Savitribai Phule Pune University
Semester VII (Computer Engineering)

Blockchain Technology (Code : 410243)

Chapter 3 : Blockchain Platforms and Consensus in Blockchain

Q. 1 Give Different types of blockchain. State their advantages and disadvantages.

Ans. : **Types of Blockchain**

Fig. 3.1 shows the types of blockchain.

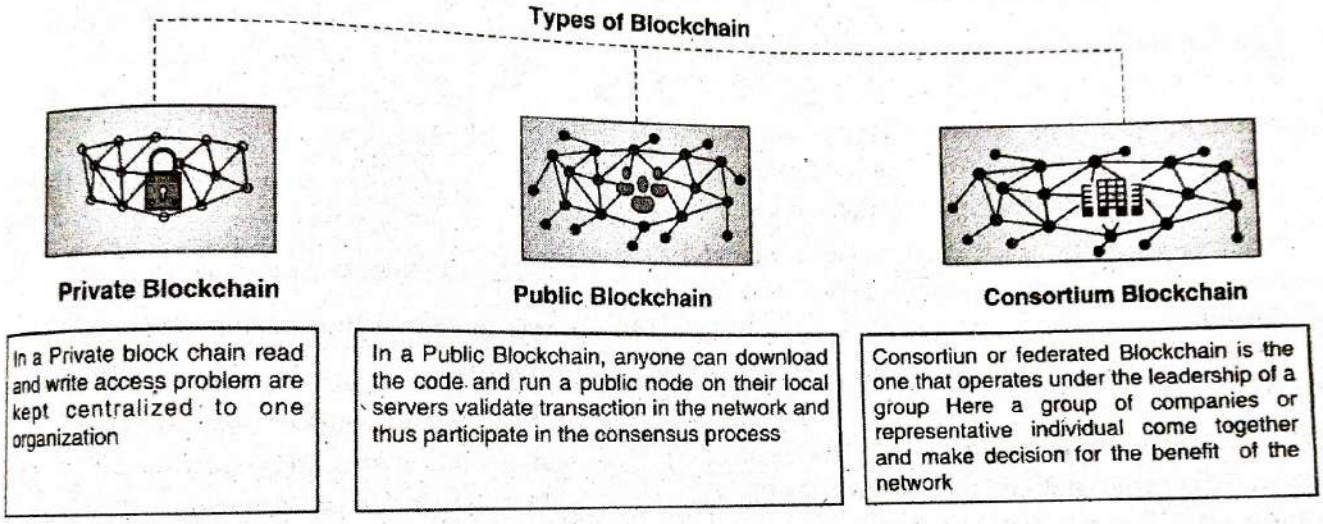
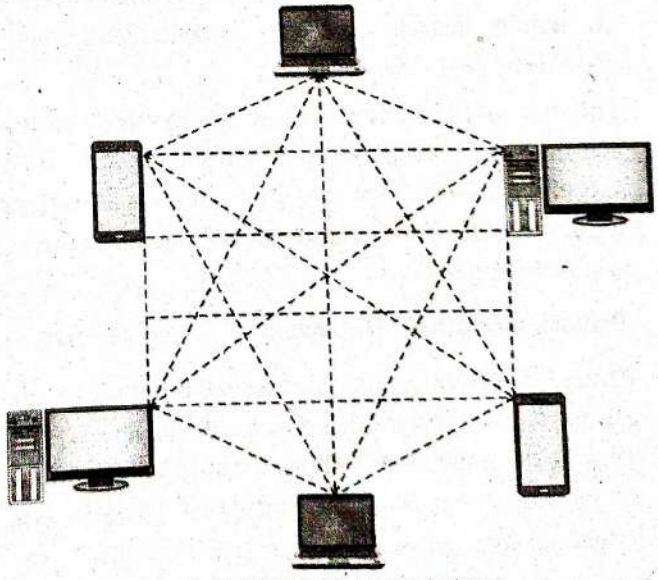


Fig. 3.1 : Types of Blockchain

1. **Public Blockchains**

- As the name suggests, public blockchains are open to the public, they are not owned by anyone. Anyone can participate as a node in the decision-making process. Users may or may not be rewarded for their participation. Bitcoin and Ethereum are both public blockchains.
- Bitcoin and other cryptocurrencies originated from public blockchains, which also played a role in popularizing Distributed Ledger Technology (DLT).
- Public blockchain is non-restrictive and anyone with internet access can sign on to a blockchain platform to become an authorized node. This user can access current and past records and conduct mining activities, the complex computations used to verify transactions and add them to the ledger. No valid record or transaction can be changed on the network, and anyone can verify the transactions, find bugs or propose changes because the source code is usually open source.



Public Blockchain: Permissionless
An open network system where all the devices can freely access without any kind of permission. The ledger is shared and transparent.

Fig. 3.2 : Public blockchain

- Examples of public blockchains are Bitcoin, Ethereum, Dash, Monero, and Litecoin etc.

Advantages of Public Blockchains

1. One of the advantages of public blockchains is that they are completely independent of organizations, so if the organization that started it ceases to exist the public blockchain will still be able to run, as long as there are computers still connected to it.
2. Another advantage of public blockchains is the network's transparency. As long as the users follow security protocols and methods fastidiously, public blockchains are mostly secure.

Disadvantages of Public Blockchains

1. The network can be slow, and companies can't restrict access or use.
2. If hackers gain 51% or more of the computing power of a public blockchain network, they can unilaterally alter the data in the blockchain.
3. Public blockchains also don't scale well. The network slows down as more nodes join the network.

Use cases

- The most common use case for public blockchains is mining and exchanging cryptocurrencies like Bitcoin. However, it can also be used for creating a fixed record with an auditable chain of custody, such as electronic notarization of affidavits and public records of property ownership.
- This type of blockchain is ideal for organizations that are built on transparency and trust, such as social support groups or non-governmental organizations. Because of the public nature of the network, private are likely to avoid it.

2. Private Blockchain Networks

- Private blockchains operate on closed networks, and are useful for private organizations and businesses. That is, they are open only to a group of individuals or organizations who have decided to share the ledger among themselves.
- Companies can use private blockchains to customize their authorization preferences and accessibility, parameters to the network, other important security options, etc.
- A private blockchain network is managed by only one authority. They're also known as permissioned enterprise blockchains or blockchains.

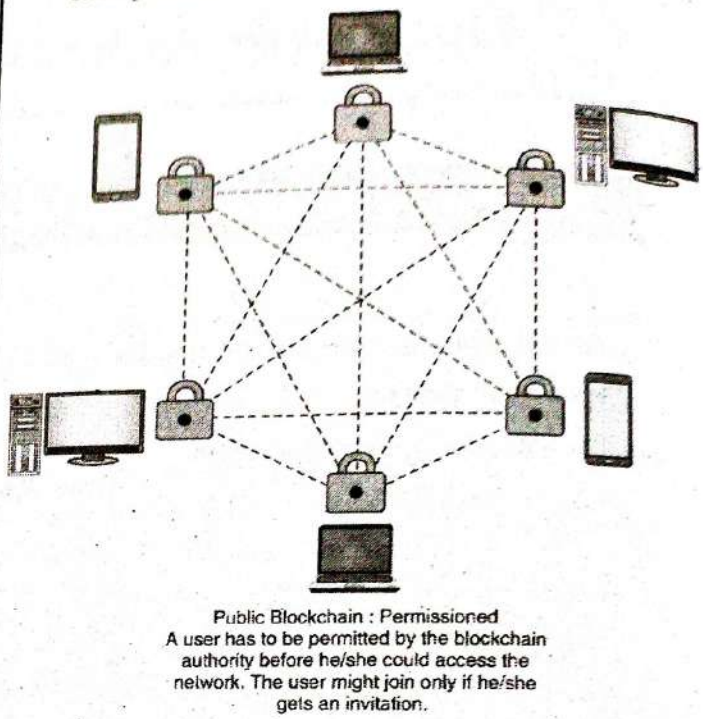


Fig. 3.3 : Private Blockchain Network

Advantages of Private Blockchain Networks

1. The controlling organization sets permission levels, security, authorizations and accessibility. For example, an organization setting up a private blockchain network can determine which nodes can view, add or change data. It can also prevent third parties from accessing certain information.
2. As users or Nodes are limited in size, private blockchains can be very fast and can process transactions much more quickly than public blockchains.

Disadvantages of Private Blockchain Networks

1. It is more difficult to achieve full trust in the information, since centralized nodes determine what is valid.
2. Less number of nodes can also mean less security. The consensus method can be compromised If a few nodes go rogue.
3. The source code from private blockchains is often closed and proprietary.
4. Users can't independently audit or confirm closed, which can lead to less security.
5. There is no anonymity on a private blockchain.

Use cases

- The speed of private blockchains makes them ideal for cases where the blockchain needs to be cryptographically secure but the controlling entity doesn't want the information to be accessed by the public.
- Other use cases for private blockchain include supply chain management, asset ownership and internal voting.

3. Consortium Blockchain

- The next type of blockchain is Consortium blockchains that have both public and private components, except multiple organizations which will manage a single consortium blockchain network. To set these types of blockchains can initially be more complex but they can offer better security. Consortium blockchains are optimal for collaboration with multiple organizations.
- In a consortium blockchain, the consensus procedures are controlled by preset nodes. It has a validator node that validates initiates and receives transactions. Member nodes can initiate or receive transactions.
- A consortium blockchain consists of two types of users. They are :
  1. The users who can access the blockchain.
  2. The users who have control over the blockchain and decide who should have permission to access the blockchain.

Advantages of Consortium Blockchain

1. A consortium blockchain tends to be more scalable, secure and efficient than a public blockchain network.
2. Like private and hybrid blockchain, it also offers access controls.

Disadvantages of Consortium Blockchain

1. Consortium blockchain is less transparent than public blockchain.
2. It can still be compromised if a member node is breached; the blockchain's own regulations can impair the network's functionality.

Use cases

1. Payments and Banking are two uses for this type of blockchain. Different banks can band together and form a consortium, deciding which nodes will validate the transactions.
2. This type of blockchain is good for tracking food and medicine supply chains where different parties are involved.

Q. 2 Differentiate between different type of Block Chain.

Ans. : Comparison of Different Types of Blockchain

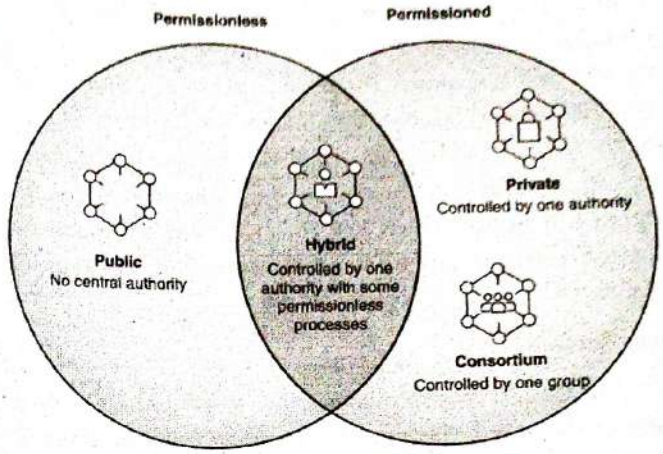


Fig. 3.4 : Types of blockchain

Public Blockchain	Private Blockchain	Consortium Blockchain
Anyone can run full node.	Not everyone can run a full node.	Selected members of the consortium can run a full node.
Anyone can make transactions.	Not everyone can make transactions.	Selected members of the consortium can make transactions.
Anyone can review/audit the blockchain.	Not everyone can review/audit the blockchain.	Selected members of the consortium can review/audit the blockchain.
Examples : Bitcoin, Litecoin, etc.	Examples : Ripple (XRP) and Hyperledger	Examples : r3, EWF

Q. 3 Explain Bitcoin and it's working. State how the value of bitcoin is decided.

Ans. : Bitcoin

Bitcoin is the first application of the blockchain technology as well as it is the first Cryptocurrency in the world. In the year 2009 Satoshi Nakamoto introduced bitcoin, based on the conceptual framework put forward by some researchers in the late 90's. It follows the exact structure of a typical Blockchain with P2P shared network, cryptographically protected data Distributed ledgers.

Bitcoin Working

It is very simple to use Bitcoin and we don't need any technical knowledge or programming skills for using Bitcoin. For using the Bitcoin Blockchain we have to create an account for it. For that, the simplest way is to create a digital wallet. BitCore, Coinbase, Exodus, etc. are a number of digital wallet service providers. While creating an account the user has to provide a 'Key' it is similar to a password. By using this key the wallet will generate a valid bitcoin Private key- Public Key pair. The public key is visible to all and it is the visible account ID of the user. While the private key the user keeps by himself, it is the access key to his account. If a person loses his private key he loses access to his account and his money.

Buy Bitcoin

The easiest way to own Bitcoin is to buy them from a bitcoin exchange. There are a number of online bitcoin exchanges which exchange normal currency to bitcoin. People can exchange their normal currency for bitcoin and move it to their wallet. Another way to own bitcoin is to participate in Bitcoin mining.

Transactions

Sending bitcoin from one account to another is called a transaction. It is usually done through wallets. The wallet app will provide an interface where we can input the account Id of the recipient and the amount we wish to transfer. Once we have made the transaction, the miners will verify the transaction and add to the blockchain ledger if it is a legitimate one. In Bitcoin, the transactions are cost-free. Usually, a transaction validation time is about 10 minutes in bitcoin, but if we give a small transaction fee we can speed up the process.

Value of Bitcoin

- General question that may arise in anyone's mind is 'who determines the value of bitcoin. As we know there is no central bank or any other designated agency to control it; then how the value is determined, or who determines it?
- The answer lies in the basic economics, which is demand and supply. Following is the simplest model to determine the value of bitcoin.

T : Total bitcoin transaction/second

D : Duration that a BTC needed by a transaction

S : Supply of the bitcoin

P : Price of the bitcoin

We have

S/D = Bitcoins available per second

T/P = Bitcoins needed per second

- According to the demand-supply rule, when the supply of bitcoin increases the demand decreases consequently the price will also decrease. And when the demand increases the supply of bitcoin will also decrease, consequently the price of the bitcoin will also increase.
- At an equilibrium state, where the supply S over D, is equal to the demand T over P. We can deduce the price P as

$$\frac{S}{(D)} = \frac{T}{P}$$

Equilibrium state :

$$P = \frac{TD}{S}$$

- The value of bitcoin basically depends on the demand and supply. It is evident that a single authority can't control the value of bitcoin, rather it is determined strictly based on the user transaction.

Q. 4 What is bitcoin mining ? Explain the functionality of miners.

Ans.: Bitcoin Mining

- Mining is the most interesting as well as the most important topic in bitcoin. This is the process by which new transactions are validated and added to the 'blockchain'. Miners are the nodes who participate in the mining process. This demands dedicated mining hardware and thus, not all nodes are involved in mining.
- When a new bitcoin transaction happens in the network that is broadcasted on the network. The miners listen to this broadcasting and engage in transaction verification. Once the transactions are verified they are added to a block permanently.

Working of Miners

- The mission is to find a hash value for the new block. The miner who finds the hash value first is rewarded with some bitcoins called block reward. Now it is 12.5 BTC. The reward is halved every 210,000 blocks or roughly every 4 years. Finding hash value is not a big deal. Every node can do that.

- Therefore, a difficulty level is associated with it to make the nodes compete with each other. The difficulty level is a measure of how difficult it is to find the hash. Difficulty level shrinks the set of hash values that a block can have. Without difficulty level, the hash can have any of the values within the super gigantic set of 2^256 possibilities (since the length of hash = 256 bits). By associating a difficult level, the target set is reduced considerably.
- The difficulty level is specified in terms of a number of zeroes, which means the miner has to find a hash value which starts with a specified number of zeroes. The nodes keep finding different hash values and check whether it satisfies the required difficulty level. Since the data of a block remains the same, the hash is always the same.
- Therefore, the only possibility to try out different hash values is by associating a nonce with the content of the block. The nonce is an arbitrary string of 32-bit length. i.e. H(block + nonce) Being a small target set, the probability of finding success is reduced.
- The miners keep changing the nonce in a brute force manner and the corresponding hash is computed each time. This is the real game and the computational power of nodes really matters here because the miners have to try out large combinations of 'Nonce'. The node which is equipped with dedicated hardware and high computational power has a greater chance to win this game and get the block reward. Those who find hash first will broadcast the block along with the nonce. By receiving this, others stop mining and validate whether the received hash satisfies the specified difficulty level. If yes, the nodes show their acceptance by adding it to the blockchain.

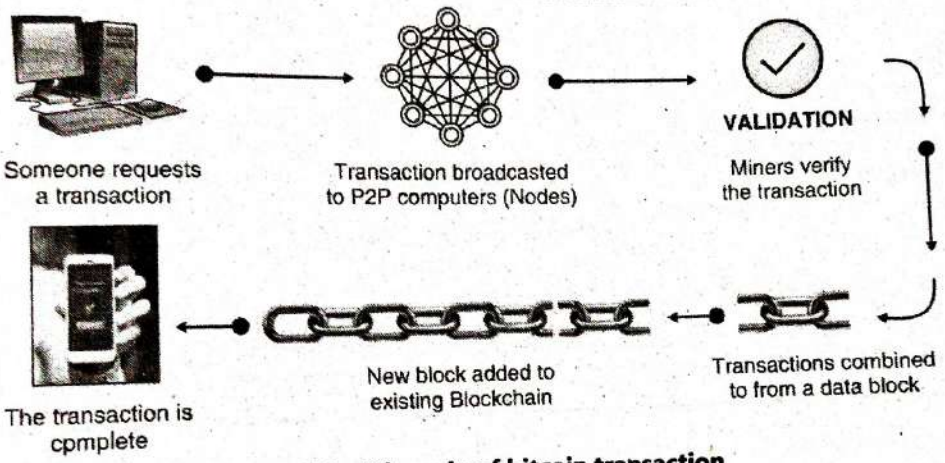


Fig. 3.5 : Life cycle of bitcoin transaction

Q.5 Explain Ethereum and Dapp.

Ans. :

1. **Ethereum**

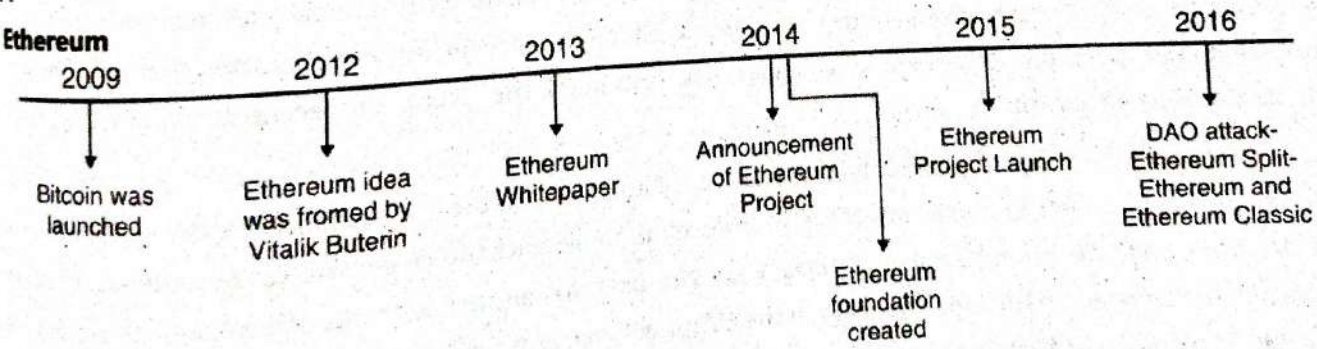


Fig. 3.6 : History of Ethereum

- Ethereum is an Open Source Blockchain platform which allows anyone to develop and deploy Blockchain based Applications. Any kind of application including cryptocurrency, tokens, wallets, social apps etc. can be developed and deployed in a Distributed Environment of Ethereum. In other words, rather than sticking with the cryptocurrency alone, Ethereum opened the possibilities of the 'blockchain' and 'distributed ledger' technology to other application domains.

- Ethereum is not a single network rather it is more like a protocol for inter-network communication. Actually, in Ethereum many networks exist alongside. The community Ethereum Network, Community test network and other private Blockchain networks like :
  - Private network
  - Public test network
  - Main Ethereum network
- World Wide Web (WWW) brought the individual networks under a single umbrella. Similarly, Ethereum incorporated all blockchain functionalities in a single network and avoided creation of individual blockchains for each purpose.

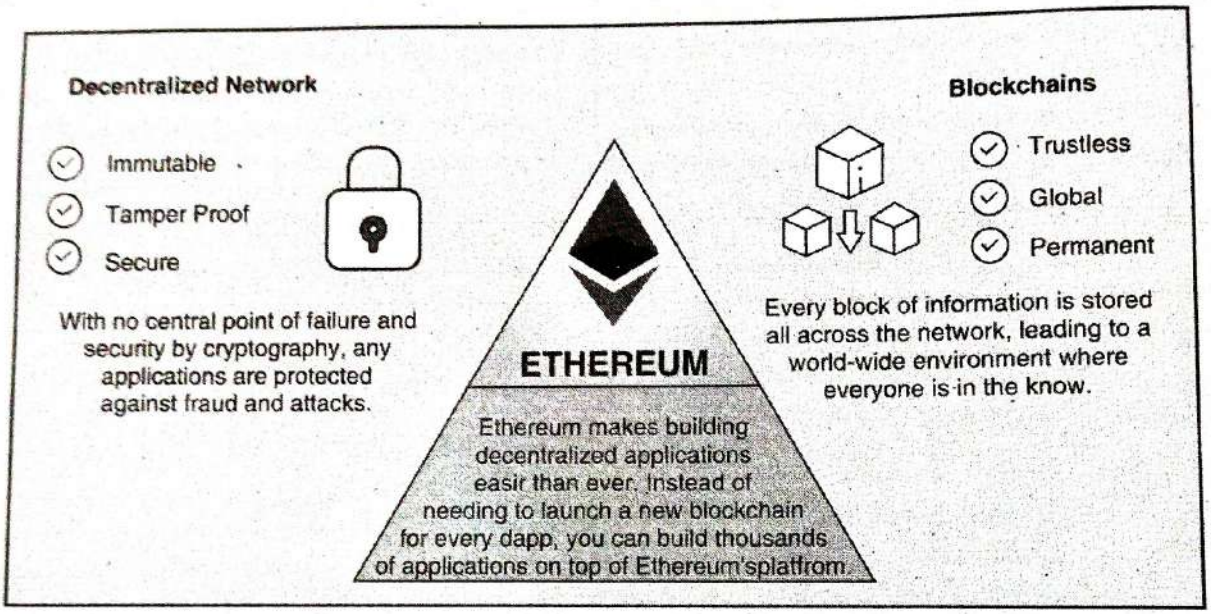


Fig. 3.7

2. Dapp :

- DApp is the 'Decentralized Applications' running on the blockchain. They are the applications that run on blockchain without any centralized control. We can say bitcoin is a decentralized application that runs on Bitcoin blockchain. But it is the Ethereum blockchain that extended the scope of decentralized application and popularized the word DApp.
- DApp uses the shared ledger instead of a server to record and store all the transactions. The DApps will have a set of backend codes as well as a user interface. In Ethereum, these backend codes will contain the smart contract and the front end will provide a user interface for the user to interact with the blockchain. Once the smart contracts are deployed on the blockchain, then the DApp will become accessible in the blockchain. Then any node in the blockchain network can use the DApp.
- The DApps can be developed for any business use cases. Any application that is currently running on the client-server model can be implemented as a DApp. Some examples of Ethereum DApp : Green Ether Project, splitcoin, The immortals.

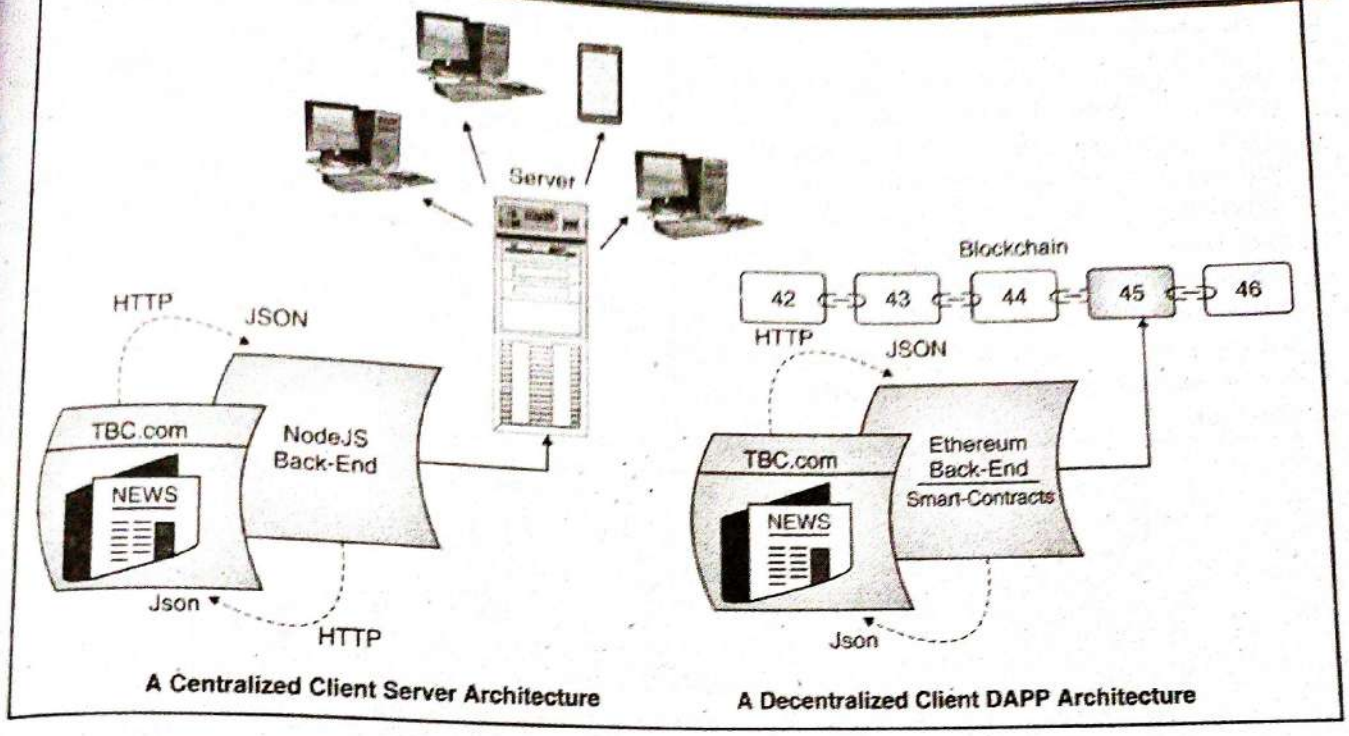


Fig. 3.8

Q. 6 What is hyperledger and hyperledger fabric ?

Ans. : Hyperledger

- Hyperledger Foundation is a non profit organization that brings together all the necessary resources and infrastructure to ensure thriving and stable ecosystems around open source software blockchain projects.
- Hyperledger is a collaborative effort from different industry leaders to frame an open source, Cross-Industry Blockchain aided technologies. The movement basically aims to develop distributed ledgers that can support enterprise level business transactions. The entire project is developed on the open source platform. Even though the project is hosted and driven by the free folk of the internet 'Linux Foundation', technology giants like IBM, Intel, Samsung and many more have already become part of the project.
- The project was announced in December 2015 by Linux foundation, and soon it became popular as leaders from different business domains like banking, healthcare, finance, supply chain, IoT, manufacturing etc. joined the movement. As of now with 170+ members, the project is the largest blockchain technology consortium and it is entirely funded by its members
- Hyperledger Foundation hosts a number of enterprise-grade blockchain software projects. The projects are conceived and built by the developer community for vendors, end user organizations, service providers, start-ups, academics and others to use to build and deploy blockchain networks or commercial solutions. The Hyperledger Foundation staff is part of a larger Linux Foundation team that has years of experience in providing program management services for open source projects.
- Following Fig. 3.9 shows the design philosophy followed by all Hyperledger projects.

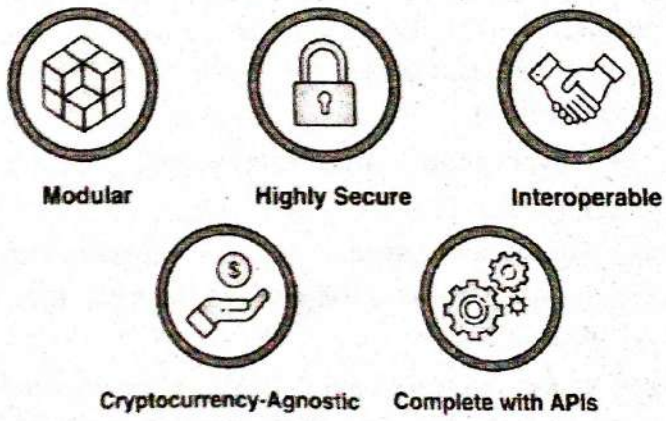


Fig. 3.9 : design philosophy followed by all Hyperledger projects

What Hyperledger does

- The Hyperledger Foundation is focused on consortium networks that link a group of stakeholders to streamline critical, often proprietary business processes and transactions. There is no one Hyperledger blockchain network. Instead, businesses, consortia, and other organizations deploy Hyperledger technologies to build networks that support their needs. With this approach, these networks, or multiparty systems, are modular and flexible enough to support different industries and use cases.
- The diverse and growing Hyperledger ecosystem means enterprises can mix and match technologies to balance privacy and performance; create permissioned, permissionless, or hybrid networks; integrate with legacy systems; or even tap into a cryptocurrency "mainnet". The Hyperledger Foundation does not sell any of these technologies as products or services.

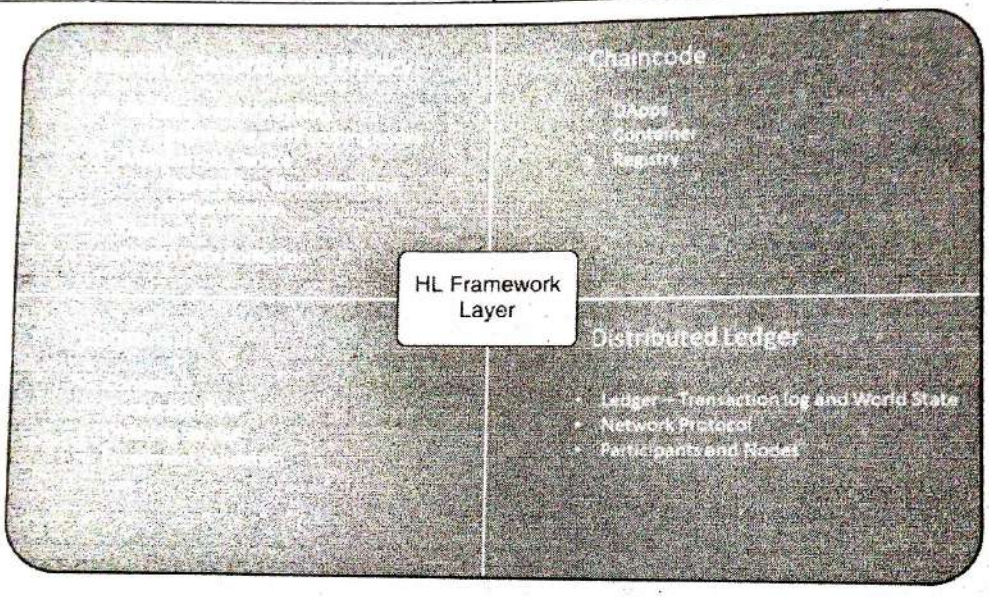


Fig. 3.10 : Hyperledger framework layer

- Hyperledger projects are vendor neutral, meaning that they can be deployed in products and solutions by any company, anywhere in the world. As a result, Hyperledger technologies are used in everything from powering global trade networks and supply chains to fighting counterfeit drugs, banking "unbanked" populations, and ensuring sustainable manufacturing.
- The Hyperledger Architecture has following components :

  i) **Consensus Layer :** It is responsible for verifying blocks of transactions and agreeing on their order.

  ii) **Smart Contract Layer :** It is responsible for transactions pro- cessing7 (proposal takeover, execution and validation).

  iii) **Communication Layer :** It is responsible for P2P transport.

  iv) **Data Store Abstraction :** It is responsible for different data- stores which can be used by other modules.

  v) **Crypto Abstraction :** It is responsible for crypto algorithms.

  vi) **Identity Service :** It enables the establishment of a root of trust during setup of a blockchain instance, the enrollment and registration of identities during network operation, and authentication and authorization.

  vii) **Policy Service :** It is responsible for policy management.

  viii) APIs required for interactions with applications.

  ix) **Inter-operation Service :** In charge of supporting the inter-operation between different blockchain instances.

