CSE446: Blockchain & Cryptocurrencies

Lecture – 9: Bitcoin-4

Agenda

- Bitcoin components
  - Users
  - Node & Network
  - Blockchain

Bitcoin script

- Every transaction input and output use the scripting capability in Bitcoin
- Bitcoin script allows a user to impose a restriction (condition) as to which user can use it
- scriptPubkey is called the locking script as it locks the value in the output to a certain bitcoin address
  - Only who can prove that they own that address can use this bitcoin

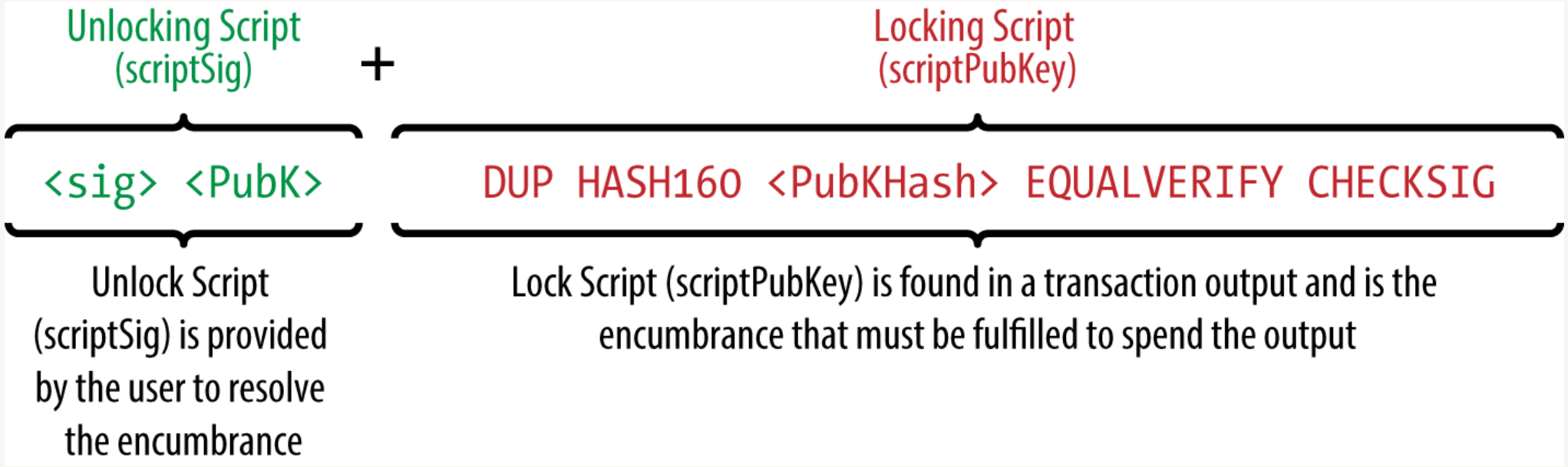
https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06.asciidoc

Bitcoin script

- When someone would like use a tx output, they need to use it as a transaction input
- A proof is needed to claim the ownership of the tx input
- scriptSig is the required proof
- scriptSig contains a digital signature which unlocks the locking script
  - Digital signature proves the ownership over the locked Bitcoin address

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06.asciidoc

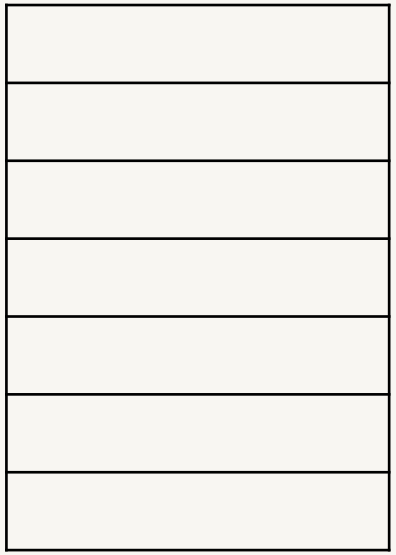
Bitcoin script locking + unlocking



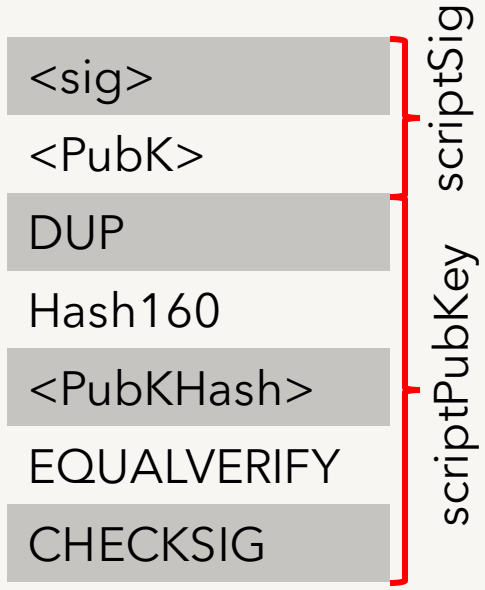
Move from left to right

Source: http://chimera.labs.oreilly.com/books/1234000001802/ch05.html

Bitcoin script locking + unlocking

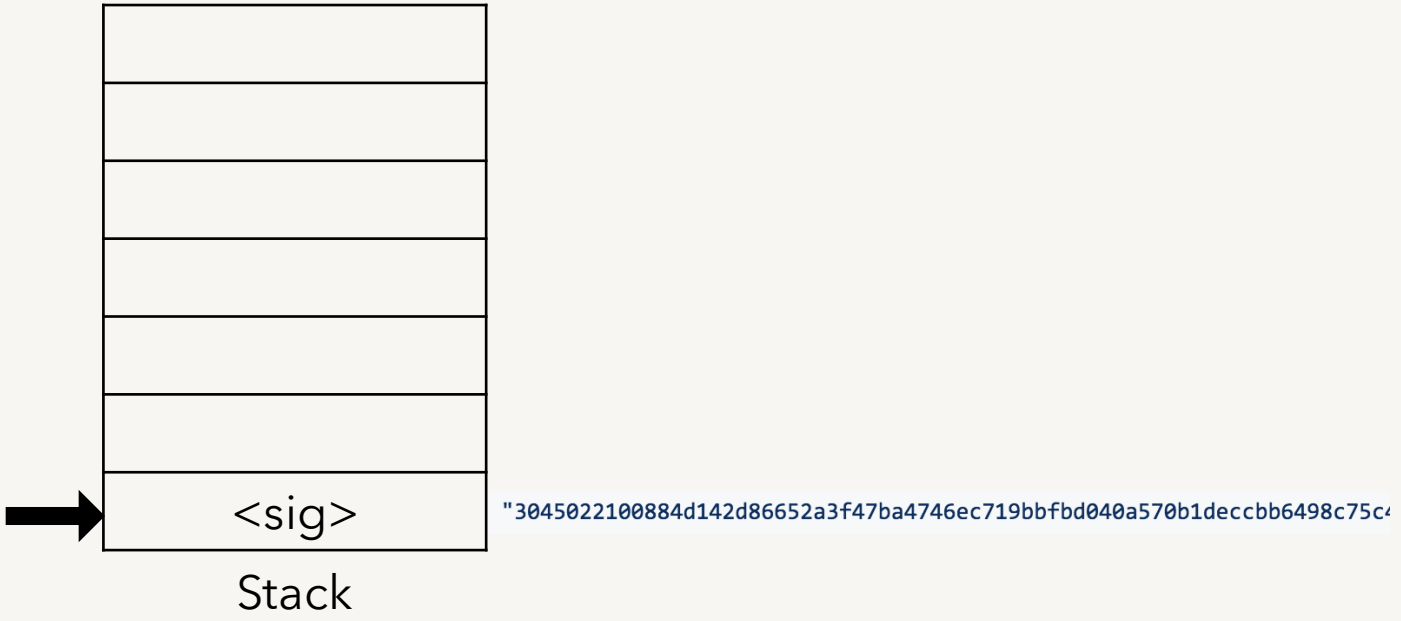


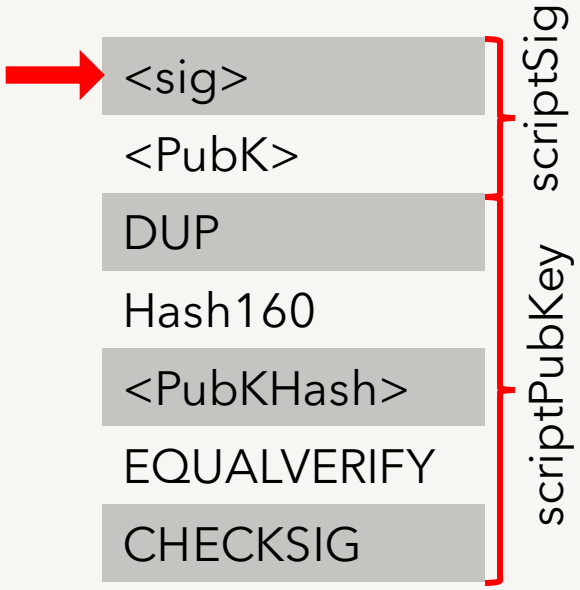
Stack



- Bitcoin uses a stack as presented in the left
- Locking and unlocking script are placed as shown in the right
- The script is executed line by line, top to bottom for this figure
- Explanation is added here

