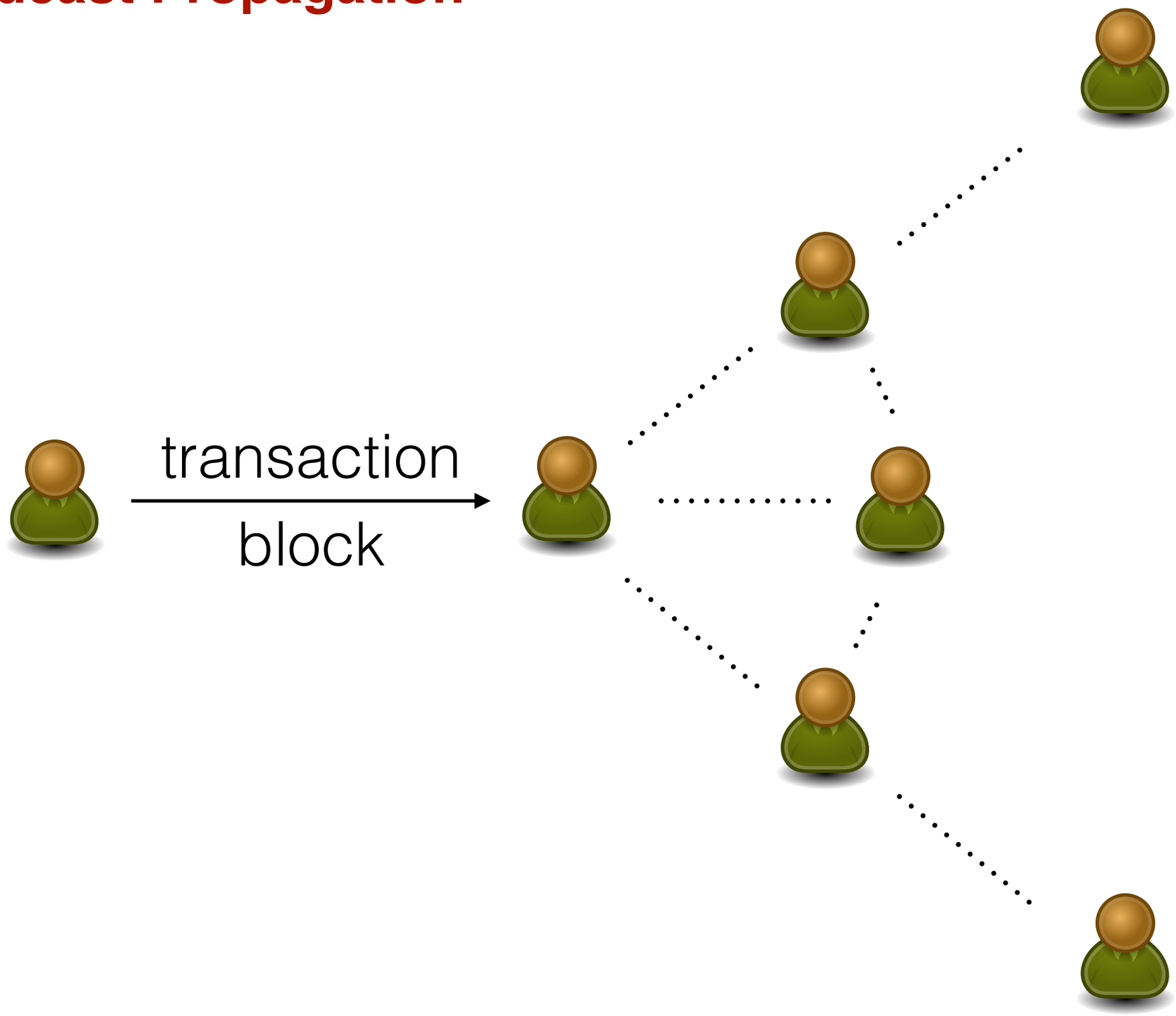
