CSE446: Blockchain & Cryptocurrencies

Lecture – 7: Bitcoin-2

Agenda

- Bitcoin components
  - Users
  - Node & Network

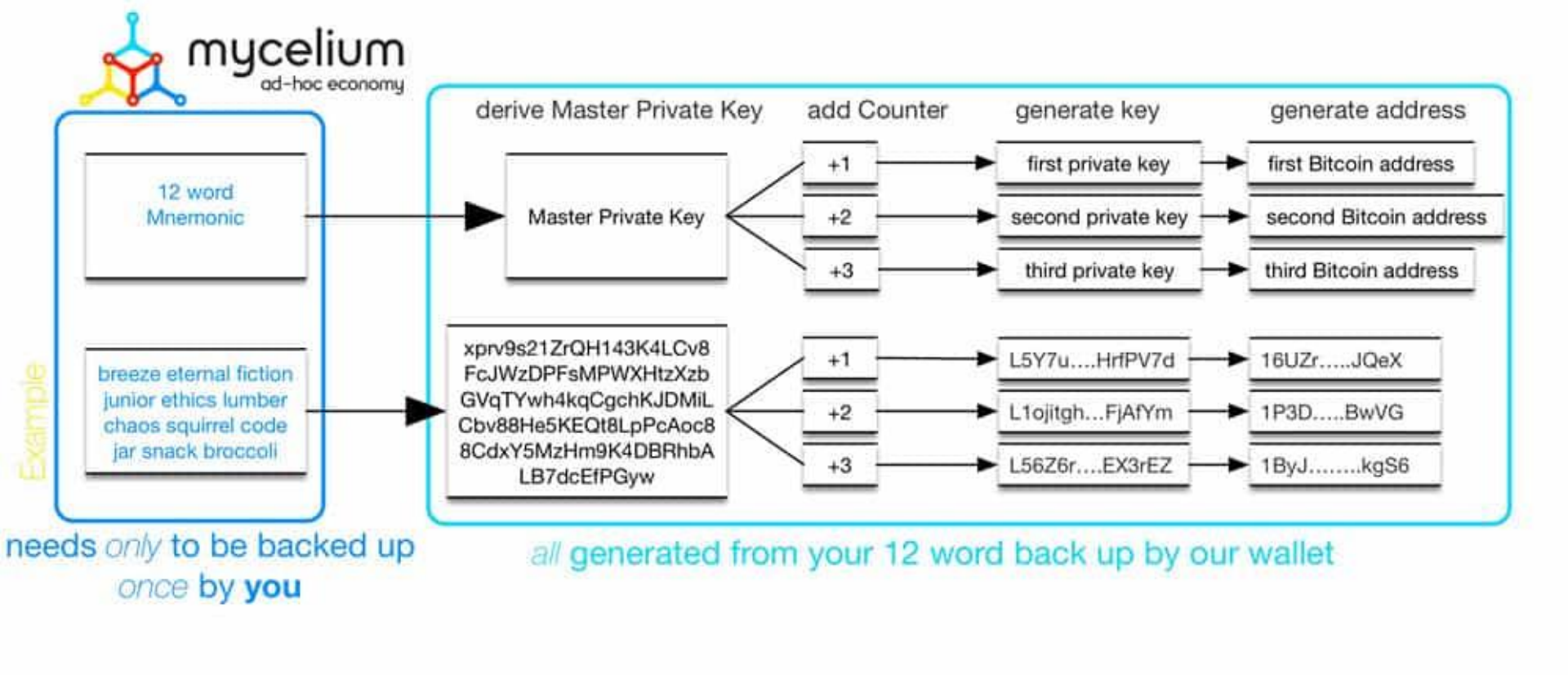
HD wallet

- A Hierarchical Deterministic (HD) is a key creation and transfer protocol which allows creating child keys from a parent key in a hierarchical way
  - Wallets using the HD protocol are called HD wallets
  - The single starting parent key is known as a seed
- The seed allows a user to easily back up and restore a wallet without needing any other information

HD wallet

- Seeds are typically serialised into human-readable words in a **Mnemonic** phrase
- A mnemonic phrase, mnemonic recovery phrase or mnemonic seed is a list of words which store all the information needed to recover a Bitcoin wallet
- Such Mnemonic words must be stored securely and must never be typed on any website

