Date 31/1/25 Friday

Blockchain

(:lecture 3-4)

- decentralized tech
- no single authority that makes decisions
- once data is published, no one can change the data
- if you have to update, make a new block & attach to the block that needs updating so a ledger of history is maintained
- Data is immutable, data cant be deleted
- BC is like a linked list

Hashing Algo: SHA < 256 (num of bytes) / 512

64 char

input → SHA-256 → output (hash)

① → accepts input of any size (single char or 1 GB) but generates fixed size output (256 bytes)

→ By seeing the output, the hacker can not assume what size of input was, what kind (img or text) etc cz output will always be fixed (64 char in SHA-256)

②

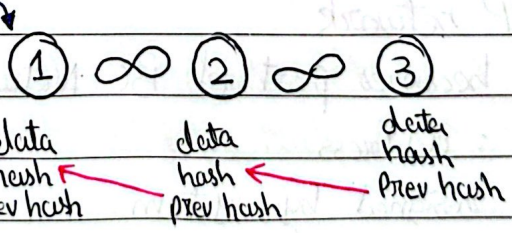
→ Can not reverse the hash & find input

③

→ Avalanche Effect: even a single bit of data would result in a diff hash

Genesis Block:-

genesis block



→ the first block in BC

→ behind / prev is null

* if you give an input to a hash algo that will produce an output. if you give it 100 times, then same output
same input will always generate same hash

Date

- every block has its unique thumbprint => hash of a block which is a unique identifier

Traversal :-

- if the hash of a prev block matches the prev hash of the next block then easy, no changes made
- Keep doing this until you reach genesis block

if hash of prev block ≠ prev hash of next block

then changes have been made

★ Forging = forge the chain
if you change a block then the hash changes, so when the hash changes, go to the next block & change the prev hash.

→ Keep doing this & the entire chain will be forged

P2P Network :-

- distributed P2P network
- when a person becomes part of BC Network, the system assigns a unique identity : address
- unique address assigned by system
- real identity not shown in network
- reduces biasedness, no special importance given to anyone
- nodes are anonymous

Date

Blockchain Network : P2P distributed network → each node has a local copy of BC

* After some designated time, the copies of all the nodes are verified & checked that if all the copies are same or not
  ↳ mejority matters, solution to key forging
  ↳ check reflection as well

Data Updation :-

(A)

- the data comes to a node, it does verification & attaches the Block to it's copy.

- The node A, sends it's copy or the data to others, they perform checks as well & attach it if the data is valid

- The reflection is made by seeing the copies of all nodes & by checking the reflection, all nodes update their copy

Miners :-

- Working Nodes = Miners
- All Miners are equivalent, Data is given block by block in BC
- Miners have to compete among themselves to get the right to attach the block & initiate it (like Node A) ↑

Date

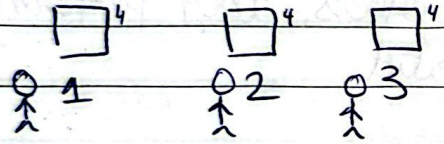
What is Mining?

→ there is an avg time in which a block should be attached

→ the algorithm generates a competition after a while like eg a puzzle, who wins the competition first, will get the right to initiate block 3 will notify others

→ every block has a block number : block num is public

→ all miners create a local block



all miners will now compete for the Block 4

3 miners, all will have same prev hash, all will attach Block 4

Nonce : Number only used once
↳ decided by miners

miners keep changing the nonce to find diff hashes

The system generates a cryptographic puzzle : generates a hash & asks the miners to generate a hash below the target hash

* Golden Nonce : the nonce in which the puzzle is solved, the nonce below the target hash

Date 7th feb, 25 Friday

Lecture 5 & 6

→ cryptographic puzzle is mostly for fairness in miners
→ Nonce is unsigned int, 32-bit number
→ if Miner has more computation power then the probability of winning the puzzle is more
→ Every block has a timestamp in Unix formest

Timestamp :-

→ each block has a timestamp
→ this timer keeps on running until the puzzle is not solved
→ When Golden Nonce found, timer stops
→ Timestamp tells when exactly the puzzle was solved
→ e.g

a person has a lot of computation power, the TS rn is 44, a person searches up all the 4 Billion hashes & golden nonce not found, as soon as the TS becomes 45, person will try all 4 billion hashes again, diff hashes will now be generated cuz of TS changing: avalanche effect so now chance of Golden Nonce to be found comes again.

