Blockchain

A - blockchain
B - cryptocurrency
C - smart contract

A - Blockchain

- What is Blockchain
- hashing Algorithm
- Immutable Ledger
- Distributed P2P Networks
- What is Mining?
- consensus Protocol

Why should I study Blockchain

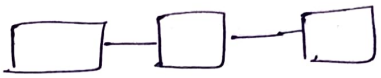
- Blockchain is a disruptive technology_
  - ↳ changes traditional tech. to new enhanced way
- Internet → communication
  Blockchain → Trust
  - e.g. NGO
    we donate money. Is NGO using our money properly used? i.e. can we verify.

What is Blockchain?

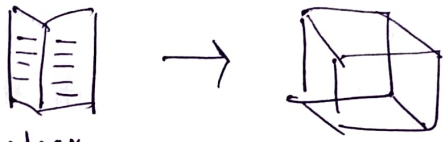
Idea :- (Research Paper)

Stuart Haber
W. Scott Stornetta

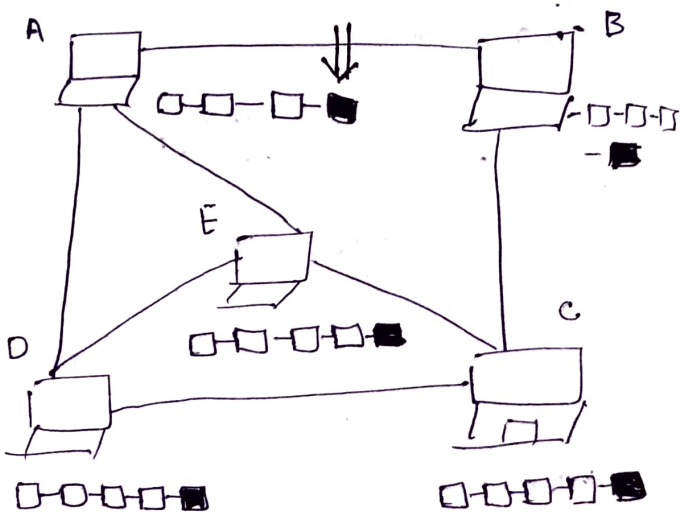
- Blockchain is a distributed immutable ledger. which is completely transparent.



e.g



Ledger Book → Block (The data noted in block can never erased)



If A makes any transcation that every computer connect to the blockchain will get updated. that's why It is known as distributed

Applications of Blockchain -1

(1) Product Tracking
(2) Healthcare System
(3) Smart Contracts
(4) International Wire Transfer

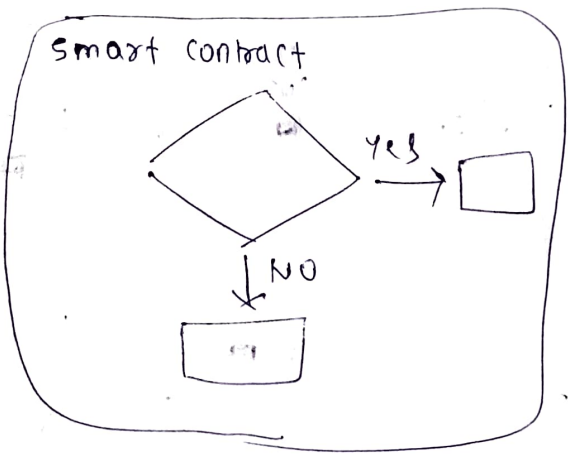
(1) Product Tracking

We can track product from origin → transfer →

e.g:- Denmark supermarket implement Blockchain.
Scan QR code you will get detailed information.

