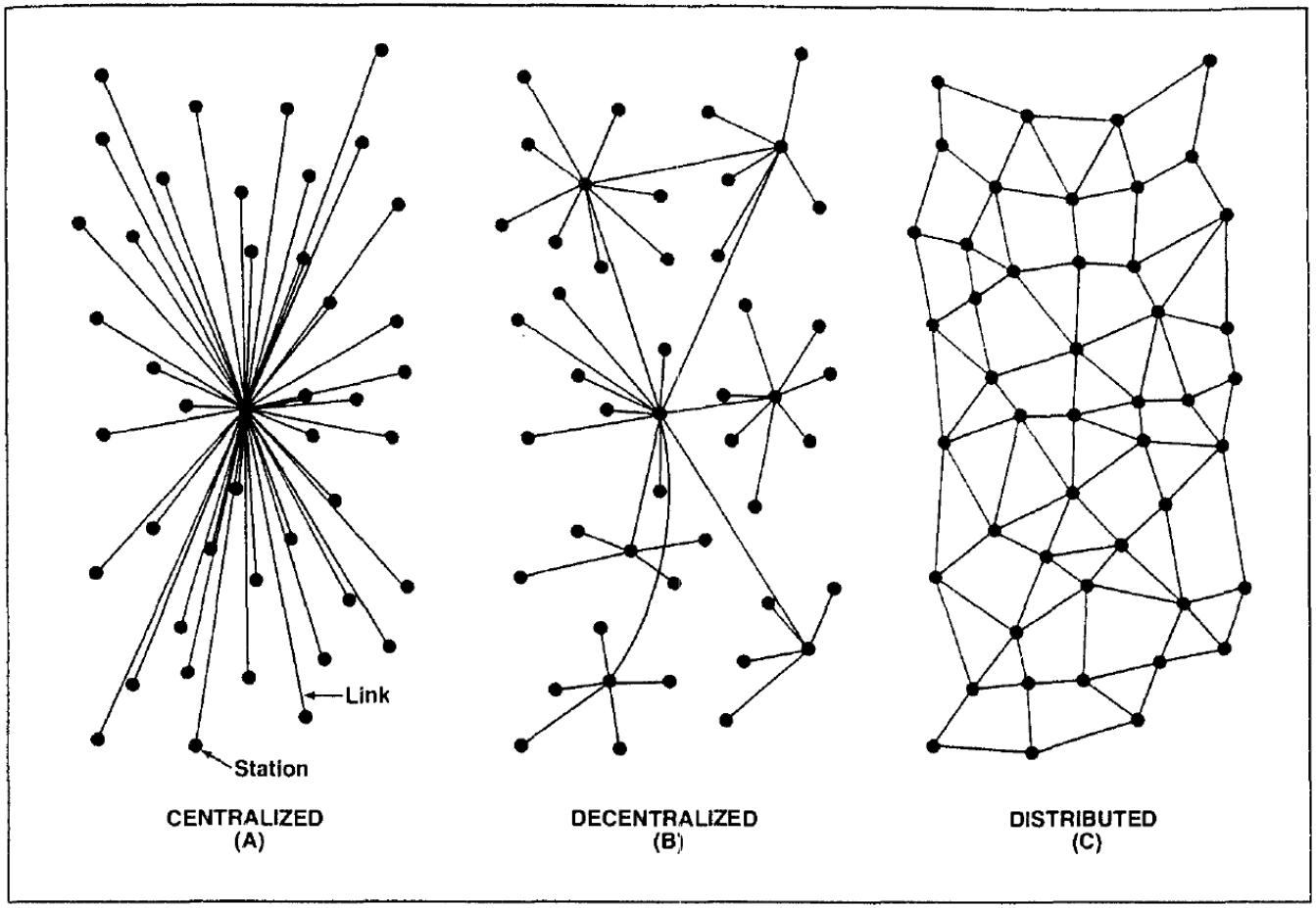
Bitcoin and Cryptocurrency Technologies
Lecture 6: Bitcoin Network

Yuri Zhykin

Mar 13, 2025

Peer-to-Peer Networks 1/2

- **Peer-to-peer (P2P) network** is a *distributed* system architecture that partitions tasks or workloads between *equally privileged*, *equipotent* nodes called *peers*.



