

## Blockchain Introduction:

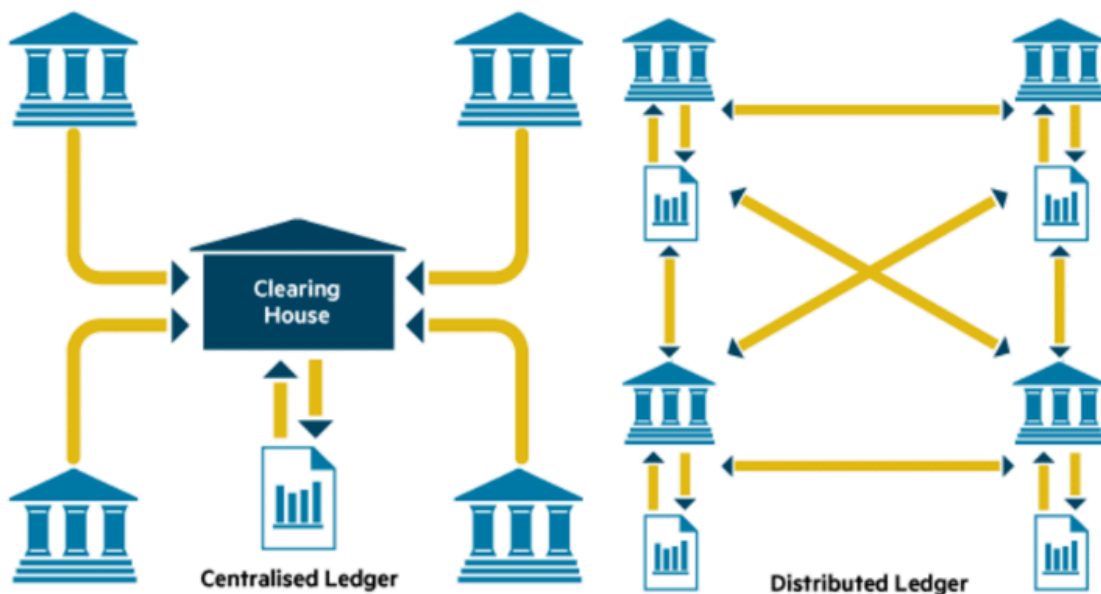
Blockchain Technology Mechanisms & Networks, Blockchain Origins, Blockchain Objectives, Blockchain Users & Adoption, Blockchain Challenges, P2P Systems, Hash Pointers and Data Structures, Blockchain Transactions



## 1. Blockchain Technology Mechanisms & Networks

### Distributed Ledger:

- A decentralized database shared across nodes in the network.
- Each participant has access to the entire ledger in real-time.

A distributed ledger is a network that records ownership through a shared registry



Division	Centralized Ledger Management	Distributed Ledger Management
Cloud Storage		
Type	Centralized management	Distributed management
Notarization and management entity	Notarize all transaction details by the central third party	-All transaction participants view, notarize, and manage transaction details -Transaction history is shared and archived for all network participants
Cost	The high cost of maintenance(management)	-Low system deployment costs -Low maintenance costs
Characteristics	-Advantages: (1) quick transaction speed, (2) ease of control -Disadvantages: Vulnerable to security (Dos vulnerable to attacks and hacking)	-Advantages: (1) Maintaining transparency in transaction information, (2) No DDos attack, (3) No forgery of transaction details. -Advantages: (1) relatively slow transaction speed, (2) the complexity of control

# How does blockchain differs from Distributed Ledger

## BLOCKCHAIN VS DISTRIBUTED LEDGERS



### WHAT IS A BLOCKCHAIN?

Blockchain is a database system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. Blockchain is one type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash.



### WHAT IS A DISTRIBUTED LEDGER?

A distributed ledger is a database spread across computers, nodes, and different locations. Through decentralisation each node maintains the ledger independently in real-time, and this maintenance by all the nodes brings transparency and immutability.

### WHAT'S THE DIFFERENCE?

Blockchain technology is only one type of distributed ledger and therefore, not every distributed ledger is a blockchain. The difference is the mode of storage of information in both.

### Blockchain

### Distributed Ledger



#### STRUCTURE

Data is a chain of blocks.

A database spread across different nodes.



#### SEQUENCE

Blocks are set in a particular sequence.

No need to follow blockchain's sequence of data.



#### CONSENSUS

Power hungry because of PoW or PoS mechanism.

No need of a consensus mechanism and therefore, more scalable.



#### TOKENS

Most blockchains do use token economy but it's not a must.

No need to use a token or any kind of cryptocurrency.



