The Societal Impact of Blockchain

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia · Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Jared Tufts
Fall 2016, Spring 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: Jared Tufts Date 4/30/2020
Jared Tufts

Approved:_____ Date_____
Michael Gorman, Department of Engineering and Society

The Societal Impact of Blockchain

Response to Comments

The comments provided by Professor Gorman were incredibly helpful in evaluating my thesis. Due to his suggestions, I drastically expanded upon my reasoning for using Actor Network Theory as an STS framework, including the actors and what effects they could have on each other through the network. I also added a figure that shows the Actor-Network diagram for blockchain technology at the suggestion of Professor Gorman, since I agreed that it would make the description of the network clearer. I also went more in depth with my description of Anticipatory Governance as an STS framework that can be used for blockchain. I explained what role the government can play, and what goal it should have in terms of guiding blockchain technology to particular use cases.

I added some of the changes from the comments from my presentation into the thesis. These mostly include more in-depth explanations of Actor Network Theory and Anticipatory Governance. I decided, however, to not to discuss too much of where the government should go in terms of anticipatory governance, but to leave it open ended and simply evaluate multiple possibilities or benefits of small or big regulation.

Introduction

In December of 2017, the price of Bitcoin skyrocketed up to an all-time high of $19,783. It had started the year around $1,000. [1] This pushed Bitcoin into the forefront of society, and people who had never had any reason to get involved with this new technology had suddenly heard about it, and often started investing in it. For the weeks prior to this December 17 peak, cryptocurrencies were all over the news, and it seemed like the only place their value could go

[1] Avi Salzman (2019), *Bitcoin Peaked 2 Years Ago. New Competition Is on the Way.*

was up. Then the price of Bitcoin fell 73% in 2018, and the rest of the crypto market fell with it. People lost a ton of money when this bubble burst, but Bitcoin had managed to cement itself across the world as something to watch out for. Where will this technology go next? Most people associate blockchain with Bitcoin, but blockchain has a wide range of uses, despite cryptocurrency being the most popular use currently. In order to examine where blockchain and cryptocurrencies can go in the future, it is important to examine the history of this technology. How have governments and corporations reacted to the introduction of this technology, and what steps could they take in the future? To examine the effect blockchain could have on society, I will use the STS frameworks Actor-Network theory and Anticipatory Governance to determine what the future could look like as this technology gets adopted more and more.

Bitcoin

The focus of blockchain as of right now is mostly around cryptocurrency, specifically Bitcoin. This has been, so far, the most widely used and most well-known application of blockchain. Therefore, the exploration of how blockchain has grown and changed in the past will focus around Bitcoin and cryptocurrency. Comparisons can later be drawn, however, to the impact that blockchain technology could have in the future.

The first known reference to a blockchain-like system was in 1991 in a collection of papers written by Haber and Stornetta.[2] They came up with the blockchain idea as a method for timestamping digital documents in a secure, immutable way. Blockchain technology is a data management technology to make data be incorruptible and unchangeable. In 2008, a group of people or an individual going by the name Satoshi Nakamoto (whose identity is currently

[2] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, & Steven Goldfeder (2016), *Bitcoin and cryptocurrency technologies: a comprehensive introduction*

unknown) wrote a paper detailing how a secure payment system could be created using blockchain and a peer-to-peer network.[3] A peer-to-peer network in this context means that every computer in the network contains a copy of the blockchain; therefore, the majority of computers must agree on any changes made to the blockchain. This means that no one person or entity has control over this network. Using a peer-to-peer network was the final piece to the puzzle for effective electronic currencies, since you don't need a central control point. This paper resulted in the creation of Bitcoin as we know it about a year later.

