Block Chain Technology

▼ **Discuss why an organization might decide to implement a block chain solution?**

- Enhanced security,
- greater transparency,
- instant traceability,
- increased efficiency and speed
- automation.

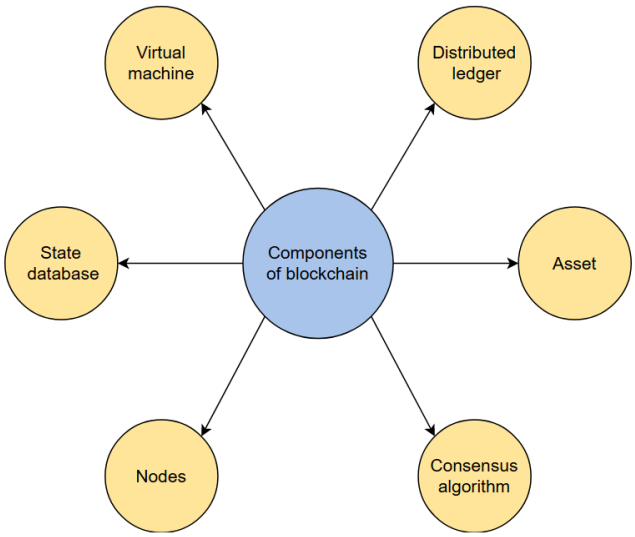
▼ **Describe four components of block chain technology**

▼ …

Blockchain technology has the following five core components that include but are not limited to the following.

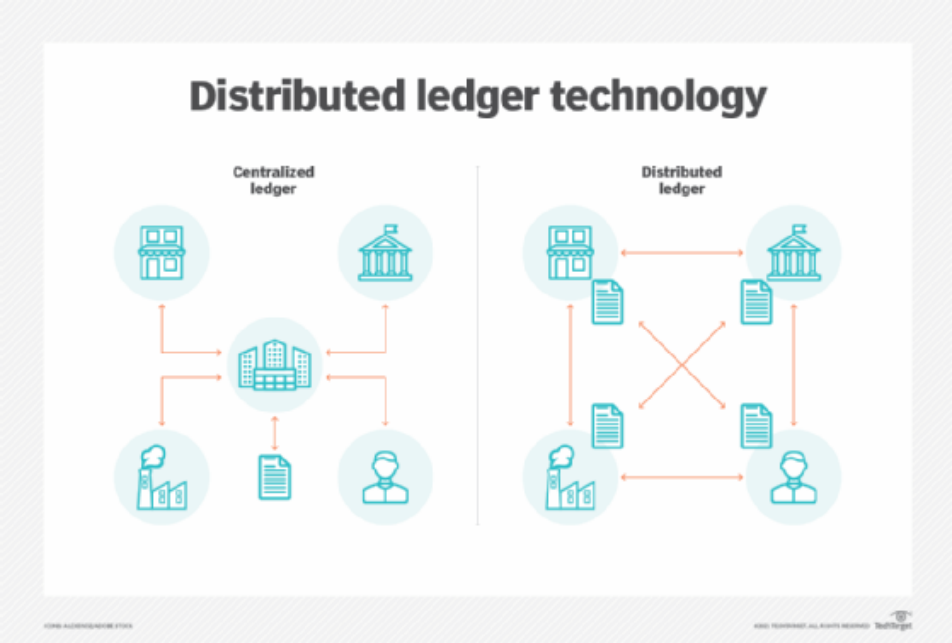
- First, every blockchain has a tamper-resistant ledger, which is where the transactions and other information that have occurred on the blockchain network are stored.
- Second, this information stored on the ledger is approved, before posting on the network itself, via some sort of consensus methodology that enables network members to jointly confirm that data are presented correctly.
- Third, any blockchain is defined by the encryption protocols used to safeguard information, with the most famous iteration being the SHA-256 encryption protocol used by the bitcoin blockchain.
- Fourth, the management of this entire process (i.e., the way in which data are confirmed and added to the network itself) is generally managed by full nodes, playing an important role in maintaining the integrity of the blockchain network.
- Fifth, every blockchain is in some way defined by the peer-to-peer (P2P) nature of transactions that underpin the entire blockchain ecosystem, which greatly reduces the need for intermediaries and other third-party organizations.

A blockchain network consists of nodes, a distributed ledger, an asset, and a consensus algorithm. Sometimes, it also includes a virtual machine and a state database.



The components of a blockchain

- **Nodes**
  - Nodes form the structure of the blockchain network. Nodes on the network are tasked with different responsibilities, such as a miner and a validator. Nodes are devices with computational power and a node application installed. Different blockchains have different node applications containing the data and the rules to act as nodes on the respective blockchain.
- **Distributed ledger**
  - The distributed ledger is also known as the database of the blockchain. Every node on the network has a copy of the ledger to provide fault tolerance to the network. A ledger is immutable and visible to everyone on the blockchain network. It is made up of sequentially linked blocks containing assets. Blocks are linked together using the previous block's hash.



- **Asset**
  - An asset can be virtually anything, either physical or non-physical, having a value recognized by the nodes in the network. Some examples of assets are as follows:
    - **Financial transactions:** Blockchains like Bitcoin and Dogecoin use a ledger to store the data of transactions of their cryptocurrencies.
    - **Code blocks:** Blockchains like Ethereum use it to store code in the form of smart contracts, which serves as the basis of the concept of Dapps.
    - **Medical records**: Private blockchains usually store patients' medical records to maintain integrity in an untrustworthy environment.
    - **Business transactions:** Businesses can use private blockchains while performing transactions involving other businesses to ensure the integrity of the product and that certain conditions are met, leading to more security and accountability.
- **Consensus algorithm**
  - A consensus algorithm is what makes blockchain a successful alternative for centralized applications. In the case of centralized applications, the central authority is trusted by all users to execute the transactions reliably. However, in the absence of a central authority, this responsibility falls upon the nodes in the network. Blockchains use consensus algorithms like Proof of Work (POW) and Proof of Stake (POS) to reach consensus in an untrustworthy environment. The consensus algorithm sends the transaction performed by the miner to the validator nodes to reach a consensus. If consensus is reached, the transaction is added to the ledger, or else it is discarded.
- **Virtual machine**
  - Blockchains like Ethereum run virtual machines on their nodes. They are used to execute code written in smart contracts. This is done to ensure that if the code being executed on the nodes contains malware, it will not affect the node executing the code.

Instead, it will just affect the virtual machine running on top of the actual hardware saving the node.

- **State Database**
  - It is a key-value database that represents the current state of the network. It is calculated by traversing the ledger. It is used to save time during transactions, as during every transaction, the updated state of the network is required, and the traversal of the whole ledger in every transaction will slow down the network.

▼ **Public Ledgers**

- A ledger is a record-keeping system: it tracks value as is moves around, so the viewer can always see exactly what value resides where at a given moment. Traditional finance systems like banks use ledgers to track all transactions completed within a period.
- A public ledger is
  - an open-access network; anyone can join at any time.
  - fully decentralized, and no single entity controls the blockchain network.
- The Bitcoin and Ethereum blockchains are both considered public ledgers.
- Public ledgers are also the most secure blockchains; they maintain a pseudo-anonymous system for their users' identities. While all transactions are recorded publically, user identities remain private.
- This means that while you can view any wallet address with its balance and transaction records, you cannot gain access to the identity of the wallet owner.

▼ **Bit coin**

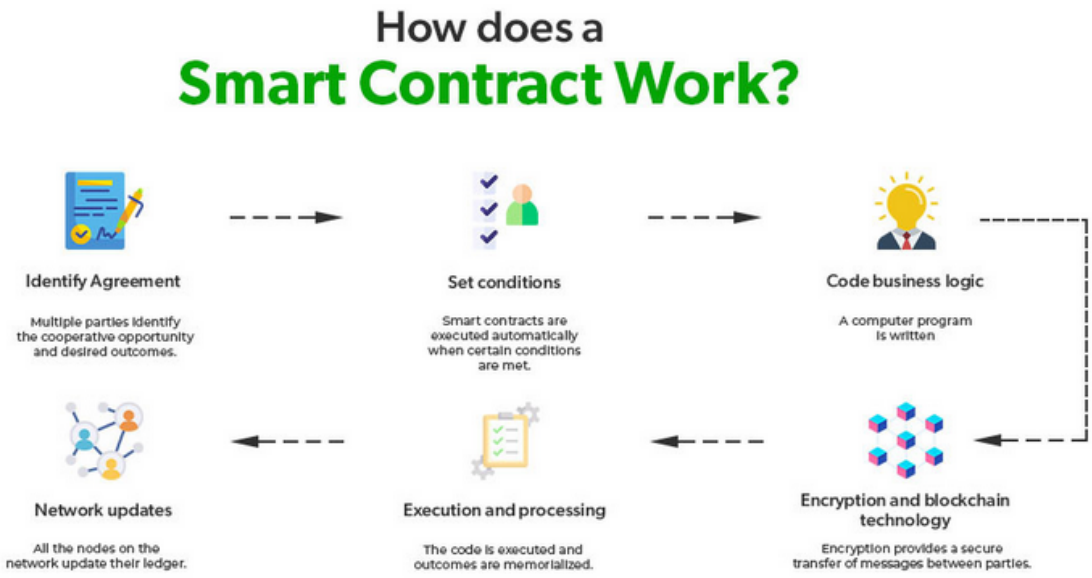
- Bitcoin emerged out of the 2008 global economic crisis when big banks were caught misusing borrowers' money, manipulating the system, and charging exorbitant fees. To address such issues, Bitcoin creators wanted to put the owners of bitcoins in-charge of the transactions, eliminate the middleman, cut high interest rates and transaction fees, and make transactions transparent. They created a distributed network system, where people could control their funds in a transparent way.
- The transaction is secured and made trustworthy by running it on a peer-to-peer network that is akin to a file-sharing system.

▼ **Smart Contracts**

- A Smart Contract (or cryptocontract) is a computer program that directly and automatically controls the transfer of digital assets between the parties under certain conditions.
- The bitcoin network was the first to use some sort of smart contract by using them to transfer value from one person to another.
- The smart contract involved employs basic conditions like checking if the amount of value to transfer is actually available in the sender account.
- Later, the Ethereum platform emerged which was considered more powerful, precisely because the developers/programmers could make custom contracts in a **Turing-complete**

language.

- It is to be noted that the contracts written in the case of the bitcoin network were written in a Turing-incomplete language, restricting the potential of smart contracts implementation in the bitcoin network.
- if/then/when…
- **Features of Smart Contracts**
  - **Distributed:** A smart contract is replicated and distributed by all the nodes connected to the network
  - **Deterministic:** Smart contracts can only perform functions for which they are designed only when the required conditions are met.
  - **Immutable:** Once deployed smart contract cannot be changed, it can only be removed as long as the functionality is implemented previously.
  - **Autonomous:** There is no third party involved
  - **Customizable**
  - **Transparent**
  - **Self-verifying:** These are self-verifying due to automated possibilities.
  - **Self-enforcing:** These are self-enforcing when the conditions and rules are met at all stages.

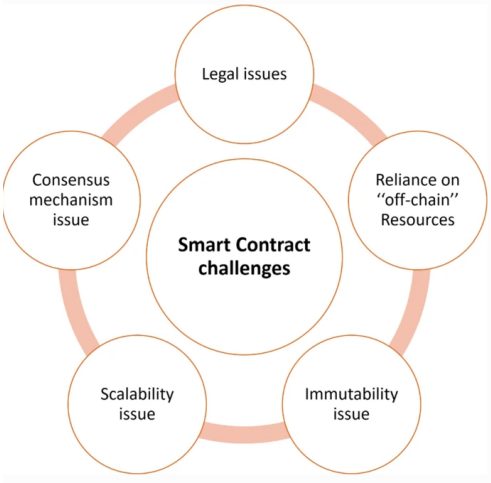


▼ **Chain code**

https://hyperledger-fabric.readthedocs.io/en/release-1.3/chaincode.html

▼ **Identify potential issues that companies face with smart contracts in the supply chain.**

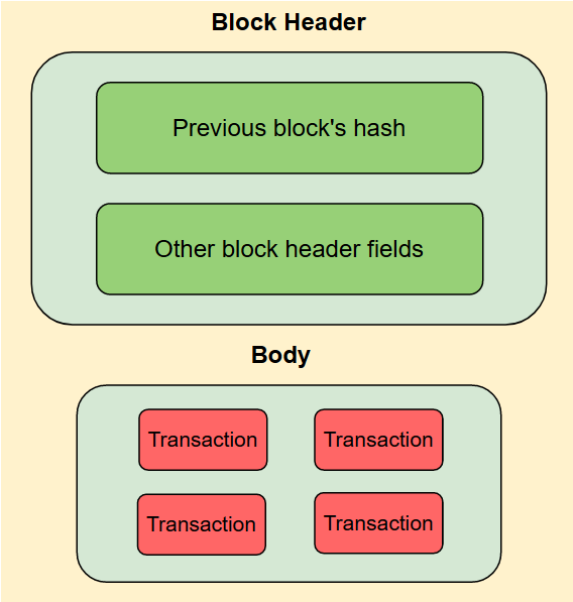
- **Legal issues**
  - The legal issue of smart contracts is another crucial aspect of smart contract challenges. For example, the European General Data Protection Regulation (GDPR) stipulates that citizens have a “right to be forgotten” which is inconsistent with the immutable nature of blockchain-enabled smart contracts.
- **Reliance on “off-chain” Resources**
  - Several smart contracts require receiving information or parameters from resources that are not on the blockchain itself, so-called off-chain resources. For this purpose, oracles are used as trusted third parties that retrieve off-chain information and then push that information to the blockchain at predetermined times. Although existing oracles are well tested, their use may introduce a potential “point of failure”.
- **Immutability issue**
  - dark side of the immutability concept in smart contracts lies mainly in the fact that in the event of any errors made in the code, the immutability feature of a smart contract prevents it from being rectified.
- **Scalability issue**
  - Scalability is the primary concern for many blockchain networks. For instance, the Ethereum blockchain can verify 14 transactions per second, which is slow as compared with Visa that can handle up to 24,000 transactions per second.
- **Consensus mechanism issue**
  - The consensus mechanism plays the leading role to maintain security, scalability, and decentralization in the blockchain networks at the same time. There are several existing consensus algorithms, including Proof-of-Work (PoW), Proof-of-Stake (PoS), etc. Although the PoW algorithm enables security in the blockchain, it wastes resources. Thus, many organizations switch from the PoW algorithm to new consensus mechanisms that promise lower fees for transactions as well as lower energy costs for the block production process.



▼ **Block in a Block chain**

- **Block** is a place in a blockchain where data is stored. In the case of cryptocurrency blockchains, the data stored in a block are transactions. These blocks are chained together by adding the previous block's hash to the next block's header. It keeps the order of the blocks intact and makes the data in the blocks immutable.
- **Structure of blocks**

  The structure of a block is different for every blockchain. However, a general structure of a block is as follows:

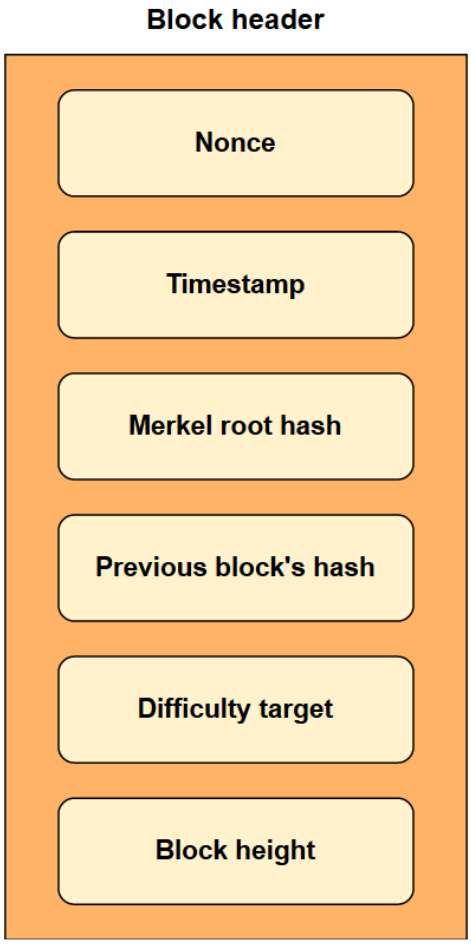


Block's structure

- A block consists of the following two main parts:
  - **Header**
  - **Body**
- **Header**

  A block's header contains information about the block and the miner. It is further divided into subparts which are as follows:
  - **Previous block's hash—**This is the hash of the previous block. It chains the blocks together and makes the data in the previous blocks immutable. If data in the previous blocks is changed, then the hash of that block will change causing the unchaining of the blockchain.
  - **Other block header fields—**These fields can vary depending on the different requirements of different blockchains.
    Some of the common fields are as follows:
    - **Nonce:** This is an integer that a miner changes to change the hash of the block to achieve the network's difficulty.

- **Timestamp:** This is the time at which the block was mined. It is usually in the Unix time.
- **Difficulty:** It is the current difficulty level of the network. It is stored in different formats in every blockchain.
- **Merkel root hash:** Hashes pair off transactions until only one hash remains, called a root hash or a Merkel root hash.
- **Block height:** The number of blocks mined between the genesis block and the current block.



Structure of a Bitcoin blockchain's block header

- **Body**

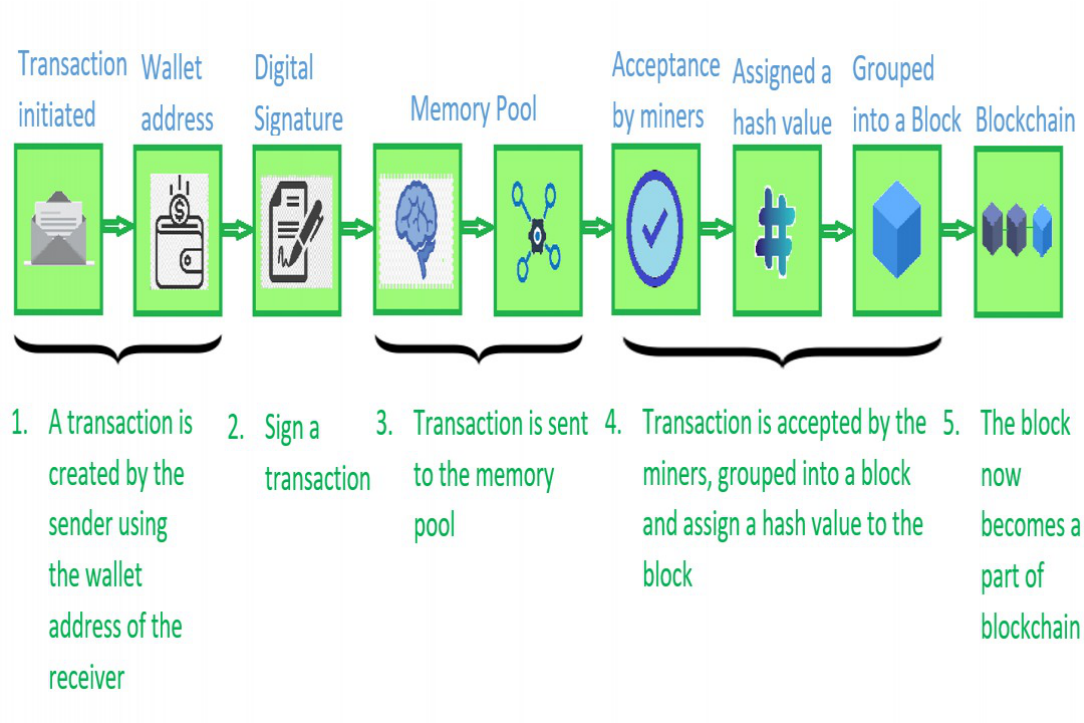
  It includes all the data stored in the block, such as transactions. Every blockchain has a different format for storing transactions. An array of transactions is stored in the body of the block.

▼ **Transactions**

- Blockchain technology is mostly about the transactions that we make digitally for ourselves. Eventually, these transactions make their way to the various blocks that become part of the

Blockchain later on. So, it is important to understand the transaction life cycle in Blockchain technology.

- This lifecycle follows the journey of a single transaction as it makes its way through each stage in the process of joining the blockchain. Transaction in simple words is the process of sending money by the sender and the receiver receiving it. The Blockchain transaction is also quite similar, but it is made digitally.
- **Transaction life-cycle in Blockchain**

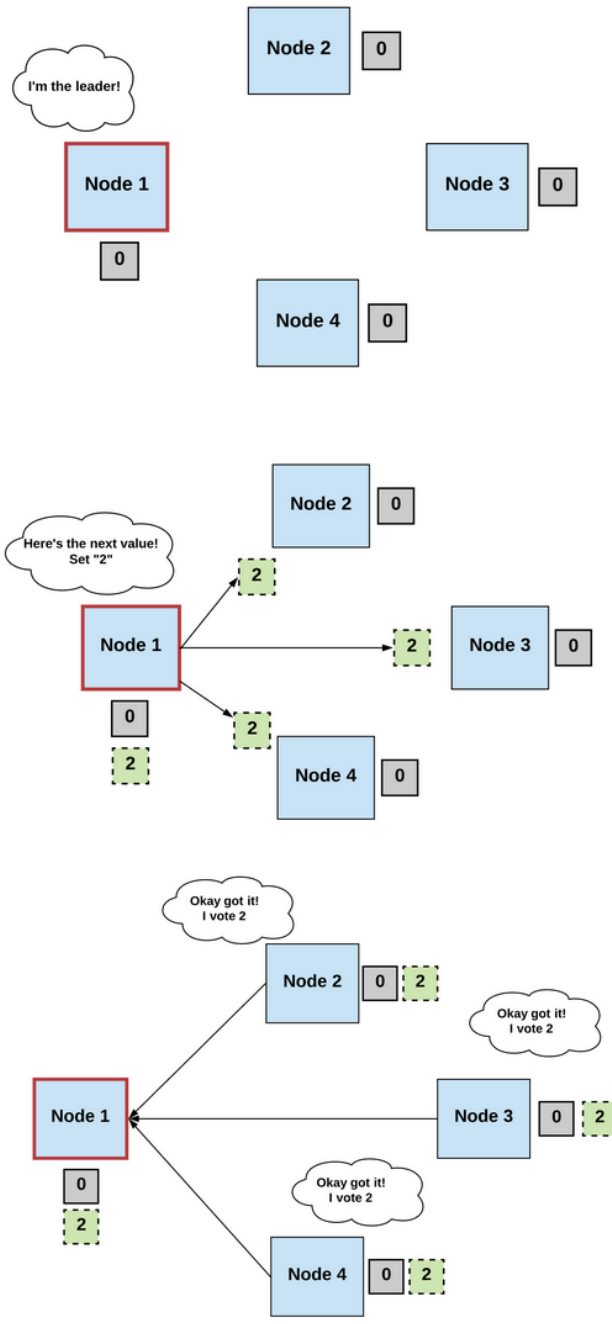


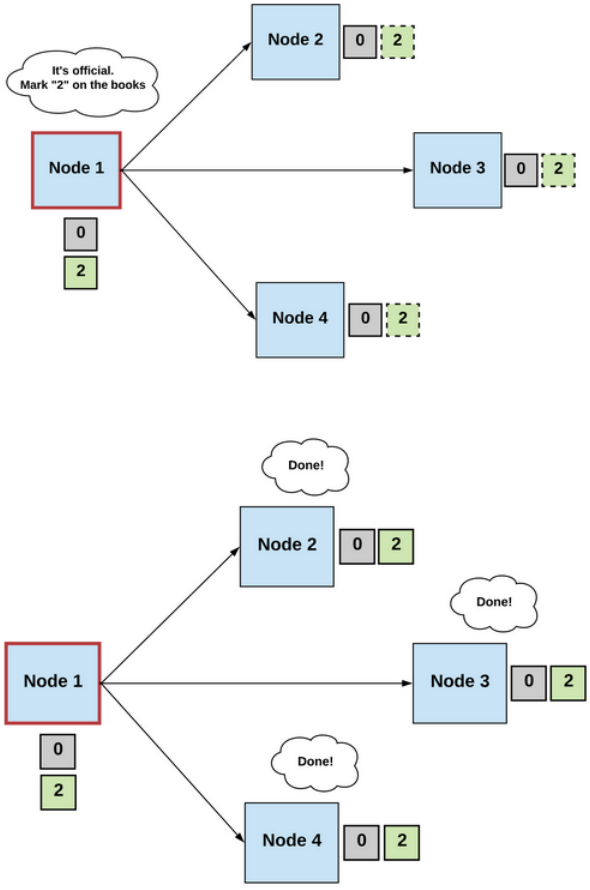
▼ **Distributed Consensus**

- A procedure to reach a common agreement in a distributed or decentralized multi-agent platform.
- It is important for the message passing system.
- **Features :**
  - It ensures reliability and fault tolerance in distributed systems.
  - In the presence of faulty individuals, it is Ensure correct operations.
- Generally, we can define a consensus algorithm by three steps:
  - **Step 1: Elect**
    - Processes elect a single process (i.e., a leader) to make decisions.
    - The leader proposes the next valid output value.
  - **Step 2: Vote**

- The non-faulty processes listen to the value being proposed by the leader, validate it, and propose it as the next valid value.

