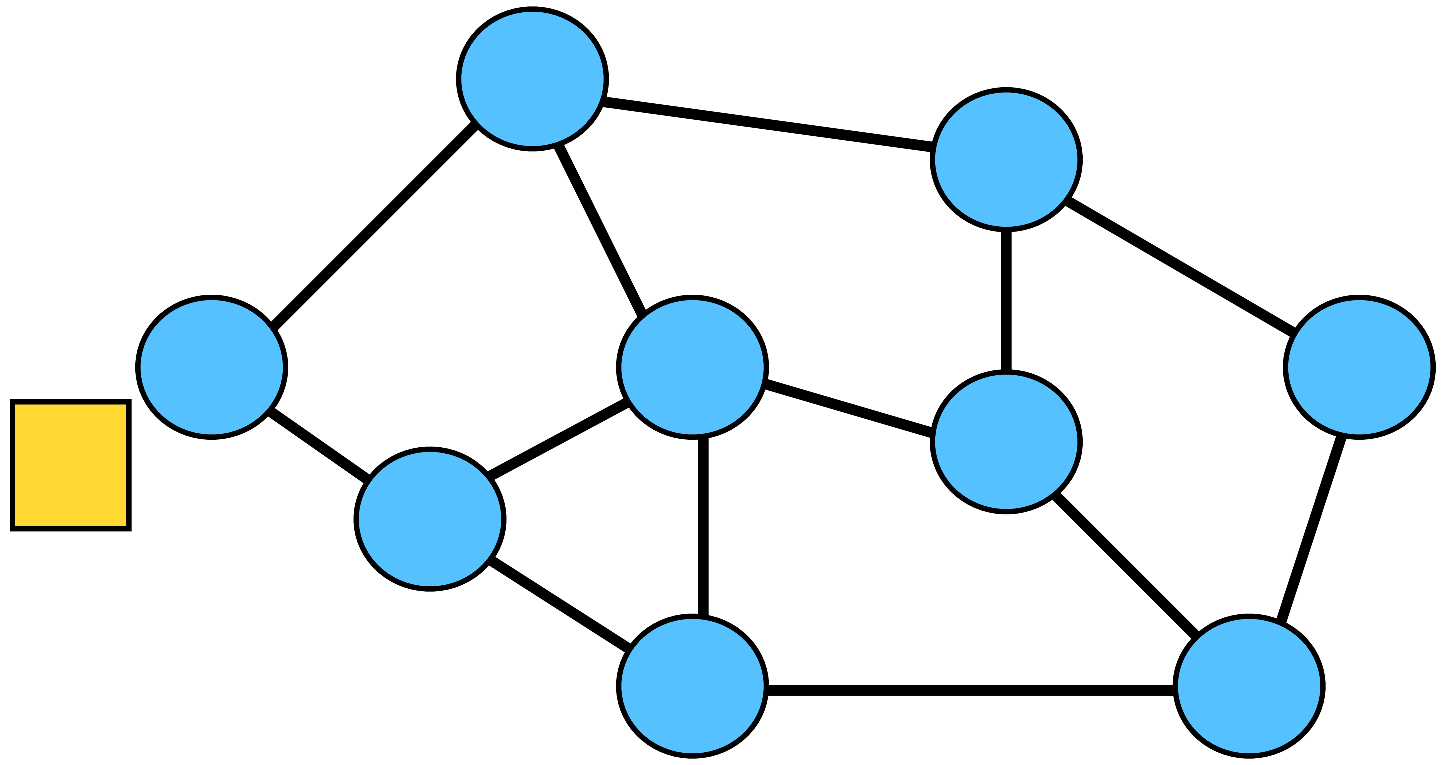
Network attacks

Leander Jehl

P2P Networking

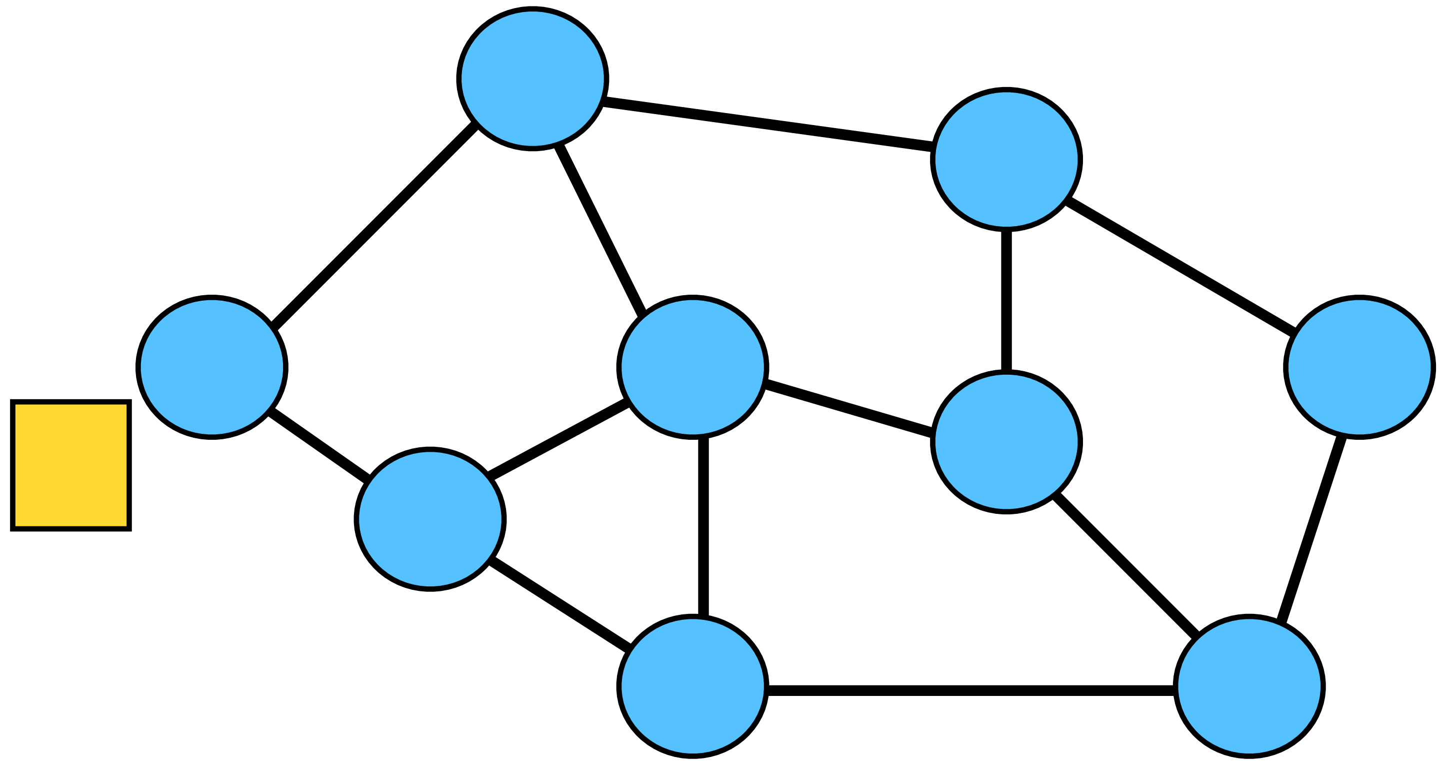


Bitcoin:

- 10.000 nodes
- each node randomly chooses 8 nodes to connect to
- nodes refuse connection when they have 128.

How can you broadcast a 1Mb block?

P2P Networking



Broadcast block:

- Broadcast inventory message including block hash
- Receiving new inventory, request block
- Send block

Block is only send from one neighbor

P2P Networking

Broadcast block:

- broadcast inventory
- request block
- send block

Block is only send from one neighbor

Timeout:

- On request set timeout
- If block not received within timeout, send new request (to different neighbor)

Bitcoin:

- Timeout is 20 minutes

P2P Networking - Delivery denial attack

Broadcast block:

- broadcast inventory
- request block
- send block

Block is only send from one neighbor

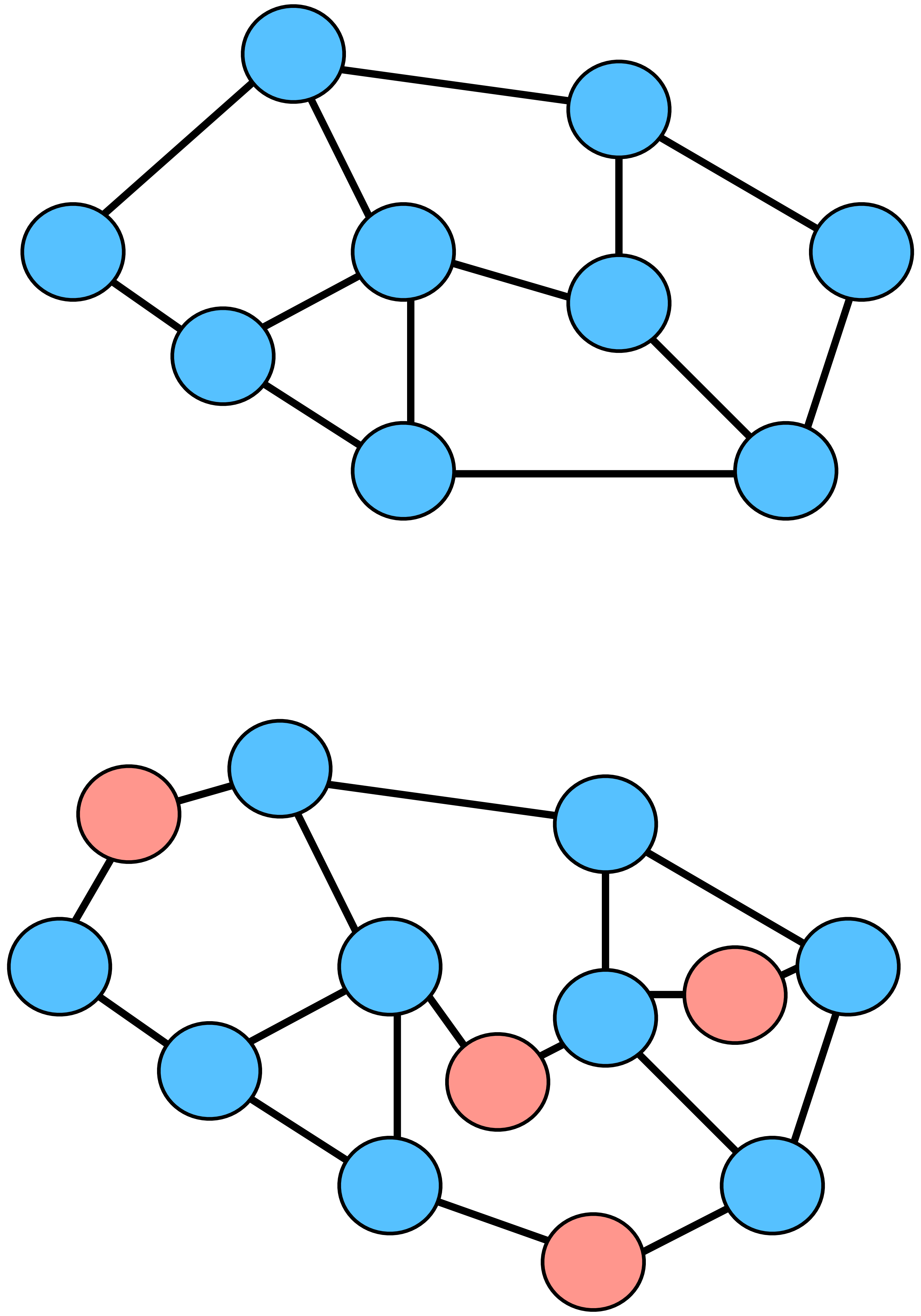
Delivery denial attack

- send out inventories
- do not send block

P2P Networking - Sybil attack

Sybil attack

- Attacker registers many nodes
- *Can affect connectivity*
- *Can affect network latency*

