Bitcoin: How does it Work and Where is it Going?

Merrilee Gibbs Davolt

Abstract

This thesis will introduce and develop the ideas behind electronic forms of monetary transaction, focusing on a new technology called Bitcoin. In an effort to analyze Bitcoin, we must discuss what money is at its core, its role in the economy, and its importance in society. The launch of Bitcoin, its potential pros and cons and how it could impact our current system will all be discussed. The importance of the science behind Bitcoin, the blockchain, and how this could be implemented is examined. Questions are posed and ideas are offered about how this technology may impact our current economic system.
Money

In order to analyze Bitcoin, it is crucial that we first understand some fundamental concepts about money in the United States. Money in the form of U.S. dollars plays a large role in our economy. We use it to buy things we want and need, we accept it in exchange for our physical and mental labors, and we can’t imagine how we could function without it. But there was a time when money didn’t serve as an economic backbone. Before paper money, gold and silver were exchanged, and earlier yet, goods and services were traded on a personal level to ensure that peoples’ needs were met. European settlers in what is now the United States were familiar with the idea of money, because most were exposed to it in their homelands. But in a new and undeveloped land, paper money was scarce and its value wasn’t as secure so far away from home. As new Americans cut their ties to Europe, establishing their own country also involved establishing their own currency. So, use of money wasn’t a luxury that many had access to, and instead they reverted back to simple bartering of goods until they could establish a new currency of their own\(^1\) (History, n.d.).

The first use of paper money dates back to around 960 A.D. in China (Bellis, 2015). Originally, these paper notes simply served as representation of gold that was being held in banks. They were like a receipt for the gold deposits that had been made with the banker. The paper only derived its value from the gold in the vault, but people began to exchange the paper instead of carrying around bulky, heavy gold pieces (Karlan, 2013).

Today, the money that we use is not based on any amount of gold or other commodity. We trust that it has value because our government insists that it has value and we trust that it

\(^1\) The Federal Reserve Bank of Boston gives a detailed timeline of money in the early U.S. in its publication titled “History of Colonial Money”.
operates as such. Money like this, that isn’t commodity, backed is known as fiat money (Karlan, 2013). We have reached the point where every major currency is no longer commodity backed.

However, fiat money has seen a lot of downfalls and has faced much scrutiny (Jones, n.d.). Since it is controlled by the government, the government can devalue money to inflate its way out of debt. Additionally, since money is no longer backed by gold, some are worried about whether it will retain its value or whether it will fail. Returning to the gold standard is something that has been suggested by politicians such as Ron Paul who stated “Gold rose to nearly $1800 an ounce after the Fed’s most recent round of quantitative easing because the people know that gold is money when fiat money fails,” (Should United, 2013). However, most economists agree that returning to a gold standard would do nothing to help our economy and might even do more damage to a system that is still growing after our last recession. Economist Paul Krugman, a Nobel Prize winner stated “returning to a gold standard ‘an almost comically (and cosmically) bad idea,’” (Should United, 2013).

In an article by Glenn Zorpette, he suggests that most would concede that our current system is okay, so why change it? Well, for as long as there has been government, there has been opposition to government. Technology has made an exponential impact in our daily lives and our transactions are done electronically more and more often. But the government controls the currency, and banks and credit card companies have access to all our transaction history. Even when the transactions we are making are perfectly sound and legal, many Americans would prefer that their financial information stay private. An example of such a proponent is the aforementioned Ron Paul, who prefers a more limited government. Continuing to use cash allows for this privacy, but electronic transactions are much more convenient.
Many people have been working to offer some other way to facilitate transactions apart from use of the U.S. dollar that accomplishes all the things that the dollar currently accomplishes (Zorpette, 2012). This fiat money on which we so heavily rely shares three important characteristics with every other form of money that are laid out by Cecchetti and Schoenholtz. In order to challenge the dollar, any competing currency would need to successfully accomplish these characteristics. Firstly, money is a means of payment. We want to receive it so that we can spend it to get other things that we want. Both parties in any transaction have to be willing and able to give and accept it. Next, as a unit of account money serves as a standard by which we compare things. One unit must be equivalent to one unit when comparing the price of apples to that of oranges. Lastly, as a store of value money must retain a relatively constant value from day to day. A ten-dollar bill received today should be worth ten dollars tomorrow (Cecchetti, 2014).