Peer-to-Peer Networks 2/2

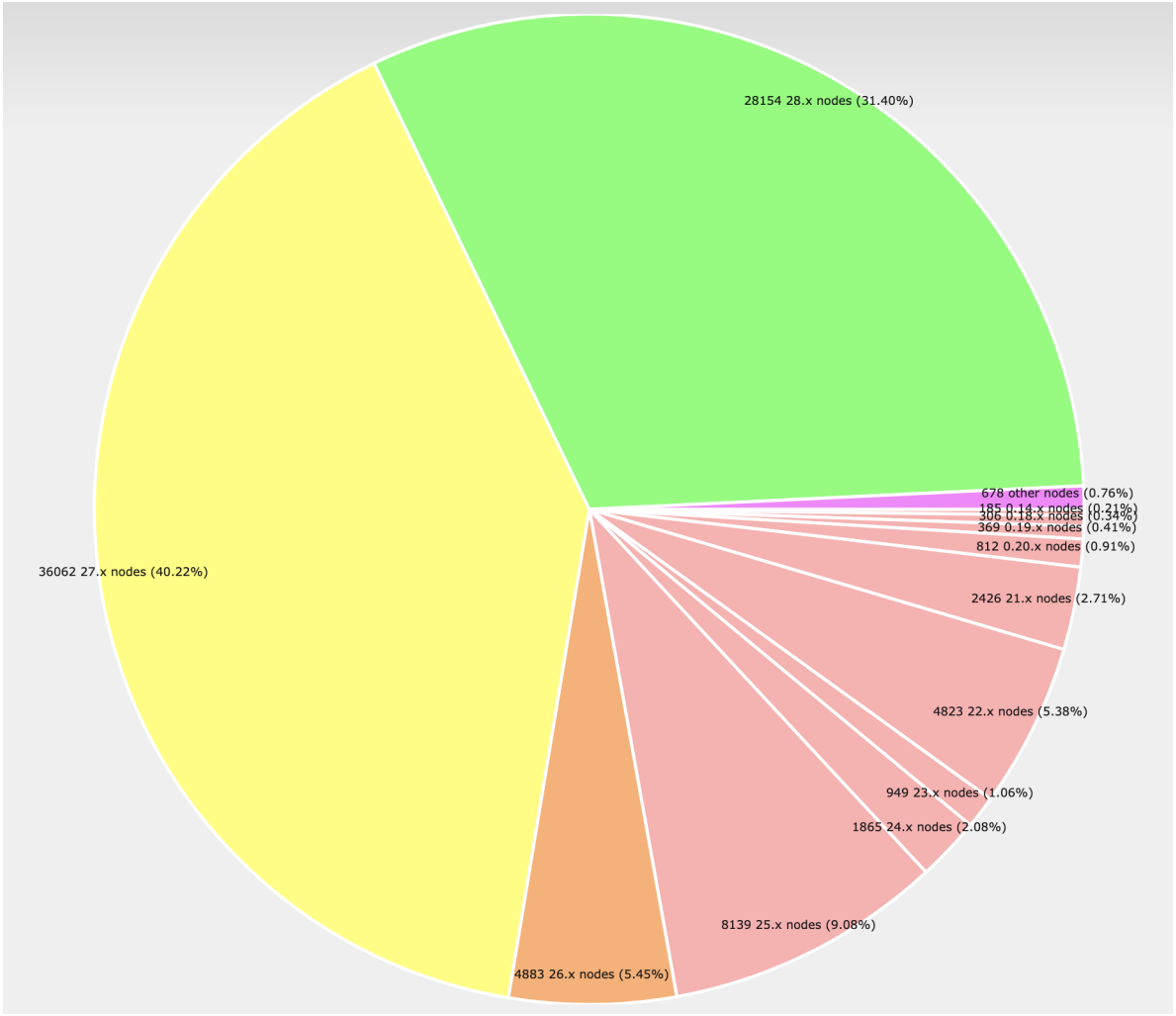
- In **centralized** systems, a successful attack on the **server** disables the whole system.
- In **decentralized** systems, a successful attack on a **hub** results in a temporary network partition, but the system remains operational.
- In **peer-to-peer** systems, a successful attack on a **peer** has no effect on the network *if the network is big enough*.
- Examples: **Napster** and **BitTorrent**.