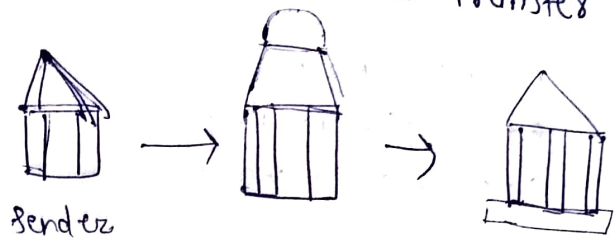
(2) Smart Contract

kind of program



Assuming a product gets accepted if temp. less than 30

(3) International Wire Transfer

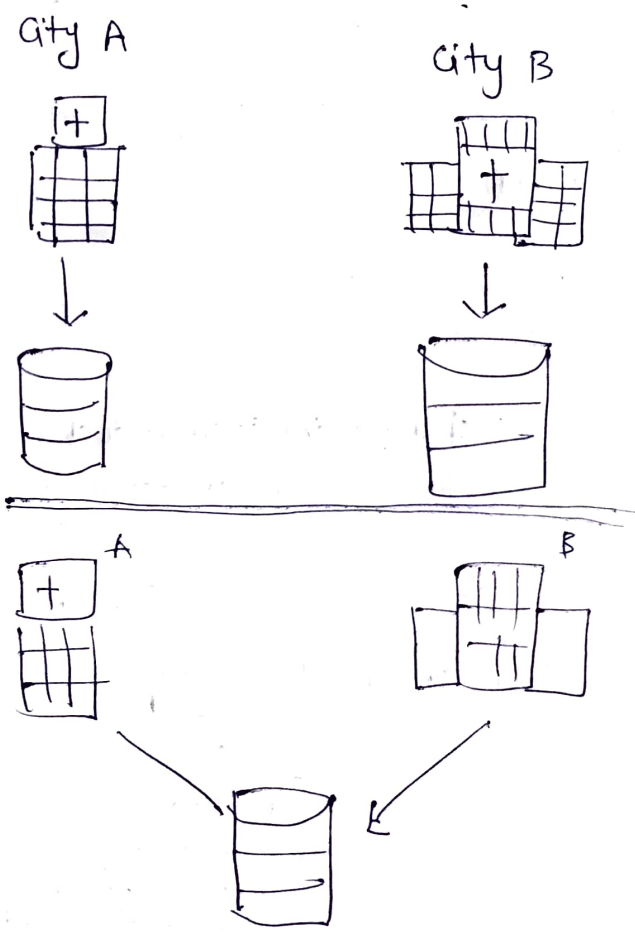


Disadvantages

- Huge fees
- Time Taking

Few Banks Adopting Blockchain
- JP Morgan

(4) Healthcare System



Applications of Blockchain - 2

(1) Transfer contracts and Wills

We are moving away from the days when contracts or wills were made on paper with different middlemen involved. Blockchain technology, paper wills, contracts, and inheritances may now be replaced with digital ones.

(2) Protection of copyright and royalties

Many copyright & ownership regulations on music, films, blogs, and other internet content are required in today's world. Blockchain technology can make these regulations more secure and easy to apply. It also provides content creators and artist with real-time & genuine royalty distribution statistics. Any type of digital material download might be traced to guarantee that artist or author gets their fair share.

(3) Voting

(4) Cryptocurrency

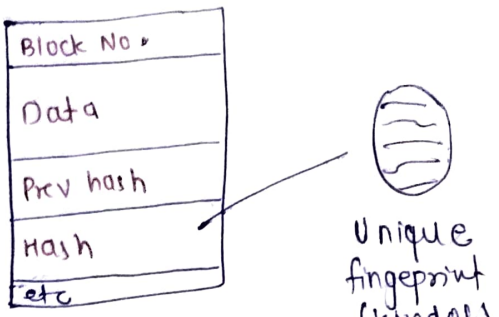
(5) Assest Administration

(6) Blockchain applications for anti-money laundering

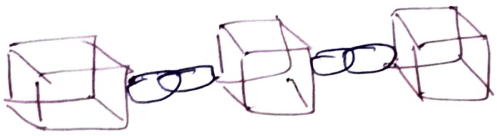
(7) Blockchain for Advertising

(8) Management of the Supply chain.

