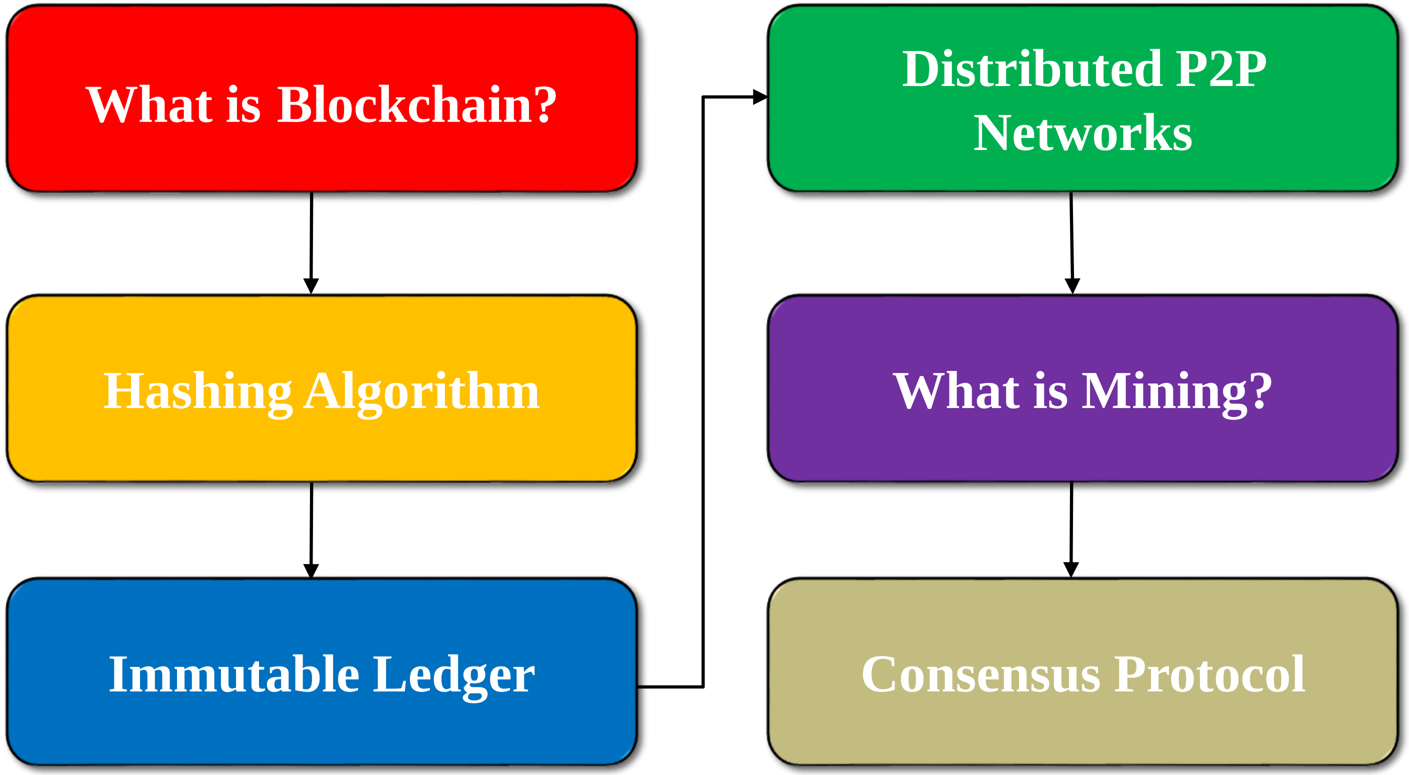
Blockchain

Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.

Contents – Module A



What is Blockchain?

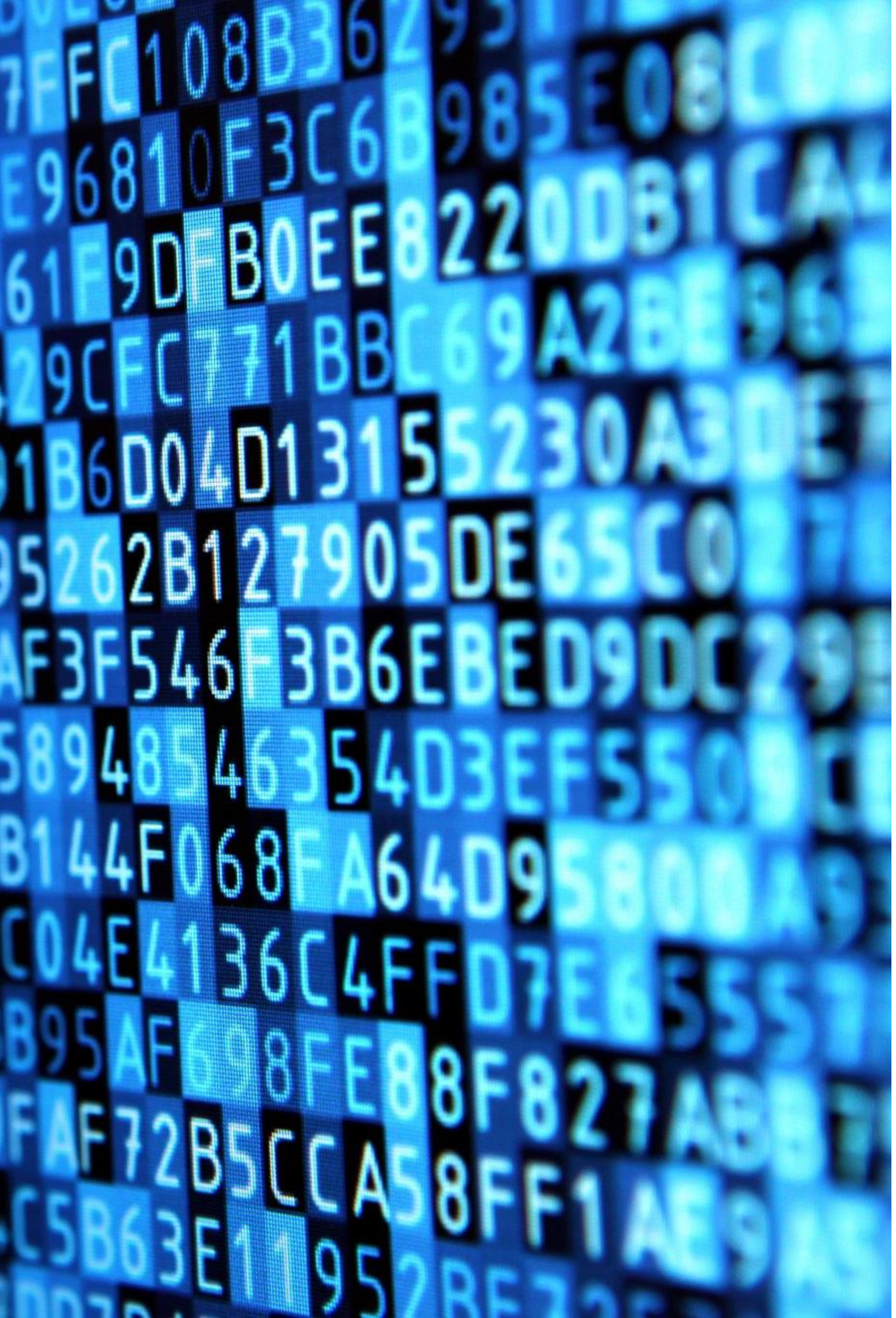
Hashing Algorithm

Immutable Ledger

Distributed P2P Networks

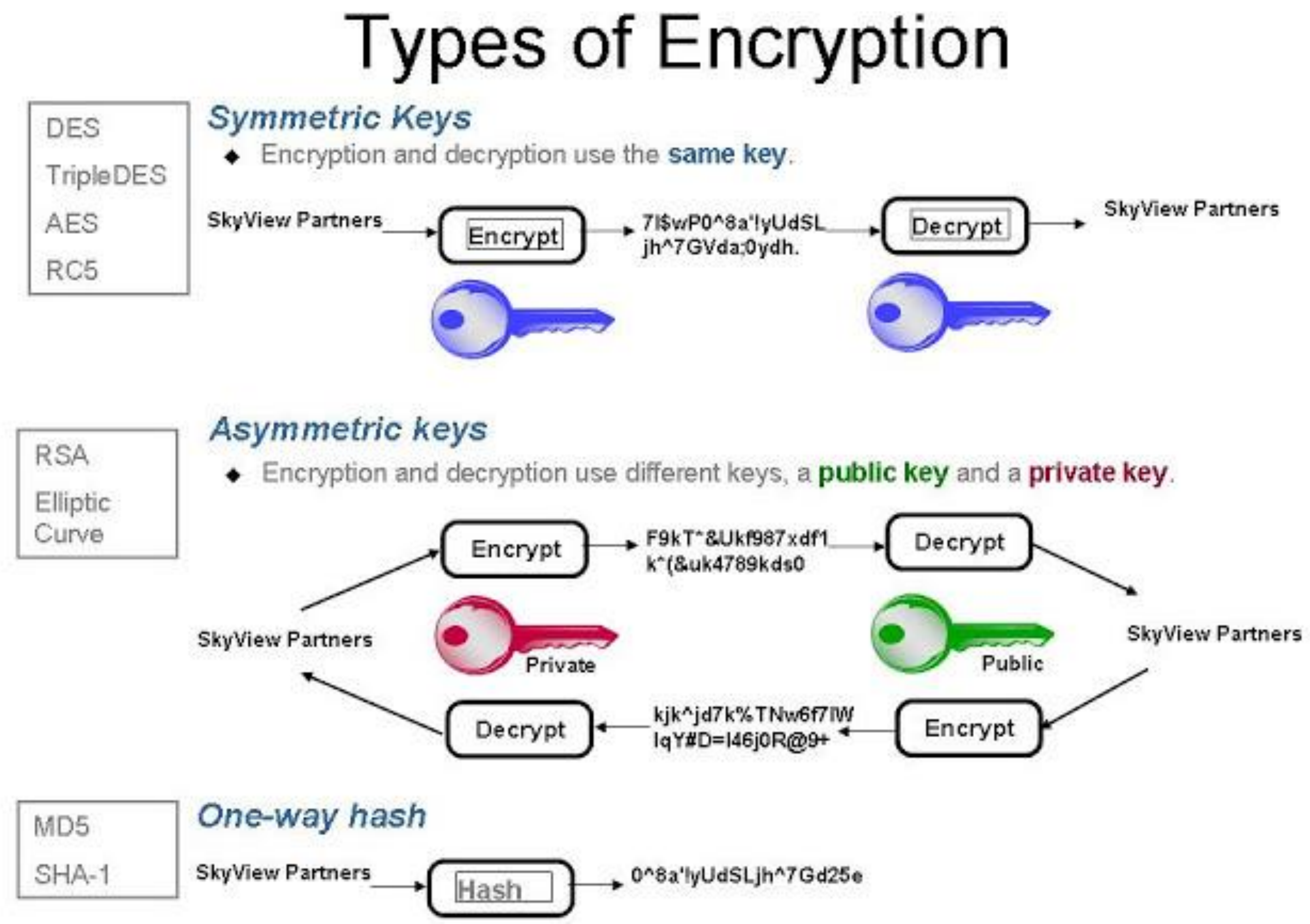
What is Mining?

Consensus Protocol



Hashing Algorithm

What a Hash is?