Hyperledger Fabric

- Hyperledger Fabric is a blockchain framework implementation initially developed by Digital Asset and IBM and now hosted by Linux Foundation under the hyperledger project. Fabric joined the hyperledger project for incubation in early 2016 and after 1 year of incubation, it became the first project to get into the 'active' state. On July 11, 2017, the hyperledger Technical Steering Committee announced their first production-ready distributed ledger codebase, Hyperledger Fabric V1.0.
- The Fabric platform is intended as a foundation for developing blockchain applications, products or solutions. The fabric is a Private and Permissioned system which delivers a high degree of confidentiality, resilience, flexibility, and scalability. It adopted a modular architecture and supports pluggable implementations of different components like consensus, membership services etc. Like other blockchain technologies, Fabric has a ledger and smart contracts. The smart contract in the fabric is known as chaincode and it is in the chaincode the business logic is embedded.

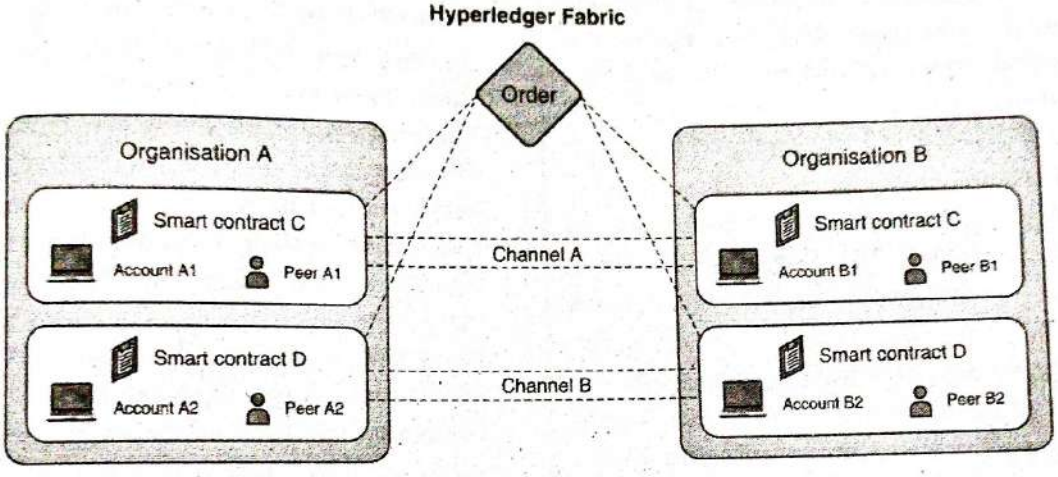


Fig. 3.11 : Enterprise blockchain protocol to develop on the Hyperledger fabric

- The following features impart a high degree of security and privacy for the fabric framework.
  1. **Channels :** The private blockchains built on fabric protocol. Each channel consists of only the authorized partners.
  2. **Visibility settings :** It is possible to restrict who can see the input data using visibility settings.
  3. **Data Encryption :** The data can be Hashed or Encrypted before calling the chaincode.
  4. **Data Access Restriction :** By embedding access controls into the chaincode logic, it is possible to restrict data access to certain roles in the organization.
  5. **File encryption :** Ledger data at rest can be encrypted using file system encryption, and data-in-transit can be encrypted using TLS protocol.
- In the Fig. 3.11 there are two channels created in-between Organisation A and Organisation B. Channel A shares the information only in-between peer A1 and Peer B1 through shared contract C, while Channel B shares the information only in-between peer A2 and Peer B2 through shared contract D.

Q. 7 What are the objective of Blockchain Consensus Mechanism and also explain types of consensus Algorithm ?

Ans. : Consensus in Blockchain

Consensus algorithms are a primary part of blockchain technology. They are used to guarantee that the "main chain" at every node of the network is the same. This results in a consistent state of the blockchain across all the nodes in the network. Blockchain consensus algorithm is that, it is a procedure via which all the peers of a Blockchain network reach a common acceptance or consensus about the real-time state of the distributed ledger.

Objectives of Blockchain Consensus Mechanism

1. **Fair & Equitable :** Consensus mechanisms enable everyone to participate in the network and use the same fundamentals. Thus, it justifies the property of open-source and decentralization of the blockchain system.
2. **Unified Agreement :** The protocols enclosed in the Distributed blockchain network ensures that the data involved in the process is genuine and accurate, and the status of the public ledger is up-to-date.
3. **Alignment of Economic Incentive :** A consensus blockchain protocol, rewards for good behavior and punishes bad actors. In this way, the economic incentives are regulated too.
4. **Prevention of Double Spending :** Consensus mechanisms ensure that only those transactions are included in the public transparent ledger which are verified and validated. This solves the traditional problem of double-spending, i.e, spending a digital currency twice.
5. **Fault Tolerant :** Another feature of the Consensus method is that it ensures that the blockchain is fault-tolerant, consistent, tested and reliable. This implies that, the governed system would work infinite times even in the case of failures and threats.

Types of Consensus

- With the basics of Blockchain consensus methods being covered, let's look at the popular types of consensus mechanisms.
- Different consensus algorithms are used for the process of validation of transactions depending on the platform used to implement it. These algorithms are nothing but the set of rules defined to regulate the proper performance of the system. To prevent malicious activities in blockchain technology different consensus algorithms used are :
  - Proof of Work (POW)
  - Proof of Stake (POS)
  - Practical byzantine fault tolerance (PBFT)
  - Delegated Proof of Stake (DPoS)
  - Proof of Burn (PoB)
  - Proof of Activity (PoA)
  - Proof of authority
  - Proof of Elapsed Time (PoET)
  - Proof of Weight (PoWeight)
  - Proof of Trust (PoT)
  - Proof of Capacity (PoC)
  - Proof of Importance (PoI),
  - Raft Algorithm Proof of Vote (PoV)
  - Leased Proof of Stake (LPoS) etc.
- When a transaction occurs it is validated by some nodes. The term Validity here refers to the sufficiency of money with the sender and the digital signature of the sender. After verifying the validity, the block holding the transaction is added to the chain which can be identified by all other nodes.
- A node can append a block holding various transactions by distributing it to another node which has requested to add this node to the current chain. The only limitation in this method is that, if every node requests its preferable node, then it creates chaos in the system. To prevent this, the consensus algorithm is introduced, which holds an agreement made between all nodes about which blocks should be appended, and which nodes are permitted to append their proposed blocks. Many versions of the consensus algorithm have been proposed till date.
- Consensus can be implemented through various ways such as lottery-based algorithms like Proof of Work (PoW) and Proof of Elapsed Time (PoET) or by voting-based methods which include Paxos and Byzantine Fault Tolerance (BFT). These methods depend upon various fault tolerance models and network requirements.
- The lottery-based algorithm is also known as the Nakamoto consensus, which is named after the founder of Bitcoin. In this algorithm a person is elected as a validator, who makes decisions about the next node to be appended.

Q. 8 Explain Proof of work ?

Ans. : Proof of Work

- It is the first consensus algorithm used in blockchain technology to confirm the transaction and add a new block to the chain. It is based on the principle of a very challenging problem to find the solution and easy to verify that solution. It includes special nodes in the network to do calculations to solve the complex mathematical puzzle called miners which requires a lot of computational resources.

- The mathematical puzzle complexity depends on the users in the network, network load, current power, and time required to confirm the transaction.
- The solution generated from the mathematical puzzle is called a hash and it must be smaller than the hash of the block for which the new block is to be accepted, known as the target hash. Miners need to guess the nonce which is attached to the hash content of the block, rehash the value, and again compare with the target hash, one can apply a trial and error method to get the solution.
- The target hash is adjusted after every 2016 blocks are mined. The PoW consensus algorithm widely uses SHA -256 cryptographic protocol. The major drawbacks of the PoW algorithm are increased consumption of energy and resources, and 51% of the hash rate attack.

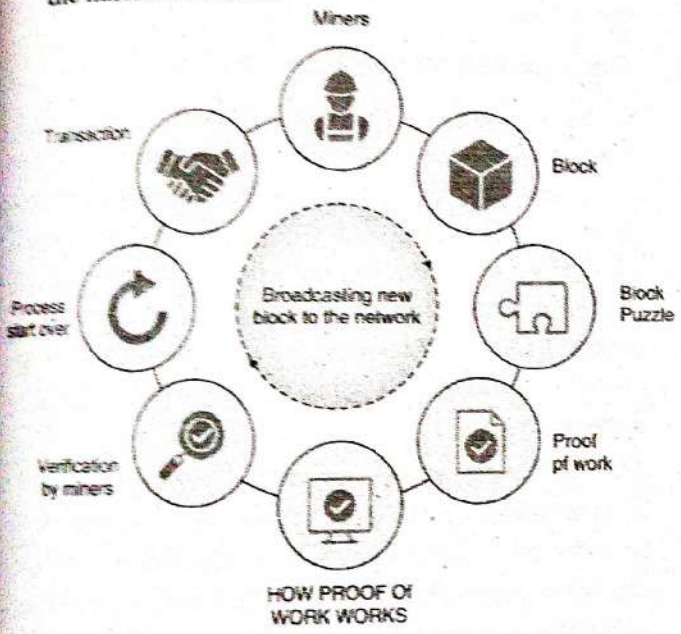


Fig. 3.12 : The working of PoW

- Proof of work (PoW) is the first consensus protocol used for cryptocurrency that permits the blockchain users to obtain consensus in Bitcoin. This protocol also uses the Merkle tree, Peer-to-Peer (P2P) network to create, broadcast and verify blocks in the blockchain network.
- PoW also experiences costly digital computation since it includes various techniques to accomplish the process. The properties of PoW are described as follows :
- The main objective of PoW is to manage the consensus; a newly entered node can detect the current state of the network based on the protocol rules.
- PoW is developed for permission-less public distributed ledgers and for mining processes, it consumes more computational resources.
- To construct a new block, the miner should solve a cryptographic puzzle, and the user who solves the puzzle first will avail the reward by broadcasting the result in the network.
- The protocol maintains the transactions in each block in a linear fashion and a block consists the set of transactions.
- The cryptographically signed transaction will be accepted only if the signature is validated and verified in the network.
- This protocol fairly distributes a reward. If 'p' fraction of whole computation power is determined with the miner, then they would have a probability 'p' to mine the subsequent blocks.
- The challenge-response computation process is called as mining.
- If any conflict arises, then the protocol releases multiple branches of blocks, however the longer one is retained as the trusted branch.

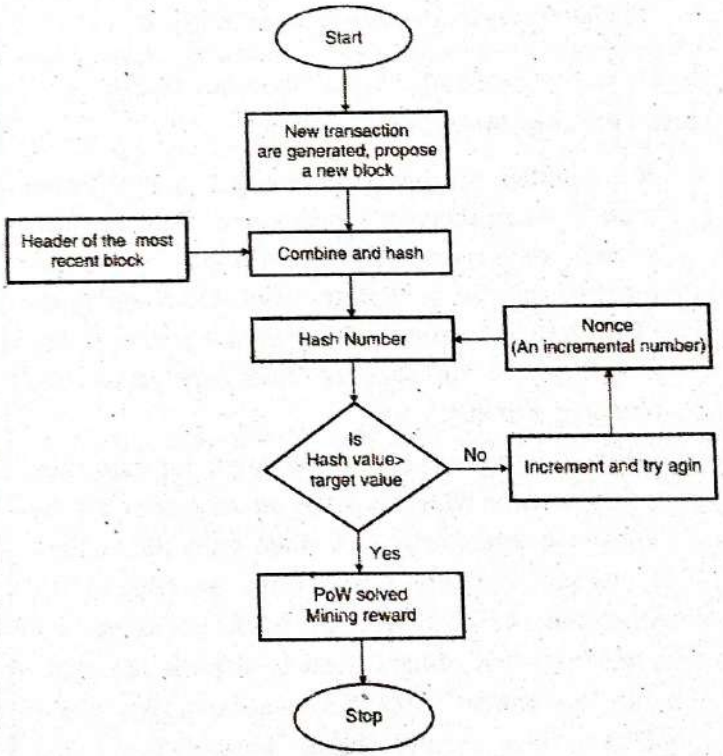


Fig. 3.13 : Flow chart of steps involved in Proof of work

- PoW presents mining that involves a step for the validation of a block (group of transactions) in the network by providing the computational proof of the completed work.

- Once a transaction is started, the available miners in the network compete with each other for becoming first by solving a cryptographic puzzle and form the block. The solution to the block among other peers is broadcasted by the miner who solves the puzzle successfully and the solution is verified to make the new block acceptable on the chain.

Analysis :

- PoW is a power-consuming protocol that requires a vast amount of computation power which is simply a wastage of resources.
- In PoW, the difficulty level increases and along with it the power required to solve the cryptographic puzzle also increases.
- PoW is extremely vulnerable to Sybil attacks, Denial-of-Service (DoS) attacks and selfish mining attacks. The requirement of high computational power by PoW also guarantees a high level of security. 51% of computational power is required by the attacker which is simply impossible considering the difficulty level of this protocol.
- An Application-Specific Integrated Circuit (ASIC) is the hardware that manages the mining process.

Q. 9 What is the Proof of Stake Consensus algorithm ?

Ans. : Proof of Stake (PoS)

- It is another consensus mechanism. In POS, rather than miners, there are validators. They are also known as forgers. Powerful computers are not required for POS as there is no mining competition. The significant drop in the cost and energy-saving nature on a comparative scale are some key advantages of POS.
- In POS, the miner is chosen randomly for validation of a transaction which depends on the money he/she deposits in a network called stake. More the number of stakes, more are the chances to validate the transaction. A rich stakeholder is chosen as a miner by the network. Miners need to deposit the stake before the validation of the transaction, if a miner validates the invalid block he/she loses the deposited stake.
- The amount of stake to be deposited must be greater than the reward received after transaction validation to avoid the malicious node to be added to the chain. After validation of valid transactions, miners receive the transaction fees, as well as the stake of miners, is returned. But the selection of miners based on stake may give rise to centralization as the richest person always gets the chance to validate the transaction. To prevent this problem there should be a variation in the selection of miner, the most popular method for the selection of miners are :

1. Randomized Block Selection method :

It uses the formula to select the miner where the combination of, lower the hash value and the size of the stake will get the chance to validate the block. As the size of the stake is public, all the stakeholders in the network can guess who will be the miner to validate the next transaction. Nxt and Blackcoin are examples of proof of stake based crypto-currency using a randomized block selection method to select the miner.

2. Coin Age-Based Selection method :

- In this method the miner is selected based on the coinage of the stake. The coinage is determined by taking the product of the number of coins with the number of days the coins are staked and held by the user. The coins must be held for a minimum of 30 days after staking or validating the block. The node with a large set of coins and senior stakeholder has more chances to be selected for the validation of the transaction.
- After validation of the transaction, the coinage is set to zero, and after 30 days he/she has the chance to be selected as a miner. All the stakeholders get the chance of regularly validating the block and building a healthy decentralized miner community. After validation of the transaction and adding the block to the chain, the miners receive a reward as a transaction fee which is expected by the miner to earn by staking their coins with the targeted interest rate. Peer coin is an example of proof of stake-based cryptocurrency which is based on the coin age-based selection process.
- POS is considered a safer mechanism than POW as 51% of a network needs to be owned by the hacker. Such a breach is possible but it is unlikely. Besides, it will be very expensive to hold that much stake.

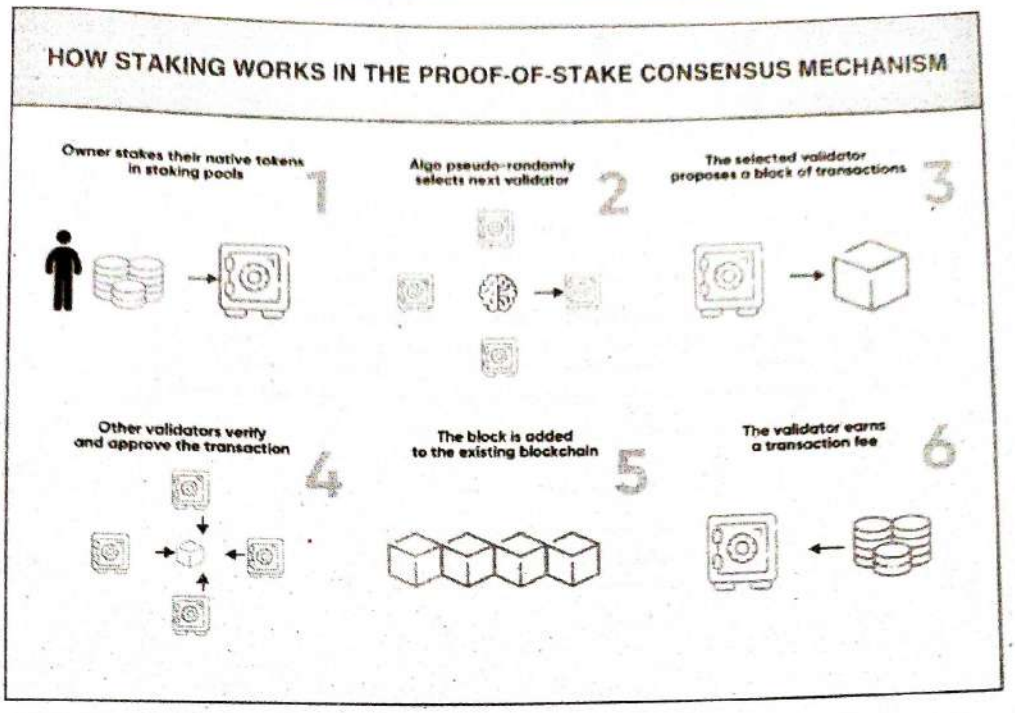


Fig. 3.14

- The various properties of PoS are described as follows :
  - The computational challenge-response process in the protocol is known as minting.
  - A new node always requires rules, protocol messages and recent state to reach the current state of the blockchain network.
  - The new coins are not being generated in PoS, hence there is no block reward and only the transaction fee will be taken by the miner in PoS.
  - The miner for a specific block is chosen based on the economic stake in the network.
- Ethereum is an open-source blockchain influenced by PoS to reach consensus. At first, it was based on PoW cryptocurrency, but later the consensus mechanism was shifted to Proof of Stake, and it became more secure and energy-efficient.
- Other PoS-based cryptocurrencies are Peercoin, Navvcoin, Neo,Decred, Dash, PivX and Reddcoin. Another popular POS blockchain platform is Cardano.

Analysis :

- POS is an eco-friendly protocol since it requires a negligible amount of computation. Furthermore, it does not need any specialized hardware for active participation.
- PoS is profitable for many stakeholders and it is also energy-efficient.
- To prevent the network from security attacks, an economic penalty approach is followed in PoS to punish the colluding participant. As a matter of fact, it is very effective because only major stakeholders can influence the network, and they will try to avoid penalties in the network. The penalty scheme is successfully implemented on the Ethereum platform.

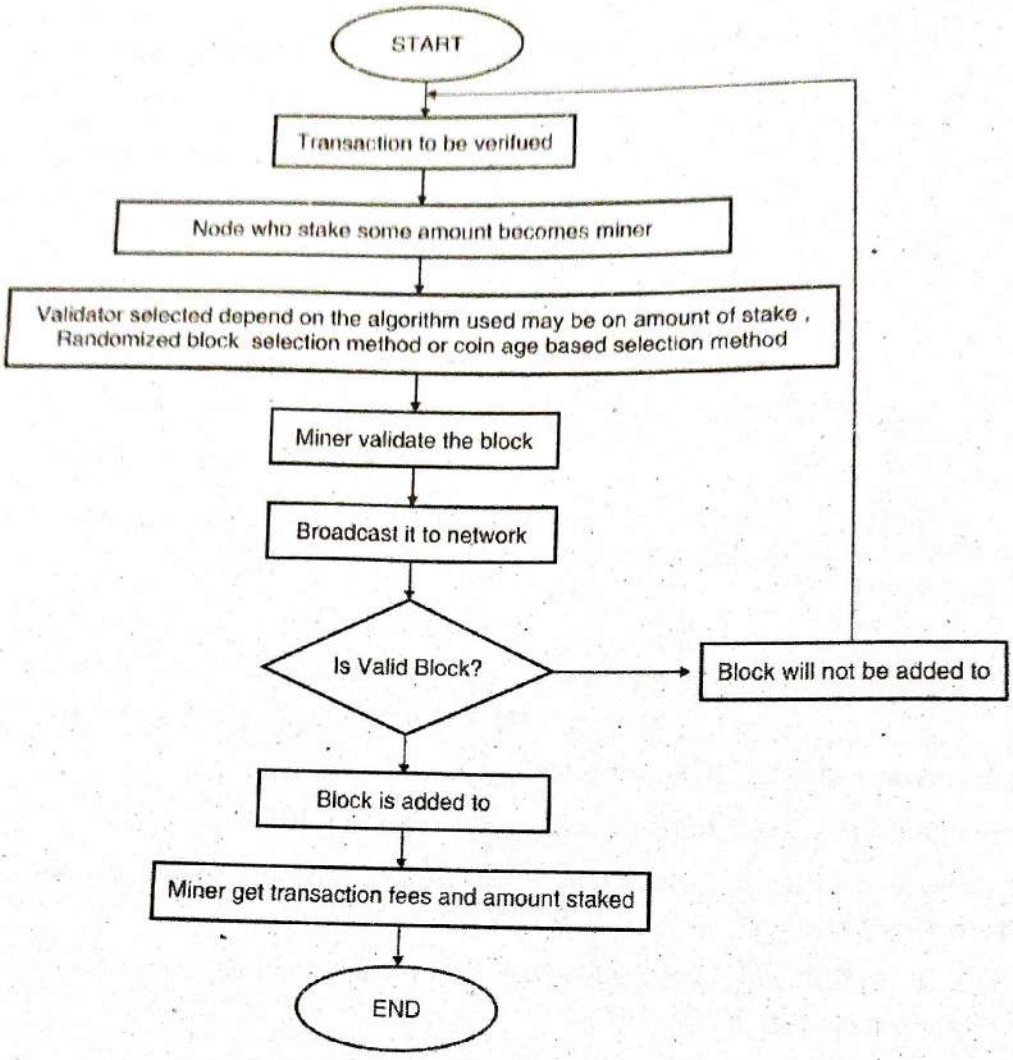


Fig. 3.15 : Flowchart of PoS

Q. 10 Explain the Proof of Elapsed time consensus algorithm.

Ans. : Proof of Elapsed Time (PoET)

- It is the Permissioned blockchain consensus algorithm. A lottery system is followed for the selection of miners. A Random waiting time slot is provided to the miners, after the waiting time is finished the miner can mine the block. During the random wait time, the miners' processor can go to sleep, hence increasing the efficiency of the system.
- PoET uses Intel-based hardware (e.g. Intel SGX), and it is specifically designed for permission-less public distributed ledgers. The participants' and transaction logs are transparent and sustainable, proving more reliability of the network.
- In the PoET protocol, each validator is assigned a 'T' random wait time to construct the block and it is tracked by it. The creation of the block in the network can be done by the validator who has successfully completed the waiting time. The protocol follows both first come first serve (FCFS) and a random lottery scheme. The entire process relies on Software Guard Extensions (SGX) which ensure trusted code execution in a safe environment
- The protocol is highly vulnerable to various security attacks and lacks security analysis. Intel Software Guard Extension is prone to rollback attacks. Hyperledger Sawtooth is a modular blockchain introduced by Intel, and it follows the PoET consensus algorithm for implementing a leader election lottery system.

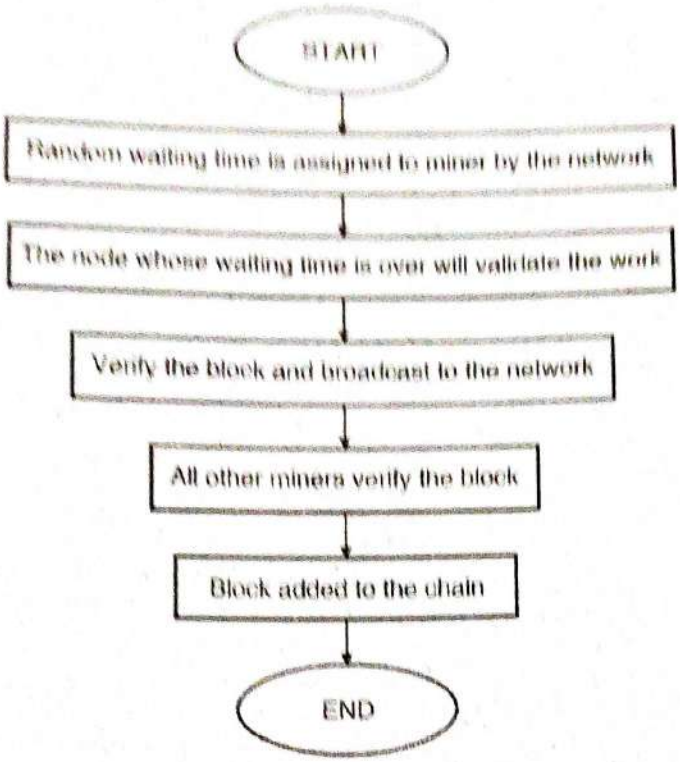


Fig. 3.16 : Steps in Proof of Elapsed Time (PoET)

Q. 11 Explain Proof of Activity and Proof of Burn Consensus Algorithm.

Ans. :

Proof of Activity (PoA)

- Proof of Activity(PoA) is the combination of the PoW and PoS algorithms. Mining in PoA begins like PoW, mathematical puzzles are generated by the server in the network and broadcast over the network. The miners try to figure out the puzzle.
- The first node who solves the puzzle demands for the reward, but the difference between PoW and PoA is that the block does not contain any transaction, they are simply templates with the header information and the mining reward address.
- After mining the blank block the PoA follows the PoS algorithm. The content in a block related to the header is used for random selection for a group of validators to sign the block.
- The node having a large number of stakes has more chances to get selected as a validator. After the block is signed by all the elected validators it will get added to the chain, if some validators do not sign the block it will get rejected and validators are looking for the next winning block. The reward after adding the block to the chain will get distributed between the validators.
- Espers and Decred coins are the two real-world implementations of this mechanism.

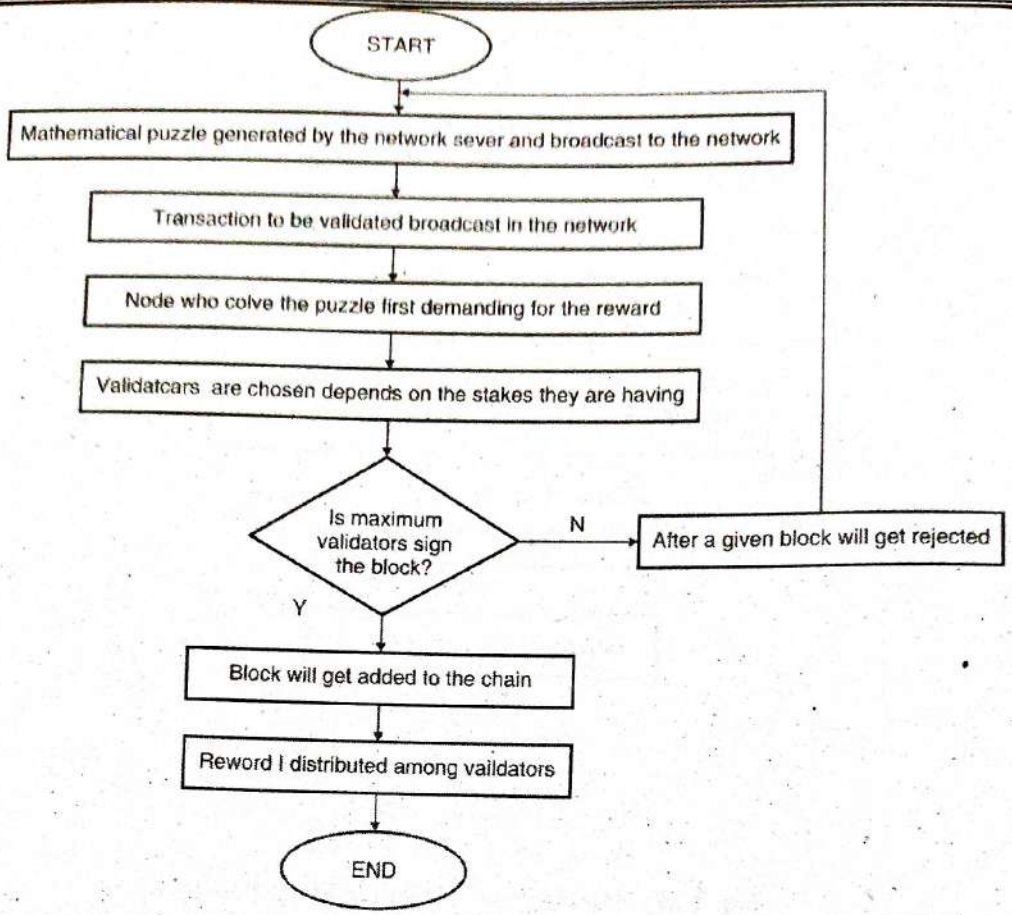


Fig. 3.17 : Flowchart of PoA

Proof of Burn (PoB)

- This algorithm is implemented to avoid double-spending attacks. It is also called PoW without wasting of energy. It follows the principle of the burning of coins and gets the right for mining. The miners get the chance of mining by burning the coins which are proportional to the number of coins burnt.
- Depending upon the number of coins burnt, the miners can buy a virtual mining rig which gives the right to validate the block. Miners send the coins to a provably unspendable address for burning. The resources used for this process are less and hence the network remains active. PoB consensus algorithm is used by the Slimcoin cryptocurrency.

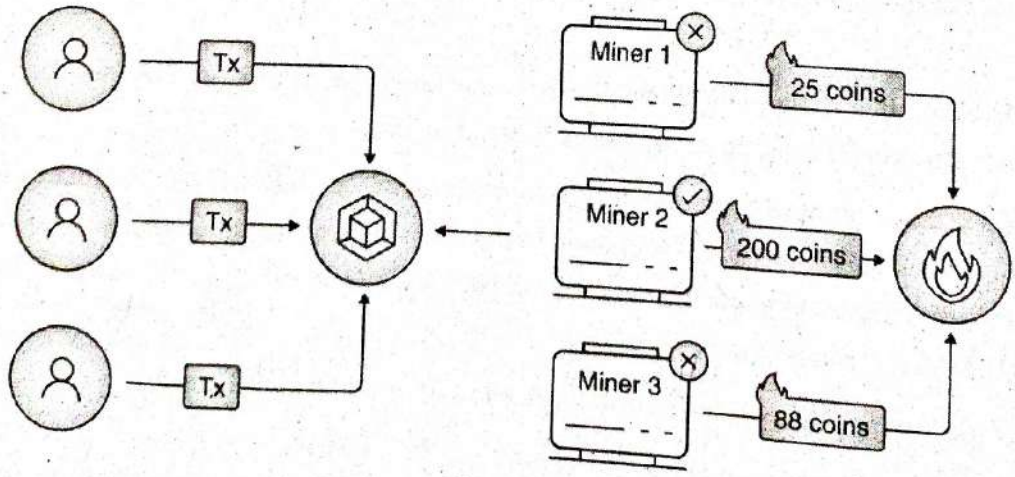


Fig. 3.18

Advantages

- Encourages long-term commitment by the miners.
- More sustainable and reduced power consumption.
- Coin burning tends to reduce the circulating supply (market scarcity).
- Coin distribution/mining tends to be less centralized.
- No need for mining hardware. Coin burns are virtual mining rigs.

