
NPTEL ONLINE CERTIFICATION COURSES

# Blockchain and its applications

**Prof. Shamik Sural**
**Department of Computer Science & Engineering**
**Indian Institute of Technology Kharagpur**

**Lecture 16: Blockchain Elements - IV**

# CONCEPTS COVERED

- Joining a Bitcoin Network
- Transaction Flooding
- Block Mining
- Block Propagation
- Forking and Propagation of Longest Chain

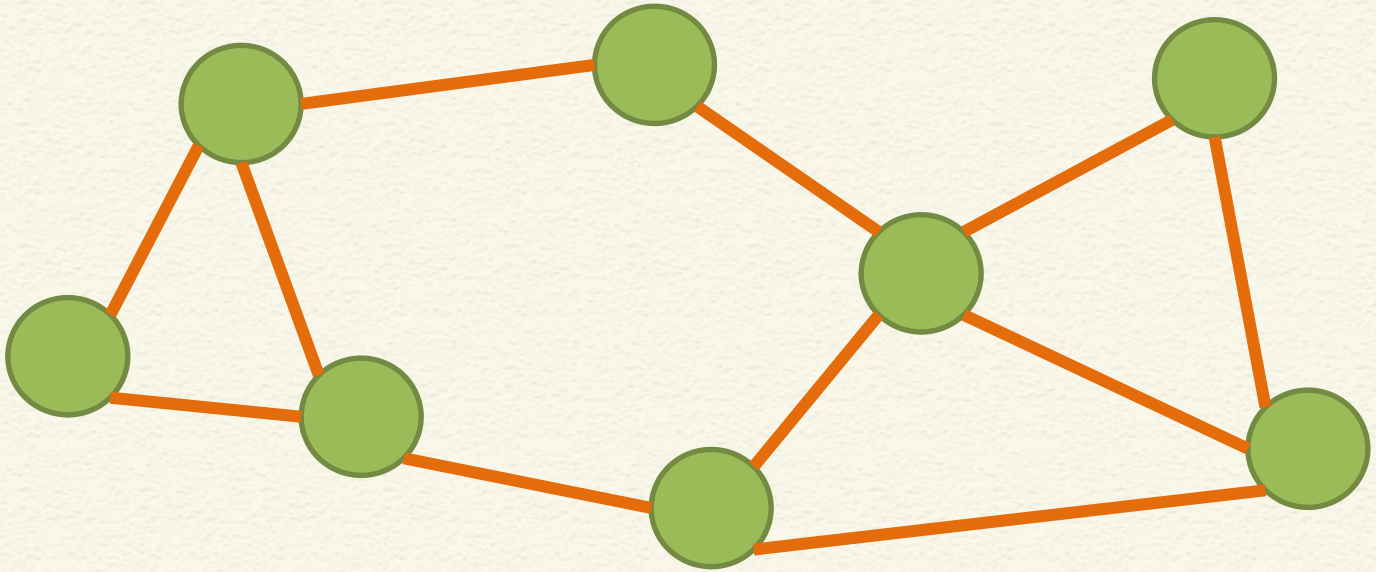
# KEYWORDS

- Bitcoin Node
- Transaction Flooding
- Block Reward
- Block Propagation
- Fork in Blockchain

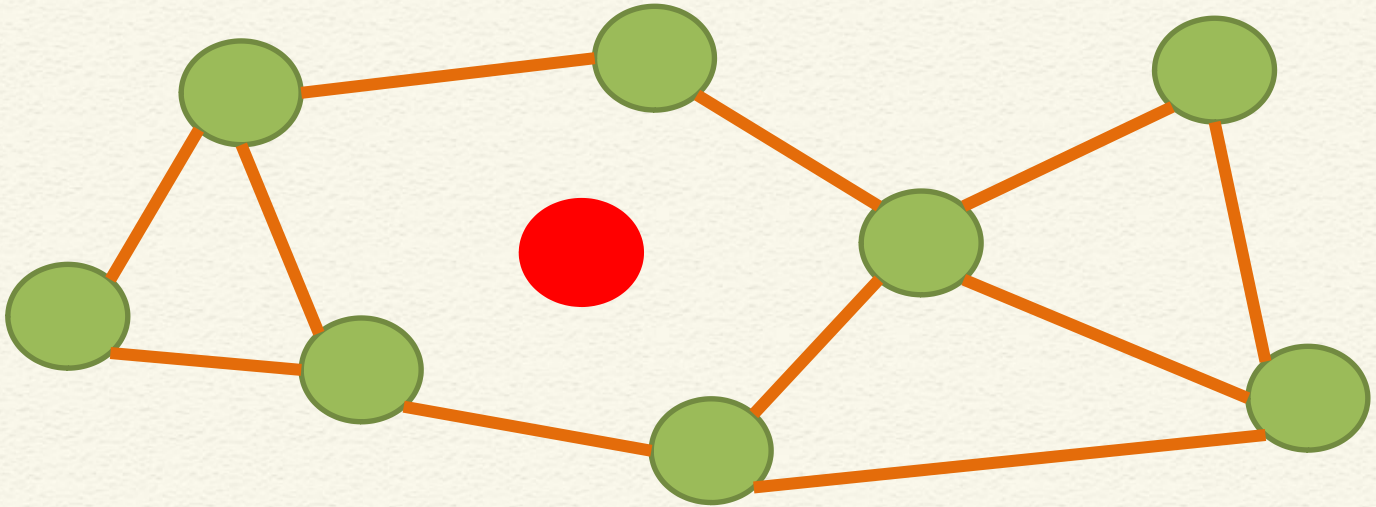
## Bitcoin P2P Network

- An ad-hoc network with random topology, Bitcoin protocol runs over TCP
- All nodes (users) in the bitcoin network are treated equally
- New nodes can join any time, non-responding nodes are removed after 3 hours

