Experimental :

Intro

- chain of records / Blocks is called Ledger
- The Ledger is shared among the network which access a public distributed ledger
- Anyone will not be able to alter the data because :-

  (1) Each user has a copy of the ledger

  (2) The data within the blocks are encrypted by complex algorithms.

Blockchain can be described as :-

(1) Collection of records

(2) linked with each other

(3) strongly resistant to alternation .

(4) protected using cryptography.

Transaction

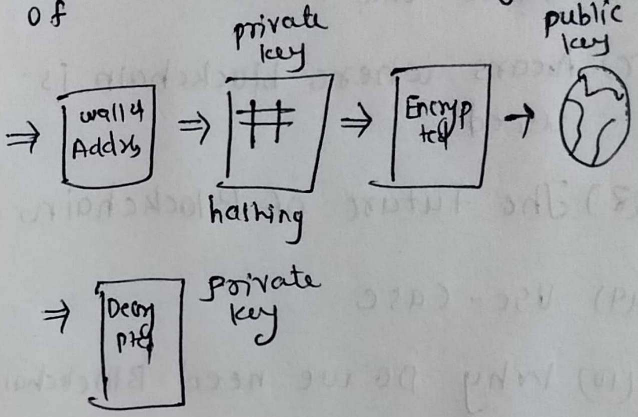
Every user in bitcoin transaction has two keys

(1) public key

(2) private key

(1) public address that everyone in the network knows of

(2) private unique address that only the user has knowledge of



- Hashing

(1) Bitcoin - SHA256

(2) Ethereum - ETHASH

Miners :-

people who validate the Blocks are called miners.

- Miners needs to solve problems
- The process of solving complex mathematical problem is called as proof of work
- and process of adding a block is called mining .

What is Blockchain ?

- A blockchain is a list of records (blocks) which stores data publicly and in chronological order.

- Secured using cryptography

- Not controlled by a central authority

- Access to anyone on the network

- Everyone has copies of the data.

Blockchain features

(1) Public distributed ledger

(2) Hash encryption

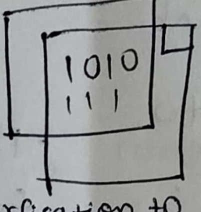
(3) proof of work

(4) Mining

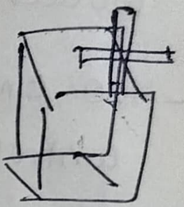
The Bitcoin story

The sender transmits the transaction details world wide

Sender



verfication to authenticate users ; by mines around the world.



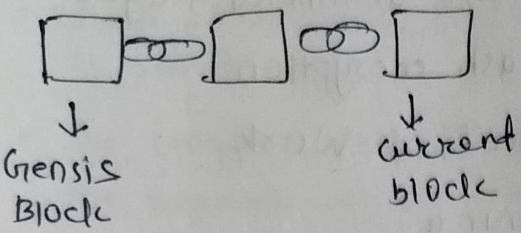
once authenticated the transaction is added to a block and made part of the blockch

receiver

Money is deducted from the senders wallet

mony is added to the receiver's wallet .

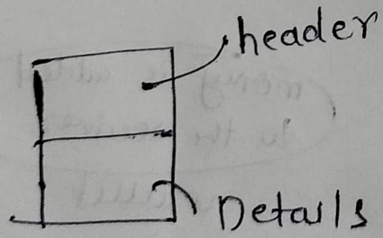
Public Distributed ledger!

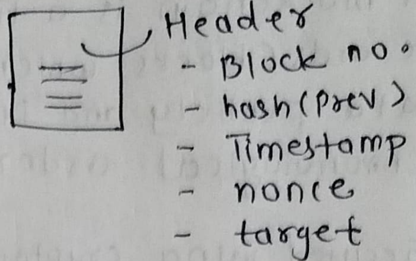


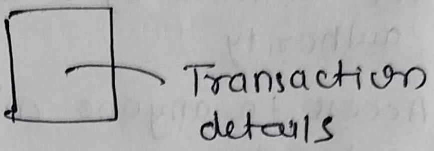
- The data within a blockchain is accessible to everyone
- Any additions to blockchain have to be approved by the users
- Any additions made to the Blockchain are permanent
- No central authority to control how it works.

Hashing Encryption

- A block is a container that holds transaction details







256 bit has value

Merkle root or hash root

- Blockchain utilizes a hash function to perform cryptogr.