Disadvantages

- For an average user, the process of burning coin is not always transparent or easily verifiable.
- The verification of the work is done by miners which tends to be delayed. It is not as fast as in Proof of Work blockchain networks.
- Not proven to work on larger scales. Much of the testing is required to confirm its efficiency and security.
- As the Bitcoins being burned are generated through PoW mining, which requires lots of resources, some say that PoB is not really eco-friendly.

Q. 12 What is BFT ?

Ans. : Byzantine Fault Tolerance (BFT)

In a blockchain network, nodes need to agree on the current state of the blockchain regularly, and that is what is known as consensus achievement. However, reaching consensus on distributed networks is not an easy, safe and efficient task. It becomes difficult to agree on a decision in a distributed network if some of the nodes act dishonestly or fail. This is the fundamental question of the Byzantine Generals' problem, which gave birth to the concept of Byzantine fault tolerance.

Byzantine Generals' Problem

- The Byzantine Generals' Problem was formed in 1982 as a logical dilemma that illustrates how a group of Byzantine generals may have communication problems when trying to agree on their next move.
- The dilemma assumes that each general has its own army and that each group is located in different locations across the city they intend to attack. The generals require to agree on either retreating or attacking. It makes no difference whether they attack or retreat, as long as all generals reach consensus, i.e., all agree on a common decision in order to execute it in coordination.
- Therefore, we may consider the following requirements :
- Each general needs to decide whether to attack or retreat (yes or no);
- Once the decision is made, it cannot be changed;
- All generals have to agree on the same decision and execute it in a synchronization.
- The prior mentioned communication problems are related to the fact that one general is only able to communicate with another through messages, which are forwarded by a courier. As a consequence, the central challenge of the Byzantine Generals' Problem is that the messages can somehow get delayed, destroyed or lost.
- In addition, even if a message is delivered successfully, one or more generals may decide (for whatever reason) to act maliciously and send a false message to confuse other generals, leading to a total defeat.

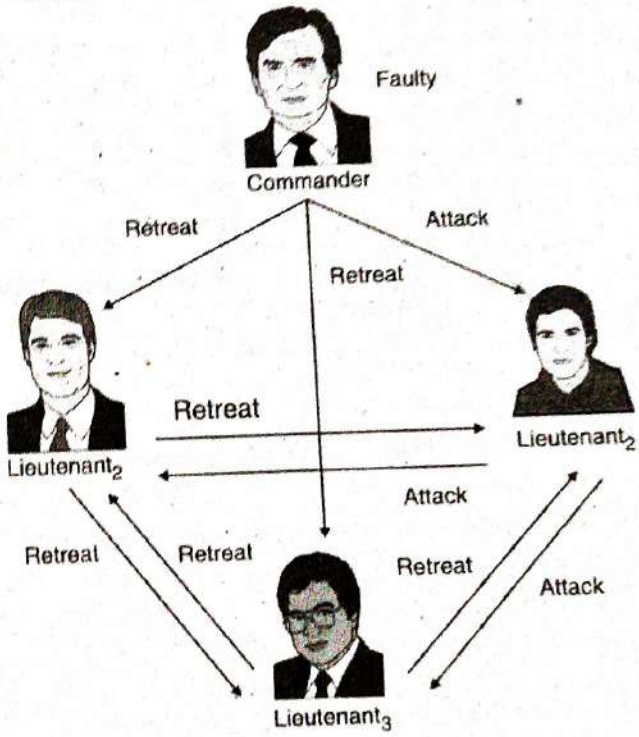


Fig. 3.19 : Byzantine Generals' Problem, leads to defeat

- If we apply the dilemma in context with blockchains, each general represents a network node, and the nodes need to reach consensus on the current state of the system. Putting it another way, in order to avoid complete failure, the majority of participants within a distributed network need to agree and execute the same action.

Byzantine Fault Tolerance (BFT) Consensus

- Therefore, the only way to accomplish consensus in these types of distributed systems is by having at least 2F +1 honest and reliable network nodes. Where F is a malicious or defective node.
- Fig. 3.20 shows that there are four nodes, with one defective node. Defective node sends the attack message to two nodes and a retreat message to one node. All other three nodes broadcast the message that it receives, so all the non malicious or non faulty nodes receive more number of attack messages than the retreat and they decide to attack and the consensus is reached.
- Byzantine Fault Tolerance (BFT) is the property of a system which is able to resist the class of failures derived from the Byzantine Generals' Problem. This means that a BFT system is able to continue operating even if some of the nodes act maliciously or fail.
- Byzantine fault tolerance-based consensus is used in the popular Hyperledger Blockchain platform used by many organizations, especially IBM. A variant of Byzantine fault tolerance called the Practical Byzantine Fault Tolerance (PBFT) is proposed by Castro and Liskov which is intended for Hyperledger Fabric.

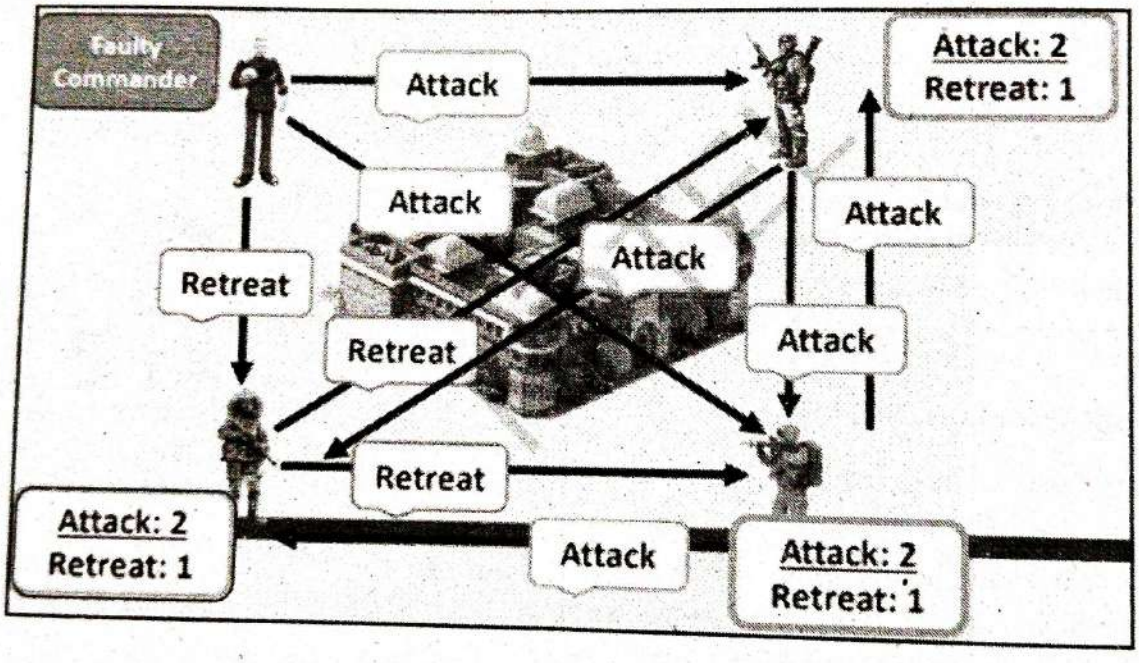


Fig. 3.20 : Byzantine Fault Tolerance (BFT) reached consensus with 2F+1 node

Chapter 4 : Cryptocurrency : Bitcoin, and Token

Q. 1 Explain Bitcoin Wallets in details ?

Ans. : Bitcoin Wallets

- A client application that speaks the Bitcoin protocol can access the protocol. "Bitcoin wallets" are most commonly used to interface with the bitcoin system, just as a web browser is most commonly used to interact with HTTP.
- As with web browsers (e.g., Chrome, Safari, Firefox, and Internet Explorer), there are many bitcoin wallet implementations and brands.
- Bitcoin wallets are one of the most actively developed bitcoin applications. Depending on the platform, Bitcoin wallets can be classified as Hot or Cold wallets :

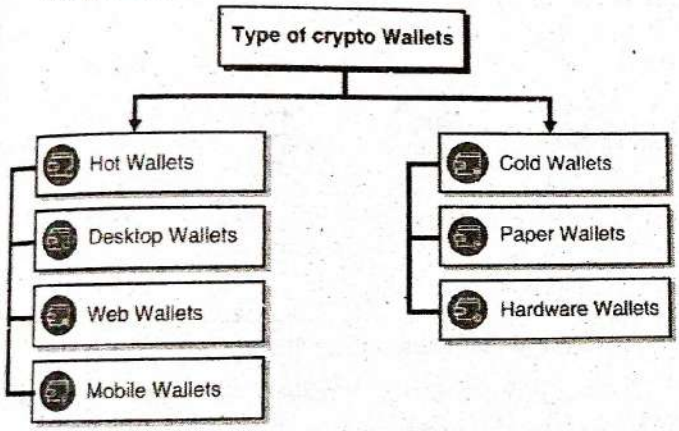


Fig. 4.1

1. **Desktop wallet :**

Desktop wallets are popular because of their features, autonomy, and control. Desktop wallets are the first type of bitcoin wallet. The use of general-purpose operating systems such as Windows and Mac OS has certain security disadvantages due to their insecurity and poorly configured nature.

2. **Mobile wallet :**

Mobile wallets are the most common type of Bitcoin wallet. Working with smartphone operating systems such as Apple iOS and Android, this wallet is a great option for new users. Many are designed to be simple and easy to use, but there are also full-featured mobile wallets for power users.

3. **Web wallet :**

A web wallet is accessed from a web browser and the user's wallet is stored on a server owned by a third party. This is similar to his webmail in that it relies entirely on third party servers. Some of these services work with client-side code running in the user's browser, putting control of the Bitcoin key in the user's hands. However, most represent a compromise of controlling the user's bitcoin key in exchange for ease of use. Storing large amounts of bitcoins in third-party systems is not recommended.

4. **Hardware wallet :**

A hardware wallet is a device that runs a secure, self-contained Bitcoin wallet on dedicated hardware. They work over USB in desktop web browsers or over Near Field Communication (NFC) in mobile devices. By handling all bitcoin-related operations on dedicated hardware, these wallets are considered highly secure and suitable for storing large amounts of bitcoin.

5. **Paper wallet :**

Keys used to control Bitcoin can also be printed for long-term storage. These are called paper wallets, but other materials (wood, metal, etc.) can also be used. Paper wallets offer a simple and highly secure way to store bitcoins for the long term. Offline storage is also referred to as cold storage.

Bitcoin wallets are also categorized by their level of autonomy and how they interact with the Bitcoin network.

6. **Full-node client :**

A full client or "full node" is a client that can store the full history of Bitcoin transactions (all transactions from any user), manage a user's wallet, and initiate transactions directly on the Bitcoin network. A full node handles all aspects of the protocol and can validate the entire blockchain and each transaction independently. A full node client consumes significant computing resources (125+ GB hard disk, 2 GB RAM, etc.) but offers full autonomy and independent transaction validation.

7. **Lightweight client :**

A lightweight client, also known as an SPV (Simple Payment Verification) client, connects to a Bitcoin full node (described above) to access Bitcoin transaction information, but stores user wallets locally, creates transactions, and independently verifies them. A lightweight client interacts directly with the Bitcoin network without an intermediary.

8. **Third-party API client :**

Third-party API clients interact with Bitcoin through a third-party system of application programming interfaces (APIs) rather than connecting directly to the Bitcoin network. Wallets can be stored by the user or by a third party server, but all transactions go through the third party.

Bitcoin Core Architecture

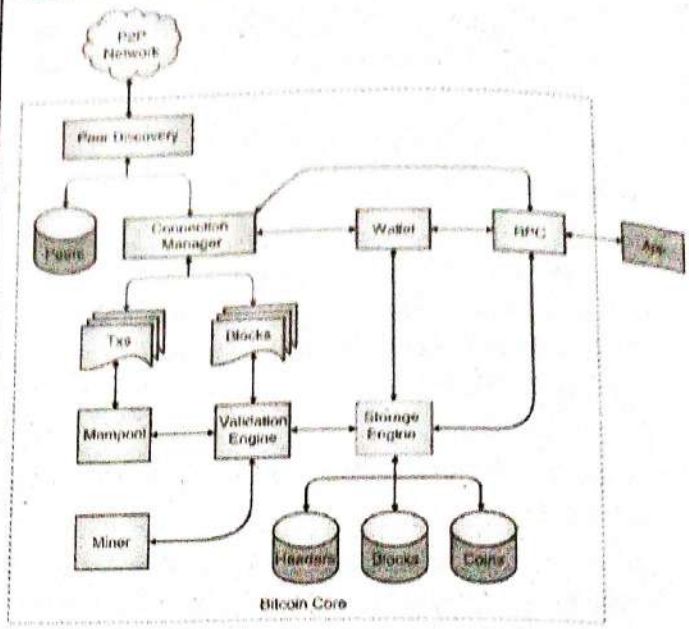


Fig. 4.2 : Bitcoin Core Architecture

Q. 2 What is Cryptocurrency ?

Ans. : Cryptocurrency

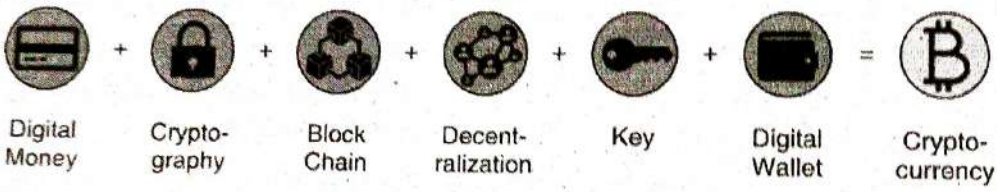


Fig. 4.3

A cryptocurrency (or "crypto") is a digital asset that can be circulated without the need for any central authority such as a government body and banks. Instead, cryptocurrencies are created using cryptographic technology to allow people to buy, sell, or trade securely.

Cryptocurrency

- Cryptocurrency is a digital or virtual currency that works on cryptographic principles. As the name suggests, they have no physical existence or are intangible. They exist only as sets of programming code. However, it offers greater security and ease of use than many existing currencies.
- Cryptocurrencies go hand in hand with blockchain technology. We have already seen how blockchain works. For cryptocurrencies, the ledger tracks cryptocurrencies generated and traded on the network. Every person on a given blockchain has a unique account ID/address. Cryptocurrencies are always associated with these accounts (currencies are debited and credited to this account).
- Users can manage their accounts through applications called wallets. Through the wallets, anyone can conduct transactions with anyone on the network (both sender and receiver must have an account). Transactions are verified by peers and added to the blockchain ledger (database). Blockchain's immutable, cryptographic ledger is therefore the backbone of cryptocurrencies.

PROS and CONS of Croptocurrency :

Sr. NO.	PROS	CONS
1.	No restrictions on payment	Lack of awareness / knowledge
2.	Maintenance of Anonimity	Use of complex technique
3.	Use of complex algorithm	Highly volatile in nature

Sr. NO.	PROS	CONS
4.	Speed of Exchange	Not Accepted everywhere
5.	No Third part involvement	Victim of theft and scam
6	Free/very less transaction fee	No reverse of payment and recovery
7	No Inflaction	Black market
8	-	Scaling issue
9	-	May not be exchanged with Fiat currency.

Q. 3 Explain Crypto Wallets in Detail ?

Ans. : Crypto Wallets : Metamask, Coinbase, Binance

1. MetaMask

- MetaMask is a web browser add-on that allows anyone to run Ethereum DApps without running a full Ethereum node. A full node installation of Ethereum consumes a lot of disk space and time. Metamask is therefore the tool that removes this hectic installation overload. Initially, Metamask was only available for Google Chrome, but now it's available for Firefox and other popular web browsers.
- The MetaMask add-on for Chrome can be added from the Chrome Web Store or the metamask.io website. This MetaMask extension provides a user interface for interacting with the blockchain. Users can connect to the main Ethereum network or "testnet" or create their own private network to run DApps on the blockchain.
- Normally, to interact with Ethereum DApps, you need web3.js (JavaScript API for Ethereum DApps) installed on your local system. Web3.js is a collection of libraries used to interact with Ethereum nodes, local or remote, over HTTP or IPC connections.
- However, MetaMask injects web3.js into each page to access the Ethereum blockchain itself. This approach eliminates the overhead of installing web3.js on your local system. After adding Metamask, users can operate the Ethereum blockchain as usual. Users can create accounts, access Ethereum DApps, and deploy their own DApps once. MetaMask retrieves data from blockchain and allows users to manage their data securely.
- Metamask provides each user with a vault account. This vault secures, stores, and controls access to tokens, passwords, certificates, API keys, and other items within blockchain apps. A vault account serves as a second level of encryption for a user's account.

Wallet seed

Metamask provides a group of 12 words called "wallet seeds" during installation. This is the user's credentials and should be kept in a secure location. Users can also create passwords for their accounts. A wallet seed or password is required to log in to metaMask. A vault account encrypts the user's metadata and stores it securely within the browser itself.

Benefits of MetaMask

- MetaMask made the Ethereum system very accessible to the average consumer, and it was a very smart move. It is clear that there are many advancements that the Ethereum ecosystem has to offer, but even accessing dApps remains a challenge for many due to the need to run a full Ethereum node. Therefore, the MetaMask tool brings great peace of mind to the average ICO investor as this tool fills this gap. MetaMask allows users to access dApps directly from Google Chrome through plugins, thus fixing most of the problems common people encounter.
- This alone is a huge improvement as this was a major challenge for many people as dApps were unresponsive due to the complex process. MetaMask also provides users with a secure identity store, allowing them to manage their identities on various websites and even using these identities to sign blockchain transactions. The tool also has a pleasant user interface that presents things well, lowering the barriers to entry and usage in terms of dApps and Ethereum. MetaMask is expected to take the Ethereum ecosystem to the next level in the coming months and years.

2. Coinbase

What is coinbase?

The Coinbase platform allows users to buy, sell, transfer, and store digital currencies securely online. Coinbase's mission is to build a financial system that is open to the world and to be a leading global brand that helps people convert digital currencies into and out of their local currencies.

Features of Coinbase

- Buying and Selling digital currency is easy.
- Sending or receiving digital currency between online crypto balances, friends, or merchants on Coinbase is free
- Security and backups are maintained by coinbase itself..
- It offers primary balance service, an exchange and merchant tools within one simple interface.
- Coinbase is a platform on which many applications are being built using API provided by coinbase.

Some of the major cryptocurrencies supported by coinbase are listed below

1)

Bitcoin (BTC)

2)

Ethereum (ETH)

3)

Ethereum 2 (ETH2)

4)

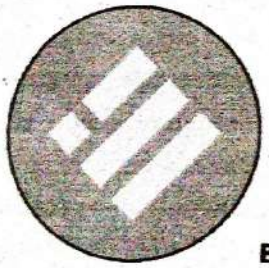
Tether (USDT)

5)

USD Coin (USDC)

6)

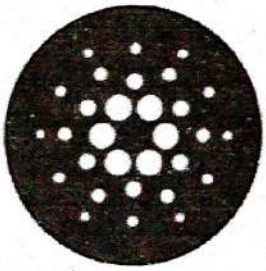
BNB (BNB)

7) 

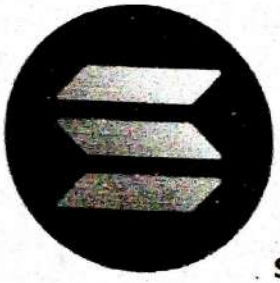
Binance USD (BUSD)

8)

XRP (XRP)

9) 

Cardano (ADA)

10) 

Solana (SOL)

3. Binance

Binance (Binary Finance) : A crypto exchange platform. Binance's matching engine can sustain 1,400,000 orders per second.

Features of Binance :

1. Spot trading
2. Margin trading
3. Futures
4. Anonymous instant exchange
5. Decentralized (on-chain) exchange

Binance supports trading pairs in the following coins :

1. BTC
2. ETH
3. LTC
4. NEO (ANS)
5. BNB (Binance Coin)

More coins will be added over time. Binance only adds coins that have strong credibility, user base, and liquidity.

Device Coverage :

Binance can offer the following cross-platform trading clients:

1. Web-based trading client
2. Android native client
3. iOS native client (pending App Store review)
4. Mobile HTML5 client (including WeChat H5 client)
5. PC (Windows) native client
6. REST API

Binance User Interface

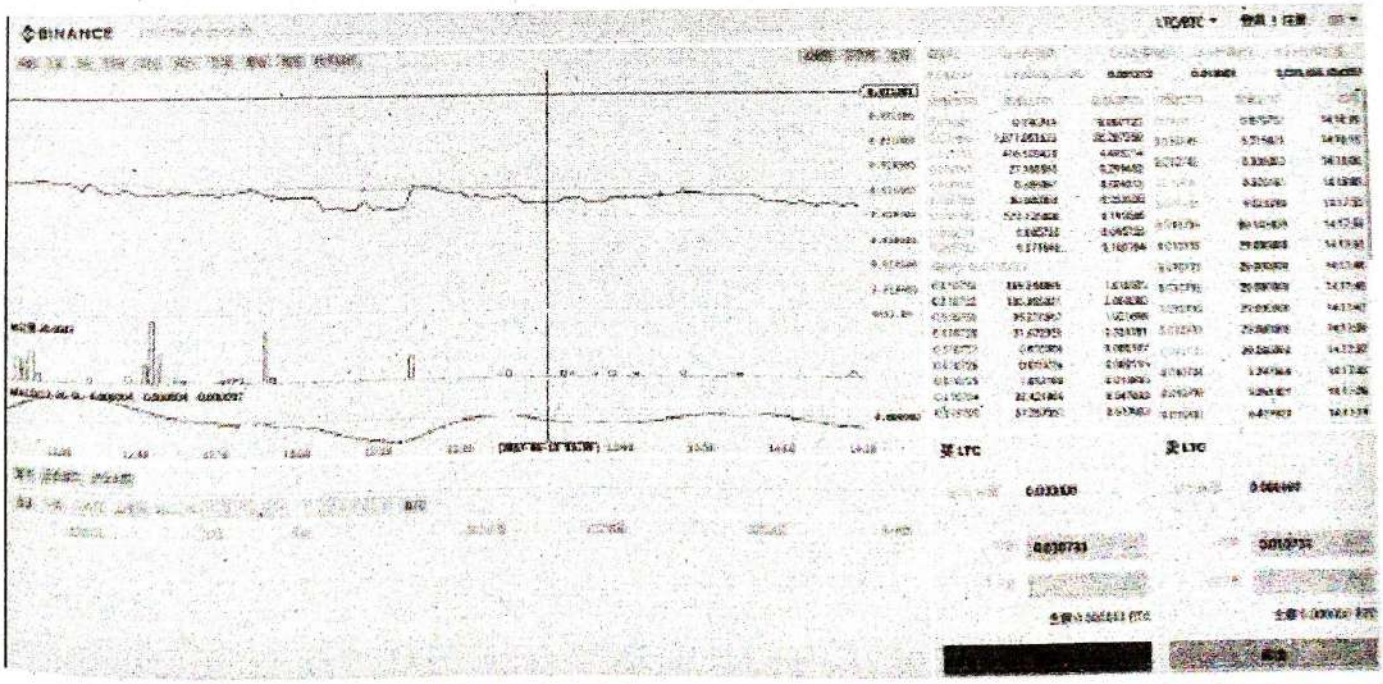


Fig. 4.5 : Web trading interface

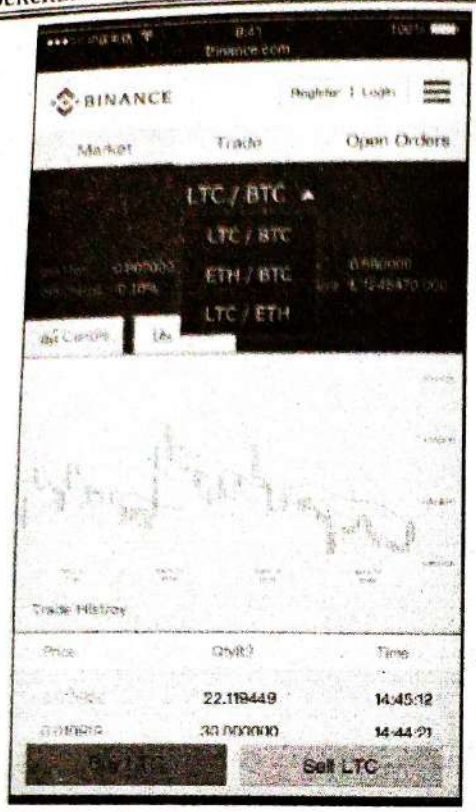


Fig. 4.6 : Mobile HTML5 Market data

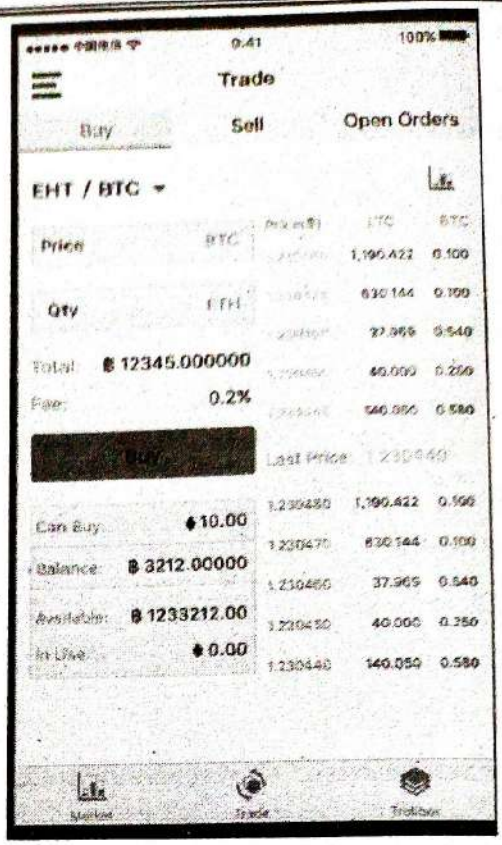


Fig. 4.7 : iOS trading page

BNB :

Binance has created two cryptocurrencies : Binance Coin (BNB) and BinanceUSD (BUSD). Launched in September 2020 as an Ethereum token and then migrated to Binance Smart Chain (BSC). BSC was eventually combined with the older Binance Chain and relaunched as the BNB chain. BNB Chain employs "Proof of Staked Authority," a hybrid of proof of stake and proof of authority. Binance Coin has the third-highest market capitalization of any cryptocurrency. Binance allows its users to pay fees for BNB exchanges.

Q. 1 What is Ethereum ?

Ans. :

Ethereum

- Learning of Blockchain technology involves information security, cryptography, economics, distributed systems, peer-to-peer networks, etc. into one. This learning curve is significantly lowered with Ethereum. Ethereum is built by developers for developers, it is a developer's blockchain.
- Ethereum is an open-source, decentralized blockchain with smart contract capabilities. Ether is the name of the platform's native cryptocurrency (ETH). Behind Bitcoin, Ether is the most valued cryptocurrency in terms of market capitalization. Ethereum is permissionless.
- According to computer science, Ethereum is a deterministic but essentially unbounded state machine that consists of a globally accessible singleton state and a virtual machine that updates that state.
- Anyone can publish permanent and unchangeable decentralized applications on the Ethereum network, allowing users to communicate with them. It enables developers to build powerful decentralized applications with built-in economic functions. It offers high auditability, availability, neutrality, and transparency. It eliminates or reduces censorship and some counterparty concerns.

Q. 2 What are Ethereum's Four stages of Development ?

Ans. :

Ethereum's Four Stages of Development

- The development of Ethereum was planned out in four stages, with significant modifications occurring in each stage. Sub releases known as "hard forks" that alter functionality in a non-backward compatible manner may be included in a stage.
- The four main development stages are :
  - Block #0, Frontier - From July 30, 2015, to March 2016, Ethereum was in its beginning stage.
  - Block #200,000, dubbed Ice Age - A hard fork to introduce an exponential increase in difficulty level, to encourage a switch to PoS when ready.
  - Block #1,150,001, or Homestead - is the second Ethereum stage and was introduced in March 2016.
  - Block #1,192,000, DAO - A hard fork that separated Ethereum and Ethereum Classic into two competing systems and paid out compensation to victims of the DAO contract hack.
  - Block #2,463,000, Tangerine Whistle - A hard fork to change the gas calculation for certain I/O-heavy operations and to clear the accumulated state from a denial-of-service (DoS) attack that exploited the low gas cost of those operations.
  - Spurious Dragon, Block #2,675,000 includes additional state clearing, and a hard fork to address additional DoS attack vectors a defense against replay attacks is also included.
  - Block #4,370,000, in the Metropolis In Byzantium At the time this book was being written, Ethereum was in its third stage, called Metropolis, which was first introduced in October 2017. The first of two hard forks slated for Metropolis is Byzantium.
  - There is one more hard fork planned for Metropolis after Byzantium, and that is Constantinople. The last phase of Ethereum's deployment, called Serenity, will come after Metropolis.

