Blockchain Technology Lab

Lab – 3

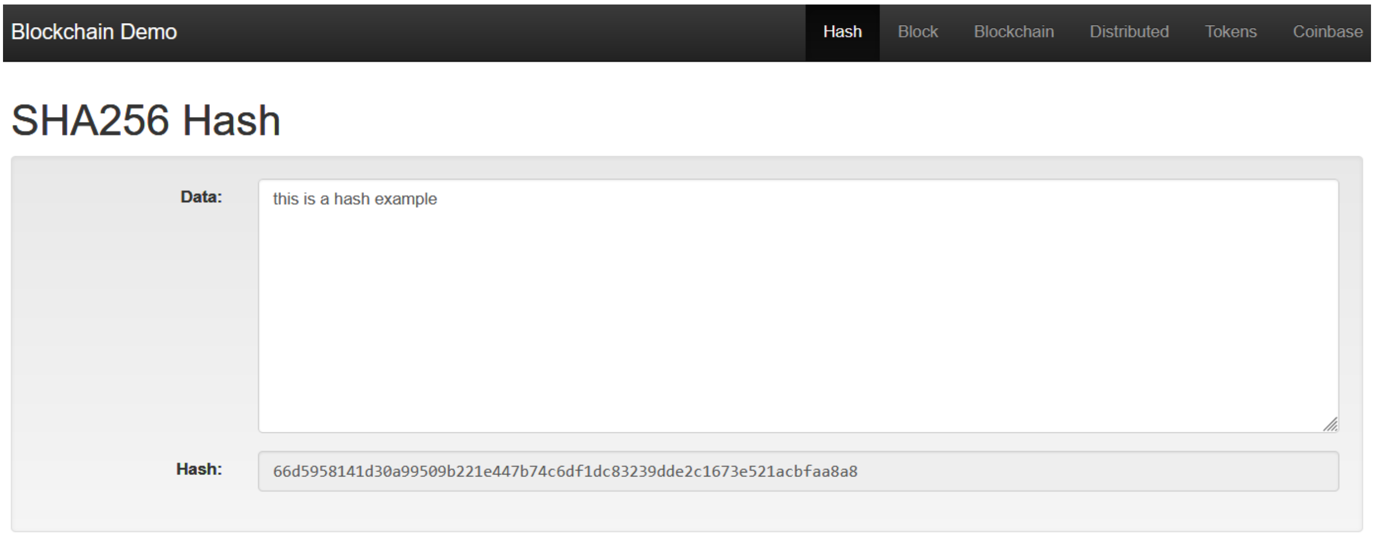
Aim : Explore a tool to learn the architecture of “Blockchain”.

Hash:

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that produces a fixed 256-bit hash value from any input. It is part of the SHA-2 family, designed by the NSA and published by NIST.

Key Characteristics:

- Fixed-Length Output: Always generates a 256-bit hash.
- Deterministic: Same input yields the same hash.
- Fast Computation: Efficiently computes hash values.
- Pre-image Resistance: Infeasible to reverse-engineer the input from the hash.
- Collision Resistance: Infeasible to find two different inputs with the same hash.



