▶ Unit II : Feature Engineering — 07 Hrs.

History, Centralized Vs. Decentralized Systems, Layers of Blockchain : Application Layer, Execution Layer, Semantic Layer, Propagation Layer, Consensus Layer, Why is Block chain important? Limitations of Centralized Systems, Blockchain Adoption So Far. **(Refer Chapter 2)**

End Sem Exam 70 Marks (Unit III, IV, V, VI)

▶ Unit III : Blockchain Platforms and Consensus in Blockchain — 06 Hrs.

Types of Blockchain Platforms : Public, Private and Consortium, Bitcoin, Ethereum, Hyperledger, IoTA, Corda, R3.

Consensus in Blockchain : Consensus Approach, Consensus Elements, Consensus Algorithms, Proof of Work, Byzantine General problem, Proof of Stake, Proof of Elapsed Time, Proof of Activity, Proof of Burn.

(Refer Chapter 3)

▶ Unit IV : Cryptocurrency - Bitcoin, and Token — 06 Hrs.

Introduction, Bitcoin and the Cryptocurrency, Cryptocurrency Basics Types of Cryptocurrency, Cryptocurrency Usage, Cryptowallets : Metamask, Coinbase, Binance. **(Refer Chapter 4)**

▶ Unit V : Blockchain Ethereum Platform using Solidity — 06 Hrs.

What is Ethereum, Types of Ethereum Networks, EVM (Ethereum Virtual Machine), Introduction to smart contracts, Purpose and types of Smart Contracts, Implementing and deploying smart contracts using Solidity, Swarm (Decentralized Storage Platform), Whisper (Decentralized Messaging Platform). **(Refer Chapter 5)**

▶ Unit VI : Blockchain Case Studies — 06 Hrs.

Prominent Blockchain Applications, Retail, Banking and Financial Services, Government Sector, Healthcare, IOT, Energy and Utilities, Blockchain Integration with other Domains. **(Refer Chapter 6)**

❑❑❑

INDEX

In Sem

UNIT I

Chapter 1 : Mathematical Foundation for Blockchain ..... 1-1 to 1-36

UNIT II

Chapter 2 : Feature Engineering ..... 2-1 to 2-42

End Sem

UNIT III

Chapter 3 : Blockchain Platforms and Consensus in Blockchain ..... 3-1 to 3-46

UNIT IV

Chapter 4 : Cryptocurrency - Bitcoin and Token ..... 4-1 to 4-16

UNIT V

Chapter 5 : Blockchain Ethereum Platform using Solidity ..... 5-1 to 5-54

UNIT VI

Chapter 6 : Blockchain Case Studies ..... 6-1 to 6-20

❑❑❑

Unit 3

CHAPTER 3

Blockchain Platforms and Consensus in Blockchain

University Prescribed Syllabus

Types of Blockchain Platforms: Public, Private and Consortium, Bitcoin, Ethereum, Hyperledger, IoTA, Corda, R3. Consensus in Blockchain: Consensus Approach, Consensus Elements, Consensus Algorithms, Proof of Work, Byzantine General problem, Proof of Stake, Proof of Elapsed Time, Proof of Activity, Proof of Burn.

3.1 TYPES OF BLOCKCHAIN PLATFORMS

GQ. Explain how public blockchains ensure the adherence of transaction and block-writing rules. **(6 Marks)**

GQ. Discuss the need for predefined mechanisms and rules to modify a public blockchain's protocols. **(6 Marks)**

GQ. Differentiate between a public/permissionless and a private/permissioned blockchain. **(4 Marks)**

GQ. List down advantages of a private/permissioned blockchain relative to a public/permissionless blockchain for enterprise usage. **(6 Marks)**

GQ. How Assest ownership use case can be implemented with private blockchain? **(6 Marks)**

GQ. Why hybrid blockchain is more suitable for medical application? **(6 Marks)**

GQ. What are the benefits of implementing banking applications with consortium approach? **(6 Marks)**

- Private and public blockchains are the two main types of blockchains. There are, however, a number of variants, including Consortium and Hybrid blockchains.
- Let's first study what characteristics the various blockchain types have in common before going into the specifics of each type. A cluster of nodes operating on a peer-to-peer (P2P) network technology makes up every blockchain.
- Each node in a network maintains a copy of the shared ledger that is promptly updated. Each node has the ability to produce blocks, send or receive transactions, and verify transactions.

Now let's have a look in detail about the four types of blockchains that are possible.

3.1.1 Public Blockchain

GQ. Describe a public blockchain and mention its current applications. **(4 Marks)**

GQ. List down advantages and disadvantages of a public blockchain. **(4 Marks)**

- A distributed ledger system without constraints and permissions is known as a public blockchain. Anyone with internet connection may sign up on a blockchain platform to join the network as an authorised node and become a part of the blockchain.
- It is permitted for a node or user who is a member of the public blockchain to view recent and old data, confirm transactions or complete proof-of-work for an incoming block, and engage in mining.
- The mining and trading of cryptocurrencies is the most fundamental usage of public blockchains. As a result, Bitcoin and Litecoin blockchains are the most widely used public blockchains.

If users adhere to security policies and procedures to the letter, public blockchains are generally secure. However, it is only risky when the participants don't really adhere to the security rules.

Example : Bitcoin, Ethereum, Litecoin

☞ Advantages

(1) Public blockchains have the benefit of being fully independent of organisations; as long as there are computers still connecting to them, the public blockchain will continue to function even if the company that launched it goes out of business. Some blockchains incentivize users to devote computer power to securing the network by offering a reward."

(2) Public blockchains also offer the benefit of a transparent network. Public blockchains are generally safe as long as their users adhere strictly to security regulations and procedures.

☞ Disadvantages

(1) The network may be slow, and companies cannot impose access or use restrictions. According to Godefroy, hackers may unilaterally change a public blockchain network if they control at least 51% of its computer power.

(2) Public blockchains also struggle with scalability. As more nodes join the network, it becomes slower.

Case studies

The mining and exchange of cryptocurrencies like Bitcoin is the most typical use case for public blockchains. It may also be used to electronically notary stamp affidavits and public documents of property ownership in order to create a permanent record with an auditable chain of custody.

For organisations that are based on transparency and trust, like social support networks or non-governmental organisations, this kind of blockchain is appropriate. Private enterprises will probably wish to stay away due to the network's open nature.

3.1.2 Private Blockchain

GQ. Describe a private blockchain and mention its current applications. **(4 Marks)**

GQ. List down advantages and disadvantages of a private/permissioned blockchain. **(4 Marks)**

- A private blockchain is an exclusive, permission-based blockchain that only functions in a closed network.
- Private blockchains are typically utilised inside of businesses or organisations where only a small group of people are allowed to participate in a blockchain network.
- The governing organisation controls the degree of security, authorizations, permissions, and accessibility.
- Therefore, private blockchains are used similarly to public blockchains but have a constrained and tiny network. Private blockchain networks are used for asset ownership, digital identity, supply chain management, voting, and other purposes.
- **Examples** of private blockchains are; Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, etc.

Advantages

(1) Permission levels, security, authorizations, and accessibility are controlled by the governing organisation. For instance, the establishment of a private blockchain network allows an organisation to control which nodes may see, contribute, or modify data. It can also block third parties from accessing particular information.

(2) Public blockchains are more like the internet, whereas private blockchains are like the intranet.

(3) Private blockchains may execute transactions significantly more quickly than public blockchains because of their size restriction.

Disadvantages

(1) Private blockchains have drawbacks, including the contentious assertion that they aren't actual blockchains because decentralisation is the foundation of the technology. Since

centralised nodes decide what is genuine, it is also more challenging to fully create confidence in the information. Less security may also result from the small node count. The consensus process may be compromised if a few nodes act erratically.

(2) Furthermore, the source code from private blockchains is frequently closed-source and proprietary. It cannot be independently audited or verified by users, which may result in inferior security. On a private blockchain, there is no anonymity either.

Case studies

- Private blockchains are the best option when a blockchain has to be cryptographically secure but the governing entity doesn't want the data to be accessible to the general public due to their speed.
- For instance, businesses may decide to utilise blockchain technology without ceding their edge over rivals to outside parties. Private blockchains can be used for auditing and managing trade secrets.
- Other use cases for private blockchain include supply chain management, asset ownership and internal voting.

3.1.3 Consortium Blockchain

GQ. Describe a consortium blockchain and mention its current applications. **(4 Marks)**

GQ. List down advantages and disadvantages of a consortium blockchain. **(4 Marks)**

- A consortium blockchain is a semi-decentralized type in which a network of blockchains is controlled by many organisations.
- Contrary to what we saw with a private blockchain, which is controlled by only one company, this is not the case.
- In this kind of blockchain, many organisations may function as nodes, exchanging data or engaging in mining.
- The typical users of consortium blockchains include financial institutions, governmental bodies, etc.

Examples of consortium blockchain are; Energy Web Foundation, R3, etc.

☞ **Advantages**

(1) Compared to a public blockchain network, a consortium blockchain is typically more reliable, scalable, and effective.

(2) It enables access controls just as private and hybrid blockchain.

☞ **Disadvantages**

(1) Compared to public blockchain, consortium blockchain is less transparent.

(2) The network's operation may still be hampered by the blockchain's own rules if a member node is attacked.

☞ **Case studies**

There are two applications for this kind of blockchain: banking and payments. A consortium made up of many banks can decide which nodes will validate the transactions. Organizations who want to track food as well as research organisations can develop a similar methodology. It's perfect for supply chains, especially those involving food and medicine.

3.1.4 Hybrid Blockchain

GQ. Describe a hybrid blockchain and mention its current applications. **(4 Marks)**

GQ. List down advantages and disadvantages of a hybrid Blockchain. **(4 Marks)**

- A hybrid blockchain combines the features of public and private blockchains.
- It makes use of both the private permission-based system and the public permission-less system features of blockchains. Users may manage who has access to what data stored in the blockchain with the help of such a hybrid network.
- Only a certain subset of the blockchain's data or records may be made public, keeping the remainder secret and confidential.

- As a result of the hybrid blockchain's flexibility, users may quickly join a private blockchain that is connected to many public blockchains.
- A hybrid blockchain's private network is often used to verify a transaction. But users can also release it in the public blockchain to get verified.
- The public blockchains increase the hashing and involve more nodes for verification. This enhances the security and transparency of the blockchain network.

Example of a hybrid blockchain is Dragonchain.

☞ Advantages

(1) Because hybrid blockchain operates in a closed environment, one of its major benefits is that outside hackers are unable to launch a 51 percent attack on the network.

(2) Additionally, it safeguards privacy while allowing for third-party contact.

(3) Compared to a public blockchain network, it has higher scalability and delivers quick and inexpensive transactions.

☞ Disadvantages

(1) This kind of blockchain can have information hidden, so it's not entirely transparent.

(2) There is little incentive for users to take part in or contribute to the network, and upgrading can be difficult.

☞ Case studies

- Real estate is one of the many interesting use cases for hybrid blockchain technology. A hybrid blockchain can be used by businesses to run systems securely while displaying some information, like listings, to the general public. Hybrid blockchain may be used to simplify procedures in the retail sector as well as in highly regulated industries like the banking sector.
- A hybrid blockchain may be used to store medical records. Users may access their information using a smart contract, but random third parties cannot see the data. Governments might also utilise it to securely communicate and keep citizen data among various entities.

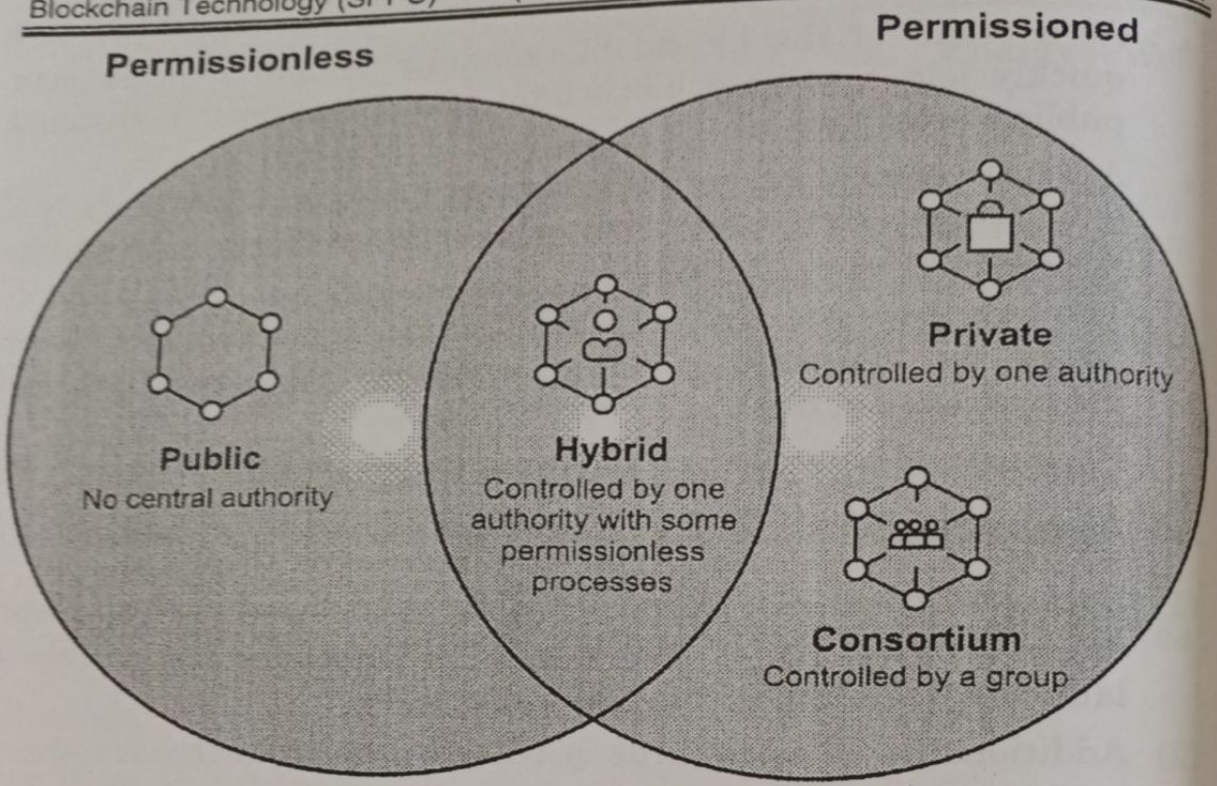


Fig. 3.1.1 : Types of blockchain

☞ **4 main types of blockchain technology**

	Public (permissionless)	Private (permissioned)	Hybrid	Consortium
Advantages	(1) Independence (2) Transparency (3) Trust	(1)Access control (2) Performance	(1) Access control (2) Performance	(1) Access control (2) Scalability (3) Security
Disadvantages	(1) Performance (2) Scalability (3) Security	(1) Trust	(1) Transparency (2) Upgarading	(1) Transparency
Use cases	(1) Cryptocurrency (2) Document validation	(1) Supply chain (2) Asset ownership	(1) Medical records (2) Real estate	(1) Banking (2) Research (3) Supply chain

Fig. 3.1.1 : Comparing different types of blockchains

3.2 BITCOIN

GQ. Write about emergence of bitcoin. (2 Marks)

GQ. How Bitcoin is different from fiat currency? (2 Marks)

- A virtual currency called Bitcoin was created to serve as money and a means of payment independent of any one person, organisation, or entity, eliminating the need for third parties to be involved in financial transactions.
- It is available for purchase on numerous platforms and is given to blockchain miners as reward for their efforts in verifying transactions.

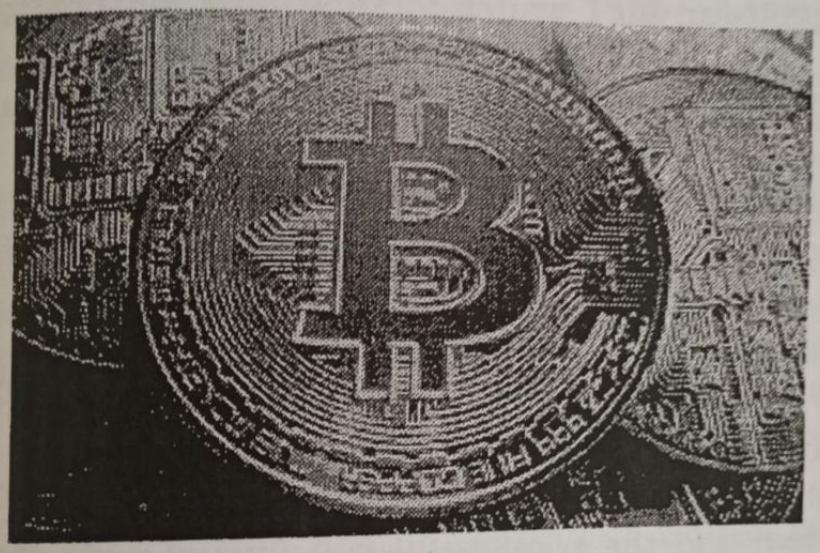


Fig. 3.2.1 : Bitcoin image

- In August 2008, the domain name Bitcoin.org was registered.
- In 2009, a developer or group of developers going by the pseudonym Satoshi Nakamoto released Bitcoin to the general world.
- Since then, it has grown to be the most well-known cryptocurrency worldwide. Many additional cryptocurrencies have been created as a result of its success.
- Block 0 the very first Bitcoin block was mined on January 3, 2009. This is also referred to as the "genesis block" and contains the text: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks," which may serve as both pertinent political commentary and as evidence that the block was mined on or after that date.

