CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

Department of Economics

D I P L O M A T H E S I S

BITCOIN — THE CRYPTOCURRENCY MEDIUM OF EXCHANGE, PURCHASING POWER, AND LONGTERM STORE OF VALUE

Author: Bc. Dominik VLASÁK, BSc

Supervisor: Ing. Petr PROCHÁZKA, MSc, Ph.D.

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Dominik Vlasák, BSc

Economics and Management

Thesis title

Bitcoin — The Cryptocurrency Medium of Exchange, Purchasing Power, and Longterm Store of Value

---

Objectives of thesis

There are three main aims of the diploma thesis. The literature review includes gaining an in-depth understanding of currency in general as well as its history; evaluating and understanding Bitcoin – both the underlying technology and the purchase, storage, and transaction ability of bitcoins. Lastly, bitcoins are examined from a medium of exchange, longterm storage of wealth, and purchasing power point of view. Ultimately, the diploma thesis is to be used as a tool to help the reader decide how to purchase and safely store bitcoin, as well as a guide to the basic minimum amount of bitcoin to acquire.

Methodology

The methods used to carry out the theoretical part of the diploma thesis include a qualitative examination of currencies and the perception of value, a quantitative evaluation of bitcoin against other top fiat currencies, linear regression analysis to identify influences in the drivers of the price of bitcoin as well as their correlation, evaluation of bitcoin volatility, and the monetary economics of bitcoin using the general equilibrium theory to define a theoretical equilibrium price for one bitcoin. Strategic analyses such as SWOT and PESTLE are used as well as the demand-side economies of scale, using Metcalfe's law.

The proposed extent of the thesis

60 pages

Keywords

Bitcoin, blockchain economics, cryptocurrencies, virtual money, digital asset

---

Recommended information sources

Antonopoulos, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 1st ed., Sebastopol, CA: O'Reilly Media, 2014. 298 pages. ISBN: 1449374042.

Burniske, Chris, and Jack Tatar. Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond. 1st ed., New York, NY: McGraw-Hill Education, 2017. 368 pages. ISBN: 1260026671.

Frisby, Dominic. Bitcoin: The Future of Money? London: Unbound, 2014. 304 pages. ISBN: 1783520779.

Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. (PDF). [cit. 2018-03-05]. Available at: https://bitcoin.org/bitcoin.pdf.

Popper, Nathaniel. Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money. New York, NY: Harper Paperbacks, 2015. 432 pages. ISBN: 006236250X.

Vigna, Paul, and Michael J. Casey. The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic Order. New York, NY: Picador/St. Martin's Press, 2016. 384 pages. ISBN: 1250081556.

Expected date of thesis defence

2017/18 SS – FEM

The Diploma Thesis Supervisor

Ing. Petr Procházka, Ph.D., MSc

Supervising department

Department of Economics

Electronic approval: 13. 3. 2018

prof. Ing. Miroslav Svatoš, CSc.

Head of department

Electronic approval: 13. 3. 2018

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 19. 03. 2018

Declaration:

I declare that I myself have worked on my diploma thesis titled "Bitcoin — The Cryptocurrency Medium of Exchange, Purchasing Power, and Longterm Store of Value" and that I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break the copyrights of any person.

In Prague on …… ……..

Bc. Dominik Vlasák, BSc

Acknowledgement

I would like to thank my mom, my little sister, my grandfather, and my grandmother for their never-ending love and support throughout my many years at CULS in Prague. Additionally, I would like to thank Ing. Jana Donátová and Ing. Peter Procházka, MSc, Ph.D. for their advice and support during my work on this diploma thesis.

Bitcoin — The Cryptocurrency Medium of Exchange, Purchasing Power, and Longterm Store of Value

Abstract

The diploma thesis looks at Bitcoin and bitcoins; the world's first mainstream digital and decentralized form of cryptocurrency. Money and Bitcoin are analyzed from medium of exchange, purchasing power, and longterm store of value perspectives. The history, origin, use, storage, acceptance, transaction abilities and costs, market dominance, valuation, volatility, and wealth distribution of currencies and bitcoins are examined. Alternatives such as gold or other currencies are also taken into consideration. The demand-side economies of scale are explained using Metcalfe's Law and a multiple regression analysis is performed, helping explain the rise in bitcoin's market price due to the network affect. Although not extraordinarily cost effective, bitcoin mining profitability is calculated with several scenarios, identifying possible use cases where mining is justifiable, even in the year 2018. As a result, the thesis includes hundreds of hours worth of research condensed into a general understanding of bitcoin and its economics, providing the reader with knowledge to make his or her own informed decision about potential involvement with the cryptocurrency.

Keywords: Bitcoin, blockchain economics, cryptocurrencies, virtual money, digital asset

Bitcoin — kryptoměnová směna, kupní síla a dlouhodobý uchovatel hodnoty

Abstrakt

Tato diplomová práce se zabývá Bitcoinem a bitcoiny; první světová decentralizovaná digitální forma kryptoměny. Peníze a Bitcoin jsou analyzovány skrze perspektivy výměny, kupní síly a dlouhodobého úložiště hodnoty. Analyzuje historii, původ, využití, skladování, přijetí, transakční schopnosti a náklady, dominantní postavení na trhu, ocenění, volatilitu a rozdělení hodnoty měn a bitcoinů. Také jsou brány v úvahu alternativy, jako je zlato nebo jiné měny. Úspory na straně poptávky jsou vysvětleny pomocí Metcalfova zákona a provádí se několikanásobnou regresní analýzou, která pomáhá vysvětlit nárůst tržních cen bitcoinu v důsledku síťového vlivu. Ačkoli to není mimořádně ziskové, ziskovost těžby se vypočítá pomocí několika scénářů, přičemž lze identifikovat případné případy použití, kdy je těžba opodstatněná, dokonce i v roce 2018. Výsledkem práce jsou stovky hodin výzkumu, které se mají za cíl obecné pochopení bitcoinu a poskytují čtenáři znalosti potřebné k utvoření vlastního informovaného rozhodnutí o potenciálním zapojení se do světa kryptoměn.

Klíčová slova: Bitcoin, blockchain ekonomika, kryptoměny, virtuální peníze, digitální rozvaha

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ASIC	Application-Specific Integrated Circuit
BTC	Informal, yet most common currency code for one unit of bitcoin
BTWTY	Currency code for the cryptocurrency Bit20
BOJ	Bank of Japan
CBOE	Chicago Board Options Exchange
CPI	Consumer Price Index
CPU	Central Processing Unit
ECB	European Central Bank
ETV	Estimated Total Value
GPU	Graphics Processing Unit
HODL	Holding onto bitcoin ["hold on for dear life"]
ISO	International Standard Organization
JPY	Japanese yen
kWh	Kilowatt-hour
MB	Megabyte
MXN	Mexican peso
OTC	Over-The-Counter [trading]
POS	Point-Of-Sale
P2P	Person To Person [Peer-To-Peer]
UTC	Coordinated Universal Time
VIX	Volatility Index
XAG	Currency code for silver
XAU	Currency code for gold
XBT	Less common (pending) official currency code for one unit of bitcoin

1. Introduction

Since its origin in 2008, bitcoin has been the talk around the world. From investors that swear by it, predicting that it will reach anywhere between $100,000 to $1,000,000 USD within the next couple of years; to non-believers of bitcoin, who say that it is a valueless bubble that is going to pop at any moment. With the proper data and reasoning, it is possible to make arguments for both sides, although no one is to say with 100% confidence what exactly the future of bitcoin involves. Ignoring the fact that there are hundreds or thousands of variables that influence the price of bitcoin, the truth of the matter is that bitcoin's price can go either way.

Bitcoin has puzzled economists, fascinated computer geniuses, and attracted the attention and interest of the regular public all over the world. The last decade has been the revolutionary birth of bitcoin and an endless number of other digital currencies, much like the birth of the Internet a few decades ago. If someone was told all the future possibilities of the Internet 30 years ago, nobody would believe them. The possibilities and applications of cryptocurrencies and the blockchain technology behind them have the possibility to make great change on this planet, revolutionizing the way that humans interact, the way the world's economies transact, and taking away monetary policy power from banking institutions, governments, central banks — putting the power of money back into the hands of the owners.

This is why Bitcoin is an excellent cryptocurrency medium of exchange, purchasing power, and longterm store of wealth.

2. Objectives and Methodology

2.1. Objectives

There are three main aims of the diploma thesis. The literature review includes gaining an in-depth understanding of currency in general as well as its history; evaluating and understanding Bitcoin – both the underlying technology and the purchase, storage, and transaction ability of bitcoins. Lastly, bitcoins are examined from a medium of exchange, longterm storage of wealth, and purchasing power point of view. Ultimately, the diploma thesis is to be used as a tool to help the reader decide how to purchase and safely store bitcoin, as well as a guide to the basic minimum amount of bitcoin to acquire.

2.2. Methodology

The methods used to carry out the theoretical part of the diploma thesis include a qualitative examination of currencies and the perception of value, a quantitative evaluation of bitcoin against other top fiat currencies, linear regression analysis to identify influences in the drivers of the price of bitcoin as well as their correlation, evaluation of bitcoin volatility, and the monetary economics of bitcoin using the general equilibrium theory to define a theoretical equilibrium price for one bitcoin. Strategic analyses such as SWOT and PESTLE are used as well as the demand-side economies of scale, using Metcalfe's law.

3. Literature Review

3.1. What is Money?

Almost all humans, all over the world, use money. It is the underlying reason of what motivates men and women around the world to work, as well as need and desire products, services, and other assets. Like a well-lubricated engine, money is what enables economies to function and prosper. [1]

Money is defined as having three basic characteristics and functions:

a) Medium of exchange
b) Unit of account
c) Store of value

In terms of a medium of exchange, money serves as the facilitator for a transaction between two or more parties during the barter of goods and services. [2] Simply stated, money exists in the place of a traditional barter system to reduce the complexity and cost associated with exchanges. Money not only enables anyone that has it to participate equally in the market, but it also enables more transactions to be executed since the amount of parties with needs and desires for products and services is potentially infinite. This differs from traditional ancient bartering where merchants and consumers brought coveted and/or surplus goods, gathered at marketplaces, and tried to find someone that had and wanted a good that another person had and wanted, and vice versa; extremely limiting trade. [3]

Second, unit of account serves as a way to measure the value of money. Unit of account is addable, divisible, and recognizable by all parties partaking in the exchange of goods and services within a particular market, and is determinant for describing the universal price of a good or service. Similar to medium of exchange, unit of account allows for more transactions by enabling merchants and consumers to “think” in the same sense, in a common definition of value. [2]

Lastly, store of value is defined as an object that holds value over time. Money is different from other stores of value such as land, structures, works of art, or precious metals in that it is readily exchangeable for other goods and services, known as fungibility.

Not only that, it is relatively straightforward and inexpensive to stockpile. The decrease in value of a currency over a period of time is commonly known as inflation, and the opposite is referred to as deflation. [2]

3.1.1. The History of Money

Long before bartering became a part of human life, about 3,000 years ago; almost all men and women were farmers, hunters, or gatherers. One human created enough food for about one human. As agricultural practices and technology gradually developed, it allowed one person to create enough food for several, tens, and recently even hundreds of humans at once. This not only supported the trade of food and livestock, but it completely revolutionized the labor market — those individuals no longer involved in creating the food supply were able to concentrate on other, more specialized lines of work. This led to a surplus of goods and services and sparked bartering, which ultimately created demand for a simple and efficient way of exchanging goods and services: currency. [5]

3.1.2. The Origin of Currency (Ledgers)

Although it is largely debated as what the "first" currency was, the first large-scale currency minting process was created by King Alyattes in Lydia, what is known as present day Turkey, around the year 600 BCE. Coins were the standard for several hundred years, as international trade began to flourish. In 1661, banknotes were first printed in Sweden and in contrast with coins; allowed for much higher denominations as well as greater efficiency and convenience of storage and transport. The first credit card was not introduced until the year 1946, in New York City, and it provided customers with a way of acquiring goods and services without the need of carrying any physical currency by promising to pay at a later date, known as a deferred payment. The evolution of money progressed even further in 2008, when contactless payment was first introduced in the United Kingdom. [5]

3.1.3. Types of Currency

Even though money is typically referred to as currency, it is important to remember that not all money is currency, yet all (recognized) currency is money. As defined by the largest financial education website in the world, [6] currency is a "liquid asset used in the settlement of debts that functions based on the general acceptance of its value within an

economy. The value of money is not necessarily derived from the materials used to produce the note or coin. Instead, the value is derived from the amount shown on its face, partnered with the public's willingness to support the displayed value." [4]

There are two basic types of currency, commodity money and fiat money. Commodity money is defined as an item that has intrinsic value. This means that even if the commodity were to no longer be used as money, it would still have value in and of itself. The classic examples of commodity money are precious metals, such as gold and silver. The opposite is true of fiat money. Fiats are currencies established by governments and central banks and have no intrinsic value of their own. This means that if the government and people lost trust in the fiat currency, banknotes would become worthless pieces of paper with numbers on them. Presently, fiat currencies are used all over the world. [7]

As of the beginning of 2018, there are 180 currencies in the world, as officially recognized by the United Nations. The United States dollar is the official legal tender in only nine countries, yet it is accepted in another roughly 20 countries and areas all over the world. There are 22 countries in the world that use their own form of the "dollar" such as the Australian dollar, the Canadian dollar, the Singapore dollar, and the now-defunct Zimbabwe dollar. Of the current 28 European Union member states, only 19 countries have become a part of the Eurozone by adopting the euro. [9]

3.1.4. How Money is Stored and Spent

Apart from money being stored in the form of currency in physical wallets and safes, commonly referred to as cash; currency is most commonly stored in banking institutions in the form of a checking account, savings account, or both. There is no debate that currency is the most widely accepted medium of exchange in economies all over the world. However, currency is not the only way to purchase goods and services as many establishments and institutions accept personal checks and debit cards. Although these forms of payments are not considered fiat currency, they are used in a similar way as currency because they are used on demand by depositors to settle debts for transactions with merchants. These stores of currency are known as demand deposits, or balances of currency held within bank accounts. [7]

Some securities offer better protection from purchasing power risk than others. Debt securities and investments are known as promised, fixed rates of returns and are the most susceptible to inflation and purchasing power risk. It is crucial that the rate of return on an investment is at least equal or preferably greater than the rate of inflation, so that the initial nest egg investment does not decrease year by year. [14]

3.2. How Money is Used

Some individuals and businesses utilize money and banking institutions without even knowing or questioning how exactly they function, or whether there is an alternative, let alone whether there is a better alternative. They use typical money and banks due to convenience, availability, and public popularity. [7]

3.2.1. Money Acceptance

It is becoming much more common for many establishments and institutions around the globe to accept personal checks, debit cards, credit cards, and mobile payments as a regular mean of settling a debt or securing a deferred payment in order to complete the transaction of a good or service. Not only must merchants invest in hardware and software to support the various types of payment methods, they must also deal with several different vendors and companies for each payment method. Merchants must constantly adapt to new technologies and regulations — and must be wary of counterfeiting and fraud. While offering various types of payment methods may allow for the increase of the number of transactions of goods and services on the market, it also creates complications within the economy and causes merchants to give up a share of their profit. [7]

3.2.2. Types of Transactions

As shown in Figure 1 on the following page, there are three main types of retail payments. Point-of-sale (POS) payments are made by consumers inside physical stores. Non point-of-sale payments include the payments from consumers to businesses (outside stores, mostly telephone and the Internet), from businesses or governments to consumers (commonly wages or benefits), and consumers to consumers (peer-to-peer). Lastly, the final use case includes payments from business to business (except in the case of large-dollar amounts). [10]

Figure 1. Major Types of Retail Payments (Use Cases)

Payments by consumers for in-store purchases (point-of-sale)
All other payments to or from consumers (non-point-of-sale) • Purchases by consumers outside of stores (mail, telephone, or Internet) • Bill payments by consumers (one-time and recurring) • Person-to-person payments (P2P) • Payments to consumers from businesses or government agencies, such as wages and benefits
Payments from businesses to businesses (other than large-dollar)

Source: Federal Reserve Bank of Kansas City (2012) [10]

Three main categories can be distinguished among payment instruments from Figure 1 on the preceding page — paper-based, electronic-based, and hybrid payments. Paper-based payments include cash and traditional checks. Electronic payments neither start nor end in paper form and are entirely processed by electronic means. Electronic payments include payment cards such as prepaid, debit, credit, and charge cards — as well as direct transfers between bank accounts. The last instrument of payment is a hybrid of the previous two; the payment begins in paper form but is largely processed by electronic means. Paper-electronic hybrid payments are possible in the United States with the enactment of "Check 21" to make it possible for paper checks to be instantly deposited into one's bank account, without the need of physically depositing the check at the bank. [10]

3.2.3. Share of Transaction Types

As shown on the next page in Table 1, the popularity of point-of-sale payment types is listed for four selected countries including Australia, Belgium, the Netherlands, and Norway. While cash dominates the transaction shares for the first three countries and PIN debit card takes second place, the opposite is true for Norway, where less than one-fourth of all transactions are facilitated by cash. In third place, payment by credit card is even less popular, ranging from being used in one-tenth of all transactions to being used less than 1% in some countries, such as the Netherlands. Even less trusted than credit cards

are prepaid cards, where in some countries such as Australia and Norway, there is no data collected. [10]

Table 1. Transaction Shares for Major Payment Methods (Percent)

Payment Method	Australia	Belgium	Netherlands	Norway
Cash	79.1	81.3	85.5	24.0
PIN Debit Card	10.9	14.8	12.9	67.8
Credit Card	10.0	1.0	0.6	8.2
Prepaid Card	—	2.9	1.1	—
TOTAL	100.0	100.0	100.0	100.0

Source: Federal Reserve Bank of Kansas City (2012) [10]

3.2.4. Payment Method Transaction Size

As proven by the Federal Reserve Bank of Kansas City, the average size of the transaction in point-of-sale varies depending on the specific payment method used in the selected countries. All amounts in Table 2 (below) are averages per transaction, measured in USD. [10]

Table 2. Average Transaction Size for Major Payment Methods (U.S. Dollars)

Payment Method	Australia[1]	Belgium	Netherlands	Norway
Cash	18.95	23.07	12.32	36.41
PIN Debit Card	72.81	65.42	57.96	61.86
Credit Card	67.82	130.04	151.32	104.98
Prepaid Card	—	6.76	3.56	—
Check	356.07	—	—	—

Source: Federal Reserve Bank of Kansas City (2012) [10]

While Australia trusts checks more than any other forms of payment, at an average transaction amount of $356.07 USD, other countries do not use checks enough to provide data. The Netherlands stand out with average transaction size for credit cards at $151.32 USD and average cash transaction size of only $12.32 USD. [10]

3.2.5. Transaction Fees

By far, the payment method with the lowest percentage total social cost of the transaction value is PIN debit card, roughly around 1% and 1.5% for the selected countries, as seen in Table 3 on the following page. In the study by the Federal Reserve Bank of

Kansas City, it states: “the social cost of a payment instrument is the sum of the resource costs incurred by all parties in transactions using that instrument.” [10]

Table 3. Total Social Costs per Unit of Transaction Value (Percent)

Payment Method	Australia	Belgium	Netherlands	Norway
Cash	3.21	3.03	3.20	5.63
PIN Debit Card	1.58	1.10	1.10	1.12
Credit Card	2.99	2.65	3.11	3.33
Prepaid Card	—	10.49	34.32	—
Check	2.29	—	—	—

Source: Federal Reserve Bank of Kansas City (2012) [10]

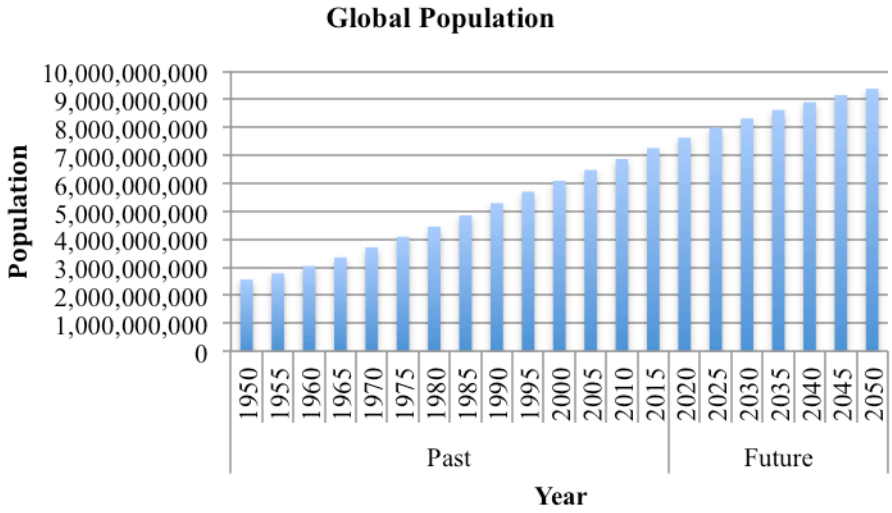
Yet again, the Netherlands stand out as more than one-third of the total transaction value is incurred by all parties dealing with prepaid cards, which suggests why other countries may be inclined to avoid that payment instrument. [10]

3.2.6. Global Population

In just the short time that it takes to read this sentence, 48 people have been brought onto this planet and 20 people have perished, leaving a net gain of 28 extra people. Every single day, approximately 381,000 human beings are born, roughly 157,000 pass away, resulting in a daily global population growth of 224,000 people. This equates to an annual worldwide population increase of 81,760,000 humans. [11]

At the time of this writing, the world population is approximately 7,460,000,000 humans. [12] It is estimated that the eight billion person milestone marker will be reached in the beginning of the year 2026. The nine billion human milestone is to be reached approximately in the summer of 2042. Finally, the 10 billion person jubilee milestone should be reached in 2062, as it is on track in Figure 2 on the next page. [11]

Figure 2. Global Population (1950-2050)



