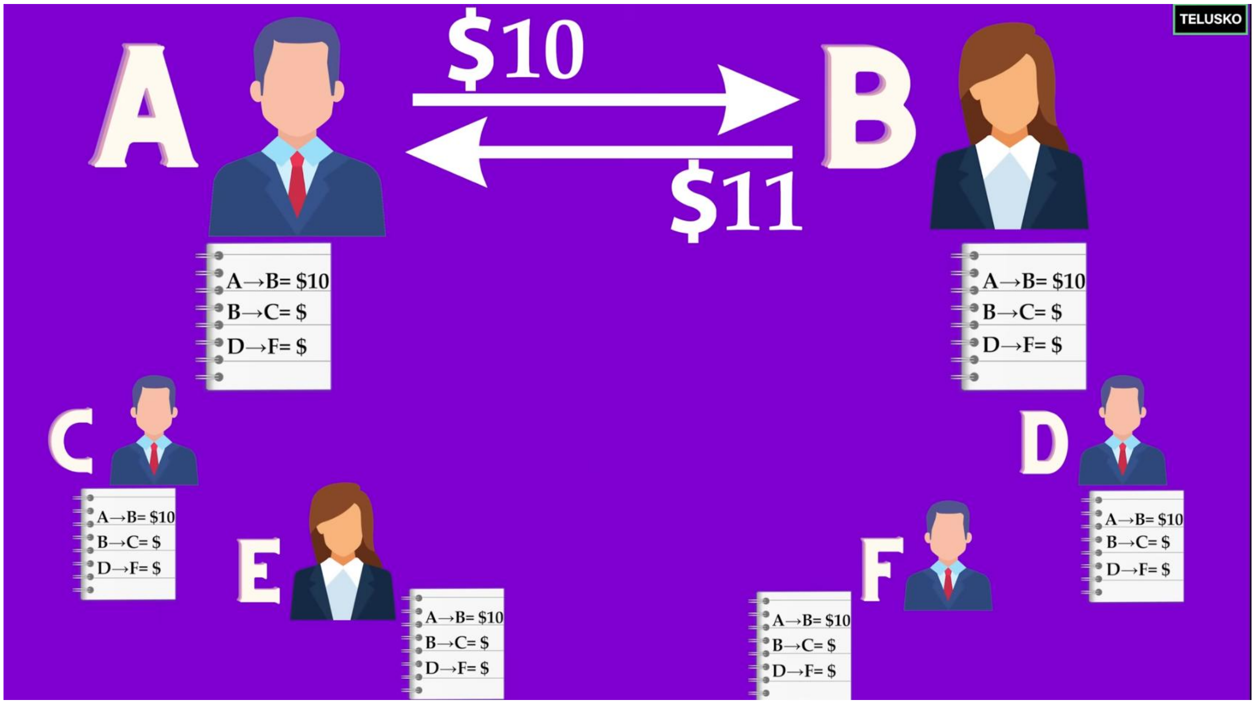
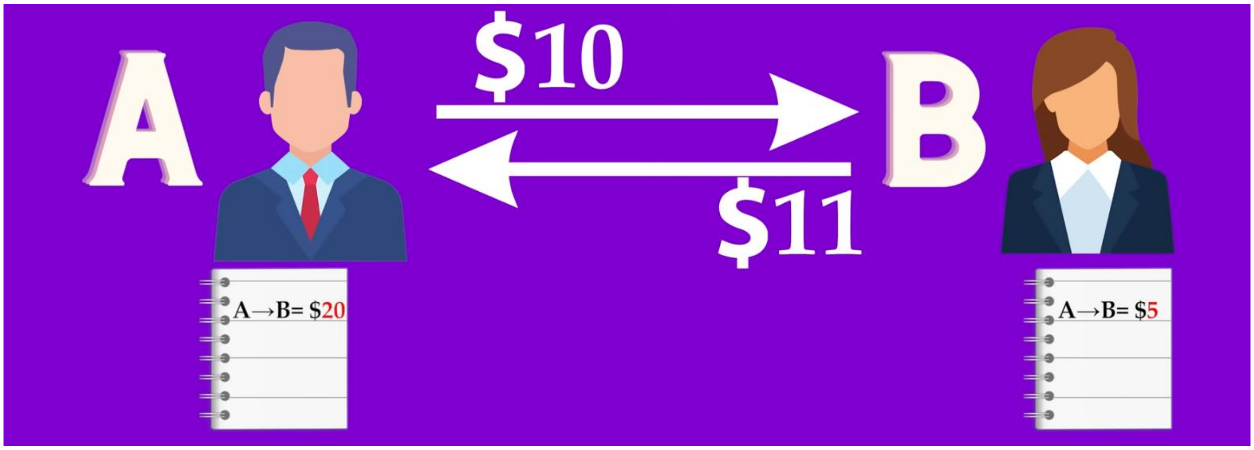
Introduction to Block-Chain key-Concepts to Understand::

a. What is Web3 have any credit on how they are using it(security)=> no control of your own data.

