



Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari



Grading: Relative



Quizzes (n-1 policy): 10%



Mid-1: 15%



Mid-2: 15%



Final Exam: 45%



Project: 6%



Assignments: 4%



Class Activities/Homework: 5%



Programming
Languages:

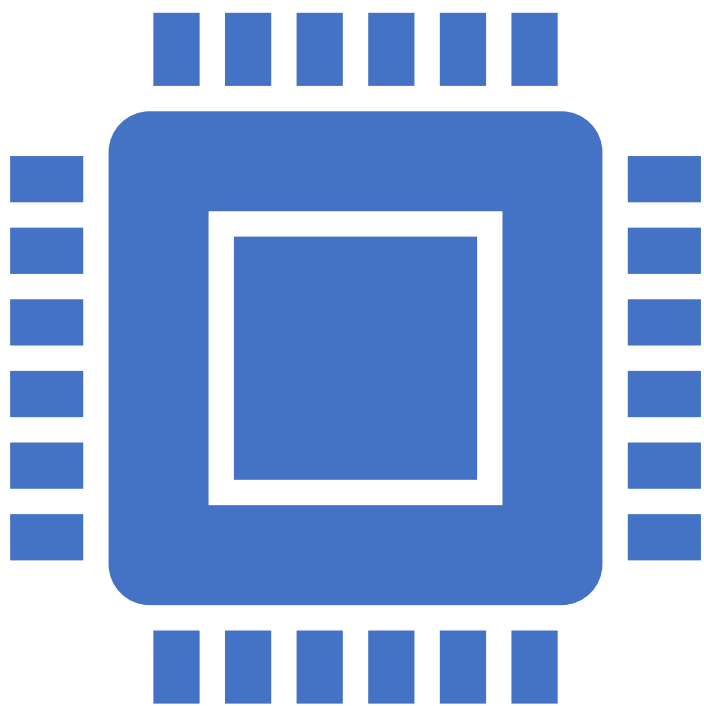


Go Language in Assignment 1

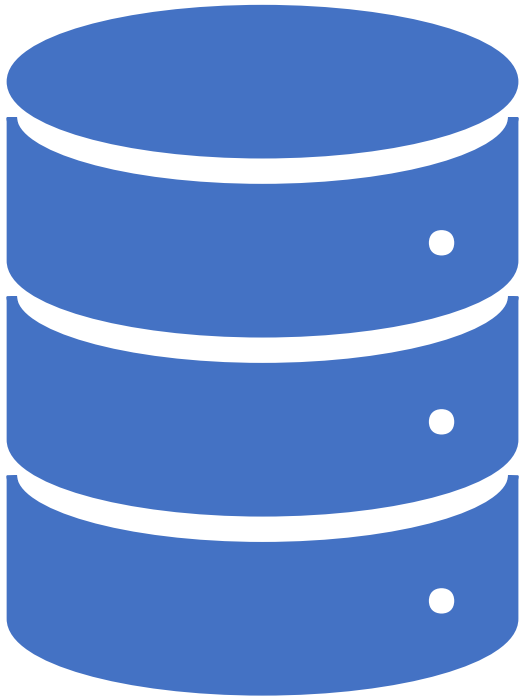
Solidity in Assignment 2, 3 and Project



What is Blockchain?



Why we need new technology?

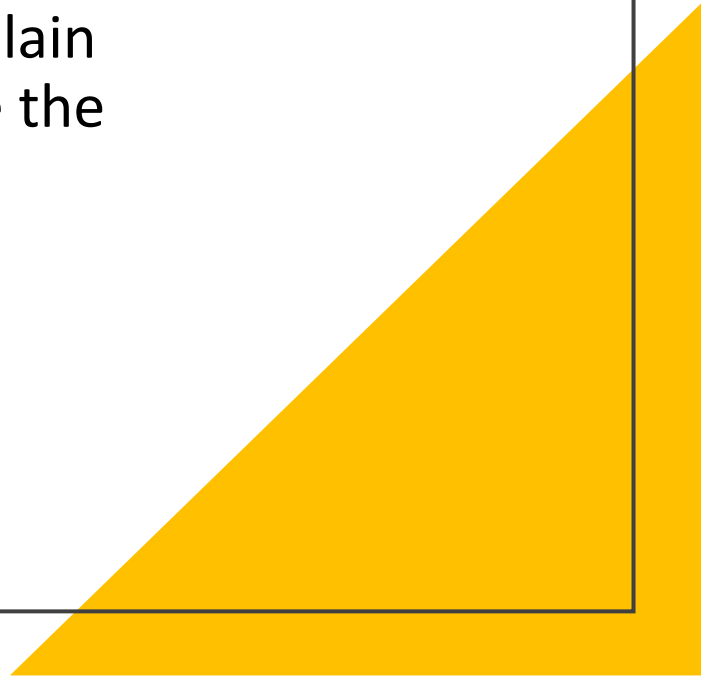


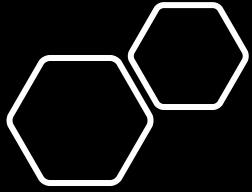
Let's talk about
traditional databases

CA-001 (Group of 2)

Name a system in which you want to use blockchain technology instead of centralised databases for storing data? Also explain how decentralized technology like Blockchain will improve the system's security.

Submission: Handwritten with roll numbers of both the students.





What is a Blockchain?

- Comparison with traditional Database
- Why we need new technology?
- Definition:
 - ❑ Distributed/Decentralized Ledger Technology

A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography

Block in Blockchain

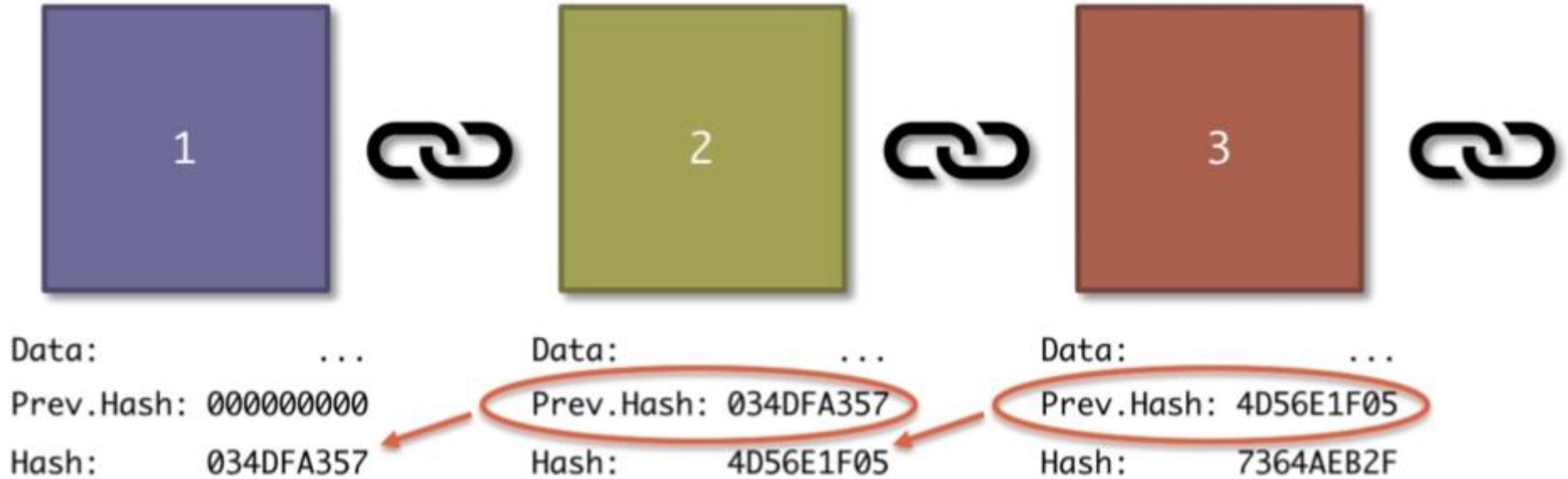
Information that a single block contains:

- Data e.g "Hello World"
- Previous Hash
- Hash - fingerprint of the block

First block is called Genesis Block

- Doesn't have a Previous hash

GENESIS BLOCK



Blockchain

Understanding SHA256 Hash:

- Different people have different fingerprints
- Fingerprint of a file is called a SHA256 Hash
- Developed by the NSA
- SHA - Secure Hash Algorithm
- 256 - number of bits it takes in memory - 64 characters long
- A file will always have the same hash
- If we change even one character, the whole hash will change
- **Requirements of a successful Hash algorithm**
 - One-way - you cannot restore or reverse engineer the document
 - Deterministic - get the same result every time
 - Fast computation
 - Avalanche effect - Even a single bit of data would result in an absolutely different hash
 - Must withstand collisions - Creating/altering documents to have the same Hash should not be possible

Immutable Ledger - 1

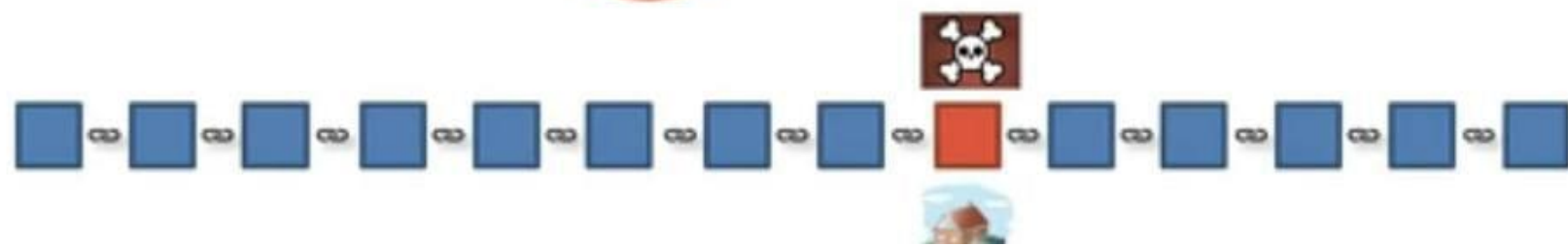
- Traditionally, you get a deed for every transaction (purchase of house)
 - Use of books, where records are kept
 - Can be altered or destroyed
- Blockchain prevents alteration of data
- Traditional ledgers are unreliable
- World Bank estimates that 70% of the population does not have entitlement to their properties.



