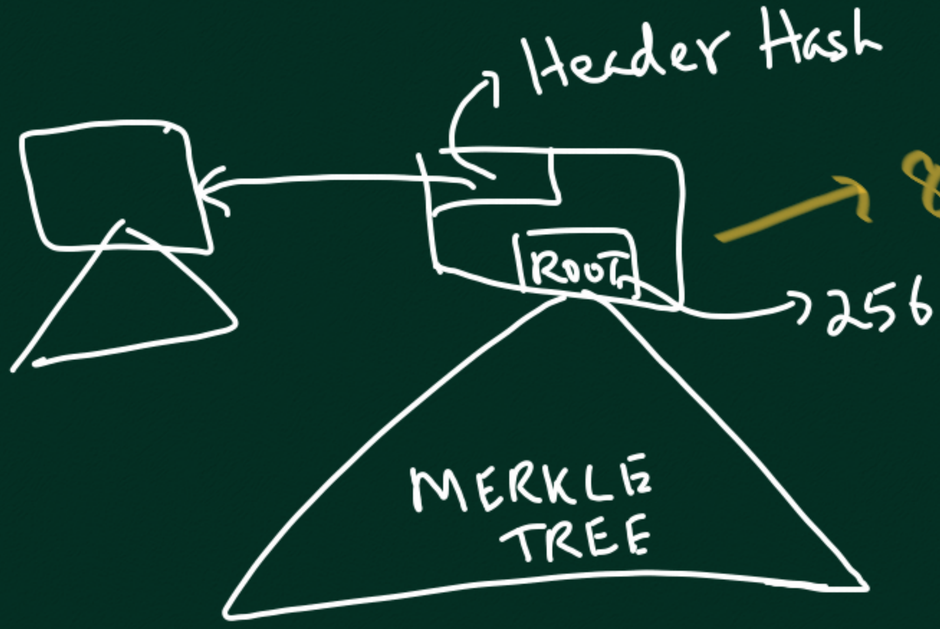


< 1MB (Satoshi)

Attendance

DIGITAL SIGNATURES.

ELLIPTIC CURVE CRYPTOGRAPHY

NIST

FUNCTIONS

(1) GENERATE KEYS (SIZE)

↓

(sk, pk)

↓ public

↓ Secret key

sk —easy→ pk (FOR ELLIPTIC CURVE CRYPTO)

pk —HARD→ sk

(2) Signature ⟵ SIGN(message, sk)

(3) isvalid ⟵ Verify(message, signature, pk)
(1/0)

ECDSA : EC Digital Signature Algo

	Size (bits)
pk	512
sk	256
message to be signed	256
Signature	512

A B

(sk_A, pk_A) (sk_B, pk_B)

