Click to verify

A blockchain is a distributed database or ledger shared across a computer network's nodes. They are best known for their crucial role in cryptocurrency systems, maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—meaning it cannot be altered. Since a block can't be changed, the only trust needed is at the point where a user or program enters data. This reduces the need for trusted third parties, such as auditors or other humans, who add costs and can make mistakes. Since Bitcoin's introduction in 2009, blockchain uses have exploded via the creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. Blockchain is a type of shared database that differs from a typical database in the way it stores information; blockchains store data in blocks linked together via cryptography.Different types of information can be stored on a blockchain, but the most common use has been as a transaction ledger. In Bitcoin's case, the blockchain is decentralized, so no single person or group has control—instead, all users collectively retain control.Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, transactions are permanently recorded and viewable to anyone. Investopedia / Xiaojie Liu You might be familiar with spreadsheets or databases. A blockchain is somewhat similar because it is a database where information is entered and stored. The key difference between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed. A blockchain consists of programs called scripts that conduct the tasks you usually would in a database: entering and accessing information, and saving and storing it somewhere. A blockchain is distributed, which means multiple copies are saved on many machines, and they must all match for it to be valid. The Bitcoin blockchain collects transaction information and enters it into a 4MB file called a block (different blockchains have different size blocks). Once the block is full, the block data is run through a cryptographic hash function, which creates a hexadecimal number called the block header hash. The hash is then entered into the following block header and encrypted with the other information in that block's header, creating a chain of blocks, hence the name "blockchain." Transactions follow a specific process, depending on the blockchain. For example, on Bitcoin's blockchain, if you initiate a transaction using your cryptocurrency wallet—the application that provides an interface for the blockchain—it starts a sequence of events. In Bitcoin, your transaction is sent to a memory pool, where it is stored and queued until a miner picks it up. Once it is entered into a block and the block fills up with transactions, it is closed, and the mining begins. Every node in the network proposes its own blocks in this way because they all choose different transactions. Each works on their own blocks, trying to find a solution to the difficulty target, using the "nonce," short for number used once. The nonce value is a field in the block header that is changeable, and its value incrementally increases with every mining attempt. If the resulting hash isn't equal to or less than the target hash, a value of one is added to the nonce, a new hash is generated, and so on. The nonce rolls over about every 4.5 billion attempts (which takes less than one second) and uses another value called the extra nonce as an additional counter. This continues until a miner generates a valid hash, winning the race and receiving the reward. Generating these hashes until a specific value is found is the "proof-of-work" you hear so much about—it "proves" the miner did the work. The sheer amount of work it takes to validate the hash is why the Bitcoin network consumes so much computational power and energy. Once a block is closed, a transaction is complete. However, the block is not considered confirmed until five other blocks have been validated. Confirmation takes the network about one hour to complete because it averages just under 10 minutes per block (the first block with your transaction and five following blocks multiplied by 10 equals 60 minutes). Not all blockchains follow this process. For instance, the Ethereum network randomly chooses one validator from all users with ether staked to validate blocks, which are then confirmed by the network. This is much faster and less energy intensive than Bitcoin's process. A blockchain allows the data in a database to be spread out among several network nodes—computers or devices running software for the blockchain—at various locations. This creates redundancy and maintains the fidelity of the data. For example, if someone tries to alter a record on one node, the other nodes would prevent it from happening by comparing block hashes. This way, no single node can alter information within the chain. Because of this distribution—and the encrypted proof that work was done—the blockchain data, such as transaction history, becomes irreversible. Such a record could be a list of transactions, but private blockchains can also hold a variety of other information like legal contracts, state identifications, or a company's inventory. Most blockchains wouldn't "store" these items directly; they would likely be sent through a hashing algorithm and represented on the blockchain by a token. Because of the decentralized nature of the Bitcoin blockchain, all transactions can be transparently viewed by downloading and inspecting them or by using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track a bitcoin wherever it goes. For example, exchanges have been hacked in the past, resulting in the loss of large amounts of cryptocurrency. While the hackers may have been anonymous—except for their wallet address—the crypto they extracted is easily traceable because the wallet addresses are stored on the blockchain. Of course, the records stored in the Bitcoin blockchain (as well as most others) are encrypted. This means that only the person assigned an address can reveal their identity. As a result, blockchain users can remain anonymous while preserving transparency. Blockchain technology achieves decentralized security and trust in several ways. To begin, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added to the end of the blockchain, previous blocks cannot be altered. A change in any data changes the hash of the block it was in. Because each block contains the previous block's hash, a change in one would change the following blocks. The network would generally reject an altered block because the hashes would not match. However, a change can be accomplished on smaller blockchain networks. Not all blockchains are 100% impenetrable. They are distributed ledgers that use code to create the security level they have become known for. If there are vulnerabilities in the coding, they can be exploited. A new and smaller chain might be susceptible to this kind of attack, but the attacker would need at least half of the computational power of the network (a 51% attack). On the Bitcoin and other larger blockchains, this is nearly impossible. By the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter. This is because the rate at which these networks hash is exceptionally rapid—the Bitcoin network hashed at a rate of around 640 exahashes per second (18 zeros) as of September 2024. The Ethereum blockchain is not likely to be hacked either—again, the attackers would need to control more than half of the blockchain's staked ether. As of September 2024, over 33.8 million ETH has been staked by more than one million validators. An attacker or a group would need to own over 17 million ETH, and be randomly selected to validate blocks enough times to get their blocks implemented. Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application. The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator, Satoshi Nakamoto, referred to it as "a new electronic cash system that's fully peer-to-peer, with no trusted third party." The key thing to understand is that Bitcoin uses blockchain as a means to transparently record a ledger of payments or other transactions between parties. Blockchain can be used to immutably record any number of data points. The data can be transactions, votes in an election, product inventories, state identifications, deeds to homes, and much more. Currently, tens of thousands of projects are looking to implement blockchains in various ways to help society other than just recording transactions—for example, as a way to vote securely in democratic elections. The nature of blockchain's immutability means that fraudulent voting would become far more difficult. For example, a voting system could work such that each country's citizens would be issued a single cryptocurrency or token. Each candidate could then be given a specific wallet address, and the voters would send their token or crypto to the address of whichever candidate they wish to vote for. The transparent and traceable nature of blockchain would eliminate the need for human vote counting and the ability of bad actors to tamper with physical ballots. Blockchains have been heralded as a disruptive force in the finance sector, especially with the functions of payments and banking. However, banks and decentralized blockchains are vastly different. To see how a bank differs from blockchain, let's compare the banking system to Bitcoin's blockchain implementation. As we now know, blocks on Bitcoin's blockchain store transactional data. Today, tens of thousands of other cryptocurrencies run on a blockchain. But it turns out that blockchain can be a reliable way to store other types of data as well. Some companies experimenting with blockchain include Walmart, Pfizer, AIG, Siemens, and Unilever, among others. For example, IBM has created its Food Trust blockchain to trace the journey that food products take to get to their locations. Why do this? The food industry has seen countless outbreaks of E. coli, salmonella, and listeria; in some cases, hazardous materials were accidentally introduced to foods. In the past, it has taken weeks to find the source of these outbreaks or the cause of sickness from what people are eating. Using blockchain allows brands to track a food product's route from its origin, through each stop it makes, to delivery. Not only that, but these companies can also now see everything else it may have come in contact with, allowing the identification of the problem to occur far sooner—potentially saving lives. This is one example of blockchain in practice, but many other forms of blockchain implementation exist or are being experimented with. Perhaps no industry stands to benefit from integrating blockchain into its business operations more than personal banking. Financial institutions only operate during business hours, usually five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see the money in your account. Even if you make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps. By integrating blockchain into banks, consumers might see their transactions processed in minutes or seconds—the time it takes to add a block to the blockchain, regardless of holidays or the time of day or week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. Given the sums involved, even the few days the money is in transit can carry significant costs and risks for banks. The settlement and clearing process for stock traders can take up to three days (or longer if trading internationally), meaning that the money and shares are frozen for that period. Blockchain can, in theory, drastically reduce that time. Blockchain forms the bedrock for cryptocurrencies like Bitcoin. This design also allows for easier cross-border transactions because it bypasses currency restrictions, instabilities, or lack of infrastructure by using a distributed network that can reach anyone with an internet connection. Healthcare providers can leverage blockchain to store their patients' medical records securely. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key so that they are only accessible to specific individuals, thereby ensuring privacy. If you have ever spent time in your local Recorder's Office, you will know that recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county's central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index. This process is not just costly and time-consuming, it is also prone to human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanently recorded. Proving property ownership can be nearly impossible in war-torn countries or areas with little to no government or financial infrastructure and no Recorder's Office. If a group of people living in such an area can leverage blockchain, then transparent and clear timelines of property ownership could be maintained. A smart contract is computer code that can be built into the blockchain to facilitate transactions. It operates under a set of conditions to which users agree. When those conditions are met, the smart contract conducts the transaction for the users. As in the IBM Food Trust example, suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of not only their products but also common labels such as "Organic," "Local," and "Fair Trade." As reported by Forbes, the food industry is increasingly adopting the use of blockchain to track the path and safety of food throughout the farm-to-user journey. As mentioned above, blockchain could facilitate a modern voting system. Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using blockchain in this way would make votes nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election. For all of its complexity, blockchain's potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above. But there are also some disadvantages. Transactions on the blockchain network are approved by thousands of computers and devices. This removes almost all people from the verification process, resulting in less human error and an accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain and not be accepted by the rest of the network. Typically, consumers pay a bank to verify a transaction or a notary to sign a document. Blockchain eliminates the need for third-party verification—and, with it, their associated costs. For example, business owners incur a small fee when they accept credit card payments because banks and payment-processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees. Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes significantly more difficult to tamper with. Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Financial institutions operate during business hours, usually five days a week—but a blockchain runs 24 hours a day, seven days a week, and 365 days a year. On some blockchains, transactions can be completed and considered secure in minutes. This is particularly useful for cross-border trades, which usually take much longer because of time zone issues and the fact that all parties must confirm payment processing. Many blockchain networks operate as public databases, meaning anyone with an internet connection can view a list of the network's transaction history. Although users can access transaction details, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like Bitcoin are fully anonymous; they are actually pseudonymous because there is a viewable address that can be associated with a user if the information gets out. Once a transaction is recorded, its authenticity must be verified by the blockchain network. After the transaction is validated, it is added to the blockchain block. Each block on the blockchain contains its unique hash and the unique hash of the block before it. Therefore, the blocks cannot be altered once the network confirms them. Many blockchains are entirely open source. This means that everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. However, it also means there is no real authority on who controls Bitcoin's code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile, then Bitcoin can be updated. Private or permission blockchains may not allow for public transparency, depending on how they are designed or their purpose. These types of blockchains might be made only for an organization that wishes to track data accurately without allowing anyone outside of the permissioned users to see it. Alternatively, there might come a point where publicly traded companies are required to provide investors with financial transparency through a regulator-approved blockchain reporting system. Using blockchains in business accounting and financial reporting would prevent companies from altering their financials to appear more profitable than they really are. Perhaps the most profound facet of blockchain and cryptocurrency is the ability for anyone, regardless of ethnicity, gender, location, or cultural background, to use it. According to The World Bank, an estimated 1.4 billion adults do not have bank accounts or any means of storing their money or wealth. Moreover, nearly all of these individuals live in developing countries where the economy is in its infancy and entirely dependent on cash. These people are often paid in physical cash. They then need to store this physical cash in hidden locations in their homes or other places, incentivizing robbers or violence. While not impossible to steal, crypto makes it more difficult for would-be thieves. Although blockchain can save users money on transaction fees, the technology is far from free. For example, the Bitcoin network's proof-of-work system to validate transactions consumes vast amounts of computational power. In the real world, the energy consumed by the millions of devices on the Bitcoin network is more than the country of Pakistan consumes annually. Some solutions to these issues are beginning to arise. For example, bitcoin-mining farms have been set up to use solar power, excess natural gas from fracking sites, or energy from wind farms. Bitcoin is a perfect case study of the inefficiencies of blockchain. Bitcoin's PoW system takes about 10 minutes to add a new block to the blockchain. At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS). Although other cryptocurrencies, such as Ethereum, perform better than Bitcoin, the complex structure of blockchain still limits them. Legacy brand Visa, for context, can process 65,000 TPS. Solutions to this issue have been in development for years. There are currently blockchain projects that claim tens of thousands of TPS. Ethereum is rolling out a series of upgrades that include data sampling, binary large objects (BLOBs), and rollups. These improvements are expected to increase network participation, reduce congestion, decrease fees, and increase transaction speeds. The other issue with many blockchains is that each block can only hold so much data. The block size debate has been and continues to be one of the most pressing issues for the scalability of blockchains in the future. While confidentiality on the blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the blockchain network. The most cited example of blockchain being used for illicit transactions is probably the Silk Road, an online dark web illegal-drug and money laundering marketplace operating from February 2011 until October 2013, when the FBI shut it down. The dark web allows users to buy and sell illegal goods without being tracked by using the Tor Browser and make illicit purchases in Bitcoin or other cryptocurrencies. This is in stark contrast to U.S. regulations, which require financial service providers to obtain information about their customers when they open an account. They are supposed to verify the identity of each customer and confirm that they do not appear on any list of known or suspected terrorist organizations. Illicit activity accounted for only 0.34% of all cryptocurrency transactions in 2023. This system can be seen as both a pro and a con. It gives anyone access to financial accounts, but allows criminals to transact more easily. Many have argued that the good uses of crypto, like banking the unbanked, outweigh the bad uses of cryptocurrency, especially when most illegal activity is still accomplished through untraceable cash. Public perception of blockchain and cryptocurrencies, in particular, remains uneasy. High-profile collapses of once-trusted cryptocurrency brokers, such as Mt. Gox back in 2014, or FTX in November 2022, persistence of various crypto scams, and general skepticism towards new technology and its bold promises, all contribute to ongoing public skepticism about a decentralized future. As of 2024, 44% of Americans still say they will never purchase a cryptocurrency. Many in the crypto space have expressed concerns about government regulation of cryptocurrencies. Several jurisdictions are tightening control over certain types of crypto and other virtual currencies. However, no regulations have yet been introduced that focus on restricting blockchain uses and development, only certain products created using it. Another significant implication of blockchains is that they require storage. This may not appear to be substantial because we already store lots of information and data. However, as time passes, the growing blockchain use will require more storage, especially on blockchains where nodes store the entire chain. Currently, data storage is centralized in large centers. But if the world transitions to blockchain for every industry and use, its exponentially growing size would require more advanced techniques to make storage more efficient, or force participants to continually upgrade their storage. This could become significantly more expensive in terms of both money and physical space needed, as the Bitcoin blockchain itself was over 600 gigabytes as of September 15th, 2024—and this blockchain records only bitcoin transactions. This is small compared to the amount of data stored in large data centers, but a growing number of blockchains will only add to the amount of storage already required for the digital world. Simply put, a blockchain is a shared database or ledger. Bits of data are stored in files known as blocks, and each network node has a replica of the entire database. Security is ensured since the majority of nodes will not accept a change if someone tries to edit or delete an entry in one copy of the ledger. Imagine you typed some information into a document on your computer and sent it through a program that gave you a string of numbers and letters (called hashing, with the string called a hash). You add this hash to the beginning of another document and type information into it. Again, you use the program to create a hash, which you add to the following document. Each hash is a representation of the previous document, which creates a chain of encoded documents that cannot be altered without changing the hash. Each document is stored on computers in a network. This network of programs compares each document with the ones they have stored and accepts them as valid based on the hashes they generate. If a document doesn't generate a hash that is a match, that document is rejected by the network. A blockchain is a distributed network of files chained together using programs that create hashes, or strings of numbers and letters that represent the information contained in the files. Every network participant is a computer or device that compares these hashes to the one they generate. If there is a match, the file is kept. If there isn't, the file is rejected. With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself in no small part because of Bitcoin and cryptocurrency. As a buzzword on the tongue of every investor across the globe, blockchain stands to make business and government operations more accurate, efficient, secure, and cheap, with fewer intermediaries. As we head into the third decade of blockchain, it's no longer a question of if legacy companies will catch on to the technology—it's a question of when. Today, we see a proliferation of NFTs and the tokenization of assets. Tomorrow, we may see a combination of blockchains, tokens, and artificial intelligence all incorporated into business and consumer solutions. The comments, opinions, and analyses expressed on Investopedia are for informational purposes online. Read our warranty and liability disclaimer for more info. 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 dappGambl, 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. Pop quiz Articles referenced include: "What is Web3?," October 10, 2023 "McKinsey Technology Trends Outlook 2023," July 20, 2023 "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.

