Smart Charlottesville: Designing the Future
(Technical Topic)

The Societal Impact of Blockchain
(STS Topic)

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Jared Tufts

November 24, 2019

Technical Project Team Members:

Sanjana Hajela, Kajal Sheth, Conner Hutson, Cory Ayers, Luke Deni, & Anthony Lancaster

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

Approved: Ahmed Ibrahim Date 4/30/2020
Ahmed Ibrahim, Department of Computer Science

SMART CHARLOTTESVILLE: DESIGNING THE FUTURE

The implementation of technical online platforms has become an increasingly popular idea to engage residents of a city with local government, and the University of Virginia plays a vital role in this due to its technical expertise. Professor Ferguson and Professor Ku are part of the STS department at the University of Virginia, and they are conducting research with their STS 4500 students to develop research ideas for transforming Charlottesville into a smart city. These ideas, however, need a platform that can be viewed and contributed to by both residents and the local government. The research problem to be solved is how to efficiently communicate these ideas, and others, to the Charlottesville community to improve the city for the future.

Currently, there is no viable platform that solves this problem of lacking communication in Charlottesville, since the research problem demands different user types and custom databases that are unavailable with platforms such as WordPress. The work done by the current capstone group of this academic year will provide the first iteration of a solution to bridge the gap for collaboration between the university and Charlottesville. The capstone project will last the entire academic year of 2019-2020.

Creating a web application public to all users will address the problem in a positive way, by working to provide a safe, non-anonymous site for community members to share ideas of changes they want in the community through engaging discussions. The website will have a feature for users to submit blueprints for proposed projects where they can also add file attachments such as pictures. The platform will require users to register and login to submit posts and interact with other users. The users will be able to look at the projects and comment on them, mark projects as “favorites” for easy access later, and connect with the authors of the blueprints

via email. Community members can also submit smaller problems around the city to gain attention from other members so they can be fixed. There will be an "about us" tab where interested visitors can get in contact with the creators of the site and learn more about this initiative. The landing page will have a map that shows the Charlottesville area with ongoing projects pinned so users can explore projects in different areas by clicking specific pins on the map. Finally, there will be a resources tab describing places users can go to learn more about projects and current city work in general.

To build this website a strict set of requirements will be collected from Professor Ferguson and Professor Ku. Requirements contain the attributes and properties of features of a system that the user wants to help solve their problems. It is important to gather system requirements to correctly understand the goals of the client and to facilitate the work of the developers to best cater towards the stakeholder's needs. Listed below are the capstone group's minimum, desired, and optional requirements:

Minimum Requirements:

1. As a user, I want to be able to comment on a blueprint to give my support or feedback.
2. As a user, I want to be able to filter through blueprints based on what category they fall under.
3. As an administrator, I should be able to manage blueprint content by hiding or removing it.
4. As an administrator, I should be able to manage the privileges of other users (students, community partners, and community members).
5. As a student, I should be able to create my own blueprint space so that others may view it.
6. As a student, I should be able to view other students' blueprints.
7. As a community member, I should be able to leave comments on a student's blueprint.

8. As a community member, I need to be able to post blueprints.
9. As a community member, I need to be able to like specific comments or blueprints.

Desired Requirements:

1. As a user, I should be able to search for keywords that define the type of blueprints posting I want to look at.
2. As a user, I should be able to view blueprints based on specific location

Optional Requirements:

1. As a user, I should be able to comment on other comments.
2. As a student, I should be able to tag my post with specific categories.

At the end of the project, we will have a collaborative, online workspace reachable by both the Charlottesville community and academics at the university. Users will be able to post ideas, gather feedback, collaborate, and connect with university resources; the university can do the same, as well as be able to identify problems in the community that may have otherwise remained hidden.

THE SOCIETAL IMPACT OF BLOCKCHAIN

Response to Comments

The comments provided by professor Gorman were incredibly helpful in evaluating my prospectus. When describing the blockchain technology, I am more descriptive than I was previously. I skimmed over some important features and pieces of information that will help the reader understand how blockchain works on a basic level. I also made it a little clearer why a consensus algorithm has that name. After much consideration, I decided to eliminate the sections on Ethereum and smart contracts to shorten the scope of the prospectus. I want to explore what impact blockchain will have on society, and both smart contracts and Ethereum are a part of this impact, but not the reasons for it. Professor Gorman also recommended I consider using a diagram, however due to the elimination of the section on Ethereum (which is where the diagram was desired), I decided that the diagram wasn't needed. I did decide to use a diagram for the blockchain however, since it will aid in my description. I would like to gather more feedback to see if maybe a diagram is useful after all. Due to suggestions, I also 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 of the blockchain technology at the suggestion of Professor Gorman, since I agreed that it would the description of the network clearer.