**Bitcoin**

That’s where Bitcoin comes into play. According to Marc Andreessen’s Article “Why Bitcoin Matters,” electronic money is an idea that has been researched and developed for several decades (Andreessen, 2014). Bitcoin is just one such developed example that caught a lot of attention in recent years. Bitcoin made its first appearance when an author using the name Satoshi Nakamoto published a paper on October 31, 2008 entitled “Bitcoin: A Peer-to-peer Electronic Cash System.”2 His paper lays out the groundwork of the Bitcoin system. The true identity of Nakamoto remains a mystery, but as the owner of over a million Bitcoins, he could have a huge impact on the Bitcoin economy (Bitcoin Creator’s, 2015). More trust could be gained if we knew who has such influence.3

---

2 Nakamoto’s paper is accessible to anyone online. See reference “Nakamoto.”
3 See National Public Radio’s segment titled “Bitcoin Creator’s Mysterious Identity Beguiles Cryptography World” for more on the story of Nakamoto’s identity.
When trying to understand what Bitcoin is and what it can accomplish, it’s helpful to think back to a time when using cash transactions was more commonplace than using a credit or debit card. Cash was simply exchanged in return for a good or service. There was no way that the cash you used could be traced back to you; your personal information wasn’t linked to the paper bills. The payment was automatic; there was no middle-man in the form of banks that exchanged funds for your transaction to be complete. The goal of bitcoin is to offer this same type of quick, secure, and anonymous transaction, while also existing in an electronic form.

The technology of Bitcoin brings with it many benefits. For some, the primary benefit is that this system is entirely separate from our current banking system, with zero government intervention on it. This attracts those that question and have concerns with government’s role in money regulation.

CoinReport lays out other major advantages and disadvantages of Bitcoin. With Bitcoin, funds can easily be exchanged across borders without the major fees they currently face. You don’t have to worry about transactions not being processed just because a bank is closed for a holiday. This helps families that are forced to be apart in order to make enough money to live, as well as travelers who can avoid transaction fees when converting currency.

All Bitcoin transactions are both transparent and protects users’ identities. This is because all Bitcoin processing computers have access to a ledger that contains all transactions since the very beginning of Bitcoin, but all that can be seen are the public addresses used in the transaction. No personal information can be found through this number and it can’t be traced back to you.

Another benefit is that Bitcoin charges little to no fees when transacting currency exchanges. Our current system can charge high fees so that charging a small amount, for
something like access to read an online magazine article, would cost more to move the money
than the original cost incurred. With Bitcoin, you can transact coins down to eight decimal
places, so small transactions are still possible.

Finally, transactions with Bitcoin are secure. Transactions in the Bitcoin ledger cannot be
reversed or undone, so merchants are assured that if they decide to accept Bitcoin, they will get
their money. This is true even in areas where fraud and crime are prevalent.

Conversely, Bitcoin has several disadvantages, which are to be expected with a currency
in its infancy. Most people have never heard of Bitcoin, so it’s not widely accepted. People will
need more knowledge of this technology if it is going to have any lasting place in our world as a
regular currency. The technology itself is very new and very foreign to people who haven’t taken
time to learn about the intricacies of the system. There are still few businesses that accept Bitcoin
as a means of payment. You can find more in bigger cities, but rural populations have little
access to spending Bitcoin at businesses in person. Even online, spending Bitcoin isn’t the
easiest feat (See Appendix).

Because of its volatility in relation to the dollar, Bitcoin’s ability to serve as a store of
value and unit of account is negatively affected. Figure 1 shows the severity of its volatility. A
lot of the people that own Bitcoin, do so as an investment, rather than a currency to be regularly
exchanged. The price of Bitcoin has seen major highs and lows in dollar value, and therefore it
hasn’t gained as much trust from the public.

Figure 1: This graph shows the value of a single Bitcoin in relation to its value in U.S. Dollars from April 2014 to March 2016 (Market Price, 2016).