Traditional Ledger



Blockchain



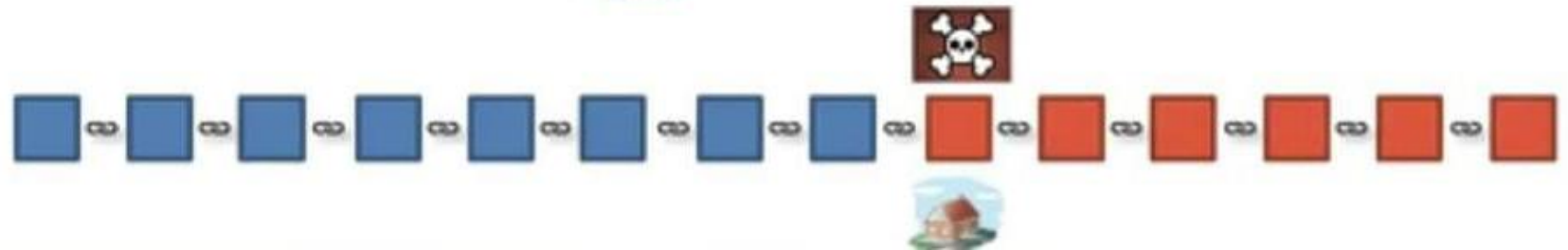
Immutable Ledger - 2



Traditional Ledger



Blockchain

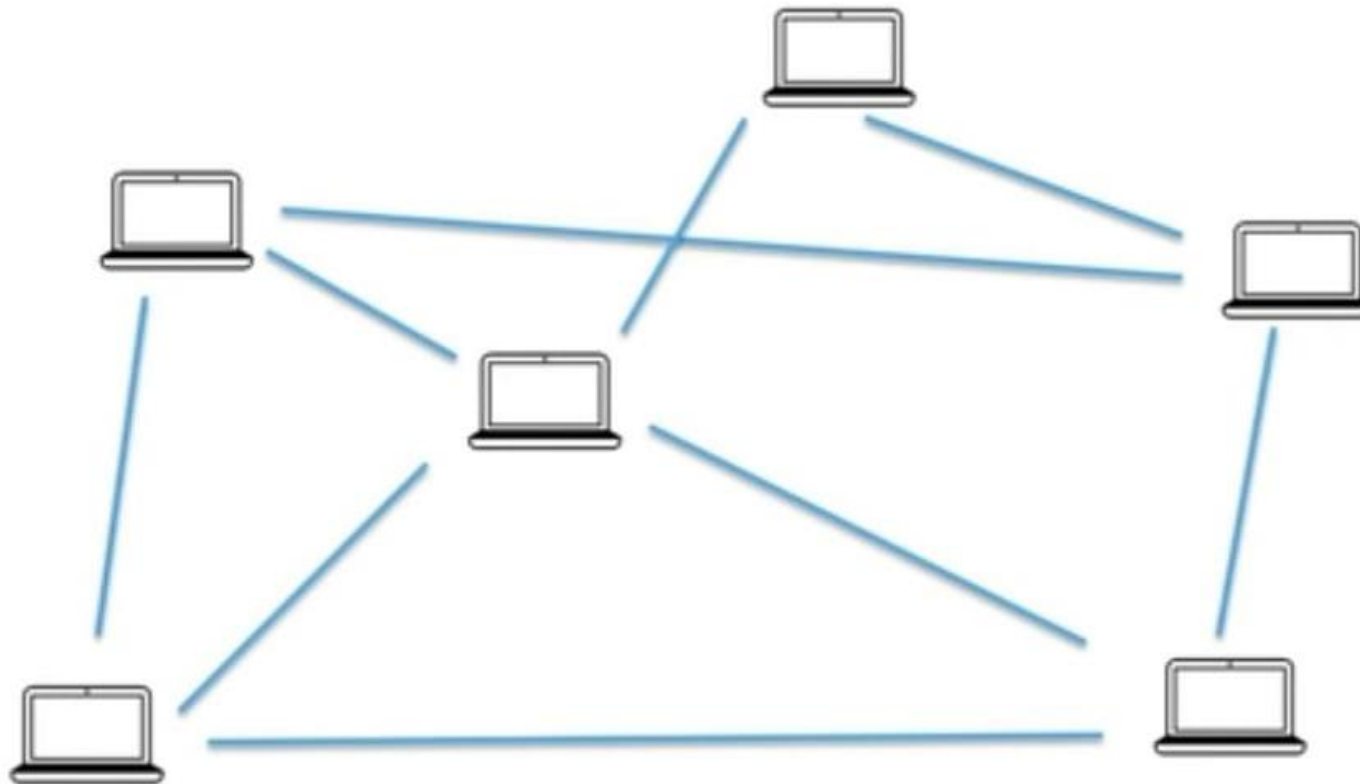


Immutable Ledger – Forge the Blockchain



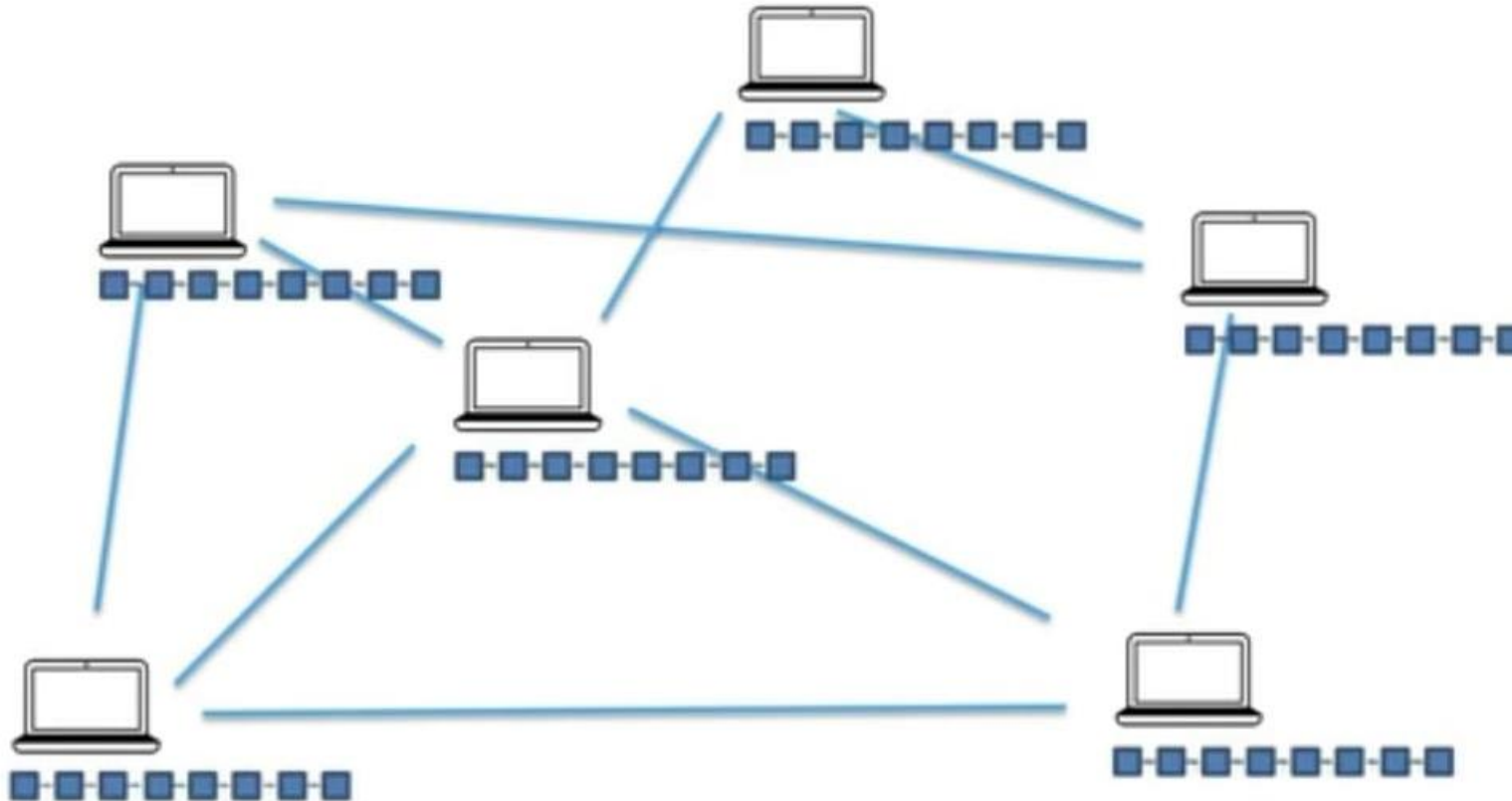
Distributed P2P Network

