Blockchain Technology

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by the consensus of a majority of the participants in the system. In basic analogy, it is easy to steal a cookie from a cookie jar kept in a secluded place than stealing the cookie from a cookie jar kept in a marketplace, being observed by thousands of people. A blockchain is characterized by the following:

- **Immutability:** Immutability means something that can't be changed or altered. This is one of the top blockchain features that help to ensure that the technology will remain as it is – a permanent, unalterable network. Blockchain technology works slightly differently than the typical banking system. Instead of relying on centralized authorities, it ensures the blockchain features through a collection of nodes. Every node on the system has a copy of the digital ledger. To add a transaction, every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof. So, without the consent of the majority of nodes, no one can add any transaction blocks to the ledger. Another fact that backs up the list of key blockchain features is that once the transaction blocks get added to the ledger, no one can just go back and change it. Thus, any user on the network won't be able to edit, delete or update it.
- **Decentralized:** The basic feature of blockchain is that data can be inserted and accessed on any node distributedly. The network is decentralized, meaning it doesn't have any governing authority or a single person looking after the framework. Rather, a group of nodes maintains the network making it decentralized. This is one of the key features of blockchain technology that works perfectly. In simple terms, Blockchain puts users in a straightforward position. As the system doesn't require any governing authority, we can directly access it from the web and store our assets there. You can store anything starting from cryptocurrencies, important documents, contracts, or other valuable digital assets. And with the help of blockchain, you'll have direct control over them using your private key. So, the decentralized structure is giving the common people their power and rights back on their assets.
- **Enhanced Security:** Unlike vulnerable websites, which can be easily attacked despite security passwords, in a blockchain, data is shared between multiple nodes without any central point, so it cannot be stolen. Data is entirely secured thanks to encryption with private and public keys. Public keys are randomly generated as a long string and publicly shared. The private key, on the other hand, is used as a password to access users' data. As it gets rid of the need for a central authority, no one can just simply change any characteristics of the network for their benefit. Using encryption ensures another layer of security for the system.
- **Distributed Ledger:** All stored data is shared multiple times among all nodes of the network. Information in a blockchain is considered as a shared file. The shared information is easily verified and accessible for anyone in the network. This also ensures that data cannot be stolen and is synchronized with other files. Most importantly, because there is no central point, the data can not be corrupted or attacked. Distributed ledger responds really well to any suspicious activity or tamper. As no one can change the ledger and everything updates real fast, tracking what's happening in the ledger is quite easy with all these nodes.

Blockchain technology enables the creation of a decentralized environment, where the cryptographically validated transactions and data are not under the control of any third-party organization. Any transaction ever completed is recorded in an immutable ledger in a verifiable, secure, transparent, and permanent way, with a timestamp and other details. Three key ideas summarize what the technology does and why it's important:

- ***Data can act just like a physical object:*** Through a physical process called "tokenization," blockchain makes it possible for a data "asset" to exist in the digital world just like a physical object does in the real world. Virtual and real become indistinguishable.
- ***There can be a single version of truth that everyone can agree on:*** When using blockchain technology, once information is captured accurately, it never needs to be verified. Operational processes can focus on first-time accuracy instead of ongoing validity, and there is never a need to reconcile anything.
- ***Intermediaries are not needed:*** Blockchain creates an absolutely reliable method for transmitting information. Party A sends item X to Party B, who gets exactly what was expected every time. With the exchange process inherently and verifiably valid, nobody needs to vouch for anything.

Blockchain Building Blocks

The building blocks vary, but they mostly include:

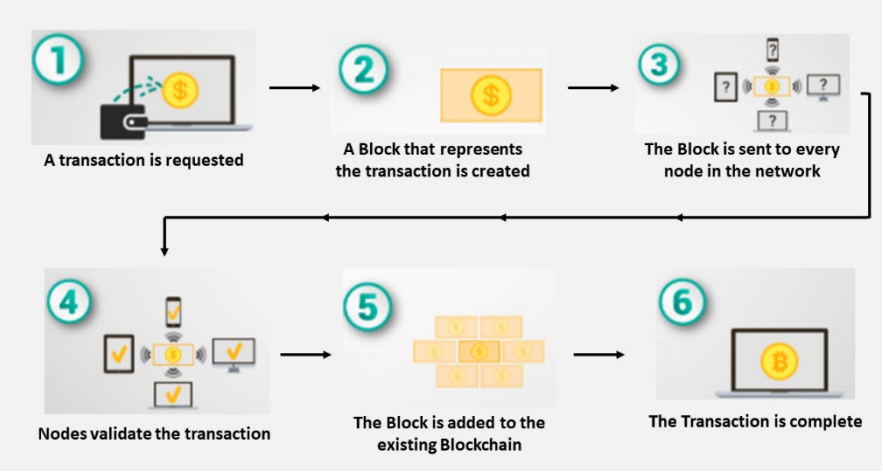
- **Encryption –** It refers to technical processes that secure data and systems, making it difficult for hackers to gain unauthorized access to information or to meddle with networks and transactions. Encryption prevents sensitive information from getting into the wrong hands and being misused or forged. This process generally falls into two categories: symmetric or asymmetric encryption. ***Symmetric key systems*** use the same key for encrypting and decrypting data and ***asymmetric systems*** use public and private key pairs for encrypting and decrypting data.
- **Digital Signatures –**They are primarily used to verify the authenticity of transactions. When users submit transactions, they must prove to every node in the system that they are authorized to spend those funds while preventing other users from also spending those funds. Every node in the network will verify the conditions of the submitted transaction and check all other nodes' work to agree on a correct state. Digital signatures can be considered as the digital counterparts of stamped seals or handwritten signatures. However, they are capable of offering better security with the reduced possibility of identity theft or impersonation.
- **Hashing –** It is an algorithm that converts a data file into a unique string of characters. Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering. Unlike encryption, which is a bidirectional transformation process in which data can be encrypted and decrypted, hashing is unidirectional. A data file is fed into a hashing function, and what emerges is a string of characters that cannot be "reversed" to derive the original data. It would not be possible to discern the original data, but it is possible to determine whether two hashes are the same and therefore represent the same primary data file – just like a human fingerprint.
- **Smart Contracts –** It is code that defines the lifecycle of one or more business objects. It is used by an application to generate transactions that record the changes to those objects. It can also be used to query the current value and transaction history of those objects. Smart contracts are basically computer programs that can automatically execute the terms of a contract.

Blockchain Architecture

These are the core blockchain architecture components:

- **Nodes –** These are simply computers that can store the blockchain's data, follow the rules of the blockchain's specific protocol, and communicate with the other nodes. Nodes can be physically located anywhere, and for this reason, they're called "distributed." Each node follows the same rules and maintains an identical copy of the blockchain data set.
- **Transaction –** It is the most basic component and the smallest building block of a blockchain system (records, information, etc.) that serves the purpose of blockchain. It may represent an exchange of something valuable (literally, a "transaction") or it may be a hash file representing something as simple as a single word or as complex as a software program. Transactions are bundled and delivered to each node in the form of a block. As new transactions are distributed throughout the network, they are independently verified and "processed" by each node. Each transaction is time-stamped and collected in a block.
- **Block –** It contains the information as a block header and transactions. Blocks are data structures whose purpose is to bundle sets of transactions and are replicated to all nodes in the network. The blocks in blockchain are created by miners. ***Mining*** is the process of creating a valid block that will be accepted by the rest of the network. Nodes take pending transactions, verify that they are cryptographically accurate, and package them into blocks to be stored on the blockchain. *Block header* is the metadata that helps in verifying the validity of a block. Simply, a block is a data structure used for keeping a set of transactions that is distributed to all nodes in the network.
- **Miners –** These are specific nodes that perform the block verification process before adding anything to the blockchain structure.
- **P2P Network:** The blockchain is a peer-to-peer (P2P) network working on the IP protocol. A P2P network is a flat topology with no centralized node. All nodes equally provide and can consume services while collaborating via a consensus algorithm. Peers contribute to the computing power and storage that is required for the upkeep of the network. P2P networks are generally more secure because they do not have a single point of attack or failure as in the case of a centralized network.

Any new record or transaction within the blockchain implies the building of a new block. Each record is then proven and digitally signed to ensure its genuineness. Before this block is added to the network, it should be verified by the majority of nodes in the system. Below is a blockchain architecture diagram that shows how this actually works in the form of a digital wallet:



How Blockchain Works (https://mlsdev.com/)

Taxonomy of Blockchain Systems

Current blockchain systems are categorized roughly into four types:

- **Public Blockchain –** It is the permission-less distributed ledger technology where anyone can join and do transactions. It is a non-restrictive version where each peer has a copy of the ledger. This also means that anyone can access the public blockchain if they have an internet connection. Public blockchains are designed to be fully decentralized, with no one individual or entity controlling which transactions are recorded in the blockchain or the order in which they are processed. Public blockchains allow all nodes of the blockchain to have equal rights to access the blockchain, create new blocks of data, and validate blocks of data. The most basic use of public blockchains is for mining and exchanging cryptocurrencies. Public blockchains are mostly secure if the users strictly follow security rules and methods. However, it is only risky when the participants don't follow the security protocols sincerely.
- **Private Blockchain –** It is a restrictive or permission blockchain operative only in a closed network. Private blockchains are usually used within an organization or enterprises where only selected members are participants of a blockchain network. The level of security, authorizations, permissions, accessibility is in the hands of the controlling organization. A private blockchain can be best defined as the blockchain that works in a restrictive environment, i.e., a closed network. It is also under the control of an entity. Thus, private blockchains are similar in use as a public blockchain but have a small and restrictive network. Private blockchains are valuable for enterprises who want to collaborate and share data, but don't want their sensitive business data visible on a public blockchain. Private blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership, etc.
- **Consortium Blockchain –** It is also known as Federated blockchains. A consortium blockchain is a semi-decentralized type where more than one organization manages a blockchain network. It is a creative approach to solving organizations' needs where there is a need for both public and private blockchain features. In a consortium blockchain, some aspects of the organizations are made public, while others remain private. Since it provides limited access to a specific group, it eliminates the risks that come with one entity controlling the network. These blockchains are more scalable and safer than public blockchains. This collaborative model offers some of the best use cases for the benefits of blockchain, bringing together a group of "frenemies" – businesses that work together but also compete against each other. Participants in consortium blockchains could include anyone from central banks, to governments, to supply chains.
- **Hybrid Blockchain –** It is a combination of the private and public blockchain. It uses the features of both types of blockchains where one can have a private permission-based system as well as a public permission-less system. With such a hybrid network, users can control who gets access to which data is stored in the blockchain. The hybrid system of blockchain is flexible so that users can easily join a private blockchain with multiple public blockchains. A transaction in a private network of a hybrid blockchain is usually verified within that network. This functionality makes it simple for businesses to operate with the transparency they are looking for without having to sacrifice security and privacy.

Common Consensus Algorithms

A **consensus algorithm** is a decision-making process for a group, where individuals of the group construct and support the decision that works best for the rest of them. It's a form of resolution where individuals need to support the majority decision, whether they like it or not. Concensus algorithms in blockchain are what make all the blockchain consensus sequences different from one another. Consensus algorithm solves the biggest problem that a distributed or multi-agent system goes through. It ensures that consensus is achieved with minimal resources, keeping integrity and transparency in the decisions it takes.

There are many types of consensus algorithms, but there are only two common types:

- **Proof of Work (PoW) –** It is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system. Whoever is the first one to get the solution to the mathematical problem gets the consensus permission to choose the block that should be added next to the platform. It is used widely in cryptocurrency mining for validating transactions and mining new tokens. Due to proof of work, Bitcoin and other cryptocurrency transactions can be processed peer-to-peer in a secure manner without the need for a trusted third party. Proof of work at scale requires huge amounts of energy, which only increases as more miners join the network. Proof of work makes it extremely difficult to alter any aspect of the blockchain, since such an alteration would require re-mining all subsequent blocks. It also makes it difficult for a user or pool of users to monopolize the network's computing power, since the machinery and power required to complete the hash functions are expensive. PoW requires nodes on a network to provide evidence that they have expended computational power (i.e., work) in order to achieve consensus in a decentralized manner and to prevent bad actors from overtaking the network. Because they are decentralized and peer-to-peer by design, blockchains such as cryptocurrency networks require some way of achieving both consensus and security. Proof of work is one such method that makes it too resource-intensive to try to overtake the network. The PoW algorithm remains the most popular because it among the few that cannot be compromised.
- **Proof of Stakes (PoS) –** It is a consensus mechanism that randomly assigns the node that will mine or validate block transactions according to how many coins that node holds. The more tokens held in a wallet, the more mining power is effectively granted to it. The proof of stake consensus protocol was created as an alternative algorithm seeking to address the scalability and environmental sustainability concerns surrounding the proof of work protocol. Proof of Stake gives mining power based on the percentage of coins held by a miner. Although the process is entirely random, still not every minor can participate in the staking. All the miners of the network are randomly chosen. If you have a specific amount of coins stored previously in your wallet, then you will be qualified to be a node on the network. It is seen as less risky in terms of the potential for miners to attack the network, as it structures compensation in a way that makes an attack less advantageous for the miner. The proof of stake seeks to address this issue by attributing mining power to the proportion of coins held by a miner. This way, instead of utilizing energy to answer PoW puzzles, a PoS miner is limited to mining a percentage of transactions that is reflective of their ownership stake. For instance, a miner who owns 3% of the coins available can theoretically mine only 3% of the blocks. Compared to PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Many blockchains adopt PoW at the beginning and transform to PoS gradually.

