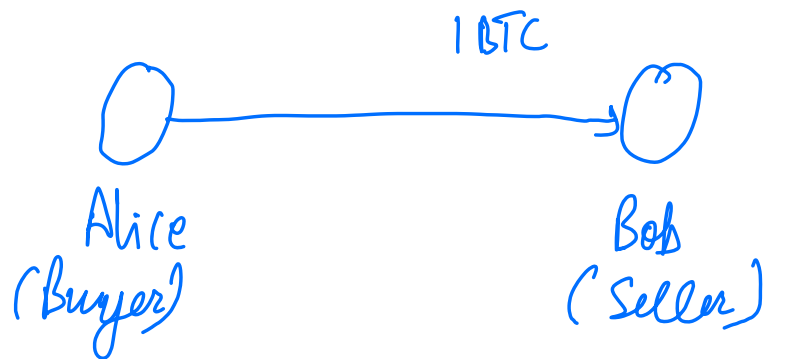
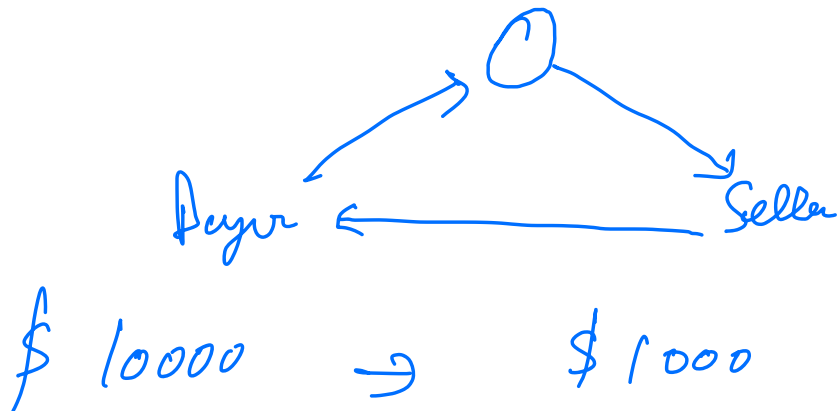


