**Bitcoin: My Two Bits**

**\*\*\*\*\*\***

Make a section where users can get together to fight back against the bad media surrounding bitcoin. Maybe it could be a forum where users can post articles and subscribe to newsletter with links to the bad media targeting bitcoin so that the community can respond with comments.

**\*\*\*\*\*\***

**Affiliate links for website**

[todo make a page on bitcoinusd.info with all affiliates]

http://www.sharethebtc.com/#whatis

**\*\*\*\*\*\***

[Erik Voorhees](http://moneyandstate.com/bitcoin-value-ponzi-schemes/#)

Erik Voorhees is among the top-recognized serial Bitcoin advocates and entrepreneurs, understanding Bitcoin as one of the most important inventions ever created by humanity. Having been a featured guest on Bloomberg, Fox Business, CNBC, BBC Radio, The Peter Schiff Show, and numerous Bitcoin and industry conferences, Erik humbly suggests that there is no such thing as a “free market” when the institution of money itself is centrally planned and controlled. This blog is about the human struggle for the separation of money and state, and about Bitcoin as the instrument by which it will happen.

<http://moneyandstate.com/bitcoin-value-ponzi-schemes/>

**\*\*\*\*\*\***

e-mail to bitcoin (a user could attach bitcoin to an e-mail)

**\*\*\*\*\*\***

Find partners to help write this book. Maybe someone that focuses on writing and is also tech savvy.

**\*\*\*\*\*\***

I can provide Bitcoin Mining Setup for homes and businesses. I will assist in buying and setting up the mining equipment. If you have space, electricity and cash, it might be a great investment. The price is currently $285/bitcoin but it spiked to over $1100 about a year ago. If the Bitcoin economy takes off, a single bitcoin could be worth thousands. You can buy bitcoin now at some of the popular exchanges more easily than this. You can do that on your own. This ad is specifically for people that might be interested in setting up mining equipment at their home or office. The mining equipment is loud, so you would not want the equipment set-up in your living quarters.

**\*\*\*\*\*\***

Make a business plan to set-up bitcoin mining operation in the barn. Calculate the math for the costs of the hardware, electricity, rent, redoing walls, etc… for 1 year and try to get business loan for that amount. Pitch the profits from the bitcoin and the profits from leasing out space to others that are interested.

\*\*\*\*\*\*

Make a website that gives 1 uBit to each unique email/bitcoin address - freemicrobit.io

**\*\*\*\*\*\***

Find a datacenter in argentina that will host hardware at cheap electricity costs. Rent a warehouse down there and hire people to monitor it. Find investors to fund it. It will get bitcoin for cheaper than the market rate if done by a crowd. Start a crowdfunding campaign to pay for it. User’s could get a share in the business. Money would be used to create the bitcoin and hold on to it until it hit a certain threshold. The threshold could be voted on by the community depending on how much they paid into it.

**\*\*\*\*\*\***

**What Can Bitcoins Be Valued At**

The value of a bitcoin could fall to a low level if there weren’t a lot of people that used it. If they were worth $1 each, then the maximum transaction would be about $14 Million and thats if they were all used in a single transaction. In international trade, that is a very small amount. If they were valued at $1,000.00 each, then they would all be worth $14 Billion. “trading in foreign exchange markets averaged $5.3 trillion per day in April 2013 (<http://en.wikipedia.org/wiki/Foreign_exchange_market>)”. If Bitcoin was to be used by a larger percentage of people to do these types of exchange, that would require the price of bitcoins to be at a minimum price. For large organizations or individuals that want to trade a billion or more dollars worth of bitcoin, then they would either have to buy about a quarter of all bitcoins in circulation. I don’t think it is unlikely for the price of bitcoins to go back up near $1,000 in the not too distant future based on how much trade happens every day in the international community. I’m not sure how accurate it is using the $5.3 trillion worth of trading in foreign exchange markets per day as an example. The actual number might be higher because this may not include every single trade between every single person on the planet in a given day. There is no way to record that as of now. Possibly in the future, all transactions on our planet would have to be recorded by some international law or treaty. That would be hard to control unless if all transactions had to be done electronically and linked to an identity. [todo <https://blockchain.info/charts/estimated-transaction-volume-usd> https://blockchain.info/charts/market-cap]

**Other Open Decentralized Networks**

Search Engines, Email, Social Networks. These could all be created in a similar fashion. They would cut out the big players that are making a huge cut in users online activities. If a community of servers could solve problems like search, social networks, shopping, almost any human to human interaction that we do with a computer. There could be nodes like “miners” in Bitcoin that would contain the correct answers for user queries. The network could intelligently organize any information and reward the organizers. An open source catalog could contain a valid list of the cheapest products that anybody could purchase. All of the computers would work together to locate the best available products for the lowest price. The could connect businesses with consumers and cut out the costs of a third party like Amazon.

**Introduction**

Bitcoin takes the bankers out of banking. It takes the treasury out of money. It takes the 3rd party out of transactions. The e-book will go over some of the basics of Bitcoin. Bitcoin is a international, decentralized network that contains a blockchain with stores of value in it at certain addresses. A user would need a password [and private key?] to access that address. Users can make transactions that transfer bitcoin from one address to another. The blockchain is an open network where anybody willing to participate is allowed if they follow the rules. In this document, I will write about some of the most important parts of the entirety of Bitcoin. I will also give my opinion on the state of the related market surrounding Bitcoin. The glossary contains information about the underlying technologies behind Bitcoin.

**History of Bitcoin**

**Is Bitcoin a Ponzi Scheme**

By no means is Bitcoin a ponzi scheme. It provides very valuable services. Bitcoin is not being sold either. A bitcoin is a store of value on the Bitcoin network. This store of value can be sent or received by anybody else with a wallet from bitcoin. This transfer of value is the same service that the major credit card companies provide. Yet, Bitcoin provides the service for nearly free or potentially free. Credit card companies charge huge fees [todo cite this] to transfer wealth from one individual to another. Take a look at how much Western Union charges to transfer money from person A in one country to person B from another country. This would be like calling the internet a ponzi scheme or calling email a ponzi scheme. Bitcoin is a protocol. That means it is just a set of standard rules that a network must follow. The rest of the network can verify if any single node is not following the rules and not accept the work that they performed. Data center provide their processing power for a fee to businesses that need a website. E-mail is free for the end user because the companies that are paying for the hosting is also placing ads and making revenues from the users that way. Since Bitcoin is such a useful financial instrument, it is not a ponzi scheme. A ponzi scheme can’t be selling a useful product. When you buy bitcoins, you are buying a tool to make trading goods and services more easily. The USD is a tool to make trading goods and services more easily. Gold used to be a good store of wealth and excellent to trade for goods and services. However, it is very inefficient to send gold back and forth between people. The dollar was a receipt of gold before they detached its value from gold. It was then set by how much money they print and what people can get with the money that they have. Some financial institutions provide services like Bitcoin does, but they charge a large amount of fees to use it. Even if Bitcoin is not successful, it will be a competitor to the current financial markets and force them to lower the prices or risk losing customers. The current institutions might try to make up for their losses by increasing their prices even more. This would, in turn, make more people try to find alternative sources.

**Bitcoin Has a Bad Name**

**Push vs. Pull**

Credit cards are a pull technology. That is, when you go to purchase a service or product, you are giving your credit card and identification information and they making a request for funds to your credit card company. The credit card company then authorizes the transaction resulting in the *pull transaction*. With bitcoin, you are sending money to the merchant directly. They don’t even have to authorize you sending them money. This is called a *push transaction*.

**Recurring Payments**

**Bitcoin ATMs (BTMs)**

**Following the Chain**

Imagine that you could follow the chain of where your money came from. With Bitcoin, you can do that. You can see where the bitcoins was created and to which accounts they were sent to by following the chain of transactions that led the money to you. Some could argue that this is an invasion of privacy. Once a person that owns some bitcoins is identified, that person can be attached to bitcoins that were used in illegal transactions. I would recommend to only purchase bitcoins from a reputable source. If you don’t, then possibly your bitcoins could be seized by a government. A court order could be made stating that you turn over your wallet, private key and password to authorities. This can be a good way to track down criminals online but some crimes are controversial such as marijuana. Could the authorities use Bitcoin to track down all the people that buy marijuana with bitcoins once they bust some dealer that has collected bitcoins from a large number of pot purchasers? Yes, they could. I don’t think the efforts would be made for small time criminals, but for larger more organized criminals, the authorities will have an extra tool to investigate. However, the criminals have access to the most advanced financial infrastructure to have ever existed on our planet. The general population does not even know about Bitcoin yet. However, criminals are using it everyday to transfer funds over borders instantly to anybody, anywhere at anytime.

**Post E-Finance**

What happens after technology takes over finance? Is the next sight on politics? Will computers handle international laws as they are starting to handle all financial transactions? There might be a autonomous system where there are an agreed upon set of laws. The system will be able to monitor all people and enforce the laws. There will be no single person that can go around the current laws. The system would be much more efficient than the current system since there are so many loopholes and contradictions in laws across borders. Will there be some blockchain technology that has all the laws that humans must abide by? The system could reward people that follow and uphold the law and it could punish people that do not follow the law. Having such a system in place might be better than the patchwork of laws that we currently have. Are there some undeniable truths about what is right and what is wrong? If an alien civilization came to our planet, would there laws be nearly identical to our own laws? There are some many thoughts to ponder about what will happen with technology in general.

**Centralization vs Decentralization**

There will have to be a balance between the two. Pure centralization would mean there is one large organization that controls everything. Pure decentralization would mean that each person contributes their own to the system. There must be a balance between the two. We can’t go too far in either direction or we won’t progress with technology.

**Fire Proof Safe**

It is necessary to keep hard copies of bitcoin in fire proof safes. A business surrounding bitcoin storage will arise.

**Independent Banks**

A high school student will have the power to start their own bank.

**Western Union**

**Banks**

**Cloud Mining Exchange**

Cloud mining is when a mining company sells the shares of their mining hardware. This is done by selling Gh/s, that is Gigahash per second. People make bids to buy or sell a certain number of Gh/s at a certain price. When someone owns the shares they get the earnings that were made from the last block that was solved. The mining company will subtract the maintenance fees from the earnings. Once the maintenance fees are higher than the earning for 10 consecutive days, they will retire the old hardware. They have generations of hardware for sale and the latest hardware gets the most earnings for the least maintenance fees. The profits made from the shares can be used to purchase more shares. And the shares that are owned can be listed in the exchange as for sale and at a higher price than what they were purchased. This may maximize the amount of earnings. However, the prices of the hardware and bitcoin may decline and it is possible to lose money between the buy/sell price and the amount of earnings versus maintenance fees.

