Mechanics of Bitcoin (3)

Bitcoin Network

Prof. James Won-Ki Hong

Distributed Processing and Network Management (DPNM) Lab.
Dept. of Computer Science and Engineering
POSTECH
Pohang, Korea

http://dpnm.postech.ac.kr
jwkhong@postech.ac.kr

Table of Contents

Bitcoin Network (1/10)

Distribution of Global Bitcoin Nodes

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Sep 12 2018 14:11:09 GMT+0900 (Korean Standard Time).

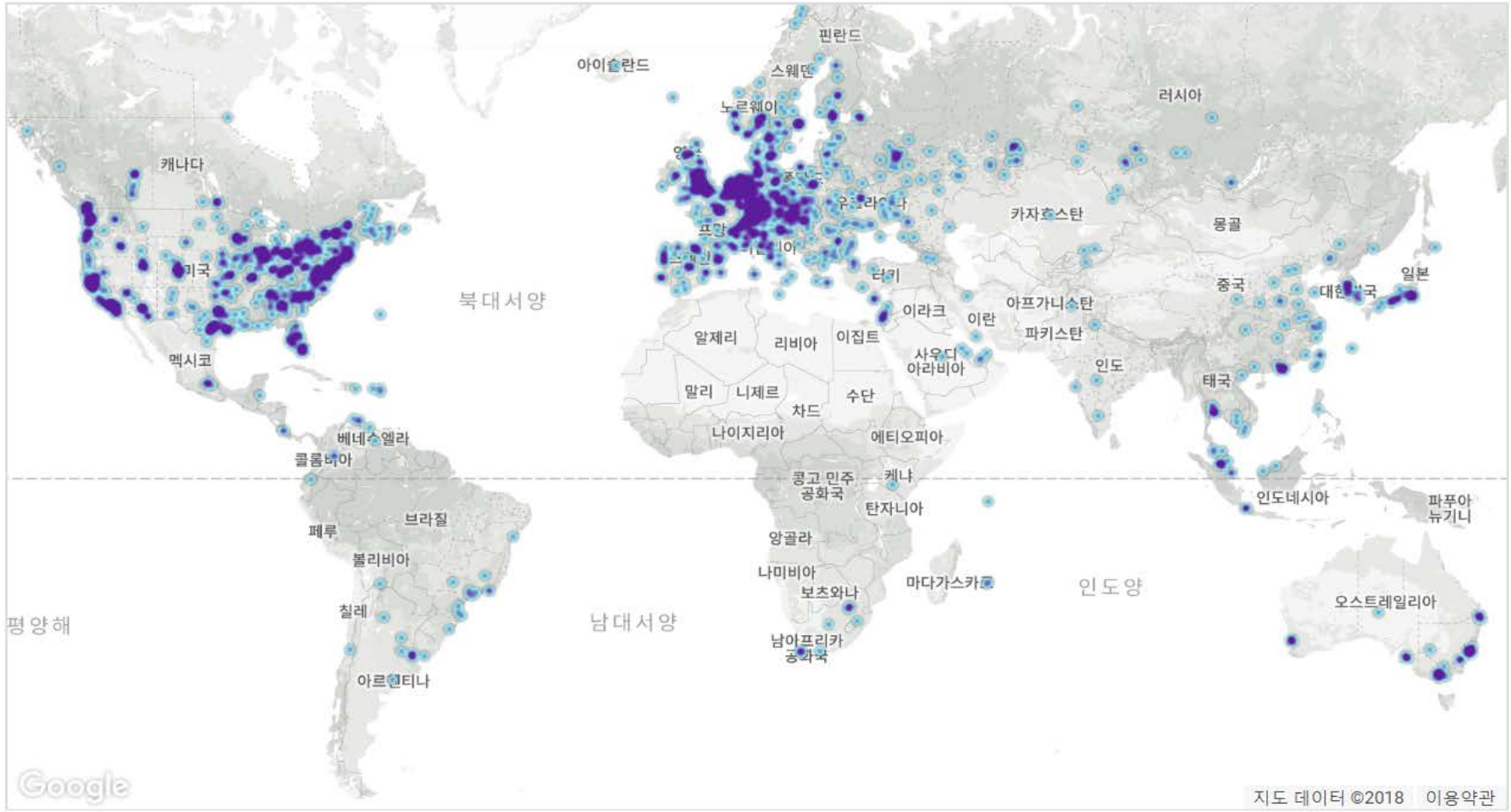
9705 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2301 (23.71%)
2	Germany	1859 (19.16%)
3	France	658 (6.78%)
4	China	642 (6.62%)
5	Netherlands	478 (4.93%)
6	n/a	458 (4.72%)
7	Canada	361 (3.72%)
8	United Kingdom	285 (2.94%)
9	Russian Federation	256 (2.64%)
10	Singapore	251 (2.59%)

