An Introduction to Bitcoin's Economics and Technology, and How Government is Adapting

Joseph Gaughan
joseph.gaughan@purchase.edu

Abstract:

Bitcoin is a global currency. Its inception came about quietly, compared to its reach today. The founder, mathematician and computer scientist Satoshi Nakamoto, is shrouded in mystery. While little is known of them, their invention of blockchain and cryptocurrency has caused considerable change to many financial systems and social contracts we use every day. There are far reaching consequences of this new technology, from its considerable amount of uses to its far reaching and innumerable abuses.

1.) Introduction

Bitcoin is a decentralized virtual currency. A scam to some, but a revolution for others. Its introduction was brought about by, and relies on, the invention of blockchain technology. Bitcoin is a global phenomenon that spurred the uninformed masses to buy, what is in reality, a couple lines of arbitrary code.

To a wide variety of individuals, it has real value. Its technology may displace many systems of social contracts we, as individuals, comply with in our daily lives; it may change what we use as money, the way we handle transactions, encryption standards, and the financial sector in general. Bitcoin is the most widely used example of a successful blockchain implementation (Nakamoto 3). However, the applications of a public, immutable ledger are as limited as the extent of human thought. Surveys indicate over 80% of companies are looking into blockchain (Rooney).

One of Bitcoin's first mainstream appeals was that it could be used to buy government controlled substances online, and may have facilitated the major advancement of many online black markets. While this trend continues, government authorities are now able to trace most transactions in a blockchain (through Doe subpoenas), diminishing its usefulness as a means to avoid prying eyes.

Being such a disruptive technology, cryptocurrency has been a hot topic in the eyes of central banks. Few countries, such as China, realize how disruptive of a technology decentralized currency may become. No country has doubted the importance of blockchain, but many fear the economic impact of Cryptocurrency on government control of the money supply, along with the lack of consumer protection.

It is a currency whose existence is not based in paper notes, but instead substantiated by an accounting system based upon “unspent transaction outputs (UTXOs)” in a blockchain, and the ownership of a *private key* that is associated with said UTXO. It exists entirely on the internet, and relies on a data structure called a blockchain (D’Agostino).

Bitcoin’s development may have been a legitimate attempt to subvert government authority, but its creation was inevitable in the field of computer science. The blockchain is based on a relatively basic “linked list” structure. Its underlying technology is a way to store data in a form that no one entity has control over -- an immutable public ledger.

After discussing the economics, fundamentals, and data structure of Bitcoin, we will discuss why Bitcoin is inherently set up to fail by the year 2030, and what needs to change if that is not to be the case.

Part 1.) Economics of Bitcoin:

2.) Principles of Bitcoin

Bitcoin was created by an individual or group named Satoshi Nakamoto. Nakamoto began coding Bitcoin in 2007 (Narayanan xxiii). Their creation was only an experiment; they were most likely never expecting the currency to take off. Because their success was unexpected, Bitcoin experiences many technical limitations. One such limitation is only 21 million coins are allowed to exist; though this may be to induce artificial scarcity. This scarcity is very misleading, and many question its existence. If Bitcoin is to be a global currency, there will be a problem as there are only a max 21 million coins for 7.7 billion people.

A cryptocurrency not only incorporates cryptography to prevent tampering and provide equivocation, but also includes a mathematical protocol on the rules for creation of the currency (Narayanan 1). This encryption has allowed the currency to operate independently from a central banking system (whose accountants and ledgers keep track of funds), bypassing the red tape and transaction costs associated with online funds transfers. No one person is able to make new Bitcoin without putting in the considerable amount of effort of mining it. This was the original intended purpose: a currency with no mediating financial institutions to be able to reverse transactions or enact transaction costs. You are your own bank, free of high fees and censorship.

Paypal blocks funds for its own reasons that you agree to when you click the box for the terms and conditions. Those terms are made intentionally vague, and too long for anyone to read and interpret correctly. As Bitcoin does not have any terms, you are left more vulnerable to fraud as a result.

Bitcoin is completely open source, and available to be studied on its Github page. Anyone is able to copy Bitcoin completely and re-release it as their own cryptocurrency. Bitcoin is currently updated by developers of the Bitcoin Core, and is protected by an MIT license. If miners do not like an update to the core, they can choose not to use it. The miners that use the most used version have the best chance of solving a block. In this way, the workers have all the power. If Atlas were to shrug, it would mean very little; as the technology is already able to stand on its own (as long as it does not become compromised).

