Blockchain Generations

There are 3 generation of blockchain

First-Generations Blockchain: Bitcoin

In the first-gen blockchain – specifically Bitcoin – was created which is a digital currency.

By empowering people with the technology to transact with one another (at a peer-to-peer level), they don't need to rely on centralized entities such as banks.

Bitcoin is the first real use case of blockchain technology and its main purpose is as a financial application , any user can send Bill digital money and there is security in that transaction.

Blockchain and bitcoin both have strong privacy because the transaction is anonymous and they can take peace in knowing that the system is secure in the technology and the trust lies in the algorithm and not a centralized figure.

Second Generation Blockchain : Ehereum

After Bitcoin's success, it was time for the next generation of blockchain, which was brought about by Ethereum. Second-generation blockchain technology does more than just document transactions. Using self-executing agreements between two parties, called smart contracts, transactions are faster and more secure than first-generation blockchain technology. Another advantage of second-generation blockchain technology is that it acts more like a digital ecosystem instead of a system only for transactions.

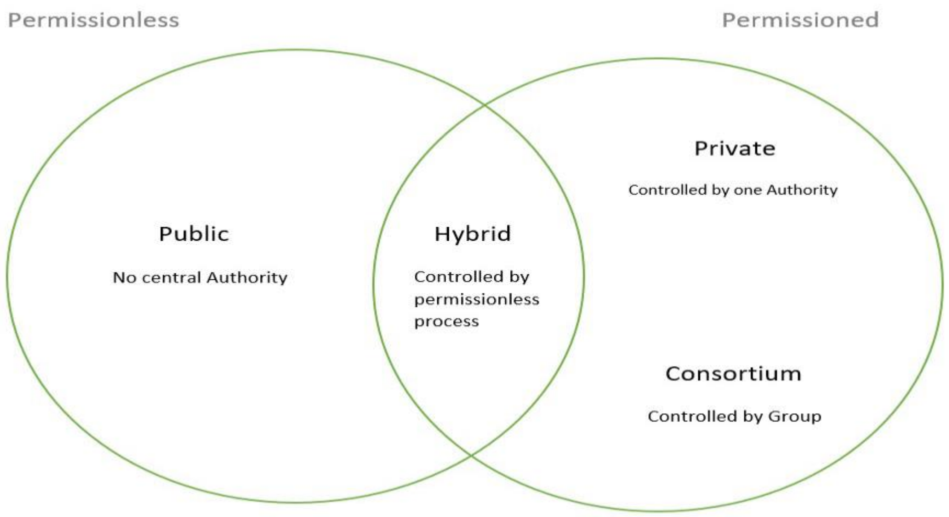
Here we get an impressive variety of functional uses including decentralized finance (DeFi),gaming, supply chain management, web browsing etc.

Third-generation blockchain: Cardano/ Polkadot /Ethereum 2.0

Even though Bitcoin and Ethereum are successful in their own ways, they will run into some issues in the future. As crypto is more readily adopted, the issue of scalability in blockchains becomes more prevalent. When too many people make transactions at a given time, fees can skyrocket and transactions take longer. With third-generation blockchains like Cardano and Polkadot, they automatically scale with demand, leading to lower fees overall. Another issue that third-generation blockchains solve is interoperability, or the sharing of data across different blockchains. While this is still being worked on, the idea is that multiple blockchains will be able to interact with each other.

Types of blockchain

There are four different major types of blockchain namely, public blockchain, private blockchain, hybrid blockchain, consortium or federated blockchain.



Public blockchain:
These blockchains are completely open to following the idea of decentralization. They don't have any restrictions, anyone having a computer and internet can participate in the network.

- As the name is public this blockchain is open to the public, which means it is not owned by anyone.
- Anyone having internet and a computer with good hardware can participate in this public blockchain.
- All the computer in the network hold the copy of other nodes or block present in the network
- In this public blockchain, we can also perform verification of transactions or records.

Advantage of public blockchain
1.Public blockchains are good, however anyone can join the public blockchain.
2.It brings trust among the whole community of users.
3.Public blockchain requires no intermediaries to work.
4.Public blockchains are brings transparency to the whole network as the available data is available for verification purposes.

Disadvantage of public blockchain

1.Public blockchain go through from a lack of transaction speed.
2.public blockchain is less scalability.
Use cases.
The most common use case for public blockchains is mining and exchanging cryptocurrencies like Bitcoin. However, it can also be used for creating a fixed record with an auditable chain of custody, such as electronic notarization of affidavits and public records of property ownership.
This type of blockchain is ideal for organizations that are built on transparency and trust, such as social support groups or non-governmental organizations. Because of the public nature of the network, private businesses will likely want to steer clear.

Private Blockchain

These blockchains are not as decentralized as the public blockchain only selected nodes can participate in the process, making it more secure than the others.

- These are not as open as a public blockchain.
- They are open to some authorized users only.
- These blockchains are operated in a closed network.
- In this few people are allowed to participate in a network within a company/organization.
- Private blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership etc.

Advantages of Private blockchain

▯The rate of the transaction is high, due to its small size. Verification of each node is less time-consuming.

▯We can modify the scalability. The size of the network can be decided manually.

Disadvantage of private blockchain

1. Trust building is one of the main disadvantages due to its central nature. Organizations can use this for malpractices.
2. Since there are few nodes if nodes go offline the entire system of blockchain can be endangered.

Use Cases: With proper security and maintenance, this blockchain is a great asset to secure information without exposing it to the public eye. Therefore companies use them for internal auditing, voting, and asset management. An example of private blockchains is Hyperledger, Corda.

Consortium blockchain

A consortium blockchain is a semi decentralized type where more than one organization manages a Blockchain network.

This is opposite to private blockchain where in which that is managed by only a single organization but in consortium blockchain, more than one organization and banks etc. It is also known as Federated Blockchain.

Consortium blockchain are typically used by government organizations and banks etc..

Advantage of consortium blockchain

1.Consortium blockchains are more secure and have better scalability

2.Consortium offers better customizability and control over resources.

3.It is also more efficient compared to public blockchain networks.

Disadvantage of consortium blockchain

1.Consortium blockchain is less transparent.

2.Regulations and restrictions can have a more impact on network functionality.

Use Cases: It has high potential in businesses, banks, and other payment processors. Food tracking of the organizations frequently collaborates with their sectors making it a federated solution ideal for their use. Examples of consortium Blockchain are Tendermint and Multichain.