**Credit Card Companies**

**Processing Bitcoin a Waste of Energy**

Does all the processing and effort done by the miners just waste resources? But, it creates the market for the software & hardware jobs in engineering and manufacturing. The results from the work that mining accomplishes is more valuable than what the mining costs. This work would be done by expensive bankers if it was not done by the computer hardware. Computers can solve problems more efficiently than people in a lot of cases. Financing may well be one of them. Obviously, individuals will need to have control over the system and they will. The energy & resources consumed in the Bitcoin network is much less than the energy & resources that are consumed with the old-fashioned method of banking & finances. This energy can be reused as a method of heat in cold climates. I personally use miners to heat an addition to my home.

**Fraud**

**Risky Owning Lots of Bitcoin**

If they are not store very carefully, they could be corrupted, lost or stolen. There have been countless tales of people losing bitcoin by computer crashes or having them stolen by hackers. $500,000,000.00 was stolen from customers on Mt. Gox. The problem of safely storing large amounts of bitcoin will stop some investors from jumping on board right away. They will wait for an easy to understand and secure solution. There will be a market for professionals to advise wealthy individuals in purchasing bitcoin for their investment portfolio. It is very dangerous to hold a large amount of cash in bitcoin since it can be lost or stolen. For Credit Card companies, they pass the fraud expenses onto the businesses and customers. The loss is distributed more in CC where in with bitcoin, it is more easy for an individual to get targeted. It would be a good general rule that if you have a large sum in bitcoin, then you better know what you are doing or hire someone that knows what they are doing. And, make sure you trust the person that is assisting you. It would be easy for them to convert your funds into bitcoin and then steal the bitcoin. That bitcoin is probably gone forever and the banks will probably not cover the losses.

**Mining Bubbles & Crashes**

Mining is directly affected by the price of bitcoin. When the price of bitcoin drops, old mining equipment becomes unprofitable and thus the operators turn it off. This in turn, makes it more profitable for the newer mining equipment since there is less competition. The rewards are assigned to the miners based on how much processing power they supply. There is a difficulty factor that can go up or down based on how much mining power there has been in the last couple of weeks. When the price of bitcoin falls, the miners make less money and the old equipment gets removed from the market. The efficient miners with the new equipment remain profitable. This process will help the mining market progress. When bitcoin price raises, people invest making faster and more efficient mining equipment. It will mine, by contributing a certain number of gigahertz per second. Providing these gigahertz costs electricity. The mining equipment that uses the least amount of electricity will make the most profits as long as the price of building hardware to get the low electricity outweighs the profit. There is an equilibrium between all of these factors where the only outcome will be a balance between the hash rate, difficulty and price. The difficulty is a factor of difficulty that makes the network as secure as possible with the amount of processing power that is currently possible. The more processing power that is contributed to the Bitcoin network, then the more secure it is. This balance should make minor spikes and drops in the hash rate over time. During price drops, there will be less hashing and the network will be less secure, but the network will be worth less. It will always remain unprofitable for someone to attack the network. Even if the hashing power drops, then the intruders could not make a profit at the current rate of the bitcoin. It is not a trivial task to intrude on the network. It would take a significant amount of resources that nobody currently has. Someone would need the processing power of 13,000 times higher than the world 500 supercomputers combined. And, if they did accomplish this, then the price of bitcoins would be worthless anyhow, so they wouldn’t make any gains. If a very powerful entity or group of entities could make huge profits by shutting down the Bitcoin networks, then it would be profitable for them. However, that would cause a fork and the developers would make efforts to stop the counter network from intruding on the newly created network. The act of taking down the Bitcoin network would be an act of cyber warfare. People from many nations have their wealth stored in Bitcoin. It is the duty of nations to protect its’ citizens from wide scale attacks. It would be the same as if a nation attacked the computer networks of businesses in a nation. The attacked nation would have the right to respond militarily. I think in the distant future, an effective attack on the Bitcoin network would be construed as an act of war against many nations. There will be terrorists and criminals that could attempt to attack the network, but that would be the same as terrorists and criminals attacked a bank. The Bitcoin network should be resilient against attacks from terrorists and criminals. Terrorists and criminals would never acquire the resources to launch an effective attack against the Bitcoin network. They would probably be able to more easily steal or buy a nuclear bomb from a nation.

**K Computer**

http://en.wikipedia.org/wiki/K\_computer

[THE HUMAN BRAIN PROJECT WILL PUSH THE BOUNDARIES OF SUPERCOMPUTING](http://www.top500.org/blog/the-human-brain-project-will-push-the-boundaries-of-supercomputing/)

http://www.top500.org/blog/the-human-brain-project-will-push-the-boundaries-of-supercomputing/

**Worlds Supercomputers**

[**http://www.top500.org/**](http://www.top500.org/)

The Bitcoin network has 256 times more processing power than the worlds top 500 supercomputers combined according to Forbes (<http://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/>). That is amazing.

(now 13,000 times faster <http://blogs.wsj.com/moneybeat/2015/01/13/bitbeat-bitcoins-price-mining-hashrate-reflect-unsynchronized-bubbles/?mod=WSJBlog> )

**Charts Growing Exponentially**

**Some Charts Flatlining**

**Western Union Will Be Going Out of Business**

**Bitcoin Unsustainable**

**Bitcoin Network vs. Other Networks**

**Financial Network**

**Facebook Servers**

**Bitcoin Weakness: Destroy bitcoins**

If wealthy and powerful people wanted to, they could slowly buy the bitcoin up and destroy them. This would take them out of the market. This would also drive up the price of bitcoin and have people not want to buy in. However, destroying bitcoins may drive up the value of the existing bitcoins in circulation. Limiting circulation of Bitcoin will certainly devalue it. It might be a weakness in Bitcoin that could be exploited by the Bitcoin opposition. This would induce people to sell their bitcoins when the price rises especially at what looks like the end of a bubble or beginning of a crash. The extremely wealthy has enough wealth to swing the bitcoin price and get a hold of a vast majority of bitcoins and then destroy them. The strategy could easily backfire and only make Bitcoin more popular. This is a purely speculative theory which is very unlikely, but it is not impossible.

**Getting People on Board**

They will need to be giving free and/or cheap bitcoins in order to get on board and trust the Bitcoin system. For the average person, a very small amount, maybe $1, should be seeded to individuals that otherwise would not get into Bitcoin. For the wealth people, a discount on bitcoins must be given to them so they can jump on board. This would be bad for the early adopters but good to get the Bitcoin market to go mainstream.

**Bitcoin For Voting & Authority**

A very small amount of bitcoins could be used as another means to moderate web content in 3rd party applications. A system could be created that is used to organize data. A content creator could put up some bitcoins for an article. Users would be able to upvote it and downvote it. The more upvotes, the more bitcoin the content creator gets back. If it goes up above the average, the content creator could get more bitcoin back then was first put up. The content creators would be rewarded by the expense of the advertisers or spammers that are posting bad content. There should be some leeway for content that is just a little below average because that just might mean it is controversial to a significant percent of the population. If it gets all downvotes, then it is most likely spam. Some content that might be good but is looked at as bad by a significant portion of the population might be labeled as spam. I think those articles could be spotted by requiring at least a few people see it and they could have a power attribute to the votes. Maybe they could upvote by +1, +2 and +3 and downvote -1, -2, -3. Voters could be shown some guidelines to not downvote a controversial issue. Sometimes a large percentage of the population has bad feelings towards some issues that were illegal or immoral that might now be regarded as legal and moral. Some of the bitcoin generated from the bad content could also be given to the customers that view the content. This could be done with money but the fees might be too high for content creators to put up a deposit. A content creator might only want to *and need to* put up $0.25 for their content. That would be impossible to do with a credit card. Amateurs might spend years attempting to create good content and want to try to publish it, but they don’t have money to pay for advertising. Google is good for organizing content so that people can find it, but they typically favor the same large media outlets. They also place a lot of advertisements that would avert users away from finding their content. This would also entice advertisers to produce better content and pay the users for finding it. That money currently goes to Google and there is a ton of it going there. That money could stay between the merchants and the customers. All of the money that gets paid to Google would remain in the pockets of the merchants and the customers. This system would also hurt entities that attempted to make bad content because they would have to fork over all their bitcoin to the customers and merchants. Add that to all the money that the merchants and customers save from having to “pay” for advertisements. Both the merchants and the customers pay for those advertisements because the merchant relies on the advertisement to reach the customer. The merchant then has to raise the price of the product to make a profit. The customer pays the increased fee. When you shop at shopping sites, the shopping site takes in a large amount of profits from their merchants and customers. A new system could be created that cut them out and give those profits directly to the merchants and customers. With well trained customers and merchants, the middle men can be cut out. When I say middle men, I mean the advertising companies, credit card companies, banks, online shopping networks. There could be more free and open international systems that are not owned by nations and corporations but are owned by the most efficient 3rd parties.

**Google Servers**

**Adding Another Factor**

For new purchases online, I wonder whether to spend bitcoin or USD when I am purchasing. If I think that bitcoin is going down, I should use bitcoin before it goes down and then just purchase bitcoin when it is at the bottom. Some people watch the markets and might be good at being able to make predictions. They could record when they bought and make sure to use it only after bitcoin reaches +20% in value versus the USD. When you receive cash, use the cash only after bitcoin reaches -20% in value versus the USD. If we still see all of this volatility, people that do this will see a maximum purchasing power versus just using one form of payment. You might want to keep 50% USD and 50% bitcoin out of all of your incoming disposable income. If you have leeway of when you can make purchases, then wait for a price dip or spike before making any purchases for goods or services.

**Nations Servers**

List servers that the US, China, Russia, EU, etc… have compared to Bitcoin

**Cyber Warfare**

**Cyber Terrorism**

**Computer Security**

**Viruses & Malware**

**Mining Rewards**

Currently, miners are getting a reward for mining. This started at 50 bitcoin and halves every 4 years. It is currently at 25 and should fall to 12.5 sometime in 2017. This keeps getting cut in half every four years until there are about 21 million bitcoin in existence. After that, miners do not get rewarded with blocks for mining. There is a transaction fee built into the system. It is currently very low since the miners get rewarded with new bitcoin instead of the transaction fees. In the future, transactions are going to cost money. This cost will have to be competitive with other services in the market.

**Transaction Fees**

For the near foreseeable future, transaction fees are an insignificant cost. The protocol of bitcoin gets updated. The entire mining community chooses whether to update to the new version or not. If they all agree, then a new version is pushed to the network. All the miners that want to stay with the majority must update their software or they will risk being excluded from the network and their mining efforts would go unrewarded. If the volume of transactions grow large enough, then the fees can be maintainable. The system would be able to make an estimate for a fee for a transaction and the time it would take to process it. A client application could negotiate the fees and the user could choose the length it takes for a transaction to process. The transactions that include a higher fee will have higher priority in the system. There will be a market for free transactions. Intelligent people will find ways to handle transactions for free by attaching an advertisement or something like that to a transaction. Some third party will be able to provide free transactions that are high in quality. Look at Gmail. It provides the highest quality e-mail there is and it is free for the user. Google makes money from the ads on the Gmail client. In the distant future when fees start to rise, there will be applications that provide rapid transactions for no fee.