Bitcoin Acct. #

3 BTC

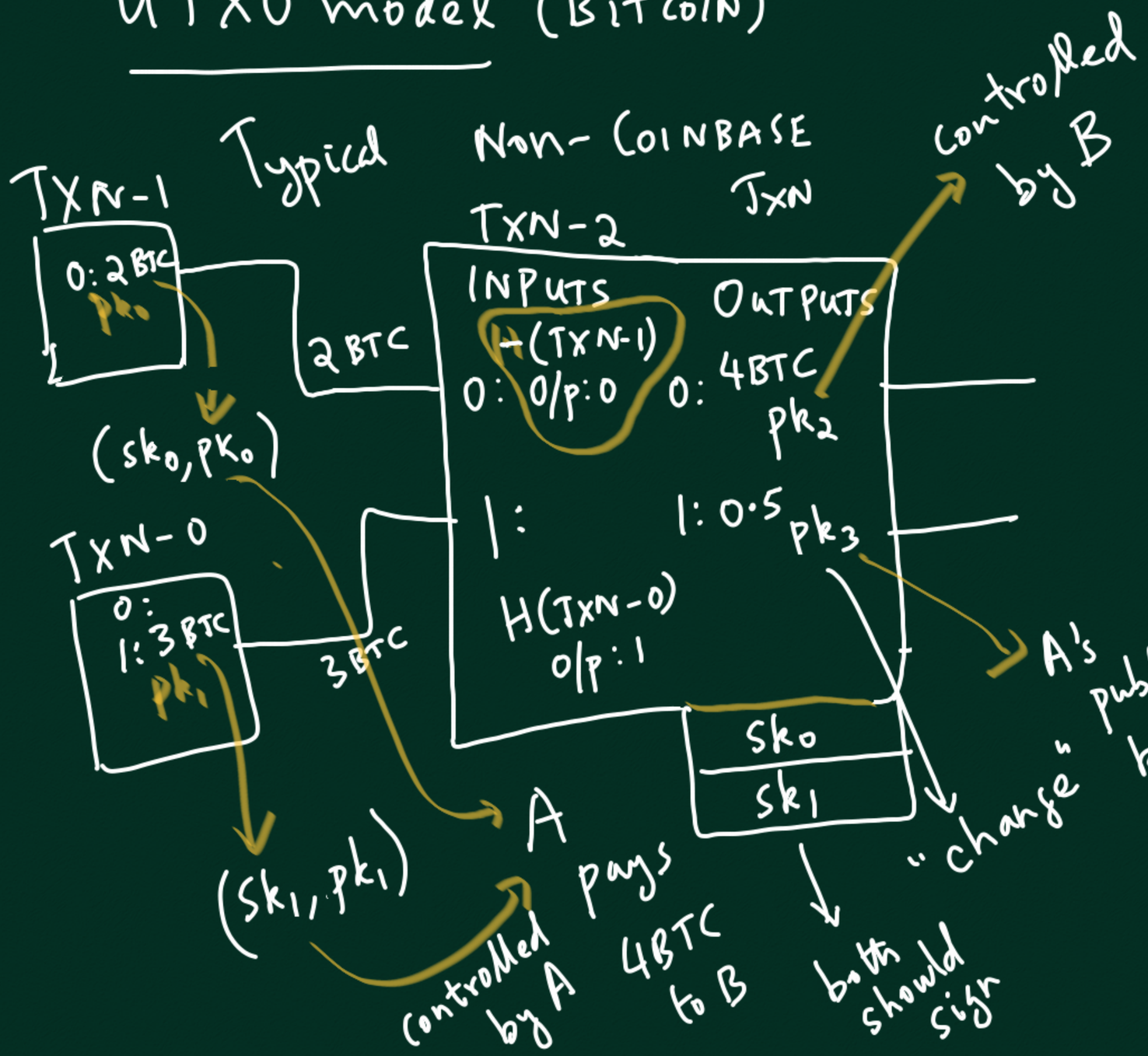
Pay 2 BTC

Txn: Want

Pay 2 BTC from pk_A to pk_B — MSG

SIGN by sk_A → SIGNATURE

UTXO model (BITCOIN)