A blockchain is a distributed database or ledger shared across a computer network's nodes. They are best known for their crucial role in cryptocurrency systems, maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—meaning it cannot be altered. Since a block can't be changed, the only trust needed is at the point where a user or program enters data. This reduces the need for trusted third parties, such as auditors or other humans, who add costs and can make mistakes. Since Bitcoin's introduction in 2009, blockchain uses have exploded via the creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. Blockchain is a type of shared database that differs from a typical database in the way it stores information; blockchains store data in blocks linked together via cryptography.Different types of information can be stored on a blockchain, but the most common use has been as a transaction ledger. In Bitcoin's case, the blockchain is decentralized, so no single person or group has control—instead, all users collectively retain control.Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, transactions are permanently recorded and viewable to anyone. Investopedia / Xiaojie Liu You might be familiar with spreadsheets or databases. A blockchain is somewhat similar because it is a database where information is entered and stored. The key difference between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed. A blockchain consists of programs called scripts that conduct the tasks you usually would in a database: entering and accessing information, and saving and storing it somewhere. A blockchain is distributed, which means multiple copies are saved on many machines, and they must all match for it to be valid. The Bitcoin blockchain collects transaction information and enters it into a 4MB file called a block (different blockchains have different size blocks). Once the block is full, the block data is run through a cryptographic hash function, which creates a hexadecimal number called the block header hash. The hash is then entered into the following block header and encrypted with the other information in that block's header, creating a chain of blocks, hence the name "blockchain." Transactions follow a specific process, depending on the blockchain. For example, on Bitcoin's blockchain, if you initiate a transaction using your cryptocurrency wallet—the application that provides an interface for the blockchain—it starts a sequence of events. In Bitcoin, your transaction is sent to a memory pool, where it is stored and queued until a miner picks it up. Once it is entered into a block and the block fills up with transactions, it is closed, and the mining begins. Every node in the network proposes its own blocks in this way because they all choose different transactions. Each works on their own blocks, trying to find a solution to the difficulty target, using the "nonce," short for number used once. The nonce value is a field in the block header that is changeable, and its value incrementally increases with every mining attempt. If the resulting hash isn't equal to or less than the target hash, a value of one is added to the nonce, a new hash is generated, and so on. The nonce rolls over about every 4.5 billion attempts (which takes less than one second) and uses another value called the extra nonce as an additional counter. This continues until a miner generates a valid hash, winning the race and receiving the reward. Generating these hashes until a specific value is found is the "proof-of-work" you hear so much about—it "proves" the miner did the work. The sheer amount of work it takes to validate the hash is why the Bitcoin network consumes so much computational power and energy. Once a block is closed, a transaction is complete. However, the block is not considered confirmed until five other blocks have been validated. Confirmation takes the network about one hour to complete because it averages just under 10 minutes per block (the first block with your transaction and five following blocks multiplied by 10 equals 60 minutes). Not all blockchains follow this process. For instance, the Ethereum network randomly chooses one validator from all users with ether staked to validate blocks, which are then confirmed by the network. This is much faster and less energy intensive than Bitcoin's process. A blockchain allows the data in a database to be spread out among several network nodes—computers or devices running software for the blockchain—at various locations. This creates redundancy and maintains the fidelity of the data. For example, if someone tries to alter a record on one node, the other nodes would prevent it from happening by comparing block hashes. This way, no single node can alter information within the chain. Because of this distribution—and the encrypted proof that work was done—the blockchain data, such as transaction history, becomes irreversible. Such a record could be a list of transactions, but private blockchains can also hold a variety of other information like legal contracts, state identifications, or a company's inventory. Most blockchains wouldn't "store" these items directly; they would likely be sent through a hashing algorithm and represented on the blockchain by a token. Because of the decentralized nature of the Bitcoin blockchain, all transactions can be transparently viewed by downloading and inspecting them or by using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track a bitcoin wherever it goes. For example, exchanges have been hacked in the past, resulting in the loss of large amounts of cryptocurrency. While the hackers may have been anonymous—except for their wallet address—the crypto they extracted is easily traceable because the wallet addresses are stored on the blockchain. Of course, the records stored in the Bitcoin blockchain (as well as most others) are encrypted. This means that only the person assigned an address can reveal their identity. As a result, blockchain users can remain anonymous while preserving transparency. Blockchain technology achieves decentralized security and trust in several ways. To begin, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added to the end of the blockchain, previous blocks cannot be altered. A change in any data changes the hash of the block it was in. Because each block contains the previous block's hash, a change in one would change the following blocks. The network would generally reject an altered block because the hashes would not match. However, a change can be accomplished on smaller blockchain networks. Not all blockchains are 100% impenetrable. They are distributed ledgers that use code to create the security level they have become known for. If there are vulnerabilities in the coding, they can be exploited. A new and smaller chain might be susceptible to this kind of attack, but the attacker would need at least half of the computational power of the network (a 51% attack). On the Bitcoin and other larger blockchains, this is nearly impossible. By the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter. This is because the rate at which these networks hash is exceptionally rapid—the Bitcoin network hashed at a rate of around 640 exahashes per second (18 zeros) as of September 2024. The Ethereum blockchain is not likely to be hacked either—again, the attackers would need to control more than half of the blockchain's staked ether. As of September 2024, over 33.8 million ETH has been staked by more than one million validators. An attacker or a group would need to own over 17 million ETH, and be randomly selected to validate blocks enough times to get their blocks implemented. Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application. The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator, Satoshi Nakamoto, referred to it as "a new electronic cash system that's fully peer-to-peer, with no trusted third party." The key thing to understand is that Bitcoin uses blockchain as a means to transparently record a ledger of payments or other transactions between parties. Blockchain can be used to immutably record any number of data points. The data can be transactions, votes in an election, product inventories, state identifications, deeds to homes, and much more. Currently, tens of thousands of projects are looking to implement blockchains in various ways to help society other than just recording transactions—for example, as a way to vote securely in democratic elections. The nature of blockchain's immutability means that fraudulent voting would become far more difficult. For example, a voting system could work such that each country's citizens would be issued a single cryptocurrency or token. Each candidate could then be given a specific wallet address, and the voters would send their token or crypto to the address of whichever candidate they wish to vote for. The transparent and traceable nature of blockchain would eliminate the need for human vote counting and the ability of bad actors to tamper with physical ballots. Blockchains have been heralded as a disruptive force in the finance sector, especially with the functions of payments and banking. However, banks and decentralized blockchains are vastly different. To see how a bank differs from blockchain, let's compare the banking system to Bitcoin's blockchain implementation. As we now know, blocks on Bitcoin's blockchain store transactional data. Today, tens of thousands of other cryptocurrencies run on a blockchain. But it turns out that blockchain can be a reliable way to store other types of data as well. Some companies experimenting with blockchain include Walmart, Pfizer, AIG, Siemens, and Unilever, among others. For example, IBM has created its Food Trust blockchain to trace the journey that food products take to get to their locations. Why do this? The food industry has seen countless outbreaks of E. coli, salmonella, and listeria; in some cases, hazardous materials were accidentally introduced to foods. In the past, it has taken weeks to find the source of these outbreaks or the cause of sickness from what people are eating. Using blockchain allows brands to track a food product's route from its origin, through each stop it makes, to delivery. Not only that, but these companies can also now see everything else it may have come in contact with, allowing the identification of the problem to occur far sooner—potentially saving lives. This is one example of blockchain in practice, but many other forms of blockchain implementation exist or are being experimented with. Perhaps no industry stands to benefit from integrating blockchain into its business operations more than personal banking. Financial institutions only operate during business hours, usually five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see the money in your account. Even if you make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps. By integrating blockchain into banks, consumers might see their transactions processed in minutes or seconds—the time it takes to add a block to the blockchain, regardless of holidays or the time of day or week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. Given the sums involved, even the few days the money is in transit can carry significant costs and risks for banks. The settlement and clearing process for stock traders can take up to three days (or longer if trading internationally), meaning that the money and shares are frozen for that period. Blockchain can, in theory, drastically reduce that time. Blockchain forms the bedrock for cryptocurrencies like Bitcoin. This design also allows for easier cross-border transactions because it bypasses currency restrictions, instabilities, or lack of infrastructure by using a distributed network that can reach anyone with an internet connection. Healthcare providers can leverage blockchain to store their patients' medical records securely. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key so that they are only accessible to specific individuals, thereby ensuring privacy. If you have ever spent time in your local Recorder's Office, you will know that recording property rights is both burdensome and inefficient.

Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county’s central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index. This process is not just costly and time-consuming, it is also prone to human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanently recorded. Proving property ownership can be nearly impossible in war-torn countries or areas with little to no government or financial infrastructure and no Recorder’s Office. If a group of people living in such an area can leverage blockchain, then transparent and clear timelines of property ownership could be maintained. A smart contract is computer code that can be built into the blockchain to facilitate transactions. It operates under a set of conditions to which users agree. When those conditions are met, the smart contract conducts the transaction for the users. As in the IBM Food Trust example, suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of not only their products but also common labels such as “Organic,” “Local,” and “Fair Trade.” As reported by Forbes, the food industry is increasingly adopting the use of blockchain to track the path and safety of food throughout the farm-to-user journey. As mentioned above, blockchain could facilitate a modern voting system. Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using blockchain in this way would make votes nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election. For all of its complexity, blockchain’s potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above. But there are also some disadvantages. Transactions on the blockchain network are approved by thousands of computers and devices. This removes almost all people from the verification process, resulting in less human error and an accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain and not be accepted by the rest of the network. Typically, consumers pay a bank to verify a transaction or a notary to sign a document. Blockchain eliminates the need for third-party verification—and, with it, their associated costs. For example, business owners incur a small fee when they accept credit card payments because banks and payment-processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees. Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes significantly more difficult to tamper with. Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Financial institutions operate during business hours, usually five days a week—but a blockchain runs 24 hours a day, seven days a week, and 365 days a year. On some blockchains, transactions can be completed and considered secure in minutes. This is particularly useful for cross-border trades, which usually take much longer because of time zone issues and the fact that all parties must confirm payment processing. Many blockchain networks operate as public databases, meaning anyone with an internet connection can view a list of the network’s transaction history. Although users can access transaction details, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like Bitcoin are fully anonymous; they are actually pseudonymous because there is a viewable address that can be associated with a user if the information gets out. Once a transaction is recorded, its authenticity must be verified by the blockchain network. After the transaction is validated, it is added to the blockchain block. Each block on the blockchain contains its unique hash and the unique hash of the block before it. Therefore, the blocks cannot be altered once the network confirms them. Many blockchains are entirely open source. This means that everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. However, it also means there is no real authority on who controls Bitcoin’s code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile, then Bitcoin can be updated. Private or permission blockchains may not allow for public transparency, depending on how they are designed or their purpose. These types of blockchains might be made only for an organization that wishes to track data accurately without allowing anyone outside of the permissioned users to see it. Alternatively, there might come a point where publicly traded companies are required to provide investors with financial transparency through a regulator-approved blockchain reporting system. Using blockchains in business accounting and financial reporting would prevent companies from altering their financials to appear more profitable than they really are. Perhaps the most profound facet of blockchain and cryptocurrency is the ability for anyone, regardless of ethnicity, gender, location, or cultural background, to use it. According to The World Bank, an estimated 1.4 billion adults do not have bank accounts or any means of storing their money or wealth. Moreover, nearly all of these individuals live in developing countries where the economy is in its infancy and entirely dependent on cash. These people are often paid in physical cash. They then need to store this physical cash in hidden locations in their homes or other places, incentivizing robbers or violence. While not impossible to steal, crypto makes it more difficult for would-be thieves. Although blockchain can save users money on transaction fees, the technology is far from free. For example, the Bitcoin network's proof-of-work system to validate transactions consumes vast amounts of computational power. In the real world, the energy consumed by the millions of devices on the Bitcoin network is more than the country of Pakistan consumes annually. Some solutions to these issues are beginning to arise. For example, bitcoin-mining farms have been set up to use solar power, excess natural gas from fracking sites, or energy from wind farms. Bitcoin is a perfect case study of the inefficiencies of blockchain. Bitcoin's PoW system takes about 10 minutes to add a new block to the blockchain. At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS). Although other cryptocurrencies, such as Ethereum, perform better than Bitcoin, the complex structure of blockchain still limits them. Legacy brand Visa, for context, can process 65,000 TPS. Solutions to this issue have been in development for years. There are currently blockchain projects that claim tens of thousands of TPS. Ethereum is rolling out a series of upgrades that include data sampling, binary large objects (BLOBs), and rollups. These improvements are expected to increase network participation, reduce congestion, decrease fees, and increase transaction speeds. The other issue with many blockchains is that each block can only hold so much data. The block size debate has been and continues to be one of the most pressing issues for the scalability of blockchains in the future. While confidentiality on the blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the blockchain network. The most cited example of blockchain being used for illicit transactions is probably the Silk Road, an online dark web illegal-drug and money laundering marketplace operating from February 2011 until October 2013, when the FBI shut it down. The dark web allows users to buy and sell illegal goods without being tracked by using the Tor Browser and make illicit purchases in Bitcoin or other cryptocurrencies. This is in stark contrast to U.S. regulations, which require financial service providers to obtain information about their customers when they open an account. They are supposed to verify the identity of each customer and confirm that they do not appear on any list of known or suspected terrorist organizations. Illicit activity accounted for only 0.34% of all cryptocurrency transactions in 2023. This system can be seen as both a pro and a con. It gives anyone access to financial accounts, but allows criminals to transact more easily. Many have argued that the good uses of crypto, like banking the unbanked, outweigh the bad uses of cryptocurrency, especially when most illegal activity is still accomplished through untraceable cash. Public perception of blockchain and cryptocurrencies, in particular, remains uneasy. High-profile collapses of once-trusted cryptocurrency brokers, such as Mt. Gox back in 2014, or FTX in November 2022, persistence of various crypto scams, and general skepticism towards new technology and its bold promises, all contribute to ongoing public skepticism about a decentralized future. As of 2024, 44% of Americans still say they will never purchase a cryptocurrency. Many in the crypto space have expressed concerns about government regulation of cryptocurrencies. Several jurisdictions are tightening control over certain types of crypto and other virtual currencies. However, no regulations have yet been introduced that focus on restricting blockchain uses and development, only certain products created using it. Another significant implication of blockchains is that they require storage. This may not appear to be substantial because we already store lots of information and data. However, as time passes, the growing blockchain use will require more storage, especially on blockchains where nodes store the entire chain. Currently, data storage is centralized in large centers. But if the world transitions to blockchain for every industry and use, its exponentially growing size would require more advanced techniques to make storage more efficient, or force participants to continually upgrade their storage. This could become significantly more expensive in terms of both money and physical space needed, as the Bitcoin blockchain itself was over 600 gigabytes as of September 15th, 2024—and this blockchain records only bitcoin transactions. This is small compared to the amount of data stored in large data centers, but a growing number of blockchains will only add to the amount of storage already required for the digital world. Simply put, a blockchain is a shared database or ledger. Bits of data are stored in files known as blocks, and each network node has a replica of the entire database. Security is ensured since the majority of nodes will not accept a change if someone tries to edit or delete an entry in one copy of the ledger. Imagine you typed some information into a document on your computer and sent it through a program that gave you a string of numbers and letters (called hashing, with the string called a hash). You add this hash to the beginning of another document and type information into it. Again, you use the program to create a hash, which you add to the following document. Each hash is a representation of the previous document, which creates a chain of encoded documents that cannot be altered without changing the hash. Each document is stored on computers in a network. This network of programs compares each document with the ones they have stored and accepts them as valid based on the hashes they generate. If a document doesn't generate a hash that is a match, that document is rejected by the network. A blockchain is a distributed network of files chained together using programs that create hashes, or strings of numbers and letters that represent the information contained in the files. Every network participant is a computer or device that compares these hashes to the one they generate. If there is a match, the file is kept. If there isn't, the file is rejected. With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself in no small part because of Bitcoin and cryptocurrency. As a buzzword on the tongue of every investor across the globe, blockchain stands to make business and government operations more accurate, efficient, secure, and cheap, with fewer intermediaries. As we head into the third decade of blockchain, it’s no longer a question of if legacy companies will catch on to the technology—it’s a question of when. Today, we see a proliferation of NFTs and the tokenization of assets. Tomorrow, we may see a combination of blockchains, tokens, and artificial intelligence all incorporated into business and consumer solutions. The comments, opinions, and analyses expressed on Investopedia are for informational purposes online. Read our warranty and liability disclaimer for more info. A blockchain is a distributed database or ledger shared across a computer network's nodes. They are best known for their crucial role in cryptocurrency systems, maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—meaning it cannot be altered. Since a block can’t be changed, the only trust needed is at the point where a user or program enters data. This reduces the need for trusted third parties, such as auditors or other humans, who add costs and can make mistakes. Since Bitcoin's introduction in 2009, blockchain uses have exploded via the creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. Blockchain is a type of shared database that differs from a typical database in the way it stores information; blockchains store data in blocks linked together via cryptography.Different types of information can be stored on a blockchain, but the most common use has been as a transaction ledger. In Bitcoin’s case, the blockchain is decentralized, so no single person or group has control—instead, all users collectively retain control.Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, transactions are permanently recorded and viewable to anyone. Investopedia / Xiaojie Liu You might be familiar with spreadsheets or databases. A blockchain is somewhat similar because it is a database where information is entered and stored. The key difference between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed. A blockchain consists of programs called scripts that conduct the tasks you usually would in a database: entering and accessing information, and saving and storing it somewhere. A blockchain is distributed, which means multiple copies are saved on many machines, and they must all match for it to be valid. The Bitcoin blockchain collects transaction information and enters it into a 4MB file called a block (different blockchains have different size blocks). Once the block is full, the block data is run through a cryptographic hash function, which creates a hexadecimal number called the block header hash. The hash is then entered into the following block header and encrypted with the other information in that block's header, creating a chain of blocks, hence the name “blockchain.” Transactions follow a specific process, depending on the blockchain. For example, on Bitcoin's blockchain, if you initiate a transaction using your cryptocurrency wallet—the application that provides an interface for the blockchain—it starts a sequence of events. In Bitcoin, your transaction is sent to a memory pool, where it is stored and queued until a miner picks it up. Once it is entered into a block and the block fills up with transactions, it is closed, and the mining begins. Every node in the network proposes its own blocks in this way because they all choose different transactions. Each works on their own blocks, trying to find a solution to the difficulty target, using the "nonce," short for number used once. The nonce value is a field in the block header that is changeable, and its value incrementally increases with every mining attempt. If the resulting hash isn't equal to or less than the target hash, a value of one is added to the nonce, a new hash is generated, and so on. The nonce rolls over about every 4.5 billion attempts (which takes less than one second) and uses another value called the extra nonce as an additional counter. This continues until a miner generates a valid hash, winning the race and receiving the reward. Generating these hashes until a specific value is found is the "proof-of-work" you hear so much about—it "proves" the miner did the work. The sheer amount of work it takes to validate the hash is why the Bitcoin network consumes so much computational power and energy. Once a block is closed, a transaction is complete. However, the block is not considered confirmed until five other blocks have been validated. Confirmation takes the network about one hour to complete because it averages just under 10 minutes per block (the first block with your transaction and five following blocks multiplied by 10 equals 60 minutes). Not all blockchains follow this process. For instance, the Ethereum network randomly chooses one validator from all users with ether staked to validate blocks, which are then confirmed by the network. This is much faster and less energy intensive than Bitcoin's process. A blockchain allows the data in a database to be spread out among several network nodes—computers or devices running software for the blockchain—at various locations. This creates redundancy and maintains the fidelity of the data. For example, if someone tries to alter a record on one node, the other nodes would prevent it from happening by comparing block hashes. This way, no single node can alter information within the chain. Because of this distribution—and the encrypted proof that work was done—the blockchain data, such as transaction history, becomes irreversible. Such a record could be a list of transactions, but private blockchains can also hold a variety of other information like legal contracts, state identifications, or a company's inventory. Most blockchains wouldn't "store" these items directly; they would likely be sent through a hashing algorithm and represented on the blockchain by a token. Because of the decentralized nature of the Bitcoin blockchain, all transactions can be transparently viewed by downloading and inspecting them or by using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track a bitcoin wherever it goes. For example, exchanges have been hacked in the past, resulting in the loss of large amounts of cryptocurrency. While the hackers may have been anonymous—except for their wallet address—the crypto they extracted is easily traceable because the wallet addresses are stored on the blockchain. Of course, the records stored in the Bitcoin blockchain (as well as most others) are encrypted. This means that only the person assigned an address can reveal their identity. As a result, blockchain users can remain anonymous while preserving transparency. Blockchain technology achieves decentralized security and trust in several ways. To begin, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added to the end of the blockchain, previous blocks cannot be altered. A change in any data changes the hash of the block it was in. Because each block contains the previous block's hash, a change in one would change the following blocks. The network would generally reject an altered block because the hashes would not match. However, a change can be accomplished on smaller blockchain networks. Not all blockchains are 100% impenetrable. They are distributed ledgers that use code to create the security level they have become known for. If there are vulnerabilities in the coding, they can be exploited. A new and smaller chain might be susceptible to this kind of attack, but the attacker would need at least half of the computational power of the network (a 51% attack). On the Bitcoin and other larger blockchains, this is nearly impossible. By the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter. This is because the rate at which these networks hash is exceptionally rapid—the Bitcoin network hashed at a rate of around 640 exahashes per second (18 zeros) as of September 2024. The Ethereum blockchain is not likely to be hacked either—again, the attackers would need to control more than half of the blockchain's staked ether. As of September 2024, over 33.8 million ETH has been staked by more than one million validators. An attacker or a group would need to own over 17 million ETH, and be randomly selected to validate blocks enough times to get their blocks implemented. Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn’t until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application. The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin’s pseudonymous creator, Satoshi Nakamoto, referred to it as “a new electronic cash system that’s fully peer-to-peer, with no trusted third party.” The key thing to understand is that Bitcoin uses blockchain as a means to transparently record a ledger of payments or other transactions between parties. Blockchain can be used to immutably record any number of data points. The data can be transactions, votes in an election, product inventories, state identifications, deeds to homes, and much more. Currently, tens of thousands of projects are looking to implement blockchains in various ways to help society other than just recording transactions—for example, as a way to vote securely in democratic elections. The nature of blockchain's immutability means that fraudulent voting would become far more difficult. For example, a voting system could work such that each country's citizens would be issued a single cryptocurrency or token. Each candidate could then be given a specific wallet address, and the voters would send their token or crypto to the address of whichever candidate they wish to vote for. The transparent and traceable nature of blockchain would eliminate the need for human vote counting and the ability of bad actors to tamper with physical ballots. Blockchains have been heralded as a disruptive force in the finance sector, especially with the functions of payments and banking. However, banks and decentralized blockchains are vastly different. To see how a bank differs from blockchain, let’s compare the banking system to Bitcoin’s blockchain implementation. As we now know, blocks on Bitcoin’s blockchain store transactional data. Today, tens of thousands of other cryptocurrencies run on a blockchain. But it turns out that blockchain can be a reliable way to store other types of data as well. Some companies experimenting with blockchain include Walmart, Pfizer, AIG, Siemens, and Unilever, among others. For example, IBM has created its Food Trust blockchain to trace the journey that food products take to get to their locations. Why do this? The food industry has seen countless outbreaks of E. coli, salmonella, and listeria; in some cases, hazardous materials were accidentally introduced to foods. In the past, it has taken weeks to find the source of these outbreaks or the cause of sickness from what people are eating. Using blockchain allows brands to track a food product’s route from its origin, through each stop it makes, to delivery. Not only that, but these companies can also now see everything else it may have come in contact with, allowing the identification of the problem to occur far sooner—potentially saving lives. This is one example of blockchain in practice, but many other forms of blockchain implementation exist or are being experimented with. Perhaps no industry stands to benefit from integrating blockchain into its business operations more than personal banking. Financial institutions only operate during business hours, usually five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see the money in your account. Even if you make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps. By integrating blockchain into banks, consumers might see their transactions processed in minutes or seconds—the time it takes to add a block to the blockchain, regardless of holidays or the time of day or week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. Given the sums involved, even the few days the money is in transit can carry significant costs and risks for banks. The settlement and clearing process for stock traders can take up to three days (or longer if trading internationally), meaning that the money and shares are frozen for that period. Blockchain can, in theory, drastically reduce that time. Blockchain forms the bedrock for cryptocurrencies like Bitcoin. This design also allows for easier cross-border transactions because it bypasses currency restrictions, instabilities, or lack of infrastructure by using a distributed network that can reach anyone with an internet connection. Healthcare providers can leverage blockchain to store their patients’ medical records securely. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key so that they are only accessible to specific individuals, thereby ensuring privacy. If you have ever spent time in your local Recorder’s Office, you will know that recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county’s central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index. This process is not just costly and time-consuming, it is also prone to human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanently recorded. Proving property ownership can be nearly impossible in war-torn countries or areas with little to no government or financial infrastructure and no Recorder’s Office. If a group of people living in such an area can leverage blockchain, then transparent and clear timelines of property ownership could be maintained. A smart contract is computer code that can be built into the blockchain to facilitate transactions. It operates under a set of conditions to which users agree. When those conditions are met, the smart contract conducts the transaction for the users. As in the IBM Food Trust example, suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of not only their products but also common labels such as “Organic,” “Local,” and “Fair Trade.” As reported by Forbes, the food industry is increasingly adopting the use of blockchain to track the path and safety of food throughout the farm-to-user journey. As mentioned above, blockchain could facilitate a modern voting system. Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using blockchain in this way would make votes nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election. For all of its complexity, blockchain’s potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above. But there are also some disadvantages. Transactions on the blockchain network are approved by thousands of computers and devices. This removes almost all people from the verification process, resulting in less human error and an accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain and not be accepted by the rest of the network. Typically, consumers pay a bank to verify a transaction or a notary to sign a document. Blockchain eliminates the need for third-party verification—and, with it, their associated costs. For example, business owners incur a small fee when they accept credit card payments because banks and payment-processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees. Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes significantly more difficult to tamper with. Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Financial institutions operate during business hours, usually five days a week—but a blockchain runs 24 hours a day, seven days a week, and 365 days a year. On some blockchains, transactions can be completed and considered secure in minutes. This is particularly useful for cross-border trades, which usually take much longer because of time zone issues and the fact that all parties must confirm payment processing. Many blockchain networks operate as public databases, meaning anyone with an internet connection can view a list of the network’s transaction history. Although users can access transaction details, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like Bitcoin are fully anonymous; they are actually pseudonymous because there is a viewable address that can be associated with a user if the information gets out. Once a transaction is recorded, its authenticity must be verified by the blockchain network. After the transaction is validated, it is added to the blockchain block. Each block on the blockchain contains its unique hash and the unique hash of the block before it. Therefore, the blocks cannot be altered once the network confirms them. Many blockchains are entirely open source. This means that everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. However, it also means there is no real authority on who controls Bitcoin’s code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile, then Bitcoin can be updated. Private or permission blockchains may not allow for public transparency, depending on how they are designed or their purpose. These types of blockchains might be made only for an organization that wishes to track data accurately without allowing anyone outside of the permissioned users to see it. Alternatively, there might come a point where publicly traded companies are required to provide investors with financial transparency through a regulator-approved blockchain reporting system. Using blockchains in business accounting and financial reporting would prevent companies from altering their financials to appear more profitable than they really are. Perhaps the most profound facet of blockchain and cryptocurrency is the ability for anyone, regardless of ethnicity, gender, location, or cultural background, to use it. According to The World Bank, an estimated 1.4 billion adults do not have bank accounts or any means of storing their money or wealth. Moreover, nearly all of these individuals live in developing countries where the economy is in its infancy and entirely dependent on cash. These people are often paid in physical cash. They then need to store this physical cash in hidden locations in their homes or other places, incentivizing robbers or violence. While not impossible to steal, crypto makes it more difficult for would-be thieves. Although blockchain can save users money on transaction fees, the technology is far from free. For example, the Bitcoin network's proof-of-work system to validate transactions consumes vast amounts of computational power. In the real world, the energy consumed by the millions of devices on the Bitcoin network is more than the country of Pakistan consumes annually. Some solutions to these issues are beginning to arise. For example, bitcoin-mining farms have been set up to use solar power, excess natural gas from fracking sites, or energy from wind farms. Bitcoin is a perfect case study of the inefficiencies of blockchain. Bitcoin's PoW system takes about 10 minutes to add a new block to the blockchain. At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS). Although other cryptocurrencies, such as Ethereum, perform better than Bitcoin, the complex structure of blockchain still limits them. Legacy brand Visa, for context, can process 65,000 TPS. Solutions to this issue have been in development for years. There are currently blockchain projects that claim tens of thousands of TPS. Ethereum is rolling out a series of upgrades that include data sampling, binary large objects (BLOBs), and rollups. These improvements are expected to increase network participation, reduce congestion, decrease fees, and increase transaction speeds. The other issue with many blockchains is that each block can only hold so much data. The block size debate has been and continues to be one of the most pressing issues for the scalability of blockchains in the future. While confidentiality on the blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the blockchain network. The most cited example of blockchain being used for illicit transactions is probably the Silk Road, an online dark web illegal-drug and money laundering marketplace operating from February 2011 until October 2013, when the FBI shut it down. The dark web allows users to buy and sell illegal goods without being tracked by using the Tor Browser and make illicit purchases in Bitcoin or other cryptocurrencies. This is in stark contrast to U.S. regulations, which require financial service providers to obtain information about their customers when they open an account. They are supposed to verify the identity of each customer and confirm that they do not appear on any list of known or suspected terrorist organizations. Illicit activity accounted for only 0.34% of all cryptocurrency transactions in 2023. This system can be seen as both a pro and a con. It gives anyone access to financial accounts, but allows criminals to transact more easily. Many have argued that the good uses of crypto, like banking the unbanked, outweigh the bad uses of cryptocurrency, especially when most illegal activity is still accomplished through untraceable cash. Public perception of blockchain and cryptocurrencies, in particular, remains uneasy. High-profile collapses of once-trusted cryptocurrency brokers, such as Mt. Gox back in 2014, or FTX in November 2022, persistence of various crypto scams, and general skepticism towards new technology and its bold promises, all contribute to ongoing public skepticism about a decentralized future. As of 2024, 44% of Americans still say they will never purchase a cryptocurrency. Many in the crypto space have expressed concerns about government regulation of cryptocurrencies. Several jurisdictions are tightening control over certain types of crypto and other virtual currencies. However, no regulations have yet been introduced that focus on restricting blockchain uses and development, only certain products created using it. Another significant implication of blockchains is that they require storage. This may not appear to be substantial because we already store lots of information and data. However, as time passes, the growing blockchain use will require more storage, especially on blockchains where nodes store the entire chain. Currently, data storage is centralized in large centers. But if the world transitions to blockchain for every industry and use, its exponentially growing size would require more advanced techniques to make storage more efficient, or force participants to continually upgrade their storage. This could become significantly more expensive in terms of both money and physical space needed, as the Bitcoin blockchain itself was over 600 gigabytes as of September 15th, 2024—and this blockchain records only bitcoin transactions. This is small compared to the amount of data stored in large data centers, but a growing number of blockchains will only add to the amount of storage already required for the digital world. Simply put, a blockchain is a shared database or ledger. Bits of data are stored in files known as blocks, and each network node has a replica of the entire database. Security is ensured since the majority of nodes will not accept a change if someone tries to edit or delete an entry in one copy of the ledger. Imagine you typed some information into a document on your computer and sent it through a program that gave you a string of numbers and letters (called hashing, with the string called a hash). You add this hash to the beginning of another document and type information into it. Again, you use the program to create a hash, which you add to the following document. Each hash is a representation of the previous document, which creates a chain of encoded documents that cannot be altered without changing the hash. Each document is stored on computers in a network. This network of programs compares each document with the ones they have stored and accepts them as valid based on the hashes they generate. If a document doesn't generate a hash that is a match, that document is rejected by the network. A blockchain is a distributed network of files chained together using programs that create hashes, or strings of numbers and letters that represent the information contained in the files. Every network participant is a computer or device that compares these hashes to the one they generate. If there is a match, the file is kept. If there isn't, the file is rejected. With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself in no small part because of Bitcoin and cryptocurrency. As a buzzword on the tongue of every investor across the globe, blockchain stands to make business and government operations more accurate, efficient, secure, and cheap, with fewer intermediaries. As we head into the third decade of blockchain, it’s no longer a question of if legacy companies will catch on to the technology—it’s a question of when. Today, we see a proliferation of NFTs and the tokenization of assets. Tomorrow, we may see a combination of blockchains, tokens, and artificial intelligence all incorporated into business and consumer solutions. The comments, opinions, and analyses expressed on Investopedia are for informational purposes online. Read our warranty and liability disclaimer for more info. Blockchain technology is changing the way we think about finance. By creating a secure and transparent way to record transactions, it is making banking, payments, and investments easier and safer. This article will explain the basics of blockchain, its effects on the finance world, and what the future holds. Blockchain is a digital ledger that keeps track of transactions securely. It helps banks work faster and makes transactions safer. Using blockchain can lower the costs of sending money across borders. Smart contracts can automate and simplify investment processes. Despite its benefits, blockchain faces challenges like regulations and the need for wider acceptance. So, let’s kick things off with the basics. Blockchain is like a digital notebook that everyone can see but no one can erase. It’s a way to keep track of information in a secure and transparent manner. Imagine a chain made up of blocks, where each block holds data. This data can be anything from transactions to contracts. The cool part? Once something is added to the blockchain, it’s super hard to change it. Blockchain has some standout features that make it special: Decentralization: No single person or company controls it. Transparency: Everyone can see the transactions. Security: It uses cryptography to keep data safe. Let’s face it, waiting for transactions to clear can be a real pain. With blockchain in banking, things are changing fast. Transactions can happen almost instantly, which means no more waiting around. This tech cuts out the middleman, making everything smoother and quicker. When it comes to money, security is a big deal. Blockchain technology offers a super secure way to handle transactions. Each transaction is recorded in a way that’s really hard to tamper with. This means that banks can keep your money safer than ever before. Who doesn’t want to save some extra cash? By using blockchain, banks can lower their costs. They don’t need as many people to handle transactions, and they can cut down on fees. This could mean lower fees for you, which is always a win. Blockchain technology makes banking easier, safer, and cheaper for everyone involved. Impact Area Benefits Streamlining Faster transactions Security Enhanced protection Cost Reduction Lower fees for customers Everyone can see the payments on blockchain, which increases trust. You know how waiting for money to cross borders can feel like watching paint dry? Well, with blockchain, that wait is getting a whole lot shorter. Instead of days, transactions can happen in just a few minutes. This is a game changer for anyone who needs to send money overseas quickly. Let’s talk about fees. Traditional banks and money transfer services love to charge you for sending money. But with blockchain, those fees can drop significantly. Here’s a quick comparison: Service Type Traditional Banks Blockchain Services Average Fee 3-5% 0.5-2% Transfer Time 1-5 days 10-30 minutes One of the coolest things about blockchain is that it’s super transparent. Everyone can see the transactions, which means less chance of fraud. This is especially important when you’re dealing with money. It builds trust, and trust is everything in finance. Whether it’s through tokenization, smart contracts, or DeFi, the future of investing looks bright. So, let’s talk about tokenization. This is where we take real-world assets, like real estate or art, and turn them into digital tokens on the blockchain. This makes it easier to buy, sell, and trade these assets. Here are some of the benefits of tokenization: Fractional Ownership: You can own a piece of something big without needing a ton of cash. Increased Liquidity: It’s easier to sell your tokens than to sell a whole property. Global Reach: You can invest in assets from anywhere in the world. Next up, we have smart contracts. These are like digital agreements that automatically execute when certain conditions are met. They make investing safer and faster. Here’s why I think they’re awesome: No Middlemen: You don’t need a broker to handle your deals. Transparency: Everyone can see the terms, so there’s no funny business. Speed: Transactions happen quickly without delays. Finally, let’s dive into DeFi. This is a whole new way of doing finance without banks. It’s all about using blockchain to create financial services. Here’s what I love about DeFi: Accessibility: Anyone with internet can join in. Lower Fees: You save money on transaction costs. Innovative Products: There are new ways to earn and invest that you won’t find in traditional finance. When it comes to using blockchain in finance, one of the biggest challenges is regulatory hurdles. Different countries have different rules, and sometimes they don’t even know how to handle blockchain yet. This can make it tough for businesses to figure out how to operate legally. Here are some key points to think about: Lack of clear guidelines: Many places don’t have specific laws for blockchain. Changing regulations: Rules can change quickly, making it hard to keep up. Global differences: What’s legal in one country might not be in another. Another big reason is scalability issues. As more people start using blockchain, it can get slow and clunky. Here’s what I mean: Transaction speed: Sometimes, it takes a while to process transactions. Network congestion: Too many users can slow things down. Cost of scaling: Making the system bigger can be expensive. Finally, we have adoption barriers. Not everyone is on board with blockchain yet, and that can hold things back. Here are some reasons: Lack of understanding: Many people don’t really get how blockchain works. Fear of change: Some folks are just scared to switch from traditional systems. Need for education: There’s a big gap in knowledge about blockchain. The scope for growth of blockchain in finance is only going to expand. Some exciting emerging trends in blockchain technology finance include: Decentralized finance (DeFi): This is where people can lend and borrow without banks. Tokenization: This means turning real-world assets into digital tokens. Think of it as making everything from art to real estate easier to trade. Interoperability: Different blockchains working together. This is huge for making transactions smoother. The future is going to chock full of potential innovations. I mean, just look at how blockchain financial services are changing the game. Here are a few ideas: Smart contracts: These are like digital agreements that automatically execute when conditions are met. Blockchain in supply chain: Tracking products from start to finish, ensuring everything is legit. Identity verification: Using blockchain to prove who you are without all the hassle. Finance and blockchain are go hand in hand and some of the implications are: Increased efficiency: Transactions will be faster and cheaper. Greater transparency: Everyone can see the same information, which builds trust. New business models: Companies will find new ways to make money using blockchain. The future of blockchain in finance looks bright! This technology is changing how we handle money, making transactions faster and safer. If you want to learn more about how blockchain can impact your financial life, visit our website for the latest updates and insights. Don’t miss out on the future! So, there you have it. Blockchain is the future of modern finance, from banks to payments and even investments, it’s changing how we handle money and who we place authority on. It’s like having a secure digital notebook that everyone can trust. As more people and businesses start using blockchain, we can expect even more changes in the future. Whether you’re a finance whiz or just curious, it’s worthwhile to keep tabs on this technology. Blockchain technology is a way to store and share information securely. It works like a digital ledger where each entry is linked to others, making it hard to change or hack. Blockchain helps banks by making transactions faster, safer, and cheaper. It allows money to be sent directly between people without needing a middleman. Yes, blockchain can speed up payments, especially for international transactions. This means you can send money across the world in just a few minutes. Smart contracts are like digital agreements that automatically execute when certain conditions are met. They help make transactions smoother and more trustworthy. Blockchain has some challenges, like needing clear rules from governments, being able to handle a lot of users at once, and getting more people to use it. We can expect new trends, exciting technology, and big changes in how money is handled. What are the Uses of Blockchain? Blockchain is currently predominantly used in cryptocurrency networks. This technology was popularized with the advent of Bitcoin, but is used by all cryptocurrencies to ensure security and transparency. Other cryptocurrencies, like Ethereum, have made changes to their blockchain network by adding features such as Smart Contracts and Decentralized Applications (DApps). Blockchains can also be for a variety of purposes, such as issuing and maintaining real estate titles and records, medical record keeping, tracking produce, livestock and medicine throughout the supply chain, verifying ownership or validity of assets or rights, trade finance and even voting mechanisms. How Does Blockchain Work? Blockchains can be understood as something simple, like an analogy of an on-line purchase, say from Amazon. Blockchain example: Amazon analogy After your purchase, you will receive an order confirmation on your email. Then, you might next receive an email confirmation that your order has been processed. The next email after that might be your order has left the warehouse and has been shipped. You might then get another email tracker that says your purchase is en route. Finally, you might get that last email that your purchase has been delivered to your door by the delivery person. That’s basically how a blockchain works. Each one of those emails or notifications you received from Amazon has been triggered each time it passes through a step and each time it does that, the action causes the order tracker to update the status of your purchase. You can also log into your Amazon account and verify each of those steps. The chain works in one direction only via a time-stamp, just like your Amazon order tracker, which means that no one can go back and tamper with earlier steps so the delivery person can’t go back and status the order to steal your purchase. This type of sequence is also called “append-only”. Think of each of the emails in the above example as a discrete block and the entire order process as a “mini”-blockchain. Distributed ledger A blockchain is simply a database of transactions, often called a distributed ledger, that has been duplicated and broadcast to network of users, who can all verify and agree on the database. Each new block, which in cryptocurrencies contains a list of transactions, that comes afterwards is time-stamped and has to be approved by a network of computer servers, called nodes, each of whom checks its validity. Once every node has checked a block, there is a sort of electronic vote, as some nodes may think the transaction is valid and others think it is a fraud. This is called consensus. If a majority of nodes say that a block is valid, then it is written into the blockchain, literally stringing together a chain of blocks. This new accepted version of the blockchain ledger is broadcast over the entire network of nodes that run the same blockchain software. All the nodes have the same copy and then the process repeats again to verify the next block to add onto the chain. Tamper resistance As more blocks are added, the transaction becomes increasingly difficult to reverse or alter, making the blockchain tamper-resistant, but not tamper-proof. Old blocks cannot be modified without also changing the data in subsequent blocks that follow it in the chain. Furthermore, all computers in the network must agree to change this old block. This is what prevents fraudulent data. If a counterfeiter attempts to create a fake record of cryptocurrency, the computers in the network will disagree with the change in an old block. The fake record will be invalid and not recorded in the network. Blockchain in Cryptocurrency In certain cryptocurrencies such as Bitcoin, the blockchain technology depends on nodes to race in search for a correct answer to a complicated computation in order to earn the right to ‘validate’ or add the block to the blockchain. This process is called “proof of work.” The first node to solve the computation and validate the block is also rewarded with new Bitcoins (where the term Bitcoin “mining” comes from) and the difficulty of solving these computations increases over time. The act of mining, thus, involves offering your computing power to the network in exchange for some cryptocurrency. Confirmation speeds and scale Different cryptocurrencies have different verification and recording protocols. Because of this, the computing power and hardware required for each block network can differ. Additionally, the confirmation speeds for transactions under different cryptocurrencies can also differ. Bitcoin confirmations may take anywhere between 10 minutes to an hour or more per confirmation. In contrast, Ethereum confirmations are generally much quicker – in the order of around 15 seconds or so. Newer blockchains, such as Ripple’s XRP Ledger, only require 3 to 6 seconds for transactions to be sorted, agreed, and added to the blockchain, even for payments internationally. Different cryptocurrency blockchains also have different throughput, called scale. While Bitcoin’s blockchain is only capable of processing 7-10 transactions per second, Ripple can process more than 1,500 transactions per second. Wallets and keys When it comes to cryptocurrencies, an important distinction is that the digital asset is actually never held by the owner but rather remains on the blockchain. The proof of ownership of the cryptocurrency is in the form of your private key, which is created when you create your account. Your private key is stored on a digital cryptocurrency wallet, which will also have a public key, which is a string of numbers and letters. It is an address that will appear within the blockchain as your transactions take place—no visible records of who did what transaction with who, only the number of a wallet. History of Blockchain Technology The concept of blockchain technology first appeared in David Lee Chaum’s Berkeley PhD dissertation in 1982 entitled ”Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups”[1]. However, blockchains came to the forefront in 2008 in the Bitcoin whitepaper published pseudonymous Satoshi Nakamoto titled “Bitcoin: A Peer-to-Peer Electronic Cash System”[2]. Additional Resources How to Buy Cryptocurrency Altcoin Guide What is the Best Time to Buy Cryptocurrency How to Trade Cryptocurrency See all cryptocurrency resources Article Sources These companies apply blockchain in finance to help the banking and finance industries find their stride. UPDATED BY Matthew Urwin | May 22, 2024 It makes sense that blockchain technology was first introduced as a way to breathe some fresh air into the financial sector. Originally created at the height of the 2008 global financial crisis as the operational backbone of Bitcoin, blockchain’s distributed ledger technology is a safe and secure method to transfer and catalog data. In short, blockchain is a public ledger capable of recording the origin, movement and transfer of anything of value. Instead of relying on a central authority, like banks, blockchain requires unanimous approval from the individual nodes in the blockchain to process a payment or transfer a good. The ledger technology is most attractive to the financial sector because it solves many problems plaguing the industry today, namely security and efficiency. Smart contractsSimplified payment processingAdvanced trading and investingLoyalty and rewards programsUpgraded digital identity management Blockchain subverts institutions in a way that makes today’s current financial industry appear archaic, so it’s no surprise the powers that be in the world of finance are looking for their seat at the table. DLT technology has the potential to expand the global economy to $1.76 trillion by 2030, and this possibility has risen with the popularity of blockchain wallets and cryptocurrencies. The word “disruptive” is used all too frequently nowadays, especially in the technology space, but blockchain truly has the ability to shake the multi-trillion dollar financial industry to its core. Here are just a few examples of blockchain in the finance sector doing just that. OpenZeppelinPropy IncUulalaSoluLabRippleMastercardVeemMakerDaoRobinhoodPublic.com Smart Contracts on Blockchain Arguably the most impactful application of blockchain in finance is its ability to efficiently establish trust through smart contracts. Smart contracts are similar to physical contracts, except the stipulations of the contract are fulfilled in real time via the blockchain. Smart contracts are beneficial, especially to the finance sector, for numerous reasons. These contracts are fulfilled instantly after all stipulations are met, do not require any middlemen and add heightened levels of security. Jeff Garzik, co-founder of blockchain company Bloq, says smart contracts are beneficial to parties looking for very specific outcomes, such as when a contract is fulfilled by both parties following all the predetermined rules and dissolves under violations. A good example of this is investing. When an individual invests in a company, the rules and stipulations are clearly established between the two parties. The unambiguous nature of the contract is helpful because the blockchain can then enforce those rules using its network of computers to check that all contractual agreements have been met (i.e., the investor has enough money, they invested in the proper amount of shares, etc.) before the investment moves forward. Smart contract technology is currently at the top of almost everyone’s needs because of its efficiency and privacy. Here are companies instituting blockchain-based smart contracts in an effort to get ahead of the curve. Founded: 2017 Location: Fully remote Chainlink Labs is a Web3 services platform that works to enhance smart contracts by connecting them to off-chain data sources. The company is the developer of Chainlink, an enterprise-grade oracle infrastructure that helps financial institutions connect their existing systems to major blockchain networks. Founded: 2015 Location: San Francisco, California OpenZeppelin builds and operates blockchain-based infrastructure for smart contract systems. The company blends easy-to-understand code with strict contract security practices to give customers a frictionless experience. The company has implemented systems for a slew of industries, including everything from social media to the financial sector. Founded: 2015 Location: Palo Alto, California Propy streamlines the real estate industry with its transaction management platform and blockchain technology. The company’s platform eliminates the need for piles of paperwork while providing a single system for handling the entire real estate transaction process. For property titles and escrows, smart contracts offer a frictionless experience while reducing the possibility of wire fraud and other threats. Founded: 2017 Location: Fully Remote Uulala is using smart contracts for bill paying, micro-credit and micro-loan agreements to serve underserved populations in the Americas. The company provides these consumers with a virtual blockchain-based wallet and rewards those who pay their bills or fulfill the stipulations of their smart contract micro-loans in virtual currency. The ultimate goal of Uulala is to help these consumers get recognized as creditworthy by larger financial companies. Founded: 2014 Location: Fully Remote SoluLab matches organizations with the appropriate blockchain developers, and the company has made the process even smoother with smart contracts. With expertise in developing and auditing smart contracts, SoluLab personalizes blockchain-based contracts for private, hybrid and public platforms. Businesses can then craft ideal smart contracts that meet their energy and security standards. Related Reading34 Blockchain Applications and Real-World Use Cases Disrupting the Status Quo Blockchain Payment Processing One of the most attractive applications of blockchain in fintech is its ability to process payments almost instantaneously and in a manner that protects data integrity. Because the basis of DLT is to bypass centralized institutions, moving money from peer-to-peer is as simple as pressing a “send” button on a phone. Once initiated, the nodes in the blockchain work to unanimously accept or deny the payment in an instant. There’s no need for cash to sit in limbo for days while the bank processes the transaction, nor is it burdened by exorbitant fees. By conducting money transfers with blockchain, both customers and banks could save an unprecedented amount of time and money. Blockchain-based currencies are also universal, meaning there are no exchange rates, international transfer fees or confusing country-by-country laws that prohibit the transfer of cryptos. Here are a few examples of companies using blockchain to shake up the payments industry. Founded: 1799 Location: New York, New York JPMorgan Chase is a global financial services firm that offers blockchain solutions for fintechs and financial institutions through its Onyx brand. Its offerings include Liink, a peer-to-peer network that facilitates secure data exchanges, and blockchain-based infrastructure for domestic and cross-border payments. Founded: 2012 Location: San Francisco, California Ripple is one of the best-known blockchain-based payment systems. The technology lets banks, corporations and cryptocurrency exchanges transfer money directly without the need for a third-party processor. With personalized integrations, the ability to track payments and the elimination of middlemen, Ripple is facilitating the efficient transfer of money around the world. Founded: 1966 Location: Purchase, New York Credit card giant Mastercard showcases patented blockchain technology that processes cryptocurrency payments on traditional credit card systems. The company realizes that blockchain-based payments are getting popular and wants customers to retain anonymity, while maintaining the speed of an already established payment infrastructure. Mastercard also aims to cut down on fraud and risk with a hybrid payment method. Founded: 2014 Location: San Francisco, California Veem supports customers with a platform that makes it easy to complete payments in various formats, including bank accounts, credit cards and blockchain currencies. Each transaction requires as little as an email address and notifies all parties involved. The company also meets all licensing standards in its active countries and states, blending efficiency with added peace of mind. Founded: 2014 Location: San Francisco, California MakerDao understands that making the transfer of money easier requires more stability in the cryptocurrency market. The company is a decentralized organization on the Ethereum blockchain that seeks to minimize its own volatility against the U.S. dollar by encouraging trading and borrowing of its Dai coin. Six ways blockchain can be used in financial services. | Video: Bython Media Blockchain Trading Blockchain technology has the capability to transform the stock market by cutting down complicated and time-consuming processes, high costs and security risks. A traditional stock market has numerous players, including investors, brokers, regulatory agencies and the centralized institution processing the investments. An investment can take up to three days to process because of communication between intermediaries, causing lag and uncertainty in the process. Blockchain, featuring smart contracts and a decentralized process, promises to bring speed, accuracy and efficiency to the investment process. Since blockchain runs on smart contracts, an investment can be fulfilled immediately, rather than waiting a few days, after the blockchain deems that investment valid. The peer-to-peer investment process — in this case an individual investing directly with a company instead of through a broker — speeds up the process and eliminates unnecessary steps. Blockchain’s tightened security encryption protocols severely minimize the risk of a financial data breach.   Blockchain has also introduced another breakthrough investment idea in the form of Initial Coin Offerings. Instead of the traditional method of raising capital in an Initial Public Offering on the stock market, ICOs offer digital tokens that represent ownership stakes in a company. More companies are turning to blockchain-based ICOs because they offer a faster, safer and more accurate way of collecting capital. ICOs have already helped raise $3.2 billion through July of 2022. These organizations are evolving the investment process into a lean, mean blockchain machine. Founded: 1992 Location: Chicago, Illinois Trading firm DRW aims to bring innovation to markets and exchanges worldwide. Cumberland is a DRW subsidiary focused on the cryptoasset space. In addition to providing expertise in spot cryptocurrency liquidity, listed options and futures, bilateral crypto options and non-deliverable forwards, Cumberland also invests in select web3 and blockchain ventures. Founded: 2013 Location: San Francisco, California Even though fintech company Cash App maintains its banking and peer-to-peer payment features, it has embraced blockchain technology. The company says it aims to enable users to buy and sell blockchain by reducing barriers to entry for cryptocurrency exchanges. Cash App also produces cryptocurrency educational content to demonstrate its commitment to what it sees as the transformative potential of blockchain for the entire finance industry. Founded: 2013 Location: Menlo Park, California Robinhood is one of the largest online trading platforms allowing investors to buy, sell and trade cryptocurrencies. Originally intended as a platform for individuals to boost their personal stock portfolios via traditional stocks, Robinhood now allows investments in blockchain-based currencies like Bitcoin and Zcash. Founded: 2019 Location: New York, New York With the goal of making investing more accessible to the general public, Public.com has developed a mobile app where customers can invest in diverse funds and manage their portfolios. An intuitive design and social feed make it easy for individuals to navigate the app while learning why people make certain investment decisions. Investors can also take their pick of popular cryptocurrencies, including Dogecoin, Ether, Bitcoin and Algorand. Founded: 2013 Location: Stamford, Connecticut Grayscale Investments serves individuals and institutions with a range of investment options, including opportunities to reap the economic rewards of blockchains. Among its collection of single assets, the firm allows clients to invest in funds covering Bitcoin, Decentraland and Ethereum. As a result, investors can branch out from traditional funding routes to explore the latest developments in the digital economy. Related ReadingBuy Your Dream Home With a Blockchain Mortgage: 7 Companies Using DLT for Lending and Credit Blockchain Loyalty and Rewards Programs Maintaining and growing a customer base can make or break many companies. It’s no coincidence that well-performing stocks — like Apple, Disney and Amazon — have expansive customer loyalty programs and millions of diehard fans. Businesses looking to increase revenue and retain customers have found another solution: blockchain-based loyalty rewards. For most companies, current loyalty programs are hard to keep data on, are outdated and are at severe risk of data breaches. In a 2018 study, IBM found that 73 percent of respondents believe businesses value profits over data security and that 75 percent won’t even buy a company’s products if they don’t trust the company to protect their personal information. Customer loyalty programs have become a target of cyber attackers, but blockchain is a potential solution for making the programs safer, larger and more precise. The finance industry, like any business, wants a piece of the massive data and profits customer loyalty rewards programs can bring. Blockchain can optimize the process further by reducing costs, enabling a seamless, real-time program and safeguarding important data. The implementation of smart contracts allows customers to collect rewards in real-time and for businesses to manage their data better. Centralizing a customer’s loyalty programs in one blockchain-based wallet encourages consumers to use their rewards more frequently. Additionally, customers will build a trust and affinity for companies using a high-level security blockchain to secure their personal information. Here are examples of companies helping to implement blockchain-based rewards programs. Founded: 1850 Location: New York, New York Although it remains an established presence in the world of fintech, American Express is still experimenting with newer financial fields such as blockchain-powered rewards programs. The company has joined forces with crypto platform Abra to offer the Abra crypto card, which allows customers to accumulate cryptocurrency rewards when they make purchases from brands within the American Express network. Founded: 2014 Location: San Francisco, California Loyyal helps businesses expand their customer loyalty programs with a Blockchain-as-a-Service platform. So far, the company has implemented blockchain rewards programs in the travel, employee incentives and credit card industries. Since its development, Loyyal’s blockchain programs have yielded 31 percent annual growth in customer program enrollment. Founded: 2009 Location: New York, New York Expanding one’s crypto portfolio becomes effortless with Venmo’s credit card, which supplies customers with crypto rewards. Purchases in transportation, grocery, entertainment and other categories can all earn spenders the right to convert cash into crypto. After activating the crypto auto purchase feature, customers can immediately invest their rewards in currencies such as Bitcoin, Litecoin and Ethereum. Digital Identity on Blockchain One of the most serious responsibilities of financial institutions is maintaining the integrity of a customer’s digital identity, comprising some of our most sensitive information. We trust banks with safeguarding our passport information, biometric scans, social security number, accounts and addresses with the expectations that these institutions will keep them private. Unfortunately, over 2.8 million consumers in 2021 reported fraud cases, including cases of stolen credit and bank information, that amounted to more than $5.8 billion in losses. Blockchain has the ability to stop hackers in their tracks. The most significant endorsement of blockchain’s security prowess came at the 2018 World Economic Forum in Davos, Switzerland. The Forum concluded blockchain increases trust, accountability and efficiency in data security. Notably, the conference indicated that the financial industry can usher in a new age of digital identity security by leveraging blockchain’s decentralized mechanisms against increased risk and cyber attacks. Here are a few companies helping the financial sector maintain the integrity of millions of digital identities. Founded: 1911 Location: Armonk, New York IBM has become one of the world’s leading corporations investing in blockchain, especially in the area of digital identity management. The computer giant helps install personalized blockchain-based “Trusted

Identity” management solutions that use decentralized ID authentication and an updated due diligence platform. This way, individuals can stay connected while monitoring who can view their personal information. Founded: 2014 Location: Sparks, Nevada Blockchains provides digital identity management software tools for its customers. Users can leverage the company’s system to create digital representations of themselves with distributed information like digital documents and devices. Key management technology provides an additional layer of security, enabling customers to control access to their data, recover lost e-wallets and perform other blockchain-related tasks. Founded: 2015 Location: San Francisco, California Civic’s secure identity platform uses multi-factor authentication on mobile apps and the web without the need for passwords. The blockchain technology privately saves encrypted customer biometric information like thumbprints, so logins to bank accounts or websites are smooth and virtually incorruptible. A unique feature of Civic’s product is that any customer can revoke their name from the blockchain at any time, permanently deleting the information and making it useless to would-be criminals. Other Blockchain Applications Founded: 2009 Location: Oakland, California Block aims to facilitate economic empowerment for consumers and businesses around the world through its family of fintech brands. The company designed a bitcoin mining chip and is now expanding the project to include development of a bitcoin mining system, which would involve miners using software and hardware to verify transactions on the cryptocurrency blockchain. This content is for informational and educational purposes only. Built In strives to maintain accuracy in all its editorial coverage, but it is not intended to be a substitute for financial or legal advice. Rose Velazquez contributed reporting to this story. Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. Blockchain is a shared, immutable digital ledger, enabling the recording of transactions and the tracking of assets within a business network and providing a single source of truth. Blockchain operates as a decentralized distributed database, with data stored across multiple computers, making it resistant to tampering. Transactions are validated through a consensus mechanism, ensuring agreement across the network. In blockchain technology, each transaction is grouped into blocks, which are then linked together, forming a secure and transparent chain. This structure guarantees data integrity and provides a tamper-proof record, making blockchain ideal for applications like cryptocurrencies and supply chain management. The key benefit of blockchain lies in its ability to provide security, transparency and trust without relying on traditional intermediaries, such as banks or other third parties. Its design reduces the risk of fraud and errors, making it especially valuable in industries where secure transactions are critical, including finance and healthcare. Additionally, blockchain helps businesses improve efficiency and reduce costs by streamlining processes and enhancing accountability. Discover expertly curated insights and news on AI, cloud and more in the weekly Think Newsletter. Blockchain technology began with the introduction of Bitcoin in 2008, created by an anonymous figure or group known as Satoshi Nakamoto. Bitcoin’s underlying technology was designed as a decentralized digital currency to enable peer-to-peer transactions without the need for a trusted intermediary like a bank. The blockchain served as a public ledger, securely recording all transactions and preventing double-spending, a key issue for digital currencies at the time. With the development of platforms like Ethereum in 2015, blockchain began to support smart contracts—digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met. This development broadened blockchain’s real-world applications, extending into areas such as real estate, finance, supply chain management, healthcare and even voting systems. Over time, blockchain has grown well beyond its cryptocurrency roots, becoming a key player in decentralized finance (DeFi) and non-fungible tokens (NFTs). Today, blockchain continues to evolve, with ongoing advancements aimed at improving scalability, privacy and its integration with emerging technologies like artificial intelligence (AI) and the Internet of Things (IoT). According to a report from Statista, blockchain technology is forecast to grow by nearly 1 trillion U.S. dollars by 2032, with a compound annual growth rate (CAGR) of 56.1 percent since 2021.1 Blockchain technology offers various benefits that transform businesses’ operations, enhancing trust, security, traceability and efficiency across multiple industries. Here are some top benefits of blockchain: Greater trust Blockchain creates a secure, members-only network, ensuring accurate and timely data access. Confidential records are shared only with authorized network members, fostering trust and creating end-to-end visibility across the system. Enhanced security Consensus among network members is required to validate data accuracy, and all validated transactions are immutable and permanently recorded. This capability guarantees that no transaction can be deleted, even by a system administrator. Better traceability Blockchain offers instant traceability with a transparent audit trail of an asset’s journey. In industries prioritizing sustainability, it enables direct sharing of provenance data, verifying ethical practices. Additionally, it can reveal supply chain inefficiencies, such as delays, driving greater accountability. Increased efficiency With a distributed ledger shared among network members, the need for time-consuming record reconciliations is eliminated. Smart contracts, which are stored on the blockchain, can automate processes and speed up transactions. Automated transactions Smart contracts facilitate the seamless automation of transactions, enhancing efficiency and accelerating real-time processes. Once predefined conditions are met, they automatically trigger the next step, reducing the need for manual intervention. Blockchain technology contains several key features that enhance security, transparency and efficiency in transactions and data management: Distributed ledger technology All network participants have access to the distributed ledger and its immutable record of transactions. This shared ledger records transactions only once, eliminating the duplication of effort typical of traditional business networks. No participant can change or tamper with a transaction after it’s been recorded in the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible. Smart contracts are self-executing agreements stored on the blockchain, where the terms are written in code and automatically executed when predefined conditions are met. They can be used for various purposes, such as transferring corporate bonds or triggering travel insurance payouts. By automating these processes, smart contracts speed up transactions, reduce the need for intermediaries and ensure transparency and security. Public key cryptography is a method used to secure transactions and data on the blockchain by leveraging two cryptographic keys: a public key and a private key. The public key serves as an address for receiving cryptocurrency or data, while the private key is a confidential key that grants control over the associated digital assets. The private key holder can authorize transactions, providing security and verifying ownership, while the public key allows others to send funds or data to the correct address. Blockchain technology records transactions securely by linking data blocks together. Each block contains important details about asset movements and ensures the integrity of the entire process. Here’s how it works. Each transaction is recorded as a “block” of data on the blockchain. These blocks capture key details about the movement of assets, whether tangible (such as a product) or intangible (such as intellectual property). The data within each block includes critical information, such as who, what, when, where, the transaction amount, and specific conditions like the temperature of a food shipment. Additionally, each block contains a timestamp, which records the exact moment the transaction is added to the blockchain. This timestamp ensures the chronological order of transactions and adds an additional layer of verifiability to the data, preventing any retrospective alterations to the recorded information. Each block is linked to the previous block and the one after it, creating a secure chain of data. This is done through cryptographic hashes, unique identifiers for each block. The hash of a block includes data from the previous block, ensuring the exact sequence and timing of each transaction. The cryptographic hash makes it nearly impossible to alter any block without changing all subsequent blocks, ensuring the integrity of the entire process. The blocks are grouped together in an irreversible chain known as a blockchain. Each new block reinforces the security and validation of the previous one, strengthening the entire chain. This makes the blockchain tamper-evident, ensuring malicious actors cannot alter or insert fraudulent transactions into the chain. Nodes in the blockchain network validate and maintain the blockchain by confirming each transaction’s validity through consensus algorithms, ensuring the system remains secure and immutable. Proof of Work (PoW) and Proof of Stake (PoS) are some of the most commonly used consensus algorithms in blockchain networks, each helping to secure the system while validating transactions. With each new block, the blockchain becomes more secure, making it nearly impossible to change past transactions. This immutability provides a trusted, transparent ledger that all network members can rely on, preventing fraud and ensuring that all transaction records are accurate and unchangeable. There are several ways to build a blockchain network. They can be public, private, permissioned or consortium-built: Public blockchain networks: A public blockchain is open for anyone to join and participate in, such as the Bitcoin blockchain. While it offers decentralization, it also comes with drawbacks, including high computational power requirements, lack of transaction privacy and potentially weaker security. These considerations are crucial, especially for enterprise blockchain use cases. Private blockchain networks: A private blockchain network, similar to a public blockchain network, is a decentralized peer-to-peer network. However, one organization governs the network, controlling who is allowed to participate, run a consensus protocol and maintain the shared ledger. Depending on the use case, this can significantly boost trust and confidence between participants. A private blockchain can be run behind a corporate firewall and even be hosted on premises. Permissioned blockchain networks: Businesses that set up a private blockchain will generally set up a permissioned blockchain network. It is important to note that public blockchain networks can also be permissioned. This places restrictions on who is allowed to participate in the network and in what record transactions. Participants need to obtain an invitation or permission to join. Consortium blockchain networks: A consortium blockchain network is managed by a group of preselected organizations that share the responsibility of maintaining the blockchain. These organizations determine who can submit transactions and access data. This type of network is ideal when multiple parties need to collaborate with shared responsibilities, such as in the energy sector, where multiple energy producers and consumers might share data about power usage and distribution. Blockchain protocols are the set of rules that govern how data is recorded, shared and secured within a blockchain network. These protocols establish the foundation for the network’s operation. However, to fully take advantage of these protocols, developers need a platform that provides the environment and tools to build, deploy and interact with decentralized applications (dApps). Blockchain platforms, therefore, build on top of these protocols, offering the necessary infrastructure and services to create and run apps within the blockchain ecosystem. While protocols define the core functionality, platforms extend this functionality by enabling the development of practical solutions. Blockchain protocols and platforms often overlap, as platforms usually rely on specific protocols to operate. Here’s a rundown of common blockchain protocols and platforms: Hyperledger Fabric, an open-source project from the Linux® Foundation, is the modular blockchain framework and has become the unofficial standard for enterprise blockchain platforms like the IBM Blockchain® Platform. Intended as a foundation for developing enterprise-grade applications and industry strategies, the open, modular architecture of Hyperledger Fabric uses plug-and-play components to accommodate a wide range of business use cases. Ethereum is a decentralized, open-source blockchain platform that allows developers to build and deploy smart contracts and decentralized applications. Ethereum Enterprise is designed specifically for business blockchain applications. Corda is a distributed ledger platform designed for businesses, enabling secure and private transactions on permissioned networks. It allows organizations to share data and execute agreements with only the relevant parties, making it ideal for industries like finance, healthcare and supply chain management. Corda prioritizes privacy, scalability and regulatory compliance. Quorum is an open-source, permissioned blockchain platform based on Ethereum, designed for enterprise use. It provides high privacy and scalability, allowing businesses to run smart contracts and conduct transactions securely within a private network. Quorum supports features like transaction privacy and faster consensus mechanisms, making it ideal for financial institutions where confidentiality and regulatory compliance are crucial. When building an enterprise blockchain application, it’s essential to have a comprehensive blockchain security strategy that uses cybersecurity frameworks, assurance services and best practices to reduce risks against attacks and fraud. This strategy should encompass key areas like identity and access management (IAM), ensuring only authorized users can access critical components, and utilize strong encryption techniques for data protection. In addition, adopting effective consensus mechanisms that are resistant to attacks is crucial for maintaining the integrity of the network. Other important security imperatives include the following: Regularly audit and test smart contracts for vulnerabilities, as flaws in their code can lead to serious security breaches. Comply with industry regulations, such as GDPR or financial standards, using privacy-enhancing technologies like zero-knowledge proofs. Integrate secure messaging protocols to facilitate confidential communication within the blockchain-based network, ensuring that messages and transactions remain private and tamper-proof. Utilize continuous monitoring and a well-defined incident response plan to ensure that any security issues are detected and addressed promptly, minimizing the impact of potential threats. Bitcoin is the first decentralized digital currency to enable peer-to-peer transactions without a central authority. It uses blockchain technology as its underlying infrastructure, acting as a distributed ledger that records and verifies all Bitcoin transactions. As the most well-known cryptocurrency, Bitcoin plays a central role in the blockchain ecosystem, but it’s also part of a much larger and evolving market. The pricing in the Bitcoin and cryptocurrency space is highly volatile, with factors such as technological advancements, market sentiment, investor demand and regulatory changes playing a significant role. Combining blockchain and AI creates new opportunities for businesses across various industries. Using blockchain’s immutable ledger and decentralization, AI can improve data transparency and security, addressing challenges like explainable AI. For example, in supply chain management, blockchain ensures the traceability and authenticity of products, while AI analyzes data to predict demand and optimize logistics. AI helps automate risk assessments in financial services, while blockchain secures transactions and ensures compliance. Beyond these applications, the integration of blockchain and AI is also making significant strides in industries like healthcare. Healthcare providers are using AI to analyze patient data for personalized treatments and blockchain solutions to ensure the privacy and security of medical records. This convergence enhances trust, boosts efficiency and supports process automation, leading to faster, more reliable business operations across industries. A blockchain is a distributed database or ledger shared across a computer network's nodes. They are best known for their crucial role in cryptocurrency systems, maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—meaning it cannot be altered. Since a block can’t be changed, the only trust needed is at the point where a user or program enters data. This reduces the need for trusted third parties, such as auditors or other humans, who add costs and can make mistakes. Since Bitcoin's introduction in 2009, blockchain uses have exploded via the creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. Blockchain is a type of shared database that differs from a typical database in the way it stores information; blockchains store data in blocks linked together via cryptography.Different types of information can be stored on a blockchain, but the most common use has been as a transaction ledger. In Bitcoin’s case, the blockchain is decentralized, so no single person or group has control—instead, all users collectively retain control.Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, transactions are permanently recorded and viewable to anyone. Investopedia / Xiaojie Liu You might be familiar with spreadsheets or databases. A blockchain is somewhat similar because it is a database where information is entered and stored. The key difference between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed. A blockchain consists of programs called scripts that conduct the tasks you usually would in a database: entering and accessing information, and saving and storing it somewhere. A blockchain is distributed, which means multiple copies are saved on many machines, and they must all match for it to be valid. The Bitcoin blockchain collects transaction information and enters it into a 4MB file called a block (different blockchains have different size blocks). Once the block is full, the block data is run through a cryptographic hash function, which creates a hexadecimal number called the block header hash. The hash is then entered into the following block header and encrypted with the other information in that block's header, creating a chain of blocks, hence the name “blockchain.” Transactions follow a specific process, depending on the blockchain. For example, on Bitcoin's blockchain, if you initiate a transaction using your cryptocurrency wallet—the application that provides an interface for the blockchain—it starts a sequence of events. In Bitcoin, your transaction is sent to a memory pool, where it is stored and queued until a miner picks it up. Once it is entered into a block and the block fills up with transactions, it is closed, and the mining begins. Every node in the network proposes its own blocks in this way because they all choose different transactions. Each works on their own blocks, trying to find a solution to the difficulty target, using the "nonce," short for number used once. The nonce value is a field in the block header that is changeable, and its value incrementally increases with every mining attempt. If the resulting hash isn't equal to or less than the target hash, a value of one is added to the nonce, a new hash is generated, and so on. The nonce rolls over about every 4.5 billion attempts (which takes less than one second) and uses another value called the extra nonce as an additional counter. This continues until a miner generates a valid hash, winning the race and receiving the reward. Generating these hashes until a specific value is found is the "proof-of-work" you hear so much about—it "proves" the miner did the work. The sheer amount of work it takes to validate the hash is why the Bitcoin network consumes so much computational power and energy. Once a block is closed, a transaction is complete. However, the block is not considered confirmed until five other blocks have been validated. Confirmation takes the network about one hour to complete because it averages just under 10 minutes per block (the first block with your transaction and five following blocks multiplied by 10 equals 60 minutes). Not all blockchains follow this process. For instance, the Ethereum network randomly chooses one validator from all users with ether staked to validate blocks, which are then confirmed by the network. This is much faster and less energy intensive than Bitcoin's process. A blockchain allows the data in a database to be spread out among several network nodes—computers or devices running software for the blockchain—at various locations. This creates redundancy and maintains the fidelity of the data. For example, if someone tries to alter a record on one node, the other nodes would prevent it from happening by comparing block hashes. This way, no single node can alter information within the chain. Because of this distribution—and the encrypted proof that work was done—the blockchain data, such as transaction history, becomes irreversible. Such a record could be a list of transactions, but private blockchains can also hold a variety of other information like legal contracts, state identifications, or a company's inventory. Most blockchains wouldn't "store" these items directly; they would likely be sent through a hashing algorithm and represented on the blockchain by a token. Because of the decentralized nature of the Bitcoin blockchain, all transactions can be transparently viewed by downloading and inspecting them or by using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track a bitcoin wherever it goes. For example, exchanges have been hacked in the past, resulting in the loss of large amounts of cryptocurrency. While the hackers may have been anonymous—except for their wallet address—the crypto they extracted is easily traceable because the wallet addresses are stored on the blockchain. Of course, the records stored in the Bitcoin blockchain (as well as most others) are encrypted. This means that only the person assigned an address can reveal their identity. As a result, blockchain users can remain anonymous while preserving transparency. Blockchain technology achieves decentralized security and trust in several ways. To begin, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added to the end of the blockchain, previous blocks cannot be altered. A change in any data changes the hash of the block it was in. Because each block contains the previous block's hash, a change in one would change the following blocks. The network would generally reject an altered block because the hashes would not match. However, a change can be accomplished on smaller blockchain networks. Not all blockchains are 100% impenetrable. They are distributed ledgers that use code to create the security level they have become known for. If there are vulnerabilities in the coding, they can be exploited. A new and smaller chain might be susceptible to this kind of attack, but the attacker would need at least half of the computational power of the network (a 51% attack). On the Bitcoin and other larger blockchains, this is nearly impossible. By the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter. This is because the rate at which these networks hash is exceptionally rapid—the Bitcoin network hashed at a rate of around 640 exahashes per second (18 zeros) as of September 2024. The Ethereum blockchain is not likely to be hacked either—again, the attackers would need to control more than half of the blockchain's staked ether. As of September 2024, over 33.8 million ETH has been staked by more than one million validators. An attacker or a group would need to own over 17 million ETH, and be randomly selected to validate blocks enough times to get their blocks implemented. Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn’t until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application. The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin’s pseudonymous creator, Satoshi Nakamoto, referred to it as “a new electronic cash system that’s fully peer-to-peer, with no trusted third party.” The key thing to understand is that Bitcoin uses blockchain as a means to transparently record a ledger of payments or other transactions between parties. Blockchain can be used to immutably record any number of data points. The data can be transactions, votes in an election, product inventories, state identifications, deeds to homes, and much more. Currently, tens of thousands of projects are looking to implement blockchains in various ways to help society other than just recording transactions—for example, as a way to vote securely in democratic elections. The nature of blockchain's immutability means that fraudulent voting would become far more difficult. For example, a voting system could work such that each country's citizens would be issued a single cryptocurrency or token. Each candidate could then be given a specific wallet address, and the voters would send their token or crypto to the address of whichever candidate they wish to vote for. The transparent and traceable nature of blockchain would eliminate the need for human vote counting and the ability of bad actors to tamper with physical ballots. Blockchains have been heralded as a disruptive force in the finance sector, especially with the functions of payments and banking. However, banks and decentralized blockchains are vastly different. To see how a bank differs from blockchain, let’s compare the banking system to Bitcoin’s blockchain implementation. As we now know, blocks on Bitcoin’s blockchain store transactional data. Today, tens of thousands of other cryptocurrencies run on a blockchain. But it turns out that blockchain can be a reliable way to store other types of data as well. Some companies experimenting with blockchain include Walmart, Pfizer, AIG, Siemens, and Unilever, among others. For example, IBM has created its Food Trust blockchain to trace the journey that food products take to get to their locations. Why do this? The food industry has seen countless outbreaks of E. coli, salmonella, and listeria; in some cases, hazardous materials were accidentally introduced to foods. In the past, it has taken weeks to find the source of these outbreaks or the cause of sickness from what people are eating. Using blockchain allows brands to track a food product’s route from its origin, through each stop it makes, to delivery. Not only that, but these companies can also now see everything else it may have come in contact with, allowing the identification of the problem to occur far sooner—potentially saving lives. This is one example of blockchain in practice, but many other forms of blockchain implementation exist or are being experimented with. Perhaps no industry stands to benefit from integrating blockchain into its business operations more than personal banking. Financial institutions only operate during business hours, usually five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see the money in your account. Even if you make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps. By integrating blockchain into banks, consumers might see their transactions processed in minutes or seconds—the time it takes to add a block to the blockchain, regardless of holidays or the time of day or week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. Given the sums involved, even the few days the money is in transit can carry significant costs and risks for banks. The settlement and clearing process for stock traders can take up to three days (or longer if trading internationally), meaning that the money and shares are frozen for that period. Blockchain can, in theory, drastically reduce that time. Blockchain forms the bedrock for cryptocurrencies like Bitcoin. This design also allows for easier cross-border transactions because it bypasses currency restrictions, instabilities, or lack of infrastructure by using a distributed network that can reach anyone with an internet connection. Healthcare providers can leverage blockchain to store their patients’ medical records securely. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key so that they are only accessible to specific individuals, thereby ensuring privacy. If you have ever spent time in your local Recorder’s Office, you will know that recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county’s central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index. This process is not just costly and time-consuming, it is also prone to human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanently recorded. Proving property ownership can be nearly impossible in war-torn countries or areas with little to no government or financial infrastructure and no Recorder’s Office. If a group of people living in such an area can leverage blockchain, then transparent and clear timelines of property ownership could be maintained. A smart contract is computer code that can be built into the blockchain to facilitate transactions. It operates under a set of conditions to which users agree. When those conditions are met, the smart contract conducts the transaction for the users. As in the IBM Food Trust example, suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of not only their products but also common labels such as “Organic,” “Local,” and “Fair Trade.” As reported by Forbes, the food industry is increasingly adopting the use of blockchain to track the path and safety of food throughout the farm-to-user journey. As mentioned above, blockchain could facilitate a modern voting system. Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using blockchain in this way would make votes nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election. For all of its complexity, blockchain’s potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above. But there are also some disadvantages. Transactions on the blockchain network are approved by thousands of computers and devices. This removes almost all people from the verification process, resulting in less human error and an accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain and not be accepted by the rest of the network. Typically, consumers pay a bank to verify a transaction or a notary to sign a document. Blockchain eliminates the need for third-party verification—and, with it, their associated costs. For example, business owners incur a small fee when they accept credit card payments because banks and payment-processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees. Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes significantly more difficult to tamper with. Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Financial institutions operate during business hours, usually five days a week—but a blockchain runs 24 hours a day, seven days a week, and 365 days a year. On some blockchains, transactions can be completed and considered secure in minutes. This is particularly useful for cross-border trades, which usually take much longer because of time zone issues and the fact that all parties must confirm payment processing. Many blockchain networks operate as public databases, meaning anyone with an internet connection can view a list of the network’s transaction history. Although users can access transaction details, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like Bitcoin are fully anonymous; they are actually pseudonymous because there is a viewable address that can be associated with a user if the information gets out. Once a transaction is recorded, its authenticity must be verified by the blockchain network. After the transaction is validated, it is added to the blockchain block. Each block on the blockchain contains its unique hash and the unique hash of the block before it. Therefore, the blocks cannot be altered once the network confirms them. Many blockchains are entirely open source. This means that everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. However, it also means there is no real authority on who controls Bitcoin’s code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile, then Bitcoin can be updated. Private or permission blockchains may not allow for public transparency, depending on how they are designed or their purpose. These types of blockchains might be made only for an organization that wishes to track data accurately without allowing anyone outside of the permissioned users to see it. Alternatively, there might come a point where publicly traded companies are required to provide investors with financial transparency through a regulator-approved blockchain reporting system. Using blockchains in business accounting and financial reporting would prevent companies from altering their financials to appear more profitable than they really are. Perhaps the most profound facet of blockchain and cryptocurrency is the ability for anyone, regardless of ethnicity, gender, location, or cultural background, to use it. According to The World Bank, an estimated 1.4 billion adults do not have bank accounts or any means of storing their money or wealth. Moreover, nearly all of these individuals live in developing countries where the economy is in its infancy and entirely dependent on cash. These people are often paid in physical cash. They then need to store this physical cash in hidden locations in their homes or other places, incentivizing robbers or violence. While not impossible to steal, crypto makes it more difficult for would-be thieves. Although blockchain can save users money on transaction fees, the technology is far from free. For example, the Bitcoin network's proof-of-work system to validate transactions consumes vast amounts of computational power. In the real world, the energy consumed by the millions of devices on the Bitcoin network is more than the country of Pakistan consumes annually. Some solutions to these issues are beginning to arise. For example, bitcoin-mining farms have been set up to use solar power, excess natural gas from fracking sites, or energy from wind farms. Bitcoin is a perfect case study of the inefficiencies of blockchain. Bitcoin's PoW system takes about 10 minutes to add a new block to the blockchain. At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS). Although other cryptocurrencies, such as Ethereum, perform better than Bitcoin, the complex structure of blockchain still limits them. Legacy brand Visa, for context, can process 65,000 TPS. Solutions to this issue have been in development for years. There are currently blockchain projects that claim tens of thousands of TPS. Ethereum is rolling out a series of upgrades that include data sampling, binary large objects (BLOBs), and rollups. These improvements are expected to increase network participation, reduce congestion, decrease fees, and increase transaction speeds. The other issue with many blockchains is that each block can only hold so much data. The block size debate has been and continues to be one of the most pressing issues for the scalability of blockchains in the future. While confidentiality on the blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the blockchain network. The most cited example of blockchain being used for illicit transactions is probably the Silk Road, an online dark web illegal-drug and money laundering marketplace operating from February 2011 until October 2013, when the FBI shut it down. The dark web allows users to buy and sell illegal goods without being tracked by using the Tor Browser and make illicit purchases in Bitcoin or other cryptocurrencies. This is in stark contrast to U.S. regulations, which require financial service providers to obtain information about their customers when they open an account. They are supposed to verify the identity of each customer and confirm that they do not appear on any list of known or suspected terrorist organizations. Illicit activity accounted for only 0.34% of all cryptocurrency transactions in 2023. This system can be seen as both a pro and a con. It gives anyone access to financial accounts, but allows criminals to transact more easily. Many have argued that the good uses of crypto, like banking the unbanked, outweigh the bad uses of cryptocurrency, especially when most illegal activity is still accomplished through untraceable cash. Public perception of blockchain and cryptocurrencies, in particular, remains uneasy. High-profile collapses of once-trusted cryptocurrency brokers, such as Mt. Gox back in 2014, or FTX in November 2022, persistence of various crypto scams, and general skepticism towards new technology and its bold promises, all contribute to ongoing public skepticism about a decentralized future. As of 2024, 44% of Americans still say they will never purchase a cryptocurrency. Many in the crypto space have expressed concerns about government regulation of cryptocurrencies. Several jurisdictions are tightening control over certain types of crypto and other virtual currencies. However, no regulations have yet been introduced that focus on restricting blockchain uses and development, only certain products created using it. Another significant implication of blockchains is that they require storage. This may not appear to be substantial because we already store lots of information and data. However, as time passes, the growing blockchain use will require more storage, especially on blockchains where nodes store the entire chain. Currently, data storage is centralized in large centers. But if the world transitions to blockchain for every industry and use, its exponentially growing size would require more advanced techniques to make storage more efficient, or force participants to continually upgrade their storage. This could become significantly more expensive in terms of both money and physical space needed, as the Bitcoin blockchain itself was over 600 gigabytes as of September 15th, 2024—and this blockchain records only bitcoin transactions. This is small compared to the amount of data stored in large data centers, but a growing number of blockchains will only add to the amount of storage already required for the digital world. Simply put, a blockchain is a shared database or ledger. Bits of data are stored in files known as blocks, and each network node has a replica of the entire database. Security is ensured since the majority of nodes will not accept a change if someone tries to edit or delete an entry in one copy of the ledger. Imagine you typed some information into a document on your computer and sent it through a program that gave you a string of numbers and letters (called hashing, with the string called a hash). You add this hash to the beginning of another document and type information into it. Again, you use the program to create a hash, which you add to the following document. Each hash is a representation of the previous document, which creates a chain of encoded documents that cannot be altered without changing the hash. Each document is stored on computers in a network. This network of programs compares each document with the ones they have stored and accepts them as valid based on the hashes they generate. If a document doesn't generate a hash that is a match, that document is rejected by the network. A blockchain is a distributed network of files chained together using programs that create hashes, or strings of numbers and letters that represent the information contained in the files. Every network participant is a computer or device that compares these hashes to the one they generate. If there is a match, the file is kept. If there isn't, the file is rejected. With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself in no small part because of Bitcoin and cryptocurrency. As a buzzword on the tongue of every investor across the globe, blockchain stands to make business and government operations more accurate, efficient, secure, and cheap, with fewer intermediaries. As we head into the third decade of blockchain, it’s no longer a question of if legacy companies will catch on to the technology—it’s a question of when. Today, we see a proliferation of NFTs and the tokenization of assets. Tomorrow, we may see a combination of blockchains, tokens, and artificial intelligence all incorporated into business and consumer solutions. The comments, opinions, and analyses expressed on Investopedia are for informational purposes online. Read our warranty and liability disclaimer for more info. Linking the nodes to make a distributed ledger.© Vadim Shechkov—iStock/Getty ImagesBlockchain may be among the buzziest technologies to disrupt the world of finance, tied to the rise of cryptocurrency, but it’s refashioning perhaps the most archaic of all financial tech: the ledger. Yes, the system that originated from the clay tablets ancient Mesopotamians used thousands of years ago to record transactions and balances.This latest iteration, however, has bells and whistles that make the ledger capable of overturning the entire financial environment that once brought it into existence. How’s that for an upgrade?Blockchain is a digital ledger database whose recorded contents are encrypted into a sequence of blocks and distributed throughout a network of participating computers (nodes).It’s really that simple. So, what’s with all the buzz? It sounds like a slightly upgraded, shareable spreadsheet with tracked changes, right?Blockchain’s functionalities may seem plain and straightforward. But given its tweaks to the old ledger tech, it now sports a few features that would be considered impossible in the soon-to-be old world of today.Blockchain is:Immutable. Entries can’t be changed once they’re recorded. Decentralized. It’s capable of operating without third-party entities, human or not. Distributed. All participating computers have a copy of the ledger. Consensus. All transactions are verified and updated in consensus. Secure. All recorded content is individually encrypted.In short, blockchain has the potential to revolutionize almost every digital operation we know today, from sending payments and issuing contracts to undergirding complex industrial and government operations.Something this large in scale is likely to present a wide range of opportunities—but also plenty of risks—for users and investors alike.How does blockchain technology work?The critical aspect that separates blockchain from all other ledgers and databases is that it’s designed to distribute and record information on a peer-to-peer basis that, once completed, is unchangeable and incorruptible.Immutable verification is one of blockchain’s key features. All data contents are “set in stone,” so to speak, but digitally. And blockchain networks accomplish this goal using strict consensus verification procedures. So, how does it work?Digital transactions are stored in a digital “block” (sort of like a ledger entry) that’s added to a previous “chain” of blocks; hence the term blockchain. Each block has a unique “hash,” like a signature or identification code, and a time stamp to show the exact time it was validated or mined. Each block contains the previous block’s hash, forming the chain.Once a block is added to the blockchain, all nodes (participating computers) update their copy of the blockchain. This is what makes the blockchain a secure system. Any changes to the contents of a single block have to be recorded in a new block, making it nearly impossible to rewrite a block’s history.If a hacker tried to tamper with an existing block, then they would have to change all copies of that block on all participating computers in the network. That’s virtually impossible—the number of participating computers across the globe can number in the high thousands. Unless every single node in the network agrees with a change to a block, the change is discarded.What makes blockchain technology so revolutionary?There are many potential benefits that come with the adoption of blockchain technology. Here are three to consider:Blockchain can drastically reduce or nearly eliminate data tampering. Blockchain can significantly increase data security. This is why the technology is often called a “trustless network.” It means you don’t have to trust anyone to be certain that a given exchange or transaction is accurate and accurately recorded.Blockchain can make transactions more transparent and traceable. Because it’s a distributed ledger, all participating computers on a network have access to the same database (the blockchain itself). This increases transparency and access, and the hash history makes every exchange and transaction traceable.Blockchain can eliminate the need for centralized third parties. An automated network that allows for peer-to-peer transactions does away with the need for intermediaries. That may include the elimination of third-party service fees and any lag time caused by paper-based or human-driven processes.How can blockchain be used?Any industry that can use a peer-to-peer transaction system with an immutable ledger can benefit from blockchain technology. It’s easy to imagine how expansive blockchain applications can be.The cryptocurrency industry made blockchain something of a household term; decentralized and traditional finance may soon follow crypto’s cue. Other fields that may adopt blockchain technologies include non-fungible token (NFT) markets, supply chain and logistics, energy, health care, e-commerce, media, voting systems, and government and public sector operations. A key to innovation may be smart contracts—blockchain-based computer programs or transaction protocols that function as digital contracts—and the decentralized applications (dApps) that use them.Again, we’re still at the beginning stages of blockchain development. Although its potential use cases are many and various, it’s important to remember that wide-scale adoption hasn’t quite begun.What are the risks?Every unique technology comes with its own unique set of risks. Blockchain is no exception.Although the blockchain itself may not be hackable—remember, it’s an immutable ledger—the systems surrounding the blockchain can be hacked.The simplest example is that of a bad actor obtaining passwords and credentials to access digital assets. Unsecured and exposed goods can be stolen.A more sophisticated risk is that of a 51% attack. In cryptocurrency applications, this means a single entity could gain control of more than 50% of all cryptocurrency mining or staking. Once in control, the entity may not be able to alter previous blocks on the chain, but it can alter future blocks. For instance, it may be able to prevent or reverse transactions, possibly even double-spending any cryptocurrency pending a slot in the block.For large networks like Bitcoin and Ethereum, a 51% attack may be too difficult and too costly to attempt. But for smaller networks, it may be possible.How can a person invest in blockchain technology?Probably the most direct and regulated way to invest in blockchain tech is by investing in stocks of publicly traded companies that are developing blockchain networks.You can also gain indirect exposure by investing in companies involved in decentralized finance, financial technology (FinTech), metaverse technologies, cryptocurrency exchanges, or hardware designed for crypto, blockchain, or decentralized finance (DeFi) purposes.Your other options are to purchase digital assets such as cryptocurrencies or NFTs. Note that the crypto world is largely unregulated, so scams and fraudulent activity are frequently reported. Plus, cryptocurrencies and their underlying investments are highly volatile (i.e., prices tend to swing violently).The bottom lineBlockchain is an emerging technology that has the potential to disrupt and revolutionize the way we conduct business, make commercial transactions, enforce legal contracts, and even enact government policy. Its impact on today’s world can be likened to the advent of the Internet back in the 1990s.Like the early tech boom, the blockchain movement is generating plenty of innovations. They may all be unique, but they won’t all succeed or gain mass adoption. Blockchain presents investors with exciting new opportunities, but it also comes with a number of risks. Proceed with caution. A blockchain is a distributed database or ledger shared across a computer network's nodes. They are best known for their crucial role in cryptocurrency systems, maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—meaning it cannot be altered. Since a block can’t be changed, the only trust needed is at the point where a user or program enters data. This reduces the need for trusted third parties, such as auditors or other humans, who add costs and can make mistakes. Since Bitcoin's introduction in 2009, blockchain uses have exploded via the creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. Blockchain is a type of shared database that differs from a typical database in the way it stores information; blockchains store data in blocks linked together via cryptography.Different types of information can be stored on a blockchain, but the most common use has been as a transaction ledger. In Bitcoin’s case, the blockchain is decentralized, so no single person or group has control—instead, all users collectively retain control.Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, transactions are permanently recorded and viewable to anyone. Investopedia / Xiaojie Liu You might be familiar with spreadsheets or databases. A blockchain is somewhat similar because it is a database where information is entered and stored. The key difference between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed. A blockchain consists of programs called scripts that conduct the tasks you usually would in a database: entering and accessing information, and saving and storing it somewhere. A blockchain is distributed, which means multiple copies are saved on many machines, and they must all match for it to be valid. The Bitcoin blockchain collects transaction information and enters it into a 4MB file called a block (different blockchains have different size blocks). Once the block is full, the block data is run through a cryptographic hash function, which creates a hexadecimal number called the block header hash. The hash is then entered into the following block header and encrypted with the other information in that block's header, creating a chain of blocks, hence the name “blockchain.” Transactions follow a specific process, depending on the blockchain. For example, on Bitcoin's blockchain, if you initiate a transaction using your cryptocurrency wallet—the application that provides an interface for the blockchain—it starts a sequence of events. In Bitcoin, your transaction is sent to a memory pool, where it is stored and queued until a miner picks it up. Once it is entered into a block and the block fills up with transactions, it is closed, and the mining begins. Every node in the network proposes its own blocks in this way because they all choose different transactions. Each works on their own blocks, trying to find a solution to the difficulty target, using the "nonce," short for number used once. The nonce value is a field in the block header that is changeable, and its value incrementally increases with every mining attempt. If the resulting hash isn't equal to or less than the target hash, a value of one is added to the nonce, a new hash is generated, and so on. The nonce rolls over about every 4.5 billion attempts (which takes less than one second) and uses another value called the extra nonce as an additional counter. This continues until a miner generates a valid hash, winning the race and receiving the reward. Generating these hashes until a specific value is found is the "proof-of-work" you hear so much about—it "proves" the miner did the work. The sheer amount of work it takes to validate the hash is why the Bitcoin network consumes so much computational power and energy. Once a block is closed, a transaction is complete. However, the block is not considered confirmed until five other blocks have been validated. Confirmation takes the network about one hour to complete because it averages just under 10 minutes per block (the first block with your transaction and five following blocks multiplied by 10 equals 60 minutes). Not all blockchains follow this process. For instance, the Ethereum network randomly chooses one validator from all users with ether staked to validate blocks, which are then confirmed by the network. This is much faster and less energy intensive than Bitcoin's process. A blockchain allows the data in a database to be spread out among several network nodes—computers or devices running software for the blockchain—at various locations. This creates redundancy and maintains the fidelity of the data. For example, if someone tries to alter a record on one node, the other nodes would prevent it from happening by comparing block hashes. This way, no single node can alter information within the chain. Because of this distribution—and the encrypted proof that work was done—the blockchain data, such as transaction history, becomes irreversible. Such a record could be a list of transactions, but private blockchains can also hold a variety of other information like legal contracts, state identifications, or a company's inventory. Most blockchains wouldn't "store" these items directly; they would likely be sent through a hashing algorithm and represented on the blockchain by a token. Because of the decentralized nature of the Bitcoin blockchain, all transactions can be transparently viewed by downloading and inspecting them or by using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track a bitcoin wherever it goes. For example, exchanges have been hacked in the past, resulting in the loss of large amounts of cryptocurrency. While the hackers may have been anonymous—except for their wallet address—the crypto they extracted is easily traceable because the wallet addresses are stored on the blockchain. Of course, the records stored in the Bitcoin blockchain (as well as most others) are encrypted. This means that only the person assigned an address can reveal their identity. As a result, blockchain users can remain anonymous while preserving transparency. Blockchain technology achieves decentralized security and trust in several ways. To begin, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added to the end of the blockchain, previous blocks cannot be altered. A change in any data changes the hash of the block it was in. Because each block contains the previous block's hash, a change in one would change the following blocks. The network would generally reject an altered block because the hashes would not match. However, a change can be accomplished on smaller blockchain networks. Not all blockchains are 100% impenetrable. They are distributed ledgers that use code to create the security level they have become known for. If there are vulnerabilities in the coding, they can be exploited. A new and smaller chain might be susceptible to this kind of attack, but the attacker would need at least half of the computational power of the network (a 51% attack). On the Bitcoin and other larger blockchains, this is nearly impossible. By the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter. This is because the rate at which these networks hash is exceptionally rapid—the Bitcoin network hashed at a rate of around 640 exahashes per second (18 zeros) as of September 2024. The Ethereum blockchain is not likely to be hacked either—again, the attackers would need to control more than half of the blockchain's staked ether. As of September 2024, over 33.8 million ETH has been staked by more than one million validators. An attacker or a group would need to own over 17 million ETH, and be randomly selected to validate blocks enough times to get their blocks implemented. Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn’t until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application. The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin’s pseudonymous creator, Satoshi Nakamoto, referred to it as “a new electronic cash system that’s fully peer-to-peer, with no trusted third party.” The key thing to understand is that Bitcoin uses blockchain as a means to transparently record a ledger of payments or other transactions between parties. Blockchain can be used to immutably record any number of data points. The data can be transactions, votes in an election, product inventories, state identifications, deeds to homes, and much more. Currently, tens of thousands of projects are looking to implement blockchains in various ways to help society other than just recording transactions—for example, as a way to vote securely in democratic elections. The nature of blockchain's immutability means that fraudulent voting would become far more difficult. For example, a voting system could work such that each country's citizens would be issued a single cryptocurrency or token. Each candidate could then be given a specific wallet address, and the voters would send their token or crypto to the address of whichever candidate they wish to vote for. The transparent and traceable nature of blockchain would eliminate the need for human vote counting and the ability of bad actors to tamper with physical ballots. Blockchains have been heralded as a disruptive force in the finance sector, especially with the functions of payments and banking. However, banks and decentralized blockchains are vastly different. To see how a bank differs from blockchain, let’s compare the banking system to Bitcoin’s blockchain implementation. As we now know, blocks on Bitcoin’s blockchain store transactional data. Today, tens of thousands of other cryptocurrencies run on a blockchain. But it turns out that blockchain can be a reliable way to store other types of data as well. Some companies experimenting with blockchain include Walmart, Pfizer, AIG, Siemens, and Unilever, among others. For example, IBM has created its Food Trust blockchain to trace the journey that food products take to get to their locations. Why do this? The food industry has seen countless outbreaks of E. coli, salmonella, and listeria; in some cases, hazardous materials were accidentally introduced to foods. In the past, it has taken weeks to find the source of these outbreaks or the cause of sickness from what people are eating. Using blockchain allows brands to track a food product’s route from its origin, through each stop it makes, to delivery. Not only that, but these companies can also now see everything else it may have come in contact with, allowing the identification of the problem to occur far sooner—potentially saving lives. This is one example of blockchain in practice, but many other forms of blockchain implementation exist or are being experimented with. Perhaps no industry stands to benefit from integrating blockchain into its business operations more than personal banking. Financial institutions only operate during business hours, usually five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see the money in your account. Even if you make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps. By integrating blockchain into banks, consumers might see their transactions processed in minutes or seconds—the time it takes to add a block to the blockchain, regardless of holidays or the time of day or week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. Given the sums involved, even the few days the money is in transit can carry significant costs and risks for banks. The settlement and clearing process for stock traders can take up to three days (or longer if trading internationally), meaning that the money and shares are frozen for that period. Blockchain can, in theory, drastically reduce that time. Blockchain forms the bedrock for cryptocurrencies like Bitcoin. This design also allows for easier cross-border transactions because it bypasses currency restrictions, instabilities, or lack of infrastructure by using a distributed network that can reach anyone with an internet connection. Healthcare providers can leverage blockchain to store their patients’ medical records securely. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key so that they are only accessible to specific individuals, thereby ensuring privacy. If you have ever spent time in your local Recorder’s Office, you will know that recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county’s central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index. This process is not just costly and time-consuming, it is also prone to human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanently recorded. Proving property ownership can be nearly impossible in war-torn countries or areas with little to no government or financial infrastructure and no Recorder’s Office. If a group of people living in such an area can leverage blockchain, then transparent and clear timelines of property ownership could be maintained. A smart contract is computer code that can be built into the blockchain to facilitate transactions. It operates under a set of conditions to which users agree. When those conditions are met, the smart contract conducts the transaction for the users. As in the IBM Food Trust example, suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of not only their products but also common labels such as “Organic,” “Local,” and “Fair Trade.” As reported by Forbes, the food industry is increasingly adopting the use of blockchain to track the path and safety of food throughout the farm-to-user journey. As mentioned above, blockchain could facilitate a modern voting system. Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using blockchain in this way would make votes nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election. For all of its complexity, blockchain’s potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above. But there are also some disadvantages. Transactions on the blockchain network are approved by thousands of computers and devices. This removes almost all people from the verification process, resulting in less human error and an accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain and not be accepted by the rest of the network. Typically, consumers pay a bank to verify a transaction or a notary to sign a document. Blockchain eliminates the need for third-party verification—and, with it, their associated costs. For example, business owners incur a small fee when they accept credit card payments because banks and payment-processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees. Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes significantly more difficult to tamper with. Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Financial institutions operate during business hours, usually five days a week—but a blockchain runs 24 hours a day, seven days a week, and 365 days a year. On some blockchains, transactions can be completed and considered secure in minutes. This is particularly useful for cross-border trades, which usually take much longer because of time zone issues and the fact that all parties must confirm payment processing. Many blockchain networks operate as public databases, meaning anyone with an internet connection can view a list of the network’s transaction history. Although users can access transaction details, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like Bitcoin are fully anonymous; they are actually pseudonymous because there is a viewable address that can be associated with a user if the information gets out. Once a transaction is recorded, its authenticity must be verified by the blockchain network. After the transaction is validated, it is added to the blockchain block. Each block on the blockchain contains its unique hash and the unique hash of the block before it. Therefore, the blocks cannot be altered once the network confirms them. Many blockchains are entirely open source. This means that everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. However, it also means there is no real authority on who controls Bitcoin’s code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile, then Bitcoin can be updated. Private or permission blockchains may not allow for public transparency, depending on how they are designed or their purpose. These types of blockchains might be made only for an organization that wishes to track data accurately without allowing anyone outside of the permissioned users to see it. Alternatively, there might come a point where publicly traded companies are required to provide investors with financial transparency through a regulator-approved blockchain reporting system. Using blockchains in business accounting and financial reporting would prevent companies from altering their financials to appear more profitable than they really are. Perhaps the most profound facet of blockchain and cryptocurrency is the ability for anyone, regardless of ethnicity, gender, location, or cultural background, to use it. According to The World Bank, an estimated 1.4 billion adults do not have bank accounts or any means of storing their money or wealth. Moreover, nearly all of these individuals live in developing countries where the economy is in its infancy and entirely dependent on cash. These people are often paid in physical cash. They then need to store this physical cash in hidden locations in their homes or other places, incentivizing robbers or violence. While not impossible to steal, crypto makes it more difficult for would-be thieves. Although blockchain can save users money on transaction fees, the technology is far from free. For example, the Bitcoin network's proof-of-work system to validate transactions consumes vast amounts of computational power. In the real world, the energy consumed by the millions of devices on the Bitcoin network is more than the country of Pakistan consumes annually. Some solutions to these issues are beginning to arise. For example, bitcoin-mining farms have been set up to use solar power, excess natural gas from fracking sites, or energy from wind farms. Bitcoin is a perfect case study of the inefficiencies of blockchain. Bitcoin's PoW system takes about 10 minutes to add a new block to the blockchain. At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS). Although other cryptocurrencies, such as Ethereum, perform better than Bitcoin, the complex structure of blockchain still limits them. Legacy brand Visa, for context, can process 65,000 TPS. Solutions to this issue have been in development for years. There are currently blockchain projects that claim tens of thousands of TPS. Ethereum is rolling out a series of upgrades that include data sampling, binary large objects (BLOBs), and rollups. These improvements are expected to increase network participation, reduce congestion, decrease fees, and increase transaction speeds. The other issue with many blockchains is that each block can only hold so much data. The block size debate has been and continues to be one of the most pressing issues for the scalability of blockchains in the future. While confidentiality on the blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the blockchain network. The most cited example of blockchain being used for illicit transactions is probably the Silk Road, an online dark web illegal-drug and money laundering marketplace operating from February 2011 until October 2013, when the FBI shut it down. The dark web allows users to buy and sell illegal goods without being tracked by using the Tor Browser and make illicit purchases in Bitcoin or other cryptocurrencies. This is in stark contrast to U.S. regulations, which require financial service providers to obtain information about their customers when they open an account. They are supposed to verify the identity of each customer and confirm that they do not appear on any list of known or suspected terrorist organizations. Illicit activity accounted for only 0.34% of all cryptocurrency transactions in 2023. This system can be seen as both a pro and a con. It gives anyone access to financial accounts, but allows criminals to transact more easily. Many have argued that the good uses of crypto, like banking the unbanked, outweigh the bad uses of cryptocurrency, especially when most illegal activity is still accomplished through untraceable cash. Public perception of blockchain and cryptocurrencies, in particular, remains uneasy. High-profile collapses of once-trusted cryptocurrency brokers, such as Mt. Gox back in 2014, or FTX in November 2022, persistence of various crypto scams, and general skepticism towards new technology and its bold promises, all contribute to ongoing public skepticism about a decentralized future. As of 2024, 44% of Americans still say they will never purchase a cryptocurrency. Many in the crypto space have expressed concerns about government regulation of cryptocurrencies. Several jurisdictions are tightening control over certain types of crypto and other virtual currencies. However, no regulations have yet been introduced that focus on restricting blockchain uses and development, only certain products created using it. Another significant implication of blockchains is that they require storage. This may not appear to be substantial because we already store lots of information and data. However, as time passes, the growing blockchain use will require more storage, especially on blockchains where nodes store the entire chain. Currently, data storage is centralized in large centers. But if the world transitions to blockchain for every industry and use, its exponentially growing size would require more advanced techniques to make storage more efficient, or force participants to continually upgrade their storage. This could become significantly more expensive in terms of both money and physical space needed, as the Bitcoin blockchain itself was over 600 gigabytes as of September 15th, 2024—and this blockchain records only bitcoin transactions. This is small compared to the amount of data stored in large data centers, but a growing number of blockchains will only add to the amount of storage already required for the digital world. Simply put, a blockchain is a shared database or ledger. Bits of data are stored in files known as blocks, and each network node has a replica of the entire database. Security is ensured since the majority of nodes will not accept a change if someone tries to edit or delete an entry in one copy of the ledger. Imagine you typed some information into a document on your computer and sent it through a program that gave you a string of numbers and letters (called hashing, with the string called a hash). You add this hash to the beginning of another document and type information into it. Again, you use the program to create a hash, which you add to the following document. Each hash is a representation of the previous document, which creates a chain of encoded documents that cannot be altered without changing the hash. Each document is stored on computers in a network. This network of programs compares each document with the ones they have stored and accepts them as valid based on the hashes they generate. If a document doesn't generate a hash that is a match, that document is rejected by the network. A blockchain is a distributed network of files chained together using programs that create hashes, or strings of numbers and letters that represent the information contained in the files. Every network participant is a computer or device that compares these hashes to the one they generate. If there is a match, the file is kept. If there isn't, the file is rejected. With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself in no small part because of Bitcoin and cryptocurrency. As a buzzword on the tongue of every investor across the globe, blockchain stands to make business and government operations more accurate, efficient, secure, and cheap, with fewer intermediaries. As we head into the third decade of blockchain, it's no longer a question of if legacy companies will catch on to the technology—it's a question of when. Today, we see a proliferation of NFTs and the tokenization of assets. Tomorrow, we may see a combination of blockchains, tokens, and artificial intelligence all incorporated into business and consumer solutions. The comments, opinions, and analyses expressed on Investopedia are for informational purposes online. Read our warranty and liability disclaimer for more info. TrinetixInsightsThe What, Why, and How of Blockchain in FinanceWhile not all CFOs view blockchain adoption as their #1 task, Gartner expects this technology to be a crucial part of the BFSI sector by 2025. The unprecedented changes affecting the world of finances leave no space for hesitation. To be ready for the future and whatever challenges it has in store, companies must start introducing innovation right here, right now.For that reason, blockchain technology's flexibility, transparency, and security are gaining traction and are worth exploring by any leader wishing to secure their success in the future.Blockchain technology is based on a relatively simple concept. It's a non-centralized database shared across a massive network of computers, also known as nodes. Blockchain stores information in blocks strung together into a chain of data (hence the name). It's a rather stark contrast to more traditional ways of data storage, such as tables. Another difference is that once blockchain data is added, it becomes an immutable part of a timeline.Decentralized databaseData can't be changedBased on the distributed ledger network architectureFull transparencyMore complicated to implementCentralized databaseData can be modifiedBased on the client-server architectureLimited access to dataEasier to implementWhile its decentralized structure and immutable recordkeeping made blockchain perfect for the cryptocurrency sector, there is more to blockchain than Bitcoin transactions.As rapid digitization makes paper-reliant approaches less convenient, blockchain technology can help financial organizations abandon bureaucracy and move to a new level of efficiency, safety, and cost-effectiveness.There is a common assumption that hackers and phishers are more likely to attack small companies than large corporations. However, the cases of giants like Facebook, Marriott, and even Microsoft show that the size of their target doesn't dissuade hackers. Quite on the contrary, they're emboldened by it.This is why cybersecurity remains one of the biggest concerns of CFOs and CIOs across the BFSI, prompting them to expand their safety measures beyond firewalls and antimalware programs.How can blockchain fintech solutions help with protecting company data?Decentralized databaseTo hackers, stealing data is like carjacking. They get their hands on the entire database. They sell it on the darknet. They move on to their next target. Therefore, no matter how many firewalls and defenses companies put up, one successful hacking attempt is all it takes to lose valuable data, reputation, and money. Blockchain sabotages hackers' efforts by removing the main vulnerability — a centralized database. Instead, it replaces it with encrypted data, scattered across multiple nodes.Even if hackers break into one of the nodes, they would only get an encrypted data block for their efforts, which is worth nothing without the rest of the database. To continue with the carjacker analogy, the thieves break into the garage expecting to steal a car, but all they find is a steering wheel. They can keep collecting car parts in hopes to assemble a car — or they can quit and do something more rewarding.Data hashingTo further prevent data hacking, each block of the data chain is protected by hashing – a special code that converts data into a fixed value i.e. unique string of numbers.Unlike encryption which can be deciphered and tampered with if a third party gets their hands on the key, hashing is a one-way transformation that instantly notifies users whenever there is an attempt to modify the contents of the block. Hashing makes blockchain data more resistant to hacking and ensures immutable recordkeeping.Improved privacyAnother safety point worth mentioning is transparency and privacy of document processing. Blockchain-based ledgers are accessible only by participants with special permission, preventing any third parties from compromising the business. This feature is particularly relieving for trading participants who expect full clarity and safety guarantees.Regulatory complianceBlockchain technology helps companies provide solid proof of compliance. For instance, time-stamped recordkeeping provides regulators with solid data audits for compliance verification. Also, blockchain enables regulators to be more proactive, granting them real-time read-only access to the company's permissioned blockchain. With regulators engaged as participants, companies can optimize the financial and time resources necessary for audit reporting while staying compliant with all required regulations.While cybercriminals are constantly coming up with new ways to access data, innovation-driven blockchain technology is capable of preventing most modern security threats and ensures safe, responsible, and regulated data processing.Blockchain's ability to slice through inefficiency and streamline financial operations makes it great for all areas of financial services.Simplified trading processesTraditional trading required every participant to collect an individual database containing all the documents related to their current trading operation. In the course of trading, these documents would be exchanged between the participants and expanded according to the trade progress. In addition to generating vast amounts of paperwork, this procedure also generates vast amounts of frustration due to constant duplicates and setbacks. Implementing blockchain in finance curbs bureaucracy, replacing a paper mountain of invoices and shipment documents with just one digital ledger. This ledger keeps track of the trade and is available to all participants, ensuring they all are on the same page regarding trade progress.Back-and-forth transactionsFor many entities and people, cross-border payments meant standing in long lines in the bank, filling out several forms, and waiting for at least five days for the money to arrive. However, the use of blockchain technology in finances managed to break this vicious cycle, introducing clients to faster and safer transactions across the globe. According to Deloitte, companies connected to a blockchain-based platform were able to complete their transactions in three hours, with considerably fewer delays and errors compared to paper-based systems.Single source of truthReconciliation of data between buyers and suppliers, intracompany data silos often disrupt decision-making. When there isn't enough data or not enough confirmed data, leaders can't get a clear picture of their transactions, so they struggle with outlining future steps and optimizing their relationships with suppliers. Blockchain fintech solutions are capable of facilitating both external and internal company processes by building a solid chain of immutable and confirmed data that is regularly updated and evenly distributed across all systems and departments. With no vital information withheld or missed out, C-level executives have all the data to move forward with decision-making and invest in projects that are guaranteed to pay off.To put it simply, blockchain thrives in every paper-cluttered industry, removing piles of paperwork and replacing them with fresh and dynamic data that can fuel the company's processes and accelerate its growth.This advantage stems directly from blockchain's ability to cut through the bureaucracy, skipping extra steps and focusing on the most important matters. However, there are also more cost-reducing benefits worth mentioning.Reduced IT costsSupporting an IT department, complete with maintenance expenditures, and hiring more IT experts to keep the expanding network running takes up a large chunk of a company's budget. This leads to CFOs being more reluctant to try new solutions or implement new technologies to preserve their OpEx and CapEx balance. Providing a single string of data across multiple systems, the blockchain-based digital ledger helps companies cut operating and IT expenses. According to PwC, using blockchain in finance can save institutions around $20 billion per year on infrastructure. Additionally, blockchain fintech solutions allow financial institutions to finally let go of cumbersome and outdated legacy systems, freeing more resources and opportunities for improving their tech assets.Budget-friendly operationsA simplified and consistent data structure brought by blockchain fintech solutions lets companies save up on a number of expensive operations. For instance, post-trade settlement is a rather costly procedure. However, using blockchain for finance procedures like these employees can complete reconciliations and settlements in fewer steps at a lower cost. Given that not all financial and business institutions have regained their footing since 2020, blockchain fintech solutions can be useful for expenditure optimization.Increased valueAs digitalization and automation become the future of the BFSI sector and many other areas, manual tasks are logically becoming the way of the past. As blockchain in finance covers processes that used to be handled manually, employees get more time to work on more complicated, value-building tasks. Such features as automated report generation and improved data lineage also ensure better navigation through the business landscape, helping companies avoid pitfalls and make the most relevant decisions. This way, adopting blockchain for finance delivers a revenue boost, while reducing expenses.Compared to more traditional on-premise solutions, blockchain is a guaranteed return on investment, allowing leaders to save money on various financial operations and employee management. At the same time, using blockchain in finance opens the door to numerous opportunities.Smart contracts are the most illustrative example of how blockchain in finance can help companies automate their processes. A smart contract is a codified set of rules that operates on an "if-then" logic. Smart contracts are designed to set the deal into motion once certain conditions, indicated in the rules, are met by all participating sides.For example, if a smart contract oversees that the payment should be made after the shipment arrives on a specified date and at a specified time, the routine is the following:The shipment arrives within the agreed time period.The smart contract receives a notification that the condition has been fulfilled.The smart contract automatically initiates the payment process.Smart contracts can be adapted to various procedures, from triggering transactions to service delivery. Their adaptive and flexible nature makes them ideal for banking, trading, and insurance. For instance, Arbol, a fintech company, uses smart contracts for more accurate weather and climate coverage for its clients. Other companies, like Insurwave, found smart contracts to greatly improve their operational efficiency by simplifying and streamlining the transactional process and claims assessments.Know Your Client (KYC) systems are one of those banking aspects where financial institution leaders find themselves torn between convenience and safety. A traditional KYC system consists of multiple verification steps, obligating clients to provide many documents (ID, credit card information, etc.) to the bank whenever they need to initiate an operation.While the repetitiveness of these procedures is already enough to increase customer frustration, long waiting times, connectivity issues, and simple human error add up to a bad experience. In the end, potential clients are reluctant to interact with banks — and more likely to switch to an institution offering better client service.On the one hand, as vexing as KYC systems can be, their design follows a greater purpose — fraud prevention. On the other hand, modern customers vote with their feet, prompting financial leaders to look for the right convenience/safety balance.The use of blockchain in finance provided solutions that appealed to both financial leaders and clients by introducing new, improved KYC systems. Compared to traditional ones, a blockchain-based KYC doesn't require multiple verification procedures. A client only needs to create a profile once. After this, their data will be safely shared with the bank they want to work with.Whenever a customer initiates a procedure, their profile will be updated accordingly, helping them keep track of their transactions. Blockchain-based KYC systems also offer configurable privacy settings, letting clients control access to their data.Nobody likes to be not in control, especially when their money is at stake. This situation is particularly accurate for investors. Since 2020, investors have been demonstrating a growing need for clarity and transparency. They have also become less eager to join hedge funds. Doing so would result in them putting their trust and finances in the hands of a fund manager, who might keep them in the dark about potential operations, transactions, and ROI. As hedge funds aren't legally obligated to disclose such information to investors, there is no way for the latter to secure transparency.The intervention of blockchain in finance allows putting end to the investors' concerns by giving them all the control. Blockchain-based funds are platforms where investors can instantly access all necessary data on their progress, invest or withdraw their money, make decisions and evaluate the situation on the market.This is exactly the transparency that modern investors are searching for, which is why PwC observed at least 38% of hedge funds investing in digital assets.Just a decade ago, SWIFT was considered to be the best thing that could happen to the banking industry. This system has connected over 11,000 financial organizations across 200 countries, building a solid foundation for economic growth and shaping international financial relations.Nowadays, the pressure of ever-growing and shifting customer expectations exposes SWIFT as an outdated, cumbersome, and high-maintenance system. Naturally, it doesn't mean that SWIFT is going anywhere soon. Nevertheless, the growing presence of blockchain in finances is slowly taking over by countering SWIFT-related pain points with its solutions.Instant transactionsBlockchain makes global transactions a matter of hours rather than days, expanding the number of operations a company can execute within a day. Many blockchain platforms wrap up cross-border payments within 25 minutes.Reduced feesA transaction fee is a cut taken by both the sending bank and the receiving bank to verify the procedure. Since blockchain-based P2P transactions are based on disintermediation, clients pay a considerably lower fee (ranging between $0 to $30) since there is no third party to charge customers for transaction verification.Anti-fraud mechanismsAs an archaic system, SWIFT is particularly vulnerable to fraud. Its less-than-robust encryption system and exploitable flaws make it a welcome target for scammers. One of the most well-known examples is the Bangladesh Bank fraud of 2016, when criminals managed to steal $81 million by altering the SWIFT software on the bank's computers, hiding all traces of transaction fraud. Blockchain data is recorded immutably, making it impossible to alter. In addition, if there is something wrong with the payment process, the system doesn't proceed with the transfer, and both parties receive a notification.These benefits make blockchain a viable alternative to SWIFT. Implementing blockchain in finance offers more control to clients, grants them more visibility and provides greater financial inclusion, enabling more people to send cross-border payments for acceptable fees. For that reason, adopting blockchain for finance at a large scale is expected to completely transform the approach to transactions in the future, allowing for a better, safer, and people-centered experience.Using blockchain technology in finance innovation resulted in the birth of the brand new approach to banking and lending known as DeFi (decentralized finance). That change marks a new era of intermediary-free banking and lending operations.With their value going up to $200 billion by 2022, DeFi systems have been making a powerful impact on banking and lending areas, empowering them with a number of innovations.DeFi transactions take intermediaries out of the equation to speed up the process and ensure safety via a secure global network that complies with international regulations and ensures transparent exchange between the parties.Blockchain helps exporters and importers build trust by transferring shipment paperwork to a digital format that is regularly updated and easily accessible by all trading parties.Blockchain enables the creation of decentralized platforms for monitoring commodities, debts, stocks, and other unique digital assets and tracking their ownership. This way, clients don't have to wait until they're matched with the asset owner on the stock exchange. It also relieves them from paying fees to banks that outsource day-to-day asset management.Blockchain introduces more complex loans that provide an approximate outline of a syndicated loan structure, helping consumers to take personal loans. Smart contracts oversee the lending process.Lenders gain read-only access to applicants' records and their credit history to make more weighted decisions on loan approvals. At the same time, the borrowers don't have to submit their sensitive data to credit agencies that can fall victim to data leaks.As blockchain-based lending operates on the same disintermediation principles as blockchain-empowered banking, clients can borrow funds at a low-interest rate.The potential for disruption is immense. While banking has been more active in harnessing the possibilities delivered by blockchain, the blockchain-based transformation of the lending process is still a work in progress. However, with startups like Bloom productizing innovative ideas, we're guaranteed to witness revolutionary lending projects in the future.Overall, blockchain can be applied to a wide range of industries – from healthcare to real estate. But it's the BFSI sector that was the trailblazer in adopting blockchain technology for various operational needs. Many banks using blockchain started doing it back in 2016 when multiple organizations were still hesitant about embracing the technology. By 2022, the implementation of blockchain in finances has gone beyond banking, taking root in insurance, trade and various financial service areas.Uses blockchain fintech solutions for faster and facilitated fund transfers and improved KYC system.Launched the B2B Connect blockchain platform for B2B payments in 2016. By 2019, the B2B Connect platform was covering 64 countries.Developed a blockchain platform for banking, completing a syndicated loan worth €150 million.Actively utilizes blockchain for the trade sector, completing transactions