More (97) »



https://bitnodes.earn.com/

Bitcoin Network (2/10)

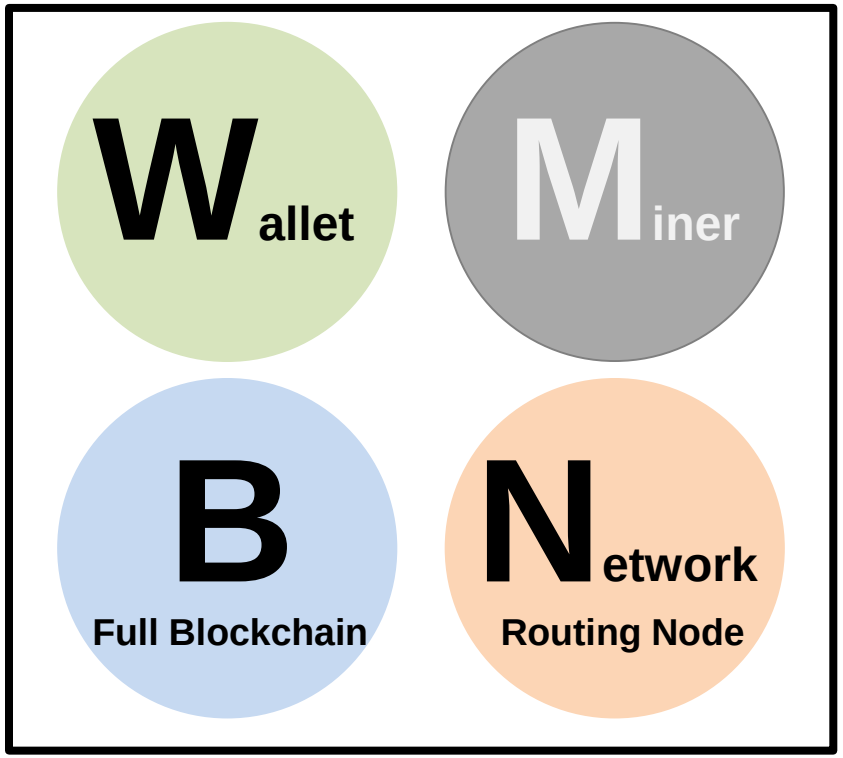
- **Peer-to-Peer Network (P2P) Architecture**
  - All nodes participating in the network have equal status
  - All nodes share the role of supplying the network service
- **Bitcoin Network**
  - Electronic money system of the P2P system
  - It can be implemented and maintained only on an equal and decentralized P2P aggregation network
- **Expanded Bitcoin Network**
  - Include **Bitcoin P2P protocol** / **Pool mining protocol** / **Stratum protocol** …

Bitcoin Network (3/10)

- **Types and roles of Nodes**

User wallets running on devices with resource constraints such as smart phone are becoming SPV (Simple Payment Verification) **nodes**