We haven’t neared it yet, but by design there is a maximum number of Bitcoins that can be created. This will cause the price of Bitcoins to stabilize in the long run. This highlights the concern some have regarding the Fed’s control of the dollar – it might create a large surplus causing inflation. With Bitcoin, there is no problem with a large surplus since there is no government intervention or control and there is a finite limit on the number of Bitcoins.

However, this also highlights what some would see as a major drawback. Without the ability to increase the number of Bitcoins, the currency can’t grow with a growing economy (Cecchetti, 2014).

Since Bitcoin is decentralized, there is no formal group of people in control of it. However, there are individuals who have taken it upon themselves to popularize Bitcoin, invest in it, and address some of these disadvantages. A man by the name of Gavin Andresen has taken a large interest in Bitcoin and serves as the chief scientist at Bitcoin Foundation, where their “focus is to foster education, engage in advocacy, increase adoption and encourage development
of bitcoin and blockchain technology worldwide,” (About Us, n.d.). In early 2011, Andresen participated in the first Bitcoin transaction where a physical good was bought and sold. He purchased a pair of Alpaca socks from an alpaca farmer who lived nearby (Andresen, n.d., Open Source, 2011).

Andresen has played a major role in Bitcoin’s success, but he is not to be confused with Marc Andreessen, who was cited earlier in this report. Marc Andreessen is a co-founder at Andreessen Horowitz, alongside Ben Horowitz. Andreessen Horowitz is a company that “backs bold entrepreneurs who move fast, think big, and are committed to building the next major franchises in technology,” according to their website (About Andreessen, n.d.). As a company, they have invested $50 million in start-ups related to Bitcoin (Andreessen, 2014).

**Blockchain**

What is even more interesting than Bitcoin as a currency is the computer science on which Bitcoin relies. The highly technical Blockchain is the backbone of Bitcoin technology.\(^4\) The complexity of this highly technical idea was best explained in a YouTube video titled, “How Bitcoin Works Under the Hood.”

On a simpler level, the coins must first be created through a process called ‘mining.’ Computer processors that perform these functions are the ‘miners’ of Bitcoin. Mining involves solving large, complicated mathematical problems, but this is done solely through the computational power of the miner’s computer. Every new mining computer starts by getting a record of the entire Blockchain, from the beginning. All of these mining computers work together and serve together as a blockchain network using the Internet. There is no central

---

\(^4\) To view Blockchain in action, visit https://blockchain.info/.
location for the technology and no one individual controls it. Collectively, the blockchain network of computers controls Bitcoin.

Anyone can offer up their computer power to mine and begin doing so by downloading appropriate software. Miners are rewarded small fractions of Bitcoin in return for their work. This reward is received if you are the first one to solve the algorithmic problem that is presented by beginning a new transaction. These are the “little-to-no” transaction fees for spending and receiving Bitcoin, which are much less than transaction fees from banks. Still, to make money as a miner, one would have to take into account how much they are spending on energy to run their computer. Miners earlier on in Bitcoin’s life were able to make significant amounts of money. At this point, it is, however, possible to come out behind in an endeavor to make money mining Bitcoin. There are calculators accessible online that can figure out how much you could make or lose based on your computer power and cost of electricity, among other things.

Since there is a chance for earning some profit in mining, when a new transaction comes in, many computers quickly begin working on the mathematical problem associated with the transaction. This serves to insure that transactions are speedy and secure. And as new transactions are added to the Blockchain, past ‘blocks’ in the chain become more and more secure. Figure 2 gives a visual of what takes place to form a block in the chain. Once a block is added to the chain it can’t be undone and you can’t spend Bitcoin if you don’t have any to spend. This is important because, instead of keeping a separate ledger of how many Bitcoins a user has, the blocks instead reference past transactions where they received Bitcoins, in order for the user

---

5 Learn more about mining software at: https://www.bitcoinmining.com/bitcoin-mining-software/.
6 One such calculator is available at: http://www.bitcoinx.com/profit/.
to ‘spend’ the Bitcoins. The references in the blockchain serve as the ledger which keeps track of each individual’s account and how many Bitcoins they own.