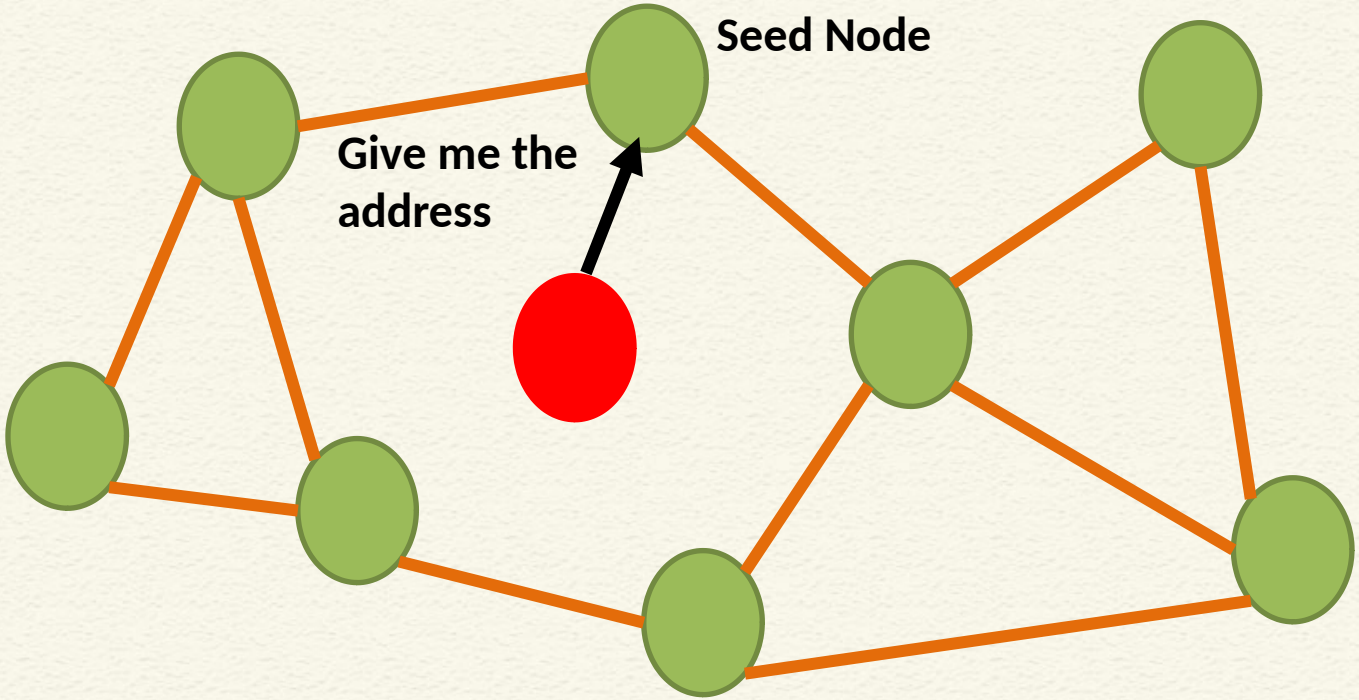
# Joining in a Bitcoin P2P Network



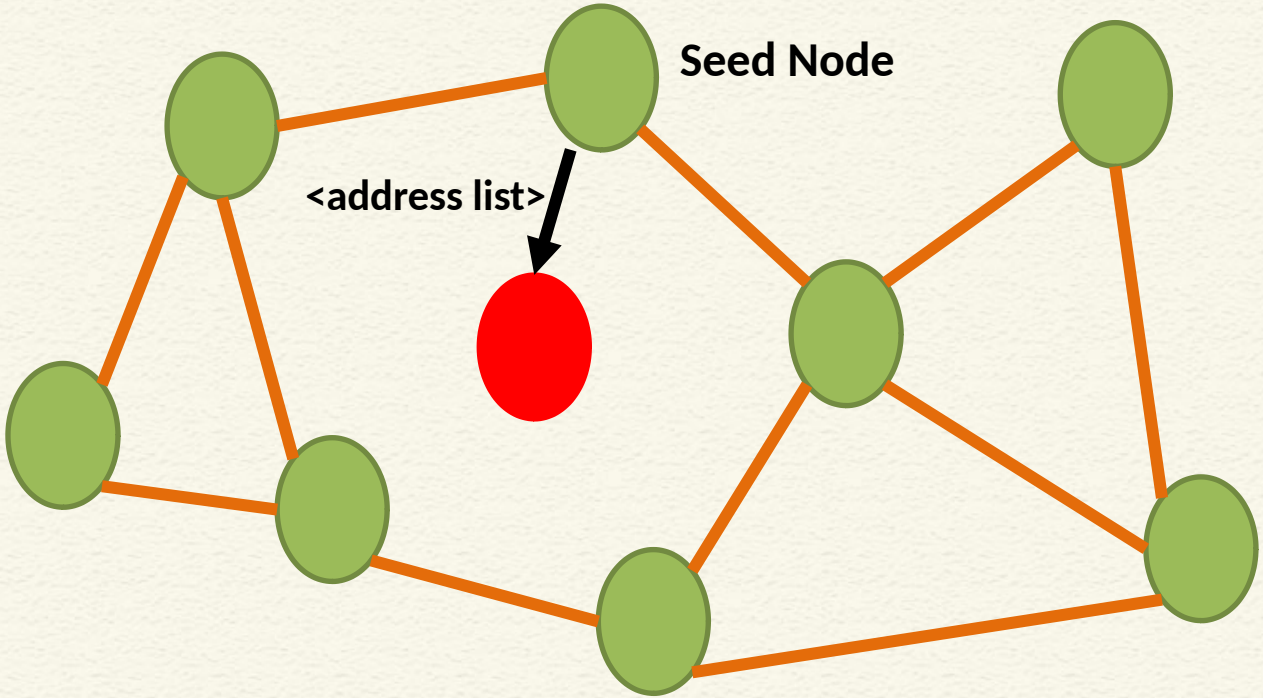
# Joining in a Bitcoin P2P Network



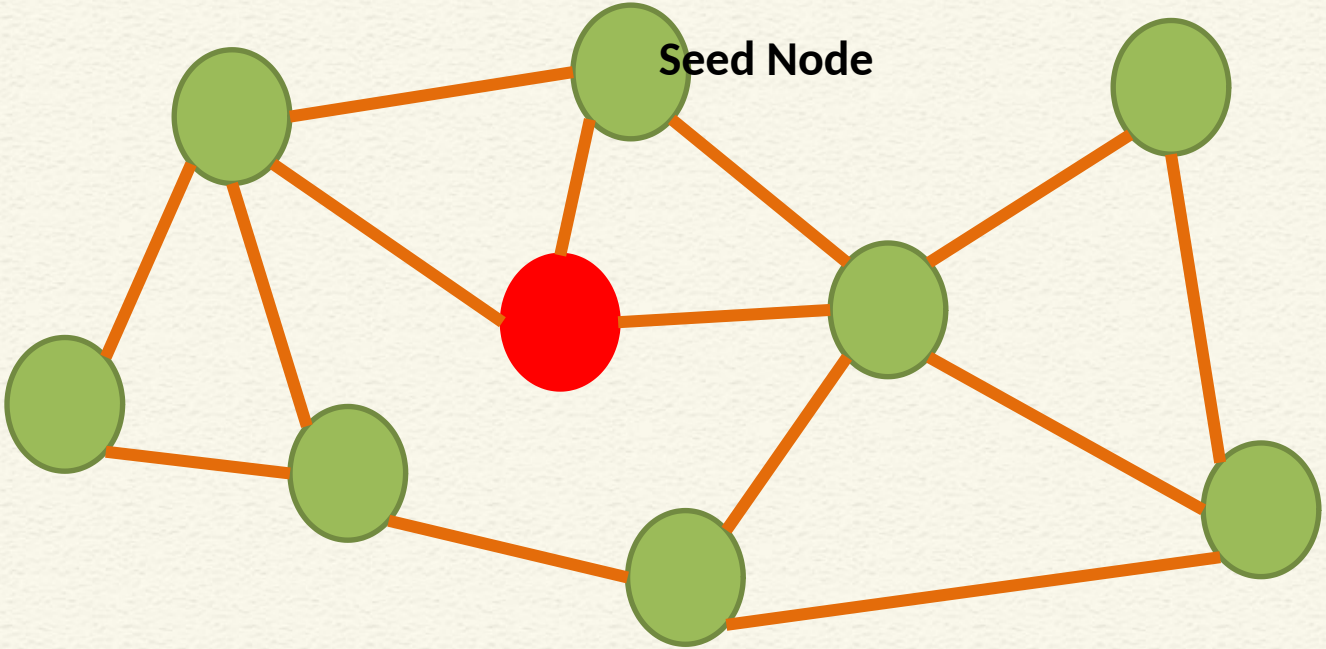
# Joining in a Bitcoin P2P Network



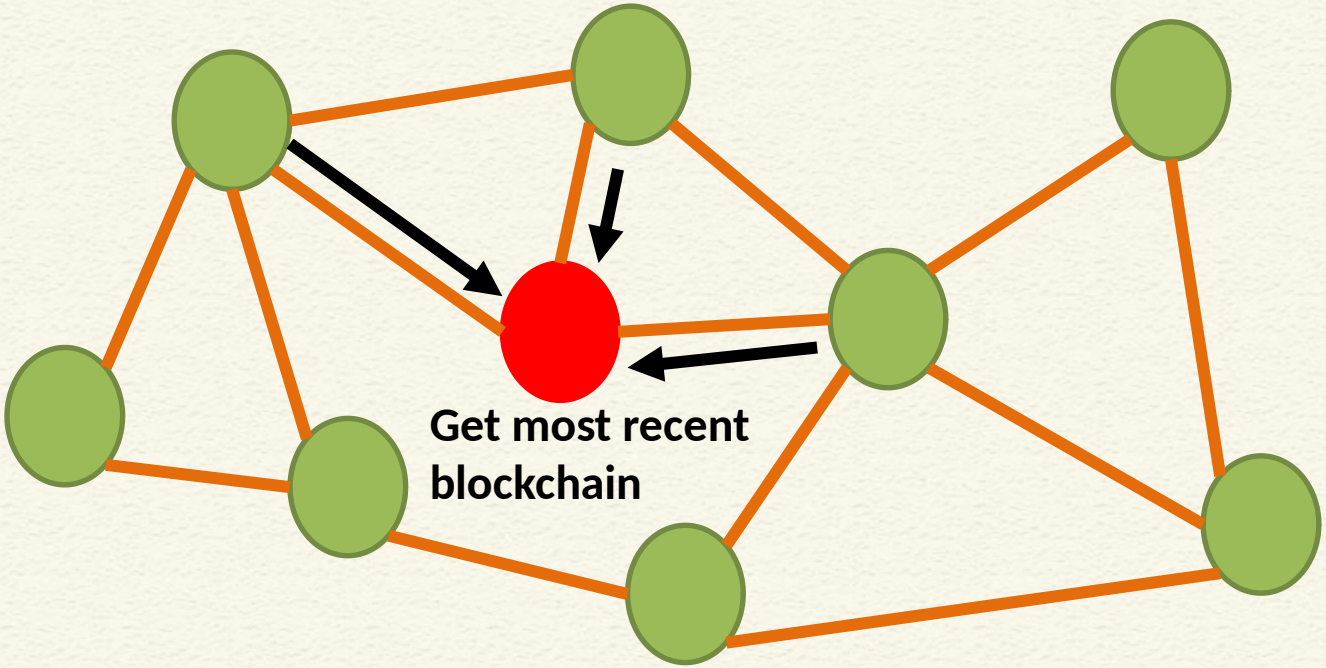
