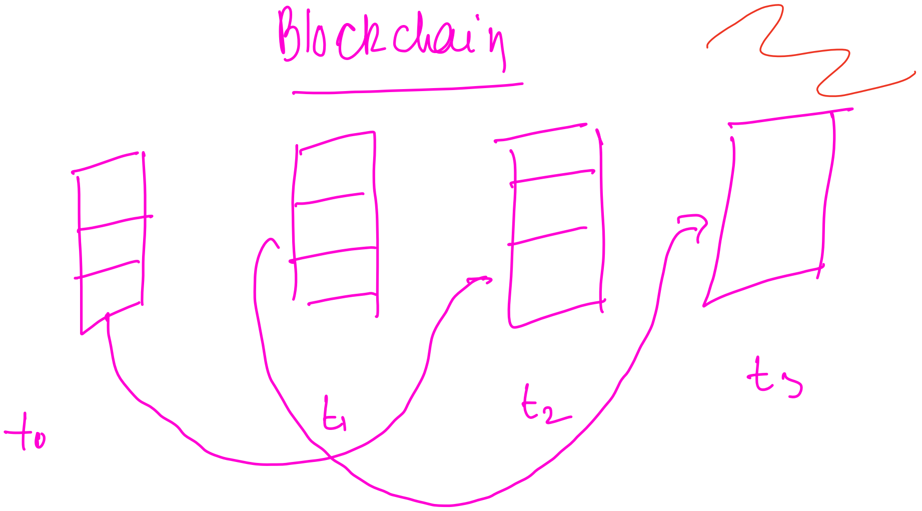
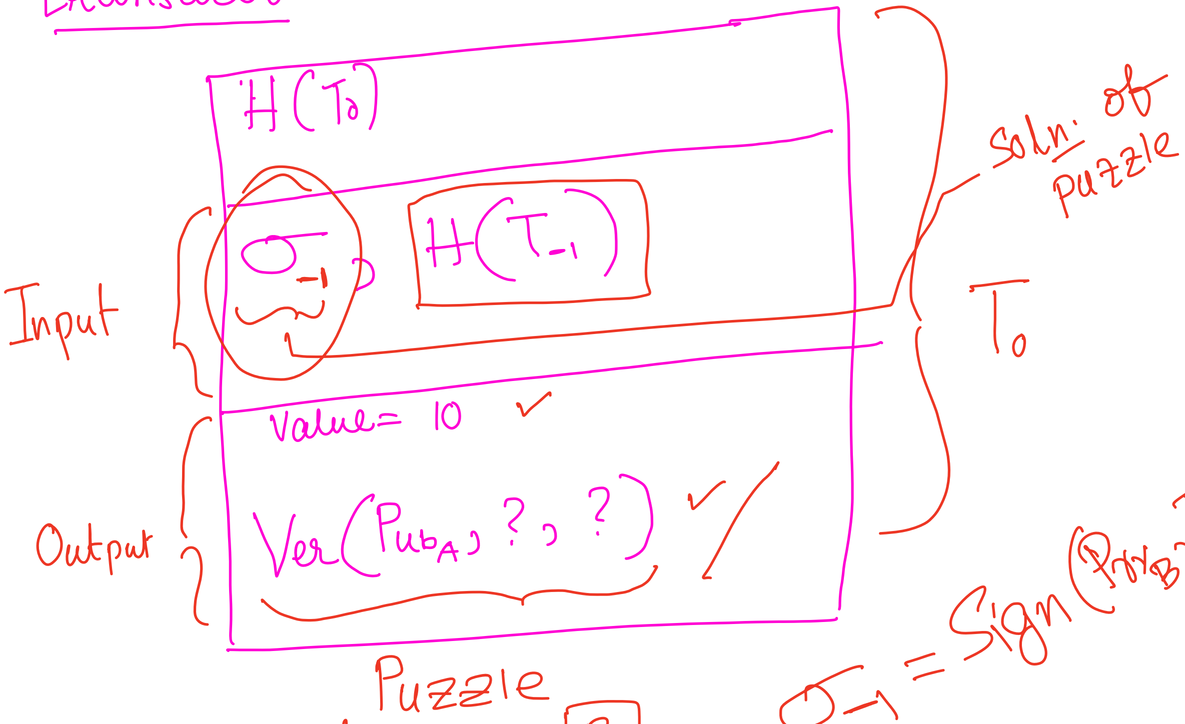
Blockchain



