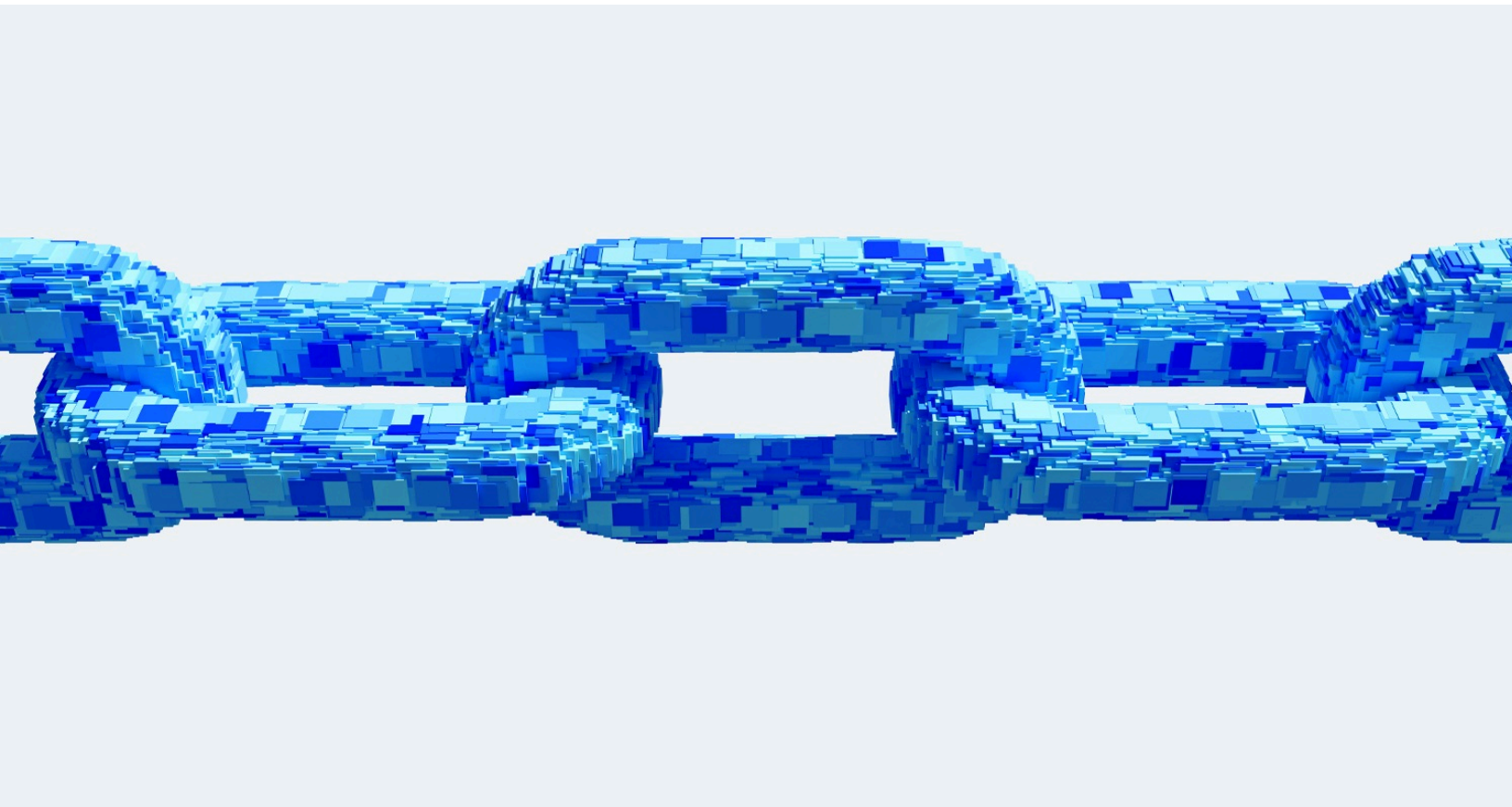


McKinsey Explainers

# What is blockchain?

Blockchain is a secure database shared across a network of participants, where up-to-date information is available to all participants at the same time.



**Blockchain is one** of the major tech stories of the past decade. But beneath the surface chatter there's not always a deep, clear understanding of what blockchain is, how it works, or what it's for. Despite its reputation for impenetrability, the basic idea behind blockchain is pretty simple. And it has major potential to [change industries from the bottom up](#).

