The role of pivotal Data Structures in Blockchain Technology

Dr. S. Vidhya

Associate Professor, KG College of Arts and Science, Coimbatore, Tamilnadu.

Abstract

A blockchain is a decentralized and distributed digital ledger that saves transactions on thousands of computers around the globe. This technology was developed to support digital currency bitcoin and is measured the most operational technology. One of the major component of blockchain is distributed ledger. This paper is proposed to be and overview of some basic concepts data structures that are integrated in distributed ledger of blockchain technology.

1 INTRODUCTION

A blockchain is the time stamped series of immutable records that are manipulated by the group of computers. There is no centralized authority. The information in the blocks can be viewed by anyone.

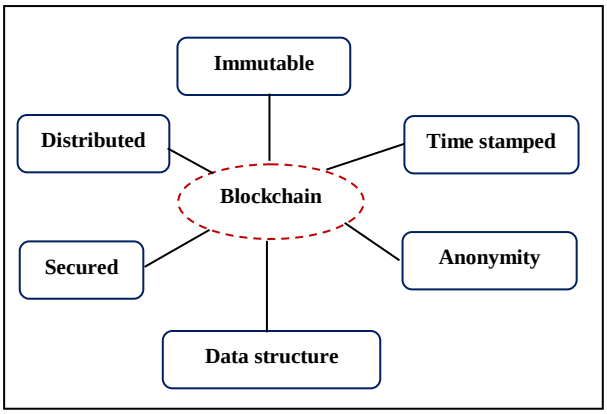

Figure 1 : Characteristics of Blockchain technology

- Immutable means the content cannot be changed. The data in the block cannot be altered. Once a block of information is stored on blockchain, it cannot change.
- There is no centralized server to manage the functionality of the blockchain. It uses special type of network referred as peer-peer network.
- The timestamp in blockchain is mainly used for verification purpose. A timestamp is referred as “Proof of existence”. Any digital data can be timestamped.

- Cryptography hash plays a major role in blockchain technology. It maintains the data integrity in blockchain.
- Transactions on the blockchain are not completely anonymous, personal information about users is limited to their digital signature or username.
- The basic data structures used in blockchain technology are linked list, Balanced tree and Hashing.

2 DATA STRUCTURES

Data structures are used to store and organize the data. The data structures are main classified into linear and non-linear. The linear data structures are array, sta

ck, queue and linked list. The non-linear data structures are tree, graph and hash table.

The three main data structures concepts used in blockchain are linked list, Self-balanced binary tree and Hash table.

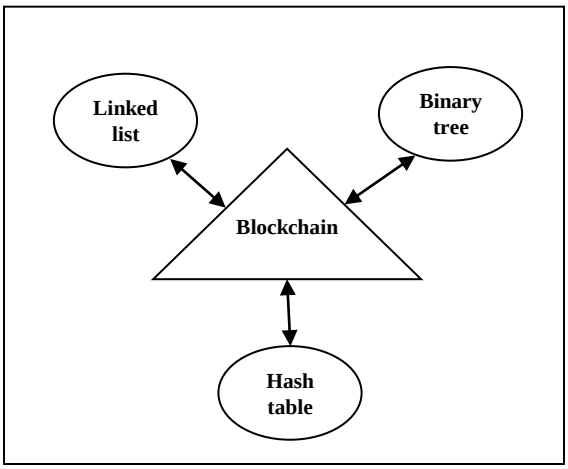

Figure 2: Data structures used in Blcokchain

2.1 Linked List

Linked list is a collection of nodes each node consists of two fields such as data and link. The link field specifies the address of the next node. In single linked list the address of the last node is null.

In linked list a new node can be added or inserted anywhere. We can insert a new node in the middle, at the beginning or at the end of the linked list.

The two main variations between blockchain and linked list are :

a. In blockchain, the new blocks are added only at the end of the chain.

b. The blocks are connected through unique hash codes.

The operation of adding a new block in blockchain is similar to linked stack in which the insertions are take place at one end called as top. The blockchain does not support deletion operation.