Blockchain

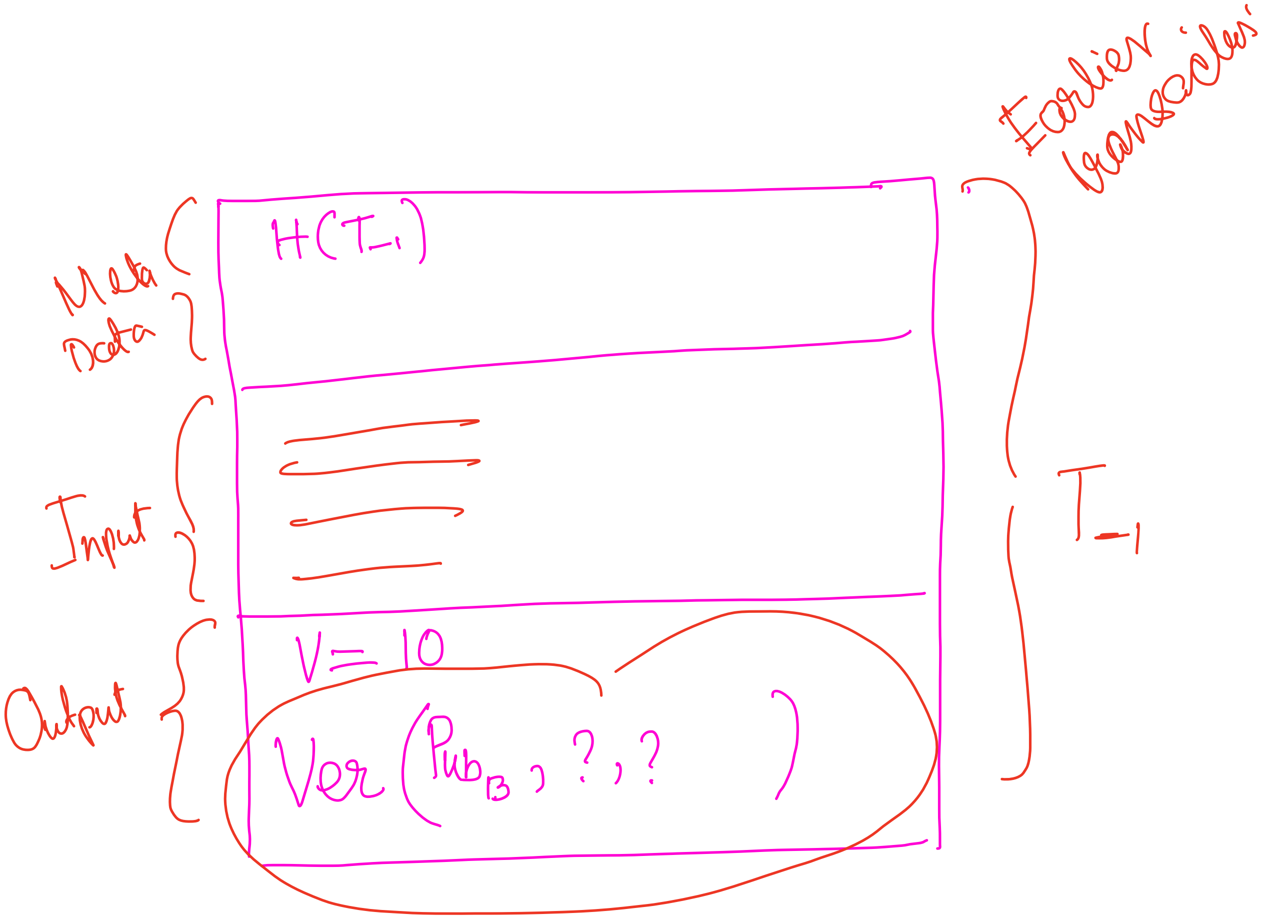
Later transaction

A transaction



$$\sigma_{-1} = Sign(Priv_B, T_0)$$

Who created T_0? $\boxed{B}$



- How to prove that T_0 Redeems T_{-1}?
- How to prove that T_0 is VALID w.r.t. T_{-1}

$\Longrightarrow$ σ_{-1} is okay with

$$\mathrm{Ver}(Pub_B, \underline{?}, \underline{?})$$

$$\Longrightarrow \mathrm{Ver}(Pub_B, \sigma_{-1}, \underset{\uparrow}{\underline{\boxed{message}}}) = 1$$

