**DHA Suffa University**



**Department of Computer Science**

**CS 2001L – Data Structures and Algorithms Lab**

**Fall 2019**

# Lab 07 – Blockchain

**Objective:**

To learn implementation of blockchain using linked list and arrays.

**What is Blockchain?**

In simple words, Blockchain can be defined as a chain of the block that contains information. The blockchain is used for the secure transfer of items like money, property, contracts, etc. without requiring a third-party intermediary like bank or government. Once a data is recorded inside a blockchain, it is very difficult to change it.

The blockchain is a software protocol (like SMTP is for email). However, Blockchains could not be run without the Internet. It is also called meta-technology as it affects other technologies. It is comprised of several pieces: a database, software application, some connected computers, etc.

The first block in the chain is called the Genesis block. Each new block in the chain is linked to the previous block.

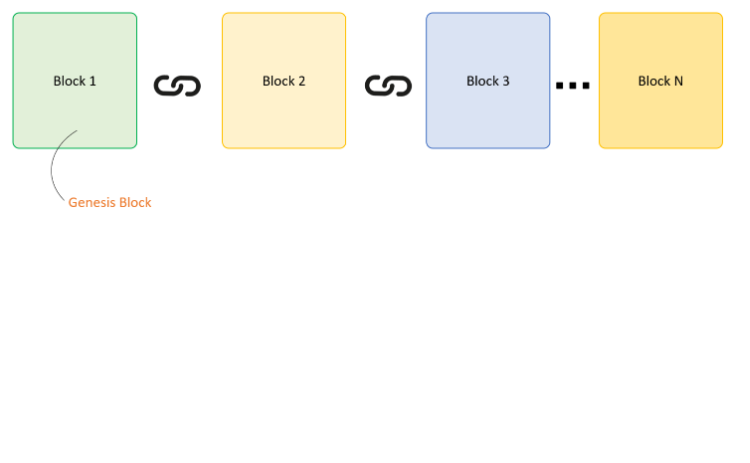


Figure 7.1 – Blockchain example

### **What does a block look like?**

A Blockchain is a chain of blocks which contain information. The data which is stored inside a block depends on the type of blockchain.

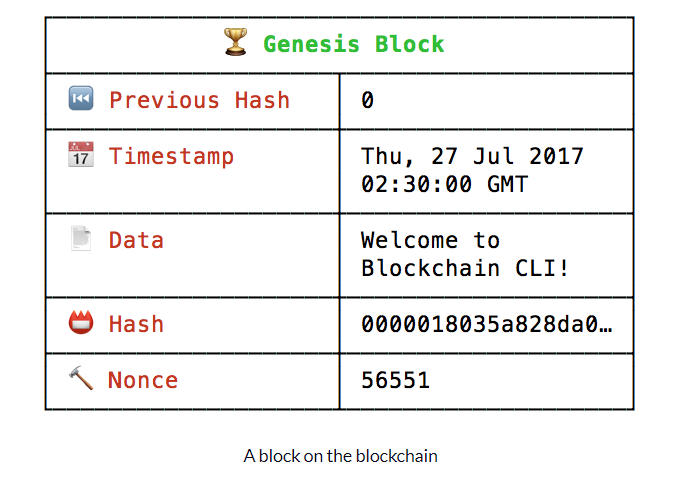


Figure 7.2 – a block on the blockchain

**Hash:** Is the block valid?

**Previous Hash:** Is the previous block valid?

**Timestamp:** When was the block added?

**Data:** What information is stored on the block?

**How is the hash calculated?**

A hash value is a value of a fixed length that uniquely identifies data. The hash is calculated by taking the previous block hash, timestamp, block data. The SHA256 algorithm will calculate a unique hash, given those inputs. The same inputs will always return the same hash.

It can be understood as a fingerprint which is unique to each block. It identifies a block and all of its contents, and it's always unique, just like a fingerprint. So once a block is created, any change inside the block will cause the hash to change.