Data base function of full node. It has a copy of entire blockchain



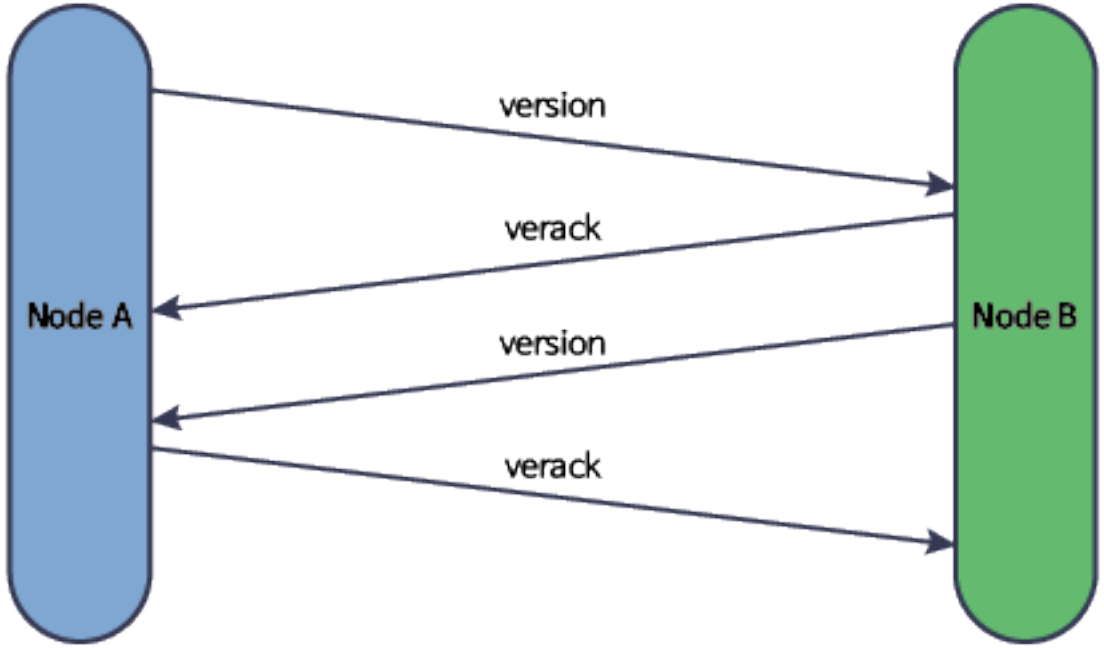
The mining node runs dedicated machine to run the PoW Algorithm and compete with other nodes to create a new block

Every node verifies and propagates transactions and blocks, and maintains connections with neighboring nodes

Bitcoin Network (4/10)

Network Discovery (1) – Discovery

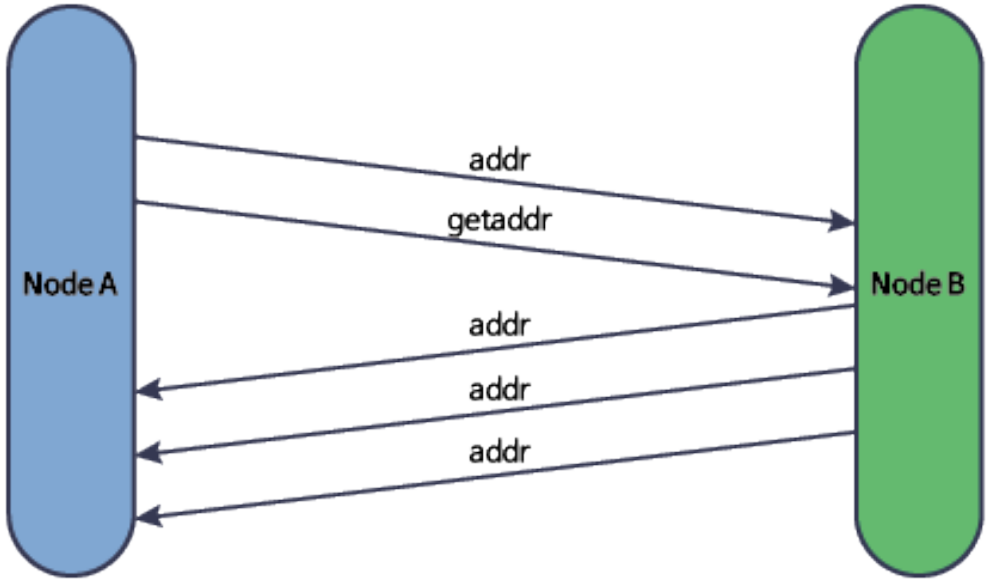
- A new node must discover other bitcoin nodes on the network and connect to it
  - At least one existing node
- Geographic location of the other nodes is not important
  - Network topology is not geographically defined
  - Any existing Bitcoin node can be selected **at random**



