PRACTICAL 2

| Name:	Harsh Shah	Semester:	VII	Division:	6
Roll No.:	21BCP359	Date:	01-08-24	Batch:	G11
Aim:	To demonstrate blockchain technology using online tools.				

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
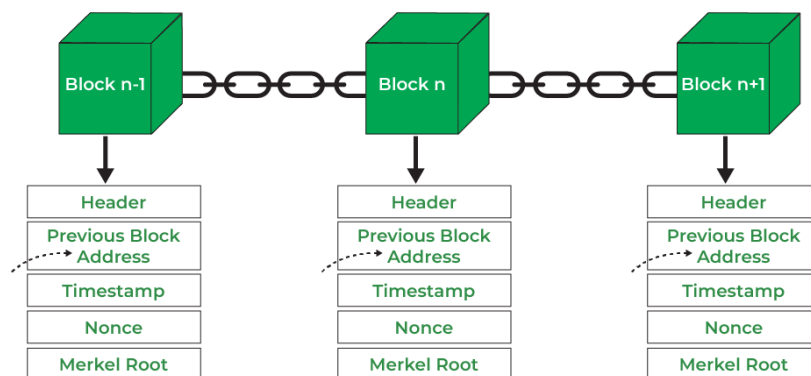
Components of Block

- **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

Data:	
Hash:	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

- SHA256 Hash for some data

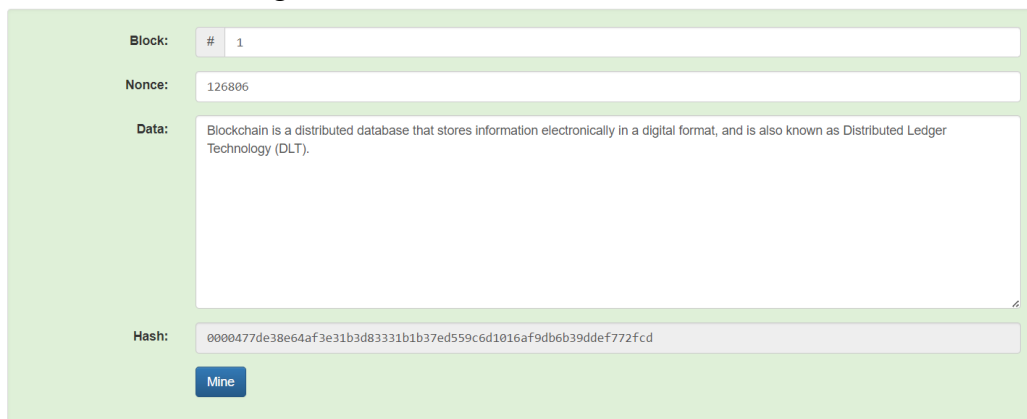|	
Data:	A block in a blockchain is a file that permanently stores transaction data. Blocks are the building blocks of a blockchain and are essential to its architecture.
Hash:	330d9159a86abc97b6934f253ff18b8759710b04571d1553992e3c1f7a768d3d

Block

- Empty Block

Block:	# 1
Nonce:	72608
Data:	
Hash:	0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a

Mine

- Block - 1 after Mining

Block:	# 1
Nonce:	126806
Data:	Blockchain is a distributed database that stores information electronically in a digital format, and is also known as Distributed Ledger Technology (DLT).
Hash:	0000477de38e64af3e31b3d83331b1b37ed559c6d1016af9db6b39ddef772fcd

Mine

Blockchain

- Empty Blockchain

Block:	# 1		Block:	# 2		Block:	# 3
Nonce:	11316		Nonce:	35230		Nonce:	12937
Data:			Data:			Data:	
Prev:	0000000000000000000000000000000000000000000000000000000000000000		Prev:	000015783b764259d382017d91a36d206d0600e2cbb3567748f		Prev:	000012fa9b916eb9078f8...
Hash:	000015783b764259d382017d91a36d206d0600e2cbb3567748f		Hash:	000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd844		Hash:	0000b9015ce2a08b61216...
Mine			Mine			Mine	

- Blockchain before Mining

Block:	# 1		Block:	# 2		Block:	# 3
Nonce:	11316		Nonce:	35230		Nonce:	12937
Data:	This is the first block of blockchain		Data:			Data:	
Prev:	0000000000000000000000000000000000000000000000000000000000000000		Prev:	580e7a90867a0533c0599fcf2a1dc4381d7dd1f486ad9396500		Prev:	5c08057221e993d3599037f8...
Hash:	580e7a90867a0533c0599fcf2a1dc4381d7dd1f486ad9396500		Hash:	5c08057221e993d3599037f82e78db50d85c5c86d66594f110a		Hash:	21aa3cfef8033fc3fe4aaaec...
Mine			Mine			Mine	

- Blockchain after mining

Block:	# 1		Block:	# 2		Block:	# 3
Nonce:	71804		Nonce:	35230		Nonce:	12937
Data:	This is the first block of blockchain		Data:			Data:	
Prev:	0000000000000000000000000000000000000000000000000000000000000000		Prev:	000006dfbd422da95bd3b61ca2df65c80b80f7d652571bd7d0e		Prev:	98ad08c2791aebbb171bd2167ba724...
Hash:	000006dfbd422da95bd3b61ca2df65c80b80f7d652571bd7d0e		Hash:	98ad08c2791aebbb171bd2167ba724895d180cdf2c351eb491c		Hash:	c166867fbc4fcd7726aca40df94793...
Mine			Mine			Mine	

Block:	# 1		Block:	# 2		Block:	# 3
Nonce:	71804		Nonce:	30464		Nonce:	12937
Data:	This is the first block of blockchain		Data:	This is the second block of blockchain		Data:	
Prev:	0000000000000000000000000000000000000000000000000000000000000000		Prev:	000006dfbd422da95bd3b61ca2df65c80b80f7d652571bd7d0e		Prev:	0000ee40aa97f937b79cb3326ce305ac...
Hash:	000006dfbd422da95bd3b61ca2df65c80b80f7d652571bd7d0e		Hash:	0000ee40aa97f937b79cb3326ce305ac8721973ae5936ecbaf1		Hash:	fcf447fec85d766999bfd4d973c9b88b...
Mine			Mine			Mine	

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.