participants. (Investor Glossary, 2013) As it pertains to bitcoin, the theory would describe a situation where there is always a greater fool present who is willing to overpay during an overheated market. This would lead a rational investor to buy under the belief that another party is willing to pay an even higher price and expect that the bitcoin can be resold to a "greater fool" in the near future. These often risky investments are made with the assumption that they will be able to sell off the bitcoin for profit because someone will be bidding at an even higher price, rather than determining if the asset is

actually worth the purchasing price in the first place. This phenomenon fuels the volatility of bitcoin while posing high downside risk. Eventually, no greater fool will exist to purchase the overpriced asset and a price crash ensues. The greatest fool is left "holding the bag".

In the investing world, taking big risks in cases where there is potentially much to gain and very little to lose is a common strategy among speculators. With bitcoin, the payment system works and there is huge potential in the usability of it, so it will likely have some value for at least the foreseeable future. However, the real upside comes when you consider how early on in its development and adoption we are. With a sizable investment in bitcoin there are risks you will lose most of it, but just as likely and even more so is the situation where you could realize substantial gains.

Some advocates would say that digital currencies, and the industries it is creating, represent perhaps the biggest investment opportunity the world has ever seen. The true worth of bitcoin as a system lies in that it is distributed sharing of unduplicatable digital assets over an internet protocol. Consider investing in bitcoin not only to increase your net worth, but because the rise of digital currencies is inevitable. To resist such a trend would be equivalent to going against evolution or attempting to swim upstream a swiftly flowing river. Bitcoin has potential to facilitate the greatest wealth transfer in the history of mankind.

The 21st Million

The world's first trillionaire by USD valuation could quite possibly be the creator of bitcoin, Satoshi Nakamoto. If bitcoin continues to climb the ladder of exponential price appreciation, than once Nakamoto decides to move his money and make transactions with it, there will be a seismic shift in the perceived supply of money.

The Nakamoto wallets comprise roughly 5.5% of the total bitcoin which will ever be in circulation and about 9.3% which are available today. If there is one party controlling five percent of all currency that will ever be created in an economy, this poses a huge risk to the integrity of decentralization in the first place. One in ten bitcoin today lies dormant, but alive.

Truly, the mammoth wallets owned by Satoshi Nakamoto are one of the biggest threats to price stability and market viability of bitcoin.

At this point, not much can be done about the large volume of bitcoin that lie hidden in Nakamoto's wallets. We don't know which addresses they belong to and we only have estimates of the amount they hold. What many assume is that Nakamoto has multiple wallets rather than one, and that they have since discontinued their mining activities.

If bitcoin should continue to challenge the status quo, and be a serious threat to the established legacy businesses, it is indeed worthwhile to ask the types of questions which would seek to uncover the identity of a party which controls the largest stake in an emerging economy. Satoshi has no obligation to reveal their identity, yet if bitcoin should become worth 10 or 100 times its current value, questions about their identity may haunt those who are deeply invested in this emerging digital economy, both in terms of financial and ideological investment.

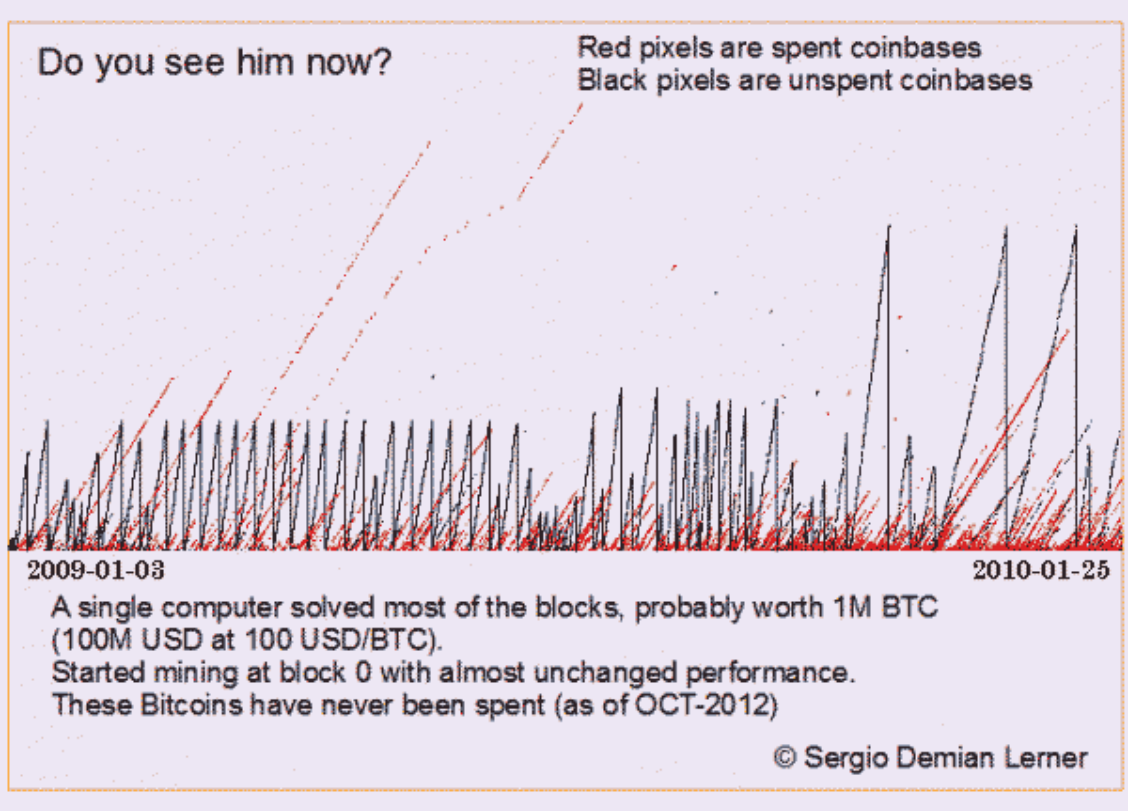


FIGURE 9: BITCOIN UNSPENT COINBASES (LERNER, 2013)

Almost all are owned by a single entity, and that entity began mining right from block 1, and with the same performance as the genesis block. It can be identified by constant slope segments

that occasionally restart. Also this entity is the only entity that has shown complete trust in Bitcoin, since it hasn't spent any coins (as last as the eye can see). I estimate at eyesight that Satoshi fortune is around 1M Bitcoin. – Sergio Demian Lerner

Another perspective to consider is whether the stashes of bitcoin Satoshi Nakamoto holds could be purposefully destroyed. If Nakamoto were to take such a route, say in the name of equality, it would cause a bullish run on the rest of the bitcoin in circulation because of increased scarcity of money supply. Destroying their stash of bitcoin could be done by either misplacing the private key to a wallet or sending a transaction to an unclaimed wallet address.

Lost coins only make everyone else's coins worth slightly more. Think of it as a donation to everyone. – Satoshi Nakamoto

When it comes down to it, the effect bitcoin has on the world may correlate sharply with the causes Nakamoto dedicates their purchasing power to, if they do eventually move their money. Money has a profound way of influencing people. Business leaders recognize the opportunity to shake up the world that comes with owning massive capital. Nakamoto can either use that ability to power the common good, or for less noble reasons. Perhaps if they decides to use their holdings on personal pleasures, while forgoing the opportunity to make positive changes outside the borders of bitcoin, then we may have overestimated the heroics of the great anonymous wizard Satoshi Nakamoto from day one. Regardless, do not let anyone tell you the identity of Satoshi Nakamoto is *not* important.