Initial handshake

Bitcoin Network (5/10)

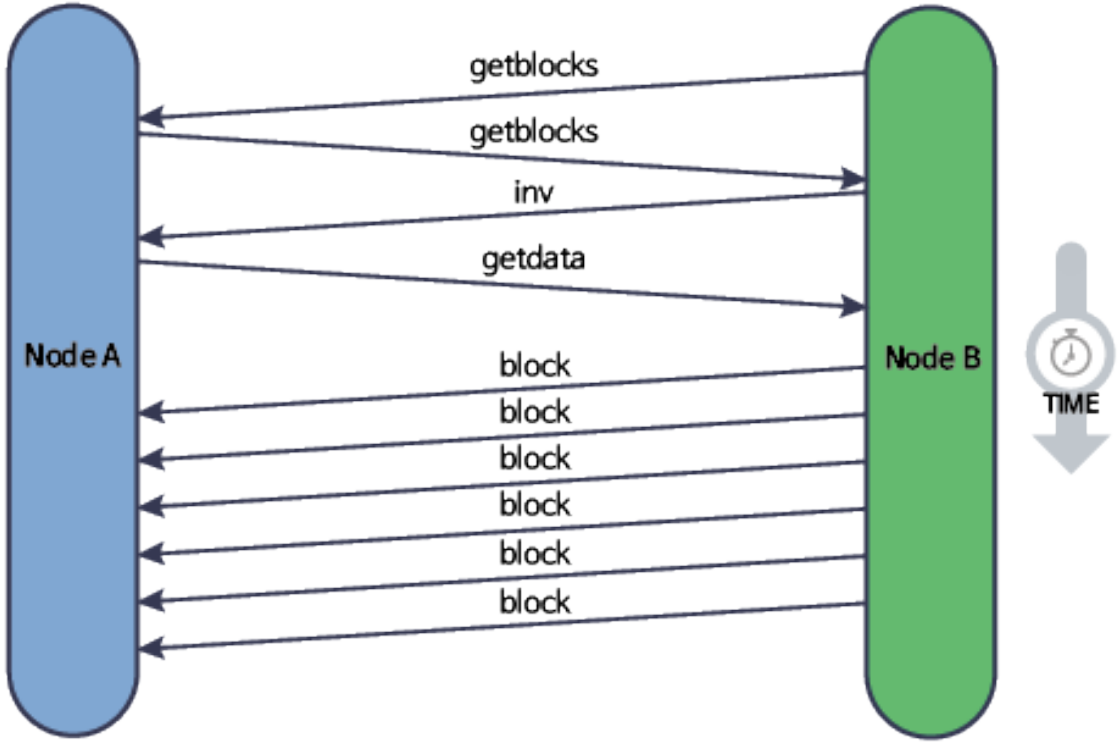
- **Network Discovery (2) – After the connection**
  - New node will send an **addr** and then **getaddr** to its neighbors
    - **addr:** Contain its own IP address
    - **getaddr**: Ask its neighbors to return a list of IP addresses of other peers
  - A node must connect to a few different peers to establish diverse paths
  - A node will remember its most recent successful peer connection
    - To quickly reestablish connections with its former peer network



Address Propagation

Bitcoin Network (6/10)