Bitcoin Network 1/2

- **Bitcoin Network** is a **peer-to-peer** network that consists on **Bitcoin nodes** that propagate blocks and transactions via the **gossip protocol** and validate them according to **consensus rules**.
- According to bitnodes.io, Bitcoin network has approximately **21,000** *reachable* nodes, compared to 16,000 in 2022 and 10,000 in 2021.
- According to luke.dashjr.org, estimated total number of **full** nodes (i.e. nodes that perform validation of chain data) is around **100,000** nodes.

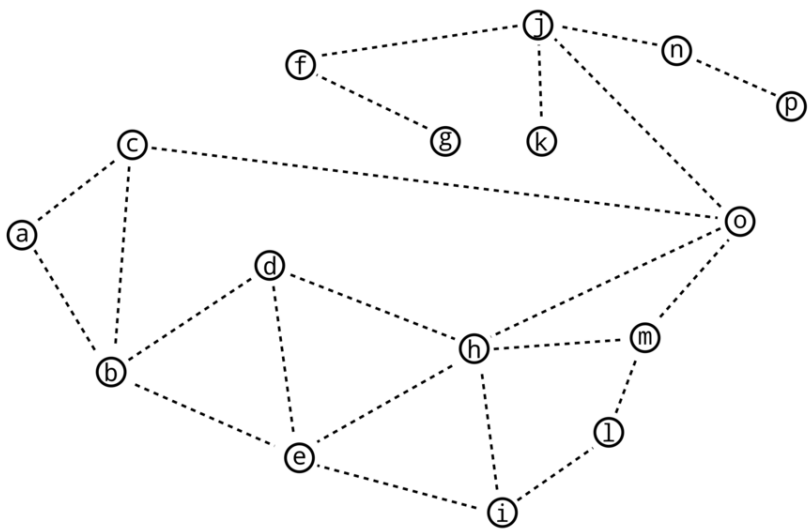
Bitcoin Network 2/2

- According to luke.dashjr.org, 71.62% of all nodes run the most recent software (Bitcoin Core 28.x, 27.x).



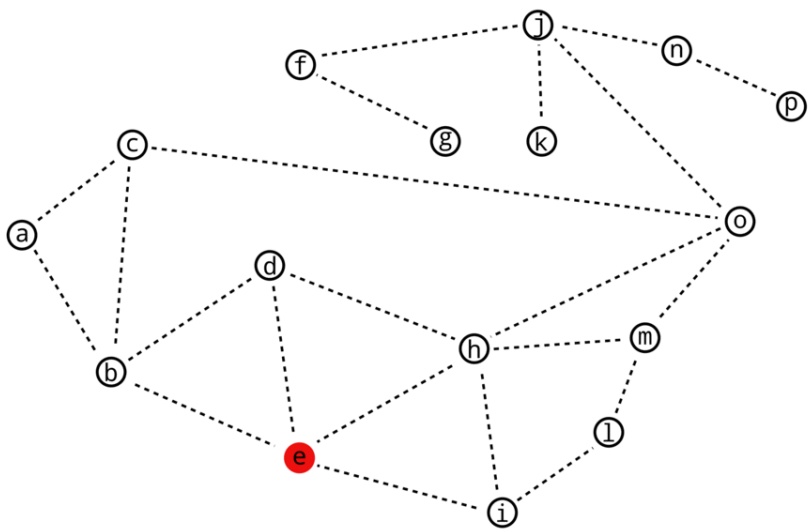
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread.
- **Receive information from one of their neighbours and pass it on to as much of their neighbours as possible.**
- **Bitcoin gossip protocol** is a gossip protocol for propagating new blocks and transactions as well as providing old blocks from storage to new peers on-demand.