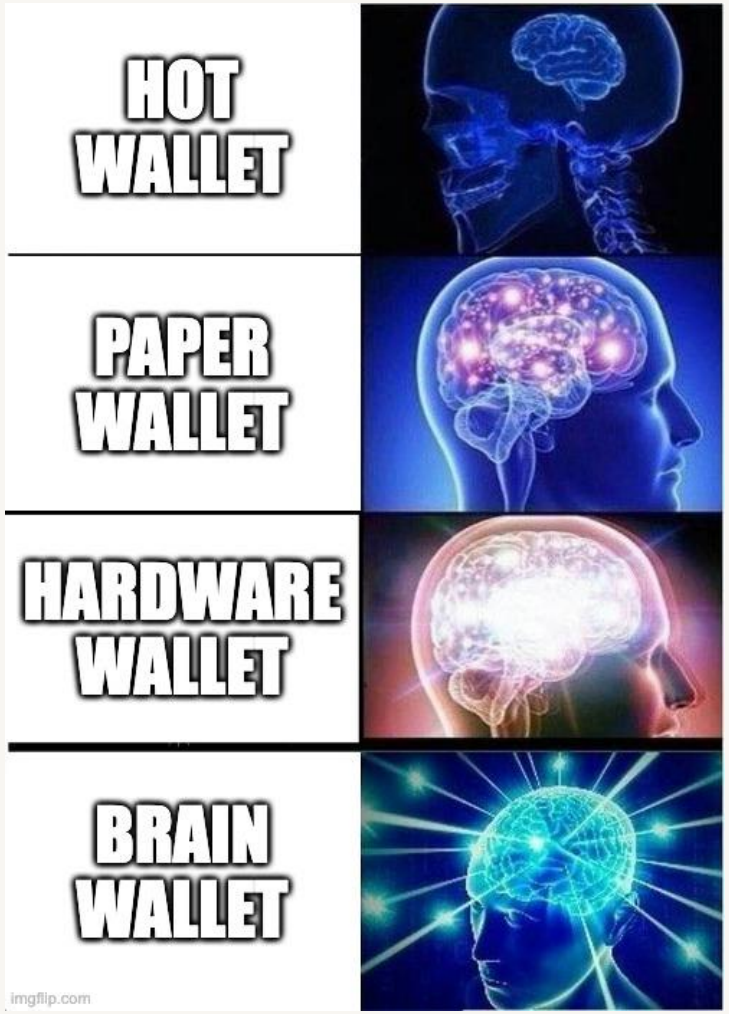
HD wallet



https://coinsutra.com/wp-content/uploads/2017/07/HD_Wallets.jpg

Brain wallet

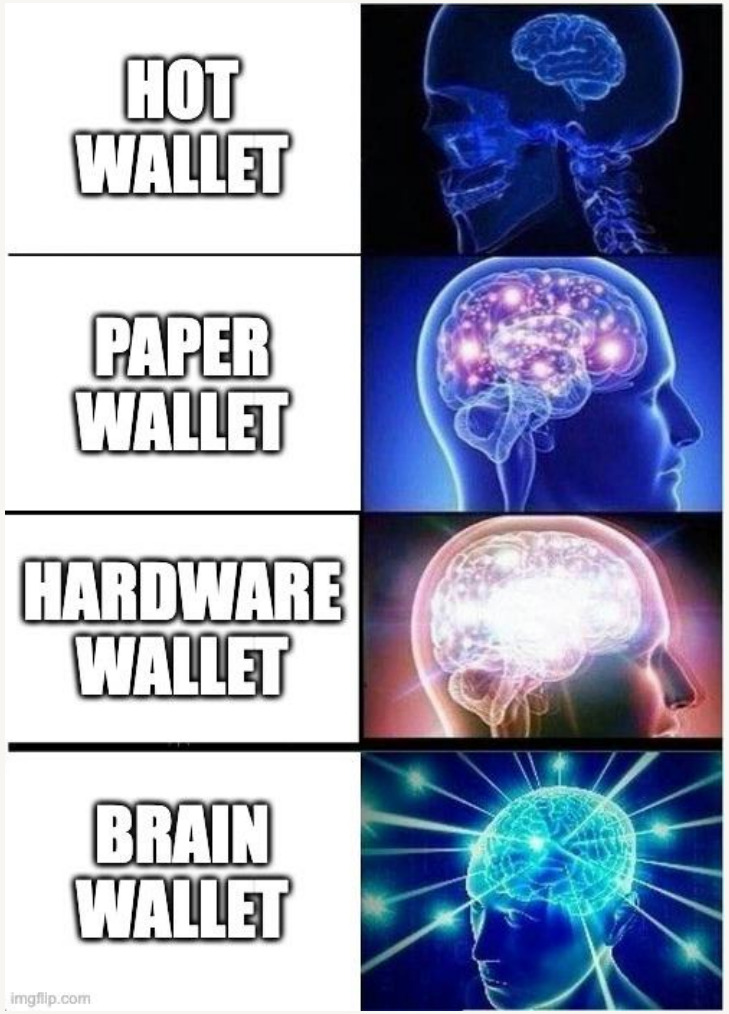
- A brain wallet refers to the concept of storing Bitcoin’s private key in one's own mind by memorising a seed phrase
- If the seed is not recorded anywhere, the Bitcoins can be thought of as being held only in the mind of the owner
- If a brain wallet is forgotten or the person dies or is permanently incapacitated, the Bitcoins are lost forever
- Using memory techniques allow them to be memorised and recalled easily



https://i.imgflip.com/6x41nq.jpg

Brain wallet

- Private keys will be generated from a seed (mnemonic words/passphrase)
- Use the passphrase to generate a private key
  - E.g. hashing the passphrase
- Then generate the public key from the private key using a standard algorithm
- The passphrase needs to be securely created, otherwise an adversary could easily guess
- If the passphrase is long, it will be difficult to memorise

