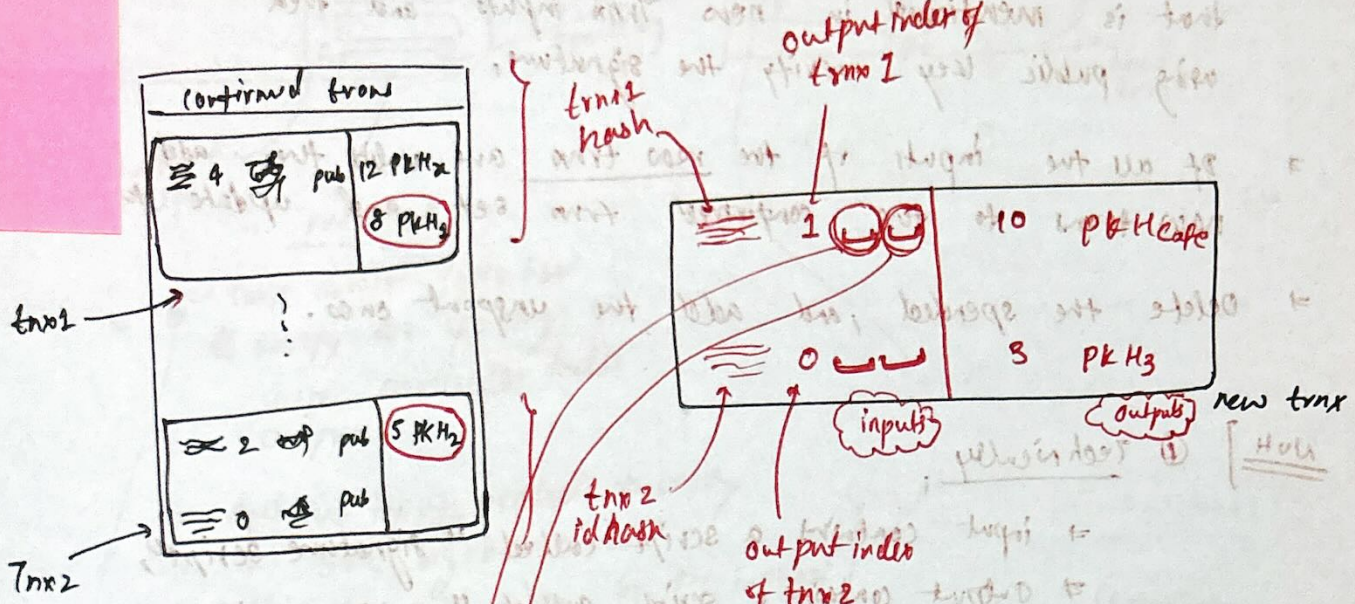
# Bitcoin

## # Transactions




⇒ A trnx can have multiple inputs, each input will have trnx id hash, output index, etc.

public key of (PkH3)

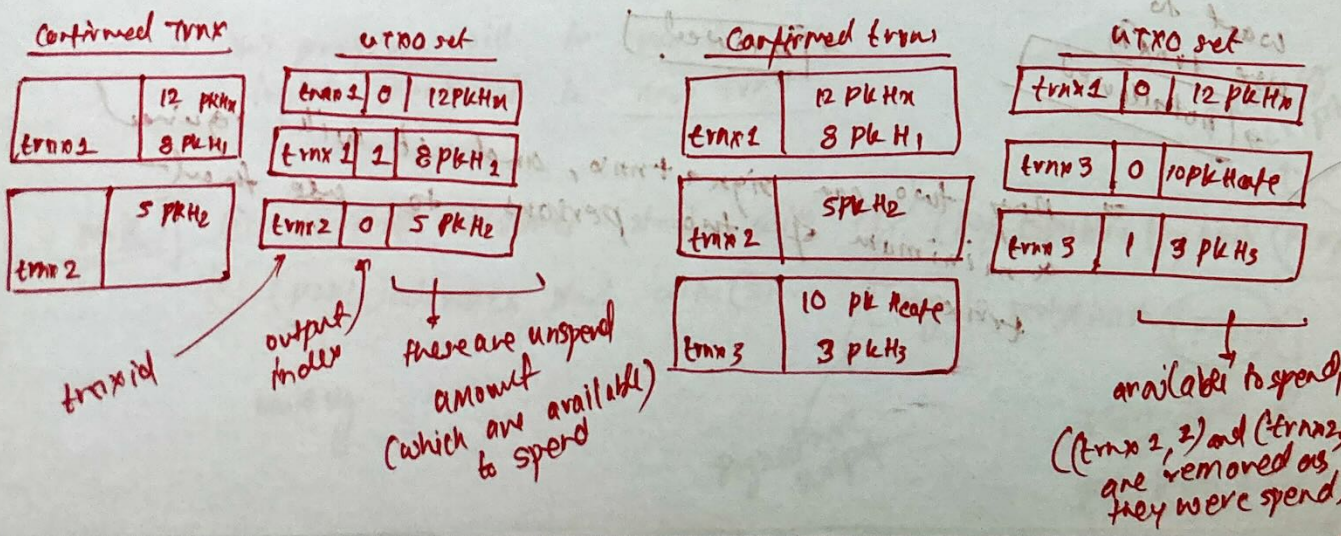
⇒ A trnx can have multiple outputs, each output have amount, and public add to which that amount send.

