

# Scalability

## 1. BITCOIN-NG



## L1 Scaling

L1: stored on blockchain Data Computation  
Done by miners

A diagram illustrating L1 scaling. It shows "Data" being stored on the blockchain. The word "Computation" is written below "Data", with an arrow pointing down to the text "Done by miners".

L2: a) on chain   
b) off-chain   
computation off-chain (not by miners)

A diagram illustrating L2 scaling. It shows two options: "a) on chain" and "b) off-chain". "a) on chain" is connected to a box labeled "computation off-chain (not by miners)". "b) off-chain" is also connected to the same box. The word "off-chain" is written above the box, and "computation" is written below it.

## Attendance

Extra Class: Wed  
8:30 am - 9:30

Away: Sep 22-26

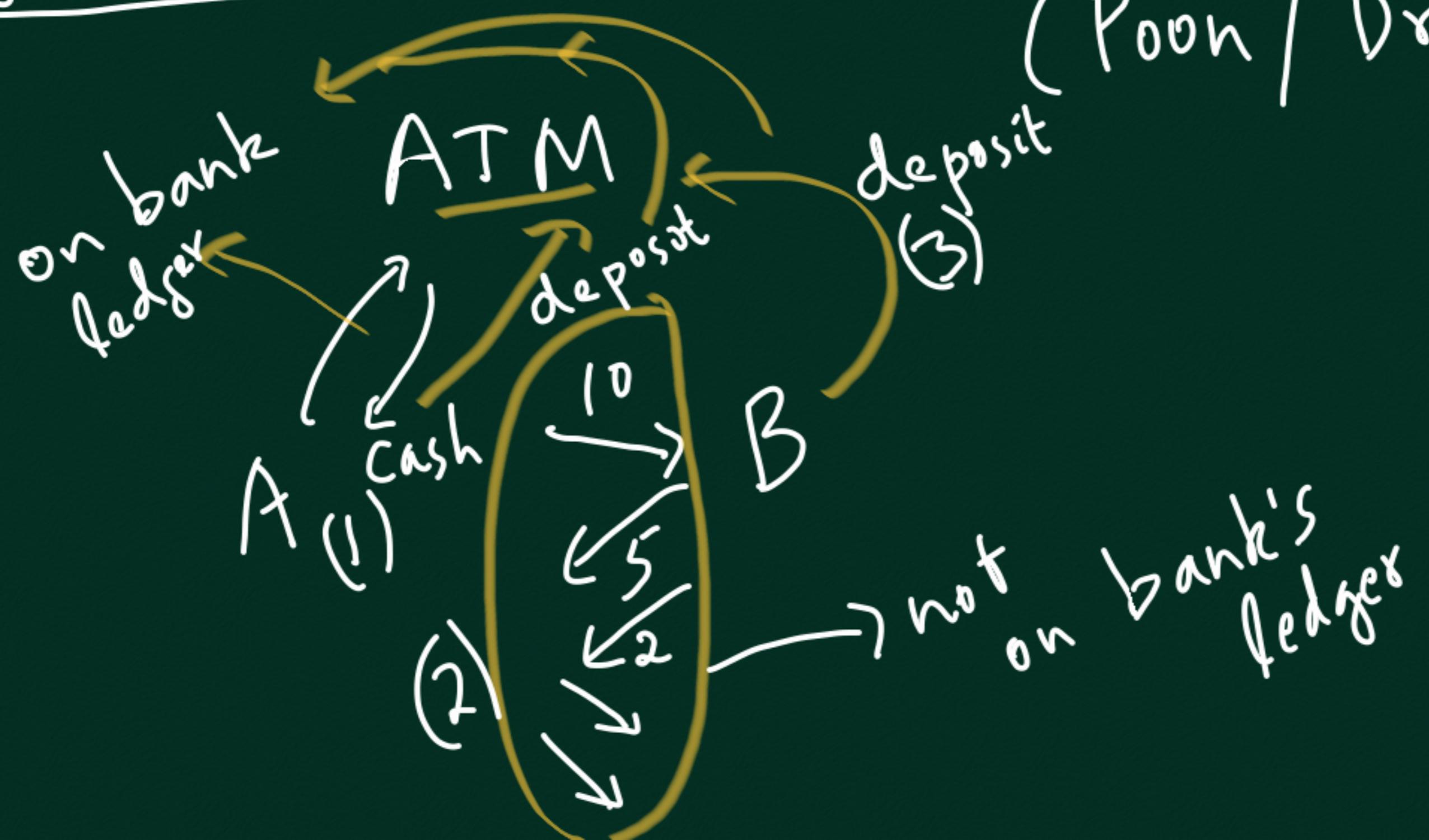
MID SEM

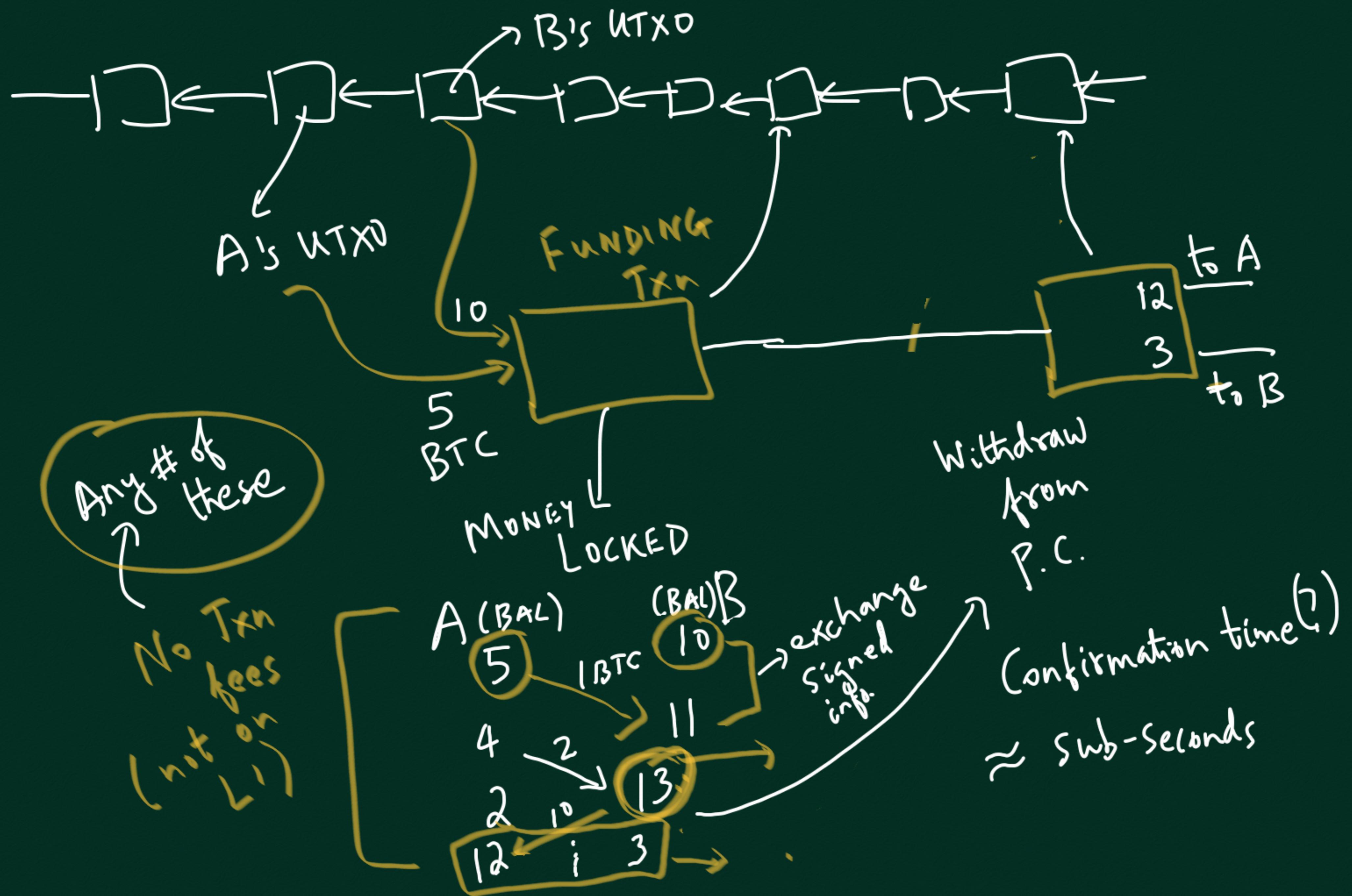
15<sup>th</sup>, 18:30 - 20:30

LA 001

L2 → Payment Chl. Networks ( Bitcoin / Ethereum )  
...  
→ Rollups ( Ethereum )

