
Kick start your Blockchain Journey: What you should know before writing your first Smart Contract

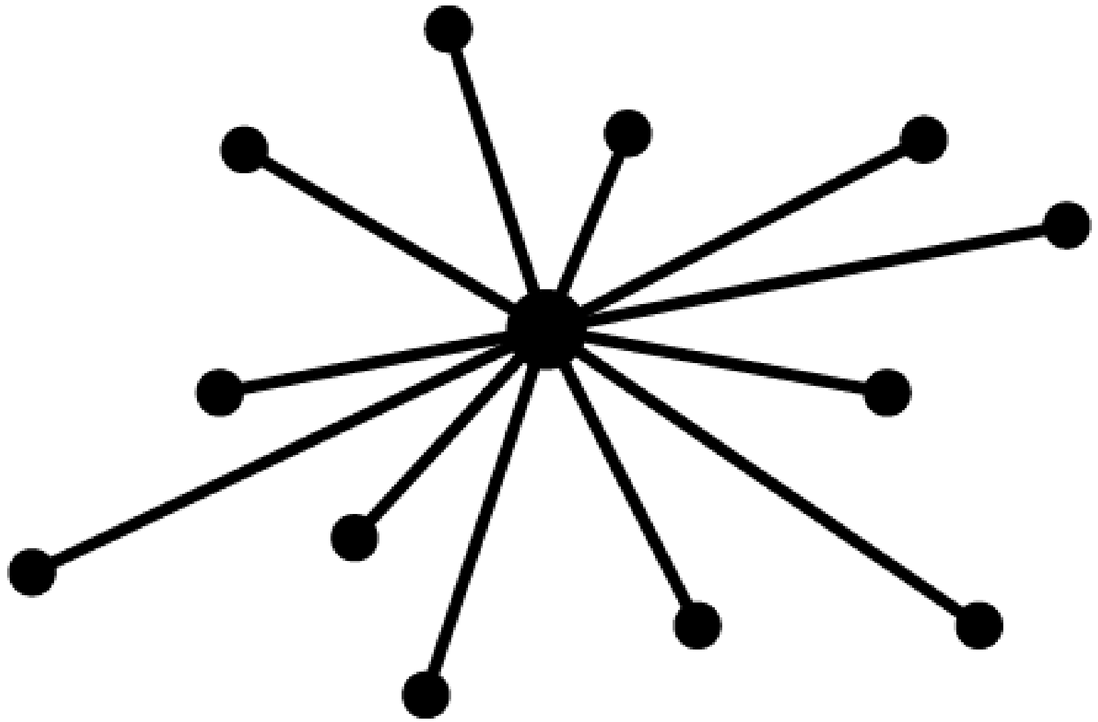
Mohamed Abdessamed Rezazi

Blockchain Auditor @Code4rena

Lead Judge auditor @CodeHawks

Whitehat @Immunefi

Software Architecture - Centralized-



Client/Server relation

Software Architecture - Centralized-

Advantages

- Smooth personal experience
- Easy maintenance
- Quick updates

Software Architecture - Centralized-

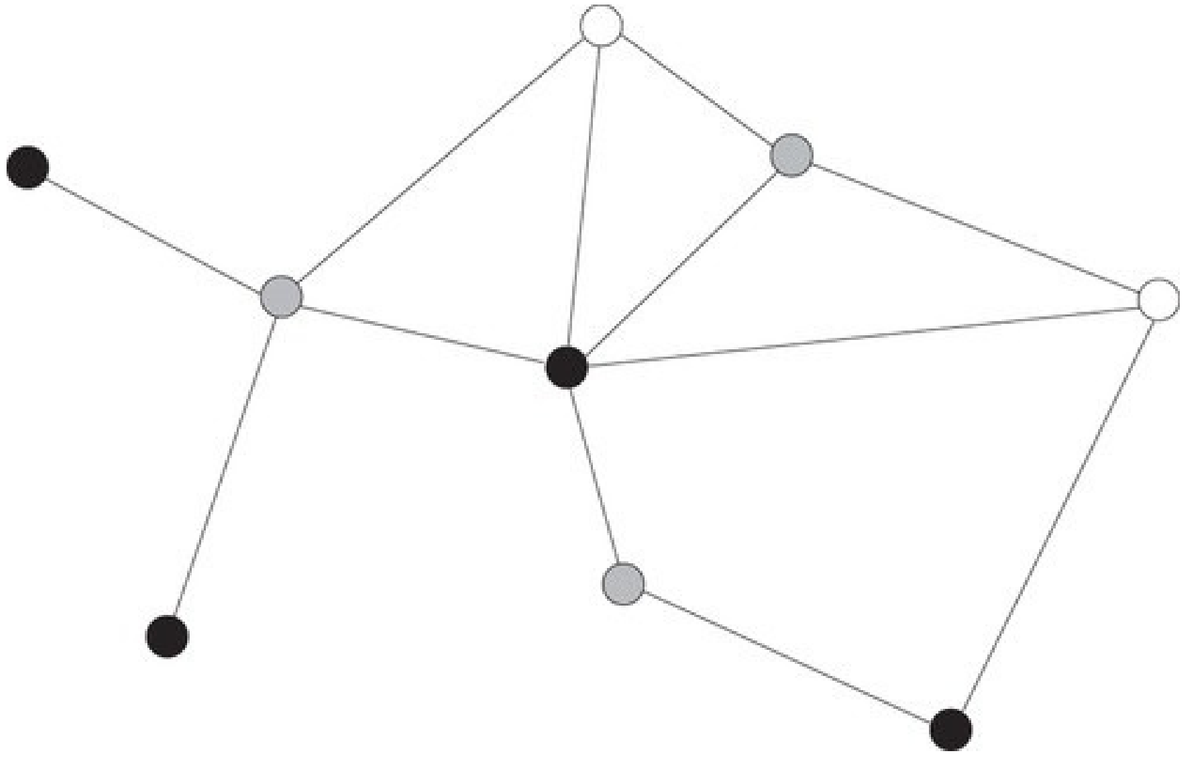
Advantages

- Smooth personal experience
- Easy maintenance
- Quick updates

Disadvantages

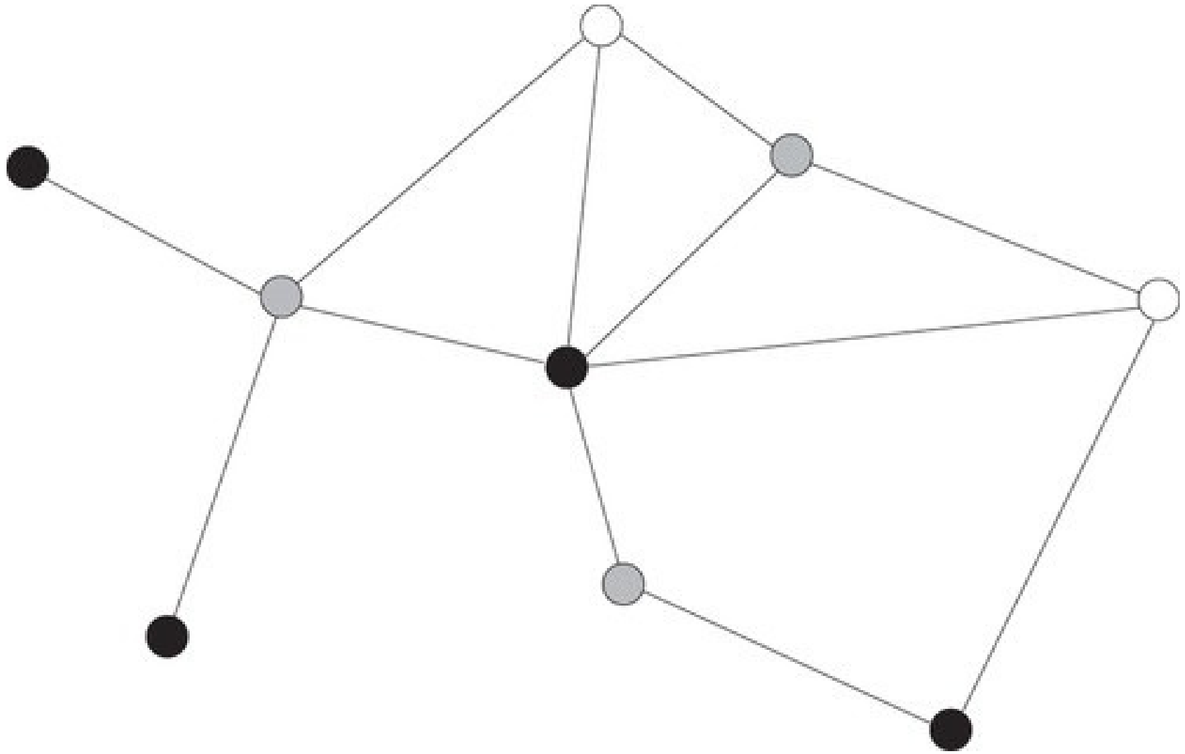
- **ONE single point of failure**
- Less possibility of data backup
- Master/slave architecture

Software Architecture - Peer to peer-



- All nodes are equal

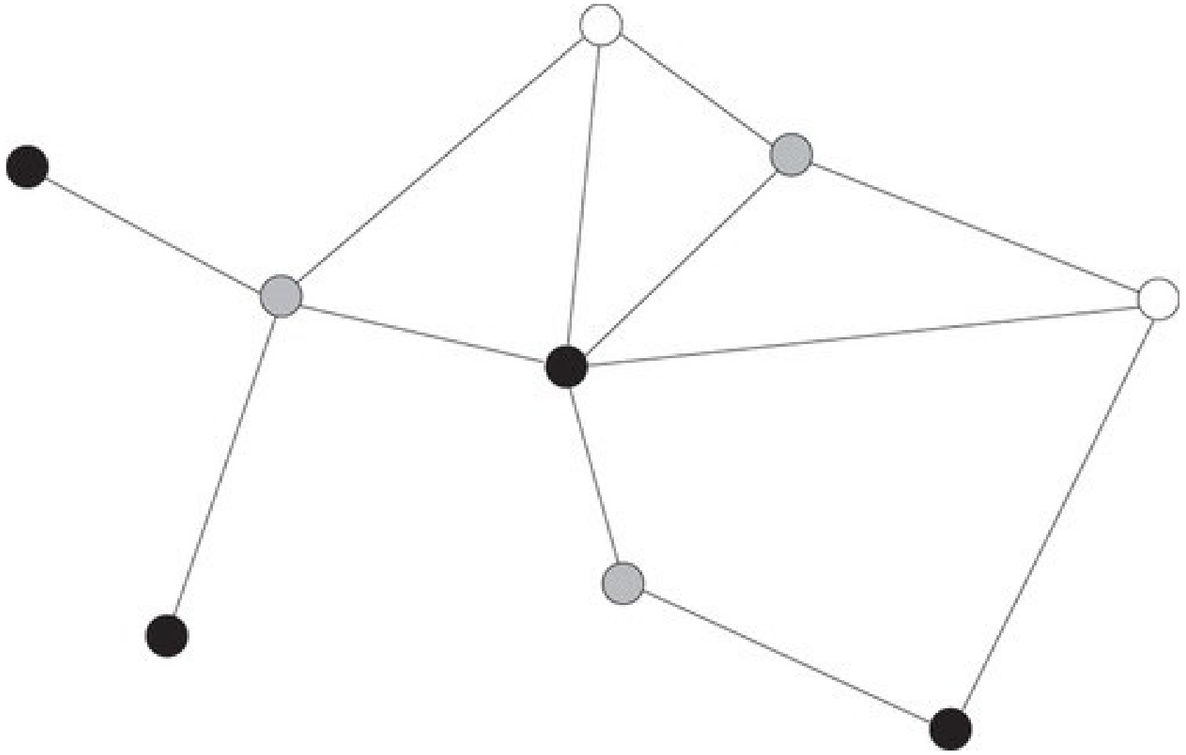
Software Architecture - Peer to peer-



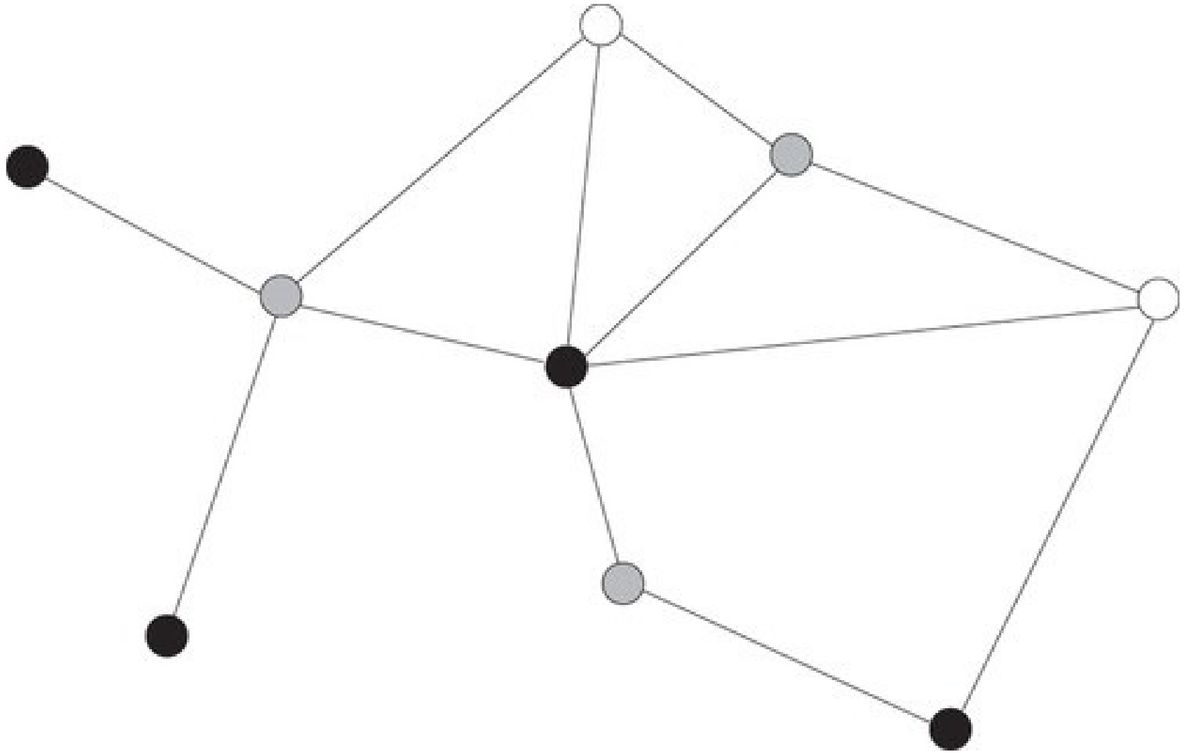
- All nodes are equal
- Nodes share their computational resources

Software Architecture - Peer to peer-

Obsatcles



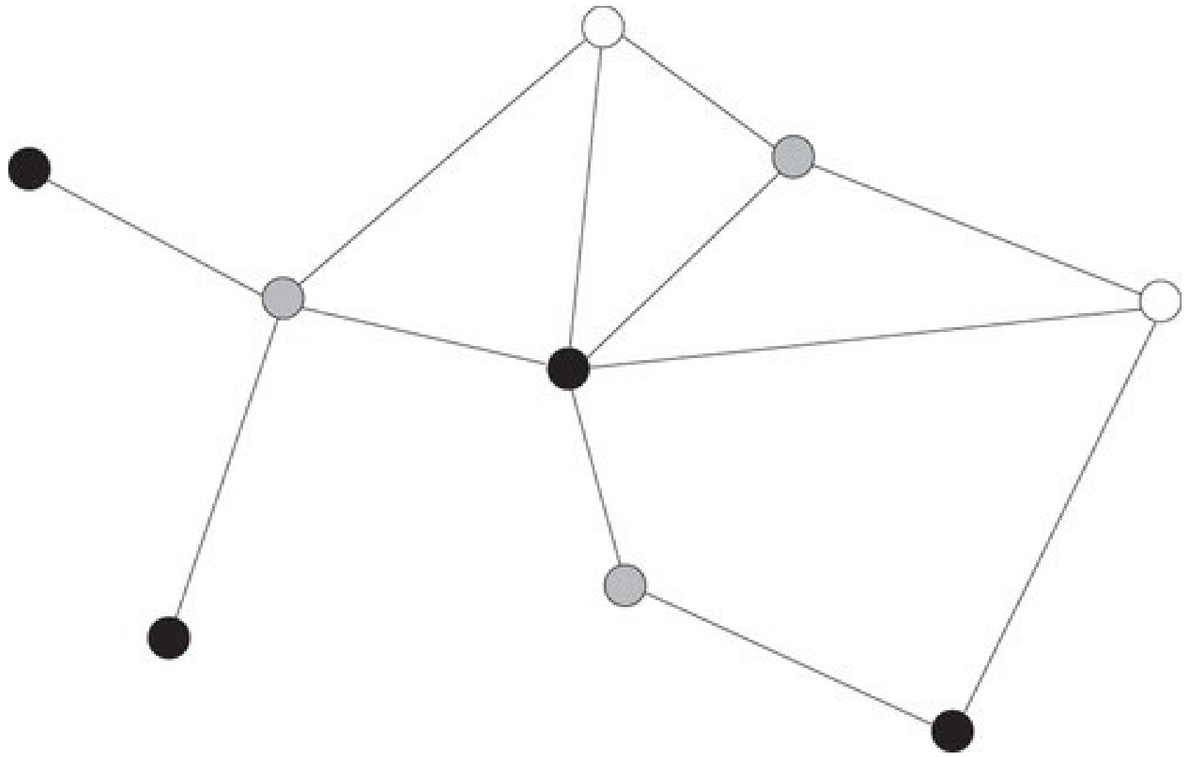
Software Architecture - Peer to peer-



Obsatcles

- coordination headache

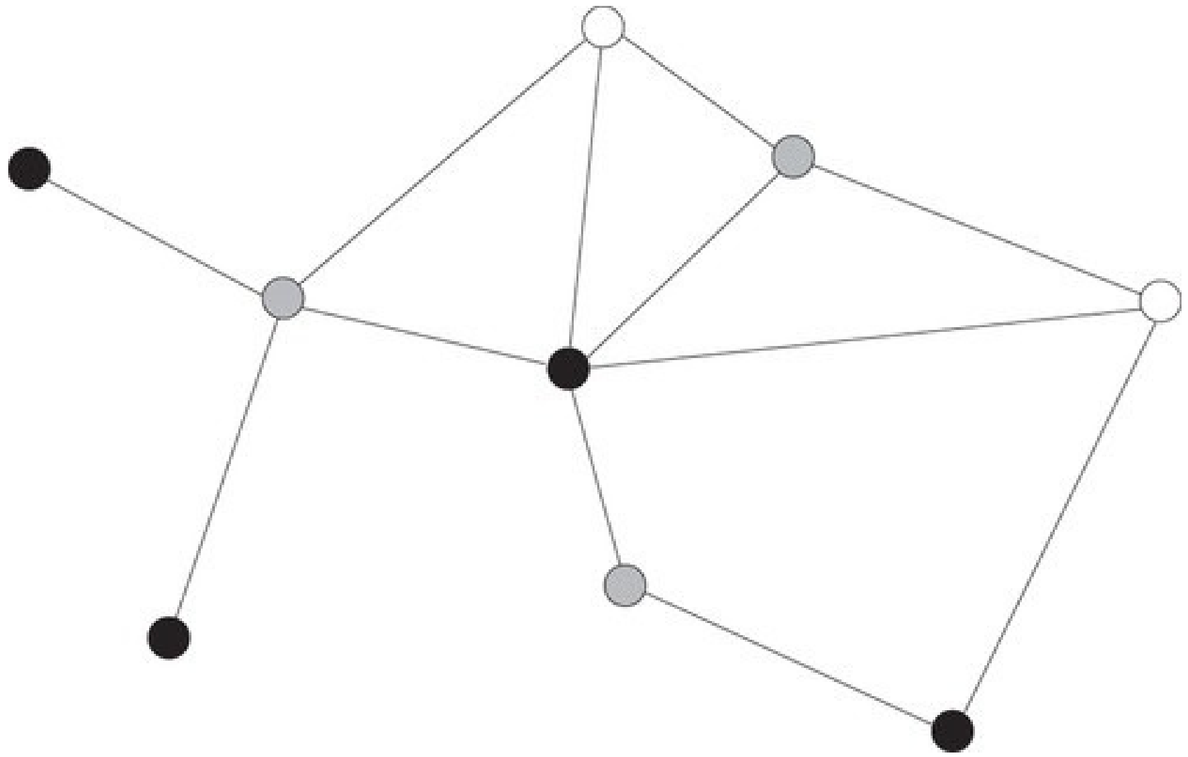
Software Architecture - Peer to peer-



Obsatcles

- coordination headache
- Communication overhead

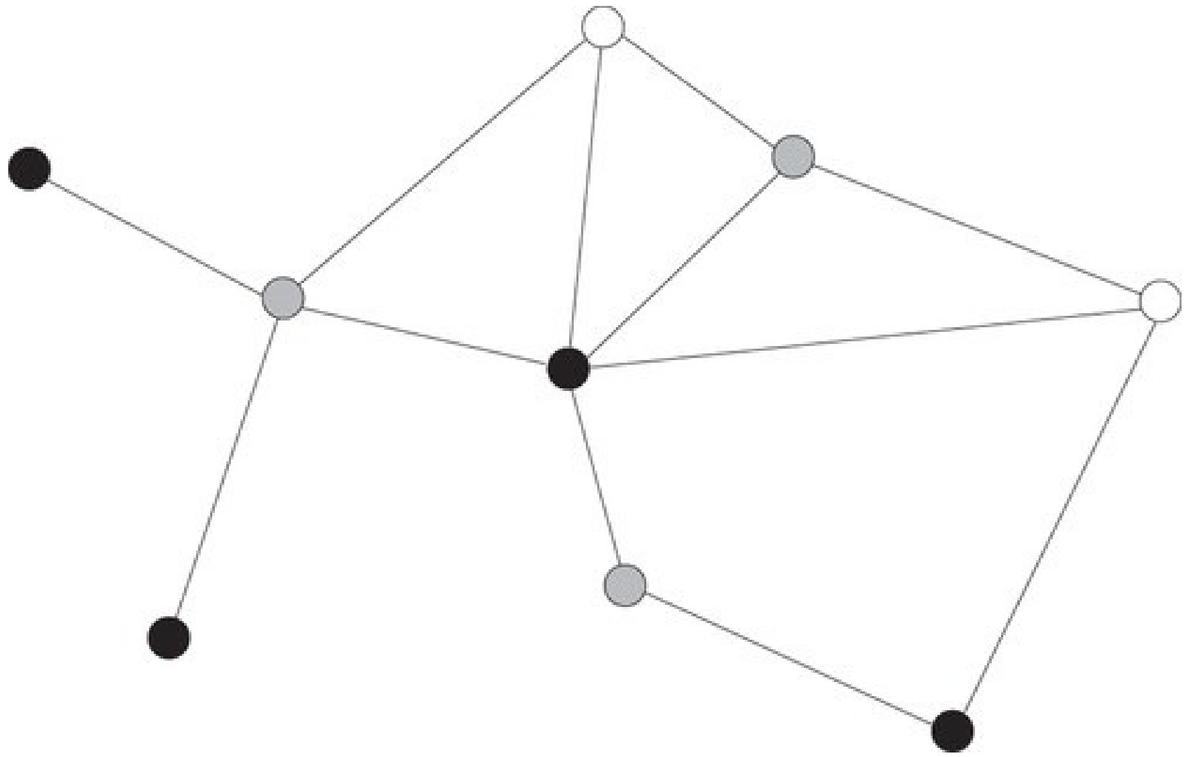
Software Architecture - Peer to peer-



Obsatcles

- coordination headache
- Communication overhead
- Number of peers is unknown

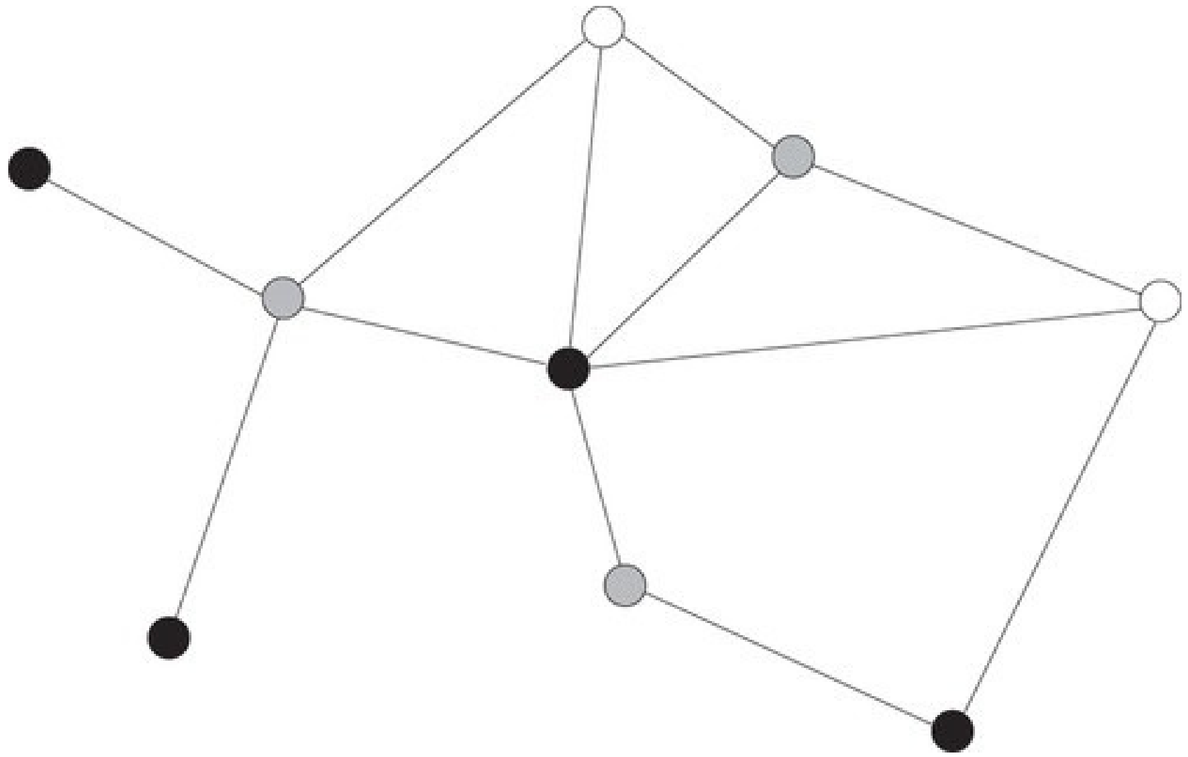
Software Architecture - Peer to peer-



Obsatcles

- coordination headache
- Communication overhead
- Number of peers is unknown
- Trustworthiness is unknown

Software Architecture - Peer to peer-



Obsatcles

- coordination headache
- Communication overhead
- Number of peers is unknown
- Trustworthiness is unknown
- Malicious peers

Byzantine Generals problem

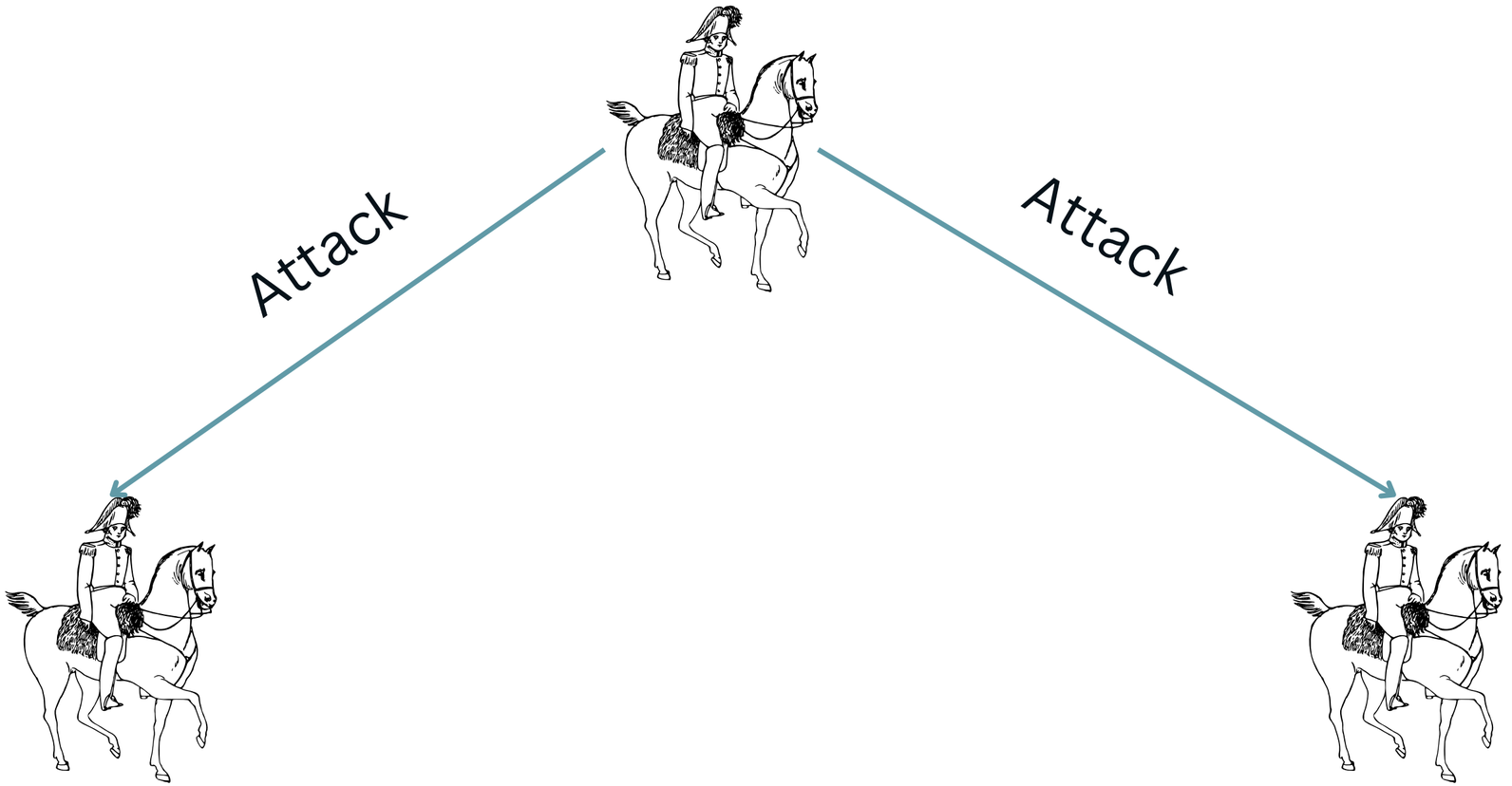
Byzantine Generals problem

Byzantine Generals problem

Byzantine Generals problem

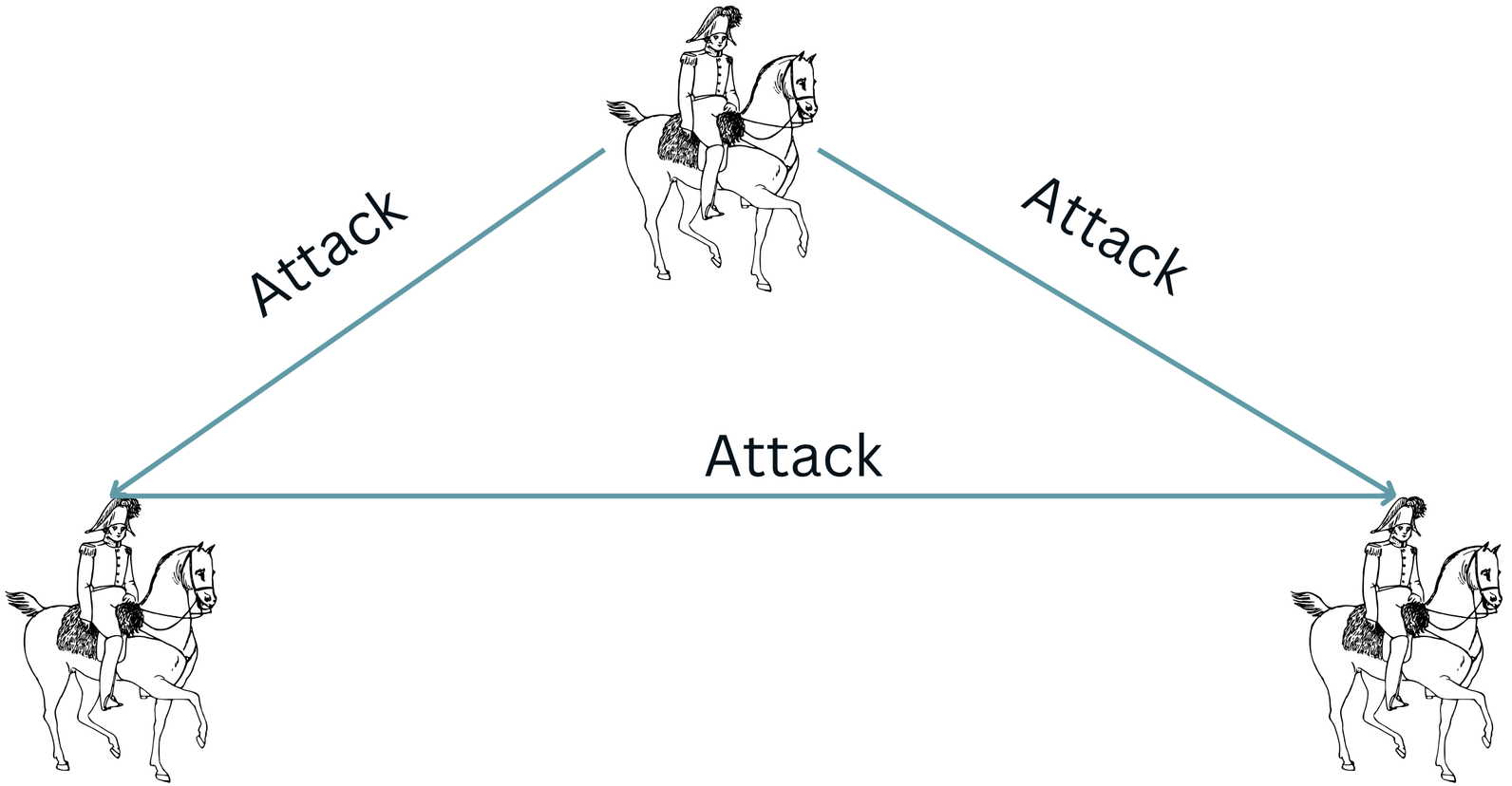
Byzantine Generals problem

Byzantine Generals problem



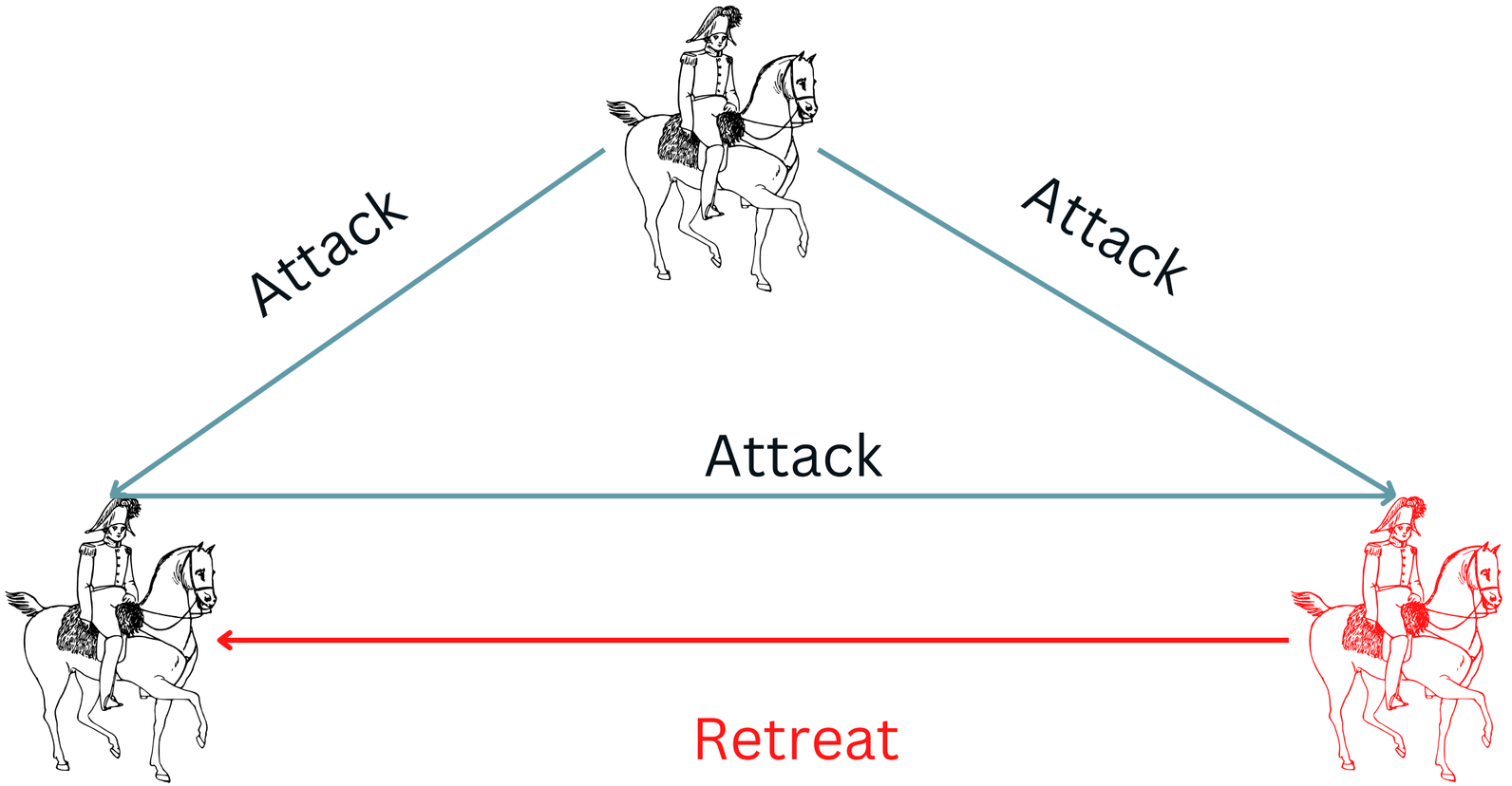
Byzantine Generals problem

Byzantine Generals problem



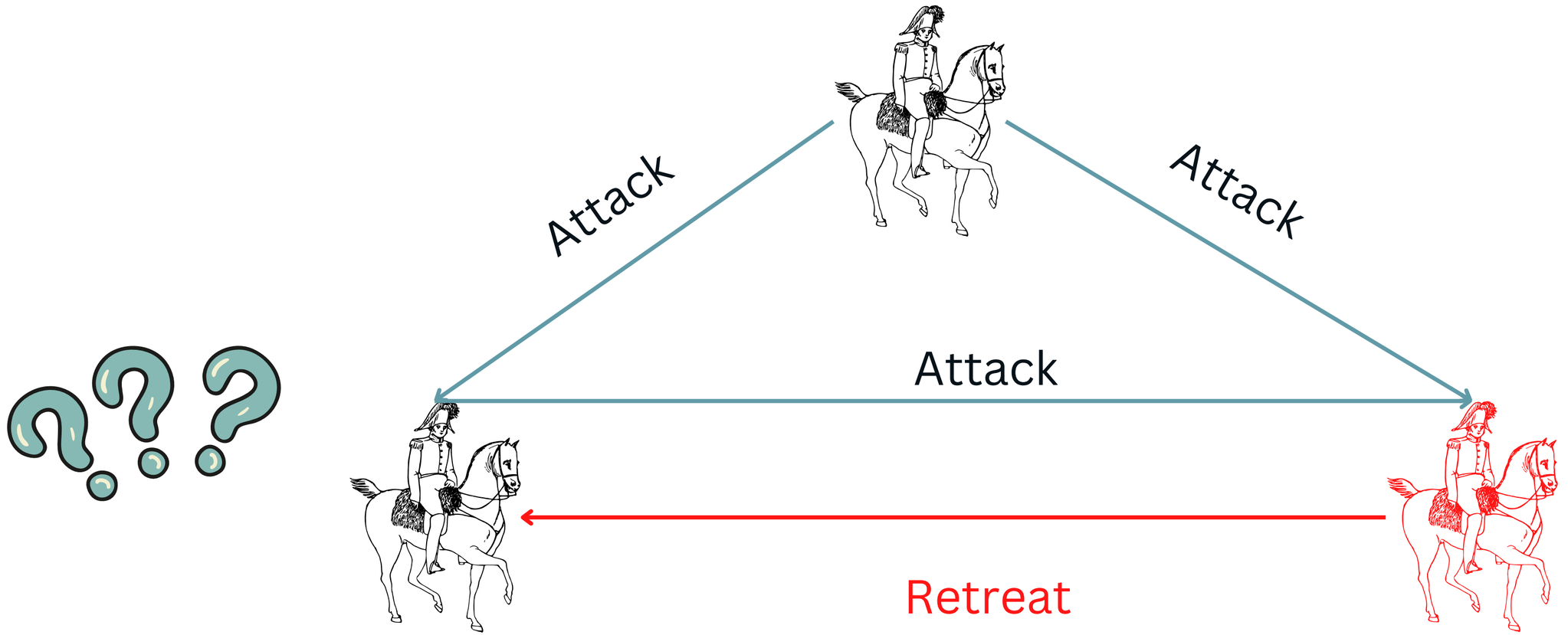
Byzantine Generals problem

Byzantine Generals problem



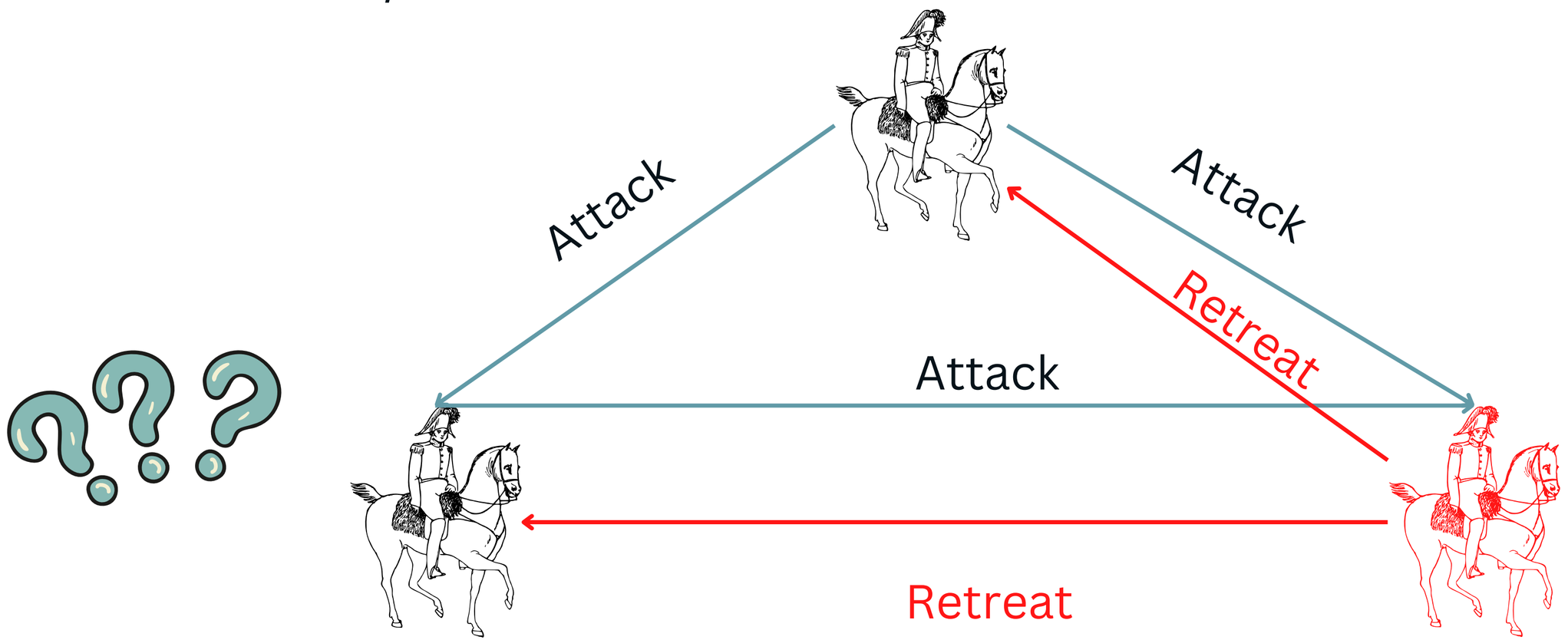
Byzantine Generals problem

Byzantine Generals problem



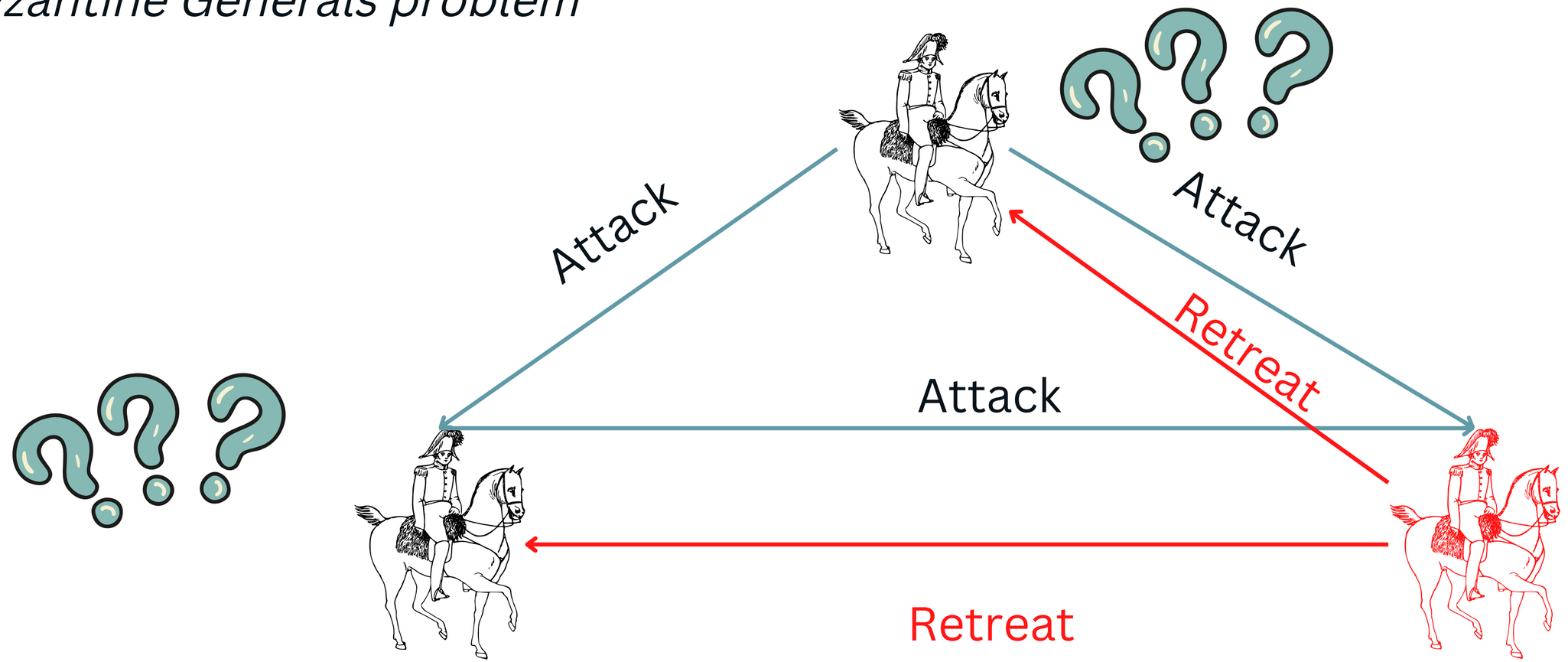
Byzantine Generals problem

Byzantine Generals problem



Byzantine Generals problem

Byzantine Generals problem



The potential of P2P systems

P2P systems can change the whole industry with a simple idea: **replace middlemen with peer to peer interactions**

The potential of P2P systems

What's exciting about P2P systems is the **disintermediation**, ***Blockchain is a way to achieve that***

Software Architecture, Blockchain location

The purpose of the blockchain is to **achieve integrity** and **security** in **purely distributed peer-to-peer systems** that consist of an **unknown number of peers** with **unknown trustworthiness**

Identifying the term *Blockchain*

The term Blockchain can be defined in several ways:

Identifying the term *Blockchain*

The term Blockchain can be defined in several ways:

- As a name for an algorithm

Identifying the term *Blockchain*

The term Blockchain can be defined in several ways:

- As a name for an algorithm
- As a Data Structure

Identifying the term *Blockchain*

The term Blockchain can be defined in several ways:

- As a name for an algorithm
- As a Data Structure
- As a suit of technologies

Unpacking Ethereum

Unpacking Ethereum

Core Concepts

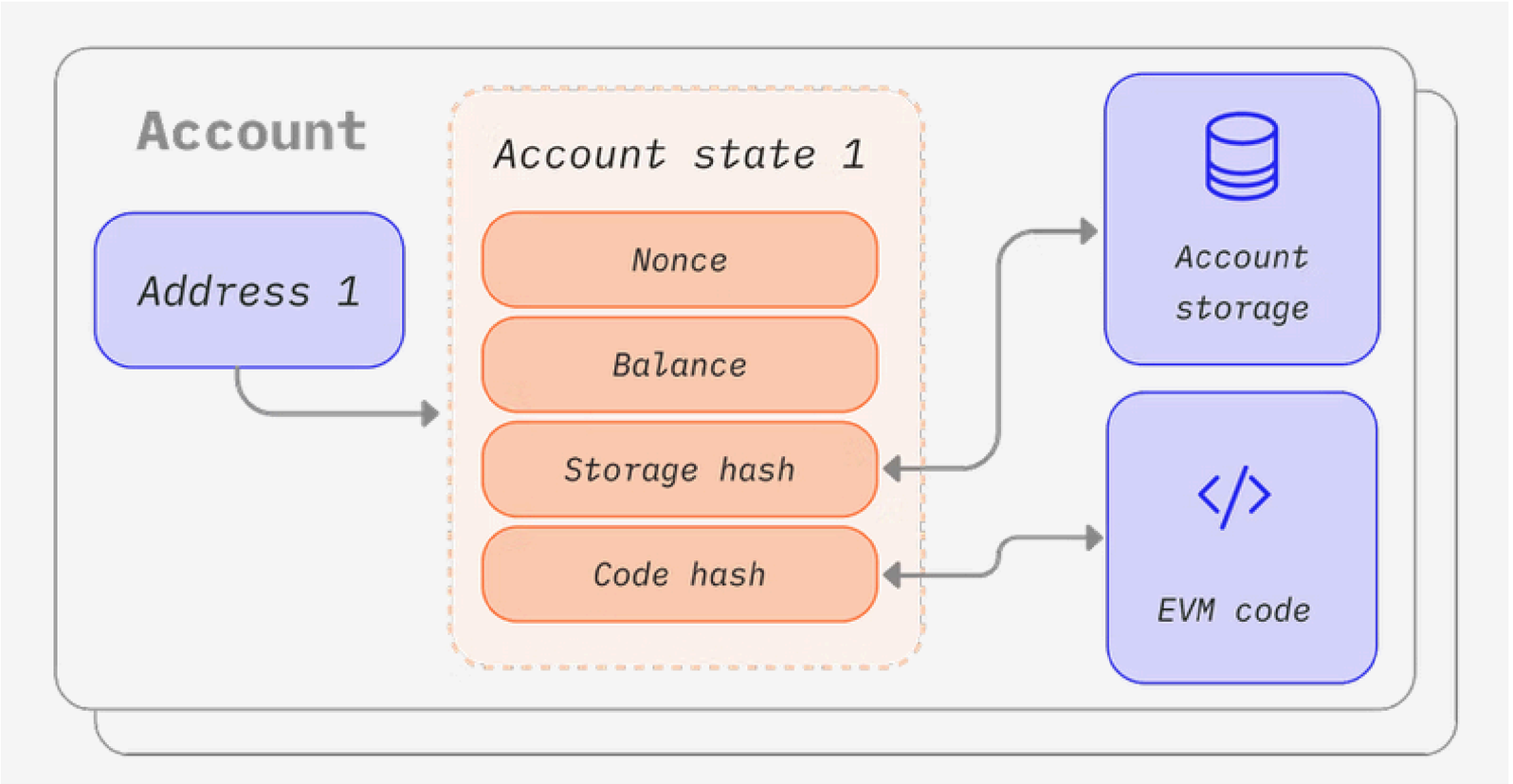
- Account
- Transaction
- Block
- Blockchain
- Distributed Ledger
- Consensus
- Nodes & Clients
- Ethereum Virtual Machine

Abdessamed Rezazi

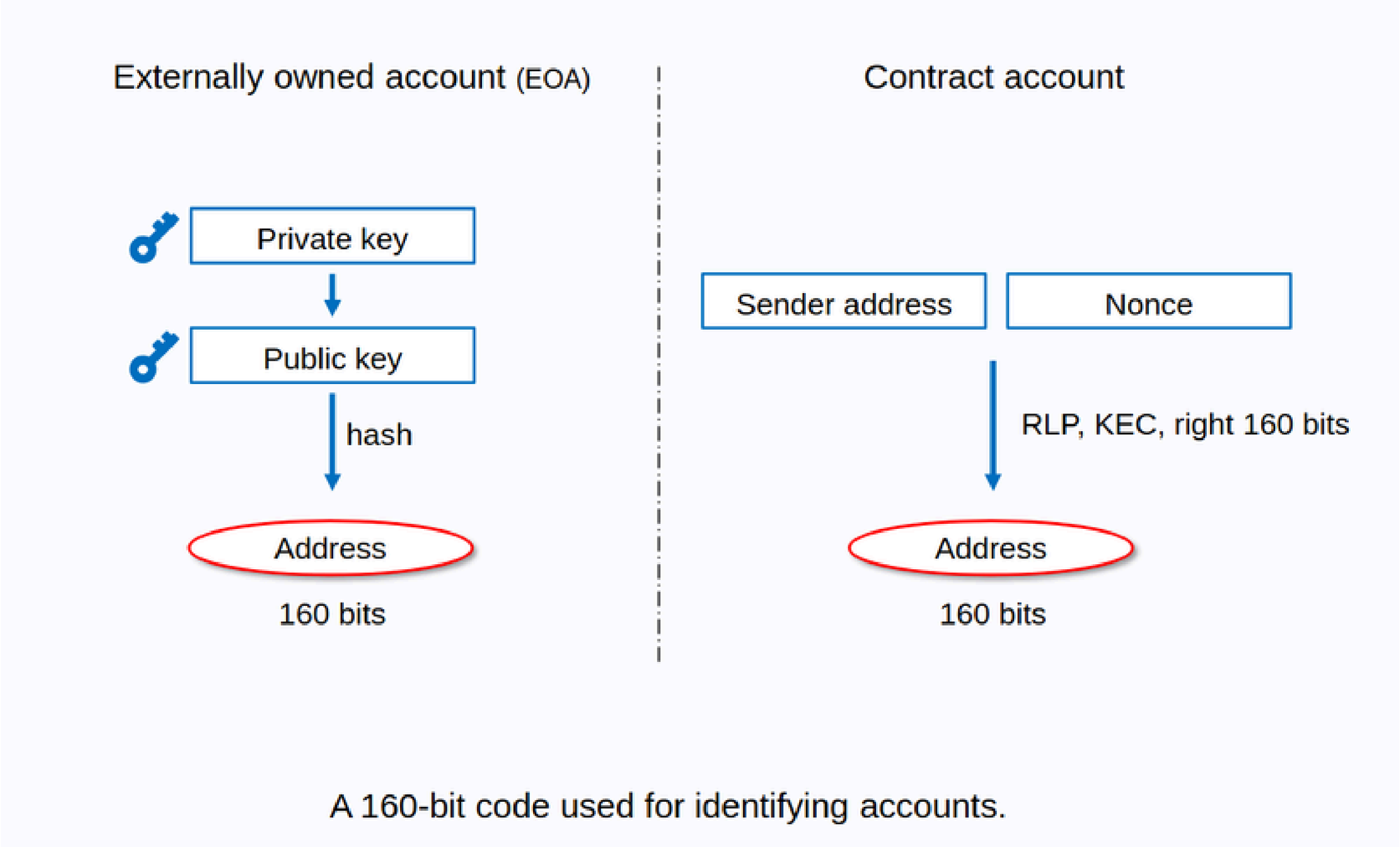
Accounts

There are two types of accounts in Ethereum:

- External Owned Accounts (EOAs)
- Smart Contracts



Accounts



Ethereum EVM illustrated

Accounts

- EOAs are controlled by a private key

  The private key is generated based on ECC cryptography

- Smart Contracts are controlled by the code

  The smart contract address is generated based on the deployer’s address + nonce (**CREATE** opcode)

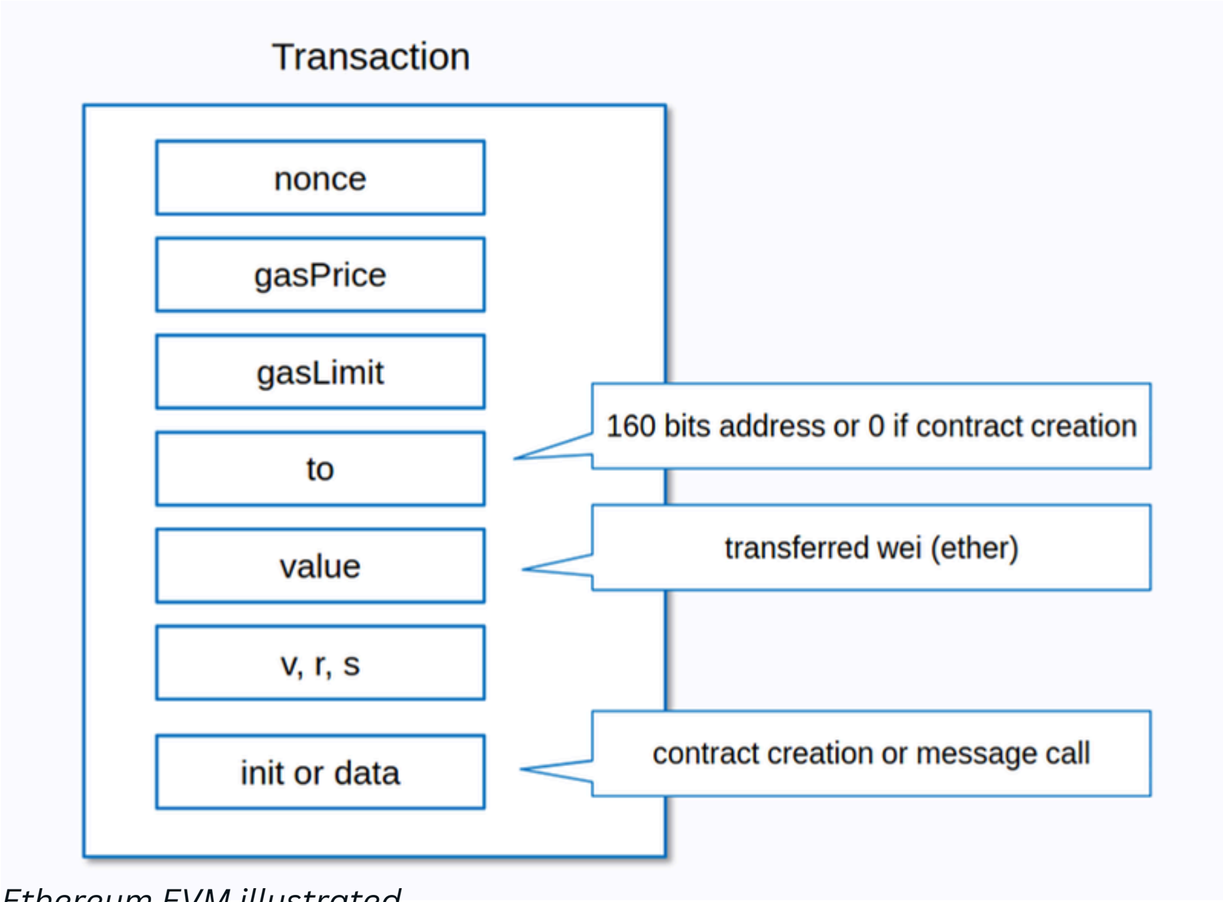
Transactions

An Ethereum transaction refers to an action initiated by an externally-owned account, and it triggers a **state update**

Ethereum Docs

Transactions

A transaction is an **object** that describes the action to be executed



Ethereum EVM illustrated

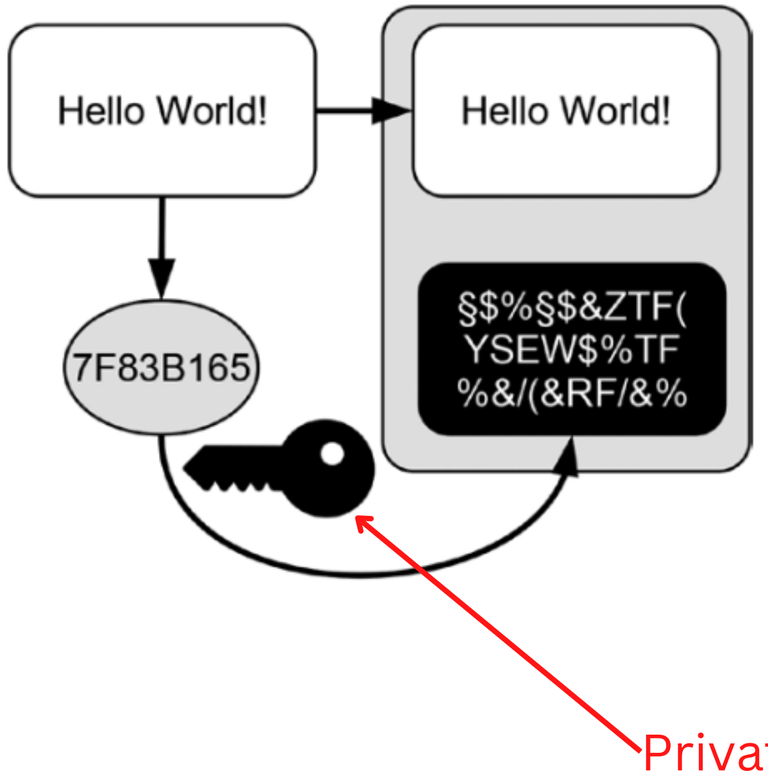
Abdessamed Rezazi

Transactions

- The peer-to-peer system under consideration is open to everyone. Hence, everyone may create transactions and can submit them to the system.
- Only the lawful owner of an account should be able to transfer property or ownership rights associated with his or her account to another account.
- Digital Signatures allows transactions authorization

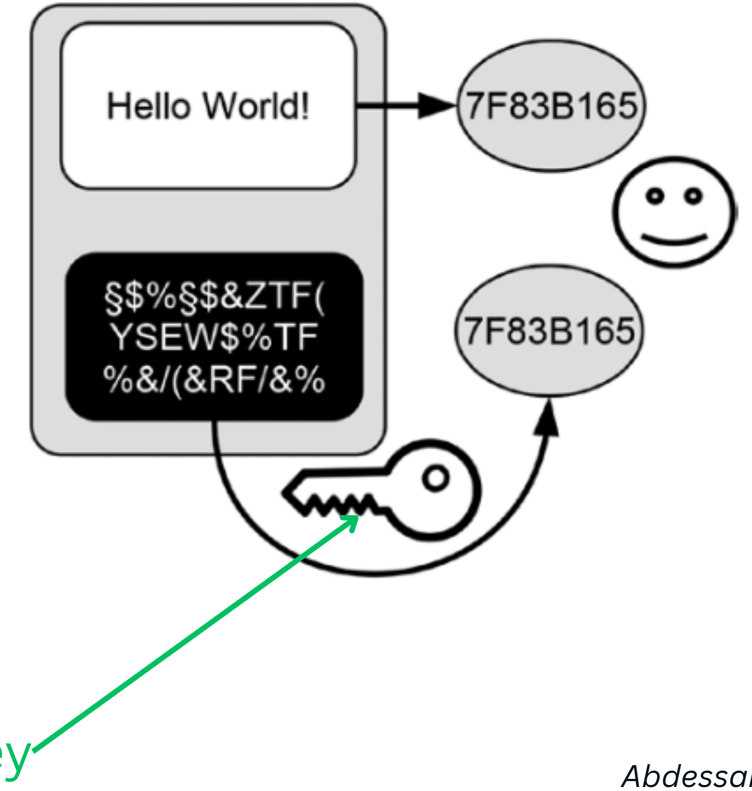
Digital Signatures

Creating Signatures



Submit transaction

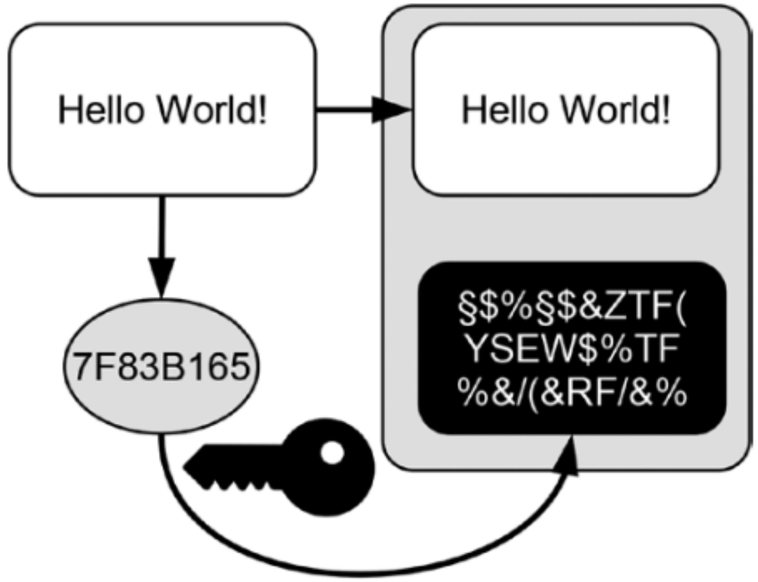
Verifying Signatures



Abdessamed Rezazi

Digital Signatures

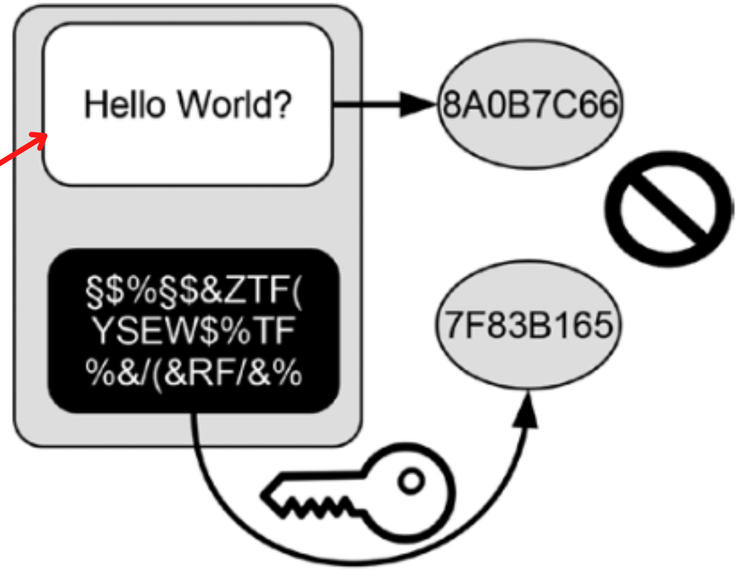
Creating Signatures



Submit transaction

Modifying the Tx

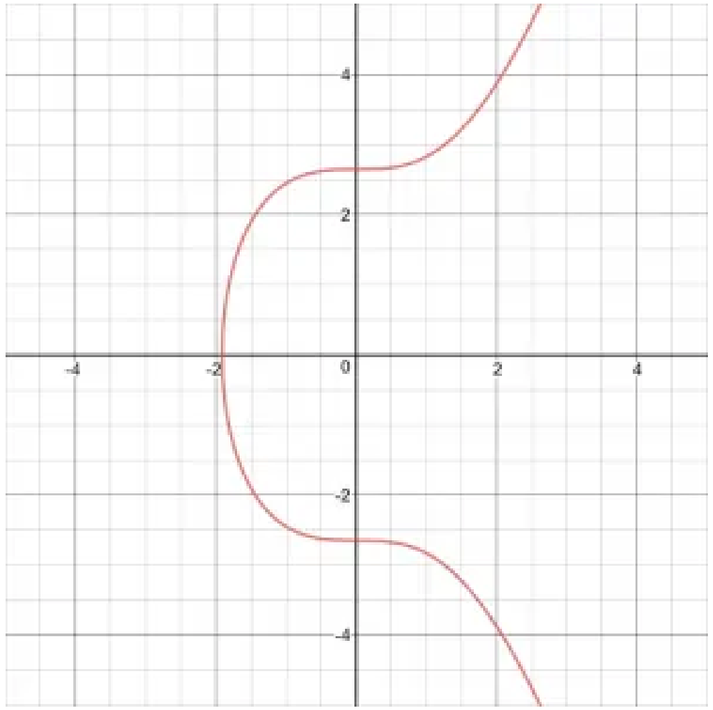
Verifying Signatures



Abdessamed Rezazi

Digital Signatures

Ethereum and Bitcoin use ECDSA for digital signatures based on **SECP256k1** curve



$y^2 = x^3 + 7$

Digital Signatures

The secp256k1 curve has:

- **Generator point** G is a specific point on the elliptic curve
- **Order n** of the subgroup of elliptic curve points, generated by G, which defines the length of the private keys (e.g. 256 bits) and is a prime number

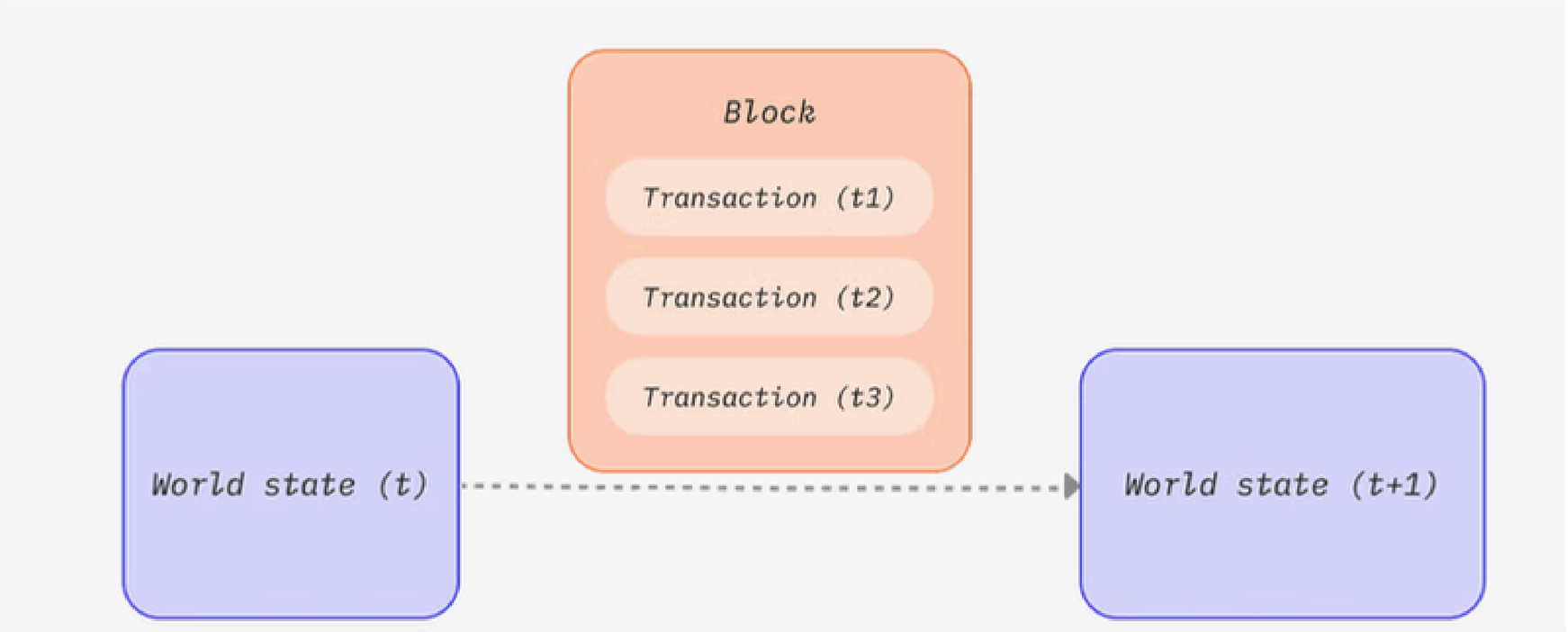
Digital Signatures

Digital signature creation

- Calculating the message hash **h = hash(msg)**
- Generating **securely a random** number k
- Calculating the random point **R** = k * G and take its x-coordinate: r = R.x
- Calculating the signature proof s using the formula: s = k^-1 * (h + p * r) mod n
- return (r, s)

Blocks

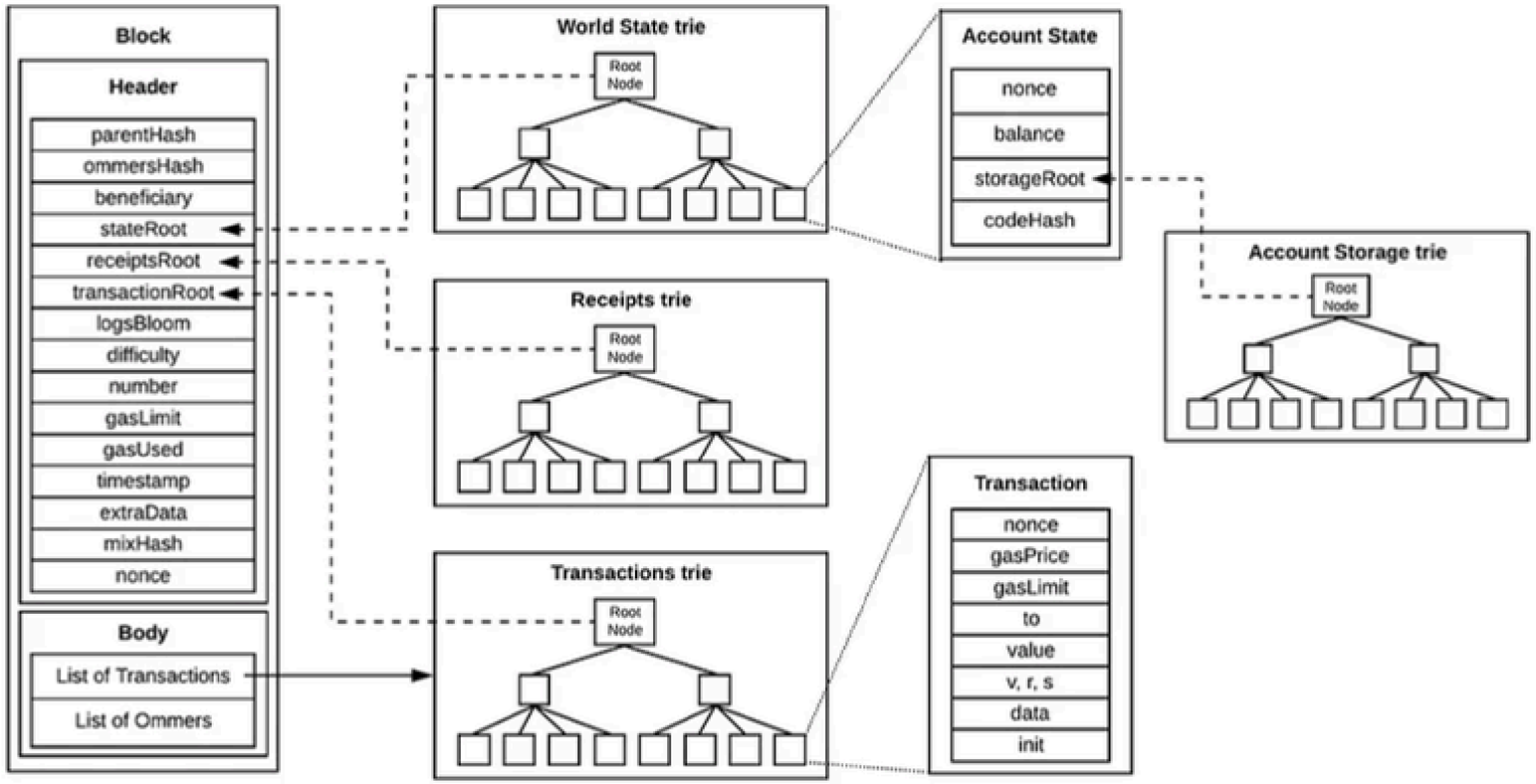
Transactions are batched into blocks. dozens (or hundreds) of transactions are committed, agreed on, and synchronized **all at once**.



Ethereum Docs

Blocks

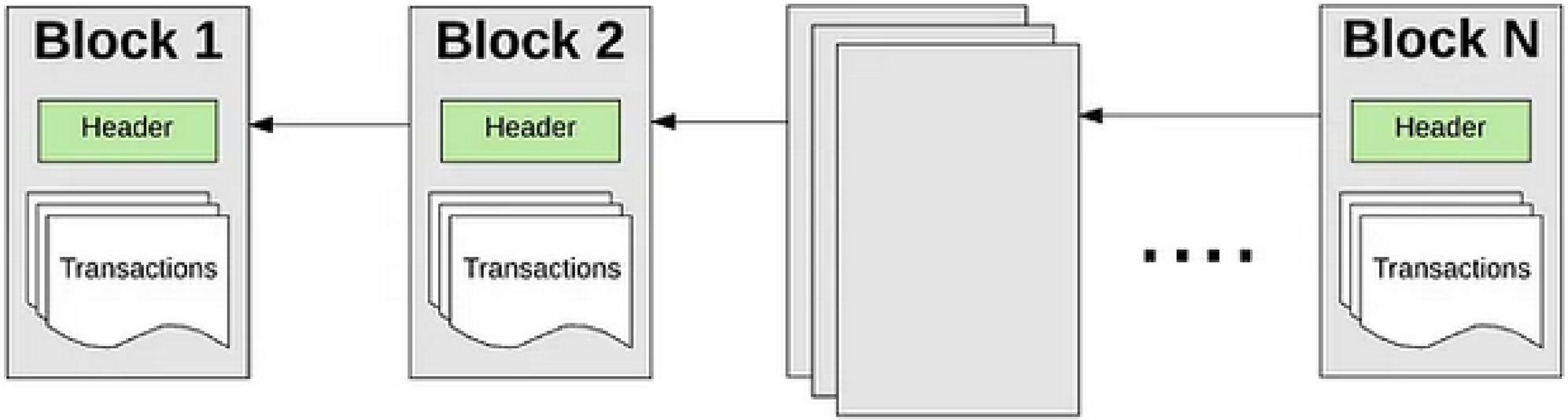
Transactions are batched into blocks. dozens (or hundreds) of transactions are committed, agreed on, and synchronized **all at once**.



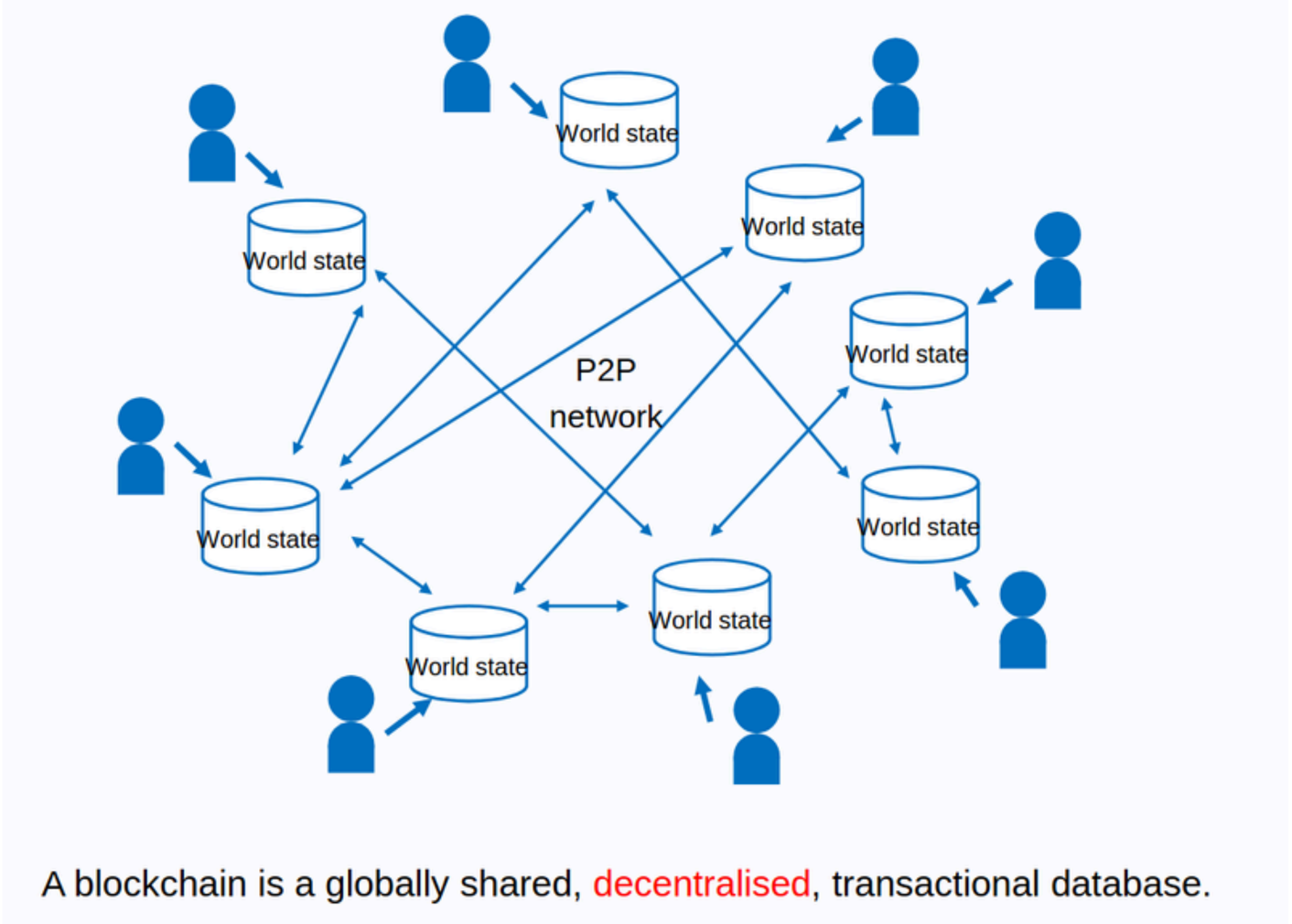
Abdessamed Rezazi

Blockchain

Each block is chained cryptographically together with its previous block. Hence, the term **Blockchain**



Distributed Ledger

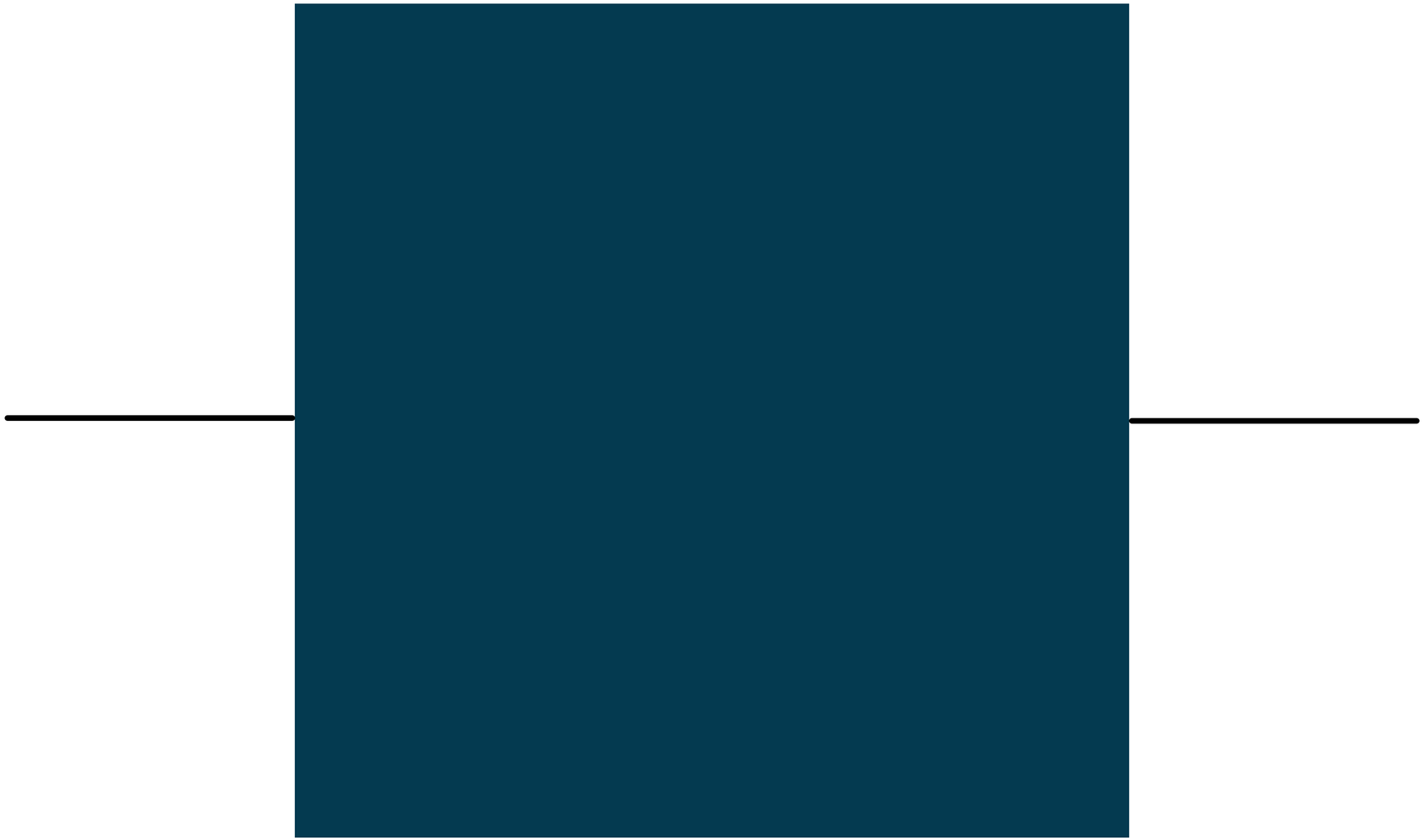


EVM Illustrated

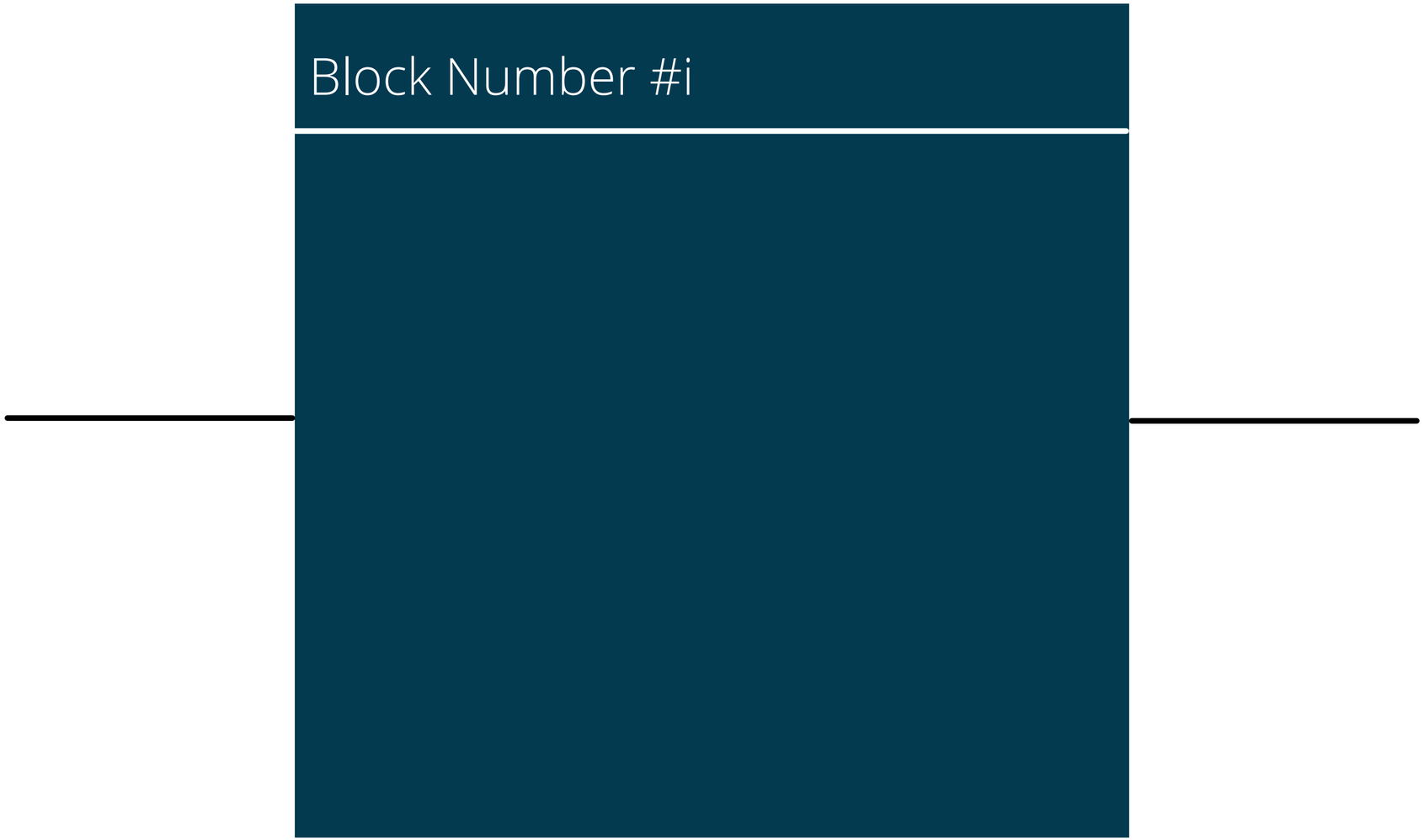
How Mining works

How block is created in Bitcoin? Aka Mining

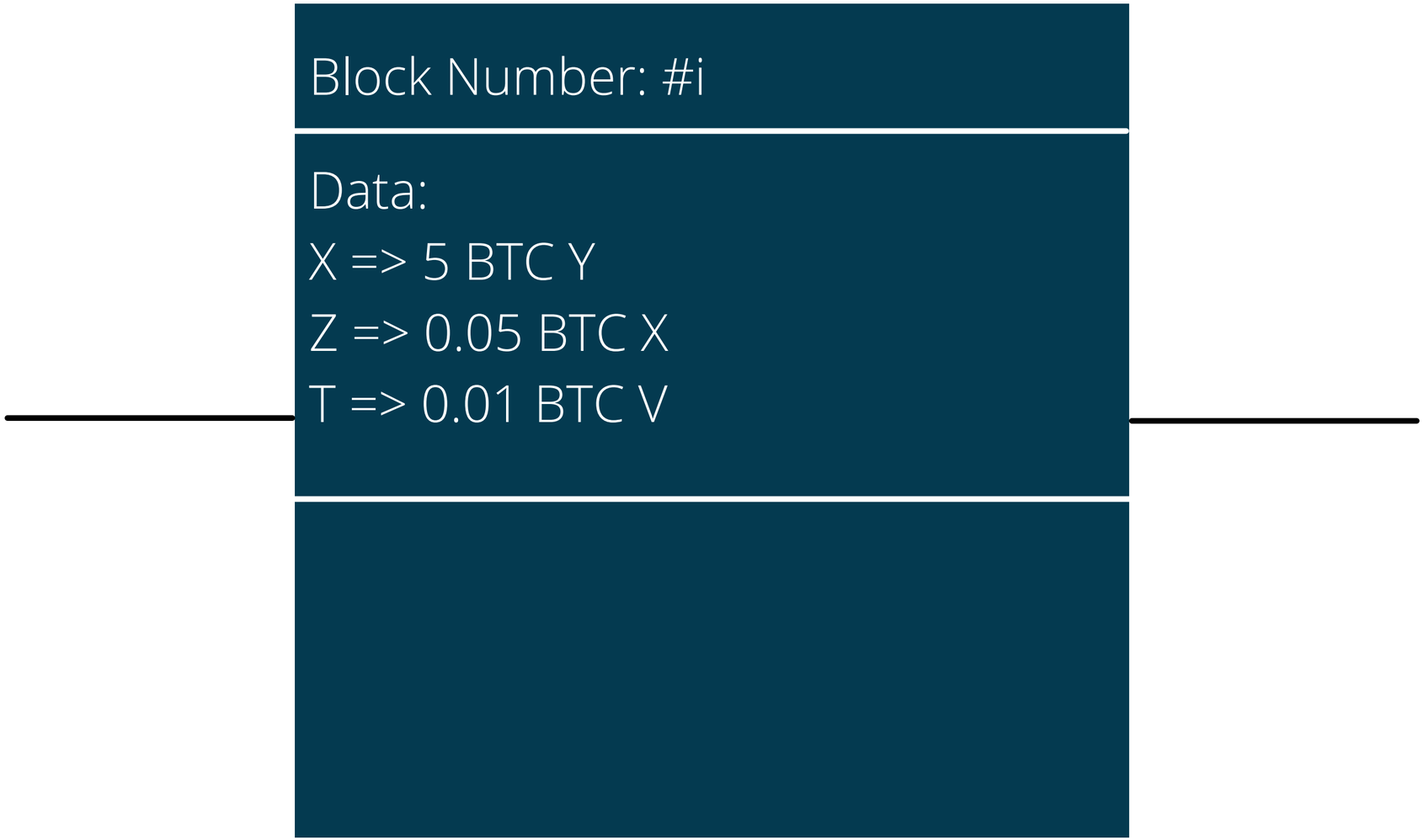
How mining works



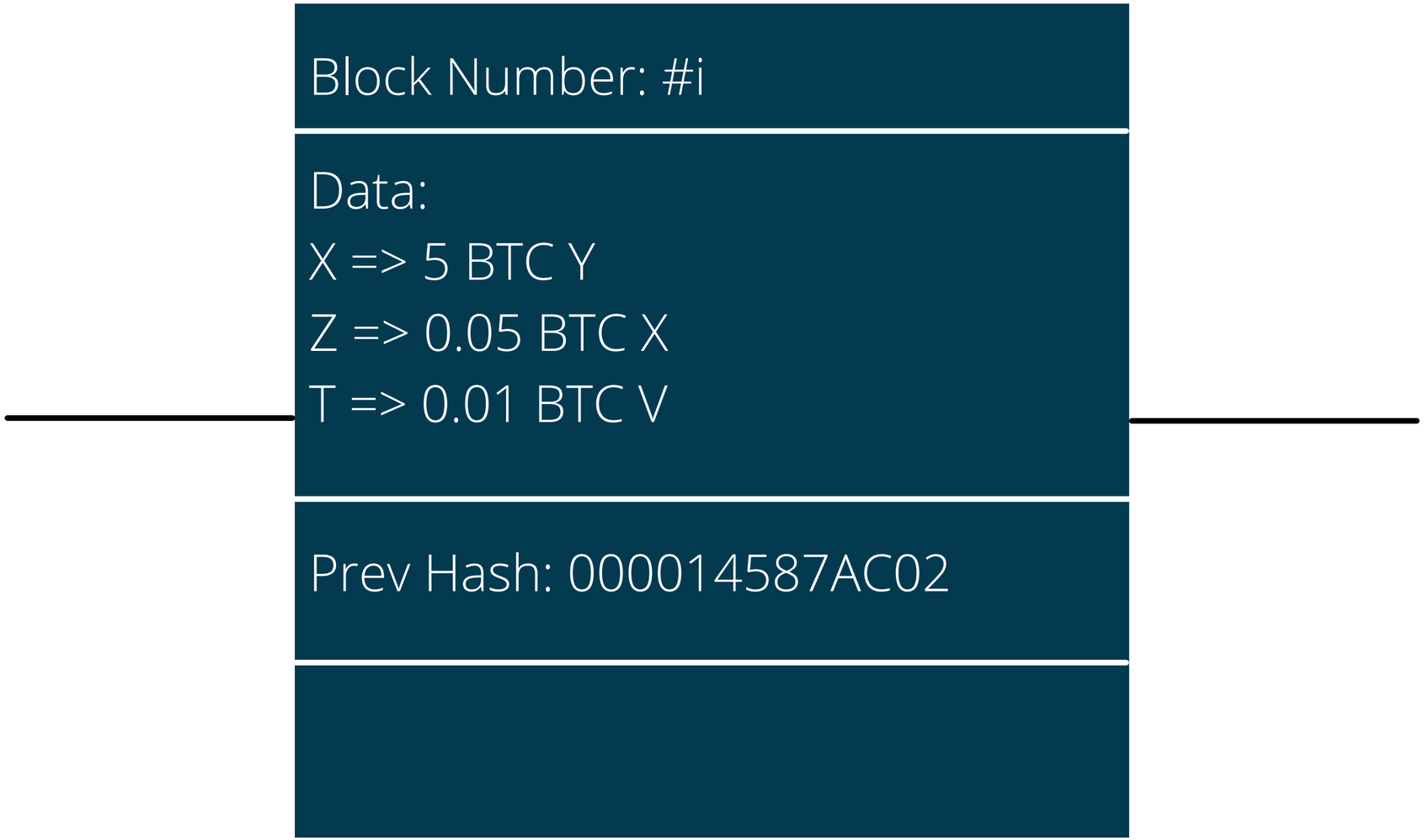
How mining works



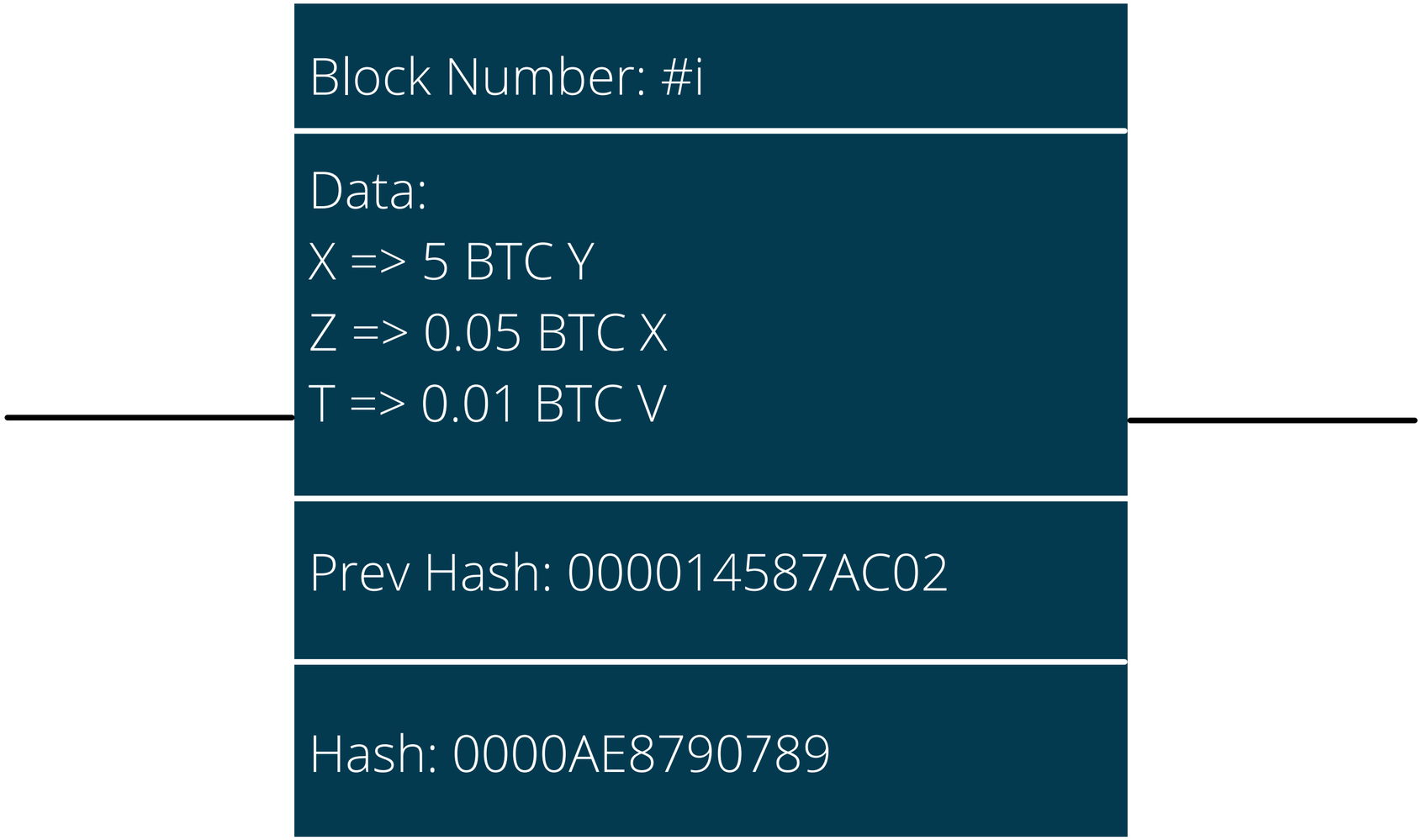
How mining works



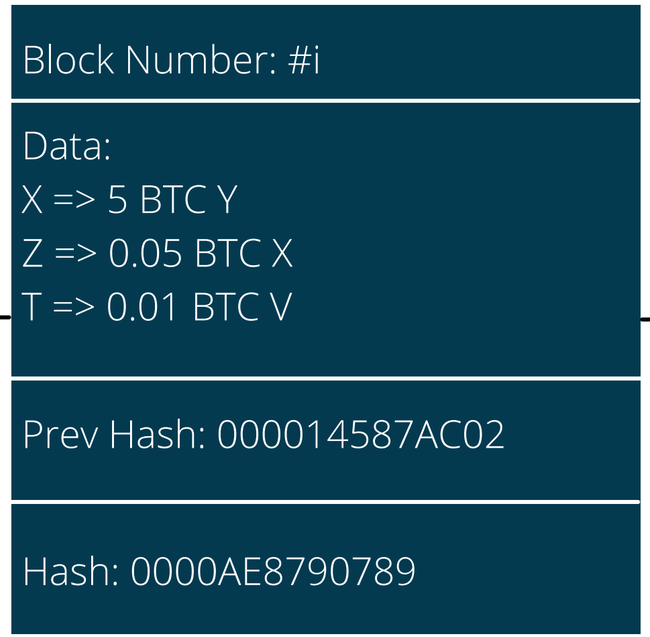
How mining works



How mining works

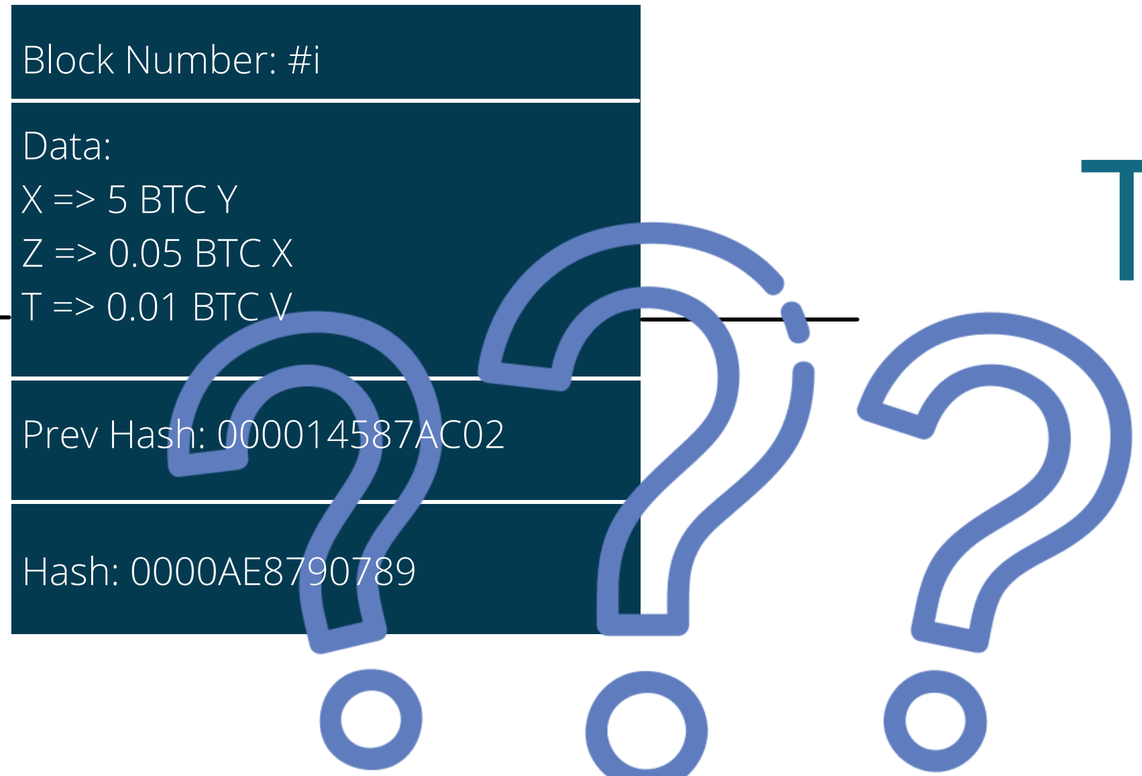


How mining works



Hash: hash_func(Block number , data, Prev Hash)