Blockchain Platforms

Blockchain platforms allow the development of blockchain-based applications. They can either be *permissioned* or permissionless. Here are the best blockchain platforms to use and to build a blockchain embedded ecosystem surely and quickly:

- **IBM Blockchain:** IBM is the pioneer company to use blockchain for creating efficient and transparent business operations. The blockchain platform of IBM is a popular platform to use. This platform provides a managed and full-stack blockchain-as-a-service offering that allows users to deploy their blockchain components in a user choice environment. Users can create, use, and grow their blockchain network by using this IBM blockchain platform. The IBM Blockchain developer tool was designed to be flexible, functional, and customizable.

- **Tron:** Tron is known as an operating system that is based on blockchain. It mainly allows users to build decentralized apps and exchange media assets. The TRX currency is being used to obtain access to specific operating software functionalities. As a result, the token's primary function is to be used on the Tron platform. Tron was created with one particular goal: to assist content producers in getting better compensated for their labor. The platform is based on a few ideas; one of them is that all information on the forum is open and not under the jurisdiction of central power. Content providers can be rewarded with digital assets, like the TRX currency or other currencies backed by TRX, in exchange for their work. This platform is a high-performance one, and it can handle 2000 transactions per second.
- **Stellar:** Stellar is a digital currency technology-based payment protocol. It handles millions of transactions every day. It enables cross-border payments between any two currencies in a matter of seconds. It resembles other blockchain-based coins in several aspects. It also provides the benefits of creation, trading, and sending digital representations of all forms of money, like, dollars, bitcoin, pesos, and much more. The public owns this blockchain platform because a transaction's basic charge on the Stellar platform is a small fee connected with every transaction execution. This charge is not intended to generate a profit. It serves as a deterrence to malicious behavior.
- **Tezos:** Tezos is designed to provide safe and correctness of code for digital assets and high-value cases. It is an open-source blockchain platform that is used across the globe for creating a decentralized blockchain network. It performs the peer-peer transaction and can deploy intelligent contacts. It is a self-governing blockchain platform. The self-amending cryptographic mechanism of Tezos is different, and this feature makes it unique from all other blockchain platforms.
- **Corda:** Corda is widely known as a business-oriented open-source blockchain initiative. Corda can create interconnected blockchain systems that enable transactions to be carried out safely and confidentially. It's an innovative contract platform. It allows firms to deal seamlessly with one another. It permits companies to keep track of transaction operations in a shared ledger, eliminating the requirement for participating individuals to double-check their transactions after engaging with one another. It is mainly used in sectors like construction, health, and finance.
- **Ethereum:** Ethereum, also known as ETH, is a leading blockchain platform these days. It allows users to create new financial applications, decentralize markets, make games, cryptocurrency wallets, and much more. The main aim of this platform is to nullify the third parties' access who save data for further financial instrument tracking. Ethereum has the largest community of core protocol developers, crypto-economic researchers, cypherpunks, and mining organizations. Ethereum has also built a large online support community to keep everyone up-to-date with product enhancements and updates.
- **Hyperledger Fabric –** It is a platform that is used to create applications and solutions using a modular architecture. It has a membership service and consensus. It includes a wide range of modular and versatile designs which can be used for various industrial uses. It can enable a network of networks. Members of the fabric network can use network work together in this platform. Hyperledger Fabric provides the user a secure and scalable platform to support their confidential contracts and private transactions.
- **Open-Chain –** It is an open-source blockchain platform. It is designed to manage digital assets in a secure, robust, and scalable manner. It uses Partitioned Consensus, and every instance of it has a single authority for valid transactions. This platform is designed based on client-server architecture, which makes it more efficient and reliable. No miner involvement exists in this platform, so the open-chain blockchain platform gives direct, accessible, and instant transactions.

References:

Blockchain architecture (2019). Citing sources. Retrieved on November 4, 2021, https://www.edureka.co/
Blockchain platforms (2020). Citing sources. Retrieved on November 5, 2021, https://www.blockchain-council.org/
Consensus algortihms (2021). Citing sources. Retrieved on November 5, 2021, https://www.investopedia.com/
Crosby, M. Verma, S., Kalyanaraman, V., & Pattanayak, P. (n.d.). *Blockchain technology: Beyond bitcoin.* Sutardja Center for Enterpreneurship and Technology.
Fuchs, P. (2019). *Blockchain: Everything you need to know.* Mercer LLC.
Taxonomy of blockchain systems (2021). Citing sources. Retrieved on November 4, 2021, https://101blockchains.com/
Understanding blockchain technology and how to get involved (2018). Citing sources. Retrieved on November 4, 2021, from https://www.researchgate.net/publication/346463547
Zheng, Z., Wang, H., Dai, H. & Xie, S.. (2017). *An overview of blockchain technology: Architecture, consensus, and future trends.* Institute of Advance Technology.