Blockchain

Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network. A blockchain database stores data in blocks that are linked together in a chain. The data is chronologically consistent because you cannot modify the chain without consensus from the network. As a result, you can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts, and other transactions. The system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of these transactions.

Traditional database technologies present several challenges for recording financial transactions. For instance, consider the sale of a property. Once the money is exchanged, ownership of the property is transferred to the buyer. Individually, both the buyer and the seller can record the monetary transactions, but neither source can be trusted. The seller can easily claim they have not received the money even though they have, and the buyer can equally argue that they have paid the money even if they haven’t.

To avoid potential legal issues, a trusted third party has to supervise and validate transactions. The presence of this central authority not only complicates the transaction but also creates a single point of vulnerability. If the central database was compromised, both parties could suffer.

Blockchain mitigates such issues by creating a decentralized, tamper-proof system to record transactions. In the property transaction scenario, blockchain creates one ledger each for the buyer and the seller. All transactions must be approved by both parties and are automatically updated in both of their ledgers in real time. Any corruption in historical transactions will corrupt the entire ledger. These properties of blockchain technology have led to its use in various sectors, including the creation of digital currency like Bitcoin.

Features of Blockchain:

* Decentralization in blockchain refers to transferring control and decision making from a centralized entity (individual, organization, or group) to a distributed network. Decentralized blockchain networks use transparency to reduce the need for trust among participants. These networks also deter participants from exerting authority or control over one another in ways that degrade the functionality of the network.
* Immutability means something cannot be changed or altered. No participant can tamper with a transaction once someone has recorded it to the shared ledger. If a transaction record includes an error, you must add a new transaction to reverse the mistake, and both transactions are visible to the network.
* A blockchain system establishes rules about participant consent for recording transactions. You can record new transactions only when the majority of participants in the network give their consent.(consensus)
* Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.
* With blockchain, as a member of a members-only network, you can rest assured that you are receiving accurate and timely data, and that your confidential blockchain records will be shared only with network members to whom you have specifically granted access.(greater trust)
* With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated. And to speed transactions, a set of rules — called a smart contract — can be stored on the blockchain and executed automatically.

Consensus mechanisms form the backbone of all cryptocurrency blockchains, and are what make them secure. Before delving into the different consensus mechanisms, let’s first define what it means for blockchains to achieve consensus.

In order to guarantee that all participants in a blockchain network agree on a single version of history, blockchain networks like Bitcoin and Ethereum implement what’s known as consensus mechanisms (also known as consensus protocols or consensus algorithms). These mechanisms aim to make the system fault-tolerant.

Consensus is the process by which a group of peers — known as ‘nodes’ — on a network determine which blockchain transactions are valid and which are not. Consensus mechanisms are the methodologies used to achieve this agreement. It’s these sets of rules that help to protect networks from malicious behaviour and hacking attacks.

There are many different types of consensus mechanisms, depending on the blockchain and its application. While they differ in their energy usage, security, and scalability, they all share one purpose: to ensure that records are true and honest. Here’s an overview of some of the best-known types of consensus mechanisms used by distributed systems to reach consensus.

Consensus mechanisms types:

1. Used by Bitcoin and many other public blockchains, Proof of Work (PoW) was the very first consensus mechanism created. It is generally regarded as the most reliable and secure of all the consensus mechanisms, though [concerns over scalability](https://cointelegraph.com/news/proof-of-work-vs-proof-of-stake-for-scaling-blockchains) are rife. While the term ‘proof of work’ was first coined in the early 1990s, it was Bitcoin founder Satoshi Nakamoto who first applied the technology in the context of digital currencies.

In PoW, ‘miners’ essentially compete against one another to solve extremely complex computational puzzles using high-powered computers. The first to come up with the 64-digit hexadecimal number (‘hash’) earns the right to form the new block and confirm the transactions. The successful miner is also rewarded ​​with a predetermined amount of crypto, known as a ‘block reward’.

As it requires large amounts of computational resources and energy in order to generate new blocks, the operating costs behind PoW are notoriously high. This acts as a barrier of entry for new miners, leading to concerns about centralisation and scalability limitations.

But it’s not just the costs that are high. The most common criticism of PoW is the impact the electrical consumption has on the environment. This has led many to seek more sustainable, energy-efficient consensus protocols, such as Proof of Stake (PoS).

2. As the name suggests, this popular method of consensus revolves around a process known as ‘[staking](https://crypto.com/university/staking-crypto)‘. In a Proof of Stake (PoS) system, ‘validators’ pledge a stake of digital currency for a chance to be randomly chosen to validate a block, which earns them a reward. The process is not unlike a lottery, whereby the more coins staked, the better the odds. Unlike in PoW, where miners are incentivised by block rewards (newly generated coins), those who contribute to the PoS system simply earn a transaction fee.

