① ~~#13~~ Blockchain #17

DATE: / /

PAGE NO.:

24 Sep 2022

Agenda → Demo Basic blockchain

Today Agenda

1) Hash
2) Block
3) Block chain
4) Distributed Blockchain
5) Asymetric Cryptography work

# Hash SHA 256 → (Bitcoin)

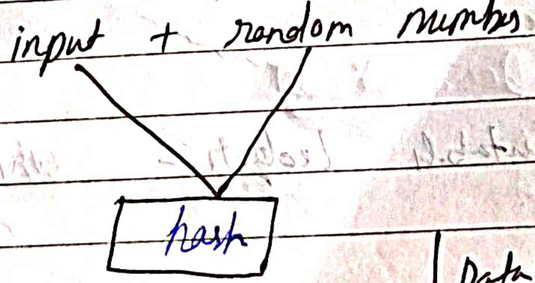
properties 1) Every hash is 64 characters long

64 key

- Changing one single letter change completely full change.

particular input → hash is always (–, . etc)

Deterministic

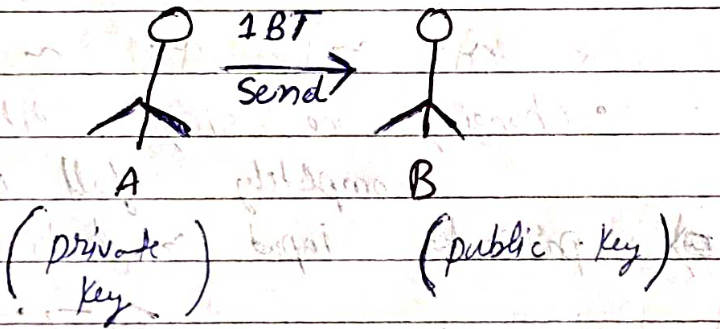


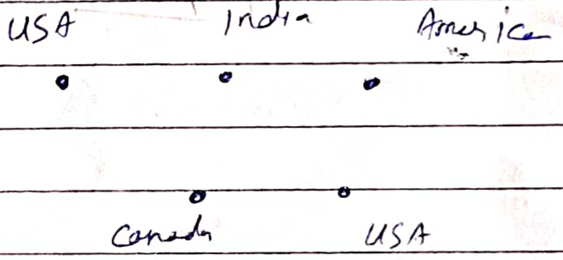
Data:

Hash:

# Block

Block : 1
Nonce : 85869
Data : tx1 - a-b
tx2 - c-d
tx3 -
tx4 -
Hash : 64 character





- Once data entry that's no change data future.
- Immutable ledger - Which means once add no change data.

NONCE - Number only once

# decimal 0-9
hexadecimal 0-9 a-f

10 unique element 16 characters
6 unique element 0000
0101

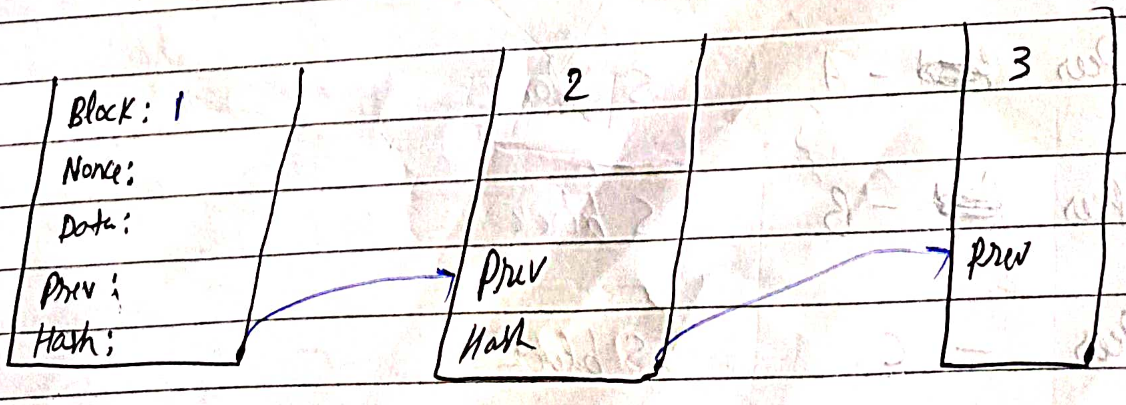
64 x 4bit/character = 256 bit / 64 characters

