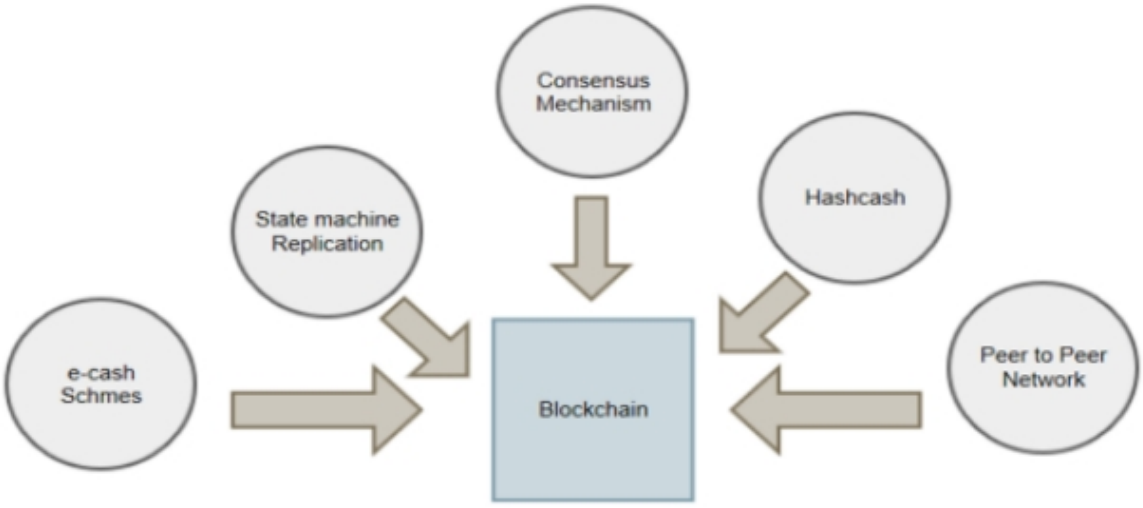
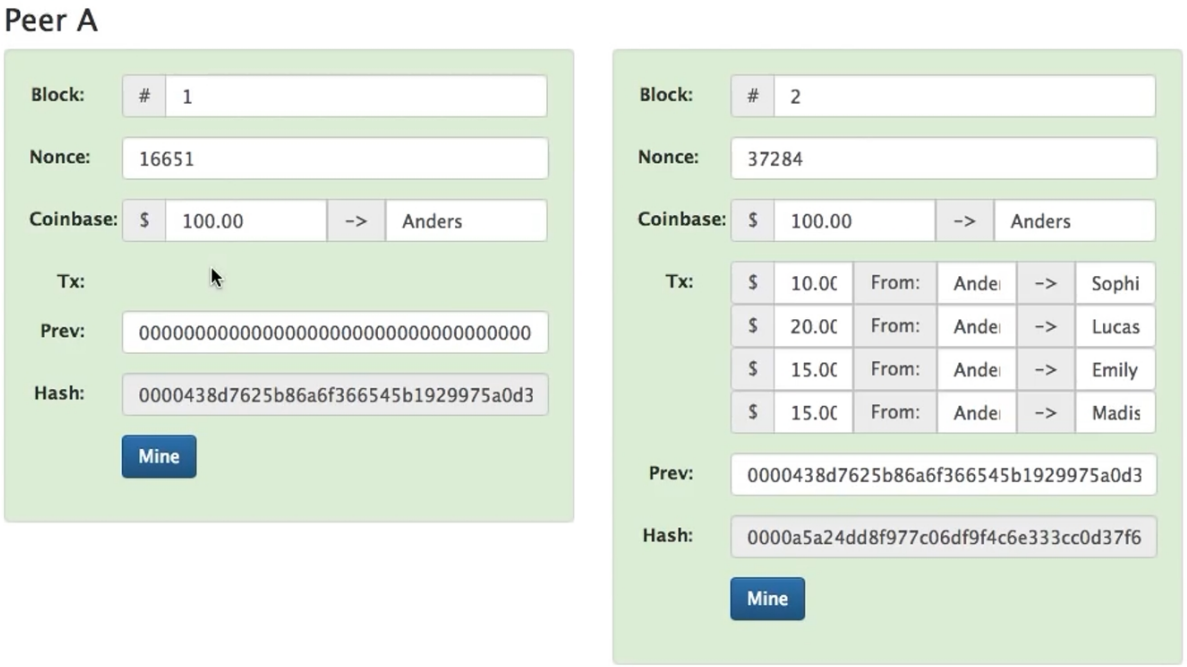
For clarifications Contact Ph: 09353205447, Email:bbaktech@gmail.com