Peer-to-Peer Network

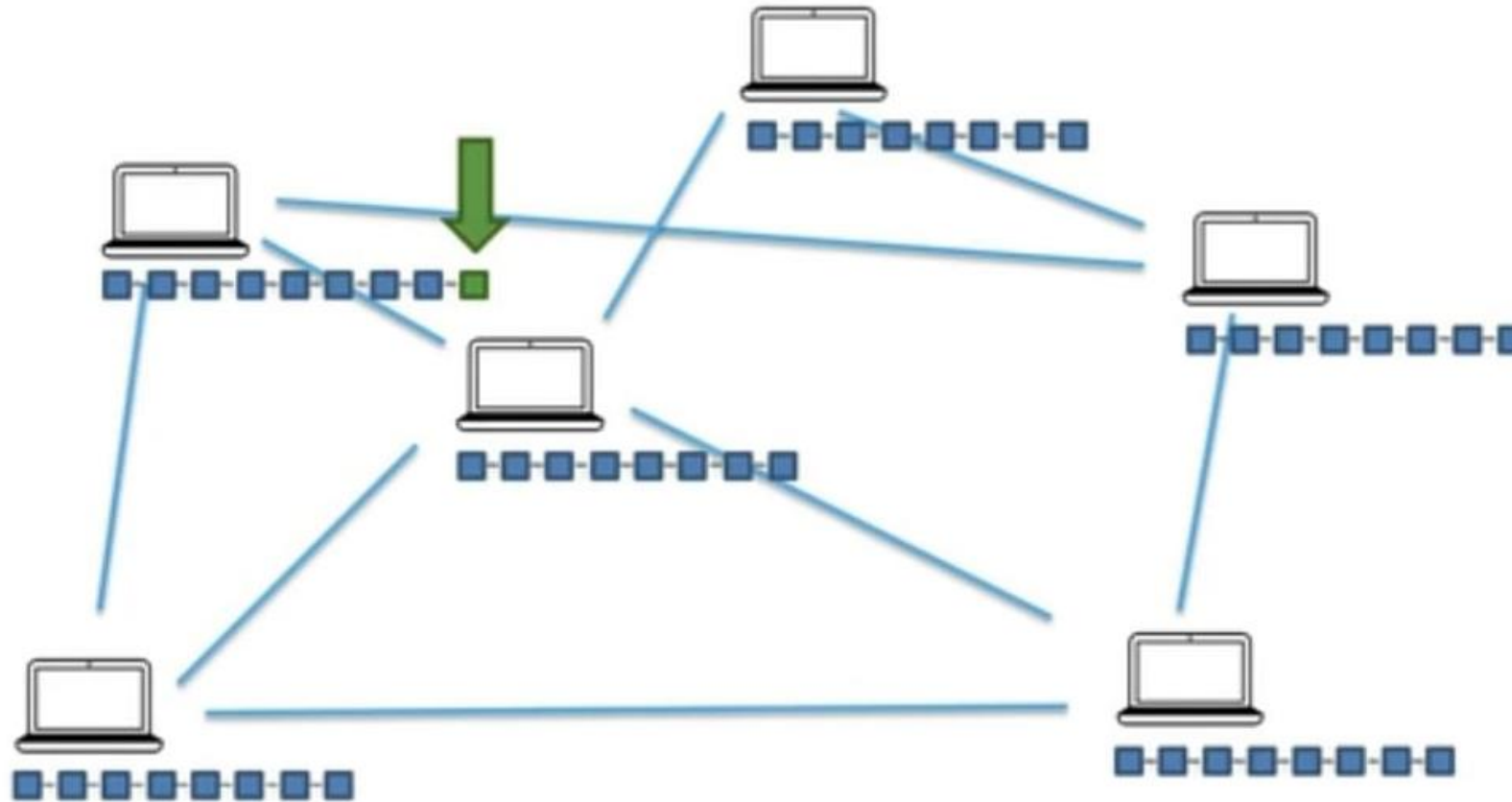


Anonymity: No real identity

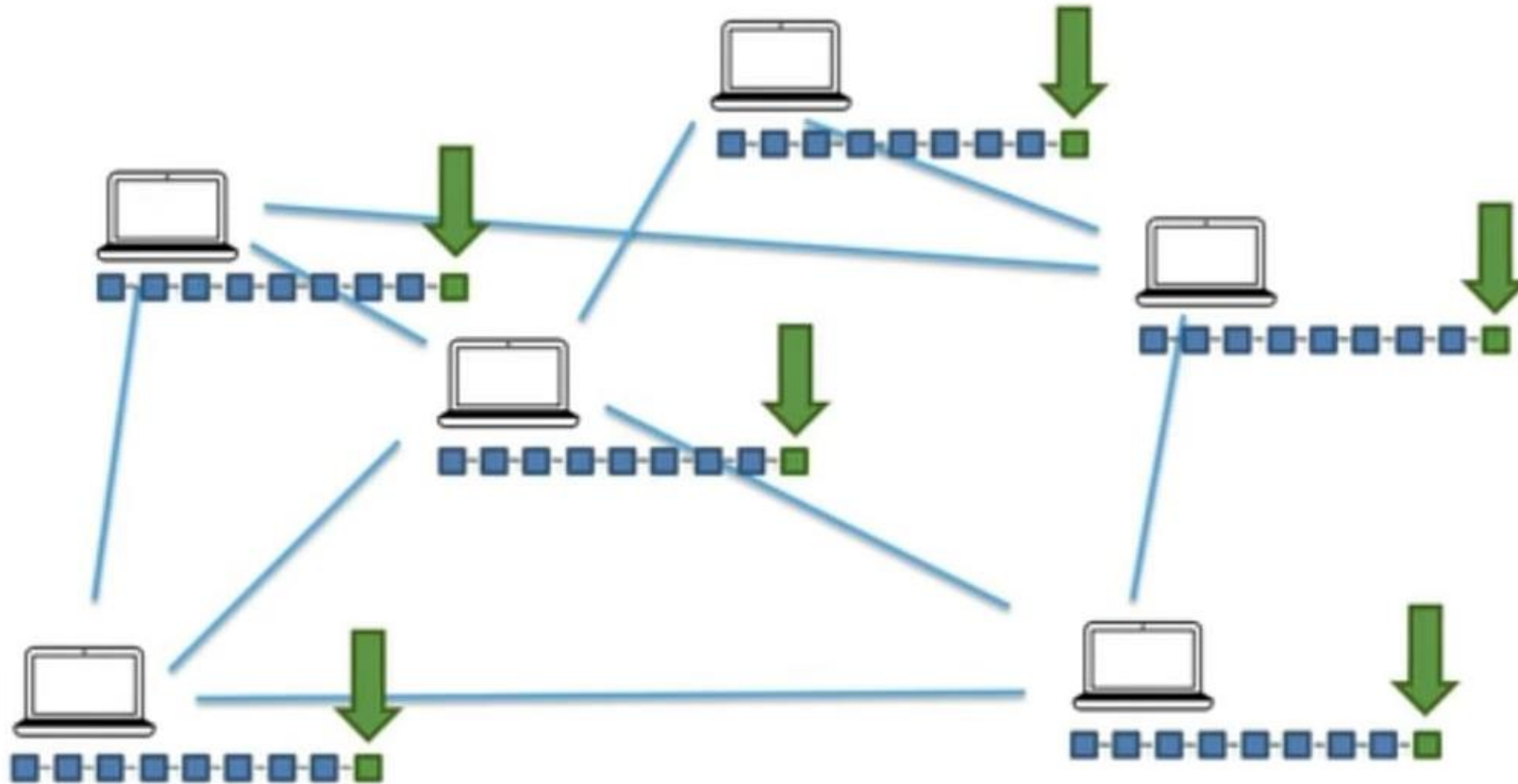
Each Node has a copy of Blockchain



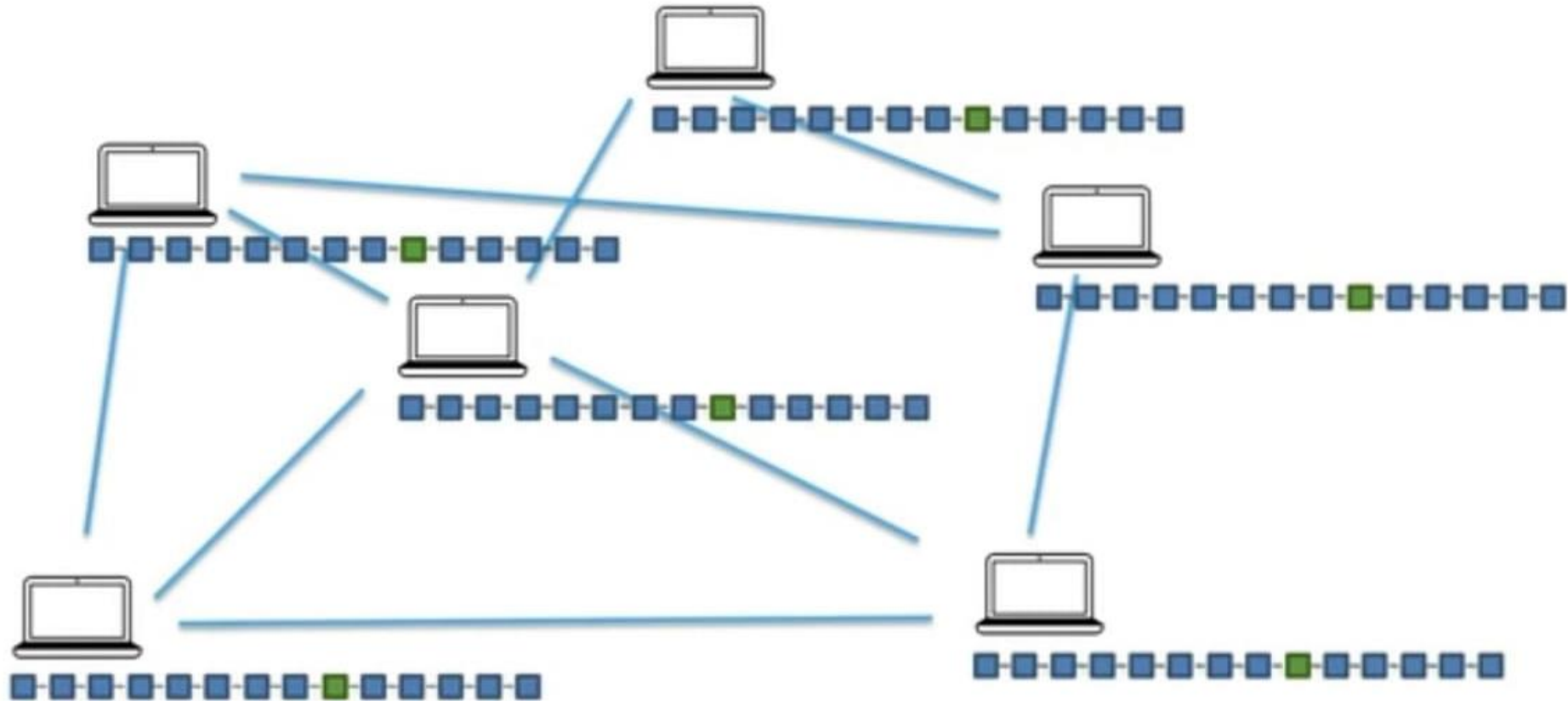
If a block is added to a Blockchain