Put simply, blockchain is a technology that enables the secure sharing of information. Data, obviously, is stored in a database. Transactions are recorded in an account book called a ledger. A blockchain is a type of *distributed* database or ledger, which means the power to update a blockchain is distributed between the nodes, or participants, of a public or private computer network. This is known as distributed ledger technology (DLT). Nodes are rewarded with digital tokens or currency to make updates to blockchains.

Blockchain allows for the permanent, immutable, and transparent recording of data and transactions. This, in turn, makes it possible to exchange anything that has value, whether that's a physical item or something more intangible.

A blockchain has [three central attributes](#):

- First, a blockchain database must be cryptographically secure. That means you need two cryptographic keys to access or add data on the database: a public key, which is basically the address in the database, and the private key, which is an individualized key that must be authenticated by the network.
- Next, a blockchain is a *digital* log or database of transactions, meaning it happens fully online.

- And finally, a blockchain is a database that is shared across a public or private network. One of the most well-known public blockchain networks is the [Bitcoin blockchain](#). Anyone can open a Bitcoin wallet or become a node on the network. Other blockchains are private networks. These are more applicable to [banking and fintech](#), where people need to know exactly who is participating, who has access to data, and who has a private key to the database. Other types of blockchains include consortium blockchains and hybrid blockchains, both of which combine different aspects of public and private blockchains.

For all its potential, blockchain has yet to become the game changer some expected. So how can we know what's real and what's just hype? And can companies still use blockchain to build efficiency, increase security, and create value? Read on to find out.

*Learn more about McKinsey's [Financial Services Practice](#).*

## How does blockchain work?

A deeper dive may help in understanding [how blockchain and other DLTs work](#).

When data on a blockchain is accessed or altered, the record is stored in a "block" alongside the records of other transactions. Stored transactions are encrypted via unique, unchangeable hashes. New data blocks don't overwrite old ones; they are "chained" together so any changes can be monitored.

These blocks of encrypted data are permanently “chained” to one another, and transactions are recorded sequentially and indefinitely, creating a perfect audit history that allows visibility into past versions of the blockchain.

When new data is added to the network, the majority of nodes must verify and confirm the legitimacy of the new data based on permissions or economic incentives, also known as [consensus mechanisms](#). When a consensus is reached, a new block is created and attached to the chain. All nodes are then updated to reflect the blockchain ledger.

In a [public blockchain network](#), the first node to credibly prove the legitimacy of a transaction receives an economic incentive. This process is called “mining.”

Here’s a theoretical example to help illustrate how blockchain works. Imagine that someone is looking to buy a concert ticket on the resale market. This person has been scammed before by someone selling a fake ticket, so she decides to try one of the blockchain-enabled decentralized ticket exchange websites that have been created in the past few years. On these sites, every ticket is assigned a unique, immutable, and verifiable identity that is tied to a real person. Before the concertgoer purchases her ticket, the majority of the nodes on the network validate the seller’s credentials, ensuring that the ticket is in fact real. She buys her ticket and enjoys the concert.

## What is proof of work and how is it different from proof of stake?

Remember the idea of consensus mechanisms? There are two ways blockchain nodes arrive at a consensus: through private blockchains, where

trusted corporations are the gatekeepers of changes or additions to the blockchain, or through public, mass-market blockchains.

Most public blockchains arrive at consensus by either a proof-of-work or [proof-of-stake](#) system. In a proof-of-work system, the first node, or participant, to verify a new data addition or transaction on the digital ledger receives a certain number of tokens as a reward. To complete the verification process, the participant, or “miner,” must solve a cryptographic question. The first miner who solves the puzzle is awarded the tokens.

Originally, people on various blockchains mined as a hobby. But because this process is [potentially lucrative](#), blockchain mining has been industrialized. These proof-of-work blockchain-mining pools have attracted attention for the amount of energy they consume.

In September 2022, Ethereum, an open-source cryptocurrency network, addressed concerns about energy usage by upgrading its software architecture to a proof-of-stake blockchain. Known simply as “the Merge,” this event is seen by cryptophiles as a banner moment in the history of blockchain. With proof of stake, investors deposit their crypto coins in a shared pool in exchange for the chance to earn tokens as a reward. In proof-of-stake systems, miners are scored based on the number of native protocol coins they have in their digital wallets and the length of time they have had them. The miner with the most coins at stake has a greater chance to be chosen to validate a transaction and receive a reward.