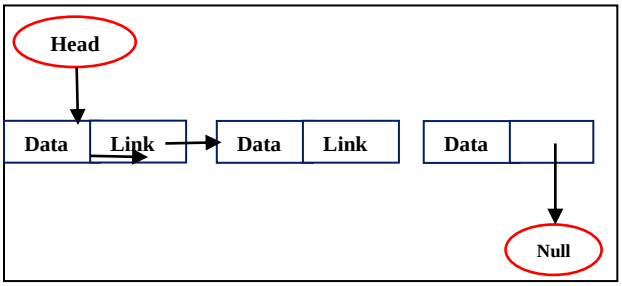

Figure 3: Single linked list

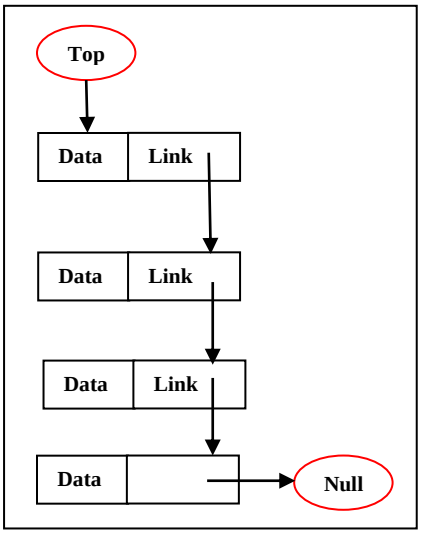

Figure 4: Linked stack

Blockchain is similar to linked stack in which insertions take place in one end. The changes in block and deletion of block are not allowed in blockchain technology.

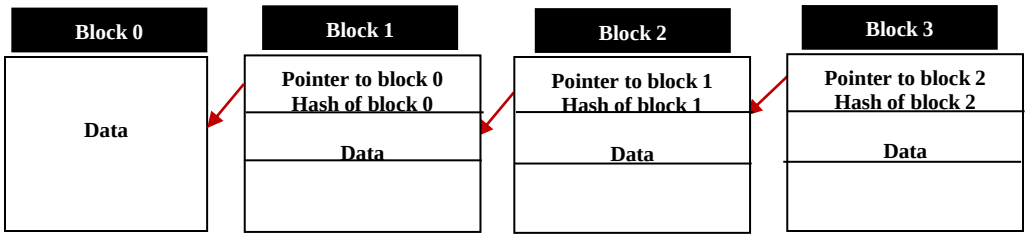

Figure 5: Blockchain

The hash stored in the hash pointer is the hash of the entire data of the previous block, which also includes the hash pointer to the block before that one. This makes it's impossible to alter a block in the blockchain without letting others know.

2.2 Binary tree

A Merkle tree is a non-linear, binary, hash tree data structure used for efficiently summarizing and proving the integrity of large sets of data.

In Merkle tree, each node having 0, 1 or 2 children. This property implies Merkle tree is a binary tree. Each leaf node represents Hash of block of data, the non-leaf node represents Hash of its children nodes. All the leaf nodes are at the same level of depth.

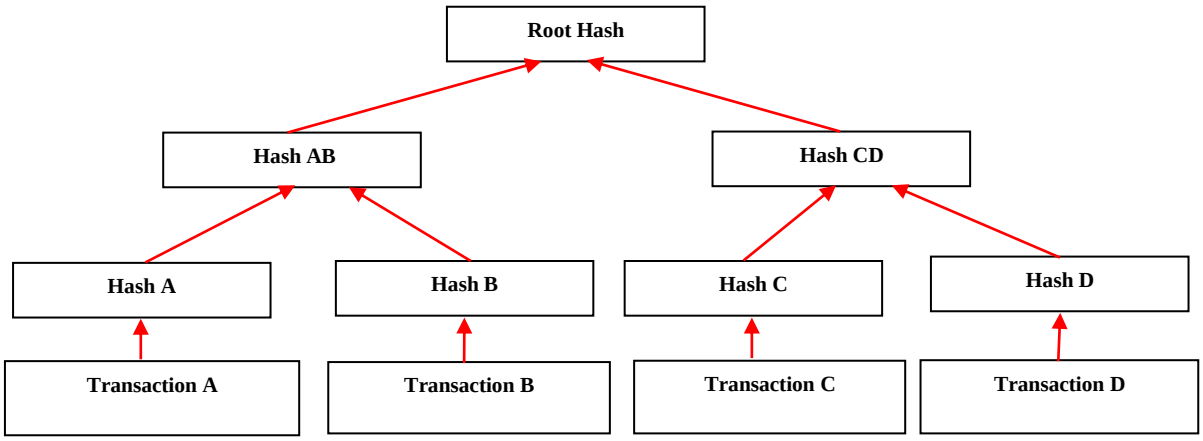

Figure 6: Merkle tree

Merkle tree should consist of even number of leaf nodes. If the number of transactions are odd, the last transaction is duplicated to make even number of leaf nodes. The Merkle tree occupies less amount of memory or disk space. It is computationally easy and fast. The main advantage of Merkle tree is that part of the data set can be verified without the need of full data set.