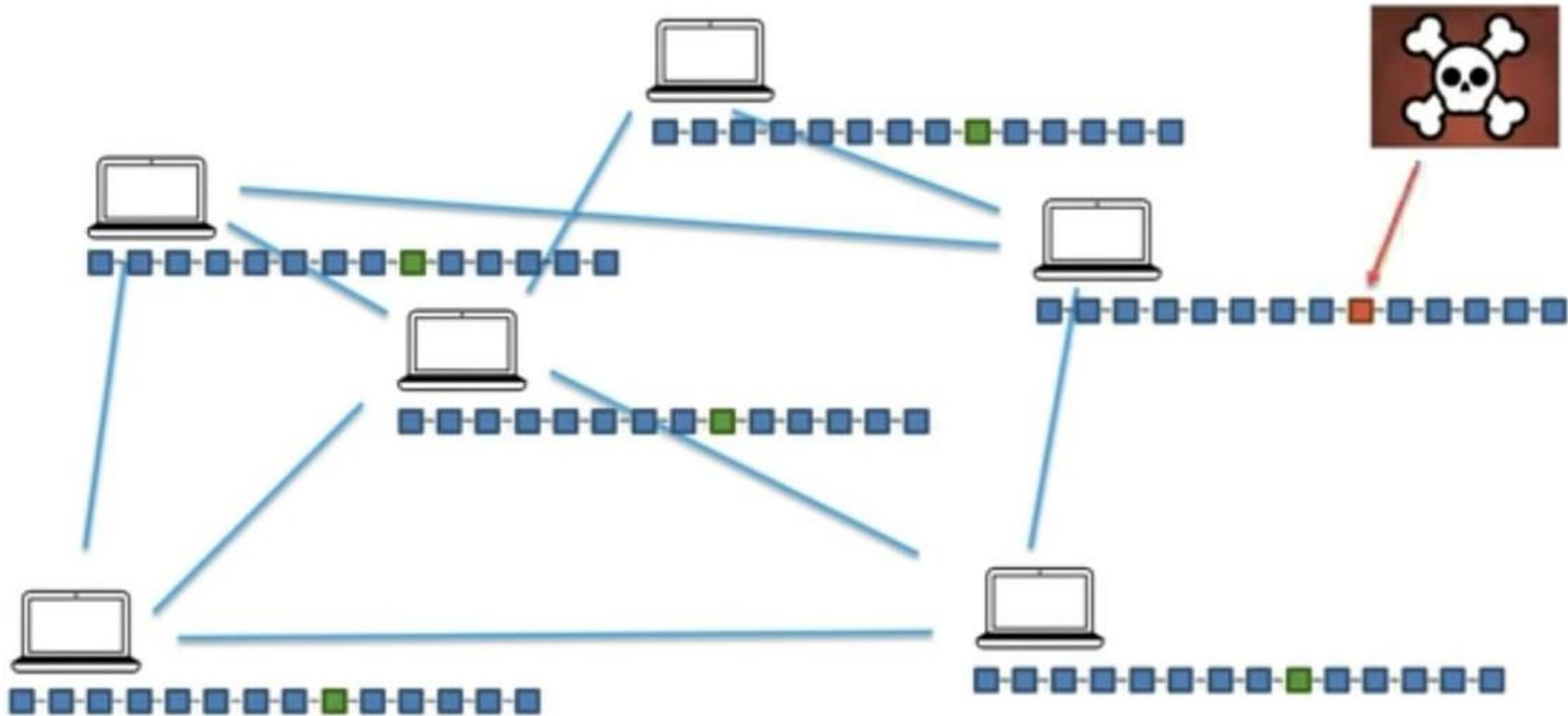
Whole network must update it's copy



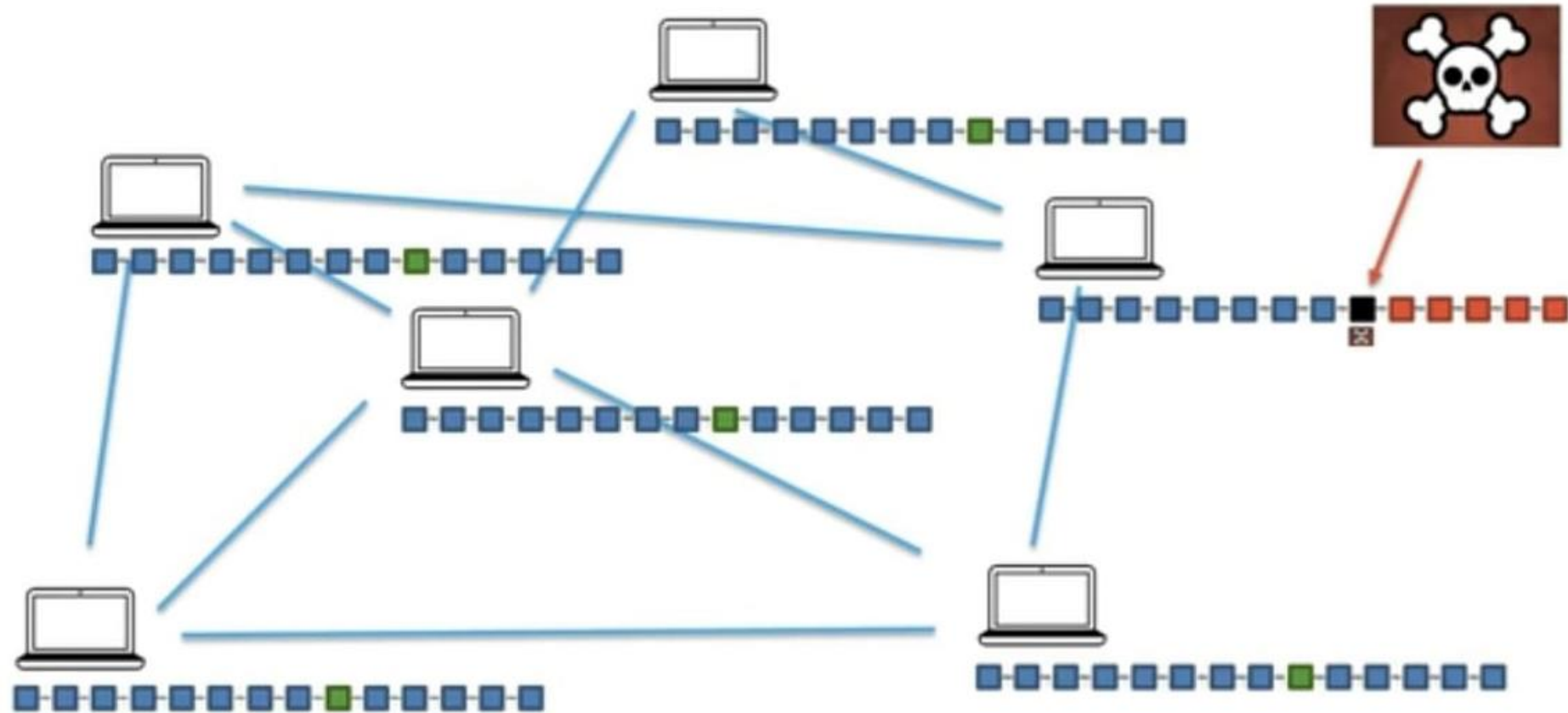
With the passage of time, more and more blocks are being added



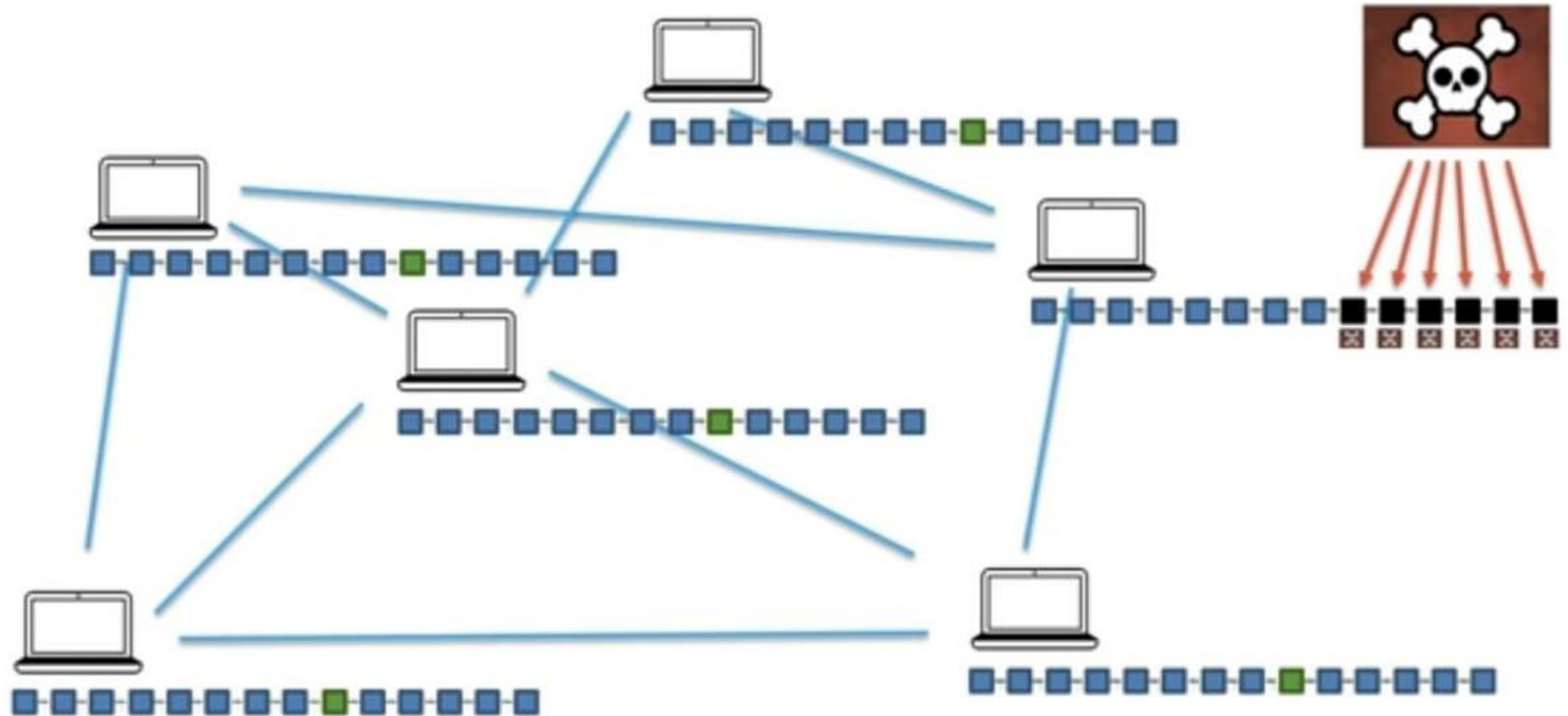
Someone attacking on blockchain through the network node