- Get to know Torrent Networks works
- In Web2 Your data on free Google services or YouTube are being traded while you thought its free and you don't have any credit on how they are using it(security)=> no control of your own data.
- The applications that are running on distributed networks(DAPs)

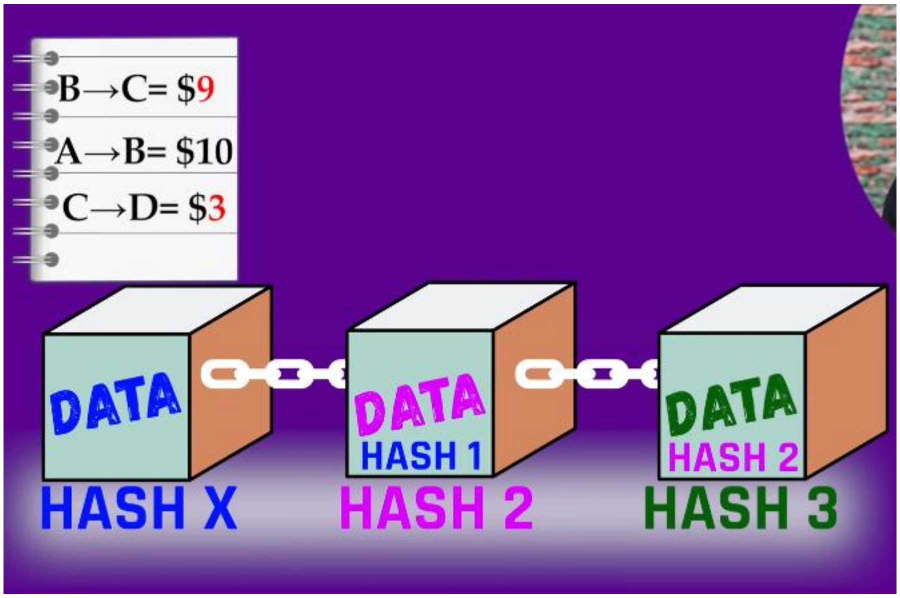


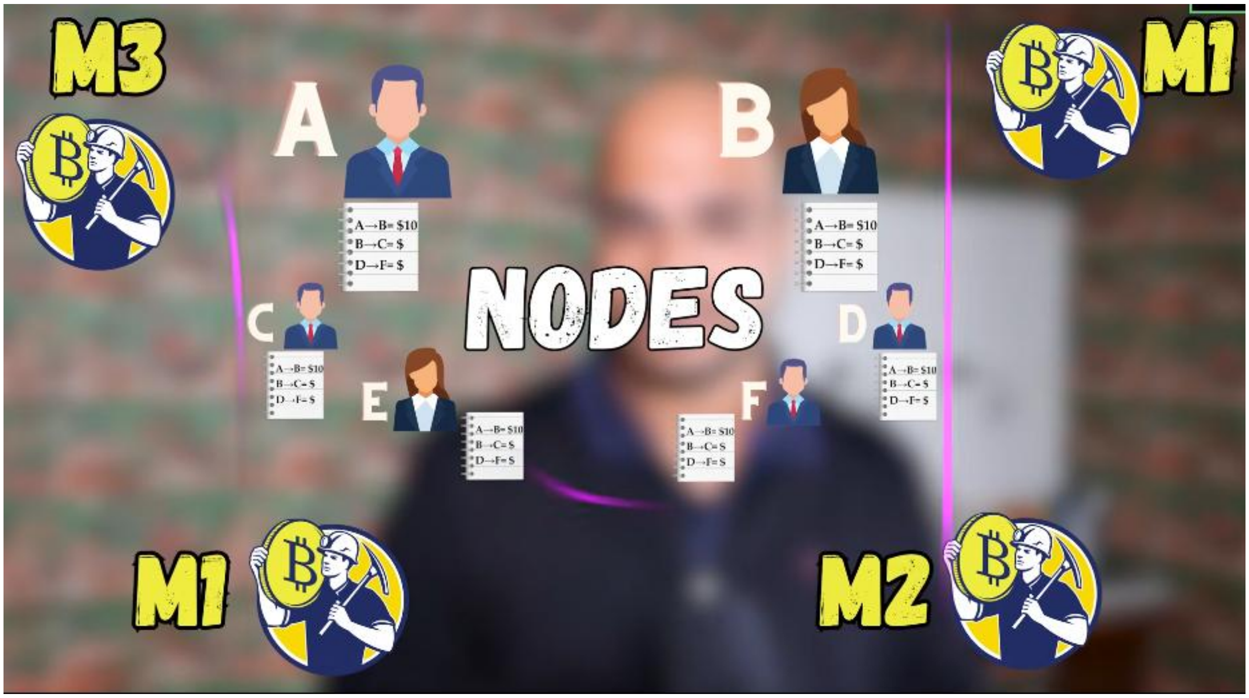
-
- On Web3 you own your data.