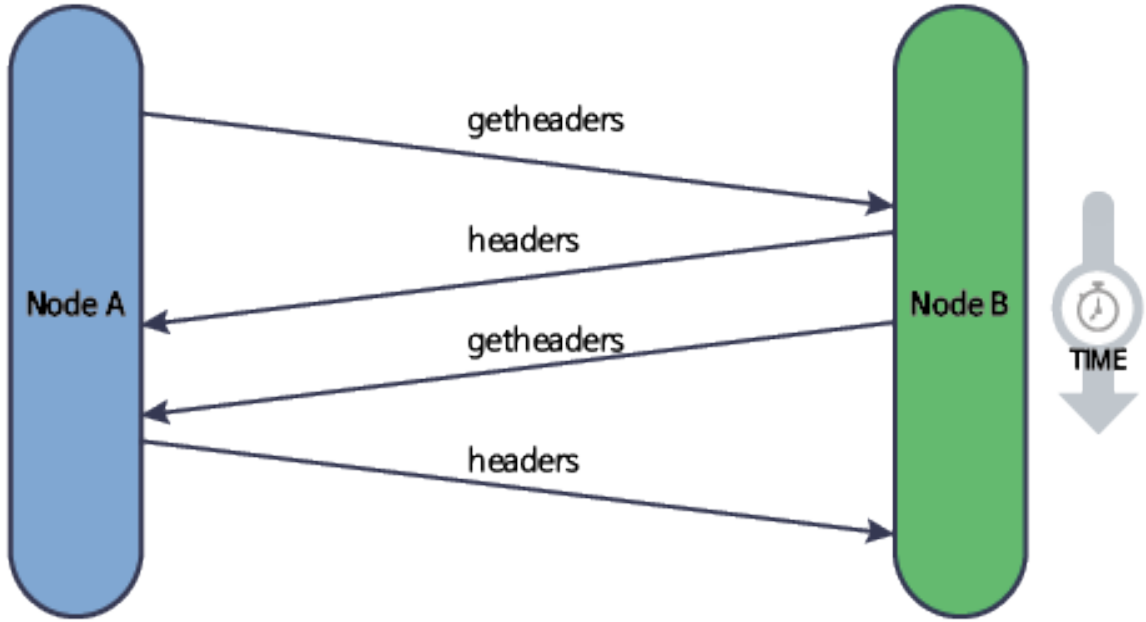
- **Full Node**
  - Maintain a complete and up-to-date copy of the bitcoin with all the transactions
  - Independently build and verify transactions
    - Starting from the first block to the latest known block in the network
    - Plus, for updates about new blocks of transactions
  - The first thing a full node will do is to construct a complete blockchain



Synchronizing the blocks

Bitcoin Network (7/10)

- **Simplified Payment Verification (SPV) Node**
  - Operate itself without storing the full blockchain
    - For space- and power-constrained devices
  - Download only the block headers
    - Do not download the transactions included in each block
    - 1,000 times smaller than the full blockchain
  - Verify transactions
    - Peers provide partial views of relevant parts of the blockchain with SPV node on demand



