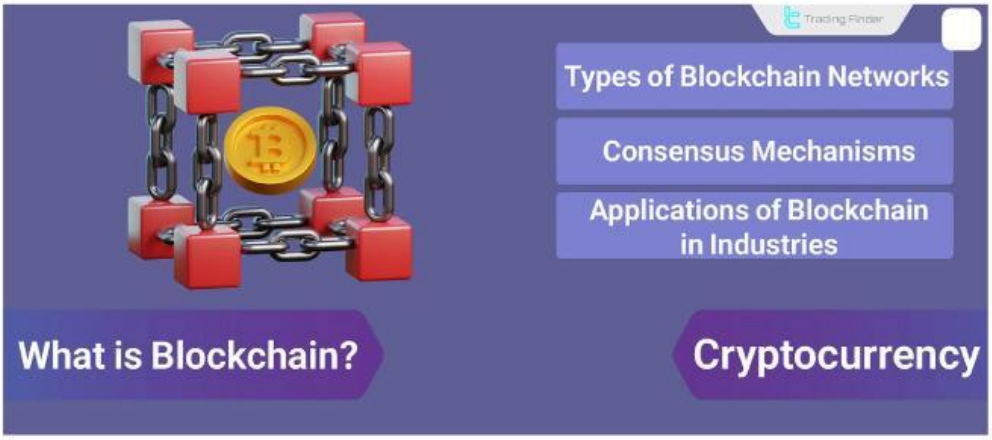
What is Blockchain? [Applications of Blockchain in Cryptocurrency and Banking]

Blockchain is a revolutionary form of **data storage**, thanks to its unique features like **decentralization, immutability, transparency, security**, and **highspeed**.

In a **blockchain network**, each block stores a specific volume of data and is encrypted using a **hash algorithm**; in this way, blockchain has extensive applications in **cryptocurrencies** and the **modern banking industry**.



Blockchain is a decentralized database with broad applications in areas like cryptocurrency, banking, and insurance

What is Blockchain?

Blockchain, or **blockchain network**, is a **decentralized, tamper-proof storage platform (database)** that stores digital information.

In blockchain, each block stores a specific amount of data (such as cryptocurrency transaction information, smart contract details, etc.) and is connected to each other using **hash encryption**; this feature turns blockchain into an immutable chain of data.

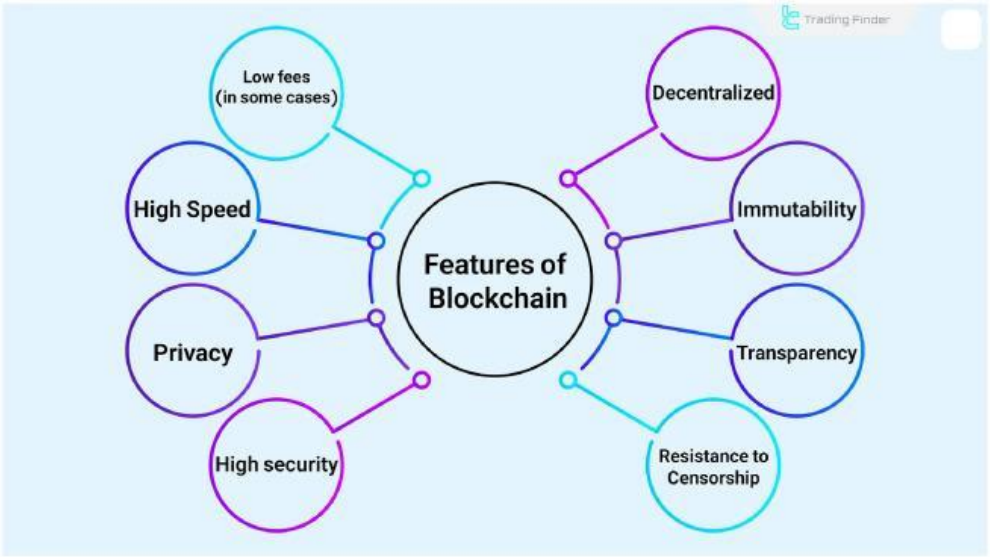
Structure of a Block in Blockchain Includes:

- **Data**: Financial transactions, asset ownership, medical records, etc.
- **Current block hash**: Identifier of the current block
- **Previous block hash**: For linking to the previous block

Features of Blockchain

In the structure of the **blockchain network**, each miner (transaction validator) has a copy of the database. If any change occurs in block data, the network will **reject** that block.

To change the information, an individual would need to control over **51% of the network power**; this is **very expensive** and due to the **global scale of participants**, is practically **impossible**.



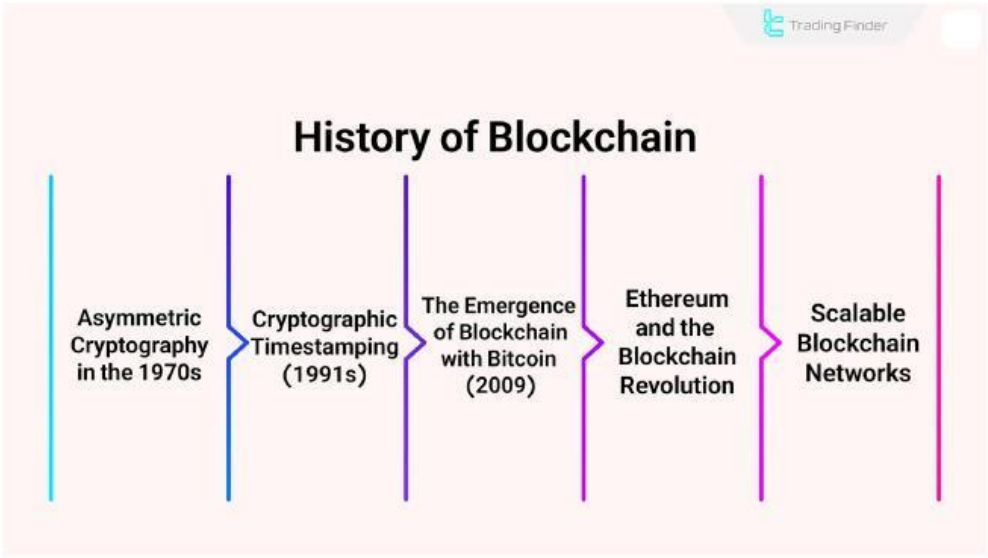
Storing information in a fast, secure, and transparent way in a decentralized space are some of the key features of blockchain

Blockchain Features:

- **Decentralized**: Blockchain distributes data among network users without needing a central authority, making it resistant to censorship and sanctions;
- **Immutability**: Every block contains the hash of the previous block. If someone changes the past data, the hash becomes inconsistent, exposing fraud to the network;
- **Transparency**: All transaction data can be viewed through **Blockchain Explorers**;
- **Censorship Resistance**: No government or organization can block transactions or data;
- **Low fees in some cases**: For example, in blockchains like Litecoin, transaction fees are lower than traditional payment systems;
- **High Speed**: Some **blockchain networks** like Solana can process thousands of transactions per second;
- **Privacy**: Blockchains like Monero or Zcash conceal user identities and transaction amounts;
- **High Security**: Blockchain uses irreversible **hash-based encryption** and a global distribution of nodes to create a tamper-proof and secure system.

History of Blockchain

The **Blockchain database** has its roots in **cryptography** and **computer science**. Before the emergence of blockchain and **Bitcoin** in 2009, theories about **asymmetric encryption** and **data sharing between nodes** laid the groundwork for blockchain infrastructure.



