Blockchain use cases and applications

A cryptocurrency is a digital or virtual currency secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Most cryptocurrencies exist on decentralized networks using blockchain technology—a distributed ledger enforced by a disparate network of computers.

A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.

Cryptocurrencies are digital or virtual currencies underpinned by cryptographic systems. They enable secure online payments without the use of third-party intermediaries. "Crypto" refers to the various encryption algorithms and cryptographic techniques that safeguard these entries, such as elliptical curve encryption, public-private key pairs, and hashing functions.

Central to the appeal and functionality of Bitcoin and other cryptocurrencies is blockchain technology. As its name indicates, a blockchain is essentially a set of connected blocks of information on an online ledger. Each block contains a set of transactions that have been independently verified by each validator on a network.

Every new block generated must be verified before being confirmed, making it almost impossible to forge transaction histories. The contents of the online ledger must be agreed upon by a network of individual nodes, or computers that maintain the ledger.1

Experts say that blockchain technology can serve multiple industries, supply chains, and processes such as online voting and crowdfunding. Financial institutions such as JPMorgan Chase & Co. ([JPM](https://www.investopedia.com/markets/quote?tvwidgetsymbol=jpm)) are using blockchain technology to lower transaction costs by streamlining payment processing.

Cryptocurrencies have attracted a [reputation as unstable investments](https://www.investopedia.com/tech/question-why-should-anyone-invest-crypto/) due to high investor losses due to scams, hacks, bugs, and volatility. Although the underlying cryptography and blockchain are generally secure, [the technical complexity](https://www.investopedia.com/analyze-crypto-6456223) of using and storing crypto assets can be a significant hazard to new users.

Advantages of Blockchain:

Cryptocurrencies represent [a new, decentralized paradigm for money](https://www.investopedia.com/tech/question-why-should-anyone-invest-crypto/). In this system, centralized intermediaries, such as banks and monetary institutions, are not necessary to enforce trust and police transactions between two parties. Thus, a system with cryptocurrencies eliminates the possibility of a single point of failure—such as a large financial institution setting off a cascade of global crises, such as the one triggered in 2008 by the failure of large investment banks in the U.S.

Cryptocurrencies promise to make transferring funds directly between two parties easier without needing a trusted third party like a bank or a credit card company. Such decentralized [transfers](https://www.investopedia.com/terms/t/transfer.asp) are secured by the use of [public keys](https://www.investopedia.com/terms/p/public-key.asp)and [private keys](https://www.investopedia.com/terms/p/private-key.asp) and different forms of incentive systems, such as [proof of work](https://www.investopedia.com/terms/p/proof-work.asp) or [proof of stake](https://www.investopedia.com/terms/p/proof-stake-pos.asp).

Because they do not use third-party intermediaries, cryptocurrency transfers between two transacting parties can be faster than standard money transfers. Flash loans in [decentralized finance](https://www.investopedia.com/decentralized-finance-defi-5113835) are an excellent example of such decentralized transfers. These loans, which are processed without backing collateral, can be executed within seconds and are used in trading.

Cryptocurrency investments can generate profits. Cryptocurrency markets have skyrocketed in value over the past decade, reaching almost $2 trillion. [Bitcoin was valued](https://www.investopedia.com/tech/how-much-worlds-money-bitcoin/) at more than $680 billion in crypto markets as of November 2023.20

The [remittance](https://www.investopedia.com/terms/r/remittance.asp) economy is testing one of cryptocurrency's most prominent use cases. Cryptocurrencies such as Bitcoin [serve as intermediate currencies](https://www.investopedia.com/tech/bitcoins-best-use-isnt-currency-its-overseas-remittances/) to streamline money transfers across borders. Thus, a fiat currency is converted to Bitcoin (or another cryptocurrency), transferred across borders, and subsequently converted to the destination fiat currency without third-party involvement.