- **Step 3: Decide**
  - The non-faulty processes must come to a consensus on a single correct output value. If it receives a threshold number of identical votes which satisfy some criteria, then the processes will decide on that value.
  - Otherwise, the steps start over.

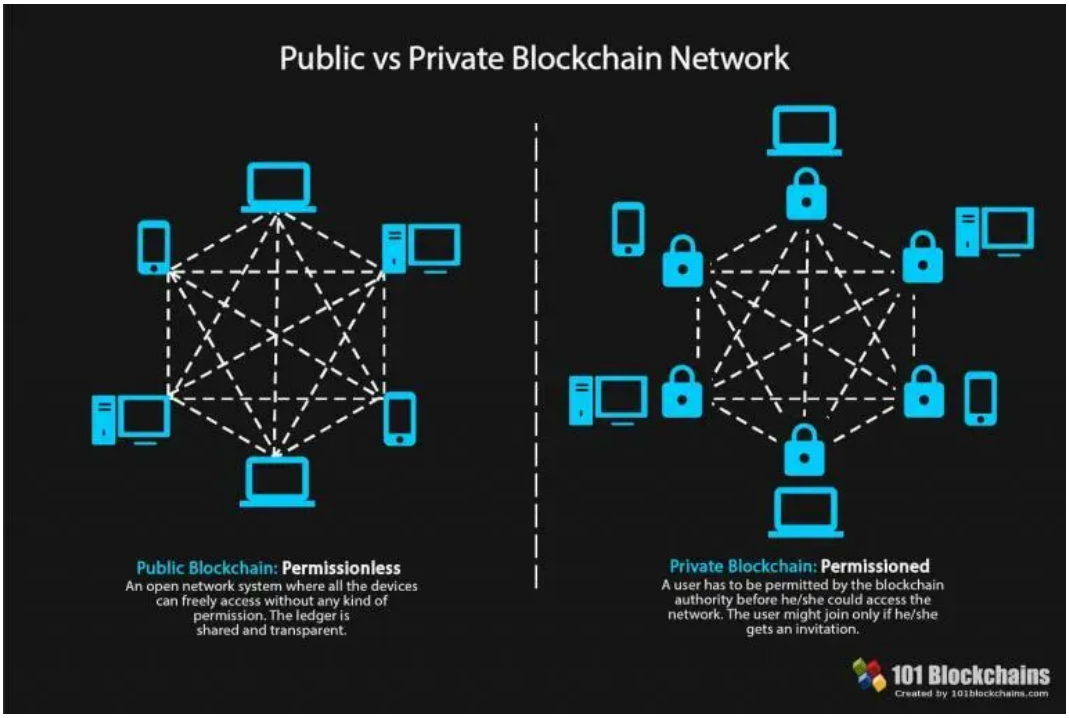




▼ Public vs Private Block chain

Basis of Comparison	Public BlockChain	Private BlockChain
Access	In this type of blockchain anyone can read, write and participate in a blockchain. Hence, it is permissionless blockchain. It is public to everyone.	In this type of blockchain read and write is done upon invitation, hence it is a permissioned blockchain.
Network Actors	Don’t know each other	Know each other
Decentralized Vs Centralized	A public blockchain is decentralized.	A private blockchain is more centralized.
Order Of Magnitude	The order of magnitude of a public blockchain is lesser than that of a private blockchain as it is lighter and provides transactional throughput.	The order of magnitude is more as compared to the public blockchain.
Native Token	Yes	Not necessary
Speed	Slow	Fast

Basis of Comparison	Public BlockChain	Private BlockChain
Transactions pre second	Transactions per second are lesser in a public blockchain.	Transaction per second is more as compared to public blockchain.
Security	A public network is more secure due to decentralization and active participation. Due to the higher number of nodes in the network, it is nearly impossible for ‘bad actors’ to attack the system and gain control over the consensus network.	A private blockchain is more prone to hacks, risks, and data breaches/ manipulation. It is easy for bad actors to endanger the entire network. Hence, it is less secure.
Energy Consumption	A public blockchain consumes more energy than a private blockchain as it requires a significant amount of electrical resources to function and achieve network consensus.	Private blockchains consume a lot less energy and power.
Consensus algorithms	Some are proof of work, proof of stake, proof of burn, proof of space etc.	Proof of Elapsed Time (PoET), Raft, and Istanbul BFT can be used only in case of private blockchains.
Attacks	In a public blockchain, no one knows who each validator is and this increases the risk of potential collision or a 51% attack (a group of miners which control more than 50% of the network’s computing power.).	In a private blockchain, there is no chance of minor collision. Each validator is known and they have the suitable credentials to be a part of the network.
Effect	Potential to disrupt current business models through disintermediation. There is lower infrastructure cost. No need to maintain servers or system admins radically. Hence reducing the cost of creating and running decentralized application (dApps).	Reduces transaction cost and data redundancies and replace legacy systems, simplifying documents handling and getting rid of semi manual compliance mechanisms.
Examples	Bitcoin, Ethereum, Monero, Zcash, Dash, Litecoin, Stellar, Steemit etc.	R3 (Banks), EWF (Energy), B3i (Insurance), Corda.



▼ Discuss whether a public block chain requires its own native cryptocurrency to provide incentives to its validator network.

- By creating its own native cryptocurrency, the blockchain network can reward validators for their contribution by issuing block rewards and transaction fees payable on such cryptocurrency.
- If this was not the case, validator's compensation would be limited to transaction fees paid by users through two alternative mechanisms, each with burdensome implications:
  1. compensating validators through a nonblockchain ("off-chain") system or
  2. compensating validators through a blockchain compatible external cryptocurrency (crosschain atomic swaps).
- In both alternatives, blockchain users would require accepting some features present on the payment system or external blockchain, as well as losing noncompatible attributes. For example, both options would constrain blockchain transactions speeds to the transaction speed of the off-chain payment system or external blockchain. It would restrict the universe of potential users and validators to those individuals and insti- tutions with access to the selected payment system. For the case of pay- ments through traditional financial networks, it would most likely require eliminating the blockchain's anonymity and pseudonymity attributes since validators would need to be identifiable to receive payments.

▼ Understanding Cryptocurrency to Block chain

- A cryptocurrency is a coded string of data representing a currency unit. Peer-to-peer networks called blockchains monitor and organize cryptocurrency transactions, such as buying, selling, and transferring, and also serve as secure ledgers of transactions. By utilizing encryption technology, cryptocurrencies can serve as both a currency and an accounting system.

- difficult to counterfeit because of this security feature
- decentralized and not subject to government or financial institution control
- trading is speculative and complex, and it involves significant risks
- the transaction cost is low to nothing at all
- International cryptocurrency transactions are faster than wire transfers too
- Cryptocurrency can be stored in several ways, but the most common is through a digital wallet. A digital wallet can be software-based, web-based, or hardware-based.

▼ **Permissioned Model of Block chain**

- Permissioned blockchains are blockchain networks that require access to be part of.
- **In these blockchain types, a control layer runs on top of the blockchain** that governs the actions performed by the allowed participants.
- A permissioned system is also known to have a restriction on the consensus participants, making permissioned networks highly configured and controlled by the owners.
- **Benefits of Permissioned Blockchains**
  - **Efficient performance:** When we compared permissioned blockchains to permissionless blockchains, they offer better performance. The core reason behind this is the limited number of nodes on the platform. This removes the unnecessary computations required to reach consensus on the network, improving the overall performance.
  - **Proper governance structure:** Permissioned networks do come with an appropriate structure of governance. This means that they are organized. Administrators also require less time to update the rules over the network, which is considerably faster when compared to public blockchains.
  - **Decentralized storage:** Permissioned networks also make proper use of blockchain, including utilizing its decentralized nature for data storage.
  - **Cost-Effective:** There is no doubt that permissioned blockchains are more cost-effective when compared with the permissionless blockchains.
- **Drawbacks of Permissioned blockchains**
  - **Compromised security –** A public or private blockchain has better security as the nodes participate in a consensus method properly.
  - **Control, Censorship, and Regulation –** In an ideal world, these permissioned blockchains should work as that of a public blockchain, but with regulations. However, the regulations bring censorship to the network, where the authority can restrict a transaction or control it from happening.

Permissioned Blockchain vs Permissionless Blockchain		
Category	**Permissioned**	**Permissionless**
Speed	Faster	Slower
Privacy	Private membership	Transparent and open - anyone can become a member
Legitimacy	Legal	Allegal
Ownership	Managed by a group of nodes pre-defined	Public ownership - no one owns the network
Decentralization	Partially decentralized	Truly decentralized
Cost	Cost-effective	Not so cost-effective
Security	Less secure	More secure

▼ **Overview of Security aspects of Block chain**

- Blockchain is a distributed ledger technology (DLT) designed to engender trust and confidence in an environment.
- Blockchain is a decentralized ledger system that’s duplicated and distributed across a whole network of computer systems.
- It allows information access to all designated nodes or members who can record, share, and view encrypted transactional data on their blockchain.
- Blockchain security is a complete risk management system for blockchain networks, incorporating assurance services, cybersecurity frameworks, and best practices to mitigate the risks of fraud and cyber-attacks.
- **Blockchain Security Challenges**
  - **Routing attacks.** Blockchains depend on immense data transfers performed in real-time. Resourceful hackers can intercept the data on its way to ISPs (Internet Service Providers). Unfortunately, blockchain users don’t notice anything amiss.
  - **51% attacks.** Large-scale public blockchains use a massive amount of computing power to perform mining. However, a group of unethical miners can seize control over a ledger if they can bring together enough resources to acquire more than 50% of a blockchain network’s mining power. Private blockchains aren’t susceptible to 51% attacks, however.
  - **Sybil attacks.** Named for the book that deals with multiple personality disorder, Sybil attacks flood the target network with an overwhelming amount of false identities, crashing the system.
  - **Phishing attacks.** This classic hacker tactic works with blockchain as well. Phishing is a scam wherein cyber-criminals send false but convincing-looking emails to wallet owners, asking for their credentials.
- **Best Practices For Building Secure Blockchain Solutions**
  - **Use of Cold Wallet:** Cold Wallets do not connect to the Internet, therefore users can secure their private keys. The wallet is not prone to cyberattacks.

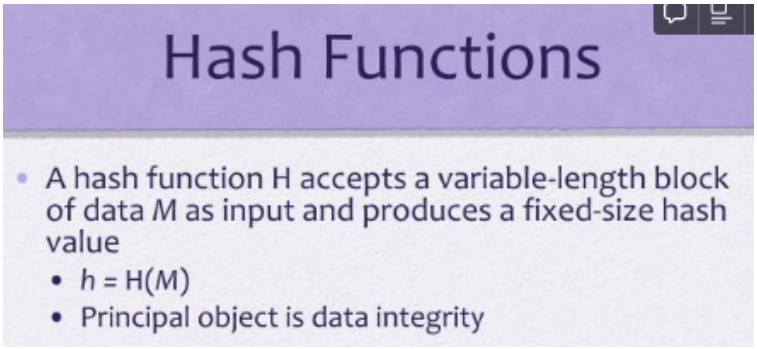
- **Avoid Phishing:** Phishing attacks are common nowadays. Users should not click malicious advertisements. They should remove all the spam emails.
- **Blockchain Penetration Testing:** Those who create blockchain networks should get penetration testing done by an ethical hacker to test the strength of the security blockchain networks and find vulnerabilities if present.
- **Secure keys:** Keys should be secured by the user. Strong cryptographic keys should be used Users should not share the keys with other users.
- **Use private permissioned blockchain:** Business entrepreneurs should use private permissioned blockchain. The permission is necessary as each user is verified before allowing them to enter the blockchain.

- **Blockchain Security For The Enterprise**
  - Each user should be verified before allowing them to access the blockchain.
  - All transactions within the blocks are validated by business users and are agreed upon by a consensus mechanism.
  - The blocks should be immutable so that once a transaction is done, it cannot be reverted.
  - Businessmen should use strong cryptographic keys.
- **Blockchain Security Examples**
  - **CoinBase:** It is a California-based company. It secures the passwords and wallets in a secure database. It is run purely on encryption so that no hackers can have access to it.
  - **Javvy:** It is a Georgian company that uses Artificial Intelligence to detect fraudulent activity. It also built a universal wallet to keep easy track of users' money.
  - **JP Morgan:** A famous US-based company. It uses blockchain technologies for private transactions. JP Morgan also developed Quorum for secured private transactions. It also uses the concept of cryptography in transactions.

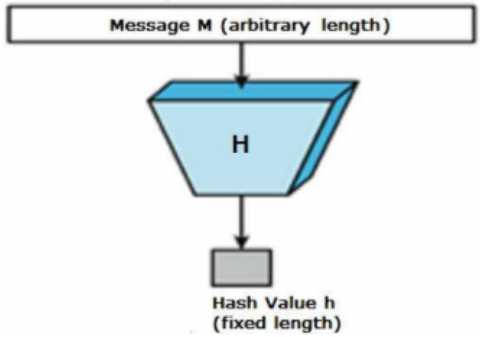
▼ **Cryptographic Hash Function**

1. **Hash Function**

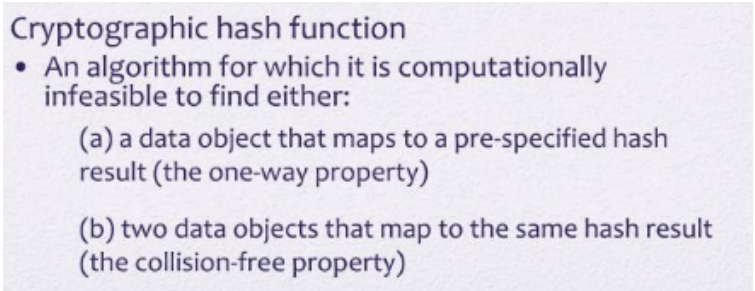
   a. A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

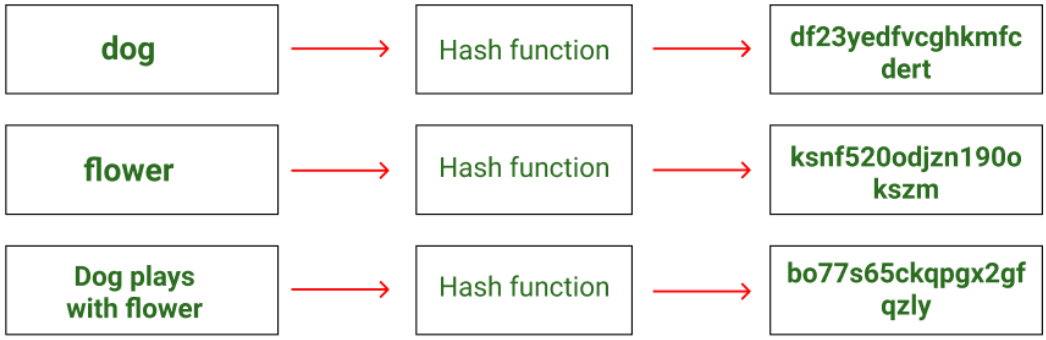


1. Values returned by a hash function are called message digest or simply hash values. The following picture illustrated hash function-

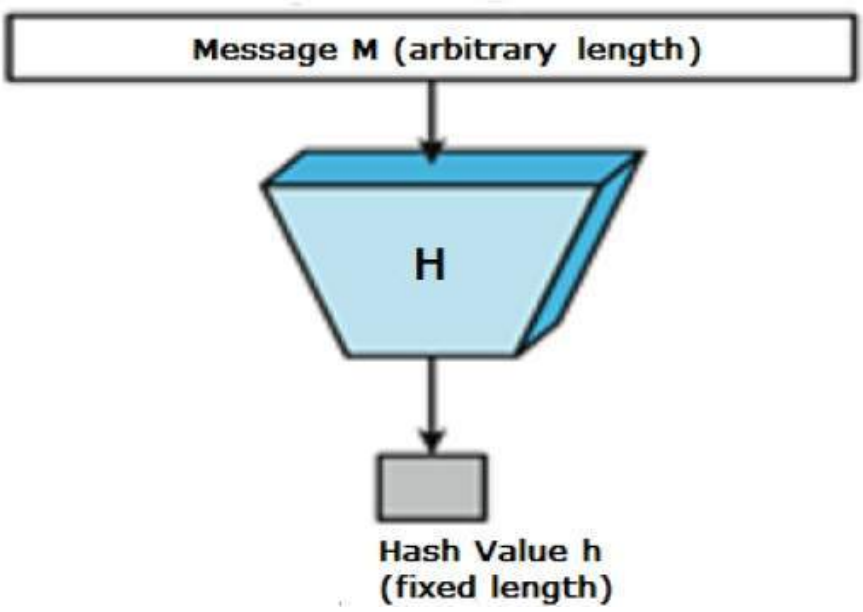


2. **Cryptographic Hash Functions**
   a. A **cryptographic hash** is a function that outputs a fixed-size digest for a variable-length input. A hash function is an important cryptographic primitive and extensively used in blockchain.
   b. They are efficient and are **well-known for one property: they are irreversible**. **It's a one-way function** that's only meant to work in one direction.
   c. For example, SHA-256 is a hash function in which for any variable-bit length input, the output is always going to be a 256-bit hash.





3. **Features of Hash Functions**
    a. **Fixed Length Output (Hash Value):** Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data.
    b. **Efficiency of Operation:** Computationally hash functions are much faster than a symmetric encryption.



▼ **Properties of a hash function**

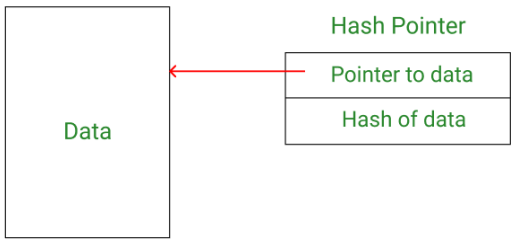
- **Pre-Image Resistance:** This property means that it should be computationally hard to reverse a hash function. This property protects against an attacker who only has a hash value and is trying to find the input.
- **Second Pre-Image Resistance:** This property means given an input and its hash, it should be hard to find a different input with the same hash.
- **Collision Resistance:** This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.

Properties for Cryptographic Hash Functions

1. Easy to compute:
   - Given message m, hash function $h(m)$ is easy to compute.
2. One-way function $y = h(x)$:
   - Given y, it is very hard to find x.
3. Collision-free: (1. strong version and 2. weak version)
   1) It is very hard to find messages m_1 and m_2 with $h(m_1)=h(m_2)$.
   2) Given m_1 and $h(m_1)$, it is very hard find $m_2 \neq m_1$ with $h(m_2)= h(m_1)$.

▼ **Hash pointer**

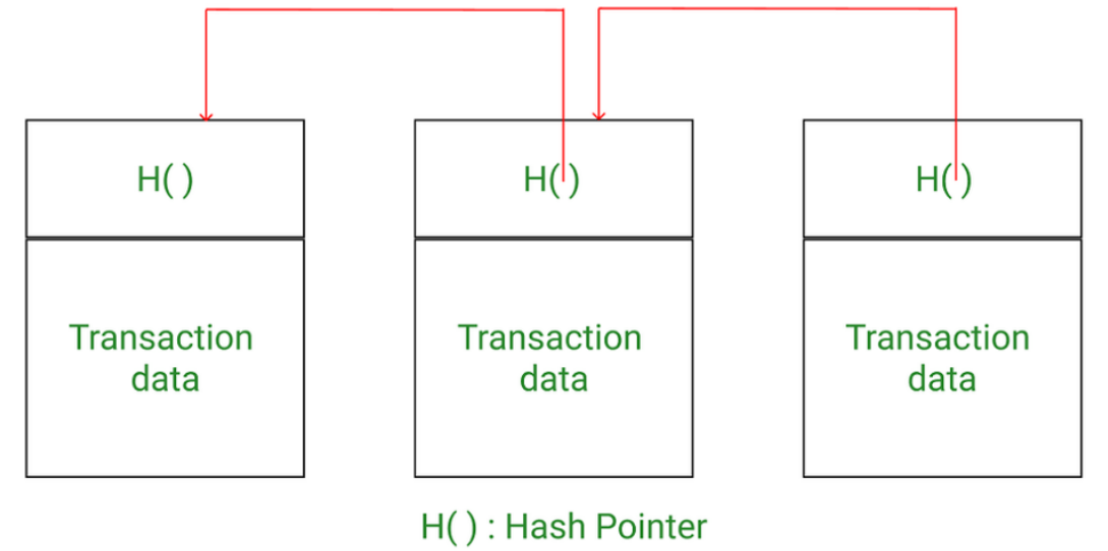
- A regular pointer stores the memory address of data. With this pointer, the data can be accessed easily.
- On the other hand, a hash pointer is a pointer to where data is stored and with the pointer, the cryptographic hash of the data is also stored.
- So a hash pointer points to the data and also allows us to verify the data.
- A hash pointer can be used to build all kinds of data structures such as blockchain and Merkle tree.



▼ **Blockchain Structure**

The blockchain is a proficient combination of two hash-based data structures—

1. **Linked list:** This is the structure of the blockchain itself, which is a linked list of hash pointers. A regular linked list consists of nodes. Each node has 2 parts- data and pointer. The pointer points to the next node. In the blockchain, simply replace the regular pointer with a hash pointer.