# Joining in a Bitcoin P2P Network



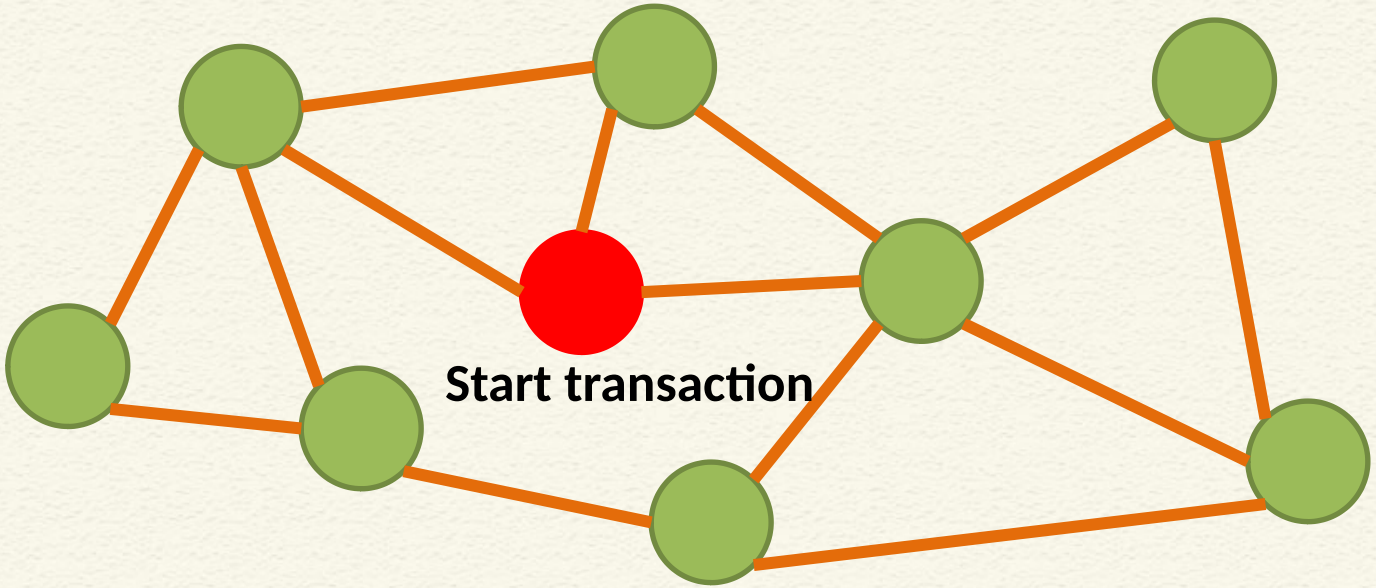
# Joining in a Bitcoin P2P Network



# Joining in a Bitcoin P2P Network



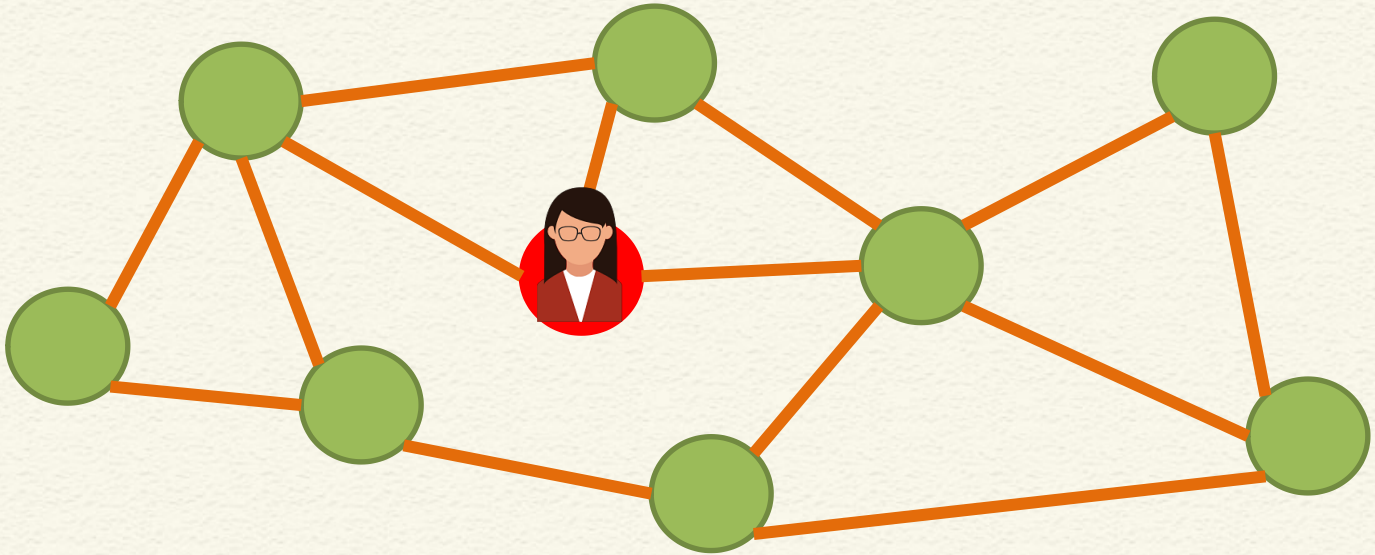
# Joining in a Bitcoin P2P Network



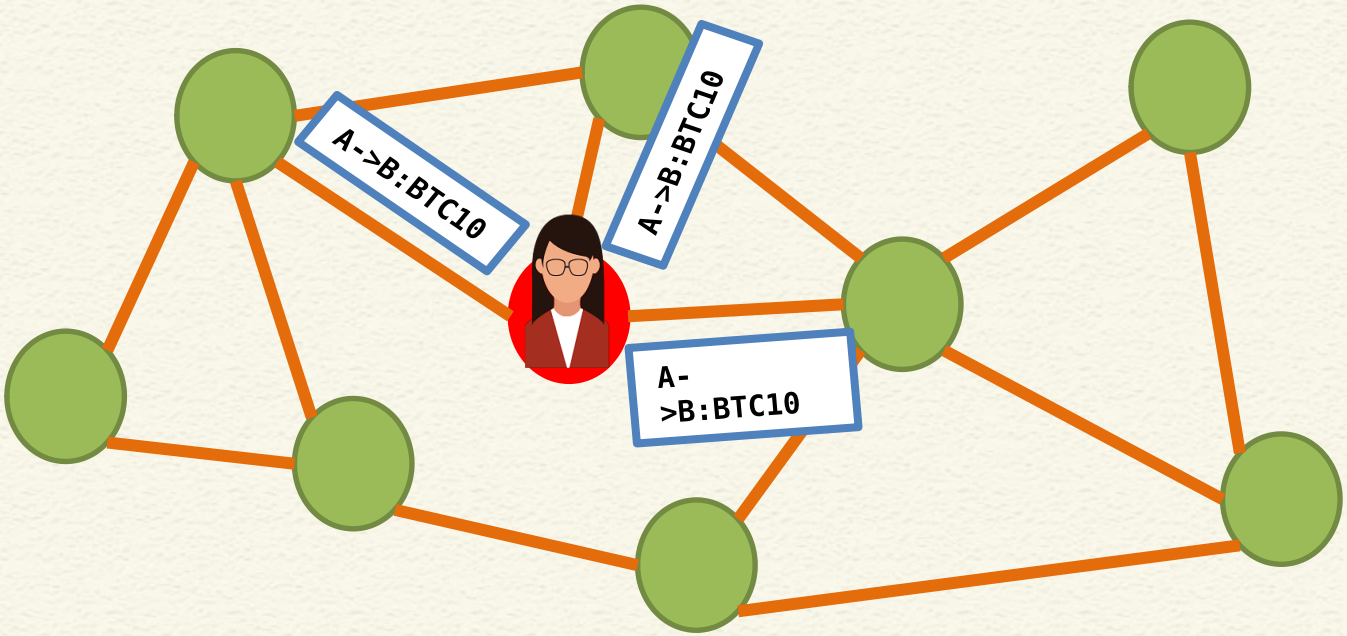
## Transactions in a Bitcoin Network

- Alice