Bitcoin script locking + unlocking

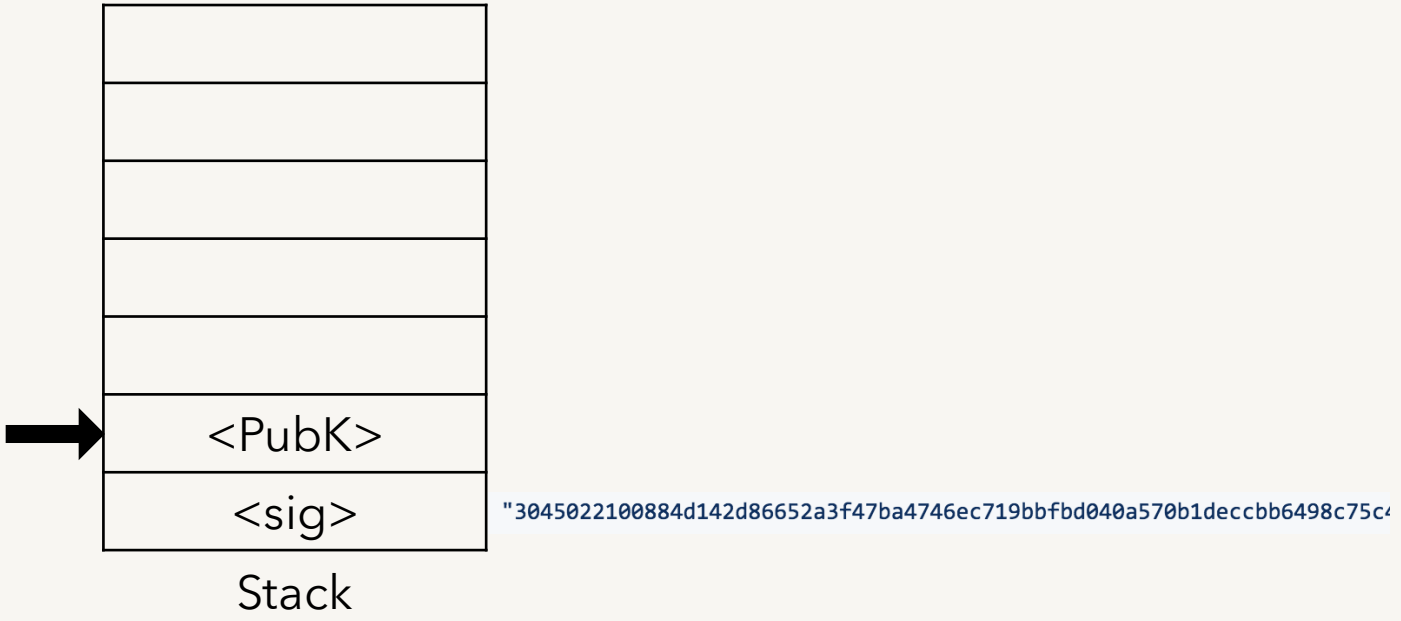




Current command: <sig> represents the signature in the input

- The signature from the input is pushed in the stack
- The black arrow represents the current top item in the stack

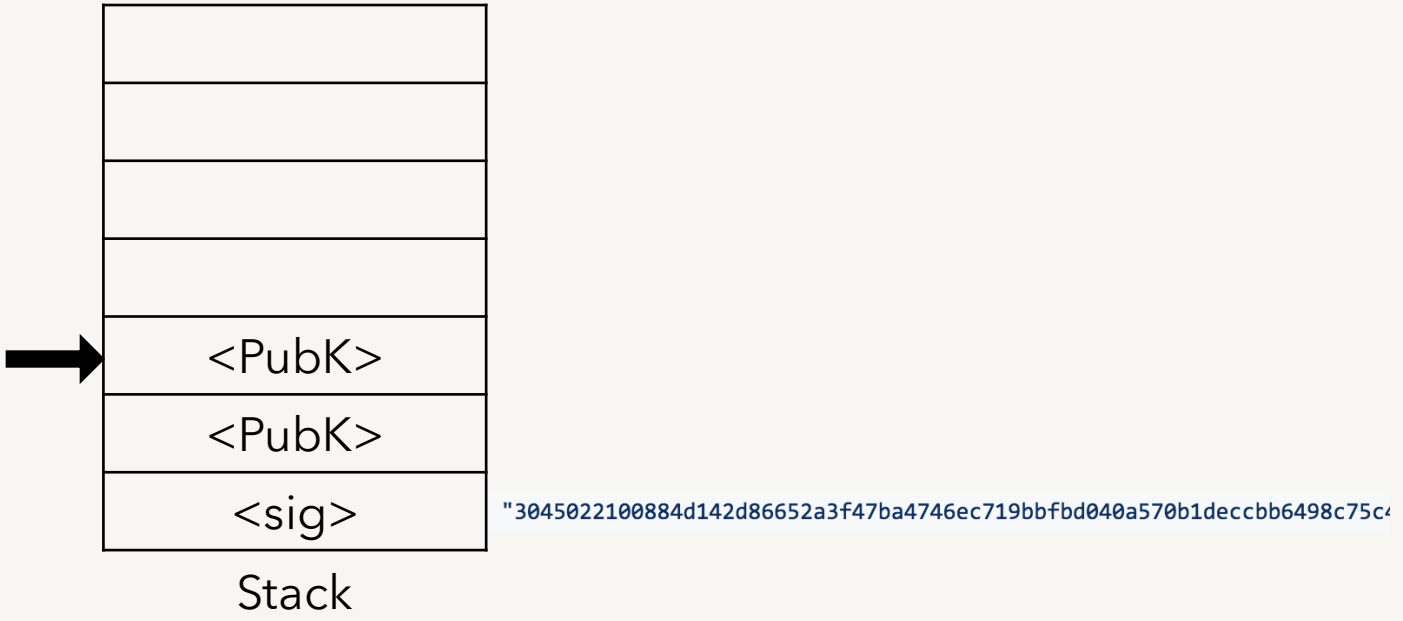
Bitcoin script locking + unlocking

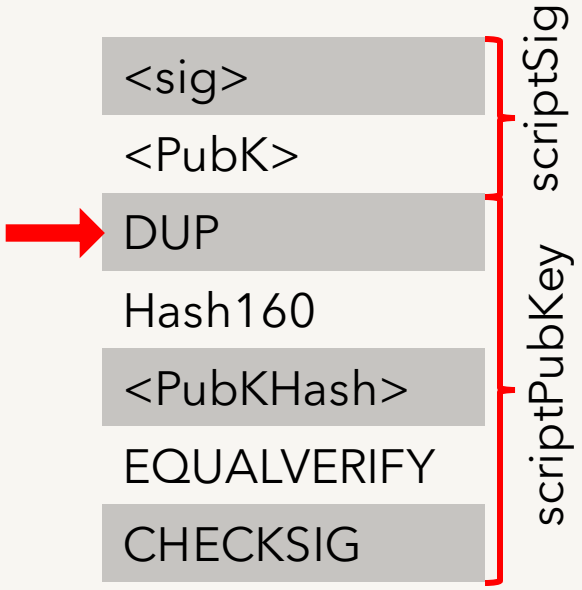


Current command: <PubK>

- The public key of the input is pushed in the stack

Bitcoin script locking + unlocking





Current command: <DUP>

- The DUP command duplicates the value from the top of the stack and pushes it in the stack
- In real bitcoin script, <DUP> is represented with <OP_DUP>

Bitcoin script locking + unlocking

Current command: <Hash160>

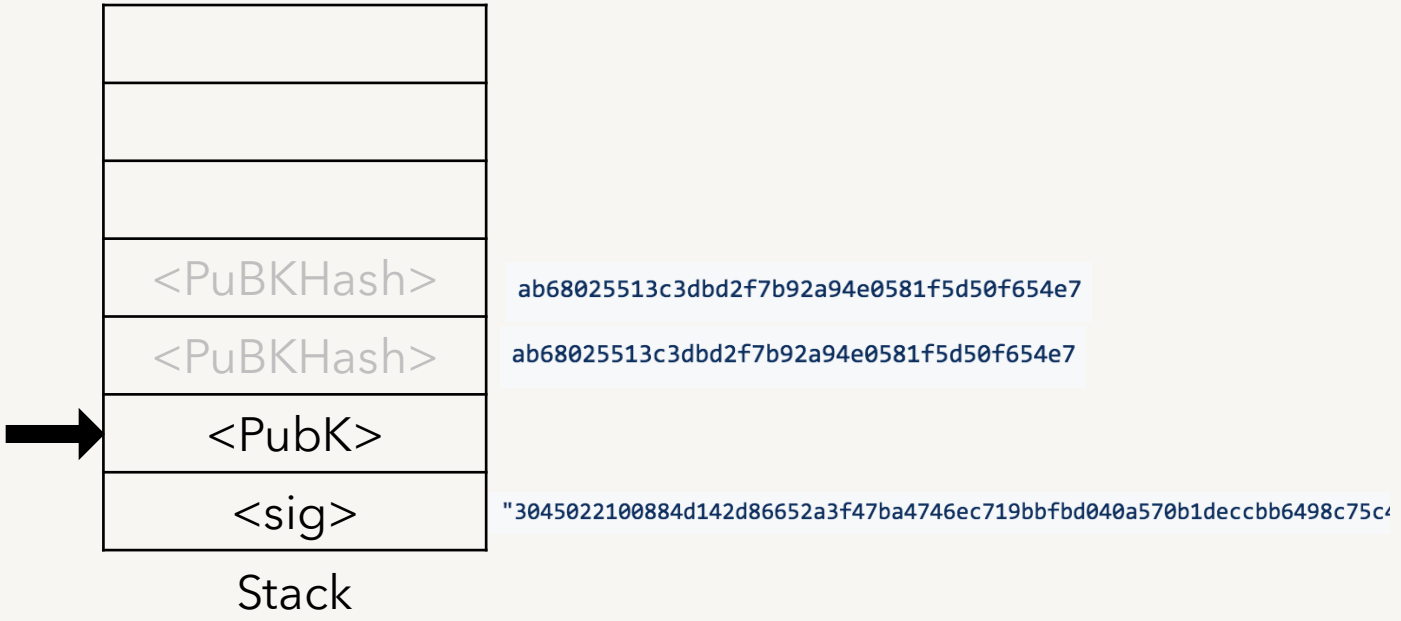
- The Hash160 command pops the top item from the stack, creates its hash and pushes the hash back in the stack
- In real bitcoin script, <Hash160> is represented with <OP_Hash160>