PoS is seen as a more sustainable and environmentally friendly alternative to PoW, and one that’s more secure against 51% attacks. However, as the system favours entities with a higher number of tokens, PoS has drawn criticism for its potential to lead to centralisation. Prominent PoS platforms include Ethereum — which [transitioned from PoW to PoS](https://crypto.com/university/what-is-the-ethereum-merge) in 2022 — Cardano (ADA), Solana (SOL), and Tezos (XTZ).

3. A modification of the PoS consensus mechanism, Delegated Proof of Stake (DPoS) relies upon a reputation-based voting system to achieve consensus. Users of the network ‘vote’ to select ‘witnesses’ (also known as ‘block producers’) to secure the network on their behalf. Only the top tier of witnesses (those with the most votes) earn the right to validate blockchain transactions.

To vote, users add their tokens to a staking pool. Votes are then weighted according to the size of each voter’s stake — the more skin in the game, the more voting power. Elected witnesses who successfully verify transactions in a block receive a reward, which is usually shared with those who voted for them.

Witnesses in the top tier are always at risk of being replaced by those deemed more trustworthy, who get more votes. They can even be voted out if they fail to fulfil their responsibilities or try to validate fraudulent transactions. This helps to incentivise witnesses to remain honest at all times, ensuring the integrity of the blockchain.

Though less prevalent than PoS, DPoS is regarded by many as being more efficient, democratic, and financially inclusive than its predecessor. It is used by Lisk (LSK), EOS.IO (EOS), Steem (STEEM), BitShares (BTS), and Ark (ARK).

Key components of Blockchain technology:

1.A distributed ledger is the shared database in the blockchain network that stores the transactions, such as a shared file that everyone in the team can edit. In most shared text editors, anyone with editing rights can delete the entire file. However, distributed ledger technologies have strict rules about who can edit and how to edit. You cannot delete entries once they have been recorded.

2.Companies use smart contracts to self-manage business contracts without the need for an assisting third party. They are programs stored on the blockchain system that run automatically when predetermined conditions are met. They run if-then checks so that transactions can be completed confidently. For example, a logistics company can have a smart contract that automatically makes payment once goods have arrived at the port.

3.Public key cryptography is a security feature to uniquely identify participants in the blockchain network. This mechanism generates two sets of keys for network members. One key is a public key that is common to everyone in the network. The other is a private key that is unique to every member. The private and public keys work together to unlock the data in the ledger.

For example, John and Jill are two members of the network. John records a transaction that is encrypted with his private key. Jill can decrypt it with her public key. This way, Jill is confident that John made the transaction. Jill's public key wouldn't have worked if John's private key had been tampered with.

Each blockchain network has various participants who play these roles, among others:

* **Blockchain users.** Participants (typically business users) with permissions to join the blockchain network and conduct transactions with other network participants.
* **Regulators.** Blockchain users with special permissions to oversee the transactions happening within the network.
* **Blockchain network operators.** Individuals who have special permissions and authority to define, create, manage, and monitor the blockchain network.
* **Certificate authorities.** Individuals who issue and manage the different types of certificates required to run a permissioned blockchain.

Blockchain is a special type of database management system that has more features than a regular database. We describe some significant differences between a traditional database and a blockchain in the following list:

* Blockchains decentralize control without damaging trust in the existing data. This is not possible in other database systems.
* Companies involved in a transaction cannot share their entire database. But in blockchain networks, each company has its copy of the ledger, and the system automatically maintains consistency between the two ledgers.
* Although in most database systems you can edit or delete data, in blockchain you can only insert data.

The term cloud refers to computing services that can be accessed online. You can access Software as a Service (SaaS), Product as a Service (PaaS), and Infrastructure as a Service (IaaS) from the cloud. Cloud providers manage their hardware and infrastructure and give you access to these computing resources over the internet. They provide many more resources than just database management.If you want to join a public blockchain network, you need to provide your hardware resources to store your ledger copy. You could use a server from the cloud for this purpose too. Some cloud providers also offer complete Blockchain as a Service (BaaS) from the cloud.

Bitcoin and blockchain might be used interchangeably, but they are two different things. Since Bitcoin was an early application of blockchain technology, people inadvertently began using Bitcoin to mean blockchain, creating this misnomer. But blockchain technology has many applications outside of Bitcoin.

Bitcoin is a digital currency that operates without any centralized control. Bitcoins were originally created to make financial transactions online but are now considered digital assets that can be converted to any other global currency, like USD or euros. A public Bitcoin blockchain network creates and manages the central ledger.

**Bitcoin network**

A public ledger records all Bitcoin transactions, and servers around the world hold copies of this ledger. The servers are like banks. Although each bank knows only about the money its customers exchange, Bitcoin servers are aware of every single Bitcoin transaction in the world.

Anyone with a spare computer can set up one of these servers, known as a node. This is like opening your own Bitcoin bank instead of a bank account.

**Bitcoin mining**

On the public Bitcoin network, members mine for cryptocurrency by solving cryptographic equations to create new blocks. The system broadcasts each new transaction publicly to the network and shares it from node to node. Every ten minutes or so, miners collect these transactions into a new block and add them permanently to the blockchain, which acts like the definitive account book of Bitcoin.