I met with Professor Gorman again and we discussed the possibility of using a trading zone framework. I decided that is was not the correct framework, since all the actors here do not communicate in any way. They are not coming together and sharing knowledge, as most of their goals are completely contradictory to each other and they are each pulling the blockchain

technology in their own direction. I included a description of why a trading zone would not work. I also included an exploration of the government's role in blockchain and possible routes for future research after a recommendation from Professor Gorman.

History of Blockchain

The first known reference to a blockchain-like system was in 1991 in a collection of papers written by Haber and Stornetta.[1] They came up with the blockchain idea as a method for timestamping digital documents in a secure, immutable way. In their model, each document is sent to a server, which adds it to the end of the list and gives it a pointer (a link) to the previous document. If the data in a document changes, then the pointer becomes invalid. This allows the order of the documents to become practically immutable. Cryptocurrencies expand upon this initial idea by making the blockchain decentralized, rather than through a centralized server.

In 2008, a group of people or an individual going by the name Satoshi Nakamoto (whose identity is currently unknown) wrote a paper detailing how a secure payment system could be created using blockchain and a peer-to-peer network.[2] 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 peer-to-peer network solution was the final piece to the puzzle for effective electronic currencies. This (along with proof-of-work) allows for complete trust across the network, since no centralized entity controls the blockchain. This paper resulted in the creation of Bitcoin as we know it about a year later.

[1] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, & Steven Goldfeder (2016), *Bitcoin and cryptocurrency technologies: a comprehensive introduction*
[2] Satoshi Nakamoto (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*

While Bitcoin was a very important step forward in terms of decentralized currency, people took more notice of the underlying technology – blockchain. This was the first example of it being used successfully in practice, and people became excited to see the plethora of other opportunities it could be used for to decentralize the world around us.

Description of Blockchain Technology

A blockchain is basically a decentralized database containing a growing list of records, whether that be of ownership or of something else, that everybody has access to. Every node (computer in the network) has a copy of the blockchain, and each data record contained within the blockchain is "irreversible, verifiable, and traceable".[3] A blockchain is made up of "blocks" that connect to one another, creating a "chain", shown in Figure 1. Blocks are added to the blockchain through a process called mining. Mining entails solving a very complex puzzle to create a hash to represent a block – this hash is mathematically difficult to create but easy to verify, since it just has to satisfy a predetermined inequality. Each hash is made up of the data in the block that is being created and the hash of the previous block. Each hash also has a "nonce", which is the value that is changed so that a new hash can be found to satisfy this inequality. A nonce is needed since the data in this block and the hash of the previous block are both constant values, so a value is needed that can be changed allowing different hashes to be created until one satisfies this inequality and a new block can be created. Example hashes are shown in Figure 1. Each transaction is verified by the nodes in the blockchain network and then sent to a mining

[3] Mark Van Rijmenam & Philippa Ryan (2019), *Blockchain: Transforming Your Business and Our World*

node. This node adds the transaction to the block it is attempting to create. Once the block is successfully created, it is added to the blockchain as shown in Figure 1.[4]