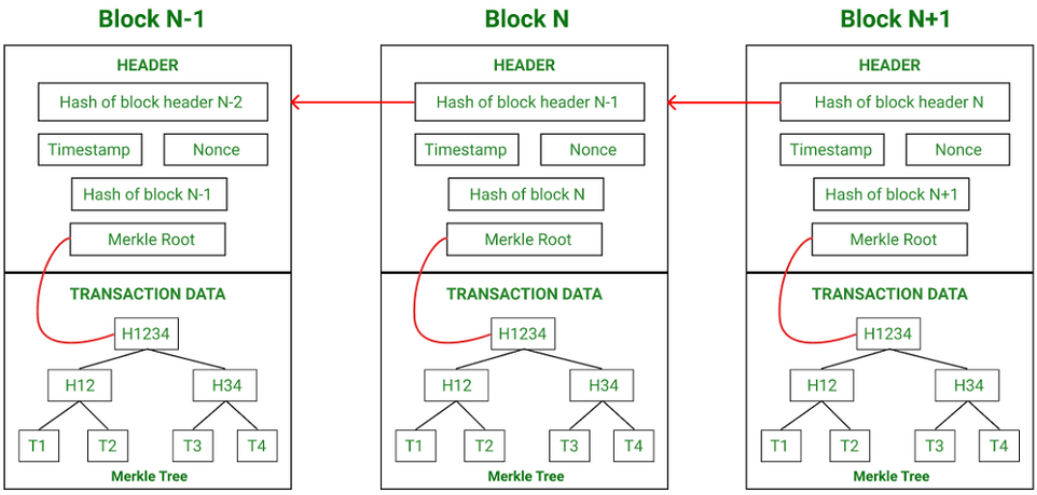


Blockchain as linked list with hash pointers

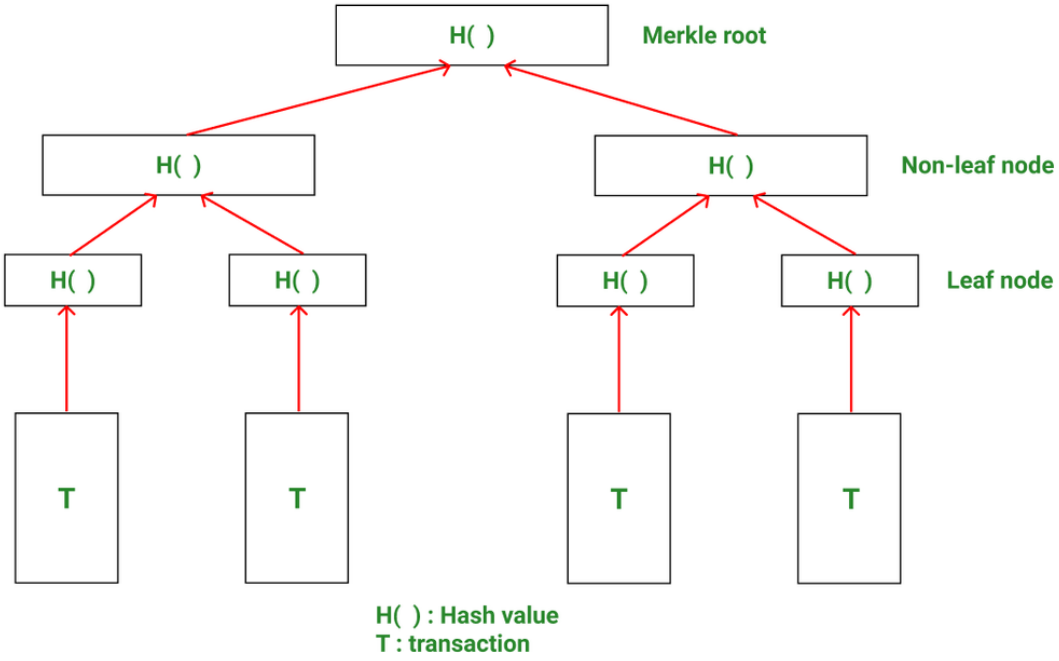
2. **Merkle tree:** A Merkle tree is a binary tree formed by hash pointers, and named after its creator, Ralph Merkle.

▼ **Merkle tree**

- Merkle trees, also known as Binary hash trees, are a prevalent sort of data structure in computer science.
- A Merkle tree is a binary tree formed by hash pointers, and named after its creator, Ralph Merkle.
- As mentioned earlier, each block is supposed to hold a certain number of transactions. Now the question arises, how to store these transactions within a block? One approach can be to form a hash pointer-based linked list of transactions and store this complete linked list in a block. However, when we put this approach into perspective, it does not seem practical to store a huge list of hundreds of transactions. What if there is a need to find whether a particular transaction belongs to a block? Then we will have to traverse the blocks one by one and within each block traverse the linked list of transactions.
- This is a huge overhead and can reduce the efficiency of the blockchain. Now, this is where the Merkle tree comes into the picture. Merkle tree is a per-block tree of all the transactions that are included in the block. It allows us to have a hash/digest of all transactions and provides proof of membership in a time-efficient manner.
- **So to recap, the blockchain is a hash-based linked list of blocks, where each block consists of a header and transactions. The transactions are arranged in a tree-like fashion, known as the Merkle tree.**

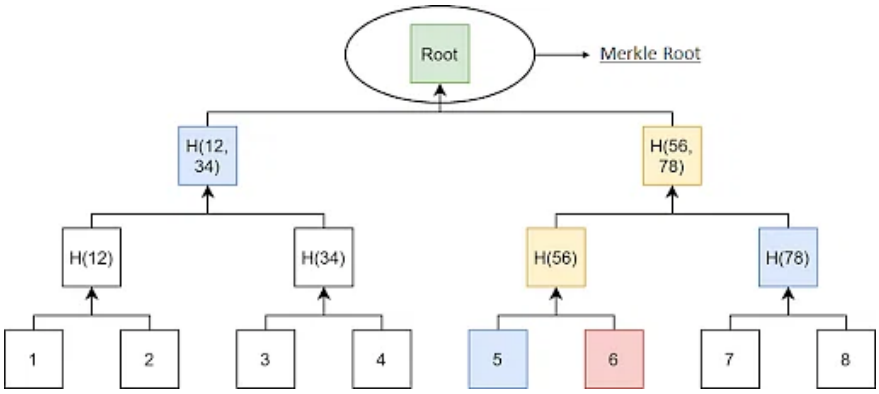


- In bitcoin and other cryptocurrencies, they're used to encrypt blockchain data more efficiently and securely.
- It's a mathematical data structure made up of hashes of various data blocks that summarize all the transactions in a block.
- It also enables quick and secure content verification across big datasets and verifies the consistency and content of the data.
- **Merkle Tree Structure**

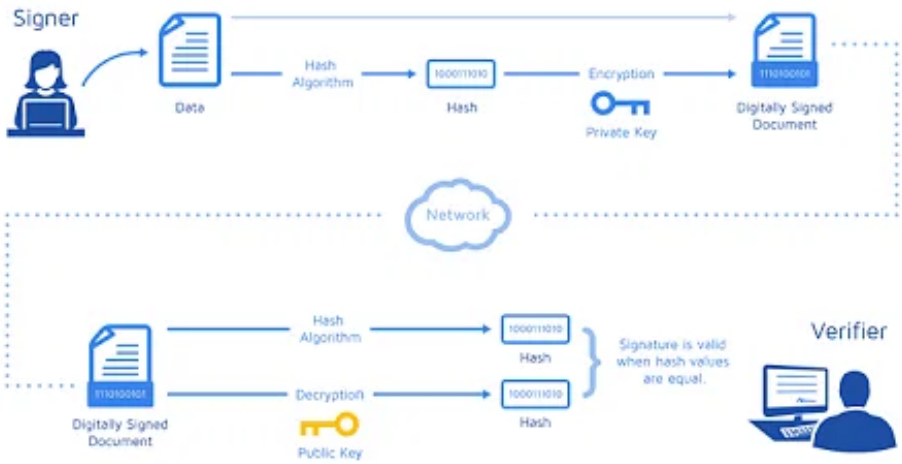


- **What Is a Merkle Root?**
  - A Merkle root is a simple mathematical method for confirming the facts on a Merkle tree.

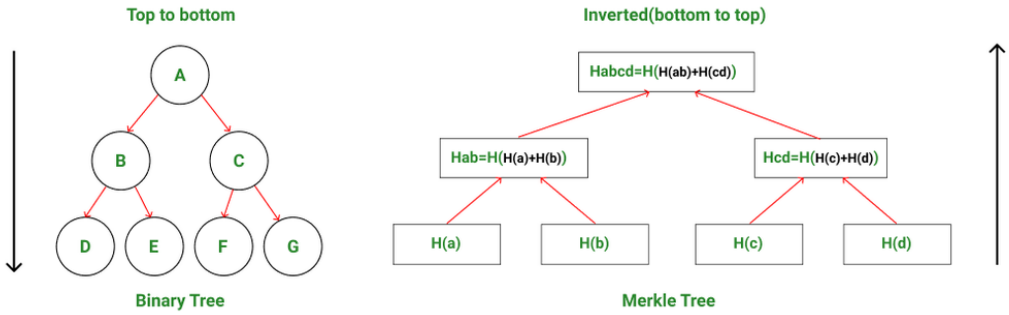
- They're used in cryptocurrency to ensure that data blocks sent through a peer-to-peer network are whole, undamaged, and unaltered.
- They play a very crucial role in the computation required to keep cryptocurrencies like bitcoin and ether running.



- **Working of Merkle Trees**
  - A Merkle tree totals all transactions in a block and generates a digital fingerprint of the entire set of operations, allowing the user to verify whether it includes a transaction in the block.

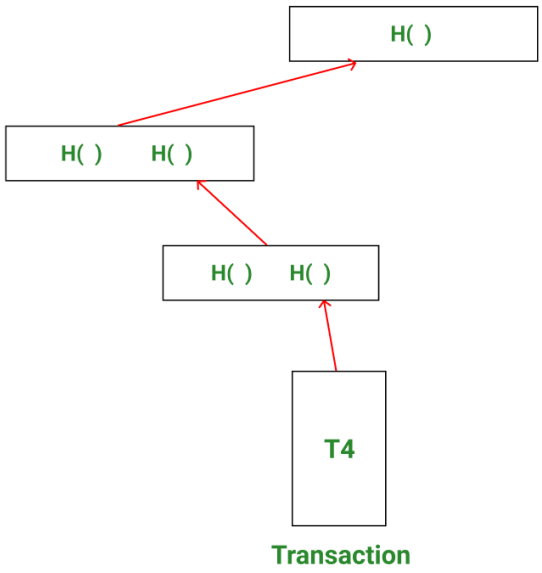


  - Merkle trees are made by hashing pairs of nodes repeatedly until only one hash remains; this hash is known as the Merkle Root or the Root Hash.
  - They're built from the bottom, using Transaction IDs, which are hashes of individual transactions.



  - Each non-leaf node is a hash of its previous hash, and every leaf node is a hash of transactional data.

- **Benefits of Merkle Tree in Blockchain**
  - **Validate the data's integrity:** It can be used to validate the data's integrity effectively.
  - **Takes little disk space:** Compared to other data structures, the Merkle tree takes up very little disk space.
  - **Tiny information across networks:** Merkle trees can be broken down into small pieces of data for verification.
  - **Efficient Verification:** The data format is efficient, and verifying the data's integrity takes only a few moments.
- **Proof of Membership**
  - A very interesting feature of the Merkle tree is that it provides **proof of membership**.
  - **Example:** A miner wants to prove that a particular transaction belongs to a Merkle tree Now the miner needs to present this transaction and all the nodes which lie on the path between the transaction and the root. The rest of the tree can be ignored because the hashes stored in the intermediate nodes are enough to verify the hashes all the way up to the root.

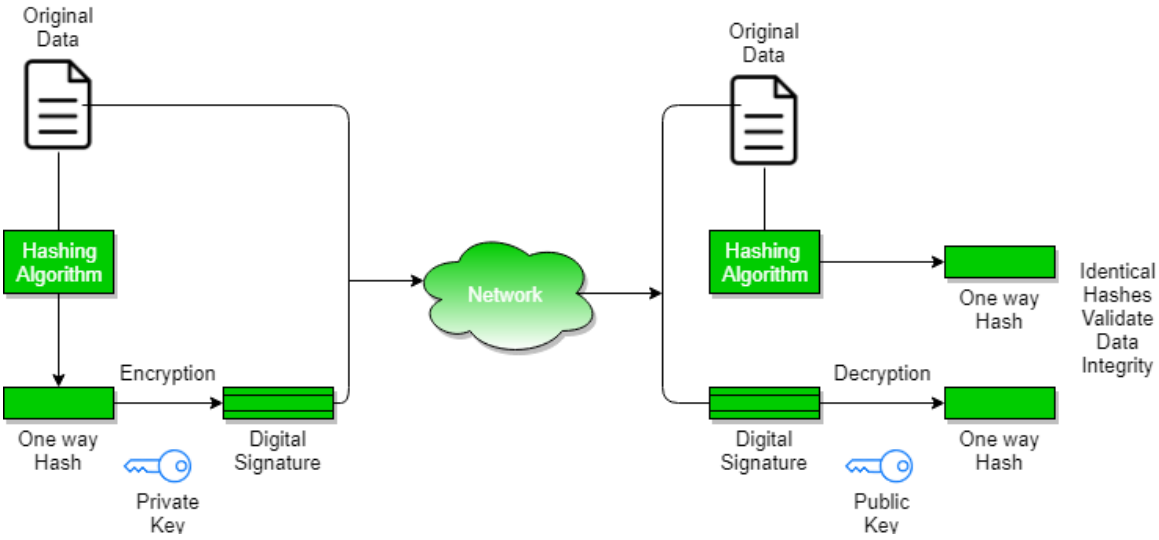


Proof of membership: verifying the presence of transactions in blocks using the Merkle tree.

- **If there are n nodes in the tree then only log(n) nodes need to be examined. Hence even if there are a large number of nodes in the Merkle tree, proof of membership can be computed in a relatively short time.**

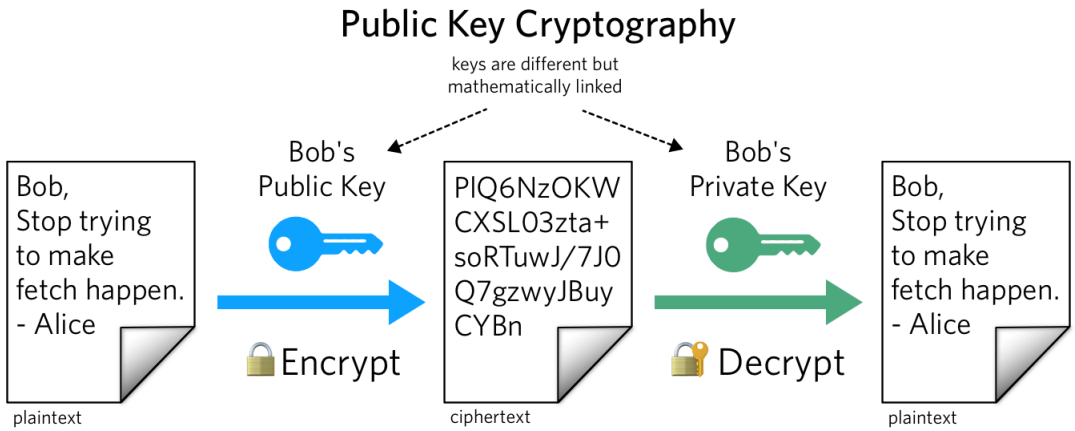
▼ **Digital Signature *(working?)***

- Encryption and decryption address problems of eavesdropping, but they do not address tampering and impersonation. However, public-key cryptography does address the problems of tampering and impersonation.
- You can use your private key for encryption and your public key for decryption. Although this is not desirable when you are encrypting sensitive data, it is an important part of digitally signing any data. Rather than encrypting the data itself, you can create a one-way hash of the data and then use your private key to encrypt the hash. The encrypted hash, along with other information like the hashing algorithm, is known as a digital signature.
- Below figure shows a simplified view of how you can use a digital signature to validate the integrity of signed data.



▼ Public Key Cryptography

- Public key cryptography involves a pair of keys known as a public key and a private key (a public key pair), which are associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published and the corresponding private key is kept secret. Data that is encrypted with the public key can be decrypted only with the corresponding private key.
- RSA public key pairs can be any size. Typical sizes today are 1024 and 2048 bits.
- Public key cryptography enables the following:
  - Encryption and decryption, which allow two communicating parties to disguise data that they send to each other. The sender encrypts, or scrambles, the data before sending it. The receiver decrypts, or unscrambles, the data after receiving it. While in transit, the encrypted data is not understood by an intruder.
  - Nonrepudiation, which prevents:
    - The sender of the data from claiming, at a later date, that the data was never sent
    - The data from being altered.



UNIT 2

▼ **Define the three major characteristics of money that Bitcoin possesses**

Bitcoin has three major characteristics of money

- **First**, bitcoin is divisible similar to how fiat currency units are divisible into smaller units of previously existing units. The division takes place digitally in the form of bitcoin and other cryptocurrencies, but the divisibility still exists.
- **Second**, any medium of exchange (money) must also be useful as a unit of account, which bitcoin partially fulfills. Despite prior price volatility and continued lower levels of volatility, bitcoin has a value in other forms of currency. In fact, after the 2017 price bubble, volatility decreased substantially.
- **Third**, any medium of exchange must be portable. That is, it must be able to be transferred across borders and boundaries. As a digital medium of exchange, bitcoin is easily portable and can be transferred across borders without fees.
- divisible
- convertible
- portable

▼ **Creation of coins**

- Cryptocurrencies are ‘mined’. For better understanding of how cryptocurrencies are created, we can refer to Bitcoin, which is created by the process of ‘mining’. The ‘Mining’ process involves massive amounts of powerful computer hardware and resilient software. Mining is the process by which cryptocurrency transactions are verified and new units of cryptocurrency are created.
- Each time a cryptocurrency transaction takes place, a cryptocurrency miner, who also serves as a node on the blockchain on which these transactions are taking place, tries to decrypt the block containing the transaction information. For example, if Person Y wants to send 0.1 Bitcoins to Person Z, then miners on the Bitcoin blockchain compete to be the first to decrypt the block that contains the transaction information.
- Decrypting the block not only authenticates the transaction, but also provides the information about who sent how many Bitcoins to whom and at what time and date. Once the block has been decrypted and has been accepted by most of the nodes on the blockchain as being authentic, the block is added to the blockchain.
- Now, the verification process is pretty resource intensive in terms of the computational power required. As such, individual miners often find the process too expensive and so they join pools to collectively use computing power.
- **Cryptocurrency (Bitcoin) Mining Reward**
  - So, the question is, if the mining process is so expensive, why do miners compete to decrypt blocks? The answer to this lies in the rewards mechanisms. In return for their services, the cryptocurrency miner is rewarded with a fraction of new units of the cryptocurrency. In other words, the miners are paid in the cryptocurrency that they

choose to mine. So, if a miner chooses to decrypt a Bitcoin block, then they will be paid in Bitcoin.

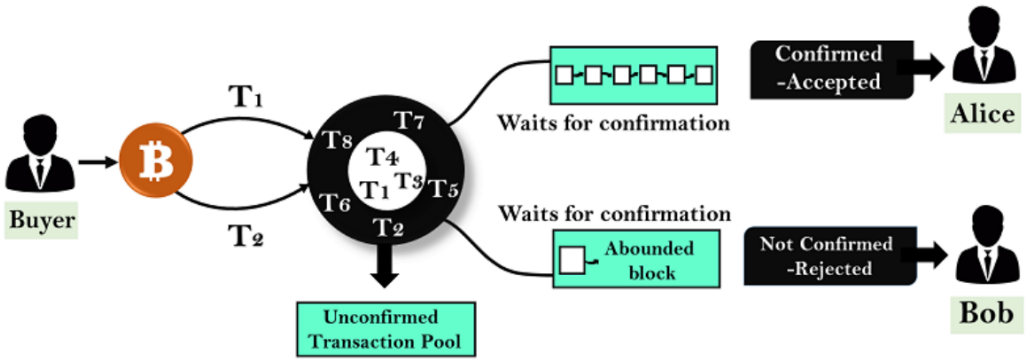
- By pooling their resources, miners increase their chances of success and spread out the costs, but they also then get only a share of the rewards.

▼ **Coins vs Tokens**

- Cryptocurrencies are largely divided into two groups—coins and tokens. Coins and tokens are distinct and different from each other, and each has potential advantages for different types of businesses.
- A coin is that application of cryptocurrencies that runs on its own blockchain, which is where all the transactions take place. Some of the larger examples of coins are Bitcoin, Etherium, Dogecoin, etc. These are the assets that people can invest in and exchange. If somebody wants to create a new coin, they would have to create a new blockchain.
- A token, on the other hand, functions on top of an existing blockchain infrastructure and are often used like smart contracts, which can be used for physical objects as well as services, physical and digital. One of the main reasons companies consider issuing a token is for a security token offering, which various projects and start-ups use to raise funds.

▼ **Double spending**

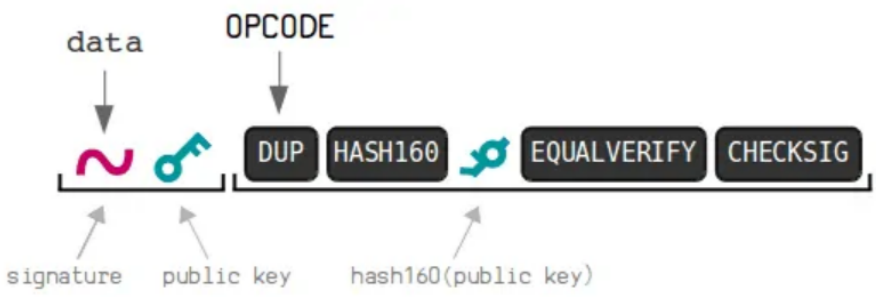
- Double spending means spending the same money twice.
- In a physical currency, the double-spending problem can never arise. But in digital cash-like bitcoin, the double-spending problem can arise. Hence, bitcoin transactions have a possibility of being copied and rebroadcasted. It opens up the possibility that the same BTC could be spent twice by its owner.
- **How Bitcoin handles the Double Spending Problem?**
  - Bitcoin handles the double-spending problem by implementing a confirmation mechanism and maintaining a universal ledger called blockchain.
  - Let us suppose you have 1 BTC and try to spend it twice. You made the 1 BTC transaction to Alice. Again, you sign and send the same 1 BTC transaction to Bob. Both transactions go into the pool of unconfirmed transactions where many unconfirmed transactions are stored already. The unconfirmed transactions are transactions which do not pick by anyone. Now, whichever transaction first got confirmations and was verified by miners, will be valid. Another transaction which could not get enough confirmations will be pulled out from the network. In this example, transaction T1 is valid, and Alice will receive the bitcoin.



▼ **Bit coin Scripts**

- Bitcoin Script is the language Bitcoin uses to do everything it can do, from sending funds from a wallet to allowing the creation of multi-user accounts. All these functionality contained in a simple extensible and powerful tool that we will know next.
- This is based on a series of linear structures, known as **stack**, which contain existing data in order **LIFO (Last In - Firt Out).**
- This language is not Full Turing because its functionality is limited and **cannot loop**
- In the Bitcoin network, each Bitcoin Script is divided into two types of scripts, the **scriptSig & scriptPubKey**.
  - First, the **scriptSig** is the unlock script, which requires a public key and a digital signature.
  - The second, the **scriptPubKey**, is the blocking script, which contains a public key hash, also called a Bitcoin address.
- On the other hand, there are the **OP_CODES (Operation Code)** that in the operation are the following:

OP_DUP	Duplicate the item on the top stack.
OP_HASH160	The input is encoded twice: first with SHA-256 and then with RIPEMD-160.
OP_EQUALVERIFY	Verify that the data entered is correct and valid.
OP_CHECKSIG	The outputs, inputs, and script of the entire transaction are summarized in a hash. The signature used must be a valid signature for this hash and must be next to the public key.



▼ **Bit coin P2P Network**

- **Peer-to-peer (P2P)** networks are a type of network architecture where each node or participant has the same capabilities and functions as both client and server. In P2P networks, all nodes are equal, and resources such as files, data, and computing power are shared directly among the users without the need for a central server.
- **Role of P2P in Blockchain**
  - P2P is a technology that is based on a very simple principle, and that is the concept of decentralization. The peer-to-peer architecture of blockchain allows all cryptocurrencies to be transferred worldwide, without the need of any middle-man 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.
- **Validation of transactions**
  - Each node contains a copy of the transaction records and participates in the process of adding new blocks to the chain.
  - Based on the consensus mechanism used, the nodes compete by solving extremely complex mathematical problems to validate transactions and add blocks to the chain.
  - The node which adds blocks to the chain is rewarded with the native cryptocurrency of the blockchain.
  - Nodes are thus able to ensure only valid transactions are included in the ledger, ensuring its integrity is maintained.
- **Pros**
  - Because of P2P networking capability, even if one peer gets down, the other peers are still present. Thus nobody can take down the blockchain.
  - P2P networks offer greater security compared to traditional client-server systems.
  - When you are using cloud computing to store your data, you need to trust AWS and Google drives, but with the blockchain, because it utilizes peer to peer network you don’t need to trust any third parties which can modify your crucial data. These are non-resistant to censorship by central authorities.
  - These networks are **virtually immune to the Denial-of-Service (DoS) attacks**.

- The distributed peer-to-peer network, when paired with a majority consensus requirement, gives blockchains a relatively high degree of resistance to malicious activity.

- **Cons**
  - P2P network in blockchain, however, raises few concerns. As in blockchain, instead of a central server, **distributed ledgers must be updated on every single node, adding transactions requires a considerable amount of computational power.**
  - Although this provides an increased level of security, it significantly reduces efficiency, and this acts as one of the main hindrances in terms of scalability and mass adoption.