Blockchain Technology

Introduction:

Blockchain technology is a type of technology that is tamperproof, clear, secure, and highly immutable. blockchain is a digital ever-growing list of data records. Such a list is comprised of many blocks of data, which are organized in chronological order and are linked and secured by cryptographic proofs





It is a database of record of transactions, which is distributed, and which is validated and maintained by a network of computers around the world. Instead of a single central authority such as a bank, the records are supervised by a large community and no individual person has control over it and no one can go back and change or erase a

transaction history. As compared to a conventional centralized database, the information cannot be manipulated due to blockchain's built in distributed nature of structure and confirmed guarantees by the peers.

blockchain is distributed among the Nodes. Blockchain allows anyone on the network to access everyone else's entries which makes it impossible for one central entity to gain control of the network. Whenever someone performs a transaction, it goes to the network and computer algorithms determine the authenticity of the transaction. Once the transaction is verified, this new transaction is linked with the previous transaction forming a chain of transactions. This chain is called the blockchain.

Blockchain technology is based on decentralized network meaning it operates as a peer-to-peer network.

Hashing Technics:

The SHA-256 algorithm generates an almost unique, fixed-size 256-bit (32-byte) hash. This is a one-way function, so the result cannot be decrypted back to the original value.

Currently, SHA-2 hashing is widely used, as it is considered the most secure hashing algorithm in the cryptographic arena.

SHA-3 is the latest secure hashing standard after SHA-2. Compared to SHA-2, SHA-3 provides a different approach to generate a unique one-way hash, and it can be much faster on some hardware implementations. Similar to SHA-256, SHA3-256 is the 256-bit fixed-length algorithm in SHA-3

NIST released SHA-3 in 2015, so there are not quite as many SHA-3 libraries as SHA-2 for the time being. It's not until JDK 9 that SHA-3 algorithms were available in the built-in default providers.

Digital Signature:

In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

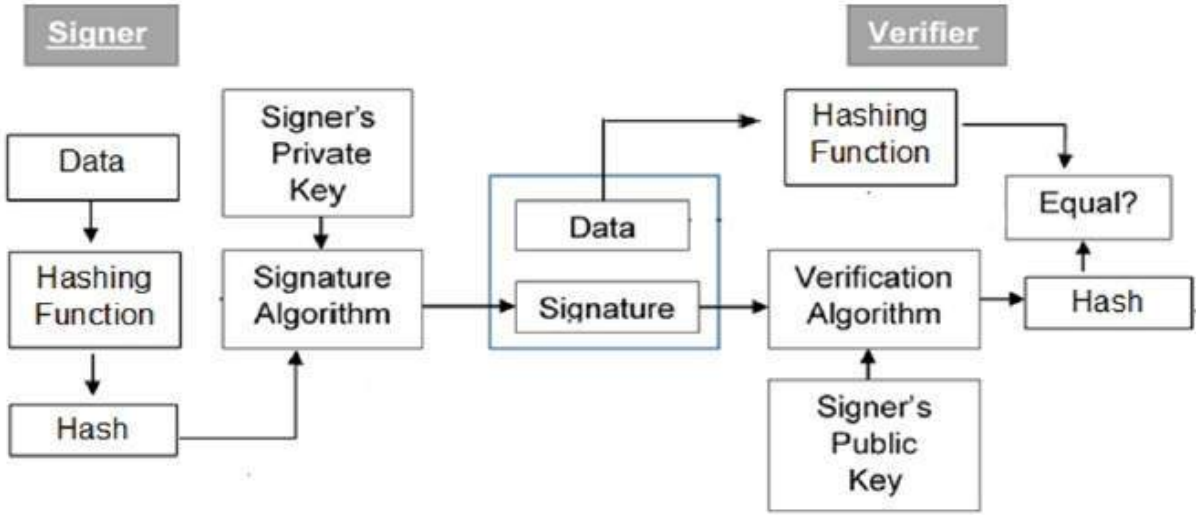
The Cryptography of a digital signature is possible with two key terms:

Private Key: The account holder holds a key which is a random hexadecimal number. Private Key will be confidential to the account holder rather than exposed to the real world.