- Bitcoin rewards are halved every 210,000 blocks. For instance, in 2009, the block reward was 50 brand-new bitcoins. The third halving took place on May 11, 2020, reducing the reward for finding a block to 6.25 bitcoins.
- The smallest unit of a bitcoin, which is divisible to eight decimal places (100 millionths of a bitcoin), is known as a satoshi.
- If necessary, and if the participating miners accept the change, Bitcoin could eventually be made divisible to even more decimal places.
- Bitcoin, as a form of currency, isn't too complicated to understand. For example, if you own a bitcoin, you can use your cryptocurrency wallet to send smaller portions of that bitcoin as payment for goods or services. However, it becomes very complex when you try to understand how it works.

3.2.1 Blockchain Technology for Bitcoin

- A blockchain and the network needed to power it include cryptocurrency. A distributed ledger, or blockchain, is a shared database that stores data. The blockchain uses encryption to protect the data inside.
- On the blockchain, when a transaction occurs, data from the previous block is transferred to a new block with the new data, encrypted, and the transaction is validated by validators, or miners, in the network.
- A new block is created and a new bitcoin is created and provided as a reward to the miner(s) that validated the data in the block once a transaction has been confirmed, and they are then free to use, hold, or sell the new Bitcoin.
- Bitcoin uses the SHA-256 hashing algorithm to encrypt the data stored in the blocks on the blockchain. Simply explained, a 256-bit hexadecimal integer is used to encrypt transaction data that is stored in a block. That number contains all of the transaction data and information linked to the blocks before that block.
- Transactions are queued up to be verified by network miners. In the Bitcoin blockchain network, many miners simultaneously attempt to validate the same transaction.
- The nonce, a four-byte number contained in the block header

that miners are attempting to solve, is worked on by the mining software and hardware.

- The block header is hashed, or randomly regenerated by a miner repeatedly until it meets a target number specified by the blockchain. The block header is "solved," and a new block is created for more transactions to be encrypted and verified.

3.2.2 Security of Bitcoins

- The US National Security Agency's SHA-256 algorithm provides a framework for the cryptography used by bitcoin.
- It is very difficult to crack this since there are 2256 times as many potential private keys as there are atoms in the universe (estimated to be somewhere between 1078 to 1082).
- Although there have been a number of high-profile instances of bitcoin exchanges being hacked and having money stolen, these firms almost always kept the digital currency for the benefit of their users. In these instances, the website rather than the bitcoin network was compromised.
- Theoretically, an attacker could incorporate a consensus that they controlled all bitcoin into the blockchain if they had control over more than half of the bitcoin nodes now in use. However, this becomes less feasible as the number of nodes increases.
- The fact that bitcoin has no centralised control is a genuine issue. Anyone making a mistake with a transaction on their wallet is therefore helpless.
- There is no one to turn to if you unintentionally transmit bitcoins to the wrong person or forget your password.

3.2.3 Mining for Bitcoin

GQ. How mining process is carried out in Bitcoin? **(4 Marks)**

- The process of mining is what keeps the bitcoin network running and creates new currency.
- Every transaction is broadcast openly on the network, and miners group sizable groups of transactions together into blocks by performing a cryptographic computation that is exceedingly difficult to produce but very straightforward to verify.

- The blockchain is updated when the first miner to solve the subsequent block broadcasts it to the network and is confirmed to be accurate. A quantity of freshly produced bitcoin is subsequently given to the miner as reward.
- The software for bitcoin has a hard limit of 21 million coins. There will never be anything more than that. By the year 2140, all of the coins will be in use. By lowering the size of the rewards, the programme roughly doubles the difficulty of mining bitcoin every four years.
- When bitcoin was originally introduced, even a simple computer could practically instantly mine a coin. Now that it demands rooms full of sophisticated hardware, including highest graphics cards that are skilled at doing the computations, mining can occasionally become more expensive than it is worth due to a fluctuating bitcoin price.
- Fees of varied amounts are added by the sender as an incentive for miners, who also decide which transactions to group into a block.
- These fees will remain as a motivator for mining after all coins have been created. Due to the fact that it supports the Bitcoin network's architecture, this is necessary.

3.2.4 Drawbacks with Bitcoin

GQ. What are the drawbacks of Bitcoin? **(2 Marks)**

- A number of things have been said against bitcoin, including how energy-intensive the mining process is.
- Energy use at the University of Cambridge is tracked by an online calculator, and by the start of 2021, it was projected to use more than 100 terawatt hours year. To put things in context, the UK consumed 304 terawatt hours overall in 2016.
- Critics have pointed out that cryptocurrencies are an ideal tool for conducting black market transactions, and this has led to links between cryptocurrencies and criminal activity.
- In actuality, money has served this purpose for ages, and bitcoin's open ledger may serve as a tool for law enforcement.

3.3 ETHEREUM

GQ. Compare Bitcoin and Ethereum. (4 Marks)
GQ. How Ethereum development took place? (4 Marks)
GQ. Write a short note on DeFi. (2 Marks)
GQ. What is Non fungible tokens? What are its applications? Explain with example. (4 Marks)

- Ethereum is a platform that enables the creation of decentralised apps and organizations as well as asset keeping, trading, and communication.
- You retain control over your own data and what is shared, so using Ethereum doesn't need you to give up all of your personal information.
- Ether, an Ethereum-specific cryptocurrency, is used to pay for some services on the Ethereum network.
- 2013 have seen the creation of Ethereum by programmer VitalikButerin.
- Gavin Wood, Charles Hoskinson, Anthony Di Iorio, and Joseph Lubin were other Ethereum founders.
- Crowdfunding for development work started in 2014, and on July 30, 2015, the network launched. Anyone may publish permanent and unchangeable decentralised applications on Ethereum, allowing users to communicate with them.
- Ethereum is a decentralised blockchain platform that creates a peer-to-peer network for safely executing and validating smart contract application code. Participants can do business with one another using smart contracts without the need for a reliable central authority.

Fig. 3.3.1 : Ethereum

- Participants have complete ownership and visibility over transaction data since transaction records are immutable, verifiable, and securely disseminated across the network.
- Ethereum accounts that users have created both send and receive transactions. As part of the cost of completing transactions on the network, a sender must sign transactions and spend Ether.
- The native Solidity programming language and Ethereum Virtual Machine provide an incredibly versatile platform on which to construct decentralised apps.
- Developers of decentralised applications that use Ethereum to create smart contracts get access to a large ecosystem of developer tools and well-established best practises.
- With wallets like MetaMask, Argent, Rainbow, and others offering simple and direct user interfaces through which to interact with the Ethereum blockchain and the smart contracts deployed there, this maturity also extends to the quality of the user-experience for the average user of Ethereum applications.
- The vast user base of Ethereum encourages programmers to release new apps on the network, thus solidifying Ethereum as the go-to platform for decentralised applications like DeFi and NFTs.

- Future decentralised applications that need higher transaction throughput can be built on a more scalable network using the backwards-compatible Ethereum 2.0 protocol, which is presently being developed.

Decentralized Finance (DeFi)

- Developed on top of blockchain networks, DeFi is a network of financial apps. Because it is open and programmable, runs without a centralised authority, and lets developers to create new models for payments, investing, lending, and trading, it differs from conventional financial networks.
- Customers may quickly create safe decentralised financial apps by utilising distributed networks and smart contracts. DeFi companies, for instance, currently provide goods that make it possible to trade on decentralised exchanges, earn interest on bitcoin holdings, and conduct peer-to-peer lending and borrowing. Compound, Aave, UniSwap, and MakerDAO are a few of the well-known DeFi systems.

Non-Fungible Tokens (NFTs)

- NFTs are one-of-a-kind, indivisible digital tokens that may be used to demonstrate the origin of valuable assets, whether they be digital or physical. NFTs, for instance, can be used by an artist to tokenize their creations and guarantee that they are original and theirs.
- The blockchain network stores and updates the ownership information. Because they enable interoperability between gaming platforms, NFTs are likewise becoming more and more popular in the gaming sector.
- For instance, CryptoKitties, the first NFT project on Ethereum, allowed users to acquire digital cat collectibles backed by NFTs.

Fig. 3.3.2 : Non fungible tokens

- A card game called Gods Unchained uses NFTs to provide players complete ownership of all of their in-game possessions.
- NFTs are gaining popularity as more companies look to tokenize assets and provide users with tamper-proof lineage information about their assets.

3.3.1 Bitcoin Vs Ethereum

Table 3.3.1 : Comparison of Bitcoin and Ethereum

	Bitcoin	Ethereum
Founded	2009	2015
Market dominance	42%	18%
Consensus mechanism	Proof of work	Proof of stake
Block time	10 minutes	12-14 seconds
Max supply	21 million	Unlimited

3.4 HYPERLEDGER

GQ. What type of blockchain is Hyperledger? **(2 Marks)**

GQ. What are different features of Hyperledger? **(4 Marks)**

GQ. Justify how and why Hyperledger is more suitable for enterprise grade applications. **(4 Marks)**

GQ. Compare Hyperledger with Ethereum. **(4 Marks)**

- Providing the necessary framework, rules, guidelines, and tools to construct open-source blockchains and related applications for usage across several sectors, Hyperledger is a global enterprise blockchain initiative.
- Projects from Hyperledger include a range of permissioned blockchain systems that are enterprise, where network users are familiar with one another and have an inherent incentive in taking part in consensus-making.

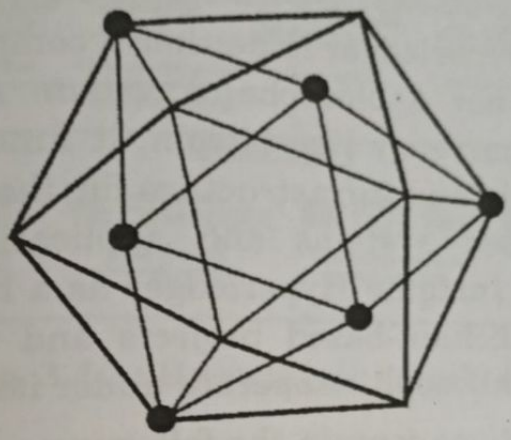


Fig. 3.4.1 : Hyperledger

- A company may implement multiple modular blockchain solutions and services using the parts that are offered under the Hyperledger umbrella to dramatically increase the effectiveness of their operations and business processes.
- The Linux Foundation, which has its headquarters in San Francisco, California, launched the Hyperledger project in December 2015.
- Today, there are more than 120 member companies, up from its initial 30 member companies.
- In order to improve the efficiency, performance, and transactions of different business processes, Hyperledger was established with the goal of speeding up industry-wide collaboration for the development of high-performance and dependable blockchain and distributed ledger-based technological framework.
- Leading companies from the financial, banking, Internet of Things (IoT), supply chain management, manufacturing and production, and technology sectors are part of the global collaboration known as Hyperledger. Big brands like Bosch, Daimler, IBM, Samsung, Microsoft, and Hitachi American

Express, JP Morgan, and Visa, in addition to a host of blockchain-based startups like Blockforce and ConsenSys are among them.

3.4.1 Hyperledger's Organizational Structure

GQ. Draw and explain various components of Hyperledger green house. **(4 Marks)**

In essence, Hyperledger is neither a company nor a network of cryptocurrencies nor a blockchain system. Although it does not support a cryptocurrency like bitcoin, it functions by offering the required standards and infrastructure for the creation of a variety of blockchain-based systems and applications for use in the industrial sector. Imagine Hyperledger as a hub, where numerous independent blockchain-based projects and tools that follow its specified design philosophies operate under its umbrella.

The several initiatives contain the following :

- Hyperledger Fabric is a framework for creating different blockchain-based products, services, and software programmes for commercial usage.
- Fabric has now incorporated Hyperledger Composer, a defunct layer, as well.
- Hyperledger Cello offers an on-demand "as-a-service" deployment mechanism for using blockchain (Blockchain-as-a-Service).
- Hyperledger Explorer is a dashboard utility that allows for the monitoring, searching, and maintenance of blockchain developments and related data.
- Hyperledger Burrow is a permissioned Ethereum smart-contract blockchain node that handles transactions and executes smart contract code on the Ethereum Virtual Machine (EVM).
- Hyperledger Sawtooth is an enterprise-level, permissioned, modular blockchain platform that uses an innovative Proof of Elapsed Time consensus algorithm.

Hyperledger Caliper is a blockchain benchmark tool that is used to evaluate the performance of a specific blockchain implementation.

The Hyperledger Greenhouse

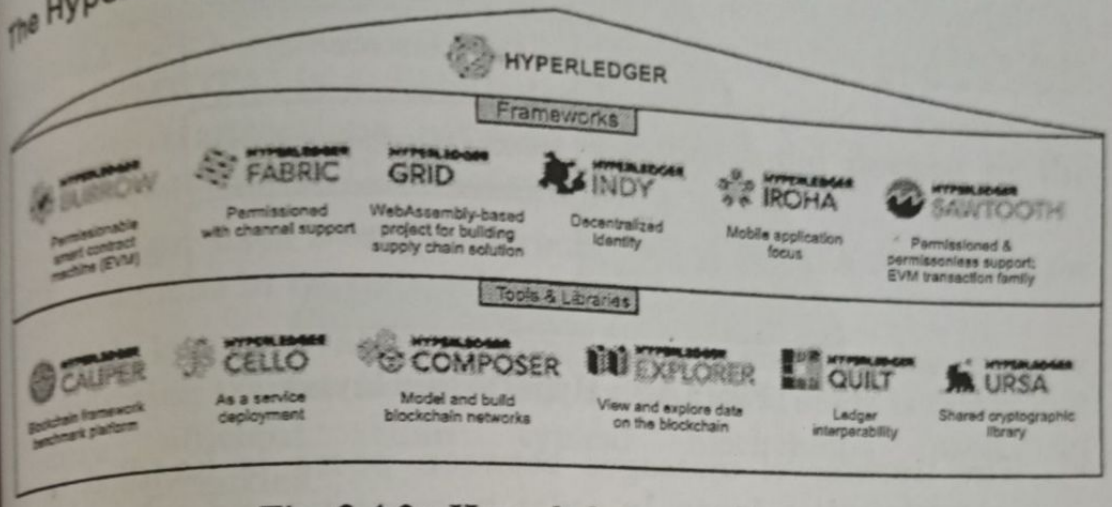


Fig. 3.4.2 : Hyperledger greenhouse

All such projects under the Hyperledger umbrella follow the design methodology that supports a modular and extensible approach, interoperability, and security features. The projects remain agnostic to a particular token or cryptocurrency, though a user can create one as required.

3.4.2 Hyperledger Technology Layers

GQ. What are the layers in Hyperledger architecture? **(4 Marks)**

The primary business elements used by Hyperledger in its architecture are as follows:

The consensus layer is in charge of establishing an understanding of the sequence and validating the accuracy of the collection of transactions that make up a block.

Processing transaction requests and approving only legitimate transactions are the responsibilities of the smart contract layer.

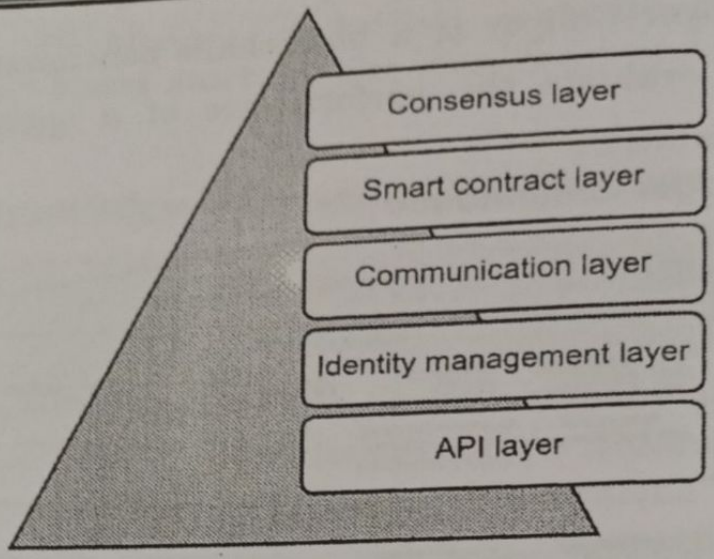


Fig. 3.4.3 : Hyperledger layers

- The transfer of messages between peers is handled by the communication layer. In order to preserve and validate users' and systems' identities and build trust on the blockchain, identity management services are a must.
- Applications and clients from outside sources can connect to the blockchain using the API, or application programming interface.

