CSE446: Blockchain & Cryptocurrencies

Lecture – 10: Bitcoin-4

Agenda

- Bitcoin components
  - Blockchain

Bitcoin mining

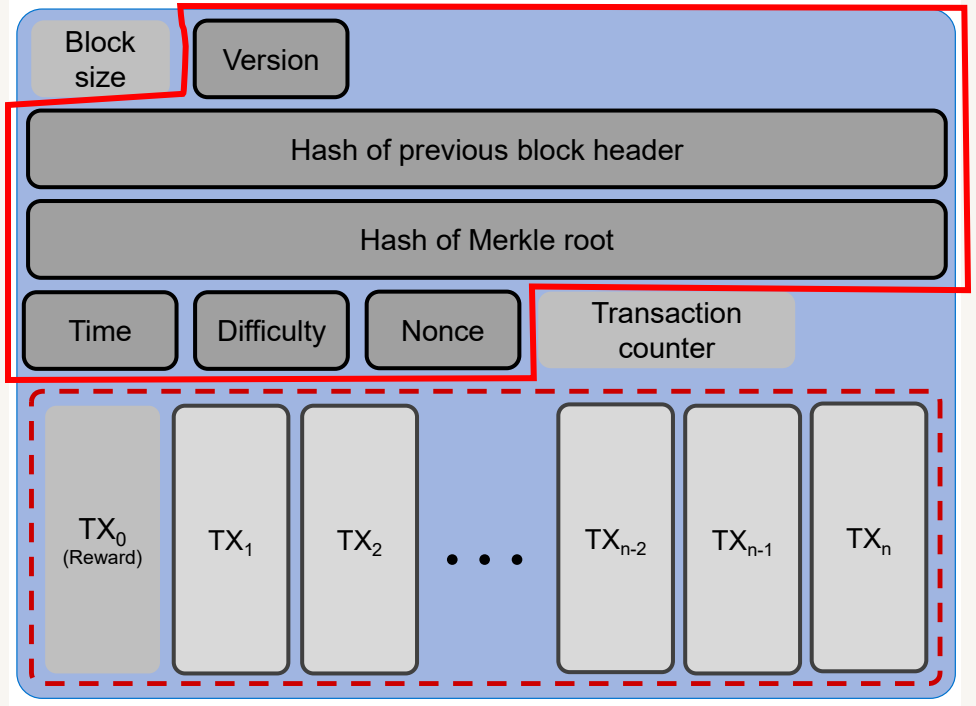
- Every miner node listens for transactions and puts them in its transaction pool (mempool)
- From the pool, transactions are combined to form a block
- Forming a block is not enough, a valid block needs to be created
- To create a valid block, a “proof of work” needs to be provided
  - It resembles a cryptographic puzzle whose solution can only be found by a brute-force mechanism, thus it is like participating in a lottery

Bitcoin mining: PoW

- Facilitates a search puzzle (trying to find a value matching a criterion)
- Requires large amount of tries (like a lottery)
- High investment costs (for powerful h/w facilitating faster tries)
- High energy costs (to maintain the powerful h/w)
- Leads to arms race (every miner is competing with others)
- High attack costs (need to outperform the majority of miners)
- Fully anonymous mining (miner identities are bitcoin address)

Bitcoin mining: PoW

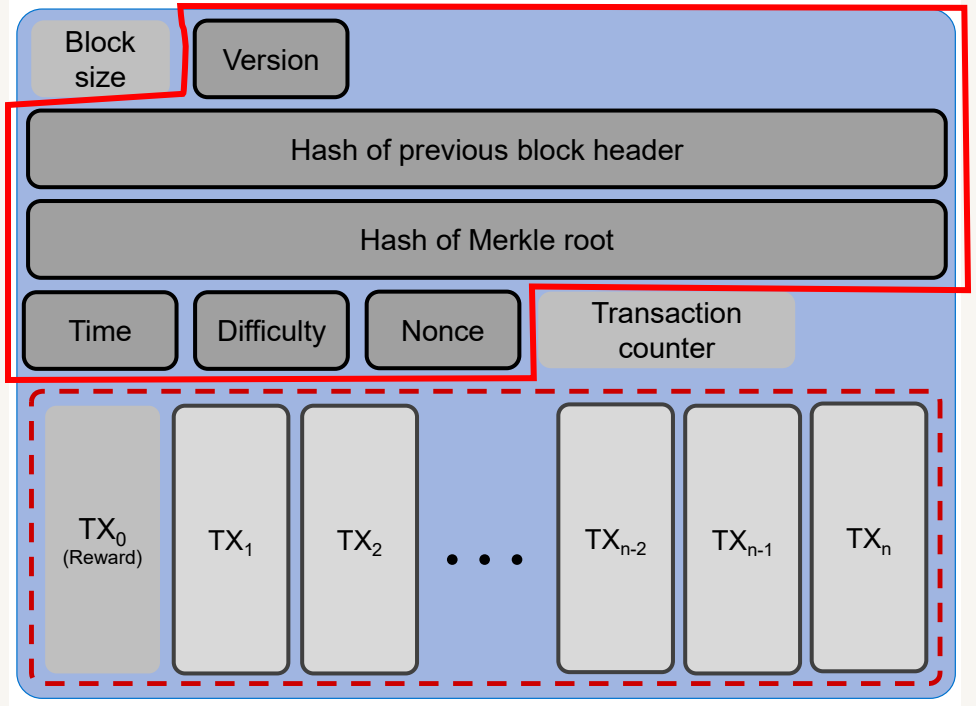
- It combines several data from the block header and tries to find a value which matches a certain condition
- These six fields are used to calculate the header hash
  - E.g. to calculate the hash of the previous blocks, these six values from the previous block header are double hashed with SHA-256
  - We denote this as H



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

Bitcoin mining: PoW

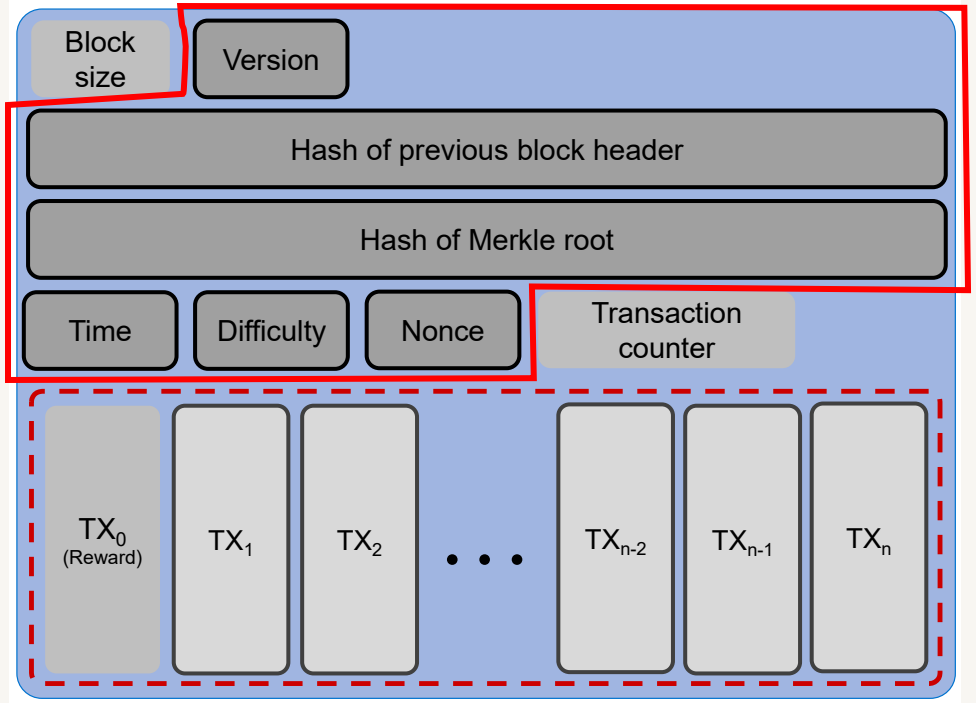
- V: Version is a fixed number representing the protocol rule used for this particular block
- M: Hash of Merkle root is the merkle root of all transactions in the block
- T: Time is a UNIX epoch time (number of seconds elapsed since 00:00:00 UTC on 1 January 1970)
- D: Difficulty is a dynamic value representing the target
  - The puzzle solution must be less than this target
- N: Nonce is changed until a solution to the puzzle is found



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

Bitcoin mining: PoW

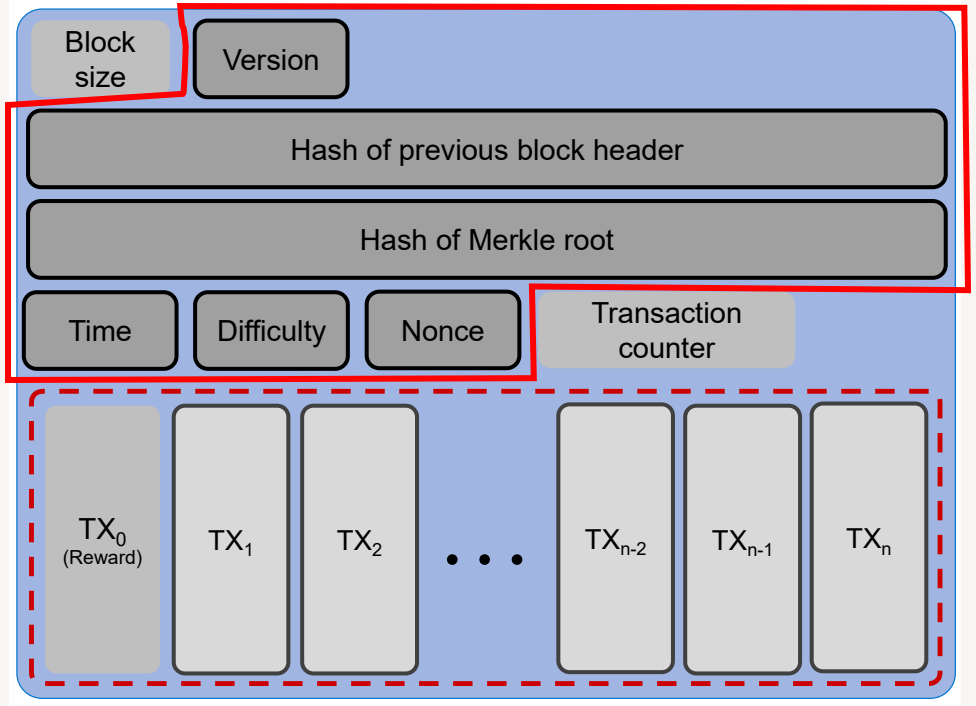
- So the search puzzle is this:
  - SHA256(SHA256(V || H || M || T || N)) < D
- V is mostly same
- H is same for all nodes (why?)
- T is same (very unlikely, but let's assume this)
- Assuming all nodes have the same txs in their mempool, M will never be same (why??)



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

Bitcoin mining: PoW

- So the search puzzle is this:
  - SHA256(SHA256(V || H || M || T || N)) < D
- V is mostly same
- H is same for all nodes (why?)
- T is same (very unlikely, but let's assume this)
- Assuming all nodes have the same txs in their mempool, M will never be same (why??)
  - As TX0 represents the coinbase transaction where the output is different for all miner nodes (address of the miner node)
- Change N to find the solution