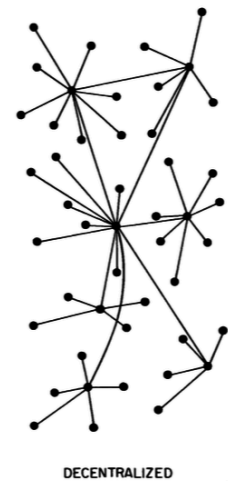
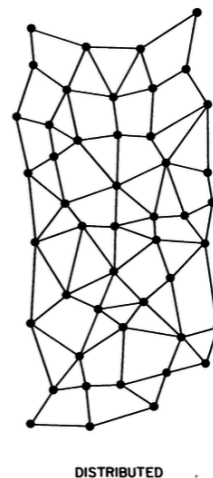
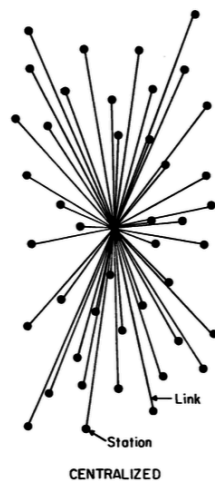
#### APPLICATIONS

Many institutions and enterprises already use blockchain technology.

Most projects are still under development and therefore, no real-life implementations yet.

# How do we compare centralized system vs decentralized system vs distributed system

	Centralized	Distributed	Decentralized
<i>Network/hardware resources</i>	Maintained & controlled by single entity in a centralized location	Spread across multiple data centers & geographies; owned by network provider	Resources are owned & shared by network members; difficult to maintain since no one owns it
<i>Solution components</i>	Maintained & controlled by central entity	Maintained & controlled by solution provider	Each member has exact same copy of distributed ledger
<i>Data</i>	Maintained & controlled by central entity	Typically owned & managed by customer	Only added through group consensus
<i>Control</i>	Controlled by central entity	Typically, a shared responsibility between network provider, solution provider & customer	No one owns the data & everyone owns the data
<i>Single Point of Failure</i>	Yes	No	No
<i>Fault tolerance</i>	Low	High	Extremely high
<i>Security</i>	Maintained & controlled by central entity	Typically, a shared responsibility between network provider, solution provider & customer	Increases as # of network members increase
<i>Performance</i>	Maintained & controlled by central entity	Increases as network/hardware resources scale up and out	Decreases as # of network members increase
<i>Example</i>	ERP system	Cloud computing	Blockchain



## **Types of Blockchains:**

1. **Public:** Open to everyone (e.g., Bitcoin, Ethereum).
2. **Private:** Restricted access, managed by a single entity.
3. **Consortium:** Semi-decentralized, governed by a group.
4. **Hybrid:** Combines public and private blockchain features.

### **1. Public Blockchain Networks**

Bitcoin and other cryptocurrencies originated from public blockchains, which also played a role in popularizing distributed ledger technology (DLT). Public blockchains also help to eliminate certain challenges and issues, such as security flaws and centralization.

DLT distributes data across a peer-to-peer network rather than stored in a single location. A consensus algorithm verifies information authenticity; proof of stake (PoS) and proof of work (PoW) are two frequently used consensus methods.

### **2. Private Blockchain Networks**

Private blockchains operate on closed networks and tend to work well for private businesses and organizations. Companies can use private blockchains to customize their accessibility and authorization preferences, network parameters, and other important security options. Only one authority manages a private blockchain network.

### **3. Consortium Blockchains**

Like permissioned blockchains, consortium blockchains have public and private components, except multiple organizations will manage a single consortium blockchain network. Although these blockchains can initially be more complex to set up, once they are running, they can offer better security. Additionally, consortium blockchains are optimal for collaboration with multiple organizations.

### **4. Hybrid Blockchains**

Hybrid blockchains combine public and private blockchains. Some parts are public and transparent, while others are private and accessible only to authorized and specific participants. This makes hybrid blockchains ideal for use in cases where a balance between transparency and privacy is required. For example, in supply chain management, multiple parties can access certain information, but sensitive data can be kept private.

## Sidechains

Sidechains are different blockchains that run parallel to the main blockchain, allowing for additional functionality and scalability. They enable developers to experiment with new features and applications without affecting the main blockchain's integrity. For example, sidechains can be used to create decentralized applications and implement specific consensus mechanisms. They can also be used to handle transactions on the main blockchain to reduce congestion and increase scalability.