Public Key: A random hexadecimal number that is shared publicly. To create a public cryptography digital signature, the message will be signed digitally first; then, it is encrypted with the sender's private key and with the public key of the receiver. To decrypt the messages shared between the sender and receiver, the receiver has to decrypt the inner layer of the information with the Public key of the sender and decrypt the information's outer layer using the private key the receiver holds.

Model of Digital Signature:

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration –



The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.

- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Advantages of digital signature:

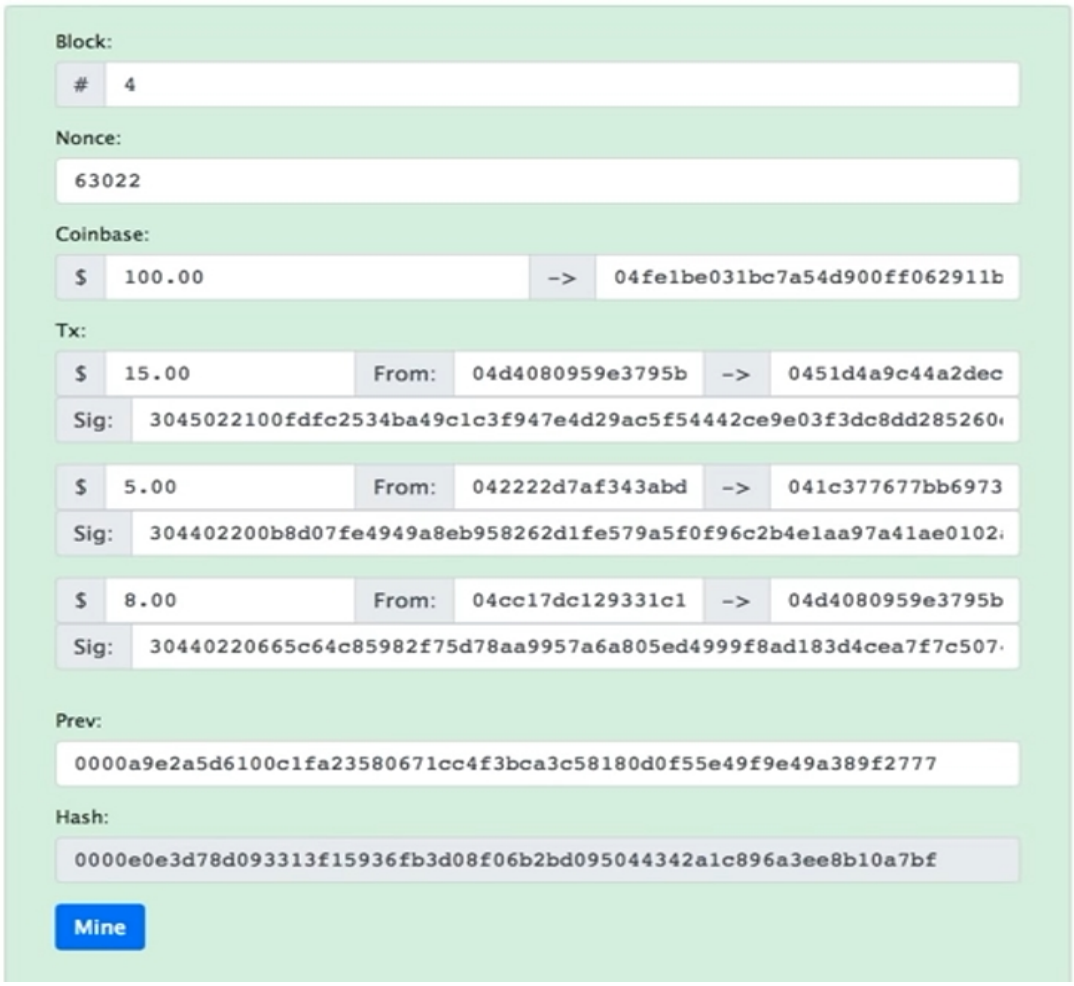
Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

Blockchain Components:

Each chain is based on three crucial components: blocks, nodes, and miners.

Blocks: Blocks are the clusters of data that act as the chain's links, and include two important numbers called nonces and hashes. Nonces are 32-bit whole numbers generated when a block is created, while hashes are 256-bit numbers linked to the nonce and used to identify that specific block's data (think of them as fingerprints). After a blockchain's first block (or "genesis block") is created, its nonce generates a hash, at which point the block is considered signed and permanently bound to the nonce and hash. This makes the block's data cryptographically secure.