Bitcoin shares the properties of any currency: durability, portability, fungibility, scarcity, divisibility, and recognizability. Over 83% of all possible Bitcoins have been mined. The current market capitalization, as of February 23, 2019, is about $70 billion.

Once all Bitcoins are paid out to miners, no more will be generated. After which miners will be compensated only with transaction costs picked up by consumers as processing fees. This is where our issue with Bitcoin’s longevity is raised.

There are many incentives to use Bitcoin as a currency and as a medium of exchange, which drives its value (and therefore its price) as a currency up.

3.) What Determines Price of Bitcoin?

The price of anything is determined by scarcity, human and natural diversity, intrapersonal value, and imperfect knowledge. Our key focus is Bitcoin’s value -- why would you ever want this currency whose value is mostly extrinsic?

Bitcoin has very little intrinsic value. There is little use for Bitcoin besides as a means of exchange and a currency. Most of its value is extrinsic, as it relies on factors outside its value as a couple lines of code. Bitcoin, without its market and uses other than currency, is barely worth the electricity that’s used to mine it.

Companies have popped up as service providers for Bitcoin; everything from collective mining, online wallets (Bitcoin storage), and exchange. Coinbase and Blockchain Inc. are among the most popular Bitcoin service providers. The more people gaining access to Bitcoin, the greater its demand.

Bitcoin wallet software is now easy to access. It is as if someone were handing you cash through the internet; you don’t even need a bank account. Anyone with an internet connection and something worthy of exchange can trade Bitcoin. There are no third parties to go through -- the blockchain is a peer-to-peer network (Nakamoto 1). It is easier to manage than cash.

As with any currency, the value is determined by what it is able to be traded for. The first Bitcoin transaction for payment was recorded in May of 2010. A user on online Bitcoin forum “bitcointalk” offered 10,000 Bitcoins (about $41 at the time) for a couple of pizzas. He wanted two so he could eat and have some left over for the next day. He claimed to be a miner and knew he was giving away about $15 USD extra, but he didn’t care. Back then, he would have been mining thousands of worthless Bitcoins an hour. This is probably the most expensive pizza in history, traded for $13 million adjusted to recent BTC exchange rate.

4.) Potential Uses of Bitcoin

Bitcoin is potentially anonymous. Transactions are unregulated and there is no easy way to find who took part in a Bitcoin transaction. However, all transactions require a key from both users, most transactions require a physical id, shipping requires an address, and larger transactions must be reported to government authorities.

Bitcoin is a decentralized application; no single entity can control what happens to the price of Bitcoin and the ecosystem (Coindesk). Unlike, say for instance, Warren Buffett attempting to buy over 1/10th of the earth's investment grade silver in 2002. The currency stability does not depend on what members of government are mucking up this time (NPR). In recent years, however, this has changed.

Electronic payment services are sometimes difficult to use. This is mostly due to extensive regulations put in place to protect consumers. Sellers on sites like eBay often have their accounts frozen when they do not accept a return or a package gets lost in the mail. From personal experience (over 100 eBay sales), eBay almost always sides with the consumer in disputes. I have had to accept returns for unopened 60 year old pure silver Wallace silverware that was opened and returned, even when "no returns" was in the listing. This shows their values lie with the "customer is always right" principle, even when the customer is completely wrong. Bitcoin lacks these protections for consumers, so it is better for sellers, but not consumers.

In 2010, PayPal stopped all foreign and domestic transactions within India, leaving consumers and sellers on sites like eBay with their accounts and money frozen. Only recently has Paypal reopened Indian domestic transactions again (Paypal). Since Bitcoin has no complaint system or central authority, you cannot have your Bitcoin frozen or be stopped from sending and receiving, even from places like Syria and China.

Many countries, especially in South America and East Asia, have wildly unpredictable inflation rates. Venezuelan economist Carlos Hernández often states proudly that he owns no bolivars, keeping his liquidity totally in bitcoin, as opposed to another foreign currency. Bolívar soberanos (Sovereign Bolivar), the fiat currency of his home country, is projected to inflate at 1 million points a year.