**Buy/Sell at Spread**

People can make make possible making money by buying and selling at the same time around the asking price. Try to buy at 0.00000001 above the highest listing order and sell at 0.00000001 below the lowest selling price. If you continue to do this and keep a spread between the buys and sells, then there is a profit to be made. This will create a window between the buy and sell. As long as the buys and sells take place at some point in time, than a profit is to be made. This can get complicated because the value of a US dollar that the bitcoin gets exchanged for might change. There should be an equilibrium between the value of a dollar and a bitcoin keeping it at a fair market level. However, the money invested into the bitcoin would be locked up and the investor would not be able to invest that money into anything else. Bitcoin makes it easy to automate this task. Just like in traditional trading, there are bots that are constantly buying and selling hoping to maximize their profits.

**Nations Will Need To Participate**

The economies of each of the nations will have to start participating in mining. This is especially true if a lot of individuals in that economies has assets at stake in the blockchain. The IRS already labeled bitcoin as an asset. Nations will be responsible to keep the integrity of the ledger. They will need to invest into monitoring the ledger. A lot of the assets of its’ citizens are at stake. There will be regulation

**Regulation**

**Miners Selling Cloud Contracts**

Miners can make more money by selling 12 month contracts because they can sell the hashing power at current rates and by the time 6 months has passed, the company can buy twice the hashing power for the same price in terms of processing and electricity. Note that moore’s law states computational power on standard chips doubles every 2 years. Since the ASICs for bitcoin mining came into existence over the past couple of years, the computational power for the bitcoin mining computers has doubled every 6 months and it appears as though this doubling every 6 months will continue here on forward.

**Mutually Assured Destruction**

Mutually Assured Destruction is when two countries won’t have a serious conflict with each other because both sides have to potential to destroy the other. Like a nuclear war between superpowers, there can be no winners. The Bitcoin network lives on the principle. Too many people have investments in Bitcoin to allow it to fail. Nobody would benefit from somebody breaking the integrity of Bitcoin. If someone pulls a 51% attack, then people would lose the trust in the system and bitcoin would lose all of its value. Any parties that are interested in Bitcoin will attempt to prevent such an attack. The overwhelming majority of the Bitcoin network and their supporters would back the integrity of the system. Governments will back the integrity of the system. However, there will be controversy when governments start freezing wallet addresses on the blockchain that contain illegally obtained bitcoin.

**Network of Trust**

If all the parties can come to a fair agreement of how much hashing power, then there wouldn’t need to be a race to the bottom by wasting efforts on mining. It is naturally competitive as to reward the parties with the most hashing power. Like in real life, no one party will want to take over more than 51% because the value of the system will dwindle. Someone that has control of 51% of the network will want to keep the integrity of the transactions - they would not benefit from altering any information in the network. It will maintain a natural balance between people around the world. People around the world will want to be friendly with each other. A majority of people are good and the network is an image of the miners and users of Bitcoin. It is a trust based system. The value of a bitcoin will be worth what people will make it worth. People will naturally make the Bitcoin network worth what it provides. If it does provide all the services of banking and credit cards and a whole lot more, then it will be extremely valuable. All parties that are involved with Bitcoin will want it to continue to succeed. An attack from outside the bitcoin network would be the most likely. However, it would be cheaper for an outside party to buy into the network and try to control it from within. Terrorists will not ever acquire enough power to take down 51% of the network. Governments may have the power to do this. But, the governments that have that much power would be able to acquire control of much of bitcoin through mining and purchasing bitcoin.

**Bitcoin vs Checks and Balances**

A transaction and store of value system like the current financial institutions use checks and balances to ensure the integrity of their network. Any business can be audited to make sure all transactions are accurate and complete. Is the current setup of checks and balances more efficient than Bitcoin mining? I can’t answer that for sure, but a competitor, like Bitcoin, will ensure that the financial institutions are working as efficiently as possible. They will have to be able to compete with the services that Bitcoin is offering and they have to do it with either more quality or for cheaper. Options are always a good thing for consumers. It will force the financial sector to compete for customers. They may use many methods to compete.

**Attention in Media**

It can be profitable for news agencies to report on the fallacies of Bitcoin. These reports, in turn, make Bitcoin less valuable. It is a downward spiral. However, people communicate with each other. There are lots of people using Bitcoin. They will teach their friends of its’ advantages. Their friends will teach their friends and that cycle will continue until the general public is educated about the facts of Bitcoin.

**Court Orders**

Could courts ban transactions from being processed if they know that those funds are illegal? A court has jurisdiction over its own borders. Will the miners listen to those court orders? If the transactions in the history mapped to some bitcoin in an innocent persons wallet by legal transactions, could that money be seized? With the USD, money that was stolen can be seized by authorities. I’m not sure how far down a chain the US government could seize dollars that originated from an illegal activity, but similar laws might be applied to bitcoin in the future.

**General Beliefs About Bitcoin**

**Economies Will Have to Balance**

The economies will have to find a new equilibrium with Bitcoin factored into the equation. Bitcoin provides technology that has never been seen before. The concept of international trade has been around for around 10,000 years or more.

**Ancient Economies**

**Future Economies**

**How to Secure Bitcoin**

**How to Backup Bitcoin**

**Bitcoin Scalibility**

**I will let Satoshi Nakamoto answer this:**

**Long before the network gets anywhere near as large as that, it would be safe for users to use Simplified Payment Verification (section 8) to check for double spending, which only requires having the chain of block headers, or about 12KB per day. Only people trying to create new coins would need to run network nodes. At first, most users would run network nodes, but as the network grows beyond a certain point, it would be left more and more to specialists with server farms of specialized hardware. A server farm would only need to have one node on the network and the rest of the LAN connects with that one node.**

**The bandwidth might not be as prohibitive as you think. A typical transaction would be about 400 bytes (ECC is nicely compact). Each transaction has to be broadcast twice, so lets say 1KB per transaction. Visa processed 37 billion transactions in FY2008, or an average of 100 million transactions per day. That many transactions would take 100GB of bandwidth, or the size of 12 DVD or 2 HD quality movies, or about $18 worth of bandwidth at current prices.**

**If the network were to get that big, it would take several years, and by then, sending 2 HD movies over the Internet would probably not seem like a big deal.**

**Satoshi Nakamoto**

**Link:** [**http://www.mail-archive.com/cryptography@metzdowd.com/msg09964.html**](http://www.mail-archive.com/cryptography@metzdowd.com/msg09964.html)

**Bitcoin Integrity**

**Growing Pains**

Google had its’ problems with web spam, computer viruses, and many more. These problems still exist even after Google has been around since 1998. Bitcoin has been around since 2008 and it has had problems like Mt. Gox and other illegal activity that happens using bitcoin. Mt. Gox had nothing to do with the core technology of Bitcoin. It was a third party that stole the bitcoin that people had stored on their servers. It is believed to be an inside job.

**Mt. Gox**

**Banks Reserves**

The money that you have in your bank is not technically at your bank. The banks lend the money out and are only required to hold about 15% of their customers funds. The rest is, of course, covered by the FDIC up to certain limits. If there is a mass adoption of Bitcoin, then all the funds that get converted to bitcoin come away from the banks. Banks will no longer have that money to lend out and collect interest on. The banks will have to compete with Bitcoin for the customers money. This competition is a good thing because banks will be incentivised to keep you depositing their funds there.

**Banks Loaning Your Money**

**Moving Resources**

For every dollar that goes into Bitcoin, it is taken away from somewhere else. That is, if an investor is holding $25,000.00 in Apple stock and they sell that to invest in Bitcoin, then the value of Apple will go down. This will affect the resources that Apple has. The economy has plenty of room to adjust to Bitcoin. Bitcoin has a current market value of about $4 Billion USD. This does not count the value in the businesses surrounding Bitcoin. Investors poured about $300 Million into start-ups focusing on Bitcoin. That is up from $100 Million the year before. This amount of funding going into something this early shows that Bitcoin is a serious contender in the international digital financial market. And, if that is the case then the value of Bitcoin should adjust to what it is worth. If it account for just 1% of the economy, then that is [find some statistics and do some math here].

**Energy Costs**

The cost of energy to mine coins will be factored into the equation to figure out how much a bitcoin is worth. The amount of energy to provide the equivalent amount of computer power decreases over time. For example, the AntMiner S1 has a Power efficiency of 2 W/GH/s on wall. That is, it costs 2 watts of power to process 1 gigahertz in one second. The AntMiner S5 has a Power Efficiency of 0.51 W/GH/s. Another word for W/GH/s would be a Joule. Over time, we will use lesser and lesser energy to provide the same amount of processing power. This fact makes it so the costs to maintain the Bitcoin network do not grow exponentially.

**Use on Social Networks**

**Use on Games**

**Use for Shopping**

**Use for Gambling**

**Store of Value**

**Same as Stock**

**Bitcoin is Two Way**

A lot of other currencies are one way. That is, the user can transfer their US dollar so that it can be used in a software application and it can never be returned back to a US dollar. Bitcoin are two ways. A user can easily convert it back to US dollars. A user could start using a software system with zero bitcoin, earn bitcoin, and finally trade the bitcoin for US dollar.

**Mining Causes Heat**

This heat needs to be put to use for it to be efficient. It would be useful in colder parts of the world. A mining community could exist in a colder part of the world. Heating the community would be profitable. Who could have imagined something like this even 20 years ago? I have two AntMiner S5s running in my spare room that is semi attached to my house. I think it might have been an addition that was put there in the 1960’s, but it gets ice cold in there. I use it as my little hobby/work room and it is free heat. I know it is not profitable with the current prices to mine bitcoin at home anymore because of the costs. I did it as a hobby/educational scientific & engineering research type of a project. I will hold onto the bitcoin until they, hopefully, reach higher levels. If they ever reach the peak of $1150 again, it will be fairly profitable for me to mine bitcoins. But, then again, I could have used that money to just simply buy bitcoins and that would have been more profitable in the hypothetical scenario where the value of a bitcoin again reaches $1150. The only profitable mining can be done by large data centers with very cheap electricity. The cheapest electricity is in China - that is where most mining is done. KnCMiner is setting up mining facilities in the arctic where cool air is free and the electricity will be generated by solar and/or wind. That type of bitcoin mining that is going to survive for a very long time. The others will die in a process of selection of the most fittest mining operations.

**Money Exchange**

Western Union charges about $40 to send $500 from one party another. Bitcoin can do this potentially for free or negligible amounts of transaction fees. It might be one penny. Bitcoin beets Western Union in terms of price.

**Digital Contracts**

A third-party could use Bitcoin to create digital wallets. One user could create and store the first half of the password and the other user could create and store the second half of the password. This could help parties come into an agreement without as much risk. If one party does not honor their commitments, then the funds are stuck in the wallet forever. This could entice both sides of the parties to honor their agreements.

**blockchain a Living Entity**

**Transparency**

There will be software built around Bitcoin and finance that will allow anybody in the world to pay with or accept payment in any currency transparently. The conversions should be automated.

**Articles Containing Bitcoin Increasing**

They are on some large name companies website also.