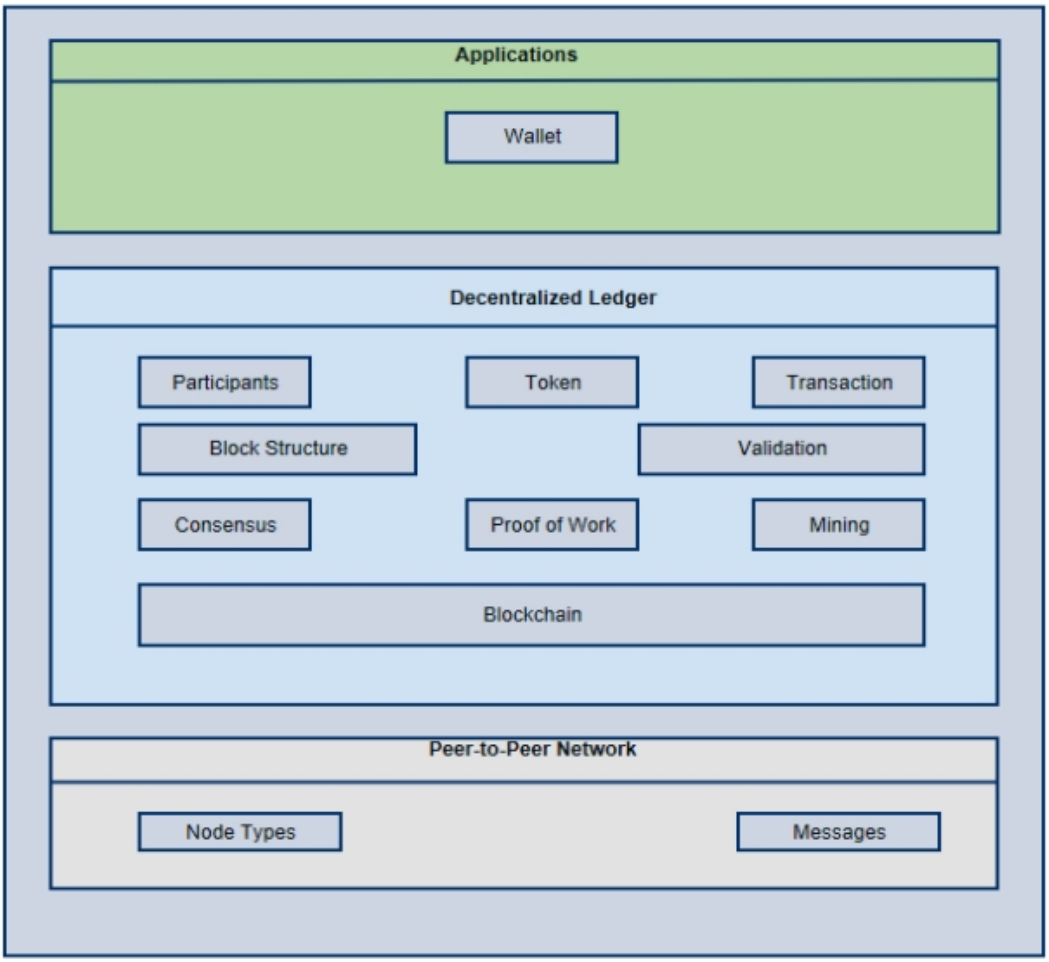
Nodes: Nodes are essentially devices that are capable of participating in a blockchain. When a new node joins a blockchain, it is given its own copy of the chain, and in order to make additions or changes to the chain as a whole, the node's actions must be algorithmically approved by the blockchain's network. For example, if one node creates a new block, that block is sent to everyone on the network, and the other nodes confirm that the block is viable and hasn't been tampered with. This communal agreement is known as "consensus," and it is the framework of a blockchain's impeccable security.

Miners: miners are responsible for changing (or "mining") a blockchain's data, creating new blocks by means of consensus. This is done by finding the right nonce-hash combination in a single block (also known as the "golden nonce"). Since each block has a unique nonce and hash linked to the hash of the previous block, there are billions of possible nonce-hash combinations that must be mined to successfully change the block; making mining a time-consuming process warranting high-level math skills and advanced analytical software. However, when a change is finally executed and accepted by the network, the miner is rewarded financially.

