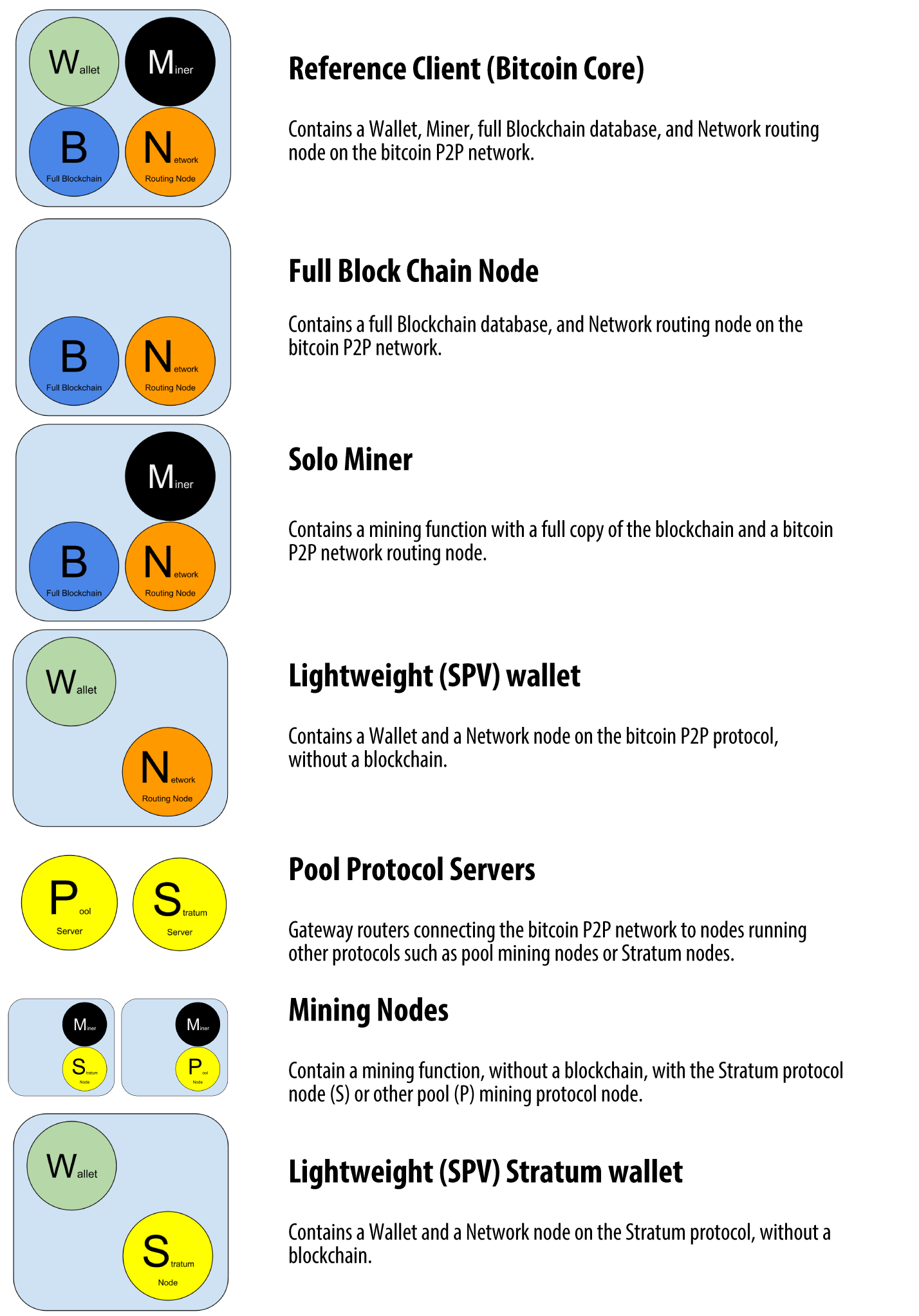
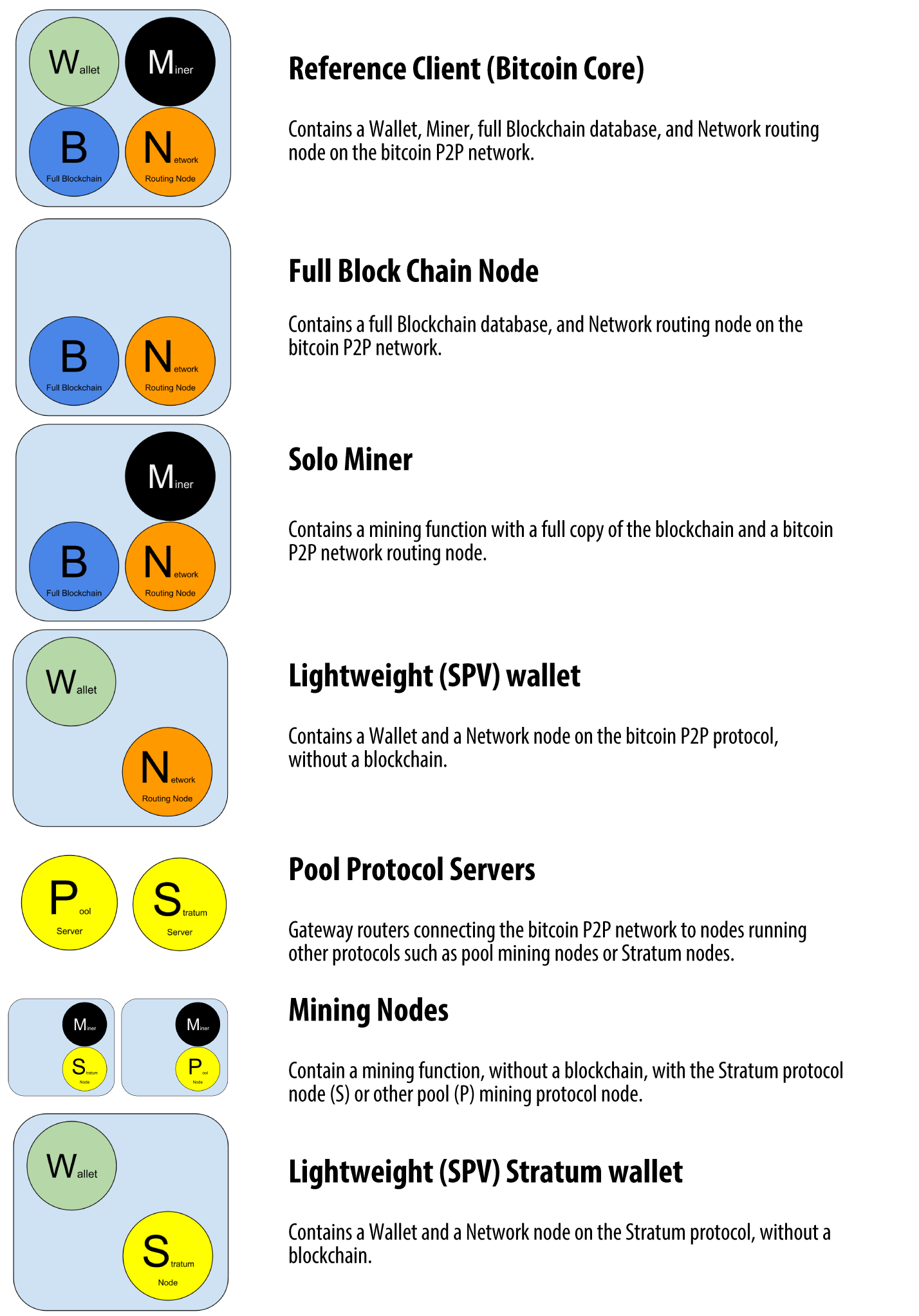
