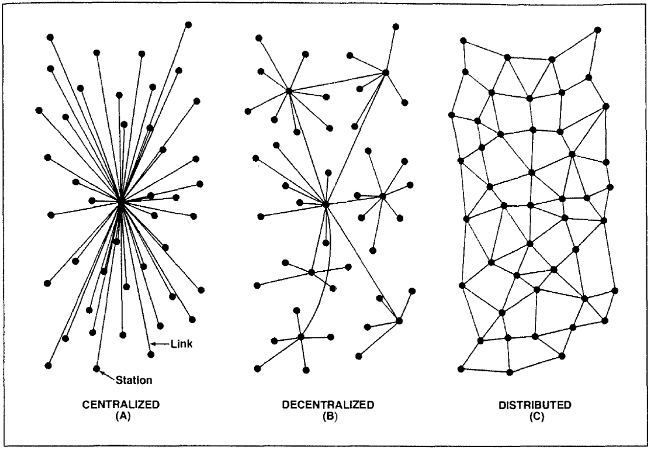
Bitcoin and Cryptocurrency Technologies
Lecture 6: Bitcoin Network

Yuri Zhykin

Mar 29, 2021

Peer-to-Peer Networks 1/2

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



Peer-to-Peer Networks 2/2

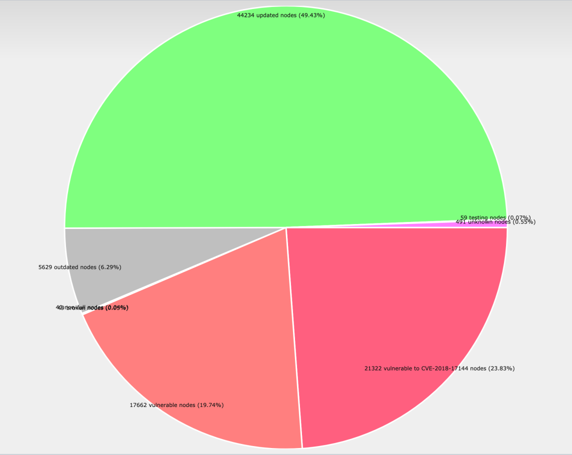
- In **centralized** applications, successful attack on the **server** disables the whole application.
- In **decentralized** applications, successful attack on a **hub** results in a temporary network partition, but the application remains operational.
- In **peer-to-peer** applications, successful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

Bitcoin Network 2/3

- **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 **10,000** *listening* (i.e. publicly visible) nodes, but the total number of **full** nodes (i.e. nodes that perform validation of chain data) is around **100,000** nodes.
- As of today, 49.5% of all nodes run the most recent software (Bitcoin Core v0.20.1 and v0.21.0).

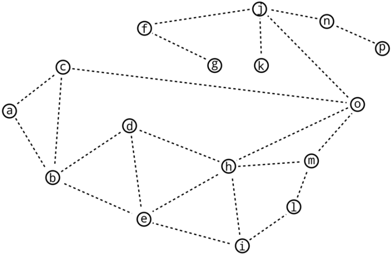
Bitcoin Network 3/3

- As of today, 49.5% of all nodes run the most recent software (Bitcoin Core v0.20.1 and v0.21.0).



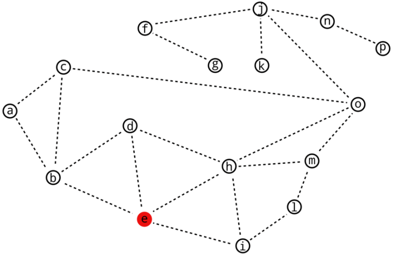
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread - nodes receive information from one of their neighbours and pass it on to all other neighbours.
- **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.



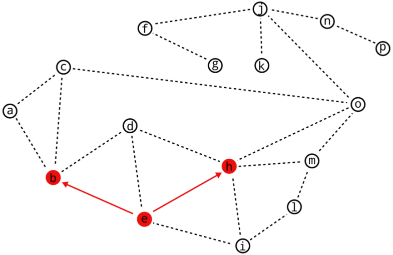
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread - nodes receive information from one of their neighbours and pass it on to all other neighbours.
- **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.



