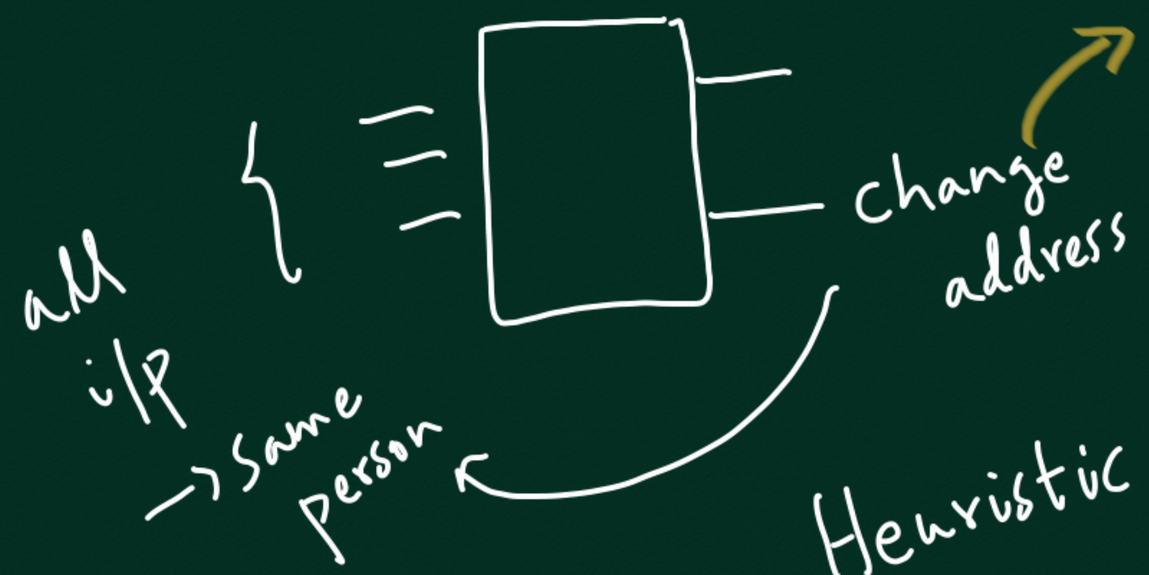
Anonymity

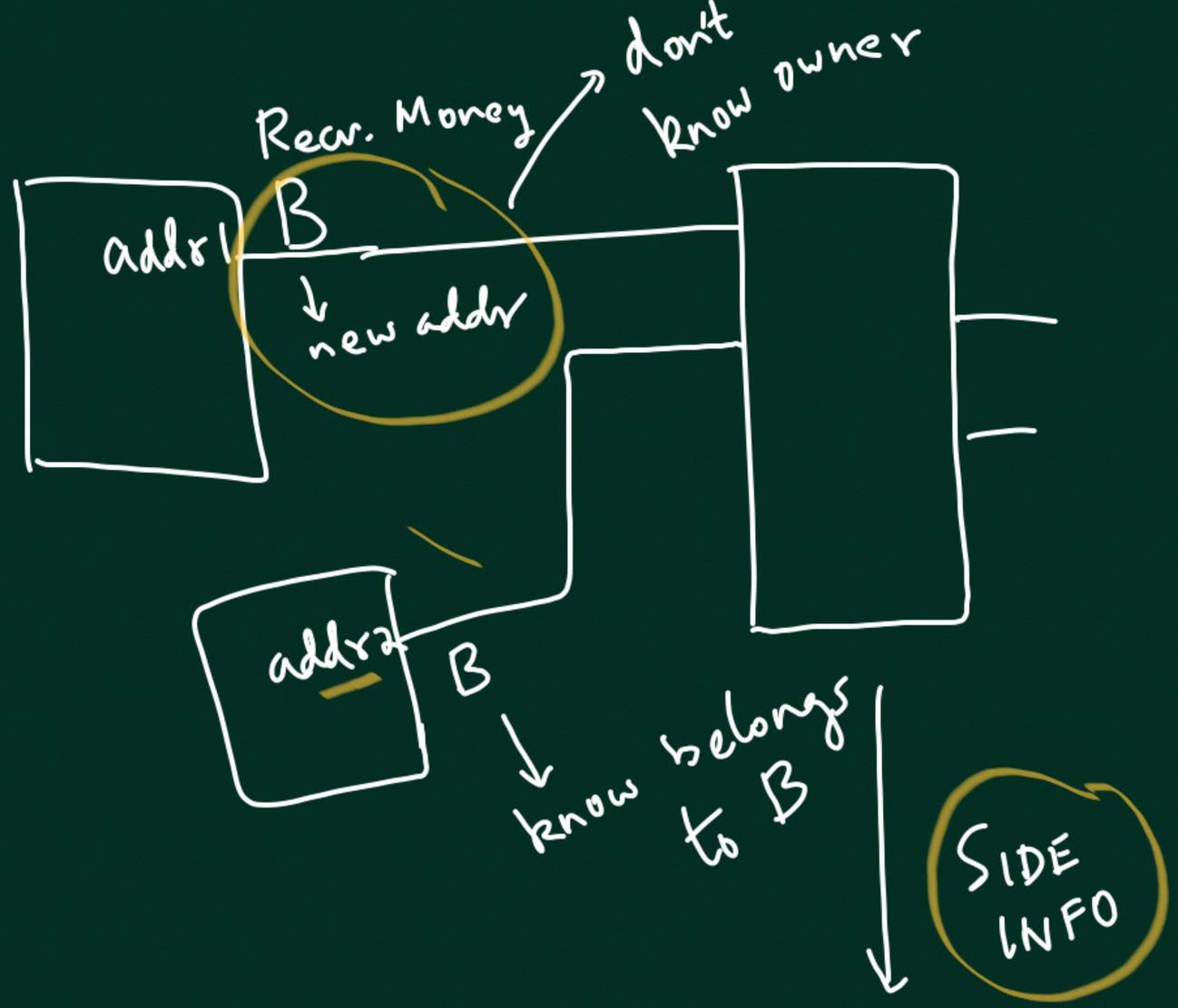
BTC

- All txns are known to all
- Only Addr., no names

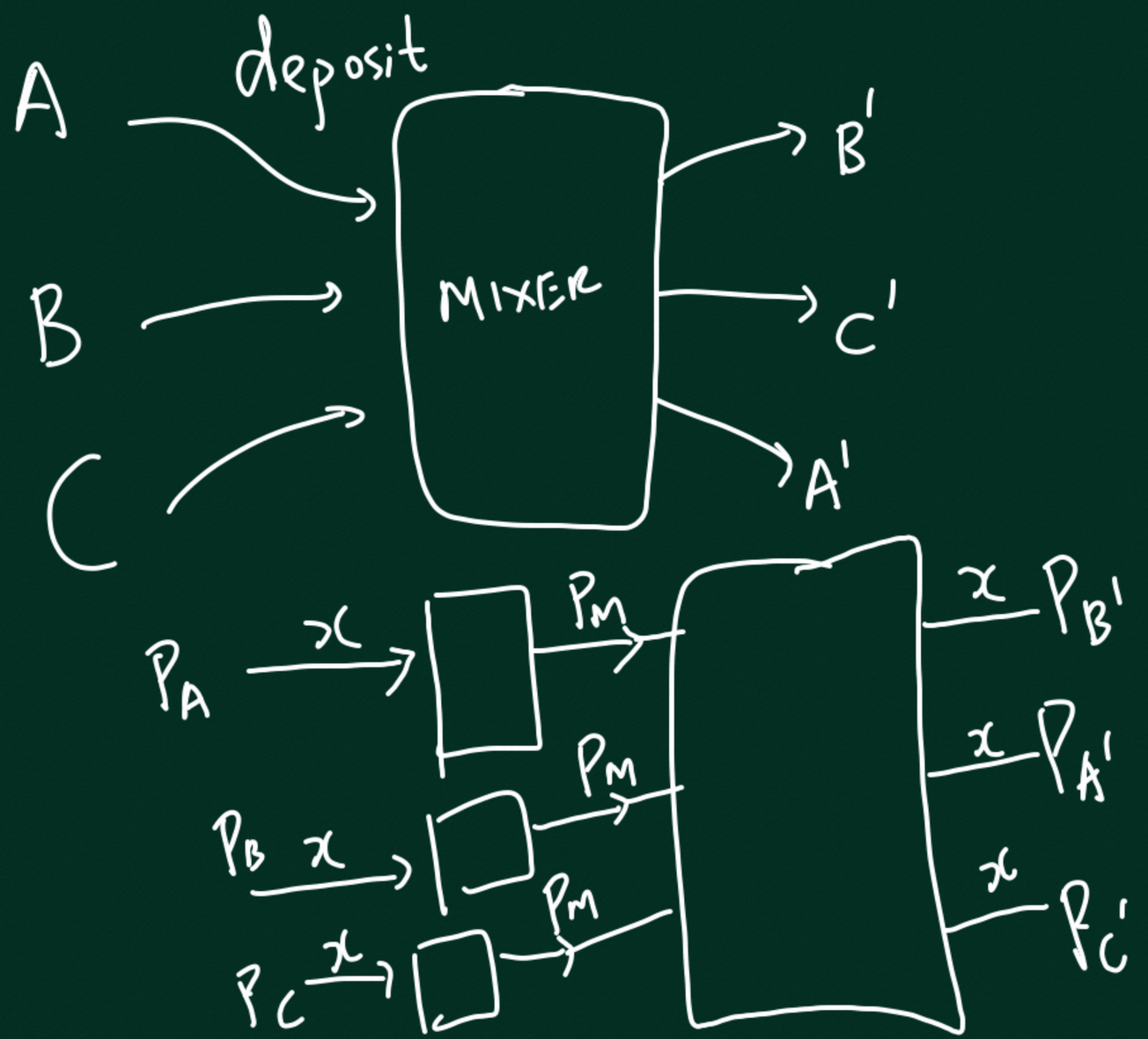