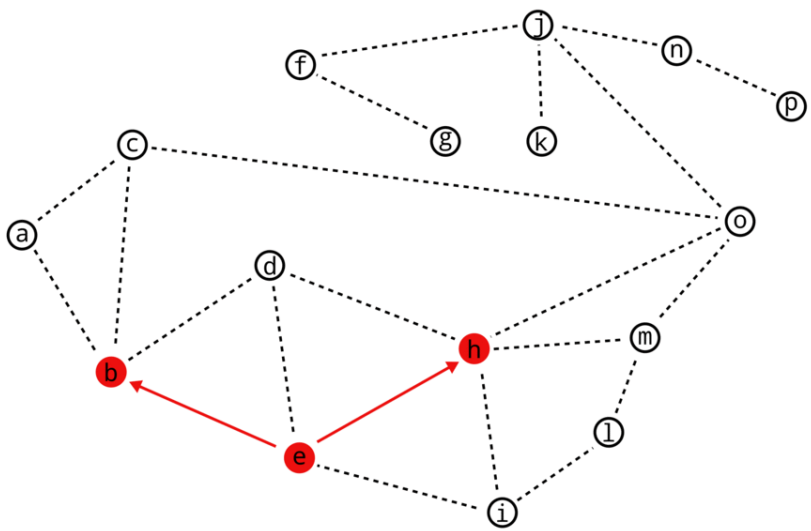
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread.
- **Receive information from one of their neighbours and pass it on to as much of their neighbours as possible.**
- **Bitcoin gossip protocol** is a gossip protocol for propagating new blocks and transactions as well as providing old blocks from storage to new peers on-demand.



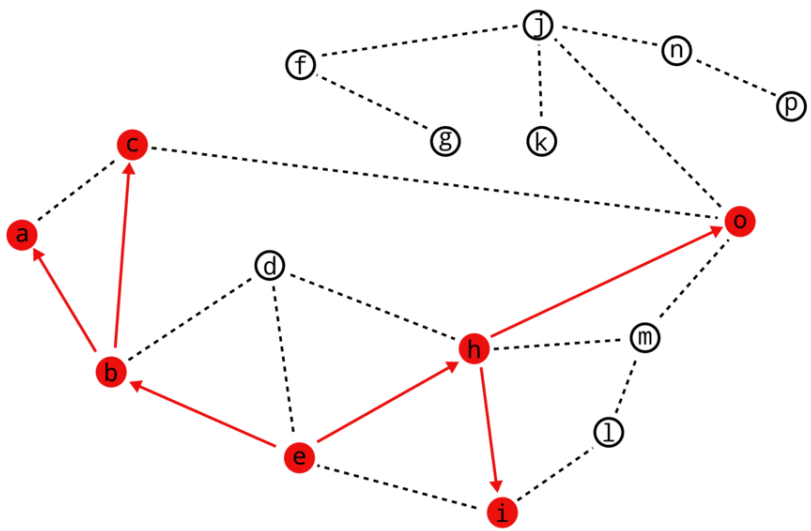
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread.
- **Receive information from one of their neighbours and pass it on to as much of their neighbours as possible.**
- **Bitcoin gossip protocol** is a gossip protocol for propagating new blocks and transactions as well as providing old blocks from storage to new peers on-demand.



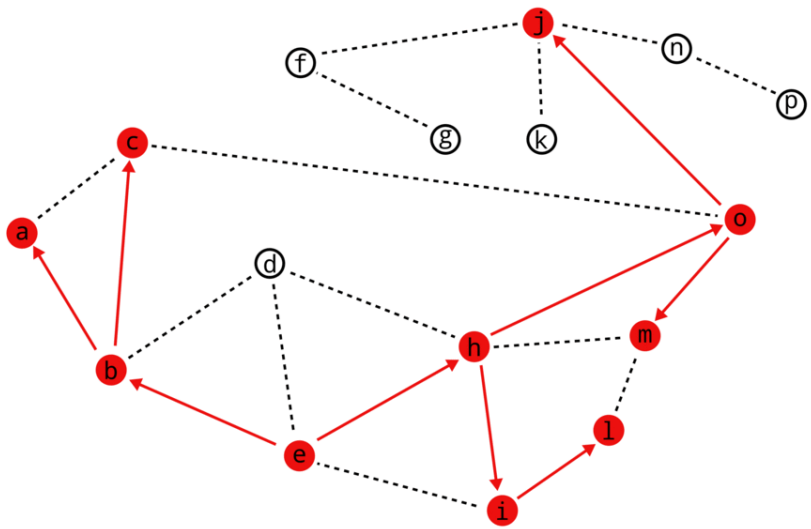
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread.
- **Receive information from one of their neighbours and pass it on to as much of their neighbours as possible.**
- **Bitcoin gossip protocol** is a gossip protocol for propagating new blocks and transactions as well as providing old blocks from storage to new peers on-demand.