SHA 256 — Numbers of bits
(0-9) + (a-f)

SHA512 new algorithm

# Blockchain

- Bitcoin
- Etherium
- Polkadot



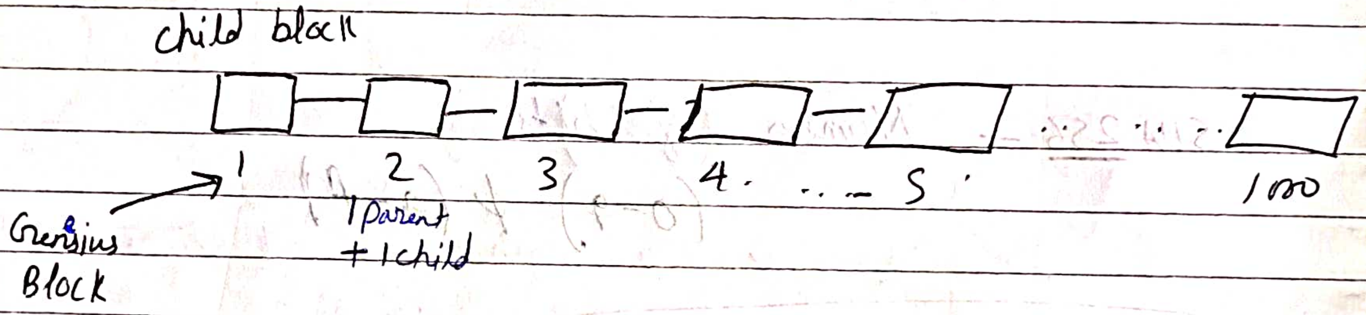
Mine – check authentic or not
Green ✓
Red ✗

## Hash chaining

Combined data stores

## Block chain

• It is block & chain of all block combination to connect



hard coded → file → code of first block.

1) Genesius Block → 1 child → Creator of blockchain (Mother)
2) Block → 1 child + 1 parent

## # Distributed (Decentralized)

Peer – A 5 block

Peer – B 5 block

Peer – C 5 block

Block chain Voting

- there are three people

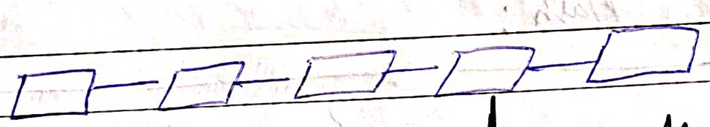
2/3 66.6% → Authentic

- 2 people 0006e469
- 1 — 000c.age

Why decentralized secure?

majority win

Peer A



↓ centralized why?

