Attendance

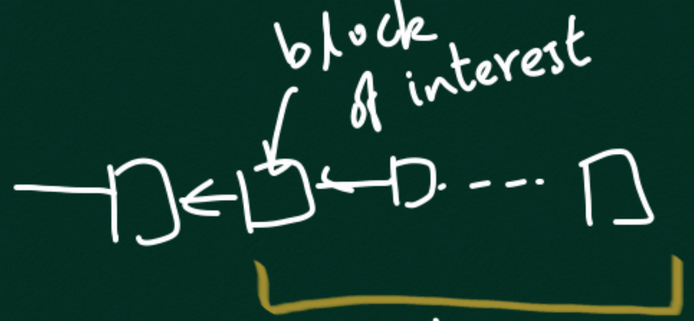
neglect network delays

$p = 1 - q$; q ; Net. Delay = Δ → max. time for info. to propagate

If $q < \frac{p}{1 + \Delta \cdot p}$ (const) → $\frac{1}{\text{inter-arrival time of blocks}}$

$q \overset{??}{<} p$

$\frac{\Delta \approx 10s.}{600} \approx \frac{1}{60}$ for bitcoin



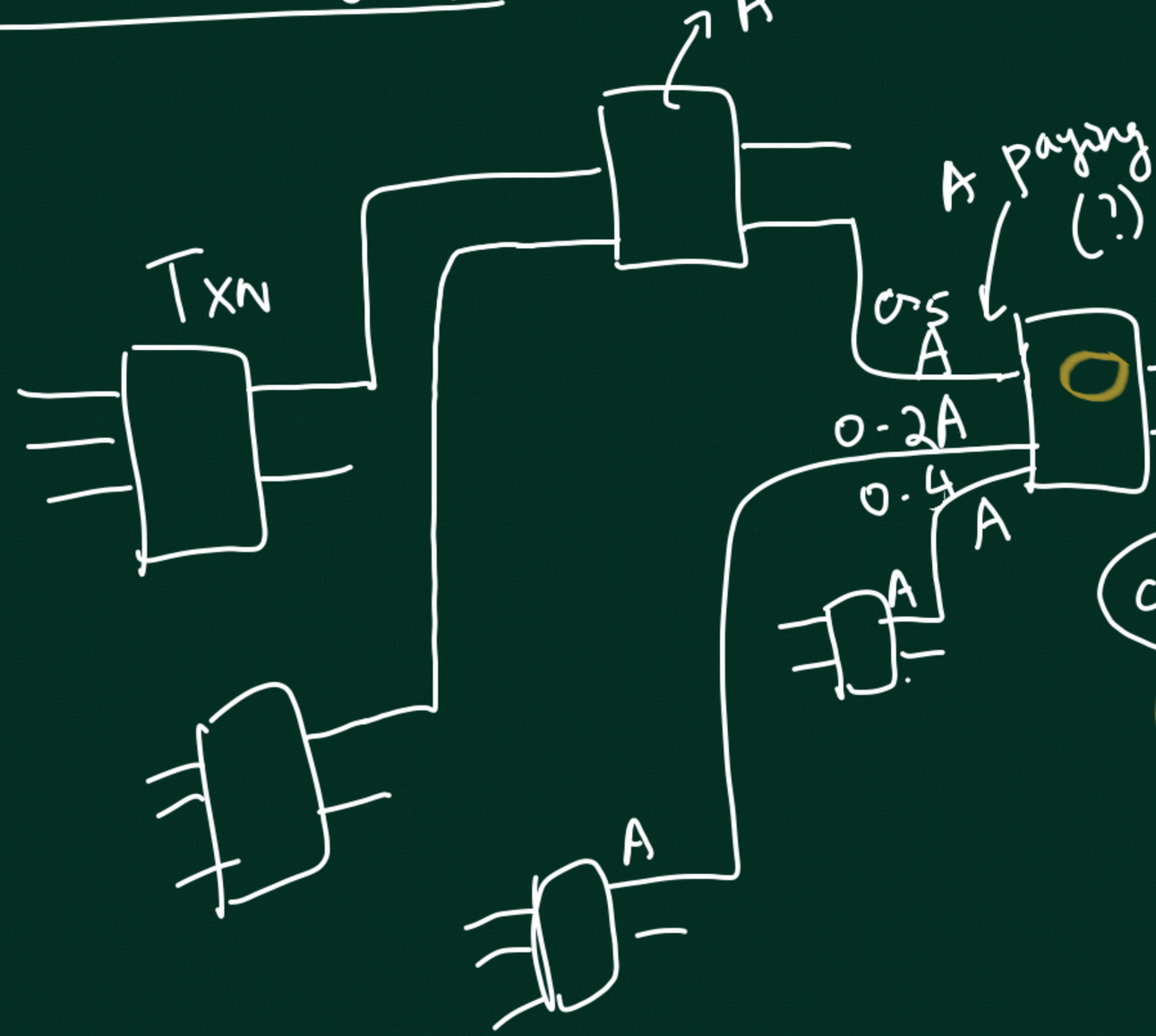
Prob. of block being orphaned $\approx e^{-\text{Const.}\,k}$

