Bitcoin Digital Currency and the Blockchain Technology: More Than Flash in the Pan?

Elizabeth Trinh
Stanford University

Abstract
The term “Bitcoin” conjures up a variety of associations, such as gamers in dark basements, technology enthusiasts in the San Francisco Bay Area, and deceitful, yet highly persuasive “businessmen” involved in Ponzi schemes. Although there is a sense of skepticism surrounding this novel technology, Bitcoin has overcome many negative stereotypes to revolutionize the monetary system. Big names like the New York Stock Exchange and Goldman Sachs have recognized and praised the technology, and an increasing number of businesses like Tesla and Overstock.com are accepting bitcoin. Influential players internationally are endorsing Bitcoin, which validates the notion that Bitcoin—or at least the technology behind it—is not going away any time soon. Unlike the U.S. dollar and most other forms of legal tender, Bitcoin is a decentralized entity that removes the middleman from the equation. Instead of being a part of a system that is often tarnished by greed and human manipulation, Bitcoin is governed by mathematics and encryption processes. Admittedly, there are several issues with Bitcoin, such as its vulnerability to theft and fraud; however, there are many advantages to this currency. A more modern and possibly more economic alternative than the archaic Visa and MasterCard, which were founded in the 1950s and 1960s, respectively, and haven’t been updated since. While Bitcoin will not supplant the U.S. dollar due to an assortment of challenges, Bitcoin holds promise for the future of finance and consumerism. The Bitcoin technology of a block chain has already mobilized many financial institutions to embrace the emerging technology by piloting Bitcoin projects. It is not unrealistic to assume that there is a high potential for a system similar to Bitcoin to replace traditional fiat currency.
Introduction to Bitcoin
In the summer of 2011, a 25-year-old electrical engineer traveled from Connecticut to Southern California (Hill, 2013). His cross-country road trip would have been more conventional had he paid in U.S. dollars, but this young man chose to use only Bitcoin.* Since the release of Bitcoin in early January of 2009 (Davis, 2011), there have been numerous stories of people across the globe using Bitcoin as currency. Individuals of all demographics are using the virtual currency for everyday consumption, such as buying pizza, registering for a dating website, or shopping at a superstore. More notably in the political domain, the 2016 United States Presidential candidate Rand Paul accepted donations for his campaign in Bitcoin (Pagliery, 2015).

The term ‘Bitcoin’ can conjure up a variety of negative associations, ranging from gamers in dark basements and technology enthusiasts in the Silicon Valley to deceitful, yet highly persuasive ‘businessmen’ involved in Ponzi schemes (U.S. Securities and Exchange Commission, n.d.). Although there is a sense of skepticism surrounding this technology, Bitcoin has overcome many negative stereotypes to revolutionize the monetary system. Major institutions, such as the New York Stock Exchange and Goldman Sachs, have recognized and praised the technology (Popper, 2015), and an increasing number of businesses like Tesla and Overstock.com are accepting Bitcoin as payment (Goodman, 2014). Influential players internationally are endorsing Bitcoin, which validates the notion that Bitcoin—or at least the blockchain technology behind it—is not going away any time soon.

Unlike the U.S. dollar and most other forms of legal tender, which requires users to trust a central party such as a federal institution, Bitcoin is a decentralized entity that removes the middleman from the equation. Instead of being a part of a system that is often tarnished by greed and human manipulation, Bitcoin is governed by mathematics and encryption processes. Admittedly, there are several issues with Bitcoin; however, there are many advantages to this currency. A more modern and possibly more secure method of payment, Bitcoin is more economic and works faster than the archaic Visa and MasterCard, which were founded in the 1950s and 1960s, respectively, and have not been updated since.

Some sources such as Emin Gun Sirer, an Associate Professor at the Department of Computer Science at Cornell University, believe that Bitcoin will not supplant the U.S. dollar due to an assortment of challenges. Others, however, believe that Bitcoin holds promise for the future of finance and consumerism (Sirer, 2015). The Bitcoin technology of a blockchain has already mobilized many financial institutions to

* Bitcoin with a capital “B” is the name of the currency. It denotes the technology of the payment system and/or the open-source software, which means that its source code is made available for anyone to access. Bitcoin or bitcoins with a lowercase “b” refers to the unit of currency. Throughout this paper, I will employ this distinction.
embrace the emerging technology by numerous Bitcoin projects. It is possible to imagine the high potential for a system similar to Bitcoin to replace traditional fiat currency.

