Lecture 03: Proof of Work

https://andersbrownworth.com/blockchain/block

https://www.ibm.com/think/topics/blockchain
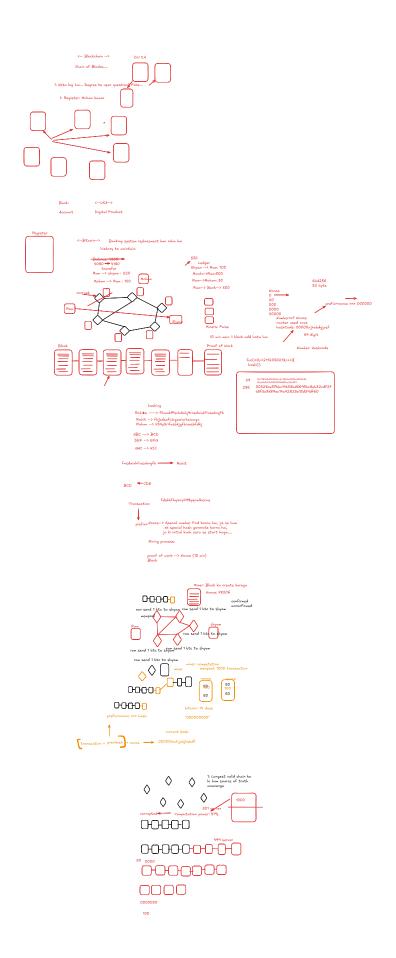

Artucle Reading

1. https://www.geeksforgeeks.org/computer-networks/sha-256-and-sha-3/

2. https://www.movable-type.co.uk/scripts/sha256.html

Prefix + nonce ⇒ Hash

[Transcation + Prev Hash] + nonce → 000scvdfvasvvd

<-- Blockchain -->

Chain of Blocks.....

DU CA

1: Neta log hai... Degree ke upar question/Fake....

1: Register: Mohan kumar

.

Bank: <--USA-->

Account   Digital Product

Register

<--Bitcoin-->   Banking system replacement kar raha hai
                 history ko maintain

Balance: 1000
4080 → 9180
transfer
Ram --> shyam : 220
Mohan --> Ram : 100

570
Ledger
Shyam --> Ram: 100
Moshn-->Ram:500
Ram-->Rohan: 30
Ram-> Bank-> 300

Mohan

corrupt

Ram

Shyam

Miners: Paise

10 min mein 1 block add hota hai

Sid4256
32 byte

Nonce:
0
00
000
0000
00000

prefix+nonce === 000000

Number==? Nonce:
number used once
hashCode: 00000xjhxtdgjasF
69 digit

Number: Hashcode

Block   Proof of Work

for(n=0;i<2112030213;i++){
  hash(\)
}

39   :3UTEP6U5f0NG2u7c782fvD1BSzE9PS97h
      4Hjd4LuF4hZS940GLHDLuW4yt4
286   D0328ce576bc19b33bd6695bc8eb32cdf2f
      b5f3a7d89ec14a42125c15d39df60

hashing
Rohit: -----> Fihwohffsvbdohj9rnsdaivhFiusokngfb
Rohit --> Fhjkdsafjuhgwzivrkeiwvga
Rohan --> 434y3rifosbkjgfbiwadsfdkj

ABC ---> BCD
DEF --> EFG
GHI --> HIJ

Fnsdaivhfiusokngfb ------> Rohit

BCD ← CDE

Transaction   fdskhfhwjory998yyowkerwg

prefix+Nonce--> Special number find karna hai, jis se hum
                ek special hash generate karna hai
                jo ki initial kuch zero se start hoga....

Mining process:

proof of work --> Nonce (10 min)
Block

Miner: Block ko create karega

Nonce: 48206

confined
unconfirmed

ram send 1 btc to shyam   ram send 1 btc to shyam

mempool

Ram

shyam

ram send 1 btc to shyam

ram send 1 btc to shyam   ram send 1 btc to shyam

ram send 1 btc to shyam

miner   miner: competition
        mempool: 1000 transaction

nonce   nonce
50   50   50
         50   100
         50   50

bitcoin: 14 days

'000000000'

prefix+nonce ==> hash

current Hash

[transaction + prevHash + nonce] --> 00000bcvhjahjhshdf

1: Longest valid chain ko
hi hum source of truth
maanenge

1000

501 server
corrupted ← Computation power: 51%

499 server

50   0000

0000000

100