Investors are now flocking to Bitcoin as an alternative to gold (Gershman). The currency started with a value under a cent. In July of 2010, Bitcoins went from \$0.008 to \$0.08, a 10x's increase. Tyler and Cameron Winklevoss had their bid for a Bitcoin-based ETF rejected by the Securities & Exchange Commision, which they had filed four years prior (Cochrane). A few other ETFs have had their bids rejected as well.

Bitcoins can be bought with a credit or debit card. By allowing currency to be bought with credit, the need for cash advances is negated. A cash advance is one of the most expensive credit card transactions that can be processed. Some credit card companies have caught on, adding the typical cash advance interest to the transaction. This depends on the transaction code the credit card company assigns to the Bitcoin vendor; some users report no extra interest charged on varying cards.

5.) Potential Abuses of Bitcoin

Bitcoin is the currency most used on black market TOR browser websites. TOR (The Onion Router) is a secure browser that operates via bouncing a user's internet traffic through a network of volunteers around the world. TOR is not just used for black market services; it is used in places where government keeps a close eye on internet traffic and to access blocked websites, such as Facebook in China.

The most known TOR black market Bitcoin exchange is the Silk Road 3. It is the third attempt at a public global drug market, the first 2 having been taken down by various authorities. It is very easily accessible, and I have done so for the purpose of this paper. These marketplaces have had a history of high commissions, ranging from four to eight percent (D'Agostino), making them lucrative for whoever's involved in the operation. Drug sales have been globalized for a while (drugs grown in Central & South America are smuggled into the US), but Silk Road was the first successful attempt at using a mass medium to sell drugs (Soska).

If a drug dealer is willing to risk a felony by receiving contraband through the mail, they can buy the best grade drugs for the best price possible, thanks to globalization. 28 grams of middle-grade marijuana (what consumers typically have access to) in New York is $200, but 50 grams of "Amsterdam coffeeshop weed" from Silk Road 3.0 vendor "Diabolito" (name of a notorious 19th century cuban pirate) costs $135. "Diabolito" also sells 4 types of weed, 2 types of ecstasy, 72% pure amphetamine, and what they claim is the "best quality fake currency." They have been operating for over 3 months, with 884 individual reviews left for goods they have provided. Consumers on Silk Road can leave reviews for vendors; in turn, vendors try not to rip people off with cut product or just bad service. While globalization of drug sales leads to more drugs sold, the quality and relative safety of the drugs goes up due to buyer ratings.

Part 2.) Government Reaction:

6.) Repercussions for unprecedented damages

In May of 2015, the original Silk Road's founder, Ross Ulbricht, was sentenced to multiple life sentences in prison (Paul). He began hosting the website in February 2011, and was shut down in October 2013. Judge Katherine Forrest of Federal District Court in Manhattan, is quoted as saying to Ulbricht "what you did was unprecedented… and in breaking that ground as the first person (Ross had to be exemplified)." She was right; Silk Road was the first relatively successful online anonymous marketplace. It introduced a new level of anonymity far superior to anything prior, thanks to Bitcoin, online or in real life (Soska 1).

Ulbricht attempted to challenge US laws regarding the sale and distribution of drugs, but Forrest deflected his arguments; Stating they were privileged and that "No drug dealer from the Bronx selling meth or heroin or crack has ever made these kinds of arguments to the court" (Paul). The US government calculated Silk Road 1.0's total gross revenue to have been $214 million (Soska 40), and he was charged with the death of 6 young people.

Silk Road 2 was run on the other side of the country in San Francisco, but its host, Blake Benthall, was caught much quicker. He was too busy buying luxury cars with Bitcoin to care about anything -- and that is how the FBI and ICE found him. The staff was infiltrated by at least one undercover law enforcement special agent before the site was operational. He was brought up on 5 charges that carry high sentences (D'Agostino).

Sileni, a "higher quality Silk Road" dark web site, is run by 2 Silk Road 3.0 admins. The only sellers allowed on this site are hand-selected top sellers from Silk Road, the best of the best criminals (ones that do not get caught). The goods cost more than Silk Road; this is in exchange for more stealthy packaging, faster shipping, no risk the seller you are buying from is a DEA agent, etc.

