Network attacks and updates

Selfish mining ~>

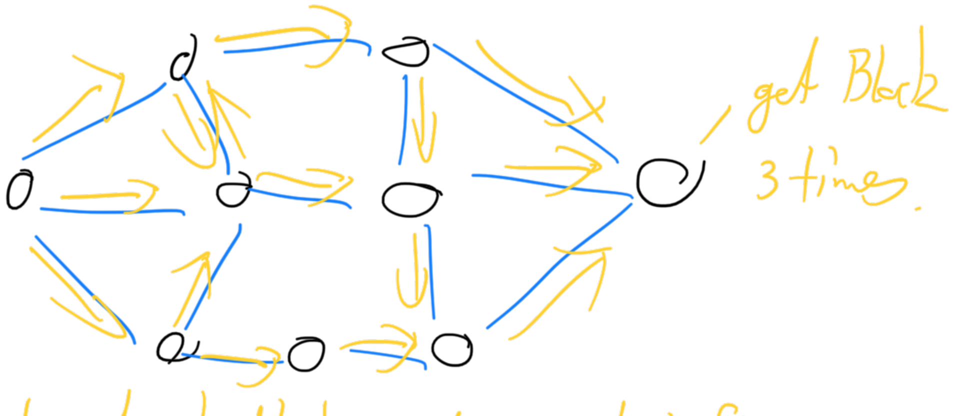
Network power allows attacks even with small fraction.

Bitcoin Networking

- > 10.000 Nodes
- each nodes chooses 8 nodes to connect to
- Nodes take at most 128 connections.

Breadcasting:

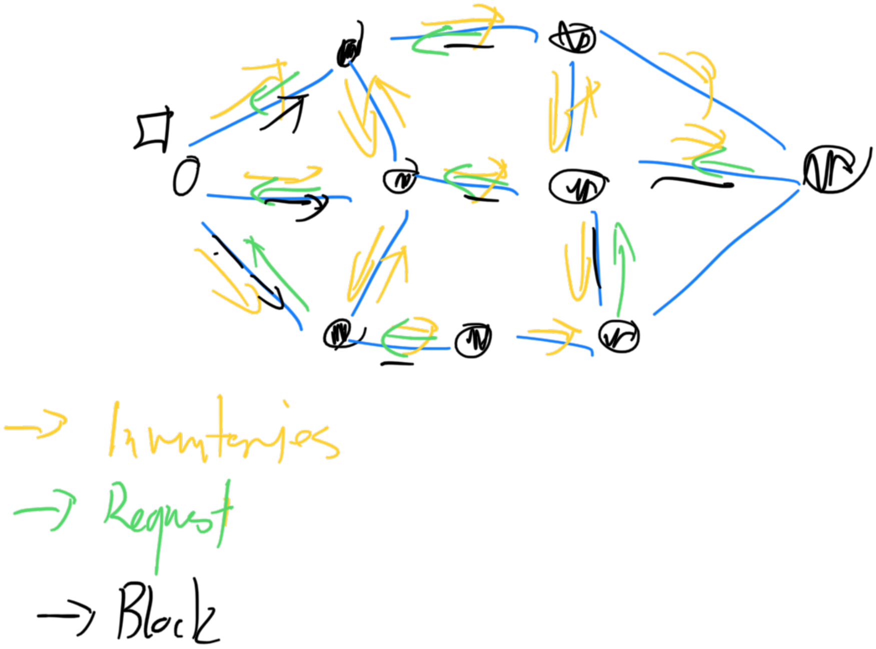
Block is big 1MB

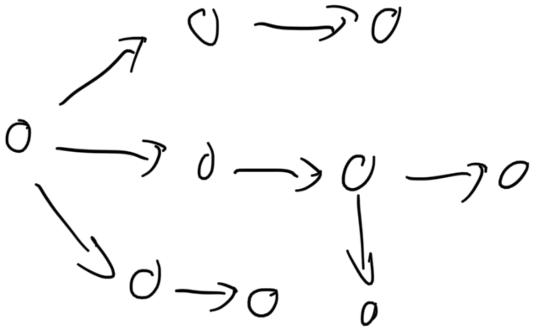


broadcast block ~> too much trafic.