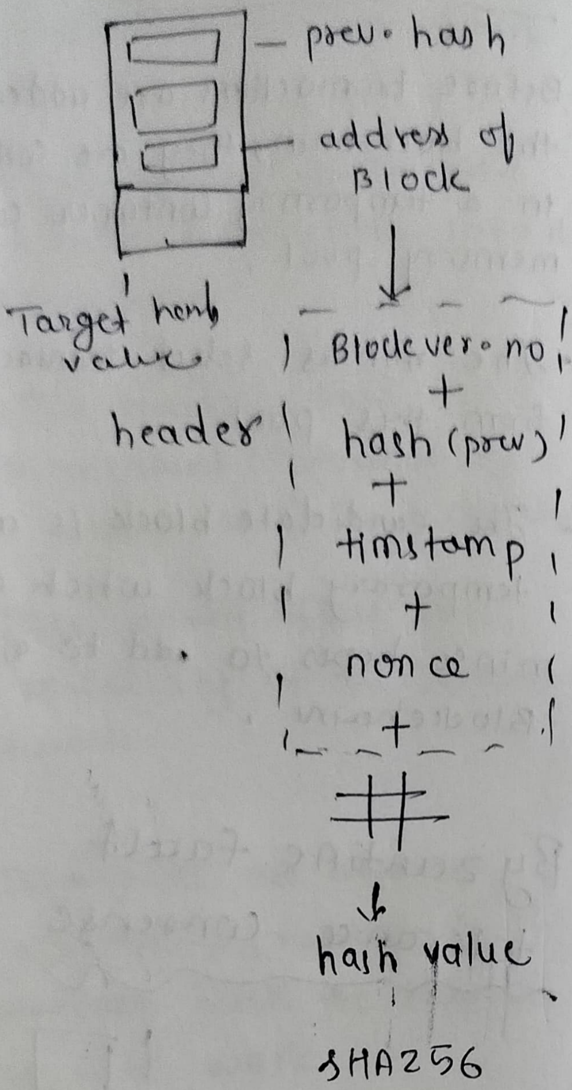
- properities of hashing function:-

(1) These are deterministic

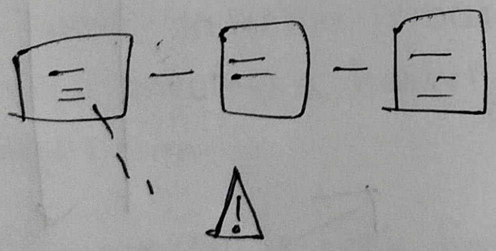
(2) Small changes in the data can drastically change the output

(3) Can be computed easily

(4) Are one way functions

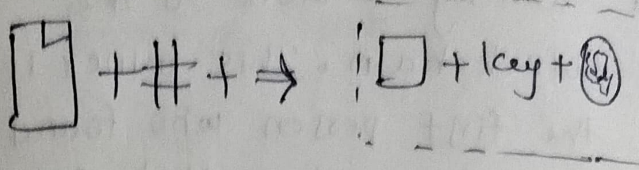


- SHA256 ensures that alterations to data can be easily detected.



- To ensure security, blockchain also includes digital signature.

- Users are provided their own private key & public key.



Proof of Work

- proof of work involves people around the world (called miners) competing to be the first one to add a block to the blockchain.

compete → solve → reward

Nonce → They need to find a hash value that satisfies certain predefined conditions