Applications of Bitcoin

- Fair Txn
- Micropayment
- Lottery



bitcorn.com



Multisig

2-out of 3 Multisig

Alice, Bob, Judy
1 BTC (or no)
Alice → (circled) 2 out of 3 sign

After fair Tim
Alice receive good -> (Pay to Bob) Alice, Bob

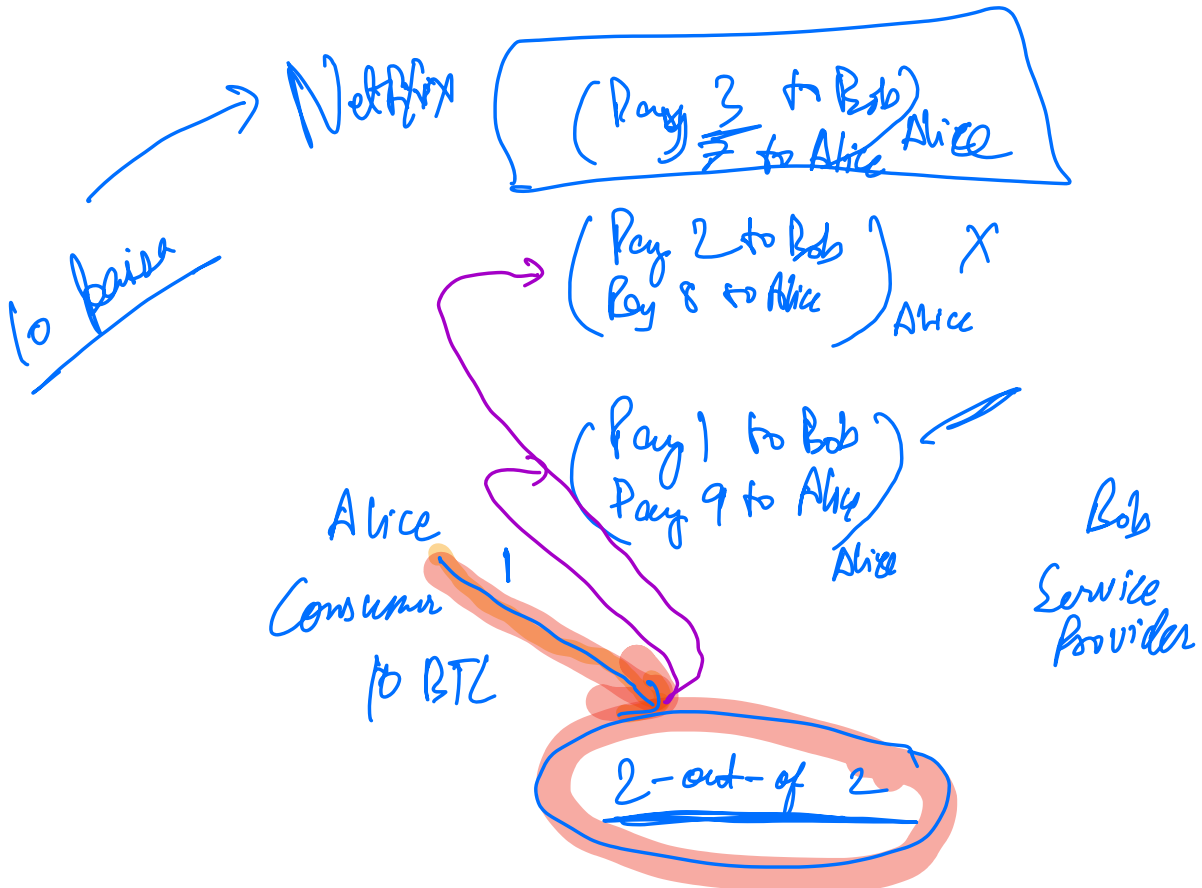
(Pay to Alice) Alice, Judy

(Pay to Bob) Bob, Judy

TXO 1

(Multisig addr)

↓ 1 BTC - tran fee
address (Alice / Bob)



Bob - extremely rich provider

[(Sign of both Alice and Bob)
OR
Pays back to Alice (Timout: curr block + 100 AND Alice)]

0 0 - 0
0 1 - 1
1 0 - 1
1 1 - 1

Lottery (0 - 1000)
(R = 500)

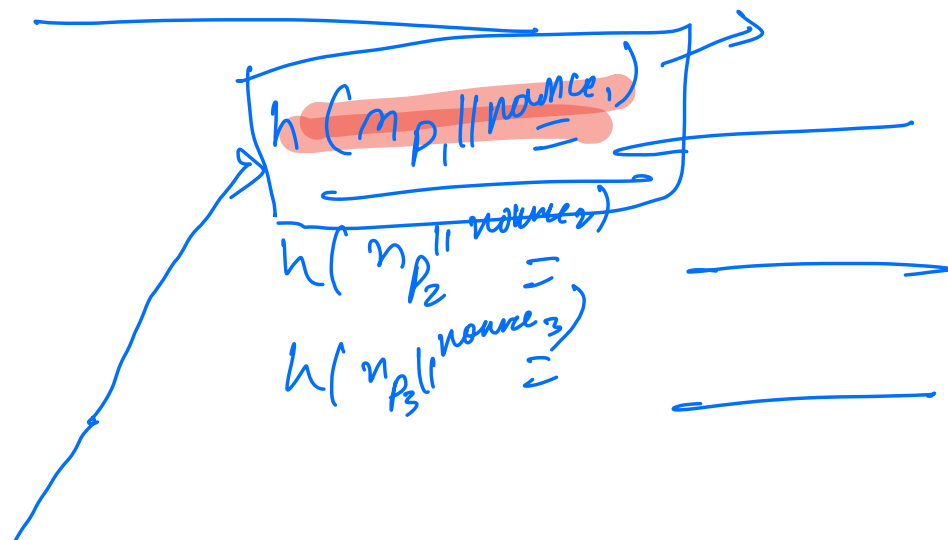
$P_1 (n_{P_1})$

$P_2 (n_{P_2})$

$P_3 (n_{P_3})$

$h(\quad) \Rightarrow \underline{\hspace{2cm}}$
256 bit

Commitment Phase



$h(|| | | \underline{9998716775})$

Reveal

(np_i, source_i)

$h(np_i || \text{source}_i)$

$h(\text{Random}_1)$

$h(\text{Random}_2)$

$h(\text{Random}_3)$