UNIT – 1 : INTRODUCTION TO BLOCKCHAIN

Introduction of the Course:

Blockchain is a decentralized and distributed ledger technology that enables secure and transparent record-keeping of digital transactions. It gained prominence as the underlying technology for cryptocurrencies like Bitcoin, but its applications extend far beyond digital currencies. Blockchain is a revolutionary concept that has the potential to transform various industries by providing a tamper-resistant and transparent way to record and verify transactions.

Key features of blockchain include:

1. **Decentralization:** Unlike traditional centralized systems where a single authority or intermediary controls the database, blockchain operates on a decentralized network of computers (nodes). Each node has a copy of the entire blockchain, ensuring a distributed and resilient system.
2. **Consensus Mechanism:** To validate and add new transactions to the blockchain, a consensus mechanism is employed. Various consensus algorithms, such as Proof of Work (PoW) and Proof of Stake (PoS), ensure agreement among participants on the validity of transactions without the need for a central authority.
3. **Immutability:** Once a block of transactions is added to the blockchain, it is extremely difficult to alter or delete the information contained within it. This immutability is achieved through cryptographic hashing and the interconnected nature of blocks.
4. **Transparency:** All participants in a blockchain network have access to the same information. Transactions are visible to all nodes, providing transparency and reducing the risk of fraud or manipulation.
5. **Smart Contracts:** Smart contracts are self-executing contracts with the terms directly written into code. They automatically enforce and execute the terms of an agreement when predefined conditions are met. Smart contracts run on the blockchain, eliminating the need for intermediaries.
6. **Security:** Cryptography is fundamental to the security of blockchain. Transactions are secured using cryptographic techniques, and the decentralized nature of the network makes it resistant to hacking or attacks on a single point of failure.

Blockchain technology finds applications in various sectors beyond finance, including supply chain management, healthcare, voting systems, identity verification, and more. It has the potential to streamline processes, enhance security, and reduce costs by eliminating the need for intermediaries in many transactions.

Objective of the Course:

The primary objective of this course is threefold:

1. **Broad Overview of Blockchain Concepts:**
   - *Objective:* Provide students with a broad overview of essential concepts in blockchain technology.
   - *Implication:* Students will develop a foundational understanding of the key principles, mechanisms, and components that constitute blockchain technology, laying the groundwork for more in-depth exploration.
2. **Familiarity with Bitcoin and Ethereum Protocols:**
   - *Objective:* Familiarize students with the Bitcoin and Ethereum protocols.
   - *Implication:* By delving into the Bitcoin and Ethereum protocols, students will gain insights into the foundational technologies that underpin blockchain systems, preparing them for subsequent applications and programming.
3. **Understanding Different Types of Blockchain and Consensus Algorithms:**
   - *Objective:* Introduce students to various types of blockchains and consensus algorithms.
   - *Implication:* Students will explore the diverse landscape of blockchain design, gaining an understanding of different blockchain types and consensus mechanisms that contribute to the uniqueness of each blockchain network.

Scope of the Course:

The course scope encompasses a range of topics crucial to blockchain technology:

- **Distributed Systems:**
  - *Scope:* Understanding the basic notion of distributed systems.
  - *Outcome:* Students will grasp the principles that define distributed systems, laying the groundwork for comprehending the decentralized nature of blockchain.

- **Immutable Distributed Ledger and Trust Model:**
  - *Scope:* Exploring the working of an immutable distributed ledger and the trust model defining blockchain.
  - *Outcome:* Students will learn how blockchain achieves immutability, transparency, and a trust model through its distributed ledger system.

- **Essential Components of a Blockchain Platform:**
  - *Scope:* Illustrating the essential components of a blockchain platform.
  - *Outcome:* Students will be able to identify and explain critical components such as nodes, blocks, consensus mechanisms, and cryptographic elements that constitute a blockchain platform.

Outcome of the Course:

Upon successful completion of the course, students will be equipped with the following outcomes:

1. **Explanation of Distributed Systems (CO-1):**
   - *Outcome:* Students will be able to explain the basic notion of distributed systems, providing a solid understanding of the principles governing decentralized networks.
2. **Working of Immutable Distributed Ledger and Trust Model (CO-2):**
   - *Outcome:* Students will demonstrate an understanding of how blockchain achieves an immutable distributed ledger and a trust model, ensuring transparency and reliability.
3. **Illustration of Essential Components of a Blockchain Platform (CO-3):**
   - *Outcome:* Students will illustrate the essential components of a blockchain platform, demonstrating their ability to identify and explain key elements that constitute a functional blockchain system.

By achieving these objectives and outcomes, students completing the course will be well-prepared to engage with blockchain technology in various capacities, whether in development, analysis, or decision-making roles within the dynamic blockchain landscape.

Introduction to Blockchain Technology:

Blockchain could be a data structure that could be a growing list of information blocks. The knowledge blocks area unit coupled along, such recent blocks can't be removed or altered. Blockchain is the backbone Technology of the Digital CryptoCurrency BitCoin.

