Reflection Paper

My Experience of The Class

Sanchit Singhal

Fall 2018 – November 30, 2018

INF385T – Introduction to Blockchain w/ Lance Hayden

School of Information

Before this semester, I knew little to nothing about Blockchain, its history, the technology, and its functional capabilities. Of course, like many others, I had heard of it 'revolutionizing' the world – but wasn't quite sure what and how that was supposed to happen. I had a few friends who had invested in Bitcoin and made some good money when the prices shot up towards the end of 2017. I remember, consequently, watching a 45-minute documentary on cryptocurrencies – which mainly focused on Satoshi Nakamoto, the unknown entity that authored the bitcoin white paper, created the first distributed ledger system, and deployed the original implementation. Intrigued, I watched a second video about Silk Road and the controversy that had surrounded it. It was around this time when I was registering for courses during the Fall 2018 semester at UT and I found "Introduction to Blockchain" listed in my department. This seemed like the perfect opportunity to build a solid foundation and get an overview of the concepts in the technology – I signed up for the class. Now that I reach the end of the semester, I look back at this decision and I'm really glad I decided to take this course. This class was perfectly suited to what I was looking for: through readings, online material, lectures with Lance, discussions with my peers, and guest speakers, I was able to work my way through various outlooks of the technology. This paper will be a self-reflection about my experience in the class and how it has changed my understanding of Blockchain.

The first few sessions of the class really set up the rest of the semester. On the first day itself it was clear that this was going to a popular subject – more than 15 people who were wait-listed came to attend UT's first Blockchain course. The students that I did get to interact with throughout the semester were great – it was a really diverse set of backgrounds (both technical and otherwise), and some of my favorite activities in the semester turned out to be participating in fun, but informative discussions with them. Lance promoted this type of active learning which really helped me learn in an engaging way. A lot of ethical issues around Blockchain are not really black and white; this style helped me understand the grey areas by gaining insights from differing viewpoints.

During our first module, we started of by discussing the history of Blockchain and its roots as an ideologist construct of crypoanarchists and cypherpunks to break-free from centralized authority. I still find it interesting to compare where Blockchain technology is heading and wonder what the original creators would have to say about it. As we continued down the historical path, I learned about Digicash, an electronic money company back in the early nineties, that solved the double-spend problem through hash functions, a cryptographic one way trip for data. This concept really struck home when I got to play around with Merkle Trees in the first lab. It was a smooth transition but this is the point of the class where we really started "getting under the hood" of Blockchain. I learned about the peer-to-peer network structure which enables a distributed system for the Blockchain so that the nodes are able to share computing resources. We also investigated the formal trust problem of The Byzantine General's Problem. Putting these concepts together, I was finally able to understand the artifact that had sparked my interest in the technology in the first place: Bitcoin – a distributed, triple entry ledger system. But after learning it at a technical level, I realized that this was much more than just a digital currency. The concepts that stem and make Blockchain what it is enables much more; a paradigm shift altogether. The rest of the course focused more on Blockchain, but over and above its role in Bitcoin and we started looking at some of the more recent developments.

For me, the one of the most interesting ideas was consensus mechanisms and the variety of flavors that they come in. Although Bitcoin uses the Proof of Work algorithm, there is

also Proof Stake - more environmentally friendly alternative – which does not require the expense of electricity to mine blocks. Another interesting concept that this class introduced to me was the idea of second generation Blockchains such as Ethereum as opposed to a first generation one like Bitcoin. This new generation is a Turing complete computer which allows to run any program that is entered into it. This feature, known as a Smart Contract, written in a programming language, allows for any sort of agreement between parties without the need of an intermediary. Taking this idea one step further allows for dAPPS (distributed applications) which is software that can be run across the network. Although I am still trying to full understand the Web 3.0 architecture, as a technologist, I am definitely able to see the potentials that such an infrastructure can provide. It is during this exploration, Lance introduced me to the idea of IFS (InterPlanetary File System): a peer-to-peer, open source file system that houses documents for the entire world. It's ideas like these that make me believe that Blockchain might be just as revolutionary as the Internet was.

After covering some of the basics, learning the terminology, and going over additional specifics of how Blockchains function, we started looking at applications and use cases. This module especially appealed to me – it helped give me some perspective into how the technology is being used today and proposals for future uses. By nature, I am quite a practical, pragmatic person and this portion of the class allowed me to consider implementation details for real-world utilization. Having a mental map of the differences between public vs private and permission vs permissionless really brought clarity to tailoring a solution for a specific use case. I even got to partake in a project in which I worked with a team to pitch a real Blockchain project: we designed a monetary supply-chain platform for donation management. This exercise was valuable for understanding how to apply the theory to perform a real-world business solution and appreciating situations in which Blockchain is and isn't useful. Lance did a great job over the course of the semester at inviting a lot of guest speakers to come and interact with us as a class. I feel like that also enhanced my understanding of current industry practices around Blockchain. It was eye-opening to understand its applications in identity management, health case, ownership rights, and governance. Many of these projects I could understand but I would still like to learn more about ICOs and this phenomena around alternative funding. I am definitely going to try and stay up to date with development in this space. One of the assignments in the class, the first case study, also gave me the opportunity to explore some potential use cases in the Oil and Gas industry. I am most probably going to work at an upstream petroleum firm upon graduation and having already done research in the field, I'll be arriving full of ideas that I can share with my colleagues-to-be.

One of my other favorite parts of the class were the discussions regarding the philosophies and implications of the solutions being presented from the viewpoints of the society, capitalism, and technology. It's particularly interesting to examine the role of private corporations and their adoptions of these tools in contrast with the ideas of the cypherpunks. It was also fascinating to debate on the role of this technology on our future cultural impact – specifically the pros and cons of the idea of law by code. During these analyses, it was also important to focus on constraints that Blockchain still need to overcome. Issues such as scalability and standards present opportunities for budding developers such as myself to work on.

Fortunately a lot of the work in Blockchain is open-source and I would love to potentially work on some of the forks that out there on Github. My second case study focused on learning

to become a Blockchain Developer and one of the suggestions from my research was to get involved myself. Heeding my own advise, I am currently working on writing a smart contract in Solidity. Although it is relatively rudimentary at the moment, I plan on progressively building my skill in the language to pursue more and more complex structures. Although I am primarily doing this as a personal project, I do envision smart contracts playing a bigger role in my professional career. As mentioned, maybe I'll be able to convince my team at my job to deploy parts of the business workflow on a Blockchain to manage certain processes through this kind of automation; there are multiple supply-chain opportunities that can be pursued. In conclusion, I have certainly come a long way in my understanding of Blockchain through this introductory class. I was hoping Lance would offer an intermediate class in the Spring semester – I would have definite taken that – but regardless, I do feel like I have built a foundation from which I can build upon. I would like to thank Lance for being a terrific instructor that really brought a lot of fun to the semester but also my peers in the classroom – I got to learn from each of them. I hope to cross paths with both Lance and my peers again in our Blockchain journeys!