History:

Satoshi Nakamoto is considered as the inventor of blockchain technology when he published a paper on bitcoin in 2008 as “Bitcoin: A Peer-to-Peer Electronic Cash System,”. The abstract of the paper was on the direct online payment from one source to another source without relying on a third-party source. The paper described an electronic payment system based on the concept of cryptography. Nakamoto’s paper provided a solution to the double spending where a digital currency cannot be duplicated, and no one can spend it more than once. The paper stated the concept of public ledger where an electronic coin transaction history can be traced and confirmed if the coin has not been spent before and to prevent double spending issue.

Blockchain Architecture:



Blockchain technology works on the concept of decentralized database where these databases exist in multiple computers (Nodes) and every copy of these database are identical, due to decentralized structure of blockchain, it has made the blockchain as a temper proof technology. Blockchain can be considered as a peer-to-peer network that run on the top of the internet.

Blockchain architecture can be mainly divided in three layers which are Applications, Decentralized Ledger and Peer-to-Peer Network. Applications is the top layer pf the network which is followed by the Decentralized Ledger and the bottom layer is the Peer-to-Peer Network.

Application layer: contains the application software of the Blockchain. For example, Bitcoin wallet software creates and stores private and public keys enabling users to keep control over the unspent bitcoins. Application layer provides a human readable interface where users can keep track of their transactions.

Decentralized Ledger is the middle layer in a blockchain architecture that confirms a consistent and temper-proof global ledger. In this layer, transactions can be grouped into blocks which are cryptographically linked to one another.

Transactions can be defined as the exchange of tokens between two participants and every transaction goes through validation process before it is considered as a legitimate transaction.

Mining is the process of grouping transactions into a block that is added to the end of the current blockchain. consensus

Blockchain uses a proof-of-work(**consensus**) algorithm to decide the chain that has required the most cumulative effort to build and to assure among all the nodes to determine the blockchain's legit(legal). The bottom layer in the blockchain architecture is the **Peer-to-Peer Network** where Node types play different roles and various messages are exchanged to main the Decentralized Ledger.

Applications

It provides application interfaces on top of the blockchain and used for keeping the cryptocurrencies secure. This software can be installed on your computer or mobile devices or also can be hosted on a third-party platform.

Decentralized Ledger

A decentralized ledger is a shared and replicated database which is synchronized among the members (Node) of the network. It maintains the records of transactions among the participants in the network. The ledger is responsible for keeping records of transactions among the participants. Blockchain has a property of a database except the fact that it stores the information in the header and data is stored in the form of a token or a cryptocurrency. It is required to group the newly validated transactions into block as the first step of recording transactions in the ledger. Any participant in the blockchain can gather new transactions create blocks that can be appended to the blockchain.

A block mainly consists of transactions and the hash pointer, timestamps and the nonce.

Nodes perform various functions depending on its role in the blockchain network.

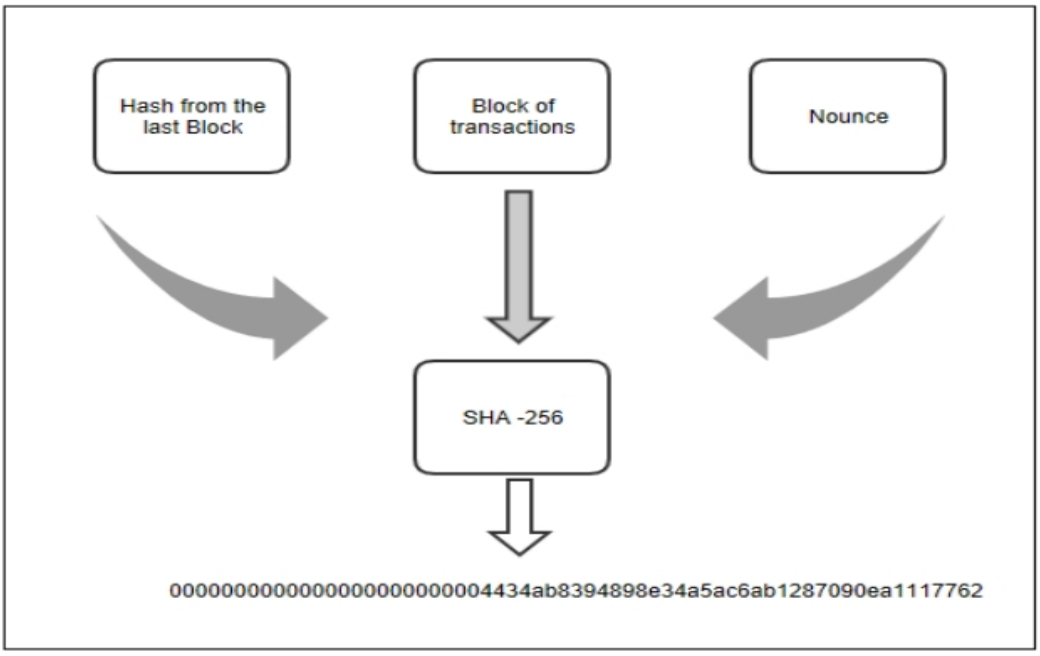
A node can be called a **miner** when it proposes and validates transactions and perform mining to provide consensus to secure the blockchain. It can perform functions such as simple payment verification etc., and functions depending on the blockchain used.