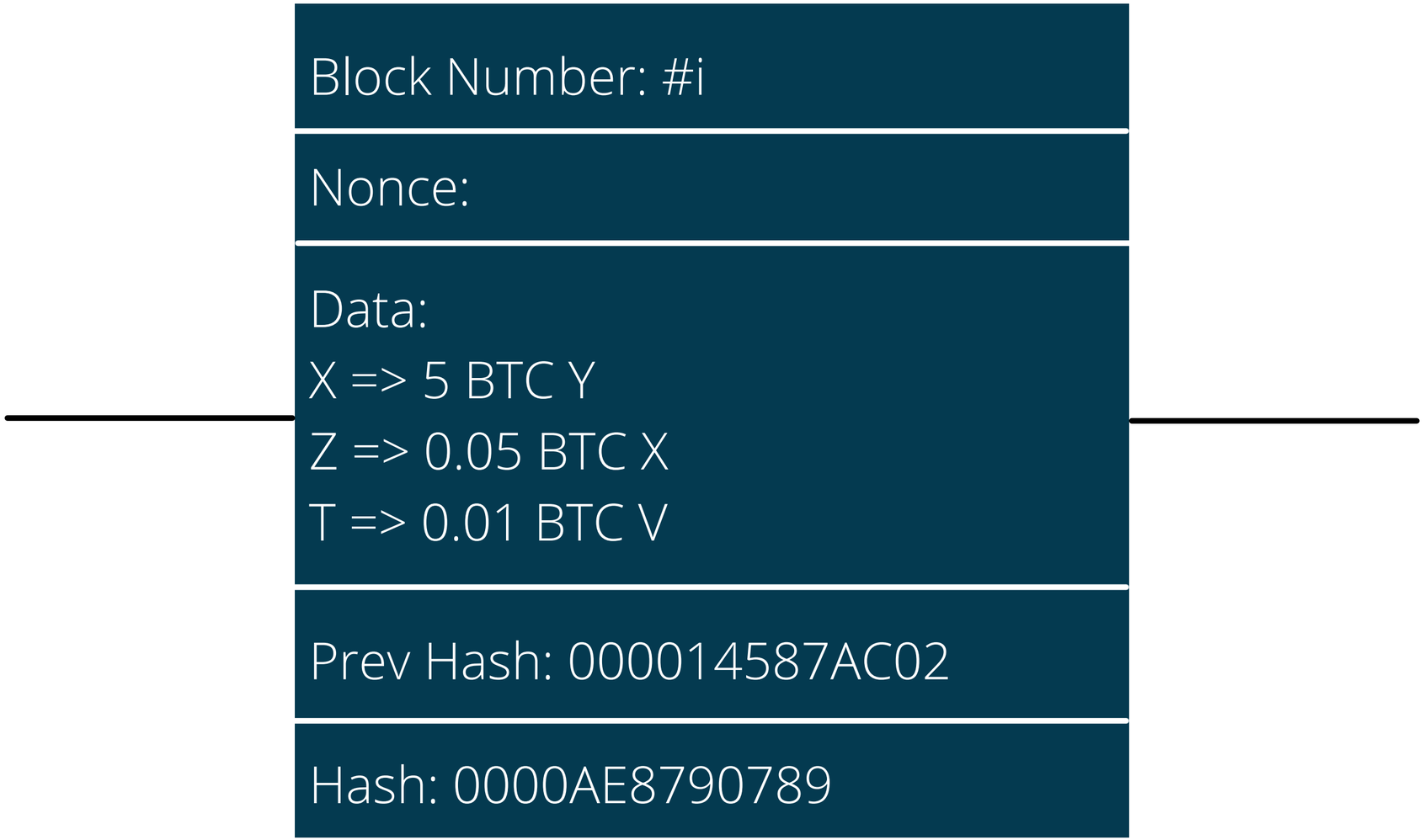
How mining works



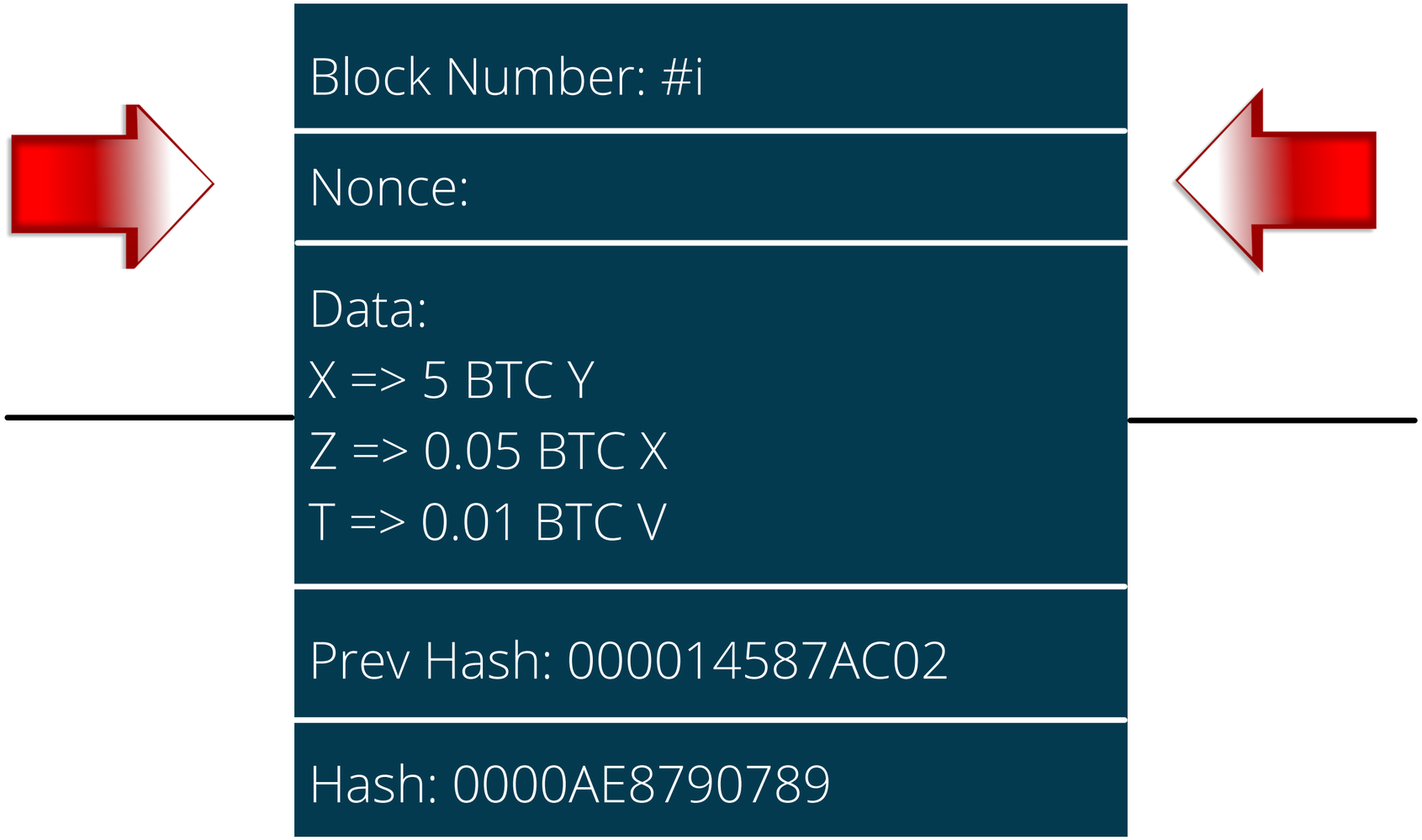
That Simple?

Hash: hash_func(Block number , data, Prev Hash)

How mining works



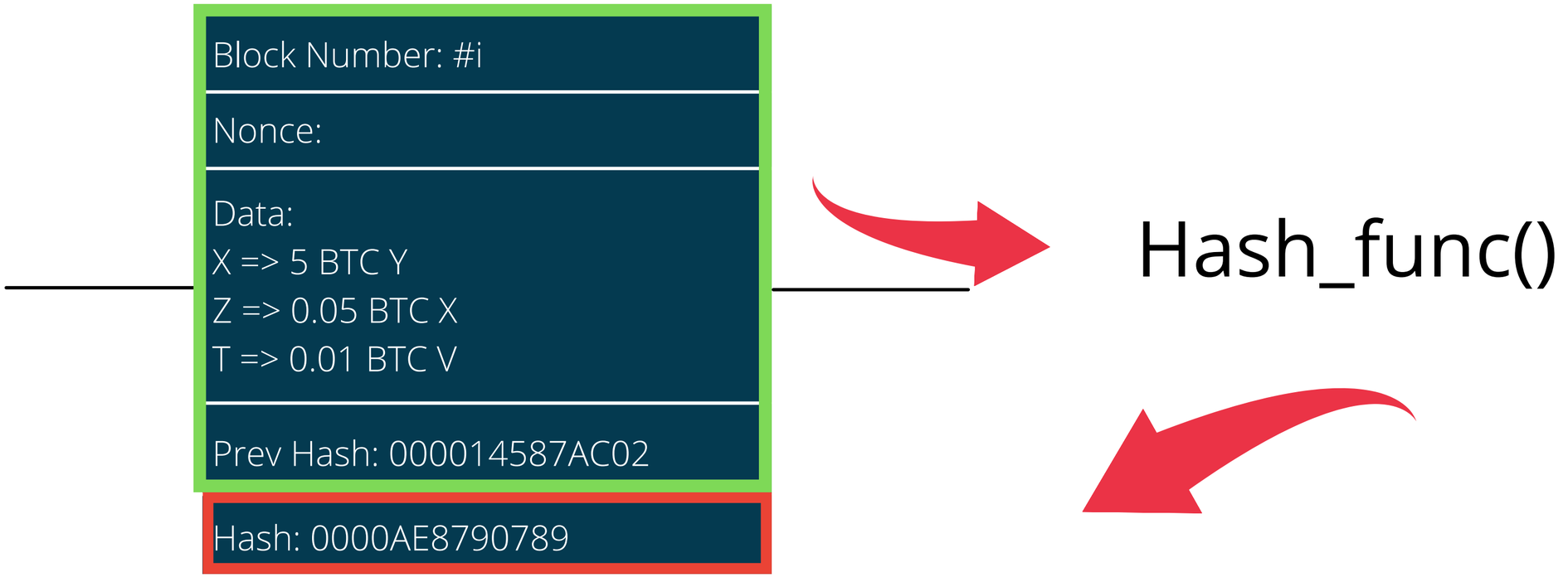
How mining works



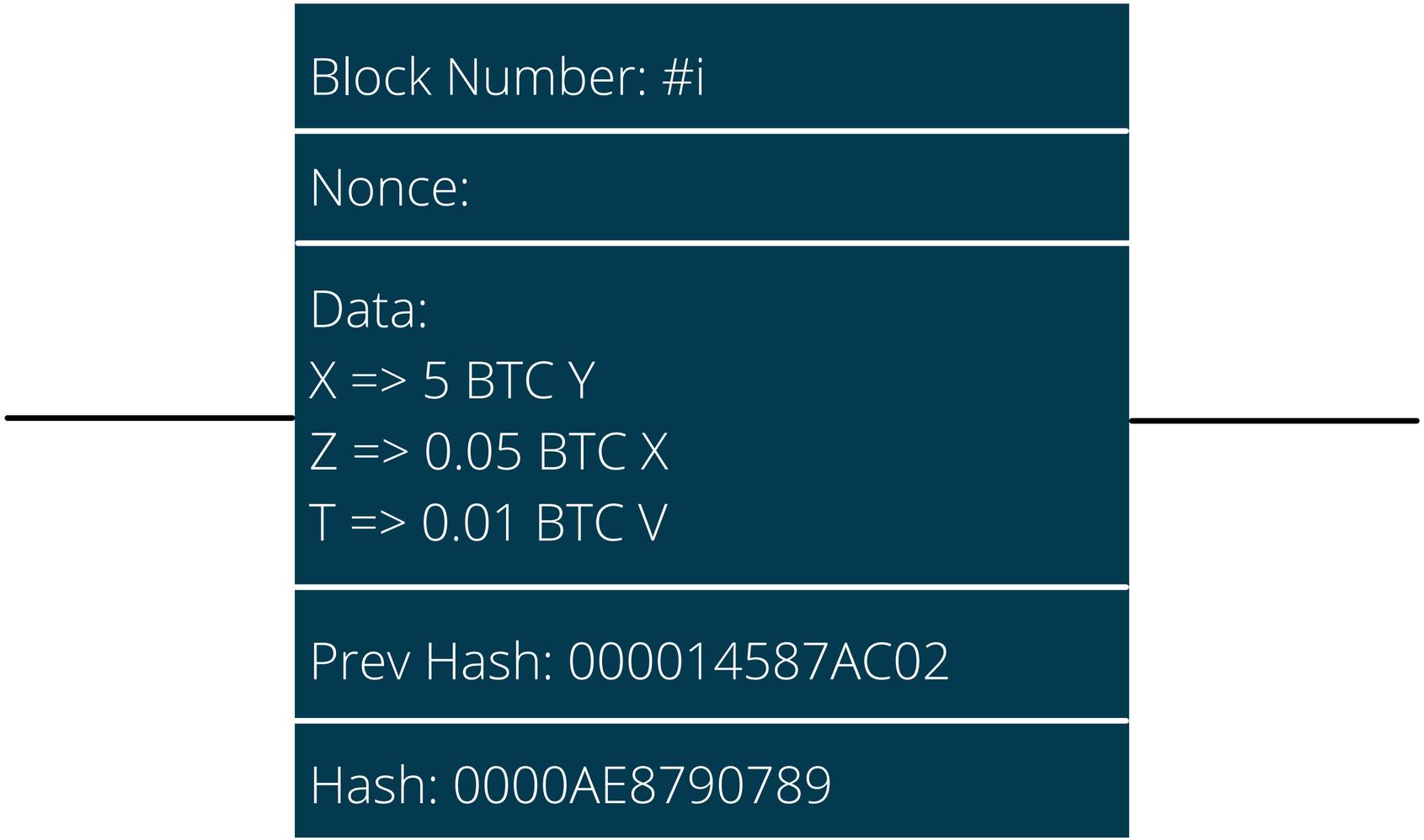
How mining works

How mining works

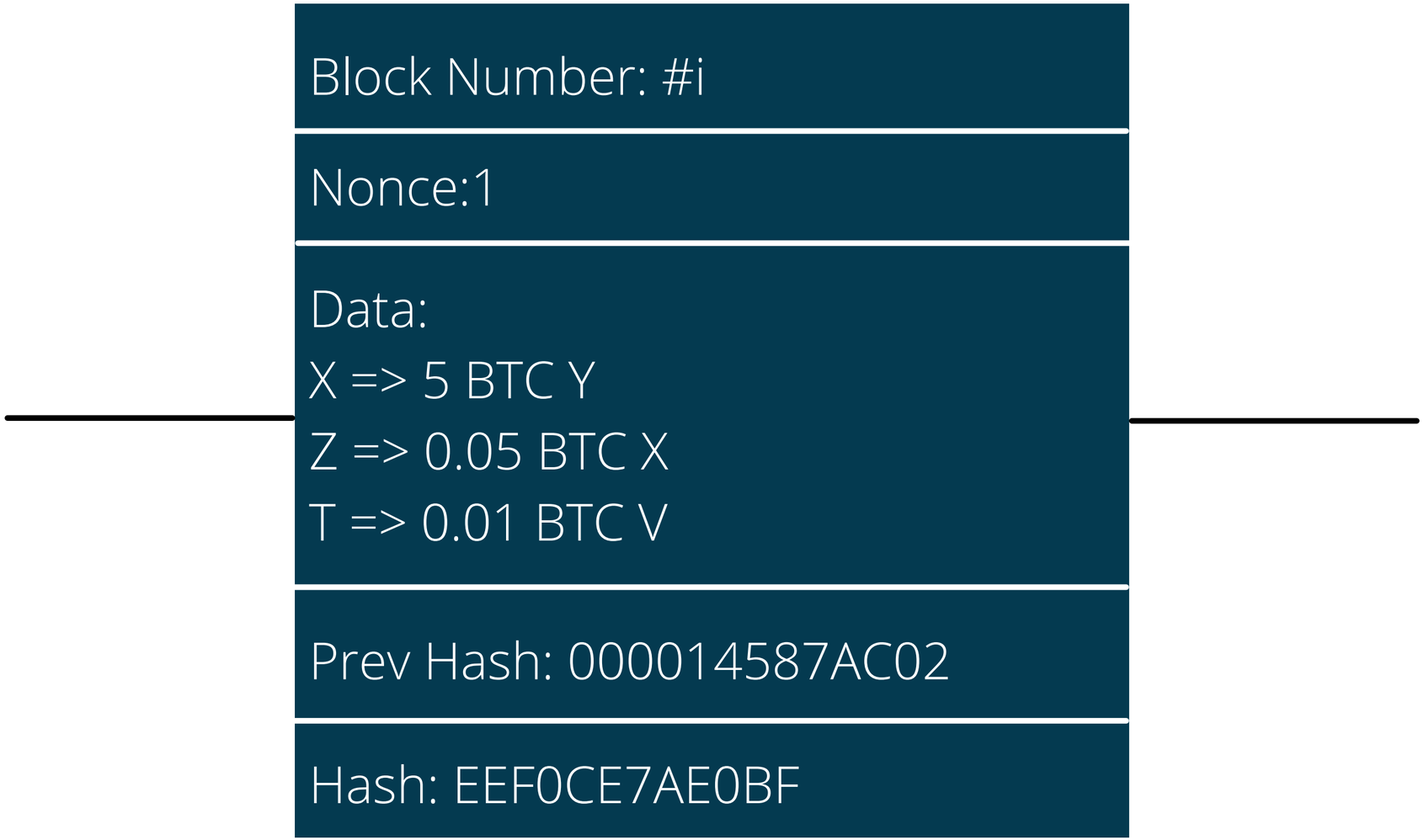
How mining works



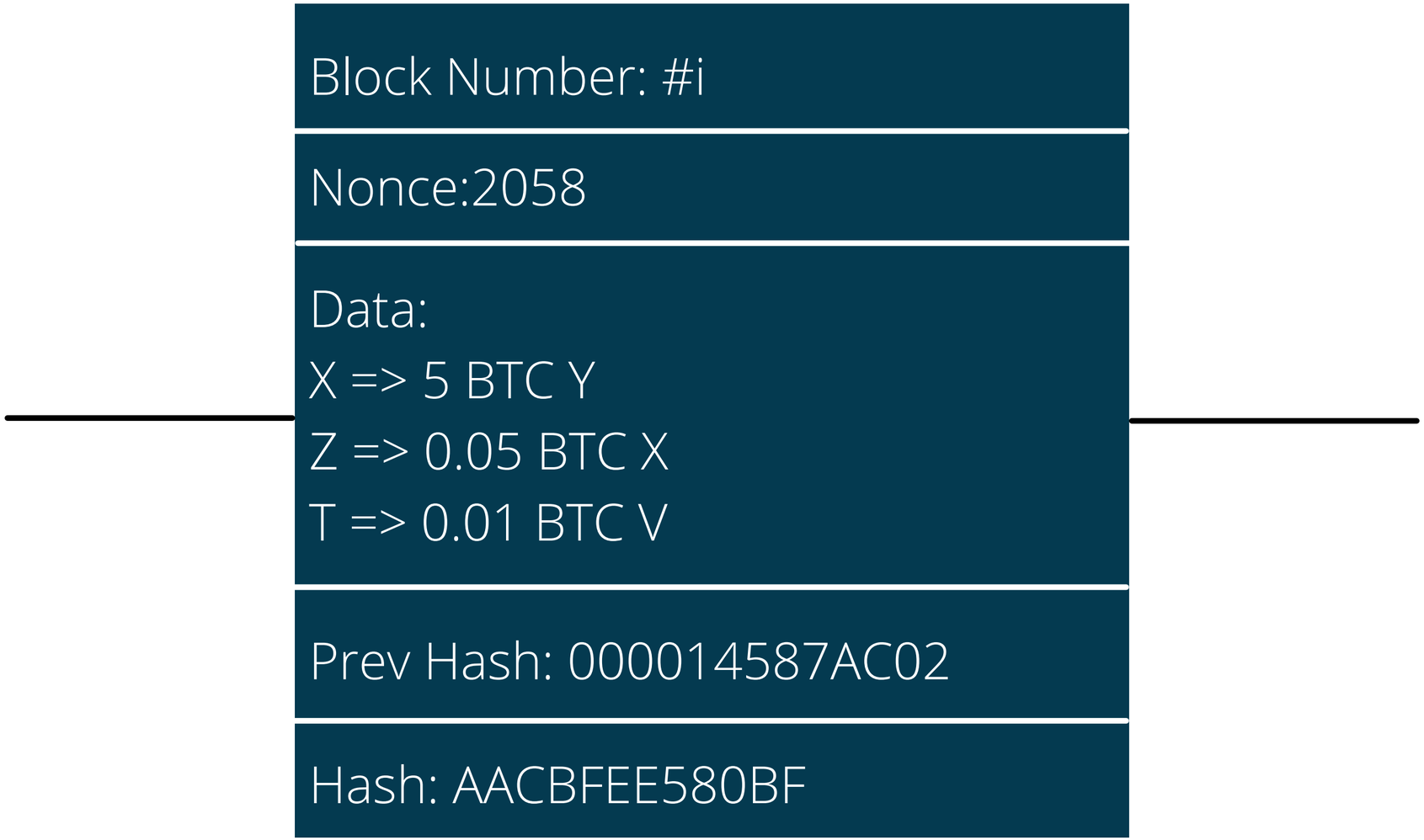
How mining works



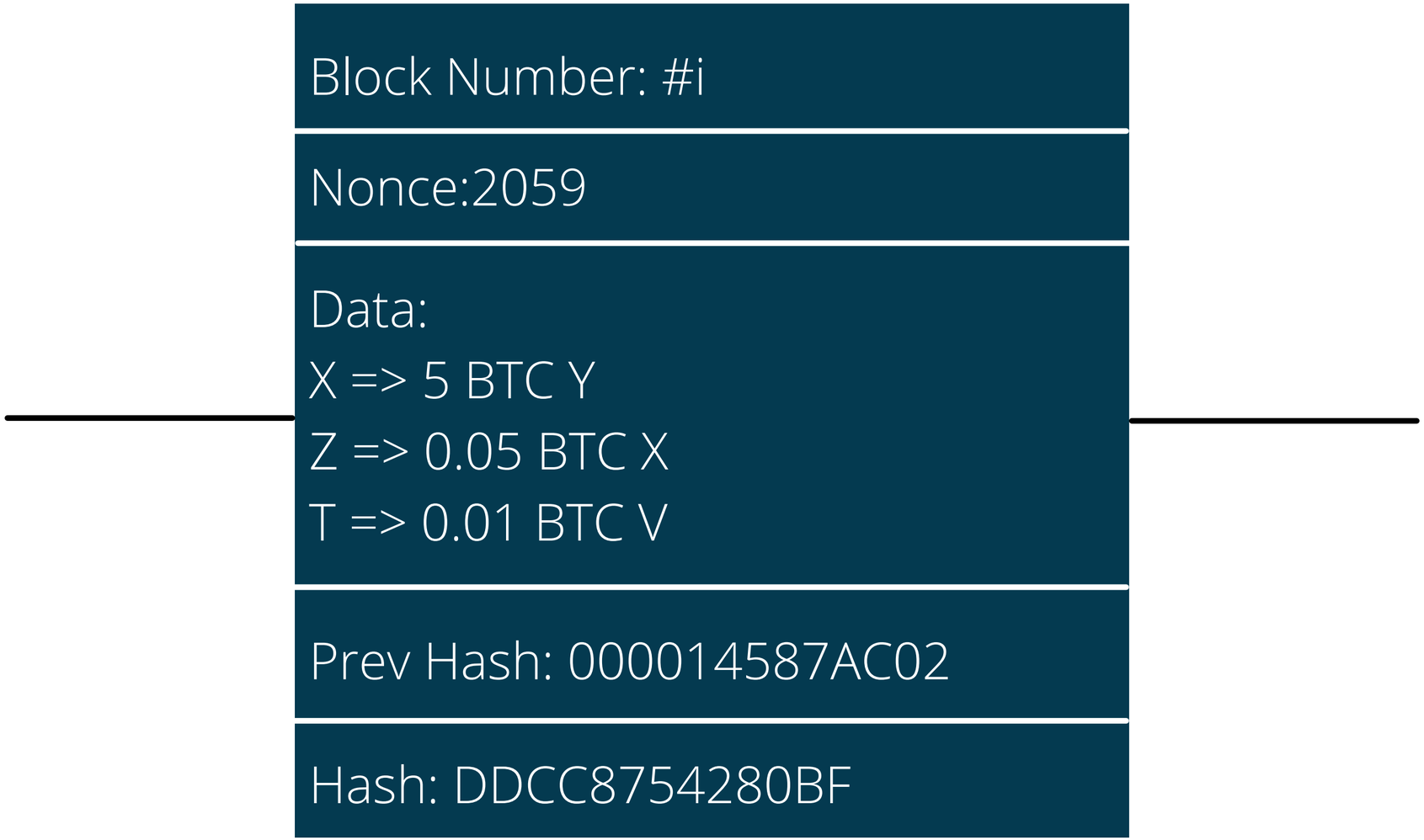
How mining works



How mining works



How mining works



How mining works

Hash is a Number:

How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08

How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08

All possible hashes

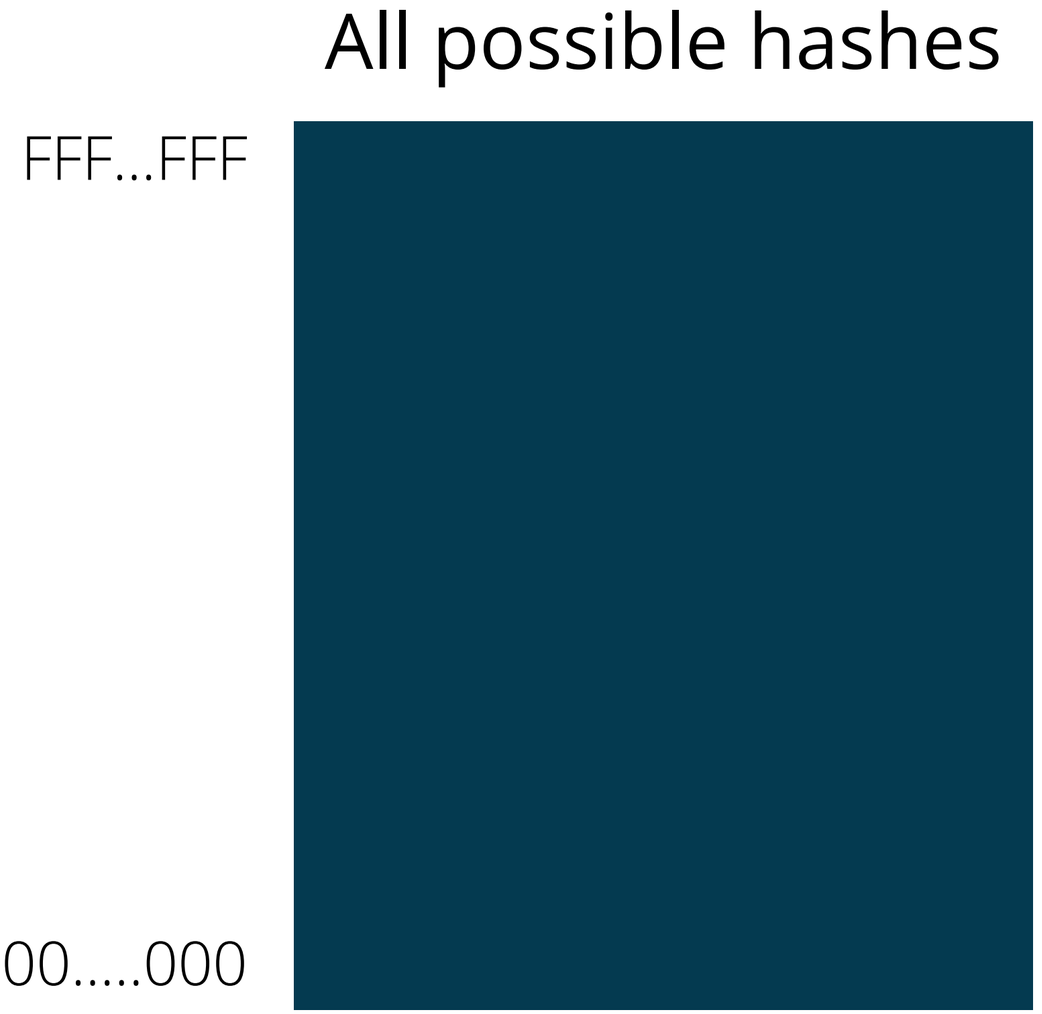
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



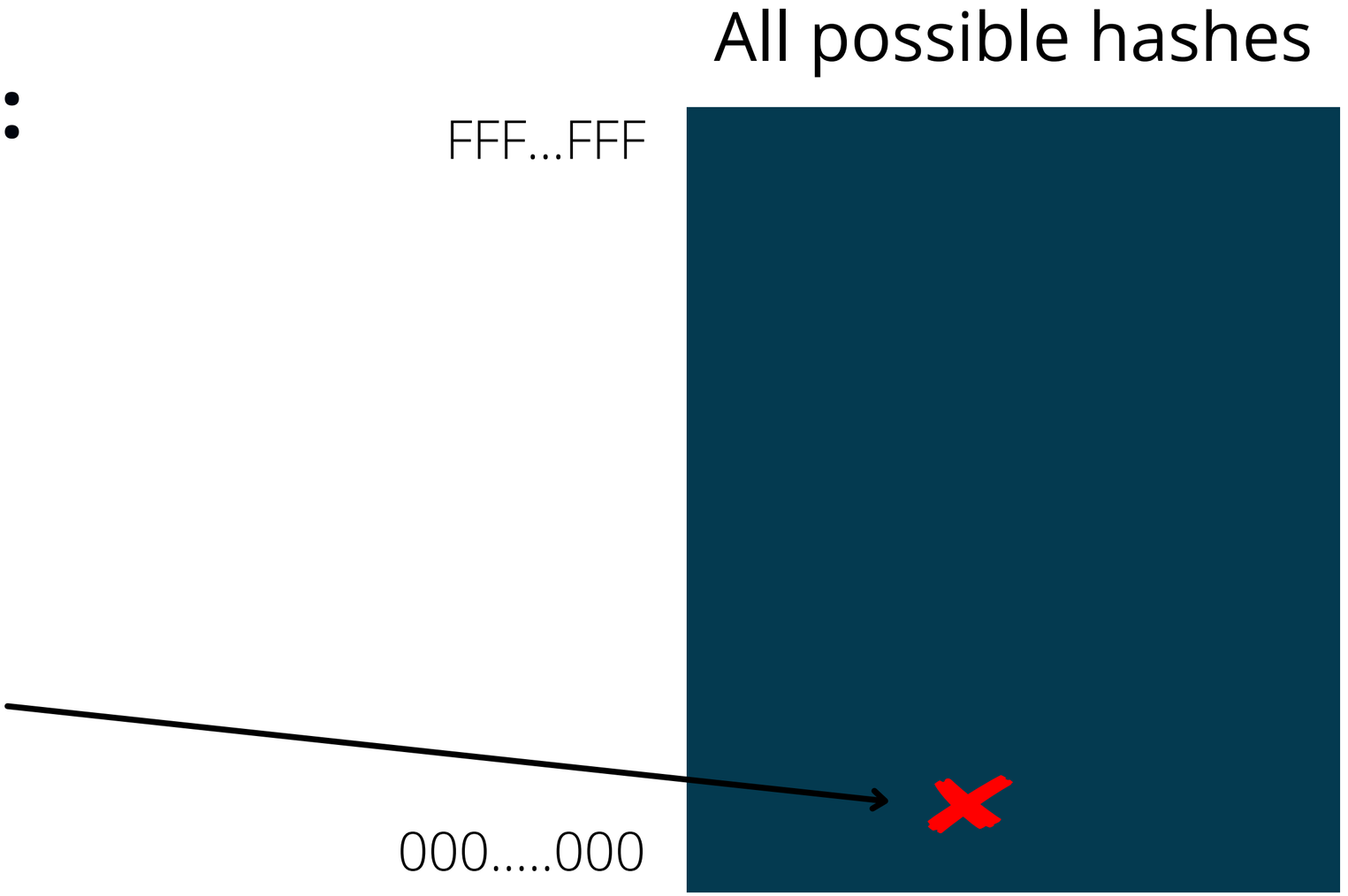
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



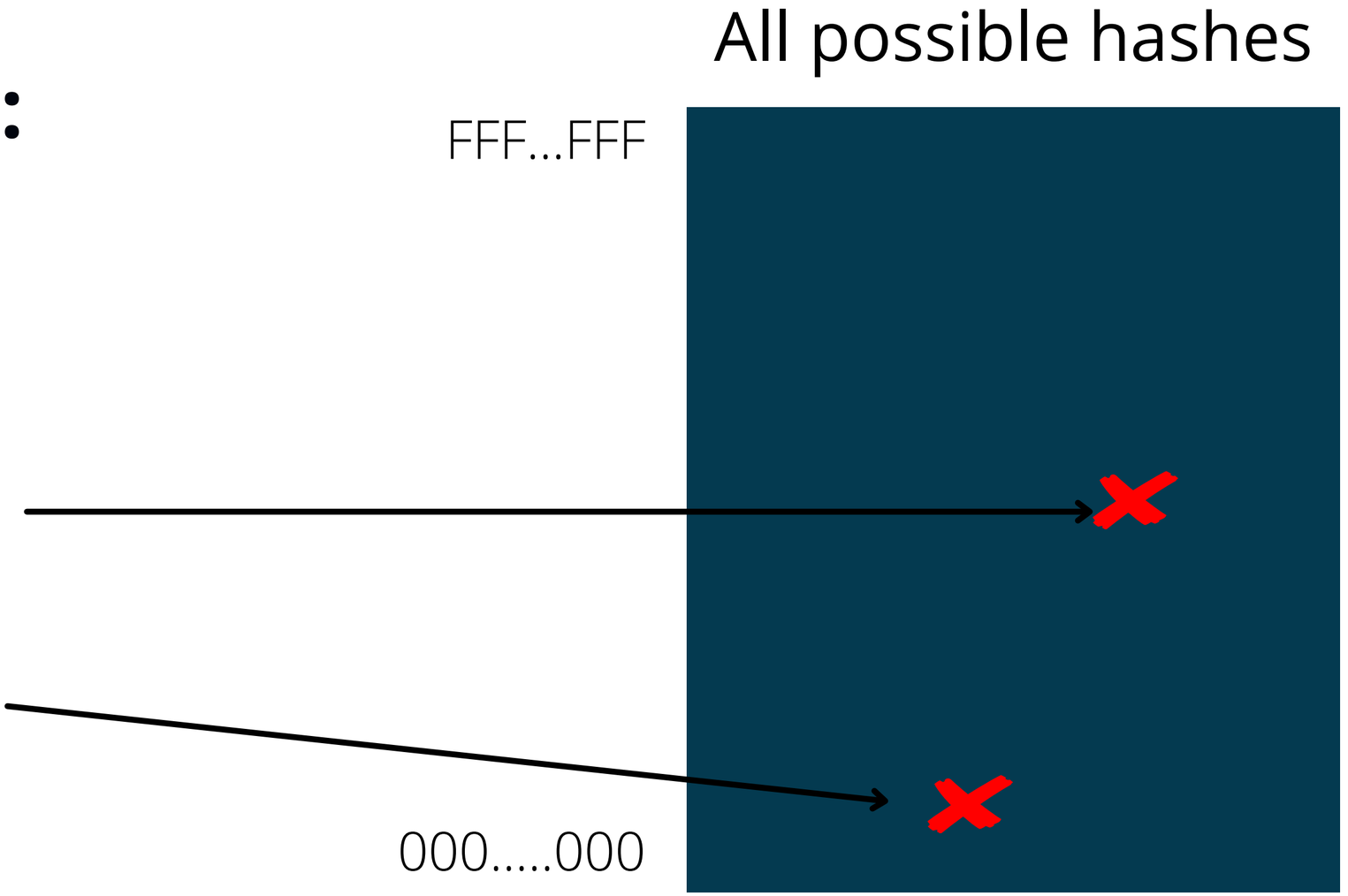
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



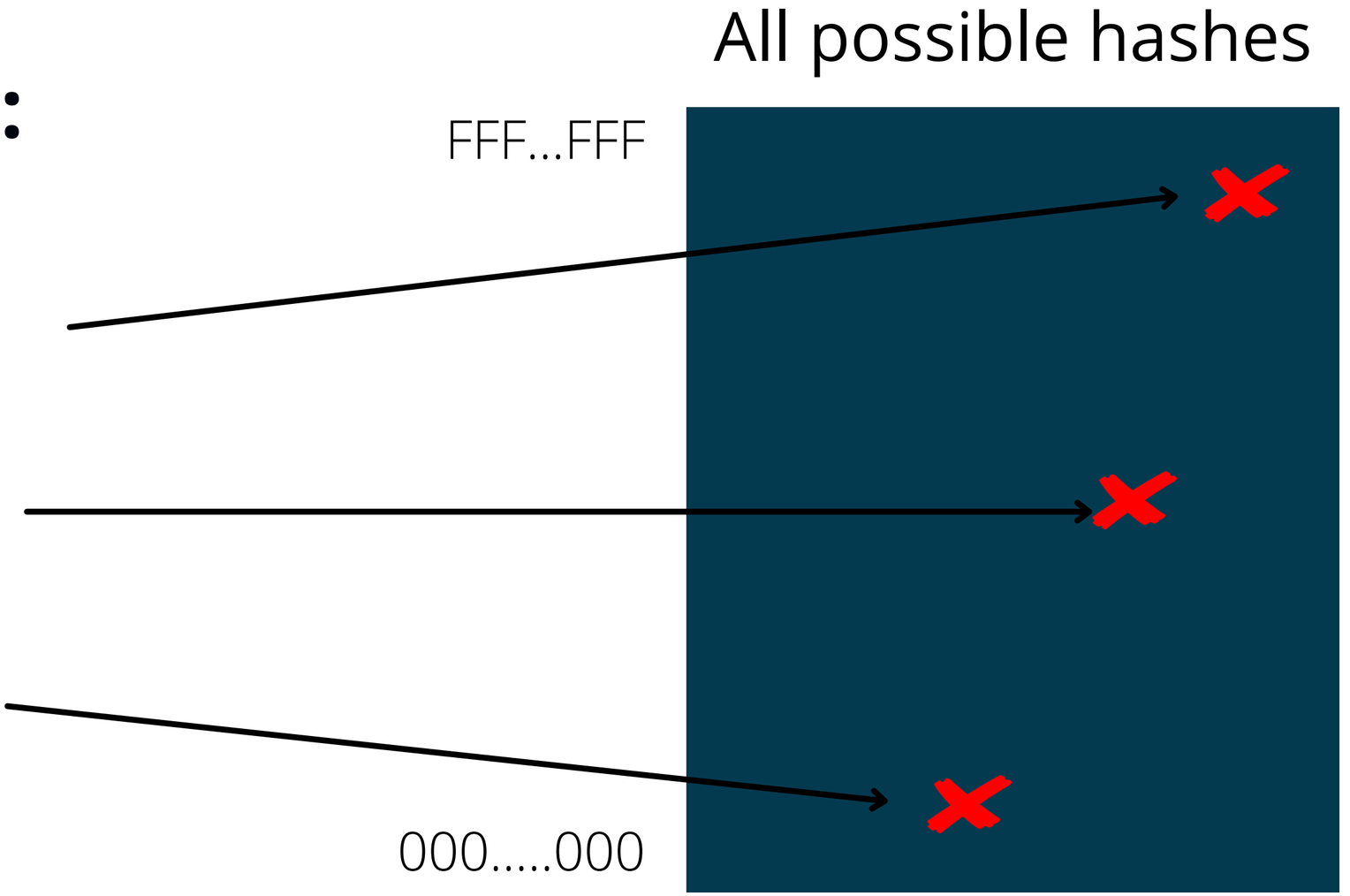
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



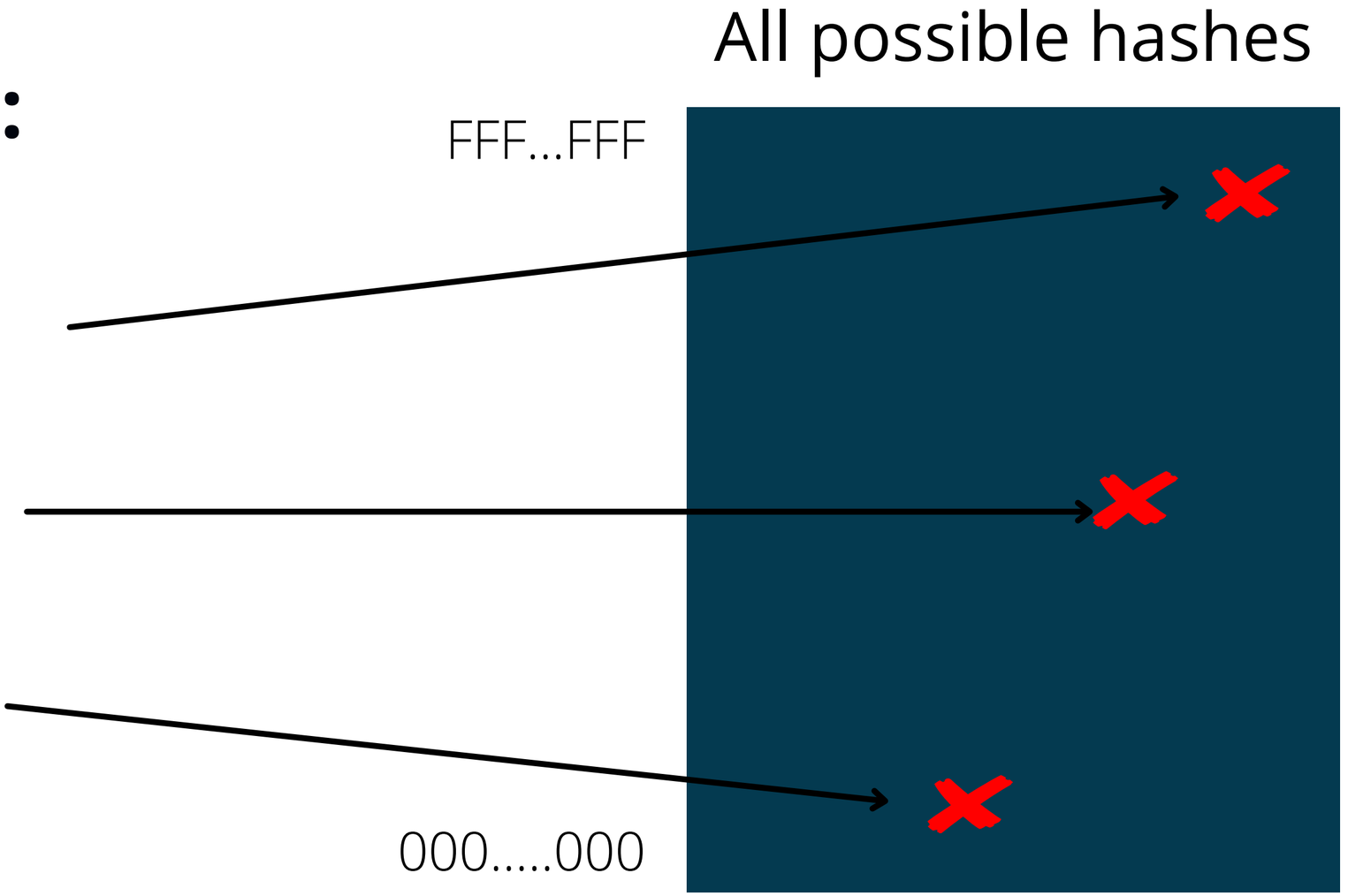
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



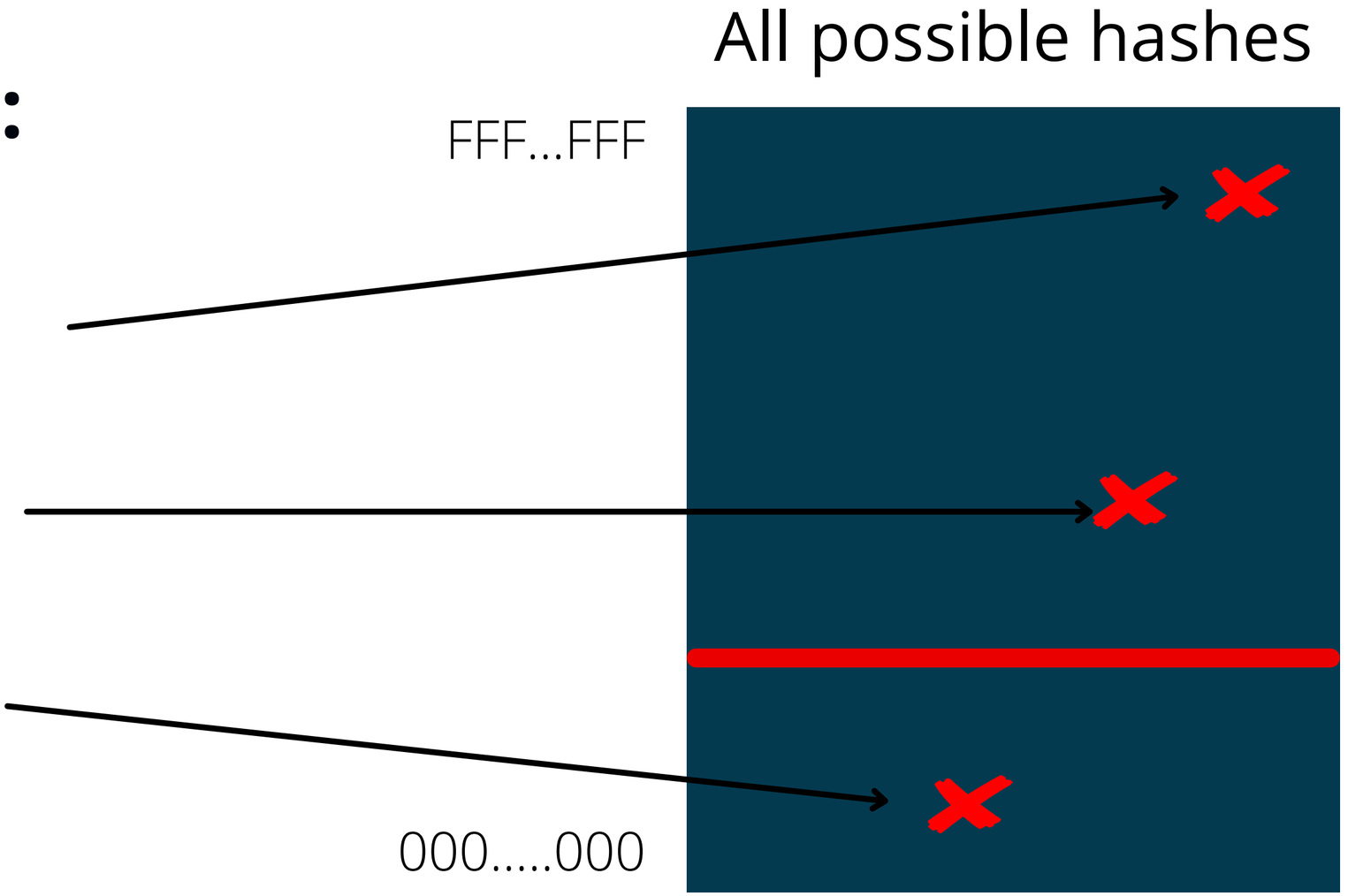
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



