208077

CSC 341: DATA STRUCTURES

ASSIGNMENT: Discuss briefly on Blockchain Technology

A blockchain is “a distributed database that maintains a continuously growing list of ordered records, called blocks.” These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.” Blockchain was invented by Satoshi Nakamoto.

Blockchain can be used for for payment processing and money transfers, digital IDs, data sharing, copyright and royalties, Internet of Things network management and for healthcare. The primary benefit of blockchain is as a database for recording transactions, but its benefits extend far beyond those of a traditional database. Most notably, it removes the possibility of tampering by a malicious actor, as well as time savings. Blockchain slashes transaction times from days to minutes. Transaction settlement is faster because it doesn’t require verification by a central authority. Cost savings because, transactions need less oversight. Participants can exchange items of value directly. Blockchain eliminates duplication of effort because participants have access to a shared ledger. It also provides tighter security because blockchain’s security features protect against tampering, fraud, and cybercrime.

Data Structure of Blockchain Technology

The blockchain data structure is an ordered, back-linked list of blocks of transactions. A block is a package data structure. According to Bitcoin Book, a block is a container data structure that clusters transactions for incorporation in the public ledger known as the blockchain. The blockchain can be stored as a flat file, or in a simple database. The block is composed of a header that includes metadata, accompanied by a lengthy record of transactions that advance its size. A complete block, with all transactions, is almost 10,000 times greater than the block header. The block header is made up of metadata (Data about data).

The Bitcoin Core client stores the blockchain metadata using Google’s LevelDB database. Blocks are linked “back,” each referring to the previous block in the chain. The blockchain is often visualized as a vertical stack, with blocks layered on top of each other and the first block serving as the foundation of the stack. The visualization of blocks stacked on top of each other results in the use of terms such as “height” to refer to the distance from the first block, and “top” or “tip” to refer to the most recently added block.

Although a block has just one parent, it can temporarily have multiple children. Each of the children refers to the same block as its parent and contains the same (parent) hash in the “previous block hash” field. Multiple children arise during a blockchain “fork,” a temporary situation that occurs when different blocks are discovered almost simultaneously by different miners (see Blockchain Forks). Eventually, only one child block becomes part of the blockchain and the “fork” is resolved. Even though a block may have more than one child, each block can have only one parent. This is because a block has one single “previous block hash” field referencing its single parent.

The “previous block hash” field is inside the block header and thereby affects the current block’s hash. The child’s own identity changes if the parent’s identity changes. When the parent is modified in any way, the parent’s hash changes. The parent’s changed hash necessitates a change in the “previous block hash” pointer of the child. This in turn causes the child’s hash to change, which requires a change in the pointer of the grandchild, which in turn changes the grandchild, and so on. This cascade effect ensures that once a block has many generations following it, it cannot be changed without forcing a recalculation of all subsequent blocks. Because such a recalculation would require enormous computation, the existence of a long chain of blocks makes the blockchain’s deep history immutable, which is a key feature of bitcoin’s security.

Merkle Trees

Each block in the bitcoin blockchain contains a summary of all the transactions in the block, using a merkle tree. A merkle tree, also known as a binary hash tree, is a data structure used for efficiently summarizing and verifying the integrity of large sets of data. Merkle trees are binary trees containing cryptographic hashes. The term “tree” is used in computer science to describe a branching data structure, but these trees are usually displayed upside down with the “root” at the top and the “leaves” at the bottom of a diagram.

Merkle trees are used in bitcoin to summarize all the transactions in a block, producing an overall digital fingerprint of the entire set of transactions, providing a very efficient process to verify whether a transaction is included in a block. A Merkle tree is constructed by recursively hashing pairs of nodes until there is only one hash, called the root, or merkle root. The cryptographic hash algorithm used in bitcoin’s merkle trees is SHA256 applied twice, also known as double-SHA256.

When N data elements are hashed and summarized in a merkle tree, you can check to see if any one data element is included in the tree with at most 2*log2(N) calculations, making this a very efficient data structure.

Merkle trees are used extensively by SPV nodes. SPV nodes don’t have all transactions and do not download full blocks, just block headers. In order to verify that a transaction is included in a block, without having to download all the transactions in the block, they use an authentication path, or merkle path.

Features of Blockchain Technology

1. **Decentralization**

Decentralization in blockchain refers to transferring control and decision making from a centralized entity (individual, organization, or group) to a distributed network. Decentralized blockchain networks use transparency to reduce the need for trust among participants. These networks also deter participants from exerting authority or control over one another in ways that degrade the functionality of the network.

2. Immutability

Immutability means something cannot be changed or altered. No participant can tamper with a transaction once someone has recorded it to the shared ledger. If a transaction record includes an error, you must add a new transaction to reverse the mistake, and both transactions are visible to the network.

3. Consensus

A blockchain system establishes rules about participant consent for recording transactions. You can record new transactions only when the majority of participants in the network give their consent.

Key components of Blockchain Technology

A distributed ledger

A distributed ledger is the shared database in the blockchain network that stores the transactions, such as a shared file that everyone in the team can edit. In most shared text editors, anyone with editing rights can delete the entire file. However, distributed ledger technologies have strict rules about who can edit and how to edit. You cannot delete entries once they have been recorded.

Smart contracts

Companies use smart contracts to self-manage business contracts without the need for an assisting third party. They are programs stored on the blockchain system that run automatically when predetermined conditions are met. They run if-then checks so that transactions can be completed confidently. For example, a logistics company can have a smart contract that automatically makes payment once goods have arrived at the port.

Public key cryptography

Public key cryptography is a security feature to uniquely identify participants in the blockchain network. This mechanism generates two sets of keys for network members. One key is a public key that is common to everyone in the network. The other is a private key that is unique to every member. The private and public keys work together to unlock the data in the ledger.