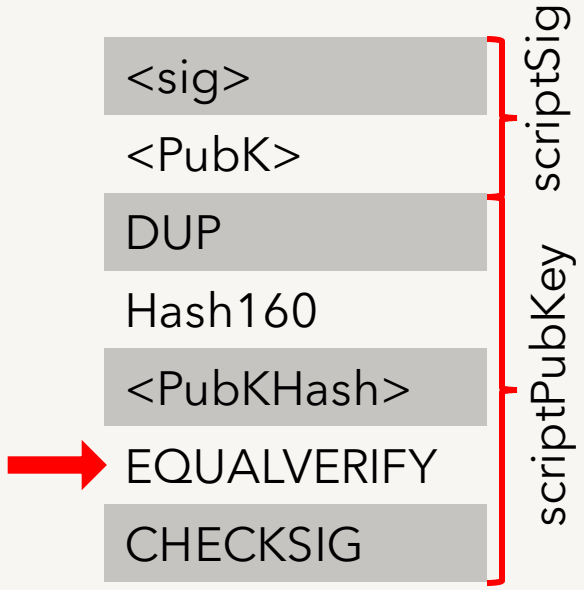
Bitcoin script locking + unlocking

Current command: <PubKHash>

- The public key hash specified in the tx output is pushed to the stack

Bitcoin script locking + unlocking

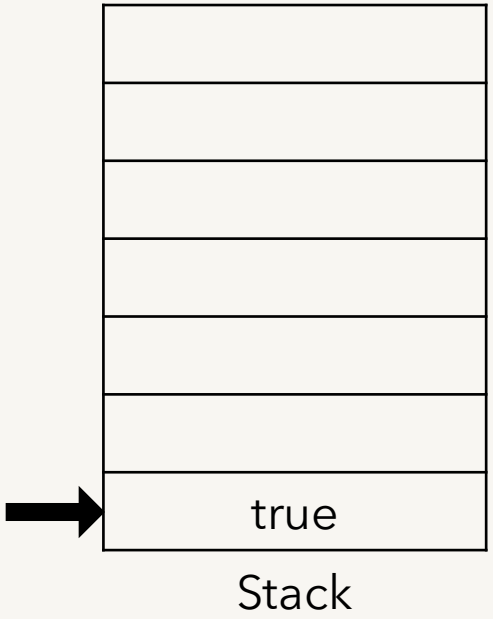


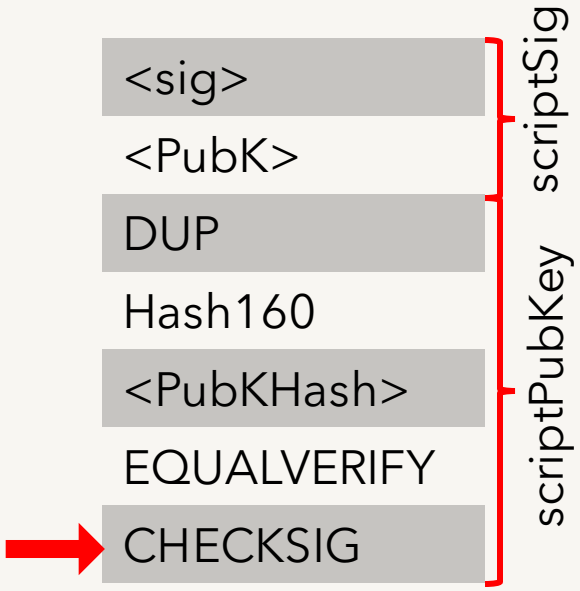


Current command: <EQUALVERIFY>

- This command checks if the top two items in the stack are equal or not. If not equal, an error is thrown. Otherwise two items are popped from the stack
- In real bitcoin script, <EQUALVERIFY> is represented with <OP_EQUALVERIFY>

Bitcoin script locking + unlocking





Current command: <CHECKSIG>

- This command pops two items from the stack and verifies the signature using the public key. If the verification is successful, a true value is pushed otherwise a false value is pushed. In real bitcoin script, <CHECKSIG> is represented with <OP_CHECKSIG>

Transaction verification

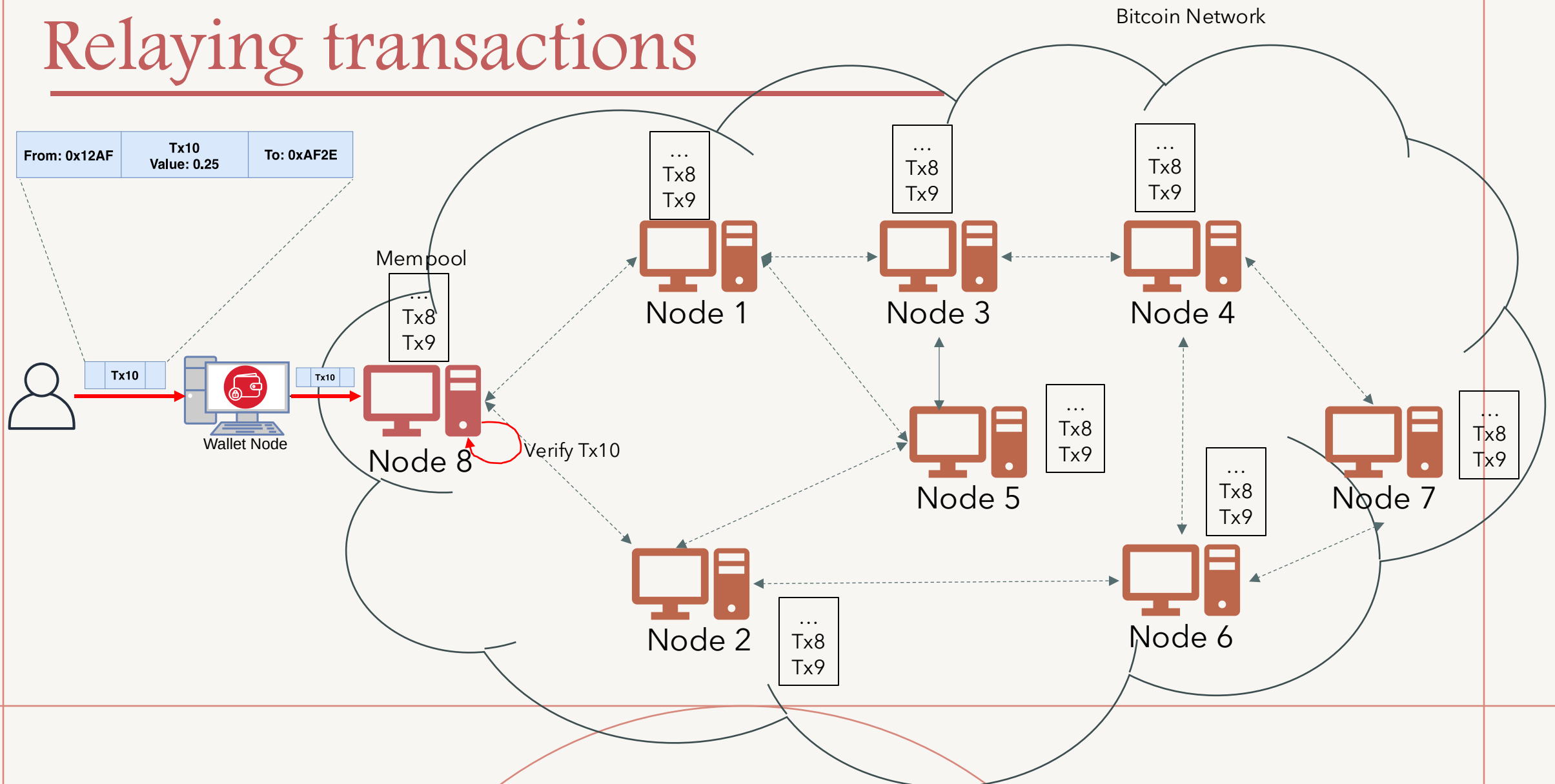
- When a node receives a transaction, it verifies the transaction with a number of steps
  - Check syntactic correctness
  - Make sure neither in (except for a coinbase tx) or out lists are empty
  - Reject if we already have matching tx in the pool, or in a block in the blockchain
    - Every node maintains a transaction pool called mempool, consisting of txs not inserted in a block yet
  - For each input, if the referenced output does not exist (e.g. never existed or has already been spent), reject this transaction
  - Reject if the sum of input values < sum of output values

Transaction verification

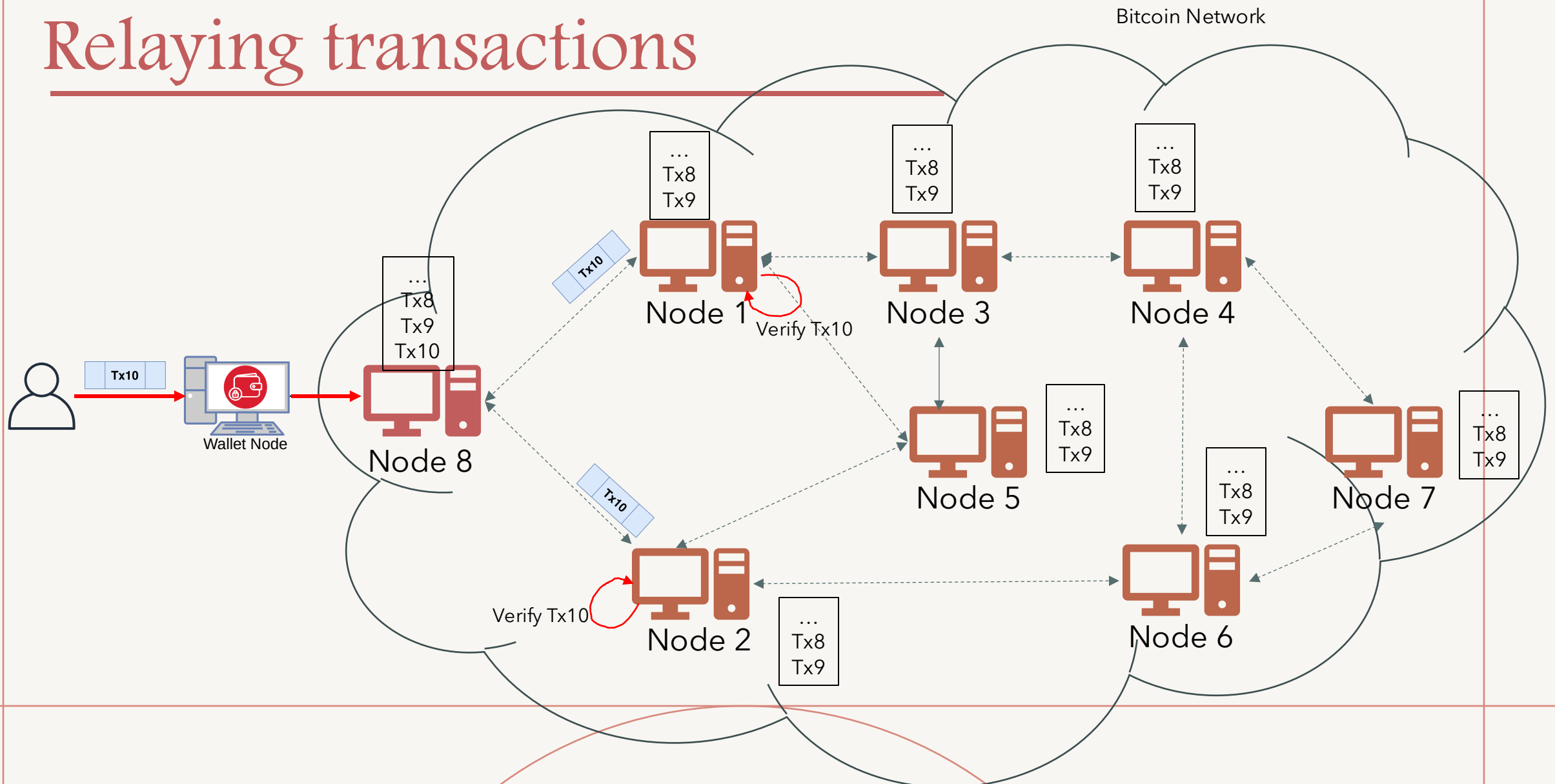
- Reject if transaction fee (defined as sum of input values minus sum of output values) would be too low to get into an empty block
- Verify the scriptPubKey accepts for each input; reject if any are bad