Hybrid Blockchain

It is the mixed content of the private and public blockchain, where some part is controlled by some organization and other makes are made visible as a public blockchain.

- It is a combination of both public and private blockchain.
- Permission-based and permission less systems are used.
- User access information via smart contracts

Hybrid blockchain architecture is entirely customizable. The hybrid blockchain members can decide who can participate in the blockchain or which transaction are made public.

Advantage of hybrid blockchain

1. Rules can be changed according to the user's needs.
2. works in a closed ecosystem without the need to make everything public.
3. hybrid offers good scalability compared to the public network.

Disadvantage of hybrid blockchain

1. Upgrading to the hybrid blockchain can be challenge.
2. not completely transparent.

Use Case: It provides a greater solution to the health care industry, government, real estate, and financial companies. It provides a remedy where data is to be accessed publicly but needs to be shielded privately. Examples of Hybrid Blockchain are Ripple network and XRP **token**

Benefits and Limitations of Blockchain

The benefits of blockchain technology are given below

1.Digital freedom and decentralization:

The entire blockchain network is a decentralized one as it gives every users its digital freedom.There is no central authority that controls all the other users in the network. Every node is independent in functioning.

2.Security :

Blockchain technology is highly secured.The security method in the blockchain is cryptography that ensures that hackers cannot change or tamper with the data records

3.Transparency and trust

As blockchains are shared and everyone can see what is on the blockchain, this allows the system to be transparent and as a result trust is established.

4.Highly secure

All transactions on a blockchain are cryptographically secured and provide integrity.

5.Faster Processing: Blockchain technology speed of the transaction increased to a very extent.

6. Low transaction cost : As there are no intermediaries in a transaction within the blockchain network, the transaction cost are also lowered.

7.Immutable Data : One cannot change a data record or information that is once stored or added as a block in the blockchain .the data in the blockchain is immutable that is no one can make changes in it and it gets a permanent place in the blockchain.

8.consensus-based: The blockchain concept is entirely consensus-based, that is for every transaction that takes place between nodes in a blockchain, a request for its verification is sent to all the other nodes.After all the nodes verify a transaction, it goes into the memory pool to make a new block.

Limitations of blockchain

1.Higher cost: the underlying cost of implementing blockchain technology is huge. The transaction cost is also high.
2.Scalability : It is one of the biggest drawbacks of blockchain technology as it cannot be scaled due to the fixed size of the block for storing information. The block size is 1 MB due to which it can hold only a couple of transactions on a single block.
3.Immutable: In blockchain one cannot make any modification/ updations to any of the records. The data once written in a block can not be removed or erased.
4.Private keys: To access the assets or the information stored by the user in the blockchain, they need private keys. If a user who forgets its private key in blockchain are eventually logged out of their wallet and no one can get it back .

5.Expertise Knowledge :Implementing and managing a blockchain project is hard. It requires knowledge from the business to go through the whole process.

6.Interoprabiliy: There are multiple types of blockchain networks which work differently, trying to solve the problem in their own unique way which leads to interoperability issues where these chains are not able to communicate effectively.

Challenges of blockchain

1**.Scalability:** Blockchains are having trouble effectively supporting a large number of users on the network. There is need to increase capacity of blockchain.
2.Public Perception: The biggest drawback in the way of the success of Blockchain is the perception it holds in the eyes of people. Firstly, people don't see it be a part of mainstream functioning. Secondly, most of the people believe that this technology will not last long. The feature like the lack of

governance, easy access to become a member of public Blockchain and lack of regulation further deteriorates the image of Blockchain in the eyes of people. All these factors contribute as challenges for the growth of this Technology.

3.Security: The blockchain maintains confidentiality to protect users from hackers and hence provides privacy. But the blockchain network can be used for illegal activities and trade purpose.

Users who make online transaction using blockchain are not given blockchain network and newer crypto currencies are prone to 51%attackers.

4.Cost: The blockchain technology does not come free. To validate transactions ,bitcoin uses the proof of work (PoW) system.

The bitcoin requires appreciable amount of computational power to validate transactions. This energy is far from free and costs money.

5.Privacy: The bitcoin blockchain is designed to be publicly visible. All the information pertaining to a transaction is available for anyone to view. While this feature may be important in some context it becomes a liability if distributed ledgers are to be used in sensitive environments for example government data or financial data.

Application /usage of blockchain

1.Banking: Blockchain distributed-ledger architecture has the potential to enhance security, speed and operational efficiency for banks in several business areas such as payments, asset management, loyalty and loans.

2.Cloud storage: Cloud storage allows for decentralised storage and for that reason are less prone to attacks which will cause systemic harm and extensive data loss.

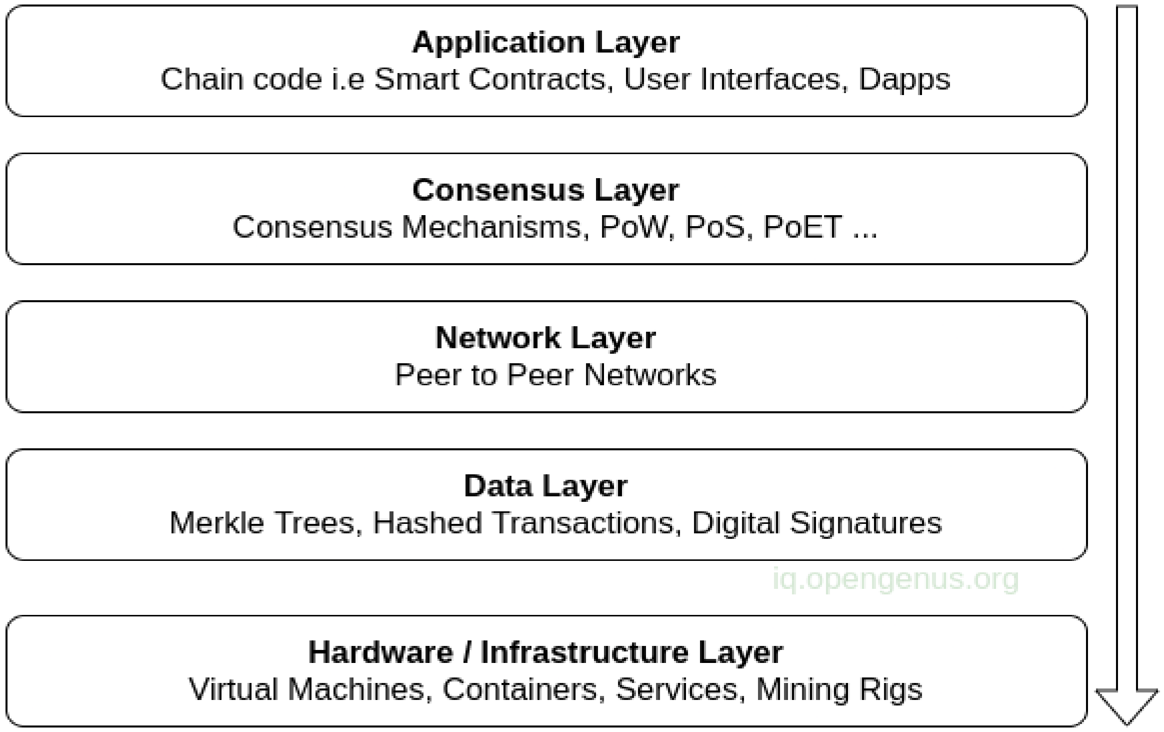
3.cryptocurrency: Blockchain technology acts as the backbone of cryptocurrency systems like bitcoin. Cryptography is an encrypted digital currency that everyone can use as a medium of exchange in transactions.

