# Blockchain DLOC Sem VII

# CSDC7022 : Block Chain

## Module - 1 : Introduction to Block Chain (4 Hours)

Instructors : Dr. Nupur Giri & Mrs. Lifna C S

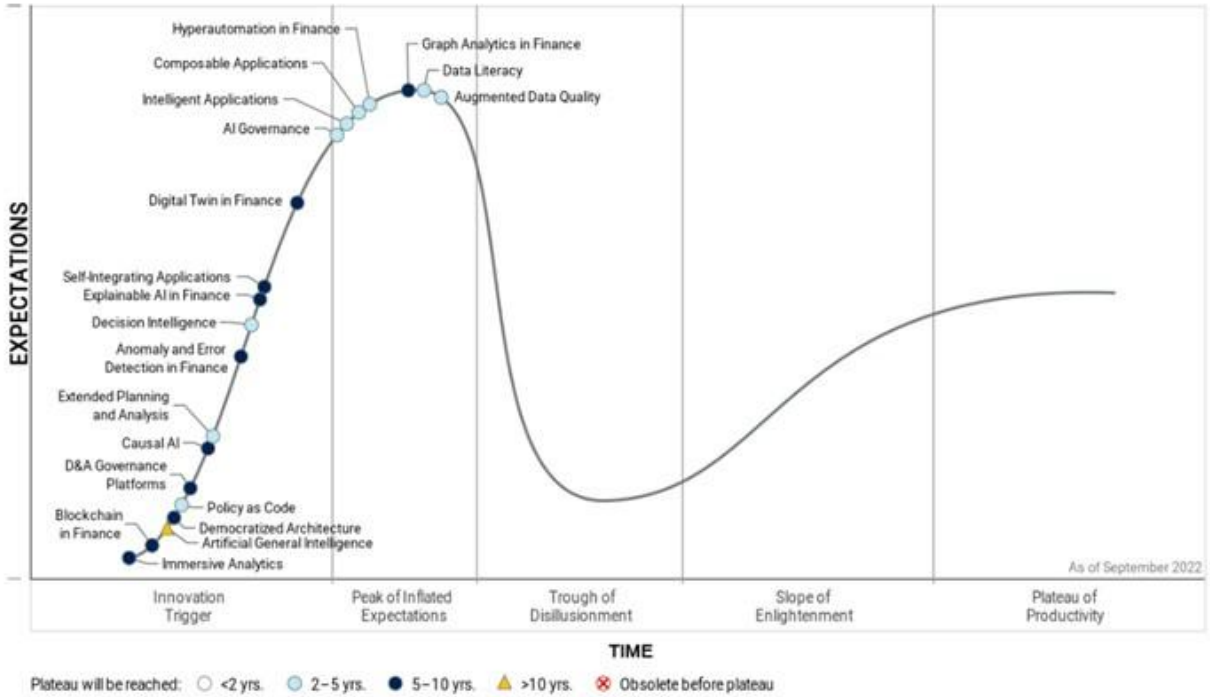
*Department of Computer Engineering, VESIT, Mumbai*

# Topics to be covered

- Why to learn Blockchain ?
- What is Web 3.0 ?
- What is a Blockchain?
- Origin of blockchain (cryptographically secure hash functions),
- Foundation of blockchain:
  - Components of blockchain (Consensus Protocol)
  - Block in blockchain,
  - Merkle trees
- Types: Public, Private, and Consortium,
- Limitations and Challenges of blockchain

# Why to learn Blockchain ?

Figure 1: Gartner Hype Cycle for Emerging Technologies in Finance, 2023




Source: Gartner (November 2022)

# Why to learn Blockchain ?

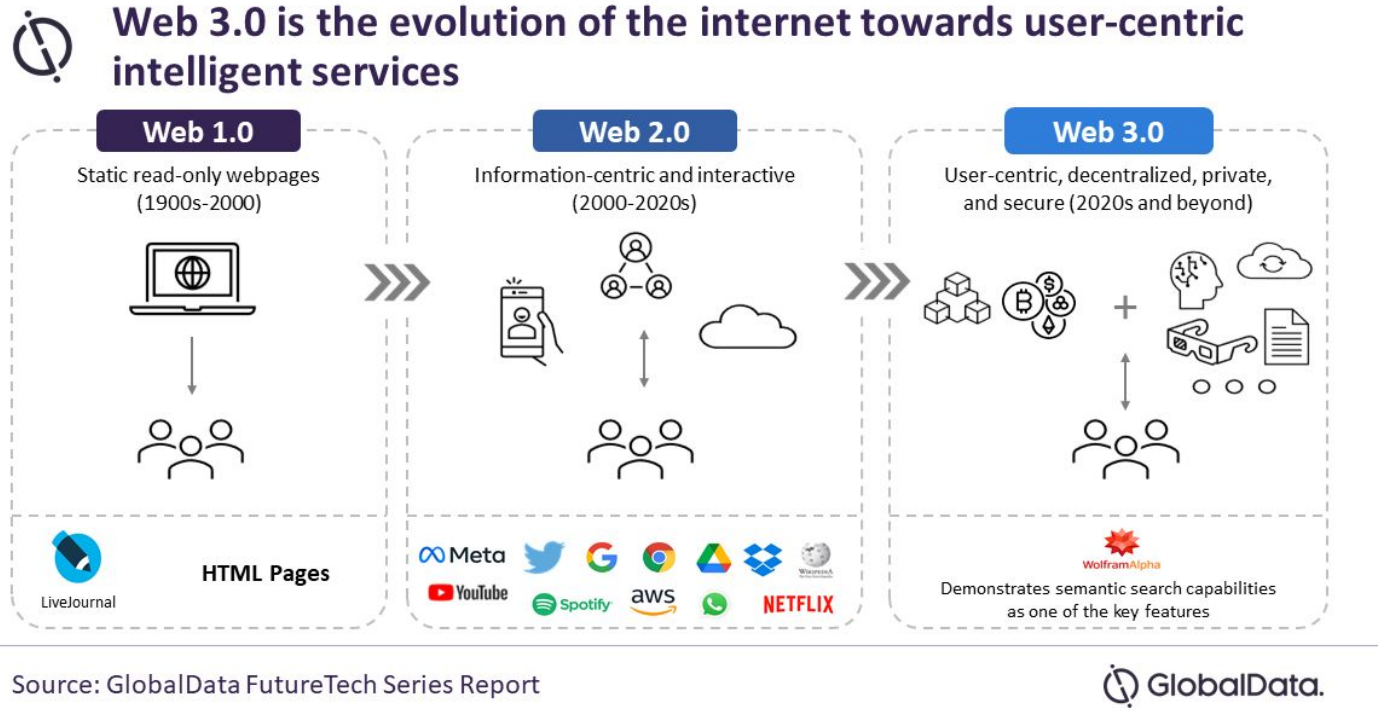
**Current Scenario**

- Internet is owned by Technical Giants
- Huge Transaction fees by 3rd Parties
- Time to complete Transactions..
- Ownership for Content Creators
- Lack of Transparency

**Blockchain Offers …**

- Decentralized with P2P Network
- Trust in a Trustless Network
- Immutable
- Security through Cryptography
- Transparency

# What is Web 3.0?




Courtesy : https://www.globaldata.com/wp-content/uploads/2022/03/220302_Web3.0_7and9_1.png

# What is Blockchain ?

- A Blockchain is “an **open**, **distributed ledger** that can record transactions between two parties **efficiently** and in a **verifiable** and **permanent** way” (Iansiti, Lakhani 2017)

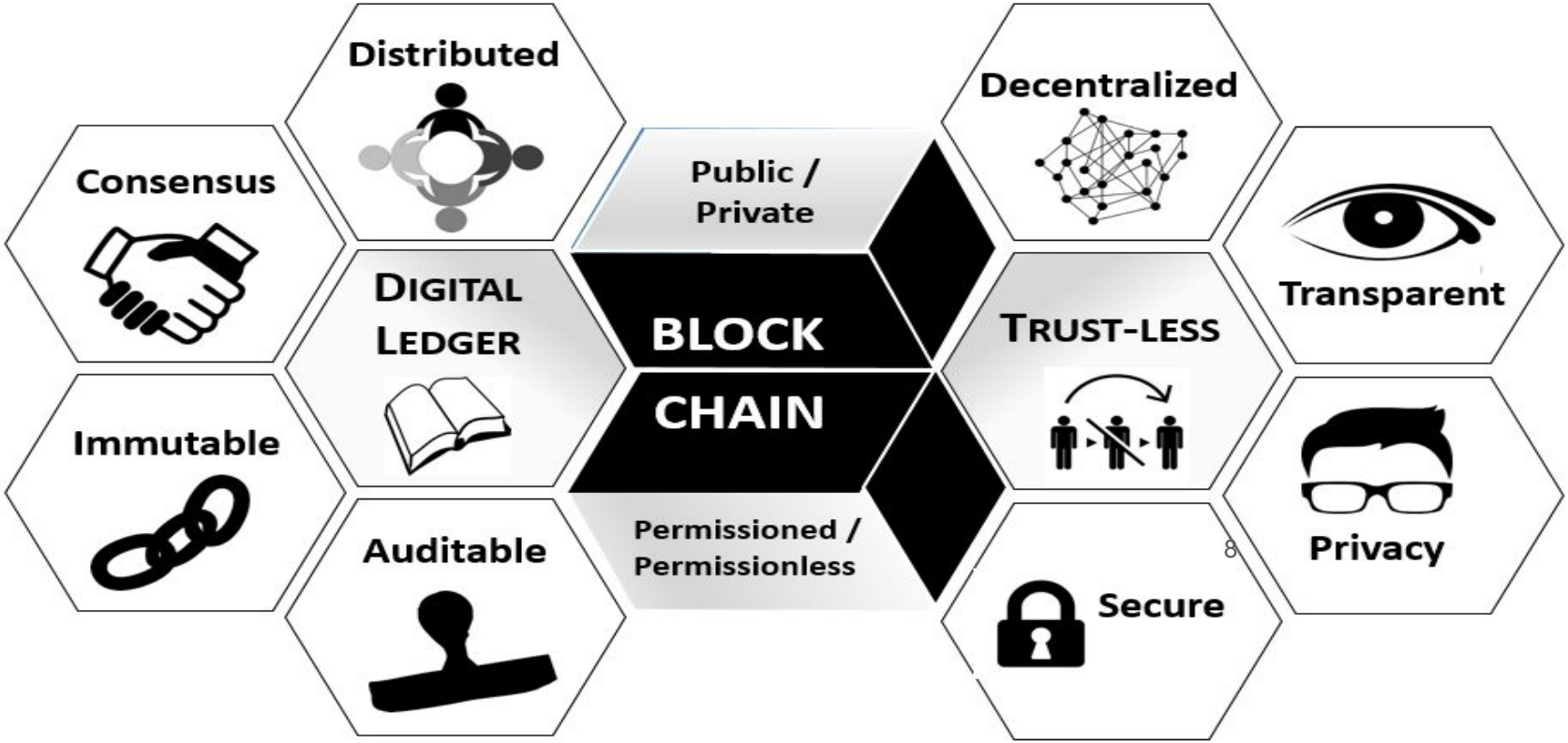
- The keywords: **Open** (accessible to all), **Distributed or Decentralized** (no single party control), **efficient** (fast and scalable), **verifiable** (everyone can check the validity of information), **permanent** (the information is persistent)

Courtesy : https://nptel.ac.in/courses/106105184

# What is Blockchain ?

- Blockchain is a **digital public ledger** that records **online transactions**.
- Blockchain ensures **confidentiality, integrity and privacy**.
- When a **new block** is added to a blockchain, it is **linked to the previous block** using a **cryptographic hash**.
- This ensures the **chain is never broken** and that **each block is permanently recorded.**
- It is also **intentionally difficult** to alter past transactions in blockchain since **all the subsequent blocks must be altered first**.

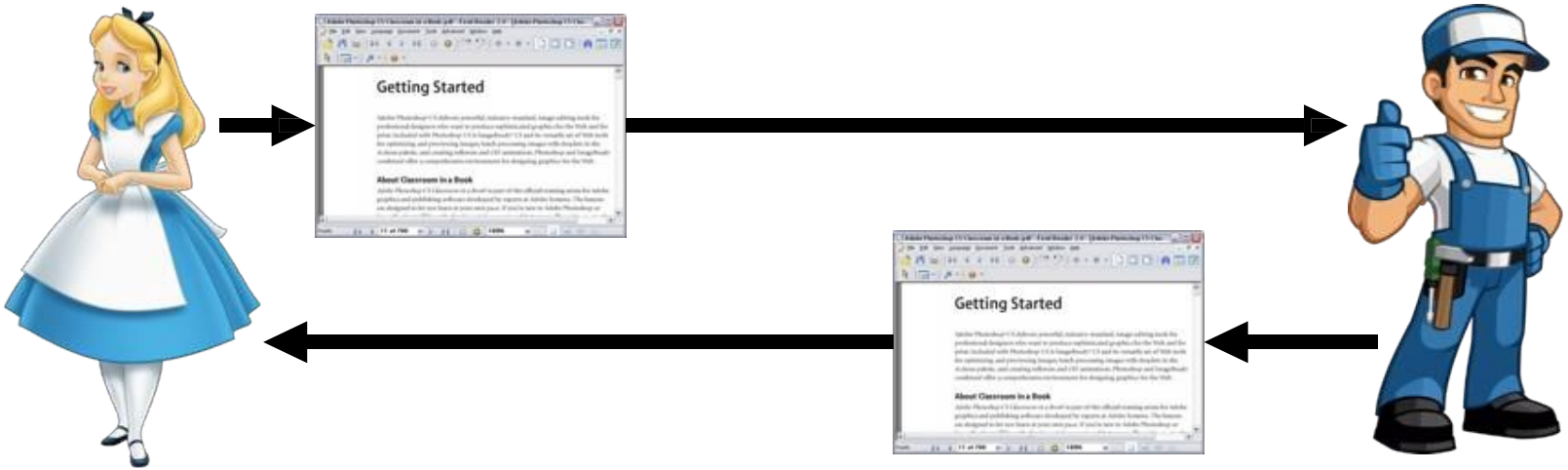
# Characteristics of Blockchain




Courtesy : Chandramouli et.al

# Example Scenario

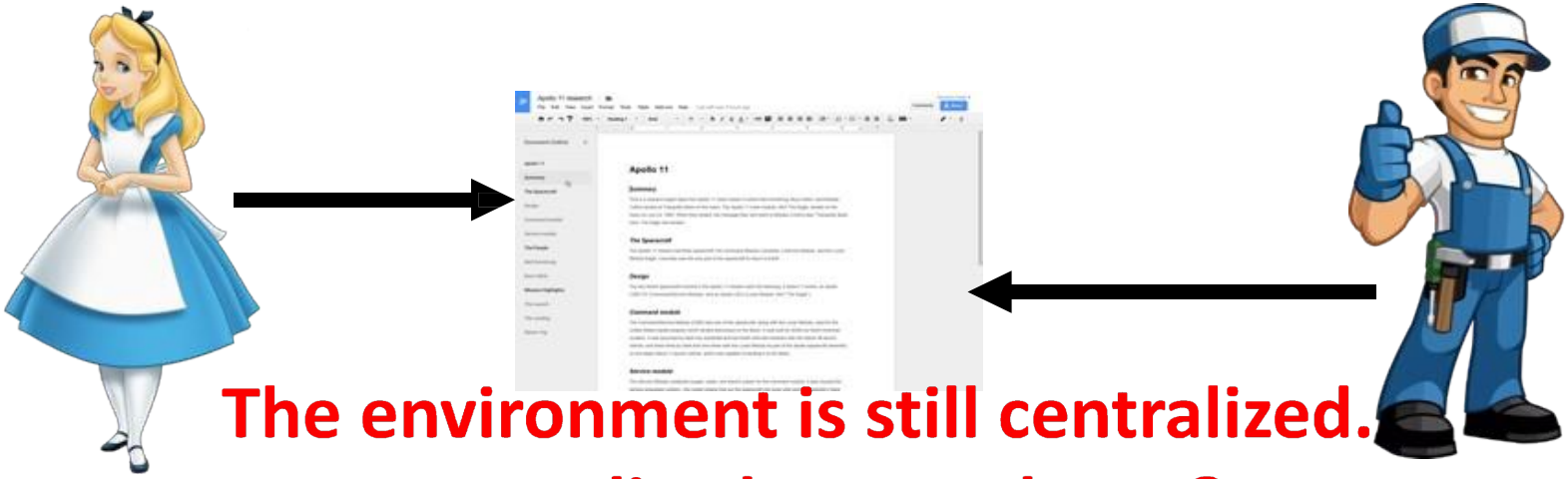
- Traditional way of sharing documents




Courtesy : https://nptel.ac.in/courses/106105184

# Example Scenario

- Shared Google doc – both the users can edit simultaneously



**The environment is still centralized.**

**Does centralized system harm?**

Courtesy : https://nptel.ac.in/courses/106105184

# Example Scenario

## Problems with a Centralized System

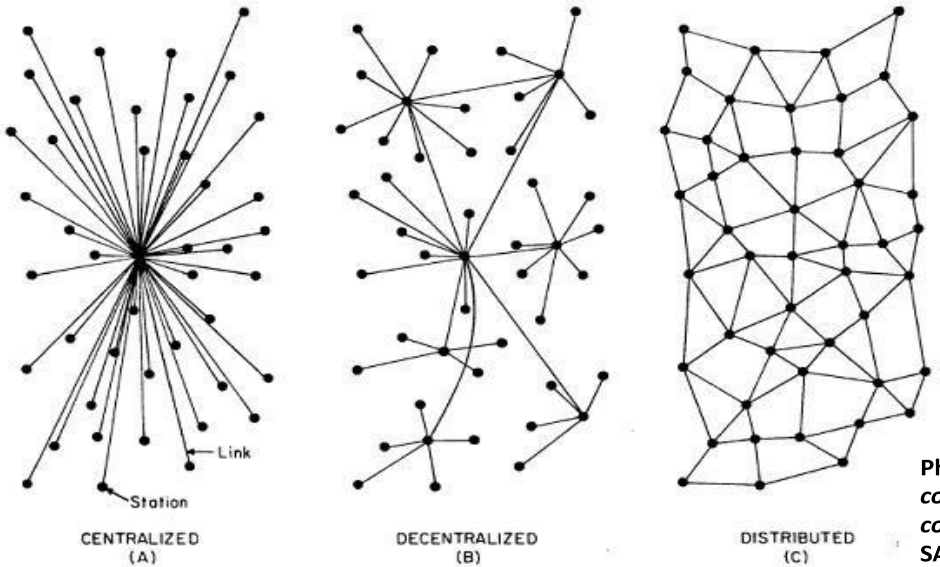
**A single point of failure**

- If you do not have sufficient bandwidth to load Google doc, you'll not be able to edit
- What if the server crashes?

Courtesy : https://nptel.ac.in/courses/106105184

# Example Scenario

## Centralized vs Decentralized vs Distributed




**Complete reliance on single point (centralized) is not safe**

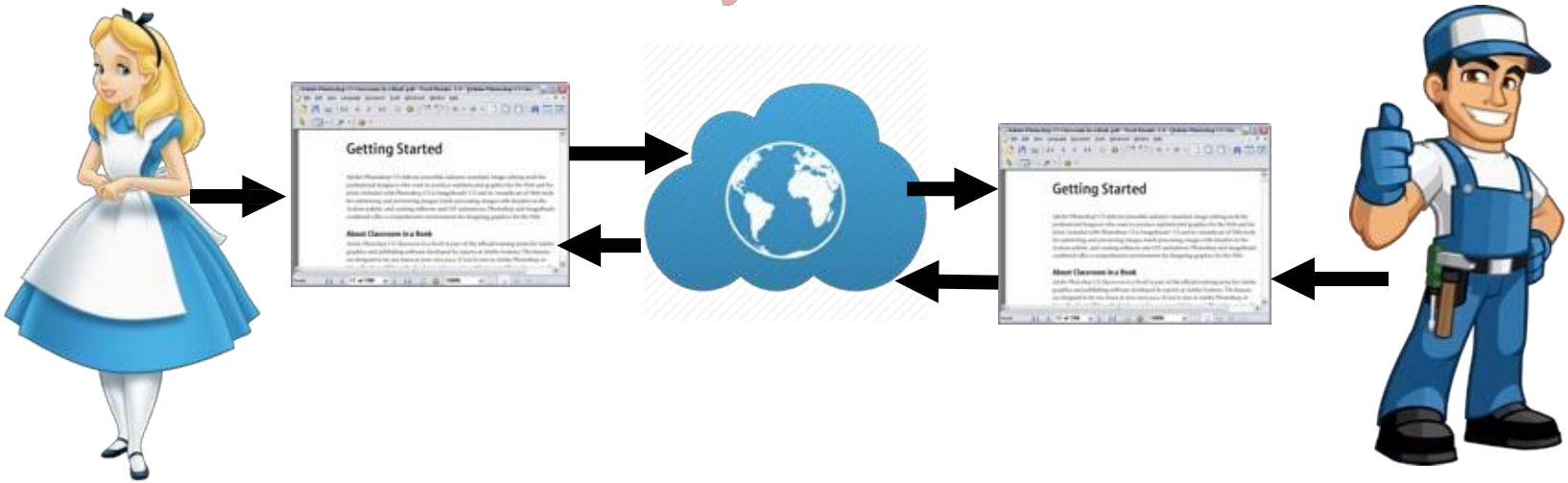
- **Decentralized: Multiple points of coordination**
- **Distributed: Everyone collectively execute the job**

**Photo courtesy: Baran, Paul. *On distributed communications: I. Introduction to distributed communications networks.* No. RM3420PR. RAND CORP SANTA MONICA CALIF, 1964.**

Courtesy : https://nptel.ac.in/courses/106105184

# Example Scenario

## A Plausibly Ideal Solution

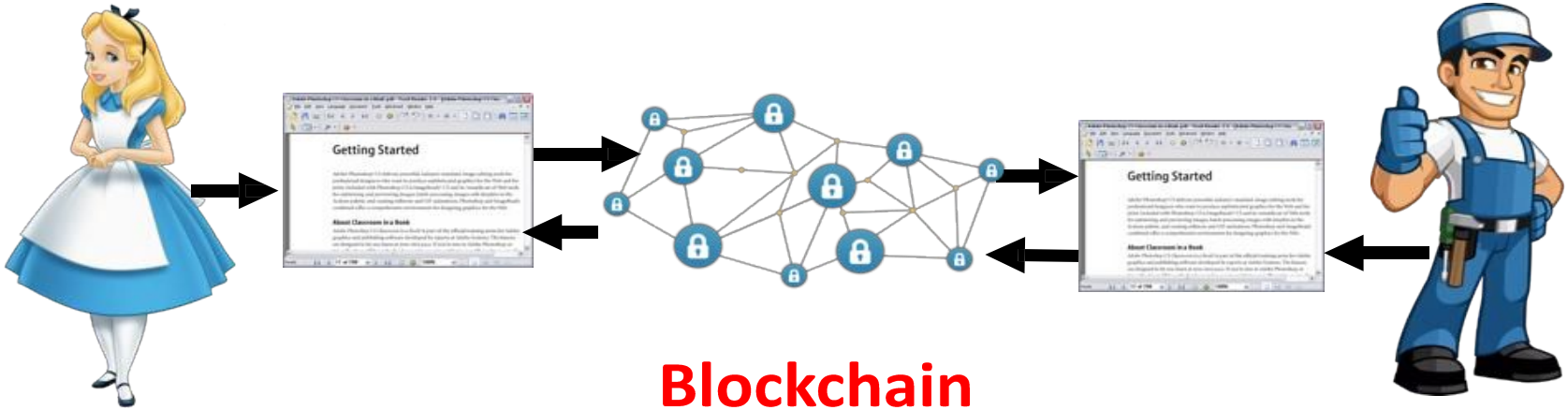



**Everyone edits on their local copy of the document – the Internet takes care of ensuring consistency**

Courtesy : https://nptel.ac.in/courses/106105184

# Example Scenario

## Blockchain – The Internet Database to Support Decentralization



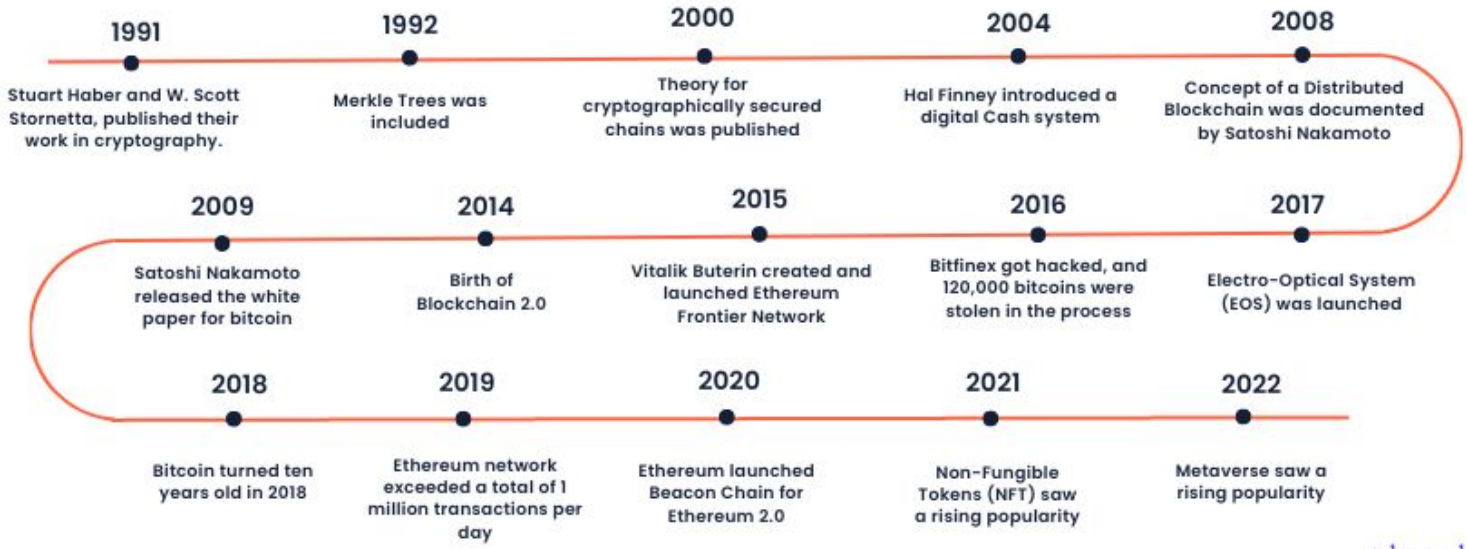

**Blockchain**

**A decentralized database with strong consistency support**

Courtesy : https://nptel.ac.in/courses/106105184

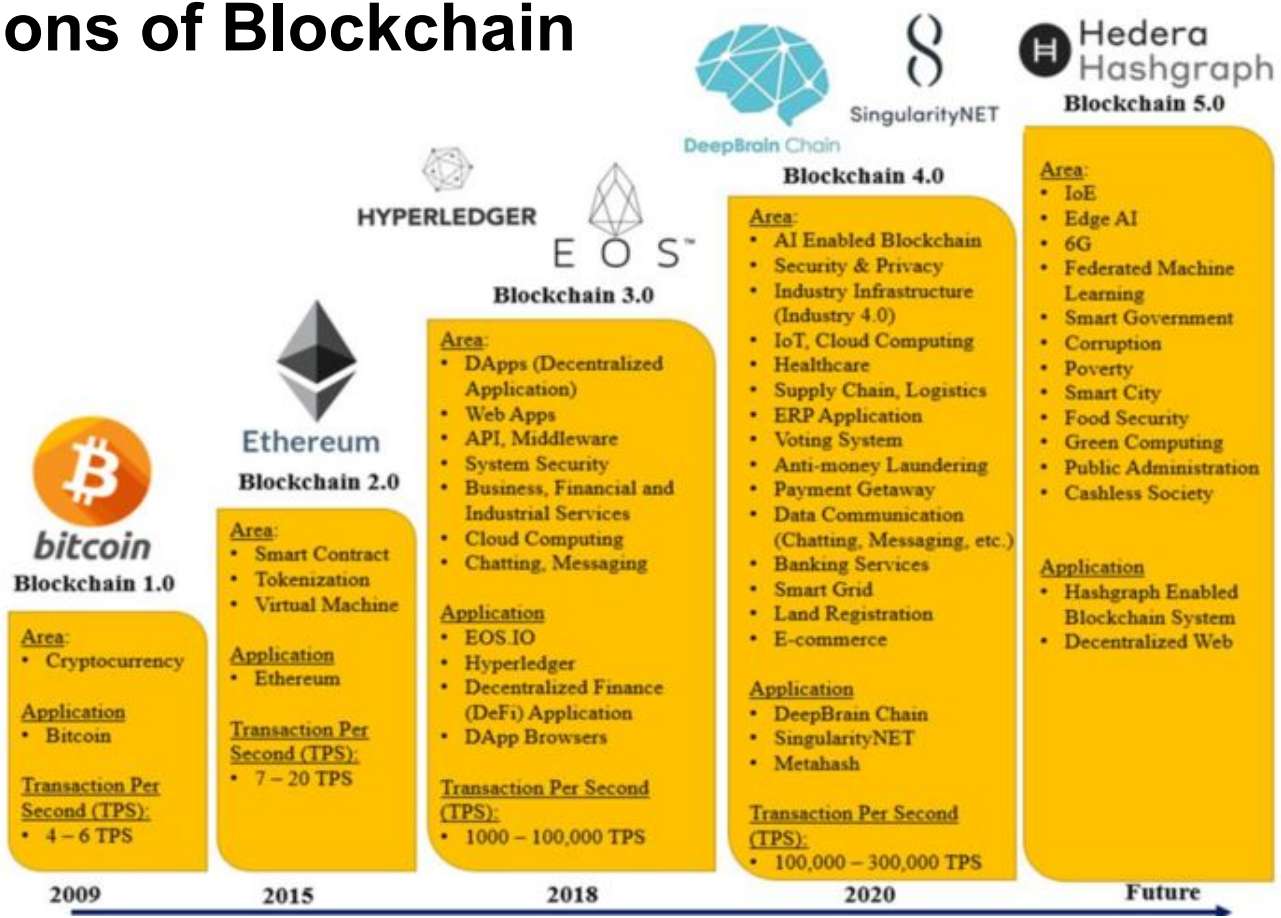
# Origin of Blockchain

## Blockchain History Timeline




Courtesy : https://www.theknowledgeacademy.com/blog/history-of-blockchain/

# Generations of Blockchain



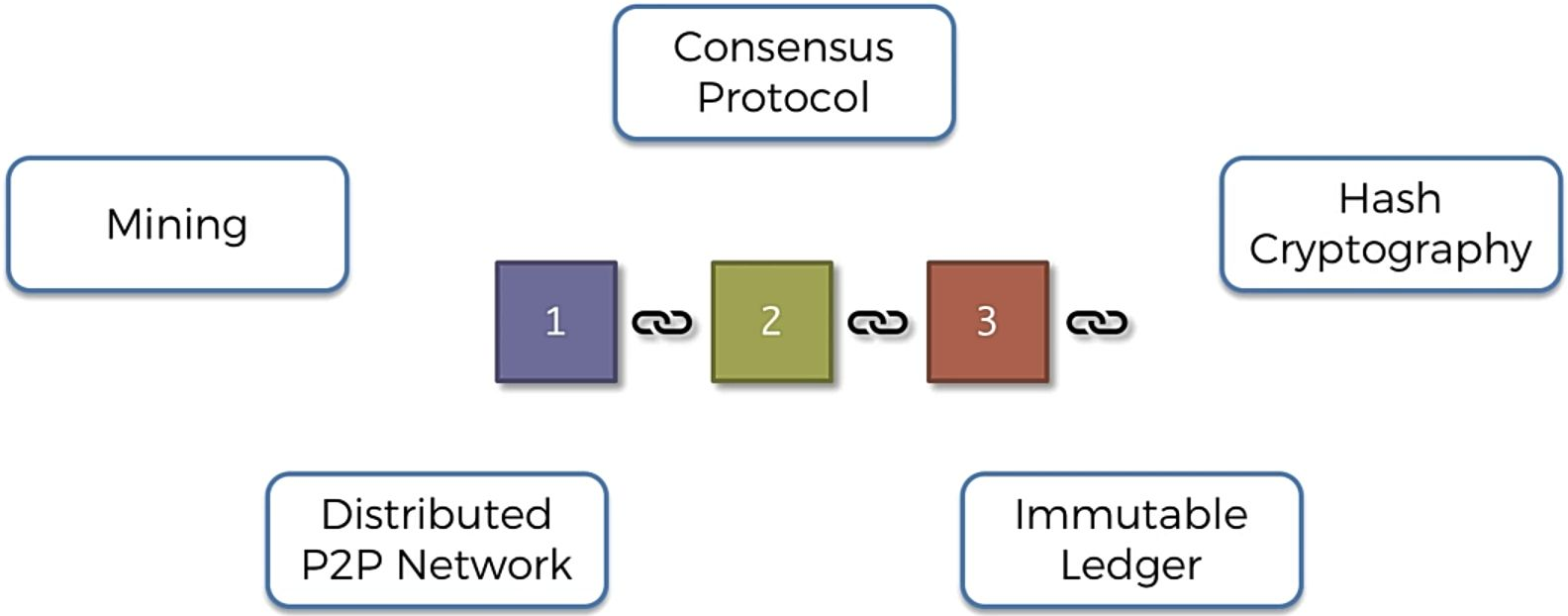

Courtesy : Research Gate

# Comparison between different Generations of Blockchain

| Parameter | Blockchain 1.0 | Blockchain 2.0 | Blockchain 3.0 | Blockchain 4.0 |
|---|---|---|---|---|
| Application | Monetary region | Non-monetary region | Commerce platforms | Industry 4.0 |
| Instance | Bitcoin | Ethereum | Cardano, IOTA, Anion | Unibright, SEELE |
| Energy utilization | Maximum | Reasonable | Power Competent | Very well-organized |
| Price | Costly | Inexpensive | More Cheaper | Cost efficient |
| Speed | 7 TBS | 15 TBS | 1000 TBS | 1M TBS |
| Inter communiqué | Not approved | Not approved | approved | approved |
| Inter operation | No | No | Yes | Highly |
| Scalability | No | Poor | Scalable | Highly |
| Verification | Via miners | Via smart contracts | In-built confirmation Via dApps | Sharding Automated confirmation |
| Consensus mechanism | PoW | Assigned PoW | Proof of stake, authority | Proof of integrity |
| primary theory | Distributed Ledger | Smart contracts | dApps | Blockchain with AI |

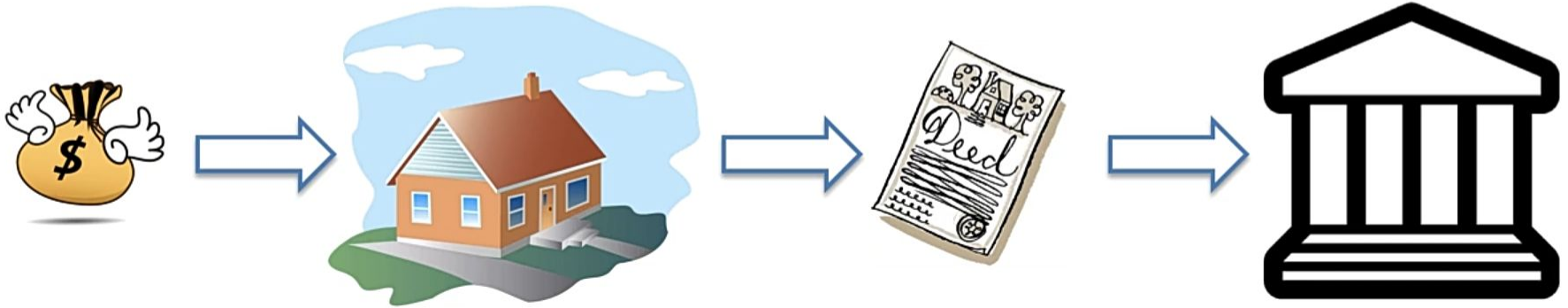
Courtesy : Research Gate

# Blockchain

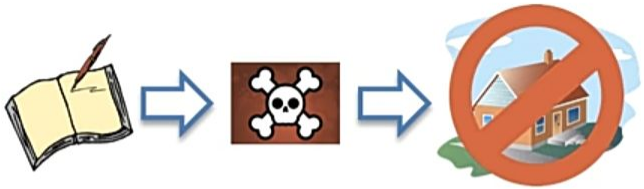



Courtesy : Super Data Science

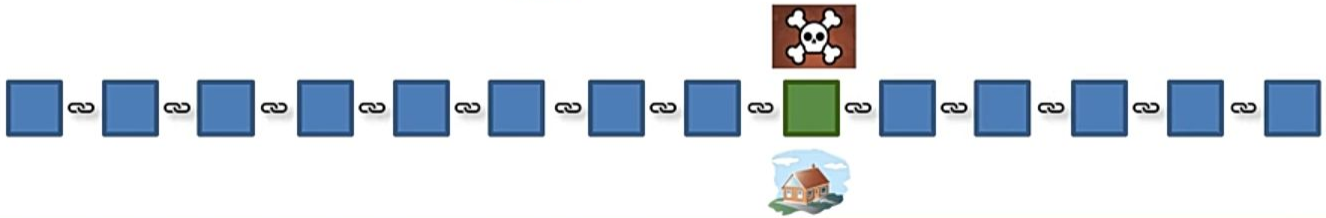
# Immutable Ledger



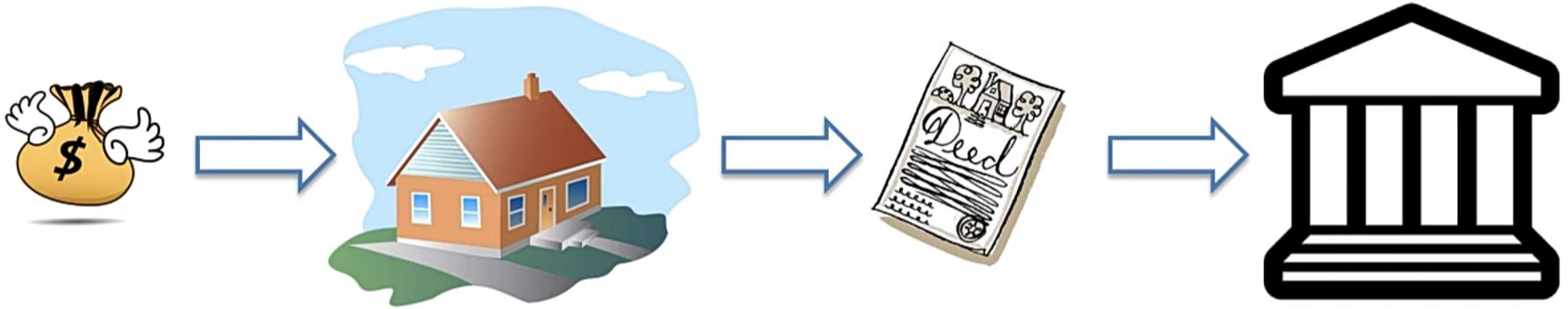

Traditional Ledger



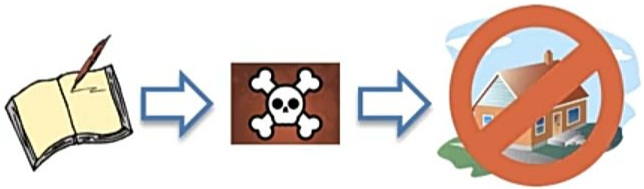
Blockchain



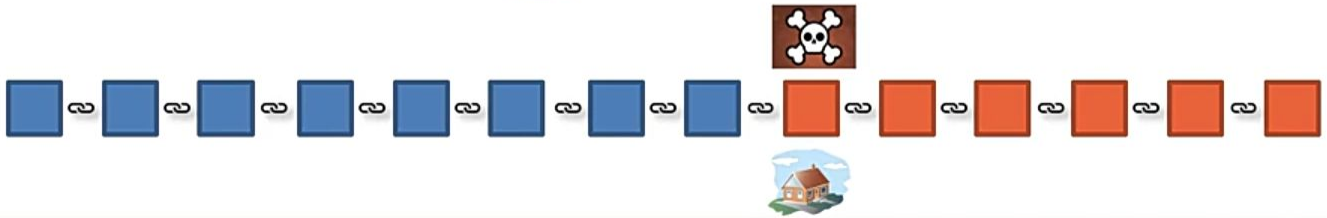
# Immutable Ledger



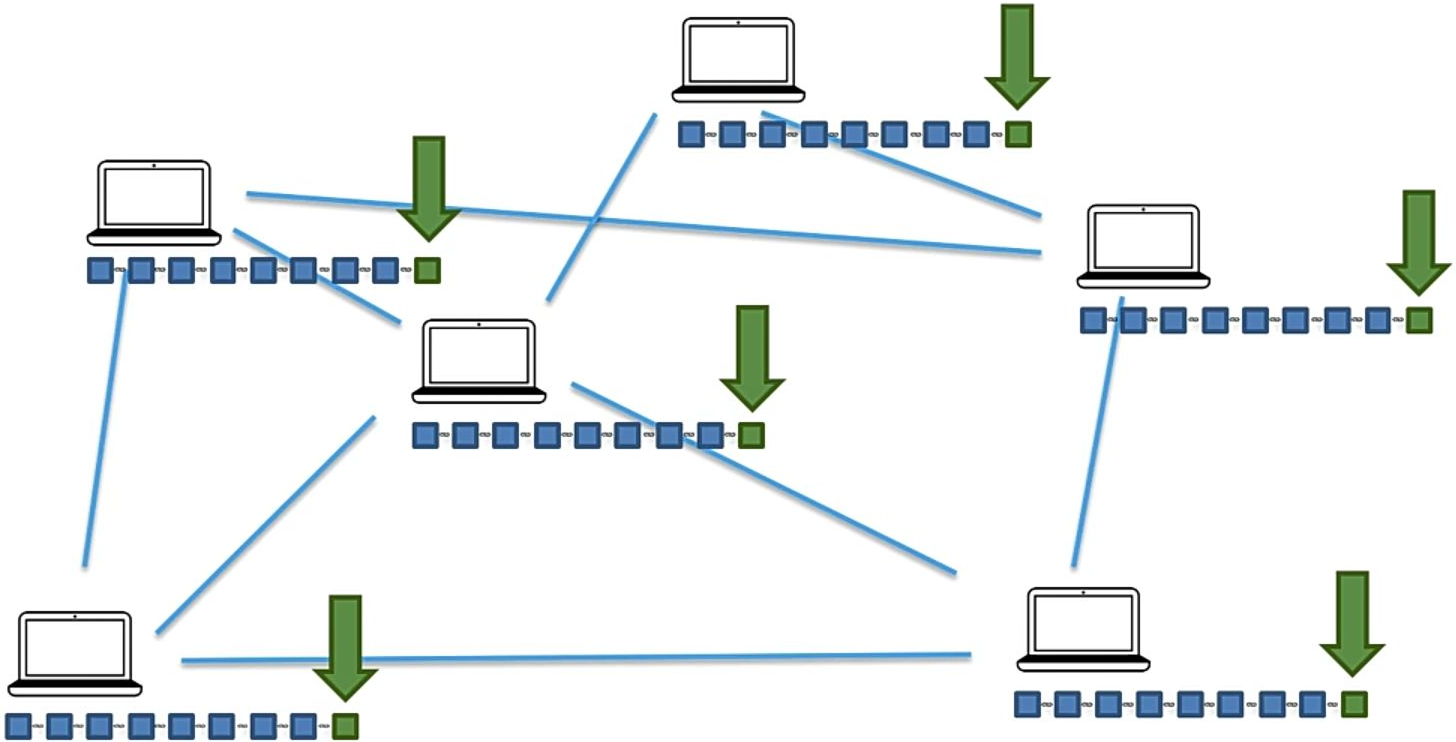

Traditional Ledger



Blockchain

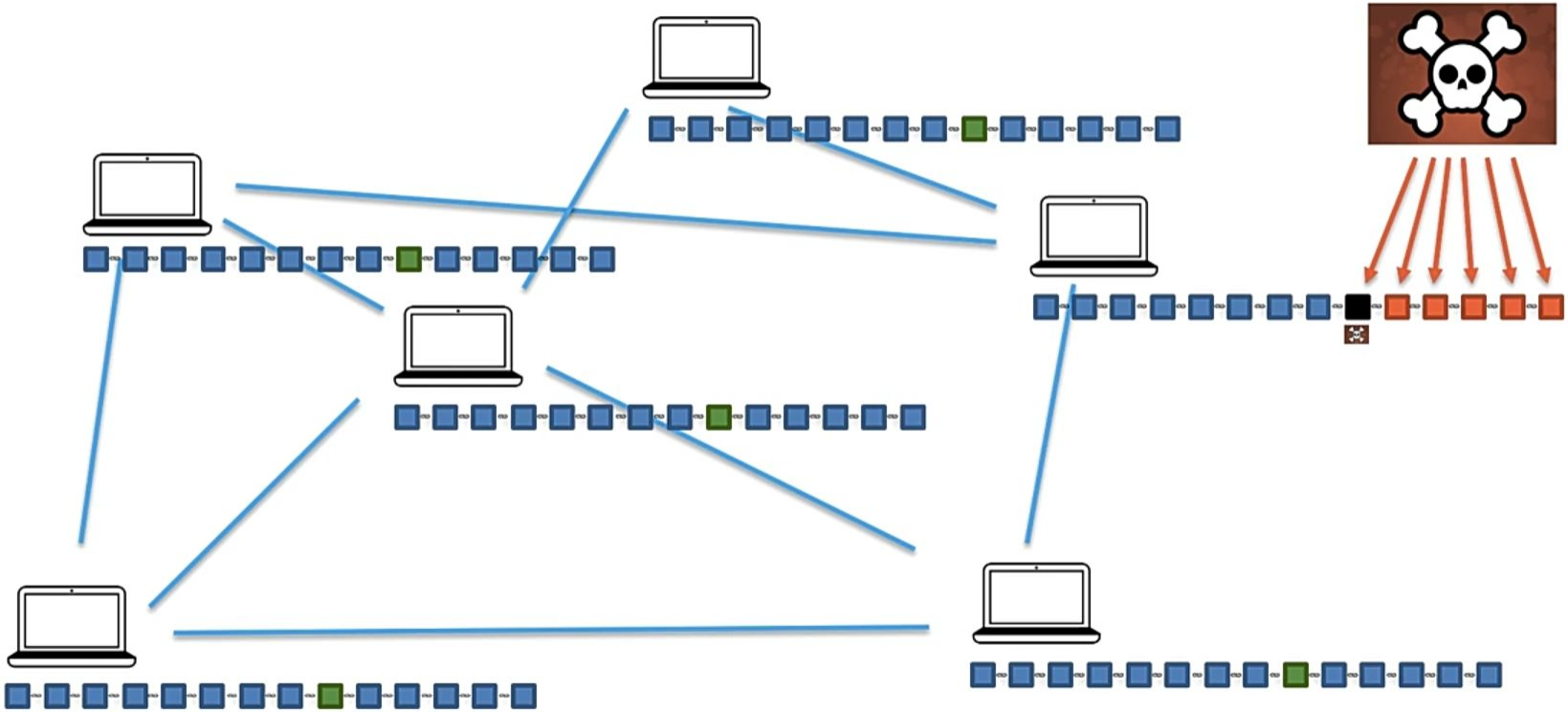


# Distributed P2P Network



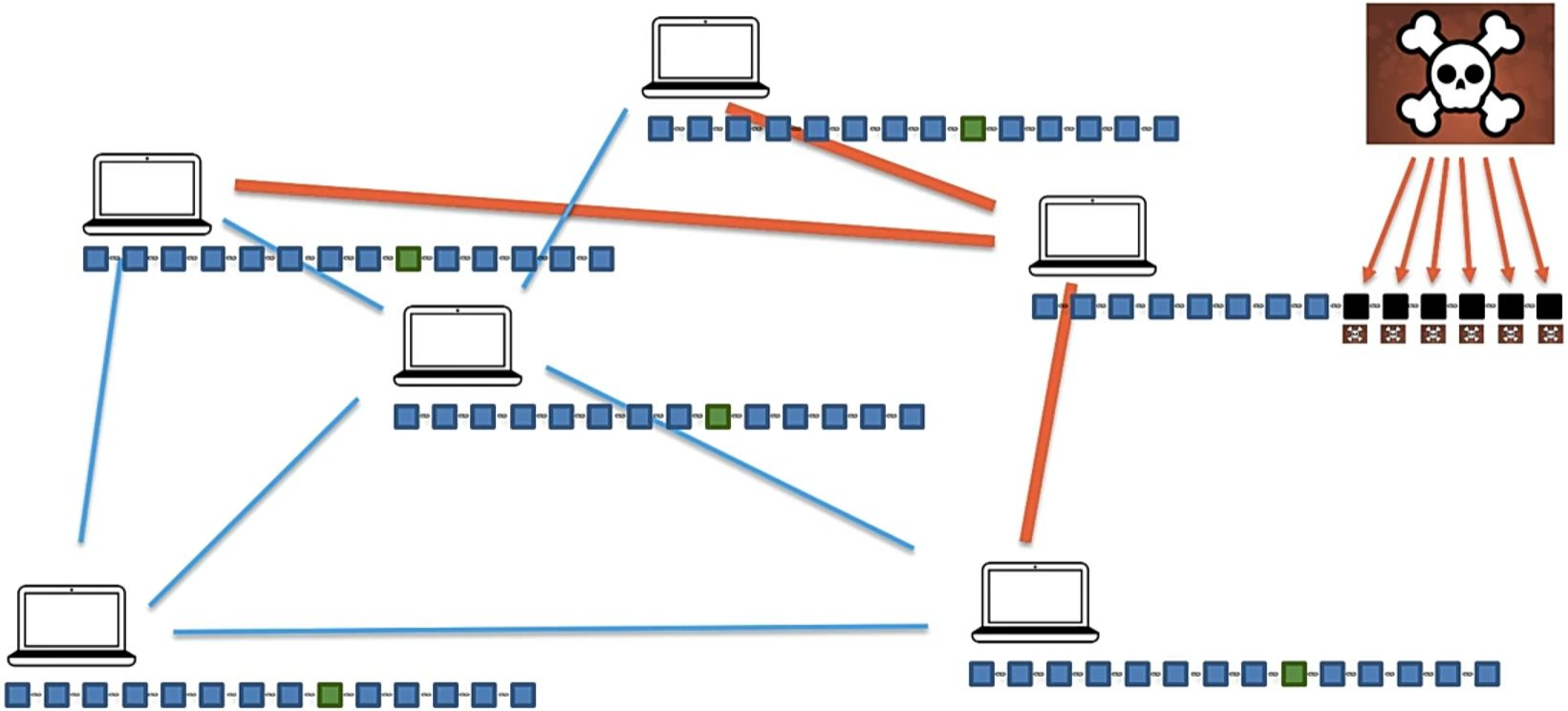
Courtesy : Super Data Science

# Distributed P2P Network



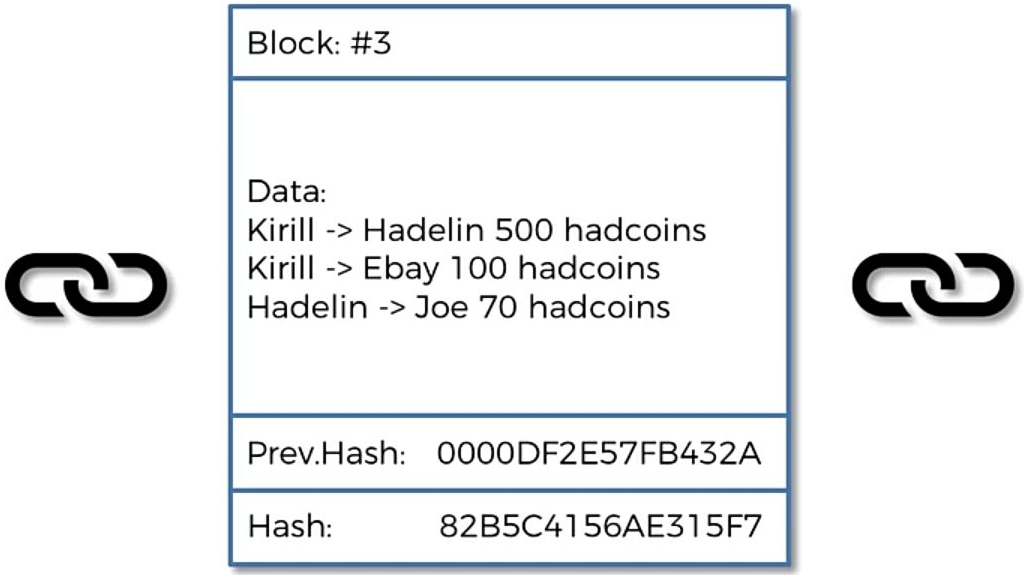
Courtesy : Super Data Science

# Distributed P2P Network



Courtesy : Super Data Science

# How Mining Works ?

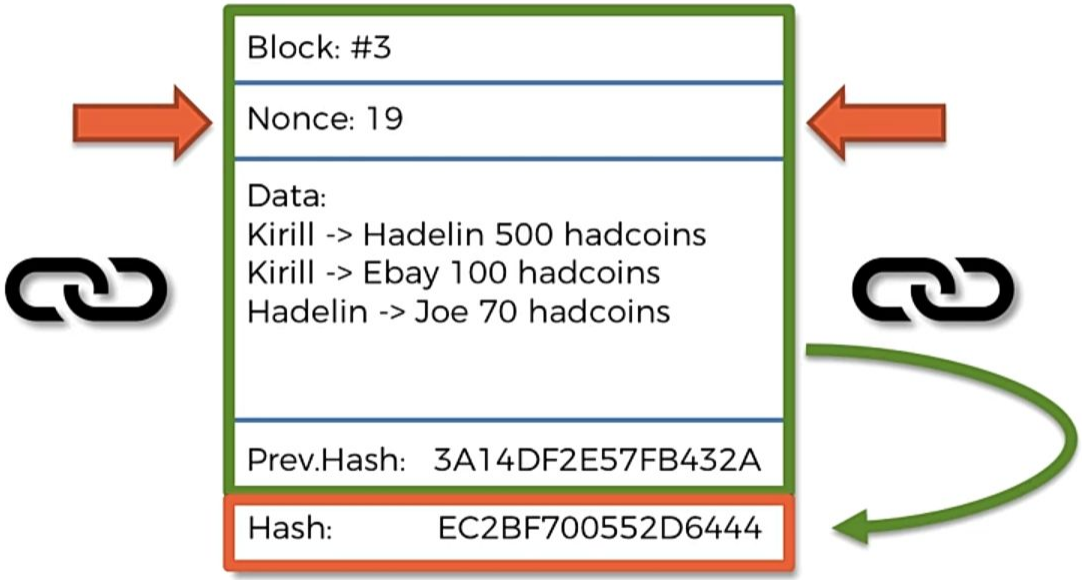



Courtesy : Super Data Science

# How Mining Works ?

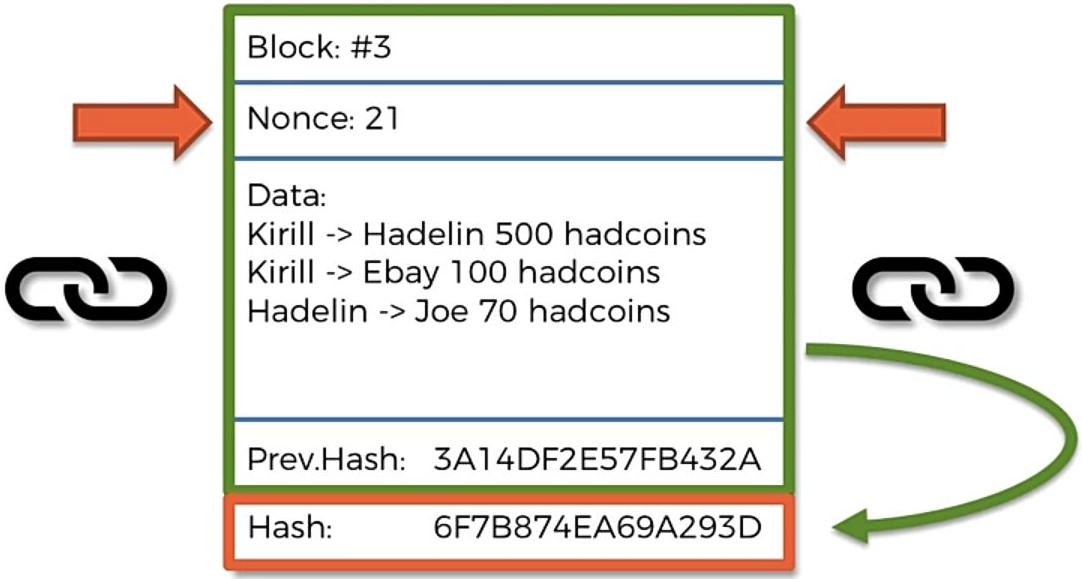

Courtesy : Super Data Science

# How Mining Works ?



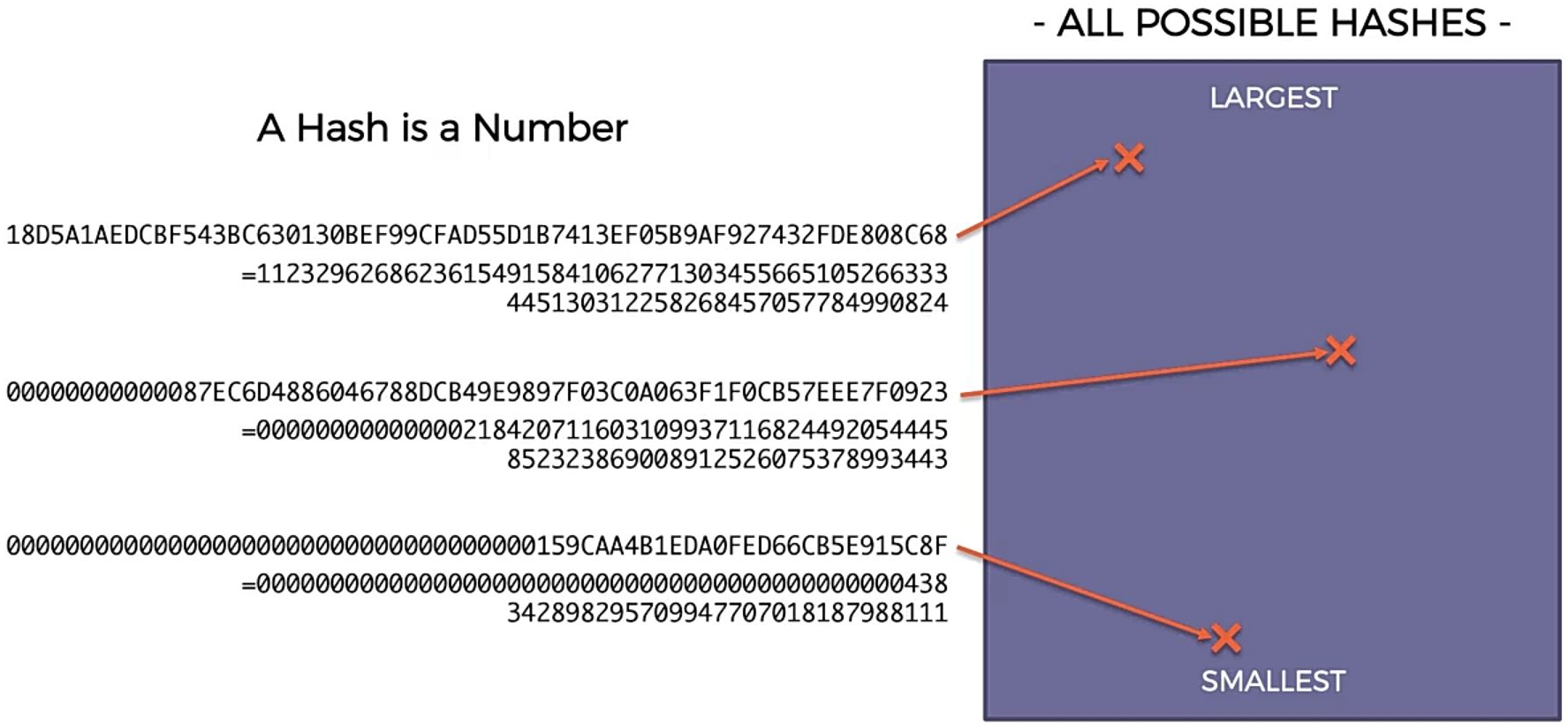

Courtesy : Super Data Science

# How Mining Works ?




Courtesy : Super Data Science

# How Mining Works ?




Courtesy : Super Data Science

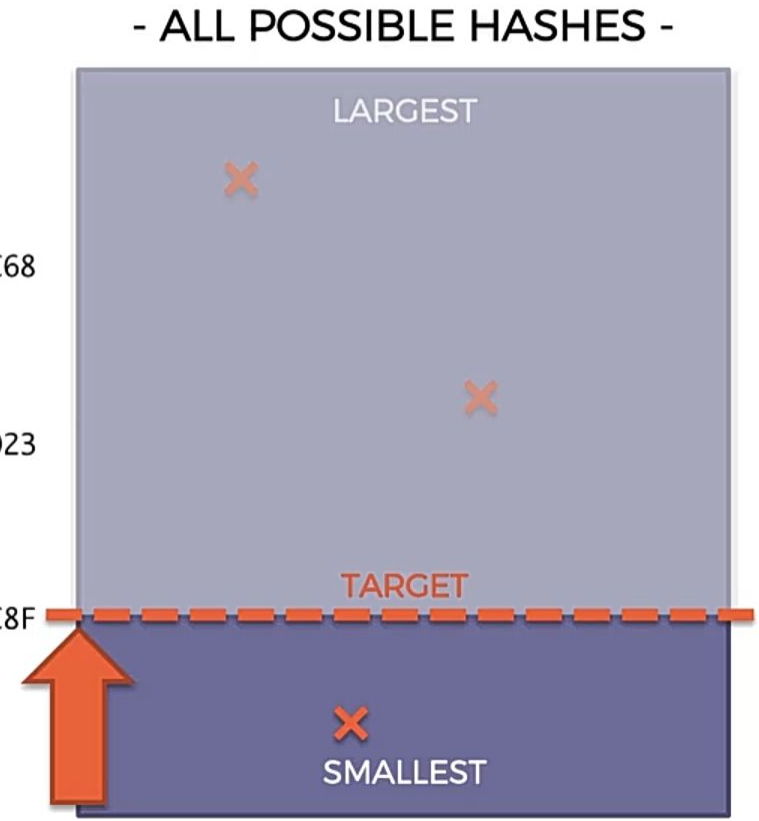
# How Mining Works ?

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

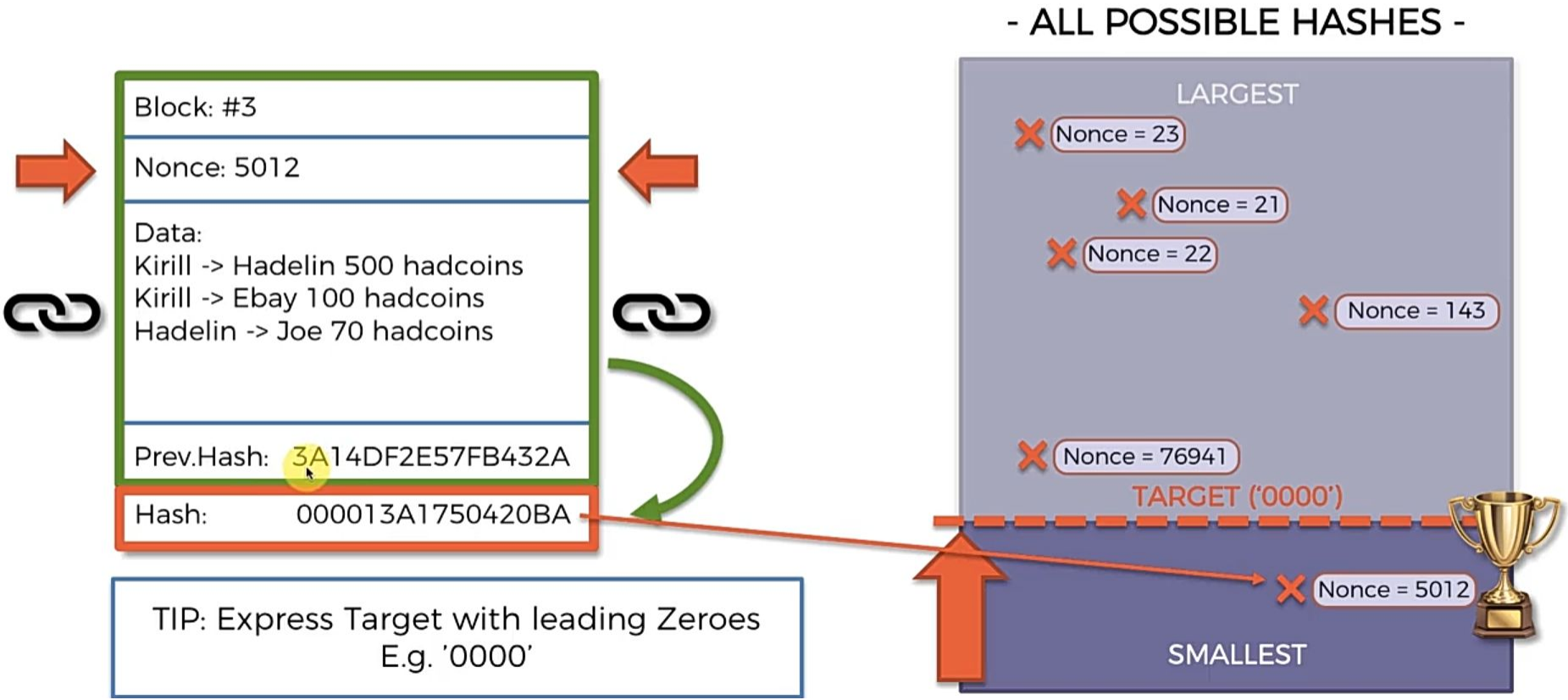
00000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F

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




Courtesy : Super Data Science

# How Mining Works ?

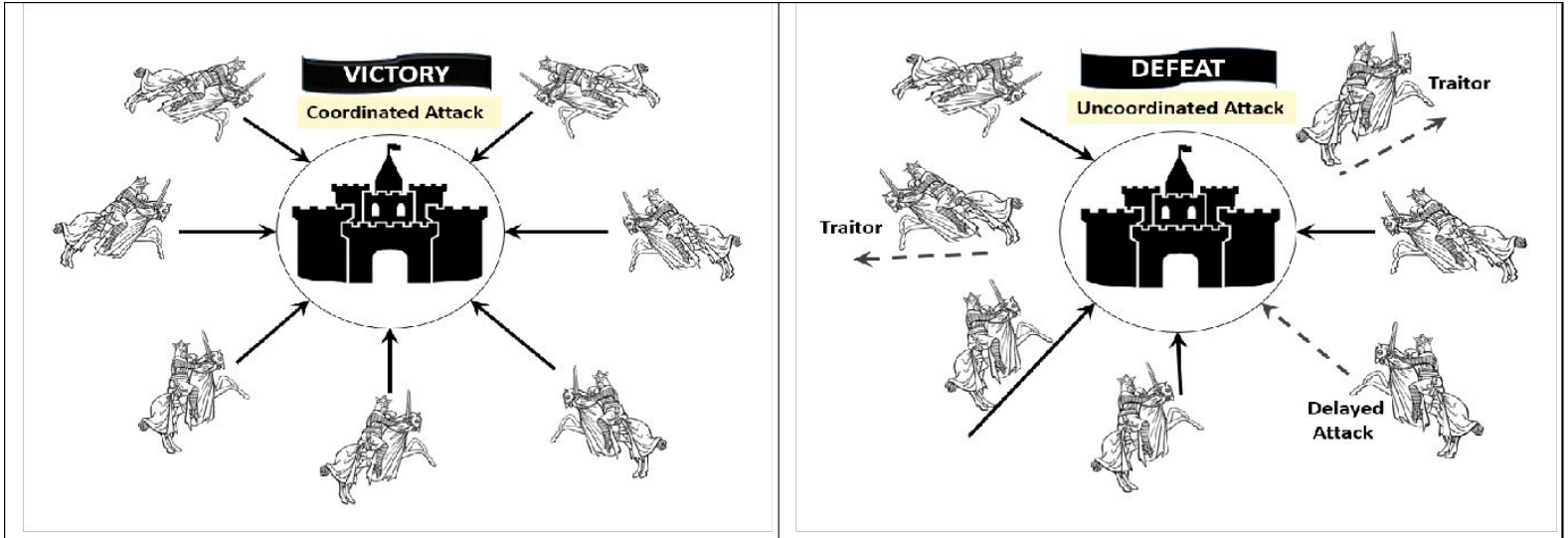


# What is Consensus?

- As per Webster dictionary, a consensus is a **general agreement or opinion shared by all the people in a group.**
- A protocol is a **system of standard rules that are acceptable by all parties** to control the exchange of information in a network. Thus, a **consensus protocol** in Blockchain can be defined as **a set of rules and procedures for attaining a unified agreement (consensus) between the participating nodes** on the status of the network.
- The consensus protocol **aims to overcome the classic problem of a distributed computing system known as the Byzantine Generals Problem**

Courtesy : Super Data Science

# Byzantine General Problem




Coordinated attack leading to victory

Uncoordinated attack leading to defeat

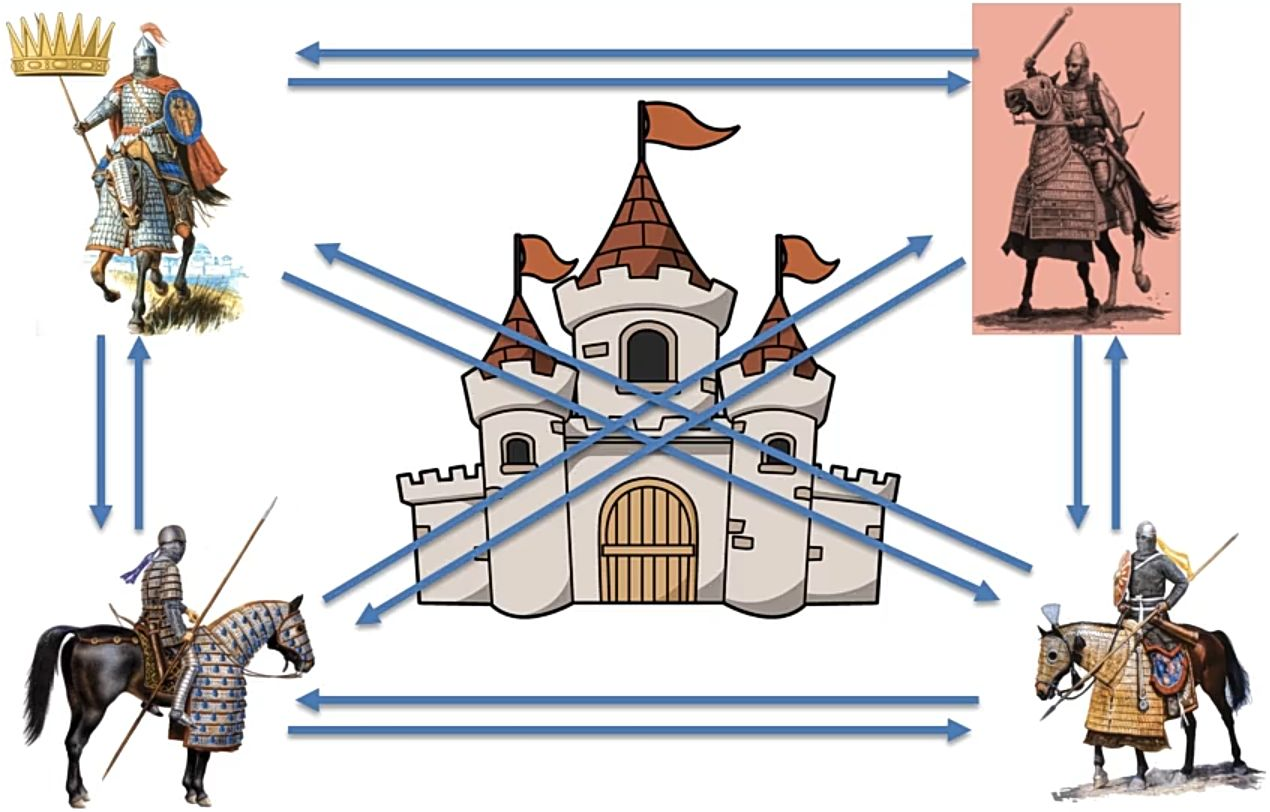
Figure 2.12: Byzantine Generals Problem

Courtesy : Super Data Science

# Objectives of Consensus Protocol

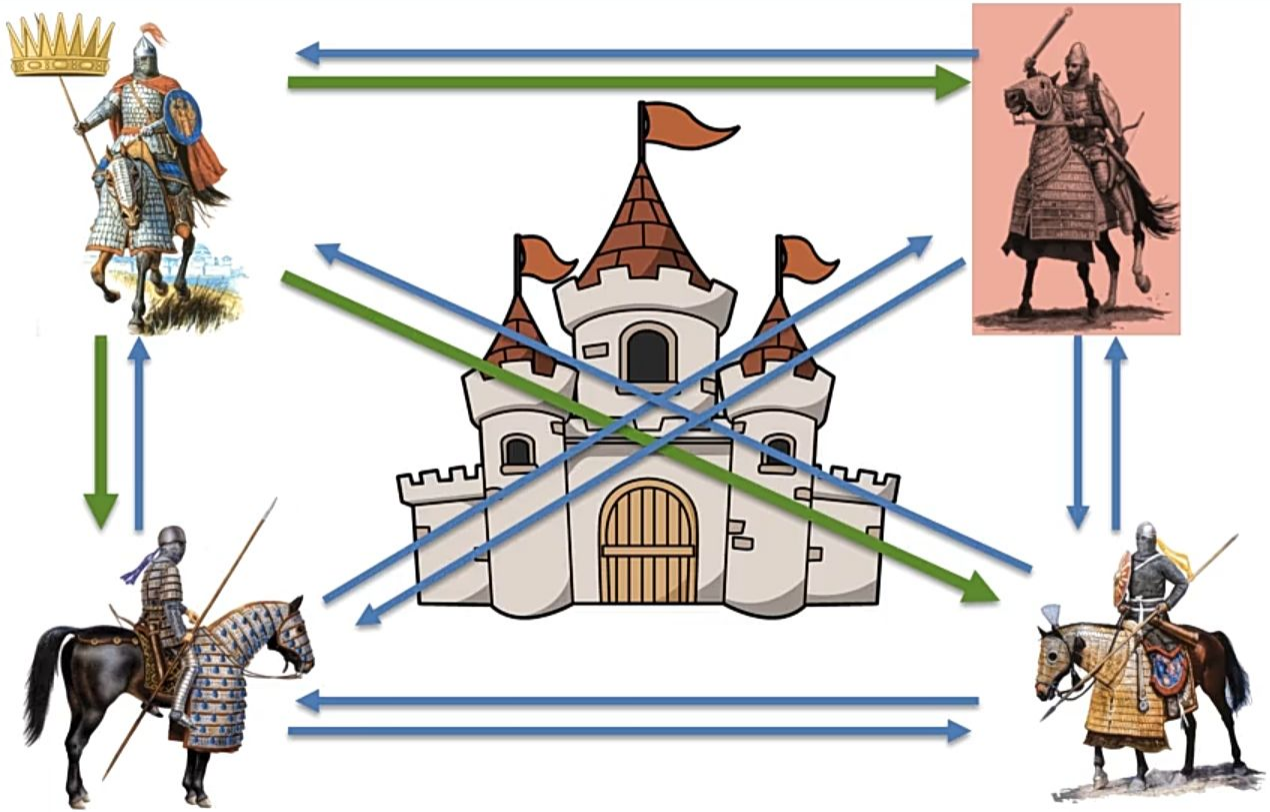

Courtesy : Super Data Science

# Byzantine Fault Tolerance



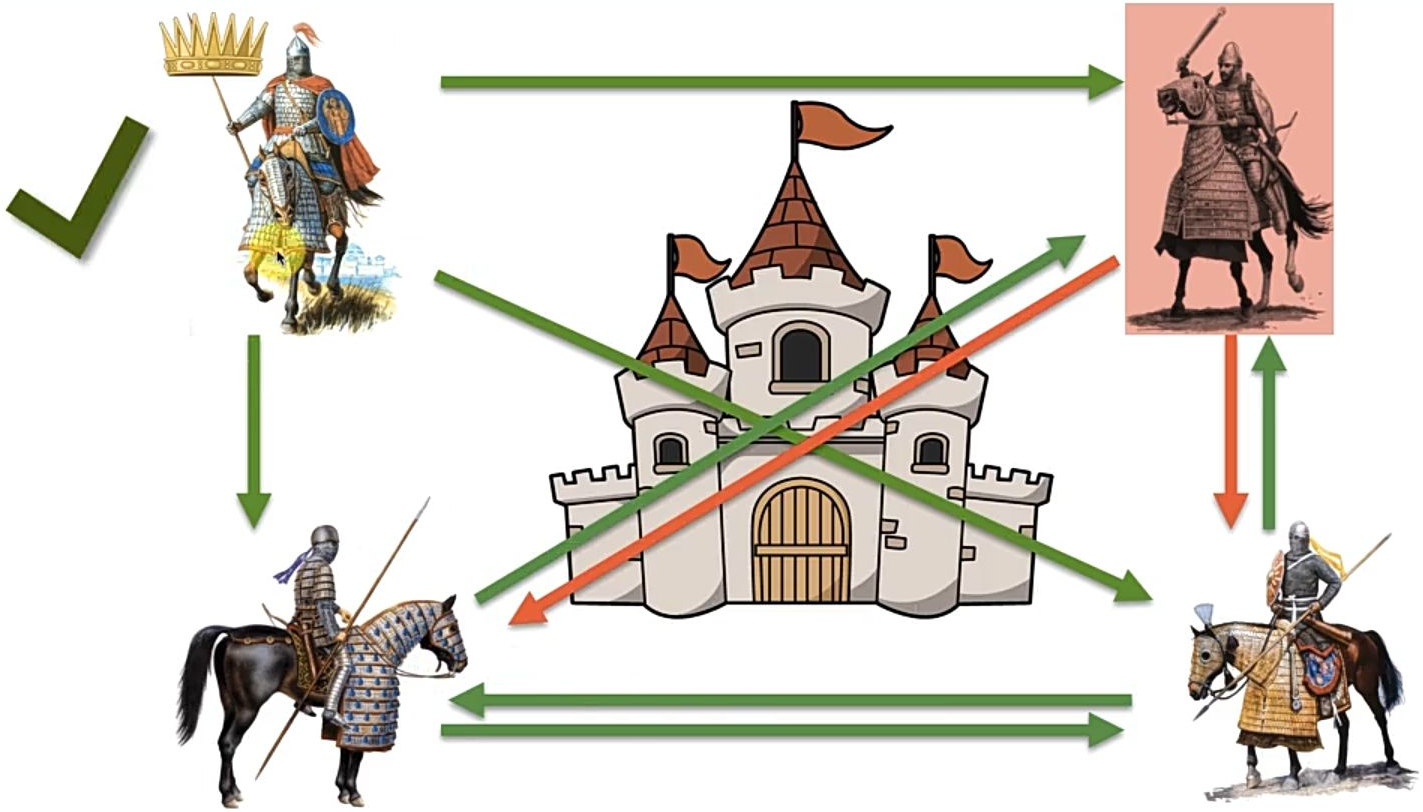
Courtesy : Super Data Science

# Byzantine Fault Tolerance



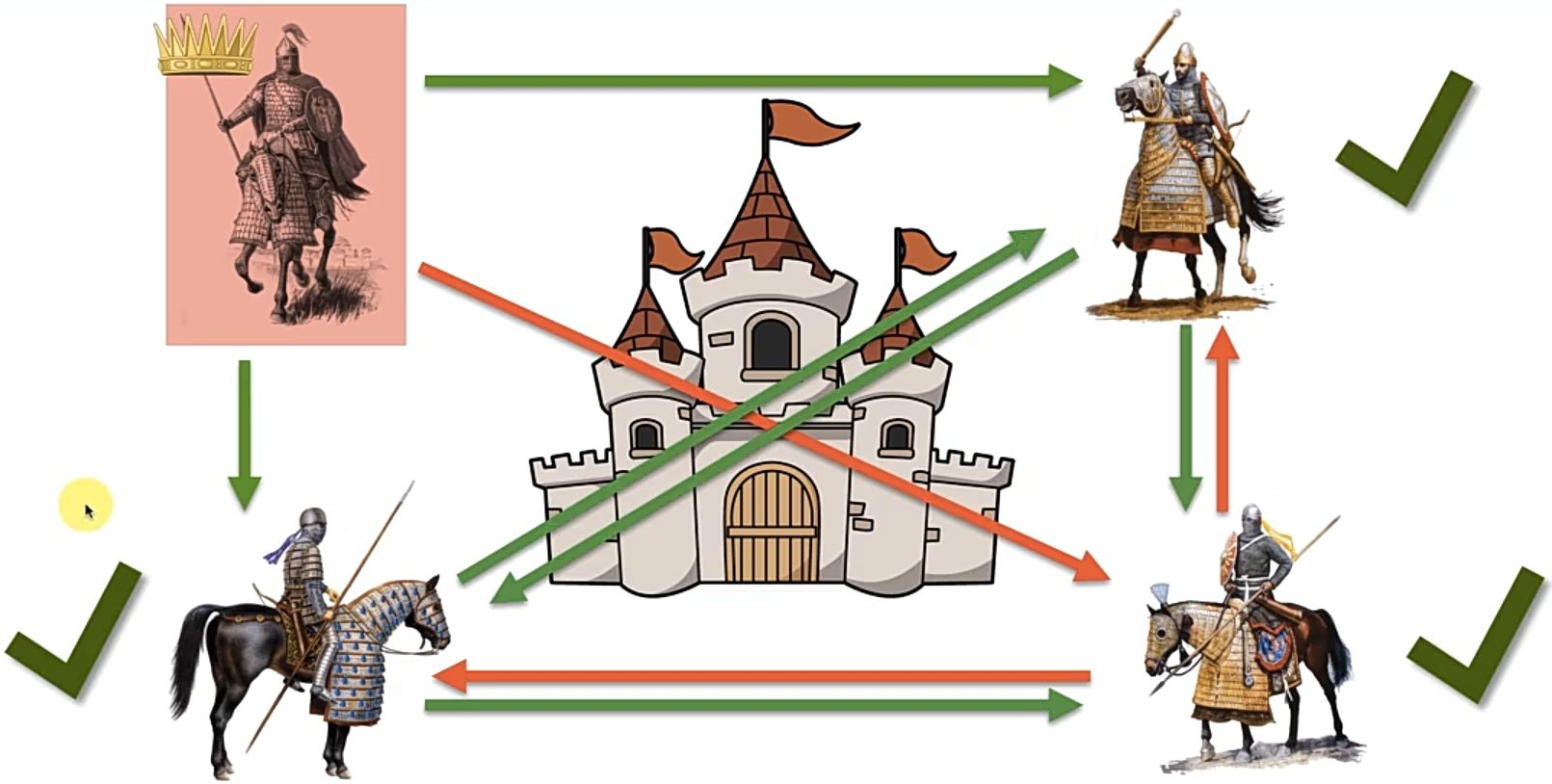
Courtesy : Super Data Science

# Byzantine Fault Tolerance



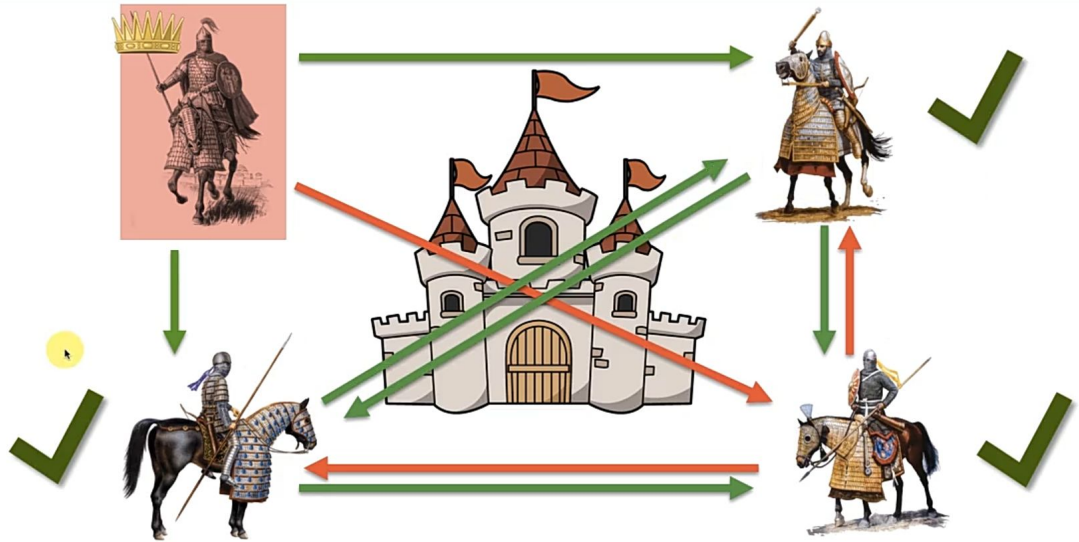
Courtesy : Super Data Science

# Byzantine Fault Tolerance



Courtesy : Super Data Science

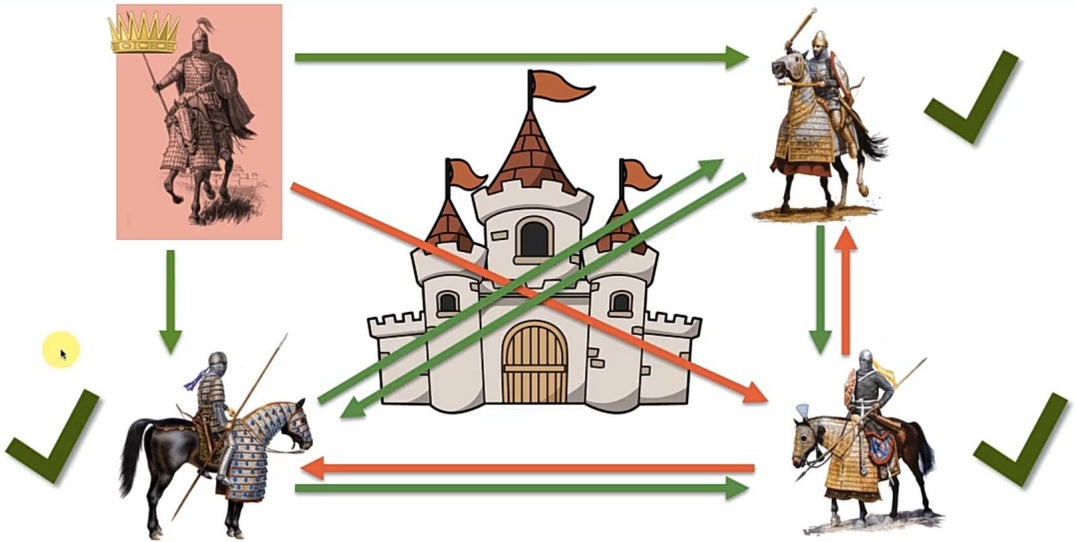
# Byzantine Fault Tolerance



- What is the level of tolerance ?
- What if there are 2 traitors in this network ?
- **Not more than** ⅓ in the Army can be traitors.

Courtesy : Super Data Science

# Byzantine Fault Tolerance

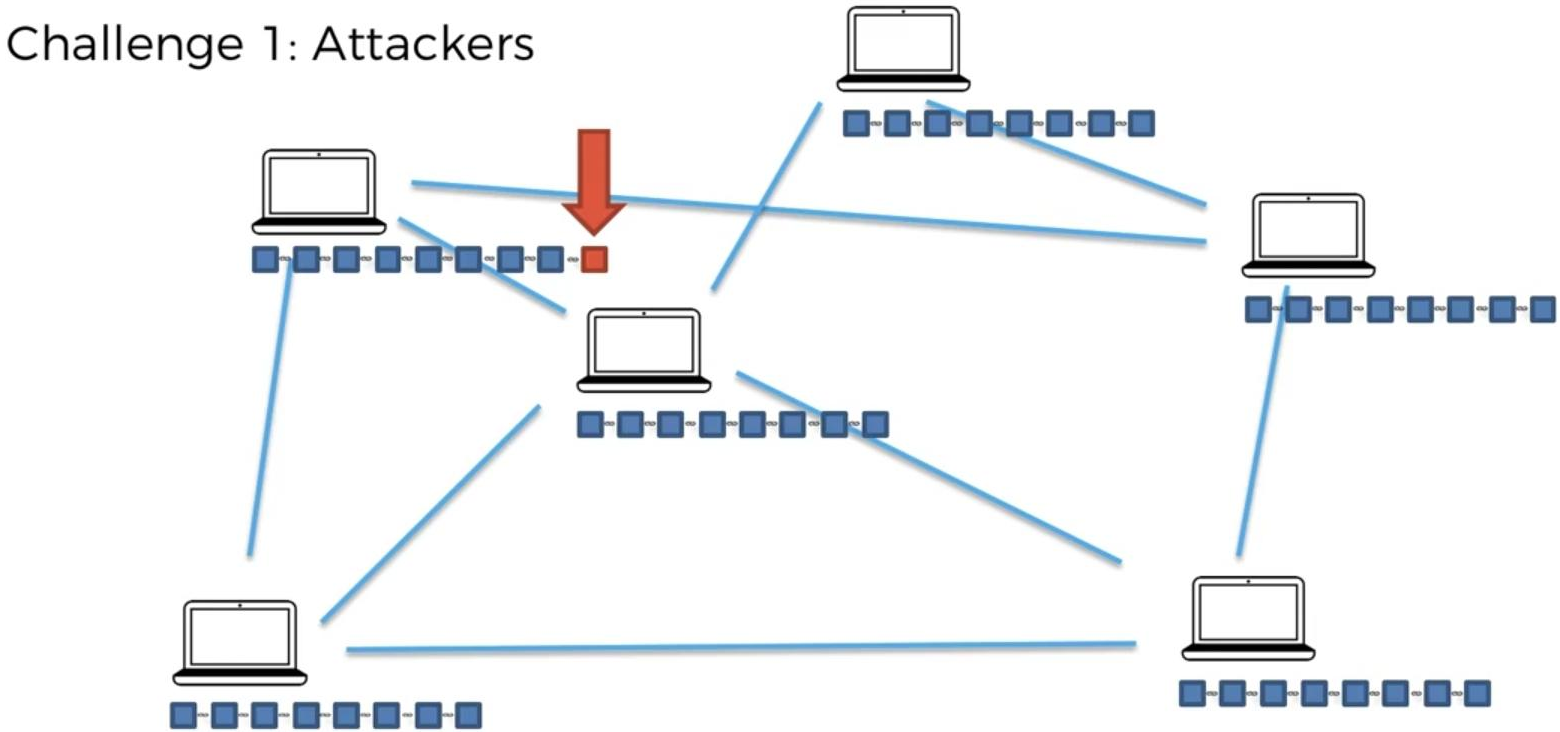


## Applications of BFT

- Blockchain
- Aeroplane Circuits
- Nuclear Power Plants
- Rockets, etc …

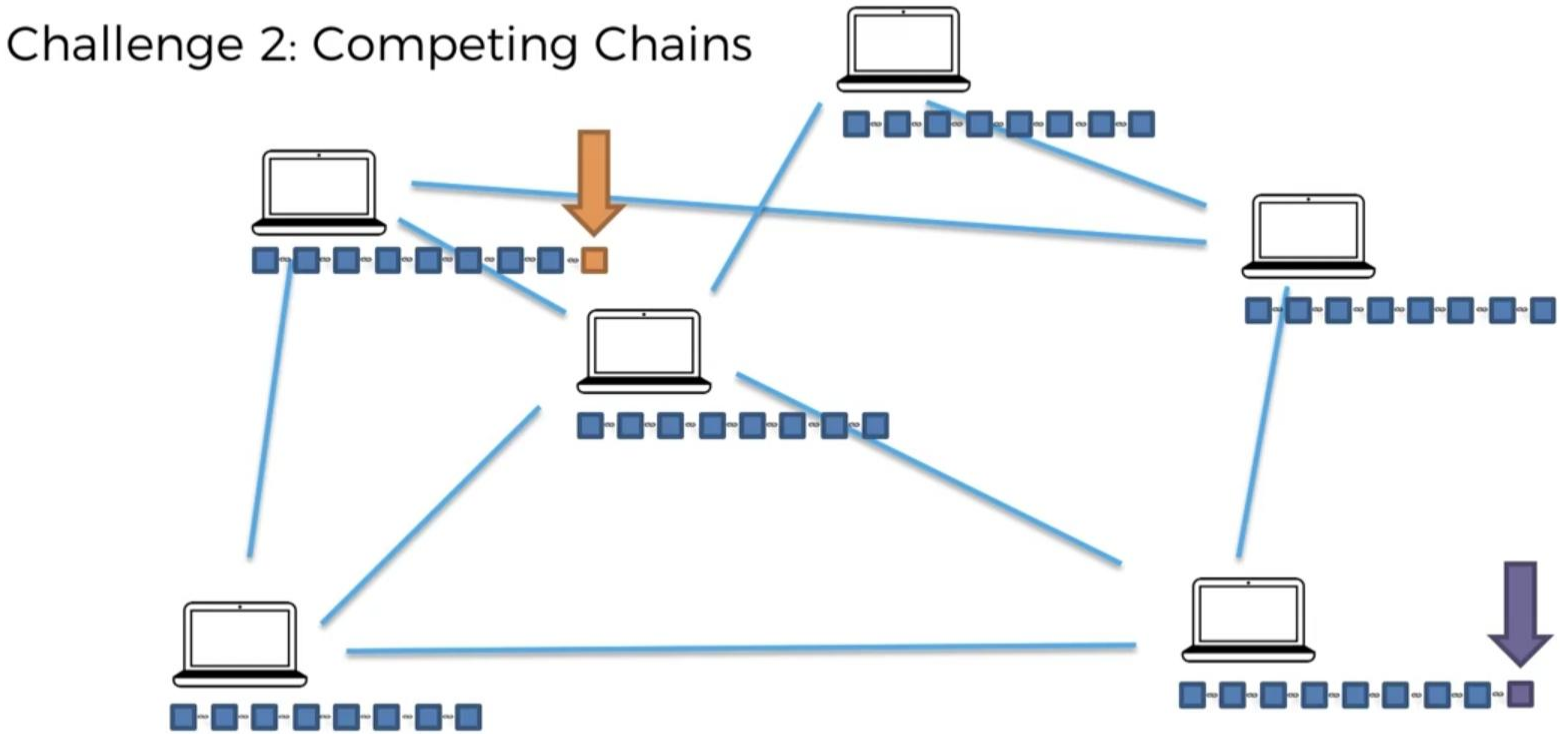
Courtesy : Super Data Science

# Challenges Addressed by Consensus Protocol



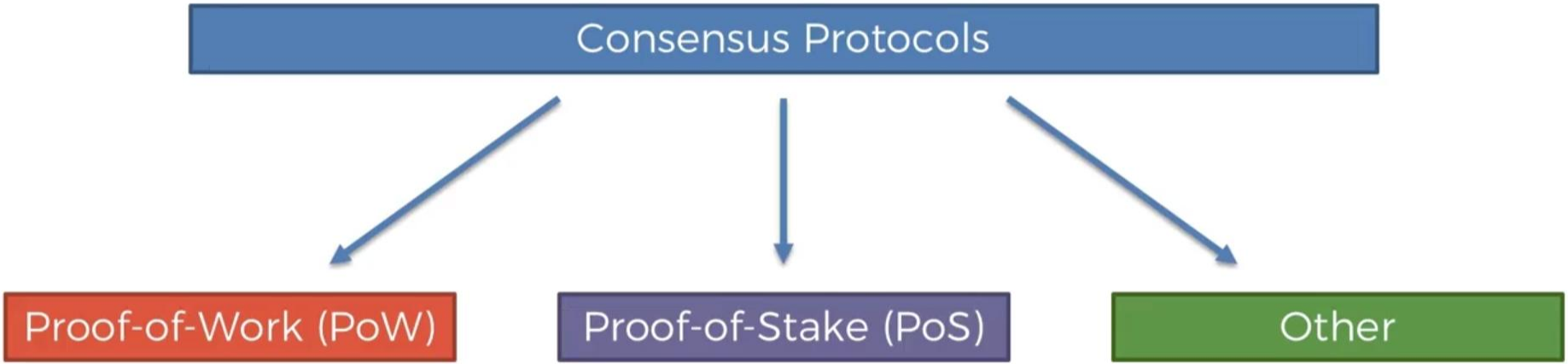

Courtesy : Super Data Science

# Challenges Addressed by Consensus Protocol



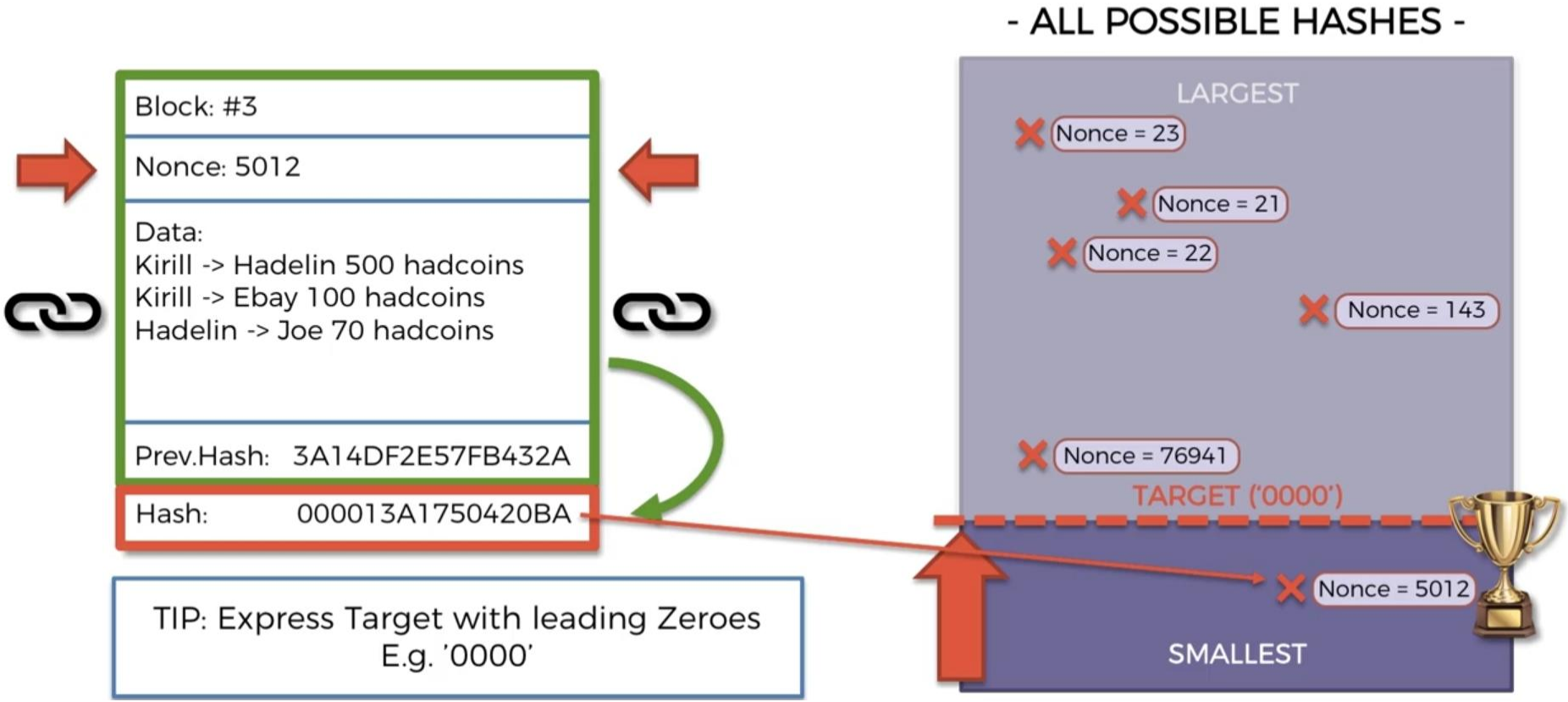

Courtesy : Super Data Science

# Consensus Protocol



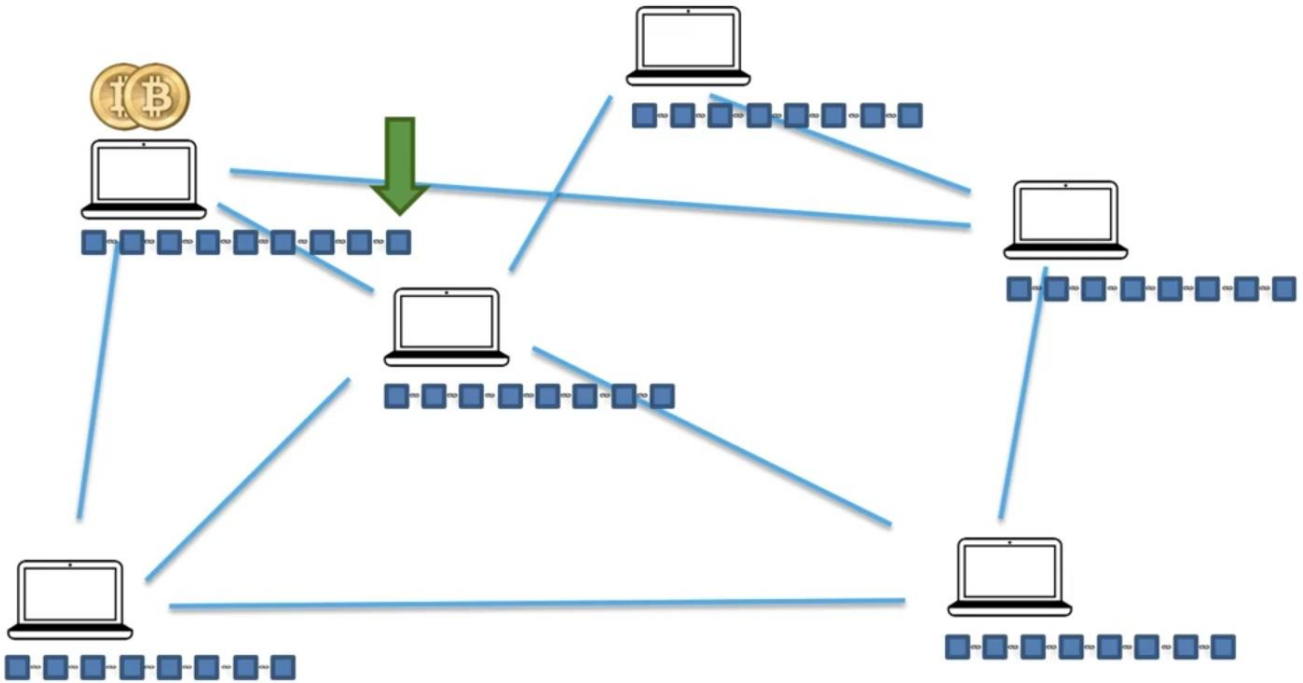

Courtesy : Super Data Science

# Consensus Protocol - Cryptographic Challenge




Courtesy : Super Data Science

# Consensus Protocol - Attackers Challenge

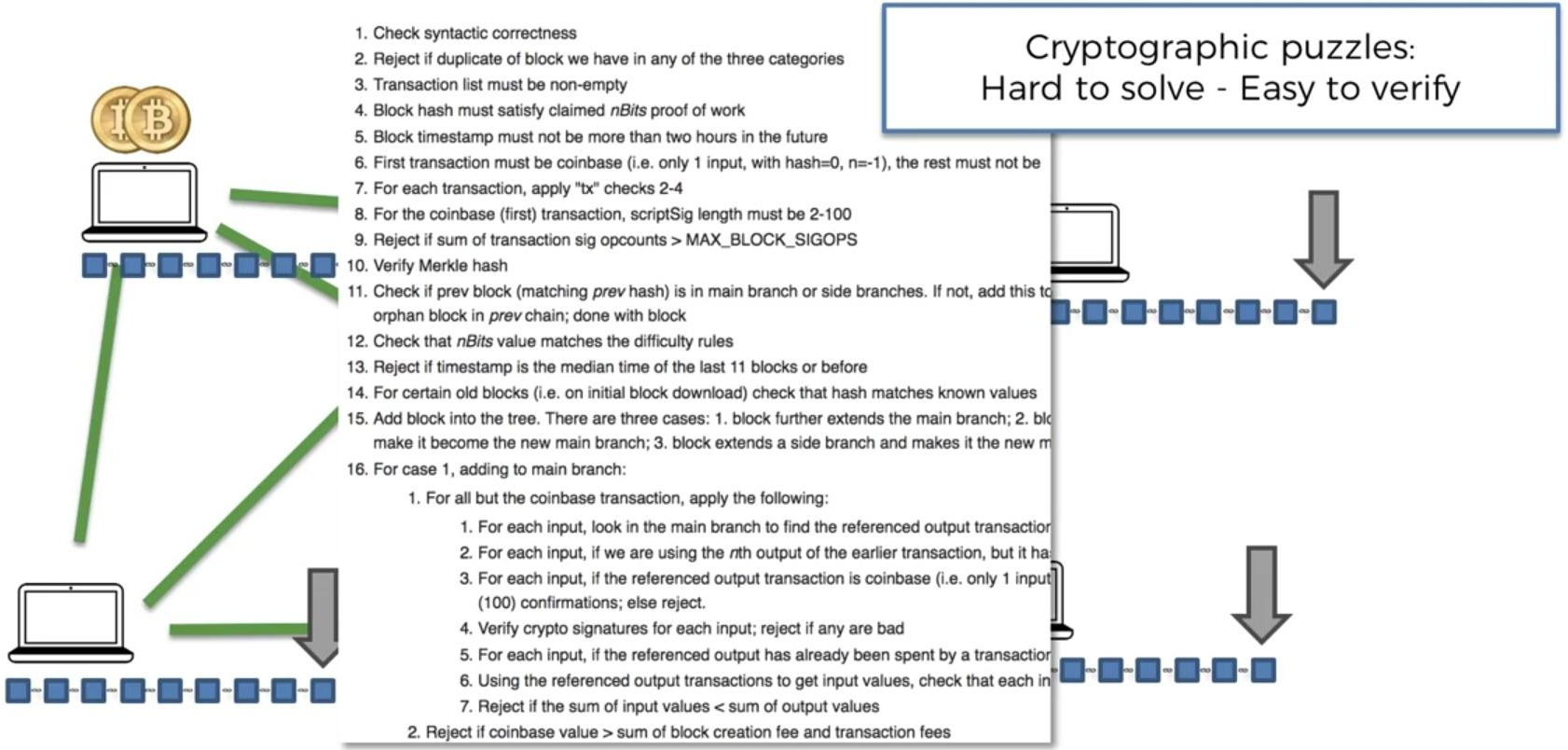


**Miners get incentives for** :

1. **Adding a block**
2. **To play fair**
3. **From the transaction fees**

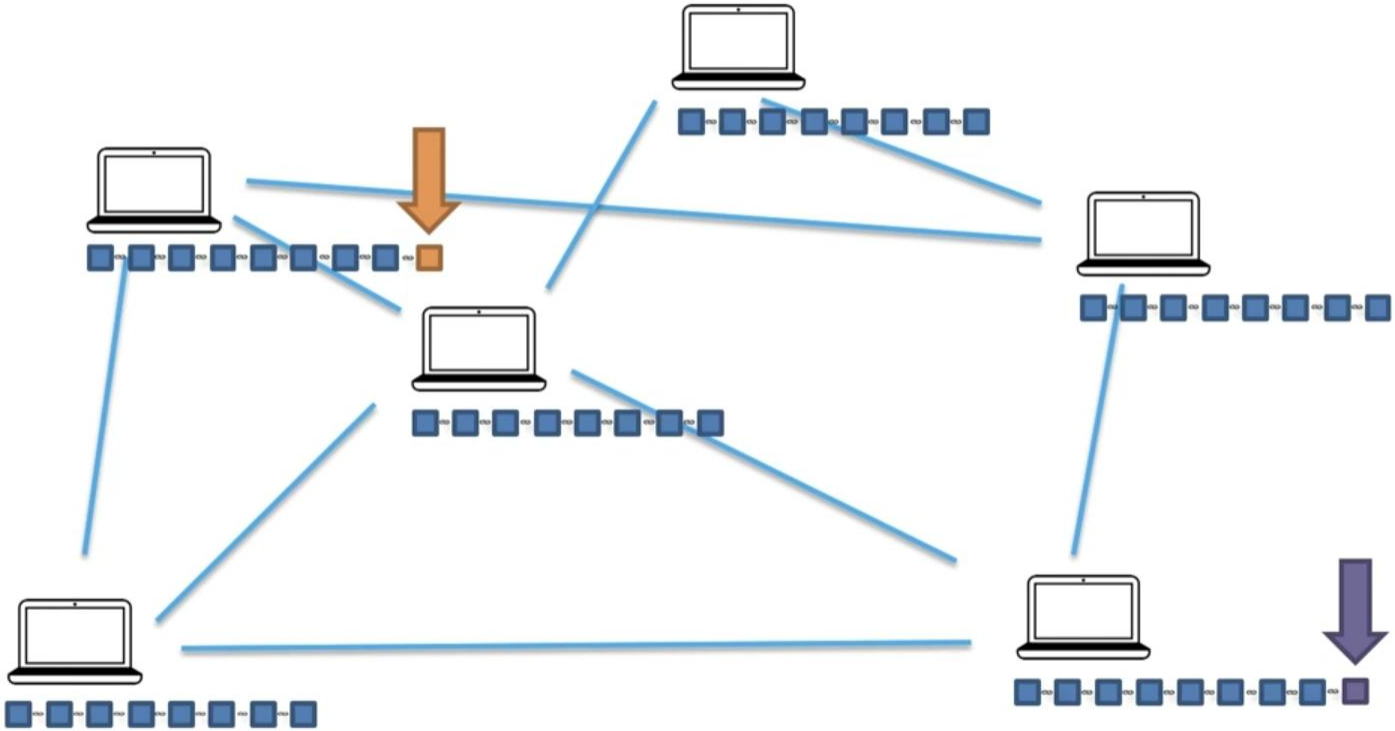
Courtesy : Super Data Science

# Consensus Protocol - Attackers Challenge



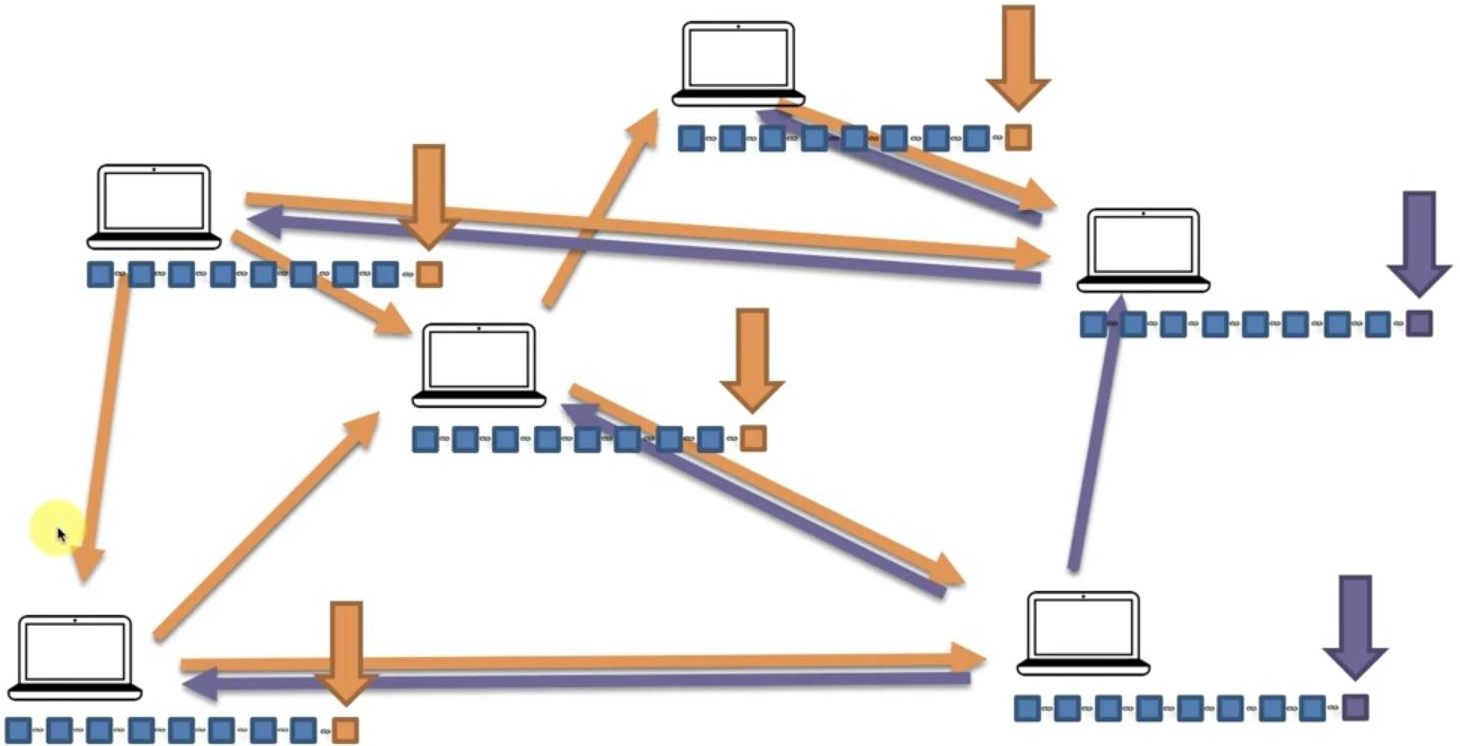

Courtesy : Super Data Science

# Consensus Protocol - Competing Chains



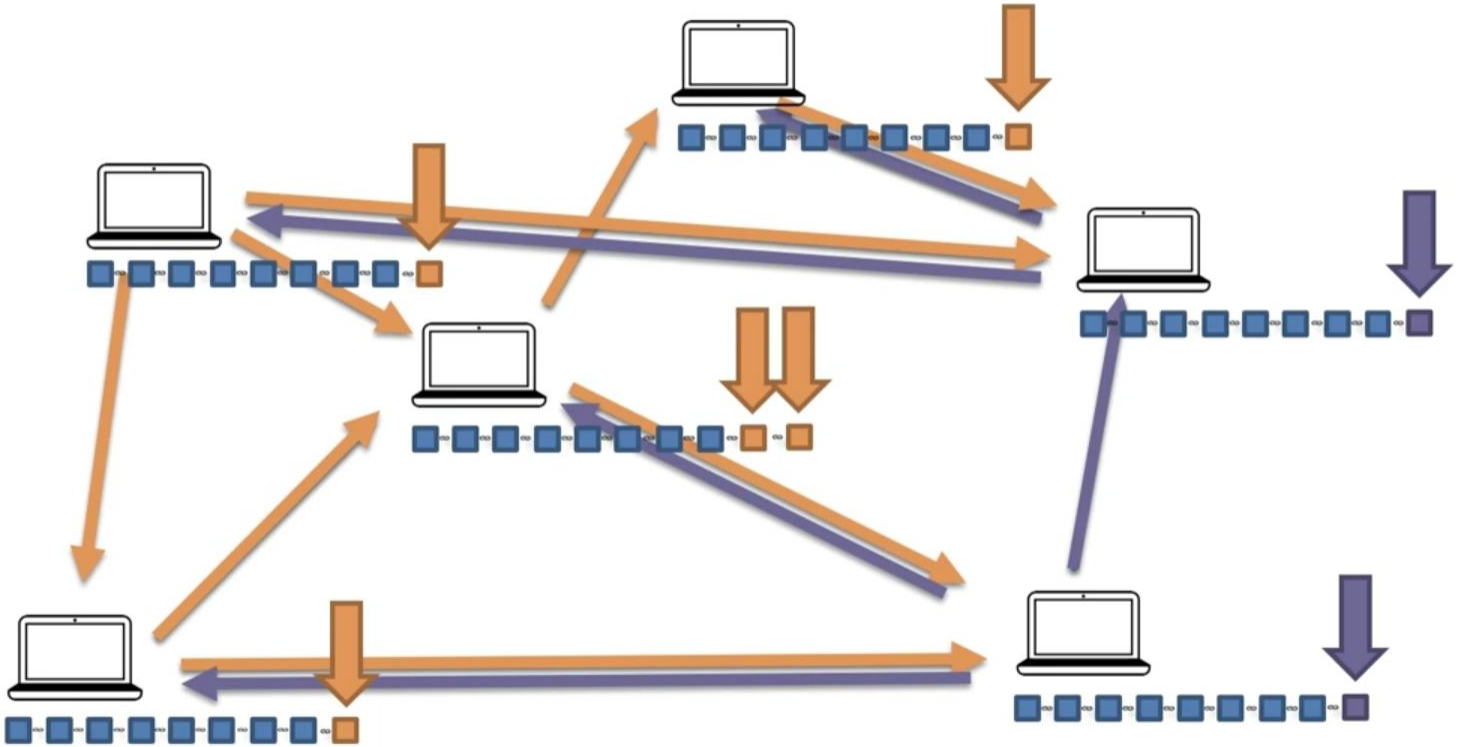
Courtesy : Super Data Science

# Consensus Protocol - Competing Chains



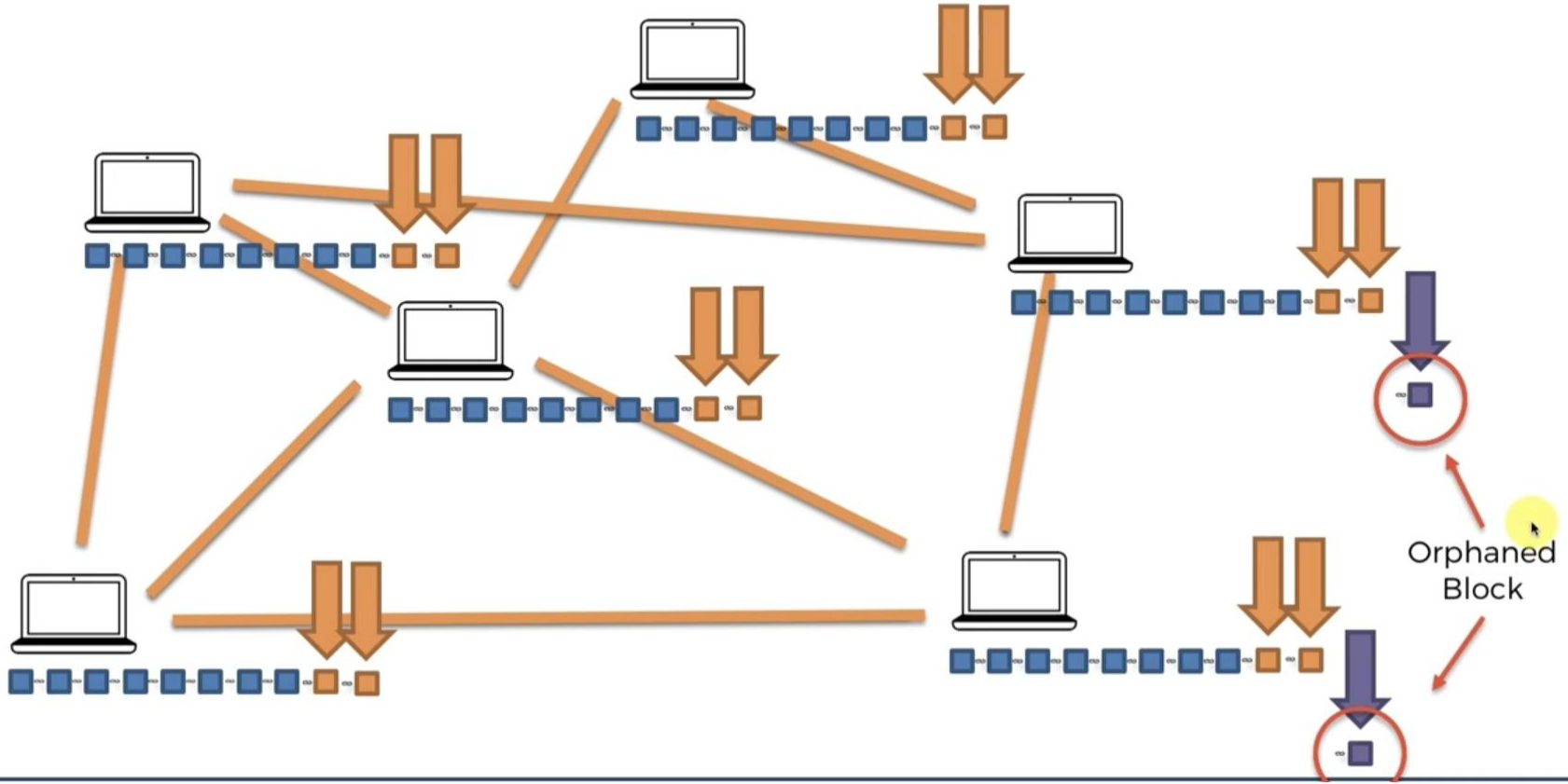
Courtesy : Super Data Science

# Consensus Protocol - Competing Chains

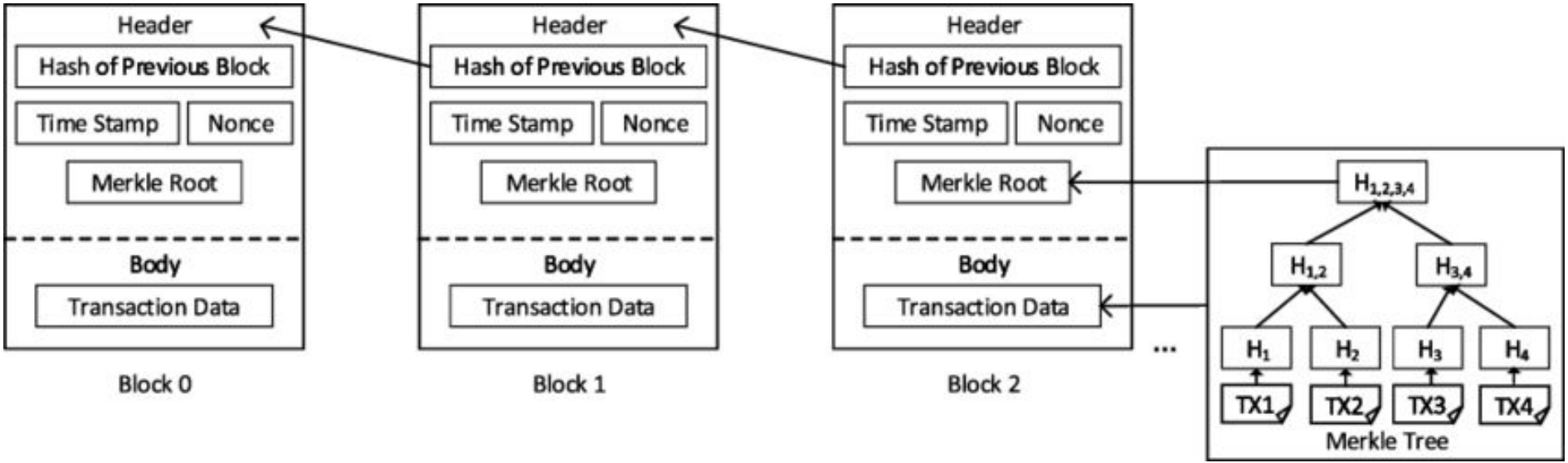


Courtesy : Super Data Science

# Consensus Protocol - Competing Chains



# Block in a Blockchain




Courtesy : Himanshi Blog

# Block in a Blockchain

## Elements of a Block

- **Block Height –** It's the sequence number of the block in the chain of blocks. Block Height: 1 is the genesis block (first block in the network).
- **Block Size –** It's a 4-bytes or 32-bit field that contains the size of the block. It adds size in Bytes. Ex – Block Size: 216 Bytes.
- **Block Reward –** This field contains the amount awarded to the miner for adding a block of transactions.
- **Tx Count –** The transaction counter shows the number of transactions contained by the block. The field has a maximum size of 9 bytes.
- **Block Header –** The Block header is an 80-Byte field that contains the metadata – the data about the block.

Courtesy : Himanshi Blog

# Block in a Blockchain

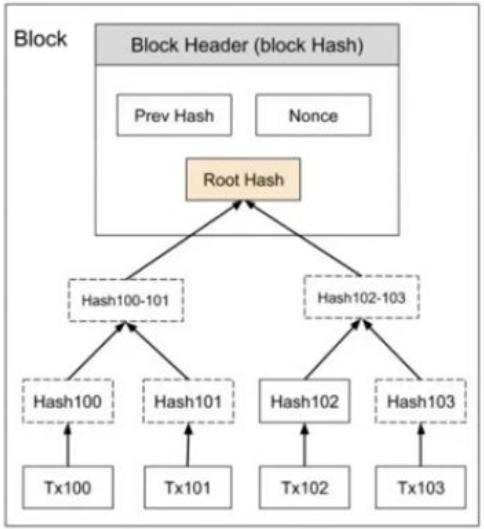
**Components of the Block Header.**

- **Time**
  - It's the digitally recorded *moment of time when the block has been mined.*
  - It is used *to validate the transactions*.
- **Version** –
  - It's a *4-bytes field* representing the *version number of the protocol used.*
  - Usually, for *bitcoin, it's '0x1*'.
- **Previous Block Hash** –
  - It's a *32-bytes field that contains a 256-bits hash* (created by SHA-256 cryptographic hashing) This *helps to create a linear chain of blocks.*
- **Bits** –
  - It's a *4-bytes field* that tells the *complexity to add the block*.
  - It's also known as "*difficulty bits*." According to PoW, the block hash should be less than the difficulty level.
- **Nonce** –
  - It's a *4-bytes field that contains a 32-bit number*. These are the only changeable element in a block of transactions. In PoW, miners alter nonce until they find the right block hash.
- **Merkle Root** –
  - A *32-bytes field containing a 256-bit root hash*.
  - It's *constructed hierarchically combining hashes of the individual transactions in a block.*

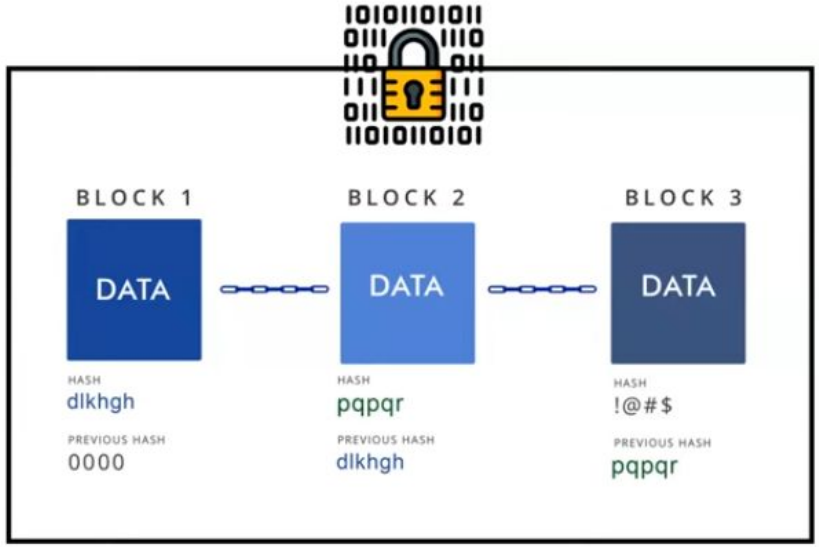
Courtesy : Himanshi Blog

# What is a Merkle Tree ?

Merkle trees are a type of data structure commonly used in computer science. They are used to encrypt blockchain data more effectively and securely in bitcoin and other cryptocurrencies.




Merkle Tree

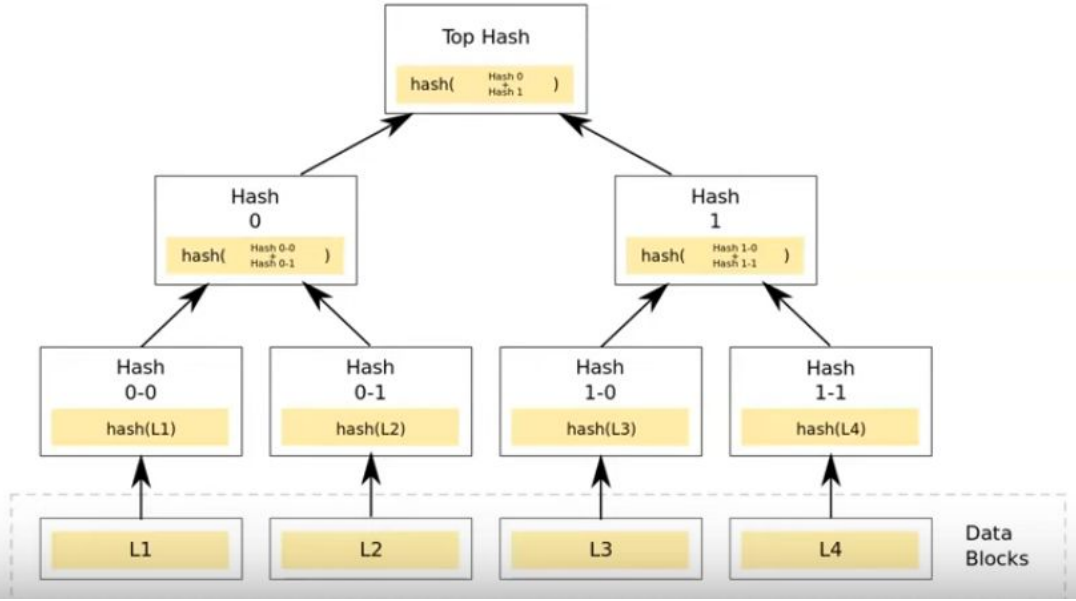



Blockchain Data encrypted Securely

Courtesy : Ravikiran A S Blog

# What is a Merkle Tree ?

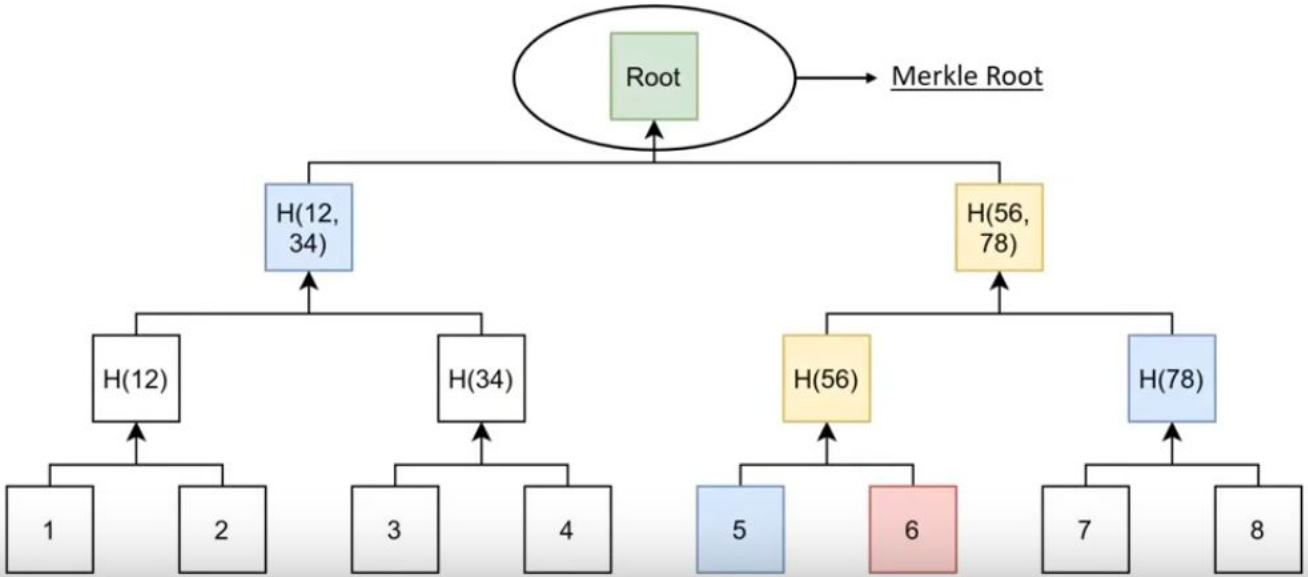
It's a mathematical data structure or a method of organizing data, made up of hash number of various data blocks of transactions performed of the Blockchain Network. It acts as a summary of all the transactions.




Courtesy : Ravikiran A S Blog

# What is a Merkle Root ?

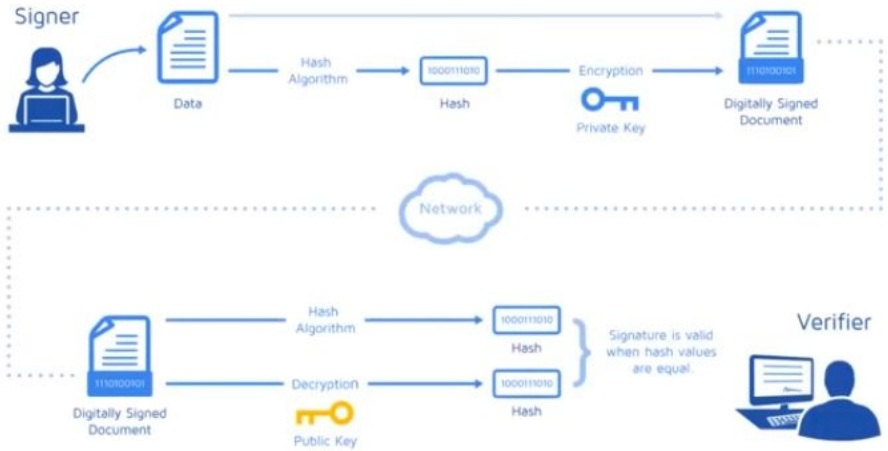
Merkle root is a simple mathematical method for confirming the facts on a Merkle tree. They're used in cryptocurrency to ensure that data blocks sent through a peer-to-peer network are secure.




Courtesy : Ravikiran A S Blog

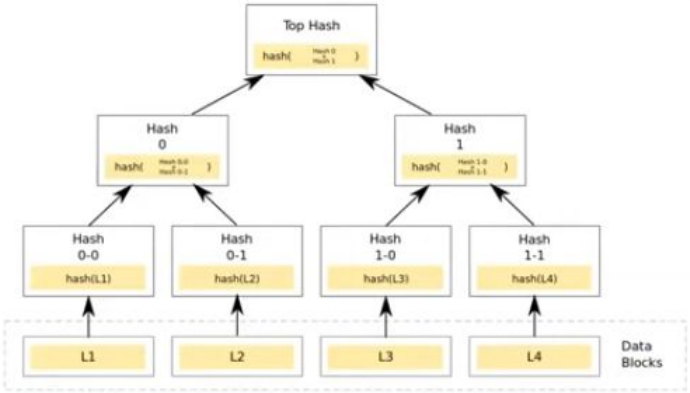
# How does a Merkle Tree work ?

A Merkle tree totals all transactions in a block and generates a digital fingerprint of the entire set of operations, allowing the user to verify whether a transaction is included in the block.




Courtesy : Ravikiran A S Blog

# Benefits of Merkle Tree




Validate the data's integrity

Takes little disk space

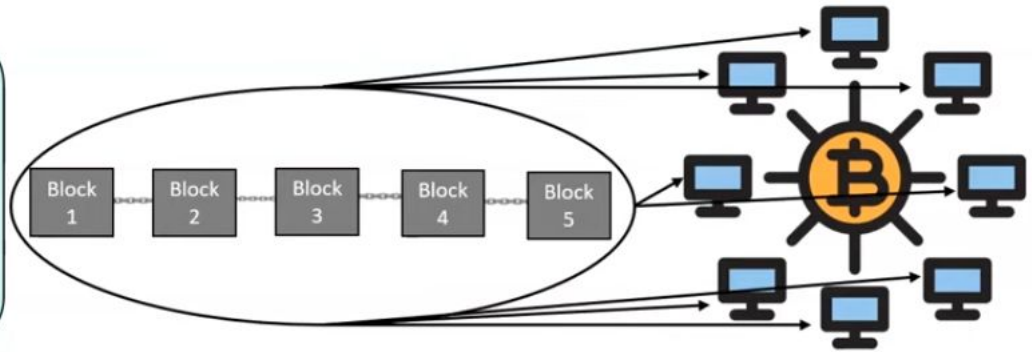
Tiny information across networks

Efficient Verification

Courtesy : Ravikiran A S Blog

# Why is it essential for Blockchain ?

If Bitcoin didn't include Merkle Trees, for example, every node on the network would have to retain a complete copy of every single Bitcoin transaction ever made.

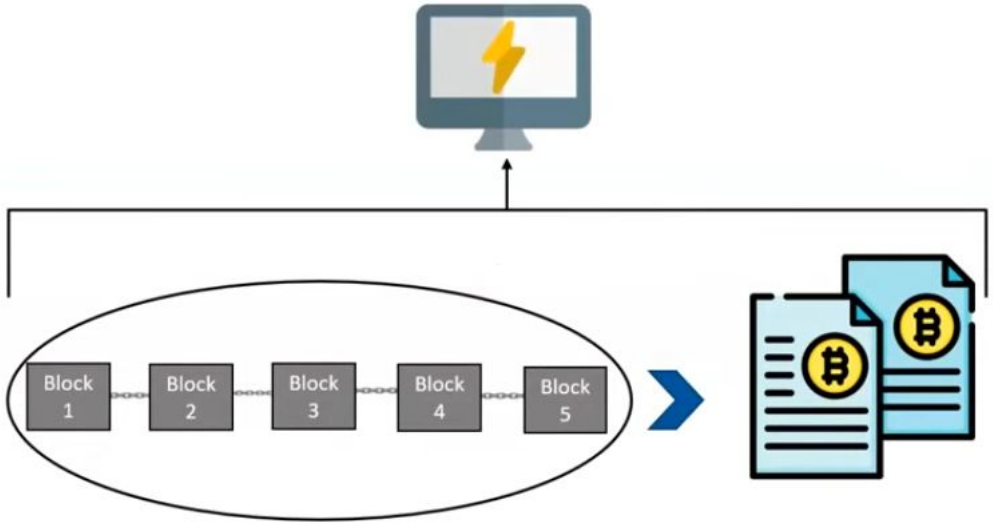



Too much information for every node to validate on their own

Courtesy : Ravikiran A S Blog

# Why is it essential for Blockchain ?

To confirm that there were no modifications, a computer used for validation would need a lot of computing power to compare ledgers.

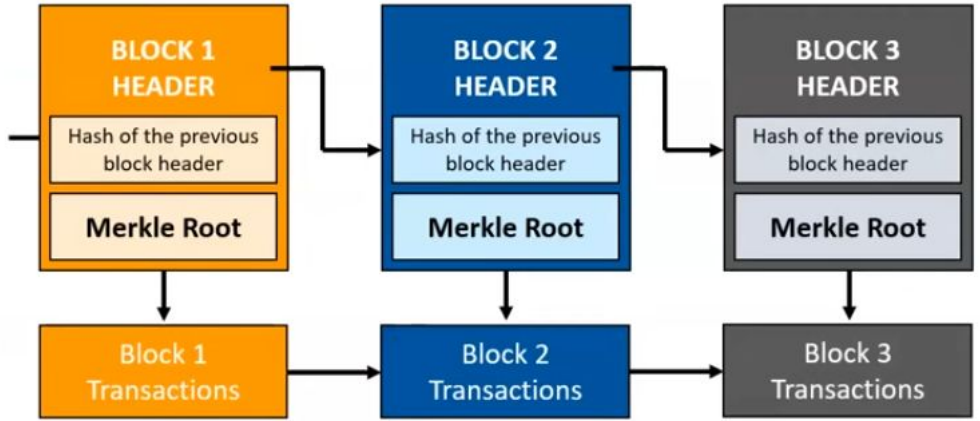



Comparing ledgers using a lot of computing power

Courtesy : Ravikiran A S Blog

# Why is it essential for Blockchain ?

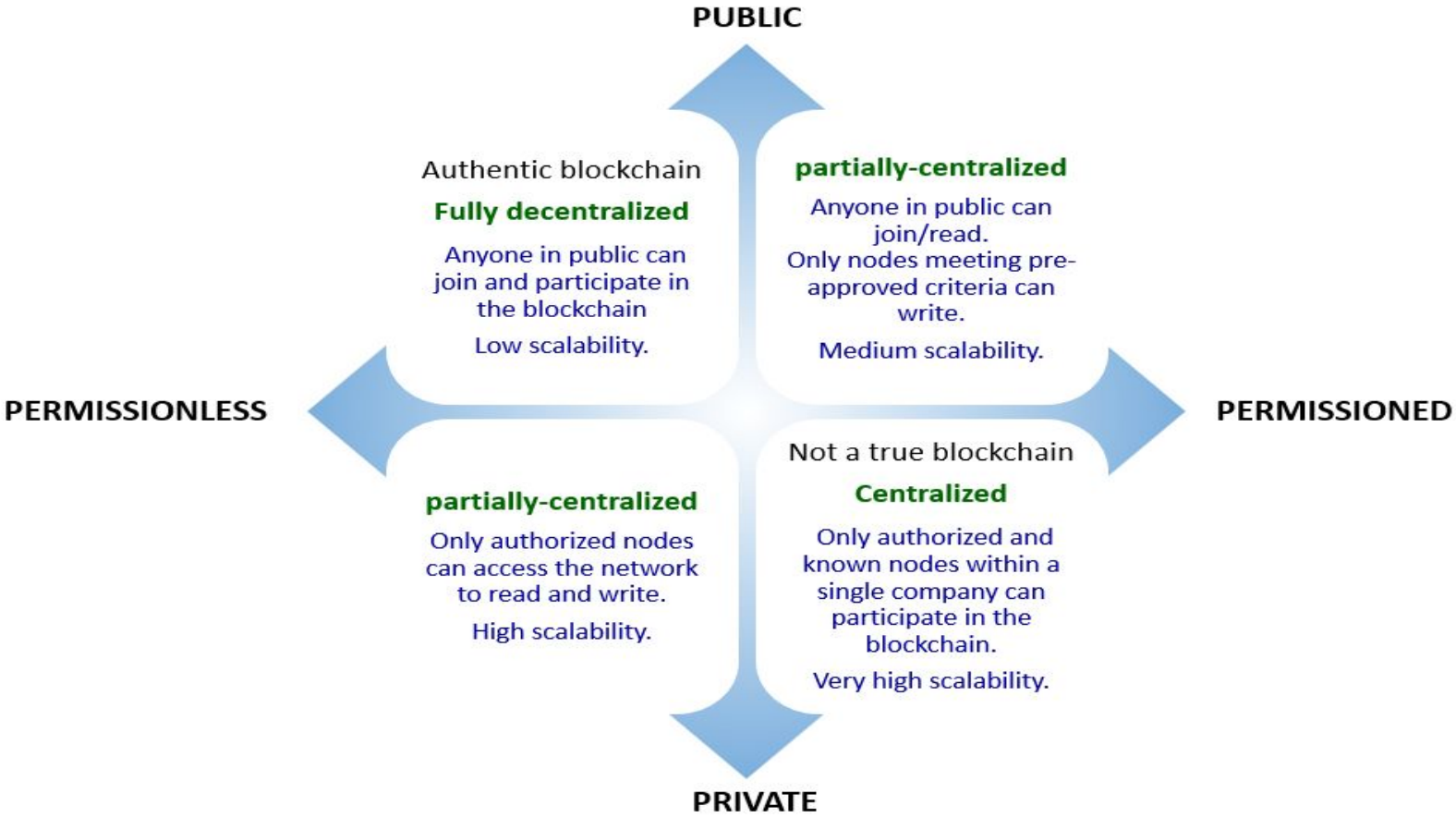
Merkle Trees hash records in accounting, thereby separating the proof of data. Proving that given information across the network is all that is required for a transaction to be valid.



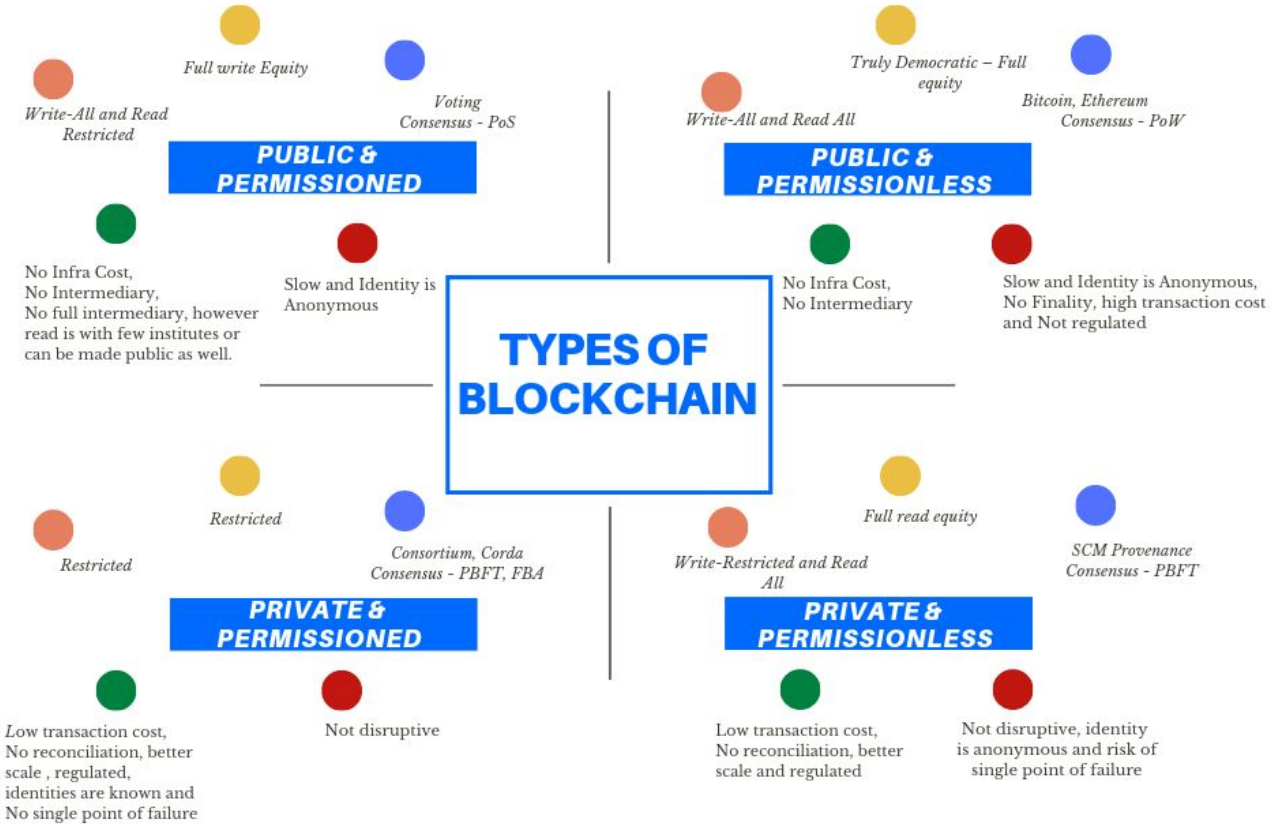

Merkle Tree breaking the data into tiny parts of information

Courtesy : Ravikiran A S Blog

# Types of Blockchain

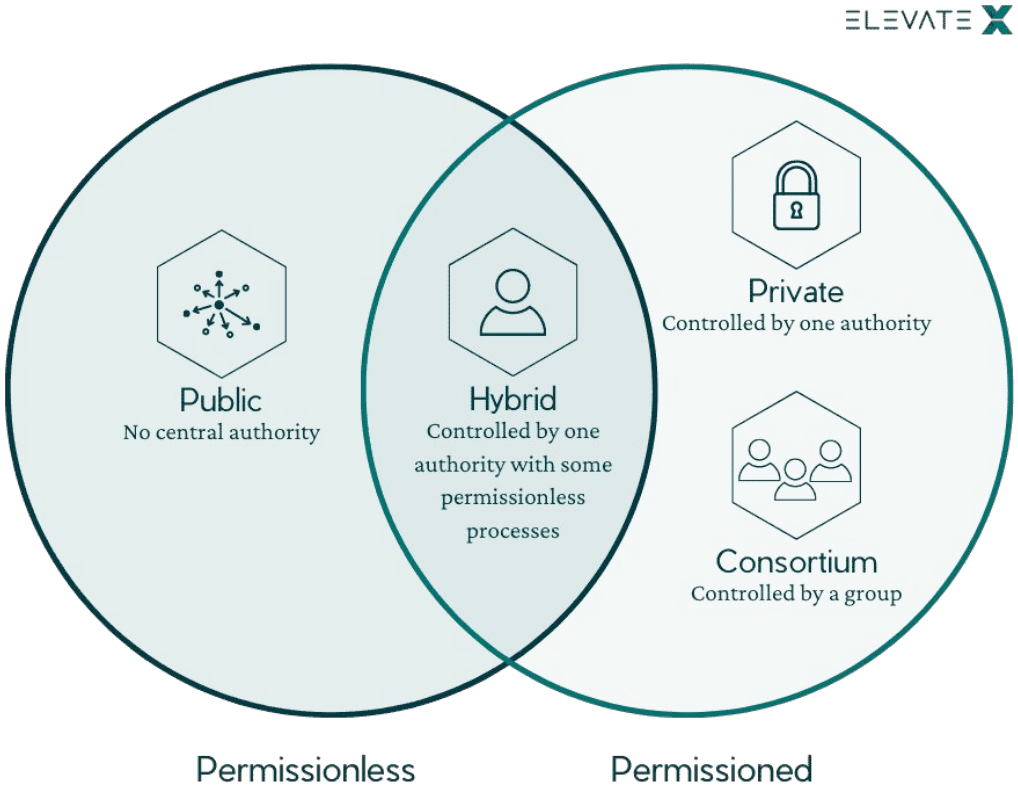


# Types of Blockchain

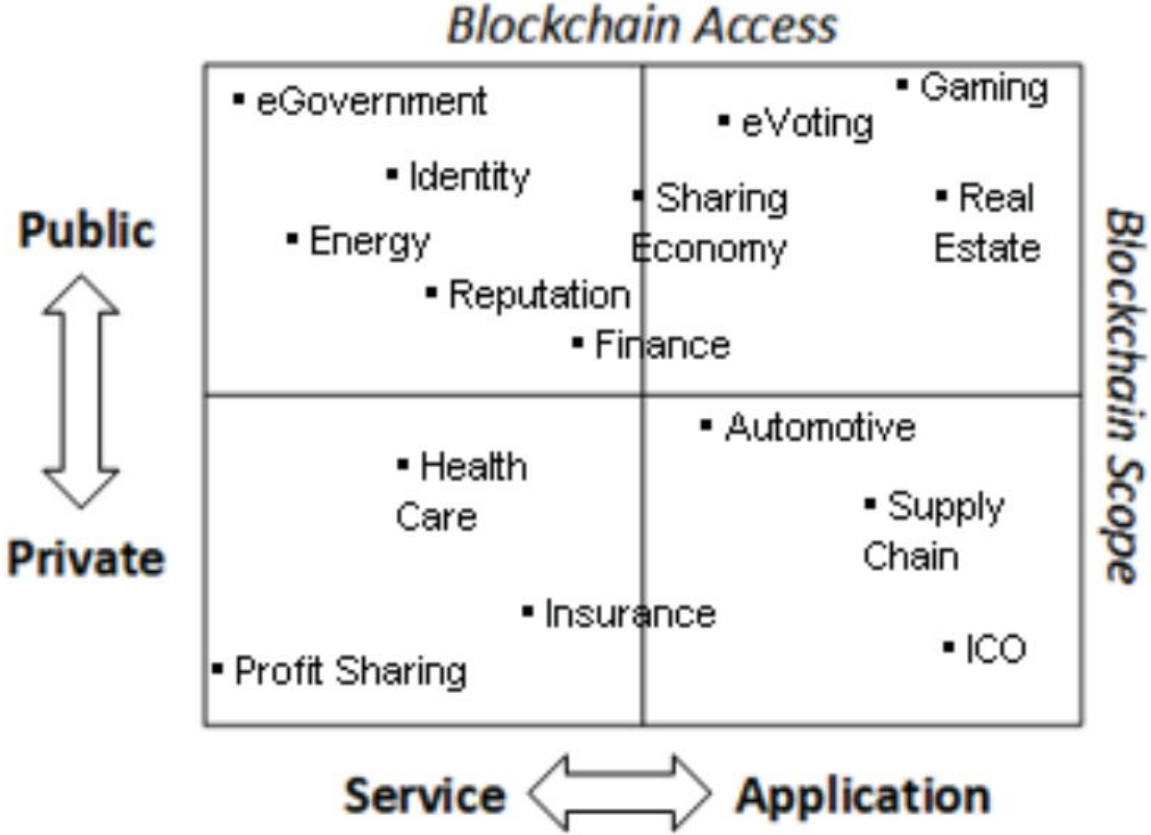



Courtesy : PacktPub

# Types of Blockchain



# Types of Blockchain



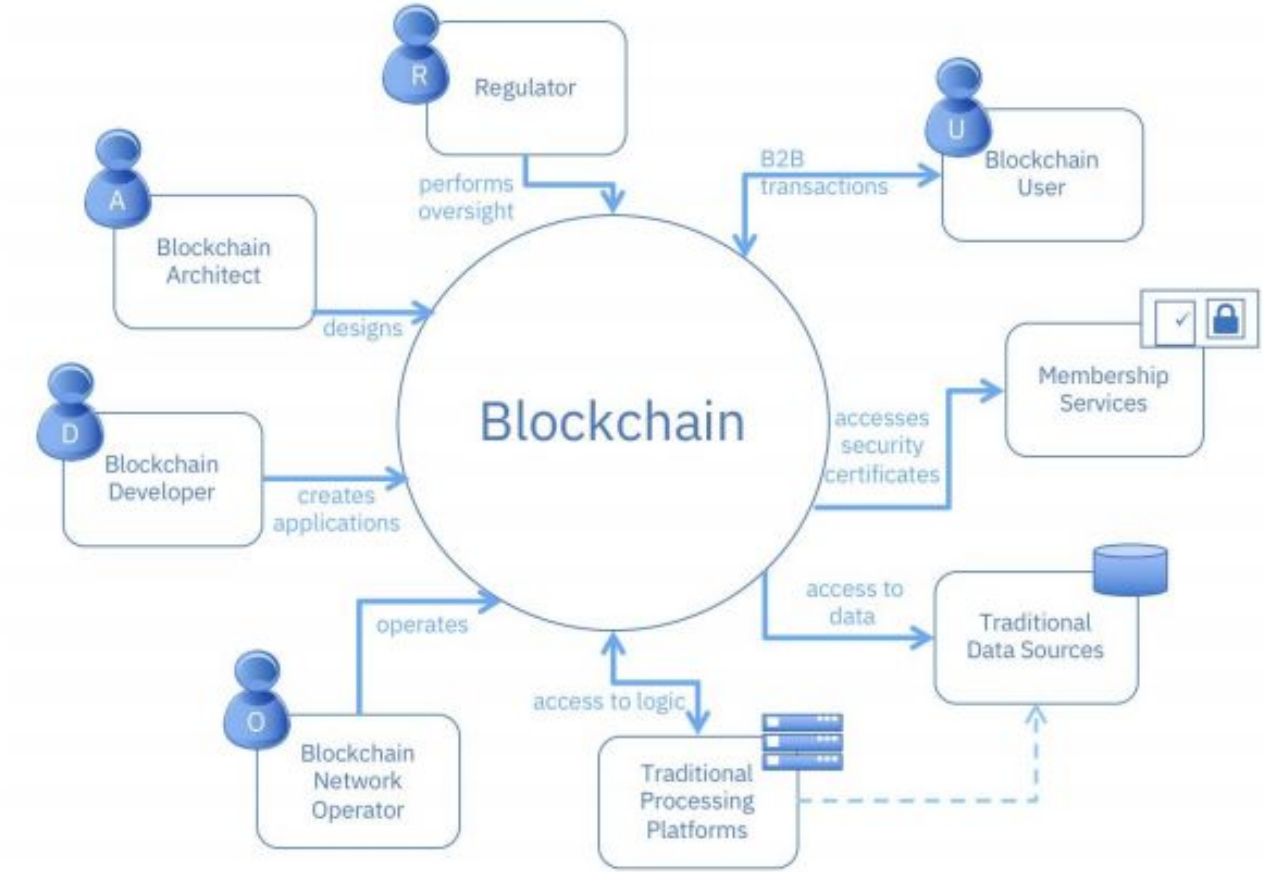

Courtesy : Noah Fields

# Types of Blockchain

| | Public (permissionless) | Private (permissioned) | Hybrid | Consortium |
|---|---|---|---|---|
| ADVANTAGES | + Independence<br>+ Transparency<br>+ Trust | + Access control<br>+ Performance | + Access control<br>+ Performance<br>+ Scalability | + Access control<br>+ Scalability<br>+ Security |
| DISADVANTAGES | – Performance<br>– Scalability<br>– Security | – Trust<br>– Auditability | – Transparency<br>– Upgrading | – Transparency |
| USE CASES | ▪ Cryptocurrency<br>▪ Document validation | ▪ Supply chain<br>▪ Asset ownership | ▪ Medical records<br>▪ Real estate | ▪ Banking<br>▪ Research<br>▪ Supply chain |

Courtesy : Christine Campbell

# Actors in a Blockchain




Courtesy : Ravi Natarajan LinkedIn

# Limitations and challenges of blockchain


Courtesy : Witscad

# Thank you