One person only controller,

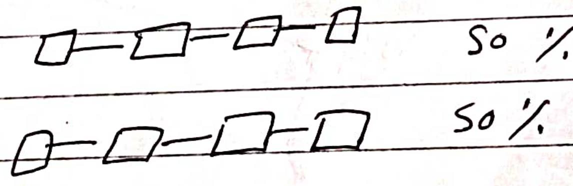
Mutable – changed data

immutable – can't be chang data

ex– North Korea is centralized

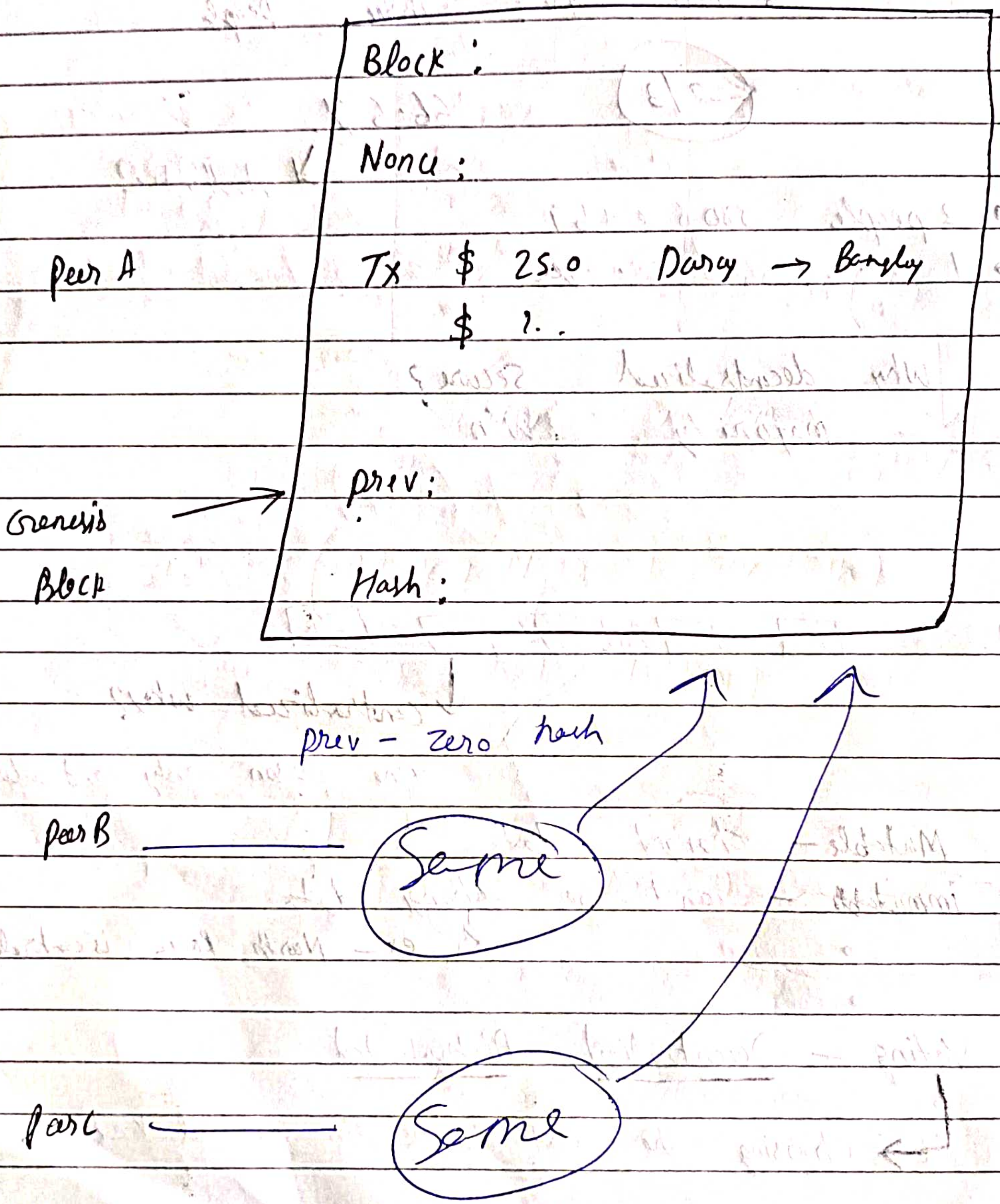
Voting – Decentralized, Distrubuted

→ Choosing the next block in the blockchain.

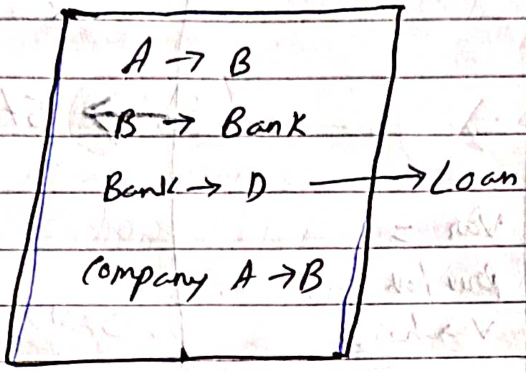


Who add one more block & fast who win

# Tokens


Block :
Nonce :
Tx $ 25.0 Darcy → Bangley
$ ?..
prev:
Hash:
Peer A
Genesis Block
prev - zero hash
Peer B
Same
Peer C
Same