Blockchain began with cryptography in the 1970s and became mainstream with Bitcoin in 2009

Asymmetric Cryptography in the 1970s

In the 1970s, two scientists, **"Whitfield Diffie"** and **"Martin Hellman"**, introduced the concept of asymmetric cryptography, creating a major breakthrough in data security and laying the foundation of **Blockchain technology**.

This revolutionary idea enabled individuals to encrypt and send messages without sharing private keys. Each person has a pair of **public** and **private keys**. The public key encrypts data and is shared openly, while the private key decrypts data and must remain secret. In cryptocurrency, a **wallet address** is the **public key**, and the **wallet password** is the private key.

Cryptographic Timestamping

In 1991, **Stuart Haber** and **W. Scott Stornetta** introduced **Cryptographic Timestamping** to securely store digital documents. This system is used for hashing algorithms to create a data chain that included the hash of the previous data block — much like today's **Blockchain**. It marked the first practical step toward developing a **Blockchain network**.

The Emergence of Blockchain with Bitcoin (2009)

In response to the 2008 financial crisis, **Bitcoin** was launched in 2009 by the pseudonymous figure **"Satoshi Nakamoto"** to create a decentralized financial system with no intermediaries.

On January 3, 2009, Nakamoto **mined the first Bitcoin block**, which included the message: "Chancellor on the brink of second bailout for banks," a direct criticism of the traditional banking system.

Years later, the first cryptocurrency exchanges appeared, and Bitcoin mining was even possible using home computers.

Ethereum and the Blockchain Revolution

In 2015, **"Vitalik Buterin"** introduced **Ethereum**, which introduced **smart contracts** to the **Blockchain**. These contracts execute automatically on the **Blockchain network** without intermediaries. **Their key traits are immutability**, **security**, and **transparency**.

Smart contracts have wide applications in **DeFi (Decentralized Finance)**, **supply chain management**, **real estate transactions**, **NFTs**, **Blockchain gaming**, and **electronic voting**.

For instance, in DeFi, users can obtain loans without intermediaries, trade via decentralized exchanges, or earn passive income through **staking**.

In supply chains, goods can be tracked from origin to delivery, and smart contracts can trigger payments **automatically**.

Scalable Blockchain Networks

As **Blockchain** usage grew, the issue of **scalability** became prominent due to limited block size and processing time.

When the network gets congested, users have to pay higher fees for faster confirmation, leaving cheaper transactions to wait longer.

Solutions like **Ethereum 2.0**, **Solana**, and **Polygon** addressed scalability issues. Ethereum 2.0 replaced **PoW (Proof of Work)** with **PoS (Proof of Stake)** to increase transaction speed and reduce computational load.

Sharding is another approach, splitting the database into smaller parts to enable **parallel transaction processing**. For example, Ethereum can process up to **5000** transactions per second with sharding, compared to just **30** without it.

Blockchain Security

Blockchain security is ensured through **decentralization**, **encryption**, and **consensus** mechanisms. Millions of nodes globally store validated data copies, and transactions are verified by either **miners (PoW)** or **validators (PoS)**.

Because these validators operate worldwide, there is no single point of failure, making the **Blockchain network** highly secure.

Hashing in Blockchain

Hash encryption is critical to **Blockchain security** due to its **irreversibility**. Each block's data is encrypted with a unique hash, and it also includes the previous block's hash.

If someone changes a block's content, its hash changes, causing a mismatch with the next block's stored hash — leading to rejection by the network.

Moreover, nodes continuously verify hashes. Any inconsistency causes the network to discard the altered data.

In PoW, altering even one block demands enormous computational power, making tampering practically **impossible**.

Decentralization of Blockchain

Unlike centralized systems with a **single point of failure**, **Blockchain** is governed by millions of nodes worldwide. In centralized systems, all data is at risk if the server is compromised.

But in a decentralized **Blockchain network**, data is distributed and stored in various nodes, making data theft or manipulation unfeasible.

