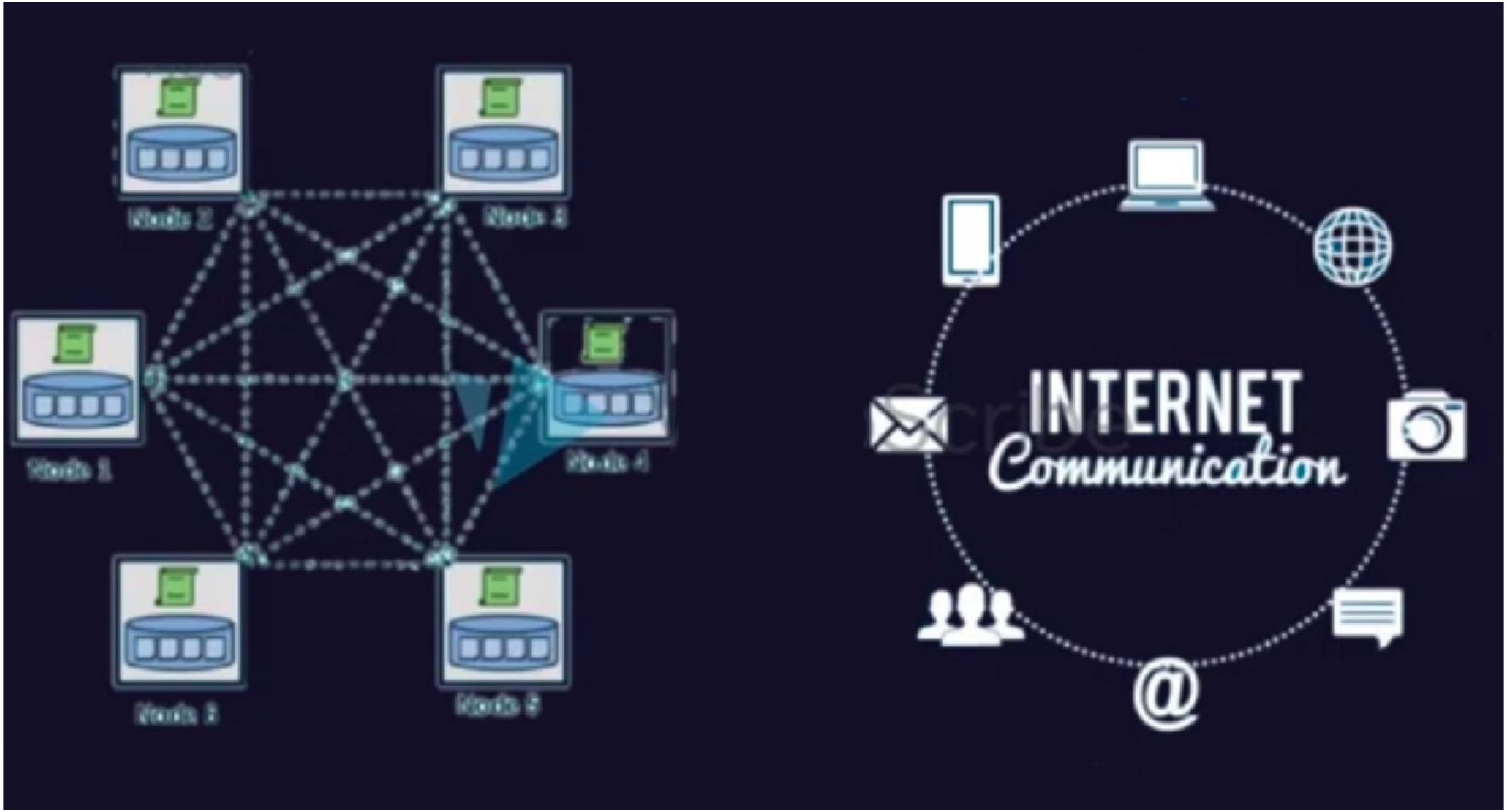
Block Chain / Block Chain Architecture

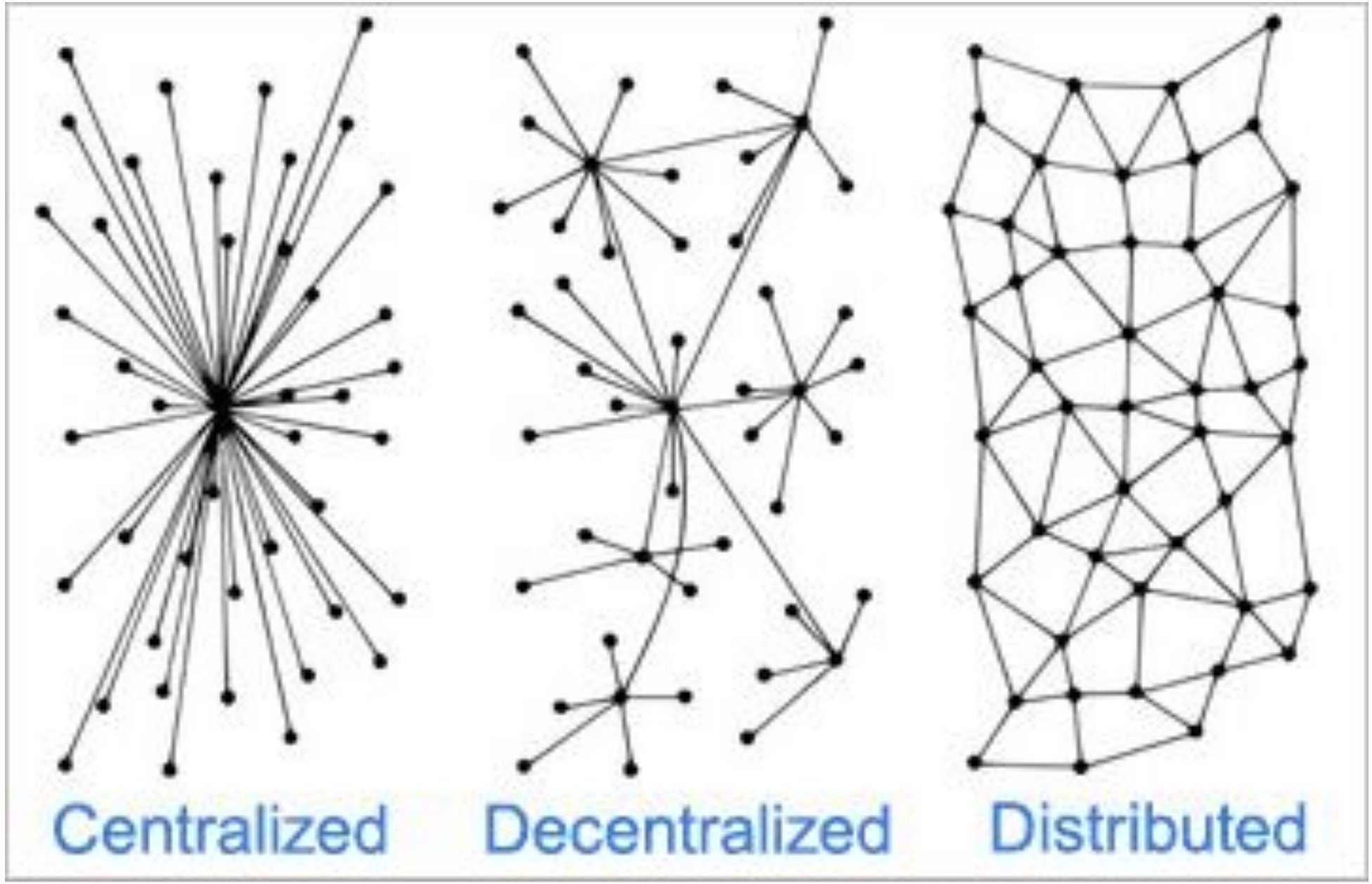
- A Decentralized computation and Information sharing platform that enables multiple authoritative domain who do not trust each other to corporate co-ordinate collaborate in a rational decision making process

A blockchain is an open financial ledger or record in which every transaction is authenticated and authorized.

A blockchain is designed as a decentralized network of millions of computers, commonly referred to as nodes.