- If the verification is successful:
  - Add it to a transaction pool inside the node (mempool)
  - Add it to wallet if the output belongs to the addresses controlled by the user's wallet
  - Relay the transaction to peers

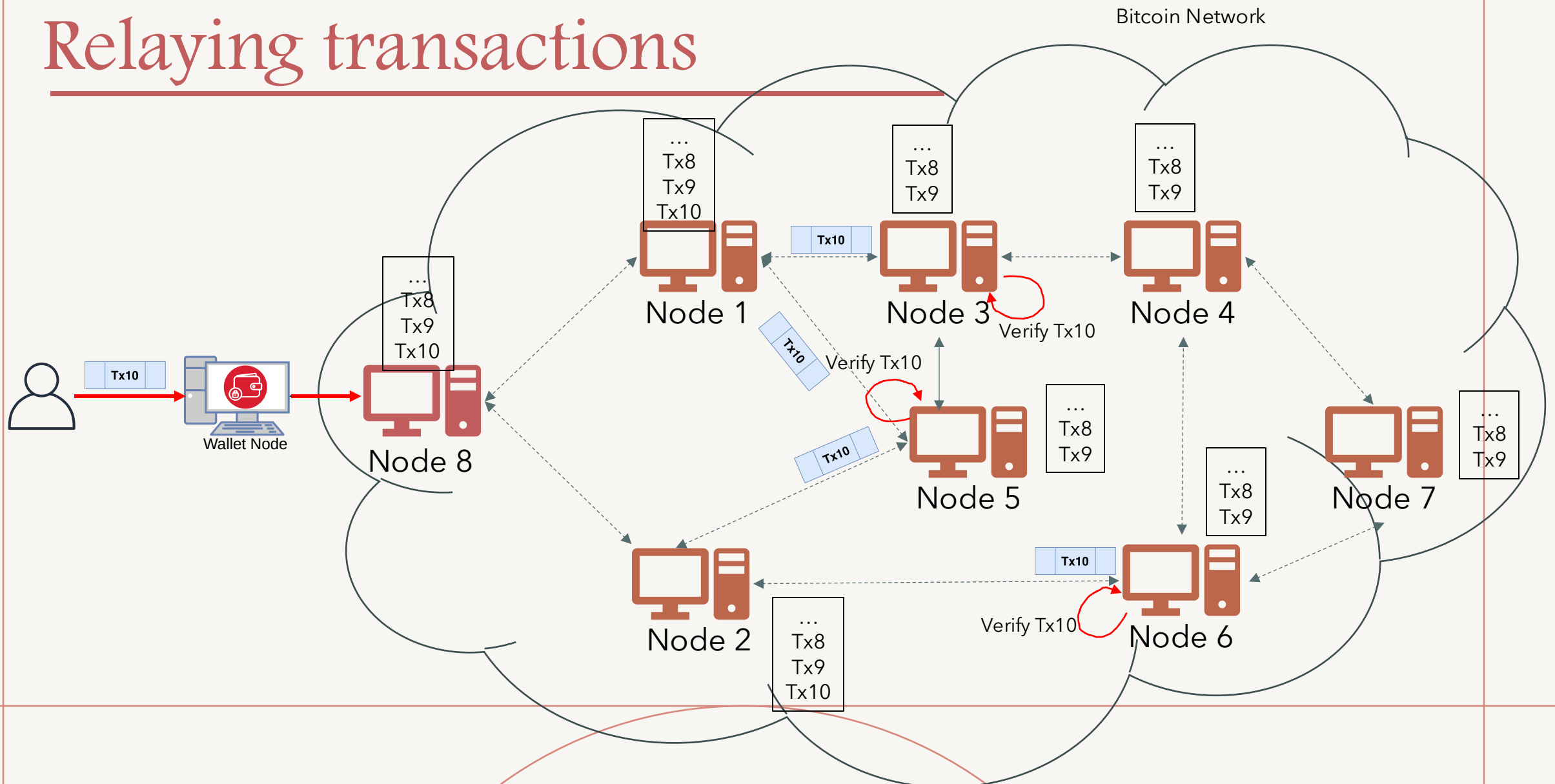
Relaying transactions



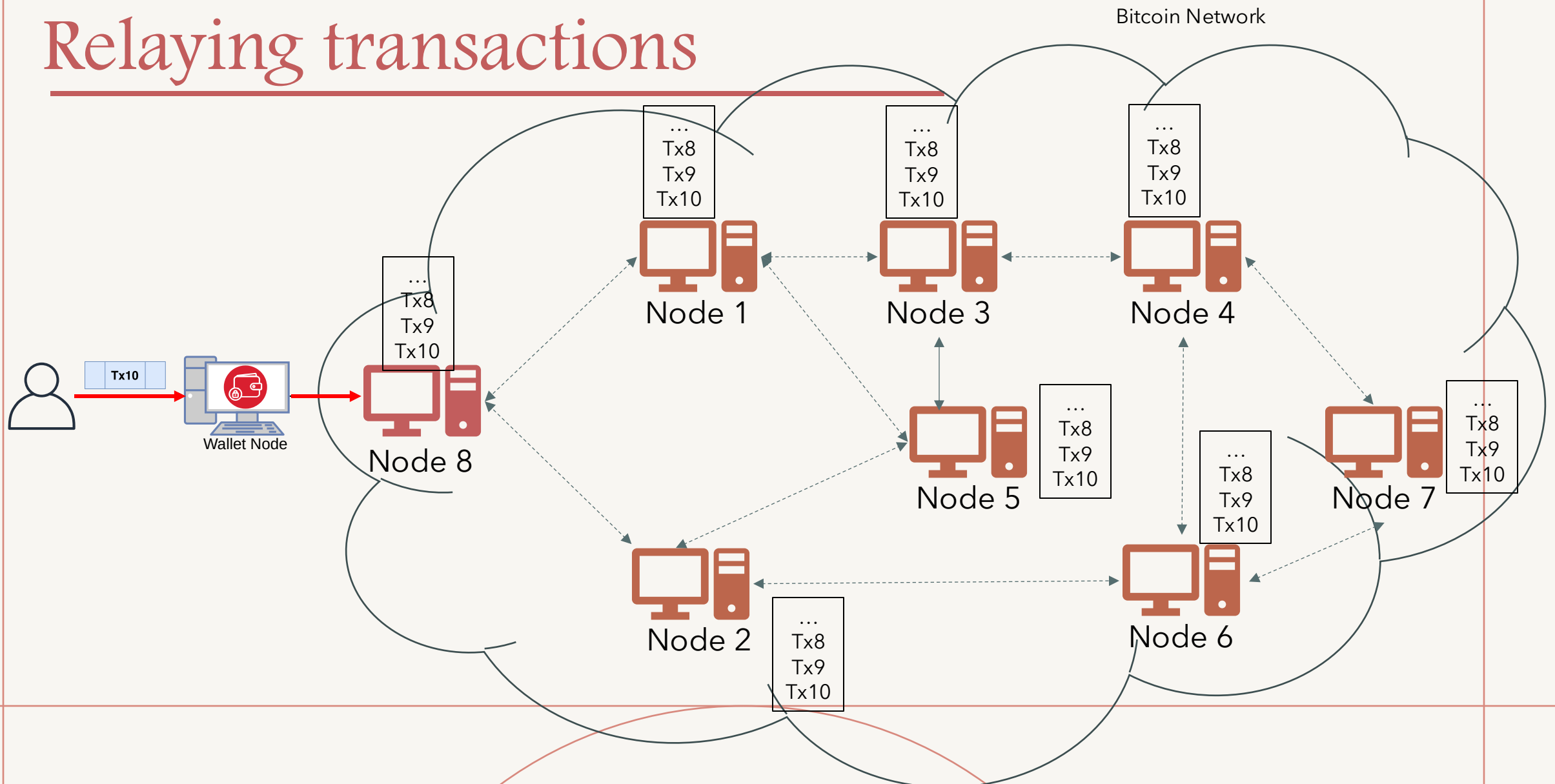
Relaying transactions



Relaying transactions



Relaying transactions



Block

- Relayed transactions are combined into a block
- A newly created block contains the most recent transactions that did not exist in previous blocks
  - Each transaction can appear **only once** in a block
- Each block is also propagated into the network
- Each block is identified by an identifier, called block id
  - The block id is created by double-hashing the block header (discussed later)
- The network is set to create **one block every 10 minutes**
- A transaction in a valid block is called confirmed

Block

Table 1. The structure of a block

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1–9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch09.asciidoc