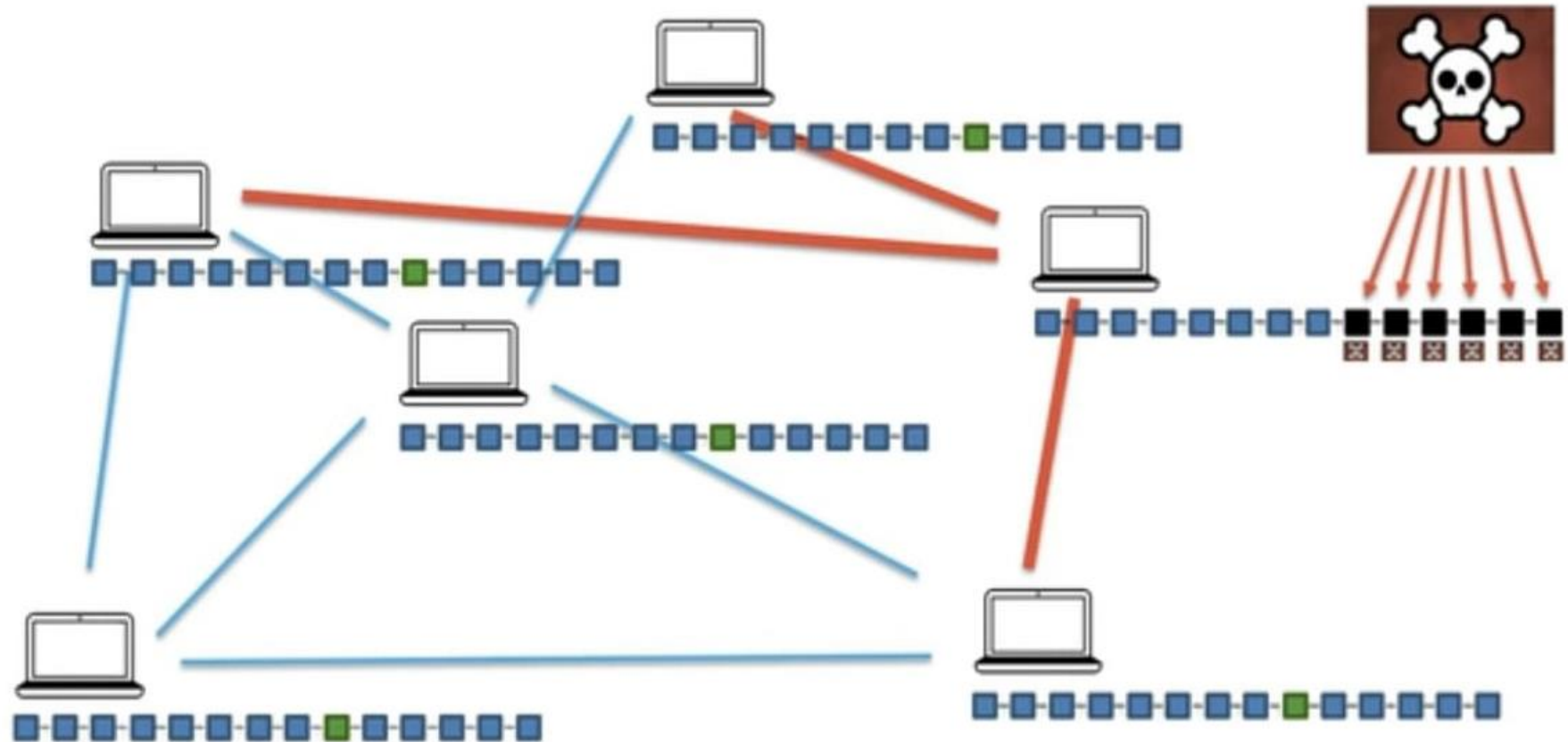
Hacker has to forge the blockchain



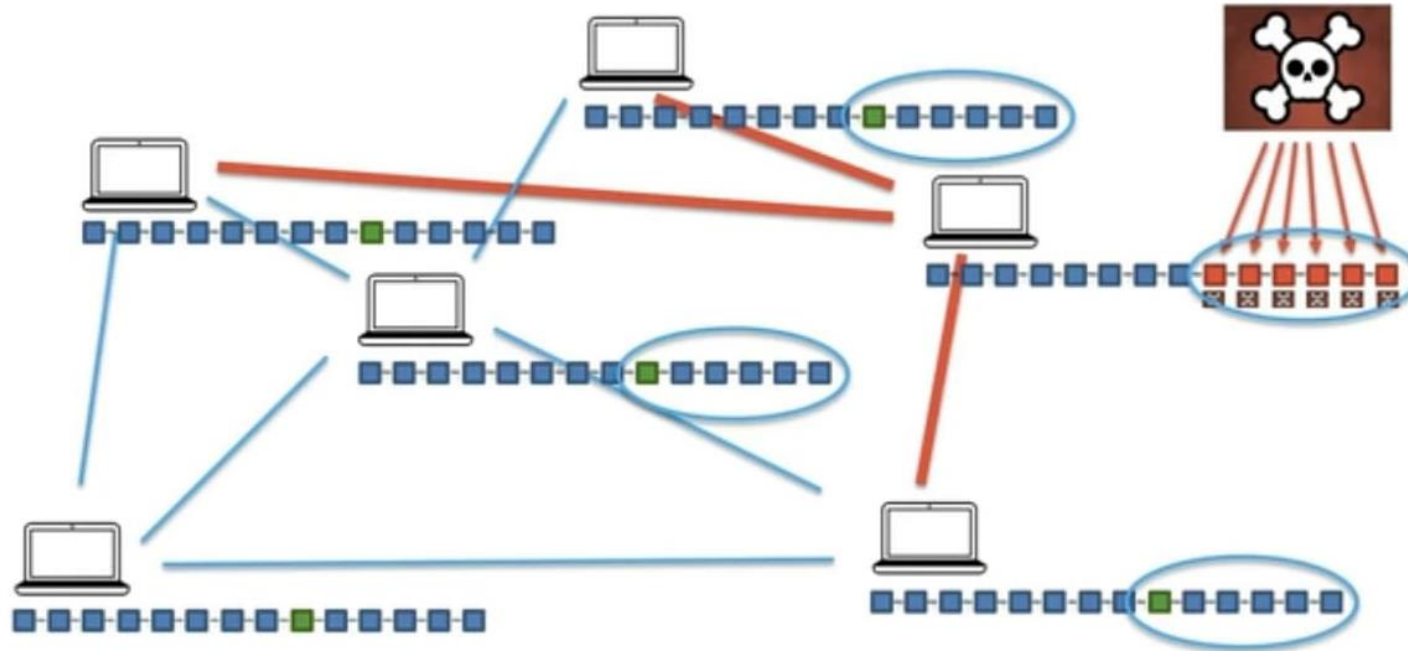
Hacker successfully forged the blockchain



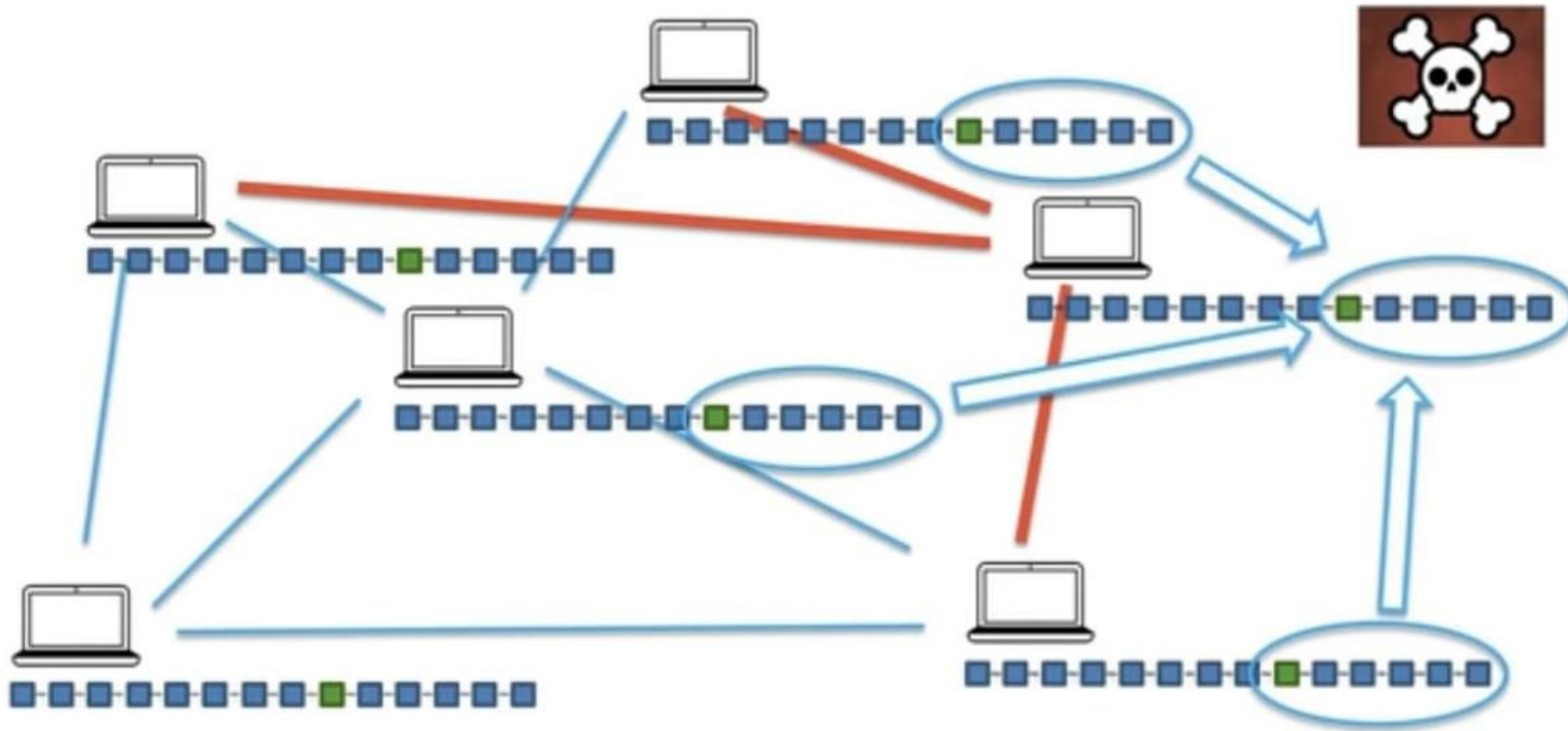
Network is constantly looking at peers to have the same copy of Blockchain



Copy of attacked node is not consistent with the majority

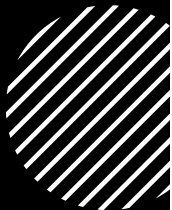


Correct copy is Restored





Network Entities



Users



Miners



What is Mining?