Privacy

+ No names or identities on block chain
  - ↳ no KYC

— ve : all txns visible to all

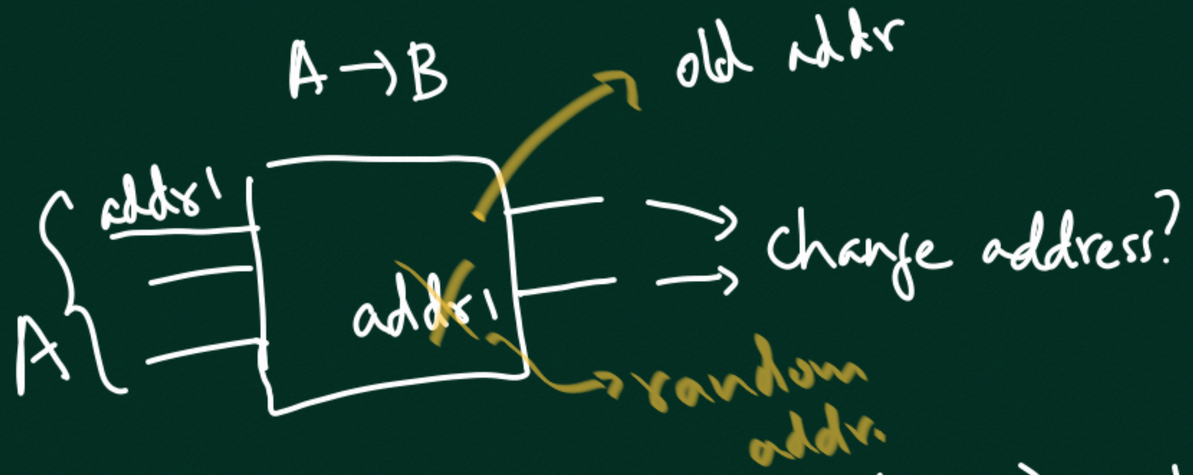
Transaction graph



Are there known public keys?

