COMP 1011 Individual Project Report

The Blockchain Implementation

COMP, The Hong Kong Polytechnic University

LIU Minghao

21096308D

April 20th, 2022

1 Introduction

This report is an introduction to the Blockchain System project. In this report I will present some of the statements and objectives of the project, the design of the whole blockchain system, the data types and structures used, and some of the libraries used in the program.

2 Technology Background

Blockchain technology is a system where users can record information and store the information entered in blocks, while also encrypting the hash of the block and transferring it to the next block. The blockchain system is difficult or impossible to hack and the stored data is difficult to tamper with, making it a secure transmission system.

3 Project Objectives

The objective of the blockchain system I created is to allow the user to enter the information to be stored and encrypt it with a hash function based on the information entered. The encrypted information is then transferred to the next block via the blockchain. The user can find the desired block in three ways, including by block number, the text or the hash values of a particular block. On the other hand, the user can look up the hash value of all blocks in the blockchain, including the hash value of this block and the previous hash value. It is also possible to view the information stored in the blockchain. This project also includes a check on the security of the chain transfer if the hash values do not match. The user will be prompted that the information transmitted by the blockchain has been maliciously modified.

4 Blockchain Design

For this blockchain system project, there are four features available here for users to choose from.

4.1 Add New Block

In the add block section, my design is for the user to enter the data they want to store, which will go through a hash function and be encrypted by the "SHA1" algorithm to generate a hash value. The hash of the previous block will also be read in the chain table. The index, the text and the two hashes will be stored as a structure each, in an array called "block_chain". The address of the previous block is passed to the next block using the "*next" operation of the chain table. Like figure 1 shows:

```
hash = hash_function(text);

block->block_array[i].index = i + 1;
block->block_array[i].text = text;
block->block_array[i].p_hash = p_hash;
block->block_array[i].hash = hash;

p_hash = hash;
block->max_size++;
```

Figure 1: Block store information.

4.2 Search Block Information

For a blockchain system, providing the user with the ability to perform information checks is very useful for security and open source. When a user wishes to check the information stored in a blockchain system, the system will give the user three options, including searching by block index, the text or the hash values of a particular block. When the user enters the correct index, text or hash value, the system will automatically retrieve the block that matches the information entered. If it is possible to match the relevant information in the block chain, all information about the matched block is returned, including the index, text and two hash values (current and previous). Otherwise, the system informs the user that the information sought does not exist. Like figure 2&3 shows:

```
for (int i = 0; i < block->max_size; i++)
{
    if (block->block_array[i].text == text)
    {
        information(block, i);
        check = true;
    }
}
```

Figure 2: Search by Text.

```
for (int i = 0; i < block->max_size; i++)
{
    if (block->block_array[i].hash == hash)
    {
        information(block, i);
        check = true;
    }
}
```

Figure 3: Search by Hash Value.

4.3 Print Blockchain Information

As a blockchain system, the user is given the ability to query the entire blockchain for hash values and stored text.This function allows the user to check out if the stored information is incorrect and also to see more clearly the connections between the hash values.Like figure 4 shows:

```
for (int i = 0; i < block->max_size; i++)
{
    cout << "\tBlock No." << i + 1 << endl;
    cout << "\tText: " << block->block_array[i].text << endl;
    cout << endl;
}
```

Figure 4: Print Blocks Text.

4.4 Check Blockchain Integrity

The immutability is based on the rules of the blockchain. The verification function in the system is designed to maintain the immutability of the blockchain system to improve the security of the transmission. By comparing the hash values of the two blocks before and after it is clear that if the blockchain system is tampered with maliciously, the hash values of the two are different. The system will return the index of both blocks for the user to check

the problem.

```
bool check = true;
for (int i = 0; i < block->max_size - 1; i++) // Check all hash values, compare with their previous hash values
{
    if (block->block_array[i + 1].p_hash != block->block_array[i].hash)
    {
        cout << "\tThe chain between block " << i + 1 << " and block " << i + 2 << " exists problems" << endl;
        check = false;
    }
}
```

Figure 5: Check Blockchain Integrity.

5 Data Structure

In this blockchain system, I use the Call by Reference function, Array and Linked List.

5.1 Call by Reference

In this project, the call by reference function is used to help me transfer variable values between functions and functions. For example, in the "search_block" function, call by reference allows the user to print out blocks and their information with the same effect under three different choices. This has greatly improved the efficiency of the project and reduced code repetition. On the other hand, call by reference allows my code to call the contents of the "block_chain" array directly rather than in the same function, which definitely increases the efficiency of the project.

5.2 Array and Linked List

In this project, the complementarity between using arrays and linked lists made it easier for me to create blockchains to store blocks. Storing in this way also makes it very easy to find and retrieve specific blocks.

6 Library

<iostream> is used for normal input and printing of data, <cstring> and <string> is used for string copying and string input, "SHA1.cpp" and "SHA1.hpp" are used for the "SHA1" function to generate hash values, and "#Define" is used to define a max value of 1000.

7 Conclusion

In this project, I learnt the concepts of blockchain technology and making blockchain systems. In addition, I tried out some new data structures such as call by reference and linked lists to make my programming logic more familiar.