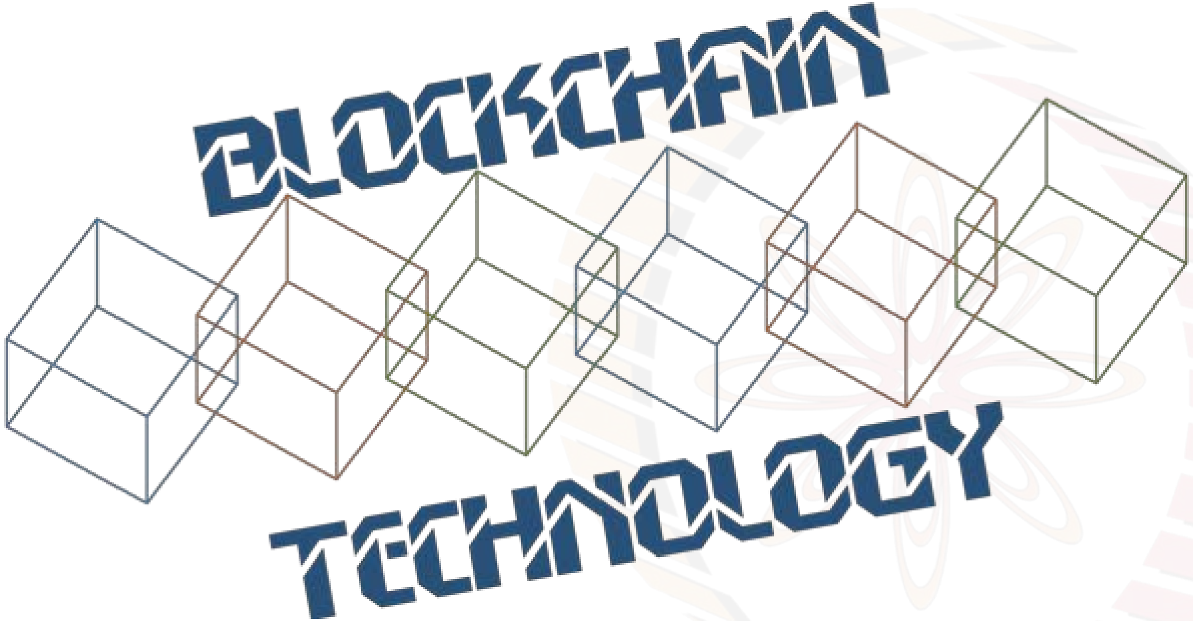
BLOCKCHAINS

ARCHITECTURE, DESIGN AND USE CASES

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA

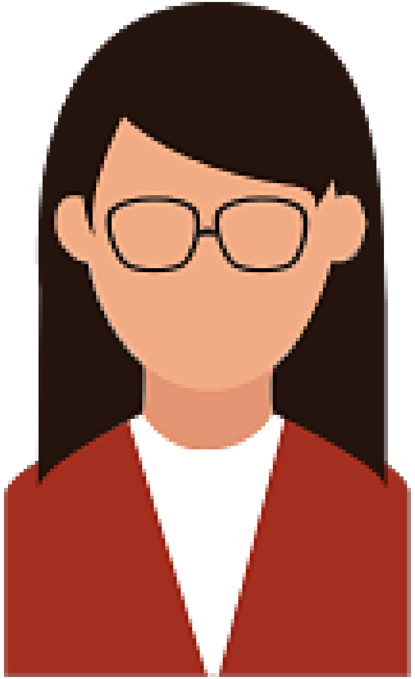
Image courtesy: http://beetfusion.com/



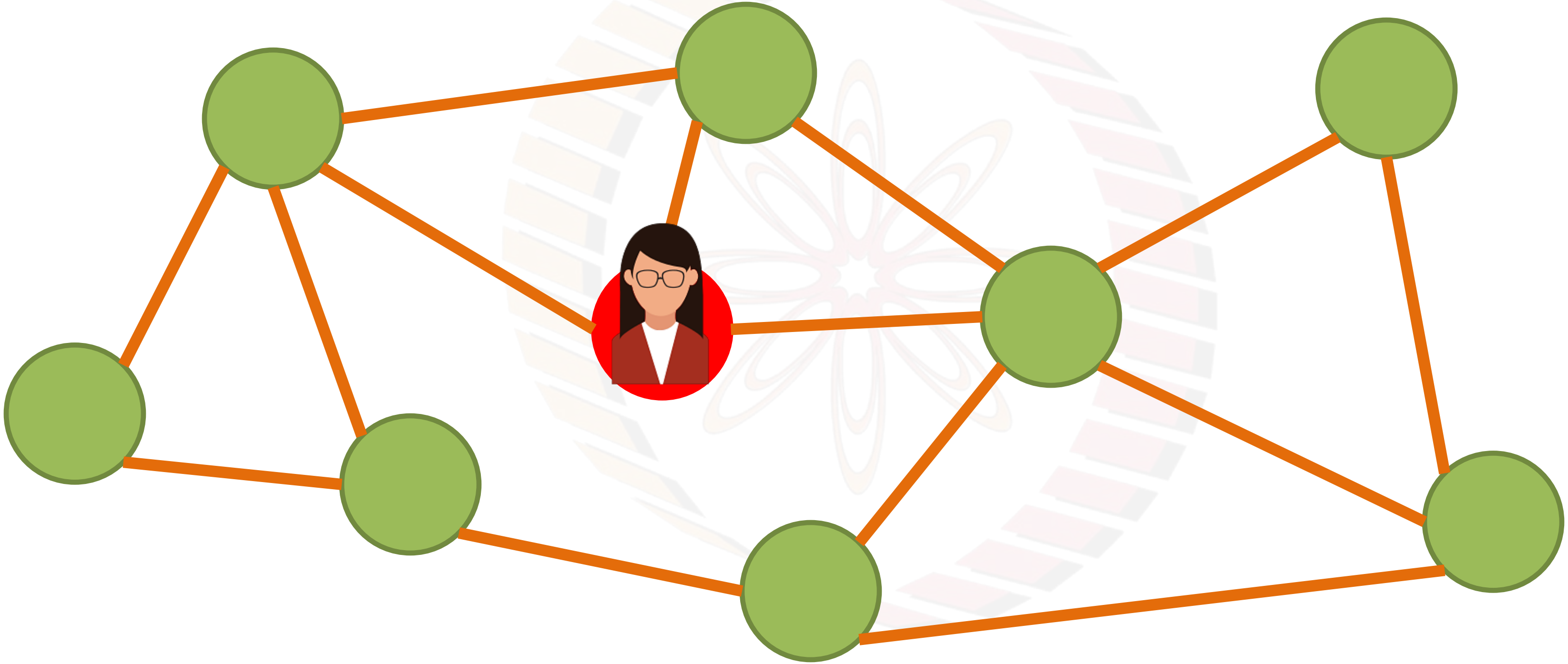
BITCOIN BASICS III

Transaction in a Bitcoin Network