Heuristics

- All inputs have same owner



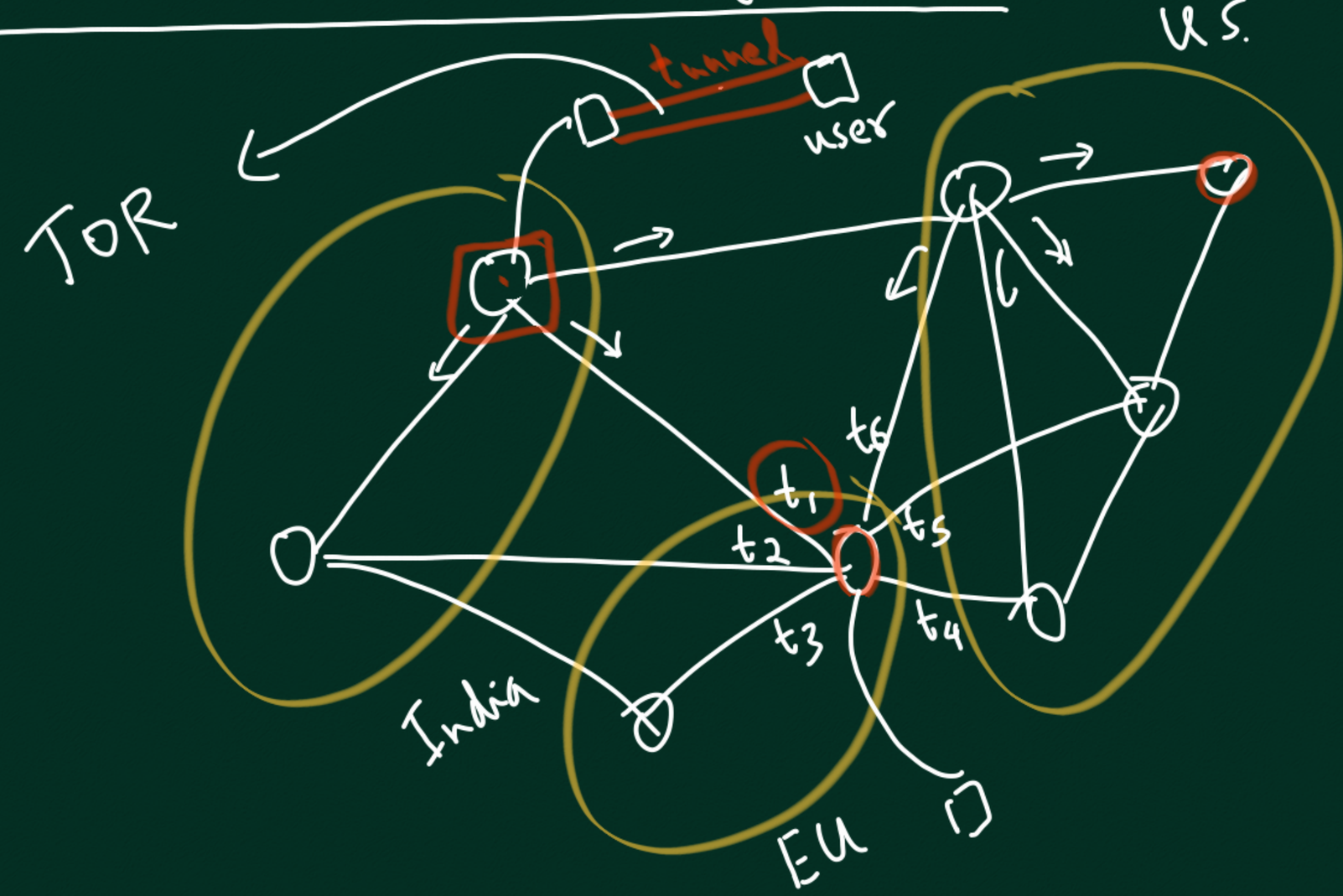
Fistful of bitcoin – (2013) Micklejon et al.

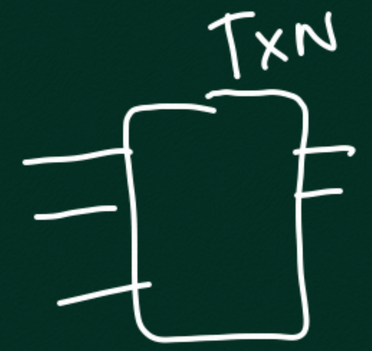
Wallet Software ⟶ early days, ch. add. was in particular o/p (e.g. 1st o/p)

Soln: randomly place change address

But, people used old addr. to receive money.