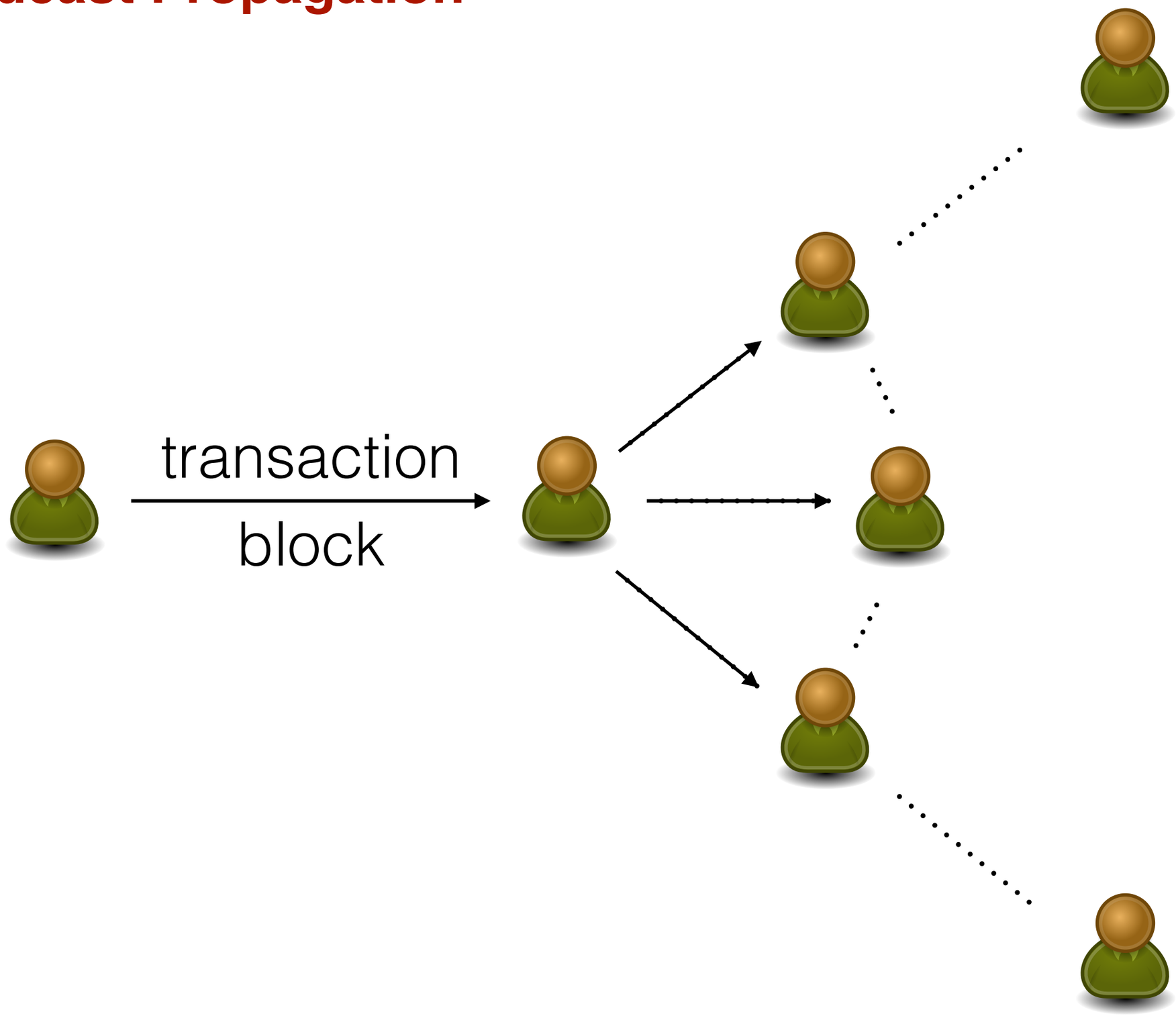
Network Gossip Protocol