Merkle tree is a directed acyclic graph. These are graphs that contain no cyclic dependencies meaning it is always possible to calculate an acyclic path to the root of the graph. They are directed, meaning nodes have a parent/child relationship.

2.3 Hash table

The blocks in the blockchain are uniquely identified by the hash value. The hash value is calculated using SHA-256 algorithm. SHA is a Secured Hash Algorithm. Cryptographic hash function are mathematical function applied on digital data.

Figure 7: Hashing

The output of this algorithm is fixed length string with the size of 32 bytes. The main purpose of hashing in blockchain technology is easy identification and verification of integrity.

Properties of hash function

a. Hash function is deterministic. For any given input, a hash function produces same output.

b. The output of a cryptographic hash function must not expose any information about the input. This is called pre-image resistance.

c. Hash function is collision resistance that is two different input never hashes into same output.

The use of hash function is to identify the block in the large set of blocks. The hash table consists of blockchain transactions and their corresponding hash values. The hash table reduces the search time of the particular block in the blockchain.

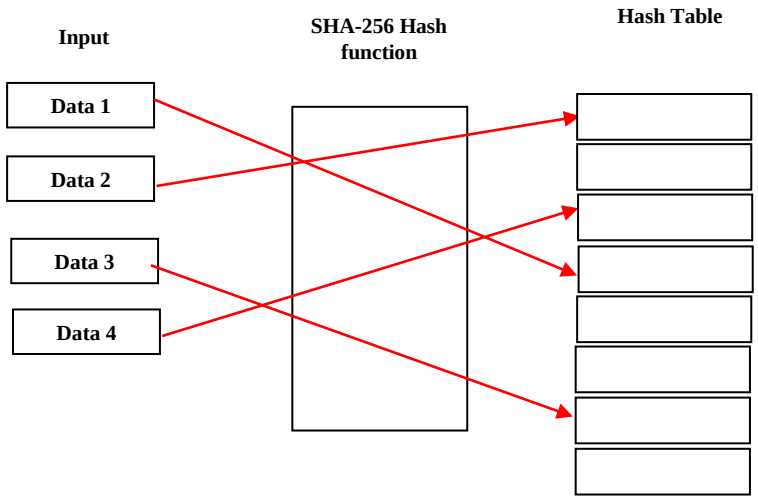

Figure 8: Blockchain with Hash table

The hash values are used as index in memory or disk to access the particular block.

A special type of hash table Distributed Hash Table(DHT) can also be used in blockchain technology. In this blockchain the block can be accessed by all the peers. Each block and transaction are replicated in the DHT of the peers.

3 CONCLUSION

This paper explains how the basic data structures concepts are integrated in blockchain technology. This is helpful to the beginners for the better understanding of blockchain technology. It is an emerging technology with a wide range of applications. Since the better understanding of the core concepts of blockchain, a reader can innovate many new ideas and applications in the future.

REFERENCES

[1] *Yahya Hassanzadeh-Nazarabadi, Alptekin K¨up¸c¨u, and Oznur ¨ Ozkasap, LightChain: A DHT-based Blockchain for Resource Constrained Environments. pp. 1-46.*

[2] *Xiaojing Yang et al, Research and Analysis of Blockchain Data, Journal of Physics: Conference Series. pp 1-8.*

[3] *Alan G. Labouseur, Matthew Johnson, Thomas Magnusson, Demystifying Blockchain by Teaching It in Computer Science∗ Adventures in Essence, Accidents, and Data Structures.*

[4] *Zibin Zheng, Shaoan Xie1, Hongning Dai, Xiangping Chen, and Huaimin Wang, An overview of Blockchain technology: Architecture, Consensus and Future trends.*

[5] *Min Xu, Xingtong Chen, Gang Kou, A Systematic review of Blockchain Technology.*