joins the Bitcoin network by opening her applet
- Alice makes a transaction to Bob: **`A->B: BTC 10`**
- Alice includes the scripts with the transactions
- Alice broadcasts this transaction in the Bitcoin network

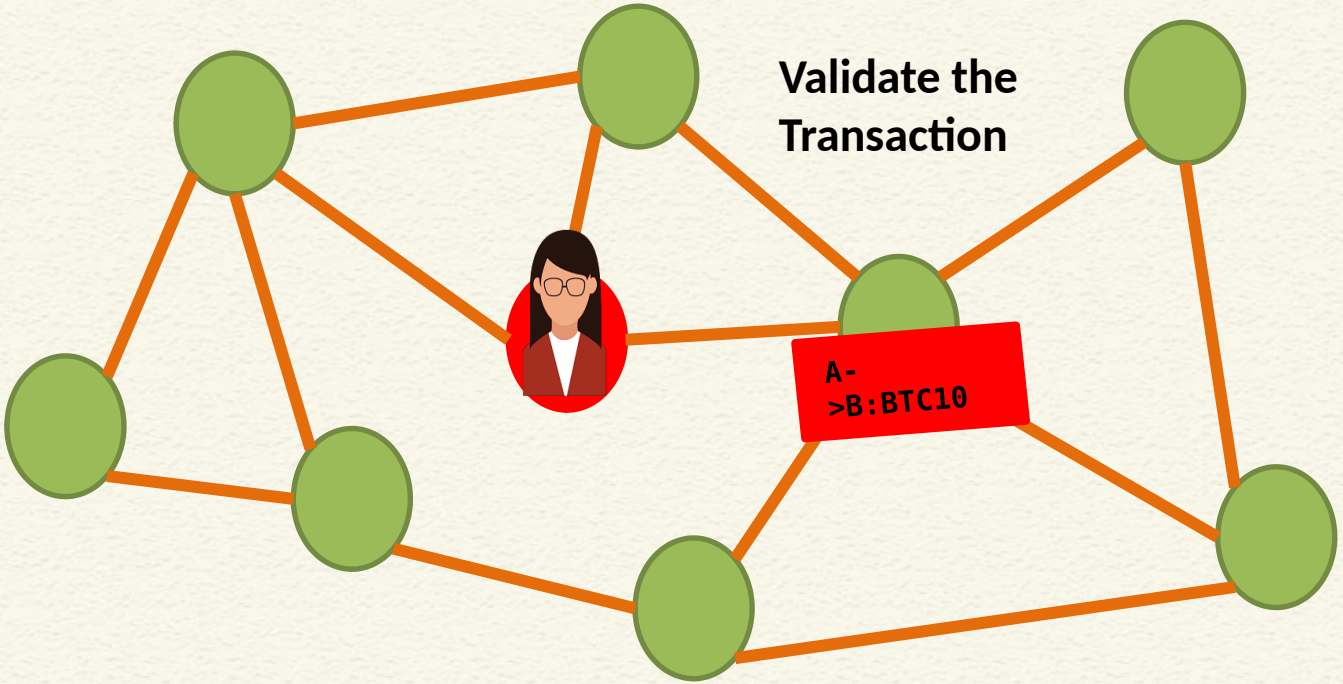
# Transaction Flooding in a Bitcoin Network



