Achtatou Sean
Sergei Tickomirov

University of Luxembourg

Bachelor in Computer Science

The Block Chain

(Short Version)

Semester 2 - 2017-2018

1.Introduction

This research work, for a semester project in the Bachelor in computer Science in the University of Luxembourg, is about the study of a new system used to establish secured digital transaction between people in the world on the internet: the Block Chain. The goal of this project is to attempt to convince the people to trust the Block Chain security system, since it might be used in a near future around the world for our transaction. To achieve this, we need get to know with several functions belonging to the Block Chain and prove, for each, their security.

2.Project Description

2.1. Domain

The domain of this project concerns one of the many interesting world of the computer science: the cyber-security. With the evolution of technology and their difficulties, today, the cyber-security is now considered as well important for the start of any system or program to be secured, according to its level of importance, or if the user wish to secure it better than it already is.

For this project, the cyber-security is evolving around the Block Chain. This last is used as an effective secured way to establish transaction, between several users by peer to peer connections.

2.2. Objectives

The main objective of this project is to provide to the people unaware, a new way of thinking about the security of the computer science. We worked on the security of the Block Chain system, that is well used for many programs since several years. Several computer scientists having provided research on it, concluded that it was computationally impossible to break the Block Chain's security. The goal for this project is to show it is indeed correct.

As conclusion, we should all be convinced, that it is indeed one of the best security system nowadays, and we can trust that system for now to secure our transactions.

2.3. Constraints

The first of the constraints is the understanding of the average mathematics. We are not in the basics of the security, but a level higher, consequently several notation has to be understood to be able to follow.

The second constraint is the capability to implement some basics algorithm for a given language. All the programs are being implemented on Python 3. It is a simple language that is quite simple to use and to learn.

The last constraint is the security domain of the computer science. The security of the Block Chain is based on several notions such as the cryptography.

3.Background

3.1. Scientific

3.1.1. Security in computer science

The security in computer Science is becoming really important since several years. It is the only way for the users to get a protection against an attempt of security breach leading to a corruption of their private data.

3.1.2. Secured algorithms

The technology is evolving. Since the beginning of computers attacks, the computer scientist provides new types of counter-attacks to these, creating more secured algorithm, providing a better security for their users.

3.1.3. Notion of cryptography

The cryptography is one important notion which has been used since the Romain Empire. This stay one of the most efficient way to encrypt and decrypt data using keys and complex algorithms.

3.1.4. Why get interested to the block chain?

The technology in computer is evolving from days to days, and the security is one side which is prioritized. The system of the Block Chain may consequently, in a near future, become the main method for our transaction around the world.

3.2. Technical

3.2.1. Block chain visualization

The Block Chain, compared to the most of the used network on the Internet is using, is based on a peer to peer network, meaning each users are directly connected between them, while a server based would rely on a centralized server.

3.2.2. Hash function in the Block Chain

There exist two types of Hash function. The Cryptographic, which must respect several properties providing security to the Block Chain. And non-cryptographic, which is more used to only avoid data corruption.

3.2.3. Digital signature in the Block Chain

The digital signature, based on the cryptography, is used to provide a signature to the user's transaction. It relies on three secured algorithms:

- Creation of a private and public key for the user
- Signature of the transaction.
- Verification of the signature.

3.2.4. Merkle tree in the Block Chain

The Merkle Tree is a function used inside a Block of the Block chain, whose algorithms is used to verify if a transaction is a membership or not of the block.

4.Results

4.1. Hash Function

For the Hash function, we verified the properties relied to its security. At the end of the tests and based on the results, we realized some of the properties were time secured. Indeed, one of the properties, such as Collision-Resistant, make it impossible for an adversary to break the algorithm in a time interval of several years nay decades because the time taken to break it would increase exponentially. All the verified properties of the Hash Function are satisfying the fact that it has been used in the Block Chain algorithm to make it well secured.

4.2. Digital Signature

For the Digital Signature, we verified as well the properties relied to its security. The verification about the security of the properties of the Digital Signature were obviously satisfied. Moreover, we analyzed the types of attacks which could happen for the algorithm to be broken, and provided an explanation on how the adversary would be able to use each type of those attacks. It results that the Digital Signature attacks were almost impossible to accomplish. Consequently, the use of the Digital Signature in the Block Chain make it well secured to be used.

4.3. Block Chain

A project we had to do is to create a local Block Chain, allowing us to provide a way to understand how a real Block Chain would be operating. Since we worked in local, the use of a digital signature algorithm was not needed because there were no users. The final project is well satisfying. The local Block Chain is able to simulate how the Block Chain would operate at live time. It can add new transactions; mine those transactions, which is an operation done by miners in a real block chain, meaning it creates a new block with the transactions which will be add to the Block Chain and calculate the block properties.

5.Conclusion

In conclusion of this project, we can tell the Block Chain algorithm is indeed well secured, thanks to the contents of the several analyzed functions, which seems to provide an efficient security. And consequently, the Block Chain system might be used in our day life as our future transaction method around the world.