Disseminate block

- Broadcasts an inventory:
  Block info without data
- Request blocks from one neighbor





Problem:

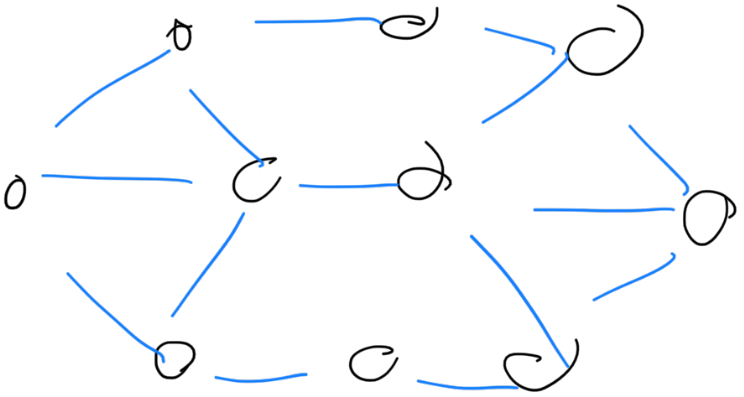
What if you get inventory, but no block

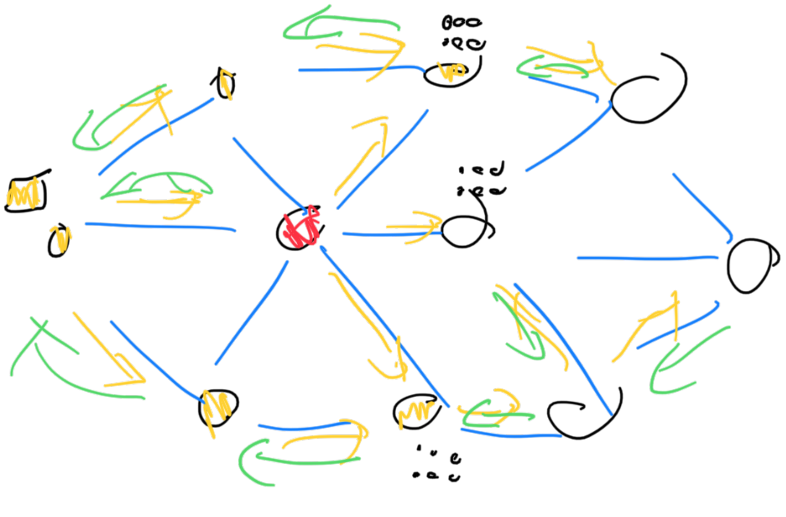
- Set timer on sending request

- on timeout, send request to different node

Delivery denial attack

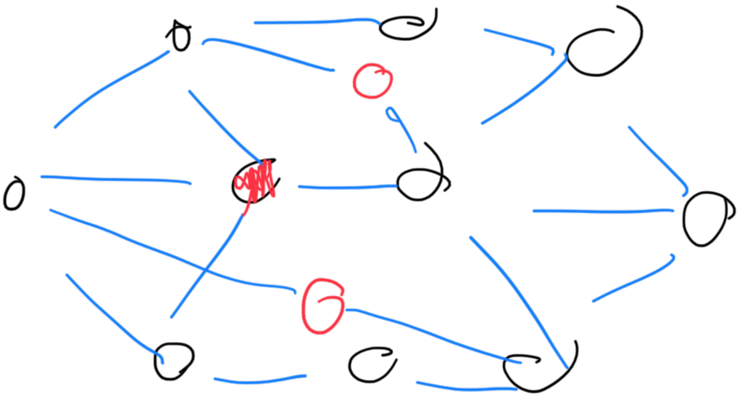
- send out inventories
- do not send block.





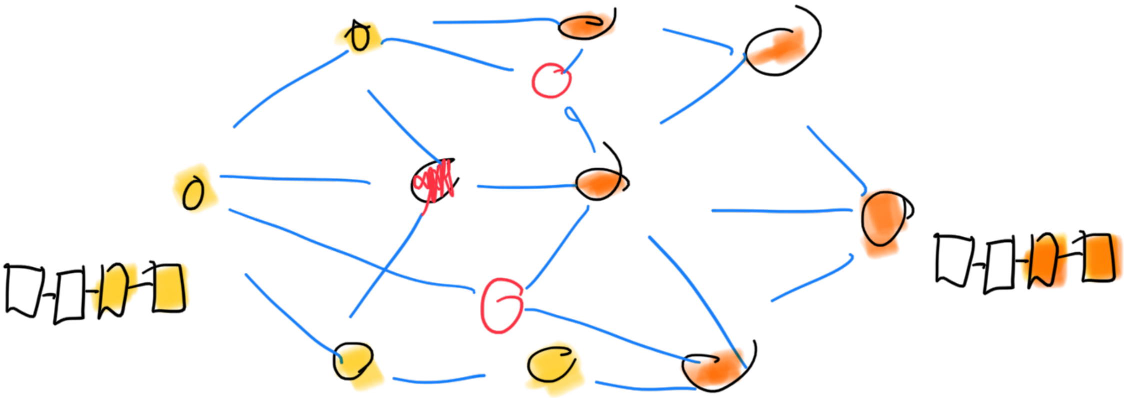
Sybil attack

- Attacker can register multiple nodes
- Can affect connectivity.