These illicit markets come and go. Buying contraband online will always be cheaper than locally -- consumers need to be convinced to take the risk, and competition on a global scale and larger operations means marginal revenue is closer to marginal cost for global firms. By firms, I mean larger drug operations that can afford to produce larger quantities at lower costs. Former Manhattan U.S. attorney Preet Bharara is quoted as saying "Let's be clear - this Silk Road, in whatever form, is the road to prison. Those looking to follow in the footsteps of alleged cyber criminals should understand that we will return as many times as necessary to shut down noxious online criminal bazaars. We don't get tired." Law enforcement has cut off the heads of many illicit online markets so far, but will they ever be able to address the underlying issues of why they keep appearing? Could it be the new level of potential anonymity cryptocurrency provides?

7.) Pressure from Governments

The IRS is ramping up pressure on Bitcoin service providers, focusing mostly on Coinbase Inc., to release customer records. Coinbase claims a customer base of 6.2 million across 33 countries, and has facilitated the exchange of over $6 billion in Bitcoin. The IRS wanted the records of all its US customers from 2013-2015, but after hearing Coinbase's argument, accepted the data of only 13,000. If you are one of those 13,000, the IRS is able to track you through your wallet software, if you have not mixed your coins or regenerated your public keys. The IRS wanted to investigate persons of interest: checking for laundering, hiding income, etc. via Coinbase. It served a John Doe notice to meet this end.

Michael Beckerman, chief executive officer of the Internet Association, stated in an email: “(The summons) amounts to nothing more than asking for large amounts of hay in the hope they might find a needle.”

At this point, it would be much easier and safer to go to a Casino and buy chips to hide your cash than buy and store Bitcoin, which have a digital signature (unless personally mined by the owner or traded physically). Much of what is driving Bitcoin’s popularity is its anonymity, take that away, and the demand for Bitcoin will fall. However, with anonymity comes abuse.

8.) Nothing on the Internet is Ever Deleted

You should never buy from one of these markets. As we have seen with the IRS John Doe notice, your transaction in the Bitcoin Blockchain may become compromised even years after the matter. Anyone with access to external information about your identity and one of your Bitcoin public keys, like the IRS, can find whom you’ve transacted with in the Bitcoin Blockchain, and how much money is associated with your wallet ID. Who knows what new methods governments and individuals will come up with to perform blockchain forensic analysis? The only individual who could stay truly anonymous would have to be knowledgeable enough in web security and privacy to invent a new method that has not been cracked already; then they would have to keep this new method a secret.

Part 3.) Technology Behind Bitcoin:

9.) How Bitcoins Are Traded By Consumers

Bitcoins are traded with what are called keys. There are public and private keys, and they are stored in one's wallet.

The public key is randomly generated in association with ones wallet address. The public key is the bitcoin address that receives the money. It is less important to keep safe than the private key, as the public key's only function is to allow the wallet to receive money. There are reasons to advertise this key online, such as a way to donate to websites and such. If the public key becomes compromised, it is easy to regenerate within your wallet software.

The private key is a 256-bit number that can be represented in a multitude of ways. The private key is the bitcoin address that proves ownership of an unspent transaction (UTXO), a.k.a. sends the money. To have a bitcoin is to know the private key associated with its UTXO. It is important to keep the private key a secret, as the user of the private key, in the eyes of the bitcoin network, is the owner of it (Coindesk). The most common way to store a private key is to reduce the key expression to 32 bytes using hexadecimal format. Here is an example:

Hexadecimal:
E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA
33262

- 64-bytes binary
- Each character is 4 bits, producing 256-bits

Binary:
111010011000011100111101011110011100011011011000011111011100000011
111011011010100101011101111000011000110011001110001001111101000100
010100110010000100110011000000111101101001100001111100100000101111
0101100111111111000010001100111010101000110011001001100010

- 256-bits binary

Every website that is HTTPS uses some kind of digital signature. A digital *signature* is a way to verify someone's identity online. It is a signed certificate that proves to the computer, and you, that the sender is the correct person/website/entity. Bitcoin's cryptography incorporates an elliptic curve digital signature algorithm. This ensures that funds are spent only by their rightful owner.

Bitcoin is difficult to trade due to its unspent transaction output (UTXO) model. An individual bitcoin cannot be divided without a transaction occurring. When a bitcoin transaction occurs, the coin is split in to the portion that is sent to the recipient, and the rest which is sent back to the sender.

Many transactions are lost in the system, unless a transaction fee is paid to miners to catalyze the verification in the blockchain. The average fee is high during times of high trading volume, and makes trading using bitcoin expensive sometimes. You may pay a $16 fee for trading $25 worth of Bitcoin. However, there are no fees or recurring charges after the transaction (unless authorized by the user). Bitcoin is a push technology, meaning each payment has to be initiated by the customer.

