19ZO03
INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

19ZO03 - INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Course Objectives:

1. Understand the Block chain Technology and its application in processing Crypto Currency
2. Familiarize with Ethereum, Smart contracts, Solidity language and Hyper Ledger
3. Apply Block chain technology for real world scenarios.

Course Outcomes:

CO1: Understand the Basics of Distributed Systems, Cryptographic primitives and Blockchain

CO2: Comprehend the importance, creation and use of Bit coin and Crypto currency

CO3: Identify the use of Ethereum in Distributed Applications, Smart contracts and Decentralized autonomous organizations (DAOs)

CO4: Identify the use of Hyper Ledger in creating Smart contracts.

CO5: Apply hyperledger Fabric and Etherum platform to implement the Block chain Application

Text Books:

1) Imran Bashir,' Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks', Packt Publishing Limited 2017.

2) Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 'Bitcoin and cryptocurrency technologies: a comprehensive introduction', Princeton University Press, 2016

INTRODUCTION: Distributed System, P2P system, Hadoop Distributed File System, Distributed Hash Table, ASIC resistance, issues, Distributed Ledger Technology- Private, public and permissioned ledgers - Cryptographic primitives- public key cryptography- Digital Signature Algorithm -Hashing- Blockchain evolution- Structure of blockchain – Life of Blockchain application - consensus – Byzantine General problem and Fault Tolerance (11)

BLOCKCHAIN 1.0 - BITCOIN AND CRYPTOCURRENCY :

Block Hash - structure of block – syntax , structures, and validation - transaction life cycle- transaction types – Hash computation and Merkle Hash Tree -Bit coin and importance- Creation of coins–Bitcoin P2P Network-, Bitcoin protocols - Mining strategy and rewards – PoW and PoS – Difficulty, hash rate– Wallets- Double spending – forking- Token, Coinbase - practice on MTH (12)

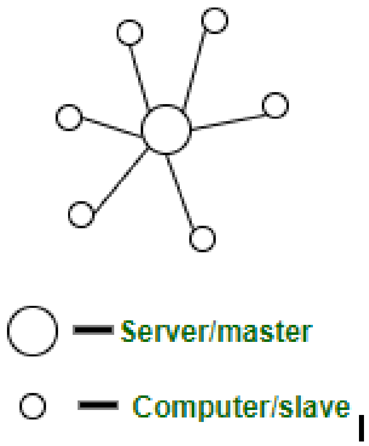
BLOCKCHAIN 2.0 - ETHEREUM : Distributed applications (Dapps), Smart contracts, Ethereum Virtual Machines, Ethereum high level design, Ethereum addresses, Ethereum accounts, Transactions, Currency, Gas, Tokens, Decentralized autonomous organizations(DAOs), Bitcoin vs Ethereum – Trie- Solidity programming – writing smart contracts – remix IDE – TestNet- sample exercises - issues in solidity programming (12)

BLOCKCHAIN 3.0 – HYPERLEDGER: Fabric- Architecture, Identities and Policies, Membership and Access Control, Channels, Transaction Validation, Writing smart contract using Hyperledger Fabric. (5)

APPLICATIONS : Know Your Customer (KYC), Food Security, Mortgage over Block chain, Block chain enabled Trade , Cross border payments (5)

Centralized

Centralized systems are systems that use client/server architecture where one or more client nodes are directly connected to a central server.



Characteristics of Centralized System

✓Presence of a global clock:

✓One single central unit

✓Dependent failure of components

Limitations of Centralized System

✓Can’t scale up vertically after a certain limit

✓Denial of Service

Distributed System

- A Distributed system is a collection of independent computers , interconnected via a network, capable of collaborating on a task.
- A Distributed system can be characterized as a collection of multiple autonomous computers that communicate over a communication network and have following features:
  - ❖No Common physical clock
  - ❖Enhanced reliability
  - ❖Increased performance and cost ratio
  - ❖Access to geographically remote data and resources
  - ❖Scalability

Overview – Distributed Systems

- Distributed systems connect autonomous processors by communication network.
- The software component that run on each of the computers use the local operating system and network protocol stack.
- It achieve a common goal.

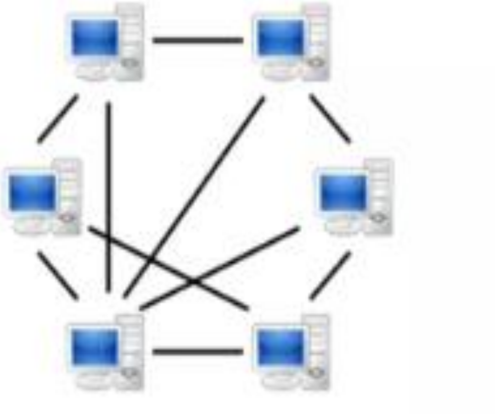
Example: Google's search engine is based on a large distributed system, but to a user, it looks like a single, coherent platform.

Motivation for Distributed system

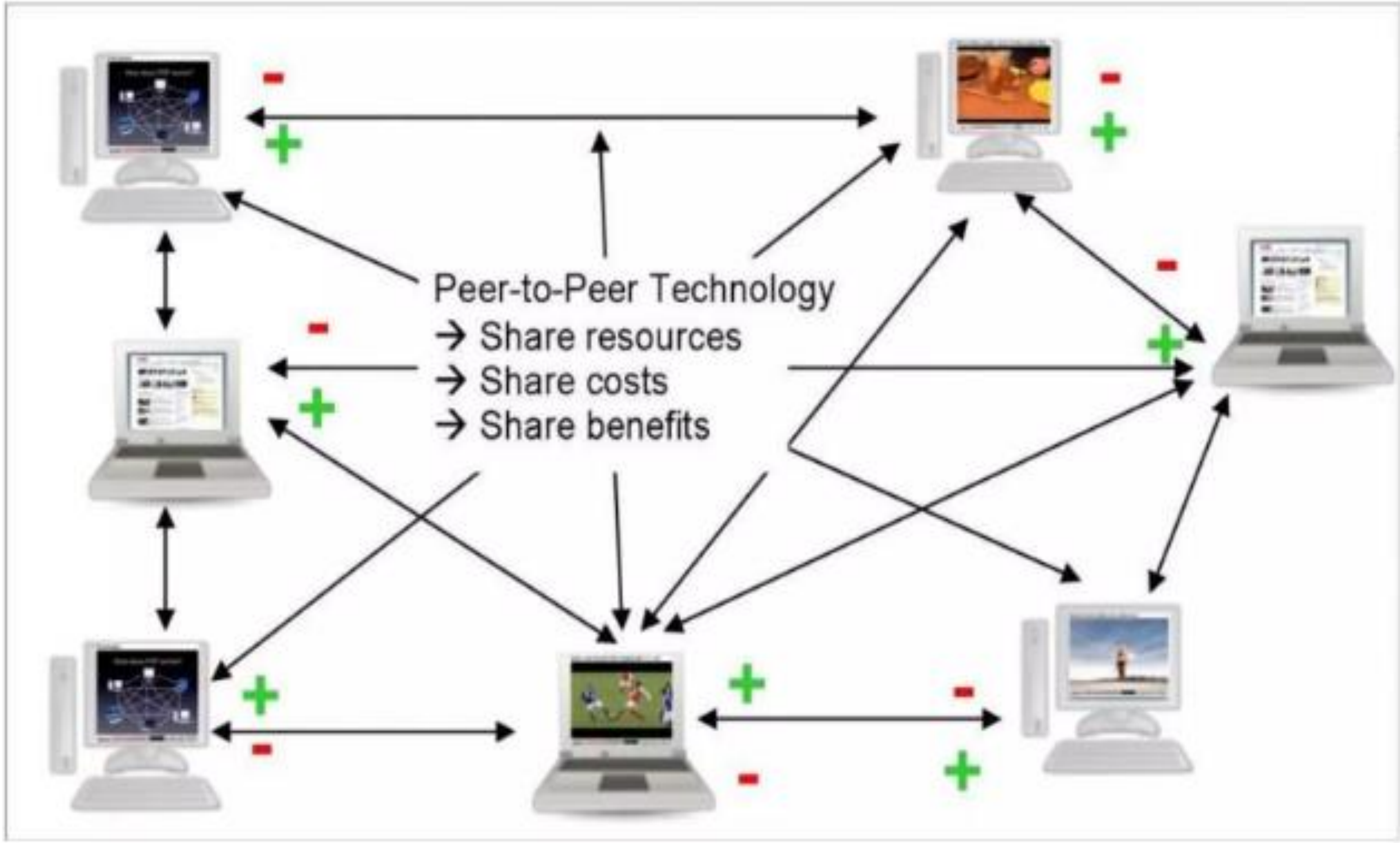
- **Inherently distributed computation** that is many applications such as money transfer in the banking, or reaching a consensus among the parties that are geographically distant, the computation is inherently distributed.
- **Resource sharing** the sharing of the resources such as peripherals, and a complete data set and so on and so forth.
- **Access the geographically remote data and resources**, such as bank database, supercomputer and so on.
- **Reliability** enhanced reliability possibility of replicating the resources and execution to enhance the reliability.

Peer-to-Peer Networking

A Peer to Peer network has no dedicated Servers. Here in Peer to Peer network, a number of workstations (or clients) are connected together for the purpose of sharing devices, information or data. All the workstations are considered as equal. Any one computer can act as client or server at any instance. This network is ideal for small networks where there is no need for dedicated servers, like home networks, small business networks, or retail shops. The Microsoft term for Peer to Peer network is Workgroup.



P2P Networking Example



Peer-to-Peer Technology
→ Share resources
→ Share costs
→ Share benefits

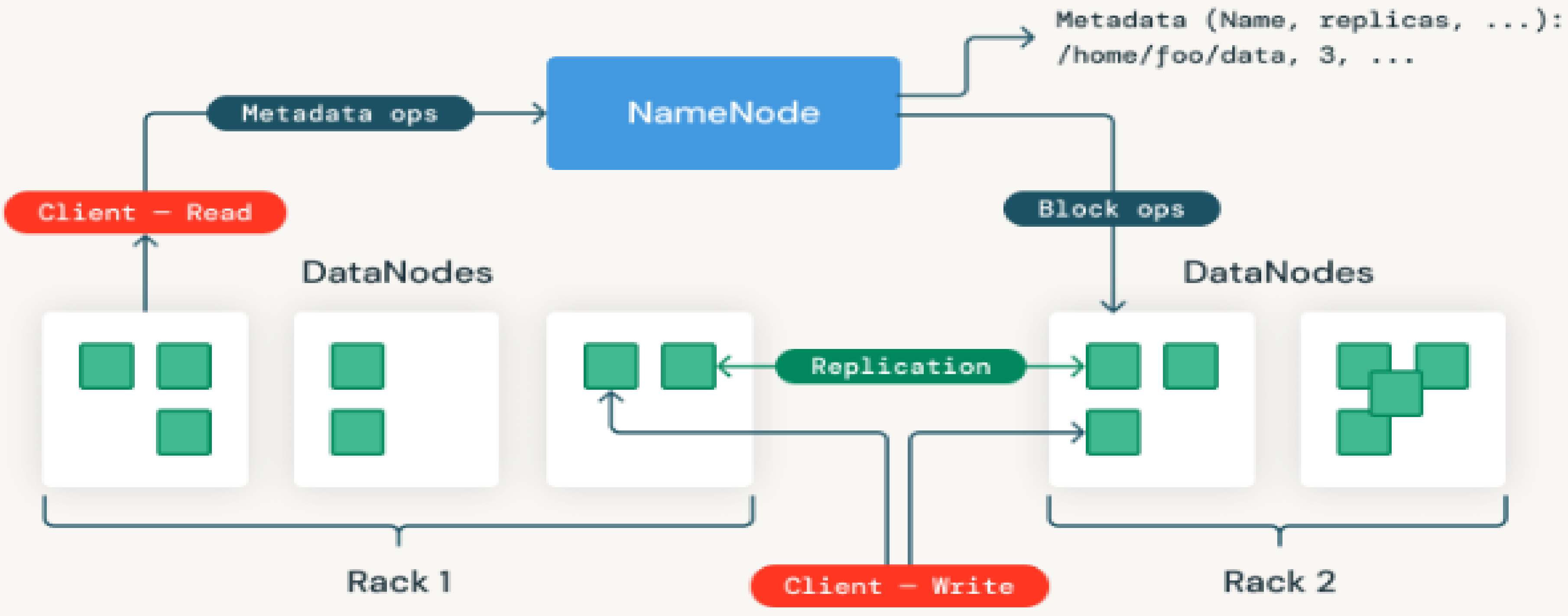
Hadoop Distributed File System

- **HDFS (Hadoop Distributed File System)** is a unique design that provides storage for *extremely large files* with streaming data access pattern, and it runs on *commodity hardware*. Let's elaborate on the terms:
- ***Extremely large files***: Here, we are talking about the data in a range of petabytes (1000 TB).
- ***Streaming Data Access Pattern***: HDFS is designed on principle of *write-once and read-many-times*. Once data is written large portions of dataset can be processed any number times.
- ***Commodity hardware:*** Hardware that is inexpensive and easily available in the market. This is one of the features that especially distinguishes HDFS from other file systems.

Hadoop Distributed File System

- **Nodes:** Master-slave nodes typically form the **HDFS cluster.**
- **Name Node (Master Node):**
  - Manages all the slave nodes and assigns work to them.
  - It executes file system namespace operations like opening, closing, and renaming files and directories.
  - It should be deployed on reliable hardware that has a high configuration. not on commodity hardware.
- **Data Node(Slave Node):**
  - Actual worker nodes do the actual work like reading, writing, processing, etc.
  - They also perform creation, deletion, and replication upon instruction from the master.
  - They can be deployed on commodity hardware.

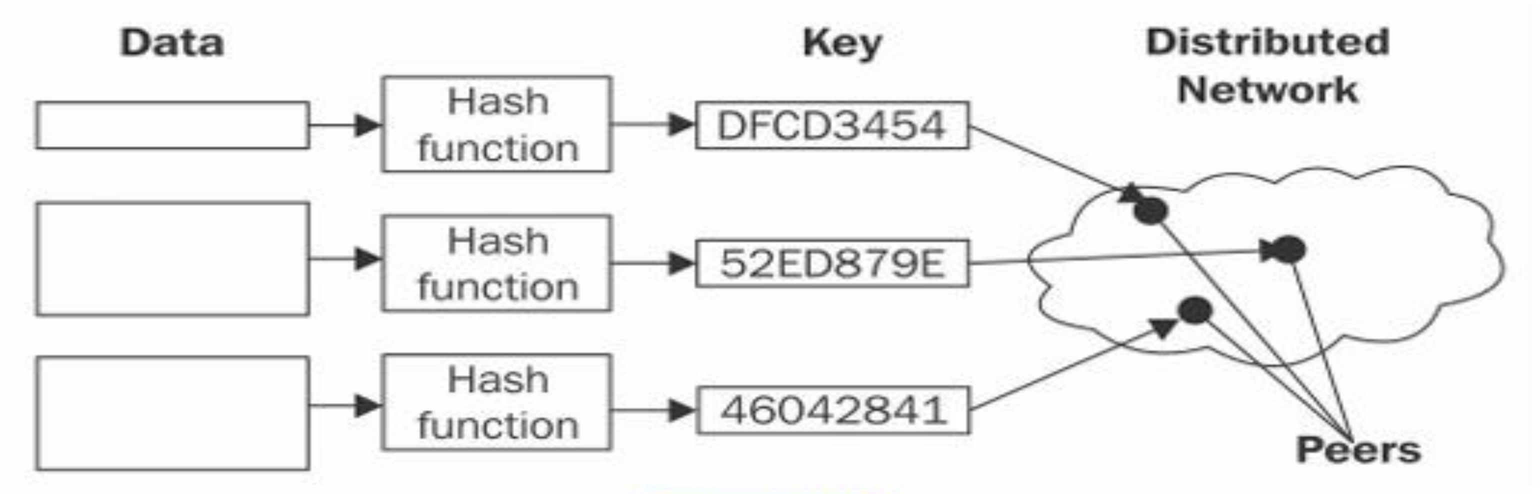
HDFS Architecture



Distributed Hash Table

- A hash table is a data structure that is used to map keys to values.
- Internally, a hash function is used to calculate an index into an array of buckets from which the required value can be found.
- Buckets have records stored in them using a hash key and are organized into a particular order.
- DHT as a data structure where data is spread across various nodes, and nodes are equivalent to buckets in a peer-to-peer network.

Distributed Hash Table



Distributed hash tables

- Data is passed through a hash function, which then generates a compact key.

- This key is then linked with the data (values) on the peer-to-peer network.

- When users on the network request the data (via the filename), the filename can be hashed again to produce the same key, and any node on the network can then be requested to find the corresponding data.
  DHT provides decentralization, fault tolerance, and scalability

ASIC

- ASICs are specialized hardware designed for a specific mining task and offer a significant advantage over general-purpose hardware like CPUs and GPUs.

ASIC resistance:

- ASIC resistance in blockchain refers to the design of a cryptocurrency's mining algorithm and protocol to prevent or significantly hinder the use of Application-Specific Integrated Circuits (ASICs) for mining.
- ASIC resistance aims to promote decentralization by allowing a wider range of participants to mine using readily available hardware.

What are ASICs?

- ASICs are custom-designed integrated circuits optimized for a specific task, in this case, mining a particular crypto currency.

- They can perform hashing operations much faster and more efficiently than general-purpose hardware, giving them a competitive edge in mining.

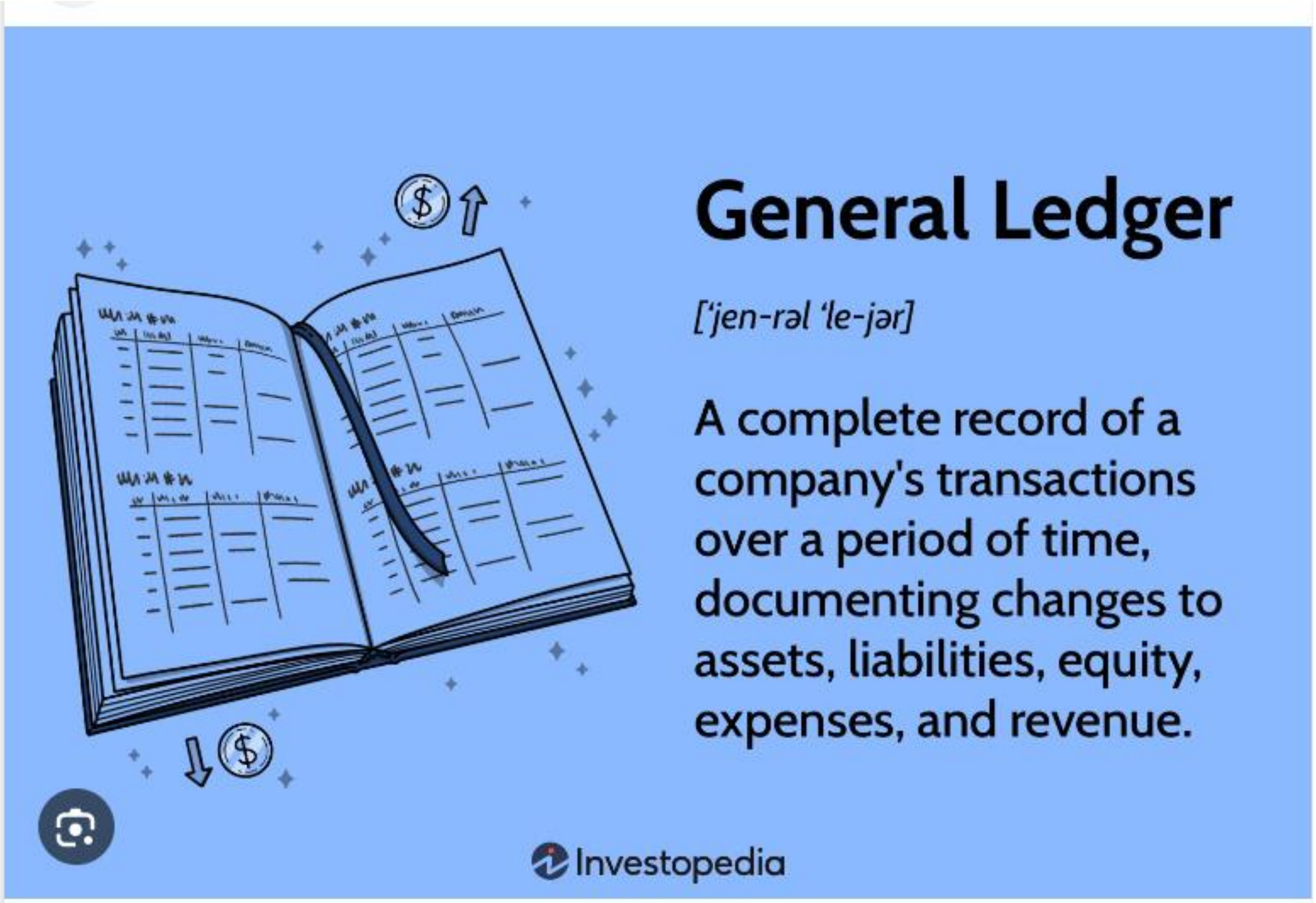
How is ASIC Resistance Achieved?

- **Memory-Hard Algorithms:**
Some algorithms are designed to require significant amounts of memory to perform calculations, making it difficult and expensive to build ASICs that can efficiently handle them.
- **Algorithm Variability:**
Changing the mining algorithm frequently can make it challenging for ASIC manufacturers to keep up with the latest specifications.
- **Focus on General-Purpose Hardware:**
Some algorithms are specifically designed to be more efficient on CPUs or GPUs, making ASICs less advantageous.

Examples of ASIC-Resistant Cryptocurrencies:

- **Monero:** Uses the RandomX algorithm, optimized for CPUs, making it difficult for ASICs to compete.
- **Grin and Ravencoin:** Also known for using ASIC-resistant algorithms.

Ledger



General Ledger

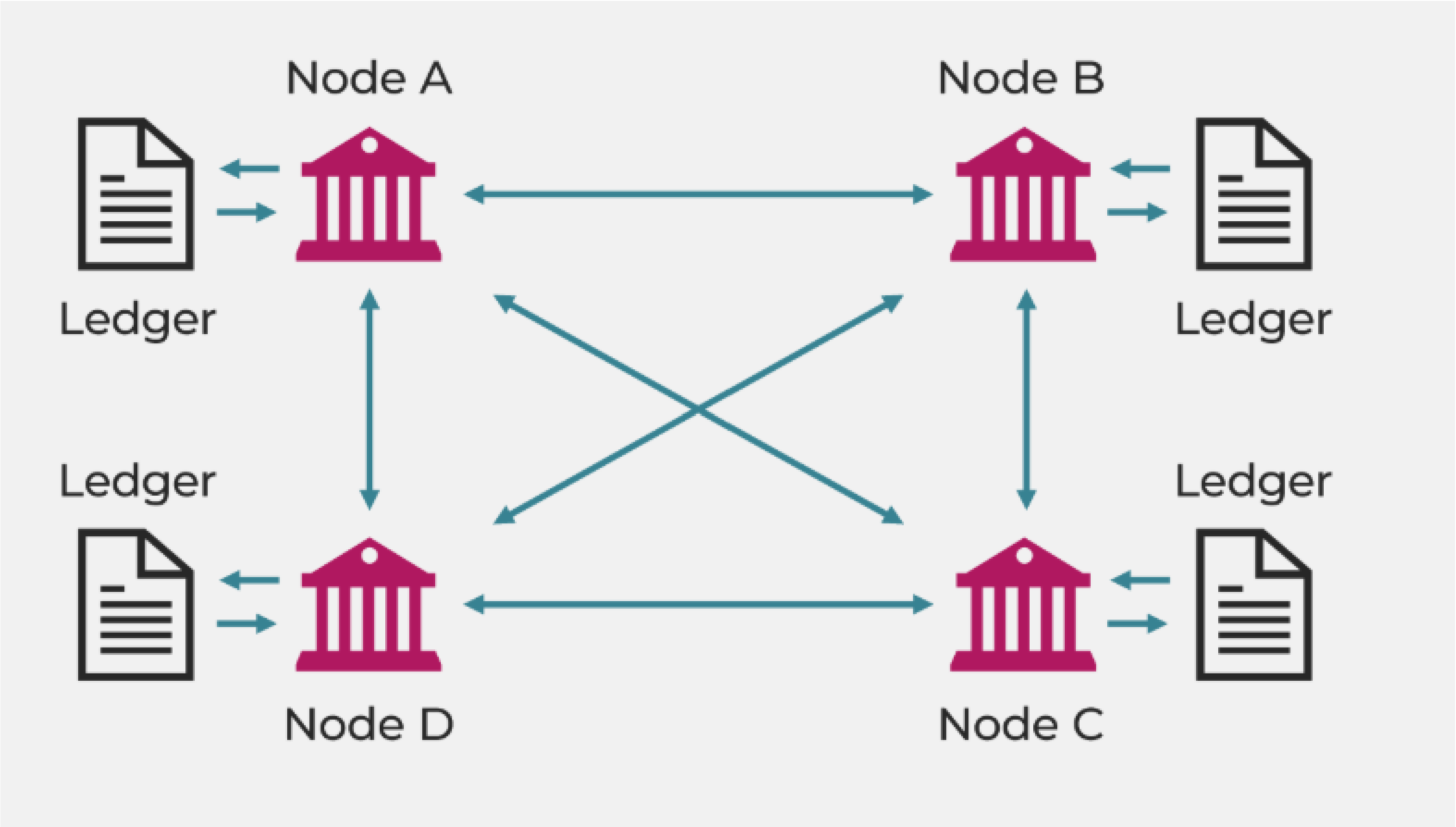
[‘jen-rəl ‘le-jər]

A complete record of a company's transactions over a period of time, documenting changes to assets, liabilities, equity, expenses, and revenue.

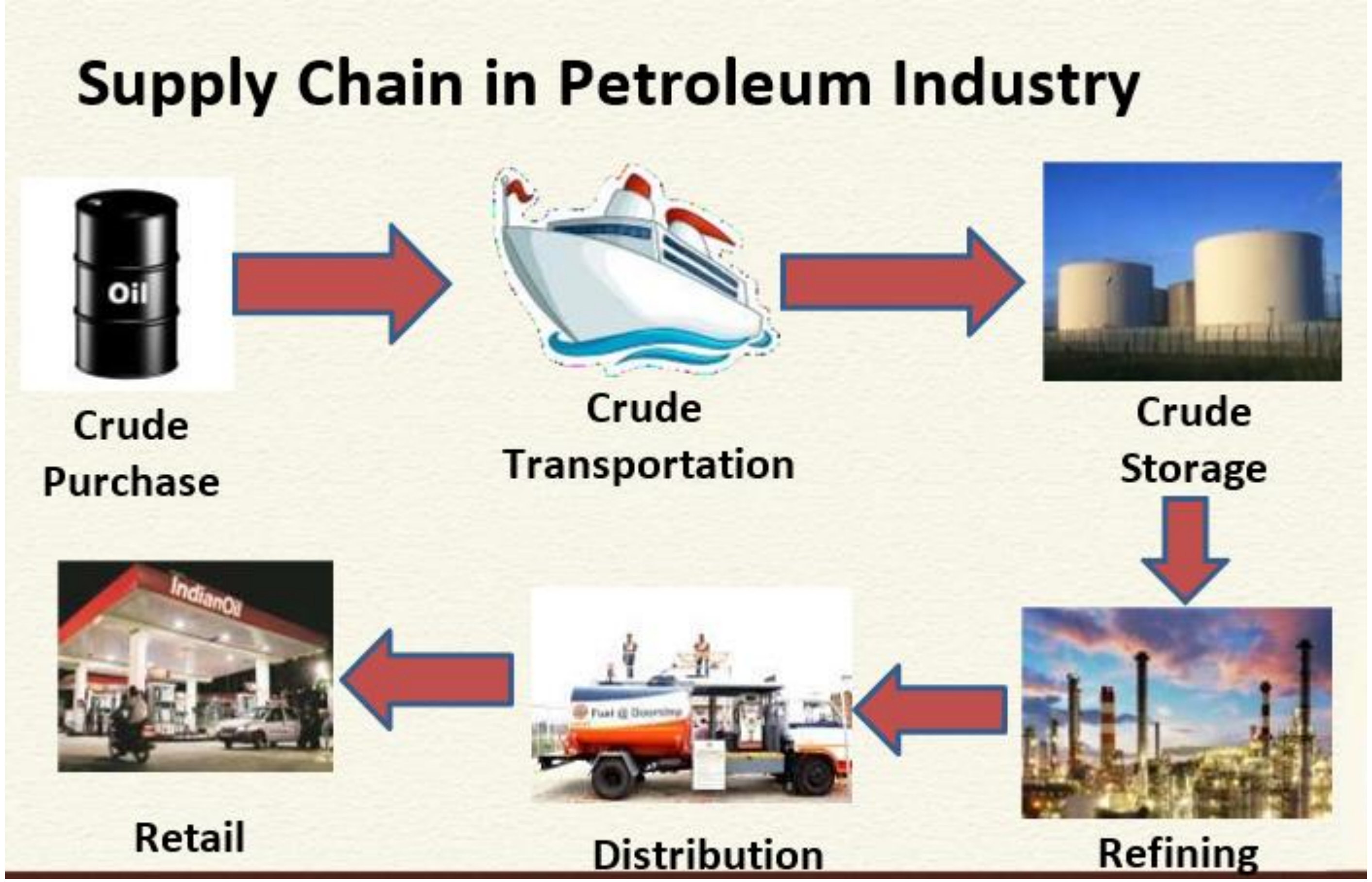
Distributed ledger

- Blockchain is a distributed ledger, which simply means that a ledger is spread across the network among all peers in the network, and each peer holds a copy of the complete ledger.
- A distributed ledger is distributed among its participants and spread across multiple sites or organizations. This type of ledger can be either private or public. The fundamental idea here is that, unlike many other blockchains, the records are stored contiguously instead of being sorted into blocks.
- All blockchains are fundamentally distributed ledgers, all distributed ledgers are not necessarily a blockchain.

Distributed ledger



USE CASE – How Blockchain works?



Supply Chain in Petroleum Industry

Requirements for a Successful Supply Chain

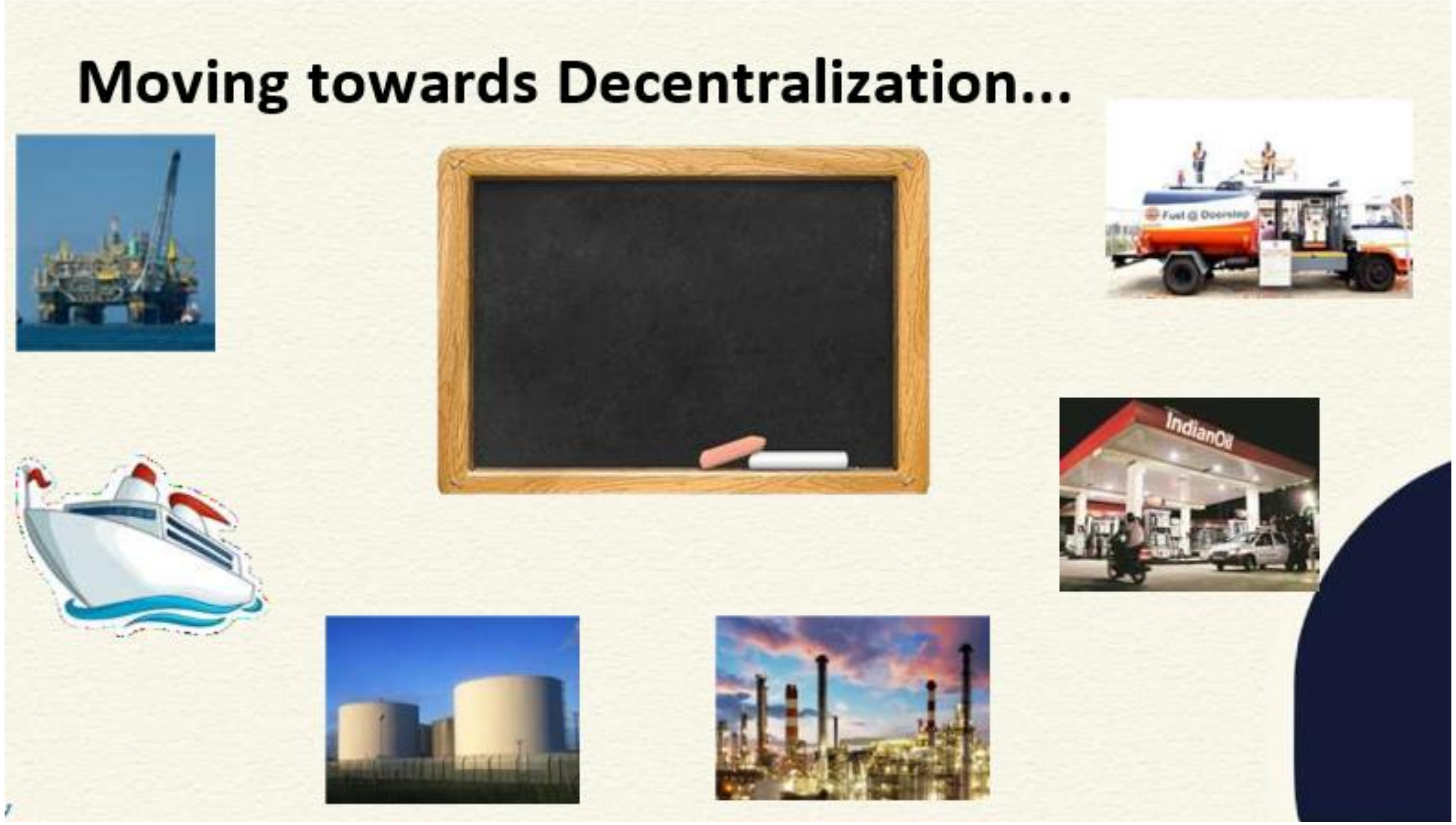
- Minimization of material procurement
- Maximization of manufacturing capacity and sales
- Meet demand numbers
- Respond quickly to market opportunity by purchasing the production shortfall from other players
- Objective of each production unit would be to maximize the throughput and its margin
- Procurement would purchase the feedstock with not the best yields at lowest cost

- **What is the guarantee that the information submitted is correct?**
- **What if someone denies the information later on?**

Here Blockchain is the answer!!!

Decentralization and Blockchain

- You have a network of different players (businesses, enterprises, commercial establishments, Government or Private bodies, or even the individuals)
- Everyone has their own interest they want to fulfil their goal
- They do not trust each other
- If they cooperate, the society gets benefited
- **Trustless Decentralization = Blockchain**



Moving towards Decentralization…

Moving towards Decentralization...

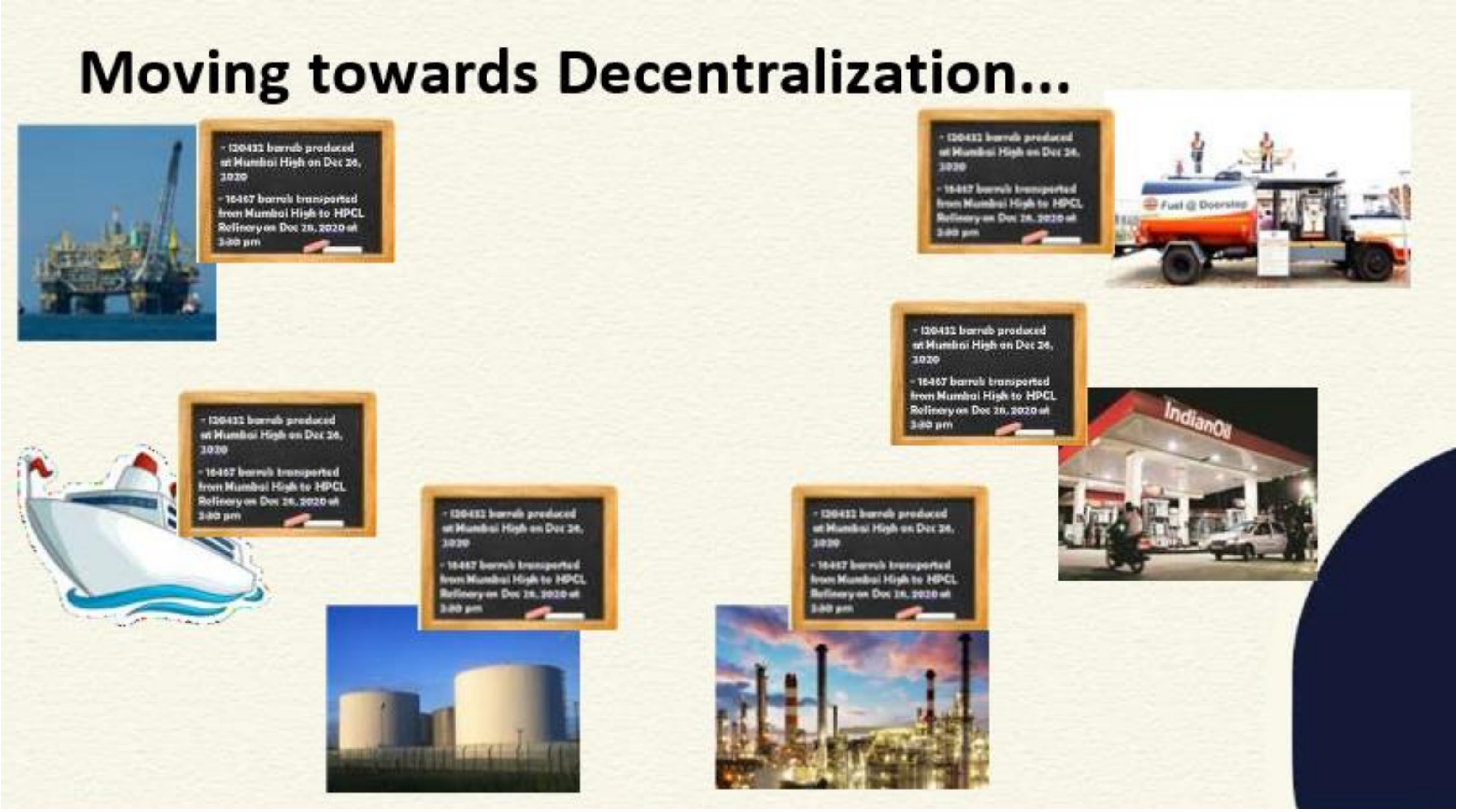
- 120432barrels produced at Mumbai High on Dec 26, 2020

- 16467barrels transported from Mumbai High to HPCL Refineryon Dec 26,2020at 2:30 pm

- The Board has infinite space, you do not need to erase anything
- Everyone can see all the logs and verify
- Any change in information is visible to everyone
- The board is not erasable and no one can deny later.

- Who will maintain this board?
- Buy Cloud from Amazon?
- Who will provide the cost?
- If one of the industry maintains it, how to check **that it is not a fraud?**

Let everyone maintain the same copy of the board Individually and Independently



Moving towards Decentralization...

- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm
Fuel @ Doorstep
IndianOil

- No one is the sole owner of the data, but everyone has the copy of the data. There is no central database.
- Everyone holds exactly the same copy of the data at the same instance of the time.
- An immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later.
- There is no central database to store the chain – everyone keeps a copy of the chain and process data locally.
- New information is added to the chain in the form of new blocks
- Blockchain ensures that every party has the same view of the blockchain always

Moving towards Decentralization...

- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm

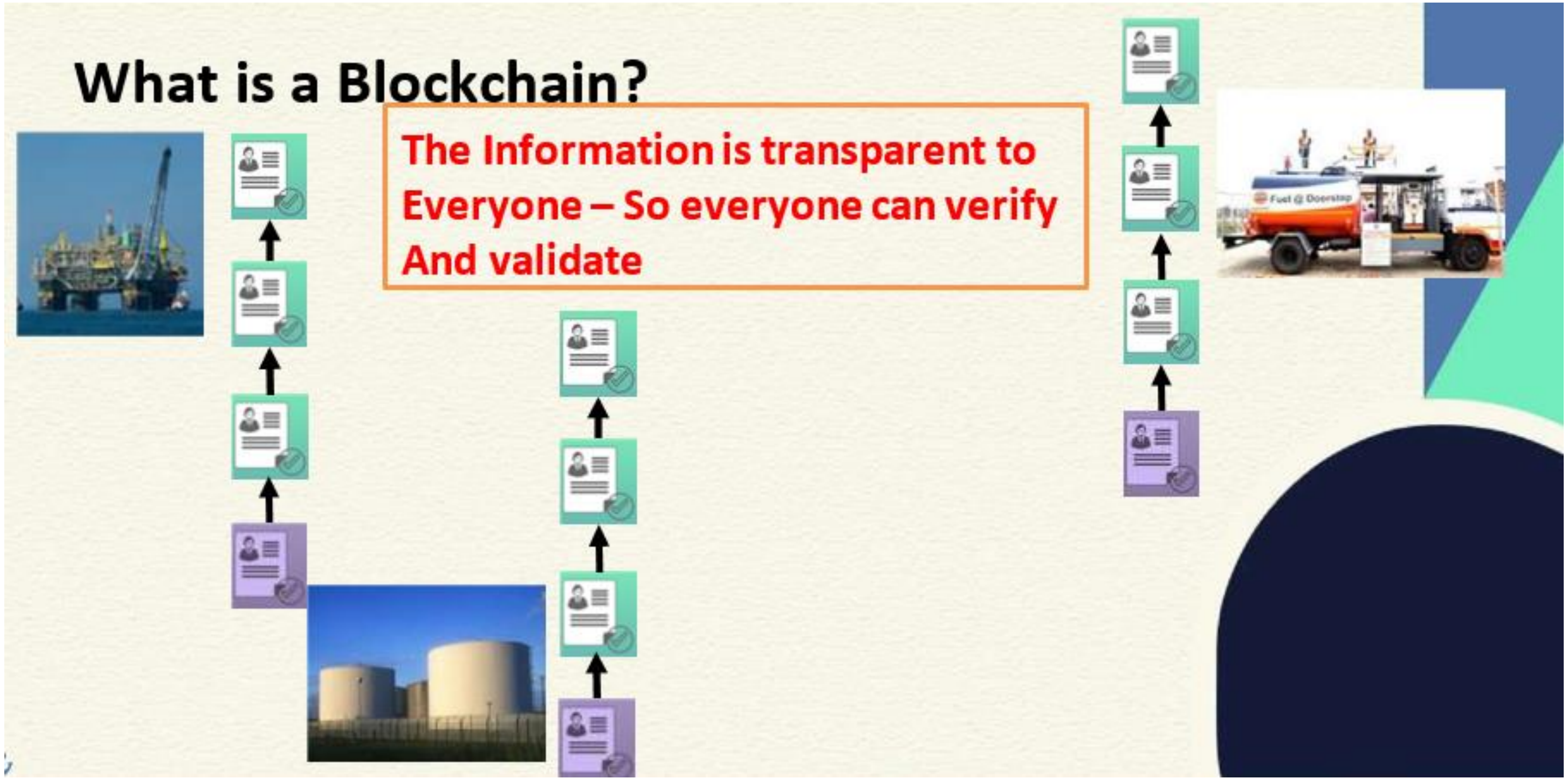
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm

- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm

- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm

- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm

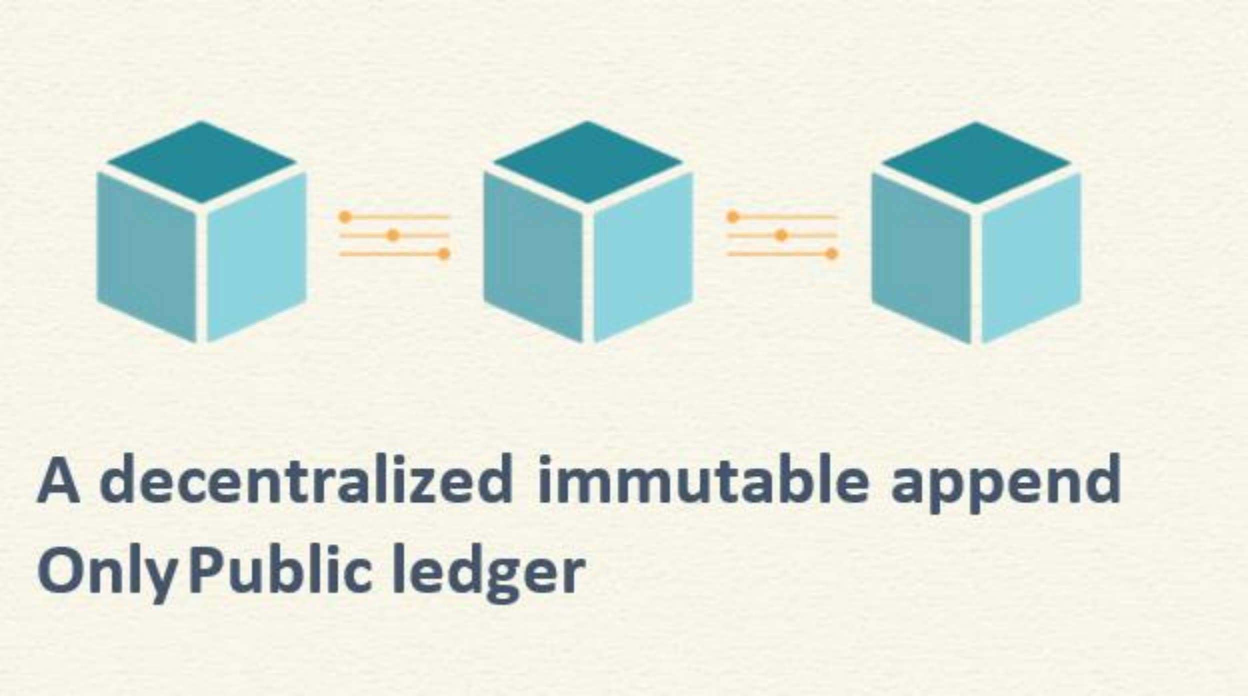
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 3:00 pm



What is a Blockchain?

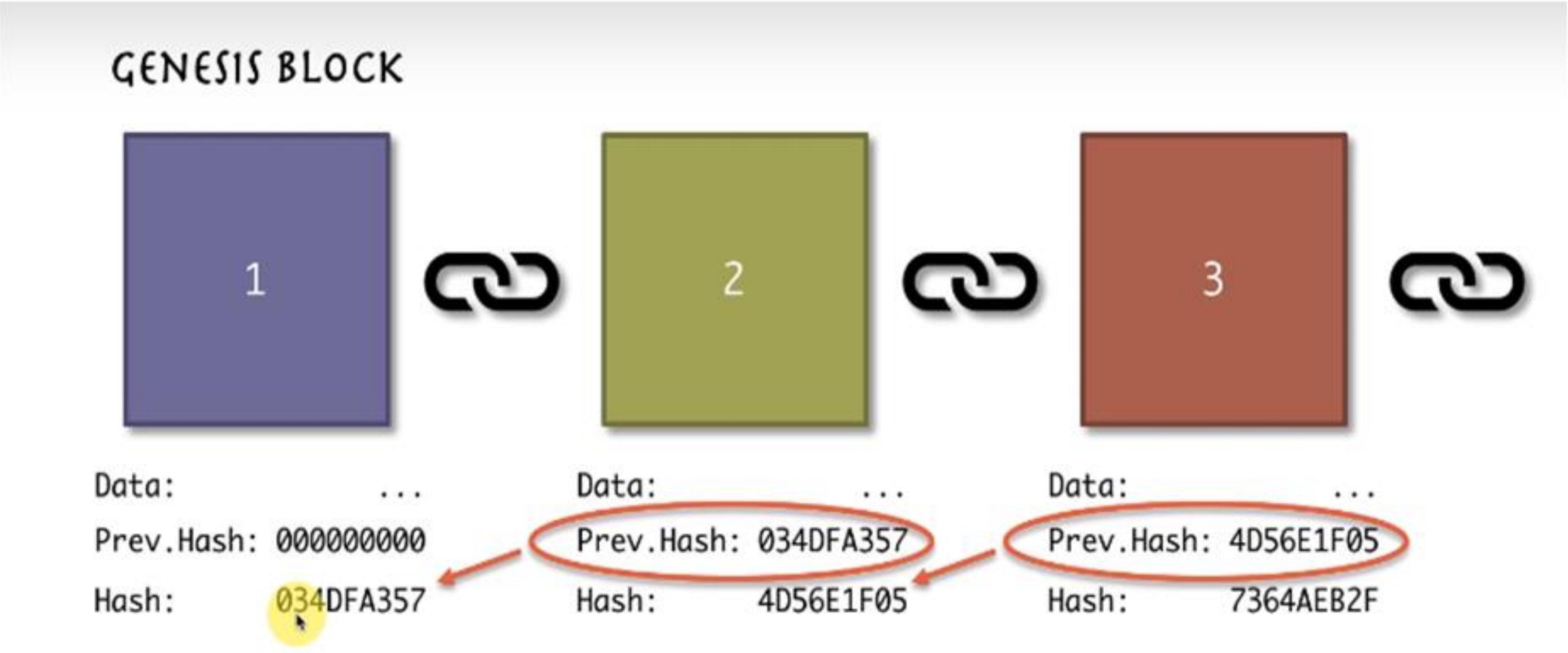
The Information is transparent to Everyone – So everyone can verify And validate

Blockchain



A decentralized immutable append OnlyPublic ledger

BLOCKCHAIN



Data: ...
Prev.Hash: 000000000
Hash: 034DFA357

Data: ...
Prev.Hash: 034DFA357
Hash: 4D56E1F05

Data: ...
Prev.Hash: 4D56E1F05
Hash: 7364AEB2F

WHATIS BLOCKCHAIN?

Stuart Haber

W. Scott Stornetta

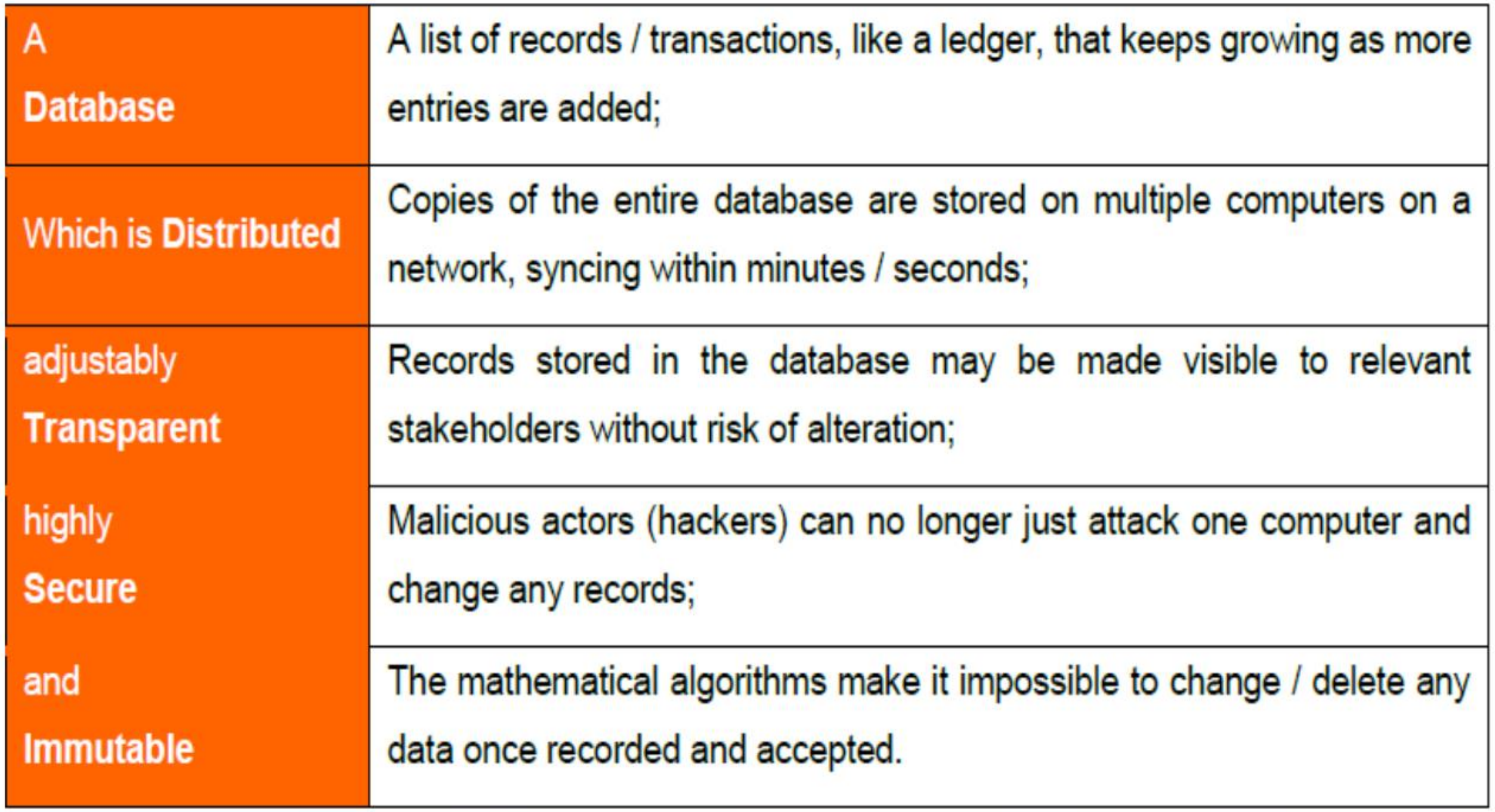
A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

– *Wikipedia*

Blockchain?

- Blockchain at its core is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

Blockchain?



A **Database**	A list of records / transactions, like a ledger, that keeps growing as more entries are added;
Which is **Distributed**	Copies of the entire database are stored on multiple computers on a network, syncing within minutes / seconds;
adjustably **Transparent**	Records stored in the database may be made visible to relevant stakeholders without risk of alteration;
highly **Secure**	Malicious actors (hackers) can no longer just attack one computer and change any records;
and **Immutable**	The mathematical algorithms make it impossible to change / delete any data once recorded and accepted.

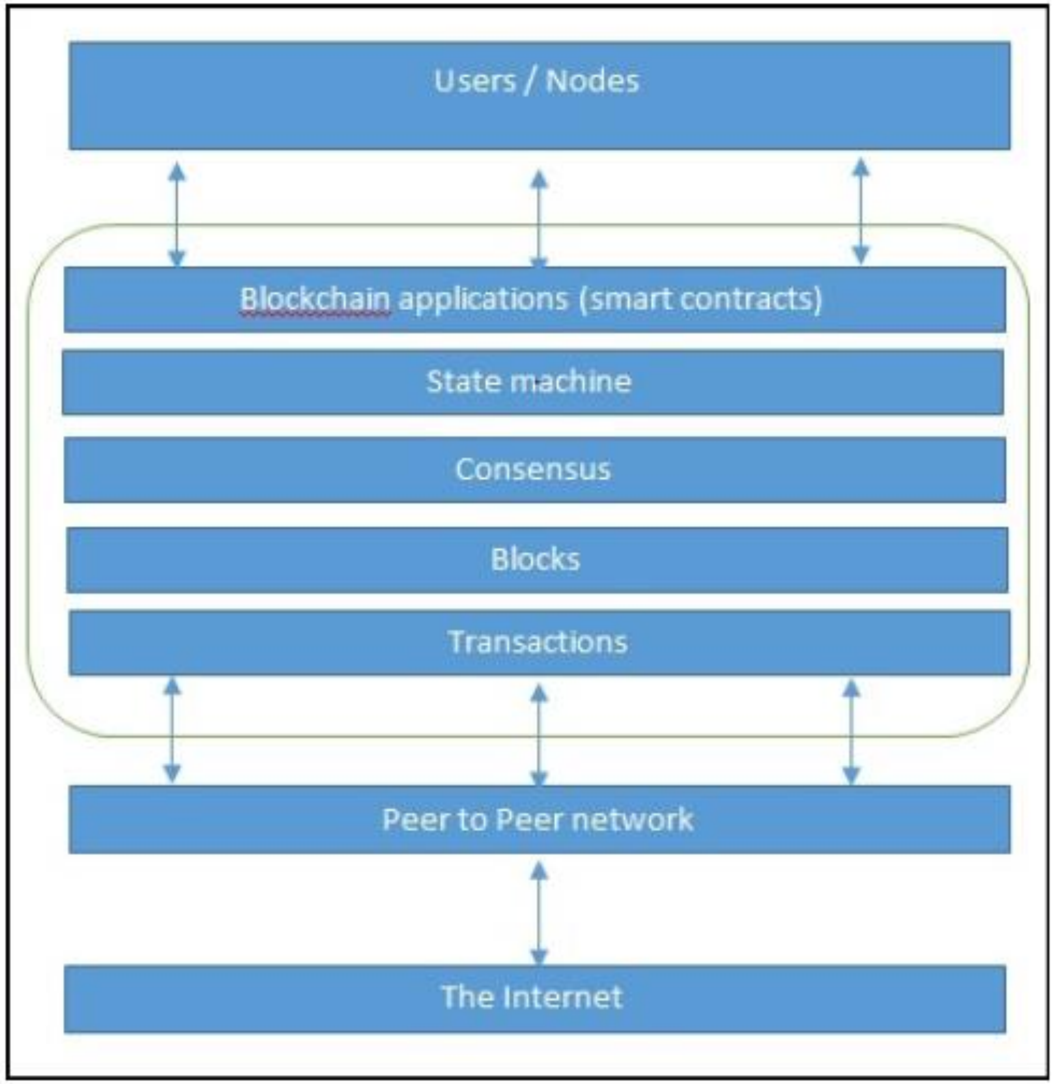
- Value
- Trust
- Truth
- Secure

The network view of a blockchain

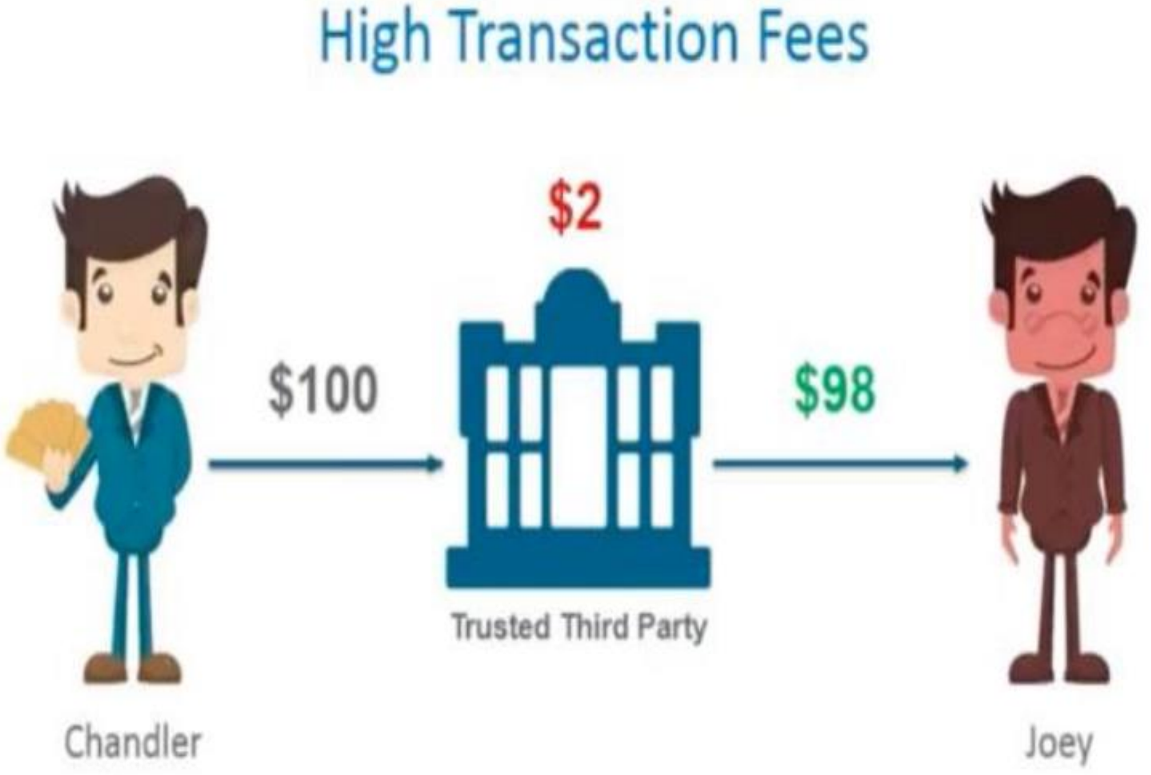
✓Blockchain can be thought of as a layer of a distributed peer-to-peer network running on top of the Internet.

✓It is analogous to SMTP, HTTP, or FTP running on top of TCP/IP.

✓From a business point of view a blockchain can be Defined as a platform where by peers can exchange values using transactions without the need for a central trusted arbitrator.



Why Blockchain?

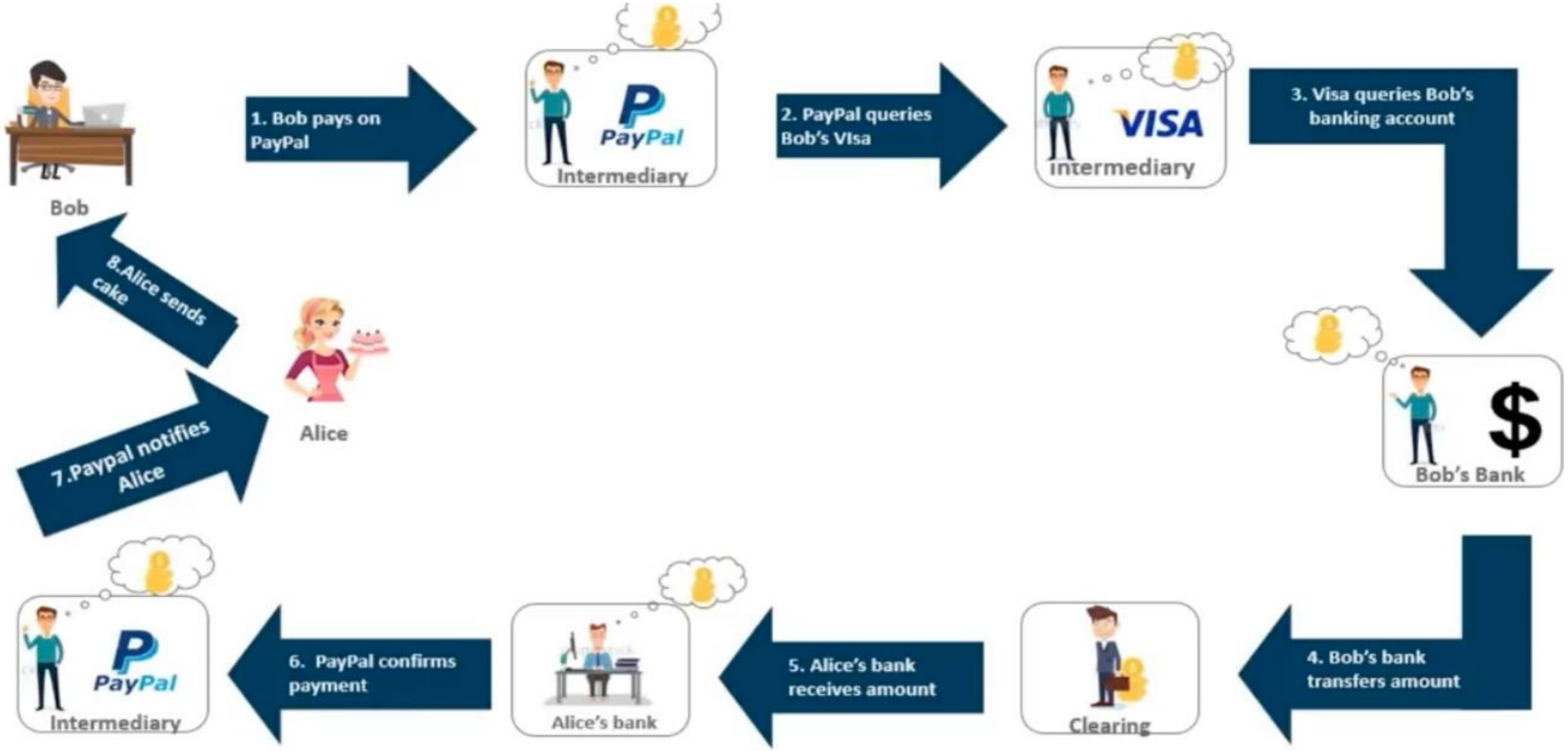


Traditional Transaction

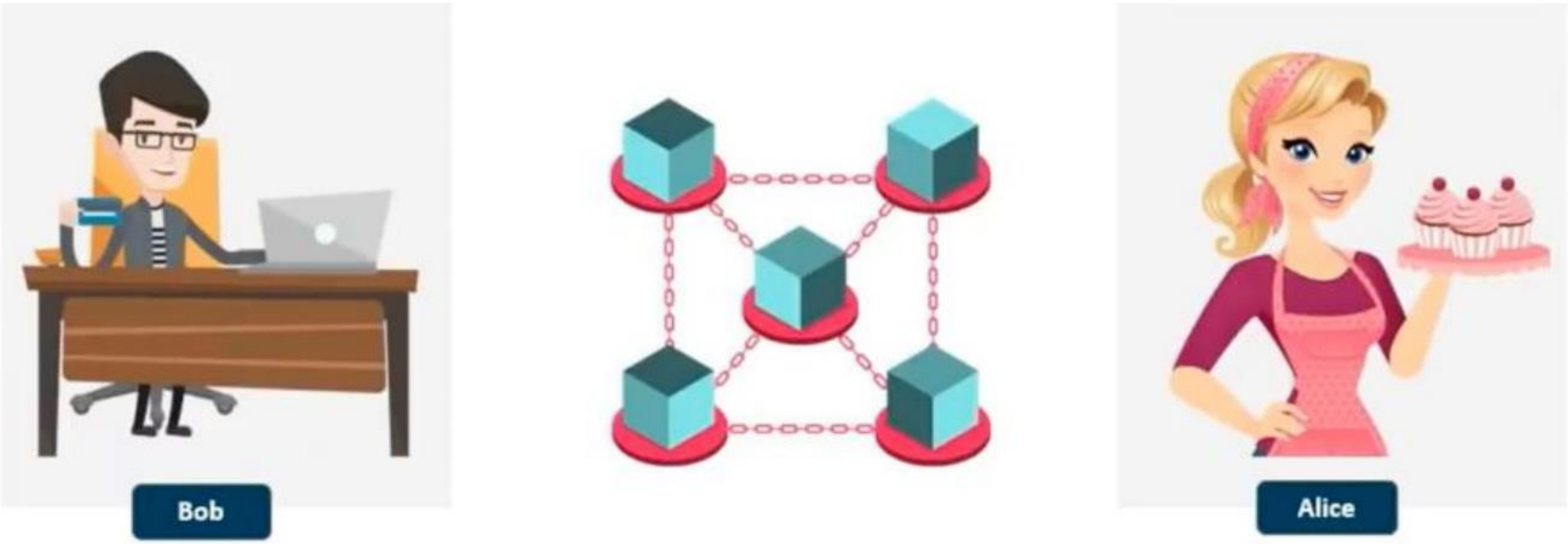
Bob wants to buy a cake from Alice's bakery. He needs to pay Alice in advance

Alice will send the goods to Bob once she has received the money…or a proper proof that she will receive it

Traditional Transaction flow

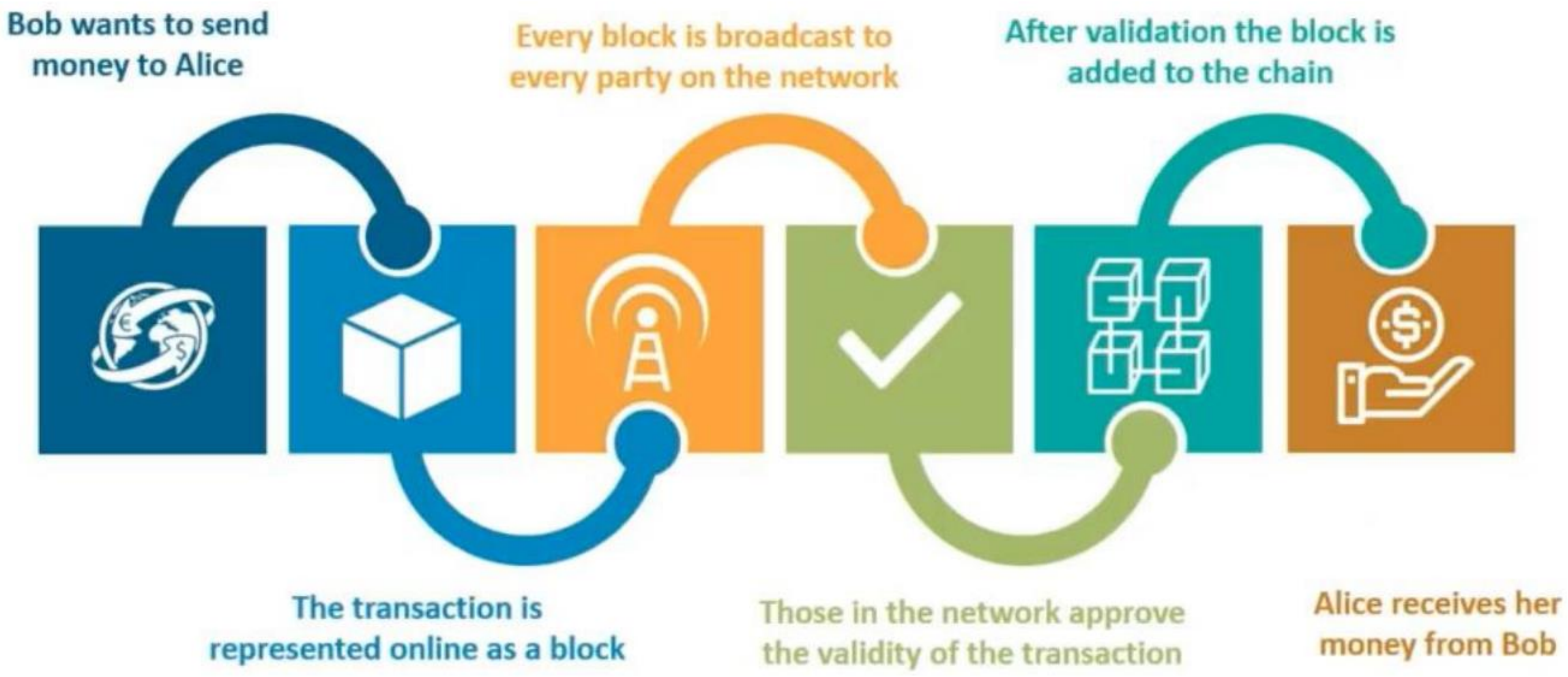


How Blockchain works??



Bob want's to send money to Alice over a blockchain network!

Blockchain Transaction flow!!!


Bob wants to send money to Alice
The transaction is represented online as a block
Every block is broadcast to every party on the network
Those in the network approve the validity of the transaction
After validation the block is added to the chain
Alice receives her money from Bob

Types of blockchain

- **Public Blockchains**
- **Private Blockchains**
- **Semi-private Blockchains**
- **Permissioned ledger**
- **Fully private and proprietary Blockchains**
- **Tokenized blockchains**
- **Tokenless blockchains**

Public blockchains

- As the name suggests, open to the public and **anyone can participate** as a node in the decision-making process.
- Users may or may not be rewarded for their participation.
- These ledgers are **not owned by anyone** and are publicly open for anyone to participate in.
- All users of the **permission-less ledger** maintain a copy of the ledger on their local nodes and use a **distributed consensus** mechanism in order to reach a decision about the eventual state of the ledger.

- **Private blockchains :** is controlled by a single organization that permits only verified members to join its network.
- **Semi-private blockchains/consortium:** combines public and private blockchain characteristics Here part of the **blockchain is private** and **part of it is public**.
  - ✓The private part is controlled by a corporation or group of enterprises. whereas the **public part** is open for **participation by anyone**.
  - ✓A consortium blockchain's primary goal is to promote organizational collaboration to address industry-specific challenges.

Permissioned ledger

- A permissioned ledger is a blockchain whereby the **participants of the network are known** and already trusted.
- Permissioned ledgers do not need to use a **distributed consensus mechanism**, instead an ***agreement protocol*** *can be used to maintain a shared* version of truth about the state of the records on the blockchain.
- There is also no requirement for a permissioned blockchain to be private as it can be a public blockchain but with regulated access control.

Distributed ledger

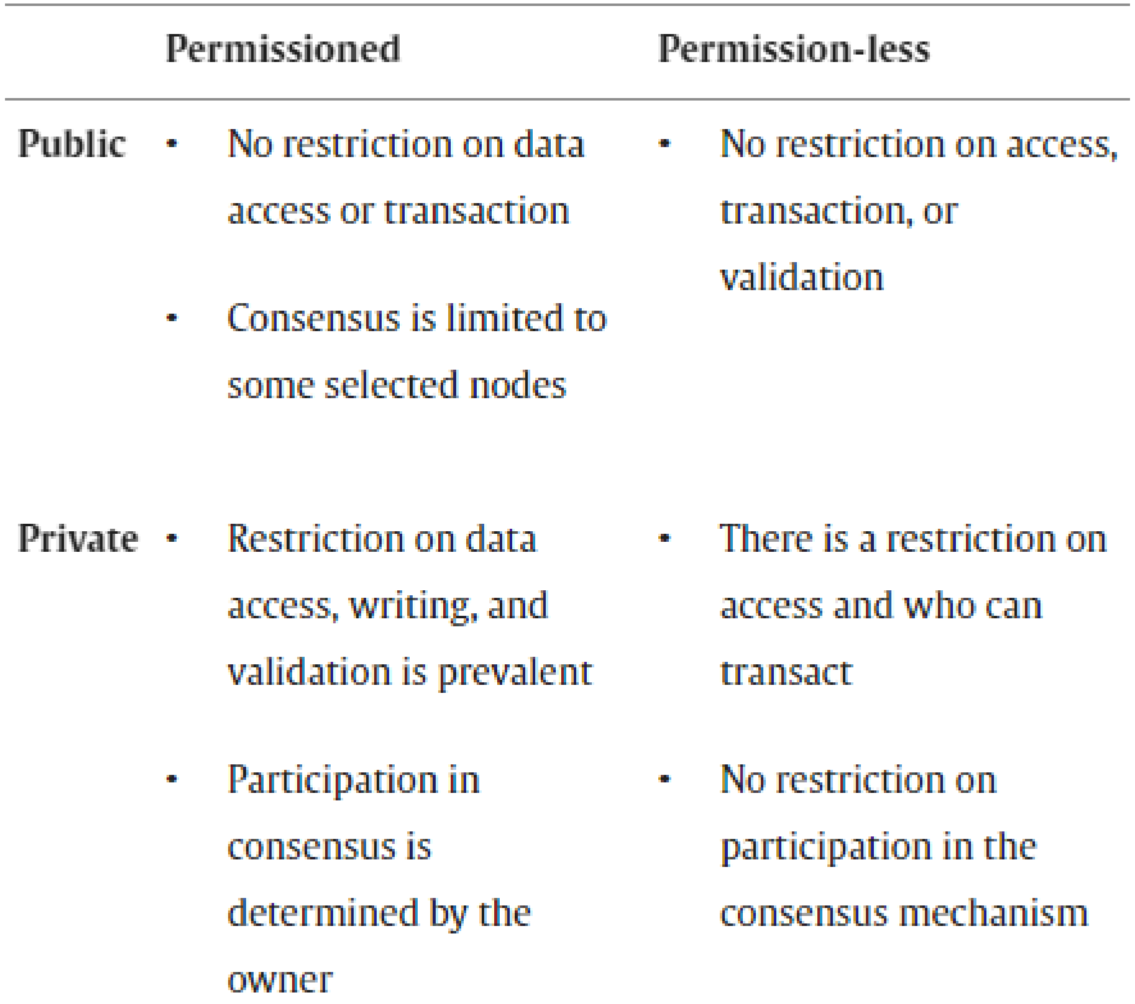
- As the name suggests, this ledger is distributed among its participants and spread across multiple sites or organizations.
- This type can either be **private or public**. The key idea is that, unlike many other blockchains,
- The records are stored contiguously instead of sorted into blocks. This concept is used in Ripple

Distributed Ledger Technology

- From a financial sector point of view, DLTs are permissioned blockchains that are shared and used between known participants.
- DLTs usually serve as a shared database, with all participants known and verified.

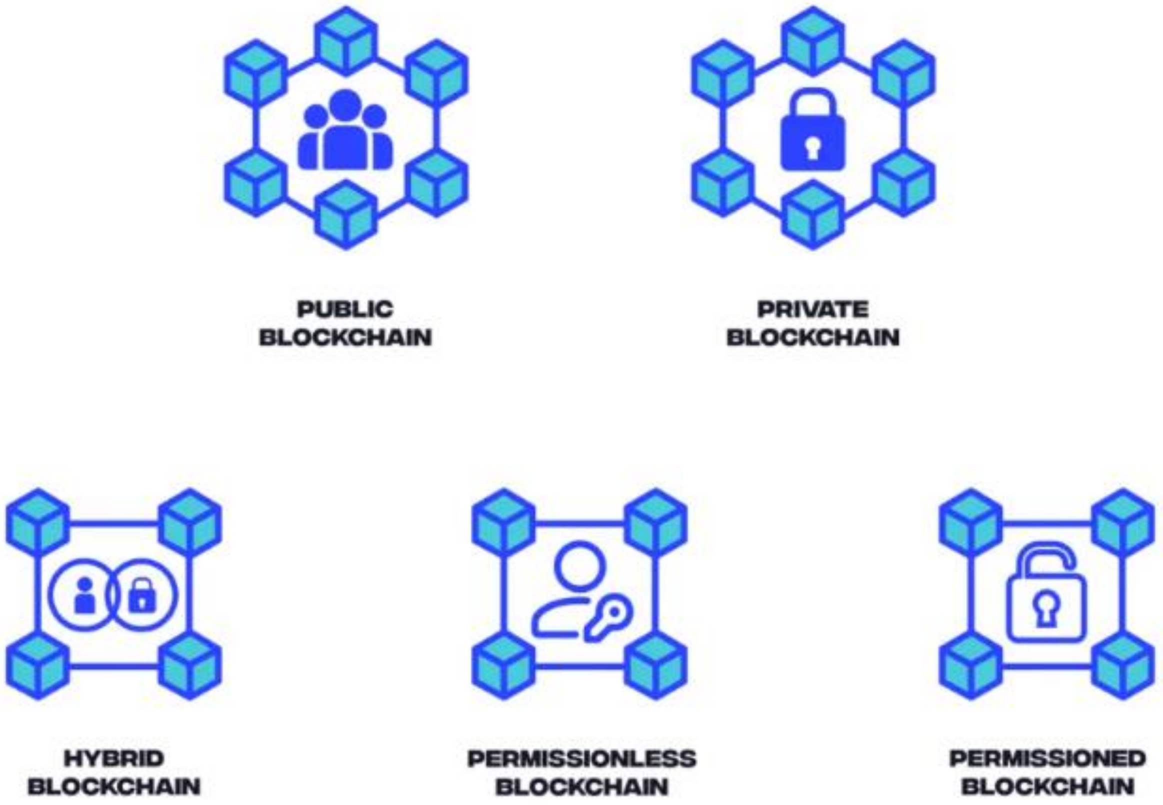
- **Tokenized :** These blockchains are standard blockchains that generate cryptocurrency as a result of a consensus process via mining or via initial distribution.
- Eg: **Ethereum, Solana, Polygon**
- **Token less:** blockchains are designed in such a way that they do not have the basic unit for the transfer of value. However, they are still valuable in situations where there is no need to transfer value between nodes and only the sharing of data among **various trusted parties** is required.
- No cryptocurrency is used for operations or fees
- Eg: **Corda (by R3)** – designed for enterprise use, financial institutions.
- **Hyperledger Fabric** – permissioned enterprise blockchain.
- **Hedera**

Public vs Private

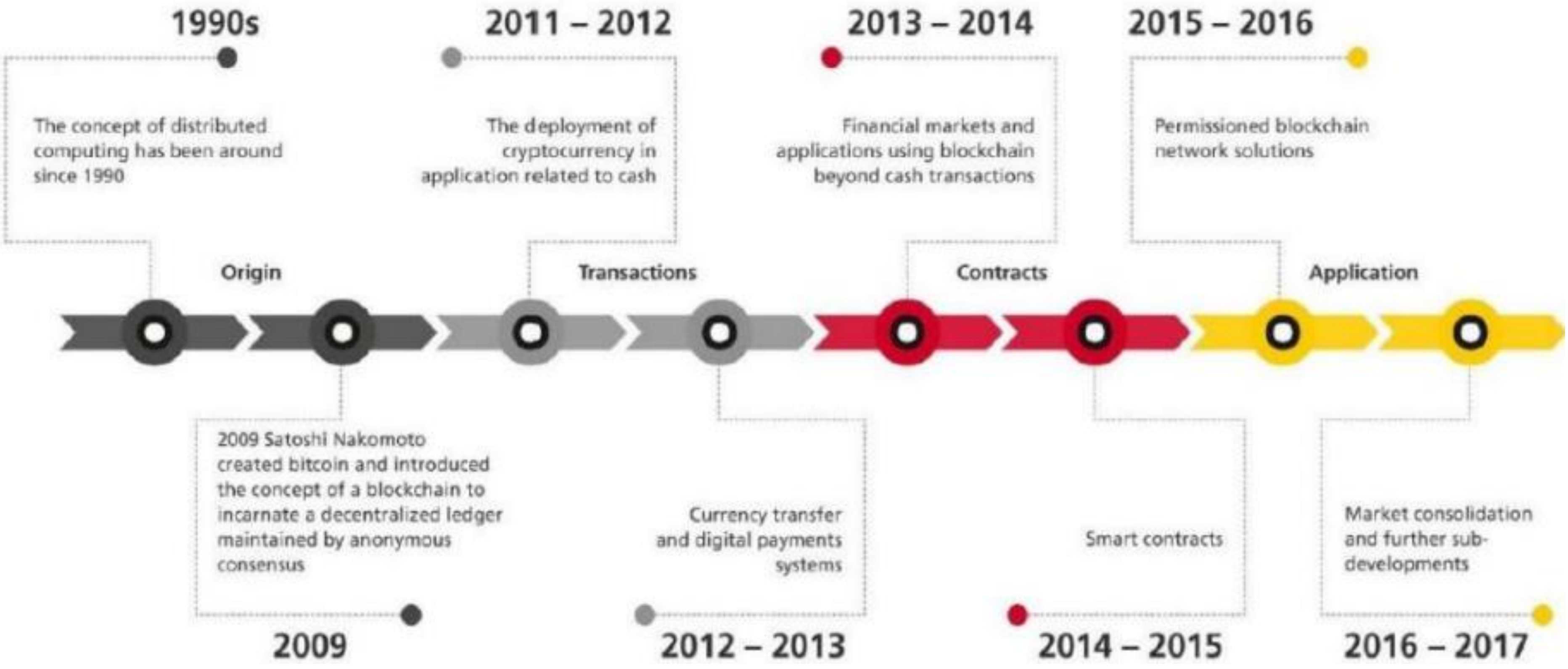


	Permissioned	Permission-less
Public	• No restriction on data access or transaction • Consensus is limited to some selected nodes	• No restriction on access, transaction, or validation
Private	• Restriction on data access, writing, and validation is prevalent • Participation in consensus is determined by the owner	• There is a restriction on access and who can transact • No restriction on participation in the consensus mechanism

Types of Blockchain



Blockchain Evolution



1990s

The concept of distributed computing has been around since 1990

2009

2009 Satoshi Nakomoto created bitcoin and introduced the concept of a blockchain to incarnate a decentralized ledger maintained by anonymous consensus

2011 – 2012

The deployment of cryptocurrency in application related to cash

2012 – 2013

Currency transfer and digital payments systems

2013 – 2014

Financial markets and applications using blockchain beyond cash transactions

2014 – 2015

Smart contracts

2015 – 2016

Permissioned blockchain network solutions

2016 – 2017

Market consolidation and further sub-developments

Blockchain was introduced with the invention of bitcoin in 2008 and then with its practical implementation in 2009.

1. Conceptual Foundation (1990s)

- **Distributed computing** ideas emerge
- Forms the basis for future blockchain models

2. Blockchain Origin (2009)

- **Bitcoin** introduced by **Satoshi Nakamoto**
- Blockchain used as a **decentralized public ledger**

3. Transaction Phase (2011–2013)

- Cryptocurrency applied to **cash transactions**
- Rise of **digital payments** and **currency transfer**

4. Contract Phase (2013–2015)

- Expansion to **financial markets**
- Emergence of **smart contracts** (e.g., Ethereum)

5. Application Phase (2015–2017)

- **Permissioned blockchains** for enterprise use
- **Market consolidation** and industry-wide adoption
- Focus on **custom apps**, scalability, and security