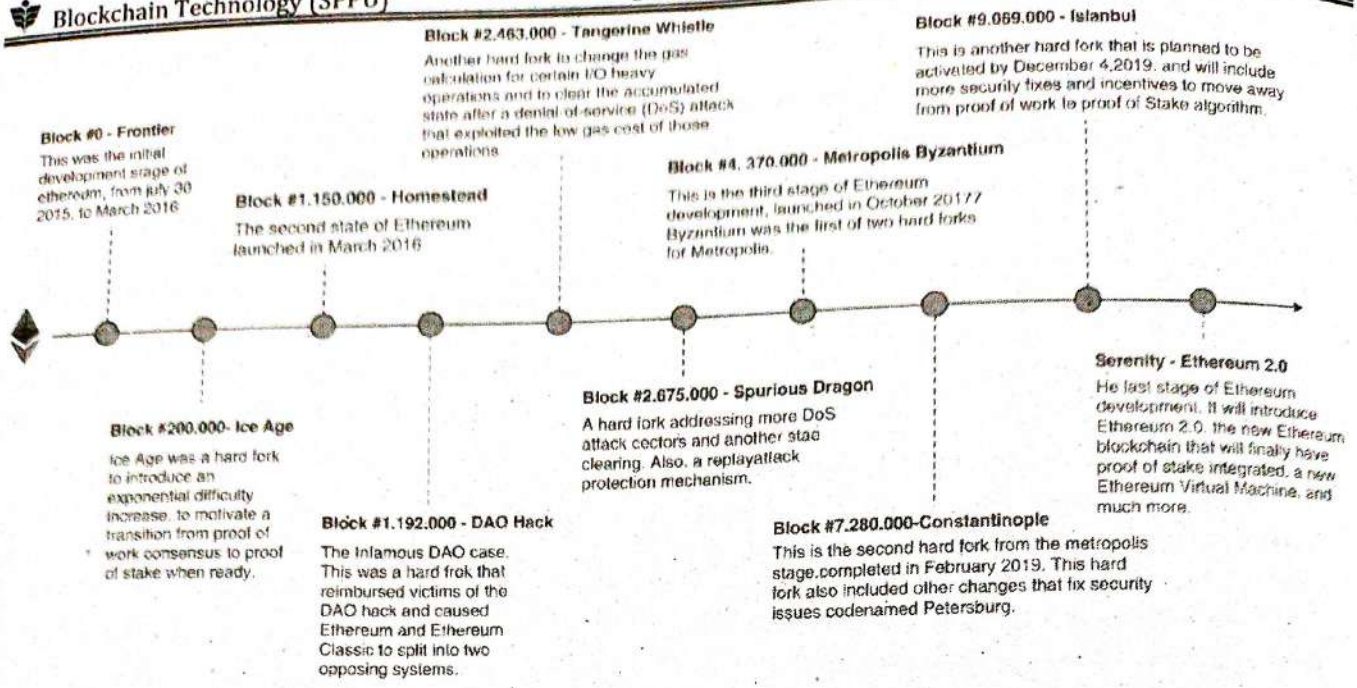


Fig. 5.1

Q. 3 Explain Ethereum as a General purpose Blockchain and also explain components of Ethereum?

Ans. : Ethereum : A General-Purpose Blockchain

- Ethereum is a distributed state machine. Ethereum, however, tracks the state changes of a general-purpose data store, or a store that can keep any data expressible as a key-value tuple, as opposed to just tracking the status of currency ownership. Every value in a key-value data store is identified by a key; for instance, the value "Mastering Ethereum" is identified by the key "Book Title." This performs some of the same functions as Random Access Memory (RAM), the data storage type preferred by the majority of general-purpose computers.
- Ethereum has a memory that stores both data and code, and it uses the Ethereum blockchain to track how this memory changes over time. Ethereum has the ability to load code into its state machine, execute that code, and store the resulting state changes in its blockchain, much like a general-purpose stored-program computer. Ethereum's distributed global state is subject to consensus rules when it comes to state modifications.
- Like other blockchains, Ethereum may be seen as a transaction-based state machine. The core idea is that in the Ethereum blockchain, a genesis state is transformed into a final state by executing transactions incrementally. The final change is then acknowledged as the state's final, undeniable manifestation. The Ethereum state transition function is displayed in the diagram below, where the execution of a transaction has led to a state transition :

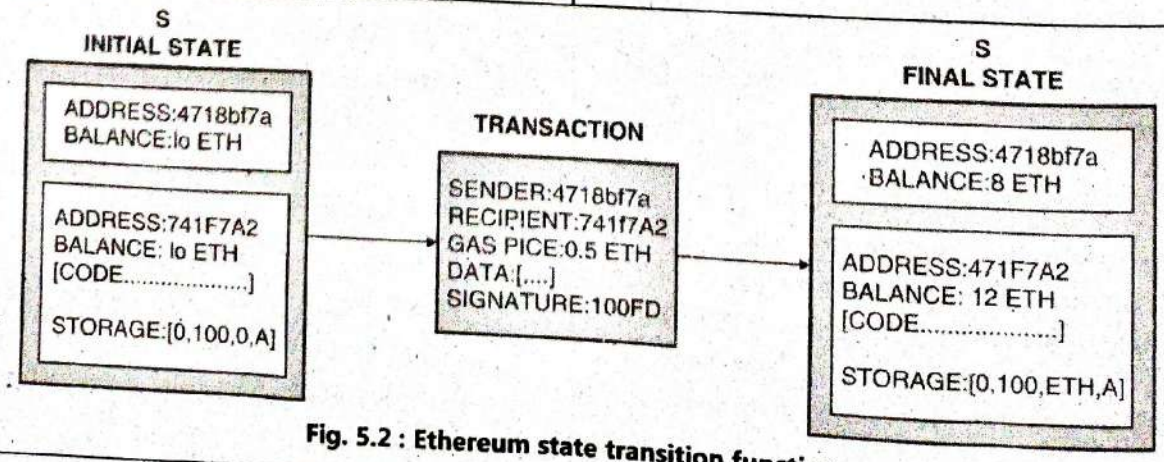


Fig. 5.2 : Ethereum state transition function

- In the example before, a transfer of two ether is started from address 4718bf7a to address 741f7a2. The initial state depicts the situation prior to the transaction's execution, while the final state shows how the situation has changed. In state transition, mining is crucial. The world state is saved as the state on the Ethereum network. This is referred to as the global state in the Ethereum blockchain.

Components of Ethereum

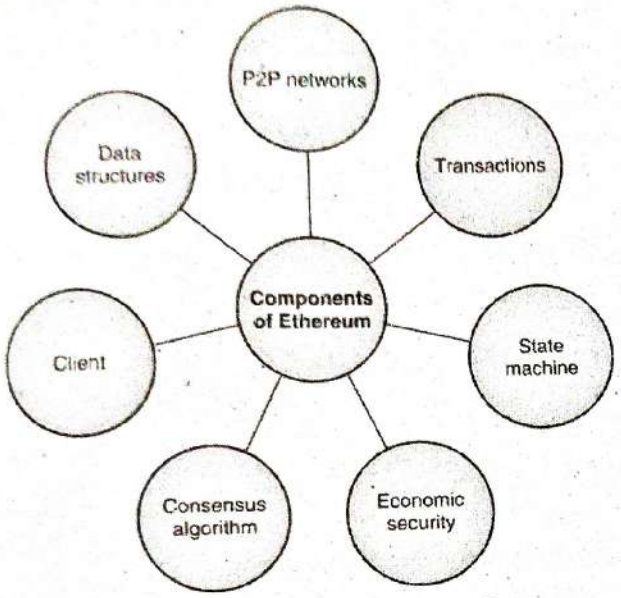


Fig. 5.3

The elements of a blockchain system for Ethereum are more fully outlined in "Components of a Blockchain" as follows :

- **The P2P network** The *ÐEVp2p* protocol is used by Ethereum, which runs on the Ethereum main network, accessible at TCP port 30303.
- **Consensus regulations :** The Yellow Paper of Ethereum has mentioned, the standard specification, of Ethereum's consensus regulations.
- **Transactions :** In an Ethereum transaction, a sender, receiver, data, and value payload are all included in a network message.
- **State machine :** The stack-based Ethereum Virtual Machine (EVM), which runs bytecode, processes Ethereum state transitions (machine-language instructions). The "smart contracts" that run on the EVM are authored in high-level languages (like Solidity) and compiled to bytecode.
- **Data structures :** The state of Ethereum is kept locally on each node in the form of a database (often Google's LevelDB). This database holds the system state and transactions in a serialised hashed data structure known as a Merkle Patricia Tree.
- **Consensus algorithm :** Ethereum makes use of the Nakamoto Consensus, a version of Bitcoin's consensus algorithm that uses sequential single-signature blocks to calculate the lengthiest chain and, consequently, the most recent state. But there are soon-coming plans to switch to the Casper PoS weighted voting method.
- **Economic security :** Ethereum utilises the PoW algorithm Ethash at the moment, but PoS will eventually replace it at some time in the future.
- **Clients :** There are a number of interoperable client software implementations for Ethereum, the two most well-known of which are Go-Ethereum (Geth) and Parity.

Q. 4 What are DApps ?

Ans. : Decentralized Applications (DApps)

- The original goal of Ethereum was to create a general-purpose blockchain that could be customized for a number of applications. However, Ethereum's ambition swiftly grew to include a DApp development platform. DApps offer a more comprehensive viewpoint than smart contracts. A smart contract and a web user interface are the very minimum of what a DApp is. A DApp is a web application that is based on open, decentralized, peer-to-peer infrastructure services in a broader sense.
- A DApp Architecture is composed of at least :
  - A web frontend user interface - A frontend layer on the user side.
  - Smart contracts on a blockchain - A backend hosted in the blockchain network.
- Many DApps also contain additional decentralized elements, such as :
  - A decentralized (P2P) messaging protocol and platform (Whisper).
  - A decentralized (P2P) storage protocol and platform (Swarm).
- In the frontend, if you are familiar with Bootstrap or any other framework, you can continue using it. You won't need to create accounts, manage user accounts, or log in to access your DApps, as the network is anonymous, and we only deal with anonymous accounts (addresses), without identification. On Ethereum, the backend operations are ensured by the smart contract, which is validated by the peer-to-peer network. The following diagram shows the interactions between the frontend and backend in the typical DApp.

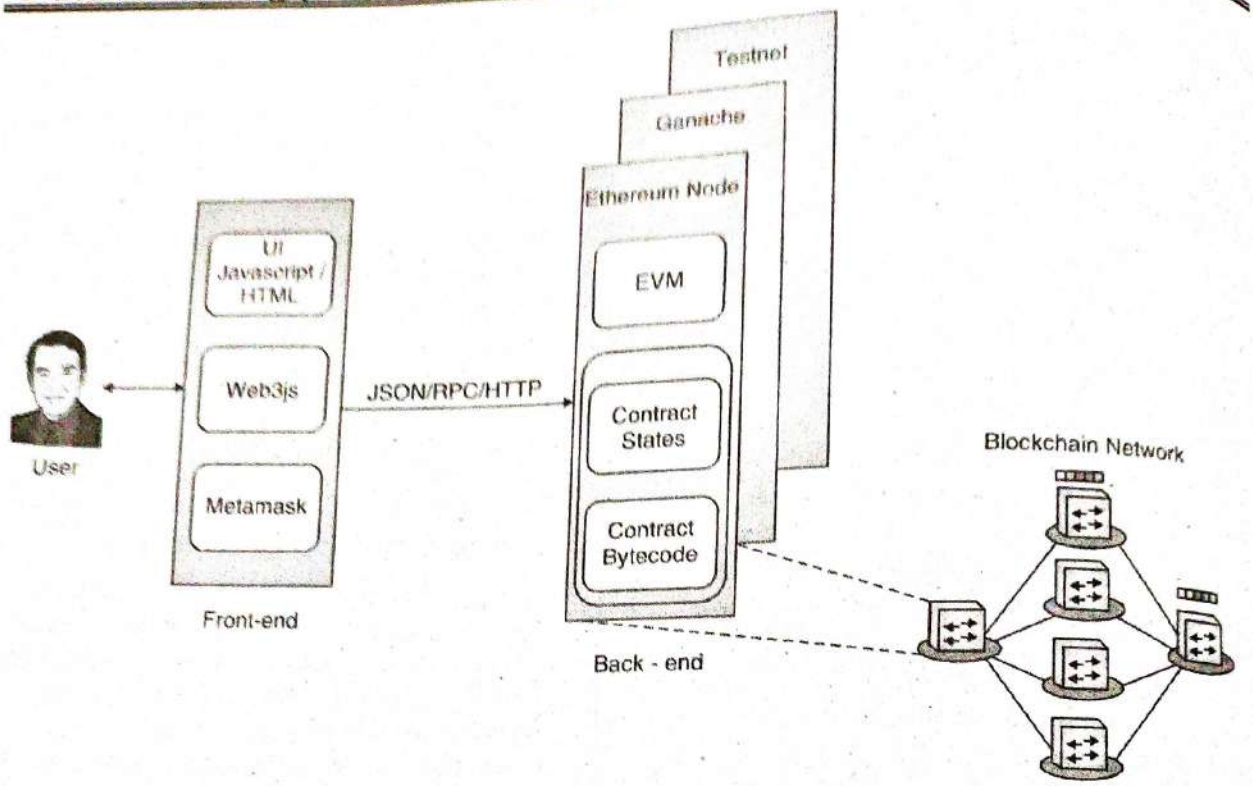


Fig. 5.4 : Interactions between the frontend and backend in the typical Dapp

A DApp must meet the following criteria :

- While the front-end code can be in any language, the back-end code must comprise smart contracts ;
- The back-end code must run on a decentralized blockchain ;
- A DApp must have open-source code;
- Execution of the DApp must be autonomous;
- The app must use a crypto token created using a standard cryptographic algorithm, for e.g. 'proof of work' (POW);
- No one entity should control the majority of crypto tokens;
- A DApp must store data in a decentralized blockchain and while doing so, it must adhere to cryptographic standards.

Q. 5 Explain Types of Ethereum Networks ?

Ans. : Types of Ethereum Networks

For development, testing, or production use cases, one can access various Ethereum environments known as networks. Since Ethereum is a protocol, it is possible for different autonomous "networks" to adhere to the protocol without communicating with one another. Your Ethereum account will work across the different networks, but your account balance and transaction history won't carry over from the main Ethereum network. For testing purposes, it's useful to know which networks are available and how to get testnet ETH to play around with.

1. Public Networks

Anyone in the world with an internet connection can access public networks. On a public blockchain, anyone may view, add, and validate transactions, as well as read previously created transactions. The inclusion of transactions and the network's status are decided by consensus among peers.

Ethereum Mainnet

It is the main public Ethereum blockchain that has real value, Real ETH, and real consequences. Ethereum's Mainnet is the primary network at the moment. https://etherscan.io, is the block explorer for ethereum mainnet which displays extensive information of all the mined blocks and other information. You can use this to learn more about the Ethereum blockchain.

Ethereum Testnets

- In addition to Mainnet, there are public testnets. Before deploying smart contracts to the Mainnet, testnets networks are used by authors of smart contracts or protocols to test potential smart contracts and protocol updates in a real-world setting. Any contract code you write should be tested on a testnet before being released to the mainnet.
- Most testnets use a proof-of-authority consensus mechanism. This means a small number of nodes are chosen to validate transactions and create new blocks – staking their identity in the process. In Testnets rewards are not given for proof-of-work mining.
- It is anticipated that Ropsten, Sepolia, and Goerli will all be proof-of-stake networks. There are no marketplaces for ETH on testnets since it has no real value. The majority of users obtain testnet ETH from faucets since you need it to interact with Ethereum. The majority of faucets are web applications where you may enter an address and request for dummy ETH.
    - **Ropsten Test Network :** Ropsten was a proof-of-work testnet that went through The Merge to proof-of-stake in May 2022. It can be used to test applications on a merged network, but it is not expected to be maintained long term and is likely to be deprecated before summer 2023.
    - **Kovan Test Network :** A very old proof-of-authority testnet for those still running Open Ethereum clients.
    - **Rinkeby Test Network :** A proof-of-authority testnet for those running old versions of the Geth client.

Public Testnet Advantages and Disadvantages

Regardless of whether you decide to operate a full node, you should probably run a public testnet node. Let's examine some of the benefits and drawbacks of using a public testnet.

Advantages :

1. A testnet node requires substantially less data to sync and store.
2. In a few hours, a testnet node can sync completely.
3. Test ether, which is needed for transactions and contract deployment, has no value and is available for free from a number of "faucets."
4. Testnets are public blockchains that have a large user base and active contracts.

Disadvantages :

1. On a testnet, test ether is used instead of "real" money. Because there is nothing at risk, you cannot evaluate security against actual adversaries.
2. Some features of a public blockchain are impossible to evaluate in a real-world setting on a testnet. For instance, transaction fees, although necessary to send transactions, are not a consideration on a testnet, since gas is free.
3. The testnets do not experience network congestion like the public mainnet sometimes does.

2. Private Networks

If nodes on an Ethereum network are not connected to a public network (i.e. Mainnet or a testnet), then the network is private. Private here does not refer to protected or secure, but refers to reserved or isolated. It has many of the same benefits and drawbacks as the open testnet, but it also differs in some ways.

Advantages :

1. You mine the first block yourself, and No syncing
2. No need to obtain test ether; you "award" yourself mining rewards that you can use for testing.
3. Only you are there, no other users
4. No other contracts, only your contract is there in a network after you launch it.

Disadvantages :

1. Because there are no other users, it operates differently from a public blockchain. For transaction space or transaction sequencing, there is no competition.
2. You are the only miner, which makes mining more predictable and prevents you from testing various situations that take place on a public blockchain.
3. Since there are no other contracts, you must deploy all dependencies and contract libraries that you want to test.
4. To test specific scenarios, you cannot duplicate certain public contracts and their addresses (e.g., the DAO contract).

Q. 6 What is Ethereum Virtual Machine : EVM ?

Ans. : Ethereum Virtual Machine : EVM

- The Ethereum Virtual Machine, or EVM for short, is the heart of the Ethereum protocol and its functionality.
- In the Java ecosystem, programmers create Java code in any Java IDE, compile it into bytecodes, and then load those bytecodes into the Java Virtual Machine, or JVM, behind the scenes using a Java class loader, where they are then executed. Java programs can run on a variety of implementations and underlying hardware platforms thanks to the JVM standard, which outlines the requirements for a JVM implementation.
- Similar to this, smart contract and DApp developers in Ethereum write their smart contracts in high-level languages like Solidity, compile them into bytecodes, then upload them to the blockchain for invocation and execution. The Ethereum smart contract runtime execution environment is known as the EVM. It comes with a different implementation of Ethereum client. EVMs are basically responsible for providing a runtime that can execute code written in smart contracts. It has access to its own storage data as well as contract and externally owned accounts. It has limited information about the current transaction but no access to the entire ledger. The Ethereum execution components are called EVMs. An EVM's function is to run a smart contract's code line by line.
- All execution instructions have a finite number of computing steps so the amount of gas available for every given smart contract execution makes the EVM a "quasi-Turing-complete" state machine.
- All Ethereum accounts and smart contracts live within the Ethereum protocol, which was created specifically to maintain the uninterrupted, continuous, and immutable operation of this unique state machine. Ethereum only has one "canonical" state at any one point in the chain, and the EVM establishes the procedures for calculating a new valid state from block to block.
- Ethereum is a distributed state machine Instead of a distributed ledger. The Ethereum state is a substantial data structure that includes all accounts and balances in addition to a machine state that can execute any machine code and can vary from block to block in accordance with predetermined rules.

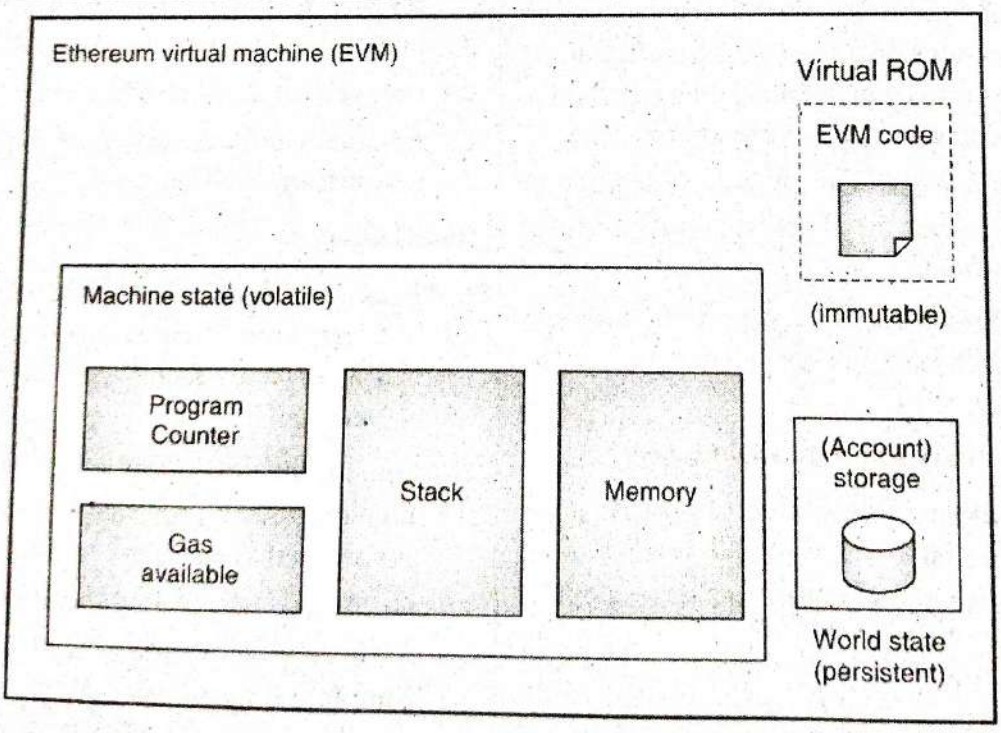


Fig. 5.5

he Ethereum State Transition Function

It generates a predictable-deterministic result from an input. Therefore, it is highly beneficial to more formally define Ethereum's state transition function as follows :

$$Y(S, T) = S'$$

- The Ethereum state transition function Y(S, T) creates a new valid output state S' from an old valid state (S) and a fresh set of valid transactions (T).

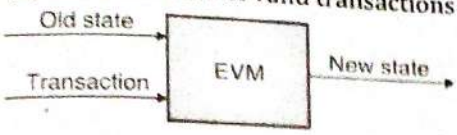


Fig. 5.6 : EVM state machine

State

The state of Ethereum is maintained through a massive data structure known as a modified Merkle Patricia Trie, which keeps all accounts connected via hashes and reducible to a single root hash published on the blockchain.

Transactions

The instructions from accounts that have been cryptographically signed are known as transactions. There are two types of transactions : those that result in message calls and those that result in contract generation. The contract generation process results in the formation of a new contract account with compiled smart contract bytecode. Every single time a message call is made to that contract from another account, its bytecode is executed.

EVM Instructions

- The EVM operates as a stack machine with a depth of 1024 items. For the convenience of usage with 256-bit cryptography, each item is a 256-bit word (such as Keccak-256 hashes or secp256k1 signatures).The transitory memory that the EVM maintains during execution (in the form of a word-addressed byte array) does not persist between transactions.
- However, contracts do include a Merkle Patricia storage trie (in the form of a word-addressable word array), linked to the relevant account and a component of the global state. The EVM opcodes that make up the compiled smart contract bytecode carry out common stack operations like XOR, AND, ADD, SUB, and others. A number of blockchain-specific stack operations, including ADDRESS, BALANCE, BLOCK HASH, etc., are also implemented by the EVM.

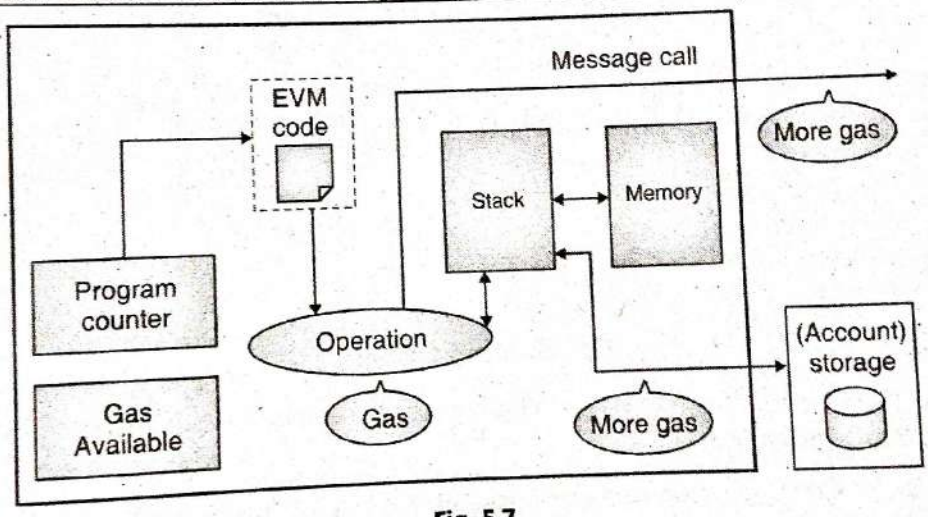


Fig. 5.7

The EVM Instruction Set (Bytecode Operations)

EVM executes around 140 operations or opcodes that are divided into the following 11 categories. All of the opcodes and their complete descriptions are available in the Ethereum Yellow Paper (https://github.com/ethereum/ yellowpaper):

- Stop and arithmetic operations
- Comparison and bitwise logic operation
- KECCAK256
- Environmental information
- Block information
- Stack, memory, storage, and flow operations
- Push operations
- Duplication operations
- Exchange operations
- Logging operations
- System operations

Q. 7 Explain Smart Contracts and its types ?

Ans. :

Introduction to Smart Contracts

- Externally owned accounts (EOAs) and contract accounts are the two main types of accounts available in Ethereum, as we have seen previously.
- Users have control over EOAs, frequently through third-party software, such as a wallet program. Contrarily, contract accounts are managed by computer programs that are run by the Ethereum Virtual Machine and are sometimes referred to as "smart contracts." In summary, contract accounts have both related code and data storage, whereas EOAs are simple accounts without either.
- Over the years, the phrase "smart contract" has been used to refer to a wide range of different things. A series of promises specified in digital form, including protocols within which the parties carry out the other promises, is what cryptographer Nick Szabo first described when he first invented the phrase in the 1990s. In the context of an Ethereum Virtual Machine as a component of the Ethereum network protocol, i.e., on the decentralized Ethereum world computer, immutable computer programs that run deterministically are referred to as "smart contracts."

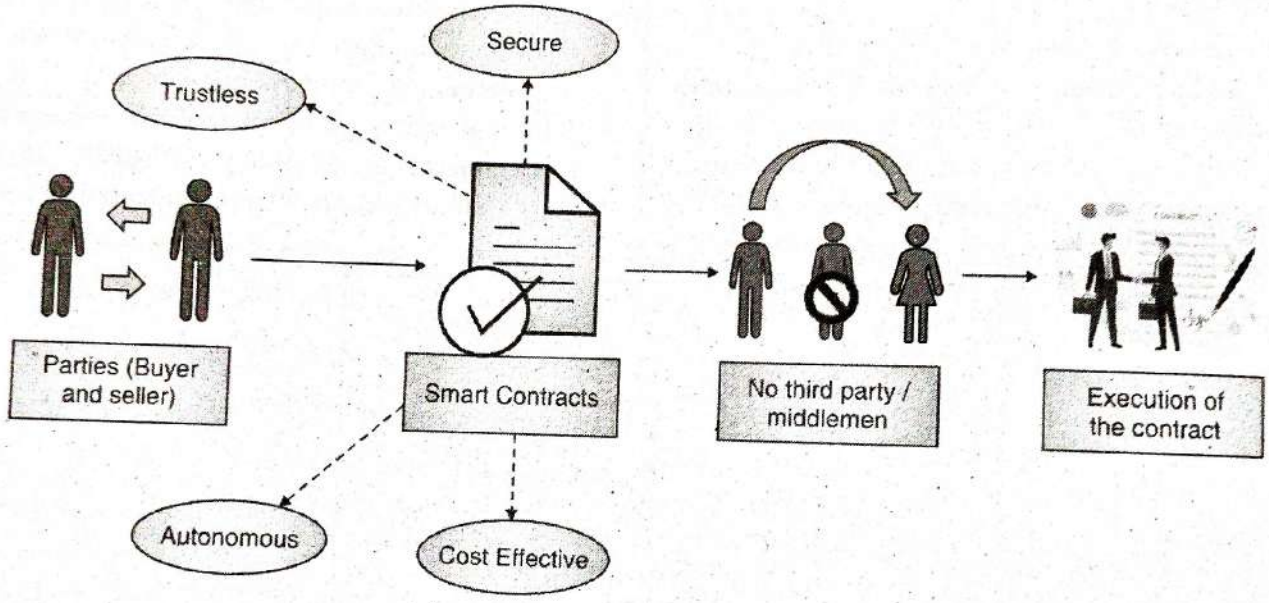


Fig. 5.8 : Smart Contracts

- **Computer programs :** Smart contracts are nothing but simple computer programs. In this situation, the word "contract" has no legal significance.
- **Immutable :** A smart contract's code cannot change after it has been deployed. In contrast to conventional software, changing a smart contract requires deploying a new instance.
- **Deterministic :** Given the circumstances of the transaction that triggered the execution of the smart contract and the condition of the Ethereum blockchain at the time of execution, the outcome of the execution of a smart contract is the same for each user who runs it.
- **EVM context :** Smart contracts operate with a very limited execution context. They can access some information about the most recent blocks, the context of the transaction that called them, and their own state.
- **Decentralized world computer :** Every Ethereum node has a local instance of the EVM running, but because all of these instances share the same starting state and end state, the system as a whole functions as a single "world computer."

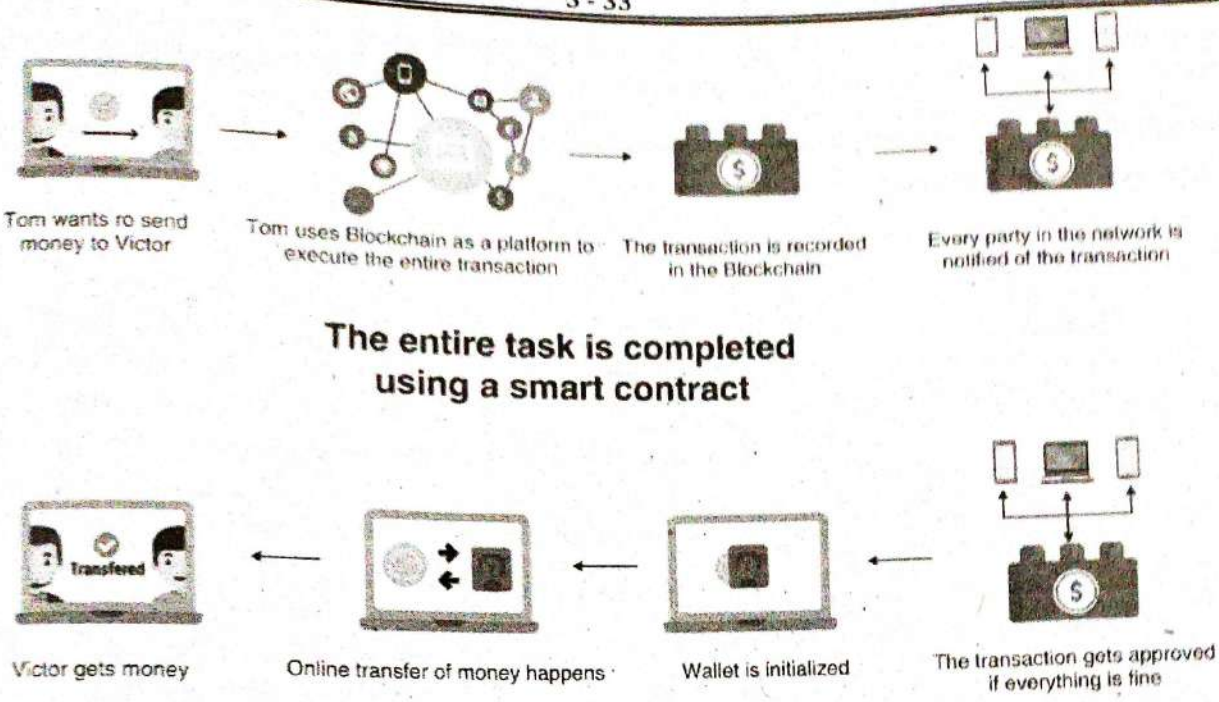


Fig. 5.9

Life Cycle of a Smart Contract

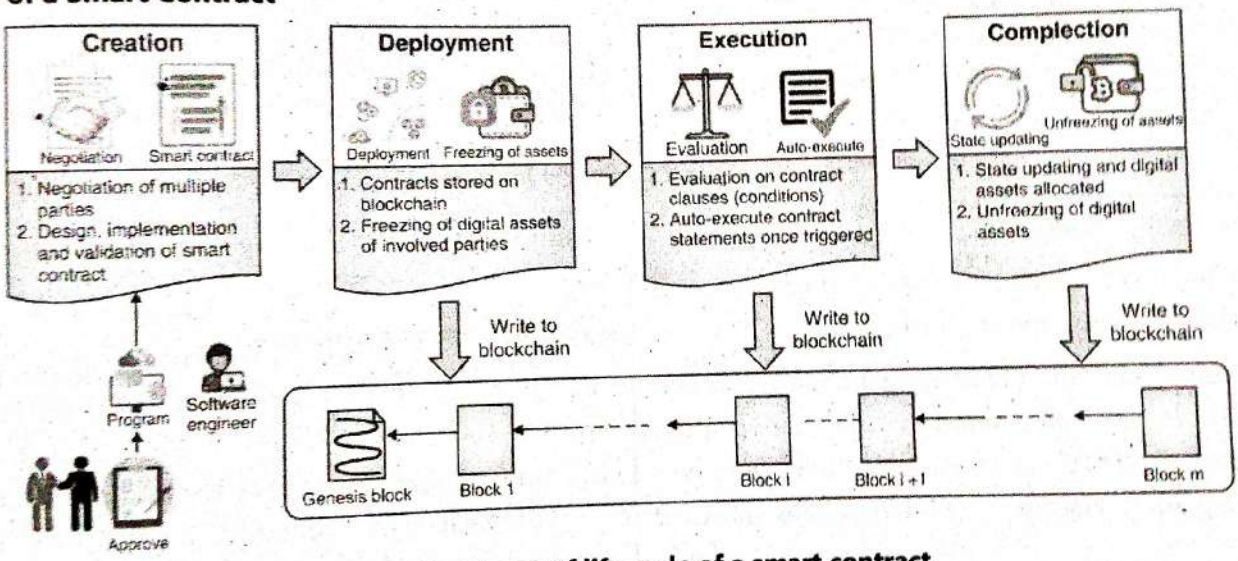


Fig. 5.10 : Stages of life cycle of a smart contract

- Most smart contracts are created using a high-level language like Solidity. However, they need to be compiled into the low-level bytecode that the EVM uses before they can be used. They are then deployed on the Ethereum network after being created via a unique contract creation transaction. An Ethereum address that is derived from the contract formation transaction as a function of the originating account and nonce uniquely identifies each contract.
- Contracts only take effect when a transaction calls them, which is important. All Ethereum smart contracts are ultimately carried out as a result of a transaction started by an EOA.
- All parts of a transaction are executed, and only if all execution successfully concludes are any changes to the overall state (contracts, accounts, etc.) recorded. Successful termination means that the program is executed without an error and reaches the end of execution.
- All of the effects (changes in state) are "rolled back" if execution fails due to an error, making it appear as though the transaction never took place. A failed transaction has no impact on the contract or account state other than the fact that it was attempted and that the ether used for gas during execution was debited from the originating account.