10.) How Bitcoins are Mined

New Bitcoins are generated through a process called mining. Miners host a Bitcoin Blockchain node (a.k.a. server). The blockchain is a public ledger of all Bitcoin transactions that are completed by individuals trading via the bitcoin network. Miners receive new transaction records made by individuals trading bitcoin, and add them to the copy of the blockchain they are hosting. Juxtaposed to the centrality of our current trusted third parties (governments, banks, accountants, notaries, and paper money), the blockchain maintains collective bookkeeping via the internet. The ledger is public and fully distributed across the Bitcoin network. This is what prevents Bitcoins from being reused after a transaction or counterfeited; the system always knows how many Bitcoins should exist. Once a transaction has been verified by at least six miners, it would take half the total power of the Bitcoin network for an attacker to tamper with a transaction: thousands of terahertz of processing power, costing over 400 megawatts of power per second (equivalent to powering over 200,000 US homes for a year). It is a very secure system.

When miners receive a new transaction record, they each add it to the block they're currently attempting to solve. A Block is a page in the blockchain ledger. It contains some or all recent transactions on the Bitcoin network, details from the previous Block (creating a chain of blocks), and other types of data. Bitcoin miners have equal access to new transactions, making the market very competitive. Each transaction via the Bitcoin Blockchain takes about 8-10 minutes, after which the blockchain will have recorded the Bitcoins in client A's wallet as spent, return the change to the sender and add the appropriate amount of Bitcoins to client B's wallet.

Each time a transaction is recorded, a new hashcode is generated. A hashcode is a general programming term used to describe a number that is generated by a program. The bitcoin hashcode is compared to the current difficulty level set by the bitcoin network -- which is based on the properties of mathematics. If the hash is below the difficulty that is set, the block is solved (Nakamoto 15). The hashrate is the number of times the hashcode function can be computed per second. The hash is also called a proof of work. There are many different hashes that can solve a block, and a proof of work can be easily verified when it is sent to the rest of the blockchain. The more miners hosting the blockchain, the more blocks get solved. The difficulty adjusts so 2,015 blocks should be solved every 2 weeks. If 2,015 blocks are solved earlier or later, the difficulty rises or falls, respectively. As of April 2019, solving a block currently generates 12.5 inherently anonymous Bitcoins (unable to be traced since they have not been traded yet) paid out to the lucky winner.

Every 210,000 blocks, the amount of Bitcoins paid out per block is halved. It is a geometric sequence; the starting reward was 50 BTC so, with n=number of times 210,000 blocks has been reached, the equation is:

$$\sum_{n=0}^{\infty} 50(\frac{1}{2})^n = \text{current bitcoin reward}$$

While it is possible to solve the current block after only one transaction (the gambler's fallacy), the expected time it would take for my 7 year old office computer's non-specialized hardware to solve one block (using my gpu's clock speed, CUDA core count, and memory frequency to calculate hashing rate) is 6,446,736 years to solve one bitcoin block. Top of the line modern ASIC (application specific integrated circuit) chips can solve over a trillion hash codes per second. There are only about 4 out of 21 million bitcoins left to mine.

An individual's chances to solve a block years ago was much higher. As processing power increases, so does the difficulty. Mining began with enthusiasts using typical consumer CPUs, and their varying server relatives. Since then, it has been a race to having a comparative advantage in efficiency and speed over other miners. GPU mining was later realized to give speeds 50-100x's higher than a CPU. Special purpose chips have now been invented just for hosting applications such as the blockchain ledger. ASIC and FPGA (field programmable gate array) chips have made the opportunity costs of GPU mining, let alone CPU, more expensive than the expected Bitcoin payout. ASIC chips must be purpose built for Bitcoin mining. Using an ASIC device is the most efficient way to mine, delivering the fastest mining speeds at the lowest energy consumption. An ASIC computer fully capable of running a mine is purchasable at the price point of $400, and it will blow any general integrated circuit (cpu or gpu) out of the water, in terms of hashing rate. The increase in speed leads to an increase in difficulty; An application specific chip is almost required for any mine to be close to profitable (Hesoid).