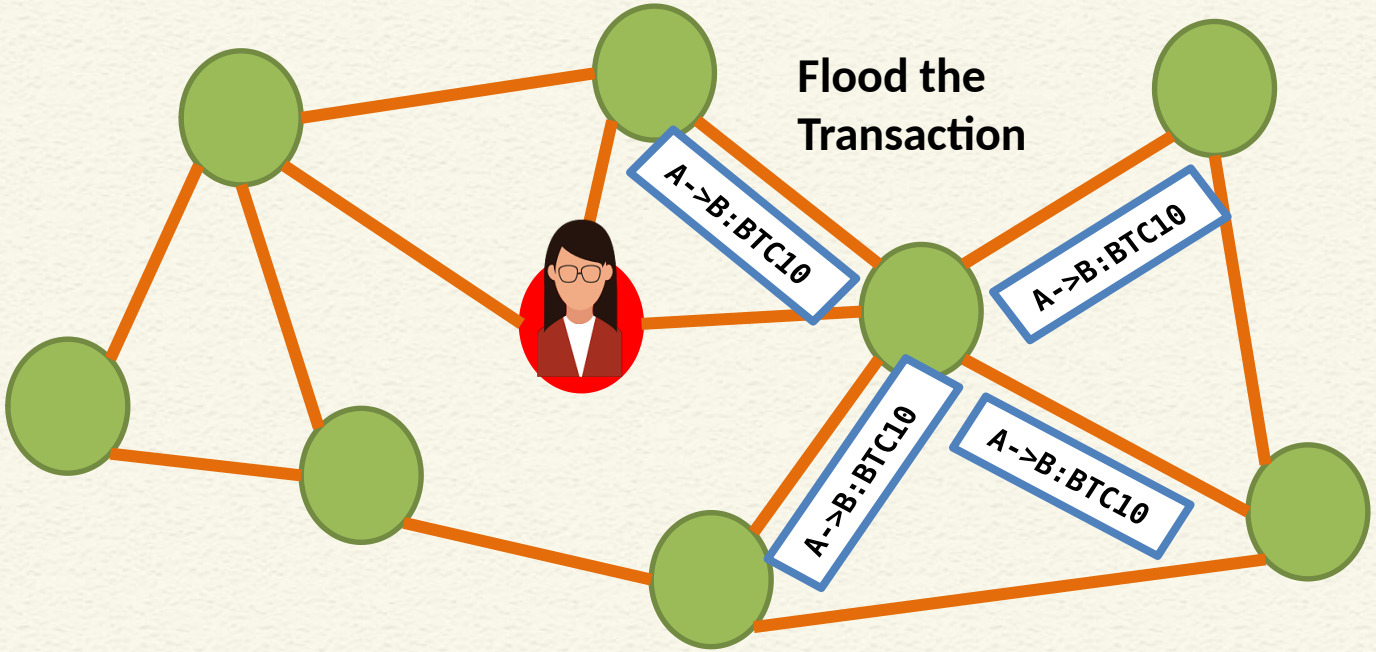
# Transaction Flooding in a Bitcoin Network



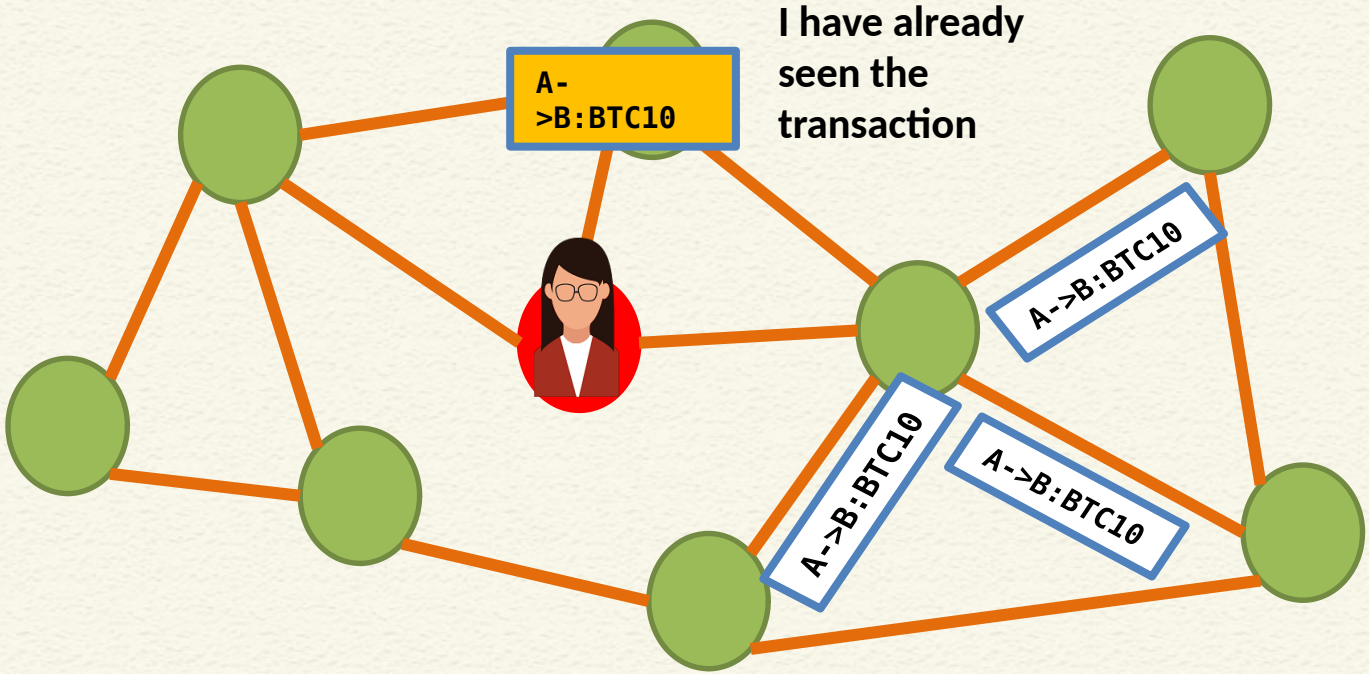
# Transaction Flooding in a Bitcoin Network