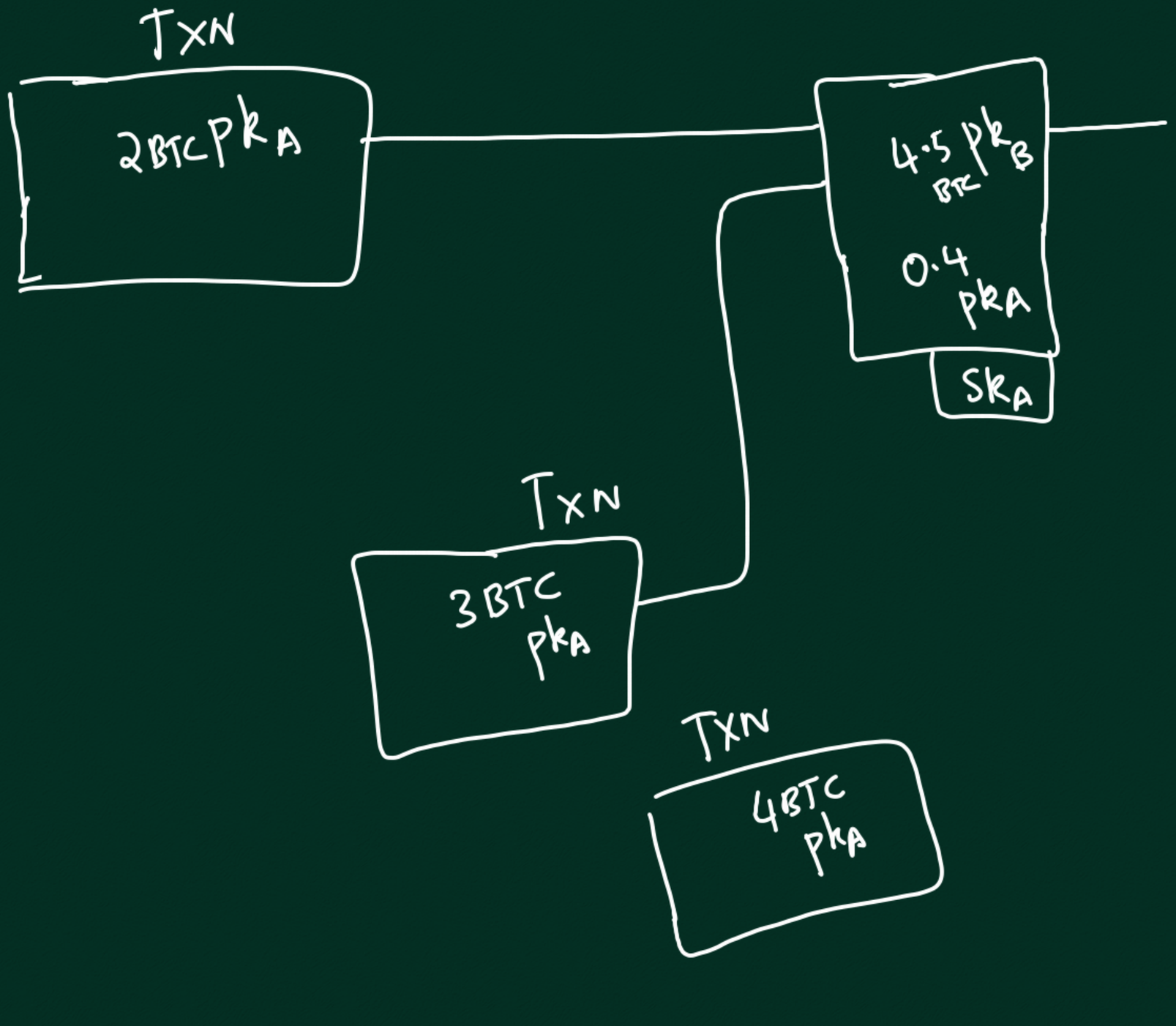


RULE: Sum of i/p BTC — Sum of o/p BTC

Can be taken as txn fee

UTXO: Unspent TXN Output

RULE: new TXN should take input only from UTXOs


TXN
2BTC pk A
4.5 pk B
BTC
0.4
pkA
SkA
TXN
3BTC
pkA
TXN
4BTC
pkA

COINBASE

1st txn in a block

VARIOUS FIELDS → WHY?

height (distance in blocks from Genesis)

No inputs (except dummy input)

Output: (BTC = $\sum$ txn fees + mining reward)

