Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari

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

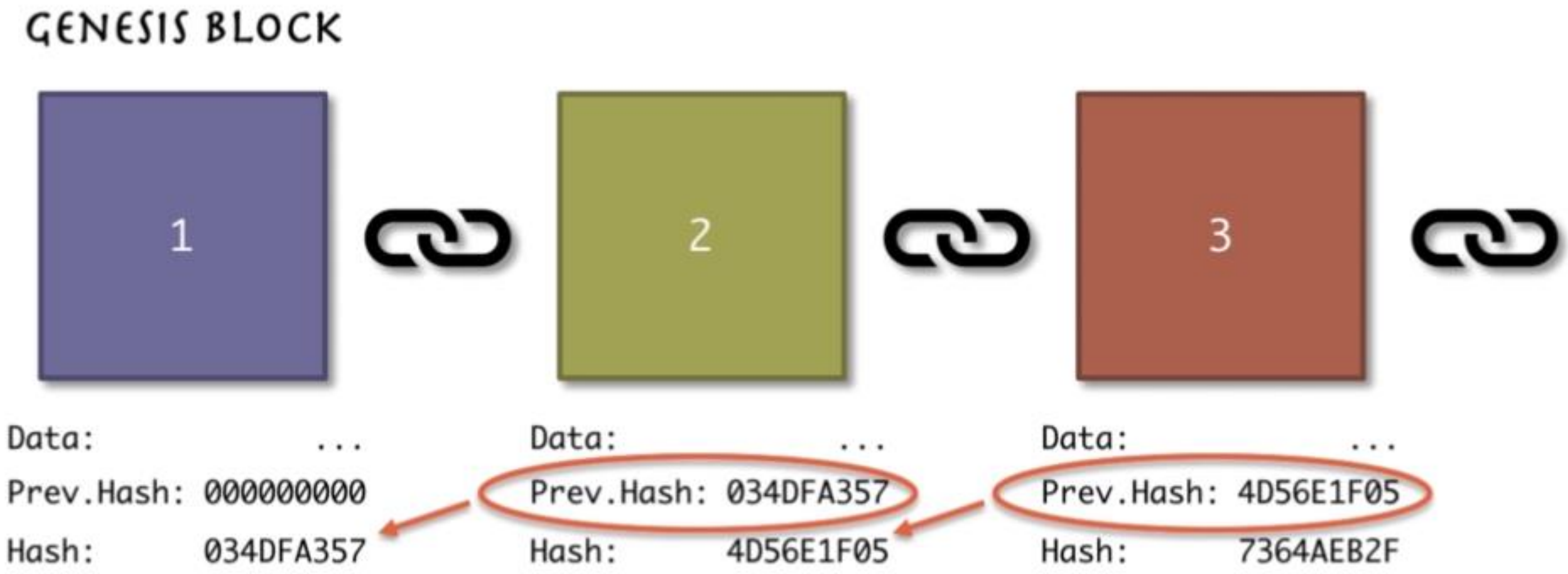
Block in Blockchain

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



```
Data:                 ...     Data:                 ...     Data:                 ...
Prev.Hash: 000000000          Prev.Hash: 034DFA357          Prev.Hash: 4D56E1F05
Hash:      034DFA357          Hash:      4D56E1F05          Hash:      7364AEB2F
```

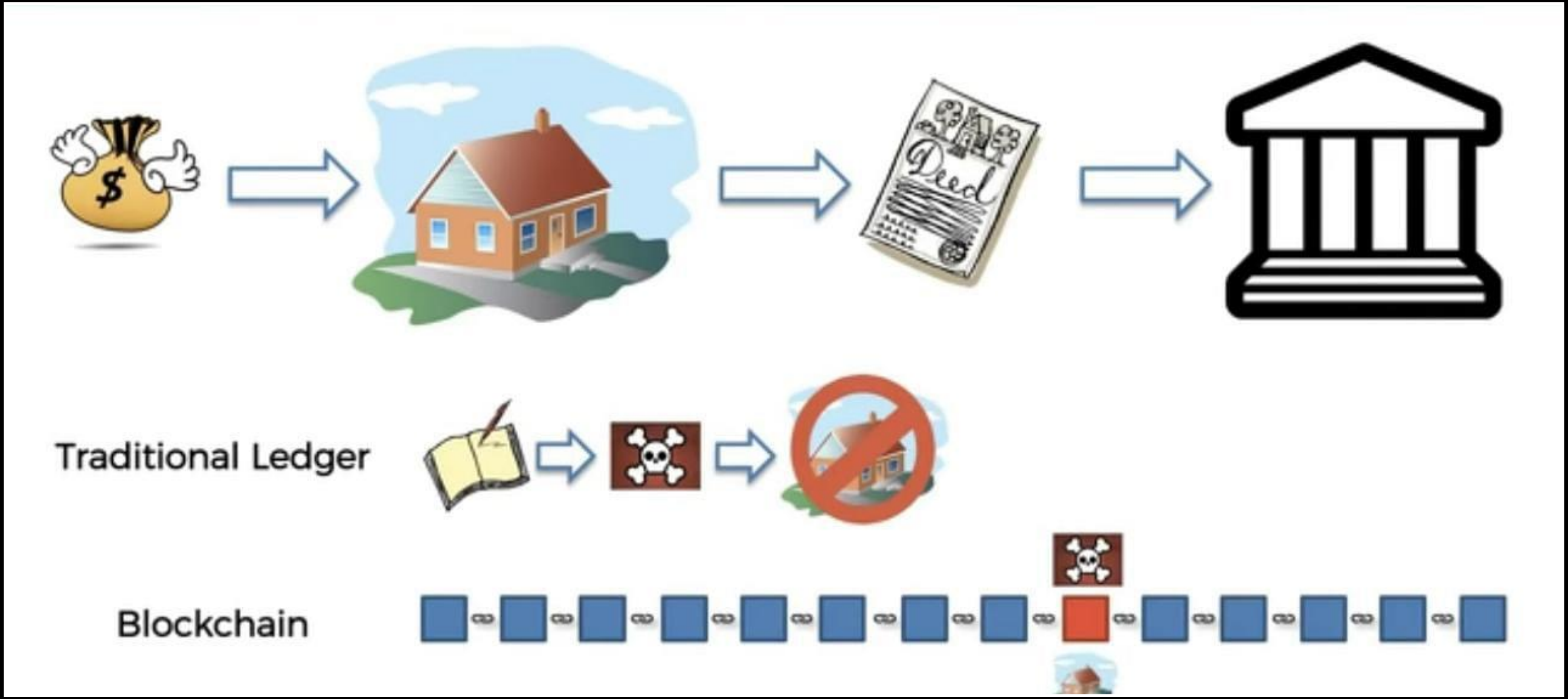
Blockchain

Understanding SHA256 Hash:

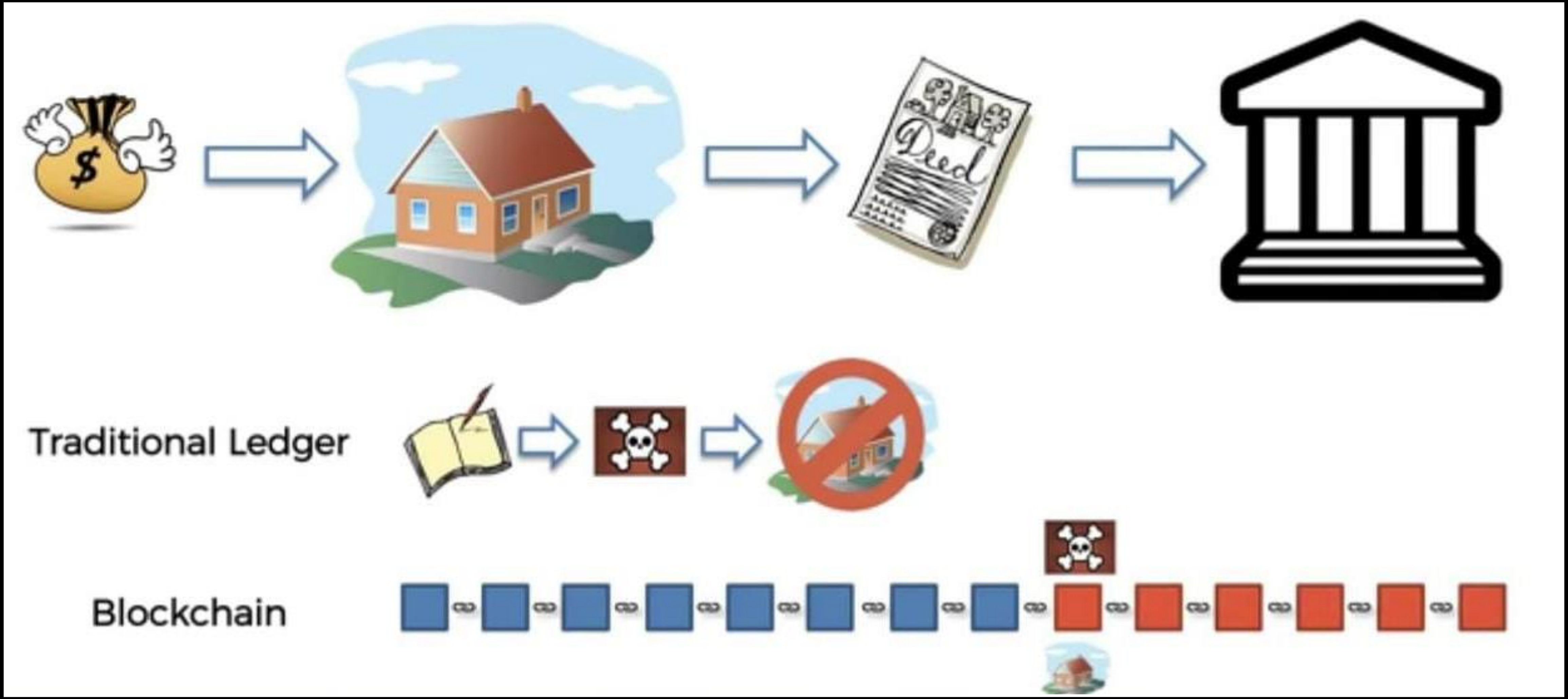
- Different people have different fingerprints
- Fingerprint of a file is called a SHA256 Hash
- Developed by the NSA
- SHA - Secure Hash Algorithm
- 256 - number of bits it takes in memory - 64 characters long
- A file will always have the same hash
- If we change even one character, the whole hash 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.



