# Day 5 Blockchain Notes

**What is a Blockchain Block?**

A block in a blockchain is a container for transaction data. It consists of a list of transactions, a timestamp, and a cryptographic hash that links it to the previous block. This structure ensures the integrity and immutability of the data.

**Example**: In Bitcoin, each block contains a list of Bitcoin transactions, a timestamp, and the hash of the previous block.

**Hash Functions and Merkle Trees:**

- **Hash Function**: A hash function is a cryptographic algorithm that converts input data into a fixed-size string. Even a small change in the input results in a completely different hash.

**Example**: Bitcoin uses the SHA-256 hash function to create unique identifiers for each transaction.

- **Merkle Trees**: A Merkle tree is a binary tree of hashes that allows efficient and secure verification of transaction data. The root of the tree is called the Merkle root and represents all the transactions in a block.

**Example**: In Bitcoin, a Merkle tree is used to summarize all the transactions in a block. The Merkle root is included in the block header, making it easy to verify the integrity of the transactions.

**Nonce and Proof of Work:**

A nonce is a random number that miners use to find a valid block hash. In Proof of Work, miners

must guess the nonce that, when combined with the block's data, results in a hash that meets specific criteria.

**Example**: In Bitcoin, miners must find a nonce that produces a hash starting with a certain number of zeros. This process requires computational power and energy.

**Chain Formation and Security:**

Blockchain forms a chain by linking each block to the previous one using its hash. This structure makes it nearly impossible to alter any data in the blockchain, ensuring the integrity and security of the system.

**Example**: If someone tries to change a transaction in an old block, its hash will change, breaking the chain. This would immediately be detected by other miners, ensuring the blockchain's security.