- 

b. What is Block-Chain?

- Moving from Centralized->Decentralized (who will control our own data?).
- Data on Web3 is immutable (everyone can see if someone want to make forgery).
- If someone try to modify data as a **miner** on web3 we can notice him/her a kick him out of our network.



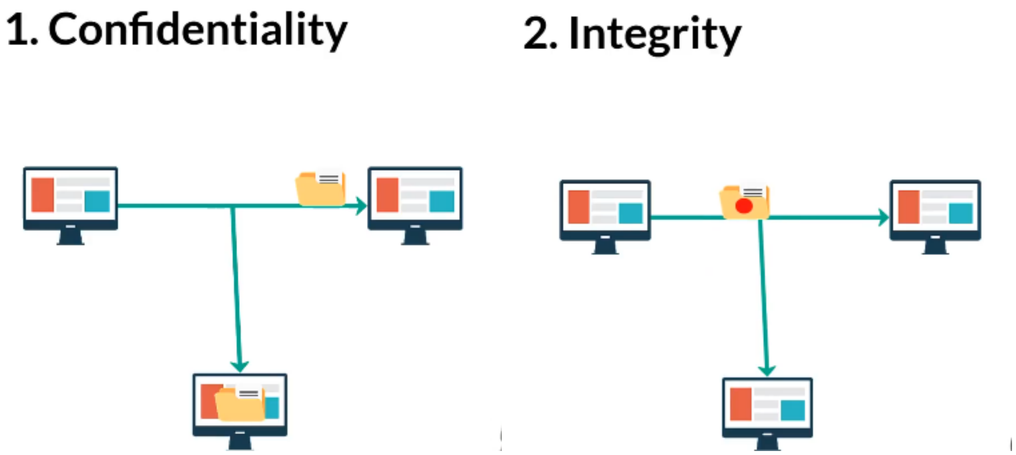


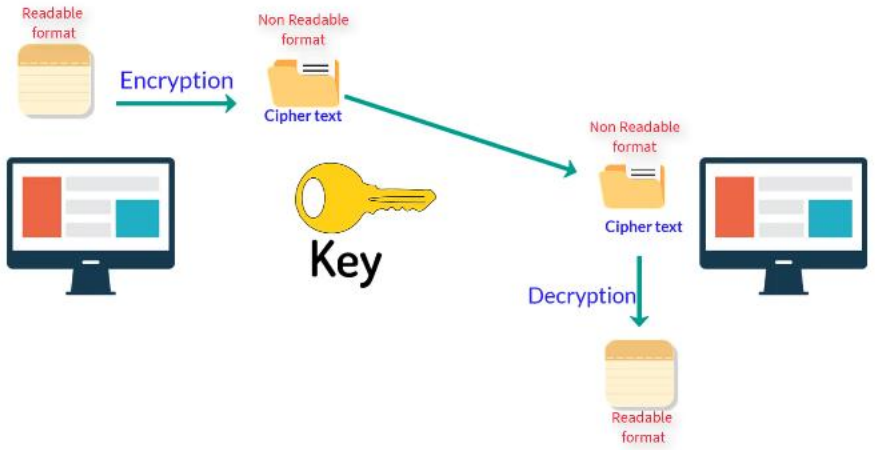
c. Why Block-Chain (who, why, and what are prerequisites)

- Block chain provide **Trust**
- Prerequisites are cryptography and distributed computing.

d. Cryptography.