Synchronizing the block headers

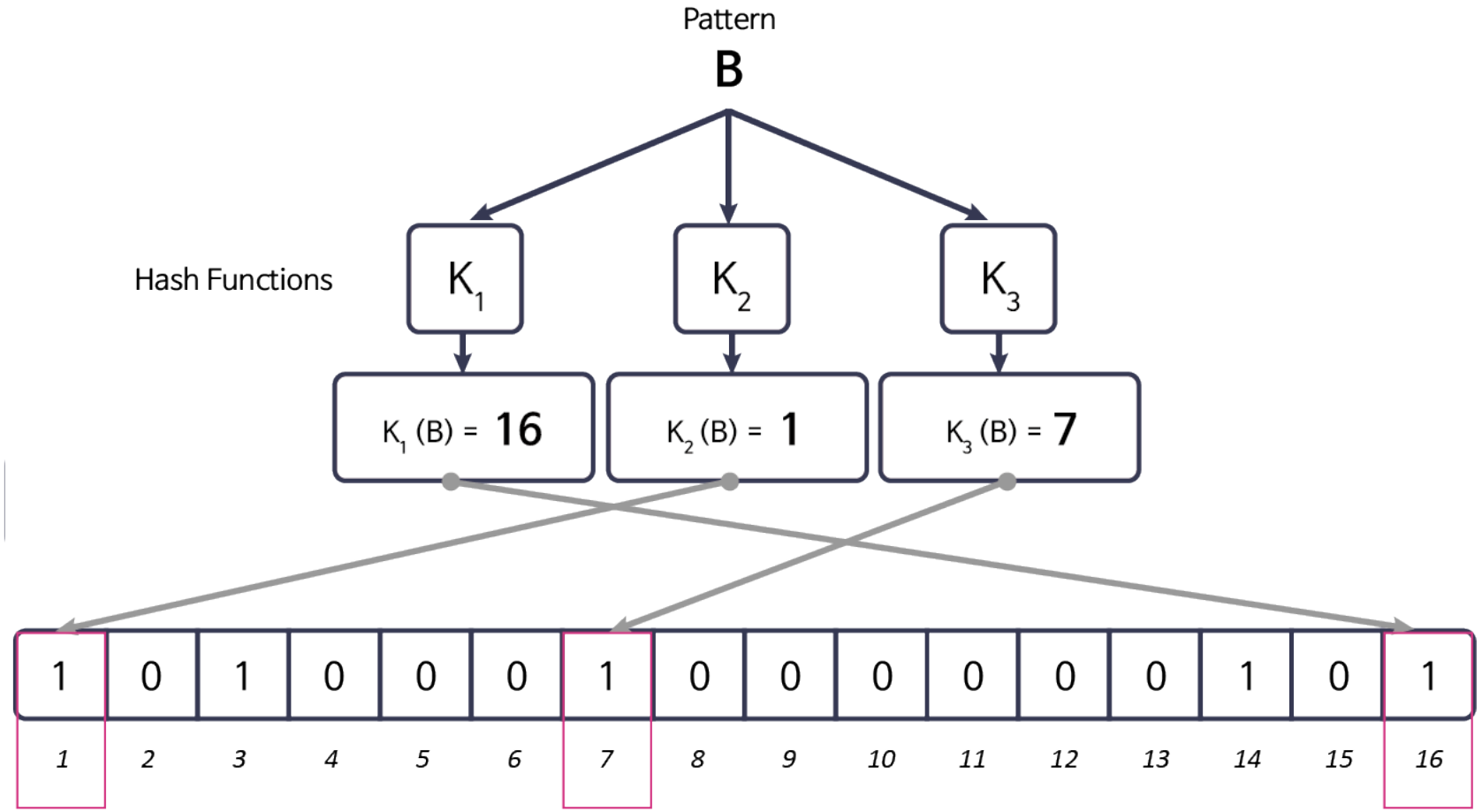
Bitcoin Network (8/10)

Bloom Filter (1)

- Uses Bloom filters to speed up wallet synchronization
- A probabilistic search filter
  - A way to describe a desired pattern without specifying it exactly
- Offer an efficient way to express a search pattern while protecting privacy
  - By asking their peers for matched transactions, without revealing exact addresses
- Allow an SPV node to specify a search pattern for transactions
  - Be able to be tuned towards **precision** or **privacy**
- Steps – for an SPV node
  1) Initializes a bloom filter as empty
  2) Make a list of all the addresses in its wallet
  3) Create a search pattern matching the transaction output
  3) Add each of the search patterns to the bloom filter
  4) Send the bloom filter to the peer