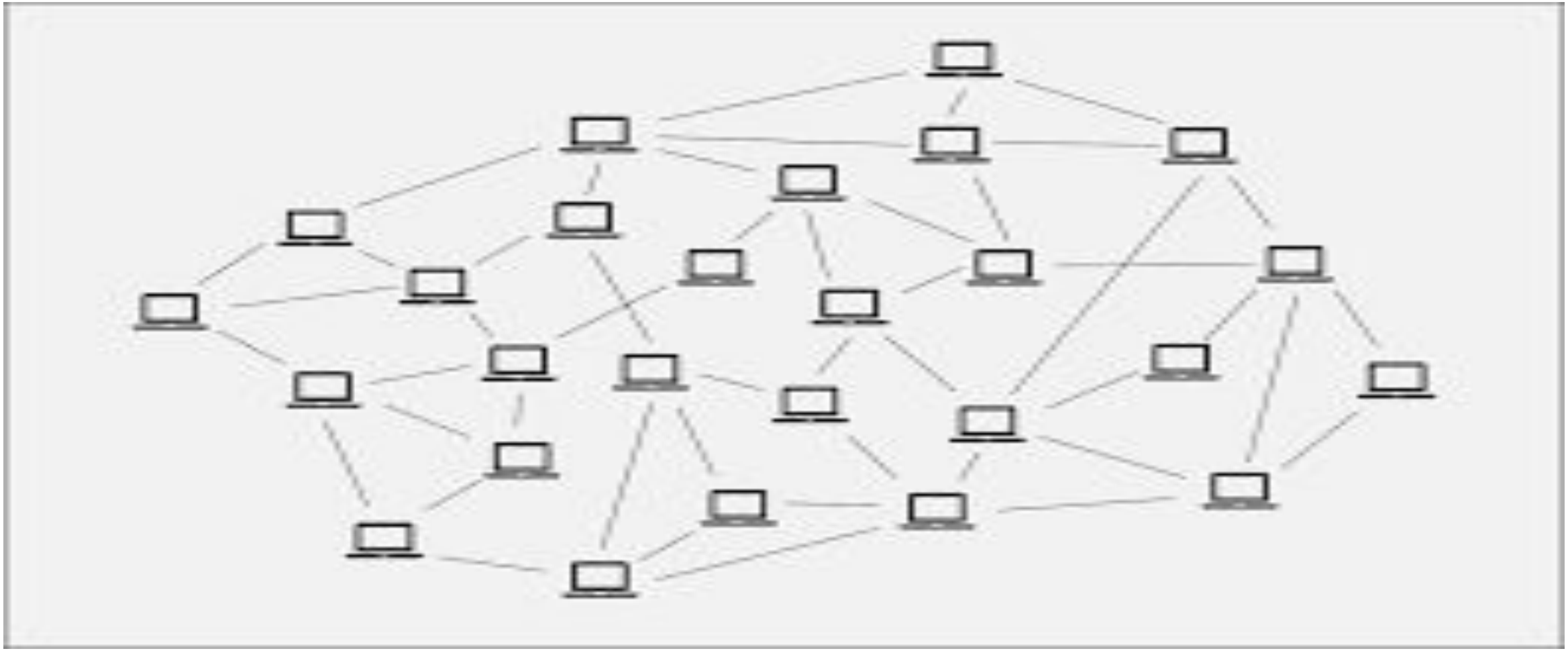
Since there's no centralized information in a blockchain architecture, a blockchain is literally impossible to hack.


INTERNET
Communication



Components of a blockchain architecture:

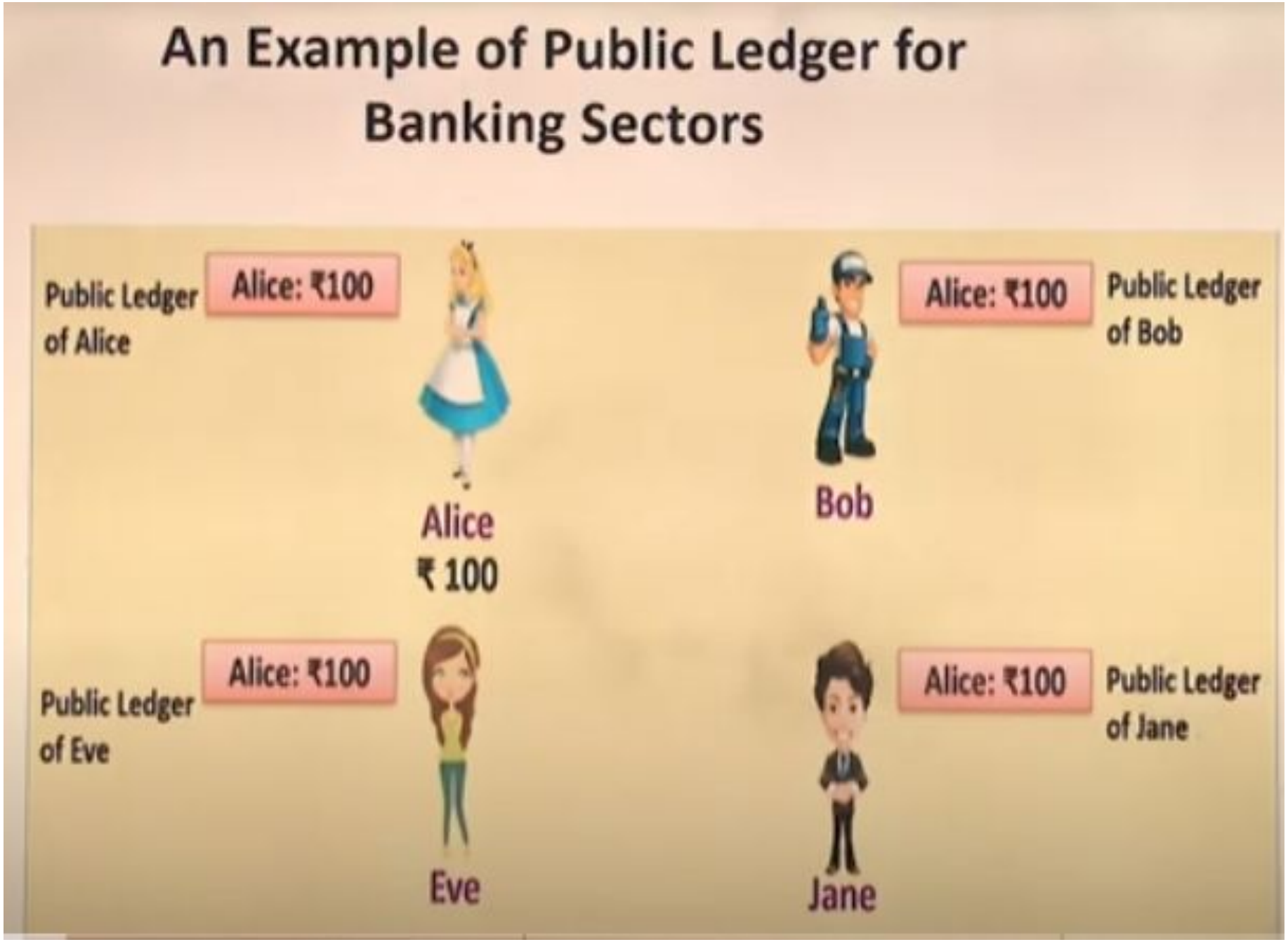
1.Node — A computer in the blockchain architecture (each node has an independent copy of the entire blockchain ledger)



2. Transaction — A data record verified by block chain participants that serves as an almost immutable confirmation of the authenticity of a financial transaction.

Block chain works like a public ledger. A Local copy of each and every transaction is being synchronized with each and every node.

An Example of Public Ledger for Banking Sectors



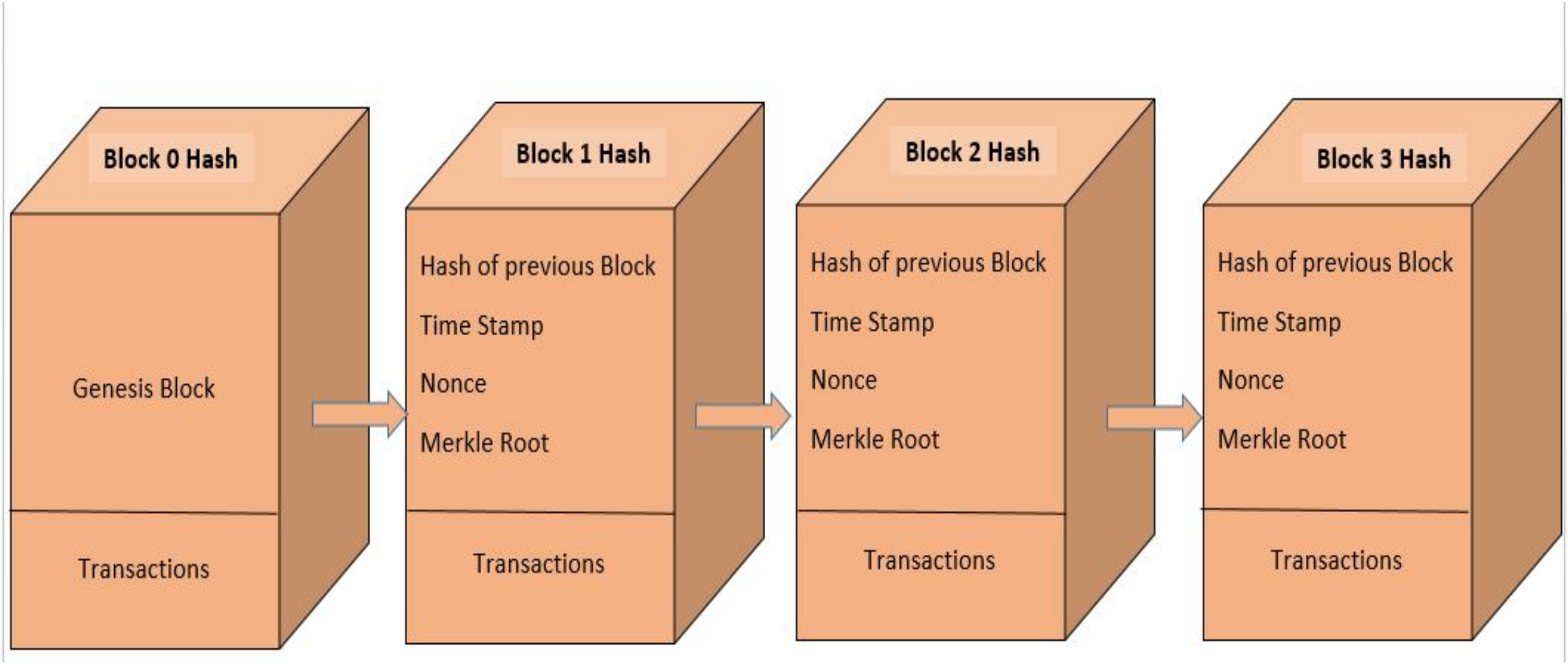
Blockchain and Public Ledger

Blockchain works like a public ledger

We need to ensure a number of different aspects

- **Protocol for commitment** Ensures that every valid transaction from the clients are committed and included in the blockchain within a finite time.
- **Consensus** Ensures that the local copies are consistent
- **Security** Data needs to be tamper-proof.
- **Privacy and authenticity** The data or transactions belong to various clients privacy and authenticity need to be ensured

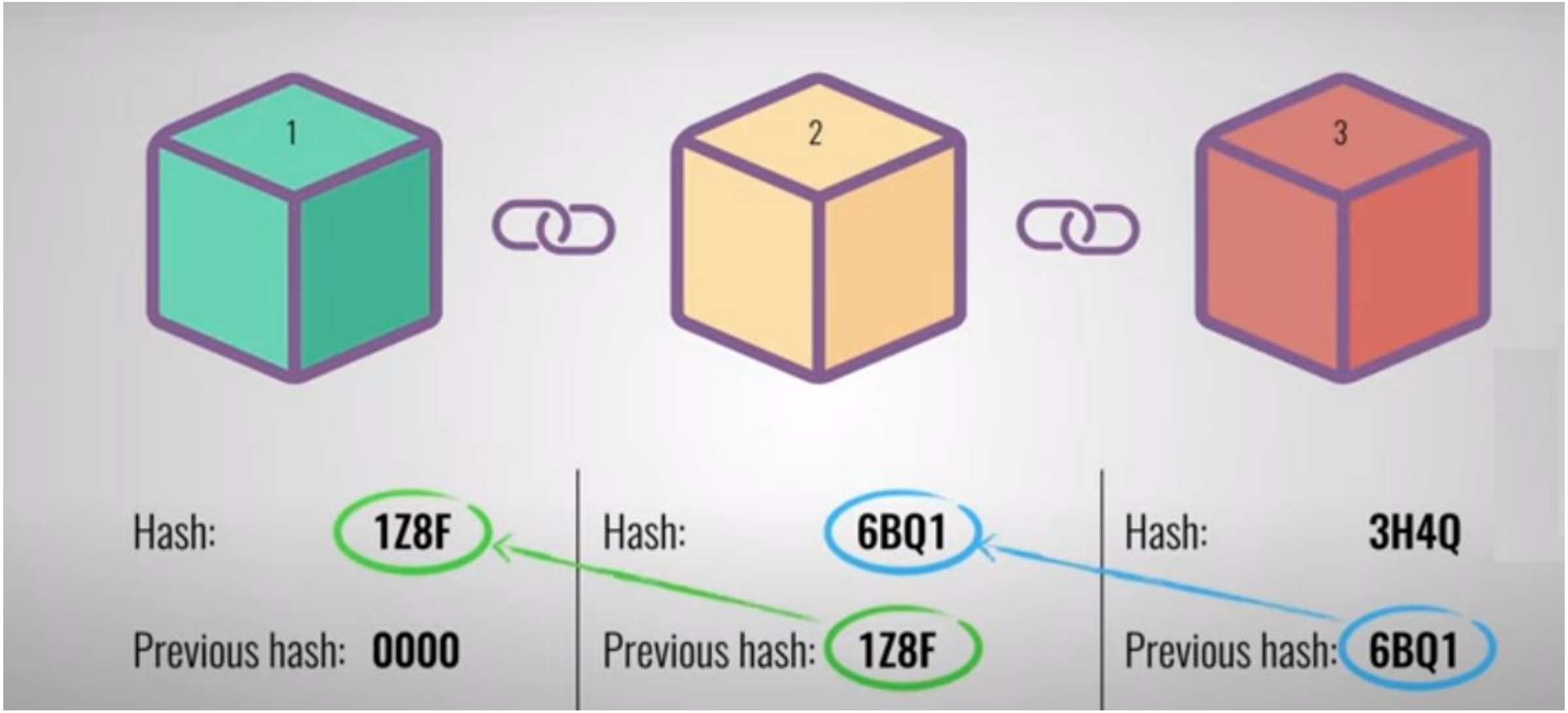
3)Block — A record or sealed data compartment that contains:

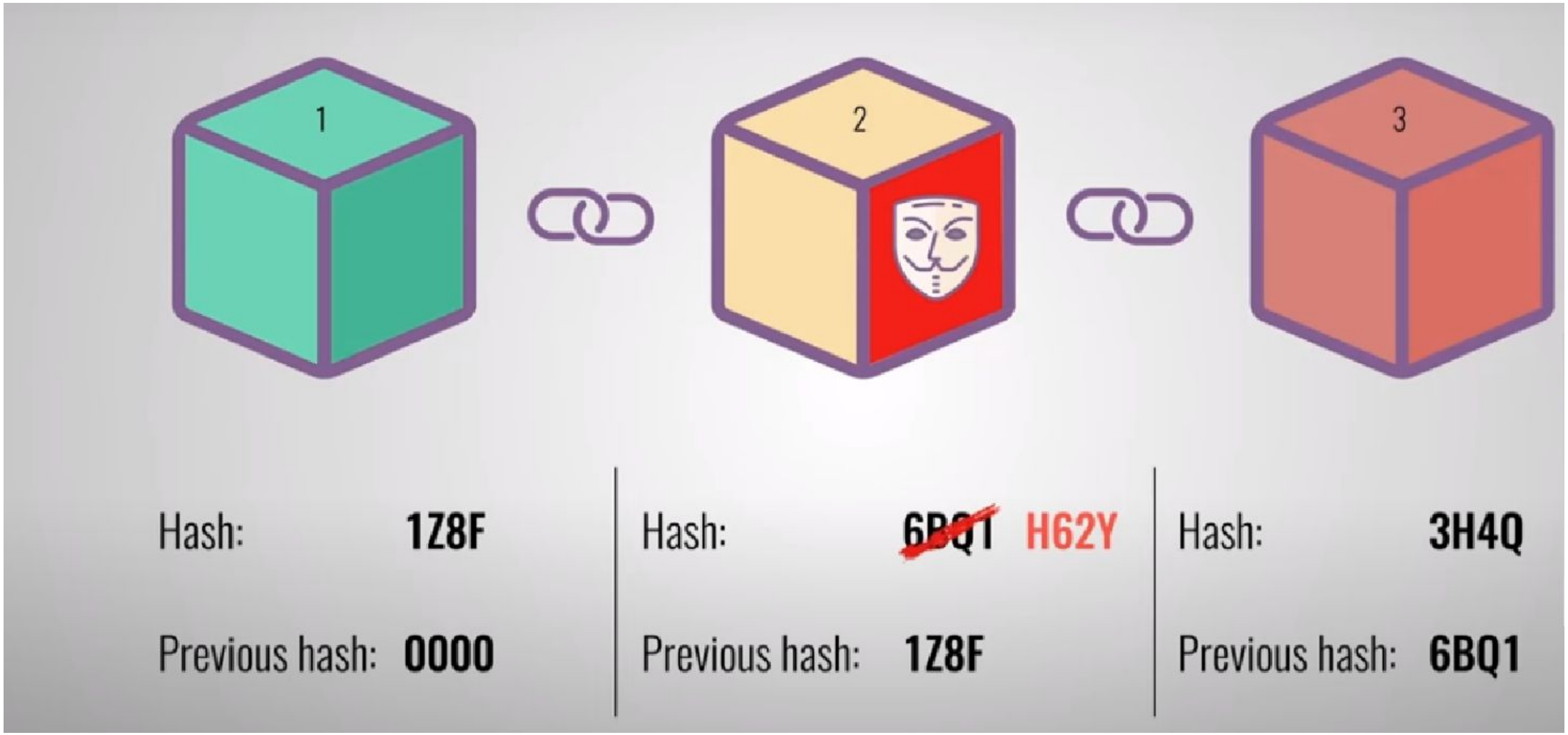


Hash of the block:-

A hash code is an alphanumeric representation of data. A block's hash is unique to that block, and it changes if any of its underlying data changes in any way.

2) Hash of the previous block:-




1
2
3
Hash: 1Z8F
Previous hash: 0000
Hash: 6BQ1 H62Y
Previous hash: 1Z8F
Hash: 3H4Q
Previous hash: 6BQ1

Genesis Block:-

Every block in a blockchain stores a reference to the previous block. In the case of Genesis Block, there is no previous block for reference.

In technical terms, it means that the Genesis Block has it's "previous hash" value set to 0. This means that no data was processed before the Genesis Block. All other blocks will have sequential numbers starting by 1, and will have a "previous hash" set to the hash of the previous block.

Time stamp:-

This timestamp tells when the block was created, so it also helps to keep the chain in chronological order.

Nonce:-

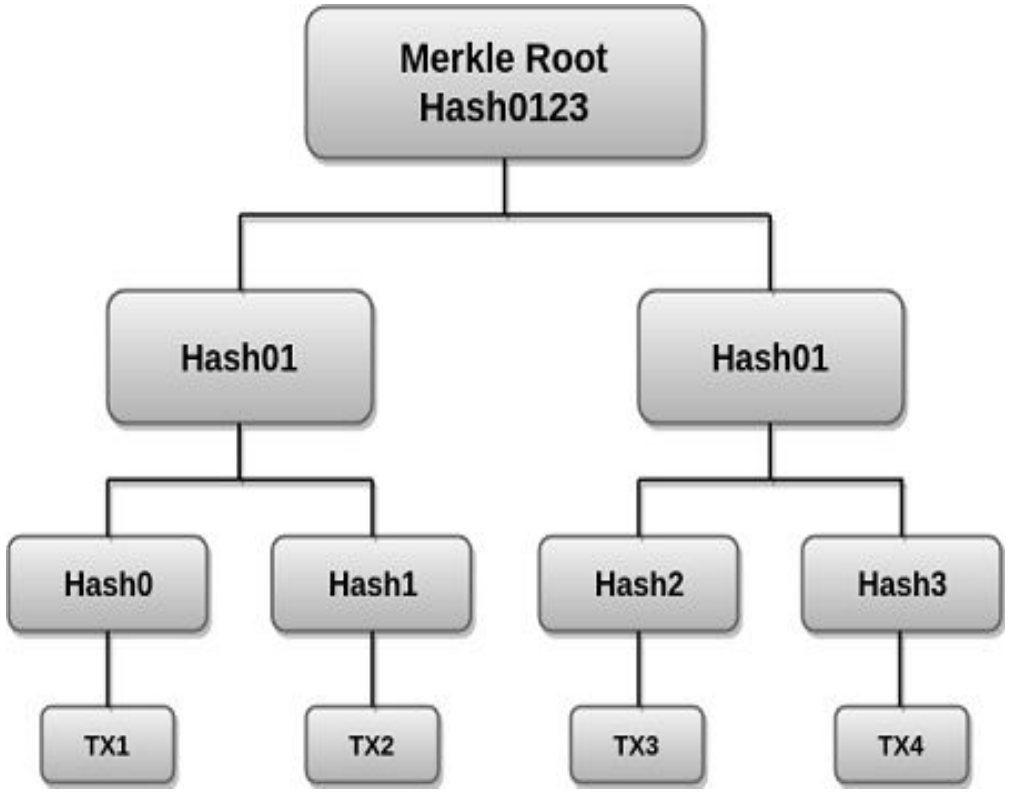
A nonce is a term derived from "number used once." a nonce is a random number generated by a miner to solve a cryptographic puzzle. The puzzle is part of the process of adding a new block to the blockchain, known as mining.