11.) Collective Mining

Collective mining is a subscription based service where people buy “shares” of a mining operation. The more people pay in, the more hardware and bandwidth a server host can afford, leading to faster mining speeds. It is akin to community supported agriculture in that the more people pay in, the greater the payout for all. With difficulty rising, technology improving, and more miners entering the market every day, collective miners band together to evenly distribute Bitcoins that are paid when a block is solved to “shareholders.” Server hosts, of course, take out electricity and fixed costs, as well as a cut for themselves.

12.) Anonymity on the Bitcoin Network

To stay somewhat anonymous, users employ virtual private networks, end-to-end encryption (a technology Bitcoin employs in its hashing functionality, but is typically absent in vanilla payment technology), and PeerBlockers while exchanging Bitcoins. Users with malicious intent use what are called a Bitcoin “mixer” or “tumbler” to launder the Bitcoins they have obtained. Bitcoins in themselves are traceable (unless the private keys are transferred outside the bitcoin network or generated via mining), via the blockchain. A mixer protects the user from “blockchain analysis,” a process where someone with interest in tracking activity can view all a user's transactions in the blockchain with some form of external identification and the user's public key and one private key. Financial institutions may request this as a Bitcoin Credit check (Chainalysis). A mixer changes the Bitcoins in your wallet into different Bitcoins, throwing off the paper trail.

13.) Why You Should not Invest In or Use Bitcoin

Bitcoin is uninsured: no FDIC, no purchase protection, no fraud prevention. Someone with access to your wallet's stored private keys can steal every Bitcoin you have in it, then disappear; then you are stuck. Thousands of people report Bitcoins being stolen from their accounts. The most lucrative thefts are targeted at online services, which store a copious supply of member's private keys. The largest theft was from users of an illegal marketplace called "Sheep Marketplace." A Vendor exploited a vulnerability in the site's security to steal 40,000 BTC at once from site admins and users alike. The thief's transactions have been able to be traced in the blockchain, but no real-life information has been found on the thief, meaning they are still anonymous (Jeffries).

Many intelligent individuals believe the Sheep Marketplace owner absconded with escrow funds, conveniently claiming it was stolen. Kyle Soska, a Ph.D. student in the Department of Electrical and Computer Engineering at Carnegie Mellon University, believes the the site owner had done so (Soska 36). Nothing you do online is safe; stealing Bitcoin, regardless if it is from criminals or law-abiding citizens, is extremely difficult to trace without some sort of identification.

Some Banks have machine learning algorithms to detect fraudulent transactions, but Bitcoin does not care. It is up to you to keep your coins secure.

With no central authority, the Bitcoin system will begin to lose traction once the amount of Bitcoins paid per block is reduced to single digits per reward. When the next 210,000 blocks is achieved, miners take an immediate 50% pay cut on already increasing difficulty. This increase will cause some miners with higher variable costs (less optimized and powerful equipment) to shut down temporarily or drop out (unless benevolent or an enthusiast), lowering the difficulty. For the lowered difficulty to offset this pay cut, the 2,015 blocks per 2 weeks quota would have to take twice as long to solve (only possible if total computational power of all servers is halved, or about half of firms stop mining) or the price of Bitcoin doubles by the time each the payment is halved. This would lead to longer wait times for transactions with low transaction fees, meaning less demand for bitcoin, and a fall in the price. Miner's only incentive to operate at that point is by charging transaction fees, but one of the dogmas of Bitcoin is that it is cheap to use. While the price of a Bitcoin has increased exponentially, the chance of an individual solving a block has gone down significantly. Even if my predictions are incorrect, the last block with bitcoins allocated to its completion is projected to be solved around 2030; This means there will be no further incentive to mine.