The Genesis of Bitcoin: Who is Satoshi Nakamoto?
On the night of Halloween in 2008, a computer programmer or a group of people by the pseudonym of Satoshi Nakamoto published a paper entitled “Bitcoin: A Peer-to-Peer Electronic Cash System” on the Internet (MIT License, 2015). Describing Bitcoin protocol and software in a mere nine pages, Nakamoto invented a peer-to-peer virtual currency that eliminated the need for a third-party intermediary. With the press of a button on the evening of January 3, 2009, Nakamoto launched the system, and the first bitcoins were created (Bitcoin History, n.d.).

Nakamoto continued to work on the Bitcoin software with other programmers and developers until mid-2010, when he transferred control of the source code to Gavin Andresen, the Chief Scientist of the Bitcoin Foundation, and other prominent members of the Bitcoin community. Gradually, Nakamoto reduced his involvement. With the final statement of “I’ve moved on to other things,” he vanished in April of 2011 (O’Leary, 2014). On the Bitcoin ledger that displays the record of all transactions, there are approximately one million bitcoins in Nakamoto’s public wallet. In early November of 2015, a single bitcoin was valued at $384 (Price, 2015), which means that Nakamoto held more than the equivalent of 350 million U.S. dollars in 2015. The value of one bitcoin is now about $8,500, and at the end of 2017, the price of one bitcoin reached an all-time high of almost $20,000 (Morris, 2017), making Nakamoto a multibillionaire. However, since his disappearance, not a single bitcoin has been touched.

Although systems such as Hashcash, B-money, and BitGold, emerged first, Bitcoin was regarded as the first cryptocurrency because it appealed to the sentiments of the right audience at the right time. Different from the U.S. dollar, which obliges its users to have faith in financial institutions and the government that backs the currency, Bitcoin removed the necessity of these intermediary parties. Born “just as the failures of the modern banking system became apparent—as well as widespread disappointment in the politicians who enabled them and the regulators who failed to catch them” (Pagliery, n.d.), Bitcoin gained many adherents because Nakamoto reached out to a libertarian and anti-authoritarian congregation that firmly latched onto the concept of a decentralized currency. According to Sirer, the initial adopters of Bitcoin first promoted the new currency in New Hampshire, where the libertarian movement was based. Although Bitcoin is not as decentralized as most ardent supports consider it to be, Joseph Bonneau, a postdoctoral researcher of the Applied Crypto Group at Stanford University, concurs that the political value that libertarians and anarchists assign to Bitcoin has proven to be successful in
marketing the currency (Bonneau, 2015). In recent years, the allure of Bitcoin has grown to encompass a wider audience, including everyday individuals, technologically savvy programmers, criminal masterminds, and even the finance industry.

Mehran Sahami, a Professor of Computer Science at Stanford University, equates Bitcoin to the “tulip craze” in the 1600s when tulips were priced at absurdly high costs before the market for the bulbs suddenly collapsed (Sahami, 2015), but Sirer extols Bitcoin as “best thing since sliced bread” (Sirer, 2015). Sirer attributes Bitcoin’s success partially to the creation myth behind the technology. Like the stories of the Chinese Cosmic Egg or the Norse frost giant Ymir, the tale behind Bitcoin’s origins is shrouded in mystery. As a result of this secrecy, the distinction between fact and fiction has become blurred. This enigma has proven to be valuable for social adoption, as the question of who Satoshi Nakamoto really is has drawn a large following and attracted media frenzy. In fact, Nakamoto was nominated for the 2016 Nobel Prize in Economics by Bhagwan Chowdhry, a Professor of Finance at UCLA Anderson School, because “[t]he invention of bitcoin—a digital currency—is nothing short of revolutionary. It offers many advantages over both physical and paper currencies” (Chowdhry, 2015). To this day, while there have been countless theories, the real identity of Satoshi Nakamoto remains unknown.

The Innovative Technology Behind Bitcoin
From cows and cowry shells to metal coins and banknotes, money has changed over the course of human history. With the widespread distribution and usage of personal computers and smartphones, the technological landscape has been rapidly evolving; however, the global monetary system has yet to catch up. Fiat money has been relatively static, and the arrangement of using paper money and credit cards is outdated. Bitcoin, unlike the U.S. dollar, Chinese yuan or the Indian rupee, is not an entity—all that exists are Bitcoin addresses.