Attendance
Busy Slots Email



Heuristic:

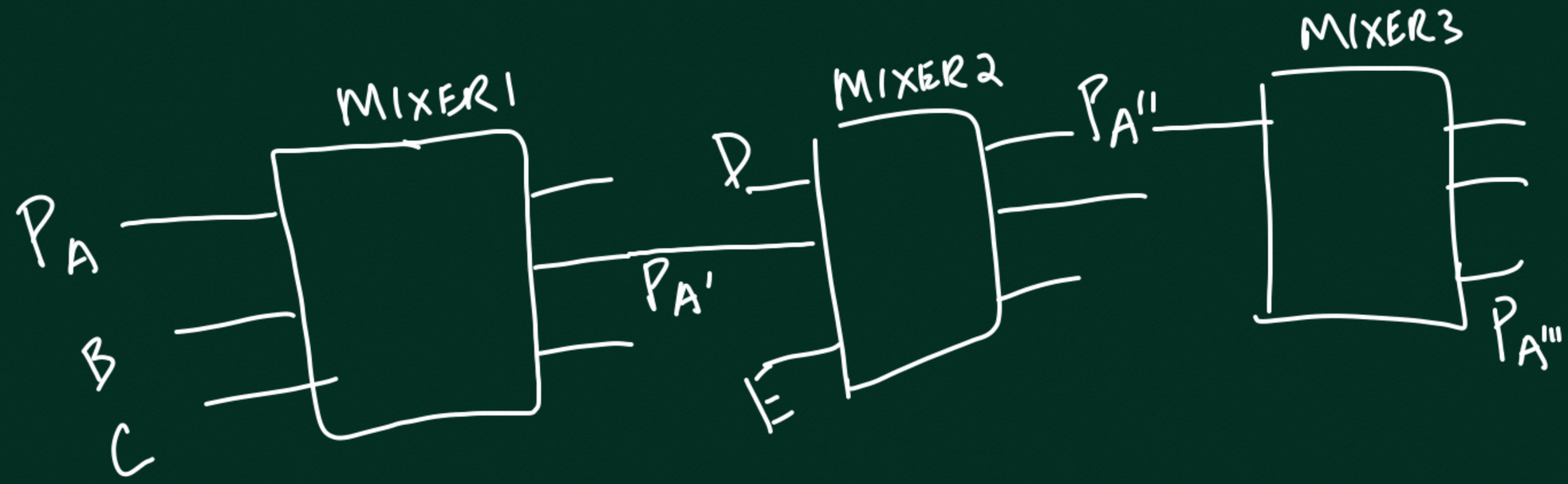

Recv. Money
don't
know owner
addr1
B
new addr
addr2
B
know belongs
to B
SIDE
INFO

