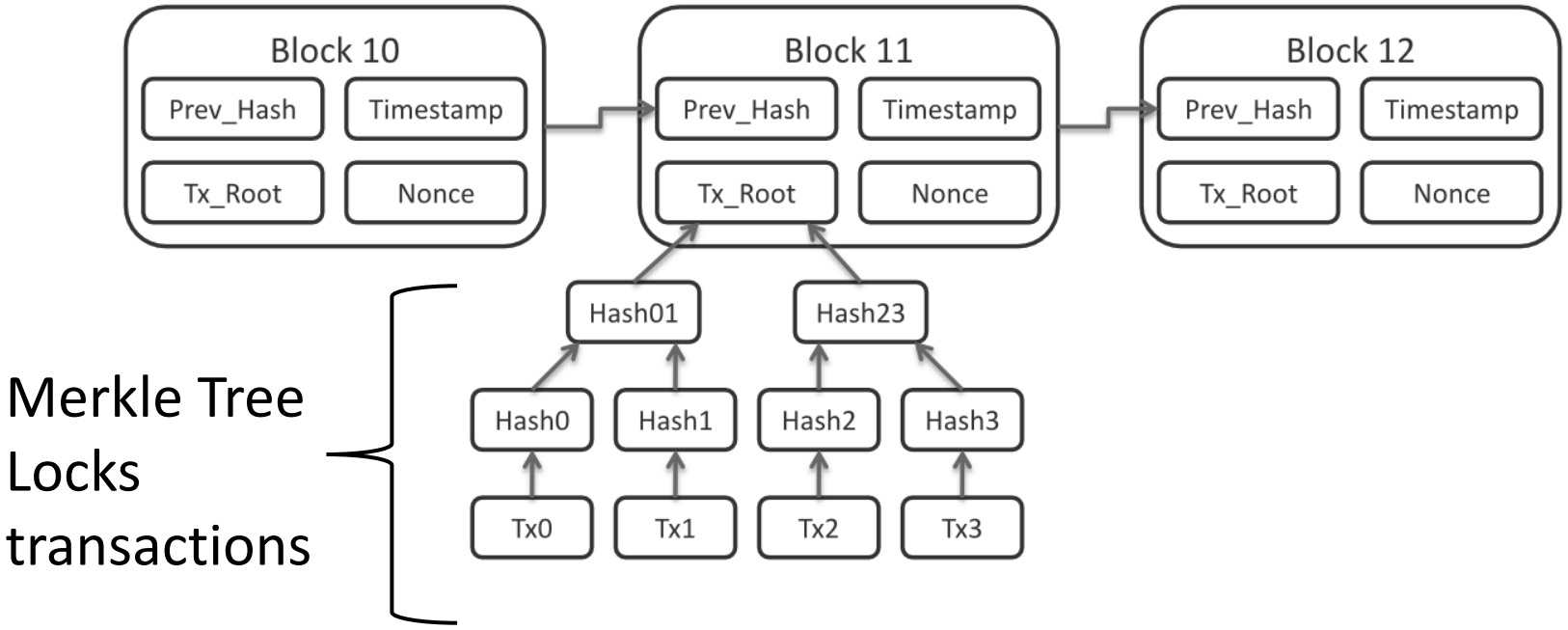