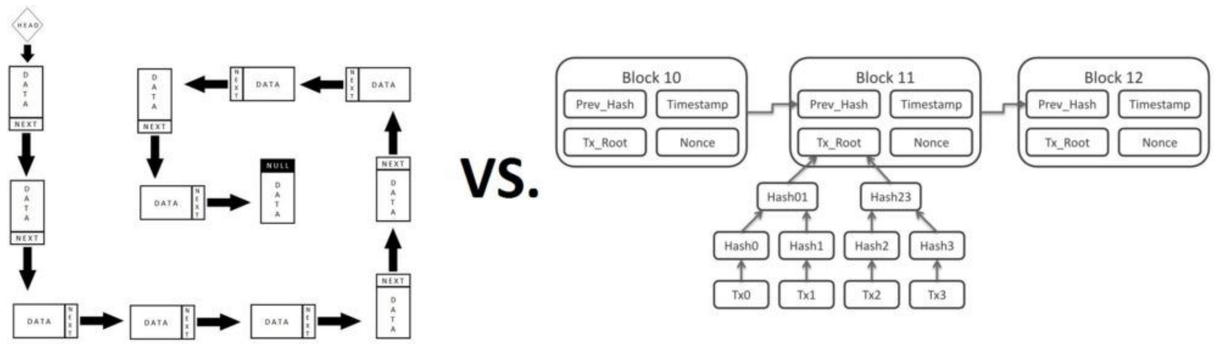
If a powerful enough quantum computer comes in to existence, it may be able to find collisions in Bitcoin's SHA-256 mining algorithm -- a process that would normally take years with the most powerful current equipment. Also, if quantum computers are only used to attack and not mine Bitcoin, the user of the quantum computer could easily take over a significant portion of the Bitcoin network, and cause significant issues.

If a typical consumer is unable to trade Bitcoins without it taking days to exchange them or having to pay an integer transaction fee, as they normally would with a credit card, they would be better off paying with their fiat currency, credit card, or another cryptocurrency. Bitcoin's hashing algorithm, and therefore anonymity, is becoming increasingly less effective as both government and individuals find work arounds and exploits to use against the blockchain.

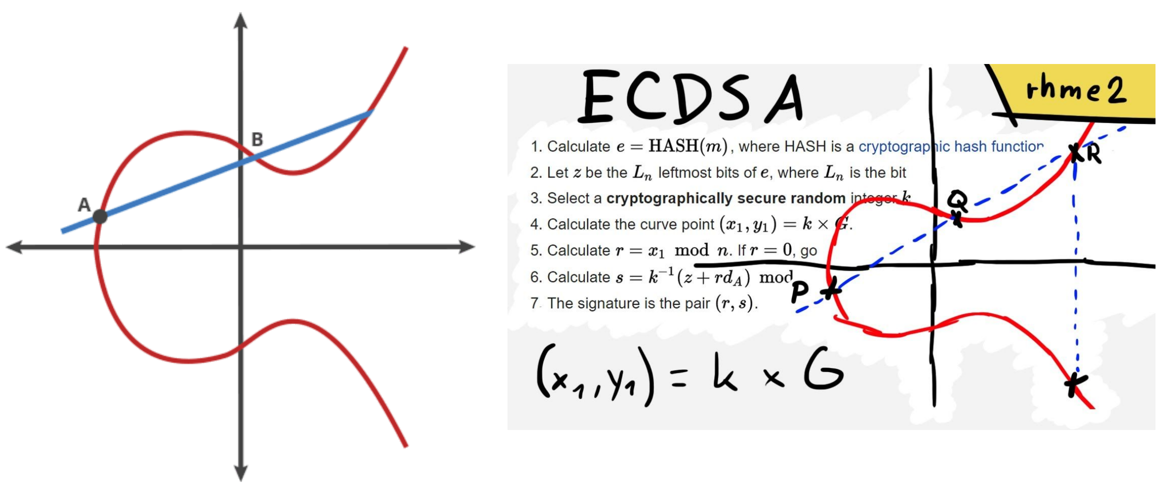
Take away the anonymity and low transaction fees, and what is the advantage of Bitcoin over another cryptocurrency? The principles of Bitcoin will survive, and, from the ashes, I feel a better form of cryptocurrency will arise.

Appendix:

A.) Picture of linked list structure vs merkle tree of Bitcoin:



B.) Picture of Elliptic Curve Digital Signature Algorithm:



C.) *[My cryptocurrency, PurchaseCoin]*

https://github.com/Shoneys/PurchaseCoin

D.) *Presentation on value of Bitcoin, which lays in the proof of work*

https://docs.google.com/presentation/d/1SlaKK5fVgc9ZmK_rw3_K9RW0gW4CkpPK7g5s58-XvP0/edit?usp=sharing

E.) *Presentation on cryptography, with emphasis on Bitcoin's algorithms*

https://docs.google.com/presentation/d/1De7jyiTVYly_qjsCARAGcx0Jp9GVRhN3fjtHiCvJxPE/edit?usp=sharing

Works Cited:

Cochrane, Matthew. "So You Want to Invest in Bitcoin: Here's What You Should Know." The Motley Fool. N.p., 25 Mar. 2017. Web. 28 Mar. 2017.