MIXERS

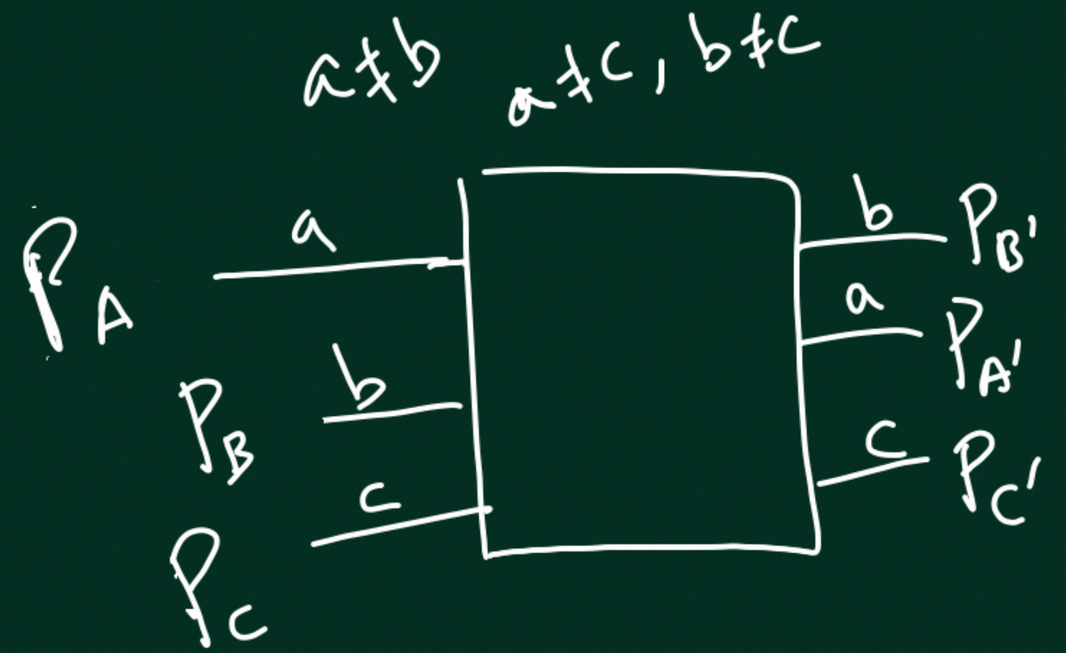


Principles of Good Mixing

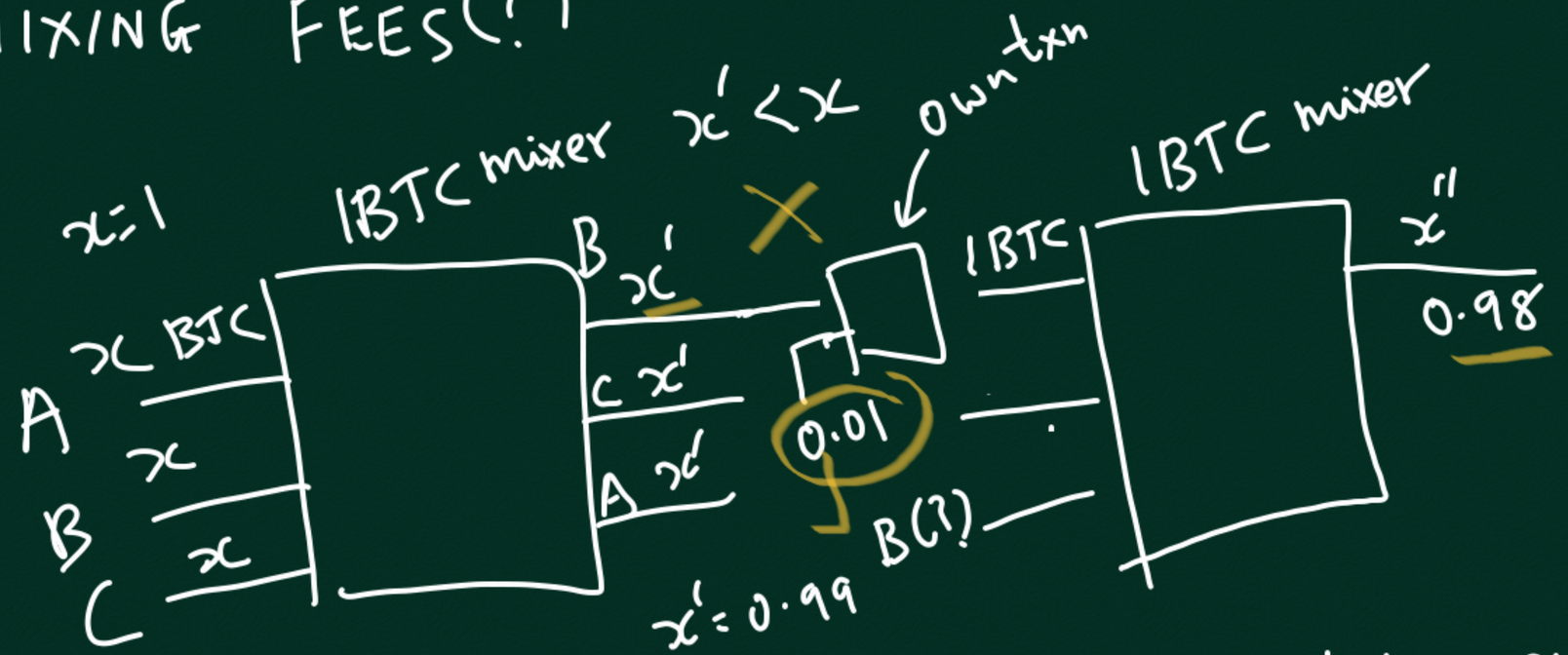
(1) Customers Should Mix Many Times



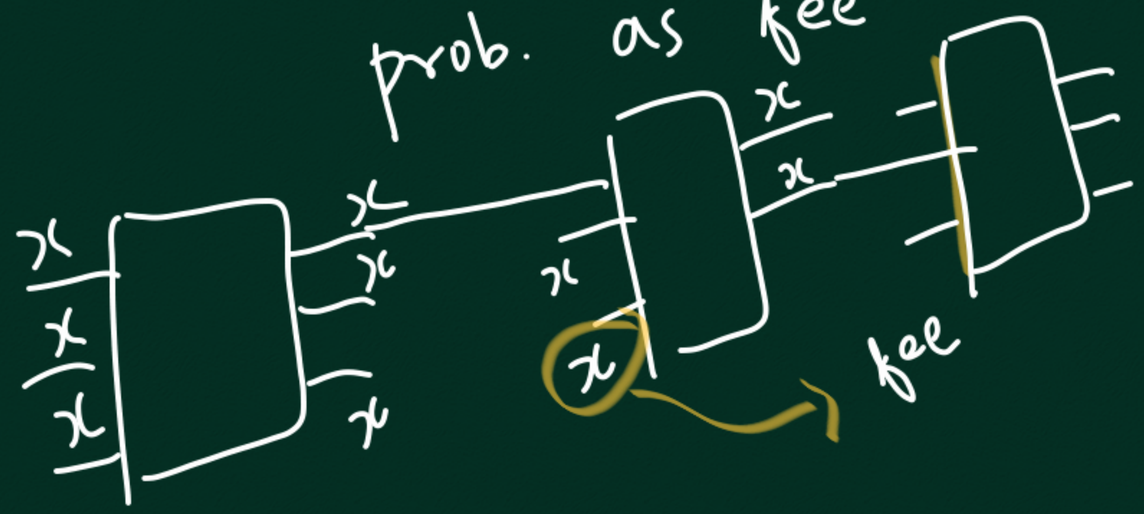
(2) MIXING SERVICE : EACH MIXER — TAKE SAME INPUT AMOUNT (CHUNKS)