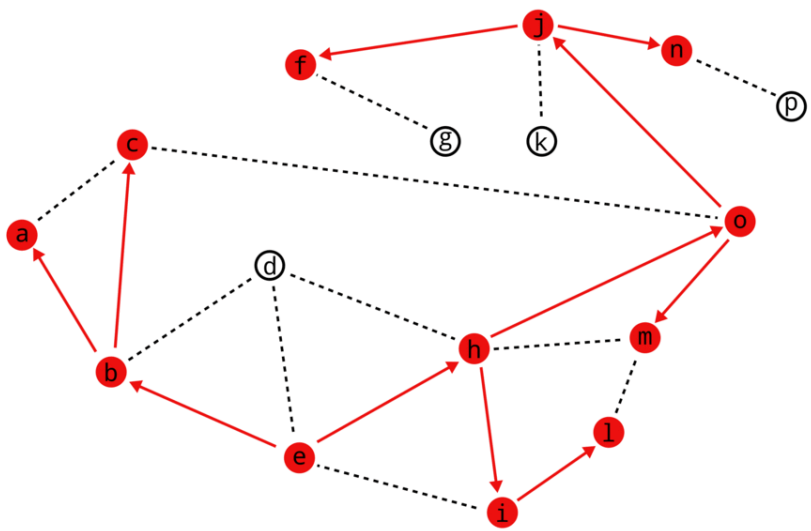
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread.
- **Receive information from one of their neighbours and pass it on to as much of their neighbours as possible.**
- **Bitcoin gossip protocol** is a gossip protocol for propagating new blocks and transactions as well as providing old blocks from storage to new peers on-demand.



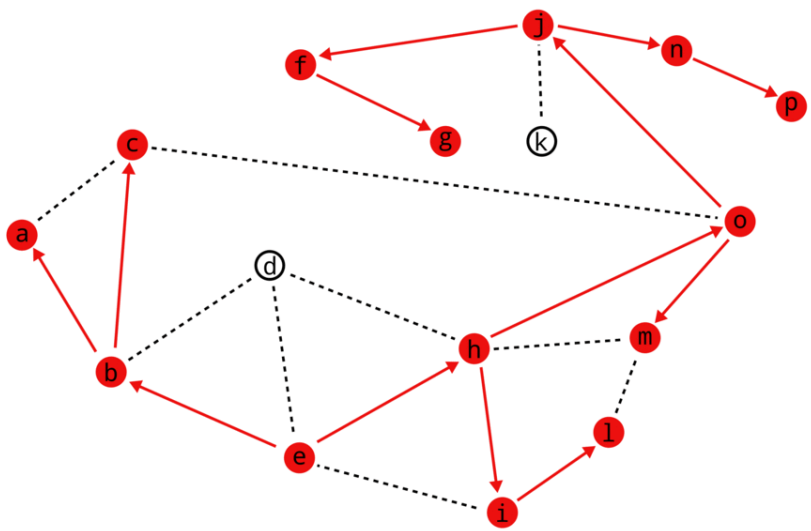
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread.
- **Receive information from one of their neighbours and pass it on to as much of their neighbours as possible.**
- **Bitcoin gossip protocol** is a gossip protocol for propagating new blocks and transactions as well as providing old blocks from storage to new peers on-demand.



Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread.
- **Receive information from one of their neighbours and pass it on to as much of their neighbours as possible.**
- **Bitcoin gossip protocol** is a gossip protocol for propagating new blocks and transactions as well as providing old blocks from storage to new peers on-demand.