- It is crucial to keep in mind that a contract's code cannot be altered, as was previously indicated. A contract can, however, be "deleted," which removes the code and its internal information (storage) and leaves a blank account.

Q. 8 What is Purpose of Smart Contracts and also state its types ?

Ans. : Purpose of Smart Contracts

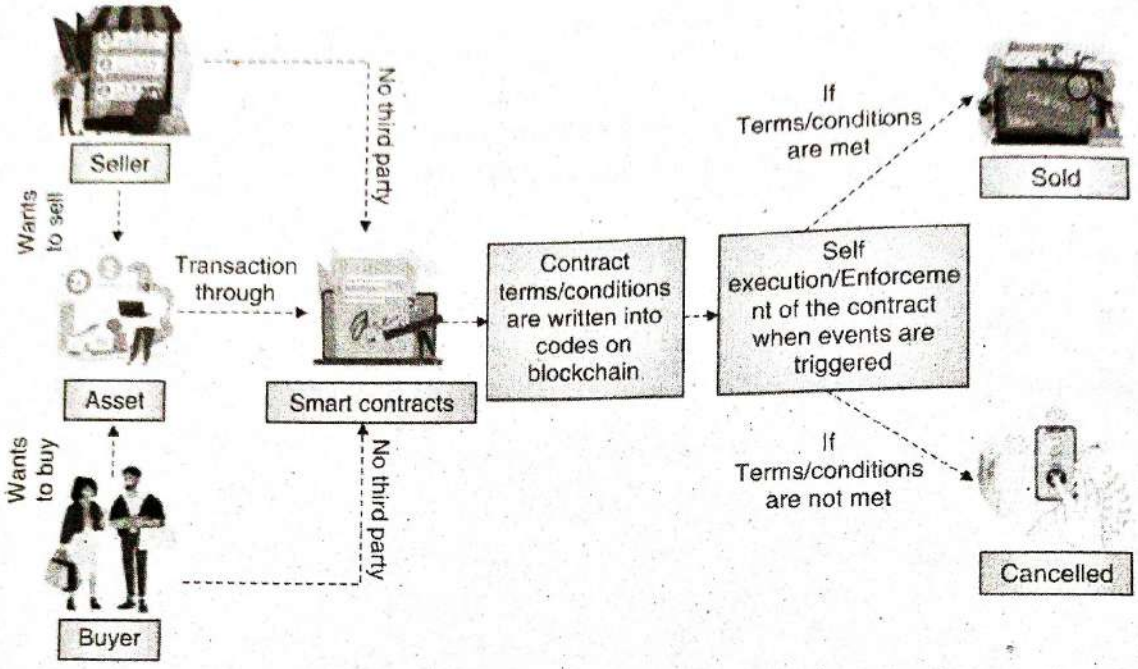


Fig. 5.11 : Smart Contracts functioning

Let us explain the process

- When buying or selling an asset, there are two interested parties (a buyer and a seller).
- The terms or clauses of their agreement are encoded in codes entered into a smart contract between the two parties, which is entirely digital and self-executing on a decentralized blockchain network and.
- These rules outline the conditions that must be met by both parties in order for the contract to be automatically enforceable. When all parties agree to these conditions, the transaction is completed.
- The smart contracts platform provides top-notch security and total transparency. Additionally, it prevents data manipulation and enables the two parties to track the transaction. However, the identity of the parties involved are kept a secret.

Examples :

Smart contracts examples are common in industries like property rights, intellectual property, banking and insurance, legal services, e-government, crowd funding, etc.

Types of Smart Contracts

There are three types of self-executing contracts based on their applications :

1. **Smart Legal Contracts :** These contracts are legally enforceable and require the parties to fulfill their contractual obligations. Failure to do so may result in strict legal actions against them.
2. **Decentralized Autonomous Organizations :** These are blockchain communities that are bound to specific rules coded into blockchain contracts combined with governance mechanisms. Hence, any action taken by the community members gets replaced by a self-enforcing code.
3. **Application Logic Contracts :** These contracts contain an application-based code that remains in sync with other blockchain contracts. It enables communication across different devices, such as the merger of the Internet of Things with blockchain technology.

Q. 9 How to implement and deploy smart contracts ?

Ans. : Implementing and Deploying Smart Contracts using Solidity

How to Write Simple Contract : HelloWorld

- The first smart contract we will write to print Hello world. Following is the solidity code for the same. solidity is the most popular high-level language for writing smart contracts. The first line specifies the version of the compiler that is to be used to compile our code. pragma is solidity expression. We have specified the minimum version of the solidity compiler as 0.5.0. Code statements end with a semicolon. The line number 2 is a comment :

  // Our first contract is HelloWorld!

- Comments are not included in the executable EVM bytecode are and for humans to understand the meaning or logic of code statements. Our actual contract starts at line number 3 is :

  contract HelloWorld

- It declares a contract object, which is similar to a class declaration in C++ or Java language.
- All the lines of the contract are included in between curly braces ({}), which define a scope like many other programming languages. The next line number 5 declares the string variable named "stateVariable" as private and initialized with the string "Hello World !".

  string private stateVariable = "Hello World !";

- We have declared the function at line number 6, function name is GetHelloWorld(), which is the public function, means it is also accessible outside the contract and this functions returns the string, that's why it is written as returns (string memory), we have not passed any argument to the function here. The scope of the function is defined by curly braces ({}). GetHelloWorld() is declared as a view function which means a function that only reads but doesn't alter the state variables defined in the contract.

  function GetHelloWorld() public view returns (string memory)

  {

  return stateVariable;

  }

- The function ends at line number 9 by (}) and the contract ends at the line number 10 by (}).

- Following is the complete code for the contract

```
1. pragma solidity ^ 0.5.0;
2. // Our first contract is HelloWorld!
3. contract HelloWorld
4. {
5. string private stateVariable = "Hello World !";
6. function GetHelloWorld() public view returns (string
memory)
7.     {
8.     return stateVariable;
9.     }
10.}
```

How to Implement Smart Contracts?

- There are multiple smart contracts authoring tools including Visual Studio. However, the easiest and fastest way to develop smart contracts is to use a browser-based tool known as Remix. Remix is available on http://remix.ethereum.org. Remix provides a rich integrated development environment in a browser for authoring, developing, deploying, and troubleshooting contracts written using the Solidity language.
- Remix is an open source tool that can be downloaded from https://github.com/ethereum/browser-Solidity and compiled to run a private version on a local computer. Another advantage of running Remix locally is that it can connect to local private chain networks directly.

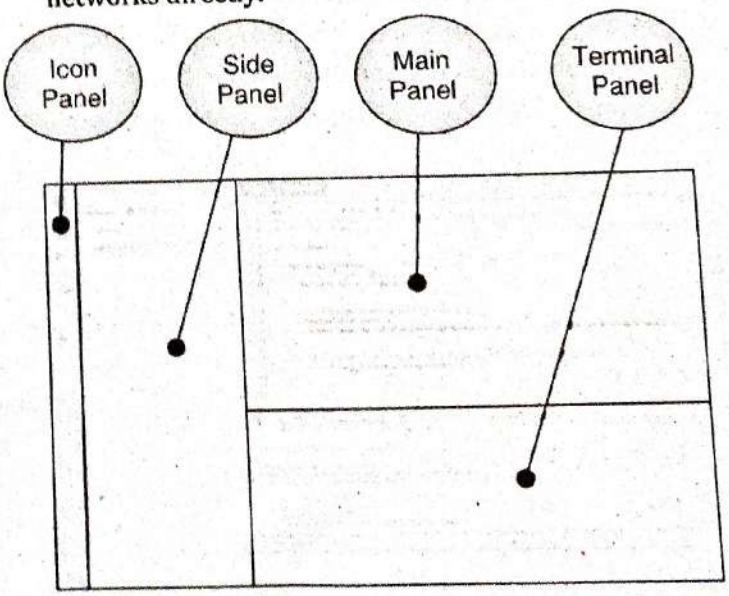


Fig. 5.12 : Remix-IDE Layout

1. Icon Panel - click to change which plugin appears in the Side Panel

2. Side Panel - Most but not all plugins will have their GUI here.
3. Main Panel - In the old layout this was just for editing files. In the tabs can be plugins or files for the IDE to compile.
4. Terminal - where you will see the results of your interactions with the GUI's. Also you can run scripts here.

When you load remix - the icon panel shows these icons by default.

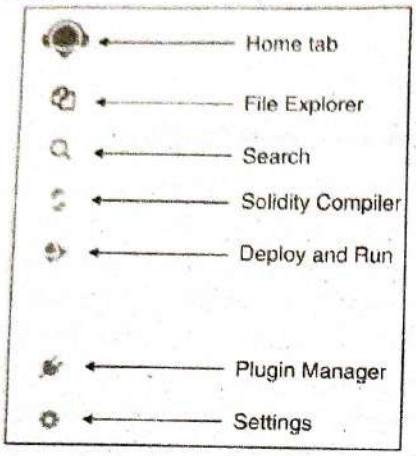


Fig. 5.13 : Icon Panel at Page Load

- In Remix everything is a plugin hence the Plugin Manager is very much important.
- Let us see how to write and sample HelloWorld contract that will just give the message "Hello World !" in solidity by using Remix Ide.

1. The first thing we need to do is to create a new work space, for creating a new workspace click on + icon in side panel, it will pop up a window for Workspace name, Give the workspace name say suppose sample

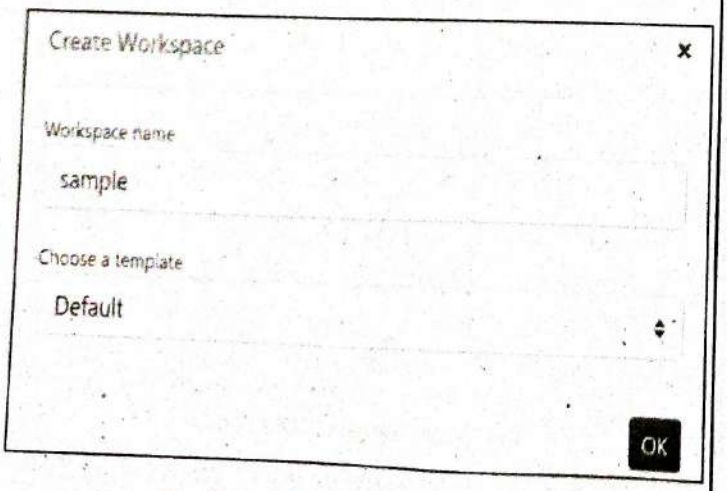


Fig. 5.14 : Creating a workspace

2. Created the workspace "sample".

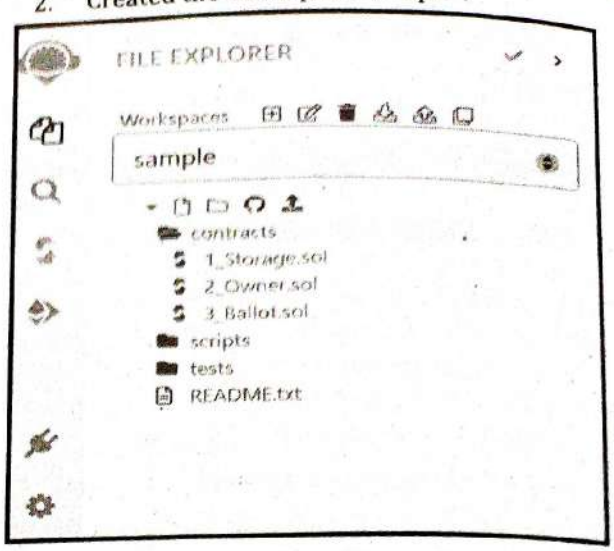


Fig. 5.15 : Created workspace "Sample"

3. Now we need to create a new file to write a code, for that click on create new file icon, which is present in the workspace..

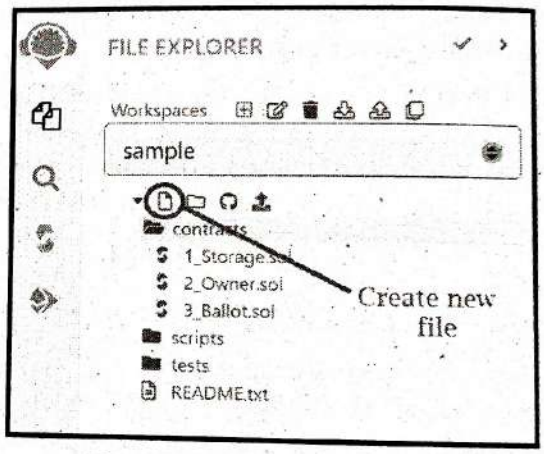


Fig. 5.16 : Create new file icon

4. Give the file name "helloworld", by default it will create the file with .sol extension. This will create a blank contract.

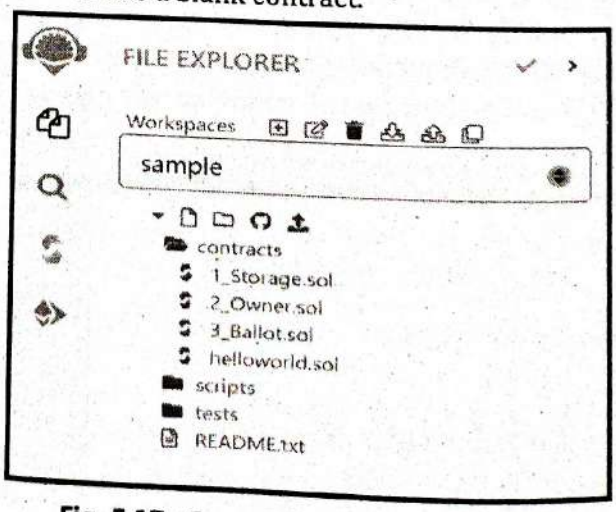


Fig. 5.17 : Ccreated file "helloworld.sol"

5. Type the following code of the "`HelloWorld`" in a main panel

```
pragma solidity ^ 0.5.0;
// Our first contract is HelloWorld!
contract HelloWorld
{
  string private stateVariable = "Hello World !";
  function GetHelloWorld() public view returns (string memory)
  {
    return stateVariable;
  }

}
```

6. Once the code is typed, click on the solidity compiler icon present in the icon panel. Then select the compiler greater than 0.5.0 from the drop down list, present inside the side panel. Then click on the button Compile "helloworld.sol". On the successful compilation of the code Remix will show a small green tick on the solidity compiler icon.

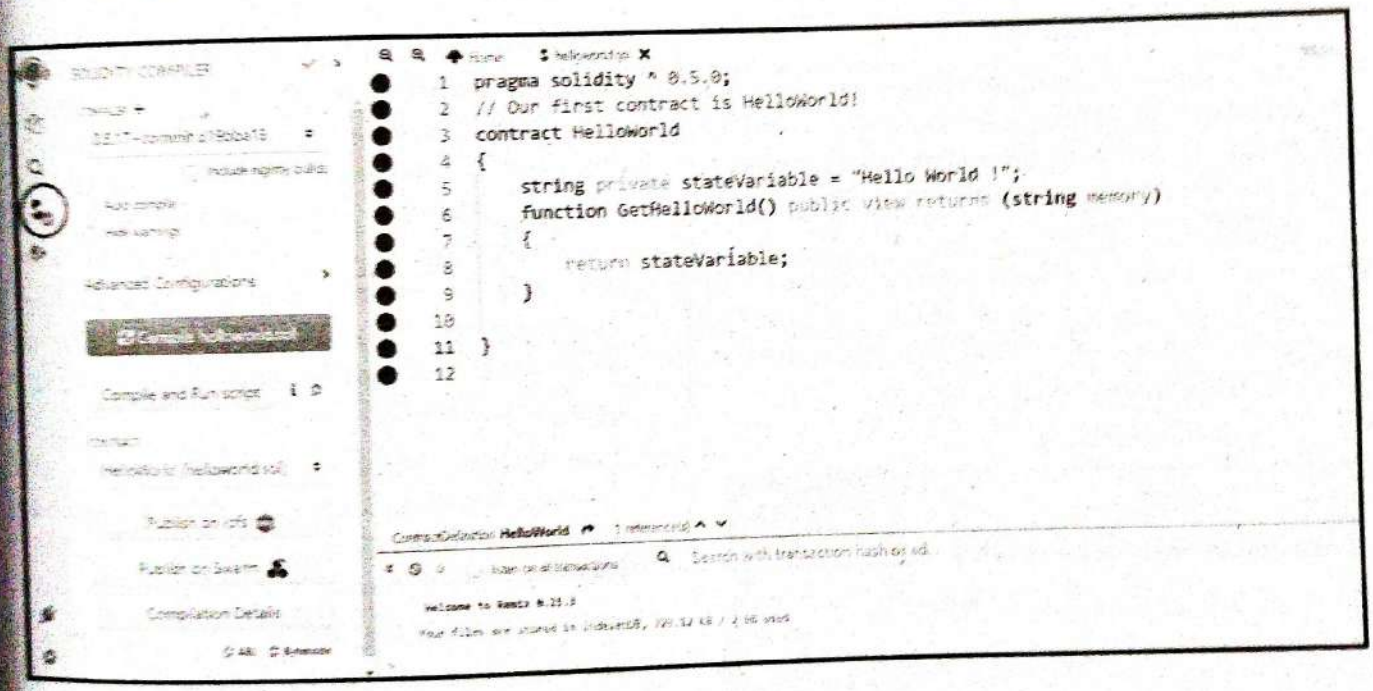


Fig. 5.18 : Compile "helloworld.sol"

7. Now the next important action is to deploy the smart contract, for that click on the deploy and run transitions icon, which is present in the Icon panel. It will show DEPLOY & RUN TRANSACTIONS window, then click on the Brown color Deploy button , then you can see the Deployed Contracts at the bottom, click on that you will see the button named GetHelloWorld, which is our function in the contract, click on that button, you will see the message 0:string : Hello World. This means our code is successfully deployed by a dummy smart contract account.

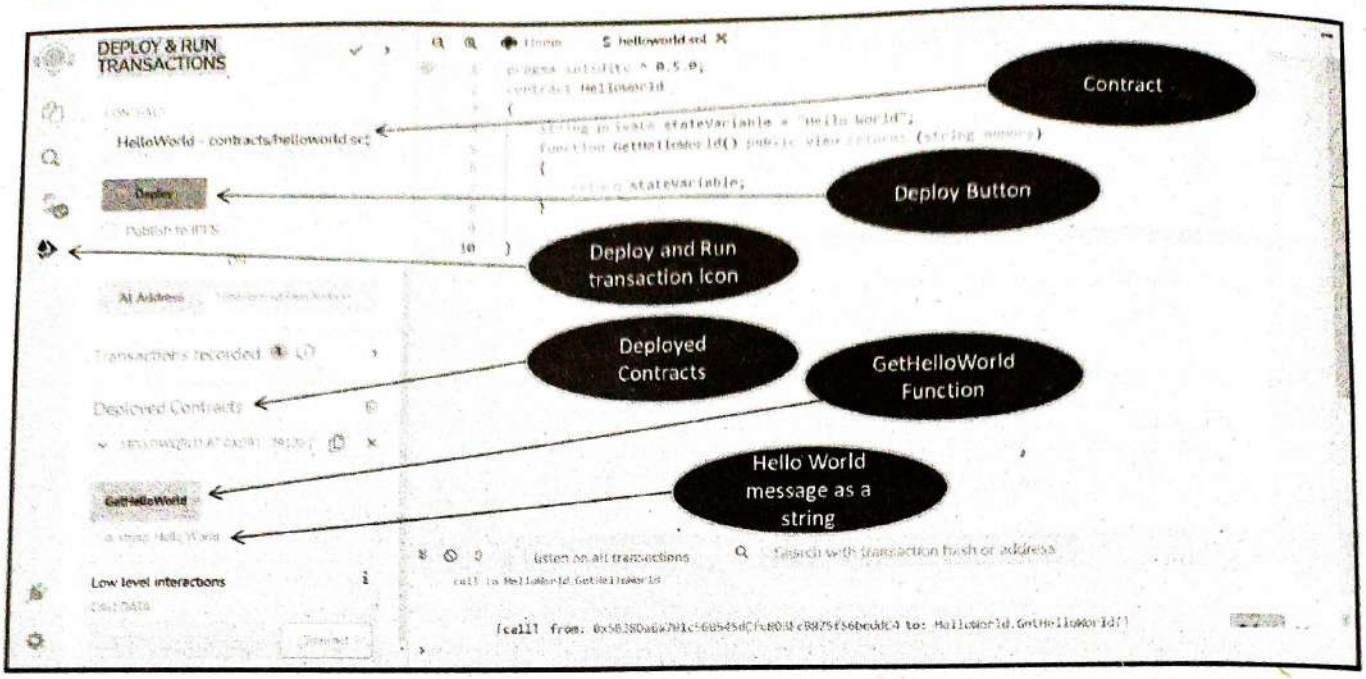


Fig. 5.19 : Our first contract is HelloWorld!

How are Contracts Deployed?

- Remix makes deployment of contracts a breeze; however, it is performing a lot of steps behind the scenes. It is always useful to understand the process of deploying contracts to have finer control over the deployment process.
- The first step is the compilation of contracts. The compilation is done using the Solidity compiler. The compiler generates the following two major artifacts
  - ABI definition
  - Contracts bytecode

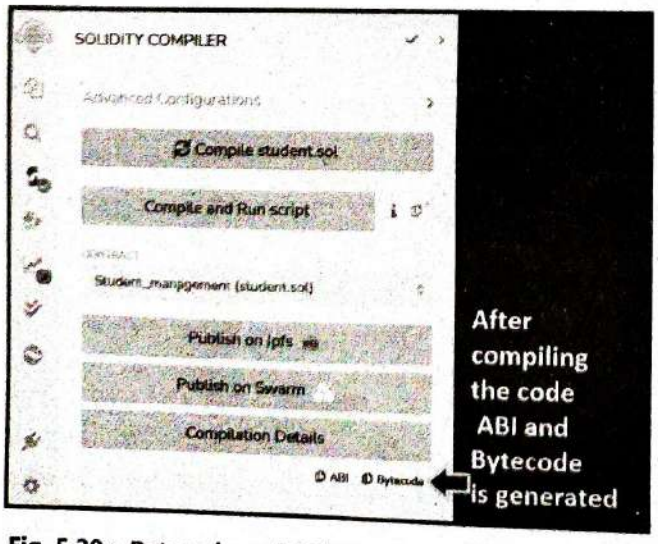


Fig. 5.20 : Bytecode and ABI (Application Bin Interface) file location

- Think of the Application Binary Interface (ABI) as an interface consisting of all external and public function declarations along with their parameters and return types. The ABI defines the contract and any caller wanting to invoke any contract function can use the ABI to do so. The bytecode is what represents the contract and it is deployed in the Ethereum ecosystem. The bytecode is required during deployment and ABI is needed for invoking functions in a contract.
- A new instance of a contract is created using the ABI definition. Deploying a contract itself is a transaction. A transaction is created for deploying the contract on Ethereum. The bytecode and ABI are necessary inputs for deploying a contract.
- As any transaction execution costs gas in Ethereum, appropriate quantity of gas should be supplied while deploying the contract. As and when the transaction is mined, the contract is would be available for interaction through contract address. Using the newly generated address, callers can invoke functions within the contract.

Following is the contents of the ABI file for the code helloworld.sol. ABI file represented in JSON format.


```
[
  {
    "constant": true,
    "inputs": [],
    "name": "GetHelloWorld",
    "outputs": [
      {
        "internalType": "string",
        "name": "",
        "type": "string"
      }
    ],
    "payable": false,
    "stateMutability": "view",
    "type": "function"
  }
]
```


Following Fig. 5.21 shows the sample contents of Bytecode file


```
{
"linkReferences": {},
"object": "6080604052604051806040016040528060d81526020017f48656c6c6f20576f726c6420210000000000000000000000000
8818152602001828054600181600116156101000203166002900480156101 4b5780601f106101205761010080835404028352916020019
"opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE PUSH1 0x40 MLOAD DUP1 PUSH1 0x40 ADD PUSH1 0x40 MSTORE DUP1 PUSH1 0x
H2 0xDE SWAP2 SWAP1 PUSH2 0xE2 JUMP JUMPDEST POP SWAP1 JUMP JUMPDEST PUSH2 0x104 SWAP2 SWAP1 JUMPDEST DUP1 DU
0x1F AND DUP1 ISZERO PUSH2 0xA5 JUMPI DUP1 DUP3 SUB DUP1 MLOAD PUSH1 0x1 DUP4 PUSH1 0x20 SUB PUSH2 0x100 EXP
P POP POP POP POP SWAP1 POP SWAP1 JUMP INVALID LOG2 PUSH6 0x627A7A723158 KECCAK256 SIGNEXTEND 0xDF 0xD5 PUSH2
"sourceMap": "64:173:0:-;;;89:46;;;
```

Salient features of DISC

1. Strong protection against blocking access to or altering content once published.
2. Data remains private and protected when data is uploaded or downloaded without the permission of central authority.
3. Maintains Data Integrity.

Swarm Storage Structure

- Chunk is the official unit of storage used in Swarm, where data of at most 4KB size can be stored along with its unique address. Swarm allows dApps developers to store and broadcast the data among the network peers or blockchain users in a secure environment.
- Swarm architecture is designed to provide database services, node-to-node message passing functionality, media streaming platforms, etc.
- In-built BZZ tokens are governed by Ethereum smart contracts and serve as a reward for the nodes that contribute resources.
- Participants in Swarm Network are identified in Kademlia DHT by hash of Ethereum address of Swarm base account. Kademlia is DHT, where self-organized computer systems in the network can communicate with each other by sharing resources, all without a central registry.
- Swarm is best suited for small chunks of data associated with Ethereum smart contracts, but not a good idea for a huge database. Swarm's Primary goal is to provide a decentralized and redundant store of Ethereum's public records, especially for dApp codes and blockchain data.
- Ways of storing data on Swarm Global Pinning and Postage Stamp.
  1. **Global Pinning :** Users store data on their drive, this method resembles the method used in IPFS to store data. It's free of charge as we store our own data, but nodes are not anonymous and must face redundancy.
  2. **Postage Stamp :** This concept is like checks, where storage nodes can issue BZZ tokens if they prove that they are storing your content, the content is stored in DHT in the correct location.

Working with Swarm

When any type of readable source, such as images, text or video format are uploaded to Swarm network, the Swarm API cuts the data into fixed size chunks (max. 4KB), thus creating a unique cryptographic hash for each part. Hash of these chunks will be used to create another hash of the new chunk. Content is mapped to a fragment tree, this creates a Merkle tree. Root hash of the tree is used as an address to retrieve uploaded files.

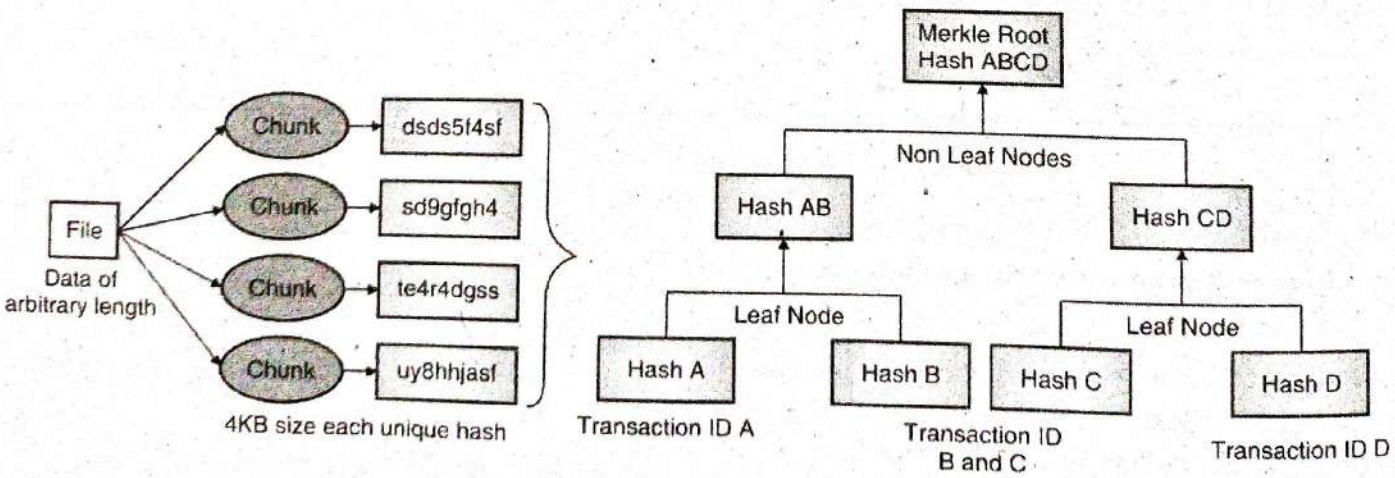


Fig. 5.22

Swarm Distributed Storage Architecture

- Apart from chunk Merkle trees, Swarm provides a crucial layer known as Manifest files, that specifies collection of documents, where each document defines its path, unique cryptographic hash, and its content type.

ex.

```
{
"entries": [{
"hash": "sdf5sdew46.........sdht5",
"contentType": "text document",
"path":" xyz.pdf"
}
```

- Swarm requires an Ethereum account to connect to Ethereum Blockchain. Swarm network uses BZZ wire Protocol, which is based on devp2p/RLPx transport protocols for communication among Ethereum nodes.
- Devp2p/ RLPx is TCP-based (Transmission Control Protocol) transport protocol used for P2P communication among Ethereum nodes, whereas RLPx carries Encrypted messages belonging to one or more nodes to send and receive chunk packets.

Whisper : Decentralized Messaging Platform

- Whisper is a decentralized peer-to-peer messaging, censor-resistant communication protocol that DApps use to communicate with each other. It provides a simple API to send and receive messages with utmost security.