What is Blockchain?

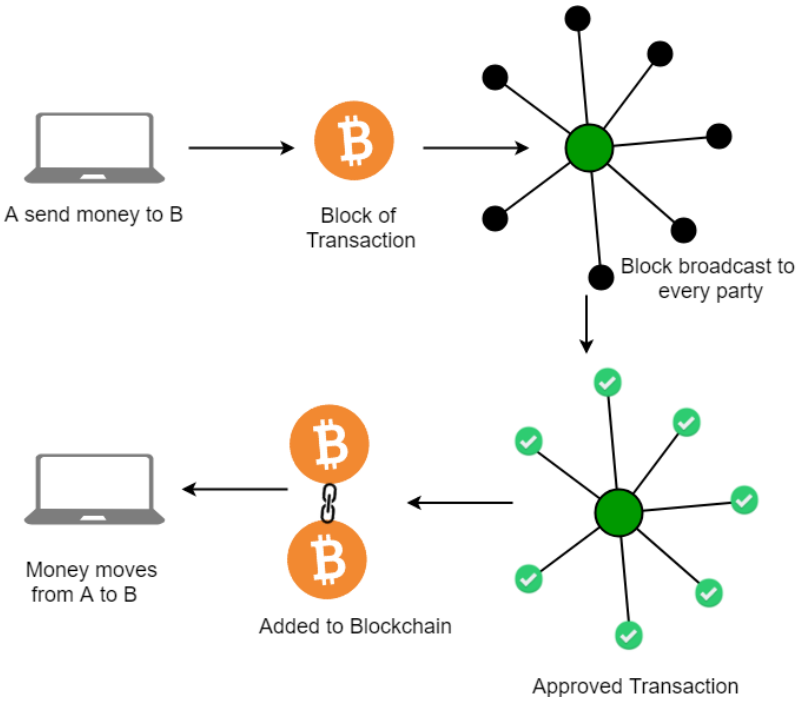
The blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties. Each transaction is verified by the majority of participants of the system.

It contains every single record of each transaction. Bitcoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first came to light when a person or group of individuals name 'Satoshi Nakamoto' published a white paper on "*BitCoin: A peer-to-peer electronic cash system*" in 2008.

Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction.

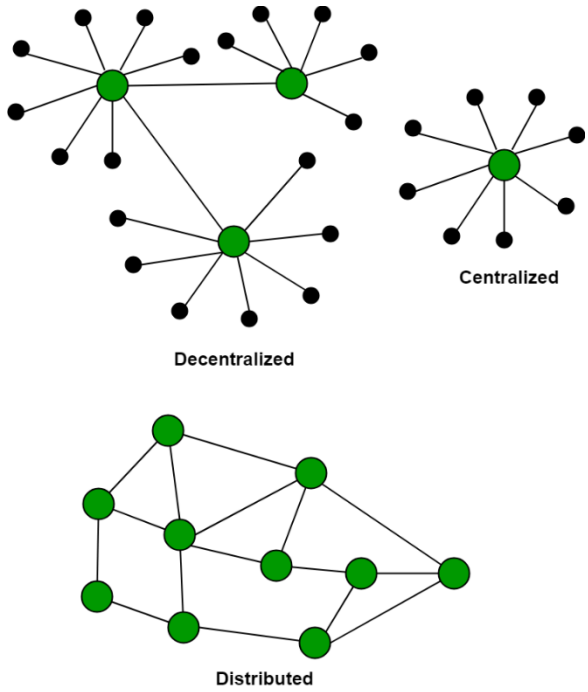
How does Blockchain Technology Work?

One of the famous use of Blockchain is Bitcoin. Bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the Internet. Each transaction protects through a digital signature.



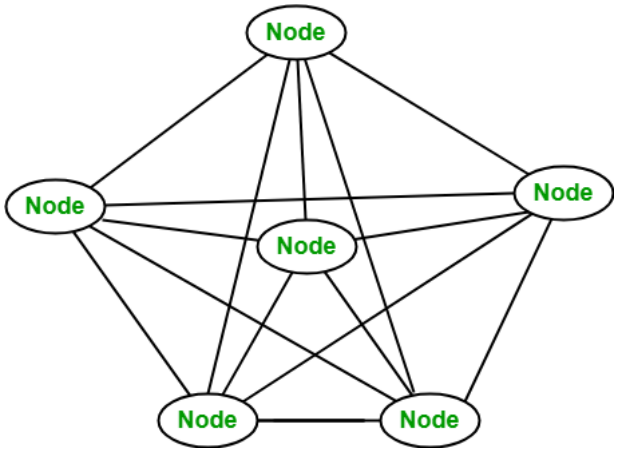
Blockchain Decentralization:

There is no Central Server or System which keeps the data of the Blockchain. The data is distributed over Millions of Computers around the world which are connected to the Blockchain. This system allows the Notarization of Data as it is present on every Node and is publicly verifiable.