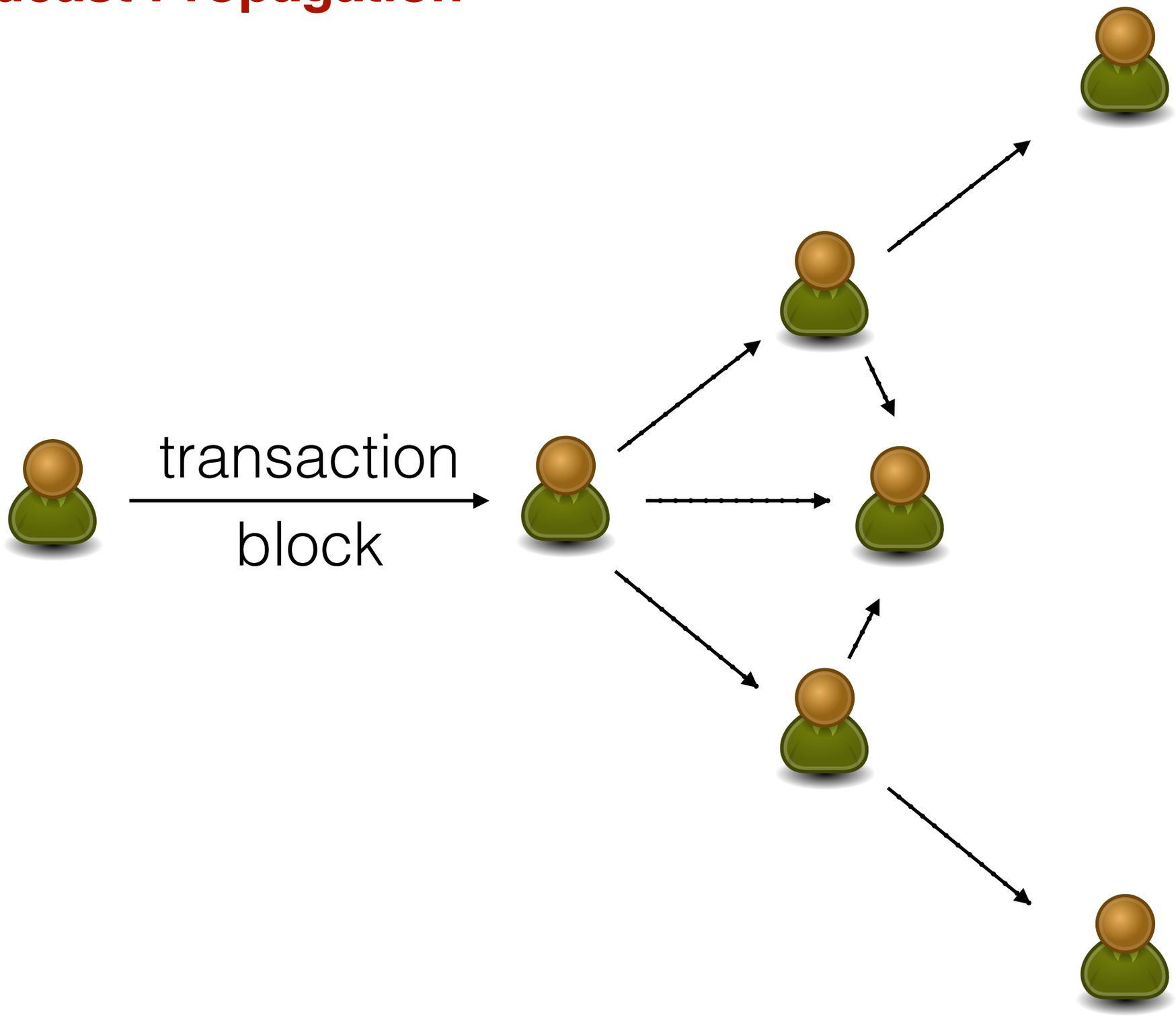
Broadcast Propagation



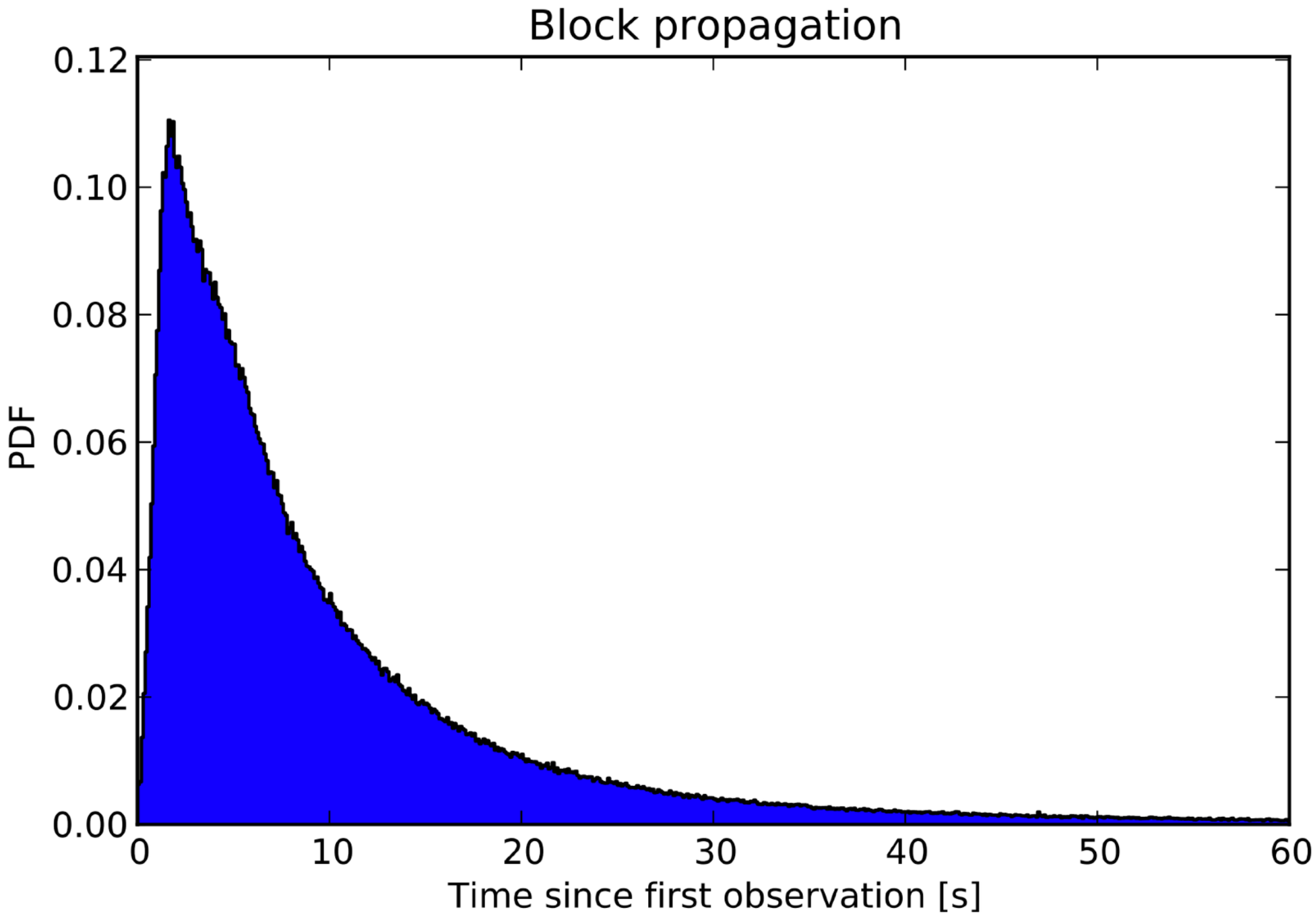
Broadcast Propagation



Broadcast Propagation

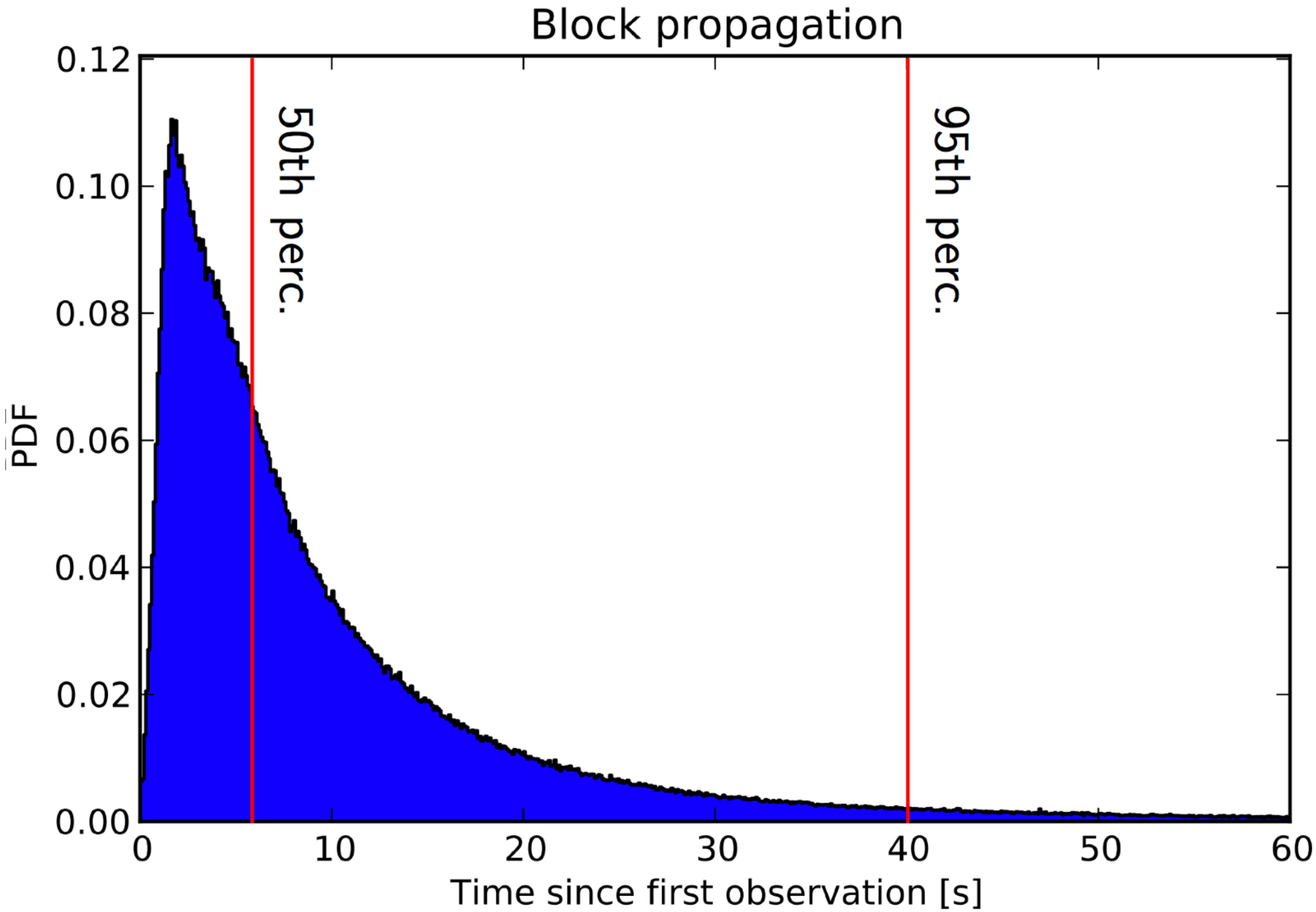