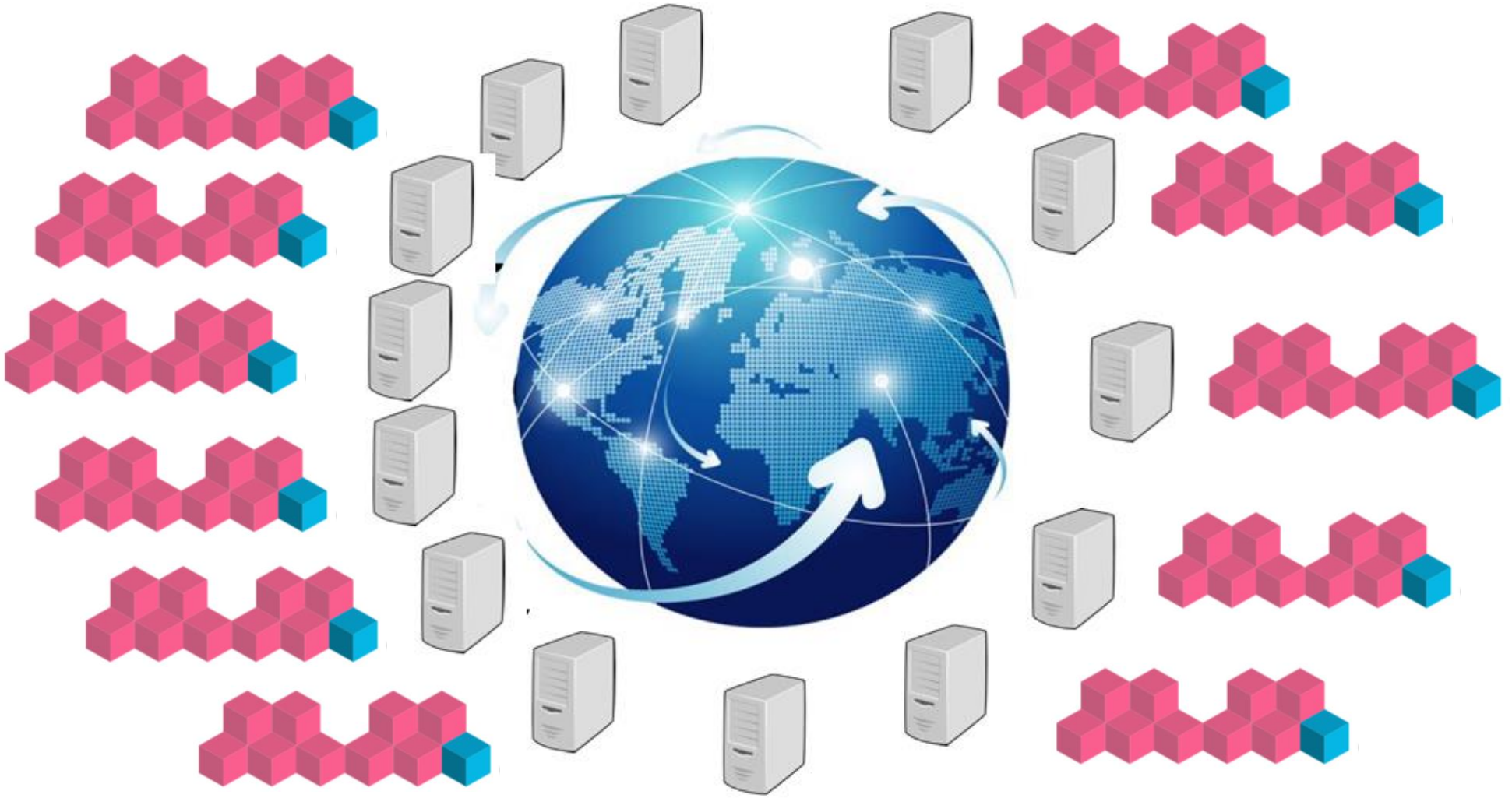