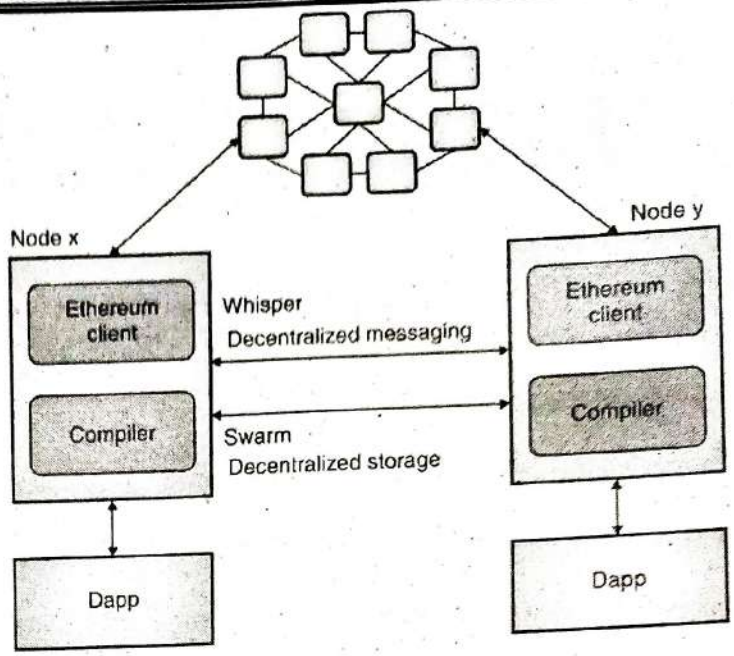


Fig. 5.23

- A lot of services we rely on today aren't secure and leaks in the system result in massive data breaches, the government can track our movements, and corporations keep an eye on our routines and shopping habits. Whisper's goal is to change that by making privacy an option for everyone. Whisper is a secure communication service, equipped with a built-in wallet, capable of transferring and managing digital assets on the messenger.

❑❑❑

Chapter 6 : Blockchain Case Studies

Q. 1 Explain in brief about layered view of blockchani ?

Ans. :

A Layered View of Blockchain

- As shown in Fig. 6.1, blockchains can be abstracted into three distinct layers.
- Layer 1 of blockchain is BFT Byzantine Fault Tolerance (BFT) consensus, also known as state machine replication, which is a generic approach to failure tolerance. BFT consensus can take many forms, from traditional BFT protocols to PoW-based consensus. Regardless of how consensus is reached, all forms must solve the same problem: how to enable nodes to reach consensus on the total order (i.e., consistency) of transactions submitted by clients in the form of requests. After the nodes reach an agreement on the order, the data/operations of the transactions are processed in the order of the transactions. As a result, distributed nodes function as if they were centralised nodes.
- This ensures that there is only one client transaction sequence, known as "the longest chain." The smart contract, which is essentially software code, is the second layer of blockchain. A smart contract is an interface through which blockchain developers can implement new functions.
- The execution of business transactions can then be facilitated, verified, or enforced using smart contracts. A smart contract is a programme that links the underlying consensus protocols with layer 3 applications and use cases.

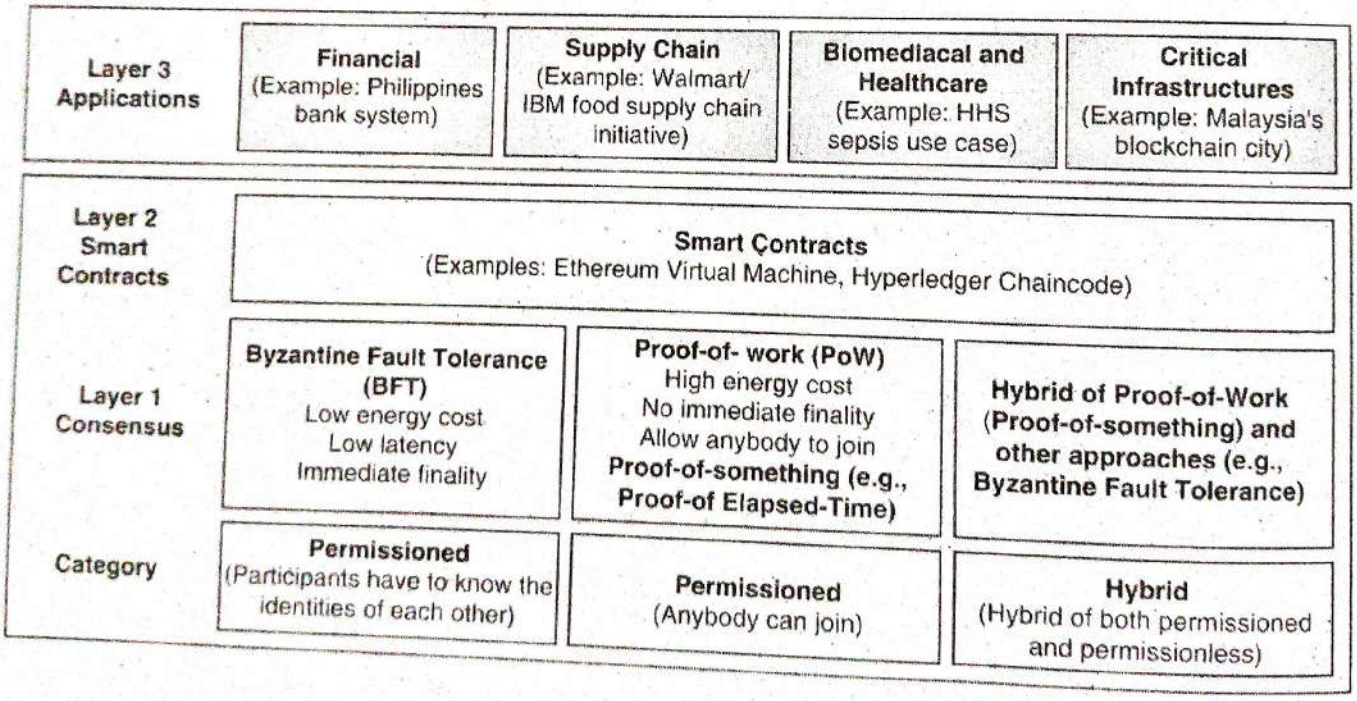


Fig. 6.1 : Overview bolckchains : Categories, underlying techniques and use cases

- Following Fig. 6.2 shows prominent blockchain applications in the sector of healthcare, energy, IOT, smart city, Digital Content management etc.

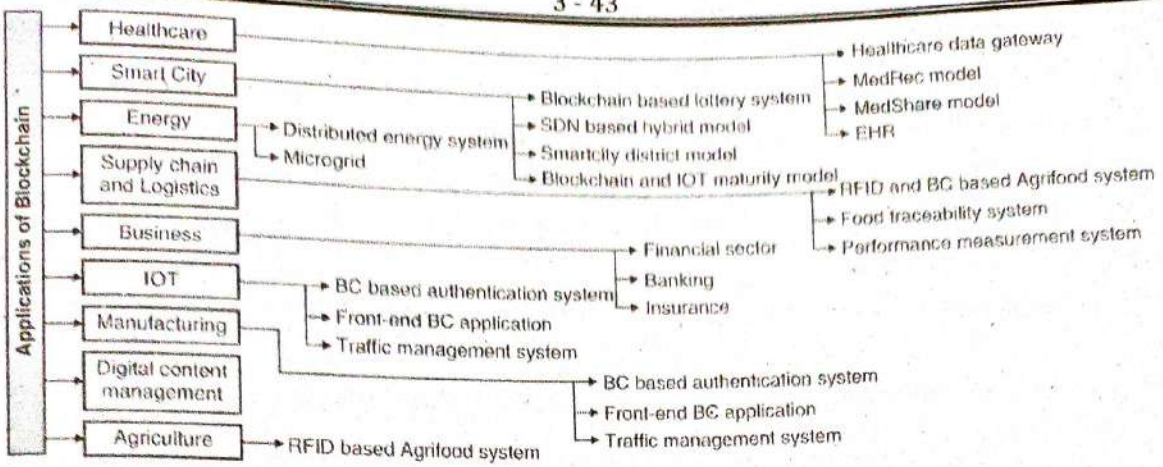


Fig. 6.2

Q. 2 Explain how Blockchain is useful for retailers ?

Ans. : Blockchain in Retail

Blockchain has the potential to open up a plethora of new options for the retail industry. Let's take a deeper look at blockchain's function in the retail business. The dependability, sustainability, and quality of tracking and assisting in management procedures of blockchain may provide retail sectors with the ultimate digitalization they require.

Use Cases in Retail

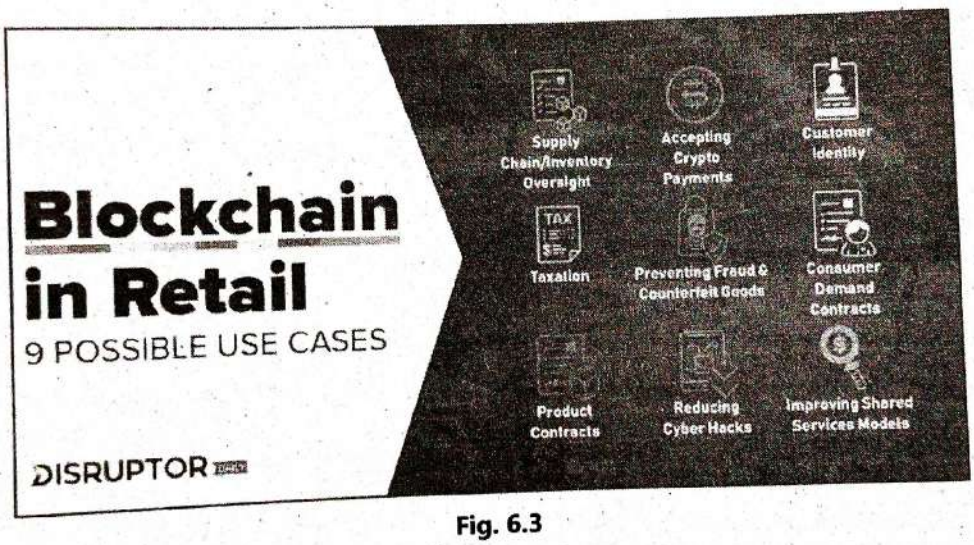


Fig. 6.3

Some of the use cases are as below :

1. **Supply chain / inventory oversight**

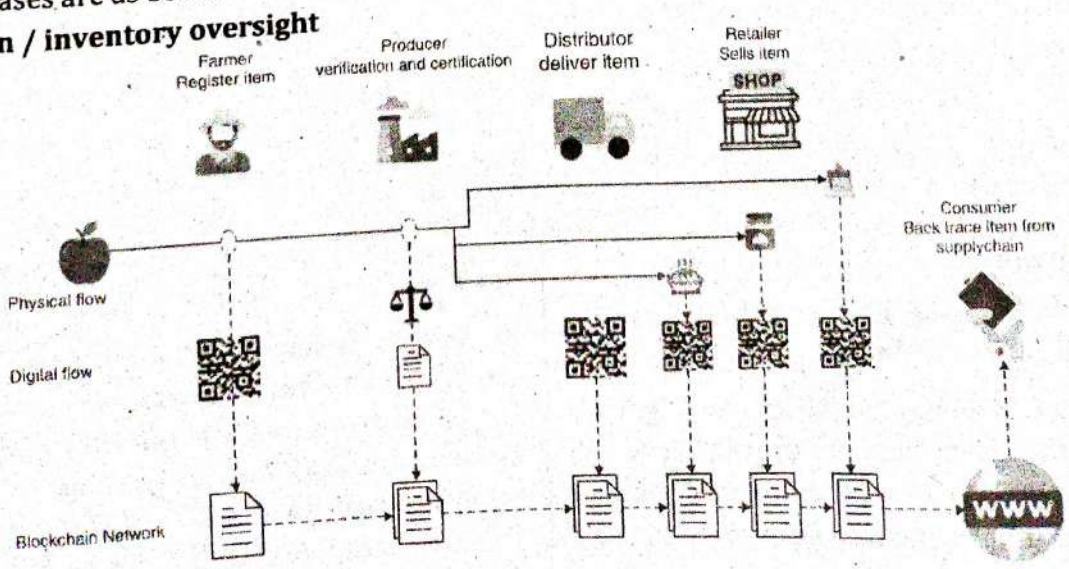


Fig. 6.4

2. **Taxation :**

Blockchain's core attributes mean that it has significant potential for use in tax :

a) Transparency – blockchain provides provenance, traceability and transparency of

b) transactions Control – access to permissioned networks is restricted to identified users Security – the digital ledger cannot be altered or tampered with once the data is entered.

c) Fraud is less likely and easier to spot

d) Real-time information – when information is updated, it's updated for everyone in the network at the same time.

3. **Preventing fraud and counterfeit Goods :** Following block diagram shows With iot fights counterfeiting across the product life cycle

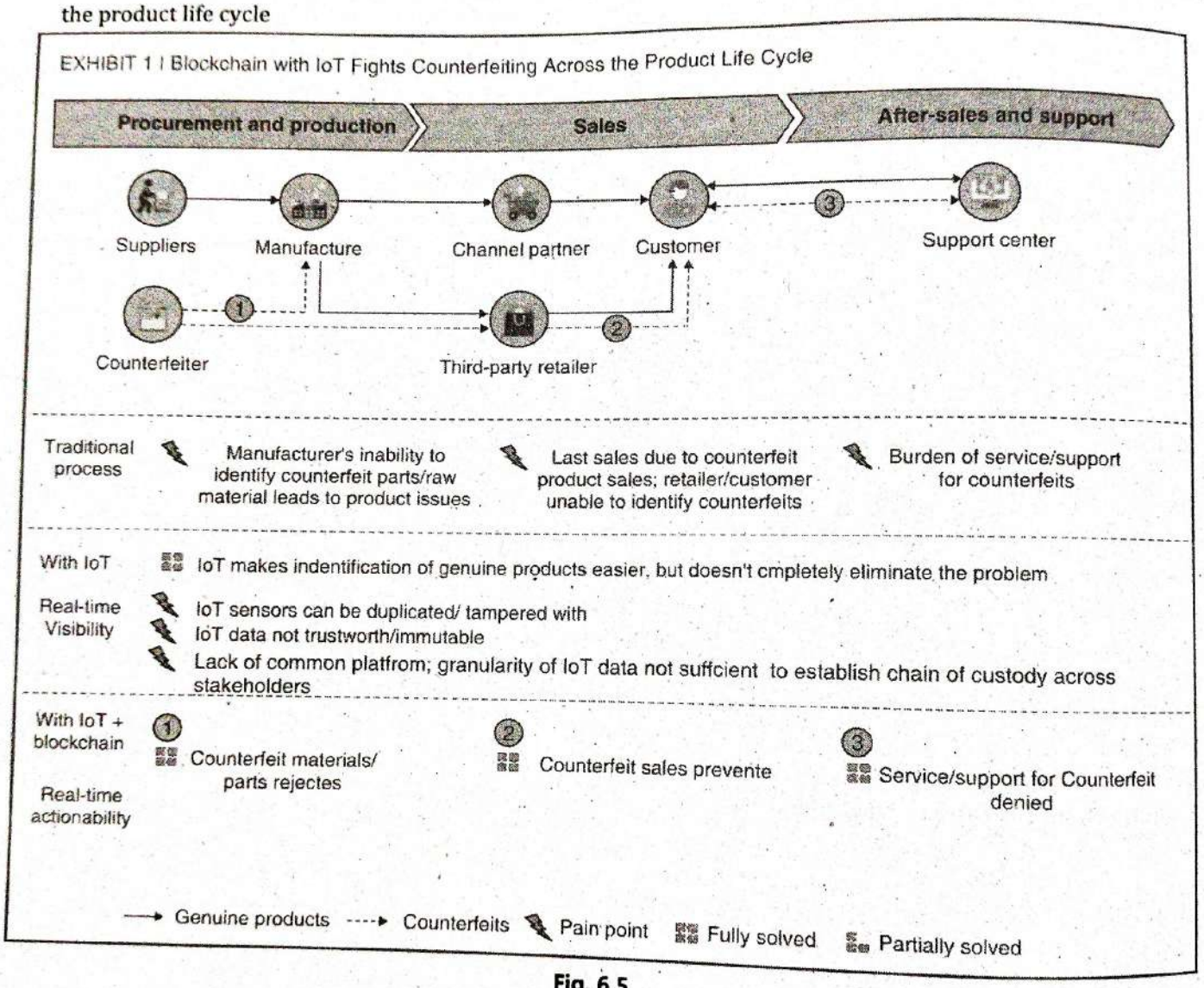


Fig. 6.5

4. **Customer identity**

- The Blockchain Solution to Digital Identity Management
- Blockchain can empower users to have greater control over their own identity. Organizations can use the information only with customers' consent and no central entity would be able to compromise a consumer's identity.

Key Benefits :

1) **Proper Inventory Management :** Retailers need proper inventory management if they want to increase overall efficiency. In reality, there is no downfall associated with it. Inventory management helps businesses track products, their expiration dates, and consumer interest, so businesses can only benefit from this.

Blockchain in retail will help businesses manage their inventory more efficiently. help you to In addition, you can save a lot of money by automating the process of product shortages or product surpluses based on consumer demand in real time.

2) **Use of Crypto as A Payment Method :** Cryptocurrency payment methods are another major application of blockchain in the retail market. As you know, the cryptocurrency market is exploding right now. Furthermore, it seems that different countries want to work on central bank digital currencies, which are in fact a crypto version of fiat money. So it looks like cryptocurrencies will be the money of the future. Here, retail businesses can stay ahead of the game by using existing cryptocurrencies as official payment for products. In fact, it is a good strategy to excite consumers and help them pay for products using digital and secure coins seamlessly.

3) **Reducing Cyber Hacks :** Another popular blockchain in retail use cases is cyber hacker defense. The retail industry regularly faces security threats. As a result, it can quickly turn into a major security hole leading to massive revenue loss. Furthermore, it also means that consumers won't be able to trust companies with their data, which doesn't make a good impression on the brand. But with the use of blockchain here, the scenario can change dramatically. Since blockchain can provide highly secure protocols against cyberattacks, there will be no more security breaches. As a result, blockchain can begin to increase revenue by protecting the network from a third-party entity.

4) **Streamline Retail Sales Tax :** One of the other benefits of blockchain in retail is the process of streamlining retail taxes. In fact, every year every retail business has to pay taxes based on their sales. However, many people tend to avoid paying this $14.5 billion in taxes! Furthermore, most of these tax evasions happen to online retailers. If this continues, companies could even be charged for doing this. Therefore, to solve this problem, automated blockchain-based sales tax collection can help collect taxes based on the amount of sales or profits made. What's more, retailers can upload their documents, which will be properly verified online. It's really a great way to pay your taxes on time and avoid any legal problems.

Q. 3 Explain the features of Public blockchain.

Ans. : Public Blockchain

- Public blockchains are open networks that allow anyone to participate in the network i.e. public blockchain is permissionless. In this type of blockchain anyone can join the network and read, write, or participate within the blockchain. A public blockchain is decentralized and does not have a single entity which controls the network. Data on a public blockchain are secure as it is not possible to modify or alter data once they have been validated on the blockchain.
- Some features of public blockchain are :
  - **High Security :** It is secure Due to Mining (51% rule).
  - **Open Environment :** The public blockchain is open for all.
  - **Anonymous Nature :** In public blockchain every one is anonymous. There is no need to use your real name, or real identity, therefore everything would stay hidden, and no one can track you based on that.
  - **No Regulations :** Public blockchain doesn't have any regulations that the nodes have to follow. So, there is no limit to how one can use this platform for their betterment
  - **Full Transparency :** Public blockchain allow you to see the ledger anytime you want. There is no scope for any corruption or any discrepancies and everyone has to maintain the ledger and participate in consensus.
  - **True Decentralization :** In this type of blockchain, there isn't a centralized entity. Thus, the responsibility of maintaining the network is solely on the nodes. They are updating the ledger, and it promotes fairness with help from a consensus algorithm .
  - **Full User Empowerment :** Typically, in any network user has to follow a lot of rules and regulations. In many cases, the rules might not even be a fair one. But not in public blockchain networks. Here, all of the users are empowered as there is no central authority to look over their every move.
  - **Immutable :** When something is written to the blockchain, it can not be changed.

- **Distributed** : The database is not centralized like in a client-server approach, and all nodes in the blockchain participate in the transaction validation.

Q. 4 What is Trade Finance ? How can blockchain technology be useful for it?

Ans. : Trade Finance

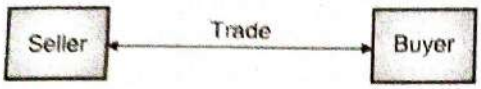


Fig. 6.6

Finance for commerce is referred to as trade finance, and it includes both domestic and international trade transactions. A buyer and a Seller of products and services are both necessary in a transaction. These transactions can be facilitated by a number of intermediaries, including banks and other financial institutions, who can finance the trade. Trade finance is typically offered by intermediaries and takes the form of letters of credit (LOC), guarantees, or insurance.

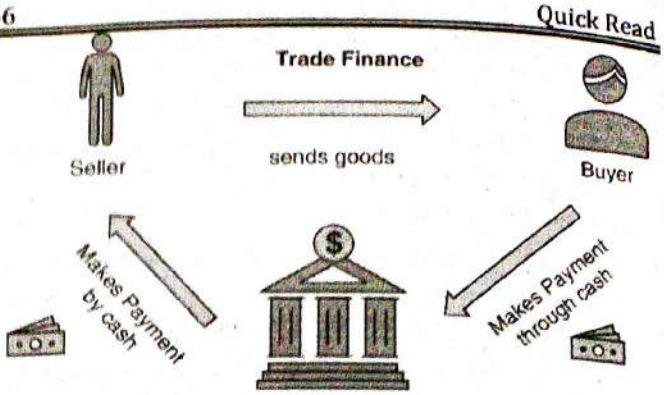


Fig. 6.7 : Trade Finance

Two major terms used in Trade Finance are : Letter of Credit (L/C) and Bill of lading (BL or BoL)

1. Letter of Credit (L/C)

- A letter of credit (L/C) is a bank document that ensures the buyer will pay the seller once the items have been received.
- If the buyer is unable to make the payment on the purchase, the bank would be obligated to cover the entire or remaining amount of the transaction.

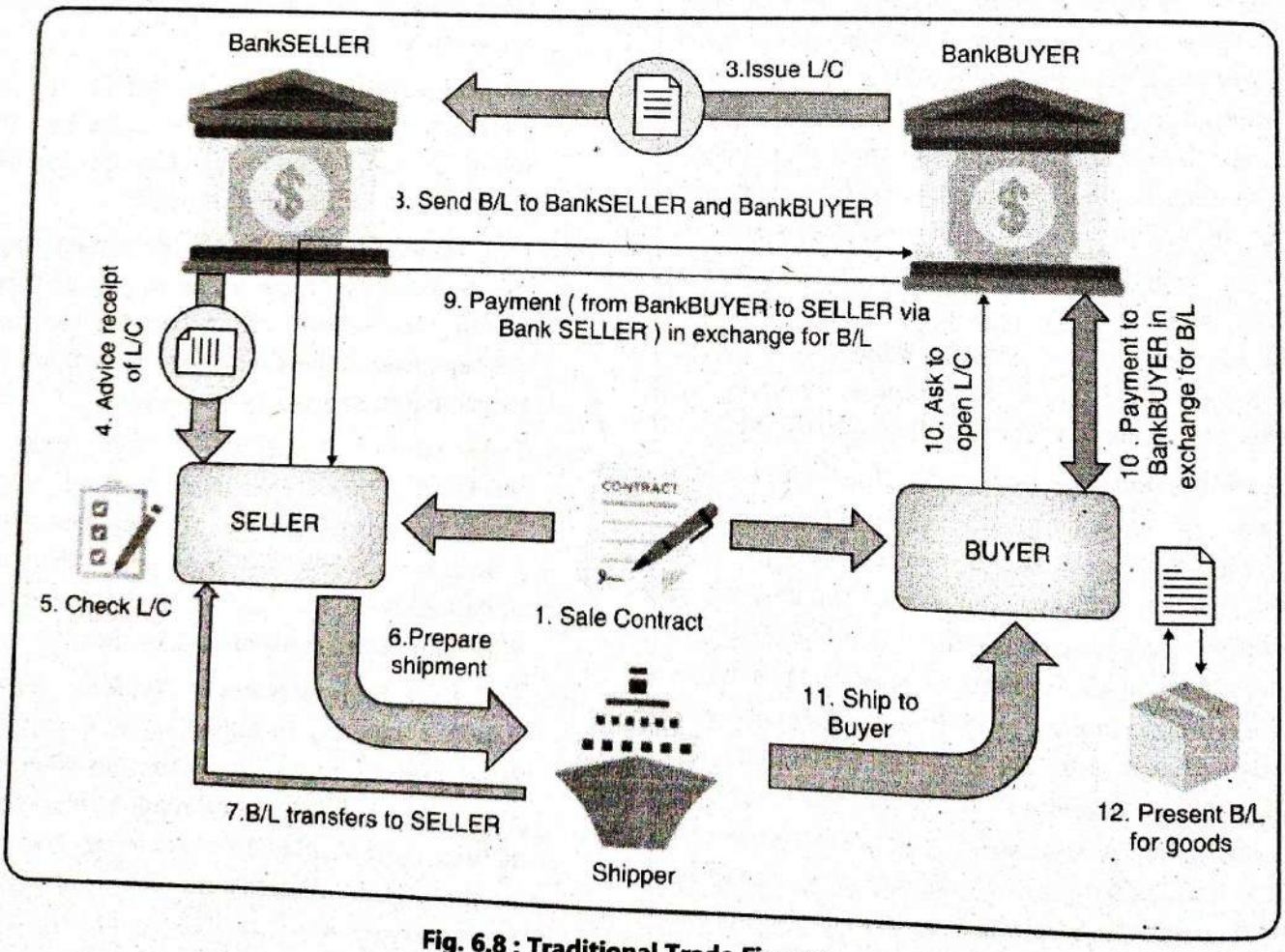


Fig. 6.8 : Traditional Trade Finance

2. Bill of Lading (BL or BoL)

- Regardless of the method of transportation, a bill of lading (BL or BoL) is a legal document that must be signed by an authorized representative from the airline, shipper, and recipient and be included with the delivered goods.
- The bill of lading serves as a shipment receipt when the carrier delivers the items to a specific area.
- Steps involved in Traditional Trade Finance are as follows :

1. The first stage in trade is the creation of a sale contract between a seller and a buyer.
2. The buyer instructs their bank to write a letter of credit (L/C) and send it to the bank of the seller.
3. The buyer suggests that the seller confirm the L/C that was obtained for the exchange of items.
4. The shipper supplies the seller with shipping documentation such as a bill of lading (B/L or BoL), and the seller arranges for the buyer's shipment.
5. The buyer then pays their bank for the B/L, which they then give to the shipper when the items are delivered in order to receive them.

Automated Processes

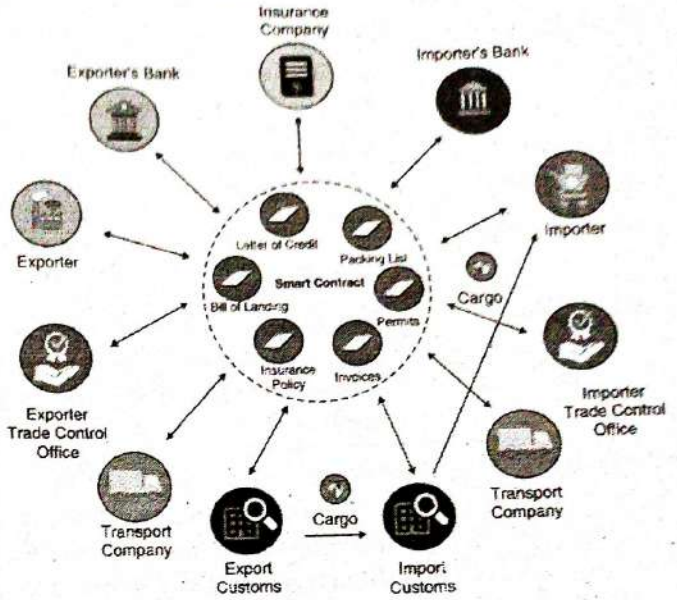


Fig. 6.9 : Trade finance using Blockchain

- Smart contracts can automate financing procedures. For instance, rather than having to wait for a months, finance for an upstream supplier can be approved and sent as soon as a shipment has been confirmed by a third party.

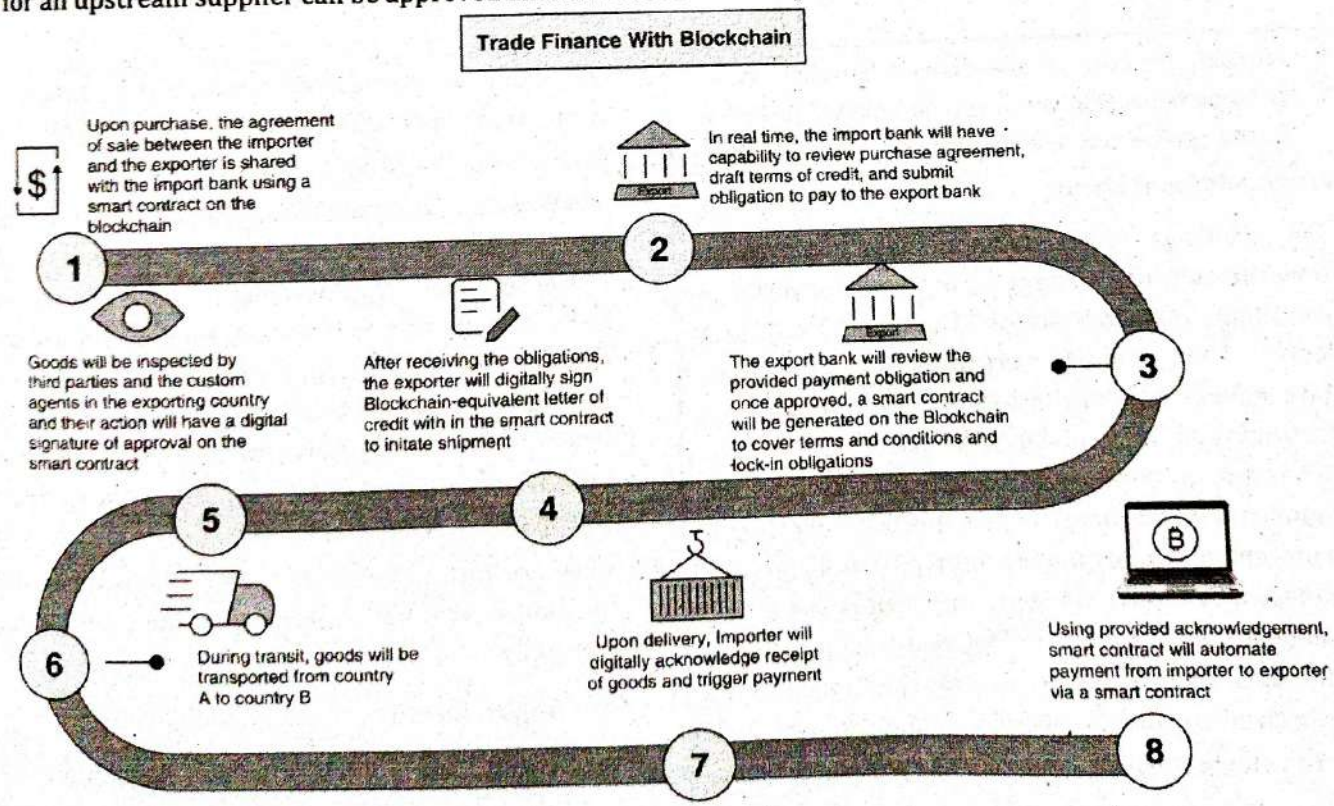


Fig. 6.10 : Stepwise trade finance process with blockchain

Following Table 6.1 gives the comparison between Trade Finance without Blockchain and with Blockchain.

Table 6.1

	Trade Finance without Blockchain	Trade Finance with Blockchain
Trust Mechanism	Relying heavily on an approved central party to act as an intermediary (such as banks) to handle trade	Building a trustworthy trading environment through the use of distributed ledger technology that is immutable and consensus-based
Fraud and authenticity	Being in the center causes fraud and business problems.	Reduce the tempering problem
Document type	Processing done by Manual way and using paper	On a distributed ledger, a digital document
Bill of Lading	Lots of preparation for the presentation. Long distance delivery, difficult ownership transfer with multiple handovers	Reduced transfer and delivery times because of digitization; blockchain-based B/L presentations
Traceability	Various participants in complex economic procedures; Uncertainties in tracking asset identities, ownership, and shipment status brought on by handovers	A member database that may be searched for a credit rating analysis, improving the user experience
Information transmission	Manual processing is time- and money-consuming; Coordinated data manipulations that could lead to system failure or cyberattacks	Consensus process with tamper-proof features; event-driven mechanism with smart contract parameters. Less privacy and security issues with consortium chain.