- Confidentiality (none can see that data)
- Integrity (none can modify our data)
- Non repudiation. (proof of message transferred).
- Authentication. (None must send message to someone’s else behalf).
- Crypt(Hidden)-Graphy(Written)=>Encryption

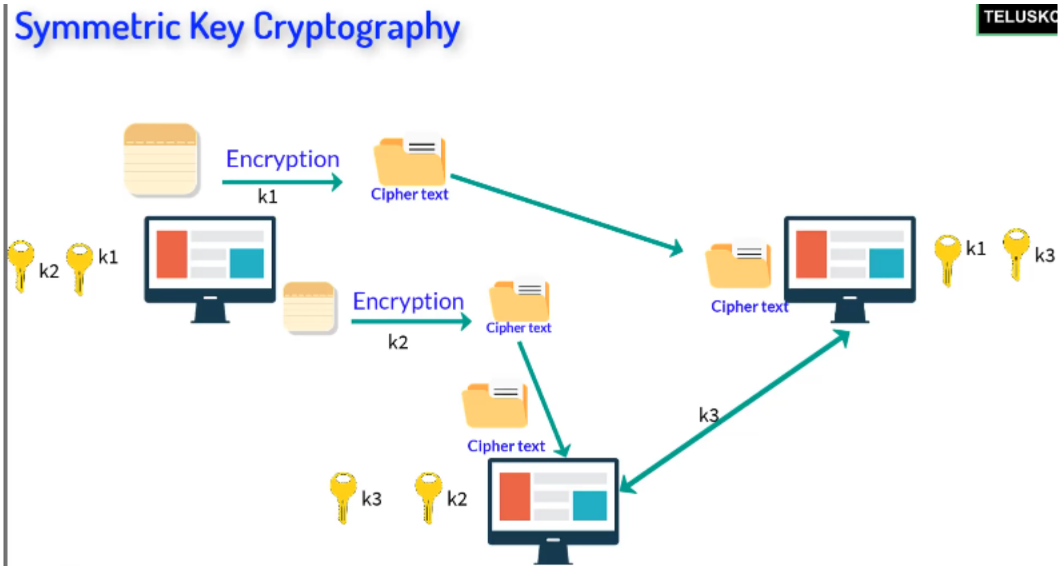


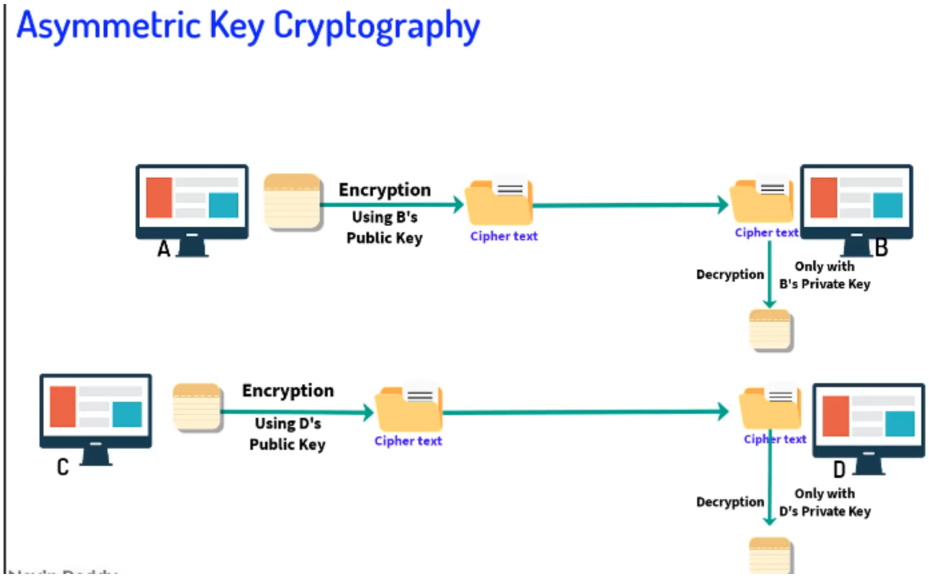


e. Types of Cryptography

- **Symmetric-Key Cryptography** (same key=> tedious).

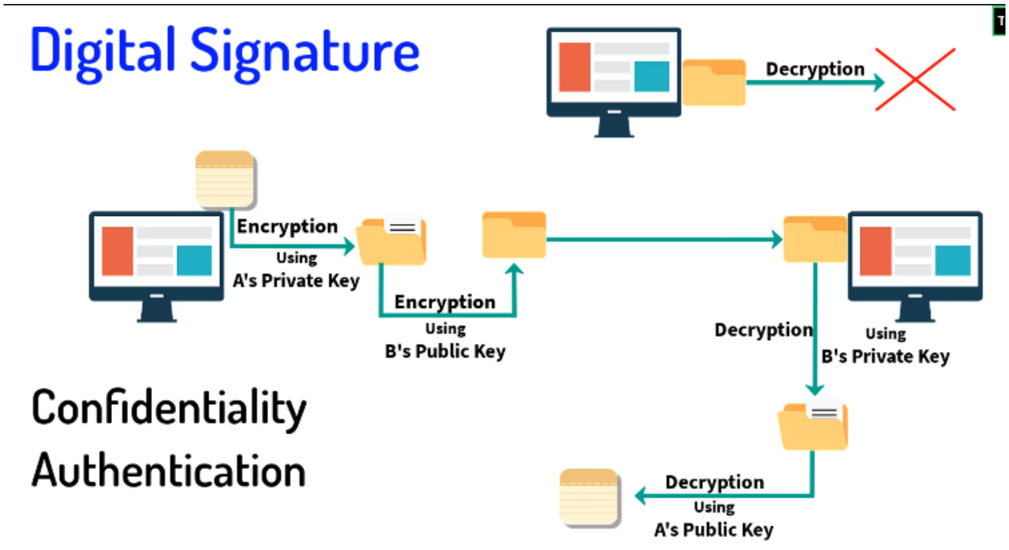
  As number of user increase we need to increase number of keys..
- **Asymmetric-Key Cryptography** (public and Private key)