Ballance attack

- Perform sybil and forwarding attack
- Try to enforce that parts of the network mine on different forks

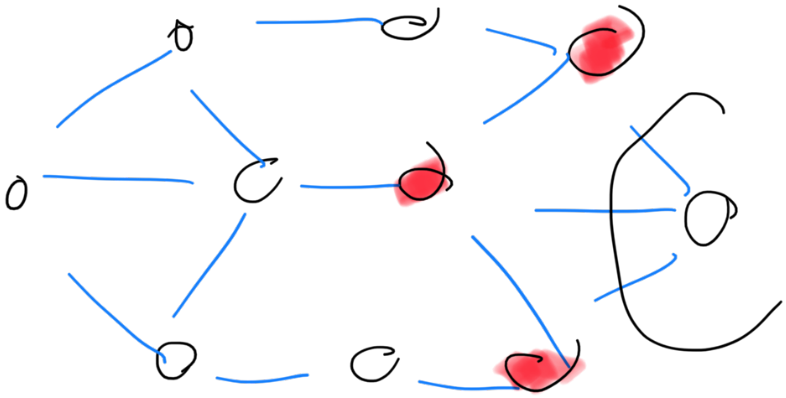


→ double spending

Eclipse attack

- Sybil attack targeted at one node

- Cut of one node
- Double spend



Updating a blockchain

software versions, -> need to update

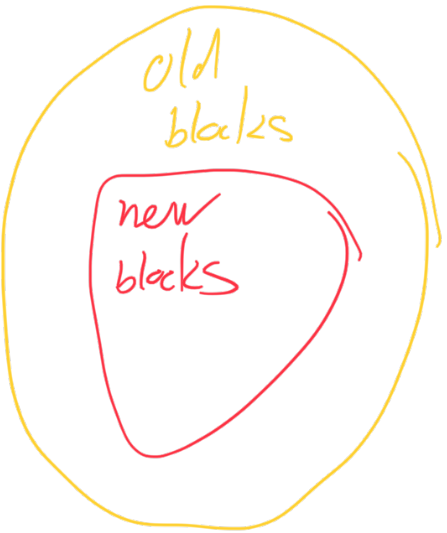
- fix bugs
- new features

every node updates to new version when he wants (or not at all)

How to introduce changes:

- Soft fork

Some blocks / transactions from the old version are no longer valid under the new version



- If majority of miners update, old version disappears.

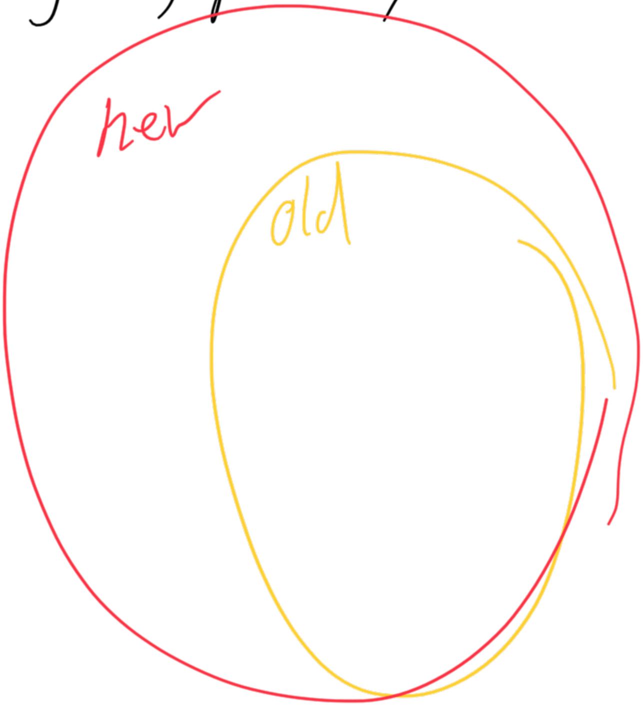
Exp: • security update: disallow something
• new feature using previously ignored parameter.

Hard fork

Some new blocks were not valid under old format:

E.g. • introducing new feature
optional

If majority updates, two versions appear.



Hard and soft fork