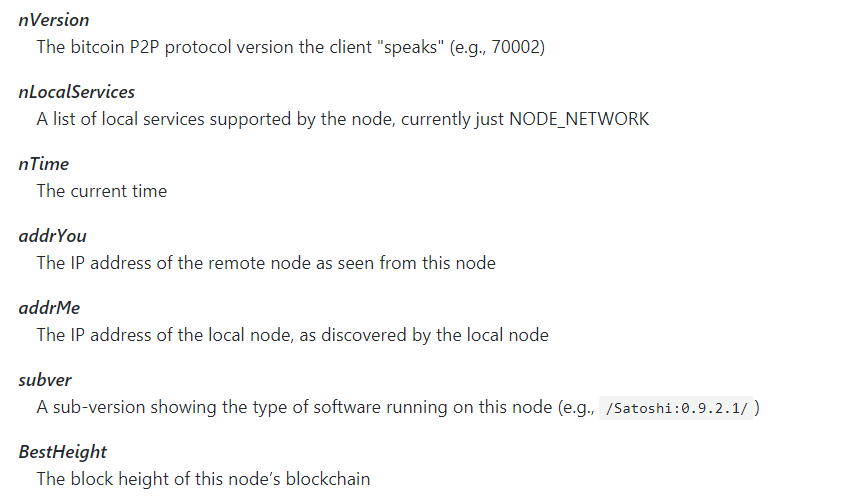
**The Bitcoin Network**