Disadvantages of Blockchain:

Though they [claim to be an anonymous form of transaction](https://www.investopedia.com/tech/top-bitcoin-myths/), cryptocurrencies are pseudonymous. They leave a digital trail that agencies like the Federal Bureau of Investigation (FBI) can follow. This opens up the possibility for governments, authorities, and others to track financial transactions.

Cryptocurrencies have become a popular tool with criminals for nefarious activities such as money laundering and illicit purchases. The case of [Dread Pirate Roberts](https://www.investopedia.com/tech/ross-ulbricht-dark-net-pirate/), who ran a marketplace to sell drugs on the dark web, is already well known.21 Cryptocurrencies have also become a favorite of hackers who use them for ransomware activities.22

In theory, cryptocurrencies are meant to be decentralized, their wealth distributed between many parties on a blockchain. In reality, ownership is highly concentrated. Just 100 addresses hold roughly 15% of circulating bitcoin and total value.23

One of the conceits of cryptocurrencies is that anyone can mine them using a computer with an Internet connection. However, mining popular cryptocurrencies require considerable energy, sometimes as much energy as entire countries consume. The expensive energy costs and the unpredictability of mining have concentrated mining among large firms whose revenues run into billions of dollars.

Mining is the term used to describe the process of creating cryptocurrency. Transactions made with cryptocurrency need to be validated, and mining performs the validation and creates new cryptocurrency. Mining uses specialized hardware and software to add transactions to the blockchain.

Not all cryptocurrency comes from mining. For example, crypto that you can’t spend isn't mined. Instead, developers create the new currency through a hard fork. A hard fork creates a new chain in the blockchain. One fork follows the new path, and the other follows the old. Crypto you can’t mine is typically used for investments rather than purchases.

Cryptocurrency is available as coins or tokens. The difference between them is that tokens are assets that exist on a blockchain, while coins can be virtual, digital, or tangible. Coins are more like traditional money; a digital coin has its own blockchain.  Conversely, a token is created on an existing blockchain and can be used as currency or to represent asset ownership.

The first cryptocurrency introduced was Bitcoin, the most commonly traded one. Ethereum is the second most valuable cryptocurrency and can be used for complex transactions. Other more common cryptocurrencies, called altcoins, include Cardano, Solana, Dogecoin, and XRP.

How to get started with cryptocurrencies?

To start with cryptocurrency, you’ll need to **choose a broker or crypto exchange**. An exchange is an online platform where you can trade cryptocurrencies. Brokers use interfaces that interact with exchanges.

An exchange allows you to trade without a third party. Should you decide to use an exchange, you’ll need to find buyers for your cryptocurrency. A broker can do that for you. Here are the steps to start trading cryptocurrencies.

**1. Create and fund your account.**

When you’ve selected a broker or exchange, the next step is to open an account. You’ll want to keep a form of identification nearby since some platforms require it. Once you verify your identity, you can fund your account. Depending on your funding method, you may need to wait a few days for it to clear into your crypto account.

**2. Buy crypto.**

You can make your first cryptocurrency purchase when your account is set up and verified. You’ll find many options. You can purchase as much or as little as you’d like. When you’ve selected the one you want to start with, you’ll need to enter the ticker symbol and the amount you wish to purchase. Some of the more traded cryptocurrencies and their symbols are:

* Bitcoin (BTC)
* Ethereum (ETH)
* Dogecoin (DOGE)
* Tether (USDT)
* USD Coin (USDC)
* Uniswap (UNI)

**3. Select a storage method.**

Most often, you’ll store cryptocurrency in a wallet. When you purchase from a broker, you might not have an option regarding how you store your crypto. However, you can choose between a hot or cold wallet when purchasing through an exchange.

**Hot wallets**

A hot wallet offers online storage that you can access from a computer, phone, or tablet. A hot wallet has a security risk because it’s stored on the internet and is more susceptible to cyber-attacks.

**Cold wallets**

A cold wallet doesn’t connect to the internet. You can store your cryptocurrency in an external drive, such as a USB device. You’ll receive a keycode to keep in a safe place. Should you lose the keycode, you may lose your cryptocurrency.

