SCALABILITY

Throughput: # txns / sec

Confirmation Latency

Amt. of Computation of smart contracts

Attendance

BTC	ETH (1.0)
7 txn/sec	10-15 txn/sec

1 hour (six conf.)

Similar

$T_1, T_2, \sim, T_n$

100ms of Computation per block (15 sec per block)

A

B

Hdr + Hashes of txns

don't have info

Validate

time

B

C

Validate

A

B

C

D

1 MB

10-min inter arrival

A's block

D's block

Hdr

Txns

? send hashes

Ideas: Modify Consensus Protocol To Get Higher Throughput

L_1 L_2

Layer-1

Layer-2 Off-chain storage or Computation of txns

main blockchain

Payment Chl Networks

(in theory: ∞ scalability, low confirmation time)

Any program P → C Proof code

I → P → O

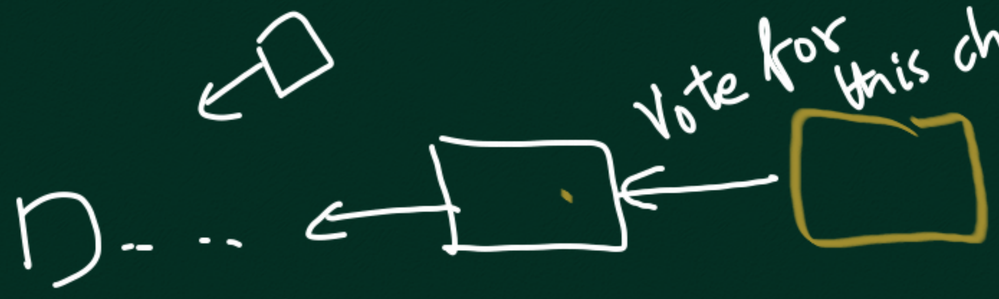
Rollups

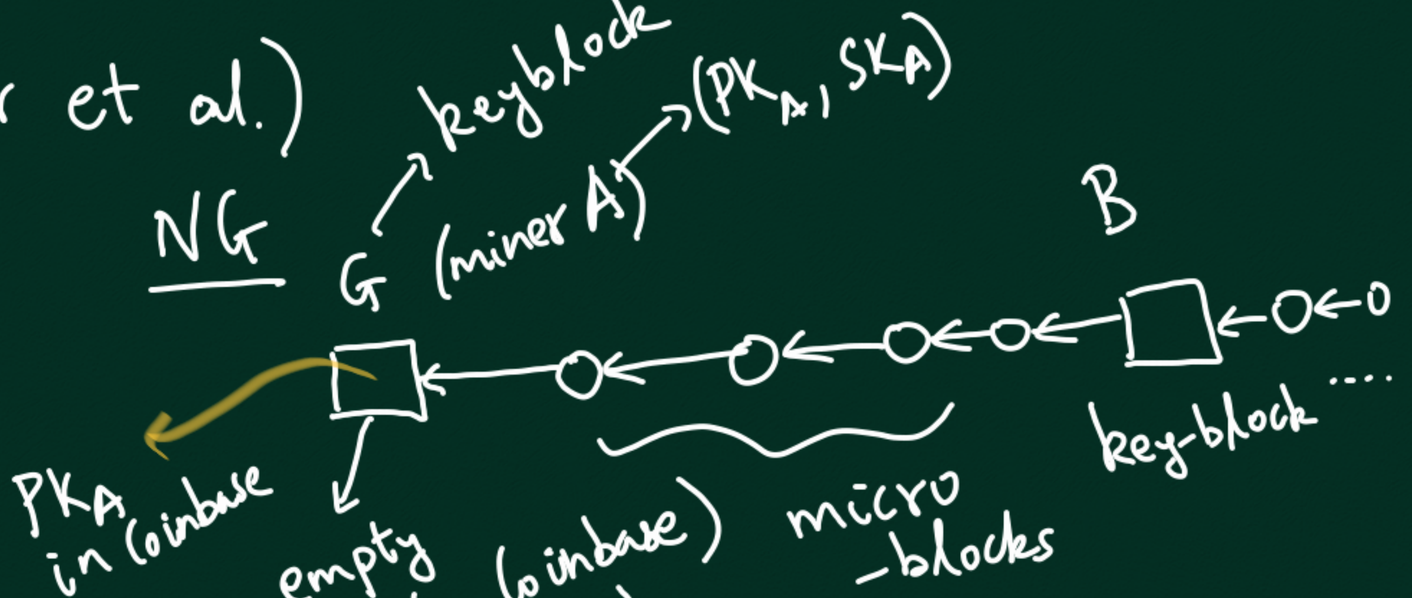
Optimistic

2k-rollups

I → C → O

BITCOIN-NG (Sirer et al.)