Network level de-anonymization



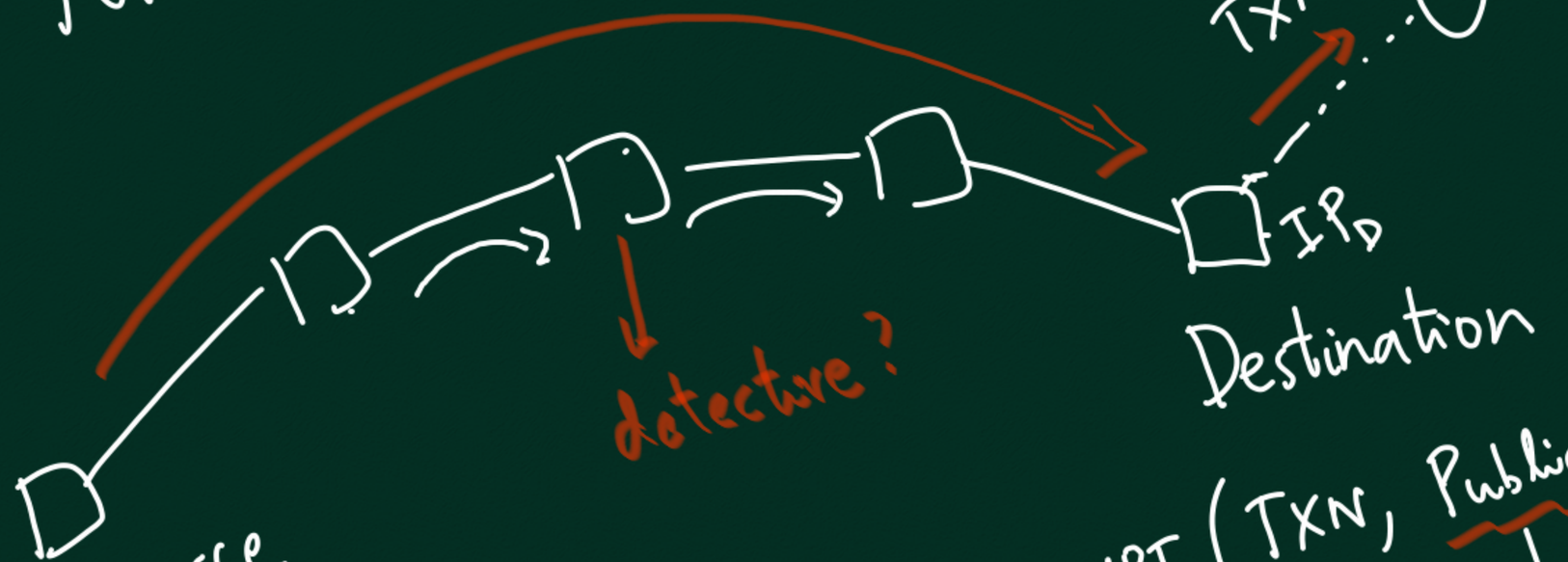


Ransomware

Onion routing

TOR → not Bitcoin network

MSG (TXN) → Encrypted



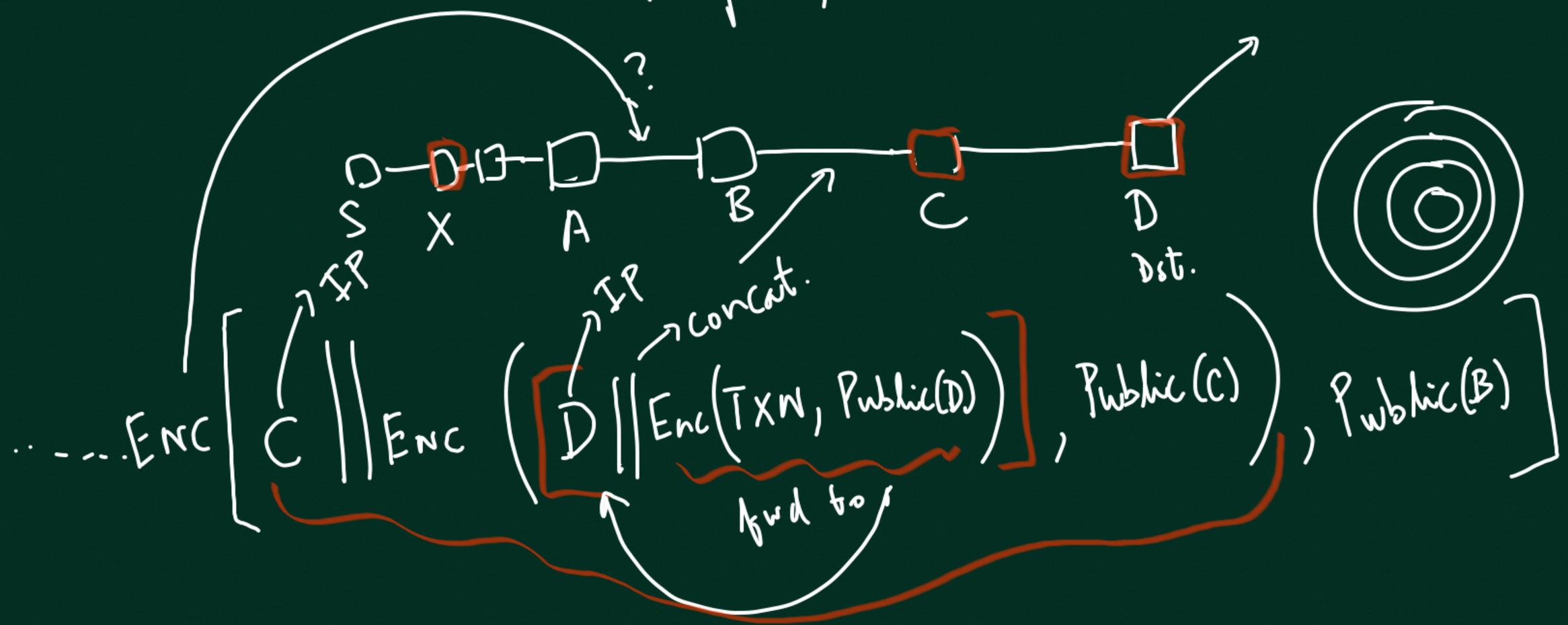
Encrypt (TXN, Public(D))

Decrypt (, Secret(D)) ← not bitcoin

TXN

What TOR tries to achieve:

Intermediate TOR node only knows neighbours in path, not Src. & Dst.