Technological Unemployment

When advances in computer science were first conceived, many people believed integrating these advances into everyday life would make our condition much more automated, integrated, and efficient. Some even believed it would usher in a utopian society, where human suffering was no longer required to persist and evolve. Rather, machines would fill the positions undesirable and

offer radical new ways of using computational power to solve complex problems. In some cases, this has been achieved, but it has also come at a cost. We now live in a society which is inextricably tied to technology and science, yet we have positioned ourselves so that only a tiny fraction of the population even begins to understand these advances. People today are arguably more disconnected and distracted than ever, feeling lost without the aid of a smartphone and outsourcing their critical thinking to Google searches. As technology continues to become increasingly complex, this cognitive gap will continue to widen.

Technological unemployment has become an increasing reality as more and more skillsets have been automated by applications we have developed in computing. As Reid Hoffman, a founder of LinkedIn states, "As massive technical innovation radically reshapes our world, we need to develop new business models, new technologies and new polices that amplify our human capabilities, so every person can stay economically viable in an age of increasing automation."

Bitcoin's ability to hold information in a publicly distributed ledger will disrupt far more than simple financial services, and in doing so the workers in these industries will be shifted into positions that utilize innate human drives of creativity, reasoning, and critical thinking. As McAfee and Brynjolfsson assert in *The Second Machine Age,* "Rapid and accelerating digitization is likely to bring economic rather than environmental disruption, stemming from the fact that as computers get more powerful, companies have less need for some kinds of workers.

Bitcoin technology will not lead to long term structural unemployment, but it may uproot several particular industries and well established financial businesses. In the short run, payment processors and money transmitter businesses will be the first to feel bitcoin's wrath, wiping away financial services businesses which tie high fees to the transfer of money. Firms like Western Union and MoneyGram will see their remittances business wither away due to a fee-free alternative.

Technological progress is going to leave behind some people, perhaps even a lot of people, as it races ahead." (Brynjolfsson & McAfee, 2014) There has never been a better time to be a person with the ability to recognize these trends and put the proper skillsets to use. Likewise, there has never been a worse time to be a worker with ordinary and replaceable skills. Those who fail to make this adjustment will be much worse off.

Chapter 5: Political Implications

This may be the purest form of democracy the world has ever known, and I for one am thrilled to be here to watch it unfold.

– Paco Ahlgren, financial analyst at Wi-Fi Alliance, perspective on bitcoin

Untaxed Bitcoin is a Human Right

In 1991 a man named Phil Zimmerman released a software messaging system which could offer people a way to send text-based communication in a secure manner backed by the mathematical principles of public key cryptography amongst a host of contemporary hashing and compression standards. Zimmerman felt a need to create something that would give users an outlet for information confidentiality in an age where increasing threats of privacy invasion meant online communications were subject to prying eyes of government authority. These authorities were overstepping their boundaries of legal jurisdiction and attempting to exercise coercion in a domain where their actions came at the cost of information freedom. Originally designed as a human rights tool, the software encryption came to be published under an open-source license and adopted as an IETF standard. This software would be called 'Pretty Good Privacy', or PGP for short.

The publishing of the PGP software landed Zimmerman in a three-year criminal investigation by the US Government, who classified the encryption as military-grade weaponry. As they claimed, the distribution of source code represented a "munitions export without licence". During this time, encryption procedures which comprised keys larger than 40 bits were categorized as munitions under the US export regulations. The smallest keys PGP used were 128 bits, thus at the time they fit within the legal definition of munitions. If convicted, the penalties for violation were substantial.

Years before the government had placed encryption, a method for scrambling messages so they can only be understood by their intended recipients, on the United States Munitions List,

> *alongside bombs and flamethrowers, as a weapon to be regulated for national security purposes. Companies and individuals exporting items on the munitions list, including software with encryption capabilities, had to obtain prior State Department approval.*
>
> — *Electronic Frontier Foundation: EFF's History*

Zimmerman argued the case in a creative manner, publishing the entirety of the source code in a physical book, relying on the principle that weapons, bombs, and software may be restricted goods and were justly under the regulation of the state. Books however, were protected under first amendment rights. In early 1996 the case was closed with no charges lain against Zimmerman or any subsequent party. Since that time, PGP has gone on to become the most widely used and trusted email encryption.

Economic Munitions

In the same way which PGP was originally classified as a sort of weapon, could bitcoin as well be seen as a type of munitions? Given that bitcoin is based upon the same public key cryptography that PGP originally was, and that a representation of a bitcoin key pair contains 512 bits of data, could it then be argued that bitcoin is nothing more than an exercise in the practice of mathematics, and if so is backed by constitutional rights to the freedom of speech?

Two federal appeal courts have already established the rule that cryptographic software source code is protected by first amendment rights to free speech, namely in the cases of *Bernstein v. United States* and *Junger v. Daley*. In both such cases, it was ruled that government regulations preventing its distribution and use of such software were unconstitutional.

Bitcoin is a powerful weapon in the fight for economic freedom. The difference lies in the idea that this time, the weapon is in the hands of every individual, and made accessible to anyone, anywhere; and that is a most dangerous opposition for the enemies of liberty. How can the state lay claim that they have an inherent right to control that which they do not issue, cannot control, and which under their very constitution is protected by first amendment rights of free speech?

How will a bitcoin dominated state print money to fuel war? Who will protestors have to blame in a system where no one controls their financials but themselves? How will the state tax a commodity which they have no legal jurisdiction over? In many regards, bitcoin is representation of economic munitions.

> *Bitcoin is not about making rapid global transactions with little or no fee. Bitcoin is about preventing monetary tyranny. That is its raison d'être. Monetary tyranny can take many ugly forms. It can be deliberate inflation, persecutory capital controls, prearranged defaulting within the banking cartel, or even worse, blatant sovereign confiscation. Sadly, those threats are a potential in almost any jurisdiction in the world today.*
>
> *—Jon Matonis*

War is not funded overtly, but rather discretely and stealthily through an array of macroeconomic looting. A war is first waged against its own people in the form of economic initiatives and later against a foreign threat through military action. Offensive militarization requires dipping into the homeland honeypot, almost always alongside a healthy combination of media propaganda which simultaneously moves the population towards a mindset of fear and/or seduces them into believing that this action is heroic and patriotic. Because of this, it then becomes a social taboo to not be fearful of the consequences of external threat (you are aloof) and it also becomes taboo not to want to fight (you are a coward). The state does not serve to save the people from catastrophe, nor does it exist to revitalize the patriotic spirit of a nation, it cares nothing of the subjects it governs. It exists to advance the agenda of the conspiring exclusive who issue the orders from the very beginning.

There is no glory in fighting violent battles and there exists no fear but our own self-imposed limitation. The entire facade is an illusion; an act of smoke and mirrors.

Taxation

How will governments levy taxation on an asset they have little or no control over? In a world where there is no means to confiscate or control property on behalf of another individual, the

need for the state would cease to exist. Mass taxation on digital currency is not feasible. As we have seen, developments in the field of bitcoin have been focused on increasing the anonymity and resiliency against taxation efforts. This is a trend which will continue until a solution is devised which is capable of withstanding even the most sophisticated attacks from government forces. Such a currency would carry with it enormous market demand which would be attributed to its inability to be taxed.