Smart contracts

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

Smart contracts work by following simple “if/when…then…” statements that are written into code on a blockchain. A network of computers executes the actions  when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

Benefits of smart contracts:

* Speed, efficiency and accuracy-Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there’s no paperwork to process and no time spent reconciling errors that often result from manually filling in documents.
* Trust and transparency-Because there’s no third party involved, and because encrypted records of transactions are shared across participants, there’s no need to question whether information has been altered for personal benefit.
* Security-Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.
* Savings-Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays and fees.

Because smart contracts execute agreements, they can be used for many different purposes. One of the simplest uses is ensuring transactions between two parties occur, such as the purchase and delivery of goods. For example, a manufacturer needing raw materials can set up payments using smart contracts, and the supplier can set up shipments. Then, depending on the agreement between the two businesses, the funds could be transferred automatically to the supplier upon shipment or delivery.

Real estate transactions, stock and commodity trading, lending, corporate governance, supply chain, dispute resolution, and healthcare are only a few examples where smart contracts can be used.

The primary benefit of smart contracts is similar to the benefit of blockchain technology—they remove the need for third parties. Other benefits of this technology are:

* **Efficiency**: They speed up contract execution
* **Accuracy**: There can be no human error introduced
* **Immutability**: The programming cannot be altered

Some of the downfalls of smart contracts are:

* **Permanent**: They cannot be changed if there are mistakes
* **Human factor**: They rely on the programmer to ensure the code addresses the terms of the contract
* **Loopholes**: There may be loopholes in the coding, allowing for contracts to be executed in bad faith

Decentralized Applications (DApps)

Most apps today run on centralized networks, operated by a controlling authority.

For example, social media networks, banks, and streaming services hold your data on centralized [servers](https://brave.com/glossary/server/). When you access these apps, a request is sent to their servers, and the result is sent back to you, assuming your credentials (username and password) are valid. While this centralization is efficient, it generates huge amounts of user data. And that means unwanted exposure to hacks, creepy advertising, and [Big Tech](https://brave.com/glossary/big-tech/) companies like Google profiting off your data.

This is just how today’s [Web 2.0](https://brave.com/web3/versus-web1-and-web2/) Internet works. But things are quickly changing as we enter a [Web3](https://brave.com/web3/what-is-web3/) world.

Fortunately, Web 2.0’s shortcomings have raised data [security](https://brave.com/glossary/security/) awareness, generating more interest in peer-to-peer, decentralized solutions like [blockchain technology](https://brave.com/web3/intro-to-blockchain/). Blockchain networks are decentralized, eliminating the need for Big Tech intermediaries. Both shared consensus and automated smart contracts make this functionality possible.

We can contrast these two different systems with an example. For example, let’s say you want to send money to a friend:

With a DApp, you simply log in into your [crypto wallet](https://brave.com/web3/what-is-crypto-wallet/), select the amount you want to send and confirm the transaction; a smart contract takes over to complete the exchange. At the same time, blockchain validators work together to verify your transaction, generating a permanent record on a blockchain.

With Web 2.0, by contrast, the process of sending US dollars to your friend occurs on a centralized network. This means a bank handles every component of your transaction. They own the data, and they decide if the transaction is valid or not.

DApps are a collection of interconnected smart contracts—which are automatically executable bits of code on a blockchain network. Behind the scenes, each smart contract performs a specific function within the application. Think of smart contracts as programmable Lego blocks: By stacking and compiling smart contracts, developers can create entire decentralized apps.

While the front-end of a DApp may be indistinguishable from a traditional app, it’s the decentralized back-end that distinguishes DApps from their Web 2.0 counterparts. Instead of storing an app on centralized servers, DApps are stored across the many distributed computers—or “nodes”—that make up a blockchain network.

