

Introduction to Ethereum Blockchain

By

Upendra Kumar Manve
(Engineering Manager at FRACSN)



Ethereum is an Open-source, public,
blockchain-based distributed computing
platform.

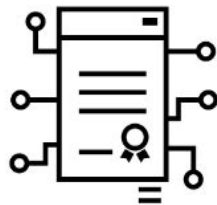


ETHER (ETH) is the currency to payout the miners and carryout operations on Ethereum platform.



Bitcoin Vs Ethereum

- Ethereum is Originally derived from Bitcoin.
- Bitcoin is a Digital Currency and Ethereum is World Computer.
- Bitcoin is used for storing value and pure exchange of money.
- Ethereum is used when some logical computations has to be done and can also be used for exchange of money.



Smart Contracts

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

One Way Hashing

And Its Importance in Blockchain

Hello World



SHA-256

b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

Hello World



SHA-256

Digest
Signature

b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

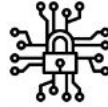


SHA-256

2d8c2f6d978ca21712b5f6de36c9d31fa8e96a4fa5d8ff8b0188dfb9e7c171bb

Length : 64

Hello World



SHA-256

b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

Hello world



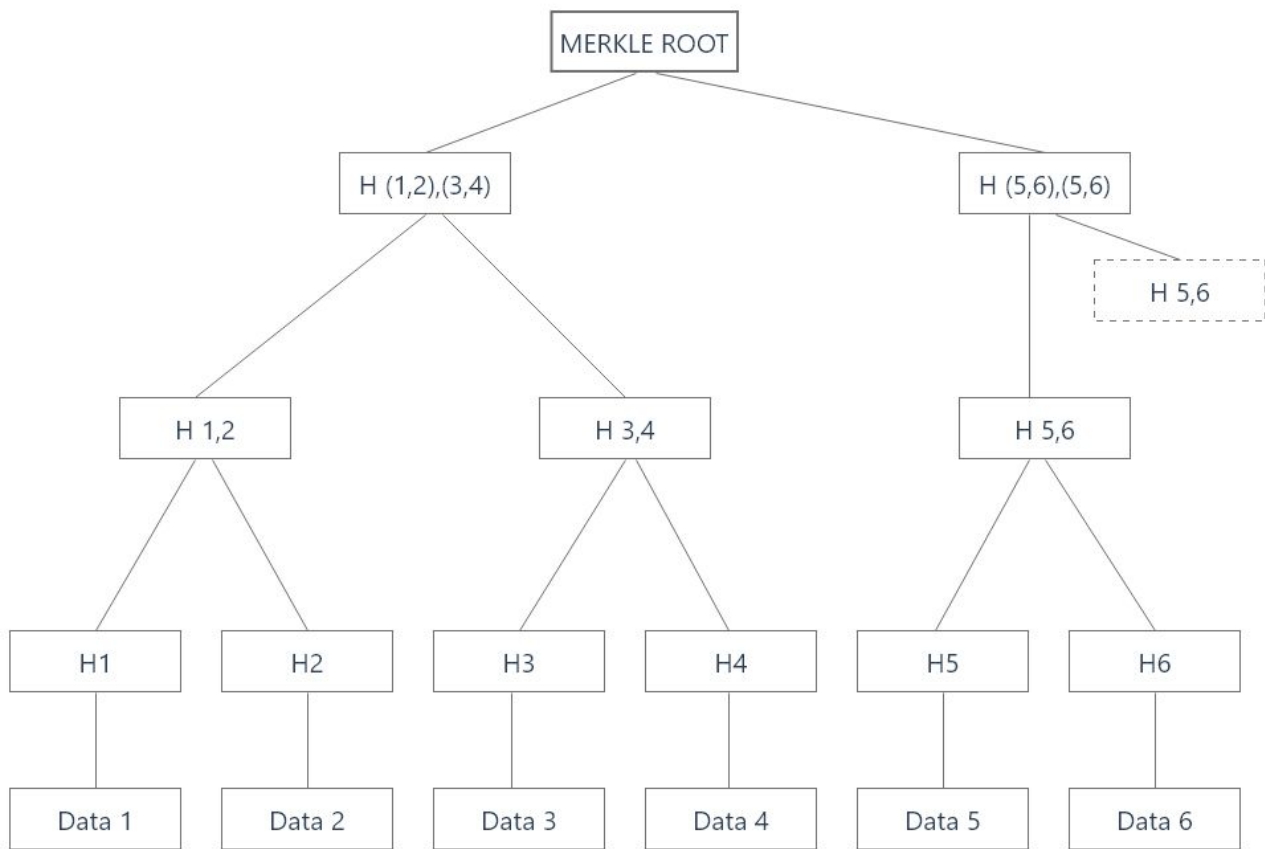
SHA-256

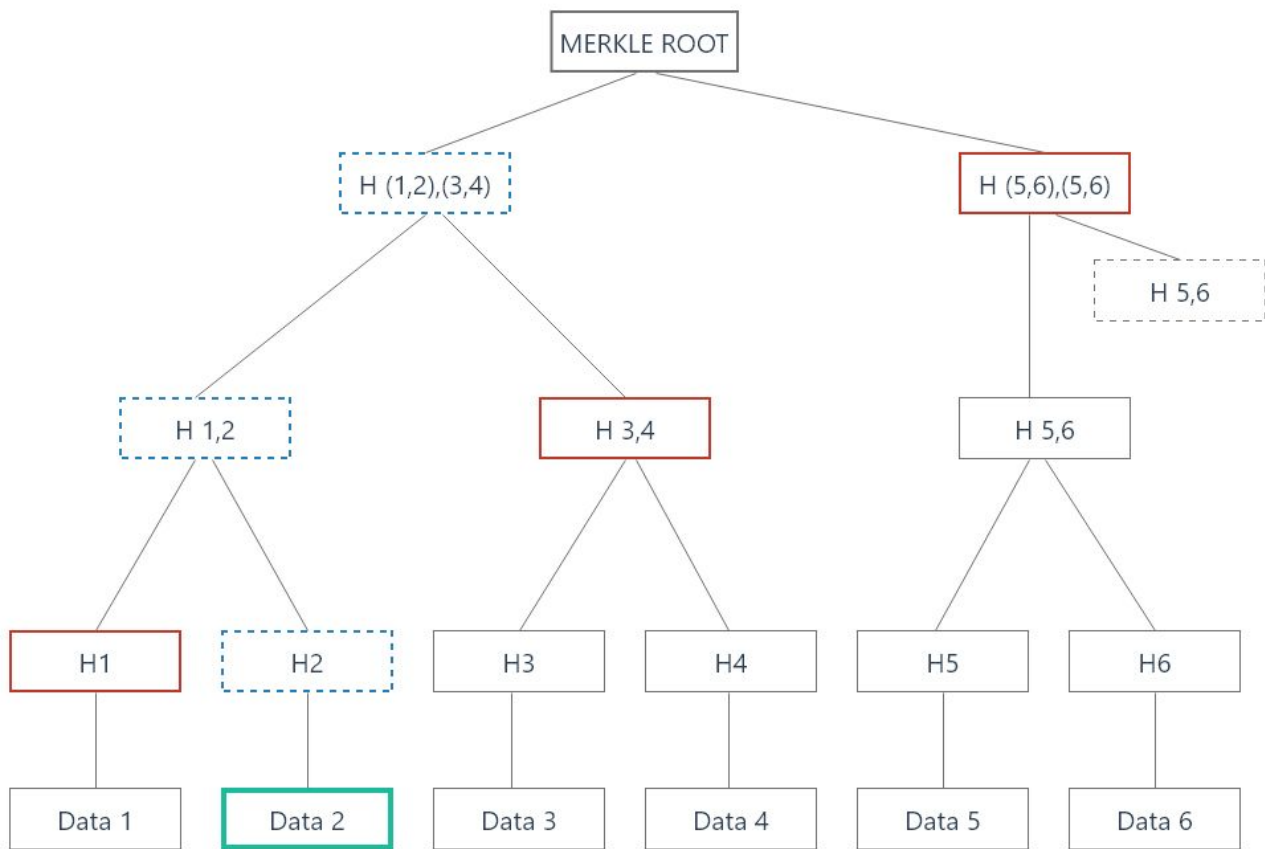
64ec88ca00b268e5ba1a35678a1b5316d212f4f366b2477232534a8aeca37f3c