Payment Chl. Networks: LIGHTNING NETWORK  
( Poon / Dryja ) → 2016





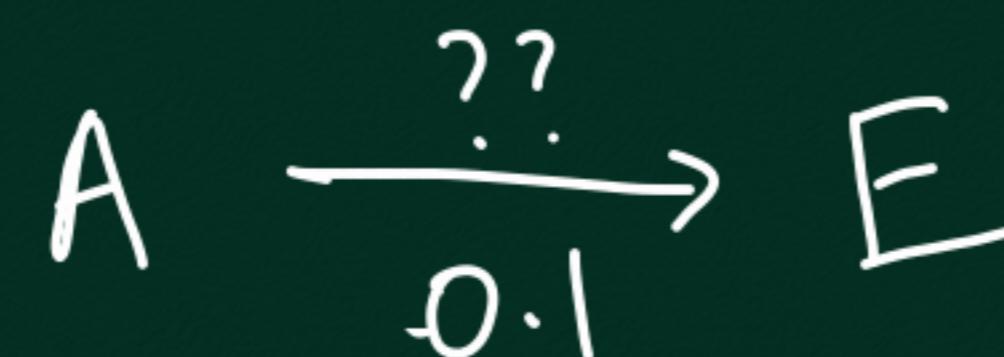
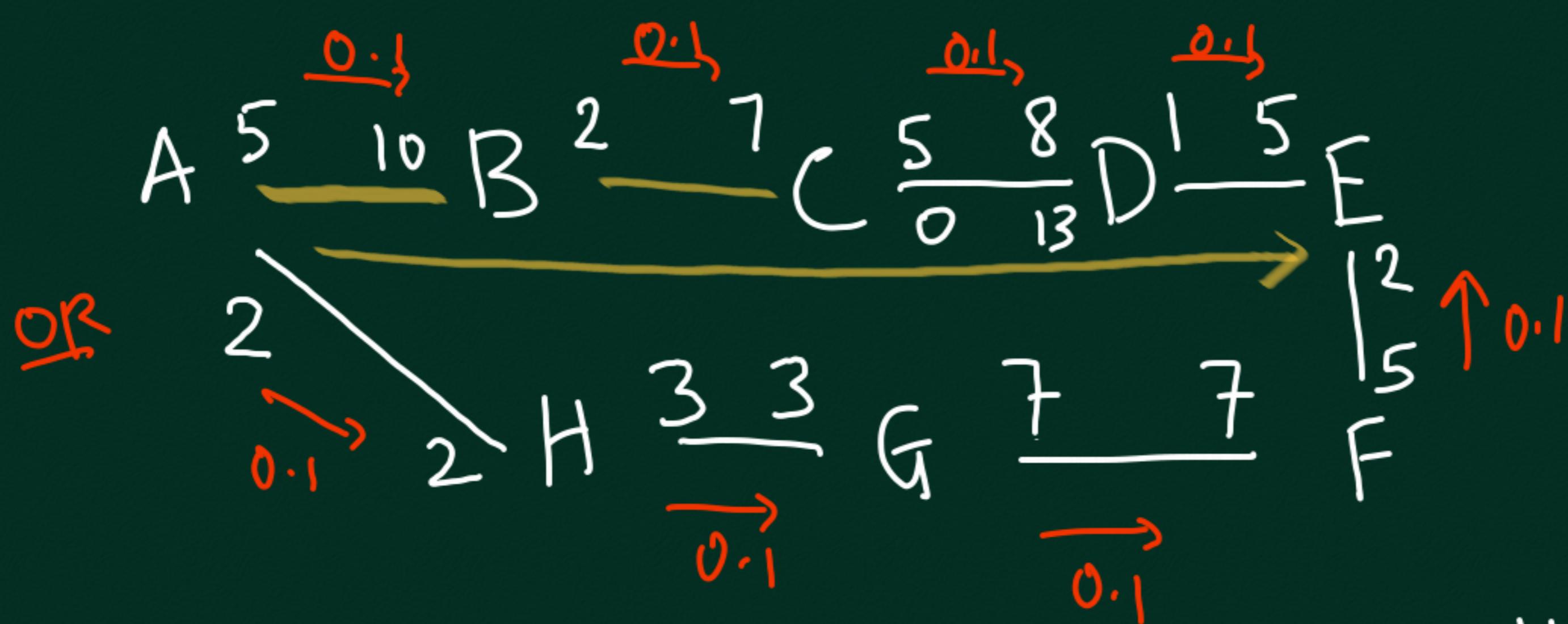
What we want

