Blockchain Network

PLAN

1. Key contributions and findings
2. Aspect of Blockchain network
3. Block propagation
4. Transaction propagation

Papers for the presentation

- Understanding blockchain: definitions, architecture, design, and system comparison
- Information propagation in the Bitcoin network
- Survey on Blockchain Networking: Context, State-of-the-Art, Challenges

Key contributions and findings

- Compares blockchain platforms (Bitcoin, Ethereum, Hyperledger Fabric, IOTA) with a focus on network formation and node roles.
- Highlights the impact of network topology on efficiency and security, identifying vulnerabilities.
- Explores optimization methods for block and transaction propagation and their implications.
- Synthesizes insights across multiple blockchain platforms, updating perspectives on their structure and security risks.
- Identifies gaps in formal validation and protocol robustness against specific attacks.

Aspect of Blockchain network

Network Formation & Node Roles

- Bitcoin & Ethereum: Full nodes maintain the ledger; SPV nodes rely on them.
- Hyperledger Fabric: Uses private channels for isolated communication.
- IOTA: Uses nodes for transaction relay.
- Different platforms take distinct approaches to network structure.

Aspect of Blockchain network

Network Topology & Security Risks

- Bitcoin: Decentralized P2P with random outbound connections.
- Cardano & Ripple: Introduce specialized nodes for added security.
- Vulnerabilities: Network partitioning, eclipse attacks, BGP hijacking, and DDoS threats require mitigation strategies.

Aspect of Blockchain network

Incentives in Blockchain Systems

- Nodes participate for rewards (e.g., Bitcoin miners earn block rewards & fees).
- Competition ensures transaction processing and system integrity.

Aspect of Blockchain network

Communication Protocols & Propagation Efficiency

- Bitcoin: Push-gossip, 95% of nodes receive a block in ~40s.
- Ethereum: Similar model, but more efficient (95% reachability in ~211ms).
- Hyperledger Fabric: Combines push-pull with strict access control.
- IOTA: Uses flooding and privacy-focused messaging.

Block Propagation in Blockchain

How its works

- **Process:** Blocks are re-propagated as soon as their validity is checked (e.g., proof of work verification).
- **NewBlock & NewBlockHashes Messages:**
  - The full block is sent to a small fraction of peers (total peers).
  - Other peers receive only the block hash and may request the full block later if needed.

Block propagation in Blockchain

Impact of Network Latency & Throughput

- **Latency:** The time for a block to reach nodes; affected by distance, internet quality, and network traffic.
- **Throughput:** The percentage of nodes receiving a block within a set time; large block sizes slow down propagation.

Block propagation in Blockchain

Challenges of Delayed Block Propagation

- **Forks:** Delays can lead to blockchain forks, which complicate consensus and reduce integrity.
- **Solution:** Faster propagation methods are needed to minimize delays.

Block Propagation in Blockchain

Methods for optimizing block propagation

- Compressed Block Encoding (Reducing Bandwidth Usage)
  - Xtreme Thinblocks (XThin)
  - Graphene
  - Velocity
- Mining Communication & Relay Networks
  - Stratum Mining Protocol
  - Weak Blocks
  - Relay Networks

Block propagation in Blockchain

Methods for optimizing block propagation (Next)

- Ethereum’s State Synchronization
- Incentives for Faster Block Propagation
    - Selfish Mining Attacks:
    - SPV Mining (Simplified Payment Verification):

Block propagation in Blockchain

Assess of optimizing methods provided for block propagation

Method	Real-World Use?	Limitations
Compact Blocks (Bitcoin Core)	☑ Yes	Slower if too many transactions are missing
XThin (Bitcoin Unlimited)	☑ Yes	Less used than Compact Blocks
Graphene	🚧 Limited adoption	Higher computational complexity
Stratum Mining Protocol	☑ Yes	Vulnerable to attacks
Weak Blocks (BitcoinNG, Flux)	🚧 Limited (other blockchains)	Not in Bitcoin Core
Relay Networks (FIBRE, Falcon)	☑ Yes	Centralization risks
Ethereum Fast Sync	☑ Yes	Trust concerns for state snapshots

Transaction propagation

How its works

- Ensures that user transactions **reach miners** for block inclusion.
- Uses a **flooding-based (gossip) protocol** where peers relay transactions.
- **Relay Mechanism:**
    1. **Broadcasting** the transaction.
    2. **Validation** by network nodes.
    3. **Propagation** to other nodes.
    4. **Mempool storage** until mined.
    5. **Miner selection** (high-fee transactions prioritized).

Transaction propagation

Security Threats and challenges in transaction propagation

- Amplified DDoS Attack
- Transaction Replacement & Double-Spending
- Information Eclipsing & 0-Confirmation Risks
- Privacy Concerns
- Lack of Incentives for Nodes

Conclusion

- **Transaction propagation is crucial** but **vulnerable** to attacks, delays, and privacy risks.
- **Fee-based filtering helps mitigate spam** but doesn’t fully prevent DDoS.
- **Privacy solutions like Dandelion++ reduce traceability risks**.
- **Incentive mechanisms are needed** to ensure nodes participate fairly in transaction relay.