4.Healthcare: With the help of blockchaining, we can store information about patients and drugs in a database securely. Doctor can access patient records and history to analyze a case better at a given point to ensure proper treatment.

5.Supply Chain Management: with blockchain ,as products change hands in a supply chain from manufacturing to sales, transaction can be documented in a permanent decentralized register, which reduces delays, additional costs and human errors.

6. Smart contract: Smart contracts in blockchain are digital, self-executable contracts recorded and stored in a blockchain once created. A smart contract is a programmed file containing all the terms and conditions of a contract between two parties and it automatically executes itself once all the condition are met.

Layered Architecture of blockchain Ecosystem


Application Layer
Chain code i.e Smart Contracts, User Interfaces, Dapps
Consensus Layer
Consensus Mechanisms, PoW, PoS, PoET ...
Network Layer
Peer to Peer Networks
Data Layer
Merkle Trees, Hashed Transactions, Digital Signatures
iq.opengenus.org
Hardware / Infrastructure Layer
Virtual Machines, Containers, Services, Mining Rigs

1.Hardware or Infrastructure Layer

Blcokchain technology based on the peer to peer network of computers that computes transactions validates and stores them in an ordered form in a shared ledger. This results in a distributed database that records all the data, transactions and various relevant information. Blockchains are based on peer-to-peer information sharing. The network of computers which contribute to the computing power of the blockchain form the hardware layer

Computer in a peer to peer network is known as node. Nodes are accountable for validating transactions, organizing them in to blocks, broadcasting them to the blockchain network and it keeps on.

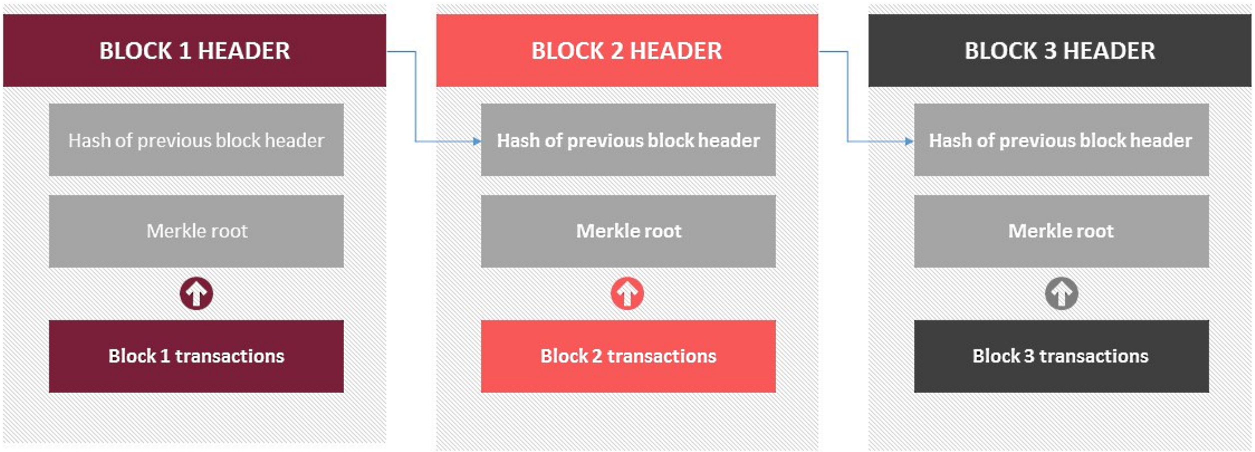
Reaching agreement the nodes commit the block to the blockchain network and update their local ledger copy. When device gets connected to a blockchain network then it is used as node.

2. Data Layer:

The next layer after the hardware layer is the data layer where details of transactions are stored. The transaction stored on a block (the fundamental unit of a blockchain) has details of the crypto sent, the public key of the receiver and the private key of the sender. Each block which has data is connected to the previous block and the next block which is generated. Only the genesis block, the first block of the network, is connected forwards and not backward.

Within each block, there is another data structure referred to as the *Merkle tree* which is a binary tree of hashes. Each block has a root hash which is a combination of all transaction hashes in the block.

The Merkle tree is what prevents transactions from being mutated because if they are the hash changes. Hashing produces a fixed-length string that is unique for any input meaning if even a single character in a transaction changes, the hash is bound to change making the transaction invalid. If the transaction is invalid, so is the block. If a block is invalid it is rejected by other nodes and it is not part of the chain.



3.Network Layer

The network layer also known as a peer-to-peer layer .It is responsible for inter-node communication and also called propagation layer.

Network layer takes care of block propagation, transactions and discover. Network layer ensures that nodes can reveal each other and able to communicate synchronize and propagate with each other to maintain valid current state of the blockchain network.

There are two kinds of node i.e. full node and light node. Full nodes guarantee that validation and verification of transaction , enforcement of consensus rules and mining whereas light nodes only keep the header of the blockchain and can send transaction.

4.consensus layer:

Consensus layer is essential to the existence of blockchain platforms.

Consensus layer is responsible for validating the blocks, ordering the blocks and ensuring everyone agrees on it.

Consensus layer create a definite set of agreements between nodes across the distributed peer to peer network.

Consensus layer ensures that power remains distributed and decentralized.