f. Digital Signature. (solve problems in network)

- We need to know who is exactly sending the data (like written letter signed to confirm its you).

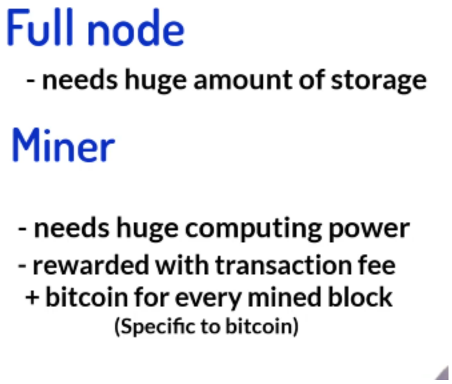


Digital Signature

Confidentiality
Authentication

g. Nodes in Block Chain.

- Full Node needs at least good processing CPU’s and GPU’s in 188GB and it verify and store block-chains.
- Partial Node can be like PC/cellphones to download the app and use to trade (on purpose).



Full node

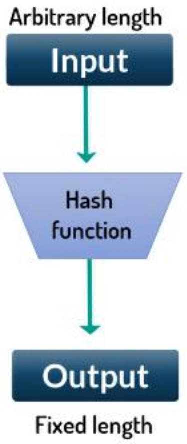
- needs huge amount of storage

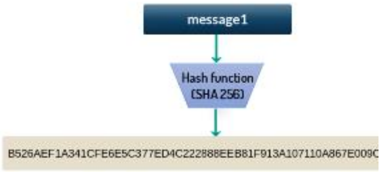
Miner

- needs huge computing power
- rewarded with transaction fee
+ bitcoin for every mined block
(Specific to bitcoin)

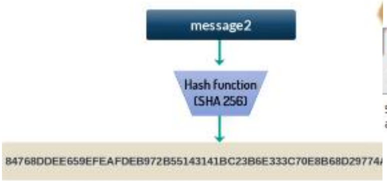
h. Hashing in Block-Chain

- You cannot get data back in hashing like encryption-where it uses decryption.
- We can use algorithms like MD (Message Digest), SecureHashAlgorithm(SHA).

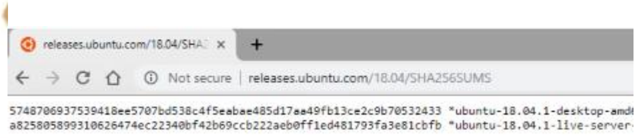




```
B526AEF1A341CFE6E5C377ED4C222888EEB81F913A107110A867E009C
```



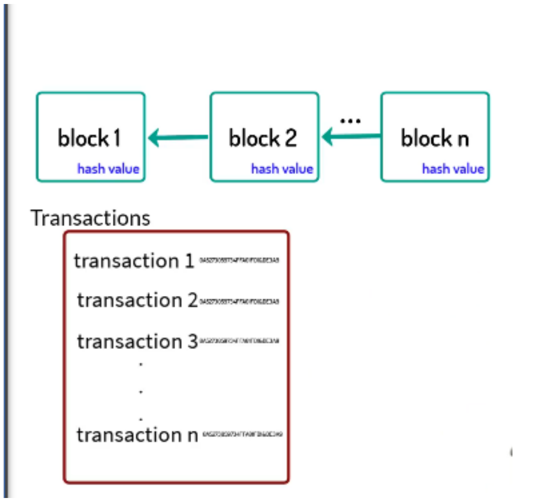
```
84768DDEE659EFEAFDEB972B55143141BC23B6E333C70E8B68D29774
```