Table 3.4.1 : Comparison of Ethereum and Hyperledger

	Ethereum	Hyperledger Fabric
Public vs. Private	Public	Private
Permissions	Permissionless	Permissioned
Governance	Decentralized	Federated
Consenus Mechanism	Proof-of-Work	Pluggable BFT
Smart Contract Languages	Solidity, Vyper	Go, Java, Javascript (Node.js)
Private Transactions	No	Yes
Ideal Use Cases	Tokenization (stablecoins, NFTs), DeFi, public transaction settlement	B2B data exchange, transaction settlement, and non-repudiation

3.5 IOTA

GQ. Write a short note on IOTA. (4 Marks)

GQ. State about various issues in current system and how IOTA addresses them? (4 Marks)

- IOTA (MIOTA) is a distributed ledger designed to record and execute transactions between machines and devices in the Internet of Things (IoT) ecosystem.
- The ledger uses a cryptocurrency called MIOTA to account for transactions in its network.
- IOTA's key innovation is Tangle, a system of nodes used for confirming transactions. IOTA claims that Tangle is faster and more efficient than typical blockchains used in cryptocurrencies.
- The IOTA Foundation, the nonprofit foundation responsible for the ledger, has inked agreements with prominent companies, such as Bosch and Volkswagen, to extend the platform's utility among connected devices.

3.5.1 Understanding IOTA

- Billions of devices were connected to the Internet by 2020. Within this Internet of Things (IoT) ecosystem, devices can exchange data and payment information with multiple other devices in transactions conducted throughout the day.
- IOTA wants to replace existing device transaction methods with its own.
- The ledger, according to its creators, serves as a "public permission-less backbone for the Internet of Things that facilitates interoperability between various devices."
- Simply put, this implies that anybody will be able to access it and that it will facilitate transactions between linked devices.
- IOTA's creators assert that it addresses a number of issues that are present in cryptocurrencies created on conventional blockchains.
- These issues include scalability, network speed issues, and the concentration of mining power in the hands of a small number of people.

- Scalability in the context of cryptocurrencies refers to the challenge of increasing the volume of transactions that a blockchain can handle without affecting other metrics.
- Those problems are primarily caused due to a backlog of transactions on Bitcoin's blockchain.
- The backlog itself is due to a variety of reasons, from small block sizes to the difficulty of puzzles that miners must solve to earn the cryptocurrency as a reward.
- IOTA solves these problems by reconfiguring the blockchain architecture into Tangle, a new way of organizing data and confirming transactions.

3.5.2 History of IOTA

GQ. Write about history of IOTA? **(4 Marks)**

- Sergey Ivancheglo, Serguei Popov, David Sønstebø, and Dominik Schiener, who joined later, together co-founded IOTA.
- The project was announced in October 2015 through a post announcing a token sale in an online bitcoin forum.
- IOTA has its origins in the Jinn project. The goal of the project was to create general-purpose processors, or ternary hardware, which is low-cost and energy-efficient technology, for usage in the IoT ecosystem. In September 2014, Jinn performed a crowd sale for its tokens. During the crowd sale, almost 100,000 tokens were sold, bringing in a total of $250,000.
- Because they were advertised as profit-sharing tokens, which may be considered security tokens, the Jinn tokens quickly got into trouble. Initial coin offers (ICOs) were still developing at the time, and it was unclear how regulated they were. A new token sale was performed in 2015, and Jinn was rebranded as IOTA.
- This time, the tokens were advertised as utility tokens. Holders of Jinn tokens might trade them for equivalent tokens under the new system. David Snsteb claimed that because of the Jinn project, IOTA was "spawned," hence introducing IOTA first and Jinn afterwards made sense.
- IOTA's founding transaction was a balance transfer to an address that included all of the MIOTA, the cryptocurrency it uses, that would ever be mined.

- However, according to sources, a screenshot of the genesis transaction has not yet been discovered online.
- Other "founder" addresses received these tokens in distribution. There are 27 quadrillion MIOTAs expected to exist in all.
- The creators of IOTA claim that the total number of MIOTAs "nicely" corresponds to the largest integer value that can be used in JavaScript. During the 2016–2017 bull market, MIOTA attained a high valuation of $14.5 billion three months after making its debut on cryptocurrency exchanges.
- However, like the majority of other cryptocurrencies, its value eventually fell.

3.5.3 Concerns About IOTA

GQ. What are the drawbacks of IOTA ? (4 Marks)

- IOTA has primarily been criticised for its technological flaws. Similar to the majority of cryptocurrencies, IOTA's mechanism is new and untested.
- A phishing assault on its network led to the $3.94 million loss of MIOTA. The IOTA development team published a blog post in reaction to the hack that outlined how to create a secure seed when utilising its cryptocurrency.

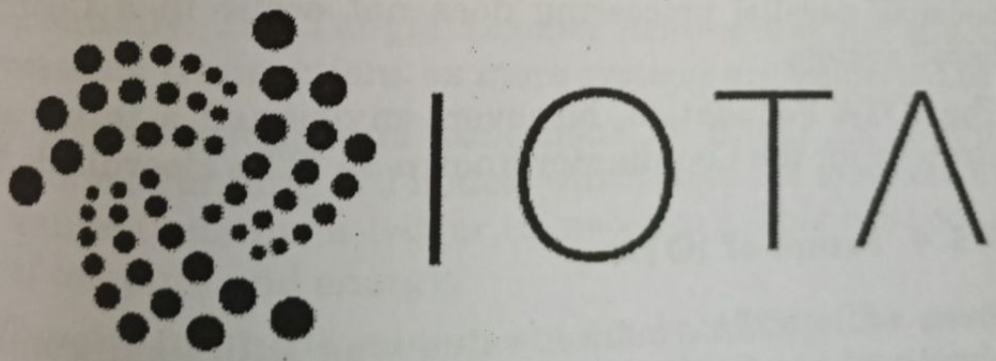


Fig. 3.5.1 : IOTA

- The creators of IOTA are rumoured to have "rolled" their cryptocurrency. In other words, they didn't employ the popular SHA-256 hash function that is used in Bitcoin, instead designing their own encryption technique from scratch. IOTA's Curl hash function has been revealed to have significant vulnerabilities by the researchers at MIT's Digital Currency Initiative.

- When given two alternative inputs, the function yielded the same result. Collision is a characteristic that indicates a malfunctioning hash function.
- The MIT team said that a malicious party may have used their method to damage or steal user cash from Tangle in their investigation of the issue. The flaw has been fixed by the IOTA team.
- There may be flaws with IOTA's claims that the usage of Decentralized Acyclic Graph (DAGs)would solve the scaling challenges that plague blockchains.
- The co-founder of Ethereum, VitalikButerin, has questioned whether hashgraphs, which serve as the foundation for DAG, can address scalability problems. According to him, the problem of a blockchain's dependence on computer memory and processing power is not resolved by the existing iterations of hashgraphs. Hashgraph systems are nevertheless limited in their ability to scale by the power and speed of the individual machines that make up their network.
- In order to guarantee transaction security as of 2020, IOTA's network utilised a central server called a Coordinator. Due to the Coordinator's implementation, a single point of failure has been introduced, undermining the system's claims to be decentralised. It has also slowed down the network's pace because parallel processing does not occur in a Coordinator-based system.
- The IOTA Foundation, however, envisioned a future removal strategy for the Coordinator known as "The Coordicide."

3.5.4 Future of IOTA

- Even while IOTA's market value was still significantly lower than it was in 2017, towards the end of 2020, things appeared to be looking up for this cryptocurrency.
- As of December 19, 2020, it has a market valuation of more over $900 million, up from $446 million at the beginning of 2020.
- That is a gain of more than 100%, but it wasn't an easy route. IOTA stands out from other cryptocurrencies and draws interest from investors because to its ongoing partnerships with major organisations and concentration on the expanding

Internet of Things (IoT). IOTA has a market worth of almost $3.2 billion as of September 28, 2021, so it must be functioning.

3.5.5 How Is IOTA Different From Bitcoin ?

GQ. Compare IOTA with Bitcoin. (4 Marks)

- Several fundamental ideas and topological limitations of a blockchain are eliminated in IOTA as a remedy to Bitcoin's issues.
- The cryptocurrency used by IOTA, MIOTA, is premined, and consensus of transactions happens otherwise than it does on a blockchain. A brand-new data structure called Tangle has been suggested by IOTA developers as a mechanism to arrange numerical representations in a computer's memory.
- Tangle is a nonsequential network of nodes known as a Decentralized Acyclic Graph (DAG). As a result, each node in a Tangle can connect to several other nodes.
- However, they are only linked in one way, therefore a node cannot refer to itself. Because a normal blockchain is a sequential linked set, it is also a DAG.
- However, IOTA's Tangle is a parallel architecture that allows transactions to be handled concurrently rather than sequentially. The Tangle becomes more secure and effective at processing transactions as more systems are connected to it.
- For confirmations and consensus in Bitcoin, a network of computers running full nodes, which store the complete history of transactions for a ledger, is necessary. This method uses a lot of compute and energy.
- In Tangle, full node miners are not necessary. The amount of time and memory required to validate a transaction is decreased by using references to two prior transactions to confirm each new transaction.
- As a last stage, the Proof of Work (PoW) challenge is added to the transaction, which is simple and quick to solve. The two selected transactions are referred to as tips.
- The transaction is approved by the IOTA system using a tip selection mechanism using "confidence" as a parameter. Let's say a deal has already received 97 approvals.

- There is then a 97 95 % confidence that a node will eventually accept it.
- The idea of "confidence" is connected to a transaction's weight. The weight of a transaction increases as it passes through Tangle. The more approvals a deal receives, the more weight it carries.
- A transaction is published to the whole network once it has been confirmed. Once that transaction has been confirmed, another unconfirmed one may select it as one of its tips to confirm itself.
- This method of confirming a transaction results in no fees and low power consumption, enabling MIOTA to be used across a wide variety of devices and machines with different power requirements.

3.6 R3 CORDA

GQ. Enlist and explain essential features of R3 Corda? **(6 Marks)**

- On September 15, 2015, the top financial companies in the world formed the R3 consortium. The consortium has evolved into an ecosystem with more than 300 members now that actively contribute to the field of distributed ledger and blockchain technology.

r3.c·rda

Fig. 3.6.1 : R3 Corda

- R3 made the decision to use blockchain technology to address actual business issues in areas that are both complex and heavily regulated. R3 created a custom blockchain framework they called "Corda" after realising there wasn't one already on the market that could fulfil their needs.
- Corda is an open-source blockchain project that was created with business in mind.

- It lets you create interoperable blockchain networks that carry out transactions in complete secrecy. Smart contract technology from Corda enables direct, valuable commercial transactions.

3.6.1 Differentiating Factors of Corda from Blockchain Framework

Privacy

- Any system using distributed ledger technology must prioritise privacy. It's because your data will inevitably be spread over several nodes and servers that belong to various commercial firms. The only persons with access to a transaction's information in R3's Corda are those participating in the transaction and those who need to confirm the transaction's origin.
- It indicates that two or more people can conduct business together while only disclosing information that is essential.
- This stands in sharp contrast to public blockchain frameworks or certain limited private blockchain frameworks, which broadcast the transaction or its information throughout the whole network.

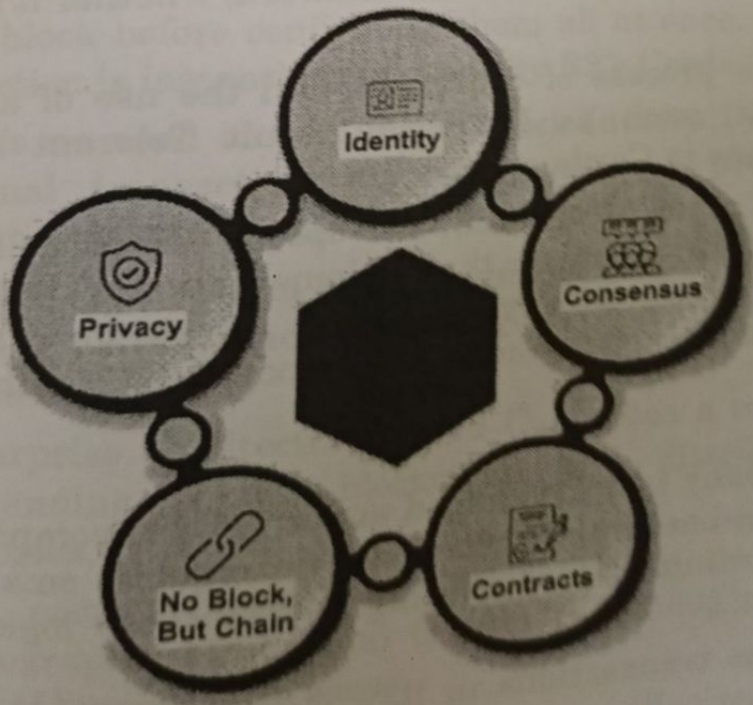


Fig. 3.6.2 : Identity

- Enterprises and corporations would prefer the Corda blockchain framework's privacy feature.Like other comrade frameworks, Corda does not include any gossip protocols which broadcasts all transactions to the network.
- The essential need for creating a closed network of the system among known participants becomes the identification of various parties in the DLT system through a permissioned blockchain.
- Parties can be sure of the members of the blockchain network's identification using R3 Corda. A key component of a global decentralised ledger where you are blind to other players is identity.
- The ability of Corda to assign a single user profile to any legal entity, be it a company or an individual, is made feasible by the KYC requirements of all network members.

Consensus

- Through the use of consensus, organisations on a distributed and decentralised network can come to some agreement about the transactions taking place between them.
- It is critical to know this idea in order to spot fraud and uphold the integrity of any blockchain network, whether it is public or private.
- Through a process of consensus and the use of a variety of algorithms, such as Byzantine Fault Tolerant algorithms, transactions in Corda are confirmed.
- Like any other blockchain, the special characteristics of the Corda network allow for the implementation of several distinct consensus pools employing various algorithms, providing its users with a pluggable consensus model based on their needs.

Contracts

- Any company being managed across several companies over a blockchain-based distributed system requires smart contracts and programme files encoding the business logic and rules validation.
- To process transactions in R3's Corda, all participants must deterministically execute the same code in order to validate the proposed ledger revisions.

- The available languages are high-level and productive, rather than arcane ones like Solidity, just like Ethereum. Examples include Java and Kotlin.
- Only the validation chain of each related transaction is required for the validation function of the CorDapp (Corda Distributed Applications) contract code.

No Block, But Chain

- The UTXO input/output model, which is the foundation of Corda's functionality, is remarkably similar to the transaction structure used in conventional blockchains like Bitcoin.
- However, unlike other commercial blockchain frameworks, such as Hyperledger Fabric, which groups together a number of transactions between "n" participants across the channel into a block based on various criteria, the storage and verification do not result in a chain of blocks.
- In a cryptographically linked (chained) chain, Corda binds each transaction to the transactions it depends on rather than to a prior block comprising a different set of transactions.
- Contrary to other business blockchain solutions described above, Corda does not batch together transactions based on certain criteria on a regular basis and wait for confirmation into a block before confirming them all at once. Instead, each transaction is instantly confirmed by R3's Corda.
- There is no need to wait for a "block interval" or for a lot of additional transactions to follow. As we progress, every transaction is confirmed.
- Corda provides several notaries on the same network, greatly enhancing privacy and facilitating quicker and more efficient transactions.
- An enterprise architecture called Corda has a comprehensive understanding of the blockchain and distributed ledger technologies.
- It is a perfect blockchain platform since it lacks chains or cryptographic blocks. and is versatile enough to fit into a number of business use cases.