→ miner's pk

MINING REWARD

2009: 50 BTC /block

HALVING every 4 years

SATOSHI: 1M BTC

↳ still UTXOs

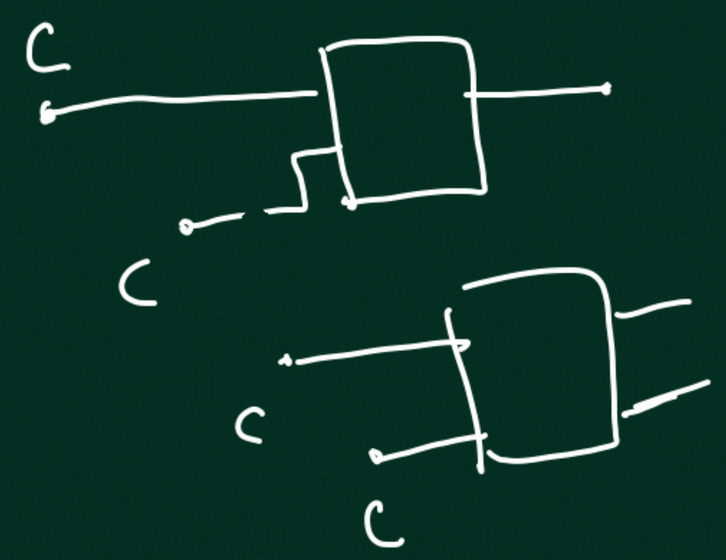
Hal Finney

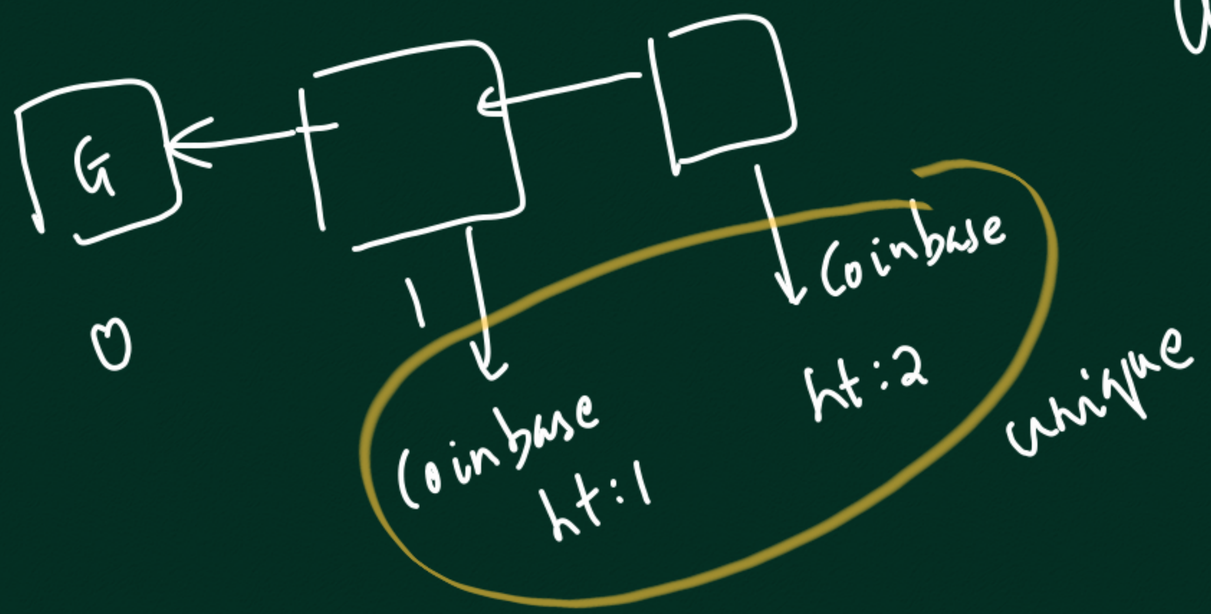
pay (1st txn)