Consensus Mechanism

To validate transactions and add new blocks, **network-wide agreement (consensus)** is essential. In **PoW**, miners solve complex math problems to create blocks, making attacks **expensive and complicated**.

In **PoS**, validators are selected based on staked coins, and tampering results in loss of their stake, discouraging manipulation.

How Blockchain Works?

Node confirmation is required to register, validate, and execute a transaction in **Blockchain**. The user signs the transaction with a private key and sends it to the "**unconfirmed transaction pool**."

The digital signature confirms the owner, while nodes validate the signature using the public key.

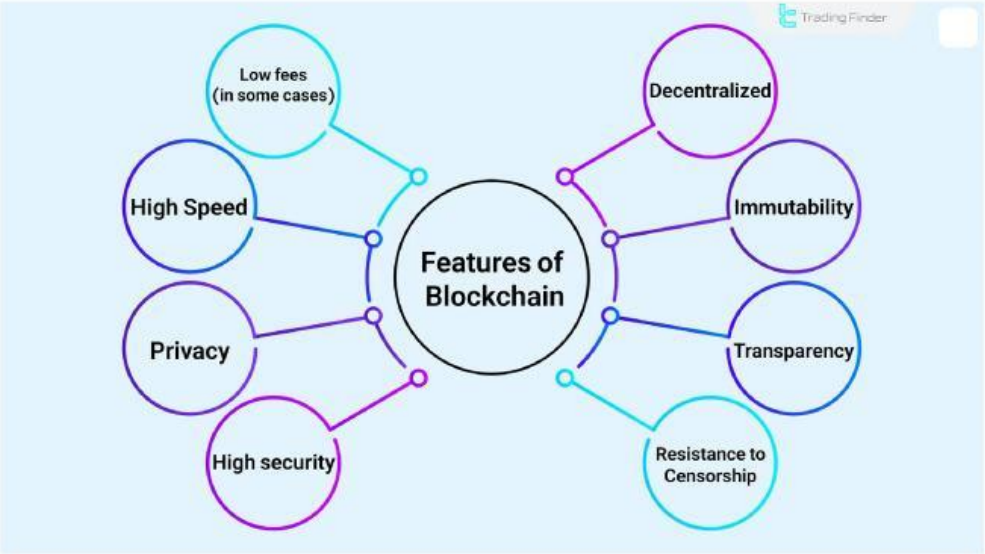
Miners or validators then confirm the transaction by checking the wallet balance and signature, and usually select high-fee transactions to add to a new block.

Steps to Create a New Block and Confirm a Transaction:

1. **Data collection:** Nodes gather data from users. Each transaction must be validated — wallet balance and digital signature are checked;
2. **Transaction selection:** Miners pick some transactions, usually those with higher fees;
3. **Broadcast to nodes:** The block is reviewed independently by other nodes;
4. **Node confirmation & addition:** After confirmation, the block is added to the **Blockchain network**, and the transaction is finalized.

In Which Industries is Blockchain Network Used?

Blockchain is most known for its role in the **cryptocurrency industry**, but thanks to its unique features, the **Blockchain network** can be applied in any field that requires secure data storage.



Storing information and transferring money in healthcare, government, finance, and banking sectors is possible through the Blockchain network