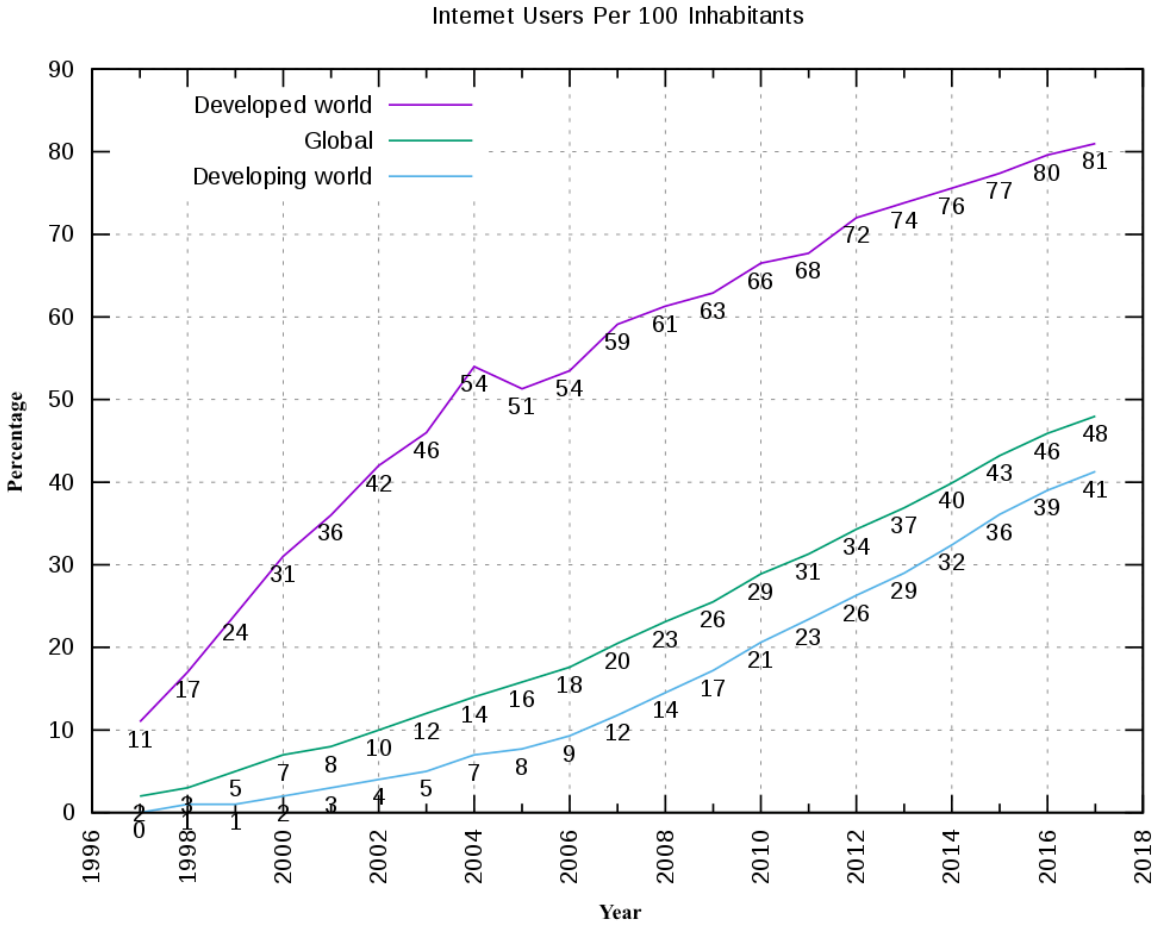
Source: United States Census Bureau (2018, own creation) [11]

The one billion human being population mark was reached in the year 1804, with the two billion mark coming in 1927, which took a total of 123 years. Before one billion people had been reached, it had taken the whole era of human history, more than 8,000 years total. The six billion milestone was reached on July 22, 1999, and the seven billion milestone was reached on March 12, 2012. The same billion extra people that took 123 years in 1927, now took less than 13 years in 2012. [11]

While the population is steadily increasing, the rate at which the population is growing is actually slightly decreasing. The current population growth rate is currently at about 1.14% annually. The global growth rate reached its peak in 1963, at approximately 2.19%. Therefore, the rate of population increase has almost halved since 1963, and it is projected to continue to decline in forthcoming years. Currently, it is projected the global population growth rate will be less than 1% by 2020, and will continue to decrease to less than 0.5% by 2050. Most recent calculations state that the world population will nearly stabilize at just above 10 billion persons around 2062. [11]

3.2.8. Global Internet Users

Figure 3. Share of Internet Users per 100 Inhabitants (1996-2018)



Source: International Telecommunications Union (2017, Jeff Ogden and Jim Scarborough, modified) [13]

From Figure 3 seen above, it is clear that the developed world is the leader among the percentage of Internet users per 100 inhabitants, with 81% of the population having adopted the Internet by the year 2017. The adoption rate of the developing world is about half of that, at about 41% of inhabitants having adopted the Internet. The global average is very closely mirrored with the developing world; only about 7% higher, with approximately 48% of the world's population connected to the Internet. This means that there are almost four billion people in the world currently without access to the Internet, something that many people in the developed and developing worlds may take for granted. [13]

3.4. The Purchasing Power of Money

Purchasing power is known as the value of a currency as defined in terms of the amount of goods or services that one unit of money can buy. Purchasing power is crucial due to the fact that inflation decreases the amount of goods or services one is able to purchase, all else being equal. Purchasing power is often measured in a traditional economic sense by comparing against a price index such as the Consumer Price Index (CPI) or measuring volatility. [14]

3.4.1. Total Global Currency in Circulation

Table 4. Currency Distribution of Over-the-Counter Foreign Exchange Turnover

Currency	2001		2004		2007		2010		2013		**2016**	
	Share	Rank	Share	Rank	Share	Rank	Share	Rank	Share	Rank	**Share**	**Rank**
USD	89.9	1	88.0	1	85.6	1	84.9	1	87.0	1	**87.6**	**1**
EUR	37.9	2	37.4	2	37.0	2	39.0	2	33.4	2	**31.4**	**2**
JPY	23.5	3	20.8	3	17.2	3	19.0	3	23.0	3	**21.6**	**3**
GBP	13.0	4	16.5	4	14.9	4	12.9	4	11.8	4	**12.8**	**4**
AUD	4.3	7	6.0	6	6.6	6	7.6	5	8.6	5	**6.9**	**5**
CAD	4.5	6	4.2	7	4.3	7	5.3	7	4.6	7	**5.1**	**6**
CHF	6.0	5	6.0	5	6.8	5	6.3	6	5.2	6	**4.8**	**7**
CNY[3]	0.0	35	0.1	29	0.5	20	0.9	17	2.2	9	**4.0**	**8**
SEK	2.5	8	2.2	8	2.7	9	2.2	9	1.8	11	**2.2**	**9**
NZD[3]	0.6	16	1.1	13	1.9	11	1.6	10	2.0	10	**2.1**	**10**
MXN[3]	0.8	14	1.1	12	1.3	12	1.3	14	2.5	8	**1.9**	**11**
SGD[3]	1.1	12	0.9	14	1.2	13	1.4	12	1.4	15	**1.8**	**12**
HKD[3]	2.2	9	1.8	9	2.7	8	2.4	8	1.4	13	**1.7**	**13**
NOK[3]	1.5	10	1.4	10	2.1	10	1.3	13	1.4	14	**1.7**	**14**
KRW[3]	0.8	15	1.1	11	1.2	14	1.5	11	1.2	17	**1.7**	**15**
TRY[3]	0.0	30	0.1	28	0.2	26	0.7	19	1.3	16	**1.4**	**16**
RUB[3]	0.3	19	0.6	17	0.7	18	0.9	16	1.6	12	**1.1**	**17**
INR[3]	0.2	21	0.3	20	0.7	19	0.9	15	1.0	20	**1.1**	**18**
BRL[3]	0.5	17	0.3	21	0.4	21	0.7	21	1.1	19	**1.0**	**19**
ZAR[3]	0.9	13	0.7	16	0.9	15	0.7	20	1.1	18	**1.0**	**20**
DKK[3]	1.2	11	0.9	15	0.8	16	0.6	22	0.8	21	**0.8**	**21**
PLN[3]	0.5	18	0.4	19	0.8	17	0.8	18	0.7	22	**0.7**	**22**
TWD[3]	0.3	20	0.4	18	0.4	22	0.5	23	0.5	23	**0.6**	**23**
THB[4]	0.2	24	0.2	22	0.2	25	0.2	26	0.3	27	**0.4**	**24**
MYR[4]	0.1	26	0.1	30	0.1	28	0.3	25	0.4	25	**0.4**	**25**
HUF[3]	0.0	33	0.2	23	0.3	23	0.4	24	0.4	24	**0.3**	**26**
SAR[4]	0.1	27	0.0	32	0.1	32	0.1	34	0.1	34	**0.3**	**27**
CZK[4]	0.2	22	0.2	24	0.2	24	0.2	27	0.4	26	**0.3**	**28**
ILS[4]	0.1	25	0.1	26	0.2	27	0.2	31	0.2	29	**0.3**	**29**
CLP[4]	0.2	23	0.1	25	0.1	30	0.2	29	0.3	28	**0.2**	**30**
IDR[4]	0.0	28	0.1	27	0.1	29	0.2	30	0.2	30	**0.2**	**31**
COP[4]	0.0	31	0.0	33	0.1	33	0.1	32	0.1	33	**0.2**	**32**
PHP[4]	0.0	29	0.0	31	0.1	31	0.2	28	0.1	31	**0.1**	**33**
RON[4]	...	37	...	40	0.0	34	0.1	33	0.1	32	**0.1**	**34**
PEN[4]	0.0	32	0.0	35	0.0	36	0.0	36	0.1	35	**0.1**	**35**
OTH	6.6		6.6		7.7		4.7		1.6		**2.1**	
Total	**200.0**		**200.0**		**200.0**		**200.0**		**200.0**		**200.0**	

Source: Bank for International Settlements (2016) [8]

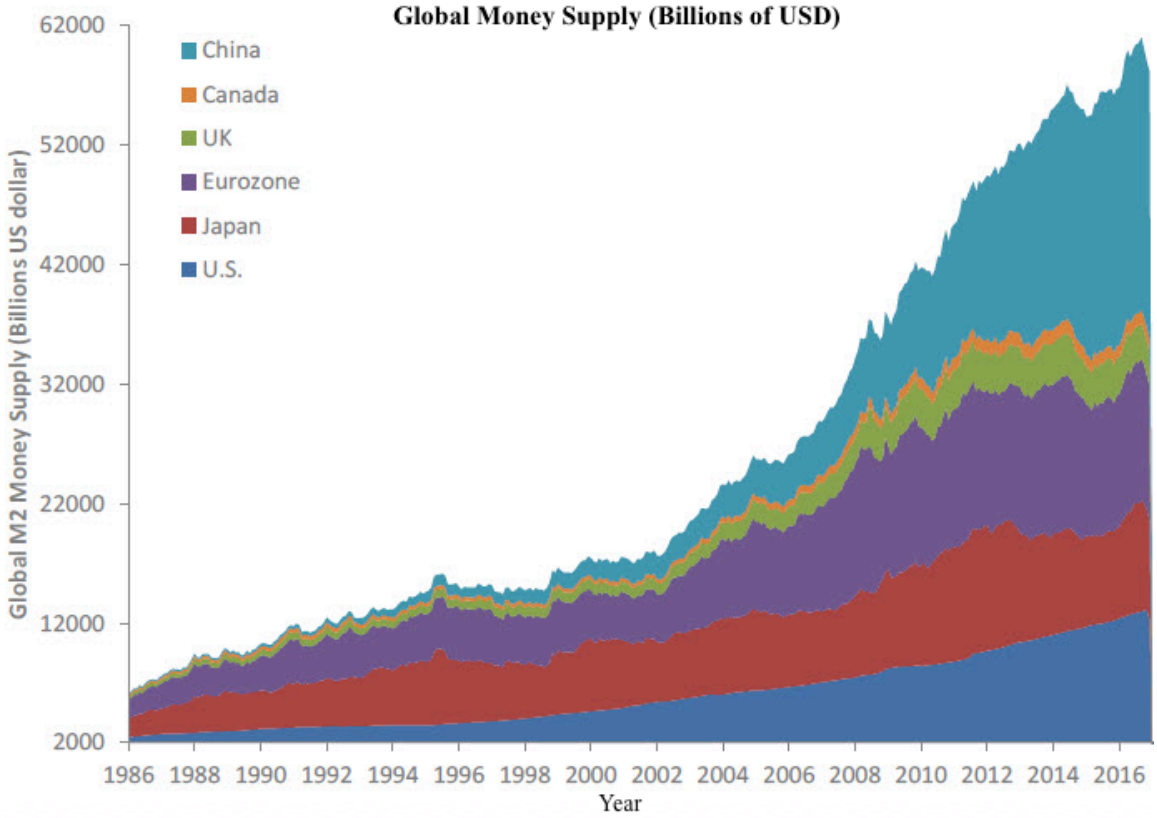
As seen in Figure 4 (above), approximately 76.7% of all global currency distribution of over-the-counter foreign exchange turnover consists of only the top four currencies of the 180 officially recognized currencies in the world. [9] These four currencies consist of the United States dollar (USD), euro (EUR), Japanese yen (JPY), and pound sterling (GBP). It is important to note that "the sum of the percentage shares of

individual currencies totals 200% instead of 100%, this is because two currencies are involved in each transaction. The turnover of some countries may be underestimated owing to incomplete reporting of offshore trading. Turnover for years prior to 2013 may be underestimated owing to incomplete reporting of offshore trading in previous surveys. Methodological changes in the 2013 survey ensured more complete coverage of activity in emerging market and other currencies." [8]

3.4.2. Global Money Supply

In the days when gold was used as a medium of exchange, a specific country's potential economic prosperity and flexibility were greatly dependent on how much gold that country owned. During the late 1920s and early 1930s, in order to recover from the Great Depression, many countries gave up on the "gold standard" in favor to printed fiat currencies with little or sometimes no financial backing whatsoever. At present, many investors believe that the world's central banks have gone too far and fear that the excessive printing of currency may eventually lead to hyperinflation and the collapse of that currency. Many currencies are not backed by anything other than the full faith and credit of that country or region, and its public's acceptance of that currency. On the next page is the selected global money supply of China, Canada, the United Kingdom, the Eurozone, Japan, and the United States. [15]

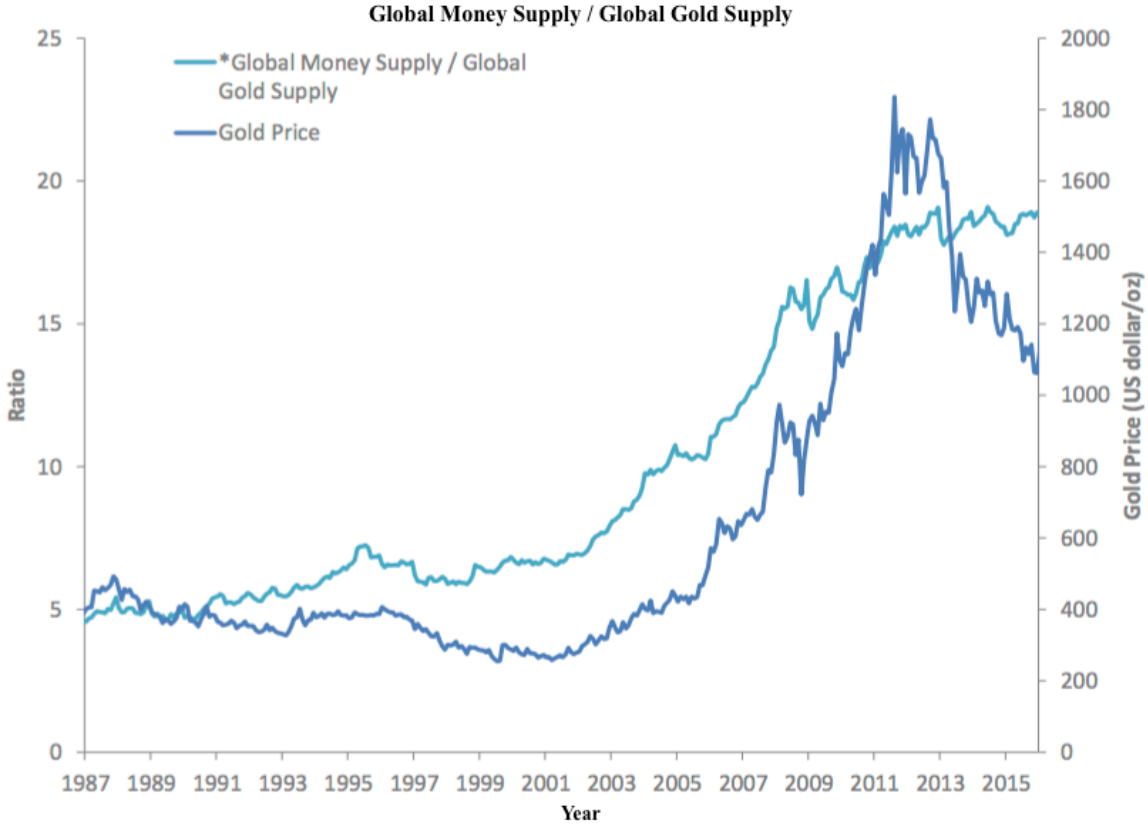
Figure 4. Global Money Supply (Billions of USD)



Source: Wells Fargo Investment Institute (2017, modified) [15]

As emphasized in Figure 4 (above), the global money supply has been astronomically increasing. At around 60 trillion USD in 2016, the global money supply has more than doubled in the last 10 years and more than quadrupled in the last 20 years. It is no coincidence that the total global money supply greatly increased as a result of the 2008 financial crisis. With global inflation rates running below norms in recent years, the fear of excessive money printing should not be dismissed. [15]

Figure 5. Ratio of Global Money Supply Over Global Gold Supply



Source: Wells Fargo Investment Institute (2017, modified) [15]

Figure 5 shows the comparison between the ratio of the total global money supply over the total global gold supply as well as the price of gold in USD per ounce. The global money supply divided by global aboveground gold supply is illustrated in light blue and the dark blue line depicts the price of gold. One way of saying that the world's central banks might be overprinting currencies is if the light blue line is rising — meaning that fiat money supplies are growing faster than the gold supplies. In recent years, that ratio of global money supply over the global gold supply has stopped moving higher, translating into sinking gold prices and less fear of overprinting currencies. [15]

3.4.3. Influences on Purchasing Power

When currency purchasing power fluctuates, it changes in the form of a loss or gain and this is what decides how much consumers can buy with a given amount of money. When prices increase, consumers lose purchasing power and when prices decrease, consumers gain purchasing power. Some causes of purchasing power loss may include government regulations, inflation, and natural or manmade disasters. Two causes of purchasing power gain include deflation and technological innovation. [14]

Even 10 years later, the effects on the loss of purchasing power are still felt in the aftermath of the 2008 global financial crisis as well as the European sovereign debt crisis. Thanks to increased globalization and the introduction of the euro, currencies are even more inevitably linked. As such, governments initiate policies to control inflation, protect purchasing power, and prevent recessions. [14]

3.4.4. Roles of Central Banks

Within each currency, the central bank is unique apart from other banks in that it has legal monopoly status, which gives it the privilege to issue bank notes and cash. Many central banks are not government agencies and therefore sometimes considered being politically independent; however, even if a central bank is not legally owned by the government, its privileges are still established and protected by law. Privately owned commercial banks are limited to issuing demand liabilities, such as checking deposits. Although it varies depending on the country, central banks' duties and the justification for their existence usually consists of three main areas. [17]

Firstly, central banks manage and control the money supply by issuing currency and setting interest rates on loans and bonds. Central banks usually raise interest rates in order to slow growth and avoid inflation — and lower rates to increase growth, industrial activity, and consumer spending. Central banks manipulate monetary policy in an effort guide the economy and achieve economic goals, such as full employment. Secondly, central banks regulate member banks through capital requirements, reserve requirements (that dictate how much banks are permitted to loan to customers and how much capital banks must keep on hand), and deposit guarantees. Central banks also manage foreign exchange reserves and provide loans and services for that nation’s banks and branches of government. Lastly; in times of despair, the central bank also acts as an emergency lender to distressed commercial banks, other institutions, or even the government. For instance, by purchasing government debt obligations, the central bank provides a relatively politically attractive alternative to taxation when the government is in need of increasing income. [17]

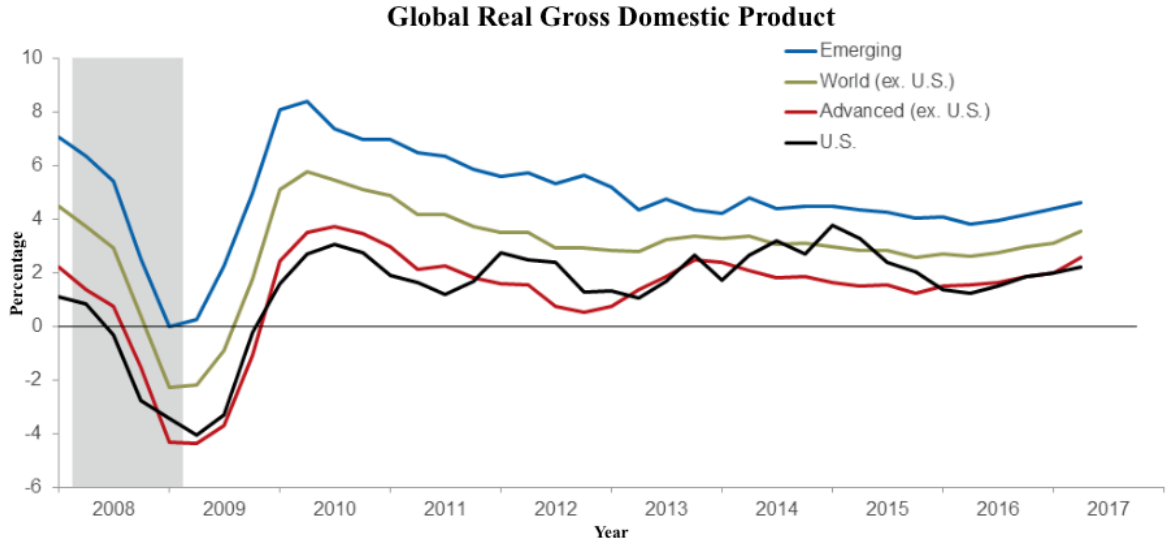
3.4.5. Inflation and Deflation

In 2008, the United States Federal Reserve kept interest rates near zero and established a plan called quantitative easing. Although initially controversial, quantitative

easing essentially saw the U.S. Federal Reserve buy government and other market securities in order to lower interest rates and increase the money supply. The idea was to increase the market's capital, which spurred increased lending and liquidity. Once the economy stabilized, due in part to the policy above and a multitude of other complex factors, the U.S. stopped its policy of quantitative easing. [14]

In an effort to help stop deflation in the Eurozone after the European sovereign debt crisis and to bolster the euro's purchasing power, the European Central Bank also pursued quantitative easing. The European Economic and Monetary Union also ratified strict regulations in the Eurozone on accurately reporting sovereign debt, inflation, and other financial data. As a general rule, countries attempt to keep inflation fixed at a rate of about 2%, as moderate levels of inflation are acceptable, with high levels of deflation leading to economic stagnation. [14]