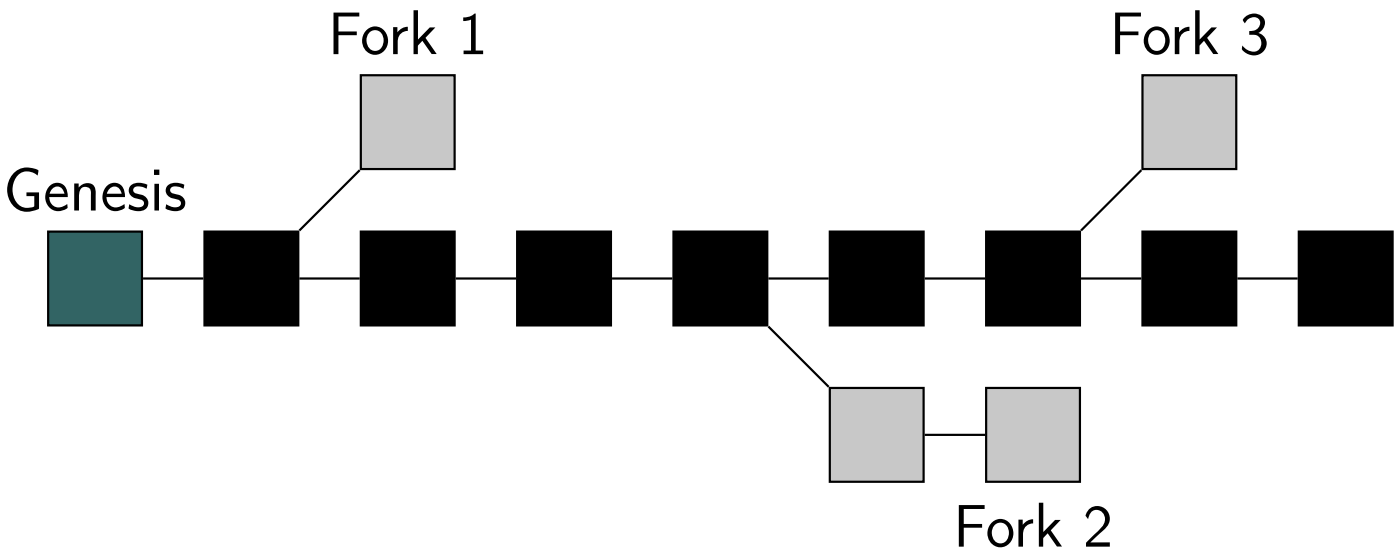


Bitcoin Network Node

- **Bitcoin node** is a member of Bitcoin network, a piece of software that executes the gossip protocol and validates blocks and transactions.
- A newly started Bitcoin node:
  - initializes the connections to several nodes via DNS seeds,
  - performs **initial block download** (**IBD**),
  - builds necessary indices (UTXO set),
  - starts listening for new blocks and transactions,
  - rejects invalid blocks and transactions,
  - accepts and re-broadcasts valid blocks and transactions.

Chain Reorganization 1/2

- When a new block is received that does not belong to the current chain, node attempts to reconnect it to the chain by finding the **fork point**.
- Once the block is reconnected, **the chain that took more energy to build** (has the most cumulative **chainwork**) is chosen as the valid chain.



Chain Reorganization 2/2

- **Chainwork** is the total number of hashes that are estimated to have been necessary to produce the current chain.
- **Headers-first IBD mode** makes IBD efficient by downloading the whole chain as headers first, and only then asking for whole blocks.

Mempool

- **Mempool** is an in-memory data structure that contains all known valid transactions that have not been included in any block yet.
- Nodes maintain a **combined UTXO set** that consists of all UTXOs in the chain and all UTXOs in the mempool.
- When a node receives a new valid transaction, it adds it to the mempool.
- When a node receives a new valid block, it removes all transactions in that block from the mempool.
- When a node receives a new transaction that conflicts with a transaction in its mempool, it rejects the new transaction unless it fits **RBF** (**Replace By Fee**) rules.

Mining

- **Miner nodes** are regular nodes that build new blocks from mempool transactions.
- A miner selects a number of transactions (2000-4000, usually sorted by fee) to build a **block template** within the **size limit**.
- Mining hardware performs a brute-force computation of the **Proof of Work** ($HASH256(Block) < Target$).
- When/if the block has been mined (i.e. PoW solution found), the miner broadcasts it to the network via the gossip protocol.
- If another miner "finds" a different block at the same time, the network eventually resolves the conflict via a chain reorganization.

Transaction Lifecycle 1/2

- A transaction **destroys** a subset of chain/mempool UTXOs and **creates** a set of new mempool UTXOs.
- A **finalized** valid transaction is propagated via gossip protocol to all nodes on the network.
- A transaction usually remains in the mempool until its fee exceeds the threshold for the next block.
- While in the mempool, a transaction can be "bumped" higher in the using
  - **Replace By Fee** (**RBF**) or
  - **Child Pays For Parent** (**CPFP**).

Transaction Lifecycle 2/2

- Eventually a transaction is included in one of the blocks.
- Once the block mined and propagated through the network, every node in the network
  - removes the transaction from the mempool,
  - applies the transaction to the UTXO set (removes destroyed UTXOs and adds created ones).
- At this point the transaction becomes **confirmed**.

The End

Thank you!