In order to spend 8 coin you need to provide a signature of (new trnx hash + earlier index) with "PkH1 private key".

⇒ total input amount = total output amount (i.e 8+5 = 10+3)

## # unspend Transaction output set (UTXO set).

Earlier → Now



## To check a new trnx inputs are valid or not

⇒ then find the trnx id with output index, from UTXO set, that is mentioned in new Trnx inputs and then using public key verify the signature.

⇒ If all the inputs of the new trnx are valid then add new trans to the confirmed trnx set and update the UTXOset.

⇒ Delete the spended, and add the unspent ones.

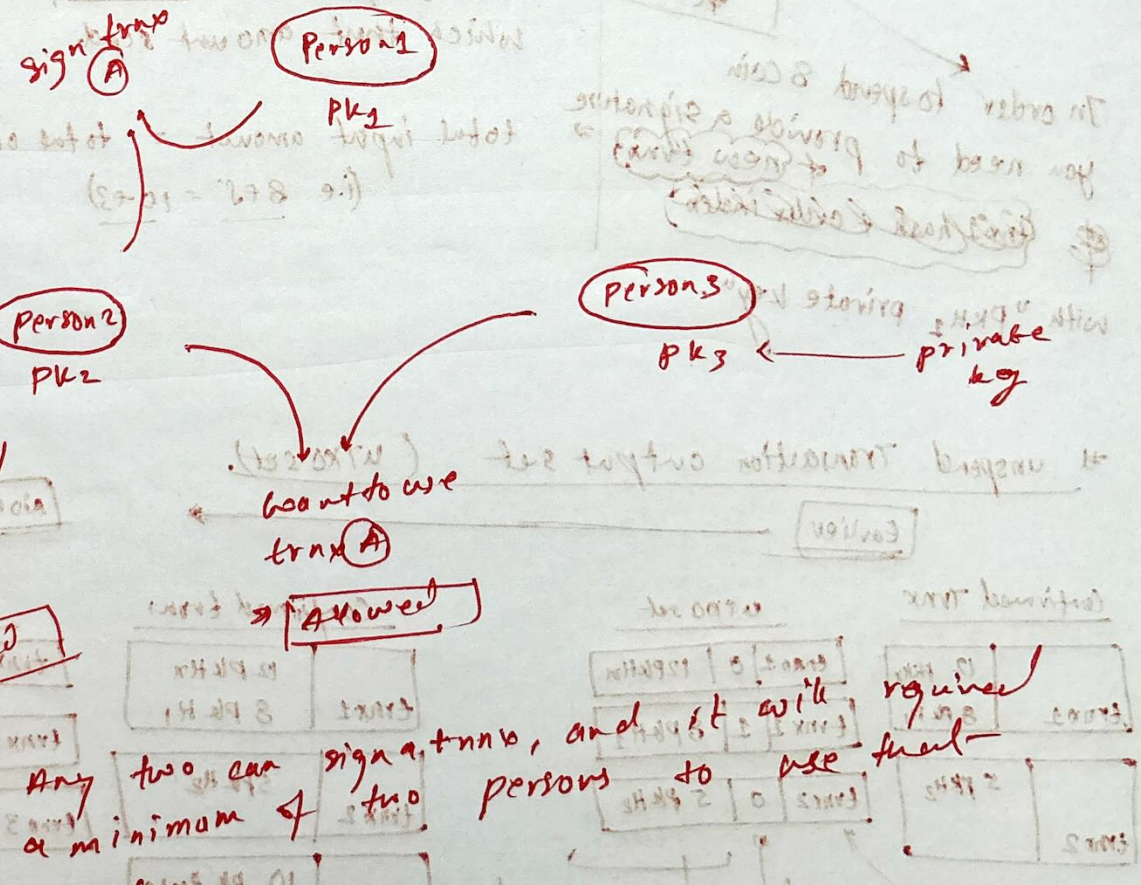
**Note** ] ① Technically,

⇒ input contains a script called "signature script",

