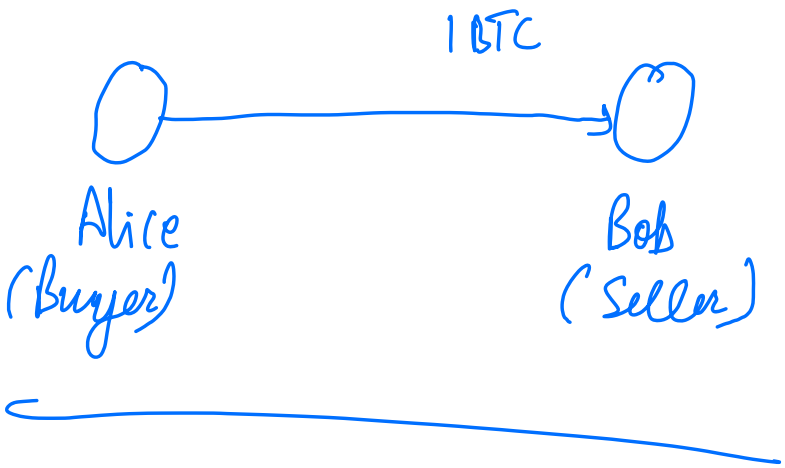
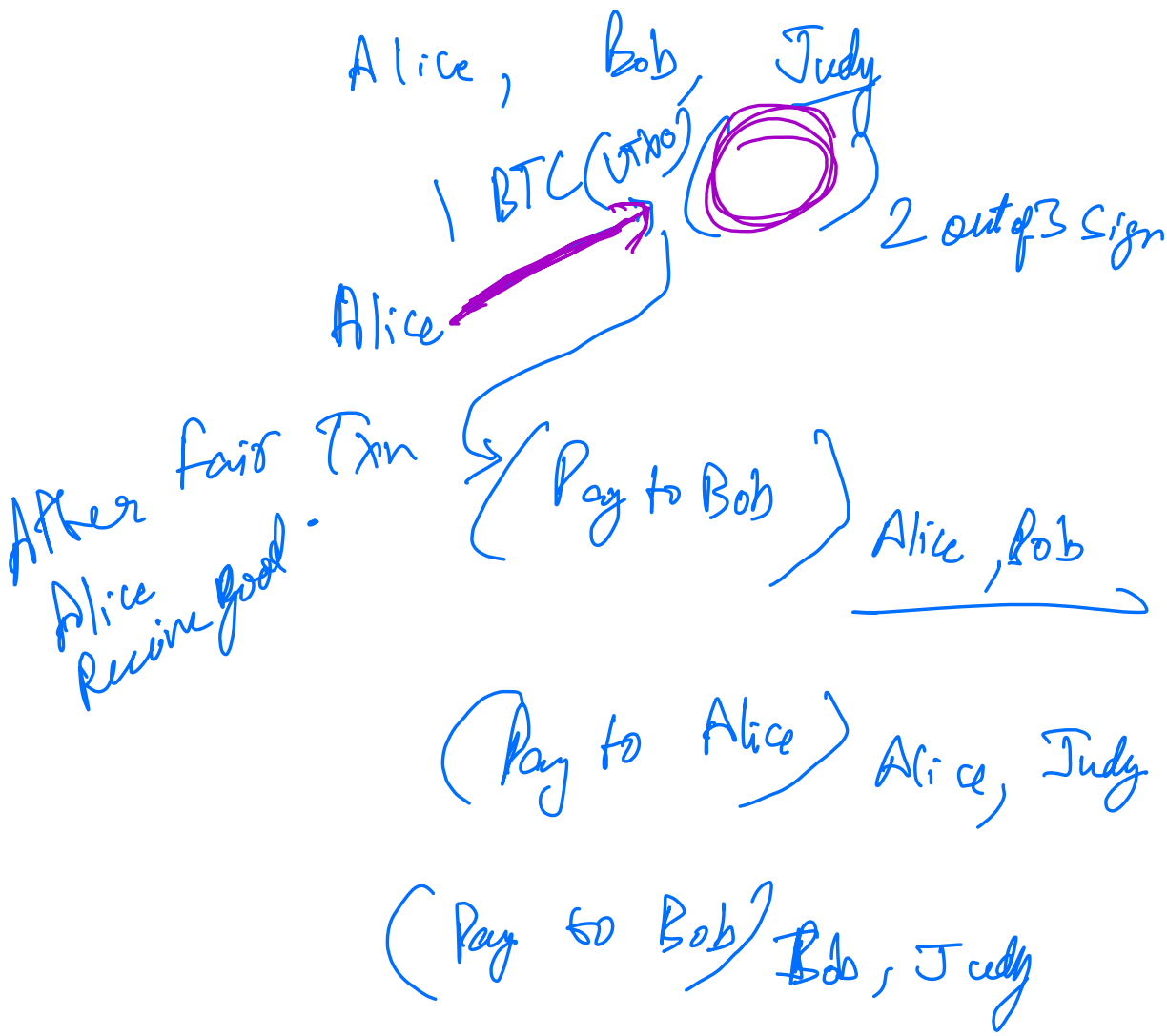
Applications of Bitcoin