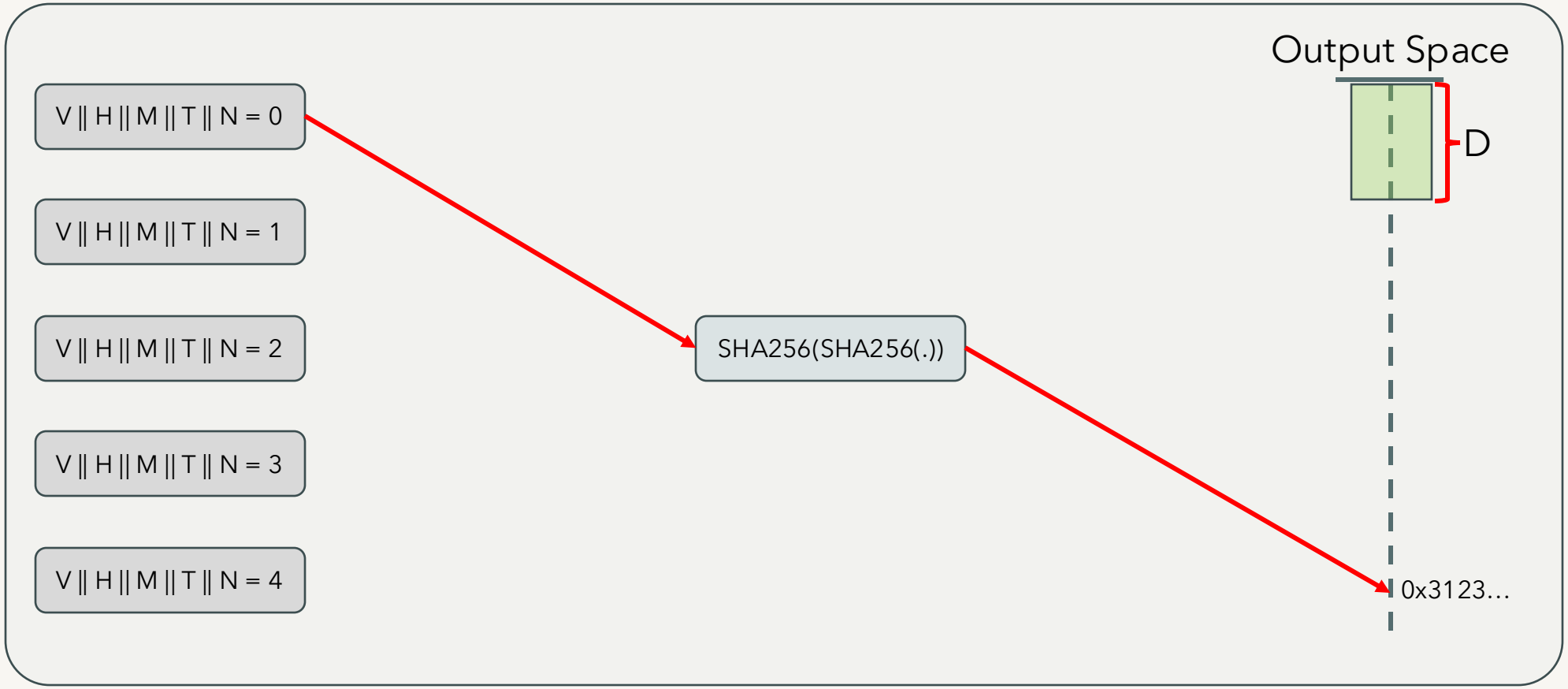


Bitcoin Basics- Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

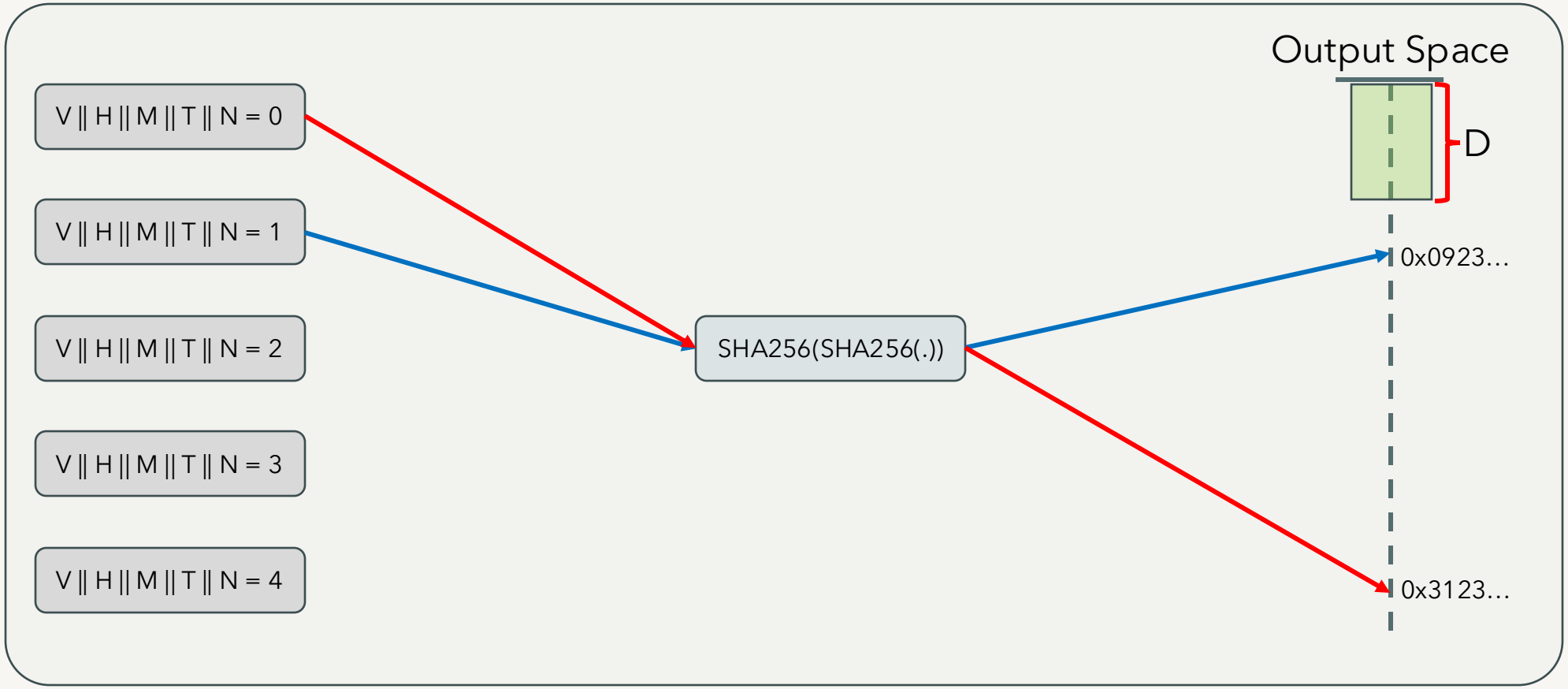
Bitcoin mining: PoW

B number of blocks are already in blockchain. Solving for the B+1 block

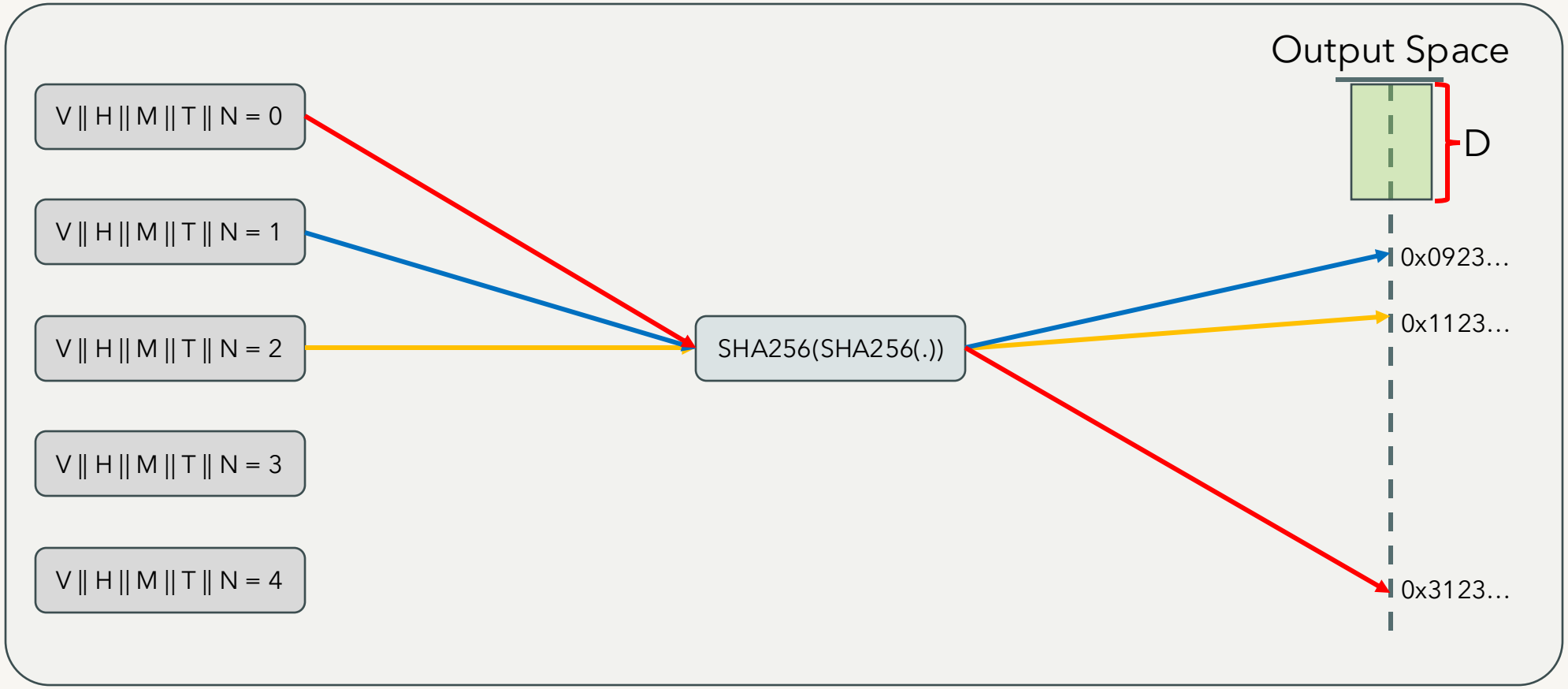
Bitcoin mining: PoW



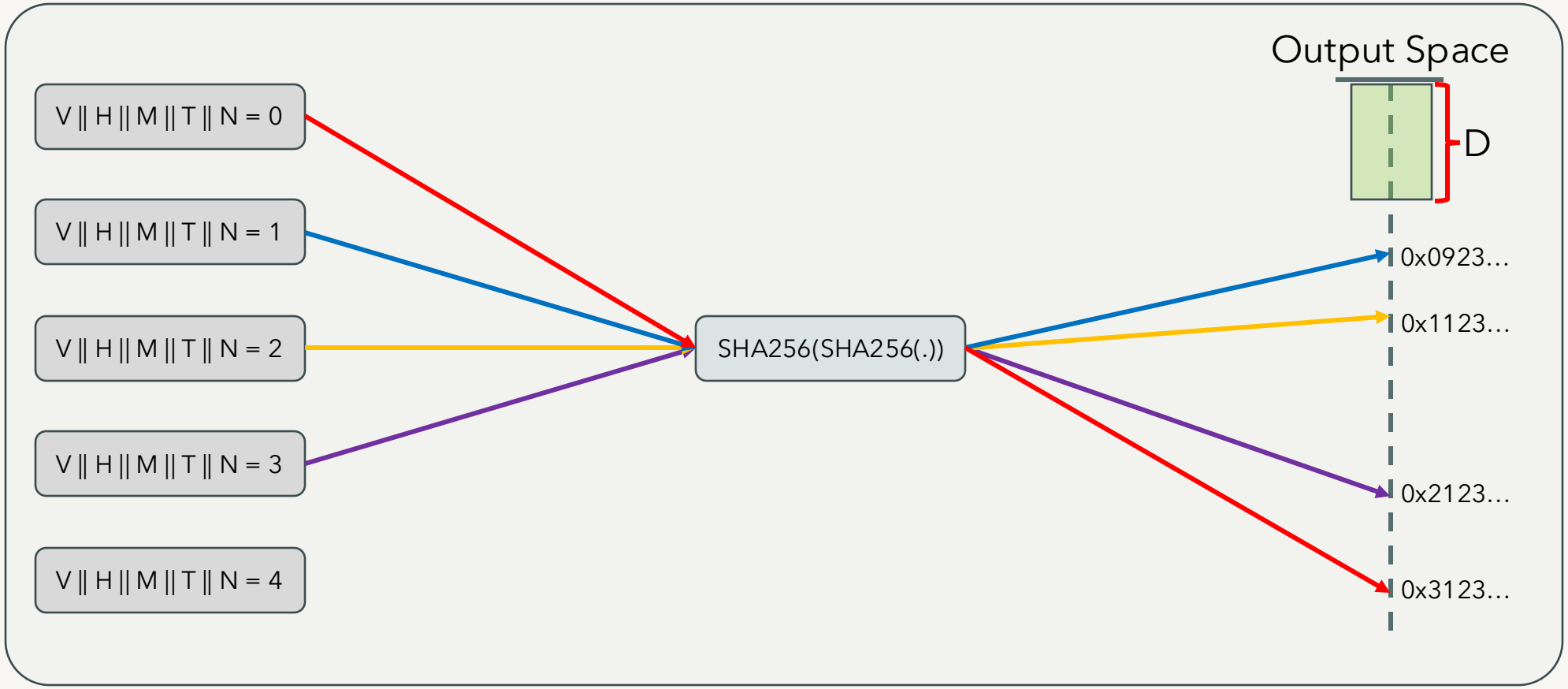
Bitcoin mining: PoW



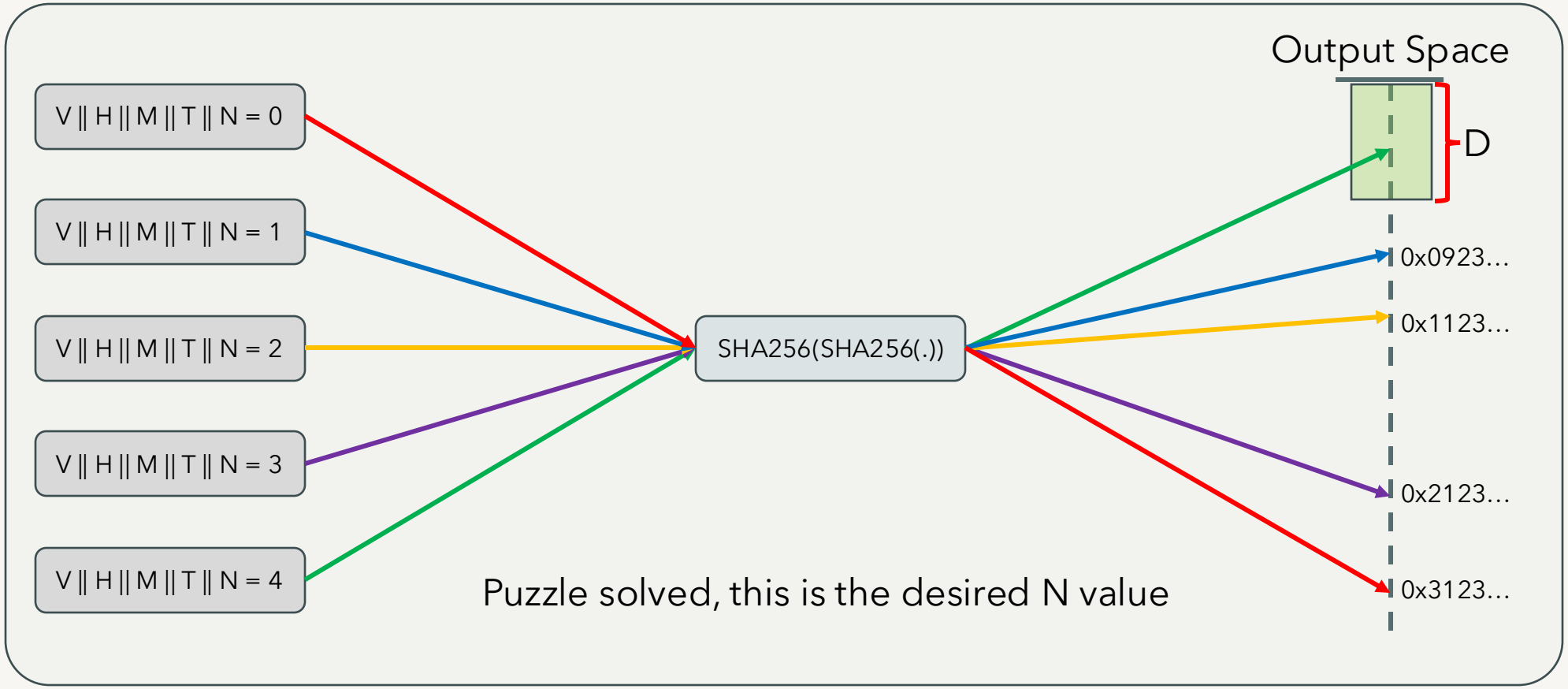
Bitcoin mining: PoW



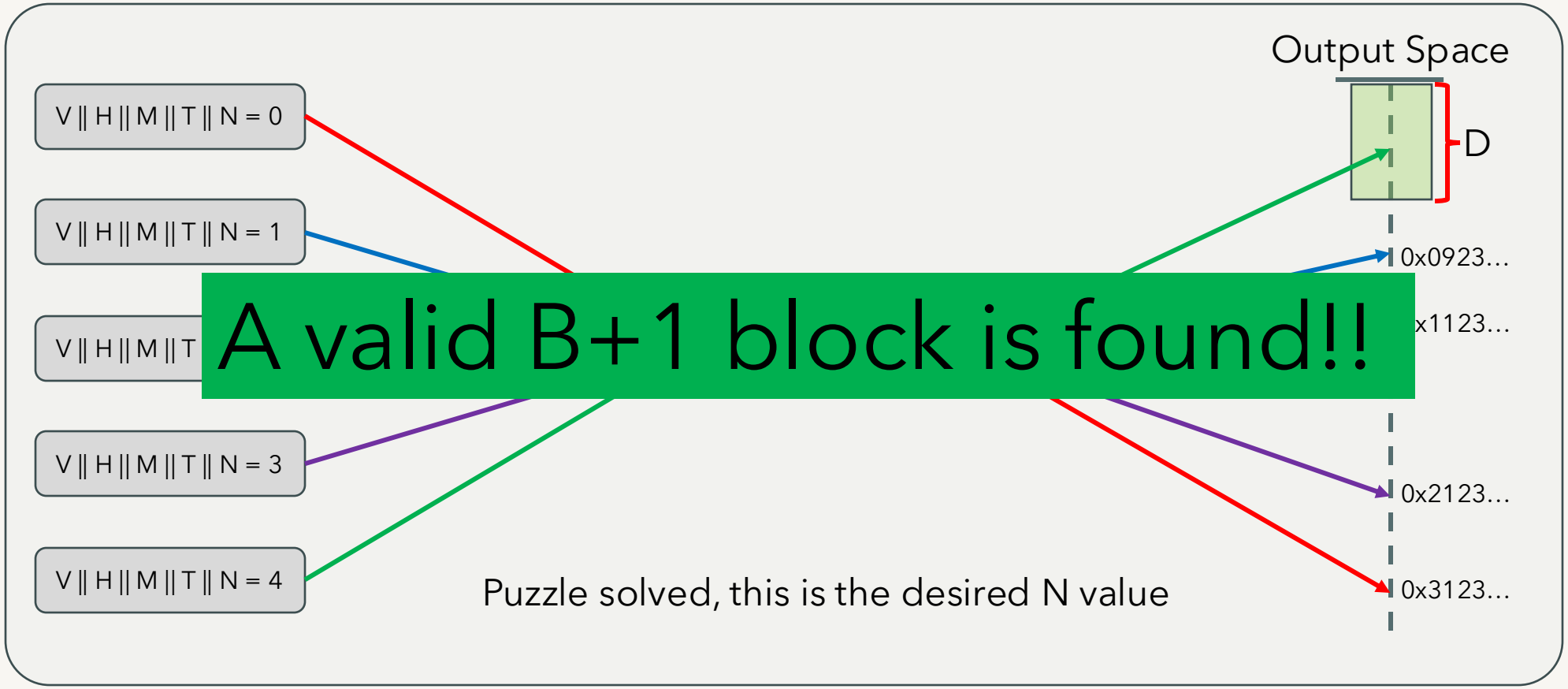
Bitcoin mining: PoW



Bitcoin mining: PoW



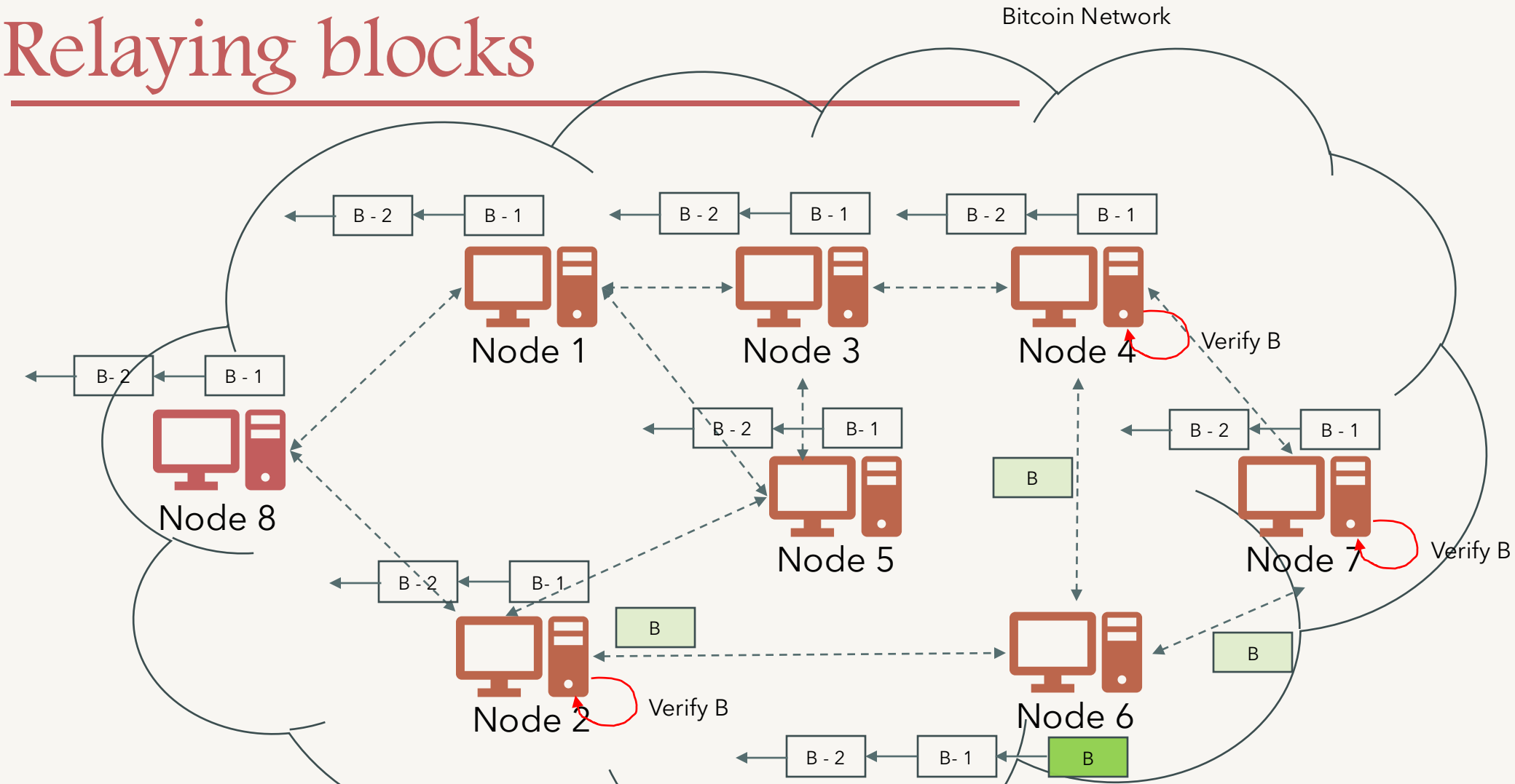
Bitcoin mining: PoW



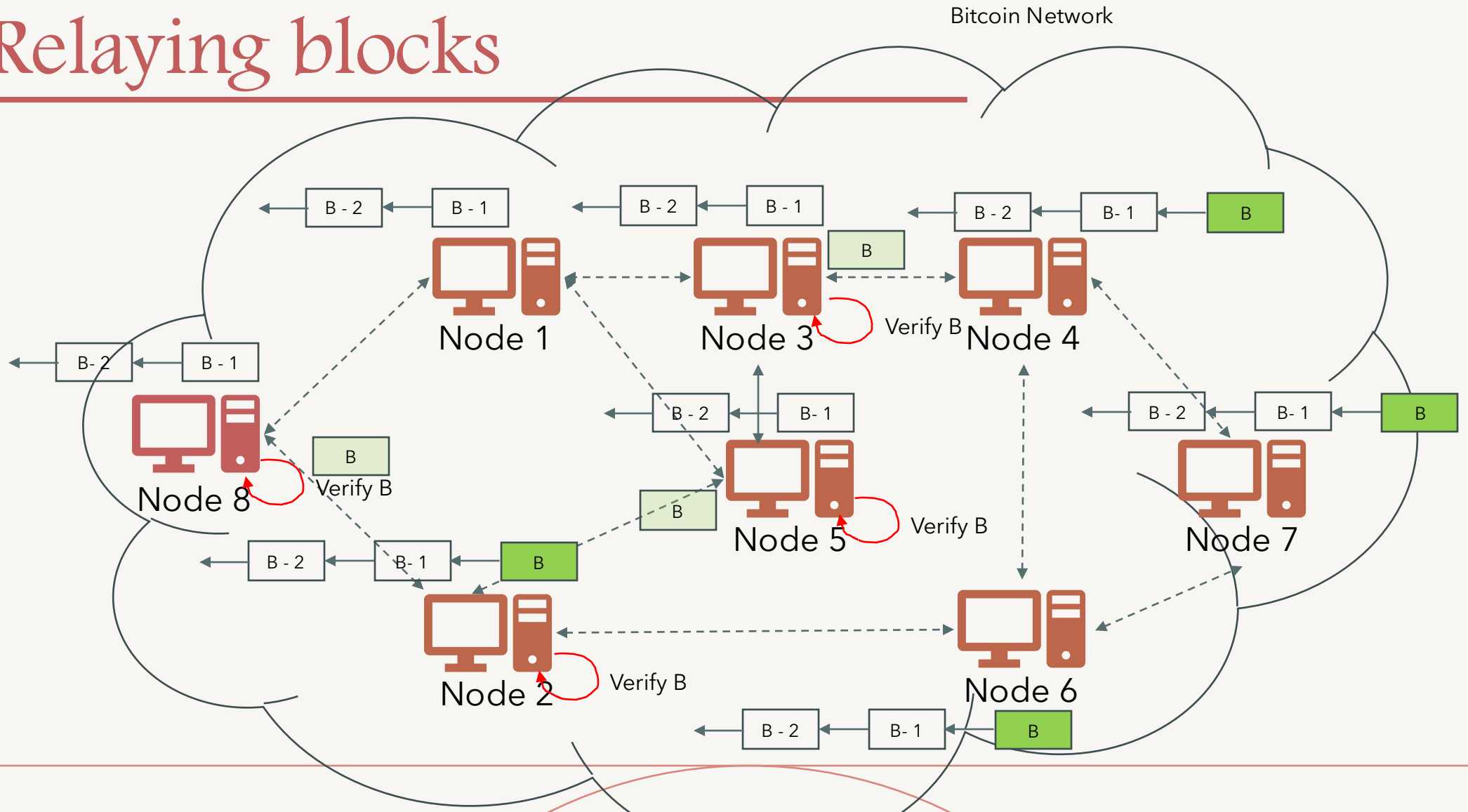
Bitcoin mining

- Once a valid block is found, the respective miner broadcasts the block in the network
- All (full and miner) nodes verify if the block is valid
- The rules for checking block validity
  - All of its transactions are valid
  - The desired double hash value is indeed less than the difficulty target
- They include the block in the blockchain and starts the same procedure for the next book

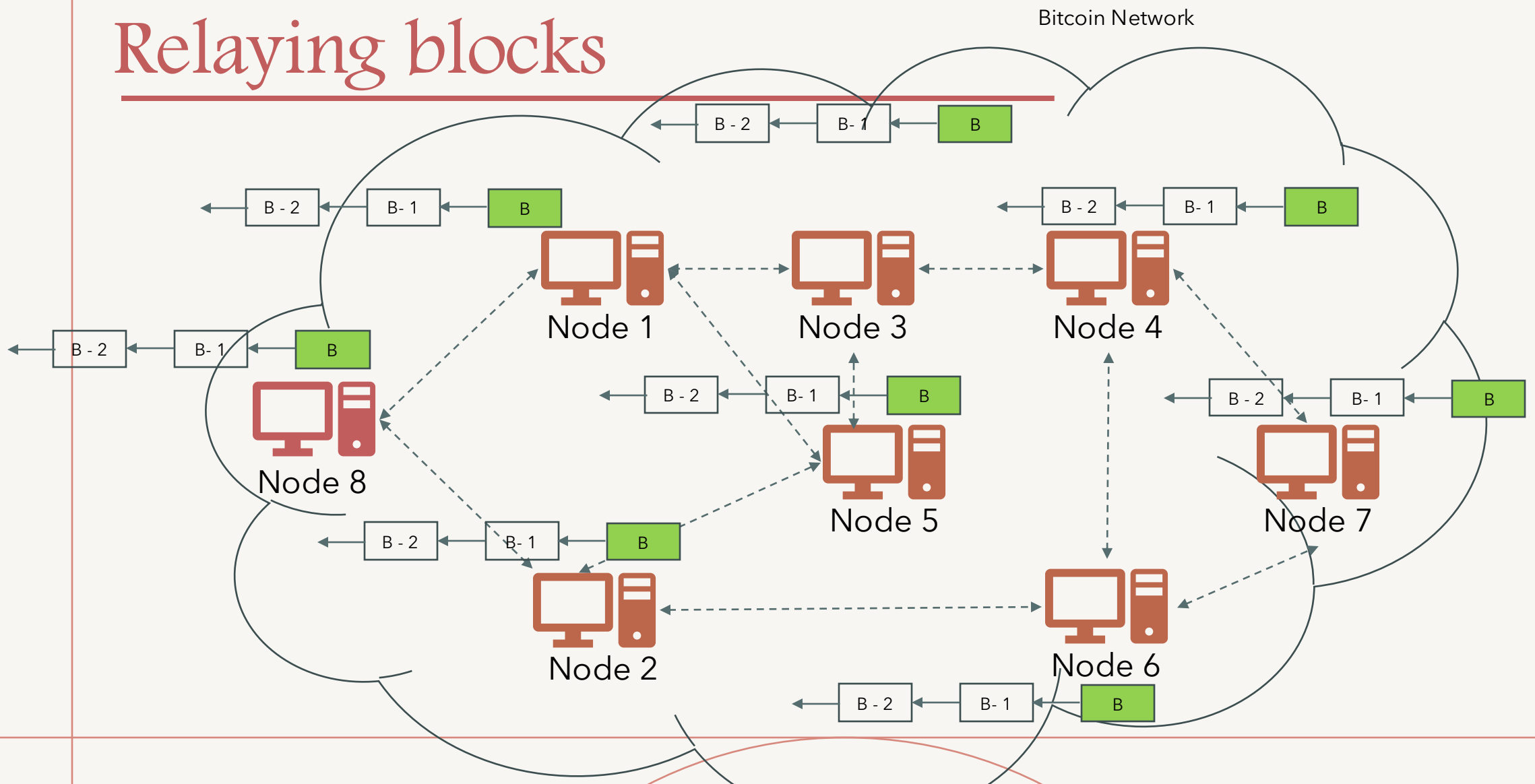
Relaying blocks



Relaying blocks



Relaying blocks



Bitcoin mining

- Solving the puzzle implies that a leader has been implicitly selected
  - Similar to the RAFT's blockchain leader selection algorithm
- The selected leader has created the block
- All other nodes will follow his instruction to include the block
- However, unlike RAFT, we need to ensure that