Block

Table 2. The structure of the block header

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

Pointer to the previous block

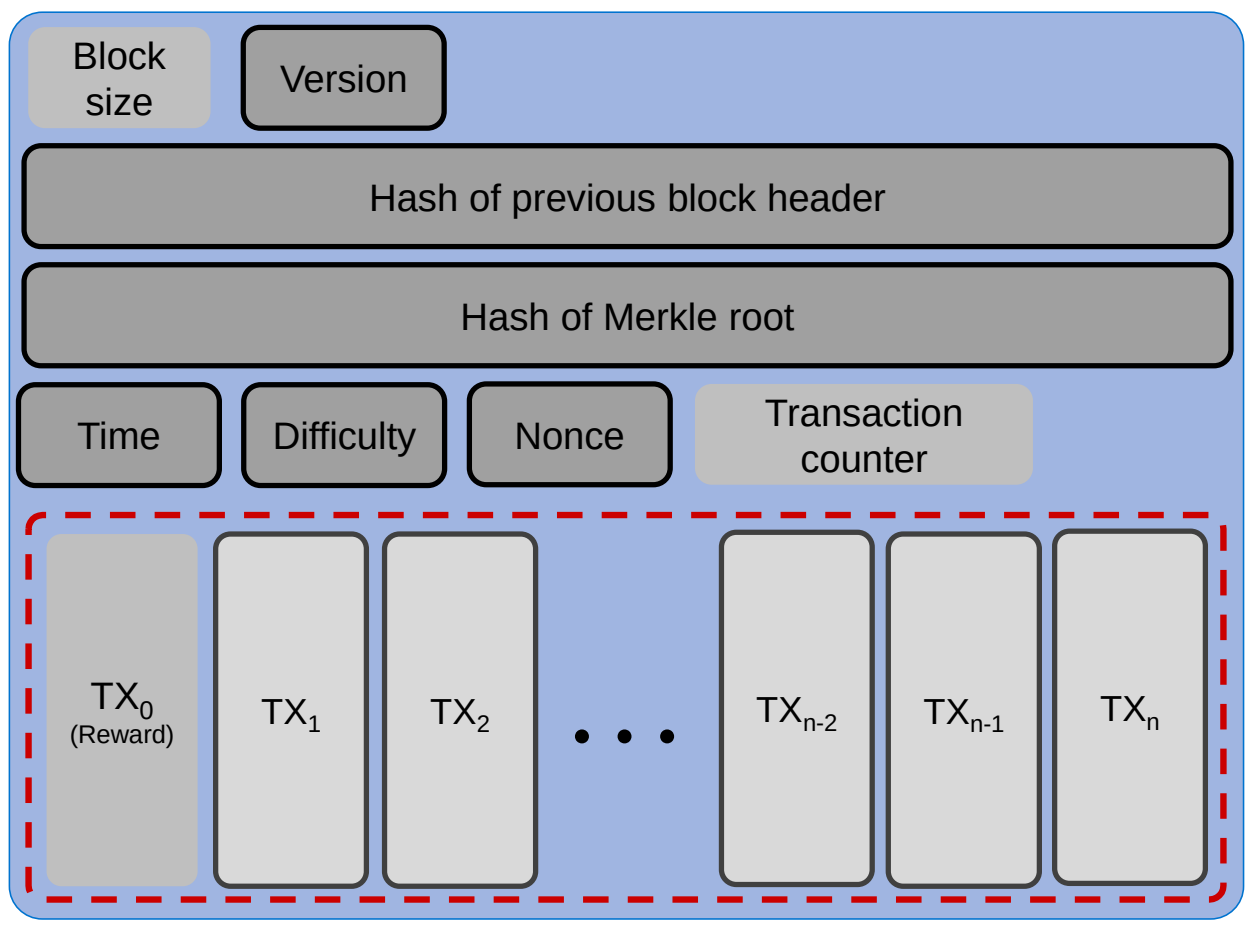
A hashed data structure of all Transactions in the block

Time when this block is created

These two fields are used to achieve consensus, will be discussed later

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch09.asciidoc

Block

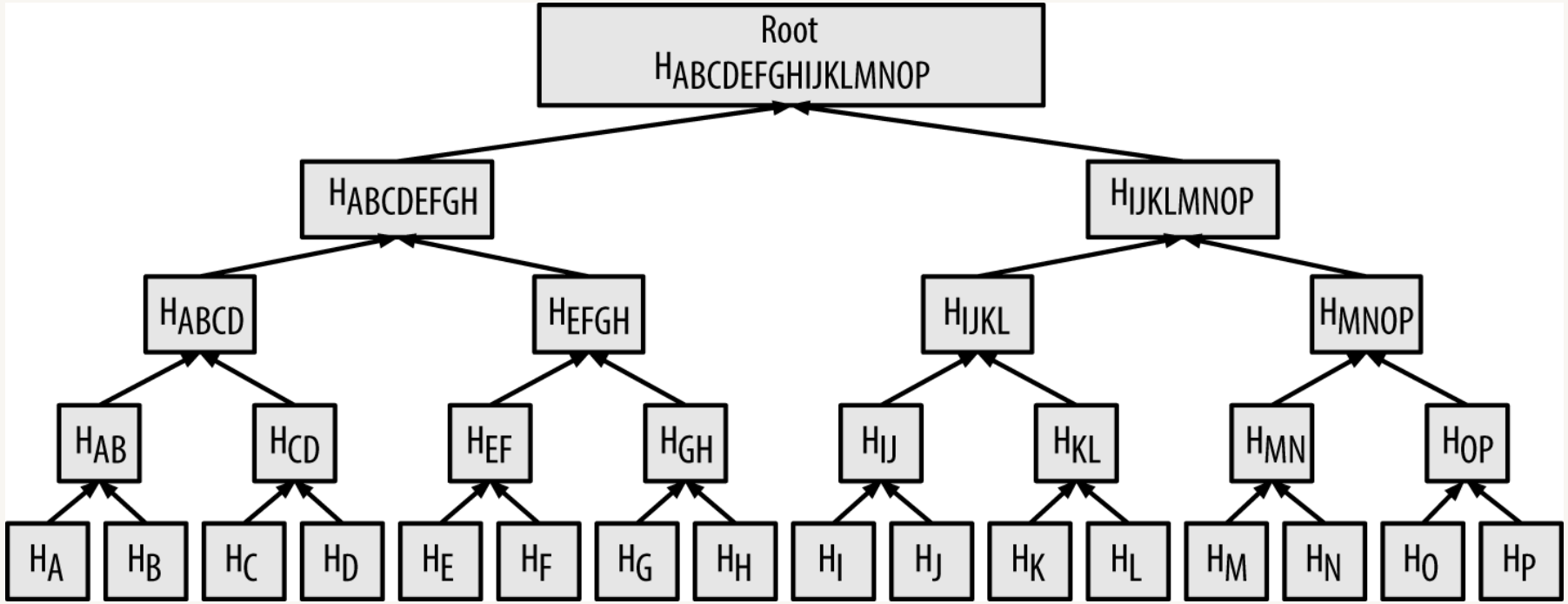


Bitcoin Basics- Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Block

- Merkle trees are used in bitcoin to summarise all the transactions in a block
  - producing an overall digital fingerprint of the entire set of transactions
  - providing a very efficient process to verify the inclusion of a transaction (proof of membership)
- A merkle tree is a balanced binary tree, containing an even number of leaf nodes
  - if a tree needs to be constructed with an odd number of leaf nodes, the last element is duplicated
- It is constructed by recursively hashing pairs of nodes until there is only one hash, called the *root*, or *merkle root*
- The cryptographic hash algorithm used in bitcoin's merkle trees is SHA256 applied twice, also known as double-SHA256

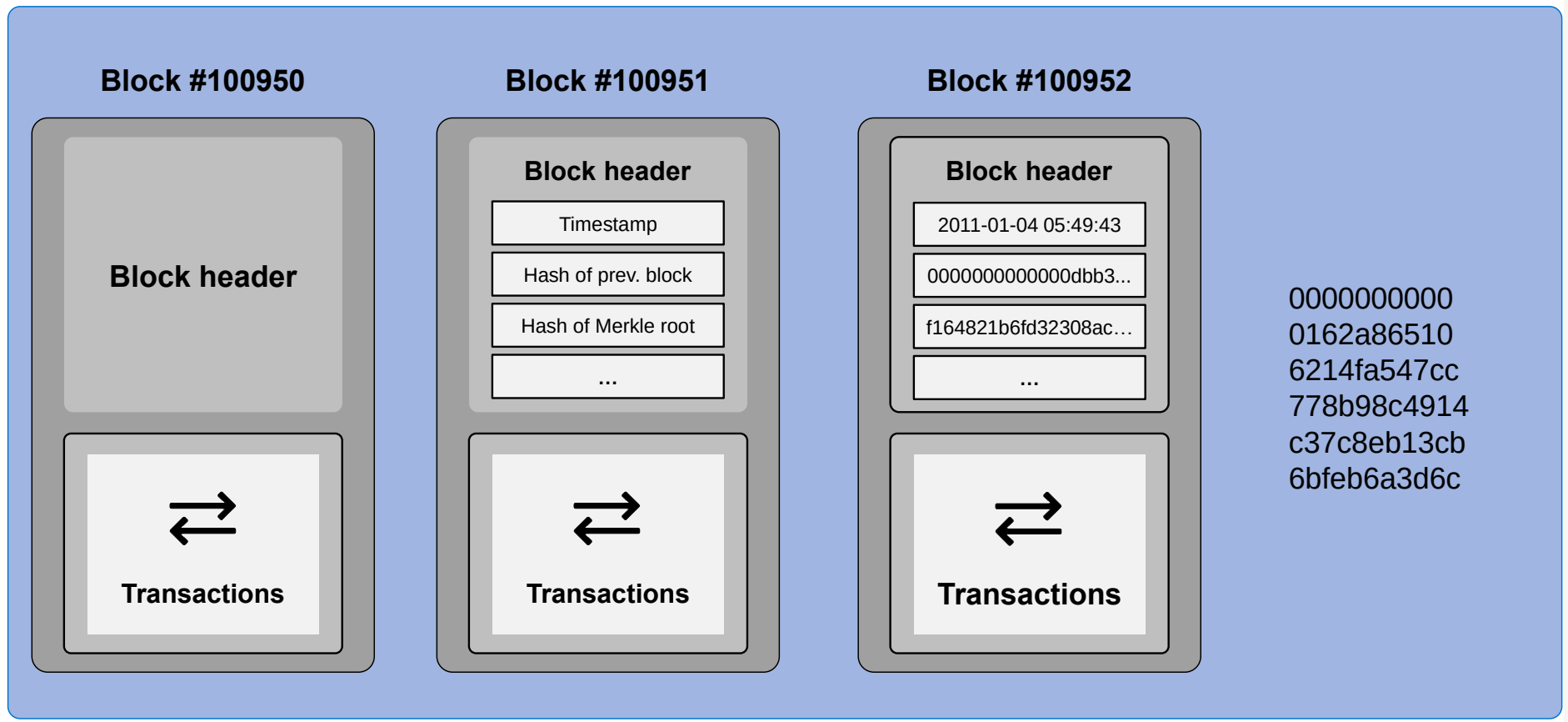
Block



$H_A = SHA256(SHA256(TX_A)$, $H_{AB} = SHA256(SHA256(H_A \| H_B)$

https://raw.githubusercontent.com/bitcoinbook/bitcoinbook/develop/images/mbc2_0904.png