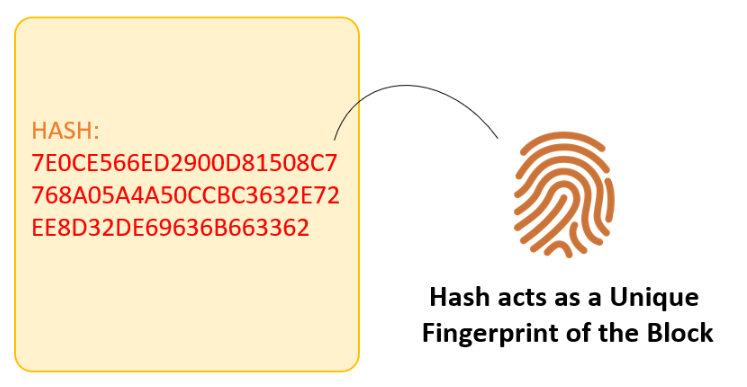


Figure 7.3 – Hash of a Block

Therefore, the hash is very useful when you want to detect changes to intersections. If the fingerprint of a block changes, it does not remain the same block.

Each Block has

* Data
* Hash
* Hash of the previous block

Consider following example, where we have a chain of 3 blocks. The 1st block has no predecessor. Hence, it does not contain has the previous block. Block 2 contains a hash of block 1. While block 3 contains Hash of block 2.

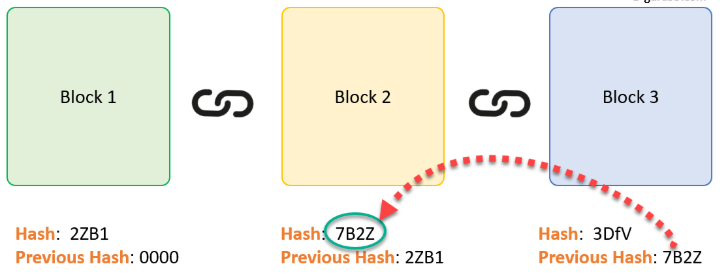


Figure 7.4 – Chain of blocks connected with the help of previous hash

Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain so secure. Let's see how it works - Assume an attacker is able to change the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of the Block 2. This makes Block 3, and all succeeding blocks invalid as they do not have correct hash the previous block.

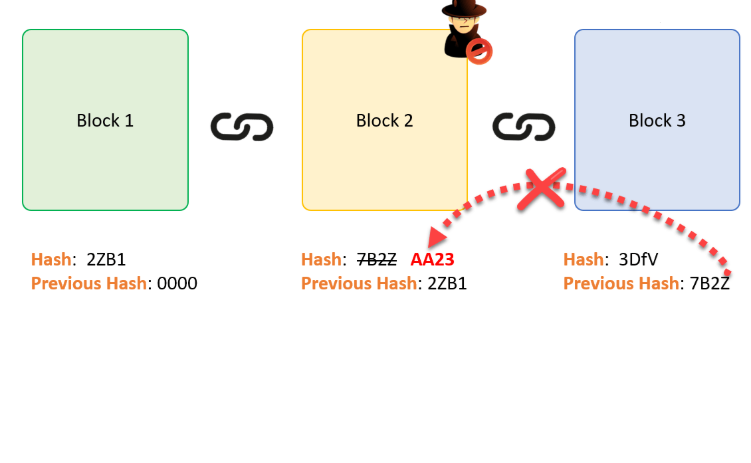


Figure 7.5 – Attacker manipulating data

**Proof of Work**

Hashes are an excellent mechanism to prevent tempering but computers these days are high-speed and can calculate hundreds of thousands of hashes per second. In a matter of few minutes, an attacker can tamper with a block, and then recalculate all the hashes of other blocks to make the blockchain valid again.

To avoid the issue, blockchains use the concept of Proof-of-Work. It is a mechanism which slows down the creation of the new blocks.

A proof-of-work is a computational problem that takes certain to effort to solve. But the time required to verify the results of the computational problem is very less compared to the effort it takes to solve the computational problem itself.

**Why does this matter?**

It matters because it keeps the blockchain immutable.

If we have the following blockchain A → B → C, and someone wants to change data on Block A. This is what happens:

Data changes on Block A.

Block A’s hash changes because data is used to calculate the hash.

Block A becomes invalid because its hash no longer has four leading 0’s.