How mining works? (The Nonce)

Information that a Block has:



Block: #3
Data: Kirill -> Hadelin 500 hadcoins Kirill -> Ebay 100 hadcoins Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:



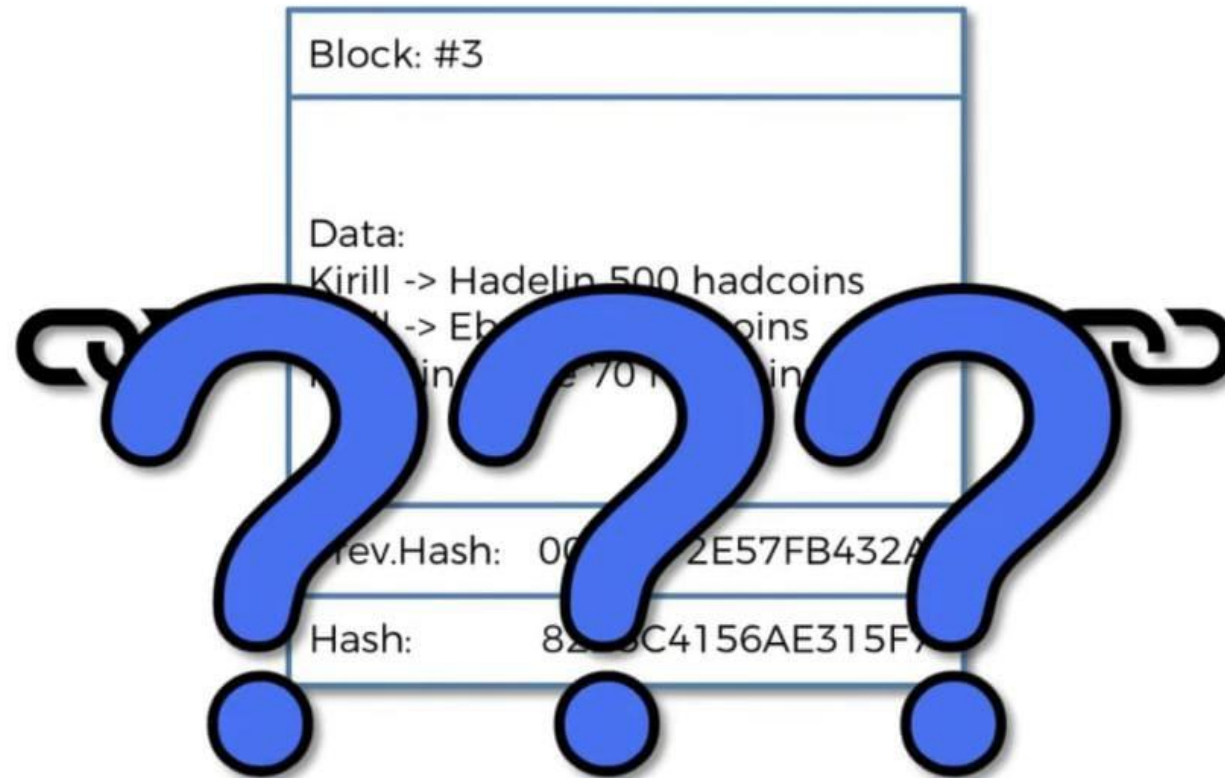
Computing Hash of a Block



Block: #3	
Data: Kirill -> Hadelin 500 hadcoins Kirill -> Ebay 100 hadcoins Hadelin -> Joe 70 hadcoins	
Prev.Hash:	0000DF2E57FB432A
Hash:	82B5C4156AE315F7



If a generation of hash is this much simple, then for what the miners are in race ?



The Nonce

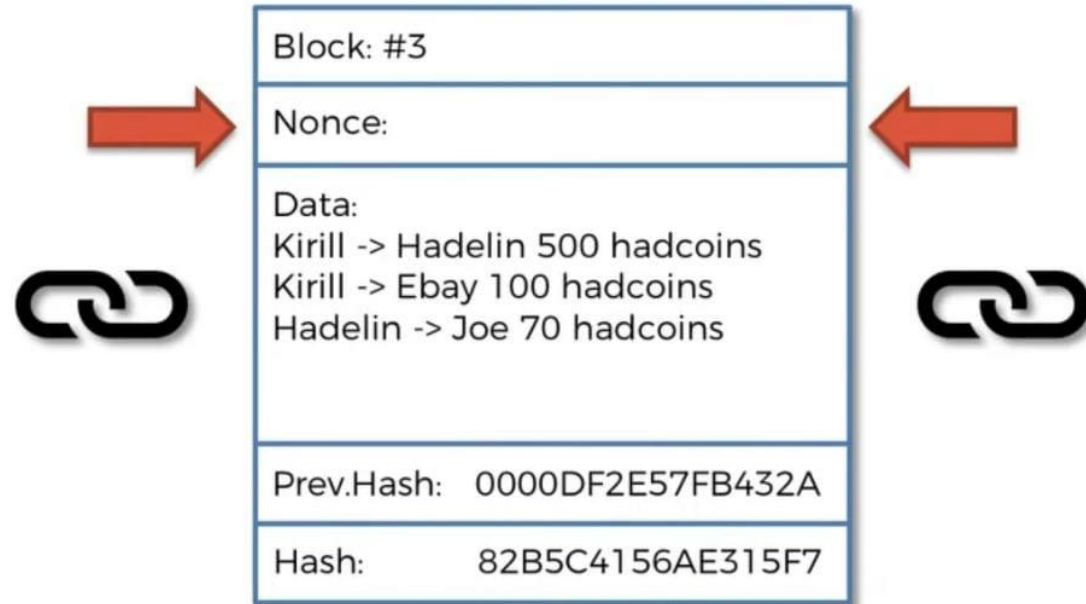
- Nonce: Number only used once
- Nonce is also included in computing the Hash along with Block Number, Data and Previous Hash
- The nonce keeps on changing which results in the changing of the Hash.