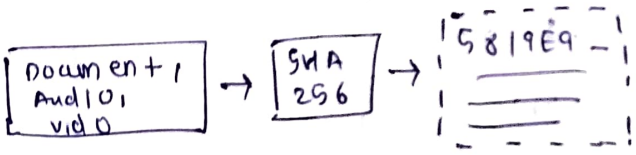
Hashing Algorithm



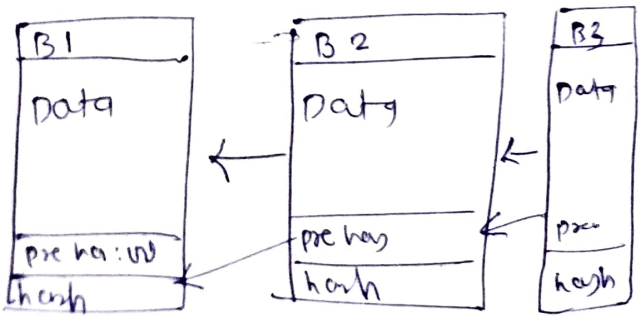
Block



Hash → SHA 256 Algo.
The hash is generated with the help of SHA 256 Algorithm



This has 64 hexadecimal characters. Each character is of 4 bits. So in total it has $64 \times 4 = 256$ bits



Genesis Block

Requirements of Hash Algo.

(1) one way Data → Encrypted Data (← ✗ Data)

(2) Deterministic

ABC → 845

(3) fast Computation

(4) Withstand Collisions

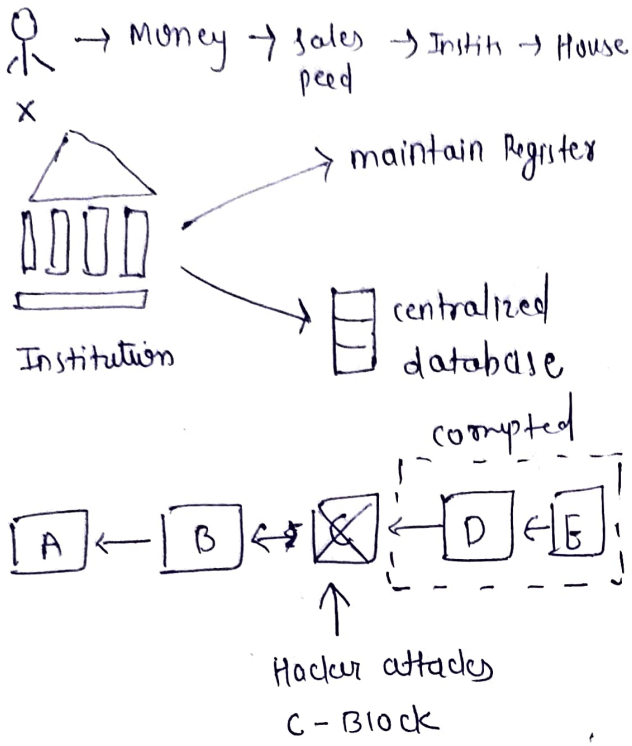
(5) Avalanche Effect

if any single value changed then SHA-256 value will be changed.