Types of Encryption

Symmetric Keys

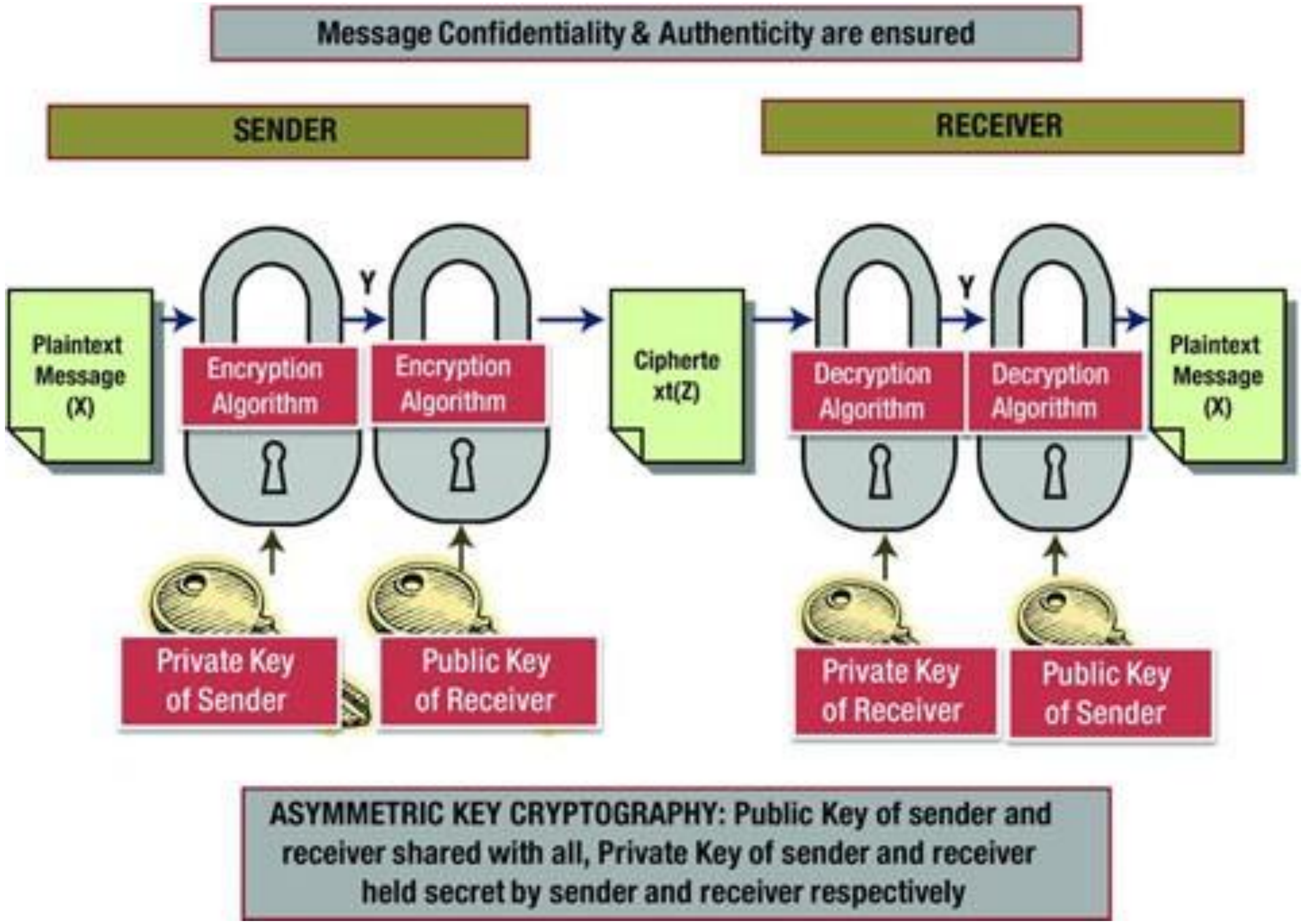
- Encryption and decryption use the **same key**.

Asymmetric keys

- Encryption and decryption use different keys, a **public key** and a **private key**.

One-way hash

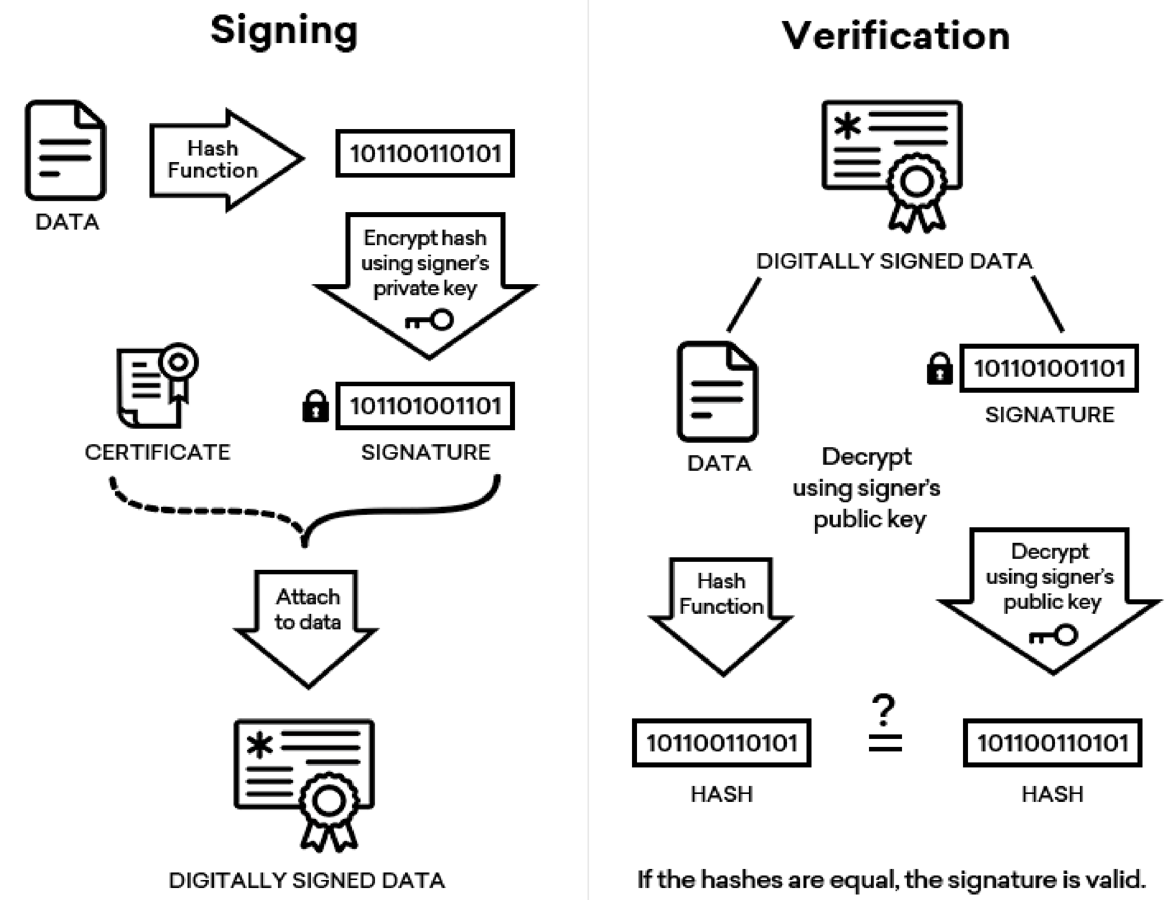
Confidentiality and Authenticity



Message Confidentiality & Authenticity are ensured

ASYMMETRIC KEY CRYPTOGRAPHY: Public Key of sender and receiver shared with all, Private Key of sender and receiver held secret by sender and receiver respectively

Digital Signature



If the hashes are equal, the signature is valid.

What a Hash is?

- A fixed size numeric representation of the contents of a message.
- Also known as message digest
- Computed by a hash function (One way cryptography).
- Hash function has no key, so it is not reversible.
- For same message you always get the same hash
- Computationally infeasible to find two messages that hash to the same digest.

What a Hash is?

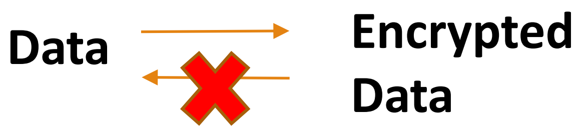
Hash Properties:

1. Computationally efficient
2. Deterministic (Same input same output hash code)
3. Pre-image resistant (Finding another message has a specific hash code)
4. Collision Resistant
5. Drastically/ dramatically changes with minimal change in the input

Hashing Algorithm

The five requirements of Hash Algorithm-

One Way



Deterministic

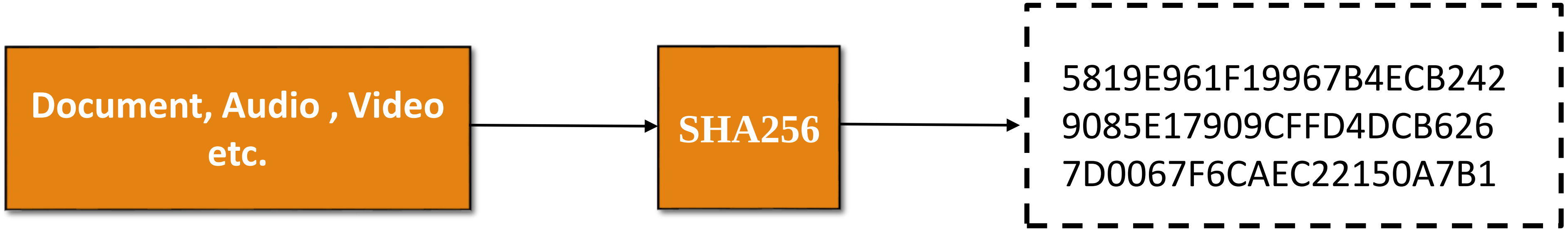
ABC → 845

Fast Computation

Withstand Collisions

Avalanche Effect

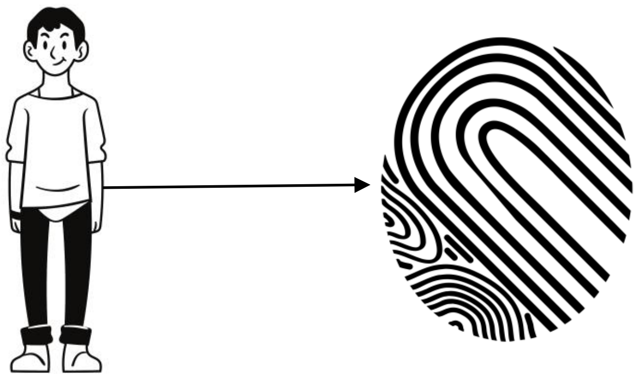
Hashing Algorithm

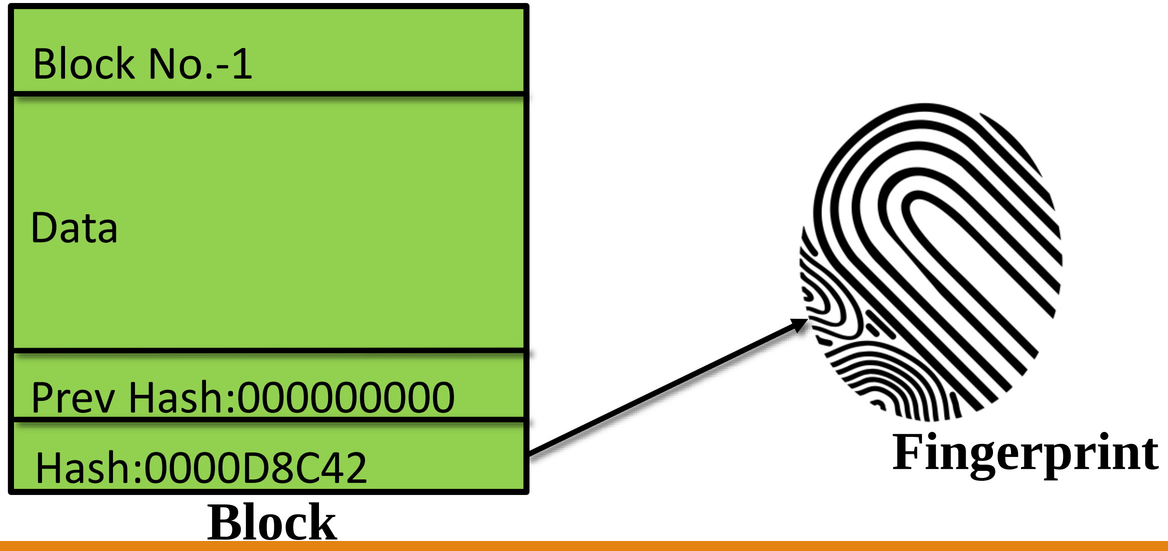


This has **64 hexadecimal characters.**
Each character is of **4 bits.**
So in total it has 64* 4 bits i.e. **256 bits**.