with greater accuracy.Migrated its paper-based data to blockchain to remove duplicates and prevent data discrepancies.Built a robust blockchain-based architecture for managing all financial transactions and regulations.Developed a smart blockchain platform to handle complex insurance processes.Uses blockchain technology for sharing real-time policy data and documents and providing bancassurance solutions.Built an automated platform for filing insurance claims and checking the insurance status of family members.The massive shift of influential industrial figures to blockchain drives the point home — blockchain belongs in finances. It's here to stay.So, is the future of blockchain clear? Is blockchain the future? Or are there pitfalls that stand in its way?Indeed, there is a lot to discover and improve regarding blockchain — modern blockchain platforms are currently hard at work removing flaws like low scalability and high energy consumption. However, multiple companies and businesses worldwide enjoy the benefits of blockchain fintech apps right here, right now — a trend noticed by Gartner, Deloitte, and PwC. So far, they have been accurate in their prognosis. Even though many business leaders used to be on the fence about implementing blockchain in finance, they were growing more accustomed to the idea even before the major digital shift in 2020.This tendency was observed in 2018 when at least 66% of respondents participating in Deloitte's CFO survey acknowledged that they might lose their competitive edge if they don't start adopting blockchain for finance. Today, when the need for digital transformation has become even more glaring, decision-makers understand that they can no longer afford to merely dabble in blockchain-based platforms — otherwise, their competitors might be the ones to leverage the power of smart contracts and fast transactions.So, what can be said about the future of blockchain in finance? It still has a long way to go before it gains presence in nearly every area of BFSI. Nevertheless, it's going steady on its journey from a cryptocurrency bedrock to a BFSI strategy game-changer, and there is no doubt it will evolve into a must-have component of every financial institution by 2026.Incorporating blockchain technology in finance is a guaranteed push towards better client experiences, employee productivity, data security, and operational efficiency. However, much like any disruptive innovation, blockchain needs a calculated and structured implementation strategy that is tailored to specific business needs.Therefore, if you have been planning to inject more productivity with blockchain, but want to get started the right way, omitting all pitfalls and setbacks – we're here for you.Our blockchain developers and consultants will help you with mapping out the right strategy and must-have features of your future blockchain addition and deliver a robust and highly efficient product—seamlessly integrated into your current workflow.So, if you're up for transforming your BFSI organization and replacing paper-cluttered environments with cutting-edge digital assets – let's chat and bring your vision to life.Blockchain makes a difference in any paper-cluttered industry, removing extra paperwork and intermediaries from transactions. At the same time, it provides a decentralized, single source of data, letting participants track trade operations, financial transactions, and other procedures in chronological order. This application of blockchain in finance brings institutions to a new level of transparency, security, and efficiency.Depending on the finance area, blockchain fintech solutions can be used to facilitate trading via smart contracts, streamline intracompany data movement by providing a digital ledger containing all the necessary information for audits, reporting, and financial analysis; or build a transparent platform for investors who expect full visibility.Blockchain can transform nearly every industry that could use less bureaucracy and more digitization — it provides the agility, security, and delivery speed necessary to meet customers' needs while keeping up with safety and data processing regulations. When it comes to applying blockchain technology in finance, it can deliver the transparency needed for financial transactions and enhance anti-fraud measures to keep banking operations untampered by scammers. All these benefits can be gained while cutting costs on IT structure, making blockchain a potent upgrade to a wide range of financial organizations.Ready to explore tomorrow's potential? A blockchain is a distributed database or ledger shared across a computer network's nodes. They are best known for their crucial role in cryptocurrency systems, maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—meaning it cannot be altered. Since a block can't be changed, the only trust needed is at the point where a user or program enters data. This reduces the need for trusted third parties, such as auditors or other humans, who add costs and can make mistakes. Since Bitcoin's introduction in 2009, blockchain uses have exploded via the creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. Blockchain is a type of shared database that differs from a typical database in the way it stores information; blockchains store data in blocks linked together via cryptography.Different types of information can be stored on a blockchain, but the most common use has been as a transaction ledger. In Bitcoin's case, the blockchain is decentralized, so no single person or group has control—instead, all users collectively retain control.Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, transactions are permanently recorded and viewable to anyone. Investopedia / Xiaojie Liu You might be familiar with spreadsheets or databases. A blockchain is somewhat similar because it is a database where information is entered and stored. The key difference between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed. A blockchain consists of programs called scripts that conduct the tasks you usually would in a database: entering and accessing information, and saving and storing it somewhere. A blockchain is distributed, which means multiple copies are saved on many machines, and they must all match for it to be valid. The Bitcoin blockchain collects transaction information and enters it into a 4MB file called a block (different blockchains have different size blocks). Once the block is full, the block data is run through a cryptographic hash function, which creates a hexadecimal number called the block header hash. The hash is then entered into the following block header and encrypted with the other information in that block's header, creating a chain of blocks, hence the name "blockchain." Transactions follow a specific process, depending on the blockchain. For example, on Bitcoin's blockchain, if you initiate a transaction using your cryptocurrency wallet—the application that provides an interface for the blockchain—it starts a sequence of events. In Bitcoin, your transaction is sent to a memory pool, where it is stored and queued until a miner picks it up. Once it is entered into a block and the block fills up with transactions, it is closed, and the mining begins. Every node in the network proposes its own blocks in this way because they all choose different transactions. Each works on their own blocks, trying to find a solution to the difficulty target, using the "nonce," short for number used once. The nonce value is a field in the block header that is changeable, and its value incrementally increases with every mining attempt. If the resulting hash isn't equal to or less than the target hash, a value of one is added to the nonce, a new hash is generated, and so on. The nonce rolls over about every 4.5 billion attempts (which takes less than one second) and uses another value called the extra nonce as an additional counter. This continues until a miner generates a valid hash, winning the race and receiving the reward. Generating these hashes until a specific value is found is the "proof-of-work" you hear so much about—it "proves" the miner did the work. The sheer amount of work it takes to validate the hash is why the Bitcoin network consumes so much computational power and energy. Once a block is closed, a transaction is complete. However, the block is not considered confirmed until five other blocks have been validated. Confirmation takes the network about one hour to complete because it averages just under 10 minutes per block (the first block with your transaction and five following blocks multiplied by 10 equals 60 minutes). Not all blockchains follow this process. For instance, the Ethereum network randomly chooses one validator from all users with ether staked to validate blocks, which are then confirmed by the network. This is much faster and less energy intensive than Bitcoin's process. A blockchain allows the data in a database to be spread out among several network nodes—computers or devices running software for the blockchain—at various locations. This creates redundancy and maintains the fidelity of the data. For example, if someone tries to alter a record on one node, the other nodes would prevent it from happening by comparing block hashes. This way, no single node can alter information within the chain. Because of this distribution—and the encrypted proof that work was done—the blockchain data, such as transaction history, becomes irreversible. Such a record could be a list of transactions, but private blockchains can also hold a variety of other information like legal contracts, state identifications, or a company's inventory. Most blockchains wouldn't "store" these items directly; they would likely be sent through a hashing algorithm and represented on the blockchain by a token. Because of the decentralized nature of the Bitcoin blockchain, all transactions can be transparently viewed by downloading and inspecting them or by using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track a bitcoin wherever it goes. For example, exchanges have been hacked in the past, resulting in the loss of large amounts of cryptocurrency. While the hackers may have been anonymous—except for their wallet address—the crypto they extracted is easily traceable because the wallet addresses are stored on the blockchain. Of course, the records stored in the Bitcoin blockchain (as well as most others) are encrypted. This means that only the person assigned an address can reveal their identity. As a result, blockchain users can remain anonymous while preserving transparency. Blockchain technology achieves decentralized security and trust in several ways. To begin, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added to the end of the blockchain, previous blocks cannot be altered. A change in any data changes the hash of the block it was in. Because each block contains the previous block's hash, a change in one would change the following blocks. The network would generally reject an altered block because the hashes would not match. However, a change can be accomplished on smaller blockchain networks. Not all blockchains are 100% impenetrable. They are distributed ledgers that use code to create the security level they have become known for. If there are vulnerabilities in the coding, they can be exploited. A new and smaller chain might be susceptible to this kind of attack, but the attacker would need at least half of the computational power of the network (a 51% attack). On the Bitcoin and other larger blockchains, this is nearly impossible. By the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter. This is because the rate at which these networks hash is exceptionally rapid—the Bitcoin network hashed at a rate of around 640 exahashes per second (18 zeros) as of September 2024. The Ethereum blockchain is not likely to be hacked either—again, the attackers would need to control more than half of the blockchain's staked ether. As of September 2024, over 33.8 million ETH has been staked by more than one million validators. An attacker or a group would need to own over 17 million ETH, and be randomly selected to validate blocks enough times to get their blocks implemented. Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application. The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator, Satoshi Nakamoto, referred to it as "a new electronic cash system that's fully peer-to-peer, with no trusted third party." The key thing to understand is that Bitcoin uses blockchain as a means to transparently record a ledger of payments or other transactions between parties. Blockchain can be used to immutably record any number of data points. The data can be transactions, votes in an election, product inventories, state identifications, deeds to homes, and much more. Currently, tens of thousands of projects are looking to implement blockchains in various ways to help society other than just recording transactions—for example, as a way to vote securely in democratic elections. The nature of blockchain's immutability means that fraudulent voting would become far more difficult. For example, a voting system could work such that each country's citizens would be issued a single cryptocurrency or token. Each candidate could then be given a specific wallet address, and the voters would send their token or crypto to the address of whichever candidate they wish to vote for. The transparent and traceable nature of blockchain would eliminate the need for human vote counting and the ability of bad actors to tamper with physical ballots. Blockchains have been heralded as a disruptive force in the finance sector, especially with the functions of payments and banking. However, banks and decentralized blockchains are vastly different. To see how a bank differs from blockchain, let's compare the banking system to Bitcoin's blockchain implementation. As we now know, blocks on Bitcoin's blockchain store transactional data. Today, tens of thousands of other cryptocurrencies run on a blockchain. But it turns out that blockchain can be a reliable way to store other types of data as well. Some companies experimenting with blockchain include Walmart, Pfizer, AIG, Siemens, and Unilever, among others. For example, IBM has created its Food Trust blockchain to trace the journey that food products take to get to their locations. Why do this? The food industry has seen countless outbreaks of E. coli, salmonella, and listeria; in some cases, hazardous materials were accidentally introduced to foods. In the past, it has taken weeks to find the source of these outbreaks or the cause of sickness from what people are eating. Using blockchain allows brands to track a food product's route from its origin, through each stop it makes, to delivery. Not only that, but these companies can also now see everything else it may have come in contact with, allowing the identification of the problem to occur far sooner—potentially saving lives. This is one example of blockchain in practice, but many other forms of blockchain implementation exist or are being experimented with. Perhaps no industry stands to benefit from integrating blockchain into its business operations more than personal banking. Financial institutions only operate during business hours, usually five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see the money in your account. Even if you make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps. By integrating blockchain into banks, consumers might see their transactions processed in minutes or seconds—the time it takes to add a block to the blockchain, regardless of holidays or the time of day or week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. Given the sums involved, even the few days the money is in transit can carry significant costs and risks for banks. The settlement and clearing process for stock traders can take up to three days (or longer if trading internationally), meaning that the money and shares are frozen for that period. Blockchain can, in theory, drastically reduce that time. Blockchain forms the bedrock for cryptocurrencies like Bitcoin. This design also allows for easier cross-border transactions because it bypasses currency restrictions, instabilities, or lack of infrastructure by using a distributed network that can reach anyone with an internet connection. Healthcare providers can leverage blockchain to store their patients' medical records securely. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key so that they are only accessible to specific individuals, thereby ensuring privacy. If you have ever spent time in your local Recorder's Office, you will know that recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county's central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index. This process is not just costly and time-consuming, it is also prone to human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanently recorded. Proving property ownership can be nearly impossible in war-torn countries or areas with little to no government or financial infrastructure and no Recorder's Office. If a group of people living in such an area can leverage blockchain, then transparent and clear timelines of property ownership could be maintained. A smart contract is computer code that can be built into the blockchain to facilitate transactions. It operates under a set of conditions to which users agree. When those conditions are met, the smart contract conducts the transaction for the users. As in the IBM Food Trust example, suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of not only their products but also common labels such as "Organic," "Local," and "Fair Trade." As reported by Forbes, the food industry is increasingly adopting the use of blockchain to track the path and safety of food throughout the farm-to-user journey. As mentioned above, blockchain could facilitate a modern voting system. Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using blockchain in this way would make votes nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election. For all of its complexity, blockchain's potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above. But there are also some disadvantages. Transactions on the blockchain network are approved by thousands of computers and devices. This removes almost all people from the verification process, resulting in less human error and an accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain and not be accepted by the rest of the network. Typically, consumers pay a bank to verify a transaction or a notary to sign a document. Blockchain eliminates the need for third-party verification—and, with it, their associated costs. For example, business owners incur a small fee when they accept credit card payments because banks and payment-processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees. Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes significantly more difficult to tamper with. Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Financial institutions operate during business hours, usually five days a week—but a blockchain runs 24 hours a day, seven days a week, and 365 days a year. On some blockchains, transactions can be completed and considered secure in minutes. This is particularly useful for cross-border trades, which usually take much longer because of time zone issues and the fact that all parties must confirm payment processing. Many blockchain networks operate as public databases, meaning anyone with an internet connection can view a list of the network's transaction history. Although users can access transaction details, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like Bitcoin are fully anonymous; they are actually pseudonymous because there is a viewable address that can be associated with a user if the information gets out. Once a transaction is recorded, its authenticity must be verified by the blockchain network. After the transaction is validated, it is added to the blockchain block. Each block on the blockchain contains its unique hash and the unique hash of the block before it. Therefore, the blocks cannot be altered once the network confirms them. Many blockchains are entirely open source. This means that everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. However, it also means there is no real authority on who controls Bitcoin's code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile, then Bitcoin can be updated. Private or permission blockchains may not allow for public transparency, depending on how they are designed or their purpose. These types of blockchains might be made only for an organization that wishes to track data accurately without allowing anyone outside of the permissioned users to see it. Alternatively, there might come a point where publicly traded companies are required to provide investors with financial transparency through a regulator-approved blockchain reporting system. Using blockchains in business accounting and financial reporting would prevent companies from altering their financials to appear more profitable than they really are. Perhaps the most profound facet of blockchain and cryptocurrency is the ability for anyone, regardless of ethnicity, gender, location, or cultural background, to use it. According to The World Bank, an estimated 1.4 billion adults do not have bank accounts or any means of storing their money or wealth. Moreover, nearly all of these individuals live in developing countries where the economy is in its infancy and entirely dependent on cash. These people are often paid in physical cash. They then need to store this physical cash in hidden locations in their homes or other places, incentivizing robbers or violence. While not impossible to steal, crypto makes it more difficult for would-be thieves. Although blockchain can save users money on transaction fees, the technology is far from free. For example, the Bitcoin network's proof-of-work system to validate transactions consumes vast amounts of computational power. In the real world, the energy consumed by the millions of devices on the Bitcoin network is more than the country of Pakistan consumes annually. Some solutions to these issues are beginning to arise. For example, bitcoin-mining farms have been set up to use solar power, excess natural gas from fracking sites, or energy from wind farms. Bitcoin is a perfect case study of the inefficiencies of blockchain. Bitcoin's PoW system takes about 10 minutes to add a new block to the blockchain. At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS). Although other cryptocurrencies, such as Ethereum, perform better than Bitcoin, the complex structure of blockchain still limits them. Legacy brand Visa, for context, can process 65,000 TPS. Solutions to this issue have been in development for years. There are currently blockchain projects that claim tens of thousands of TPS. Ethereum is rolling out a series of upgrades that include data sampling, binary large objects (BLOBs), and rollups. These improvements are expected to increase network participation, reduce congestion, decrease fees, and increase transaction speeds. The other issue with many blockchains is that each block can only hold so much data. The block size debate has been and continues to be one of the most pressing issues for the scalability of blockchains in the future. While confidentiality on the blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the blockchain network. The most cited example of blockchain being used for illicit transactions is probably the Silk Road, an online dark web illegal-drug and money laundering marketplace operating from February 2011 until October 2013, when the FBI shut it down. The dark web allows users to buy and sell illegal goods without being tracked by using the Tor Browser and make illicit purchases in Bitcoin or other cryptocurrencies. This is in stark contrast to U.S. regulations, which require financial service providers to obtain information about their customers when they open an account. They are supposed to verify the identity of each customer and confirm that they do not appear on any list of known or suspected terrorist organizations. Illicit activity accounted for only 0.34% of all cryptocurrency transactions in 2023. This system can be seen as both a pro and a con. It gives anyone access to financial accounts, but allows criminals to transact more easily. Many have argued that the good uses of crypto, like banking the unbanked, outweigh the bad uses of cryptocurrency, especially when most illegal activity is still accomplished through untraceable cash. Public perception of blockchain and cryptocurrencies, in particular, remains uneasy. High-profile collapses of once-trusted cryptocurrency brokers, such as Mt. Gox back in 2014, or FTX in November 2022, persistence of various crypto scams, and general skepticism towards new technology and its bold promises, all contribute to ongoing public skepticism about a decentralized future. As of 2024, 44% of Americans still say they will never purchase a cryptocurrency. Many in the crypto space have expressed concerns about government regulation of cryptocurrencies. Several jurisdictions are tightening control over certain types of crypto and other virtual currencies. However, no regulations have yet been introduced that focus on restricting blockchain uses and development, only certain products created using it. Another significant implication of blockchains is that they require storage. This may not appear to be substantial because we already store lots of information and data. However, as time passes, the growing blockchain use will require more storage, especially on blockchains where nodes store the entire chain. Currently, data storage is centralized in large centers. But if the world transitions to blockchain for every industry and use, its exponentially growing size would require more advanced techniques to make storage more efficient, or force participants to continually upgrade their storage. This could become significantly more expensive in terms of both money and physical space needed, as the Bitcoin blockchain itself was over 600 gigabytes as of September 15th, 2024—and this blockchain records only bitcoin transactions. This is small compared to the amount of data stored in large data centers, but a growing number of blockchains will only add to the amount of storage already required for the digital world. Simply put, a blockchain is a shared database or ledger. Bits of data are stored in files known as blocks, and each network node has a replica of the entire database. Security is ensured since the majority of nodes will not accept a change if someone tries to edit or delete an entry in one copy of the ledger. Imagine you typed some information into a document on your computer and sent it through a program that gave you a string of numbers and letters (called hashing, with the string called a hash). You add this hash to the beginning of another document and type information into it. Again, you use the program to create a hash, which you add to the following document. Each hash is a representation of the previous document, which creates a chain of encoded documents that cannot be altered without changing the hash. Each document is stored on computers in a network. This network of programs compares each document with the ones they have stored and accepts them as valid based on the hashes they generate. If a document doesn't generate a hash that is a match, that document is rejected by the network. A blockchain is a distributed network of files chained together using programs that create hashes, or strings of numbers and letters that represent the information contained in the files. Every network participant is a computer or device that compares these hashes to the one they generate. If there is a match, the file is kept. If there isn't, the file is rejected. With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself in no small part because of Bitcoin and cryptocurrency. As a buzzword on the tongue of every investor across the globe, blockchain stands to make business and government operations more accurate, efficient, secure, and cheap, with fewer intermediaries. As we head into the third decade of blockchain, it's no longer a question of if legacy companies will catch on to the technology—it's a question of when. Today, we see a proliferation of NFTs and the tokenization of assets. Tomorrow, we may see a combination of blockchains, tokens, and artificial intelligence all incorporated into business and consumer solutions. The comments, opinions, and analyses expressed on Investopedia are for informational purposes online. Read our warranty and liability disclaimer for more info.