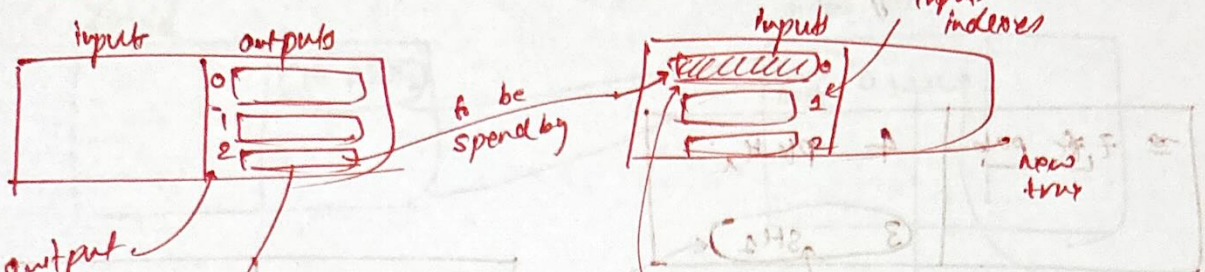
⇒ output contains a script called "pubkey script".

## Multi sig

Example: 2 of 3 multisig



# Scripts (for normal addresses)




**programs**

⇒ code which tells how to verify the spending of these particular index outputs

⇒ And the inputs needed to verify it like signature, and public key is given by the inputs of the trxn that is using it

signature
public key
} from inputs index

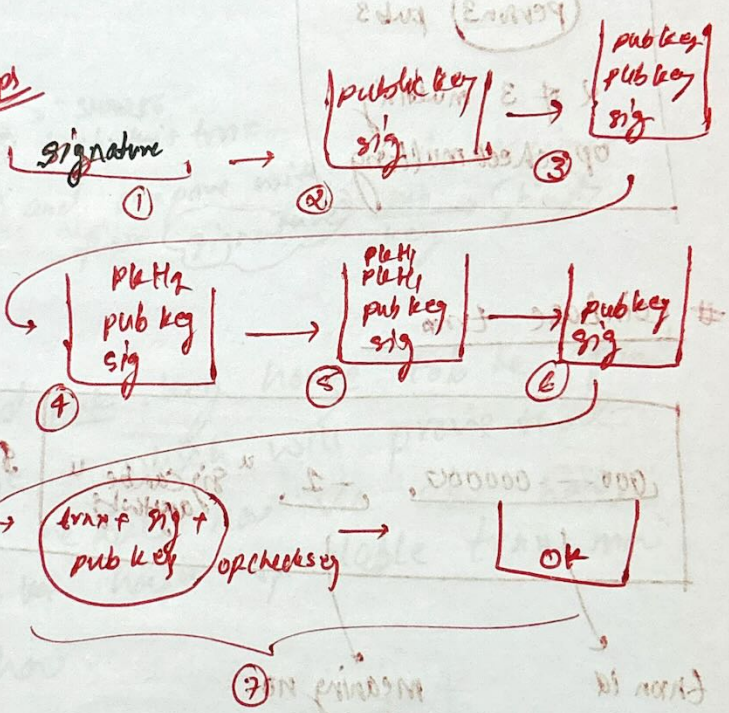
Signature script

from outputs index

- OP_DUP
- OP_HASH160
- PkH2
- OP_EQUALVERIFY
- OP_CHECKSIG

pub key script

steps




⇒ This program will be run for all inputs mentioned in new trxn.