**Books & eBooks on Bitcoin**

They are growing [cite sources]

**Credit Limit**

Users need to be able to get a credit limit with Bitcoin. This also needs to be reported to some credit bureaus. A system called Ripple might be able to accomplish this.

**Credit History**

People like to have their spending recorded on their credit reports. This shows to the banks that they are capable of repaying a debt. If someone only used bitcoin then they could not build a credit history that is widely accepted lie TransUnion, Equifax and Experian. If there was a serious credit agency that could be listed at the end for specifically bitcoin credit history. Bitcoin could allow for an effective international credit reporting agency.

**Opinion**

It will be useful for micro payments online. I personally like it for that. I like to pay $1 or so for goods. I wouldn't give a company my credit card or bank information for such a small amount. I have been signed up for cycled billing for a minimum 12 months at $29. I should have read the terms and conditions. It would be harder for businesses to do that with bitcoin.

They will be good for international orders also... the international credit card transactions sometimes fail and have to be manually approved

It is cheaper than western union and paypal if you convert USD to bitcoin for free.

Businesses usually pay about 3% CC fees and those are passed on to the customers. If the businesses/consumers could lower their prices by 3% for bitcoin customers, it would cut out the banks 3% fee for almost each and every transaction. It adds up after the same $100 gets a 3% transaction fee 10 times as the money spreads through the economy.

**Cryptography**

**Hoarders**

Hoarding will have to be balanced. If wealthy individuals hoard all of the bitcoin, then people will not want to buy it, so they have to sell some a fair market rate. They price should not skyrocket too much because nobody will buy it when it does and everybody that has it will want to sell it when it does. Again, the price should find an equilibrium. There is a finite amount of bitcoin - there will only be 21,000,000 bitcoin ever and there is currently about 14,000,000. Most bitcoin has already been mined and pretty much all of it will be mined by 2024. There are currently 7,000,000,000 people on the planet. That is 0.003 bitcoin per person on the planet. That seems like a very small amount of bitcoin per person. The numbers are not really important. Give 0.003 a name, like a millibit, then there are 3 millibits per person. The numbers are infinitely divisible. So people will be able to make transactions at small increments like 0.000003 bitcoin - this is called 3 microbits. Even if wealthy individuals hoard all of the bitcoin, the majority of people will still be able to make cheap or nearly free transactions with bitcoin. This will make a lot of competition for the current banking markets. It will also make competition for creditors. It may go as far as making a strong competition against national currencies.

**Based on Computing Power**

It would be difficult to create a new cryptocurrency that is as fair as bitcoin because if it did start getting big, the people that were in early will get rewarded more than later on.

A system could not be based on pure randomness for each wallet because whoever has the most wallets would get the most bitcoin. It will end up being a race for whoever has the most computing power. Bitcoin has a good lead on any new cryptocurrency since it has had so much time to mature. Currently, the newcomers with the most hashing power will earn the biggest rewards. If a similar system came out now, then the few major miners would take a majority of the mining reward. It would be a monopoly on the system. It is good that there were some little guys that got in at the beginning of Bitcoin. It is still the beginning of Bitcoin.

**Printing Hard Copy of Bitcoin**

It will be possible to have a wallet containing bitcoin converted to paper. Further, someone could verify that the paper wallet still contains the bitcoin. This would be done with a barcode. The password could be built into the barcode, so that it could be redeemed by whoever possesses it. A potential security problem for this would be that someone could steal it by taking a picture of it. A scratch off surface such as on lottery tickets could be utilized. A trusted corporation could manufacture a large number of these scratch cards and sell them at a small mark-up. It would be a huge business. The government is not as efficient as the free market! There have already been offline hard versions of bitcoin created <https://en.bitcoin.it/wiki/Casascius_physical_bitcoins> Casascius. These physical coins can hold value of 1, 10, 100 or 1000 bitcoins. I have a feeling there will be a version two of these items in smaller decrements and cheaper mediums like scratch off tickets.

**Anonymity**

**Liquidity**

Many large companies liquidate their bitcoin immediately after receiving it. If this is how bitcoin will be utilized by many companies, then this may cause the bitcoin to stay at lower prices for a while. People will want to buy bitcoin for its’ benefits of shopping online and other reasons. Then they will spend the bitcoin and it will be sold again. However, there will be hoarders that will buy up the bitcoin and wait for the price to rise. This will work over time and it will work short term if people buy in the crashes and sell in the bubbles. Then again, when a lot of people are buying during a crash, then the price will rise. If a lot of people are selling during a bubble, the price will fall. Again, some equilibrium will be found with this as an important factor.

**Balancing Account**

Some variation of a spending & saving account could conceptually be created. They would contain an equal amount of bitcoin and dollar when adding funds to it could be used to maximize saving and spending. If the price of bitcoin has fallen since making a deposit, then spend cash on the current purchase. If the price of bitcoin has risen since making a deposit, then spend bitcoin on the current purchase.

**Amplification**

A wealthy individual could have a large impact on the market. The way the buys and sells are setup is that people make a bid to buy or sell a certain number of bitcoin at a certain price. There are only so many bitcoin listed on the market **[insert image of buy/sell graph]** . If someone wanted to buy 100,000 bitcoin, they would not be able to buy that many at the current market rate. They would have to buy some of those bitcoin from sellers that list their price at higher than the current market rate. This would in turn bring the rate up. A single exchange might not be able to handle that many bitcoin. The wealthy individual would be better off buying 10,000 bitcoin from each of the major exchanges. Further, they would be better of buying a percentage of these bitcoin each day over a longer period of time. However, they would risk that the price goes into a temporary bubble or a longer term increase in price. There would need to be a carefully planned entry into the market for these individuals to get a maximum amount of bitcoin for the most minimal price possible. There would be no perfect solution for this. It is a gamble on the unknown of the market.

**Digital Funds In General**

People are going to want an international digital currency. People want access to their funds in any currency that they would want online. This needs to be done without the user having to do any manual actions.

**Arbitrage**

Arbitrage is when investors buy a bitcoin from one exchange at a lower price and sell it at another price for a higher price. This balances the price between the exchanges. It can be profitable for the investors engaged in this activity. It is a risk, though. If the price is crashing before they make the buy and sell.

**High Prices**

The high price of bitcoin are making it so average people will not buy or use Bitcoin. The prices need to come down so that people will buy them and use them. Once more people use Bitcoin, then the value of the market will increase. Once the value of the market increases, bitcoin will have a higher price tag. The price will find an equilibrium between this and several other factors. The price to mine a bitcoin will be factored into the price. Why would someone pay $400 for a bitcoin when they can mine one for $300 or less? The price to mine a bitcoin has been decreasing. This decrease will hit a critical point and then start getting more expensive to mine. The halving of the block reward that is predicted for around 2016 will make for a price increase of a possible factor of 2. Moore’s law suggests that computing power on a processor doubles every two years. For the ASICs that mine bitcoin, they have doubled every 6 months. This will make it cheaper and cheaper to mine bitcoin until around 2016. However, if the demand for bitcoin increases to a number larger than what the miners are generating and selling, then current bitcoin holders will sell their holding or the price will rise. Buyers will have to be willing to spend the higher amount of cash for a bitcoin or wait for someone to sell at a lower price. Some people depend on selling their bitcoin to pay their bills, so they can’t wait forever to buy bitcoin. All of these factors will make for a natural market. There could be short-lived crashes and bubbles, but I think the price will stay at around the price of mining with the supply & demand also factored into the equation.

**Hot Commodity**

People will want to get into Bitcoin. They have seen the potential. The psychological effect of 1 bitcoin is going to have an impact on the price of a bitcoin since there are only 14 million now and there will never be more than 21 million. It wouldn’t be hard to see a market of millions of people in Bitcoin in the near future. A lot of them will want to have at least 1 bitcoin just in case if the price does go up. Investment firms are hiring people specializing in Bitcoin. They will be pitching Bitcoin to investors that have large quantities of money. Some of them will want to buy hundreds, thousands or tens of thousands of bitcoin or more. It is a very powerful network that is capable of handling a large portion of national and international transactions for a much cheaper price than what is currently available. It will be a great asset that should increase in value.

**Outsourcing Financing to Machines**

Bitcoin can manage financing for cheaper than the current banks.

**Trading Stocks**

The value of a stock counts on the value of the service that the business provides. Bitcoin has a valuable service. The value of this service will be reflected in the value of a single bitcoin and in the value of the businesses surrounding bitcoin. As long as the 51% of the servers is not taken over by a malicious attacker, then bitcoin should retain some value. Even if the 51% attack was to happen, there would be a fork that the rest of the community would start moving forward with.

**Infinitely Divisible**

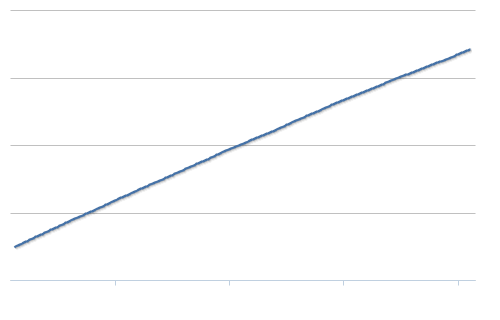
A bitcoin can be divided up to very small parts. My sample wallet address 1HdXXkqjmHcTdX5FyMMUkARP6i4rtr1C74 from Bitcoin Core currently states a balance of 0.00007303 BTC.

**Volatility Insurance**

Companies are afraid to hold onto bitcoin that they receive because it could go down by 20% in the next few days. That would make them lose money on a sale. An insurance to cover volatility could be created. It could be commission based on the fluctuations. The insurance company would collect a percentage of the increase in value in an exchange to cover the dips in value. This would take the risk out of a crash for some companies that may hold bitcoin.

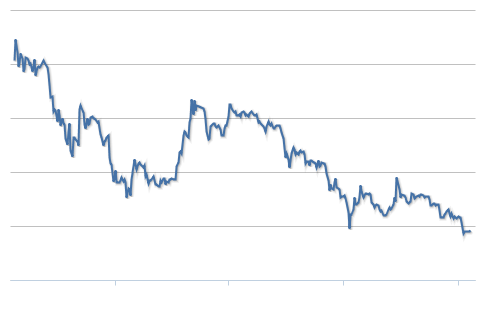
**Hash Rate**

The hash rate has grown to be very powerful and a lot of companies have been dedicated to hashing Bitcoin. The network is currently at about 300 Terahertz (300,000,000 hertz). Hertz means cycles per second. I would not be surprised to see this number get very large. It is growing at an exponential rate. It could soon be measured in petahertz, exahertz, zettahertz or yottahertz. Those are real words, too! petahertz means 100,000,000 cycles per second. Yottahertz means 100,000,000,000 cycles per second. The network is currently around 300,000,000 hertz.



