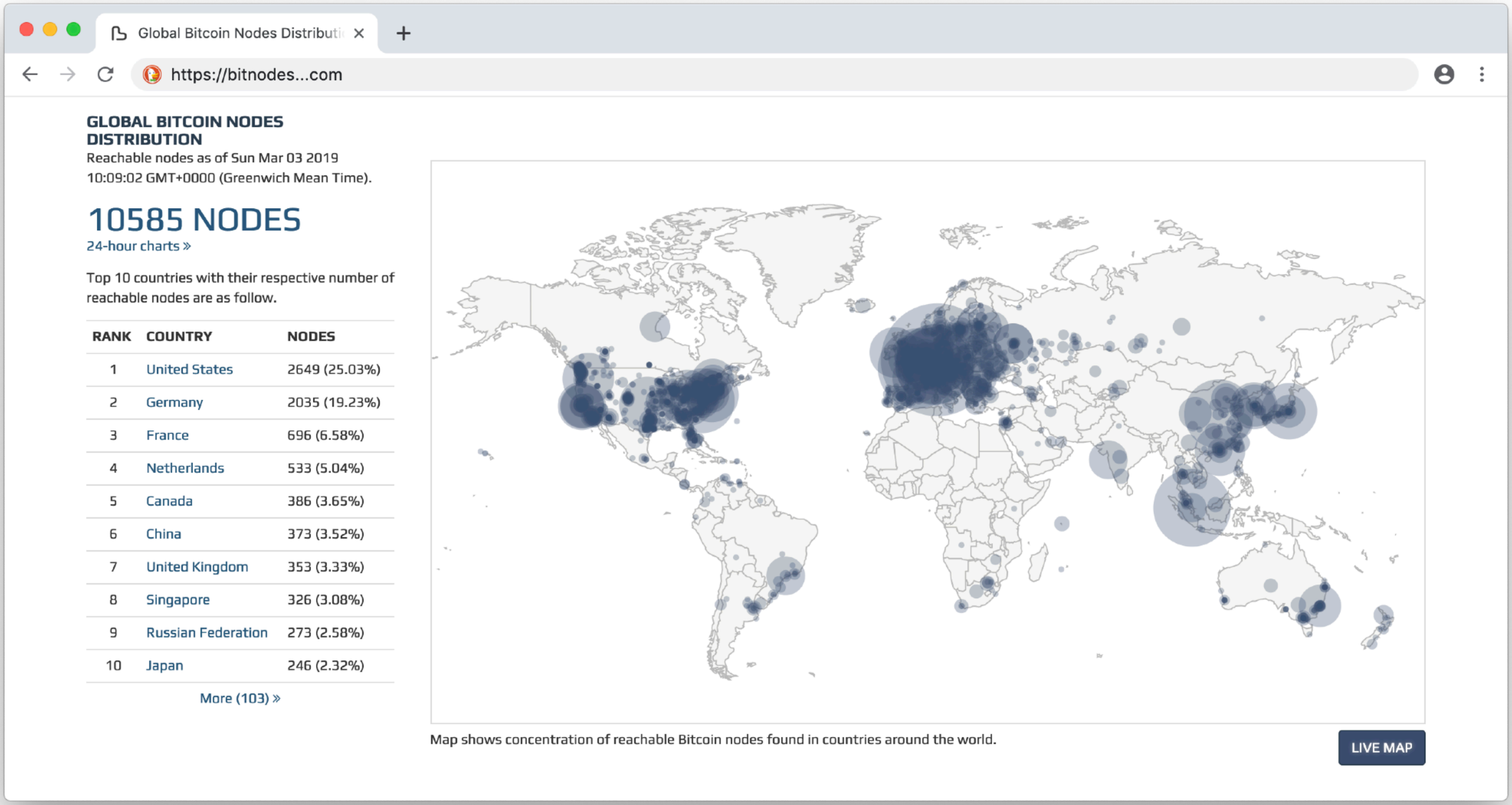
Blockchain Privacy Network Layer

Peer to Peer Network

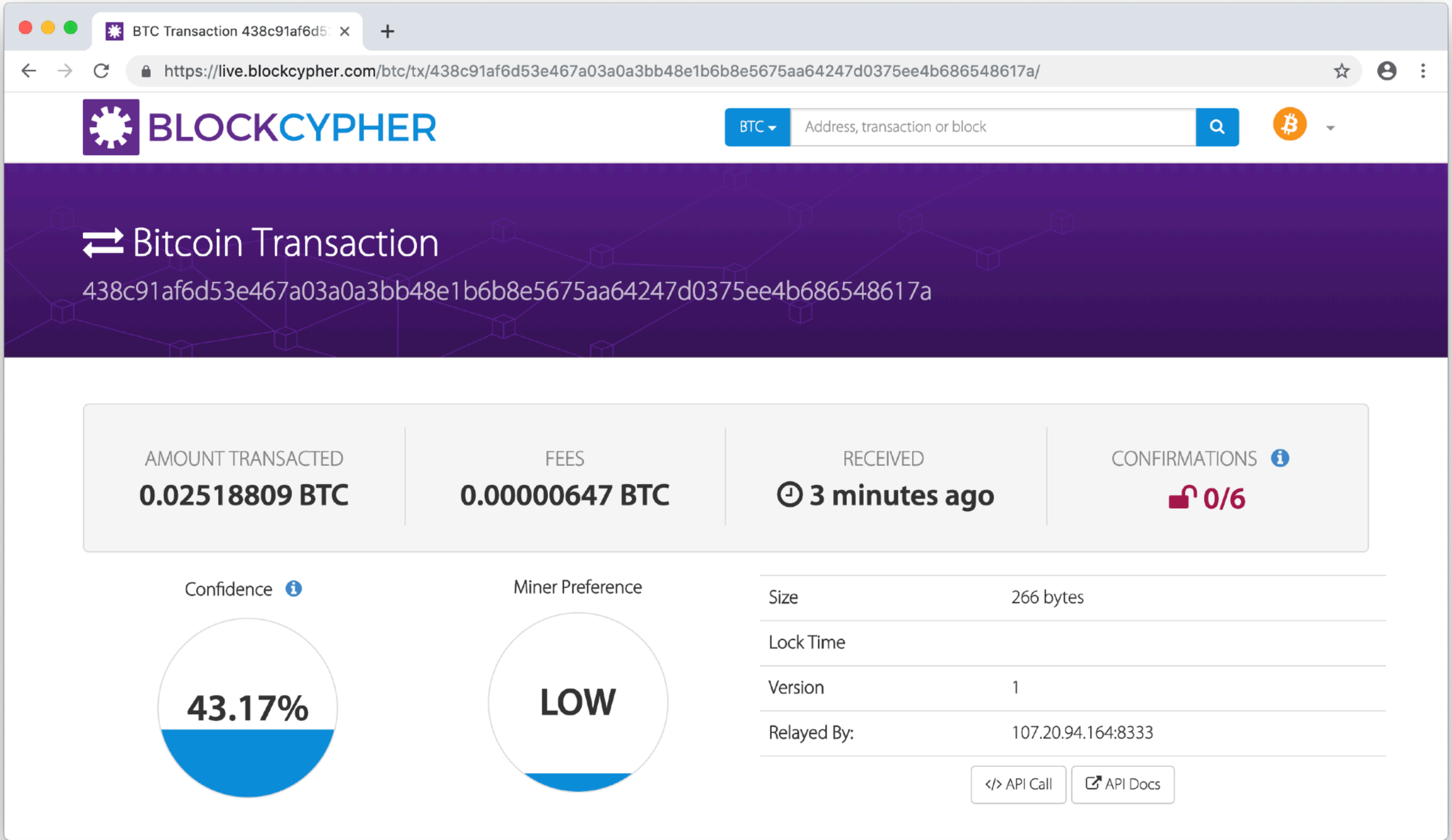
- Loosely connected network
- Validating nodes / Lightweight clients / Miner



Network Privacy Leakages