Income tax is a modern phenomenon that has been around just long enough so that the current generation has stopped questioning the assumption that it is necessary. In truth, income tax targets the earned means of survival for individuals, yet is collected before civilian access is granted. Dependency upon the system comes at the cost of the individual being under the heel of an authority which enforces taxation through intimidation; in one regard this enforcement echoes slavery.

In our own estimation, it becomes quite clear that taxation will refocus into its rightful positioning as a voluntary contribution to an external body of administration. No longer will taxation be enforced through coercion, but become a voluntary act towards a particular cause. As it stands today, this is not how we view the state but rather free market forces at play.

No different than night or day, ying or yang, 1's or 0's, our money has been transmuted into bits and bytes. What does this scenario mean for our conventional state institutions? It means that because our money supply is now a practice in science, and the encryption applications which underlie its functionality are subversive to external control by design, the state no longer has the means necessary, nor the inherent legal right to control money. Bitcoin's killer application has been here since its very inception: the nation state will no longer exist.

Parallels Between Bitcoin and the Printing Press

The printing press is widely considered one of the most influential inventions is human history because, for the very first time, it destroyed a centuries-old monopoly on the publication and dissemination of knowledge. Johannes Gutenberg's movable type technology, invented in Mainz, Germany (circa 1439), ushered in a permanent change in the structure of society as it began an

era of mass communication and the dismantling of a stranglehold on the interpretation of written word. Unrestricted circulation of books made information free flowing and gave birth to revolutionary ideas which, under the current establishment -- the church, would never have been permitted.

With authority waning, political and religious institutions of the time saw their influence eroding and fought viciously to prevent it. The church was up in arms. The "Royal Family" was furious. They even went as far as forging **new laws** which held that only printers with special license's and prior approval were allowed to print books, multiply knowledge and spreading culture for citizens.

500 years ago, the spread of knowledge came from a central source. Anyone or anything that violated that customary authority was quelled and prosecuted. Does this sound familiar?

As his first work with his new invention, Johannes Gutenberg decided to print a 42-line latin bible. As their first work of the blockchain innovation, Satoshi Nakamoto produced the *genesis* block -- an allusion to the first passages of that same bible.

> *Under no circumstances did the church allow the citizens to spread information on their own, they governed the whole law enforcement; prevention, punishment and harassment.*
>
> *Today, we know the only right thing for the evolution of society was to let that knowledge go free. That Galileo Galilei was right. Even if he was infringing on the knowledge monopoly. We're talking about a time when the church went out in full force, promoting the idea that citizens didn't have to, learn to read and write, since the priest would tell them everything they needed to know anyway. The church knew what it would mean if they lost their control.*
>
> *- Charlie Shrem/Rick Falkvinge, Nothing New Under the Sun (Falkvinge, 2014)*

How much influence would the source of spiritual knowledge have on the masses of people, and would the source of money issuance have a similarly persuasive effect on those same masses?

Much in the same way the printing press enabled individuals to connect with their proto-nationalist self (identification according to common attributes such as religion or language) could bitcoin allow transcendence to a sort of **supranational identity**?

Not only does bitcoin have revolutionary implications for the decentralization of money supply, but it also has roots in free thought. An individual's ability to express information through the medium of the blockchain grants the ability to make it virtually unalterable. It is a permanently recorded history not only of transactions, but a forever-engraved ledger of information.

More than ever, our past is stored on a global mind, a database of events unfolded: the internet. The parties which control these channels of information are in a place of extreme power, as they are able to oversee, to a large extent, historical records.

Rather than history being controlled by the entities which control the present, we now have a digital medium to record history, thereby breaking Orwell's dictum of '*Who controls the past controls the future; who controls the present controls the past.*' Bitcoin is a way to propagate information in a way that we have never seen before.

Bitcoin Inherent Regulation

Bitcoin has regulation built into the very nature of its existence, just not through our conventional idea of what regulation looks like. Because of the technological nature of cryptocurrencies, our regulations put on these types of systems will always be, to a large degree, futile. Cryptocurrencies have established their own set of rules and guidelines through the source code they are built upon, forcing legal frameworks upon this type of 21st century innovation will ultimately cause more suffering and friction than necessary. The only choice of regulation we have in terms of cryptocurrencies is not to try and fit them inside some existing doctrine, but to abide by their laws of finance and information freedom. Bitcoin is a system which will only be governed effectively through digital law, an approach which functions solely through a medium of technology itself.

With the recent backlash from the announcement of the New York State Department of Financial Services' regulations on cryptocurrency, it is necessary to return to the roots of what

makes bitcoin beautiful -- the fact that it does not recognize traditional, 20th century forms of law-making; it does not require the approval of human counterparts. To understand why bitcoin will not be limited by the wordsmithing of lawmakers (and dangerously broad legal frameworks at that), one needs to undergo a paradigm shift in what we hold as conventional legal structures.

Bitcoin, and cryptocurrency is destined to be regulated effectively only through technology itself. It will not bend to the whim of those who still hold conventional forms of law making as relevant today. Times have changed. We can only look to the past for answers so often, and every now and again a disruption of our conventional standards arises which refuses to be pigeon-holed.

Decentralized networks make conventional law-making look like horse drawn carriages to a Model T engine. When Henry Ford conducted market research with his customer base, he reported they would consistently ask for a "faster horse". Instead a making a faster horse, he created something entirely new: the Model T.

Bitcoin is not simply an alternative to current financial system, it is a bold new redesign of our money which stands independent of that which came before it.

A Fight for Liberty

Increasingly, technologies have come along which aid individuals in the path to individual empowerment. Such technologies have been invented which give freedom of expression, freedom of speech, and freedom of disclosure. When someone considers the idea of freedom, people generally agree that it is an end in itself. To be free is to be exempt from external authority and restriction. After considering Viktor Frankl's profound publication, *Man's Search for Meaning*, one might conclude that "there is no desire beyond freedom but to let it ensue". The internet gave us freedom to distribute communication around the world, and now blockchain networks give us the freedom to decentralize resources of information, bitcoin being the first implementation of such in the form of a shared financial ledger.

This new type of system may offer the ability to essentially "be your own bank", however, it does not guarantee that the future global currency most used will be decentralized and entirely outside the control of legacy establishment. In a similar way the internet disrupted the telegraph and

democratized information transmission, bitcoin is disrupting money and making it harder for current governments to control people's finances. This will not happen overnight, as governments will fight and claw their way to retain control of money issuance and power until their bitter end. The internet did however, make it much easier for governments to gather information willingly volunteered unto social networks by citizens. Will bitcoin come to represent a similar tool for surveillance in the near future?

Once bitcoin becomes more mainstream, when more people understand the benefits and implications, governments will initially attempt to control the handling of currency through the businesses and bottlenecks which it can be monitored through, and this attempt will be met with as much success as limiting file sharing, illegal downloads, and Tor operations. The attempts to control this network will be met with stiff resistance, ultimately technology reigning superior.

There will be no collision with government regulation. Bitcoin does not collide; it flows around like water around the system.

As we have plainly seen with the rise of bitcoin, money is fundamentally a collective agreement, and because global superpowers have the ability to mold that perception which establishes conformity, it will take a certain length of time before bitcoin and cryptocurrencies are able to mature through their growing pains and reach mass levels of adoption with the mainstream consumer.