Miner:

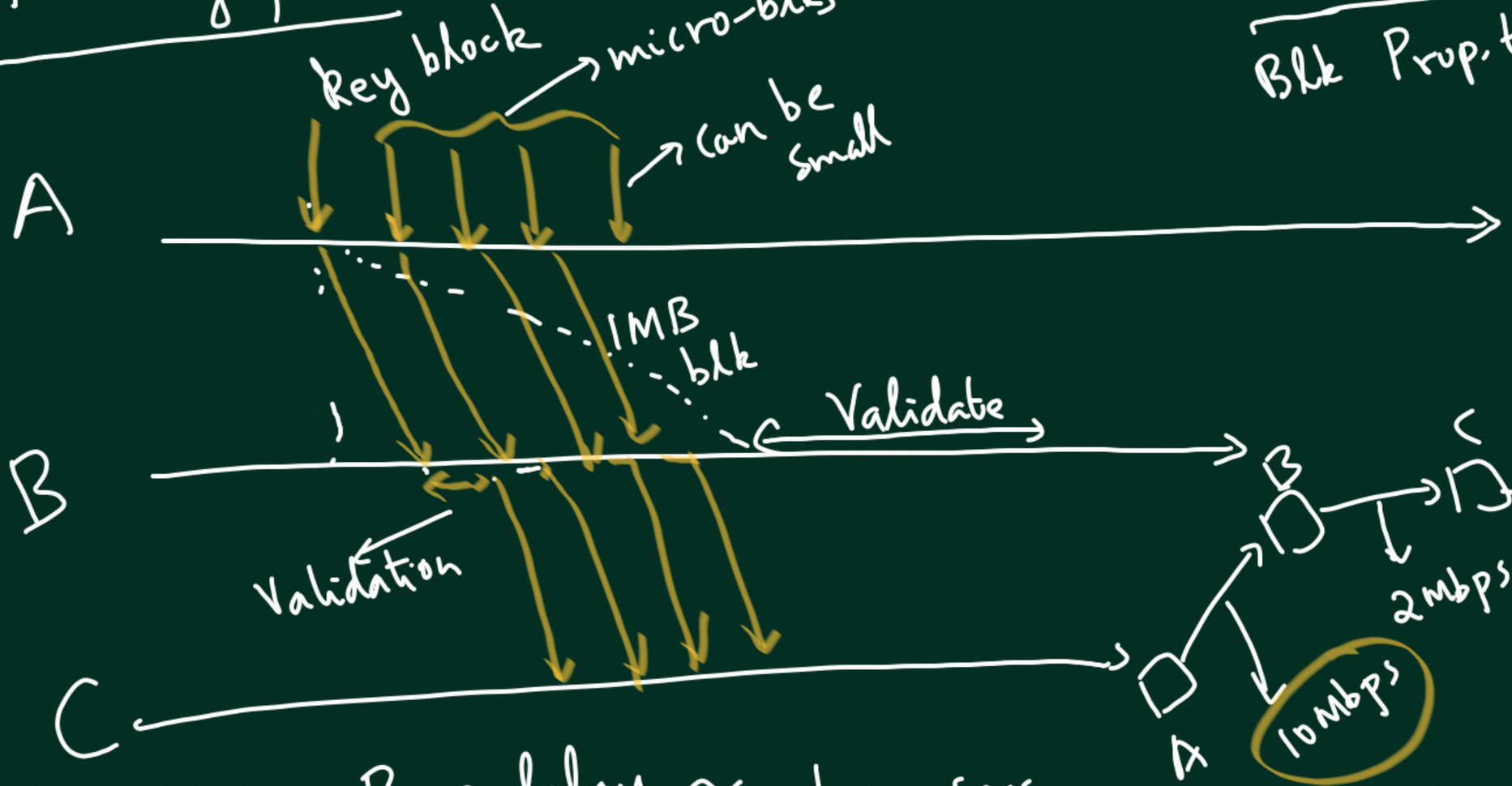
- Select txns
- Orders txns
- PoW → voting mechanism
  - leader election (miner who creates block)

Separate NG

- No PoW
- only txns
- signed by SK_A

PRISM

Throughput?