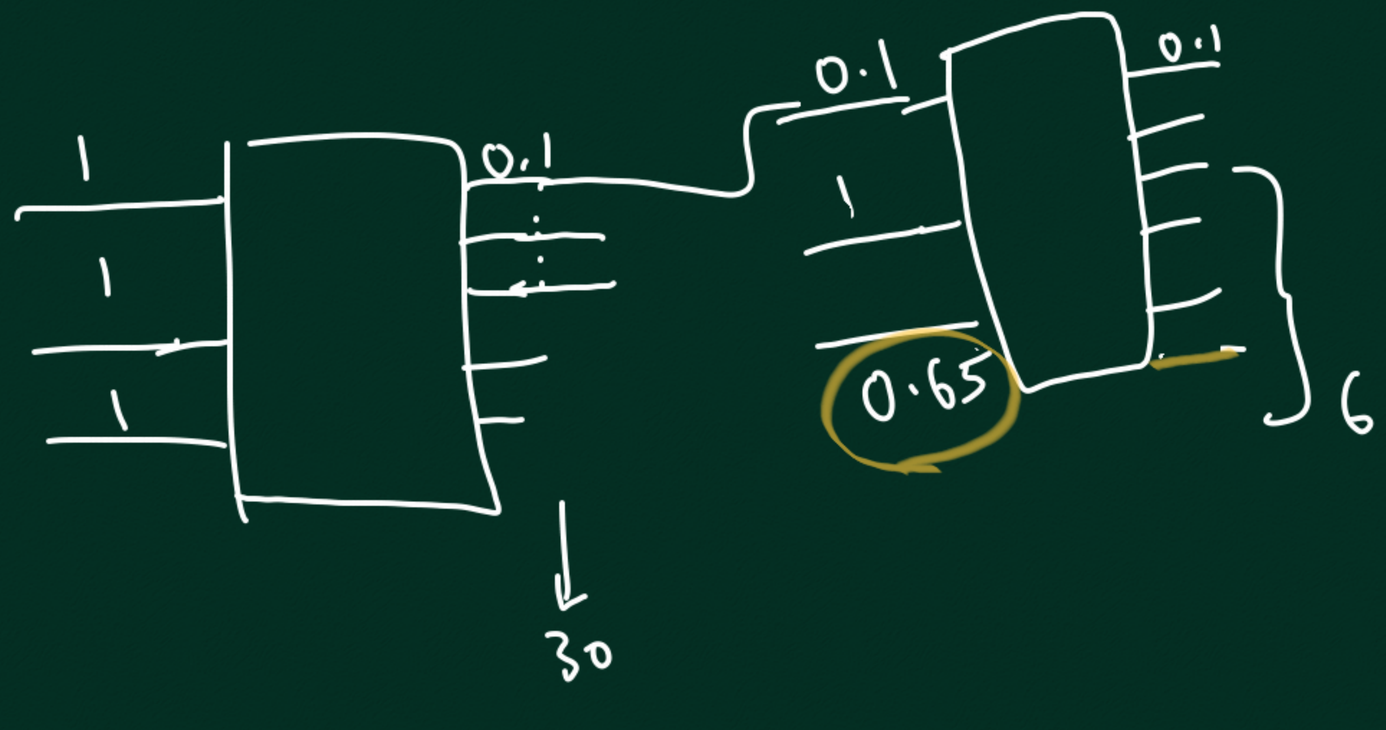


(3) MIXING FEES(?)