Memory Pool : MemPool where all transactions are present

Original Blockchain had the block size of 1 Mb, exclude all the space for other variables & then add as many transactions as possible

Miners mostly choose those transactions which have relatively higher fees, those transactions are removed from the Mempool & added in the data of the Blockchain

Date

Change Block Configuration :-

this happens when a miner with high computation fees has tried all the 4 Billion hashes, the timestamp also has not changed so we dont want the honest miner to wait so what will the miner do now ?

=> The miner will now change the data/transactions present in the Block. Even if one transaction is changed, Now he can generate 4 Billion hashes that will be diff.

cuz

Miner can't change :

1) Timestamp
2) Prev Hash
3) Block Number

but

Nonces have all been tried so now only option is Data

Consensus Protocol :-

→ Such rules on which the working nodes & the end-users agree on e.g the person who solves puzzle can publish block

→ This protocol works on top of P2P network

Date

Consensus Protocols

Proof of Work (POW) ← Consensus Protocols → Other

Consensus Protocols ↓

Proof of Stake (POS)

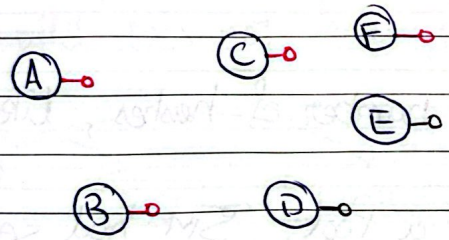
Challenges :

1) Attackers
how to secure network in times of attack

2) Competing Chains

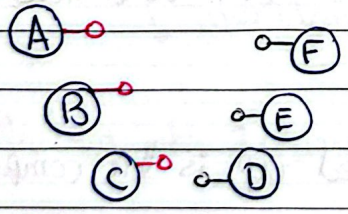
In distributed P2P networks, some nodes get the info quickly & some later cuz of latency.

e.g



A & D both solve puzzle at the same time but due to latency issues D could not timely distribute the block before A so now pink block will be attached everywhere cuz of majority is the authority

In the scenario, that network has 2 chains then the longest valid chain will be chosen => this situation happens when



50% network has pink, other 50% has black so now when the puzzle comes again & someone from pink chain like A, B or C solve the puzzle then they will attach the block. So now they have 2 blocks & other has only one & the black ones cant start the next puzzle until they accept the pink chain.

Date 21st feb 25 Friday

Lecture 7 & 8

- end-users can access the mem pool, everyone has copies of it
- all the participants can view which transactions are in the mem pool. & can then (miners) take out a few for mining & block formation.

e.g

i do a transaction, first it is added in my mem pool & then through the distributed systems, it is added in everyone's mem pool. Miners can take out transactions, if Miner A picks my transaction, it will be removed from all the copies of the mem pool.

=> Minning Pools :-

different miners join a group & divide the number of hashes, like

- 5M
- 10M
- 1M

3 Miners have joined a Pool, 5M had searched & hashed 10 million, 1M had done 15 million & the 10M was in 1st Million but found the Golden Nonce so now the reward will be divided according to the computation power spent. 1M will receive more reward cuz he used more resources.

The computation power of the miners when summed up is the computation power of the Bitcoin

=> if the 51% of the computation power is with one individual or a pool, then centralization has occured

-> put constraint on the computing power of the Pool.

Date

Byzantine fault tolerance :-

↑ this is dependent on the honesty of miners

- a log is maintained about every miner, e.g a miner participated in 10 decisions & 6 of them were wrong, then what will network do?

→ All this should be specified in the consensus protocols ahead of time

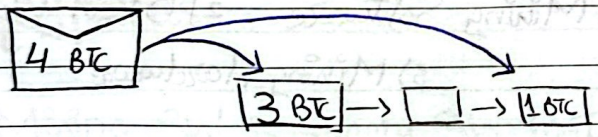
- depends on number of miners & their honesty, tolerence factor is 33 %

hungry

Transactions & UTXOs

↳ unspent transactions output

- crypto wallet does not hold your currency, it's on the chain



wallet holds pointers to the chain where you've done transactions

1.) Choose the smallest gap, like the closest, it may be individual or a combination of multiple.