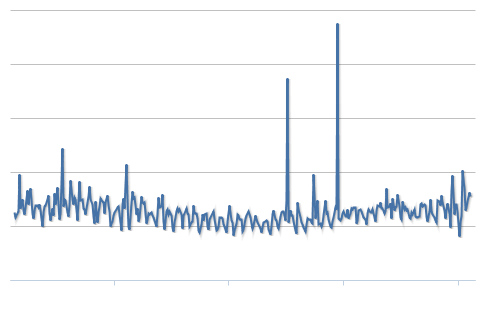
**Total Bitcoins in Circulation**

A graph showing the historical total number of bitcoins which have been mined.



**Market Capitalization**

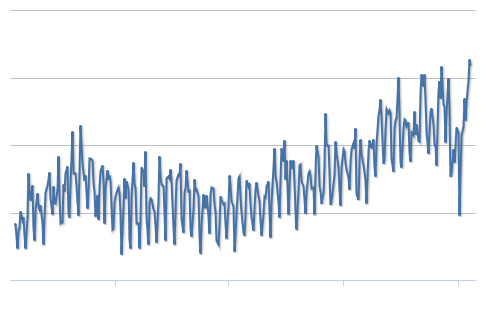
A graph showing the total number of bitcoins in circulation \* the market price in USD.



**Total Transaction Fees**

A chart showing the total BTC value of transaction fees miners earn per day.

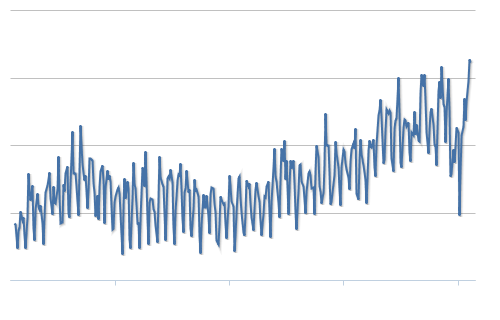
* **Transaction Fees in USD**
* [**Network Deficit Per Day**](https://blockchain.info/charts/network-deficit) **- Shows difference between transaction fees and cost of bitcoin mining.**



**Number of Transactions**

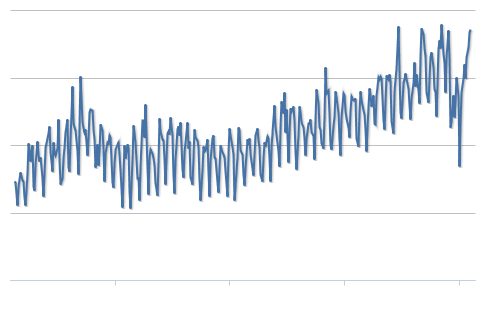
A chart of the total number of unique bitcoin transactions per day.

* **Total Number of transactions**



**Number of Transactions excluding Popular Addresses**

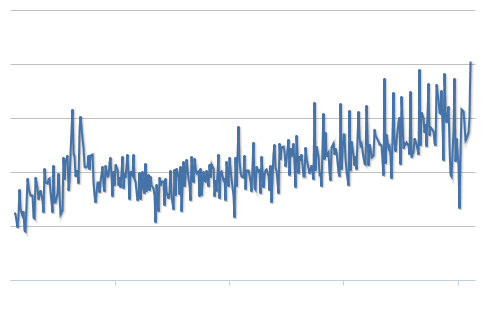
A chart showing the total number of unique bitcoin transactions per day excluding those which involve any of the top 100 most popular addresses popular addresse[s](https://blockchain.info/popular-addresses).



**Number of Transactions excluding Long Chains**

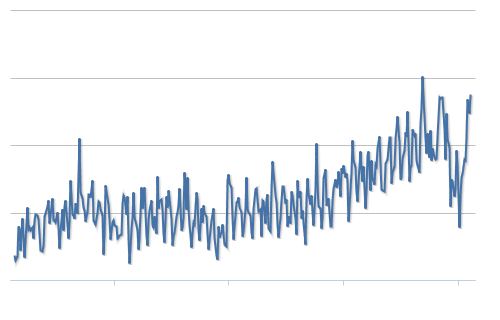
A chart showing the total number of bitcoin transactions per day excluding those part of long chain transaction chains. There are many legitimate reasons to create long transaction chains however they may also be caused by coin mixing or possible attempts to manipulate transaction volume.

* **Number of Transactions Excluding Chains Longer Than 10**
* **Number of Transactions Excluding Chains Longer Than 100**
* **Number of Transactions Excluding Chains Longer Than 1000**
* **Number of Transactions Excluding Chains Longer Than 10,000**



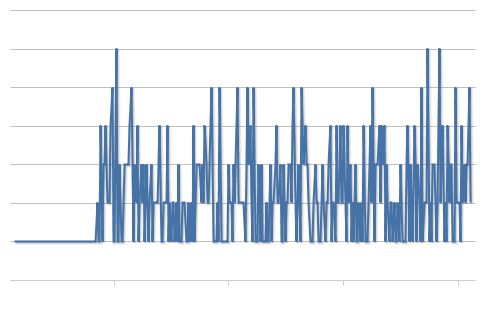
**Number of Unique Bitcoin Addresses Used**

A chart of the number of unique bitcoin addresses used per day.



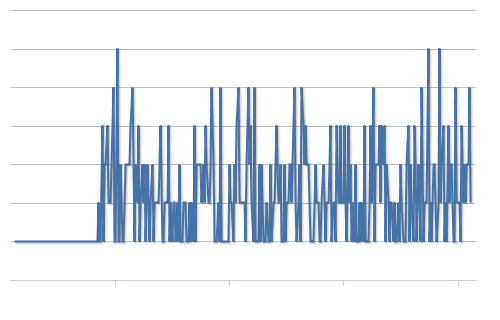
**Average Number of Transactions per Block**

A chart of the average number of transactions per block.



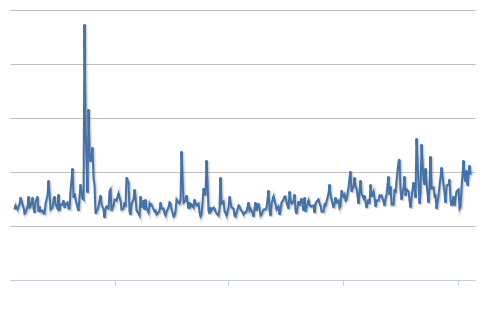
**Number of Orphaned Blocks**

Number of blocks mined per day not part of the main chain.



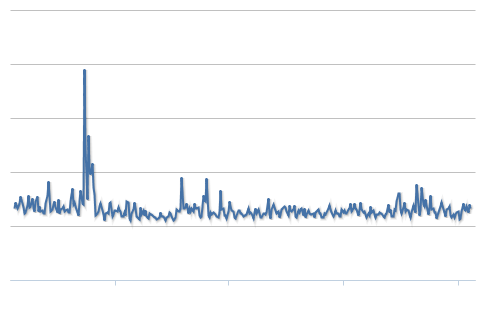
**Total Output Volume**

The total value of all transaction outputs per day. This includes coins that were returned to the sender as change.



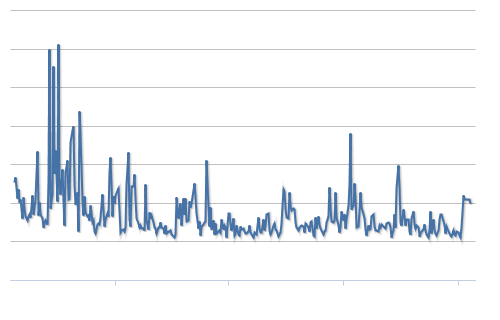
**Estimated Transaction Volume**

Similar to the total output volume with the addition of an algorithm which attempts to remove change from the total value. This may be a more accurate reflection of the true transaction volume.



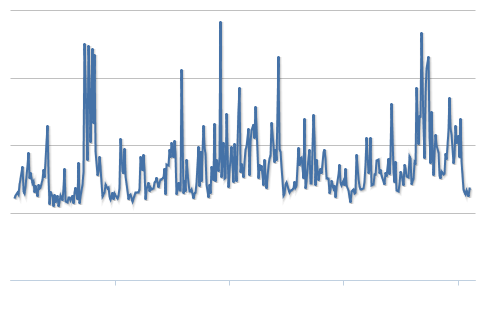
**Estimated USD Transaction Volume**

The Estimated Transaction Volume in USD value.



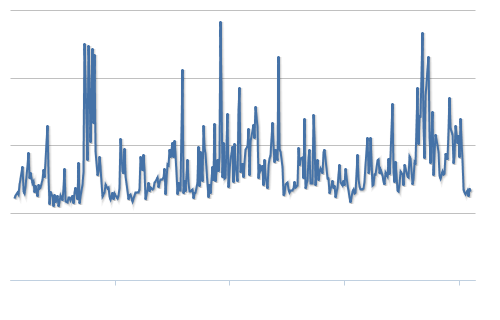
**USD Exchange Trade Volume**

A chart showing the USD trade volume from the top exchanges.



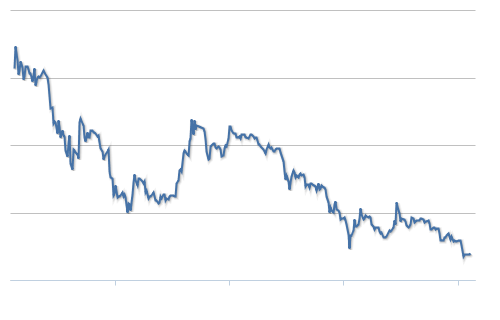
**Trade Volume vs Transaction Volume Ratio**

Chart showing the relationship between BTC transaction volume and USD exchange volume. Discussion



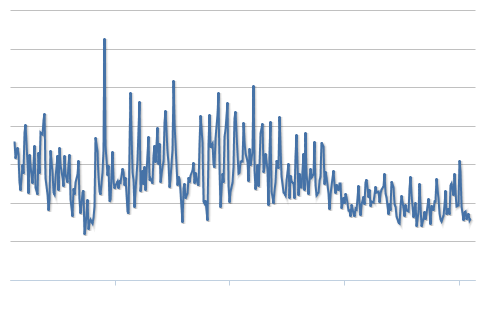
**Market Price (USD)**

A chart showing the USD market price from the major exchanges



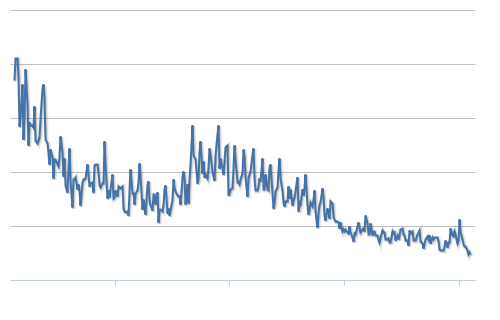
**Cost % of Transaction Volume**

A chart showing miners revenue as percentage of the transaction volume.