3.7 CONSENSUS IN BLOCKCHAIN

GQ. What is Consensus mechanism in blockchain? Enlist different algorithms of consensus. (4 Marks)

GQ. What is the need of consensus in blockchain? (4 Marks)

GQ. What are the goals of consensus mechanism? (2 Marks)

- We see new developments in blockchain technology every day. No matter how hard we work to understand the most recent technologies, there is always something new to learn.
- Have you ever wondered where all these blockchain technology came from? Well, the fundamental building block of this ground-breaking technology is consensus algorithms.
- The blockchain consensus algorithms are what distinguish one blockchain consensus sequence from the others.
- The blockchain network allows infinite numbers of individuals to coexist in the same space.
- Why then do they never conflict with one another or coexist? The answer is in the architecture of the blockchain network.
- The architecture is cleverly designed, and consensus algorithms are at the core of this architecture.

3.7.1 Introduction to Consensus Algorithms

The technical definition would be :

- Consensus algorithms are methods for collective decision-making in which members of the group create and support the decision that will benefit the group as a whole.
- People are required to support the majority decision in this type of resolution, whether they agree with it or not.
- Simply said, it's a way for a group to make decisions. Consider an example to help. Consider a group of 10 individuals who wish to decide on a project that will benefit them all.
- While everyone of them is free to make a suggestion, the one that will best benefit them will likely receive the most support. Whether or not they agreed with the decision, others had to deal with it.

- Now imagine the same thing with thousands of people. Wouldn't that drastically make it way more difficult?
- Consensus algorithms don't only concur with the majority votes, they also agree with one that is advantageous to everyone. Thus, the network constantly benefits.
- Blockchain consensus models are tools for promoting fairness and equality online. A consensus theorem is the name given to the consensus mechanisms that were employed for this agreement. These blockchain consensus models have certain specific goals, like:

(1) **Reaching a consensus** : The method collects as many agreements from the group as it can.

(2) **Collaboration** : Each group strives to reach a deeper understanding that benefits the interests of the group as a whole.

(3) **Cooperation** : Everyone will set aside their personal interests to operate as a team.

(4) **Equal Rights** : Each voter's vote is equally important. This implies that every voter's vote counts.

(5) **Participation :** Every member of the network must take part in the voting process. Nobody will be excluded or able to do so without a vote.

(6) **Activity** : Each group member participates actively. Nobody in the group is more accountable than the others.

- Now that we have a better understanding of the entire network, let's explore into the blockchain technology.
  - It's a novel method of database organisation.
  - can keep track of everything that changes based on the network.
  - The information is organised into blocks of information.
- Therefore, blockchain technology will not implement the decentralisation process; it will simply let you establish a new organised database. Because of this, the blockchain is regarded as the foundation of the whole decentralised network.
- The process is actually fairly easy. The only way to get to an agreement is through these Blockchain consensus models. However, without standard consensus techniques, there cannot be any decentralised system.

- Even whether the nodes trust one another or not won't matter. They will be required to adhere to specific standards and come to a consensus. You must examine each Consensus method to do this.

3.7.2 Different Types of Consensus Algorithms

- Proof-of-Work
- Proof-of-Stake
- Delegated Proof-of-Stake
- Leased Proof-Of-Stake
- Proof of Elapsed Time
- Practical Byzantine Fault Tolerance
- Simplified Byzantine Fault Tolerance
- Delegated Byzantine Fault Tolerance
- Directed Acyclic Graphs
- Proof-of-Activity
- Proof-of-Importance
- Proof-of-Capacity
- Proof-of-Burn
- Proof-of-Weight

Let's explore some of them in detail.

Proof of Work

GQ. Which consensus mechanism is used by Bitcoin and How? **(4 Marks)**

GQ. Describe the process of PoW. **(4 Marks)**

GQ. What are the drawbacks of PoW? **(4 Marks)**

GQ. Explain whether the electrical energy and equipment costs required by PoW are justified. **(4 Marks)**

GQ. Explain what is likely to happen to the PoW mining industry after the most recent halving of bitcoin. **(4 Marks)**

GQ. What is Byzantine Generals problem? How PoW solves it? **(4 Marks)**

GQ. How Bitcoin provides the solution to Byzantine Generals problem? **(4 Marks)**

- The first and original Blockchain algorithm presented to the

blockchain network is proof of work. The algorithm adds a new block to the chain and confirms the transaction.

- In this method, minors (a group of individuals) compete with one another to complete the network transaction. Mining is the process of competing with one another.
- He is rewarded as soon as miners have successfully produced a valid block. Bitcoin is the most well-known application of Proof of Work (PoW). This blockchain consensus mechanism is used by several blockchain technologies to validate all of their transactions and add appropriate blocks to the network chain.
- All of the information pertaining to the blocks is gathered via the decentralised ledger system. However, each transaction block needs to be treated with careful attention.

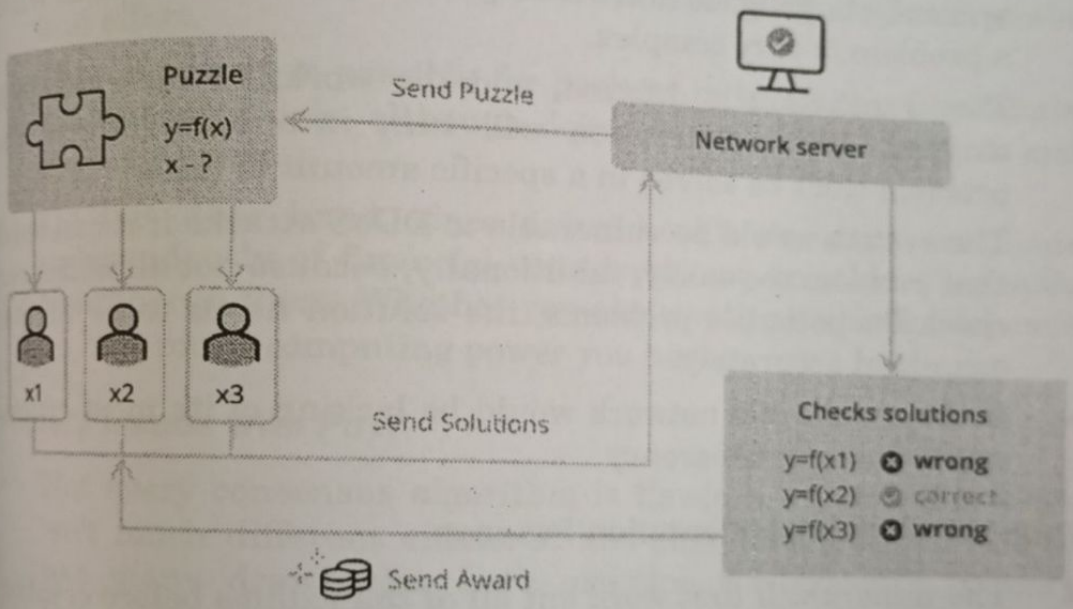


Fig. 3.7.1 : Proof of Work

- Producing proof of work can be a random process with low probability. In this, a lot of **trial and error** is required before a valid proof of work is generated.
- The main idea behind this technology is to readily provide solutions to challenging mathematical problems.
- To begin with, these mathematical problems demand a lot of computational power. For instance, understanding the Hash Function or how to determine the output without knowing the input. Another is integer factorization, which also applies to

crossword puzzles.

- This occurs when the server suspects a DDoS attack, and the consensus mechanisms need a lot of computation to confirm it. The miners are helpful in this situation. The hash is the solution to the entire mathematical equation problem.
- Proof of work, however, has some limitations. The network appears to be expanding rapidly, requiring a lot of processing power. The system's overall sensitivity is rising as a result of this process.

Why Has the System Developed Such Sensitivity?

- Most of the time, the blockchain consensus sequence depends on reliable data and information. But the system's speed is seriously lacking. It takes a long time to produce a block when a problem is very complex.
- The transaction is delayed, and the workflow as a whole is stopped. Block generation will turn into a miracle if the problem can't be solved in a specific amount of time.
- The system would be vulnerable to DDoS attacks if it can solve that problem too easily. Additionally, because not all nodes can check for potential problems, the solution needs to be further examined accurately.
- If they could, the network would be lacking of its most crucial component: transparency.

Proof of Work Implementation Process

- The miners will first work out all of the riddles before creating new blocks and confirming transactions. It's impossible to predict how difficult a problem could be.
- The maximum number of users, the lowest current power, and the network's total load all play a significant role.
- Each new block has a hash function that also contains the hash function from the preceding block. The network therefore offers an additional layer of security and stops any breaches. When a miner completes the problem, a new block is generated and the transaction is confirmed.

Where Exactly Is the Blockchain Proof of Work Consensus Algorithm Used?

- Bitcoin is the most popular one. This particular blockchain consensus algorithm was first introduced by Bitcoin. Based on the total network power, the Blockchain consensus models allowed for any change in the puzzle's level of difficulty.
- The time it takes to make a new block is roughly ten minutes. The same mechanism is also offered by other cryptocurrencies, including Litecoin as a consensus example.
- Ethereum, a platform that uses blockchain technology, employed proof of work in about three to four significant applications. Ethereum, however, has shifted to Proof of stake.
- **Blockchain Technology :** Use Proof of Work because PoW provides DDoS protection and reduces mining stake overall. The blockchain algorithms present a good amount of challenge for hackers. The system requires a lot of computational power and effort.
- This is why it is possible for hackers to break the Blockchain consensus models, although doing so would be expensive and time-consuming.
- On the other hand, since network-wide decisions are made independently of financial considerations, no miners are able to influence them. Whether you can create new blocks depends on how much computing power you have.

Primary issues with PoW

- Not every consensus algorithm is flawless, and proof of work isn't much different either. It has many benefits, but it also has many drawbacks. Let's examine the system's primary flaws.
- Greater Energy Consumption The blockchain network is made up of millions and millions of specially built microchips that continually hash data.
- Currently, Bitcoin delivers 20 billion hashes per second. The network's miners hash data using a special type of microprocessor.
- This process gives the network an additional layer of defence against botnet attacks.
- The proof-of-work-based blockchain network's high degree of security consumes a lot of energy. In a world where energy is getting scarcer, the increased consumption is becoming an

issue. Miners on the system must pay a significant amount of money owing to power use. The best solution to this problem would be a cheap source of energy.

Centralization of Miners

- With the energy shortage, the focus will shift to less expensive electricity-related solutions. However, if a bitcoin miner-manufacturer rises, it would be the biggest issue.
- The manufacturer has a certain amount of time before becoming more power-hungry and attempting to introduce additional rules into the mining system.
- The decentralised network will become centralised as a result of this circumstance. This makes it yet another significant issue that these Blockchain algorithms are confronting.
- The 51% Attack
- This attack might result in the majority of users being under control and the majority of the mining power being captured.
- In this case, the attackers would have complete control over the network. They can stop other people from generating new blocks. Attackers can also receive rewards based on their tactics.
- Imagine that X is using the blockchain network to transfer Y some bitcoin. Y is not a part of the attack, but X is.
- The transaction is completed, but the attackers prevent any currency from being transmitted by forking the chain.
- In other cases, the miners will join in a particular branch. On certain blocks, they will have the highest processing power combined.
- Other blocks with a shorter life are thus excluded. Therefore, Y won't get the money.
- This isn't a profitable solution, though. After the incident is widely publicised, a lot of mining power will be consumed, people will start to leave the network, and gradually the cost of trade will decrease.

The Byzantine Generals Problem

- Game theory's "Byzantine Generals Problem" identifies the

challenges decentralised parties have in reaching consensus without the help of a reliable central authority.

- How can members of a network agree on a certain truth when no member has access to other members' identities?
- The Byzantine Generals analogue in game theory . The problem is that Byzantium city is under attack by multiple generals.
- They have encircled the city, but they must determine when to launch an attack as a group.
- They will succeed if every general launches an attack at once, but they will fail if each general launches an attack independently.
- The generals are unable to communicate securely with one another since Byzantium's defenders might intercept or falsifiably broadcast any signals they send or receive. How can the generals organize to attack at the same time?

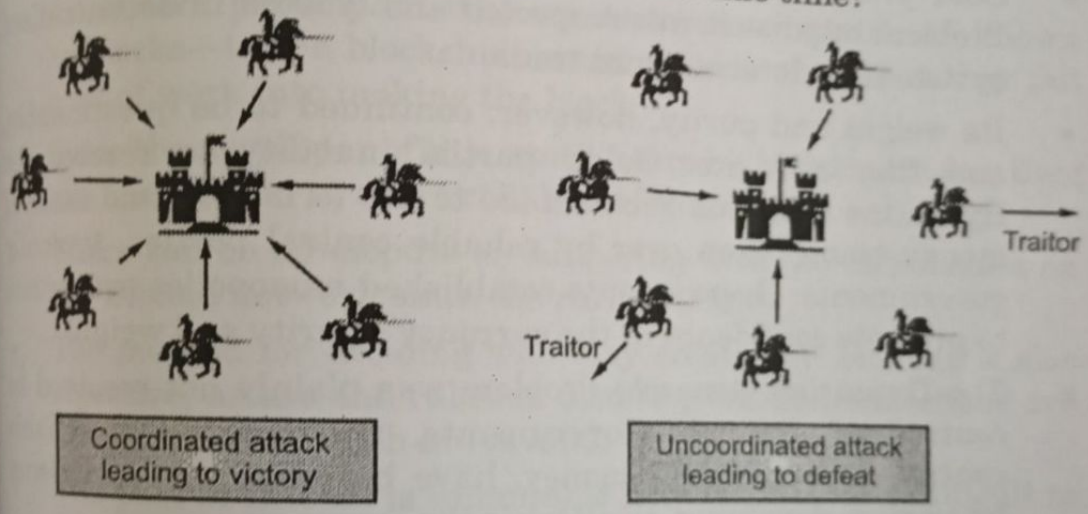


Fig. 3.7.2

- Only decentralised systems are prone to the Byzantine Generals problem because they lack a reliable information source and a mechanism to validate the data they gather from other members of the network.
- In centralised systems, it is assumed that a central authority would publish accurate information and guard against the network's spread of incorrect or fraudulent information.
- For instance, in the conventional financial system, banks are relied upon to accurately report to customers their balances and transaction histories. A central bank or government is

trusted to restore trust if a bank does seek to lie to or cheat its consumers.

- The Byzantine Generals problem, which demands that truth be verified in an unreliable manner, cannot be solved by centralised systems.
- Instead, they decide not to face the issue at all and sacrifice efficiency for trustlessness. The central government may corrupt centralised systems, though.

The Problem of the Byzantine Generals and Money

- A great example of the Byzantine Generals Problem is money. How can a community create a kind of payment that all members can rely on and accept? For a considerable part of history, communities have chosen to use uncommon items like shells or glass beads or precious metals as currency.
- Gold provided a partial solution to the Byzantine Generals Problem because it was respected and trusted in decentralised systems like international trade.
- Its weight and purity, however, continued to be questionable, and they still are. Gold's partial inability to resolve the Byzantine Generals Problem led to the formation and issue of money being taken over by reliable central parties, typically governments. Governments established monopolies over mints to promote confidence in the currency's purity and weight.
- The Byzantine Generals Problem was plainly not resolved by centralised systems. Governments, the apparently reliable central authorities for money, have betrayed that confidence by seizing, devaluing, or altering the currency.
- A money would need to be verifiable, untraceable, and counterfeit-resistant in order to solve the Byzantine Generals Problem. This accomplishment was not made until the creation of Bitcoin.

How Bitcoin Solves the Byzantine Generals Problem?

- Bitcoin was the first realized solution to the Byzantine Generals Problem with respect to money.
- Prior to Bitcoin, a number of initiatives and programmes that aimed to produce money independent of the government all ended in failure.

Blockchain Addresses the Issue of Double Spend

- Bitcoin required a mechanism to control ownership and avoid double spending in order to function as a currency. Bitcoin employs a blockchain, a public, distributed ledger that records a history of all transactions.
- The blockchain is the truth that all parties must agree upon in the Byzantine Generals analogy.
- They might construct a working, trustless currency without a centralised authority if all nodes, or participants of the Bitcoin network, could agree on which transactions took place and in what sequence.

Proof-of-Work Solves the Byzantine Generals Problem

- By employing a Proof-of-Work method to provide a clear, objective set of rules for the blockchain, Bitcoin was able to resolve the Byzantine Generals Problem.
- A network participant who wants to contribute data—known as blocks—to the blockchain must provide proof that they put a lot of work into making the block.
- Since the developer of this work incurs high expenditures, they are encouraged to share reliable information.
- There can be no dispute or tampering with the information on the Bitcoin network since the rules are fair.
- The method for deciding who may create new bitcoins is also objective, as are the rulesets dictating which transactions are acceptable and which are invalid.
- The past of Bitcoin is immutable because it is very difficult to remove a block after it has been added to the network.
- Members of the Bitcoin network may therefore always agree on the blockchain's current status and all of its transactions. Each node independently confirms the validity of blocks based on the Proof-of-Work requirement and transactions depending on additional criteria.
- All nodes on the network will instantly identify fraudulent information as objectively incorrect and ignore it if any member of the network tries to broadcast it.
- Bitcoin is a trustless system because each node can independently validate all data on the network, eliminating the need to rely on other users.