Randomly
different

Merkle Tree

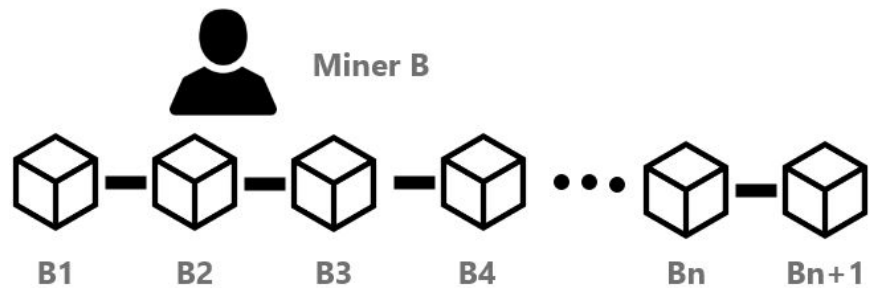
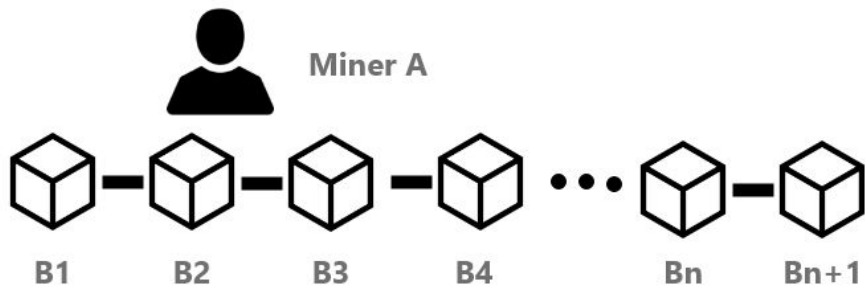
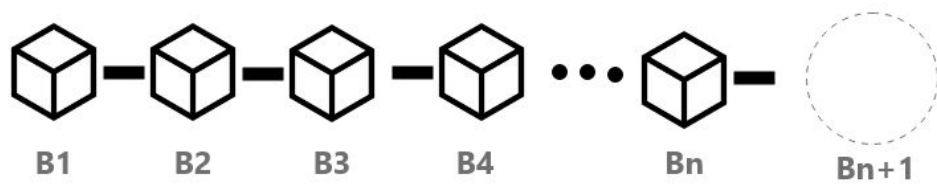
Merkle Proof