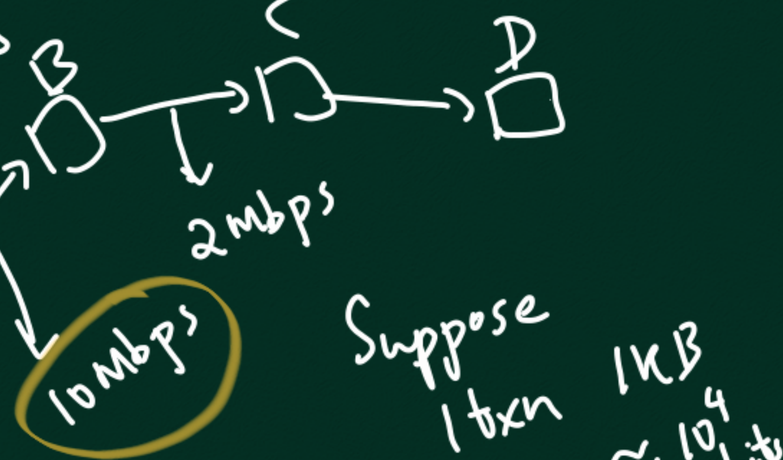


Prop. delay $\approx$ 1 secs (of key block)

Key blk IAT = 60 sec (1 min)

$$\frac{\text{Blk. IAT}}{\text{Blk Prop. time}} = \frac{600}{10} = 60 \quad \text{(BTC)}$$