Blockchain Nodes:

A node is a computer connected to the Blockchain Network. Node gets connected with Blockchain using the client. The client helps in validating and propagating transactions onto the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain. The Node connected to the Blockchain which helps in the execution of a Transaction in return for an incentive is called Miners.



Disadvantages of the current transaction system:

- Cash can only be used in low-amount transactions locally.
- The huge waiting time in the processing of transactions.
- The need for a third party for verification and execution of Transactions makes the process complex.
- If the Central Server like Banks is compromised, the whole system is affected including the participants.
- Organizations doing validation charge high process thus making the process expensive.

Building trust with Blockchain:

Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with it's that you don't need to when operating on a Blockchain network. Blockchain builds trust through the following five attributes:

- **Distributed:** The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain. All this is done in real time as there is no central server controlling the data.
- **Secure:** There is no unauthorized access to Blockchain made possible through Permissions and Cryptography.
- **Transparent:** Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.
- **Consensus-based:** All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.
- **Flexible:** Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Networks can evolve in pace with business processes.

What are the benefits of Blockchain?

- **Time-saving:** No central Authority verification is needed for settlements making the process faster and cheaper.
- **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of the shared ledger.

- **Tighter security:** No one can tamper with Blockchain Data as it is shared among millions of Participants. The system is safe against cybercrimes and Fraud.
- **Collaboration:** It permits every party to interact directly with one another while not requiring third-party negotiation.
- **Reliability:** Blockchain certifies and verifies the identities of every interested party. This removes double records, reducing rates and accelerating transactions.

Application of Blockchain:

- Leading Investment Banking Companies like Credit Suisse, JP Morgan Chase, Goldman Sachs, and Citigroup have invested in Blockchain and are experimenting to improve the banking experience and secure it.
- Following the Banking Sector, the Accountants are following the same path. Accountancy involves extensive data, including financial statements spreadsheets containing lots of personal and institutional data. Therefore, accounting can be layered with blockchain to easily track confidential and sensitive data and reduce human error and fraud. Industry Experts from Deloitte, PwC, KPMG, and EY are proficiently working and using blockchain-based software.
- Booking a Flight requires sensitive data ranging from the passenger's name, credit card numbers, immigration details, identification, destinations, and sometimes even accommodation and travel information. So sensitive data can be secured using blockchain technology. Russian Airlines are working towards the same.
- Various industries, including hotel services, pay a significant amount ranging from 18-22% of their revenue to third-party agencies. Using blockchain, the involvement of the middleman is cut short and allows interaction directly with the consumer ensuring benefits to both parties. Winding Tree works extensively with Lufthansa, AirFrance, AirCanada, and Etihad Airways to cut short third-party operators charging high fees.
- Barclays uses Blockchain to streamline the Know Your Customer (KYC) and Fund Transfer processes while filling patents against these features.
- Visauses Blockchain to deal with business-to-business payment services.
- Unilever uses Blockchain to track all their transactions in the supply chain and maintain the product's quality at every stage of the process.
- Walmart has been using Blockchain Technology for quite some time to keep track of their food items coming right from farmers to the customer. They let the customer check the product's history right from its origin.

- DHL and Accenture work together to track the origin of medicine until it reaches the consumer.
- Pfizer, an industry leader, has developed a blockchain system to keep track of and manage the inventory of medicines.
- The government of Dubai looking forward to making Dubai the first-ever city to rely on entirely and work using blockchain, even in their government office.
- Along with the above organizations, leading tech companies like Google, Microsoft, Amazon, IBM, Facebook, TCS, Oracle, Samsung, NVIDIA, Accenture, and PayPal, are working on Blockchain extensively.

Is Blockchain Secure?

Nowadays, as the blockchain industry is increasing day by day, a question arises is Blockchain safe? or how safe is blockchain? As we know after a block has been added to the end of the blockchain, previous blocks cannot be changed. If a change in data is tried to be made then it keeps on changing the Hash blocks, but with this change, there will be a rejection as there are no similarities with the previous block.

Just imagine there is a who hacker runs a node on a blockchain network, he wants to alter a blockchain and steal cryptocurrency from everyone else. With a change in the copy, they would have to convince the other nodes that their copy was valid.

They would need to control a majority of the network to do this and insert it at just the right moment. This is known as a 51% attack because you need to control more than 50% of the network to attempt it.

Timing would be everything in this type of attack—by the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter.

Blockchain Project Ideas:

Here are a few project ideas for beginners looking to learn more about blockchain technology:

1. **Cryptocurrency Wallet:** Create a simple cryptocurrency wallet application that allows users to send and receive digital assets.
2. **Blockchain Explorer:** Develop a web-based application that allows users to view and search the transactions on a specific blockchain.
3. **Smart Contract:** Implement a simple smart contract on the Ethereum blockchain that can be used to manage a digital token or asset.