- Fair Txn
- Micropayment
- Lottery



Multisig

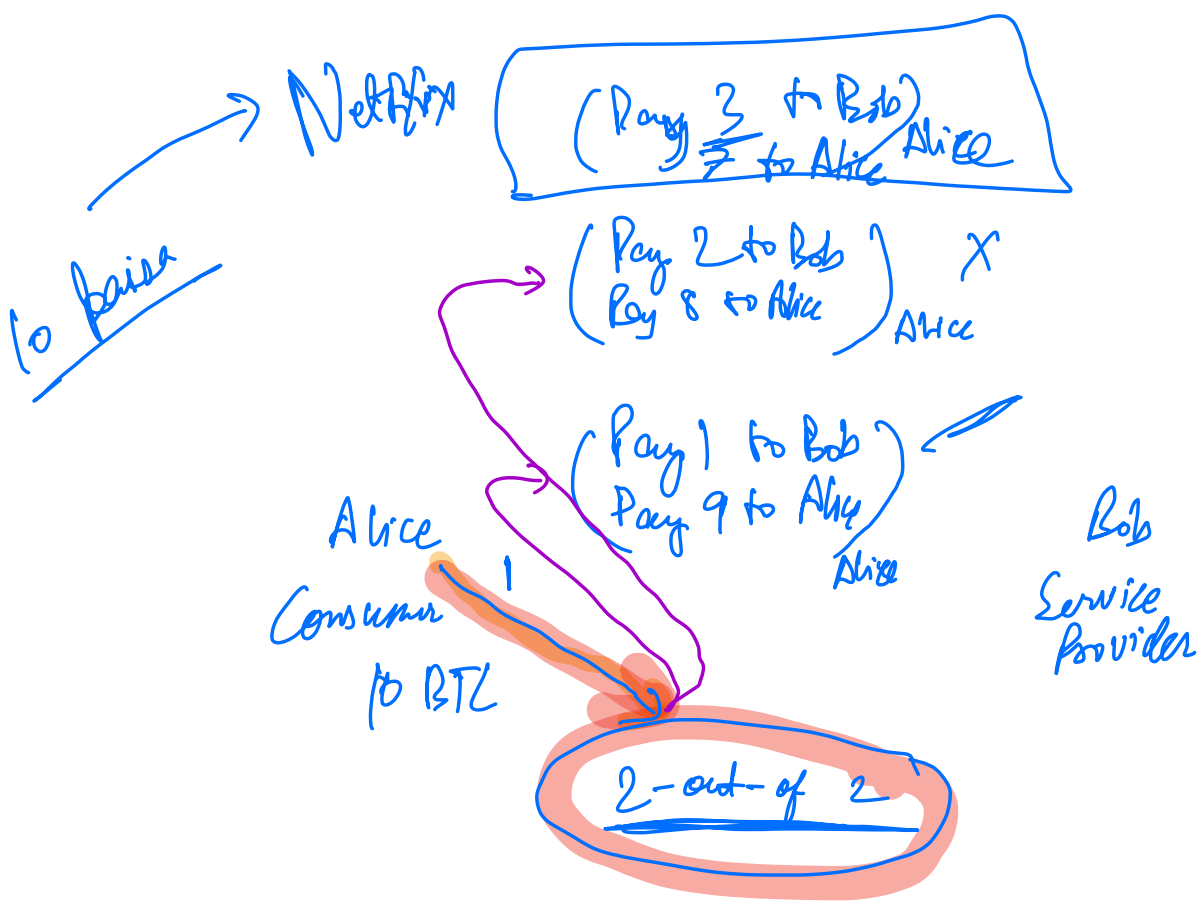
2- out of 3 Multisig



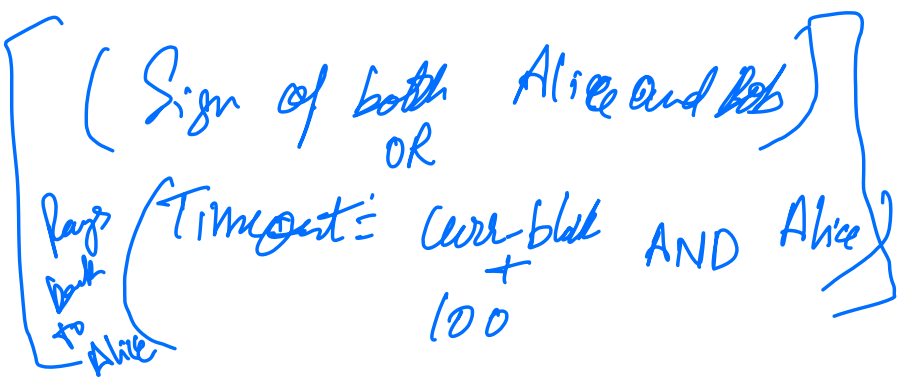
UTXO 1 (Multisig addr)

↓ 1 BTC - tx fee

