

# COMP 1011 Project Report

## A Blockchain Implementation

COMP, The Hong Kong Polytechnic University

JIANG Guanlin

21093962D

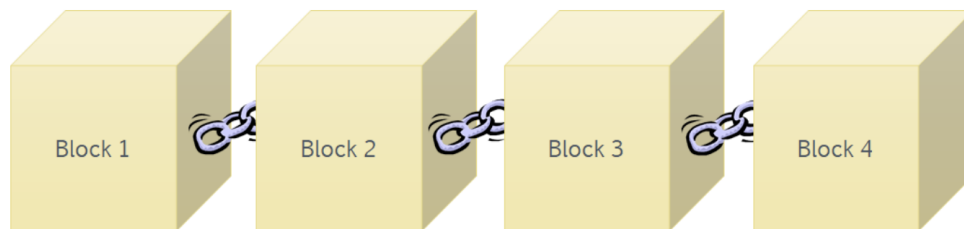
April 20th, 2022

# 1 Introduction

This report introduces the creating parts of this Blockchain System project. In this report, I will explain the statement and objective of project, how to design the whole blockchain system, some data structures I used, and the explain the libraries used in this project.

## 2 Technology Background

Blockchain Technology is a system which can recording the information and linked the every information to storage with timestamp also encrypt to the hash value to blocks. It makes blockchain system difficult or impossible to hack, cheat, steal, even change some data. Like in figure 1:



*Figure 1: Example of Add New Block.*

## 3 Objectives

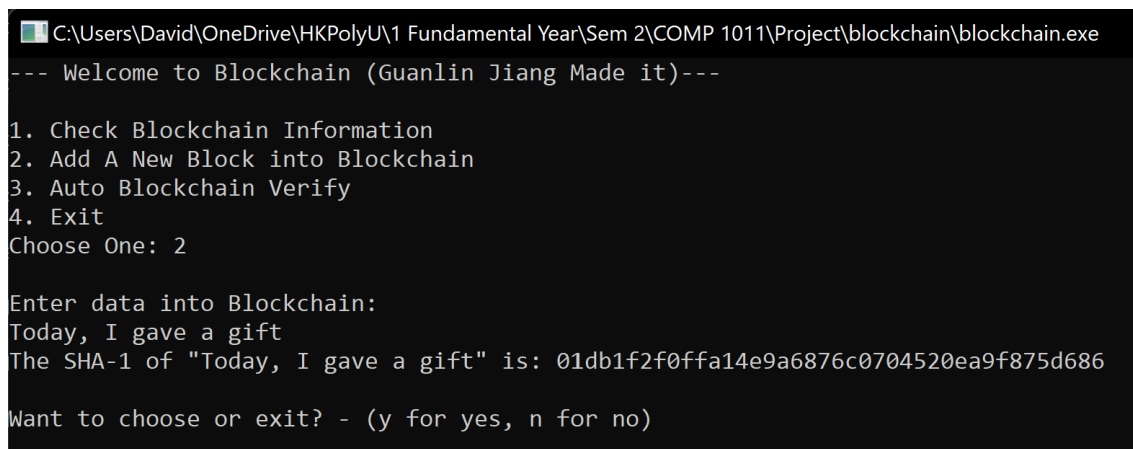
The objectives for this Blockchain System that I want to this save the data that people input, use the hash to link the block, and every block will be linked. Also, protecting the data security that can prevent data from being maliciously tampered with and alert managers to urgent review. Checking the information in this blockchain system will be add the time, hash, and data in to block.