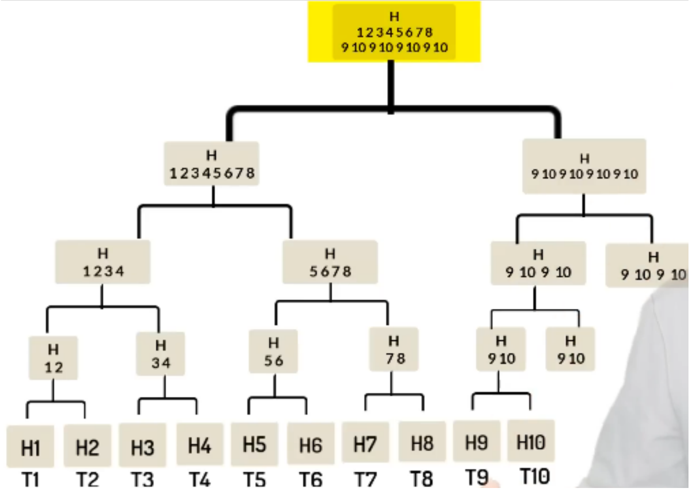

releases.ubuntu.com/18.04/SHA
Not secure
releases.ubuntu.com/18.04/SHA256SUMS

```
5748706937539418ee5707bd538c4f5eabae485d17aa49fb13ce2c9b70532433 *ubuntu-18.04.1-desktop-amd
a8258058993106264 74ec22340bf42b69ccb222aeb0ff1ed481793fa3e81cbfb *ubuntu-18.04.1-live-server
```

i. MerkleTree_MerkleRoot.

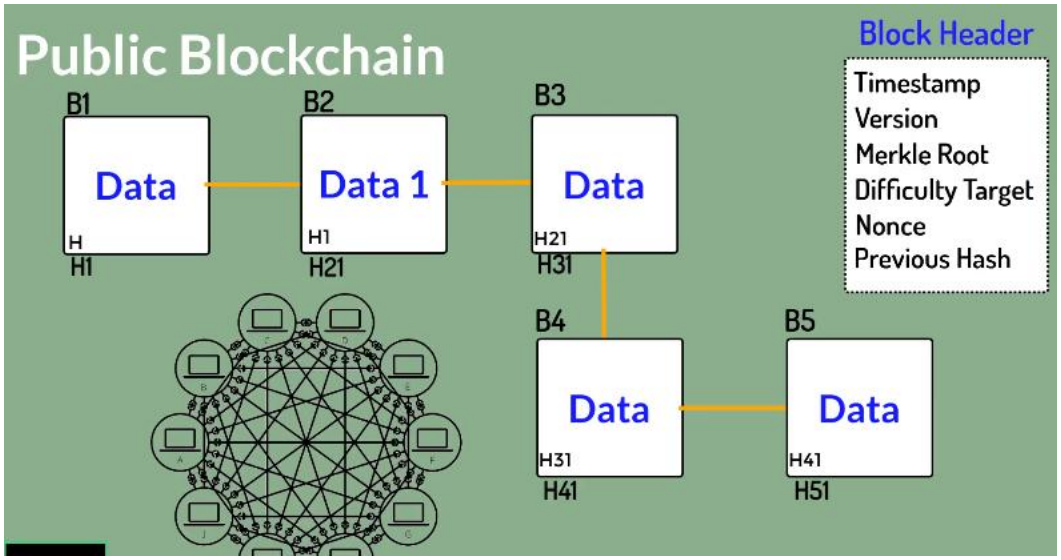
- We need to have only one hash for each transaction.





j. Blok_chain_Technology_Architecture

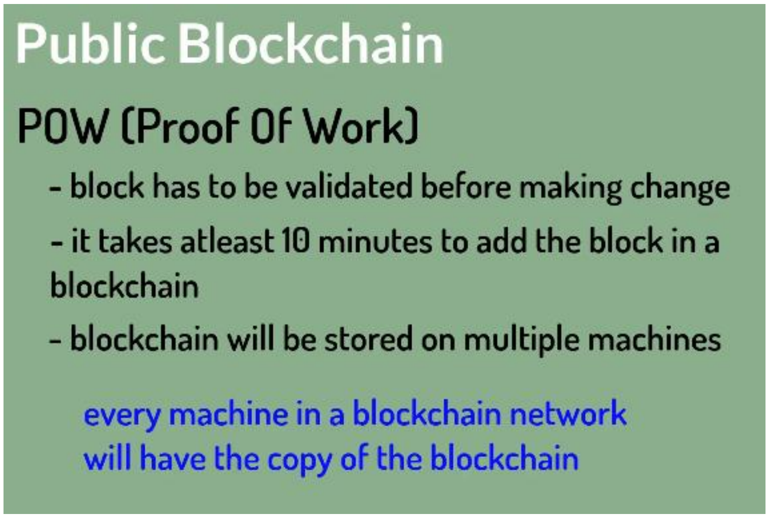
- Consensus Algorithm give nodes to verify your proof of work
- To add or modify data to block chain you need 50% majority.