Hashing Algorithm

- Fingerprint Authentication is used to recognize/ identify an individual in a group of people
- Likewise, a hash of a block is used to recognize/ identify a block in the Blockchain





Block No.-1

Data

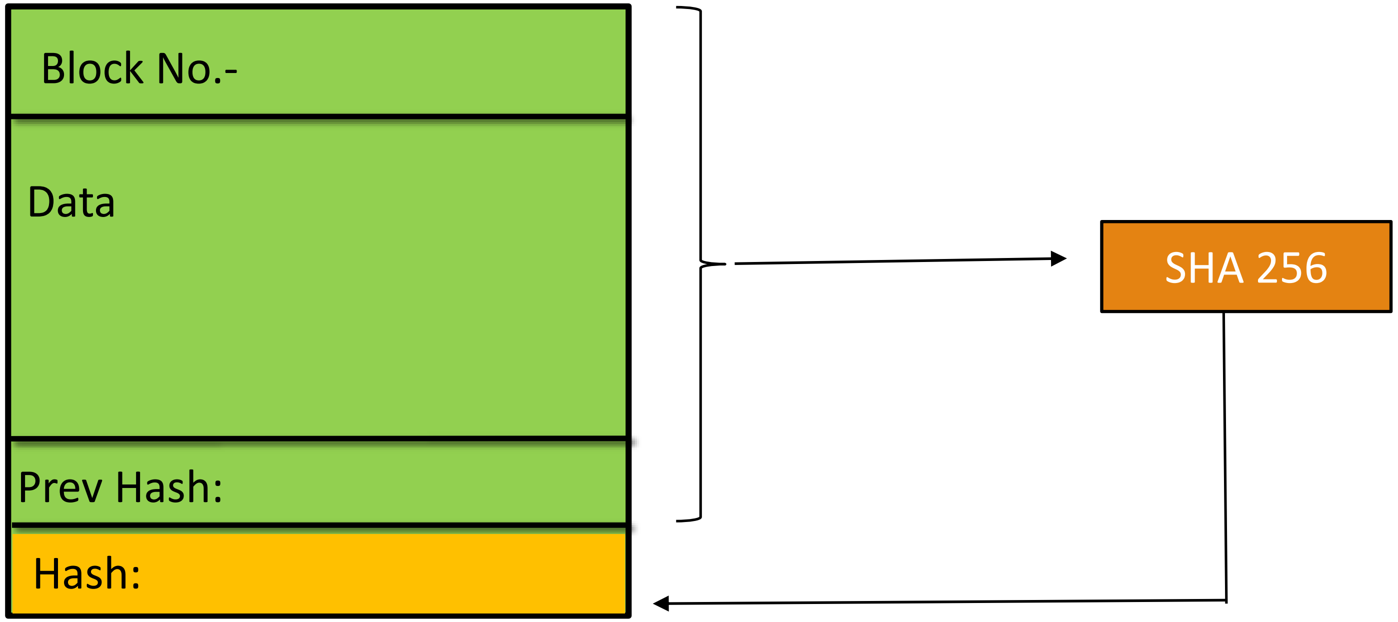
Prev Hash:000000000

Hash:0000D8C42

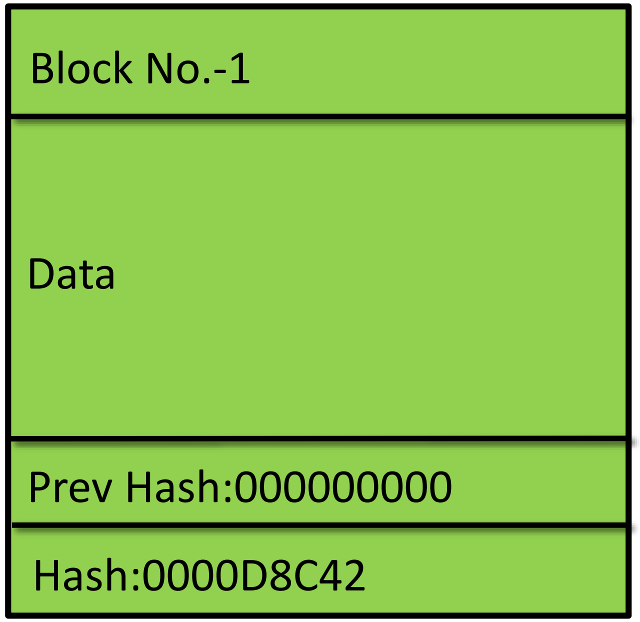
Block

Fingerprint

Hashing Algorithm



Hashing Algorithm



Block No.-1

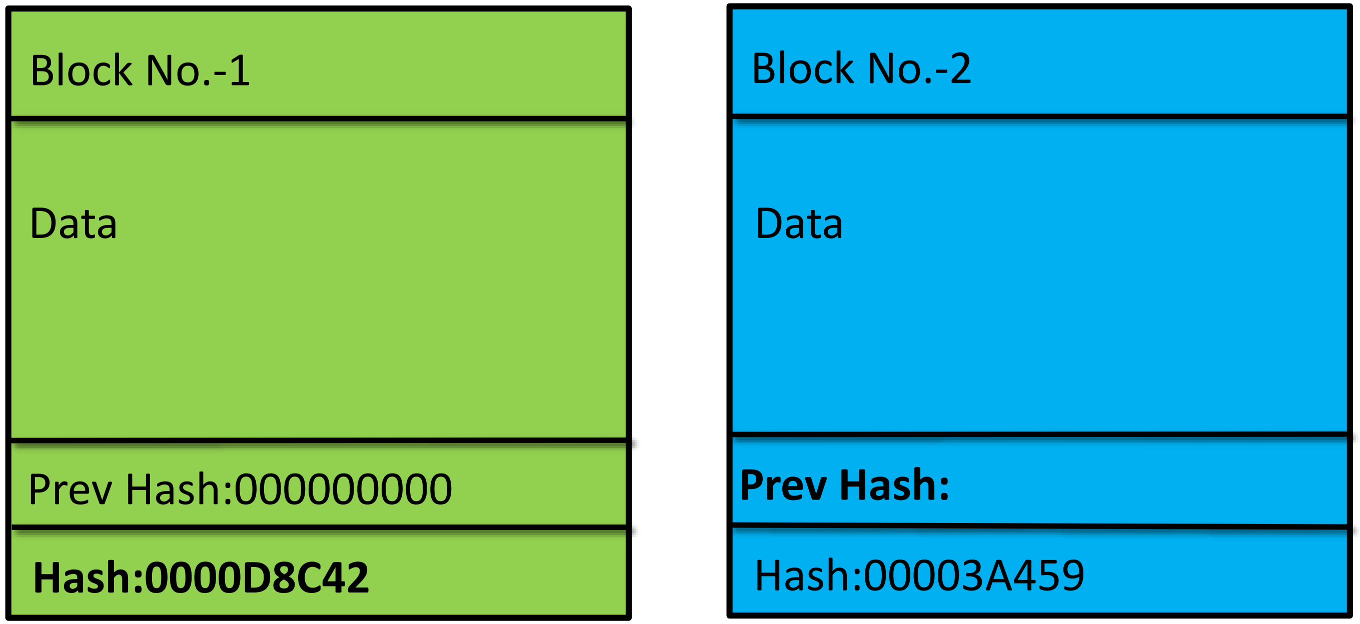
Data

Prev Hash:000000000

Hash:0000D8C42

Block

Hashing Algorithm



Block No.-1

Data

Prev Hash:000000000

Hash:0000D8C42

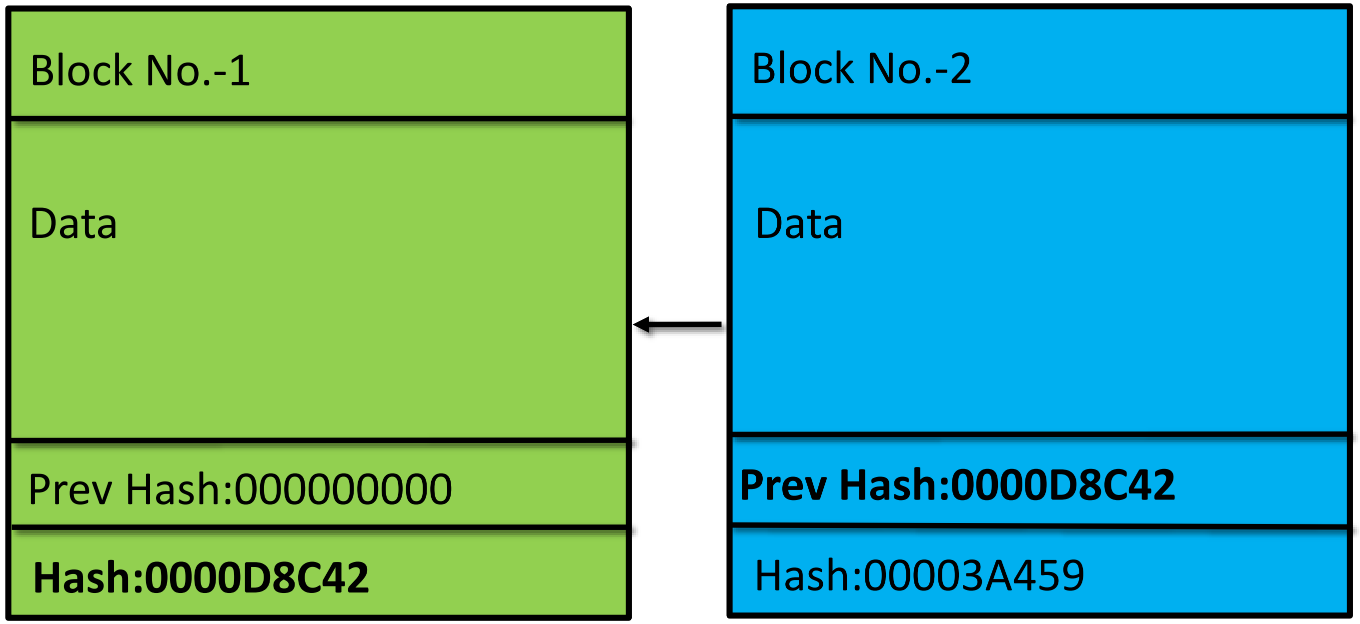
Block No.-2

Data

Prev Hash:

Hash:00003A459

Hashing Algorithm



Block No.-1

Data

Prev Hash:000000000

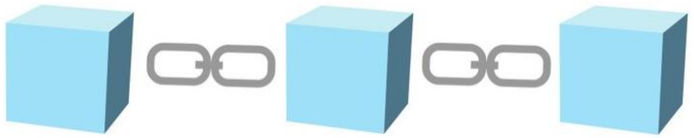
Hash:0000D8C42

Block No.-2

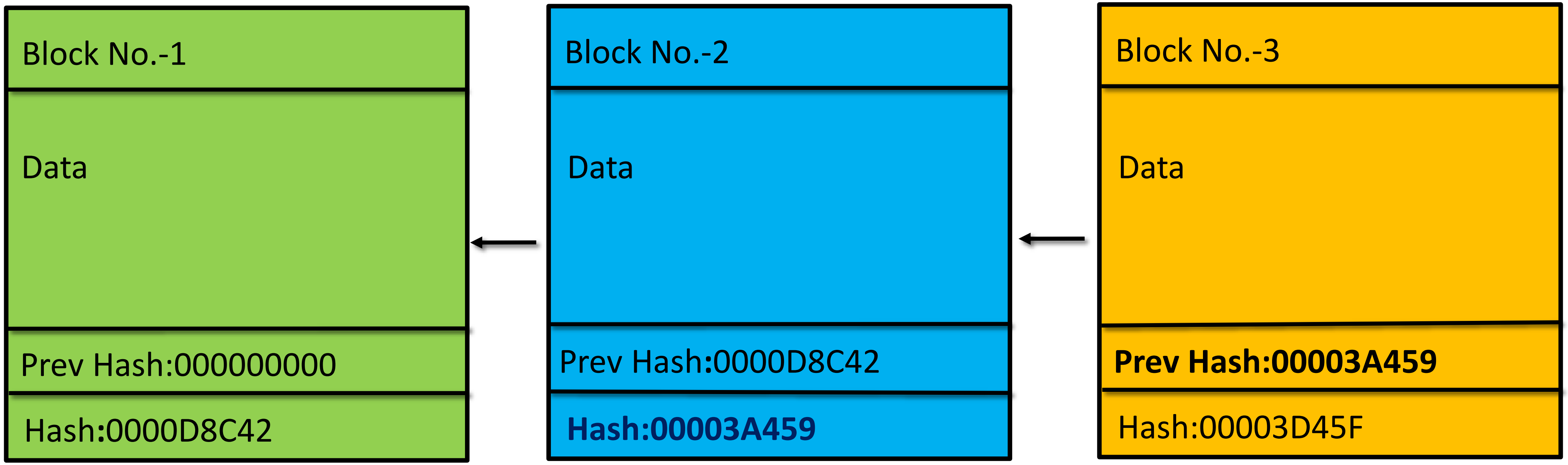
Data

Prev Hash:0000D8C42

Hash:00003A459



Hashing Algorithm



Block No.-1

Data

Prev Hash:000000000

Hash:0000D8C42

Block No.-2

Data

Prev Hash:0000D8C42

Hash:00003A459

Block No.-3

Data

Prev Hash:00003A459

Hash:00003D45F

Genesis Block

Hashing Algorithm Demo

Online demonstration (Hash, Block and Blockchain)

https://andersbrownworth.com/blockchain/

Running your Node Server

https://github.com/anders94/blockchain-demo/

Immutable Ledger

Immutable Ledger

- Consider you want to buy a house for yourself.
- You need cash, and a contract
- Submit the documents to government institution for registration
- The information is recorded either in a register book or centralized database

Money

Sales Deed

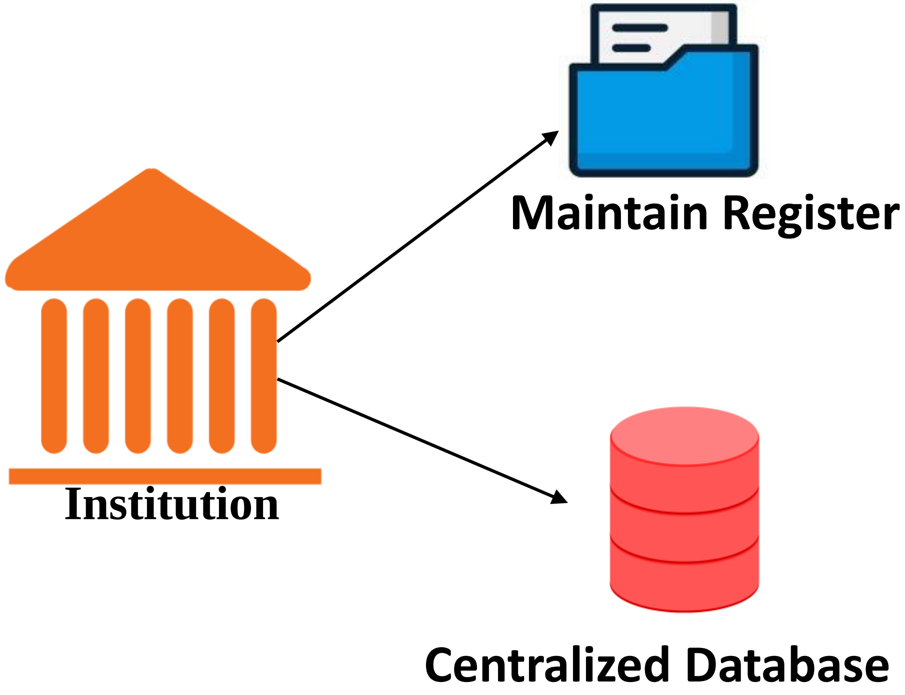
Institution

House

Immutable Ledger

- **Register book:**
  - The register can be destroyed
  - Easily altered by someone
- **Centralized database:**
  - The record can be hacked and changed
  - The government employee can change the record

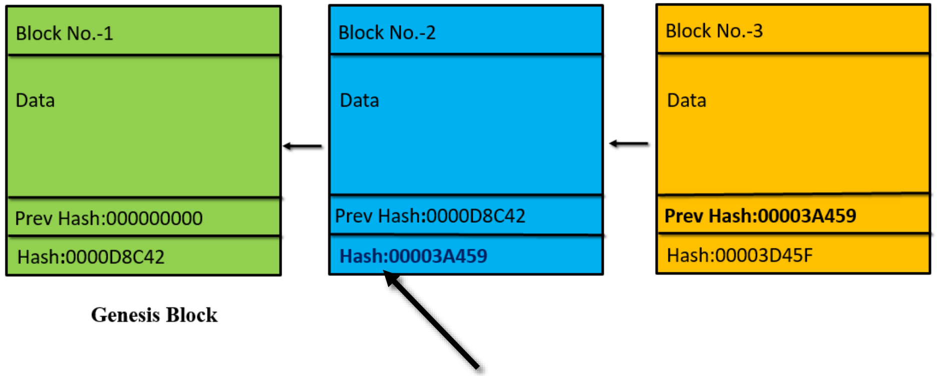
Let’s check, the Immutable register on Blockchain