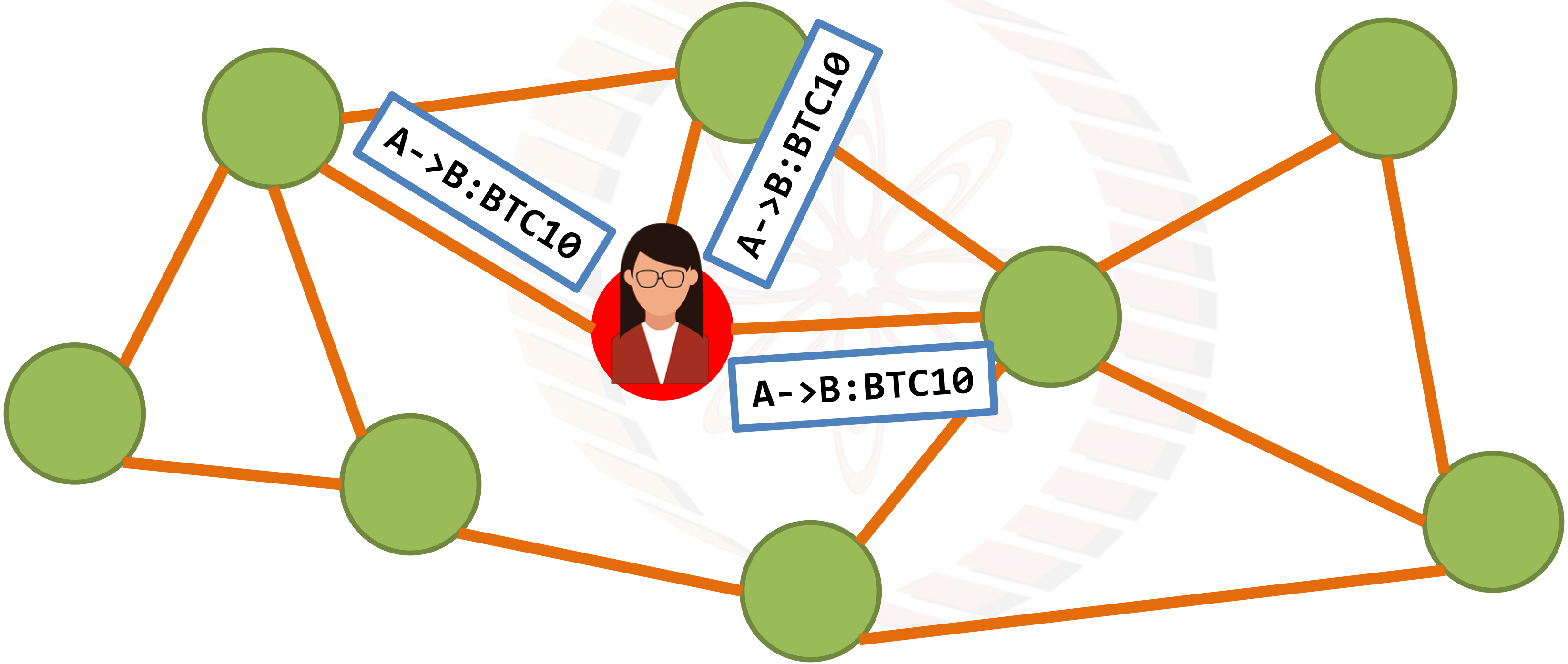
- Alice joins the Bitcoin network by opening her applet
- Alice makes a transaction to Bob: **`A->B: BTC 10`**
- Alice includes the scripts with the transactions
- Alice broadcasts this transaction in the Bitcoin network



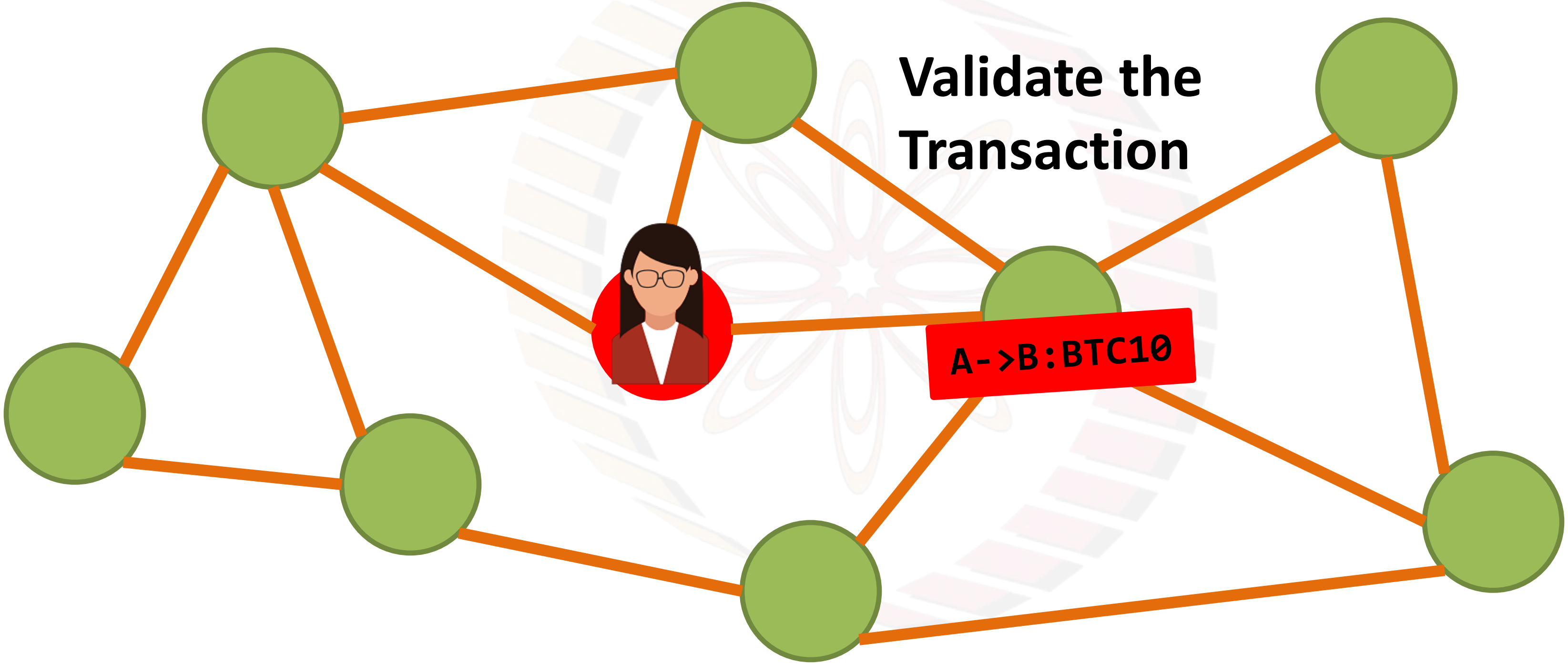
Transaction Flooding in a Bitcoin Network