5.Application Layer

Application layer is divided into two sublayer i.e application layer and execution layer. Application layer comprise of the application that are used by end users to interact with the blockchain network. E.g smart contracts, chain code and dApps etc for these applications blockchain network is the backend and they connect via APIs.

Execution layer is the sublayer which consist of chaincode ,smart contracts and underlying rules.

Application send instructions to execution layer which ensure the deterministic nature of the block chain and performs the execution of transactions.

Components of blockchain

The main components of any blockchain ecosystem are given below.

Node Application

Node Application specify that every computer ,connected to the internet, if its wants to participate in. Node application not free from any restriction for example in case of Bankchain as a block ecosystem only banks are allowed to participate.

Distributed /shared Ledger(Database)

The distributed ledger means the shared databases and contents accessible to the participants of a particular blockchain ecosystem.

The shared ledger lists down the rules or guidelines that need to be followed ,for example if we are running a bitcoin node application, then we have to follow by all the rules set down in the program code of the bitcoin node application.

3.Consensus Algorithm

The consensus algorithm provides stability and security to the data in the blockchain. It is represent the status of the network and how the nodes in the network arrive at an agreement regarding what transactions to accept.

Also what protection used the blockchain from tampering is the fact that changing block can be done only by making a new block from its predecessor and it also requires regenerating all successors and redoing their contents.

It is to be noted that every block in the blockchain contains a hash of its predecessor block thus having a chain of blocks with enormous amount work contained them.

Core components of blockchain architecture:

1.Transactions is the smallest building block of a blockchain system (recodes ,information ec)that serves as the purpose of the blockchain.

2. Block is a data structure used for keeping a set of transactions which is distributed to all nodes in the network.

3.Chain is a sequence of blocks in a specific order.

4.Node is a user or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)

5.Consensus is a set of rules and arrangements to carry out blockchain operations.

6.Miners are the specific nodes which perform the block verification process before adding anything to the blockchain structure**.**

Cryptography

Cryptography in Blockchain is a type of internet security that is used to provide security and helps users maintain data on the web providing credibility and data security. Cryptography technologies make use of mathematical codes for storing and transmitting data values in a more secure format. To clearly understand the application of cryptography in blockchain.

- **Encryption** is the process of encrypting the plaintext so that the cipher text can be produced plaintext is transformed into cipher text using the encryption algorithm .
- **Decryption** is the reverse of the encryption process. In this the cipher text is converted back to the plaintext (original) using a decryption algorithm.
- **Key:** A key is usually a number or set of numbers on which the cipher oprates. Encryption and Decryption algorithms make use of a key to encrypt to decrypt messages respectively.
- **Cipher:** The mathematical function, i.e. a cryptographic algorithm which is used to convert plaintext to ciphertext(Random sequence of bits).

Objectives and Goals of cryptography in blockchain

1.Data Confidentiality assures that private or confidential information is not made available to unauthorized users.

2. Data integrity assures that information and programs are changed only in a specified and authorized manner.

3.Availability ensuring timely and reliable access to and use of information

4. **Authentication** ensures to the receiver that the data received has been sent only by an identified and verified sender.

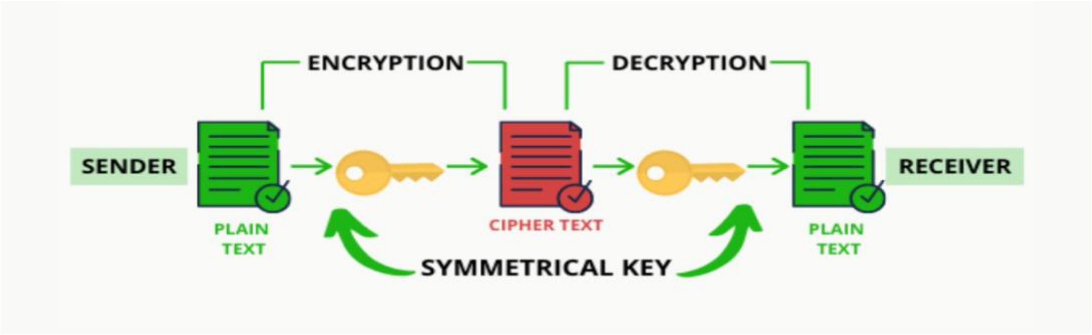
Types of Cryptography

The two types of cryptography are:

- **Symmetric-key cryptography.**
- **Asymmetric-key cryptography.**

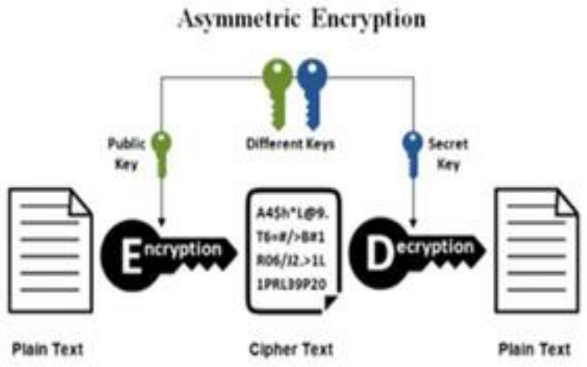
1. **Symmetric key Cryptography:** Symmetric cryptography is a simple form of cryptography which uses a single key to encrypt and decrypt data. This key can be anything ranging from a number to a word to a random string of characters . This key is then used to encypt the data after which the data can get sent across a network safely.

   To decrypt the data the receiver needs the key(the same one that the sender used to encrypt the data)



2. **Asymmetric key Cryptography (public key cryptography).**
   Blockchains are mainly use asymmetric cryptography, also known as public key cryptography. Public key cryptography uses the keys in pair, public and private key. Asymmetric cryptography uses these key- pairs in order to encrypt and decrypt data.

   The public key is for encryption that can be distributed commonly, but the private key is not share with anyone. Public key cryptography is mostly used between two users or two servers in a secure way.



What is AES?

It stands for Advanced Encryption Standard, developed in 2001. As triple-DES was found to be slow, AES was created and is six times faster than the triple DES. It is one of the most widely used symmetric block cipher algorithm used nowadays. It works on bytes rather than bits.

What is DES?

It stands for Data Encryption Standard, developed in 1977. It is a multi-round cipher that divides the full text into 2 parts and then work on each part individually. It includes various functionality such as Expansion, Permutation, and Substitution, XOR operation with a round key.