Proof of Stake

GQ. How Proof of Stake algorithm works? (4 Marks)
GQ. Q. What is the need of PoS? (4 Marks)
GQ. How PoS overcomes the drawbacks of PoW? (4 Marks)
GQ. How PoS addresses 51% attack issue? (4 Marks)
GQ. What are the drawbacks of PoS? (4 Marks)
GQ. Enlist and explain benefits of PoS. (4 Marks)
GQ. What is Delegated PoS? (4 Marks)
GQ. Discuss whether business owners are likely to be comfortable with a Proof-of-Stake (PoS) blockchain. (6 Marks)

- A consensus algorithm called proof of stake addresses the key problems with the proof-of-work algorithm.
- This one requires each block to be validated before the network can add it to the blockchain ledger.
- This one has a small amount of Twist. Miners may participate in the mining process by staking their currency.
- A novel idea called proof of stake allows each participant to mine or even validate brand-new blocks solely based on their currency holdings. Therefore, in this case, having more coins increases your chances.
- The minors in this consensus process are preselected.
- Even if the process is completely random, not all minors are allowed to take part in the staking.
- The network's miners are all selected at random. You will be eligible to join the network as a node if you have a certain number of coins already held in your wallet.
- You must deposit a particular quantity of currency after becoming a node in order to be eligible to become a miner.
- The validators will then be chosen via a vote mechanism. At the conclusion of the process, the miners will stake the minimum amount needed for the unique wallet staking.
- Actually, the procedure is fairly easy. According to the wallet, new blocks will be generated in direct proportion to the quantity of currencies. For instance, if you own 10% of the coins, you may mine 10% of the new blocks.
- A number of proof of stake consensus algorithms are used by

various blockchain technologies.

- However, all algorithms function identically while mining new blocks. Each miner will get a share of the transaction fees in addition to the block reward.

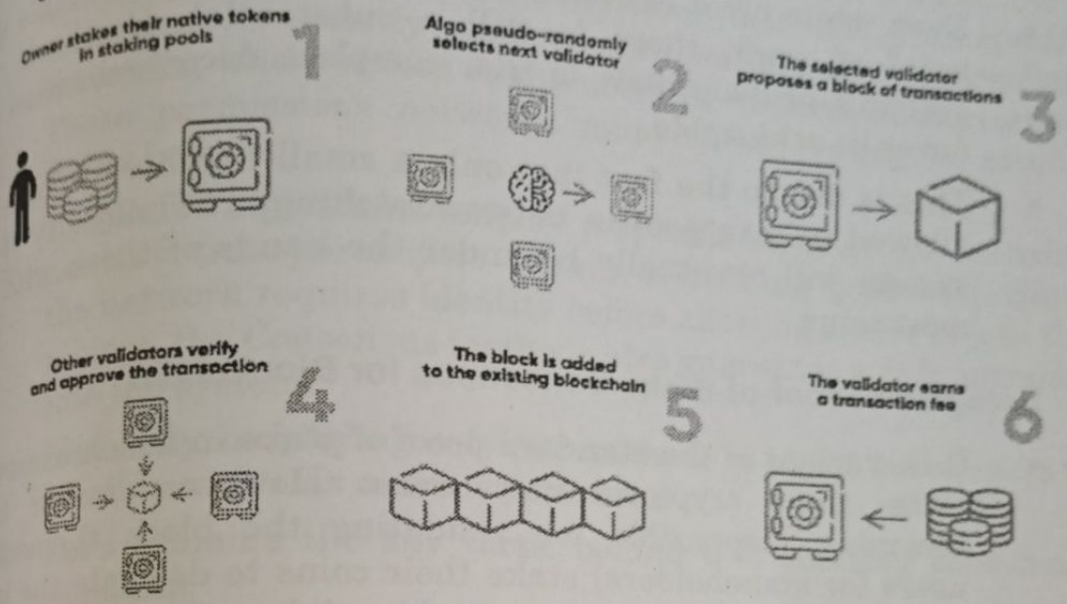


Fig. 3.7.3 : Proof of Stake

How Does The Proof of Stake Pooling Work?

- There are many methods to participate in stacking. You can join a pool and make profit there if the stake amount is too high. Two methods exist for doing it.
- You can first loan your currency to another user who will join the pool and share the profits with you. To stake with, you'll need to try and locate a trustworthy partner.
- Joining the pool is another option. By doing this, the profit from that particular pool will be divided among all participants according to the amount staked.

Benefits as Proof of Stake

- First off, these consensus methods don't need a lot of powerful hardware support. All you need is a working computer and a steady internet connection. Transactions may be confirmed by anybody with sufficient coins on the network.
- A network investment won't lose value over time as other investments do. Only changes in pricing will have an impact on the profit. The blockchain's proof of stake consensus process

uses substantially less energy than proof of work. It doesn't even require a lot of electricity.

Additionally, it lessens the risk of a 51% attack.

- Even while proof of stake appears to be more profitable than proof of work, there is still a substantial drawback. The system's primary flaw is that complete decentralisation will never be achievable.
- This is due to the fact that only a small number of nodes are allowed to take part in network staking. The majority of the system will eventually be under the hands of those with the most coins.

Delegated Proof-of-Stake Consensus for Blockchain

- It is variant of the standard proof of stake in which users still stake their cryptocurrency coins. However, rather than becoming responsible for validating the block themselves, users (or stakeholders) stake their coins to delegate the work by voting on the node that would validate the block on their behalf.
- Thus the consensus mechanism got its name "Delegated Proof of Stake". Once the nodes have been elected, they're responsible for reaching a consensus between themselves to validate transactions and add blocks to the Blockchain.
- The technology is highly reliable and gives the entire process an additional level of flexibility.
- Delegated Proof of Stake is the ideal option if you want quick, effective, decentralised consensus mechanisms.
- Here, the stakeholders' problem is entirely resolved in a democratic manner. Every element in the network has the ability to act as a delegate.
- Here, the nodes are referred to as delegates rather than miners or validators.
- This technology can complete a transaction in less than one second by working out block production! Additionally, this system was created to guarantee the highest level of protection against regulatory issues.

☞ Proof of Elapsed Time (PoET)

GQ. What is proof of elapsed time? How it works ? **(6 Marks)**

GQ. What Blockchains use proof of elapsed time? (2 Marks)

GQ. What is an advantage of using consensus algorithm proof of elapsed time PoET instead of proof PoW? (4 Marks)

- One of the top consensus algorithms is PoET. This specific technique is mostly utilised in permissioned blockchain networks, where access to the network requires authorization. These permissions networks must choose voting or mining rights policies.
- The PoET algorithms employ a specific strategy for ensuring network transparency to ensure everything goes well. Since the network requires identity before allowing a user to join the miners, the Consensus methods also guarantee a safe entrance into the system.
- Naturally, employing only fair methods to select the winners is possible with this consensus process.
- Let's examine the key tactic behind this amazing consensus sequence.
- Every user on the network needs to wait for a certain duration of time, but this time limitation is pretty arbitrary.
- The participant who has completed their fair share of waiting time will be allowed to add a new block to the ledger.
- The programme must take into account two things in order to defend these cases.
  - Whether the winner made the random number selection initially?
- He or she might pick an arbitrary little period and win the game first.
  - Did the person actually wait the allotted amount of time?
- PoET is dependent on a unique CPU requirement. It is referred to as the Intel Software Guard Extension. This Software Guard Extension supports the network's use of unique codes.
- PoET uses this system and makes sure the winning is purely fair.

Proof-of-Activity

GQ. What is Proof of Activity? How it functions? (4 Marks)

GQ. How PoA deals with 51% Attack issue? **(4 Marks)**

GQ. What are the drawbacks of PoA? **(4 Marks)**

- The Litecoin founder and three other authors had a wonderful idea while people were arguing the issue of Proof-of-Work vs. Proof-of-Stake.
- They posed a straightforward query to the world: Why can't the PoW and PoS be combined rather than opposed against one another?
- As a result, the interesting hybrid concept known as Proof-of-Activity was born. It combines the finest two qualities, making it less power-hungry and more secure against attacks.

The Function of Proof-of-Activity

- The mining process begins with the Proof-of-Activity blockchain consensus mechanism in the same way as it does with the PoW algorithm. For a prize, the miners must solve a complicated puzzle.
- So where is PoW's main difference? In a PoW network, miners create blocks with a completed transaction.
- Miners only mine the block templates in Proof-of-Activity. These templates contain two elements: the header data and the reward address for the miners.
- When these block templates are mined by the miners, the system switches to the Proof-of-Stakes algorithm.
- A block's header information identifies a random stakeholder. The pre-mined blocks are then validated by these parties.
- A validator's probability to confirm a block rises with the amount of stack they currently possess. That specific block enters the blockchain only after being validated.
- The best of the two consensus algorithms is utilised in this manner by Proof-of-Activity to validate and add a block to the blockchain. Additionally, the network shares the transaction fees fairly across the validators and miners.
- Thus the system acts against the "tragedy of the commons" and creates a better solution for block validation.

The Effects of Proof of Activity

- The 51 % attack is one of the main challenges a blockchain

must deal with. The likelihood of the 51 percent attack is nil according to the consensus theory.

- It occurs because neither the miners nor the validators can command a majority since adding a block to the network requires an equal contribution from both groups.
- The Proof-of-Activity blockchain consensus mechanism, however, is said to have serious faults by some critics.
- The mining function will result in a significant increase in energy usage like the first one.
- Second, there is no way to prevent the validators from signing their own work twice using Proof-of-Activity. The consensus theorem is somewhat put on the back foot as a result of these two key shortcomings.
- Two popular blockchains adopt the Proof-of-Activity – Decred and Espers. Still, they have some variations. In reality, Decred is getting considered as the more popular one than the Espers consensus theorem.

Proof-of-Burn

GQ. Write a shot note on Proof of Burn. (4 Marks)
GQ. What is Eater address in Proof of Burn? (2 Marks)
GQ. What are the pros and cons of Proof of Burn? (4 Marks)

- Impressively, this consensus sequence is pretty good. Some of the coins will be burned to protect the PoW cryptocurrency! A few coins are sent to a "Eater Address" by the miners, which triggers the process.
- These coins cannot be used in any way by the Eater Addresses. Since the burned coins are recorded in a ledger, they are actually unusable as currency. Additionally, the person who burned the money will receive a reward.
- The burning is indeed a loss. However, the harm is just momentary because the procedure will eventually protect the coins against hackers and their cyber-attacks.
- Additionally, the process of burning raises the stakes of the substitute coins.
- In such a case, a user is more likely to mine the future block

and will receive more rewards in the future. Burning may therefore be utilised as a mining privilege.

- A cryptocurrency that makes use of this blockchain consensus protocol is the counterparty, which is a great example of consensus.

The Eater Address

- Users transfer bitcoin to the Eater Addresses to burn them. A private key is not associated with an Eater Address.
- Therefore, no user will ever be able to access these addresses to use the coins stored there. Additionally, these addresses are created randomly.
- Although these coins are unavailable or "gone forever (!)," they are nonetheless included as part of the supply and given the burned label. The Advantages and Disadvantages of Proof-of-Burn Algorithm
- The main intent for burning the coins is to increase stability. We are aware that long-term gamers frequently keep coins for a very long period in order to benefit.
- By providing more stable currency and long-term commitment, the system benefits those long-term investors. Additionally, this improves decentralisation and develops a more evenly distributed network.
- But no matter how you look at the situation, burning coins is wasteful! Even some eater addresses contain Bitcoins worth more over $100,000. There is no way to get the money back; they lose everything.

Chapter Ends...

❑❑❑

Unit 4

CHAPTER 4

Cryptocurrency - Bitcoin and Token

University Prescribed Syllabus

Introduction, Bitcoin and the Cryptocurrency, Cryptocurrency Basics Types of Cryptocurrency, Cryptocurrency Usage, Cryptowallets: Metamask, Coinbase, Binance.

4.1 INTRODUCTION TO CRYPTOCURRENCY

GQ. What is Cryptocurrency ? Explain in brief.

- Cryptocurrency is a kind of digital asset that enables safe transactions using distributed ledger, or blockchain, technology.
- Despite the widespread misunderstanding of the technology, several central banks are considering introducing their own domestic cryptocurrency.
- Since 1998, the concept of "cryptocurrencies" has been discussed.
- B-Money and Bit Gold were the first known attempts to create a digital cryptocurrency, but neither proved successful.
- Digital or virtual currencies that operate on cryptographic principles are known as cryptocurrencies.
- As implied by the name, they are not substantial or have no actual presence.

- They are essentially a collection of computer programming codes,but offers greater usefulness and security than many current currencies.
- Blockchain technology, which we have previously studied in earlier chapters, is the foundation of cryptocurrency.
- In the case of cryptocurrencies, the ledger records all transactions made and created using those currencies on the network. Each user on a certain blockchain will have a distinct account Id or address. Currency is Debited and Credited to this account.
- These accounts are constantly connected to the cryptocurrency.
- Wallets, an application, allows users to manage their accounts.
- Both the sender and the recipient need to have accounts. Anyone on the network may transact with anyone else using their wallets.
- Nodes verify the transactions, which are then recorded on the blockchain ledger. Therefore, the unchangeable and encrypted blockchain record serves as the foundation of bitcoin.
- The encryption system, peer-to-peer network, and lack of a central authority or central server to govern are other important characteristics of blockchain that are also relevant to cryptocurrencies.
- Each cryptocurrency will use a blockchain system to operate.
- Bitcoin, which uses the bitcoin blockchain, is one of the most well-known cryptocurrencies.
- Another cryptocurrency that is quickly expanding and uses the Ethereum protocol is ether.
- In compare to conventional currencies, cryptocurrencies provide participants a very high level of anonymity.
- A user's account ID will be the only part of his identification that may be seen; everything else will be encrypted.The true identify of a user will not be known to the participants.
- There are various benefits and drawbacks to cryptocurrencies.
- The current cryptocurrency market is highly competitive and fragmented. Experts identifiedmore factors that will determinate and rise the attractiveness and confidence in using cryptocurrency.

The cryptocurrencies should be:

(1) Cost effective to issue
(2) Available immediately
(3) Governed and regulated
(4) Instantly liquid—liquidity should be instantly generated or generated
(5) on demand
(6) Secure and immutable—cannot be double spent
(7) Trusted—backed by a lender of last resort (e.g. a central bank)
(8) Free from fractional reserve banking in its crypto-form
(9) Transparent with transaction finality (directly or remotely)
(10) Add purpose to economic activity (commerce) and have sustainable value
(11) Have standards to enable interoperability
(12) Be legitimate—a competent authority to impose these standards

4.2 BENEFITS OF CRYPTOCURRENCY

GQ. State and explain the advantages of cryptocurrency.

(1) Compared to current banking systems, cryptocurrencies allow extremely quick transactions. A transaction may be validated in Bitcoin in as little as 10 minutes, while it takes Ethereum roughly 10 seconds.

(2) Transactions performed using cryptocurrencies are completely anonymous; neither the person who made the transaction nor the recipient can be determined. Only the sender's and receiver's network addresses will be used by the participants. These participants' identities won't be made public on the shared ledger.

(3) There are no payment restrictions. Transactions are not subject to any limitations. The user is able to send money at any moment, from any location to any location. No time restrictions, such as bank holidays, apply.

(4) The majority of bitcoin transactions are free. Or the fee is significantly lower than the current fees for banking transactions. Anyone may conduct transactions in bitcoin without having to pay any transaction fees. In order to expedite their transaction, the user may also choose to charge transaction fees. In other words, if someone pays a transaction fee, more miners will arrive to validate the transaction, which speeds up the process.

(5) Cryptocurrencies are among the safest payment methods on the market right now. It possesses the "unchanging" quality, which means that if a blockchain-based cryptocurrency transaction has already taken place, it cannot be undone. Therefore, the likelihood of fraudulent transactions is quite low.

(6) Most cryptocurrencies operate on a decentralised network, and their exchange rates are dynamically determined by supply and demand variables. Such autonomous cryptocurrencies cannot be stopped by by government law or other means. A government's sole option is to limit the currency's ability to be converted into regular money. They are unable to halt cryptocurrency transactions, though.

(7) Transactions using cryptocurrencies do not require the use of a user's identify. All additional information is securely scrambled and will only be used to access the wallet addresses of the sender and recipient. No personal information will be given to the recipient of a cryptocurrency when it is sent to another person or organisation. Between two accounts, just the sum of bitcoin will be transferred.