Immutable Ledger

- If the hacker changes block C
- All the blocks after block C will be corrupted

Hashing Algorithm



Block No.-1

Data

Prev Hash:000000000

Hash:0000D8C42

Genesis Block

Block No.-2

Data

Prev Hash:0000D8C42

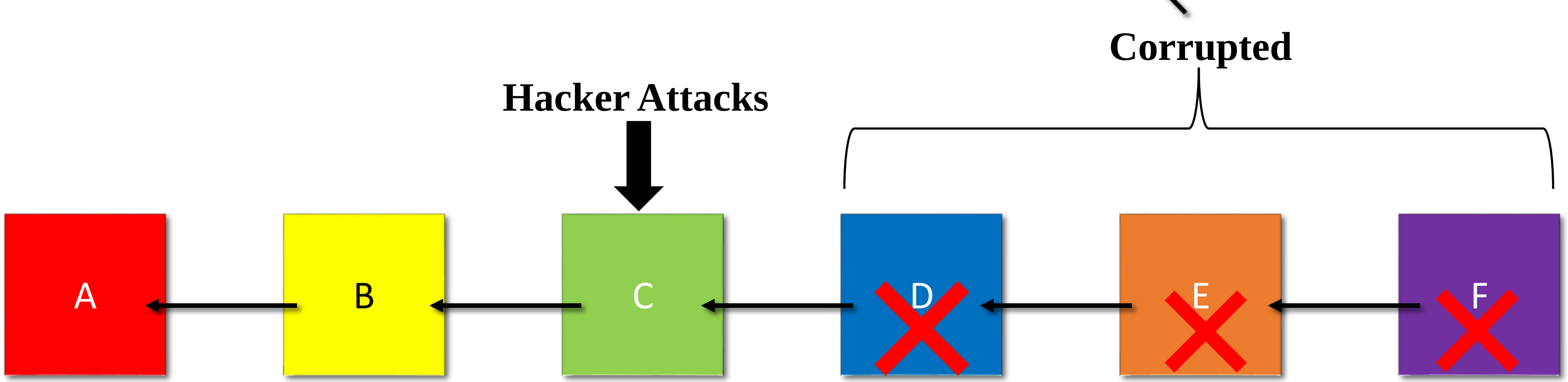
Hash:00003A459

Block No.-3

Data

Prev Hash:00003A459

Hash:00003D45F



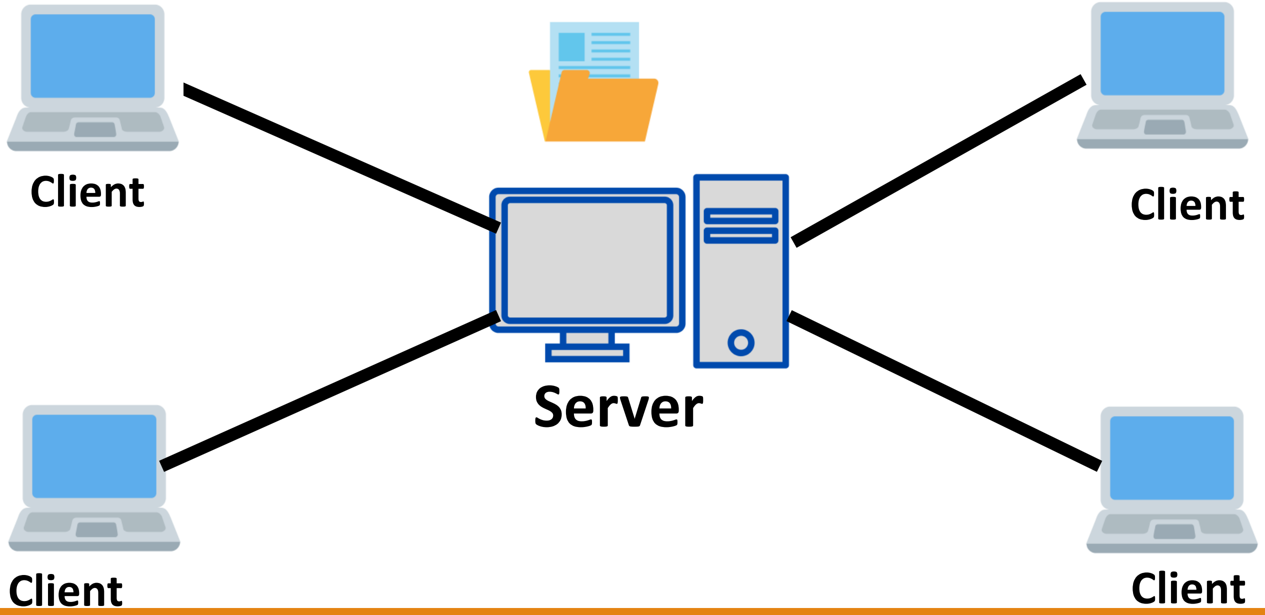
Corrupted

Hacker Attacks

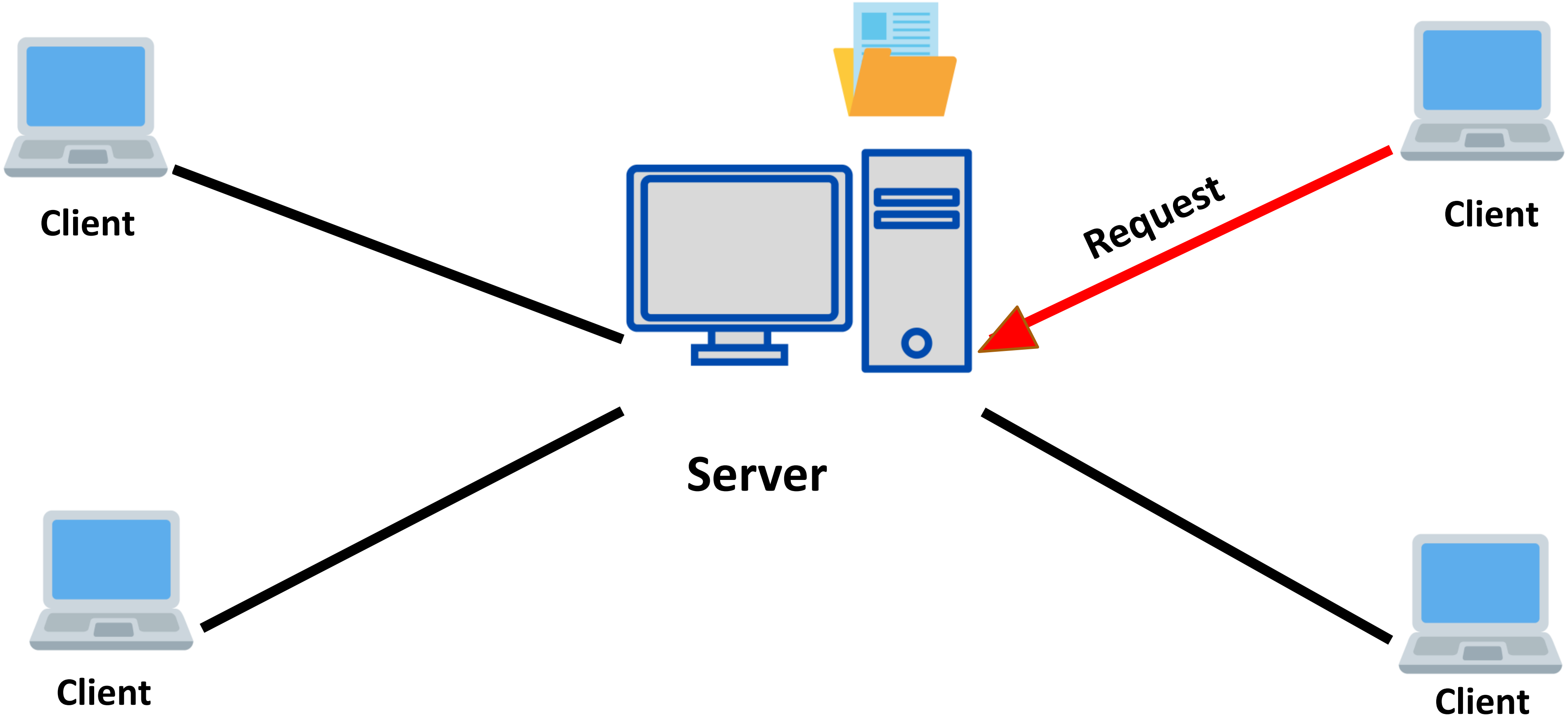
What is a P2P network?

What is a Centralized Network?

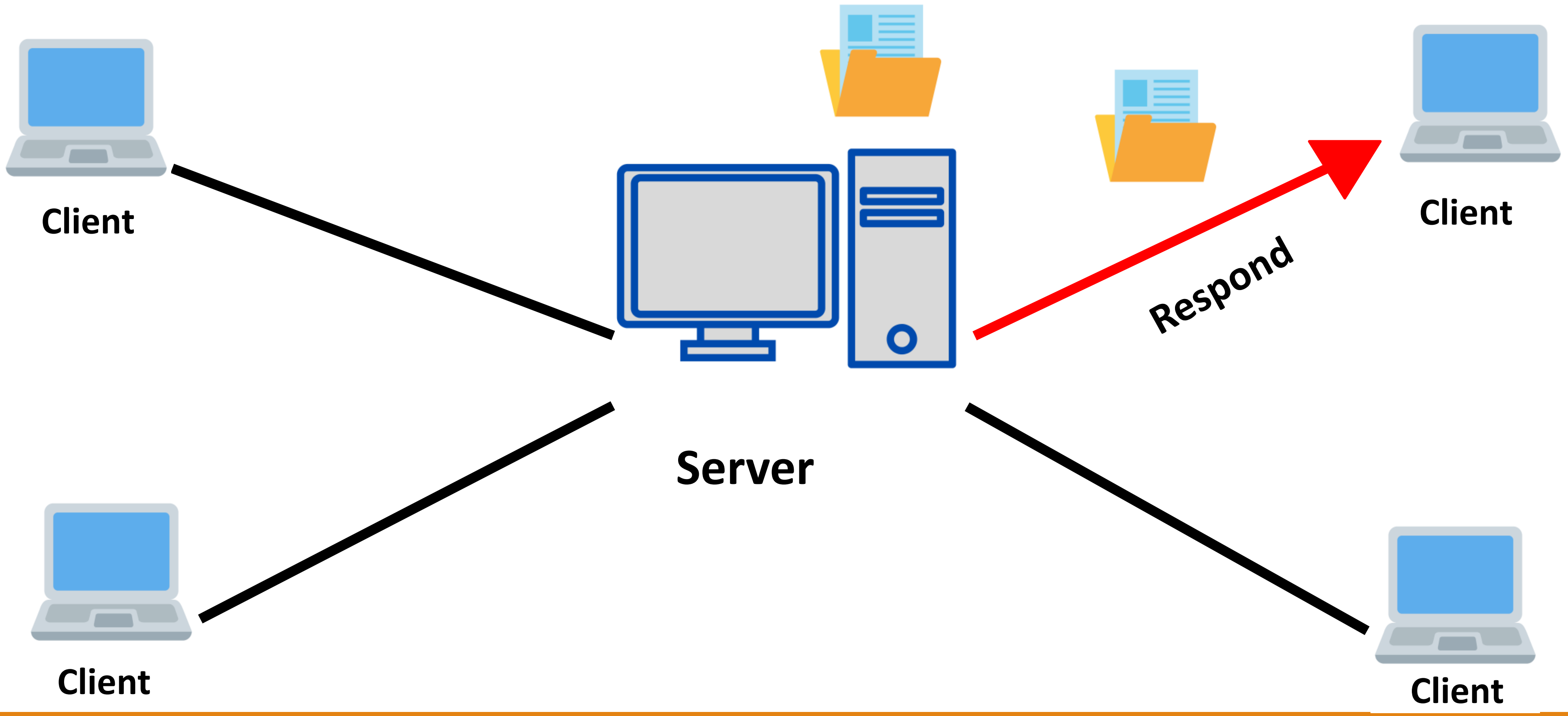
- Client Server Model
- Data stored on Server
- Client requests data from Server
- Server sends client the required data
- Hacker can easily hacks the Server and corrupts the data
- i.e. Banks, Social Networks, etc.



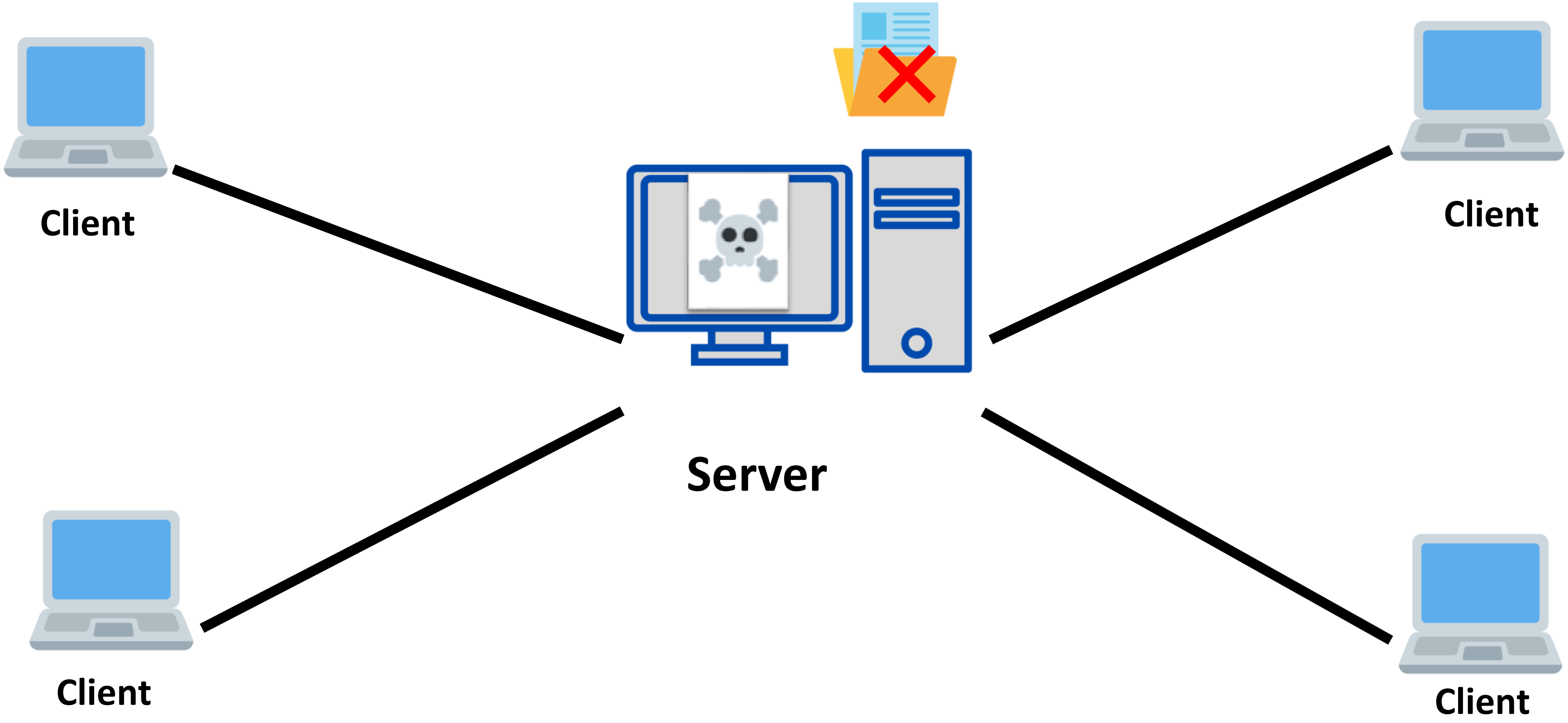
What is a Centralized Network?



What is a Centralized Network?



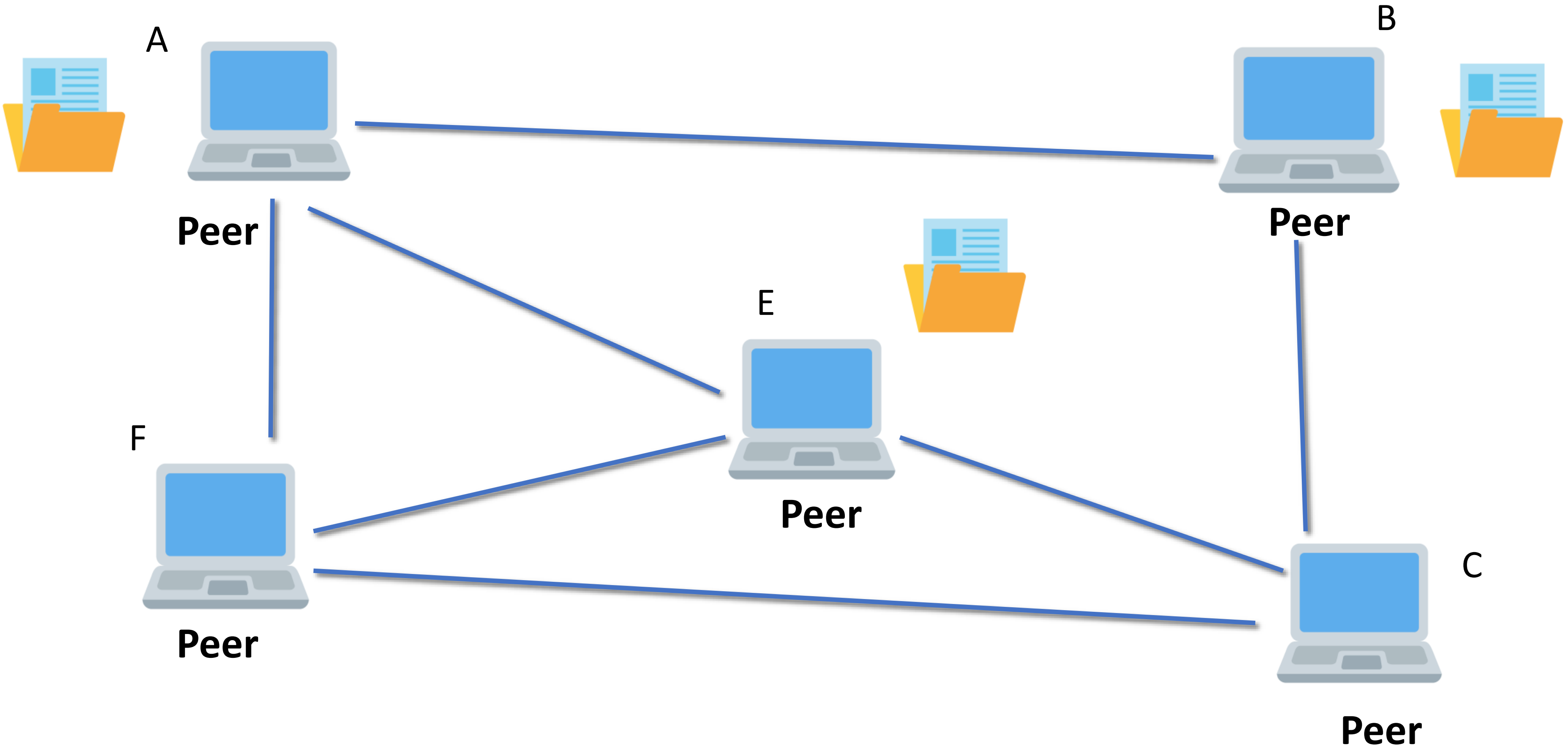
What is a centralized network?