! important : CHECK all Combos

Q. Where do transaction fees come from?

There is an escrow state (intermediate state), where your currency is held.

Date

Bitcoin Mining Pool :-

=> Mining pools are groups of cooperating miners that agree to share Bitcoin block rewards in proportion to their contributed mining hash power

=> desirable to the average miner as they make miner rewards more predictable

=> Miners can join & leave mining groups whenever they want, choose to redirect their mining/hashing power to a different pool at any time.

=> Main benefit is to generate more consistent payouts

=> Before joining a pool miners need : 1) Mining Software 2) Bitcoin Wallet
3) Mining Hardware

Largest Pools :-

1) Foundry → USA → mines 30% of all blocks
2) Antpool → China → mines 23% of all blocks
3) F2pool → China → mines 10% of all blocks
4) ViaBTC → China → mines 9% of all blocks
5) Binance Pool → Malta-exchange Binance → 8% of all blocks

How to join?

=> A need mining pool will only pay you if you have your own mining ASIC or hardware

Date

1) Get an asic miner : Asics are computers designed for bitcoin mining, connect your ASIC to the mining pool

2) Get mining Software : Connect your miner to the Bitcoin Network using Mining Software. Connect to the pool using info provided by the Mining Pool

3) Get Bitcoin Wallet : allows you to receive your mining awards, pool will ask you for your wallet address

All mining pools charge a fee & a real mining pool will only pay you if you have your own mining ASIC or hardware

Keypoints:-

- Mining SW is simply SW that allows you to connect your mining ASIC to the Bitcoin Network

- Cloud miners claim to have mining hardware that mines for you, mostly scams

- Mining HW is specialized computers created solely for the purpose of mining bitcoins. More powerful HW & more energy efficient -> more profitable it will be to mine bitcoins.

Mining Pool	Cloud Mining
They are for people who have mining HW to split profits.	Cloud Mining is where you pay a service provider to mine for you & you get the rewards

Date 7th March 25 Friday

Lecture 9 & 10 (After Mid I)

3 layers of crypto world:
1) Technology: blockchain <-> public / private/permissioned } 2 types of BC-based networks
2) Protocol: bitcoin / ethereum / waves / ripple / neo
3) Token: ICO (initial coin offerings)

Not necessary to attach a coin to the protocol. When the network is not published, the choice is of the developers if they want a coin or not but if the network is published, the update will only be possible if the working nodes agree (majority of working nodes).
e.g Hyperledger based solutions do not have coins

Bitcoin Protocol:-

-> Set of rules -> Verification -> Proof of Work
-> Digital Signatures -> Consensus Algos -> Decision-Making

Bitcoin & Ripple do not have tokens, Waves Ethereum & Neo have tokens

Q. Label Protocols (diagram will be given, label)?
Q. Which Protocols have tokens?

Satoshi Nakamoto gave a white paper in academia, white paper is a solution-based paper where they document their research, findings etc. Mostly for developers

Date

Bitcoin was solely made to introduce cryptocurrency.
When a developer issues a coin, they set the initial price of the coin, and provide proof to the government that we have e.g 21 million bitcoin etc

-> When Bitcoin was made, it had 21 million coins. 50 btcs were given to the miners as reward and in 2010 the price of the coins increased.

-> 21 million coins are made but not all are valid. They are made valid in points etc like 3.1, 6.5 etc

Bitcoin Ecosystem:

1.) Nodes
2) Miners
3) Large Mines -> govt institutes, big companies
4) Mining Pools

* 10 minutes is the Block Freq in terms of time. 10 min is avg time

Bitcoin Monetary Policy :-

1) The Halving
When 210k blocks are added in the Bitcoin, the mining reward becomes half
Approx 4 years

2) Block Frequency

Divide: $\frac{\text{block number}}{210k}$ = ans

if e.g 4 then divide

$\frac{50}{ans}$

Date

When bitcoin has 21 million coins which are valid then mining reward will become zero

The mining reward is coming from the protocal

When mining reward becomes zero then the transaction fees will be even more than the mining reward