As a result, DApps share common attributes not found across centralized platforms:

No single point of failure: Unlike traditional apps, DApps are more reliable because blockchain networks span multiple nodes. If Instagram crashes, all users can lose access to the app because Instagram’s servers are centralized. It’s much less likely a DApp will go offline because each node would need to fail simultaneously to produce an outage.

Open source transparency: The decentralized nature of blockchain technology relies on [open-source](https://brave.com/glossary/open-source/) code that’s accessible to all network members. In an ecosystem without intermediaries, users must identify and verify each app to avoid scams and exploitative malware.

No central authority: Without a central authority, blockchains must utilize “consensus mechanisms”—complex systems for thousands of independent nodes to come together in agreement—to ensure the validity of all transactions. Whenever a DApp transaction occurs, the entire network is responsible for verification, as opposed to a single authority like a bank.

Utility tokens: Like how you pay to access traditional apps, many DApps integrate a utility token that guides platform economics. For example, many utility tokens enable decentralized governance, in-app transactions, and reward programs, among other use cases.

There are many different types of dApp that can be used by a range of users and industries. The [Ethereum](https://www.techopedia.com/definition/32571/ethereum-cryptocurrency) blockchain has become a popular platform to host dApps.

Decentralized finance (DeFi) apps: DeFi apps provide financial services without the need for traditional financial institutions to act as intermediaries. DeFi apps provide [lending and borrowing](https://www.techopedia.com/cryptocurrency/best-defi-lending-platforms), trading, and [yield farming](https://www.techopedia.com/cryptocurrency/best-yield-farming-crypto-platforms) options determined by smart contracts. DeFi apps include lending protocol Compound and decentralized exchange (DEX) Uniswap.

Decentralized social media: [Social platforms built on blockchains](https://www.techopedia.com/is-nostr-the-answer-to-social-network-concerns) aim to give users control over their data and provide rewards – often in the form of cryptocurrency tokens – for contributing content. Decentralized social media apps include microblogging platforms Mastodon and Steemit.

Decentralized gaming: [Games that run on blockchains](https://www.techopedia.com/cryptocurrency/best-crypto-games) can use [non-fungible tokens](https://www.techopedia.com/definition/34529/non-fungible-token-nft) (NFTs) to represent ownership of in-game items and reward users for their gameplay with cryptocurrencies. Developers can create content connected to a game, and players can vote on the way the game functions. Decentralized gaming apps include Axie Infinity, Gods Unchained, and The Sandbox.

Decentralized music: Decentralized music platforms provide an alternative to centralized streaming services, empowering artists to control their work and receive a fair share of the revenue they generate. Examples include Audius, OPUS, and BitSong.

Decentralized file storage: Decentralized storage apps use the peer-to-peer functionality of blockchain platforms to create a distributed network of storage space. This is designed to make them more secure, fault-tolerant, and resistant to data breaches than centralized storage. Decentralized storage apps include Storj, Filecoin, and Swarm.

Supply chain management: DApps for [supply chain management](https://www.techopedia.com/definition/23789/supply-chain-management-scm) enable businesses to track the movement of physical goods from the manufacturer to the consumer. They aim to enhance transparency and authenticity throughout the supply chain.

Disadvantages of DApps:

* Limited modification: Once deployed, a dApp is likely to require ongoing changes to make enhancements or correct bugs and security risks. However, it can be challenging for developers to update dApps because it is difficult to modify data and coding once they are published to the blockchain.
* Some blockchains use energy-intensive PoW consensus mechanisms, raising concerns about the environmental impact of the dApps that run on them.
* While immutability ensures data integrity, it also means that blockchain transactions are irreversible. This makes it difficult to retrieve lost or stolen funds or rectify mistakes.

Decentralized Identity Management System

Compared to centralized identity systems, which store all user information in a single database controlled by an authority, decentralized identity systems distribute user data across a network. This distribution improves security against cyberattacks because attackers need to compromise multiple nodes instead of just one central database. Additionally, it gives users more control over their data, allowing them to selectively grant access to specific credentials and attributes, boosting privacy and user empowerment.