NAKAMOTO SATOSHI

Very central intelligence

CIA

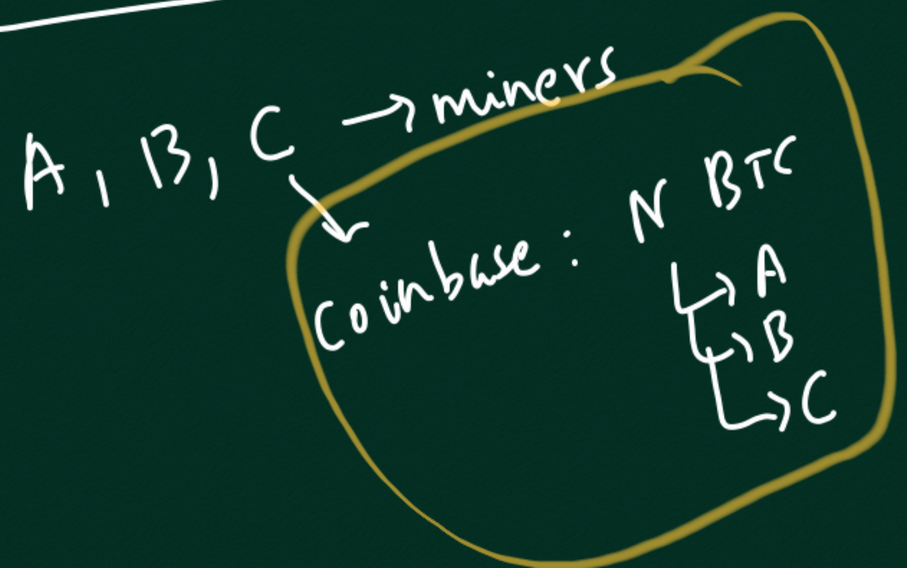




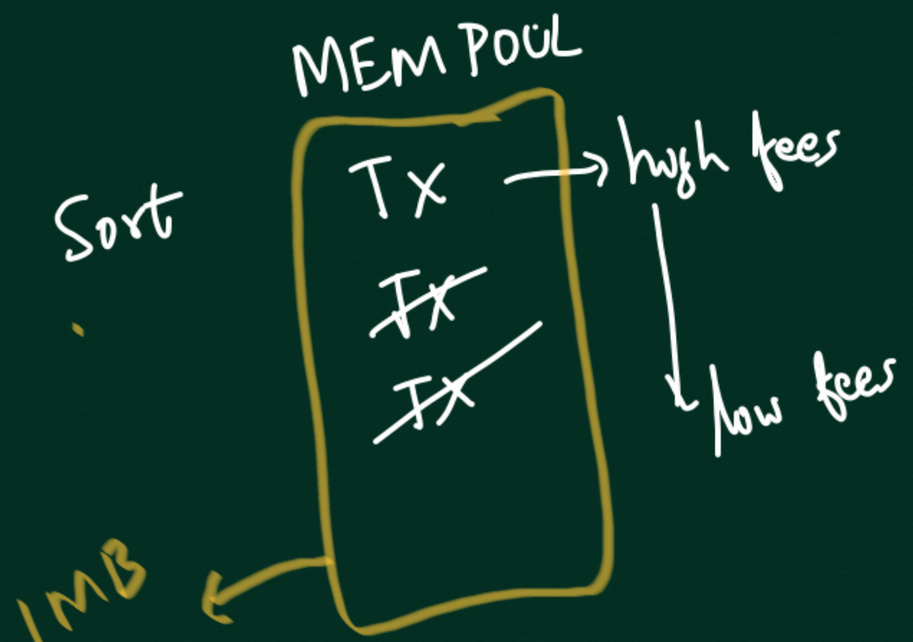
Use induction
prove that all
non-coinbase txns
are unique