AES and DES are both examples of symmetric block ciphers but have certain dissimilarities.

	AES	**DES**
1.	AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
2.	The date of creation is 2001.	The date of creation is 1977.
3.	Byte-Oriented.	Bit-Oriented.
4.	Key length can be 128-bits, 192-bits, and 256-bits.	The key length is 56 bits in DES.
5.	Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	DES involves 16 rounds of identical operations
6.	AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
7.	AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.

	AES	**DES**
8.	It can generate Ciphertext of 128, 192, 256 bits.	It generates Ciphertext of 64 bits.
9.	It is faster than DES.	It is slower than AES.
10.	It is flexible.	It is not flexible.
11.	It is efficient with both hardware and software.	It is efficient only with hardware.

Hashing

A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length. The fixed bit length can vary (like 32-bit or 64-bit or 128-bit or 256-bit) depending on the hash function which is being used. The fixed-length output is called a hash. This hash is also the cryptographic by product of a hash algorithm. The following properties of cryptographic hashing makes the blockchain data structure functionally powerful.

Bitcoin uses SHA- 256 hash function that produces a hash of size 256 bits(32 bytes).

The following properties of cryptographic hashing makes the blockchain data structure functionally powerful:

1.Collision free :It is impossible to find two input texts input texts that produces the same has value.

2.Easy to Generate : It is easy to generate a hash value for a particular input using hash function.

3.Irreversible: It is impossible to generate original text from the hash value.

4.Commitment: It is not feasible to modify the original text without resulting a change in hash value thus enabling data integrity.

Hash function has two main features

1.Pre-image Resistance: The hash function works in only one direction i.ewe cannot deduce the input from the output .Consequently for two sets of inputs even if the inputs only differ by the smallest detail, the outputs should be different and not resemble one another.

2. Collision Resistance: When a hash function produces the same or identical output for two different inputs this is called a collision.It is imperactive that collisions are avoided in order to guarantee data integrity.If two pices of data produce same hash then one can be interchanged with the other, leading to a breakdown of continuity.

Types of Cryptographic Hash Functions

1. Secure Hashing Algorithm(SHA-0, SHA-1, SHA-2, and SHA-3)
2. RACE Integrity Primitives Evaluation Message Digest (RIPEMD)
3. Message-Digest Algorithm**(** MD2, MD4, MD5, and MD6)

4. BLAKE2

Working of Hashing

When user sends message to another user over a network,a hash of intended message is generated and encrypted by using a hash function and is sent along with the message. The result of the hash is known as hash or digest .

When the message is received, the receiver decrypts the hash as well as the message . Then the receiver creates another hash from the message. If the two hashes (received and created) are identical when compared, then it can be said that a secured transmission has occurred and the message has been correctly received.

Digital Signature

Digital signature is a digital code which include with an electronically transmitted document with this digital code we can verify first of all whether the content of the document is authenticated or not.

Digital signatures are used in blockchain where the transactions are digitally signed by senders using their private key before broadcasting the transactions to the network. Digital signatures in blockchain use **public key cryptography** which is also known as **asymmetric cryptography**.

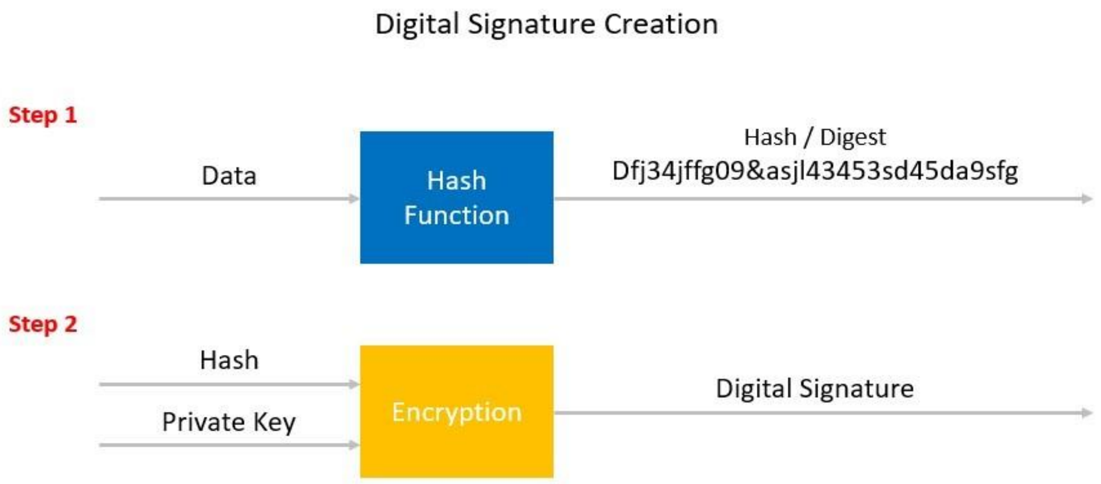
Digital signature, therefore, serves following purposes:

- The message has been created by a known sender. This is also known as **authentication**.
- The sender cannot deny having sent the message. This is known as **non-repudiation**.
- The messages has not been altered during transmission. This is **integrity**.

Digital Signatures Creation & Verification

Sarah that wants to create a digital signature for transmitting a transaction or a data. She needs public and private keys.

In the first step the transaction to be transmitted is hashed. Once the data is hashed, she uses her private key to encrypt the hash. This encrypted hash is the digital signature. This digital signature is embedded with the actual transaction and transmitted.

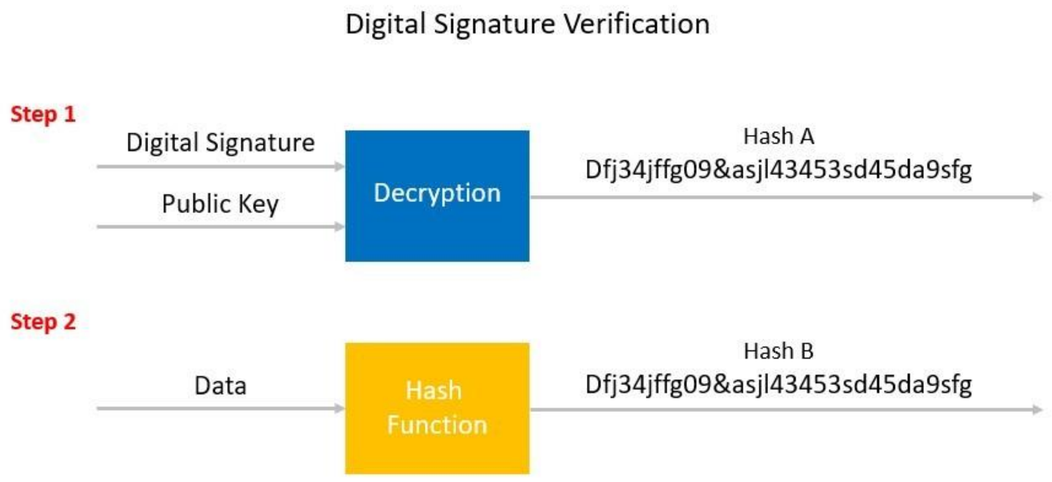


All network participants receive the digital message with digital signature including John.