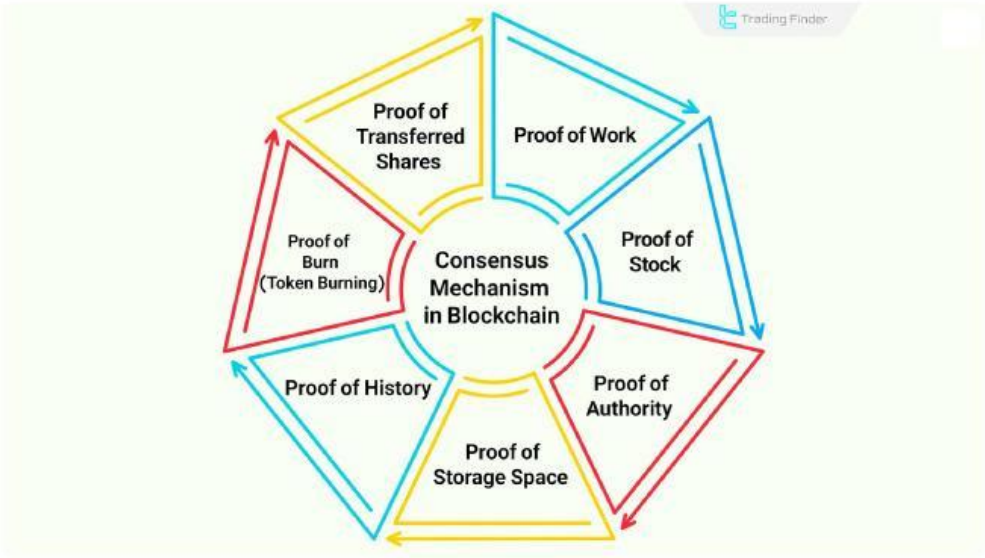
Some Applications of Blockchain in Different Industries:

- **Finance and Banking Industry**: In banking, collaborations like Ripple have significantly accelerated international transactions. Also, decentralized lending is possible via Blockchain;
- **Cryptocurrency Industry**: Blockchain is the core infrastructure for crypto transactions and records all trades;
- **Supply Chain**: Blockchain enables product tracking from production to consumption. For example, IBM Food Trust uses Blockchain to track food products;
- **Healthcare**: Some hospitals use Blockchain for secure storage and sharing of patient medical records;
- **Government Services**: Secure electronic voting, land/property registration, and digital identity management (like tamper-proof passports);
- **Art and Intellectual Property**: Through **NFTs**, ownership of artworks is recorded on Blockchain, allowing creators to claim rights without lawyers.

Consensus Mechanisms in Blockchain

The **consensus mechanism** determines how information is validated in a blockchain. In each mechanism, **nodes** must reach consensus through **different methods** to **confirm data**; for example, in **PoW** (Proof of Work), this process involves **purchasing hardware** and **solving complex mathematical problems**.

Consensus mechanisms differ in terms of **energy consumption**, **degree of decentralization**, **security**, **scalability**, and **node** rewards. For instance, **PoW** offers **very high security**, but in some cases, **data validation** (scalability) is **slower** than other mechanisms.



Types of consensus mechanisms vary in scalability, security, energy use, and decentralization

Types of Blockchain Consensus Mechanisms:

- **Proof of Work (PoW)**: Miners solve **hash puzzles** to **create blocks**. It's secure but **energy-intensive** and **less scalable**;
- **Proof of Stake (PoS)**: Validators are chosen based on **staked coins**. It's **more scalable** and **energy-efficient** than PoW;
- **Delegated Proof of Stake (DPoS)**: Users vote for representatives to validate transactions. It **combines democracy** and **decentralization**, though voting manipulation is a risk;
- **Proof of Authority (PoA)**: Only **pre-approved nodes** can validate data. It offers high scalability and suits **private Blockchain networks**;
- **Proof of History (PoH)**: Unlike **PoW/PoS**, **PoH** validates transactions through immutable, **timestampedhash records**;
- **Proof of Space (PoSpace)**: Users **share storage space** with the network to earn validation rights. **Low energy use** is its key advantage;
- **Proof of Burn (PoB)**: Users **burn coins** to gain mining rights. It reduces supply and boosts value but wastes resources;

- **Byzantine Fault Tolerance (BFT):** Transactions are validated by a two-thirds majority of nodes and works even with some malicious participants — suitable for **private**, **trusted** networks.

Types of Blockchain Networks

Blockchain networks differ based on their applications and characteristics. For example, a **public blockchain** is **decentralized**, and data is **publicly** and **transparently accessible**; in a **public blockchain**, anyone can become a **node**, making it suitable for cryptocurrencies like Bitcoin.