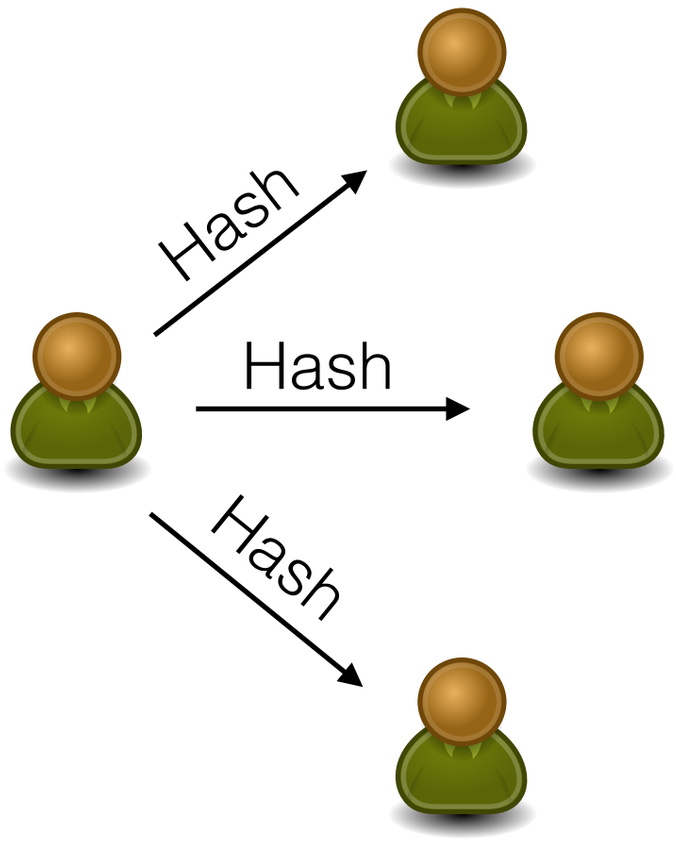
- IP addresses of other nodes
- Client version -> Fingerprinting
- Port scans can reveal operating system
- Which transactions are forwarded?
- I see a transaction first from you, are you the originator?