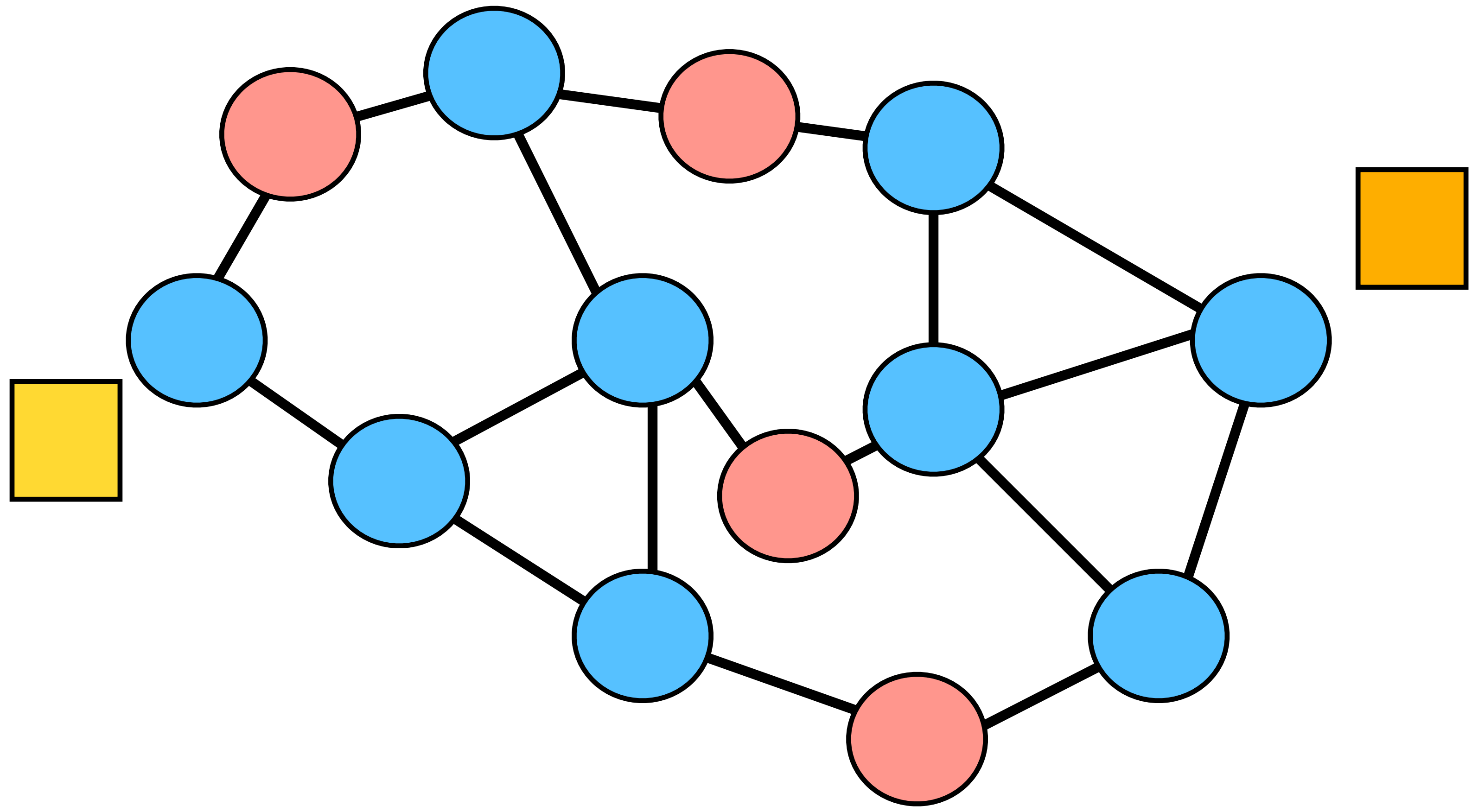


P2P Networking - Ballance attack

Ballance attack

- Perform sybil attack

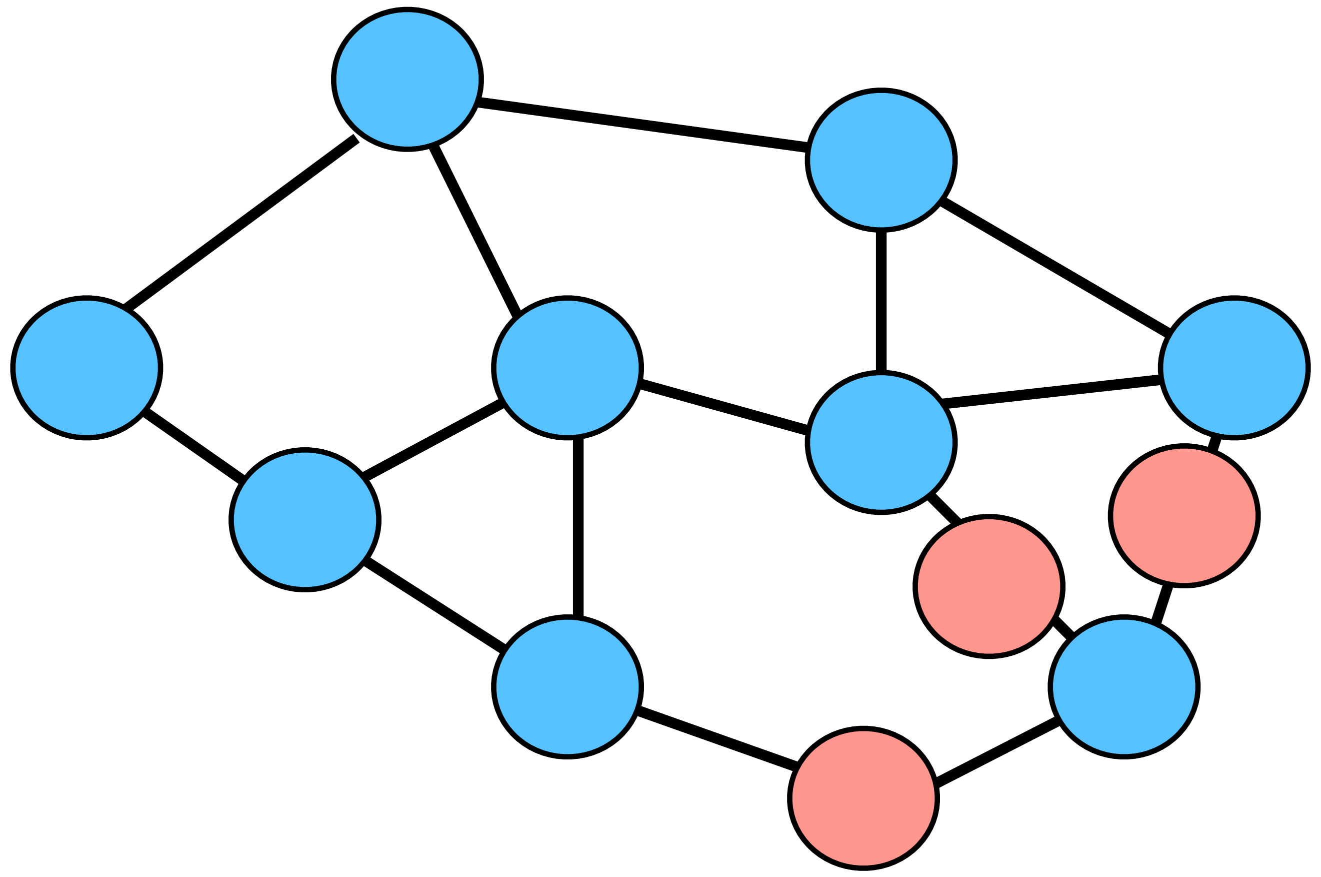
- *Try to enforce that partitions of the network mine on different forks*



P2P Networking - Eclipse attack

Eclipse attack

- Perform sybil attack tageted at one node
- *Effect what blocks target node sees*



P2P Networking - Eclipse attack

What is the real bitcoin?