SHA256 Hash

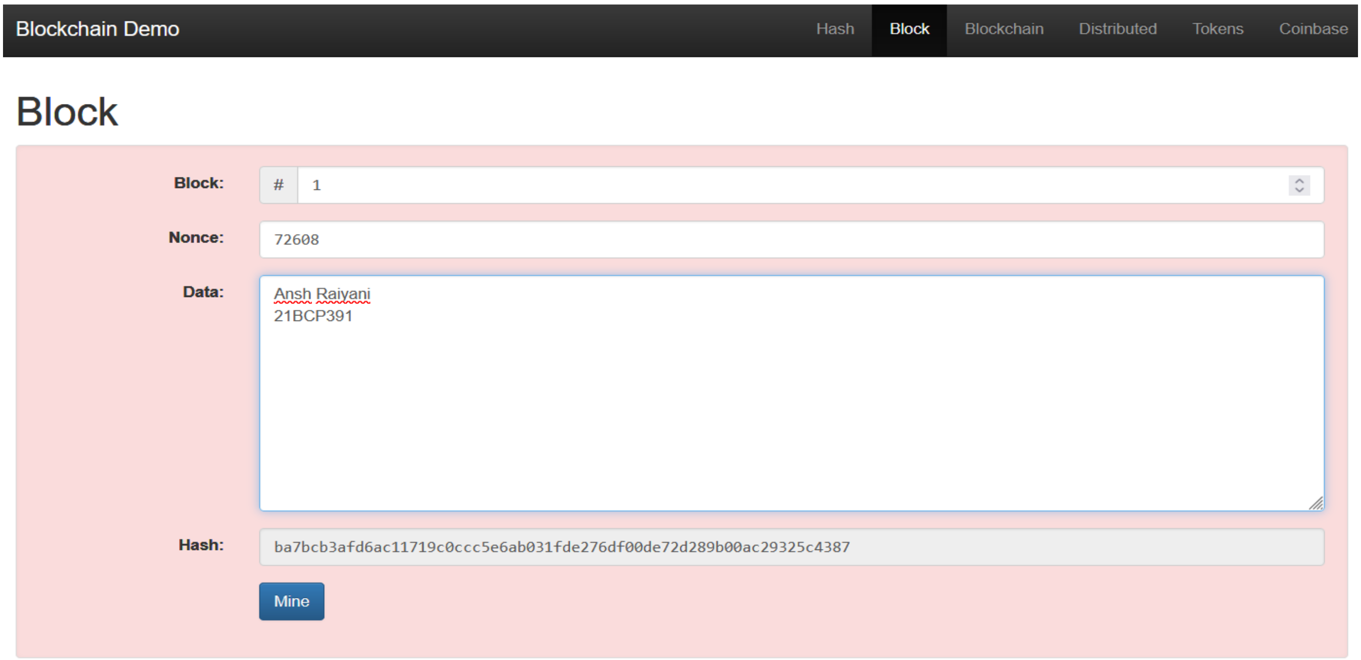
Data: this is a hash example

Hash: 66d5958141d30a99509b221e447b74c6df1dc83239dde2c1673e521acbfaa8a8

Block:

Basic Structure of Block:

1. Block Number: Unique identifier for every block.
2. Nonce: To make a block valid, we have to add a number called nonce to the input to create a hash that starts with 4 zeros. There is a consensus in a blockchain network that governs what is considered to be a valid hash. In the case of this example, a hash starting with 4 zero will be considered correct.
3. Data: This field contains the data stored in the block
4. Hash: The hash field shows the SHA-256 hash value of the block, which includes the block number, nonce, and data.



