Summary on Blockchain Networking

Blockchain is decentralized immutable digital ledger system that keeps record of transactions of any type of values. Information is stored in blocks that are propagated over the entire blockchain network for processing, validation and recording purpose. Blockchain network consists of Peer to Peer (P2B) communication protocol and nodes. The network facilitates the decentralized communication between the nodes that continuously need to know the status of the validation of the transactions in consideration.

Besides other layers like data storage layer and contract layer, communication layer is the nervous system of the blockchain technology, that need to be fast, reliable, and secure. All computing devices that are involved in the formation of the blockchain network are categorized into core nodes and clients or lightweight nodes. Cryptocurrencies that have been developed as primary application of blockchain technology, uses different network architecture and protocols. For example, in bitcoin, Ethereum and IOTA, only full nodes are part of the blockchain network where transactions are been propagated, and light nodes connects to the full nodes for their choice, while transactions are submitted and propagated through channels that are isolated from other channels in Fabric.

As blockchain network is a homogeneous network of nodes, nodes in the network forms random graph. In the network topology, when a node joins a blockchain network, the node sends queries and learns about other nodes by asking their neighbors for known addresses and by listening for advertisements of new addresses and messages. When a node leaves the network, it´s address will linger for several hours before that eventually be removed by their neighbors from their known address sets. By default, connection pool size p for a bitcoin node is 8, while the real size of the connection pool is bigger and in average to be 32 for nodes that allows incoming nodes. For a node that is behind a network address translation or behind the firewall, the simultaneous open connection cannot be more than 8.

In the distributed ledger blockchain network, only the transaction (Tx) and the block messages (block) is of importance for bookkeeping, updating, and synchronizing throughout the network. For maintaining the block size smaller, it should not be sent again ang again to the nodes that already have received it. During propagating blocks by using gossip-protocol in the blockchain network, they are therefore not forwarded directly. The figure below shows the protocol for forwarding the block message in blockchain network. As we can see from the figure, when a block is received by a node in the blockchain network, it first verifies the block before it transmits an “inv” message to its neighbor to broadcast the availability of the block. The inv message of approximately 61 bytes contains transactions hashes and block hashes. After scanning through its database, the

receiving node will send a getData request to the sender, if it doesn't already know the transaction or the block. After receiving the request from Node B, Node A delivers the block to node B. The block continues to propagate throughout the network, for verification. The verification of block includes verification of each transaction in the Block. Transactions verification requires random access of data stored in discs and the block message can be very large during the propagation. Verification time, handshaking time between the nodes and propagation time will cause propagation delay in the network.

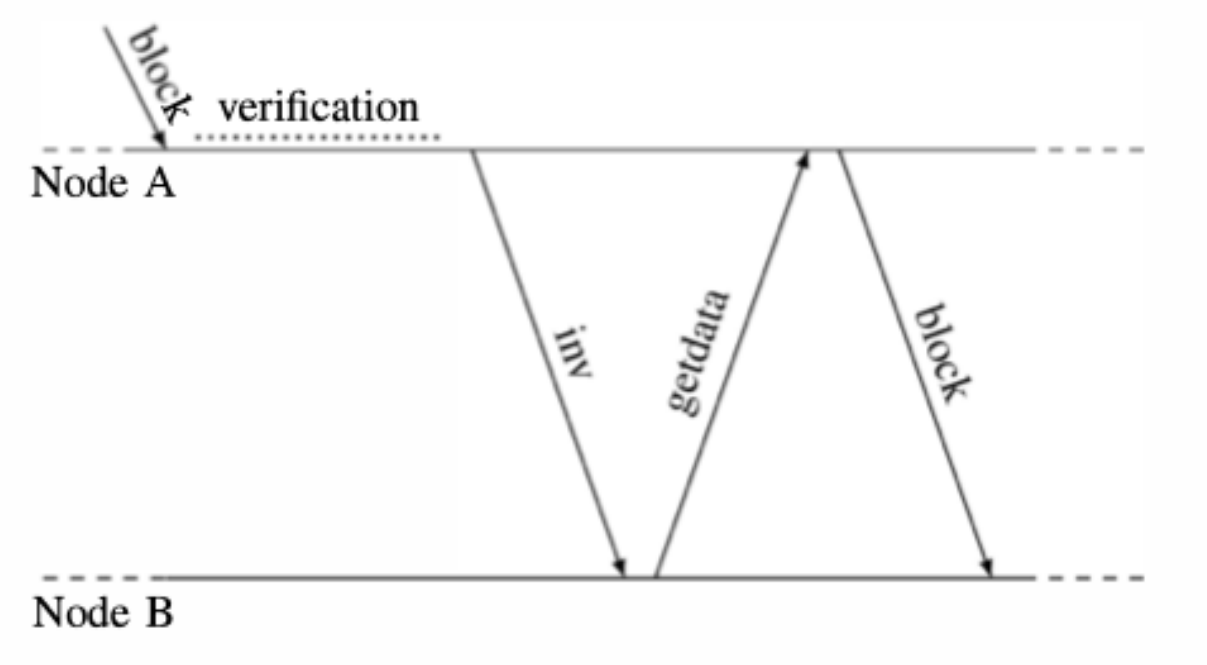


Figure: Showing communication protocol for forwarding of block message in blockchain network, by a single hop from Node A to Node B

Question to AI:

Why does a node send block to another neighbor node instead of solving itself, in the blockchain network?

Answer:

In a blockchain network, nodes work together to maintain the integrity and operation of the network. When a node receives a new block, it shares this block with its neighboring nodes, rather than trying to validate or mine the block itself for several reasons:

1. **Decentralization and Redundancy:** Blockchain networks are designed to be decentralized. By propagating blocks throughout the network, redundancy is ensured. This means that even if some nodes go offline, the blockchain can still be accessed from other nodes.

2. **Verification Rather Than Mining:** When a node receives a block, its primary task is to verify that the block is valid rather than to mine it. Mining is a separate process that involves solving cryptographic puzzles, and it is only relevant for nodes competing to add the next block to the blockchain (common in Proof of Work systems like Bitcoin).

3. **Efficient Propagation:** Quickly propagating blocks through the network ensures that all nodes are working with the latest version of the blockchain and reduces the likelihood of forks or disagreements about the state of the blockchain.

4. **Consensus Mechanism:** Different blockchains use various consensus mechanisms. For instance, in Proof of Work (PoW), not every node will or needs to mine. Only certain nodes, known as miners, will package transactions into a block and attempt to solve the PoW puzzle to add that block to the blockchain. After a block is mined, it is shared with other nodes to achieve consensus about the new state of the blockchain. In Proof of Stake (PoS) and other consensus mechanisms, nodes might take on different roles related to validation rather than mining.

5. **Efficiency and Network Health:** Allowing each node to only perform its specialized function (such as validating or propagating transactions and blocks) improves the overall health and speed of the network.

6. **Avoiding Duplicate Work:** If each node tried to solve every block independently, it would result in a huge amount of redundant work, which is inefficient. Instead, nodes rely on a smaller subset of the network (miners or validators) to perform the resource-intensive tasks, while others help in maintaining the network by propagating transactions and blocks.

By sending the block to another neighbor node, each node aids in rapid dissemination throughout the network, allowing for efficiency, resiliency, and a consensus across the blockchain's distributed ledger.

References:

Information Propagation in the Bitcoin Network, Christian Decker,* Roger Wattenhofert

Understanding blockchain: definitions, architecture, design, and system comparison, Roman Vitenberg, Mohammad Hossein Tabatabaei, Narasimha Raghavan Veeraragavan

Chat Gpt