Broadcast Propagation



* Christian Decker et al., Information Propagation in the Bitcoin Network

Broadcast Propagation



* Christian Decker et al., Information Propagation in the Bitcoin Network

Propagation Methods

Standard

- Send first the hash of an object, transaction/block
- Recipient requests the object
- Sender transmits the object

Send Headers

- Send first the block header (no more block hash)
- Then block

Unsolicited Block Push

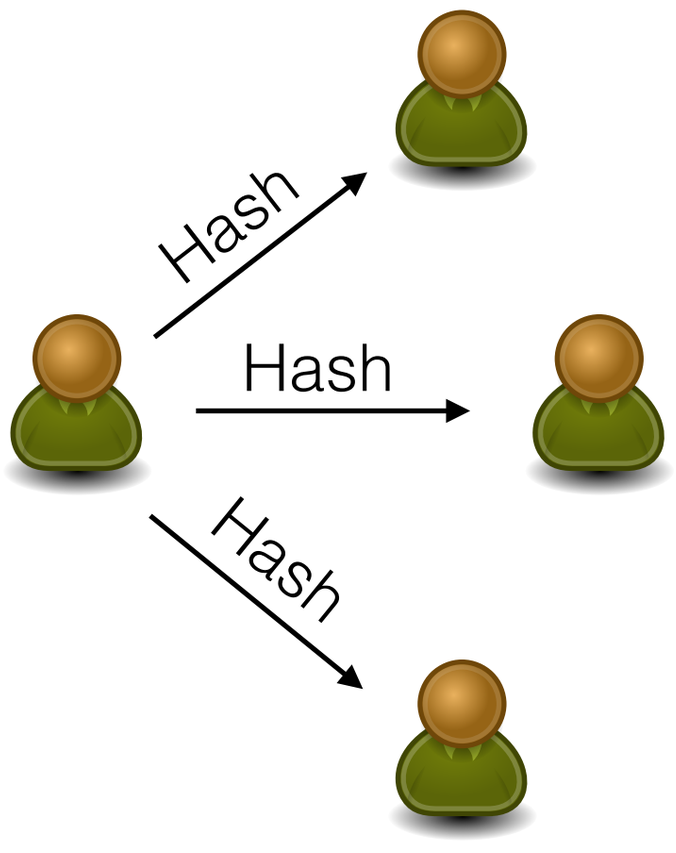
- Miners can push a block directly, without pushing the header