Distributed P2P network

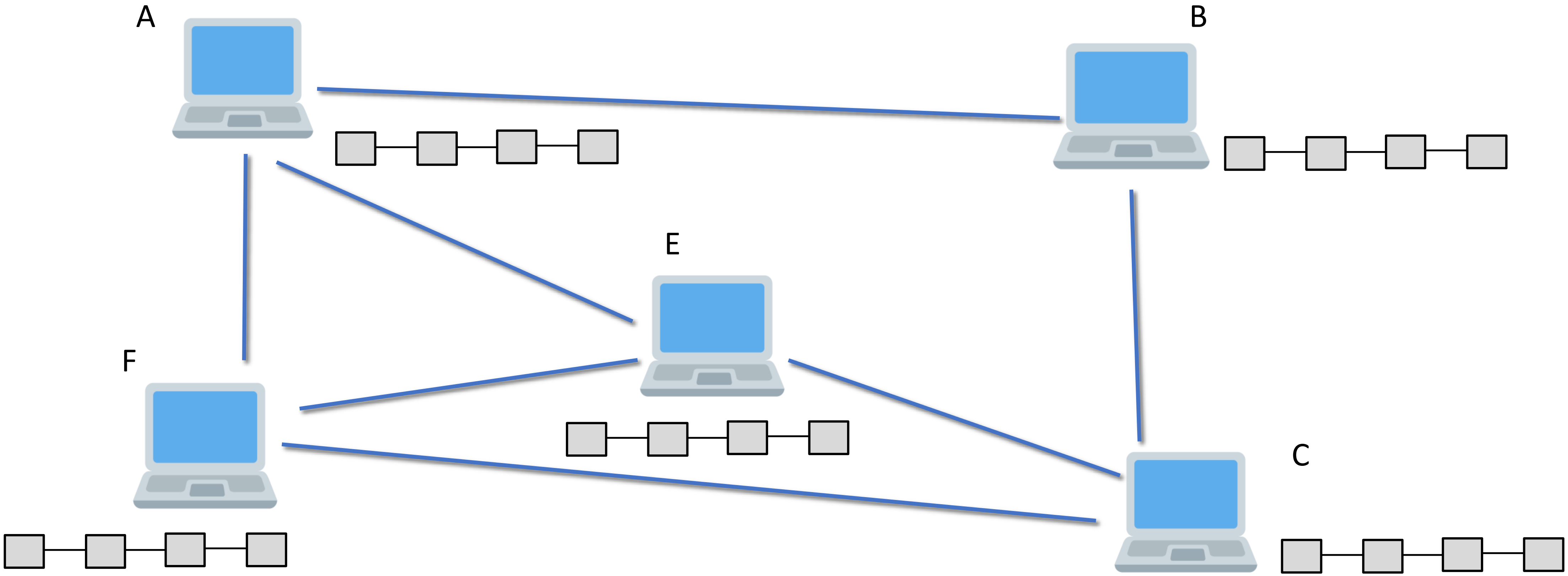
- No client and no server
- All peer are equal
- The data is stored with multiple peers
- Peers directly request data from each other
- Hacker has to hack all the peer simultaneously, to corrupt the data, which is almost impossible