Public Blockchain

Block Header

- Timestamp
- Version
- Merkle Root
- Difficulty Target
- Nonce
- Previous Hash

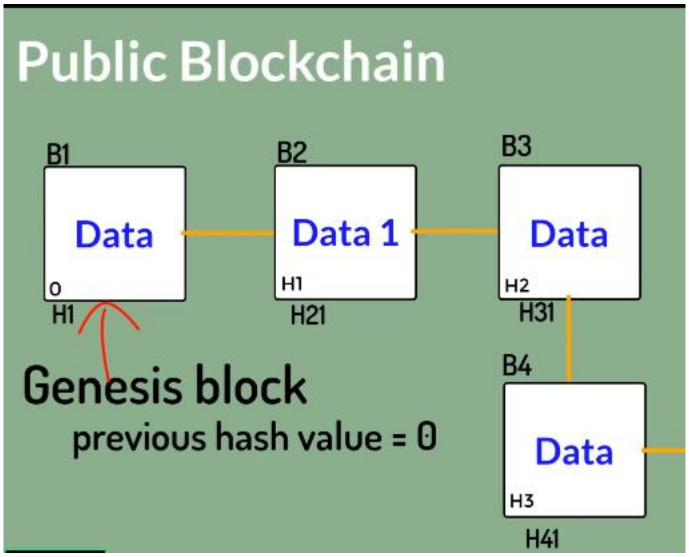


Public Blockchain

POW (Proof Of Work)

- block has to be validated before making change
- it takes atleast 10 minutes to add the block in a blockchain
- blockchain will be stored on multiple machines

every machine in a blockchain network
will have the copy of the blockchain



Public Blockchain

Genesis block

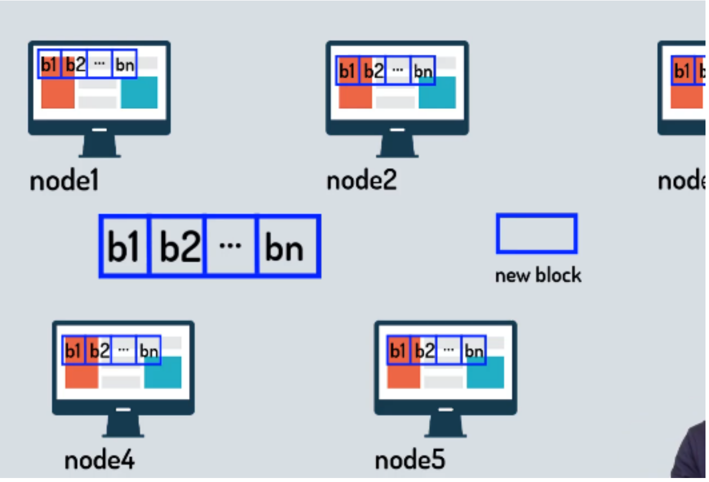
previous hash value = 0

k. Types of Block chain

- Public Block-Chain is open and everyone can be part of it (slow we need POW).
- Private Block-Chain is specifically for a single company (fast-> no need of POW).
- Federated Block-Chain is group of people /companies.

l. Consensus in Block-Chain

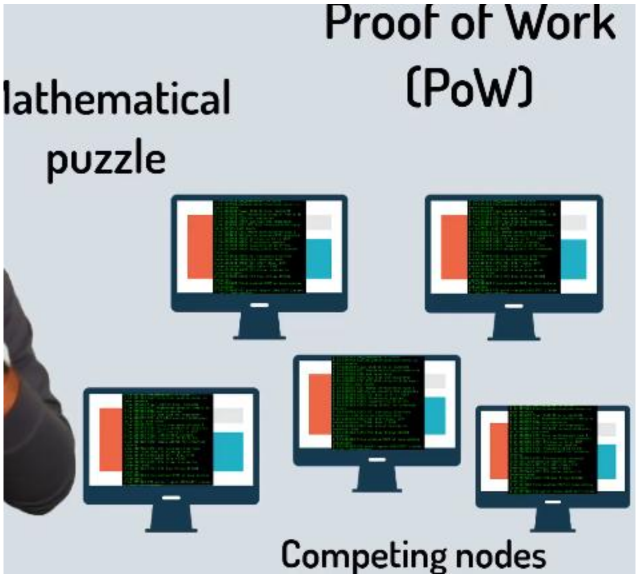
- We give miners (not malicious) puzzle to solve and use their computing power, one who wins, add the block-to chain and got rewards. And using consensus we can agree on some state on block-chain network.
- Algorithms like POW(work),
- POS(stake) where too much investors(coins$) got trust.
- POET (Elapsed time), POD (deposit), POC(capacity)