$$= \frac{60}{1} \quad \text{(NG)}$$



Suppose 1 txn 1KB $\approx 10^4$ bits

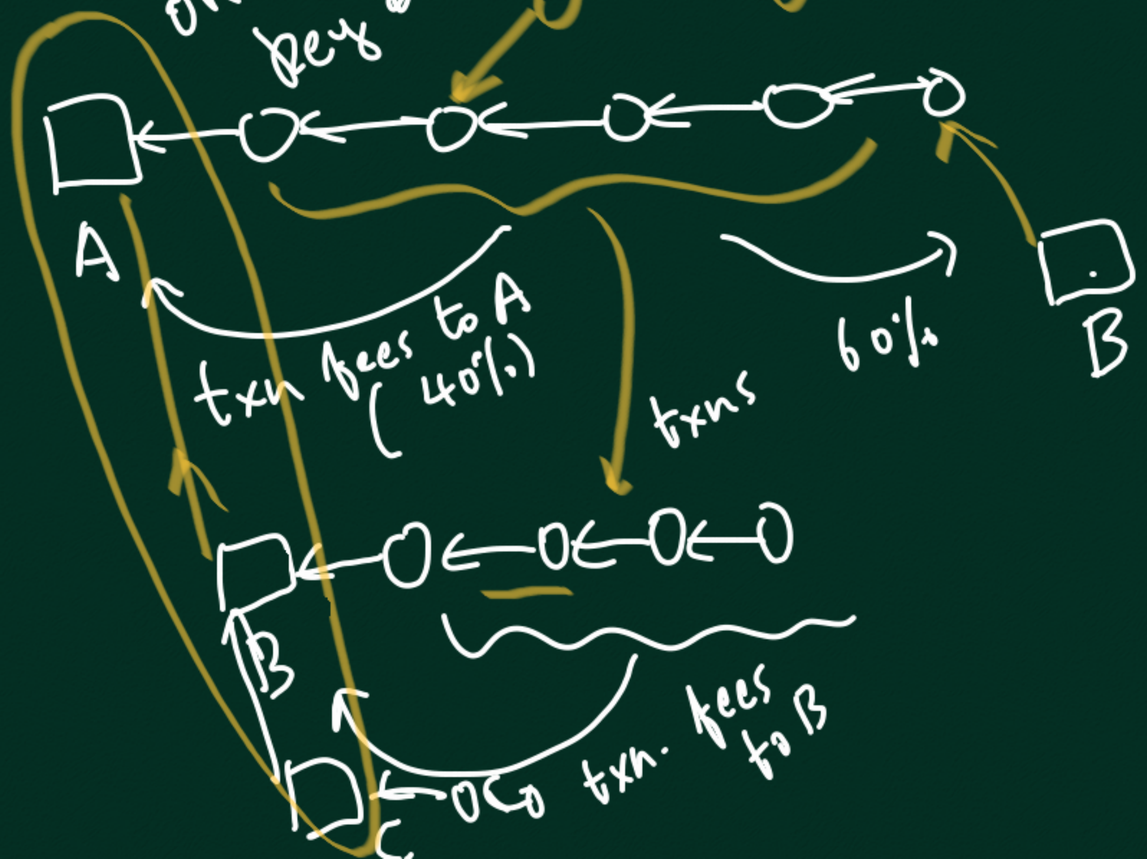
$\frac{10^7}{10^4} = 10^3$ txns/sec

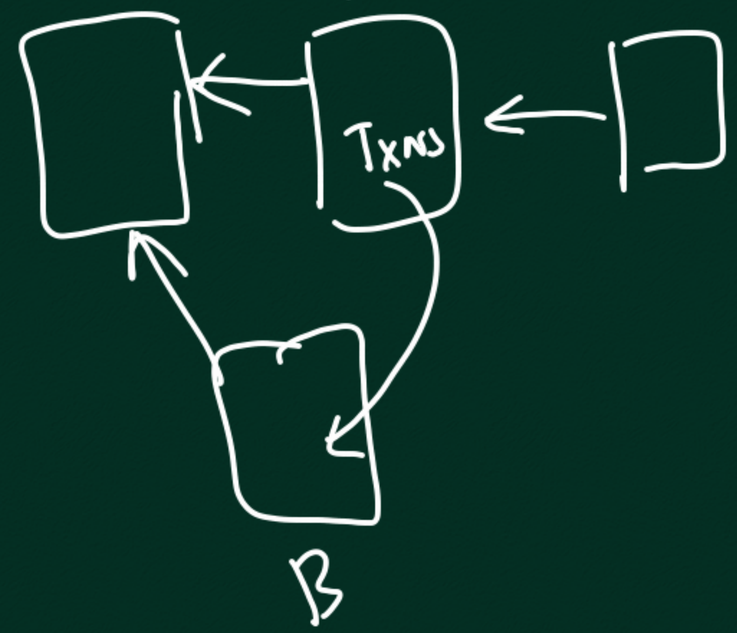
Confirmation Latency?

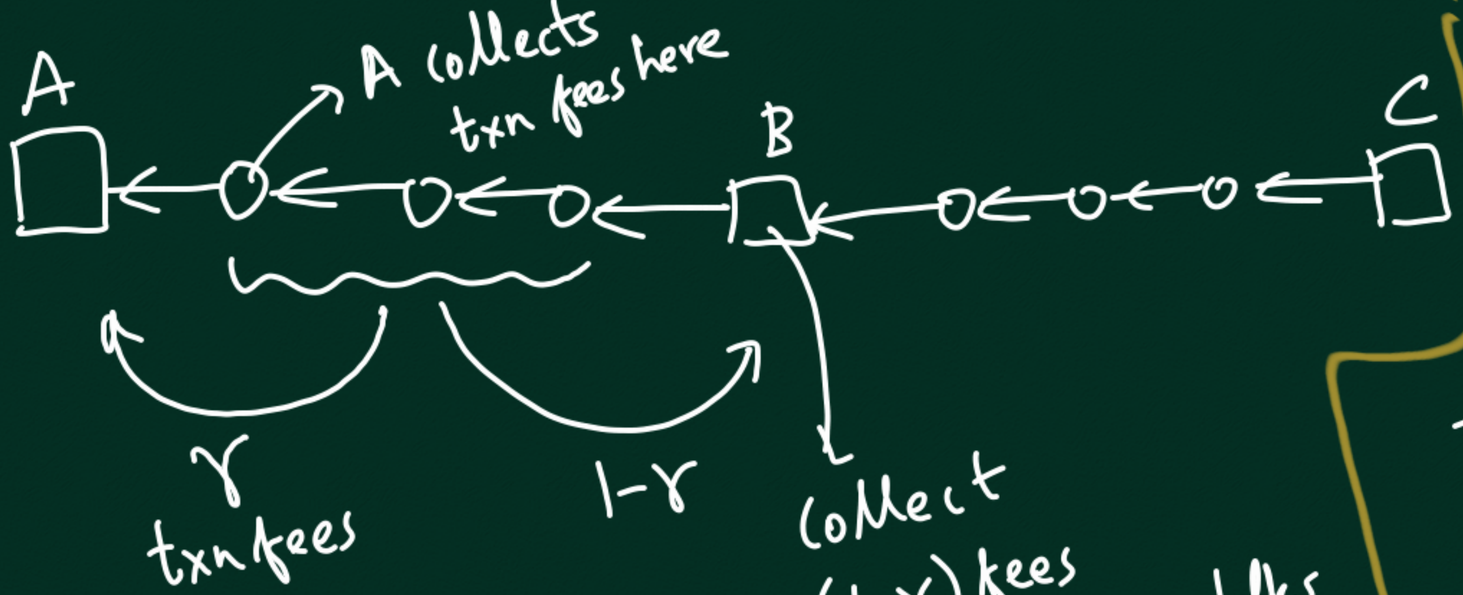
Six Confirmations : 1 hour Bitcoin.