  - The node is not byzantine
- The block and transaction checking algorithm ensure this

Difficulty adjustment

- Difficulty is used to implicitly select a leader
- It has another purpose: to ensure that a block is created in 10 minutes in average
- Why is the block time constant and fixed to 10 minutes?
- > 10 minutes -> Too slow
  - Transactions take longer to be included
  - Network capacity decreases as a smaller number of transactions are handled
- < 10 minutes -> Too fast
  - Higher possibility of chain forking, leading to multiple “realities”
  - Empty blocks

Difficulty adjustment

- How to ensure a constant time (in average) for block generation?
- The difficulty is fixed dynamically and adjusted after every 2016 blocks in around 14 days, (14 x 24 x 6 = 2016)
- The difficulty also reflects the total hashing (computing) power of the nodes in the network
- For example
  - if more blocks were produced in the last 14 days, it implies that the hashing power has increased, therefore, the difficulty is not enough to produce a block in 10 minutes
  - Solution: increase the difficulty and vice versa

Difficulty adjustment

1. Measure, how long the last 2016 blocks took to get mined. (=T)
2. Calculate the factor of speed (two Weeks / T) (=F)
3. The difficulty gets increased (F > 1) or decreased (F < 1).
   - 3a. Maximum increase: 4. Maximum decrease: 0,25.
4. The process is done every 2016[1] blocks.