John uses Sarah's public key to decrypt the digital signature. This generates the hash value of the document.

John applies the same hash algorithm on the received transaction as well. This result is the hash value of the received data.

John then compares both hash values. If the hash values match, its a proof that the data is not altered and that it is owned by Sarah.


Digital Signature Verification
Step 1
Digital Signature
Public Key
Decryption
Hash A
Dfj34jffg09&asjl43453sd45da9sfg
Step 2
Data
Hash Function
Hash B
Dfj34jffg09&asjl43453sd45da9sfg

Crptocurrency

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It’s a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets.

Cryptocurrency received its name because it uses encryption to verify transactions. This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers. The aim of encryption is to provide security and safety.

Digital currency Bitcoin

Bitcoin (BTC) is a cryptocurrency, a virtual currency designed to act as money and a form of payment outside the control of any one person, group, or entity, thus removing the need for third-party involvement in financial transactions. It is rewarded to blockchain miners for the work done to verify transactions and can be purchased on several exchanges.

Bitcoin was introduced to the public in 2009 by an anonymous developer or group of developers using the name Satoshi Nakamoto.

It has since become the most well-known cryptocurrency in the world. Its popularity has inspired the development of many other cryptocurrencies.

Digital Currency Ethereum

Blockchain technology is being used to create applications that go beyond just enabling a digital currency. Launched in July 2015 by Vitalik Buterin, Ethereum is the largest and most well-established, open-ended decentralized software platform.

Ether is the cryptocurrency generated by the Ethereum protocol as a reward to miners in a proof of work system for adding blocks to the blockchain. It is the only currency accepted in the payment of transaction of fees, which also go to miners.

Ethereum enables building and deploying smart contracts and decentralized applications (dApps) without downtime, fraud, control, or interference from a third party.

To accomplish this, Ethereum comes complete with its own programming language that runs on a blockchain.

Smart Contract

The smart contract executes on the ethereum blockchain decentralized platform and its terms and condition of an agreement are written in to code.

The agreements simply the exchange of shares, money, any asset or property.

There are two used programming languages for writing ethereum smart contract as a solidity and Serpent.

A smart contract is a set of lines of code that is uploaded and stored to check a contract’s validity and containing a set of rules under which the parties who share the smart contract agree to interact with each other.

It is automatically executed when previously determined and defined terms and conditions are met. The smart contract is defined and executed inside a distributed blockchain.

Benefits of smart contracts with blockchain

Trust: smart contracts automatically execute transactions following predetermined rules and the encrypted records of those transactions are shared across participants. Thus nobody has to question whether information has been altered for personal benefit.

Speed and Accuracy: smart contracts are digital and automated so you won't have to spend time processing paperwork or reconciling and correcting the errors that are often written in to documents that have been filled manually.

Savings: the cost is minimized by removing intermediaries.

Security: Blockchain transactions records are encrypted and that makes them very hard to hack. Protects data and transaction from fraud. It is impossible to change or update the data inside a block.

Application of smart contracts:
1.Insurance: Smart contracts can identify false claims and prevent forgeries**.**

2.Copy Righted Content: Smart contracts can protect ownership rights such as music or books.

3.Transportations: Shipment of goods can be easily tracked using smart contract.

4.Employment Contract: Smart contracts can be helpful to facilitate wage payments.

Blockchain Use Cases:

1. **Voting**
Blockchain technology has the ability to make the voting process more easily accessible while improving security. Hackers would be no match to blockchain technology, because even if someone were to access the terminal, they wouldn't be able to affect other nodes. Each vote would be attributed to one ID, and with the ability to create a fake ID being impossible, government officials could tally votes more efficiently and effectively.

2.**Supply Chain Management**
Blockchain's immutable ledger makes it well suited to tasks such as real-time tracking of goods as they move and change hands throughout the supply chain. Using a blockchain opens up several options for companies transporting these goods. Entries on a blockchain can be used to queue up events with a supply chain — allocating goods newly arrived at a port to different shipping containers,

3.Capital Markets

For capital markets, blockchain unlocks easier, cheaper, and faster access to capital. It reduces the barriers to issuance and enables peer-to-peer trading, faster and more transparent settlement and clearing, reduced costs, decreased counterparty risks, and streamlined auditing and compliance.

4. **Healthcare and the Life Sciences**

Blockchain-based healthcare solutions will enable faster, more efficient, and more secure medical data management and medical supply tracking. This could significantly improve patient care, facilitate the advancement to medical discoveries, and ensure the authenticity of drugs circulating global markets.

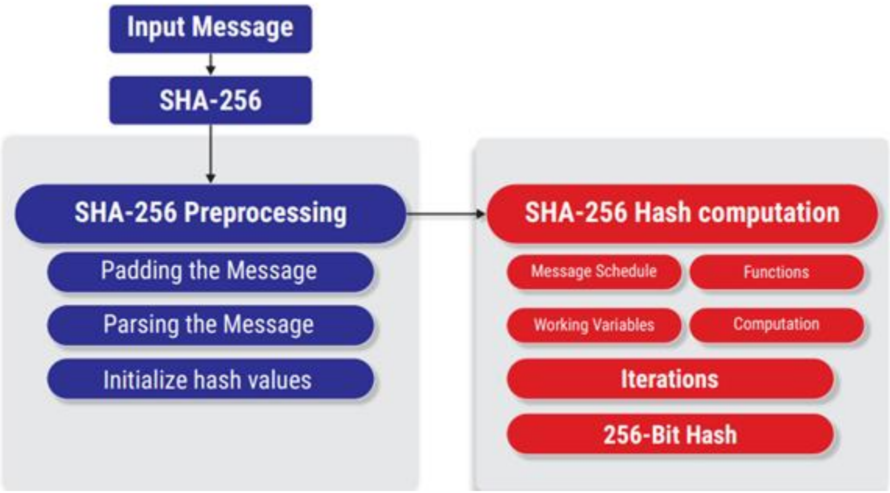
5. Real Estate

Enterprise Ethereum enables the digitization of assets and financial instruments. This enhances fractionalization of ownership, expanded access to global markets, increased liquidity, and democratized access to real estate investment opportunities.