Block B’s hash changes because Block A’s hash was used to calculate Block B’s hash.

Block B becomes invalid because its hash no longer has four leading 0's.

Block C’s hash changes because Block B’s hash was used to calculate Block C’s hash.

Block C becomes invalid because its hash no longer has four leading 0's.

The only way to mutate a block would be to mine the block again, and all the blocks after. Since new blocks are always being added, it’s nearly impossible to mutate the blockchain.

**Why do we need Blockchain?**

Here, are some reasons why Blockchain technology has become so popular.

**Time reduction:** In the financial industry, blockchain can play a vital role by allowing the quicker settlement of trades as it does not need a lengthy process of verification, settlement, and clearance because a single version of agreed-upon data of the share ledger is available between all stack holders.

**Reliability:** Blockchain certifies and verifies the identities of the interested parties. This removes double records, reducing rates and accelerates transactions.

**Unchangeable transactions:** By registering transactions in chronological order, Blockchain certifies the unalterability, of all operations which means when any new block has been added to the chain of ledgers, it cannot be removed or modified.

**Fraud prevention:** The concepts of shared information and consensus prevent possible losses due to fraud or embezzlement. In logistics-based industries, blockchain as a monitoring mechanism act to reduce costs.

**Security:** Attacking a traditional database is the bringing down of a specific target. With the help of Distributed Ledger Technology, each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.

**Collaboration :** Allows parties to transact directly with each other without the need for mediating third parties.

**Decentralized:** There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated, and all valid transactions are added one by one.

**Important Real-Life Use Cases of Blockchain**

**1.Dubai: The Smart City**

In the year 2016, smart Dubai office introduced Blockchain strategy. Using this technology entrepreneurs and developers will be able to connect with investor and leading companies. The objective is to implement blockchain base system which favors the development of various kind of industries to make Dubai 'the happiest city in the world.'

**2. Incent Customer retention**

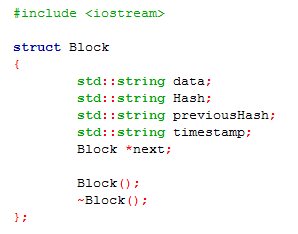
Incent is CRaaS (Consumer retention as a service) based on the Blockchain technology. It is a loyalty program which is based on generating token for business affiliated with its related network. In this system, blockchain is exchanged instantaneously, and it can be stored in digital portfolios of user's phone or accessing through the browser.

**3. Blockchain for Humanitarian Aid**

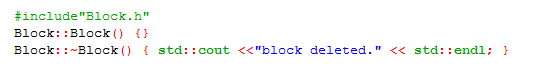
In January 2017 the united nations world food program started a project called humanitarian aid. The project was developed in rural areas of the Sindh region of Pakistan. By using the Blockchain technology, beneficiaries received money, food and all type of transactions are registered on a blockchain to ensure security and transparency of this process.