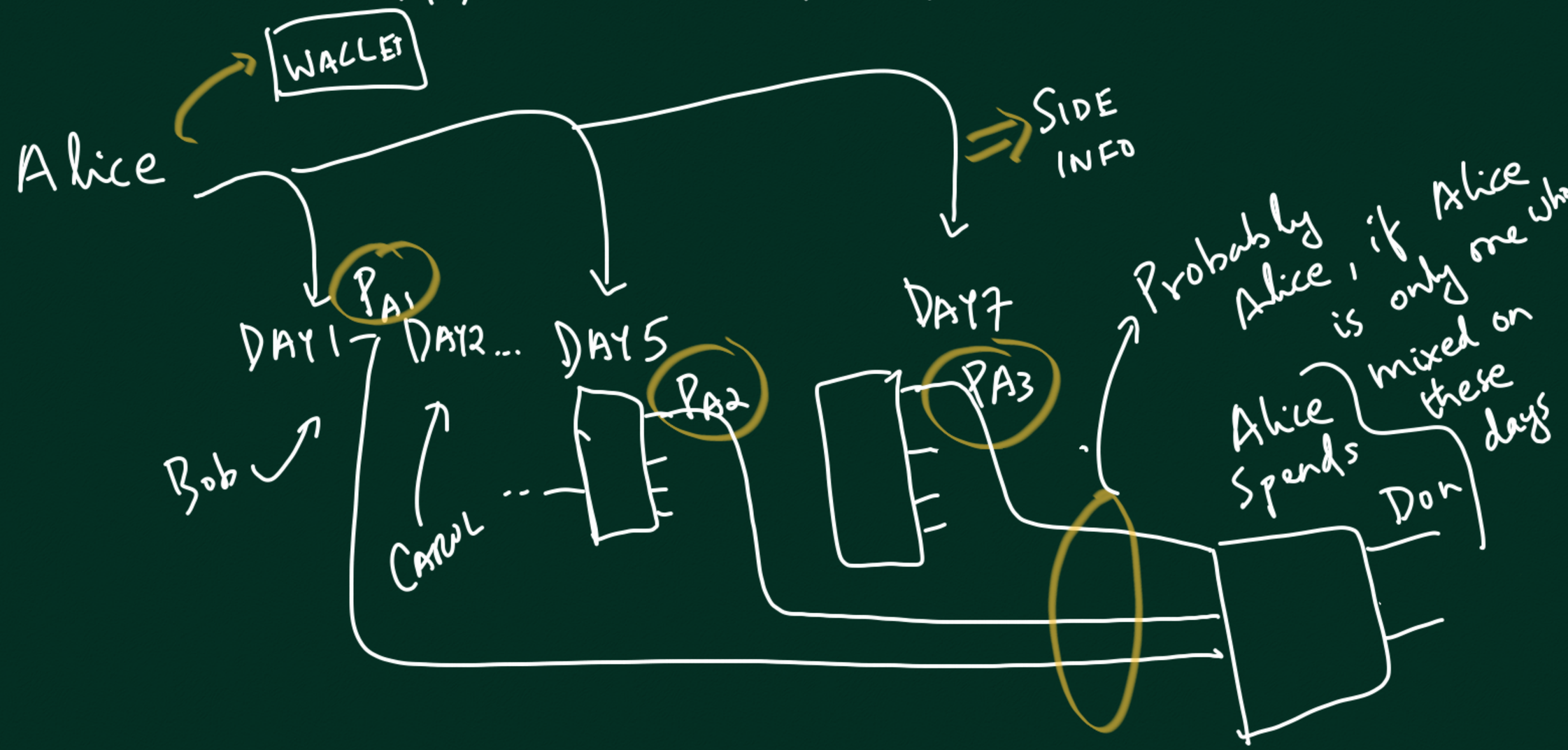


$x' = x$, randomly take one i/p with some prob. as fee



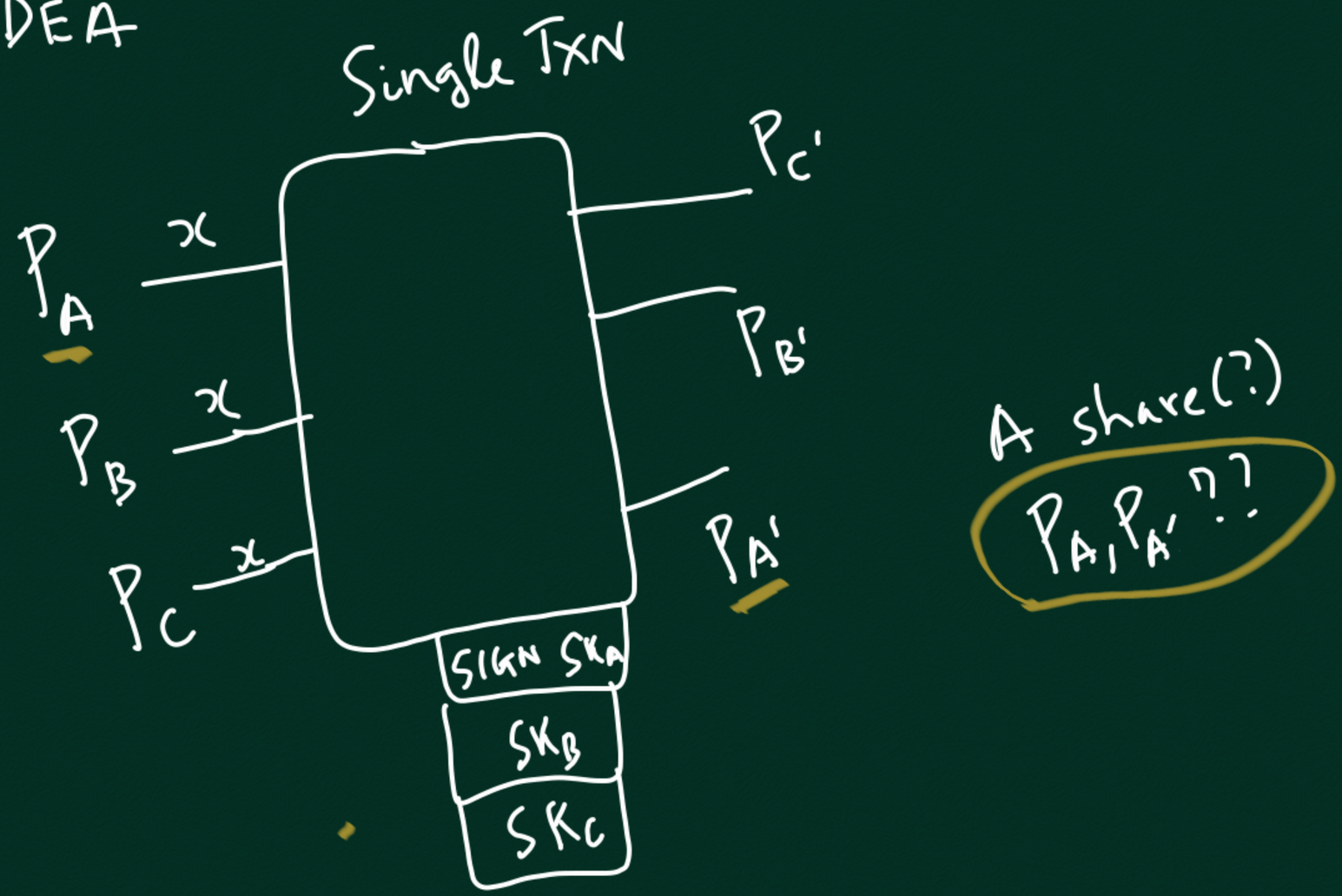

1
1
1
0.1
30
0.1
1
0.65
0.1
6

(4) Customer's Wallet Should Continuously Mix In Background



DECENTRALIZED MIXING

IDEA



A share(?)

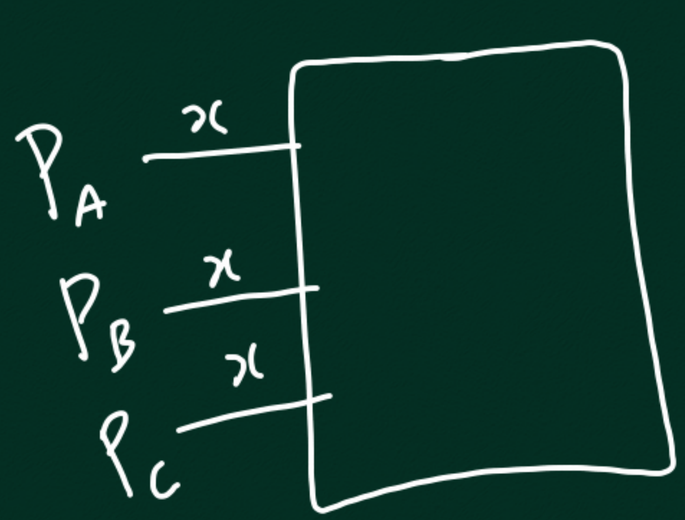
$P_A, P_{A'}$??