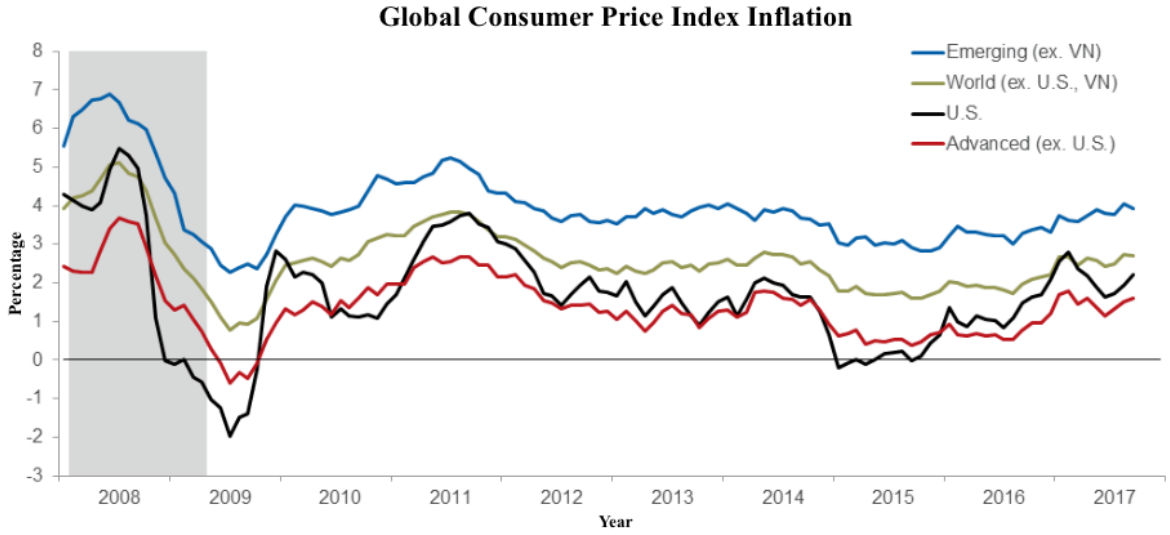
Figure 6. Global Gross Domestic Product (Adjusted for Inflation)



Source: Federal Reserve Bank of Dallas (2017, Kelvinder Virdi, modified) [16]

The shaded areas on the left hand side of Figure 6 and Figure 7 highlight the financial crisis of 2008, and have a drastic decline on emerging, world, advanced, and United States markets — both for global gross domestic product (GDP) as well as global consumer price index (CPI). [16]

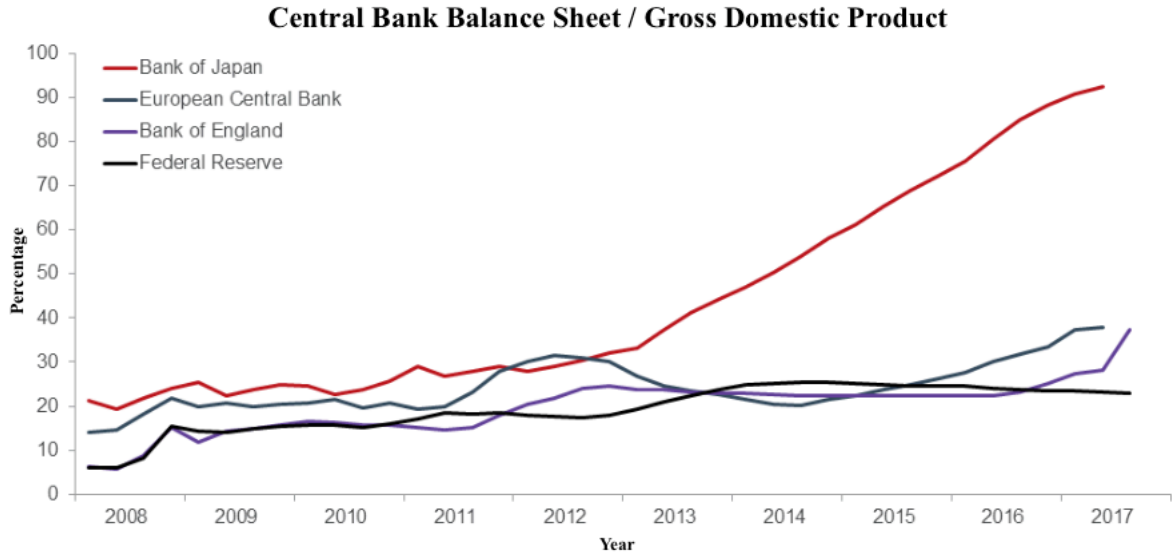
Figure 7. Consumer Price Index Inflation Around the World



Source: Federal Reserve Bank of Dallas (2017, Kelvinder Virdi, modified) [16]

It is important to note that Venezuela is excluded from the Consumer Price Index inflation data shown above in Figure 7, as the country stopped reporting inflation rates in December of 2013. [16]

Figure 8. Selected Central Bank Quantitative Easing (Share of GDP)

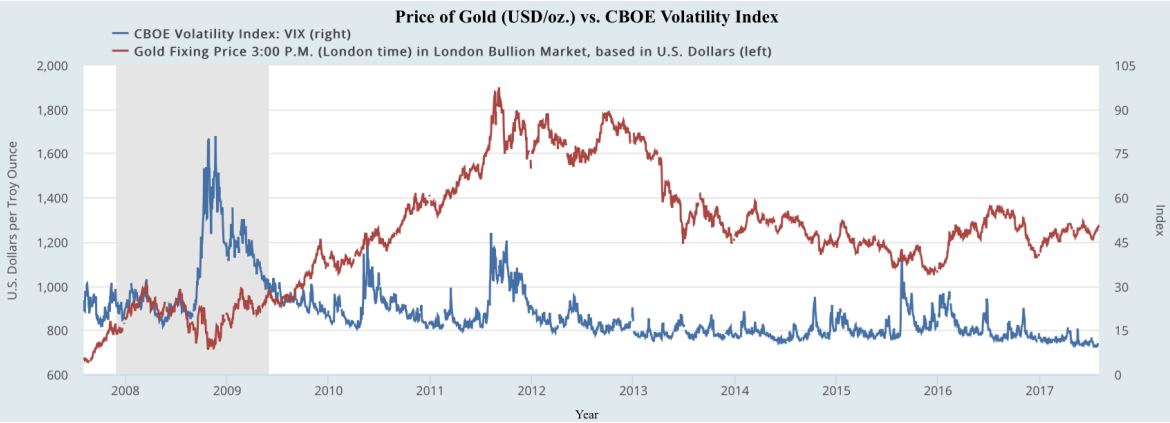


Source: Federal Reserve Bank of Dallas (2017, Kelvinder Virdi, modified) [16]

Above, Figure 8 depicts the amount of money four selected central banks spend on quantitative easing shown in percentage as the central bank's balance sheet over said country's gross domestic product. The central banks included are the Bank of Japan (BOJ), the European Central Bank (ECB), the Bank of England, and the Federal Reserve System (central bank of the United States). [16]

3.4.6. Volatility

Figure 9. Price of Gold (USD/oz.) vs. CBOE Volatility Index (Percentage)



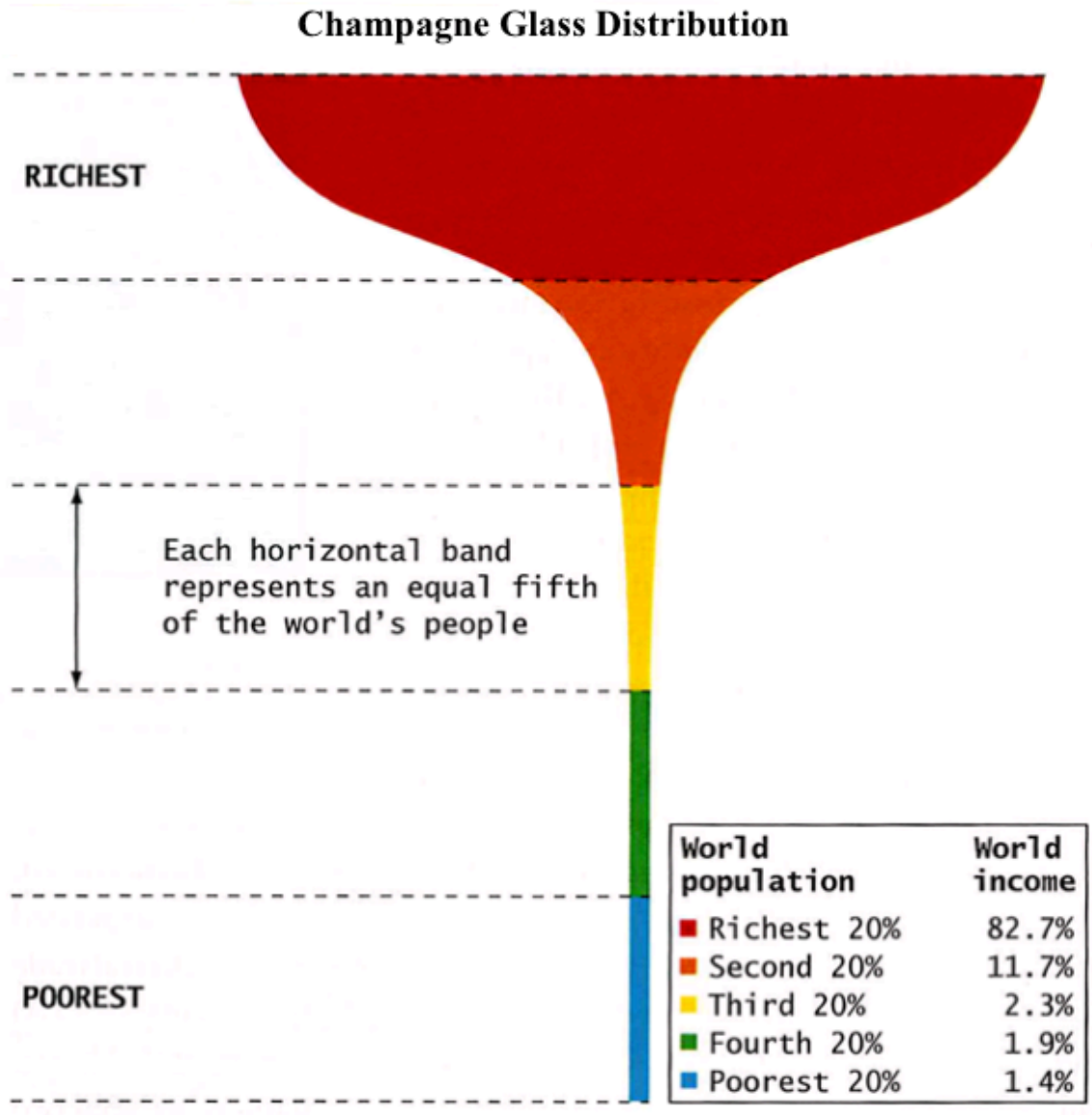
Source: Federal Reserve Bank of St. Louis (2018, modified) [18]

As seen above, Figure 9 compares two volatilities. Shown with a red line, on the left hand side of the figure, is the price of gold in USD per troy ounce on the London bullion market. The blue line tracks the Chicago Board Options Exchange (CBOE) volatility index (VIX), on the right hand side of the graph. The volatility index calculates market expectation of near-term volatility conveyed by stock index option prices. Once again, the financial crisis of 2008 and its aftereffects are depicted with a shaded background around the years 2008 and 2009. [18]

One finance giant's head of asset allocation, Russ Koesterich, stated that "changes in the VIX Index – a measure of US equity volatility – explain nearly 20% of the variation in the relative return between gold and the S&P 500 Index." He also went on to mention "when volatility rose, gold outperformed the S&P 500 price return by roughly 2% on average." [19]

3.4.8. Fiat Currency Wealth Distribution

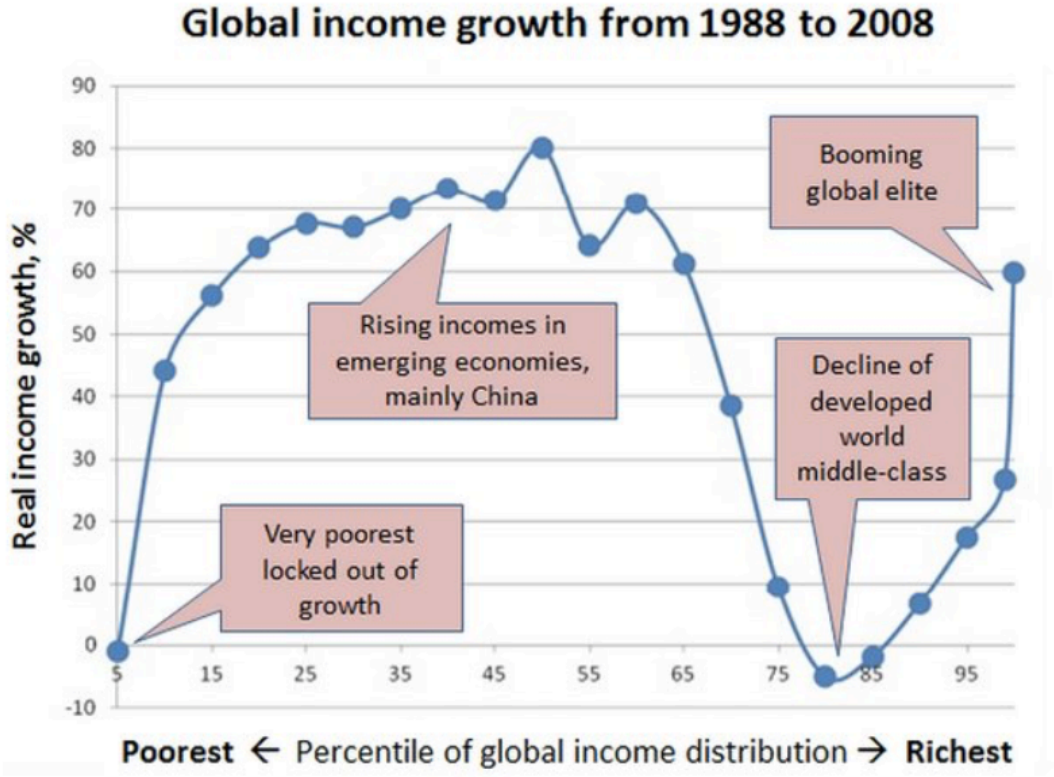
Figure 10. Champagne Glass Distribution of Global Wealth



Source: Champagne-Glass Distribution of Wealth, (2012, Jenny Kong, modified) [20]

Figure 10 above shows the champagne-glass distribution of wealth, developed by Dalton Clark Conley, an American sociologist. He coined the term due to the unequal, global distribution of income that strikingly resembles a wine glass. Each horizontal band equates to one proportionate fifth of the world's total population. As such, the figure clearly shows that the top 20% of the wealthiest people in the world own more than four-fifths of the world's total income. Oppositely, 60% of the world's poorest individuals (almost two thirds of the globe) have only about one-twentieth of the world's total income and wealth. [20]

Figure 11. Global Income Growth (1988-2008)



Source: Business Insider (2014, James T. Plunkett) [21]

On the horizontal axis of Figure 11 (above), every income percentile is plotted ranging from the poorest to the richest of the total global population. On the vertical axis, real income growth is shown as a percentage and ranges from -5% to 80% depending on whether the individual is living in extreme poverty, an emerging economy, developed-world middle class, or part of the booming elite. Although the figure concentrates on the years 1988 to 2008, the chart looks unchanged even 10 years later. It is visible that lower income percentiles have seen enormous growth since the late 1980s. Emerging economies and the rise of the Chinese middle class represents much of this growth. Next is the middle class of the developed world, which has seen almost no real income growth over the past few decades. This probably explains much of the current anger over inequality. Last is the surge of the ultra-elite, the global 1%, which have had fantastic success all these years. [21]

Developed in 2012 by Branko Milanovic, an authority on global inequality, the global inequality chart is dubbed the “elephant chart” or “elephant graph” thanks to its left to right hand side distinctive inverted “S” shaped appearance similar to that of an elephant’s body, head, and upwards swinging trunk. [22]

3.5. What is Bitcoin?

"Bitcoin: A Peer-to-Peer Electronics Cash System" is a document written by Satoshi Nakamoto. The abstract describes:

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes [network computers] that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone." [23]

The idea describes a system based on a distributed peer-to-peer cashless and electronic currency that can be transferred from one individual to another quickly and securely, anywhere in the world, without the need of a banking institution. It is possible to use as "digital cash" to send and receive payments to and from friends, consumers, or merchants. [24]

3.5.1. The History of Cryptocurrency and Satoshi Nakamoto

The nine-page document written by Satoshi Nakamoto, nicknamed the "white paper," was first made public in November of 2008, with the domain address "www.bitcoin.org" registered just three months prior. Although supposedly claiming to be a 36-year old Japanese man, going by the alias "Satoshi Nakamoto," the mysterious individual outlined the core elements of the Bitcoin system and wrote the fundamentals for the process behind it, known as the blockchain. [25]

Though Satoshi seemed to be a real person, albeit a genius at that, he interacted heavily with other developers for several years as he improved Bitcoin while never revealing anything that could pin down who he really was. Later in April 2011, Nakamoto announced he had “moved on to other things” and was never officially heard of again. For someone that was able to invent a cryptographically secured currency, Nakamoto fully concealed his identity. Still, even 10 years later, no one knows who he really was, and it is argued that it could be a man, woman, team of people, or possibly even an entire organization. Whoever it was clearly had an extreme mastery of economics, cryptography, programming, and peer-to-peer networking. Nakamoto was also amazingly skilled at writing in English. [25]

3.5.2. The Origin of Blockchain (Public Double Ledger)

It is presumed that part of Bitcoin’s deployment was in answer to the 2008 global financial crisis, when the crisis was at its ultimate height. One month before the “white paper” document was made available on the Internet, it was sent around an online cryptography mailing list, via email. [26]

Similar to a bank’s transaction ledger or a city recorder’s record book, a block is simply put: a file that holds a permanent record of some or all recent transactions within that digital currency. The block also contains a reference to block immediately before it, and *that* block holds a reference to the previous block and so on and so forth. Over time, one by one, blocks are organized by linear sequence into a chain of blocks (known as the blockchain). Miners constantly process new transactions: creating blocks — and as blocks are buried deeper into the blockchain, they are permanent and become increasingly difficult to complete. This gives rise of Bitcoin's irreversible transactions. [27]

Blocks are completed and added to the blockchain roughly every 10 minutes and there is no limit to the maximum number of blocks that may be created, meaning there is no limit to the number of Bitcoin transactions that may take place in the future. [27] As of March 20th, 2018, there are some 515,000 blocks in the Bitcoin blockchain. [31]

3.5.3. Bitcoin Safety and Security

Within the introduction of the white paper, Satoshi Nakamoto brilliantly describes the trust system that Bitcoin is built on:

"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party." [23]

The level of trust provided by Bitcoin undoubtedly adds to its value and is useful and attractive to bitcoin owners and potential bitcoin owners alike.

3.5.4. Double-Spending

Continuing in the introduction of the white paper, Nakamoto goes on to mention a viable solution to the prevention of double spending:

"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes." [23]

Simply stated, transactions take place directly between two parties and without the need of a third party middleman. In a sense, each bitcoin owner is essentially his or her own private bank. After bitcoins are recorded as being involved in a transaction, they are part of a block that itself is part of the single longest and fastest-growing blockchain (thanks to significant worldwide computational effort). Users are confident that the transaction has been accepted and permanently recorded by the computers in the network (miners) and users are prevented from creating a second transaction using the same bitcoin. In order for a user to defy this system and double-spend his or her coins, he or she would need to muster up more computing power than all other Bitcoin users combined. [33]

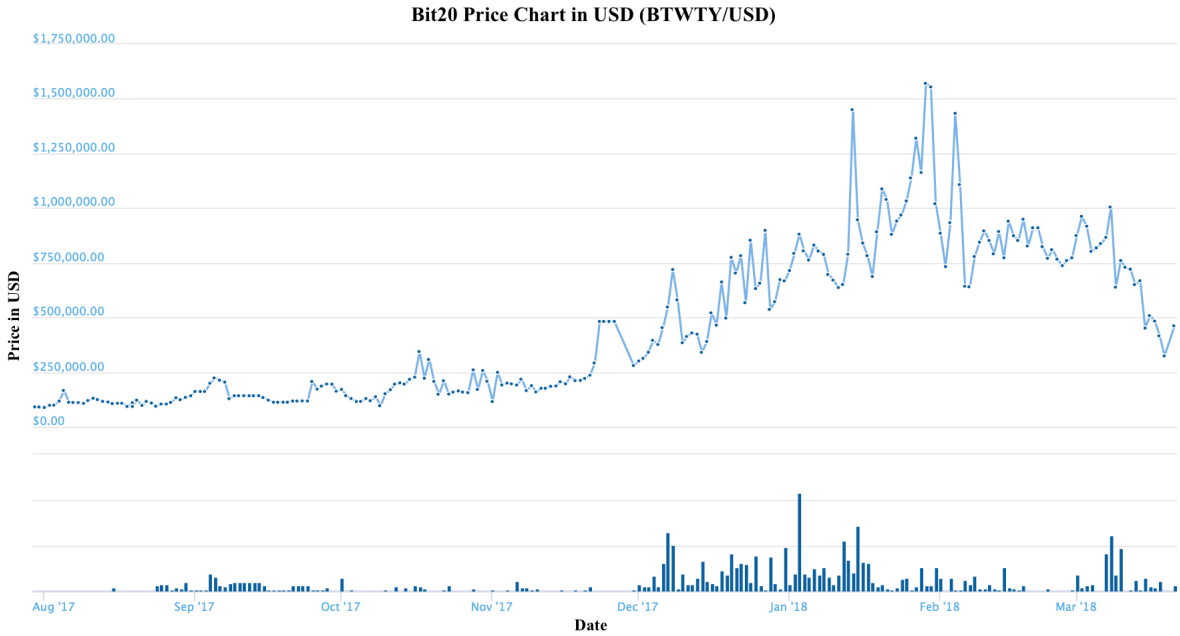
3.5.5. Other Types of Cryptocurrencies

Even though Bitcoin is the first, original, and legacy cryptocurrency, it paved the way for hundreds upon hundreds of other digital similar and different currencies. As of March 26th, 2018, there are a total of 1,587 cryptocurrencies [28] in existence, as reported by CoinMarketCap — a website that keeps track of alternative bitcoin currencies (called "altcoins") as well as Bitcoin itself. The website valuates cryptocurrencies using the market capitalization technique. An altcoin's market capitalization is calculated by multiplying its total current supply with its average current market price (per coin). Dozens of new altcoins are created each month. [29]

As of August 4th, 2017, Coinmarketcap.com was visited more than WSJ.com (The Wall Street Journal). WSJ.com was listed as the 555th most visited website in the world while Coinmarketcap.com was listed as 547th. [60]

One cryptocurrency that draws significant attention is called "Bit20" (BTWTY) even though it is relatively new. When it was first introduced on July 30th, 2017, it had a price of $91,026.40 USD per coin, granted there is only one coin in circulation. [30]

Figure 12. Bit20 Price Chart in USD (Aug. 2017-Mar. 2018)