The idea of virtual currency is not a novelty, but Bitcoin is different from past digital systems because it employs the novel development of the blockchain. The blockchain is a shared online ledger, or a collection of financial accounts, that presents all transactions in chronological order to all computers on the network without revealing personal information about the parties involved. When a transaction occurs, the buyer and the seller interact directly in a peer-to-peer manner, and their actions go on a publicly visible record. Once something is added onto the blockchain, it cannot be changed; there are no reverse transactions, and the Bitcoin protocol makes it practically impossible to double spend bitcoins. Bitcoin is pseudonymous, not anonymous, as each user and every bitcoin have special, encrypted addresses comprised of strings of characters. Bitcoins are kept in a digital wallet that is comparable to a bank account. While the
blockchain displays the public address, each individual has a private key unique to his or her wallet.

Bitcoin has no central monetary authority that controls the system. Instead, Bitcoin incorporates a consensus mechanism. Whereas in a centralized structure, there is a central authority that maintains and updates the system, Bitcoin is self-regulating. Hundreds of thousands of miners work to verify and authenticate activities on the blockchain. Bitcoin also has a set supply growth rate that is based on mathematical algorithms detailed by a publicly available computer program. Only 21 million bitcoins will be generated in total, and this number will be reached by 2140 (Hill, 2013). Every ten minutes, a computer program generates Bitcoin by solving increasingly complex mathematical problems in a process known as mining (Khan Academy, n.d.). When a program deciphers the problem, it creates a “block,” which is encrypted with hashed transaction values. Miners are users on the network who confirm the transactions before officially adding them to the blockchain. Mining is similar to a competitive lottery in that miners do not have control over which blocks of transactions are added or when they are added to the blockchain (Davis, 2011). For transactions to be authorized, they must abide by strict cryptographic rules that are enforced by the network. In addition, mining requires a lot of electricity to run the Bitcoin software, compelling some miners to purchase specialized machines with stronger computing power. Others have coordinated mining pools that harness the power of multiple computers to mine at the same time. In exchange for performing these tasks, miners are rewarded with additional bitcoins.

Although Bitcoin has reached an unprecedented level of security, the technology is at a cusp. This is not to say that the technology is underdeveloped, but rather there are several weaknesses that could potentially pose a threat to the system. While many of these issues were taken into consideration during the design of Bitcoin, research is still being conducted to solve inherent problems within the database.

Is Bitcoin an Accomplice to Crime?
As a result of the pseudonymous, incognito nature of Bitcoin, the virtual currency has been known to be used in money laundering, the purchase of contraband, the hiring of assassins, and other illicit items and services. The Silk Road, an infamous online marketplace that accepted only Bitcoin, was founded in February of 2011, and it was used to facilitate these unlawful operations (Yermack, 2014). Fostering criminal activity like the sale of illegal drugs, the Silk Road linked Bitcoin with lawlessness for a period of time. In October of 2013, Ross Ulbricht, the operator, was arrested, and the Silk Road was shut down, but the damage was done. For some time after the closing of Silk Road, people who intended to use Bitcoin for more legitimate purposes did not want to touch bitcoins that criminals had handled because they were tainted. Mark A. Lemley, a
Professor of Law at the Stanford Law School asserts “the existence of anonymous, untraceable currency facilitates unlawful transactions because it might make it easier for people to buy illegal stuff… [but this dilemma is not Bitcoin-specific because] the whole Internet has this problem” (Lemley, 2015).

The appeal of Bitcoin to hackers and perpetrators of fraud and theft further deterred people from using the virtual currency. In 2014, hackers allegedly targeted Mt. Gox, a Japanese-based online exchange that was the largest platform for global Bitcoin transactions (The Economist, 2014). Consequently, millions of dollars in Bitcoin vanished, and the U.S. Department of Homeland Security closed down the website shortly afterward. It is still unknown as to whether the disappearance of bitcoins from Mt. Gox was the result of security vulnerabilities or fraud. According to Mehran, highly publicized circumstances like what happened to the Silk Road and Mt. Gox created a sense of apprehension to using Bitcoin (Sahami, 2015).

Be that as it may, Sirer argues that “for every one bad person, [Bitcoin provides] a bunch of good uses” for more people who are benign (Sirer, 2015). Comparable to the beginning of the Internet, the negativity surrounding Bitcoin is driven by the lack of understanding of its potential. Bitcoin is no different from the U.S. dollar with respect to its usage in criminal activity. Arguably, the dollar is less traceable than Bitcoin. It is perhaps easier to audit where bitcoins have come from and where they are going because anyone can observe what occurs on the ledger, which makes tracking financial crime less difficult.