- Bitcoin ETF information

Gershman, Jacob. "IRS Crackdown on Bitcoin Exchange Fuels Privacy Worries." The Wall Street Journal. Dow Jones & Company, 27 Mar. 2017. Web. 28 Mar. 2017.

- IRS John Doe notice and market uncertainty

"Everything you need to know about Bitcoin mining." Hesiod Services LLC, n.d. Web. 28 Mar. 2017.

- Explains mining process and Blockchain

Nakamoto, Satoshi. "Frequently Asked Questions." FAQ - Bitcoin. Bitcoin, n.d. Web. 09 May 2017.

- Frequently Asked Questions about Bitcoin

CoinDesk. "How do bitcoin transactions work?" CoinDesk. CoinDesk, 20 Mar. 2015. Web. 09 May 2017.

- Explains private and public keys and wallet address

Jeffries, Adrianne. "How to steal Bitcoin in three easy steps." The Verge. N.p., 19 Dec. 2013. Web. 09 May 2017.

- Explains how easily Bitcoin can be stolen and laundered

Nagamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” 2008. Web. 1 May 2017.

- Basic explanations for many Bitcoin principles

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin: A Peer-to-Peer Electronic Cash System (2008): 1-9. Bitcoin. Web. 5 May 2017.

- Nagamoto’s thesis for cryptocurrency.

Narayanan, Arvind, Joseph Bonneau, and Edward W. Felten. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton U Press, 2016. Print.

- Defines cryptocurrency and provides history

D'Agostino, Vincent. "Blake Benthall Criminal Complaint." Scribd. US Attorney's Office, n.d. Web. 09 May 2017.

- Criminal complaint against Blake Benthall, life sentence

Paul, Kari. "Unsealed Transcript Shows How a Judge Justified Ross Ulbricht's Life Sentence." Motherboard. Vice, 5 Oct. 2015. Web. 09 May 2017.

- Transcript of Ross Ulbricht’s Trial

“Latest Bitcoin Version Release Notes." GitHub. N.p., n.d. Web. 9 May 2017. <https://github.com/bitcoin/bitcoin/blob/v0.12.0/doc/release-notes.md#relay-and-mining-priority-transactions>.

- Release notes for latest version of Bitcoin Blockchain client. Details new features for priority transactions, in which users are able to allocate more btc for a faster transaction processing speed.

Soska, Kyle. "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem." Proceedings of the 24th USENIX Security Symposium(2015): n. pag. USENIX. Web. 8 May 2017.

- How Bitcoin has furthered the development of online drug sales and marketplaces.

Rooney, Kate. “84% Of Companies Are Dabbling in Blockchain, New Survey Says.” *CNBC*, CNBC, 27 Aug. 2018, www.cnbc.com/2018/08/27/84percent-of-companies-are-dabbling--in-blockchain-new-survey-says-.html.

- How many companies are looking in to Bitcoin

Pizza for Bitcoins?, bitcointalk.org/index.php?topic=137.

- First bitcoin valuation, pizza reference

Joffe-Walt, Chana. “How Fake Money Saved Brazil.” *NPR*, NPR, 4 Oct. 2010, www.npr.org/sections/money/2010/10/04/130329523/how-fake-money-saved-brazil.

- Hyperinflation in South America

“Bitcoin Is A Hedge Against Bolivar-Induced Financial Suicide, Claims Venezuelan Economist.” *NewsBTC*, 24 Feb. 2019, www.newsbtc.com/2019/02/25/bitcoin-hedge-bolivar-financial-suicide-venezuelan-economist/.

- Carlos Hernández views on Bitcoin. “Not owning bitcoin is financial suicide.”

“PayPal Launches Domestic Operations in India.” *PayPal*, www.paypal.com/stories/us/paypal-launches-domestic-operations-in-india.

- Paypal reopens operations in India; written in positive tone, seems odd for the hardship they caused

Links:

https://www.chainalysis.com/

- Bitcoin Blockchain analysis service

https://dnstats.net/other/BitBlender

- Abstract, finds TOR urls

http://reloadedudjtjvxr.onion

- Silk Road URL, accessible via TOR browser. Changes frequently

http://Bitblendervrfkzr.onion

- Bit Blender URL, accessible via TOR browser