Fibre (Fast Internet Bitcoin Relay Engine) Network

- Optimized network for miners

Standard Transaction/Block advertisement

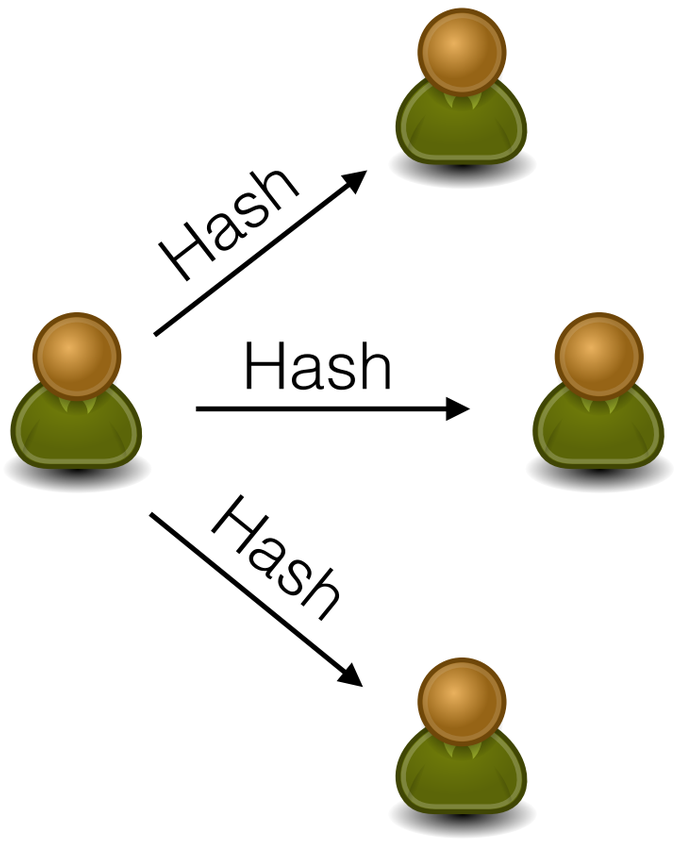
1. Transaction/Block
   hash broadcast



Broadcast

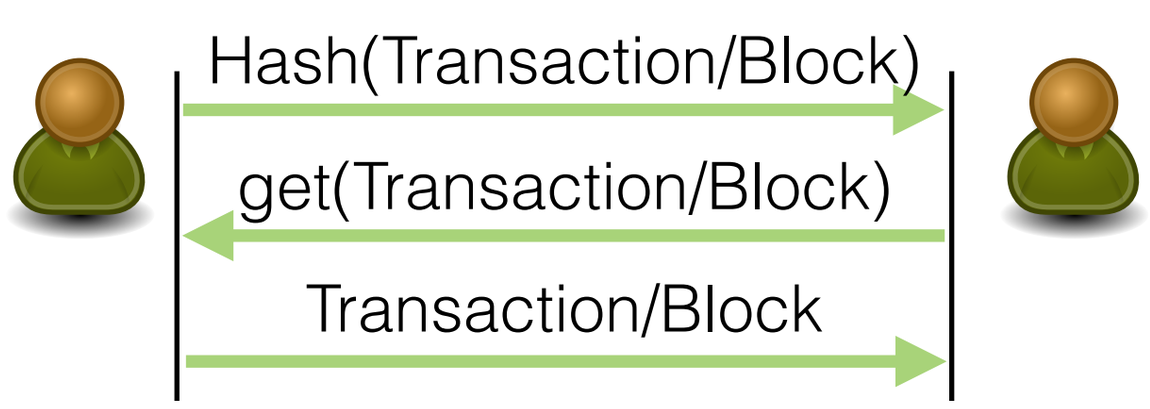
Standard Transaction/Block advertisement

1. Transaction/Block hash broadcast



Broadcast

2. Transaction/Block request

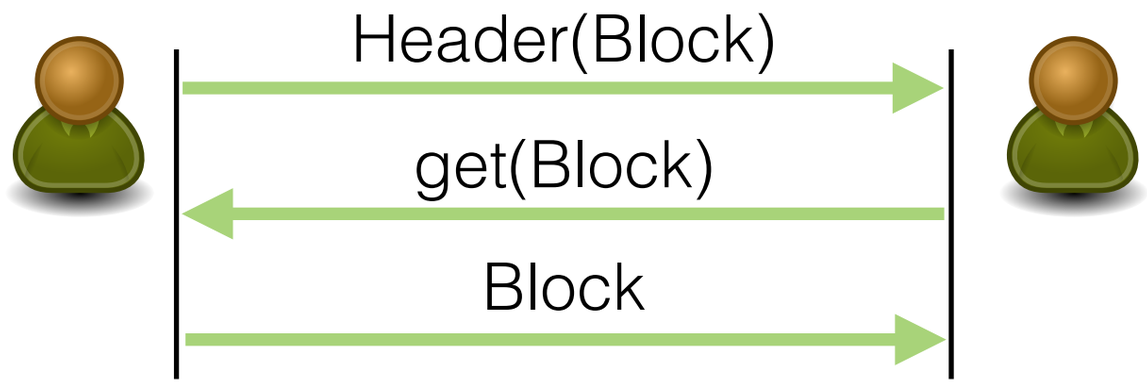


Request from only 1 peer!

