The Bitcoin Network

Outlines

I. Peer-to-Peer Network Architecture

   A. No special node, all are equal.

   B. P2P protocol

II. Node

   A. Wallet (W)

   B. Miner (M): solve Proof-of-Work algorithm

   C. Full Blockchain (B)

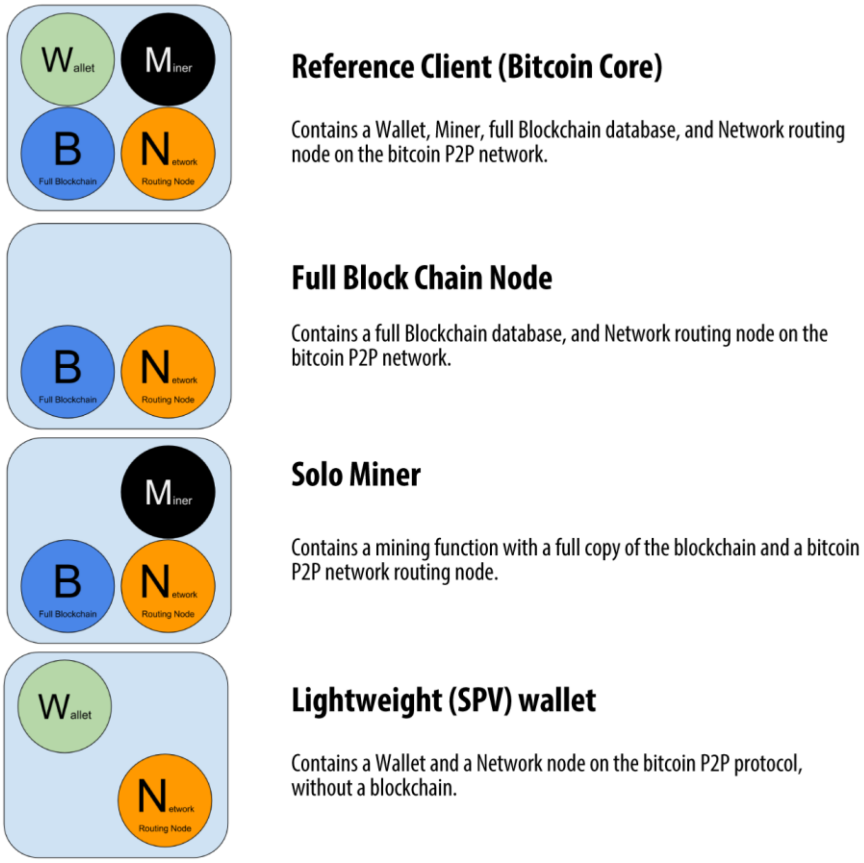
   D. Routing Network (N)

   E. Full Node: maintain complete Blockchain

   F. SPV: simplified payment verification, maintain a subset of the Blockchain.

   G. Mining node:

   H. Pool mining server and stratum server: node connecting subnodes.



Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.

Full Block Chain Node

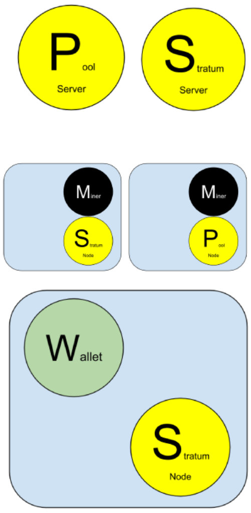
Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.

Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.

Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.



Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.

Mining Nodes

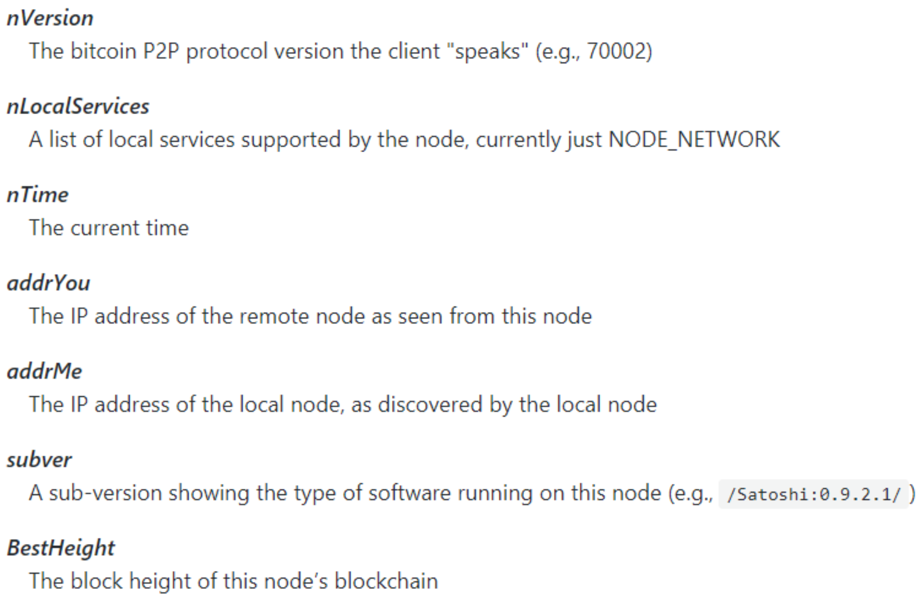
Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.

Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

III. Network Discovery

A. Handshake message



nVersion
The bitcoin P2P protocol version the client "speaks" (e.g., 70002)

nLocalServices
A list of local services supported by the node, currently just NODE_NETWORK

nTime
The current time

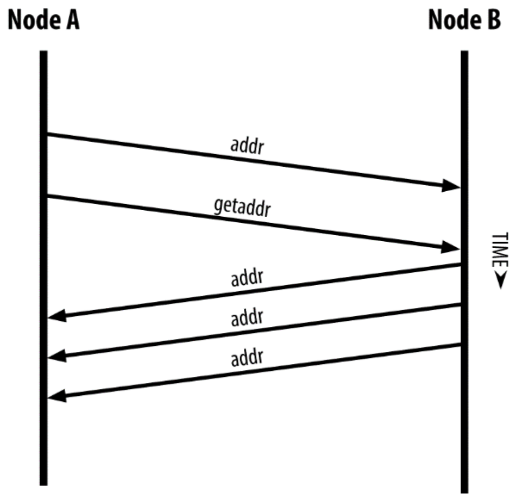
addrYou
The IP address of the remote node as seen from this node

addrMe
The IP address of the local node, as discovered by the local node

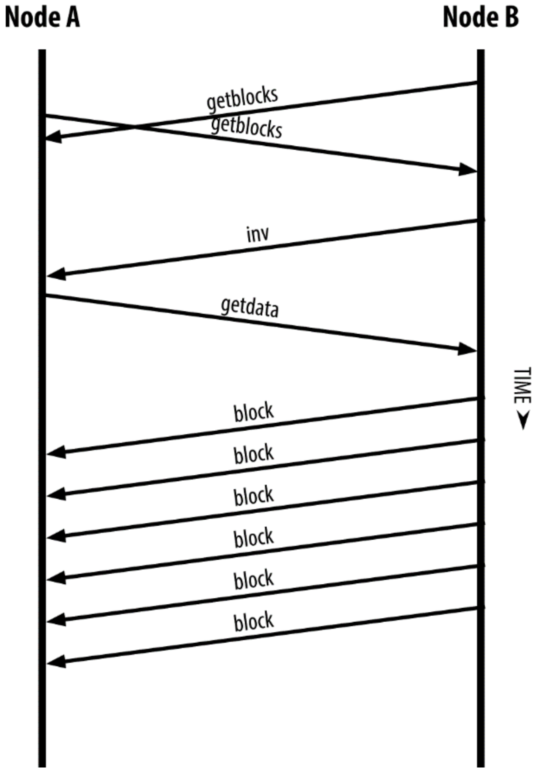
subver
A sub-version showing the type of software running on this node (e.g., `/Satoshi:0.9.2.1/`)