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

Difficulty adjustment

- What does it mean when F > 1?
  - 2016 blocks have been produced in less than 14 days
- When can it happen?
  - When the number of node has increased, resulting in more computing (hashing power) in the network
- In order to ensure the limit of 1 block/10 minutes, difficulty gets increased ensuring that the next 2016 blocks take more than 14 days
  - thus averaging 2016 block in 14 days = 1 block/10 minutes
- Similarly, F < 1 means, the hashing power has decreased, and the miners are finding it difficult to mine blocks in average 10 minutes
  - Solution: reduce the difficulty

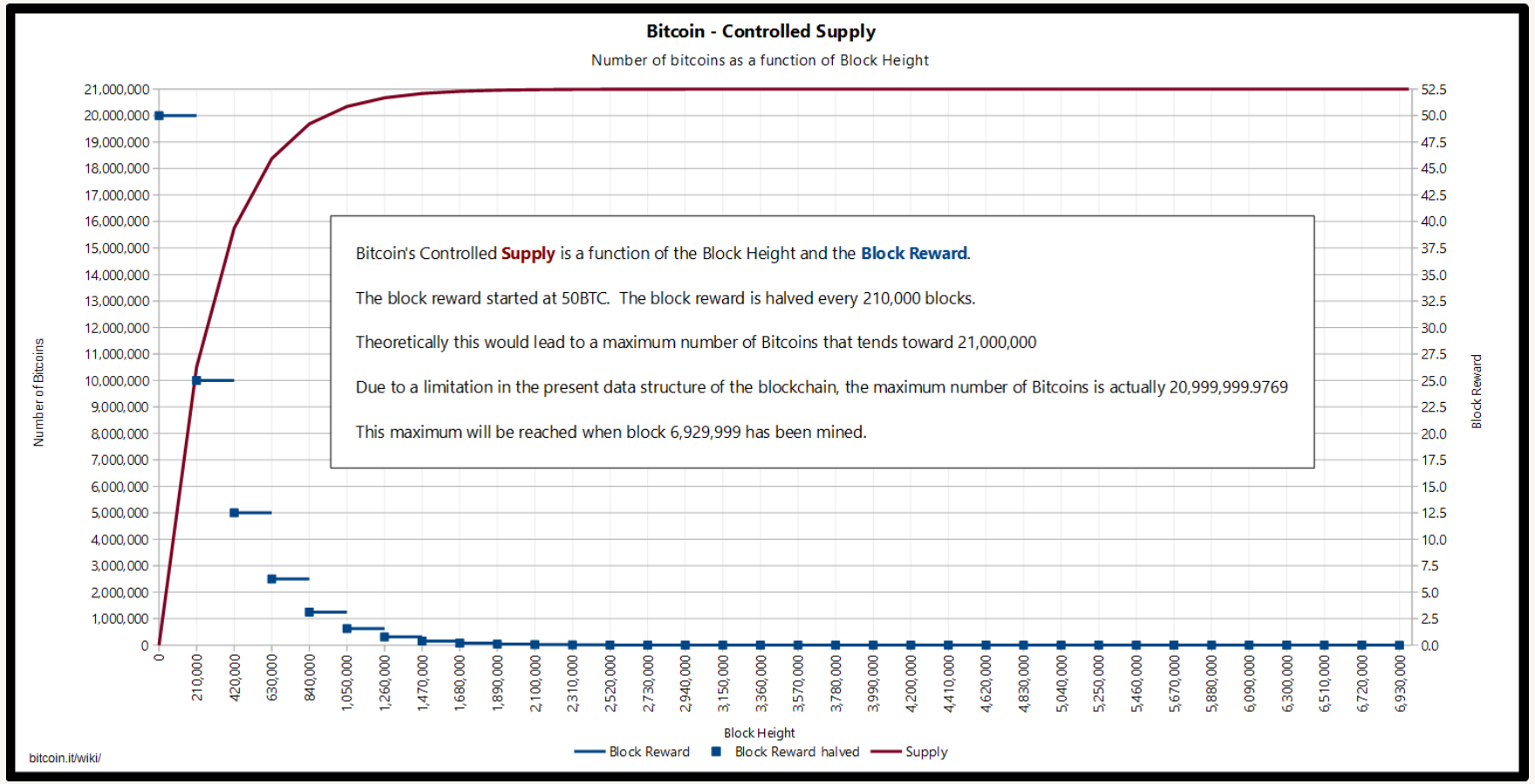
Bitcoin reward

- The miner who solves the puzzle is rewarded with new Bitcoins
- Number of reward is halved in every 210000 blocks (~ 4 years)
  - Currently, it is 3.125 bitcoin
- It is included as the first (***coinbase***) transaction which is output to a miner's address, or an address selected by the miner
- As rewards get halved in every 210000 blocks
  - at some point the rewards will reach towards an asymptotically zero
- This represents a geometric series and we can calculate the maximum of bitcoin that will be produced before reaching asymptotically zero
  - The number is 21 millions bitcoins

Bitcoin reward

- Currently more than 94.5% of bitcoins have already been created
- Thus bitcoin represents a limited resource, much like any natural resource
  - Hence, the creation of bitcoin is coined as mining
- This is why bitcoin is regarded as a deflationary currency as there is no mechanism to create additional bitcoin once 21M bitcoins are created
- Will bitcoin system cease to function at that point?

Bitcoin reward



https://en.bitcoin.it/wiki/Controlled_supply

Bitcoin mining game

- Bitcoin mining can be a profitable income source
- There can be 450 (3.125 x 6 x 24) bitcoins mined per day (in average)
  - Around 51M USD in today's price
- Let's assume that there are 10 miners in the network each with equal hashing power of 10terahash/sec (they have the same h/w for bitcoin mining), 1 terahash/sec = 1 trillion hash/sec
  - So each day each miner earns 51M/10 = 5.1M USD
- Now, one miner thinks of increasing his hashing power to 20 Th/sec
  - Resulting more blocks mined by him than others
- Others noticing that they also increase their hashing power to 20 th/sec

Bitcoin mining game

- Now the whole network has miners each having a hashing power of 20 th/sec
  - All earning the same value of 5.1M USD per day
- As more computing power means more blocks are generated, breaking the 2016 blocks in 14 days law
- To adjust this, difficulty is increased and so less blocks in next 14 days
- If again some miner wants to increase their computing power
  - the same cycle will repeat, resulting in a mining game or arms race

Bitcoin hashrate

https://blockchain.info/charts/hash-rate

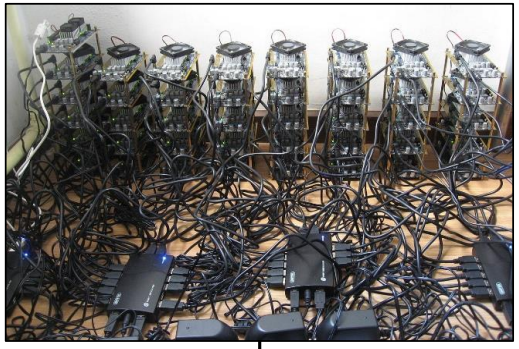
Bitcoin mining game

2009
CPU

CPUs were the first hardware to mine Bitcoins.

2010
GPU

GPUs are faster than CPUs. First mining software was introduced in 2010.



2011
FPGA

FPGA (field programmable gate array) are much more energy effective than GPUs.

2013
ASIC

ASIC (application-specific integrated circuit) are chips specially designed for mining. Fastest mining.

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

Bitcoin mining game

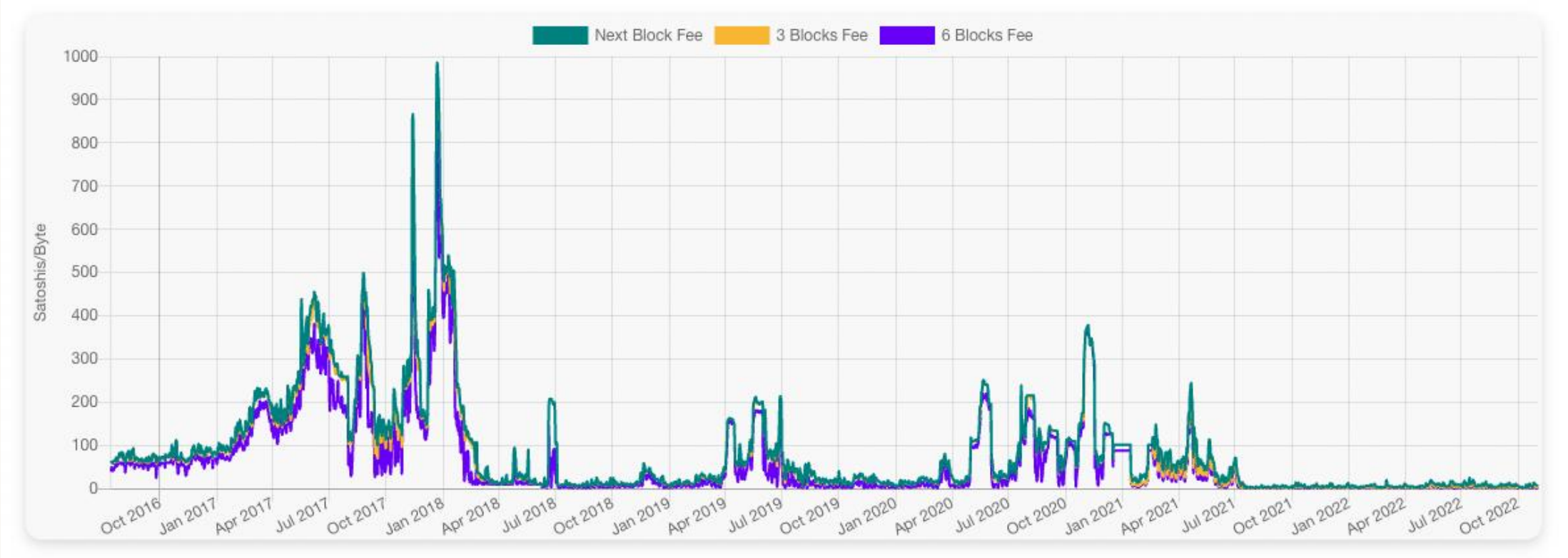
https://www.businessinsider.in/photo/83808381/worlds-largest-bitcoin-mining-rig-seller-isnt-taking-any-new-orders-for-foreseeable-future.jpg?imgsize=545771

https://imageio.forbes.com/specials-images/imageserve/610091d201bb5cdbd6af3be5/The-Belly-of-the-Beast--At-Riot-Blockchain-s-bitcoin-mining-facility-in-Rockdale-/0x0.gif?height=948&width=711&fit=bounds

Bitcoin mining game

- A miner also receives an additional incentive via fees
- If a transaction does not provide any fee, miners will simply ignore it as it is not profitable for them
- The effect of this is that users compete with each other to include their transactions in the block
- This increases the fee over time

Bitcoin mining game

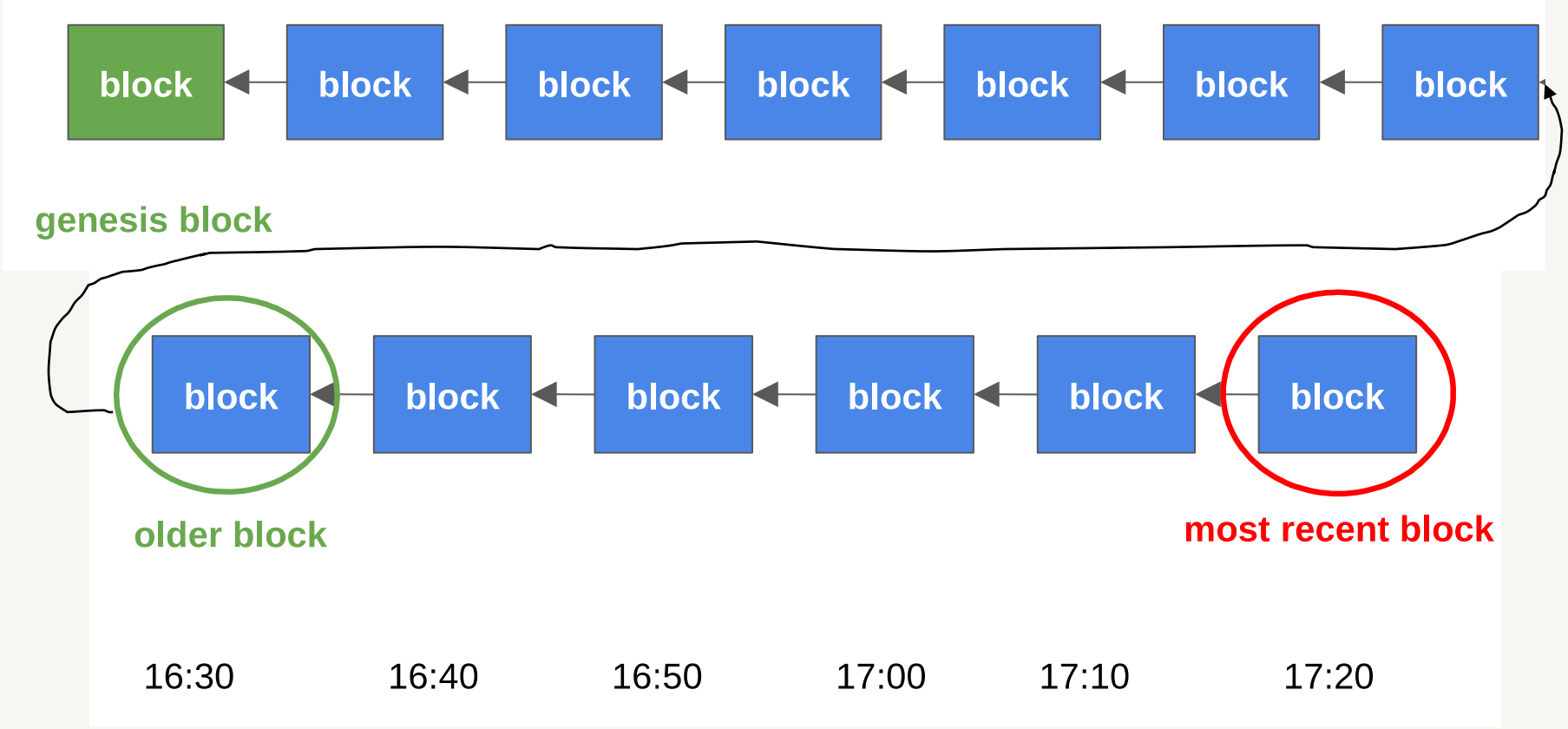


https://privacypros.io/tools/bitcoin-fee-estimator/

Bitcoin blockchain

- The blockchain data structure is an ordered, back-linked list of blocks of transactions
- The blockchain can be stored as a flat file, or in a simple database
  - The Bitcoin software stores the blockchain metadata using Google's LevelDB database
- The blockchain is often visualised as a vertical stack, with blocks layered on top of each other and the first block serving as the foundation of the stack
  - Thus creating the notion of "height" to refer to the distance from the first block, and "top" or "tip" to refer to the most recently added block
- The first block is known as the genesis block