Control of this financial power will transition to those with the intellectual willpower who contribute to the technology in a way which is the most beneficial, as determined by market forces. The money power of the 21st century will take a giant leap towards meritocracy and away from monopolization and manipulation. Cryptocurrencies have an inherent regulation, that of a cyberpolitical nature. Truly, bitcoin is code as law.

Given that cryptocurrencies operate in the digital realm, one without consideration for geographical or standard political boundaries, government structures themselves will see a radical shift, colluding in order to control the financial information and currency without borders in what may eventually give rise to a supranational government configuration.

Bitcoin is now entering the phase where governments are fighting adoption and the fact that they have no leverage over this bold new design of money. The people who are still not taking this movement seriously are the people who will benefit the least and will be swept up in the decision making of those who are informed and prepared for this massive change in political economic nature of our governments.

Milton Friedman himself once posed the idea of replacing central banking institutions with a computer capable of mechanically managing the supply of money. He proposed a fixed monetary rule, called Friedman's k-percent rule, where the money supply would be calculated by known macroeconomic and financial factors, targeting a specific level or range of inflation. Under this rule, there would be no leeway for the central reserve bank as money supply increases could be determined "by a computer" and business could anticipate all monetary policy decisions. Will we ever see Friedman's computerized banking institution put into action? Considering the mining network of cryptocurrencies are the closest thing to an authority, and mining will only get more specialized and thus centralized in the future, we may well already be on the path towards it. A type of central computing network which holds the majority of computing power over the bitcoin network may come to describe accurately the approaching supranational government configuration.

Bitcoin Will End the Nation State

Satoshi Nakamoto set in motion the unraveling of the nation state and the end of central banking … two closely related institutions that have directed history since history has been recorded. When we come to understand the economic and technological implications of bitcoin, we arrive at a somewhat startling yet undeniable conclusion: that bitcoin will end the nation state.

> *We know what happened to organized religion in the wake of the gunpowder revolution. Technological developments created strong incentives to downsize religious institutions and lower their costs. A similar technological revolution is destined to downsize radically the nation-state early in the new millennium.*
>
> *– James Dale Davidson, William Rees-Mogg, The Sovereign Individual*

Bitcoin as an Economy Independent of the Nation State

Many observers of bitcoin argue that its value needs to be pegged to a stable, conventional currency in order to assess its value. They claim that bitcoin is too volatile to be taken seriously, and thus, serves as only a novel financial and technological innovation for moving money. What these observers' fail to realize is that bitcoin does not need to be pegged to a national currency any more than the sun requires the gravitational pull of the earth. The sun has no concern for the deviations on the trajectory of the Earth just as bitcoin has no concern for the developments within national economies. Speculation is the only reason critics will argue that bitcoin needs to be pegged to a national unit of account, and for those actors, bitcoin cares not.

Many observers of bitcoin also argue that for the sake of adoption, bitcoin needs exchange businesses and ATMs in order to grow its user base and subsequently, its market capitalization. On top of these businesses, the conventional thinker will also argue that proper regulation needs to be enforced on these operations for the 'good of the investor'. We certainly don't want another episode of Mt.Gox do we? Although exchange businesses and ATMs certainly do serve to hasten the adoption process, they are not required for the expansion of the bitcoin economy. The mining process serves as the issuance authority. The miners are the employees of the bitcoin network, and thus the true citizens in the digital economy.

Bitcoin is a [Nationally] Untaxable Money Supply

Let us begin with a simple premise: you cannot levy taxes on an encrypted money supply through judicial authority. Bitcoin is untouchable by the nation state and can be used potentially anonymously. In his *Code 2.0* manifesto, Lawrence Lessig described law as a multiplicity of factors, regulation being just one among many. Other factors include the free market, social norms, and architecture. In the bitcoin economy the architecture is source-code. Truly, bitcoin is code as law and the blockchain represents a sort of constitution for the digital economy.

No amount of lobbying, congressional hearings, or bitlicenses will make a measurable impact in the long run. Because bitcoin is untouchable by the nation state, the lifeblood of these

conventional bodies or governments will wither and die. Increasingly, politicians will struggle to squeeze the revenue from their citizens in order to pay for the ever-bloating expenses and programs it has conceived. When the lifeblood of the nation state, the tax revenues, have run dry, that is when we can confidently proclaim that the great empires of nations are dead. The empires whose watch oversaw the advancement and destruction of society to extremes previously unheard of, will be no more.

Bitcoin Transitions the Nature of Violence

The most dominant currency today is held in place because the authority which issues it has the greatest ability to impose and defend from violence. The United States Federal Reserve Note is the global reserve currency not because of the nation's unyielding belief in freedom, or the sound monetary policies of its leaders. The USD is the world currency because, as we have seen in times past, when someone threatens to detach themselves from their dependence of it, thereby compromising its position as the king, the authority subverts its own laws and seeks to destroy those who would attempt to disarm its dominance.

Bitcoin, on the other hand, transcends physicality and cannot be destroyed by any nation state. In the cyber domain, the economic returns on violence transition to those who are capable of executing cyberwarfare and thefts through the medium of digital technology itself, The cyberdomain is and will continue to be a haven for those with the technical intellect to command a machine to do what they want it to, rather than the original instructions it was given.

Because bitcoin transitions the theft of money and the issuance of money to the digital realm, the nature of violence too is placed within a context which can only be acted upon by participants who dwell in cyberspace. What kinds of violence could be imposed through financial mediums of a digital realm?

One such example we have seen is the rise of *randsomware*. Randsomware is a sort of virus which locks down important files and only unlocks them after a certain amount of bitcoin have been sent to an address. This type of cybercrime is already causing massive disruptions among corporations and will continue to have important implications for the intersession of crime and the digital medium.

Another act of violence could be considered the collectivization of data on the movement, holdings, and relationship of financial information in a digital economy such as bitcoin. A huge incentive presents itself for data mining the blockchain and analyzing the various relationships and patterns of spending. Much like the internet of today, the bitcoin network initially presents itself as a bastion of liberty and anonymity, but is in truth destined to become the most surveillanced form of money ever to exist.

Everything you've come to know about pensions, government subsidies, social welfare programs, and nationality as an ideology, will be obliterated by the implications of bitcoin. We have an emerging digital economy, which for the very first time, is able to operate completely independent of physical or central actors. We have a money supply which is based on the science of mathematics and therefore, has its very use backed by a human right to the freedom of speech, yet more importantly, we now have a money supply which is made technically impractical to tax with our current methodologies due to encryption technology. We have a network of financial information which transitions the nature of violence, that of cybercrime, to the digital realm.

These factors combined will ensure that the nation state as it exists today will be irrevocably disrupted in a societal shift unseen since the dethroning of religious institutions during the 15th and 16th centuries. This time, the major difference is that it will happen much more quickly, and have much more pervasive effects than almost anyone is anticipating.

The Incoming Surveillance of Bitcoin

In many ways, the internet, which was originally seen as a tool of expression has also come with the vulnerability of being a perfect outlet for surveillance. Our online, mobile, and electronic communications are under constant surveillance from institutions with vested interest in collecting an assortment of important political, personal, and economic data. The bitcoin blockchain houses a vast amount of economic data and with it, the possibility of tracking spending patterns which leads to gathering political and personal data as well. Could it be that technologies such as bitcoin, which initially promise greater individual freedom, will be subverted by institutions of power into a twisted form of panopticon?

Privacy is a non-negotiable human right. It is important to identify matters of national security, but having the right to privacy is more valuable than destroying both privacy and the potential to do harm for the false promise of 'security'.