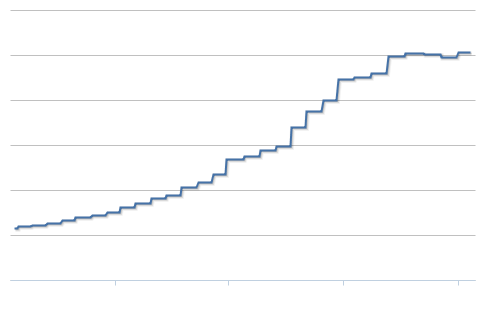
**Cost per Transaction**

A chart showing miners revenue divided by the number of transactions.



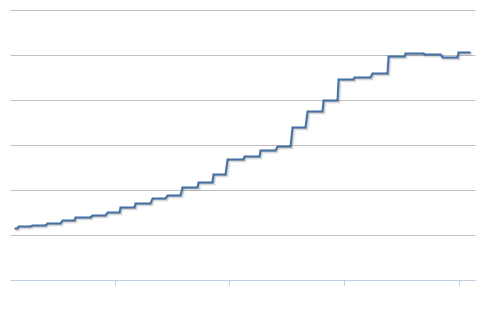
**Hash Rate**

The estimated number of giga hashes per second (billions of hashes per second) the bitcoin network is performing.



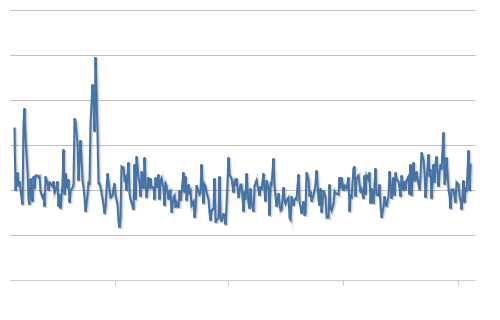
**Difficulty**

A chart showing difficulty changes over time. Difficulty is a measure of how difficult it is to find a new block compared to the easiest it can ever be.



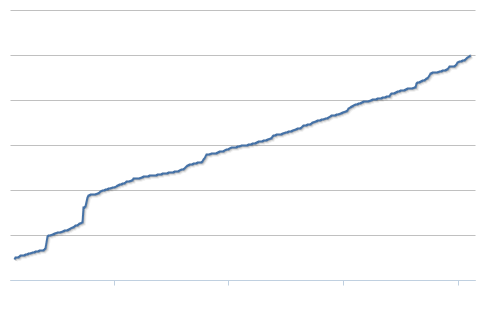
**Miners Revenue**

Historical chart showing (number of bitcoins mined per day + transaction fees) \* market price.



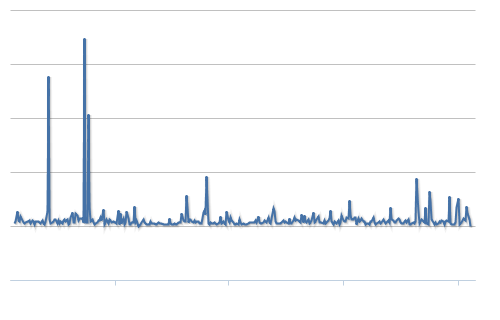
Average Transaction Confirmation Time

The Average time take for transactions to be accepted into a block.



Bitcoin Days Destroyed Cumulative

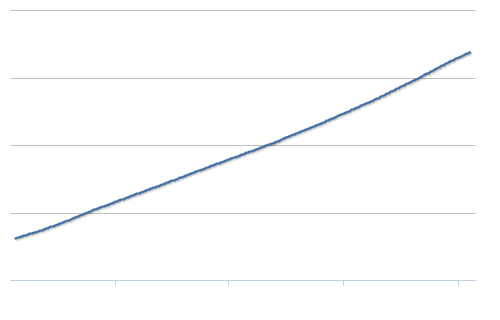
Bitcoin Days Destroyed is a measure of the transaction volume of Bitcoin. If someone has 100 BTC that they received a week ago and they spend it then 700 bitcoin days have been destroyed. If they take those 100BTC and send them to several addresses and then spend them then although the total transaction volume could be arbitrarily large the number of bitcoin days destroyed is still 700.



Bitcoin Days Destroyed

A none cumulative version of Bitcoin Days Destroyed.

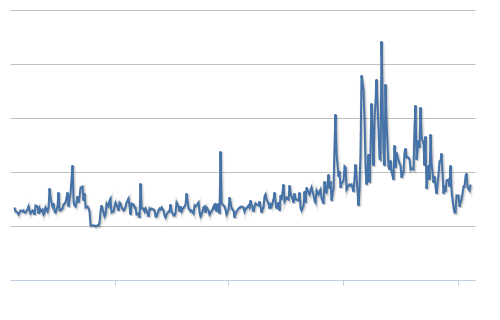
* **Bitcoin Days Destroyed (Filtered By Min Age 1 Week) - Filtered by minimum input age of 1 week.**
* **Bitcoin Days Destroyed (Filtered By Min Age 1 Month) - Filtered by minimum input age of 1 month.**
* **Bitcoin Days Destroyed (Filtered By Min Age 1 Year) - Filtered by minimum input age of 1 year.**



Blockchain Size

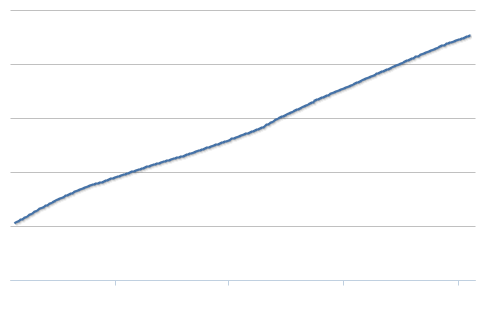
The total size of all block headers and transactions. Not including database indexes.

* **Average Block Size - The Average block size in MB**



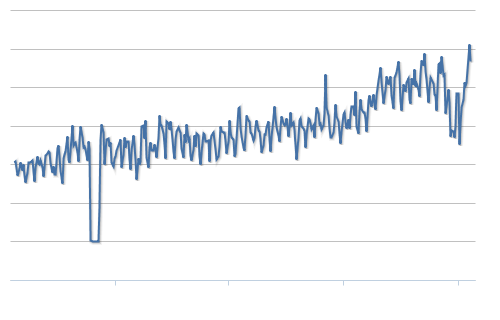
My Wallet Transaction Volume

24hr Transaction Volume of our My Wallet service.



My Wallet Number of Users

Number of wallets hosts using our My Wallet Service.



My Wallet Number of Transactions per Day

Number of transactions made by My Wallet users per day.

**Trustless Currency**

The parties do not need to trust each other for an exchange to happen. For credit cards and ACH, a lot of trust is required. That is not so much for the credit card case, but it is not a good experience to have your credit card numbers stolen. Your credit card company is responsible to cover any unauthorized purchases on your account. With bitcoin, if you use it properly, somebody can’t steal any bitcoin from you if you don’t give them your password and/or private key.

**Insured Accounts FDIC**

There are currently insured accounts available at some exchanges. I’m sure more will grow. They are responsible for any bitcoin that was lost or stolen because of them. This includes hackers attacking their systems. It does not include someone getting ahold of your username and password. Also, they usually have 2 factor authentication so they would need your password and either your email or cellphone authentication. Authentication would be done by sending an e-mail with a confirmation link or sending a text message with a confirmation code that needs to be entered into the site before a transaction can take place. Fund that are stolen from a traditional debit card are usually not insured. However, funds stolen off of a credit card are usually covered by the credit card company. Those funds come from the consumers through fees and high interest rates. The problem with insurance is relatively easy to address for Bitcoin. Corporations will provide this service. They will need to make a profit for that service, so bitcoin holders that choose these services will probably pay for them. Some companies make their profits through other ways that will offload the costs to the customer.

**Irreversible Transactions**

**Bitcoin Scratch Off Cards**

It would be simple for a company to create a scratch card that holds a small value of bitcoin. They could be redeemed by a store and hold a remaining balance. These would be much more convenient and much cheaper than prepaid credit cards.

**Etc…**

The US Dollar Could Be crypto currency in the future

Which CryptoCurrency will be most “hashed” will be advanced

A new CryptoCoin could surpass Bitcoin quickly if enough computing resources were put towards it

Bitcoin will succeed because it has such a powerful network (blockchain) backing it.

There will be over 14 million that want 1 bitcoin for their investment portfolio

There will be over 1 million that want 14 bitcoin for their investment portfolio

There will be a few very rich people that will want much more than 14 bitcoin

Then, there will be the rest of the people that will want much less.

Bitcoin sidechain technology will work well because it could guarantee a store of value backed by bitcoin.

Someone should invent a bitcoin mining space heater. In the future, all heat would come from mining bitcoin or crunching other numbers in homes and businesses.

**Estimate**

If someone was to ask me what the price of bitcoin will be at the end of 2015, I would say that it could be between $250 and $2000. I don’t think that is a fair question due to the volatility of bitcoin. The price will dip and peak at a moments notice. A more fair question to ask would be what will the average price of bitcoin be for the entire 2015 year. I think that price would be in the range of $200-$600. I can not see the price of a bitcoin falling below what it costs to mine a bitcoin. I would approximate it that it costs at least $200 a bitcoin to mine. That might not be accurate, but whatever the price is, I think it will be a barrier that the price will not fall below. If the price does fall below, the money used to mine bitcoin will be redirected to purchasing bitcoin directly from the people that already own bitcoin. This will, in turn, cause more people to stop mining and that, in turn, will make it more profitable to mine bitcoin. This cycle will ensure that bitcoin does not fall below the $200 threshold for any significant period of time.

**Volatility**

There are very few bitcoin relative the number of people that there are. People are psychological creatures and 1 bitcoin will be a milestone for someone to own. If there are 14 million such people that will want to own 1 bitcoin, the price of a bitcoin will skyrocket. There does not yet exist 14 million bitcoin and it will not happen for at least a few months into 2015. By the end of 2015, there will be about 14.5 million bitcoin. 90% of these bitcoins will be hoarded by investors and people that got into bitcoin very early.

**Market Manipulation**

There will be a lot of rich and average people that will want to use the market to make a profit. They will be attempting buy at low prices and sell them at high prices. This will make the market swing up and down. This will hurt the average person because they will not have the best judgement as to when to buy and when to sell. They will buy the bitcoins when they need them or at a random time buy them for future use. The people that buy bitcoins on a downward slope will be forfeiting wealth to the people that buy and sell stocks for profit. This will hurt Bitcoin by stopping some people from entering the bitcoin market.

**Uses**

**Value**

The value of the bitcoin is set by the popular exchanges. It works similar to the stock market. People list a certain number of bitcoins for sale on the exchange. This is called a sell order. People make bids to buy a certain number of bitcoins at a certain price. This is called a buy order. If somebody places a buy order for a price at or above a previously listed sell order, then a “buy” occurs. If somebody places a sell order for a price at or below a previously listed buy order, then a “sell” occurs. This will set the price. The latest trade price will be the current value of a bitcoin. This is affected by supply and demand. Some people think that bitcoin will be worth thousands of dollars someday. This has a chain reaction that affects the price. If enough people think they will be worth thousands of dollars someday, then the value will go up. This could feed itself and make them worth thousands of dollars someday. This is not a pyramid scheme because there is great utility in Bitcoin. The value of the network needs to be considered. It is a powerful network of computers that are hashing at a rate of 340,000,000 GH/s. That is a powerful network and the blockchain might be the most encrypted and secure piece of information that exists. It will have a history of all the transactions that happened on the blockchain. This will be an excellent way to store & exchange wealth.