Proof of work is defined as a **consensus algorithm** that verifies the accuracy of data. For example, Bitcoin uses hashcash as a proof of work for bitcoin transactions.

Miners are required to complete a proof of work to verify the transactions in the block so that it can be accepted by the network. Proof of work ensures security and consensus in the blockchain network. During the verification, a block receives a hash (id). To verify the next block, this hash is added to the current block of transactions. In the next step, add a nonce-which is defined as a random number that can be used only once, to the end of next block. Hash function is used to change this random number to generate a string that contains number of zeros in front of it.

Proof of work is costly to maintain, and it can have future scalability and security issues as it always relies on the miners' incentives. There is an advanced solution called as "proof-of-stake," which is lucrative to enforce, and it identifies who gets to update the consensus and defers unwanted forking of the underlying blockchain.

No confidential information is transferred in a blockchain network and all the transactions are visible to every node in the network. This peer-to-peer network does not require any additional protection and can be built on any physical infrastructure.



It requires all nodes on the network to solve a cryptographic puzzle by applying the brute force formula. Take for example if the ethereum blockchain has a new transaction which are tentatively committed and they are based on POW output, a selected block created by the winning node is broadcasted to all the nodes, at specific synchronization interval. Once the block is transmitted using a peer to peer network to other nodes the same is included in the blockchain and any other tentative transaction

are rolled back (by rule of probability the consensus is achieved by 51% if power rather than 51% people count).

The reason for the proof of work concept is because compared to other algorithm it is considered secure as it makes it almost impossible for the concept to be attacked unless a miner acquires 51% of computing power which it is made impossible by the blockchain structure.

The main difference between proof of work and proof of stake is that **proof of stake relies on staking, while proof of work relies on mining**.

The main difference is that **proof-of-work requires burning an external resource (mining hardware) while proof of stake does not**. Proof-of-work criticizes that if price/Bitcoin rewards/fees drop then fewer people have incentives to mine. This is turn reduces the security of the system.

the goal of a consensus algorithm in a public blockchain network is to let many different users agree on the current state of the blockchain even though they don't trust each other or any central authority. This is a challenging problem, and until the launch of Bitcoin network, it had remained unsolved.

Proof-of-Work

Bitcoin's solution was to use something called Proof-of-Work aka PoW (or "mining," or "hashing"). Here participating users worked to solve difficult mathematical problems, and then published the solutions. It takes real-world resources like computers and electricity to find these answers. Therefore, there's no way to "cheat" and pretend that you represent a bigger portion of the mining power on the network than you actually do. As a result, PoW algorithms can use the number and difficulty of solutions being found to measure how much of the network agree on the current state of the blockchain.

The only way to prevent the legitimate users from agreeing to the situation of the blockchain is to control enough of the total computing power that you can pretend the group disagrees with itself. Also, even that your opinion is the real consensus, and all the other users are lying about the state of the blockchain. That requirement for resources is a good thing. This is because it means that interfering with the group's consensus takes a lot of resources (a.k.a. money).

Unfortunately, PoW consensus algorithms as we presently know them require a constant, ongoing expenditure of resources just to work normally. The work has to happen regardless of whether someone is trying to interfere or not. Also, someone has to pay for it. Most existing PoW Blockchains, such as Bitcoin, pay for these costs with the pre-agreed creation of coins. This is also known as inflation. This salary has to be ruled out.

