ĐẠI HỌC NGÂN HÀNG THÀNH PHỐ HỒ CHÍ MINH

Chapter 3

CONSENSUS PROTOCOL AND MINING

TP. HCM 2022

OVERVIEW

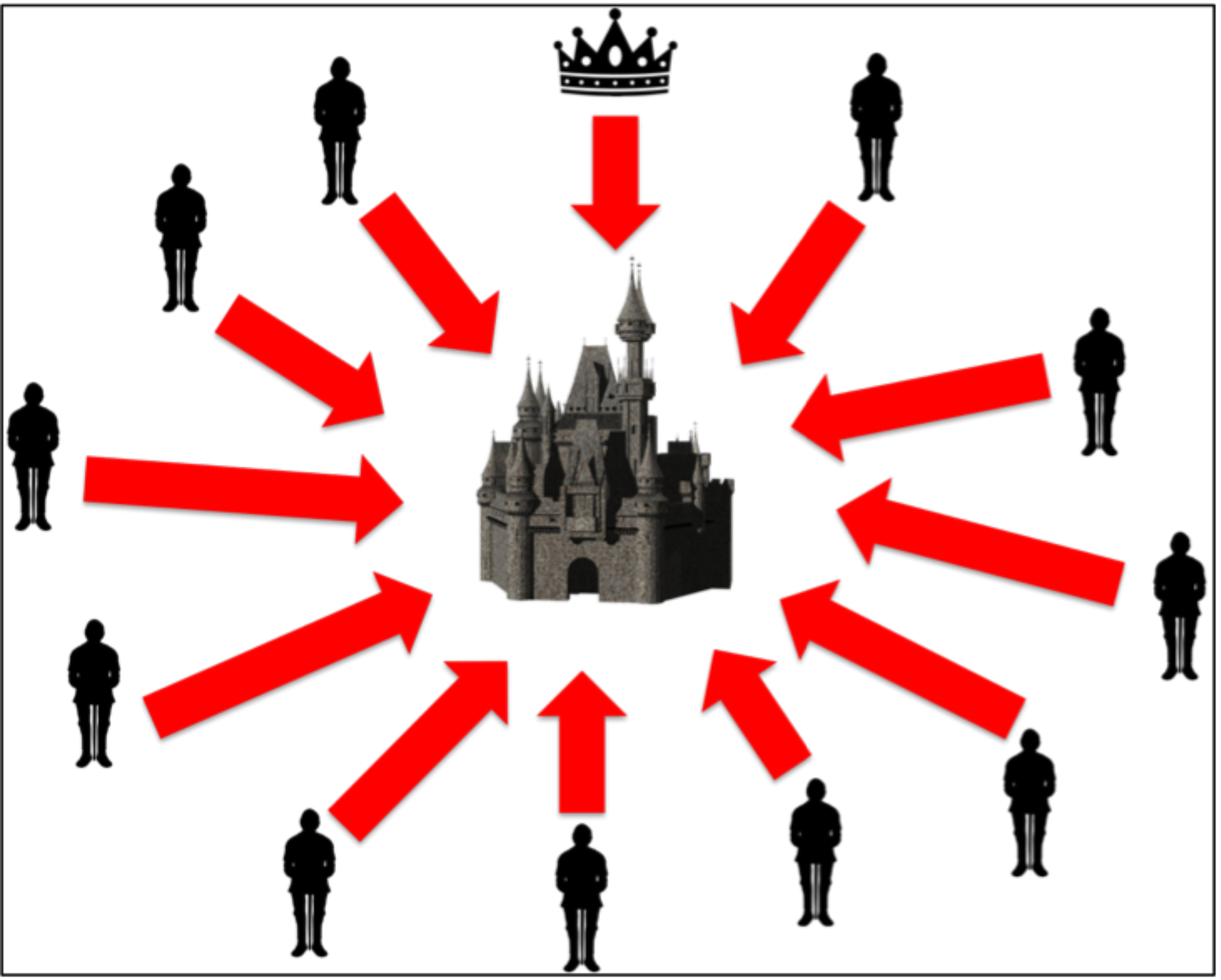
- The Byzantine Generals Problem
- Proof of Works
- Proof of Stakes
- Crypto currency mining

THE BYZANTINE GENERALS PROBLEM

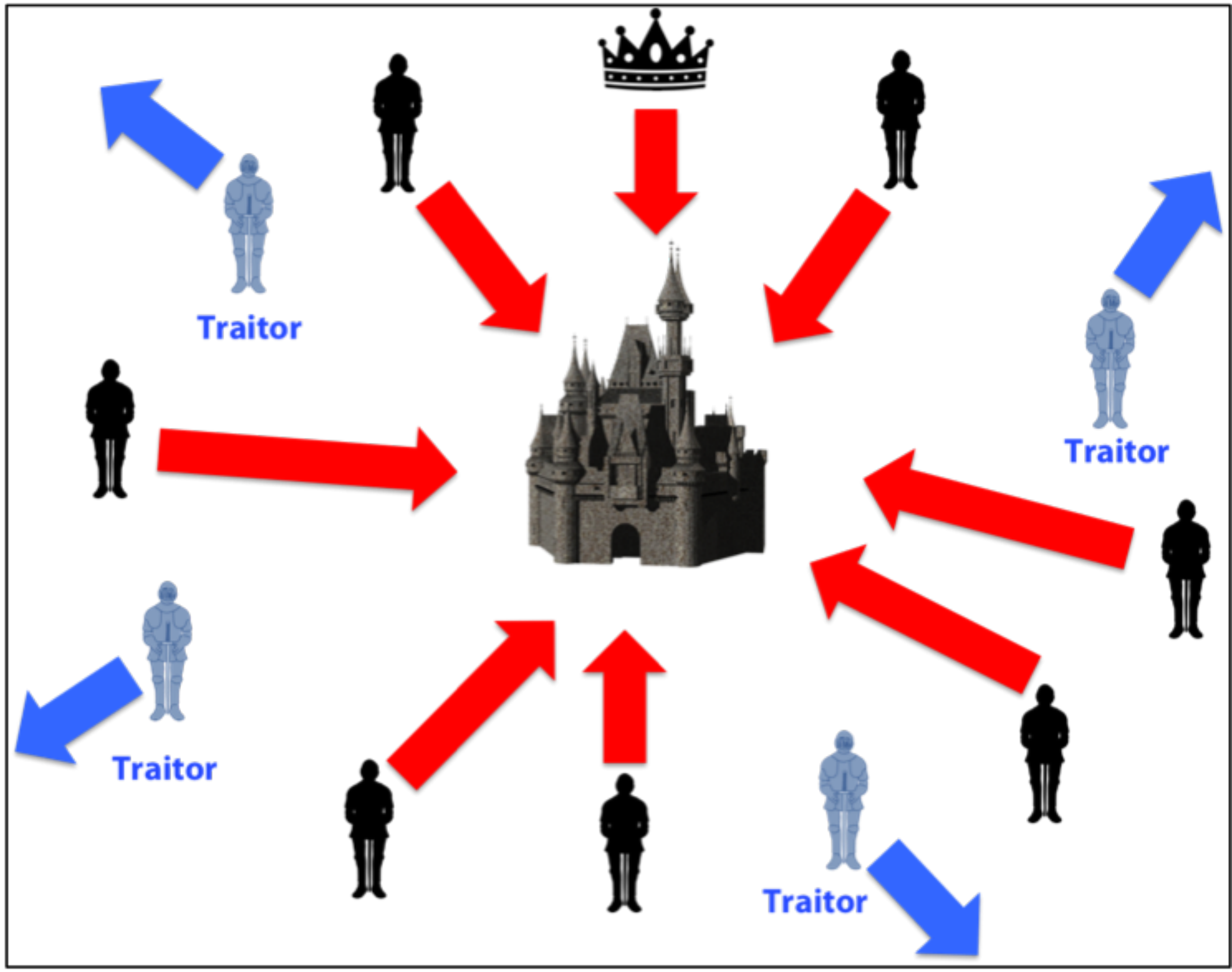
The abstract problem:

- Each division of Byzantine army is directed by its own general.
- There are n Generals, some of which are traitors.
- All armies are camped outside enemy castle, observing enemy.
- Communicate with each other by messengers.
- Requirements:
  - G1: All loyal generals decide upon the same plan of action
  - G2: A small number of traitors cannot cause the loyal generals to adopt a bad plan
- Note: We do not have to identify the traitors.

THE BYZANTINE GENERALS PROBLEM



Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

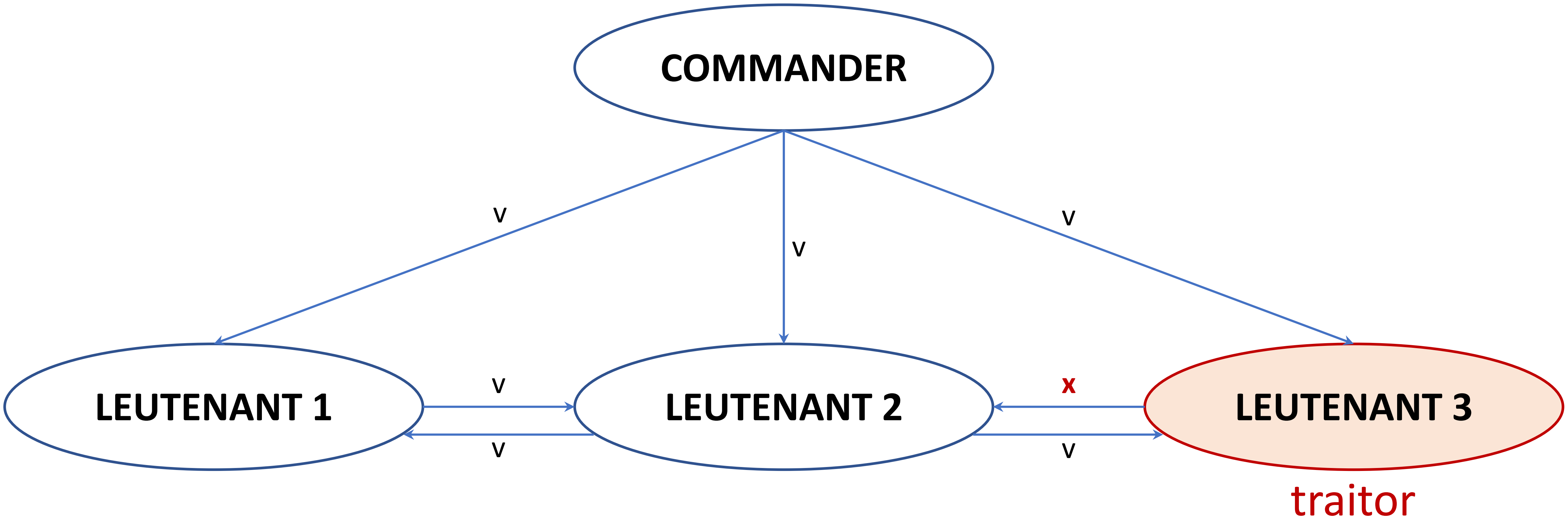
SOLUTION I: ORAL MESSAGES

A commanding general must send an order to his n-1 lieutenant generals such that:

- All loyal lieutenants obey the same order
- If the commanding general is loyal, then every loyal lieutenant obeys the order he sends

L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," ACM TOPLAS, vol. 4, pp. 382–401, July 1982.

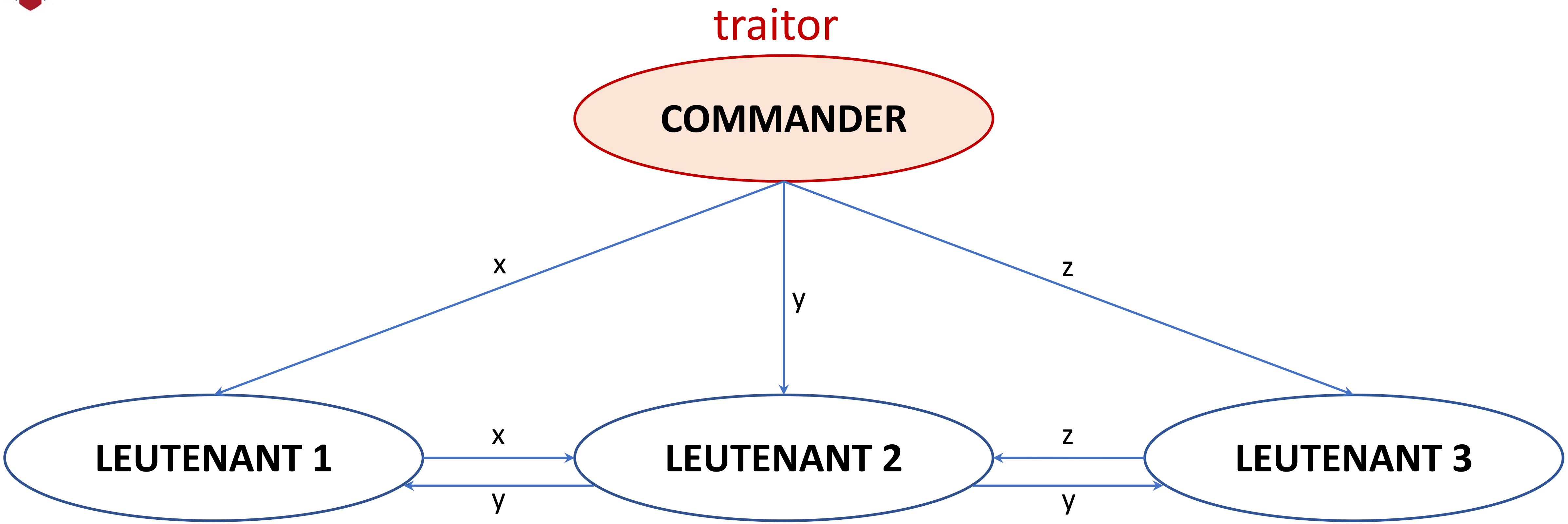
SOLUTION I: ORAL MESSAGES



Final decision = majority(v,v,x) = v

L. Lamport, R. Shostak, and M. Pease, “The Byzantine generals problem,” ACM TOPLAS, vol. 4, pp. 382–401, July 1982.

SOLUTION I: ORAL MESSAGES



Final decision = majority(x,y,z) = default decision (retreat)