We are a community floating on a mote of dust somewhere in the universe. No one can promise you security.

We would even go as far to say anonymity is a human right as well, because at the moment we come into this world we have no identity attached to us but the sole characteristic of being human. Anonymity should thus always be an option.

The fact that bitcoin is digital is precisely why it will lead to an increase in surveillance of payments. Although the bitcoin public ledger of transactions carries with it the potential to be used anonymously, most people do not and will not use it this way. In truth, it is very trivial to destroy the anonymity of your bitcoin wallet into a fully translucent view of your financial life projected to whoever cares enough to know.

The difference in determining if your spending is anonymous is where your real-world identity is not linked to the wallet address. If it is linked, any transaction you make can be followed through the blockchain and your spending habits can be monitored, a most opportunistic scenario for surveillance purposes.

If bitcoin is adopted by a more mainstream audience, and if not used in conjunction with some third party service, people's spending habits will be as hidden as their social media activity or browsing history is today. The idea remains that the concept of the blockchain ledger itself is neither good nor evil for privacy, but the actions the user takes to preserve anonymity and withhold sensitive data will determine the utility they receive while using it.

Bitcoin Neutrality

Technology neutrality describes the principle where the applications of the technology can be applied to a variety of different scenarios without preference for any economic, political, or cultural dichotomy. A current example of this would be the debate over net neutrality and

whether all packets of data should be treated equally rather than giving certain corporations access to 'super highways' of electronic transmission.

With bitcoin, it will retain its usefulness only if it is made a standard independent of external desires and control while exerting no discrimination over characteristics of transactions being made over the blockchain. The bitcoin network must handle every amount of transaction and every wallet address identically. Similarly, a transaction should be treated identically, independent upon the IP address the wallet was created with. Neutrality as a principle is built into bitcoin today, but it will only survive if it is vigorously defended. There will be plenty of opportunities to defend it because, as we have seen, institutions of power will want to infiltrate these types of networks and use them to systematically serve the already established firms and disenchant competition. This infiltration of control is what we are seeing happen with the internet protocol today and is not limited to handling of data, but also handling of censorship as well.

Censorship 2.0

Amateur nation states today disallow online communications and rule the use of bitcoin as illegal. The superpowers use these technologies entirely differently, instead as a kind of law enforcement tool. The professionals use the internet, and will use the blockchain, to identify criminal activity. We live in a world where everyone has the right to speak, but the power now transitions to those being heard. That opportunity is made available by a level playing field and afforded to only those who command the merit of being heard. Segregation of the net fundamentally opposes the neutral playing field principle of the internet and is therefore a form of censorship. Because opposition against net neutrality would fundamentally make it harder for certain actors to be heard, it is a form of censorship and entirely against the principle of free speech.

This emerging form of censorship, censorship 2.0 as it may be called, is unlike previous forms we've seen before. This time, it comes from a technical angle (data mining, network infrastructure) and also a mental angle (convinced of your will to free thought but you are

unknowingly being deceived). The mental angle comes from the purposeful diversion of dialogue in online exchanges, something most readers are not even aware of.

Scalability of the Bitcoin Network

With bitcoin, the focus of development has circled around solving the problem of how to make the payment system more scalable. At current, the system has a limitation of 7 transactions per second. Comparatively to MasterCard or VISA who do ~5000 transactions per second, the bitcoin network is clearly not meant to be a retail point-of-sale system. Developers who aim to increase the transaction rate can do so by lowering the requirements for transaction verification, ultimately increasing the number of queries going through the blockchain and therefore, the block size. If the block size is to increase to a point where running a full node (a computer with a full log of the bitcoin network transactions) was much more taxing on hardware, fewer miners would exist and therefore the mining process would tend to centralize. However, as Moore's Law has shown us, storage capacity may be able to keep pace with an ever-expanding blockchain file size, therefore mitigating the issues of scalability.

Anonymity as a Human Right

Bitcoin is often hyped as a potentially-anonymous method of making transactions, but how many people actually use it in this way? We can plainly see that privacy is a very weak point in the current developments within bitcoin. It is easy to trace spending patterns through the blockchain, IP addresses, and wallet reuse. However, the question remains, will anonymizing techniques be enhanced in the coming years, or will bitcoin development bend to the whim of policy makers and advocates of 'stopping criminal behavior'?

Many ill-informed users of technology will almost always hear the word anonymity and spout out the question "doesn't that allow terrorists to do terrible things?" "What about money laundering?" These are perspectives riddled with a fallacy of short-sightedness and reactive rather than proactive measures.

> *Those who surrender freedom for security will not have, nor do they deserve, either one.*
>
> *– Benjamin Franklin*

Technology as a Neutral Tool

Technology is a tool which extends the physical and mental capabilities of humans. Not limited to individual use, technologies also enable collective humanity to extend their ability to exert control over their natural world, thus extending their physical capabilities. A nuclear fission reactor allows collective humanity the ability to control an aspect of natural and extract tremendous amounts of energy from it. Technologies themselves do not facilitate, exclusively, actions which could be described as good or evil.

In terms of expanding individual capabilities, take for example a stone hammer. The hammer is an extension of the human body which allows its user to smash things and also build things. It is not the hammer which decides if it is going to bash in someone's skulls or bash in spikes for a new railroad. The user of the technology is always the one who decides how it is to be used, and therefore the user, not the technology itself should be the target of concern when it comes to potential to cause harm.

It is not the tool that allows a terrorist the capabilities to commit a crime. It is not the technology which is the final enabler of harming others. The enabler of these types of acts is the terrorist's mindset, which is what someone seeking to solve the problem should be focused on in the first place. Why would such an individual commit this crime? What are their motivations for doing so? The reactive measure is to remove and prevent access to the tools which assist them in committing the acts. The proactive measure is to study the individuals' motivations, understand them, and instill a constructive mindset in them. Reactionary measures are shortsighted and always limited in effectiveness. Proactive measures target the root of the problem and begin by seeking to understand the individual before judgments or actions are taken.

You Are Either Anonymous or Not

Anonymity is a binary concept. You either have anonymity or you do not, there is no middle ground. There is no such thing as being mostly anonymous. Anonymity is perfect privacy and in a world where the issues of privacy will continue to be debated and individual rights will continue to be strained, we should each strive for preserving the option of anonymity.

We believe anonymity is a human right because, at the moment we come into this world, we have no identification attached to us other than the sole characteristic of being human. We have no name, no title, no social security number. Indeed the only form of identification we have is that we are man, a position which should be preserved as an option.

Bitcoin allows individuals for the first time to control their financial lives outright and with that comes to opportunity to keep the details of one's financial life hidden from all friends, family, and third parties. If you can go anywhere in the world, carry with you your financial life, and retain perfect privacy, that is a very beautiful thing.

It is imperative that individuals and developers hold anonymity as a core principle within their beliefs, as anything other than anonymity, is not perfect privacy. That ability to retain financial anonymity is a human right and one which will become increasingly valuable as our lives merge with digital technologies which carry the potential for absolute identifiability or anonymity.

The Rise of Supranational Governance

If we were to assume that eventually, some sort of world government configuration will take the place of individual, fragmented sovereign states, what would it look like? Will it be a communion of our wisest political leaders under one flag and all people agreeing upon the laws which govern in a democratic vote? Will we all tune in right around suppertime to watch the 'president of the world' elections and root for the party with which we most closely relate to? Will we finally be among a utopian society where true democracy is the staple ideology?