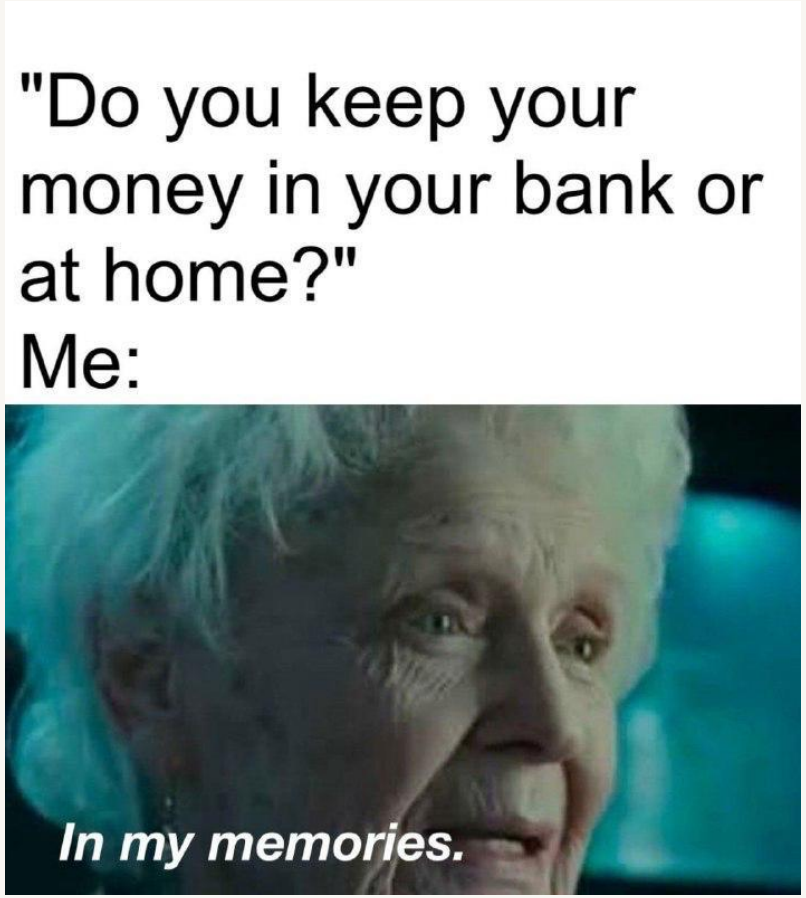


https://i.imgflip.com/6x41nq.jpg

Brain wallet

- To memorise a seed with this method you must invent a story which hits the words as "keynotes”
- Let the key phrases are the following
  - witch collapse practice feed shame open despair creek road again ice least
- “Imagine going through a room and seeing your sister dressed as a **witch**, playing the jenga boardgame until the tower **collapses** and so on”

Brain wallet



Custodial wallet

- Let other people / companies store your bitcoins / cryptocurrencies for you
- No access to the private key, coins can only be used through a certain interface / website
- Very common within most exchanges
  - The money is sent to the exchange, the account on the platform has now a new balance which can be traded or paid out
- However: Very dangerous!
- Many exchanges got hacked, users lost their funds. Be careful!

Bitcoin Node & Network

- All nodes are connected to a common p2p network
- Every node runs a bitcoin implementation (bitcoind, bcoin, etc.)
  - implementations are open source
- Anyone can freely join the network
- Nodes do not have to trust the network!
- Everybody assumes that neighbours may lie (byzantine behaviour)
- Every node receives messages, acts on them and passes these messages to its known neighbours according to protocols
  - malicious nodes can suppress messages and behave beyond protocols rules

Bitcoin Node & Network

REACHABLE BITCOIN NODES
Updated: Sun Nov 17 23:04:54 2024 +06

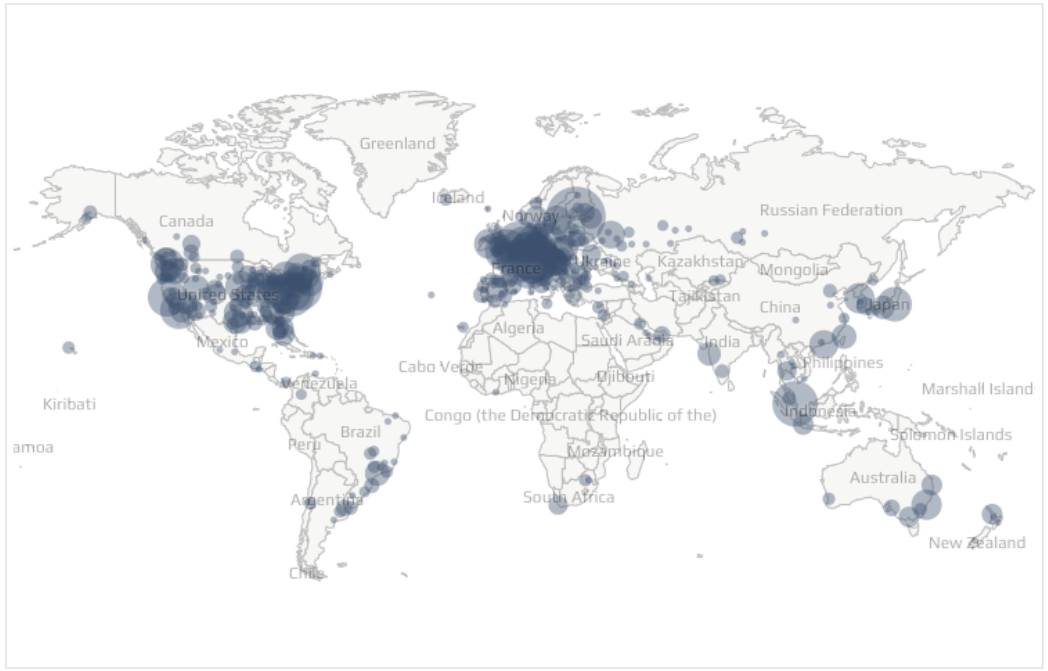
19657 NODES **CHARTS**

IPv4: +0.2% / IPv6: +7.2% / .onion: +3.7%

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

RANK	COUNTRY	NODES
1	n/a	12593 (64.06%)
2	United States	1963 (9.99%)
3	Germany	1288 (6.55%)
4	France	447 (2.27%)
5	Finland	380 (1.93%)
6	Netherlands	327 (1.66%)
7	Canada	267 (1.36%)
8	United Kingdom	207 (1.05%)
9	Switzerland	177 (0.90%)
10	Singapore	156 (0.79%)

All (93) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world. **LIVE MAP**

https://bitnodes.io/

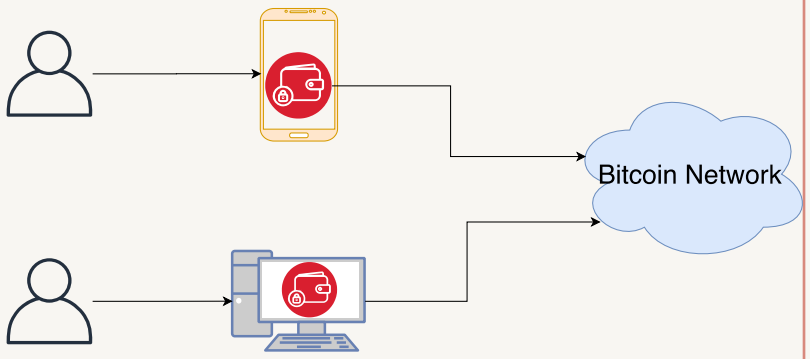
Live map available: https://bitnodes.io/nodes/live-map/

Bitcoin Node

- Bitcoin has four types of nodes:
  - Wallet node
  - Light node
  - Full node
  - Miner node