## Blockchain Layers

Blockchain layers refer to the concept of building multiple layers of blockchains on top of each other. Each layer can have its own consensus mechanism, rules, and functionality which can interact with other layers. This ensures greater scalability, as transactions can be processed in parallel across different layers. For example, the Lightning Network, built on top of the Bitcoin blockchain, is a second layer solution that enables faster and cheaper transactions by creating payment channels between users.

## Blockchain Origins

### Key Milestones:

1. **1980s-1990s:**
  - David Chaum introduces concepts of cryptographic systems.
  - Merkle Trees developed for efficient and secure data structures.
2. **2008:**
  - Satoshi Nakamoto's Bitcoin whitepaper published.
  - Introduces decentralized digital currency.
3. **2009:**
  - Bitcoin Genesis Block mined.
4. **2013:**
  - Vitalik Buterin proposes Ethereum for decentralized applications.

### Philosophical Roots:

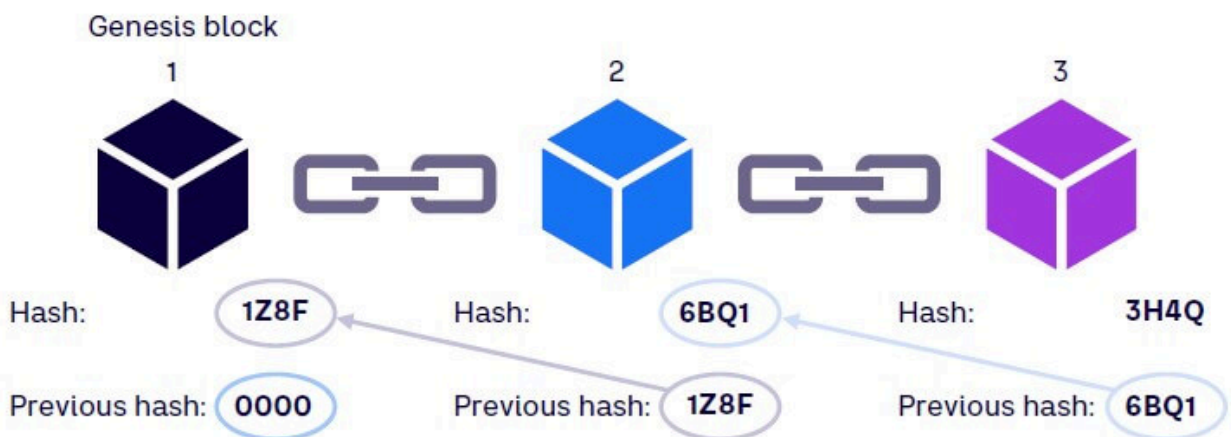
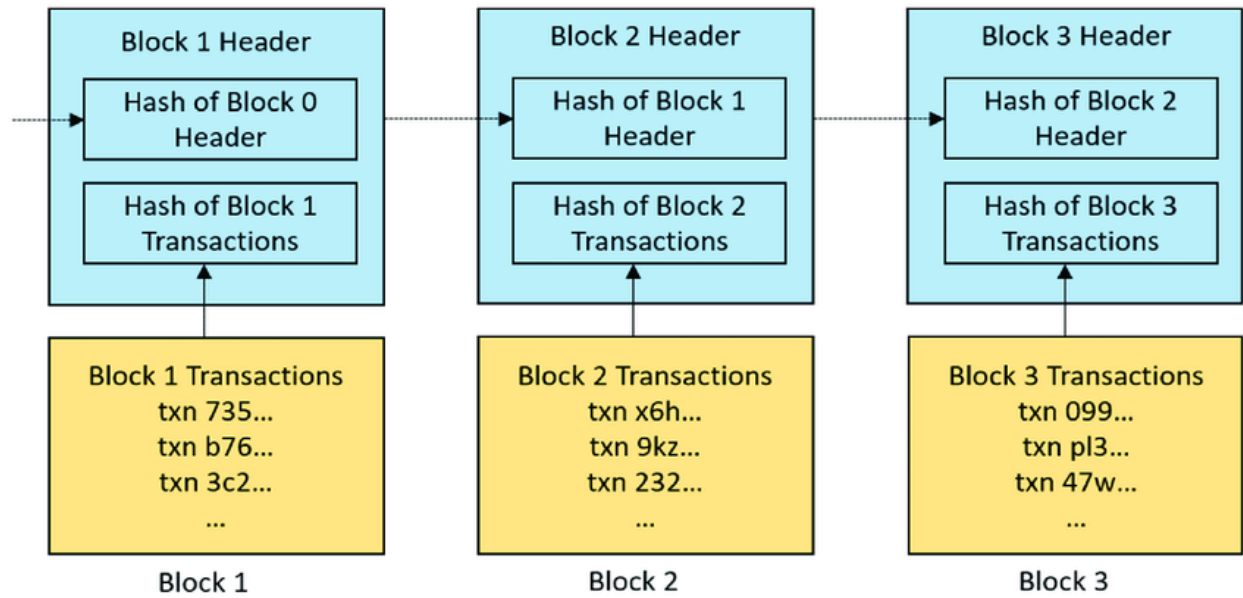
- Trustless systems: Eliminate reliance on centralized authorities.
  - Decentralization: Empower participants directly.
  - Transparency: Ensure visible and immutable records.
-

