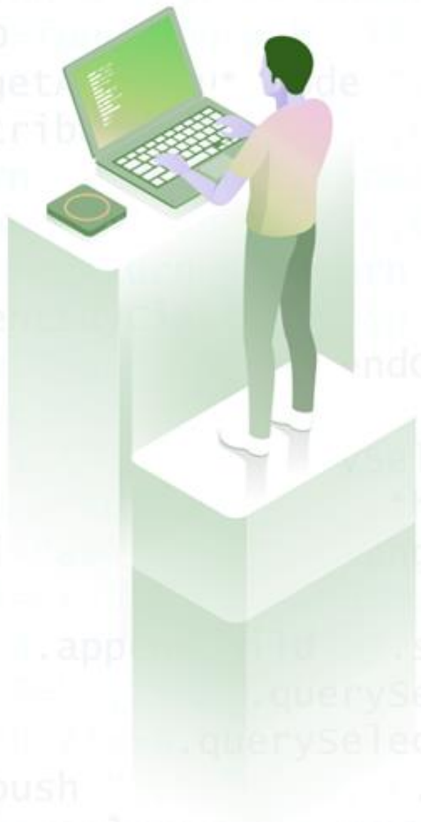
TECHNOLOGY

IIT KANPUR
Indian Institute of Technology, Kanpur

Professional Certification Program in Blockchain

TECHNOLOGY



Introduction to Blockchain

Learning Objectives

By the end of this lesson, you will be able to:

- Identify present business challenges
- Analyze ledger system and peer-to-peer networks
- Classify centralized, distributed, and decentralized systems
- Identify the components of a Blockchain

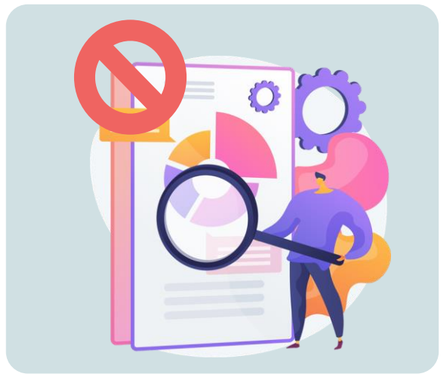
TECHNOLOGY

Challenges Faced by Modern Businesses

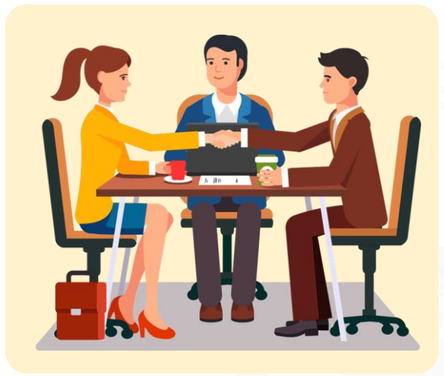
Challenges Faced by Modern Businesses

Blockchain can help tackle the following business challenges:

Lack of Trust



No Transparency



Mediator Charges

Manual Processes

Information Security

Lack of Trust

- In business, two or more untrusted parties might need to interact with each other or transact in an untrusted medium.
- Hence a mechanism was required where people could do business with untrusted parties.

Lack of Transparency

- Most organisations keep their data/systems private and this hinders their transparency.
- Lack of transparency eventually leads to lack of trust, which can stunt their growth.

Mediator Charges

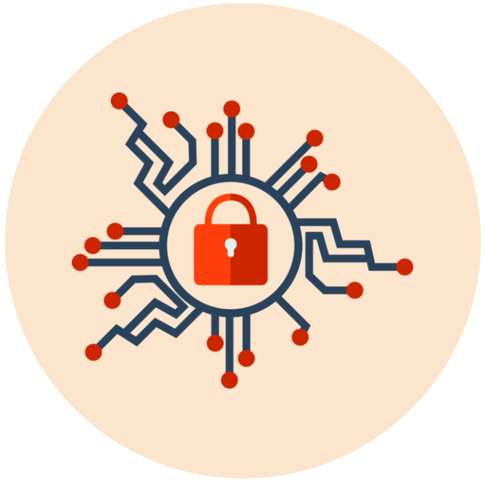
- Mediators, also referred to as middle-men, form a crucial part of business today.
- They help various parties reach an agreement, but their drawback is that they charge a hefty fee.

Manual Processes

- Though we live in the digital age, most of our important procedures such as property registration and census registration are still manual.
- Manual procedures are error prone due to human intervention.
- This can be avoided using a neatly designed computer system.

Information Security

- Information/Data is an asset to business.
- Loss or leak of such data can lead to losing money and reputation.



TECHNOLOGY

What is Blockchain?

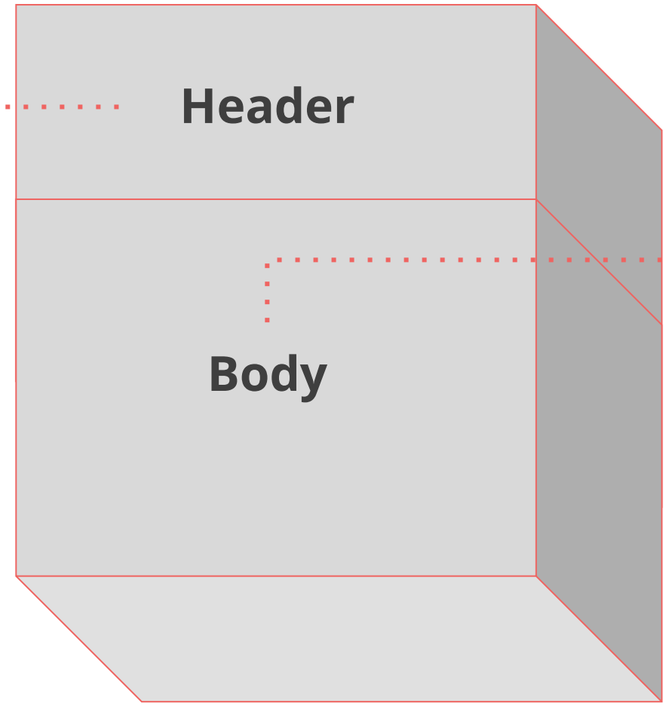
Blockchain Introduction

Blockchain is a peer-to-peer, decentralized, and distributed system. It is cryptographically secure, append-only, immutable, and updateable via a consensus or agreement among all the peers.

Components of a Block

Header

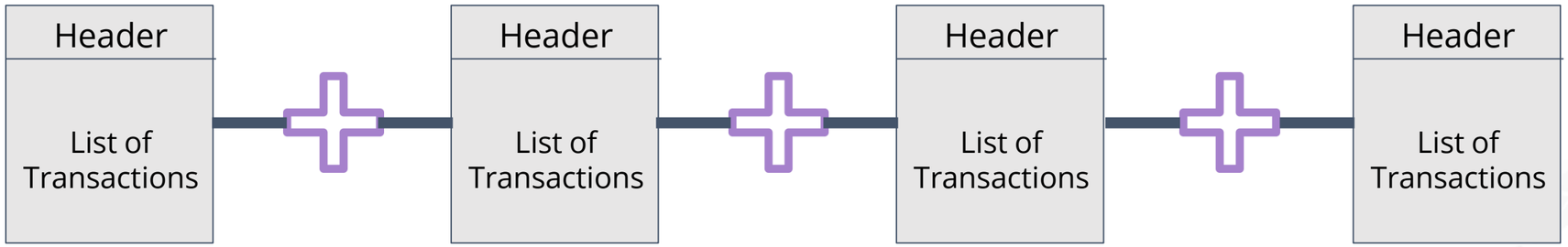
Consists of the version of the block, hash of the previous block, the merkle root hash, and the timestamp of creation



Body

Consists of the list of transactions recorded by the nodes and the nonce added by its miner

Components of a Blockchain



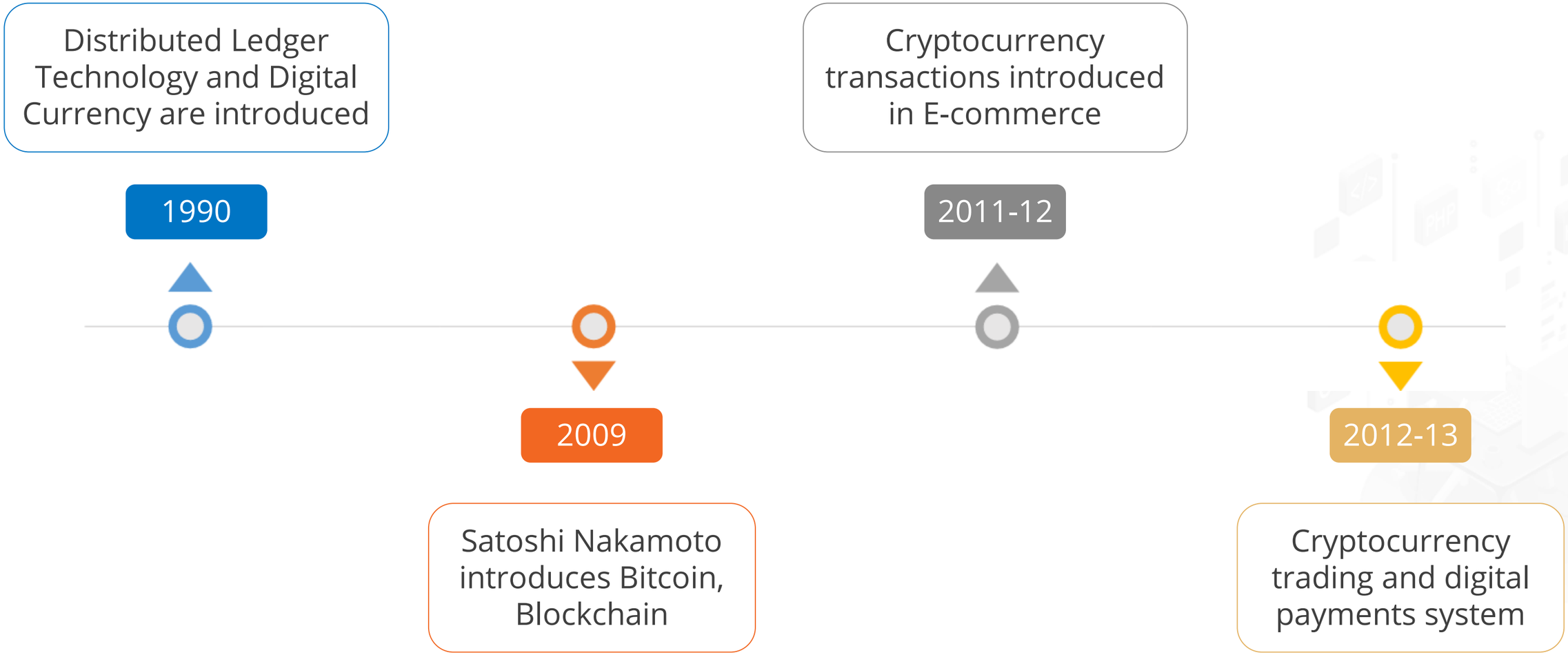
Block

It is a container to store the encrypted transaction details and the hash details of the previous block

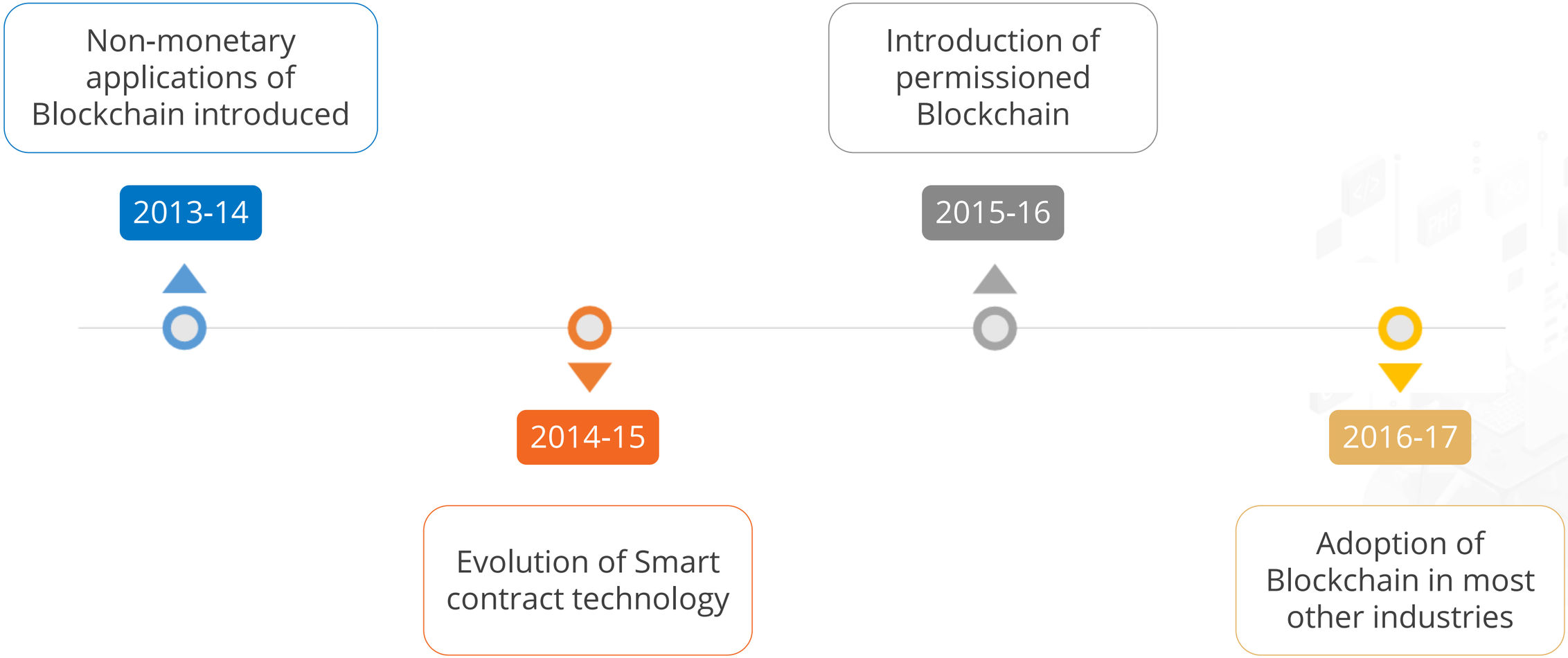
Chain

It is much like a continuous list of blocks attached to each other. Every block has the hash value of its previous block and its next block (if created)

History of Blockchain



History of Blockchain



Features of Blockchain

Transparency

Public ledger, consensus make data available to all

Immutability

Data cannot be altered, only appended

High Availability

Distributed, P2P architecture makes it more durable

Security

Cryptographically secure hashes to encrypt data

Cost Efficiency

Transaction cost is minimized by eliminating mediators

Difference Between Blockchain and Database

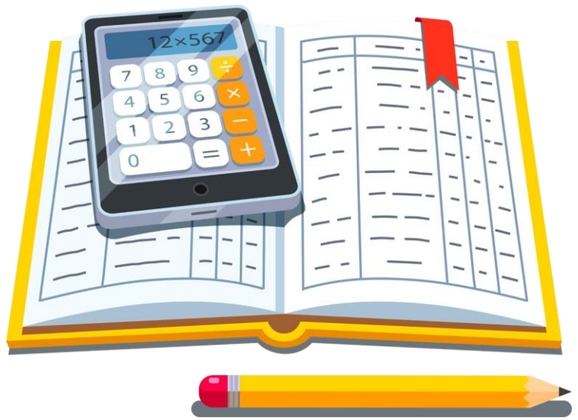
Database	Blockchain
Centralized network	Decentralized and distributed (peer-to-peer) network
All CRUD operations are supported	Only append operation possible
Data can be changed anytime with the correct privileges	Data is completely immutable in an ideal scenario
Difficult to scale for high availability	Highly available as distributed network is implemented
Data is not completely private. The database admin can read all the data present	Only hashes of actual data are encrypted and stored in the block

TECHNOLOGY

Building Blocks of Blockchain

Ledger

Ledger is a record keeping document where you keep track of all your transactions.



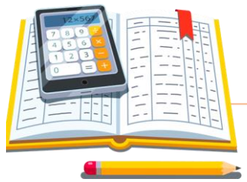
Evolution of Ledger

Papyrus

Simple arithmetic transactions recorded on a paper-like material

Ledger Book

Used scientific methods to store transaction records in a book

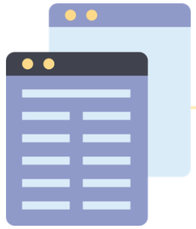


Spreadsheet

A modern, electronic version of a ledger book

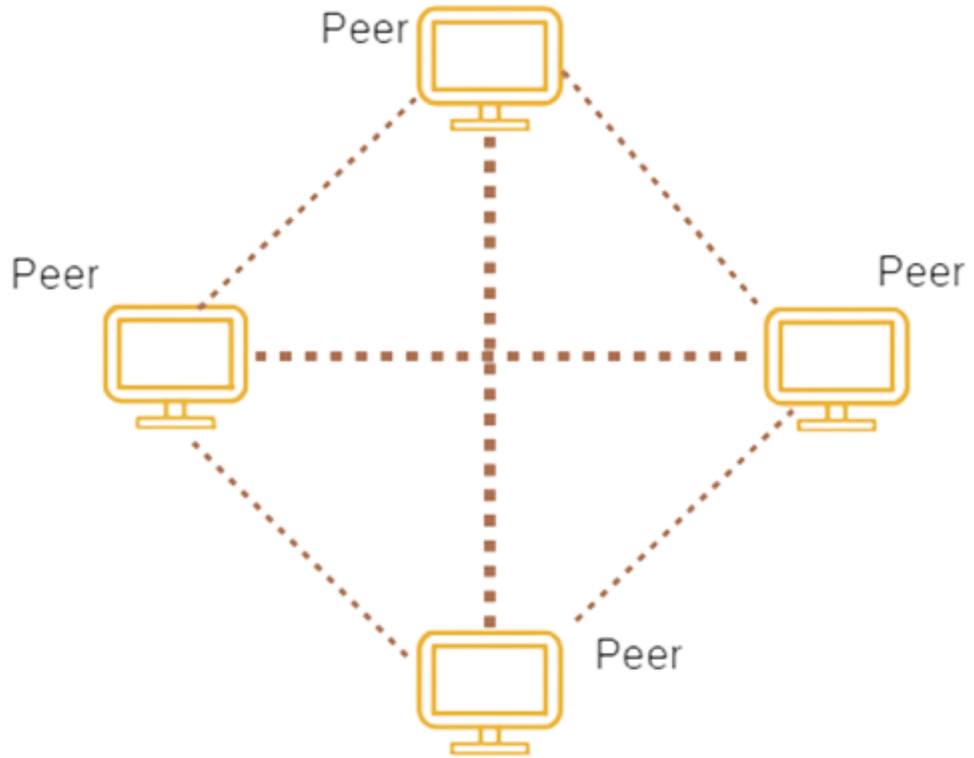
Distributed Ledger

The ledger is replicated at multiple nodes to maintain high availability and transparency



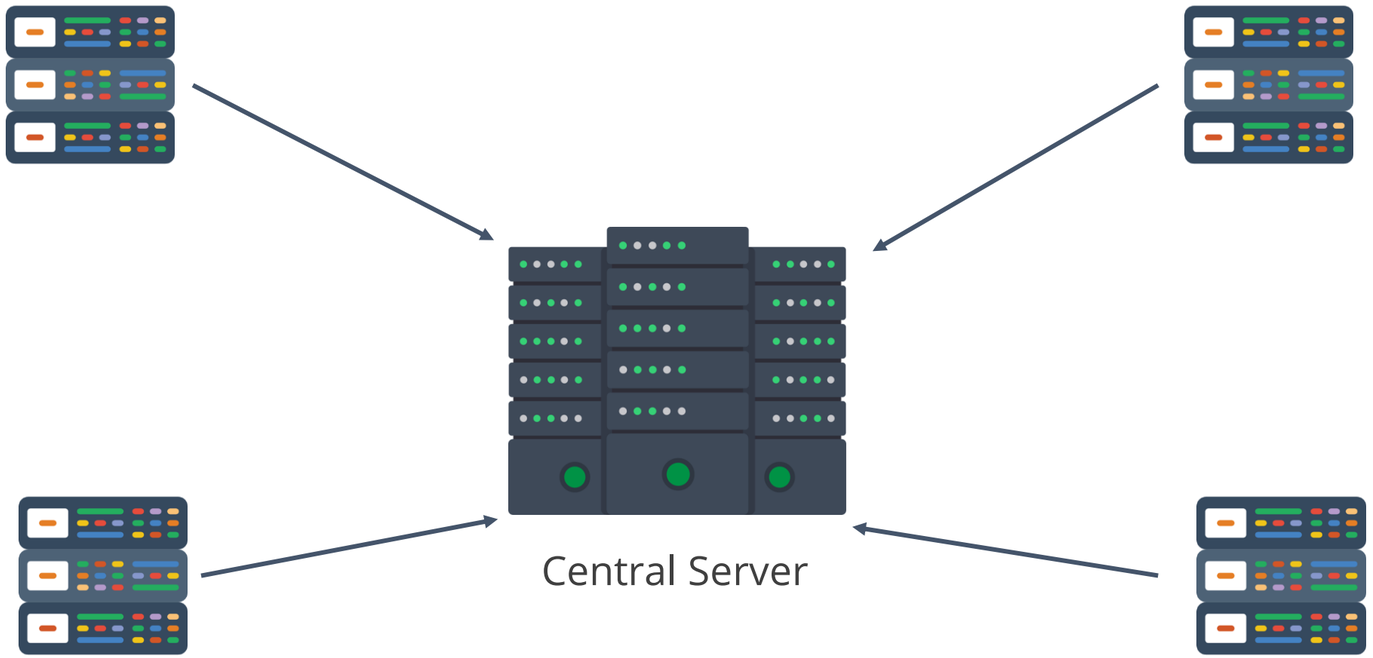
Peer-to-Peer Network

Peer-to-Peer (P2P) Network is a network architecture where multiple computers are connected to each other, and all nodes have equal responsibilities and access to resources in the network



Centralized System

Centralized systems are those where one person or entity has full control and authority over the system.

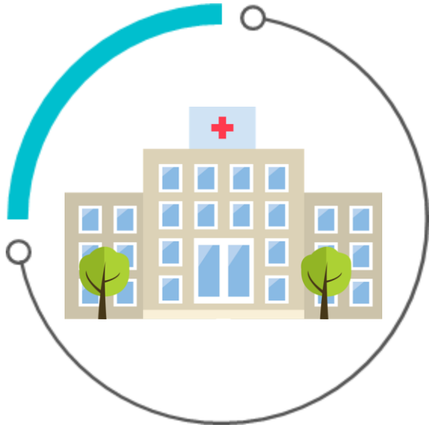


Centralized System

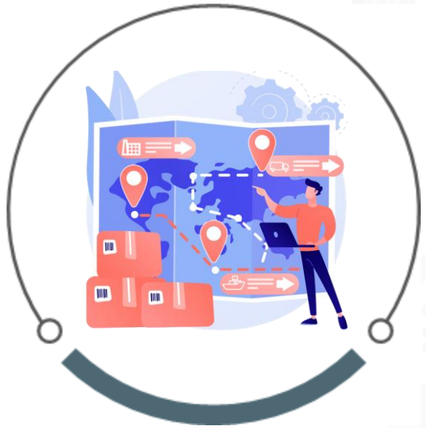
Most notable establishments and services today have a centralized architecture.
A few examples are:

Banking

Governance



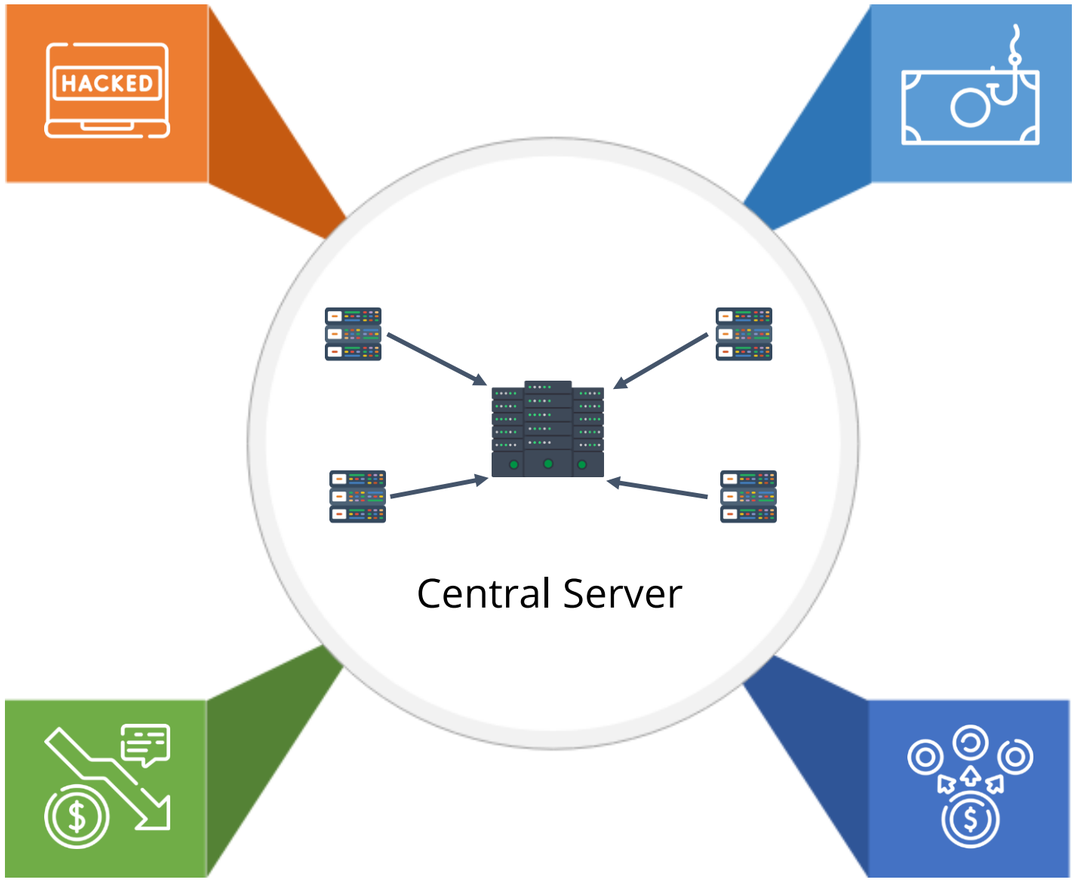
Hospitals



Supply Chain

Drawbacks of Centralized System

Easily prone to hacking



May facilitate fraudulent activities

Leads to financial crisis

High transaction cost

Drawbacks of Centralized System

Prone to Hacking

- All the data is stored at one central place
- Easy to compromise one central server
- Easy to compromise the person who manages that central system

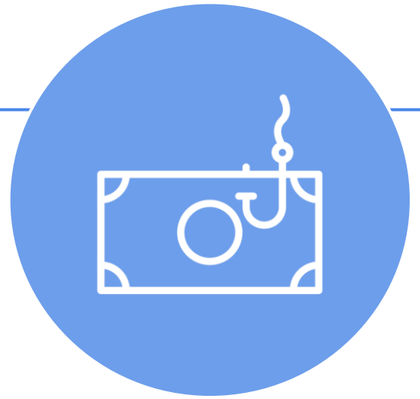
Financial Crisis

- One person or entity has full control on the data
- That one person or central authority can manipulate the data as needed for their financial gain

Drawbacks of Centralized System

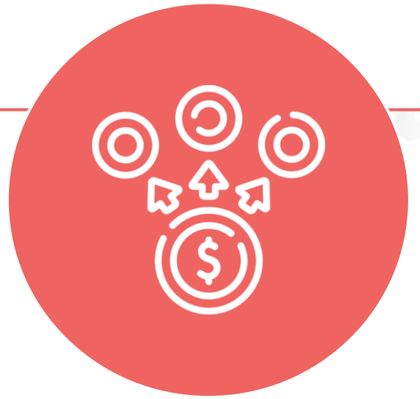
Fraudulent Activities

- Information can be hidden
- Back entries can be altered



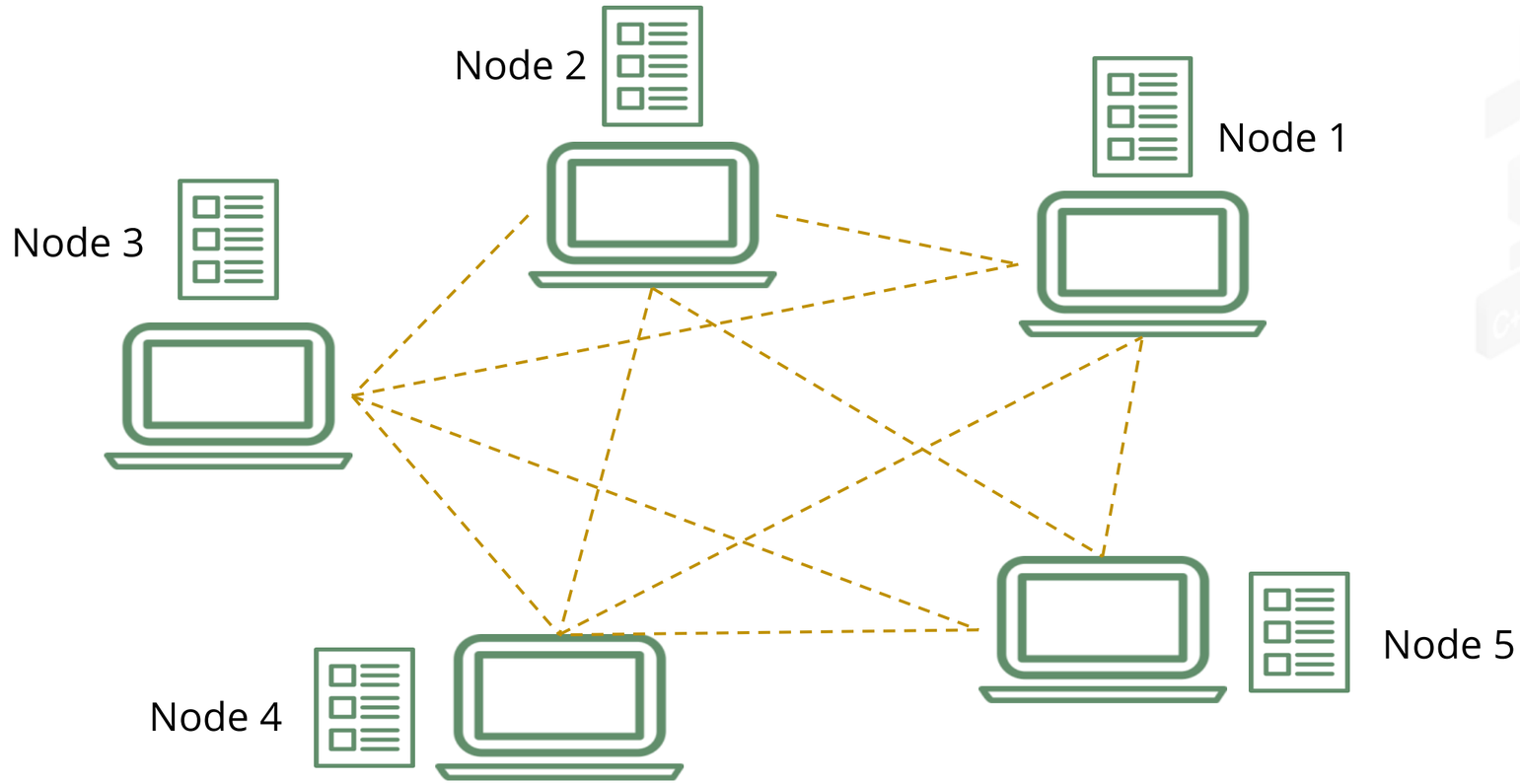
Transaction Cost

- Involvement of middle man
- High transaction fee

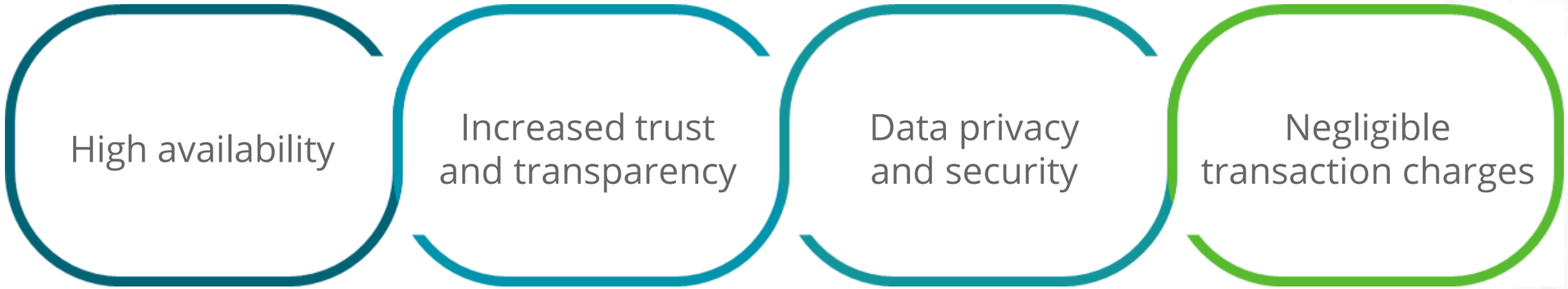


Distributed and Decentralized System

In such systems, the resources and computation are shared among all the participating nodes, and the decision-making responsibility is split equally among these nodes.



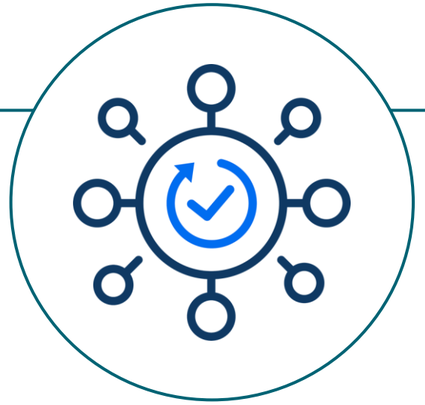
Benefits of Decentralized and Distributed System



Benefits of Decentralized and Distributed System

High Availability

- Network is still up and running even if 90% of nodes are down
- Peers are distributed across the globe



Increased Trust

- Due to high transparency
- Anyone can see and validate the data
- Nothing is hidden from users

Benefits of Decentralized and Distributed System

Data Privacy

- All the data stored on the network is encrypted
- Only the hashes of private data are stored and not the personal data

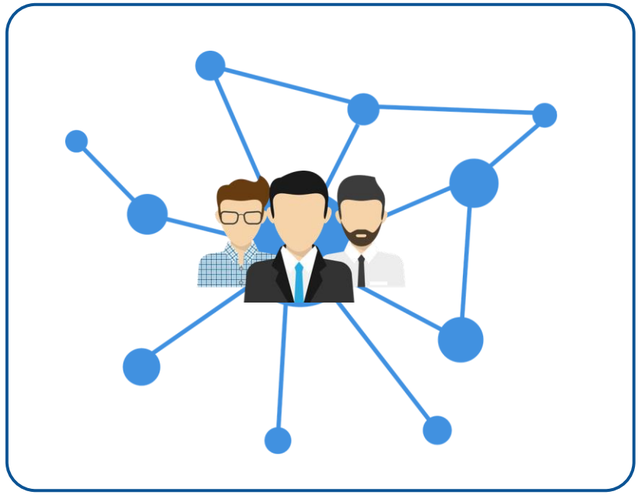
Low Transaction Cost

- Network is maintained by peers not by central authority
- There can be a minimal fee based upon the network size, security, and the number of transactions but it is way less than that of the centralized system

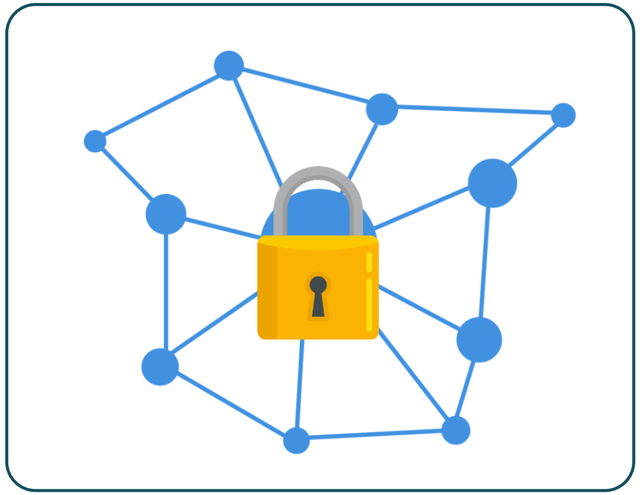
Types of Blockchain

Types of Blockchain

There are three general types Blockchain technology is categorized into:



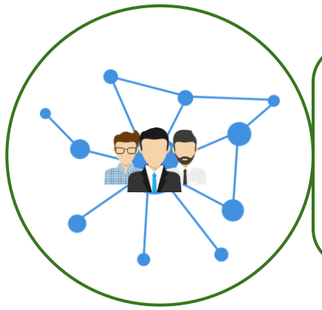
Public



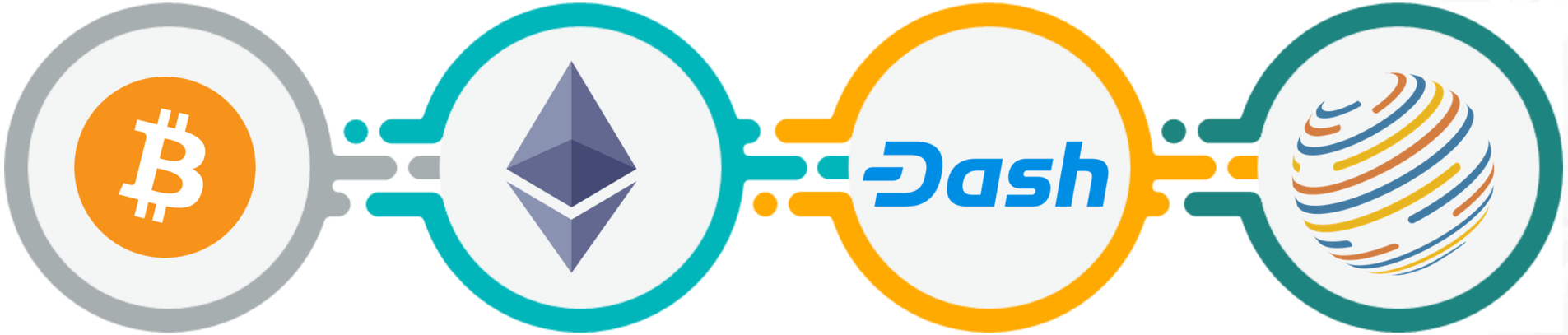
Private

Permissioned

Public Blockchain

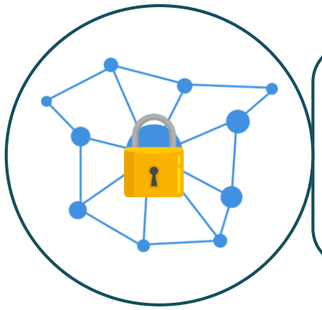


- Transactions and data are viewable by all participants
- Participant identity can be kept anonymous



Bitcoin | Ethereum | Dash | Factom

Private Blockchain

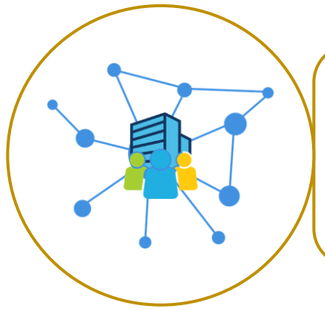


- Transactions are secret and are only visible to the admin
- All participants are known and belong to the same organization

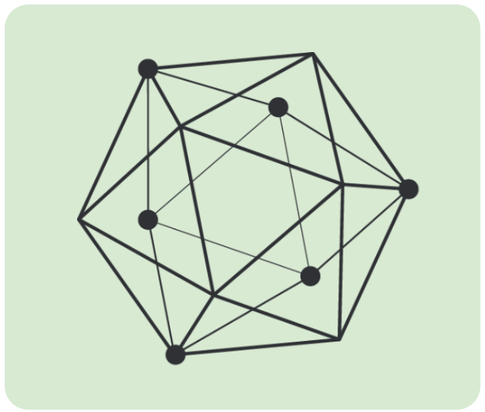
MultiChain

BlockStack

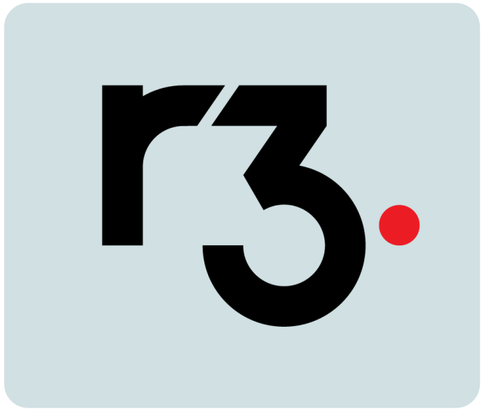
Permission/Consortium Blockchain



- Transactions are semi-secret and are visible to specific members
- All participants are known and their identities are linked to their real-life identities



Hyperledger



R3

Ripple

Public Vs Private Vs Permissioned Blockchain

	Public	Private	Permissioned
Consensus Determination	All participating members	Only admins	Any member with the right access level
Data Access	Public	Restricted	Restricted to certain degree
Immutability	Almost impossible to tamper	Can be mutated	Can be mutated
Resource Required	Low	High	High
Centralization	No	Yes	Semi-centralized
Consensus Process	Permissionless	Needs permission	Needs permission

Key Takeaways

- Identifying business challenges such as lack of trust, mediator charges, no transparency, and no privacy
- Identifying the key components of a Blockchain: distributed public ledger, decentralized system, cryptography, and consensus
- Defining a Blockchain and block, and how they are linked to one another
- Understanding the three different types of Blockchain, their applications, and differences