

①

#20

08 Oct 2022

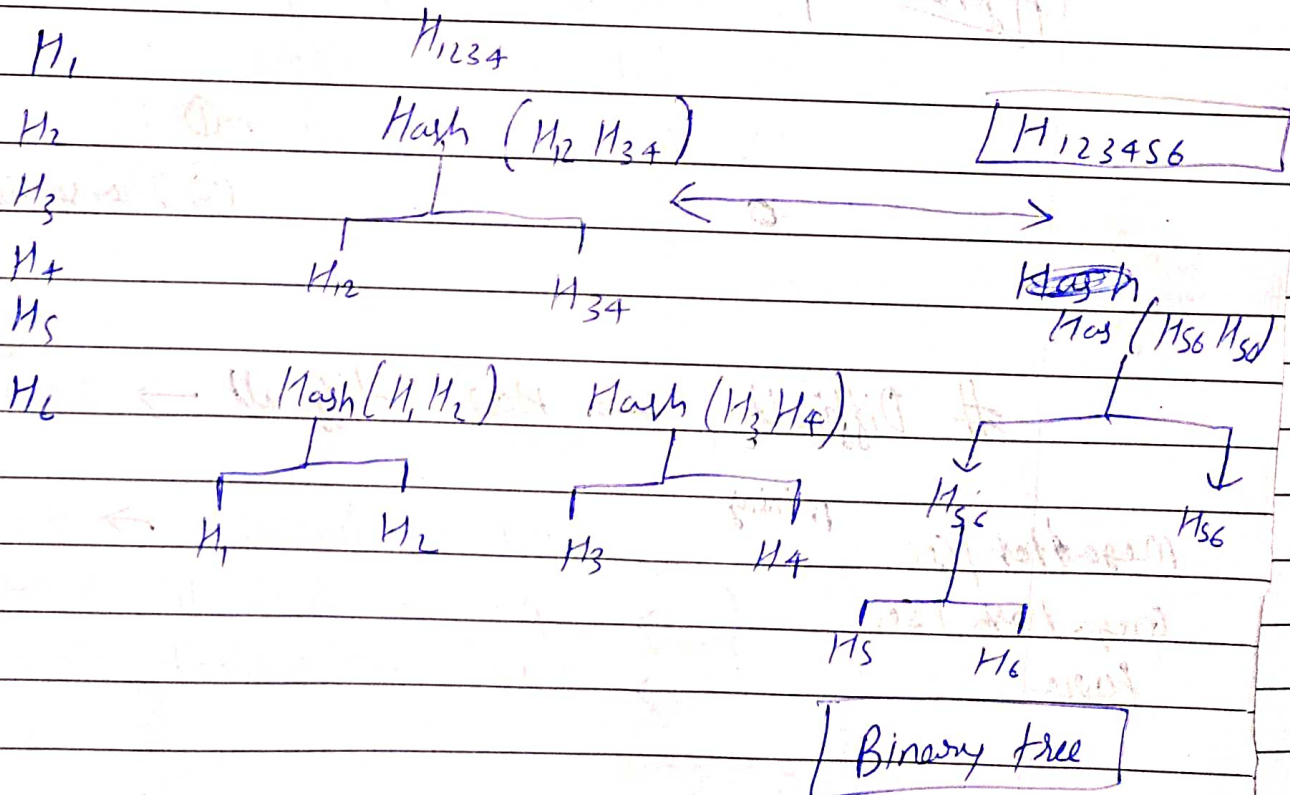
Today Agenda — Merkle tree

Segwit

Coinbase maturity

Coinbase Maturity → reward the miner

#Merkle tree



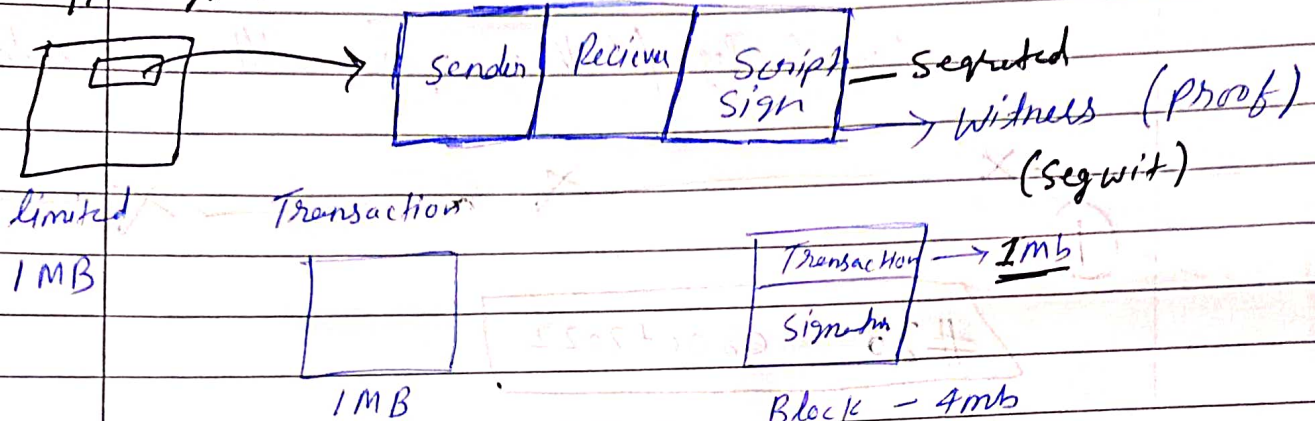
(2)

Fork - Copy data

\* Turing complete programming language

BIP (Bitcoin Improvement Process)

# Segwit



Hard Fork used

~~Hard Fork~~

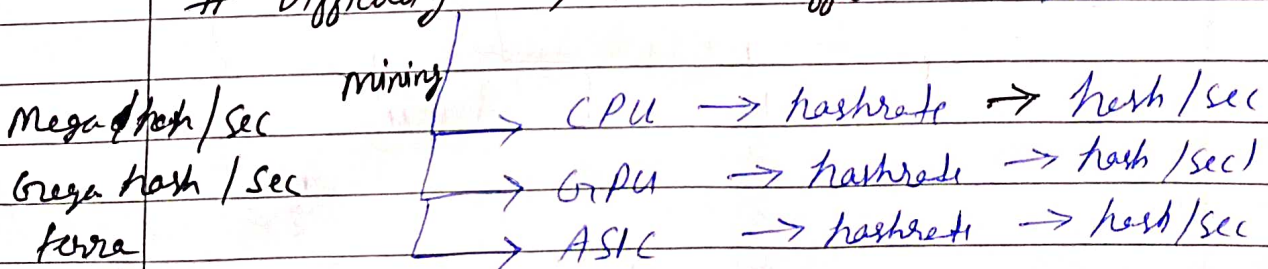
@ Sangeen Sth

Agenda -

Agenda

- 1) Calculate Difficulty
- 2) Block Creation fees
- 3) Consensus rules
  - ① Block cons
  - ② Transaction rules

# Difficulty → How difficult → guess nonce





③

Mastering bitcoin

1 mega meen - 1 lakh \$

1/1

Very easy to calculate nonce

Increase difficulty

2014 → CPU GPU

2019 → GPU ASIC

2022 →

Difficulty adjustment

→ Average time / block is 10 minutes

\* Every 2 weeks average block time check

↑ 1 Week of October → avg mining 15 min  
↓ 3 Week of October → avg time 10 min

10 min calculate → 2 weeks

2016 block

2016 2016 2016 2016 . . . . .

Certain block → fees structure

210000 blocks → reward divided

Coinbase reward divided by 2

50

25

12.5

6.25

miner control the price

Price of BTC increase

④

- 4 year halving cycle
  - 2140 → 21 million
- ↑↑      ↓      no mining reward  
transaction fees increasing

## # Protocol rules

# Consensus mechanism → part of blockchain

Architecture

Proof of concept

Bit coin consensus

Proof of Work

list of rules

## Syntactic correctness

Transaction

amount

UTXO

Block

prev hash

out pub

merkle root

\_\_/\_\_/\_\_

Block / target hash

Block no  
+  
correct nonu  
+  
all hash  
+  
prev hash

Tomorrow Agenda

- Modules
- Events
- Create a Server

Bitcoin Whitepaper  
↓ story mode

X

X