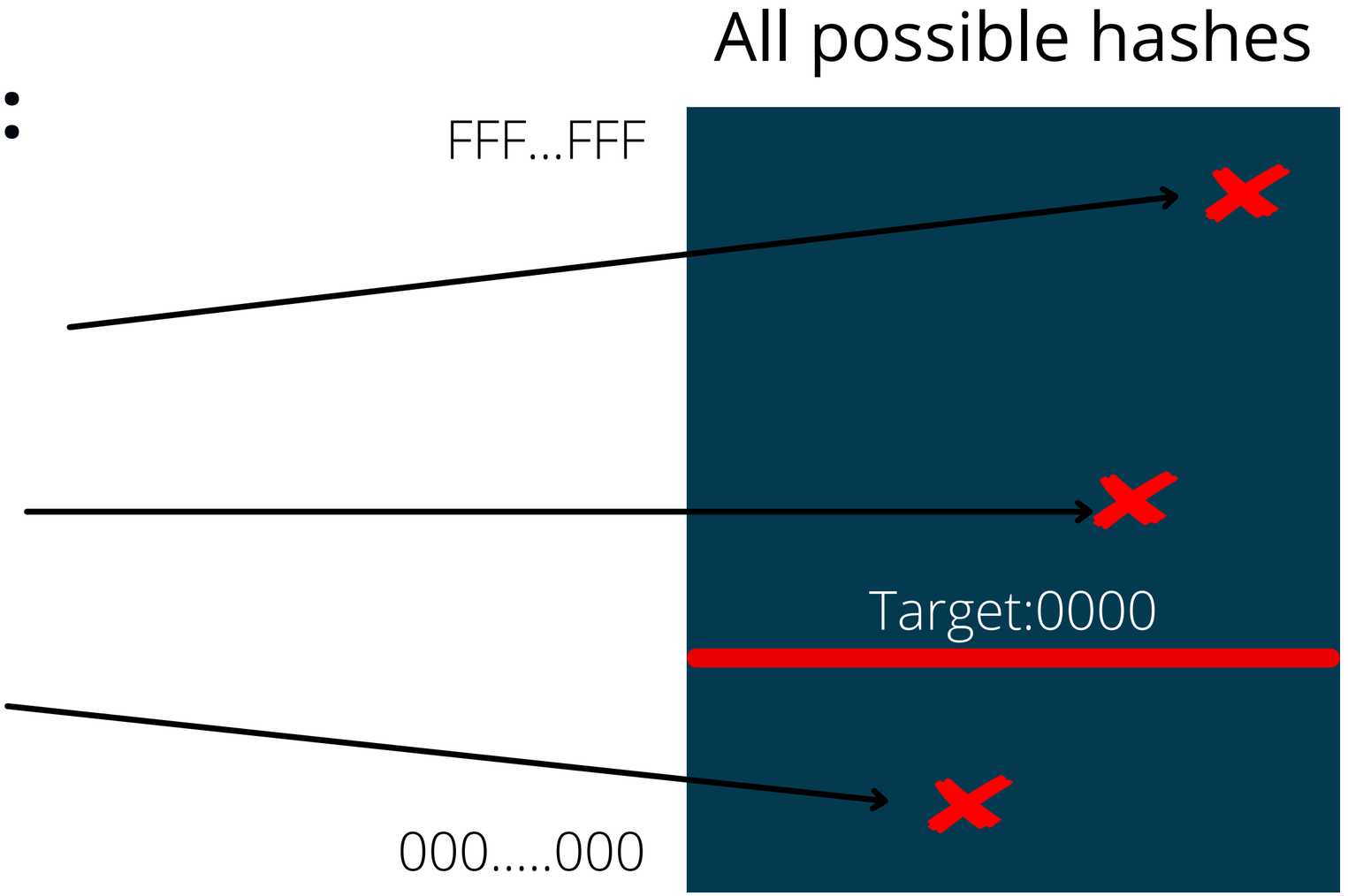
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

00000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



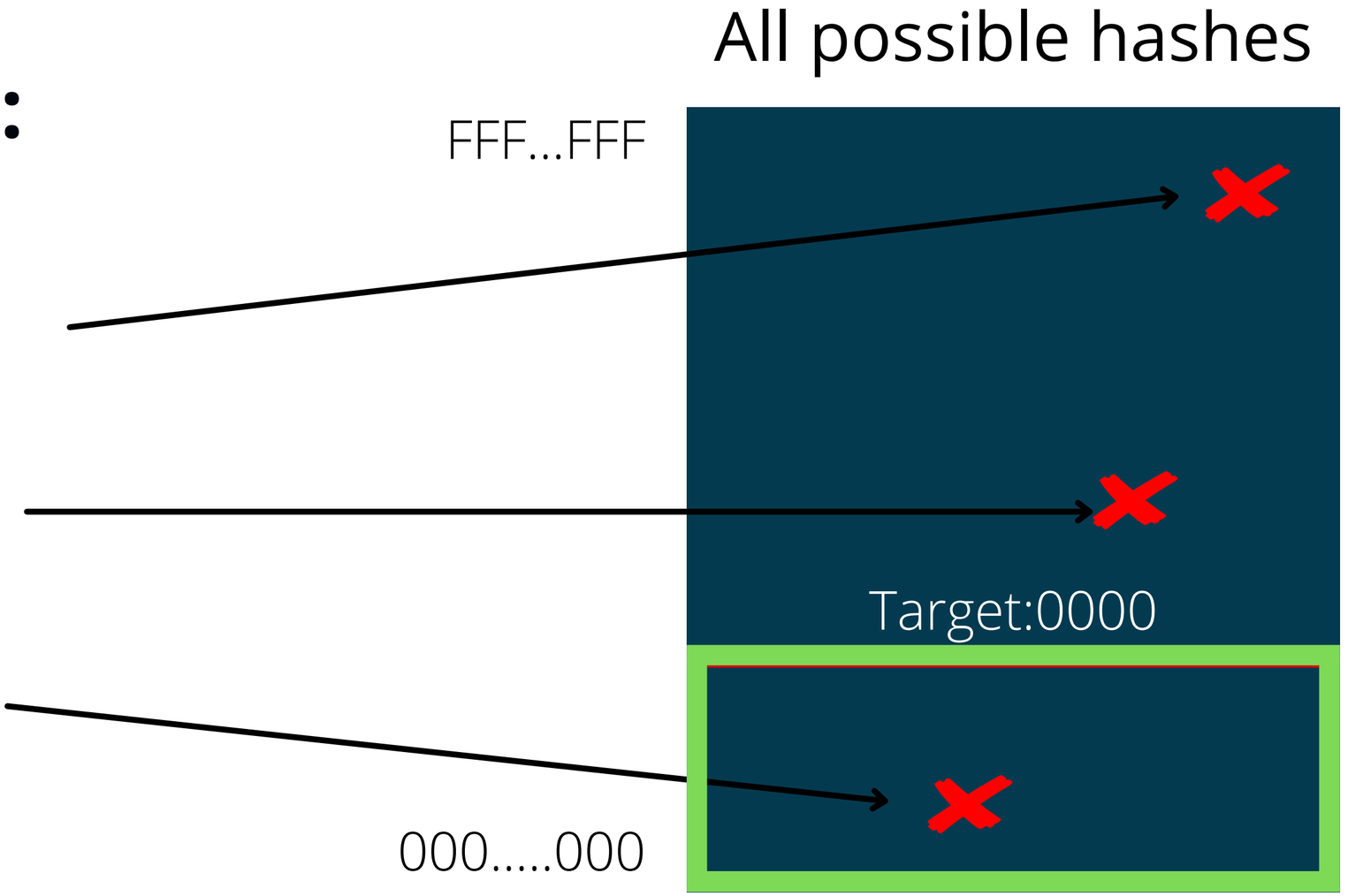
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

0000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



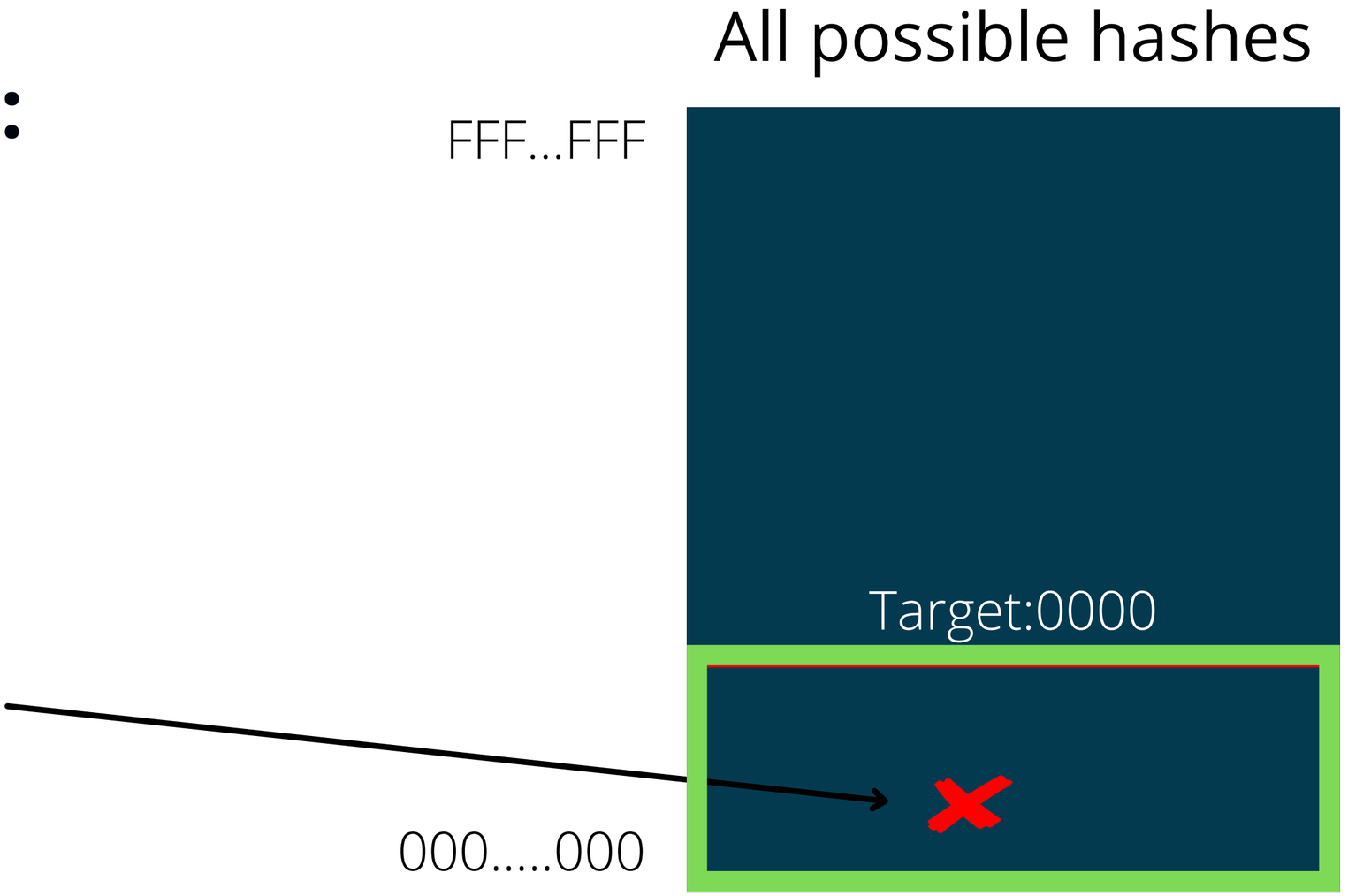
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896884c7d659a2feaa0c55ad015a
3bf4f1b2b0b822cde587015b0f00a08

0000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



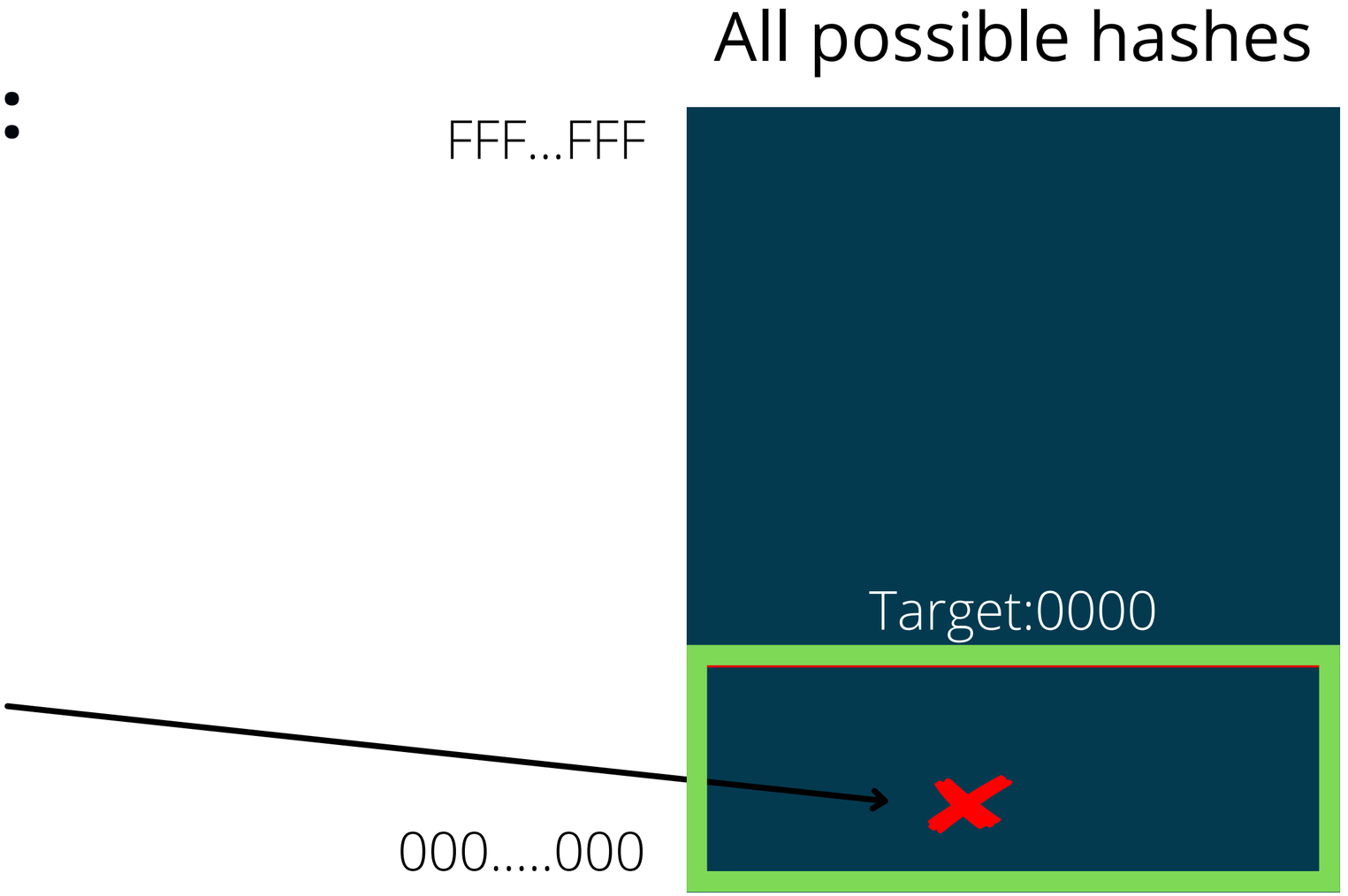
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896[illegible]59a2feaa0c55ad015a
3bf4f1b2[illegible]de587015b0f00a08

0000000000000000000eaa0c55ad015a
3bf4f1b2b0beeeee15d68880f00a08



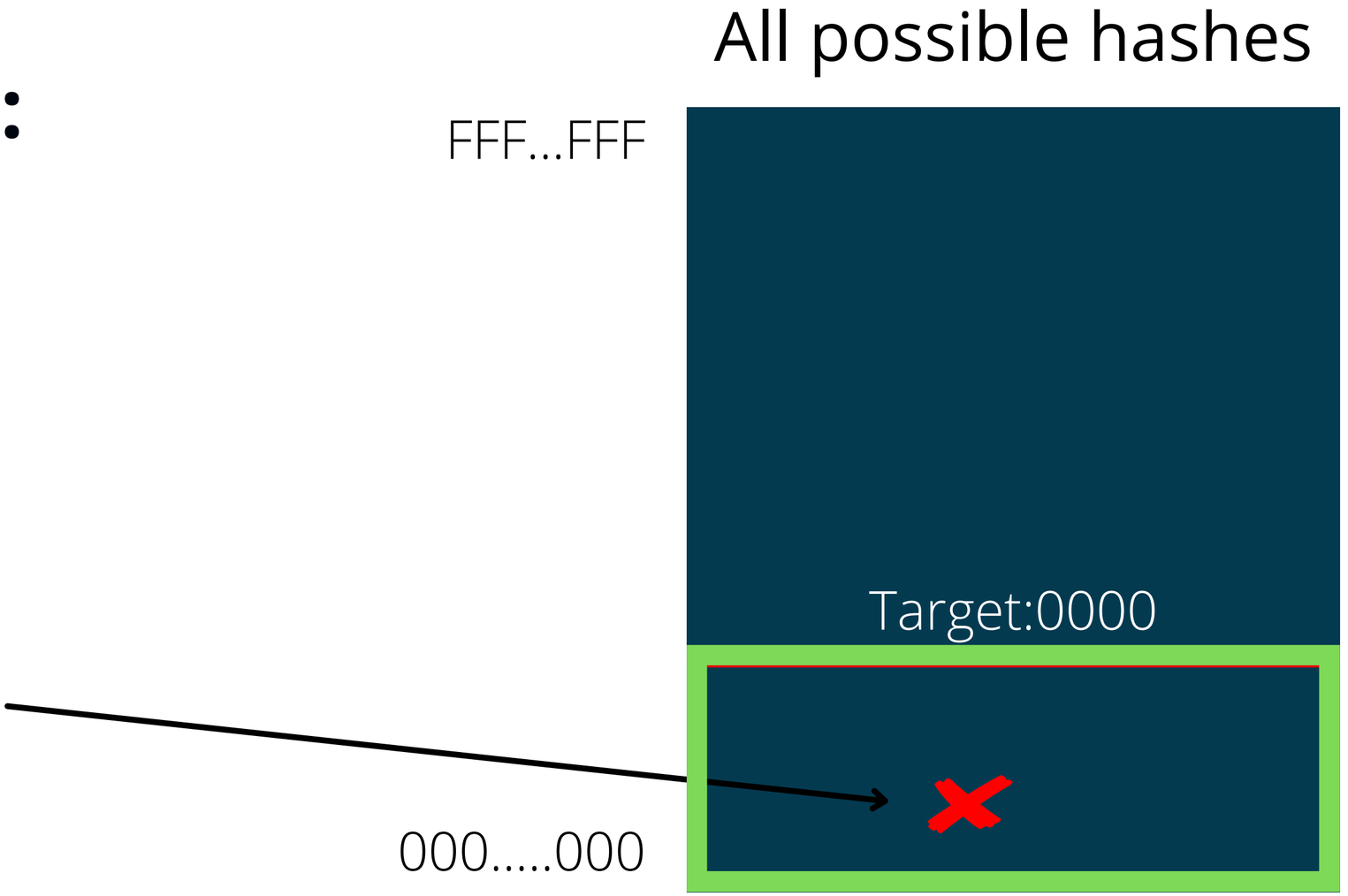
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896[illegible]59a2feaa0c55ad015a
3bf4f1b2[illegible]de587015b0f00a08

000000000000000[illegible]000eaa0c55ad015a
3bf4f1b[illegible]ee[illegible]ee15d68880f00a08



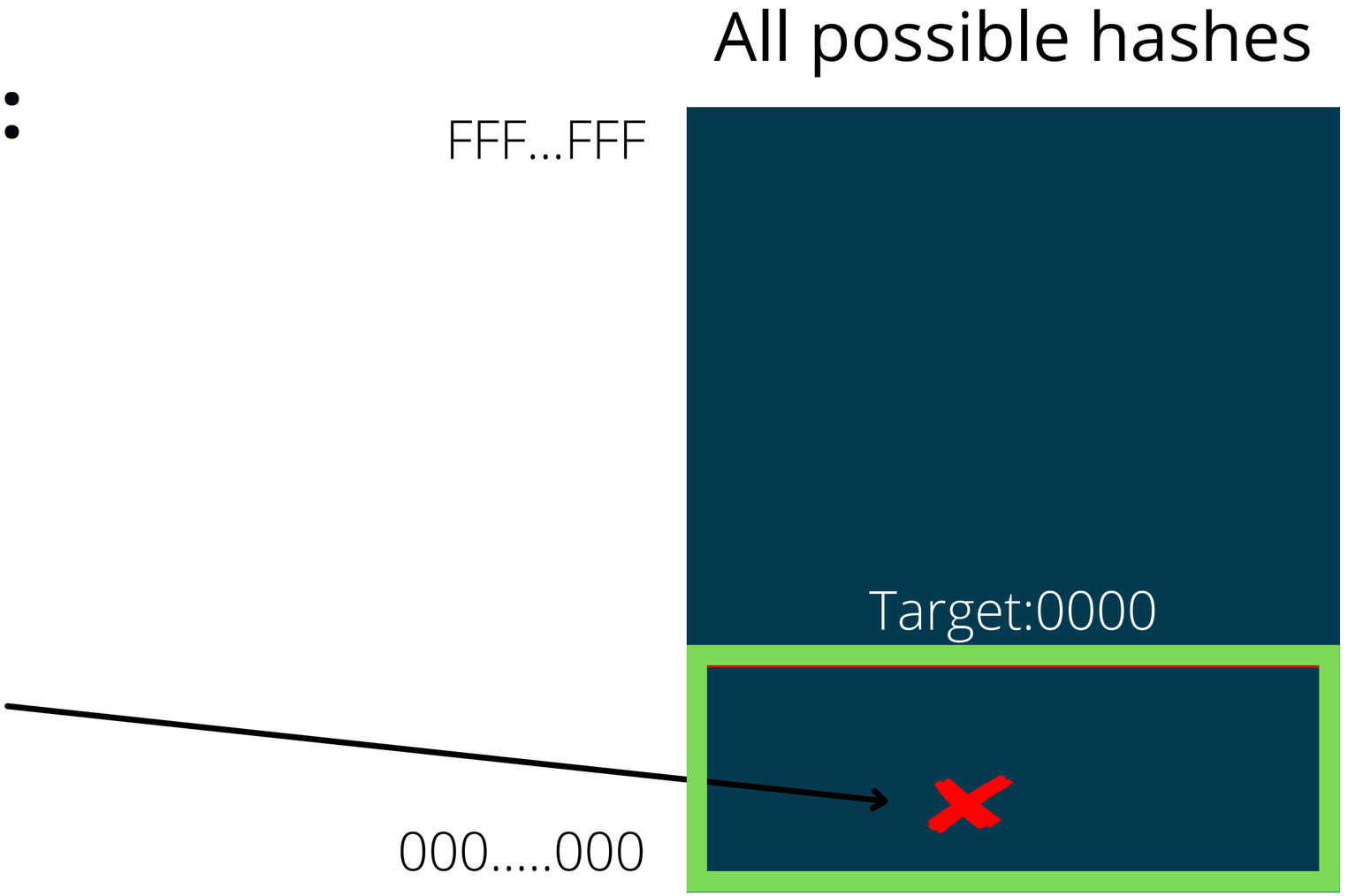
How mining works

Hash is a Number:

9f86d081884c7d659a2feaa0c55ad015a3
bf4f1b2b0b822cd15d6c15b0f00a08

000EC5896[illegible]59a2feaa0c55ad015a
3bf4f1b2[illegible]de587015b0f00a08

000000000000000[illegible]000eaa0c55ad015a
3bf4f1b[illegible]ee[illegible]ee15d68880f00a08



How mining works

Lets resume...

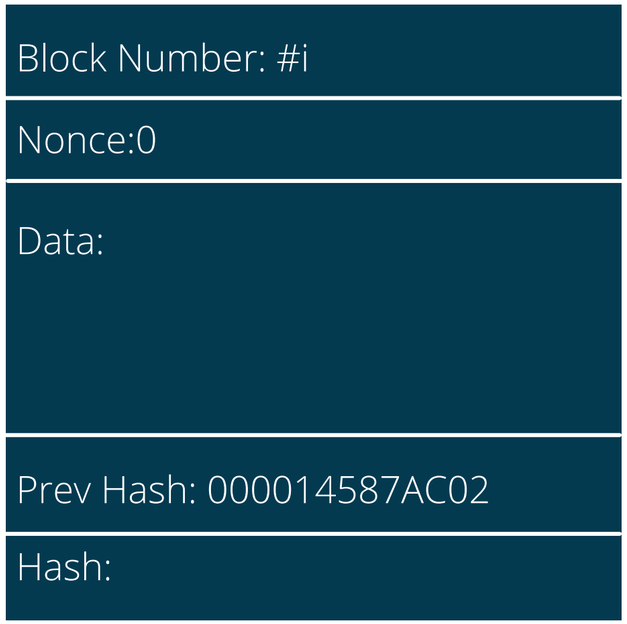
How mining works

How mining works

Data comes in...

How mining works

Data comes in...



How mining works

All possible hashes

Block Number: #i

Nonce:0

Data:

Prev Hash: 000014587AC02

Hash:

How mining works

Block Number: #i

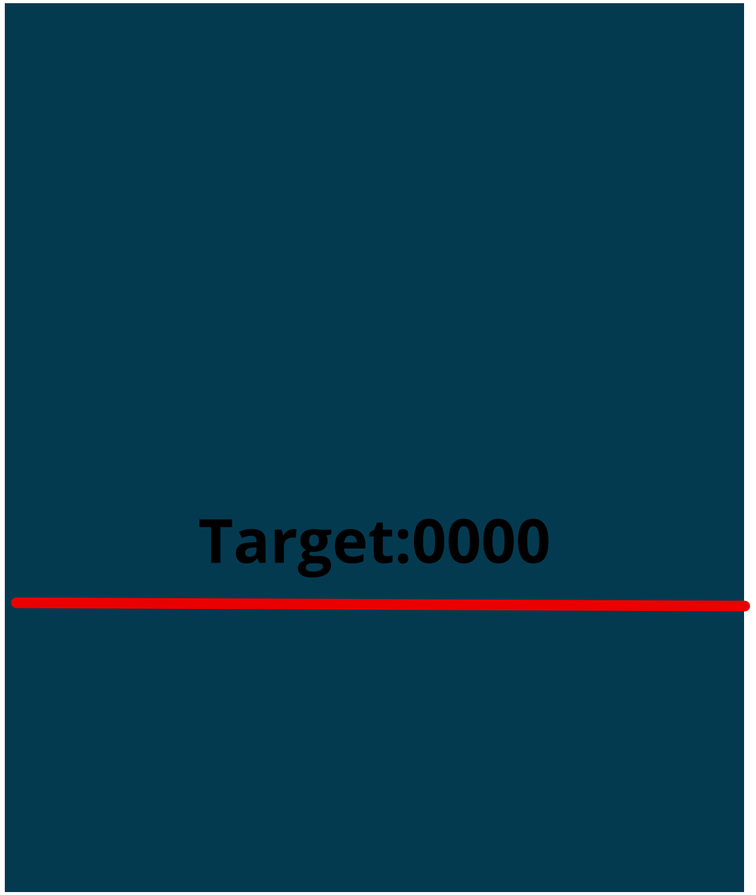
Nonce:0

Data:

Prev Hash: 000014587AC02

Hash:

All possible hashes



How mining works

Block Number: #i

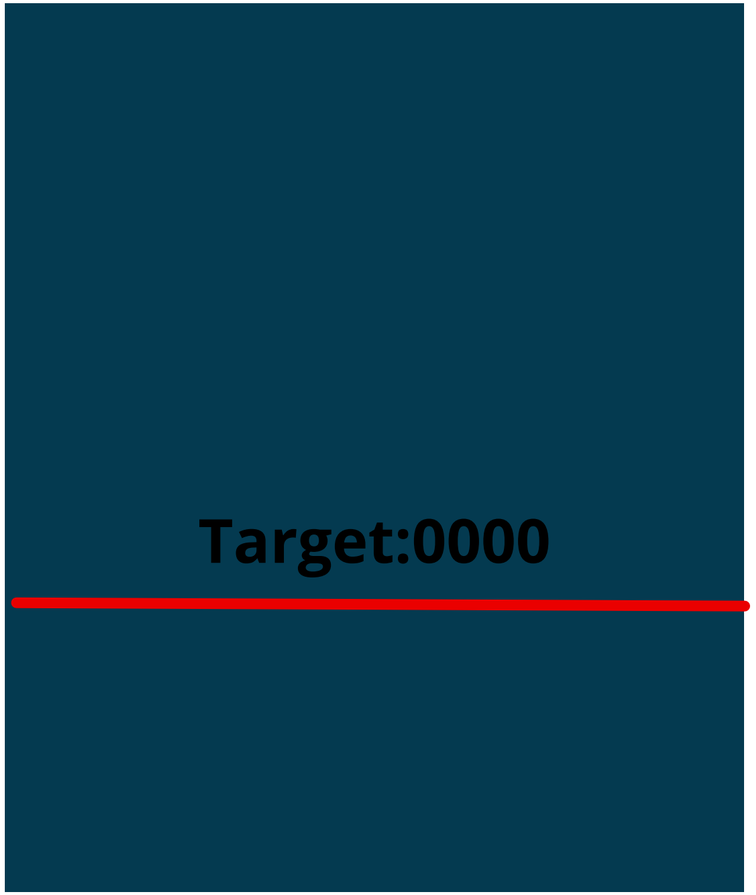
Nonce:0

Data:

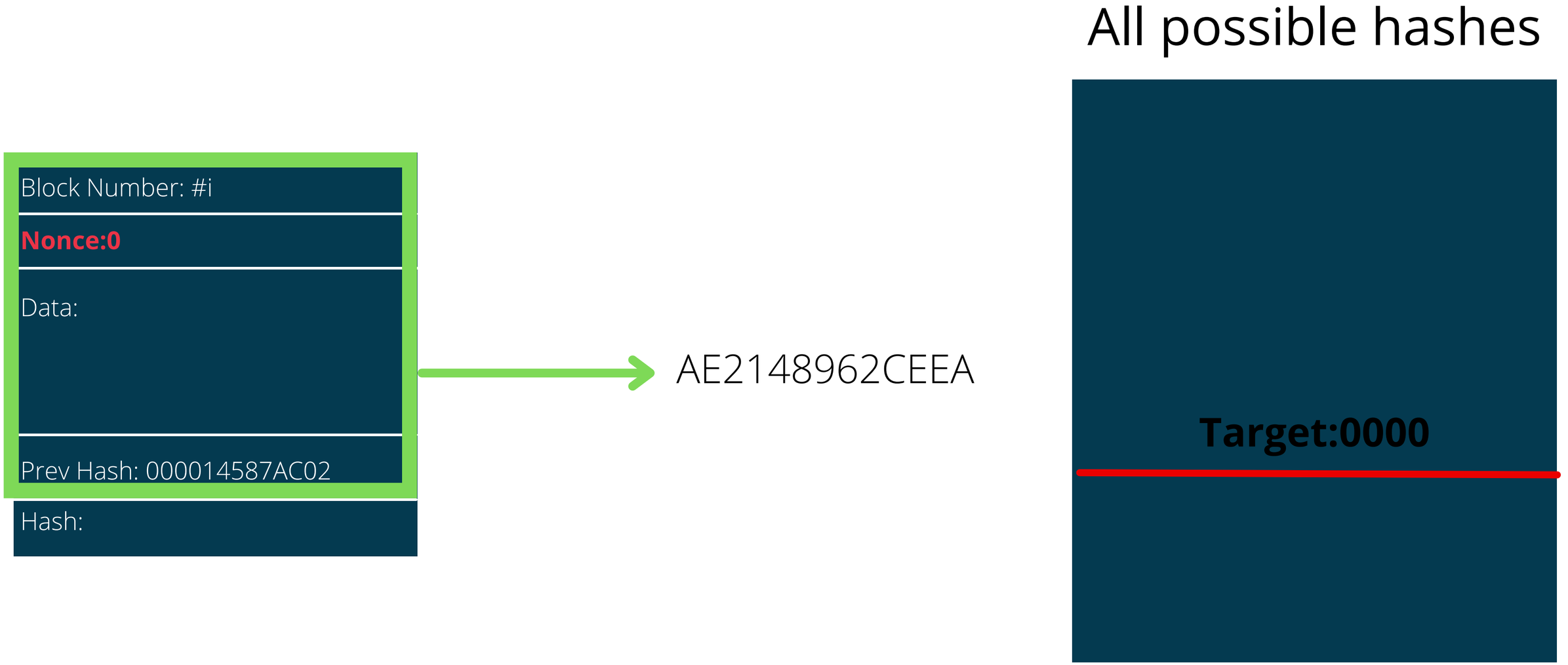
Prev Hash: 000014587AC02

Hash:

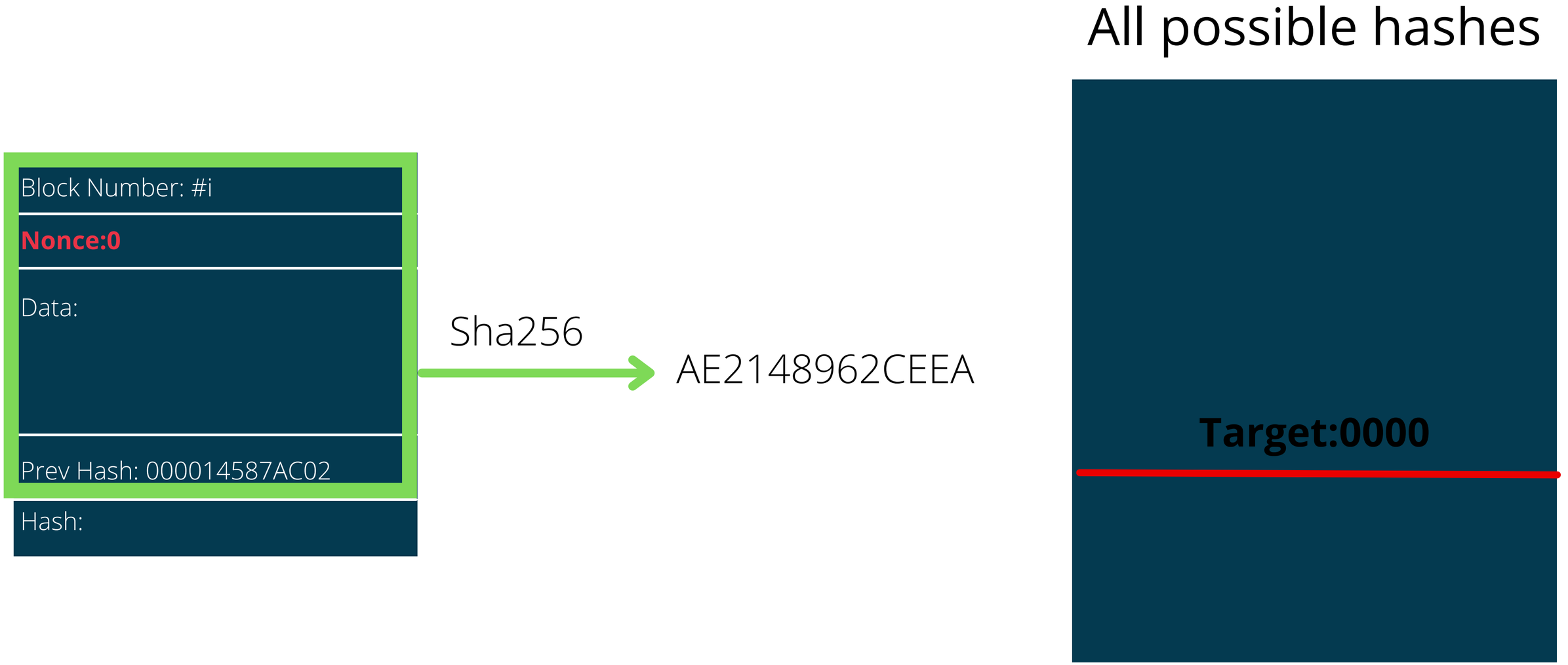
All possible hashes



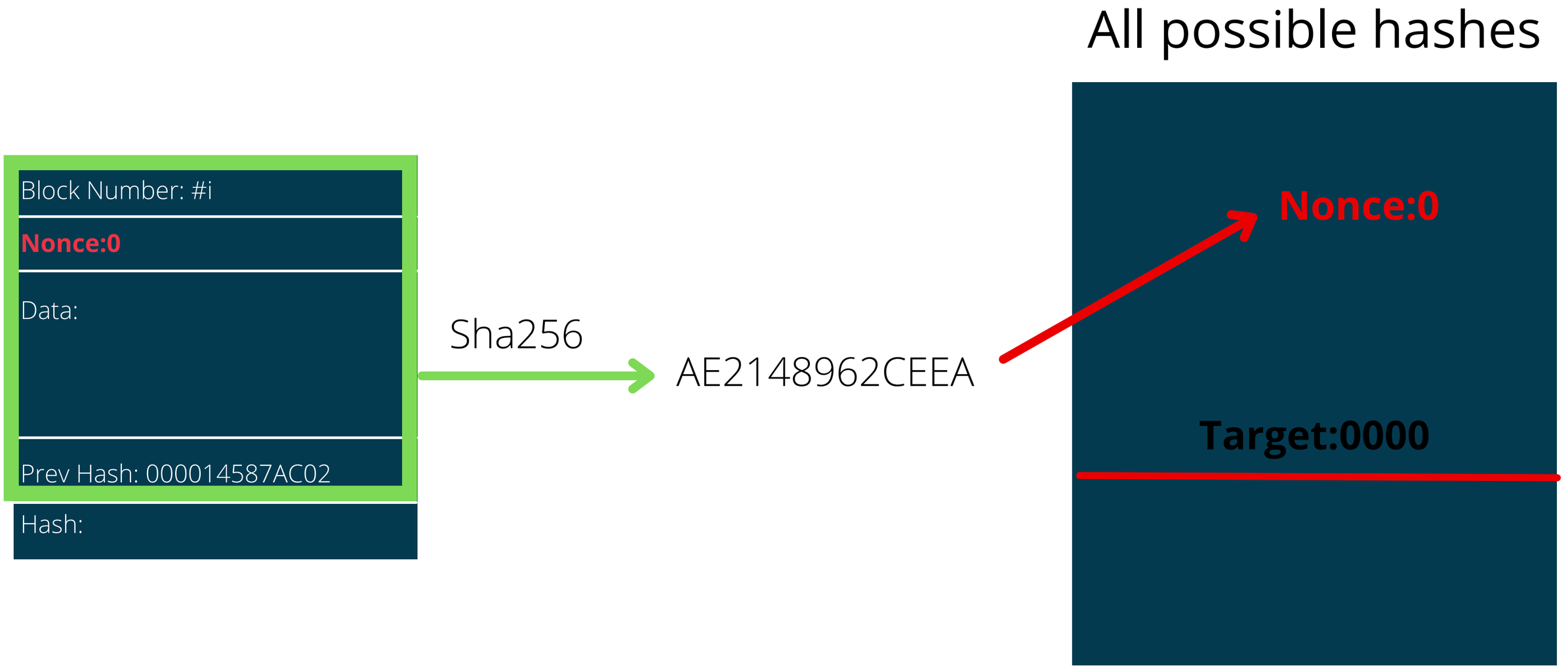
How mining works



How mining works



How mining works



How mining works

How mining works

Block Number: #i

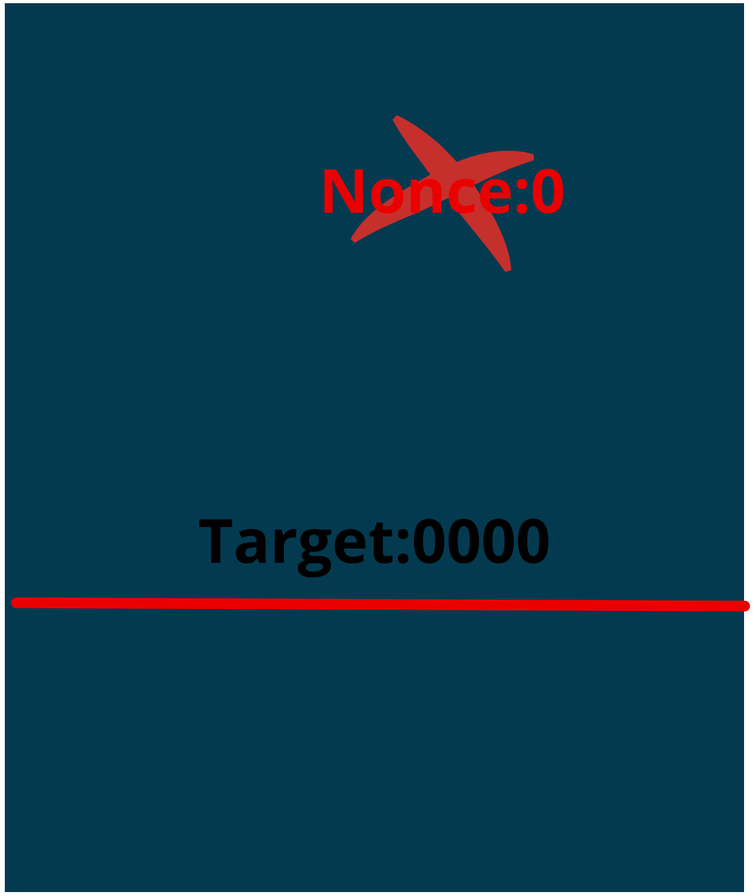
Nonce:7502

Data:

Prev Hash: 000014587AC02

Hash:

All possible hashes



How mining works

Block Number: #i

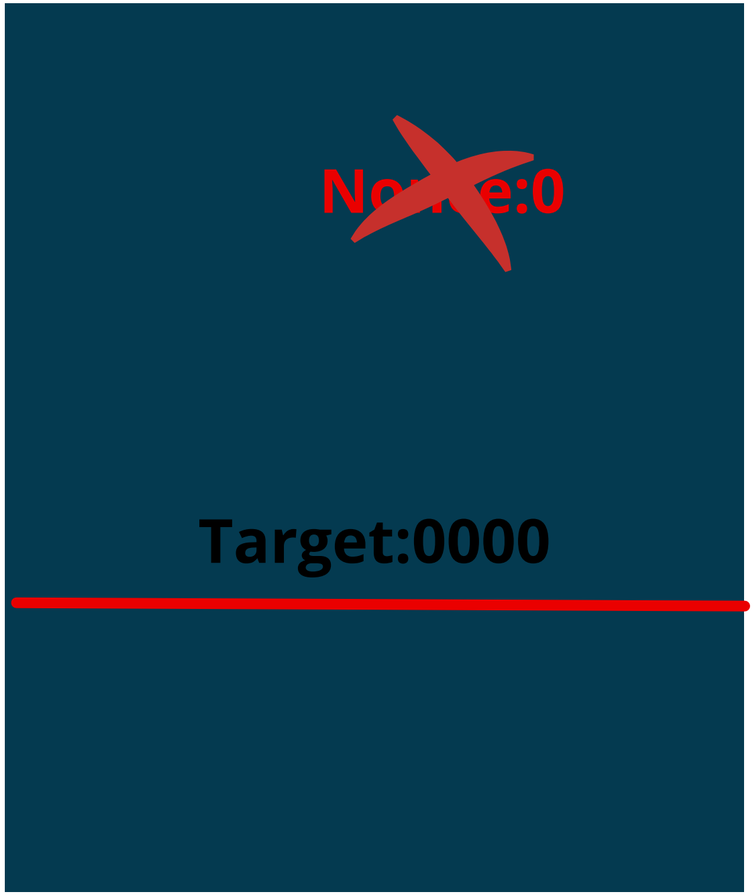
Nonce:7502

Data:

Prev Hash: 000014587AC02

Hash:

All possible hashes



How mining works

Block Number: #i

Nonce:7502

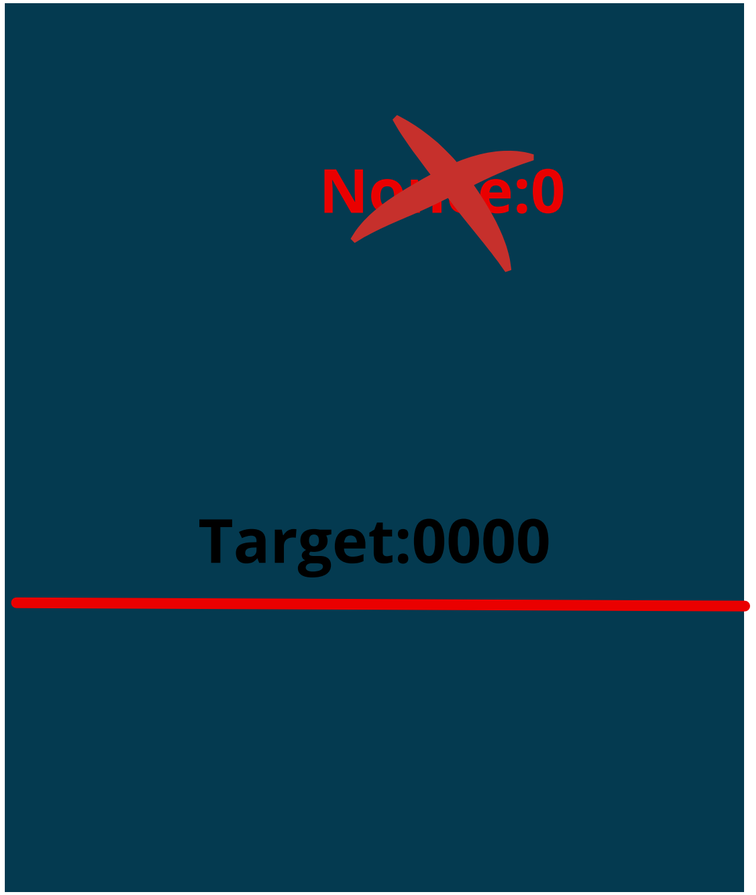
Data:

Prev Hash: 000014587AC02

Hash:

00077854ACD12

All possible hashes



How mining works

Block Number: #i

Nonce:7502

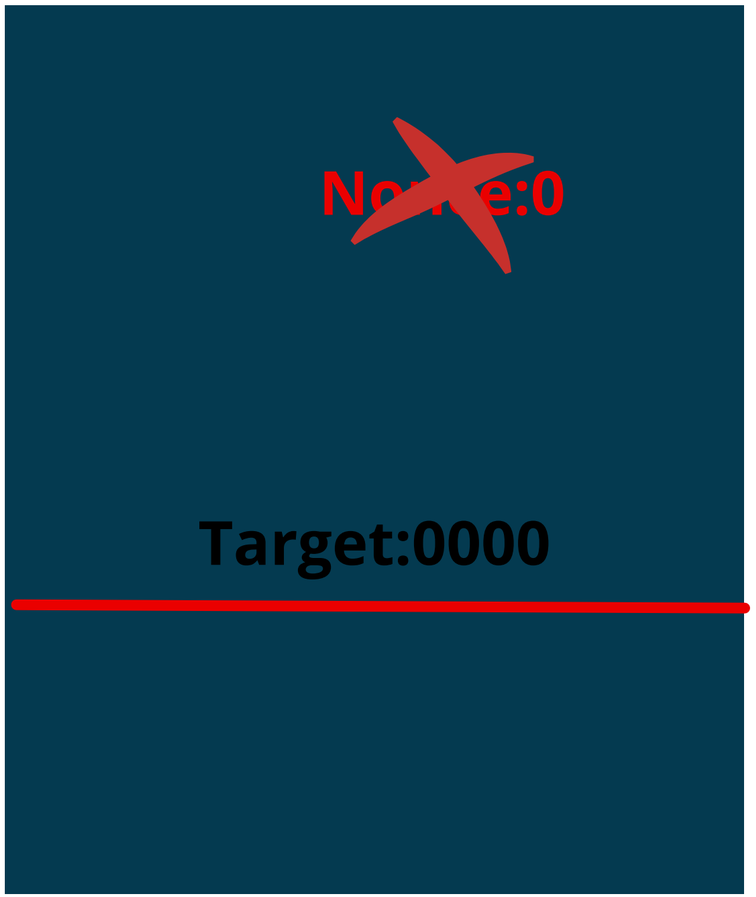
Data:

Prev Hash: 000014587AC02

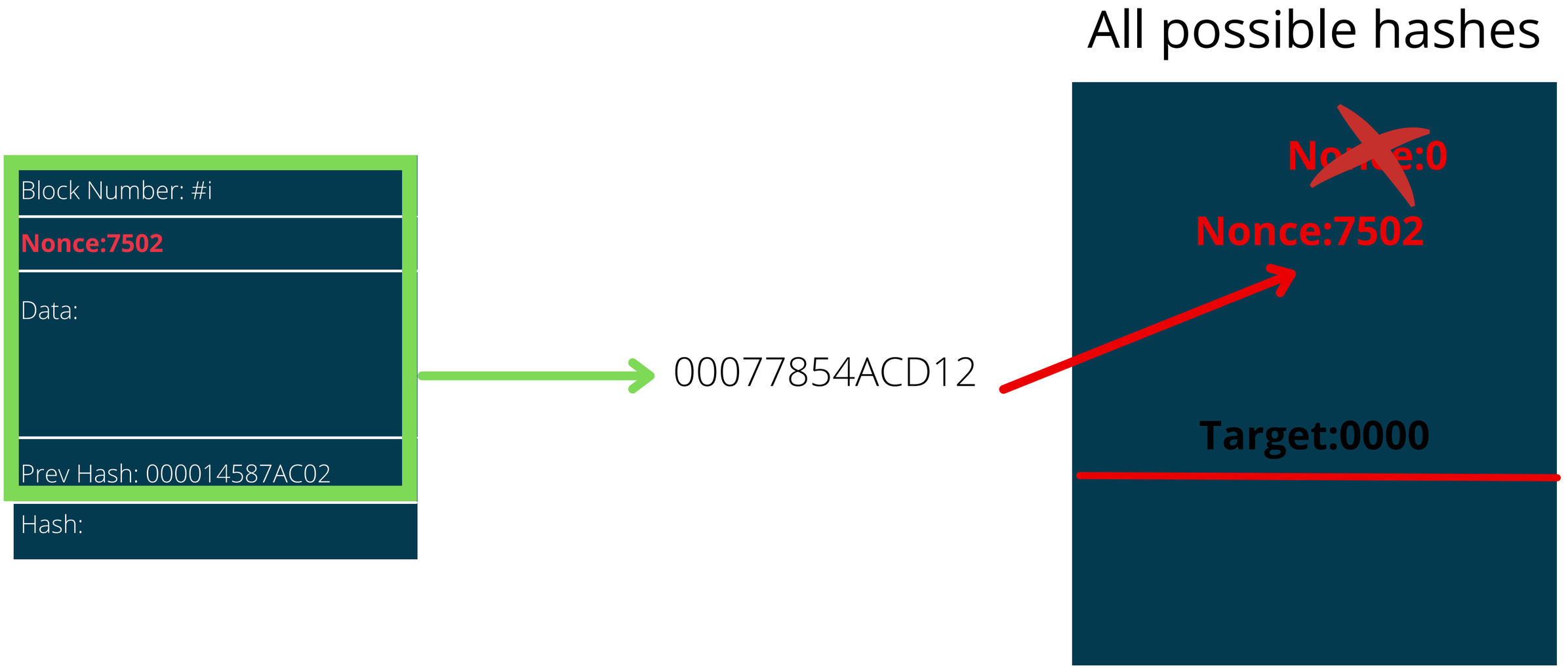
Hash:

00077854ACD12

All possible hashes



How mining works



How mining works

How mining works

Block Number: #i

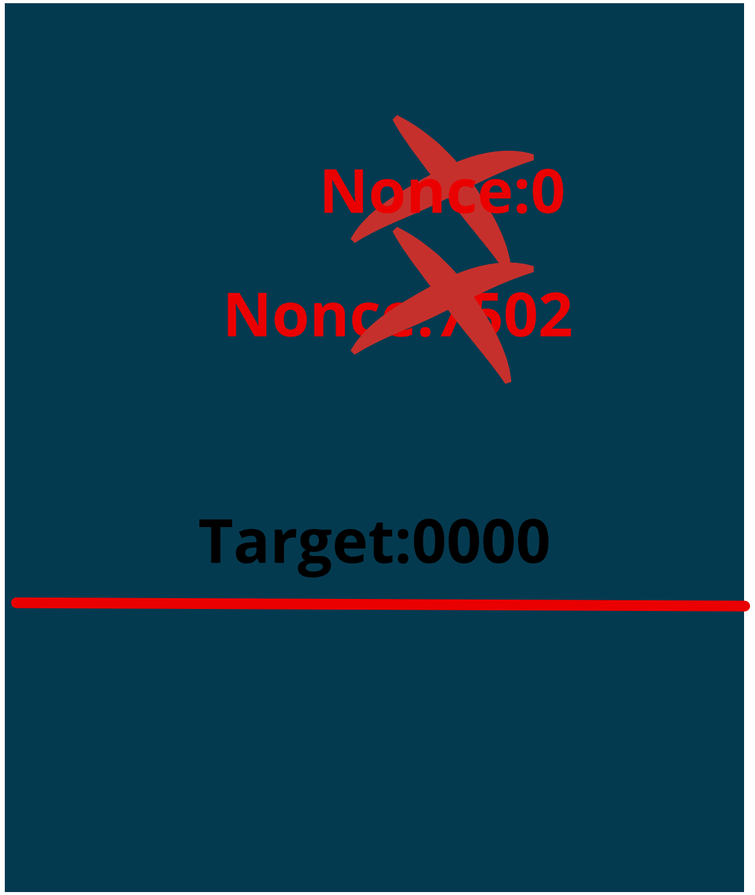
Nonce:7503

Data:

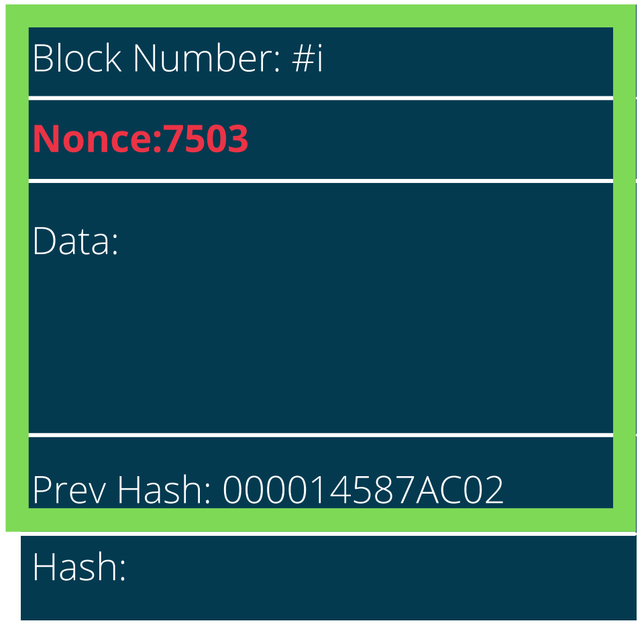
Prev Hash: 000014587AC02

Hash:

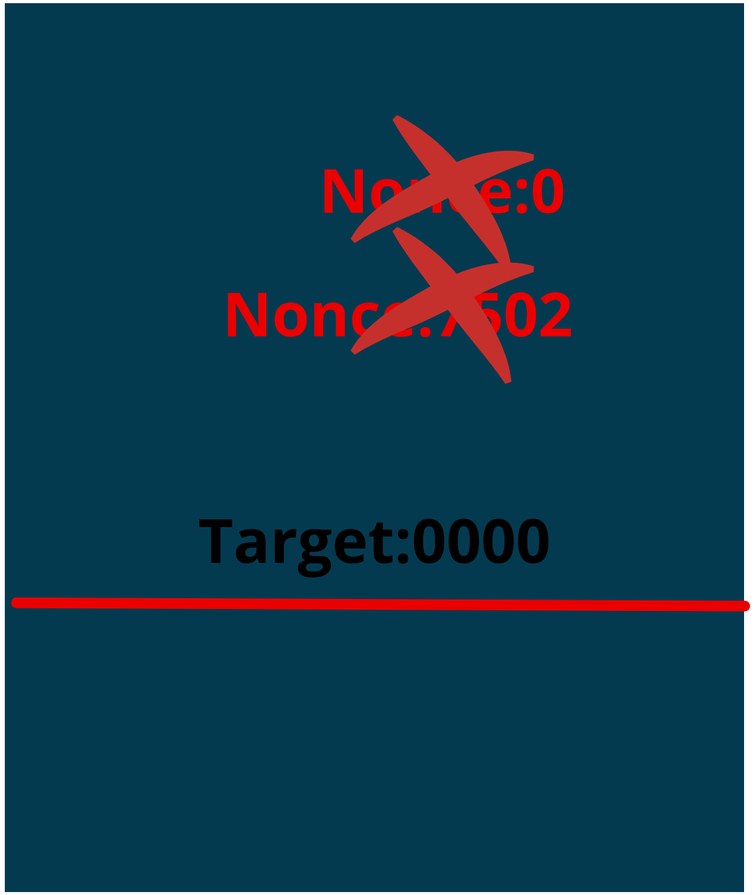
All possible hashes



How mining works



All possible hashes



How mining works

Block Number: #i

Nonce:7503

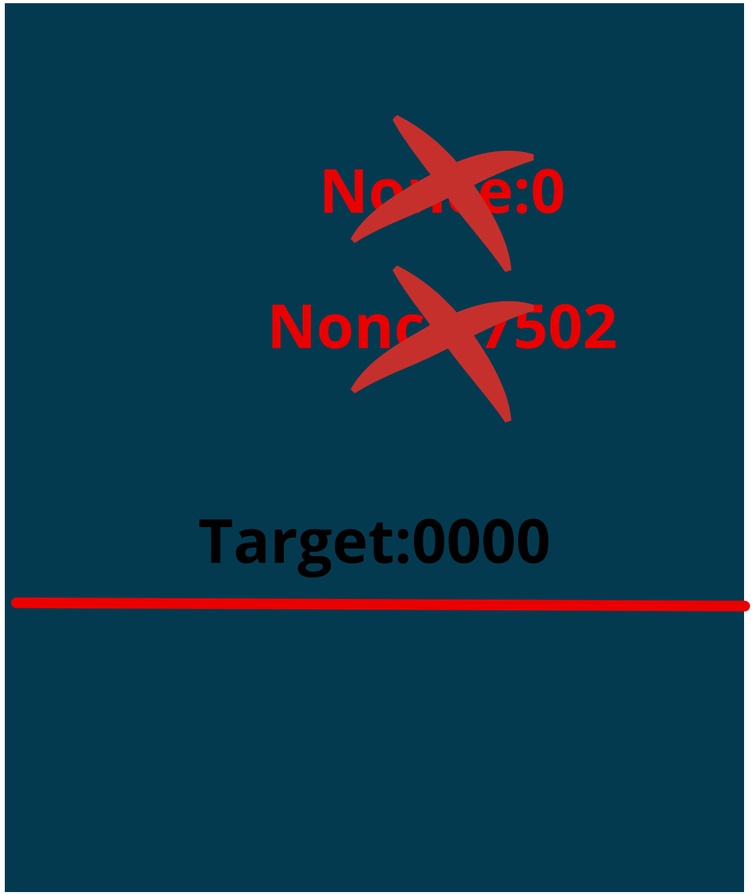
Data:

Prev Hash: 000014587AC02

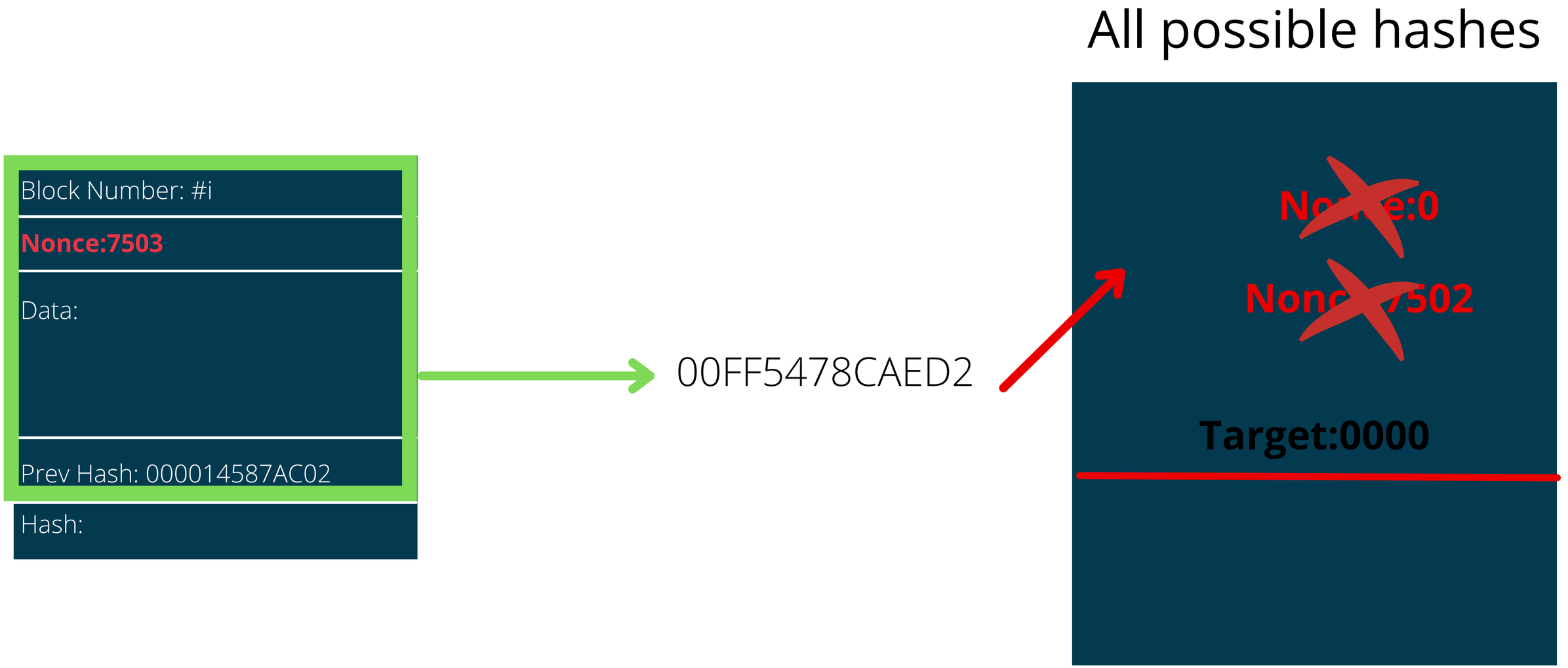
Hash:

00FF5478CAED2

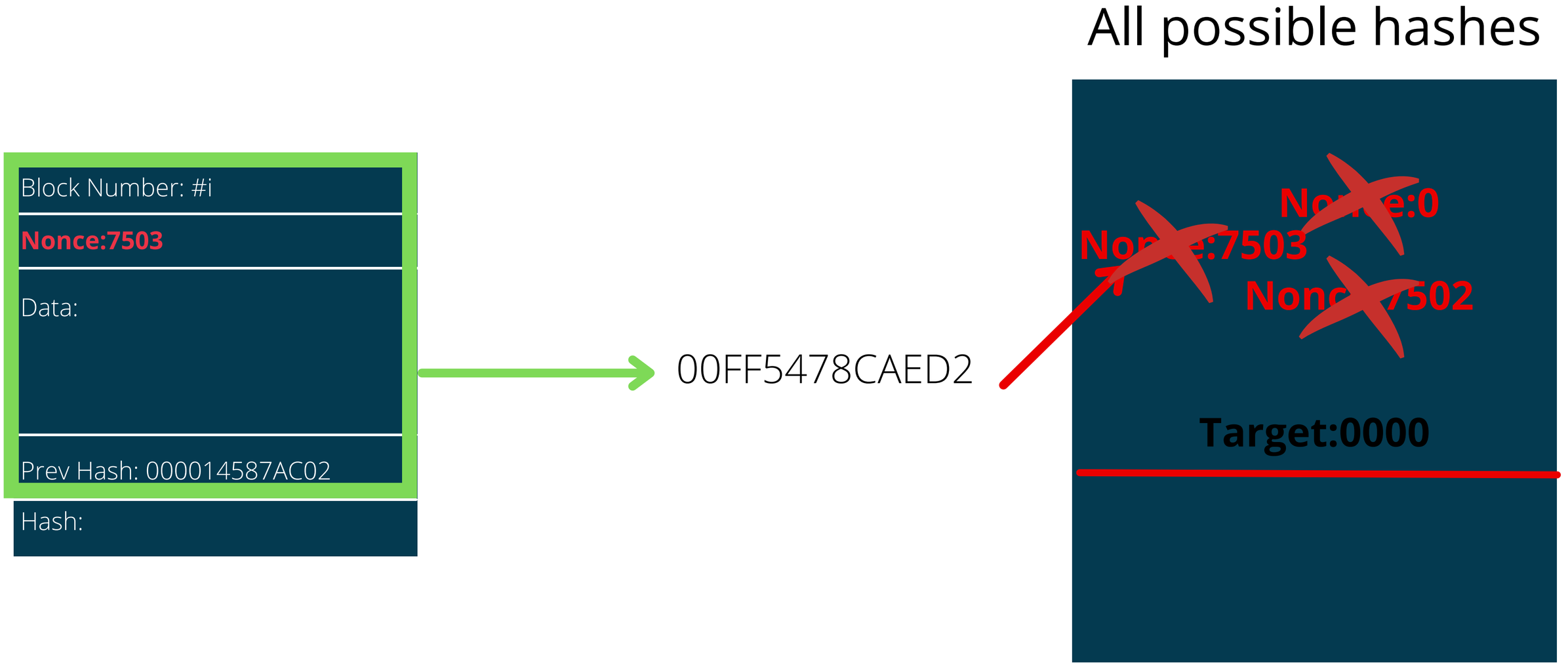
All possible hashes



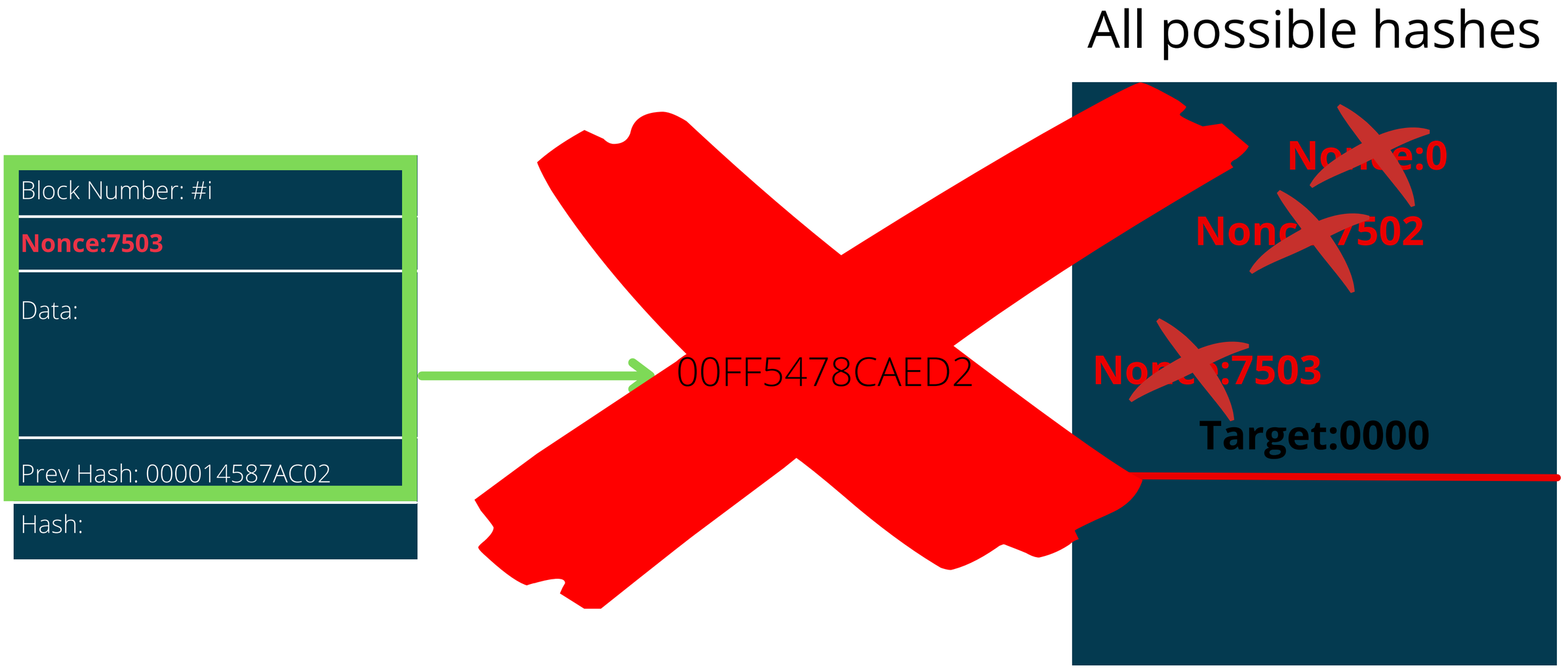
How mining works



How mining works



How mining works



How mining works

Block Number: #i

Nonce:79

Data:

Prev Hash: 000014587AC02

Hash:

All possible hashes

How mining works

Block Number: #i

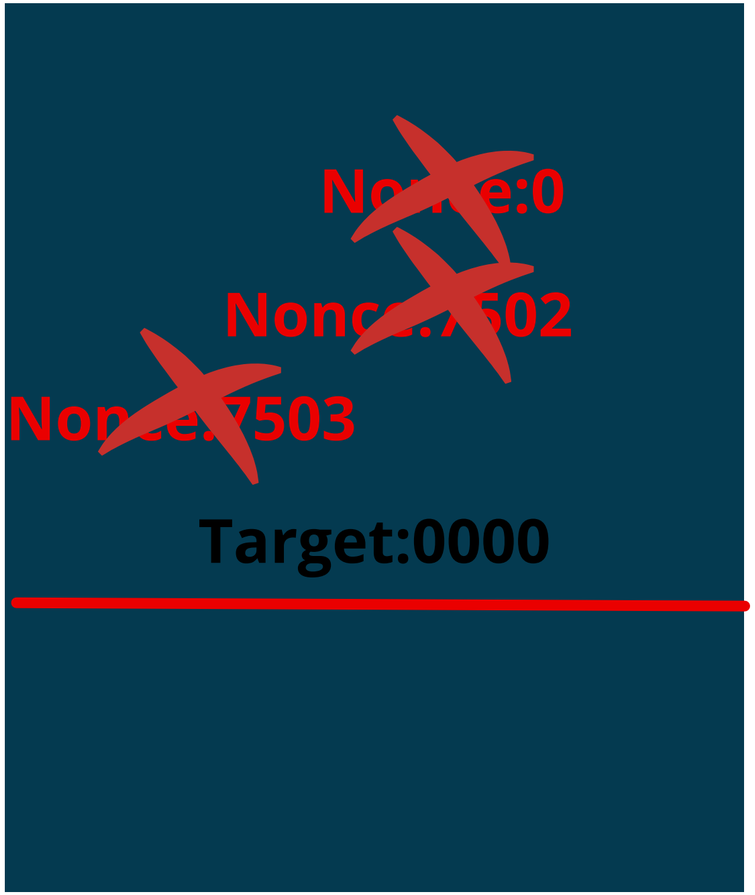
Nonce:79

Data:

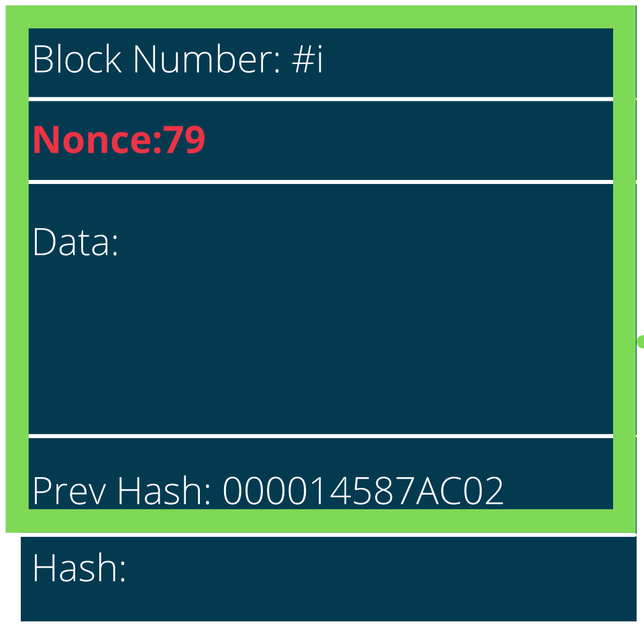
Prev Hash: 000014587AC02

Hash:

All possible hashes

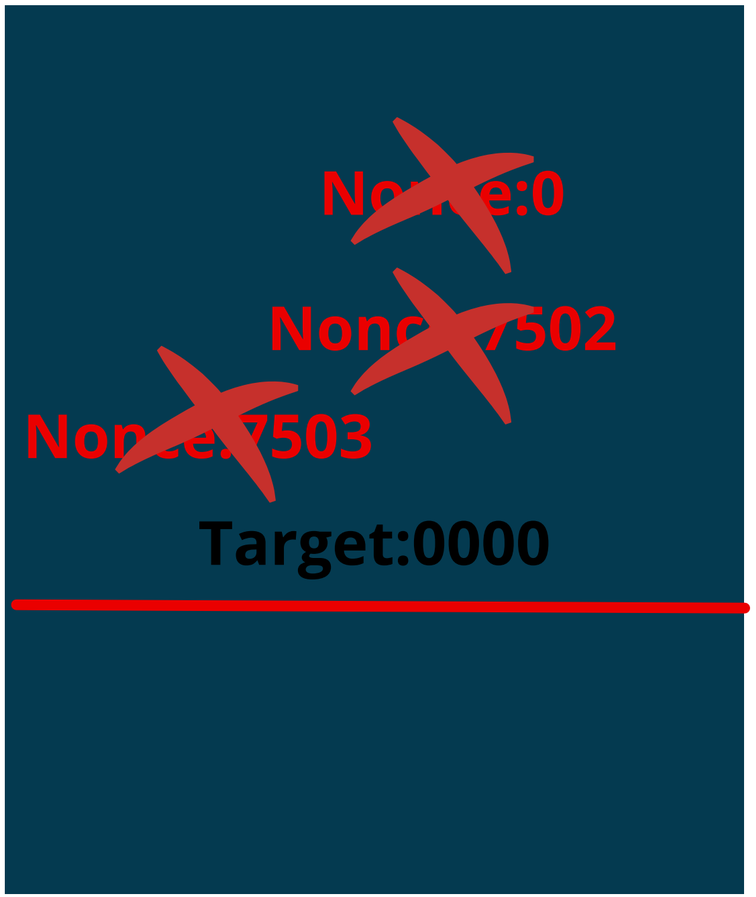


How mining works

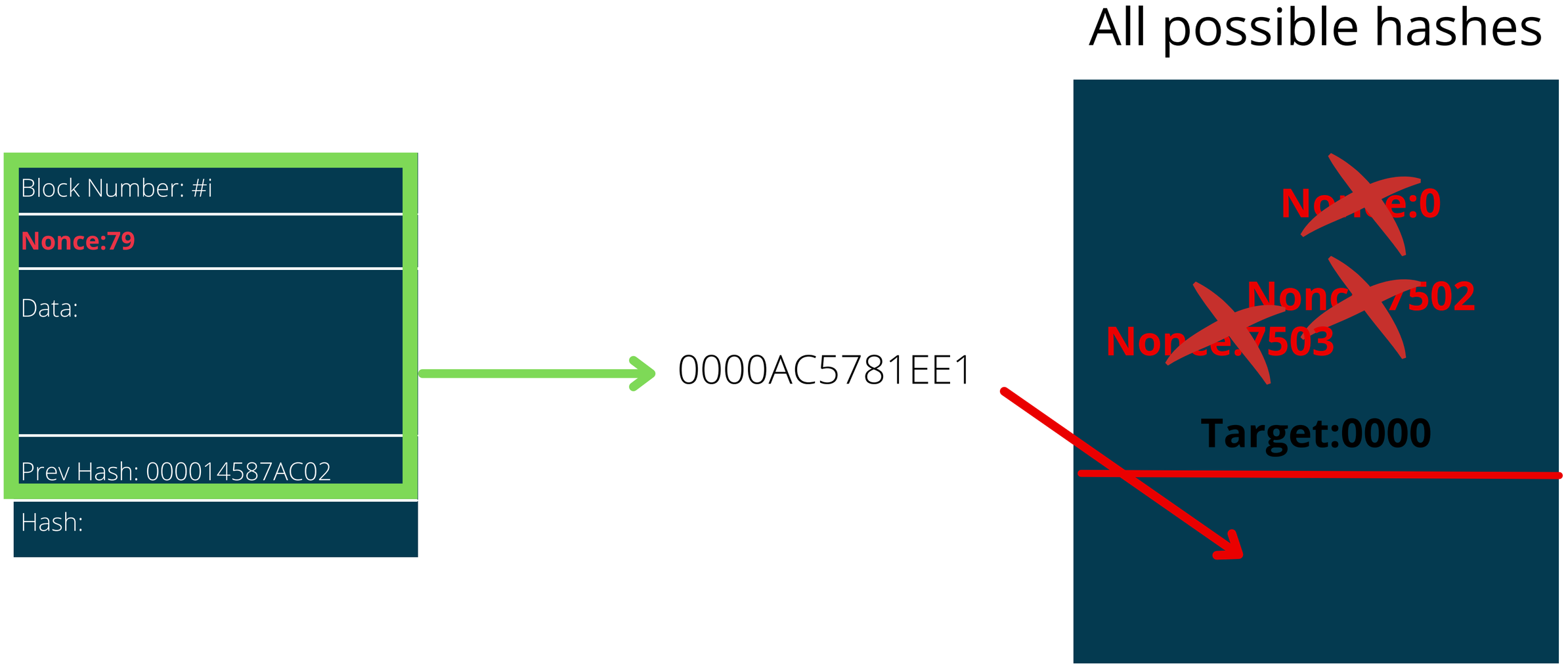


0000AC5781EE1

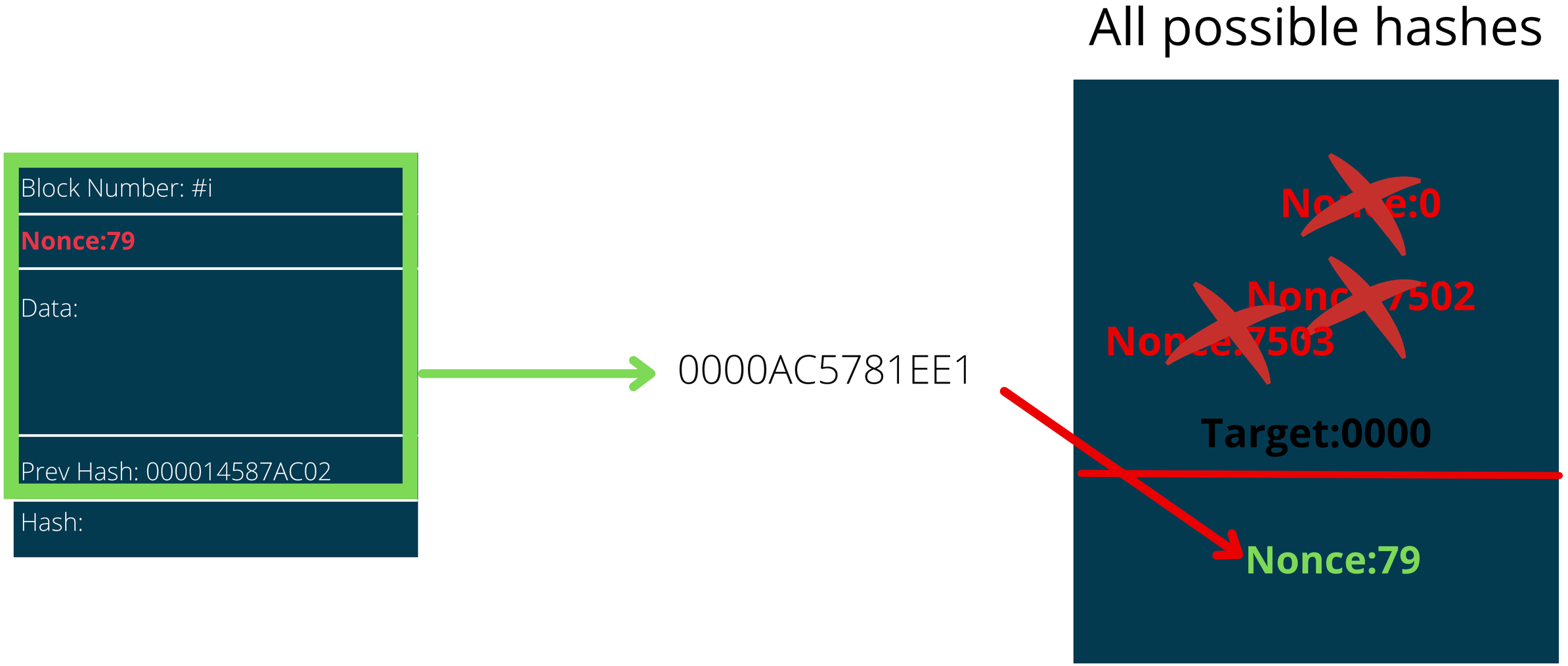
All possible hashes



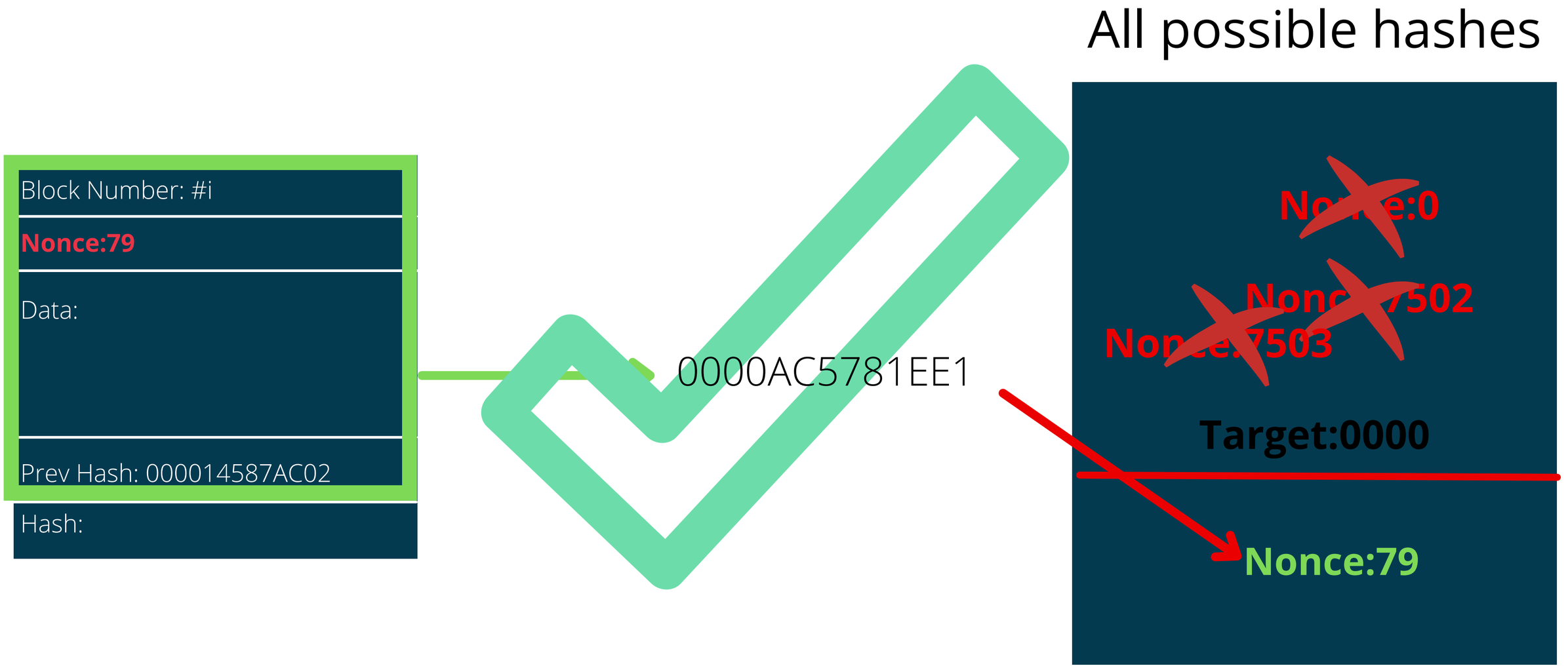
How mining works



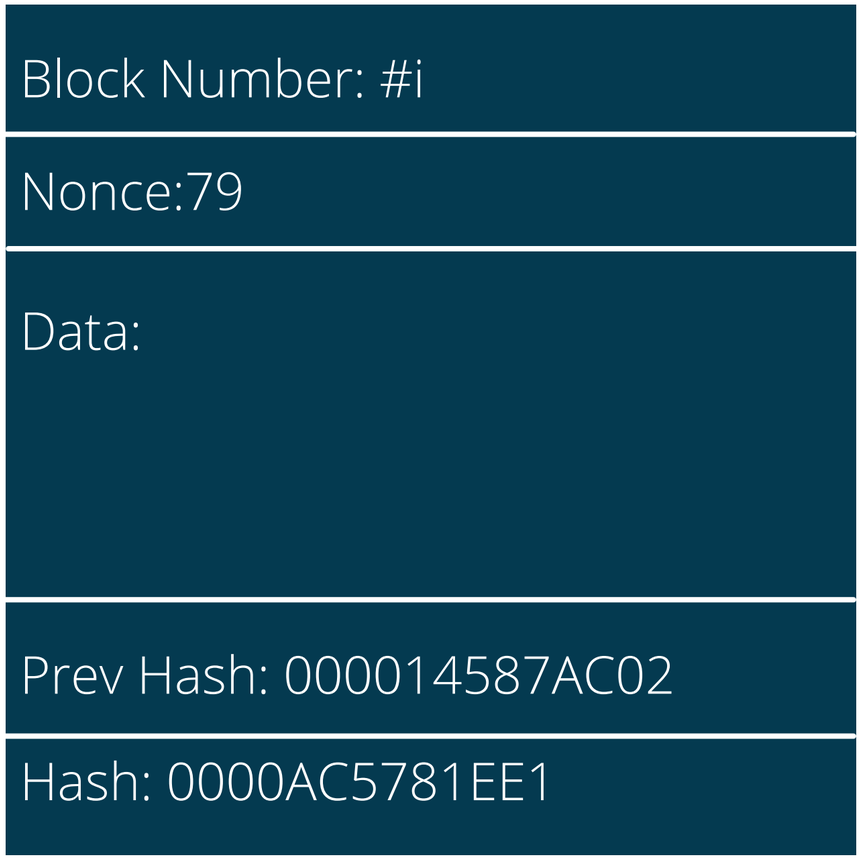
How mining works



How mining works



How mining works



How mining works -Understanding mining difficulty

Calcul probability of getting valid Hash:

How mining works -Understanding mining difficulty

Calcul probability of getting valid Hash:

Current Target: 0000000000000000000FFF.....FFF

22 leading Zeros

How mining works -Understanding mining difficulty

Calcul probability of getting valid Hash:

Current Target: 0000000000000000FFF.....FFF

22 leading Zeros

All possible hashes: FFF.....FFF

How mining works -Understanding mining difficulty

Calcul probability of getting valid Hash:

Current Target: 0000000000000000FFF.....FFF

22 leading Zeros

All possible hashes: FFF.....FFF

Total possible 64 digit hexa numbers: 16^64 = 10^77

How mining works -Understanding mining difficulty

Calcul probability of getting valid Hash:

Current Target: 0000000000000000FFF.....FFF

22 leading Zeros

All possible hashes: FFF.....FFF

Total possible 64 digit hexa numbers: 16^64 = 10^77

Total possible valid hashes: 16^(64-22) = 2*10^51

How mining works -Understanding mining difficulty

Calcul probability of getting valid Hash:

Current Target: 0000000000000000FFF.....FFF

22 leading Zeros

All possible hashes: FFF.....FFF

Total possible 64 digit hexa numbers: 16^64 = 10^77

Total possible valid hashes: 16^(64-22) = 2*10^51

Probability that randomly picked hash is valid: (2*10^51)/(10^77) =

How mining works -Understanding mining difficulty

Calcul probability of getting valid Hash:

Current Target: 0000000000000000FFF.....FFF

22 leading Zeros

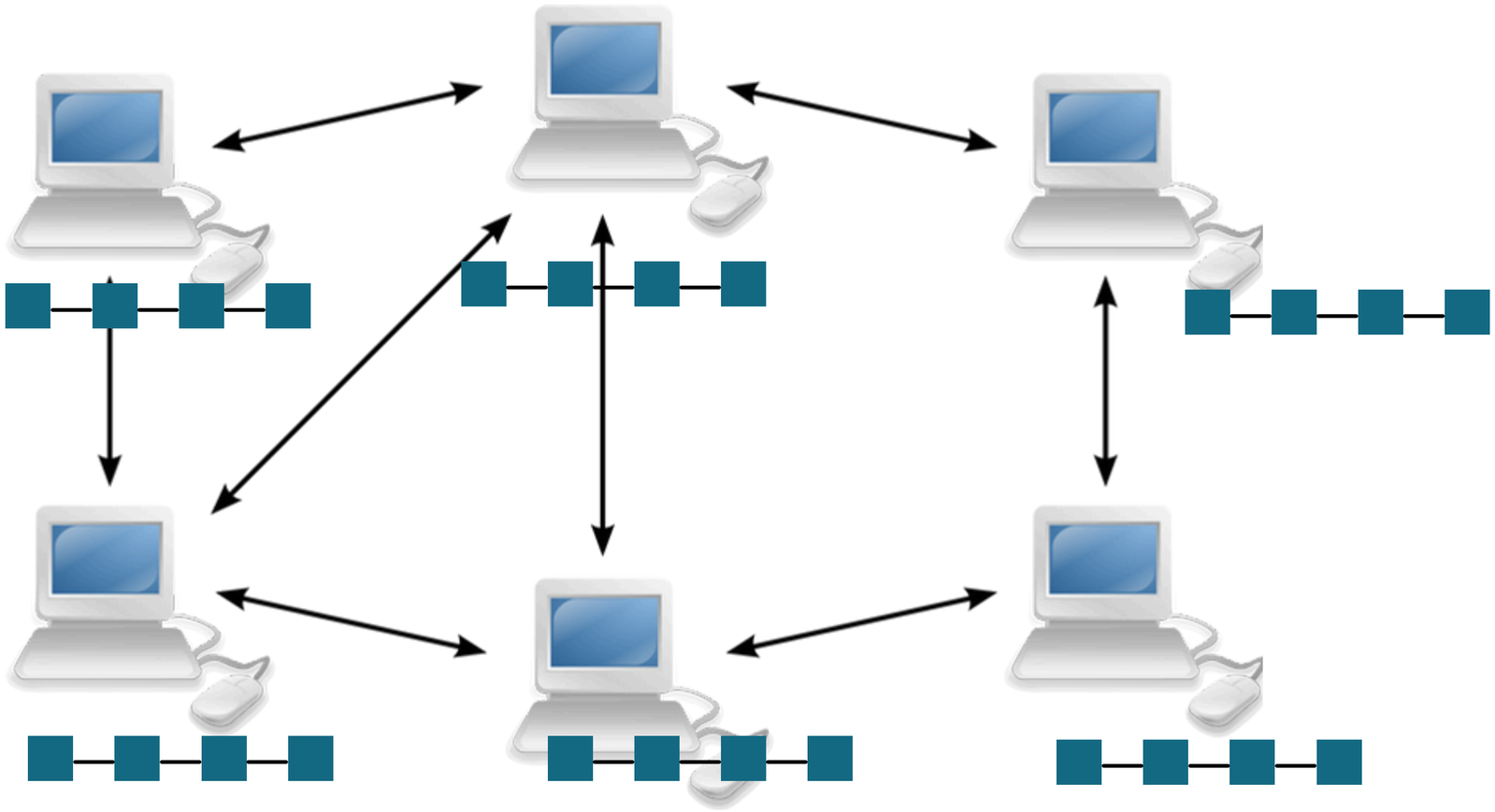
All possible hashes: FFF.....FFF

Total possible 64 digit hexa numbers: 16^64 = 10^77

Total possible valid hashes: 16^(64-22) = 2*10^55

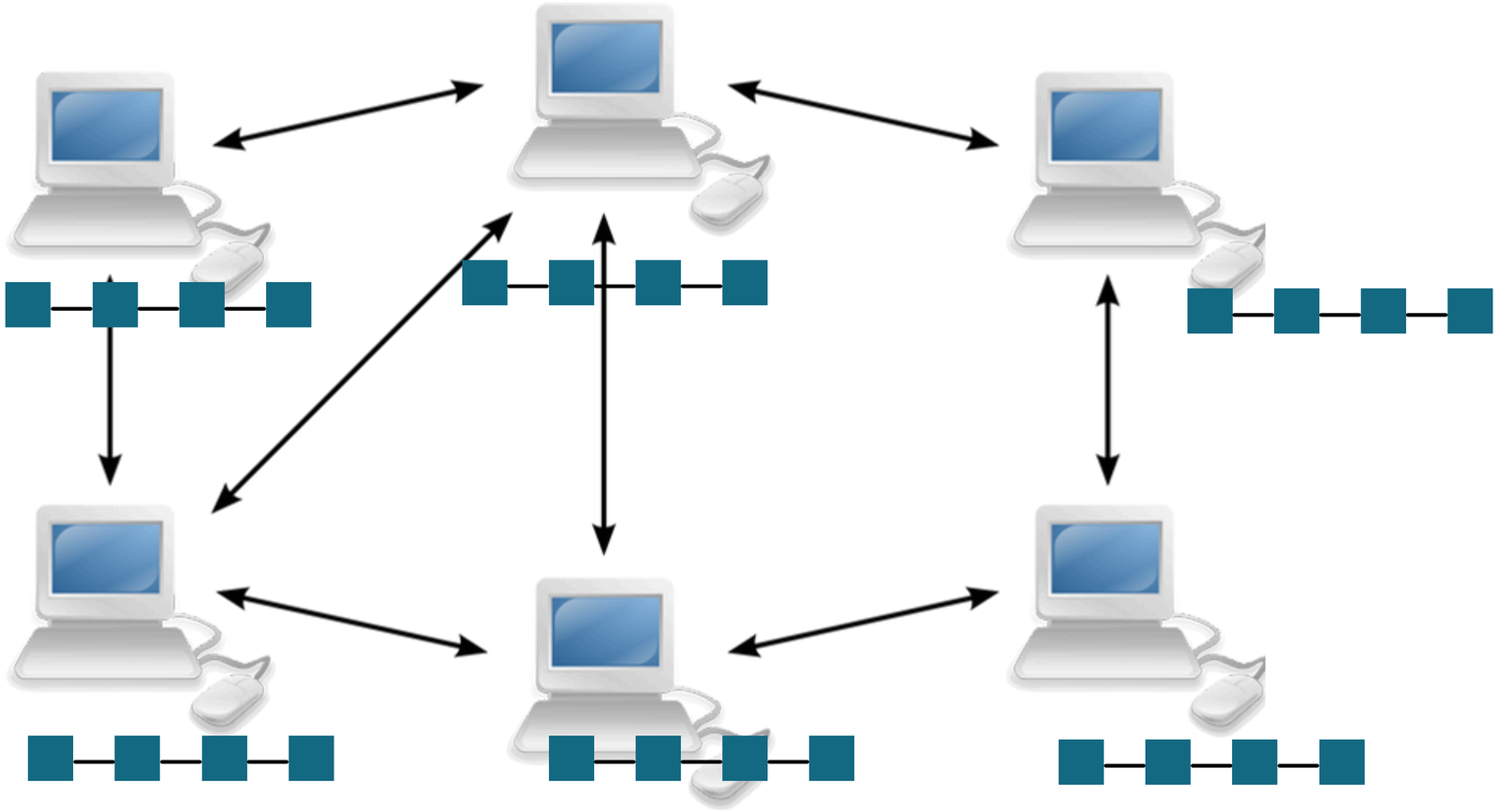
Probability that randomly picked hash is valid: (2*10^51)/(10^77) = **2 * 10^(-22)**

