What Is Blockchain?

ITIF Technology Explainer Series • www.itif.org

Blockchains are digital ledgers that record information that is distributed among a network of computers.

Blockchains consist of a series of digital "blocks" that are securely linked together using cryptography. These blocks record information such as financial transactions, agreements between parties, and ownership records. Each computer in the network, referred to as a node, can store a copy of the blockchain. The nodes form a distributed peer-to-peer network, where updates are shared and synchronized between all nodes.

Whereas in the past users needed a trusted intermediary, such as a bank or government agency, to ensure the integrity of these types of records, blockchains eliminate the need for a central authority. Instead, blockchains maintain agreement between all participants using a "consensus protocol"—a set of rules that allows nodes to determine when to add new information to the blockchain.

Consensus protocols are designed to make the blockchain resistant to tampering. For example, one popular method, known as "proof of work," requires nodes in the network to compete to solve complex cryptographic puzzles before a new block can be added. Solving these puzzles is computationally complex, requiring nodes to engage in a certain amount of work, but verifying that the puzzle has been solved is computationally simple. Because each block includes a piece of information about the previous block in the chain, nodes cannot retroactively modify a block without first solving the cryptographic puzzle for that block and every block after it—a task that is too difficult for any node to accomplish on its own. Other consensus protocols use different techniques to prevent tampering, each with various benefits and drawbacks.

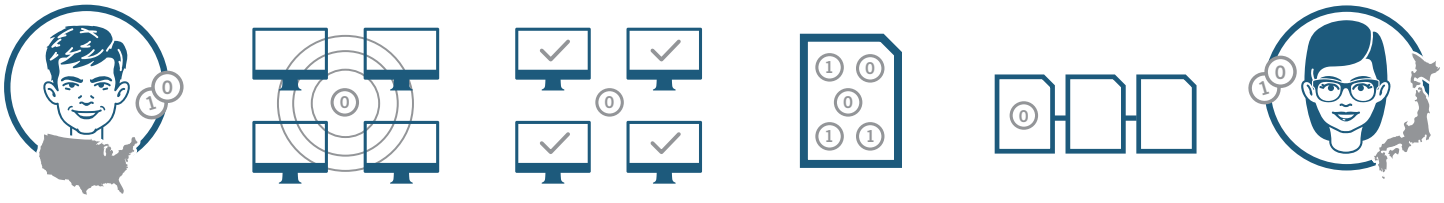
There are both public and private blockchains. In a public blockchain, anyone can join and become a node in the network. Public blockchains are set into motion by developers, and then volunteers join the peer-to-peer network. In a private blockchain, the operator sets up a permissioned network that places restrictions on who can participate and what transactions they can access and conduct. Therefore, public blockchains typically can be easier to start, more transparent, and more redundant, and private blockchains can enable more privacy, greater scalability, and faster transaction clearing.

Why Now?

In 2009, an individual using the name Satoshi Nakamoto created and released the code for the first blockchain system. The code could run easily on commodity hardware, and users quickly shared it over the Internet. It combined several advanced cryptographic techniques to enable the peer-to-peer digital currency system called Bitcoin. This system, for the first time, eliminated a fundamental problem with distributed payment systems by making it impractical for any participant to defraud the system by spending the same unit of digital currency more than once.

Besides revolutionizing digital currencies, Nakamoto's blockchain concept also created a secure digital ledger system that has many applications for both the public and private sector. As a result, many companies, developers, and governments have begun to explore how to apply blockchain to a variety of problems.

How a Blockchain Works



1. A transaction is initiated.
2. The transaction is broadcast to every node in the network.
3. The nodes form a consensus on whether the transaction is valid.
4. The nodes add valid transactions to a "block."
5. The block is added to the blockchain.
6. The transaction is complete.

Prospects for Advancement

Since 2009, there has been a frenzy of investment in companies offering blockchain systems, cryptocurrencies, and other related services. These investments have led to important innovations. For example, blockchain systems have enabled the creation of "smart contracts"—executable code that uses the blockchain to execute and enforce an agreement between parties, such as renting digital assets or licensing music. While some blockchain applications are maturing, others are still in their nascent stages as researchers seek to improve blockchain systems to address problems such as scalability and efficiency.

