# B & C C.

## Properties of blockchain:

→ Decentralized ledger technology
→ Data is not modifiable/deletable, only new logs can be added for all operations. [Immutability]
→

* first block of a blockchain is called Genesis block.

---

Hashing. SHA - 256
(property ↓ Hexadecimal output

Avalanch Effect


own hash is built by hashing data & prev hash in this block.

MARVEL

## Distributed P2P network.

* miners are working nodes in blockchain
* user nodes are end user nodes.

* all nodes are anonymous, every node gets a unique address

* in a blockchain network a single miner is selected who can add a block.

* all nodes have copies of all blocks

* Voting system to ensure integrity of all copies of

blockchain in network

* just like Raft consensus algo in PDC.

**Mining**:

**Nonce**: Number only used once.
↳ an attribute in block.

**The cryptographic puzzle**: System generates a hash, miners have to generate any hash equal or less than that system hash, whoever generates the same hash first wins & is able to add a new block

* That answer hash is made by testing multiple nonce by miners, the winner nonce is called **golden Nonce**.

# BCC.

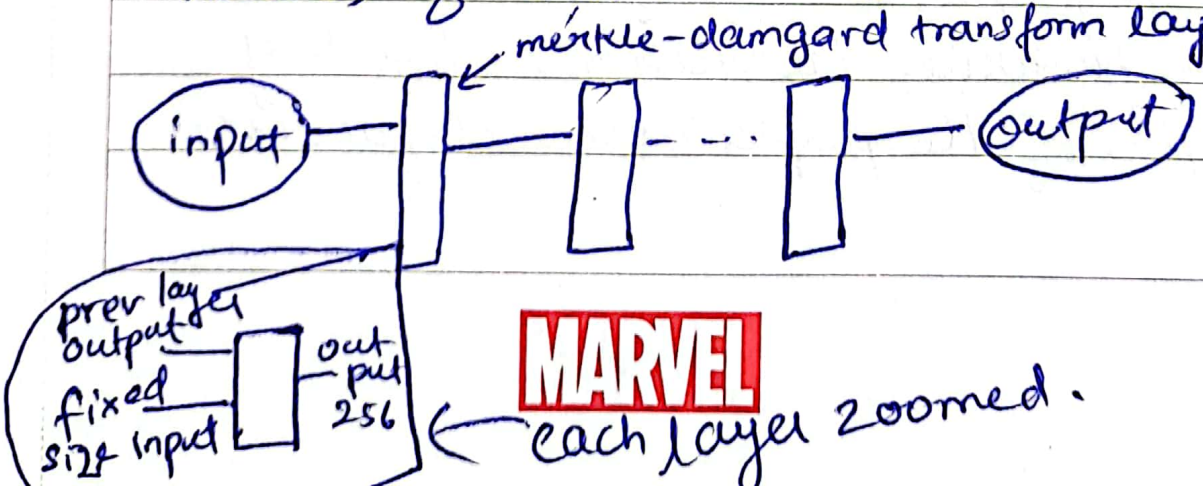
* golang

* **tolerance factor** : after a certain number of false votes from a specific node, that node is disabled.

* **Byzantine fault tolerance** :
  → if system has 1/3 or less traitors, system is safe.
  → Tolerance factor is 33%.

* **Merkle-Damgard transform**

* **Merkle tree** is a binary tree which store the collective hashes of child nodes



**Consensus protocol:** supervision algorithm

- proof of work (POW) ← used in Bitcoin
- proof of stake (POS) ← used in Ethereum

**competing chain:** when the network contains two or more valid chains. The block which loses is called the **orphan block.**

# BCC

## 3 layers in cryptocurrency.

→ Technology : blockchain
→ protocol : ripple, waves etc. bitcoin, eth
→ Tokens.

Q mention some names of protocols of cryptocurrency? imp
Ans: waves, Etherium, Bitcoin, Neo, Ripple.

