IN5420-Blockchain Networking

Survey on Blockchain Networking: Context, State-of-the-Art, Challenges (section 1 to 5)

In most of cryptocurrencies there are two roles: peer and miner. Peer create and send transactions. BItcoin and Ethereum are build on top of TCP. Communication pattern- simple flooded-based strategy. Another network topology. Capacities of channel represent financial balances. To prevent malicious nodes from flooding the network with invalid blocks, nodes use a store-and-forward model. Each node verifies a full block before forwarding it to others. Increasing the rate of transmitting txs→increasing the size of block→lower transmittion rate : scalability problem. When blocks propagate too slowly in a blockchain network, nodes cannot process them quickly because new blocks arrive faster than nodes can download and validate them. It is important that the speed at which blocks are received is greater than the speed at which they are created.

Problem of data overhead: When a new block is created, most of the transactions are already in the nodes' mempool. X-thin - retransmit only lacked tx, compact blocks. Relay networks achieves this by disseminating blocks without full block verification and retransmitting known transactions.

In ETH two validation: block header validation and state validation (more power).Risks of SPV mining increases the likelihood that the chain will continue based on a block containing errors, since subsequent miners do not fully verify transactions. SPV mining is a compromise between speed and security. Problems with transaction propogation: Amplified DDos attacks, Information Eclipsing and 0-Confirmation policies (can be fake transactions), Privacy (miss of anonim : Dandellion is solution), Incentives (reward for information distributing).

Different nodes: core, relay (protection), edge (generate transactions). DHT tables - resource to get an info about node. Node asks a pecial dns servers to get info about active nodes.

Eclipsing attack- isolating some nodes.

Section IV.C in Understanding blockchain: definitions, architecture, design, and system comparison

Types of nodes: Bitcoin and ethereum - full and lightweight nodes. HyperLedger Fabric and Iota - client connect to the networks. Bitcoin 12.6 s time to get a block, send it to the network and in eth - 109 ms, becuase you can get a part of blocks. Hyperledger - push/pull with getting info from customers. IOTA same as ETH. In bitcoin a lot of clustering occurs, that decrease the delays.

In eth transactions are encypted. IOTA - Authenticated andencrypted messages, partial anonymity. Hyperledger - authenticated channels

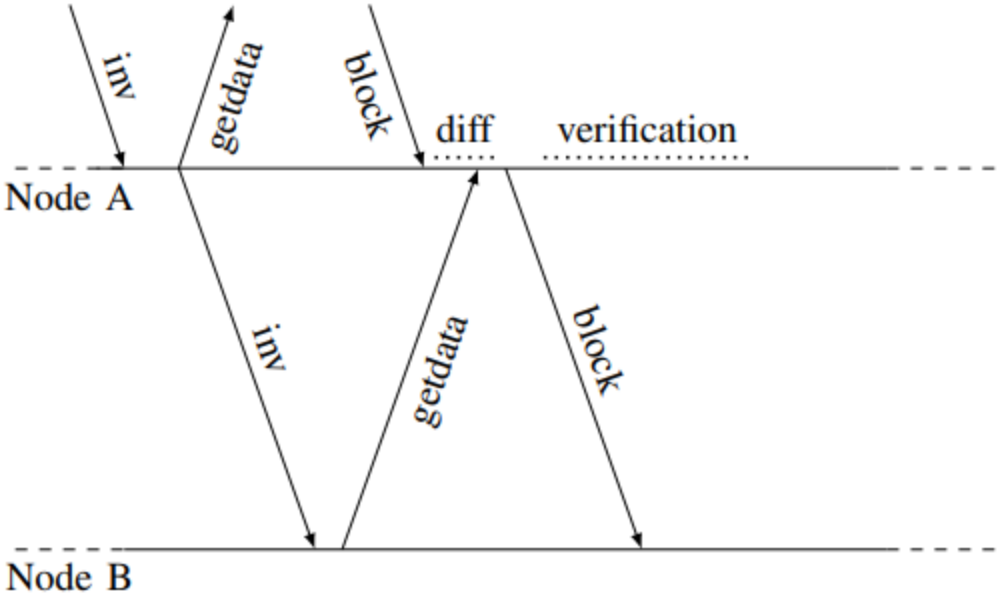
Information propagation in the Bitcoin network

It takes few hours to leave the network. Each network holds p connections, if less - connect to the random node. Problem of network fragmentation.

Node after verifing sending inv message to neighbour, neighbour getdata, retransmitt the block. Propogation delay depends on size, more than 20kB it is constant and before increases.

Information Ellipsing- do not accept invalid block, it can lead to fork. Due to PoW block finds forks itself, without external. The odds of getting firked is 1.78%. With increasing of block size and blockhain the odds of forks will increase.

Speeding up the propogation: minimize verification- divide into two phases(difficulty check, tx validation), pipelining block propogation (inv msg before full check, disadvantage: inv spam) and connectivity increase (star-sub graph). This all lead to increasing odds of fork to 0.78%


inv
getdata
block
diff
verification
Node A
inv
getdata
block
Node B