L. Lamport, R. Shostak, and M. Pease, “The Byzantine generals problem,” ACM TOPLAS, vol. 4, pp. 382–401, July 1982.

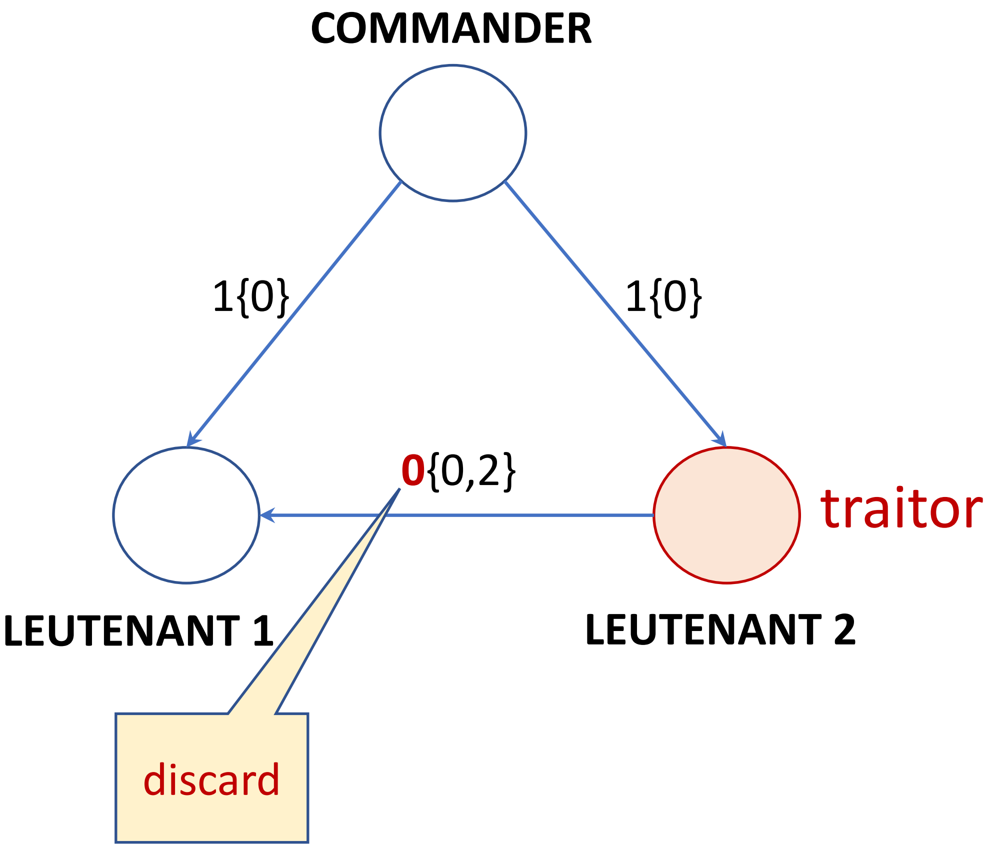
SOLUTION II: SIGNED MESSAGES

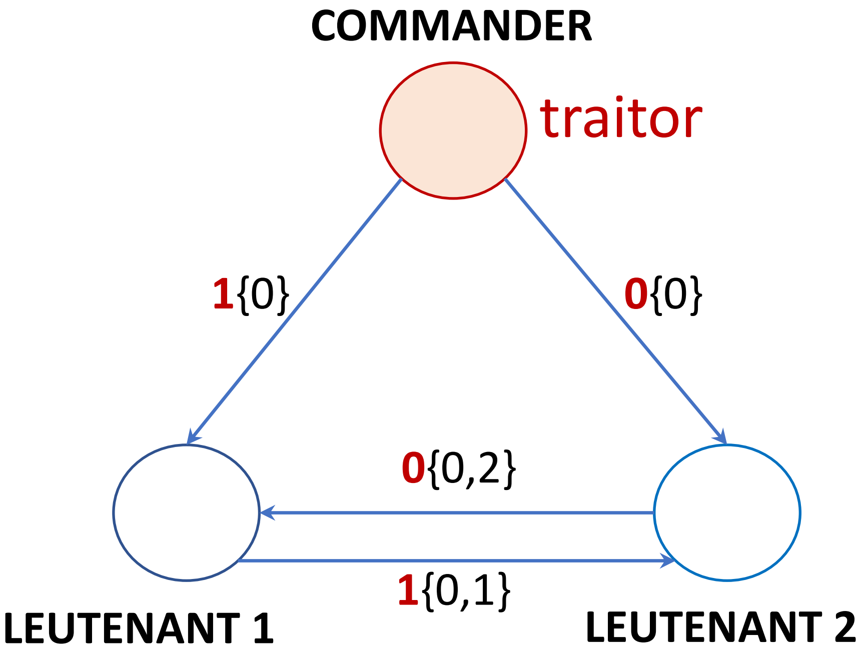
A signed message satisfies all the conditions of oral message, plus two extra conditions:

- Signature cannot be forged. Forged message are detected and discarded by loyal generals.
- Anyone can verify its authenticity of a signature.

Signed messages improve resilience.