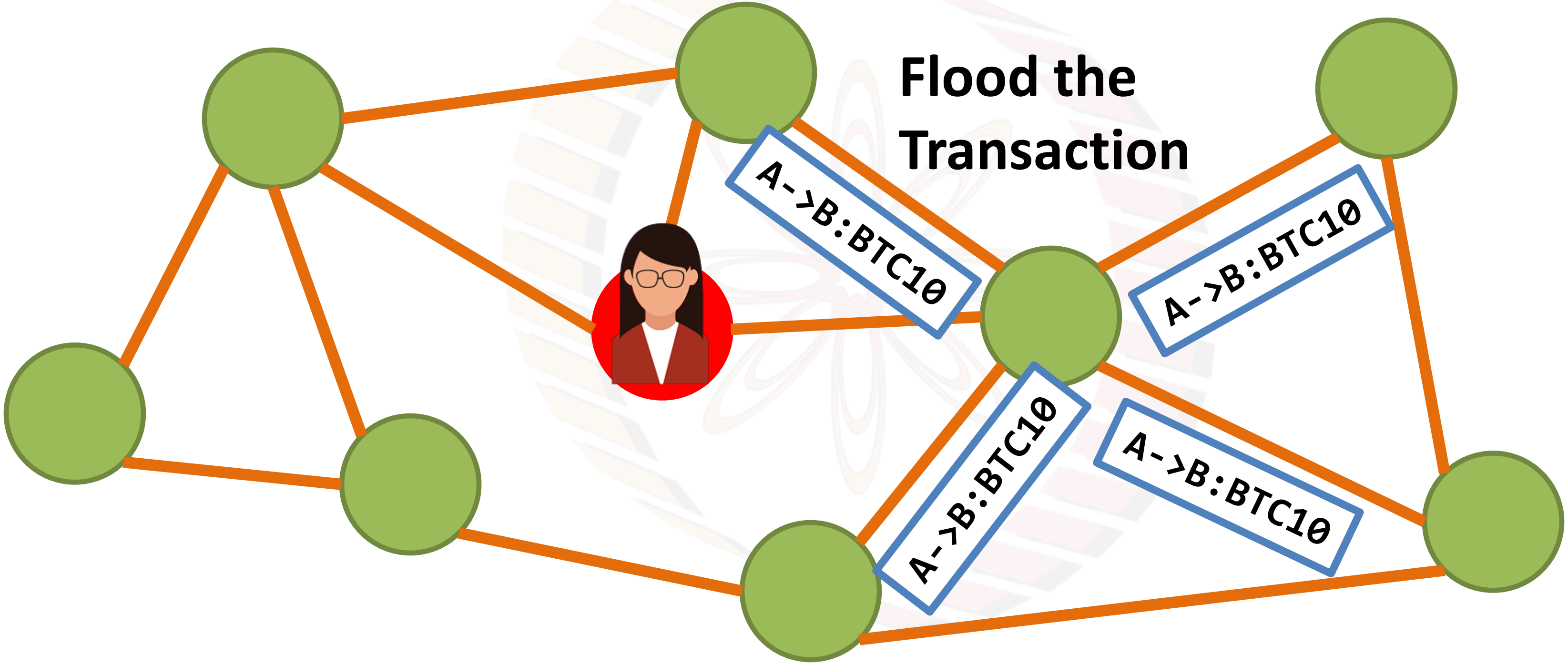
Transaction Flooding in a Bitcoin Network



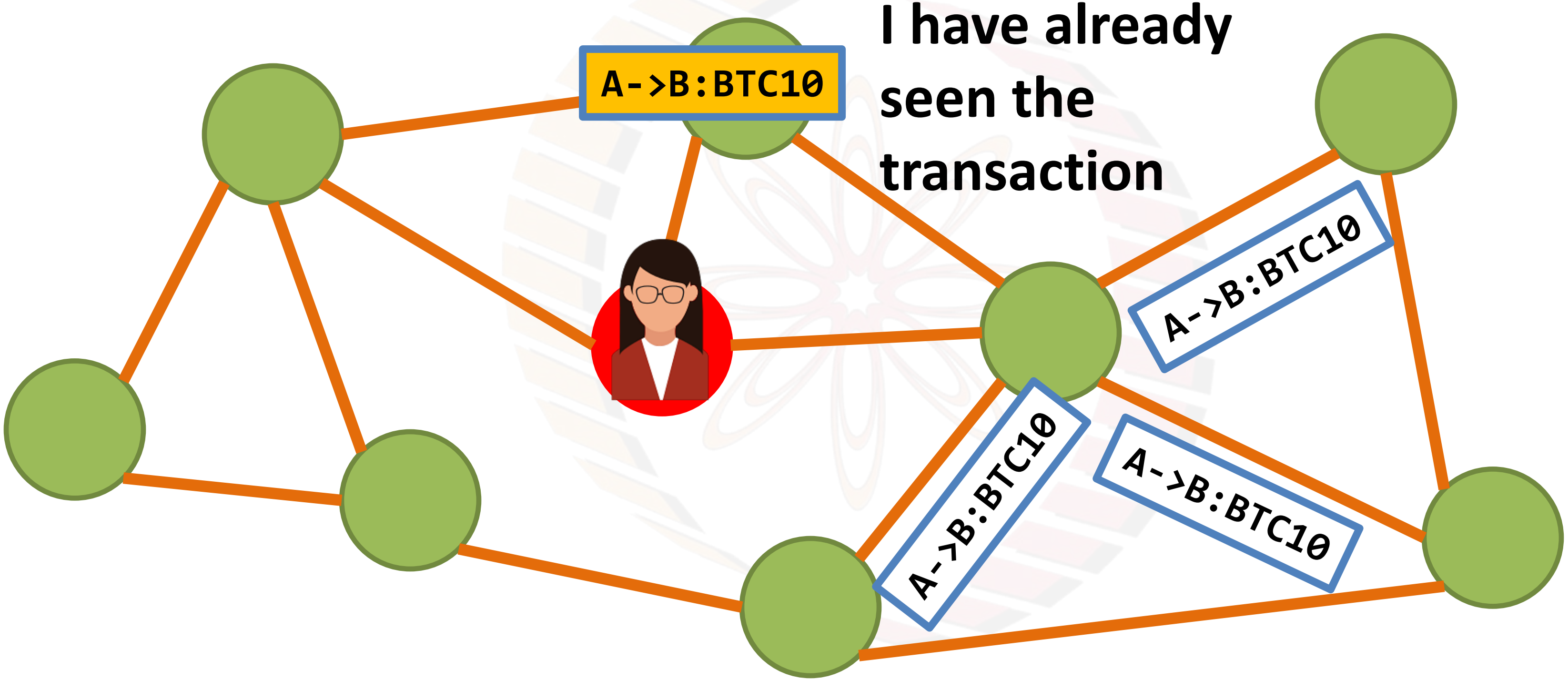
Transaction Flooding in a Bitcoin Network