*Learn more about [proof of stake](#).*

## How can businesses benefit from blockchain?

Blockchain and DLTs could create new opportunities for businesses by decreasing risk and reducing compliance costs, creating more cost-efficient transactions, driving automated and secure contract fulfillment, and increasing network transparency. Let's break it down further:

- *Reduced risk and lower compliance costs.* Banks rely on “know your customer” (KYC) processes to bring customers on board and retain them. But many existing KYC processes are outdated and drive costs of as much as \$500 million per year, per bank. A new DLT system might require only one KYC verification per customer, driving efficiency gains, cost reduction, and improved transparency and customer experience.
- *Cost-efficient transactions.* Digitizing records and issuing them on a universal ledger can help save significant time and costs, which can matter more in some trades than in others. In a letter of credit deal, for example, two companies opted for a paperless solution and used blockchain to trade nearly \$100,000 worth of butter and cheese—clearly a time-sensitive transaction. By doing so, a process that previously took up to ten days was reduced to less than four hours—from issuing to approving the letter of credit.
- *Automated and secure contract fulfillment.* Smart contracts are sets of instructions coded into tokens issued on a blockchain that can self-execute under specific conditions. These can enable automated fulfillment of contracts. For example, one retailer wanted to streamline its supply-chain-management efforts, so it began recording all processes and actions, from

vendor to customer, and coding them into smart contracts on a blockchain. This effort not only made it easier to trace the provenance of food for safer consumption but also required less human effort and improved the ability to track lost products.

*Learn more about McKinsey's [Financial Services Practice](#).*

## How are blockchain, cryptocurrency, and decentralized finance connected?

Blockchain enables buyers and sellers to [trade cryptocurrencies online](#) without the need for banks or other intermediaries.

All digital assets, including cryptocurrencies, are based on blockchain technology. [Decentralized finance \(DeFi\)](#) is a group of applications in cryptocurrency or blockchain designed to replace current financial intermediaries with smart contract-based services. Like blockchain, DeFi applications are decentralized, meaning that anyone who has access to an application has control over any changes or additions made to it. This means that users potentially have more direct control over their money.

## What else can blockchain be used for?

Cryptocurrency is only the tip of the iceberg. Use cases for blockchain are expanding rapidly beyond person-to-person exchanges, especially as blockchain is paired with other emerging technologies. Examples of other blockchain use cases include the following:

- With blockchain, companies can create an indelible audit trail through a sequential and indefinite recording of transactions. This allows

for systems that keep static records (of land titles, for example) or dynamic records (such as the exchange of assets).

- Blockchain allows companies to track a transaction down to its current status. This enables companies to determine exactly where the data originated and where it was delivered, which helps to prevent data breaches.
- Blockchain supports smart contracts.

### What are some concerns around the future of blockchain?

While blockchain may be a [potential game changer](#), there are doubts emerging about its [true business value](#). One major concern is that for all the idea-stage use cases, hyperbolic headlines, and billions of dollars of investments, there remain [very few practical, scalable use cases](#) of blockchain.

One reason for this is the emergence of competing technologies. In the payments space, for example, blockchain isn't the only fintech disrupting the value chain—60 percent of the nearly \$12 billion invested in US fintechs in 2021 was focused on payments and lending. Given how complicated blockchain solutions can be—and the fact that [simple solutions are frequently the best](#)—blockchain may not always be the answer to payment challenges.

Looking ahead, some believe the value of blockchain lies in applications that democratize data, enable collaboration, and solve specific pain points. McKinsey research shows that these specific use cases are where blockchain holds the most potential, rather than those in financial services.

*Learn more about McKinsey's [Financial Services Practice](#).*

### How might blockchain evolve over time?

McKinsey estimates that there will be [two primary development horizons](#) for blockchain over the next decade:

- *Growth of blockchain as a service (BaaS)*. BaaS is a cloud-based service that builds digital products for DLT and blockchain environments without any setup requirements for infrastructure. This is currently being led by Big Tech companies.
- *Interoperability across blockchain networks and outside systems*. Increased interoperability will mean that disparate blockchain networks and external systems will be able to view, access, and share one another's data while maintaining integrity. Hardware standardization and scalable consensus algorithms will enable cross-network use cases—such as the [Internet of Things](#) on blockchain infrastructure.

These trends will be enabled partly because of increased pressure from regulators and consumers demanding greater supply chain transparency, and partly because of economic uncertainty, as consumers seek out independent, centrally regulated systems. And large corporations launching successful pilots will build confidence for consumers and other organizations.