Figure 2: Each transaction builds on others to form the ‘blocks’ of Blockchain (Great Chain, 2015).

To the user, none of the complicated mechanisms of Blockchain are seen. The mining operations all take place in the background. Bitcoins can easily be bought by someone who has little to no past experience with Bitcoin⁷ (CuriousInventor, 2013).

What’s Next for Bitcoin

Bitcoin still has many disadvantages that are being addressed. The fact that most people have never heard of it is its biggest drawback, and is one that will simply take more time to

---

⁷ To buy Bitcoins, simply visit a website like https://www.coinbase.com/.
overcome. However, Marc Andreessen argues that the Blockchain technology is simply a huge breakthrough in computer science that cannot be ignored.

Even if not in the form of a currency, Blockchain has other advantages. Its technology could guarantee security and an ability to buy and sell easily. An example would be home sales which require a lot of paperwork today. The Economist’s article “The great chain of being sure about things” tells the story of a Honduran woman who was evicted and whose home was demolished, after having lived there for thirty years, because her government didn’t have the paperwork stating that she owned the land. Her information was eventually found, but it was too late. She is one of many people who live in a place with poor records of property rights. Blockchain offers a secure way to store information of this type, and many other types (Great Chain, 2015).

People have been working to develop a program that will allow users to safely spend and receive “money” over the internet. Bitcoin allows them to do so without a user spending the same Bitcoin that they have already spent. They can try, of course, but the technology of Blockchain ensures that their fraudulence will not go unnoticed and will be corrected. Since the Blockchain is kept up by every computer that serves as a miner for the program, Bitcoin has been and always will be decentralized. Bitcoin users will never have to worry about the government coming in and taking over this system, because to do so, they would have to come into individual homes and take control of hundreds of thousands of computers. This just isn’t feasible or legal in the world in which we live.

However, the world we live in still heavily relies on and trusts in the dollar. Bitcoin would need to gain a lot of trust from everyday consumers and business owners. With the volatility in the price of a Bitcoin, it is far from gaining that trust. Over time, its price has begun
to tend towards stabilization. Just like a dollar today is very close to being equal in value to a dollar tomorrow, so Bitcoin needs to have a very stable value day-to-day. Many of the people that have bought into Bitcoin have done so as a means of investment. The value of Bitcoin has gone up, so people have had a reason to let their money sit in Bitcoin and grow. If Bitcoin is going to succeed as a currency, rather than an investment, there needs to be less of a reason to let it sit to gain value and more of a reason to spend it and use it in everyday transactions. In order for Bitcoin to gain popularity, it needs to successfully accomplish these three characteristics of money: a means of payment, a store of value, and a unit of account.

Many are critical of Bitcoin’s future, especially those more closely related to the success and sustainability of the U.S. dollar, for example the Federal Reserve. Some would argue that Bitcoin is a major breakthrough, but that it doesn’t quite have what it takes to stick around for much longer. Still others see a bright future for Bitcoin, but realize that it may take a while for that success to be evident. Two people felt so strongly in either direction that they decided to place a bet on the future of Bitcoin. They stated their opinions and declared the terms of the bet on a segment of NPR’s Planet Money titled “Episode 515: A Bet Over Bitcoin.” One is a co-founder and partner at Andreessen Horowitz, Ben Horowitz, who has a Master’s degree in Computer Science. The other, Felix Salmon, is a financial blogger at the international news agency, Reuters. These two men formalized a bet on air with National Public Radio that aired on February 5, 2014.

Horowitz believes that Bitcoin has a bright future. To him, the way it merges computer science and economics is revolutionary. He points out that companies that do business online are

---

8 For a perspective presented from the Federal Reserve Bank of St. Louis, see reference “Thorton.”
subject to high fees and can’t accept business from certain countries. Bitcoin solves these issues and many more. He acknowledges that people do seem to be storing their money in Bitcoin, but believes that when it reaches a more stable price, additional people will use it as a currency. On the other hand, Salmon believes that Bitcoin is not the solution to the problems with the current system. Since there is a maximum number of Bitcoins that can be mined, it will in the long run become a deflationary currency, which is something we haven’t seen in a long time. He doesn’t believe that people will begin to use it as an everyday currency.