BlockChain Operations
John R Williams, MIT
Transforming the FinTech Revolution

Merkle Tree Locks Transactions and Hashes Chain Blocks

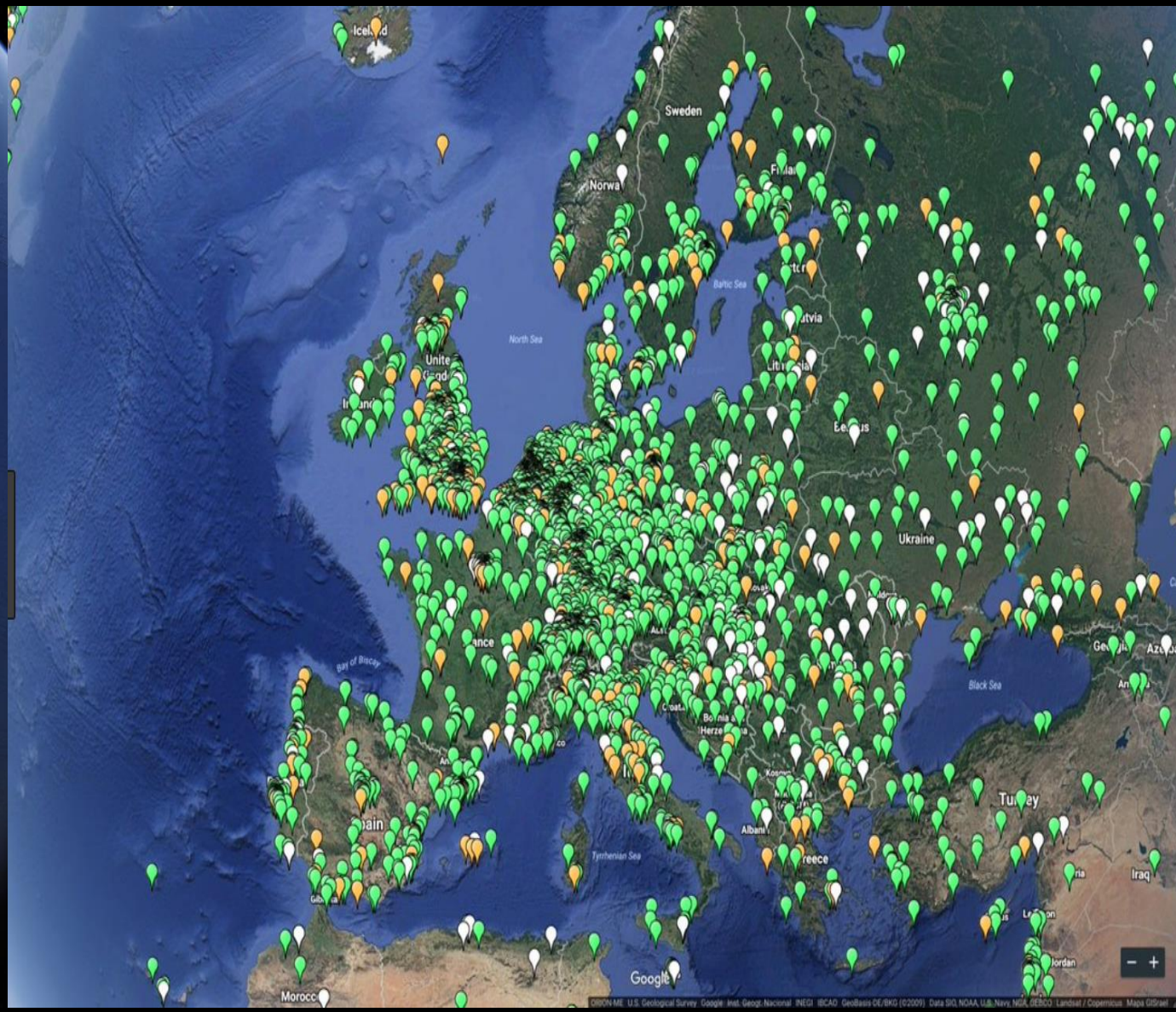
Hash(Prev_Hash + Tx_Root + Nonce) → 000000bc9xxx



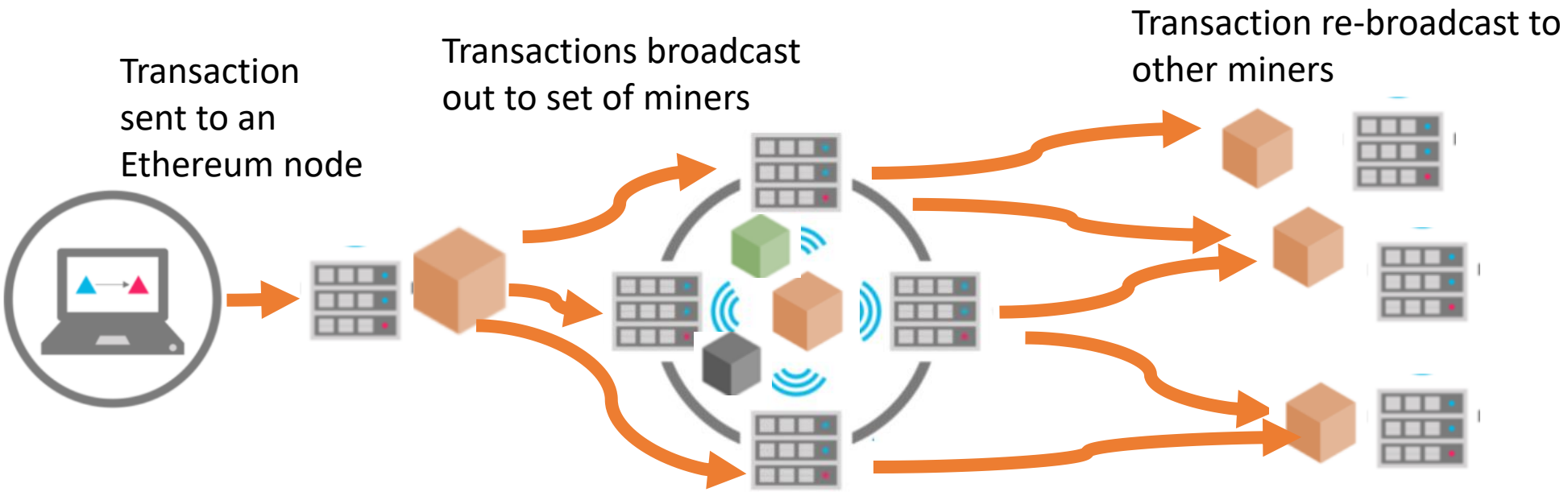
Can we build a system where we all agree on the exact same transactions and their order?