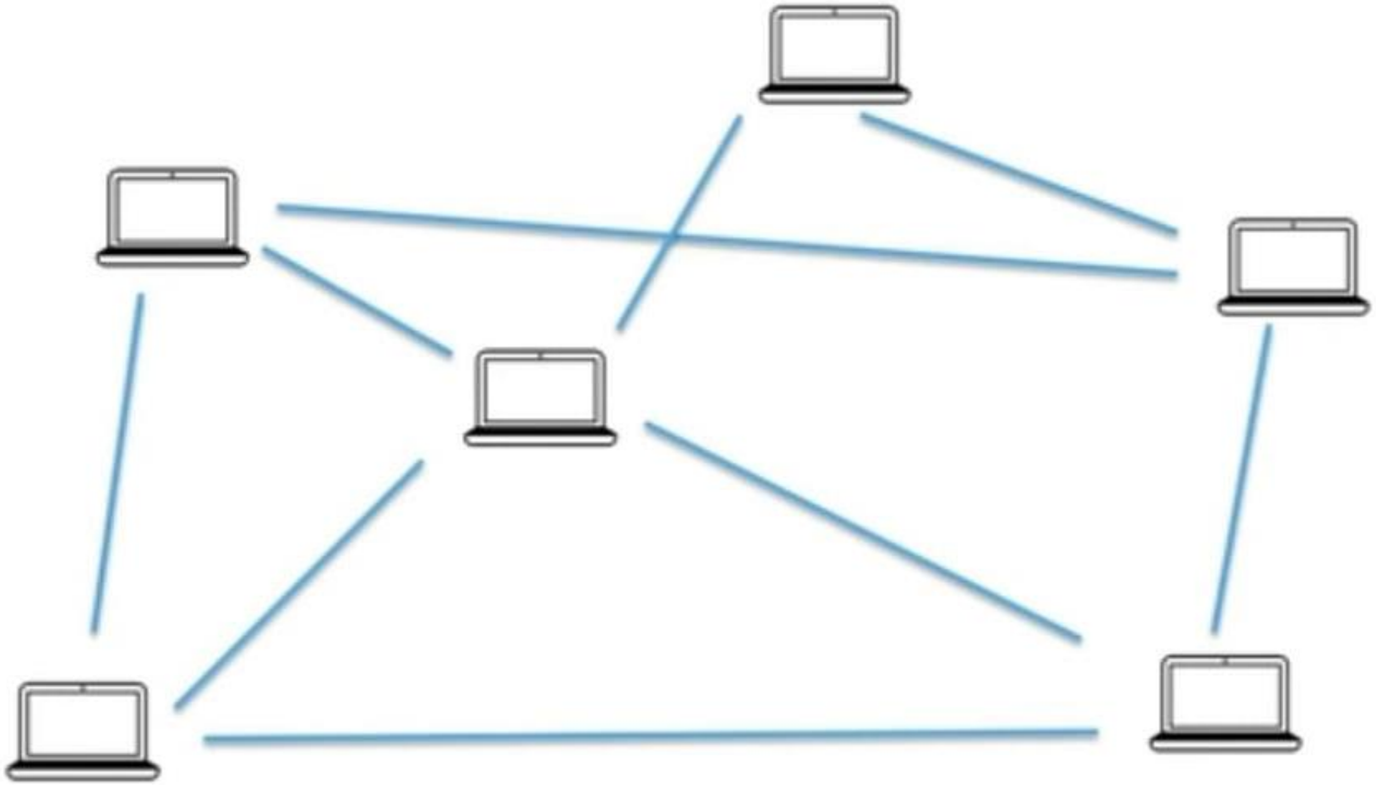
Immutable Ledger - 2



Immutable Ledger – Forge the Blockchain

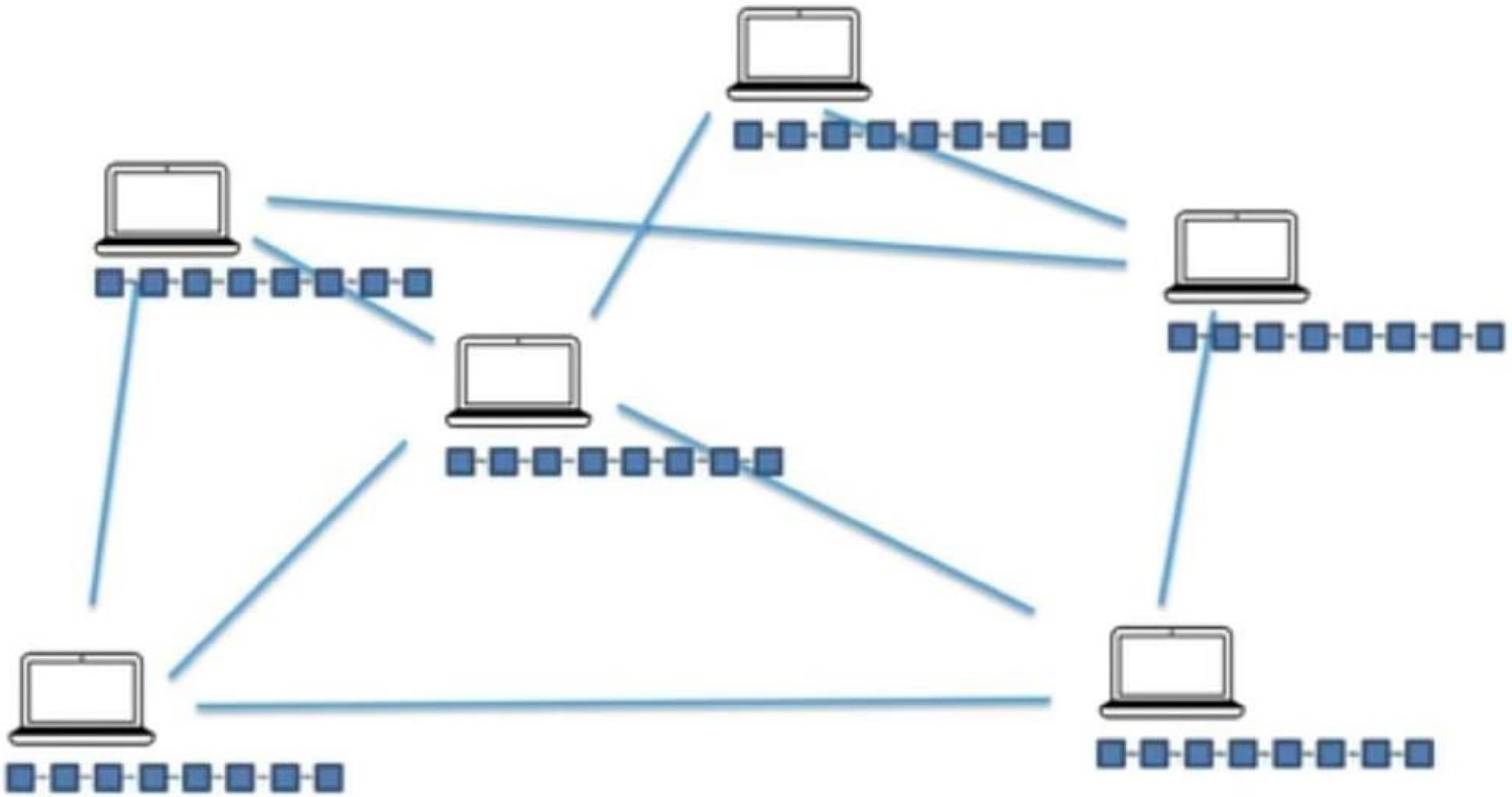