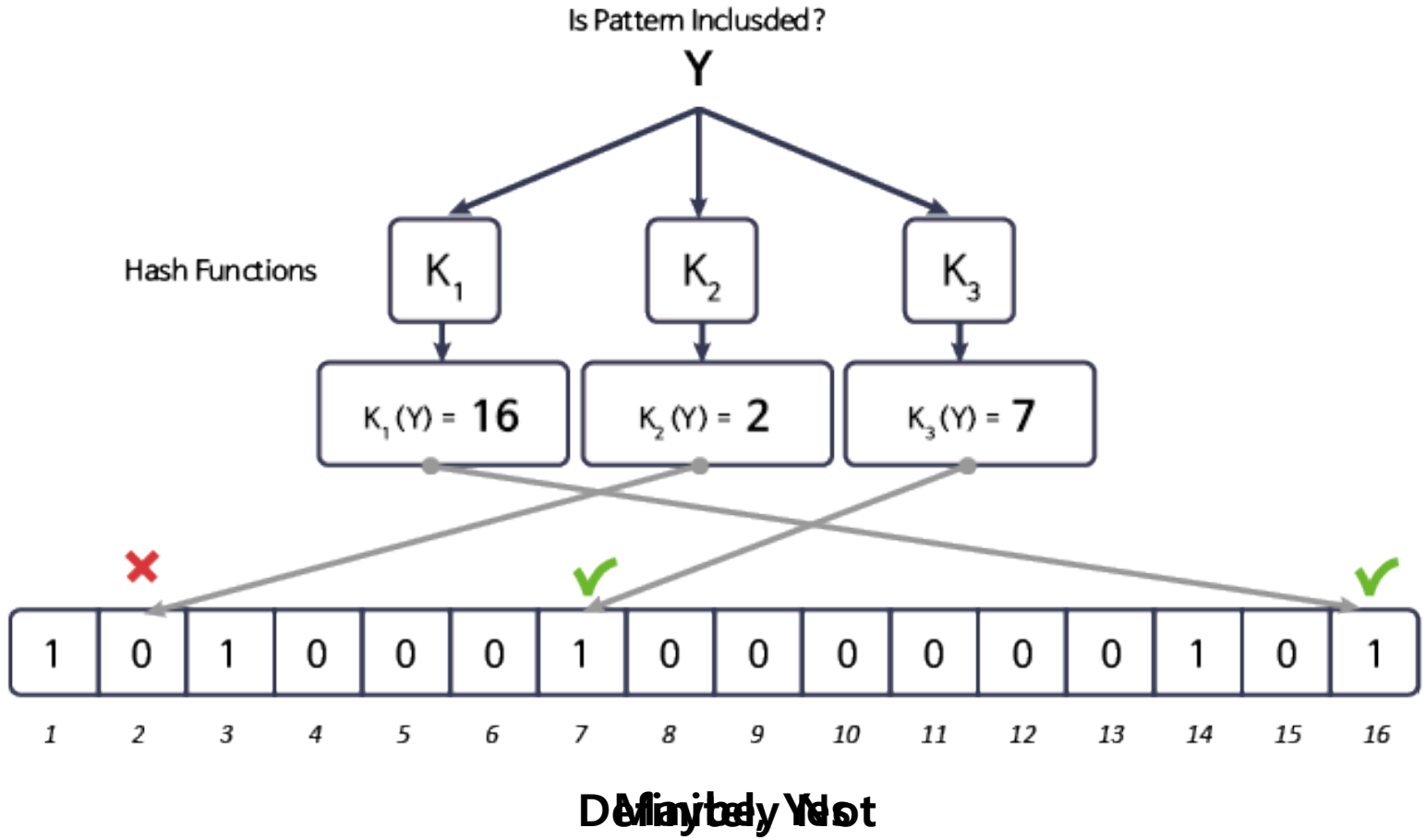
Bitcoin Network (9/10)

- **Bloom Filter (2) -** Adding a pattern “A”/“B” to the simple bloom filter
  - A simple bloom filter
    - 16 bit field and 3 hash functions



Bitcoin Network (10/10)

- **Bloom Filter (3) -** Testing the existence of pattern “X”/”Y” in the simple bloom filter



Summary

- **Bitcoin Network**
  - Peer-to-Peer Network (P2P) Architecture
  - Types and roles of Nodes
  - Network Discovery
  - Block / Header Synchronization
  - Bloom Filter

References

- Bitnodes, https://bitnodes.earn.com/
- Andreas M. Antonopoulos, **Mastering Bitcoin,** O'Reilly, 2014
- https://en.wikipedia.org/wiki/Bloom_filter