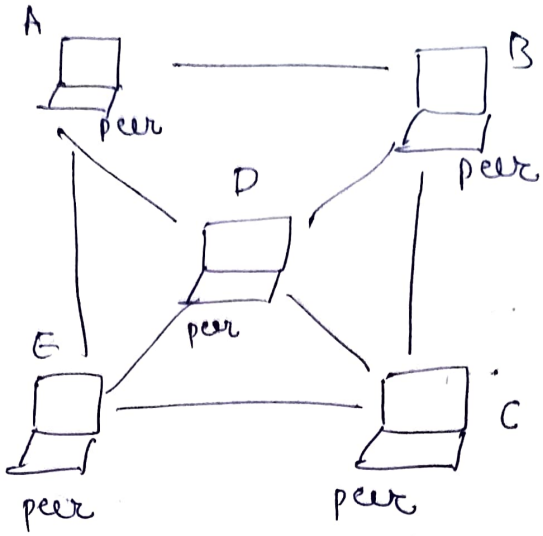
Practical :-

sha256-hash-generator

Immutable Ledger

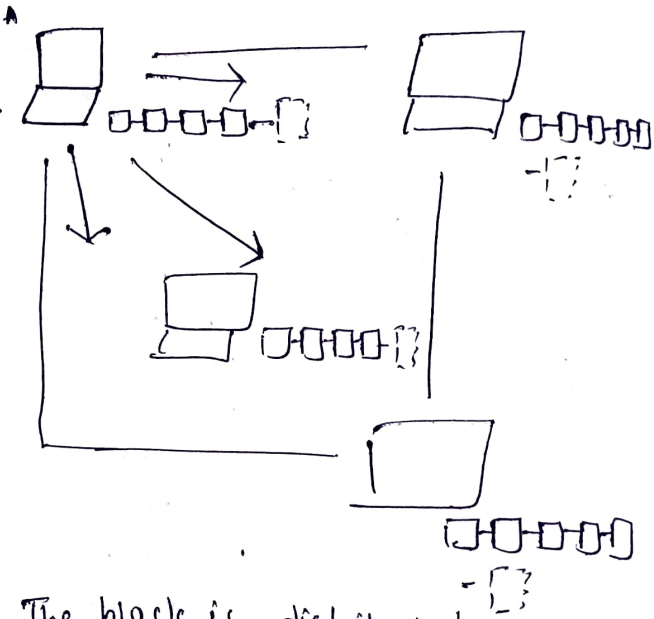


Distributed P2P network



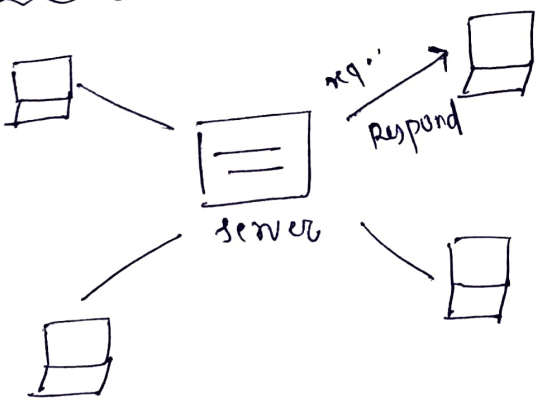
What is a P2P network?

- Blockchain works on P2P network

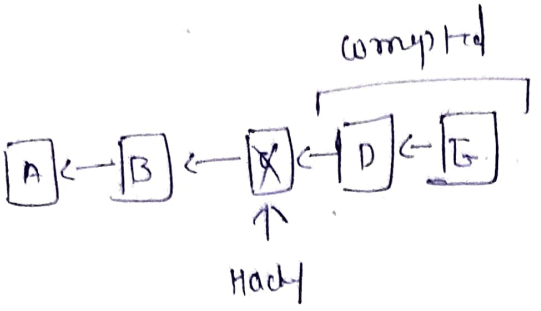


The block is distributed across the network.