BestHeight
The block height of this node’s blockchain

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



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



D. Update Blockchain to the BestHeight eveytime connect to the network

IV. Simplified Payment Verification Nodes

A. Lightweight client run on space- and power-constrained devices.

B. Download only the block header, not transactions (1000 times smaller)

C. Tourist analolgy: see article

D. Full nodes verify to the genesis block. SPV does not. (height vs depth)

E. Cannot verify a transaction does not exist (vulnerable to DDoS attack)

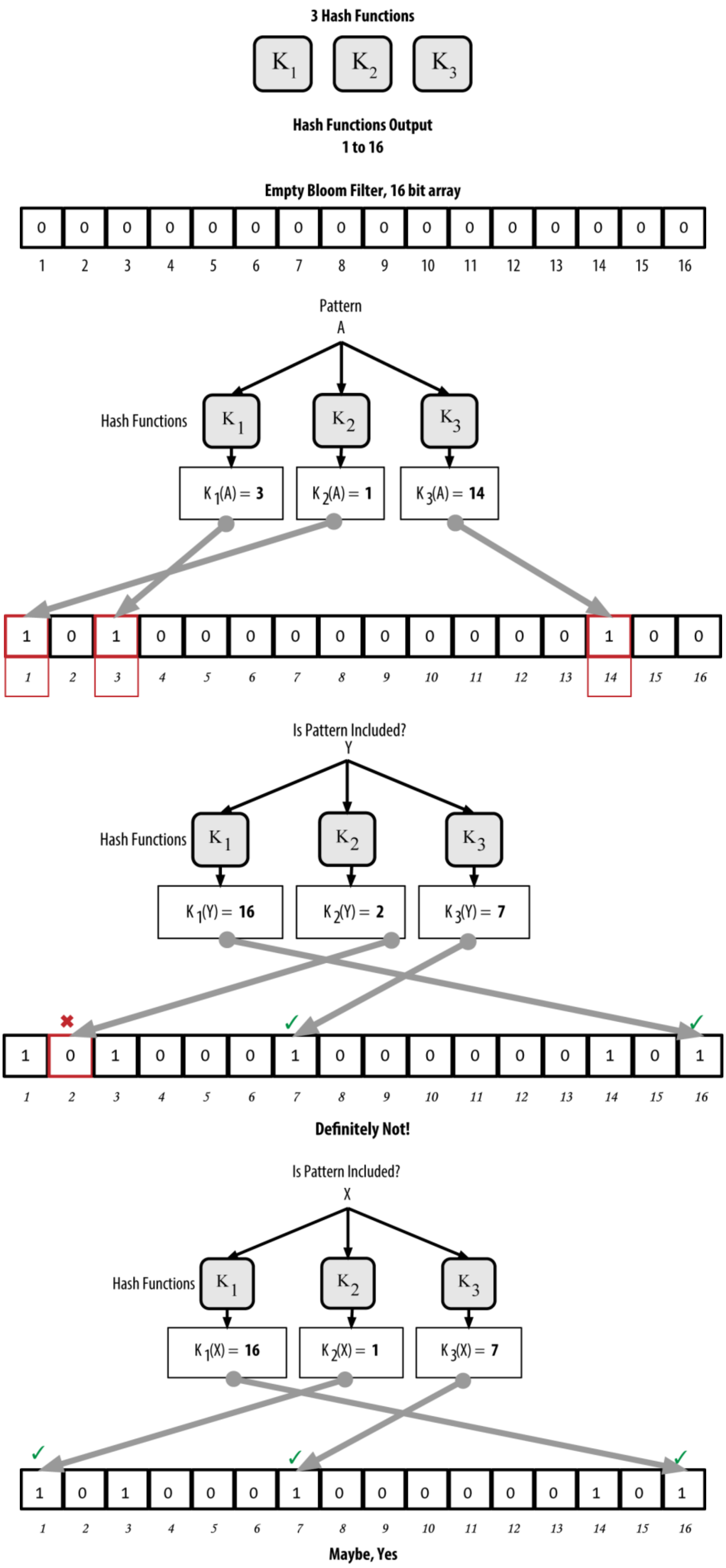
F. Random access to honest node. (vulnerable to network partitioning and Sybil attack)

G. Destroy User’s privacy (download only related headers)

V. Bloom Filters

A. Probabilistic search filter protects privacy.

B. Query a partial information


3 Hash Functions
K1
K2
K3
Hash Functions Output
1 to 16
Empty Bloom Filter, 16 bit array
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Pattern
A
Hash Functions
K1
K2
K3
K1(A) = 3
K2(A) = 1
K3(A) = 14
1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Is Pattern Included?
Y
Hash Functions
K1
K2
K3
K1(Y) = 16
K2(Y) = 2
K3(Y) = 7
✖
✓
✓
1 0 1 0 0 0 1 0 0 0 0 0 0 1 0 1
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Definitely Not!
Is Pattern Included?
X
Hash Functions
K1
K2
K3
K1(X) = 16
K2(X) = 1
K3(X) = 7
✓
✓
✓
1 0 1 0 0 0 1 0 0 0 0 0 0 1 0 1
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Maybe, Yes