Potential growth could be inhibited by a few factors: for one, several well-known applications have inherently limited scalability, including energy or infrastructure requirements. Further, uncertainty about regulatory or governance developments could keep consumers shy—for instance, if there is a lack of clarity on who will enforce smart contracts. The unresolved threat of cyberattacks also remains a fear for potential blockchain users. And finally, other tech trends—[namely AI](#)—have sucked up all the oxygen (and funding) in the room.

## What do NFTs have to do with blockchain?

Nonfungible tokens (NFTs) are minted on smart-contract blockchains such as Ethereum or Solana. NFTs represent unique assets that can't be replicated—that's the nonfungible part—and can't be exchanged on a one-to-one basis. These assets include anything from a Picasso painting to a digital “This is fine” dog meme. Because NFTs are built on top of blockchains, their unique identities and ownership can be verified through the ledger. With some NFTs, the owner receives a royalty every time the NFT is traded.

The NFT market [is extremely volatile](#): in 2021, one NFT created by the digital artist Mike Winkelmann, also known as Beeple, [was sold](#) at Christie's for \$69.3 million. But NFT sales have shrunk dramatically since summer 2022. As of 2023, according to a report from crypto analysis firm dappGamb1, [95 percent](#) of NFTs are worth practically nothing.

*Learn more about McKinsey's [Financial Services Practice](#).*

## How secure is blockchain?

Blockchain has been called a “[truth machine](#).” While it does eliminate many of the issues that arose in Web 2.0, such as piracy and scamming, it's not the be-all and end-all for digital security. The technology itself is essentially foolproof, but, ultimately, it is only as noble as the people using it and as reliable as the data they are adding to it.

A motivated group of hackers could leverage blockchain's algorithm to their advantage by taking control of more than half of the nodes on the network. With this simple majority, the hackers have consensus and thus the power to verify fraudulent transactions.

In 2022, hackers did exactly that, [stealing](#) more than \$600 million from the gaming-centered blockchain platform Ronin Network. This challenge, in addition to the obstacles regarding scalability and standardization, will need to be addressed. But there is still significant potential for blockchain, both for business and society.

*For a more in-depth exploration of these topics, see McKinsey's [“Blockchain and Digital Assets”](#) collection. Learn more about McKinsey's [Financial Services Practice](#)—and check out [blockchain-related job opportunities](#) if you're interested in working at McKinsey.*

*Articles referenced include:*

- [“What is Web3?”](#), October 10, 2023
- [“McKinsey Technology Trends Outlook 2023,”](#) July 20, 2023

Find more content like this on the  
**McKinsey Insights App**



Scan • Download • Personalize



- [“Forward Thinking on tech and the unpredictability of prediction with Benedict Evans,”](#) April 6, 2022, Janet Bush and [Michael Chui](#)
- [“Seven technologies shaping the future of fintech,”](#) November 9, 2021, Dick Fong, Feng Han, Louis Liu, John Qu, and Arthur Shek
- [“CBDC and stablecoins: Early coexistence on an uncertain road,”](#) October 11, 2021, Ian De Bode, [Matt Higginson](#), and Marc Niederkorn
- [“Blockchain and retail banking: Making the connection,”](#) June 7, 2019, [Matt Higginson](#), Atakan Hilal, and Erman Yugac
- [“Blockchain 2.0: What’s in store for the two ends—semiconductors \(suppliers\) and industrials \(consumers\)?,”](#) January 18, 2019, Gaurav Batra, Rémy Olson, Shilpi Pathak, Nick Santhanam, and Harish Soundararajan
- [“Blockchain’s Occam problem,”](#) January 4, 2019, [Matt Higginson](#), [Marie-Claude Nadeau](#), and Kausik Rajgopal
- [“Blockchain explained: What it is and isn’t, and why it matters,”](#) September 28, 2018, [Brant Carson](#) and [Matt Higginson](#)

*This article was updated in June 2024; it was originally published in December 2022.*

## Get to know and directly engage with McKinsey’s senior experts on blockchain

[Brant Carson](#) is a senior partner in McKinsey’s Vancouver office, and [Marie-Claude Nadeau](#) is a senior partner in the Bay Area office, where [Michael Chui](#) is a McKinsey Global Institute partner.

Designed by McKinsey Global Publishing  
Copyright © 2024 McKinsey & Company. All rights reserved.