Bitcoin blockchain



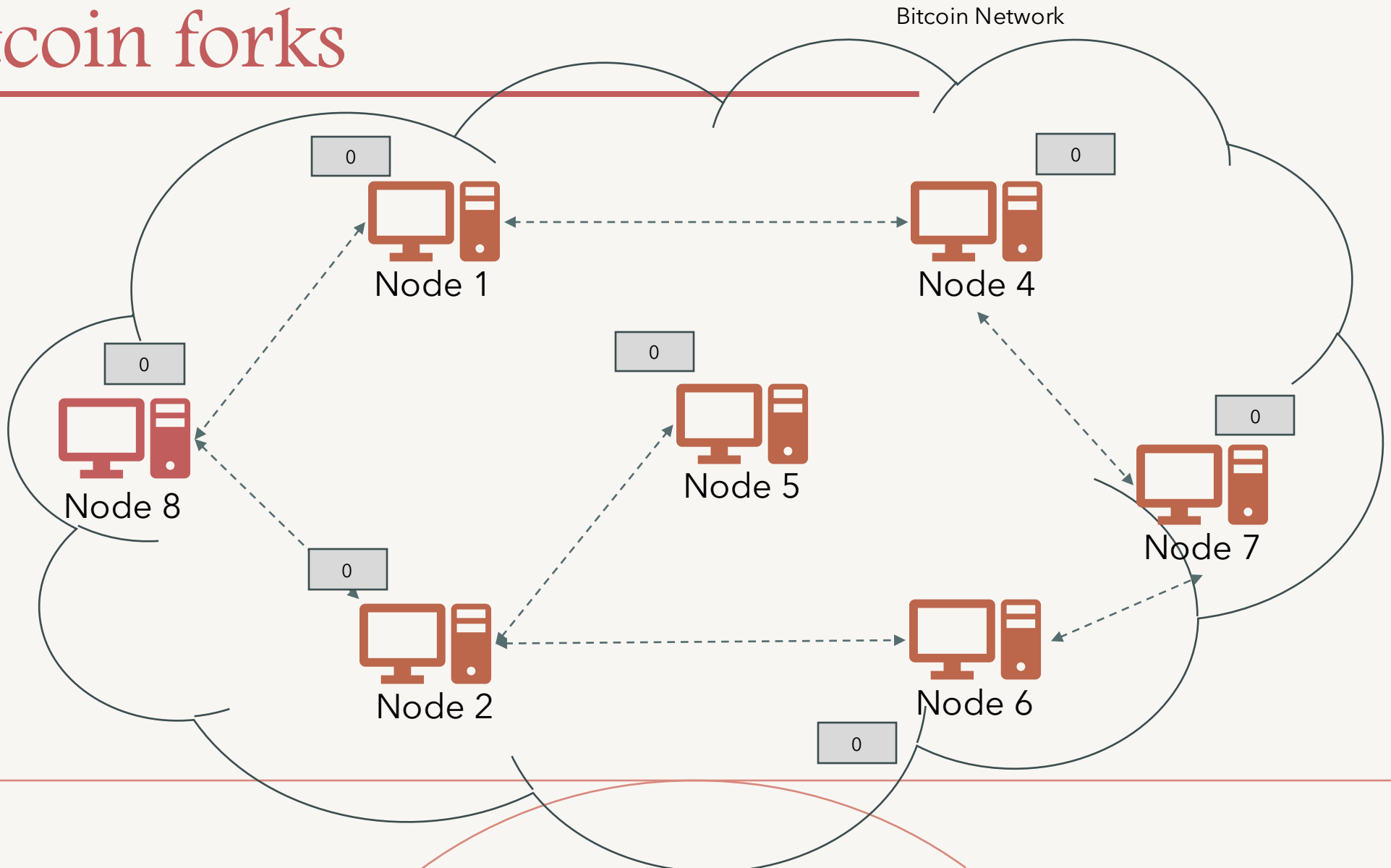
Bitcoin consensus

1. Transaction Broadcast: Every node who receives transactions or creates them, broadcasts them to the network, making everyone aware of new transactions
2. Block Building: Every miner node collects the valid transactions, orders them and creates a new block containing the transactions
3. Random Node Selection: A miner node is randomly chosen out of the network, e.g. by solving the PoW puzzle. It is able to propose its block to the network
4. Block Validation: Other nodes receive the block from the randomly chosen node and validate whether it is correct. A correct block only contains valid transactions
5. Block Acceptance: Other nodes show their acceptance for this block if the nodes build new blocks on top of the recently proposed block

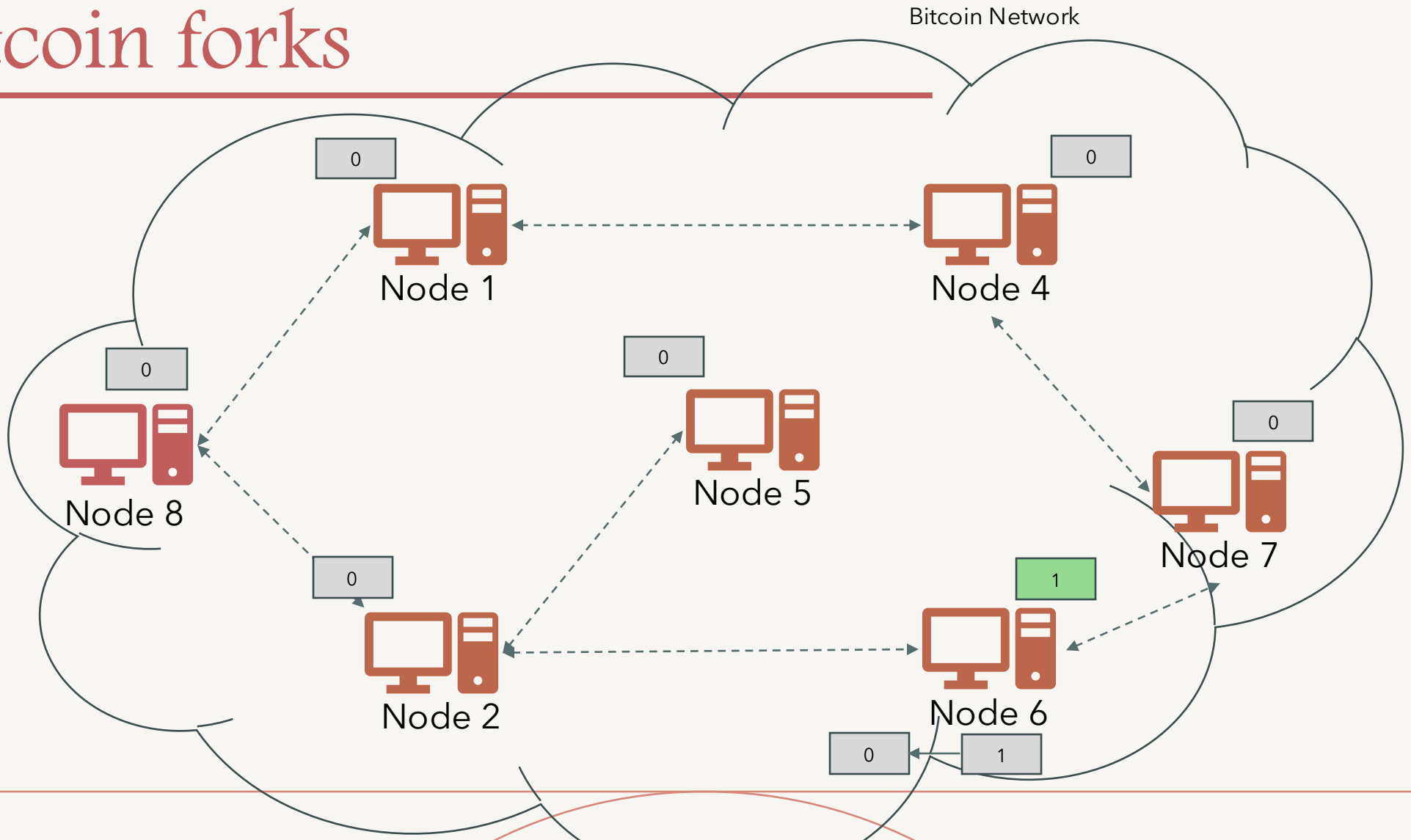
Bitcoin consensus

- Each node independently extends the blockchain
  - Remember that there is no coordination mechanism
  - There are also byzantine nodes in the network. Who do you trust?
- What happens when two miners generate valid blocks simultaneously?
- Also a block does not reach every node simultaneously
  - There will always be a network propagation delay due to miners residing in different geographical locations
  - Each node initially may have different views of the chain, known as a fork