4. **Voting System**: Create a blockchain-based voting system that allows for secure and transparent voting while maintaining voter anonymity.
5. **Supply Chain Management:** Develop a blockchain-based system for tracking the movement of goods and services through a supply chain, providing greater transparency and traceability.
6. **Decentralized marketplace:** Create a decentralized marketplace using blockchain technology where the goods and services can be directly bought by the customers without any intermediary.
7. **Identity Management:** Create a decentralized digital identity management system that allows users to control their personal information and share it securely with others.

These are just a few examples, there are many other possibilities to explore within Blockchain technology.

Future Scope of Blockchain Technology:

Finance, supply chain management, and the Internet of Things are just a few of the sectors that blockchain technology has the power to upend (IoT). The following are some potential uses for blockchain in the future:

- **Digital Identity:** Blockchain-based digital IDs might be used to store personal data safely and securely as well as offer a means of establishing identity without the need for a central authority.
- **Smart Contracts:** A variety of legal and financial transactions could be automated using smart contracts, self-executing contracts with the terms of the agreement put straight into lines of code.
- **Decentralized Finance (DeFi):** Using blockchain technology, decentralized financial systems might be built that support peer-to-peer transactions and do away with conventional intermediaries like banks.
- **Supply Chain Management:** Blockchain technology can be applied to a permanent record of how goods and services have been moved, enabling improved openness and traceability across the whole supply chain.
- **Internet of Things (IoT):** Blockchain technology may be used to build decentralized, secure networks for IoT devices, enabling them to exchange data and communicate with one another in an anonymous, safe manner.

In general, blockchain technology is still in its early stages and has a wide range of potential applications.

Advantages of Blockchain Technology:

1. **Decentralization:** The decentralized nature of blockchain technology eliminates the need for intermediaries, reducing costs and increasing transparency.
2. **Security:** Transactions on a blockchain are secured through cryptography, making them virtually immune to hacking and fraud.
3. **Transparency:** Blockchain technology allows all parties in a transaction to have access to the same information, increasing transparency and reducing the potential for disputes.
4. **Efficiency:** Transactions on a blockchain can be processed quickly and efficiently, reducing the time and cost associated with traditional transactions.
5. **Trust:** The transparent and secure nature of blockchain technology can help to build trust between parties in a transaction.

Disadvantages of Blockchain Technology:

1. **Scalability:** The decentralized nature of blockchain technology can make it difficult to scale for large-scale applications.
2. **Energy Consumption:** The process of mining blockchain transactions requires significant amounts of computing power, which can lead to high energy consumption and environmental concerns.
3. **Adoption:** While the potential applications of blockchain technology are vast, adoption has been slow due to the technical complexity and lack of understanding of the technology.
4. **Regulation:** The regulatory framework around blockchain technology is still in its early stages, which can create uncertainty for businesses and investors.
5. **Lack of Standards:** The lack of standardized protocols and technologies can make it difficult for businesses to integrate blockchain technology into their existing systems.
6. Overall, the advantages of blockchain technology are significant and have the potential to revolutionize many industries. However, there are also several challenges and disadvantages that must be addressed before the technology can reach its full potential.

History of Blockchain:

The history of blockchain dates back to the early 1990s, and its evolution has been marked by key technological developments and the emergence of various blockchain-based applications. Here's a brief overview of the history of blockchain:

1991 - 2008: Precursors to Blockchain -

1. **Cryptographic Advances (1991 - 1992):** Stuart Haber and W. Scott Stornetta introduced a cryptographically secure chain of blocks to timestamp digital documents, preventing backdating or tampering. Although not a complete blockchain, their work laid the foundation for secure, time-stamped records.
2. **Hashcash (1997):** Computer scientist Adam Back introduced Hashcash, a proof-of-work system designed to curb email spam. It involved solving computational puzzles, which became an integral part of later blockchain systems.
3. **B-Money (1998) and Bit Gold (2005):** Wei Dai proposed B-Money, a concept for an anonymous, distributed electronic cash system. In 2005, Nick Szabo introduced Bit Gold, a decentralized digital currency system with elements resembling later blockchain concepts.

2008: The Birth of Bitcoin -

1. **Bitcoin Whitepaper (2008):** On October 31, 2008, an individual or group using the pseudonym Satoshi Nakamoto published the Bitcoin whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." This paper outlined the principles of a decentralized, trustless, and transparent digital currency system.
2. **Genesis Block (2009):** On January 3, 2009, Nakamoto mined the first block, known as the Genesis Block, marking the launch of the Bitcoin blockchain. This event included a coded message referencing a headline from The Times, cementing the historical significance.

2010 - 2013: Early Development and Altcoins -

1. **Mining Pools and GPU Mining (2010):** Bitcoin mining became more widespread, leading to the creation of mining pools to combine computational resources. Graphics Processing Units (GPUs) also replaced Central Processing Units (CPUs) for mining.
2. **First Bitcoin Exchange (2010):** The first exchange for trading Bitcoin to fiat currency, BitcoinMarket.com, was established, enabling users to buy and sell Bitcoin with traditional currencies.