Etherium Nodes

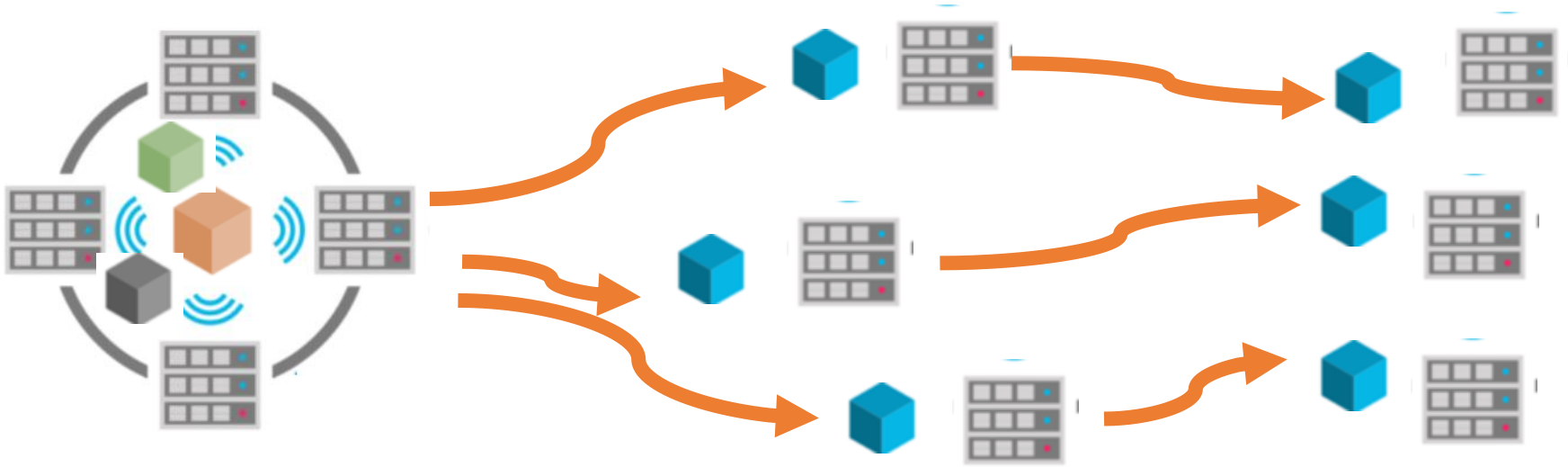


Transaction sent to one Ethereum node. That node broadcasts it to others who broadcast to others …

