PRACTICAL 3

Name:	Harsh Shah	**Roll No.:**	21BCP359
Division:	6	**Batch:**	G11
Aim:	Exploring tools to understand the architecture of Blockchain.		

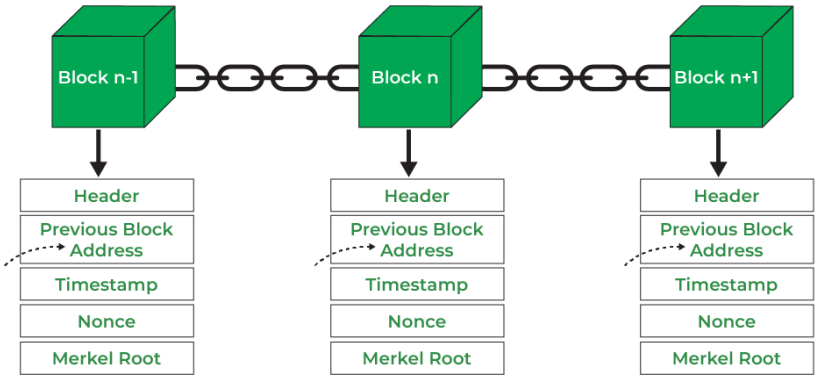
Block

A block in a blockchain is a digital record of transactions or data. Each block contains a list of transactions that have occurred within a specific period. The block also includes a reference to the previous block in the chain, creating a chronological order. This reference is typically a cryptographic hash of the previous block's contents.

Blockchain

Blockchain is a decentralized digital ledger that records and tracks transactions and assets in a business network. It's a shared, immutable database that stores a continuously growing list of ordered records, called blocks, which are linked using cryptography.

Architecture of Blockchain



Components of Block

- **Block Header**: This contains metadata about the block, including:
- **Previous Block Hash**: A reference to the hash of the previous block in the chain.
- **Block Hash:** A unique identifier for the block generated by hashing the block header. This hash serves as the block's fingerprint and is used to link to the previous block, ensuring the chain's immutability.
- **Timestamp**: The time when the block was created.
- **Nonce**: A random number used in the mining process to ensure the hash meets certain conditions.