- Multiple networks could exist

Updating a blockchain

Updating a blockchain

- Nodes may not adopt the newest version

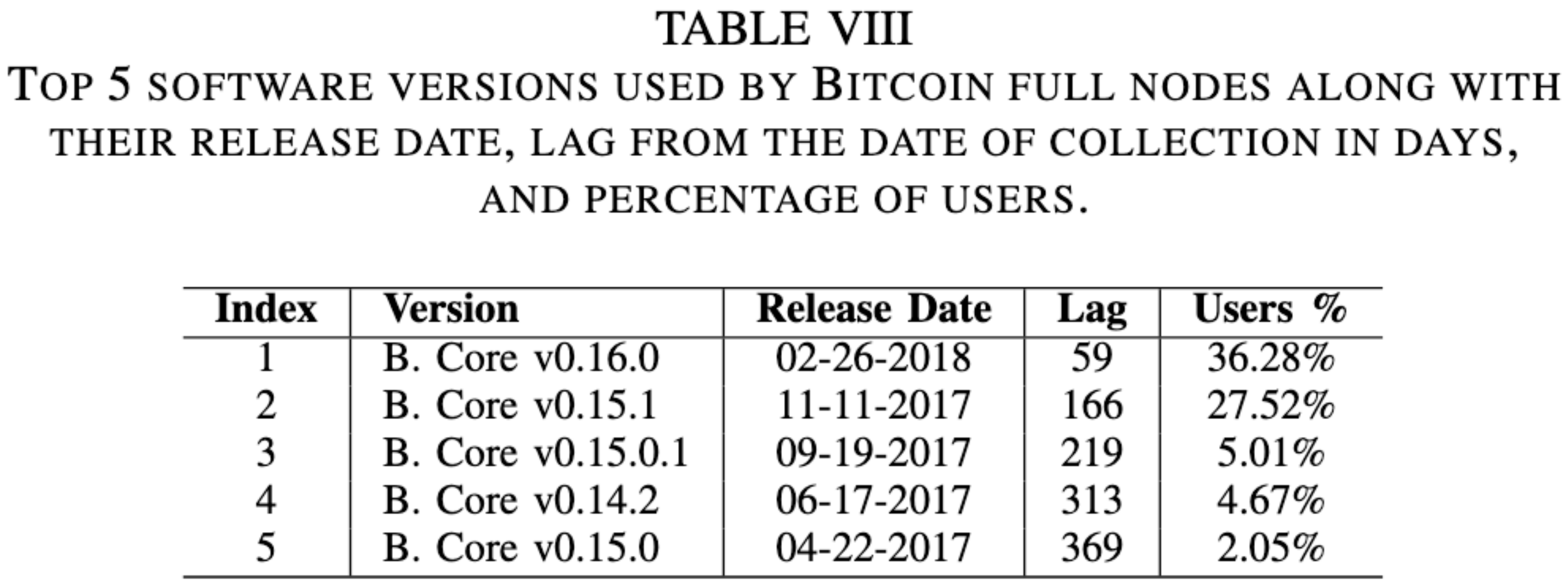


TABLE VIII

TOP 5 SOFTWARE VERSIONS USED BY BITCOIN FULL NODES ALONG WITH THEIR RELEASE DATE, LAG FROM THE DATE OF COLLECTION IN DAYS, AND PERCENTAGE OF USERS.

Index	Version	Release Date	Lag	Users %
1	B. Core v0.16.0	02-26-2018	59	36.28%
2	B. Core v0.15.1	11-11-2017	166	27.52%
3	B. Core v0.15.0.1	09-19-2017	219	5.01%
4	B. Core v0.14.2	06-17-2017	313	4.67%
5	B. Core v0.15.0	04-22-2017	369	2.05%

Saad et.al., ICDCS’19

Updating a blockchain

- Need to Update to
  - fix security problems
  - include new features

  - How to introduce breaking changes?

Updating a blockchain

Soft-Fork

- Some transactions/blocks valid under the old version are no longer valid.
- New version transactions/blocks are valid under the old version
  - E.g. security updates, disallow something
  - E.g. new feature using previously ignored parameter
- If majority of miners update, old version disappears.

Updating a blockchain

Hard-Fork

- All transactions/blocks valid under the old version are still valid.
- New transactions/blocks are not valid under the old version
    - E.g. new feature
- If majority of miners update, two version appear.

Updating a blockchain

Hard-and-Soft Fork

- Transactions/blocks valid under the old version no longer valid.
- New transactions/blocks are not valid under the old version
  - E.g. fundamental change
- Two versions appear.