Transaction Flooding in a Bitcoin Network



Transaction Flooding in a Bitcoin Network



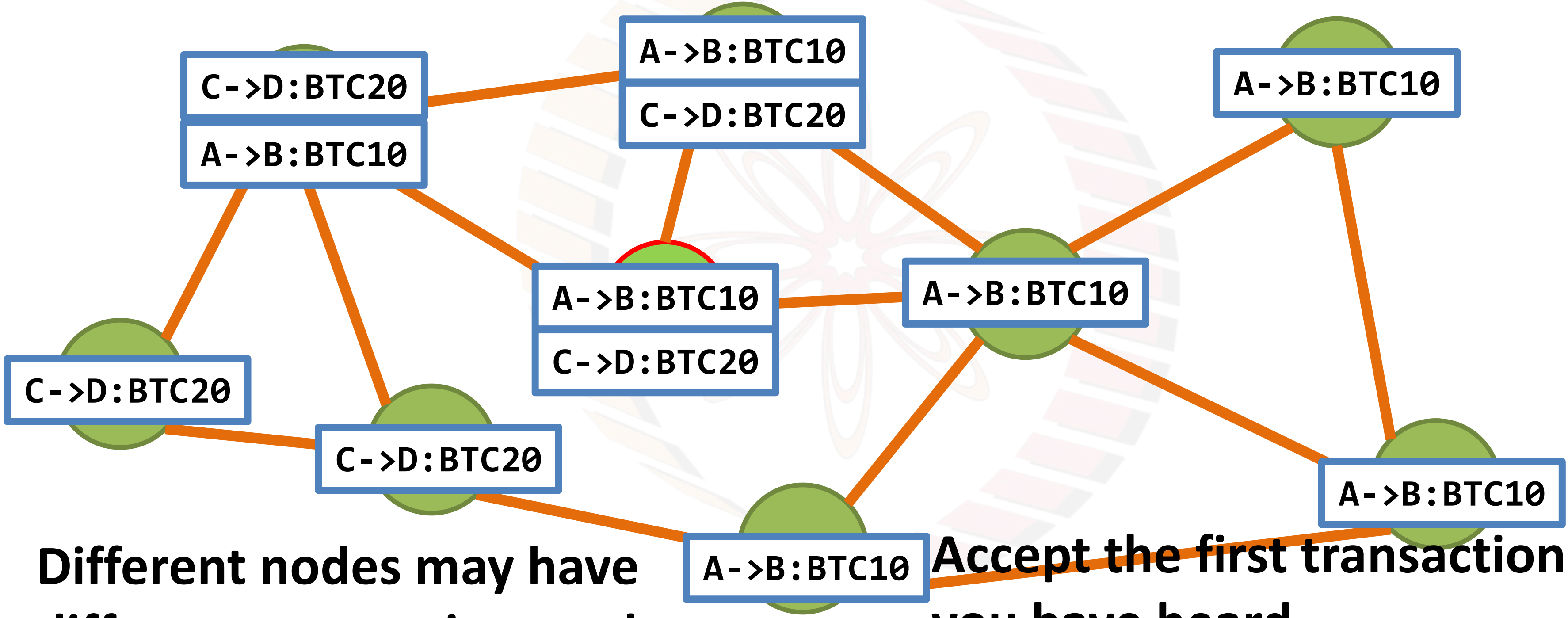
Which Transactions Should You Relay?