Quite simply, this picture hardly paints an accurate picture of what we have coming towards us.

> *The next step in human evolution would be a race that could put their trust in each other, not in their rulers or politicians.*
>
> - *S.E. Sever, Writer*

More than anything, the average individual will do away with their notion of nationalism and adopt the ideology of a world citizen. Not confined to artificial borders or boundaries, these individuals will have the opportunity to experience unprecedented wealth accumulation. Unlike

any time before in history, they will be subversive to judicial taxation strategies due to the very nature of digital money which will continually offer alternatives for increased security, functionality, and anonymity – although it is quite likely these **payment systems will be under surveillance** to a degree previously unmatched.

Rise of Knowledge

Governing ability will continue to collectivize under those who are able to enforce economic compliance upon the largest collective of actors. However, knowledge as a commodity will see an increase in value previously unheard of. This is precisely because knowledge allows the creation of new wealth and the ability to rearrange matter in a more valuable form. Knowledge is more valuable than hard resources in the long-run because with knowledge you can create value and market your skills to gain financing. With financing you cannot necessarily gain more knowledge. A large quantity of money cannot grant you knowledge. To the degree in which knowledge production is not financed, the value of financing declines and value of knowledge production increases. Google's rise to one of the largest global market-capitalizations, surpassing Exxon-Mobile is anecdotal evidence that knowledge capital is outpacing hard capital.

> *As mankind has progressed through hunting, agriculture, industry, then now software, the proportion of mankind's time devoted to production with hard resources and manual labor has decreased. This allowed more time for man to pursue the creation of knowledge. Knowledge's proportion of GDP measured in units of the relative value of time expended (instead of money spent) is inexorably increasing. The "relative value of time expended" is the knowledge value, thus knowledge production becomes a greater proportion of value in the GDP.*
>
> - *Demise of Finance, Rise of Knowledge (CoolPage, 2013)*

Breaking of Orwell's Dictum

We live in an age where everything is quickening. We hold the world's information within an arm's reach and we expect minimal delay between any type of transaction or query. Moving

forward, the **velocity of money** as well will reach escape velocity, unleashed from its analog roots as it assumes a new *digital* makeup.

What is less commonly talked about is the idea that our collective recollection of history is also quickening. More than ever, our past is stored on a global mind, a database of events unfolded: the internet. The parties which control these channels of information are in a place of extreme power, as they are able oversee, to a large degree, historical records.

Bitcoin can serve as a challenge to this consolidation of power because it provides a distributed publishing network which can store historical records for as long as the integrity of the blockchain remains intact. In fact, many users are already uploading files of all kinds and storing them in the bitcoin blockchain. After an analysis of the blockchain, researcher Ken Sherriff found surprises such as a **tribute to Nelson Mandela**, the bitcoin whitepaper, and a large volume of 'mysterious encrypted data'. (Sherriff, 2014)

Blockchain networks and autonomous corporations hold the potential to break **Orwell's dictum** of '*Who controls the past controls the future; who controls the present controls the past.*'

> *We are now approaching the state of Orwell's dictum, perfect dictum, that 'he who controls the present controls the past'. He who controls the Internet servers controls the intellectual record of mankind, and by controlling that, controls our perception of who we are, and by controlling that, controls what laws and regulations we make in society.*
>
> - *Julian Assange, WikiLeaks*

Blockchain technologies are already being used as publishing mechanisms and will continue to be as we increase our understanding and the complexity of these distributed databases. Rather than history being decided by the entities which control the present, we now have a potentially-unownable digital medium to record history.

Conclusion

Bitcoin is disruption of our monetary system through technological innovation, but implications of its arrival will not be limited to the financial realm. In the long run, there are few reasons why the value of bitcoin will not appreciate and its functionality not be adopted other than if a security flaw is found within the source code. After extensive review from security researchers from around the world and attempts to crack the technology from the most talented hackers, no such flaw has been found.

A direct relationship exists between the value of bitcoin and the number of people who accept it and understand its uses. Therefore, the network effect assumes that as more people come to learn the benefits of using bitcoin over paper money, and more people exchange and purchase using cryptocurrencies, their value will appreciate.

There will come a day when we look back at this time with supremacy on our reliance of money transmitters and central banking, unmistakably evolved from a distributed ledger of information and finance. Bitcoin may not provide the definitive answer or lone currency to make this transition happen, but it provides the blueprints for something far more complex in nature, and a cashless future which is approaching whether individuals are prepared or not. Bitcoin is quite astonishingly the best and cleanest payment mechanism the world has ever seen.

Our current monetary system is built upon the notion of a confidence game. In a world where the capacity to defend from and exert violence is shifting to the cybereconomy, the powers that be can no longer can sustain the US dollar as the staple of the world economy. Combined with the fact that bitcoin is nationally untaxable – the lifeblood of governments cannot be gleaned from a cryptographic money system - and we are left with the undeniable conclusion that bitcoin, and the larger trend of decentralization, will bring an end to the nation state configuration.

An evolution into a digital economy will ignite possibilities across the globe like never before. Micropayments sent across the globe with no time delay, financial mobility for citizens who would previously have their livelihood tied to a government organization, and the potential for

accessibility in regions which do not have the banking infrastructure of the western world paint a picture of a vastly different and swiftly approaching tomorrow. We foresee a sizable increase in the velocity of money made possible by the frictionless payment system bitcoin outlines.

A great step forward lies in the opportunity to base a future economy on the mathematical laws of the universe, outside the grasp of human error and manipulation. At its fullest potential, bitcoin has the ability to serve as a legitimate currency commodity, store of value, and system upon which increasingly complex value-transfer protocols can be built. As a project which calls out to be explored and adopted, bitcoin remains the most important development of the early 21st century.

To think how far the world wide web has come since not only its introduction, but the advent of web programming languages just a decade ago, and you get an idea of how disruptive blockchain technology will be on the way we store, distribute, and compile information. These networks will not be hosted by a centralized server or corporation operating in the physical dimension, but rather a digital grid maintained by collectivized computing power. Machines around the world will syndicate to form the foundation of networks which have the ability to revolutionize a great number of industries and provide vast stores of verifiable information near instantaneously.

These networks will largely have no need for human intervention and in doing so will form an autonomous agent outside the control of a single source. Governments, because of their hierarchical nature, will have a difficult time counteracting the effects of these decentralized self-governing forces. These independent agents will bring about remarkable innovation, but also be open to seriously potent and nefarious intentions. Regulations and man-made laws will have minimal effectiveness on counteracting both the adoption and subsequent effects of these creations, as focus will shift increasingly toward greater allocation of resources to developing internet technology for military and economic purposes. Therefore, it is essential we experiment, understand, and inform people of the consequences and benefits bitcoin technology brings if we are to minimize intentions targeted towards greed and fear in an effort to create a future which serves the populous of the planet for generations to come.

About the Author

As the man behind Diginomics, Travis Patron is an author, speaker, and researcher into bitcoin and the emerging digital economy in ways which strengthen individual rights to privatize and grow their economic livelihood. Studying at the University of Saskatchewan, Travis holds degrees in both economic relations and commerce while continuing to pursue self-education in the areas of computing science. He is also an advisory board member of the LifeBoat Foundation, a nonprofit organization dedicated to encouraging scientific advancements while combating existential threats.

Travis believes as the rate of technological complexity continues to increase, so too will the difficulty of problems faced. Fortunately, he says, we are operating in the most ambitious and informed society to date.