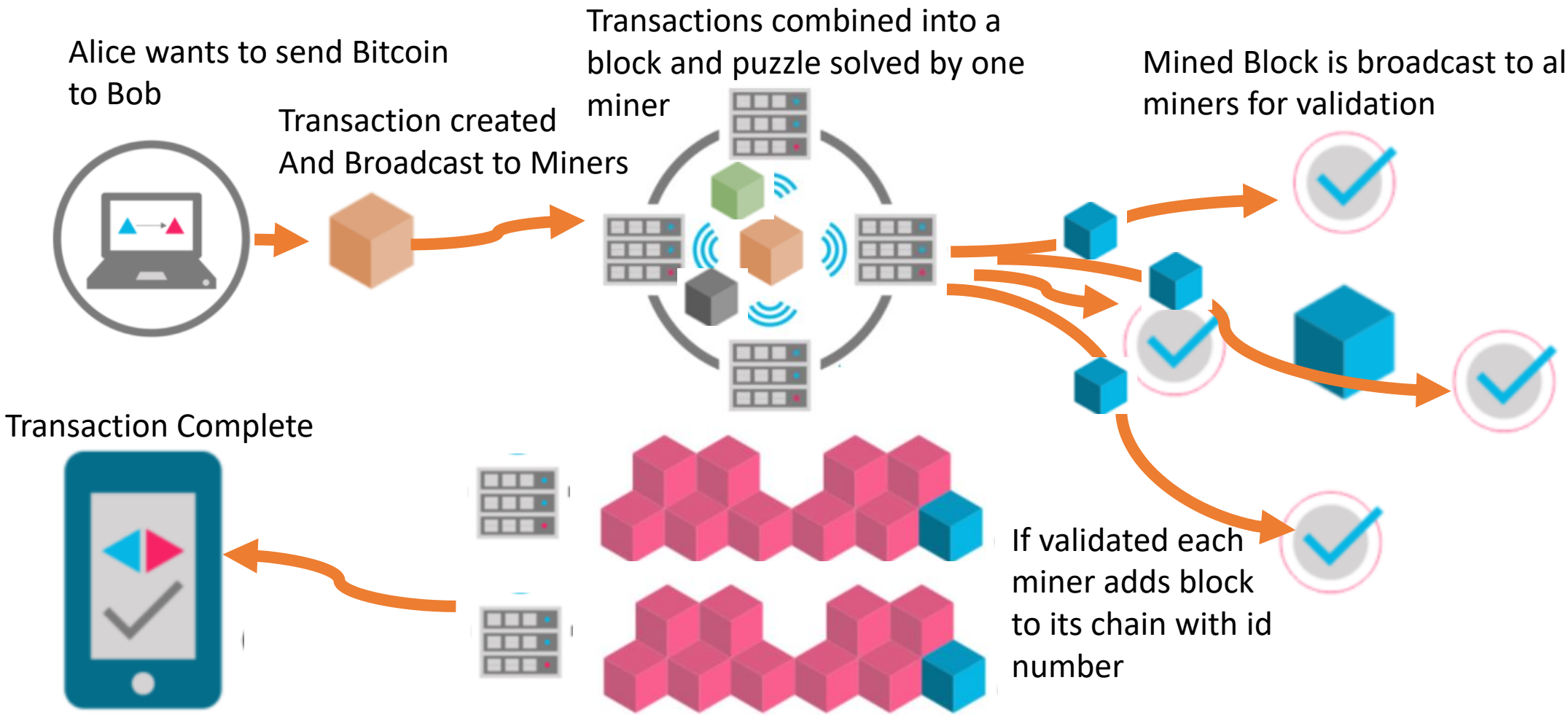


Your transaction may or may not be combined into a block. Miners race to form a valid block by solving puzzle