# Transaction Flooding in a Bitcoin Network



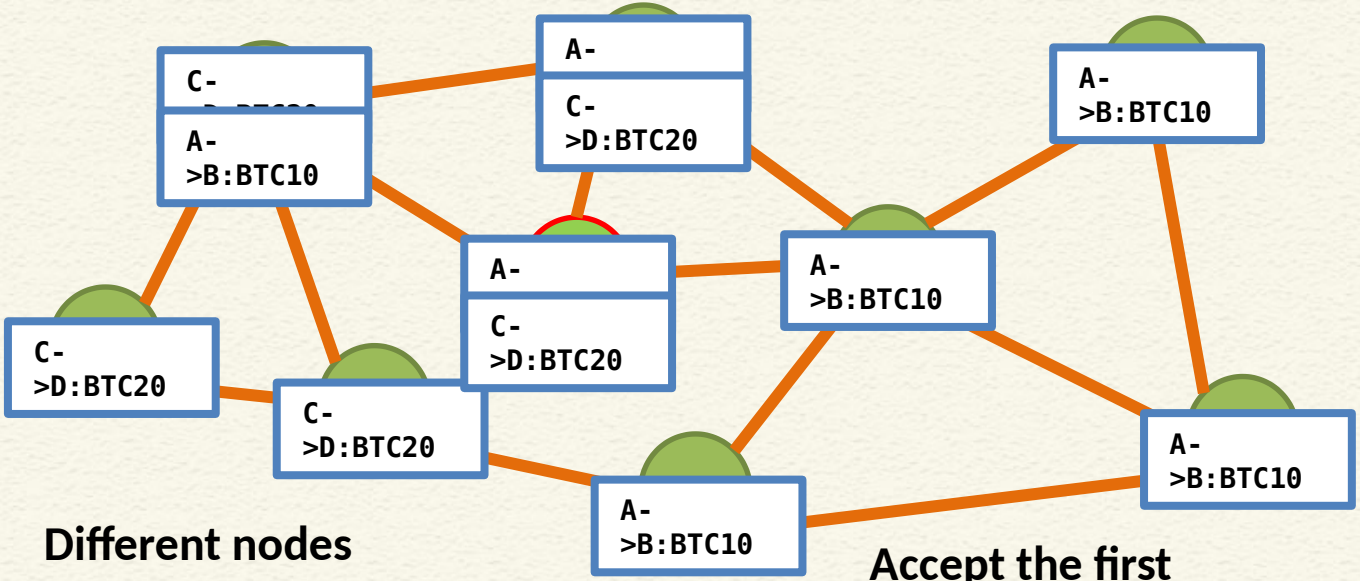
# Transaction Flooding in a Bitcoin Network



## Which Transactions Should You Relay?

- The transaction is valid with current blockchain
  - No conflict
  - No double spending
- The script matches with a pre-given set of whitelist scripts – Avoid unusual scripts, avoid infinite loops
- Does not conflict with other transactions that I have relayed after getting the blockchain updated – avoid double spending

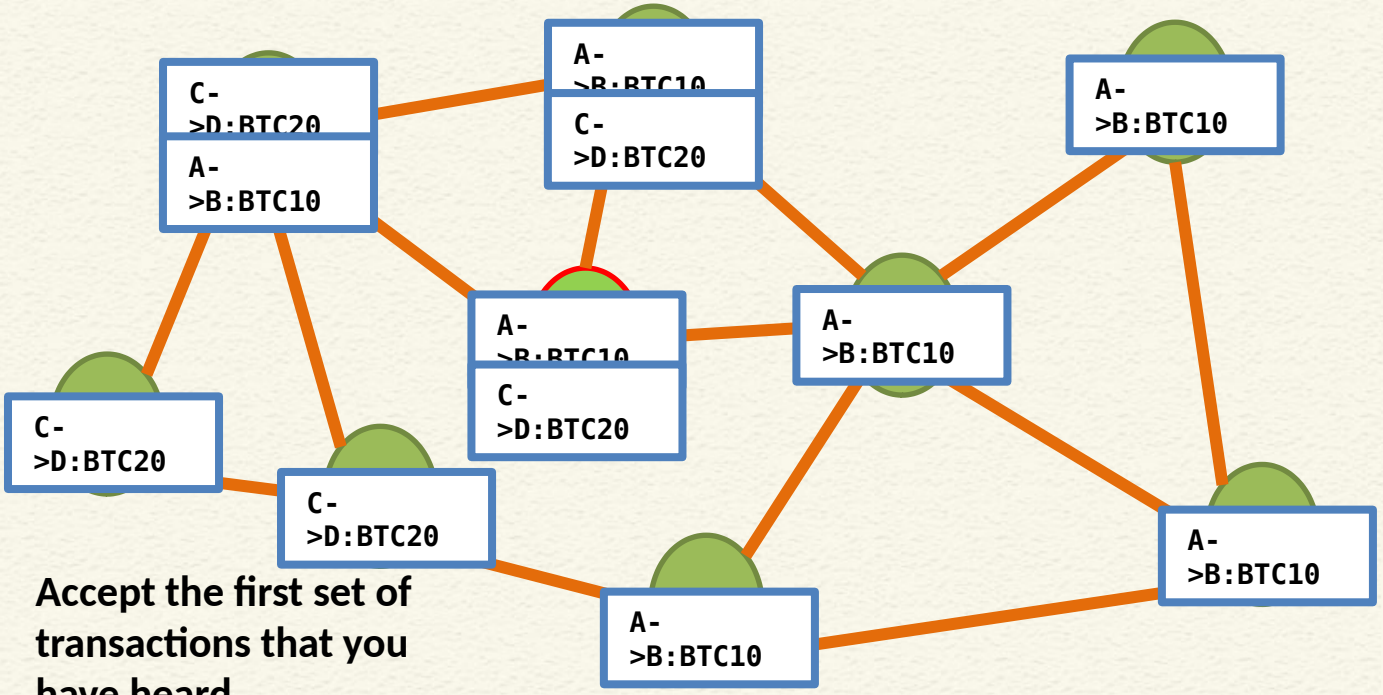
# Transaction Flooding in a Bitcoin Network




