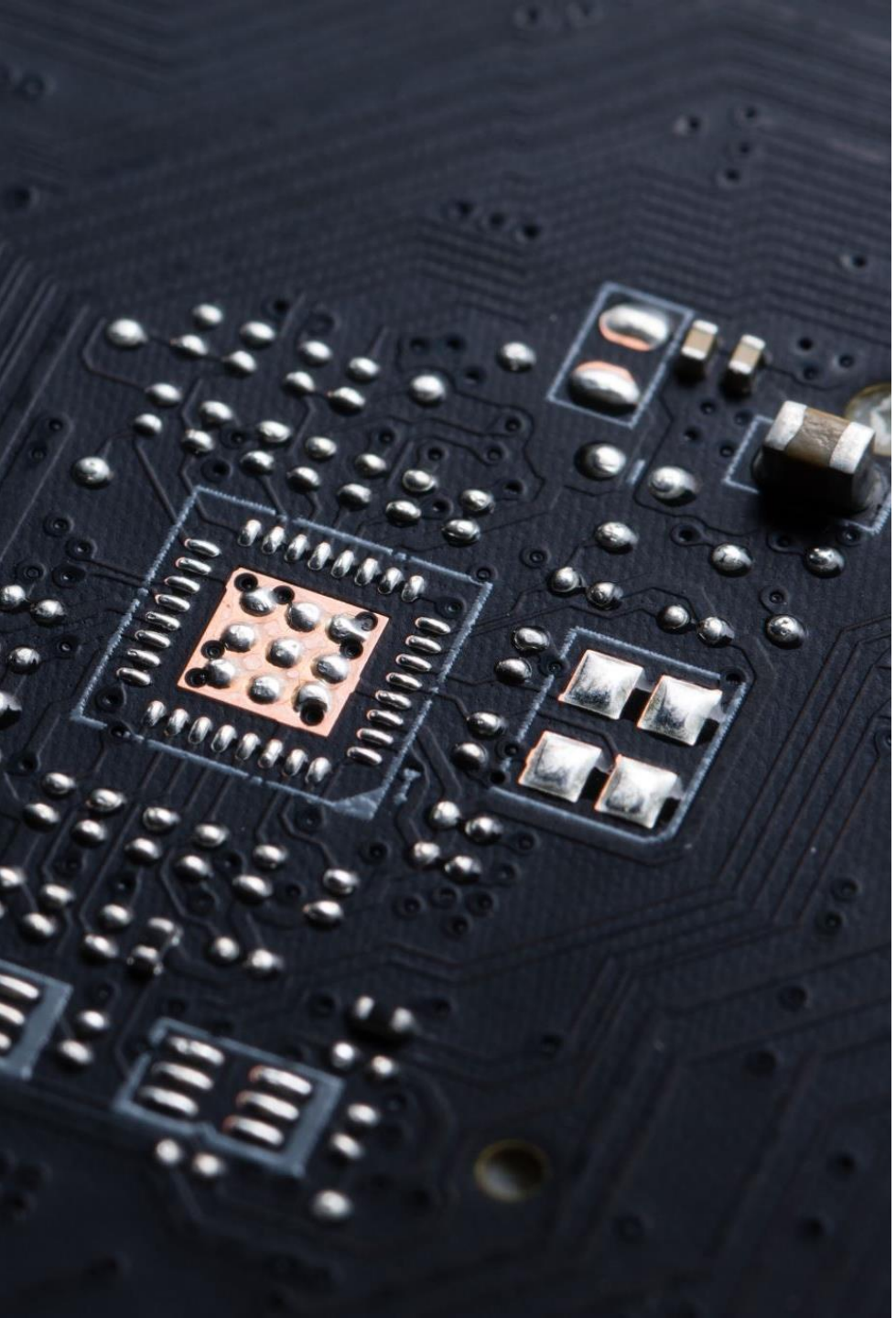
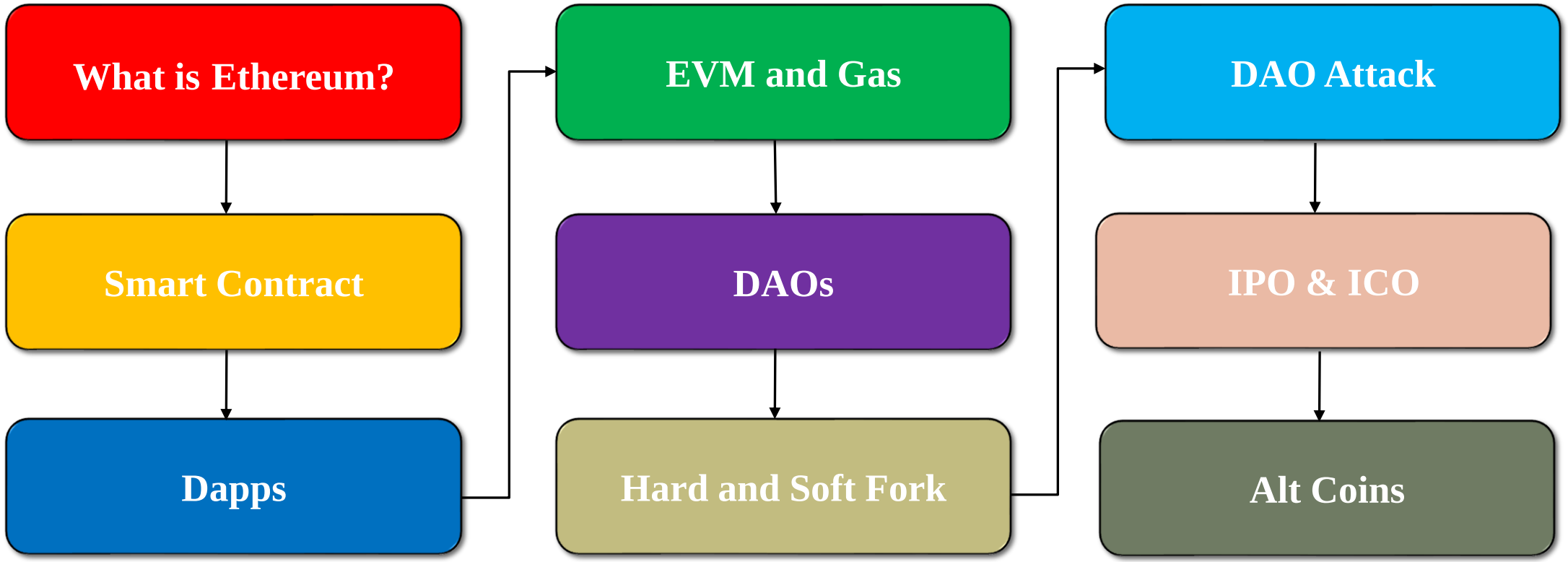
Blockchain