Regulating a Decentralized, Digital Currency
As it has gained traction and become more accepted, Bitcoin has attracted the attention of government officials all over the world. During Bitcoin’s early stages, many governments were rather slow to respond to Bitcoin. Today, the demand for Bitcoin, which is measured by the amount of daily transaction flow, is concentrated in China and the U.S (Yermack, 2014). The United States has enacted a virtual currency law, which authorizes the Commodity Futures Trading Commission to have some oversight over Bitcoin. Also, any trading with virtual currency must be registered with the Securities and Exchange Commission. It appears that the U.S. government is not trying to shut down Bitcoin, as the current federal legislation in place is in relative support of the cryptocurrency. Instead, the government is building upon previous legislation. For example, in 2013 the Financial Crimes Enforcement Network, an agency within the U.S. Treasury Department, published parameters in which “virtual currency users could be categorized as money services businesses” (CoinDesk, 2014). According to Sirer, “if the [U.S.] government was trying to kill Bitcoin, Bitcoin would be dead by now” (Sirer, 2015). Most agencies and institutions in the government, including the Department of Justice and the
Federal Reserve, have acknowledged the legitimate uses of virtual currencies. Further, former Federal Reserve Chairman Ben Bernanke wrote in a letter to the senators claiming that virtual currencies “may hold long-term promise, particularly if the innovations promote a faster, more secure, and more efficient payment system” (Tracy, 2013). However, the principal questions at hand should be to consider to what extent should the government regulate Bitcoin, and how should the government effectively apply legislation to a technology that is advancing at a speed faster than regulators are accustomed to acting.

Bonneau holds that there are three main camps in this dispute. A majority of users in the Bitcoin community do not want Bitcoin legislation to exist. They posit that the software itself is self-regulating through cryptography, and they consider government Bitcoin policies an undermining of the decentralization principles on which Bitcoin was created. On the other hand, there are businesses, on the other hand, that are more in favor of policies that make their industries seem more authentic, although not all businesses are supportive of this idea. Academics and researchers, the third and smallest faction, are less troubled by this prospect, as regulation does not necessarily affect their work (Bonneau, 2015). While over-regulation may pose a problem, under-regulation has proven to be as dangerous, which is illustrated by the situations regarding the Silk Road and Mt. Gox. Congress has the power “To coin Money, regulate the Value thereof, and of foreign Coin, and fix the Standard of Weights and Measures” (“The Constitution of the United States”, n.d.), and because digital currency lies in an unchartered domain, the regulations that the U.S. government imposes on Bitcoin will set precedent for future virtual currencies.

Recently, the U.S. government has been scrutinizing the virtual currency in an attempt to confront criminal activity linked to Bitcoin. In addition to policies issued by the federal government, several state authorities, including New York, California, and Connecticut, have implemented initiatives to safeguard businesses and consumers (Murphy, 2015). Of the three listed examples, New York state has established the most publicized framework. The New York legal regulation requires companies accepting bitcoins to be licensed and to keep a comprehensive record of their customers (Reader, 2015). This directive, however, discredits the assurance of privacy that Bitcoin promises. In addition, the application to obtain a New York “BitLicense” costs about thousands of dollars, and the paperwork is extensive and excessive even. Only a handful of BitLicenses have been awarded, and many applicants have been denied. Bitcoin businesses have criticized the New York Bitcoin legislation, as it has been difficult to fulfill. Various companies have either left the state or shut down. The establishments that have chosen to move to another state comprise mostly of start-ups including Bitfinex, Eobot, and Poloniex (Roberts, 2015).
While one of the roles of the U.S. government is to set rules for society, America’s founding fathers never envisioned the technology-driven world that we live in today. The actions that the government takes toward regulating Bitcoin, or any future digital currency for that matter, must be well-motivated as to not hinder the technological progress of the invention. David Mazieres, a Professor of Computer Science at Stanford University and the Chief Scientist of Stellar Development Foundation, compares Bitcoin regulation to a “wildcard” (Mazieres, 2015). Although policies may provide the Bitcoin community with some sense of security, the U.S. government is in a delicate quandary because excessive regulation could harm the future of virtual currencies. Still, in order to keep Bitcoin from continuing down the road that will make it an offshore industry or an exchange ruled by China, federal regulation is necessary and perhaps even inevitable.