The Silk Road

Bitcoin started to make a name for itself in 2011 as a tool used by criminals to make illegal purchases. The most famous instance of this is the Silk Road. The Silk Road was a website on the internet that was a complete free market, allowing people to sell and buy drugs, weapons, fake ids, and more.[4] The Silk Road was started by Ross Ulbricht, with a pseudonym of 'Dread Pirate Roberts' (DPR), in February 2011.[5] All communication on the site used PGP encryption, and it was only accessible using the Tor browser, which allows users to surf the internet anonymously.[6] The key to making this internet market function so efficiently, however, was that all payments were done using Bitcoin, since it was easy, fast, and most importantly, anonymous. This marketplace was worrisome to many governments around the world, and a big reason for that was that it worked. One would think that an online, illegal marketplace would be full of scams, bad products, and unreliable buyers and sellers. However, due the site's ease of use and the ability for buyers and sellers to gain a reputation based on reviews, it functioned

[3] Satoshi Nakamoto (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*
[4] Michael Castelluccio (2017), *THE SILK ROAD ON THE DARK WEB*
[5] Michael Castelluccio (2017), *THE SILK ROAD ON THE DARK WEB*
[6] Jamie Bartlett (2014), *The Dark Net*

extremely well. This did start to put a stain on Bitcoin's name, however, as shown by Senators Chuck Schumer and Joe Manchin, who asked the Attorney General and the DEA to shut down the Silk Road stating, "The only method of payment for these illegal purchases is an untraceable peer-to-peer currency known as bitcoins."[7] Bitcoin allows sites like this to exist, which can make the general public hesitant to trust it.

The Silk Road's existence already starts to show a disconnect in what many people want from the technology and what the government wants. There have always been people who want to be completely free of the government, but now due to emerging technologies such as blockchain and cryptocurrency, they are able to. The Silk Road was never just about the ability to buy and trade illegal goods and services; it was the freedom. In April 2012, DPR wrote "Silk Road is about something much bigger than thumbing your nose at the man and getting your drugs anyway. It's about taking back our liberty and our dignity and demanding justice."[8] In the same post, he also wrote, "I won't rest until children are born into a world where oppression, institutional violence and control, world war, and all the other hallmarks of the state are as ancient history as pharaohs commanding armies of slaves." [9] There are a plethora of other posts that don't show somebody who just wants easier access to drugs; but as a radical libertarian who wants freedom from all government control. Many Silk Road users supported him in this goal. When the Silk Road was taken down by the FBI in October 2013, other markets popped up to fill the void.[10] There is a growing community of people who want to be free of government control, and are eager to use technology such as cryptocurrencies to do it. The government, however,

---

[7] David Kushner (2015), *The Rise & Fall of a Bitcoin Kingpin*

[8] Andy Greenberg (2013), *Collected Quotations Of The Dread Pirate Roberts, Founder Of Underground Drug Site Silk Road And Radical Libertarian*

[9] Andy Greenberg (2013), *Collected Quotations Of The Dread Pirate Roberts, Founder Of Underground Drug Site Silk Road And Radical Libertarian*

[10] Jamie Bartlett (2014), *The Dark Net*

wants to prevent any illegal activity from occurring and maintain regulation over the monetary system. The government has historically come out ahead of such disagreements over societal direction, but with cryptocurrency and blockchain providing one of the final pieces for a free marketplace, this could change.

The Collapse of Mt. Gox

Cryptocurrency has the potential to drastically change society, but will the general public ever accept something that is not controlled by a single entity? Most monetary systems in the world are controlled by their respective governments, and it is part of the reason why people feel safe using the currency. They know that the money is backed up by the federal government. With cryptocurrencies, however, the only reason it has value is because other people also agree it has value. This makes Bitcoin feel very risky to average people when exploring what to do with their money. While there is a big community of people who are pushing Bitcoin and other cryptocurrencies in order to be free from government control, that same government control over the money supply makes many people feel safe. The failure of Mt. Gox, a Bitcoin exchange, was a big event that had a negative impact on the viability of Bitcoin.