Different nodes may have different transaction pools

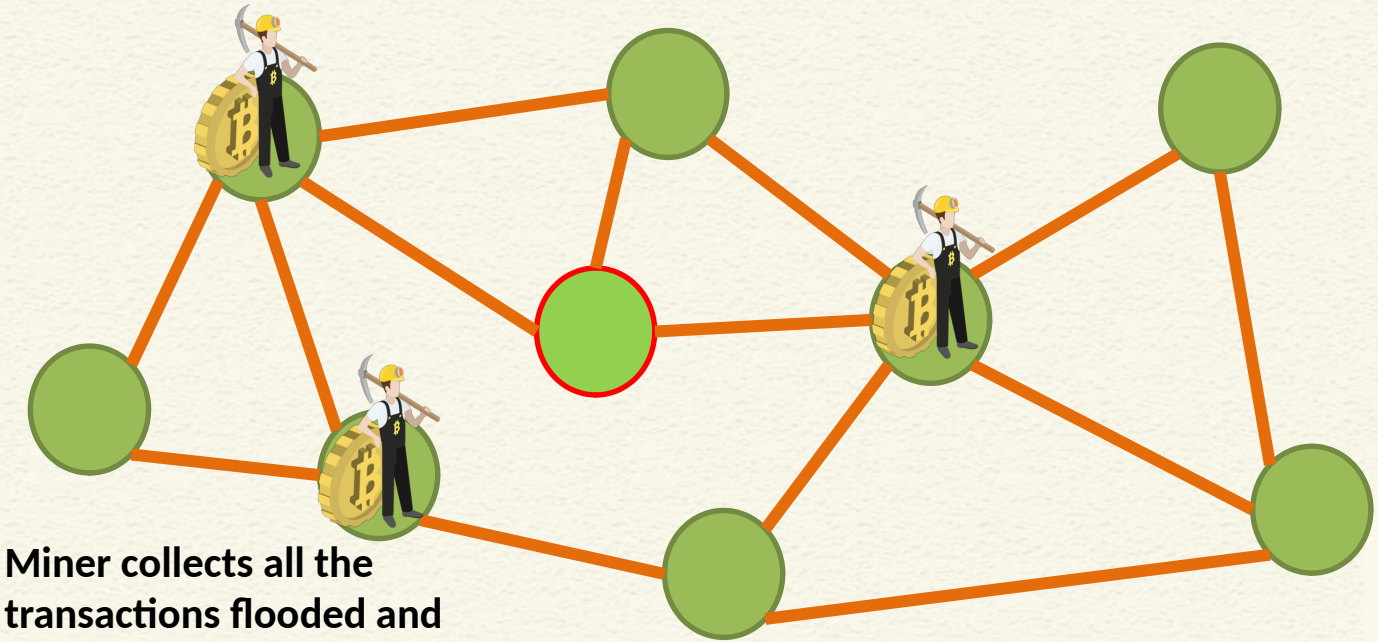
Accept the first transactions that you have heard

# Transaction Flooding in a Bitcoin Network



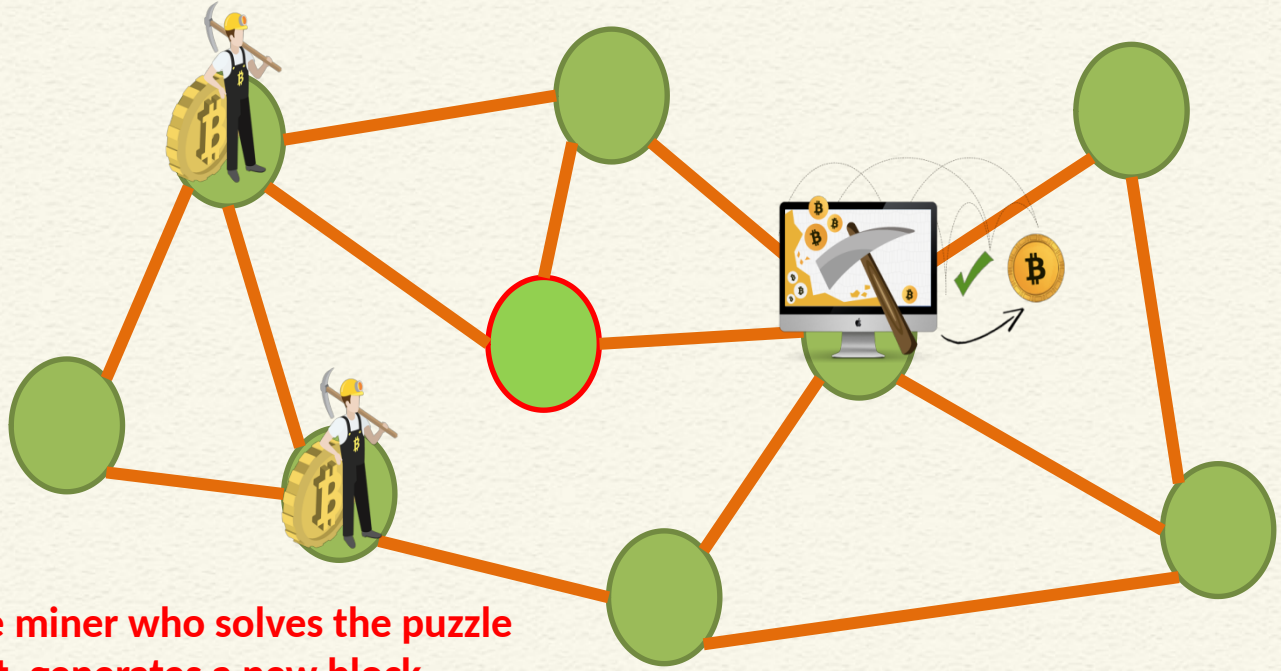

Accept the first set of transactions that you have heard

# Mining in a Bitcoin Network



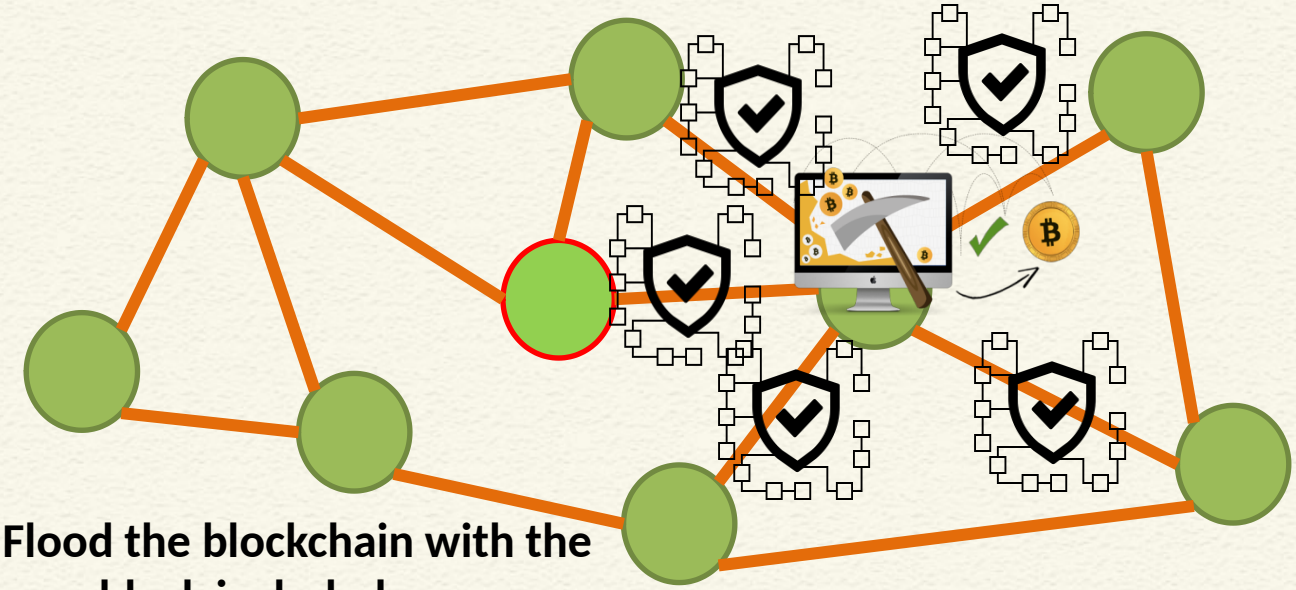
Miner collects all the transactions flooded and starts mining