centralized

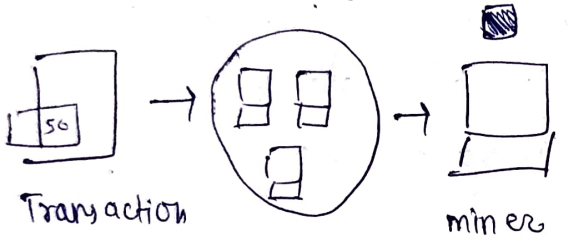


- We can recover our corrupted data



Blockchain Mining

Suppose we made a transaction using bitcoin

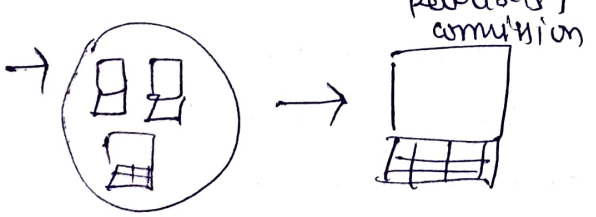


Transaction

miniers pick to Add to network or create block

miner solved problem first

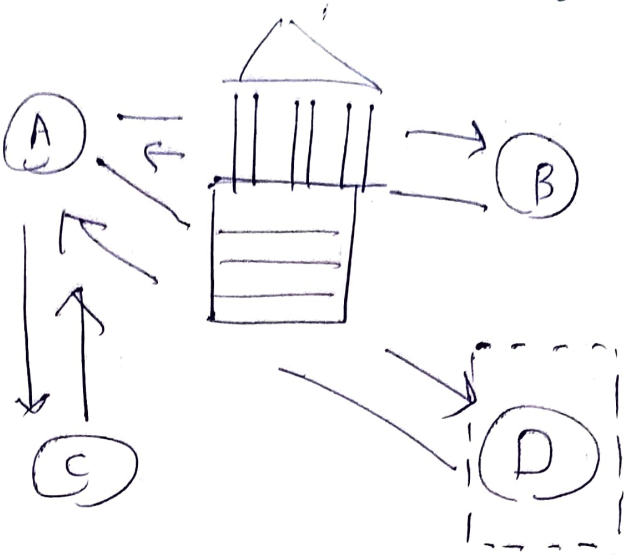
Solve Mathematical problem



check valid or not by miners

Block is added

Byzantine Generals Problem



Traitor

Practical Byzantine Fault Tolerance by Miguel castro

Layman Lang Expln:-

If majority says yes then its yes .... (Majority wins)

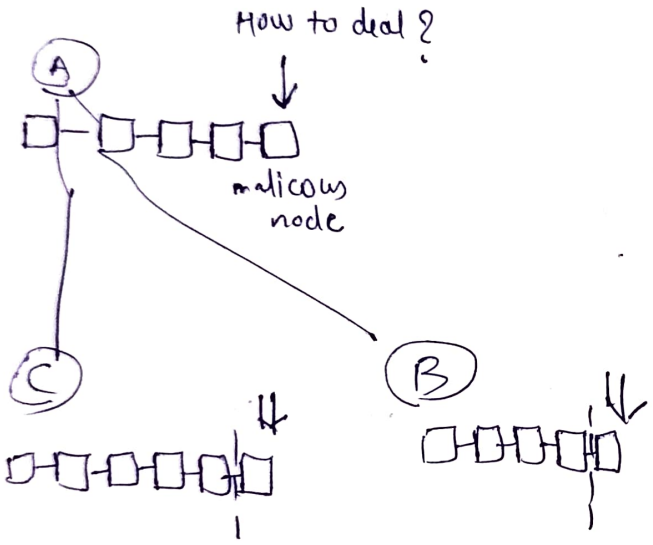
How it works in Blockchain?

Consensus Protocol

It protects us from
(1) Prevent attacks
(2) Competing chain problem

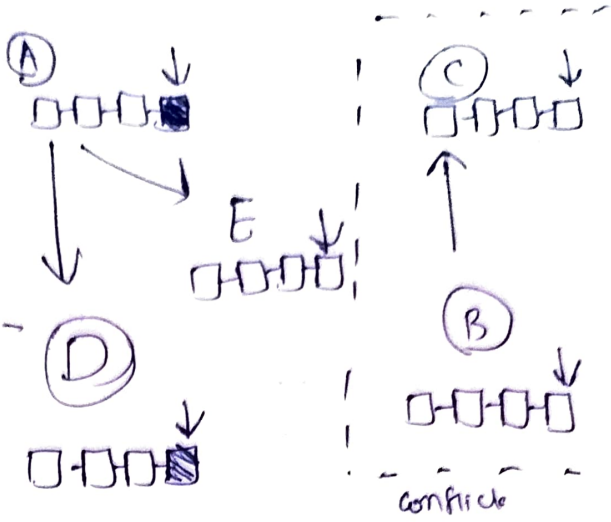
Types of Consensus Protocol:-

(1) Proof of Work (POW)
(2) Proof of Stake (POS)
(3) Others.



Whole network checks new Block it is valid or not when it is verified then Block is added.

(2) Competing chain problem



The longest Blockchain will get accepted & others will get discarded.

- The consensus protocol of blockchain is much better than the Byzantine fault tolerance as consensus protocol only needs a 51% majority while Byzantine need appro. 66%.

- All the transaction in the orphan block will be dropped and the miner that had mined the block will not get any reward.

- So that is why wait for the 6 confirmations before assuming payment to be successful.