Mt. Gox was built by Jed Mc-Caleb, and was originally a site to exchange Magic: The Gathering cards. In mid-2010 Mt. Gox transitioned into being a Bitcoin exchange, and Mark Karpeles took over the exchange in early 2011. At this point, the Silk Road was gaining popularity, and in order to maintain legitimacy he offered to assist with any investigation, stating "Ultimately, we are pursuing a goal of accepted legitimacy, both for bitcoin and our exchange." [11] Despite, or possibly because of, the rise of the Silk Road, Mt. Gox gained rapid popularity and

[11] David Kushner (2015), *The Rise & Fall of a Bitcoin Kingpin*

grew to the point of processing around 80% of all Bitcoin transactions and moved about 4 million dollars a month at its peak. [12] The problem with Mt. Gox though was that it was one of the only exchanges, but was very poorly run. Late in February 2014, Mt. Gox released that they were hacked, and 750,000 Bitcoins were stolen. These bitcoins were valued at around $473 million. Mt. Gox later declared bankruptcy, and many customers lost their money. [13]

The collapse of Mt. Gox hurt the value of Bitcoin, and hurt many people's confidence in the system. When you don't have government support of a financial system, it is much harder for people to get their money back, making things like this able to happen much easier. Bitcoin transactions are not reversible, due to the underlying blockchain technology, so you cannot get your money back if it is stolen without the assistance of the thief. As cryptocurrency grows, people are going to have to weigh the risks and educate themselves on where is the safest place to keep their cryptocurrency. This goes beyond cryptocurrency, however. In our current centralized world, if a hack happens, people know who to blame and can point the finger at that company. In a decentralized world, if something goes wrong it becomes more difficult to determine whose fault it was and to correct whatever it is that went wrong.

Government Regulation

How has the United States government responded to the rise of Bitcoin? The government has the ability to make a huge impact in encouraging or discouraging the use of any cryptocurrency as actual currency. As Bitcoin gained popularity, due to its use in criminal activity and general use, the government started to pay attention.

[12] David Kushner (2015), *The Rise & Fall of a Bitcoin Kingpin*
[13] Sean Michael Kerner (2014), *Despite a Tumultuous 2014, Bitcoin Still Has Value.*

The IRS first issued guidance on cryptocurrency in 2014 by classifying it as property for tax purposes.[14] In 2019, the IRS expanded this guidance to be more specific, including information about hard forks. A hard fork is when a cryptocurrency splits into the old blockchain and a new blockchain. This creates a new cryptocurrency that exists alongside the old one. The IRS stated that if you receive cryptocurrency as a result of a hard fork, you must include the fair market value of the cryptocurrency in your gross income.[15] In summary, cryptocurrency is recognized as property under the IRS.

In 2013, the Financial Crimes Enforcement Network (FinCEN), which is part of the Department of the Treasury, determined that money transmitter laws and the Bank Secrecy Act (BSA) apply to cryptocurrency exchanges. The goal of the BSA is the prevention of money laundering and similar illegal activity by "imposing a comprehensive reporting and recordkeeping regime designed to assist with law enforcement efforts to identify and investigate suspicious transactions."[16] Due to the application of these laws, cryptocurrency appears to be recognized as money under the Department of Justice.[17]

The Securities and Exchange Commission (SEC) has also begun dealing with cryptocurrencies. In the case SEC v. Shavers, cryptocurrency was determined to be currency and that investments in cryptocurrency "is subject to regulation under federal securities law." [18] Due to this ruling, securities regulations apply to cryptocurrencies. While the SEC also recognizes cryptocurrencies as money, they say that they can be considered securities as well.

---

[14] Internal Revenue Service (2014), *Notice 2014-21*
[15] Internal Revenue Service (2019), *Revenue Ruling 2019-24*
[16] Kevin V. Tu (2018), *Perfecting Bitcoin*
[17] Joseph Evans et al. (2018), *New York Department of Financial Services Guidance Complicates a Crowded Virtual Currency Regulatory Landscape*
[18] Kevin V. Tu (2018), *Perfecting Bitcoin*

There has not been much new regulation that is specific to cryptocurrency. The biggest piece of regulation that falls under this category is New York's BitLicense, which simply places regulations on this business to make cryptocurrencies generally safer. [19] It is fairly obvious that there is some inconsistency in how cryptocurrencies are classified and treated across the government. The government's main goals have been to stop illegal activity and to protect consumers, and the regulations they have enacted show that. The inconsistencies in the regulation and how cryptocurrencies are classified, however, show a government that does not know what to make of cryptocurrency yet. This is important, because while the government is attempting to control cryptocurrency to make it safer for users and investors, they also seem to be letting the technology grow and are waiting to see what direction it takes. A cryptocurrency like Bitcoin becoming accepted as payment across the country will most likely lead to different laws and regulations than a different cryptocurrency becoming widely used such as Ethereum, which focuses on harnessing the blockchain technology to build applications rather than as a payment method.