## Bitcoin Ecosystem

* Nodes
* miners
* Large miners
* Mining pools

## Bitcoin's monetary Policy

* The Halving → {Block reward keeps halving every 4 years}
* Block Frequency

# BCC.

**Nonce Range** : The nonce range is **0 to 4billion**. ↘ in Bitcoin.

* **Blocksize** in a blockchain is **fixed**. i.e you can only fit a certain number of transactions in it.
* **Bitcoin** has block size of **1MB**.
* nonce is a **32-bit unsigned** number
* ↳ range is 0 – 4billion

* **Timestamp** is also added to the block. (unix form) ↺
* BTC has 1 min time to update.
* can customize the format & updation time of timestamp in block.
* **Mempool** : a pool of transactions, all public.

* rather than waiting for the timestamp to update, if your computation power is alot you can pick more transactions from mempool & replace the existing transactions in block. This is called Change Block Configuration.

* Balance = sum of all unspent transactions

* Timestamp stores the time the block was mined.

* When user wants to spend the amount. Blockchain finds closest values of unspent amounts from blocks in combos or single.

* The transaction used to send some amount is marked as "spent" & if any amount is not used in that transaction is added as a new

transaction to the user's UTXO.

* Escrow state

## Wallets

* public key can be retreived using private key but not vice versa.
* Each account has separate private, public keys even if all accounts belong to same user.

## Digital Signature

### sender side

message → hashed → encrypted by private key → signature

### receiver side

message → hashed

signature → decrypted by public key of sender → match (with)

if = then valid ✓ otherwise


forged!!

Bitcoin uses ECDSA standard

↓

Eliptic curve digital signature algorithm

* public key is the unique identity of a node in blockchain (hashed)
  bitcoin address ↙

* HD (Hierarchical Deterministic) wallets:

* master Private Key: seed phrase.
  ↑
  a phrase of random words.

* BIP-19 standard. ↺
  algo to generate seed phrase.
  ↳ 13 word standard also available
  12 word, 24 word → 25 word standard also available.
  ↓
  a dictionary

# Ethereum

* Vitalik Buterin built an IDE to build similar protocols like Bitcoin called Ethereum.

* Ethereum supports many languages but the most popular one is Solidity.

* Solidity is a turing-complete language.

What does it mean for a language to be turing complete?

① Have conditional capability
② Have arbitrary amount of memory and be able to jump within this memory i.e "loops or go-tos"

# Smart Contracts.

→ Programs
→ Immutable } due to blockchain
→ Distributed } technology

* Smart Contracts can replace intermediary persons e.g a kickstart that collects funds from people who support an idea, but if the goal won't reach, return all money.

**Security issues with smart contracts in Ethereum:**

① Viruses & access to private files
② Infinite loop / heavy computations

The first issue is dealt by **EVM: Ethereum Virtual Machine**
→ whenever a user wants to use any app made on Ethereum

EVM is the medium to connect to it. "a computer specialized in processing smart contracts" is how EVM can be defined.

* The more complex the smart contract is to compile the more gas fees it takes. The compilation is what EVM does.

* Gas fee solves the issue of heavy codes.
* restricts people to write complex code.

* Gas fees are denominated in small units of ETH called gwei (short for gigawei) where 1 gwei = 1 billionth of ETH i.e 0.000000001

MARVEL

## Decentralized Autonomous organizations (DAOs)

* in DAOs, the human intervention is simply replaced with smart contracts. Every process that has a set of specific conditions is written in code.

## Segregated witness (SegWit)

SegWit address these two issues in Bitcoin:

* Scalability
* Malleability

| Legacy (old version) | SegWit (update) |
| --- | --- |
| * Block size = 1 MB<br>* consists of a base block of 1MB containing inputs, signatures & outputs | Block size = 4 MB<br>* Consists of a base & an extended 3MB block which contains the signature so it cannot be used to tamper block id (witness data) |

## The DAO attack:

attackers discovered a vulnerability in the smart contract & exploited it to receive $50 million in tokens to their account.

↳ after DAO attack:

| hard fork | soft fork |
| --- | --- |
| ↓ | ↓ |
| Compulsory updates | updates on choice |

↳ Crypto Forks

* Fork is simply a change/update in a protocol.

e.g

ETH — ethereum

ETC — ethereum classic.