Distributed P2P Network

Peer-to-Peer Network

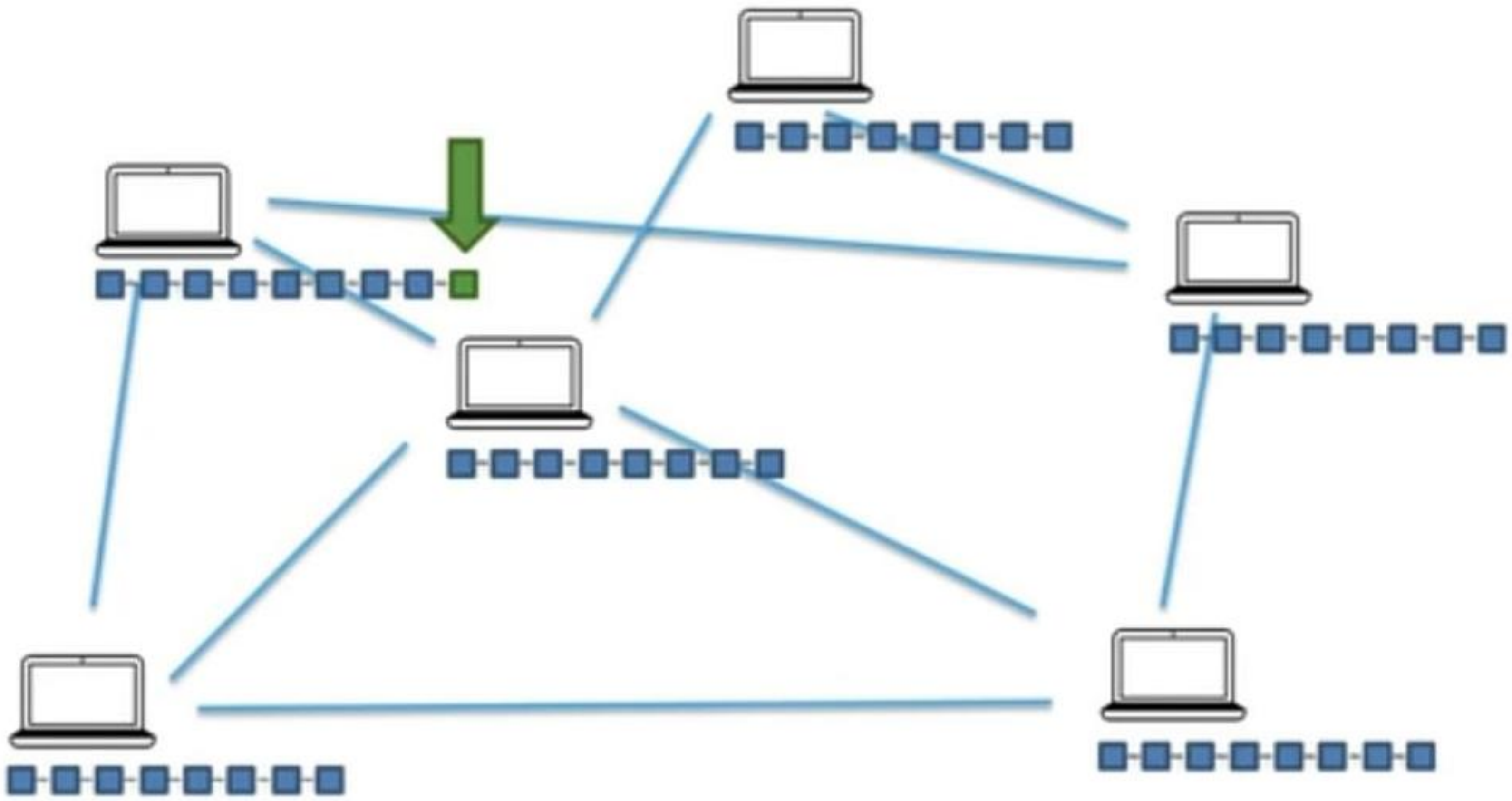


Anonymity: No real identity

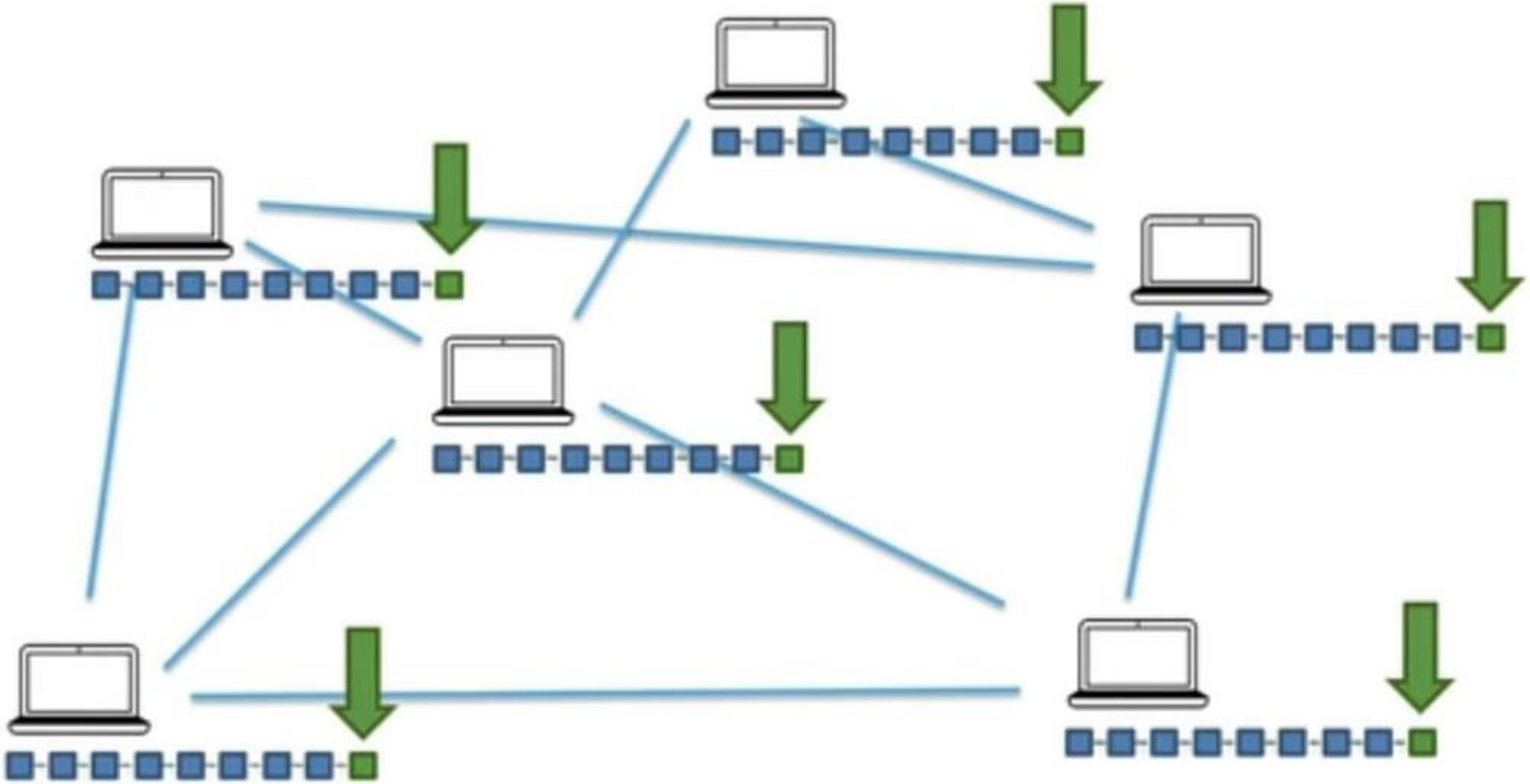