# Block Generation



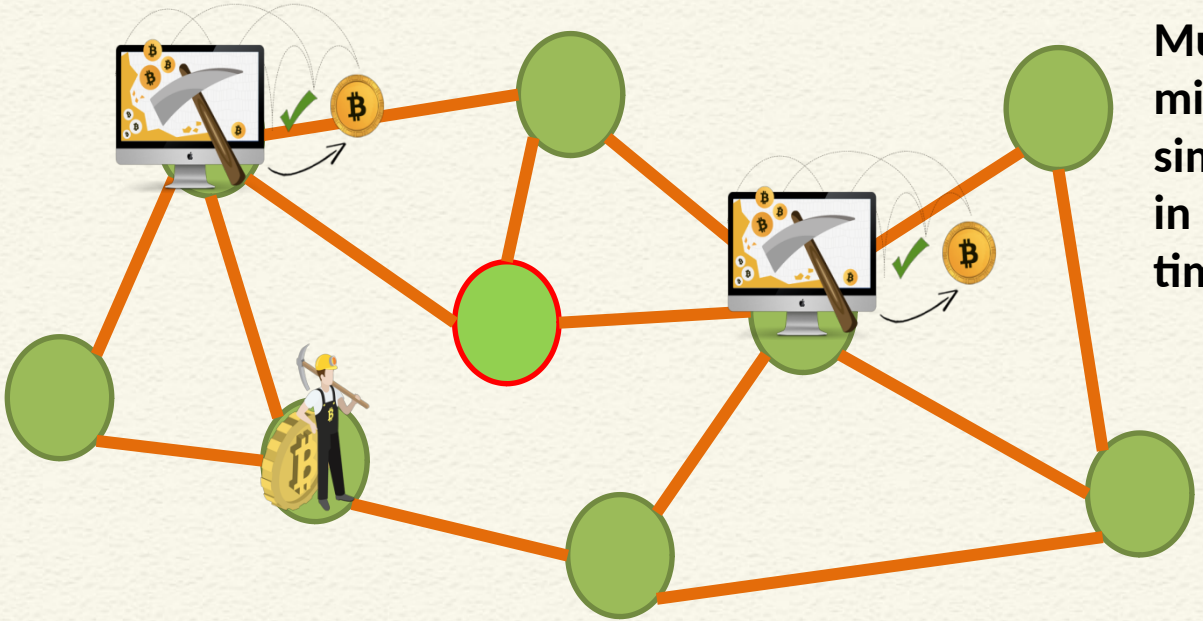
The miner who solves the puzzle first, generates a new block

# Block Flooding



Flood the blockchain with the new block included

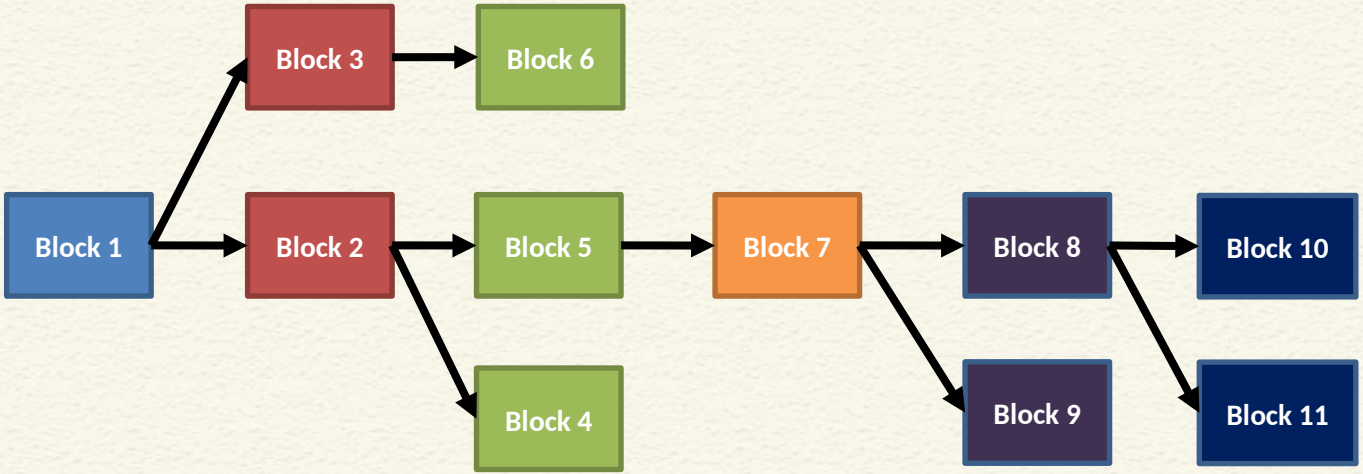
## Block Propagation



Multiple miners can mine a new block simultaneously or in a near identical time

"Forks" may get created

# Block Propagation – Accept the Longest Chain




- "Accidental" forks occur rarely. Even if they occur, eventually only one becomes part of the longest chain
- There are "intentional" forks of two type: hard forks and soft forks to come up with new versions like Bitcoin Cash, etc., or to upgrade software versions

## Which Block to Relay

- Block contains the correct hash based on the existing blockchain
- All the transactions inside the block are valid
  - Check the scripts
  - Validate with the existing blockchain
- The block is included in the current longest chain
  - Do not relay the forks

# CONCLUSIONS

- Shown how a new node can join the bitcoin network
- Creation and propagation of transactions
- Accumulating transactions and mining new blocks
- Propagation of new bitcoin blocks
- Discussed how forking is handled in a blockchain

# REFERENCES


- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Blockchain: Hype or Innovation by Tatiana Gayvoronskaya and Christoph Meinel, Springer (2021)
- Any other standard textbook on blockchain/bitcoin


Thank
you