Distributed P2P network

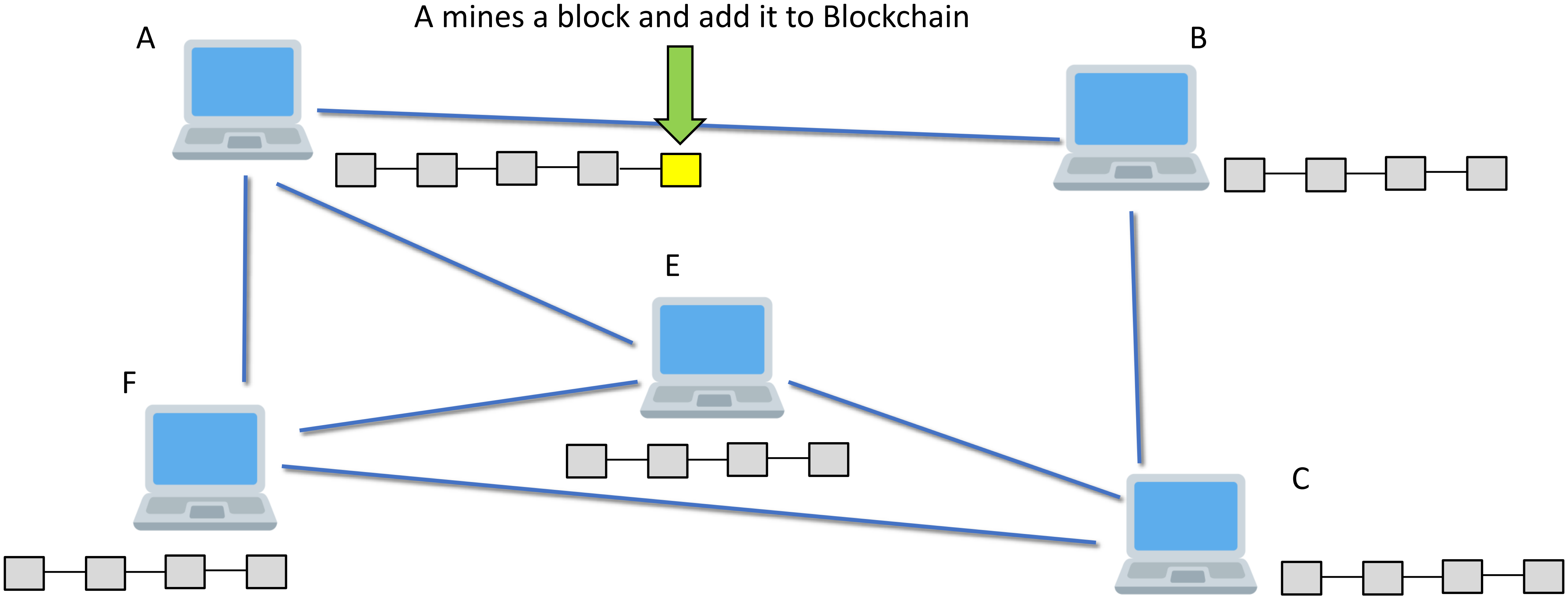


Distributed P2P network in Blockchain

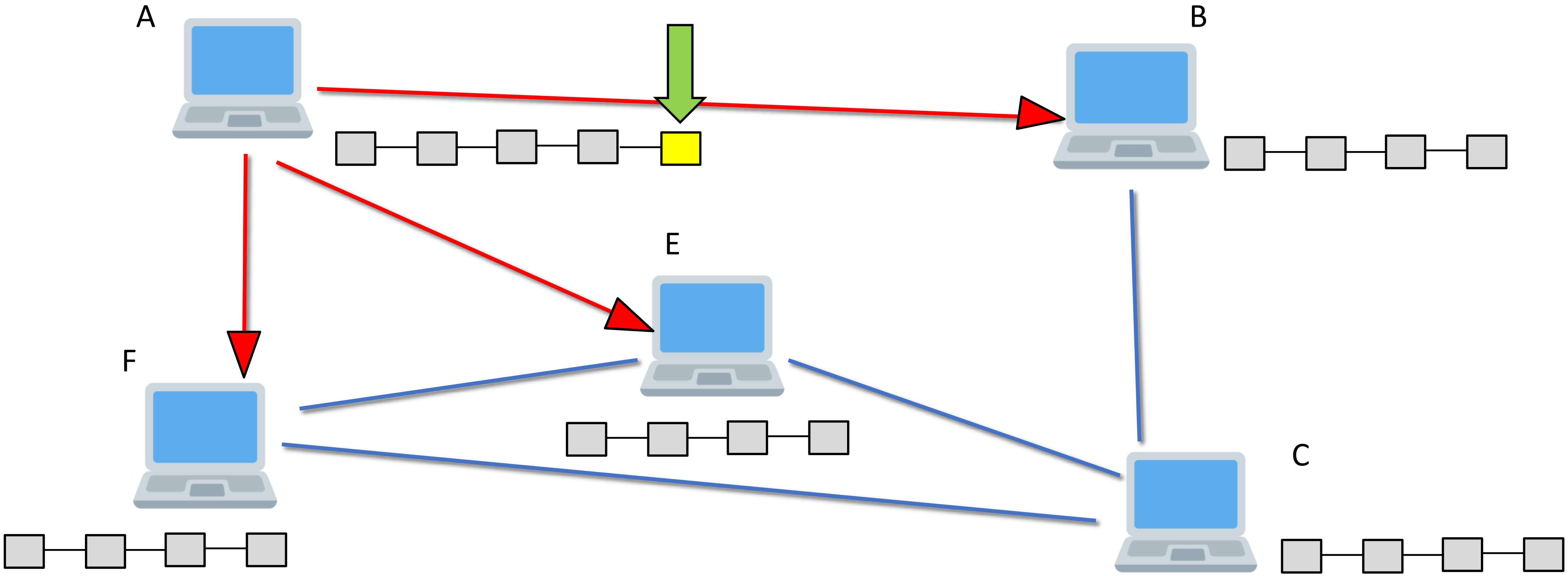
Distributed P2P network



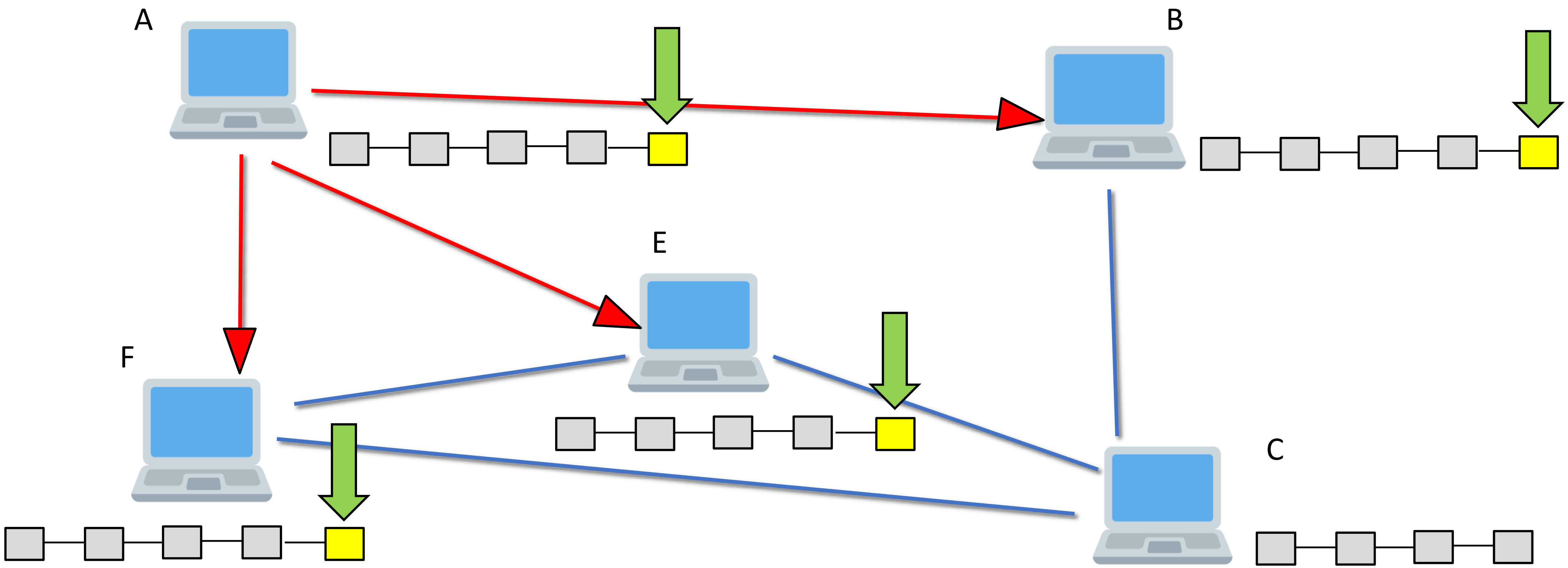
Distributed P2P network



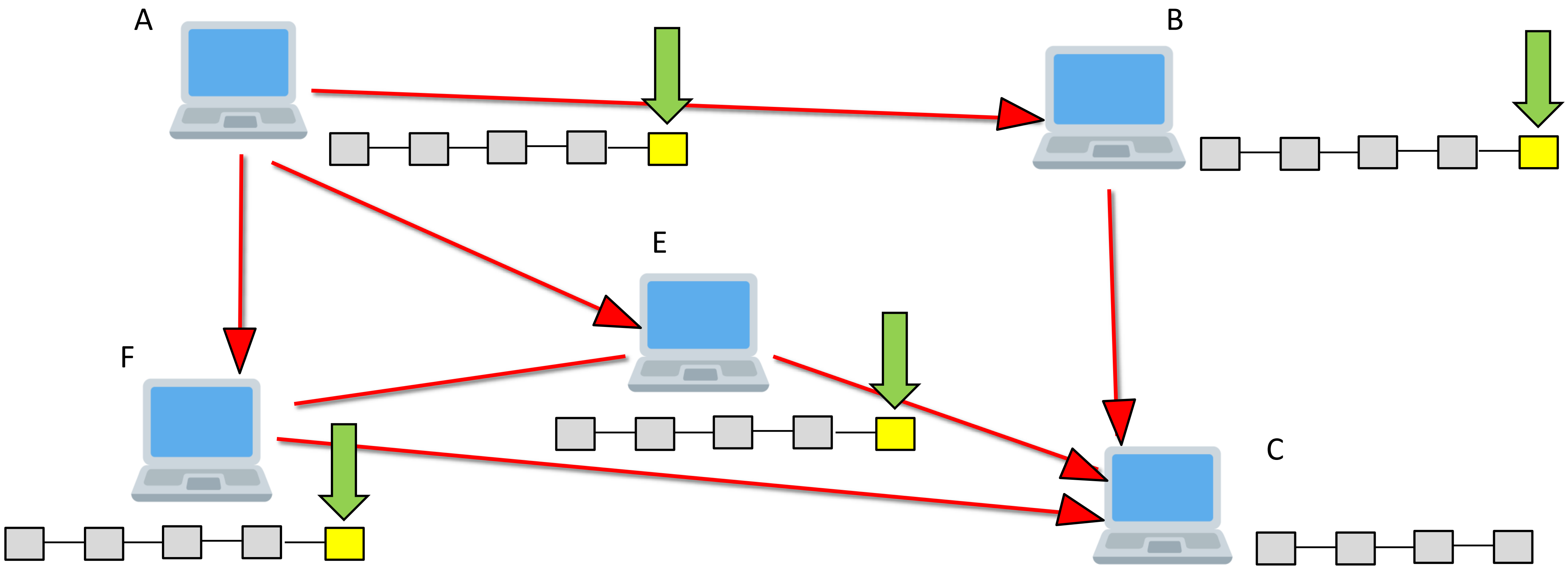
Distributed P2P network



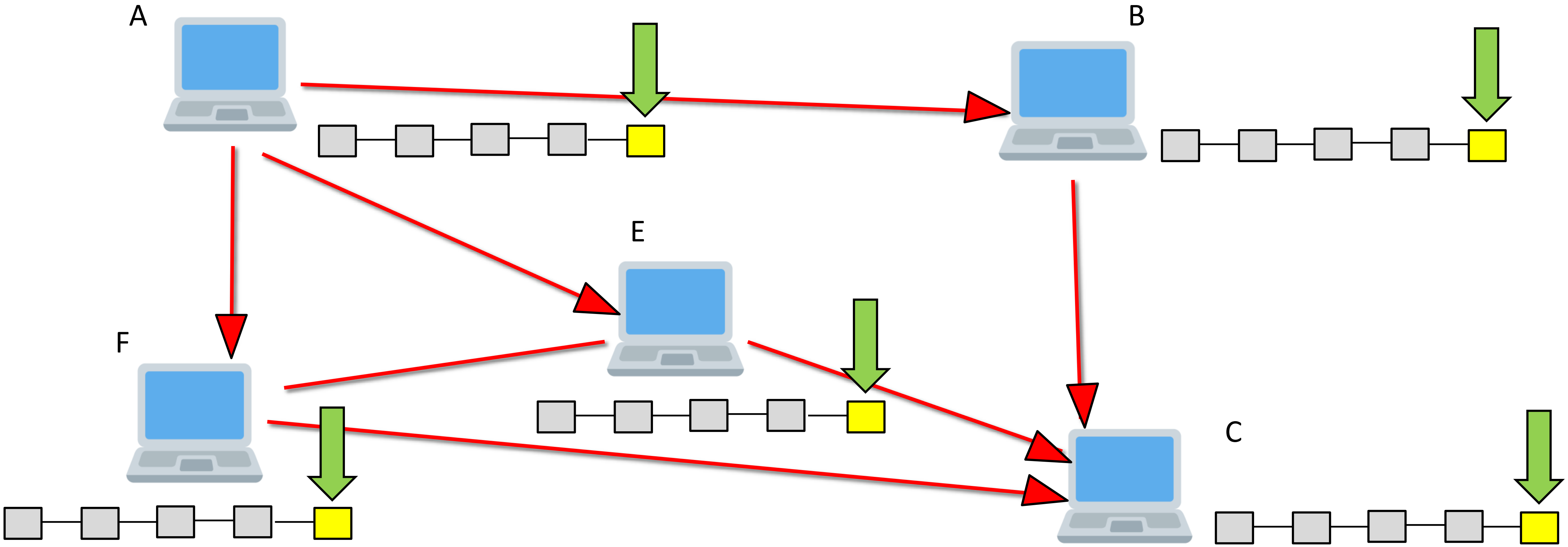
Distributed P2P network



Distributed P2P network



Distributed P2P network



Distributed P2P network

Q)Why we need Distributed P2P network in Blockchain?

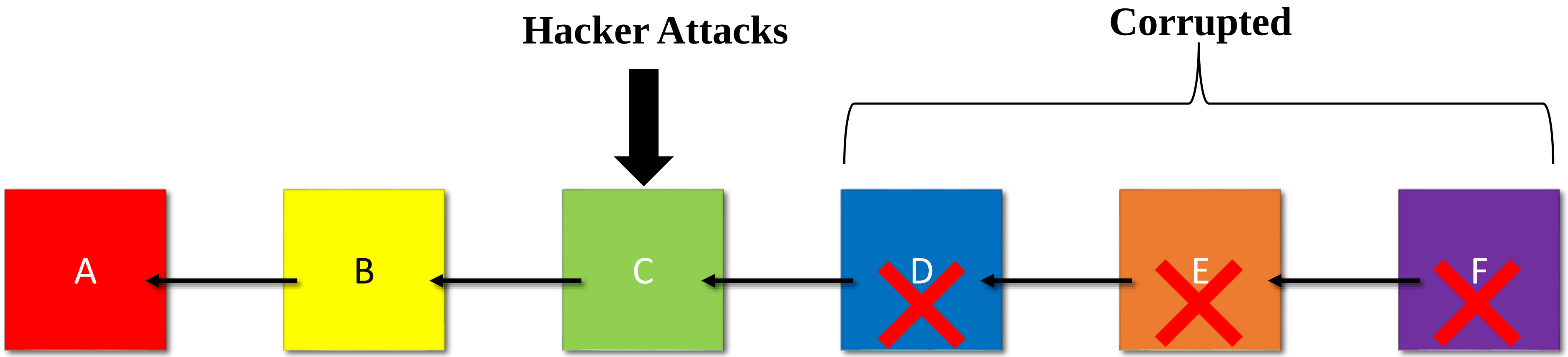
- To resist tempering in a Blockchain
- To recover tempered data

Distributed P2P network

How data is recovered using Distributed P2P network.

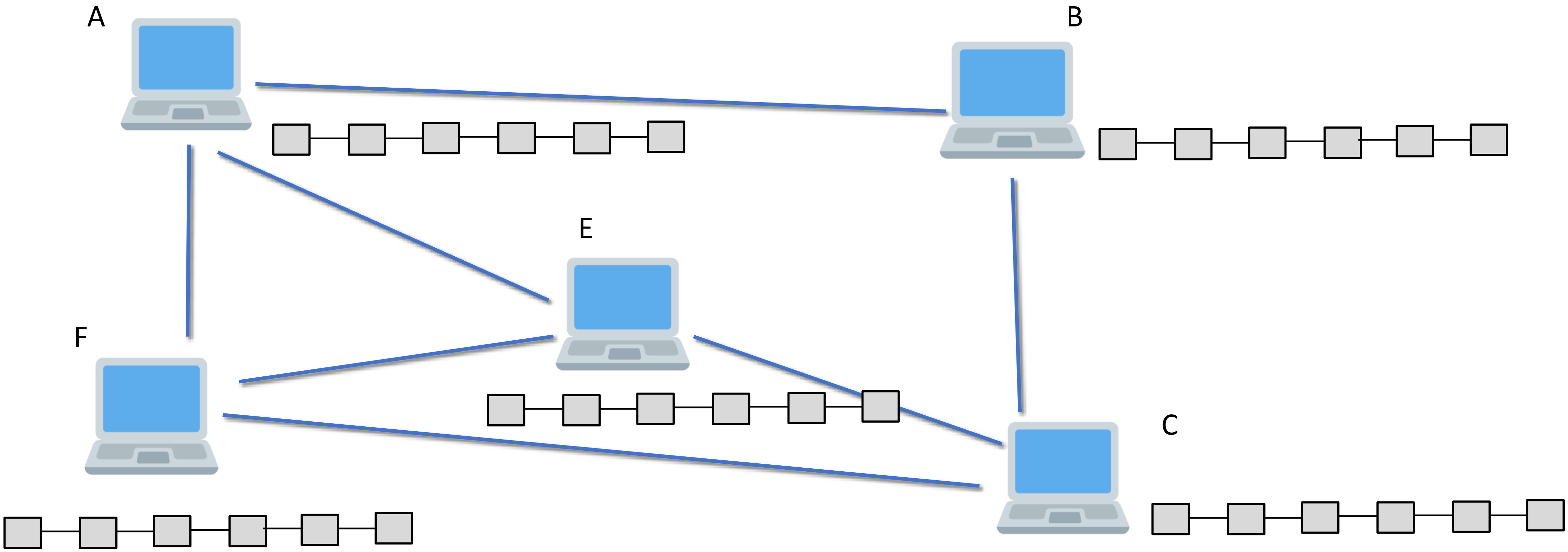
- If hacker change a block of a specific node
- The change is reflected in the succeeding blocks
- Thus, it will invalidate all the succeeding blocks
- However, if a hacker is smarter, he will also change the succeeding blocks
- The other peers will update the node that your blocks are changed
- The chain will be recovered back