**Charts**

TODO make a paragraph describing each chart from blockchain.info

**Cost**

It is expensive to run the bitcoin network. However, the network has so much utility, that it is worth the costs.

**Fork**

A fork is in Bitcoin is when there are two separate version that have been worked on and they share a previous point where they were the same. For example, github hosts software projects for developers. If someone has a public project up there, I could fork a copy of the current version and start working on it. The original developer would also be working on the original version. We would both save our copy and they would be different and not share the changes that were made by both of the parties. Some people suggest that a fork in the bitcoin could be used. It would take a majority of the miners to approve a different version that will be accepted by the community.

**51% Attack**

**Government Take Over Bitcoin Network**

**Government Fork a Different Version**

**Nations Fork a Different Version**

**Updating the Protocol**

**Myths About Bitcoin**

**Facts About Bitcoin**

**Major Mining Pools**

**Mining Hardware**

**Mining At Home**

**GPUs**

**ASICs**

**Worth**

What is Bitcoin worth? The current market value (number of bitcoins X USD trade rate) is around $4 billion. It was up to $12 billion about a year ago.

TODO: Some other comparable companies, assets, etc… that are worth $1 Billion - $100 Billion.

**Alternative Uses**

A lot of people are hoping that bitcoin will be used by the mainstream for daily purchases. I think it will be used by a niche and be very good at what it does. My guess is that it will be used mostly for:

1. A store of wealth
2. Investment
3. Online Micro-purchases
4. Online Tipping
5. Transfer of wealth between individuals
6. Banking & Currency for Undeveloped Countries
7. Buying Illegal Goods & Services

**Unfair**

A lot of people argue that it is unfair that the ownership of all the bitcoins is skewed towards such a small number of people. With the maturity of bitcoin compared to any other crypto-currency, it would be hard to make another more fair currency. Whoever gets in on the next currency first will have more coins. If the algorithm was designed to not rewards so many coins at the beginning, then that would make it more fair for people that come in later. With the price lowering as of early 2015, this should force some of the early adopters to sell some of their bitcoins to others that are interested in joining the market.

In the long run, there will be some early adopters that might join the status of billionaire (USD). Currently, there are 1,645 billionaires in the world. There were 268 newcomers in 2014. There is plenty of room for a few more of them. The creator of Bitcoin, Satoshi Nakamoto, has over 1 million bitcoins. When the price of bitcoin surged to over $1,100, Satoshi’s worth was valued over $1 Billion. However, if he tried to sell them all for $1,1000 each, the demand would fall and the price of the bitcoin would fall with it. I don’t think bitcoin is going to shift the wealth of the world very much. Those early adopters would be better off slowly selling bitcoins over the years. If they sell too many, the price will plummet. If they hold onto them, the price should rise, but it will be lowered once they start to sell them. They will need to sell some of them to live a billionaire lifestyle. Not everybody accepts bitcoin as a payment. Even if they do accept bitcoin as a payment, then the bitcoin will be distributed more. Wealthy people will get their hands on their share of the bitcoin. They have to power to manipulate the bitcoin markets and get it from the early adopters for cheaper than what it will be worth. In the long run, I think the bitcoin will end up in the pockets of some of the existing rich people.

**Bitcoin as an Investment**

**Side-chain Applications**

**Xapo**

https://xapo.com/

**Bitcoin is Decentralized**

Some people argue that is not decentralized and that a small group of miners have control of the system.

**Killer Apps**

**Hot List**

There could be a hot list added to Bitcoin. If enough miners agreed to update the core code, then hot list of addresses holding stolen bitcoin could be frozen. This would render them unspendable to make it not so profitable for bad people to steal bitcoin from people. This would be hard to maintain and it should be hard for a person to place addresses in their but it would be beneficial. The original holder of the bitcoin would have to prove that the bitcoin is indeed theres. Once it is on the host list, it would be worth little to nothing. This might even influence some hackers to give the bitcoin back for an agreed small percentage of legal bitcoin.

**Bitcoin Credit & Financing**

People want credit. There is currently no credit with Bitcoin. You will not, yet, get the same 0% APR for 18 months with a $10,000 limit as easily as you could with VISA/MasterCard/American Express/Discover. People would rather spend money that they don’t have to pay immediately. Most people have debt that they would rather put that money towards so they don’t have to pay interest on it. That entire concept is another story. Hopefully, there will be Bitcoin credit cards where people with excellent credit can get a 10 bitcoin credit where they must pay back just like they do with current credit cards.

**Altcoins**

I don’t think an alt-coin will replace Bitcoin. It will have a small hash history and therefore be less mature. The new alt-coin would be worth about the same price as bitcoin in terms of computing power. Buying a crypto-currency will be directly proportional to how much effort it takes to create it. However, this will not hold true for alt-coins that die. If they get abandoned, then they will not be worth as much to a bitcoin in terms of computing power consumed in their generation. There will be cases where an alt-coin rewards more to mine than bitcoin. However, miners will switch their hardware to that alt-coin and then bitcoin will be easier to mine. This will enforce the price of all of the crypto-currencies to be balanced in the long-term. Some lucky people might get in early on some new alt-coins that will take off and it will be extremely profitable. But as soon as the price for an alt-coin starts rising, more miners will throw their equipment at it.

**Superior Digital Currencies**

A currency that had all the abilities that Bitcoin has but was cheaper to mine would be superior. Is mining necessary? Is there a way to make a value exchange network that does not require such expensive computational power? A large network of trust might be able to be built where each node in the network receives a small reward for processing a transaction might be conceivably built. However, the heat giving off from mining is, in my mind, just as a valuable resource as the processing that is going on. This heat needs to be utilized in homes and businesses in areas that are cold.

**Proof of Work**

\*\*\*\*\*\*

It is "proof of work." Miners use computer power to solve the math problems and when someone gets an answer that if "proof" they did work to get it. If someone want to game the system (something like counterfeiting) they would need to do more work than all the other miners combined. That would be too expensive and difficult to do and that secures the system.

**\*\*\*\*\***

Proof of Work is the hashing that a miner does to show that a large investment was made to verify the transactions. The rest of the nodes then validate the miners work. This is necessary because if there was no proof of work, then there would be bad nodes that would try to manipulate the system. This ensures that there will be no bad actors because it would be expensive to attempt and difficult to achieve. An alternative proof of work might be effective. A node gains power through validating transactions. The more correct transactions that the node has verified, the more power it has on the network. As soon as a powerful node is caught making an incorrect transaction, then they would lose power. The network would also correct the inaccurate transaction The transactions would have to have a maximum of a single unit. This system is feasible and it is not so expensive to operate. If a system like this could verify transactions as Bitcoin does, then Bitcoin could be in trouble. Bitcoin would be an ancestor system and I think it will always be around even for memories sake.

**Bitcoin Will Hold Value**

Even if Bitcoin is replaced with a superior digital currency, it will continue to maintain some value. Whether it will be a collector’s item in the future or adopted as the mainstream digital currency is a thought to ponder. I’m certain that a competitor to the current financial system will come into existence.

**BitIndex**

https://panteracapital.com/bitindex/

**Free Markets**

The USA was founded on beliefs of a free market. Is it a free market only for certain commodities?

**Current Systems Are a Monopoly**

It is currently a monopoly. People have no alternatives to the current banking systems. Will the government try to make alternatives to the current VISA/MasterCard/American Express/Discover/Western Union illegal?

**“The” Money of the Future**

Bitcoin will not be “the” money of the future. It will be “a” money of the future. It will have applicability in the international free market. The free markets in the world have always won and caused for greater innovation. Markets that are not free will fall behind the free markets.

**Bitcoin Whitepaper**

**Bitcoin is Open-Source**

**Bitcoin is Web 3.0**

Web 3.0 is finally here and it is Bitcoin!

**Linux**

**Replacing Obsolete & Old Infrastructure**

There are going to be battles replacing the obsolete & old financial infrastructure that is in place. They will take as much action as possible in court & media campaigns to continue maximizing their profits. Bitcoin offers new & improved services over the old.

**Transfer of Wealth**

A lot of wealth may transfer to some of the early adopters of the technology from the hands of the current class of wealthy individuals. The late stage early adopters will gain some amount wealth, but not that much. The very early adopters are the group commonly labeled as “techies” or “hackers”. They are, for the most part, regular people that are interested in computer science & computer engineering.

**The Internet**

**E-Commerce**

**Crazy Claims**

To claim that Bitcoin can provide all the services of the Banks, Credit Card companies, PayPal, Western Union to name a few sounds crazy, but they all store and exchange wealth. Bitcoin is very effective at storing and exchanging wealth. The part about storing wealth might be argued against since people that bought at $1100 and now it is at $275, but this is probably just a dip in a long-term rising value.

**Charitable Donations**

When you donate money to a 3rd world country, not all of that money reaches there. [todo: find some percentages]. If you wanted to donate $1, probably about $0.10 will reach the hunger child that you wanted to feed. With Bitcoin, it will be possible to donate $1 to starving children and $1 will reach its targeted donation. The implications of what Bitcoin could do for the world are huge. It is a nearly free to use money transfer system. There will be applications where it will be absolutely free to send money. The applications will generate revenue with the traffic to its’ services just like Gmail provides free e-mail and Facebook provides free social networking.

**Advancement of Processing**

Bitcoin is speeding up the rate at which computation advances. This has huge impacts on the timelines of predicted processing power. There are 3 important milestones:

1. All the computers on the planet are equivalent to one human brain
2. One computer is equivalent to one human brain
3. On computer is equivalent to all the human brains on the planet

This is comparing apples to oranges some would argue, but brains and computer processors are more similar than most people think. We may see some or all of these milestones achieved in our lifetime. The implications of these could be a theme of many books, so I can’t get into it too deeply. Stephen Hawkings has already warned us. If you are interested in learning more about this, I would suggest researching topics such as Robotics, Artificial Intelligence, Neural Networks, Data Mining and Natural Language Processing just to name a few.

