University of Manitoba

COMP 4520 – Undergraduate Honours Project Proposal

Blockchain for Education

Zack Holmberg | 7777823 | holmbezt

Supervisor: Robert Guderian

I. Abstract

I believe that blockchain technology can potentially impact countless aspects of the current digital landscape, from topics such as commerce to data management/storage and everything in between. With this in mind, I strongly believe that it is critical for future students to have a strong educational foundation regarding blockchain/distributed ledger technology so that students are prepared to adopt and work with the technology at an industrial and academic level.

II. Introduction

Blockchain technology is arguably the most disruptive technology to surface in the last decade. I foresee a future with many interconnected distributed blockchains, each of which have the potential to be specialized to suit the purposes of its creators, but also may require communication with other blockchains. Thus, any understanding and implementation of blockchain technology should be as modular as possible. For my Honours Project, I will construct a modular blockchain that will be incorporated into the current Computer Science curriculum, in the form of assignments, labs and potentially course material.

III. Preparation

My level of preparedness for the undertaking of this project is showcased by many different experiences. First and foremost, in COMP 3010 I gained a deep understanding of distributed systems, which blockchain is. Furthermore in 3010, I did my Term Paper on blockchain technology, which allowed me to develop a strong understanding of this technology and its potential applications, which is how the idea

for this project was born. As part of my paper, I wrote a simple blockchain example, more specifically a basic implementation of a cryptocurrency, that could serve as a skeleton for which the blockchain in this project can be built upon.

Additionally, through taking other courses such as COMP 2140, COMP 3170 and COMP 3350, I have developed a thorough understanding of data structures, algorithms and software engineering, which are all essential for this project.

IV. Related Work

On October 31, 2008, the world was changed forever when a whitepaper, titled "Bitcoin: A Peer-to-Peer Electronic Cash System" was published under the pseudonym Satoshi Nakamoto. In this paper, Nakamoto introduced the cryptocurrency known as "Bitcoin". Additionally, Nakamoto detailed the implementation of the cryptocurrency known as the Blockchain (Nakamoto, 2008).

In 1991, 17 years before Nakamoto released their paper, Stuart Haber and W. Scott Stornetta published the article "How To Time-Stamp a Digital Document" in the Journal of Cryptology. Haber and Stornetta's article proposed using hash values of documents and saving those values alongside a timestamp (Stornetta, 1991). Then, records would be linked in a chain-like data structure, akin to a linked list, by storing hashes of previous records. Additionally, their timestamping protocol makes use of private key digital signatures to authorize submitted data (Stornetta, 1991).

With regards to work regarding the modular blockchain concept, the Hyperledger project is an excellent initiative. The Hyperledger project plans to "ambitiously move towards a modular architecture resulting in 'pluggable' components for setting up blockchain networks." (Teis, n.d.). Furthermore, the Hyperledger project seeks to have their code and ideas be reused by other projects, thus contributing to a standardization of the blockchain technology over time.

With respect to my own work, the cryptocurrency that I developed for my COMP 3010 Term Paper would be an excellent piece of code to leverage for this project. Other examples of related work include the repositories of various simple and complex cryptocurrencies and blockchain platforms, which can be found in excess with a quick google search. However, as far as I can find, there exists no public

custom and modular blockchain within the University of Manitoba Computer Science curriculum or academic labs. Furthermore, I can find no implementation of such a blockchain on the internet whatsoever.

V. Problem Statement

The goal of this project is to develop a custom blockchain that can be used as a pedagogical tool that will help teach future students about blockchain technology, as well as other various topics already in the curriculum, such as data structures and algorithms, distributed systems, networks, etc.

VI. Methodology

September	October	November	December
- Finalization of project scope and stakeholders - Begin conceptualization and design of the blockchain implementation.	- Finalize the design of the blockchain implementation - Begin development of the blockchain. - Specifically, complete at least one portion of the blockchain, such as the distributed systems component/candidate course assignment of the blockchain. - Begin considering the written report layout and the material that I want to cover within it.	- Continue development of the blockchain. - Goal will be to be complete at least three topic portions of the blockchain. - Finalize the written report layout and material. - Begin working on written report.	- Complete the development of the blockchain. - Complete the written report. - Present the blockchain and written report to stakeholders and supervisor.

VII. Requirements

The only requirements needed for this project is the supervision of Robert Guderian, as well as the advisement of potential stakeholders within the Computer Science department, who have already been consulted and involved in the inception of this proposal.

VIII. Deliverables

An implementation of a blockchain, whether it be a cryptocurrency or platform (which uses smart contracts), will be developed as part of this project. This blockchain will be designed to enable it to be used in various courses in the form of assignments and labs. A report that dives more specifically into the design of the blockchain, applications of the blockchain and possible future work will be included in the report as well.

More specifically, through the consultation of various academics within the Computer Science department, the following course-specific applications for the aforementioned blockchain implementation were conceived:

- *COMP 3010 Distributed Systems:* Blockchain exists, creating a peer to hold the blockchain. Could add consensus items, mining. Recovery.
- *COMP 4140 Cryptography:* Applying hashing, Public/Private key implementations. Work with the blockchain, and design or implement a hash component to a running chain.
- *COMP 4580 Computer Security:* Attack the blockchain, do a 51% attack. Explain consensus and peer-to-peer security. Make a compliant, but malicious peer.
- *COMP 2140 Data Structures and Algorithms:* Using the material in the written report and the blockchain itself for an assignment to help educate students on a variety of topics, including but not limited to linked lists, hashing, and blockchain technology itself.

IX. References

Block. (n.d.). Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Block

Block 0. (n.d.). Retrieved from Blockchain.com: https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Bayer D., Haber S., Stornetta W. S. (1993). Improving the Efficiency and Reliability of Digital Time-Stamping.

Marco-Gisbert, S. S. (2019). Assessing Blockchain Consensus and SecurityMechanisms against the 51% Attack. MDPI applied sciences, 1-17.

Michael Nofer, P. G. (2017). Blockchain.

Mining. (n.d.). Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Mining

Nakamoto, S. (2008, October 31). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from bitcoin.org: https://bitcoin.org/bitcoin.pdf

Stornetta, S. H. (1991). How To Time-Stamp a Digital Document. Journal of Cryptology, 99-111.

Teis, D. S. (n.d.). *Position statement: Hyperledger Project*. Retrieved from https://www.w3.org/2016/04/blockchain-workshop/interest/teis.html

Voshmgir, S. (2019). What is Blockchain? In S. Voshmgir, Token Economy.

Zibin Zheng, S. X. (n.d.). An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends. 2017 IEEE 6th International Congress on Big Data. 2017.