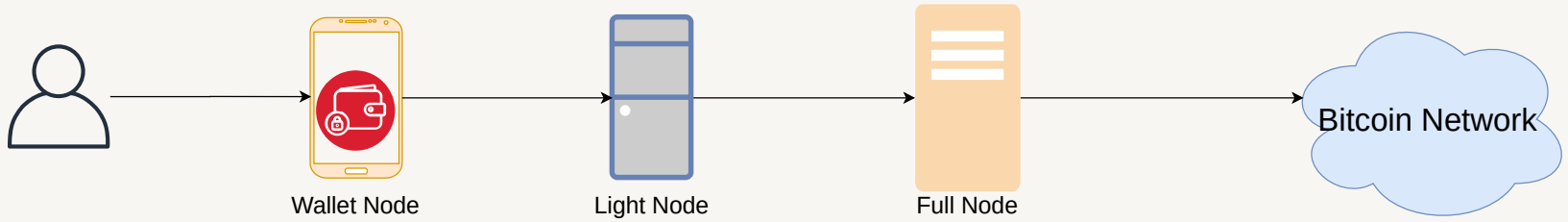
Bitcoin Node types: wallet node (user)

- The wallet owner owns different private keys
- He is the owner of all stored currencies on these addresses
- He sends money by signing and publishing new transactions to a connected light node, full node or miner node



Bitcoin Node types: light node (software)

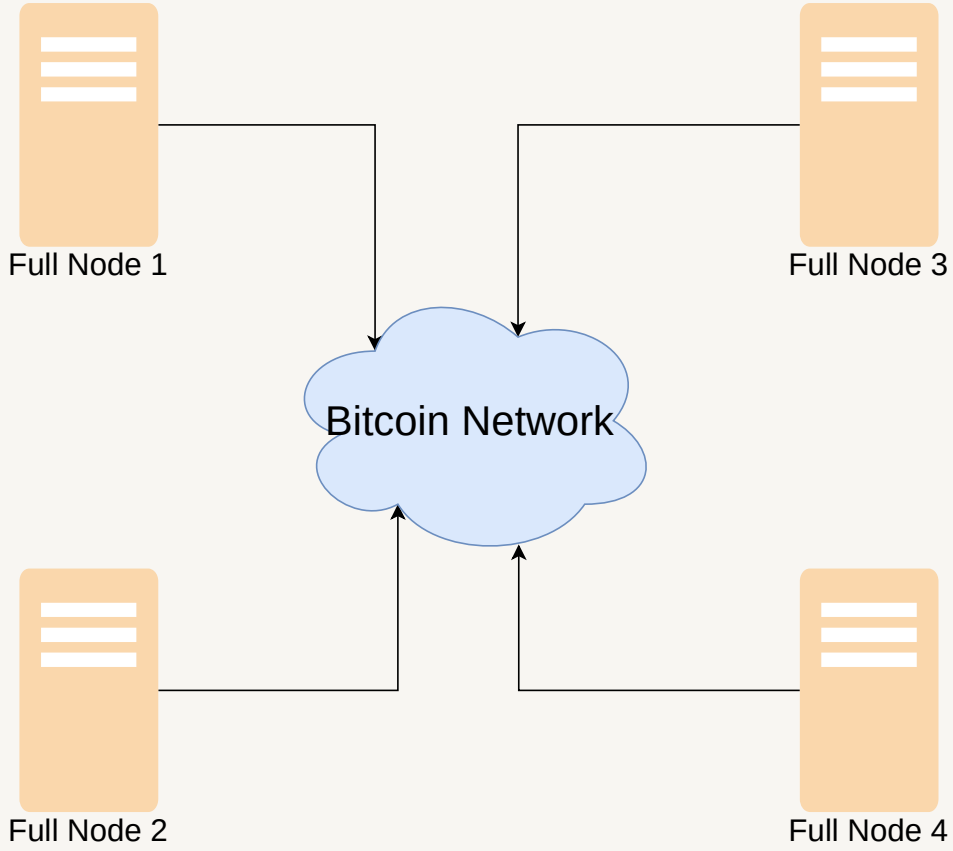
- The light node can act as a relay for transactions of one wallet owner
- It validates whether a single transaction of the wallet owner was executed correctly
- The light node also requires a full node to connect to the network
- Almost no relevance in practice today
- Today, centralised services are used to create transactions



Bitcoin Basics- Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Bitcoin Node types: full node (software)

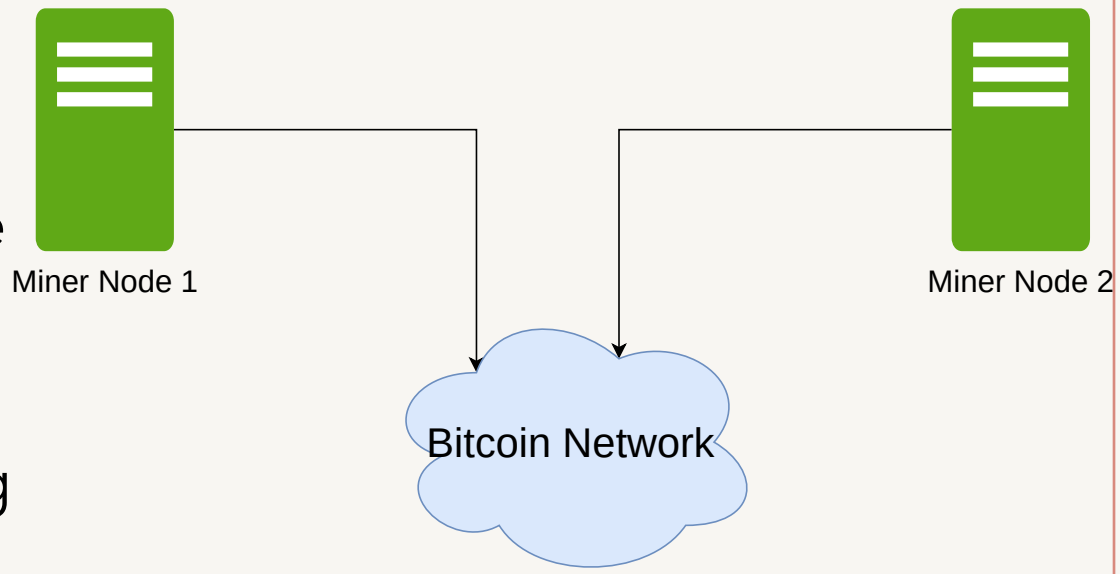
- The full node maintains the complete blockchain
- Its record of the chain is complete
  - it contains every single transaction and block until the genesis (first) block
- Is connected to other full nodes and exchanges information
- Namely:
  - Validates every transaction and block it receives
  - Relays all new transactions and blocks