Blockchain



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

Bitcoin mining

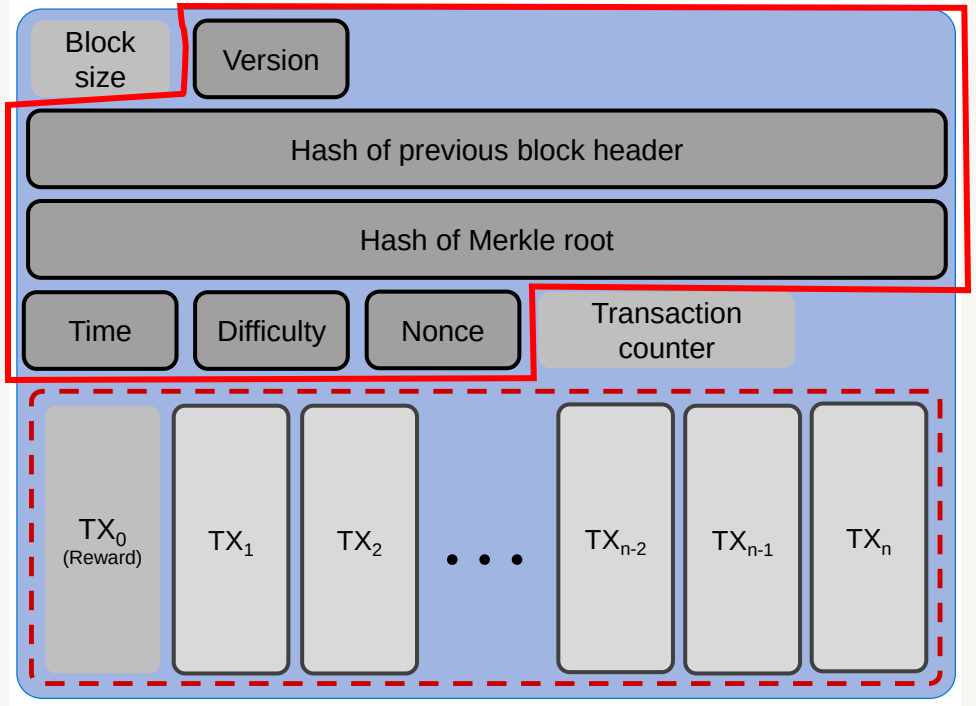
- Every miner node listens for transactions and puts them in its transaction pool (mempool)
- From the pool, transactions are combined to form a block
- Forming a block is not enough, a valid block needs to be created
- To create a valid block, a “proof of work” needs to be provided
  - It resembles 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

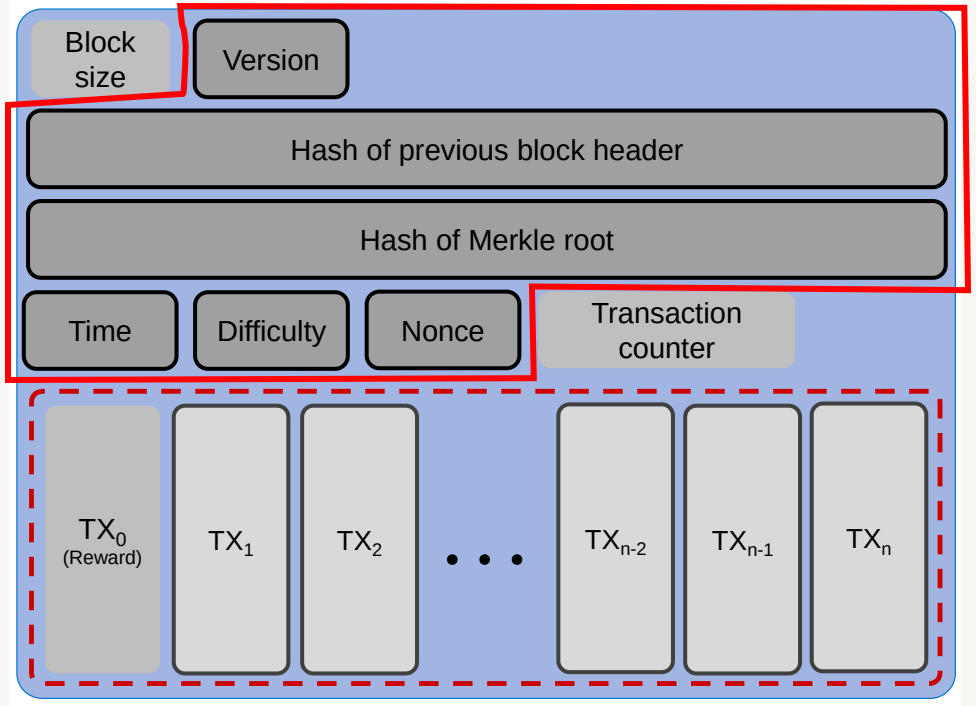
- It combines several data from the block header and tries to find a value which matches a certain condition
- These six fields are used to calculate the header hash
  - E.g. to calculate the hash of the previous blocks, these six values from the previous block header are double hashed with SHA-256
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

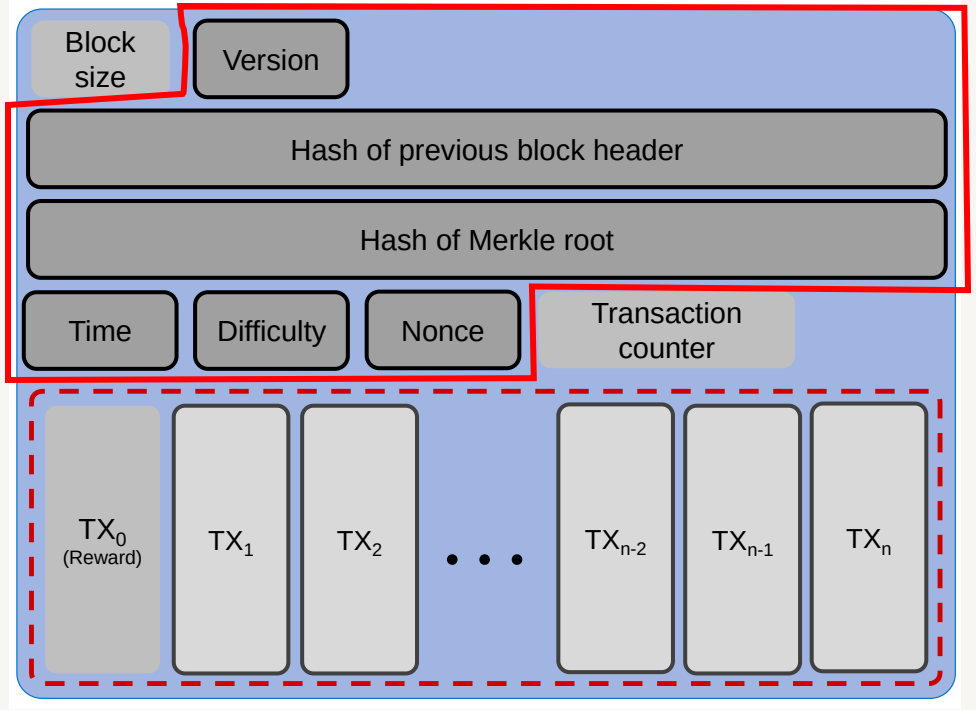
- V: Version is a fixed number representing the protocol rule used for this particular block
- M: Hash of Merkle root is the merkle root of all transactions in the block
- T: Time is a UNIX epoch time (number of seconds elapsed since 00:00:00 UTC on 1 January 1970)
- D: Difficulty is a dynamic value 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

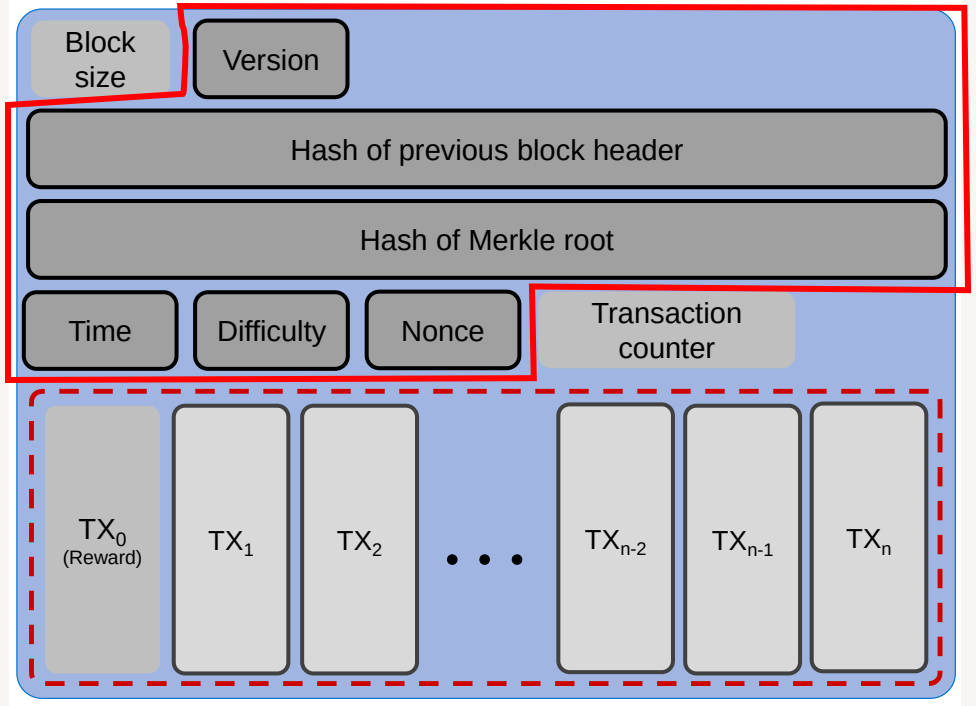
- So the search puzzle is this:
  - SHA256(SHA256(V || H || M || T || N)) < D
- V is mostly same
- H is same for all nodes (why?)
- T is same (very unlikely, but let's assume this)
- Assuming all nodes have the same txs in their mempool, M will never be same (why??)