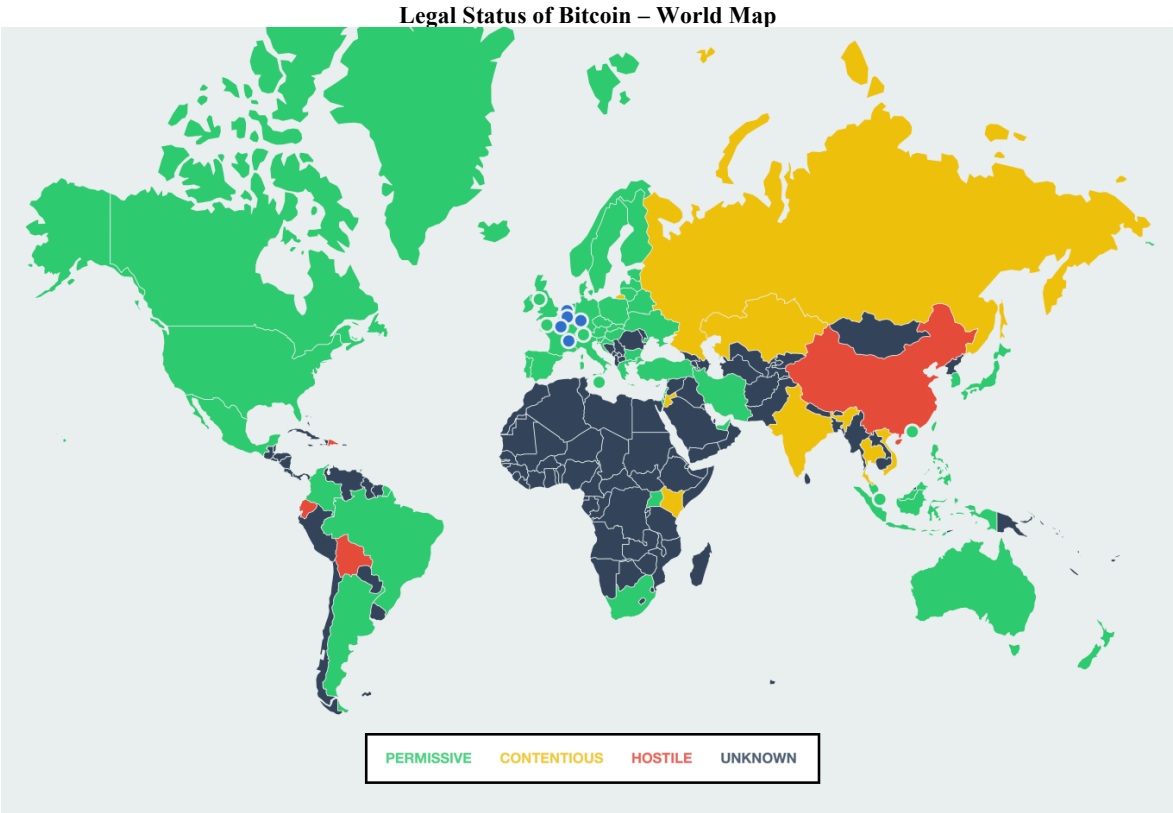
Source: CoinGecko (2018, modified) [30]

As seen in Figure 12 above, the value of Bit20 peaked on Sunday, January 29th, 2018; at a price point of $1,570.580.00 USD per coin. Near the bottom of the figure, depicted with dark blue column bars, is the total daily transaction volume. [30]

3.5.6. Legal Status of Bitcoin

As visually represented by Figure 13 on the following page, the legality surrounding Bitcoin varies from one country to another. Bitcoin is permissible in most of North America, Europe, as well as Australia. Russia and India are contentious; the legal use of Bitcoin carries certain restrictions. In China, the Dominican Republic, and a couple South American countries, Bitcoin is fully or partially prohibited. [34]

Figure 13. Worldwide Legality of Bitcoin



Source: BitLegal (2018, modified) [34]

3.5.7. Currency or Asset?

Even more than legal status, the classification of Bitcoin greatly varies by country. Countries define it as money, currency, property, a commodity, or even an asset. Some countries have slight combinations and variations such as defining it as a "virtual asset" or "digital money" but do not recognize it as legal tender. Other countries may not recognize cryptocurrencies at all, or even go on to prohibit them — both scenarios present examples where the country does nothing to prevent/decrease Bitcoin involvement, or oppositely; where a country goes above and beyond to do everything in their power to stop users of bitcoin. [35]

3.5.8. Tax Laws on Bitcoin

As defined by Bitcoin.org: "Bitcoin is not a fiat currency with legal tender status in any jurisdiction, but often tax liability accrues regardless of the medium used. There is a wide variety of legislation in many different jurisdictions which could cause income, sales, payroll, capital gains, or some other form of tax liability to arise with Bitcoin." [32]

3.6. What are Bitcoins?

A bitcoin is the unit of account of the Bitcoin cryptocurrency based on the blockchain. Although the idea of Bitcoin took place near the end of 2008, the first bitcoins emerged and came into existence on January 3rd, 2009; by Satoshi Nakamoto himself. These first 50 coins were born thanks to 30,000 lines of code written with an autonomous software program run by a computer, called "mining" (homage to gold mining). [26]

Bitcoin is most commonly associated with the informal currency code "BTC" but is synonymous with the albeit pending formal ISO 4217 standardized currency code "XBT." As in the cases of gold (XAU) and silver (XAG), three-character currency codes that begin with the letter "X" are part of nongovernmental units of currency. [36]

Figure 14. Bitcoin Symbol

Source: Bitcoin Wiki (2015, "TheRealSteve") [37]

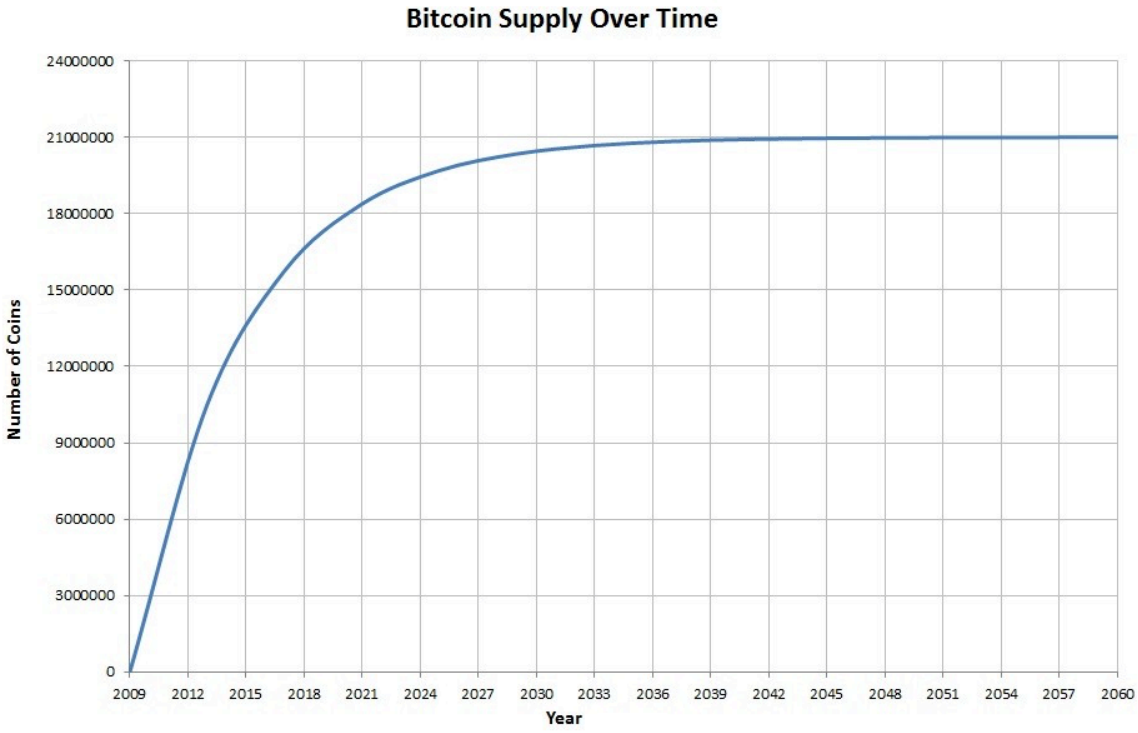
The most often used symbol for Bitcoin, by far, is a capital letter "B" with two falling strokes at both the top and bottom — pictured in Figure 14 above. Satoshi Nakamoto designed this symbol that was intended to look unique and one-of-a-kind in order to set it apart from other digital currencies and their respective symbols. The symbol represents the Bitcoin network as well as the bitcoin currency unit itself, where it is used much like the dollar sign (i.e. $10/B10). The currency unit of a single "bitcoin" is equal to that of 100 million Satoshi: the smallest unit of bitcoin (expressed as "0.00000001" in decimal form). A penny is one-hundredth of a dollar, yet a Satoshi is one hundred-millionth of a bitcoin. [37]

3.6.1. Controlled Supply of Bitcoins

As mentioned by Satoshi Nakamoto in an early email post in 2009, "coins have to get initially distributed somehow, and a constant rate seems like the best formula." [40] This geometrically decreasing-supply algorithm was selected because it very closely approximates the rate at which highly valuable commodities such as gold are mined. It functions on the basis of the block reward amount halving every 210,000 blocks, roughly

every four years, depending on the average block time. This way, the block reward decreases logarithmically. [38]

Figure 15. Projected Cumulative Supply of Bitcoins (2009-2060)



Source: Own creation (2018)

Above is the original projected total supply of bitcoins from 2009, when the first 50 bitcoins were mined, to 2060; when it was projected that the last block reward would rewarded to a miner. This final block of the Bitcoin blockchain that will generate a reward will be block number 6,929,999. [24]

3.6.2. Bitcoin Currency Creation

Unlike traditional currencies that are minted and printed, bitcoin is born into a digital world as part of the public ledger, and has no physical attributes. This virtual "money printing" is part of a predefined Bitcoin algorithm and generally speaking; cannot be altered. Coins come into existence as part of a reward for the miners running the Bitcoin infrastructure and marketplace, enabling the trade of bitcoins. When Satoshi himself mined the first block, called the genesis block, it introduced the first 50 bitcoins onto the market. These 50 bitcoins are technically particular in the fact that they can never be spent — the inflow of those 50 coins was not registered as a transaction on the global database, since they were generated from the first block. All following rewards to other miners that came

as a result of solving subsequent blocks are eligible for spending. However, since the reward is received as a result of completing a block, and blocks are added approximately every 10 minutes, this translates into a steady supply of bitcoin being put into circulation. [38]

3.6.3. Mining Rewards

There are two ways in which miners are motivated to run their networks and blockchain software in order to run the Bitcoin platform. Both rewards are received in units of bitcoin. The first is a received portion of each transaction as part of all transactions included in the block for which the miner is solving. This is further discussed in section 4.2.4. [Bitcoin] "Transaction Fees." The second incentive for miners comes in the form of a reward that increases the total amount of bitcoin in circulation, as was explained in the previous section. It is crucial to note that the award is received among miners (nodes) in the form of a lottery-based system. Since there are countless number of miners all competing to add a block to the blockchain by facilitating transactions, the winner is picked at random based on probability — that miner get to add a block and consequently receives the reward. Choosing a winner using a lottery-based system prevents a conflict of interest that would otherwise occur if miners were affiliated with either the sending or receiving party of the transactions the miners validate. Because the Bitcoin community runs the reward lottery as a whole, there is no central authority that exists to choose a winner. It is embedded within the algorithm and cannot be altered. [39]

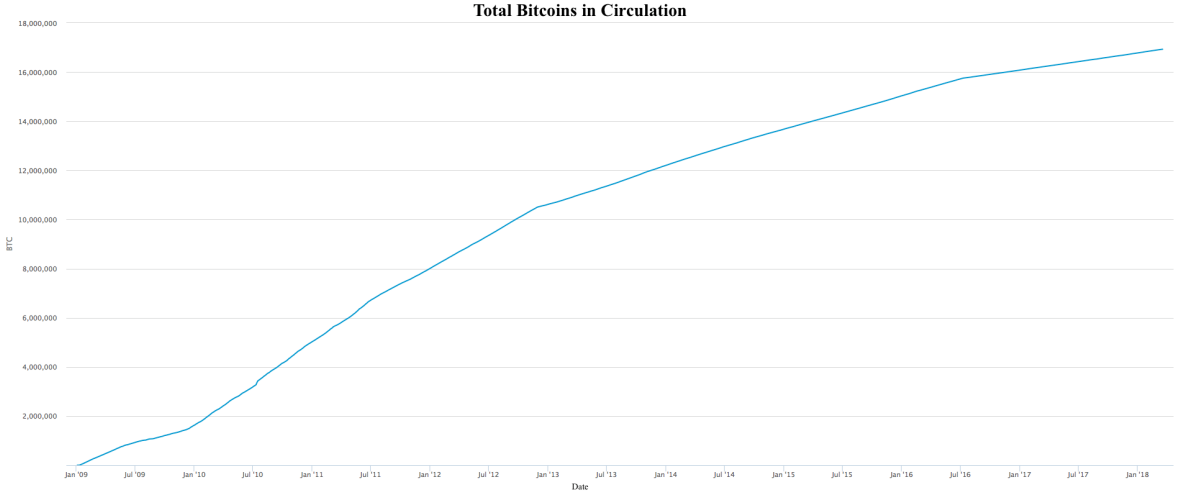
3.6.4. Reward Halving

In order to decrease incentivization as widespread Bitcoin adoption continues, part of the algorithm also includes the halving of block rewards every 210,000 blocks. As the supply of new bitcoin is a function of the block height and block reward, the maximum number of bitcoins ever in existence equates to roughly 21 million. As a result of a limitation in the present data structure of the blockchain, the actual maximum number of bitcoins is precisely 20,999,999.9769 BTC. [38]

Block number 210,000 was solved on November 28th, 2012, so the reward was automatically cut in half from 50 BTC to 25 BTC per block. As a result, the total number of bitcoin in circulation at that moment was 10.5 million, or half of the target cap. The third and current reward era occurred on July 9th, 2016; being halved again to 12.5 BTC

per block solved. It is estimated that the next block halving will occur in the year 2020, when block number 630,000 will be solved and the miner reward will be reduced yet again, to 6.5 BTC per block solved. [38]

Figure 16. Total Bitcoins in Circulation (Jan. 2009-Jan. 2018)



Source: Blockchain (2018, modified) [41]

Seen above in Figure 16 is the total amount of bitcoins in circulation for the nine years of their existence. On the horizontal axis is the date from January 2009 to January 2018 and on the vertical axis is the amount of bitcoins, ranging from one million to 18 million. [41]

At the time of writing, almost 17 million bitcoins have been mined and produced. This means that slightly more than 80% of the 21 million maximum bitcoins have been distributed, which signifies that only about four million bitcoins remain to be mined and put into circulation. If all variables were held equal to those of March 22nd, 2018 and the block time were to remain constant; the Bitcoin block reward halving would occur in approximately 800 days, on May 31st, 2020. [42]

4. Analysis and Interpretation

4.1. Bitcoin Ownership

Before an individual can assume possession of bitcoins, there are many factors to take into consideration. Some of these interests include the cost of the bitcoin; how, when, and where they will be acquired; how and where they will be stored, eligibility for future bitcoin forks, and prevention of future loss. [24]

4.1.1. Acquisition of Bitcoin

There are countless ways to obtain bitcoin: accept them as a mean of payment for a good or service, purchase them at an online trading platform, purchase them on an online exchange, buy them at a local Bitcoin ATM (automated teller machine), buy them in-person from someone locally, or earn bitcoins through either solo mining or pool mining. There also exist some ways to receive bitcoin completely free of charge, such as websites that provide free samples and offers. [24]

Apart from the various procurement methods, there are also a variety of methods to pay for the bitcoins, as well as a few limitations. Viable forms of payment include debit card, credit card, gift card (United States), physical cash currency, bank transfer, personal check, and money order. One common payment method that stands out as going so far as banning the exchange with bitcoin is PayPal. The worldwide online payment system bans accounts that have anything to do with bitcoin likely because the Bitcoin network is a direct competitor with their business model and there exists a possibility for fraudulence during transactions among bitcoin and PayPal. That said, there is a workaround for the purchase of Bitcoin via PayPal, although the process holds higher transaction fees when compared to those of other payment methods. [61]

4.1.2. Storage of Bitcoin (Short-Term vs. Long-Term)

Another variable to consider is the length of the proposed storage, whether it is short-term or long-term. The secure storage and access of bitcoin is always a concern, especially in the case of long-term ownership, where one seemingly simple mistake could become a lifetime of regret. Yet another factor of ownership length to consider is the tax restriction. American citizen bitcoin owners that sell their cryptocurrency prior to one year

of ownership will incur a short-term capital gains tax and those with more than one year of ownership will incur a long-term capital gains tax. [44]

Longterm storage of bitcoin is often called HODL or HODLing, which began as a typo but is now associated with the acronym “hold on for dear life.” [62]

4.1.3. Bitcoin Wallets

One of the last decisions that must be made before acquiring and owning bitcoin, one must choose where the bitcoins will be stored and accessed. These “places” are known as wallets, but rather than actually holding the virtual currency, wallets provide a way for the bitcoin owner to access one’s bitcoin address (one’s public key). A bitcoin wallet can hold many private keys and as mentioned earlier, many bitcoin owners have multiple wallets. If the wallet is well thought out, it makes it seem as though the bitcoin are actually on/in the wallet. This makes using bitcoin more convenient and intuitive. Although there are countless different types of wallets, there are two basic subcategories: (software) virtual wallets that reside on one’s computer or mobile device, and (hardware) physical wallets such as a small electronics gadgets or even a normal piece of paper. [43]

Electronic wallets come in the form of downloaded software or are hosted in the cloud. The latter is simply a formatted file that lives on one’s computer or device and facilitates transactions. Hosted (cloud-based) wallets tend to have more user-friendly interfaces, but one must trust a third party with his or her private keys — defeating the cryptographic trust-based system that bitcoin was designed to be. [43]

Software wallets install a wallet directly onto one’s computer and give the owner the security that to control his or her keys. Most have relatively simple configurations and are free of charge. One disadvantage is that they require more maintenance in the form of backups. Without one’s private keys backed up and stored elsewhere, if one’s computer gets stolen or corrupted, all bitcoins are lost for good. Software wallets also require greater security precautions; if one’s computer is hacked and the thief accesses the wallet or private keys, he or she also gets hold of the bitcoins on that wallet. [43]

Online (or cloud-based) wallets offer increased convenience — one can generally access his or her bitcoin from any device if he or she has the correct keys. They are easy to set up, most are free of cost, and they come with desktop and mobile apps which make it

easy to spend and receive bitcoin. The main disadvantage is low security. With the private keys stored in the cloud, one must trust the host's security measures, trust that the platform will not disappear with one's money, and trust that the system will not close down and deny access to bitcoin owners. Some leading online wallet services are directly attached to exchanges, such as Coinbase and Blockchain. Others offer additional security features like offline storage, as in the case of Coinbase and Xapo. [43]

Mobile wallets are available as apps on one's smartphone, which especially useful if he or she want to pay for something using bitcoin in a shop; or if one wants to buy, sell, send, or receive bitcoin while on the move. All of the online wallets and most desktop ones mentioned above have dedicated mobile versions, while others such as Abra, Airbitz and Bread were created with mobile in mind. [43]

Hardware wallets are small devices (similar to a USB flash drive) that occasionally connect to the web to enable bitcoin transactions or to view one's total balance. They are extremely secure, as they are generally offline and technically considered unable to be hacked. They may however be lost or stolen, along with the bitcoins that belong to the stored private keys. Many large investors keep their hardware wallets in secure locations such as bank vaults. Some notable examples of hardware wallets are Trezor (a Czech company), Keepkey, Ledger, and Case. [43]

Paper wallets are perhaps the simplest of all wallets as they are pieces of paper on which both the private and public keys of a bitcoin address are printed. These wallets are considerably secure and suitable for longterm storage since they are not connected to a network or the Internet and do not require access to electricity, software, or hardware. Naturally, these wallets are easier to misplace, damage, or deteriorate over time. With platforms such as WalletGenerator and BitcoinPaperWallet, one can easily create a new address and print the wallet straight from a printer. After this, it is possible to send some bitcoin to that address and then store the paper safely, give it away as a gift, or provide it as a form of payment for a good or service. [43]

4.1.4. Bitcoin Forks

Bitcoin forks occur when two miners find a valid computation within a short period of time. The solution is spread by both miners to be verified by their neighbors. Due of

this, the network will be split into two during the process. One block is considered by half of the network to be the next additional block in the blockchain, while the other network's half will consider a different block. Most of the time, this problem is quickly resolved. The chance of finding two blocks within a couple of seconds of each other as well as succeeding two block rewards is rare. The fork will be resolved by the network that finds the next block, since this blockchain has the higher complexity and difficulty. These forks are categorized into hard forks, soft forks, and accidental forks. [62]

A hard fork means that older software versions are incompatible with software upgrades. In order to validate new transactions and participate continuously, each miner should be able to upgrade to new the software. Miners who do not upgrade will not be able to validate the latest transactions and will become separated from the network. Because of this, the blockchain will suffer permanent divergence. Two chains will exist alongside each other and support is maintained by the minority chain or the mining participants. [62]

A soft fork, sometimes referred to as a SegWit (Segregated Witness), means older software versions are backwards-compatible with a software upgrade. Miners that were not able to upgrade may still participate in the verification and validation of transactions. Since upgrades are done by the majority of miners, this is easier to implement. As to whether miners have updated their software or not, all of them will still be able to continuously identify new blocks and maintain network compatibility. There will however, be an effect on the functionality of a miner who is non-upgraded. For instance, when a new rule changed the blocksize, the network will reject the blocks of non-upgraded miners, yet they will still be able to see that new transactions are coming in as valid. Thus, a soft fork characterizes a continuing upgrading mechanism, so that miners who have not upgraded yet need to do so, or else their functionalities will be limited. [62]

Lastly, accidental forks occur when an update is incompatible. Miners using a different software version create different ledgers from an older version and another from the latest version. When this happens, the developer of the cryptocurrency must quickly find and eliminate the bugs that are causing these incompatibilities and think of a way how those different blockchains can be combined. [62]

Essentially, forks enable bitcoin owners to double their amount of cryptocurrency, since there are two ledgers with the same transaction information. However, the "new"

digital currency does not come in the form of Bitcoin, but rather a completely new cryptocurrency of an equal amount of currency that was held in bitcoin at the time of the fork. Some well known Bitcoin fork cryptocurrencies include Bitcoin Cash (BCH), Bitcoin Gold (BTG), and Super Bitcoin (SBTC). Forks can improve the structure and stability of a cryptocurrency by code developments and improvements. The way in which Bitcoin's blockchain splits may even help in the advancement of the ecosystem of the cryptocurrency. [62]

4.1.5. Loss of Ownership

Just like gold can sink with the ship that is carrying it and money can burn in the bank that is holding it — the ownership and transaction ability of one's bitcoins can be compromised as well, disappearing forever. Bitcoins are considered "lost" when the conditions required to spend/transfer them are no longer known. Although the total maximum supply of bitcoins is limited at 21 million, the total spendable supply will always be (increasingly) less due to accidental loss, willful destruction, and technical peculiarities. [38]

As of November 2017, it was estimated that nearly four million bitcoins are eternally lost. According to research performed by a digital forensics firm that studies the bitcoin blockchain, the number of lost coins must be estimated, as it is impossible to prove the exact amount. The firm came up with both low and high estimates; between 2,780,000 and 3,790,000 bitcoins are gone for good. Of the total circulation of 16.7 million bitcoins at the time, the estimates imply that between 17% and 23% of bitcoins are considered missing — around one-fifth to one-fourth of the total amount in circulation. It is important to mention that these numbers do not include bitcoins that were hacked or otherwise compromised or stolen, as these coins are not truly lost since they are still in control by the thief. [49]