Now that their views are stated, they set the terms of the bet. They decided to give Bitcoin five years from January of 2014. So in January 2019, Planet Money will post a poll asking viewers of their site if they have used bitcoins to buy something in the past month. If ten percent or more vote that they have, this implies that Bitcoin is being used to make transactions and Horowitz wins the bet. However, Salmon wins if less than ten percent of poll participants are actively spending Bitcoin. This means that it really isn’t being used as a currency and likely has no future. The winner is rewarded with their own pair of the first item purchased with Bitcoin, a pair of alpaca socks (Horowitz & Salmon, 2014)

This bet is representative of two strong viewpoints in the world of Bitcoin. It is impossible to say how far Bitcoin will make it in the United States, but there is most assuredly a lot of potential with the tools that Blockchain has given us. Check back with NPR’s Planet Money in 2019 to learn how much of an impact Bitcoin will have had in those five short years.
References


Appendix – How to Buy and Spend Bitcoins

To learn about buying and spending Bitcoin, I contacted Dan Sokoloski, a friend of Dr. Watters, my thesis advisor. Dan had bought and used Bitcoin for a number of years and recommended I buy mine through an online Bitcoin wallet called Coinbase.

To begin, I went to the default page of coinbase.com and was prompted to enter my email address. From there, I set up an online account, giving only my name, state, and choosing a password for security. A verification email was sent to ensure that the same person was accessing the coinbase account as the email account. I verified that this was my email with the click of a button. Back on the coinbase site, I began a list of steps to purchase my first amount of Bitcoin. I was prompted to enter my cell phone number, that they would later use as another way of ensuring my identity when accessing my account on different devices or computers. I received a text message with a 7-digit code to enter on coinbase. On this page where I entered the code, I was given the option to receive a phone call to obtain the code. So, it seems that a cell phone is not crucial to the process. Next, I needed to select the bank that I would be using to pay for my Bitcoin purchase. Several big banks are listed and after clicking on one of them, you will be prompted to give coinbase your username and password for your online account with your bank.

This following message was given: “Coinbase does not store your bank login credentials, although our service provider may do so as necessary to provide services to Coinbase. More information on how your credentials are stored and used is available here.” On the other hand, I had to select “Other Bank” and offered up my bank’s routing number and my account number. I was then prompted with two options: “Instant Account Verification” and “Deposit Verification.” The first was estimated to take a few minutes, and the latter 2 - 3 business days. The first time through, I took the longer route in hopes of somehow giving less information. After taking the
shorter route my second time through, I see no benefit to using the Deposit Verification. We were then able to enter the USD amount of $10, which equated to 0.02659485 BTC at the time. Using Deposit Verification, over the course of several days, two small, random amounts of $0.09 and $0.14 were deposited into my bank account. I subsequently entered these particular amounts into coinbase to verify that this was my bank account by having access to these random numbers. Two days after those deposits were made, a $10 withdrawal was made and I was now the proud owner of two hundredths of a Bitcoin. I spent several days searching for a shopping website that we frequent that would accept Bitcoin as a form of payment. To no avail, I simply searched for somewhere online that I could spend my Bitcoin on a gift card to use elsewhere. I finally found a site called eGifter.com and a gift card that I would find useful. I was easily able to select the gift card and enter the $8.00 amount that I wanted to spend. Then, I was able to buy the card for myself or send it to a friend. I chose to send it to a friend so I could see what that process was like. I added my recipient's name, their email, a message, my email, and my name. In my online cart, I went to begin the checkout process and was prompted to create an account by giving my name, email address, and creating a password. Then, I was able to choose a payment method. I selected “Pay with Bitcoin” and a box popped up that allowed me to sign into my coinbase account. Since I signed into this account, I was sent a text message with another 7-digit code from coinbase that I had to give to ensure I was authorizing this transaction. Once that was verified, all that was left was to select “Pay - $8.00” and this part of the transaction was complete. I received an email receipt of the transaction and the person on the receiving end of the gift card purchase got the electronic gift card in their email almost immediately. The withdrawal from my Bitcoin account was there after a few short moments.