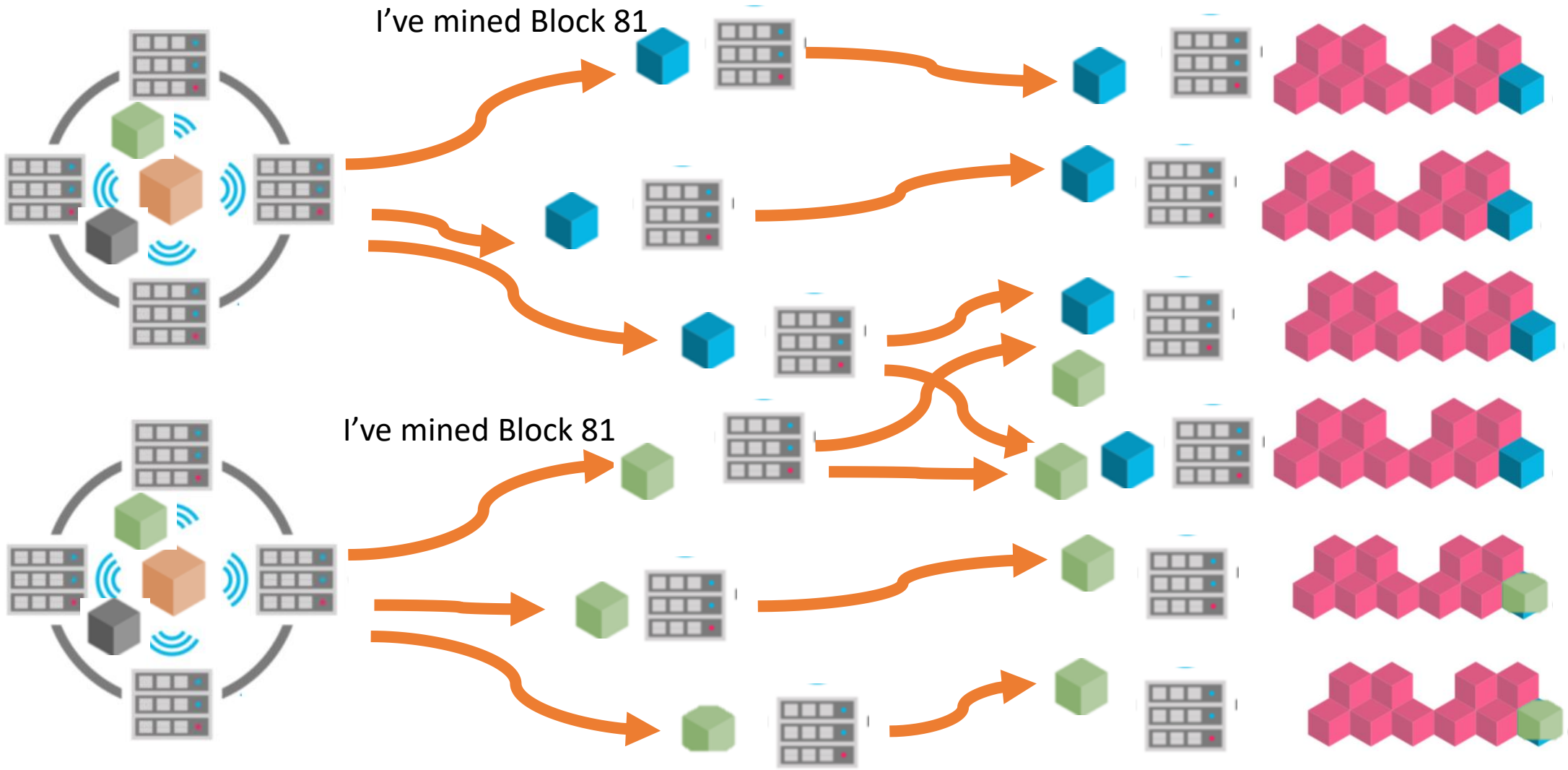
Winning miner broadcasts block to set of other miners who check solution and re-broadcast it