## 4 Blockchain Design

For this Blockchain System, here have 3 kinds of functions to be designed in Blockchain System:

### 4.1 Add New Block

In this part, I design to let people input the data they want to storage, the data will be generate the hash value which encrypted by SHA1 algorithm and that hash value will be storage in the block file, with the original data and timestamp which keep the UTC time format, also plus the previous block hash. But for first block, no previous block hash at all. Like in Figure 2:



```
C:\Users\David\OneDrive\HKPolyU\1 Fundamental Year\Sem 2\COMP 1011\Project\blockchain\blockchain.exe
--- Welcome to Blockchain (Guanlin Jiang Made it)---

1. Check Blockchain Information
2. Add A New Block into Blockchain
3. Auto Blockchain Verify
4. Exit
Choose One: 2

Enter data into Blockchain:
Today, I gave a gift
The SHA-1 of "Today, I gave a gift" is: 01db1f2f0ffa14e9a6876c0704520ea9f875d686

Want to choose or exit? - (y for yes, n for no)
```

*Figure 2: Example of Blockchain.*

### 4.2 Check the Block Information

For a open blockchain system, the information checking will be useful for security and open source. When people want to check the information storage in blockchain system, it will be print out the block structure to help people choose which block want to check. When people input the block number, the system will be read the block file and give back the information that storage in block, which include this block hash value, data, and timestamp, also include the previous block hash value. Like in Figure 3:

```

C:\Users\David\OneDrive\HKPolyU\1 Fundamental Year\Sem 2\COMP 1011\Project\blockchain\blockchain.exe
--- Welcome to Blockchain (Guanlin Jiang Made it)---

1. Check Blockchain Information
2. Add A New Block into Blockchain
3. Auto Blockchain Verify
4. Exit
Choose One: 1

<-- Block [4] <-- Block [3] <-- Block [2] <-- Block [1] <-- Block [0]

Which Block want to look? - 3

-----
Block Number: 3
hash: 24f21c90961c032a307b21ae8d1c481327161a3a
data: I study in PolyU
Timestamp (UTC): Sun Apr 17 08:08:48 2022

prev hash: d008a0484cdbc512be0328e588af0a4ec79336d0
-----

Want to choose or exit? - (y for yes, n for no) _

```

Figure 3: Example of Information Checking.

### 4.3 Check the Integrity of the Blockchain

According to the rule of Blockchain, the immutable feature. I design the auto verifying system to keep the blockchain system unchangeable. If the blockchain system have some maliciously tampered with by someone, just need to initial verifying system, the blockchain will be verifying every block to find the changed block, and stop in that block. Like in Figure 4: (the up one is blockchain unchanged, under that is the example of blockchain changed):

```

C:\Users\David\OneDrive\HKPolyU\1 Fundamental Year\Sem 2\COMP 1011\Project\blockchain\blockchain.exe

1. Check Blockchain Information
2. Add A New Block into Blockchain
3. Auto Blockchain Verify
4. Exit
Choose One: 3

prev hash: 24f21c90961c032a307b21ae8d1c481327161a3a
prev hash: 24f21c90961c032a307b21ae8d1c481327161a3a
The Blockchain Verified, no changed.

check prev one
prev hash: d008a0484cdbc512be0328e588af0a4ec79336d0
prev hash: d008a0484cdbc512be0328e588af0a4ec79336d0
The Blockchain Verified, no changed.

check prev one
prev hash: b85421ce541e8b12c5792dad04c7e962b558f7c7
prev hash: b85421ce541e8b12c5792dad04c7e962b558f7c7
The Blockchain Verified, no changed.

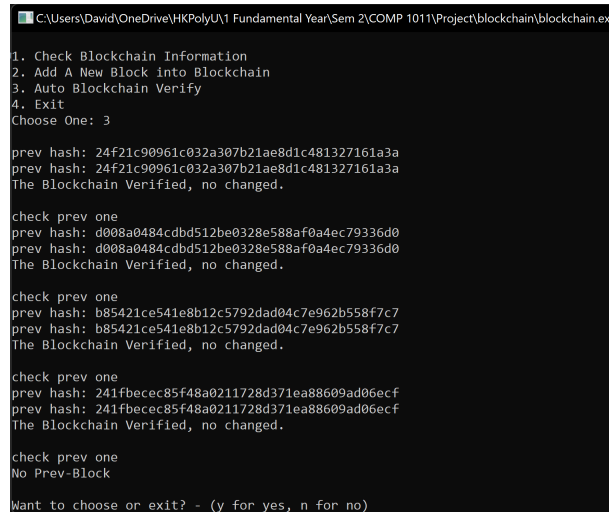
check prev one
prev hash: 241fbec85f48a0211728d371ea88609ad06ecf
prev hash: 241fbec85f48a0211728d371ea88609ad06ecf
The Blockchain Verified, no changed.

check prev one
No Prev-Block

Want to choose or exit? - (y for yes, n for no)