The amount of lost bitcoins as of mid-2017 is visually represented on the following page, in Table 5. [49]

Table 5. Lost Bitcoins (Mid-2017)

	Total as of mid-2017	Percent Lost	Lost Bitcoins
Mined Coins	604,388	0%	-
Transactional	6,066,664	2%	121,333
Out of circulation ("Hodlers")	5,110,898	50%	2,555,449
Strategic Investors	3,557,539	2%	71,151
Original Coins ("Satoshi Coins")	1,041,715	100%	1,041,715
Total	16,381,204		***3,789,648***

Source: Fortune (2017, Jeff John Roberts and Nicolas Rapp) [49]

4.2. Use of Bitcoin — Medium of Exchange and Unit of Account

Bitcoin is considered as having excellent characteristics of currency as it is portable, durable, divisible, recognizable, liquid, sparse, and impossible to counterfeit. Unlike the stock market and most banking institutions, bitcoins are able to be involved in transactions and trading 24 hours per day, seven days a week, 365 days a year. Since miners operate 24 hours a day, bitcoin owners do not need to worry about bitcoin opening and closing prices. Buyers and sellers have the freedom to engage in transacting whenever they please and Bitcoin's economy can benefit from the increased number of transactions. [32]

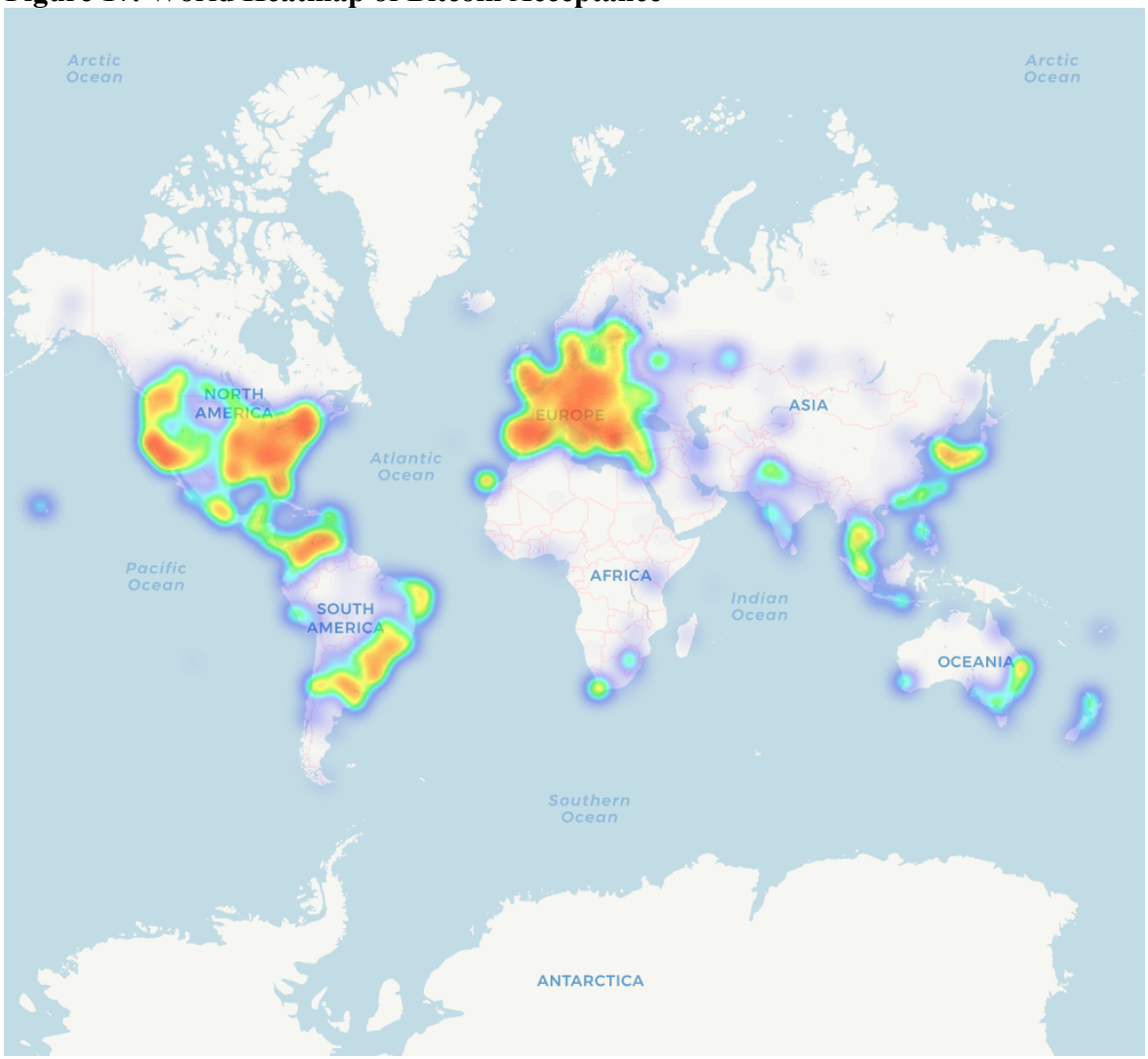
After deciding on where to acquire bitcoin and which means to pay for them with, the next step is understanding how to send and receive bitcoins. Buyers and sellers require a bitcoin address, which is a sequence of numbers, letters, and a private key. The address is public, but the private key is secret, similar to a password. The seller gives out his or her bitcoin address to the buyer who then signs a transaction using his or her private key in order to send a payment. The buyer will then release the bitcoins of a given value to the bitcoin network for verification (as well as a small transaction fee). After verification, the transaction is recorded in the blockchain ledger, and the seller's balance increases. It is important to note that a new address is typically used for each transaction, enabling anonymity. [44]

4.2.1. Acceptance

A large amount of individuals and businesses use Bitcoins all over the world, and that number is quickly growing. These include brick-and-mortar business such as restaurants and shops, apartments, and even law firms. [32] Additionally, there a large

amount of popular online services that accept Bitcoin as a possible mean of payment, these include Reddit, Wikipedia, CheapAir, (flights), Expedia (hotels), Microsoft, and Alza.cz (largest Czech online retailer). Ranging from the biggest to smallest names, there are around 100 businesses all over the world that accept bitcoins as a currency, as stated by 99bitcoins.com. [54] As of March 20th, 2018; there are over 12,115 venues that accept bitcoins in place of currency, as stated by SatoshiLab's Coinmap.org. Figure 17 (below) visually represents this in the form of a heatmap of the world. [55] On the following page, Figure 18 shows a more specific view of merchant goods and services of the United States and Europe, represented by logical symbols. [32]

Figure 17. World Heatmap of Bitcoin Acceptance



Source: Coinmap.org (2018, SatoshiLabs, modified) [55]

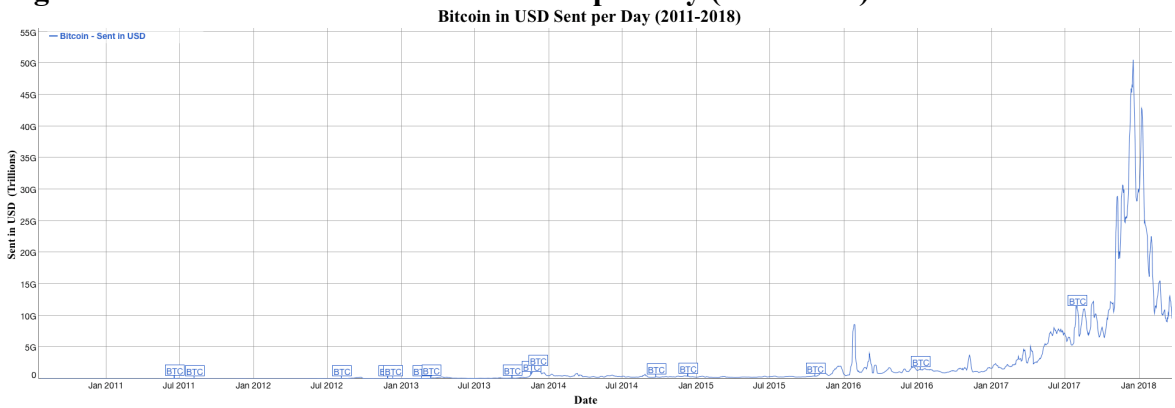
Figure 18. Detailed Map of Bitcoin Acceptance (US and Europe)

Source: Bitcoin.org (2015, useBitcoins.info) [32]

4.2.2. Types of Transactions

One of the ways a currency is analyzed is the amount of value sent per day. As of March 25th, 2018, the amount of bitcoins sent in the last 24 hours is about 880,000 BTC. This translates into a total value of approximately 7.6 billion USD traded in the last day. Although it constantly fluctuates, with the market capitalization of bitcoins momentarily valuated at roughly 146 billion USD, the total 24 hour trading volume is only about 5.2% of the total market capitalization. [48]

Figure 19. Bitcoin in Trillions of USD Sent per Day (2011-2018)



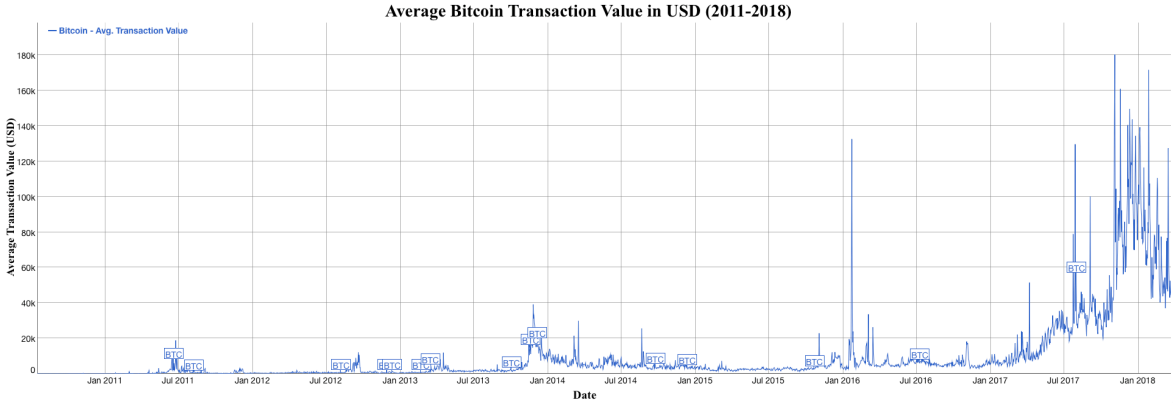
Source: Bitinfocharts (2018, modified) [57]

Seen above in Figure 19 is the dramatic rise of the USD value amount of bitcoin sent per day, from 2011 to 2018, in the form of a seven-day simple moving average. The date is on the horizontal axis in six-month increments starting from July of 2010 to January of 2018. On the vertical axis is the amount of bitcoin sent valued in trillions of USD, ranging from zero to 55 trillion USD. [57]

4.2.3. Transaction Amounts

Another way a currency is analyzed is by the amount of value sent per transaction. As of March 25th, 2018, the average transaction amount is 6.4 BTC, valued at about $55,273. The median transaction amount for that same day is about 0.067 BTC, at a value of $575.69. It is obvious that bitcoin is not being used for one of its original proposed purposes: as a way for people to buy goods and services. Because bitcoin is still relatively early in its widespread adoption, the majority of daily trading accounts for buying and selling bitcoin for other fiat currencies, such as the United States dollar, the euro, and Japanese yen. [48]

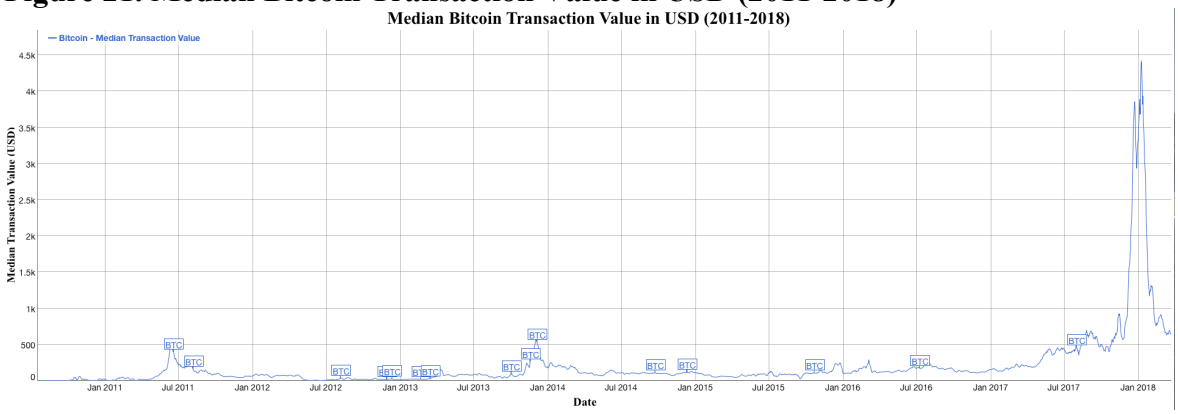
Figure 20. Average Bitcoin Transaction Value in USD (2011-2018)



Source: Bitinfocharts (2018, modified) [58]

Seen above in Figure 20 is the average USD value of a bitcoin transaction, from 2011 to 2018. Again, the date is on the horizontal axis in six-month increments starting from July of 2010 to January of 2018. On the vertical axis is the average value ranging from zero to $180,000 USD. [58]

Figure 21. Median Bitcoin Transaction Value in USD (2011-2018)



Source: Bitinfocharts (2018, modified) [59]

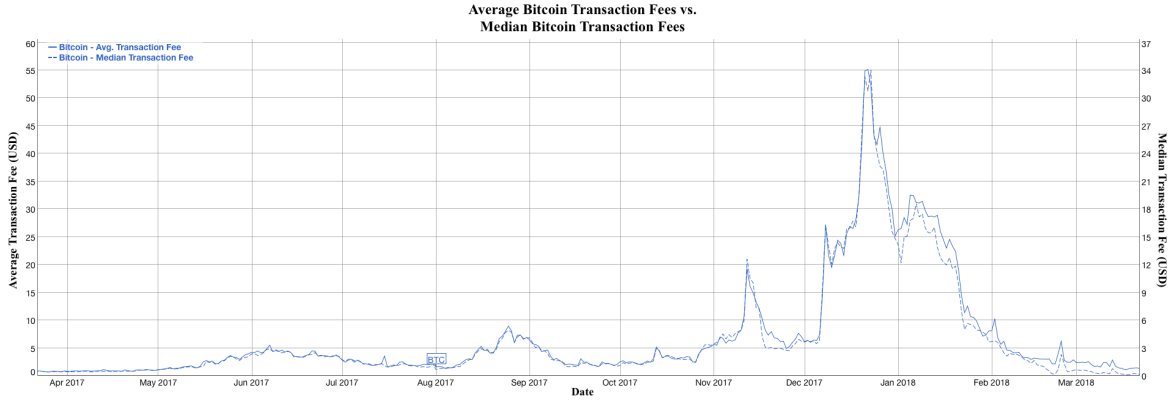
Seen on the previous page in Figure 21 is the median USD value of a bitcoin transaction, from 2011 to 2018, shown in the form of a seven-day simple moving average in order to clarify movement. Once again, the date is on the horizontal axis in six-month increments starting from July of 2010 to January of 2018. On the vertical axis is the average value ranging from zero to $4,500 USD. [59]

4.2.4. Transaction Fees

A transaction fee is a cut of the bitcoin transaction that is collected by the miner who includes that transaction in the block. The transaction fee is the difference between the amount being sent from one party and the amount being received by another party (it must be greater than or equal to zero). For a transaction to take place, the sending party decides and specifies the transaction fee amount — the higher the fee, the more likely the transaction is to be included in a block by the miners, even though it is less economically efficient and more costly for the sender (the receiving party is unaffected, unless otherwise arranged). [50]

As mentioned in section 3.6.3., transaction fees are the secondary motivation for miners, after block rewards. It is clear that the current block reward is 12.5 BTC per added block, but the amount of bitcoins received in the form of transaction fees is less known. As of March 24th, 2018, total transaction fees per added block are roughly 0.2 BTC, [48] or the equivalent of about $1,800 USD. As seen in Figure 22 below, both the average and median individual transaction fees are shown. [47]

Figure 22. Bitcoin Transaction Fees – Average vs. Median (Mar. 2017-Mar. 2018)



Source: Bitinfocharts (2018, modified) [47]

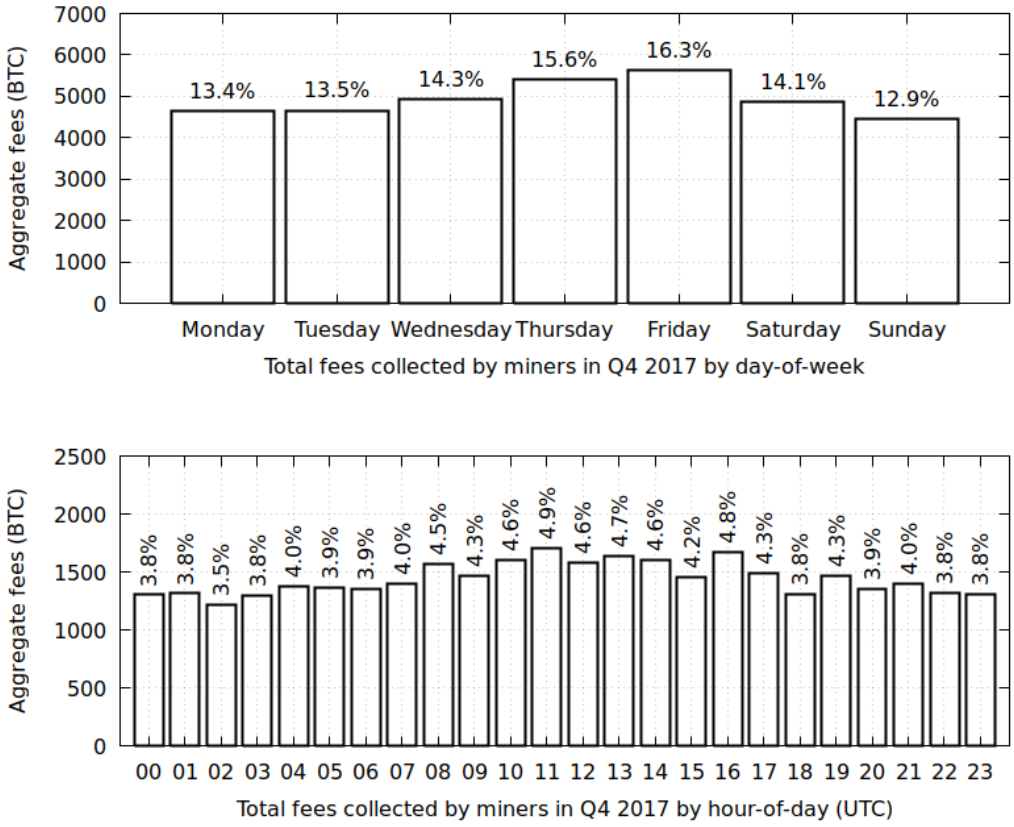
In Figure 22 above, average transaction fees in USD are listed on the left-hand side vertical axis in increments of $5 USD, ranging from $0 to $60, plotted with a solid blue

line. Median transaction fees are seen on the right-hand side vertical axis in increments of approximately $3 USD, ranging from $0 to $37, plotted with a dotted blue line. As always, the date is shown on the horizontal axis, in one-month increments, from April 2017 to March 2018. [47]

It is important to note that prior to March 2018, both average and median transaction fees were almost always below $1 USD. As reward halving continues, miners will become less dependent on block rewards and more dependent on transaction fees. In an effort to keep the platform functioning after widespread worldwide adoption, it is crucial to slowly transition to a system where transaction fees become the primary motivator of miners and the block rewards become the secondary motivator, before disappearing altogether. [47]

Aside from varying daily, transaction fees collected by miners also differ depending on the day of the week and the time of day, as seen below in Figure 23 — where miner fee data was collected from the fourth quarter of 2017. [50]

Figure 23. Share of Total Miner Fees Collected in Q4 2017 (By Day and Hour)



Source: Bitcoin Wiki (2018, "Harding") [50]

On average, miners collect more fees during the week than they do during the weekend, as seen in the figure on the previous page. Total fees collected during the intra-day cycle wax and wane with no apparent trend, aside that mid-day of Coordinated Universal Time (UTC) seems to experience slightly higher fees than the rest of the day. [50]

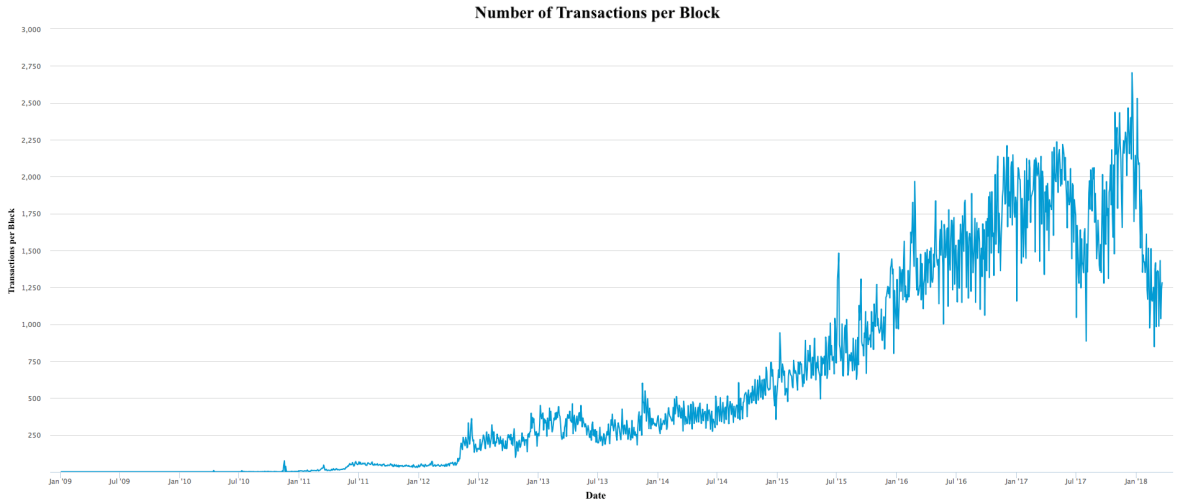
The variations in supply and demand create a marketplace for block space that lets users make a choice between confirmation time and cost. This comes in the form of either a natural (but unpredictable) increase in supply of block space, or a (somewhat predictable) decrease in demand of transactions. Senders with high time requirements may need to pay a higher than average transaction fee in order to be confirmed in a timely manner, while users under less time constraint might save money by being prepared to wait longer. Some users are willing to pay high fees while some are not. Other users desire/need a fast confirmation while some are content with waiting a while. [50]

4.2.5. Number of Transactions per Block

As stated in the documentary *Banking on Bitcoin*, the "VISA" credit card system can handle up to 25,000 peak transactions per second, the "Western Union" financial services company that focuses on the transfer of funds all over the world can handle 750 peak transactions per second, yet Bitcoin is limited to approximately seven transactions per second. [51] By design, Bitcoin was not meant for high-volume transactions. As the average transaction amount rises, the possibility for micropayments (transactions of miniscule amounts such as less than $1 USD) diminishes. [51]