Understanding of SHA 256

SHA-256 is a cryptographic hash function that belongs to the SHA-2 (Secure Hash Algorithm 2) family. It was developed by the National Security Agency (NSA) in the United States and is widely used in various applications, particularly in blockchain technology. SHA-256 is designed to take an input of any length and produce a fixed-size 256-bit output, regardless of the input size.

SHA-256 plays a critical role in ensuring the security and immutability of blockchain networks, particularly in proof-of-work (PoW) consensus algorithms. Here's how SHA-256 contributes to blockchain security.



The SHA 256 starts by converting the message to a binary number and get length 1.

The objective of this padding is to prepare the message before the hash computation begins. The padding ensures that the padded message is a multiple 512 bits.

Now we are going to parse the padded message.After the message padding,we now need to parse the message in to 512 bit blocks before the hash computation can begin.

To parse , we will take each set of 8 bits and convert the elements i.e each 4 set of 8 bits into hexadecimal values.

The hashing algorithm will then perform the necessary computations that include the iterations to create the hash. We now feed the initialize hash values that we have prepared before into the algorithms.

For the hash function computation, the algorithm will grab the message that was divided into chunks and put it through 64 rounds of operations. The output obtained in each round is fed as an input of the next computation round.

we can see the 64 rounds of operations that will be performed in the 512-bit message. Once that all the iterations are completed, we can complete the hashing process.

Immutable Ledger

A ledger in blockchain is a digital record-keeping system that contains a history of all transactions that have taken place on the blockchain. The ledger is maintained by a network of nodes and is updated in real-time as transactions occur. Each transaction is verified and recorded by the nodes, and once recorded, the transactions are immutable, meaning that they cannot be altered or deleted.

This ensures that the record of transactions remains unchanged, creating a secure and permanent history of all actions in the network. Blockchain technology is built on the principles of security, transparency, and decentralization, and immutability plays a key role in achieving these objectives. It ensures that once a transaction is recorded, it cannot be tampered with, preserving the integrity of the data and the trust in the network.

Immutable ledger resides in the concept of the hash. If hacker tries to alter anything in the block its hash will change.

Now the hash will no long match the previous hash in the second block. So, the hacker would have to change the next block and the block after that etc.ven if they were able to pull that off the blockchain belongs to multiple computers.

The hacker would need to make all of these changes simultaneously.

Blockchain is a distributed immutable ledger that is encrypted.It is immutable for two reasons: timestamp and the encryption of preceding content.

Distributed P2P Network

Peer to Peer(P2P) network is a decentralized network consists of a group of device(nodes) that collectively store and share files where each node acts as an individual peer. The peer to peer architecture of blockchain allows all crypto currencies to be transferred worldwide, without the need of any middleman or intermediaries or central server.

With the distributed peer to peer network, anyone who wishes to participate in the process of verifying and validating blocks can set up a bitcoin node.

In P2P communication is done without any central administration or server,which means all nodes have equal power and perform the same task.

Advantages of P2P Network

- **Easy to maintain:** The network is easy to maintain because each node is independent of the other.
- **Less costly:** Since each node acts as a server, therefore the cost of the central server is saved. Thus, there is no need to buy an expensive server.
- **No network manager:** In a P2P network since each node manages his or her own computer, thus there is no need for a network manager.
- **Adding nodes is easy:** Adding, deleting, and repairing nodes in this network is easy.

Disadvantages of P2P Network

- **Data is vulnerable:** Because of no central server, data is always vulnerable to getting lost because of no backup.
- **Less secure:** It becomes difficult to secure the complete network because each node is independent.

How mining works?

Blockchain mining is used to secure and verify bitcoin transactions .Mining is the process by which new bitcoin is added to the money supply. The process by which new coin generation is called mining.Bitcoin mining is the process of creating new bitcoin by solving a computational puzzle.

Miners receive two types of rewards for mining that is new coins created with each new block, and transaction fees from all the transactions included in the block.

Working of Mining:

Blockchain mining is a process used to validate new transaction. Mining is an essential activity in the blockchain network.

It is the way the peer-to-peer network verifies transactions and reaches common consensus without requiring a central authority.

The mining process starts when miners are trying to validate new transaction and record them on the blockchain.

The miners are competing to solve a difficult mathematical puzzle based on a cryptographic hash algorithm.

The solution found is called PoW .When a block is solved, all the transactions contained in the candidate block are considered validated, and the new block is confirmed .

This new block will be appended to the blockchain. The time taken to confirm a new block is approximately 10 minutes for bitcoin,but for other coins it is much faster. So, if we send or receive bitcoins, it will take approximately 10 minutes for the transactions to be confirmed. Miners receive a reward when they solve the complex mathematical problem. There are two types of rewards namely new bitcoins and transaction fees.

If we consider a block to mine first we need to collect the new transactions in to a block and then we hash the block to form a 256 bit block hash value.

When the hash initiates, the block has been successfully mined and is directed to the bitcoin blockchain network and has turned in to the identifier for the block.

In many cases the hash is not suceesful,so we need to alter the block to some extent and try again and again.

Nonce

- A nonce refers to a number or value that can only be used once. Nonces are often used on authentication protocols and cryptographic hash functions.
- In the context of blockchain technology, a nonce refers to a pseudo-random number that is utilized as a counter during the process of mining.

- Nonce is a 32-bit(4byte) random number which can be used one time. Nonce is often used on cryptographic hash functions and authentication protocols.
- The nonce in a bitcoin block is a 32-bit field whose value is adjusted by miners so that the hash of the block will be less than or equal to the current target of the network.

- In the miners test and discard millions of nonce per second until they find that golden nonce which is valid. Once, the golden nonce is found, they can complete the block and add it to the blockchain and there by receive the block reward.
- In cryptography, nonce is a random number that can be used just once in a cryptographic communication. There will be some constant information, timestamp, hash values with difficulty and the nonce which when passed through hash algorithm, SHA-256 will become a new block therefore nonce plays important role.