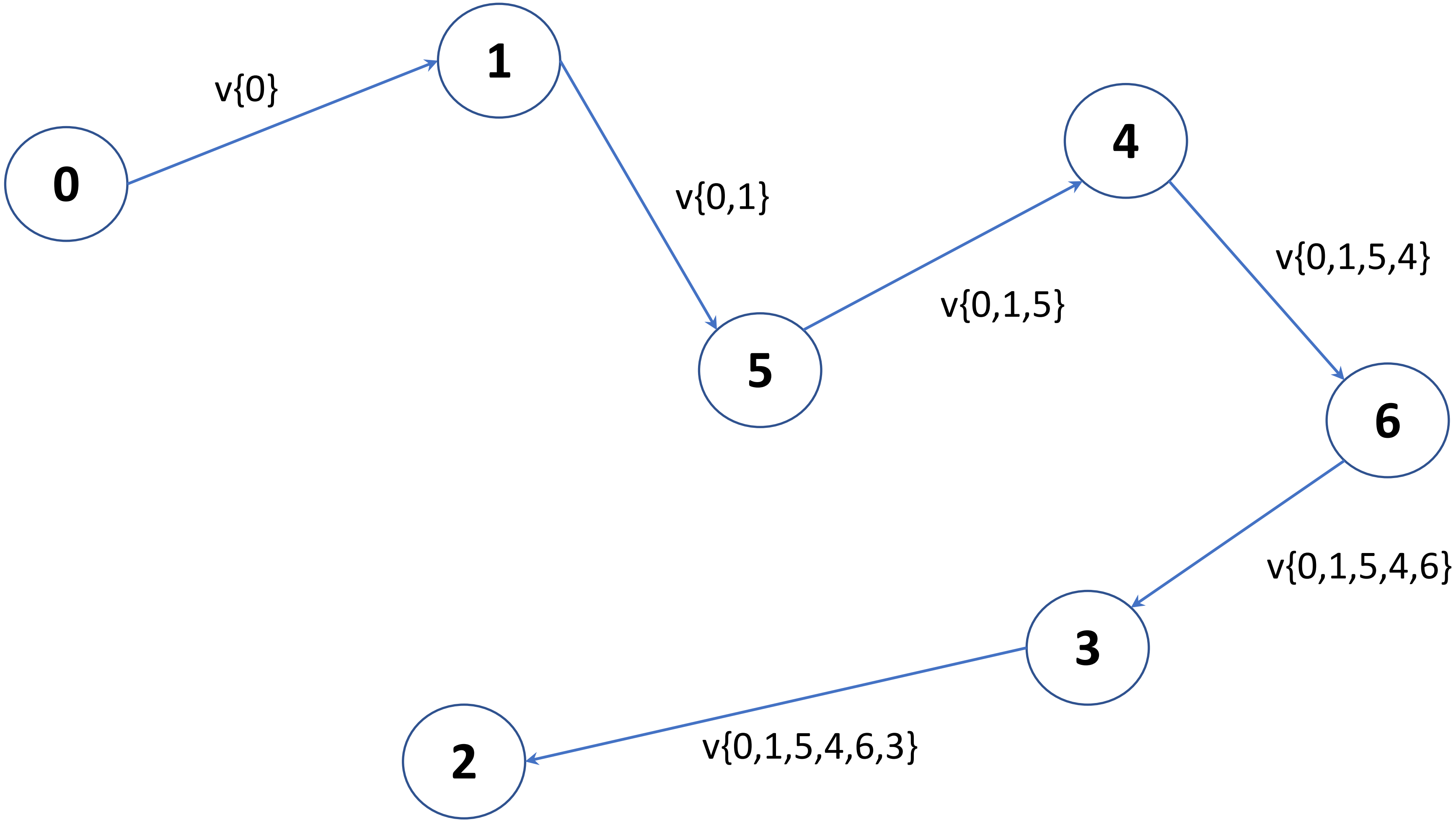
SOLUTION II: SIGNED MESSAGES



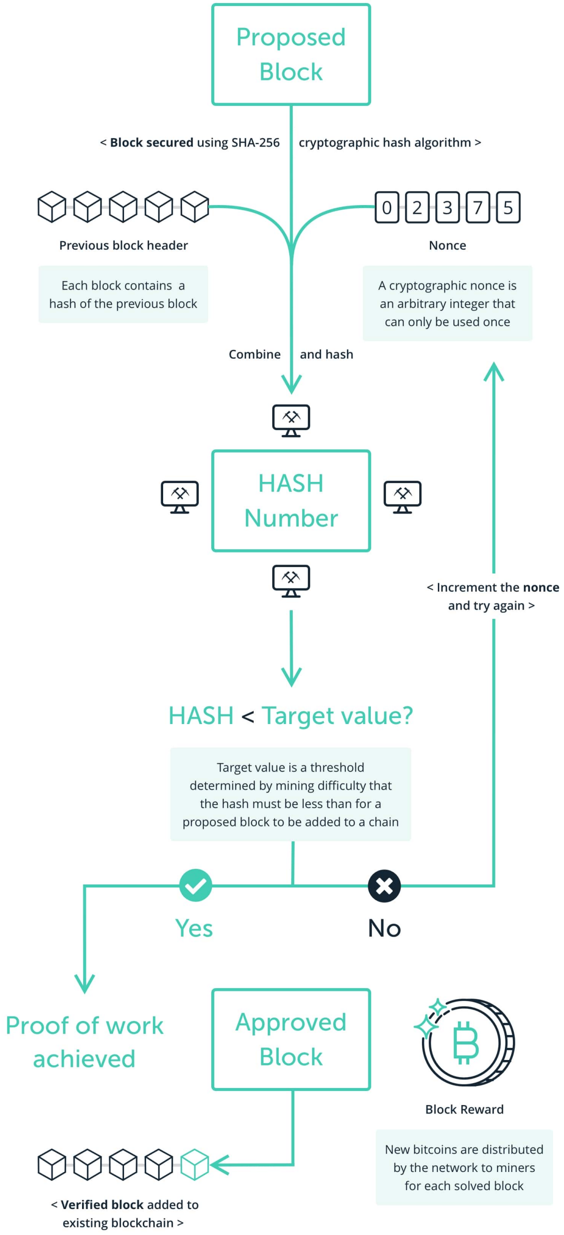


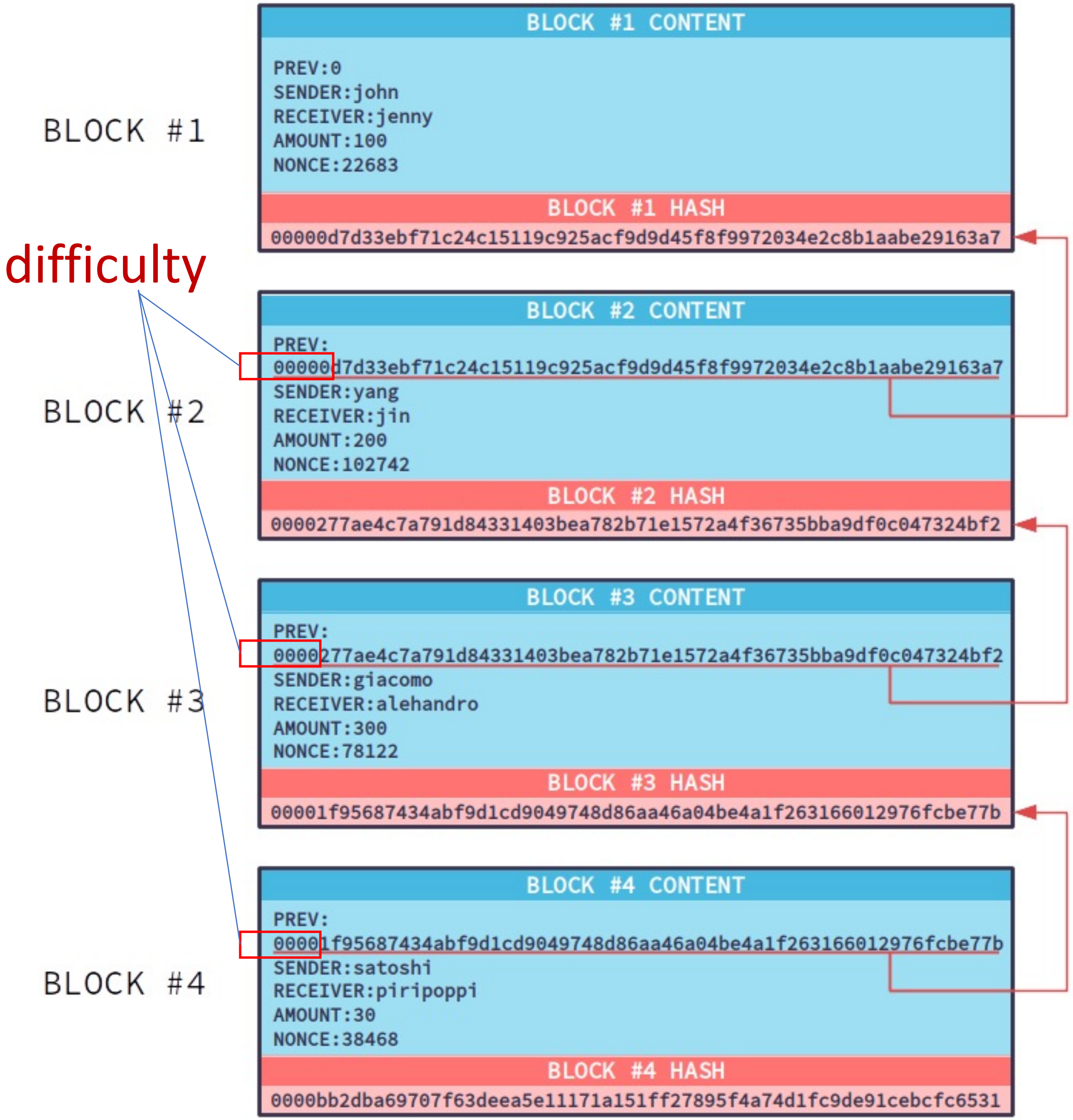
SOLUTION II: SIGNED MESSAGES

SIGNATURE PATH



BLOCKHAIN CONSENSUS – PROOF OF WORK


Proposed Block
< Block secured using SHA-256
cryptographic hash algorithm >
Previous block header
Each block contains a hash of the previous block
0 2 3 7 5
Nonce
A cryptographic nonce is an arbitrary integer that can only be used once
Combine
and hash
HASH Number
< Increment the nonce and try again >
HASH < Target value?
Target value is a threshold determined by mining difficulty that the hash must be less than for a proposed block to be added to a chain
Yes
No
Proof of work achieved
Approved Block
Block Reward
New bitcoins are distributed by the network to miners for each solved block
< Verified block added to existing blockchain >



BLOCK #1 CONTENT

PREV:0
SENDER:john
RECEIVER:jenny
AMOUNT:100
NONCE:22683