## Blockchain Objectives

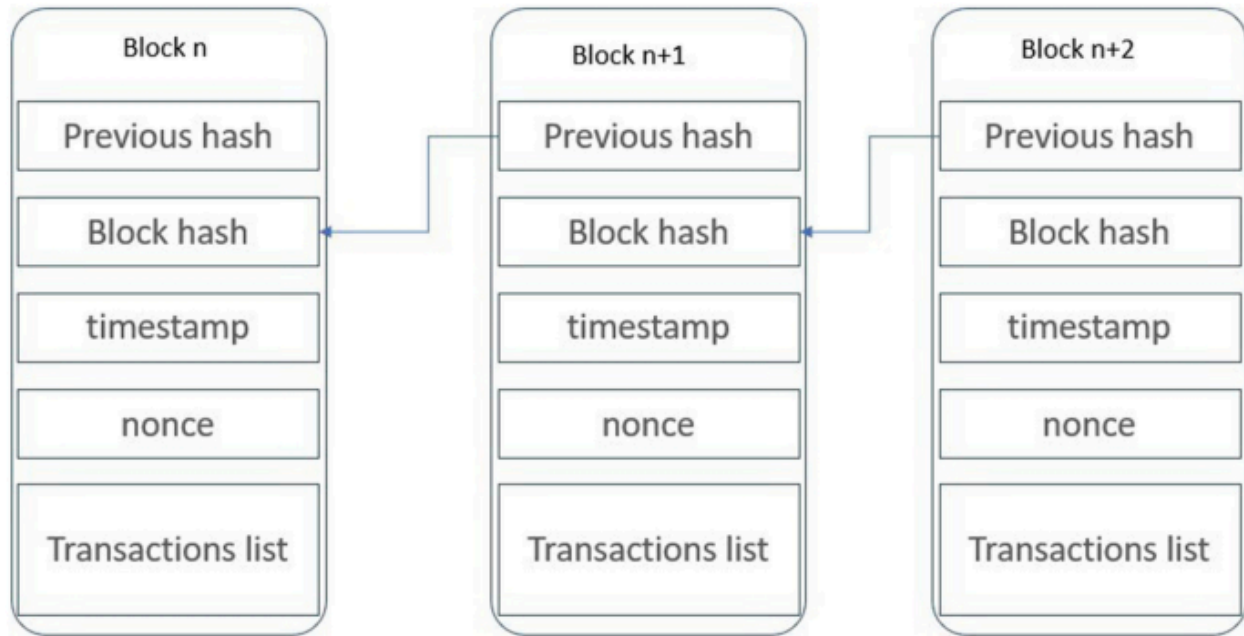
1. **Transparency:**
  - Open ledgers enable public verification of transactions.
2. **Security:**
  - Cryptographic methods ensure data integrity and prevent tampering.
3. **Efficiency:**
  - Automate processes using smart contracts.
  - Reduce intermediaries and associated costs.
4. **Decentralization:**
  - Distribute control across participants.
5. **Immutability:**
  - Data on the blockchain cannot be modified once written.

## Blockchain Challenges

1. **Scalability:**
  - Current blockchains struggle with high transaction volumes.
2. **Energy Consumption:**
  - PoW mechanisms consume vast energy.
3. **Regulation:**
  - Unclear and evolving legal frameworks.
4. **Interoperability:**
  - Difficulties in communication between different blockchains.
5. **User Experience:**
  - Complex interfaces hinder adoption.
6. **Security Risks:**
  - 51% attacks, smart contract vulnerabilities.



Source: Arthur D. Little



1. **Header:** It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.
2. **Previous Block Address/ Hash:** It is used to connect the  $i+1$ th block to the  $i$ th block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.
3. **Timestamp:** It is a system that verifies the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.
4. **Nonce:** A nonce number which is used only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.
5. **Merkel Root:** It is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.



**Figure 6:** Example of how a company might send cryptocurrency to another company using blockchain technology