Cryptographic puzzle

- To mine Bitcoins and append transactions to the blockchain, miners solve a cryptographic puzzle.

- In a cryptographic puzzle, miners generate the hash of a newly created block along with cryptographic nonce.

- The nonce is varied until the hash value becomes smaller than equal to the target value. Adding new blocks to the blockchain (called mining) requires solving a moderately difficult cryptographic puzzle. This feature prevents malicious attack in blockchain.

- To complete each other, miners will create puzzle and who solves the puzzle first is able to add the block of the transaction to the blockchain.

- The process of solving the cryptographic puzzle is referred to as Proof of work is necessary in order to build consensus among miners in the blockchain.

- In PoW the miner with computational resources has better chance to solve the cryptographic puzzle.

Byzantine Fault tolerance

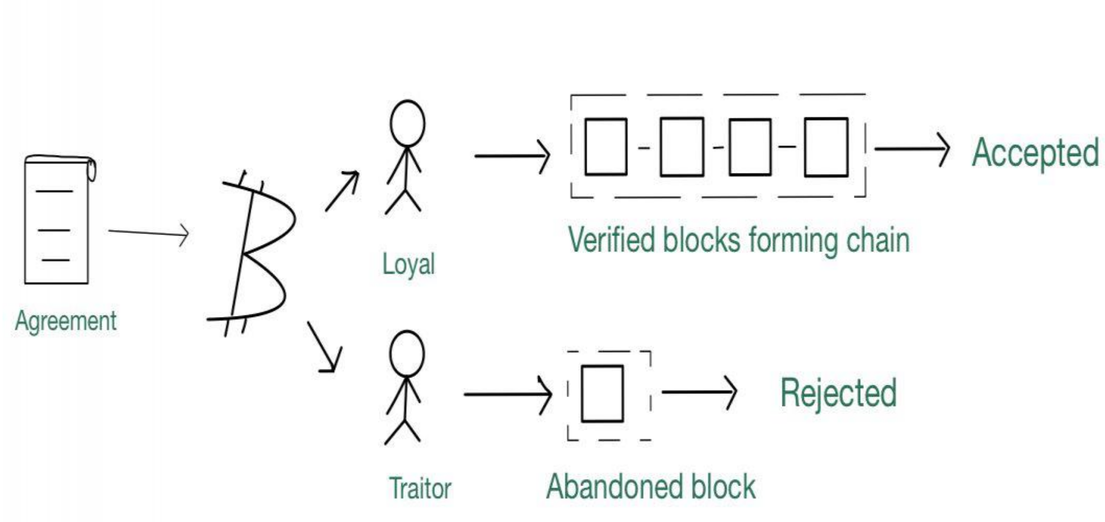
Byzantine Fault Tolerance (BFT) is the feature of a distributed network to reach consensus (agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information. The objective of a BFT mechanism is to safeguard against the system failures by employing collective decision making (both – correct and faulty nodes) which aims to reduce to influence of the faulty nodes. BFT is derived from Byzantine Generals' Problem.

Byzantine Generals' Problem

Byzantine fault tolerance can be achieved if the correctly working nodes in the network reach an agreement on their values. There can be a default vote value given to missing messages i.e., we can assume that the message from a particular node is 'faulty' if the message is not received within a certain time limit. Furthermore, we can also assign a default response if the majority of nodes respond with a correct value.
In other, a minimum of 3f+1 nodes needs to work, where f is the number of fault replicas.BFT based blockchain can tolerate atmost 30% of total nodes are malicious nodes.

Bezyantine fault tolerance is a measure of the network's ability to defend against failures that make it more difficult to achieve a consensus. Some examples of possible Bezyntine problem are:

1.Hardware components crashing or breaking.
2. Network congestion and disconnection.
3.Requests are processed in correctly.
4.Local states(the system states of one of the actors) are corrupted
5.Producing incorrect or inconsistent outputs.
6. Respond with incorrect result.
As long as two-thirds of the nodes are safe, consistency of consensus can be ensured.



What BFT ensures that every node receives the same guaranteed data. This is why even faulty devices or malicious attacks are unable to breach the protocol.

Consensus Protocol

Consensus protocols form the backbone of blockchain by helping all the nodes in the network verify the transactions.
Blockchain functions work as in a decentralized manner and records large volume transactions in real-time so there are so many issues or complexity of what is the truth is.
The key is to get consensus one way or another ,or else malicious things like double spending attack can occur. To handle this consensus algorithm comes in**.**

Proof of Work(PoW)

Proof of Work consensus is the mechanism of choice for the majority of cryptocurrencies currently in circulation. The algorithm is used to verify the transaction and create a new block in the blockchain. In this algorithm, **minors** (a group of people) compete against each other to complete the transaction on the network. The process of competing against each other is called **mining**. As soon as miners successfully created a valid block, he gets **rewarded**. The most famous application of Proof of Work(PoW) is Bitcoin.
The main working principle of proof of work is a mathematical puzzle which can easily prove the solution.
The puzzle game involves all miners competing against each other to solve the challenges, and this challenge will take approximately 10 minutes to be completed. Every single miner starts trying to find the solution to that one nonce that will satisfy the hash for the block. At some specific point, one of those miners in the global community with higher speed and great hardware specification will solve the cryptography challenge and be the winner of the game. Now, the rest of the community will start verifying that block which is mined by the winner. If the nonce is correct, it will end up with the new block that will be added to the blockchain. This whole mining mechanism needs high energy consumption and a longer processing time.

Proof of Stake(PoS)

The PoS is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm.
PoS and PoW have similar objectives they have some fundamental differences and features especially during the validation of new blocks on the blockchain network.

The Proof of Stake consensus algorithm differs with the PoW mining consensus with a mechanism where blocks are validated based on the stake of the network participants.

Under proof-of-stake (POS), validators are chosen based on the number of staked coins they have.

Here,unlike running hash functions, validators stake resources primarily in the form of digital money or tokens.
The validator of every block is then randomly selected from the stakeholders based on the amount of computational power allocated.

Proof of Stake (PoS) system may execute the algorithm in different ways,in general, the blockchain is secured by a pseudo random election process that considers a nodes allocation and the allocation determining the commitment of the party to ensure the network.
The Ethereum blockchain which is the world's largest blockchain network in terms of developer activity has initiated to switch from PoW to PoS in an attempt to increase the network scalability and reduce excessive electicity wastage.