address (Alice / Bob)



Bob - extremely rich provider



0 0 = 0
0 1 = 1
1 0 = 1
1 1 = 1

Lottery (0 ~ 1000)
(R = 500)

P_1 (n_{P_1})

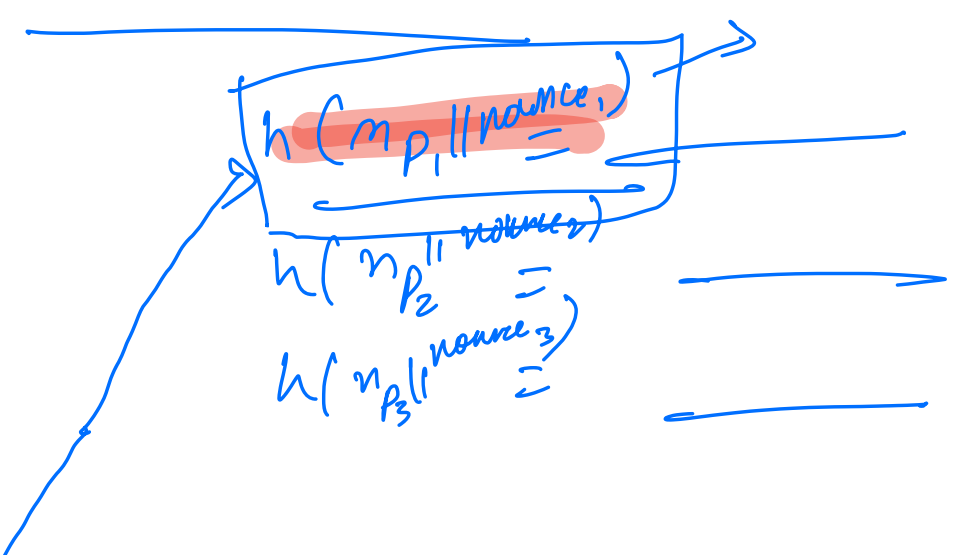
P_2 (n_{P_2})