BLOCK #1 HASH

00000d7d33ebf71c24c15119c925acf9d9d45f8f9972034e2c8b1aabe29163a7

BLOCK #2 CONTENT

PREV:
00000d7d33ebf71c24c15119c925acf9d9d45f8f9972034e2c8b1aabe29163a7
SENDER:yang
RECEIVER:jin
AMOUNT:200
NONCE:102742

BLOCK #2 HASH

0000277ae4c7a791d84331403bea782b71e1572a4f36735bba9df0c047324bf2

BLOCK #3 CONTENT

PREV:
0000277ae4c7a791d84331403bea782b71e1572a4f36735bba9df0c047324bf2
SENDER:giacomo
RECEIVER:alehandro
AMOUNT:300
NONCE:78122

BLOCK #3 HASH

00001f95687434abf9d1cd9049748d86aa46a04be4a1f263166012976fcbe77b

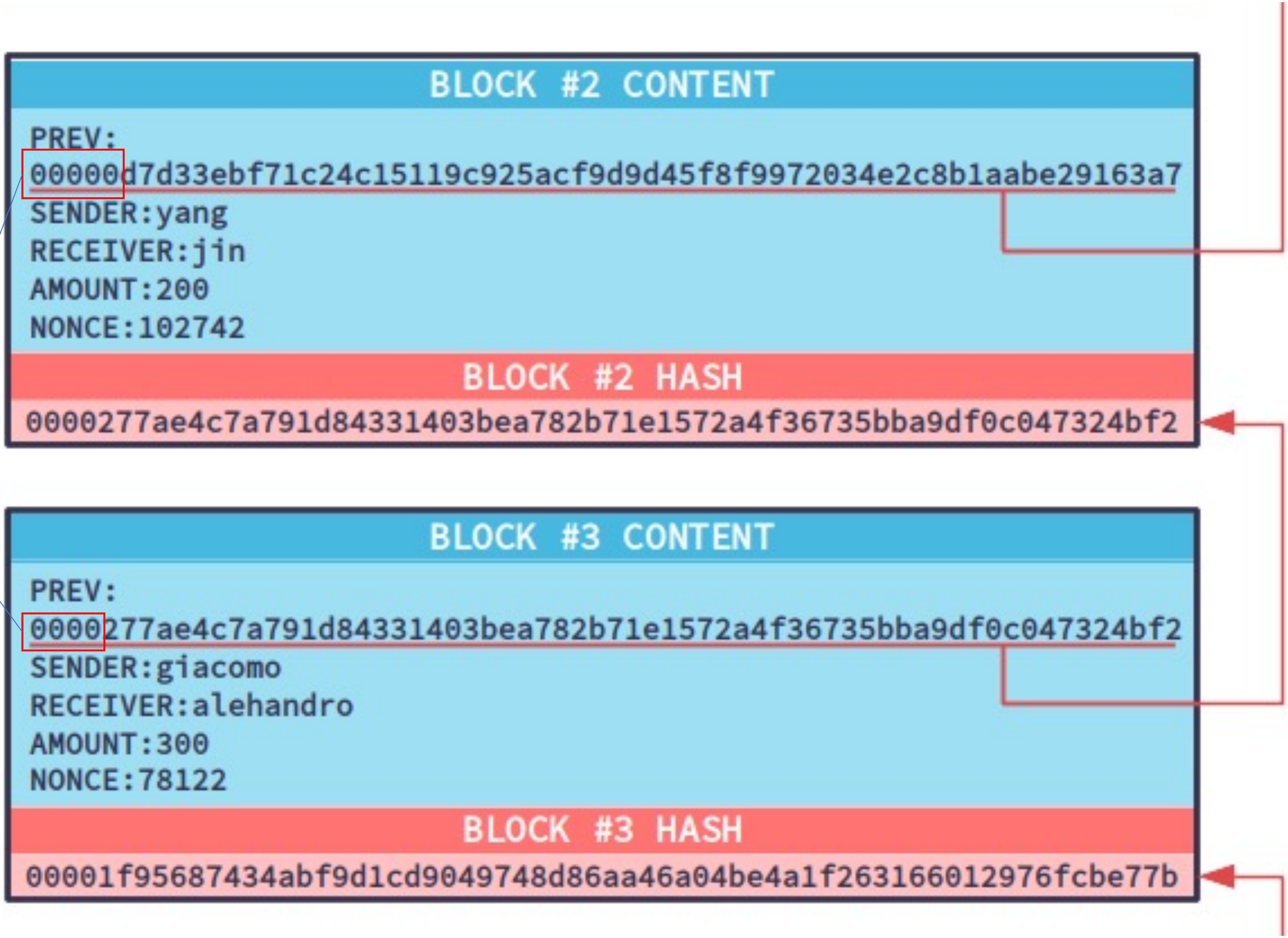
BLOCK #4 CONTENT

PREV:
00001f95687434abf9d1cd9049748d86aa46a04be4a1f263166012976fcbe77b
SENDER:satoshi
RECEIVER:piripoppi
AMOUNT:30
NONCE:38468

BLOCK #4 HASH

0000bb2dba69707f63deea5e11171a151ff27895f4a74d1fc9de91cebcfc6531

BLOCKHAIN CONSENSUS – PROOF OF WORK



BLOCK #2 CONTENT

PREV:
00000d7d33ebf71c24c15119c925acf9d9d45f8f9972034e2c8b1aabe29163a7
SENDER:yang
RECEIVER:jin
AMOUNT:200
NONCE:102742