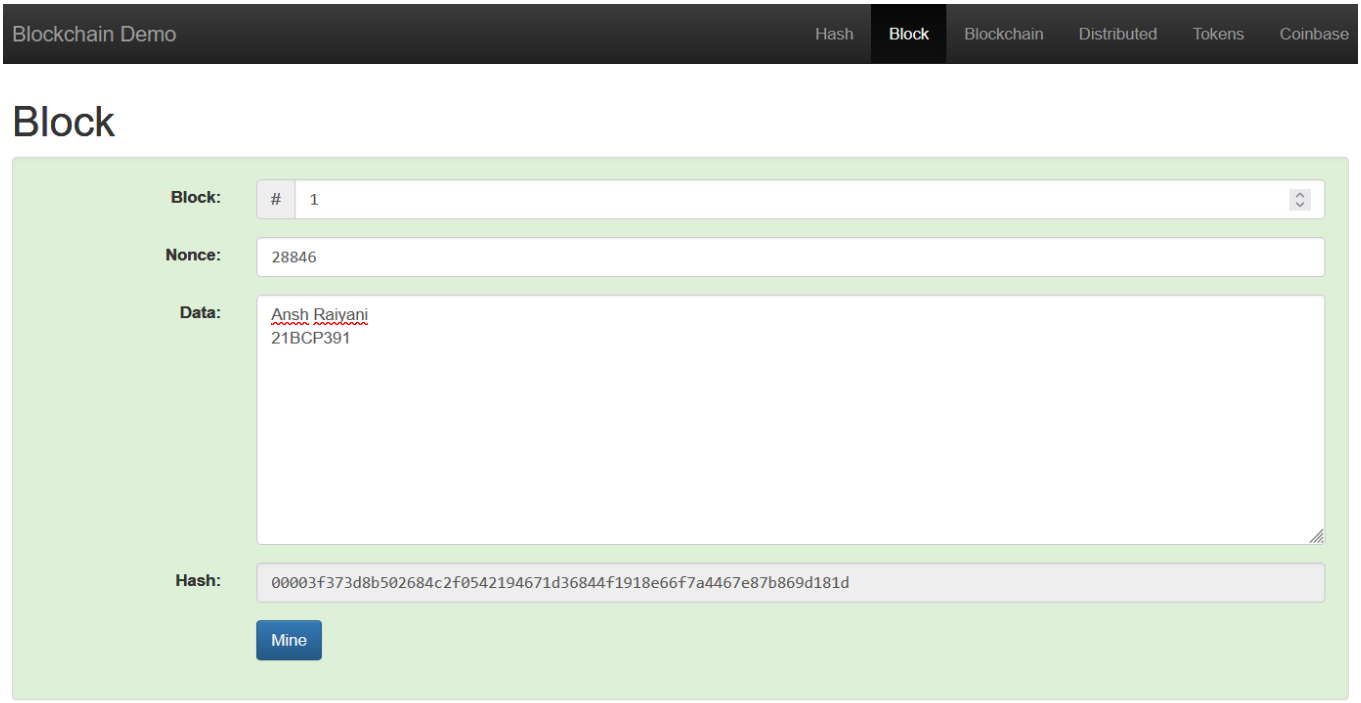
Block

Block: # 1

Nonce: 72608

Data: Ansh Raiyani
21BCP391

Hash: ba7bcb3afd6ac11719c0ccc5e6ab031fde276df00de72d289b00ac29325c4387



Block

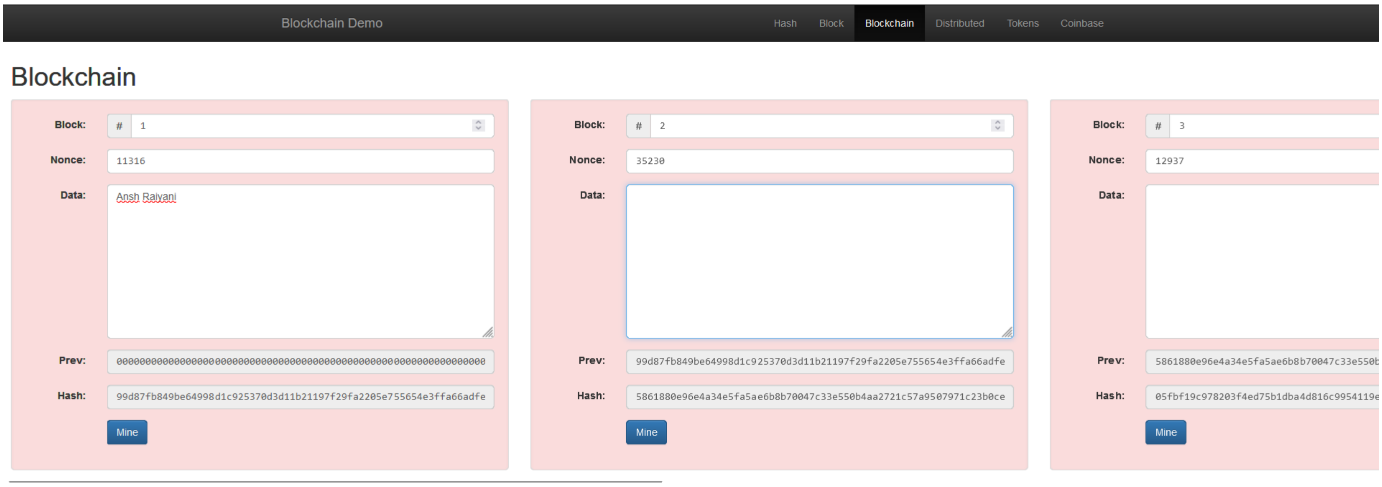
Block: # 1

Nonce: 28846

Data: Ansh Raiyani
21BCP391

Hash: 00003f373d8b502684c2f0542194671d36844f1918e66f7a4467e87b869d181d

Blockchain :