: 6 mins NG

NG:







Option-1: Expected txn fees

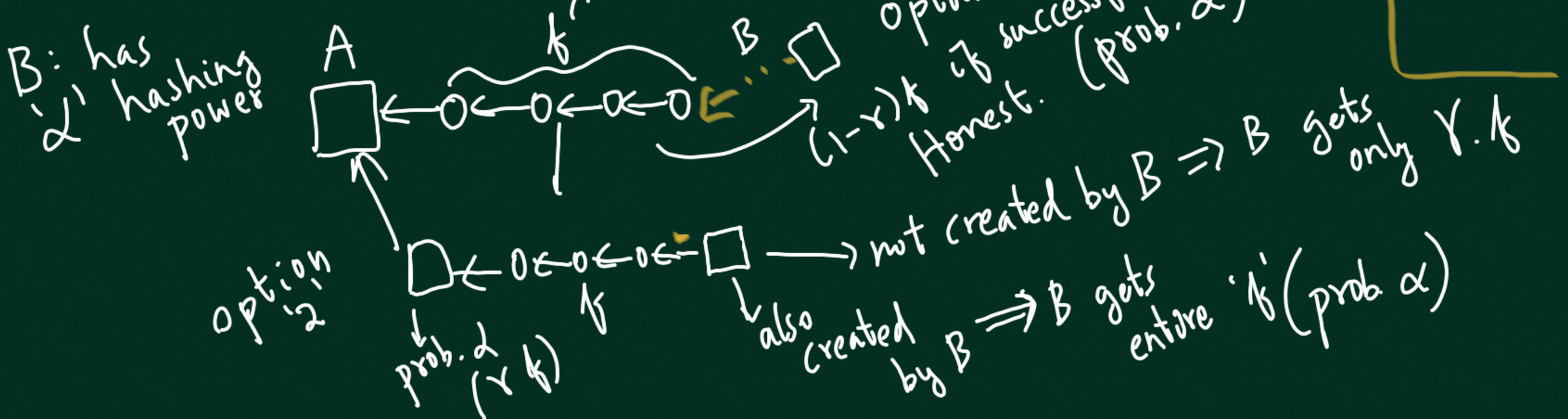
$\alpha \cdot (1-\gamma) f$

option-2:

$\alpha \left[\gamma f + \alpha (1-\gamma) f \right]$

Attack

B: has 'α' hashing power



Want

$$1-\gamma > \gamma + \alpha(1-\gamma)$$

$$1-\gamma > \gamma + \alpha - \alpha\gamma \quad \Big| \quad (1-\gamma)(1-\alpha) > \gamma$$

$$1-\alpha > 2\gamma - \alpha\gamma \quad \Big| \quad 1-\alpha > \frac{\gamma}{1-\gamma}$$

$$\frac{1-\alpha}{2-\alpha} > \gamma \quad \Big| \quad 1 - \frac{\gamma}{1-\gamma} > \alpha$$