BLOCK #2 HASH

0000277ae4c7a791d84331403bea782b71e1572a4f36735bba9df0c047324bf2

BLOCK #3 CONTENT

PREV:
0000277ae4c7a791d84331403bea782b71e1572a4f36735bba9df0c047324bf2
SENDER:giacomo
RECEIVER:alehandro
AMOUNT:300
NONCE:78122

BLOCK #3 HASH

00001f95687434abf9d1cd9049748d86aa46a04be4a1f263166012976fcbe77b

difficulty

BLOCKHAIN CONSENSUS – PROOF OF WORK

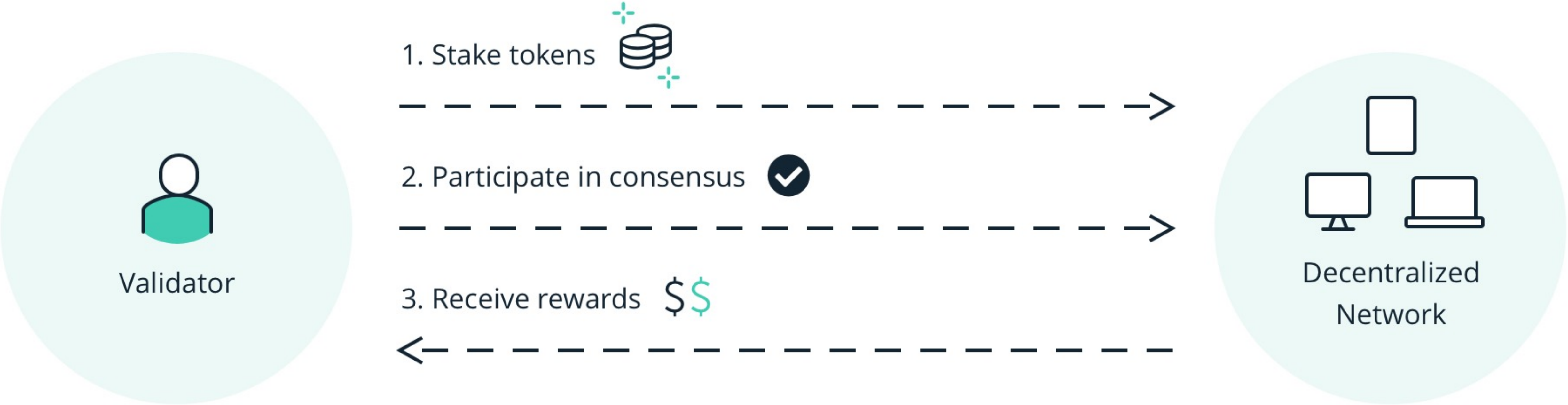
Pros

- ✓ Better ability to be decentralized
- ✓ Better security

Cons

- ✗ Slower transaction speeds
- ✗ Higher costs to validate transactions
- ✗ Higher energy consumption

BLOCKHAIN CONSENSUS – PROOF OF STAKE



BLOCKHAIN CONSENSUS – PROOF OF STAKE

BLOCKHAIN CONSENSUS – PROOF OF STAKE

Pros

- ✓ Less energy consumption
- ✓ Financial opportunities
- ✓ Faster transaction speeds

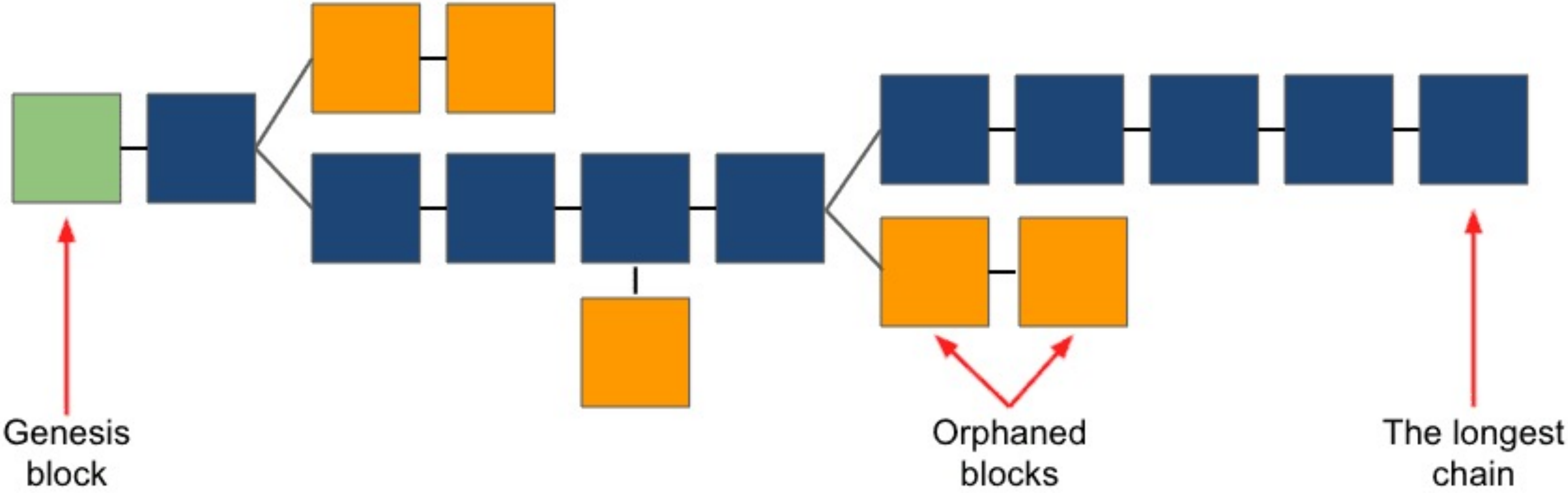
Cons

- ✗ Harder to truly decentralize the network
- ✗ Less security than PoW

BLOCKHAIN CONSENSUS

Proof of Work	vs	Proof of Stake
The first miner who solves the asymmetric puzzle is selected. Competition between miners to solve the puzzle.		Using deterministic selection process. Competition between miners to be selected.
Specialized equipment to optimize processing power.		Standard server grade unit is usually (more than) enough.
Initial investment to buy the hardware.		Initial investment to buy the stake and build the reputation.
High energy consumption		Standard energy consumption

BLOCKHAIN CONSENSUS



BITCOIN PROOF OF WORK DIFFICULTY

- Targets 10 minute average block generation time
- Defined by the # of leading zeros Hash output requires to solve PoW
- Adjusts every 2016 blocks - about every two weeks
- Currently, > 18 leading zeros (out of 64 hexadecimal characters)