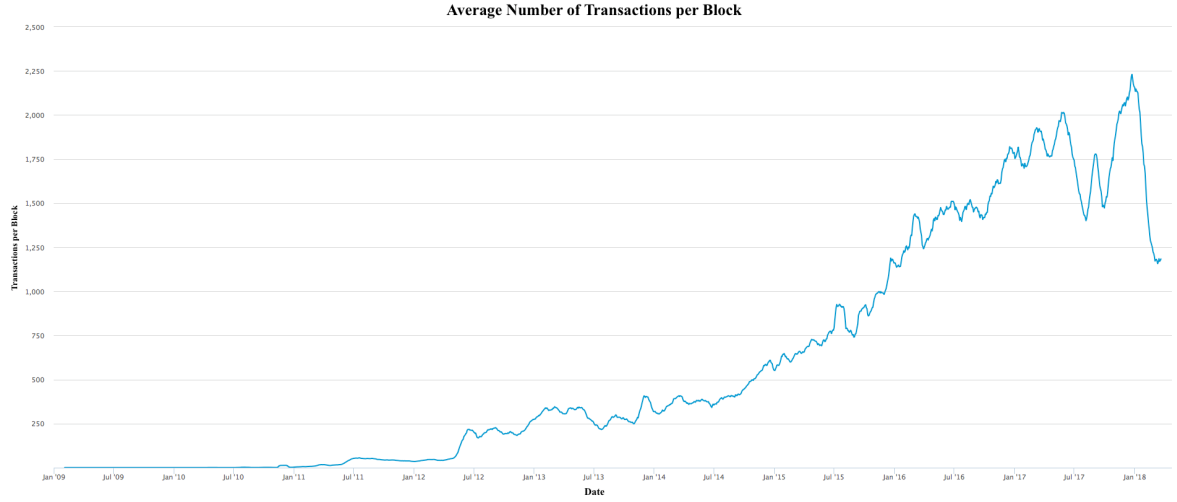
As represented in Figure 24 on the next page, the raw value number of transactions included in each completed block is shown with the date on the horizontal axis (from January 2009 to January 2018) and the number of transactions per block displayed on the vertical axis (measured in 250 unit increments from 250 to 3,000). The raw value numbers experience a great deal of variance, due to an array of countless variables. The amount of transactions per block can easily spike or sink almost 1,000 transactions in a matter of less than one week. [45]

Figure 24. Raw Value Number of Transactions per Block (2009-2018)



Source: Blockchain (2018, modified) [45]

Figure 25. Average Number of Transactions per Block (2009-2018)



Source: Blockchain (2018, modified) [45]

As with Figure 24, Figure 25 (above) shows the 30-day average number of transactions included in each block. Again, the date is on the horizontal axis (from January 2009 to January 2018) and the number of transactions per block is displayed on the vertical axis (measured in 250 unit increments from 250 to 2,500). The one-month simple moving average smoothes out the variance seen in the raw value number of transactions and gives a better understanding of the average values. Overall, the trend of the average number of transactions per block was steadily increasing up until the end of 2017, with a roughly 50% reduction in the number of transactions for the month of January 2018 alone. [45]

4.2.6. Number of Transactions per Second

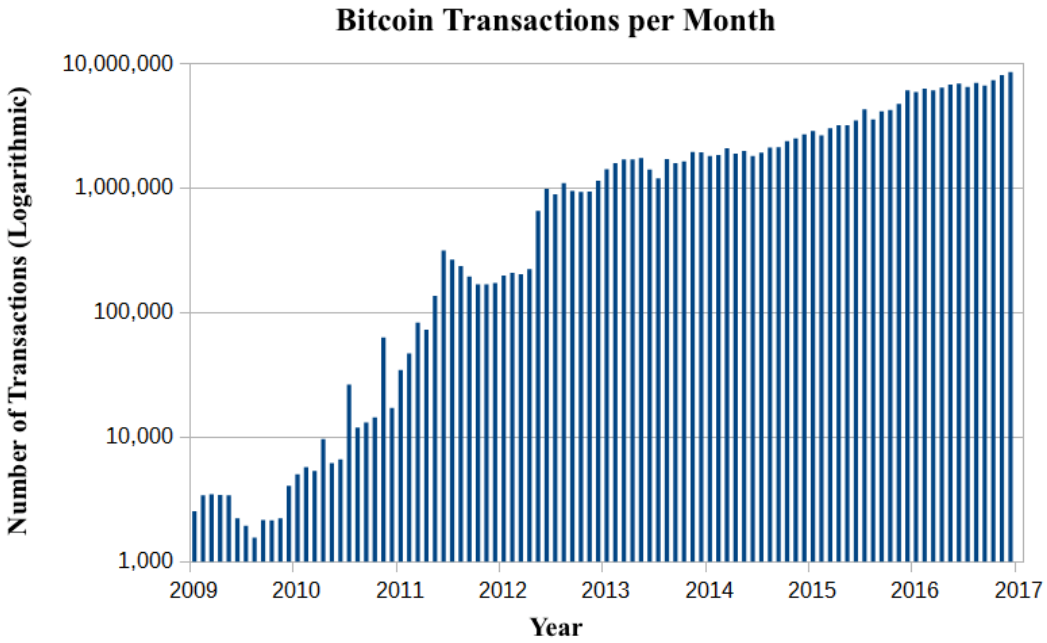
The maximum bitcoin transaction rate is known as the block size limit divided by the mean transaction size. The block size limit is well known, one megabyte (MB); however, the average transaction size is not known. Although the most common maximum number of transactions per second is usually said to be around seven, the theoretical transactions per second range from five to 10. [52]

As of yet, the most bitcoin transactions that occurred in a 24-hour timeframe occurred on Thursday, December 14th, 2018; at a total of 490,459 transactions. This equates to roughly 5.7 transactions per second, 340 transactions per hour, and 20,435 transactions per hour. [53]

4.2.7. Number of Transactions per Month

In Figure 26 below, it is clear that the number of bitcoin transactions per month is steadily rising. Not only that, the scale of the figure is logarithmic, meaning bitcoin transactions are actually growing exponentially. [56]

Figure 26. Number of Transactions per Month (2008-2017)



Source: Wikipedia (2015, "Zhitelew," modified) [56]

4.2.8. Bitcoin Owners

Due to the built-in security and anonymity of the Bitcoin, the number of bitcoin owners is a complex question to answer. Even if the total number of wallets could be verified (which it cannot), the amount would not be reflective of the number of bitcoin owners or users. This is because one person may easily have tens, hundreds, or even thousands of bitcoin addresses. Oppositely, two or more people may own one wallet, although this is much less common than the previous example. Additionally, an unknown amount of inactive wallets exist. As time goes on, it becomes more and more impossible to attempt to quantify the number of users and owners of bitcoin. [32]

For reference, as of January 18th, 2018; it was estimated that there are almost 28.5 million bitcoin wallets that have a balance of 0.001 BTC or more. At $9,000 USD per bitcoin, 0.001 BTC is worth about $9 USD. [46]

4.3. The Purchasing Power of Bitcoin

The price and popularity of Bitcoin has dramatically skyrocketed within the last nine years, yet there are still concerns about its volatility and whether or not it is some sort of scheme or get-rich-quick scam. It is important to look at the purchasing power of bitcoin by examining its lack of a central bank, price and market capitalization, volatility, and liquidity. [32]

4.3.1. Lack of a Central Bank

Bitcoin is unique in the fact that there is absolutely no central bank, central authority, or central point of attack. Since the bitcoin protocol and concept is self-sufficient and run by bitcoin developers/users all over the world, it is much like the Internet. Users are unique and no individual or group of individuals has the right to say that they own the Internet — or Bitcoin. With the proper tools and procedures, both can be accessed and used (reading and writing) by anyone from anywhere in the world, during any time of the year and day. [32]

Not even Satoshi Nakamoto himself could be considered a central bank or power of authority since the Bitcoin protocol and software he designed were openly published and any developer around the world could and still can review the code or make their own

modified version of the Bitcoin software. Just like current developers, Satoshi's influence (or potential center of authority/power) was limited to the changes he made being adopted by others; therefore, he did not control or own Bitcoin. With Nakamoto remaining mysteriously anonymous and officially abandoning the platform in late 2010, it is further proof that Bitcoin's success is unrelated to the creator, his whereabouts, and/or his actions. As long as the most popular version is used by the majority of miners and the built-upon blockchain is always the longest one; the platform will keep functioning — all without an unnecessary middleman: the central bank. [32]

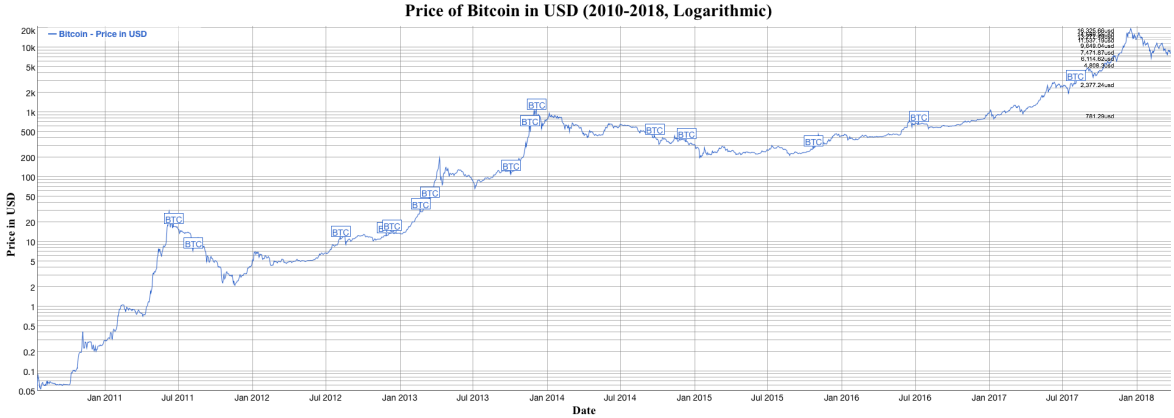
4.3.2. Price of Bitcoin

On July 17th, 2010, the price of one bitcoin was $0.0495 USD, or just under one nickel. Only $1 USD would have bought more than 20 bitcoins. Exactly seven years and five months later, on December 17th, 2017; the price of bitcoin reached its historical maximum of $19,401. The same 20 bitcoins purchased for less than a dollar, less than seven and a half years earlier, would now have a total value of over $388,000 USD. Below in Figure 27 is the all-time history of the price of bitcoin shown on a linear scale. On the next page, in Figure 28, the all-time history is shown on a logarithmic scale. [64]

Figure 27. Price of Bitcoin in USD (2010-2018, Linear)

Source: Bitinfocharts (2018, modified) [64]

Figure 28. Price of Bitcoin in USD (2010-2018, Logarithmic)



Source: Bitinfocharts (2018, modified) [64]

Although Figure 27 shows a recent decline in the price of bitcoin, Figure 28 shows a general upwards trend of the price of bitcoin in a logarithmic sense. If the price of bitcoin continues to follow this trend in the slightest sense, the growth in the price of bitcoin will be exponential. [64]

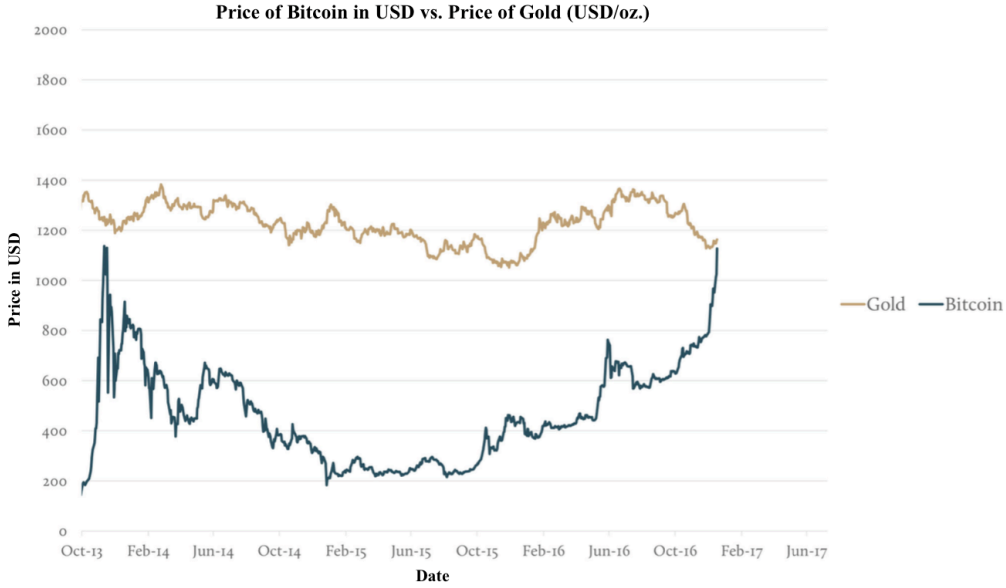
4.3.3. Bitcoin Market Capitalization

As with the price of bitcoin, the market capitalization has also drastically fluctuated. At its height, the total market capitalization of bitcoin was almost 325 billion USD, on December 17th, 2017. Exactly one month later, on January 17th, 2018; bitcoin's market capitalization was at a low of around 180 billion USD. At the time of writing, the lowest market capitalization of 2018 occurred on February 6th, 2018, when the market capitalization was at a mere 115 billion USD. The last time the market capitalization was that low, was the middle of November in 2017. [48]

4.3.4. Volatility of Bitcoin

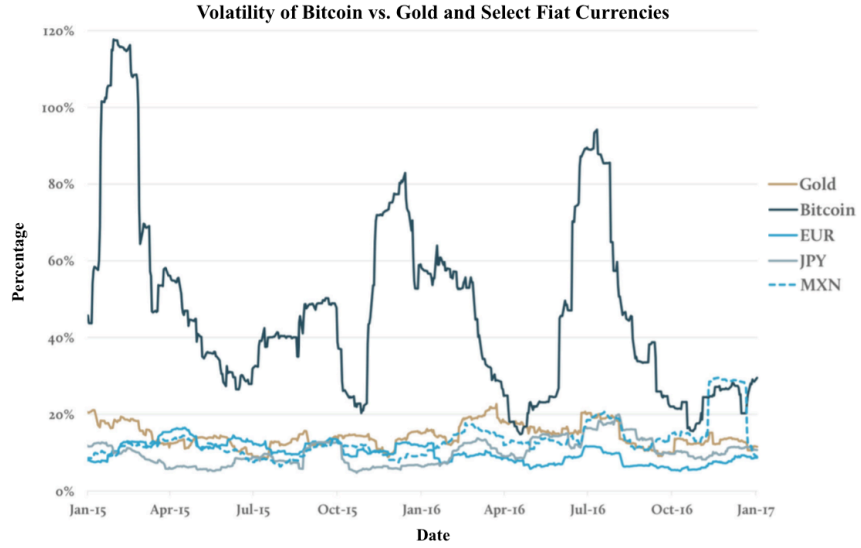
On the following page in Figure 29, the price of bitcoin is compared with the price of gold per troy ounce. The data shows the historical prices from October of 2013 to about February of 2017. [65]

Figure 29. Price of Bitcoin in USD vs. Price of Gold (USD/oz.)



Source: Goldmoney (2017, modified) [65]

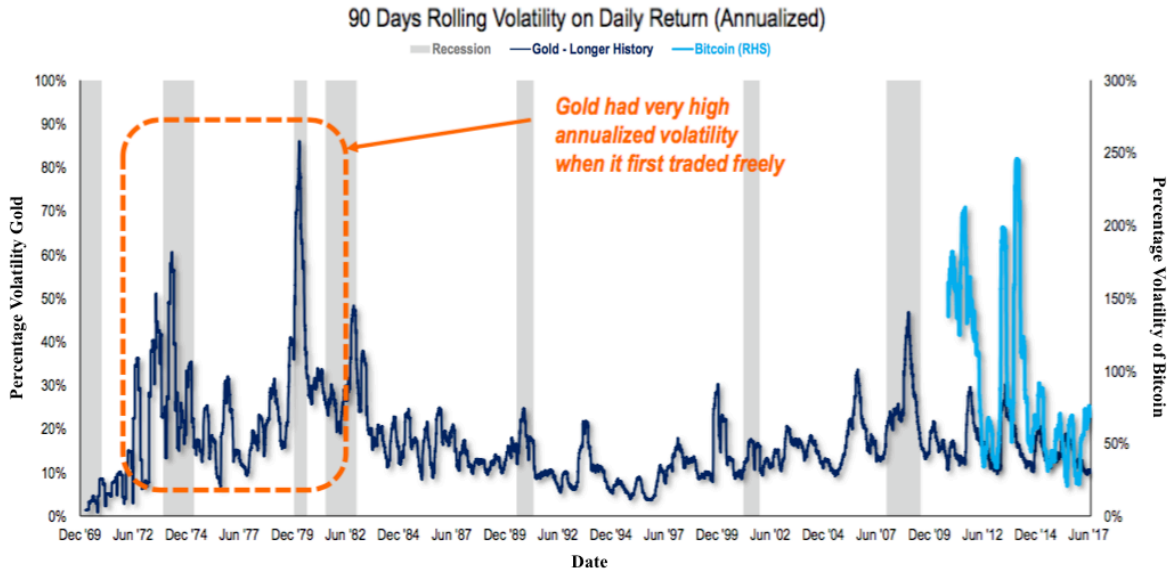
Figure 30. Volatility of Bitcoin vs. Gold and Select Fiat Currencies



Source: Goldmoney (2017, modified) [65]

As depicted above in Figure 30, gold's volatility exceeded that of bitcoin's for the first time in history. This is significant due to the fact that bitcoin is considered by many individuals to be extremely volatile while gold is considered relatively stable and constant. [65]

Figure 31. Volatility Comparison of Gold and Bitcoin (1969-2017)



Source: Fundstrat (2018, Thomas J. Lee & Co., modified) [71]

In Figure 31 above, one can see that gold's volatility in the 1970's is strikingly similar to bitcoin's price volatility around the early 2010's. Gold's volatility, seen in dark blue, is listed in percentage and is seen on the left hand side of the figure. Bitcoin's volatility, in light blue, is listed on the right hand side of the chart. The grayed out areas are periods of recession. [71]

A simple solution in order to benefit from the functions of bitcoin and its transaction ability without the worry of its volatility, is minimize the amount of time that it is held, in order to maximize its current purchasing power without running the risk of the value decreasing. Utilizing this theory: if a payment needs to be made, the exact amount in bitcoin (including the transaction fee) should be purchased with traditional currencies, after which the bitcoin payment should be sent. Contrarily, if a payment is received, the bitcoins should be immediately exchanged into the fiat currency of choice, minimizing the risk of price fluctuations. [65]

4.3.5. Liquidity of Bitcoin

As of March 28th, 2018, bitcoin's liquidity is about $2,420,000,000 USD, or about 1.8% of bitcoin's total market capitalization. Although the market capitalization share is relatively low, 2.4 billion USD speaks for itself — bitcoin has good market share, maturity, and acceptance, and is widely traded. [66]

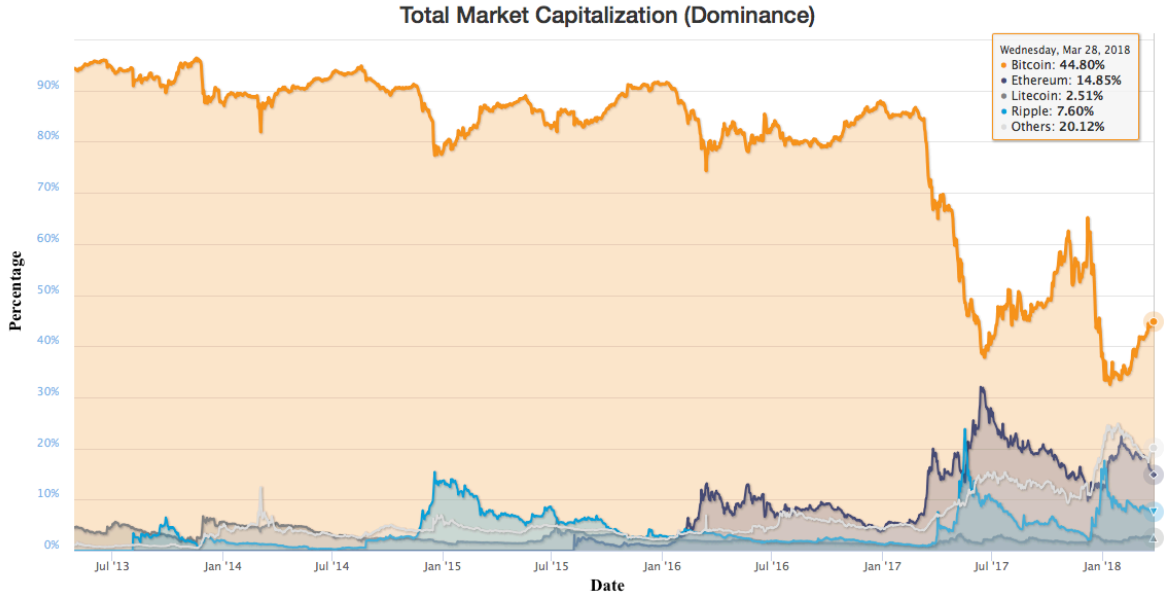
4.4. Bitcoin as a Longterm Store of Value

Bitcoin has been considered the "Swiss bank account in one's pocket" due to its useful properties that make it a prospective store of value as well as a positive investment for the future. Bitcoin's fixed supply, inability to counterfeit and double spend, and growing demand imply a growing price as the cryptocurrency continues to exhibit excellent characteristics as a longterm store of value. [63]

4.4.1. Bitcoin Dominance Among Other Cryptocurrencies

As seen below, Figure 32 shows the market dominance of bitcoin versus a few selected digital currencies. Combined, these cryptocurrencies add up to equal about 90% of all traded cryptocurrencies, as a few cryptocurrencies were omitted for graph clarity. [67]

Figure 32. Market Capitalization Dominance Among Cryptocurrencies (2013-2018)



Source: Coinmarketcap (2018, modified) [67]

From the figure above, it is clear that bitcoin is, and always has been the most dominant digital currency. On January 14th, 2018, bitcoin's dominance was at an all time low of 32.88%, but it is evident that its market capitalization was transferred over into other cryptocurrencies, rather than being lost or completely withdrawn from the digital currency world. When the price of other digital currencies diminishes, the total market capitalization of bitcoin rises, due to being the legacy and world's first and original cryptocurrency — individuals instill trust and reliability specifically into bitcoin. As of

March 28th, 2018, bitcoin's total market capitalization is at roughly 45% of all digital currency total market capitalization. [67]

No matter the cryptocurrency, except in a few cases, they all follow the price fluctuations and trends of bitcoin. Bitcoin is much more than just the original and legacy cryptocurrency, it is the leader and role model for all other cryptocurrencies. Bitcoin is to digital cryptocurrencies as the United States dollar is to the rest of the world's fiat currencies. [66]