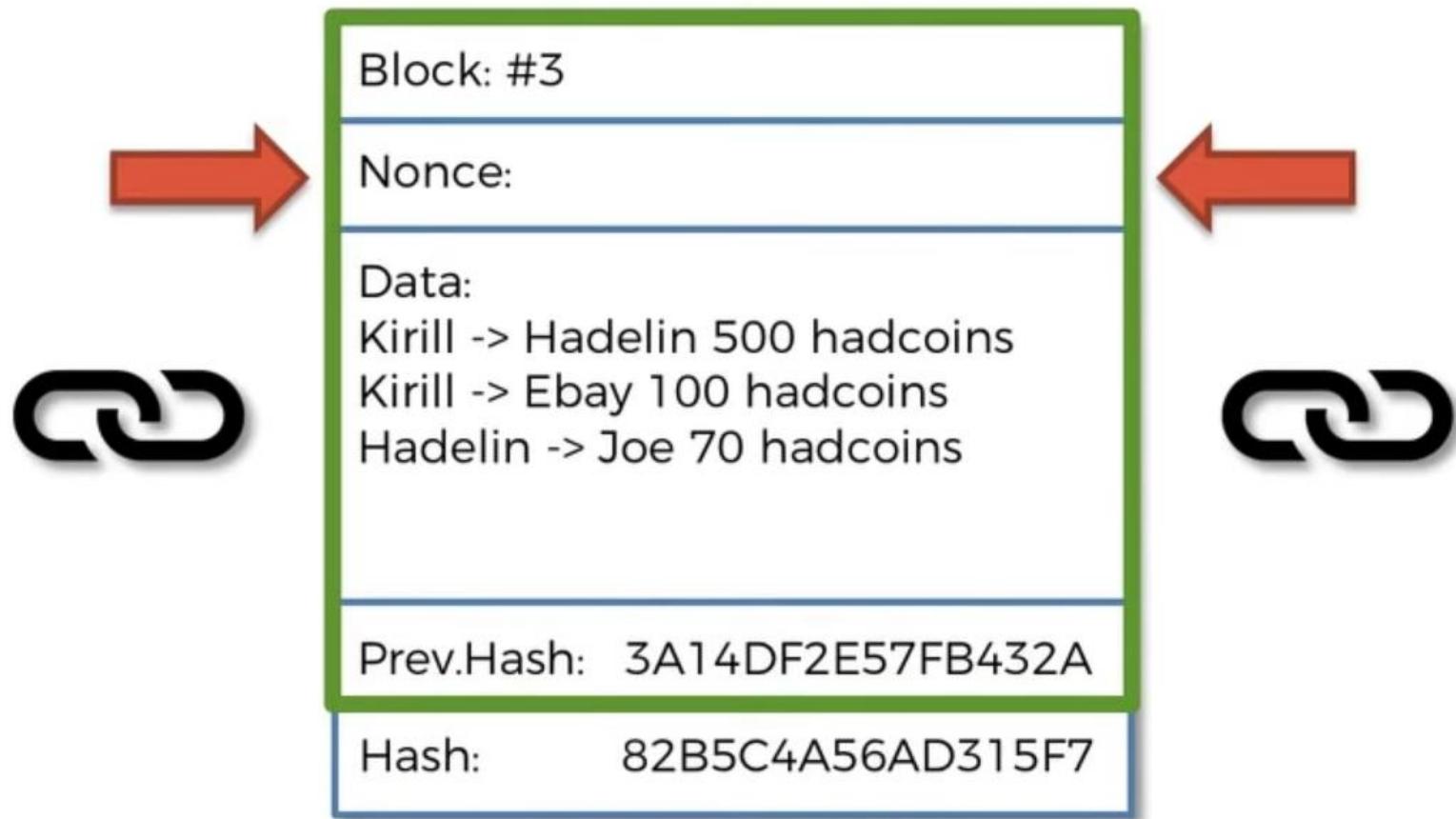


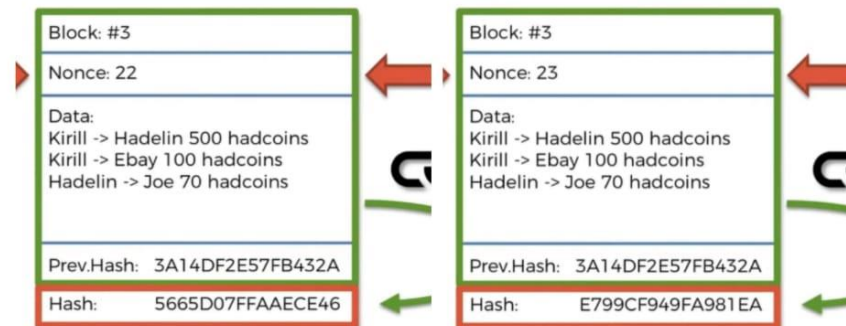
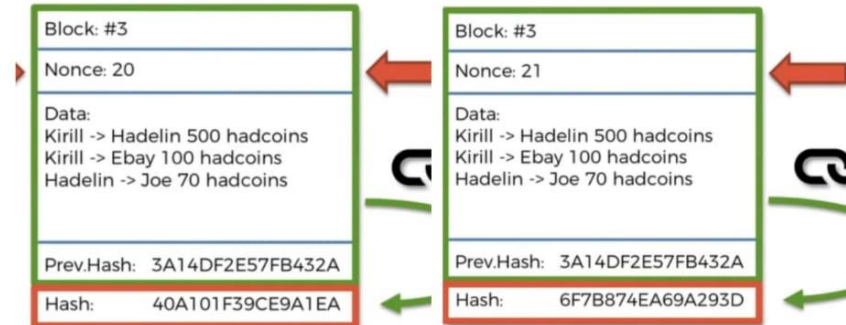
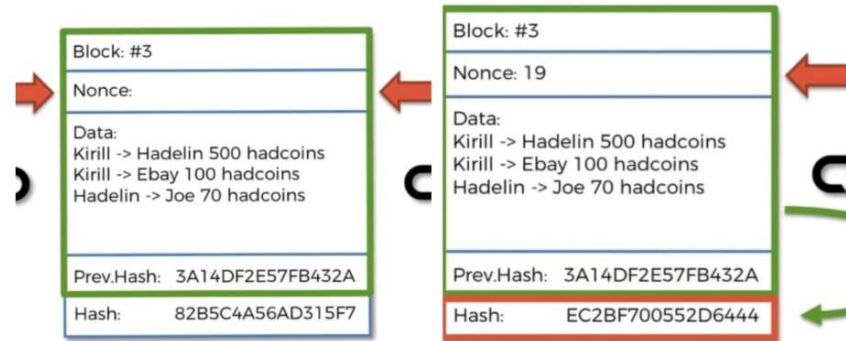
Block: #3
Nonce:
Data: Kirill -> Hadelin 500 hadcoins Kirill -> Ebay 100 hadcoins Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash: 82B5C4156AE315F7



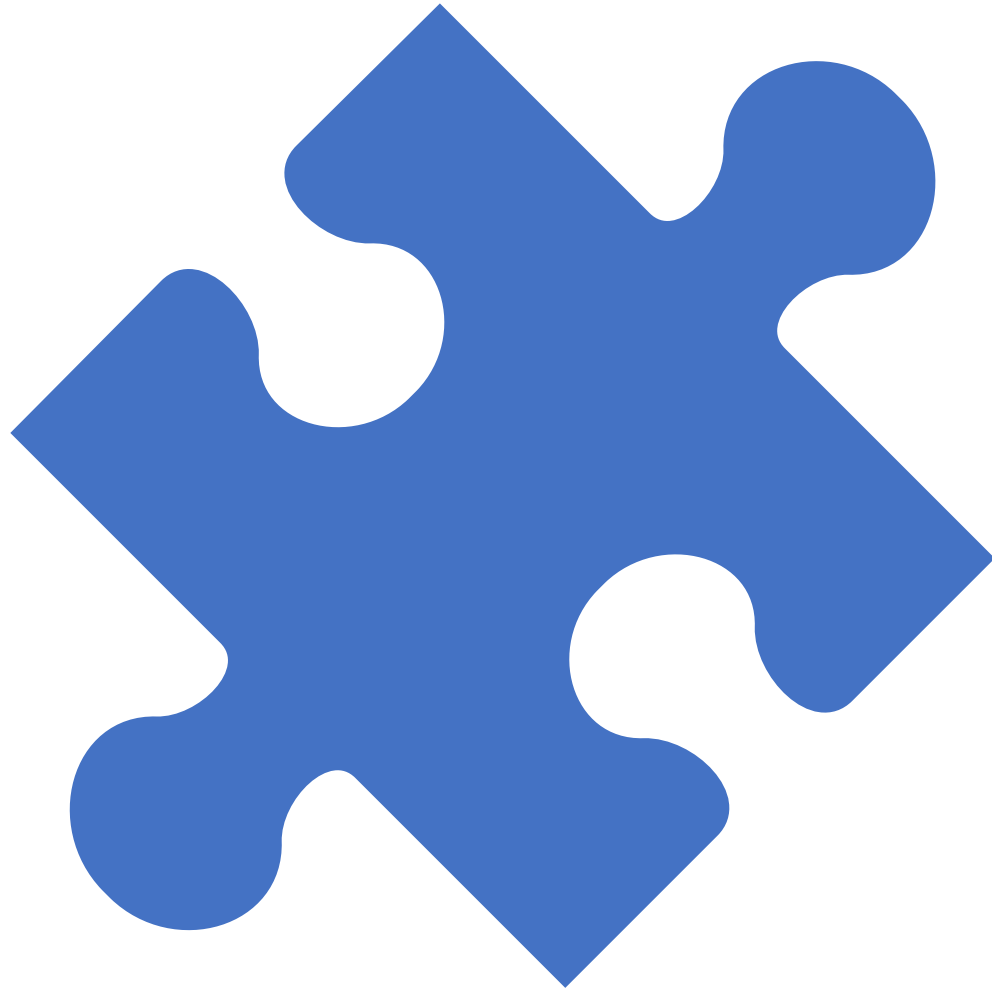
Nonce added
extra power and
flexibility to the
security of the
network







How mining
works? (The
cryptographic
puzzle)



- ALL POSSIBLE HASHES -

LARGEST

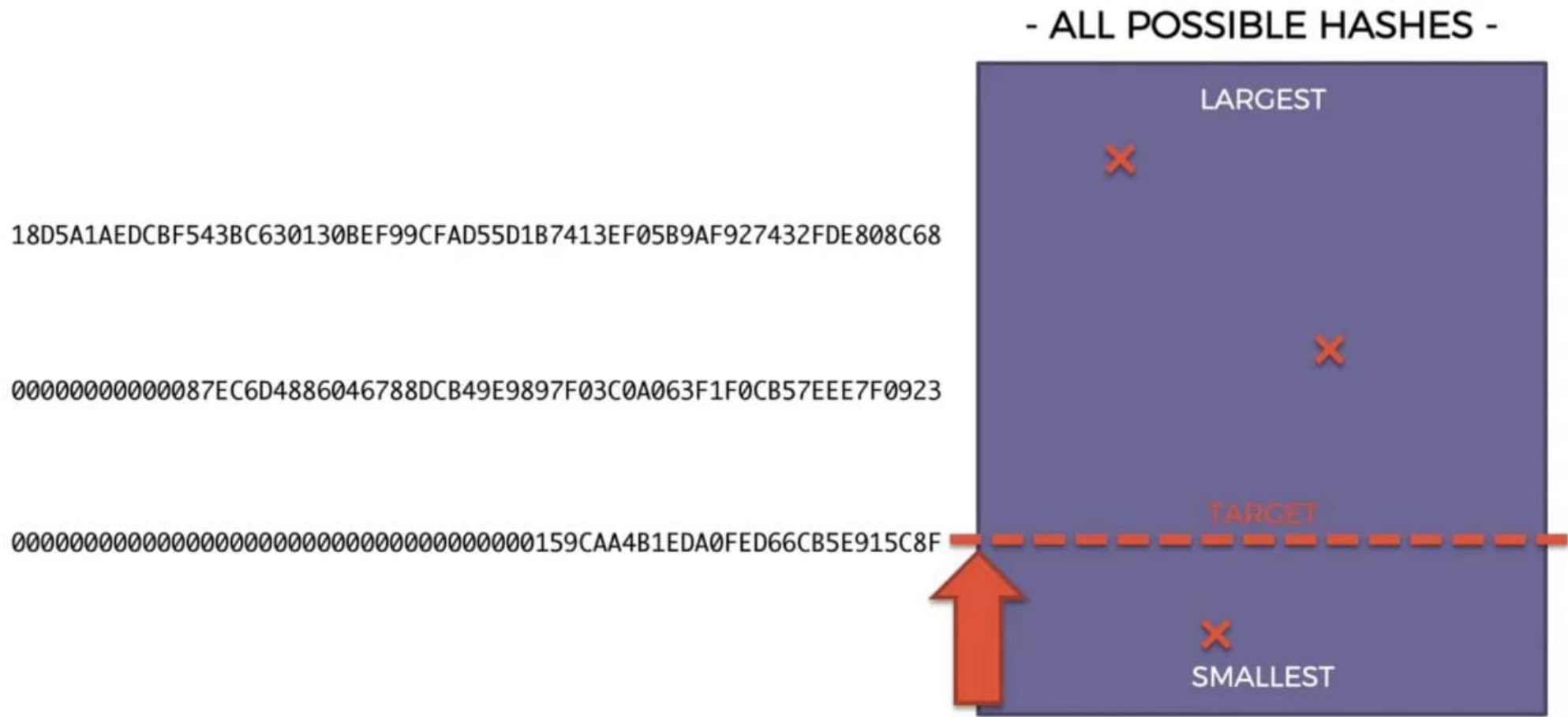
18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

SMALLEST

[illegible]

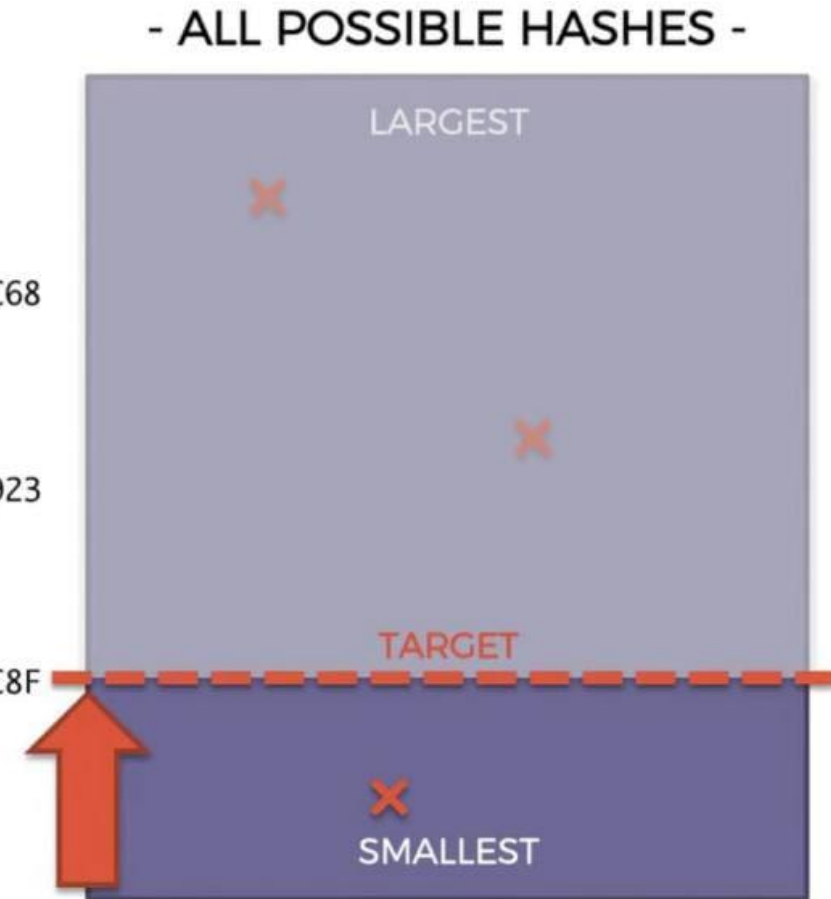
Network arbitrary selects the target for the miners