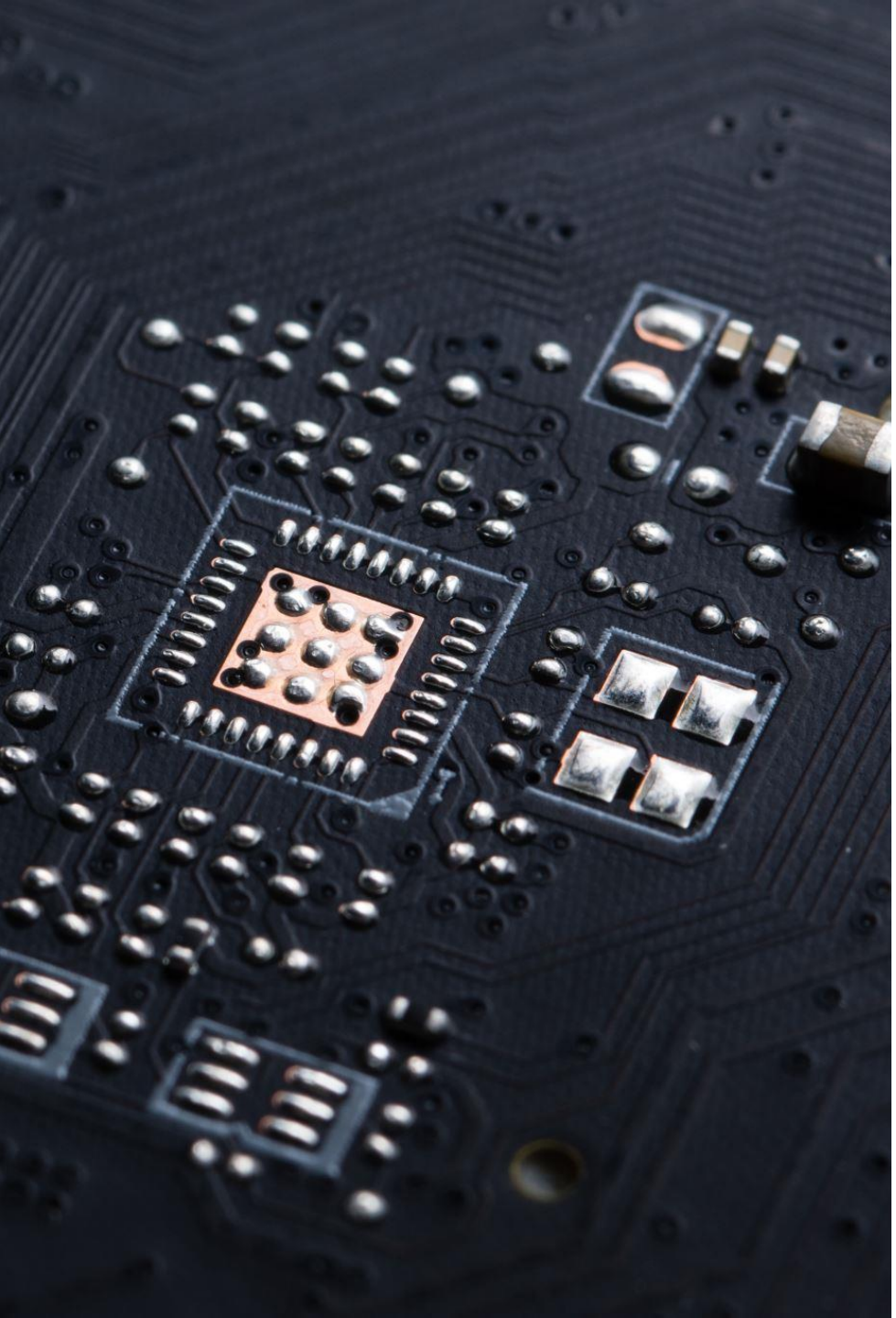
Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.



Ethereum

Contents – Module C

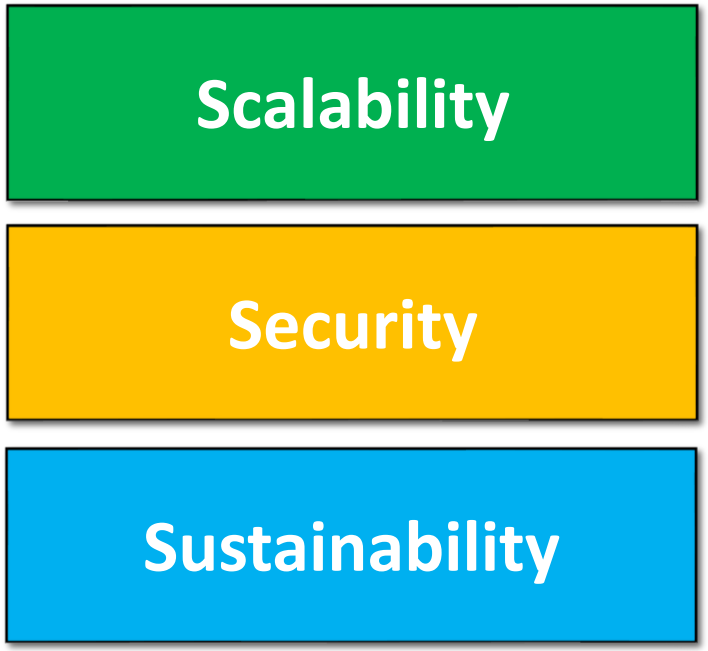




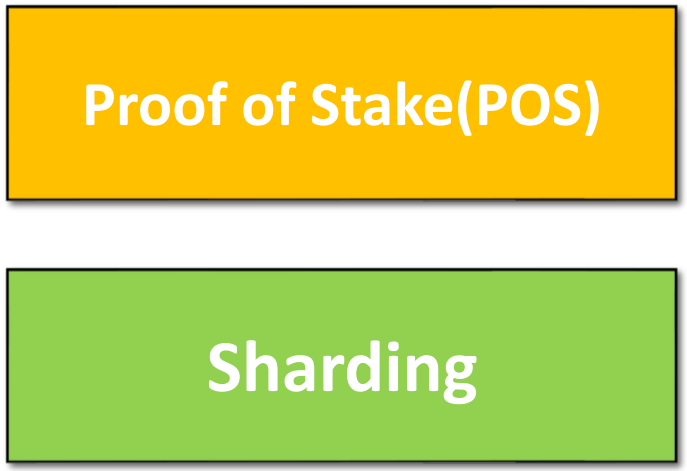
Ethereum 2.0 or Serenity

ETH 2.0

- A new version of Ethereum was introduced
- Aims to improve the network's scalability, sustainability, accessibility, and security



ETH2 Major Upgrades

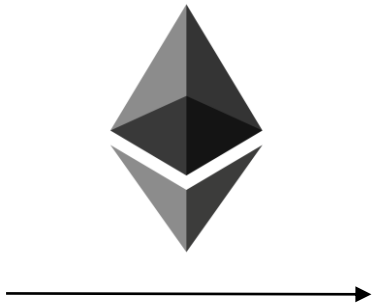


Proof of Stake (POS)