3. **Rise of Altcoins (2011 - 2013):** Alternative cryptocurrencies (altcoins) such as Namecoin and Litecoin were introduced, experimenting with different consensus mechanisms and features.

2014 - Present: Diversification and Blockchain Beyond Bitcoin -

1. **Ethereum and Smart Contracts (2015):** Vitalik Buterin introduced Ethereum, a blockchain platform enabling the development of decentralized applications (DApps) and smart contracts. Smart contracts are self-executing contracts with the terms directly written into code.
2. **Blockchain Adoption (2016 - Present):** Blockchain technology gained recognition beyond cryptocurrencies. Industries explored its potential for supply chain management, healthcare, finance, and more. Consortiums and collaborations formed to develop enterprise-grade blockchain solutions.
3. **ICO Boom and Regulatory Developments (2017):** Initial Coin Offerings (ICOs) became a popular fundraising method for blockchain projects. Regulatory scrutiny increased as governments around the world began to address the legal and regulatory aspects of blockchain and cryptocurrencies.
4. **DeFi and NFTs (2020s):** Decentralized Finance (DeFi) gained prominence, offering blockchain-based financial services. Non-Fungible Tokens (NFTs) gained widespread attention, representing ownership of digital or physical assets on the blockchain.

The history of blockchain is a story of continuous innovation and adaptation. From its humble beginnings as the foundation of Bitcoin to the diverse ecosystem of today, blockchain technology has shown its potential to revolutionize various industries and redefine how we interact with digital information and assets.

Features of Blockchain:

Blockchain technology is characterized by several key features that contribute to its uniqueness and utility across various industries. Here are some of the fundamental features of blockchain:

1. **Decentralization:**
   - **Definition:** No central authority or intermediary controls the blockchain network. Instead, it operates on a distributed network of nodes, each with a copy of the entire blockchain.
   - **Benefits:** Reduces the risk of a single point of failure, enhances security, and fosters trust among participants.

2. **Distributed Ledger:**
   - **Definition:** A decentralized database or ledger that records all transactions across the network. Every participant has a copy of this ledger.
   - **Benefits:** Enhances transparency, reduces the risk of data manipulation, and ensures a consistent view of transaction history.
3. **Consensus Mechanism:**
   - **Definition:** A process to achieve agreement among nodes on the validity of transactions added to the blockchain. Common consensus mechanisms include Proof of Work (PoW) and Proof of Stake (PoS).
   - **Benefits:** Prevents double-spending, ensures the integrity of the ledger, and maintains a synchronized network.
4. **Immutability:**
   - **Definition:** Once a block of transactions is added to the blockchain, it is extremely difficult to alter or delete. The data on the blockchain is considered immutable.
   - **Benefits:** Ensures the integrity of historical records, reduces the risk of fraud, and provides a reliable transaction history.
5. **Cryptographic Security:**
   - **Definition:** Cryptography is used to secure transactions and control access to the blockchain. Hash functions, digital signatures, and encryption play crucial roles.
   - **Benefits:** Enhances the security and privacy of transactions, protects against unauthorized access, and ensures the authenticity of participants.
6. **Smart Contracts:**
   - **Definition:** Self-executing contracts with terms written in code. These contracts automatically execute when predefined conditions are met.
   - **Benefits:** Automates and enforces contract execution, reduces the need for intermediaries, and increases efficiency in various industries.
7. **Transparency:**
   - **Definition:** All participants in the blockchain network have access to the same information. Transactions are visible to all nodes, ensuring transparency.
   - **Benefits:** Builds trust among participants, reduces the risk of fraud, and allows for easy verification of transactions.

8. **Permission Models:**
    - **Definition:** Blockchain networks can be public, private, or consortium-based, determining who can participate and validate transactions.
    - **Benefits:** Allows for flexibility in use cases. Public blockchains are open to anyone, while private blockchains restrict access to authorized participants.
9. **Interoperability:**
    - **Definition:** The ability of different blockchain networks to interact and share information seamlessly.
    - **Benefits:** Facilitates collaboration, allows for the integration of different systems, and promotes widespread adoption.
10. **Scalability:**
    - **Definition:** The ability of a blockchain network to handle an increasing number of transactions without compromising performance.
    - **Benefits:** Ensures that the blockchain can support growing user bases and transaction volumes over time.

Important Blockchain Terminologies:

- **Node:** A member of the Blockchain network.
- **Address:** An address is a string of alphanumeric characters which identify an entity in the blockchain network. Used to send and receive cryptocurrency transactions.
- **Distributed ledger:** A ledger which is maintained on many nodes in a decentralized network. The records are stored in a chronological order. This ledger can be of two types: Permissioned and Unpermissioned based on who has the access to view the ledger.
- **Peer to peer:** Also short termed as P2P. As the name suggests, interactions that happen between two peers(parties/entities) in a highly interconnected network.
- **Block:** A block is a data structure that contains all the necessary metadata about the block (Block Header) itself and contains transactions. The first block in a blockchain is called the genesis block.
- **block height:** Block height is the number of blocks connected in the blockchain. Block height is a usually measure of the amount of data in the blockchain.
- **Blockchain:** A chain of blocks which contain some metadata about the block, some transactions and joined to the previous block by the previous block's hash value.
- **Block explorer:** A tool to see statistics of a block in a blockchain.