Each Node has a copy of Blockchain



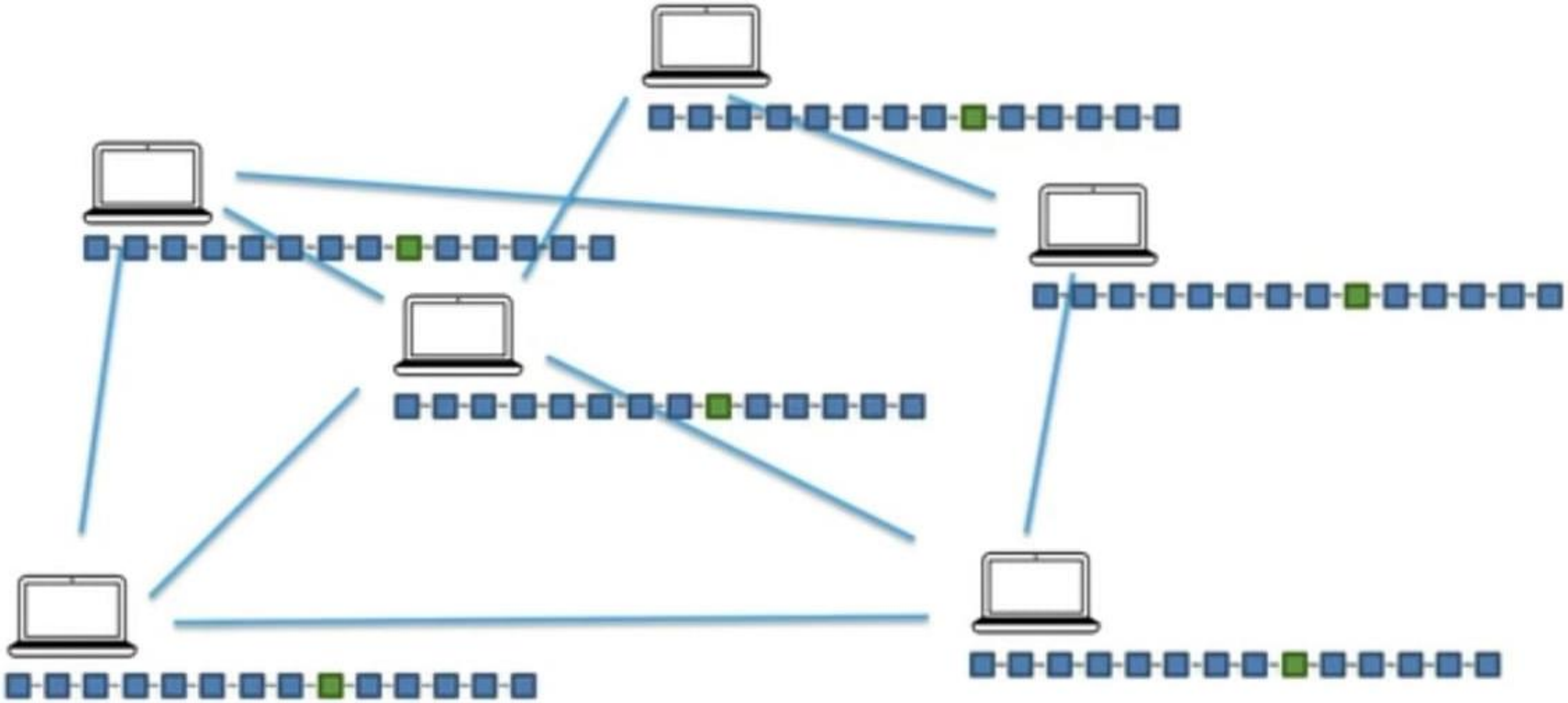
If a block is added to a Blockchain



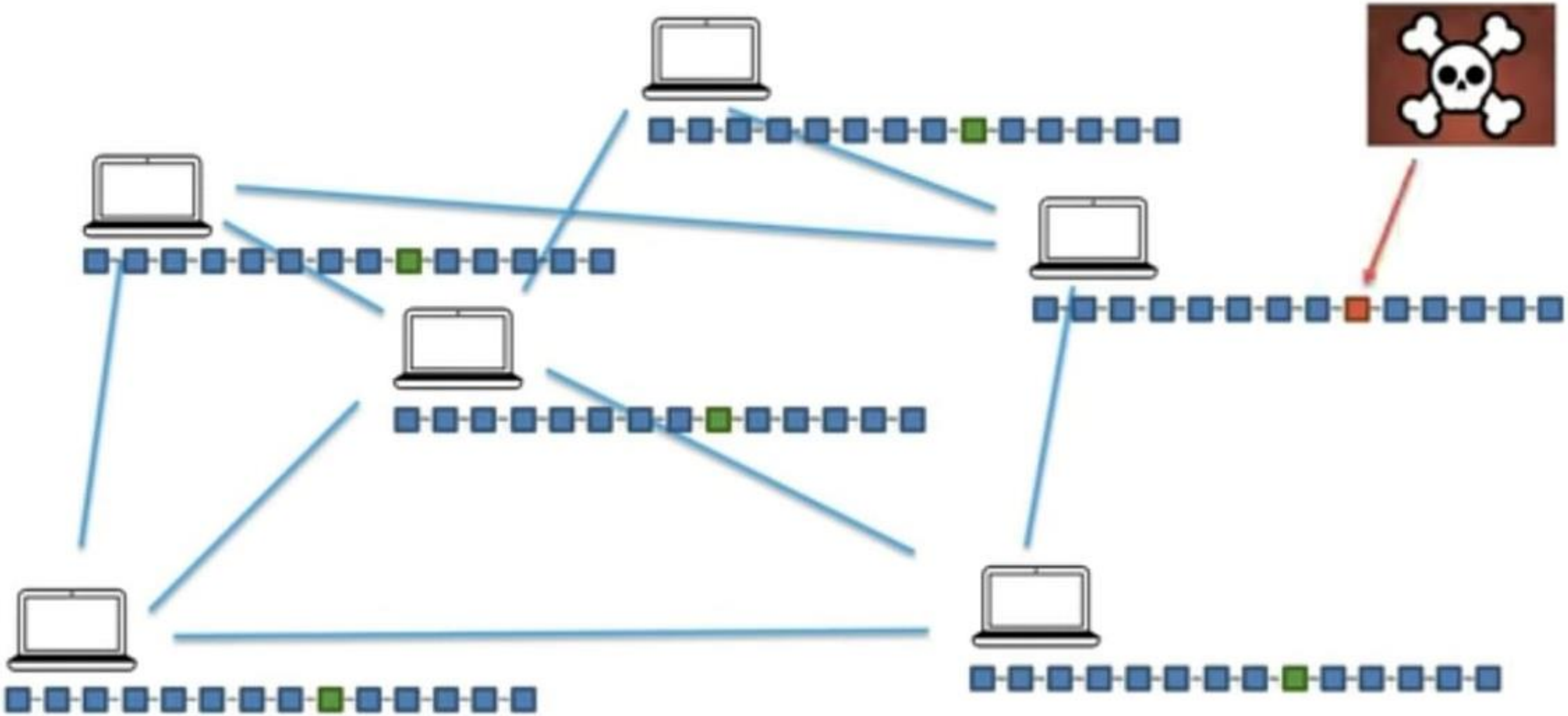