▼ **Transaction in Bit coin Network**

- Bitcoin transaction means sending bitcoin from one person to the other in the secured blockchain network. These are messages that are digitally signed using cryptography and are verified by the miners that are present in the blockchain network. The miner is the person who solves mathematical puzzles(also called proof of work) to validate the transaction.
- The transaction input is the bitcoin address from which the money was sent, and the transaction output is the bitcoin address to which the money was sent. Generally, a bitcoin transaction takes 10 to 20 minutes to confirm any transactions. if network congestion takes place, then time might take even 60 minutes.
- **Essentially, a BTC transaction is consist of three parts:**
  - **An input:**
    - This is a record of the BTC address from which X initially received the bitcoin he wants to send to Y.
  - **An amount:**
    - This is the specific amount of BTC X wants to send Y.
  - **An output:**
    - This is Y's public key; also known as his 'bitcoin address
- **Transaction Fees**
  - The transaction rate or speed is dependent on the amount the user pays for it. If a user pays a small amount, the transaction rate will be slow, the transaction will take more time to happen, vice versa is applicable here. Due to limited space, only a limited number of transactions are possible at one point in time.
- Bitcoin makes use of public-key cryptography to ensure the integrity of transactions created on the network. In order to transfer bitcoin, each participant has pairs of public keys and private keys that control pieces of bitcoin they own. A public key is a series of letters and numbers that a user must share in order to receive funds. In contrast, a private key must be kept secret as it authorizes the spending of any funds received by the associated public key.

▼ **Block Mining**

- Bitcoin Mining is the process of verifying bitcoin transactions and storing them in a blockchain(ledger).
- This process of verifying transactions is called mining.
- Bitcoin mining is a computation-intensive process that uses complicated computer code to generate a secure cryptographic system. The bitcoin miner is the person who solves mathematical puzzles(also called proof of work) to validate the transaction. Anyone with mining hardware and computing power can take part in this.
- **Types of Mining**

Individual Mining	When mining is done by an individual, user registration as a miner is necessary. As soon as a transaction takes place, a mathematical problem is given to all the single users in the blockchain network to solve. The first one to solve it gets rewarded. Once the solution is found, all the other miners in the blockchain network will validate the decrypted value and then add it to the blockchain. Thus, verifying the transaction.
Pool Mining	Pool Mining In pool mining, a group of users works together to approve the transaction. Sometimes, the complexity of the data encrypted in the blocks makes it difficult for a user to decrypt the encoded data alone. So, a group of miners works as a team to solve it. After the validation of the result, the reward is then split between all users.
Cloud Mining	Cloud mining eliminates the need for computer hardware and software. It's a hassle-free method to extract blocks. With cloud mining, handling all the machinery, order timings, or selling profits is no longer a constant worry. While it is hassle-free, it has its own set of disadvantages. The operational functionality is limited with the limitations on bitcoin hashing in blockchain. The operational expenses increase as the reward profits are low. Software upgrades are restricted and so is the verification process.

▼ **Block propagation**

- The lack of scalability is known to be the foremost obstacle standing in the way of mass adoption of blockchain technology.
- All existing blockchain projects look for solutions that could improve the performance of their network.
- After the invention of decentralized peer-to-peer network Bitcoin, researchers got interested in what determines the limits of Bitcoin's scaling.
- Soon the core issue was determined and described in terms of **block propagation time or block propagation delay**.

- It is an **average time that is needed for the new block to reach most nodes in the network**.
- In a large-decentralized network like Bitcoin, whenever the new block is generated, it is broadcasted according to the Gossip protocol.
- If some node has got the new valid block, it informs nodes connected to it about its new possession.
- Then the node transfers this block to those nodes which asked it to do that. Before the block reaches each full-node in the network, it passes through 7 intermediary nodes.
- It is important that every honest node verifies the block before relaying it to other peers.
- It is important that even in the worst-case scenario, the propagation delay should be reasonable so that miners will keep their nodes synchronized most of the time and will always verify proposed blocks.
- Whenever people talk about the scalability of the blockchain, they mention the transaction throughput of the system.
- However, people forgot that improvements in transaction throughput shouldn't compromise the network's security or raise data storage requirements for nodes desiring to participate in the network.
- These modifications could decrease the number of independent transaction validators in the network, thereby reducing decentralization.
- Transaction throughput in Bitcoin could be easily calculated using the formula:

$$(blocksize/averagetransactionsize) = transactionsperblock$$

▼ **Block relay**

- A Bitcoin Relay Network is a network that attempts to minimize the latency in the transmission of blocks between miners.
- The original Bitcoin Relay Network was created by core developer Matt Corallo in 2015 to enable fast synchronization of blocks between miners with very low latency.
- The network consisted of several specialized nodes hosted on the Amazon Web Services infrastructure around the world and served to connect the majority of miners and mining pools.
- The original Bitcoin Relay Network was replaced in 2016 with the introduction of the **Fast Internet Bitcoin Relay Engine or FIBRE**, also created by core developer Matt Corallo.
- FIBRE is a UDP-based relay network that relays blocks within a network of nodes. FIBRE implements compact block optimization to further reduce the amount of data transmitted and the network latency.
- **Relay networks are not replacements for bitcoin's P2P network**. Instead they are overlay networks that provide additional connectivity between nodes with specialized

needs. Like freeways are not replacements for rural roads, but rather shortcuts between two points with heavy traffic, you still need small roads to connect to the freeways.

▼ **Working with Consensus in Bitcoin**

- Blockchain is a distributed decentralized network that provides immutability, privacy, security, and transparency.
- There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely secured and verified.
- This is possible only because of the presence of the consensus protocol which is a core part of any Blockchain network.
- A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment.
- Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.
- Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.
- **Various consensus algorithms—**
  - Proof of Work (PoW)
  - Practical Byzantine Fault Tolerance (PBFT)
  - Proof of Stake (PoS)
  - Delegated Proof Of Stake (DPoS)
  - Proof of Burn (PoB)
  - Proof of Capacity
  - Proof of Elapsed Time

▼ **Proof of Work (PoW)—Basic introduction**

- Proof of Work(PoW) is the **original consensus algorithm** in a blockchain network
- algorithm is used to confirm the transaction and creates a new block to the chain
- In this algorithm, miners (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
- A new Block is created in every 10 Minutes. The more Miners there are, the harder the puzzle is. Mining Difficulty is adjusted every 2 weeks

- **Mining pools**
    - Mining Pool means one such Mining Unions - When Many Miners Mining by Making Pool
- **Disadvantages of POW**
    - Only one gets Reward, but a lot of Miners' Energy Wastage takes place while solving the puzzle.
    - The risk of attack increases by 51%, which is a major threat to Decentralization.
    - There is a problem of scalability (Transaction Per Second is very limited)

▼ **Hash Cash PoW**

- HashCash was a solution designed to combat spam by generating a proof of work that allowed verifying that a certain email was not spam.
- used to minimize spam and **denial of service attacks**
- technology gained wide popularity thanks to its implementation in the **Bitcoin** and many others **cryptocurrencies**
- **The objective of HashCash is to require computer work for it to be verified.**
- Once said work is verified, the user is allowed to use the resource.
- Use in email is based on adding an encrypted header to the email. This header has the information generated by the user using the HashCash system. This is a kind of seal that ensures that the mail has passed the proof of work. This seal is an identifier that shows that the sender has used the processor for a small amount of time.
- **How does HashCash work**
    - It is based on the idea that if a certain user has used their processor to generate this stamp, it is unlikely that they are a spammer. Receivers with a very low almost negligible computational cost can verify this. In this way we can guarantee that it is not spam.
- **HashCash use cases**
    - **Protection of connections**
        - Create a **connection token** generated by an interactive **HashCash cost function**. With this defense, client-server connections are protected with a hash ensuring that they cannot be "stolen" or "broken" by malicious actors.
    - **Computer file systems**
        - **hashing functions** create a unique signature for each block of stored data. Thanks to this signature, the system is able to verify their authenticity

▼ **Bit coin PoW**

- Bitcoin uses the Hashcash Proof of Work system as the mining basis.

- The miners bundle up a group of transactions into a block and try to mine. To mine it, a hard mathematical problem has to be solved.
- This problem is called the proof of work problem which has to be solved to show that the miner has done some work in finding out the solution to the problem and hence the mined block must be valid.
- The answer to the problem needs to be a lower number than the hash of the block for it to be accepted, known as the '**target hash**'.

> 💡 A target hash is a number that the header of a hashed block must be equal to or less than for a new block, along with the reward, to be awarded to a miner.
>
> The lower a target is, the more difficult it is to generate a block.

- **Challenges With PoW**
  - The 51% risk
  - Time-consuming
  - Resource consumption
  - Not instantaneous transaction

▼ **Attacks on PoW**

2 major attacks by which PoW based systems can crash

- **Sybil Attacks**
  - In this attack, the attacker attempts to fill the network with the clients under its control so that he can refuse to relay valid blocks and can perform double spending.
  - In Simple language, The attacker can include multiple nodes in the network who can collectively compromise the Proof of Work mechanism.
  - **Solution**
    - Bitcoin makes these attacks more difficult by only making an outbound connection to one IP address per /16 IP address
- **Denial of Service(DOS) Attacks**
  - The attacker sends a lot of data in the network to make it busy so that the actual transactions are not able to take place.
  - **Solutions:**
    - No forwarding of orphaned blocks
    - No forwarding of double-spend transactions
    - No forwarding of same block or transactions
    - Disconnect a peer that sends too many messages

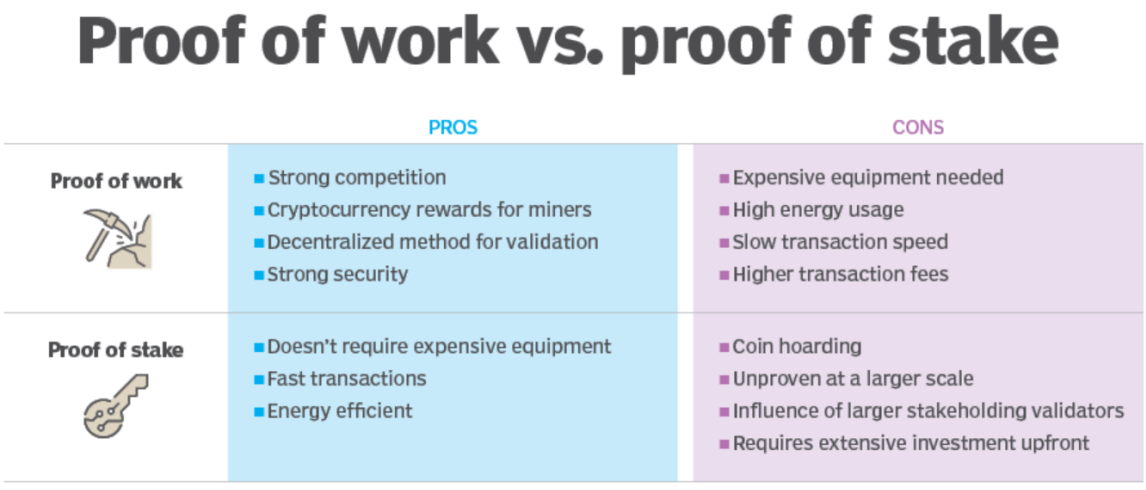
- Restrict the block size to 1 MB
- Limit the size of each script up to 10000 bytes

▼ **Monopoly problem**

- During bitcoin's early days, anyone could "mine" it using their home computer. But as the price of digital currency climbed towards $100 in 2013 (it's now over $4,000), professional mining groups with specialised computer chips emerged. Today, these groups, or pools — nearly all based in China — have become concentrated and now dominate the production of new bitcoins.
- **Why monopoly problem existed?**
  - Miners are getting less rewards over the time. So, they are discouraged to join as a miner.
  - The difficulty of puzzle is increasing which is not possible to be solved by normal hardware.
- **Solution of Monopoly Problem**
  - Proof of Stake(PoS) emerged as a solution to this problem

▼ **Proof of Stake**

- A person can mine or validate block transactions according to how many coins he or she holds. This means that the more Bitcoin or altcoin owned by a miner, the more mining power he or she has.
- The **first cryptocurrency to adopt the PoS method was Peercoin**. In Peercoin, the coinage is used as a variation of stake. Coinage is calculated by multiplying number of coins by the number of days the coins have been held.
  - If an attacker wants to attack, he/she should have more number of bitcoins.
  - If the attacker holds majority of bitcoins, then the majority affect will be on attacker only.



▼ **Proof of Burn**

- PoB works on the principle of allowing the miners to “burn” or “destroy” the virtual currency tokens, which grants them the right to write blocks in proportion to the coins burnt.
- To burn the coins, miners send them to a verifiably un-spendable address. This process does not consume many resources other than the burned coins.
- PoB works by burning PoW mined cryptocurrencies. It is power efficient unlike PoW.

▼ **Proof of Elapsed Time**

- PoET is proposed by Intel as a part of hyperledger sawtooth.
- In this each participant in the blockchain network waits a random amount of time. The first participant to finish waiting gets to be leader for the new block.
- To verify that the proposer has really waited for the random amount of time, it relies on a special CPU instruction set called Intel Software Guard Extensions (SGX). SGX allows applications to run trusted code in a protected environment.

▼ **The life of a Bitcoin Miner**

Responsibilities of a miner:

- Validate transactions and construct a block.
- Use hash power to vote on consensus and commit transactions with a newblock.
- Store and broadcast the blockchain to the peers.

How a miner mines a bitcoin?

- A miner joins the network and listens for the transactions.
- Listens for new blocks, then validate and re-broadcast a new block when it is proposed.
- Collects transactions for a predefined time and construct a new block.
- Finds a nonce to make the new block valid.
- Broadcasts the new block. Everybody accepts it if it is a part of the mainchain.
- Earns the reward for participating in the mining procedure.

▼ **Mining Difficulty**

- Mining difficulty is a measure of the amount of difficulty in finding the hash below a given target.
- Bitcoin has a global block difficulty while mining pools have a pool-specific share difficulty.
- **Difficulty Calculation in Bitcoin:**
  - In Bitcoin, the **difficulty changes for every 2016 blocks**. The desired rate is that it should take two weeks to mine 2016 blocks provided one block is mined in 10 minutes.
  - If it takes less than two weeks to mine 2016 blocks, then the difficulty is increased. If it takes more than two weeks to mine 2016 blocks, the difficulty is decreased.

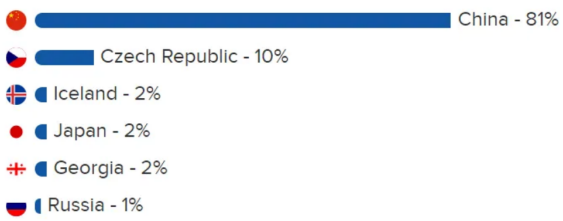
current_difficulty = previous_difficulty *(2 weeks in milliseconds)/(milliseconds to mine last 2016 blocks)

- The expected number of hashes we need to calculate to find a block with difficulty D is :

(D * 2256) / (0xffff * 2208)

▼ **Mining Pool**

- When the resources are pooled by miners, they create a mining pool.
- The processing power is shared by miners over a network to mine a new block.
- The reward is split proportionally to the amount of work each miner has contributed.
- **Slush Pool is the oldest currently active mining pool. AntPool is the largest currently active mining pool.**
- Although mining pool allows small miners to participate in the mining process, it also discourages miners for running complete mining procedure.
- Mining centralisation in China is one of Bitcoin's biggest issues at the moment.



UNIT 3 - Understanding Block chain for Enterprises

▼ **Permissioned Block chain**

- A permissioned blockchain (BC) is a secure distributed ledger maintained by a number of trusted validation nodes.
- A permissioned blockchain has all the features of the public/permissionless blockchain.
- Blockchain is run among identified and known participants.
- Users know each other but do not trust each other.
- Participants need to obtain an invitation or *permission* to join the network.
- This places restrictions on who is allowed to participate in the network, and only in certain transactions.
- **Advantages of Permissioned Blockchains**
  - Permissioned blockchain tends to be fast as they can choose their own consensus method and do not need every node for validation purposes.
  - These are far more scalable.
  - For organizations, permissioned blockchain (consortium) can offer more customizability.

- Permissioned blockchains can also follow governance structure.

- **Disadvantages of Permissioned Blockchain**
  - A permissioned blockchain is not truly decentralized.
  - They are less transparent.
  - Member's KYC is required to join the network with the admin's approval.
  - Less anonymous.

	Permission-less	Permissioned
Access	Open read/write access to database	Permissioned read/write access to database
Scale	Scale to a large number of nodes, but not in transaction throughput	Scale in terms of transaction throughput, but not to a large number of nodes
Consensus	Proof of work/ proof of stake	Closed membership consensus algorithms
Identity	Anonymous/pseudonymous	Identities of nodes are known, but transaction identities can be private/anonymous/pseudonymous
Asset	Native assets	Any asset/data/state

▼ **Permissioned model and use cases**

- **Financial Services:**
  - **Trade Finance:** Trade finance provides delivery and payment assurance to buyers and sellers. The blockchain can be used by the legal entities to sign all approvals, keeping all parties informed regarding the approval status, when goods are received and when payment is transferred from the importer's to the exporter's bank.
  - **Cross-border transactions:** Nostro(ours)/vostro(yours) accounts can become stored account transactions on a blockchain to dramatically improve transparency and efficiency through automated reconciliation of accounts.
- **Government:**
  - A considerable amount of government involves recording transactions and tracking ownership of assets, all of which can be made more efficient and transparent through the use of blockchain.
  - Organisations can apply blockchain by issuing digitally authenticated birth certificates that are unforgeable, time-stamped, and accessible to anyone in the world.
- **Supply Chain Management:**
  - **Food Safety:** Powered by IBM Blockchain, IBM Food Trust directly connects participants through a permissioned, permanent, and shared record of food origin details, processing data, shipping details, and more.

- **Global Trade:** More than $4 trillion in goods are shipped each year, with 80 percent of those shipments carried by the ocean shipping industry.Yet the cost of trade documentation is estimated to reach one-fifth of the actual physical transportation costs. Blockchain's distributed ledger technology to help speed goods on their journey from manufacturer to market, providing one universal view of the truth to unleash new transparency and remove friction.

- **Health Care:**
  - Blockchain holds the complete medical history for each patient, with multiple granularities of control by the patient, doctors, regulators, hospitals, insurers, and so on, providing a secure mechanism to record and maintain comprehensive medical histories for every patient.

▼ **Design issues for Permissioned block chains**

- A permissioned blockchain (BC) is a secure distributed ledger maintained by a number of trusted validation nodes.
- However, a validator may become compromised and send inconsistent messages to different nodes. To counter the problem, consensus protocols like Practical Byzantine Fault Tolerance (PBFT) can be used.
- Furthermore, it is necessary to identify those compromised nodes discovered during the consensus protocol.
- A compromised node may send inconsistent messages to others or accuse other nodes compromised, and it should be removed as soon as it is identified and confirmed.
- BGP (Byzantine General Protocols) protocols such as PBFT provide consensus mechanisms in permissioned BCs.
- A BGP protocol allows the network to detect the behaviour of malicious nodes, and **all working nodes can reach a consensus if the number of compromised node is less than one-third of the total number of nodes, or**
  n >= 3f +1
  where n is the number of nodes and f is the number of compromised nodes
- **PBFT has three phases**, and each node maintains its own view of the network.
- The protocol is initiated by a leader in the network. Even if the leader failed, other nodes take over the responsibility and resume the operation.
- **A simplified 3-phase process is as follows:**
  - A leader sends out pre-prepare message to all the nodes;
  - Each node received the message will produce a response, and send the response, i.e., prepare, to every node;
  - After receiving sufficient such as 2/3 prepare messages from the nodes, each can commit to the agreement, and send out the commit message to everyone.
- Thus, to reach a consensus, there will be three rounds of messaging, one for each pre-prepare, prepare, and commit message.

▼ **Smart Contracts / Execute contracts**

- A smart contract is an **agreement or set of rules** that govern a business transaction.
- It is stored on the blockchain and is executed automatically as part of a transaction.
- **Smart contracts allow transactions to be carried out without the need for a governance, legal system, central authority or external enforcement mechanism.**
- Smart contracts are created by computer programmers with the help of smart contract development tools available that are digital and compiled using programming code languages such as C++, Go, Python, Java.
- **Benefits of Smart Contract:**
  - **Trust:** All documents are encrypted on a shared ledger. Also all the entities or parties could have access to these documents.
  - **Autonomous:** All third parties become obsolete in the interactions
  - **Security:** All documents are encrypted end to end which makes them near-impenetrable by unethical methods.
  - **Redundancy:** Documents are duplicated many times over on the blockchain, and can't ever be "lost".
  - **Savings:** Smart contracts save you money by taking out the middleman.
  - **Speed:** These contracts automatically self-execute, saving you precious time.
  - **Transparency:** For organisations like governments, they could add another level of transparency to dealings.
  - **Precision:** Smart contracts execute the exact code provided, ensuring zero errors.
- **Design Limitations of Smart Contract:**
  1. **Sequential Execution:**
     - Smart Contract executes transactions sequentially based on consensus.
     - Requests to the application (smart contract) are ordered by theconsensus, and executed in the same order.
     - This give a bound on the effective throughput — throughput isinversely proportional.
     - There can be a possible attack on the smart contract platform by introducing contract which will take long time to execute.
  2. **Non-deterministic Execution:**
     - Smart-contract execution should always needs to be deterministic;otherwise the system may lead to inconsistent states (many fork inthe blockchain).
     - Iteration over a map may produce a different order in two executions like in Go Lang.
  3. **Execution on all nodes:**

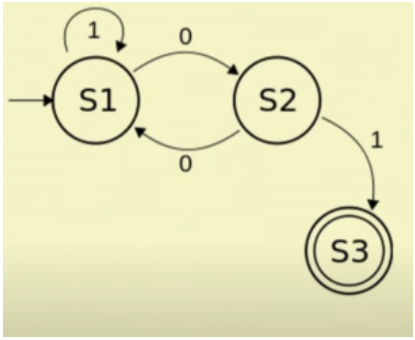
- Execute smart contracts at all nodes, and propagate the state to others to reach consensus.
- Propagate same state to all nodes, verify that the states match.

▼ **State machine replication**

- The state machine replication helps us to achieve a consensus in a permission model.
- **We do not need to execute a smart contract to all the nodes**. Rather, the selected subset of contract executor executes it and propagates it with other nodes to ensure the contract's status is propagated to all the nodes uniformly in the network, and they are on the same page.
- The distributed state machine replication technology ensures consensus in a permission blockchain environment.

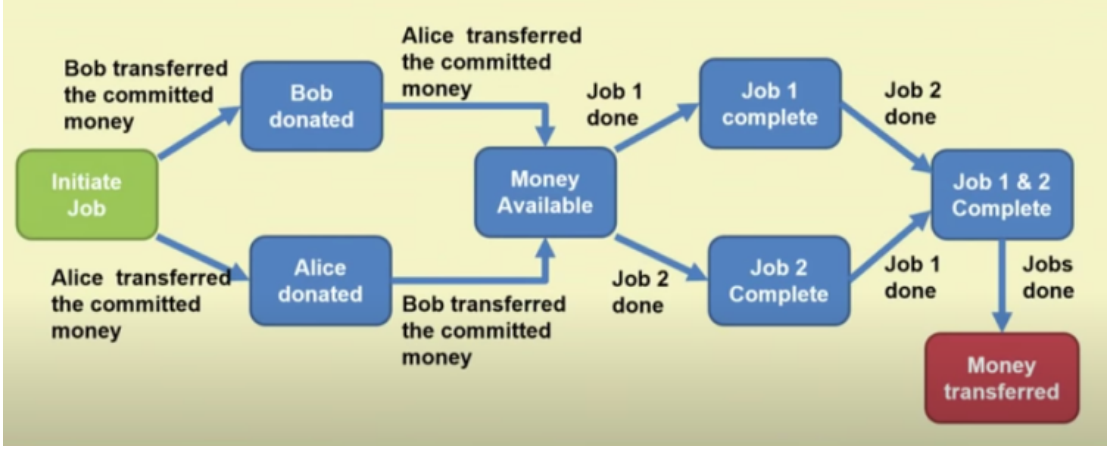
Understanding of State Machine Concept

- State Machine is characterized by a set of parameters such as set of Inputs, set of Outputs, and the Transition States.
  - A set of state (S) based on the system design
  - A set of inputs (I)
  - A set of outputs (O)
  - A transition function S x I –> S; takes the current state and input value and produces a set as the output.
  - A output function S x I –> O
  - A start state



Example of State Machine: Smart Contract – Crowd-Funding

- In general any algorithm can be represented by the finite state machine and we will understand it with an example of Crowdfunding platform in smart contract. The smart contract state machine representation are as follows:



- In the crowdfunding platform, there are mainly two parties which include the project proposes and project funders. The project proposers propose the project to the funders, and if they are interested, they will invest money in their project. The funders will release funds after the completion of a certain job. In the above diagram, Alice and Bob are the two funders, and they are transferring money after completing the proposed jobs by the proposers. Once the entire job is completed, money will be transferred to them.