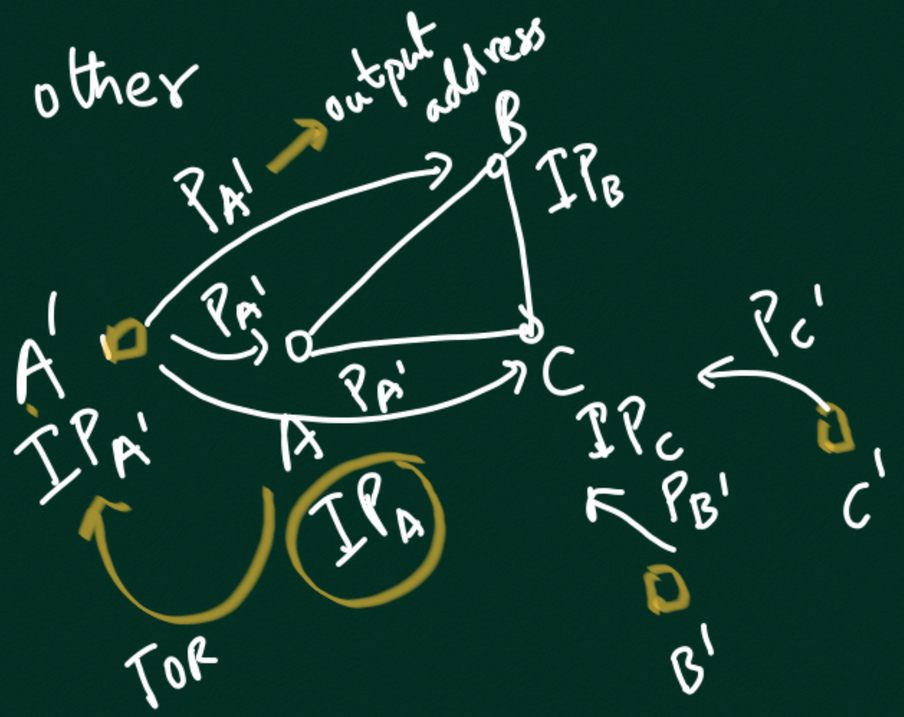
COIN-JOIN

Steps

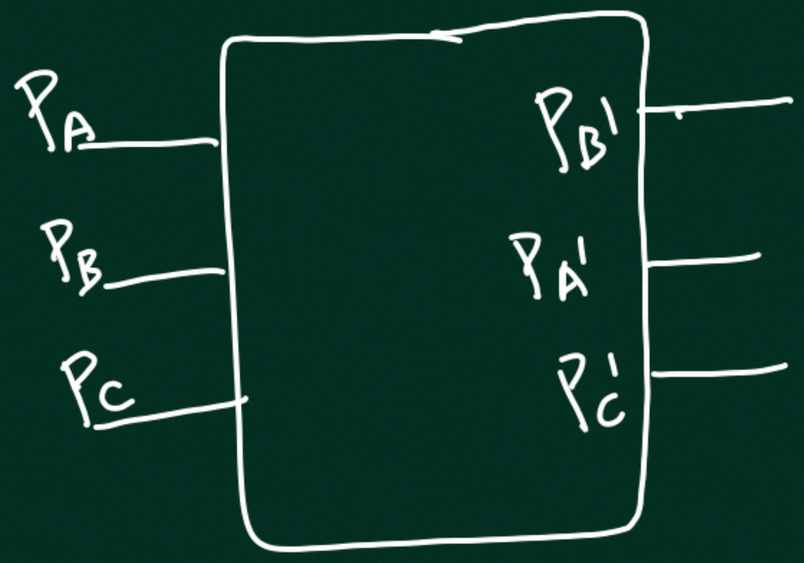
(1) Platform for A, B, C (Customers) to identify each other

(2) Share Input info with each other

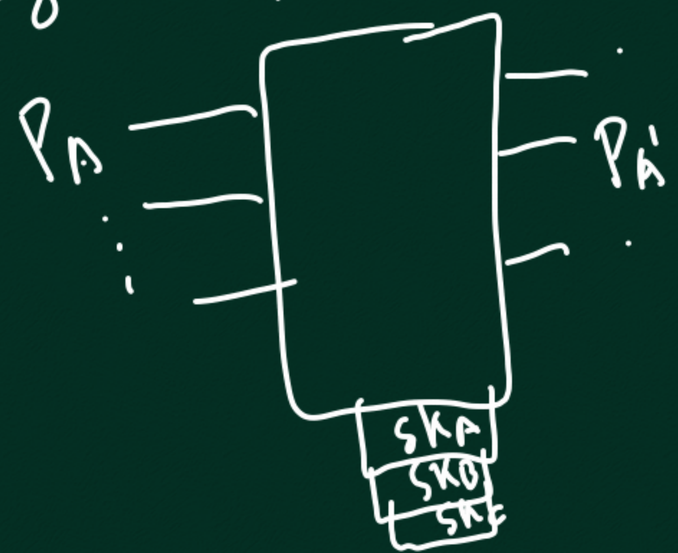




(3) Share o/p addr. using new IPs (say with TOR)



(4) Each signs txn, shares signatures with all



(5) Anyone b'casts txn to miner(s)

What can go wrong?