**Outlines**

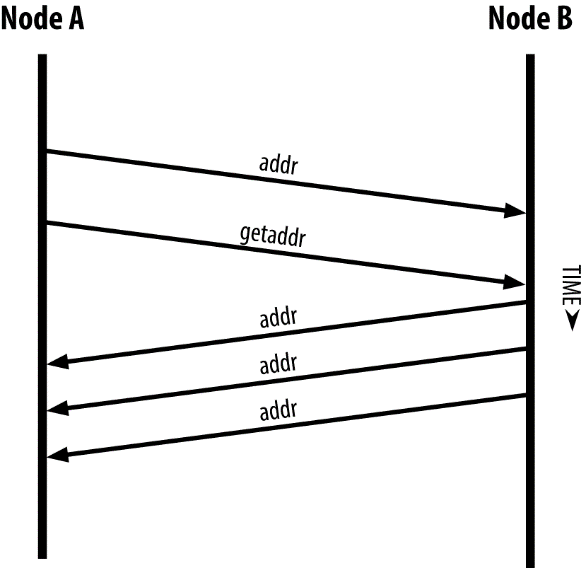
1. Peer-to-Peer Network Architecture
2. No special node, all are equal.
3. P2P protocol
4. Node
5. Wallet (W)
6. Miner (M): solve Proof-of-Work algorithm
7. Full Blockchain (B)
8. Routing Network (N)
9. Full Node: maintain complete Blockchain
10. SPV: simplified payment verification, maintain a subset of the Blockchain.
11. Mining node:
12. Pool mining server and stratum server: node connecting subnodes.



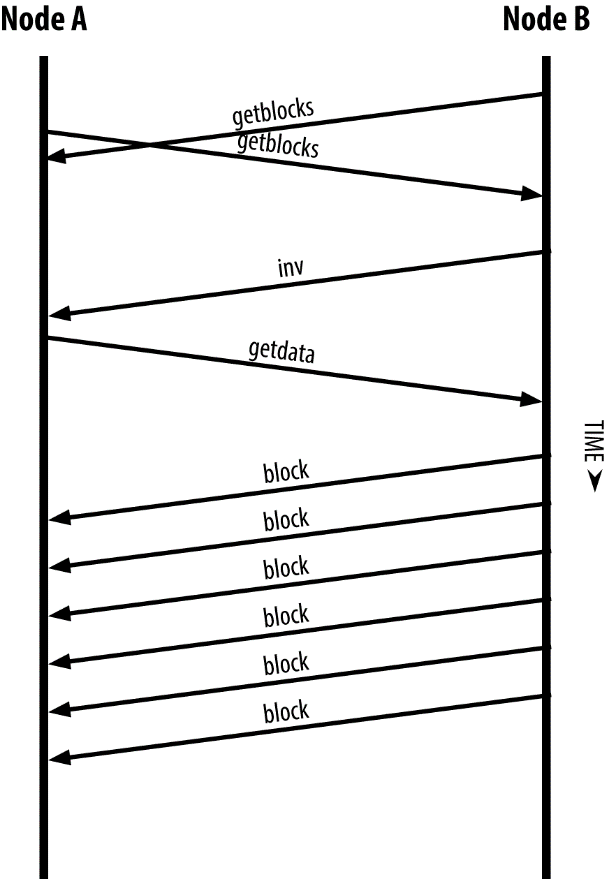
1. Network Discovery
2. Handshake message



1. Peer discovery: first to query DNS seeds, then bootstrap other peers



1. Full node can independently and authoritatively verify any transaction with reliance on any other node.(>100gb database)



1. Update Blockchain to the BestHeight every time connect to the network
2. Simplified Payment Verification Nodes
3. Lightweight client run on space- and power-constrained devices.
4. Download only the block header, not transactions (1000 times smaller)
5. Tourist analolgy: see article
6. Full nodes verify to the genesis block. SPV does not. (height vs depth)
7. Cannot verify a transaction does not exist (vulnerable to DDoS attack)
8. Random access to honest node. (vulnerable to network partitioning and Sybil attack)
9. Destroy User’s privacy (download only related headers)
10. Bloom Filters
11. Probabilistic search filter protects privacy.
12. Query a partial information