At Diginomics, we believe in the creation of a society governed by the science of mathematics and information systems, and dedicate our work to realizing the most painless and beneficial transition to such an establishment. With the advent of the information age, very smart individuals will have the opportunity to transcend governing forces which have held back human potential since the very beginning of recorded history. These early individuals will be known as *sovereign individuals* and will be governed by number itself.

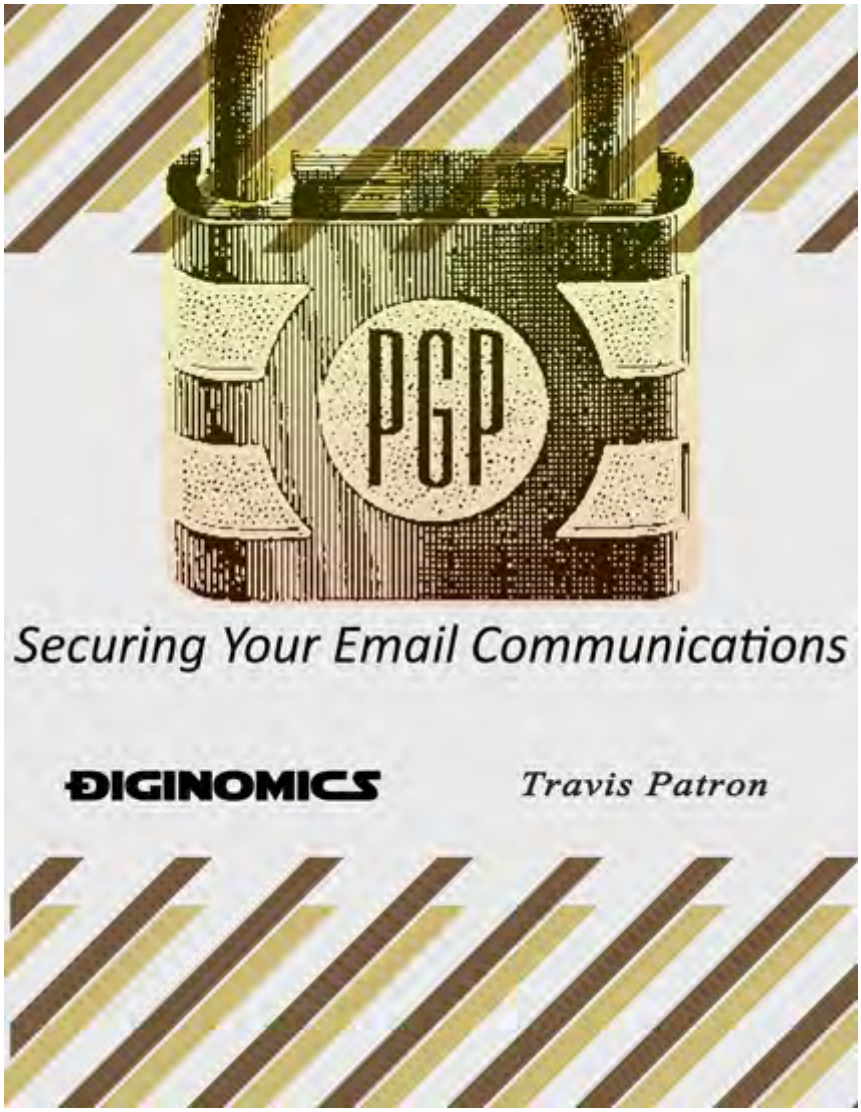
Publication Contributors:

Wallace Wood

Albert Szmigielski

Bonus Content

If you enjoyed this book, we invite you to use a special coupon code for our follow-up publication:



Use the coupon code '**HONEYBADGER**' and receive **20% off** *PGP: Securing Your Email Communications*.

Learn More

Join the Community

To learn more about the transition to an age of **diginomics**, and how you can get involved in this prescient community of entrepreneurs, software developers, computer scientists, writers, researchers, and economists committed to building a better society …

Join Now

And share this publication so that others may join our ranks!

Bibliography

Alberto Chaia, T. G. (2010, March). *Counting the world's unbanked*. Retrieved January 29, 2014, from McKinsey: http://www.mckinsey.com/insights/financial_services/counting_the_worlds_unbanked

Berezow, A. (2013, 12 24). *Bitcoin Meets Google Trends and Wikipedia*. Retrieved March 3, 2014, from Forbes: http://www.forbes.com/sites/alexberezow/2013/12/24/bitcoin-meets-google-trends-and-wi/

Bitcoin Wiki. (2012, August 4). *Brainwallet*. Retrieved February 27, 2014, from Bitcoin Wiki: https://en.bitcoin.it/wiki/Brainwallet

Bitcoin Wiki. (2014, March 3). *Controlled supply*. Retrieved March 3, 2014, from Bitcoin Wiki: https://en.bitcoin.it/wiki/Controlled_supply

Bitcoin.org. (2009). *Innovation in payment systems*. Retrieved March 1, 2014, from Bitcoin.org: https://bitcoin.org/en/innovation

Blockchain.info. (2014, January 31). *Hashrate Distribution*. Retrieved January 31, 2014, from Blockchain.info: https://blockchain.info/pools

Blockchain.info. (2014, January 31). *Market Price (USD)*. Retrieved January 31, 2014, from Blockchain.info: https://blockchain.info/charts/market-price

BlockExplorer. (2010). *Block 0 – Bitcoin Block Explorer*. Retrieved December 2013, from BlockExplorer: http://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.* W. W. Norton & Company.

BTC Geek. (2013, October 13). *Dawn of Autonomous Corporations, Powered by Bitcoin*. Retrieved March 9, 2014, from BTC Geek: http://btcgeek.com/dawn-of-autonomous-corporations/

CoinDesk. (2013, November 26). *Who is Satoshi Nakamoto?* Retrieved December 20, 2013, from CoinDesk: http://www.coindesk.com/information/who-is-satoshi-nakamoto/

Computer Hope. (2014, October 1). *Who invented the internet?* Retrieved from Computer Hope: http://www.computerhope.com/issues/ch001016.htm

CoolPage. (2013). Retrieved from http://www.coolpage.com/commentary/economic/shelby/Demise%20of%20Finance,%20Rise%20of%20Knowledge.html

Dickherber, R. (2013, May 16). *Bitcoin for Entrepreneurs*. Retrieved December 2013, from Astrohacker: http://astrohacker.com/text/bitcoin-for-entrepreneurs/

Dickherber, R. (2013, May 16). *Bitcoin for Entrepreneurs*. Retrieved November 30, 2013, from Astrohacker: http://astrohacker.com/text/bitcoin-for-entrepreneurs/

Dickherber, R. (2013, June 1). *People Who Look Like Criminals But Are Not*. Retrieved December 2013, from Astrohacker: http://astrohacker.com/text/people-who-look-like-criminals-but-are-not/

Dourado, E. (2014, January 20). *Bitcoin Volatility is Down Over the Last Three Years. Here's the Chart that Proves It*. Retrieved March 2, 2014, from Eli Dourado: http://elidourado.com/blog/bitcoin-volatility/

Ducky1. (2013, December 30). *Monthly average USD/bitcoin price & trend*. Retrieved March 4, 2014, from bitcointalk.org: https://bitcointalk.org/index.php?topic=322058.msg4227238#msg4227238

Emmett, R. B. (1946). *The Chicago Tradition in Economics.* Chicago: Routledge.