**note**

① Normall addresses start with 1, (pay to public key hash P2PKH)

② P2SH addresses start with 3. [pay to script hash (P2SH)]

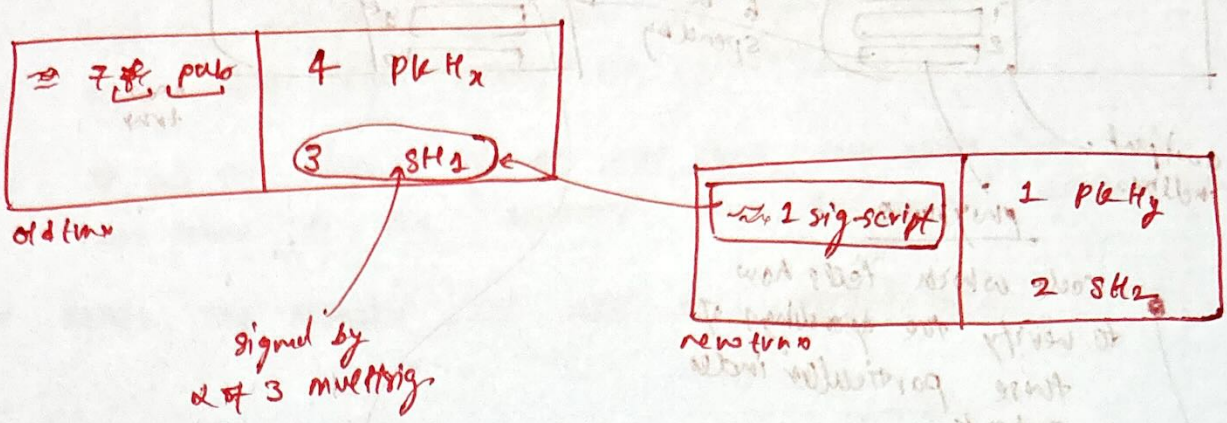
P2SH → multi sig

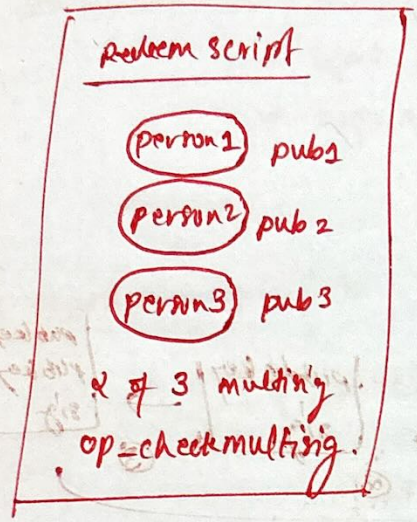
pub key script

signature script

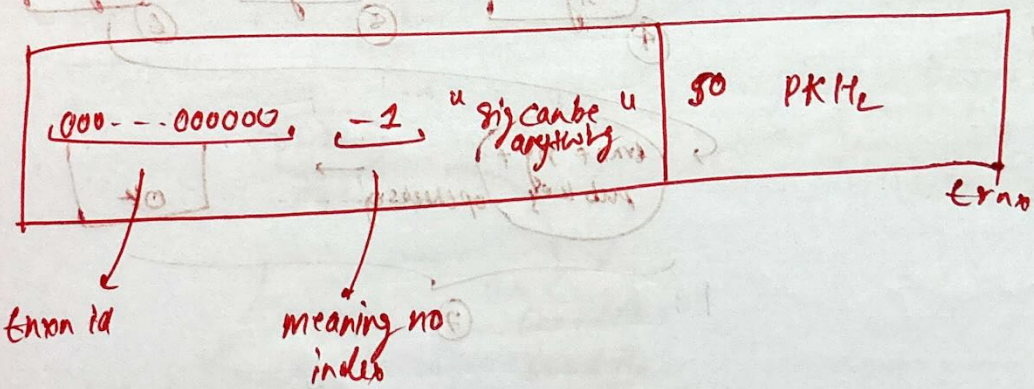
redeem script & pub key script