target adjusted every 2 weeks

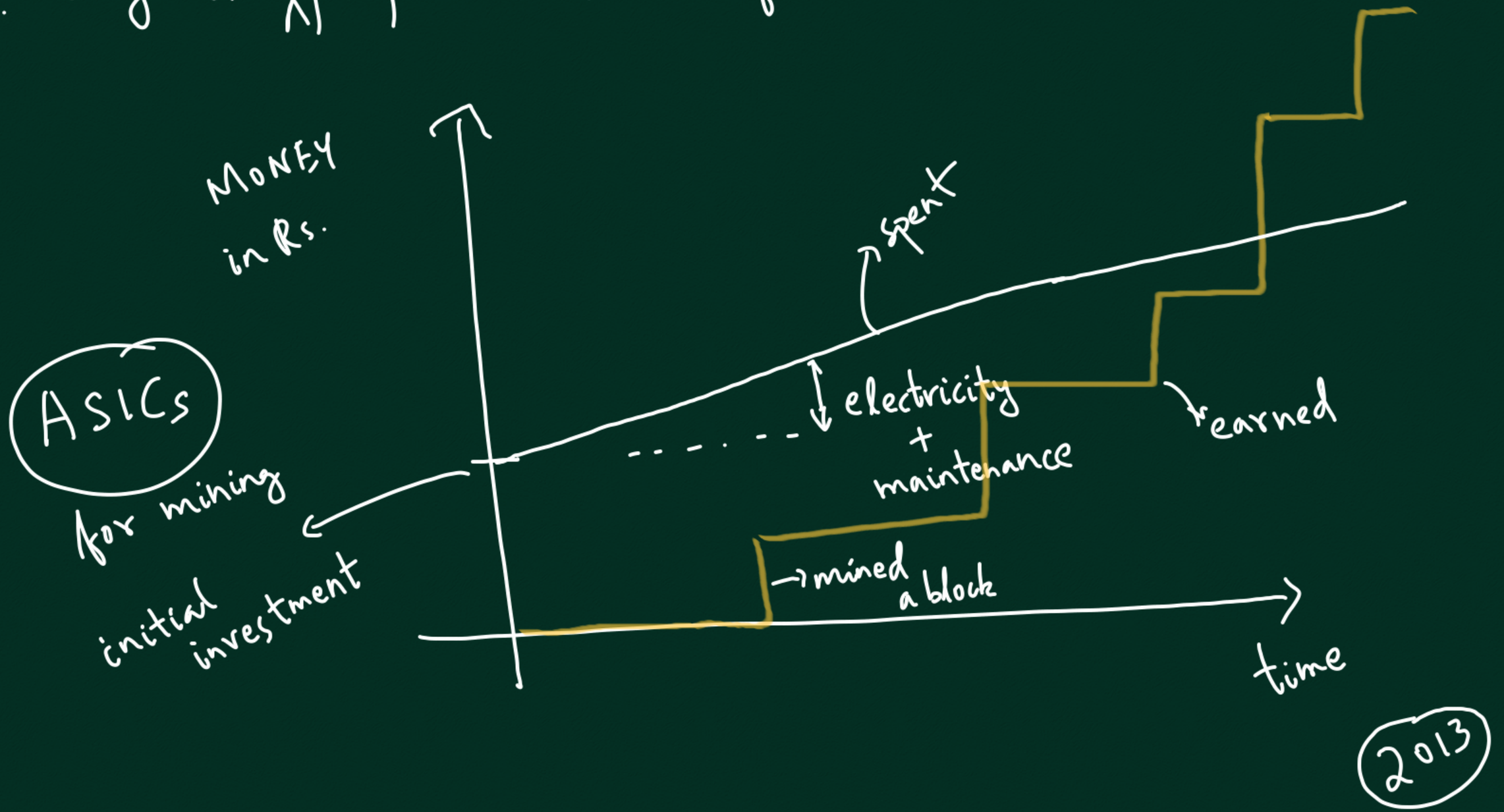
MINING POOLS



Sort



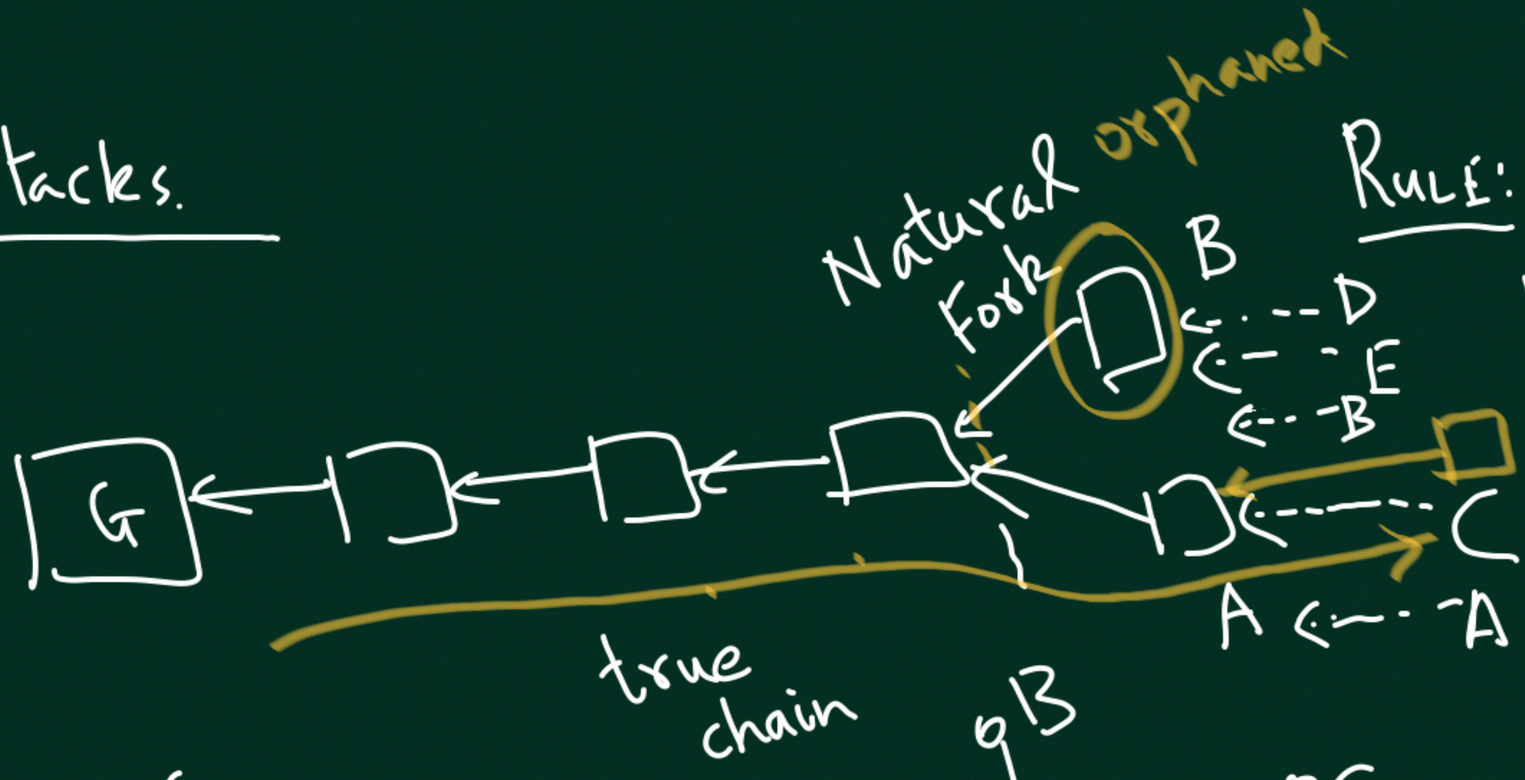
Q. Why do some people mine & follow Bitcoin Rules



Intuitively: Incentive Bitcoin network

$\sum$ mining rewards (per year) > total electricity cost for mining

Attacks.



10mins: 600 s

b'cast time $\simeq$ 10 s

of 1MB block

$\text{ratio} = \frac{600}{10} = 60$

Rule: In case of equally "long" chains, mine on last blk of 1st one seen

Rule: Mine on last blk of longest chain visible