The Ethereum Blockchain

It is difficult to discuss possible future applications of blockchain without discussing Ethereum. The Ethereum blockchain is different from the blockchain of a cryptocurrency like Bitcoin. Ethereum does have a currency, called Ether, but the main focus of Ethereum is its programmability. This means that people can create applications that are on the Ethereum blockchain. These applications, since they are on a blockchain, are decentralized so no one entity

[19] Kevin V. Tu (2018), *Perfecting Bitcoin*

controls them. Applications are built in specific programming languages that utilize smart contracts.[20]

Cryptocurrency has been blockchains biggest application so far, however there are a plethora of others that have the capability to drastically alter society. Smart contracts are one of these applications with massive potential. Smart contracts are contracts that are created and executed online automatically. They are simply pieces of code that execute when the specified conditions are met. This can range from transferring money after something is done to locking an apartment door if a tenant does not pay rent by a certain date.[21] This means that contracts are created, agreed to, and enforced all on a blockchain, making it impossible to break the contract. This can lead to some issues, however. The biggest one is what if there is a flaw in the code? Smart contracts are just pieces of code on the blockchain, so what if there is a bug that somebody can exploit? This is exactly what happened in something called the DAO-hack.

The DAO, or Decentralized Autonomous Organization, was built on the Ethereum blockchain and was basically a "decentralized investment fund." You could put money in and have a vote in where the money gets invested.[22] The DAO, since decentralized applications are built using smart contracts, executed automatically. This caused a problem when somebody was able to find a bug in the code of the smart contract. Using this bug, the hacker was able to steal $50 million. What makes this interesting, however, is that this was technically allowed in the smart contract. Smart contracts that are built with bugs will be able to be exploited, and since a blockchain is immutable, there is no easy way return the stolen Ether without cooperation from the thief. In this particular case, Ethereum made a choice to do a hard fork, splitting into

[20] Ethereum Documentation, *What is Ethereum?*
[21] Eliza Mik (2017), *Smart contracts: terminology, technical limitations and real world complexity*
[22] Klint Finley (2016), *A $50 Million Hack Just Showed That the DAO Was All Too Human*

Ethereum and Ethereum Classic. Ethereum Classic is the original blockchain where the hacker still has the stolen Ether, while Ethereum edited the blockchain by deleting the transaction, returning all the Ether to the rightful owners. This edit was possible since the majority of the Ethereum nodes downloaded the new blockchain, essentially switching the blockchain that Ethereum adds to.[23]

Smart contracts and decentralized applications obviously have a massive amount of potential to change modern society. Decentralized applications are already being used in a variety of ways, from creating a shared decentralized supercomputer to creating a decentralized version of YouTube. The DAO-hack puts this in perspective, however, and shows possible flaws with an internet of smart contracts. Small bugs in these contracts can have massive impacts on users, and these impacts might not be reversible. As decentralized applications grow, the government is going to need to find a way to guide their development, recognizing their potential to harm users. Anticipatory governance could be very useful here, finding a way to encourage the development of these technologies while also searching for ways to limit the risks.