Back to the Future
Although there is a multitude of advantages to Bitcoin, such as its cryptographic security, global accessibility, low operation expenses, and transparency, it does not come without limitations. In addition to the public’s general lack of understanding of the technology, the price of Bitcoin is volatile because the demand for bitcoins continues to change erratically and drastically. The price of Bitcoin has already skyrocketed since its creation, and with the fixed algorithms, there is no means to control the issuance of Bitcoin in the possibility of an economic downturn. With a limited amount of the currency in the system and an increasing number of users, Bitcoin has a deflationary nature. More Bitcoin users want to hold on to their bitcoins rather than to spend them. Moreover, Bitcoin needs to scale in order to accommodate a larger audience. Every ten minutes, a mathematical algorithm forges a block. The predicament is that the number of transactions is restricted by the size of the block divided by the time between blocks, which equals roughly three to seven transactions per second. Visa, on the other hand, is more equipped to handle a greater quantity of transactions. To put this in perspective, on a “boring day,” Visa manages about several thousand transactions per second (Sirer, 2015). The primary shortcoming to the universal acceptance of Bitcoin, however, is participation. There is a prevalent preconceived perception that because there is already a payment network in place to handle transactions, people do not need Bitcoin even though the foundations for the current system of Visa and MasterCard are primitive and outdated.

There needs to be a better electronic payment system, such as a virtual currency that will allow for the government to issue securities or financial instruments backed by a blockchain. The benefits of an eCommerce structure similar to that of Bitcoin are far-reaching. Relying on static banknotes and credit cards is problematic and even dangerous, and the
technology behind Bitcoin—not necessarily Bitcoin itself—may be the solution. Because Bitcoin is an experimental digital currency, its future is unpredictable, and it may not be around in the long-term. The innovative technology, conversely, has huge constructive potential. While Bitcoin may not be the money of the future, a forthcoming virtual currency that utilizes the blockchain technology by building on top of the foundation constructed by Bitcoin is a highly plausible notion. In fact, it would be even more advantageous for some system in the future to congregate the designs of both fiat money and digital currency into a better source.

Other Applications of the Blockchain

The Bitcoin public ledger is the first and most widely known application of the blockchain, which has developed significantly in recent times. Because the blockchain is a permanent record that documents events in sequential order while protecting identities, it is an innovation that has been adopted and embraced in a variety of other practices. For instance, this technology has been applied as a record-keeping system and a platform. One application of the blockchain that has been more explored is the concept of computable contracts, or “smart contracts,” that eliminate the need for a middleman, and thus, reduce human error (Vogl, 2015). Smart contracts enable computers to understand and execute some or all of the obligations in written agreements. Transacting on a decentralized network phases out escrow services and removes the requisite of trust. When parties are unfamiliar with each other, the blockchain provides a means for the different groups to enter a transaction with confidence because everything is certifiable by data. These great opportunities are in only the early stages of development, and even though the blockchain has already been used in various different fields and for many activities, this is just the beginning.

Conclusion

Money, which has always been connected to a centralized authority, is a complex subject matter. Throughout history, only governments have had the power to issue banknotes and coins, and banks and other government entities were the only resources that could facilitate transactions. While this model has been decently operational, the international monetary system in place is antiquated, and a money revolution is all but inevitable.

If one thinks of the Internet as a country, it makes sense to have a currency specific to the Internet. Although Bitcoin is not in a position to replace national currencies at the moment, the technology behind Bitcoin holds the key to the future of money. The hype surrounding Bitcoin, a formerly obscure virtual currency, has sensationalized headlines, but almost ten years after its release, this cryptocurrency is still developing. To modernize the monetary system on a global scale, Bitcoin depends on wide public acknowledgement and acceptance, which it has yet to receive.
In discussions concerning the future of Bitcoin, the positions range from critical and denouncing to positive and even exalting. While Mehran is "pretty cynical" of the existing value of Bitcoin (Sahami, 2015), Sirer considers the virtual currency an "amazing phenomenon" (Sirer, 2015), and Mazieres calls Bitcoin "a huge breakthrough" (Mazieres, 2015).

Satoshi Nakamoto’s invention has incontestably been “a disruptive influence in the twenty-first century” (Chowdhry, 2015). Against the odds, Nakamoto created currency out of lines of code that people all over the Earth value. The technology behind Bitcoin has proven to be a fundamentally new way of transacting and maintaining records online without having to rely on superfluous and costly intermediaries. Bitcoin has modernized an outmoded way of thinking, as the technology underlying Bitcoin can be used to change the world market.

References

Bonneau, Joseph. Personal interview. 18 November 2015.
Lemley, Mark A. Personal interview. 16 November 2015.
Mazieres, David. Telephone interview. 18 November 2015.


Sahami, Mehran. Personal interview. 11 November 2015.

Sirer, Emin Gun. Telephone interview. 17 November 2015.


Vogl, Roland. Personal interview. 17 November 2015.