Network Privacy Leakages



Remember?

1. Transaction/Block hash broadcast



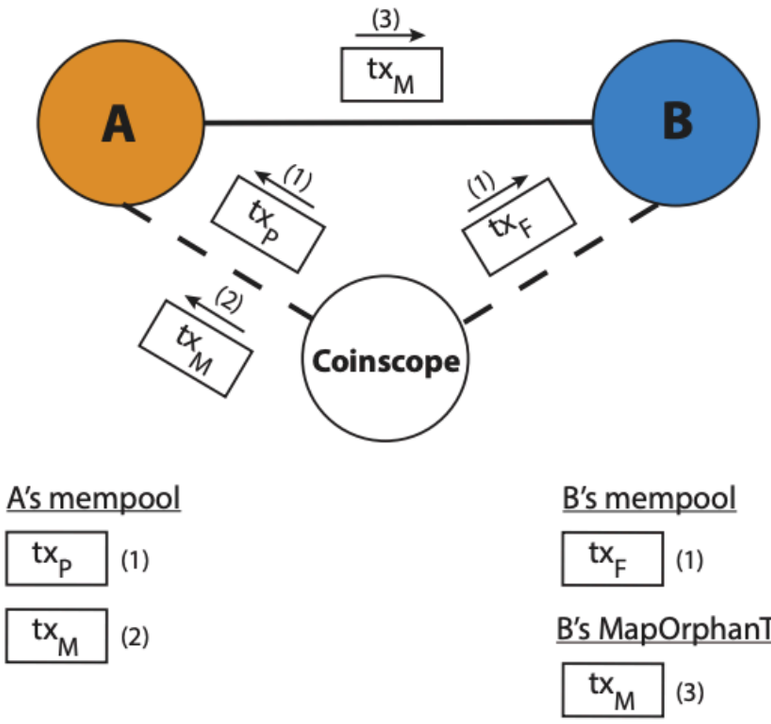
Broadcast

2. Transaction/Block request

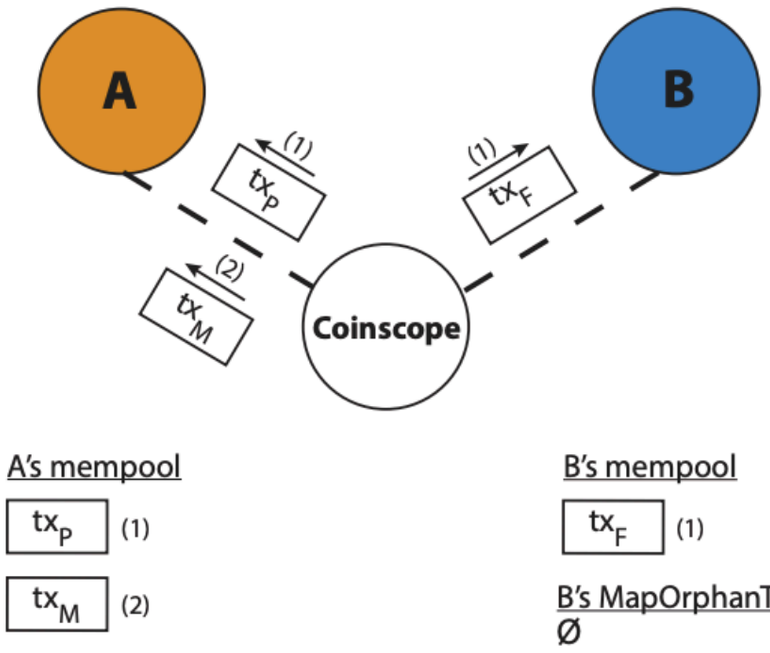
TCP/IP

Port 8333

TxProbe



(a) Basic positive edge inferring technique between two nodes.



(b) Basic negative edge inferring technique between two nodes.

https://arxiv.org/pdf/1812.00942.pdf