# script (for multisig)

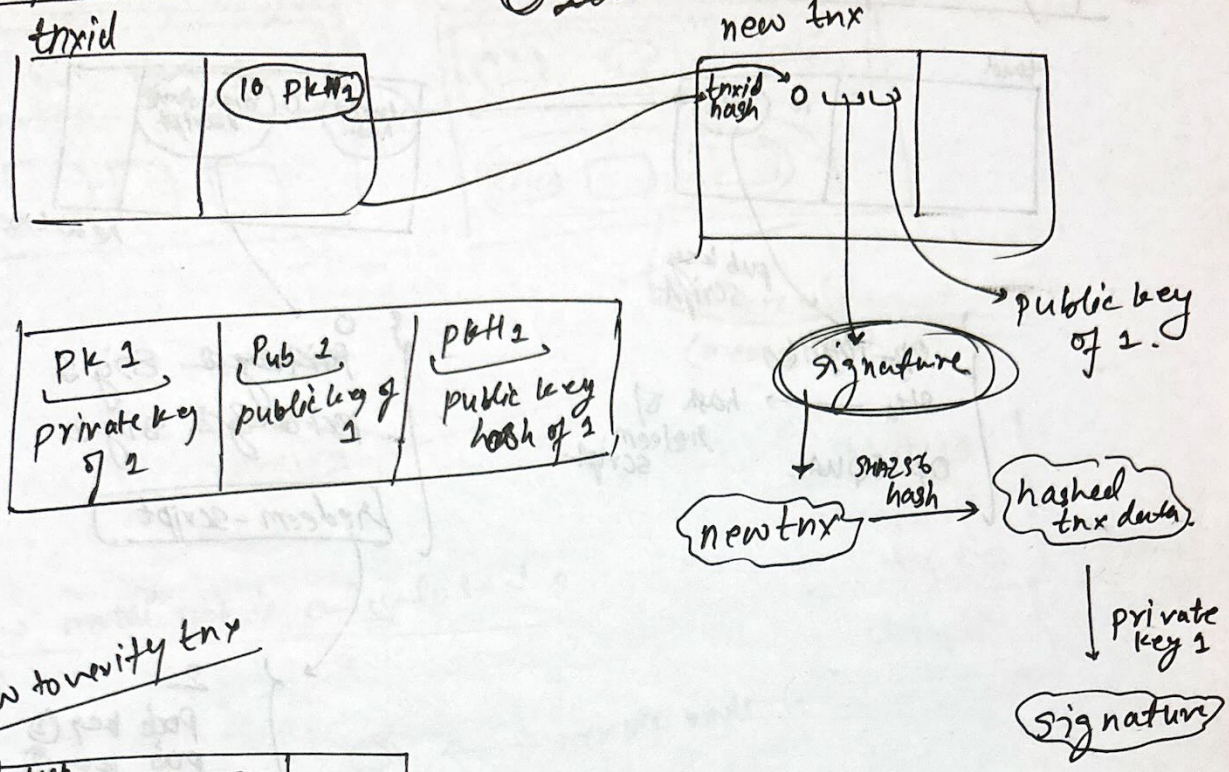



# coinBase txn

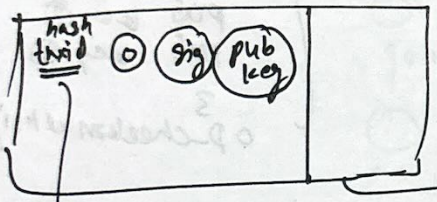


# pay 2 public hash




## (A) How to craft tnx

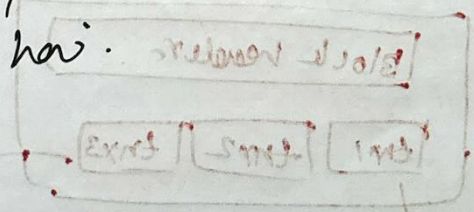
## (B) How to verify tnx



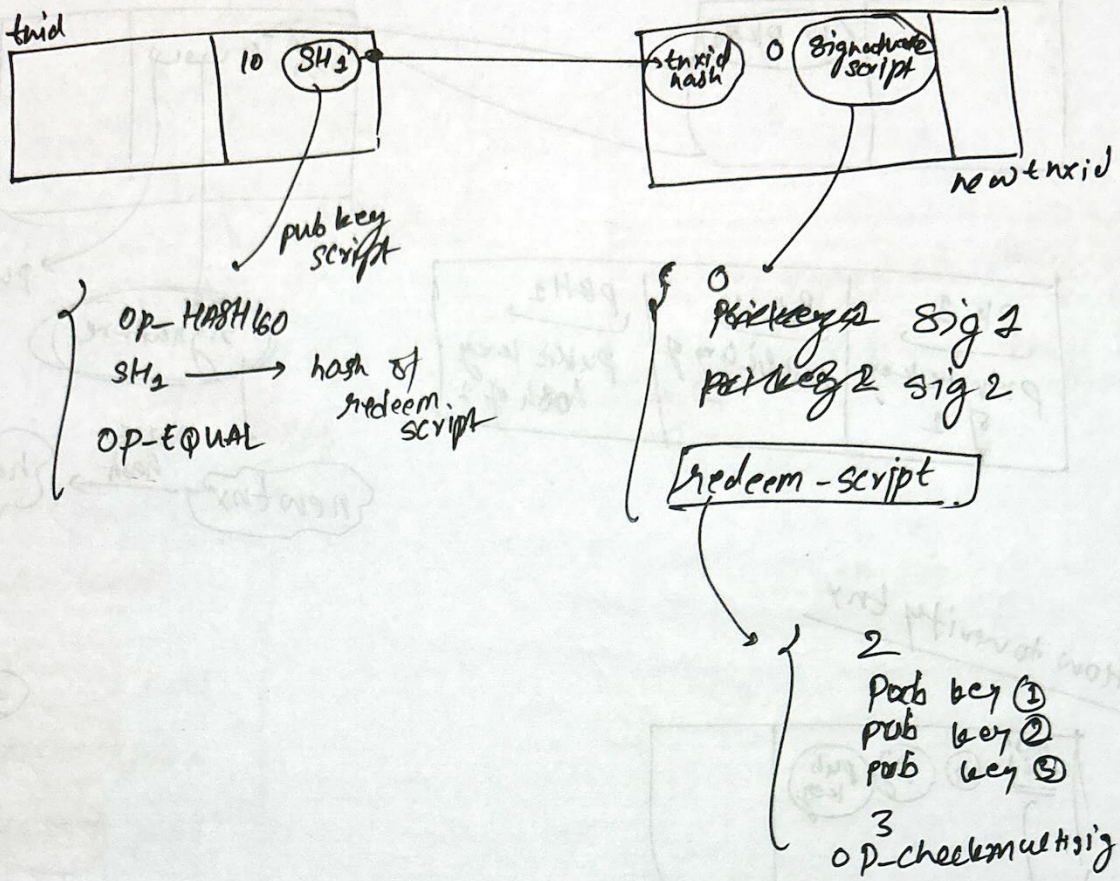

Step
1. get UTXO token
2. get public key hash
3. SHA256 hash this tnx
4. and compare with signature from hash received pub key hash

**kaise chalaye**

⇒ Agar aphe pass pri and pub key honge tab he apan sig nature bana payenge, which will prove that jo public key apan ne dali hai vo sahi hai, and wahi public key ka hash spendable tnx mai hoga, so apna he hai.