Mining requires significant computational resources and takes a long time due to the complexity of the software process. In exchange, miners earn a small amount of cryptocurrency. The miners act as modern clerks who record transactions and collect transaction fees.

All participants across the network reach a consensus on who owns which coins, using blockchain cryptography technology.

There are four main types of decentralized or distributed networks in the blockchain:

### Public blockchain networks

Public blockchains are permissionless and allow everyone to join them. All members of the blockchain have equal rights to read, edit, and validate the blockchain. People primarily use public blockchains to exchange and mine cryptocurrencies like Bitcoin, Ethereum, and Litecoin.

* Decentralization: No central authority; network consensus mechanisms govern operations.
* Transparency: All transactions are visible to anyone on the network.
* Participation: Anyone can join as a node, send transactions, or participate in the consensus process

### Private blockchain networks

A single organization controls private blockchains, also called managed blockchains. The authority determines who can be a member and what rights they have in the network. Private blockchains are only partially decentralized because they have access restrictions. Ripple, a digital currency exchange network for businesses, is an example of a private blockchain.

* Efficiency: Typically faster and more scalable than public blockchains due to the limited number of nodes.
* Privacy: Transactions can be kept confidential within the network participants.

### Hybrid blockchain networks

Hybrid blockchains combine elements from both private and public networks. Companies can set up private, permission-based systems alongside a public system. In this way, they control access to specific data stored in the blockchain while keeping the rest of the data public. They use smart contracts to allow public members to check if private transactions have been completed. For example, hybrid blockchains can grant public access to digital currency while keeping bank-owned currency private.

### Consortium blockchain networks

A group of organizations governs consortium blockchain networks. Preselected organizations share the responsibility of maintaining the blockchain and determining data access rights. Industries in which many organizations have common goals and benefit from shared responsibility often prefer consortium blockchain networks. For example, the Global Shipping Business Network Consortium is a not-for-profit blockchain consortium that aims to digitize the shipping industry and increase collaboration between maritime industry operators.

* Governance: Controlled by a consortium of organizations, not just one, making it more decentralized than a private blockchain but less so than a public one.
* Privacy and Efficiency: Can be configured to keep transactions private among consortium members while still offering higher transaction speeds and scalability.
* Use Cases: Often used in industries where multiple stakeholders need to securely and efficiently share information, such as banking, supply chain, and healthcare.

How does the blockchain work?

**Step 1 – Record the transaction**

A blockchain transaction shows the movement of physical or digital assets from one party to another in the blockchain network. It is recorded as a data block and can include details like these:

* Who was involved in the transaction?
* What happened during the transaction?
* When did the transaction occur?
* Where did the transaction occur?
* Why did the transaction occur?
* How much of the asset was exchanged?
* How many pre-conditions were met during the transaction?

**Step 2 – Gain consensus**

Most participants on the distributed blockchain network must agree that the recorded transaction is valid. Depending on the type of network, rules of agreement can vary but are typically established at the start of the network.

**Step 3 – Link the blocks**

Once the participants have reached a consensus, transactions on the blockchain are written into blocks equivalent to the pages of a ledger book. Along with the transactions, a cryptographic hash is also appended to the new block. The hash acts as a chain that links the blocks together. If the contents of the block are intentionally or unintentionally modified, the hash value changes, providing a way to detect data tampering.

Thus, the blocks and chains link securely, and you cannot edit them. Each additional block strengthens the verification of the previous block and therefore the entire blockchain. This is like stacking wooden blocks to make a tower. You can only stack blocks on top, and if you remove a block from the middle of the tower, the whole tower breaks.

**Step 4 – Share the ledger**

The system distributes the latest copy of the central ledger to all participants.

The term blockchain protocol refers to different types of blockchain platforms that are available for application development. Each blockchain protocol adapts the basic blockchain principles to suit specific industries or applications. Some examples of blockchain protocols are provided in the following subsections:

**Hyperledger fabric**

[Hyperledger Fabric](https://aws.amazon.com/blockchain/what-is-hyperledger-fabric/) is an open-source project with a suite of tools and libraries. Enterprises can use it to build private blockchain applications quickly and effectively. It is a modular, general-purpose framework that offers unique identity management and access control features. These features make it suitable for various applications, such as track-and-trace of supply chains, trade finance, loyalty and rewards, and clearing settlement of financial assets.

**Ethereum**

[Ethereum](https://aws.amazon.com/blockchain/what-is-ethereum/) is a decentralized open-source blockchain platform that people can use to build public blockchain applications. Ethereum Enterprise is designed for business use cases.

**Corda**

Corda is an open-source blockchain project designed for business. With Corda, you can build interoperable blockchain networks that transact in strict privacy. Businesses can use Corda's smart contract technology to transact directly, with value. Most of its users are financial institutions.

**Quorum**

Quorum is an open-source blockchain protocol that is derived from Ethereum. It is specially designed for use in a private blockchain network, where only a single member owns all the nodes, or in a consortium blockchain network, where multiple members each own a portion of the network.