- 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

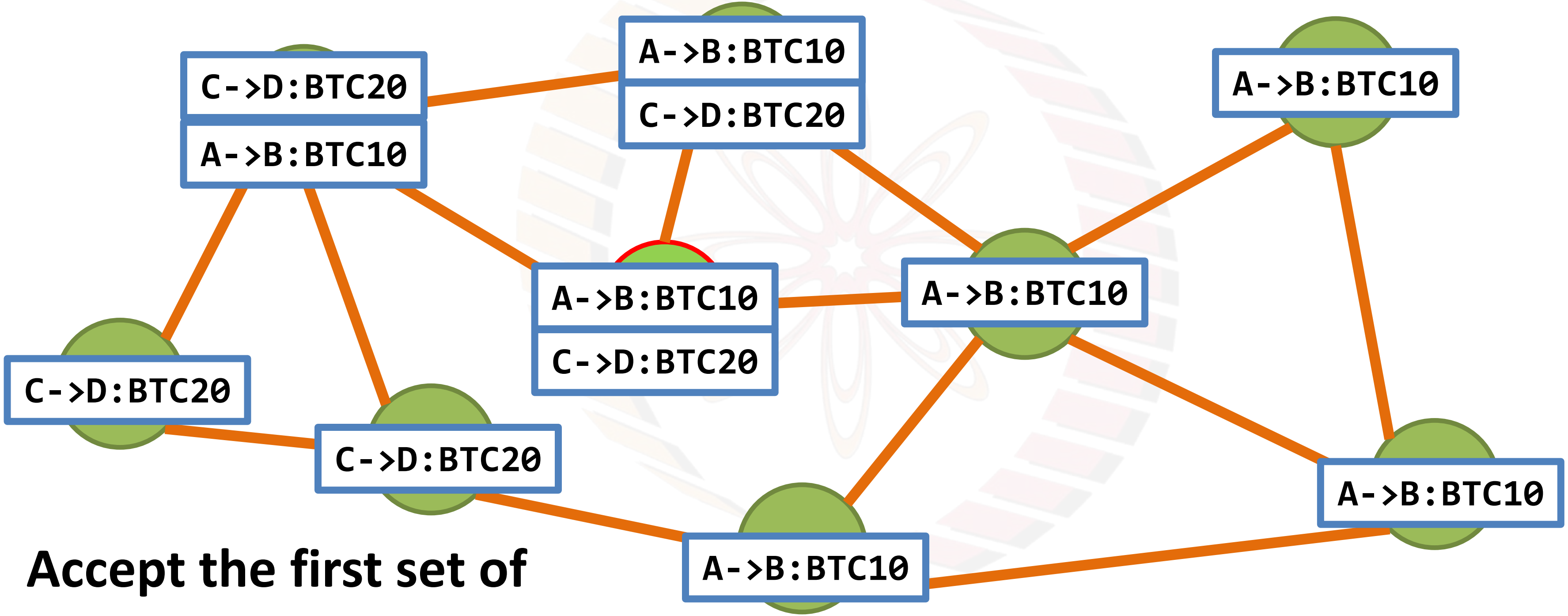
Transaction Flooding in a Bitcoin Network



Different nodes may have different transaction pools

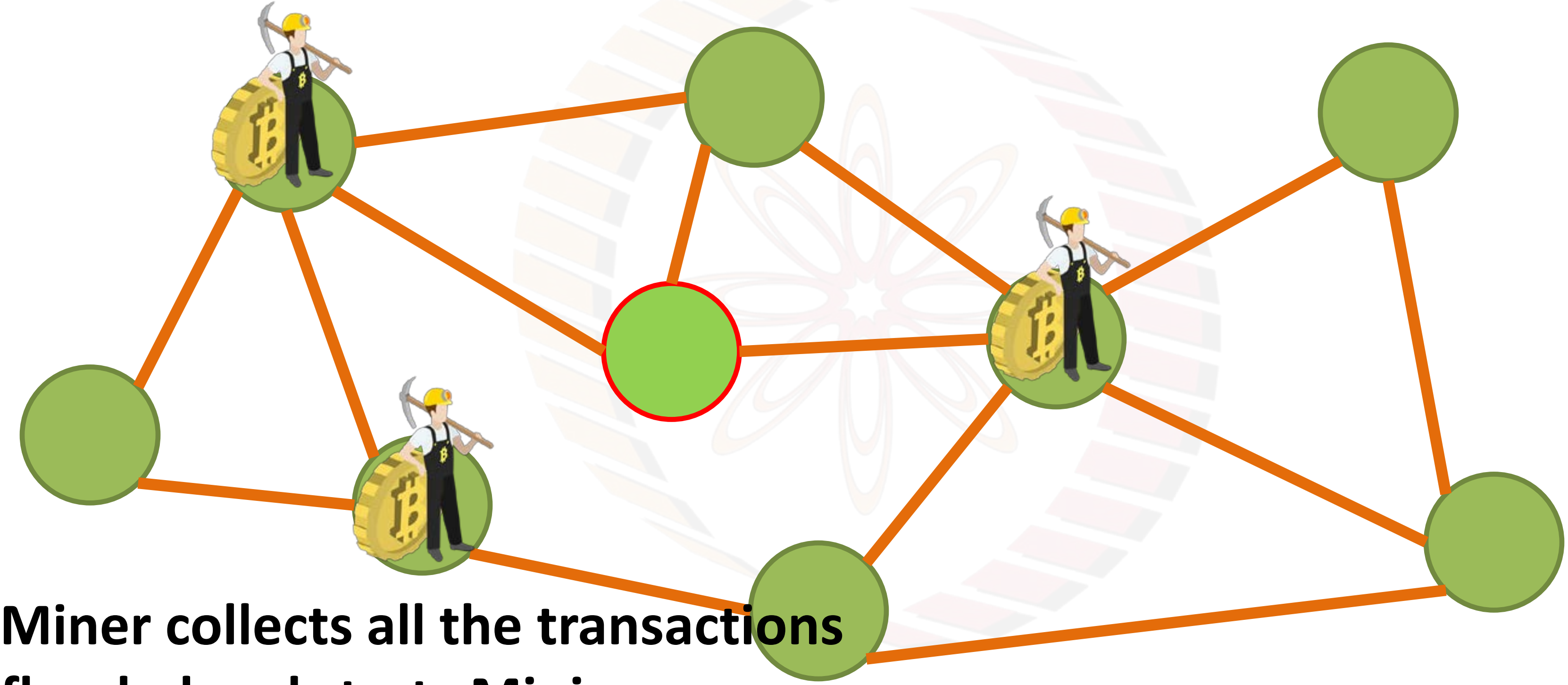
Accept the first transactions that you have heard