One of the more mature applications of blockchain is for initial coin offerings (ICOs), an alternative to raising funds from venture capital or through initial public offerings of stock. In an ICO, rather than buying an ownership stake in a company, investors are buying into a new digital currency that they expect will increase in value based on a company's proposed business model. The ICO investment process has inevitably led to some fraud, such as companies offering bogus business plans, and the practice has come under the scrutiny of several financial regulators.

A rich ecosystem of blockchain-based projects has emerged, and it continues to grow as the public and private sectors both explore new applications where this technology may prove most fruitful.

Applications and Impact

Broadly, there are six categories of blockchain applications.

First, the most prominent is for cryptocurrency—a digital currency that uses cryptography for security. While Bitcoin is the best-known example of a cryptocurrency, there are hundreds of others. Some cryptocurrencies are meant to be an alternative to an official currency, while others work with existing ones.

Second, some services use blockchain ledgers to create repositories of data that users can access, add to, and extract insights from. For example, the world's largest shipping company, Maersk, uses a blockchain application to track goods traveling across its shipping system. The system allows shipping companies, customs authorities, cargo owners, and freight forwarders to locate and identify shipping containers anywhere in the world. Similarly, some businesses are partnering with government agencies to use blockchain to securely register deeds and land titles to improve searchability and prevent fraud.

The third category primarily uses blockchains to create marketplaces for goods or services, such as computing cycles, bandwidth, or energy, or applications like peer-to-peer lending, which connect individual lenders with borrowers.

Fourth, applications use blockchain to establish the authenticity of goods or data. For example, one company uses blockchain to allow buyers to verify the authenticity of resold event tickets.

Fifth, some services use blockchains to give users more control over data or services. For example, some companies are experimenting with blockchains to improve identify management systems by embedding identity information, like driver's license numbers, on a blockchain so users can identify themselves to online services.

Finally, some applications use blockchains to automate actions. For example, Ethereum offers businesses the ability to use smart contracts, as described earlier.

Certainly, some applications overlap between different categories. For example, supply chain management applications have elements of shared ledger services and authenticity programs, as they are designed to track and authenticate real-world goods but also serve as a large repository of data for all users to access, amend, and analyze.

Policy Implications

There are four important policy implications related to blockchain. First, policymakers should actively support blockchain development and deployment, including through government use and procurement of the technology and research and development funding to test blockchain applications.

Second, policymakers should avoid laws and regulations that would effectively prevent the use of blockchain technology. Certain policies—such as mandates to weaken encryption standards, regulations that force organizations to delete data, and restrictions on where companies can store and send data—can prevent the use of blockchain technology. For example, if a country passes a law that bars companies from sending personal data abroad, it could preclude the use of a blockchain system.

Third, lawmakers should pass legislation that treats blockchain-secured records and smart contracts as legal business documents and blockchain-secure signatures as valid electronic signatures. Some U.S. states, such as Delaware and Arizona, have taken some of these steps, but there is not yet a uniform legal standard nationally.

Finally, governments should ensure regulations are not getting in the way of using blockchain technologies. Products that rely on blockchain technologies—especially those in the financial services sector—are often halted by regulatory agencies because they do not fit neatly into predetermined categories within the law. To address this problem, agencies should adopt mechanisms to better understand how companies are using blockchain and modernize regulations to permit legitimate uses.

Recommended Reading

- Alan McQuinn, Weining Guo, and Daniel Castro, "Policy Principles for Fintech" (Information Technology and Innovation Foundation, October 2016), https://itif.org/publications/2016/10/18/policy-principles-fintech.

- Robert Atkinson, Daniel Castro, and Alan McQuinn, "Comments to the New York Department of Financial Services on the Proposed BitLicense Framework" (Information Technology and Innovation Foundation, October 2014), https://itif.org/publications/2014/10/21/itif-comments-new-york-state-department-financial-services-proposed.

- Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene" (Information Technology and Innovation Foundation, February 2015), https://itif.org/publications/2015/02/02/how-and-when-regulators-should-intervene.