Demonstration

SHA256

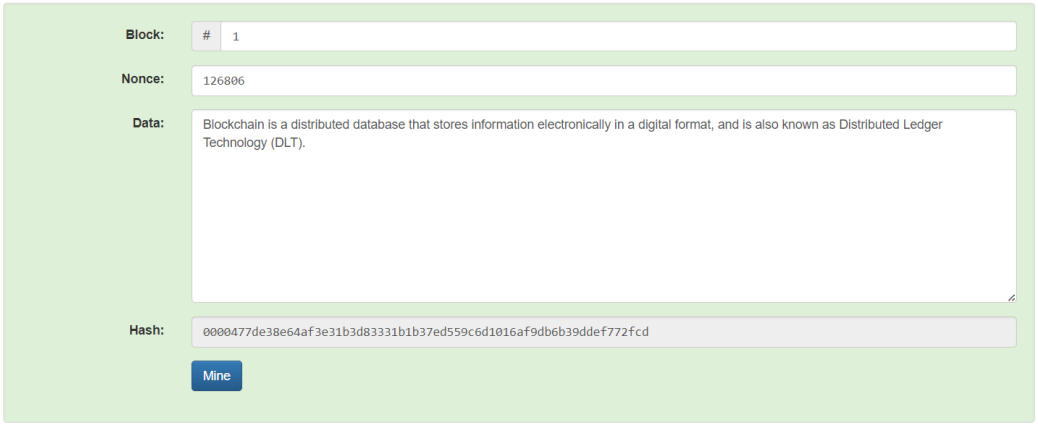
- SHA256 Hash for Empty Data

- SHA256 Hash for some data

Block

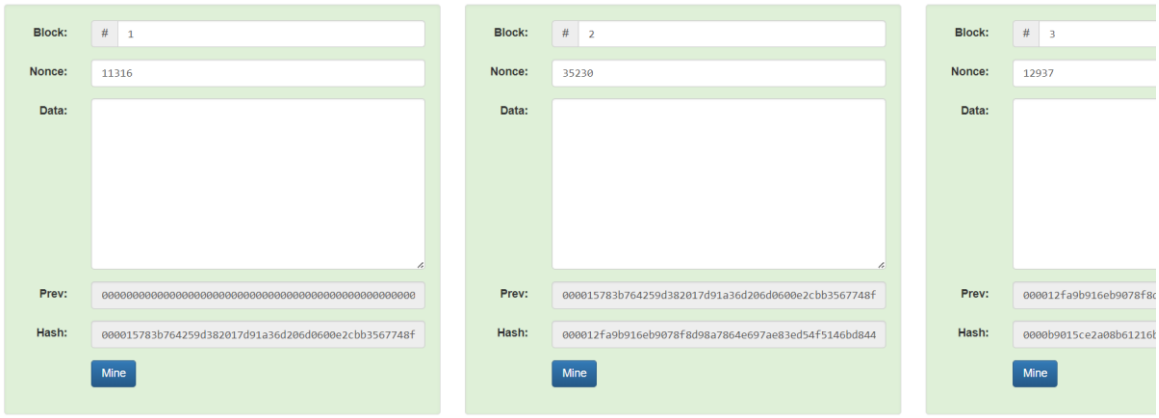
- Empty Block

- Block - 1 after Mining

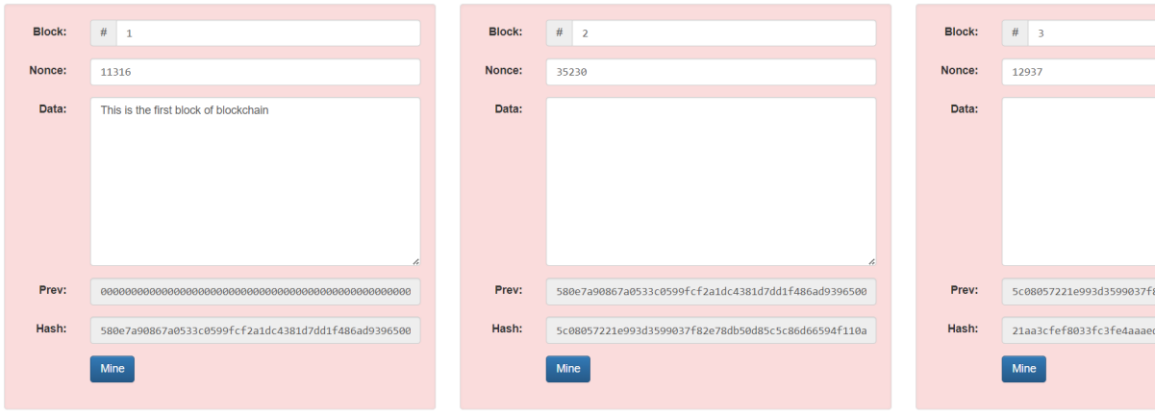


Blockchain

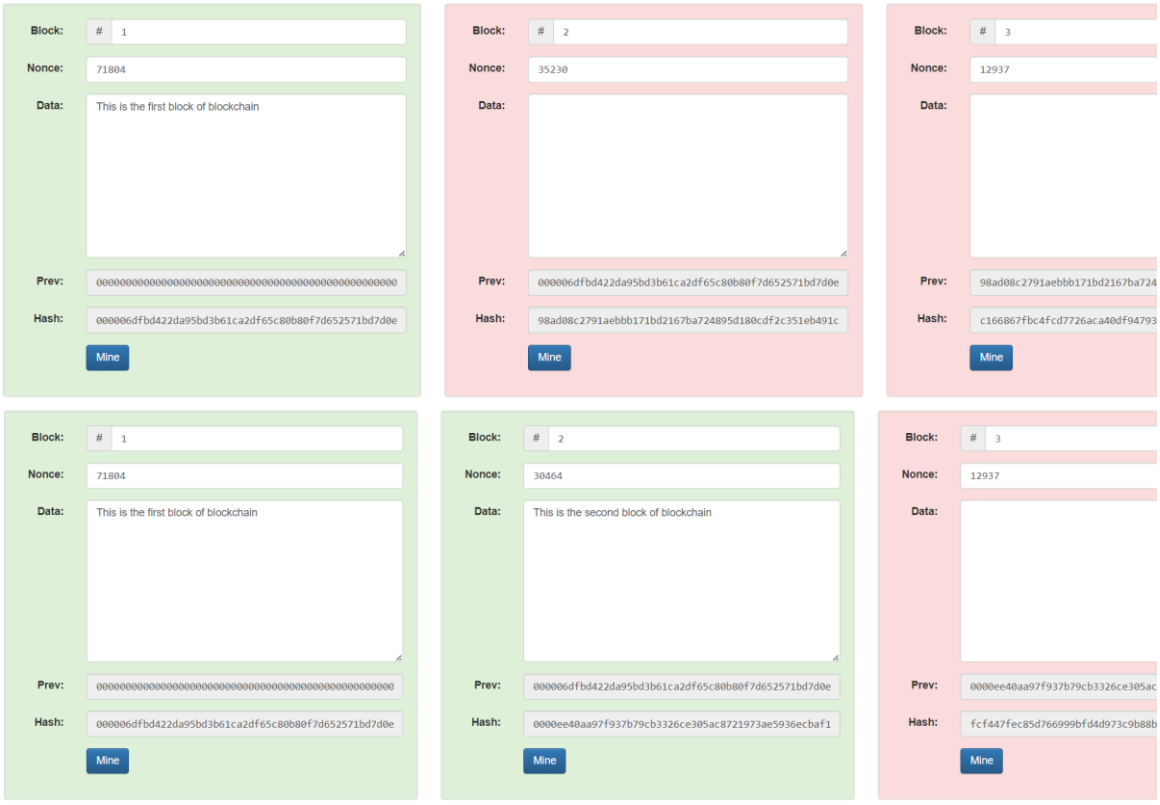
- Empty Blockchain



- Blockchain before Mining



- Blockchain after mining



Significance of Leading zeros in a hash

The leading zeros indicate the difficulty level set by the blockchain network. Miners must find a hash that meets this specific criterion. Miners repeatedly change the nonce (a random or semi-random number) and recompute the hash of the block until they find a hash that starts with the required number of leading zeros.

The network adjusts the difficulty level periodically (e.g., every 2016 blocks in Bitcoin) to ensure that blocks are mined at a consistent rate, typically every 10 minutes. This adjustment is achieved by increasing or decreasing the number of leading zeros required. The requirement for leading zeros makes it computationally expensive to find a valid hash, providing security to the network by making it difficult and resource-intensive to alter any previous blocks.

The process of finding a hash with the requisite number of leading zeros ensures that adding new blocks to the blockchain requires a significant amount of computational effort, thereby maintaining the integrity and security of the blockchain.