Future Applications of Blockchain

Since the invention of blockchain most of the history and developments have been focused around cryptocurrency, but there are many other potential applications for this technology. One big industry it has the potential to impact is the shipping industry. The shipping industry has major issues with communication due to a lack of a central communication platform, and tracking systems are extremely outdated. However, implementing blockchain will simplify all of these processes. It can provide a system that is updated in real time and

[23] Matthew Leising (2017), *The Ether Thief*

significantly reduce administrative procedures. The security of blockchain can also prevent lost shipments. If all the information is contained in the blockchain, it allows for everybody to be on the same page and reduce a lot of the costs involved with shipping. Smart contracts can also have an impact by reducing the number of intermediaries needed since the contracts will automatically execute once the conditions are met. A major asset will also be the fact that all transactions and data will be stored in the blockchain and immutable, so you will always have a full history and schedule to look back at. This avoids paper documents or even having to organize emails or online documents.[24]

Blockchain could also be a key factor in helping countries pull themselves out of poverty. Many poor countries tend to "lack good institutions that ensure strict enforcement of property rights, have the ability to deal with corrupt practices effectively, and provide equal opportunity to all members of society."[25] Blockchain can have a very positive effect on lots of these problems. Blockchain is an immutable database, so if land ownership were to be transferred to a blockchain system, it would allow people to prove that they owned specific pieces of land and nobody could alter it without the owner's consent. There are already systems in place in Ghana and Honduras attempting to do this. Blockchain also gets rid of lots of the inefficiencies in global trade. Money can be sent globally for much cheaper, and businesses will no longer have to deal with so many intermediaries.[26]

Conclusion

[24] Alen Jugović et al. (2019), *The Possibilities of Applying Blockchain Technology in Shipping*
[25] Nir Kshetri (2017), *Will blockchain emerge as a tool to break the poverty chain in the Global South?*
[26] Nir Kshetri (2017), *Will blockchain emerge as a tool to break the poverty chain in the Global South?*

Blockchain technology has a massive amount of potential to alter modern society. Cryptocurrency was the beginning, but it does not end there. Smart contracts, decentralized applications, and data storage are all possible use cases of blockchain, and the amount of security it provides to prevent data from being altered is incredible. It is clear to see how the different actors in this network are pulling this technology in various directions. Most people want to be able to purchase cheap goods and services while using an easy to use online platform, the government wants to make sure this push towards decentralization does not cause an increase in crime and people remain safe, while corporations are trying to use blockchain to streamline their production processes and get more accurate data on ordered parts. Figure 1 shows a diagram of this network:

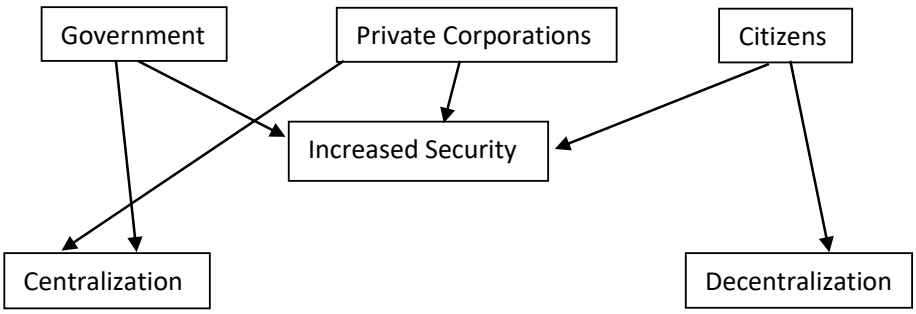

Figure 1: Blockchain Actor-Network

Currently, blockchain technology is in the very early stages of development. The upgraded security it provides and the amount of people and communities it can help is astonishing, and all the actors in the network want more security. However, as blockchain technology matures, it is going to be interesting to see how big tech companies maintain their relevance, and what role the government plays in this. Normal citizens and technology companies like Amazon or Netflix will most likely be attempting to use this technology in drastically different ways, and it'll be interesting to see how that resolves itself.