Account of HDFC Bank



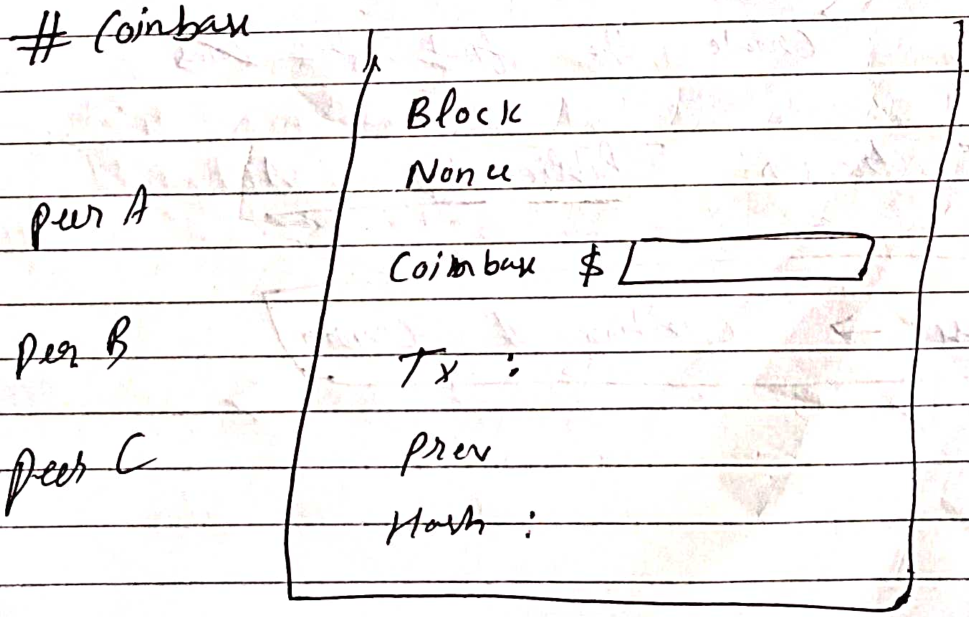
Ledger

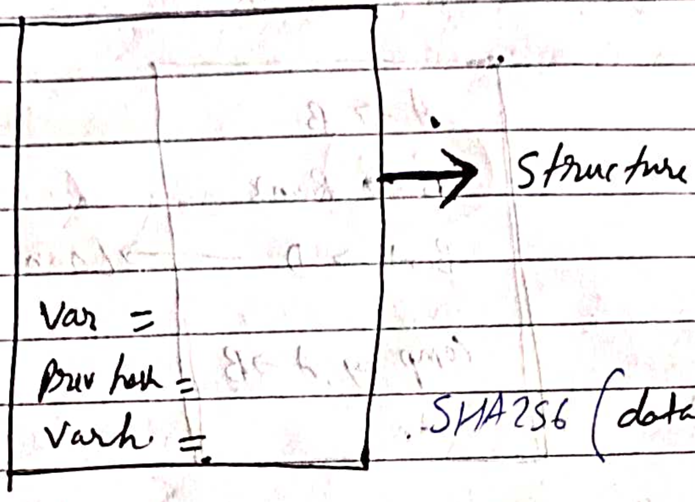
Blockchain → Cryptocurrency tx .(transaction

Money → store of value

Money → Gold reserves
↓
Valuable

# Coinbase





SHA256 (data + nonce + block)

↓

SHA256 (String + number)

Software dev team

SHA 256 (Block + Nonce + Prev Hash)

↓

Random Numbers

Reward will be generated

Genisis → Miner A

Create the first few coins

20BT transfer Public key of A

Coin base → Creation of Crypto

9

DATE : / /

PAGE NO. :

★ Who circulate crypto currency?

Node → circulate cryptocurrency

21 million → Ethuerium

Rules based System

Bit coin Software — Github

fork

24Sept 2022

#17

JAVASCRIPT

DOM — HTML + JS

Debugging → Project → idea → requirements

{ Frontend — HTML + CSS + Javascript
{ Backend — Database + API + interface

Testing — Debugging

(10) latency - On click button

Debugging - Testing functionality + error identificate + response time + latency

function -

→ code filese → Javascript

⇒ debug.html

```
          <script type = "text / javascript ">
          </script>

       < input  id = "t1"  placeholder = "text1"  type = "text" />
                                              <br> <br>
   < input  id = "t2"  placeholder = "text2"  type = "text" />>
                                              <br> <br>
   <button  onclick = "addition ()"  id = "btn Addition">
                                              Add/concatnates
     </button>

     <h2  id= "output" > </h2>

            function    addition () {
                let   a = document. getElement By Id ('t1'). Value;
                let   b = document. getElement By Id ('t2'). value;
             doument. getElement byId ("output"). inner HTML
```

inspect > Source> left hand side > call stack

Task - Try use all dom files