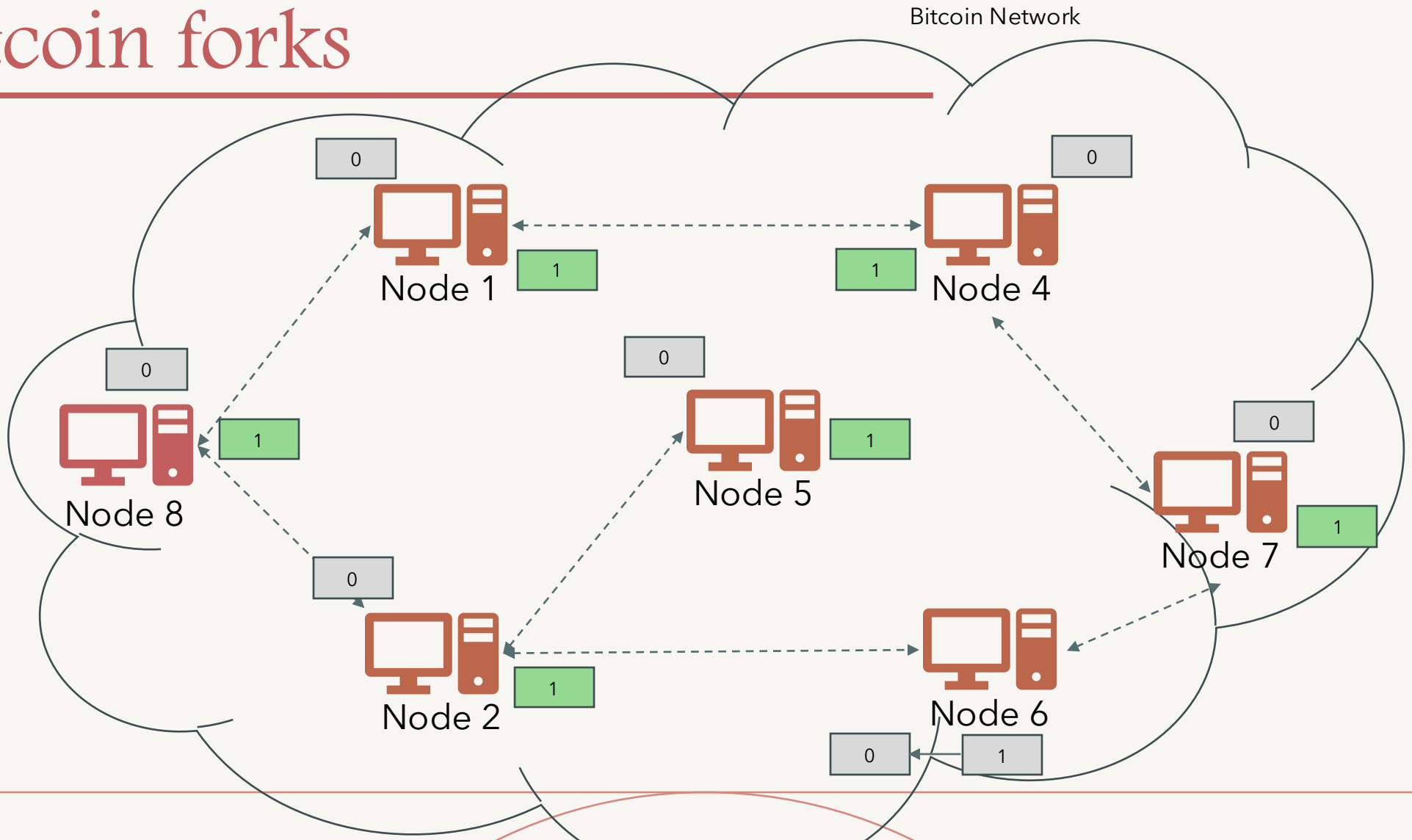
Bitcoin forks



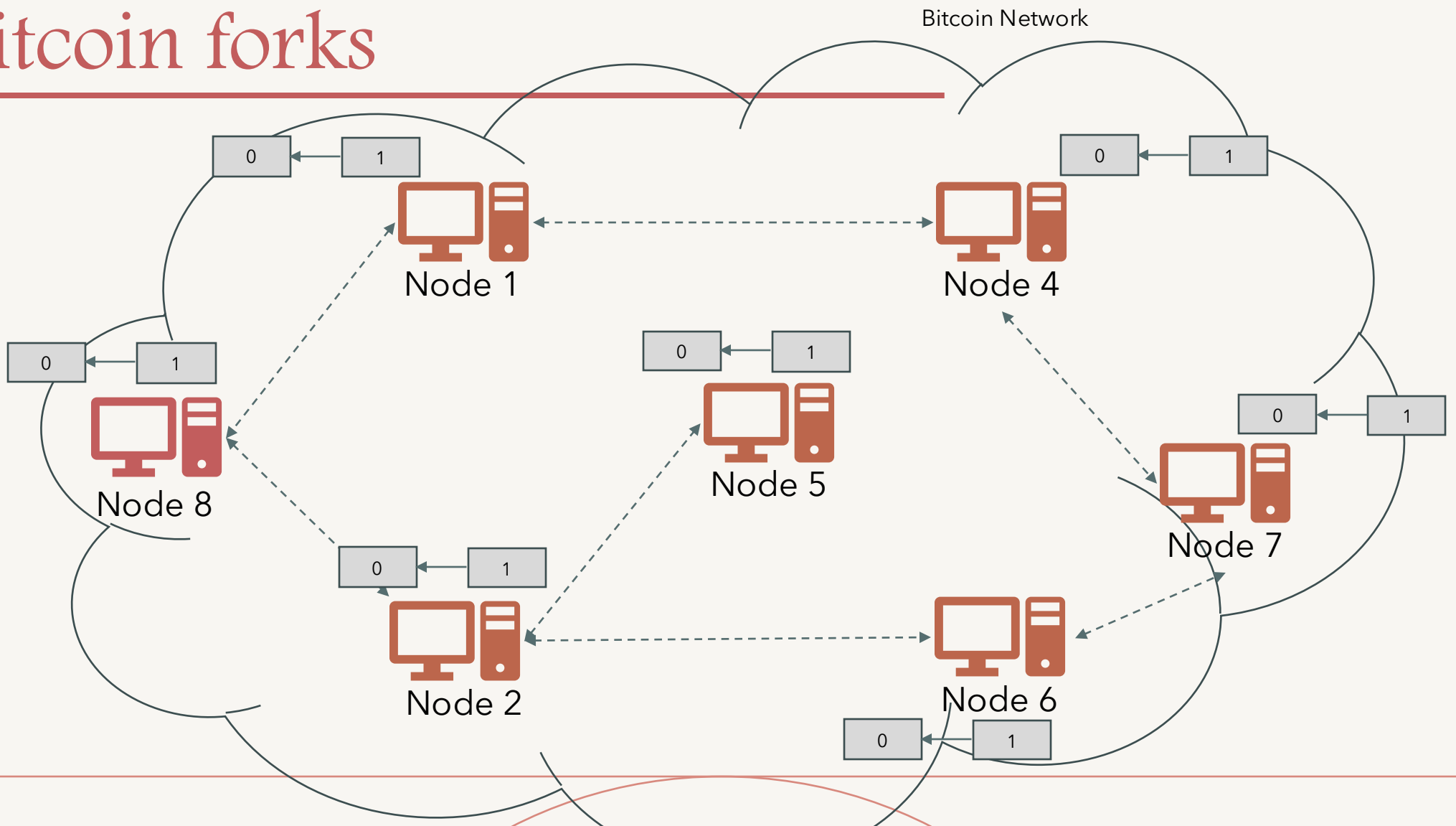
Bitcoin forks



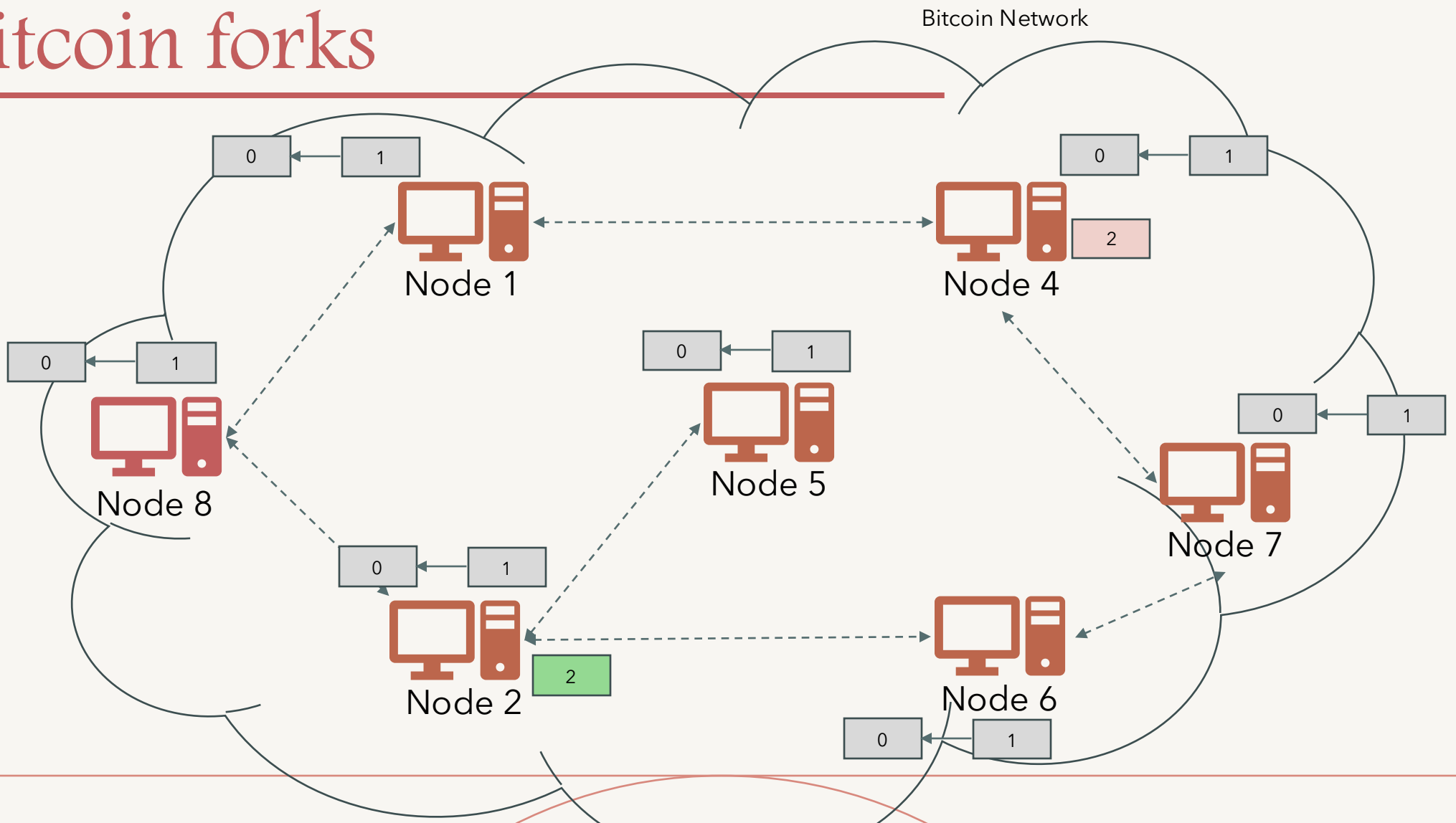
Bitcoin forks



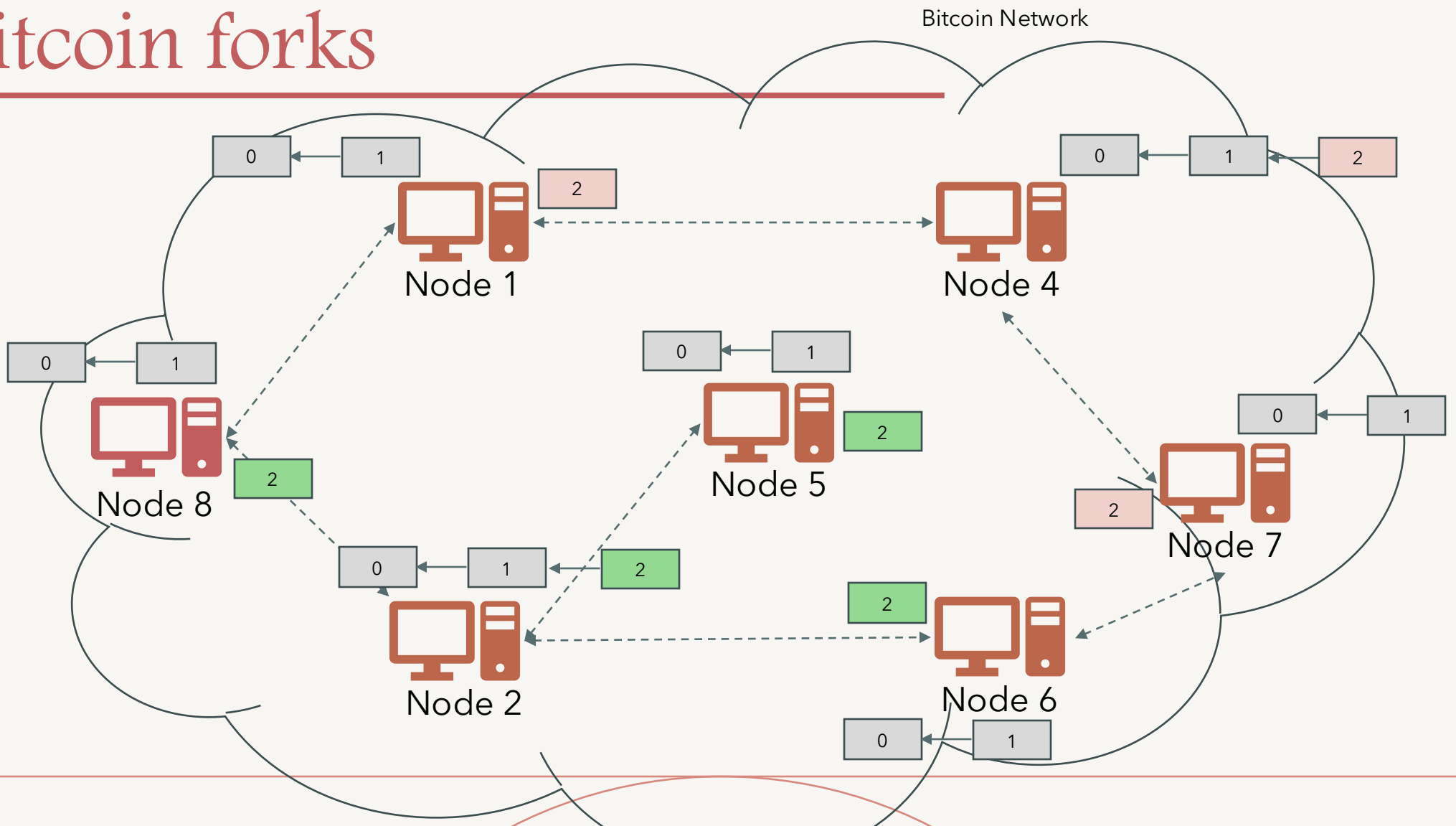
Bitcoin forks



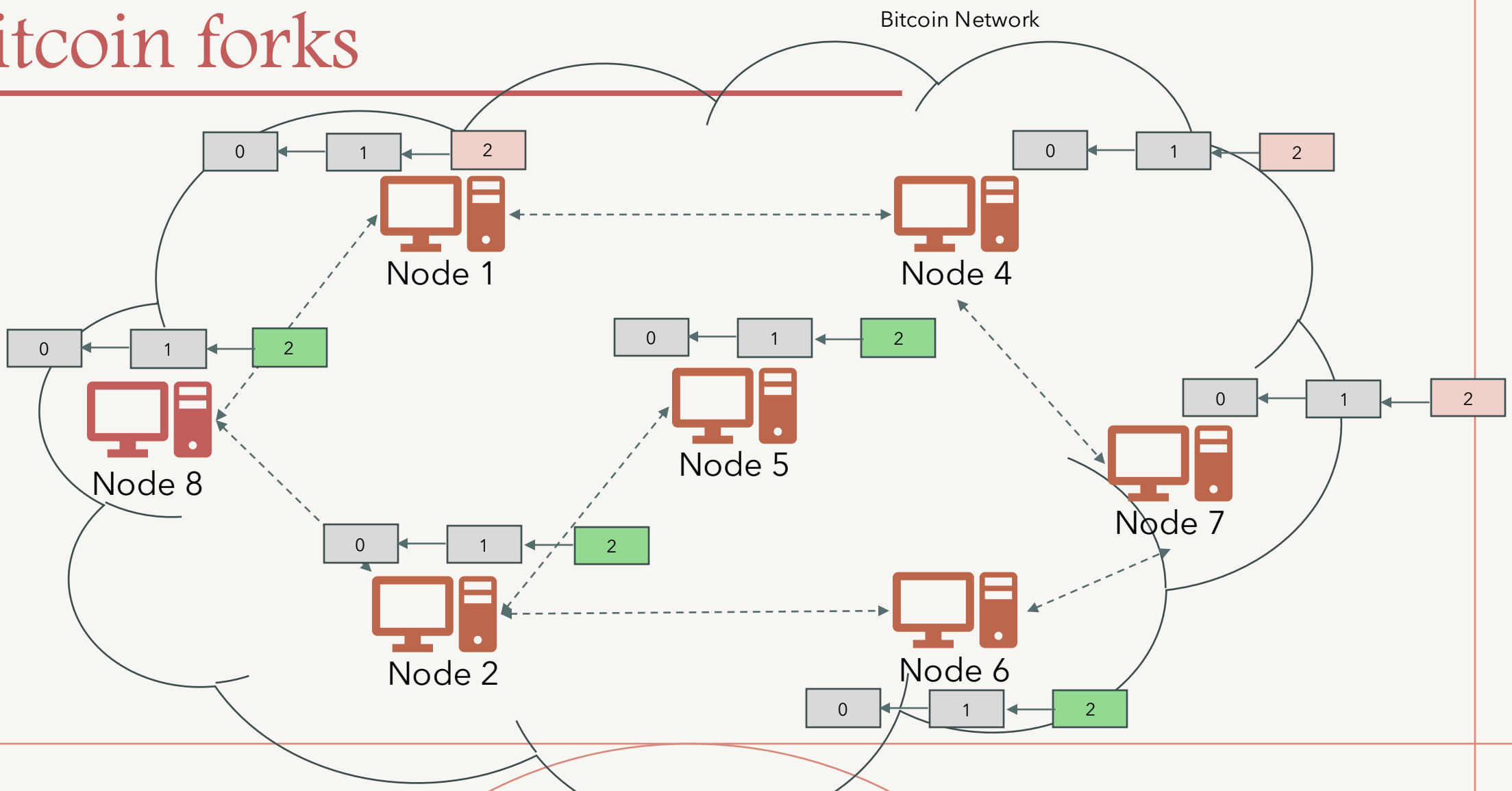
Bitcoin forks