Whole network must update it’s copy



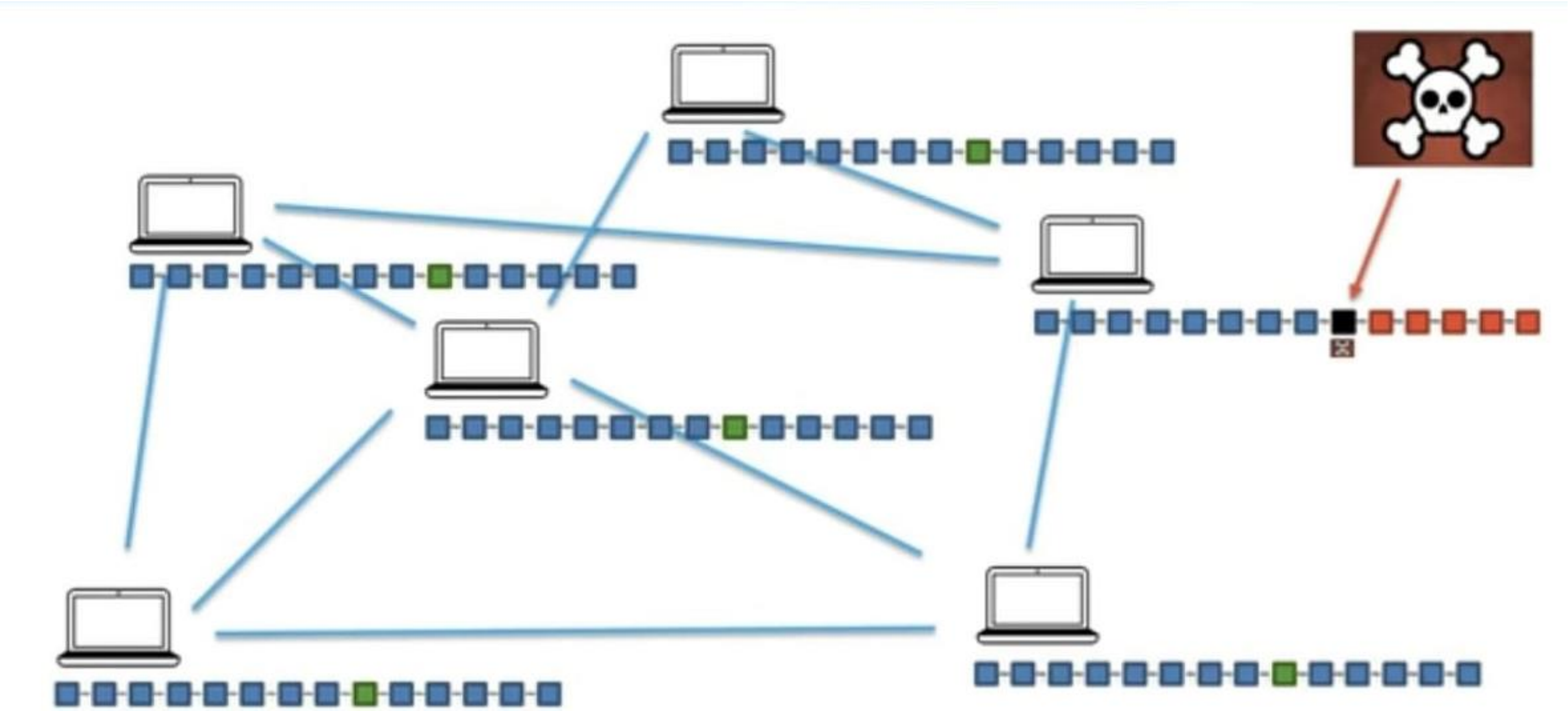
With the passage of time, more and more blocks are being added