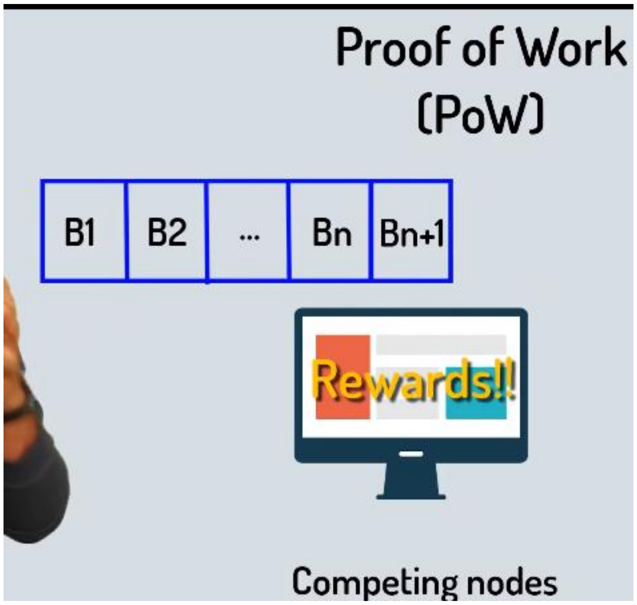


m. Proof of Work. (Bitcoin)

- There’s is a competition of math-calks who win add block in chain and get rewards.

- Issues (spending too much idle power, and may be 51% of nodes are malitious)





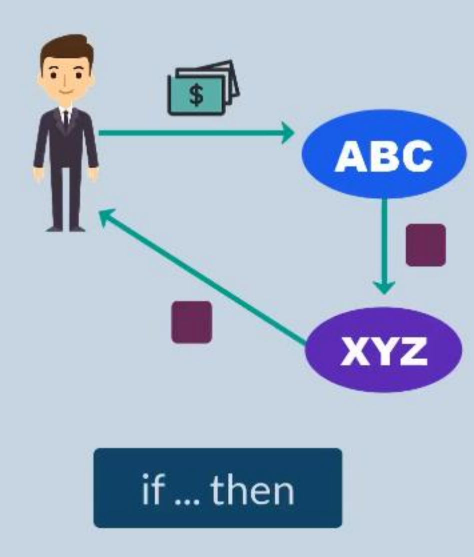
n. What is Etherium.

- BitCoin is peer-to-peer electronic cash system.(CryptoCurrency)
- To write apps/softwares we have Etherium(DApps)
- To be able to use crypto currency in ethereum we need **Ether.**

- **Def:** it's simply a platform where you can build your decentralized applications/softwares, it also has its own cryptocurrency **Ether.**

m. Smart Contracts(**Trust/secure)**.

- **Prepaid** transactions trust issues.
- **Are** lines of codes built and run on ethereum networks to make contracts.



o. Drawbacks of Block-Chain. (mostly public)

- Complexity of many terms & algorithms and even technology.
- Slow Speed [**VISA** handle 1000s transactions/sec] ! [**Bitcoin** handles 7-10 trans/sec]./day
- Wastage of resources to handle their algorithms
- Security/Privacy (the data is there in block chain; everyone can see it).
- 51% attack. (it can be hacked).

  But on private we can handle some of these issues.

p. What is HyperLedger.

- It is not block chain, company or cryptocurrency as well.
- It is a project. Hosted by Linux foundations and accepted from other big-techs(Amazon,Google,IOT,Industry,…).
- Umbrella or Greenhouse for block chain open source products. (B2B) in which you can build block chains.

q. What is NFTS?

NFTs (Non-Fungible Tokens) are like **digital ownership certificates** that prove you own a unique item on the blockchain.

Real-Life Example:

Imagine you buy a **rare, one-of-a-kind trading card** (like a special edition Pokémon or sports card). Even if other people have similar cards, yours has a unique **serial number** proving it's the only one of its kind.

Now, in the digital world, NFTs work the same way! Let's say an artist creates a **digital painting** and turns it into an NFT. When you buy that NFT:

✅ You **own** the original digital artwork (even if others copy or download it).

✅ Your ownership is **recorded on the blockchain** (a secure public ledger).

✅ You can **sell or trade** it, and the blockchain will track ownership changes.

So, NFTs make **digital things** (art, music, videos, virtual land, etc.) **unique and ownable**, just like physical collectibles. 🚀

-

Thanks!!!!!!!!!!!!