Send Headers Block advertisement

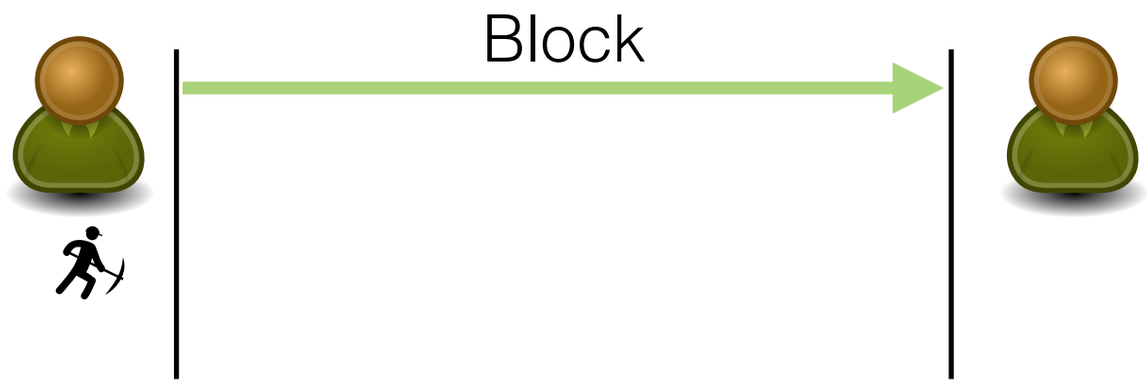
Header in Bitcoin about 80 bytes,
hash about 36 bytes

Send Headers Block advertisement

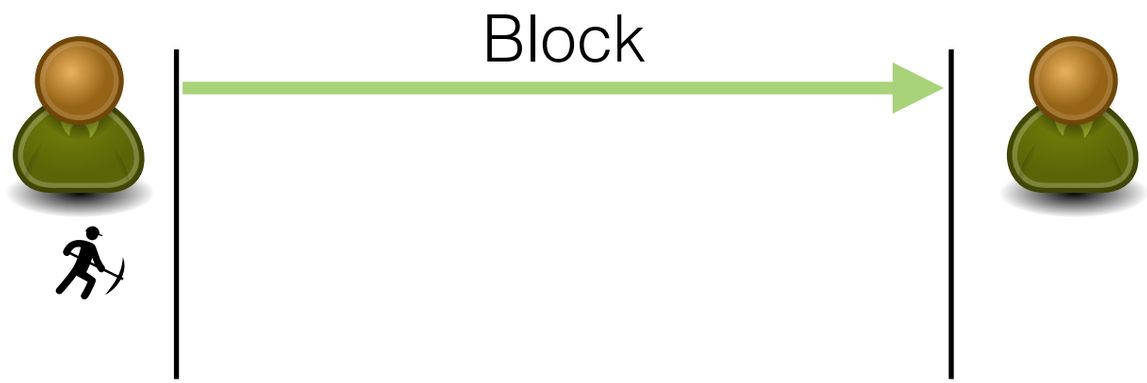


Header in Bitcoin about 80 bytes,
hash about 36 bytes

Unsolicited Block Push



Unsolicited Block Push



Nobody else knows about the block

Bitcoin Fibre

- Fibre node sends a short block sketch
  - List of short hashes, lengths

- Receiver can reconstruct block based on memory pool and construct a block with holes

- Fibre sender breaks block into chunks and sends error correction data
  - Receiver can reconstruct block, without the sender knowing what's missing.

- Once received and reconstructed the block, the fibre node emits novel chunks —> no redundancy.

- UDP based —> no ramp up

https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki