SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

Dr. Poornima B V
Assistant Professor,
Computer Science and Engineering,
Sahyadri College of Engineering and Management,
Adyar, Mangalore-575007.
Email: Poornima.cs@sahyadri.edu.in

Introduction to Blockchain Technology

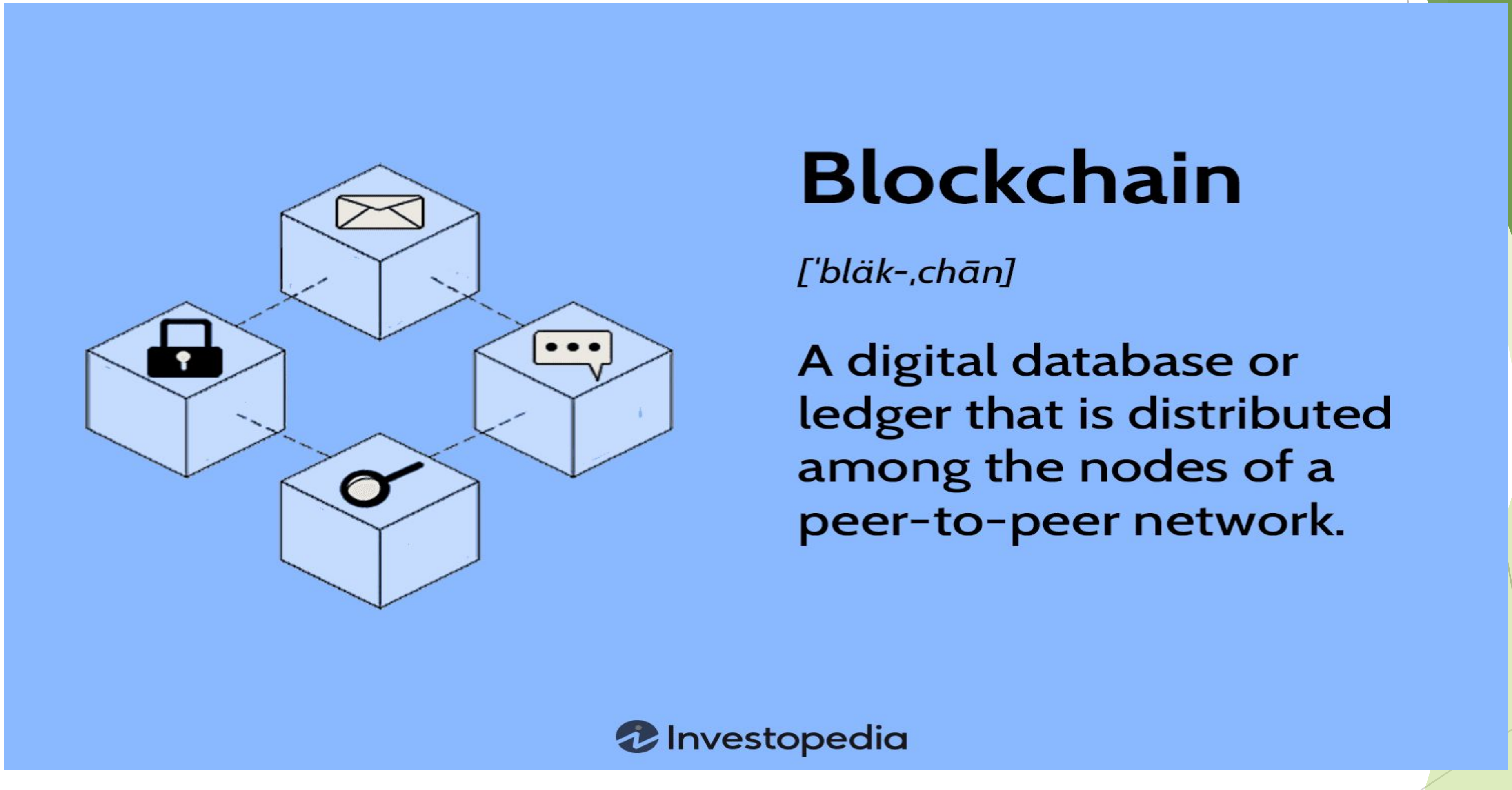
What is Blockchain Technology?

How Does Blockchain Work?

Key Features of Blockchain Technology

Real-World Applications of Blockchain Technology

Tips for Embracing Blockchain Technology

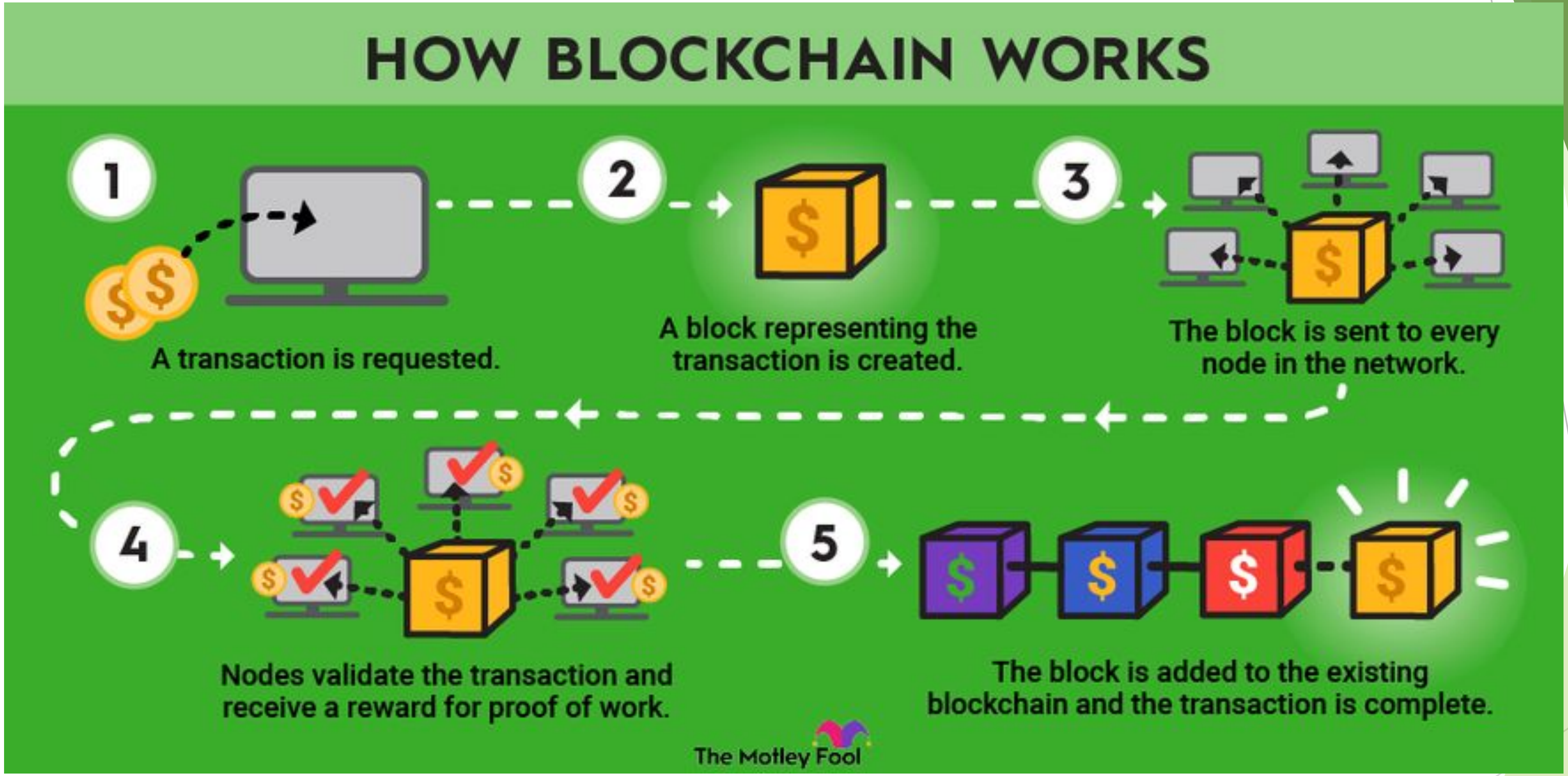


Blockchain

['bläk-,chān]

A digital database or ledger that is distributed among the nodes of a peer-to-peer network.

Investopedia



HOW BLOCKCHAIN WORKS

1 A transaction is requested.

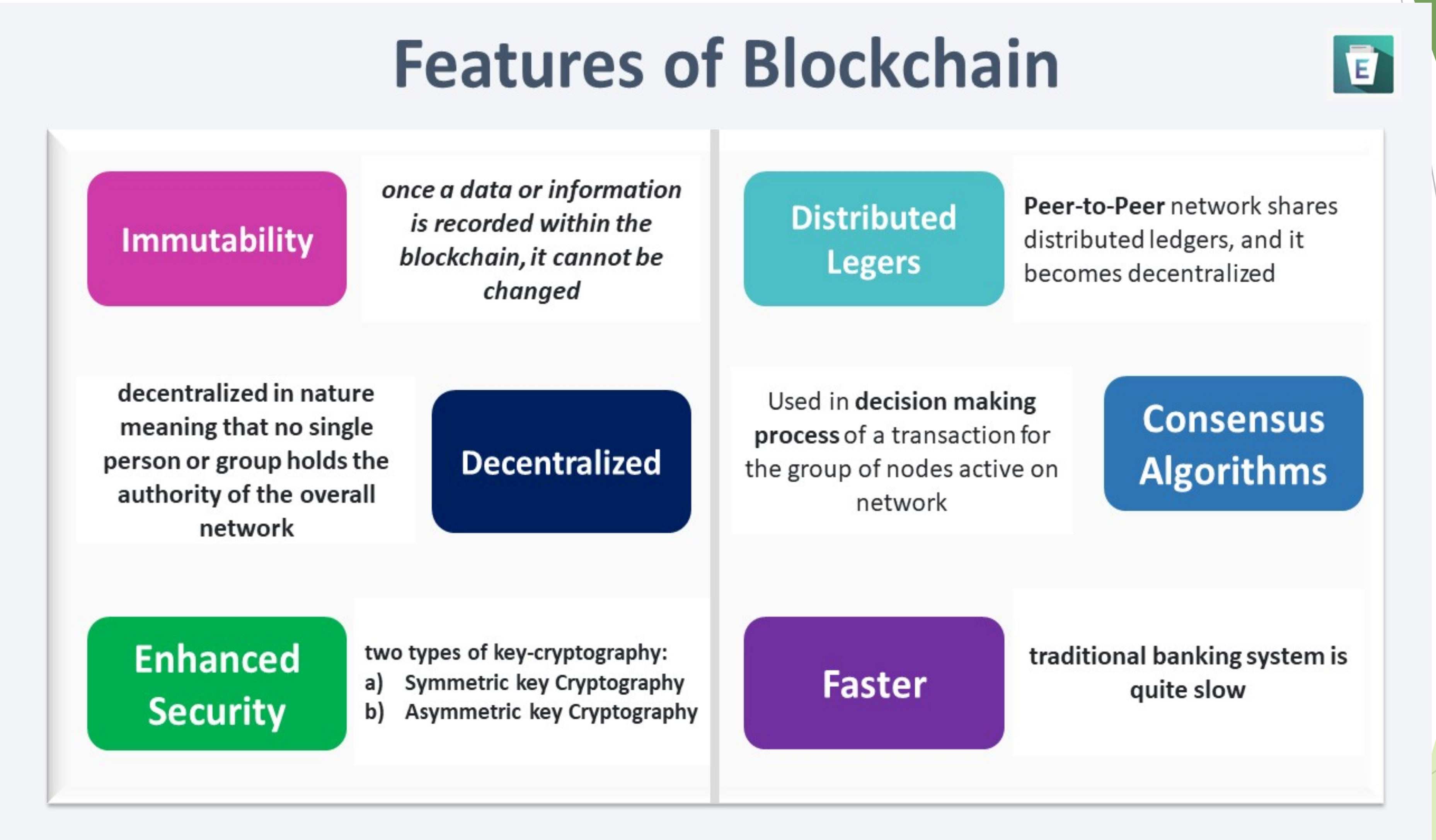
2 A block representing the transaction is created.

3 The block is sent to every node in the network.

4 Nodes validate the transaction and receive a reward for proof of work.

5 The block is added to the existing blockchain and the transaction is complete.

The Motley Fool



Features of Blockchain

Immutability

once a data or information is recorded within the blockchain, it cannot be changed

Decentralized

decentralized in nature meaning that no single person or group holds the authority of the overall network

Enhanced Security

two types of key-cryptography:

a) Symmetric key Cryptography

b) Asymmetric key Cryptography

Distributed Legers

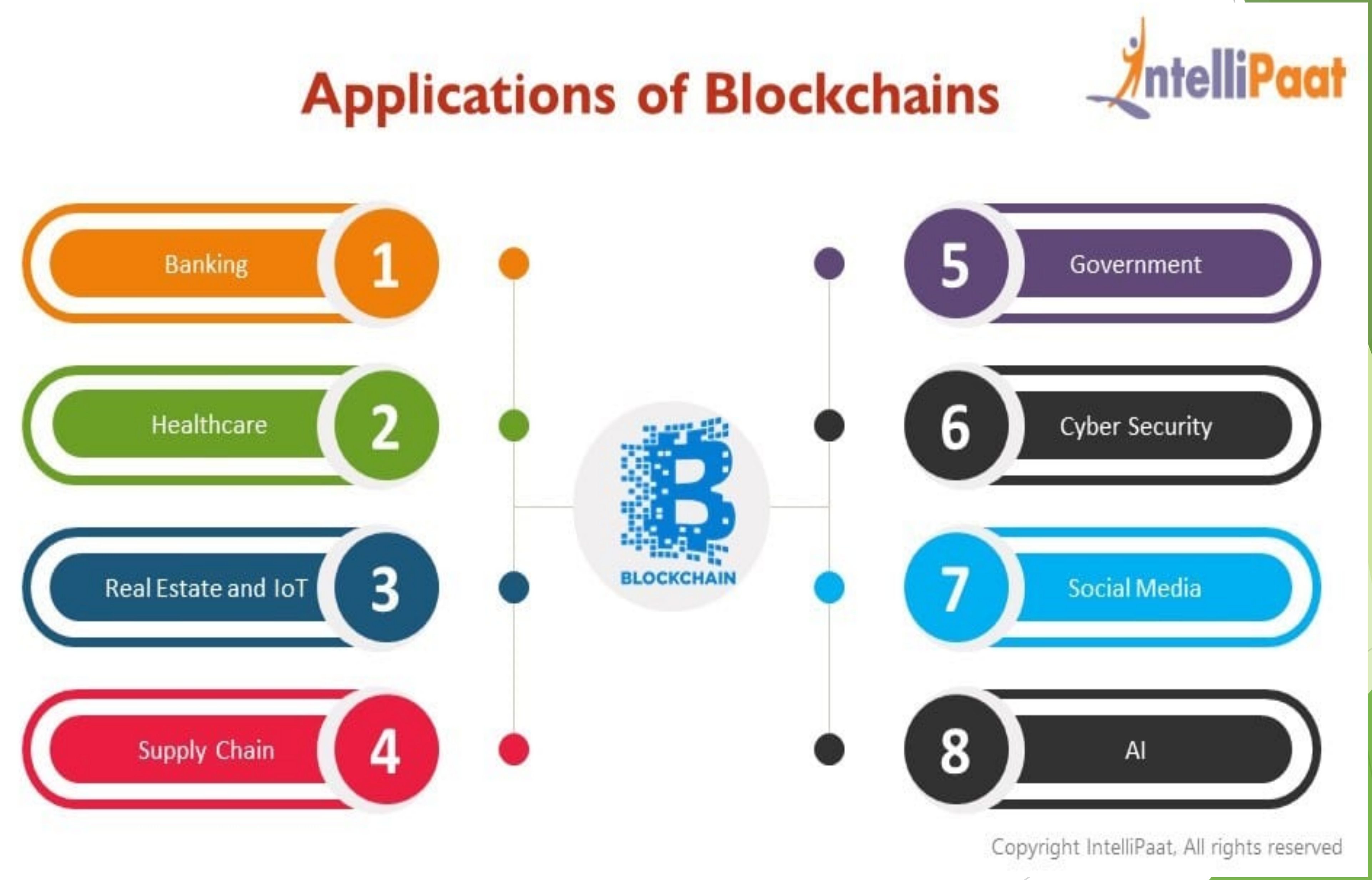
Peer-to-Peer network shares distributed ledgers, and it becomes decentralized

Consensus Algorithms

Used in **decision making process** of a transaction for the group of nodes active on network

Faster

traditional banking system is quite slow



Applications of Blockchains

IntelliPaat

1 Banking

2 Healthcare

3 Real Estate and IoT

4 Supply Chain

5 Government

6 Cyber Security

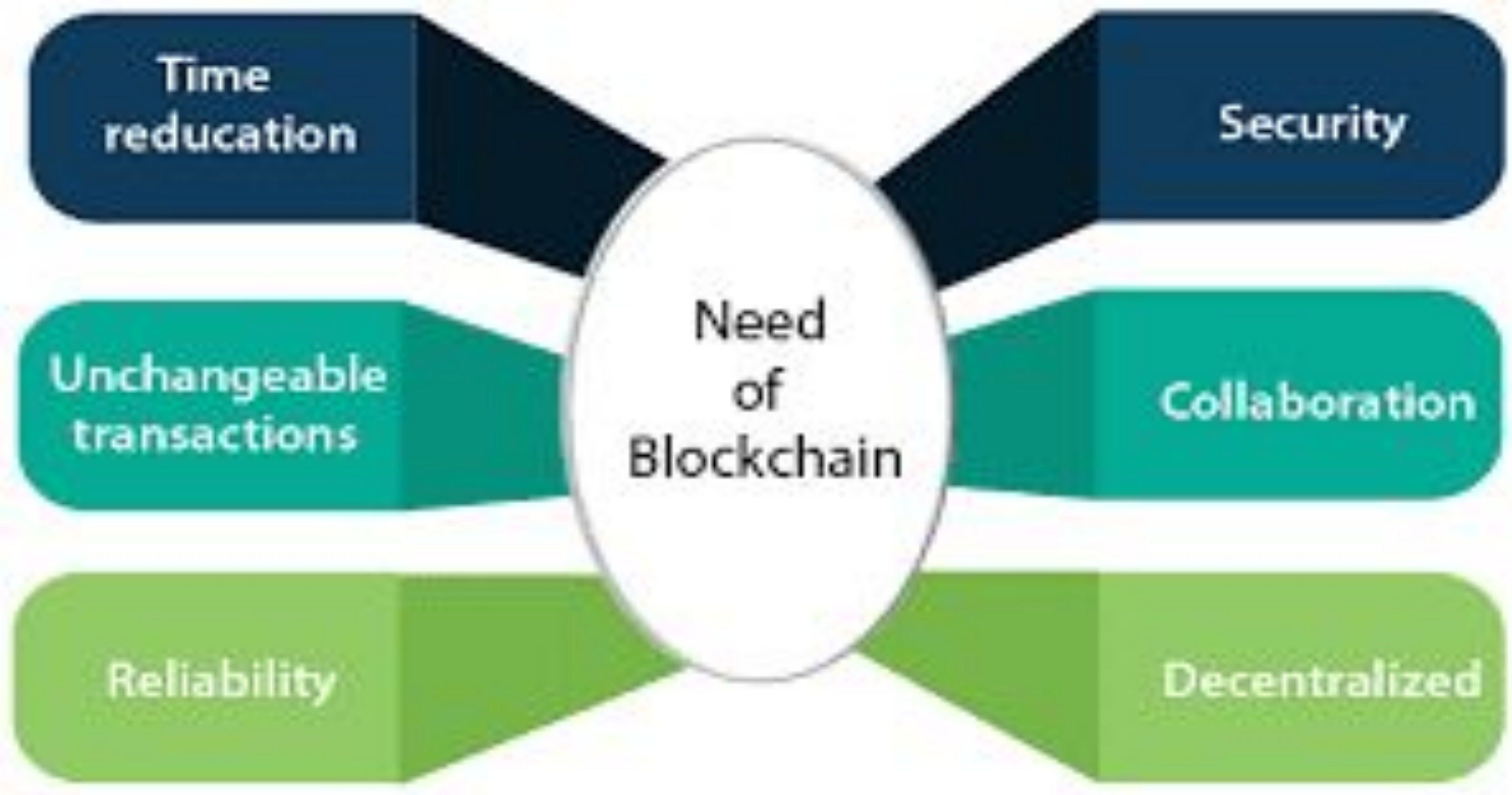
7 Social Media

8 AI

- Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the **“chain,”** in a network connected through peer-to-peer nodes.
- Typically, this storage is referred to as a ‘**digital ledger**.’ Every transaction in this ledger is authorized by the **digital signature** of the owner, which authenticates the transaction and safeguards it from tampering.
- Hence, the information the digital ledger contains is highly secured.
- In simpler words, the digital ledger is like a **Google spreadsheet** shared among **numerous computers** in a network, in which, the transactional records are stored based on actual purchases.
- The fascinating angle is that anybody can see the data, but they can’t corrupt it

Blockchain definition

- **Layman's definition**: Blockchain is an ever-growing, secure, shared record keeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.
- **Technical definition: Blockchain 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.

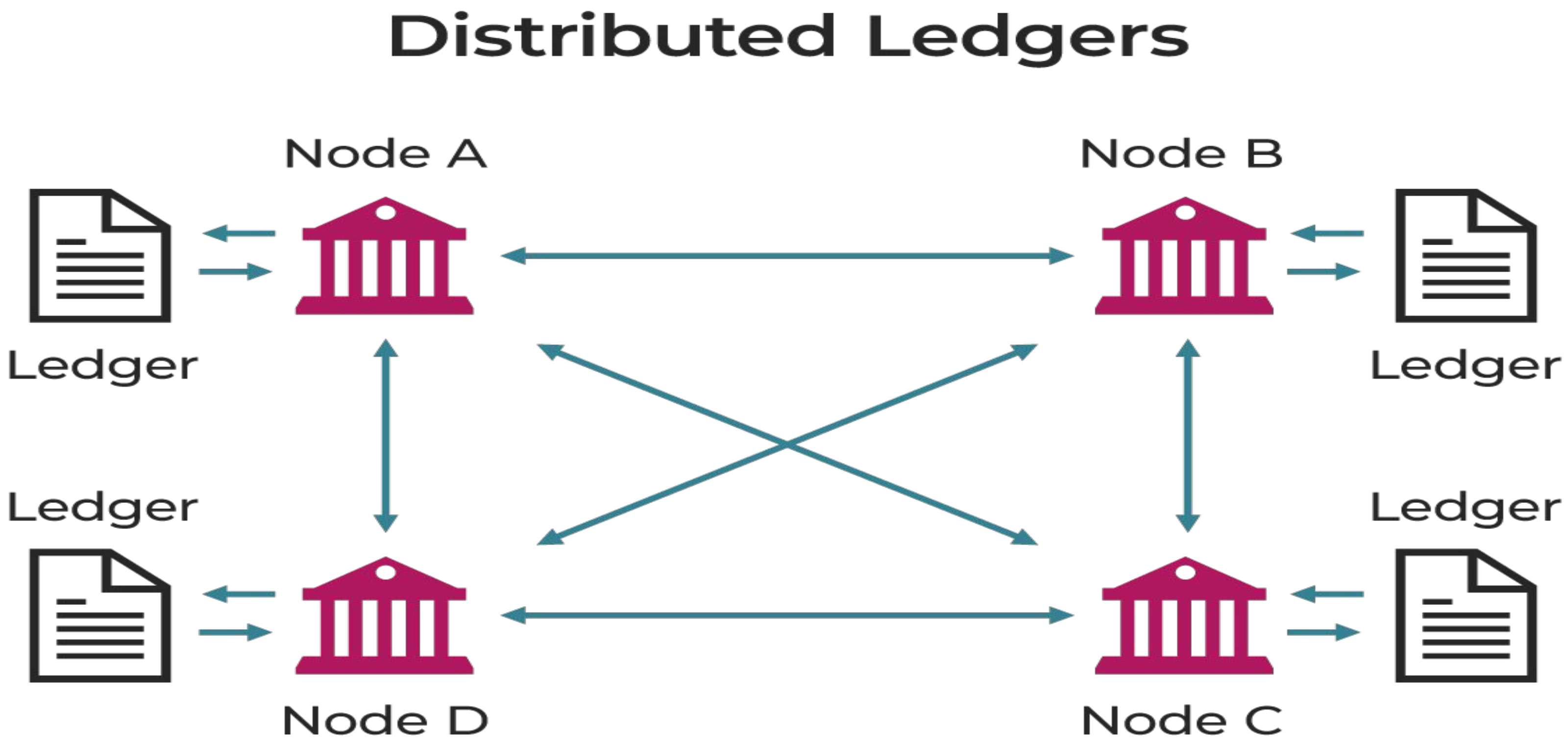

Time reducation
Security
Unchangeable transactions
Need of Blockchain
Collaboration
Reliability
Decentralized

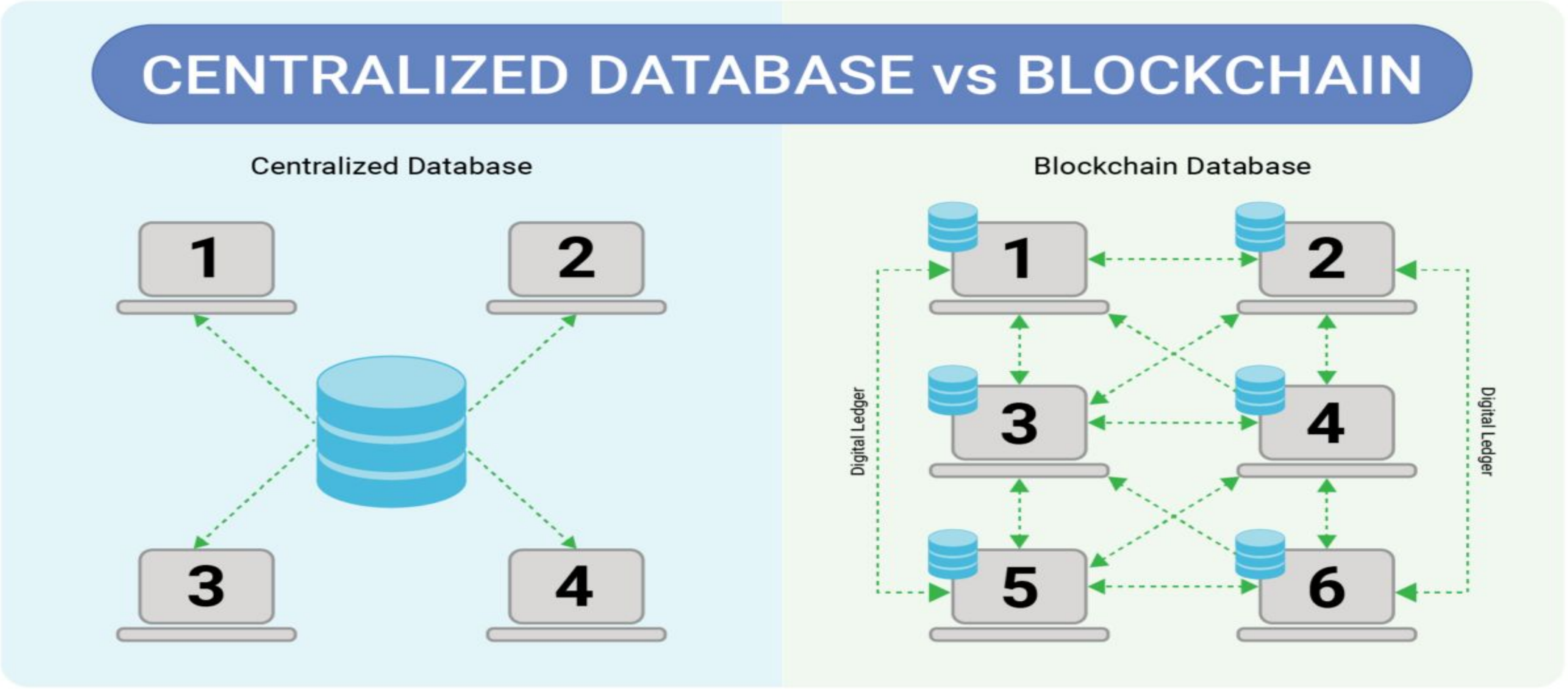
Distributed systems

- It is a distributed ledger which can be centralized or decentralized.
- A blockchain is originally intended to be and is usually used as a decentralized platform.
- It can be thought of as a system that has properties of both decentralized and distributed paradigms.
- It is a decentralized-distributed system.

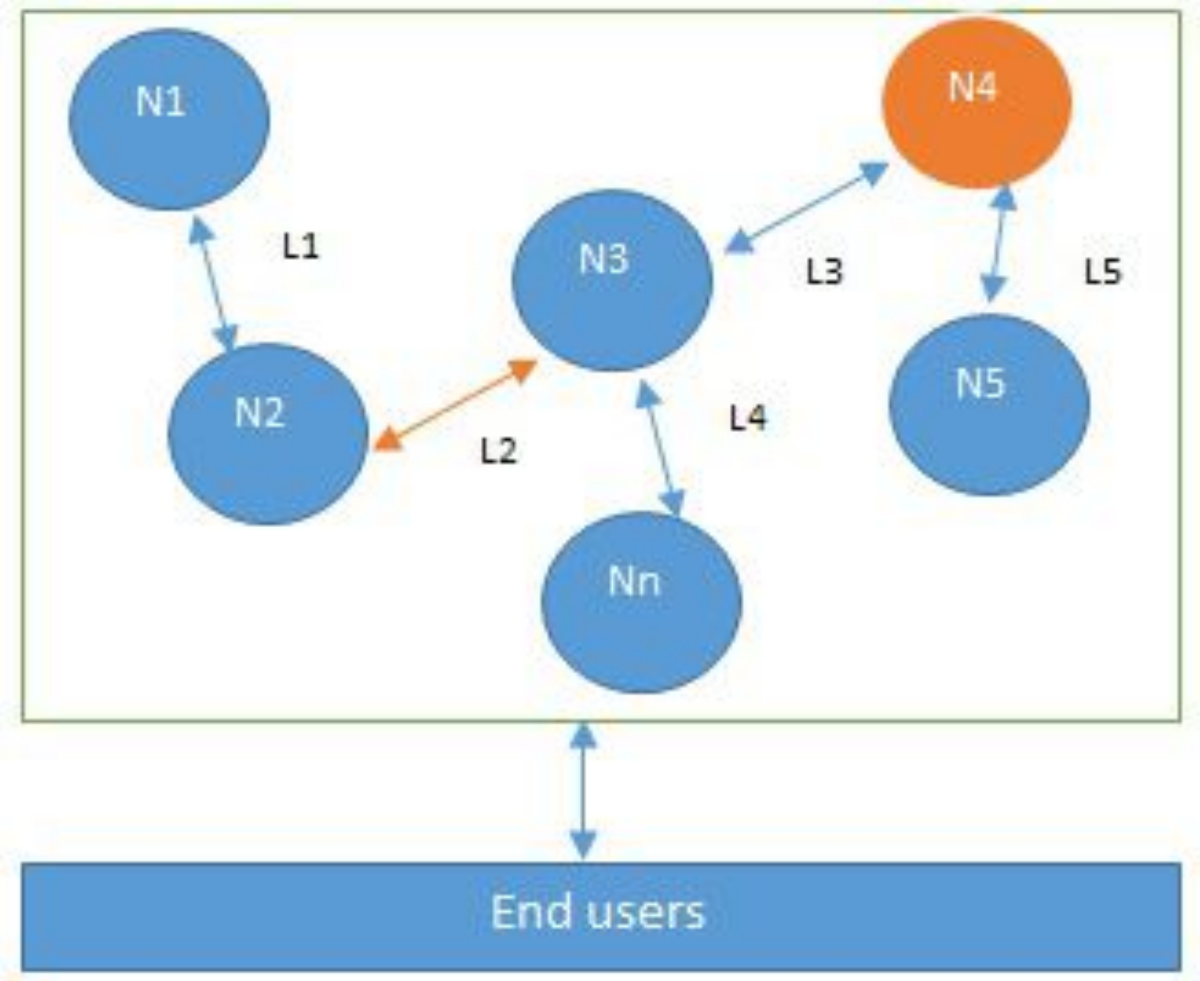
- Distributed systems are a computing paradigm whereby two or more nodes work with each other in a coordinated fashion to achieve a common outcome.
- Google's search engine is based on a large distributed system, but to a user, it looks like a single, coherent platform.
- A node can be defined as an individual player in a distributed system.
- All nodes are capable of sending and receiving messages to and from each other.

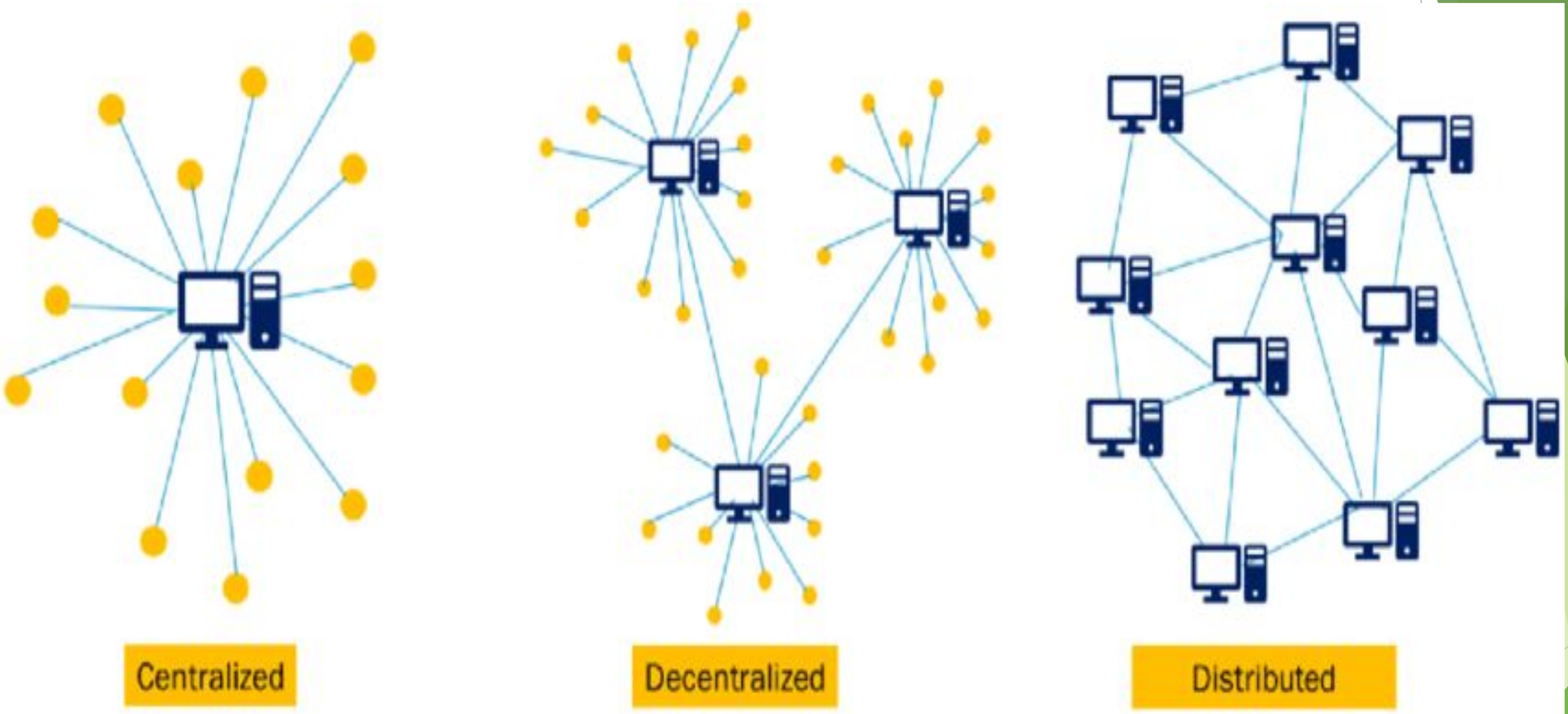
- Nodes can be honest, faulty, or malicious, and they have memory and a processor.
- A node that exhibits irrational behavior is also known as a Byzantine node.
- Byzantine node leading to possible data inconsistency.


Distributed Ledgers
Node A
Node B
Ledger
Ledger
Ledger
Ledger
Node D
Node C


CENTRALIZED DATABASE vs BLOCKCHAIN
Centralized Database
1
2
3
4
Blockchain Database
1
2
3
4
5
6
Digital Ledger
Digital Ledger

Design of a distributed system: N4 is a Byzantine node, L2 is broken or a slow network link




Centralized
Decentralized
Distributed

Challenges of Distributed System

- The primary challenge in distributed system design is **coordination between nodes and fault tolerance.**
- Even if some of the nodes become faulty or network links break, **the distributed system should be able to tolerate this** and continue to work to achieve the desired result.
- Distributed systems are so challenging to design that a **hypothesis known as the CAP theorem has been proven, which states that a distributed system cannot have all three of the much-desired properties simultaneously; that is, consistency, availability, and partition tolerance.**

Keywords in the definitions

- **Peer-to-peer**: This means that there is no central controller in the network, and all participants talk to each other directly. This property allows for cash transactions to be exchanged directly among the peers without a third-party involvement, such as by a bank.
- **Distributed ledger:** Ledger is spread across the network among all peers in the network, and each peer holds a copy of the complete ledger.

Keywords in the definitions

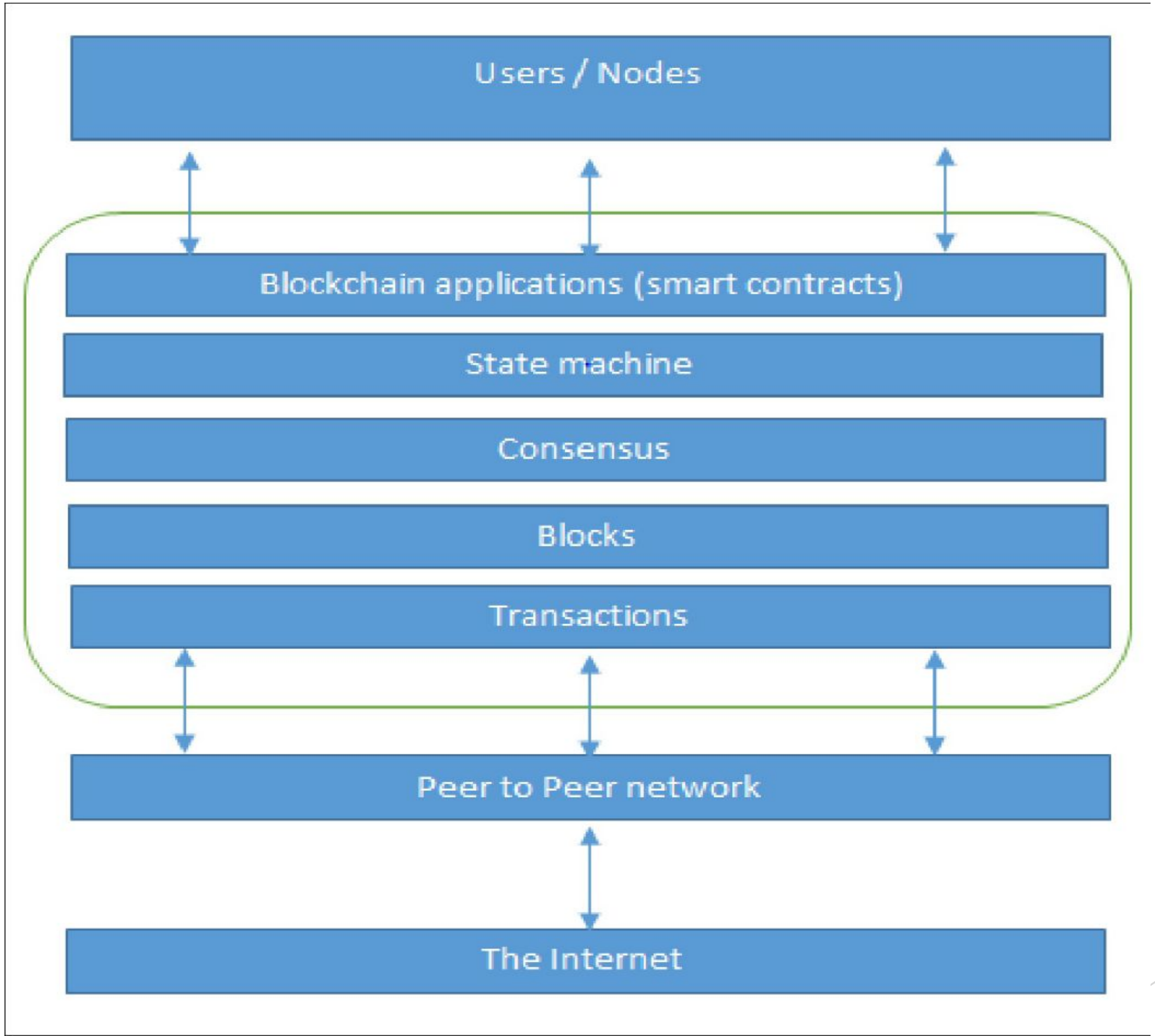
- **Cryptographically-secure:** Cryptography has been used to provide security services which make this ledger secure against tampering and misuse. These services include non-repudiation, data integrity, and data origin authentication.
- **Append-only:** Data can only be added to the blockchain in time-ordered sequential order. This property implies that once data is added to the blockchain, it is almost impossible to change that data and can be considered practically immutable.

- Non-repudiation: Ensures that a sender cannot deny having sent a message, typically using digital signatures.
- Data Integrity: Guarantees that data remains unchanged during transmission or storage, often verified using cryptographic hash functions.
- Data Origin Authentication: Confirms the source of received data, ensuring it comes from a trusted sender, usually implemented through digital certificates or message authentication codes (MACs).

Updateable via consensus

- Finally, **the most critical attribute of a blockchain is that it is updateable only via consensus**. This is what gives it the power of decentralization.
- In this scenario, no central authority is in control of updating the ledger. Instead, any update made to the blockchain is validated against strict criteria defined by the blockchain protocol and added to the blockchain only after a consensus has been reached among all participating peers/nodes on the network.
- **To achieve consensus, there are various consensus facilitation algorithms which ensure that all parties are in agreement about the final state of the data on the blockchain network and resolutely agree upon it to be true.**

The network view of a blockchain

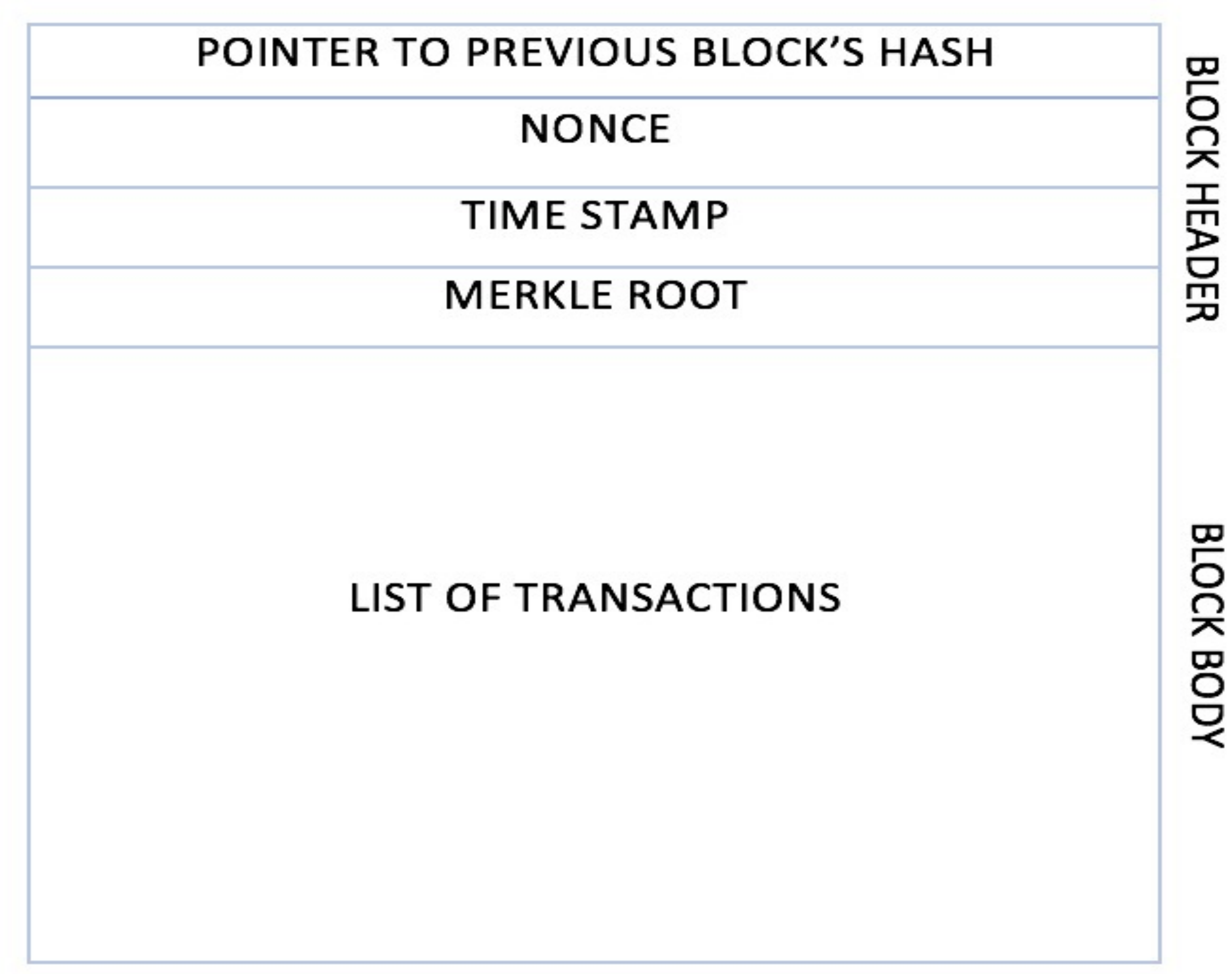


Elements of block chain

- Address
- Transaction
- Block
- Peer-to-peer network
- Scripting or programming language
- Virtual machine
- State machine
- Node
- Smart contract

- Scripts or programs perform various operations on a transaction in order to facilitate various functions. For example, in Bitcoin, transaction scripts are predefined in a language called Script, which consist of sets of commands that allow nodes to transfer tokens from one address to another.

The generic structure of a block



POINTER TO PREVIOUS BLOCK'S HASH

NONCE

TIME STAMP

MERKLE ROOT

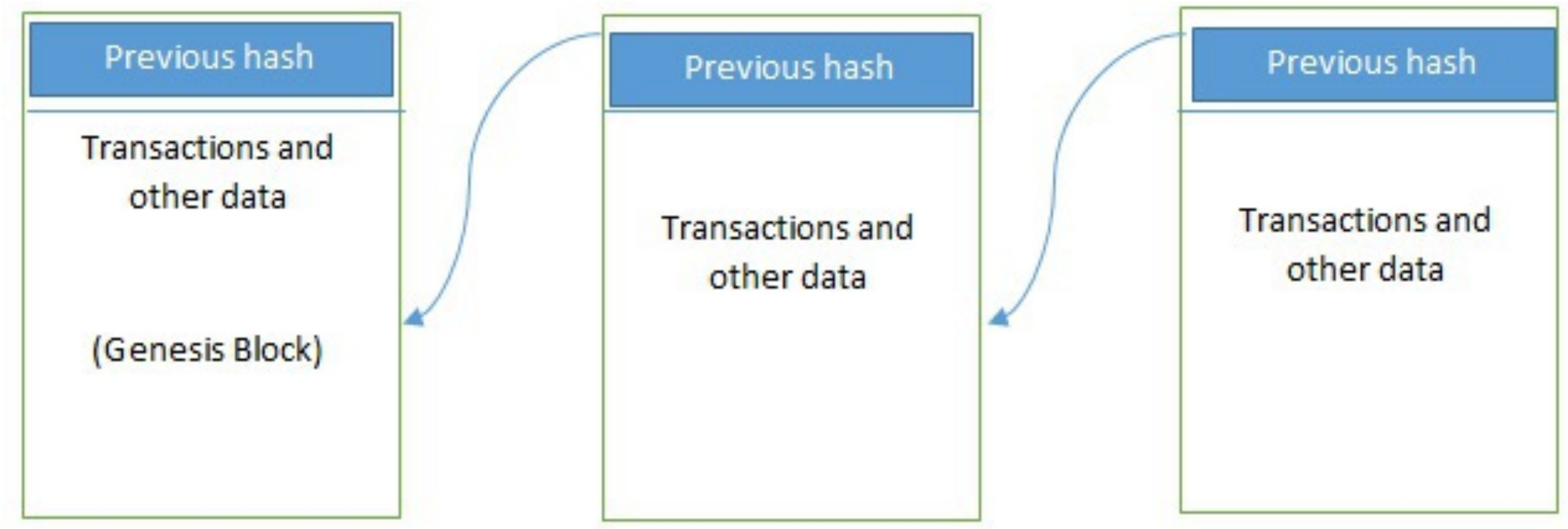
LIST OF TRANSACTIONS

BLOCK HEADER

BLOCK BODY

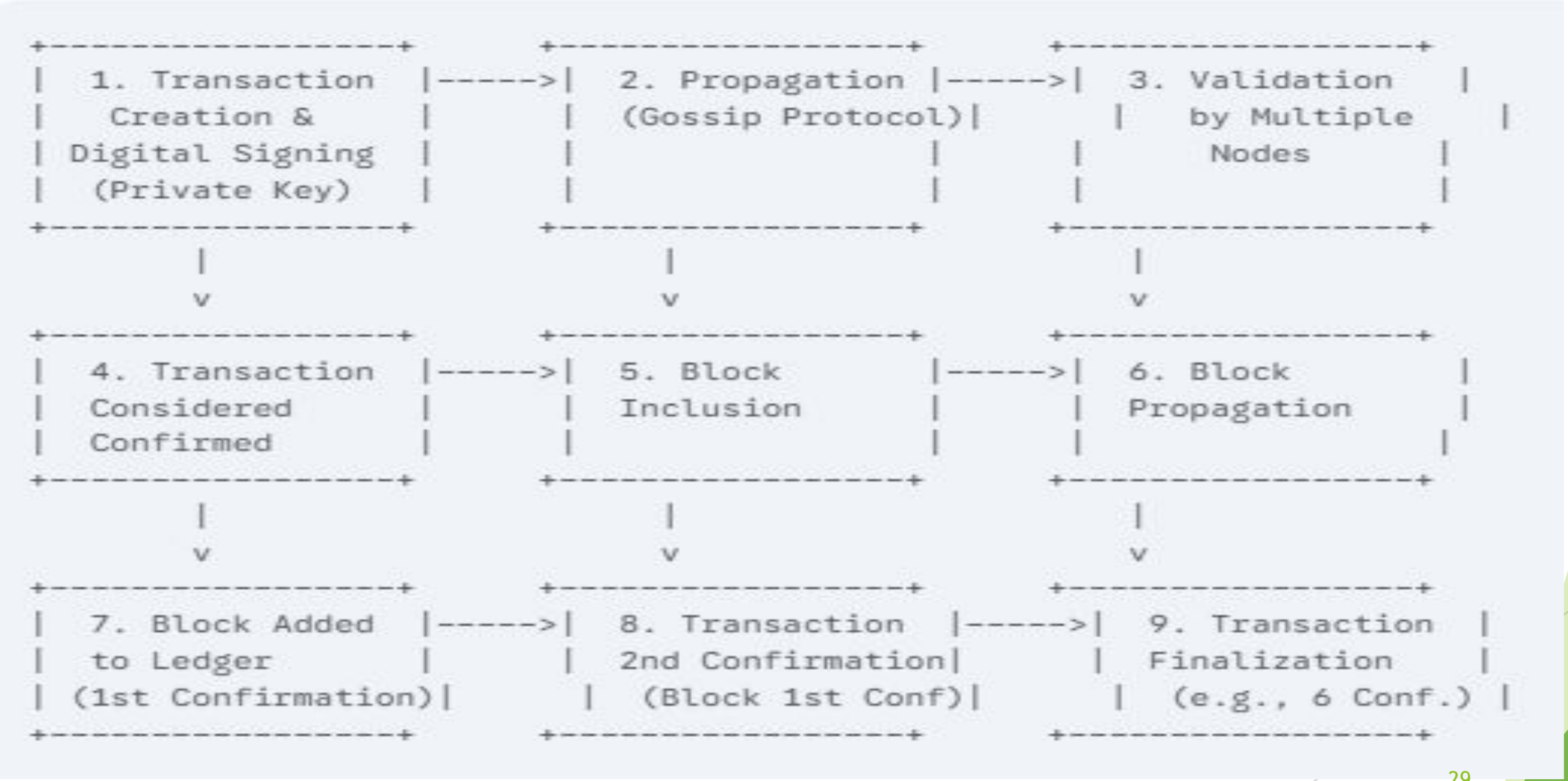
Pointer to Previous Block's Hash: Links blocks together, ensuring the chain is tamper-proof.
Nonce: A number used by miners to find a valid block hash in Proof of Work systems.
Merkle Root: The cryptographic hash representing all the transactions in the block, ensuring secure verification.
Timestamp: The exact time the block was mined, establishing the order of the blockchain.
List of Transactions: Contains the actual data (like payments or contracts) recorded in the block

Generic elements of a blockchain


Previous hash
Transactions and other data
(Genesis Block)
Previous hash
Transactions and other data
Previous hash
Transactions and other data

How blockchain accumulates blocks

1. A node starts a transaction by first creating and then **digitally signing** it with its private key.
2. A transaction is propagated (flooded) by using a flooding protocol, called **Gossip protocol**, to peers that validate the transaction based on preset criteria. Usually, more than one node are required to verify the transaction.
3. Once the transaction is **validated**, it is included in a block, which is then **propagated onto the network**. At this point, the transaction is considered confirmed.
4. The newly-created block now becomes part of the ledger, and the next block links itself cryptographically back to this block. This link is a hash pointer. At this stage, the transaction gets its second confirmation and the block gets its first confirmation.
5. Transactions are then reconfirmed every time a new block is created. Usually, six confirmations in the Bitcoin network are required to consider the transaction final.



```
+------------------+      +------------------+      +------------------+
|  1. Transaction  |----->|  2. Propagation  |----->|  3. Validation   |
|   Creation &     |      | (Gossip Protocol)|      |   by Multiple    |
| Digital Signing  |      |                  |      |     Nodes        |
|  (Private Key)   |      |                  |      |                  |
+------------------+      +------------------+      +------------------+
        |                         |                         |
        v                         v                         v
+------------------+      +------------------+      +------------------+
|  4. Transaction  |----->|  5. Block        |----->|  6. Block        |
|  Considered      |      |  Inclusion       |      |  Propagation     |
|  Confirmed       |      |                  |      |                  |
+------------------+      +------------------+      +------------------+
        |                         |                         |
        v                         v                         v
+------------------+      +------------------+      +------------------+
|  7. Block Added  |----->|  8. Transaction  |----->|  9. Transaction  |
|  to Ledger       |      |  2nd Confirmation|      |  Finalization    |
| (1st Confirmation)|     |  (Block 1st Conf)|      |  (e.g., 6 Conf.) |
+------------------+      +------------------+      +------------------+
```

The history of Blockchain

- Blockchain was introduced with the invention of Bitcoin in 2008. Its practical implementation then occurred in 2009.

Electronic cash

Since the 1980s, e-cash protocols have existed that are based on a model proposed by David Chaum.

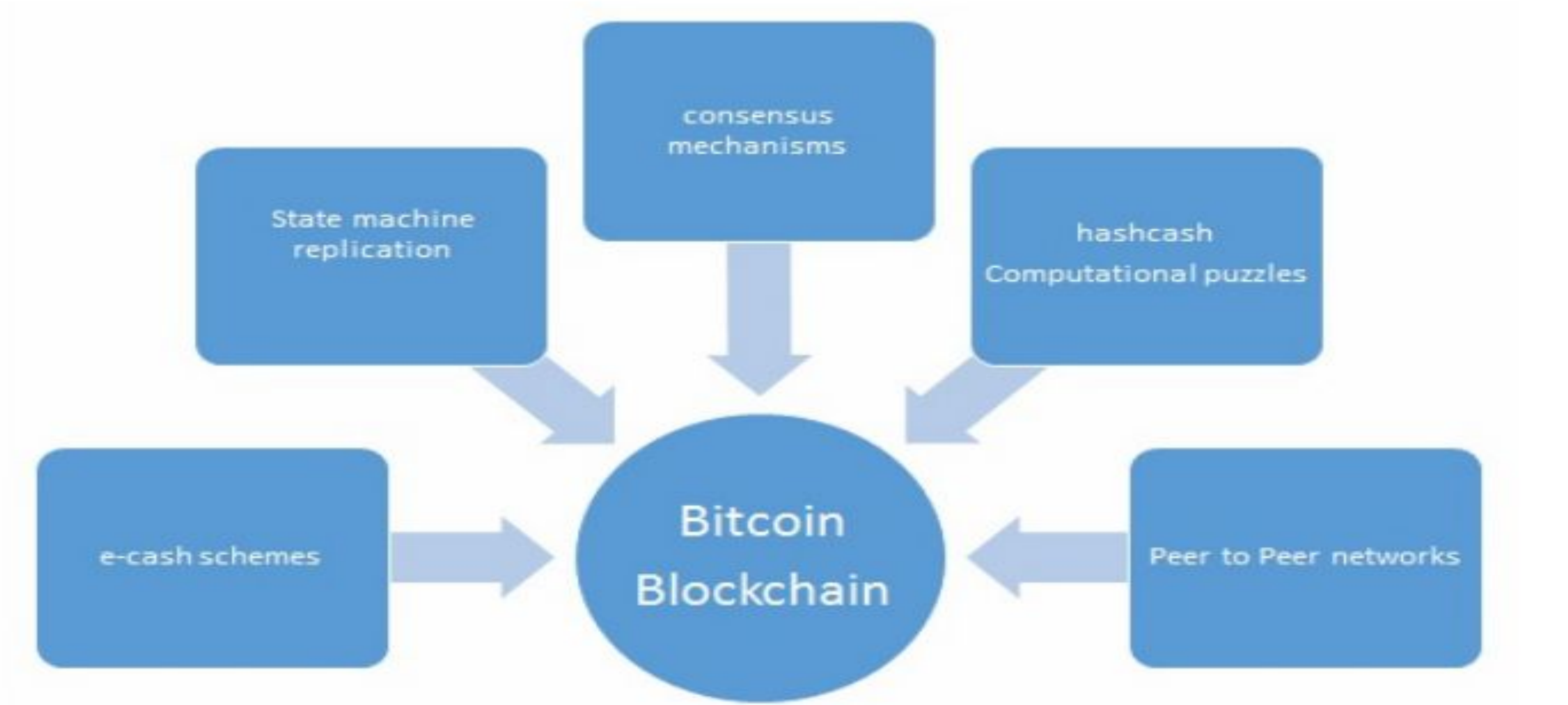
The idea of electronic cash is essential in order to appreciate the first and astonishingly successful application of blockchain, Bitcoin, or more broadly cryptocurrencies in general.

- Two fundamental e-cash system issues need to be addressed: **accountability and anonymity**
- **Accountability is required to ensure that cash is spendable only once** (double-spend problem) and that it can only be spent by its rightful owner.
- Double spend problem arises when same money can be spent twice. As it is quite easy to make copies of digital data, this becomes a big issue in digital currencies as you can make many copies of same digital cash

- **Anonymity is required to protect users' privacy.** As with physical cash, it is almost impossible to trace back spending to the individual who actually paid the money.
- David Chaum solved both of these problems during his work in 1980s by using two cryptographic operations, namely **blind signatures and secret sharing.**
- Blind signatures allow for signing a document without actually seeing it, and secret sharing is a concept that enables the detection of double spending, that is using the same e-cash token twice (double spending)

- In 2009, the first practical implementation of an electronic cash (e-cash) system named Bitcoin appeared. The term cryptocurrency emerged later.
- For the very first time, it solved the problem of distributed consensus in a trustless network. It used public key cryptography with a Proof of Work (PoW) mechanism to provide a secure, controlled, and decentralized method of minting digital currency.
- The key innovation was the idea of an ordered list of blocks composed of transactions and cryptographically secured by the PoW mechanism.

- Concepts from electronic cash schemes and distributed systems were combined to create Bitcoin and what now is known as blockchain.
- In 2008, a groundbreaking paper entitled Bitcoin: A Peer-to-Peer Electronic Cash System was written on the topic of peer-to-peer electronic cash under the pseudonym Satoshi Nakamoto.
- It introduced the term chain of blocks



State machine replication

consensus mechanisms

hashcash Computational puzzles

e-cash schemes

Bitcoin Blockchain

Peer to Peer networks

Benefits of blockchain technology

1. Decentralization
2. Transparency and Trust
3. Immutability
4. High availability
5. Highly secure
6. Simplification of current paradigms
7. Faster dealings
8. Cost Saving

Limitations of blockchain

1. Scalability
2. Adaptability
3. Regulation
4. Relatively immature technology
5. Privacy

Tiers of blockchain technology

1. Blockchain 1.0
2. Blockchain 2.0
3. Blockchain 3.0
4. Blockchain X.0

- Blockchain 1.0: This tier was introduced with the invention of **Bitcoin, and it is primarily used for cryptocurrencies**. Also, as Bitcoin was the first implementation of cryptocurrencies, it makes sense to categorize this first generation of blockchain technology to include only cryptographic currencies.
- This generation started in 2009 when Bitcoin was released and ended in early 2010.

- Blockchain 2.0: This second blockchain generation is used by **financial services and smart contracts**. This tier includes various financial assets, such as derivatives, options, swaps, and bonds. Applications that go beyond currency, finance, and markets are incorporated at this tier. Ethereum, Hyperledger, and other newer blockchain platforms are considered part of Blockchain 2.0.
- This generation started when ideas related to using blockchain for other purposes started to emerge in 2010.

- Blockchain 3.0: **This third blockchain generation is used to implement applications beyond the financial services industry and is used in government, health, media, the arts, and justice**. Again, as in Blockchain 2.0, Ethereum, Hyperledger, and newer blockchains with the ability to code smart contracts are considered part of this blockchain technology tier.
- This generation of blockchain emerged around 2012 when multiple applications of blockchain technology in different industries were researched.

- Blockchain X.0: This generation represents a vision of blockchain singularity where one day there will be a public blockchain service available that anyone can use just like the Google search engine.

Features of a blockchain

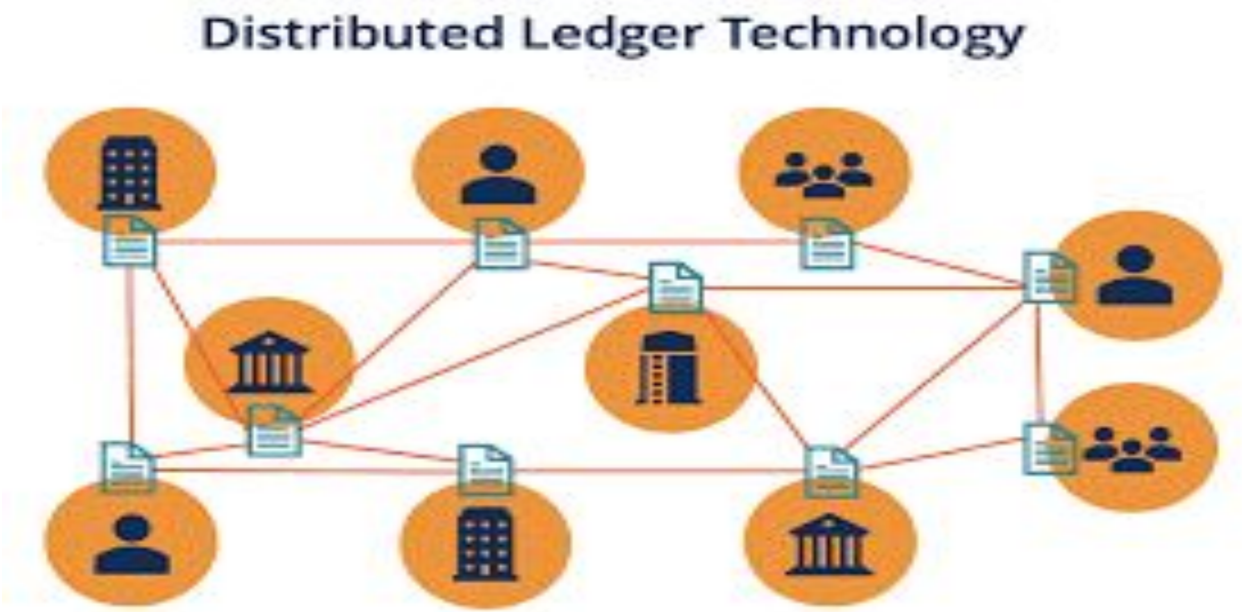
1. Distributed consensus
2. Transaction verification
3. Platform for smart contract
4. Transforming value between peers
5. Generation of cryptocurrency
6. Smart property
7. Provider of security
8. Immutability
9. Uniqueness

Distributed ledgers

- A distributed ledger is a broad term describing shared databases; hence, **all blockchains technically fall under the umbrella of shared databases or distributed ledgers**.
- All blockchains are fundamentally distributed ledgers, all distributed ledgers are not necessarily a blockchain.
- **Distributed ledger does not necessarily consist of blocks of transactions to keep the ledger growing.**
- A blockchain is a special type of shared database that is comprised of blocks of transactions.
- An example of a distributed ledger that does not use blocks of transactions is R3's Corda.

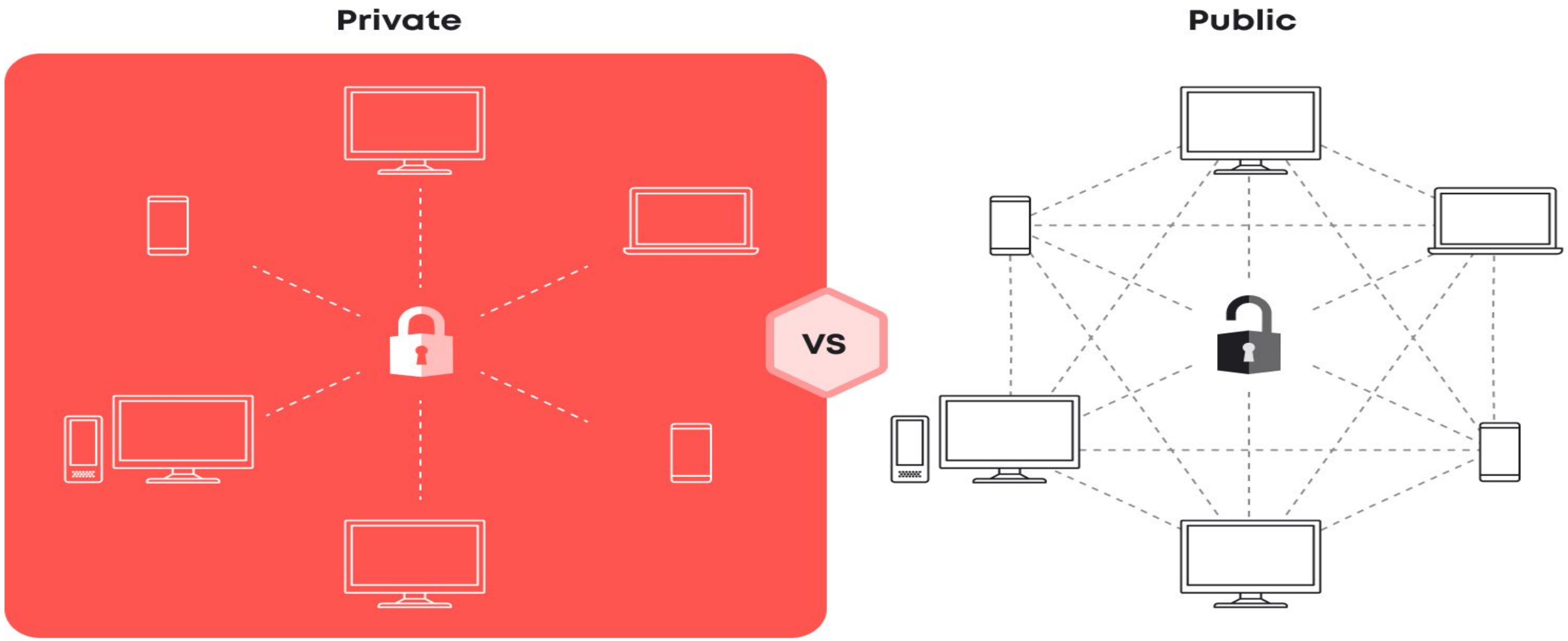
Distributed Ledger

- Corda is a distributed ledger which is developed to record and manage agreements and is especially focused on financial services industry.
- On the other hand, more widely-known blockchains like Bitcoin and Ethereum make use of blocks to update the shared database.


Distributed Ledger Technology

Types of blockchain

1. Public blockchains
2. Private blockchains
3. Semiprivate blockchains
4. Sidechains
5. Permissioned ledger
6. Shared ledger
7. Tokenized blockchains
8. Tokenless blockchains



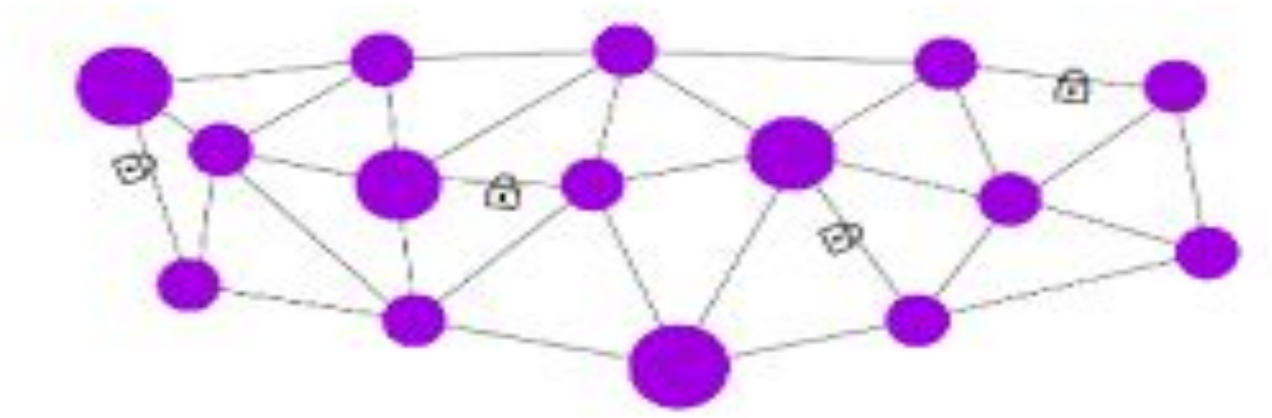
As the name suggests, public blockchains are not owned by anyone. They are open to the public, and anyone can participate as a node in the decision-making process

All users of these permissionless or unpermissioned ledgers maintain a copy of the ledger on their local nodes and use a distributed consensus mechanism to decide the eventual state of the ledger. Bitcoin and Ethereum are both considered public blockchains

- Private blockchain: They are open only to a consortium or group of individuals or organizations who have decided to share the ledger among themselves. There are various blockchains now available in this category, such as HydraChain and Quorum.

With semiprivate blockchains, part of the blockchain is private and part of it is public. With a semi-private blockchain, the private part is controlled by a group of individuals, while the public part is open for participation by anyone.

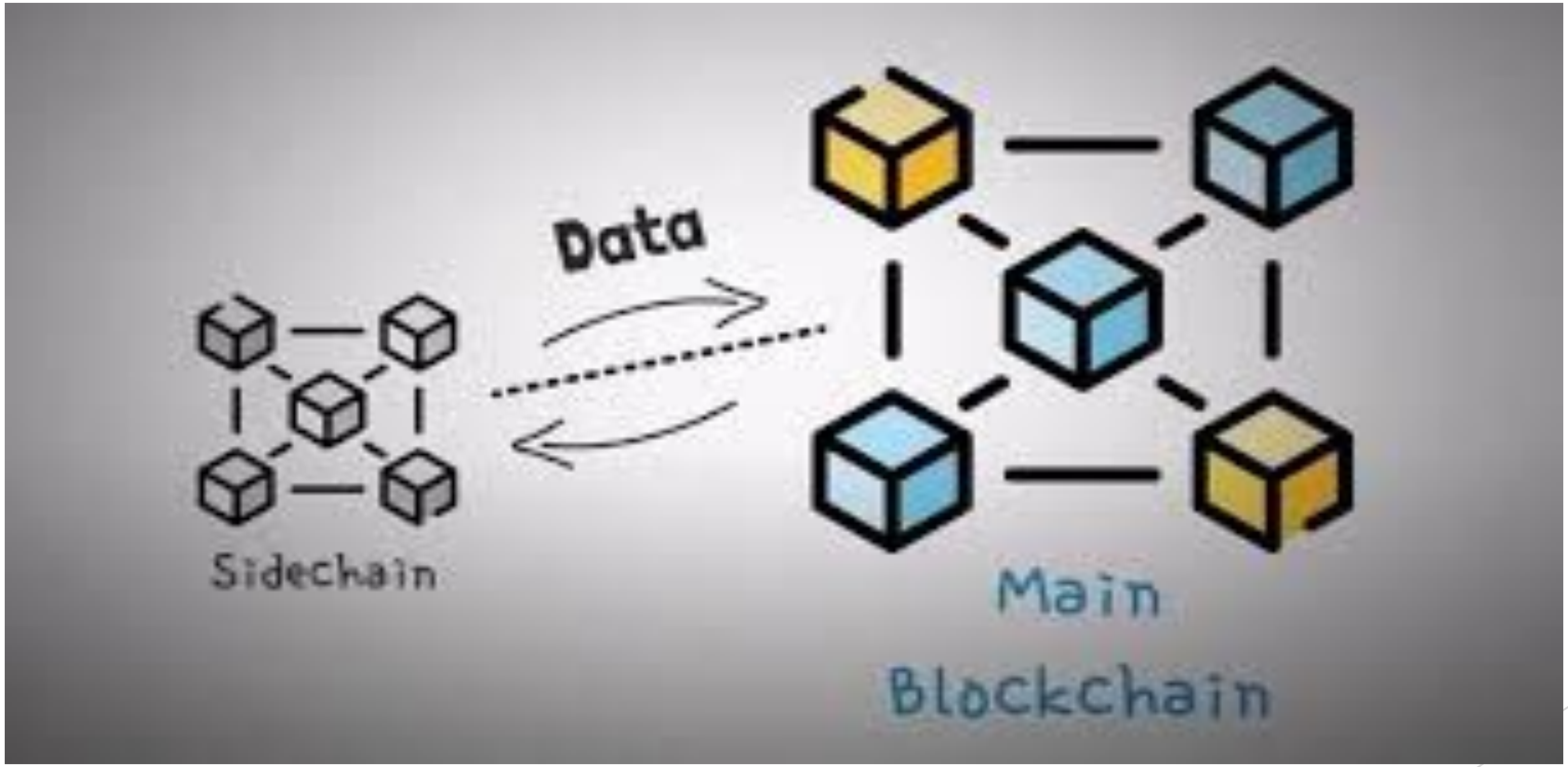
This hybrid model can be used in scenarios where the private part of the blockchain remains internal and shared among known participants, while the public part of the blockchain can still be used by anyone



Semi Private Blockchain

Sidechains

- More precisely known as pegged sidechains, this is a concept whereby coins can be moved from one blockchain to another and moved back again.

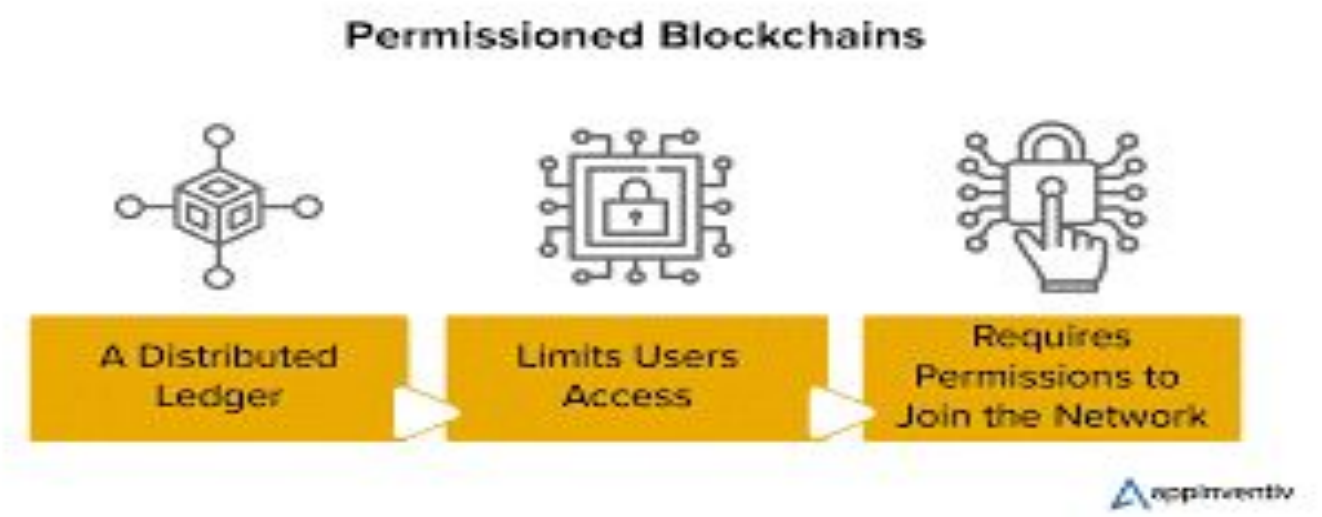


Permissioned ledger

A **permissioned ledger** is a type of distributed ledger where only authorized participants can access and validate transactions.

Unlike permissionless ledgers, where anyone can join, permissioned ledgers restrict access and often offer more privacy and faster consensus mechanisms.

These ledgers are commonly used in industries that require privacy, trust, and regulatory compliance, such as banking and healthcare.



Shared ledger

- This is a generic term that is used to describe any application or database that is shared by the public or a consortium. Generally, all blockchains, fall into the category of a shared ledger.

Tokenized blockchains

- These blockchains are standard blockchains that generate cryptocurrency as a result of a consensus process via mining or initial distribution.
- **Tokenized** refers to systems where assets or rights are represented by digital tokens, which can be traded or transferred on a blockchain or distributed ledger.

Tokenless blockchains

- This is similar to full private blockchains, the only difference being that use of tokens is not required. This can also be thought of as a shared distributed ledger used for storing data.

- **Tokenless** systems, on the other hand, do not use digital tokens to represent assets. Instead, they may rely on traditional methods for verifying transactions or ownership without the need for tokens, often focusing on the direct exchange of data or values

Consensus

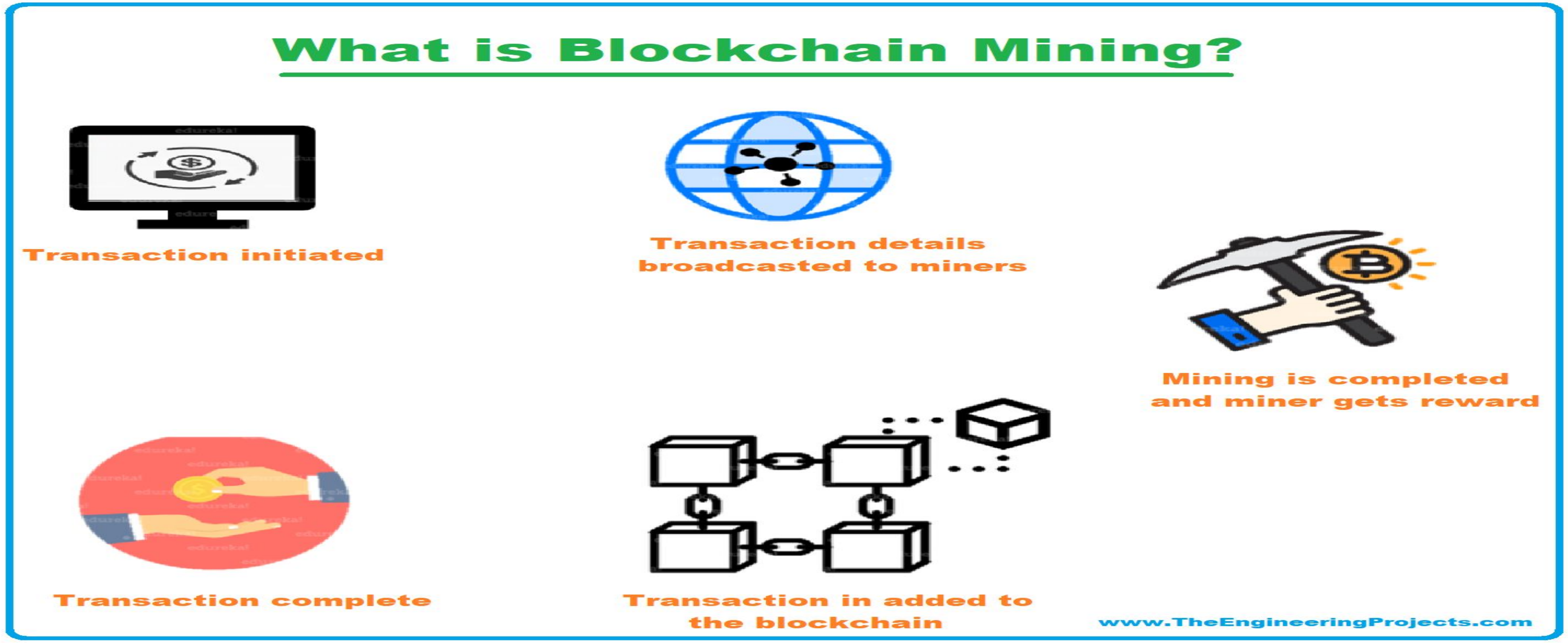
- Consensus is the backbone of a blockchain and, as a result, it provides decentralization of control through an optional process known as **mining.**
- Consensus is a process of agreement between distrusting nodes on the final state of data.
- To achieve consensus, different algorithms are used.
- It is easy to reach an agreement between two nodes (in client-server systems, for example), but **when multiple nodes are participating in a distributed system and they need to agree on a single value, it becomes quite a challenge to achieve consensus**.
- This process of attaining agreement common state or value among multiple nodes despite the failure of some nodes is known as **distributed consensus.**

Bitcoin Mining

['bit-ˌkoin mī-niŋ]

The process of verifying transactions on the Bitcoin blockchain by solving mathematical puzzles, for which miners are rewarded with new bitcoin.

Investopedia



What is Blockchain Mining?

Transaction initiated

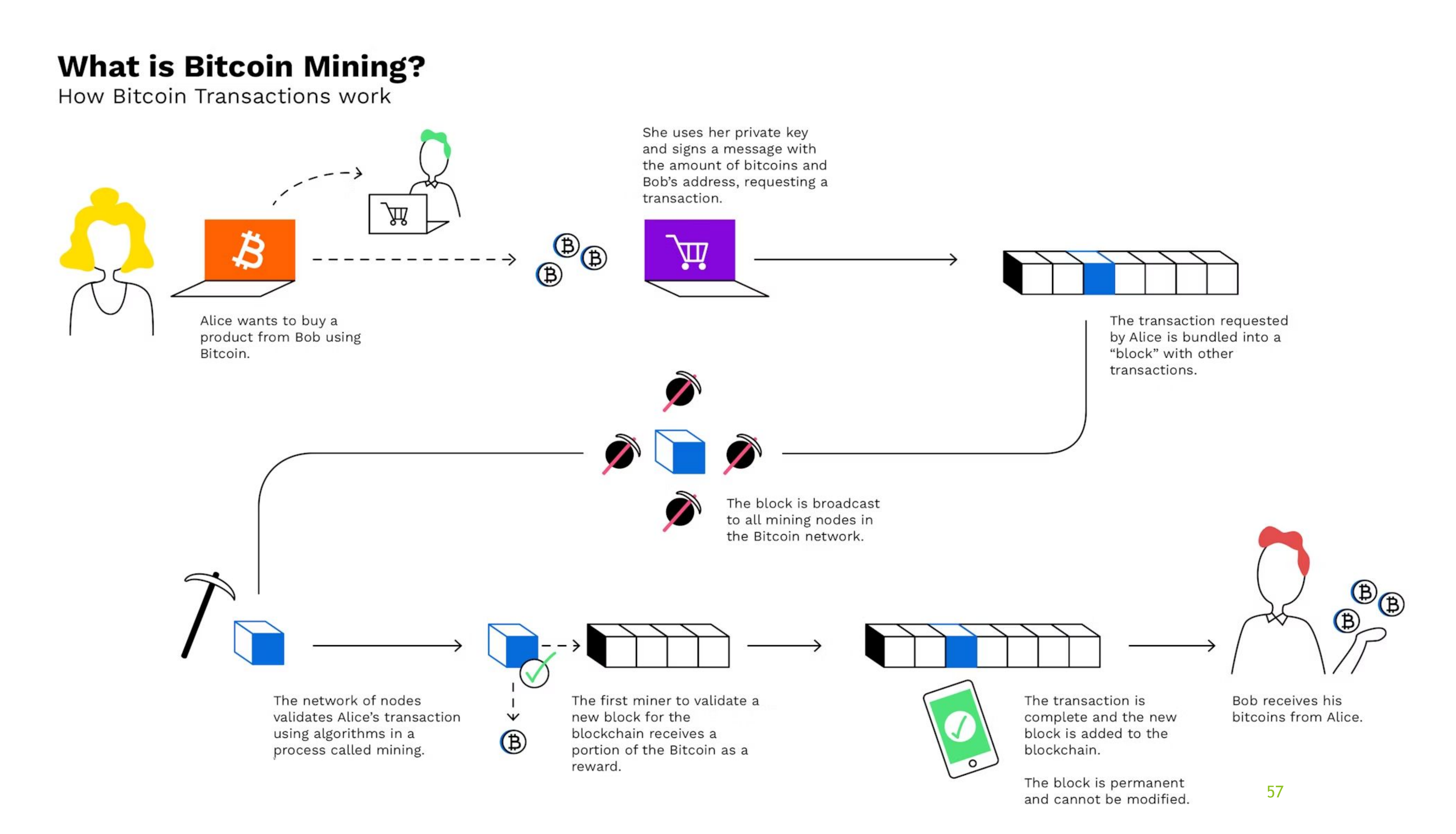
Transaction details broadcasted to miners

Mining is completed and miner gets reward

Transaction in added to the blockchain

Transaction complete

www.TheEngineeringProjects.com



What is Bitcoin Mining?

How Bitcoin Transactions work

Alice wants to buy a product from Bob using Bitcoin.

She uses her private key and signs a message with the amount of bitcoins and Bob's address, requesting a transaction.

The transaction requested by Alice is bundled into a "block" with other transactions.

The block is broadcast to all mining nodes in the Bitcoin network.

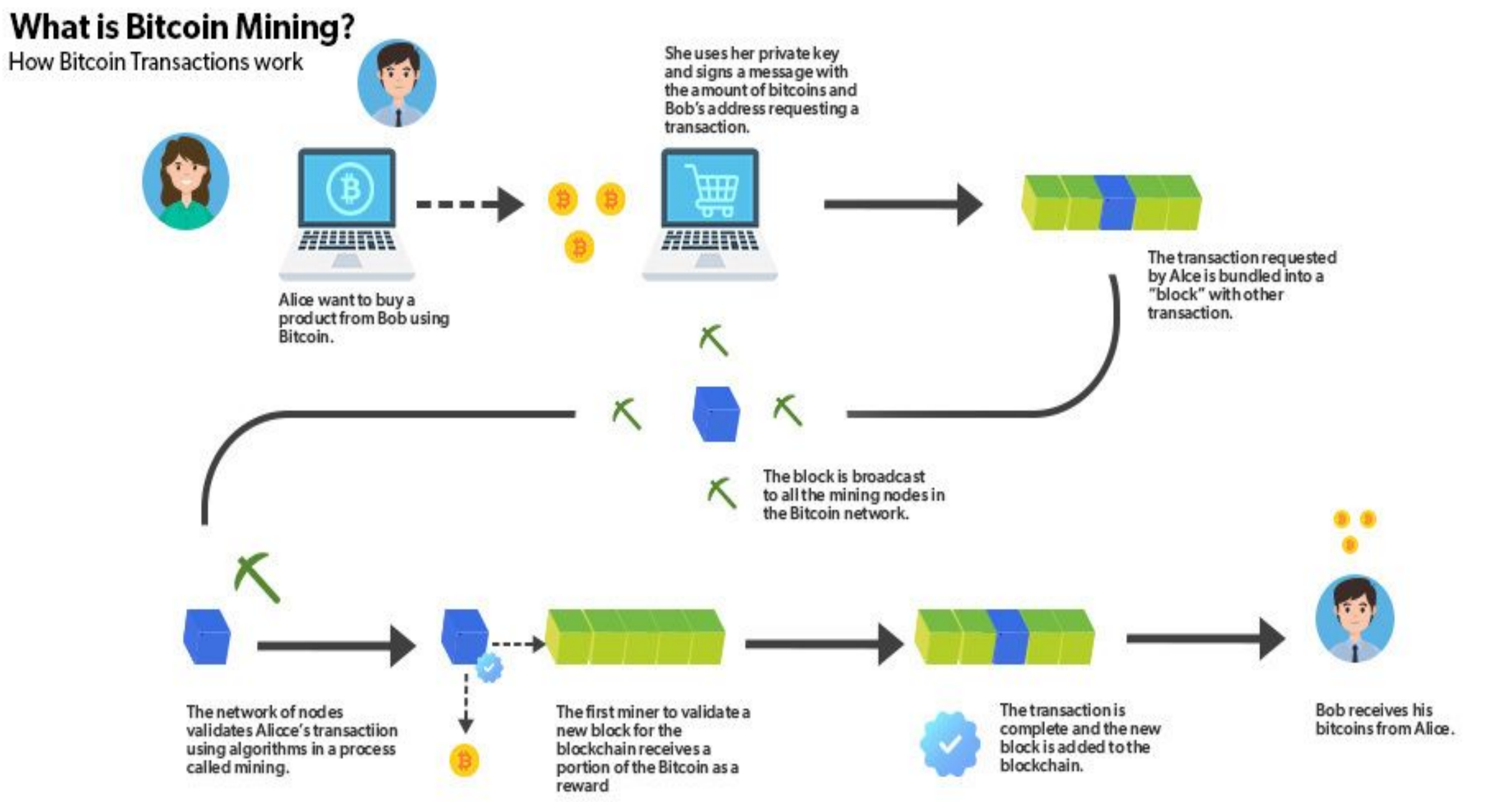
The network of nodes validates Alice's transaction using algorithms in a process called mining.

The first miner to validate a new block for the blockchain receives a portion of the Bitcoin as a reward.

The transaction is complete and the new block is added to the blockchain.

The block is permanent and cannot be modified.

Bob receives his bitcoins from Alice.



What is Bitcoin Mining?

How Bitcoin Transactions work

Alice want to buy a product from Bob using Bitcoin.

She uses her private key and signs a message with the amount of bitcoins and Bob's address requesting a transaction.

The transaction requested by Alce is bundled into a "block" with other transaction.

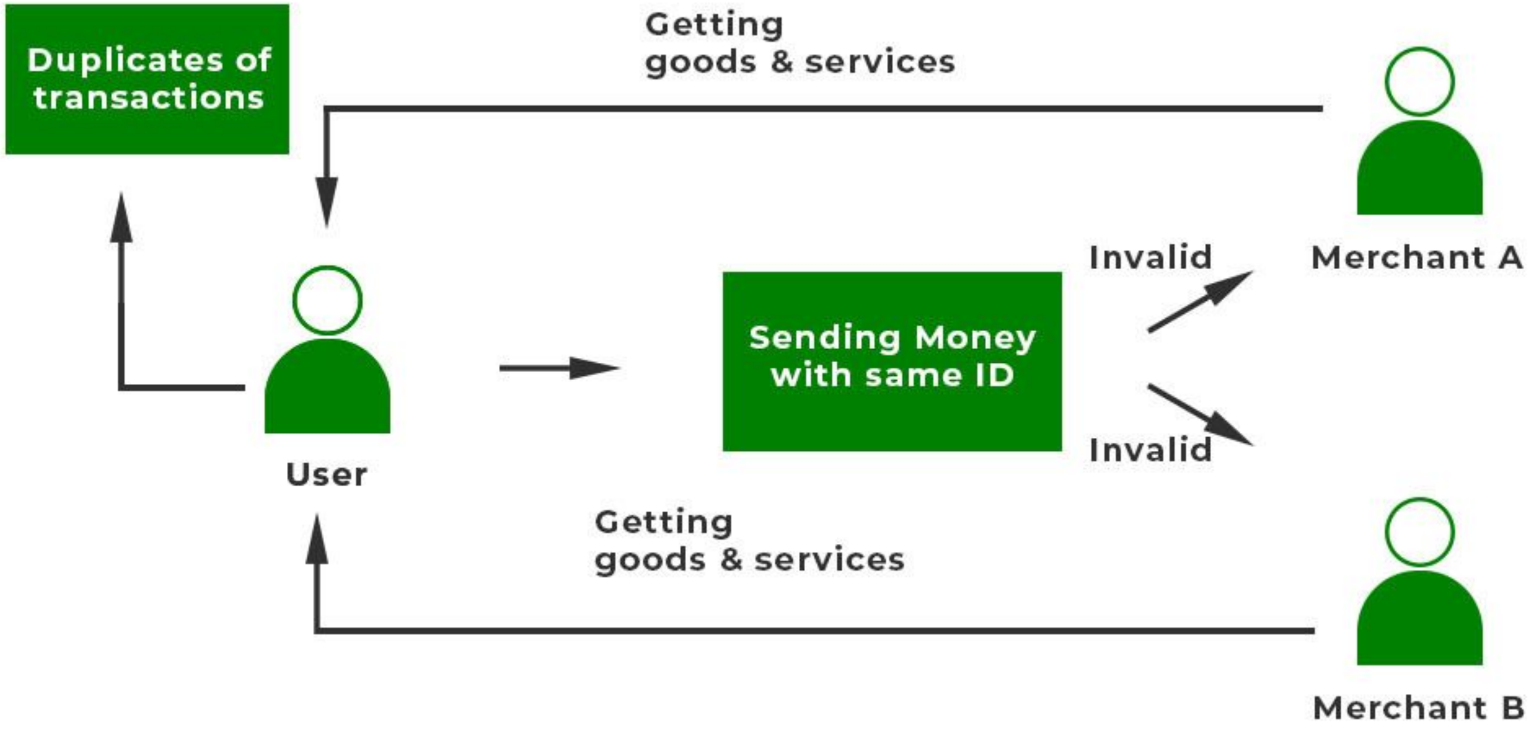
The block is broadcast to all the mining nodes in the Bitcoin network.

The network of nodes validates Alicce's transactiion using algorithms in a process called mining.

The first miner to validate a new block for the blockchain receives a portion of the Bitcoin as a reward

The transaction is complete and the new block is added to the blockchain.

Bob receives his bitcoins from Alice.


Duplicates of transactions
Getting goods & services
Merchant A
Invalid
Sending Money with same ID
Invalid
User
Getting goods & services
Merchant B

Consensus mechanism

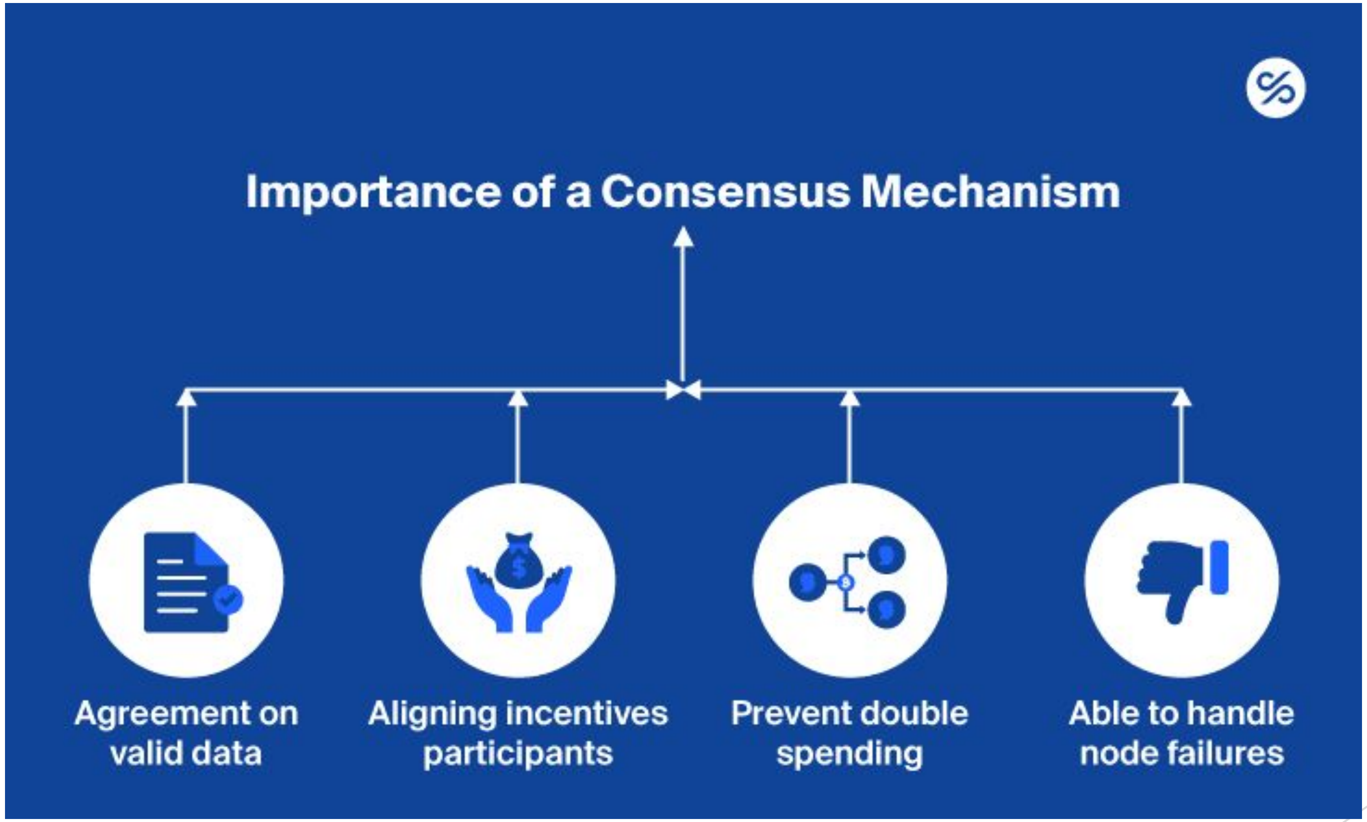
1. **Agreement:** All honest nodes decide on the same value
2. **Termination:** The consensus process must eventually end with a decision, and every honest node must reach that conclusion.
3. **Validity:** The decision made by the honest nodes must be based on something that was initially proposed by a real, honest participant.
4. **Fault tolerant:** The consensus algorithm should be able to run in the presence of faulty or malicious nodes (Byzantine nodes)
5. **Integrity:** This is a requirement that no node can make the decision more than once in a single consensus cycle

Consensus Mechanism

[kən-ˈsen(t)-səs ˈme-kə-ˌni-zəm]

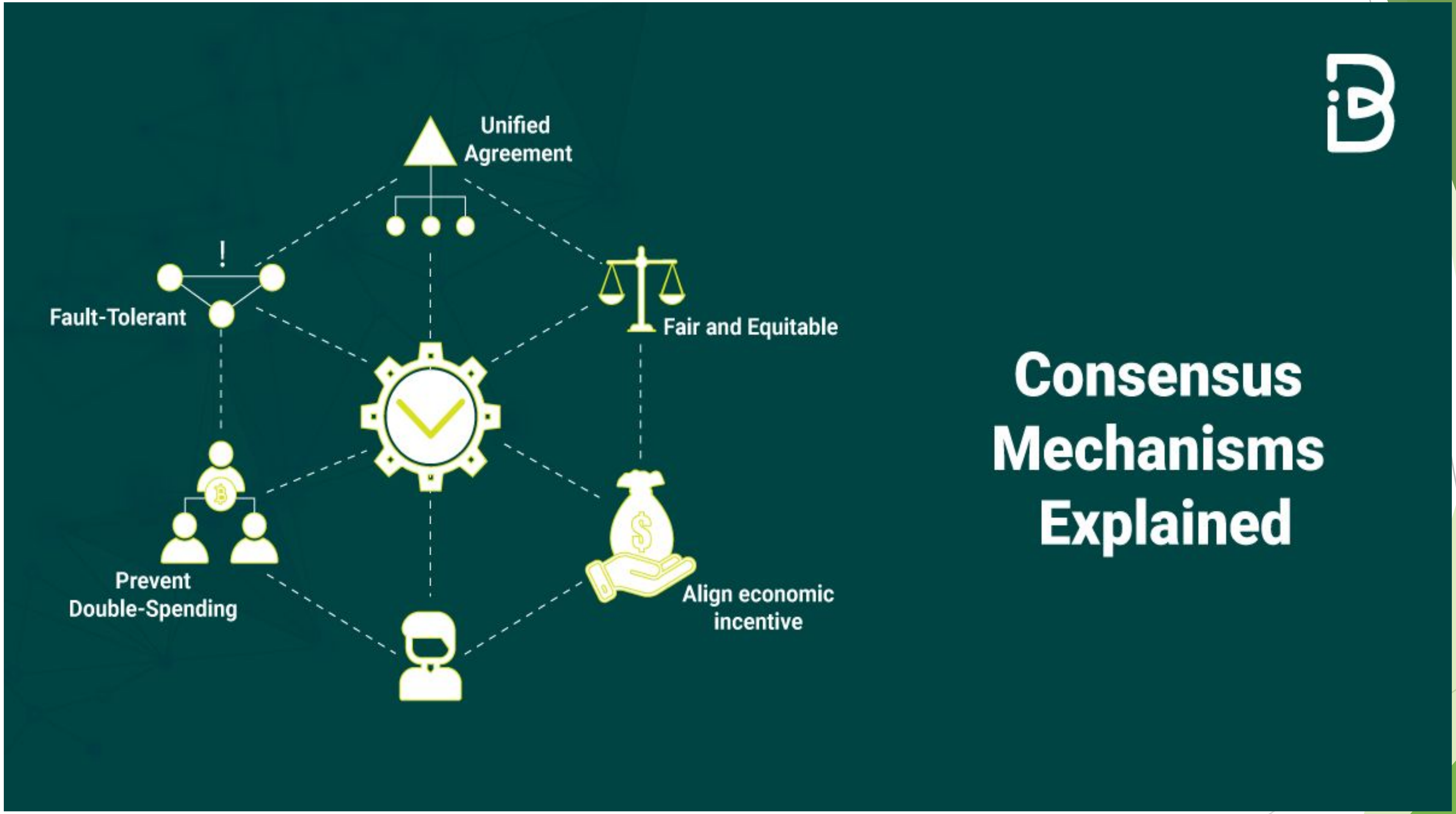
A program used in blockchain systems to achieve distributed agreement about the ledger's state.

Investopedia



Importance of a Consensus Mechanism

- Agreement on valid data
- Aligning incentives participants
- Prevent double spending
- Able to handle node failures

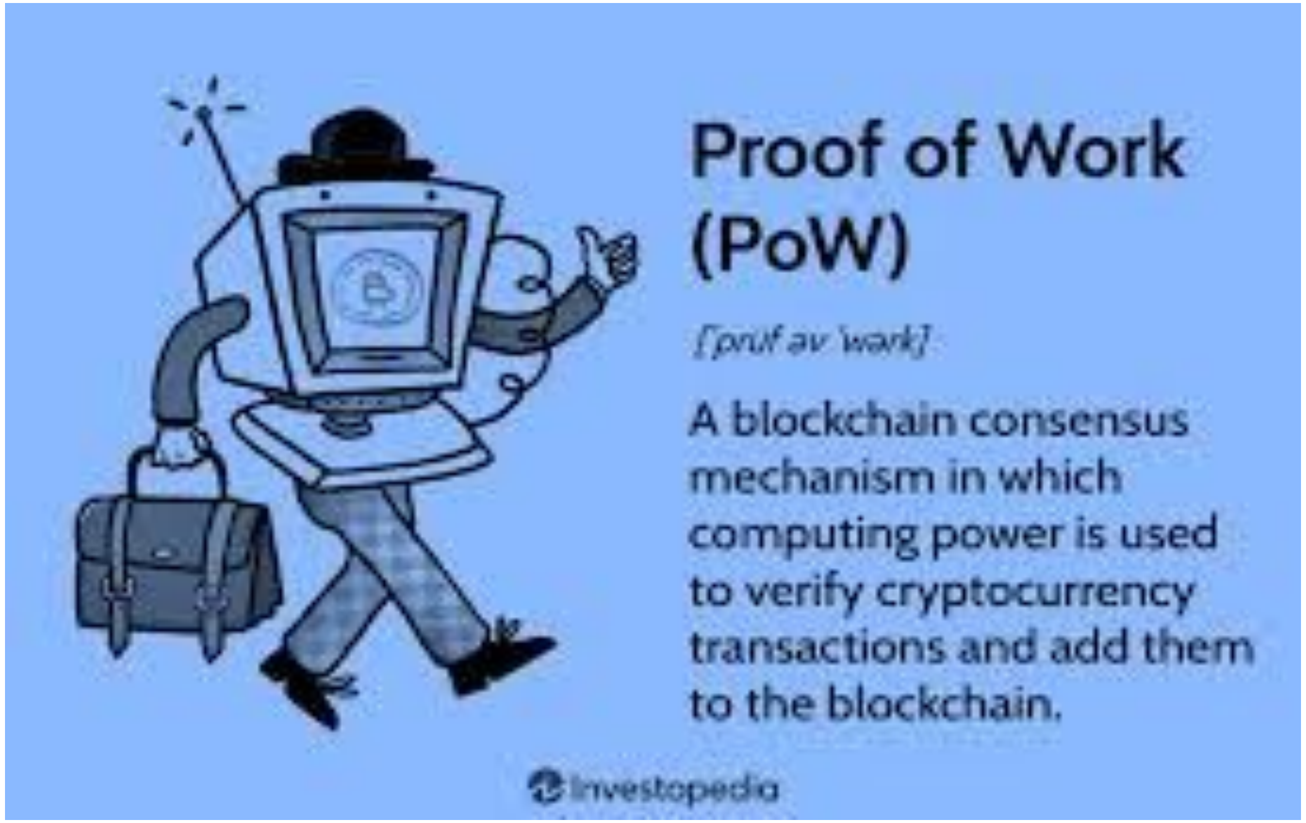


Consensus Mechanisms Explained

Types of consensus mechanisms

- All consensus mechanisms are developed to deal with faults in a distributed system and to allow distributed systems to reach a final state of agreement.
- There are two general categories of consensus mechanisms. These categories deal with all types of faults:

- **Traditional Byzantine Fault Tolerance (BFT)-based:** With no compute-intensive operations, such as partial hash inversion (as in Bitcoin PoW), this method relies on a simple scheme of nodes that are **publisher-signed messages**. Eventually, when a certain number of messages are received, then an agreement is reached.
- **Leader election-based consensus mechanisms**: This arrangement requires nodes to compete in a leader election lottery, and the node that wins proposes a final value. For example, the PoW used in Bitcoin falls into this category.

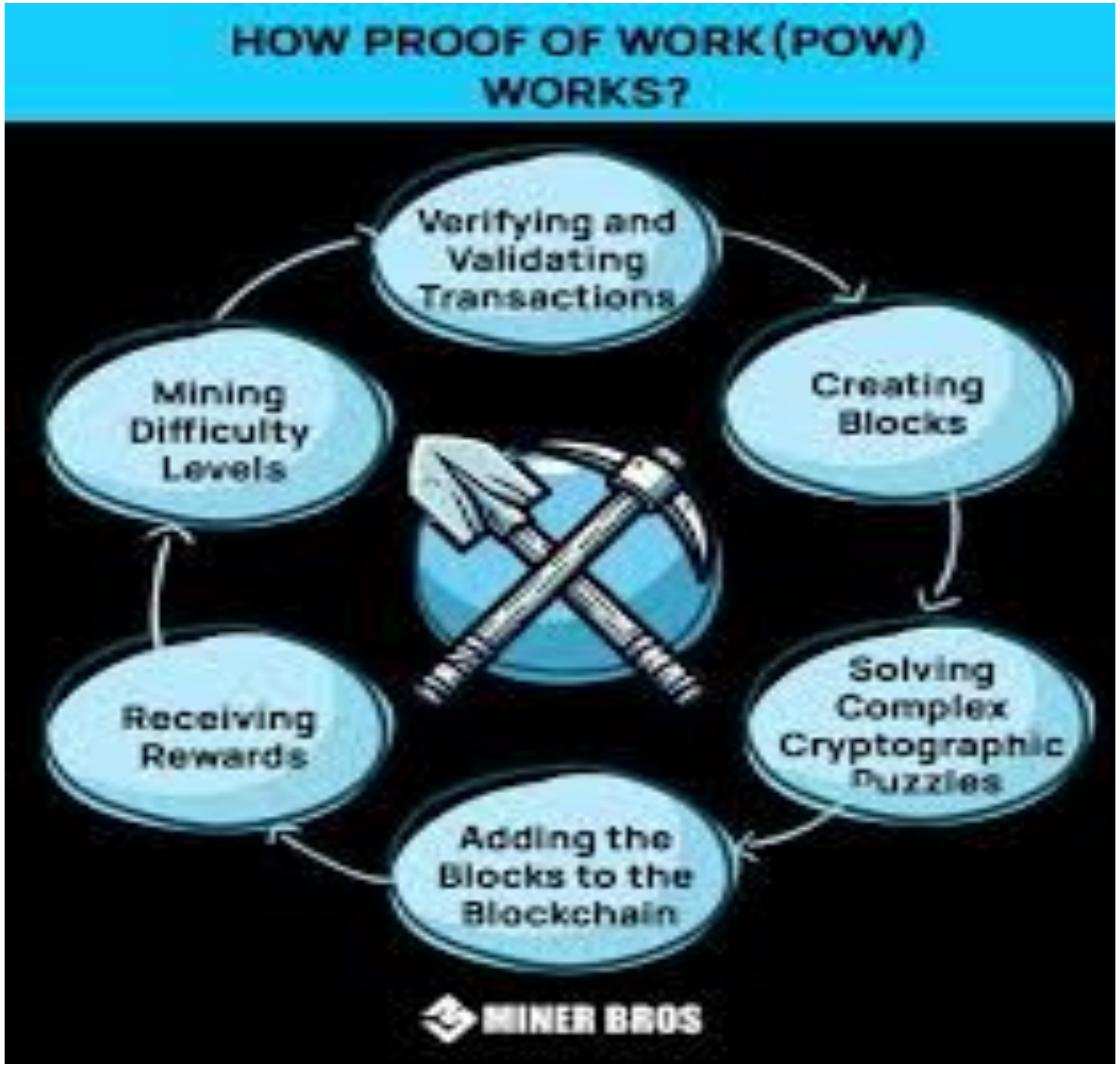


Proof of Work (PoW)

[ˈprüf əv ˈwərk]

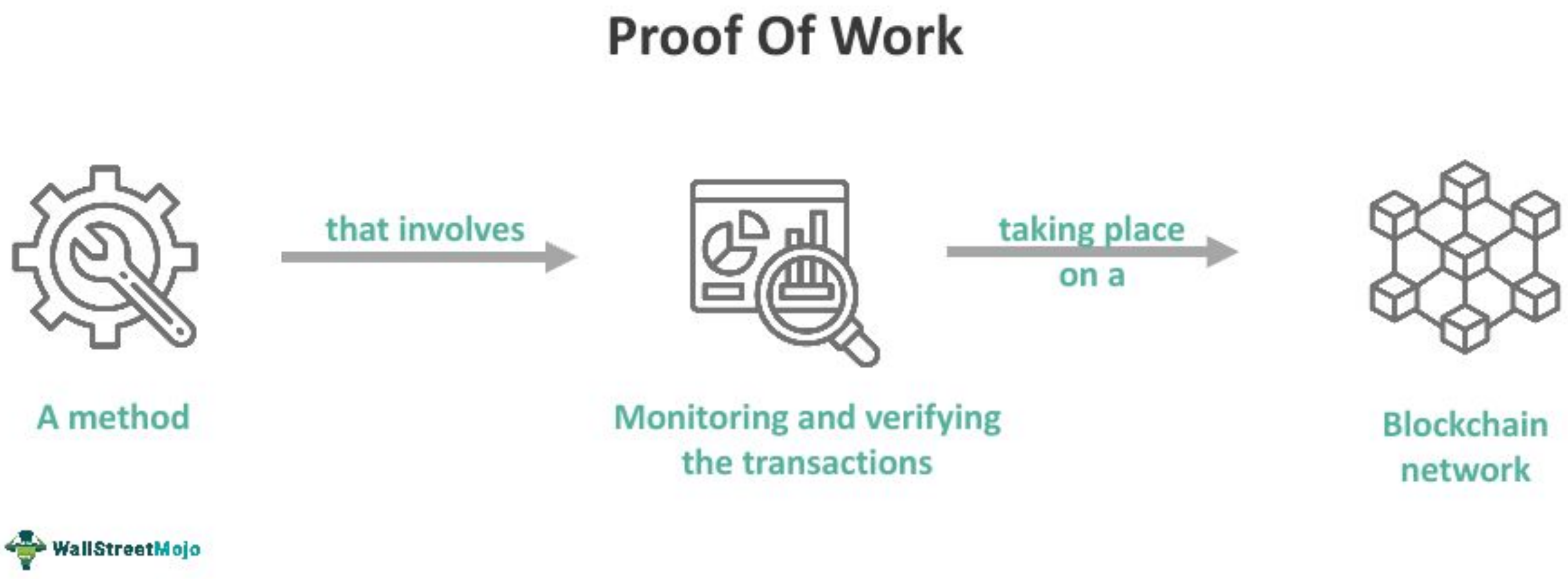
A blockchain consensus mechanism in which computing power is used to verify cryptocurrency transactions and add them to the blockchain.

Investopedia



HOW PROOF OF WORK (POW) WORKS?

Verifying and Validating Transactions
Creating Blocks
Solving Complex Cryptographic Puzzles
Adding the Blocks to the Blockchain
Receiving Rewards
Mining Difficulty Levels
MINER BROS



Proof Of Work

A method

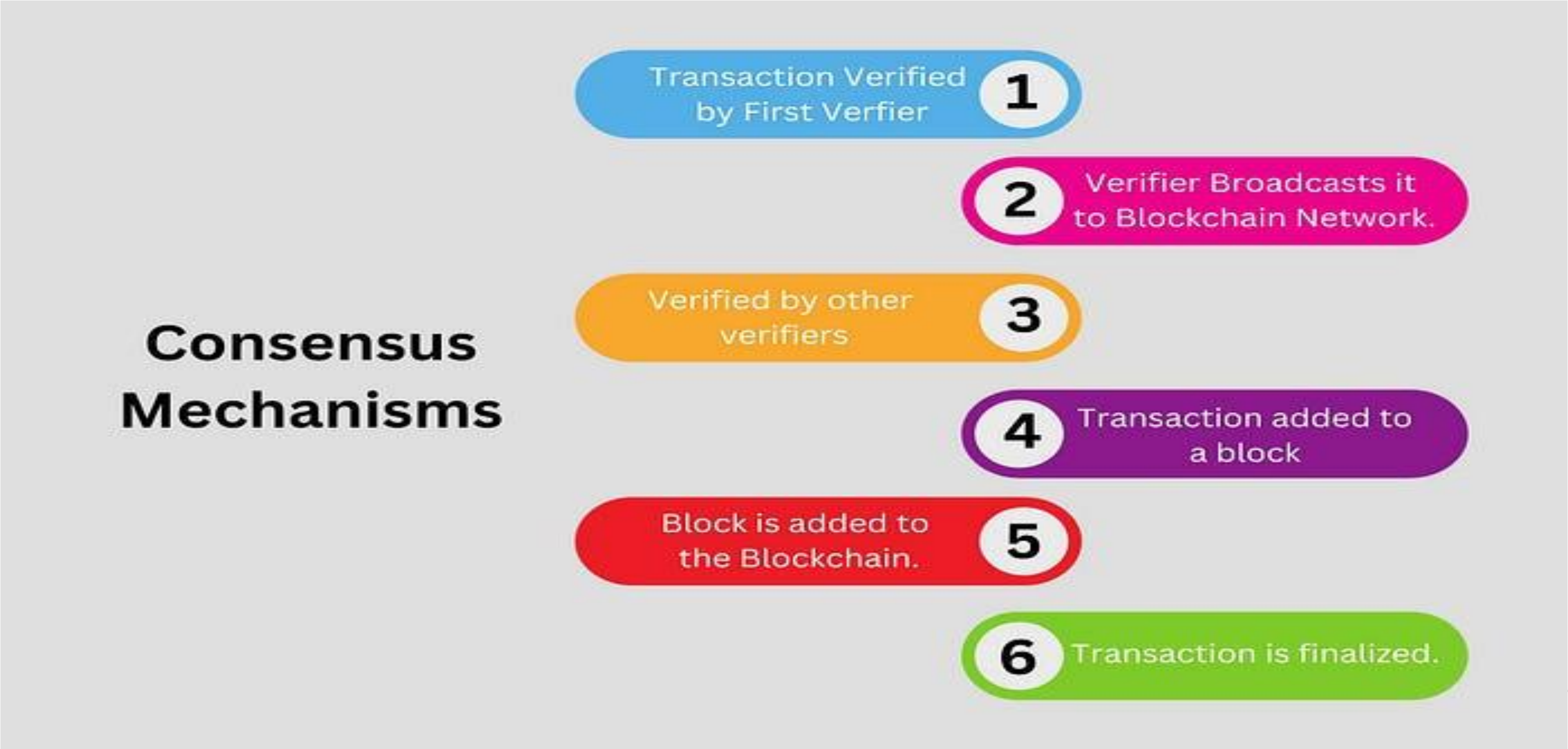
that involves

Monitoring and verifying the transactions

taking place on a

Blockchain network

WallStreetMojo



Consensus Mechanisms

1 Transaction Verified by First Verfier

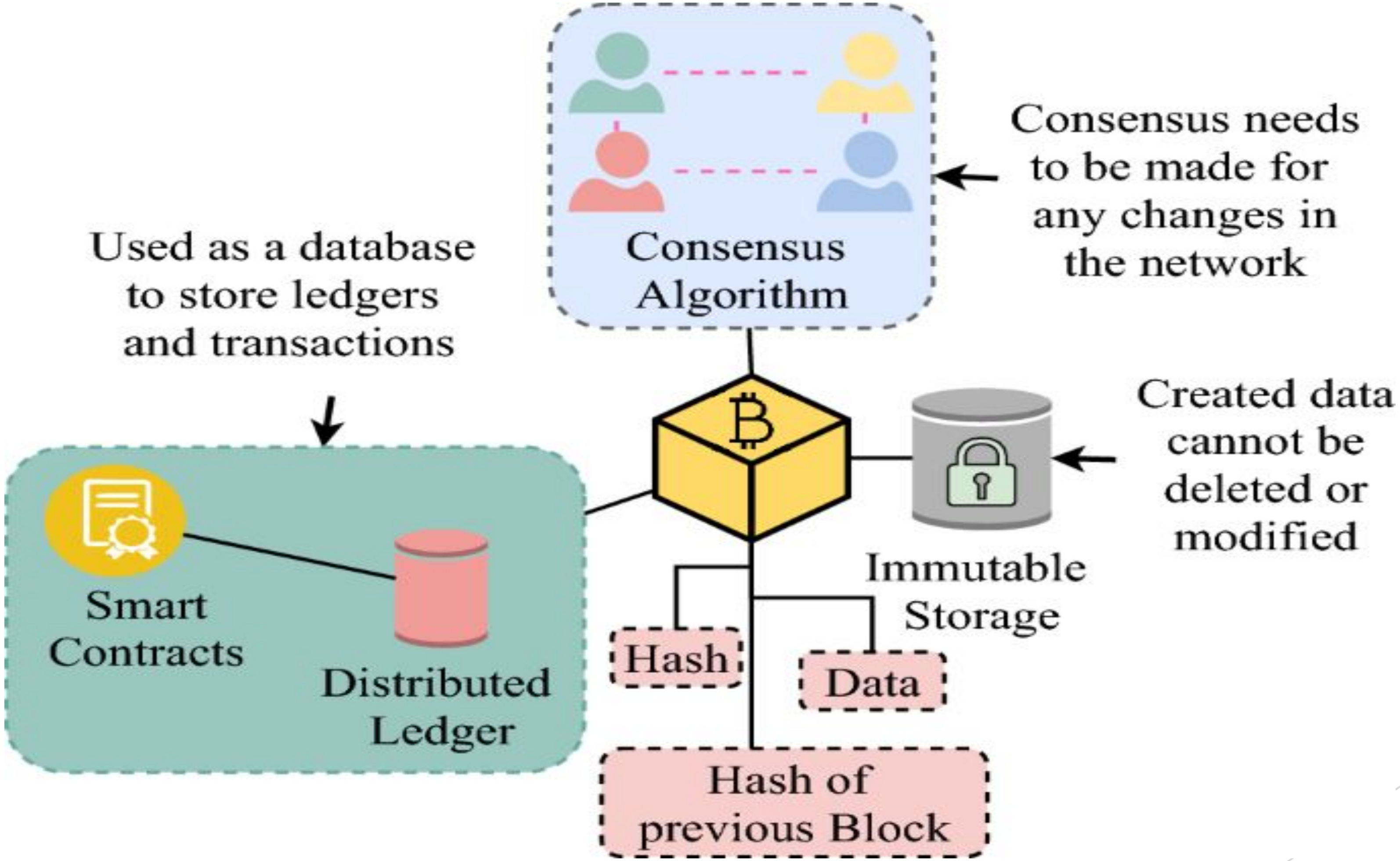
2 Verifier Broadcasts it to Blockchain Network.

3 Verified by other verifiers

4 Transaction added to a block

5 Block is added to the Blockchain.

6 Transaction is finalized.

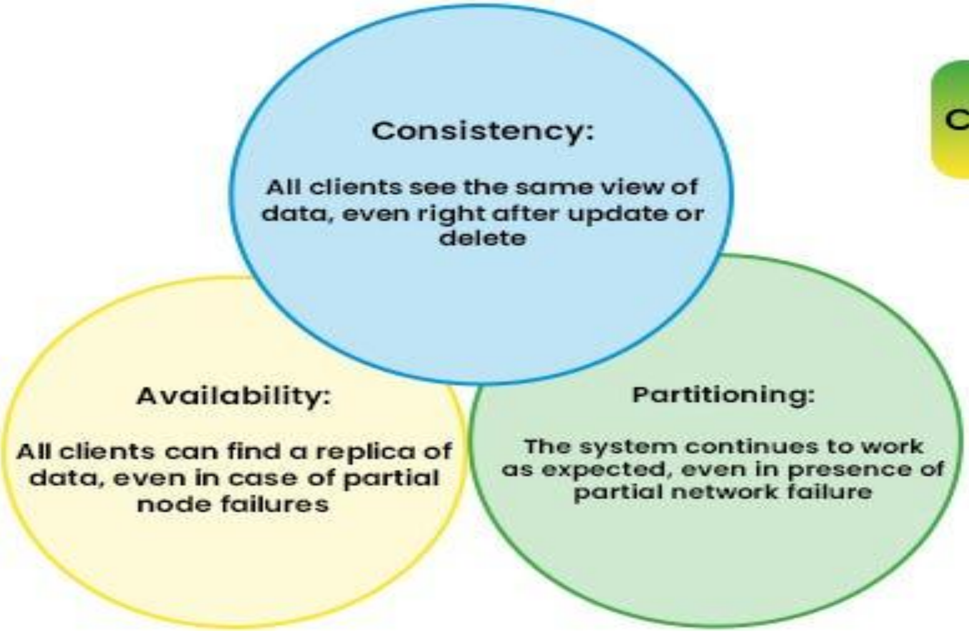

Consensus Algorithm
Consensus needs to be made for any changes in the network
Used as a database to store ledgers and transactions
Smart Contracts
Distributed Ledger
₿
Immutable Storage
Created data cannot be deleted or modified
Hash
Data
Hash of previous Block

CAP theorem and blockchain

- The theory states that any distributed system cannot have consistency, availability, and partition tolerance simultaneously:

1. **Consistency** is a property which ensures that all nodes in a distributed system have a **single, current, and identical copy of the data.**
2. **Availability:** data **is available at each node** and the nodes are responding to requests.
3. **Partition tolerance** ensures that if a group of nodes is unable to communicate with other nodes **due to network failures, the distributed system continues to operate correctly**. This can occur due to network and node failures.

CAP THEOREM



Consistency:

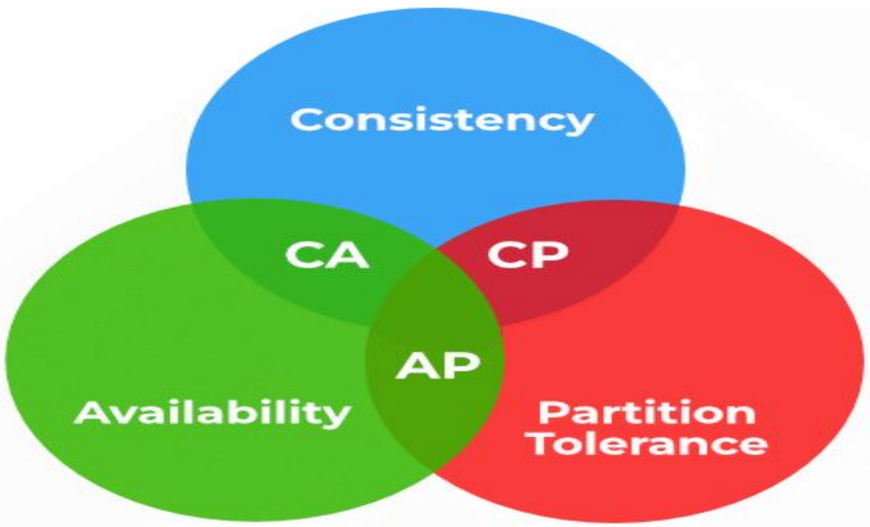
All clients see the same view of data, even right after update or delete

Availability:

All clients can find a replica of data, even in case of partial node failures

Partitioning:

The system continues to work as expected, even in presence of partial network failure



Decentralization using blockchain

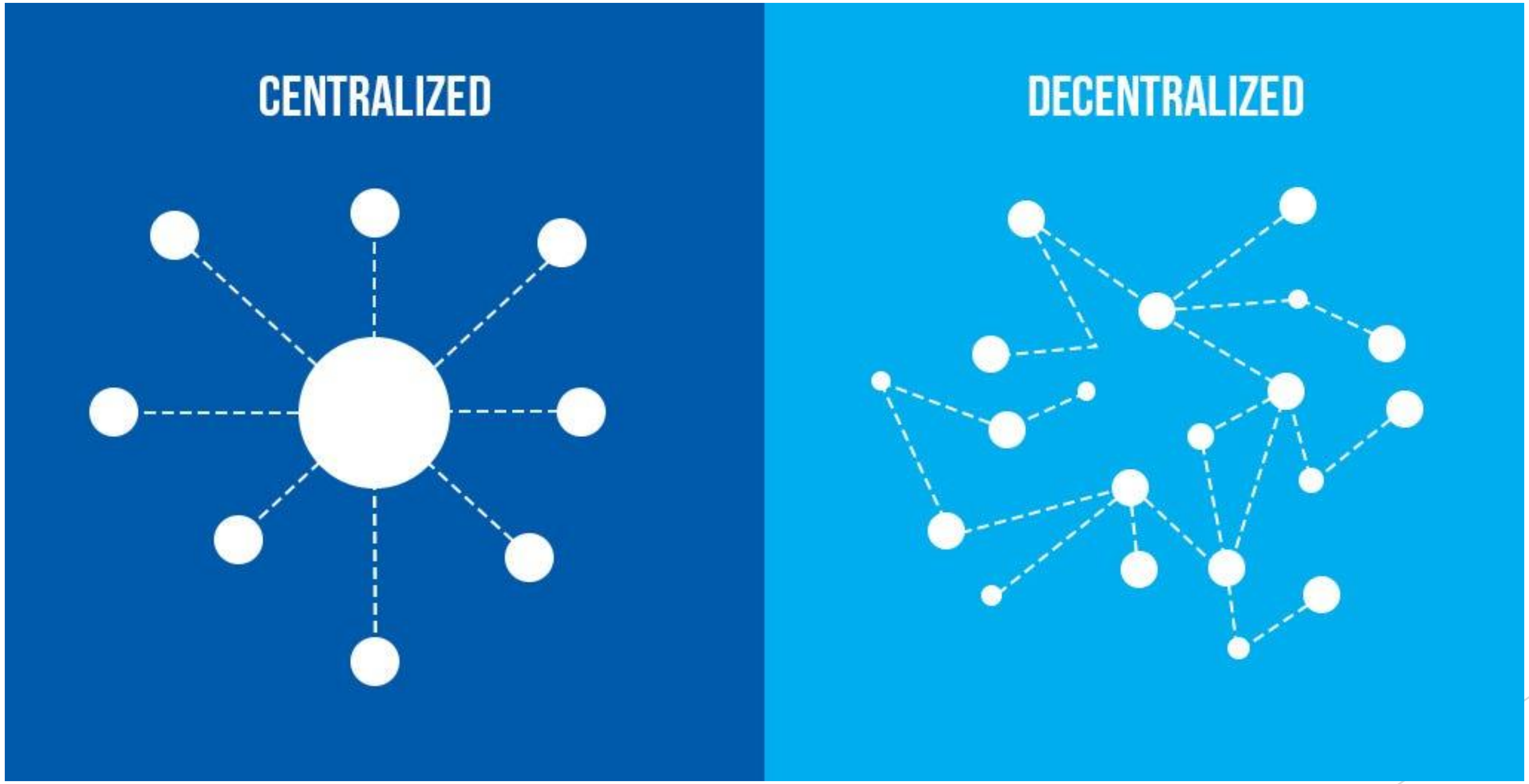
- Decentralization is a core benefit and service provided by blockchain technology.
- Blockchain is a perfect vehicle for providing a platform that does not need any intermediaries and that can function with many different leaders chosen via consensus mechanisms.
- This model allows anyone to compete to become the decision-making authority.
- This competition is governed by a consensus mechanism, and the most commonly used method is known as **Proof of Work** (**PoW**).

- Decentralization in blockchain refers to the distribution of control, decision-making, and authority across a network, rather than being controlled by a central entity (such as a government or corporation).
- In a decentralized blockchain, no single party has full control over the entire system.
- Instead, multiple participants (or nodes) collaborate to maintain, validate, and secure the blockchain, ensuring transparency, security, and trust without relying on a central authority.

Key aspects of decentralization in blockchain

- Distributed Ledger: The blockchain ledger is maintained across a network of computers (nodes), and every participant has a copy of the entire blockchain, making it harder for any single entity to manipulate or control the data.
- Consensus Mechanisms: Decentralized blockchains rely on consensus mechanisms (e.g., Proof of Work) to validate transactions and add blocks to the chain. These mechanisms ensure that all nodes agree on the state of the blockchain without requiring a central authority.

- Security: In a decentralized system, since data is spread across many participants, it is more resistant to hacking, fraud, or censorship. To alter data on the blockchain, an attacker would need to compromise a majority of the nodes, which is practically very difficult.
- Transparency and Immutability: Since the data is distributed and visible to all participants, it ensures transparency. Once data is added to the blockchain, it becomes nearly impossible to change (immutable), providing integrity to the system.

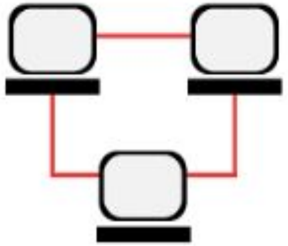

CENTRALIZED
DECENTRALIZED

DECENTRALIZED

- The control/ power is not held by a single entity. Instead it is distributed among multiple participants.
- Even if one node is corrupted/ fails, the network repairs itself.

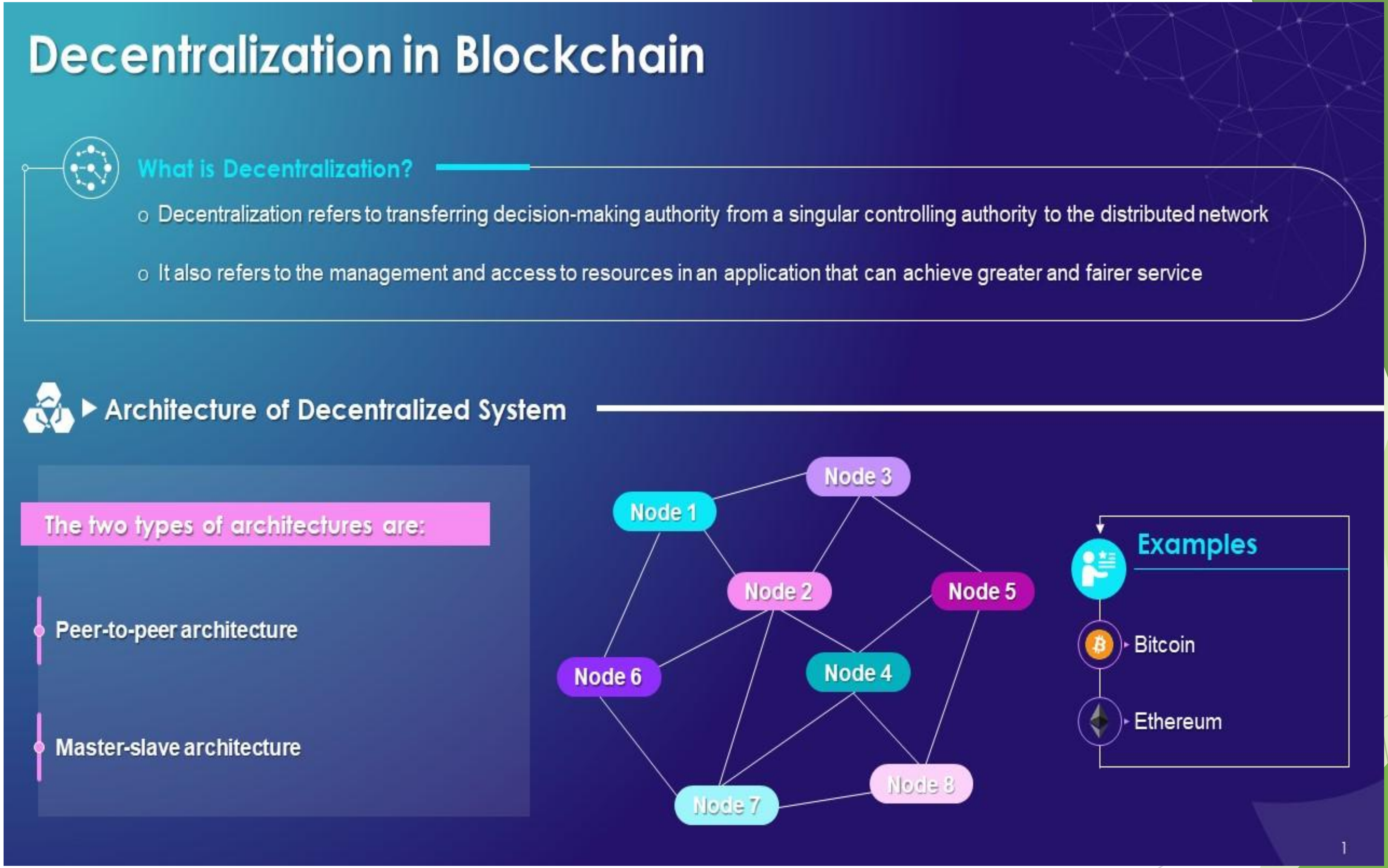
PEER TO PEER

- Direct peer to peer transaction of data or finance.
- Decentralized nature of blockchain instills trust in the process such that two unknown parties can directly interact/ transact with each other



DISTRIBUTED

- Data is distributed among the nodes(computers/ hard drives).
- Even if one node is tampered, the data does not get compromised.



Decentralization in Blockchain

What is Decentralization?

- Decentralization refers to transferring decision-making authority from a singular controlling authority to the distributed network
- It also refers to the management and access to resources in an application that can achieve greater and fairer service

Architecture of Decentralized System

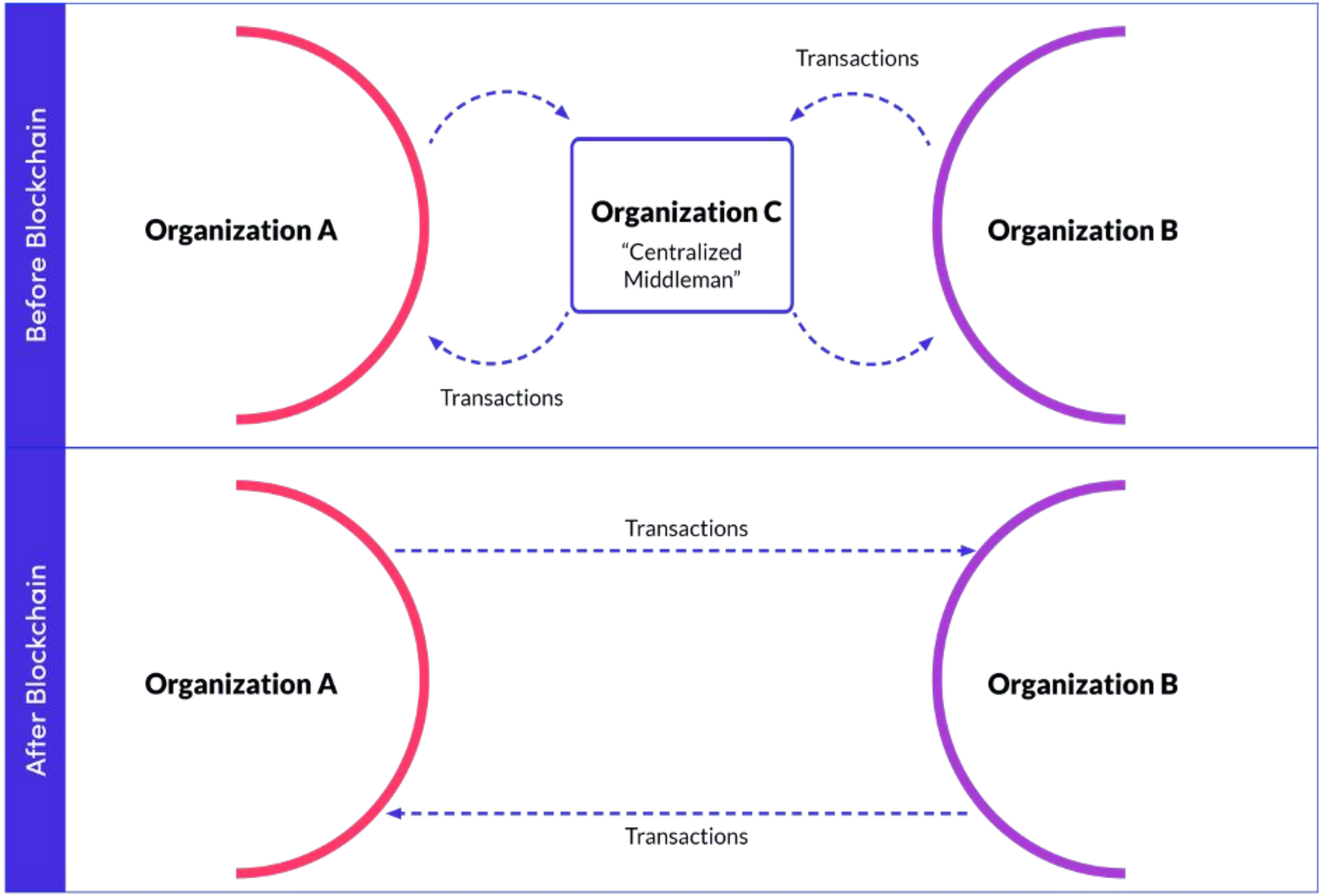
The two types of architectures are:

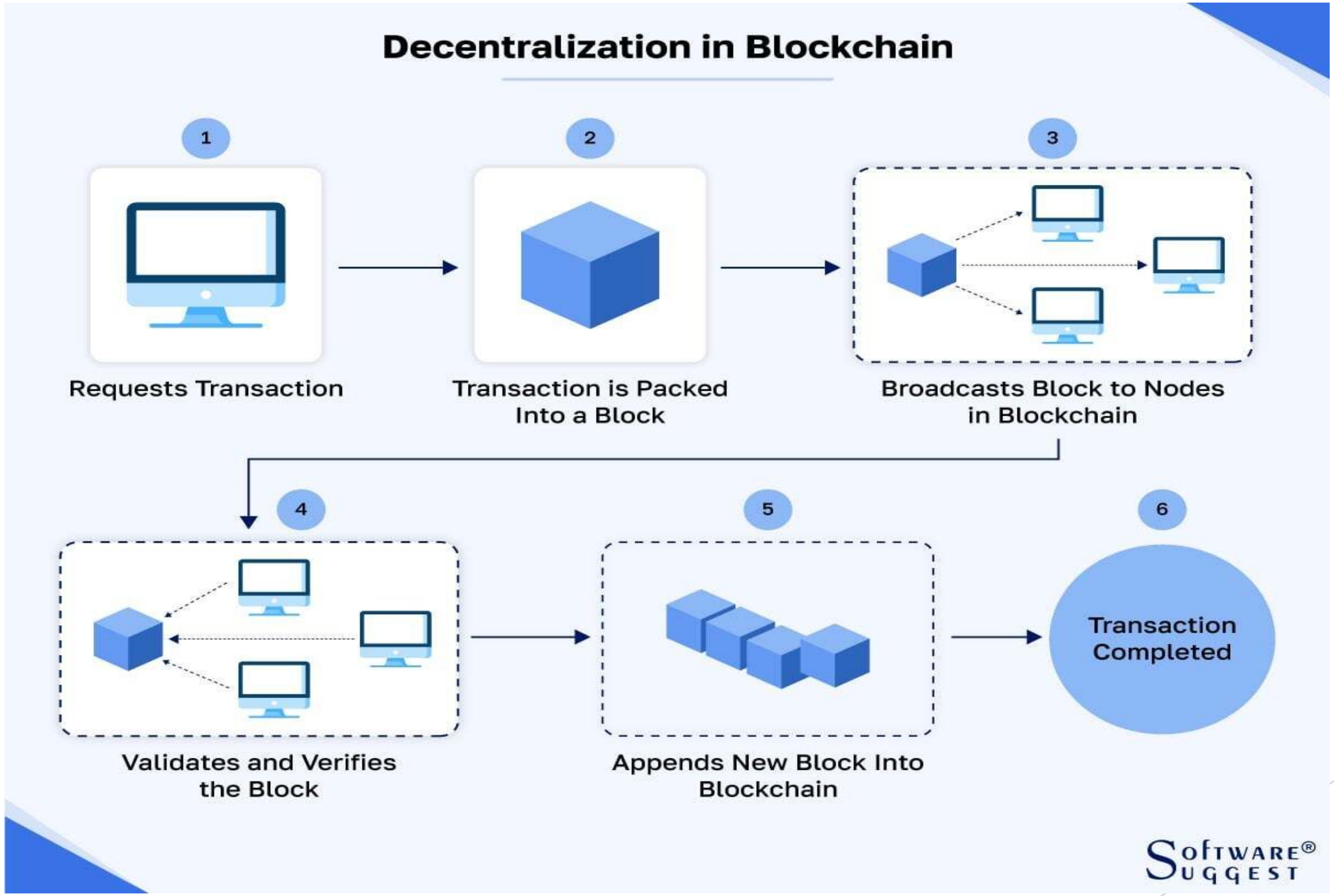
- Peer-to-peer architecture
- Master-slave architecture

Examples

- Bitcoin
- Ethereum

1


Before Blockchain
Organization A
Transactions
Organization C
"Centralized Middleman"
Transactions
Organization B
After Blockchain
Organization A
Transactions
Transactions
Organization B



Decentralization in Blockchain

1 Requests Transaction

2 Transaction is Packed Into a Block

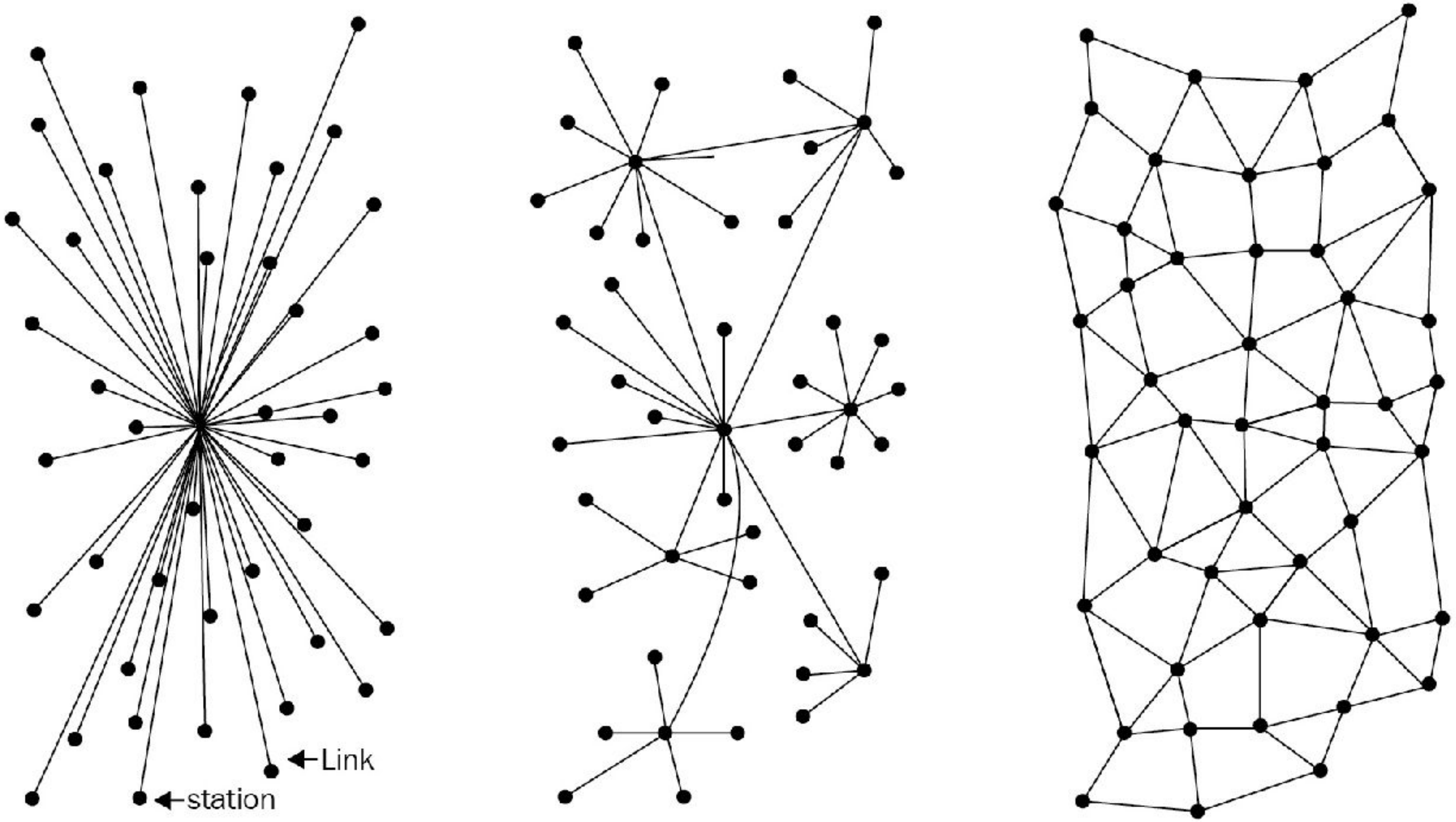
3 Broadcasts Block to Nodes in Blockchain

4 Validates and Verifies the Block

5 Appends New Block Into Blockchain

6 Transaction Completed

Different types of networks/systems



CENTRALIZED

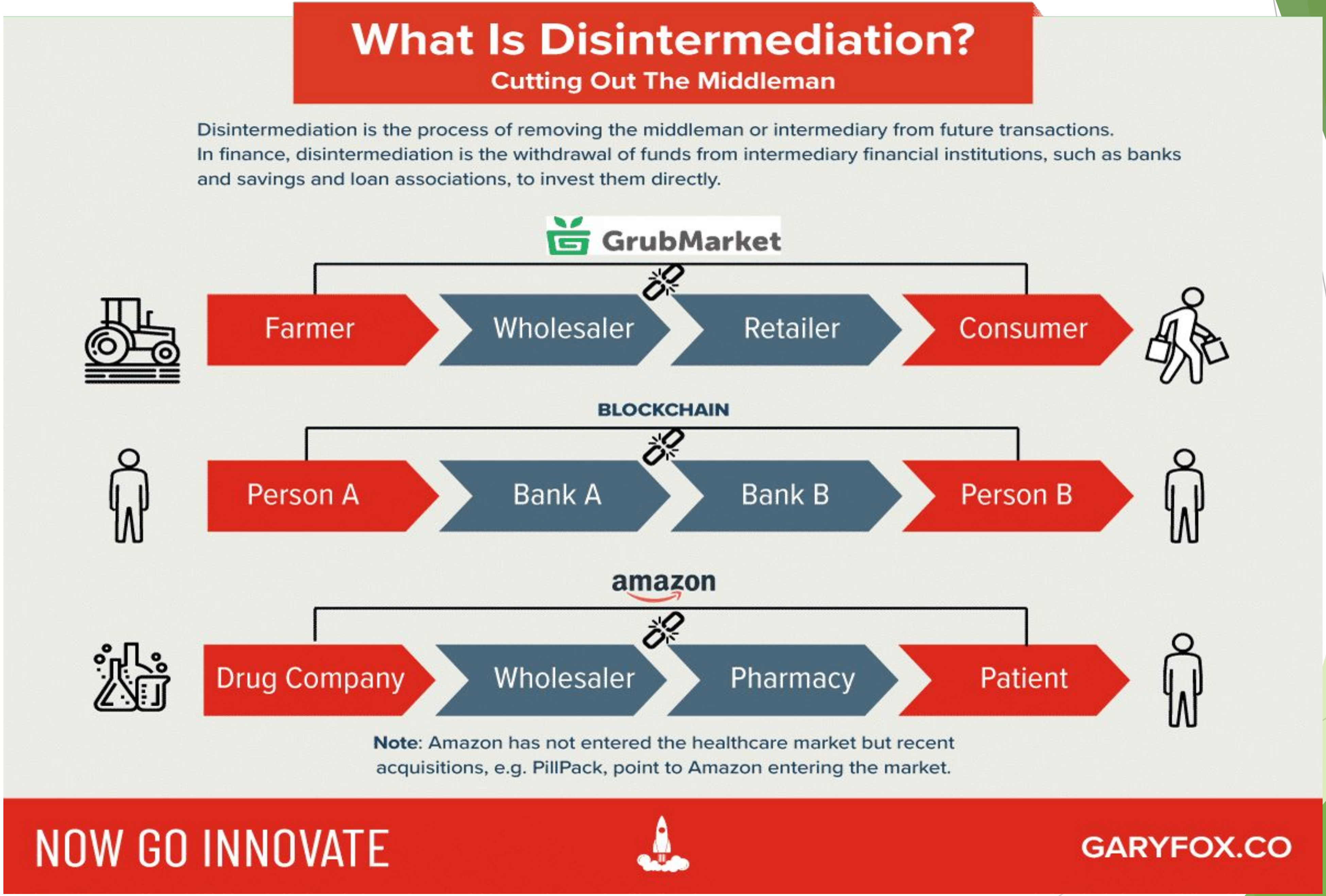
DECENTRALIZED

DISTRIBUTED

Methods of decentralization

1. **Disintermediation**
2. **Contest-driven decentralization**

- Disintermediation is when you remove the middleman (or intermediary) in a transaction.
- Normally, if you want to send money to a friend , you'd use a bank. The bank acts as a middleman, confirming and processing the payment for a fee.
- However, with blockchain technology, you can send money directly to your friend without the need for a bank. Instead of the bank keeping track of the transaction, the blockchain does it in a decentralized way, using an address for your friend.
- So, disintermediation through blockchain means you don't need a trusted middleman like a bank to handle your transactions.



What Is Disintermediation?

Cutting Out The Middleman

Disintermediation is the process of removing the middleman or intermediary from future transactions.
In finance, disintermediation is the withdrawal of funds from intermediary financial institutions, such as banks and savings and loan associations, to invest them directly.

GrubMarket

Farmer → Wholesaler → Retailer → Consumer

BLOCKCHAIN

Person A → Bank A → Bank B → Person B

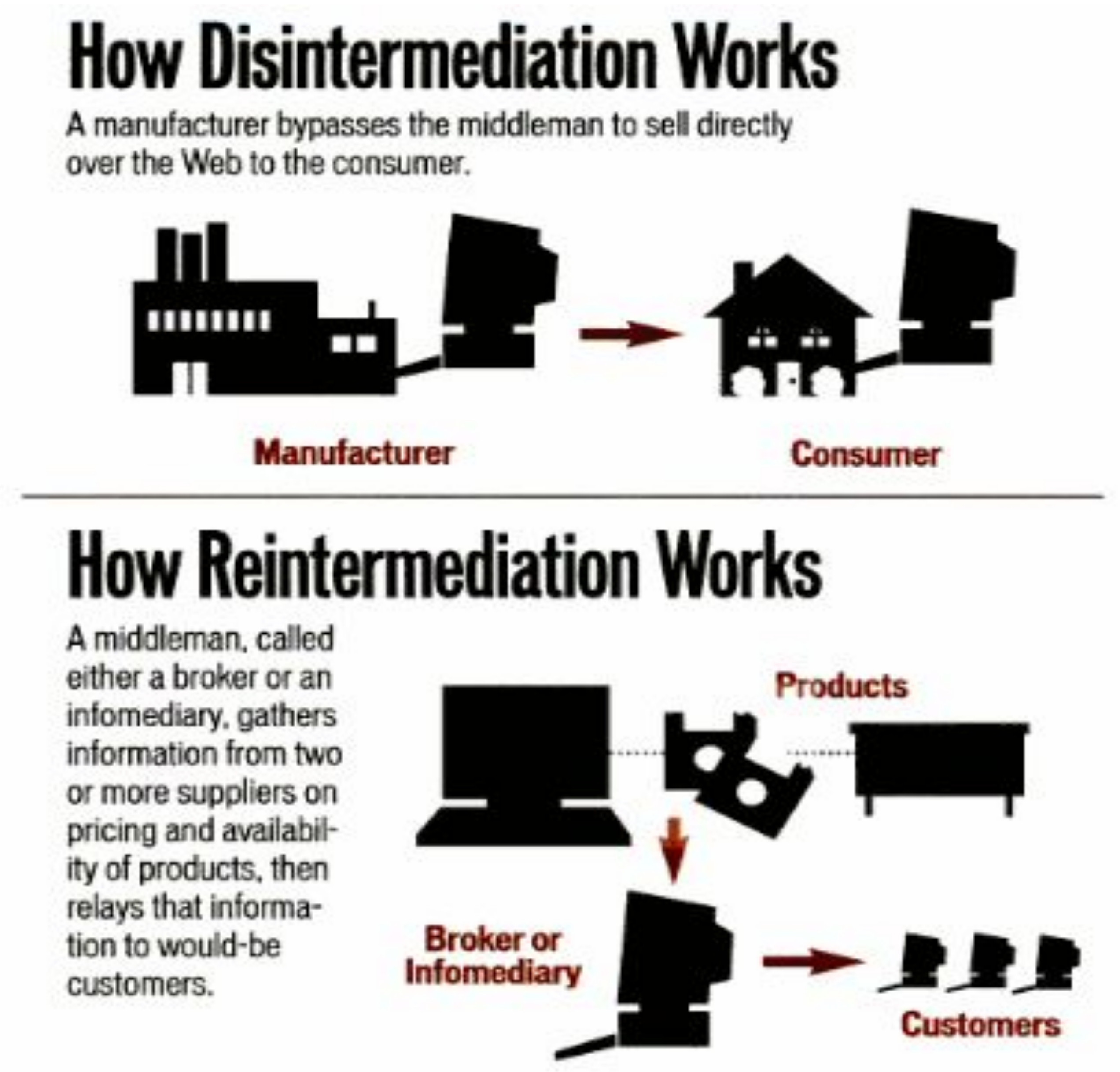
amazon

Drug Company → Wholesaler → Pharmacy → Patient

Note: Amazon has not entered the healthcare market but recent acquisitions, e.g. PillPack, point to Amazon entering the market.

NOW GO INNOVATE

GARYFOX.CO

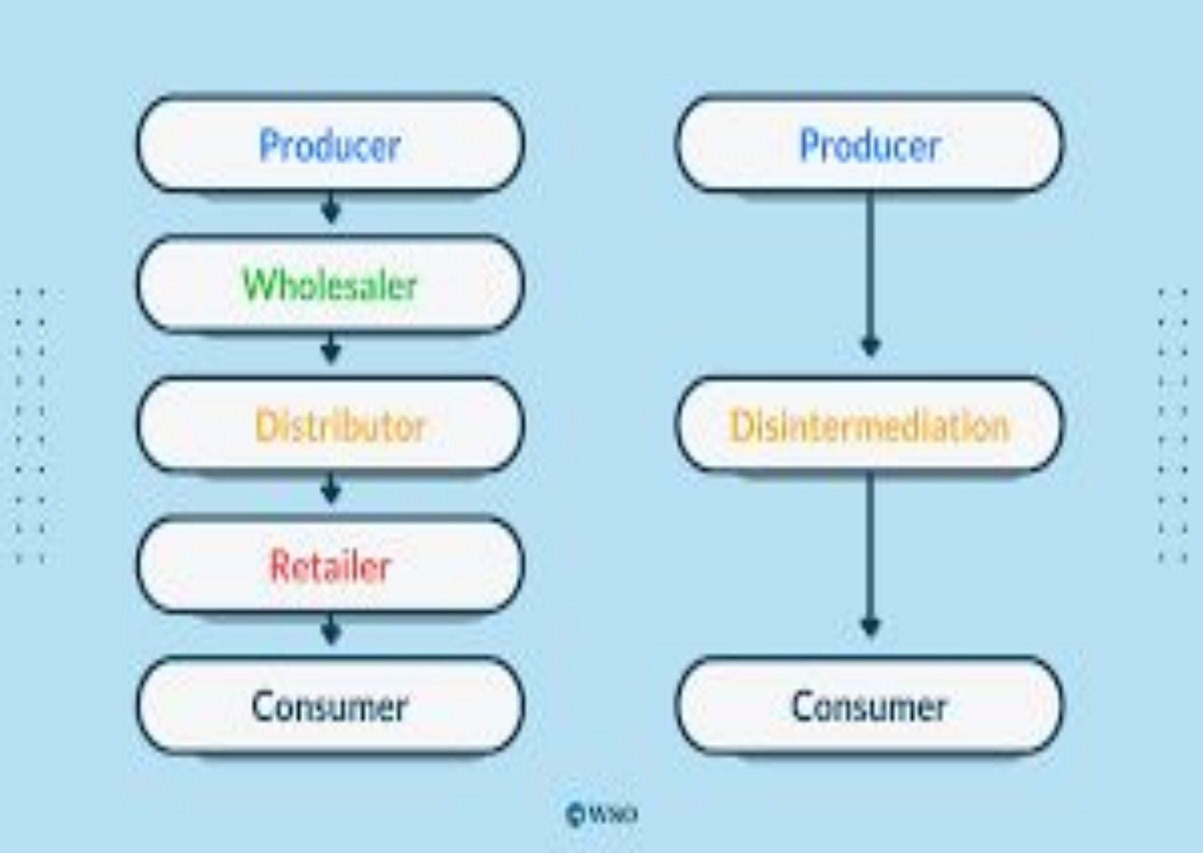


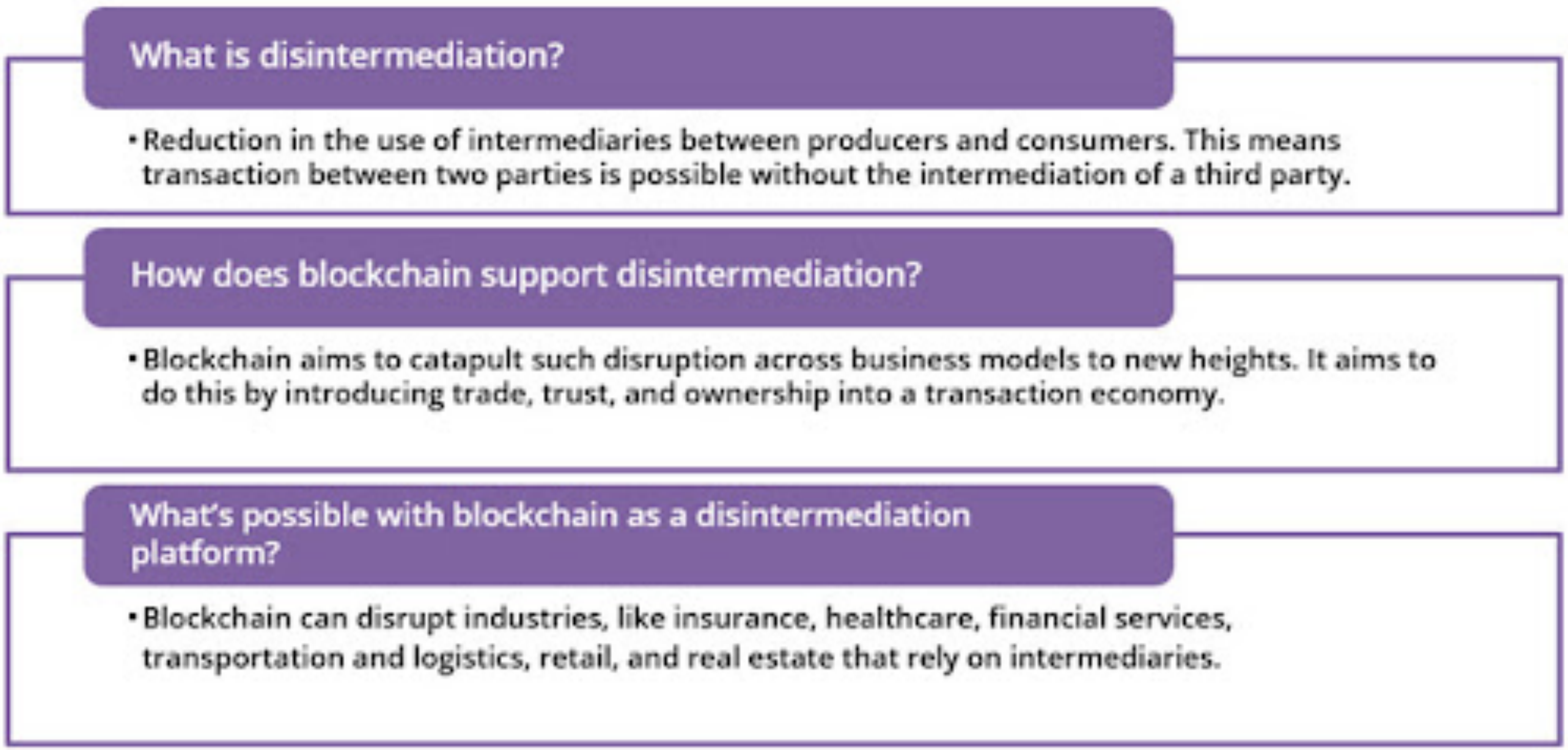
How Disintermediation Works

A manufacturer bypasses the middleman to sell directly over the Web to the consumer.

How Reintermediation Works

A middleman, called either a broker or an infomediary, gathers information from two or more suppliers on pricing and availability of products, then relays that information to would-be customers.


Producer
Wholesaler
Distributor
Retailer
Consumer
Producer
Disintermediation
Consumer
©WSO



What is disintermediation?

- Reduction in the use of intermediaries between producers and consumers. This means transaction between two parties is possible without the intermediation of a third party.

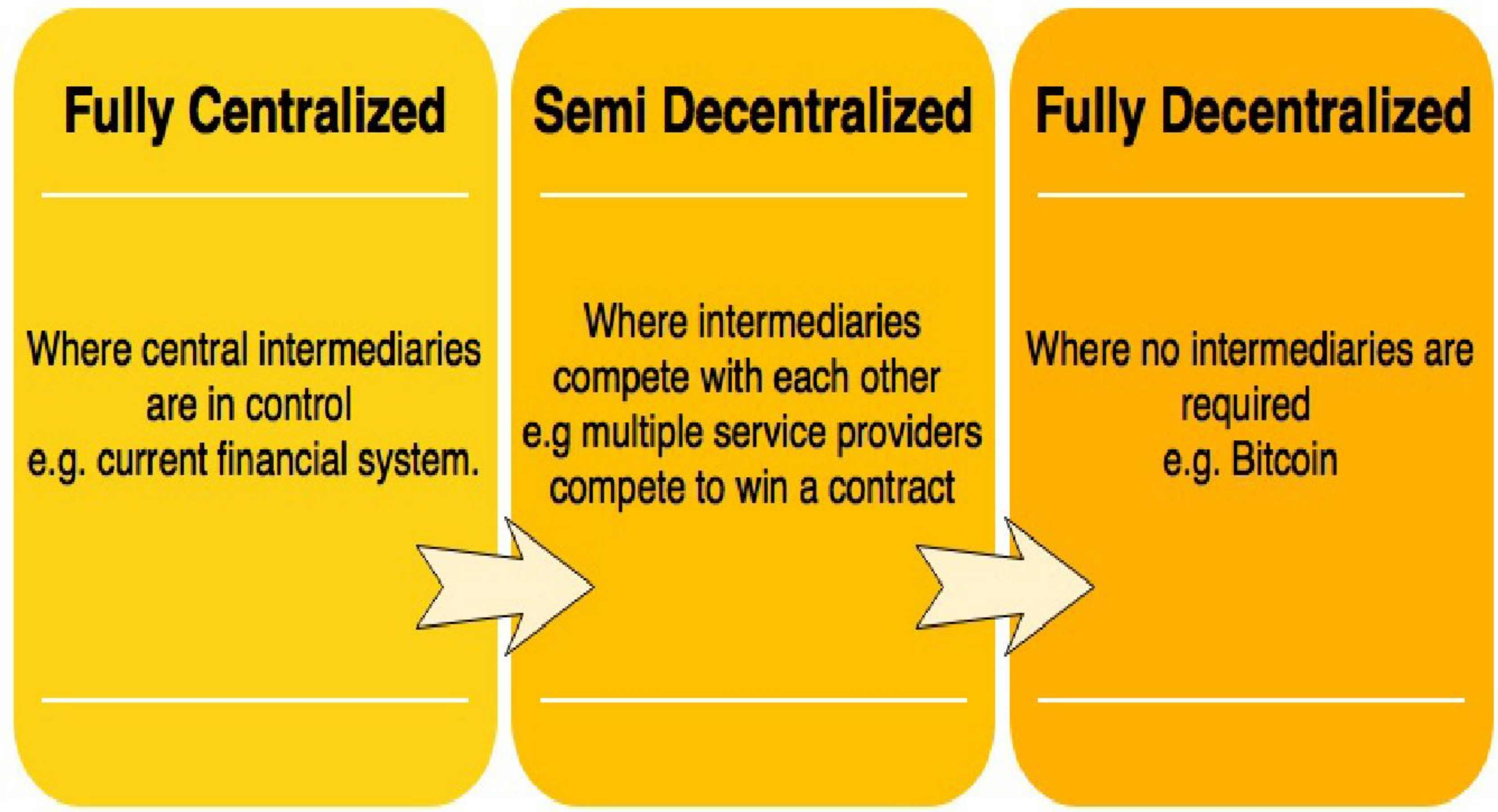
How does blockchain support disintermediation?

- Blockchain aims to catapult such disruption across business models to new heights. It aims to do this by introducing trade, trust, and ownership into a transaction economy.

What's possible with blockchain as a disintermediation platform?

- Blockchain can disrupt industries, like insurance, healthcare, financial services, transportation and logistics, retail, and real estate that rely on intermediaries.

Contest-driven decentralization



Fully Centralized

Where central intermediaries are in control
e.g. current financial system.

Semi Decentralized

Where intermediaries compete with each other
e.g multiple service providers compete to win a contract

Fully Decentralized

Where no intermediaries are required
e.g. Bitcoin

- **Contest-driven decentralization in blockchain** means using competitions or rewards to encourage people to participate in the blockchain network.
- For example, in Bitcoin, miners compete to solve complex math problems, and the first one to solve it gets rewarded with new coins.
- This competition helps secure the network because more people participate in validating transactions.
- Instead of relying on one central authority, like a bank, everyone in the network has a chance to contribute and earn rewards. This makes the system decentralized and more secure.

Routes to decentralization

- There were systems that pre-existed blockchain and Bitcoin, including **BitTorrent and the Gnutella** file sharing system, which to a certain degree could be classified as decentralized.
- The Bitcoin blockchain is typically the first choice for many, as it has proven to be the most resilient and secure blockchain and has a market cap of nearly $145 billion at the time of this writing.
- Alternatively, other blockchains, such as Ethereum, serve as the tool of choice for many developers for building decentralized applications.
- As compared to Bitcoin, Ethereum has become a more prominent choice because of the flexibility it allows for programming any business logic into the blockchain by using *smart contracts*.

Key routes to decentralization:

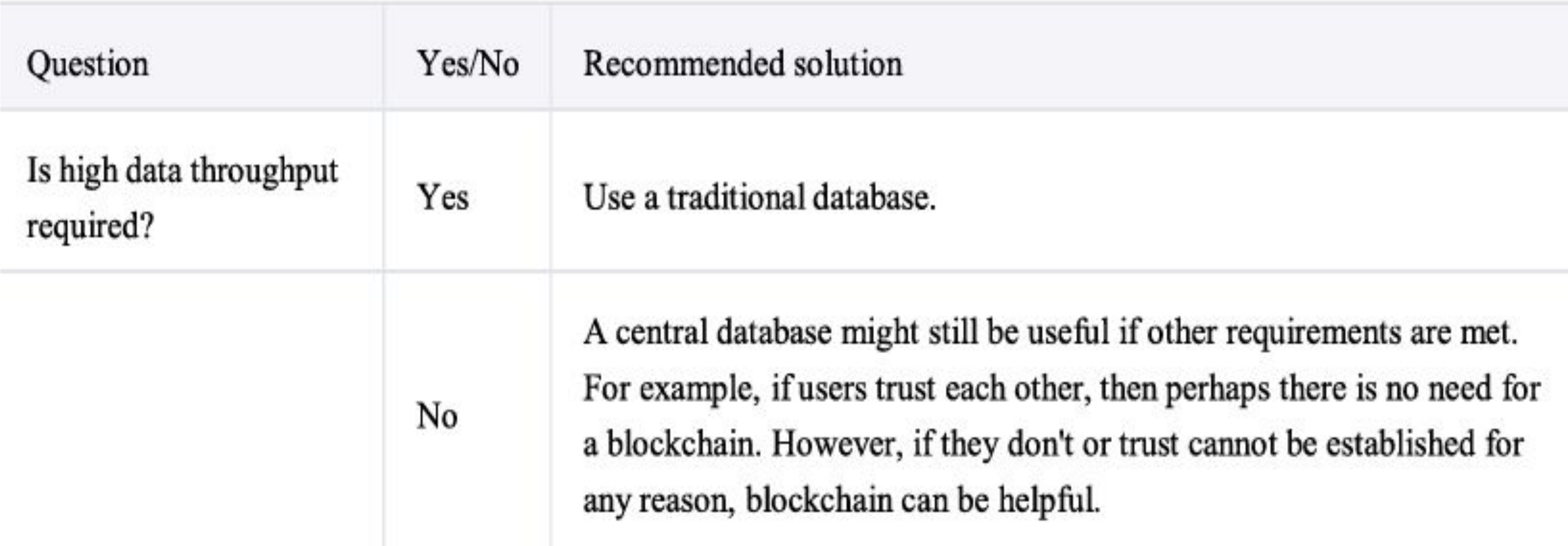
Peer-to-Peer (P2P) Networks

- In a decentralized blockchain, all participants (or nodes) communicate directly with each other without relying on a central server or authority.
- This ensures that no single entity has control over the network, and the power is distributed among many participants.

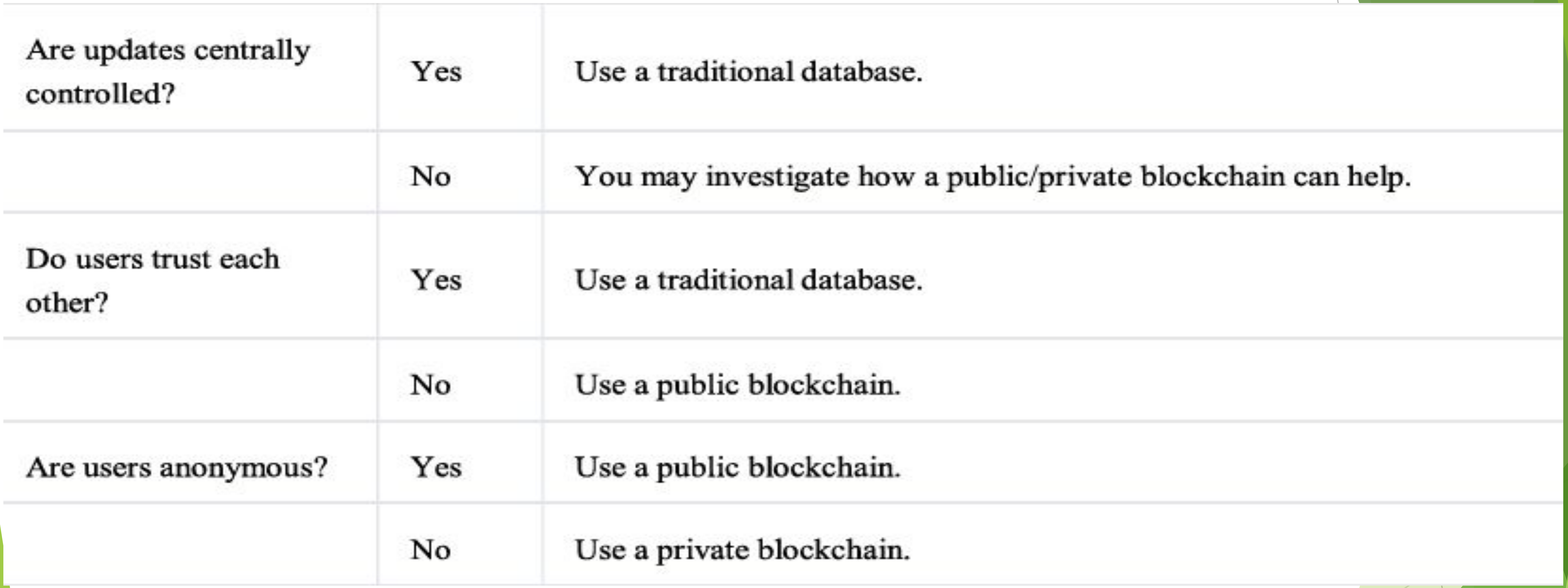
Consensus Mechanisms

- **Proof of Work (PoW)**: Miners compete to solve complex problems, and the first to solve it gets to validate transactions. This encourages decentralized participation by anyone who can provide computing power.
- **Proof of Stake (PoS)**: Validators are chosen based on how many coins they hold and are willing to "stake" as collateral. This encourages decentralization by letting anyone with a stake participate in validating transactions.
- **Delegated Proof of Stake (DPoS)**: A smaller group of elected delegates validate transactions, reducing the number of active participants but still keeping the system decentralized by using democratic voting.

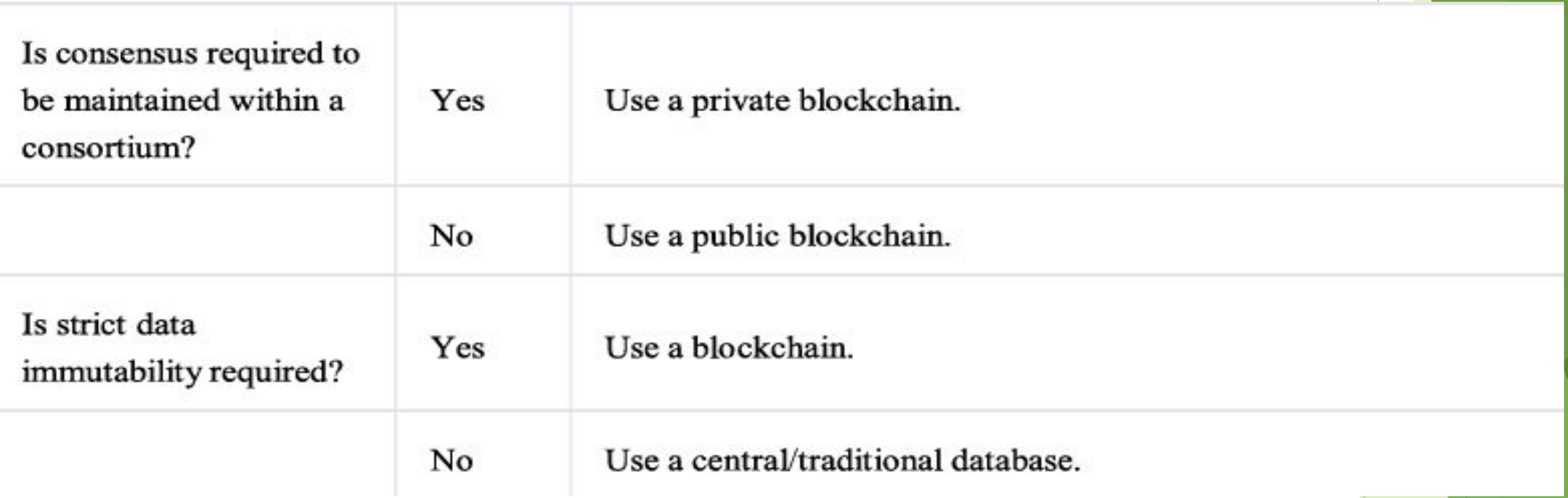
Is a blockchain really needed? When is a blockchain required? In what circumstances is blockchain preferred over traditional databases?



Question	Yes/No	Recommended solution
Is high data throughput required?	Yes	Use a traditional database.
	No	A central database might still be useful if other requirements are met. For example, if users trust each other, then perhaps there is no need for a blockchain. However, if they don't or trust cannot be established for any reason, blockchain can be helpful.



Are updates centrally controlled?	Yes	Use a traditional database.
	No	You may investigate how a public/private blockchain can help.
Do users trust each other?	Yes	Use a traditional database.
	No	Use a public blockchain.
Are users anonymous?	Yes	Use a public blockchain.
	No	Use a private blockchain.



Is consensus required to be maintained within a consortium?	Yes	Use a private blockchain.
	No	Use a public blockchain.
Is strict data immutability required?	Yes	Use a blockchain.
	No	Use a central/traditional database.

Open-Source Protocols:

- Many decentralized blockchain networks are open-source, meaning anyone can participate in their development or create their own versions of the blockchain.
- This openness promotes decentralization because it allows anyone to contribute to or fork the network.

How to decentralize

- The framework raises four questions whose answers provide a clear understanding as to how a system can be decentralized:

1. What is being decentralized? Trading or identity system

2. What level of decentralization is required? Full disintermediation or partial

3. What blockchain is used? Bitcoin or Etherium

4. What security mechanism is used?

The decentralization framework example

- A money transfer system as an example of an application selected to be decentralized. The four questions discussed previously are used to evaluate the decentralization requirements of this application. The answers to these questions are as follows:

1. Money transfer system
2. Disintermediation
3. Bitcoin
4. Atomicity