Q. 5 Explain the use of blockchain technology in the government sector. which are the different blockchain based applications available for it?

Ans. : Government Sector

- The challenge comes down to data management Governments, like all large organizations, struggle to coordinate processes across disparate stakeholders. More than most organizations, however, governments are expected to provide transparency, fairness, and accountability to the public. To be successful in these endeavors, particularly in the digital era, the challenge comes down largely to data management. Unfortunately, legacy centralized data management tools do not sufficiently meet the challenges governmrver model, and transparency is difficult to achieve where government databases are centralizedents face. Security of data is compromised by the single point of failure in the standard client-se.
- The result, for most governments, is slow, inefficient, and opaque operations for everything from land title registration to voting.
- Leveraging a new data management structure – one that uses distributed ledgers supported by blockchain and cryptography – governments can offer citizens the streamlined, on-demand services they have become accustomed to in the digital era. At the same time, governments can go above and beyond the tech-giants by offering not only improved data security, but also unprecedented transparency and accountability.
- Here are just some of the use cases of blockchain technology that governments and the public sector can apply :
  - Digital identity
  - Healthcare
  - Administration
  - Data storage
  - Registries
  - Regulation
  - Voting
  - Central banking

Digital identity

Identity management is a cornerstone of governmental services, but legacy data management tools fail to provide secure yet rapidly accessible and updateable identity. In traditional system citizens are forced to supply personal data repeatedly at multiple business and government entities and they have limited control over the utilization of this data. There is a rising demand for using a technology that supports transparent digital identity management. Blockchain-based identity management offers citizens the opportunity for self-sovereign identity, meaning citizens have granular control over access to their ID, but information contained within it is instantly verifiable.

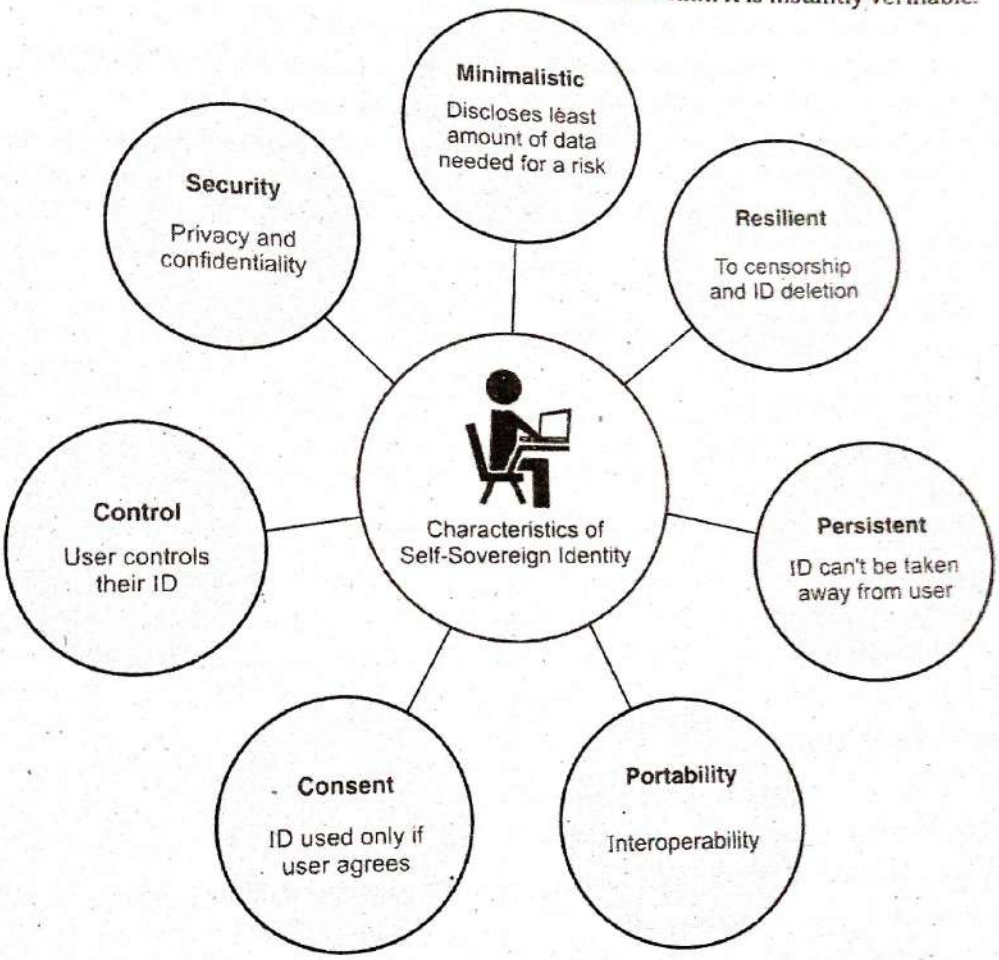


Fig. 6.11 : Characteristics of self-Sovereign identity

As a simple example, a municipal officer scanning a citizen's ID could confirm her name and, for instance, city of residence, without revealing any other sensitive information. With secure and verifiable digital identity in place, access to government-provided services is considerably streamlined. Blockchain-based self-sovereign digital ID, then, can form the basis for many other initiatives. Just a few examples include :

- Verifying academic credentials
- Interacting with the tax system
- Electronic health records
- Pensions
- Grants

Aadhaar 2.0

- The world's largest digital identity program "Aadhaar" that is administered by the Unique
- Identification Authority of India since 2009. This is a centralized system with more than 1.2 billion enrolled users that is not DLT based, but hinges heavily on biometrics to identify users.
- The main purpose of Aadhaar is to improve social service provision.
- The Aadhaar-issuing body is also exploring possibilities for the usage of blockchain technology. so it is more difficult to hack these systems than hacking the centralized or traditional servers.

Registries

- Governments and their legal branches serve as the primary source of truth on everything from land titles, to the registering of corporate entities, marriage and divorce records, criminal records, and more. Managing these registries is a complex proposition that, using legacy tools, results in corruption, fraud, high-costs, and slow processing.
- Managing registries with blockchain-supported distributed ledgers provides the needed transparency to eliminate fraud and corruption while simultaneously offering the potential for real-time updates. The latter feature is critical for speeding up notoriously slow processes like land title transfer.

Land Registry

- Land Registry is a set of documents that stores information about the legal owner of a house, the land, and all the associated assets.
- The term's land registry and record are interchangeable.
- These records are provided under the supervision of government authorities.
- They also help in giving information about the former owners as well as the date of sale.

Land Management system in India :

01	Revenue Department	• Collection of land revenue and maintenance of record of rights (ROR)
02	Survey and Settlement Department	• Maintenance of spatial land records and maps of cities and villages
03	Registration and Stamp Revenue	• Registration and maintenance of property documents and deeds • Evaluation and collection of stamp duty

Fig. 6.12

Current Challenges in Land Registry

- Difficulty in identifying the legal owner of the asset or land.
- Land dispute between legal owner and claiming owner
- Claiming owner filing lawsuit against the legal owner to recover possession of the property
- Disputed land cannot be sold or bought
- Land disputes account for 66% of all pending court cases in India
- Estimated pendency of 20 years from the time of undertaking to final resolution

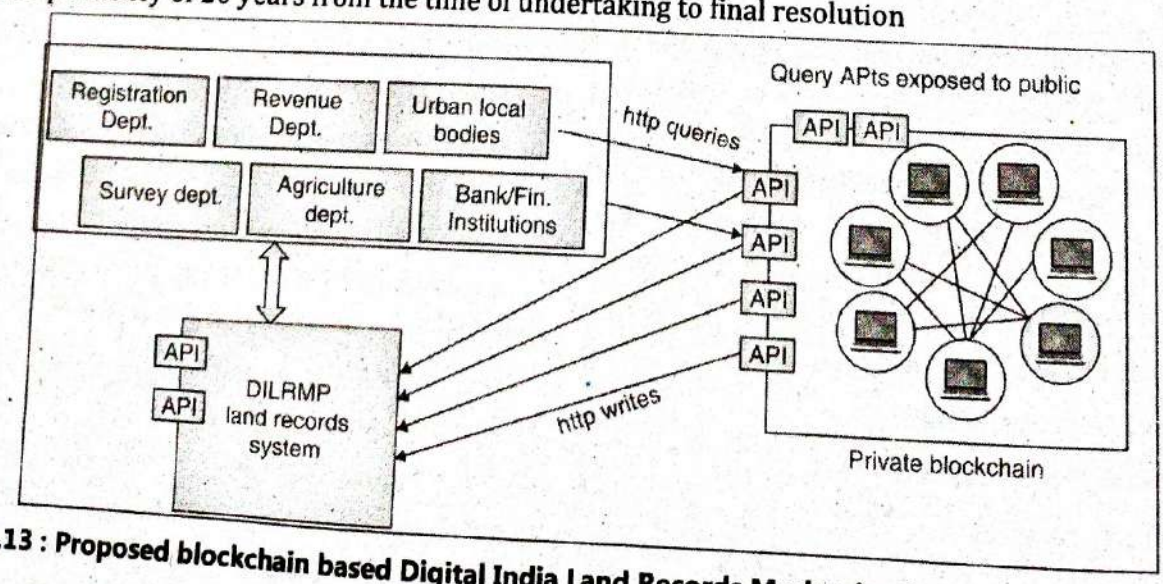


Fig. 6.13 : Proposed blockchain based Digital India Land Records Modernization Programme (DILRMP)

Benefits of blockchain based Land Registry

- The availability of data in a central location that can be accessed by all departments would enable faster disposal of requests for subsidy, mutation,
- There would be no need for trusted authority like notaries to provide attested copies of documents.
- The farmers will be assured that their land ownership cannot be changed by spurious persons.
- The farmers can obtain loans quickly.
- The facilities provided to the farmer from the agriculture / Horticulture departments / Animal Husbandry department when recorded in the blockchain will facilitate these departments to ensure that the same benefit / multiple benefits do not reach the same farmer multiple times or might not receive multiple benefits as per the terms & conditions laid down.
- Blockchain data of the property registration will be made available in the workflow system of the Registration software as well as the public for verification. This will provide the complete details of the property chain right from the first purchaser to the latest one. The Purchaser need not depend on any non-reliable personnel/agency to verify the authenticity of the document provided by the seller.
- A repository of transparent, trusted and tamper proof Property Registration documents would be available for use by citizens & the registration department.
- Citizens can verify the ownership details & complete history of the property before going in for purchase of the property

Birth, Marriage and Death Certificate

- Our identity as a human being is determined by the documents, not by appearance or physicality.
- The most important thing to prove the identity of humans is to show a government-issued document. Generally, from birth to death humans are recognized by documents because they are born with a birth certificate and they die with a death certificate.
- The main problem with these documents is that they can be falsified or manipulated by others.
- Blockchain-based digital locker, which is similar to the DigiLocker released by the Department of Electronics and Information Technology (DeitY), Govt. of India.
- It will help in treating each document as an asset by making it immutable, where documents can not only be shared but also verified.

Birth registration through blockchain

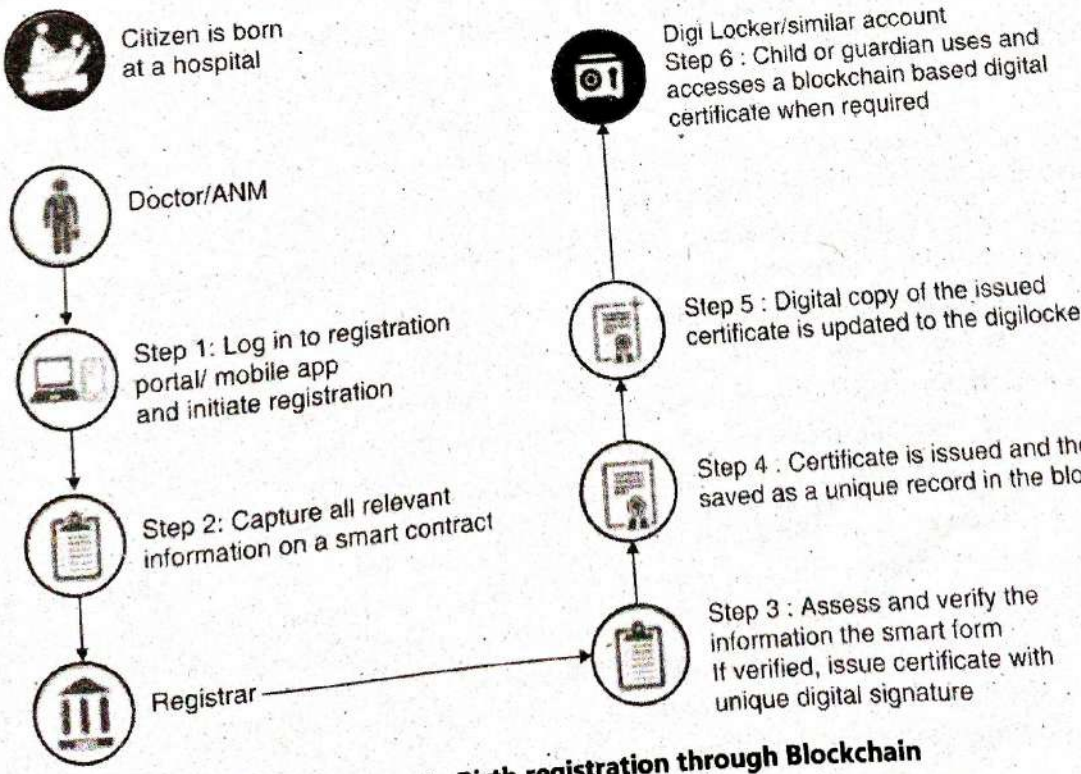


Fig. 6.14 : Birth registration through Blockchain

Healthcare

- Security, privacy, and interoperability issues inherent to legacy data management tools currently prevent the proliferation and utilization of electronic health records (EHRs), which can form the foundation for efficiency improvements in government-managed healthcare.
- EHRs built on a blockchain-supported distributed ledger can enable some or all of the following use cases :
  - Freedom of movement with the healthcare system.
  - Elimination of redundant onboarding procedures and tests.
  - Digital prescriptions that can be easily screened for potential adverse reactions.
  - More personalized healthcare.
  - Citizens taking ownership of their health data and volunteering it or selling it for research.
  - Incentives for citizens to make defined positive health-related choices.
  - Automated payments for healthcare providers and vendors.
- In addition to forming the basis of next-generation EHRs, blockchain can also be leveraged to provide universal visibility and resiliency for drug and medical equipment supply chains, as well as to improve coordination in the development of medicines and medical treatments.

Regulation

- Enforcing regulation is as onerous a task for the government as adhering to regulation is for businesses. A big part of the problem is the inadequacy of legacy tools when it comes to managing the data needed for both the enforcement of and adherence to regulation. Consider the example of aviation parts, which are subject to strict regulations throughout their lifecycle to ensure safety.
- Parts which have been approved for use (a heavily regulated process in itself) must have their hours in operation logged and adhere to a regulated schedule for overhauls. All collected data must retain its continuity in the secondary market for aviation parts. Precisely tracking the provenance of aviation parts transparently and immutably is, therefore, essential for preventing fraud and ensuring safety.
- It is also essential for authorities to have the capacity to track and trace items granularly and in real time, as it allows authorities to identify the source of substandard part or contamination, and issue timely but targeted recalls. Blockchain-supported distributed ledgers enable all of the above features and so can streamline regulation and enhance reaction capacity in the event of emergency. Some examples of industries that can benefit from blockchain-supported regulation include :
  - Aviation parts
  - Pharmaceuticals
  - Medical equipment
  - Securities
  - Food supply

Administration

Administration of government-managed programs ranging from pension systems to healthcare, education, and defense often requires coordination between disparate parties and almost always involves sensitive data that must be protected. Blockchain-supported administration systems enable real-time coordination between wide-ranging participants while also providing the needed transparency. Some examples of use cases include :

Management of Government Contracts

Posting and administering government contracts on a distributed ledger with granular read/write permission control can provide the needed balance between transparency and protection of confidentiality.

Sovereign Wealth-fund Administration

Blockchain can facilitate the transparent management of sovereign wealth funds, bolstering public confidence and ensuring adherence to, for example, sustainability goals.

Pension Administration

Combining blockchain supported digital identity with pension ecosystem partners can streamline the entire pension lifecycle, from entering the workforce to expiration.

Voting

Counting votes in a timely but secure and transparent manner is a challenge faced by every democratic government. Blockchain has been proven to support voting by improving transparency and immutability in the collation period (when, after votes that have been counted at individual polling stations, they must be aggregated with other polling stations to form a consensus for a given region).

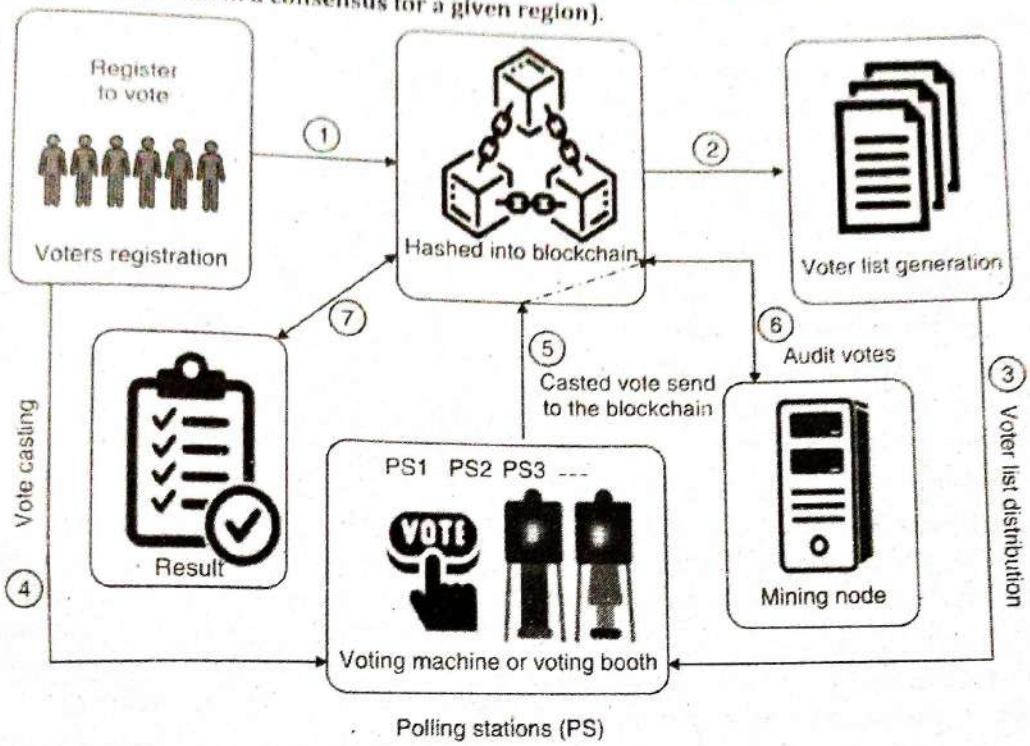


Fig. 6.15 : Architecture for Blockchain based voting system

Data Storage

Blockchain can be used to support digital storage of publicly accessible records. By distributing storage across multiple nodes, both the resiliency and the integrity of the data can be ensured.

Central Banking

(a) Central Bank Digital Currencies (CBDCs)

- CBDCs offer a way for central banks to improve management of the money supply by, for example, quickly and efficiently getting money into the hands of citizens and businesses in the event of a liquidity crisis. CBDCs also make it possible for governments to offer a higher level of transparency into the money supply
- Here are three aspects that define a central bank digital currency:
  - Digital assets. CBDCs are digital assets. They are accounted for in a digital ledger that acts as the single source of truth.
  - Central bank backed. CBDC represents claims against the central bank, just as banknotes do.
  - Central bank controls the supply of CBDC is fully controlled and determined by the central bank.

(B) Real Time Gross Settlement (RTGS)

Blockchain supported RTGS can ensure transaction privacy, provide settlement finality, and improve resiliency by eliminating the single point of failure inherent to legacy systems.

GST

The vital information which is usually needed by Tax authorities has been identified as follows :

- Registration details, Annual returns, Payments & ledgers details, Notices served on tax payers under various sections of the CGST Act.
- Registration details comprises Taxpayers registration information etc.
- Returns – Annual returns in GSTR9, GSTR 9A, GSTR

9C and Final return GSTR 10 Taxpayer payments & ledger information which reflects the GST payments status of ledgers.

- It is also necessary to know the Refund claims settled for Taxpayers.

A) Why Blockchain for GST ?

- Blockchain based GST records will be immutable, tamper free as data can be appended-only. No modification, deletion possible thereby providing all stakeholder agencies with required information for day-to-day enforcement activities.
- Stakeholders outside the GST ecosystem such as other Government enforcement agencies etc can also have access to the blockchain enabled GST records.
- Blockchain info can provide several views of same information with varying granularity and details based on the access controls defined
- Durability, Reliability – Due to decentralized/ distributed networks, blockchain does not have a central point of failure and is better able to withstand malicious attacks. Greater security makes it more reliable.
- Empowered stakeholders – Each stakeholder controls their transaction and information. Transaction authorisation is through Consensus.
- High availability can be realized with Distributed ledger architecture

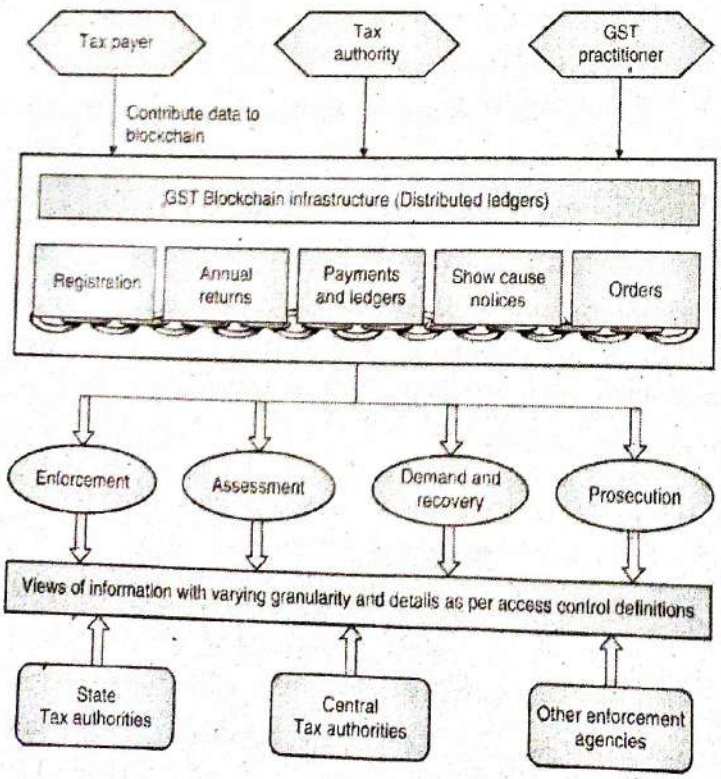


Fig. 6.16

B) Stakeholders of GST Blockchain

- State Commercial Taxes Department
- Central Board of Indirect Taxes & Customs (CBIC)
- Enforcement Directorate
- Directorate General of Foreign Trade
- Various other Central and State authorities empowered

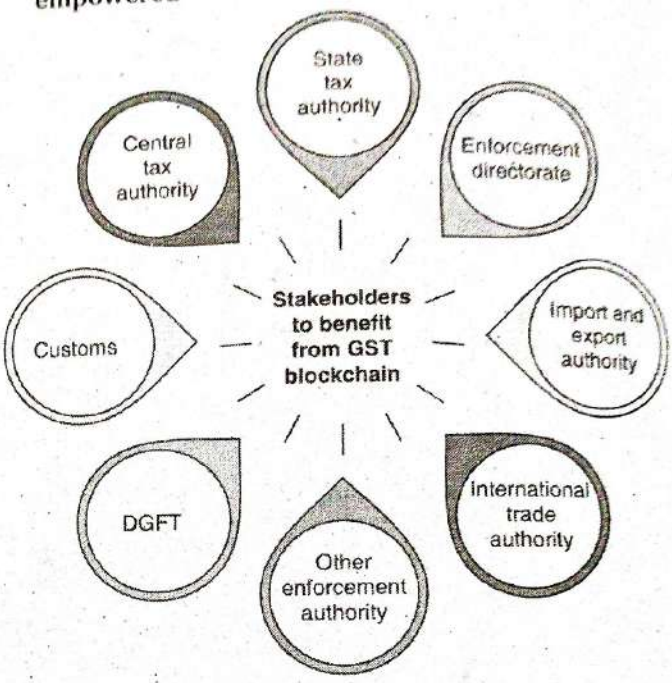


Fig. 6.17 : Stakeholders to benefit from GST Blockchain

Q. 6 How blockchain technology can be useful for storing electronic health record? give any example of it.

Ans. : Electronic Health Records (EHRs)

Challenges in Keeping Health Records

1. Medical records are stored in a hospital's centralized database.
2. Hospitals can sell or alter medical records.
3. Every time you access data from the hospital, you have to go through a maze of approvals.
4. It is difficult to get a second opinion when the data is not handy.
5. There is no control over the data.
6. In the case of relocation, you need to see a new doctor who might need health records.

Advantage of Electronic Health Records

1. Real-time, factual, and complete details about the patient are fetched.
2. Data can be accessed from any place.

3. Patients have more autonomy over their personal data.
4. Data privacy and protection will be improved.
5. Coordination between patients and various healthcare departments is improved.
6. Money and time are saved.

Challenge to Electronic Health Reports

1. It cannot accommodate multi-institutional complexities or maintain lifetime medical records
2. Data is dispersed among various institution
3. Data manipulation
4. No easy accessibility of information in the case of multi institutions

Electronic Health Record Using Blockchain

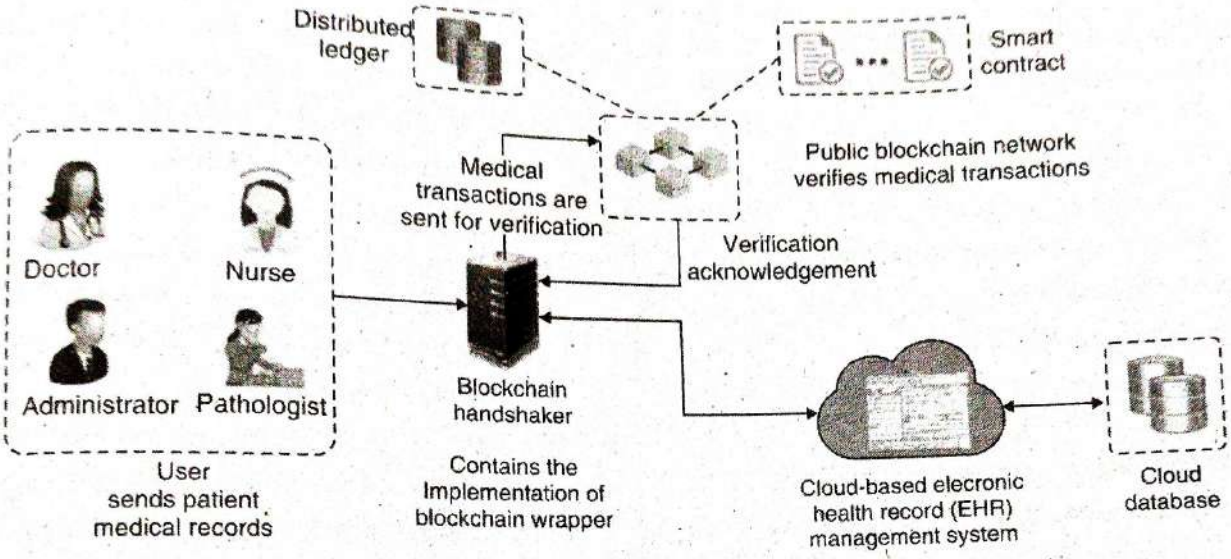


Fig. 6.18 : Electronic Health Record Using Blockchain

Q.7 Write a short note on drug and medical equipment supply chain using block chain.

Ans. : Drug and Medical Equipment Supply Chains

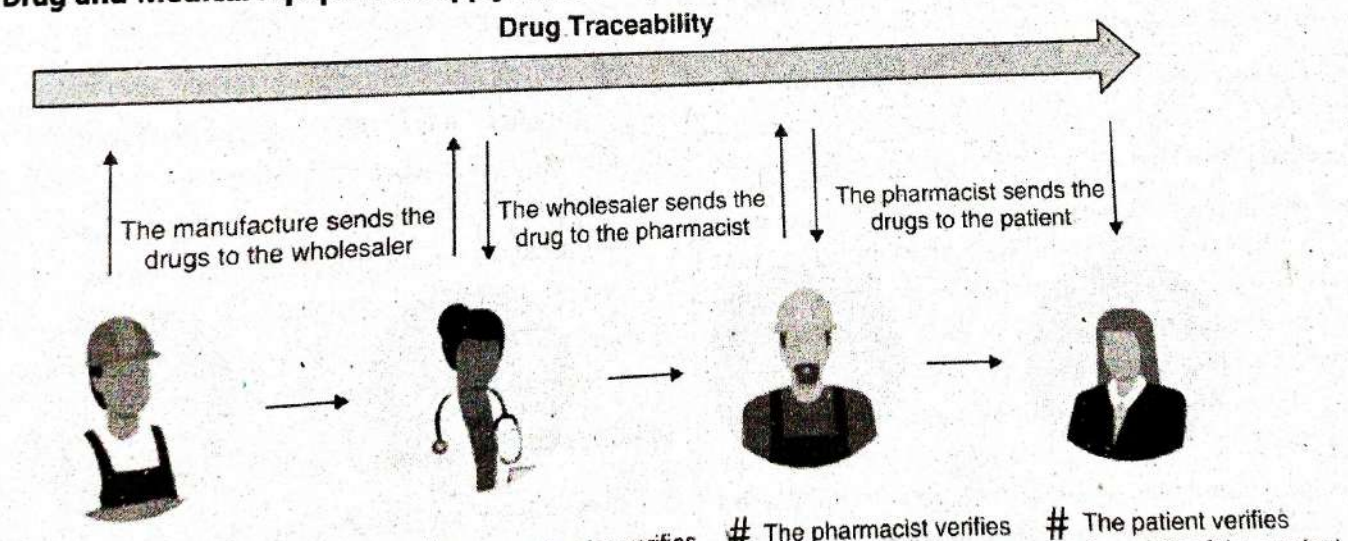


Fig. 6.20 : Blockchain based Drug Traceability system

Blockchains can be used to trace the origin of pharmaceuticals, the transport of drugs, and the procurement of raw materials. Blockchain technology also reduces the number of intermediaries involved in the pharmaceutical process, thereby reducing costs and improving safety.

Achievements of blockchain based Drug Traceability system.

Provides drug safety

- Prevents fake and counterfeit medicine use
- Tracks the side effects of medicines and use of terms may change
- Blocks the sale of recalled medicines
- Tracks the expiry dates of medicines

Prevents parallel trade and stock inadequacy

- Controls exported medicines
- Prevents stock inadequacy
- Keeps the records of all incoming and outgoing medicines
- Prevents international medicine smuggling

Prevents reimbursement frauds

- Prevents scams in medicine strips
- Prevents re-sale of the same medicine

Provides clean supply chain

- Monitors the medicine tracking from the beginning of production/export process.
- Blocks the sale of unrecorded medicines into the system

MediLedger Network

- The MediLedger Network is the industry network 2.0 for the life sciences and healthcare industry, that runs solutions for real-time alignment, rule enforcement and settlement of transactions directly between trading partners
- It is a private permissioned blockchain-based network for the healthcare industry for healthcare trading partner transactions, established in 2019 by leading companies in the life sciences and healthcare.
- Features of MediLedger Network

1. **Alignment** : The MediLedger Network gives trading partners a unified view of transaction-related data among trading partners. (ex. Contracts, customers, pricing, products)
2. **Accuracy** : The MediLedger Network blockchain enforces the accuracy of trading partner transactions automatically, against data aligned through the network and established business rules
3. **Privacy** : Participants maintain control over their private data, including which trading partners receive which updates through the secure network.
4. **Decentralization** : Data and transactions are shared through the MediLedger Network directly between trading partners, without any party sitting in the middle.