which message

↑

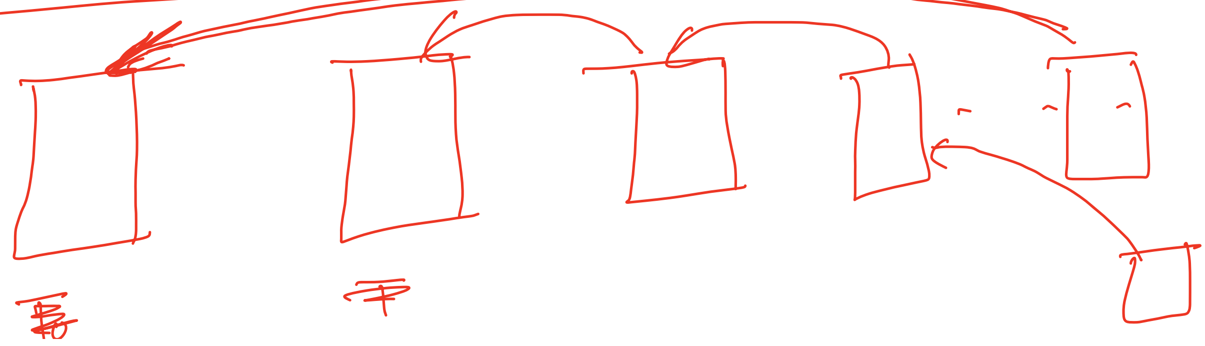
T_{-1}

how

$$\boxed{\sigma_{-1} = \text{Sign}(\text{Prev}_B \; , T_0)}$$

How all the transactions of a Blockchain are connected

Transaction Chain



timestamp

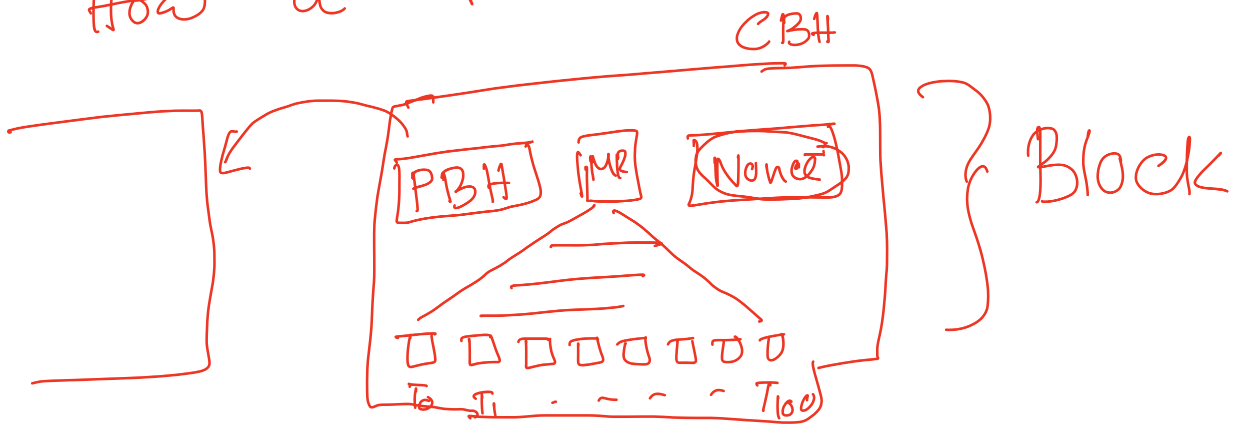
$t_0 < t_1 < t_2 < t_3 < t_4 < t_5$

- All nodes in Bitcoin network are generating transactions and broadcasting it.

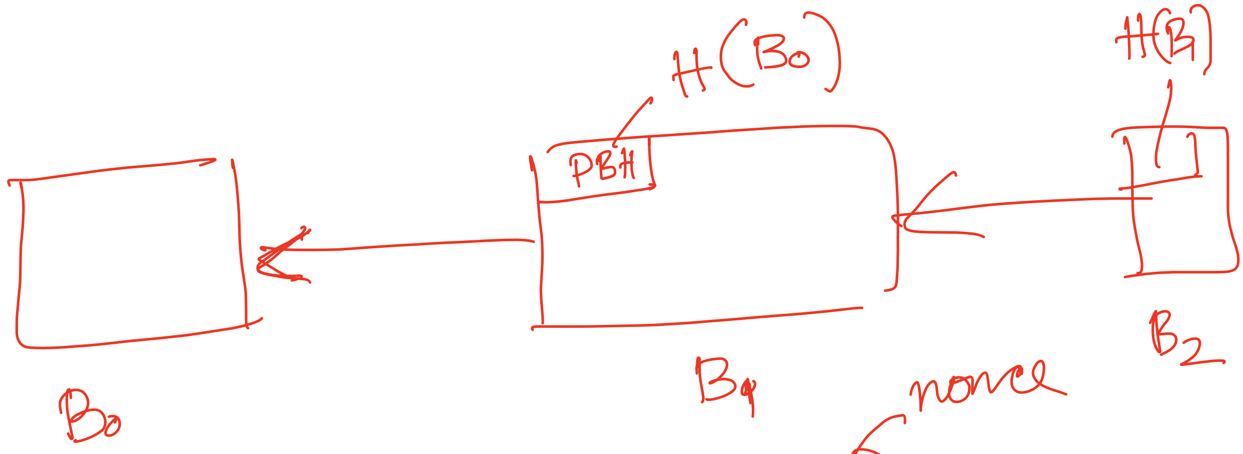
- How and who validates transactions Network-wise.

- All nodes are collecting transactions and creating BLOCKS

How a Block looks like



PBH = Previous Block hash



$$H(PBH, T_0|T_1|T_2 \cdots |T_{400} \,|\, \overset{\text{nonce}}{\boxed{x}}) \quad , MR$$

$$= \underbrace{000000000}_{200 \text{ bits}}$$

Solve for x?
from the above equation?