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

Bitcoin mining: PoW

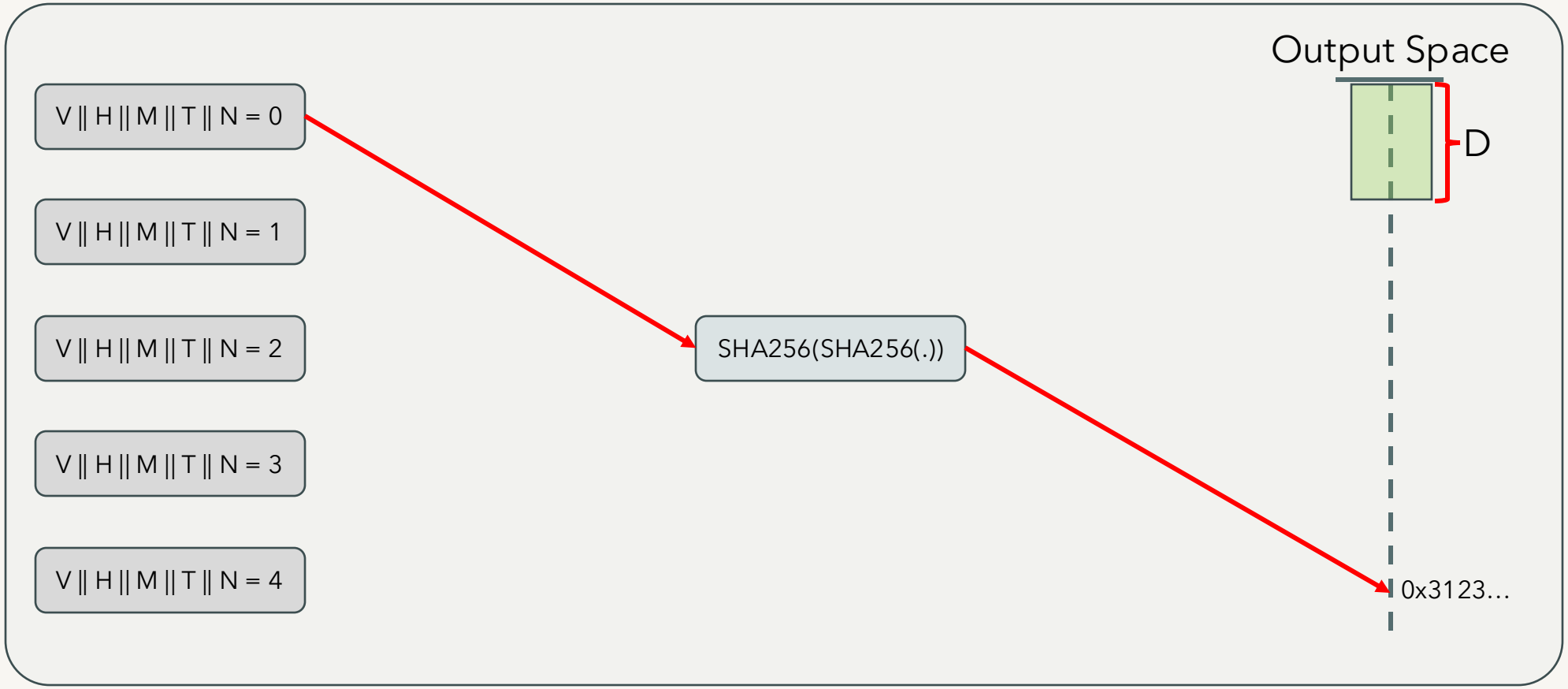
- So the search puzzle is this:
  - SHA256(SHA256(V || H || M || T || N)) < D
- V is mostly same
- H is same for all nodes (why?)
- T is same (very unlikely, but let's assume this)
- Assuming all nodes have the same txs in their mempool, M will never be same (why??)
  - As TX0 represents the coinbase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