(8) Most cryptocurrencies have a set quantity of currency in their exchequer, hence there is no inflation. It is 21 million in the case of bitcoin. There won't be any fresh bitcoins after the entire item has been mined. Therefore, depreciation is not a possibility.

(9) Immediate asset availability - the cryptocurrency will be available immediately for consumersand businesses to spend, without any waiting period.

(10) Immediate access to liquidity - the cryptocurrency will be highly liquid-liquidity generatedinstantly on demand.

(11) Free up working capital - the need for banks to hold reserves will be minimized as themoney held for use as reserves will be available for other purposes thus optimizing intradayliquidity.

(12) Transaction efficiency - cryptocurrency transactions are fast and immediate-they improve efficiency by cutting out the middle man and avoiding lengthy back-office reconciliation processes.

(13) Transaction security - central bank-issued cryptocurrency transactions can be tracked protecting security. Security is also enhanced as there is no double spending.

(14) Over and above these benefits, a central bank-issued cryptocurrency can have a much larger impact on the wider economy and for all market participants because it can :

(15) Boost economic growth-a central bank issued cryptocurrency can permanently boost economic growth.

(16) Act as an enabler for mobile and digital commerce-it can replace current immediate payment models by delivering the currency into the market in a more immediate, efficient and effective manner.

(17) Ensure stability in the financial system-a cryptocurrency can help maintain financial stability and provide policy makers with more effective tools to smooth out financial booms and busts. In periods of high inflation for fiat currencies, banks can hold cryptocurrencies, thus protecting their wealth.

(18) Work as a crypto-reserve currency-commercial banks can keep a portion of their reserves in cryptocurrency rather than in fiat currency, thus complementing the fractional reservebanking system.

(19) Effectively monitor the supply of money-a central bank issued cryptocurrency can help policy makers control the amount of money in the economy, as well as the supply of the cryptocurrency. This is currently not possible as banks create money by using deposits as loans.

(20) Lower costs-crypto currencies will enable the banking system to cut the costs of banknote issuance, circulation and handling. In addition, transaction costs will be significantly reduced especially for cross border transactions.

(21)Allow for traceability-transactions in central bank issued cryptocurrencies can be tracked, and simultaneously ensure that the users information remains protected, thus protecting privacy. A central bank issued currency follows KYB and KYC procedures which will allow the central bank to identify users when there is a need to.

4.3 DRAWBACKS OF CRYPTOCURRENCY

GQ. State and explain the disadvantages of cryptocurrency.

(1) Despite the fact that demand for "cryptocurrency" is rapidly rising, several governments have not officially endorsed transactions involving "cryptocurrency." And currently, only a few select domains are allowed to use it. Additionally, the general public is still a long way from adopting "cryptocurrencies."

(2) Variable rate might be viewed as either a benefit or a drawback. Although the exchange rate of cryptocurrencies is determined by a rigorous demand-supply law, current market patterns point to an unusual increase in that rate, particularly for Bitcoin. However, it is anticipated to return to its regular speed very shortly.

(3) Governments cannot regulate cryptocurrencies, but they may ban them and make transactions involving them unlawful. It inevitably cast a shadow on such bold, unrestrained gestures.

(4) Money launderers and the black market are drawn to cryptocurrencies because of their anonymity. Misuses are repeatedly reported since the identity is kept a secret. Undoubtedly, the potential of cryptocurrencies may be utilised to create a more transparent economic system, but before making such significant advancements, security concerns and loopholes must be addressed. We may anticipate a fully authorised cryptocurrency-based economic system in the near future since a prospective technology like this cannot be completely prevented.

(5) As the majority of cryptocurrencies lack a centralised administration, it is everyone's responsibility to keep their

account secure. Nobody can assist whomever loses the wallet key in obtaining it again.

(6) Since there are often only a finite quantity of cryptocurrencies, the supply and demand essentially determines how much they are worth. Deflation is more likely to occur in cryptocurrencies than in any other type of economic system since most of them only have a set number of units.In the case of bitcoin, if someone retains the cryptocurrency for a long period, the supply will decline while the demand rises, which would result in deflation.

4.4 INTRODUCTION TO BITCOIN

GQ. What is Bitcoin? Describe how it works.

- The first blockchain implementation in the world and the first cryptocurrency is Bitcoin.
- We have covered the definition of cryptocurrency. Let's get a bit more into the subject with the most well-known cryptocurrency, Bitcoin, in this part.
- Satoshi Nakamoto created bitcoin in 2009 using the conceptual framework proposed by certain scholars in the late 1990s.
- It does have a P2P shared network, distributed ledgers, and data that is cryptographically secured, exactly like a traditional blockchain.

4.4.1 Working of Bitcoin

- Using Bitcoin is easy; we do not need any programming expertise or technological understanding.
- The first step is to register for a Bitcoin blockchain account.
- To do that, making a digital wallet is the most straightforward method.
- Numerous wallet service providers exist, including Coinbase and BitCore.
- In order to create an account, the user must supply a "Key" that is similar to a password.

- The wallet will create a legal bitcoin private key-public key pair using this key.
- The user's visible account ID is the public key, which is accessible to everyone.
- In contrast, the user maintains the private key, which serves as his account access key, to himself.
- If someone misplaces their private key, they are unable to access their accounts and money.

4.4.2 Buy Bitcoin

- Purchasing Bitcoin via a bitcoin exchange is the simplest method to get them.
- Several online bitcoin exchanges let users convert fiat money to bitcoin.
- People may convert their regular money into bitcoin and transfer it to their wallet.
- Participation in bitcoin mining is another way to obtain bitcoin.

4.4.3 Transactions

- A transaction is when you send bitcoin from one account to another. The primary method is through wallets.
- The wallet app will have a screen where we can enter the recipient's account ID and the amount we want to send.
- The transaction will be verified by the miners when we have completed it, and if it is valid, it will be added to the blockchain record.
- Transactions with Bitcoin are free of charge. Bitcoin transaction confirmation typically takes ten minutes, however it may be sped up by paying a tiny transaction fee.

4.4.4 Bitcoin Mining

- The most significant and fascinating aspect of bitcoin is its mining.
- This is the procedure used to verify and add new transactions

to the claimed "blockchain."

- Because of the need for specialized mining hardware, not all nodes participate in mining.
- The nodes involved in the mining process are referred to as "miners.".
- Any time a new bitcoin transaction occurs in the network and is broadcast to all users.
- The miners take in this transmission when verifying transactions.
- The transactions are added to a block when they have been confirmed.
- For miners, to determine a hash value for the fresh block is the main task.
- The block reward, which is a certain number of bitcoins, is given to the miner who discovers the hash value first.
- Finding the hash value is not difficult. Each node has that ability. In order to encourage competition among the nodes, a difficulty level is attached to it. The amount of difficulty indicates how challenging it is to locate the hash.
- Difficulty level shrinks the set of hash values that a block can have. Since the hash length is 256 bits, it can have any value from the enormous range of 2^256 possible values, regardless of difficulty level.
- The target is significantly reduced by adding a level of difficulty.
- The miner must locate a hash value that begins with a specific number of zeroes since the difficulty level is expressed in terms of the number of zeroes.
- The nodes keep looking for new hash values and determine if they meet the required level of difficulty.
- Because a block's contents never changes, its hash also never changes. Consequently, the only way to experiment with alternative hash values is to associate a nonce with the block's content. The nonce is an arbitrary string of 32-bit length. i.e. H(block + nonce). Because the target set is so limited, there is a lower chance of success.

- The matching hash is calculated each time the miners use brute force to change the nonce.
- Because the miners must test out several permutations of "Nonce," this is the true game, and node computing power is crucial.
- The node with specialized hardware and high processing power has a better chance of succeeding in this game and receiving the block reward.
- The block and nonce will be announced by the first person to find hash. When they get this, other miners halt their work and check to see if the received hash meets the required degree of difficulty. If so, the nodes demonstrate their approval by including it in the blockchain.

4.4.5 The value of Bitcoin

- There is a claim that Bitcoin is worthless, because it answers no real need and solves no real problem. This claim can easily be refuted.
- Bitcoin is a global, decentralized, highly liquid, and pseudo-anonymous asset. Therefore, in any transaction, which requires all these properties, the benefits of using Bitcoin over other currencies are clear. Moreover, that is exactly the reason that most people do not appreciate these properties.
- First, most people are unaware of the damage caused by centralized monetary systems.
- Second, only rarely do they perform international financial transactions in large volumes. Third, most people are against anonymous transactions.
- However, the benefits of Bitcoin are widely recognized in the following cases :
  - (i) Where the centralized monetary system completely collapses.
  - (ii) Where the government confiscates its own citizen's assets.
  - (iii) Among populations, which are excluded from the financial and banking systems.
  - (iv) Among out casted populations.
  - (v) Among people who are keener on their privacy.
  - (vi) Among frequent travelers/flyers.

4.5 DIGITAL TOKENS

GQ. What are digital tokens?

- Digital tokens, simply known as "Tokens," are another market-shaking blockchain-based technology that is trending.
- Tokens are a digital asset that are developed on top of cryptocurrencies of a blockchain network. They are a minor variation of cryptocurrencies.
- The token may be used for a variety of things, including granting rights, paying for services, transferring data, offering incentives, getting access to further services, and many more.
- To put it another way, a token can be utilized anyway the developer or creating company sees fit.
- The tokens are a digital asset that is less liquid than a cryptocurrency and will never be utilised as one. Therefore, the value of every token that is produced will likewise be specified.
- The tokens may be refundable under specific circumstances, allowing us to trade them for cryptocurrencies.
- Wallets are used to maintain tokens, just like they are with cryptocurrencies.
- Most tokens are now produced on the Ethereum network. It is easy to create tokens using the Ethereum network. The establishment of a smart contract is all that is required to create a token in Ethereum.
- All that is required to create the tokens is the addition of the essential codes to the structure. When the token is finished, the Ethereum network can use it.

4.6 TYPES OF CRYPTOCURRENCIES

GQ. State and explain different types of cryptocurrencies.

- Despite the fact that Bitcoin was the first cryptocurrency in use by the general public, there are many different types of cryptocurrencies.

- Depending on its formulation or code design, application or use case, and other characteristics, we may classify cryptocurrencies into different types.
- You might get coins, payment tokens or altcoins, security tokens, non-fungible tokens or NFTs, decentralized finance tokens, utility tokens, and other categories.
- Coins are frequently used interchangeably with cryptocurrencies, despite the concept being used to describe all different kinds of cryptocurrencies or digital currencies.
- Even while many of them do not function as a unit of account, a store of value, or a medium of exchange-Bitcoin does-they are widely perceived as such.
- Coins, however, may be distinguished from altcoins. In addition to Bitcoin, all other cryptocurrencies that are viewed as alternatives to Bitcoin are referred to as altcoins.

(1) **Coins :** As coins are based on their blockchain, they may be distinguished from altcoins. Bitcoin on the Bitcoin blockchain and Ether, or ETH, on the Ethereum blockchain are two good examples. Building or creating a cryptocurrency begins with or follows the creation of a blockchain.

(2) **Altcoins :** They are viewed as alternatives to Bitcoin, the original cryptocurrency, even if they may all be considered coins. Also known as shitcoins, apart from Ethereum, most of the first ones were forked from Bitcoin. These include Namecoin, Peercoin, Litecoin, Dogecoin, and Auroracoin.

(3) **Tokens :** In a blockchain, tokens serve as digital representations of specific assets or utilities.Tokens are essential to getting a true grip on cryptocurrencies. They're the amount of digital resources you control on a given platform. As mentioned before, a digital wallet stores them and accessed with a key, which can be reassigned to someone else. Two types of tokens exist. First, is a native token. This type of token has an intrinsic utility. It forms the core part of a blockchain. That is to say, a blockchain could not run without a native token. Often times, they're used as an incentive to validate transactions, or create blocks.Be careful that tokens and coins have different properties. The majority of people frequently use them interchangeably, yet this is incorrect.

(4) **Bitcoin :** The king of the castle. Created in 2008, it housed the original code for blockchain technology. Its creation spurred many other cryptocurrencies. It's easily the most trusted and known virtual currency on the market, even if it has its flaws.

(5) **Ethereum :** Probably the second most well-known cryptocurrency. It allows users to do more than just use it as a virtual currency. It's an open-source blockchain. Money and assets are quickly transferred with the use of smart contracts. Assets include houses, cars, stocks, and other property owned with real-world value.

(6) **Litecoin :** One of the first cryptocurrencies to emerge after Bitcoin's initial release. It has a much shorter processing time-about 2.5 minutes-than Bitcoin's crazy 10-minute timeframe. Litecoin provides more tokens and a different mining algorithm, but it ultimately didn't take off the same way its big brother did.

(7) **Ripple :** Because every single token was mined before its release, it is quite possibly the most despised cryptocurrency by the community. This action is known as pre-mining and is a huge no-no. Essentially, this takes away the community aspect of virtual currencies. It attempts to take a decentralized platform and centralize it.

(8) **Monero :** Solved many of Bitcoin's privacy issues. It adds an additional level on anonymity to transactions. A few darknet markets (networks that require specific software or authorization to access them) started accepting the cryptocurrency in 2016, where it ultimately reached its peak.

4.7 CRYPTOWALLETS

- People dealing with cryptocurrency use a wallet as a safe depository and an instrument for incoming and outgoing payments. Let's analyze the available types of wallets and choose the most suitable one based on your computer's resources and tasks.
- There are hot and cold wallets. There are also warm wallets, but they are used much less often.
- Cold wallets are used to store money, while hot wallets are used to send and receive the currency quickly.

- As a rule, a wallet has a Private key and a Public key. The Private key belongs only to you, and you should never show it to anyone.
- You must keep it in mind as you sign all transactions with this key. At the same time, someone can use public keys to transfer money to your account.

4.8 METAMASK

GQ. Write a short note on: MetaMask.

- MetaMask is a web browser add-on which enables anyone to run the Ethereum DApps without running the Ethereum full node. An Ethereum full node installation
- will take a lot of memory as well as time; so Metamask is a tool that eliminates the overburden of this hectic installation task. Initially, Metamask was available only for Google Chrome, but now it is available for Firefox and other popular web browsers.
- MetaMask add-on for chrome can be added from chrome web store or from 'metamask.io' website. This MetaMask add-on provides a user interface for interacting with the blockchain.
- The user can connect to the Ethereum main network or 'test net' or he may create his own private network and run DApps on the blockchain.
- In normal case, a web3.js (the JavaScript API for Ethereum DApps) must be installed in the local system to interact with the Ethereum DApps. Web3.js is a collection of libraries used to interact with local or remote Ethereum node using Http or IPC connection. But MetaMask will inject the web3.js to each page for accessing the Ethereum blockchain by itself. This approach eliminates the effort of web3.js installation in the local system.
- After adding the Metamask, the user can interact with Ethereum blockchain as normal. The user can create an account, access Ethereum DApps, or deploy once own DApp. MetaMask retrieves data from the blockchain and allows the users to manage the data securely.

- The Metamask provides a vault account for each user, this vault secures, stores and tightly controls access to tokens, password, certificates, API keys and otherelements in blockchain apps. The vault account act as a second level encryption for the user account.

Wallet Seed

- The Metamask will provide a group of 12 words known as "wallet seed" while installing it. It is the user credential and it must be stored somewhere safe.
- The users can also create passwords for their account. The wallet seed or the password is necessary to log in to the MetaMask.
- The vault account willencrypt the user metadata and securely store it in the browser itself.

MetaMask Transactions

- The Metamask user interface has a default buy and send option for buying and sending Ether. The user can access his wallet, buy or send ether, check his balance and transactions from this interface.
- When the user executes a transaction from the Metamask it will send the transaction to the respective blockchain network.
- Then the corresponding validation and confirmation will occur in the blockchain as usual. In the case of 'testnet' and main network, the user can see the transaction details and confirmations in the 'Etherscan.io'.
- Example of a transaction of Ether through Metamask:For sending Ether to an account you have to specify the recipient address and the amount to be transferred in the provided interface.
- Before linking your transactions to the blockchain, the web3.js will ask yourpermission and the transaction will be submitted only after your approval.
- Once the user submits the transaction, it will be sent to the blockchain for validation. The transactions will be broadcasted to the nodes and once the validation is completed you can see the transaction details in the ether scan window. The window will display all the information regarding that transaction i.e.; block number, hash value, sender and recipient address,

number of confirmations, gas units, transaction cost, nonce etc.