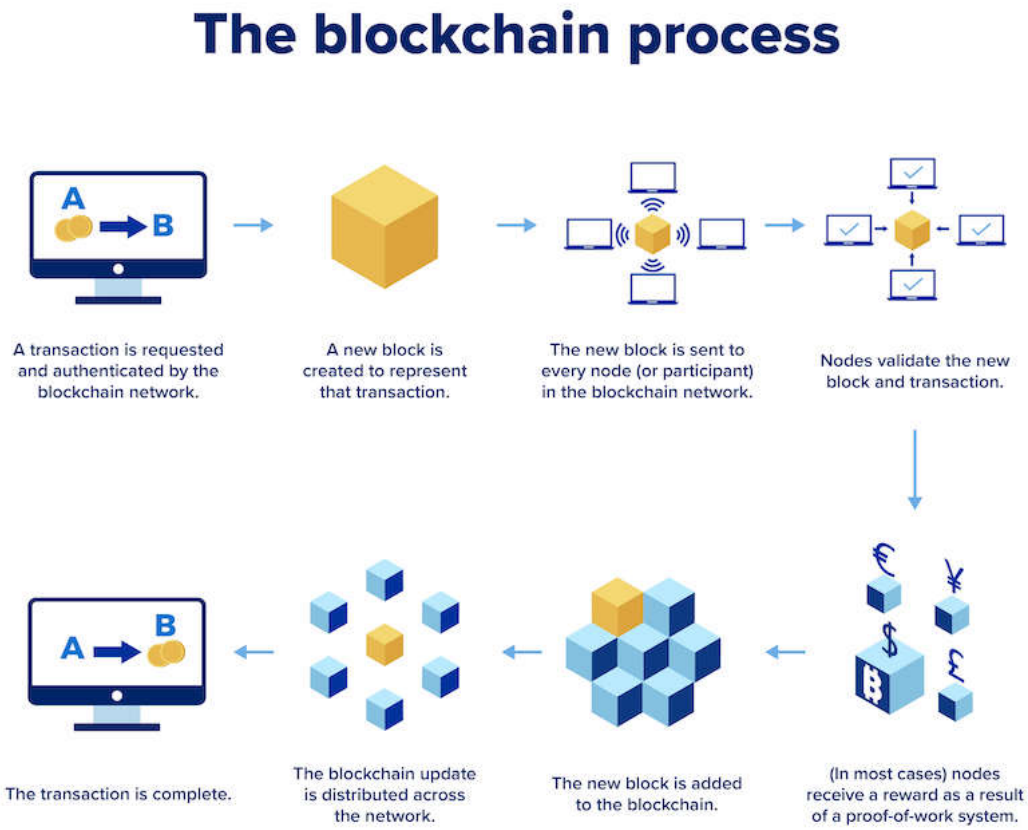
Proof-of-Stake

Proof of Stake (PoS) requires users that have a high stake at the currency (i.e. hold a lot of coins). This is to determine the next block. This has a high risk of some party

achieving monopoly of the currency. However, there are several methods to prevent that (by allocating random stakeholders to agree on a new block, and others).

Proof-of-Work vs. Proof-of-Stake

The main difference is that proof-of-work requires burning an external resource (mining hardware) while proof of stake does not. Proof-of-work criticizes that if price/Bitcoin rewards/fees drop then fewer people have incentives to mine. This is turn reduces the security of the system. Proof of stake states criticizes that since it is free to stake/add new blocks to the Blockchain, you could use it to stake several similar coins at the same time



Tiers of Blockchain:

Blockchain 1.0: This Blockchain is basically used for cryptocurrencies and it was introduced with the invention of bitcoin. All the alternative coins as well as bitcoin fall into this tier of blockchain. It also includes core applications as well.

Blockchain 2.0: Blockchain 2.0 is used in financial services and industries which includes financial assets, options, swamps and bonds etc. Smart Contracts was first

introduced in Blockchain 2.0 that can be defined as the way to verify if the products and services are sent by the supplier during a transaction process between two parties.

Blockchain 3.0: Blockchain 3.0 offers more security as compared to Blockchain 1.0 and 2.0 and it is highly scalable and adaptable and provides sustainability. It is used in various industries such as arts, health, justice, media and in many government institutions.

Generation X: This vision the concept of singularity where this blockchain service will be available for anyone. This blockchain will be open to all and would be operated by autonomous agents.

Types of Blockchain :

Blockchain has evolved greatly in the last few years and based on its different attributes, they can be divided in multiple types.