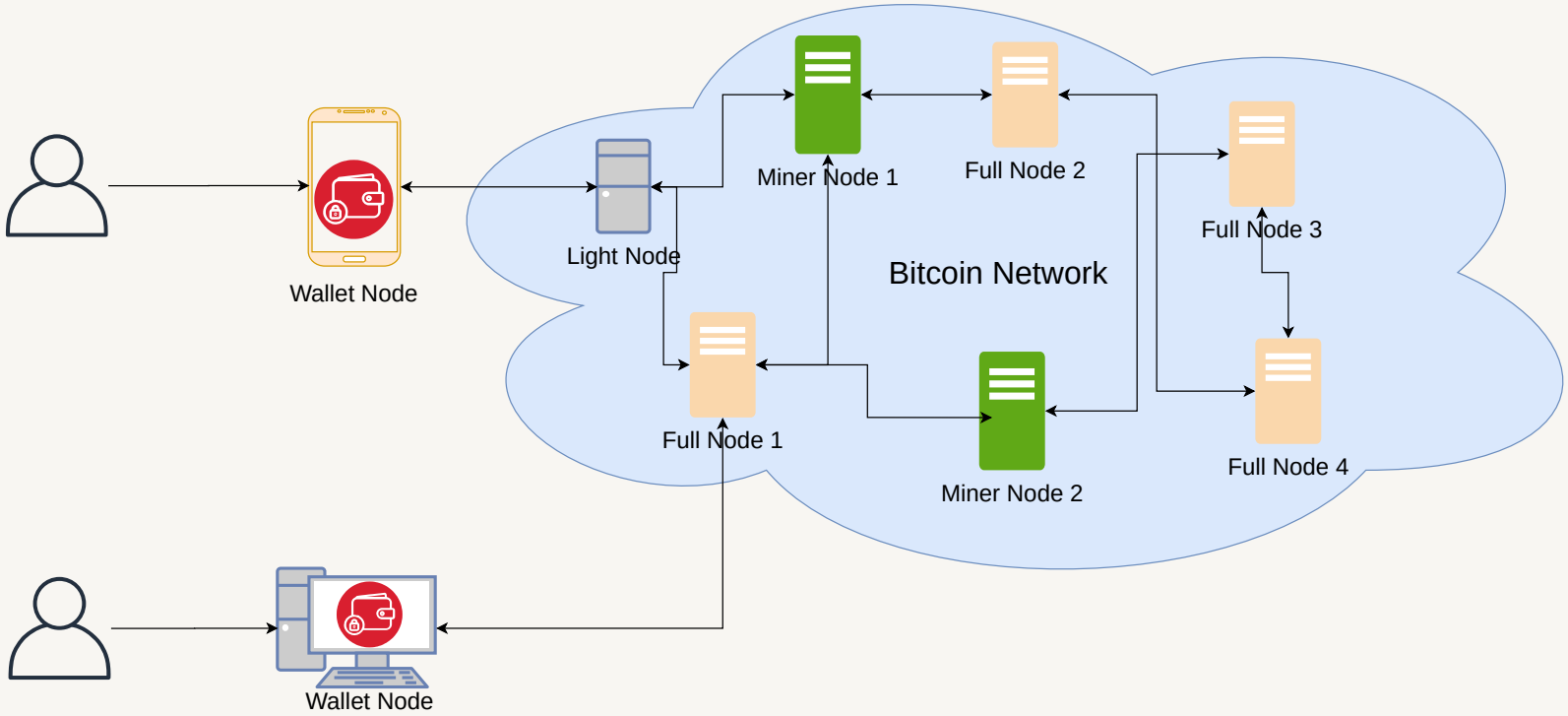
Bitcoin Basics- Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Bitcoin Node types: miner node (software)

- The miner needs the same record as a full node to work properly
- It also is connected with other nodes and maintains the network
- Additionally, the miner is responsible for creating new blocks by trying to solve the mining puzzle
- The miner gets rewarded for creating new blocks



Bitcoin network



Bitcoin P2P network

- Bitcoin nodes communicate in a decentralised fashion, meaning that no single entity or node is superior, all nodes are equal
  - Ad-hoc protocol (runs on TCP port 8333)
  - Ad-hoc network with random topology
- New nodes can join at any time
- Forget non-responding nodes after 3 hr

Bitcoin Basics- Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Bitcoin P2P network