Encyclopedia Britannica. (2012, 10 22). *Credit Card*. Retrieved October 1, 2014, from Encyclopedia Britannica: http://www.britannica.com/EBchecked/topic/142321/credit-card

Ethereum. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.* Ethereum.

Falkvinge, R. (2014, March). *Nothing New Under the Sun, Bitcoin Edition*. Retrieved February 2015, from Falkvinge on Infopolicy: http://falkvinge.net/2014/03/05/nothing-new-under-the-sun-bitcoin-edition/

Federal Reserve Board. (2014). *Bitcoin: Technical Background and Data Analysis.* Washington, D.C.

Felton, N. (2010, 12 23). Retrieved 10 11, 2014, from New York Times: http://www.nytimes.com/2008/02/10/opinion/10cox.html?ex=1360299600&en=9ef4be7de32e4b53&ei=5090&partner=rssuserland&emc=rss&pagewanted=all

Gates, W. H. (1999). *Business @ the Speed of Thought: Succeeding in the Digital Economy.* New York: Warner Books Inc.

High Tech Strategies, Inc. (2011). *Ten Reasons High-Tech Companies Fail*. Retrieved December 15, 2013, from High Tech Strategies: http://www.hightechstrategies.com/10_reasons.html

Investor Glossary. (2013). *Greater Fool Theory*. Retrieved March 03, 2014, from Investor Glossary: http://www.investorglossary.com/greater-fool-theory.htm

Johnson, S. (2014, January 2). *The 'Internet of Things' could be the next industrial revolution*. Retrieved March 10, 2014, from San Jose Mercury News: http://www.mercurynews.com/business/ci_24835528/internet-things-could-be-next-industrial-revolution

Kelly, K. (1998). *New Rules for the New Economy: 10 Radical Strategies for a Connected World.* New York: Penguin Group.

Kurzweil, R. (2000). *The Age of Spiritual Machines.* New York: Penguin Publishers.

Learn Cryptography. (2013). *51% Attack*. Retrieved January 31, 2014, from Learn Cryptography: http://learncryptography.com/51-attack/

Learn Cryptography. (n.d.). *Bitcoin Addresses*. Retrieved 10 4, 2014, from http://learncryptography.com/bitcoin-addresses/

Lerner, S. (2013, April 17). *The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius*. Retrieved December 17, 2013, from Bitslog: http://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/

Ludwig, S. (2013, February 13). *Y Combinator-backed Coinbase now selling over $1M Bitcoins per month*. Retrieved December 18, 2013, from VentureBeat: http://venturebeat.com/2013/02/08/coinbase-bitcoin/

MacKenzie, A. C. (2011, October 24). *Revealed – the capitalist network that runs the world*. Retrieved January 29, 2014, from New Scientist: http://www.newscientist.com/article/mg21228354.500-revealed--the-capitalist-network-that-runs-the-world.html#.Uug4shAo603

Moore, G. A. (1999). *Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customers.* HarperBusiness.

Murck, P. (2013, July 31). *The True Value of Bitcoin*. Retrieved March 7, 2014, from Cato-Unbound: http://www.cato-unbound.org/2013/07/31/patrick-murck/true-value-bitcoin

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Bitcoin.org.

Newman, A. (2013, May 22). *World Bank Insider Blows Whistle on Corruption, Federal Reserve*. Retrieved January 29, 2014, from The New American: http://www.thenewamerican.com/economy/economics/item/15473-world-bank-insider-blows-whistle-on-corruption-federal-reserve

P2P Foundation. (2014, March 6). *Satoshi Nakamoto's Page*. Retrieved March 7, 2014, from P2P Foundation: http://p2pfoundation.ning.com/profile/SatoshiNakamoto

Palley, T. (2006, November 26). *Milton Friedman: The Great Conservative Partisan*. Retrieved March 7, 2014, from Thomas Palley: http://www.thomaspalley.com/?p=59

Penenberg, A. (2011, October 11). *The Bitcoin Crypto-Currency Mystery Reopened*. Retrieved December 20, 2013, from Fast Company: http://www.fastcompany.com/1785445/bitcoin-crypto-currency-mystery-reopened

Rizzo, P. (2014, February 14). *Overstock to Launch New Rewards Scheme for Bitcoin Buyers*. Retrieved February 22, 2014, from CoinDesk: http://www.coindesk.com/overstock-launch-new-rewards-program-bitcoin-buyers/

Salmon, F. (2013, November 27). *The Bitcoin Bubble and the Future of Currency*. Retrieved March 3, 2014, from Medium: https://medium.com/money-banking/2b5ef79482cb

Sawyer, M. (2013, February 26). *The Beginners Guide To Bitcoin – Everything You Need To Know*. Retrieved December 20, 2013, from Monetarism: http://www.monetarism.co.uk/the-beginners-guide-to-bitcoin-everything-you-need-to-know/

Sherriff, K. (2014, February). *Hidden surprises in the Bitcoin blockchain and how they are stored*. Retrieved January 14, 2015, from Ken Sherriff's Blog: http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html

Simontie, T. (2011, May 25). *What Bitcoin Is, and Why It Matters*. Retrieved March 3, 2014, from Technology Review: http://www.technologyreview.com/news/424091/what-bitcoin-is-and-why-it-matters/page/2/

Sorrells, K. (2013). *Intercultural communication: globalization and social justice.* Thousand Oaks, Calif.: SAGE.

Surda, P. (2011). *Economics of Bitcoin.*

Taleb, N. (2012). *Antifragile: Things That Gain from Disorder.* Random House Publishing Group.

The Economist. (2013, April 27). *In dollars they trust*. Retrieved March 2, 2014, from The Economist: http://www.economist.com/news/finance-and-economics/21576665-grubby-greenbacks-dear-credit-full-shops-and-empty-factories-dollars-they

The Economist. (2014, 03 12). *Happy birthday world wide web*. Retrieved 01 11, 2015, from The Economist: http://www.economist.com/blogs/graphicdetail/2014/03/daily-chart-7

The Opte Project. (2006). *Internet Map.* The Opte Project.

Trivia. (2011, June 17). *The Network Effect*. Retrieved 10 28, 2014, from Trivia: http://prasoondiwakar.com/wordpress/tag/trivia/

Vaughan, L. (2014, February 28). *Gold Fix Study Shows Signs of Decade of Bank Manipulation*. Retrieved December 26, 2014, from Bloomberg: http://www.bloomberg.com/news/2014-02-28/gold-fix-study-shows-signs-of-decade-of-bank-manipulation.html

W3C Technology and Science Domain. (2001, August 31). *Micropayments Overview*. Retrieved March 2, 2014, from W3C: http://www.w3.org/ECommerce/Micropayments/

Wells, D. A. (1889). *Recent Economic Changes and Their Effect on Production and Distribution of Wealth and Well-Being of Society.* Cambridge, Massachusetts: Harvard Divinity School.

Wilhelm, A. (2013, September 10). *Inside Bitcoin, The Programmable Currency For Our Digital Future*. Retrieved February 27, 2014, from TechCrunch: http://techcrunch.com/2013/09/10/disrupt-sf-13-bitcoin-panel/

World Bank. (2012, April 19). *Who are the Unbanked?* Retrieved March 2, 2014, from World Bank: http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/0,,contentMDK:23174014~pagePK:210058~piPK:210062~theSitePK:282885,00.html

Figures