- **Public Blockchains:**Public blockchains are open to the public and any individual can involve in the decision-making process by becoming a node, but users may or may not be benefited for their involvement in the decision-making process. No one in the network has ownership of the ledgers and are publicly open to anyone participated in the network. The users in the blockchain use a distributed consensus mechanism to reach on a decision and maintain a copy of the ledger on their local nodes.
- **Private Blockchains:** These types of blockchains are not open to the public and are open to only a group of people or organizations and the ledger is shared to its participated members only.
- **Semi-private Blockchains:** In a semi-private blockchain, some part of the blockchain is private and controlled by a group or organizations and the rest is open to the public for anyone to participate.
- **Sidechains**: These blockchains are also known as pegged sidechains where coins can be moved from blockchain to another blockchain. There are two types of sidechains naming one-way pegged sidechain and two-way pegged sidechain. One-way pegged sidechain allows movement from one sidechain to another whereas two-way pegged sidechain allows movement on both sides of two sidechain.
- **Permissioned Ledger**: In this type of blockchain, the participants are known and already trusted. In permissioned ledger, an agreement protocol is used to maintain a shared version of the truth rather than a consensus mechanism.
- **Distributed Ledger**: In a distributed ledger blockchain, the ledger is distributed among all the participants in the blockchain and it can spread across multiple organizations. In distributed ledger, records are stored contiguously instead sorted block and they can be both private or public.
- **Shared Ledger**: Shared ledger can be an application or a database that is shared by public or an organization.

- **Fully Private of Proprietary Blockchains**: These types of Blockchains are not a part of any mainstream applications and differ the idea of decentralization. These type of blockchains come in handy when it is required to shared data within an organization and provide authenticity of the data. Government organizations use private of proprietary Blockchains to share data between various departments.
- **Tokenized Blockchains:** These are standard blockchains which generate cryptocurrencies through consensus process using mining or initial distribution.
- **Token less Blockchains:** These blockchains are not real blockchains as they do not have the ability to transfer values, but they can be useful when it is not required to transfer value between nodes and there is only the need to transfer data among already trusted parties.

Advantages of Blockchain :

- One of the biggest advantages of Blockchain is Dissemination which allows a database to be shared without a central body or entity. Because of the decentralized nature of the blockchain, it is almost impossible to temper the data as compared to conventional database.
- Users are empowered to control their information and transaction.
- Blockchains provide complete, consistent and up to date data without accuracy.
- Since blockchain does not have any central point of failure due to its decentralized network, it can withstand any security attack.
- As no central authority is required, users can be assured that a transaction will be executed as protocol commands.
- Blockchains provide transparency and immutability to the transactions as all the transactions cannot be altered or deleted.
- Blockchain's peer-to-peer connections help to identify fraud activities in the network and distributed consensus. It is almost impossible to invade a network as attacker can impact the network only when they get control of 51% of the nodes.
- By using blockchain, sensitive business data can be protected using end to end encryption.
- Users in a blockchain can easily trace the history of any transaction as all the transactions a blockchain are digitally stamped.
- Blockchain are resilient to cyber-attacks due to peer-to-peer nature and network would operate even when some of the nodes are offline or under security attack.
- Multiple copies of the data can be stored in the blockchain and hence users can avoid storing sensitive data in one place.
- Customers tend to trust more in the blockchain system due to its enhanced security.

Disadvantages of Blockchain :

- Blockchains are expensive and resource intensive as every node in the blockchain repeats a task to reach consensus.

- In blockchain, users verify a transaction based on certificate authentication, land titles, cryptocurrencies, etc. But there is no way to reverse a transaction even if both the parties involved in the transaction are ready to do so or if the transaction go sour due to some reason.
- A transaction in the blockchain is settled only when all the nodes in the blockchain successfully verifies the transaction. This could be a very slow process as the block inserted needs to be verified to mark the transaction as authentic by all the nodes. A new concept called as lightening network where transaction can be verified immediately could be good solution to this issue.
- The size of blockchain grows with an addition of a block. A node needs to store the entire history of the blockchain to be a participant in validating transactions, causing the blockchain to grow continuously. Blockchain will grow faster if it has large blocks and thereby would separate the miners and this would impact the health of the blockchain as the health is dependent on the number of nodes in the network.
- One of the disadvantage of blockchain is its complexity and complicacy to understand for a general human being. Blockchain is full of complex concepts and processes which is not yet refined so that common man can easily digest and consume the information on how to use it and hence it’s not yet ready for mainstream use.
- In blockchain, all the transaction related information is available publicly which can become a great liability when distributed ledgers are used in sensitive environments such as dealing with government data or patients medical data. The ledgers need to be altered and access should be limited with proper clearance only.