The government will serve a crucial role through anticipatory governance in making sure that blockchain technology changes our society in positive ways. Anticipatory governance is an extremely helpful tool to analyze blockchain, since it is still in the early stages of adoption and it can be used in many positive and negative ways. It will take years to adopt blockchain into our society and it has the potential to help people around the world and make economies significantly more efficient, however it can also be used for crime. An interesting factor, however, are the libertarians who want to use blockchain to free people from government. Ostensibly, it does not appear as if that would ever be possible, but blockchain is arguably one of the last pieces needed to ensure completely trustless, yet effective, markets and communication. The governments have to balance their goal of keeping people safe with making sure blockchains do not become a hub for criminal activity. As this technology develops, the government will find it much harder to regulate, tech companies will have to drastically change their profit models, and people will, at least initially, have to deal with a more complicated process for viewing content. Because blockchain has such high potential to disrupt society, the government has the duty to monitor its development. It can be used in many positive ways, especially in struggling communities around the world, but there will be challenges that are associated with that. The government might deem it necessary to control or ban the use of cryptocurrency as a payment system, in order to prevent illegal activity and emphasize blockchain as strictly a decentralized database. Whatever the government decides to do, only time will tell what the future will look like as our world inevitably grows more and more decentralized due to this powerful technology.

References

1. Avi Salzman (2019). Bitcoin Peaked 2 Years Ago. New Competition Is on the Way. *Barron's.* Retrieved from https://www.barrons.com/articles/bitcoin-new-competition-is-on-the-way-51576621343
2. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, & Steven Goldfeder (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction.* Princeton, NJ: Princeton University Press.
3. Satoshi Nakamoto (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf
4. Michael Castelluccio (2017, July). The Silk Road On The Dark Web. *Technology Workbook*, 55-56.
5. Jamie Bartlett (2014). *The Dark Net: Inside the Digital Underworld*. Melville House.
6. David Kushner (2015). The Rise & Fall of a Bitcoin Kingpin. *Rolling Stone*, (1243), 34-37.
7. Andy Greenberg (2013). Collected Quotations Of The Dread Pirate Roberts, Founder Of Underground Drug Site Silk Road And Radical Libertarian. *Forbes.* Retrieved from https://www.forbes.com/sites/andygreenberg/2013/04/29/collected-quotations-of-the-dread-pirate-roberts-founder-of-the-drug-site-silk-road-and-radical-libertarian/
8. Sean Michael Kerner (2014). Despite a Tumultuous 2014, Bitcoin Still Has Value. *eWeek*, 1-1.
9. Internal Revenue Service (2014). *Notice 2014-21*. Retrieved from https://www.irs.gov/pub/irs-drop/n-14-21.pdf

10. Internal Revenue Service (2019). *Revenue Ruling 2019-24.* Retrieved from https://www.irs.gov/pub/irs-drop/rr-19-24.pdf
11. Kevin V. Tu (2018), Perfecting Bitcoin. *Georgia Law Review, 52*(505), 518-536.
12. Joseph Evans, Lee Schneider, Andrew Kim, Lilya Tessler, David Taub, Alexandra Scheibe McDermott Will, & Emery (2018). New York Department of Financial Services Guidance Complicates a Crowded Virtual Currency Regulatory Landscape. Retrieved from https://casetext.com/analysis/new-york-department-of-financial-services-guidance-complicates-a-crowded-virtual-currency-regulatory-landscape?PHONE_NUMBER_GROUP=P&sort=relevance&resultsNav=false&q=
13. Ethereum Documentation, What is Ethereum?. Retrieved from https://docs.ethhub.io/ethereum-basics/what-is-ethereum/
14. Eliza Mik (2017). Smart contracts: terminology, technical limitations and real world complexity. *Routledge Taylor & Francis Group, 9*(2), 269-300. https://doi.org/10.1080/17579961.2017.1378468
15. Klint Finley (2016). A $50 Million Hack Just Showed That the DAO Was All Too Human. *Wired*. Retrieved from https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/
16. Matthew Leising (2017). The Ether Thief. *Bloomberg*. Retrieved from https://www.bloomberg.com/features/2017-the-ether-thief/
17. Alen Jugović, Juraj Buksa, Alex Dragoslavic, David Sopta (2019). The Possibilities of Applying Blockchain Technology in Shipping. *Scientific Journal of Maritime Research,* 274-279. https://doi.org/10.31217/p.33.2.19

18. Nir Kshetri (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South. *Third World Quarterly*, *38*(8), 1710-1732. https://doi.org/10.1080/01436597.2017.1298438