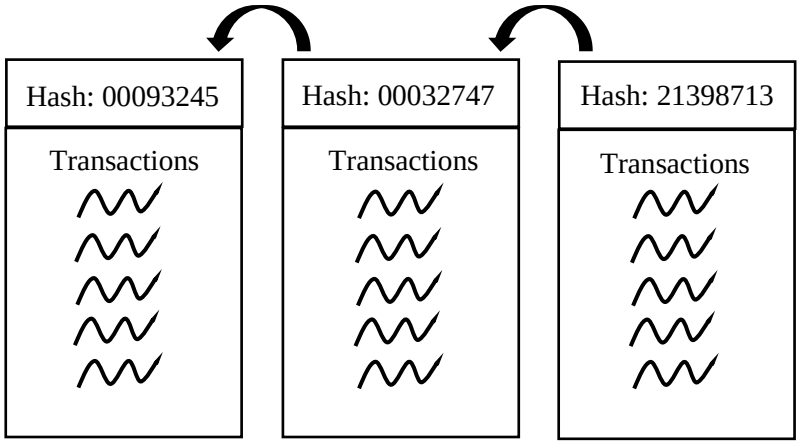

Figure 1: Blockchain

Each block header contains a consensus algorithm and a pointer to the previous block in the chain. The arrows in Figure 1 between the blocks represent the pointers described here. A consensus algorithm allows nodes in the blockchain to agree to a change without having to trust any other node in the network, which is what allows for decentralization.[5] A consensus algorithm is what is run to signal to other nodes that the block that was created is correct and can be added to the blockchain. The consensus algorithm used by Bitcoin and other leading cryptocurrencies, such as Litecoin, is called Proof of Work (PoW). This algorithm entails all mining nodes on the network racing to find a hash (that represents a specific block) which satisfies a given inequality. As soon as one does, the amount of work done is recorded in the block, which is then added to the blockchain.[6] Since each block is built upon the previous, the more blocks in the blockchain the more computational work that has been done to it. To find this hash, there is no mathematically faster way that we currently know of than pure luck. The more computing power

[4] Matthew Beedham (2019), *All you need to know about Bitcoin network nodes*
[5] Mark Van Rijmenam & Philippa Ryan (2019)
[6] Jake Frankenfield (2019), *Consensus Mechanism (Cryptocurrency)*

you have, the more possible hashes you can work through in the same amount of time. The hash of each block is built from its data, a nonce, and the hash of the previous block, which is what makes a blockchain immutable. If data is changed in one block, its hash will change. This in turn changes the hash of the block after it, causing these blocks to no longer be connected. The disconnection signals to the rest of the blockchain that a block was changed, and every node in the blockchain rejects this change.

A malicious node could also attempt to trick the network by adding a fake transaction stating they did not spend Bitcoins when they did. The malicious node would not broadcast this block as it would be rejected, since the incorrect transaction was not verified by the network. Instead, they would add it to a local blockchain and continue adding blocks to this chain. To do this, they would have to create blocks faster than every other node in the network to catch up to the official blockchain by having more work done.[7] Since nodes will treat the longest blockchain (the blockchain with the most work done to it) as the official blockchain, if the malicious node can eventually have more work done to it, it can broadcast this blockchain and it will be accepted by the network. This means that this one node would have to have more computing power than the majority of the network, which is virtually impossible.[8]

Each block's body contains the data, which can be any data that you could store in a database; however, in the case of cryptocurrency, it is a list of transactions. Each transaction has an amount the transaction is for and a digital signature, which is used by other nodes to verify the transaction.[9] A digital signature uses public key cryptography, ensuring that the data has not been changed and that the data was actually sent by the user who was supposed to have sent it.[10]

[7] Jimi S. (2018)
[8] Mark Van Rijmenam & Philippa Ryan (2019)
[9] Matthew Beedham (2019)
[10] Ravikant Agrawal (2018), *Digital Signature from Blockchain context*

Conclusion

Blockchain technology has a ton of potential. The more obvious benefits are increased security, since blockchain is decentralized, and removing intermediaries from transactions.[11] However, blockchain can go much further than this. Entire applications can be built using the blockchain technology in which code is stored in blocks instead of transactions. It can eventually make the entire internet decentralized, while right now it is in the hands of a few big tech companies. Massive companies like Dropbox or Netflix could become obsolete as blockchains become popular, since the intermediary is no longer needed – thousands of computers could be streaming videos, instead of a centralized server. There are some problems that exist right now with blockchain technology, however. One big issue is scaling – as a blockchain becomes bigger and bigger it becomes infeasible that every node in the chain will have the entire blockchain downloaded, leading to these scaling issues.[12] This is also a problem for the government, since there is no way for them to regulate this technology or what goes on while people use it. It is a public ledger that they can view just like everybody else across the world, but since no one person or group has control they cannot regulate it. Therefore, as the technology develops, they could either try to suppress it or place the blockchain under their control which would, in effect, make blockchain just a new cybersecurity technology rather than a technology that could drive change on a systemic level.