- MediLedger Network provides the Contracts & Chargebacks solution that eliminates chargeback errors, by automatically settling chargeback transactions against aligned pricing contracts and established business rules.
- Through the solution pharmaceutical and other healthcare product manufacturers, wholesalers and GPOs (A group purchasing organizatio)get a unified view of:
  - Clean/validated GPO membership rosters
  - Customer Identifier data (HIN, DEA, 340B)
  - Contract headers, pricing, customers
- With this data aligned through the network, the MediLedger blockchain can then enforce chargeback business rules against pricing contracts in real-time, ensuring chargeback accuracy. The solution eliminates manual processes for everyone involved, reduces revenue leakage, and improves trading partner and customer experience in the healthcare supply chain.

Medicines Development

- Medicines development makes use of the scientific method, whereby hypotheses are proposed then tested. An abundance of quality data enables reliable hypotheses, while even more data are needed to prove the hypotheses. Collaboration between disparate stakeholders in the medicines development process requires the secure and transparent sharing of data.

- Patient privacy and intellectual property must be upheld while at the same time data must be made available for clinical research organizations (CROs), vendors, peer reviewers, and regulators. Unfortunately, legacy data management tools are insufficient to facilitate the high level of collaboration needed amongst the disparate stakeholders in the medicines development process.
- The result is that much of the data relevant to and necessary for medicines development remains locked away, with the consequence that medicines development is unnecessarily slow and prohibitively expensive.
- Using blockchain-supported data management tools, participants in the medicines development process are empowered to collaborate. The potential use cases of blockchain-supported data management tools in medicines development include :
  - **Unlocking siloed data :** By deploying a federated learning model built on a blockchain-based infrastructure, pharmaceutical companies can form a consortium to effectively share proprietary data and leverage it for medicines research.
  - **Improved data management in clinical trials :** A decentralized blockchain-supported database with granular read/write permissions for stakeholders in the clinical trial process enables data security, immutability, and transparency.
  - **Real-time view of data collected in clinical trials :** Blockchain-supported data management in clinical trials enables a real-time view of data collected. This allows CROs and/or trial sponsors to make dramatic process efficiency improvements.

Q. 8 Explain how blockchain and IOT can work together.

Ans. : IoT and Blockchain Integration

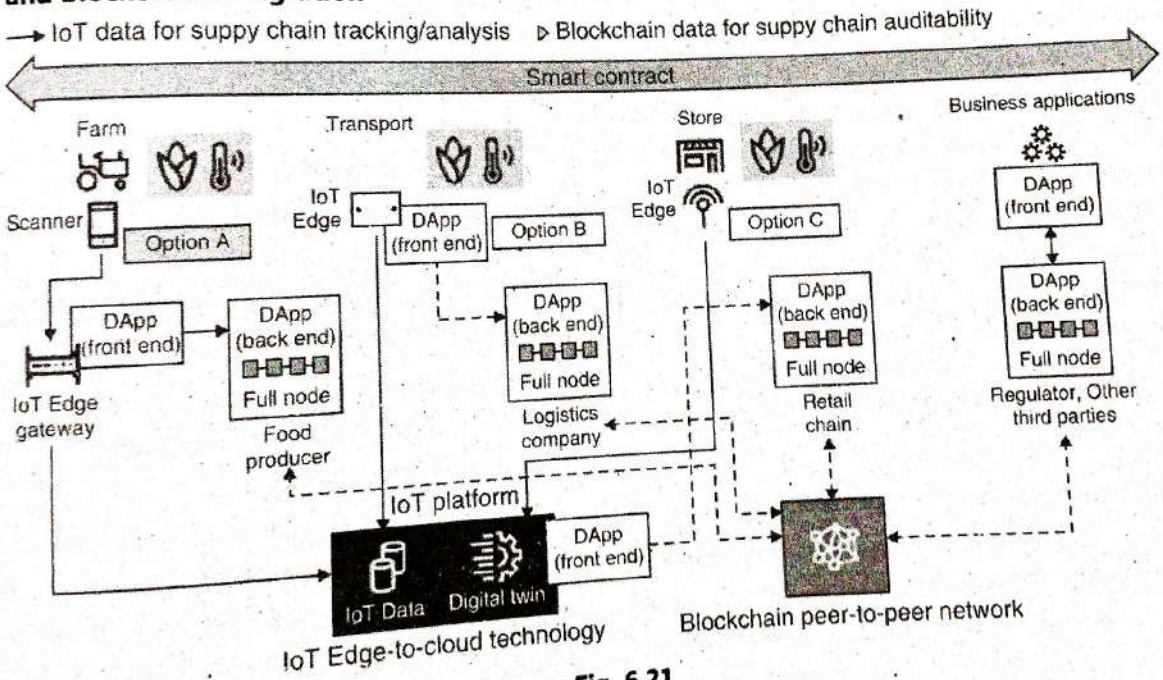


Fig. 6.21

3 Benefits

The integration of IoT and Blockchain supports trusted multi-party processes that connect elements of the physical world with the business process computing environment.

Combined environment :

- Enables immutable audit trails of critical IoT data and related business events that are shared among multiple participants and can be independently verified by each party and

- Supports smart contracts and distributed applications (called dapps) that promote automation among network participants, often by referencing information represented in technical twins number.
- The IoT Digital Twin provides visibility and monitoring of related things and events (e.g., the use of IoT devices to automatically capture the origin of products), and blockchain enables sessions the only shared version of the truth about the state of these "things" during the lifecycle and related business events.
- Enhanced security. Blockchain technology combines security with the ability to verify and authorize transactions from a trusted party, as well as encryption during data transmission and storage. Blockchain technology provides transparency about who has access, who transacts, and a record of all interactions. In addition, blockchain adds an extra layer of cryptographic security, eliminating a single point of failure, and the ability to quickly identify weak links throughout the network.
- Discount. By automating the validation and transaction processing steps on the blockchain, the entire ecosystem can be proactive with lower costs.
- Speed of transactions. This is especially true for supply chain transactions with multiple suppliers, manufacturers, distributors, and consumers. With the blockchain acting as a shared ledger to some extent, untrusted parties can exchange data directly with each other, eliminating manual processes and speeding up transactions.

Q. 9 Explain Helium Network in Details?

Ans. : Helium

HELIUM is a New Model for the Network Age :

- Helium is a distributed network of long-range wireless hotspots. The primary goal of Helium Network is to create a blockchain-powered network for the Internet of Things (IoT) devices. It is a decentralized wireless IOT network using the LoraWan system, tied to the cryptocurrency Helium Network Token.

Nodes on the network are generally owned and placed by individuals in their homes or offices, and they are rewarded for their participation in the network in payments of HNT. The network aims to provide connectivity to IoT sensor devices in areas where wireless or mobile coverage is minimal, or requires too much power.

- Thus, the Helium network is a composition of many individuals and is therefore also called the People's Network. So, Helium is building the world's first peer-to-peer wireless network for the Internet of Things devices. Devices include smart pet collars, e-scooters, medical devices, and more.

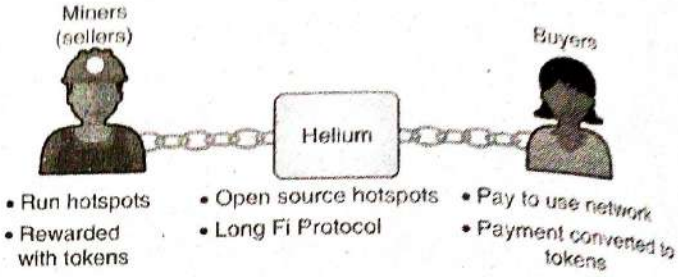


Fig. 6.22

History of Helium

Helium was founded in 2013, only a few years after the inception of Bitcoin, the original cryptocurrency.

- It was founded in 2013 by Shawn Fanning, Amir Haleem, and Sean Carey, with a mission to make it easier to build connected devices.
- Helium was launched under the company Helium, Inc. to become the first global peer-to-peer wireless network with the capacity to connect different devices and form the Internet of Things that anyone can use globally.
- It was founded with a clear mission to make it easier to build connected devices.
- Helium believes that today's wireless connectivity options are totally inadequate for the next generation of machines.
- To solve this they developed the Helium Hotspot, a combination of a physical blockchain node and wireless gateway that network participants can deploy to receive compensation in HNT, the native token.
- In order to receive rewards, Hotspots must submit proof of wireless coverage in a cryptographically verified location and time.
- Once the network is deployed, any sensor using the Helium LongFi wireless protocol can connect to the network which is intended for battery-powered devices sending small amounts of data over miles of range.

- Hotspots are rewarded in HNT based on the quality of the coverage they provide and the amount of LongFi sensor data they transport for devices on the network.
- HNT is burned to create Data Credits, a non-fungible token used for all transaction fees on the network. Data Credits are required for things like sending sensor data and asserting Hotspot location.
- Any LongFi-enabled IoT device can send data through any Helium Hotspot that's providing coverage.
- In 2019, Helium pivoted into the cryptocurrency world and witnessed moderate success. It would experience a massive boom in early 2021, going from roughly 15,000 hotspots worldwide to nearly a million by January.

What Makes Helium Unique ?

Unlike most blockchains, which focus on the decentralization of software, Helium aims to decentralize physical hardware through the interconnection of devices.

The Helium network is also powered by proof of coverage, a novel consensus algorithm created specifically for the network. The mechanism is combined with the Honey Badger Byzantine fault tolerance (HBBFT) protocol, which allows for consensus amidst certain node failures.

PoC (Proof of Coverage)

- The consensus algorithm used by the Helium network is called PoC, which is a variant of the HoneyBadger BFT algorithm. It is particularly important to note that this is not an abbreviated form of another famous proof of the capacity consensus algorithm.
- The key to Helium's PoC consensus is to prove that hotspots work where they are claimed. This consensus algorithm using radio frequency (radio frequency) has its characteristics, meaning that the RF signal is inversely proportional to the physical distance to produce power proof. Formerly google ventures were not so good.
- Every 360 blocks of time, a role called Challenger in the Helium network (the specific role shown in the figure) creates a data packet called "PoC Challenge" through the P2P network and randomly challenges a role. The whole process, called a transmitter, is based on the principle of cryptography, a more intuitive process is shown in the figure below (the two clouds in the figure represent the same network, the composition is separated).

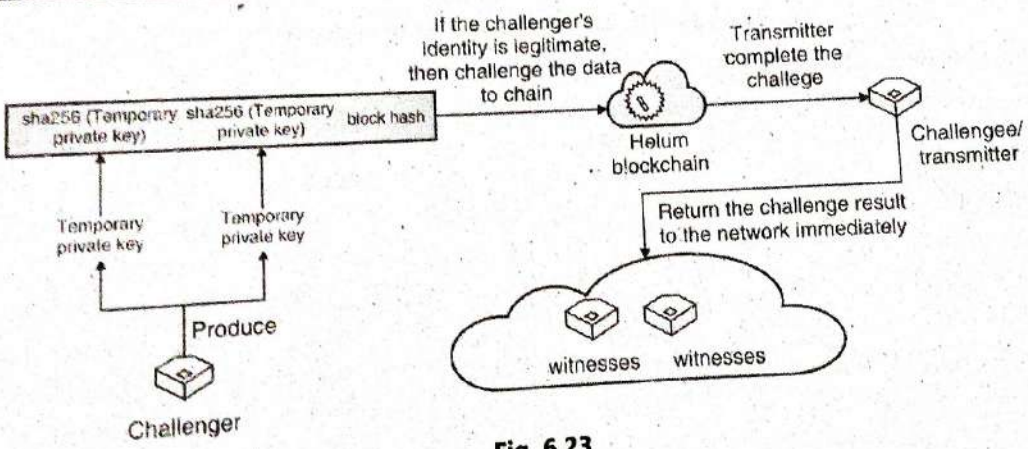


Fig. 6.23

Helium Network Working

- Hotspots are the fundamental pillars of the Helium network as they provide connectivity for IoT devices. The closer a hotspot is to another hotspot, the better, as not only makes the network denser and provides wider coverage but also increments rewards to the owner.
  - These hotspots act as nodes, allowing IoT devices to send and receive data between them and also secure the Helium blockchain.
  - When users plug a hotspot into an outlet and run it, they start mining HNT, which is rewarded to them as an incentive.

- Helium aims to create a reliable, decentralized, and global network for IoT devices that rely on the community of HNT holders.
- The network consists of nodes, i.e. Hotspots that are run by node operators who are actually HNT holders.
- By hosting Hotspots and managing nodes, users are incentivized for their participation in the network's functionality.

- WiFi already has support for IoT devices. However, supporting as many different devices as possible brings up privacy concerns. Helium solves this issue using a decentralized architecture and consensus mechanism that gives the network 200 times greater coverage compared with WiFi connection with the IoT.
- The consensus mechanism that the network runs on is known as Proof of Coverage as discussed earlier and is also responsible for distributing rewards to HNT holders and node operators. Users need to purchase a mining device from the Helium website to set up Hotspots. Miners produce radio frequencies by connecting to the network, while the Proof of Coverage mechanism validates Hotspot locations.

Helium : A decentralized wireless network :

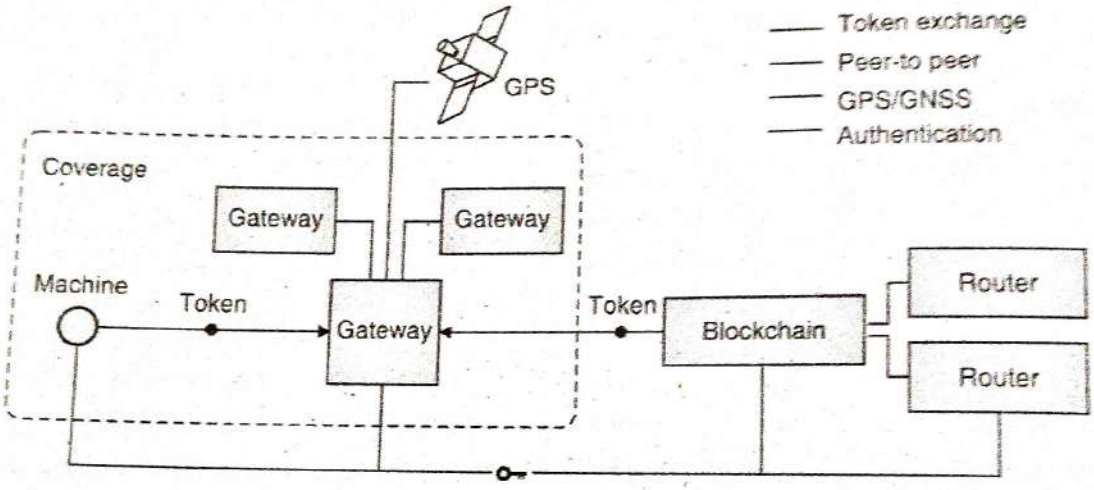


Fig. 6.24 : System overview conevticity technology

Technical Architecture of a LoRa Network

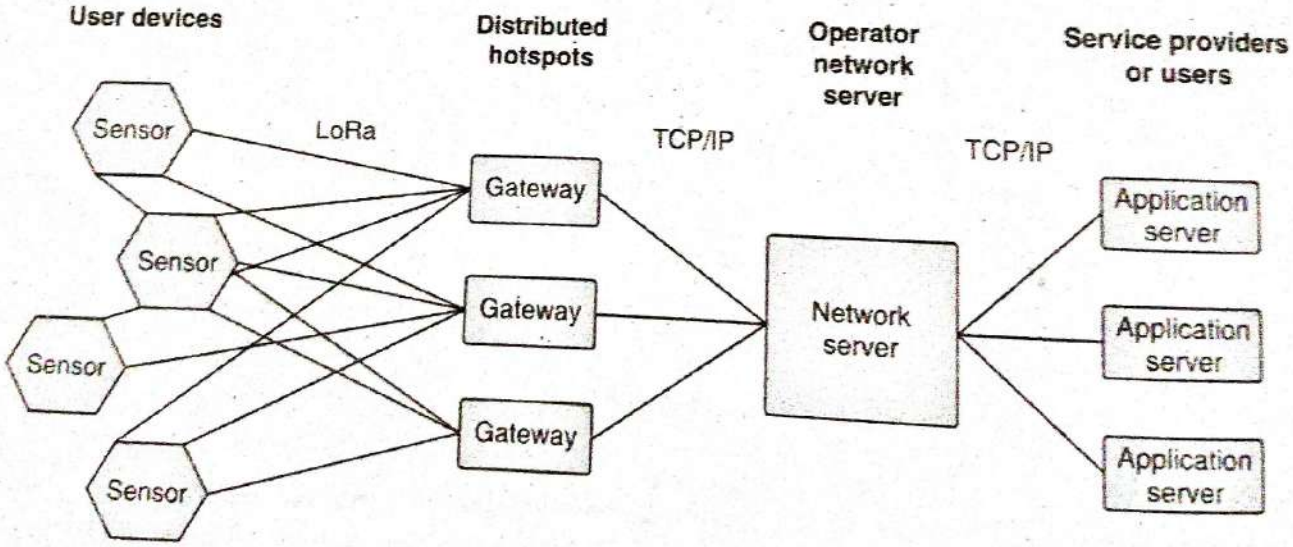


Fig. 6.25

Q. 10 Write short note on Helium key Components .

Ans. : Helium Key Components

Below are some of the key components of Helium :

1. **Helium LongFi :** LongFi is simply the proprietary name of the Helium network. LongFi is the combination between the Helium blockchain and the LoRaWan architecture. LoRaWan (Low-power wide-area network) refers to a distributed architecture sitting on top of a physical layer called LoRa (short for long range) which provides wireless, low-power communication links for IoT devices.

2. **Helium Proof of Coverage :** Now that we have explained how Helium hotspots work, let's look at how the Helium network is powered: the proof-of-coverage (PoC) consensus mechanism. The PoC consensus algorithm allows nodes (hotspots) to communicate with each other via radio frequency. It constantly tests hotspot nodes using a mechanism called PoC Challenge to verify that the hotspot nodes are where they claimed to be.

   The Challenge has three key roles, each receives a portion of HNT for carrying out their specific task :

   - **Challenger :** It is also known as the Transmitter, is the validator in charge to execute the PoC Challenge.
   - **Beaconer (Challenger) :** It is the target being tested. The challenger needs to submit what's called "challenge packets" as proof of work.
   - **Witness :** It is in charge of validating the Beaconer's challenge packets and submitting them to the Transmitter.

   The Helium network can punish nodes that act maliciously, for example: preventing other nodes in a consensus group from performing their tasks. The number of rewards that a punished validator receives decreases considerably, not to mention they can lose the chance to participate in consensus groups. All the network participants are rewarded with Helium crypto tokens (HNT) with the completion of proof of coverage and network data transfer.

3. **Helium Consensus Protocol :** It is a novel consensus protocol construction that creates a permissionless, high throughput, censor-resistant system by combining an asynchronous byzantine fault tolerant protocol with identities presented via Proof-of-Coverage.

4. **Helium and the aBFT Consensus :** The PoC mechanism leverages the HoneyBadger BFT (HBBFT) consensus, which is an asynchronous Byzantine Fault Tolerant (aBFT) algorithm. It allows network nodes to reach a consensus by themselves without worrying about time assumptions. In simpler words, nodes are capable of executing commands at their time and speed without waiting for nodes to reach an agreement. This enables the network to run without disruption and process a larger number of transactions.

5. **Helium Hotspot :** A low-cost hardware device that serves as both a Helium miner and a wireless gateway for Helium. The Helium Hotspot enables anyone to own and operate a wireless network for low-power Internet of Things (IoT) devices. The Helium Hotspot provides hundreds of square miles of connectivity and can transmit data at a fraction of the cost of a cellular network.

6. **WHIP :** An open-source wireless network protocol to locate the positions of hotspots. It is designed for low-power devices over vast areas. This protocol is designed to run on existing commodity radio chips available from dozens of manufacturers with no proprietary technologies or modulation schemes required.

7. **Proof of Location :** A system that verifies the hotspot locations via WHIP. Helium Network outlines a system for interpreting the physical geolocation of a Device using WHIP without the need for expensive and power-hungry satellite location hardware. Devices can make immutable, secure, and verifiable claims about their location at a given moment in time which is recorded in the blockchain.

   Helium aims to decentralize physical hardware through the interconnection of devices, unlike most other blockchains, which focus on the decentralization of software. It connects enabled devices through a series of hotspots, and hotspot hosts can earn the Helium cryptocurrency for being part of the network.

Q. 11 Write Pros and Cons of Helium Blockchain.

Ans. : Pros of Helium Blockchain

- **Naturally decentralized by design :** The network provides no incentive to take advantage of factors, such as the cost of cheap energy or distributing more hardware in the same place. Hence, powerful players won't need to get together to form mining pools, which frequently results in an increasingly centralized protocol (as is often the case for proof of work mechanisms such as those of Bitcoin and the current version of Ethereum).

- **Revolutionized Network :** Helium uses innovative technology that can revolutionize the world of telecommunications
- **Economical :** Mining is done via an affordable, simple device, rather than an expensive GPU. It takes only a simple installation of a hotspot by the window and one can start mining.
- **Less Wasteful :** Since the blockchain is connected through small devices, the energy needed to run them is far less than that required for the proof of work protocol.
- **Cryptocurrency Appreciation :** The Helium network is growing, and the price of its cryptocurrency is on a general upward trend. Because it's a peer-to-peer network, anyone who gets a Helium hotspot has the potential to earn Helium crypto.
- **Scalable :** Helium is scalable and secure.

Cons of Helium Blockchain

- **Competing with established companies :** Helium may be unable to gain traction, as its concept of an IoT framework is already offered by tech giants like Amazon and Google. There are also already many existing open-source IoT platforms, such as Kaa IoT and Zetta.
- **Production of Helium hotspots :** Because the Helium network is so popular and production of Helium hotspots has slowed, it can take months to receive a hotspot after purchasing it. Also, if there are not a lot of hotspots in your area, earnings will not be as high.
- **Helium Investing can be dangerous :** Every project can have a token just like Bitcoin or Ethereum. Similarly, the name of the Helium token is HNT which is available on exchanges. Investing in HNT, like any other cryptocurrency, may be hazardous. Cryptocurrencies are extremely volatile, which makes them a very riskier asset. The price of HNT has fluctuated a lot in the past, which might be a major disadvantage for certain investors, especially novices. Furthermore, HNT's fees fluctuate a lot, which is also troublesome. The Helium Network & HNT cryptocurrency could still fail, so we should not invest more than we can afford.

Q. 12 Explain Blockchain use cases in Energy and Utilities

Ans. : Blockchain Use Cases in Energy and Utilities

A. Peer-to-Peer Energy Trading

- Peer-to-peer (P2P) energy trading allows consumers to buy and sell surplus energy among themselves. And thanks to distributed ledger technology, blockchain makes this possible by eliminating middlemen, allowing true peer-to-peer exchanges. This reduces the cost of returning excess solar energy to the grid and allows consumers to purchase energy from their neighbors at lower rates than from suppliers.
- To highlight the progress blockchain has made in enabling this new business model, a report by Wood Makenzie shows that 59% of blockchain energy projects are focused on creating horizontal energy markets. row. This means that energy transmission costs can be reduced as they no longer have to be managed from centralized power plants.
- According to Aurora Energy's findings, 41.1% of consumer electricity costs are spent maintaining the infrastructure that delivers electricity from generators to customers' homes. Peer-to-peer commerce eliminates the need to maintain these expensive wires and cables, reducing costs for suppliers and consumers.
- Additionally, since all transactions are public and transparent, consumers can purchase their energy from a known source and support specific local communities if they choose.

B. Renewable Energy Certificates (RECs)

- Another compelling use case can be found for blockchain in terms of energy and sustainability, particularly when it comes to Renewable Energy Certificates (RECs).
- Through the use of an immutable digital ledger secured with encryption, vendors can mitigate fraud, and track and validate REC transactions instantly and automatically.
- This means they can avoid any double energy credit sales, as duplicate transactions are flagged as invalid. In addition, because ledger records provide cryptographic protection that makes them tamper-proof, suppliers can be sure of the source of the energy, allowing them to prove it is sustainable.

C. **Automatic Settlement of Trades**

- Automated settlement of transactions is perhaps one of the most popular ways for all types of energy and utility providers to benefit from blockchain technology. With the ability to eliminate middlemen, vendors can register and settle transactions automatically.
- Transactions can even be done on a peer-to-peer basis through smart contracts and executed between vendors without the need for a clearinghouse or broker, allowing for an approachable approach. more affordable and cost-effective approach. Since smart contracts can automatically trigger transactions and payments not only for financial transactions but also for physical transactions, blockchain use cases in oil and gas, renewable energy and Sustainable energy are also on the rise. And, according to research by EY, the average companies using blockchain in energy and utilities for transaction payments have estimated savings in the range of 30-60%.

D. **Microgrids**

- Blockchain investments in the energy sector are expected to reach more than $5.8 billion by 2025, with microchips playing a leading role in reducing transmission line losses and delaying lifts expensive network. The distributed generation nature of the microgrid provides efficient energy management, uninterruptible supply as well as reliable backup power to prevent outages.

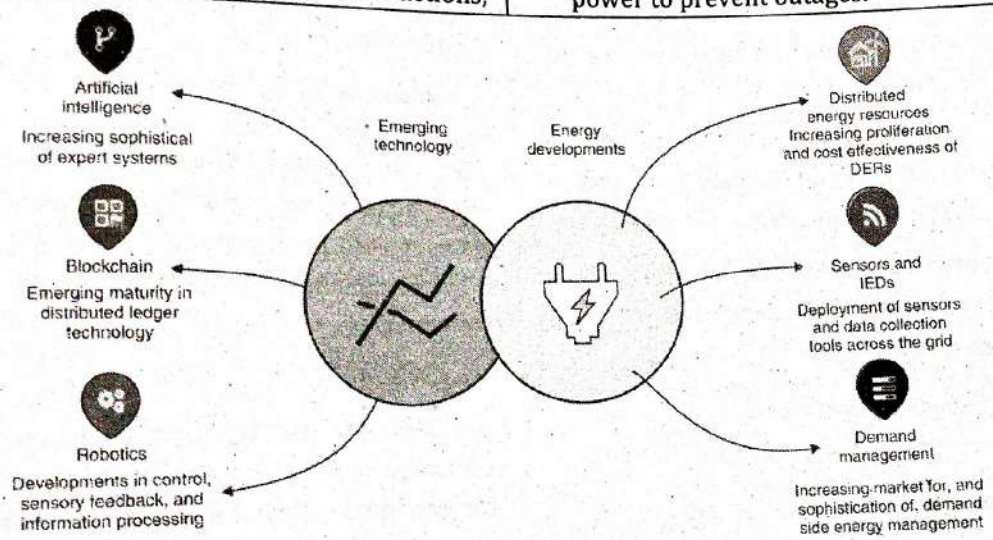


Fig. 6.26 : The 4th Industrial Revolution (4IR) and the Role of Energy

- Blockchain technology provides an efficient way to manage increasingly complex and decentralized transactions between users, from large-scale manufacturers to small retailers, utilities and merchants. This means that households and businesses can transact directly and bypass central authorities, leading to increased efficiency and reduced costs.

E. **Smart Meters**

- Blockchain investments in the energy sector are expected to reach more than $5.8 billion by 2025, with microchips playing a leading role in reducing transmission line losses and delaying lifts of expensive networks. The distributed generation nature of the microgrid provides efficient energy management, uninterruptible supply as well as reliable backup power to prevent outages.
- Blockchain technology provides an efficient way to manage increasingly complex and decentralized transactions between users, from large-scale manufacturers to small retailers, utilities and merchants. This means that households and businesses can transact directly and bypass central authorities, leading to increased efficiency and reduced costs.

Q. 13 Write key benefits of blockchain in energy ?

Ans. : Key Benefits of Blockchain in Energy

- A decrease in the price of utility bills and/or a lower cost in gas or electricity market transaction expenses, which would lessen the demand for working capital.

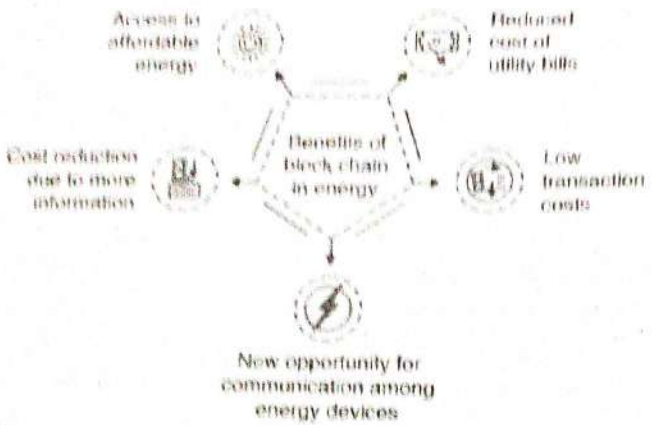


Fig. 6.27 : Benefits of Blockchain in Energy

- There are now more ways for energy equipment like water heaters, electric vehicles, batteries, solar PV systems, and others to communicate with the grid operator (smart grids).
- Cost savings as a result of better knowledge for utilities and grid operators on the grid integration of erratic renewable energy capacity.
- Local and decentralized renewable energy systems provide underprivileged communities with inexpensive energy access.

Q. 14 Explain Energy cryptocurrencies.

Ans. :

Energy Cryptocurrencies

- Renewable energy cryptocurrency attempts to incentivise solar prosumers (those who consume and generate a commodity) by compensating them. It is comparable to how bitcoin encourages miners to contribute processing power to the network by rewarding them with bitcoins for each block of transactions mined.
- The following are some of the cryptocurrencies developed to encourage renewable energy:

1. SolarCoins

SolarCoin, an MIT business, compensates individuals for generating solar energy with an alternative digital money. At the moment, one coin is worth one megawatt-hour of solar energy. SolarCoin, which is now operational in 32 countries, seeks to encourage 97,500 TWhs of worldwide solar energy generation over the next 40 years.

2. M-PAYG

M-PAYG, a Danish business, aims to greatly enhance access to renewable energy for disadvantaged people in developing nations by digitising energy access. The M-PAYG infrastructure includes a prepaid solar energy solution that enables access to solar energy to individuals and families through small-scale mobile money payments. The M-PAYG network uses bitcoins for transactions, and payment contracts are implemented on the blockchain.

3. Coinfy

Coinfy is a blockchain-based payment processing and trading platform that allows for cross-border transactions. Energy trading between off-the-grid solar enterprises and those without access to energy sources has become a possibility in underdeveloped nations due to the low transaction costs associated with blockchain payments.

4. KWHCoin

KWHCoin is a blockchain-based community, ecosystem, and cryptocurrency based on renewable energy units. Physical units of kWh energy are aggregated from multiple sources of origin in this trading system, including smart metres, sensor readings, and green button data. KWH tokens are created by tokenizing this measurable output on the blockchain. In other words, export energy is converted to KWH tokens and transferred to users' digital wallets via The Grid, a peer-to-peer energy trading app. The Grid allows anyone in the world to buy or sell renewable energy resources. KWHCoin will eventually assist the underserved in gaining energy independence.

The platform will allow renewable energy to expand and bring newfound power to the most remote areas by lowering the cost of energy transactions.

□□□