Consensus Protocol



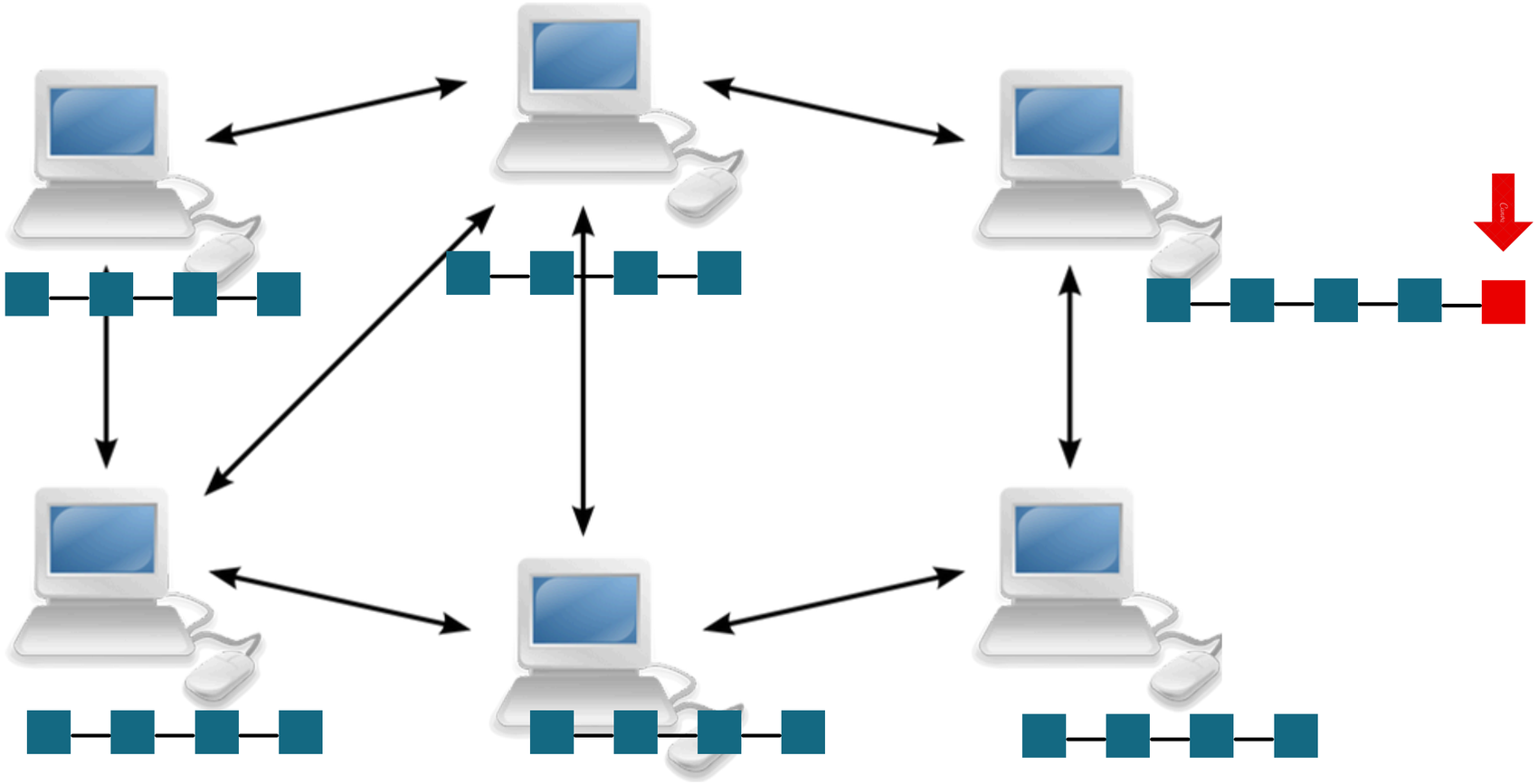
Consensus Protocol

Problem 1: Attack



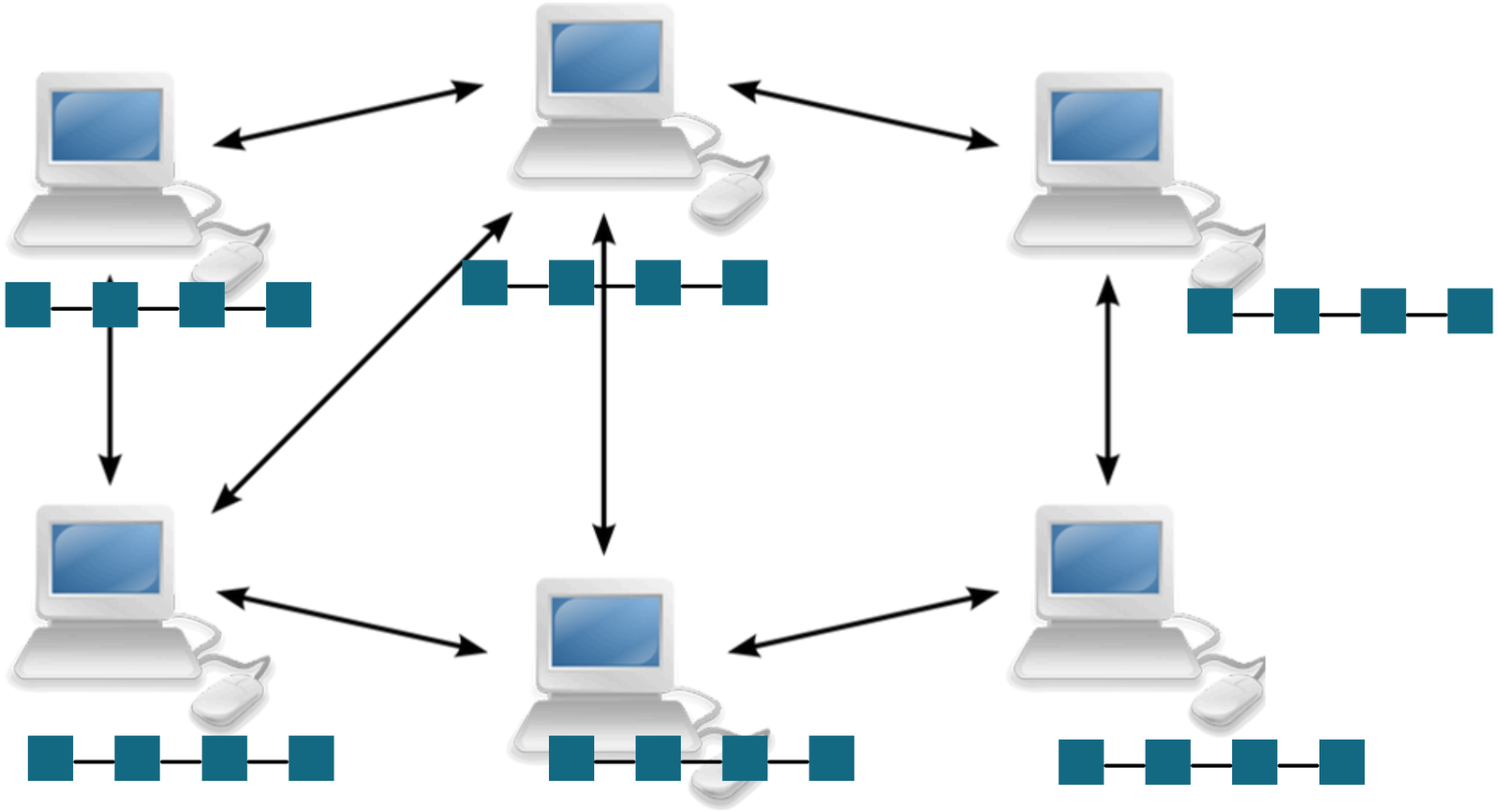
Consensus Protocol

Problem 1: Attack



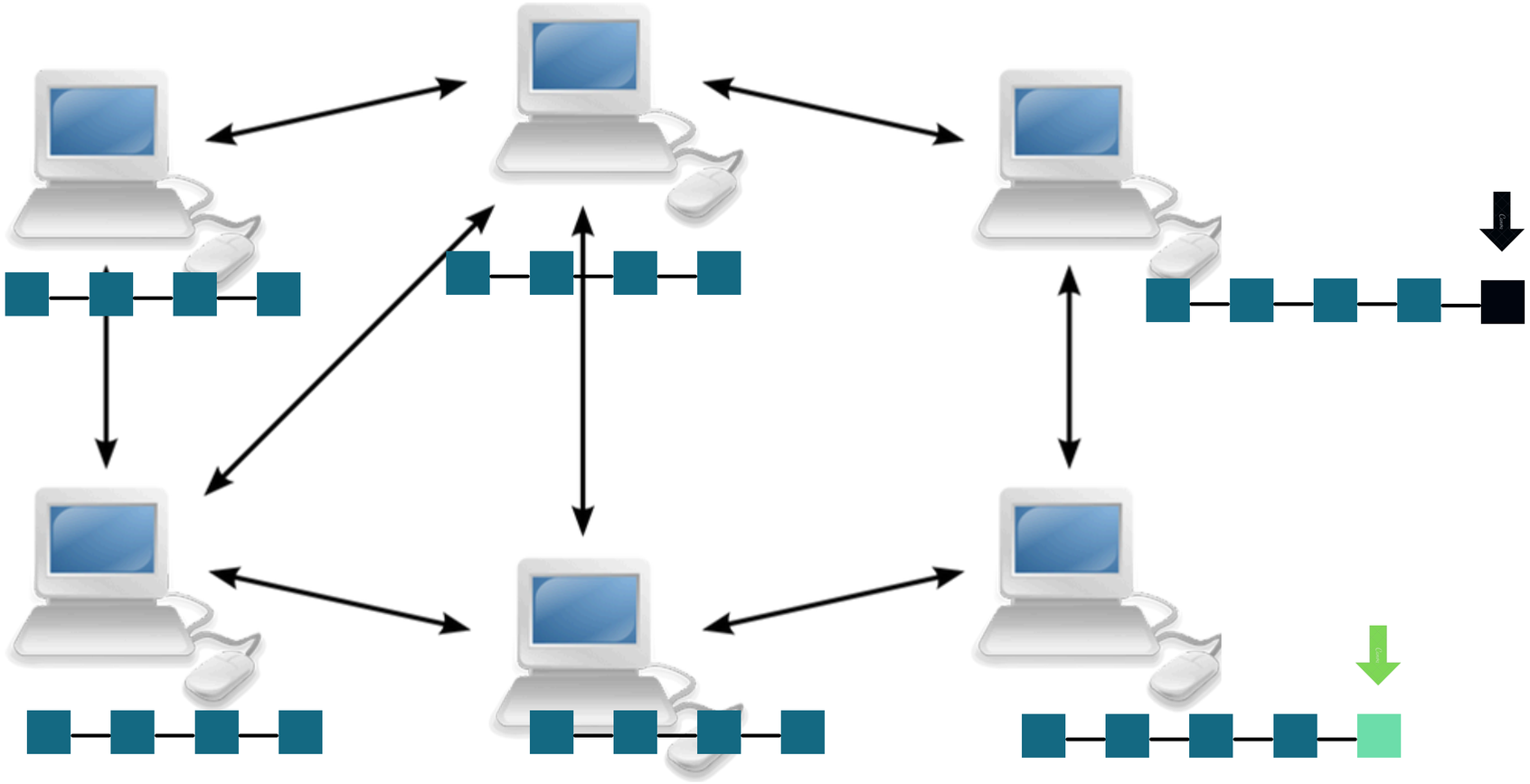
Consensus Protocol

Problem2: Competing chains



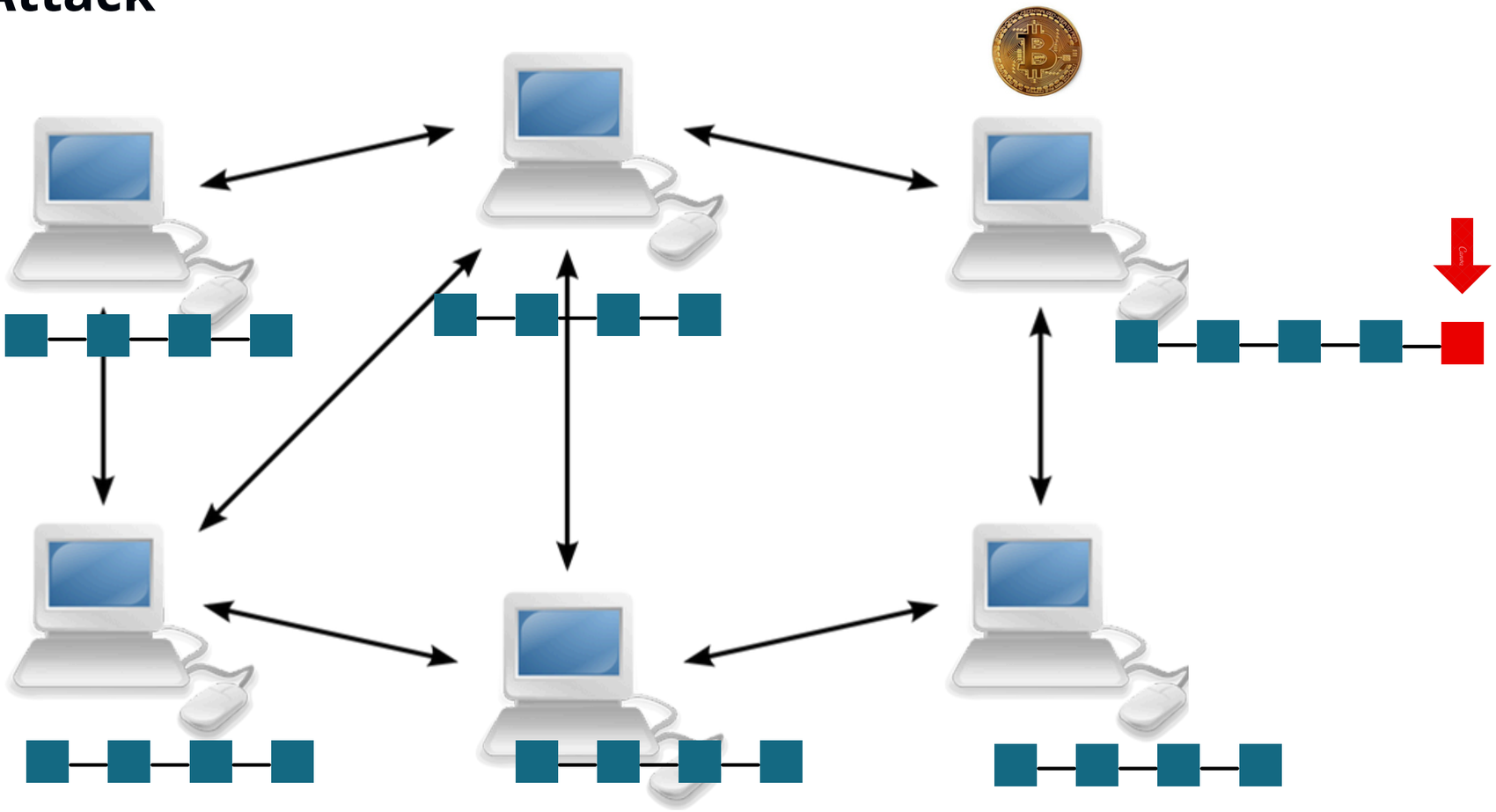
Consensus Protocol

Problem2: Competing chains



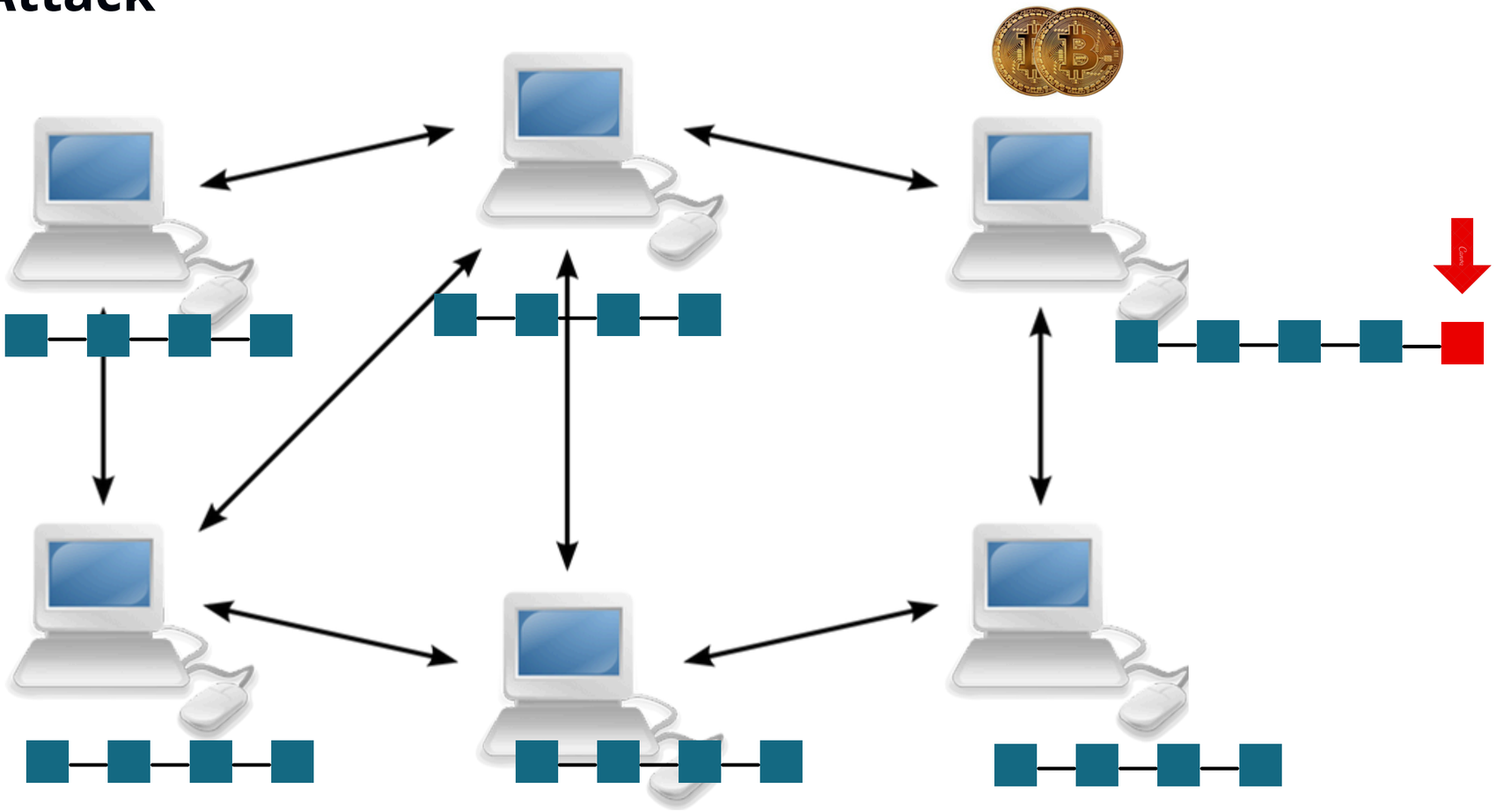
Consensus Protocol

Problem 1: Attack



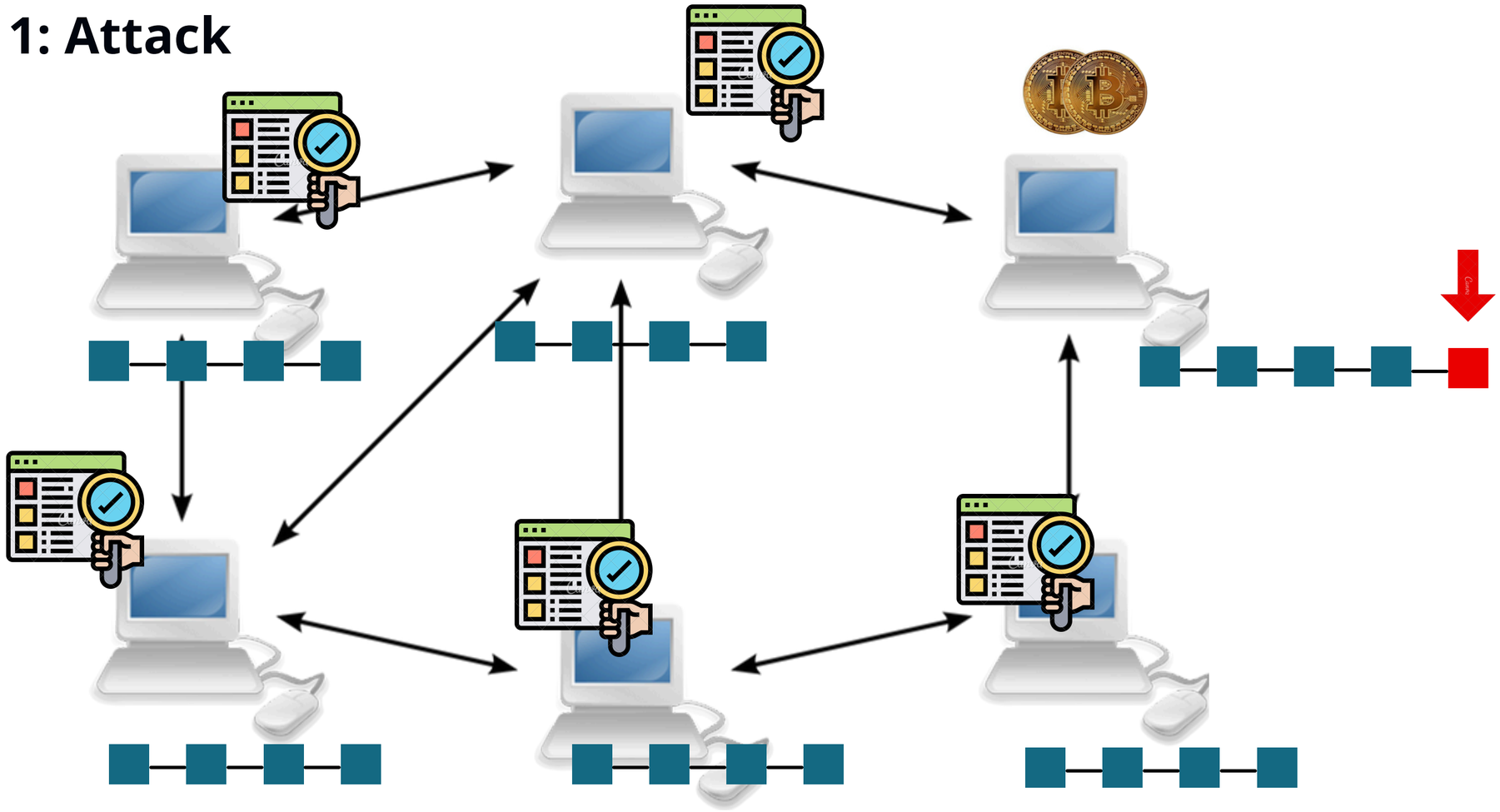
Consensus Protocol

Problem 1: Attack



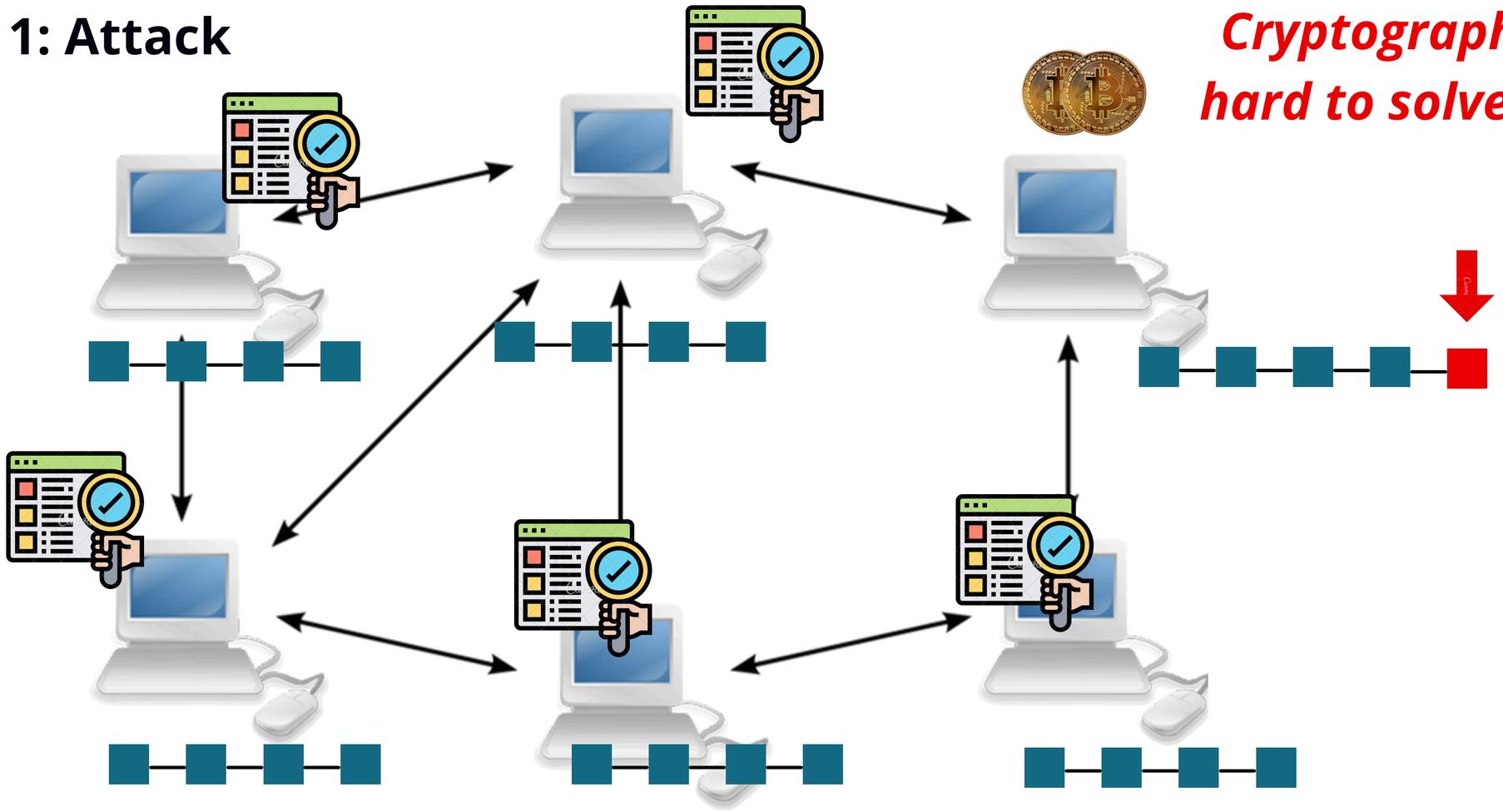
Consensus Protocol

Problem 1: Attack



Consensus Protocol

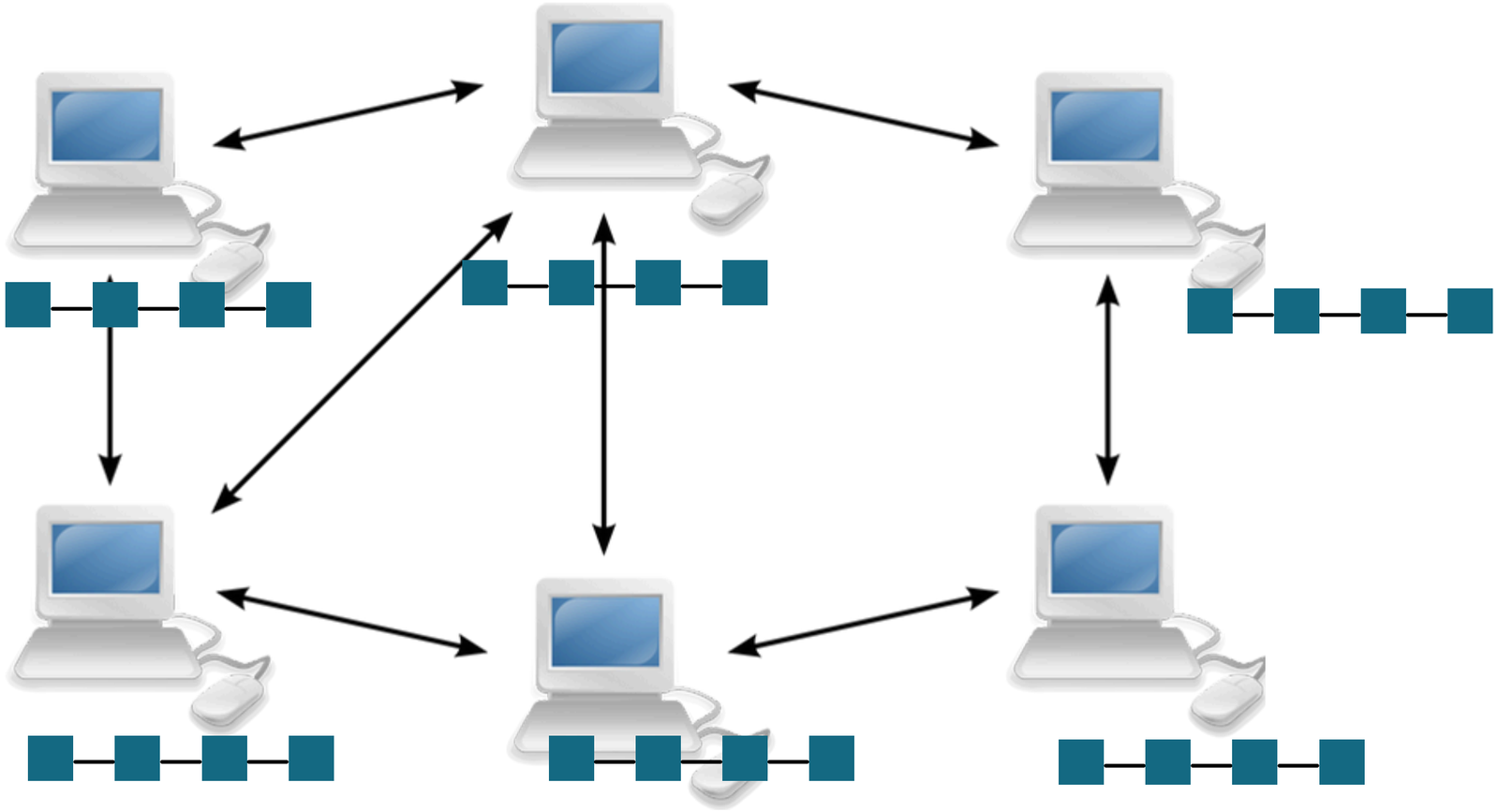
Problem 1: Attack



Cryptographic puzzles are hard to solve, easy to verify

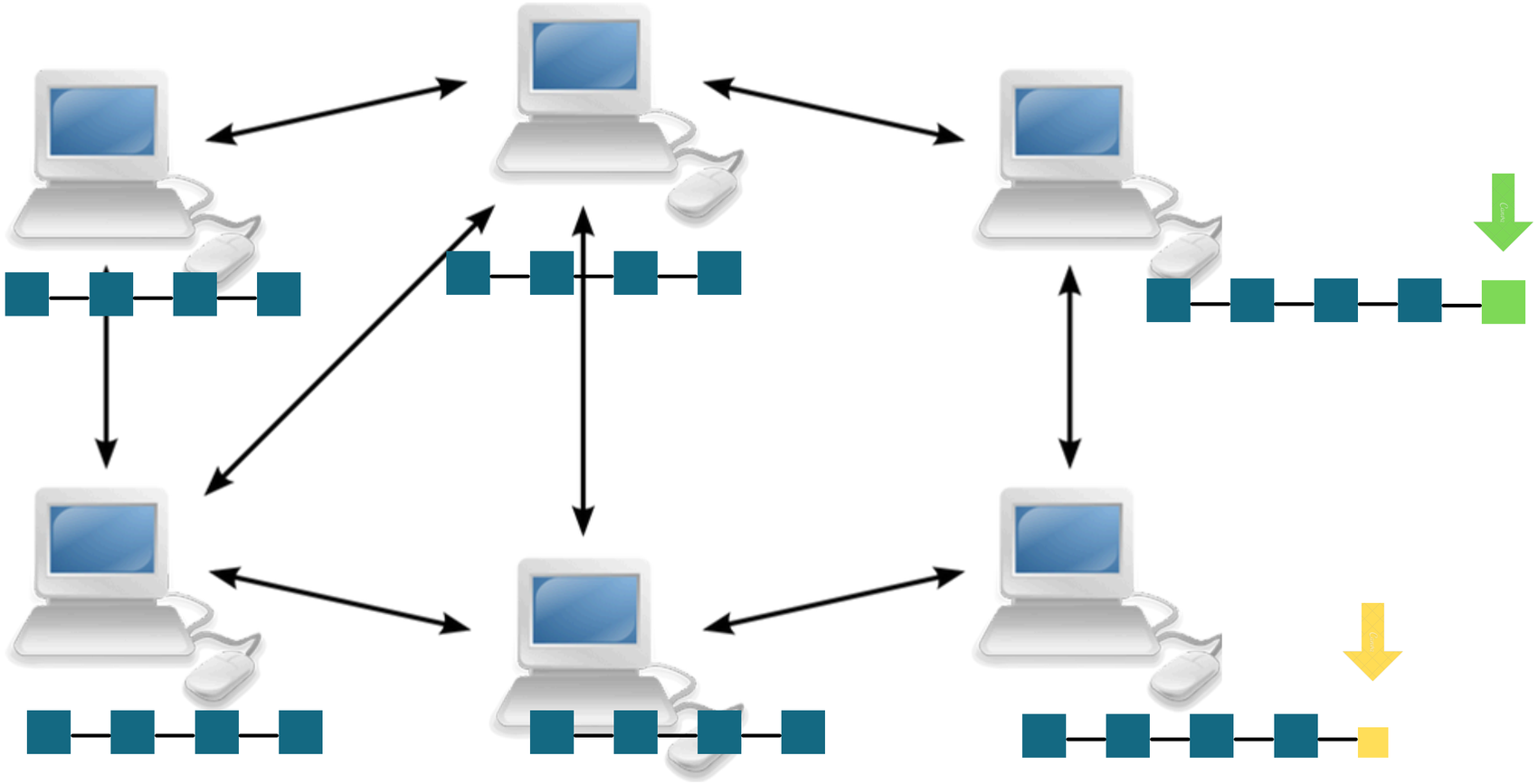
Consensus Protocol

Problem 2: Chain competing



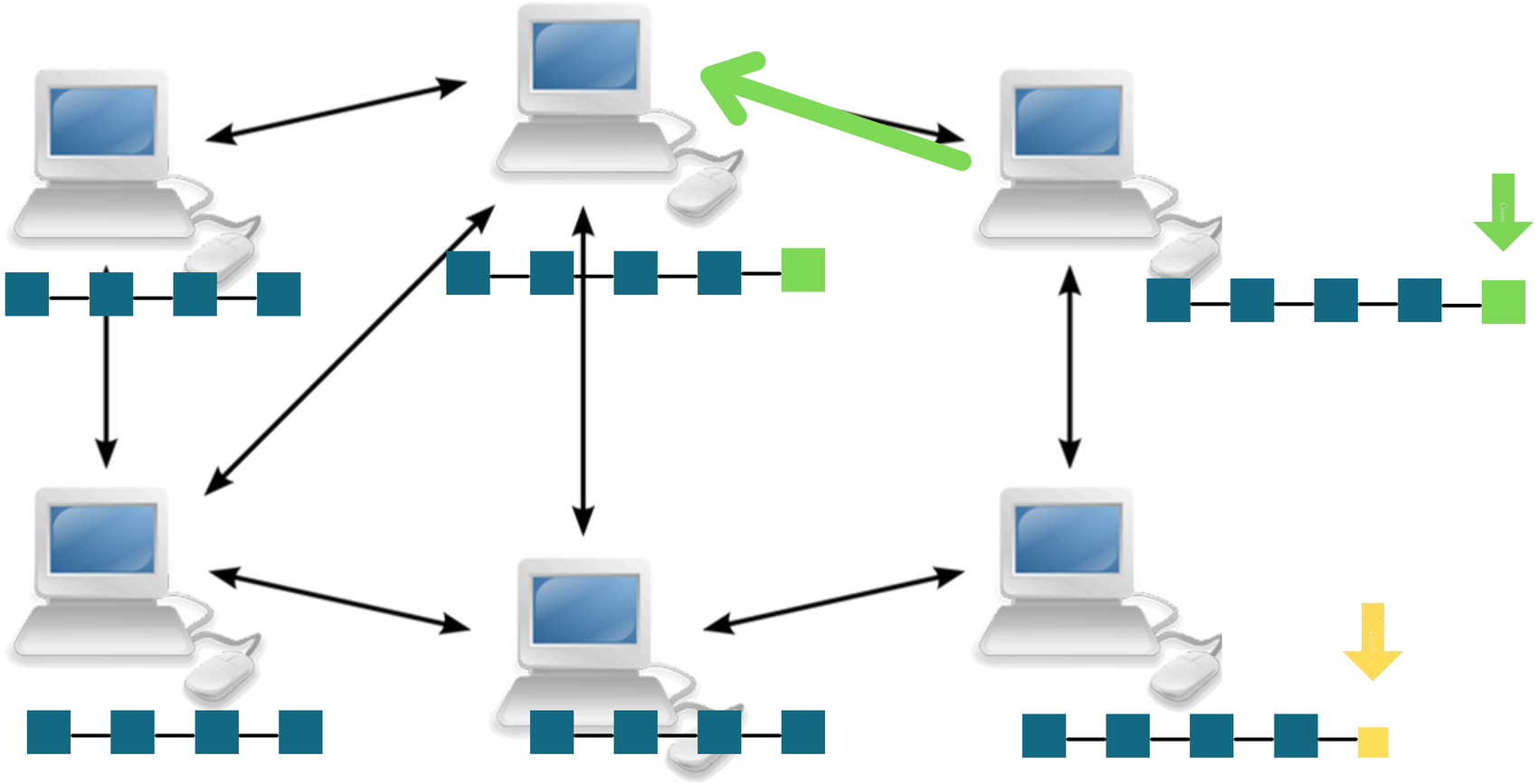
Consensus Protocol

Problem 2: Chain competing



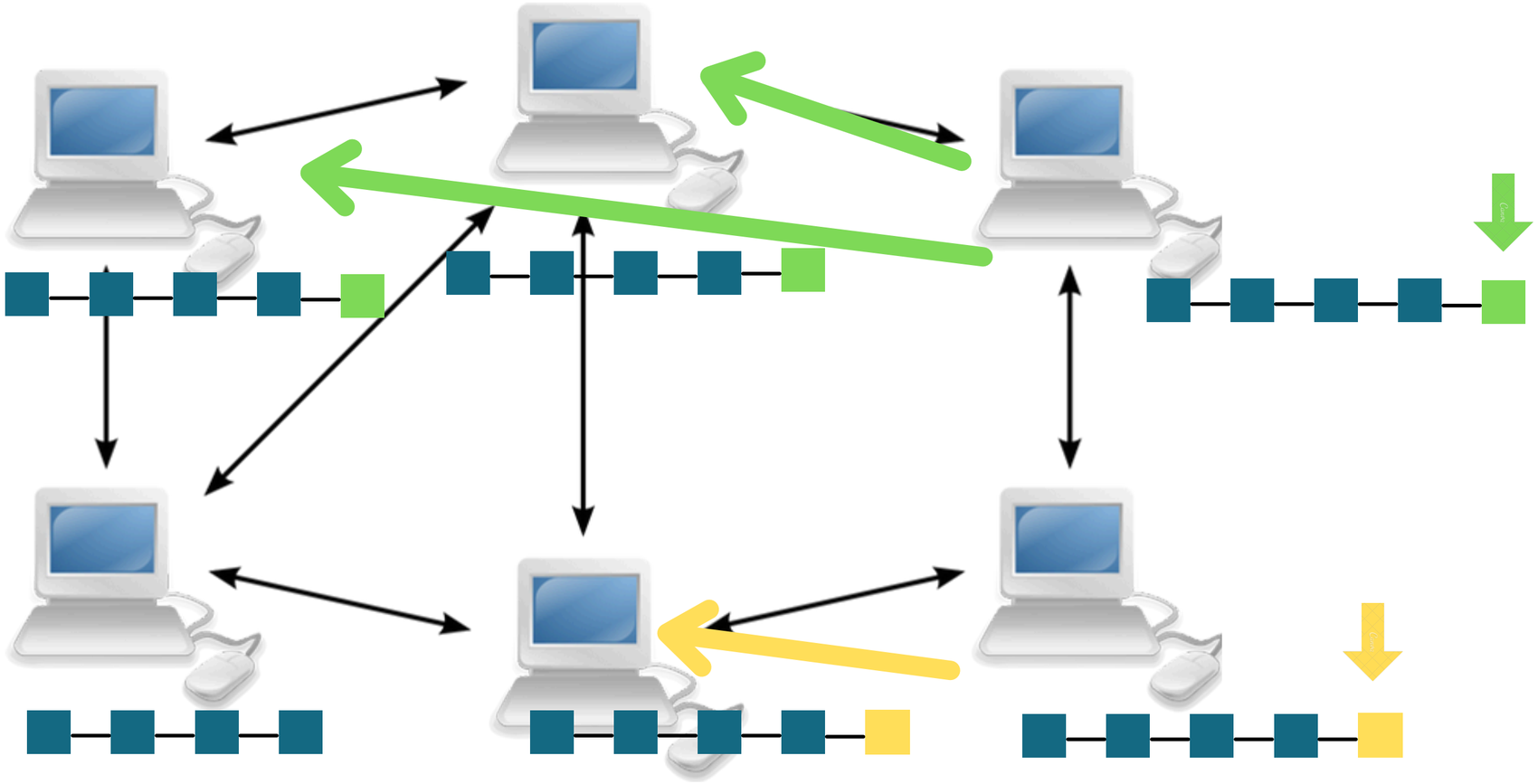
Consensus Protocol

Problem 2: Chain competing



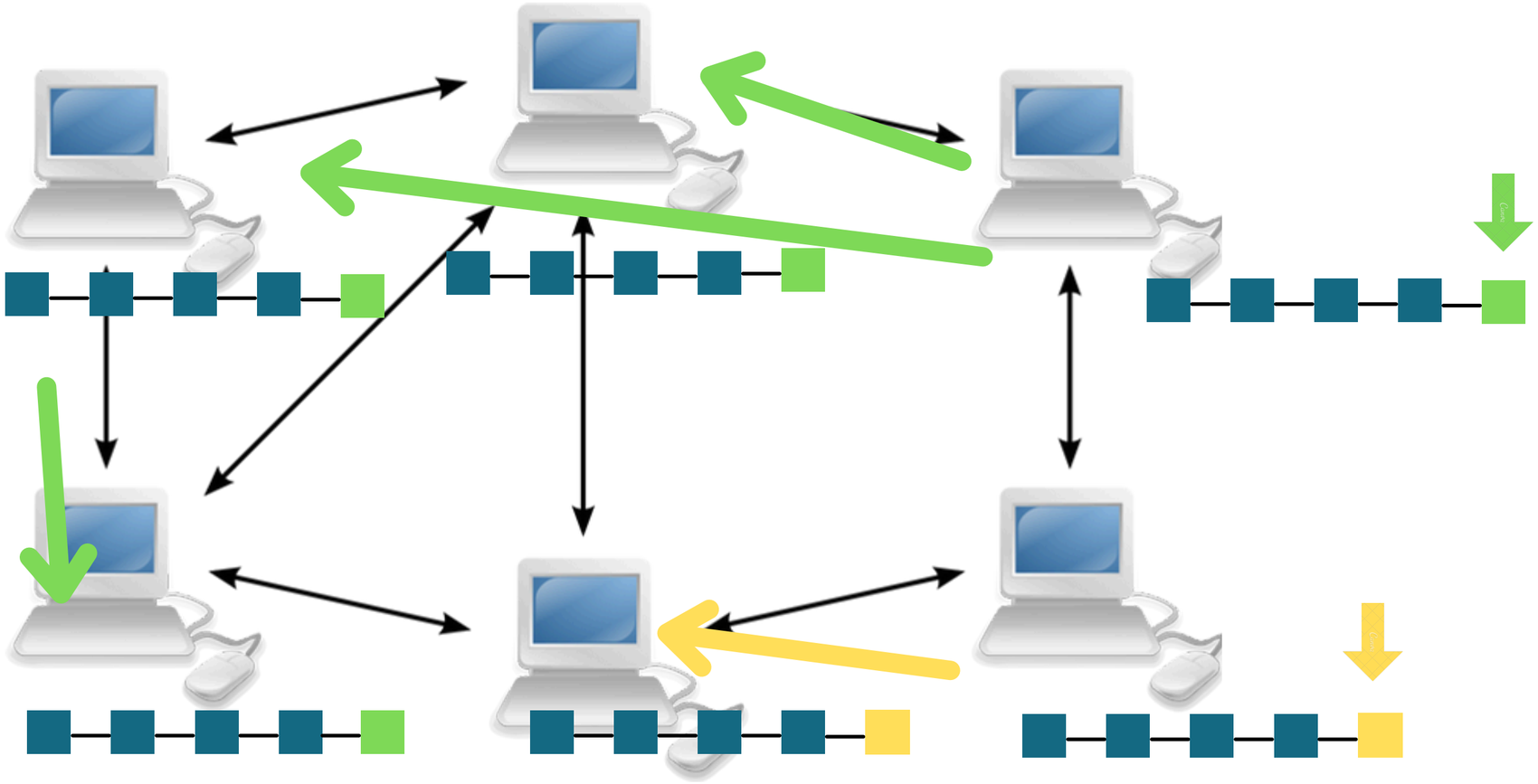
Consensus Protocol

Problem 2: Chain competing



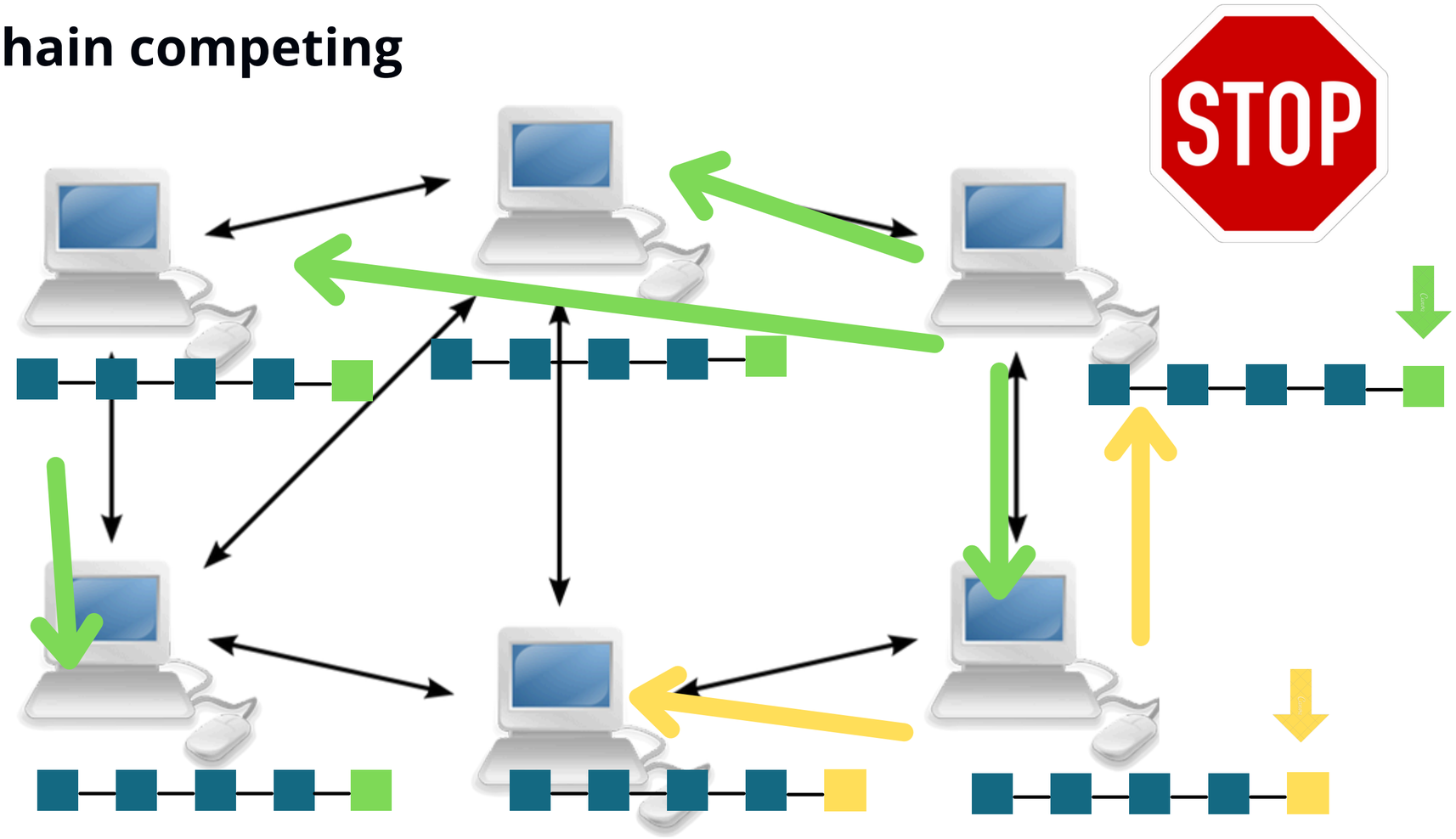
Consensus Protocol

Problem 2: Chain competing



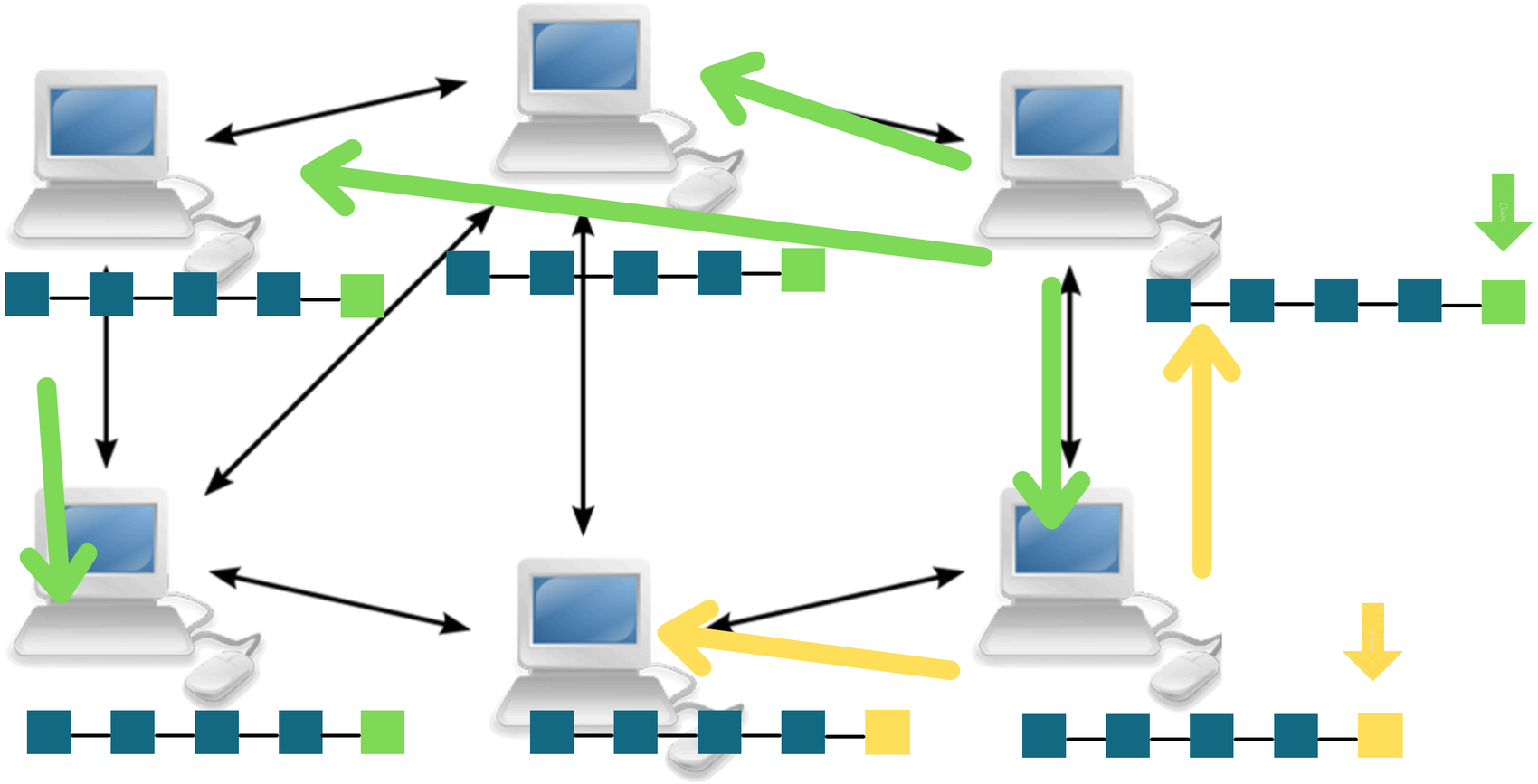
Consensus Protocol

Problem 2: Chain competing



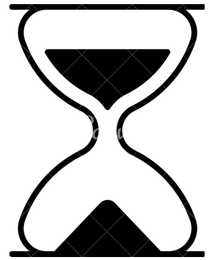
Consensus Protocol

Problem 2: Chain competing

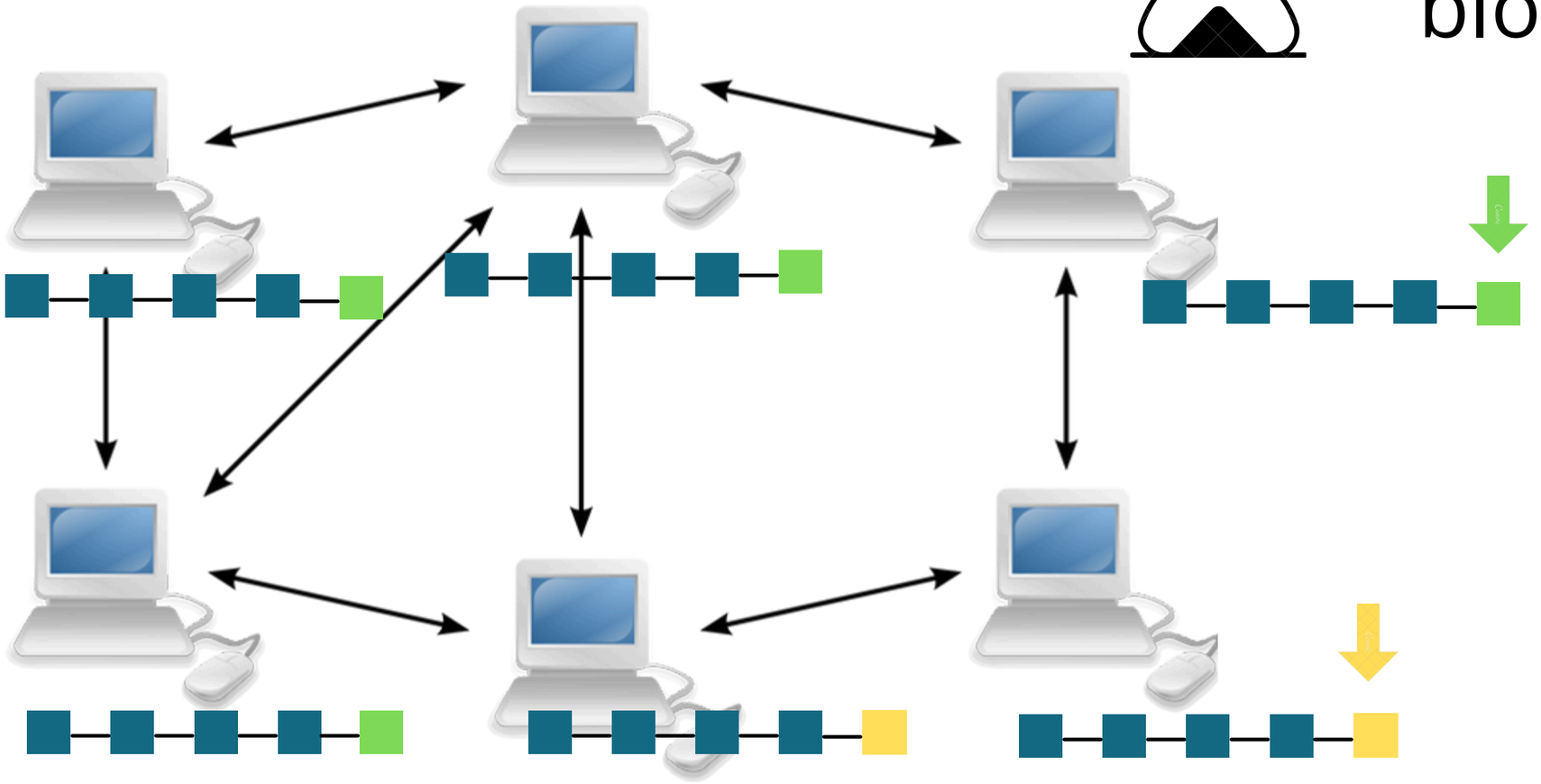


Consensus Protocol

Problem 2: Chain competing

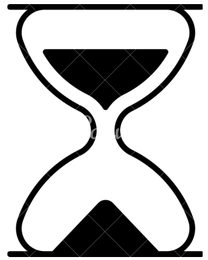


Mining new block...