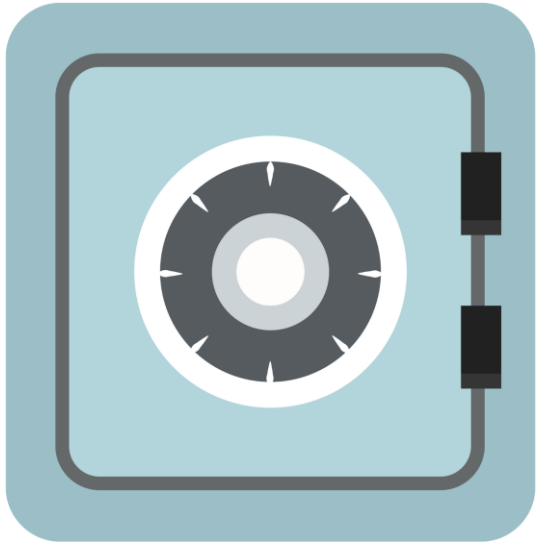
- Proof-of-Stake (PoS) is a consensus mechanism that confirms transactions and creates new blocks through randomly selected validators
- The selection is proportion to the number of holding ethers
- A minimum of 32 ETH is required to become a validator
- Block attachment is called attestation in proof of stake
- On successful attachment, the holding ethers are returned, and the transaction fee is paid
- however, on malicious work, the holding ethers are not returned, and maybe the transaction fee is not paid
- POS avoids the computational cost of proof-of-work schemes

Proof of Stake

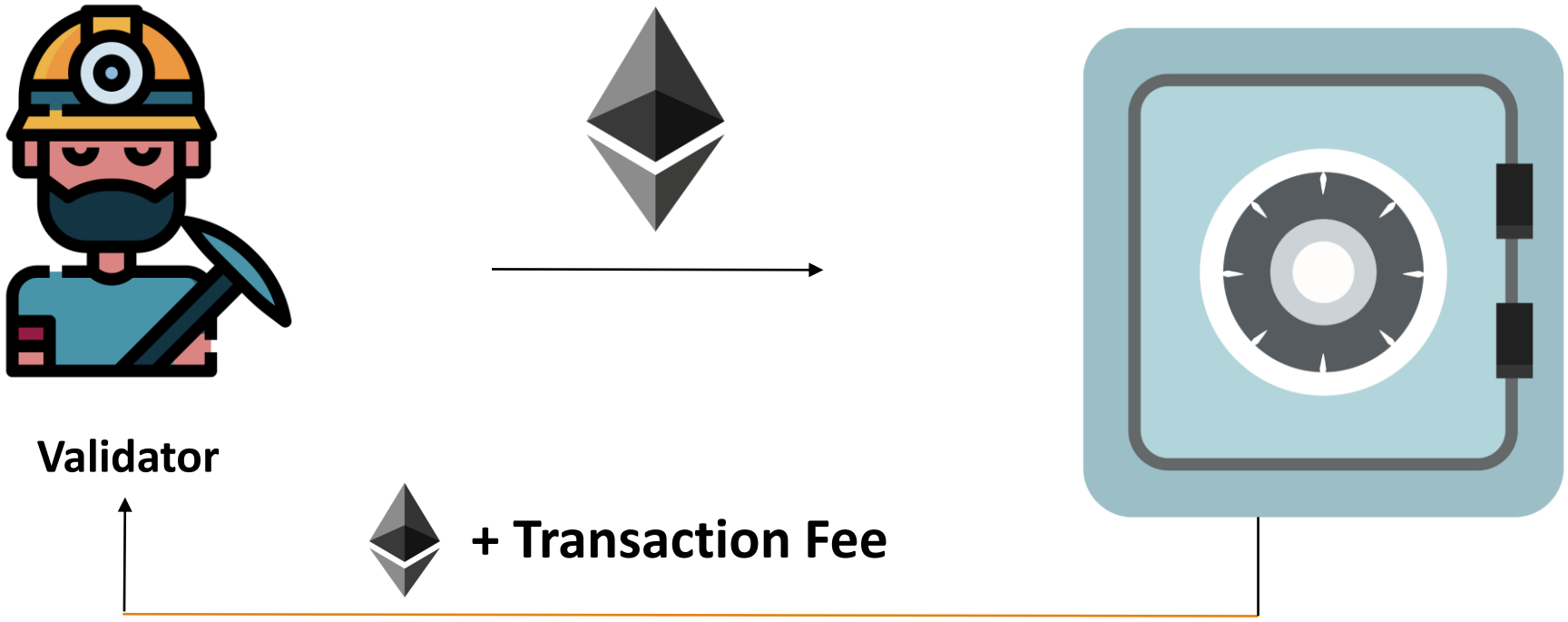
Validator



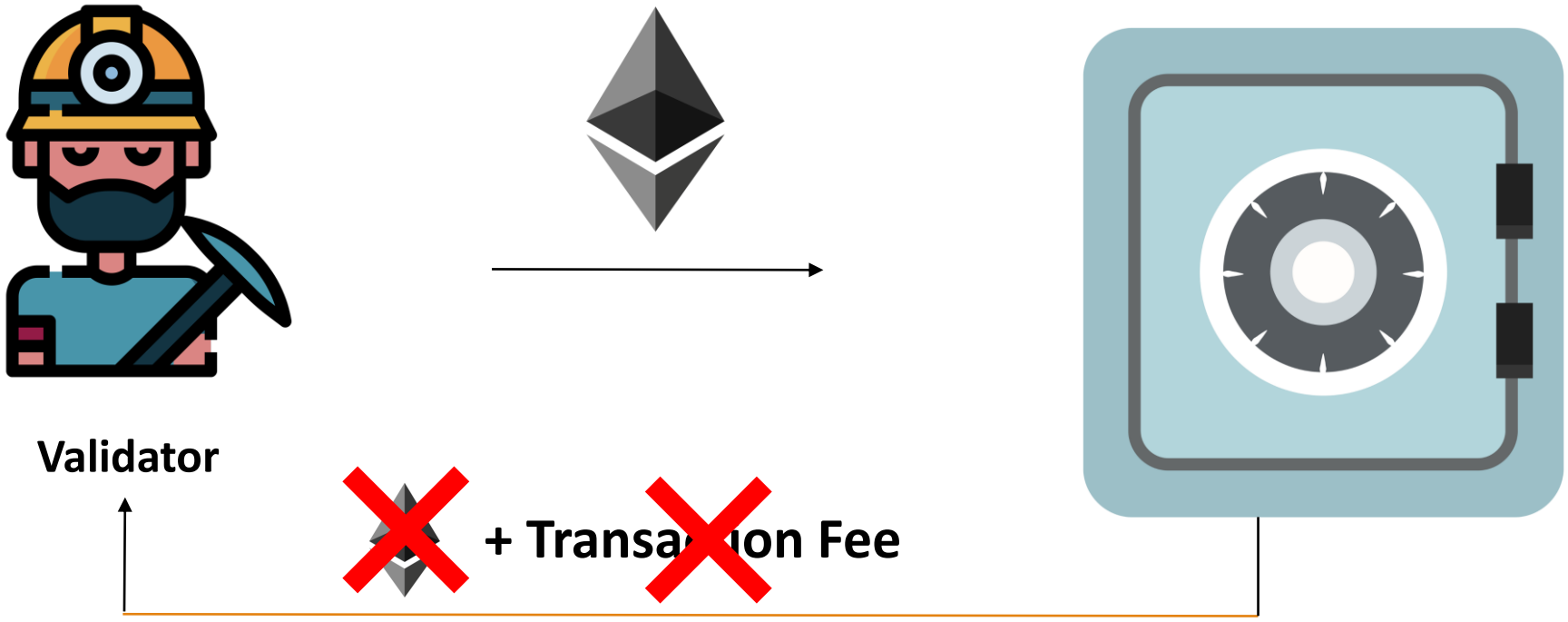
To become a validator, a participant must lock up or "stake" a certain amount of cryptocurrency as collateral.



Proof of Stake

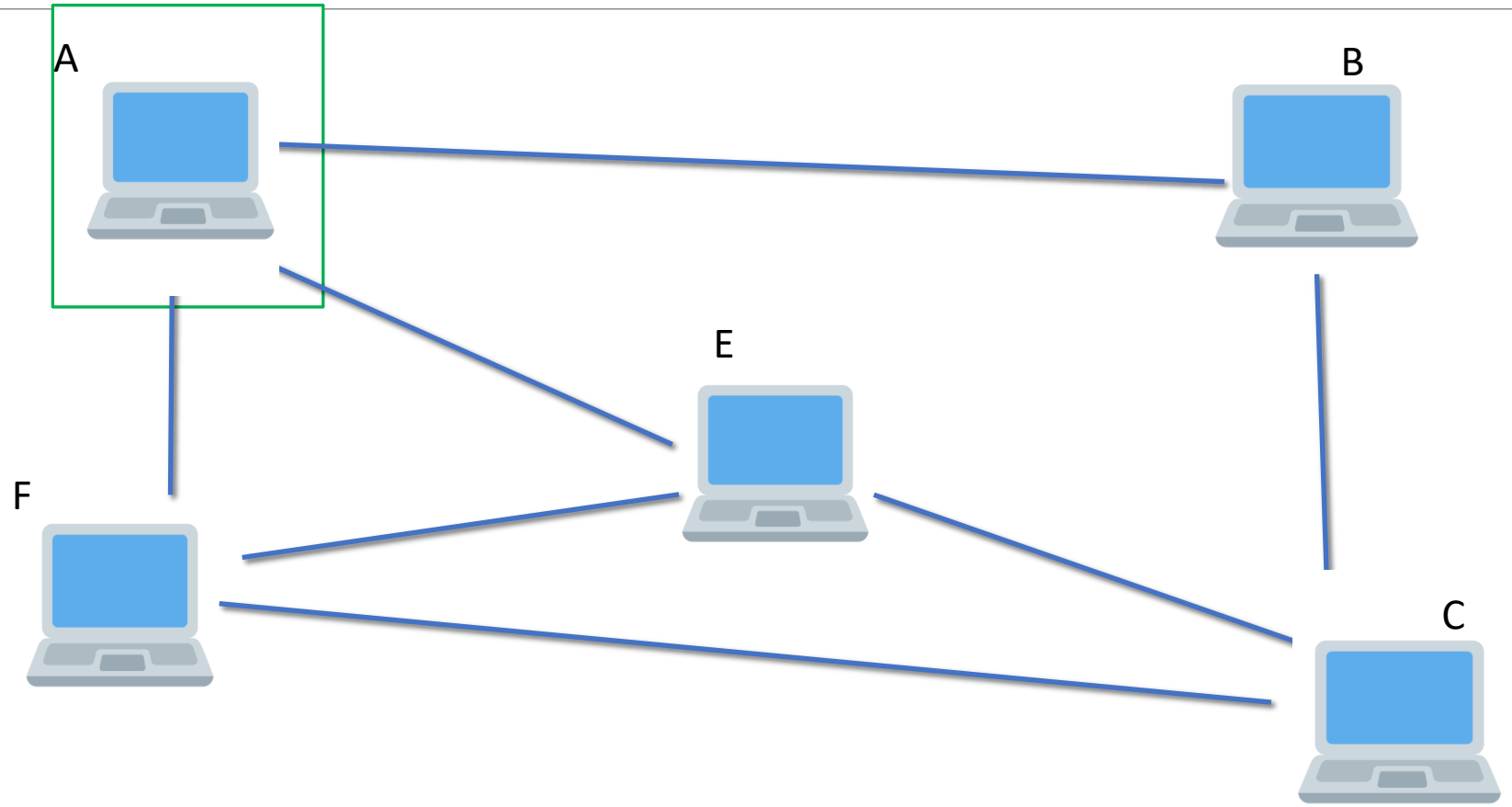


Proof of Stake



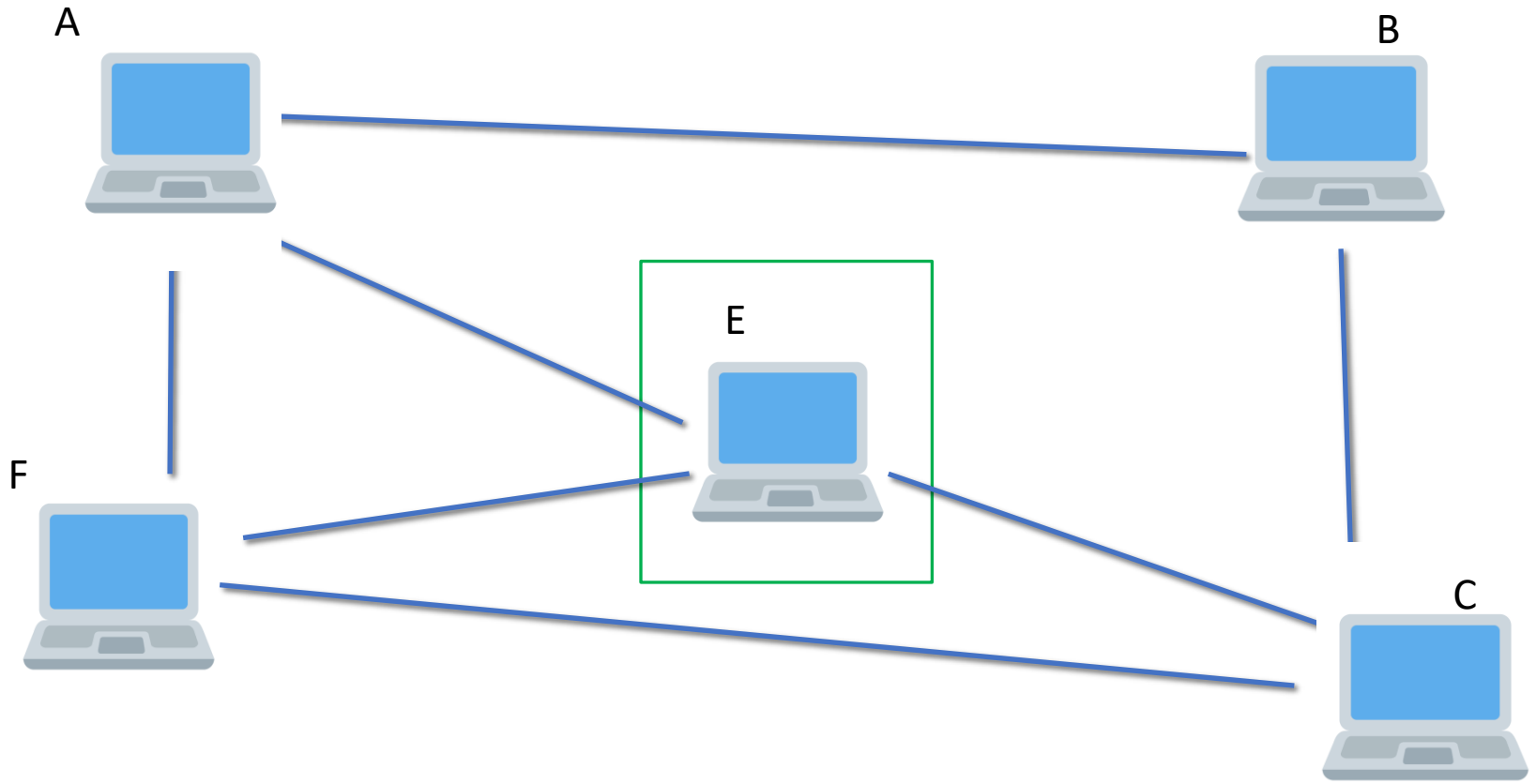
In the case of a Malicious Activity

Proof of Stake



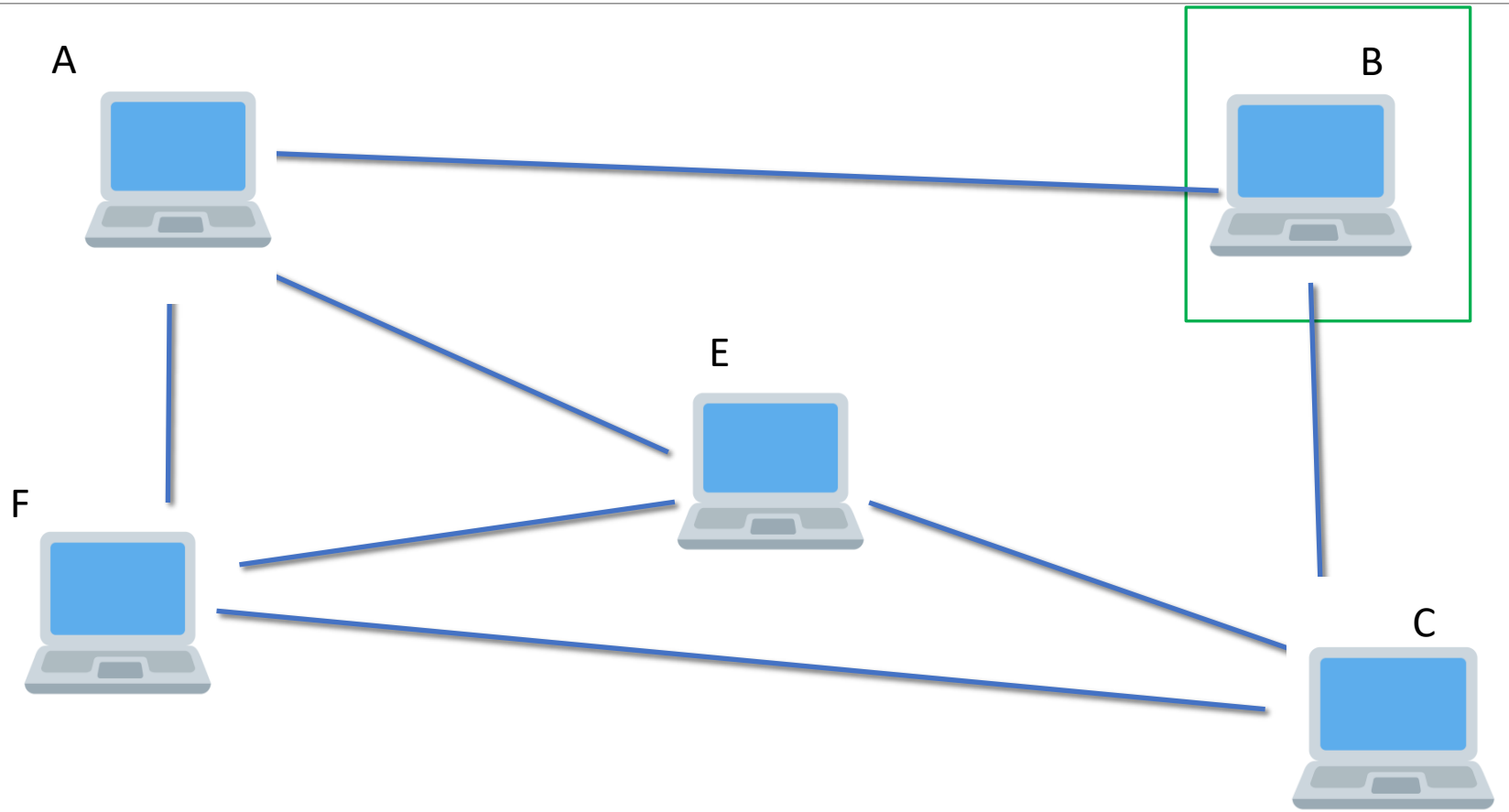
Here System (Protocol) randomly selects a Validator

Proof of Stake



Here System (Protocol) randomly selects a Validator

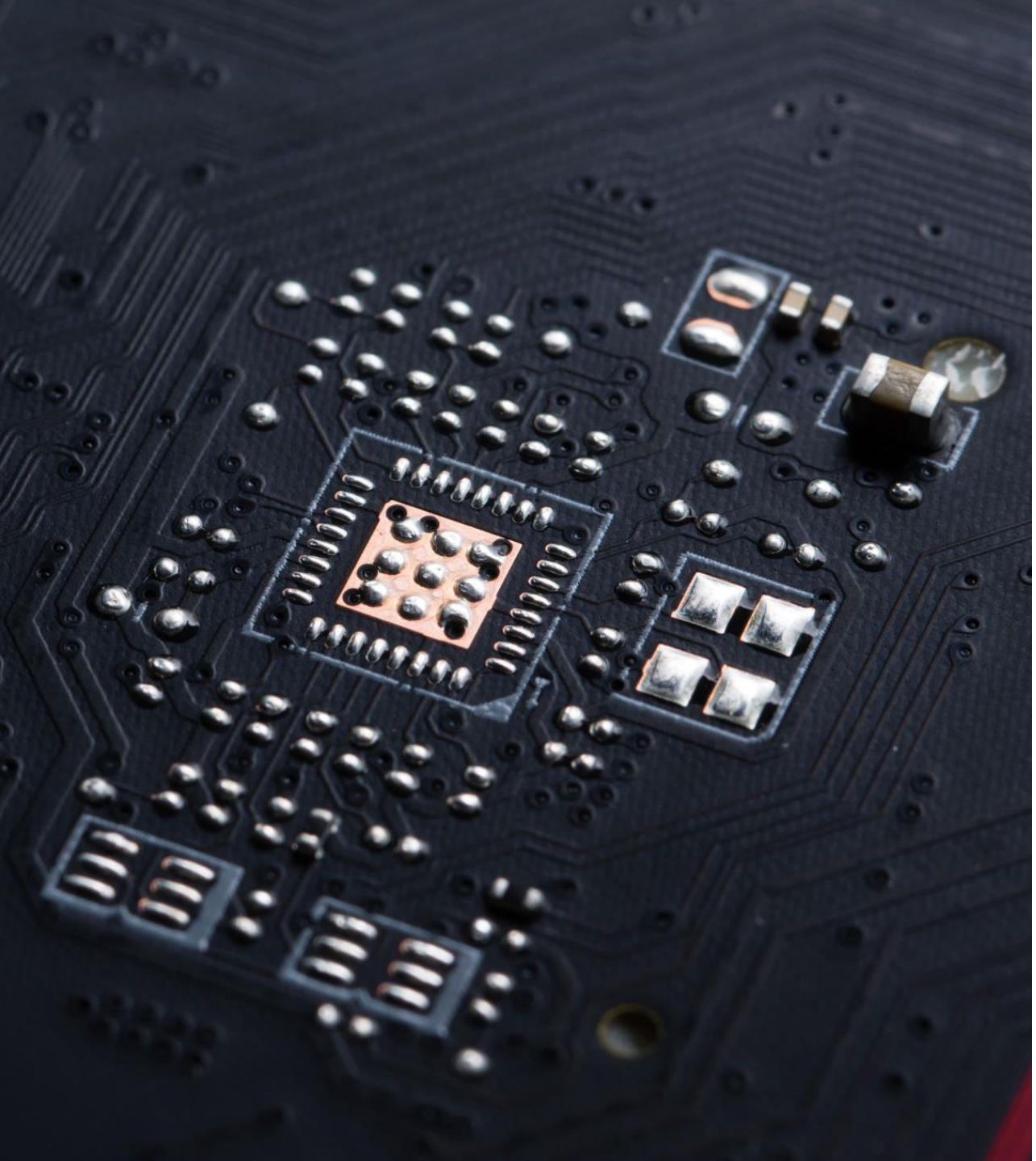
Proof of Stake



Here System (Protocol) randomly selects a Validator

Proof of Stake

Proof Of Work(PoW)	Proof Of Stake(PoS)
Miners	Validators
High performance hardware required.	Mobile or Laptop are enough.
Lots of electricity required.	Not much electricity is required.
The more hashing power you have the more blocks you can validate.	The more ETH you stake the more blocks you can validate.
Attack to happen 51% hashing power is required.	Attack to happen 51% of stake is required.
Competition is there.	Random selection is there.



Sharding

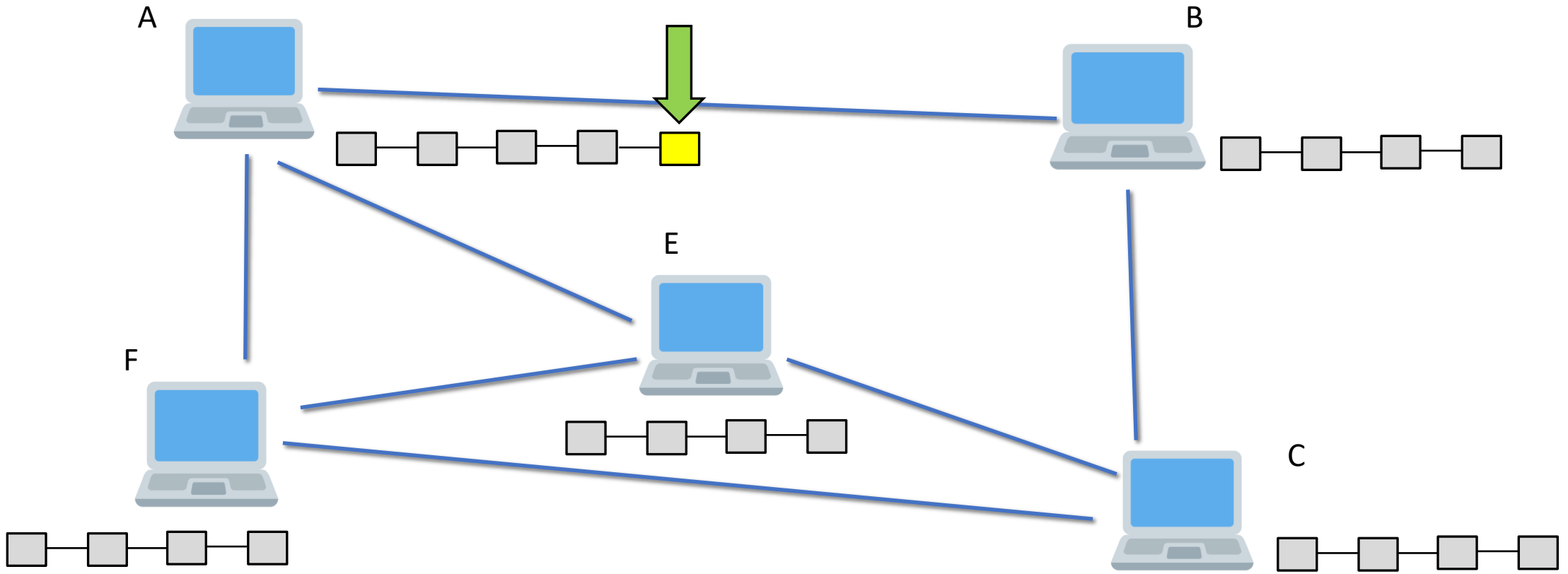
Sharding

- Consider the consensus protocol (Proof of work)

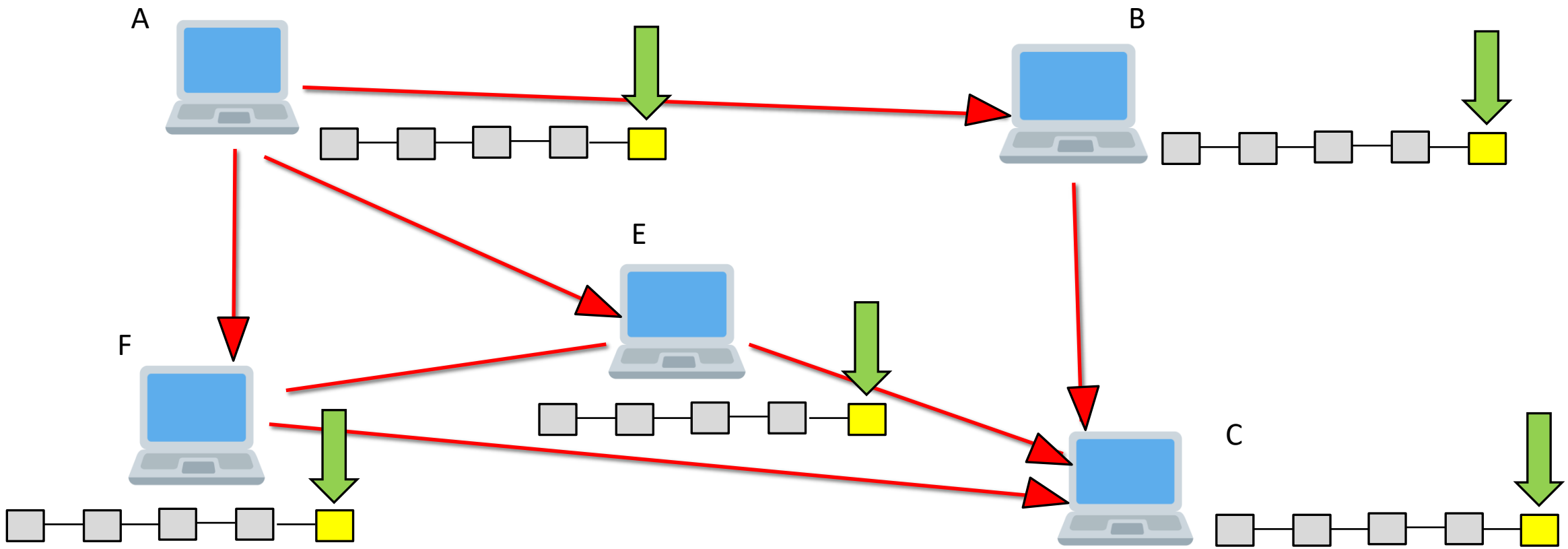
Issues:

- After mining conveying the information to all the miners
- Validation of a newly added block for which miners are not paid
- Therefore, most of their time is spent on validation
- Less number of transactions are performed per second
- A solution to this is **Sharding**

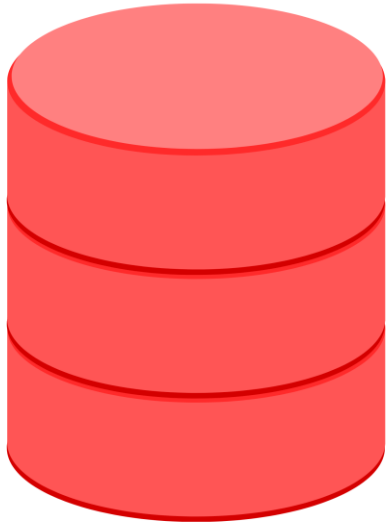
Consensus Protocol

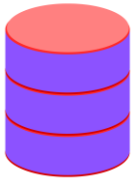


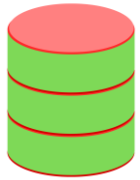
Consensus Protocol



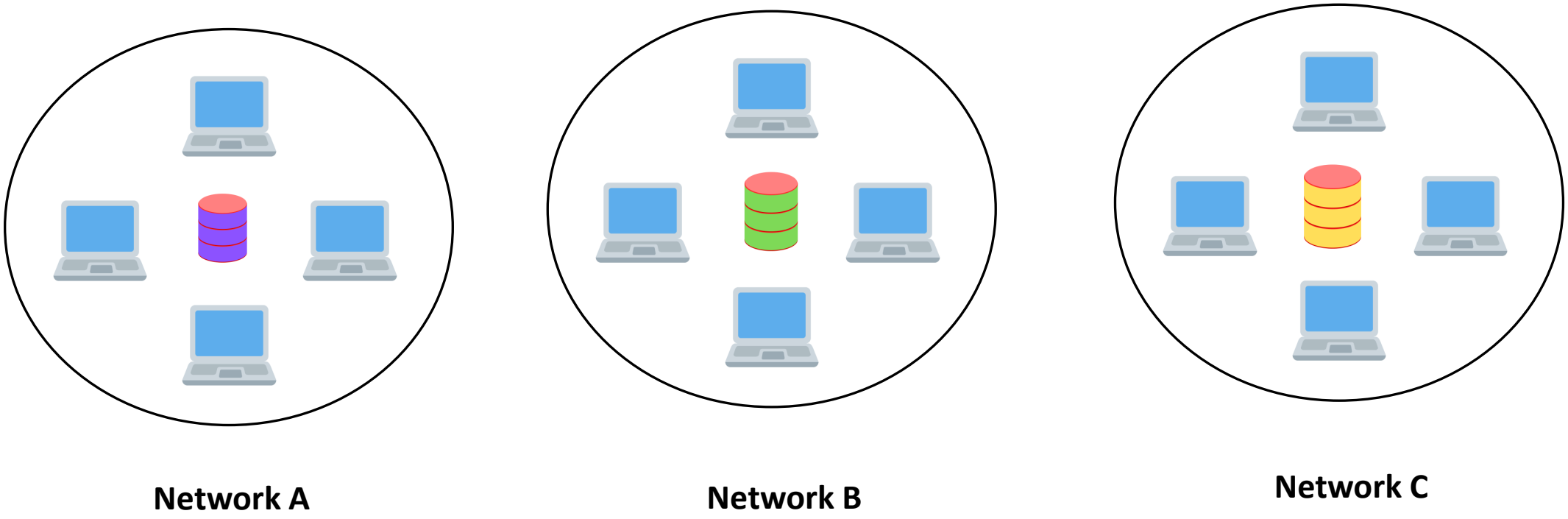
Sharding







Sharding



Network A

Network B

Network C

Sharding

- Sharding is database partitioning that separates large databases into smaller, faster, more easily managed parts.
- The smaller parts are called data shards, shard means “a small part of a whole.”
- These parts share nothing and can be deployed across multiple servers
- Unlike Replication, there is no data duplication
- Sharding spreads the load

Sharding

- Two common approaches to sharding; **horizontal** and **vertical sharding**

1. **Horizontal Sharding (Partitioning):**
    - Dividing a database into smaller partitions based on rows or records.
    - Each shard contains a subset of the data.
    - Each shard has the same schema and structure.
    - Data can be divided based on the **first letter** of the **user's name**.

Sharding

2. **Vertical Sharding:**
    - Dividing a database into smaller partitions based on columns or attributes.
    - Each shard contains a subset of the columns.
    - Each shard can have a different schema and structure.
    - Used to isolate **high-impact attributes** and to optimize data storage.