Overview of Consensus models for permissioned block chain

▼ **Distributed consensus in closed environment**

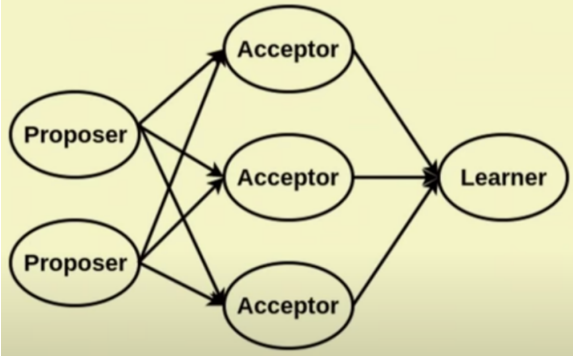
Need for Distributed Consensus

- If there is only a single decision-maker, we don't need a consensus algorithm. In the case of two decision-makers (nodes) and the presence of any faults such as crash fault, or network fault or even if the node behaves maliciously, we can not reach a consensus.
- To reach a consensus, we always require more than two nodes or decision-makers.
- In the case of multiple decision-makers, and collectively, they want to come to a certain decision, and then we require a consensus algorithm.
- The distributed consensus helps us to reach an agreement in the case of distributed computing.
- In the case of the state machine replication concept, we replicate the common status so that all the processes have the same view of the state.
- **Examples:**
  - State machine replication is the flight control system when there are multiple flights. They want to coordinate their positions among themselves in the closed distributed environment to achieve consensus.
  - Fund transferring system in a closed distributed environment.
  - Distributed leader election in a closed distributed environment where all the nodes collectively need to elect one leader in the system.
- **Faults in Distributed Consensus**

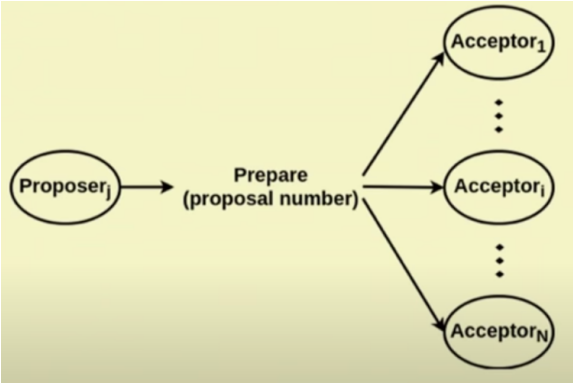
    - **Crash Fault:** A **node suddenly crashes** or becomes unavailable in the middle of communication. This may be because of hardware or software faults
    - **Network or Partitioned Faults:** A network fault occurs because of the **link failure**, and the network gets partitioned. This may be because of the edge router failures and, consequently, hamper reaching the consensus.
    - **Byzantine Faults:** A **node starts behaving maliciously**. It is a kind of fault that is very difficult to handle as the node's behavior is unpredictable. It also includes software and hardware faults.
- **Popular Distributed Consensus Algorithms**
    - Crash or Network Faults:
        - PAXOS
        - RAFT
    - Byzantine Fault (including Crash or Network Failures):
        - Byzantine fault tolerance (BFT)
        - Practical Byzantine Fault Tolerance (PBFT)

▼ **Paxos**

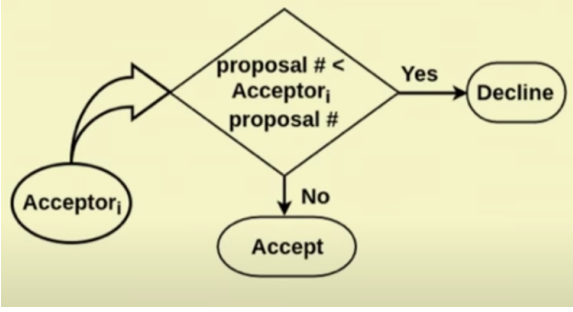
- It was the **first consensus algorithm proposed by L. Lamport in 1989.**
- The objective was to choose a single value under the crash or network faults.
- The main idea behind the Paxos consensus algorithm is straightforward, and we will understand it with an example.
  Let us consider that we are at the college and after classes, we are going to hang out all together. We have two options to hang out with classmates after classes: Subway and Coffee Cafe Day (CCD). So after classes, we can either go to Subway or CCD based on the collective decision, but everyone will go to the same place. In this case, there is no central leader. The only way to take a collective decision is that a few of them (in this case, max could be the two students) will propose an option (i.e., CCD or Subway). Others will either accept or reject that proposed option, and the majority count will be the final value, which will be the consensus.
- **Paxos: Types of Nodes**
    - **Proposer:** The proposer proposes values, and the consensus algorithm should choose that proposed values.
    - **Acceptor:** They form the consensus and accept the values. Whenever they hear a certain proposal from the proposer, the **acceptors either accept or reject the proposal**.
    - **Learner:** This learner will determine which value has been chosen by each acceptor and collectively accept that particular value.



- **Making a Proposal**
  - **Proposer Process**
    The proposer initially prepares a proposal number so that this number needs to be good enough for the proposal to be accepted by the acceptors. The proposal number forms a timeline, and the biggest number considered up to date.

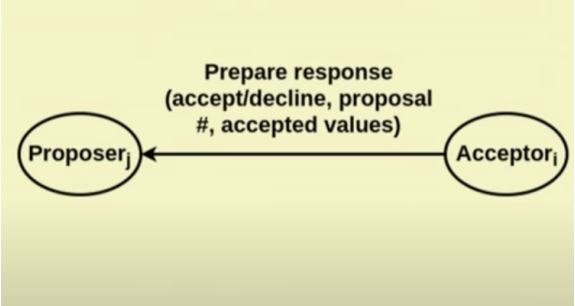


  - **Acceptor's Decision Making**
    If the received proposal number is less or equal to the already seen or received proposal number, then it rejects else it accepts. It means the acceptor compares the recently received proposal number with the currently known values for all proposer's received messages. If it gets the higher number, then it accepts; otherwise, it rejects.



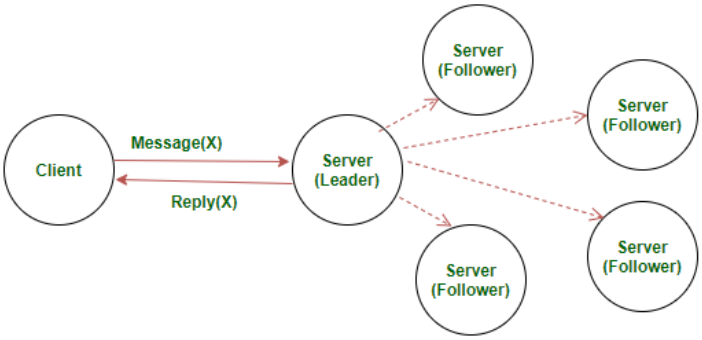
  - **Acceptor's Message**
    Acceptor prepares the response, including accept or decline status, biggest proposal number, and accepted values. The acceptor can either accept or reject a message based on the proposed algorithm. The acceptor includes the biggest number that the

acceptor has seen in the response message. It also includes the values that the acceptor has accepted to inform the proposer.



▼ **RAFT Consensus**

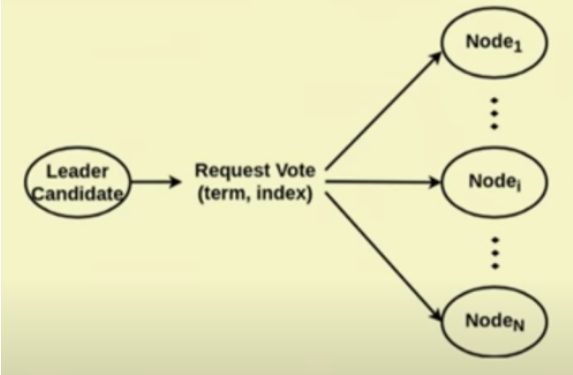
- The idea behind the Raft consensus algorithm is that the nodes (i.e., server computers) collectively select a leader, and the remaining nodes become the followers.
- The leader is responsible for state transition log replication across the followers under the closed distributed environment, assuming that all the nodes are trustworthy and have no malicious intent.
- The basic idea of Raft came from the fact that in a distributed environment, we can come to a consensus based on the Paxos algorithm and elect a leader.
- Interestingly, if we have a leader in the system, we can avoid multiple proposers proposing something altogether.
- In the case of Paxos, we don't have any straightforward mechanism to elect a leader. However, to elect a leader, multiple proposers propose the thing simultaneously. Consequently, the protocol becomes complex, and the acceptors have to accept one of the proposals from the proposer. In that case, we use the highest proposal number for the tie-breaking mechanism and embed a certain algorithm in Paxos to ensure that every proposal coming from a different proposer is unique. Thus, all these internal details make the Paxos more complicated.
- In a distributed environment and under a synchronous assumption (closed environment), it is possible to design a consensus algorithm. First, we will elect a leader and then the tasks of the leader to propose something. There will be a single proposer, and all the acceptors are followers of the leader. They may either accept or reject the leader's opinion.



- **Raft Consensus Algorithm**
  - **Electing the Leader: Voting Request**

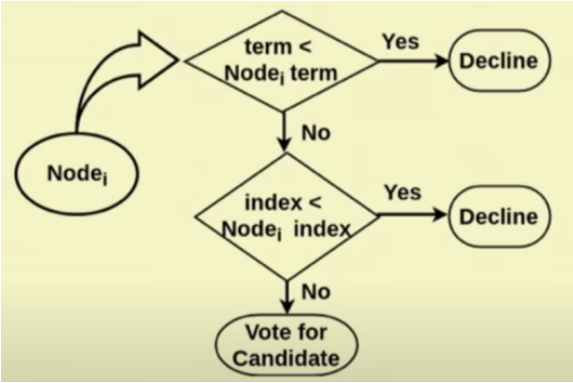
    The first part of the Raft is to elect a leader, and for that, there should be some leader candidates. The nodes sense the network, and if there is no leader candidate, then one of the nodes will announce that I want to be a leader. The leader candidate requests the votes. This voting request contains 2 parameters:

    - **Team**: The last calculated number known to candidate + 1.
    - **Index**: Committed transactions available to the candidate.



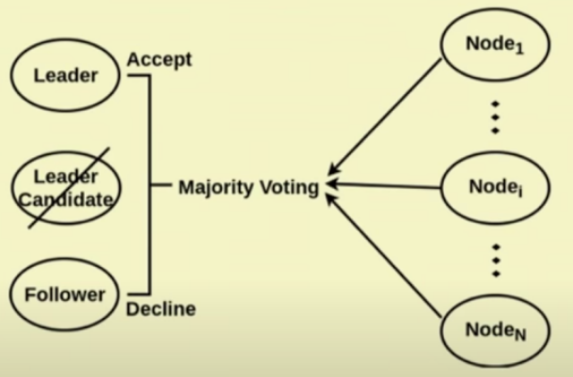
  - **Electing the Leader: Follower Node's Decision Making**

    Once the nodes receive a voting request, their task is to vote pro or against the candidate. So, this is the mechanism to elect a leader in the Raft consensus algorithm. Each node compares the received term and index with the corresponding current known values.



  - **Electing the Leader: Majority Voting**

    Every node sends their vote and candidates who get majority vote becomes a leader, and commit the corresponding log entry. in other words, If a certain leader candidate, receives majority of the vote from the nodes, then that particular candidate becomes a leader and other becomes the follower of that node.



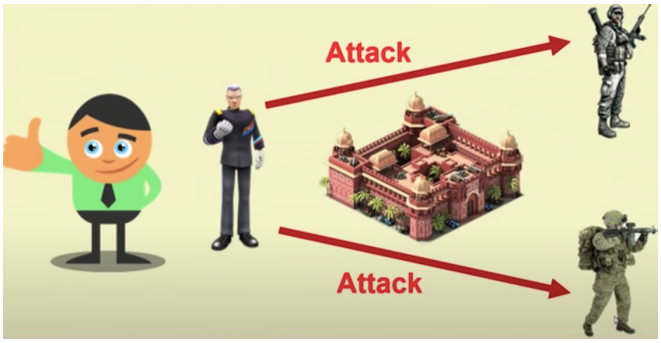
▼ **Paxos Vs. Raft Consensus Algorithm**

- The idea of Paxos was difficult to prove because the individual nodes propose certain values and the acceptors accept those values. However, there is no leader in the system, and individual nodes need to wait for a certain amount of time to see whether someone is proposing a value. If none of them proposes a value or timeout, then one of the nodes proposes a value, and the remaining nodes may accept or reject the proposal. If the node is getting a majority voting, then that node knows that its proposal is being accepted, and then it sends the accept message to all the nodes. If there are multiple proposers in the system, it becomes difficult to theoretically prove that the repeated execution of Paxos, which is called a multi-Paxos protocol, can achieve consensus in the closed distributed system.
- When the Paxos designed, there was no leader concept because electing a leader requires a consensus algorithm. But, once the system has a leader, the entire system becomes streamline. The Raft algorithm improved the concept proposed in Paxos. It is like, rather than going for repeated Paxos or multi Paxos, it preferred leader election based on the majority voting.
- In Raft, it first runs a Paxos type of algorithm to elect a leader. But, once a leader is elected, the elected leader can execute a series of transactions until either leader dies or fails. However, in Paxos, the multi-Paxos algorithm needs to run for consensus for executing each transaction.
- The Raft consensus algorithm has improved the concept of leader election and made it easy to understand and easy to prove theoretically.

	Raft	Multi-Paxos
Leader	Strong leader	Weak leader
Voting rights for the leader	Have a replica of the latest committed log	Arbitrary replica
Log replication	Guaranteed continuity	Allow voids
Log submission	Push forward the commit index	Asynchronous commit messages

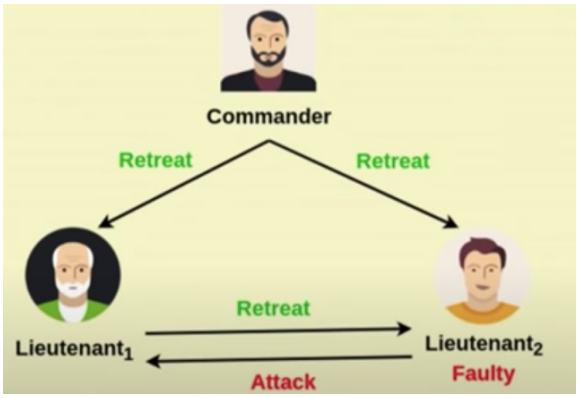
▼ **Byzantine general problem**

- Paxos and Raft consensus algorithm can tolerate up to N/2 – 1 number of Crash or Network fault, where N is the total number of nodes in the network. However, what if the nodes behave maliciously? This particular class of fault is called Byzantine fault, and the Byzantine fault came from the interesting Byzantine Generals Problem.
- Let us understand this concept with an example: The army wants to attack a certain fort, and this mission is lead by the army General, having two troupes. So, based on the scenario, the General can either make an order to attack from different sides or retreat. When the General is trustworthy, he orders the same to both the troupes.

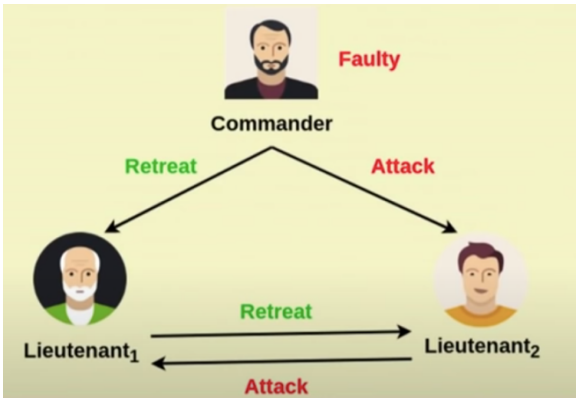


- However, when the General is malicious. The General sends an attack message to one troupe and a retreat message to another troupe. If the General becomes faulty, it becomes difficult for them to find out what to do. This particular problem is called the Byzantine Generals Problem, where a particular node can behave maliciously.

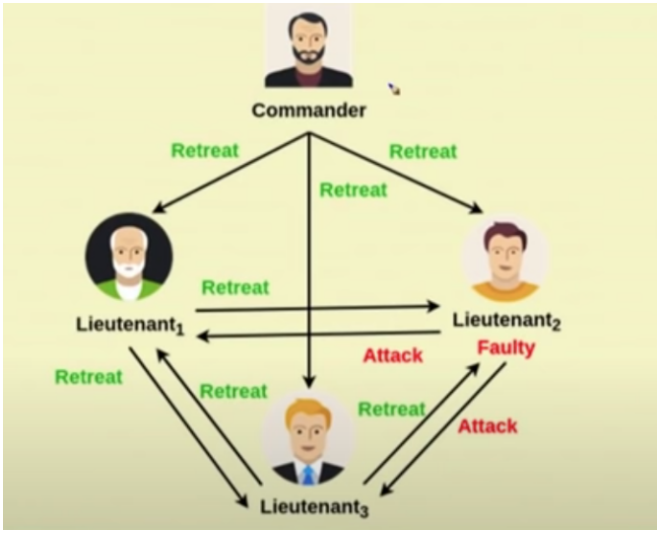
- **Three Byzantine Generals Problem**
  - **Lieutenant Faulty**



- **Commander Faulty**



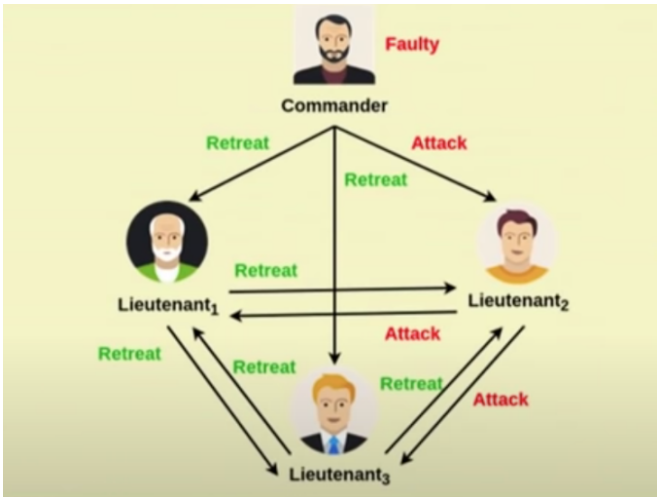
- **Four Byzantine Generals Problem**
  - **Lieutenant Faulty**



If they go for the majority voting principle, they can analyze and decide to retreat. This is illustrated as follows:

- Lieutenant (1) = {Retreat, Attack, Retreat) = Retreat
- Lieutenant (3) = {Retreat, Attack, Retreat) = Retreat

- **Commander Faulty**



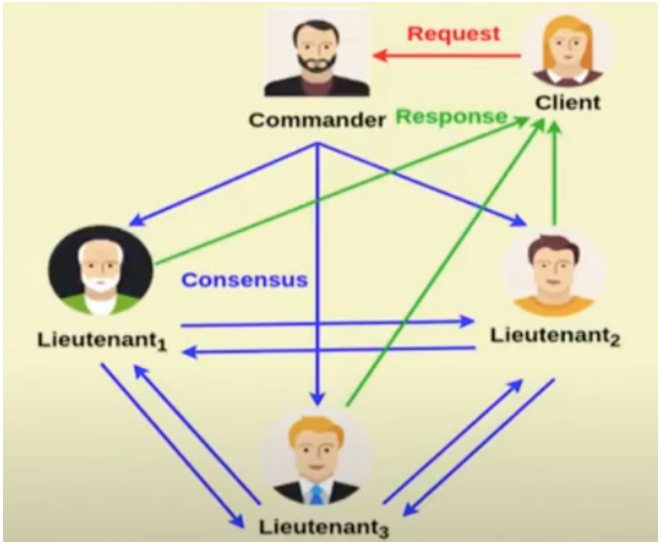
  - Lieutenant (1) = {Retreat, Attack, Retreat) = Retreat
  - Lieutenant (2) = {Retreat, Attack, Retreat} = Retreat
  - Lieutenant (3) = {Attack, Retreat, Retreat) = Retreat

▼ **Practical Byzantine Fault Tolerant (PBFT) system**

▼ **BFT over Asynchronous systems**

- Asynchronous byzantine fault tolerance (ABFT) is a property of Byzantine fault tolerant consensus algorithms, which allow for honest nodes of a network to guarantee to agree on the timing and order of a set of transactions fairly and securely.

- The algorithm is practical as it ensures safety over an asynchronous network but not liveness; otherwise, it will violate the impossibility theorem.
- However, liveness can be ensured under the weaker assumption.
- The system can also ensure Byzantine failure, and it has low overhead.
- For these properties, this algorithm is widely used in permission blockchain applications such as Tendermint, INB's Openchain, ErisDB, Hyperledger, etc.



- The broad idea about the system is as follows: A client submits the request to the commander. The commander and lieutenants are the special kinds of nodes designated to run the consensus algorithm. Once the system comes to the consensus, it sends a response back to the client whether the system has accepted the request submitted by the client or not.
- The basic assumption about the system and working environment: The system works in an asynchronous distributed system, and it can tolerate delay and out-of-order messages. It can also handle Byzantine failure where arbitrary nodes behave maliciously and privacy, tamper-proof message, and authentication.
    - The state machine is replicated across different nodes.
    - 3f + 1 replicas are there, where f is the number of faulty replicas.
    - The replicas move through successive configurations, known as views.
    - One replica is a view is primary, and others are backups.
    - Views are changed when a primary is detected as faulty.
    - A unique integer number v identifies every view.
    - Only the messages from the current views are accepted.

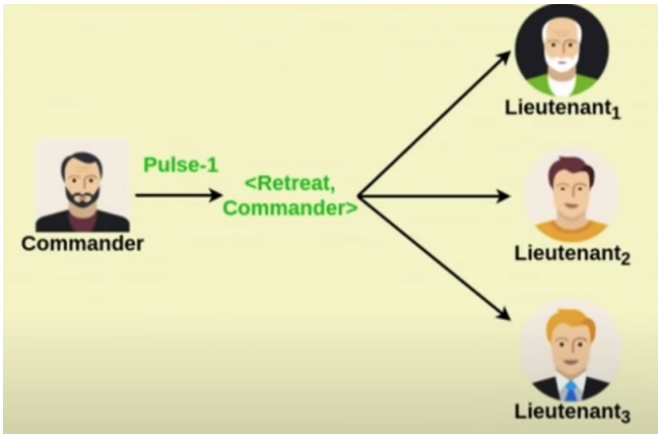
https://notepub.io/notes/blockchain-technology/permissioned-blockchain/what-is-permissioned-blockchain-practical-byzantine-fault-tolerance-algorithm/

▼ Lamport-Shostak-Pease BFT Algorithm

- The main idea behind this algorithm is: There is a commander and N lieutenants. The commander initiates the process and sends an initial message to all the lieutenants in the closed network. Later, each lieutenant forwards the value received from the commander to the other lieutenants except the sender. So at the end of the rounds, all the lieutenants must be having N-1 values, except the offline lieutenants. In the end, they will apply the majority voting principle and achieves the consensus. This is one of the first algorithms for Byzantine Generals' Problem.