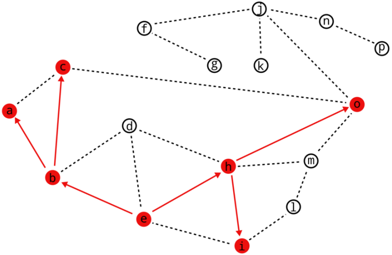
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread - nodes receive information from one of their neighbours and pass it on to all other neighbours.
- **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.



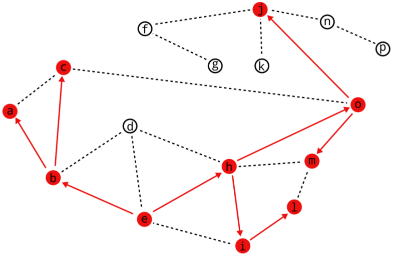
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread - nodes receive information from one of their neighbours and pass it on to all other neighbours.
- **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.



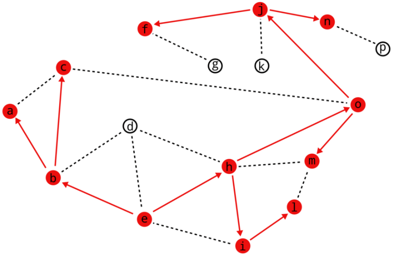
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread - nodes receive information from one of their neighbours and pass it on to all other neighbours.
- **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.



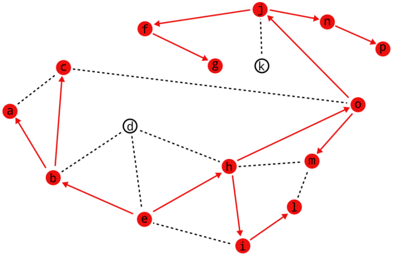
Gossip Protocol

- **Gossip protocol** (a.k.a. **epidemic protocol**) is a process of peer-to-peer communication that is based on the way *epidemics* spread - nodes receive information from one of their neighbours and pass it on to all other neighbours.
- **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 - nodes receive information from one of their neighbours and pass it on to all other neighbours.
- **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 the 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,
  - when a new block or transaction is received, node accepts and broadcasts it to its peers if is valid, and rejects it otherwise.

Chain Reorganisation

- When a new block is received that does not belong to the current chain, node attempts to reconnect it to the chain be 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.
- **Chainwork** is the total number of hashes that are expected to have been necessary to produce the current chain.
- During IBD, **headers-first mode** makes this efficient.

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 node receives a valid transaction, it adds it to the mempool.
- When node receives a new 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 (except for **replace-by-fee** (**RBF**) transactions).

Mining

- **Miner nodes** are regular nodes that maintain the mempool and use it to build the new blocks.
- Miner node sorts mempool by transaction fee and selects 2000 transactions to build a new block.
- Once a new block is build, miner node passes the block **template** to the mining hardware that starts computing proof-of-work by brute-forcing a $SHA256d(block)$ (i.e. $SHA256(SHA256(block))$) value that meets the target value.
- Once the block is mined (proof-of-work solution is found), the node broadcasts it to the network via the gossip protocol.
- If another miner mines a different block around the same time, network eventually resolves the conflict by selecting the chain with the most work (reorg).

Transaction Lifecycle 1/2

- Bitcoin transaction destroys a subset of chain/mempool UTXOs and creates a set of new mempool ones.
- Once signed, transaction is propagated via gossip protocol to all nodes on the network, including miner nodes.
- Miner nodes see the new transaction and include it in the next block template if the transaction fee meets the necessary threshold.
- If transaction fee is lower than the threshold for the next block, it remains in the mempool until all the higher-fee transactions are confirmed.

Transaction Lifecycle 2/2

- While in the mempool, transaction be “bumped” higher in the mempool using the following
  - **replace-by-fee** (**RBF**),
  - **Child Pays For Parent** (**CPFP**).
- Once the block with the transaction is mined and propagated through the network, on every node in the network that saw the new block
  - transaction is removed from the mempool,
  - transaction is applied to the UTXO set (UTXOs that are destroyed by the transaction are removed from the UTXO set and UTXOs that are created by the transaction are added to the UTXO set).

The End

Thank you!