- **Hash:** Performing a hash function on the output data in a blockchain is termed as hash. Commonly used in sentences like “the hash of “this file is 142c53v2v31vc1526v35v63v5v4”. Used in verifying cryptocurrency transactions.
- **Hash rate:** Performance of a computer mining is measured in hashes per second or hash rate.
- **Cryptographic hash function:** A function that takes a variable-size input and output is a fixed-size unique value. SHA-256 algorithm is a cryptographic hash function example.
- **Mining:** Process of solving a complex mathematical problem in order to attach the new block of transactions to the blockchain. This term is used in reference to blockchains that use Proof-of-Work as consensus mechanism. But general use of this term is prevalent too.
- **Difficulty:** Hardness with which a new block of transactions can be connected to the blockchain. In Bitcoin, the difficulty is adjusted every 2016 blocks to keep the time of mining a new block at about 10 minutes.
- **Block reward:** Reward that is given to the entity which connects the new block to the blockchain. In the case of Bitcoin, miners get a reward of 12.5 Bitcoins for attaching new block to the blockchain. In the case of Peercoin, minters get a reward of 42.64 (at the time of writing this article) Peercoins for attaching a new block of transactions to the blockchain.
- **Cryptocurrency:** A formal of digital asset which is regulated and transacted on the blockchain network. Encryption techniques are used to regulate the cryptocurrency, hence the name.
- **Satoshi:** The smallest recordable unit of currency in the Bitcoin. Currently, a satoshi is numerically equal to 0.00000001 BTC.
- **Altcoin:** An alternative to Bitcoin (ALTernative COIN). A famous altcoin is Litecoin.
- **Wallet:** A wallet is a file that contains the private keys of an entity. A wallet provides an interface to view and do transactions on the blockchain. Different wallets for different type of blockchains.
- **Consensus:** Consensus is a way for all the nodes in a network to agree on the shared state of the ledger (list of transactions). Some common consensus mechanisms are Raft, Paxos, Byzantine Fault Tolerance algorithm, Proof-of-Work(PoW), Proof-of-Stake (PoS), etc.

- **Smart contract:** A smart contract has details and permissions written in code that require an exact sequence of events to take place to trigger the agreement of the terms mentioned in the smart contract. It can also include the time constraints that can introduce deadlines in the contract. Also known as cryptocontract and digital contract. It was first put forward by Nick Szabo in 1994.
- **Transaction:** An exchange of assets between two parties/entities.
- **Transaction Fee:** A part of the digital asset (cryptocurrency) that is charged from the parties who perform that transaction as a way to pay the networks who invest their resources in order to sustain the blockchain. In a proof of stake based blockchain (like Peercoin). the transaction fee is transferred to the minter/forger once he validates the new block of transactions successfully.
- **Blockchain fork:** An act of blockchain software update which leads to splitting of a blockchain into two or more valid blockchains. There are three common types of forks in blockchain, namely, hard fork, soft fork, temporary/accidental fork.
- **51% attack:** An attack in which a single organization (of entities) performs invalid activities on the blockchain network because they control 51% of the network's resources. In the Bitcoin network, it refers to owning 51% of miners. In Peercoin, it refers to owning 51% of peercoins.
- **Double Spend:** An act of using the same digital asset (cryptocurrency) twice. Its a common type of attack in blockchains. This type of attack becomes more difficult with increasing members that add the new block to the chain.
- **Confirmation:** The confirmation is the act of successfully adding a transaction to the blockchain after verification. As a rule of thumb, more confirmations means more security against a double spend attack (permanency).
- **Testnet:** As the name suggests, a Bitcoin test blockchain which is used by the network developers to carry out tests so that the main blockchain network is not affected. Assets in a testnet do not have any value. There have been three generations of testnet at the time of writing this article i.e., Testnet1, Testnet2, Testnet3 (currently).
- **dApp:** Full form : decentralized Application. An application that is open sourced which is operated anonymously and has its data stored on a blockchain. It must have some kind of incentive for the members who help to construct the blockchain.
- **ASIC:** Full form : Application Specific Integrated Circuit. These are a type of computers which are designed for performing a special task. In the case of Bitcoin, ASIC computers are used to solve SHA-256 hashing problem which help to connect the new blocks to the blockchain.

Components of Blockchain Network:

Following are the components of a Blockchain network –

1. Node
2. Ledger
3. Wallet
4. Nonce
5. Hash

1. Node:

It is of two types – Full Node and Partial Node.