**Moore’s Law**

Moore's law is the observation that, over the [history of computing hardware](http://en.wikipedia.org/wiki/History_of_computing_hardware), the number of [transistors](http://en.wikipedia.org/wiki/Transistor) in a dense [integrated circuit](http://en.wikipedia.org/wiki/Integrated_circuit) doubles approximately every two years. The observation is named after [Gordon E. Moore](http://en.wikipedia.org/wiki/Gordon_Moore), co-founder of the [Intel Corporation](http://en.wikipedia.org/wiki/Intel_Corporation), who described the trend in his 1965 paper. His prediction has proven to be accurate, in part because the law now is used in the [semiconductor](http://en.wikipedia.org/wiki/Semiconductor) industry to guide long-term planning and to set targets for [research and development](http://en.wikipedia.org/wiki/Research_and_development). The capabilities of many digital electronic devices are strongly linked to Moore's law: [quality-adjusted](http://en.wikipedia.org/wiki/Price_index#Quality_change) microprocessor prices, [memory capacity](http://en.wikipedia.org/wiki/RAM), sensors and even the number and size of [pixels](http://en.wikipedia.org/wiki/Pixel) in [digital cameras](http://en.wikipedia.org/wiki/Digital_camera). All of these are improving at roughly [exponential](http://en.wikipedia.org/wiki/Exponential_growth) rates as well.

This exponential improvement has dramatically enhanced the effect of digital electronics in nearly every segment of the world economy. Moore's law describes a driving force of technological and social change, [productivity](http://en.wikipedia.org/wiki/Productivity#Labor_productivity), and economic growth in the late twentieth and early twenty-first centuries.

The period is often quoted as 18 months because of Intel executive David House, who predicted that chip performance would double every 18 months (being a combination of the effect of more transistors and their being faster).

Although this trend has continued for more than half a century, "Moore's law" should be considered an [observation](http://en.wikipedia.org/wiki/Observation) or [conjecture](http://en.wikipedia.org/wiki/Conjecture) and not a [physical](http://en.wikipedia.org/wiki/Physical_law) or [natural law](http://en.wikipedia.org/wiki/Natural_law). Sources in 2005 expected it to continue until at least 2015 or 2020. The 2010 update to the [International Technology Roadmap for Semiconductors](http://en.wikipedia.org/wiki/International_Technology_Roadmap_for_Semiconductors) predicted that growth will slow at the end of 2013, however, when transistor counts and densities are to double only every three years.

**Robotics**

**Proof of Existence**

The blockchain can be used to prove that a document existed at a certain date. The way that it could be done is that someone that has a document get a hash of it and place the hash at an address on the blockchain. The hash and date is now stored on the blockchain for all of eternity. A document could then be verified to have existed on the blockchain at a future date. This would be good for copyright, wills, deeds, and similar. This would be similar to getting a document notarized. It will have a signature stating that the document existed at a certain date. Courts and other legal entities only accept notarized documents from a certified notary. It would be much easier and cheaper to get a document notarized on the blockchain. It could then be sent over the internet without having ever have a printed out copy. That would be excellent for the environment since using electricity and computers is more efficient than paper. Think about how much effort is done to bring paper documents across the country. You could argue that an e-mail is also proof of existence. However, an e-mail is harder to verify and make publicly available. It is certainly not as secure of a method as using the blockchain. How would this affect the price of a bitcoin? I would argue that the more valuable the blockchain is, the more secure it would become. And, the more secure that it would become, then everything that the blockchain is used for that is useful would become more valuable.The internet is very secure for sending encrypted and unencrypted data from two points on the network. The blockchain is built into the internet and it is not going anywhere anytime soon. It might never go away, ever. It will be a public ledger to verify certain transactions at certain dates. The implications of this are huge.

**Computer Are Our Descendants**

Let’s hope they like us.

**Middle Aged & Younger Will Love Bitcoin**

They don’t have a choice. They will love Bitcoin because it is familiar to value such an item in video games and even virtual reality. Most, if not all, video games have some form of point or coin reward system. In the future, these points that people can earn just might be bitcoins or some other equivalent two-way currency. Users of video games and virtual interactive systems will enjoy being rewarded for their participation. Makers of these software systems will be able to profit from their users and in turn reward them with some type of virtual & useful currency.

**Financial System**

Bitcoin is more than just a currency. It is a large virtual and real financial system. It can exist outside of the pure software world. It can be printed onto paper just like money can and be used that way. There are actual coins that contain bitcoin value on them and they are marked with a symbol that provides evidence that the bitcoins on it have been spent. There are gift cards that are available online and at some retail stores that can be purchased and redeemed. In the future, there will be ingenious inventions that will allow Bitcoin or some similar currency be used just as the USD is used.

**Bitcoin is the Next...**

Bitcon is not the next Facebook, Apple, Google or Bank of America. It should be looked at more like the next telephone, internet or e-mail.

**Bitcoin Can’t Be Used to Pay Taxes**

I have heard a lot of arguments stating that Bitcoin is useless because it can not be used to pay taxes. This is currently the case, but it is easy to convert bitcoins to USD and possibly in the future, the IRS might reconsider. NYC is proposing allowing people to pay their parking tickets with bitcoins. This would save the people and the city to save a lot of money in financial fees with credit cards and mailing checks. Bitcoin would be useful for collecting tolls on highways. People could get a sticker on their car and have the payment automatically go through. This would save the highway management and people money by cutting out the banks from the middle of the transaction.

**Internationalization**

**Commentary**

I think the price of bitcoin is going to be hovering around the cost to mine a bitcoin. It can be calculated how much it would cost to invest in mining bitcoin versus buying bitcoin. People with deep pockets will choose the cheapest of the two. Over 3600 new bitcoin get mined every day. At $260, that is nearly $1 million everyday of new bitcoins that people will need to buy. The number of miners is growing. There is an all time high of the hash rate right now and it is growing. There are plenty of people that are buying bitcoin and saving them as a store of value. Also, the value of the USD is growing so more bitcoin can be purchased for less. There are plenty of people that want to buy bitcoin at lower prices. There are fewer people that are willing to sell the bitcoin for prices any lower. The technology and the computing power dedicated to bitcoin is huge. It will be used by the masses for many different purposes in the future. Once more people see that, more people are going to want to buy and hold onto bitcoin as a store of wealth. There are only about 13.8 million bitcoin available right now and there can only ever be 21 million bitcoin. The network behind bitcoin will be a lot more powerful than some banks holding hundreds of billions as a store of wealth. Currently, all bitcoin is worth about $4 billion. I think it will be worth hundreds of billions in the not too distant future. That being said, multiply the $260 by about 25 if all of bitcoin would be worth $100 billion. A lot of very rich people don't want to buy bitcoin because that is like funding the competitor for the current investments. Someone that is well vested into banking stocks, they don't want to see bitcoin take 10% of the market. That would be a loss for them. There are a lot of people that don't want bitcoin to succeed. There are also a lot of semi-rich and powerful people that do want to see bitcoin succeed. It will be used to send money around the world for free without having to give the banks a cut in the transfer. It will be used as simply a store of wealth. It will be used to safely make small purchases online so you don't have to worry about entering your credit card information for a $0.99 purchase at a random website. It will be worth a lot someday.

<http://www.amazon.com/Bitcoin-Internals-Technical-Guide-ebook/dp/B00DG8EPT0>

“Bitcoin is a revolutionary new digital currency that has the potential to create a paradigm shift in money and banking. No government or corporation controls Bitcoin; it's operated by a decentralized network of computers that anyone can join. This is the first time the world has ever seen such a radically new monetary system. But to fully appreciate Bitcoin, you need to see what's going on under the hood.”

**Should I Buy Bitcoin?**

In my opinion, I would say yes. Investing is always risky and this risk is higher than average. However, with great risks, come great rewards. It has the potential to go to extreme heights, but it is impossible to tell when. It could fall to a lower price and stay there for a while. We don’t know what that price might be. It could be replaced with a superior cryptocurrency. Governments could start creating their own crypto currencies. The USD might someday be a crypto-currency that will printed on paper embedded with a tiny chip.

**Should I Mine Bitcoin?**

In my opinion, I would say yes if you would enjoy doing it. It is not a significant difference compared to buying it right now. However, you could be mining bitcoin for cheaper than you could buy buy bitcoin. If the price jumps up in a few months, you won’t be able to buy it for as cheap as you could mine it. I would recommend mining bitcoin if you are a DIY hobbyist type of a person that would enjoy doing such a thing. I know it sounds silly, but heating homes in cold climates might be profitable. I just bought two AntMiner S5s because I have an un-insulated addition on my apartment that does not have heat. I live in New England. I was going to buy a space heater for that room... I do the mining as a hobby, but I think it would be a brilliant idea to make home heating systems as bitcoin miners. The components would need to be up-gradable to keep up with the growth rate of the processors required to mine. I'm thinking about getting a couple for each room... it would be cheaper than using my gas heat... a little bit loud, but i might be able to get used to it. Maybe I could attach a dryer vent around the front of it and place it in my basement having the heat come up into my apartment. This is where the future is heading. Home & Business heating will be done from the heat given off by a distributed system of supercomputers.

**Colonizing the Poles**

Another claim could be made that the profitability of mining bitcoin could be used to economically colonize the north and south pole. Portable homes that generate profits from the heat they generate could be airlifted to places in the north and south pole. There could be communities built around technology. And, even further craziness, this could lead to advancements in space travel and colonizing other planets such as mars. Heating would be expensive on mars. Maybe some complex mathematical models can be simulated with the technology that is created as a result of Bitcoin. I’m not claiming that this wouldn’t happen anyways, but Bitcoin is going to speed up the process. There is evidence that you can see by measuring the rate at which processing power grows. The amount of processing power on a chip typically doubles every two years. The processing power on Bitcoin mining power doubles every 6 months. The Bitcoin network has more 1300 times more processing power than the world's 500 most powerful supercomputers combined. These chips are very specific purpose for Bitcoin mining, but the advancements in technology will help to solve complex mathematical models. To name a few of the fields this will benefit:

* genetic sequencing,
* modeling the changes in the universe over time,
* artificial intelligence,
* quantum computing
* and, many more...

**Protocol Specification**

**https://en.bitcoin.it/wiki/Protocol\_specification**

**Community Agrees To Update**

If a general consensus among the Bitcoin miners agree to change the protocol, then this could have significant implications for the digital currency. This happens a lot for minor updates and is discussed in the Bitcoin community for major changes. There are scenarios where Bitcoin miners might want to change the having of Bitcoin rewards to every 8 years instead of every 4 years. I doubt that there would be a 51% or more agreeing to that in the community. It would be profitable for the miners to do such a thing. But, this would cause belief in the system to dwindle. People value bitcoin as a store of value and the price would plummet. Many miners are deeply vested into Bitcoin and they do not want this to happen because it would not be beneficial to them in the long run. This goes against the fundamental principles of a majority of the mining community. I don’t think that would happen. If it did, there would probably be a fork and the existing version would run in parallel to the new version. Then people would have to decide which fork to choose between. Current holders would want the old version and people that want to get on board and the miners might want the new version. I think that the community would see all the struggles that taking such an action would cause and they would not want to damage the market that they exist in.

TODO find some data, charts from <https://blockchain.info/>

Make a write up explaining what each chart means.

**Glossary**

* Bitcoin
* bitcoins
* arbitrage
* mining
* hardware
* software
* internet
* arpanet
* computer & network security
* Mt. Gox
* Silk Road
* Money Laundering
* Anonymous