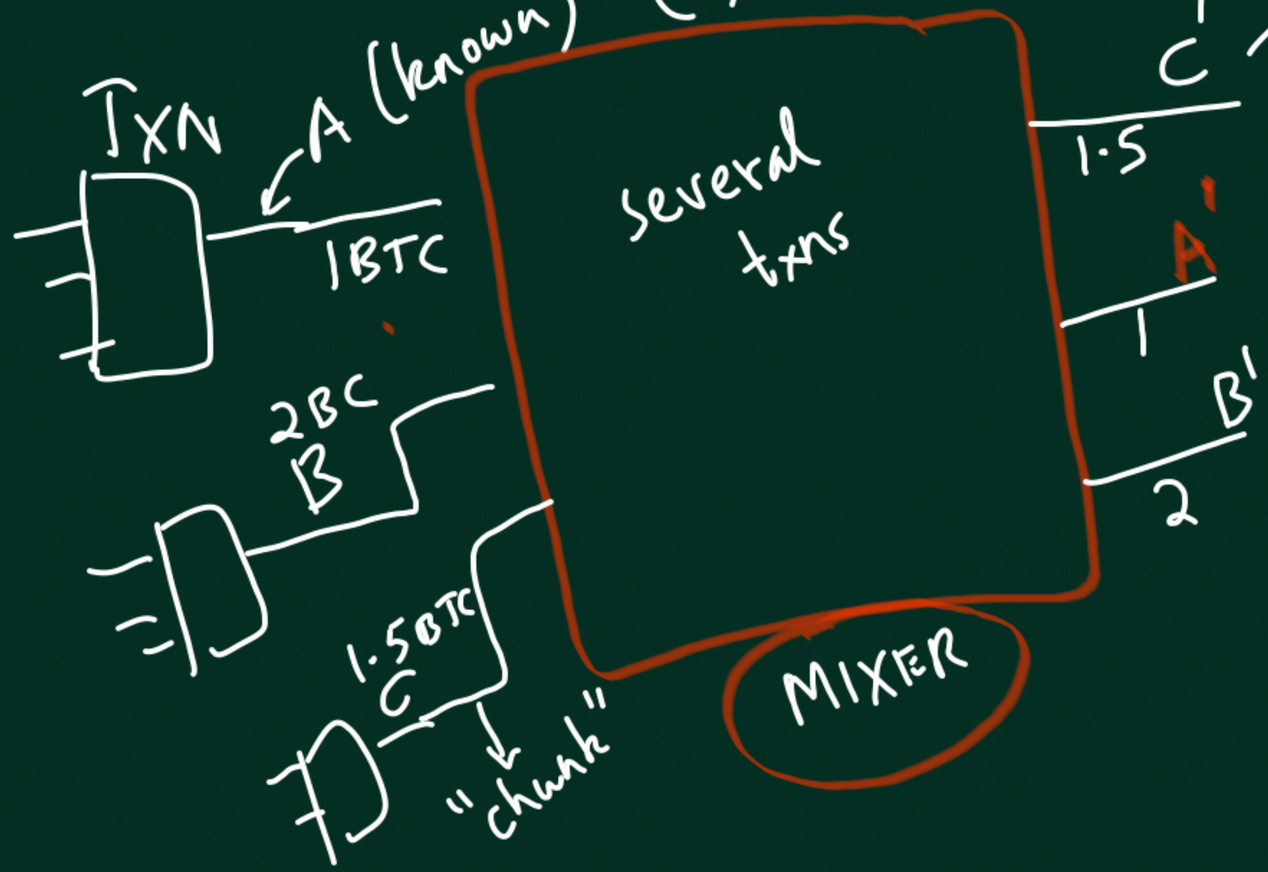


How to increase anonymity in Txn graph?

MIXING

A → Service
(1) Txfer his BTC to S.P.
(2) A' etc. to Service (S.P.) provider

Arvind Narayanan



Want (Good mixing)

- All chunks of Same amount