Hash value is generated using nonce

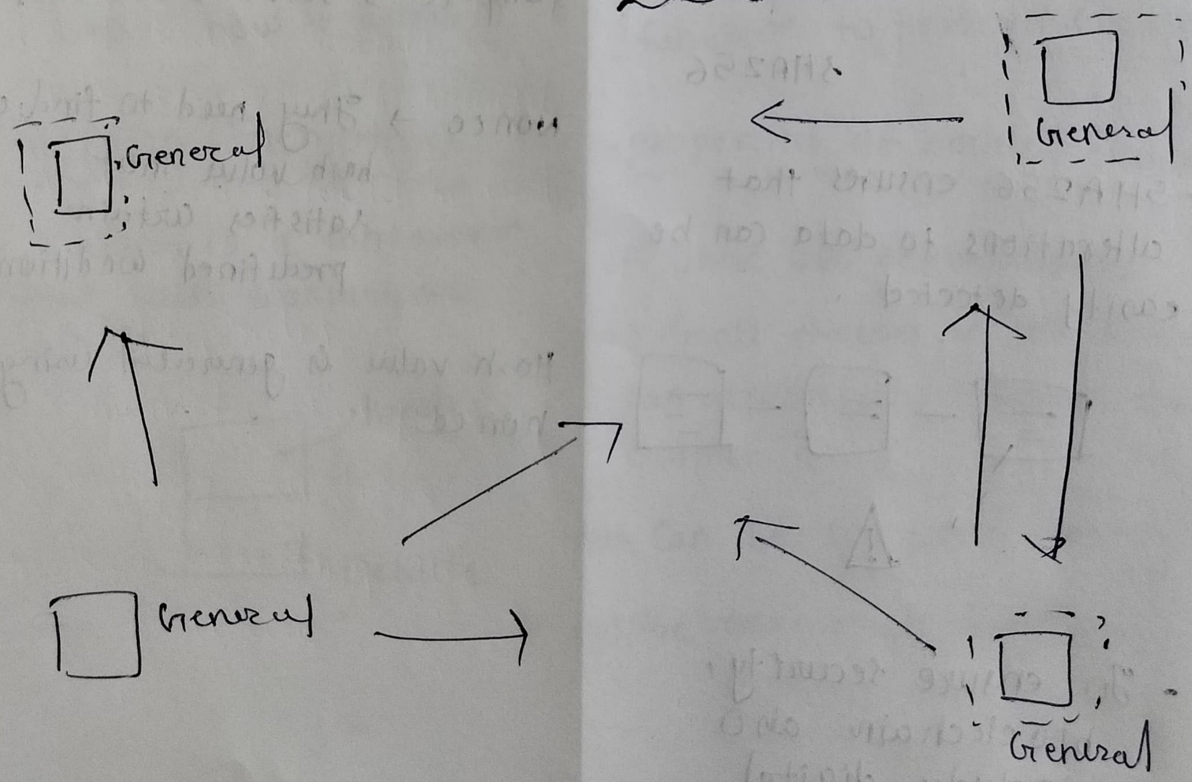
Mining

- Mining is the procrs of adding a block to the blockchain. This miner is the fist person who found a nonce value that fells within the target req.
- for doing this, the miner is rewarded.

The Candidate Block

- Before transactions are added to the blockchain, they are collected in a temporary container called memory pool.
- The miners select transactions from this pool.
- The candidate block is a temporary block which a miner hopes to add to a Blockchain.

Byzantine fault tolerance consense



- The same situation can be encountered in Blockchain as well

(1) The traitor would add invalid transaction into the Blockchain

(2) The traitor would send inconsistent information to other nodes in a Blockchain

(3) This would effect the reliability of the Blockchain network.

- Blockchains are able to achieve Byzantine fault tolerance with the help of proof of work.

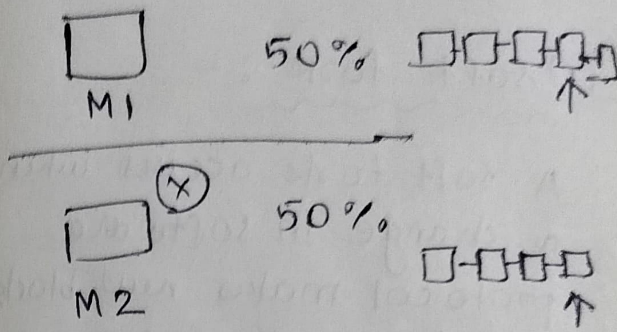
- It is effective because :-

(1) The process of adding a block to a blockchain is a work-intensive process which involves a hashing algorithm

(2) The process is very hard because it is heavily reliant on values obtained from the existing Blockchain.

(3) To have any meagninful impact the hacker would have to take a lot of time producing sufficient proof of work.

✓



- Accidential work

Fork

- A fork is said to have taken place when a blockchain diverges into two potential paths

- A fork happens when the users of a network cannot come to an agreement with regards to :

(1) A network's transaction details

(2) New rules to validate transactions.

There are two types of forks :

(1) soft fork

(2) Hard fork

(1) soft fork :-

A soft fork occurs when a change in software protocol makes new blocks added to the blockchain (following the new rules) backward compatible

- It also requires a majority of the users to commit to that change to be successful

- A soft fork would be used for :-

(1) Tighter rules

(2) cosmetic changes

(3) Adding functions

(4) Not affecting the structure

(2) Hard fork :-

- A hard fork involves a change in software protocol so radical that it forces a new blockchain to be created.

e.g Bitcoin cash