Transaction Flooding in a Bitcoin Network



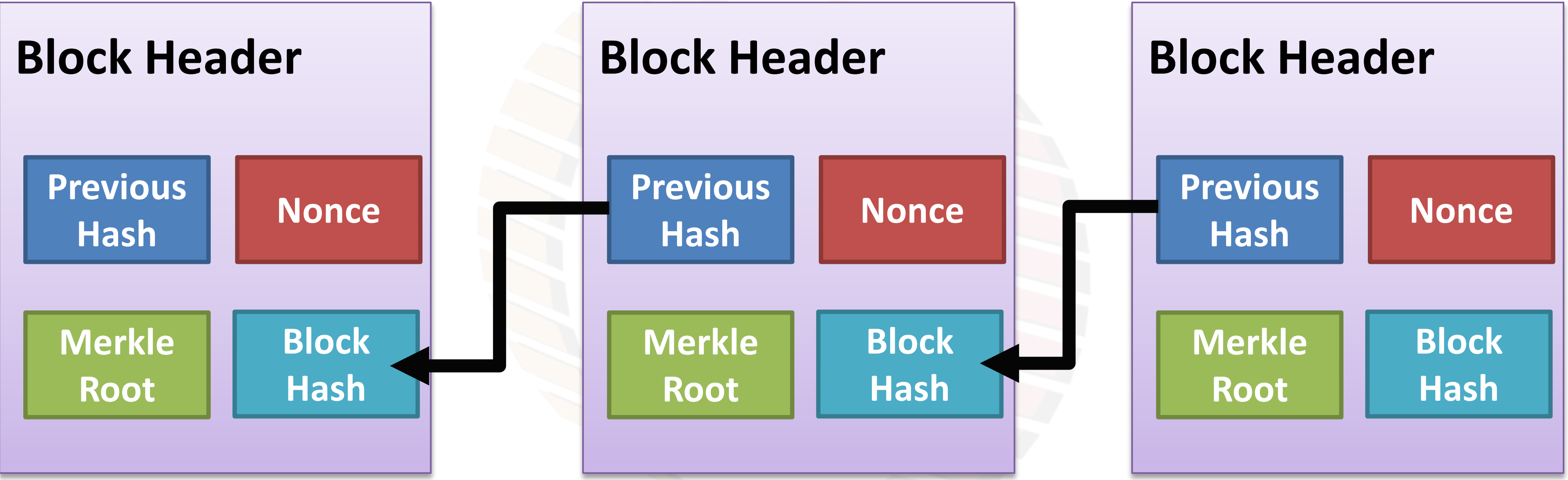
Accept the first set of transactions that you have heard

Mining in a Bitcoin Network



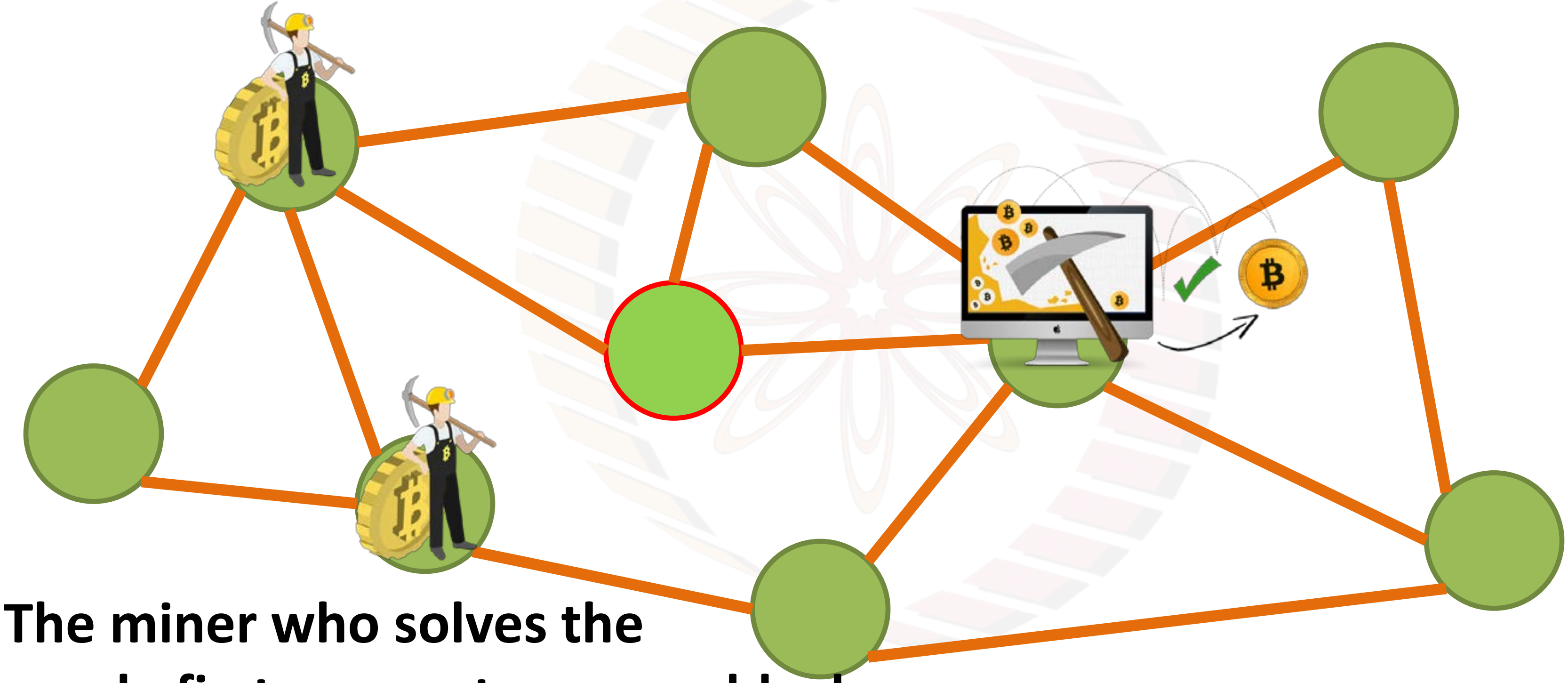
Miner collects all the transactions flooded and starts Mining