→ Transaction fees are meant to replace block rewards

Cr

Date

~ Lecture 11 & 12 ~

- end of 2008 the BC was published, in 2009 it gained hype & in 2010, its coins got worth
- Ethereum is a BC-based protocol & is used to make more BC based networks
- ↳ core purpose to introduce a platform, you can make a new BC based network & your own currency & deploy these using ethereum
- similar to Playstore, have to pay & the code is verified & checked
- Use ethereum to make the applications live, decentralized cpp & your app is then available to all ethereum users
- You can code on Ethereum
- The copy of Blockchain is with all the working nodes but they also have the CODE as well.
- authenticity of code can be backtracked as well
- He basically (Vitalic) gave the concept of decentralizing the apps
- e.g like Facebook tracks our activity & preferences etc but in Blockchain based networks the data of end users is stored locally
- Smart Contract => an agreement done in code & is automated
- In Bitcoin initially you couldnt make Dapps, the coding is done in Bitcoin Script & originally coded in C++ (cuz gives a lot of control over memory)
- Memory / Buffer overflow
- For ethereum, main coding language is Solidity (made by Etherum)
- What does it mean if a language is Turing Complete ?
  - → can you implement all kinds of logic in this language ?
  - → languages which are not Turing Complete mainly do NOT have loops
  - → Code will be running autonomously so they dont allow loops for better control in Bitcoin
- -> Bitcoin Script is not Turing Complete

Date

Lecture 13-14

- coding files in BC are called smart contracts
- Solidity Question in Mid-2
  Truffle files why & where & what change

→ What is Bitcoin Scripting Language?
Bitcoin Script

→ What is Ethereum Scripting Language?
Solidity

(i)

When working nodes becomes a part of Ethereum & become part of chain, then the code files are also downloaded on your local machine

↳ So, if a virus comes in the chain or in smart contract then your system & data is at risk

↳ For virus mitigation, access to private files etc, Ethereum suggested to set up a Virtual Machine & then clone it over there so that the access to local hardware is denied

↳ EVM

(ii)

Since loops are very dangerous, so Ethereum penalizes the developers for using extra loops. Gas Cost to penalize the developers so and user is paying it. Developers pay money to Ethereum based on their code, system & computation. Both Dev + End User pay the Gas Cost. (service charges)

Date

Ethereum Currency : Ethers + Gas Cost

Why was Gas Cost introduced?

- The fluctuations in Ether depends upon fiat currency (normal irl currency) + how many end users are buying it. If more users buy ether then the market price increases.
- The fluctuation is very unpredictable.
- Gas Cost price is decided by the developers & it is a fixed price. Any changes in Gas Cost are done when majority of the nodes agree.

What kind of money miners get?

In Bitcoin : ① Transaction Fees
② Mining / Block Reward

* Imp : Write 3 properties of Proof of Work?

① Difficult to compute the puzzle
② Easy to verify the ans of the puzzle
③ Maintain the avg time

Mining Economics :

Mining Reward > Resources Spent => Profit

Date

How wallets work ?

PK : SK

Secret

- When you sign up on a wallet then you get [Public & Private] key
- If you have multiple accounts in a Bank, they don't have any specific link together
- Private Key is like your ATM Pin & Public Key is like your account number
- [Public, Private] key are a unique pair
- So crucial to store a Private Key
- Signature : Unique identity of User
- Signatures are used for verification

Date 18th April '25 Friday

After Mid-2 :-

- Bitcoin uses ECDSA : elliptic curve digital signature algorithm
- If private key is compromised then anyone can do your signature
- If you have 3 accounts, and the private key of one account is stolen so it does not mean that the other 2 are compromised as well or that private key can be used to steal the priv key of others
- ↳ No central point of coordination
  - ↳ Decentralized Identity Management

Q. Explain Decentralized Identity Management? (2) in final mark Question

* Bitcoin encrypts the public key using SHA-256, public key/address is your identity on the network

Node address

Public Key —SHA-256→ Bitcoin Address

Q. 2 important tasks of wallets

1.) send & receive currency
2.) store the private keys

Q. Do crypto-wallets have a backup?

-> HD Wallets : provides a backup of private keys
backup of wallet

if the keys are retrieved, only then we can send & receive transactions

(hierarchically deterministic wallets

Date

→ HD Wallets were introduced cuz before you could log in ur wallet only on one device & if that device was lost, you could lose your account as well cuz if you had not logged out of your acc, you cant login elsewhere