TORNADO CASH

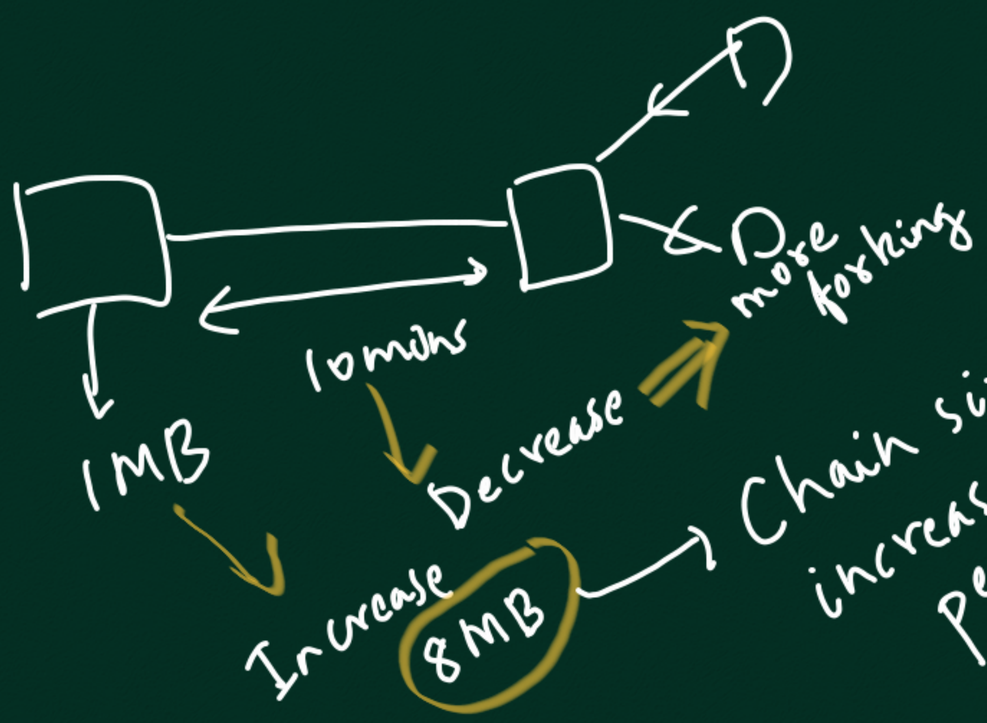
Avg. IAT $= \frac{1}{\beta}$

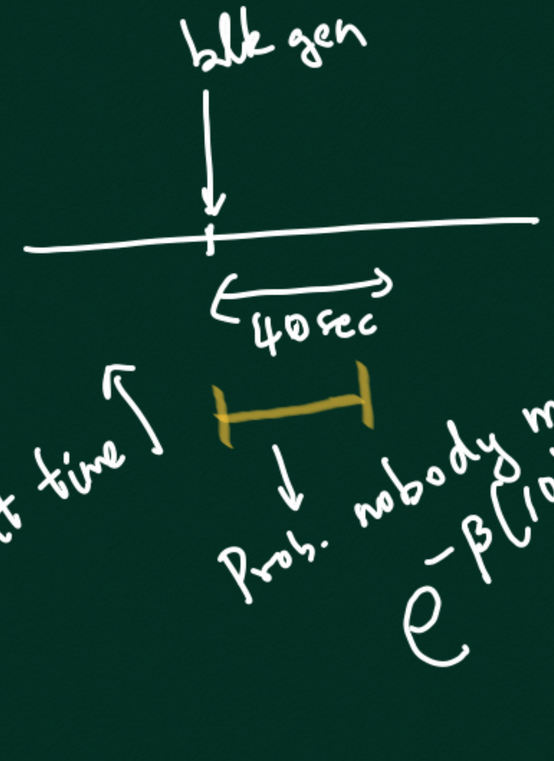
SCALABILITY

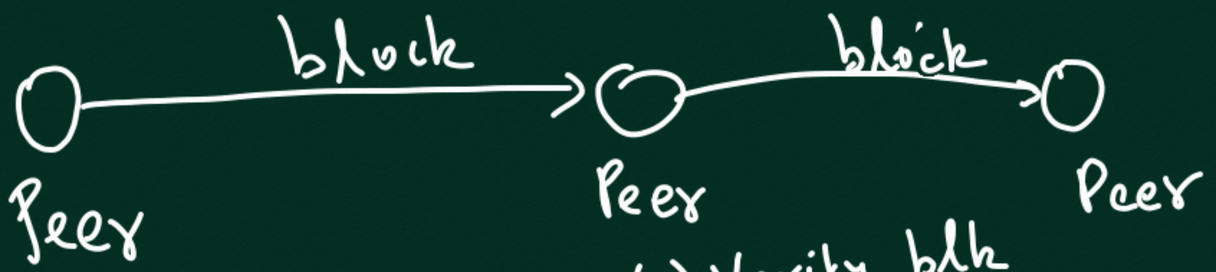
BTC: 7 txns/sec

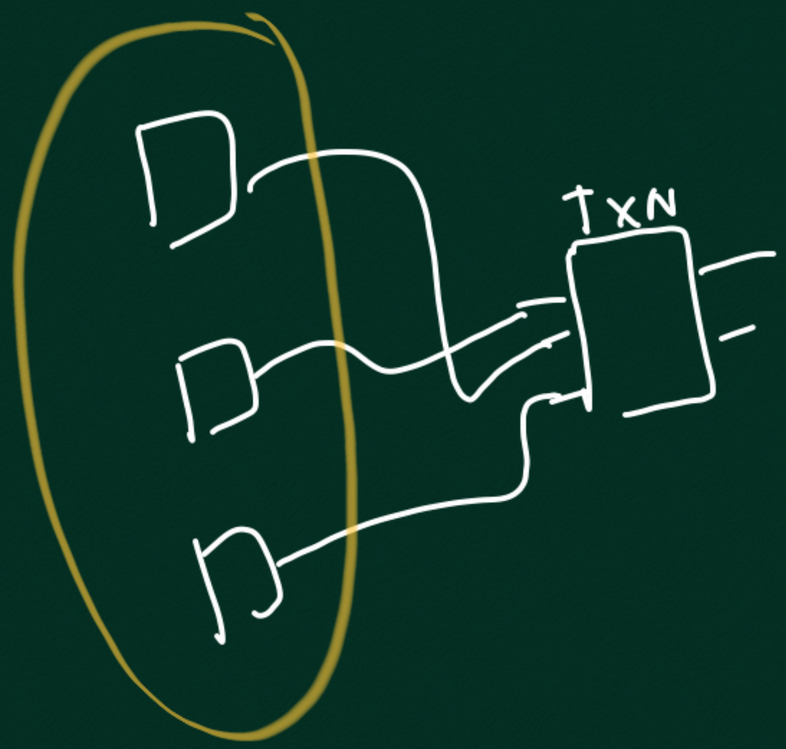
ETH: 10-20 txns/sec

50k txns/sec
VISA
Int → Exp(β)