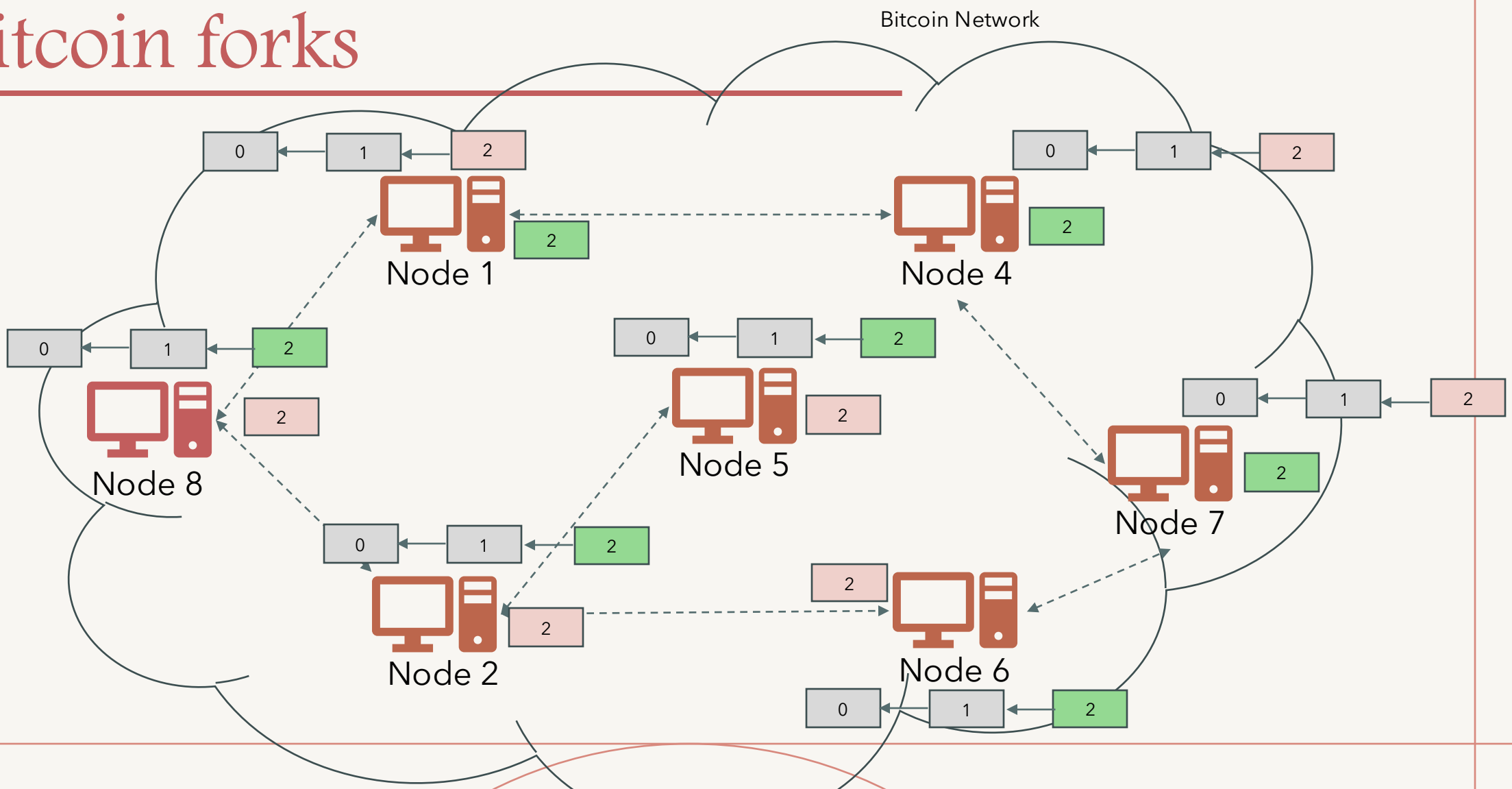
Bitcoin forks



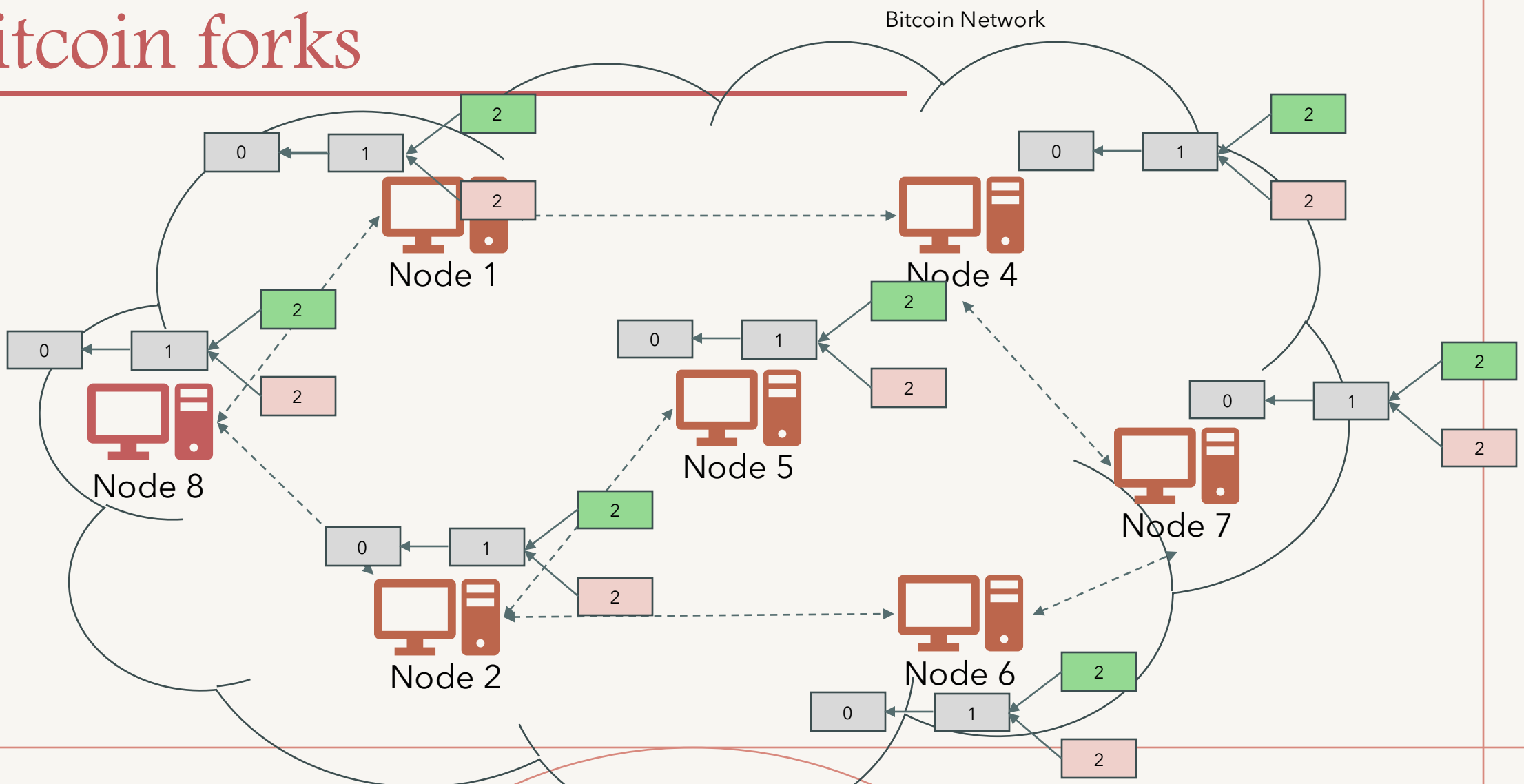
Bitcoin forks



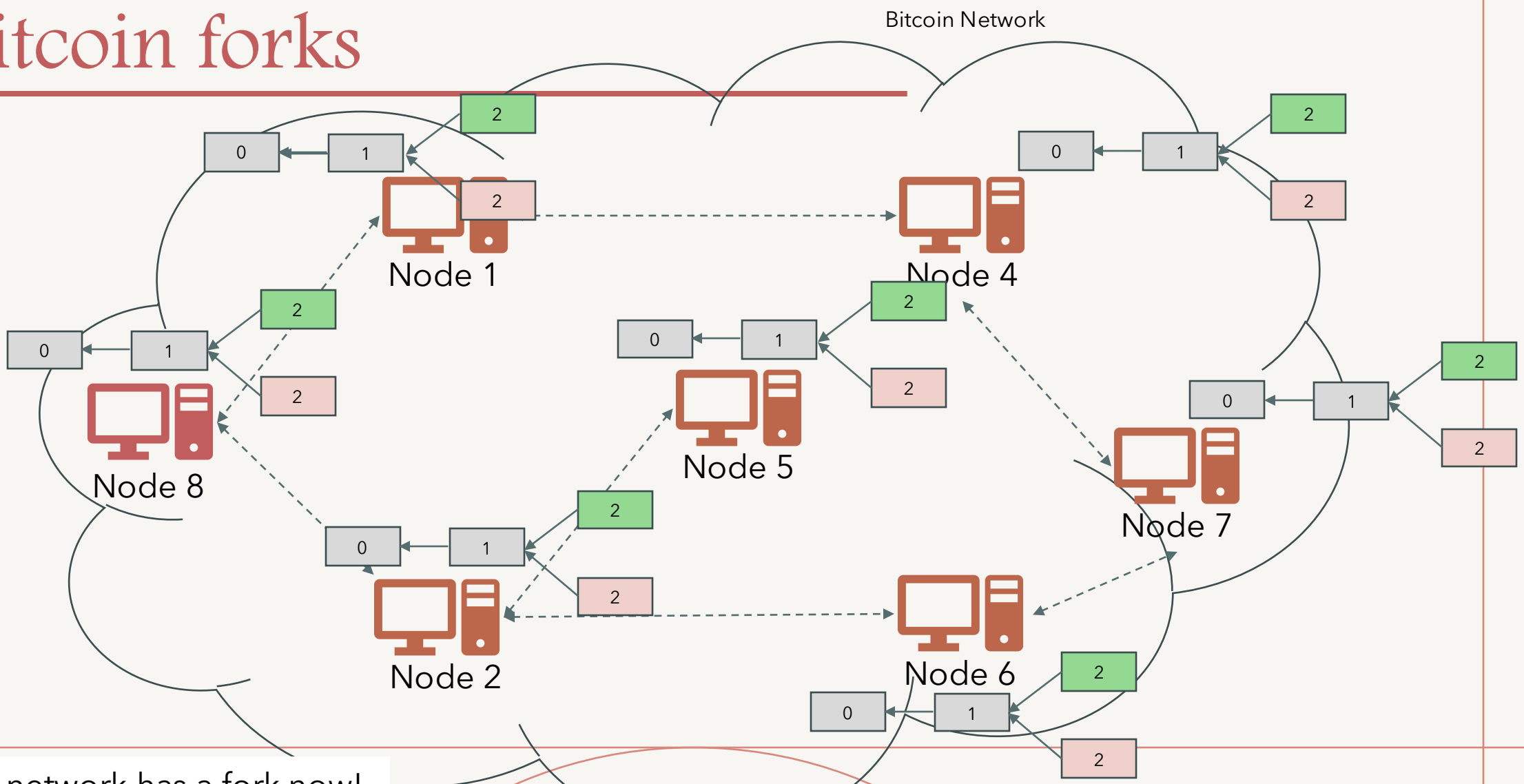
Bitcoin forks



Bitcoin forks

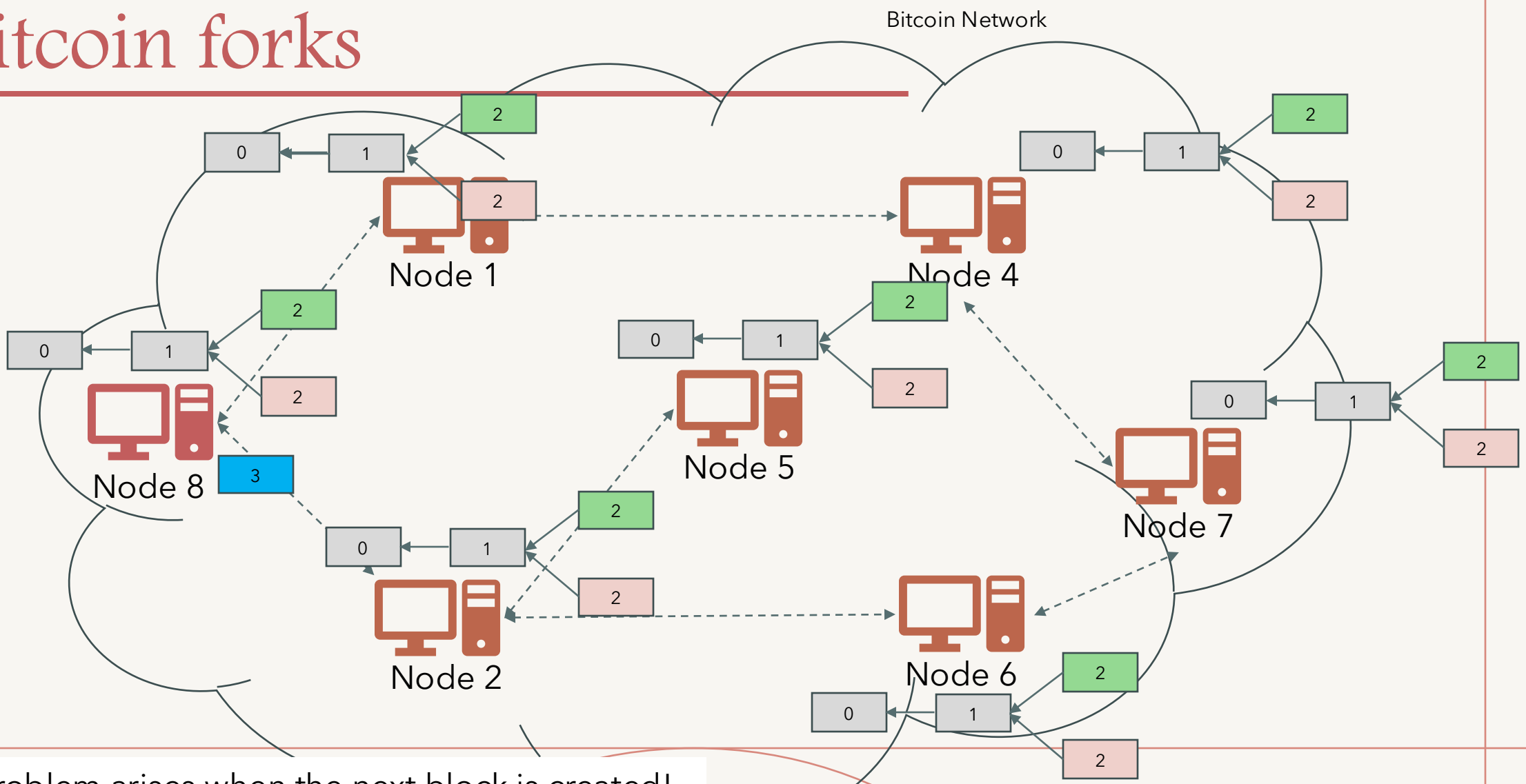


Bitcoin forks



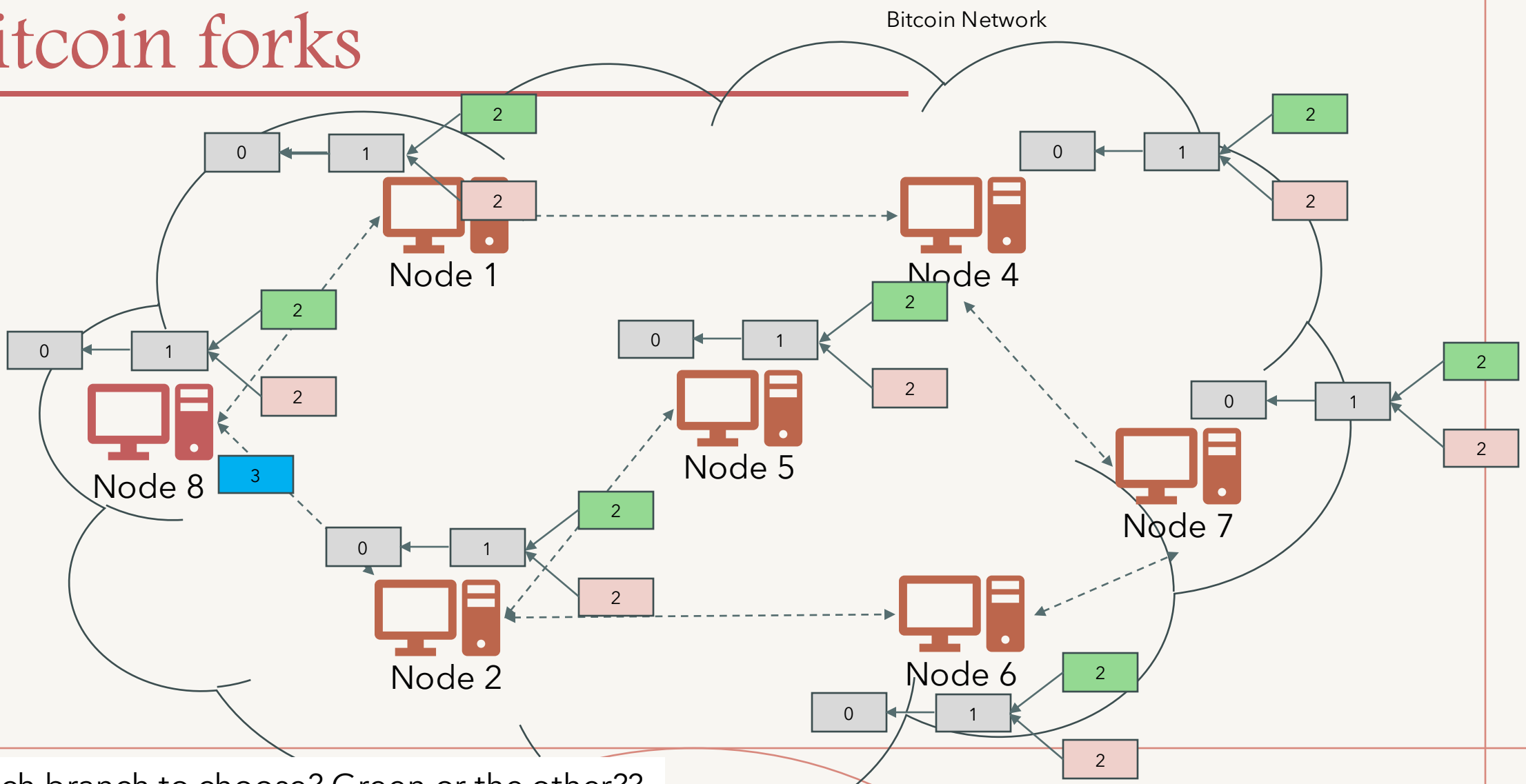
The network has a fork now!