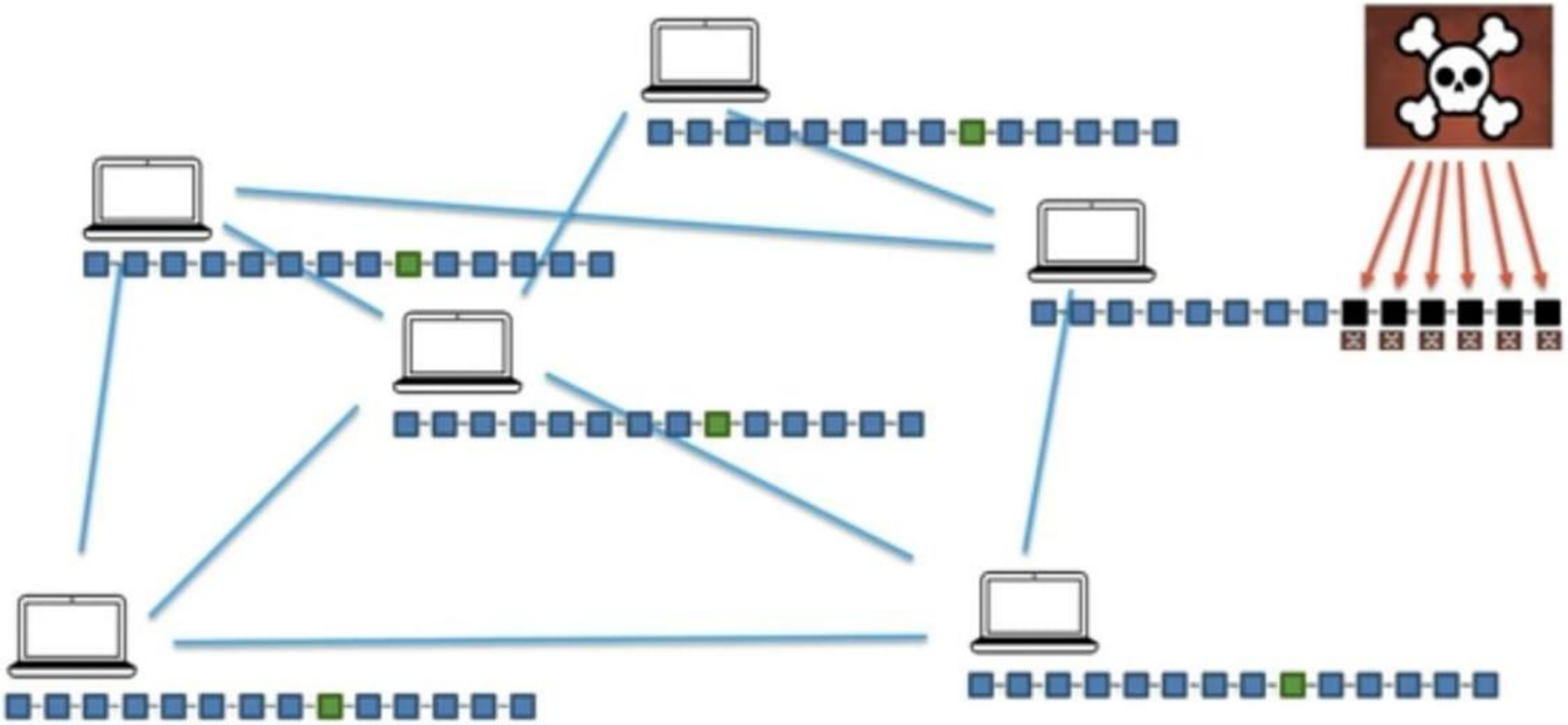
Someone attacking on blockchain through the network node