Block Generation Puzzle



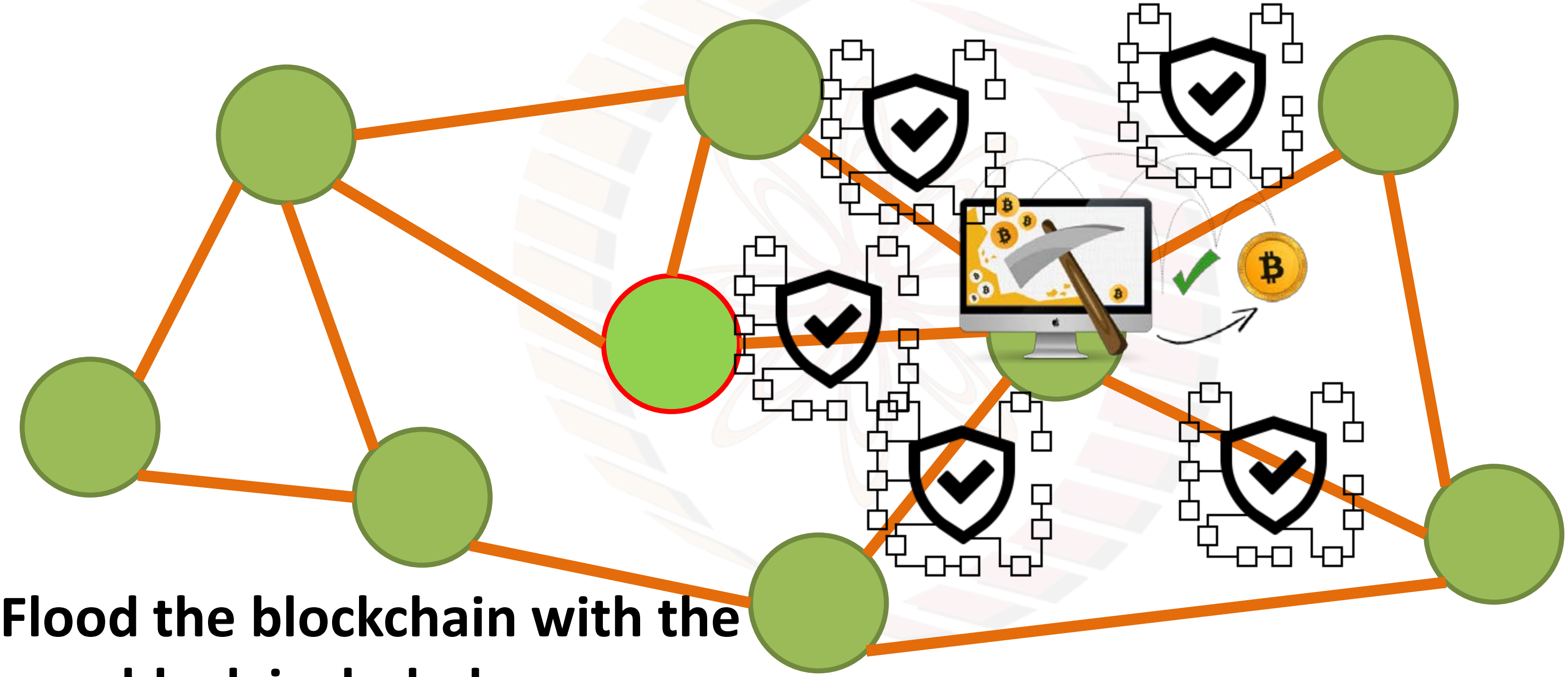
Find out the nonce which generates the desired hash (certain zero bits at the prefix - 0000000000000000004a2b84f93a285b7a7........

Block Generation



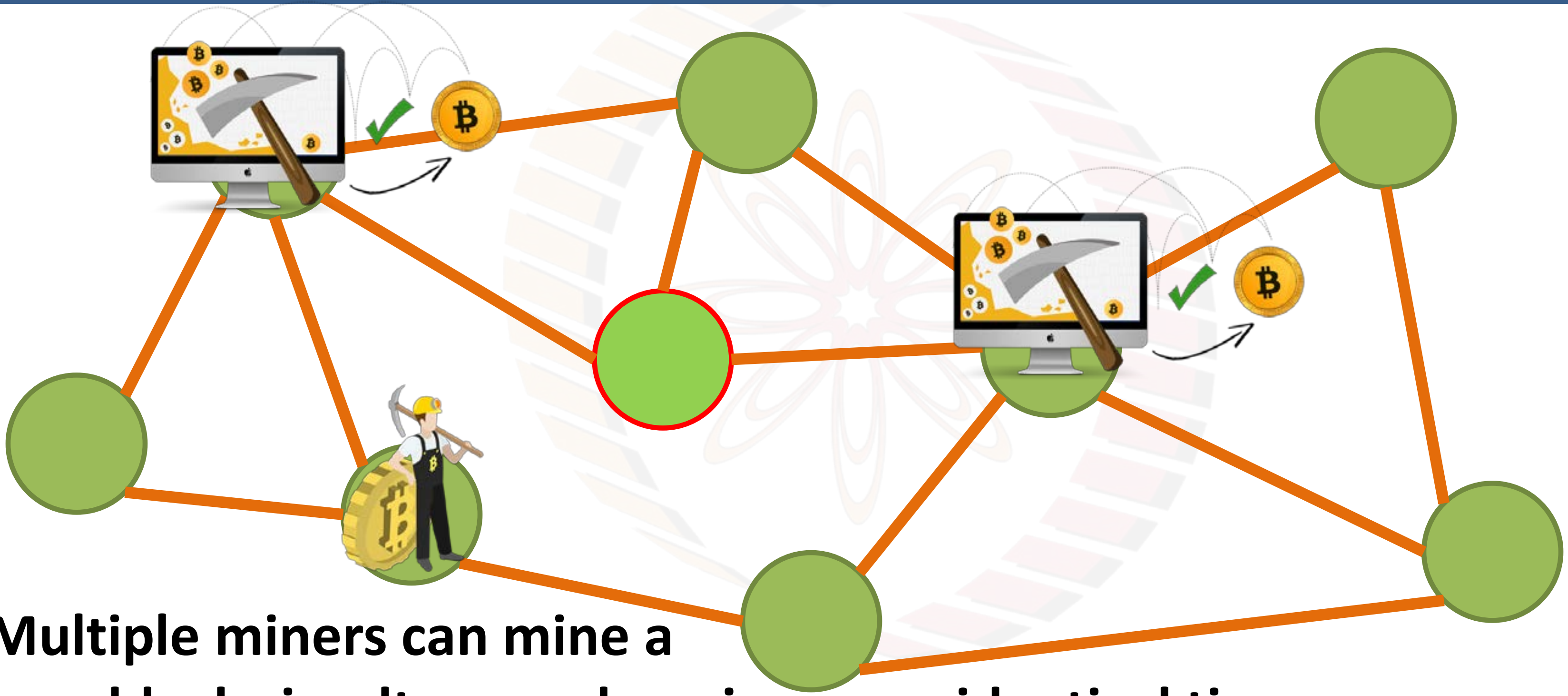
The miner who solves the puzzle first, generates a new block