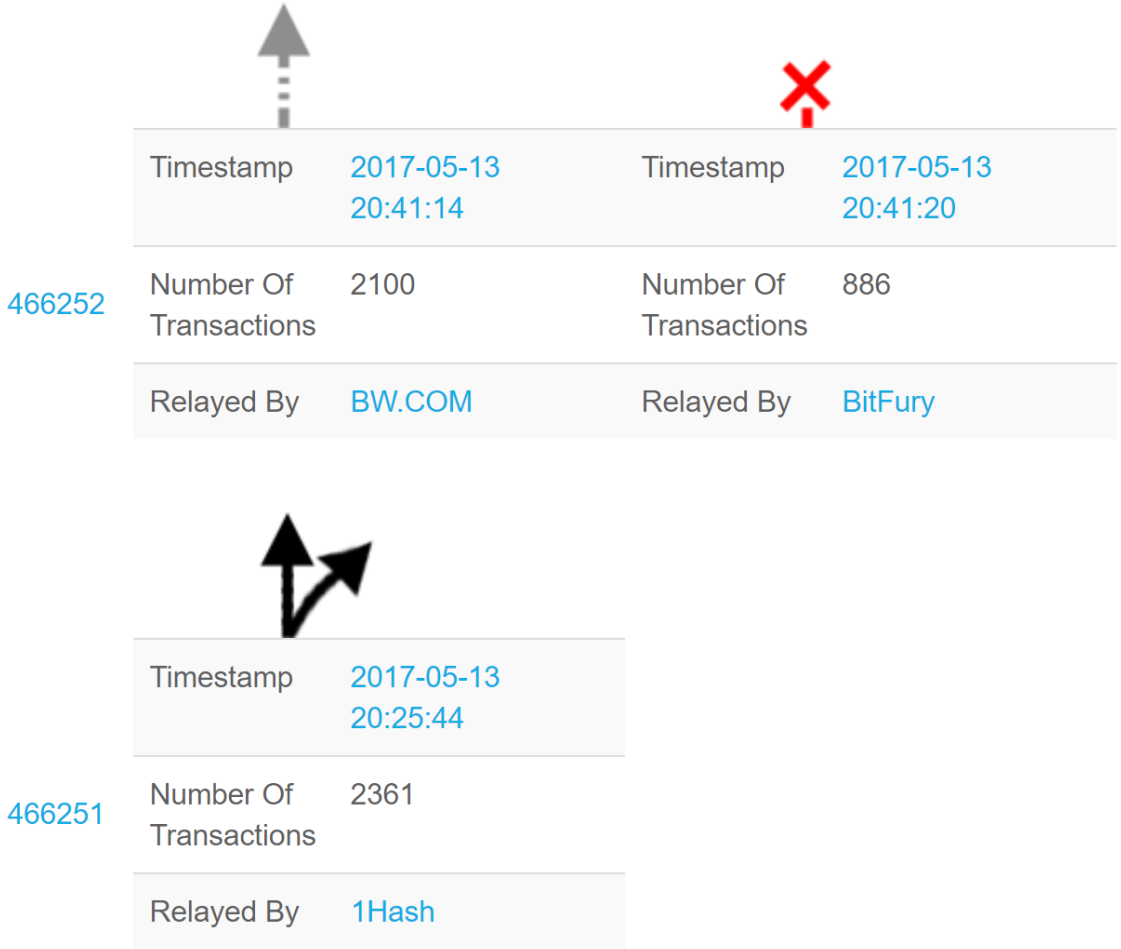
Mining a Block Workflow



Two mining pools produce different blocks at similar time

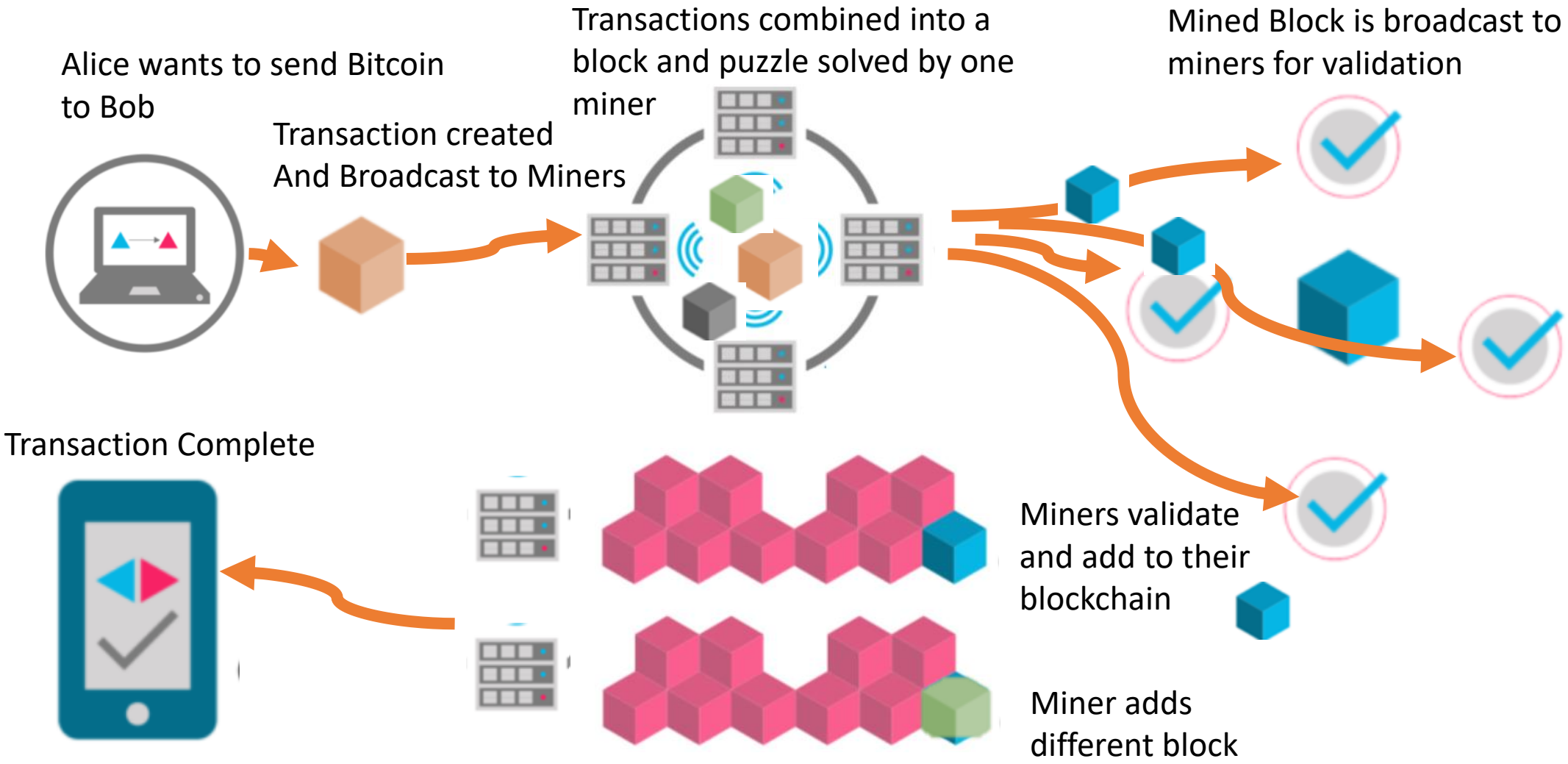


Two blocks mined at almost same time – actual Ethereum



"orphaned" block