- Block 749,952 (08/26/2022)- 19 leading zeros

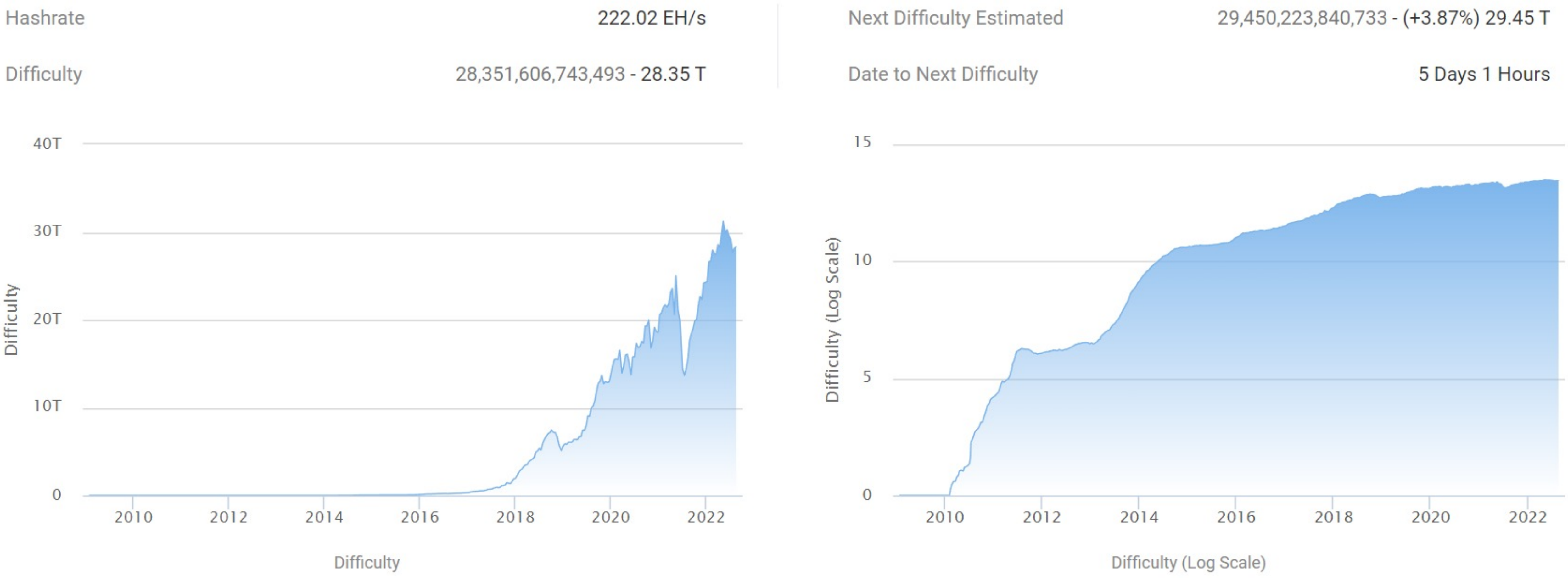
00000000000000000007edd9a88903ad4f948bf3def71a520635ec769065429a

- Genesis Block (1/3/09) – **10** leading zeros, though only required **8**

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

https://www.blockchain.com/

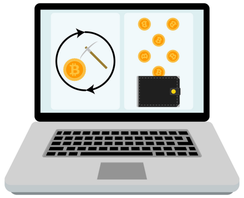
BITCOIN PROOF OF WORK DIFFICULTY



Hashrate	222.02 EH/s	Next Difficulty Estimated	29,450,223,840,733 - (+3.87%) 29.45 T
Difficulty	28,351,606,743,493 - 28.35 T	Date to Next Difficulty	5 Days 1 Hours