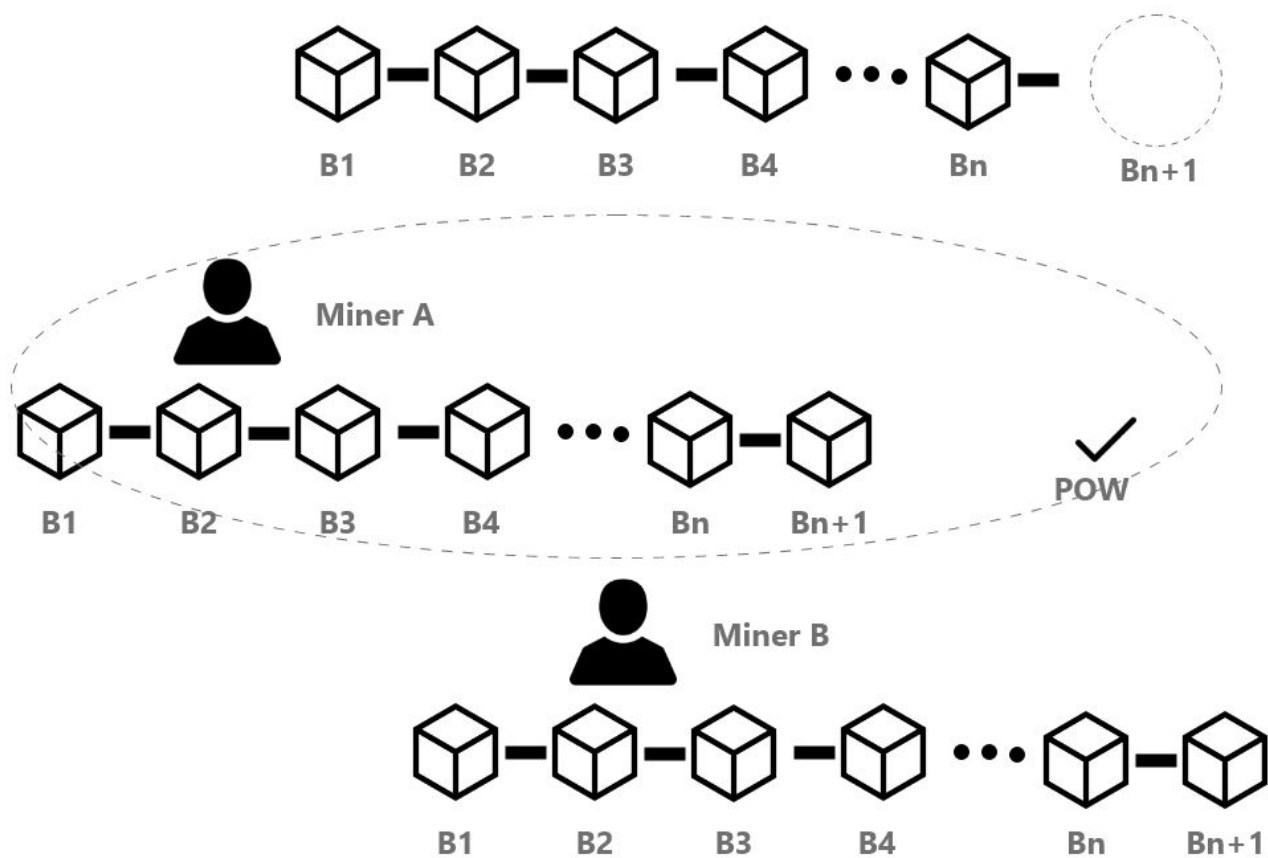




Consensus

Proof of Work Protocol





Mining Process

1. Group of Unconfirmed transaction are in transaction pool.
2. Miner picks the transaction which gives high reward and add to its Block.
3. Miner then solves the POW puzzle.
4. Once the puzzle is solved, he then Broadcasts it to the network.
5. Other miners validate and accepts or rejects the block.
6. Once accepted the miner receive reward and a new Block is successfully Mined.

BLOCK HEADER

Previous Block Hash

Merkle Root

Nonce

Nonce is the answer Miners are trying to Solve.

"CHALLENGE STRING"



BLOCK HASH



SHA256

Nonce: 5

```
0000xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

ETHEREUM BLOCK

ETHEREUM TRANSACTION

ACCOUNT TYPES

1. USER ACCOUNT

2. CONTRACT ACCOUNT

SMART CONTRACT 1

SIMPLE TOKEN CONTRACT

upendramanve@gmail.com

Ph: 9908293405

Whatsapp: 9032845139