Blockchain Consensus in BitCoin



Ethereum Wallet

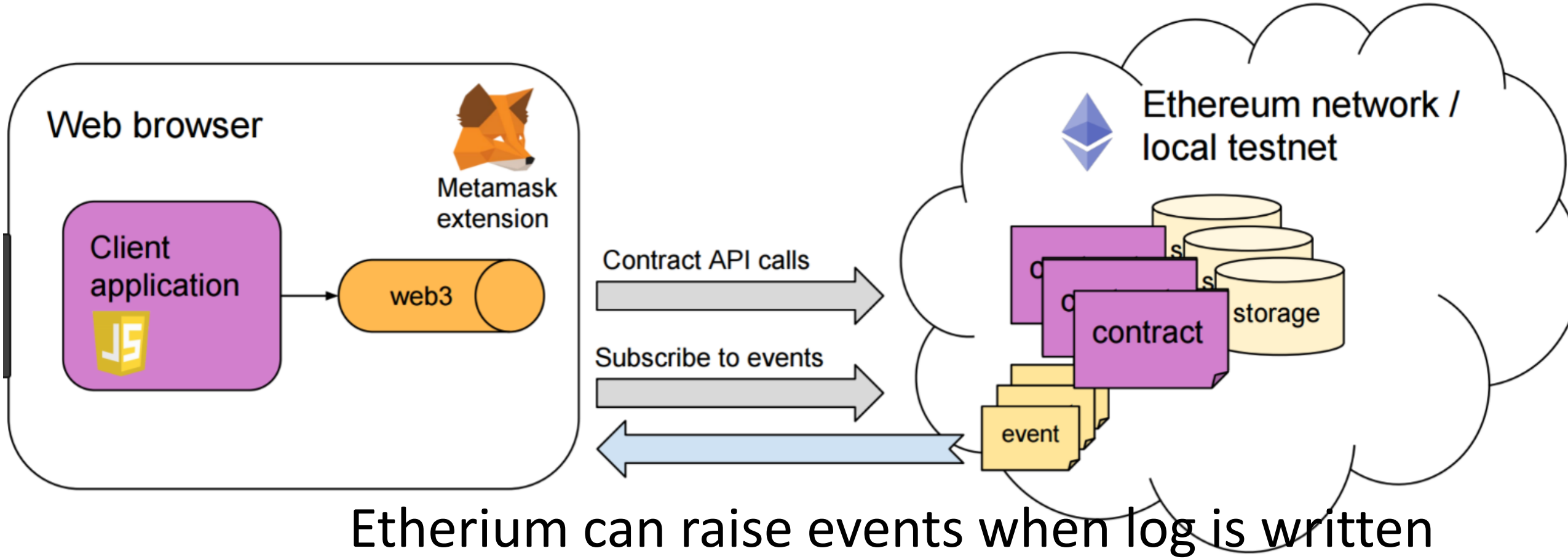
Address — *0x16E0022b17B...*

Balance — *0 Ether*

State

Logs – changes are logged and events raised

Client’s apps can monitor events



Etherium can raise events when log is written