Conversely, centralized systems consolidate all user identity data into one database overseen by a single entity, like a government or corporation. This raises privacy concerns as the authority has complete control and access to users’ information. Examples include government-issued IDs, passports, and social security numbers, which are more vulnerable to cyberattacks due to the single point of failure presented by the central database.

How does Decentralized Identity Management System work?

### ****1.Establishing a Decentralized Identity****

To begin, individuals can create their own decentralized identity through platforms offering [self-sovereign identity wallets](https://www.identity.com/digital-id-wallet-comprehensive-guide/), blockchain-based identity systems, or decentralized identity services. Notable platforms include Metamask, Sovrin, uPort, Microsoft’s ION, and protocols like ERC-725 and ERC-735.

Upon registration, you receive a [decentralized identifier (DID)](https://www.identity.com/what-are-decentralized-identifiers-dids/) – a unique, non-repeatable string of characters representing your digital presence. This DID, accompanied by a pair of cryptographic keys (public and private), forms the foundation of your decentralized identity. The public key is openly shared, acting as your identifiable marker, while the private key remains confidential, functioning as your secure access code.

### 2. Obtaining [Verified Credentials](https://www.identity.com/what-are-verifiable-credentials/)

Verified credentials are [digital certificates](https://www.identity.com/digital-certificates-key-to-secure-online-transactions/) issued by trusted entities (e.g., governments, educational institutions) affirming your identity details like name, age, or qualifications. These credentials are securely signed by the issuer and linked to your public key, ensuring their authenticity and your ownership.

These certificates also carry metadata detailing the issuing authority, issuance date, and any relevant expiration or revocation information, increasing their reliability and acceptance across various platforms.

### 3. Secure Storage of Identity Details

Your decentralized identity and credentials can be securely stored in [digital wallets](https://www.identity.com/digital-id-wallet-comprehensive-guide/). These wallets, often built on distributed ledger technology such as blockchain, provide a secure, tamper-resistant environment for your personal data, safeguarded further by [encryption](https://www.identity.com/encryption-what-is-it-and-how-it-enhances-data-security/).

### 4. Verifying Your Identity

Decentralized identity empowers you to verify your identity or share specific details without exposing unnecessary information. You control which credentials to present and the extent of information disclosed, enhancing privacy and reducing the vulnerabilities inherent in traditional identity verification methods.

This user-centric system not only streamlines identity management but also significantly enhances security and privacy, positioning decentralized identity as a cornerstone of modern digital interactions.

Blockchain in supply chains:

With blockchain, supply chain companies can document production updates to a single shared ledger, which provides complete data visibility and a single source of truth. Because transactions are always time-stamped and up to date, companies can query a product’s status and location at any point in time. This helps to combat issues like counterfeit goods, compliance violations, delays, and waste. In addition, immediate action can be taken during emergencies (e.g., in the case of product recalls), and regulatory compliance is ensured by the ledger audit trail.

Blockchain in education:

* Smart contracts can also be used to manage course content and distribution. They can automate the delivery of course materials, such as readings, videos, and quizzes, and track student progress and completion of assignments. This can help to reduce administrative workload and improve the overall organization of courses.
* The market for fake degrees (certificates) is increasing along with online learning. This is becoming a major concern for many businesses and educational institutions worldwide. So, a blockchain can easily solve this problem with certification management, where the universities can store the certificates on the blocks as immutable entries. Students may readily share these credentials using exact URLs in their email signatures, social media profiles, and resumes. Many blockchain development companies provide such certificate and identity management services. Since blockchain is decentralized, all the documents are stored in the blockchain and are immutable and verifiable since it is transparent.

Blockchain in healthcare:

* By encrypting patient data and storing it on a blockchain, healthcare providers can ensure the privacy and security of sensitive information, making it accessible only to authorized parties.
* A blockchain-based system can provide a comprehensive view of a patient's medical history in real-time, ensuring that healthcare providers have timely access to accurate information, which is crucial for making informed treatment decisions.