https://btc.com/stats/diff

EVOLUTION OF BITCOIN MINING

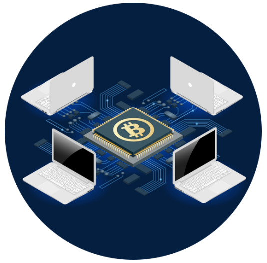


2009

CPU

GPU

2010

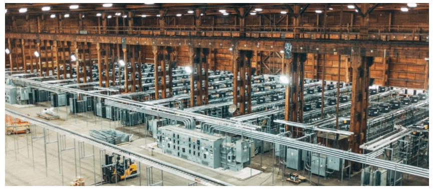


2010

Mining pools

ASIC

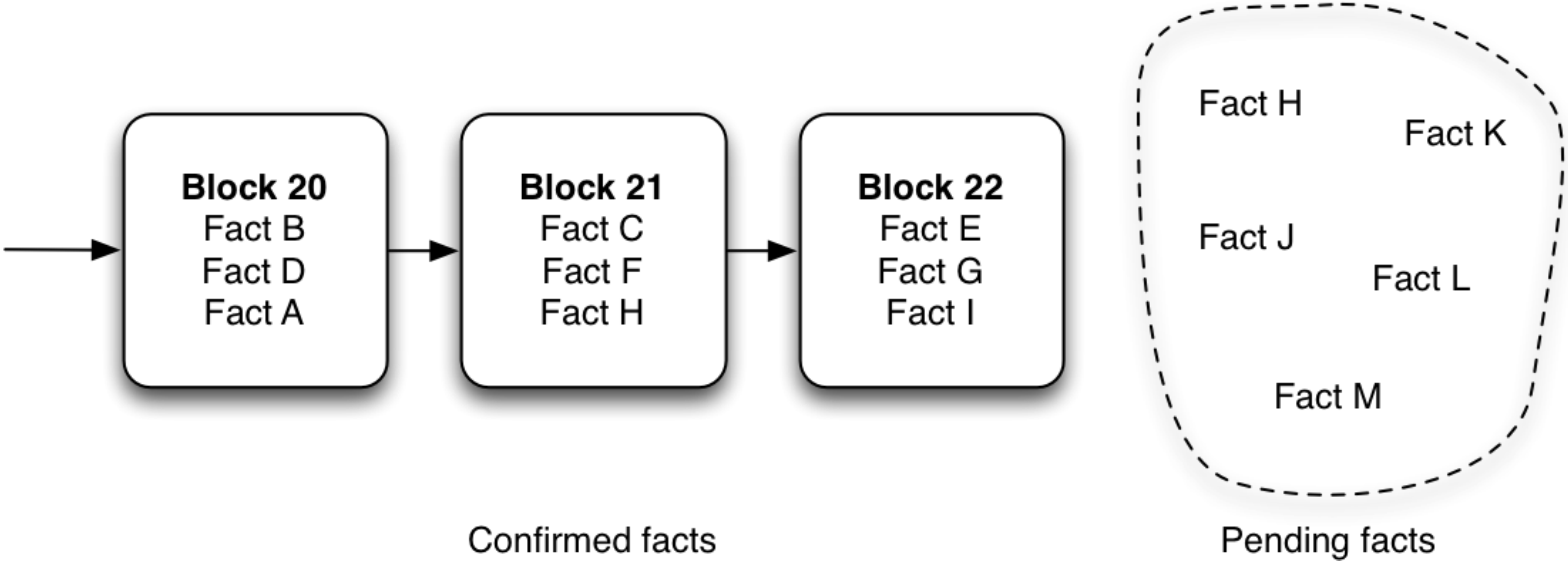
2013



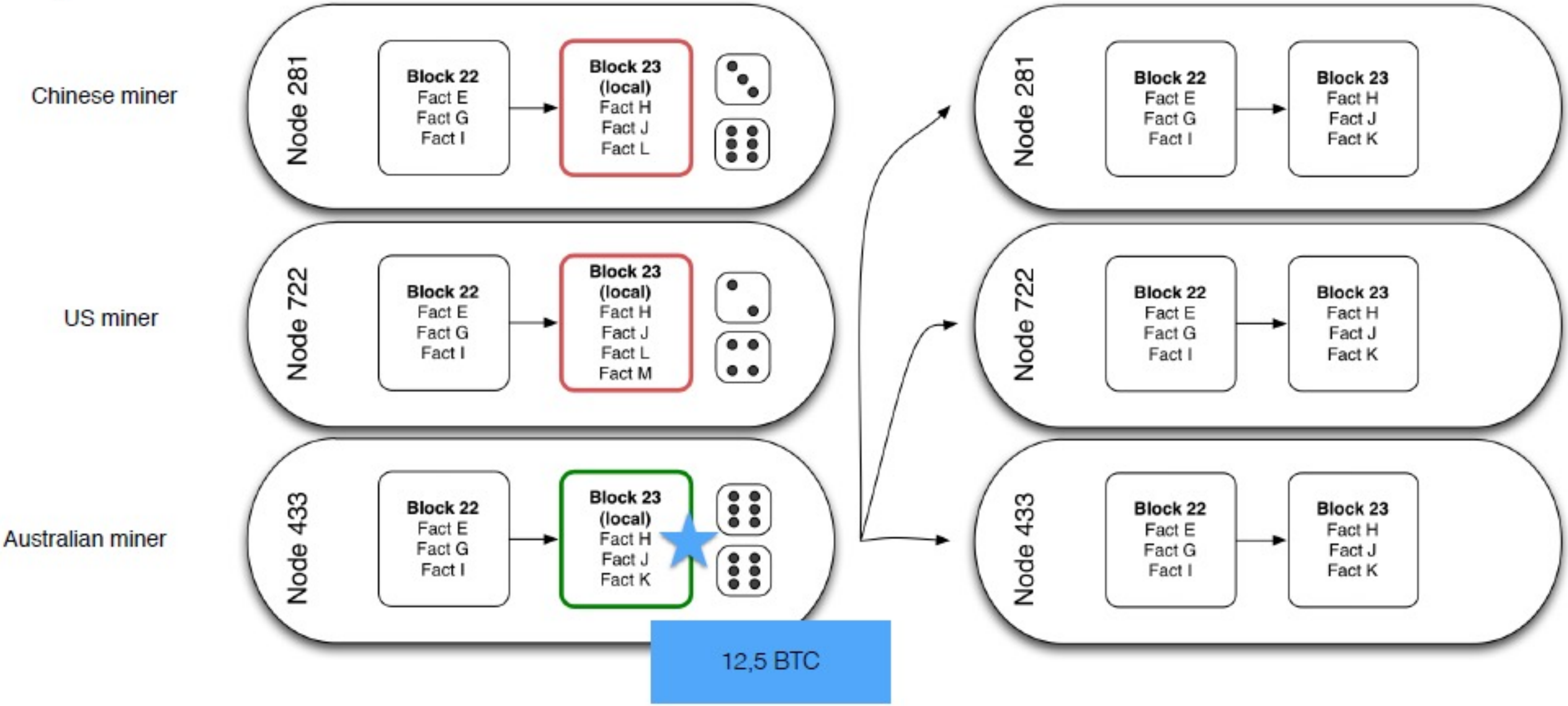
2014

Mining farms

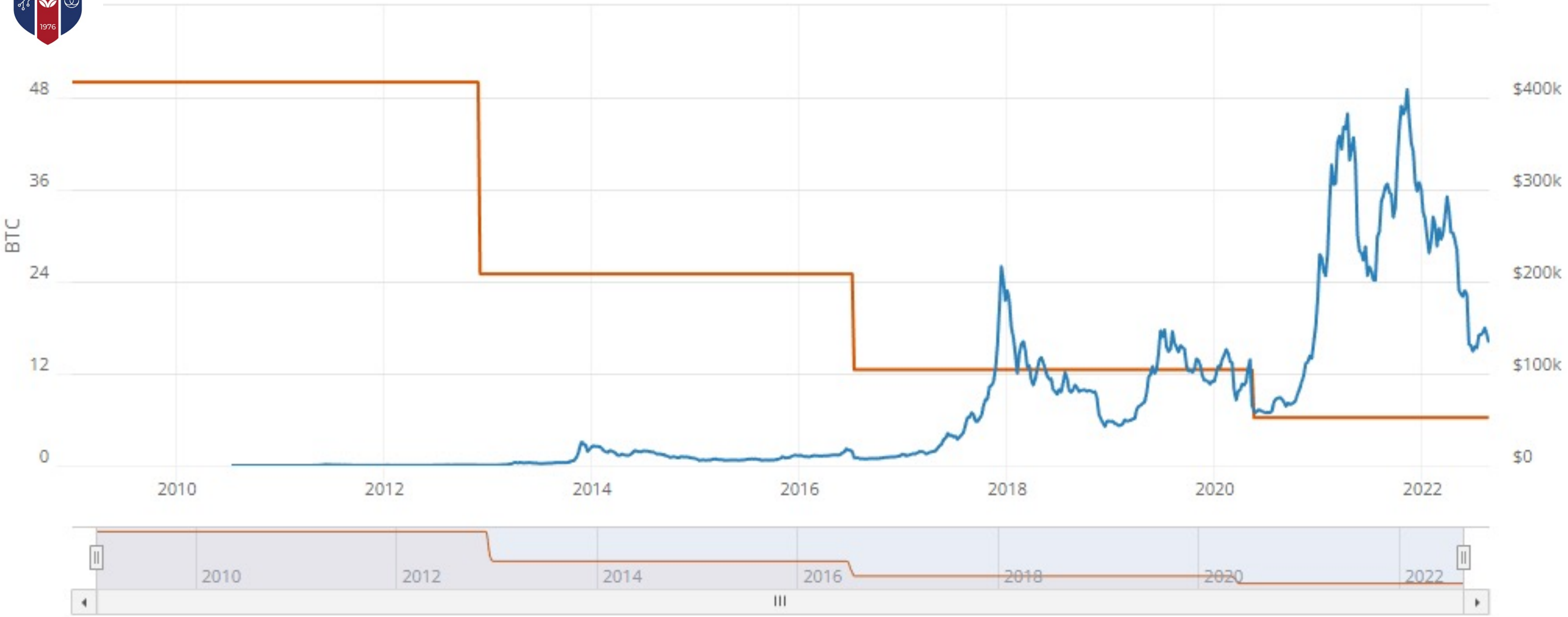
BITCOIN MINING



BITCOIN MINING



BITCOIN MINING REWARDS



Starts at **50 BTC / mined block**

Current: **6.25 BTC / mined block**

Halves every **210,000** blocks

BITCOIN NETWORK

- **Full Nodes** – Store full Blockchain & able to Validate all Transactions
- **Pruning Nodes** – Prune transactions after validation and aging
- **Lightweight Nodes** - Simplified Payment Verification (SPV) nodes – Store Blockchain Headers only
- **Miners** – Performs Proof of Work & Create new Blocks - Do not need to be a Full Node Mining Pool Operators
- **Wallets** – Store, View, Send and Receive Transactions & Create Key Pairs
- **Mempool** – Pool of unconfirmed (yet validated) Transactions

READINGS

1. *Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. Communications of the ACM, 60(12), 36-45. https://doi.org/10.1145/3132259*
2. *Ethereum white paper*

DISCUSSION