Major benfits

- Transactions per second will be increased
- Powerful and expensive computers will not be needed
- More validators will join, as no expensive computers will be required
- Load on miners will be reduced, as miners will validate limited miners' transactions
- Energy consumption will be reduced

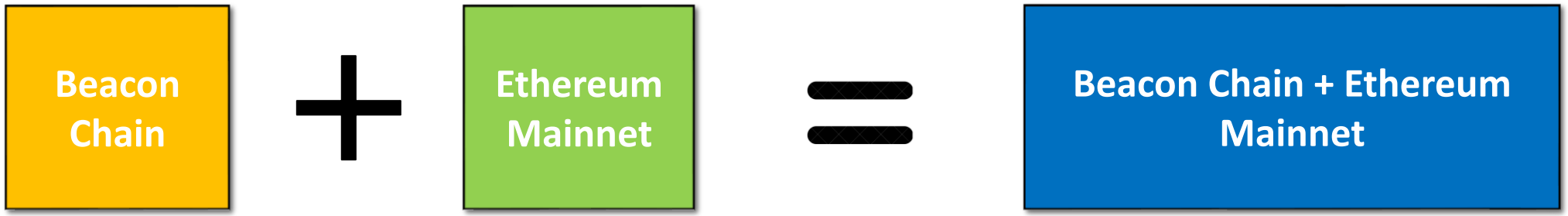
Beacon Chain

- The "Beacon Chain" is a core component of Ethereum 2.0, a major upgrade to the Ethereum blockchain, a coordination mechanism of the new network.
- Beacon chain Introduced proof-of-stake to the Ethereum ecosystem
- Merged with the original Ethereum proof-of-work chain in September 2022.
- Responsible for block creation, block propagation, and making sure the new blocks are valid.
- Rewarding the validators with ETH for keeping the network secure

Ethereum Mainnet

- Mainnet is the primary public Ethereum production blockchain
- Here the actual-value transactions occur on the distributed ledger
- When people exchange and discuss ETH prices, they are talking about Mainnet ETH.

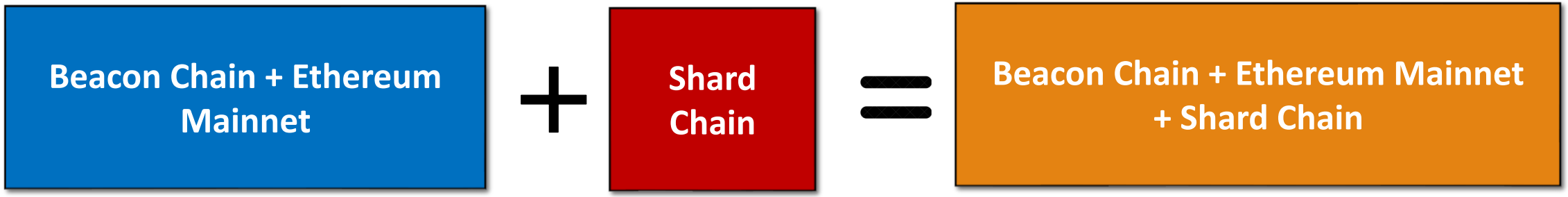
Beacon Chain integration with Mainnet

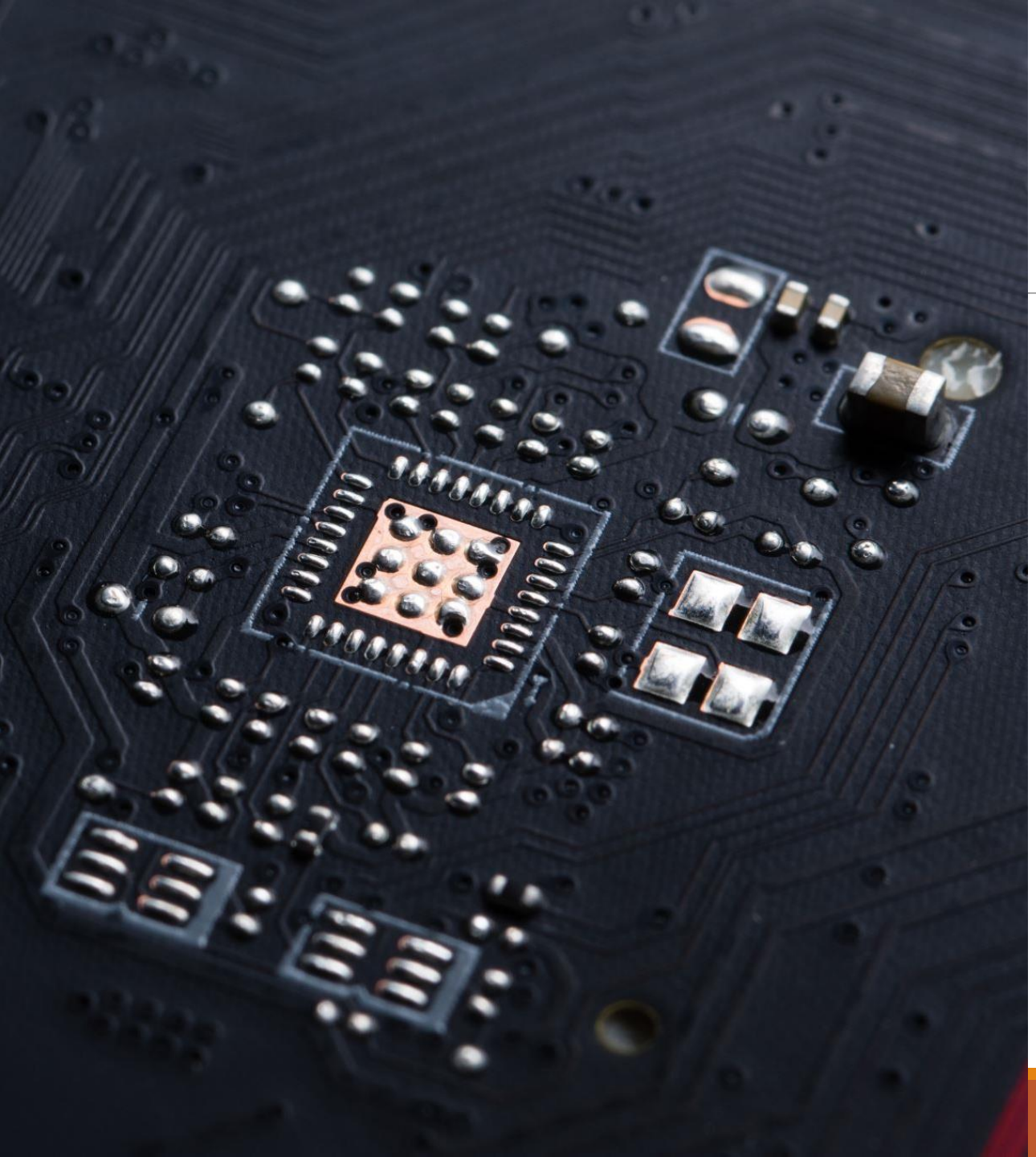


Beacon Chain integration with Mainnet along with Shard Chain

- The combination of **Beacon Chain, Ethereum Mainnet,** and **Sharding**

  is very useful





AltCoins

AltCoins

LTC
Litecoin

THETA
THETA

USDT
Tether

ADA
Cardano

LINK
Chainlink

BNB
Binance Coin

AltCoins

- Altcoins are generally defined as all cryptocurrencies other than **Bitcoin (BTC)**

Why do we need other coins?

- Adding new features and capabilities missing in the bitcoins
- Using better Consensus Protocols i.e., **Proof of Stake** instead of **Proof of Work**
- As of July 2022, there were almost 20,268 cryptocurrencies
- The largest Altcoins by market capitalization as of **September 2022** are;

Ethereum (ETH), Tether (USDT), U.S. Dollar Coin (USDC), Binance Coin (BNB), XRP (XRP), Binance USD (BUSD), Cardano (ADA), Solana (SOL), Dogecoin (DOGE)

For more details visit this site ***https://www.investopedia.com/***

The End