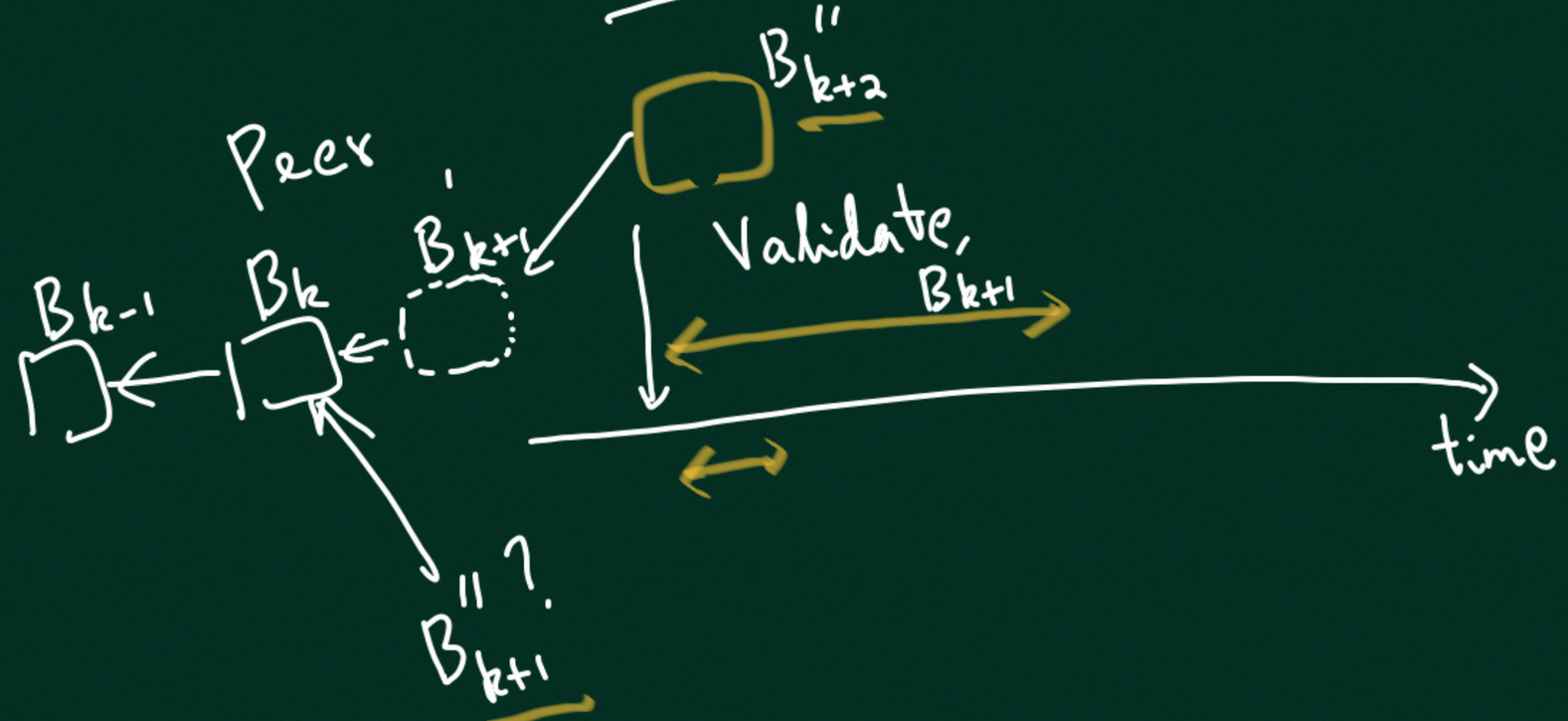




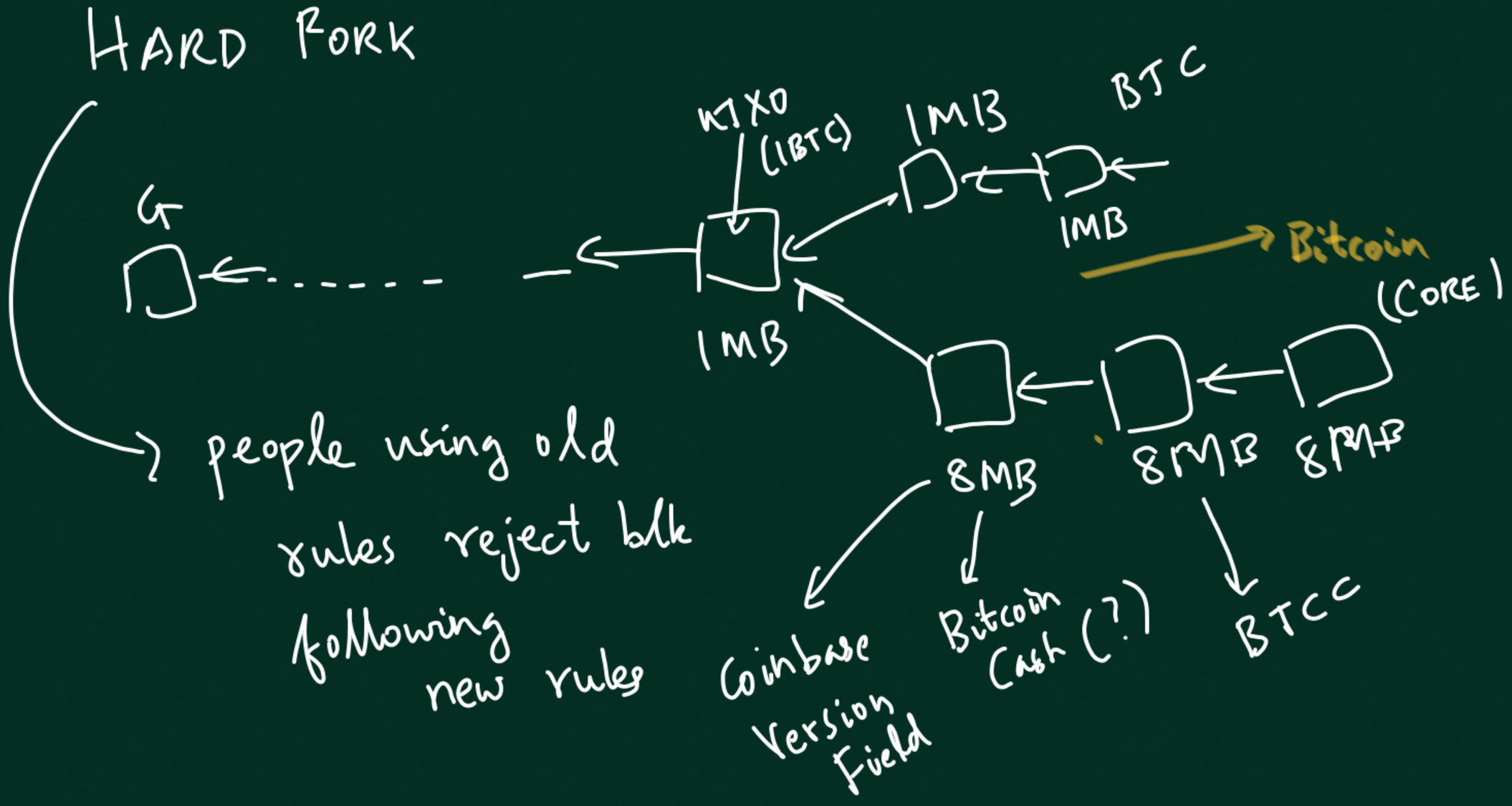




Verifier's Dilemma



HARD FORK


1MB
(1BTC)
1MB
BTC
1MB
Bitcoin
(CORE)
1MB
8MB
8MB
8MB
people using old
rules reject blk
following
new rules
Coinbase
Version
Field
Bitcoin
Cash (?)
BTCC