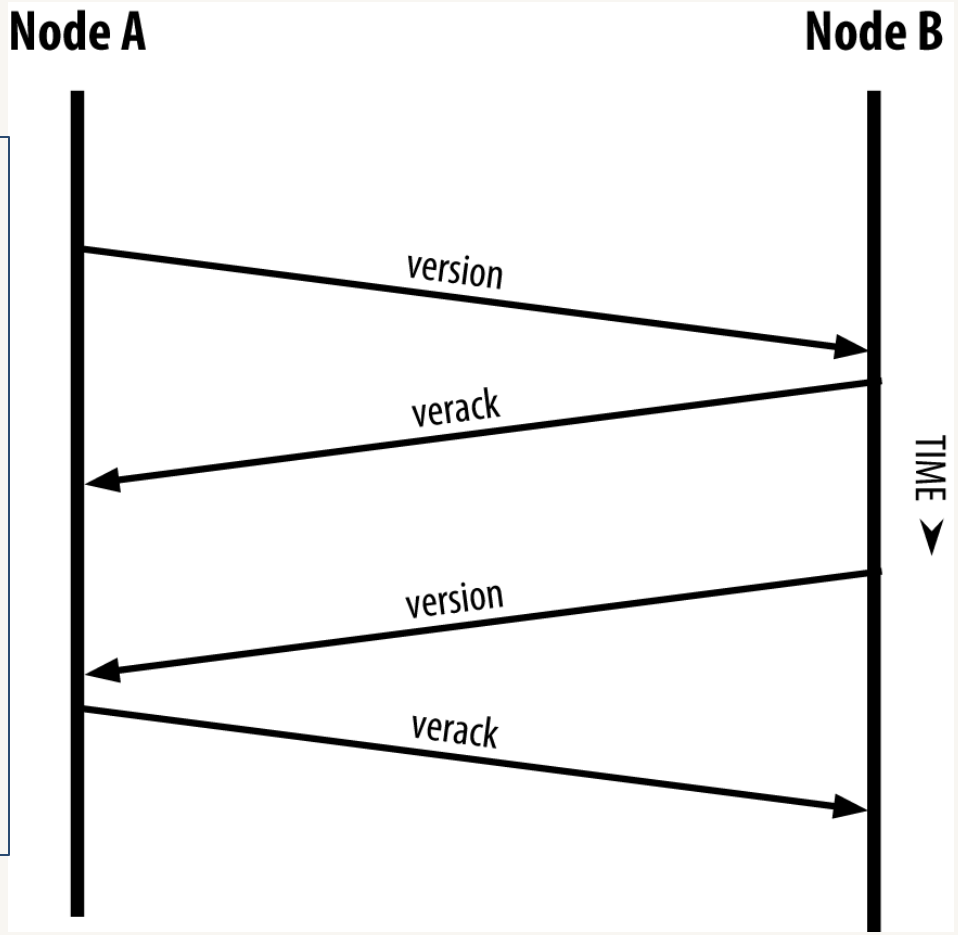
- To communicate, they need to have clear rules
  - How to find other nodes (bootstrapping)
  - How to send and receive transactions
  - How to send and receive blocks
  - How to sync the blockchain
- The basic network uses a peer-to-peer gossip protocol for
  - Node discovery, node status maintenance
  - Messages about new blocks or transactions

Node discovery/bootstrapping

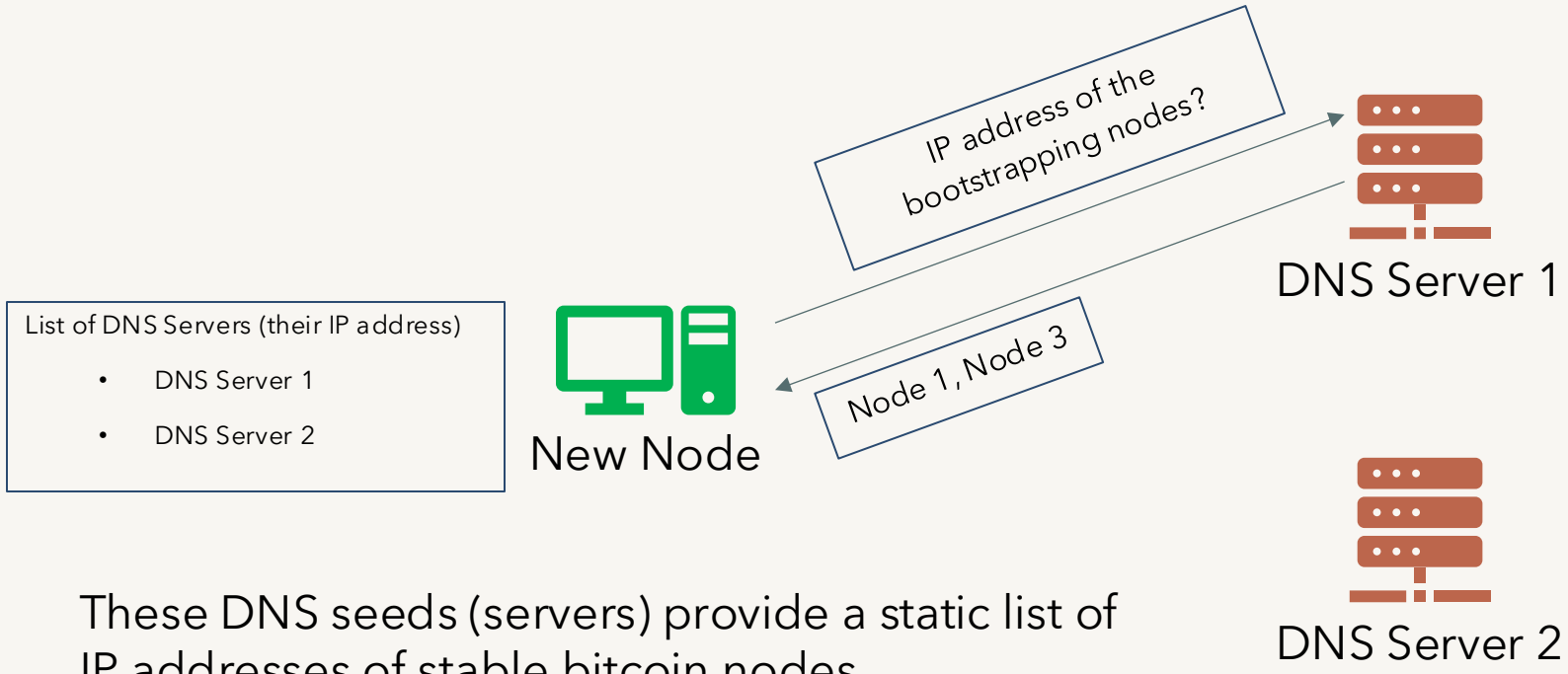
- Adding a new node into the network is called bootstrapping
- The new node needs to discover other nodes in the network to connect to the P2P network
- How does it know who to connect to?
  - Hard-coded DNS-services which offer IP-addresses of nodes
  - Hard-coded seed addresses (last resort)
  - Command-line provided addresses
  - Text-file provided addresses