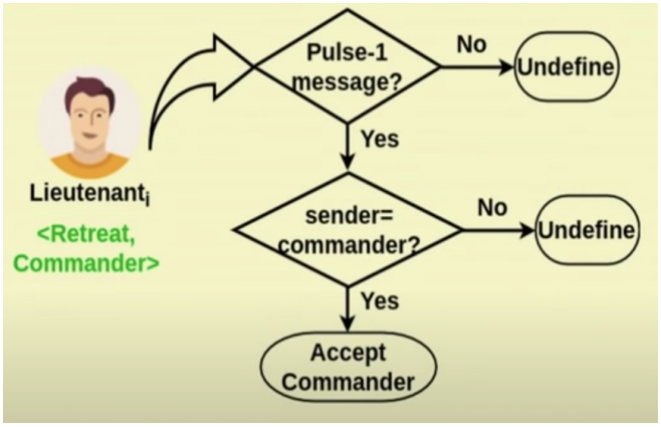
- **Base Condition for Commander**

  Pulse-1 is the initial pulse where the commander sends the message to all the Lieutenants. Broadcast (N, t=0), where N is the number of processes and t is the algorithm parameter, denotes the individual rounds. The Commander decides his own value, and in this case, the possible values are {retreat, attack}. In this example, N = 3 has three different lieutenants and is trying to reach a consensus.



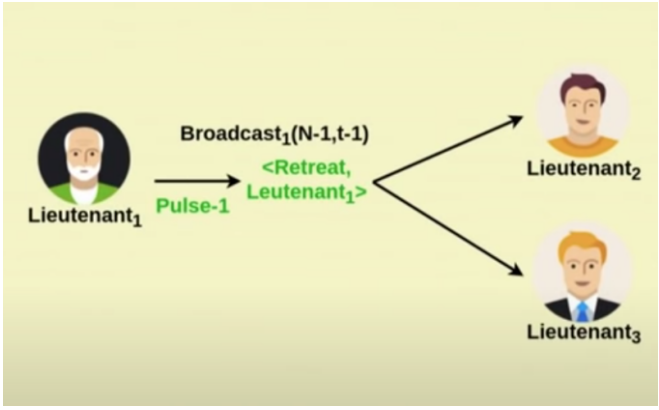
- **Base Condition for Lieutenant**

  Each lieutenant receives the message from the commander and checks whether it is a pulse-1 message or not. If it is a pulse-1 message, and the sender is the commander, accept it; otherwise, wait for a pulse-1 message. Suppose a pulse-1 message is received then broadcast this message to all other processes in the network.



- **General Condition for Lieutenant**

  All the lieutenants broadcast their values to the other lieutenants except the senders. At the end of the rounds, all the lieutenants must be having N-1 values, except the offline lieutenants. In the end, they will apply the majority voting principle and achieves the consensus.



In this agreement Protocol, after N rounds, each process must be having the N values; this is because the system is synchronous and having a reliable communication medium. Once they have, N values can apply the majority voting principle and achieve the consensus. However, to achieve consensus, the system should satisfy the below condition.

- The system must have a minimum of three lieutenants (N =3) and a commander. So, out of N number of processes (lieutenants), maximum of F number of the processes can be faulty, and F + 1 number of processes must be non-faulty such that N = 2*F + 1.
- The system should be fully connected, and the receivers always know the identity of the senders.
- The system should be synchronous and having a reliable communication medium.

UNIT 4 - Enterprise application of Block chain

▼ Cross border payments

Blockchain technology in cross-border payments can enable secure transfers between an infinite number of bank ledgers. This allows one to bypass banking intermediaries who serve as middlemen to help transfer money from one bank to another. The transaction is secure, quicker, and cheaper and has end-to-end visibility anywhere in the world.

The use of blockchain technology in cross-border payments is very different from existing methods such as SWIFT. Even SWIFT's new GPI (global payments innovation) relies on the same unidirectional messaging, which means that it is not connected to any underlying settlement process. Such a system has its drawbacks, where individuals can manipulate the banking system to commit fraud. A case in point was the Punjab National Bank fraud case, where INR 14,356.84 crore was stolen because perpetrators of the fraud made unauthorized transactions on the SWIFT network, where payment messages sent were not linked to the system that actually settled the transaction.

There are no such issues for payments processed on the blockchain. Any transactions can be settled instantly. Using the bidirectional messaging and settlement component employed in blockchain solutions, such as Ripple's, ensure that the transaction is validated on the blockchain before the funds are transferred across the ledgers of transacting parties. If for some reason the payment does not go through, both banks are immediately notified and no funds are transferred.

The use of digital assets (sometimes called crypto-currencies) such as XRP (an independent digital asset) can help financial institutions convert funds into the desired currency instantly. Given that India has the largest diaspora population in the world, this means that banks often deal with currency pairs such as SAR/INR to USD/INR. Sourcing liquidity for payments into and outside India can be onerous and costly, and the use of XRP as a bridge asset for currency conversions takes just minutes and is cheaper than what it would cost if one did a traditional fiat- -fiat to exchange. Additionally, the ability to do this in real-time would also reduce a financial institution's exposure to forex volatility as well.

Blockchain—The cross-border payments for India

Blockchain can help India's financial institutions develop world-class payment platforms. Banks and payment providers are aware of the pain points in facilitating cross-border transactions, and have made some progress in addressing them. In India, blockchain technology has been adopted by banks to help improve the payments experience for its customers. For example, last year, YES BANK has signed a partnership with Ripple to help facilitate inbound remittances from North America, the Middle East and the United Kingdom.

Apart from facilitating greater efficiencies in existing payments infrastructure, there is much to be said about what blockchain can do for India and its people. Let us consider its benefits at a more human level. For example, let's say an Indian construction worker in Dubai urgently needs to transfer funds back home for a medical emergency his family is experiencing. If his bank used blockchain technology, the remittance transfer could be completed within minutes, with fees that are significantly lower than existing methods of transferring money. Had the conventional means of cross-border payments been used, it would have taken 3-4 days, with the money going through multiple intermediaries and incurring extra fees, before finally reaching the worker's family.

Blockchain can also allow a bank's customers to use their more efficient cross-border payments service and reduce their dependency on hawala brokers, where fees can also be quite high, while improving financial inclusion amongst the Indian populace as well.

Such instances highlight the centrality of remittances to India's economy, where the World Bank has stated that India is the world's largest recipient of remittances worldwide (at about INR 4.6 trillion a year). From a macro- economic perspective, inbound remittances are often used by families for household purchases and investments. The rise in consumption levels will in return create a ripple effect, driving growth in other industries as well. Therefore, the importance of cross-border payments cannot be understated in India, and it is imperative that financial institutions look closely on leveraging blockchain technology for the broader purpose of socio-economic development.

Although much of the current debate on blockchain revolves on its 'disruptive' element and focuses on how it seeks to challenge the status quo, innovative cross- rder payment solutions built on blockchain bo technology are not here to replace financial institutions, nor do they seek to circumvent financial regulations. Blockchain technology can enable banks to improve and future-proof their cross-border payments services.

Going back to Mr Modi's address to world leaders and global CEOs at the World Economic Forum, he said: "This technology-driven world has influenced every aspect of our lives ...

Technology has the ability to bend, break and link...” With blockchain technology, we bend and break the existing system, and link the world more seamlessly through cheaper, faster and better cross-border transactions of funds. Blockchain can have a transformative impact on how cross-border payments are conducted, augmenting and reshaping entire financial infrastructures of countries.

The financial ecosystem needs to be looking at implementing thoughtful regulations that can encourage innovative solutions for cross-border payments. At the same time, any implementation of blockchain technology should be done responsibly, with a careful amount of deliberation over the security, risk and stability of cross-border payments solutions. This is the right way on how financial institutions and policy makers can reap maximum benefits with blockchain.

▼ **Know Your Customer (KYC)**

- KYC is a process by which banks obtain information about the identity and address of the purchasers.
- It’s a regulator governed process of performing due diligence for verifying the identity of clients. This process helps to make sure that banks’ services aren’t misused. The banks are responsible for completing the KYC procedure while opening accounts. Banks also are required to periodically update their customers’ KYC details. KYC may be a manual, time-consuming, and redundant across institutions. Sharing KYC information on Blockchain would enable financial institutions to deliver better compliance outcomes, increase efficiency, and improve customer experience.
- KYC processes are the backbones of a financial institution’s anti-money laundering efforts. Find out how businesses are revolutionising the long, tiresome process. Know Your Customer or KYC processes are the backbones of a financial institution’s anti-money laundering efforts.
- **According to current estimates, the amount of KYC spending rose to up to $1.2 Billion in 2020 on a global level.**
- With a whopping amount as this being spent on making KYC processes better, it is easy to assume that the process would be unhackable and issues-free. But inspite of the importance of the process, KYC continues to operate inefficiently. Clenched by labor-intensive and time-consuming tasks, the high scope of effort duplication, and the risk of error, it is estimated that 80% of KYC efforts go on gathering information and processing while only 20% of efforts are assessing and monitoring focused.

Key Problem Areas and Solution Benefits

- **Redundancy:** Most large files use similar data and processes to verify an equivalent client. is to The solution benefit eliminate the redundancy documentations that got to be verified only once before the approval information is shared.
- **Inefficiency:** Manual and time-consuming process to collect and verify documentary evidence. is to The solution benefit extend automation where documents and approvals are digitized and may be verified without manual intervention.

- **Lack of specificity:** Requirements for due-diligence are often fuzzy, creating uncertainty on compliance to avoid legal sanctions. is to standardize process i.e. The solution benefit standardized, automated KYC processes sanctioned by the regulators.

▼ **Food Security**

With global-scale food systems such as seafood, nearly 40 per cent of which is traded globally, data transparency and traceability through technologies like blockchain are important for socially and environmentally conscious decision making and to facilitate trust among stakeholders.

Global food supply chains proved brittle during the COVID-19 pandemic, leading for calls to boost the resilience of global food supply chains through improved efficiency in production, distribution and consumption of nutritious food. How could technologies like blockchain that provide data to producers, distributors and consumers be part of the solution? Big data applications may present opportunities to address inefficiencies from farm to table and improve global food security. Blockchain, a linked decentralized database that stores auditable data throughout entire supply chains, may change the game for food producers across the globe.

Blockchain agriculture means the use of blockchain in the agricultural sector to improve the operating process and get profitable results. The use of blockchain in the agricultural sector ranges from having a sustainable business and reduction of waste, to informed consumer purchasing decisions, to having smooth future transactions with fraud elimination. There is a new term that has surfaced in the marketplace, Smart Agriculture. Smart agriculture includes the utilization of natural resources and the decrease of environmental impact through the execution of ICTs (information and communication technologies), blockchain, and other modern technologies for gathering and analyzing data.

How it impacts in food security?

- **Gathering information:** Blockchain technologies can be used to consolidate information on the quality of the seed, track how crops grow and record the journey once it leaves the farm. In Canada, for example, **Grain Discovery - an online blockchain marketplace** - is an example of data being leveraged by those involved in the food system to grow and market globally competitive crops. The data could enhance transparency in supply chains by providing immutable records from production to consumption. Such data have the potential to facilitate information transfer throughout every step of the supply chain. And if blockchains are implemented with proper validation, it can **prevent illegal and unethical production and distribution** that undermines sustainability and community food security. This transparency also means consumers could make informed decisions to protect vulnerable producers and the environment. Access to product data may allow consumers to reward producers who employ good practices, such as rural smallholder farmers and fishermen who are among the most food-insecure groups.
- **Tracking pathways:** Currently, there is little evidence supporting the claim that blockchain and big data technologies are contributing to global food security. Even though the average farm is projected to generate 4.1 million data points by 2050, up from 190,000 data points in 2014, increases in global food security have not been impressive. Part of the challenge is how blockchains have been implemented until now. The corporate control of blockchains and big data platforms could even undermine food security. , **IBM For example and**

Walmart have teamed up to track produce from farm to fork. Producers and processors along the supply chain are required to input information into IBM's blockchain for the process to be entirely transparent to consumers. Traditional blockchains are decentralized and democratized in order to ensure trust between users. Corporate control of supply chain information could also leave out small-scale farmers that lack the required size, scale and technological know-how to participate. This division between large and small food producers can contribute to global food insecurity, and many researchers believe that small, as well as large farms, are required to feed the world's growing population.

- **Data and Food futures:** Before blockchain and other data technologies can help address food security, a number of challenges need to be addressed. The implementation of blockchains must be be decentralized to include small farmers and rural people. This will enable sustainable and equitable food systems and allow consumers to make informed decisions. However, as blockchains place additional responsibility on the end users, challenges such as limited digital literacy among the world's poor and infrastructure constraints may undermine true decentralization. Also, they must be integrated into broader food security promotion strategies to make them sensitive to social and environmental values critical to tackling food insecurity among diverse groups. **The untapped potential of harnessing big data through a transparent and decentralized food distribution system may support sustainable food production and provide accountability for food production.** This is crucial for efficient food systems and food security in the future. But it is important that these innovations are deployed equitably so that all stakeholders along the value chain may benefit.
- **Food Inventory Management:** Truth be told, many food organizations aren't prepared to utilize cutting edge technology to deal with their inventories. This is actually leading to wastage of the produce and the resources. Also the losses are borne by farmers. Thus, this is a huge burden for the farmers, as they don't have the required tools to manage the issue. The use of blockchain technology here can change that situation for great. Blockchain in inventory management can help farmers by monitoring the storage climate and inform you when produce will expire. In this way, you can take legitimate measures.

▼ **Mortgage over Block chain**

The mortgage industry is a relatively slow-paced industry when it comes to its various stages and processes. There's a lot of friction between each stage that makes it cumbersome to issue a loan. However, with the advent of blockchain technology, the industry has been revolutionized to quite an extent.

Blockchain technology is rapidly penetrating several industries such as finance, fashion, pharmaceuticals, and more. It can do so because of its efficient functioning structure that makes processes simpler, faster, and more reliable. Blockchain technology is acting as the fundamental framework upon which businesses are building their processes. The mortgage industry, being one of the slower sectors, has immense scope for improvement. Blockchain can cause this improvement by paving the way for a digital mortgage.

The US mortgage system is primed for rapid process and technology change, driven by shifting demographics, rising consumer expectations, technological innovations, increased regulatory expectations, and outdated legacy infrastructure. Collectively, these factors require

homebuyers, governments, and real estate and mortgage-related companies to reimagine US housing finance and homeownership. In response to these trends, digital mortgage, and housing finance solutions are forming across the US at unprecedented speed and scale.

Role Of Blockchain In The Mortgage Industry

- **Conventional Mortgage Process**
  In a conventional scenario, there are several steps involved while getting a mortgage. First and foremost, one has first to be eligible to apply. They then have to fill an application which will later be verified. Once all this has taken place, and it all goes right, a loan would be approved and sanctioned. This is a long process that easily takes about a month to two. During this, several actors are involved at various stages, which gives room for many inefficiencies and risks. There's a lot of time taken, there's a risk of improper documentation, and since it is all manually done, there's a lot of room for human error. These challenges can be solved using blockchain.
- **Mortgage Process Using**
  Blockchain One will first fill an application which will become a block. The application will be verified by not one person/authority but several nodes. After the verification, this said application will be added to the chain. The person will then need to sign and accept this loan, following which funds would be transferred to them from the entity supplying it. So, a process that takes at least 30 days will finish in a matter of days and is made entirely digital. Thus using blockchain tech as the base framework, mortgage software, and consumer lending software can be developed.

Benefits Of A Digital Mortgage

- **Better record keeping:** Each step of the process is stored as a record, and these records are on a decentralized ledger. This means there's no one central hub that manages it all. Thus, there's proper proof of all the actions that is quite difficult to tamper with. So, it becomes easier to verify all actors such as the loan borrower, the seller, and entities that approve the loans.
- **Cost efficiency:** It becomes relatively economical for one to get a mortgage compared to the conventional process, where they'd have to pay a third party to streamline the process. Here, they can do it all on their own, without any intervention from an outsider.
- **Instant Settlements:** Usually, transferring funds takes time. With this, the person will get their funds right away without having to wait.
- **Smart Contracts:** A smart contract is a set of rules that are automatically set in motion when an event occurs. It can be applied in the verification and approval process such that the rules are initially fed along with criteria. If the application follows these rules and meets the criteria, it is approved, else it's not. This way, the complete verification process can be executed automatically instead of manually carried out by multiple actors.

▼ **Block chain enabled Trade**

The trade finance industry has emerged as a key focus area for realizing the efficiencies of blockchain technology. Blockchain has the potential to disrupt the trade landscape by making it easier to reduce disputes and fraud to provide delivery and payment certainty, enable

transparency of trade asset movement, and facilitate the flow of trade receivables. The result: increased collaboration, automation and oversight in trade transactions. Trade finance by banks and other financial institutions is a vital function in international commerce, as it provides delivery and payment assurance to buyers and sellers, and it helps close the trade cycle funding gap for these parties. The growth and sustenance of the $16 trillion international trade market depends on the easy availability and robustness of financing mechanisms. For this reason, trade finance is often described as the fuel for global commerce.

Blockchain enables data to be recorded in a secure digital format by providing real-time information on transactions between different parties, be they corporations, supplier networks, investment pools, or an international supply chain. It provides all parties with a record that is secure, encrypted, transparent, easy to access, and impossible to tamper with. Although blockchain emerged within the financial system with the launch of cryptocurrency Bitcoin, today it is used in a wide range of activities, including ones that are directly or indirectly related to foreign trade. The long value chain tied to international trade includes vast, complex areas like logistics, transportation, customs administration, financing, and administrative procedures between firms, all of which could be streamlined by adopting this technology.

Blockchain optimizes processes, makes goods traceable, guarantees the security of payments and financing, facilitates the verification of digital quality and origin certifications, enables real-time sharing of information on the different stages of trade, and helps improve how related public and private services operate, among other benefits. Blockchain provides solutions for trade operations by simplifying cross-border trade, contributing to competitive improvements, and reducing transaction costs. Although blockchain has been used within foreign trade for several years, its significance has increased since the start of the COVID-19 health crisis and it is expected to play an even more prominent role in the post- pandemic world.

Benefits of blockchain enabled trade

- Lower risk and operational costs: Quickly process credits and guarantees electronically, gain deep insights into client financial positions and transaction histories, and monitor transactions from start to finish.
- Find new opportunities and markets: Discover revenue opportunities through a new class of transparent, risk-mitigated and standardized trade finance and trade credit insurance solutions.
- Establish leadership in a new era of trade: Foster greater trust and transparency in cross-border trading. Enjoy first-mover advantages by convening new trade networks and creating new trading hubs.
- Leadership in trade facilitation: We’re reinventing complex trade processes to help start, accelerate and innovate blockchain networks including the successful production development of — we.trade, now comprised of 15 banks across Europe.
- Trusted business expertise: IBM knows trade and trade processes, complex systems integration, regulated industries, and — with 500+ client engagements to date how to unlock — blockchain value. We provide the entire stack to run your business.

▼ **We Trade – Trade Finance Network**

Blockchain in Trade finance serves as the lifeblood of international trade in goods and services by enabling transactions between buyers and sellers worldwide. Trade finance provides the credit, payment guarantee, and insurance needed to facilitate the transaction on terms that would satisfy all parties. One of the difficulties involved with trade finance is the large volume of paper documents that make up much of the information flow between trading parties.

Most of the trade finance activities involve a substantial amount of physical paperwork being shuffled back and forth between the importer, exporter, importer's bank, exporter's bank, shipping company, receiving company, local shippers, insurers, and others. This reliance on documents usually has drawbacks, including the cost and time required to prepare, transmit, and check these documents. Paper documents may also be open to errors and even forgery.

Furthermore, the COVID-19 outbreak has impacted different trade finance steps, including deal origination and distribution, negotiable instruments, document transmission, authorized signatures, and shipping. Nowadays, several banks and financial institutions worldwide are trying to quickly scale their digital initiatives to move toward a world where digitalization is central to every interaction. Banks are looking to utilize technology to streamline trade by creating digital ecosystems that reduce costs and increase trade finance efficiency by replacing paper with digital data flows. The International Chamber of Commerce (ICC) survey conducted in April 2020 indicated that banks are focusing on the rapid adoption of blockchain, the digitization of documentation, and automated processing and handling software in response to the COVID-19 pandemic.

How trade finance works?

Trade finance could be understood by the following example. Let's assume that there is a company named MHW in India and this company wants to import a certain number of goods from a supplier company that is located in the United States. Let's name this supplier company as SSI. Now to import the goods the company MHW needs to pay for the goods, but it wants to make sure that the goods should arrive as ordered and thus is hesitating in processing the payment. Now on the same hand, the exporter is also hesitant to ship the goods, without being certain that the payment will arrive for the goods they supply.

Now at this step, the banks get involved to solve the issues faced by the importer and exporter company. The importer's bank issues a letter of credit to the exporter via the exporter's bank and promises to pay the required amount once the exporter bank provides the valid documents proving the ordered goods have been loaded to the ship or any other means of transport. Thus the involved banks ensure that the trust is being built between the importer and exporter parties by holding the money for each party.

Benefits of Blockchain in Trade Finance

The key benefits of blockchain technology in trade finance is that it can reduce processing time, eliminate the use of paper, and save money while ensuring transparency, security, and trust. Removing intermediaries from the process removes the risk of manipulation by the participants in the process.

Here are some major points demonstrating the advantages of blockchain in trade finance:

- **Efficiency:** Blockchain technology makes the trade finance process more efficient by completing the transactions directly between the relevant parties with no intermediary and

with digitized information. With blockchain, the parties can operate smart contracts that trigger commercial actions automatically. This allows to dramatically streamline trade finance processes, thereby cutting costs and increasing the transaction speed.

- **Traceability:** With blockchain technology, the importers and exporters can track goods and assets and where they are currently residing. Also, related asset information can be received from the previous and pass on to the new owner for possible action. This allows new financing opportunities and can improve the perfection of an interest in the trading of goods. This is considered one of the main benefits of blockchain in trade finance.
- **Transparency:** Blockchain, being a distributed ledger technology can record multiple details of the transactions against commercial agreements and can distribute the data to improve further trust. This allows reducing the risk of tampering the records and offers more options for financing trade.
- **Auditability:** Utilising Blockchain each trade finance transaction can be recorded sequentially and indefinitely. This provides a lasting audit trail for the life of the traded asset as well as better verification of assets authenticity with a reduction of compliance costs.
- **Security:** Each transaction within the trade network is verified using independently verified cryptography. The encryption and cryptographically protected keys securely transmit data between different financial institutions and thus privatize the data.

▼ **Supply Chain Financing**

Supply chain finance and blockchain technology is revolutionizing businesses around the world. As businesses expand, they build new domestic and global ties to strengthen their procurement process and find more affordable yet better solutions. While this bodes well for buyers' balance sheets, it can trigger working capital concerns. Valuable capital may get locked into supply chains, forcing businesses to scramble for solutions.

Supply chain finance is a creative way out that can help buyers as well as their suppliers. Using a supply chain finance provider, buyers can pay their suppliers early and lengthen their payment terms. Besides assisting buyers in optimizing their working capital, supply chain finance also provides an affordable way for suppliers to get cash.

However, despite these features, supply chain finance does not solve everything. For instance, it is usually reserved for the top suppliers. Small and medium-sized enterprises are left out, which is unfair as they could benefit significantly from early payments.

Fortunately, the relevant stakeholders are aware of these problems and have looked at different tools to improve supply chain finance. Many proposals have been presented, but none look better (at least right now) than using blockchain to enhance supply chain finance.

How can blockchain improve supply chain finance?

The intersection of supply chain finance and blockchain technology has remarkable benefits for the relevant stakeholders. Some of these include:

- **It increases authenticity in the supply chain**

  Supply chain finance is a massive web involving many stakeholders. From buyers to suppliers and intermediaries, there are many interested parties, and the exchange of

information is not always transparent. Each stakeholder may prioritize their needs over others, triggering delays in the supply chain.