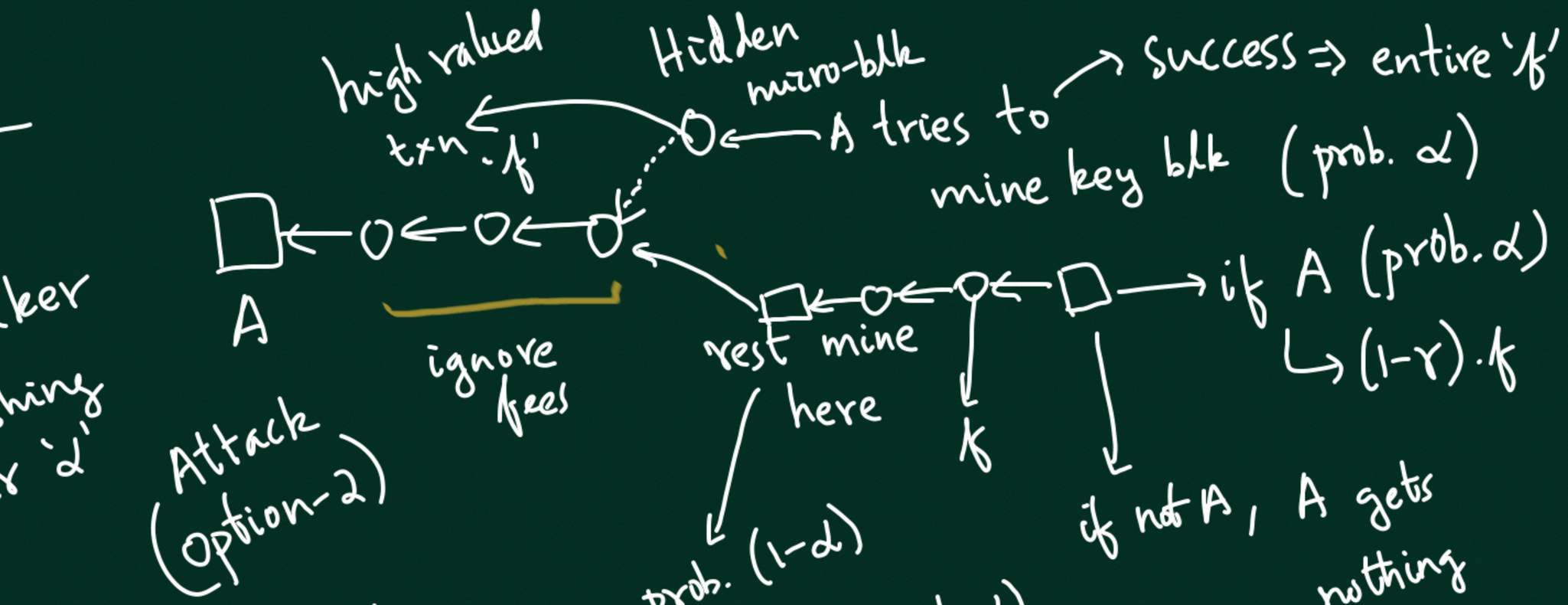
Suppose $\alpha = 0.25$ (worst case)

$$\Rightarrow \gamma < \frac{1-0.25}{2-0.25} \approx 0.43$$

$$\frac{1-0.5}{2-0.5} = \frac{0.5}{1.5} = 0.33$$

Attack

A is attacker with hashing power 'α'



option-1 (Honest) Expt. fees

$$\gamma f + \alpha(1-\gamma)f$$

option-2

$$\alpha f + (1-\alpha)\cdot\alpha\cdot(1-\gamma)f$$

Want $\gamma + \alpha(1-\gamma) > \alpha + \alpha(1-\alpha)(1-\gamma)$

$$\gamma\left[1-\alpha+\alpha(1-\alpha)\right] > \alpha + \alpha(1-\alpha) - \alpha$$

$$\gamma > \frac{\alpha(1-\alpha)}{1-\alpha^2} = \frac{\alpha}{1+\alpha}$$

Suppose $\alpha = 0.25$ worst case

$\gamma > 0.2$

$0.2 \le \gamma < 0.43$

$\gamma > \cdots \alpha$

$\frac{0.5}{1.5}$

$\gamma > 0.33$