- 1) Either party can independently quit P.C. at any time
- 2) Only latest state should be used while withdrawing

Shortcomings  
of P.C.

Watch  
Tower

- 1) Cannot pay a 3rd party (e.g. A  $\xrightarrow{\text{pay}} C$  with his 5 BTC)
- 2) Both parties need to continuously monitor blockchain for "old state" withdrawal
- 3) Net payments in either direction (limited by initial balance)



Segwit: Segregated

Witness

P.C.N.



Network

Q 1) How to ensure payment goes through after finding path with large enough bottleneck

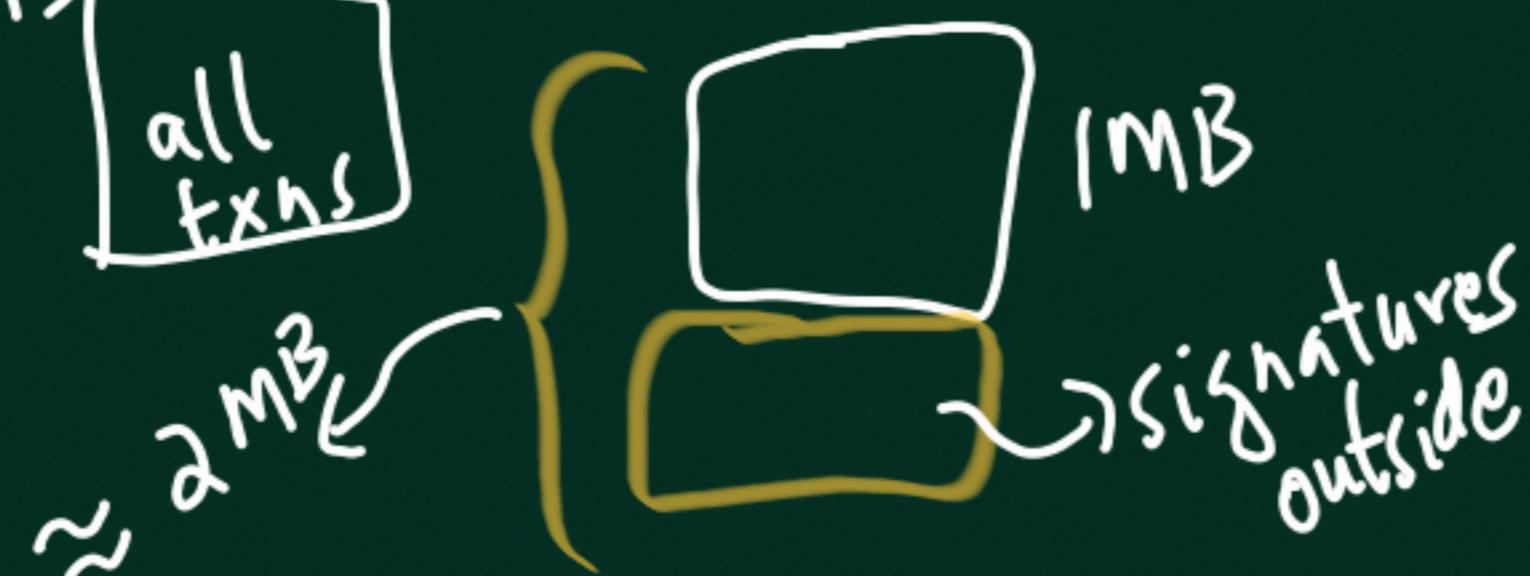
2) How to find such a path?  
 ↳ since only initial balances known.

Bitcoin

2009

Hard Fork

Soft Fork



2016  
L.N.

2019 (?)

Segwit

(Soft Fork)

L.N.  
active

BIP: Bitcoin Improvement

Proposals

EIP:

DELAYED EXEC