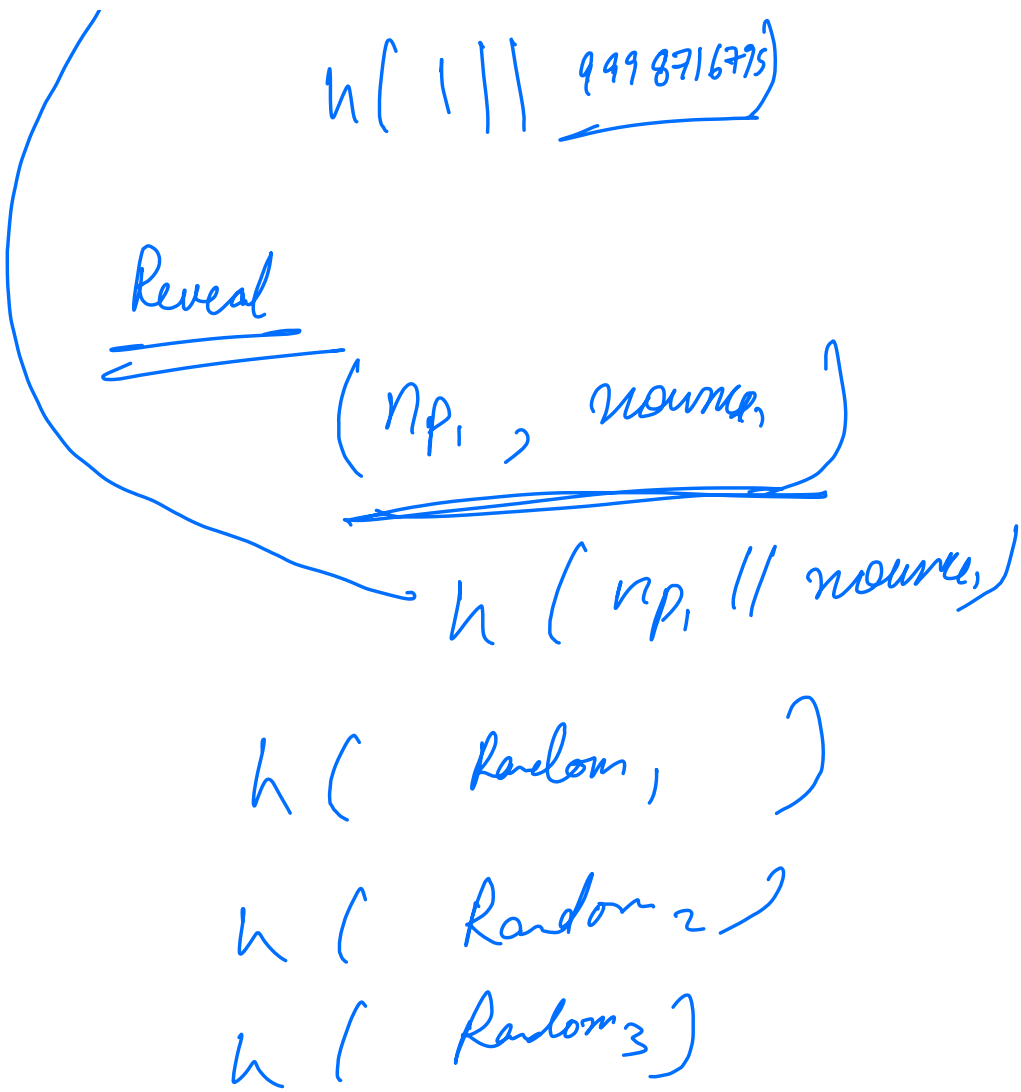
P_3 (n_{P_3})

h( ) ⇒

256 bit

Commitment Phase




h(1 || 9998716775)
Reveal
(rp1, source1)
h (rp1 || source1)
h(Random1)
h(Random2)
h(Random3)