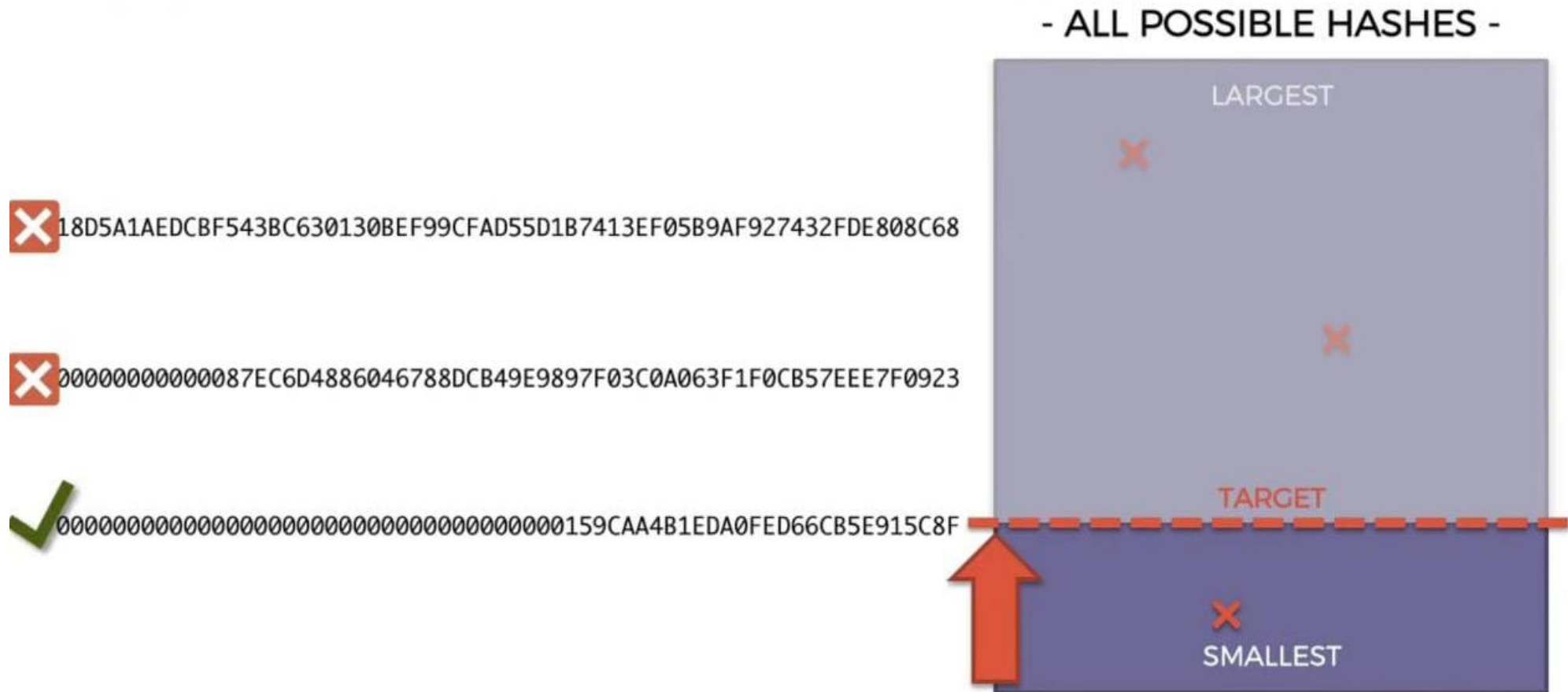
Any hash above the target doesn't count

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

[illegible]

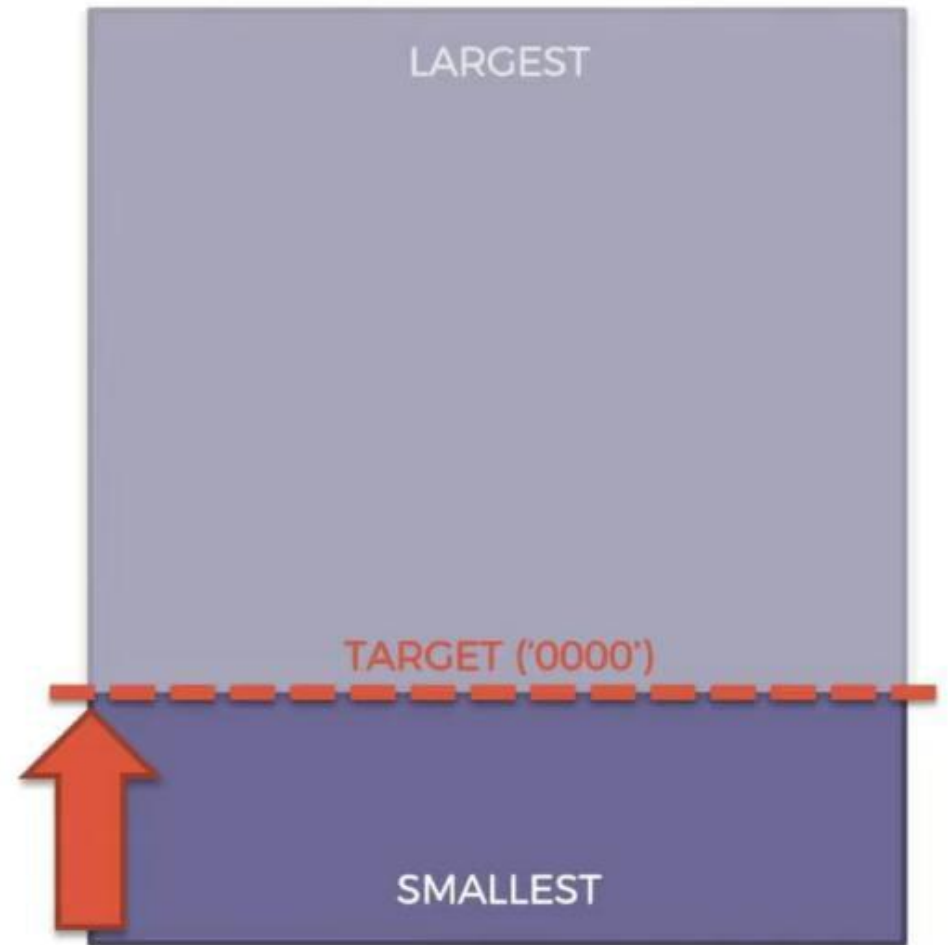
The only reason for it is to create a hurdle for the miners





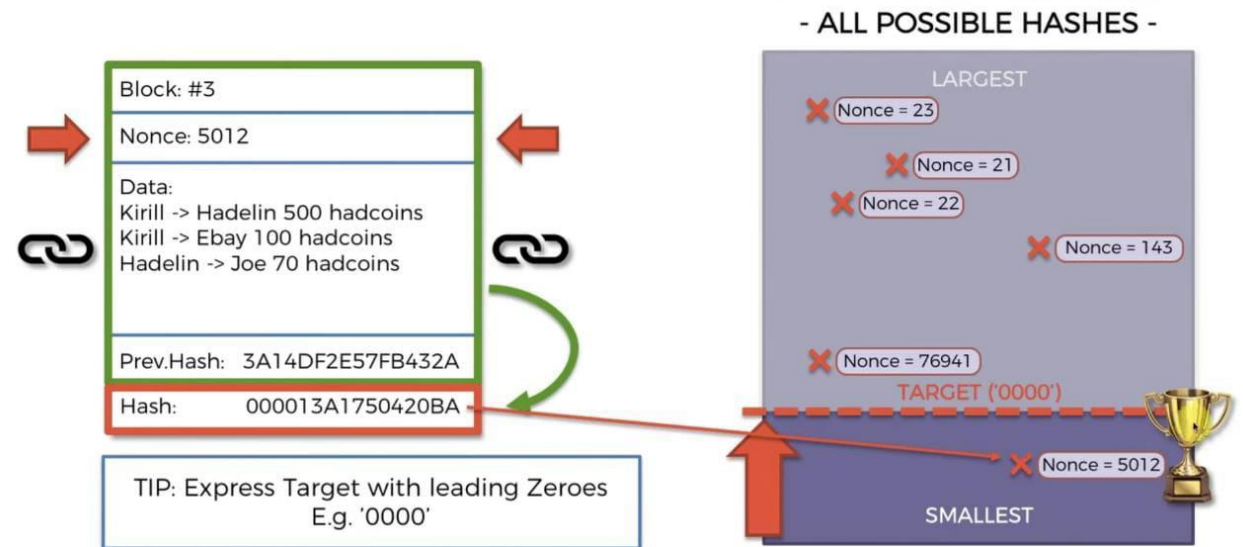
TIP: Express Target with leading Zeroes
E.g. '0000'

- ALL POSSIBLE HASHES -



Found Golden Nonce:

- If you find a hash below the target, you will be allowed to create a block
- Miners just guess the nonce to generate a hash which is below the target
- Nonce = 5012 (Golden Nonce) was able to generate a hash that is below the target and hence gets to create a block in the blockchain





Finally, we know the following about Blockchain Intuition:

- What is Blockchain?
- Understanding of SHA256
- Immutable ledger
- P2P Network
- How Mining Works – Nonce, Cryptographic Puzzle

Acknowledgement and Source:

- <https://www.udemy.com/course/build-your-blockchain-az/>