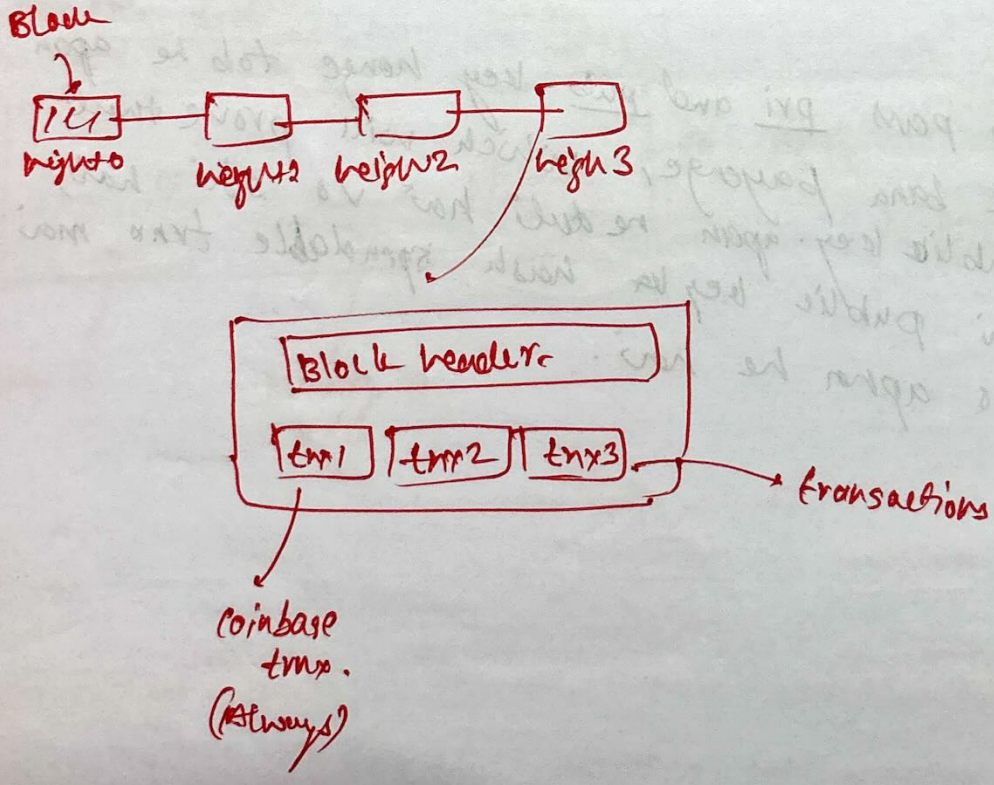


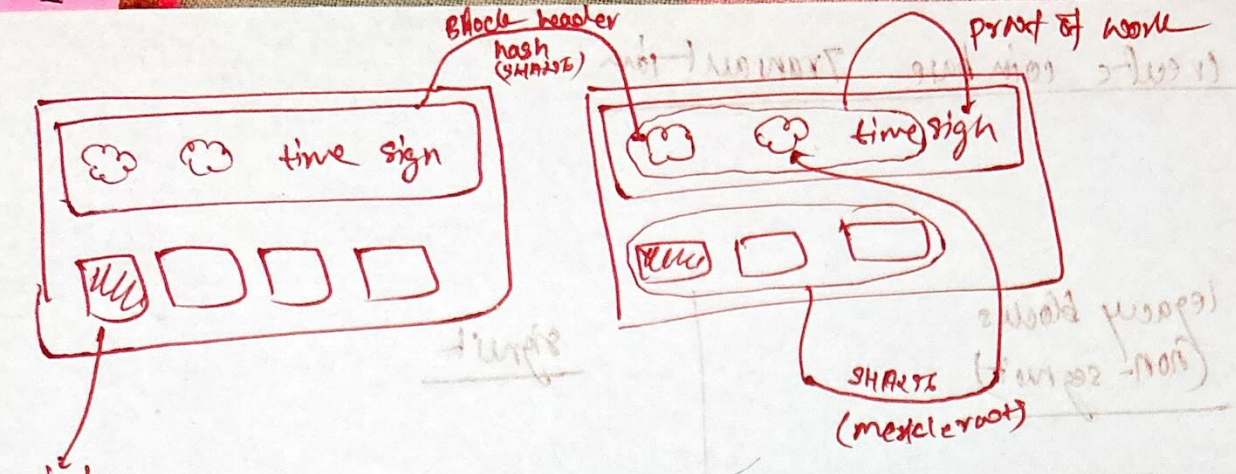
# pay to script hash (P2SH)