→ Master Key => Master Private Key (Seed phrase) : Mnemonic Phrase (Mnemonics)
12/24 words => it is a sentence, it is incoherent/non-sensical
only HD Wallet has a Master Priv Key
<-> retrieves the private key of all accounts

* The Master Public Key is used to retrieve all the public keys
* The Seed Phrase can retrieve all the wallet's keys
stored outside of the wallet for backup (one time download)(.txt file)

Key Store file: the private keys of the accounts in your wallet are encrypted & stored on this. Password-protected file & contains the encrypted version of your private keys

~ Not every digital wallet is a crypto-wallet but every crypto-wallet is a digital wallet

How do wallets work?

Categories of wallets: - hot
cold

Types of wallets: Software
Paper
Hardware

Date

Software Wallet :-

① Desktop Wallet ② Online Wallet ③ Mobile Wallet

HD Wallets : Main difference is that they provide backup

Block : [transaction data 40% / signature 60%] so if the signature is taking up so much space, then the miner will be able to add less transactions

Segregated Witness (SegWit) :-

→ segwit was introduced → the digital signature part of a transaction is segregated & saved seperately so this reduces the size of a single transaction. Size of transactions is reduced & this enables miners to increase the number of transactions in a block.

DAOs → Ethereum

- Generic organizations have roles e.g A cashier will do all the cash related work on a counter

So these roles introduce partiality & human error

So they decided to replace these humans & roles with Code files (also called Smart Contracts), work autonomously & no central authority, have fixed set of rules

↳ CODE is LAW

Date

- After being published, the developer of the DAO can not do any changes until or unless the majority of the working nodes agree:

So to introduce this concept Vitalic & his team came up with:

May
Investor-Directed Venture Capital Fund Stateless in 2016

in May DAO had: $150,000,000
after a transaction is made, the money goes to an escrow state & is held there for some time so in

June 2016: escrow state held $50,000,000 approved to be sent to an anonymous address

A hacker had found an error in the code & exploited it to send himself $50,000,000 so the entire team of ethereum & the ppl were shocked

So Ethereum released an Optional Update (Hard Fork)
↳ which divides the chain 2:

The update was that money can be returned to the escrow state to the owner/sender.

1 chain for those who accepted update
1 chain for those who rejected

Cuz of this Hard Fork Ethereum was split in 2 parts: Eth & Etc

Eth: Money returned to owner/DAO
Etc: (ethereum classic) → Money remains on child account/escrow state & will be transferred to hackers account after decided time limit

Date

Soft & Hard Forks :-

20 July, 2016 : HF on ethereum to change rules of smart contract due to DAO Attack

20 July, 2017 : SF on bitcoin to upgrade Bitcoin with Segwit Witness Feature

1 Aug, 2017 : HF on bitcoin to increase the Block size to 8 mb from 1 mb

24 Oct, 2017 : HF on Bitcoin to make ASIC resistant network

In Soft fork, the update is compulsory & the chain does not divide

On BitCoin Gold, ASICs can not be used for computation

Date 2nd May, 2025 Friday

Lecture 27 & 28

ICOs (inspired / → initial public offering (shares))

- initial coin offerings (related to IPOs in centralized world)

→ actual benefit of IPO is to raise capital for companies, the con is that the company has to share product details & units bought/sold (sensitive info) with the public

→ Vitalic & his company liked the idea of IPO but disliked the idea of sharing product details.

e.g Apple wants to raise capital in Blockchain world

① Apple will become part of a chain that has a token, Apple will apply for a token from the chain e.g (platform will provide Apple Coin)

② Apple company requested the platform for token & was given 1 million Apple Coins by the platform

③ The starting value of the coin is decided by the Owner

④ e.g Company bought each coin for 0.5 $ & now sells it to customer for $1 so this raises the capital for that company

⑤ 2 things can be done using these tokens:

① avail services using that coin

② trade

Date

⑥ Trading takes place when the coins are all finished & the demand has increased so the people that have coins can trade or sell coins to those in need.

* End User must read the specifications & the services provided by the company before purchasing the tokens.

White Papers: complete history / development & advancement of problems, used in academic world