PostLab:-

How Bitcoin Employs SHA-256

Bitcoin uses the **SHA-256 hashing algorithm** in two main ways:

1. **Mining (Proof of Work)**: Bitcoin miners compete to solve a cryptographic puzzle by finding a hash that is lower than a specified target. They repeatedly hash block data (which includes transaction information and a nonce) using SHA-256 until they find a hash that meets the network's difficulty requirements. The first miner to find a valid hash wins the right to add the block to the blockchain and receive the block reward.

2. **Address Creation**: Bitcoin uses SHA-256 as part of the process to generate Bitcoin addresses. A public key is hashed first using SHA-256 and then hashed again using RIPEMD-160 to create the address.

These uses of SHA-256 ensure the integrity and security of the Bitcoin network.