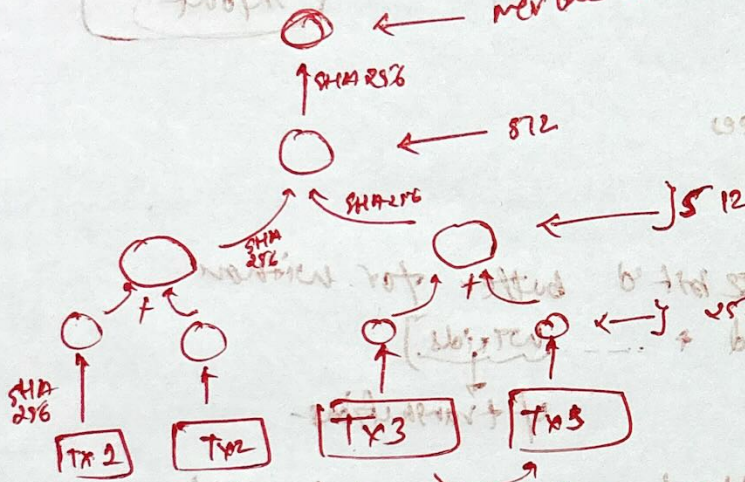

---

## Block chain

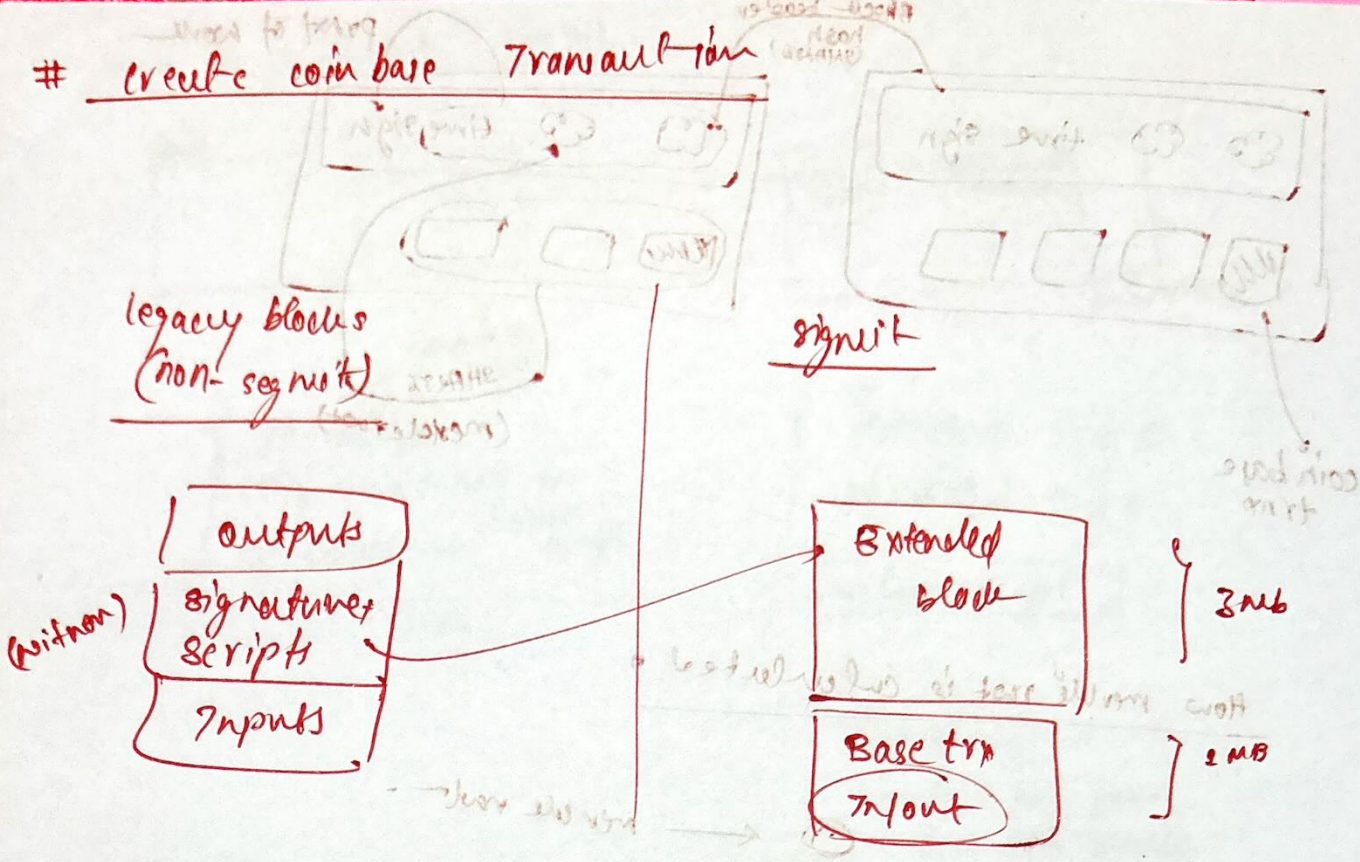





How merkle root is calculated ?



# create coinbase Transaction




NEEDS
↳ amount: fees
↳ transactions.

step ① Create 32 bit 0 buffer for witness
output ② [witness Id + ..... wtxids]
↳ of transactions

③ witness root hash = merkle root (wtxids);

④ Double SHA256 of (witness root hash) + (wtxid of coinbase)

⑤ script pub key = (6a24aa21a9ed) + (step 4 result)
↳ data op_return
for segwit safety

⑥ amount = 0

output ① step ③ amount = fees
② address = miner address.