Merkle trees

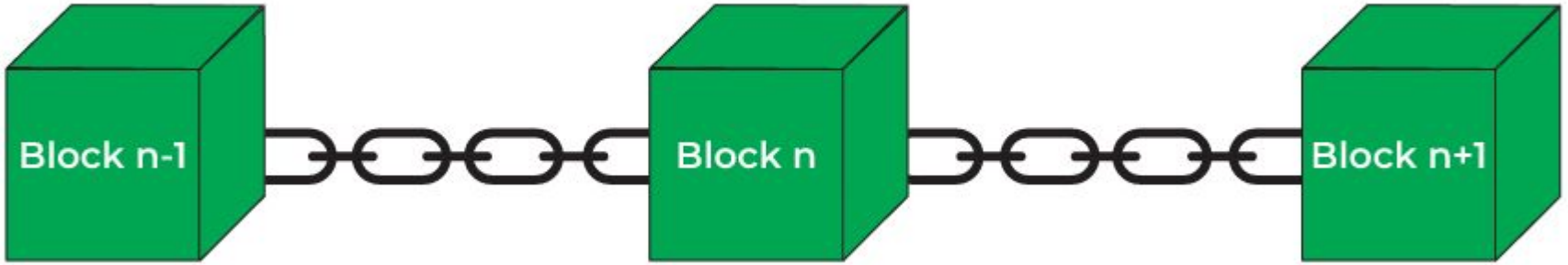
A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions.

Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. This hash is called the Merkle Root, or the Root Hash.

The Merkle Trees are constructed in a bottom-up approach.



4)Chain — A ordered sequence of blocks



5)Miners — Nodes that validate blocks before adding them to the block chain structure

6)Consensus (protocol) — A set of rules and agreements for performing blockchain operations

Step-By-Step representation of Blockchain transaction

- Joe's plan to send two Bitcoin (2 BTC) to Ann through the blockchain

Step 1 Joe request the proposed transaction Joe sent two Bitcoin from his wallet app

Step 2 The proposed transaction is broadcast to the network

Step 3 - Miners verify the transaction and bundle in it into a block along with other transactions

- The Miners will validate authenticity of the transaction i.e. status of the Joe, his balance etc

Note : Miners validate all the transactions they wish to include in the block

Step-By-Step representation of Bc transaction

Step 4 - Miners compete to solve complex mathematical puzzle

- Puzzle requires much computational power to solve
- This protects the blockchain against hackers as it would be difficult and expensive to attack the network

Step 5 The nodes verify the Miner's work

- The Miner who finds the correct hash broadcast the block to the network
- Majority of the nodes/miners need to approve or verify the block for it to be accepted into the blockchain
- Once approved the winning miner can collect the reward

Smart Contract - definition

- "A smart contract is a secure and unstoppable computer program representing an agreement that is automatically executable and enforceable"
- work on the principle that code is the law, which means that there is no need for an arbitrator or a third party to enforce, control, or influence the execution of a smart contract
- they are secure, unstoppable and executable in reasonable amount of time

Properties of smart contracts:

1)Self-executing: Smart contracts automatically execute when predetermined conditions are met. This eliminates the need for intermediaries or third parties to enforce the terms of the contract.

2)Enforceable: All contract conditions are enforced automatically.

3)Deterministic: ensure that smart contract always produce the same output for a specific input.

4)Immutable: Once deployed on a blockchain, a smart contract's code is typically immutable, meaning it cannot be altered or tampered with. This ensures the integrity and security of the contract.

5)Decentralized: Smart contracts operate on a decentralized network of nodes, which makes them resistant to tampering.

6)trustless: Smart contracts operate on a trustless system, meaning that participants can engage in transactions without needing to trust each other. The trust is placed in the code and in the blockchain.

7)Transparent: The code of a smart contract is typically open and transparent on the blockchain, allowing anyone to verify the terms and conditions of the contract. This transparency enhances accountability and trust.

https://medium.com/mobindustry/designing-a-blockchain-architecture-types-use-cases-and-challenges-9894fb7b58e

https://hacken.io/discover/blockchain-architecture-layers/

https://coincodecap.com/the-architecture-of-blockchain-technology