4.4.2. Bitcoin Deflation

As more and more bitcoins gradually become lost, the rest of the accessible bitcoins are worth increasingly more. The total amount of bitcoins in circulation when all block rewards are given out is no longer 21 million, but rather around 16 or 17 million. Even without acquiring more bitcoins, the average value amount of one's bitcoins will rise over time due to the loss of other owner's bitcoins. [49]

4.4.3. Storability

Regardless of which wallet type is chosen, potential storage capacity is incredible, ranging from one Satoshi to (almost) 21 million bitcoin. It is irrelevant whether the owner has 0.00000001 BTC on his or her wallet, or 20,000,000 bitcoin on the wallet. In the case that the wallet is physical; the proportions, weight, and ability to transport are absolutely identical — independent from the amount of bitcoins stored. [43]

The most important deciding factor for the usefulness of a bitcoin wallet is not the initial wallet cost (or lack thereof), the size, the brand, or even the type. Instead, the most important factor is not only its ability of longterm storage, but rather its ability for future retrieval and transfer of the cryptocurrency on the wallet to someone in exchange for goods, services, or other currencies. Having all the bitcoin in the world may be *valued* at hundreds of billions of USD, but without the ability to transfer them to another individual or business, they are deemed *worthless* — even though the blockchain technology behind bitcoin is extremely useful and valuable in and of itself. [43]

4.4.4. Bitcoin Wealth Distribution

As with fiat currencies, the distribution of wealth in the cryptocurrency world greatly varies. Table 6 (below) starts with a logarithmic form bitcoin balance range, the amount of addresses within that range, the share of addresses within that range out of all addresses (the amount of equally wealthy or wealthier addresses are in percentage in parenthesis), the total amount of bitcoins within that balance range, the USD value of the total coins within that range (as of March 28th, 2018), and lastly; the share of bitcoins within the balance range out of all bitcoins (in parenthesis is the cumulative percentage of equally wealthy or wealthier bitcoin addresses). [68]

Table 6. Bitcoin Distribution of Wealth

Bitcoin distribution					
Balance	**Addresses**	**% Addresses (Total)**	**Coins**	**$USD**	**% Coins (Total)**
0 - 0.001	10561645	48.89% (100%)	2,101 BTC	16,497,021 USD	0.01% (100%)
0.001 - 0.01	4889937	22.64% (51.11%)	20,538 BTC	161,251,016 USD	0.12% (99.99%)
0.01 - 0.1	3805697	17.62% (28.47%)	121,404 BTC	953,199,432 USD	0.72% (99.87%)
0.1 - 1	1653546	7.65% (10.86%)	532,464 BTC	4,180,629,723 USD	3.16% (99.15%)
1 - 10	543631	2.52% (3.2%)	1,439,868 BTC	11,305,102,491 USD	8.54% (95.99%)
10 - 100	131087	0.61% (0.69%)	4,343,097 BTC	34,099,762,582 USD	25.77% (87.44%)
100 - 1,000	15641	0.07% (0.08%)	3,686,225 BTC	28,942,339,840 USD	21.88% (61.67%)
1,000 - 10,000	1540	0.01% (0.01%)	3,372,180 BTC	26,476,621,567 USD	20.01% (39.79%)
10,000 - 100,000	112	0% (0%)	2,992,497 BTC	23,495,546,755 USD	17.76% (19.78%)
100,000 - 1,000,000	2	0% (0%)	340,211 BTC	2,671,163,541 USD	2.02% (2.02%)

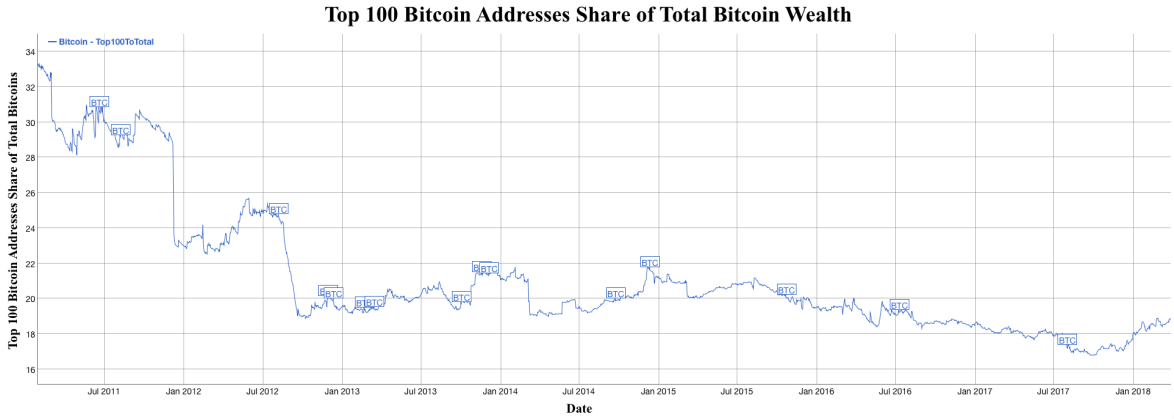
Addresses richer than						
1 USD	**100 USD**	**1,000 USD**	**10,000 USD**	**100,000 USD**	**1,000,000 USD**	**10,000,000 USD**
15,373,726	5,175,281	2,037,821	516,520	123,195	11,266	1,090

Source: Bitinfocharts (2018, modified) [68]

Near the bottom of Table 6 is the number of addresses wealthier than certain logarithmic USD amounts. The are over 15 million addresses with at least $1 USD worth of bitcoin and the number of addresses more than halves with each rise in dollar amount. Thanks to bitcoin, there are over 11,000 wallets with one million USD and more than 1,000 addresses with greater than 10 million USD. [68]

With most traditional economies and fiat currencies, the gap between the poor and the wealthy is ever widening; however, the opposite is true of bitcoin, as shown with Figure 33 on the following page. [69]

Figure 33. Top 100 Bitcoin Addresses Share of Total Wealth (2011-2018)



Source: Bitinfocharts (2018, modified) [69]

Apart from the slight rise at the end of 2017 and beginning of 2018, the percentage of the top 100 bitcoin addresses has been in steady decline since 2011, when the top 100 bitcoin wallets had more than one-third of all bitcoins in circulation. Once again, it is necessary to mention that the data is speculative because there is no way to prove or disprove the total amount of owners within the top 100, just like there is no way to prove or disprove how many individuals own more than one wallet. An individual with enough bitcoins to make it to the top 100 can easily split up his or her balance into two or more wallets in order to help conceal his or her identity, as well as disguise the fact that he or she should be in the top 100. Regardless of whether the share of the top 100 bitcoin wallets is decreasing as an illusion, as a result of the steady influx of new circulation, or as a result of demand from others, it is at least reassuring to see that the wealthiest of the wealthiest are not *increasing* their percentage stake of bitcoin. [69]

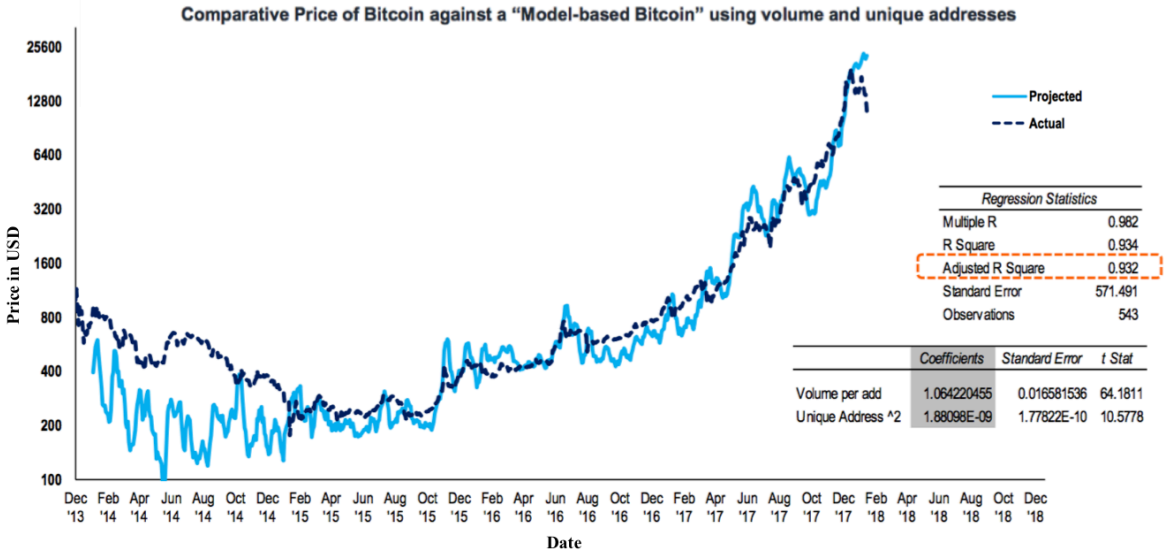
4.5. Bitcoin Network Affect — Metcalfe's Law Analysis

As the main theory for the multiple regression analysis, Metcalfe's Law was chosen to explain correlation between the market price of bitcoin (per one coin) and the squared number of unique users. [70]

Metcalfe's Law was formulated by Professor Robert Metcalfe, the inventor of Ethernet (not to be confused with Internet), around the 1980's. His theory revolves around the network affect, which is defined as "the value of a telecommunications network is proportional to the square number of connected users of the system (n^2)." Much like a telephone or fax machine, the more users there are — the more maximum utility can be harnessed from the network, both individually and as a whole. [70]

As the basis for the testing of this analysis, Fundstrat's "2018 Blockchain Outlook" was chosen. The global advisors group claim that they achieved a 93.2% adjusted R^2 using only two variables. The two variables used are the squared number of unique users and the USD volume per transaction. The goal is to recreate the data as closely as possible. Below in Figure 34 is an excerpt from the group's findings in order to make a comparison. [71]

Figure 34. Fundstrat's Comparative Bitcoin Analysis Using Metcalfe's Law



Source: Fundstrat (2018, Thomas J. Lee & Co., modified) [71]

Due to Fundstrat's near spot-on projection from about February 2015 to December 2017, [71] this was the chosen timeline for the linear regression. The regression analysis equations are as follows:

Simple economic model: $y_1 = f(x_1 + x_2)$

Multiple linear regression model: $\beta_1 y_1 = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \varepsilon$

Where:

y_1 = Market price of bitcoin (per coin)

x_1 = Number of unique users squared

x_2 = Estimated total value* in USD/transactions per day

ε = Residual value

*It is important to note that "estimated total value" (ETV) is an aggregated and approximated value that may be manipulated, regardless of the data source. It is necessary

to collect all data from the same source in order to undergo accurate analysis, and was done so from "www.blockchain.info." Blockchain defines the estimated total value as the total assumed value of transactions received by individuals in exchange for goods, services, or other currency on the Bitcoin blockchain — it does not include bitcoins returned to the sender as change during a transaction. [72]

Table 7. Metcalfe's Law Linear Regression Analysis Correlation Coefficients

	y_1	x_1	x_2
y_1	1		
x_1	0.80466219	1	
x_2	0.92693756	0.73824088	1

Source: Blockchain (2018, own calculations and creation) [72]

The independent variable x_1 (unique users squared) has a positive 80.5% correlation coefficient with the dependent variable y_1 (price of bitcoin) and the independent variable x_2 (estimated total value in USD divided by the number of transactions per day) has a positive 92.7% correlation coefficient with y_1. Variables x_1 and x_2 have a correlation coefficient of about 73.8%, meaning that multicollinearity does not exist among independent variables. Since variable x_2 has about a 12% higher correlation coefficient with y_1 than variable x_1 has with variable y_1, it can be said that Metcalfe's Law is less indicative of bitcoin's market price than variable x_2 is.

Table 8. Linear Regression Statistics

Regression Statistics	
Multiple R	0.943955086
R^2	0.891051204
Adjusted R^2	0.890630553
Standard Error	647.3861369
Observations	521

Source: Blockchain (2018, own calculations and creation) [72]

The number of observations chosen for the regression was 521, just shy of Fundstrat's 543 observations in their analysis. The value achieved for R^2 is about 89.1% (compared to Fundstrat's 93.4%) and the value for adjusted R^2 is about 89% (93.2% respectively). Although the R^2 values in this sample are slightly lower then Fundstrat's, they still help explain about 89% (with a 95% level of confidence) of bitcoin's movement through the use of two variables.

Table 9. Linear Regression Values

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%
Intercept	-606.1317076	51.7256439	-11.718205	2.7004E-28	-707.74954	-504.51388
x_1	4.14E-09	3.3637E-10	12.3034333	1.0658E-30	3.4777E-09	4.7993E-09
x_2	0.85275755	0.02505879	34.0302805	3.507E-134	0.8035282	0.90198689

Source: Blockchain (2018, own calculations and creation) [72]

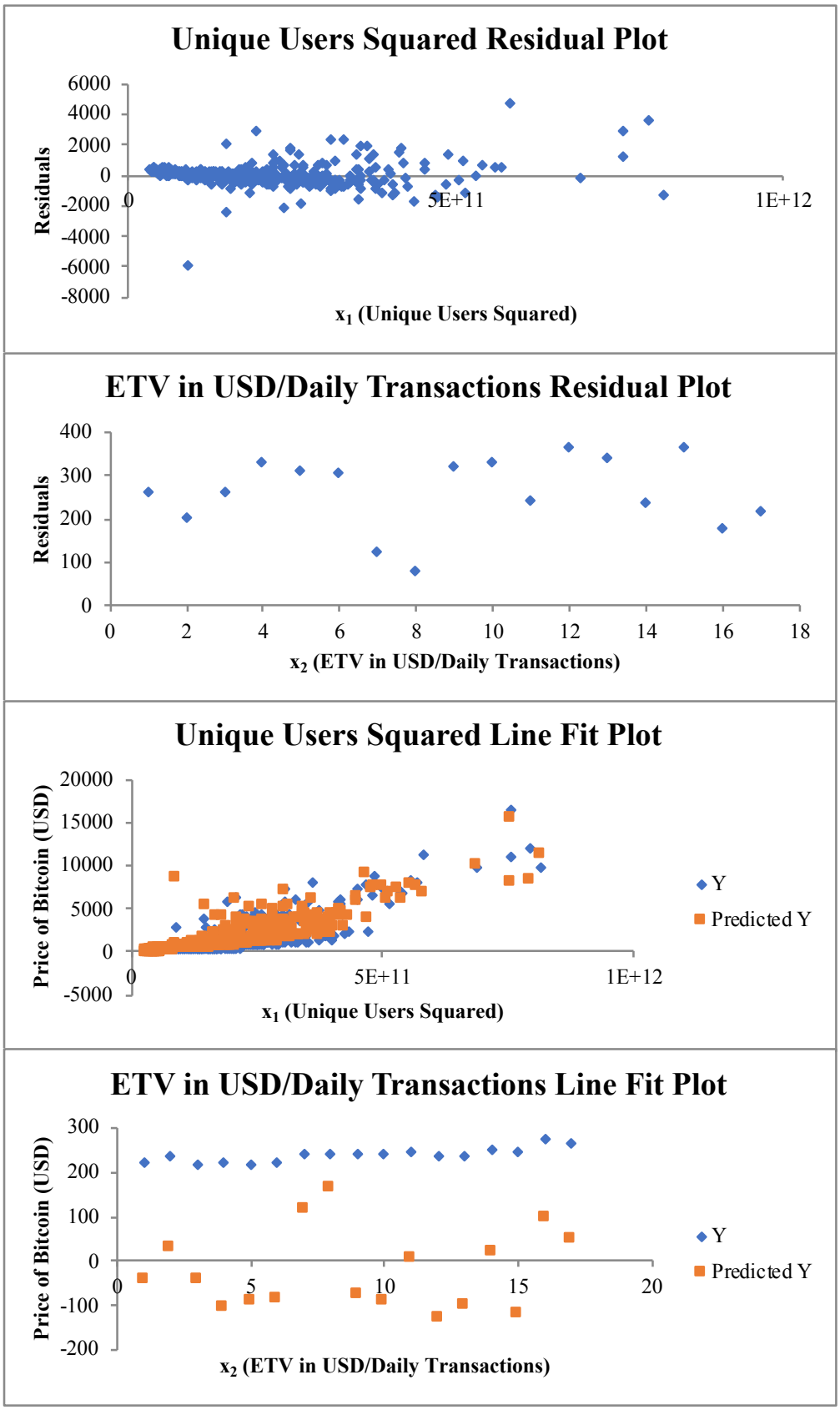
The econometric interpretation is as follows:

$$y_{1t} = -606.1317076 + (0.000002808)\, x_{1t} + (0.852757549)\, x_{2t} + u_t$$

The P-values for variables x_1 and x_2 are close to zero and less than 0.05, meaning they are both statistically significant within the model. When the number of unique users squared increases by one million units, the price of bitcoin increases by $2.808 per coin, ceteris paribus. When the estimated total value in USD divided by the number of transactions per day increases by one unit, the price of bitcoin increases $0.853, ceteris paribus. The constant variable is valued at about -$606.13.

Pictured on the following page in Figure 35 are the residual and line fit plots for the independent variables x_1 and x_2.

Figure 35. Spreadsheet Generated Residual and Line Fit Plots



Source: Blockchain (2018, own calculation and creation)

4.6. Bitcoin Mining Profitability Potential

Most individuals are well aware that bitcoin mining has not been profitable since 2013, except for a few exceptions. There are three main reasons for this, namely; mining was conducted part-time, often by individuals who had powerful gaming computers and processors with spare time and computing power. Next, most miners did not participate in mining for profit alone. Even though the blockchain rewards were enormous relative to today and the future, the price of bitcoin was insignificant compared to more recent valuations. Lastly, the existence and abundance of mining farms was nowhere near the number in operation at present. [73]

Previously, bitcoin mining occurred utilizing the computing power of graphics processing units (GPUs). Recently, the most effective way to mine bitcoins involves using application-specific integrated circuits (ASICs). [73]

4.6.1. Fixed Costs

For the profitability potential mining scenarios, the unanimously most popular "Antminer S9" device was chosen as the mining hardware. The device itself has a purchase price of about $2,000 and it is necessary to purchase a power supply for around $100. [74] Therefore, the total basic fixed costs are approximately $2,100 per mining device. For simplification, a single mining device is examined in the following scenarios. [73]

4.6.2. Variable Costs

The next cost that must be taken into consideration is electricity. The country chosen for the mining profitability scenarios is Iceland, due to its inexpensive cost of electricity in comparison with other similar countries, as well as the fact that 100% of Iceland's electricity supply comes from clean, renewable geothermal and hydroelectric resources. Yet another reason that Iceland was considered is due to the heat generated by the mining devices. Bitcoin mining in Iceland makes sense: the cold climate can help keep mining equipment from overheating, naturally cooling within mining facilities. Another, economical application for bitcoin mining is small households that rely on electricity for central heating. A few mining devices spread around households in strategic locations could replace traditional heating systems — conserving electricity all while creating revenue in the form of miner fees. Double purpose utilization is one way of offsetting the

price of mining equipment while simultaneously serving a necessary task: creating heat (which would require electricity in and of itself). [75]

The three mining scenarios include three potential kWh (kilowatt-hour) costs; $0.04, $0.10, and $0.16 USD per kWh. The remaining variables are listed in Figure 36, seen below.

Figure 36. Mining Profitability Variables

Difficulty Factor	3462542391191.6	
Hash Rate	13.5	TH/s
BTC/USD Exchange Rate	9000	
BTC/Block Reward	12.5	
Pool Fees %	1	
Hardware Cost (USD)	2100	
Power (Watts)	1375	
Power Cost (USD/kWh)	0.04 / 0.10 / 0.16	

Source: 99 Bitcoins (2018, modified) [73]

4.6.3. Mining Scenario Profit/Loss Periods

Figure 37. Estimated Profit Scenarios per kWh (4¢, 10¢, and 16¢ USD)

Duration	Calculation	Estimated Profit in USD
1 Day	Show Details	-2092.5846508627296
1 Week	Show Details	-2048.0925560391065
1 Month	Show Details	-1877.5395258818842
Half Year	Show Details	-750.4064570167641
1 Year	Show Details	606.6024351037422
Duration	**Calculation**	**Estimated Profit in USD**
1 Day	Show Details	-2094.5646508627296
1 Week	Show Details	-2061.952556039106
1 Month	Show Details	-1936.9395258818843
Half Year	Show Details	-1110.766457016764
1 Year	Show Details	-116.09756489625761
Duration	**Calculation**	**Estimated Profit in USD**
1 Day	Show Details	-2096.5446508627297
1 Week	Show Details	-2075.8125560391063
1 Month	Show Details	-1996.3395258818841
Half Year	Show Details	-1471.126457016764
1 Year	Show Details	-838.7975648962577

Source: 99 Bitcoins (2018, modified) [73]

As expected and clearly demonstrated in Figure 37 above, electricity cost has a significant impact on potential profit returns. All profit must be stated as speculative due to the lottery system used to reward bitcoin miners. Individual miners can join mining pools (group/network of miners) in order to improve the chance of becoming the rewarded miner or mining pool. Although miners in mining pools must pay a pool fee percentage, this is a good investment because it greatly increases the chances of profit, to what would otherwise most likely be zero revenue. [73]

In order to have a significant profit, it is crucial to have a low electricity tariff, efficient mining equipment, as many mining devices as possible, and good heat dissipation.

Below in Table 10 is a constructed calculation of past and future mining reward halving occurrences, with the block number, the amount of the block (reward in BTC), the past and predicted years of occurrence of the halving, the amount of bitcoin added per 210,000 block batch, the total amount of bitcoin in circulation at that halving, and finally; the amount of bitcoin remaining to be distributed into circulation in future blocks.