Distributed P2P network

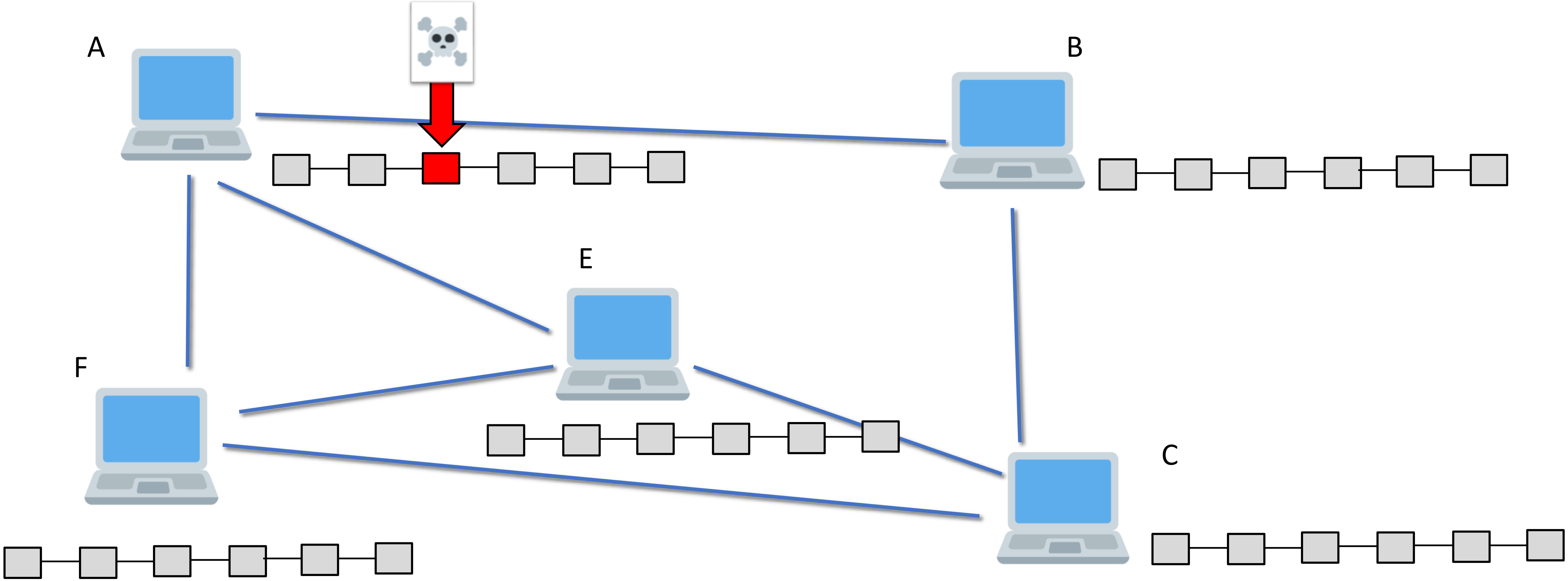


Concept of Immutability

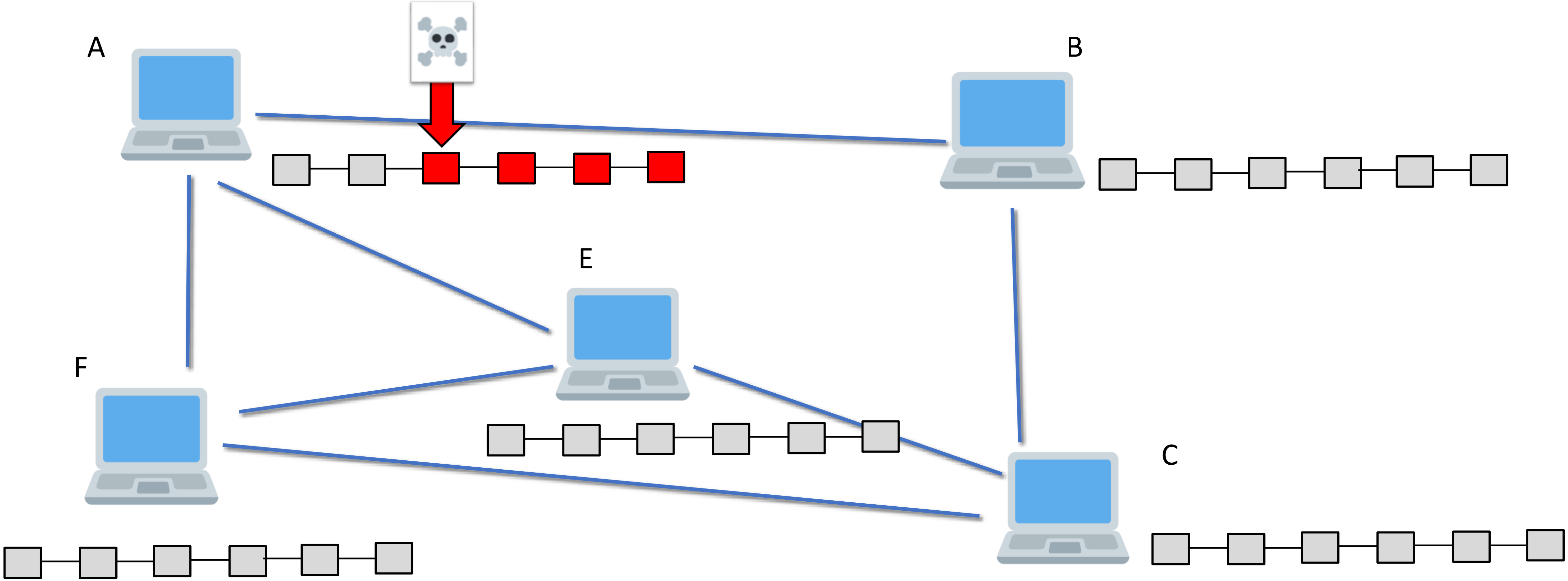
Distributed P2P network



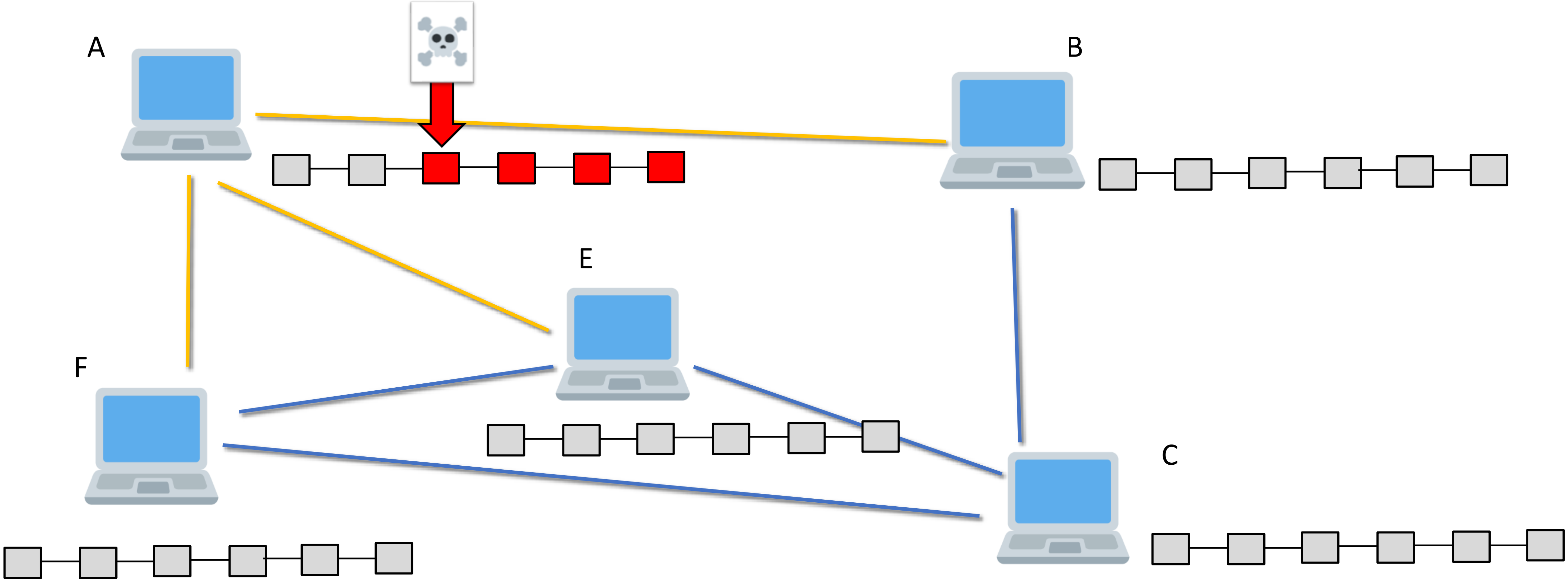
Distributed P2P network



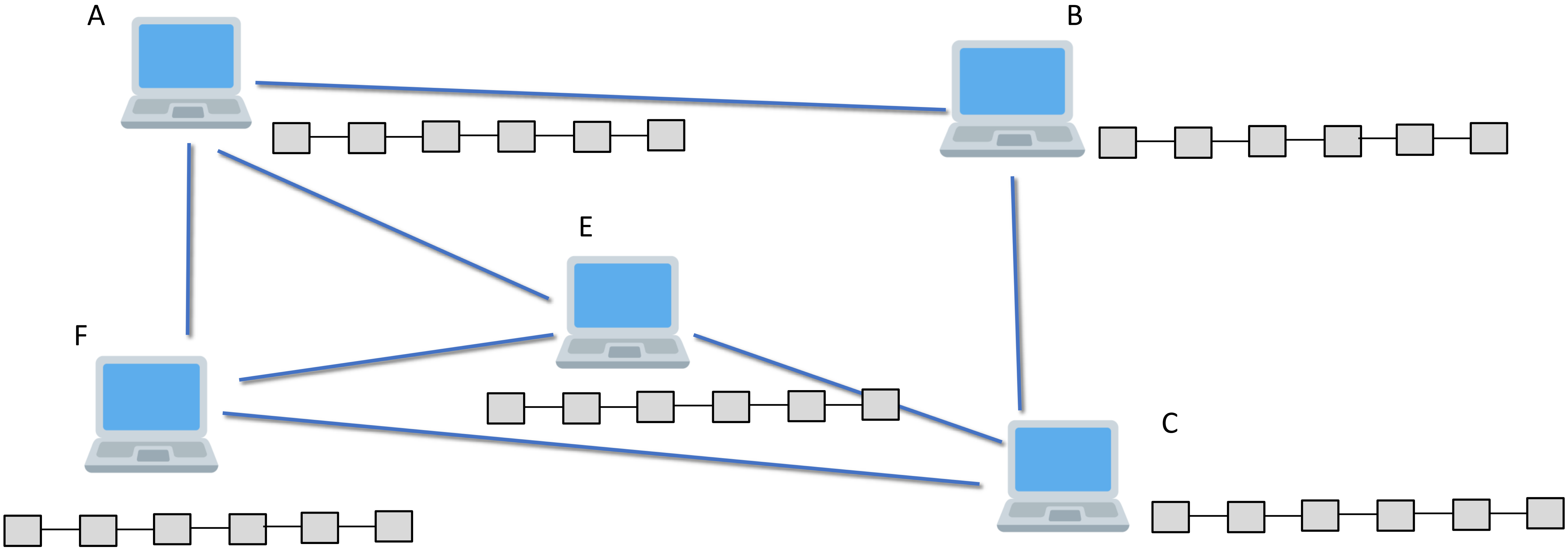
Distributed P2P network



Distributed P2P network



Distributed P2P network



Hashing Algorithm Demo

Online demonstration (Distributed Blockchain)

https://andersbrownworth.com/blockchain/

Running your Node Server

https://github.com/anders94/blockchain-demo/