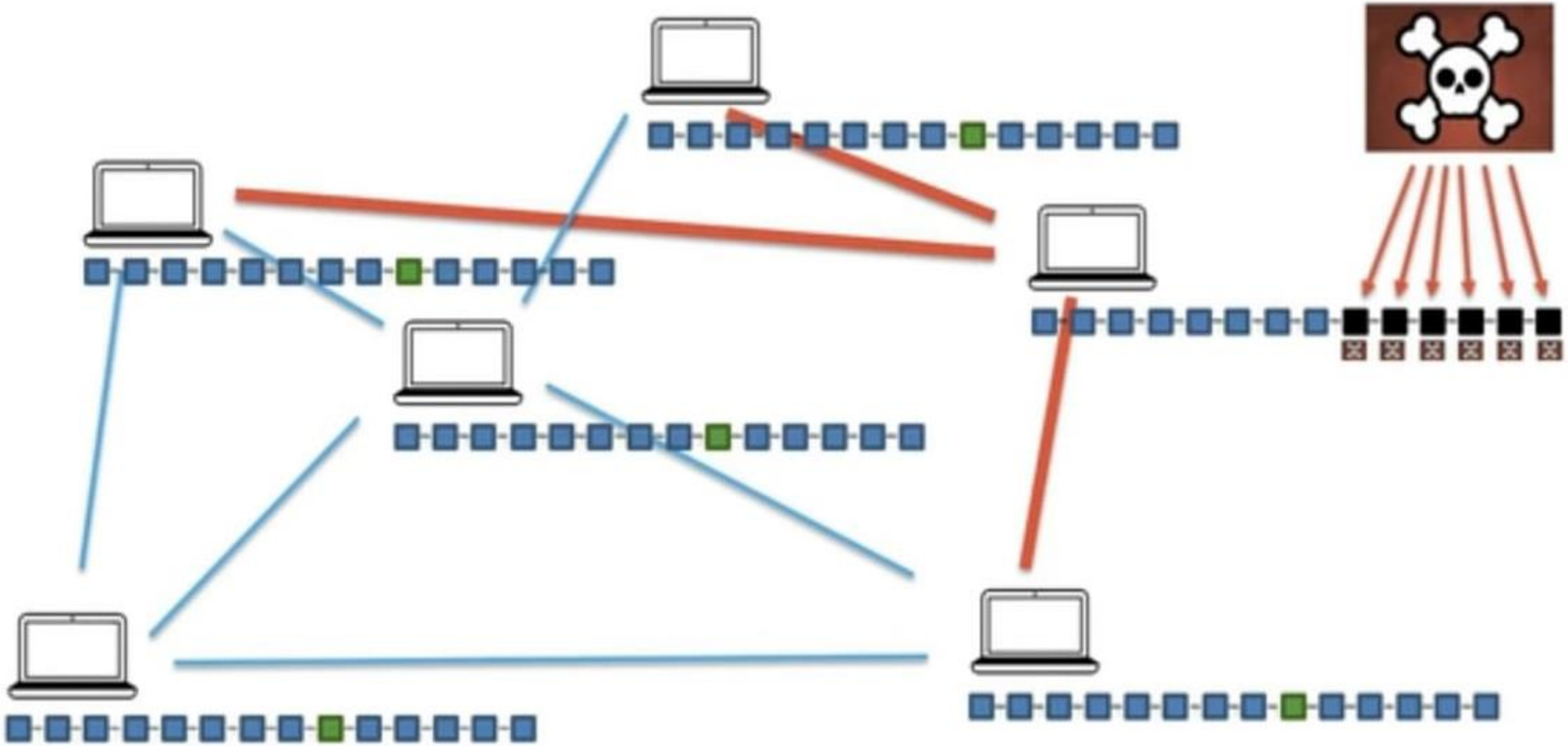
Hacker has to forge the blockchain



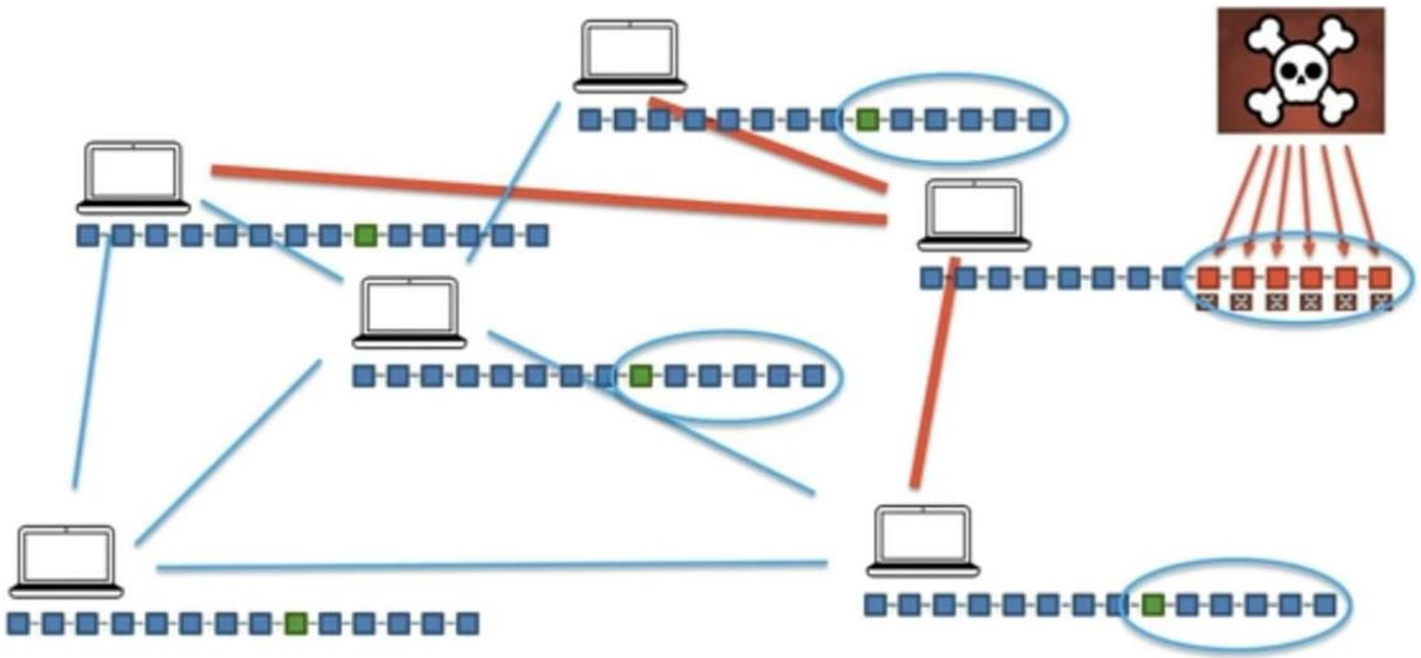
Hacker successfully forged the blockchain



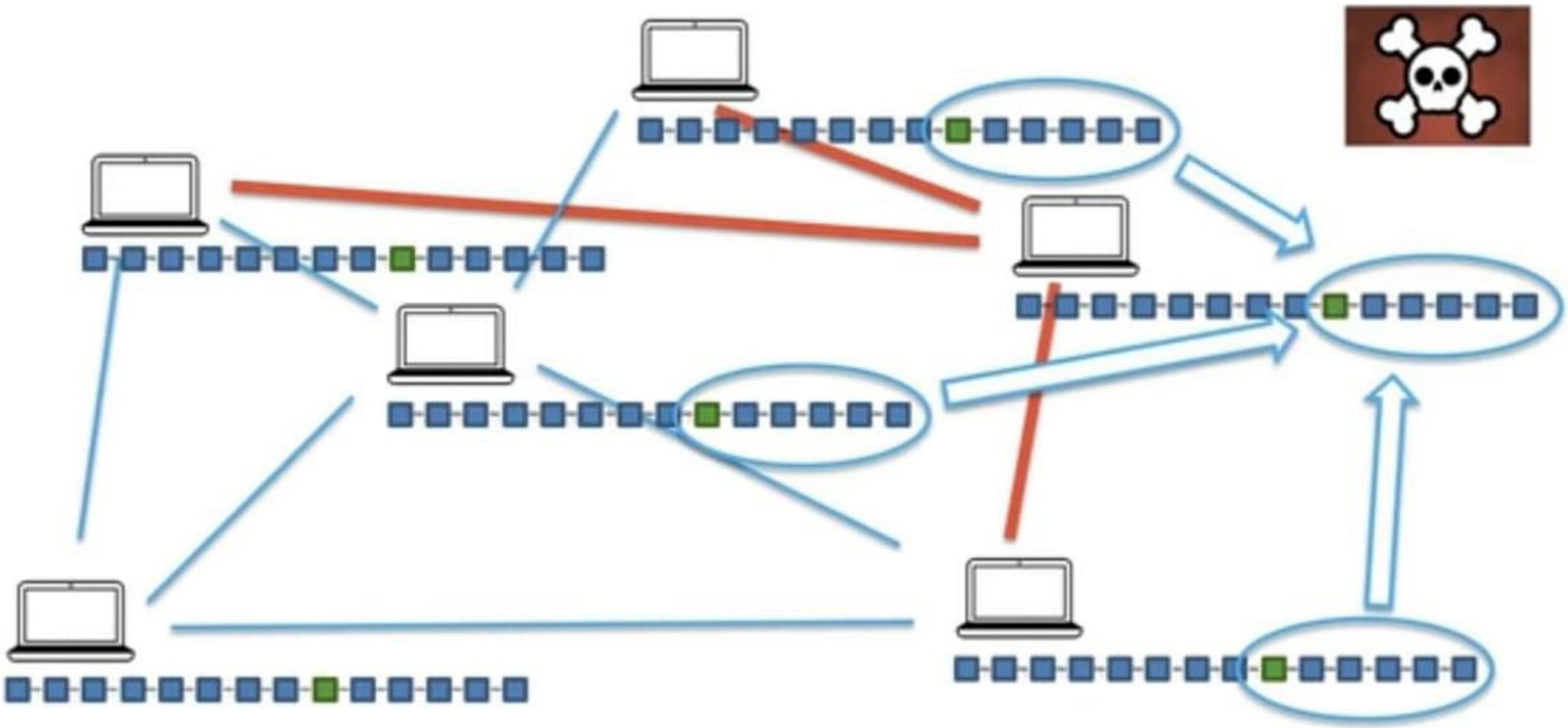
Network is constantly looking at peers to have the same copy of Blockchain



Copy of attacked node is not consistent with the majority



Correct copy is Restored



Acknowledgement and Source:

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