- GNOSIS, Maker(MKR), Token Factory, CryptoKitties etc. are some DApps that supports Metamask. Any developer can submit DApp in Ethereum with Metamask support so that the user doesn't need to install the full Ethereum node for accessing the particular app. The Metamask is the very useful tool for accessing Ethereum in low bandwidth networks. Let's hope the tool will expand the reach of 'Ethereum' to more people.

4.9 COINBASE

- Coinbase is a trading platform that allows users to buy, sell and store more than 30 different digital currencies.
- Coinbase is more geared towards beginners while Coinbase Pro, the premium service, is for avid and experienced traders who make high volume transactions and want more trading options.
- The platform is straightforward. Like many trading apps, users can see their balance and a watch list, which allows them to track the prices of different kinds of cryptocurrencies.
- Traders can also check which cryptocurrencies are the biggest movers. Coinbase Cardis also introduced, that users can use to earn rewards for spending the assets in their portfolio.
- Coinbase charges a fee for trading via the platform. Coinbase doesn't charge users to hold their assets in a digital wallet or to transfer cryptocurrency from one wallet to another within the Coinbase network, like from Coinbase to Coinbase Pro.
- Once you have your digital wallet set up, users can trade. Coinbase does not offer trading for all cryptocurrencies, but the exchange does regularly add new coins.

Chapter Ends...

□□□

Unit 5

CHAPTER 5

Blockchain Ethereum Platform using Solidity

University Prescribed Syllabus

What is Ethereum, Types of Ethereum Networks, EVM (Ethereum Virtual Machine), Introduction to smart contracts, Purpose and types of Smart Contracts, Implementing and deploying smart contracts using Solidity, Swarm (Decentralized Storage Platform), Whisper (Decentralized Messaging Platform).

5.1 WHAT IS ETHEREUM?

GQ. What is Ethereum. What the major features of it? **(4 Marks)**

Ethereum is a blockchain-based computing platform that gives programmers the ability to create and deploy decentralised apps, which are those that are not controlled by a single entity. You can design a decentralised application where the decision-making authority resides with the system's users.

Features of Ethereum

(1) **Ether :** This is Ethereum's cryptocurrency.

(2) **Smart contracts :** Ethereum supports the creation and implementation of such a contract.

(3) **Ethereum Virtual Machine :** Ethereum offers the underlying technology the software and architecture that recognises smart contracts and enables you to communicate with them.

(4) **Decentralized applications (Dapps) :** A Dapp (also spelt DAPP, App, or DApp) is a short form for a decentralised application. Decentralized apps, which are consolidated applications, are possible using Ethereum.

(5) **Decentralized autonomous organisations (DAOs) :** You may build these for democratic decision-making using Ethereum.

5.1.1 Ether

- Ether (ETH) is Ethereum's cryptocurrency. It serves as the network's fuel. It is used to cover the transaction fees and computational costs associated with every transaction carried out on the Ethereum network. Ether is a peer-to-peer currency, similar to Bitcoins.
- Ether may be used to purchase gas, which is required to process every transaction completed on the Ethereum network, in addition to paying for transactions.
- Additionally, gas must be purchased using ether if you wish to deploy a contract on Ethereum. Therefore, the execution cost a user pays to perform a transaction in Ethereum is called gas.
- Decentralized apps, smart contracts, and routine peer-to-peer payments may all be implemented with ether.

5.1.2 Smart Contracts

GQ. Explain the concept of smart contracts. How it differs from traditional systems? **(4 Marks)**

- The concept of smart contracts was first proposed by Nick Szabo in 1994. Szabo is a legal scholar and cryptographer known for laying the groundwork for digital currency.
- A smart contract is a simple computer programme that makes it easier for two parties to exchange any asset. You may wish to exchange money, stocks, real estate, or any other kind of digital asset. These contracts can be created by any user on the Ethereum network.
- The terms and conditions that were mutually agreed upon by the parties make up the majority of the contract (peers).

- A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.
- The main advantage of smart contracts is that they cannot be changed once they have been performed, and every transaction carried out on top of one is forever recorded—it is immutable.
- Therefore, the transactions associated with the original contract will not change if the smart contract is modified in the future; you cannot edit those transactions.
- Any smart contract execution on Ethereum is decentralised since the smart contract verification is carried out by anonymous network participants without the requirement for a centralised authority.
- The identities of the two parties are secure on the Ethereum network, and any asset or currency may be transferred in a trustworthy and transparent manner.
- When a transaction is completed correctly, the sender's and the receiver's accounts are updated appropriately, which builds confidence between the parties.

5.1.3 Ethereum Virtual Machine

GQ. Write a short note on EVM. **(4 Marks)**
GQ. How smart contracts are compiled on EVM? **(4 Marks)**
GQ. Elaborate the interaction of Smart contract and EVM with DApps. **(4 Marks)**
GQ. Describe cycle of smart contract execution on EVM. **(4 Marks)**
GQ. What is Gas in Ethereum? **(2 Marks)**
GQ. What are consensus mechanism used in Ethereum? **(4 Marks)**
GQ. Differentiate the mining process of Ethereum from Bitcoin. **(4 Marks)**

- EVM is intended to function as a runtime environment for compiling and deploying Ethereum-based smart contracts. The smart contract language for Ethereum i.e Solidity programming language, is understood by EVM.

- In essence, you may install your stand-alone environment, which can serve as a testing and development environment, as EVM is run in a sandbox environment.
- In other words the EVM doesn't interact with the OS so it has no access to disk, RAM or networking it's essentially self-contained.
- Once you are satisfied with the smart contract's performance and usefulness, you may deploy it on the Ethereum main network after testing it (using it) "n" times and confirming it.EVM is quasi-Turing complete machine.
- Theoretically, Turing machine can run any computation irrespective of complexity, recursion, depth, length and complication no matter how much time and storage is required to complete it. Executing instructions on EVM incurs some cost known as gas.
- Ethereum platform has built in token known as ether.
- Gas in this context means some fraction of ether which needs to be supplied along with other inputs while executing the transaction or smart contract.
- This is similar to the fuel(gas/petrol/diesel) that is required to run a motor vehicle.
- A vehicle runs as long as fuel is available. In the same manner code execution on Ethereum continues till the availability of the gas.
- Hence, EVM is known as quasi-Turing complete machine due to dependency on gas availability for execution.
- Also, gas offers protection against infinite loop scenario in smart contract programming.
- The significance of EVM is also evident in the effectiveness of preventing Denial-of-Service or DOS attacks.
- In addition, EVM is also responsible for ensuring that a specific program does not have access to the states of each other.

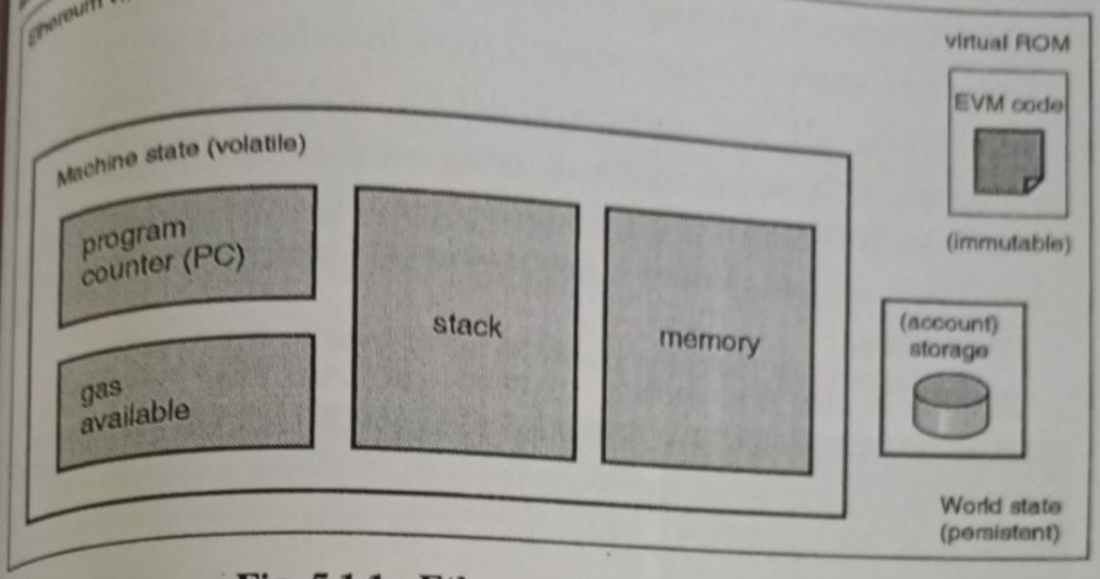


Fig. 5.1.1 : Ethereum Virtual machine

Interaction of Smart Contract and EVM with DApp

- When a external application such as Dapp wants to interact with the smart contract it needs some details about contract such as the function signatures and properties exposed by it.
- This is similar to how a distributed application interacts with an external web service using service description language.
- A smart contract program, written say solidity gets compiled to a bytecode.

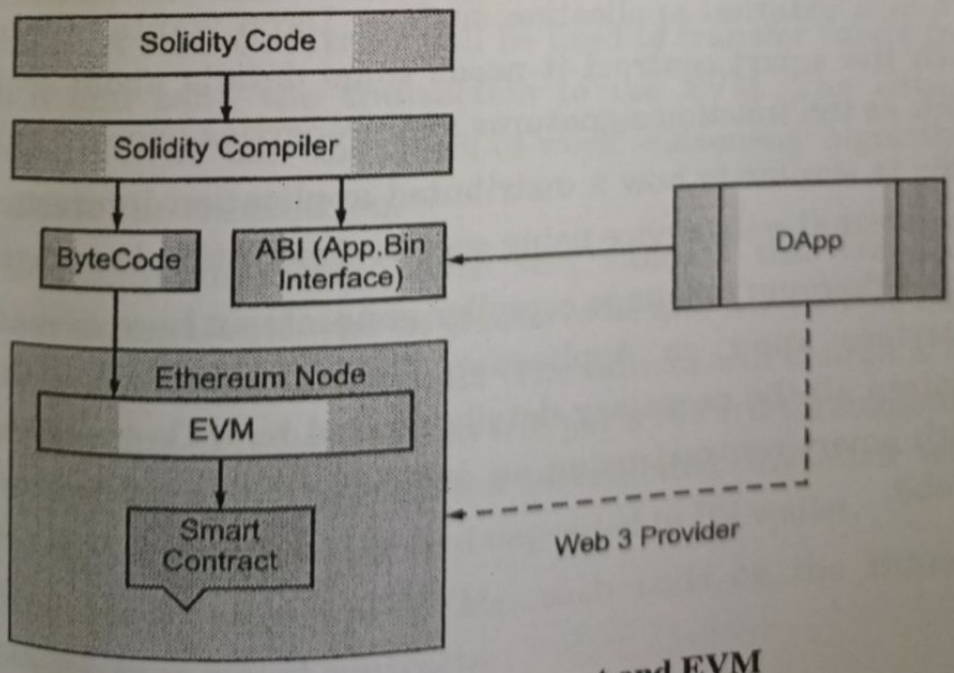


Fig. 5.1.2 : Smart contract and EVM

- The Ethereum language compiler generates a human readable interface know as Application Binary Interface (ABI).
- It contain all the necessary details needed by a Dapp to interact with smart contract using an external helper library such as Web3. Any programming language used in the smart contract is translated into bytecode that the EVM can understand.
- The EVM has the ability to read and run this bytecode. As soon as your smart contract is created in Solidity, it is translated into bytecode and deployed on the EVM, providing security against hacker attacks.

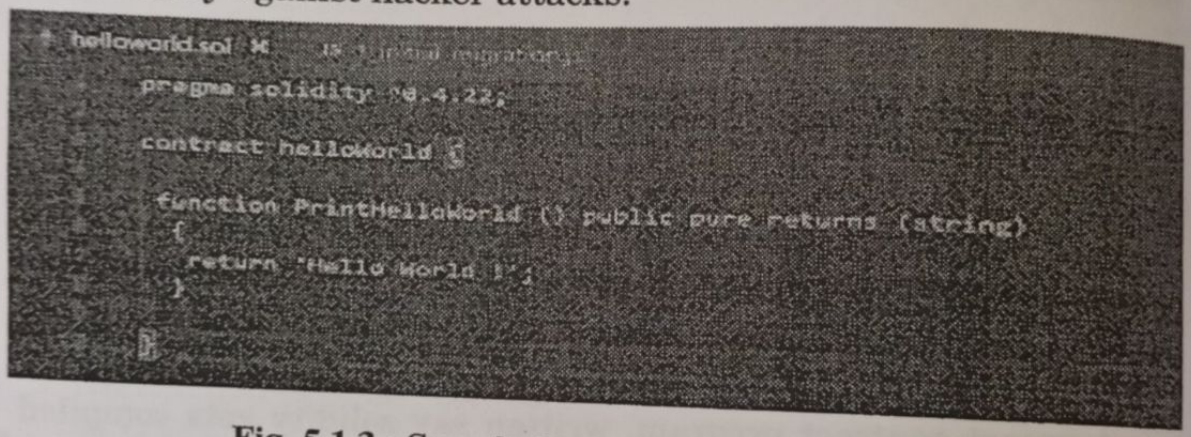


Fig. 5.1.3 : Sample Smart contract in solidity

- When a external application such as Dapp wants to interact with the smart contract it needs some details about contract such as the function signatures and properties exposed by it.
- This is similar to how a distributed application interacts with an external web service using service description language.
- The Ethereum language compiler generates a human readable interface know as Application Binary Interface (ABI). It contain all the necessary details needed by a Dapp to interact with smart contract using an external helper library such as Web3.

BYTECODE


```
{
  "linkReferences": {},
  "object": "608060405234801561001057600080fd5b5060c78061001f6000396000f300{
  "opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2 0x10
  "sourceMap": "25:163:0:-;;;;8:9:-1;5:2;;;30:1;27;20:12;5:2;25:163:0;;;;;;;
}
```


Fig. 5.1.4 : Conversion of smart contract to bytecode

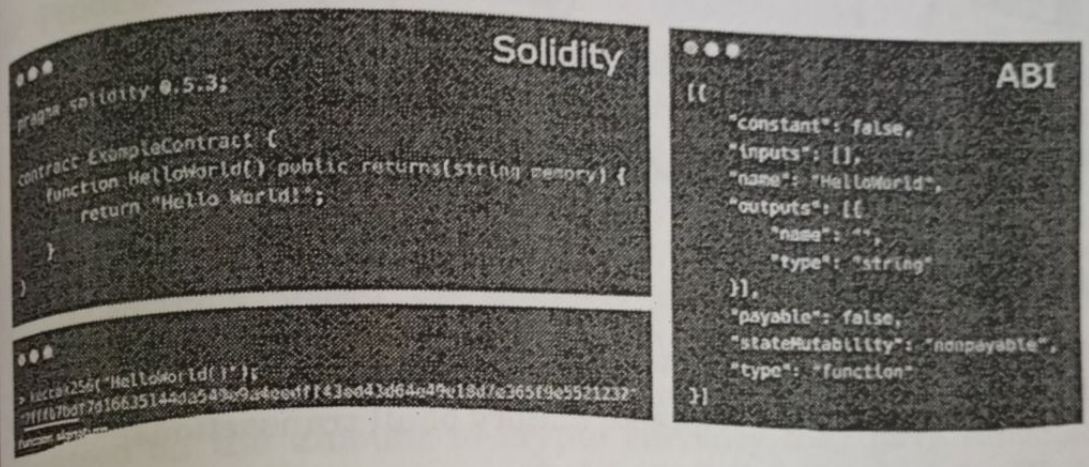


Fig. 5.1.5 : Conversion of smart contract ABI

How Does EVM Work?

- Consider the case when person A wishes to give person B 10 ethers. A smart contract will be used to transfer funds from A to B and send the transaction to the EVM. The Ethereum network will use the proof-of-work consensus algorithm to validate the transaction.
- The Ethereum miner nodes will validate this transaction, determining if A is who he claims to be and whether he has the required amount to transmit. The miners will charge a fee to validate this transaction and will get a reward throughout this process. Once the transaction is validated, the ether will be deducted from A's wallet and deposited to B's wallet.
- Using their respective EVMs, each node on the Ethereum network runs smart contracts.