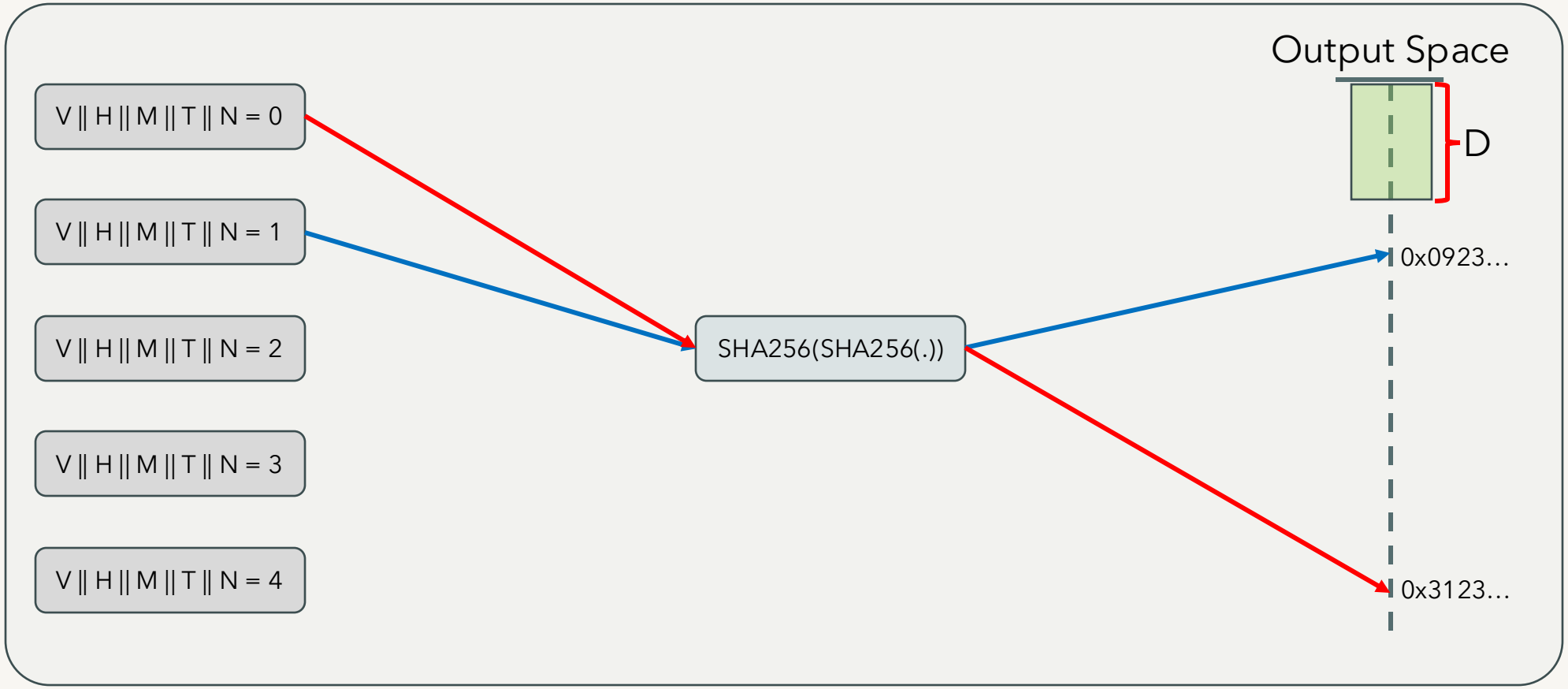
Bitcoin mining: PoW

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

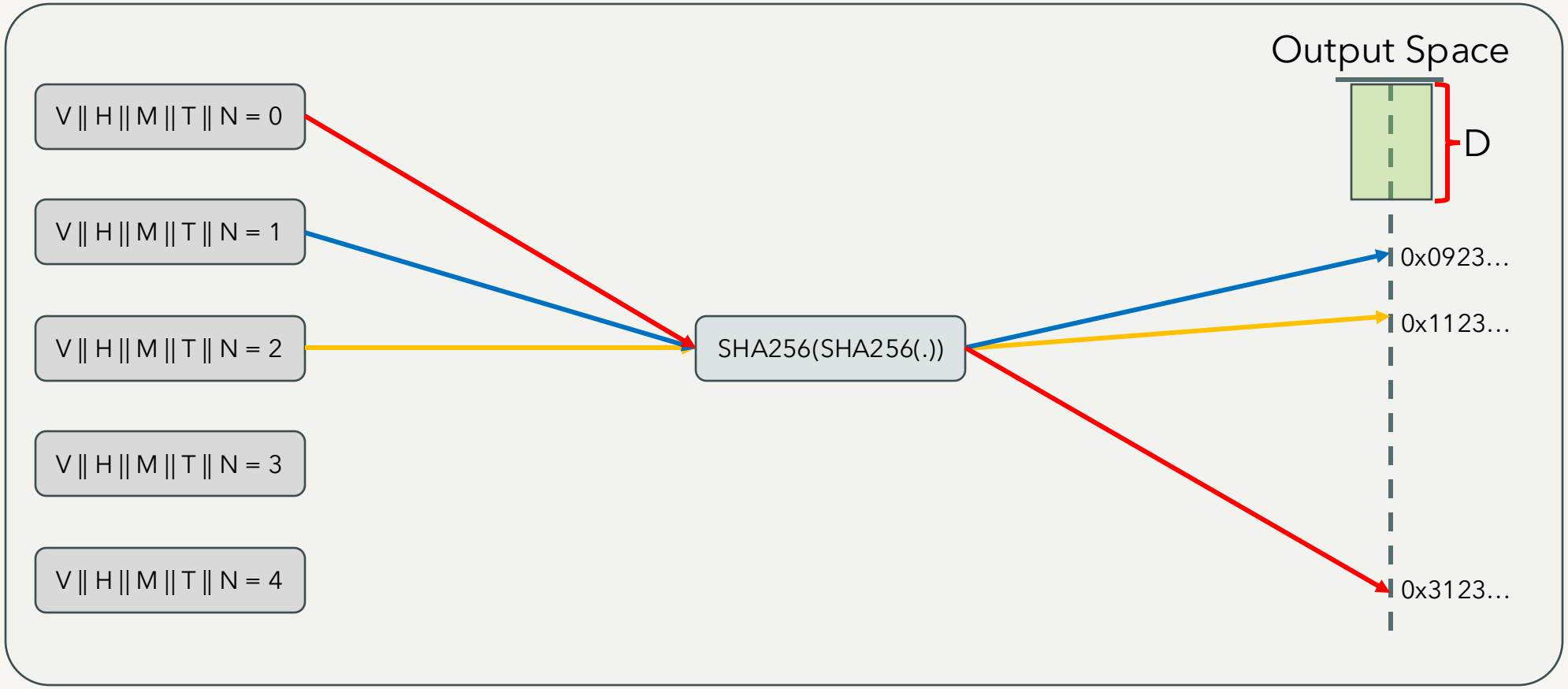
Bitcoin mining: PoW



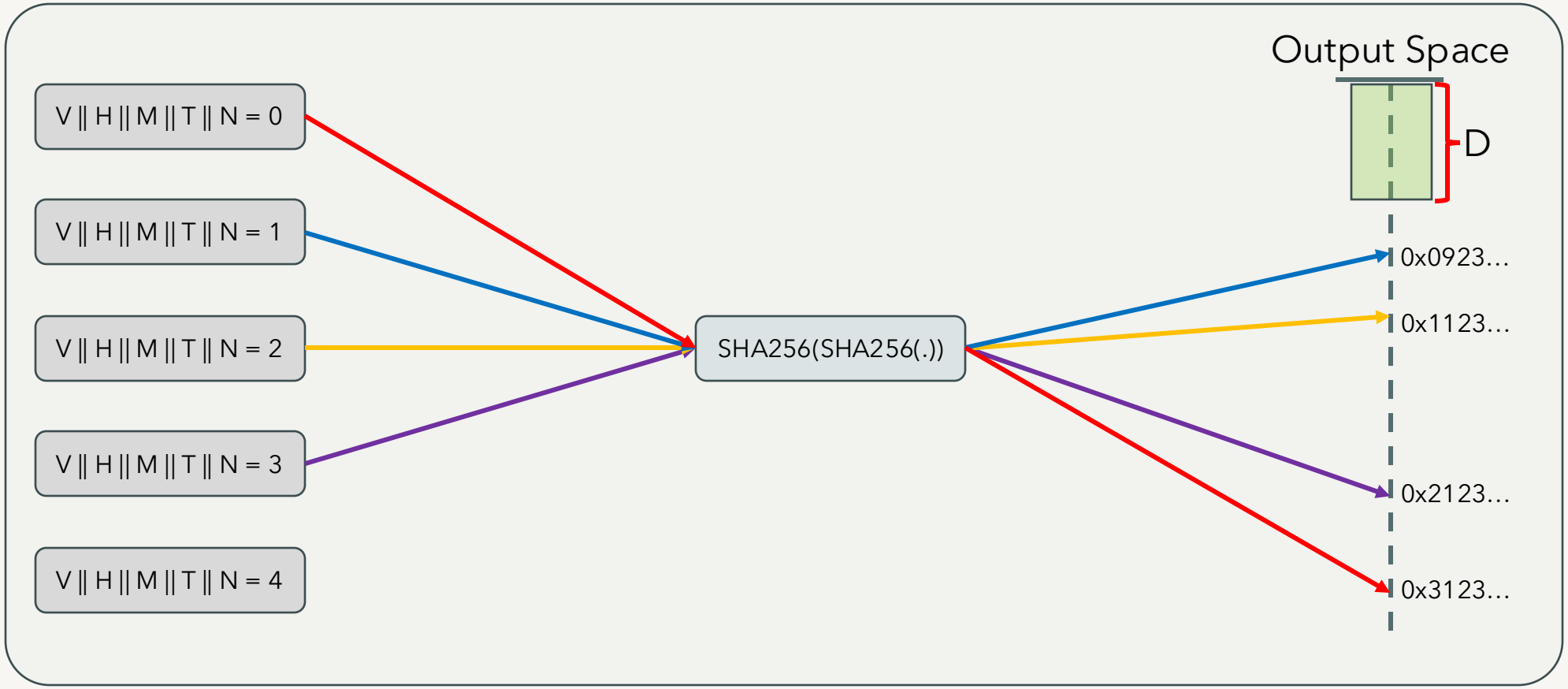
Bitcoin mining: PoW



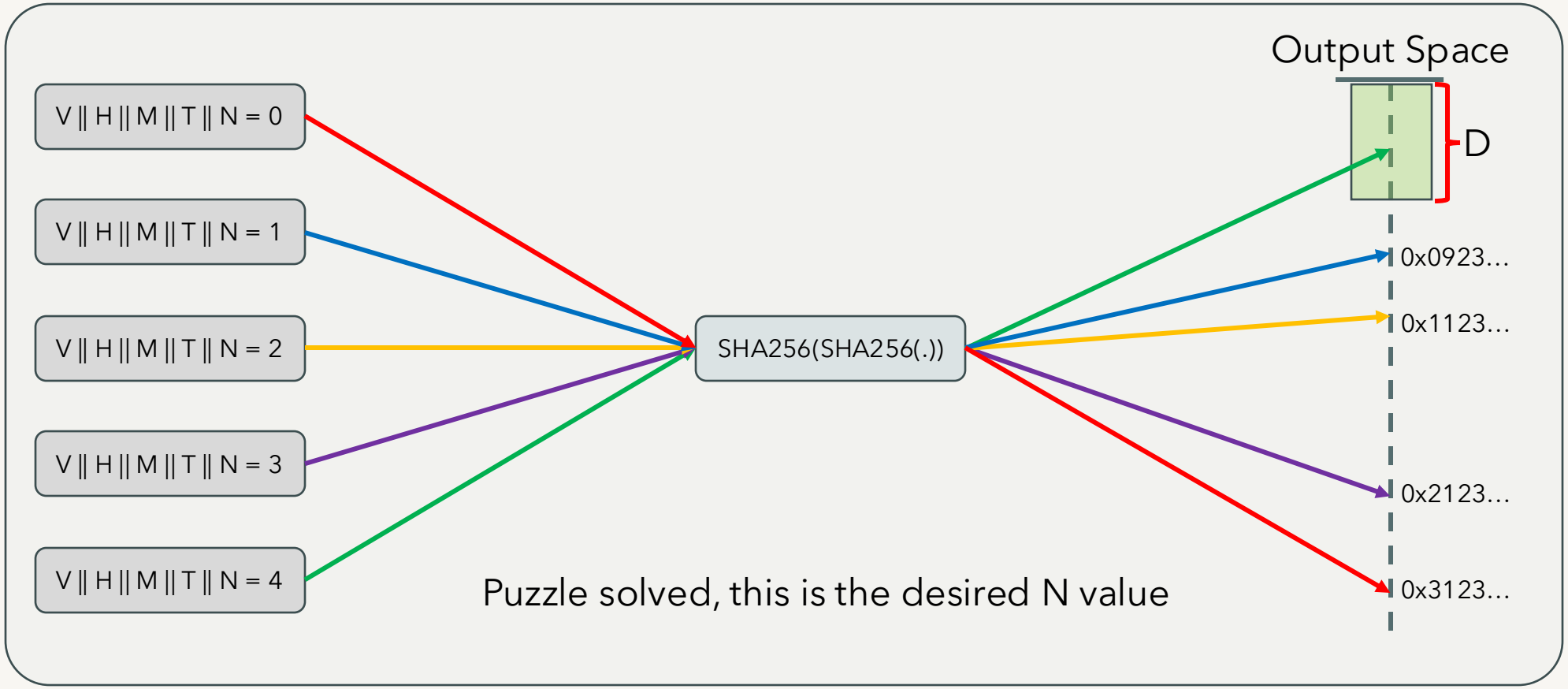
Bitcoin mining: PoW



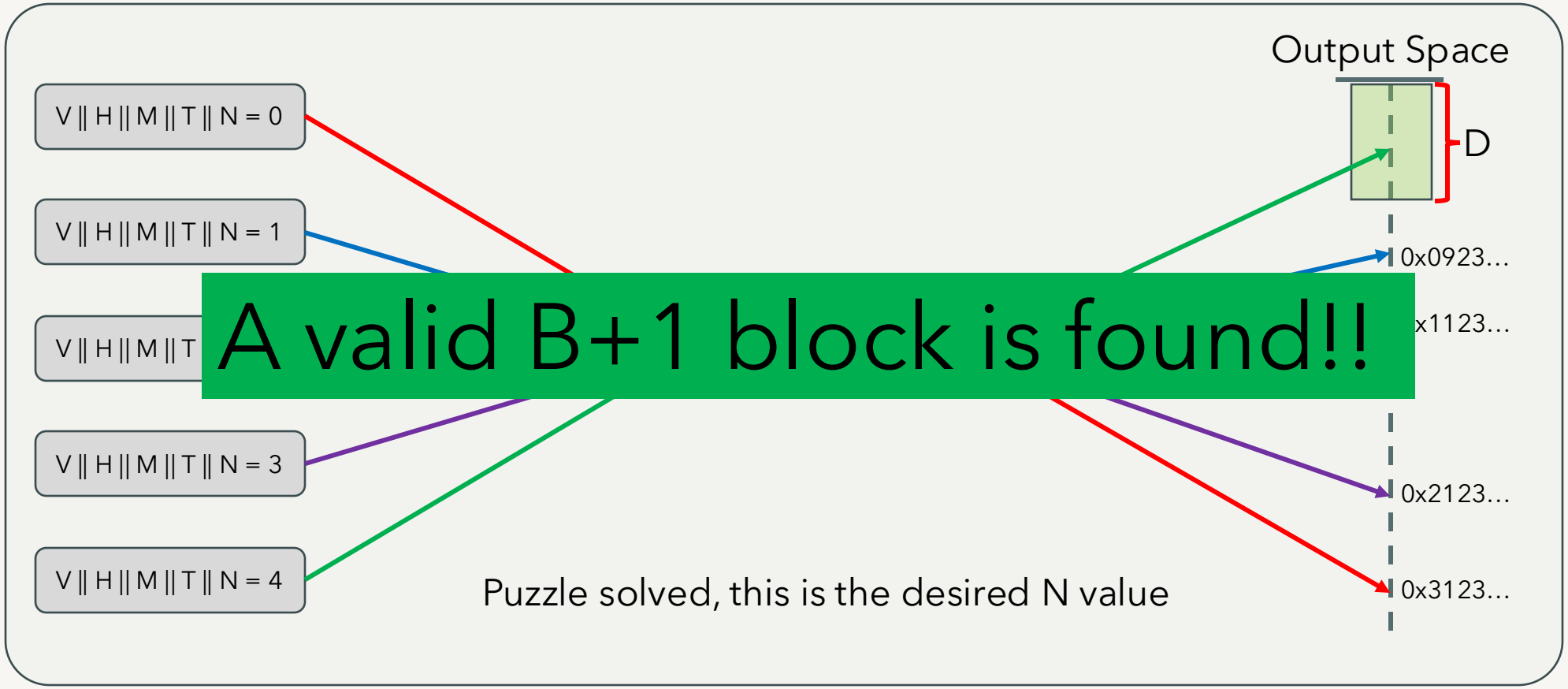
Bitcoin mining: PoW



Bitcoin mining: PoW



Bitcoin mining: PoW



Question?