Blockchain can solve this problem. Copies of the same digital ledger, which keeps the records in the network, are distributed among the stakeholders, who have access to the same information. The immutability of blockchain prevents confusion and ensures transparency and authenticity in the network. It can enhance supply chain management and smoothen the supply chain.

- **Brings inclusivity to the ecosystem**

  The existing supply chain finance ecosystem has shortfalls, especially regarding financial inclusion. Supply chain financiers usually offer to fund buyers' top 10 to 50 suppliers, leaving behind many small and medium- sized enterprises. This is unfair, as smaller suppliers can benefit more from early payments through buyer-led supply chain finance than larger counterparts.

  Blockchain technology has the potential to address this issue and make supply chain finance available to everyone. The nature of the blockchain network can allow supply chain finance providers to fund invoices sent by all the suppliers.Every transaction and information exchange is recorded on the ledger, so finance providers do not have any reason to limit financing to only the top suppliers.

- **Redefines financiers in the supply chain**

  Financial institutions are generally the financers in buyer-led supply chain finance. They are the ones that make the invoice payments to the suppliers. Buyers pay them back through a repayment plan consisting of the borrowed sum along with a small fee and interest.

  While financial institutions will remain relevant in buyer-led supply chain finance, blockchain could open up the system to other stakeholders in the ecosystem. Corporate foundations and individual investors could also participate in supply chain finance and earn returns on their investment. Platforms like CredSCF are already using blockchain to allow different financiers to leverage supply chain finance to earn returns.

- **Enhances the functioning of the supply chain**

  Information exchange is always an issue when there are many parties involved. Supply chain finance has suffered from the same ailment. Information inaccuracy is, in fact, one of the significant reasons why supply chain finance has struggled to solve the age-old issues in the supply chain.

  However, using blockchain technology in supply chain finance might be the answer. The digital, immutable ledger can keep track of information exchange, asset transfer, product quality, and timelines to smoothen the supply chain. It can reduce lags in the system, saving money and time for all the stakeholders.

▼ **Identity on Block chain**

Also known as "identity and access management", or IAM, identity management comprises all the processes and technologies within an organisation that are used to identify, authenticate and authorize someone to access services or systems in that said organisation or other associated ones.

Examples of this would range from customers and/or employees accessing software or hardware inside a company/enterprise – and the level of access, privileges and restrictions each user has while doing so – or, in a governmental setting, the issuing and verification of birth certificates, national id cards, passports or driver's licenses (that allow a user/citizen to not only prove his identity but also access services from the government and other organisations).

The problem with current Identity Management Systems

Identity has a problem. If it's paper-based, such as birth certificates sitting idly in a basement of a town hall, it's subject to loss, theft of fraud. A digital identity reduces the level of bureaucracy and increases the speed of processes within organisations by allowing for a greater interoperability between departments and other institutions. But if this digital identity is stored on a centralised server, it becomes a target for hackers. Since 2017 alone, more than 600 million personal details – such as addresses or credit card numbers – have been hacked, leaked or breached from organisations. Most of the current identity management systems are weak and outdated.

Identities need to be portable and verifiable everywhere, any time, and digitization can enable that. But being digital is not enough. Identities also need to be private and secure.

Several industries suffer the problems of current identity management systems:

- Government: The lack of interoperability between departments and government levels takes a toll in the form of excess bureaucracy. Which, in turn, increases processes' times and costs.
- Healthcare: half of the world's population does not have access to quality healthcare. The lack of interoperability between actors in the healthcare space (Hospitals, clinics, insurance companies, doctors, pharmacies, etc) leads to inefficient healthcare and delayed care and frustration for patients.
- Education: It is estimated that two hundred thousand fake academic certificates are sold each year in the USA alone. The difficulty in verifying the authenticity of these credentials leads to hiring of unqualified professionals, brand damage to the universities and the hiring companies.
- Banking: the need for login details such as passwords decreases the security of banking for users.
- Businesses in general: the current need to store clients' and employees' personal data is a source of liability for companies. A personal data breach may result in huge fines due to GDPR infringement – such as the British Airways case – or simply due to customer trust loss and consequential damage to the organisation's brand.

How Blockchain brings privacy and security to Identity Management

Through the infrastructure of a blockchain, the verifying parties do not need to check the validity of the actual data in the provided proof but can rather use the blockchain to check the validity of the attestation and attesting party (such as the government) from which they can determine whether to validate the proof.

For example, when an identity owner presents a proof of their date-of- birth, rather than actually checking the truth of the date of birth itself, the verifying party will validate the government's

signature who issued and attested to this credential to then decide whether he trusts the government's assessment about the accuracy of the data.

What are the challenges that exist in the traditional identity management system?

The present identity management system faces the following four major challenges:

1. **Identity theft**

   People share their personal information online via different unknown sources or services that can put their identification documents into the wrong hands. Also, as online applications maintain centralized servers for storing data, it becomes easier for hackers to hack the servers and steal sensitive information. According to the Breach Level Index, 4,861,553 records are stolen every day, accounting for:

   - 202,565 records every hour
   - 3,376 records every minute
   - 56 records every second

   The breach statistics indicate how quickly a hacker can steal personal or other confidential information.

2. **A combination of usernames and passwords**

   While signing up on multiple online platforms, users have to create a unique username and password every time. It becomes difficult for an individual to remember a combination of usernames and passwords for accessing different services. Maintaining different authentication profiles is quite a challenging task.

3. **KYC Onboarding**

   The current authentication process involves three stakeholders, including:

   - verifying companies/KYC companies
   - users
   - third parties that need to check the identity of the user

   The overall system is expensive for all these stakeholders. Since KYC companies have to serve requests of different entities such as banks, healthcare providers, immigration officials, etc., they require more resources to process their needs quickly. Therefore, KYC companies have to charge a higher amount for verification, which is passed to individuals as hidden processing fees. Moreover, third-party companies have to wait for a long time to onboard the customers.

   A global survey of "Know Your Customer" challenges found that global annual spending on KYC is estimated as the US $48million.

4. **Lack of Control**

   It is currently impossible for users to have control over personally identifiable information (PII). They do not know:

   - how many times PII has been shared without their consent

- where all their personal information has been stored

As a result, the existing identity management process requires an innovative change. Using blockchain for identity management can allow individuals to have ownership of their identity by creating a global ID to serve multiple purposes.

Blockchain offers a potential solution to the above challenges by allowing users a sense of security that no third party can share their PII without their consent.

By using blockchain:

- a platform can be designed to protect individuals' identities from breaches and thefts
- people can be free to create self-sovereign and encrypted digital identities
- the need for making multiple usernames and passwords can be removed

Now, let's understand how could Blockchain Identity Management work

Currently, people need the right way to manage their identity than paper- based documents. The app for Blockchain Identity management will help people to verify and authenticate their identity in real-time.

Step 1: Installation of Mobile App

An individual will first have to download the mobile app from the play store or app store to establish his/her identity.

After downloading the app in mobile phones, a user will create a profile on the app.

Once the profile is created, the user will get the unique ID number, which will help organizations access the user's identification documents.

Step 2: Uploading the documents

After the user gets ID number, they need to upload the government-issued IDs on the app that will be saved in the IPFS with hashed addresses stored in the blockchain.

The app will extract the personal information from these IDs to do self- certification of his/her details.

The user will own their data. It helps users decide the information to be shared with organizations. Without the user's consent, no data can be shared with any identity seekers.

Step 3: Smart contracts generating trust score of the person

Suppose there is a score that determines the trustworthiness of a person. Smart contracts containing the business logic can generate a trust score for a user from the information provided by them while creating a self- sovereign identity.

Step 4: Third-party companies requesting access

Every time any company will have to access specific details of a person for authentication purposes, a notification will be sent to the individuals owning the identity.

Once the user allows the companies to access their details, third parties can use the identifiable information for authenticating a person. Also, individuals will be able to trace the purpose for which their PII has been used.

Blockchain does not store the user’s data or information. Instead, the transactions made between identity holders and companies will only be recorded on the blockchain.

For example, if an immigration authority verifies the person’s identity via an app, then that transaction will be added on the blockchain and visible to all the connected nodes.

Let’s discuss the example in more depth.

Suppose a person named Alex needs to authenticate himself to apply for study abroad programs. Thus, the education center can validate his identity quickly because of the blockchain-enabled identity management app.

Alex will provide the unique ID number to the center, enabling them to submit the request for accessing information. After he validates the request, the education hub can check his documents, and the transaction will be recorded on the blockchain.

▼ **How block chain is revolutionizing the traditional business network? Explain with example.**

- According to a Deloitte survey, 53 percent of fintech companies believe blockchain has become vital for their organization.
- PwC's 2018 global blockchain survey also confirmed that 84 percent of companies, including the likes of Amazon and Facebook, are already dabbling in it.
- Blockchain is a distributed ledger technology that was launched in 2009. This ledger records transactions arranged in "blocks" and "chained" together.
- Aside from providing open-source traceable storage, blockchain offers benefits such as decentralization, security and immutability. As a consequence, this modern technology has surpassed its use for only cryptocurrencies, enabling businesses to transact and communicate seamlessly over the internet. Here are the ways in which blockchain is fundamentally transforming business-communication networks.
- **Decentralization**
    - Blockchain cannot be controlled by a single node. Therefore, it is a decentralized ledger where blocks of information are stored across a network. What this means is that even if a single node goes down, other nodes can catch transactions that were missed. And the fact that every node processes transactions takes away the possibility for a single node to bring down the entire system.
    - Further, there is no central control of the blockchain and, as such, neither government nor a central bank or higher authority can influence its use. Plus, those highly positioned in companies cannot make manipulations to the blockchain, thanks to its decentralized nature. For businesses, this means they can have secure peer-to-peer communication without relying on a central authority.
- **Data Security**
    - Data security is everything for businesses, as it ensures that their records are not susceptible to an attack. Nonetheless, businesses have been hacked time and again for relying on traditional methods of storage. In 2013, there was a data breach on Yahoo's database and three billion records were affected. Likewise, data pertaining to

Capital One credit cardholders (100 million Americans and six million Canadians) was hacked in 2019.

- Blockchain, on the other hand, is a secure platform for storing information. It uses cryptographic techniques, Merkle trees, hash functions and public and private keys to make it difficult for a hacker to alter its content. The immutable nature of this technology ensures that stored content cannot be changed. Also, its high-level security makes it less susceptible to cyberattacks. Interestingly, there are many blockchain projects (e.g. Eximchain and Signal) working on enhancing how businesses would safely communicate data.

- **Data Privacy**
  - While blockchain's content is open and accessible to anyone, there are permissioned and permissionless blockchains. The latter ensures that sensitive information is kept away from the public's eye. In this case, the data is encrypted and can only be accessed after permission has been granted. Further, a private/permission blockchain requires the owner or management's approval before participants are added to the network.
  - For this reason, there can be centralized control over who can join the network, thereby offering enhanced data privacy. For instance, blockchain projects like Dust, Debrief and many more are working to increase data privacy and efficiency and also engage clients, reducing the potential for sensitive data to be accessed by unauthorized users.
- **Transparency**
  - Blockchain has fostered singular trust among network participants, since transfers are guaranteed to be safe and secure. Much more, everyone on the network can see such transfers in real-time thanks to the transparency offered by blockchain. This helps to improve accountability and trust between business partners.
  - The immutable nature of blockchain also offers data integrity, since its content cannot be changed easily. This means that business partners cannot challenge the legitimacy of such transfers, because they are able to monitor it. A real-life use case of this is evident in the healthcare industry, where the technology is used for revenue-cycle management and fraud prevention.
- **Traceability**
  - Blockchain's content can be tracked in real-time, which has offered immense benefits to businesses. Its content is accurate at all times, and moreover, several participants of the network will see the same information irrespective of where they access it and when. It, therefore, enables large enterprises to communicate and coordinate supply chain and logistics information.
  - It is worth noting that this traceability has aided in verifying the authenticity of rare and valuable products. In this aspect, customers can easily scan a barcode to determine if the raw materials used for the products were rightly sourced. It also gives consumers the confidence that they have purchased authentic products.

- Blockchain has transformed the business-communication network in more ways than one. The distributed ledger's features, including decentralization, security, privacy, immutability and traceability, have improved the way businesses communicate and relate. It also reduces costs significantly, all of which is why any company looking to promote its growth in the the long run, needs to adopt the blockchain system.

💡 **Everledger—Diamond—40 physical traits**

UNIT 5

▼ **Block chain application development**

A blockchain is a decentralized digital ledger that saves transactions on thousands of computers around the globe.

These are registered in a way that inhibits their subsequent modification. Blockchain technology increases the security and speeds up the exchange of information in a way that is cost-effective and more transparent.

It also dispenses with third parties whose main role was to provide a trust and certification element in transactions (such as notaries and banks).

The high importance of blockchain has attracted the attention of organizations in different sectors, with banking sector being the most active at this stage.

Blockchain has resulted in the development of thousands of new job positions and new startups ranging from mobile payment solutions to health care applications.

Whether you need a prototype or a production-ready platform, our engineering team’s deep experience in cryptocurrency, data science, and serverless computing can help you leverage the benefits of blockchain. We will evaluate potential blockchains for your project, including Ethereum, Hyperledger, EOS, NEO, Tezos, and Qtum, and choose the best fit, like when to use private permissioned blockchains such as Quorum.

Our Engineering Capabilities Include:

- Blockchain deployment and development with web3, solidity, cakeshop and truffle.
- Smart contracts and custom dapp frameworks like OpenZeppelin.
- Application and data science engineering using Python.
- Enterprise native mobile apps with Swift and Objective- C.
- Web platforms using Phoneix / Elixir and serverless architecture.

Blockchain Software Development Platforms

While there are more than platforms for blockchain solutions, 25 building the top blockchain platforms that are commonly considered for blockchain/DLT development are:-

1. **Ethereum:** It is an open-source and public platform (and operating system) taken into consideration for blockchain App development and ICOs with smart-contract functionality.

Unlike bitcoin, it is flexible and adaptable – making it the first choice for every blockchain app development company for building a blockchain app.

2. **EOS:** The aim of EOS platform is to offer smart contract capability, decentralized application hosting, and decentralized storage of the enterprise solutions which solves the scalability issues found in Blockchains such as Ethereum and Bitcoin, along with eliminating all the fees incurred by the users.
3. **Multichain:** It is a platform that empowers blockchain app builders to create and deploy private blockchain solutions to be used within or between multiple organizations.
4. **Liquid Apps:** The name behind DAPP Network recently launched DSP 2.0 to make the platform a lot more flexible and powerful. They are capable of supporting a range of dApps creation.
5. **Hyperledger:** It is an open-source platform used to create advanced blockchain software development solutions. For example, building blockchain solutions based on IoT, creating blockchain apps for supply chain management, etc.
6. **IOTA:** It is an open-source DLT based solution used for providing faster and secure payment services between connected IoT devices. This platform uses directed acyclic graph (DAG) technology and offers unique characteristics, like free transactions no matter what the size of the transaction is, faster confirmation times, handling of unlimited transactions at a time, etc. which makes it the ideal platform for building payment systems.
7. **Quorum:** It is an open-source DLT and smart contract platform based on Ethereum.

Blockchain is also widely integrated in P2P payment applications for safe cashless transactions.

Factors to Consider for Blockchain App Development

1. **Nature of Platform:** While some blockchain platforms are cryptocurrency based, others are relying on smart contracts or using more than one crypto token. Determining which type is apt for you will make the Blockchain applications development process easier.
2. **Smart Contracts:** The second thing you need to pay attention to is to determine if you need a smart contract or not. A Smart contract, as you might know, is a self-executing protocol that processes, validates or enforces any trigger-based action stored on the blockchain system.
3. **Consensus Protocol:** Different blockchain development platforms work upon different consensus protocol, including Proof of Work, Proof of Stake, Proof of Elapsed time, Proof of Burn, etc. So, identifying the right platform on the basis of consensus protocol is also favorable situation.
4. **Cryptocurrency:** The next thing that you need to consider when answering How to develop a Blockchain app is whether you need the use of cryptocurrencies in your mobile application or not also plays a pivotal role in finding the right platform.
5. **Public/Private Network:** Ask yourself what kind of network you want – one where all are free to make changes or the one where authorized users only can participate. Based on the

decision, choose the platform and start creating your own blockchain application.

6. **Adoption Rate And Functionality:** It is vital to look into the Adoption rate and Community Support level for a current blockchain. Adoption rate means the degree of implementation that a specific blockchain innovation has gotten. Picking a technology that has been exceptionally embraced and adopted is a smart choice than picking one with a poor adoption level.
7. **Scalability:** Those hoping to build blockchain platforms off of existing innovation should take a gander at the transaction capability and decide whether their requirements will be met. When taking consideration into blockchain scalability three central points are thought of: speed, security, and decentralization. This is known as the Scalability Trilema and points to the fact that any developer can hope to get, at best, two out of three characteristics.

Languages to Consider for Blockchain Development

There are various programming languages that can be considered while blockchain application development. You can either begin with traditional programming languages like C++, Python, Go, and Java, or turn towards the advanced blockchain-specific languages like Simplicity and Solidity.

1. **Simplicity: Simplicity is used for smart contracts blockchain development.** The language is easy, employs static analysis, and can be seen as an improvement of the basic cryptocurrency languages like **Ethereum Virtual Machine (EVM)** and Bitcoin Script.
2. **Solidity: Solidity is a statically-typed blockchain development language used particularly for building smart contracts that run on the EVM**. With this language, you can easily implement self- regulated business logic in smart contracts, leaving a non-repudiable and authoritative record of transactions.

Blockchain Development Process

The blockchain development process consists of the following six stages:

1. Identify the Goal
2. Choose the right Blockchain Platform
3. Brainstorming and Blockchain Ideation
4. Proof of Concept
5. Visual and Technical Designs
6. Development

Let’s discuss these stages in detail.

1. **Identify problems you want to solve with blockchain**
   First of all, it is essential to develop a problem statement and understand all of the issues you want to solve with a proposed solution. Ensure that the blockchain solution will benefit your business abilities. Analyze whether you need to migrate your current solution to the blockchain, or you require a new application to be developed from scratch. For example, suppose you are a healthcare provider who wants to develop a blockchain-based health

record exchange app. In that case, you should know various use cases of the applications and what benefits they will offer to users. Once you decide that you need a blockchain solution for your business operations, the next step is to select the right blockchain platform and blockchain development tools for your project.

2. **Choose the right blockchain platform**
   As mentioned above in the article, building a blockchain from scratch requires thorough research and takes months to years to develop successfully. Therefore, you should build a blockchain app on top of a blockchain platform that meets your business requirements. You should identify the right blockchain platform for your application based on the factors like consensus mechanism and problems you want to solve. For example, you can build an Ethereum-based application to develop a decentralized public application with smart contracts. When the blockchain platform is identified, you must do a brainstorm and understand the exact business needs.

3. **Brainstorming and blockchain ideation**
   Once you identify the platform for developing a blockchain application, you should focus on drafting business requirements and brainstorming ideas. Find what technology components should be added to the blockchain ecosystem as off-chain or on-chain entities. Create a product roadmap that will help you build an application within a decided deadline. You should develop a blockchain model and conceptual workflow for the blockchain application. Also, decide if the application needs to be developed on a permissioned or permissionless blockchain network. It would help if you also decided on front-end programming languages, servers, and external databases at this stage.

4. **Doing a Proof-of-Concept**
   A proof of concept is done to represent the practical applicability of a blockchain project. It can be either a design prototype or a theoretical build-up. In Theoretical Build-up, each project requires theoretical cases so that users could understand the applicability and viability of the product. Proposals can be created to explain the project's parameters. After creating a theoretical build-up and receiving feedback, a prototype is designed, which includes:

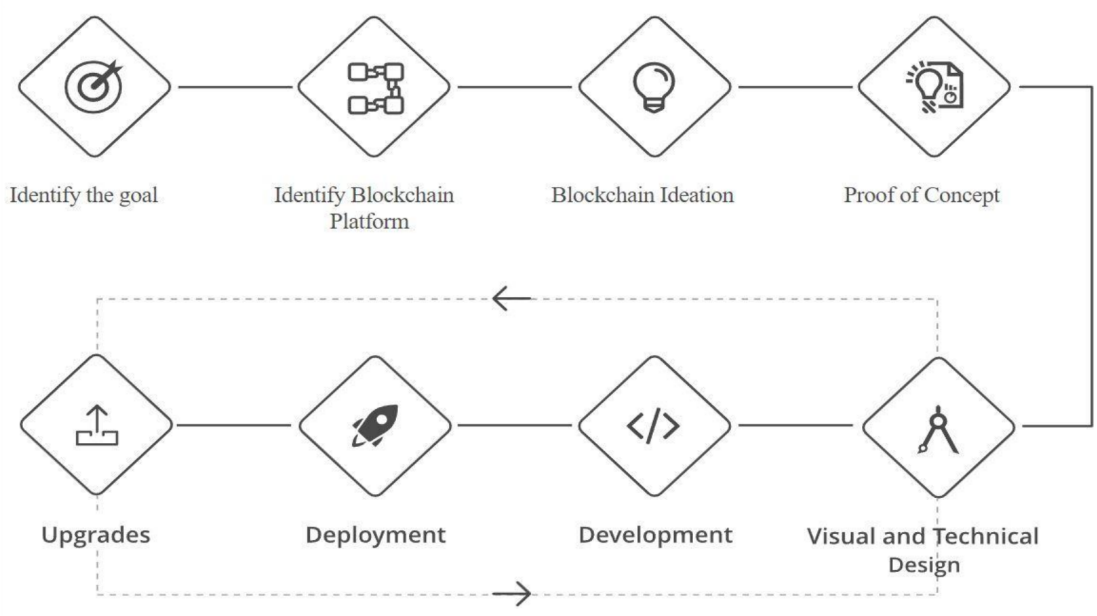
   a. sketches
   b. mockups
   c. tested product
   d. designs
   e. information architecture

   When the client approves the PoC, the next step is to prepare technical and visual designs for the application.

5. **Visual and Technical Designs**
   Since you have planned an entire application at this stage, start creating UIs for each software component. Designs APIs that will be integrated with user interfaces to run an application at the back-end. Visual designs are created to give a look and feel to the application, whereas technical designs represent the application's technology architecture.

Once the admin consoles and user interfaces are designed, the application gets ready for development.

6. **Development**
   Development is the significant phase of the blockchain development process, where you should be ready to build the blockchain app. In this specific stage, you either have to develop or integrate APIs for particular use cases of the application. The application is built under multiple versions. Firstly, an application that does not undergo formal testing is a pre-alpha version of the app. Once the client approves it, the application moves to the next stage, i.e., alpha, where the developers test the software with white-box techniques. But, the software might not comprise all the features at this stage. After the alpha version is released, the app is prepared for the beta version. During Beta Phase, the software application has the complete feature set but with some unknown bugs. Developers share the beta version with a particular group of people outside the organization to test its functionality. Once the beta version is approved and tested, the application moves to the Release Candidate version, an advanced beta version that is ready to be a final application and can be launched. After thorough testing, the application moves to the production phase and gets ready for delivery. Before an app goes live, you should deploy it on the test network to carefully test its functionalities. Administrators can also manage which versions of the app need to be deployed to various resources with provisioning when deploying an application. Once an application is provisioned, it must be hosted on the main chain. If your blockchain app is a hybrid solution, i.e., it contains both off-chain and on-chain business entities, you need to deploy it on the cloud server and app store/play store. The application should be able to upgrade according to any new business needs and prioritization. For instance, if you need to upgrade the smart contract, you should be able to deploy the new contracts without any difficulty later on. Developing and deploying an app does not mean you are done. Instead, a software application needs to be maintained post-development to ensure that it works with all types of upgrades in the future.



How long blockchain development takes?

The duration of a blockchain project depends on the application's requirements. The project is initiated with PoC, which typically takes 2-3 weeks. Once the PoC is done, it takes 4-5 weeks to develop a minimum viable product with bare minimum features. Launching an application on the main net takes around 2-3 months based on the requirements of a client.

▼ Hyperledger Fabric

The Linux Foundation (the same corporation behind the Linux Operating System) launched the Hyperledger blockchain initiative in December 2015.

