Data Structure

Merkle tree is a data structure which is used for storing the transactions of a block in Bitcoin blockchain. Merkle tree stores hash of a data in its leaf. Then, each leaf will be hashed together with its neighbor to create the parent hash node in the tree, and this process will be continued until the root of the tree. Thus, we have a hash root on top of the tree. This hash root is used mainly for verifying the stored data and preventing any modification of data in the network.

Bitcoin uses this characteristic to secure stored transactions and prevent unknown users from altering transactions. Because, any modification in each part of the transactions will change the hash of the node and consequently will alter the hash root of the tree which can be visible to other nodes verifying the blocks.

There are also other data structures that can be used for storing data in a secure and optimized space manner with providing easy ways of looking up data. One of these structures is Patricia tree which is a special case of radix trees. Radix tree is a data structure that is used mainly for storing the data in a more compressed way. In this kind of tree, each node which has a single child will be merged with it. Patricia is also a special case of this tree. It provides a cryptographically authenticated data structure which is used to store key-value bindings.

At the end, the characteristics of these data structures can be used for storing data in blockchain. All of the Merkle tries in Ethereum use a Merkle Patricia Trie. The Ethereum implementation of this data structure has some benefits. First, it makes the tree cryptographically secure because each node is referenced by its hash. Second, the hash of the node can be used for looking up that node in the tree. Finally, each branch has a specified depth and, in its leaf, the stored value can be found.