- **Full Node** – It maintains a full copy of all the transactions. It has the capacity to validate, accept and reject the transactions.
- **Partial Node** – It is also called a Lightweight Node because it doesn't maintain the whole copy of the blockchain ledger. It maintains only the hash value of the transaction. The whole transaction is accessed using this hash value only. These nodes have low storage and low computational power.

2. Ledger:

It is a digital database of information. Here, we have used the term 'digital' because the currency exchanged between different nodes is digital i.e cryptocurrency. There are three types of ledger. They are –

1. **Public Ledger –** It is open and transparent to all. Anyone in the blockchain network can read or write something.
2. **Distributed Ledger –** In this ledger, all nodes have a local copy of the database. Here, a group of nodes collectively execute the job i.e verify transactions, add blocks in the blockchain.
3. **Decentralized Ledger –** In this ledger, no one node or group of nodes has a central control. Every node participates in the execution of the job.

3. Wallet:

It is a digital wallet that allows user to store their cryptocurrency. Every node in the blockchain network has a Wallet. Privacy of a wallet in a blockchain network is maintained using public and private key pairs. In a wallet, there is no need for currency

conversion as the currency in the wallet is universally acceptable. Cryptocurrency wallets are mainly of two types –

1. **Hot Wallet –** These wallets are used for online day-to-day transactions connected to the internet. Hackers can attack this wallet as it is connected to the internet. Hot wallets are further classified into two types –

   a. **Online/ Web wallets –** These wallets run on the cloud platform. Examples – MyEther Wallet, MetaMask Wallet.

   b. Software wallets – It consists of desktop wallets and mobile wallets. Desktop wallets can be downloaded on a desktop and the user has full control of the wallet. An example of a desktop wallet is Electrum.

   c. Mobile wallets – They are designed to operate on smartphone devices. Example – mycelium.

2. **Cold Wallet –** These wallets are not connected to the internet. It is very safe and hackers cannot attack it. These wallets are purchased by the user. Example – Paper wallet, hardware wallet.

   a. Paper wallet – They are offline wallets in which a piece of paper is used that contains the crypto address. The private key is printed in QR code format. QR code is scanned for cryptocurrency transactions.

   b. Hardware wallet – It is a physical electronic device that uses a random number generator that is associated with the wallet.

The focus of wallets is on these three things –

1. Privacy
2. Transactions should be secure
3. Easy to use

Privacy of a wallet is maintained using public and private key pairs. Transactions are made secure as a private key is used both to send fund and to open the encrypted message.

4. Nonce:

A nonce is an abbreviation for “number only used once,” which is a number added to a hashed or encrypted block in a blockchain. It is the 32-bit number generated randomly only one time that assists to create a new block or validate a transaction. It is used to make the transaction more secure.

It is hard to select the number which can be used as the nonce. It requires a vital amount of trial-and-error. First, a miner guesses a nonce. Then, it appends the guessed nonce to

the hash of the current header. After that, it rehashes the value and compares this to the target hash. Now it checks that whether the resulting hash value meets the requirements or not. If all the conditions are met, it means that the miner has created an answer and is granted the block.

5. Hash:

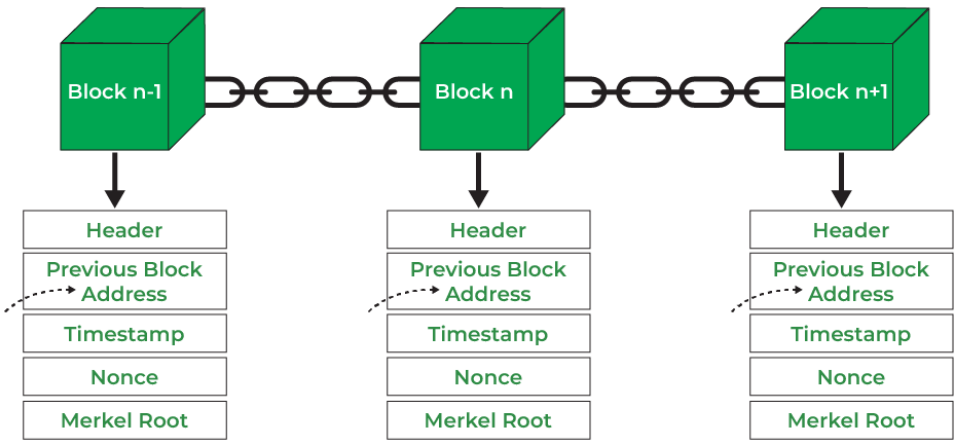
The data is mapped to a fixed size using hashing. It plays a very important role in cryptography. In a blockchain network hash value of one transaction is the input of another transaction. Properties of the hash function are as follows –

- Collision resistant
- Hiding
- Puzzle friendliness

Blockchain Structure:

Blockchain is a Distributed Ledger Technology. It is a distributed and decentralized database and it is secured ever as compared to other technologies.

Blockchain is a technology where multiple parties involved in communication can perform different transactions without third-party intervention. Verification and validation of these transactions are carried out by special kinds of nodes.