**Implementation of Blockchain using Link List**

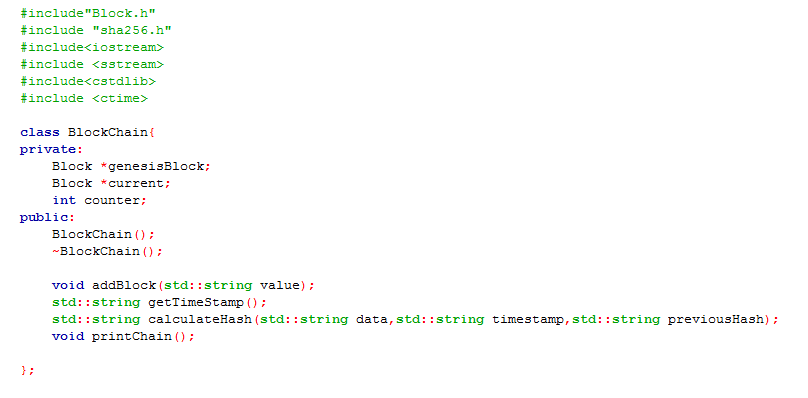
**Block.h**

****

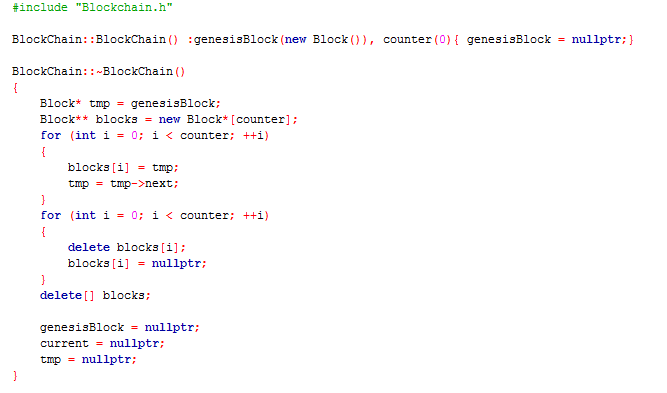
**Block.cpp**

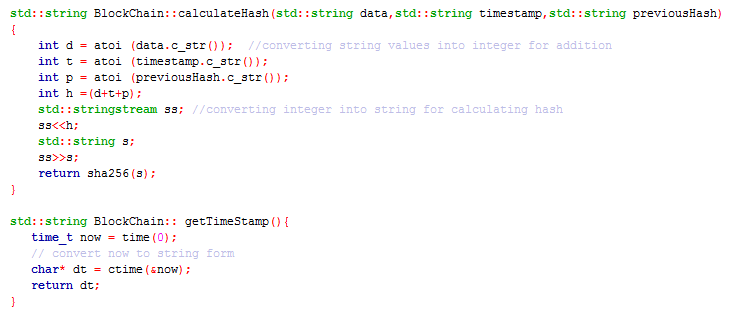
****

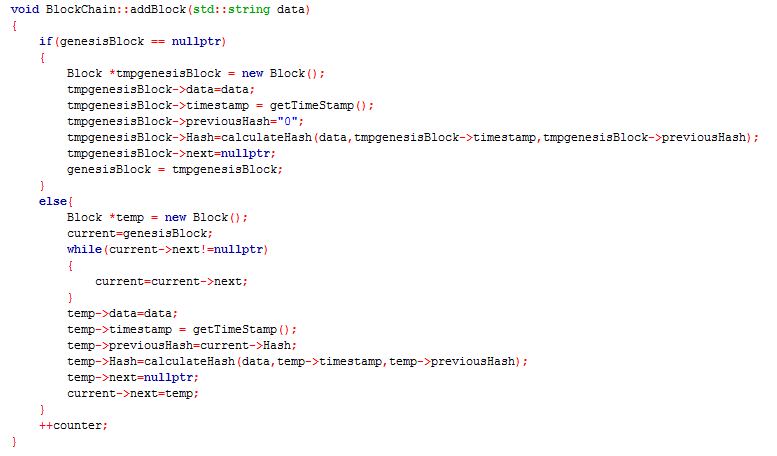
**Blockchain.h**

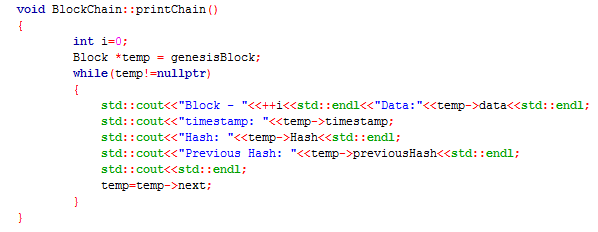
****

**Blockchain.cpp**

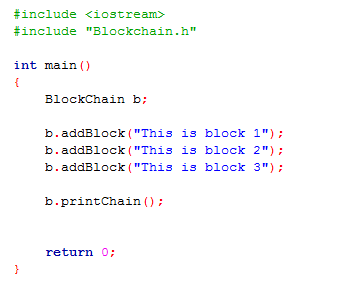
****

****

****

****

**driver.cpp**

****

**Assignment:**

Implement blockchain using arrays. Formula for calculating hash,

hash = sha256( index + data + timestamp + previoushash )

# Submission Guidelines

* **Write C++ code , separate function for each operation.**
* **Place your file in a folder named with your rollNo (cs172xxx) where xxx is your 3 digit rollno.**
* **Upload it on LMS.**