The blockchain technology is ostensibly a trading zone, however when you expand away from the cryptocurrency example and explore the technology overall there is a key difference. Trading zones are places that groups can use to exchange information about each other, however with blockchain you do not need to know anything about the other users. The system is self-

[11] Mark Van Rijmenam & Philippa Ryan (2019)
[12] Mark Van Rijmenam & Philippa Ryan (2019)

regulating, so there is no person or group at the top controlling the blockchain. The entire point of the system is that nobody has to trust any other user of the system. Also, each group is currently attempting to build their own blockchain instead of sharing one since the technology is still new. This is a very novel idea, which makes it important to explore all the ways that this technology will benefit the world. To do this, I will be using Actor-network theory since I think it is important to explore the different motivations behind growing this technology or suppressing it by different actors. Everybody is linked by their desire for increased security; however, each group has a separate goal as well. This framework will allow me to assess the social benefit through the context of the technology and how the actors around it are attempting to develop it for their own goals, making this the optimal framework to use.

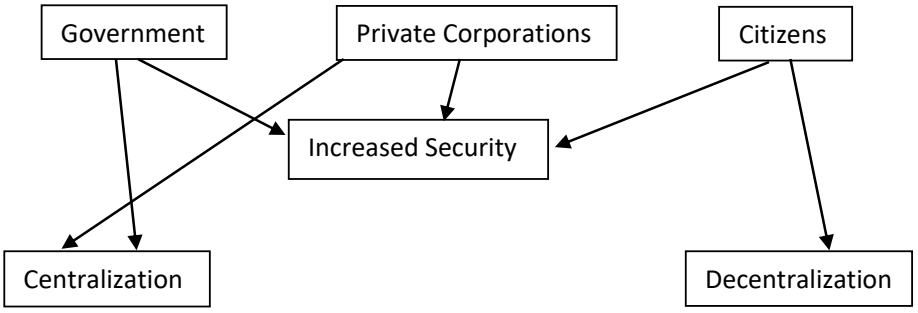

Figure 2: Blockchain Actor-Network

Figure 2 is a diagram of the current network. The actors include the people who support this technology because of their mistrust of corporations and the corporations themselves who are using this technology in-house instead of in a decentralized capacity. The government, who wants to limit the decentralization opportunities of blockchain, is also a major actor in this network. How these actors interact with each other as they try to use blockchain for their own purposes will be interesting to observe, especially since the goals of each of these actors often conflict with each other. Exploring this network will provide a great perspective on the future of

blockchain and where it will lead our society in the future. There is a ton of potential for this technology, and the competing interests of this network will each use blockchain to try to guide our society on to a different path.

There are plenty of directions this research could go. The role of the government and whether it will attempt to control, regulate, or simply use this technology is something that we still do not know. Research could also be done into how blockchain could help the world, such as helping people in poverty. I intend to research, however, how this technology could potentially impact the systems the world has had in place for centuries. A self-regulating system like blockchain removes the need for regulators and middlemen, which lots of people would be supporters for, and lots of people would not. The impact on our economy from the loss of jobs in specific fields, for example, could be problematic if blockchain technology ever gets fully implemented. Exploring where this could go is extremely interesting since it has the potential to change the world.

References

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, & Steven Goldfeder (2016). **Bitcoin and cryptocurrency technologies: a comprehensive introduction**. Princeton, NJ: Princeton University Press.
2. Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved October 31, 2019 from https://bitcoin.org/bitcoin.pdf
3. Matthew Beedham (2019). *All you need to know about Bitcoin network nodes.* Retrieved October 31, 2019 from https://thenextweb.com/hardfork/2019/03/01/bitcoin-blockchain-nodes-network/
4. Mark Van Rijmenam & Philippa Ryan (2019). **Blockchain: Transforming Your Business and Our World**. New York, NY. Routledge.
5. Jake Frankenfield (2019). *Consensus Mechanism (Cryptocurrency).* Retrieved October 31, 2019 from https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp
6. Ravikant Agrawal (2018). *Digital Signature from Blockchain context.* Retrieved October 31, 2019 from https://medium.com/@xragrawal/digital-signature-from-blockchain-context-cedcd563eee5
7. Jimi S. (2018). *Blockchain explained: how a 51% attack works*. Retrieved December 6, 2019 from https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474?