On the other hand, data in a **private blockchain network** is only accessible to **specific individuals**, and only **designated participants** can become nodes. This type of blockchain is suitable for **businesses**. In the following, we will explore the **types of blockchains** along with their applications and features.

Public Blockchains

Public blockchains are **decentralized**; anyone can perform transactions or become a node **without permission**. In a **public blockchain**, data is **visible to everyone** and offers **a high level of transparency**. Additionally, the information is **immutable**.

Public blockchains are **resistant to censorship and attacks**, and they provide **very high security**. Moreover, using a public blockchain **eliminates the need for trust or intermediaries**.
This type of **Blockchain network** is used in **Bitcoin** and **Ethereum**, and has been **widely adopted**.

Private Blockchains

In contrast to public blockchains, **private blockchains** are **centralized**, **controlled by a single organization**, and **require permission** to use. In a **private blockchain**, only **pre-approved nodes** are authorized to validate transactions, and transactions are **confirmed and executed very quickly**.

The **high speed** of private blockchains compared to public ones is due to the **absence of numerous nodes** and the **elimination of mining competition**.

Consortium Blockchains

Consortium blockchains are managed by **multiple organizations** and combine **decentralized approaches with centralized control**.

Nodes are **limited to pre-selected participants**, and **data access** may be **public in some cases** and **restricted in others**.

Applications of Consortium Blockchains:

- **International Banking**: The international banking network **RippleNet** uses a **consortium blockchain**. Transactions that take **several days in traditional SWIFT systems** are **confirmed and executed within seconds** on this network;
- **Supply Chains**: In supply chains, **consortium blockchains** are used to **track goods from origin to destination**.

Layered Blockchains

Layer 2 solutions are implemented in layered blockchains to **optimize scalability** or support **specific applications**. For example, the **Lightning Network** is a **Layer 2 solution** that allows for **faster transactions** than **Bitcoin's Layer 1**.

Hybrid Blockchains

Hybrid blockchains are **dual-layered**, classifying **public and private information** into their respective layers.

In a **hybrid blockchain**, the user performs the transaction in the **private layer**, while essential public data is made visible in the **public layer** to maintain transparency. Additionally, authorized **nodes** are responsible for validating the transaction.

Comparison of Blockchain Types

Feature	Public Blockchain	Private Blockchain	Consortium Blockchain	Hybrid Blockchain
Access	Anyone	Authorized Members	Recognized Organizations	Public + Private (Adjustable)
Centralization	Decentralized	Centralized	Semi-decentralized	Configurable
Consensus Mechanism	PoW, PoS, DPoS	PoA, PBFT	PBFT, RAFT	Hybrid
Transaction Speed	Low	High	Very High	Medium
Privacy	Public Data	Confidential Data	Members Only	Mixed & Configurable
Scalability	Limited	High	High	Good

Note: **Hybrid Consensus Mechanism** combines multiple consensus types (e.g., PoW + PoS) to leverage the advantages of both — such as security from **PoW** and efficiency from **PoS**.

Conclusion

Blockchain is a database that enables **immutable** and **decentralized** information storage. Based on its features. various **Blockchain networks** exist with different benefits. drawbacks. and use cases.

Public blockchains like Bitcoin and Ethereum are valued for **transparency** and **security** in crypto, while **private blockchains** allow only **authorized nodes** to validate, fitting for enterprises.

Each **Blockchain network** employs different **consensus mechanisms** to confirm transactions. For example, **PoW** is secure but less scalable and energy-intensive.

Source:

Our Website link :

https://tradingfinder.com/education/crypto/what-is-blockchain/

All Cryptocurrency Education :

https://tradingfinder.com/education/crypto/

TradingFinder Support Team (Telegram):

https://t.me/TFLABS