Block Flooding



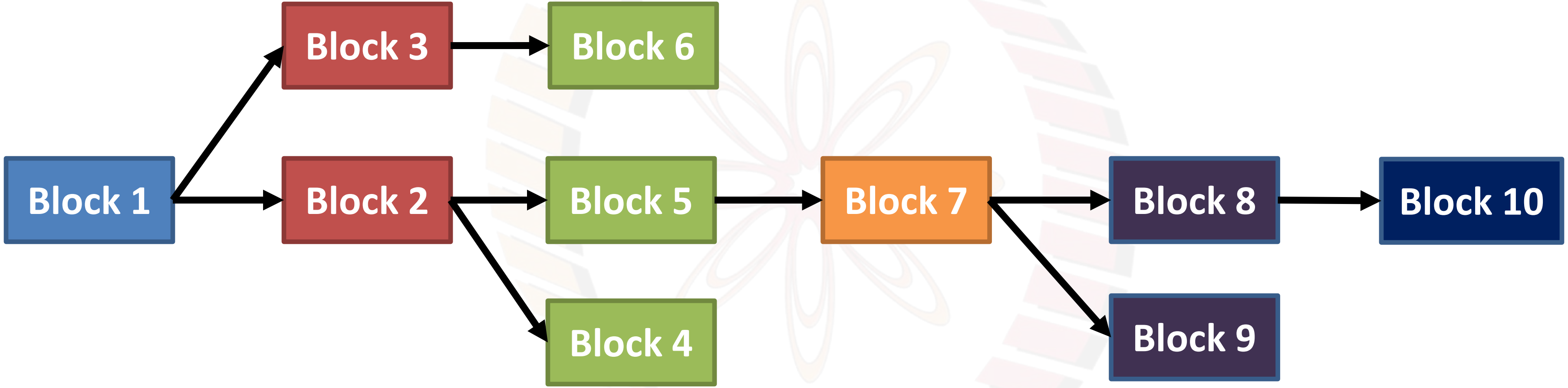
Flood the blockchain with the new block included

Block Propagation

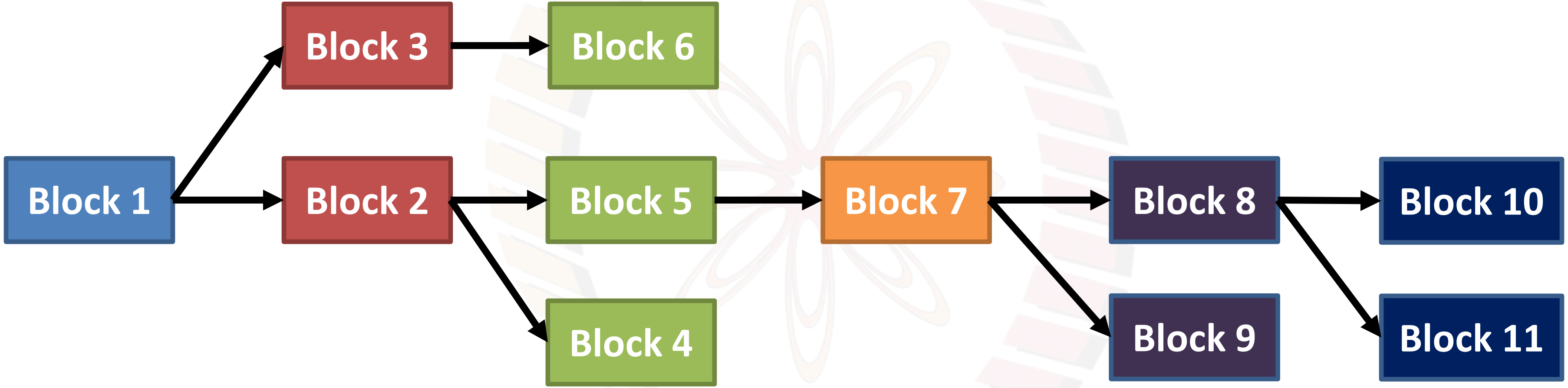


Multiple miners can mine a new block simultaneously or in a near identical time

Block Propagation – Accept the Longest Chain



Block Propagation – Accept One of the Longest Chain



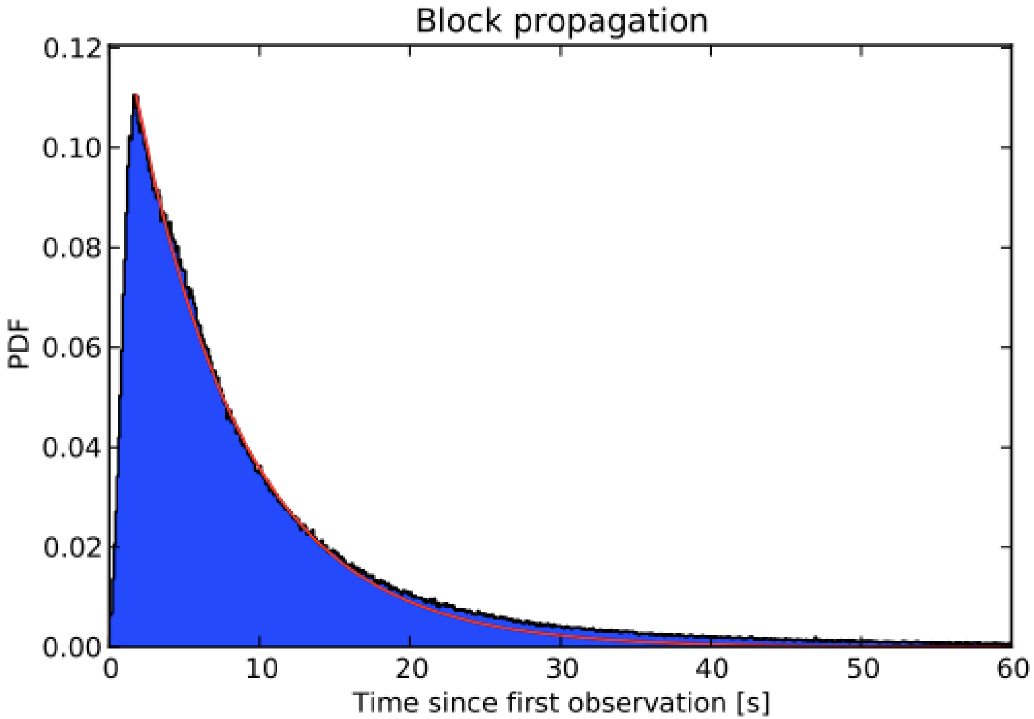
Which Block to Relay

- 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

Block Propagation Latency



Mean time = 12.6 Seconds

95% of the nodes can see the block within 40 seconds

Decker, Christian, and Roger Wattenhofer. "Information propagation in the bitcoin network." ***2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P)*****. IEEE, 2013.**

BITCOIN·DIGITAL·DECENTRALIZED·PEER TO PEER
999 FINE COPPER
MB MONETARY METALS

thank you!