```

Figure 4: Example of Verify Blockchain (Unchanged).



```

C:\Users\David\OneDrive\HKPolyU\1 Fundamental Year\Sem 2\COMP 1011\Project\blockchain\blockchain.exe
1. Check Blockchain Information
2. Add A New Block into Blockchain
3. Auto Blockchain Verify
4. Exit
Choose One: 3

prev hash: 24f21c90961c032a307b21ae8d1c481327161a3a
prev hash: 24f21c90961c032a307b21ae8d1c481327161a3a
The Blockchain Verified, no changed.

check prev one
prev hash: d008a0484cdbc512be0328e588af0a4ec79336d0
prev hash: d008a0484cdbc512be0328e588af0a4ec79336d0
The Blockchain Verified, no changed.

check prev one
prev hash: b85421ce541e8b12c5792dad04c7e962b558f7c7
prev hash: b85421ce541e8b12c5792dad04c7e962b558f7c7
The Blockchain Verified, no changed.

check prev one
prev hash: 241fbec85f48a0211728d371ea88609ad06ecf
prev hash: 241fbec85f48a0211728d371ea88609ad06ecf
The Blockchain Verified, no changed.

check prev one
No Prev-Block

Want to choose or exit? - (y for yes, n for no)

```

Figure 5: Example of Verify Blockchain (Unchanged).

## 5 Problem Statement

### 5.1 Read a Special Line of File

When I want to read the block file use in verify function, which mean I need to get the hash value in special line in that file to compare the previous hash line in next block file, so I use ignore to the next line.

### 5.2 Connect the Block Numbers

When the program shut down, the block number will be lost, so I make a index file to storage the block number for the next time reading and make the new block.

### 5.3 Verify one by one

When the program start verify the block, before I use while to write, but I think that will not good to increase the efficiency. So, I changed to the recursive which can help me to decrease the code, also help the blockchain system more efficiency.

## 6 Structure

In this Blockchain System, I use call by value, and recursive structure, and make some function to form this blockchain.

### 6.1 Call by Value

In this project, use call by value this data structure to help me transfer the variable value between function and function. For example, in hash-verify function, I use call by value to transfer the Block Number to this function, and execution the verify code in that function. Also, in block-info this function, I used call by value to transfer the information that storage in block, and form into the format, and transfer that style to the information checking, and printout. In the menu function, I also add this structure to help me transfer the choice number to the menu and run the part functions.

### 6.2 Recursive

Also, in this project, I use recursive to keep some loop easier to write, use function to call that function can be more structure in the blockchain system. For example, also in function hash-verify this part, I use recursive to make it. Use recursive in here to help me loop, without while and for, all processes will be automatically running for the Block Number -1 to the Block 0.

## 7 Library

The libraries I used are, iostream for normal input and print out the data, cstring for string copy, fstream for read and write files, ctime for get the system time and make the timestamp, SHA1.cpp and SHA1.h for generate the hash value based on sha1 of the data.

## 8 Conclusion

In this project, I learned the blockchain technology concepts and some features of make a blockchain system. Also, try some new data structure and more familiar with the programming strategy. Doing a project let me to think about the naming of variable and the familiar framework is more important.