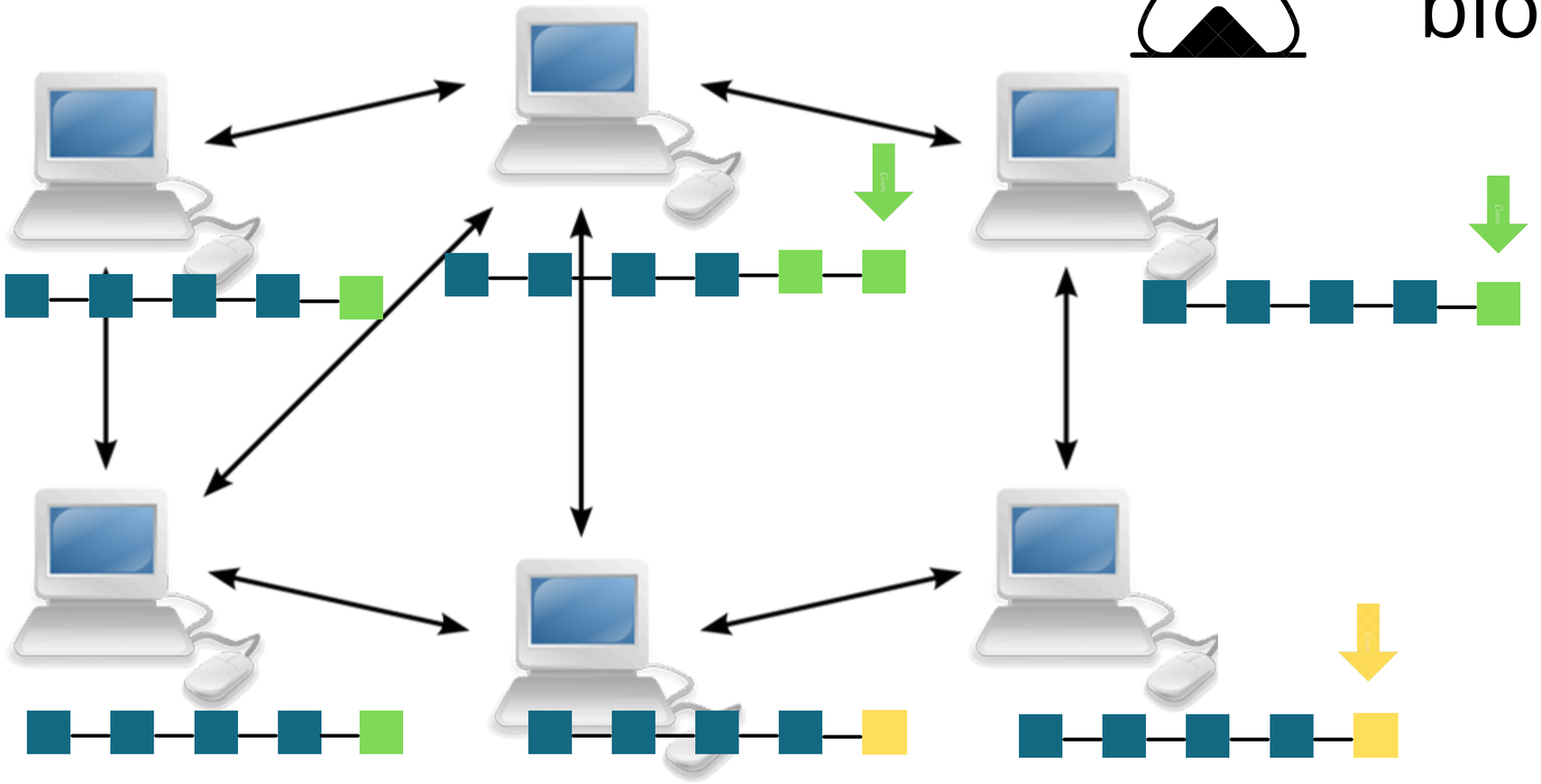


Consensus Protocol

Problem 2: Chain competing

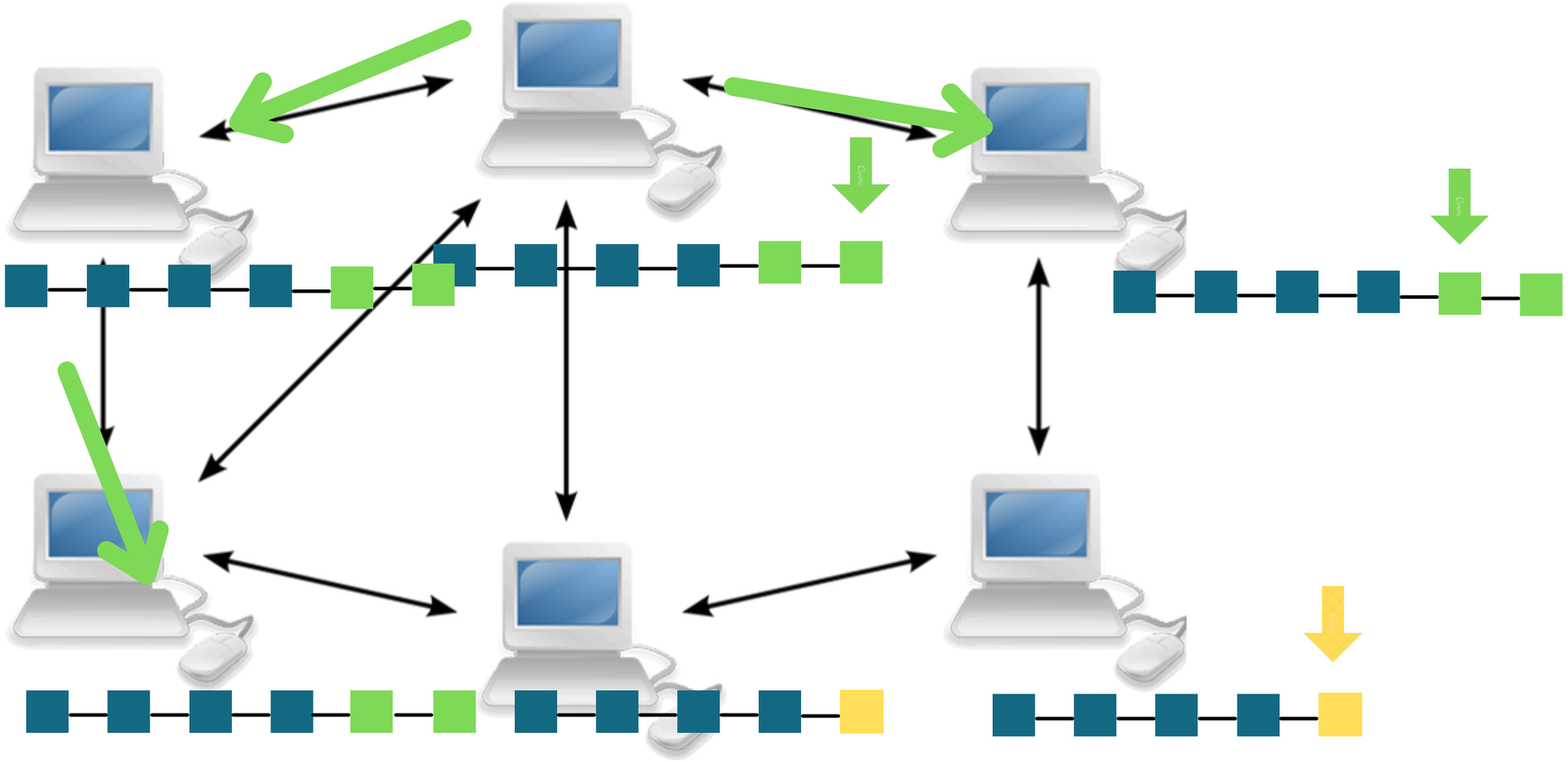


Mining new block...



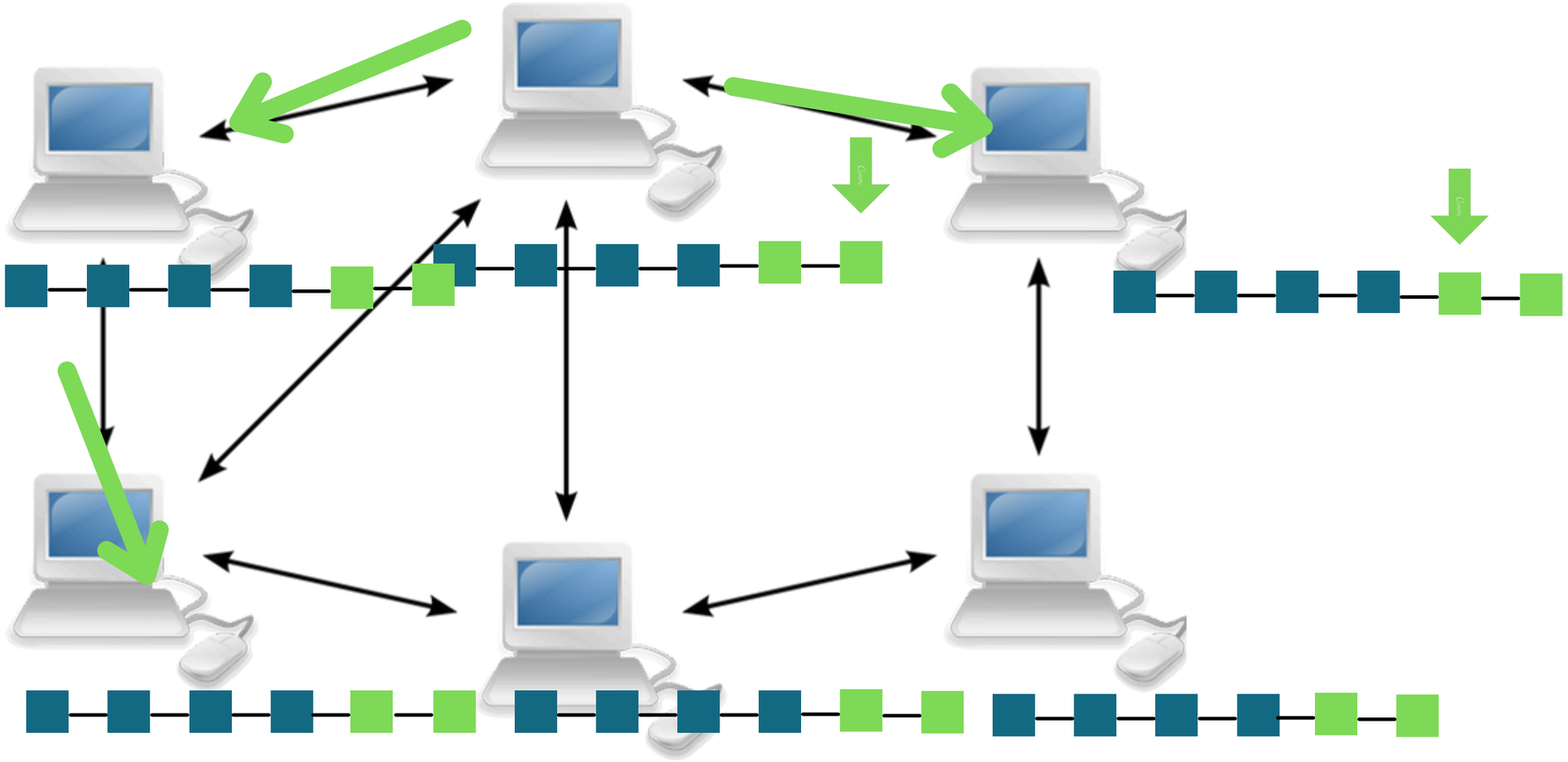
Consensus Protocol

Problem 2: Chain competing



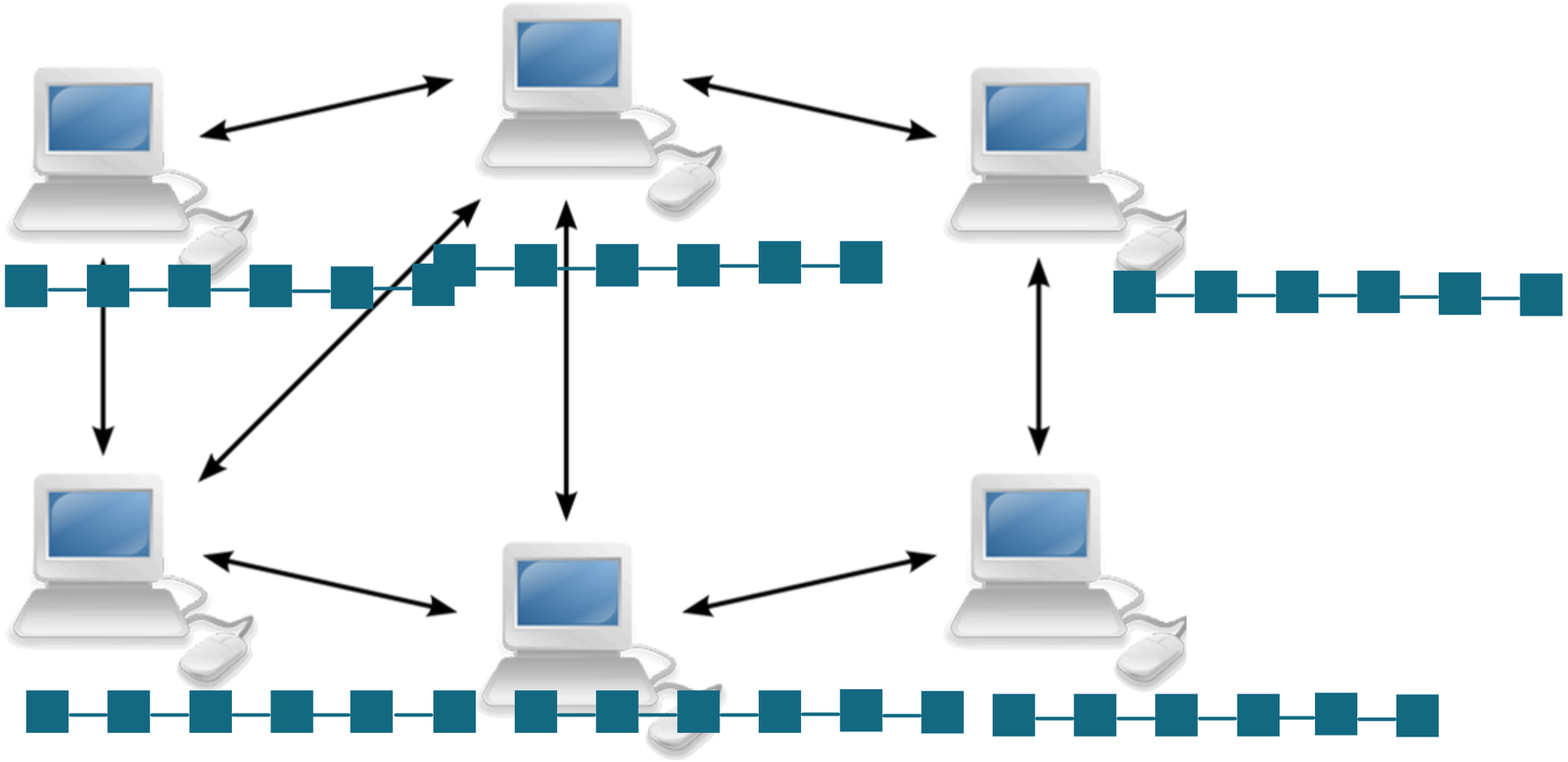
Consensus Protocol

Problem 2: Chain competing



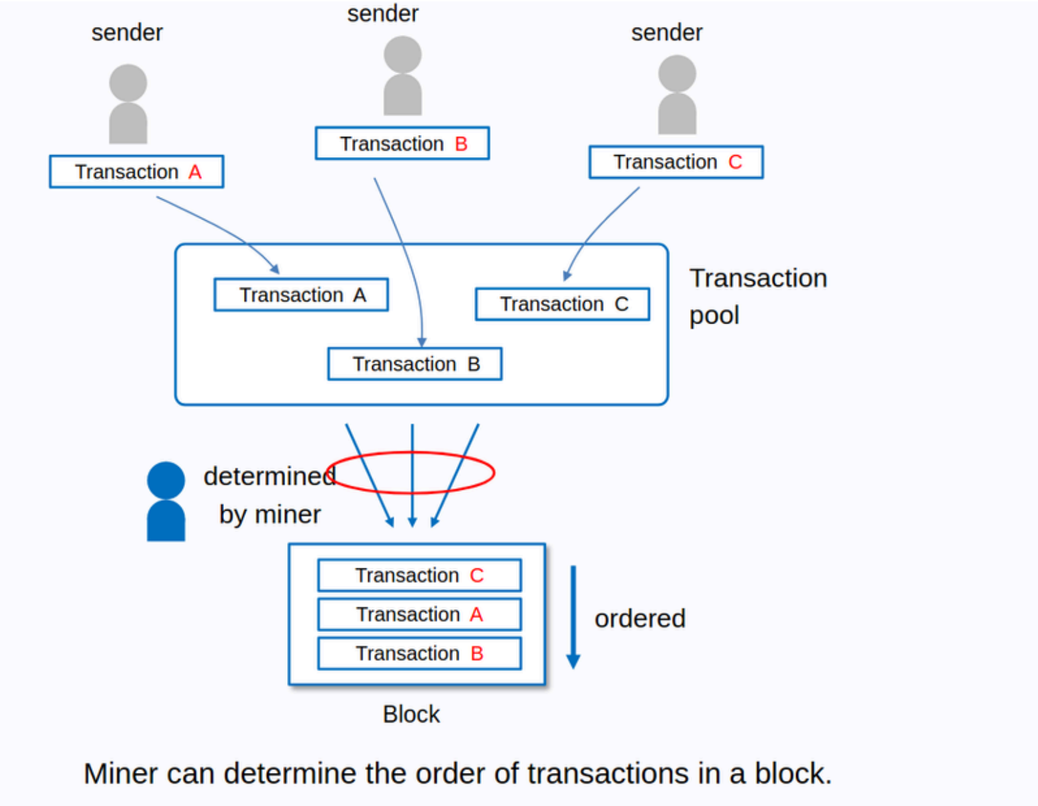
Consensus Protocol

Problem 2: Chain competing



Distributed Ledger

Transactions orders (order inner block)

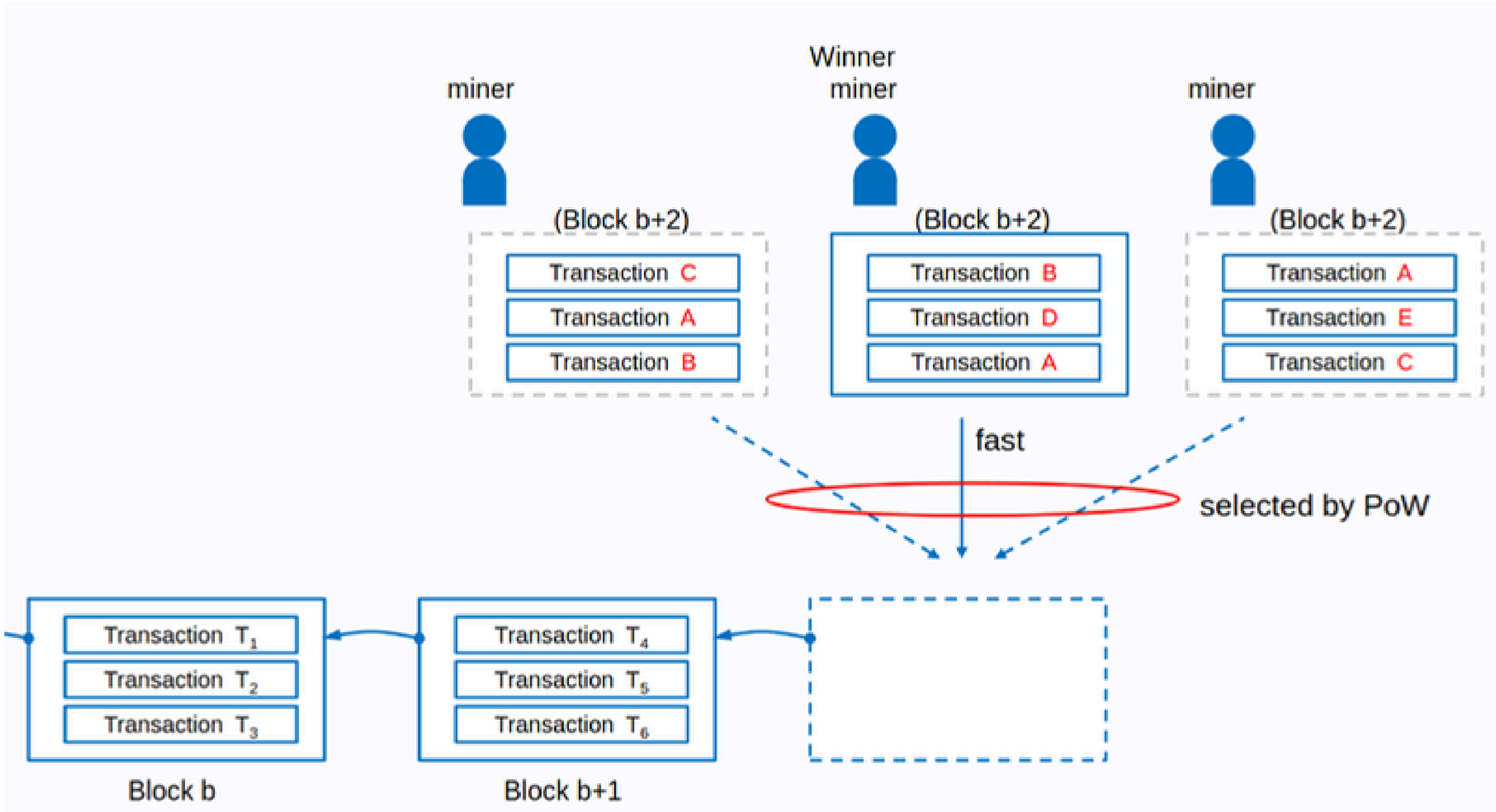


EVM Illustrated

Abdessamed Rezazi

Distributed Ledger

Blocks order (ordering inter blocks)



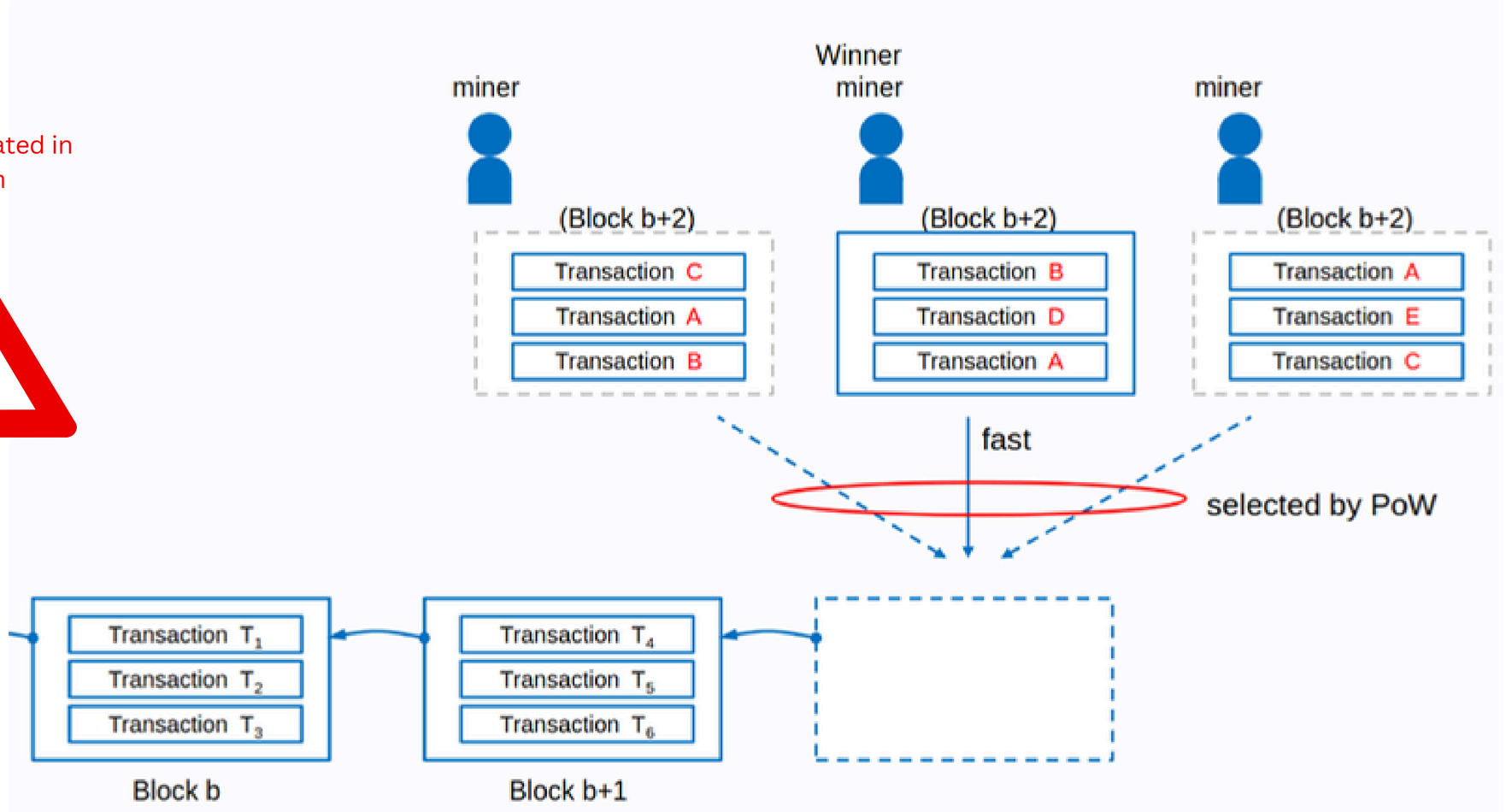
EVM Illustrated

Abdessamed Rezazi

Distributed Ledger

Blocks order (ordering inter blocks)

PoW is deprecated in Ethereum



EVM Illustrated

Abdessamed Rezazi

Consensus

Consensus is the backbone of the blockchain. It defines rules to keep the state consistent even under the presence of malicious peers

Nodes & Clients

A "node" is any instance of **Ethereum client software** that is connected to other computers also running Ethereum software, forming a network

Nodes & Clients

There are three types of nodes

- Full node

  Stores the most recent blockchain data (typically 128 recent blocks) and participates in blocks validation of new blocks

Nodes & Clients

There are three types of nodes

- Full node

  Stores the most recent blockchain data (typically 128 recent blocks) and participates in blocks validation of new blocks

- Archive node

  Archive nodes are full nodes that verify every block from genesis and never delete any of the downloaded data

Nodes & Clients

There are three types of nodes

- Full node

  Stores the most recent blockchain data (typically 128 recent blocks) and participates in blocks validation of new blocks

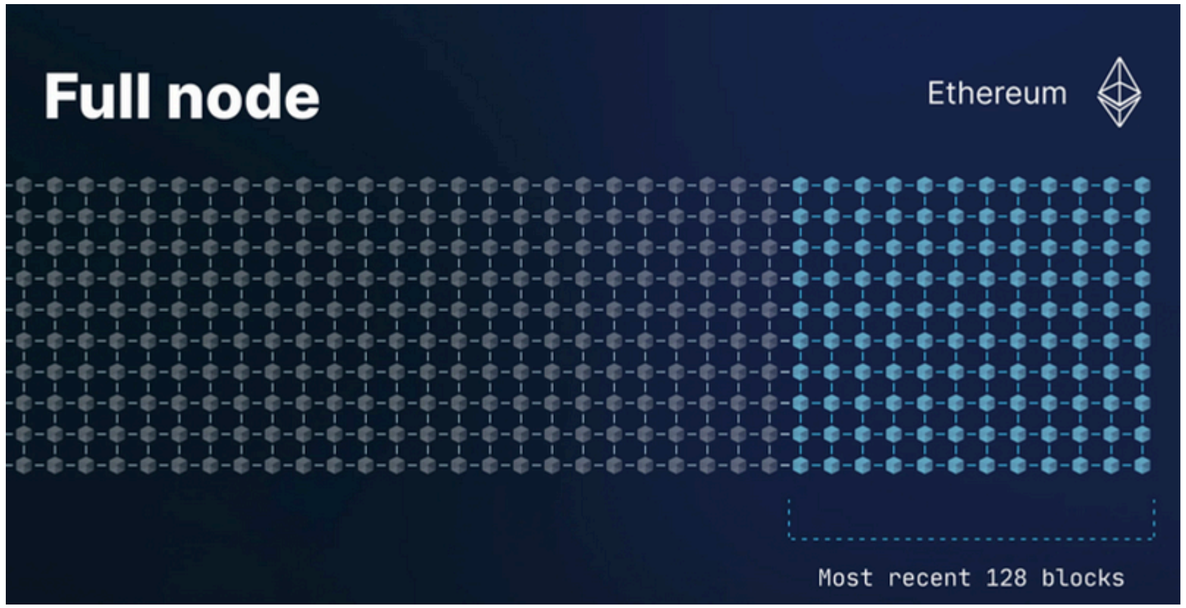
- Archive node

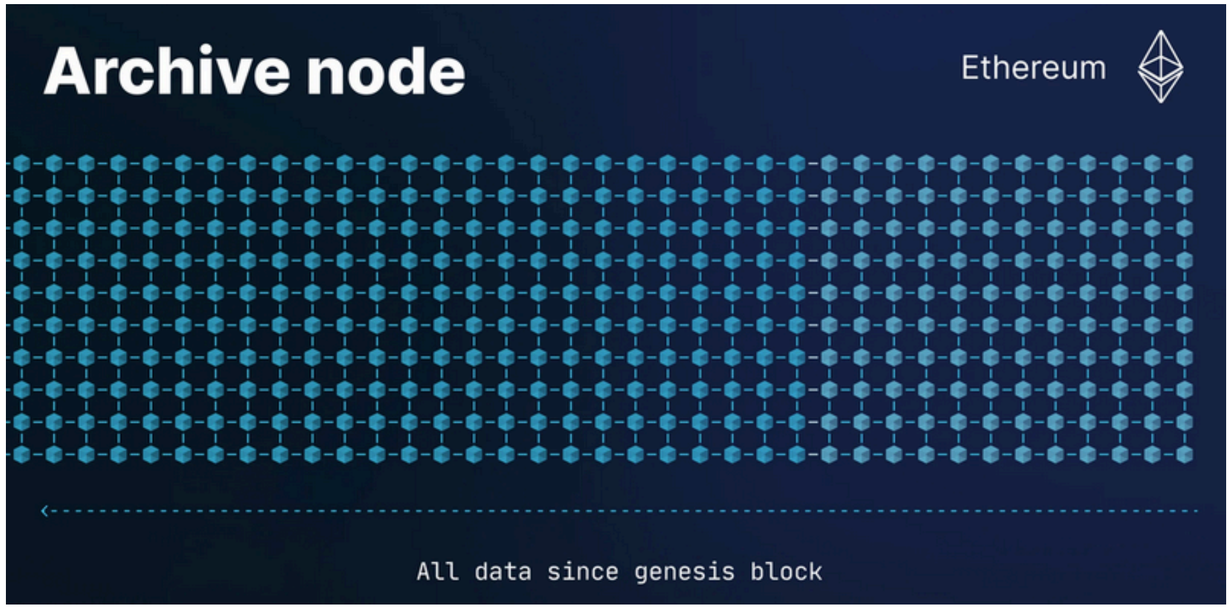
  Archive nodes are full nodes that verify every block from genesis and never delete any of the downloaded data

- Light node

  Instead of downloading every block, light nodes only download block headers. These headers contain summary information about the contents of the blocks. Any other information the light node requires gets requested from a full node. **They also participate in new blocks validation**

Nodes & Clients





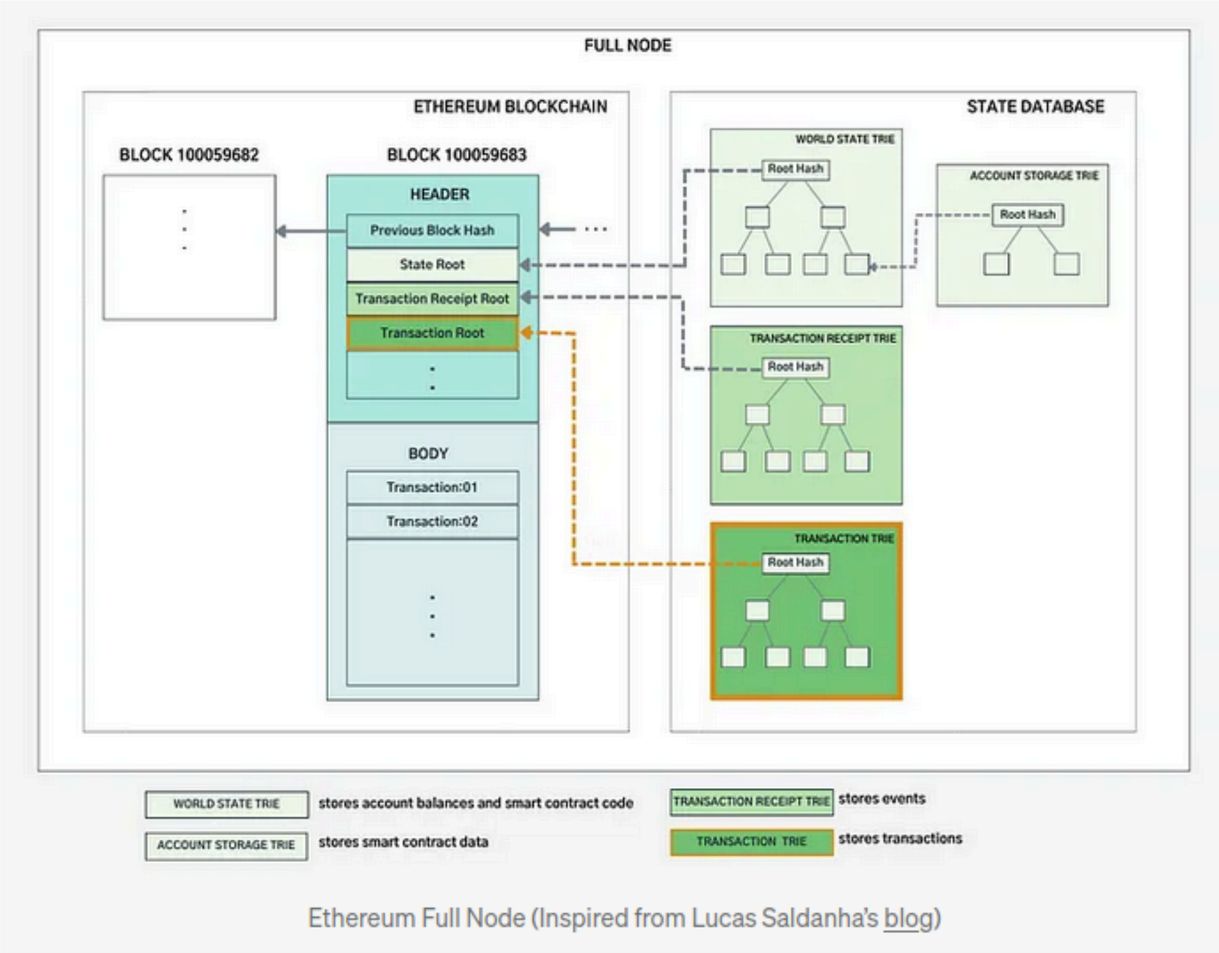
Abdessamed Rezazi

Nodes & Clients

How can light nodes participate in blocks verification if they store only block headers?

Nodes & Clients

An Ethereum full node stores two types of data : block data and state data.

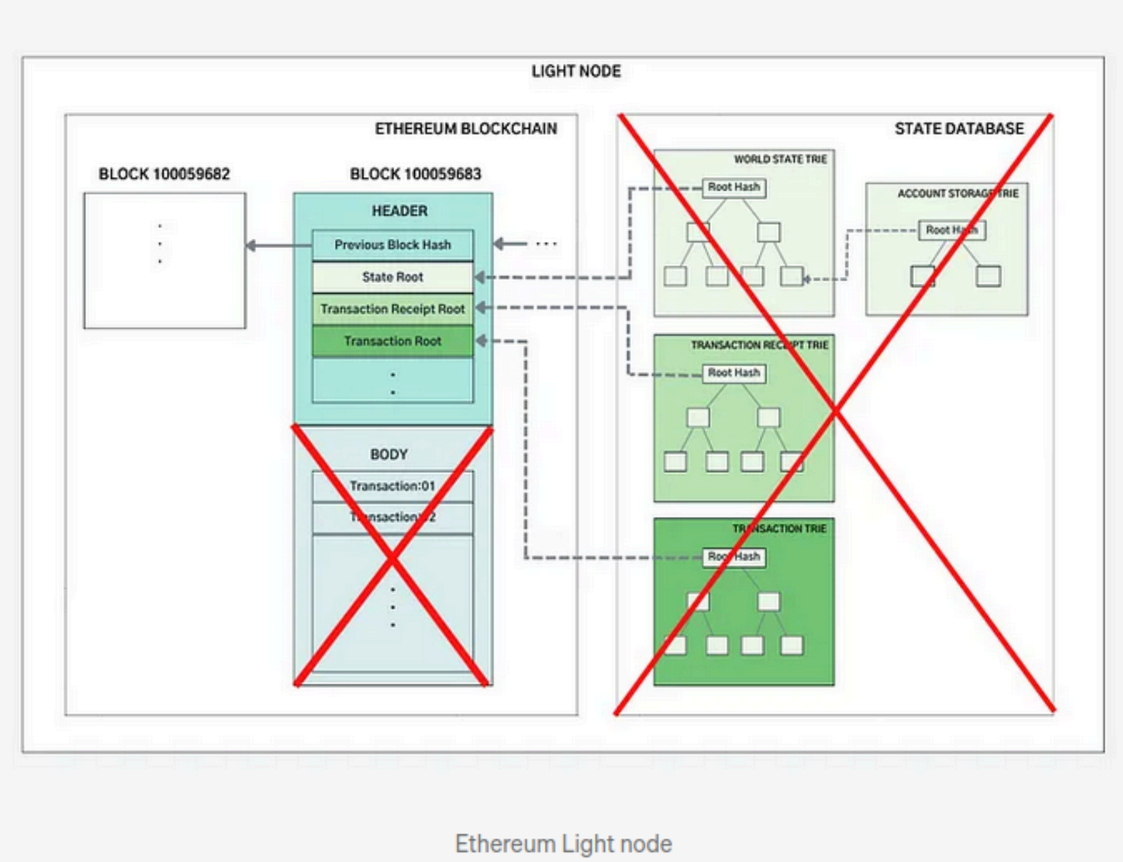


Ethereum Full Node (Inspired from Lucas Saldanha's blog)

Abdessamed Rezazi

Nodes & Clients

An Ethereum client node downloads only Block headers data

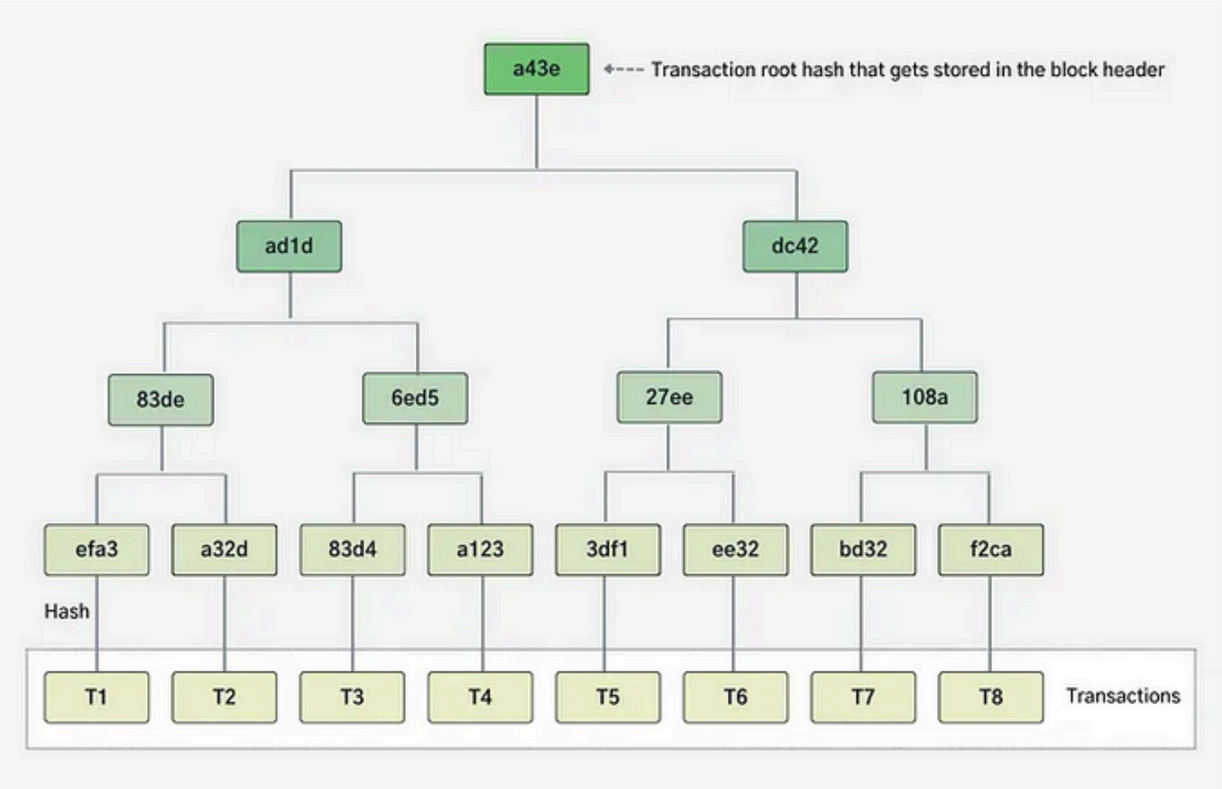


Ethereum Light node

Abdessamed Rezazi

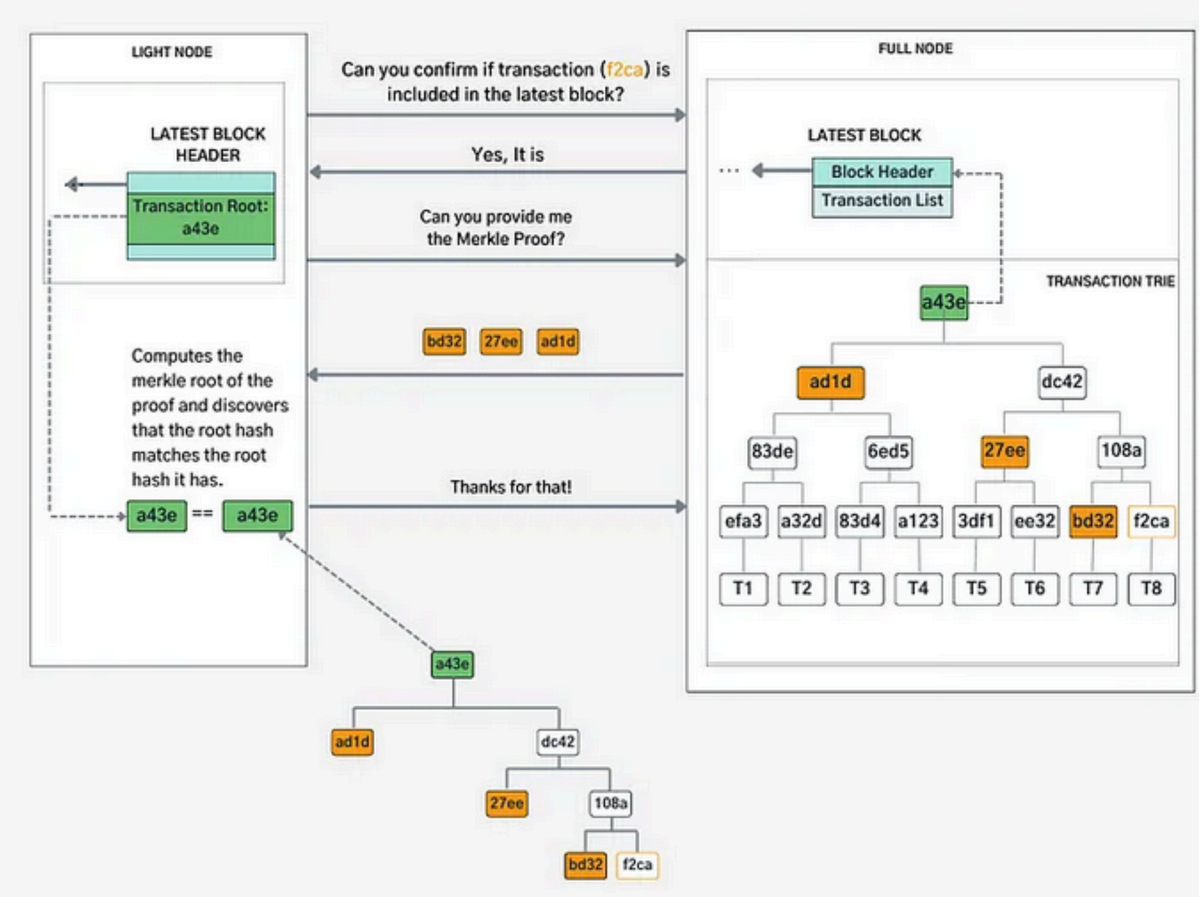
Nodes & Clients

Transactions are stored in block as Merkle Tree data structure



Nodes & Clients

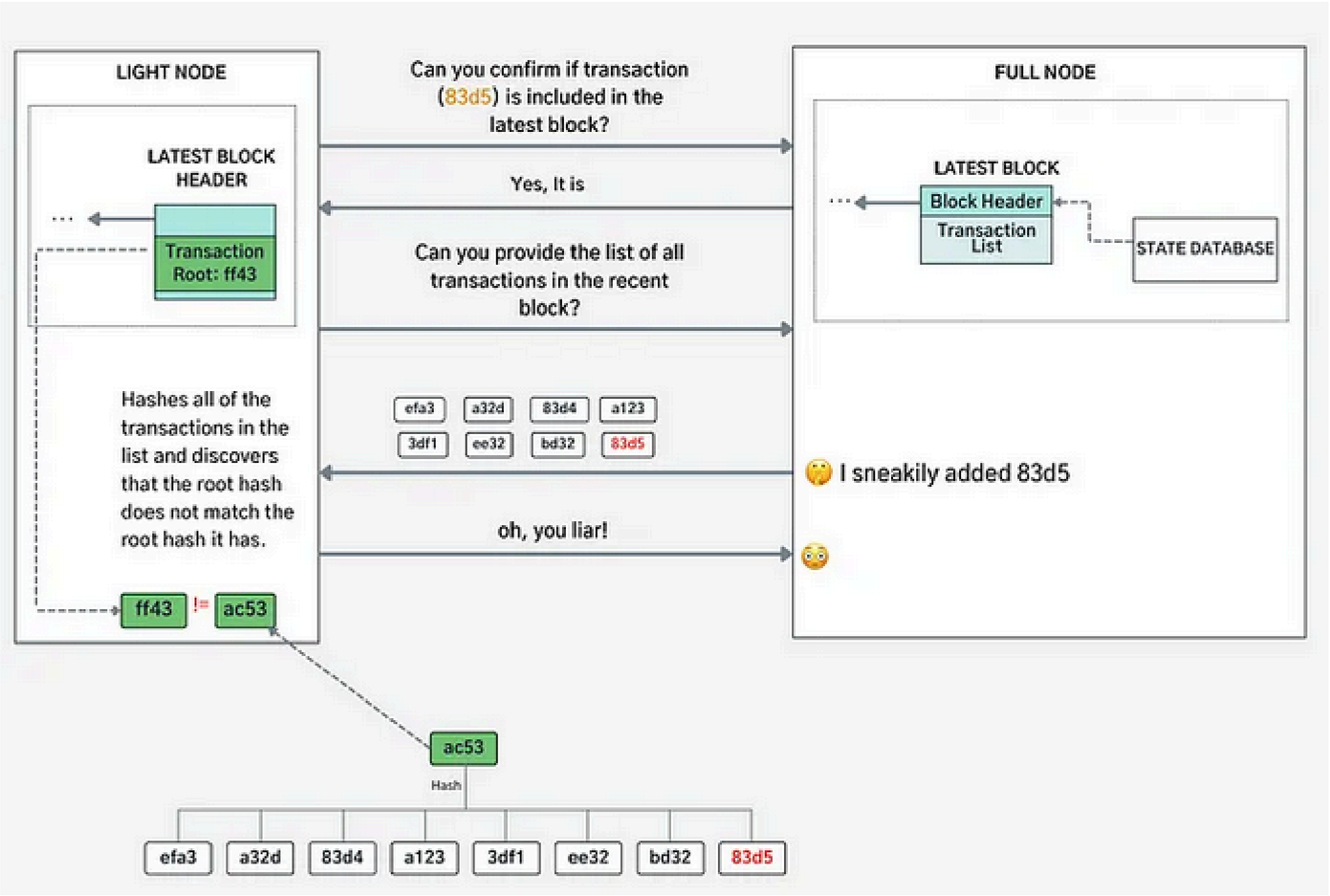
If a light client needs to verify if a transaction is included in a block, it communicates with a full node to send a Merkle proof. It turns out the full node does not need to send all transactions