Blockchain

Block: # 1

Nonce: 11316

Data: Ansh Raiyani

Prev: 0000000000000000000000000000000000000000000000000000000000000000

Hash: 99d87fb849be64998d1c925370d3d11b21197f29fa2205e755654e3ffa66adfe

Block: # 2

Nonce: 35230

Data:

Prev: 99d87fb849be64998d1c925370d3d11b21197f29fa2205e755654e3ffa66adfe

Hash: 5861880e96e4a34e5fa5ae6b8b70047c33e550b4aa2721c57a9507971c23b0ce

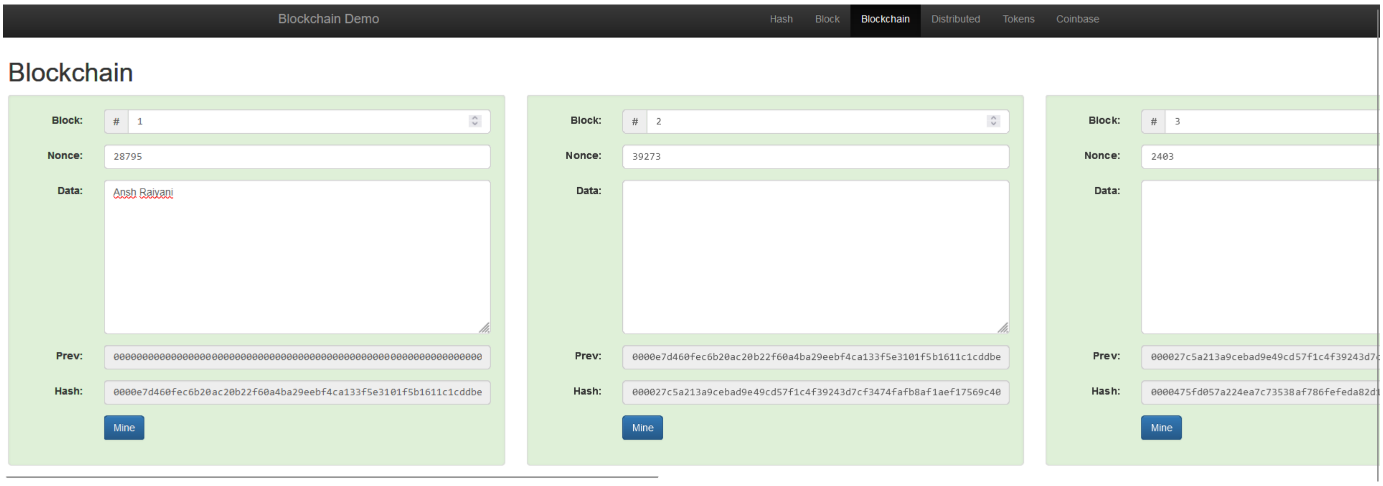
Block: # 3

Nonce: 12937

Data:

Prev: 5861880e96e4a34e5fa5ae6b8b70047c33e550b

Hash: 05fbf19c978203f4ed75b1dba4d816c9954119e



Blockchain

Block: # 1
Nonce: 28795
Data: Ansh Raiyani
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 0000e7d460fec6b20ac20b22f60a4ba29eebf4ca133f5e3101f5b1611c1cddbe

Block: # 2
Nonce: 39273
Data:
Prev: 0000e7d460fec6b20ac20b22f60a4ba29eebf4ca133f5e3101f5b1611c1cddbe
Hash: 000027c5a213a9cebad9e49cd57f1c4f39243d7cf3474fafb8af1aef17569c40

Block: # 3
Nonce: 2403
Data:
Prev: 000027c5a213a9cebad9e49cd57f1c4f39243d7
Hash: 0000475fd057a224ea7c73538af786fefeda82d

Why are there a certain number of zero's in the starting of the hash?

The leading zeros in a blockchain hash signify the difficulty level set by the network to maintain a consistent block generation time. The requirement for a hash to have a certain number of leading zeros is a way to enforce the difficulty target. A hash is simply a large number, and having more leading zeros means the hash value is smaller.

For example, a target requiring three leading zeros (e.g., `000xxxxxxxxxxxxxxxxxxxxxx`) is much harder to find than one with just one leading zero (e.g., `0xxxxxxxxxxxxxxxxxxxxxxxx`).