Bitcoin forks



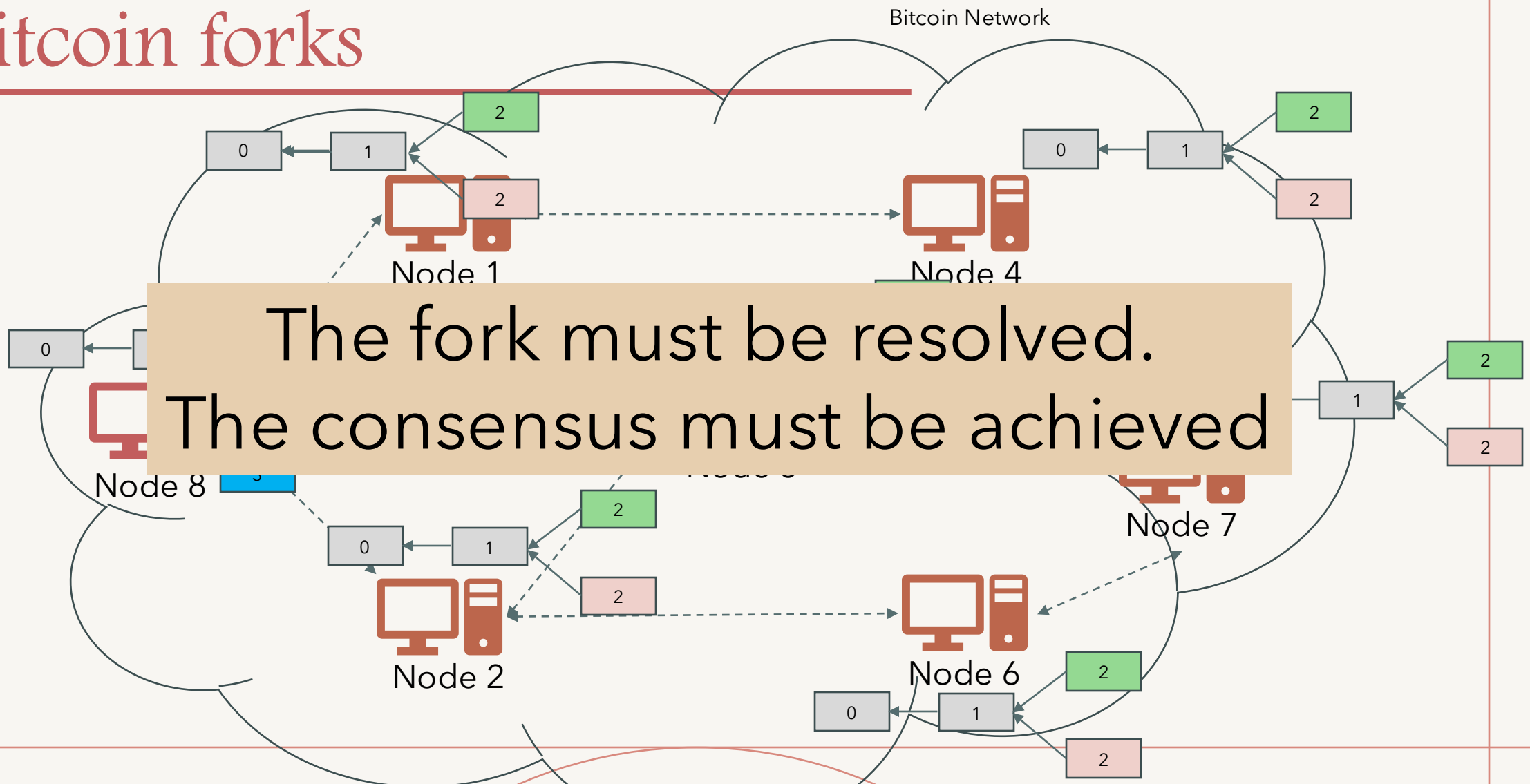
A problem arises when the next block is created!

Bitcoin forks



Which branch to choose? Green or the other??

Bitcoin forks



The fork must be resolved.
The consensus must be achieved

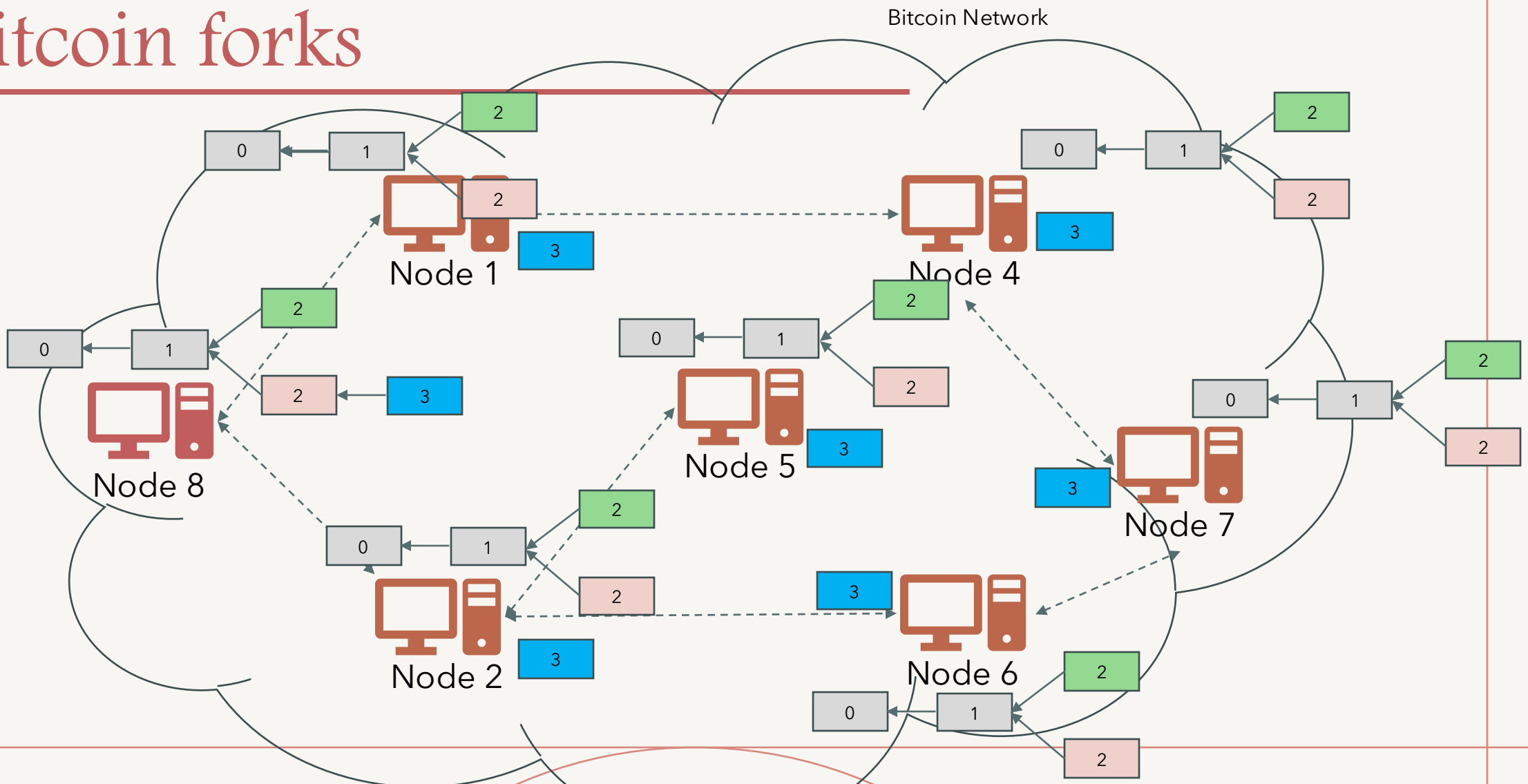
Bitcoin consensus

- To resolve the fork, each node will add the difficulty value from the genesis block to the latest block for each branch
- The nodes will select the chain with the most cumulative computation (i.e. the largest total difficulty value) demonstrated
  - Most of the time it represents the longest chain
- If the two branches have the same height having the same difficulty, we choose one at random
- The chosen block is the one on top of which we mine and/or trust for transaction confirmation

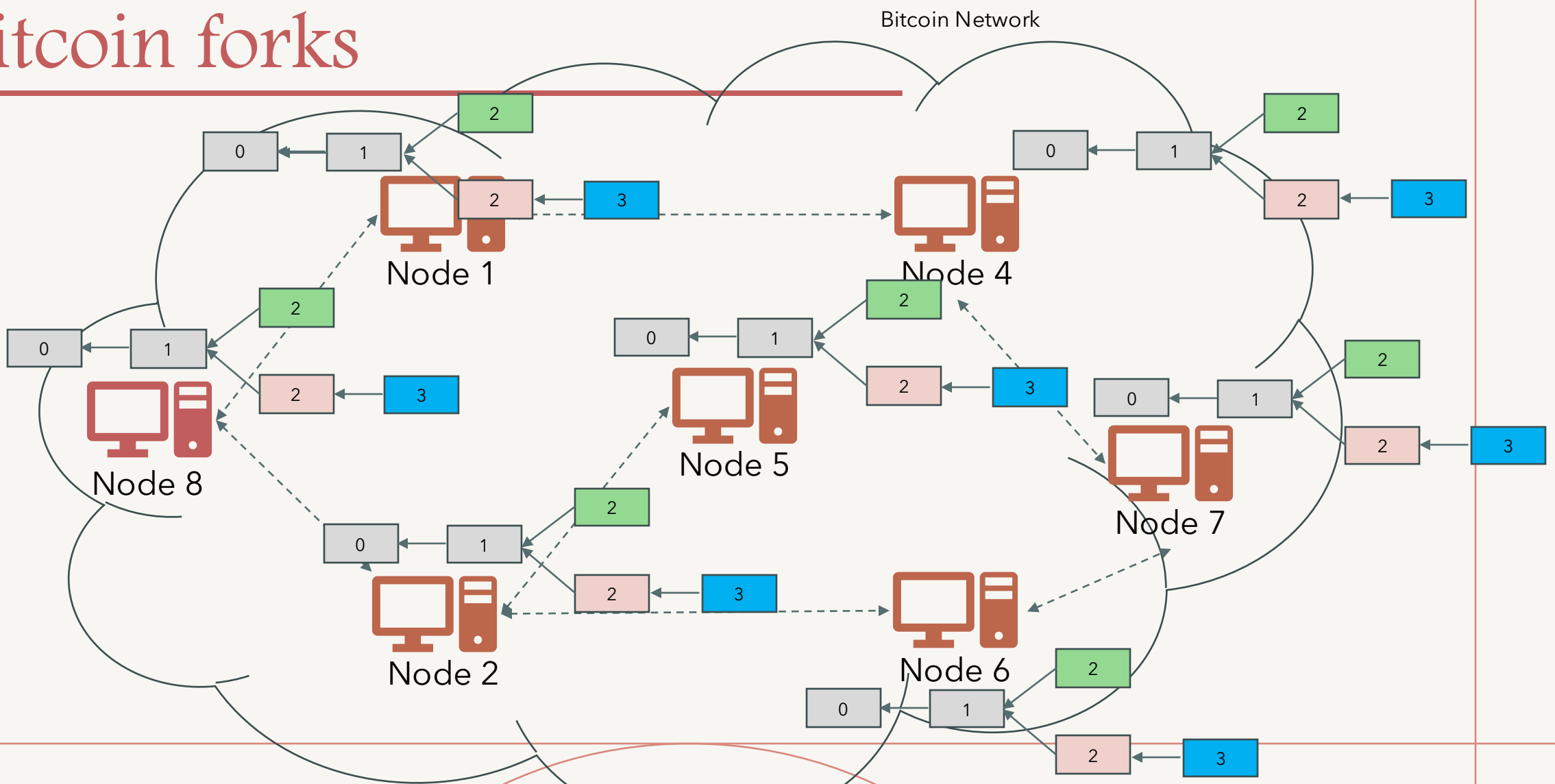
Bitcoin consensus

- Other miners start extending one of these blocks
- Over time, one of the chains starts growing over the other
  - The shortest chain is then abandoned

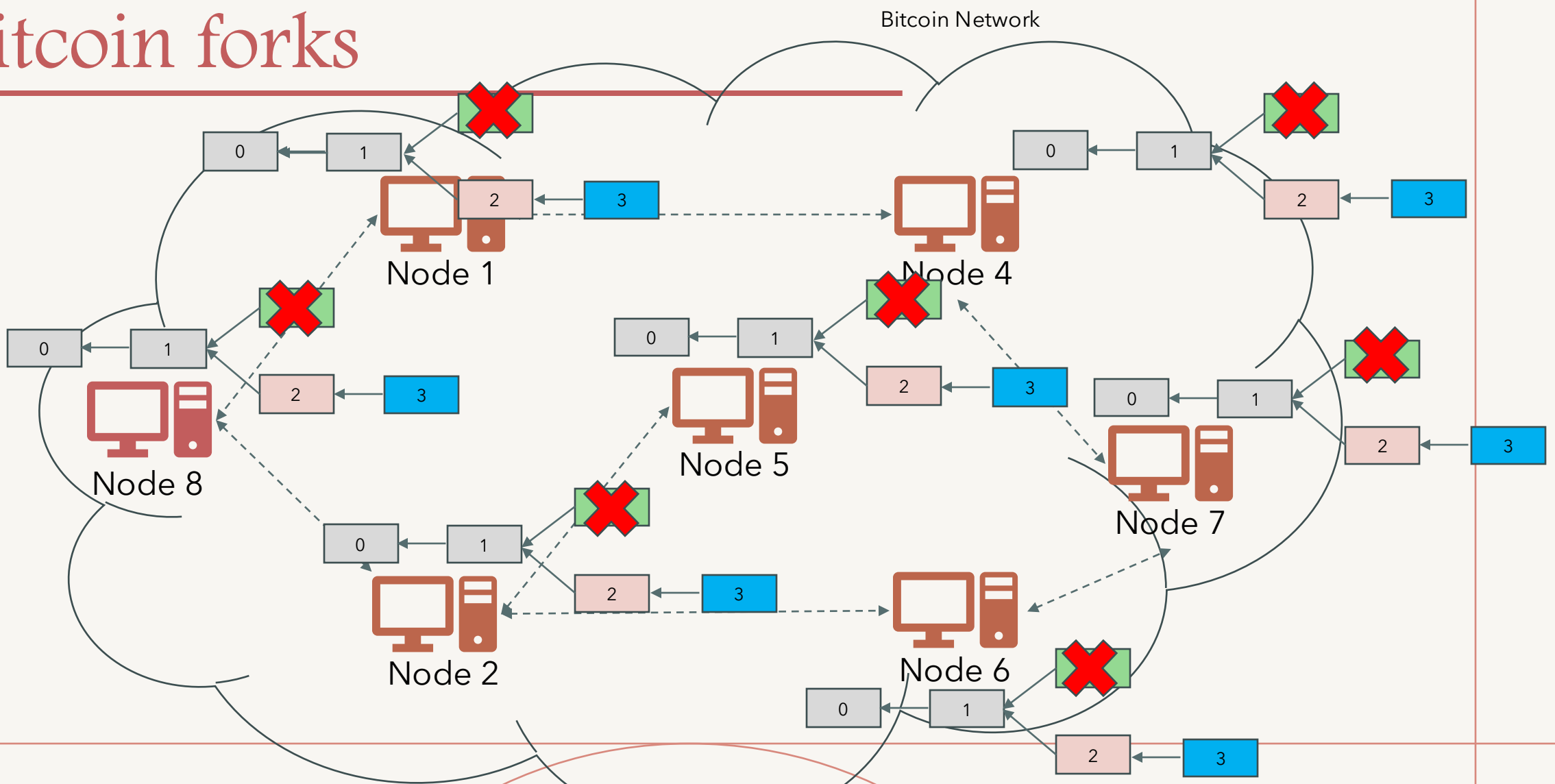
Bitcoin forks



Bitcoin forks



Bitcoin forks



Bitcoin consensus

- Transactions on the abandoned chain are checked and those are not already included are put back to the transaction pool
  - The discarded blocks are known as orphaned blocks and transactions in the orphaned block are called orphaned transactions
- Once every nodes agree to a particular chain, a consensus is achieved in a distributed fashion

Bitcoin consensus

- Order of Transactions/Blocks => Atomic Broadcast!
- New block created => A change of state!
- Every node has to agree to this => Distributed consensus!

Question?