BLOCKCHAIN | Batch 1 - Day 1 (Part 1 & Part 2) Overview

- Learning Path for Blockchain
- What is BlockChain?
- Normal DB vs Blockchain DB
- SHA - 256
- Steps of Creating Non-Updatable and Non-Deletable DB
- Blockchain in action with Peer

What is Blockchain?

- Internet is hackable
- Authenticity of the data which is uploaded?
- Tampering of the data once it is uploaded?

To Remove this all we need a system which stops the above-mentioned points, so to do that we are creating Blockchain.

In a technical way,

"A Blockchain is a constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure, Chronological and immutable way in Decentralized Distributed network"

Who is Satoshi Nakamoto?

Satoshi Nakamoto is the author of the white paper "Bitcoin: A peer to peer Electronic cash system"

As of now, no one knows who is Satoshi Nakamoto is or even if he is one person or a group of people

Why "Bitcoin: A peer to peer Electronic cash system"?

- We don't want any third party providing TRUST in the internet system
- We wish to make our own one connected system. So nice that we are fully able to trust the internet system itself
- To make a Financial system which can run by the end consumers itself, not by the bank people

Blockchain

A mix of Technology - Distributed Database & Cryptography where information is

- Verifiable
- Tamper-Proof
- Immutable

Verifiable

- You can check the data origin via blockchain Network

Tamper-Proof

- Even if you hack and change something. it will not change

Immutable

- The data stored in the Block is unchangeable

NORMAL DATABASE:-

A database is an organized collection of data, generally stored and accessed electronically from a computer system. create, read, update, and delete(CRUD) are the four basic functions of persistent storage.

CRUD vs Blockchain

In a traditional database, a client can perform four functions on data: Create, Read, Update, and Delete (collectively known as the CRUD commands).

The blockchain is designed to be an append-only structure. A user can only add more data, in the form of additional blocks. All previous data is permanently stored and cannot be altered. Therefore the only operations will be Create and Read.

Block

A block contains

- Block number
- Transaction Records
- Previous Block signature
- Mining key

Each and every block have a signature. That is called SHA-256

SHA - 256

The Sha-256 algorithm is based on the **Merkle-Damgard construction method**, according to which the initial index is divided into blocks immediately after the change is made, and those, in turn, into 16 words.

Blockchain in action with peers

- Block 1 => 0+B=C
- Block 2 => C+D=E
- Block 3 => E+F=G

B, D, F --> are data to be stored

C, E, G -->are the SHA(FP) Keys.