1. **Header:** It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.

2. **Previous Block Address/ Hash:** It is used to connect the $i+1^{th}$ block to the i^{th} block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.
3. **Timestamp:** It is a system verify the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.
4. **Nonce:** A nonce number which uses only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.
5. **Merkel Root:** It is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.

Merkle Tree:

Merkle tree also known as hash tree is a data structure used for data verification and synchronization.
It is a tree data structure where each non-leaf node is a hash of it's child nodes. All the leaf nodes are at the same depth and are as far left as possible. It maintains data integrity and uses hash functions for this purpose.

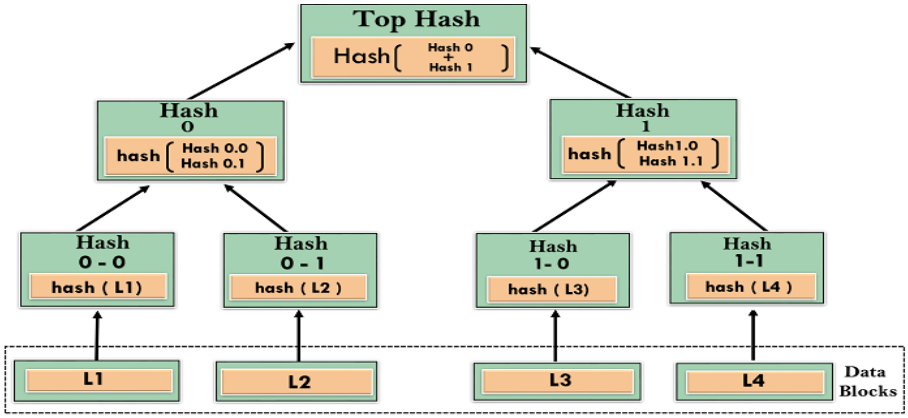
In **1992**, Merkle Trees were incorporated into the design, which makes blockchain more efficient by allowing several documents to be collected into one block.

Merkle Trees are used to create a 'secured chain of blocks.' It stored a series of data records, and each data records connected to the one before it. The newest record in this chain contains the history of the entire chain. However, this technology went unused, and the patent lapsed in 2004.

Hash Functions:

So before understanding how Merkle trees work, we need to understand how hash functions work.

A hash function maps an input to a fixed output and this output is called hash. The output is unique for every input and this enables fingerprinting of data. So, huge amounts of data can be easily identified through their hash.



This is a **binary merkel tree**, the top hash is a hash of the entire tree.

- This structure of the tree allows efficient mapping of huge data and small changes made to the data can be easily identified.
- If we want to know where data change has occurred then we can check if data is consistent with root hash and we will not have to traverse the whole structure but only a small part of the structure.
- The root hash is used as the fingerprint for the entire data.

For a Binary Merkel tree

Operation	**Complexity**
Space	O(n)
Searching	O(logn)
Traversal	O(n)
Insertion	O(logn)
Deletion	O(logn)
Synchronization	O(logn)

Applications:

- Merkle trees are useful in distributed systems where same data should exist in multiple places.
- Merkle trees can be used to check inconsistencies.
- Apache Cassandra uses Merkle trees to detect inconsistencies between replicas of entire databases.
- It is used in bitcoin and blockchain.

Is Blockchain Beyond the Law?

This sort of democratization is also proving troublesome when it comes to policing. Terrorists, warlords, and other wrongdoers can be effectively shut out of a centralized, regulated community, but it's not so easy with the leaderless blockchain. To this day, services using Tor software and the myriad iterations of black-market exchanges that sprang up following the 2014 take-down of the Silk Road darknet continue to utilize blockchain for a wide range of licit and illicit purposes.

Another important aspect of blockchain that is often overlooked is that not all blockchains are alike. Wesley Crook, CEO of cloud developer FP Complete, noted in Forbes recently that blockchain software packages come in a wide variety of designs and approaches to implementation.

Perhaps the most important element is cryptography, which should ideally incorporate the most trusted irreversible hash algorithms and public-key signing and verification tools.

Also, experience has shown that most blockchain breaches to date were the result of bugs introduced due to faulty implementation, as well as attacks on the network layer, social engineering vulnerabilities, and memory safety errors.

What's Next for Blockchain Technology?

At the moment, then, there doesn't appear to be a clear consensus as to where blockchain goes from here. To some, it is the future, to others, it is already an artifact of the past. It may be that the reason it is so difficult to gauge blockchain's fortune may be the fact the world economy itself is in such flux.

Whether it's on Wall Street, Main Street, or in the corporate world, power seems to be decentralizing everywhere as legions of connected users band together to write their own rules about work and financial success.

Perhaps the problem is in trying to force-fit blockchain into a role defined by the centralized economy where government and industry largely make the rules when in reality, it is a technology more suited to the emerging digital economy where, at the moment at least, individuals have greater leverage as to where, when and how they manage their affairs.