Node discovery/bootstrapping

- The first message to another Bitcoin peer is the version message
- Using version each node check if the other node is compatible
- If compatible, the other node sends the version acknowledgement (verack) message

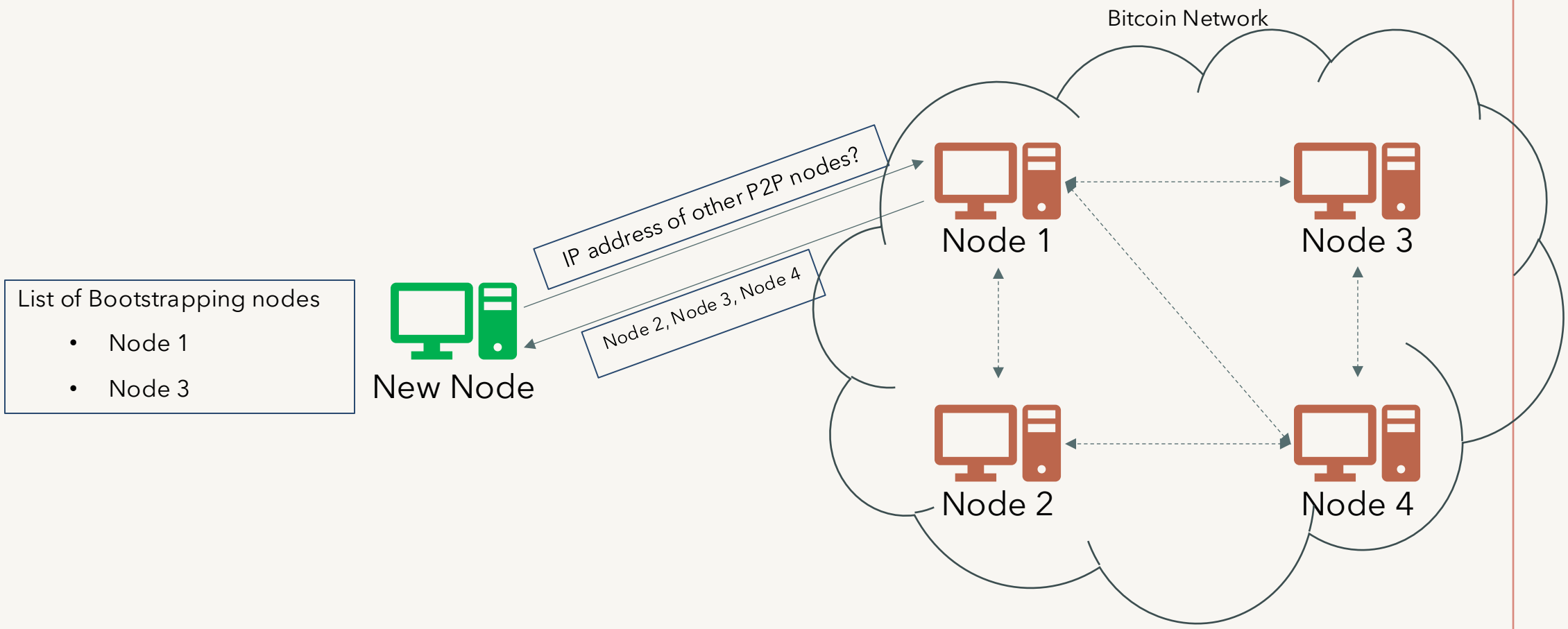


Node discovery/bootstrapping

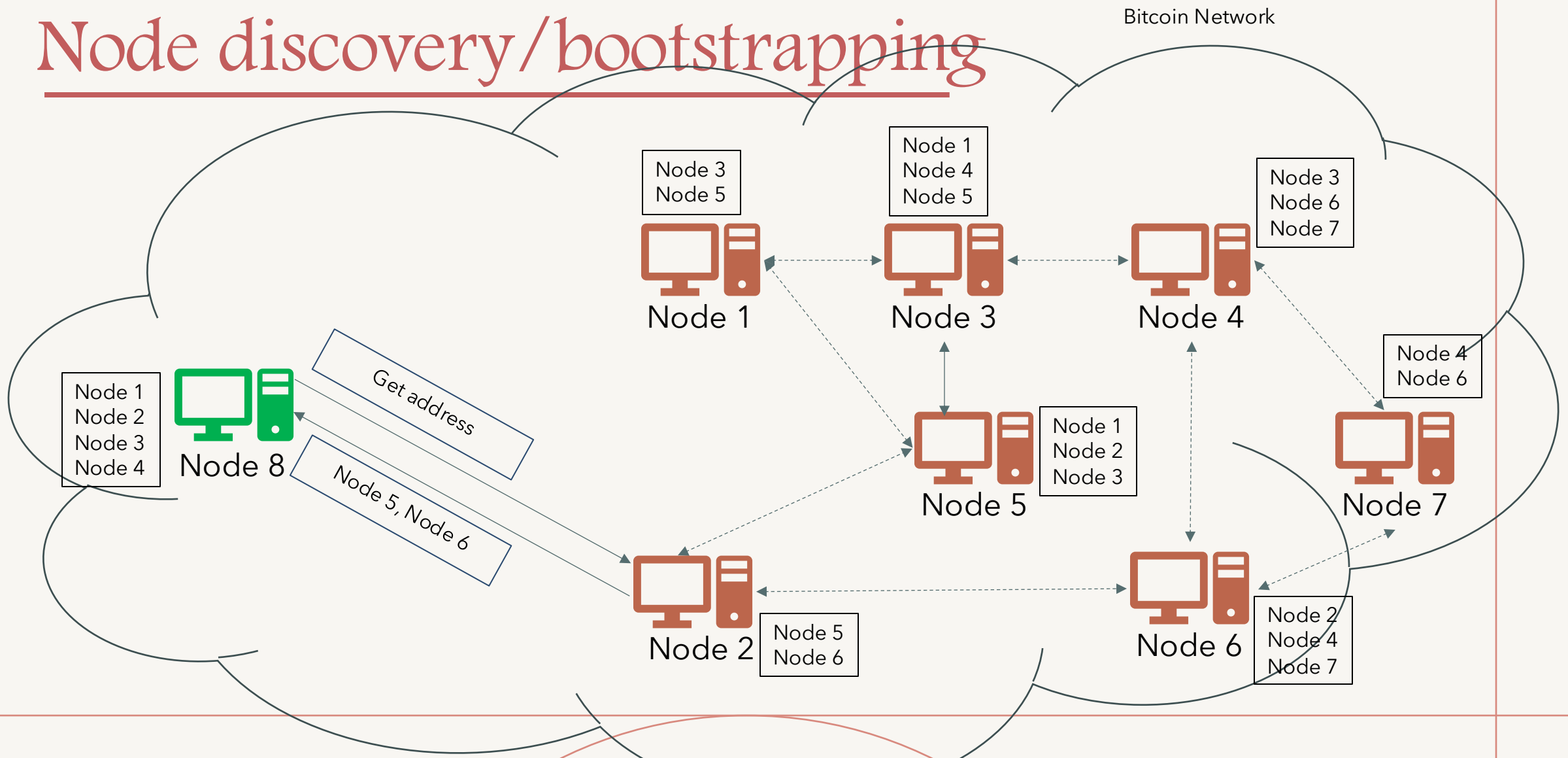


These DNS seeds (servers) provide a static list of IP addresses of stable bitcoin nodes

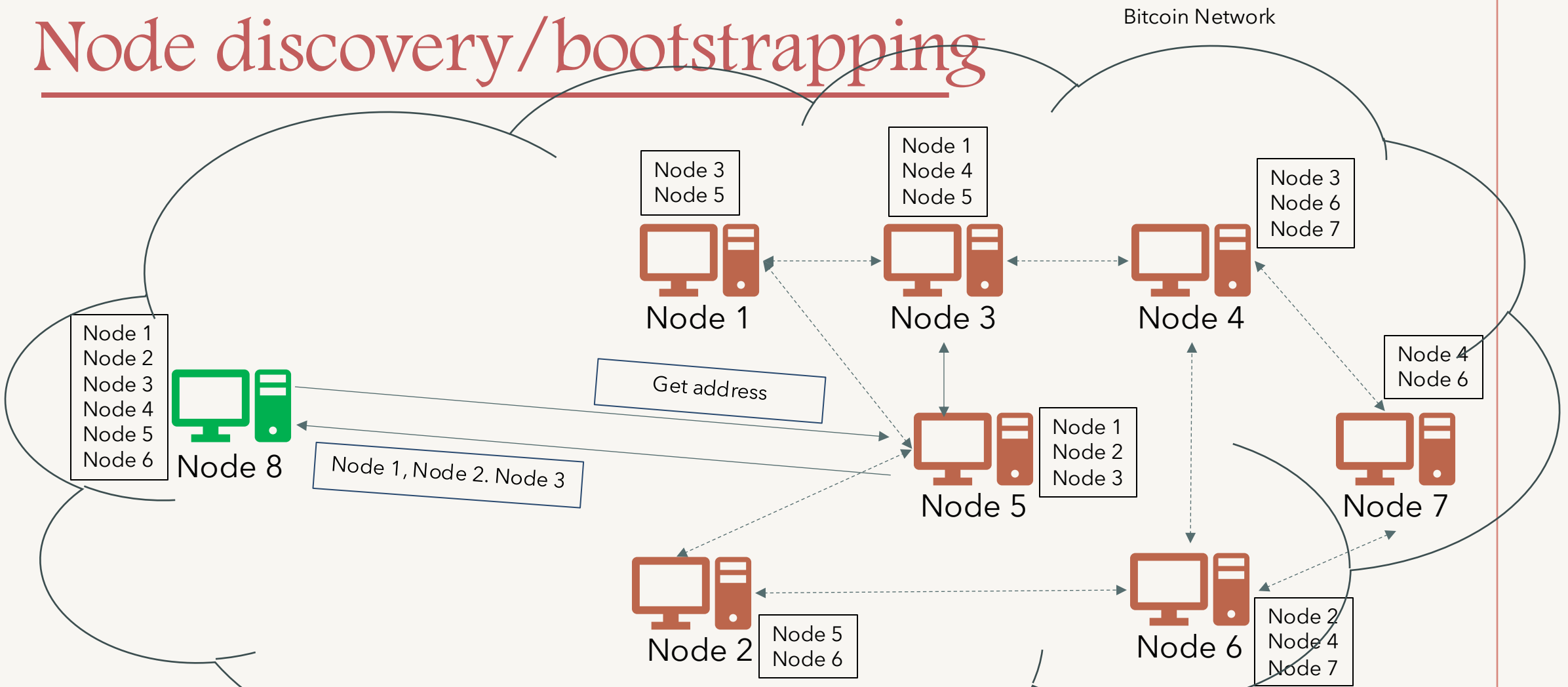
Node discovery/bootstrapping



Node discovery/bootstrapping



Node discovery/bootstrapping



Bitcoin blockchain

- There are three different things to understand
  - Transaction
  - Block
  - Blockchain

Transaction

- Transactions are the most important part of the bitcoin system
- Everything else in bitcoin is designed to ensure that transactions can be created, propagated on the network, validated, and finally added to the global ledger of transactions (the blockchain)
- Transactions are data structures that encode the transfer of values between participants in the bitcoin system
  - A transaction transfers money from somebody to somebody else
- Each transaction is a public entry in bitcoin's blockchain, the global double-entry bookkeeping ledger
  - an entry that affects at least two different accounts
- All transactions are public
- Everybody can see all transactions in a blockchain explorer


THANK YOU
QUESTIONS?