**Block chain**

Block-chain network is a string of blocks that holds transactional records through distributed ledgers like public ledgers. In recent years, digitalize ledgers have been used to store data with centralized ownership, but block-chain technology introduces a distributed and decentralized way to store data records. The first block in a block sequence is named genesis block. From the second block onwards, each block holds the hash value of the previous block and hence the sequence of blocks is created.

The block data consists of transactions and transaction numerators. An encrypted version of transactions is stored in each block. The encryption of data happens by Merkle tree algorithm. Transactions go into the hash function and then hash value is produced. Next, each of the two-hash value of each transaction forms a pair and go into another hash function to prepare a new hash value. This action continues until reaching one hash value. This procedure is called Merkle tree root hash and is represented in Figure 1.

# 

Fig. 1. Merkle Tree Root Hash

Algorithm explanation

A block-chain algorithm operates as a decentralized and distributed ledger that records transactions across multiple computers. Each transaction is grouped into a block, which is then linked to the previous block using cryptographic hashes, ensuring data integrity and security while preventing tampering. The algorithm follows these key steps:

**1. Transaction Submission**

Users initiate transactions by sending data to the block-chain application.These transactions are then broadcasted to all nodes in the network for processing.

**2. Transaction Verification**

Each node independently verifies the transaction to ensure it meets the network's criteria, such as checking for sufficient funds and validating the sender's identity.This verification process helps prevent fraudulent activities and ensures that only legitimate transactions are processed.

**3. Block Creation**

Once transactions are verified, they are grouped together into a block.

Each block contains essential information, including a timestamp, a reference to the previous block's hash, and a unique hash generated from the block's contents.

**4. Mining Process (Proof of Work)**

To add the new block to the block-chain, nodes engage in a mining process where they compete to solve a complex mathematical problem.

This process is known as Proof of Work, where the first node to solve the problem gets to add the block to the chain and is rewarded for their effort.

**5. Consensus Mechanism**

The network reaches consensus on the validity of the new block through the mining process. Once consensus is achieved, the block is considered valid and ready to be added to the block-chain.

**6. Block Addition**

The validated block is appended to the existing block-chain, and the updated ledger is distributed to all nodes in the network.

This ensures that every participant has the latest version of the block-chain.

**7. Immutability and Security**

Each block is cryptographically linked to the previous block, creating a secure chain that is resistant to tampering.

If any data in a block is altered, the hash of that block changes, breaking the chain and alerting the network to potential fraud.

**8. Transaction Completion**

The transaction is now complete, and the updated state of the block-chain reflects the new transaction. All participants in the network can view the updated block-chain, ensuring transparency and trust among users.