Table 10. Block Reward Calculations

Block	Block Reward in BTC	Occurrence (Predicted*)	BTC Added per 210,000 Blocks	Total Bitcoins in Circulation (BTC)	Bitcoin Rewards Remaining (BTC)
0	50.00000000	2009	10,500,000.0000	10,500,000.0000	10,499,999.9769
210,000	25.00000000	2013	5,250,000.0000	15,750,000.0000	5,249,999.9769
420,000	12.50000000	2016	2,625,000.0000	18,375,000.0000	2,624,999.9769
630,000	6.25000000	2021*	1,312,500.0000	19,687,500.0000	1,312,499.9769
840,000	3.12500000	2025*	656,250.0000	20,343,750.0000	656,249.9769
1,050,000	1.56250000	2029*	328,125.0000	20,671,875.0000	328,124.9769
1,260,000	0.78125000	2033*	164,062.5000	20,835,937.5000	164,062.4769
1,470,000	0.39062500	2037*	82,031.2500	20,917,968.7500	82,031.2269
1,680,000	0.19531250	2041*	41,015.6250	20,958,984.3750	41,015.6019
1,890,000	0.09765625	2045*	20,507.8125	20,979,492.1875	20,507.7894
2,100,000	0.04882812	2049*	10,253.9052	20,989,746.0927	10,253.8842
2,310,000	0.02441406	2053*	5,126.9526	20,994,873.0453	5,126.9316
2,520,000	0.01220703	2057*	2,563.4763	20,997,436.5216	2,563.4553
2,730,000	0.00610351	2061*	1,281.7371	20,998,718.2587	1,281.7182
2,940,000	0.00305175	2065*	640.8675	20,999,359.1262	640.8507
3,150,000	0.00152587	2069*	320.4327	20,999,679.5589	320.4180
3,360,000	0.00076293	2073*	160.2153	20,999,839.7742	160.2027
3,570,000	0.00038146	2077*	80.1066	20,999,919.8808	80.0961
3,780,000	0.00019073	2081*	40.0533	20,999,959.9341	40.0428
3,990,000	0.00009536	2085*	20.0256	20,999,979.9597	20.0172
4,200,000	0.00004768	2089*	10.0128	20,999,989.9725	10.0044
4,410,000	0.00002384	2093*	5.0064	20,999,994.9789	4.9980
4,620,000	0.00001192	2097*	2.5032	20,999,997.4821	2.4948
4,830,000	0.00000596	2101*	1.2516	20,999,998.7337	1.2432
5,040,000	0.00000298	2105*	0.6258	20,999,999.3595	0.6174
5,250,000	0.00000149	2109*	0.3129	20,999,999.6724	0.3045
5,460,000	0.00000074	2113*	0.1554	20,999,999.8278	0.1491
5,670,000	0.00000037	2117*	0.0777	20,999,999.9055	0.0714
5,880,000	0.00000018	2121*	0.0378	20,999,999.9433	0.0336
6,090,000	0.00000009	2125*	0.0189	20,999,999.9622	0.0147
6,300,000	0.00000004	2129*	0.0084	20,999,999.9706	0.0063
6,510,000	0.00000002	2133*	0.0042	20,999,999.9748	0.0021
6,720,000	0.00000001	2137*	0.0021	20,999,999.9769	0.0000
6,930,000+	0.00000000	2141*	0.0000	20,999,999.9769	0.0000

Source: Bitcoin Wiki (2018, own calculation and creation) [38]

4.7. SWOT

As a basic tool for strategical analysis, the SWOT method was chosen to give an overview of the aspects of bitcoin.

4.7.1. Strengths

- Linked to network that provides reliable proof of transaction history sequence
- High level of trust and anonymity
- No opening/closing prices and times for trading/buying
- Transaction fees are specified by the sender
- First original pioneer cryptocurrency legacy
- Strong bitcoin community
- Relatively fast transactions

4.7.2. Weaknesses

- Irreversible transactions
- Blocks become increasingly difficult to complete
- With each bitcoin owner being his or her “own bank” uninformed participators can misuse bitcoin
- The end of bitcoin miner rewards is imminent
- About 4 million bitcoins lost forever
- Complicated to grasp concept (not necessary for use)
- Like all currencies, possibility to support criminal activity
- Volatile and unstable

4.7.3. Opportunities

- No limit to the cumulative amount of bitcoin transactions that may take place in the future
- Two ways in which miners are motivated: mining rewards and transaction fees
- Paving the way for better and improved digital currencies
- Economic growth to individuals and regions which would have otherwise never seen success
- Technical development and advancement
- Possible to profit with bitcoin
- Possibility to run the network on 100% renewable resources in the future

4.7.4. Threats

- Establishment and fuzziness surrounding the history of bitcoin leaves it vulnerable to be undermined and questioned by experts and governments
- Possible for attacker nodes to gain CPU power (51% attack, albeit near impossible)
- Bitcoins can be hacked, stolen, or compromised

4.8. PESTLE

As the second basic tool for strategical analysis, the PESTLE method was chosen to give an even more analytical overview of the characteristics of bitcoin.

4.8.1. Political

- No need to go through financial institutions
- Some countries purposely try to stop the usage of bitcoin
- In some places, not recognized as legal tender at all
- Since it is universal, countries will either have to agree on how it will be controlled everywhere or problems can arise between countries

4.8.2. Economical

- Bitcoin led to the flourishing of other cryptocurrencies that provide competition and keep Bitcoin from becoming a monopoly
- Steady supply of bitcoin being put into circulation
- Max number of bitcoins in existence means miner reward is continuously halved
- Millions of bitcoins are eternally lost and unaccounted for
- Possible micropayments decrease and unable to do high-volume transactions

4.8.3. Social

- Makes P2P transaction more feasible/accessible
- Global access makes it very cosmopolitan; connects people from all over the world
- No central authority because of lottery-system that prevents conflicts
- To preserve the limited blocks that can be mined, needs to be a transition to miners being incentivized by transaction fees to get their profit from those
- Bitcoin/cryptocurrency community help each other

4.8.4. Technological

- Employs the use of computers; it is fully reliant on technology and electricity to function
- Technical peculiarities can contribute to loss of bitcoins

4.8.5. Legal

- Bitcoin is fully prohibited in some countries by law; it is restricted by others
- Still is attached to some sort of tax liability
- Nongovernmental unit - unprecedented in figuring out how to regulate it and what kind of power governments have over it
- Complicated “gray area” tax laws
- Short-term and longterm capital gains taxes

4.8.6. Environmental

- Uses a lot of electricity, and since most is harnessed from the burning of fossil fuels, the atmosphere is polluted
- Done electronically, so does not require deforestation for paper production

5. Conclusion

In conclusion, bitcoin is a one of a kind legacy cryptocurrency whose future fate is neither known nor accurately predictable. What is certain however, is the limited amount of bitcoins, combined with the enormous number of lost bitcoins that will never be replaced or reintroduced. This creates a dwindling limited supply and any amount of bitcoin has extreme potential to be enormously valuable. With every passing day, the opportunity to own bitcoin decreases, as more and more individuals and businesses accept, own, and use bitcoins in everyday situations.

The most important factor in owning bitcoin is not how much is owned, but rather how and where it is stored, and whether the owner has access to the cryptocurrency. Having all the bitcoin in the world may be *valued* at hundreds of billions of USD, but without the ability to transfer them to another individual or business, they are deemed *worthless*.

Using Metcalfe's Law to explain the network effect with bitcoin, it is possible to explain about 89% of bitcoin's fluctuation in price with the number of unique users and the average transaction amount in USD (with a 95% level of confidence).

Although mining is not considered substantially profitable, it is justifiable in regions where electricity is free or nearly free, especially in areas with cold climates. The persistence of technological advancement will continue to increase the computational abilities of mining equipment and mining will remain profitable for large-scale operations even if the price of electricity increases. Mining will regulate and oversee itself; if miners are profitable, they will keep mining, and if mining becomes unprofitable in one region; it opens up new mining opportunities in other areas.

Bitcoin is the ultimate form of money in electronic form. There are no restrictions as to accessing one's wallet, sending or receiving money, or what the purchased goods and services include. When used properly, it is possible to create total anonymity from the rest of the world, something that has value in and of itself. The world may only wait and see where the power of bitcoin will take it.

As a final piece of wisdom — the biggest regret with bitcoin is not wishing to have invested earlier when the price of bitcoin was lower. The biggest regret is not the price of bitcoin decreasing after having already purchased. By far, the biggest regret involved with owning bitcoin is having had purchased it when the price was low, and not having access to the coins later, when the value has risen.

6. References

[1] Investopedia. (2018). *What is Money?*. [online] Available at: https://www.investopedia.com/insights/what-is-money/ [Accessed 27 Mar. 2018].

[2] University of Minnesota. (2018). *24.1 What Is Money? | Principles of Economics*. [online] Available at: https://open.lib.umn.edu/principleseconomics/chapter/24-1-what-is-money/ [Accessed 27 Mar. 2018].

[3] Investopedia. (2018). [online] Available at: https://www.investopedia.com/terms/m/mediumofexchange.asp. [Accessed 27 Mar. 2018].

[4] Investopedia. (2018). [online] Available at: https://www.investopedia.com/terms/m/money.asp. [Accessed 27 Mar. 2018].

[5] The Telegraph. (2018). [online] Available at: https://www.telegraph.co.uk/finance/businessclub/money/11174013/The-history-of-money-from-barter-to-bitcoin.html. [Accessed 27 Mar. 2018].

[6] Investopedia. (2018). [online] Available at: https://www.investopedia.com/corp/about.aspx. [Accessed 27 Mar. 2018].

[7] Mankiw, N. Gregory (2014). Principles of Economics. p. 220. ISBN 978-1-285-16592-9. https://books.google.cz/books?id=3ubKAgAAQBAJ&pg=PA220&redir_esc=y#v=onepage&q&f=false.

[8] Bank for International Settlements. (2018). [online] Available at: https://www.bis.org/publ/rpfx16fx.pdf. [Accessed 27 Mar. 2018].

[9] Travelex. (2018). [online] Available at: https://www.travelex.com/currency/current-world-currencies. [Accessed 27 Mar. 2018].

[10] Federal Reserve Bank of Kansas City (2018). [online] Available at: https://www.kansascityfed.org/LNQfZ/QafSZ/bXjLb/cQMLW/publicat/econrev/pdf/12q2Hayashi-Keeton.pdf. [Accessed 27 Mar. 2018].

[11] Vlasák, Dominik. Economic Analysis of Small Dairy Farm in Sumava. Prague: Czech University of Life Sciences, Faculty of Economics and Management, Department of Economics, 2015. 36 pages. Bachelor Thesis supervisor Ing. Petr Procházka, MSc, Ph.D.

[12] United States Census Bureau. 2015. *Population Clock*. [ONLINE] Available at: http://www.census.gov/popclock/?intcmp=home_pop. [Accessed 05 March 2015].

[13] International Telecommunications Union. (2018). [online] Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. [Accessed 27 Mar. 2018].

[14] Investopedia. (2018). [online] Available at: https://www.investopedia.com/terms/p/purchasingpower.asp. [Accessed 27 Mar. 2018].

[15] Wells Fargo. (2018). [online] Available at: https://www08.wellsfargomedia.com/assets/pdf/personal/investing/investment-institute/wfii_golds_uniqueness_022717_ADA.pdf. [Accessed 27 Mar. 2018].

[16] Federal Reserve Bank of Dallas. (2018). [online] Available at: https://www.dallasfed.org/institute/update/2017/int1707. [Accessed 27 Mar. 2018].

[17] Investopedia. (2018). [online] Available at: https://www.investopedia.com/terms/c/centralbank.asp. [Accessed 27 Mar. 2018].

[18] St, Louis Federal Reserve. (2018). *FRED Graph | FRED | St. Louis Fed*. [online] Available at: https://fred.stlouisfed.org/graph/?g=76PN#0. [Accessed 27 Mar. 2018].

[19] BullionVault. (2018). [online] Available at: https://www.bullionvault.com/gold-news/gold-price-091320163. [Accessed 27 Mar. 2018].

[20] Anonymous. (2018). [online] Available at: http://jennyxzkong.blogspot.cz/2012/05/champagne-glass-distribution-of-wealth.html. [Accessed 27 Mar. 2018].

[21] Business Insider. (2018). [online] Available at: http://www.businessinsider.com/chart-of-recent-global-economic-activity-2014-1. [Accessed 27 Mar. 2018].

[22] The Economist. (2018). *The Economist - World News, Politics, Economics, Business & Finance*. [online] Available at: https://www.economist.com/news/finance-and-economics/21707219-charting-globalisations-discontents-shooting-elephant. [Accessed 27 Mar. 2018].

[23] Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. (PDF). [cit. 2018-03-05]. Available at: https://bitcoin.org/bitcoin.pdf.

[24] Bitcoin Wiki. (2018). [online] Available at: https://en.bitcoin.it/wiki/Help:FAQ. [Accessed 27 Mar. 2018]. [[[32]]]

[25] Hendricks, B. (2018). *Bitcoin: What's in the whitepaper?*. [online] Bbntimes.com. Available at: https://www.bbntimes.com/en/technology/bitcoin-what-s-in-the-whitepaper [Accessed 27 Mar. 2018].

[26] Bernard, Z. (2018). *Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator*. [online] Business Insider. Available at: http://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12 [Accessed 27 Mar. 2018].

[27] Bitcoin.it. (2018). *Block - Bitcoin Wiki*. [online] Available at: https://en.bitcoin.it/wiki/Block [Accessed 27 Mar. 2018].

[28] Coinmarketcap. (2018). *All Cryptocurrencies | CoinMarketCap*. [online] Available at: https://coinmarketcap.com/all/views/all/ [Accessed 27 Mar. 2018].

[29] CryptoCurrency Facts. (2018). *CoinMarketCap.Com (Website) - CryptoCurrency Facts*. [online] Available at: https://cryptocurrencyfacts.com/exchanges/coinmarketcap-com/ [Accessed 27 Mar. 2018].

[30] CoinGecko. (2018). *Bit20 Price Chart (BTWTY/USD) | CoinGecko*. [online] Available at: https://www.coingecko.com/en/price_charts/bit20/usd [Accessed 27 Mar. 2018].

[31] Blockexplorer. (2018). [online] Available at: https://blockexplorer.com/api/status?q=getBlockCount [Accessed 27 Mar. 2018].

[32] Bitcoin.org. (2018). *FAQ - Bitcoin*. [online] Available at: https://bitcoin.org/en/faq [Accessed 27 Mar. 2018].

[33] Bitcoin.it. (2018). *Help:Introduction - Bitcoin Wiki*. [online] Available at: https://en.bitcoin.it/wiki/Help:Introduction [Accessed 27 Mar. 2018].

[34] Map.bitlegal.io. (2018). *BitLegal - Welcome*. [online] Available at: http://map.bitlegal.io/ [Accessed 27 Mar. 2018].

[35] Wikipedia.org. (2018). *Legality of bitcoin by country or territory*. [online] Available at: https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory [Accessed 27 Mar. 2018].

[36] CoinDesk. (2018). *Bitcoin gaining market-based legitimacy as XBT - CoinDesk*. [online] Available at: https://www.coindesk.com/bitcoin-gaining-market-based-legitimacy-xbt/ [Accessed 27 Mar. 2018].

[37] Bitcoin.it. (2018). *Bitcoin symbol - Bitcoin Wiki*. [online] Available at: https://en.bitcoin.it/wiki/Bitcoin_symbol [Accessed 27 Mar. 2018].

[38] Bitcoin.it. (2018). *Controlled supply - Bitcoin Wiki*. [online] Available at: https://en.bitcoin.it/wiki/Controlled_supply [Accessed 27 Mar. 2018].

[39] CoinDesk. (2018). *The Blockchain Lottery: How Miners Are Rewarded - CoinDesk*. [online] Available at: https://www.coindesk.com/blockchain-lottery-miners-rewarded/ [Accessed 27 Mar. 2018].

[40] Mining?, W. (2018). *What is the Bitcoin Mining Block Reward?*. [online] Bitcoinmining.com. Available at: https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/ [Accessed 27 Mar. 2018].

[41] Blockchain.info. (2018). *Bitcoins in circulation*. [online] Available at: https://blockchain.info/charts/total-bitcoins [Accessed 27 Mar. 2018].

[42] Bitcoinblockhalf. (2018). *Bitcoin Block Reward Halving Countdown*. [online] Available at: http://www.bitcoinblockhalf.com/ [Accessed 27 Mar. 2018].

[43] CoinDesk. (2018). *How to store your bitcoins - bitcoin wallets - CoinDesk*. [online] Available at: https://www.coindesk.com/information/how-to-store-your-bitcoins/ [Accessed 27 Mar. 2018].

[44] aBitGreedy. (2018). *Bitcoin Guide 2018 | If You Read This You'll Become a Bitcoin Expert*. [online] Available at: https://www.abitgreedy.com/bitcoin/ [Accessed 27 Mar. 2018].

[45] Blockchain. (2018). *Average Number Of Transactions Per Block*. [online] Available at: https://blockchain.info/charts/n-transactions-per-block [Accessed 27 Mar. 2018].

[46] Bitcoin Market Journal. (2018). *How Many People Use Bitcoin? Updated for 2018 – Bitcoin Market Journal*. [online] Available at: https://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/ [Accessed 27 Mar. 2018].

[47] Bitinfocharts. (2018). *Bitcoin Avg. Transaction Fee vs. Median Transaction Fee chart*. [online] Bitinfocharts.com. Available at: https://bitinfocharts.com/comparison/transactionfees-median_transaction_fee-btc.html [Accessed 27 Mar. 2018].

[48] Bitinfocharts. (2018). *Bitcoin (BTC) statistics - Price, Blocks Count, Difficulty, Hashrate, Value*. [online] Available at: https://bitinfocharts.com/bitcoin/ [Accessed 27 Mar. 2018].

[49] Fortune. (2018). *Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says*. [online] Available at: http://fortune.com/2017/11/25/lost-bitcoins/ [Accessed 27 Mar. 2018].

[50] En.bitcoin.it. (2018). *Transaction fees - Bitcoin Wiki*. [online] Available at: https://en.bitcoin.it/wiki/Transaction_fees [Accessed 27 Mar. 2018].

[51] Banking on Bitcoin. (2016). [film] USA: Christopher Cannucciari.

[52] Bitcoin.it. (2018). *Maximum transaction rate - Bitcoin Wiki*. [online] Available at: https://en.bitcoin.it/wiki/Maximum_transaction_rate [Accessed 31 Mar. 2018].

[53] Bitinfocharts. (2018). *Bitcoin Transactions chart*. [online] Bitinfocharts.com. Available at: https://bitinfocharts.com/comparison/bitcoin-transactions.html [Accessed 31 Mar. 2018].

[54] Chokun, J. (2018). *Who Accepts Bitcoins As Payment? List of Companies*. [online] 99 Bitcoins. Available at: https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/ [Accessed 31 Mar. 2018].

[55] Coinmap.org - Map of Bitcoin accepting venues. (2018). *coinmap.org - Bitcoin accepting shops, ATM's & venues.*. [online] Available at: https://coinmap.org/#/map [Accessed 31 Mar. 2018].

[56] Wikipedia.org. (2018). *Bitcoin scalability problem*. [online] Available at: https://en.wikipedia.org/wiki/Bitcoin_scalability_problem [Accessed 31 Mar. 2018].

[57] Bitinfocharts. (2018). *Bitcoin Sent in USD chart*. [online] Bitinfocharts.com. Available at: https://bitinfocharts.com/comparison/sentinusd-btc.html [Accessed 31 Mar. 2018].

[58] Bitinfocharts. (2018). *Bitcoin Avg. Transaction Value chart*. [online] Bitinfocharts.com. Available at: https://bitinfocharts.com/comparison/transactionvalue-btc.html [Accessed 31 Mar. 2018].

[59] Bitinfocharts. (2018). *Bitcoin Median Transaction Value chart*. [online] Bitinfocharts.com. Available at: https://bitinfocharts.com/comparison/bitcoin-mediantransactionvalue.html [Accessed 31 Mar. 2018].

[60] Buntinx, J. (2018). *Coinmarketcap Is Now More Popular Than WSJ.com According to Alexa*. [online] The Merkle. Available at: https://themerkle.com/coinmarketcap-is-now-more-popular-than-wsj-com-according-to-alexa/ [Accessed 31 Mar. 2018].

[61] Bitcoin.it. (2018). *Buying Bitcoins (the newbie version) - Bitcoin Wiki*. [online] Available at: https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version) [Accessed 31 Mar. 2018].

[62] Schwarz, M. and Schwarz, M. (2018). *What Are Forks? + The Main Forks of Bitcoin and Ethereum Explained*. [online] aBitGreedy. Available at: https://www.abitgreedy.com/forks/ [Accessed 31 Mar. 2018].

[63] Bitcoin.it. (2018). *Bitcoin as an investment - Bitcoin Wiki*. [online] Available at: https://en.bitcoin.it/wiki/Bitcoin_as_an_investment [Accessed 31 Mar. 2018].

[64] Bitinfocharts. (2018). *Bitcoin Price in USD chart*. [online] Bitinfocharts.com. Available at: https://bitinfocharts.com/comparison/bitcoin-price.html [Accessed 31 Mar. 2018].

[65] Goldmoney. (2018). [online] Available at: https://www.goldmoney.com/images/media/Files/Insights/Research--BTC-AU-1.pdf [Accessed 31 Mar. 2018].

[66] CoinGecko. (2018). *CoinGecko: 360 Degree Overview of Cryptocurrencies Chart*. [online] Available at: https://www.coingecko.com/en [Accessed 31 Mar. 2018].

[67] Coinmarketcap. (2018). *Global Charts | CoinMarketCap*. [online] Available at: https://coinmarketcap.com/charts/#dominance-percentage [Accessed 31 Mar. 2018].

[68] Bitinfocharts. (2018). *Top 100 Richest Bitcoin Addresses and Bitcoin distribution*. [online] Bitinfocharts.com. Available at: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html [Accessed 31 Mar. 2018].

[69] Bitinfocharts. (2018). *Bitcoin Top100ToTotal chart*. [online] Bitinfocharts.com. Available at: https://bitinfocharts.com/comparison/top100cap-btc.html [Accessed 31 Mar. 2018

[70] Medium. (2018). *Valuing Bitcoin and Ethereum with Metcalfe's Law – Clearblocks – Medium*. [online] Available at: https://medium.com/@clearblocks/valuing-bitcoin-and-ethereum-with-metcalfes-law-aaa743f469f6 [Accessed 31 Mar. 2018].

[71] Bdadvanced. (2018). [online] Available at: https://bdadvanced.ipreo.com/OpenFileLink.aspx?ID1=ddcae35b-1b89-44fb-8a5e-00b9bfd6790c&ID2=475204051 [Accessed 31 Mar. 2018].

[72] Blockchain. (2018). *Bitcoin Charts & Graphs - Blockchain*. [online] Available at: https://blockchain.info/charts [Accessed 31 Mar. 2018].

[73] 99 Bitcoins. (2018). *Is Bitcoin Mining Worth It as we Start 2018?*. [online] Available at: https://99bitcoins.com/bitcoin-mining-worth-it/ [Accessed 31 Mar. 2018].

[74] Drake, N. (2018). *Best ASIC devices for Bitcoin mining in 2018*. [online] TechRadar. Available at: https://www.techradar.com/news/best-asic-devices-for-bitcoin-mining-in-2018 [Accessed 31 Mar. 2018].

[75] Usfunds. (2018). *Desperately Seeking a Cheaper Kilowatt Hour - U.S. Global Investors*. [online] Available at: http://www.usfunds.com/investor-library/frank-talk/desperately-seeking-a-cheaper-kilowatt-hour/#.Wr_qxIhubIU [Accessed 31 Mar. 2018].

[76] Antonopoulos, Andreas M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* 1st ed., Sebastopol, CA: O'Reilly Media, 2014. 298 pages. ISBN: 1449374042.

[77] Burniske, Chris, and Jack Tatar. *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond.* 1st ed., New York, NY: McGraw-Hill Education, 2017. 368 pages. ISBN: 1260026671.

[78] Frisby, Dominic. *Bitcoin: The Future of Money?* London: Unbound, 2014. 304 pages. ISBN: 1783520779.

[79] Popper, Nathaniel. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money.* New York, NY: Harper Paperbacks, 2015. 432 pages. ISBN: 006236250X.

[80] Vigna, Paul, and Michael J. Casey. *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic Order.* New York, NY: Picador/St. Martin's Press, 2016. 384 pages. ISBN: 1250081556.