This project was established as a core for both the collaborative production of fully accessible blockchain technology and distributed ledgers.

Hyperledger Fabric is a modular blockchain framework that acts as a foundation for developing blockchain-based products, solutions, and applications using plug-and-play components that are aimed for use within private enterprises.

Hyperledger Fabric is an **open source, permissioned blockchain framework**, started in 2015 by The Linux Foundation.

It is a modular, general-purpose framework that offers unique identity management and access control features, which make it suitable for a variety of industry applications such as track-and-trace of supply chains, trade finance, loyalty and rewards, as well as clearing and settlement of financial assets.

Because Hyperledger Fabric is private and requires permission to access, businesses can segregate information (like prices), plus transactions can be sped up because the number of nodes on the network is reduced.

▼ What is the need for Hyperledger in Blockchain?

Hyperledger was founded to advance the discovery as well as the adoption of cross-industry blockchain systems. It is backed by major corporations such as IBM and many others across a wide range of sectors, including finance, IoT, banking, industry, etc.

One thing to keep in mind is that Hyperledger was designed to assist and stimulate the advancement of blockchain technology, not any particular cryptocurrency.

Blockchains can transform online transactions by fostering faith, openness, and trustworthiness, as per the Hyperledger webpage. It was created solely to fulfill that ability. Around 100 companies, comprising industry titans like Nokia, IBM, and Samsung, are part of the Hyperledger blockchain, which meets every month to supervise the development of prospective blockchain frameworks. **This Hyperledger neither has any nor will have its coin. It is a vital thing to keep in mind about Hyperledger.**

This directly addresses Hyperledger's purpose: developing robust industrial applications using blockchain technology while remaining apart from the digital currency creation process.

▼ How Hyperledger Fabric Works

Traditional blockchain networks can't support private transactions and confidential contracts that are of utmost importance for businesses. Hyperledger Fabric was designed in response to this as a modular, scalable and secure foundation for offering industrial blockchain solutions.

Hyperledger Fabric is the open-source engine for blockchain and takes care of the most important features for evaluating and using blockchain for business use cases.

Within private industrial networks, the verifiable identity of a participant is a primary requirement.

Hyperledger Fabric supports memberships based on permission; all network participants must have known identities.

Many business sectors, such as healthcare and finance, are bound by data protection regulations that mandate maintaining data about the various participants and their respective access to various data points.

Fabric supports such permission-based membership.

▼ **Example of Hyperledger Fabric**

Suppose there's a manufacturer that wants to ship chocolates to a specific retailer or market of retailers (i.e., all US retailers) at a specific price but does not want to reveal that price in other markets (i.e., Chinese retailers).

Since the movement of the product may involve other parties, like customs, a shipping company, and a financing bank, the private price may be revealed to all involved parties if a basic version of blockchain technology is used to support this transaction.

Hyperledger Fabric addresses this issue by keeping private transactions private on the network; only participants who need to know are aware of the necessary details. Data partitioning on the blockchain allows specific data points to be accessible only to the parties who need to know.

▼ **Benefits of Hyperledger Fabric**

1. **Open Source-** Hyperledger Fabric platform is an open source blockchain framework hosted by The Linux Foundation. It has an active and growing community of developers.
2. **Permissioned-** Fabric networks are permissioned, meaning all participating member’s identities are known and authenticated. This benefit is particularly useful in industries including healthcare, supply chain, banking, and insurance where data cannot be exposed to unknown entities. For example, an insurance company on a Hyperledger Fabric blockchain network can share customer’s claim data with permissioned parties to maintain customer privacy.
3. **Governance and Access Control-** Fabric networks consist of channels, which are a private “subnet” of communication between two or more specific network members, members on the network can transact in a private and confidential way. Each transaction on the blockchain network is executed on a channel, where each party must be authenticated and authorized to transact on that channel. This provides an additional layer of access control and is especially useful when members want to limit exposure of the data, for example when competitors are on the same network.
4. **Performance-** Hyperledger Fabric is built to support enterprise- grade use cases, and can support quick transaction throughput from its consensus mechanism. Because Fabric is a permissioned blockchain framework, it does not need to solve for Byzantine Fault Tolerance which can cause slower performance when validating transactions on the network.

▼ **Architecture**

In this part of the article, we will learn about the design of the Hyperledger Fabric System.

1. **Assets-** Assets can vary from the physical (property investment and equipment) to the immaterial (software and trade secrets). By using the chain code transaction process, Hyperledger Fabric allows users to alter assets. In the Hyperledger Fabric system, assets are portrayed as a series of key- value pairs, with state changes registered as exchanges on a ledger path. Binary and JSON representations are available for assets.
2. **Chaincode-** Chaincode is the commercial concept software that defines one or multiple assets and the transaction methods for managing the purchase (s). The criteria for accessing or changing key-value pairs or any other dynamic database entries are enforced by Chaincode. Chaincode operations are started with a transaction idea and run against the ledger's existing state information. The implementation of Chaincode generates a collection of key-value writes that can be sent to the system and implemented to the ledgers of all users.
3. **Ledger-** All value changes in the fabric are recorded in a sequential, damage- resistant ledger. Chaincode abstractions ('transactions') supplied by interacting parties cause state shifts. Every transaction generates a collection of asset key-value pairs that have been created, updated, or deleted in the ledger. A blockchain is used to store permanent, sequential records in blocks, and a database file is used to keep track of the present fabric state. Each channel has only one ledger, which performs an error handling check is conducted before adding a block to guarantee that the conditions of assets that were fetched have not altered since chain code processing time.
4. **Security-** Hyperledger Fabric is the foundation of a transactional system in which all members are acknowledged. Cryptographic licenses are related to businesses, networking equipment, and application developers or client apps via Public Key Infrastructure. As an outcome, data access management on the system and channel stages can be regulated and managed. In this way, it makes it secure.
5. **Consensus-** Consensus has gradually been associated with a specific method within a particular target in distributed ledger architecture. On the other hand, consensus entails more than just responding on transaction execution, and this distinction is underscored in Hyperledger Fabric by its central position in the whole transaction pipeline, from request and approval to ordering, verification, and pledge. In a word, the consensus is the total authentication of the accuracy of a group of transactions that make up a block.
6. **Confidentiality-** Hyperledger Fabric uses an unchangeable ledger and a chain code that may edit and alter the present state of objects. A ledger can operate within the range of a channel — it could be broadcast throughout the existing system or privately run to include precisely a limited number of users.
   After all these situations, these parties will make a different channel, isolating and segregating their transactions and the database. A chain code can only be deployed on peers, which needs the information to the asset states to execute reads and updates to overcome situations that seek to fill the space between complete transparency and confidentiality.

When companies on a network want to maintain their transaction information secret, secret record keeping is being used to store it in a personal library that is logically independent of the channel record and available only to the allowed group of companies.

▼ **Identities**

- peers, orderers, client applications, administrators and more
- Each of these actors — active elements inside or outside a network able to consume services — has a digital identity encapsulated in an X.509 digital certificate
- union of an identity and the associated attributes a special name — **principal**
- For an identity to be **verifiable**, it must come from a **trusted** authority. A **membership service provider (MSP)** is that trusted authority in Fabric.
- The default MSP implementation in Fabric uses X.509 certificates as identities, adopting a traditional Public Key Infrastructure (PKI) hierarchical model (more on PKI later).
- **A Simple Scenario to Explain the Use of an Identity**
  - Imagine that you visit a supermarket to buy some groceries. At the checkout you see a sign that says that only Visa, Mastercard and AMEX cards are accepted. If you try to pay with a different card — let's call it an "ImagineCard" — it doesn't matter whether the card is authentic and you have sufficient funds in your account. It will be not be accepted.

  - *Having a valid credit card is not enough — it must also be accepted by the store! PKIs and MSPs work together in the same way — a PKI provides a list of identities, and an MSP says which of these are members of a given organization that participates in the network.*
  - PKI certificate authorities and MSPs provide a similar combination of functionalities. A PKI is like a card provider — it dispenses many different types of verifiable identities. An MSP, on the other hand, is like the list of card providers accepted by the store, determining which identities are the trusted members (actors) of the store payment network. **MSPs turn verifiable identities into the members of a blockchain network**.

▼ **Policies**

https://hyperledger-fabric.readthedocs.io/en/latest/policies/policies.html

▼ **Membership and Access Control**

https://www.youtube.com/watch?v=ng-hMpik9n4

https://www.youtube.com/watch?v=ng-hMpik9n4

Membership Control

https://hyperledger-fabric.readthedocs.io/en/latest/membership/membership.html

Access Control

Access control is a mechanism in computer security that regulates access to the system resources. The current access control systems face many problems, such as the presence of the third-party, inefficiency, and lack of privacy. These problems can be addressed by blockchain, the technology that received major attention in recent years and has many potentials. In this study, we overview the problems of the current access control systems, and then, we explain how blockchain can help to solve them. We also present an overview of access control studies and proposed platforms in the different domains. This paper presents the state of the art and the challenges of blockchain-based access control systems. Blockchain applications initially were limited to the cryptocurrencies and financial transactions. Invention of smart contracts leads to development of more divers applications, such as healthcare, IoT, supply chain. After reviewing many research studies based on blockchain and smart contracts, we noticed that the primary focus of many presented applications is providing an efficient and secure access control mechanism.

Access control is a required security part of almost all applications. Blockchain specific characteristics such as immutability, durability, auditability, and reliability lead to considering blockchain as a supplementary solution for access control systems. Access control systems are applied to regulate access to the system’s resources and it is the fundamental part of computer security. Access control is usually enforced against a set of authorization based on system policies.

Blockchain has desirable features that make it a trustable alternative infrastructure for access control systems. The distributed nature of blockchain solves the problem of single point of failure and other centralized management problems. Also, by eliminating third parties, we do not need to be concern about privacy leakage from their side. In addition, we can access to a trustable and unmodifiable history log. Consensus mechanisms are applied, so only valid transactions are recorded on blockchain. Furthermore, by using smart contracts, we can monitor and enforce access permissions under complex conditions. All of these features have motivated researchers to consider blockchain as an infrastructure for access control systems.

We propose to store the representation of the right to access a resource in a blockchain, allowing the management of such right through blockchain “transactions”

The main advantages of the proposed approach are:

- the right to access a resource can be easily transferred from a user to another through a blockchain transaction created by the last right owner, without the intervention of the resource owner;
- the right is initially defined by the resource owner through a transaction, and all the other transactions representing the right transfers are published on the blockchain. Hence, any user can inspect them at any time in order to check who currently holds the rights to perform a given action on a given resource. Consequently, a user who had its access request denied, can check whether the entity in charge of verifying the existence of the required right actually made the right decision.

A common way of expressing access control rights is through Attribute- Based Access Control (ABAC) policies. Roughly speaking, an attribute- based access control policy combines a set of rules expressing conditions over a set of attributes paired to the subject, to the resource or to the environment.

1. Blockchain-based access control from transactions to smart contracts.
2. Data sharing access control
3. Access control for cloud federation
4. Access control across multiple organizations
5. Access control for shared blockchains
6. Access control and self-Sovereign identities

▼ **Channels**

A Hyperledger Fabric channel is a private “subnet” of communication between two or more specific network members, for the purpose of conducting private and confidential transactions. A channel is defined by members (organizations), anchor peers per member, the shared ledger, chaincode application(s) and the ordering service node(s). Each transaction on the network is executed on a channel, where each party must be authenticated and authorized to transact on that channel. Each peer that joins a channel, has its own identity given by a membership services provider (MSP), which authenticates each peer to its channel peers and services.

To create a new channel, the client SDK calls configuration system chaincode and references properties such as anchor peers, and members (organizations). This request creates a genesis block for the channel ledger, which stores configuration information about the channel policies, members and anchor peers. When adding a new member to an existing channel, either this genesis block, or if applicable, a more recent reconfiguration block, is shared with the new member.

The election of a leading peer for each member on a channel determines which peer communicates with the ordering service on behalf of the member. If no leader is identified, an algorithm can be used to identify the leader. The consensus service orders transactions and delivers them, in a block, to each leading peer, which then distributes the block to its member peers, and across the channel, using the gossip protocol.

Although any one anchor peer can belong to multiple channels, and therefore maintain multiple ledgers, no ledger data can pass from one channel to another. This separation of ledgers, by

channel, is defined and implemented by configuration chaincode, the identity membership service and the gossip data dissemination protocol. The dissemination of data, which includes information on transactions, ledger state and channel membership, is restricted to peers with verifiable membership on the channel. This isolation of peers and ledger data, by channel, allows network members that require private and confidential transactions to coexist with business competitors and other restricted members, on the same blockchain network.

▼ **Transaction Validation**

Transaction validation is the process of determining if a transaction conforms to specific rules to deem it as valid. Validators check if transactions meet protocol requirements before adding the transactions to the distributed ledger as part of the validating process.

This validation process is carried out by nodes who store full copies of the blockchain. When nodes validate a transaction, it is added to the mempool (short for memory pool). In a proof of work network, miners are incentivized by transaction fees to confirm these transactions by including them in a block in the blockchain, establishing a clear chronological record of when the transaction occurred so that a later transaction cannot spend the same coins as in the original.

A transaction is considered valid if the sender in the transaction has an initial balance in their wallet equal to or greater than the amount being sent in the transaction (including the transaction fee). Other rules can exist depending on the specific protocol in question, but this rule is generally applicable to all protocols.

Full transaction validation includes the following checks:

1. **Transaction fields check including:**
    a. Timestamp check:
        - the transaction timestamp should be not more than 2 hours ago or 1.5 hours ahead from the current block timestamp.
        - Transaction version check: all the features required to support this version should be activated.
        - Transaction type check: all the features required to support this type should be activated.
        - Check of token amounts: the values must be non-negative.
        - Check of fields depending on the transaction type.
    b. **Sender's balance check**

        The sender should have enough funds to pay the fee. If a sponsored asset is used for the fee, the sponsor's balance is also checked.

        Depending on the type of transaction, the sender should have enough asset for transfer or for payments attached to the Invoke Script transaction. Order senders in the Exchange transaction should have enough funds to exchange.

    c. The sender's signature verification for ordinary account (without script), or account script execution if the sender is smart account, or the verifier function execution if the

sender is dApp. A similar check is performed for orders in an Exchange transaction.

d. For the Invoke Script transaction:
    - Calculation of the result of dApp callable function.
    - App balance check: dApp account should have enough funds for dApp script actions.
    - Check that the transaction fee is not less than the minimum fee based on script actions.
e. Execution of asset scripts if the transaction uses smart assets, including scripts of assets used in dApp script actions.

When receiving the transaction via the broadcast endpoint, or adding transaction to a block, or receiving a block over the network, the node performs full validation of the transaction. When receiving an Invoke Script transaction over the network, the node performs calculations of the callable function up to the threshold for saving unsuccessful transactions.

Validation Result

When the transaction is received via broadcast or over the network:

- If one of the checks failed, the transaction is discarded.
- If all the checks passed, the transaction is added to the UTX pool that is the list of transactions waiting to be added to the block.

When adding the transaction to the block, the result of validation depends on the transaction type.

For the Invoke Script transaction:

- If one of the checks 1–3 failed, the transaction is discarded.
- If checks 1–3 passed, and the calculation of the result (check 4.1) failed with an error or throwing an exception before the complexity of performed calculations exceeded the threshold for saving failed transactions, the transaction is also discarded.
- If checks 1–3 passed but checks 4–5 failed and besides the result of the callable function is calculated successfully or the complexity exceeded the threshold, the transaction is saved on the blockchain but marked as failed: "applicationStatus": "script_execution_failed". The sender is charged the transaction fee. The transaction doesn't entail any other changes to the state of the blockchain.
- If all checks passed, the transaction is saved on the blockchain as successful: "applicationStatus": "succeeded" and the sender is charged the fee.

For the Exchange transaction:

- If one of the checks 1–3 failed, the transaction is discarded.
- If checks 1–3 passed but check 5 failed, the transaction is saved on the blockchain but marked as failed: "applicationStatus": "script_execution_failed". The sender of the

transaction (matcher) is charged the transaction fee. The transaction doesn't entail any other changes in balances, in particular, the order senders don't pay the matcher fee.

- If all checks passed, the transaction is saved on the blockchain as successful: "applicationStatus": "succeeded". The matcher is charged the transaction fee as well as the order senders are charged the matcher fee.

For the other transaction:

- If one of the checks failed, the transaction is discarded.
- If all checks passed, the transaction is saved on the blockchain as successful and the sender is charged the fee.

▼ **Writing smart contract using Hyperledger Fabric**

Developing Blockchain applications really means developing smart contracts, or as they are also called: chain code. Smart contracts can be compared to stored procedures in the database world and mostly deal with getting and setting parameters on business objects, in addition to doing anything else we want them to do by using either one of the following languages: JavaScript, TypeScript, Java or Go Developing Smart Contracts for Hyperledger Fabric is best done in the open source Visual Studio Code environment.

Smart Contracts in Hyperledger Fabric

A smart contract in Hyperledger Fabric is a program, called chaincode. Chaincode can be written in **Go**, JavaScript (**node.js**), and eventually other programming languages such as Java that implement a prescribed interface. Chaincode runs in a secured Docker container isolated from the endorsing peer process. Chaincode initializes and manages the ledger state through transactions submitted by applications.

A chaincode typically handles business logic that members of the network have agreed to. The state created by a chaincode is scoped exclusively to that chaincode and can't be accessed directly by another chaincode. However, with the appropriate permission, a chaincode in the same network can invoke another chaincode to access its state.

There are two different types of chaincode to consider:

- System chaincode
- Application chaincode

System chaincode typically handles system-related transactions such as lifecycle management and policy configuration. However the system chaincode API is open for users to implement their application needs as well.

Application chaincode manages application states on the ledger, including digital assets or arbitrary data records.

A chaincode starts with a package that encapsulates critical metadata about the chaincode, including the name, version, and counterparty signatures to ensure the integrity of the code and metadata. The chaincode package is then installed on the network nodes of the counterparties.

An appropriate member of the network (as controlled by policy configuration) activates the chaincode by submitting an instantiation transaction to the network. If the transaction is approved, the chaincode enters an active state where it can receive transactions from users via client-side applications.

Any chaincode transactions that are validated are appended to the shared ledger. These transactions can then modify the world state accordingly. Any time after a chaincode has been instantiated, it can be upgraded through an upgrade transaction.

▼ Writing smart contract using Ethereum

1. **Create a Wallet at MetaMask**

   Install MetaMask in your Chrome browser and enable it. Once it is installed, click on its icon on the top right of the browser page. Clicking on it will open it in a new tab of the browser.

   Click on Create Wallet and agree to the terms and conditions by clicking I agree to proceed further. It will ask you to create a password.

   After you create a password, it will send you a secret backup phrase that can be used for backing up and restoring the account. Do not disclose it or share it with someone, as this phrase can take away your Ethers.

   Next, ensure that you are in the Main Ethereum Network. If you find a checkmark next to "Main Ethereum Network, you are in the right place.

2. **Select a Test Network**

   You might also find the following test networks in your MetaMask wallet:

- Robsten Test Network
- Kovan Test Network
- Rinkeby Test Network
- Goerli Test Network
- The above networks are for testing purposes only; note that the Ethers of these networks have no real value.

3. **Add Some Dummy Ethers in Your Wallet**
   - In case you want to test the smart contract, you must have some dummy Ethers in your MetaMask wallet.
   - For example, if you want to test a contract using the Robsten test network, select it, and you will find 0 ETH as the initial balance in your account.
   - To add dummy Ethers, click on the Deposit and Get Ether button under Test Faucet.

   To proceed, you need to click request 1 ether from faucet and one ETH will be added to your wallet. You can add as many Ethers as you want in the test network.
4. **Use Editor Remix to Write the Smart Contract in Solidity**

   We will use Remix Browser IDE to write our Solidity code. Remix is the best option for writing smart contracts, as it comes with a handful of features and offers comprehensive development experience.

   It is usually used for writing smaller sized contracts. Remix's features include:
   - Warnings like Gas cost, unsafe code, checks for overlapping variable names, and whether functions can be constant or not.
   - Syntax and error highlighting.
   - Functions with injected Web3 objects.
   - Static analysis.
   - Integrated debugger.
   - Integrated testing and deployment environment.
   - Deploy directly to Mist or MetaMask.
5. **Create a .sol Extension File**

   Open Remix Browser, and click on the plus icon on the top left side next to the browser to create a .sol extension file.
6. **Smart Contract Code to Create ECR20 Tokens**

   ERC20.sol is a standard template for ERC20 tokens.
7. **Deploy Your Contract**

   Deploy the smart contract at the Ethereum test network by pressing the deploy button at the right-hand side of the Remix window. Wait until the transaction is complete.

After the transaction commits successfully, the address of the smart contract would be visible at the right-hand side of the Remix window. At first, all the ERC20 token will be stored in the wallet of the user who is deploying the smart contract.

▼ Ripple

Ripple It is an open-source protocol designed to allow transactions in a fast and cheap manner. Ripple is not just a platform but a currency. This platform has its own currency known as XRP but also allows people to create their own currency via RippleNet. RippleNet is nothing but a network of institutional payment-providers like banks and money services firms that use solutions developed by Ripple to offer a frictionless experience to 0 0 send money globally. Although Bitcoin is one of the known cryptocurrencies, Ripple is another one to take its place in the market. Unlike traditional methods of transactions, this platform aims at making the transaction process easier and quicker, especially for the cross- rder bo payments, thus creating a better ecosystem of growth and development.

Ripple is a technology that acts as both a cryptocurrency and a digital payment network for financial transactions. It was first released in 2012 and was co-founded by Chris Larsen and Jed McCaleb. Ripple's main process is a payment settlement asset exchange and remittance system, similar to the SWIFT system for international money and security transfers, which is used by banks and financial middlemen dealing across currencies. The token used for the cryptocurrency is premined and utilizes the ticker symbol XRP. Ripple is the name of the company and the network, and XRP is the cryptocurrency token. The purpose of XRP is to serve as an intermediate mechanism of exchange between two currencies or networks as a sort of temporary settlement layer denomination.

Features and It’s Working

To make international payment transfers easier and more convenient, Ripple can be seen as the best solution. But before understanding how this platform works, it is essential to learn what are the significant challenges associated with cross-border payments.

- The international payment transfer is expensive as there is the involvement of third parties.
- The traditional method of transfer is really slow as it takes around days and even weeks.

Distinguishing Ripple and Bitcoin

Although Bitcoin and Ripple have some similarities, there are striking differences between the two.

- Bitcoin is a blockchain technology while Ripple doesn’t use blockchain but uses a distributed consensus ledger and crypto tokens called XRP.
- Bitcoin can handle a maximum of 3-4 transactions per second on-chain while Ripple has demonstrated over 1500 transactions per second in its enclaves.
- Bitcoin is a digital currency intended as a means of payment for goods and services while on the other hand Ripple is designed for banks and payment networks, is a payment settling, currency exchange and remittance system.

▼ Corda

Corda is an open-source enterprise-based blockchain designed to offer interoperability. It is a platform that is intended to record, manage, and synchronize agreements and transfer anything valuable. It allows enterprises to communicate and transact directly while maintaining transparency and without worrying about privacy and to integrate Blockchain across their operations immediately and efficiently. Moreover, Corda offers timestamping services to order transactions temporally and ignore disputes. It has a smart contract logic, which specifies constraints that ensure state transitions are valid as outlined in the contract code.

What Makes Corda Blockchain Framework Different?

- **Privacy—** Privacy is a critical focus for any distributed ledger technology system. It is because your data is bound to be distributed across multiple nodes and servers belonging to different business entities.
- **Identity—** Identification of different parties in the DLT system over a permissioned blockchain becomes a core criterion to build a closed network of the system among known participants.
- **Consensus—** Consensus is a technique through which organizations over a distributed and decentralized network come on to an agreement over the transactions happening between them.
- **Contracts—** Smart contracts and program files embedding the business logic, rules validation are part of any business being run among different organizations over a blockchain-based distributed system.
- **No Block, But Chain—** Corda’s functionality relies on the UTXO input/output model, which is very similar to the transaction system used in traditional blockchains such as Bitcoin.