Abdessamed Rezazi

Nodes & Clients

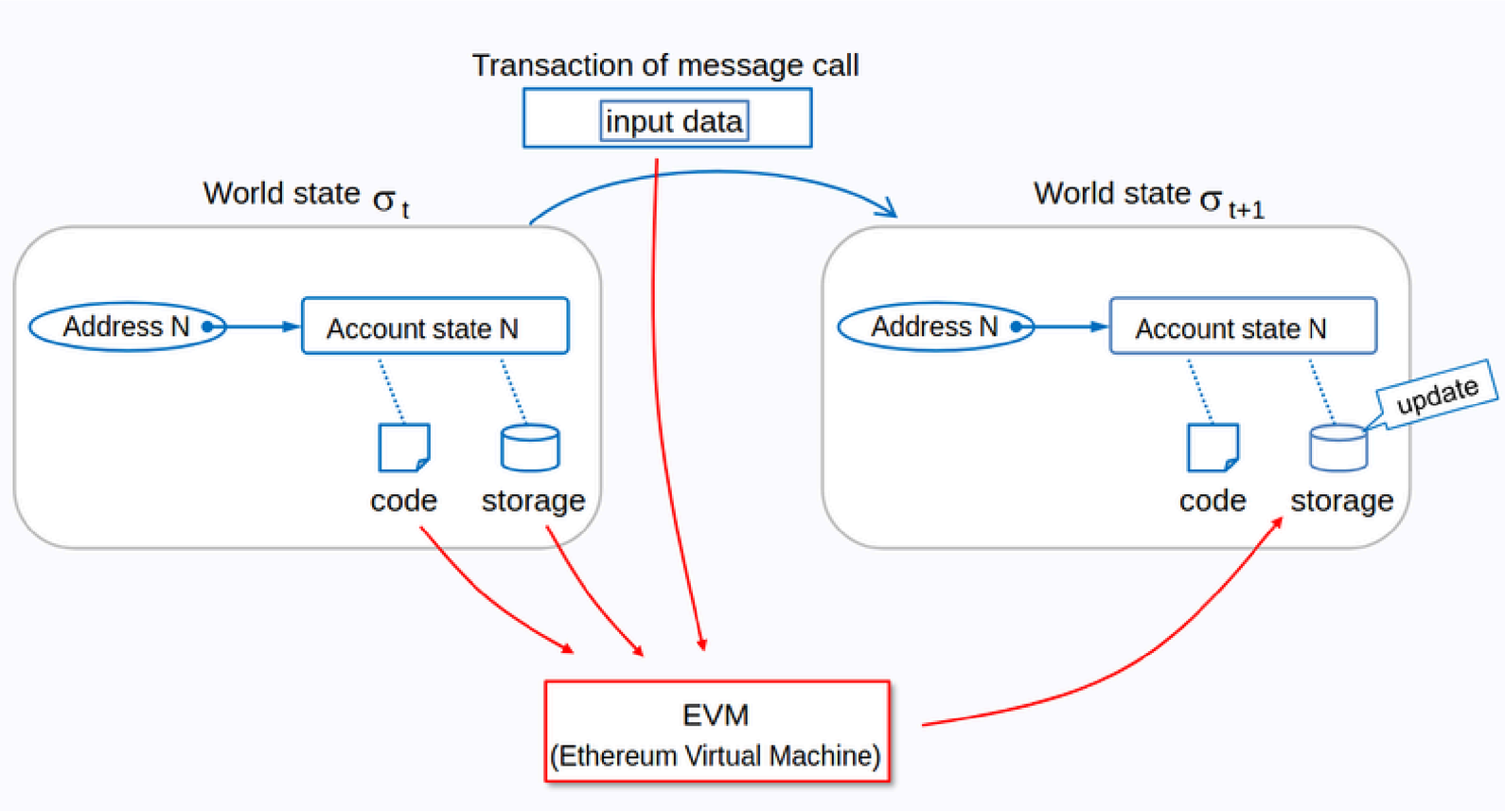
A transaction can easily be detected if it is not included in a block, given the uniqueness of hash outputs



Abdessamed Rezazi

Ethereum Virtual Machine

EVM is the execution environment where the state is updated

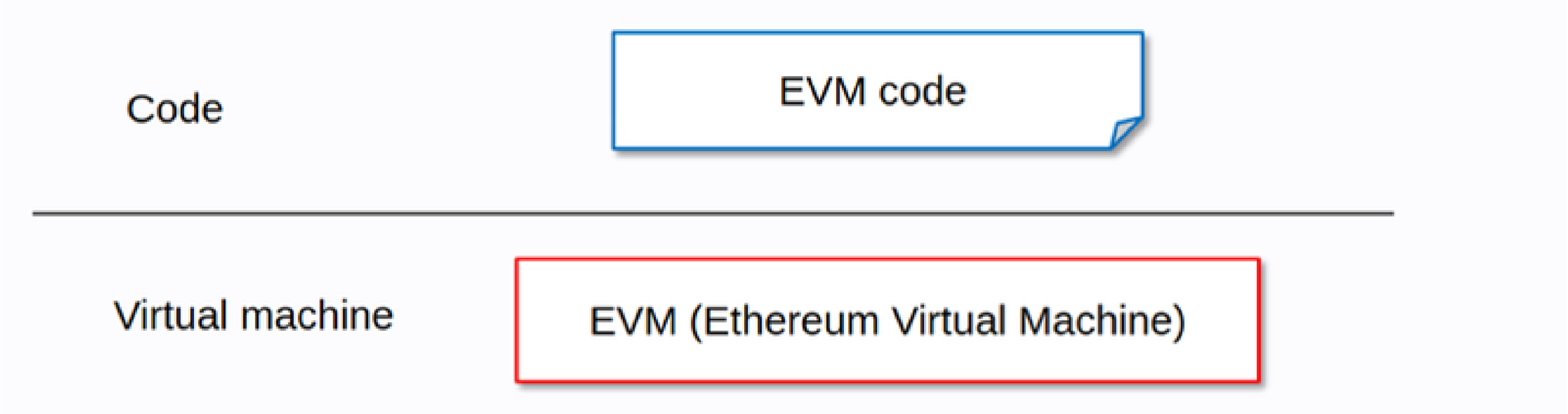


EVM illustrated

Abdessamed Rezazi

Ethereum Virtual Machine

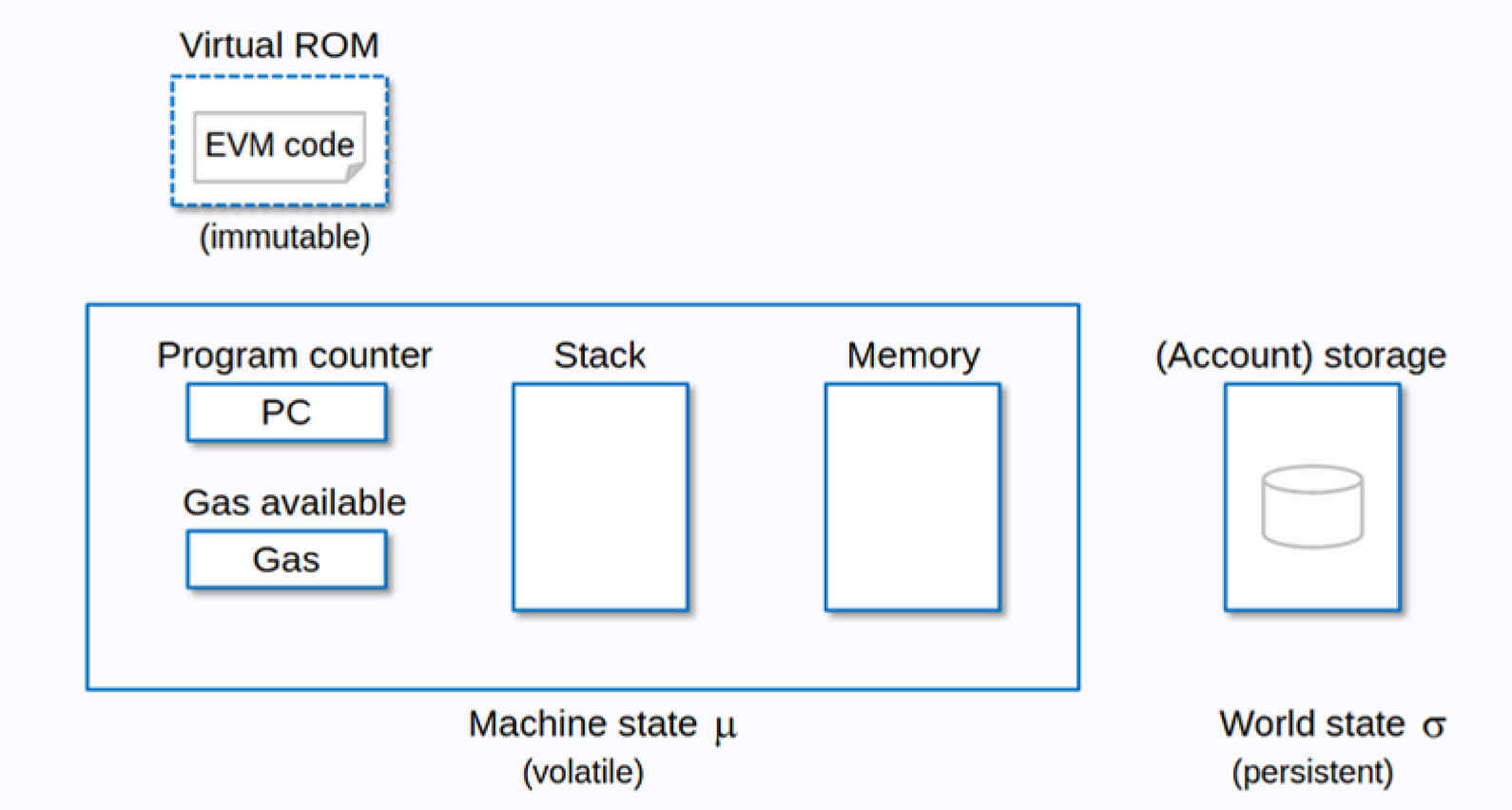
The Ethereum Virtual Machine is the runtime environment for smart contracts in Ethreum.



EVM illustrated

Ethereum Virtual Machine

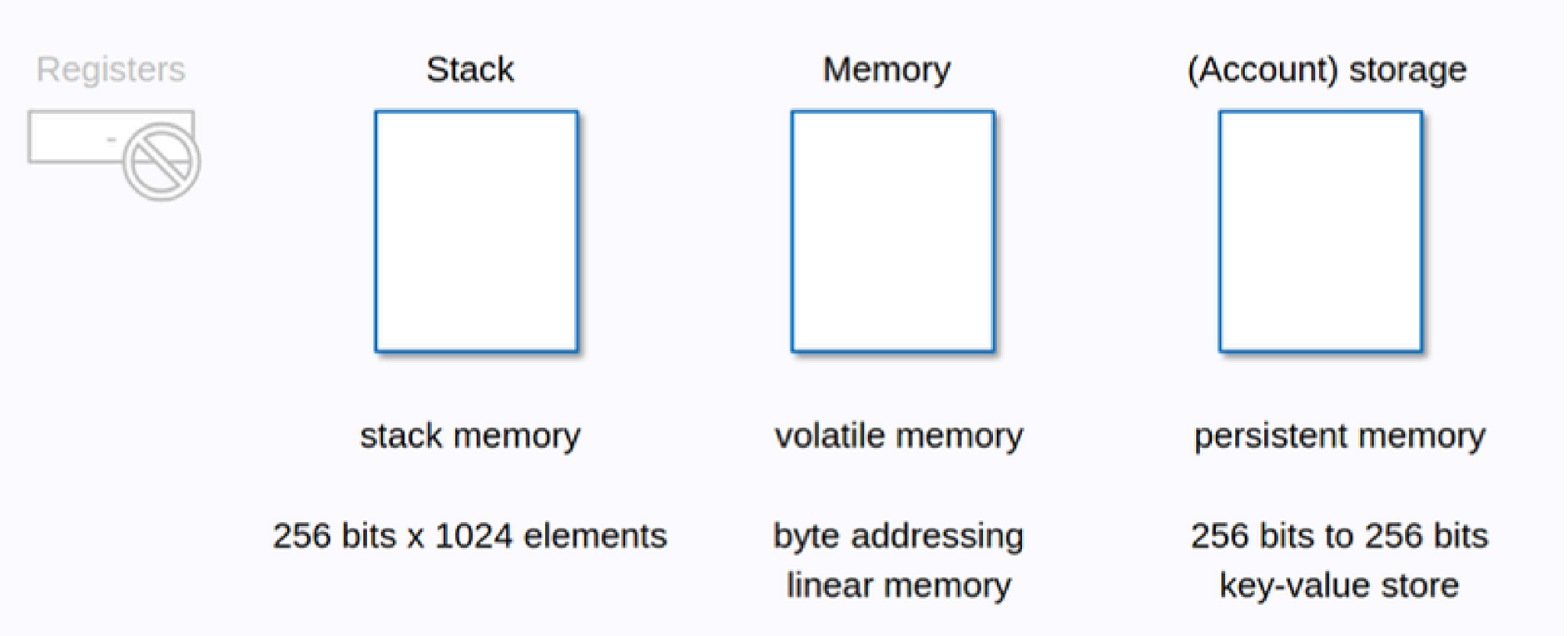
The EVM is a stack-based architecture



EVM illustrated

Ethereum Virtual Machine

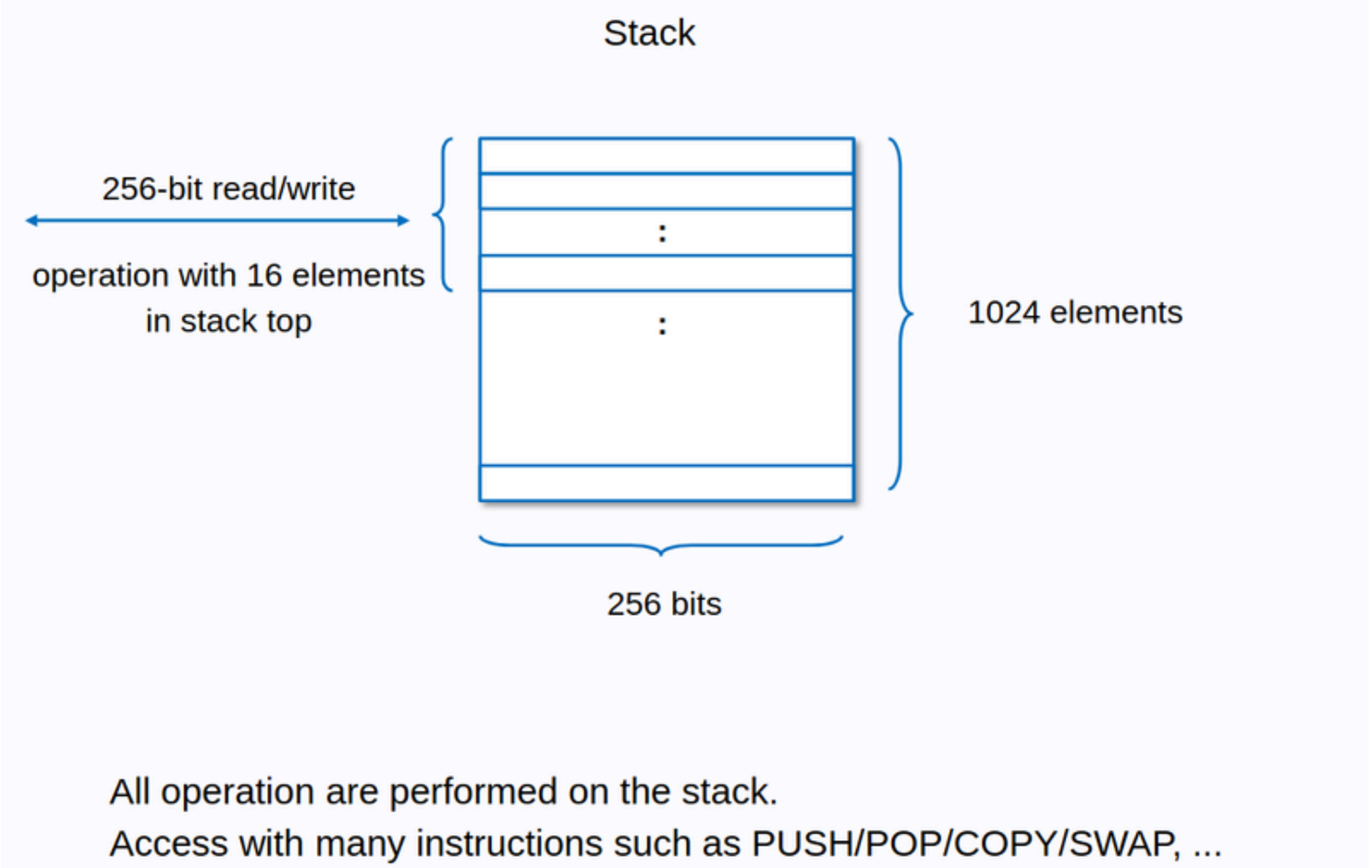
The EVM has several space resources



EVM illustrated

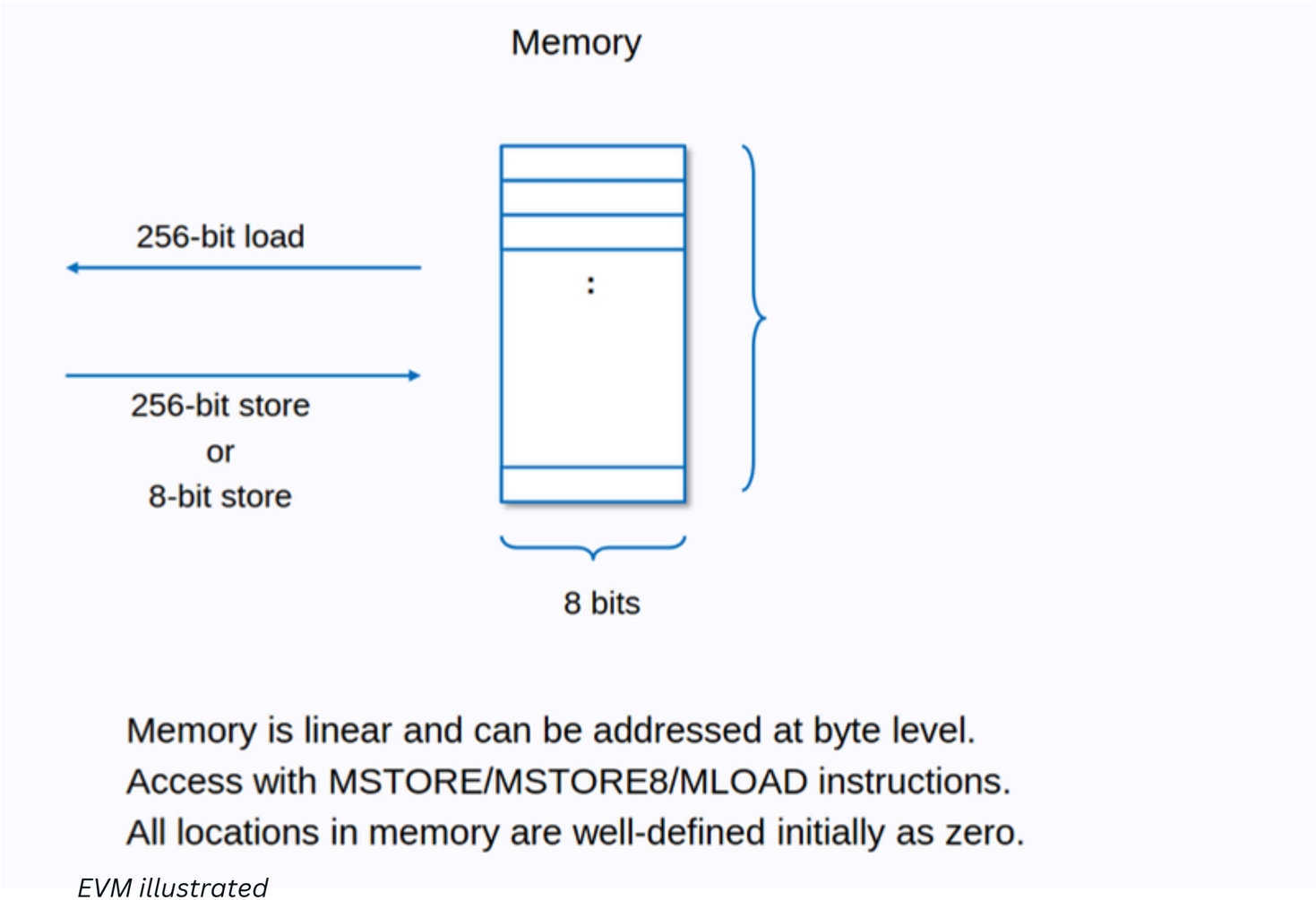
Abdessamed Rezazi

Ethereum Virtual Machine



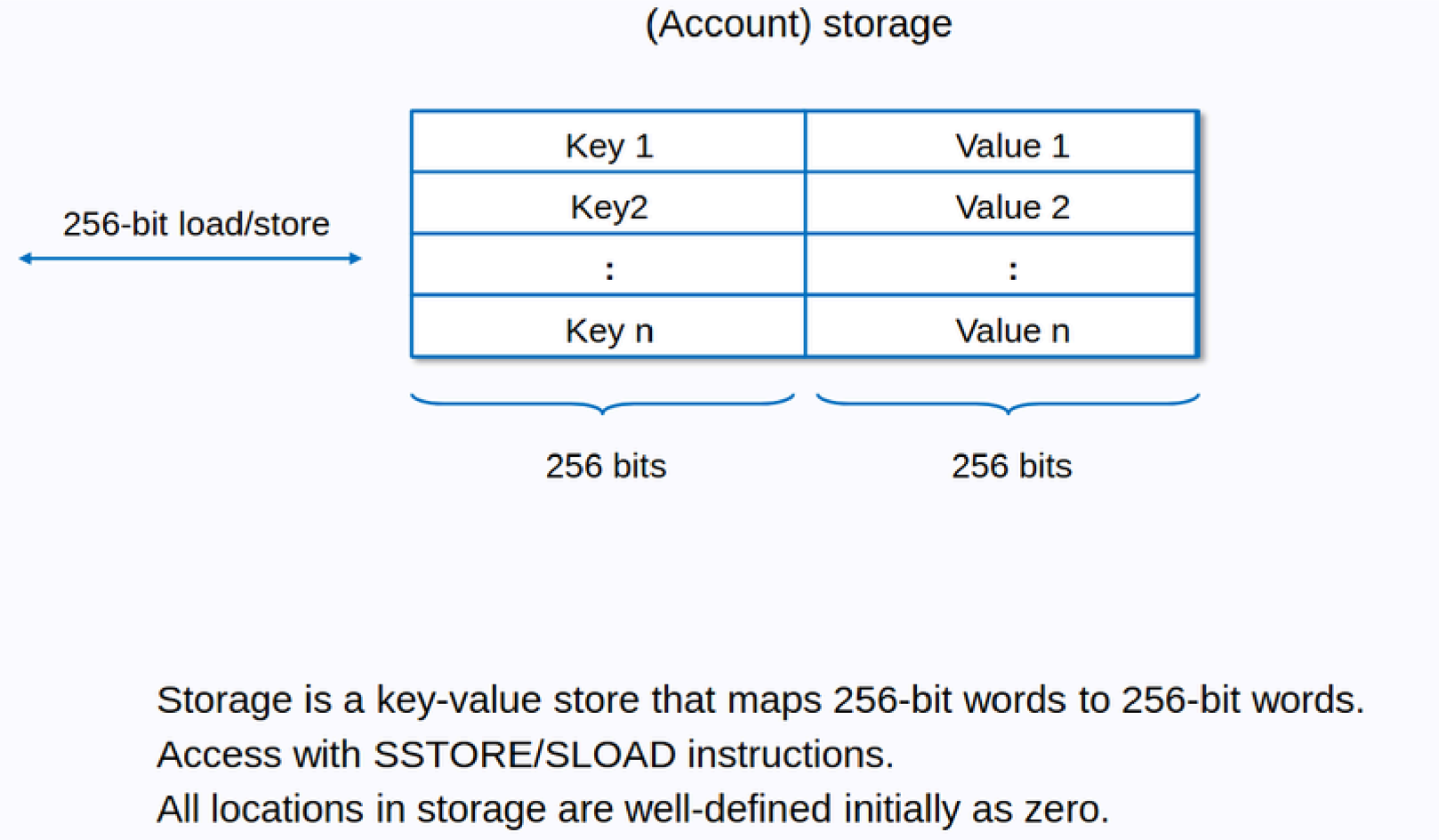
EVM illustrated

Ethereum Virtual Machine



EVM illustrated

Ethereum Virtual Machine

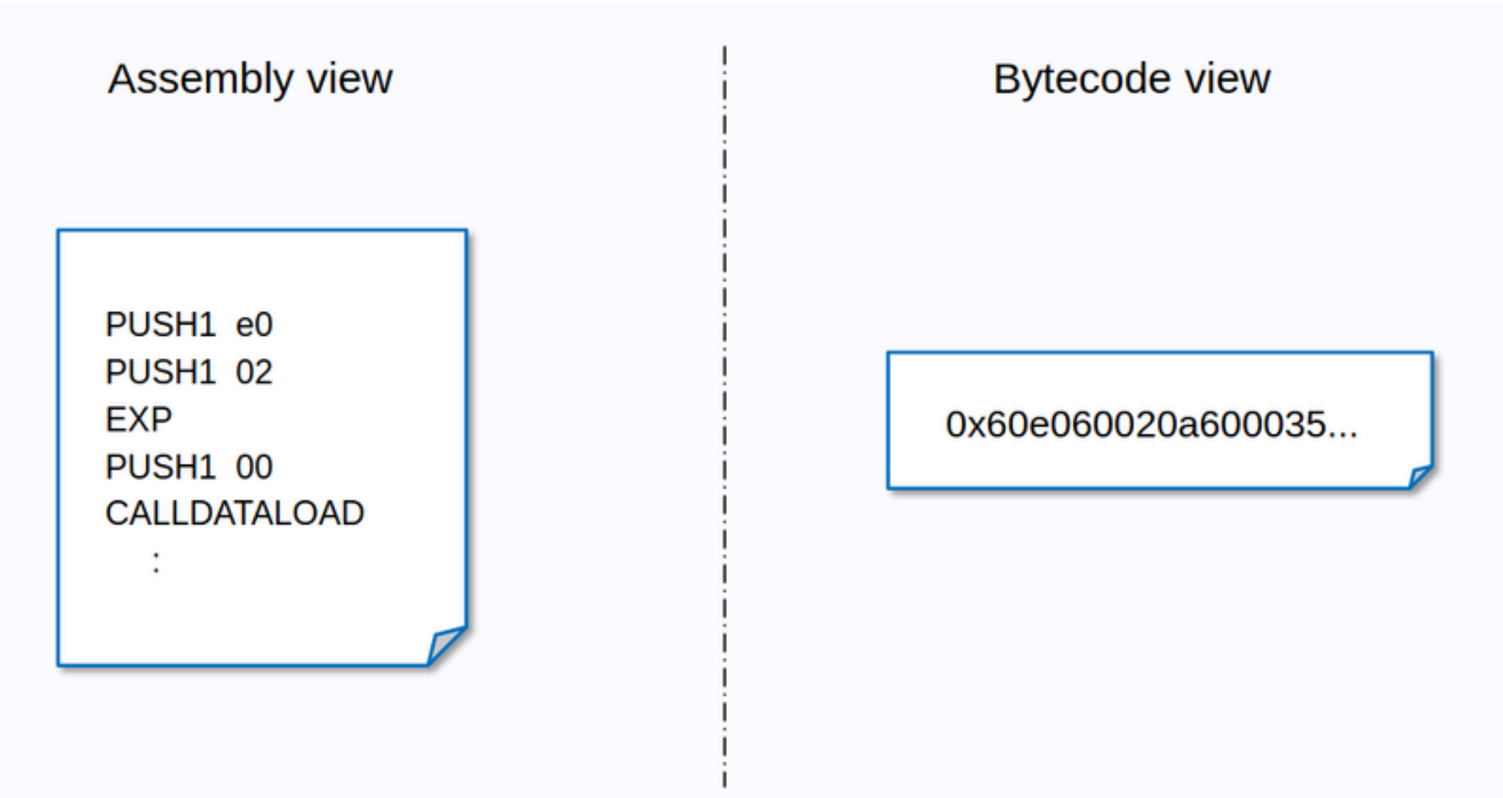


EVM illustrated

Abdessamed Rezazi

Ethereum Virtual Machine

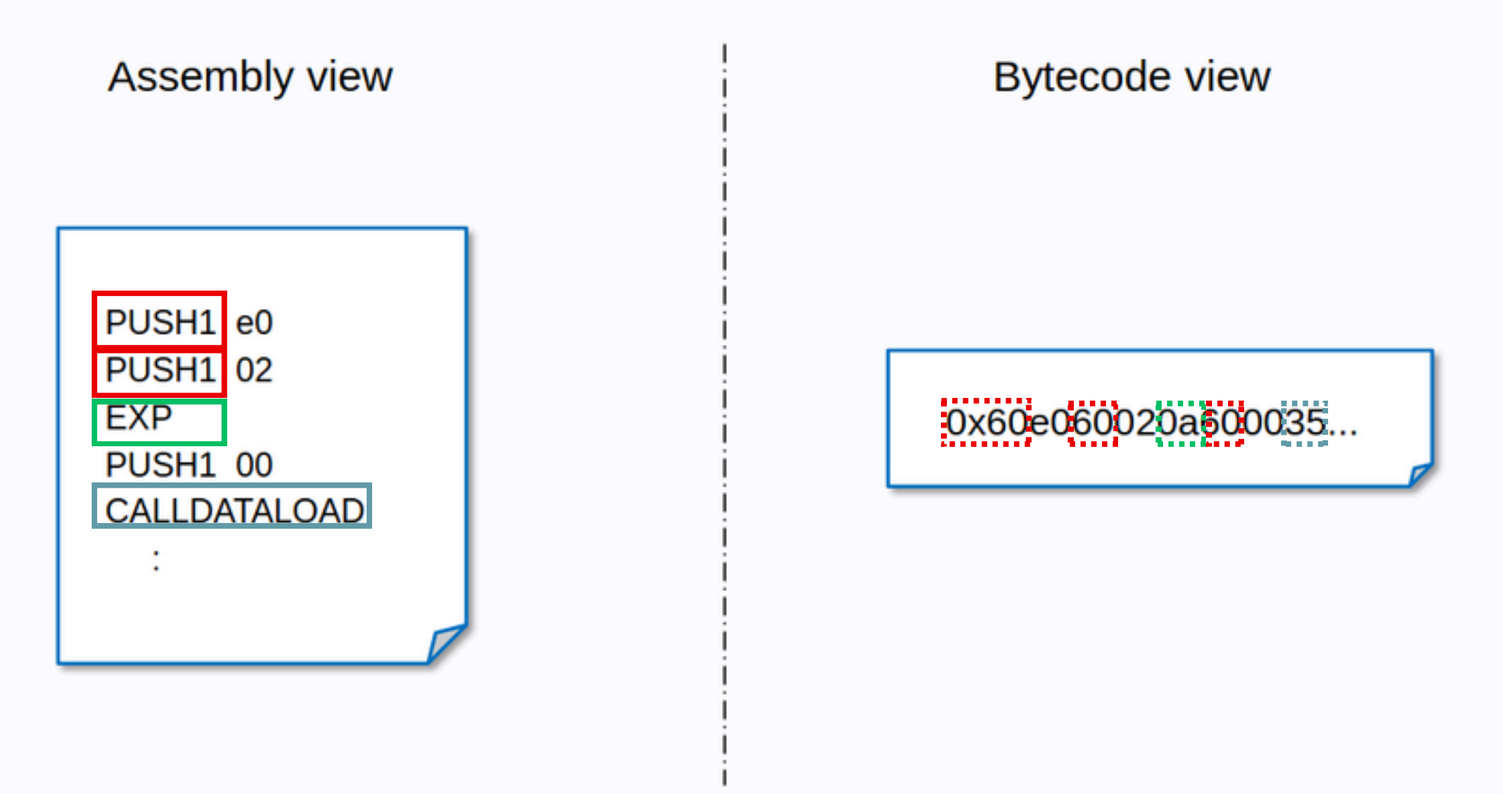
Smart contracts are compiled into Bytecode. EVM executes bytecode.
Each assembly opcode is associated with a bytecode



EVM illustrated

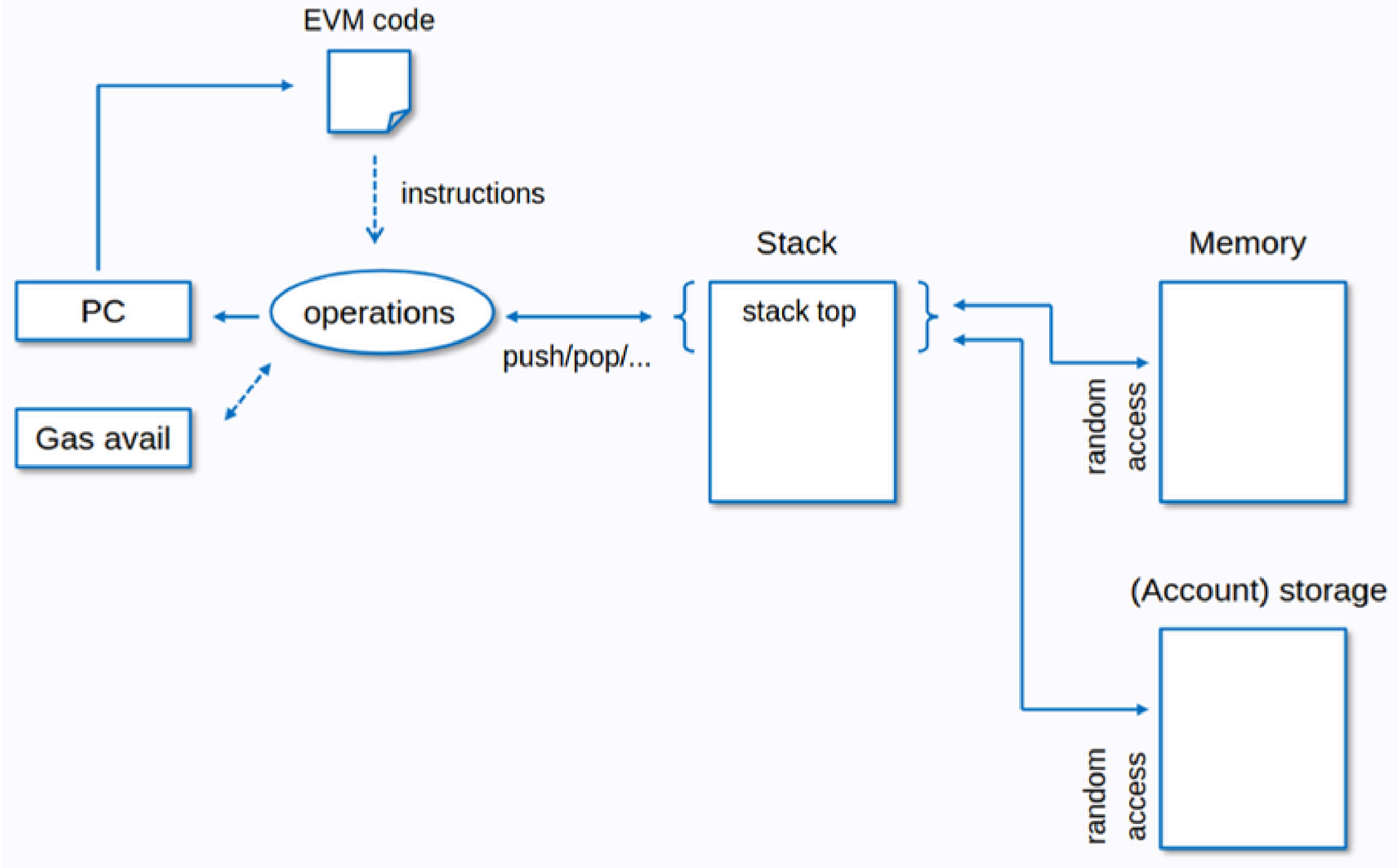
Ethereum Virtual Machine

Smart contracts are compiled into Bytecode. EVM executes bytecode.
Each assembly opcode is associated with a bytecode



EVM illustrated

Ethereum Virtual Machine



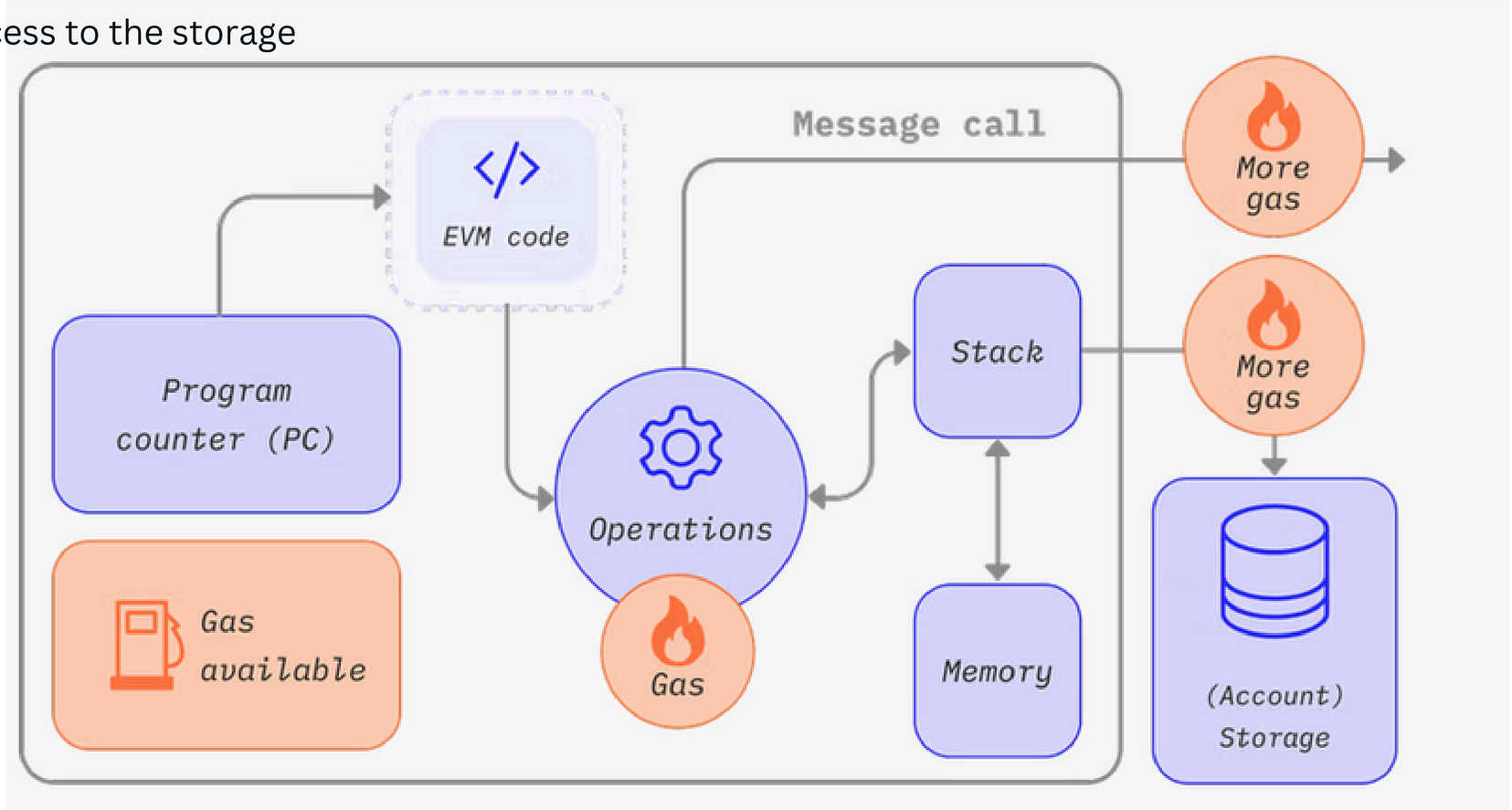
EVM illustrated

Abdessamed Rezazi

Ethereum Virtual Machine

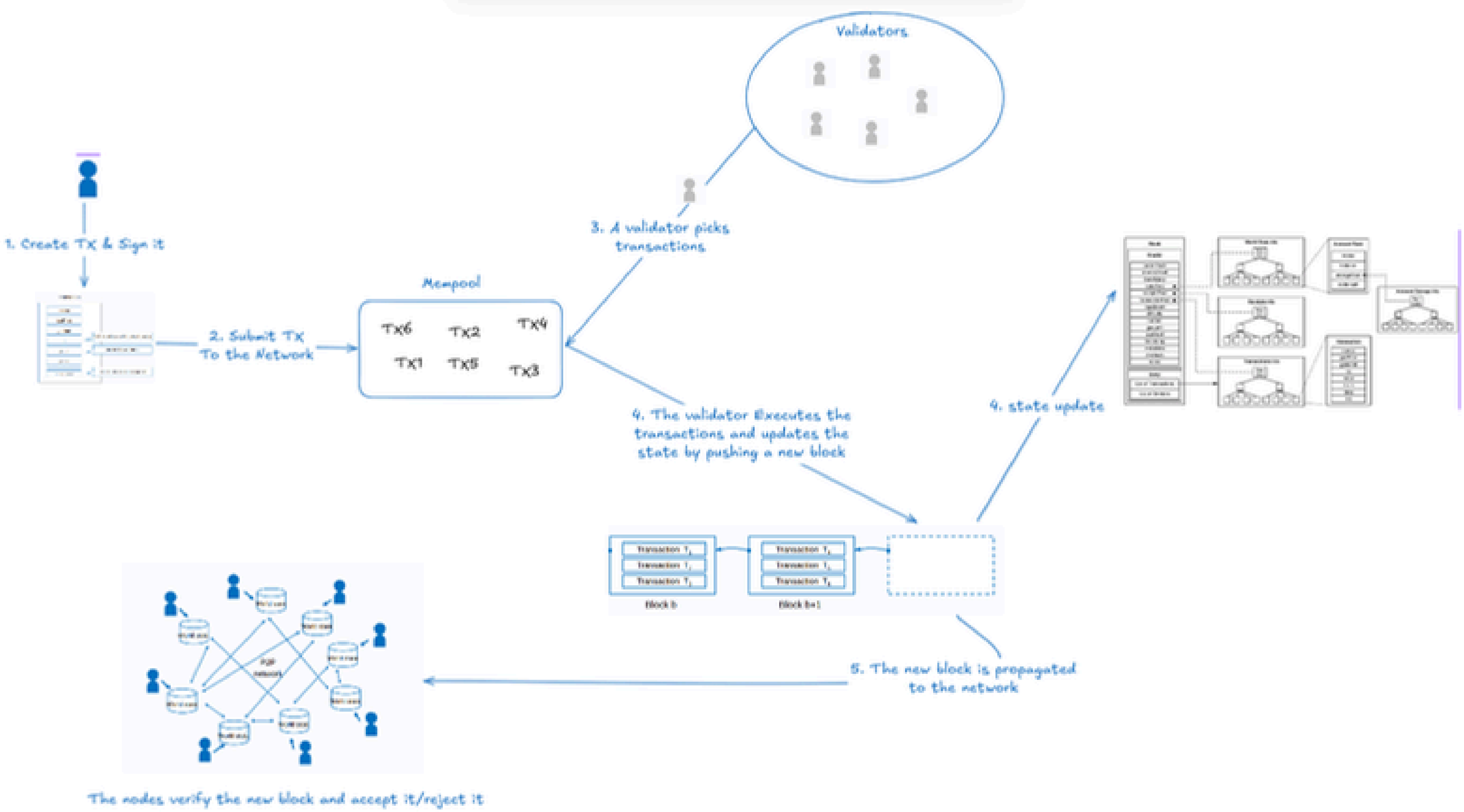
Gas is consumed on:

- each operation(opcode) executed and on each message call
- Each access to the storage

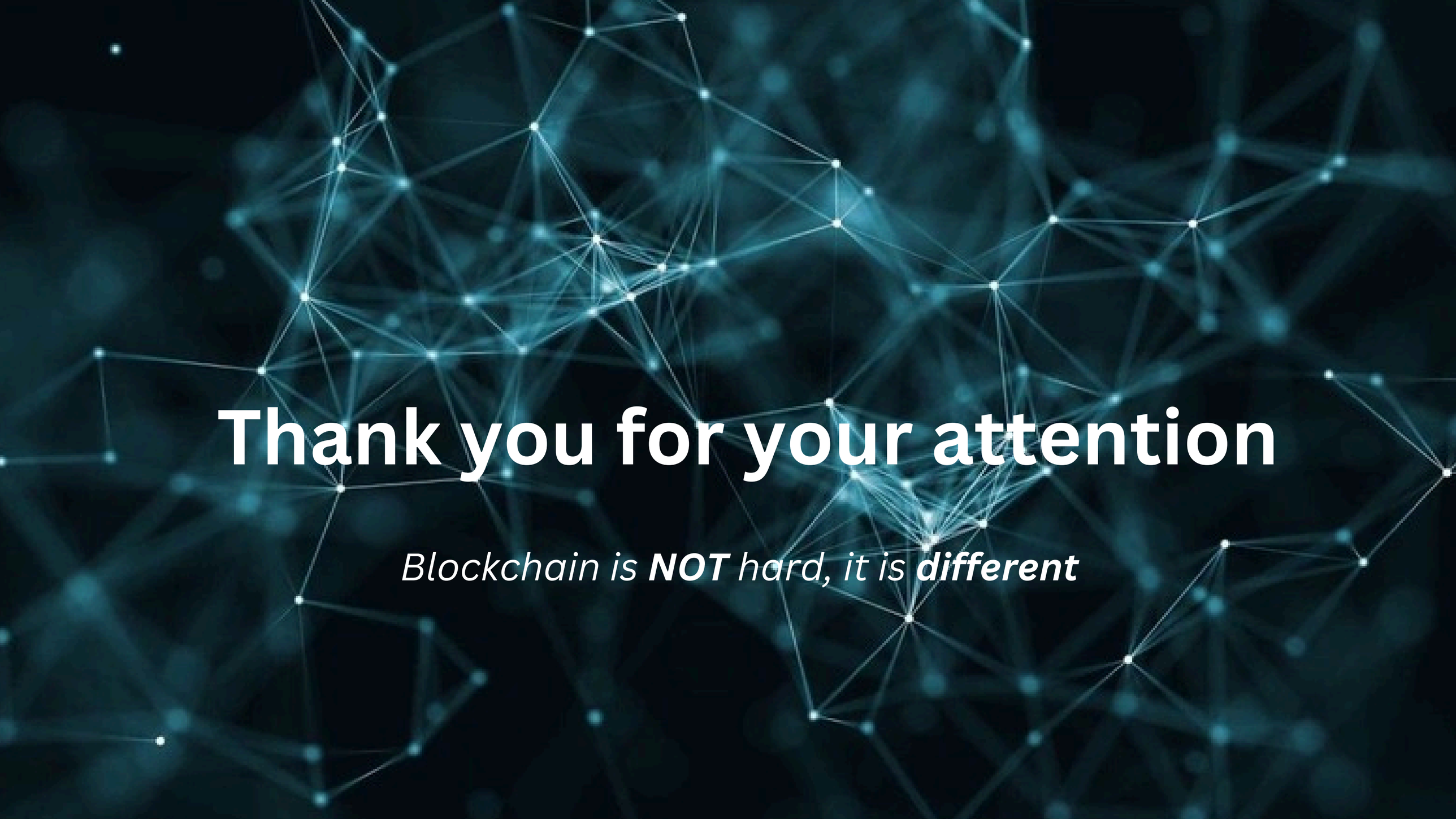


Ethereum Docs

Summary


Validators
1. Create TX & Sign it
2. Submit TX
To the Network
Mempool
Tx6
Tx2
Tx4
Tx1
Tx5
Tx3
3. A validator picks
transactions
4. The validator Executes the
transactions and updates the
state by pushing a new block
4. state update
5. The new block is propagated
to the network
The nodes verify the new block and accept it/reject it

هذا وان أصبت فمن اللّٰه وحده,
وان أخطأت فمن نفسي ومن الشيطان


Thank you for your attention
Blockchain is **NOT** hard, it is **different**