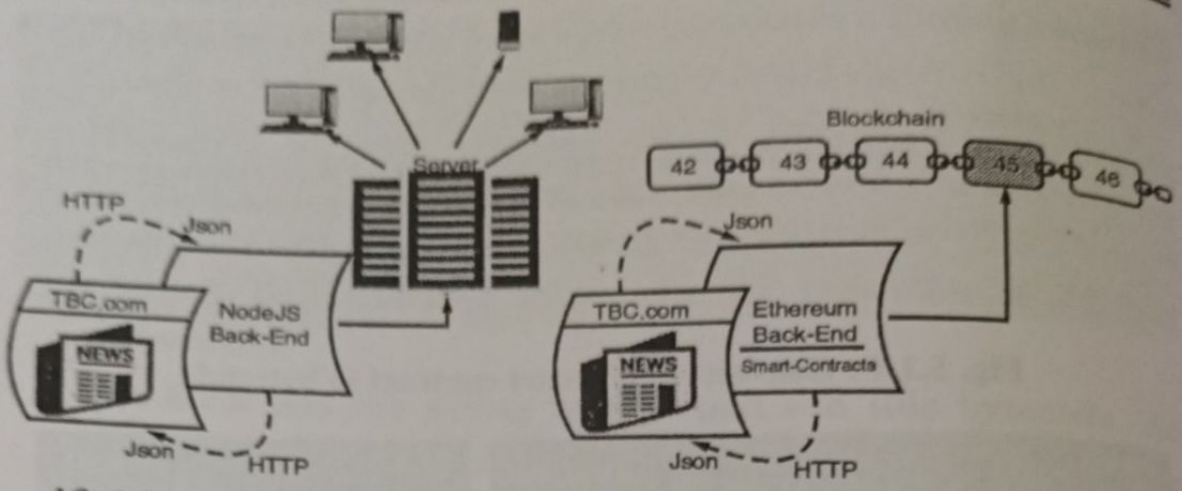


Fig. 5.1.6 : Total cycle of smart contract execution over Ethereum blockchain

☞ Proof of Work

Every node in the Ethereum network has :

- The full chain the complete history of all transactions
- The transactions linked to the smart contract as well as the history of the smart contract, which includes the address where the smart contract is deployed.
- The handle to the smart contract's current state.
- Validating the blocks is the aim of the miners on the Ethereum network. Miners employ their computing power and resources to generate the correct hash value by altering the nonce for each block of a transaction.
- The nonce will be changed by the miners and run through the Ethash algorithm, which is the hashing technique used for Ethereum. This produces a hash value that should be less than the predefined target as per the proof-of-work consensus.
- If the hash value generated is less than the target value, then the block is considered to be verified, and the miner gets rewarded. When the proof of work is completed, the result is broadcast and shared with every other node so that they may update their ledger.

- The block is uploaded to the Ethereum main blockchain and the miner is rewarded with a reward, which as of right now is three ethers, if other nodes acknowledge the hashed block as valid. Additionally, the transaction fees that were produced for validating the block are given to the miner.
- The cumulative transaction fees associated with all the transactions that are included into the block are also paid to the miner as a reward.

Proof of Stake

- Proof of stake is another procedure being developed for Ethereum. It serves as an alternative for proof of work and is intended to reduce the use of costly resources used for mining with proof of work.
- In proof of stake, the validator the miner can validate transactions based on quantity of cryptocoins he or she currently possesses before initiating the mining process.
- Therefore, the miner has a better chance of mining the block based on the amount of crypto currency they have collected thus far. In contrast to proof of work, proof of stake is now less common.

Gas

- Applications running on the Ethereum network require gas, much like a car needs fuel to run. A user must pay a fee to complete any transaction on the Ethereum network.
- In this situation, the fee is made up of ethers, and the intermediary monetary value is known as gas. Gas is a unit used on the Ethereum network to represent the amount of processing power needed to execute a smart contract or a transaction. Therefore, you would have to pay gas, which is measured in ethers, if you needed to complete a transaction that updated the network.
- The transaction fees in Ethereum are computed using a formula. The transaction fees equal the amount of gas required to execute a transaction multiplied by the gas price. "Gas limit" refers to the amount of gas used for the computation and the amount of ether a user is required to pay for the gas.

- The transaction fees in Ethereum are computed using a formula.
- The transaction fees equal the amount of gas required to execute a transaction multiplied by the gas price. "Gas limit" refers to the amount of gas used for the computation and the amount of ether a user is required to pay for the gas.

☞ How is Ethereum Mining Different from Bitcoin Mining ?

- By market capitalization, it is the second-largest cryptocurrency after Bitcoin. But unlike Bitcoin, it wasn't designed to be a kind of digital money.
- The goal of Ethereum's creators was to create a new type of global, decentralised computing platform that would take the openness and security of blockchains and apply them to a wide range of applications.
- Key distinctions between bitcoin and ethereum
- The most popular cryptocurrency is Bitcoin, while Ethereum comes in second.
- The cryptocurrency itself and the blockchain network are both referred to as Bitcoin. The terms "Ethereum" and "Ether" refer to the network and respective cryptocurrency, respectively.

Some other differences between the Bitcoin and Ethereum networks are the following :

(1) **Abbreviation** : *BTC* refers to Bitcoin currency, and *ETH* refers to Ether.

(2) **Inception :** Bitcoin is the world's first cryptocurrency, created in 2009. Ethereum came next in 2015. Ether was originally intended to complement Bitcoin, but the two coins ended up competing.

(3) **Trades enabled :** Bitcoin only transacts in digital currencies, but Ethereum provides a variety of trading options, including smart contracts.

(4) **Block your time :** Compared to 10 minutes for Bitcoin, the average block time for the confirmation of an Ether transaction is roughly 12 seconds.

(5) **Consensus System** : Both the Ethereum and Bitcoin networks have relied on proof-of-work (PoW) mechanisms to

verify transactions. As part of the Ethereum 2.0 upgrade, proof of stake (PoS) will replace the current Ethereum system in 2022.

(6) **Executable code :** Contrary to transactions on the Bitcoin network, Ethereum transactions can be attached with executable code. This enables decentralized applications and conditional transactions, which are transactions that take place only when certain conditions are met.

(7) **Encryption type :** The two blockchain networks run different encryption Ethereum runs Ethash, and Bitcoin runs Secure Hash Algorithm 256 (SHA-256) encryption.

Table 5.1.1 : Bitcoin Vs Ethererum

	Bitcoin(BTC)	Ethereum(ETH)
Founded	2009	2013
Hashing Algorithm	SHA-256	Ethash
Consensus mechanism	POW	POW now;moving to POS with Ethereum 2.0
Time is taken to mine a block	An average of 10 minutes	An average of 12-15 seconds
Executable code	Doesn't use	Does use
Reward	12.5 BTC	3 ETH

5.1.4 Decentralized Applications (DApps)

GQ. Write a short note on DApps. **(4 Marks)**

- Let's evaluate the differences between decentralised and traditional apps. For instance, when you sign in to TBC.com, an HTML-rendered online application is displayed. To access your data (your information), which is centrally hosted, the page will request an API.
- The procedure is straightforward: your front end calls the backend API, which then pulls your data from a centralised database.
- When you log in, the same web application is displayed if we make this application decentralised, but it uses a smart contract-based API to retrieve the data from the blockchain network.

- The API is therefore replaced with a smart contract interface, and the smart contract will pull its data from the blockchain network, which serves as its back end.
- The blockchain network is a decentralised network rather than a centralised database, and all transactions made using the blockchain network's smart contract are validated (verified) by the network's users (the miners).
- Therefore, every action or transaction carried out on a TBC.com-like application after it was transformed will be a decentralised action or transaction.
- A backend code that executes on a distributed peer-to-peer network makes up a Dapp. The main distinction is that it enables direct communication between end users and the decentralised application providers since it is software created to operate on the Ethereum network without being governed by a centralised system.
- An application qualifies as a Dapp when it is open-source (its code is on Github), and it uses a public blockchain-based token to run its applications.
- A token acts as fuel for the decentralized application to run. Dapp allows the back end code and data to be decentralized, and that is the primary architecture of any Dapp.

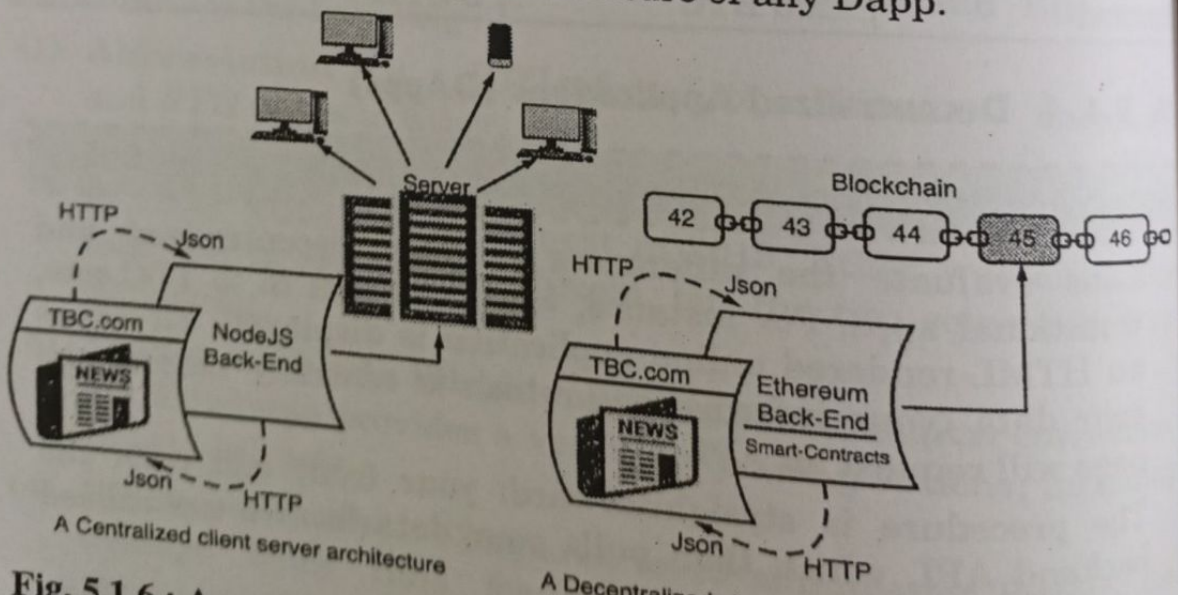


Fig. 5.1.6 : A comparison between Centralized Client-server architecture and Decentralized DApp architecture.

5.1.5 Decentralized Autonomous Organizations (DAOs)

GQ. Write a short note on Decentralized Autonomous Organization (DAO). (4 Marks)

- A DAO is a digital organisation that functions in a decentralised, democratic manner without the use of hierarchical administration.
- In summary, a DAO is an organisation where decision-making is preferably delegated to certain specified authorities or a group of designated individuals as a part of an authority rather than being centralised.
- DAOs rely on smart contracts for decision-making or, in other words, decentralised voting systems within the organisation since it lives on a blockchain network and is regulated by the protocols included in a smart contract.
- The voting mechanism, which is controlled by a decentralised application, must thus be used before any organisational decision can be taken.
- This is how it works. People contribute money through the DAO because it needs it to function and make decisions.
- Based on it, a token that represents each member's share in the DAO is issued to them. With those tokens, users may cast votes in the DAO, and the proposal's status is determined by which users cast the most votes.
- This voting procedure must be used for every decision made inside the organisation.

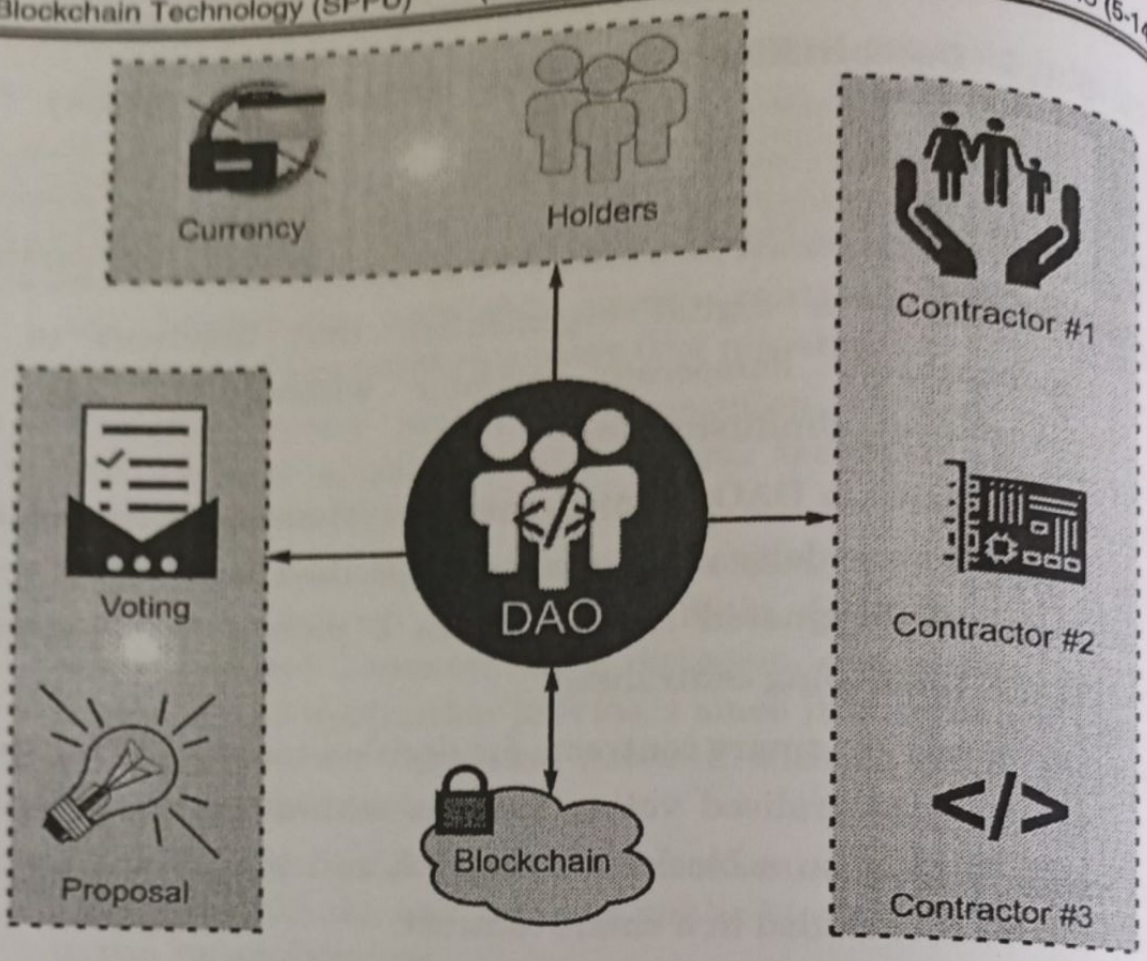


Fig. 5.1.8 : DAO's Process

5.2 THE ETHEREUM NETWORK

GQ. Enlist and explain three types of Ethereum network.

5.2.1 Types of Ethereum Network

The Ethereum network is a peer-to-peer network where nodes participate in order to maintain the blockchain and contribute to the consensus mechanism. Networks can be divided into three types, based on requirements and usage.

Mainnet

Mainnet is the current live network of Ethereum. The current version of main net is Byzantium (Metropolis) and its chain ID is 1. Chain ID is used to identify the network.

Testnet

- The commonly used test network for the Ethereum blockchain is known as Testnet. Before being implemented on the live production blockchain, smart contracts and DApps are tested on this test blockchain. Additionally, since it's a test network, study and experimentation are allowed.
- The primary testnet, known as Ropsten, has all the characteristics of various smaller and specialized testnets that were made for certain versions. Kovan and Rinkeby, for example, were created as additional testnets to evaluate Byzantium versions.

Private net

- As the name suggests, this is the private network that can be created by generating a new genesis block.
- This is usually the case in private blockchain distributed ledger networks, where a private group of entities start their blockchain and use it as a permissioned blockchain.

5.2.2 Ethereum Fork

GQ. What is Ethereum Classic? **(2 Marks)**

Ethereum Classic

- Ethereum Classic is the name of the original Ethereum blockchain.
- In 2016, a set of smart contracts on a platform known as The DAO, a decentralized autonomous organization, raised a record $150 million in an online crowdsale, the name of the crowdfunding method used to help support Ethereum.
- Shortly after that money was raised, an anonymous hacker stole $50 million DAO tokens.
- This resulted in the crypto community's decision to fork the network and to reappropriate the stolen funds. Forking is when the source code of an old open source program is used to create a new one.

- The network fork split the Ethereum blockchain into two: the original Ethereum Classic and Ethereum, the new one. This created competition between the two networks and became known as a hard fork. A hard fork is when nodes on the newest version of a blockchain no longer accept older versions.

5.3 ETHEREUM TOOL STACK

GQ. With the help of neat diagram, explain the Ethereum tool stack. **(6 Marks)**

GQ. What is testnet? Write down about Ethereum testnets. **(4 Marks)**

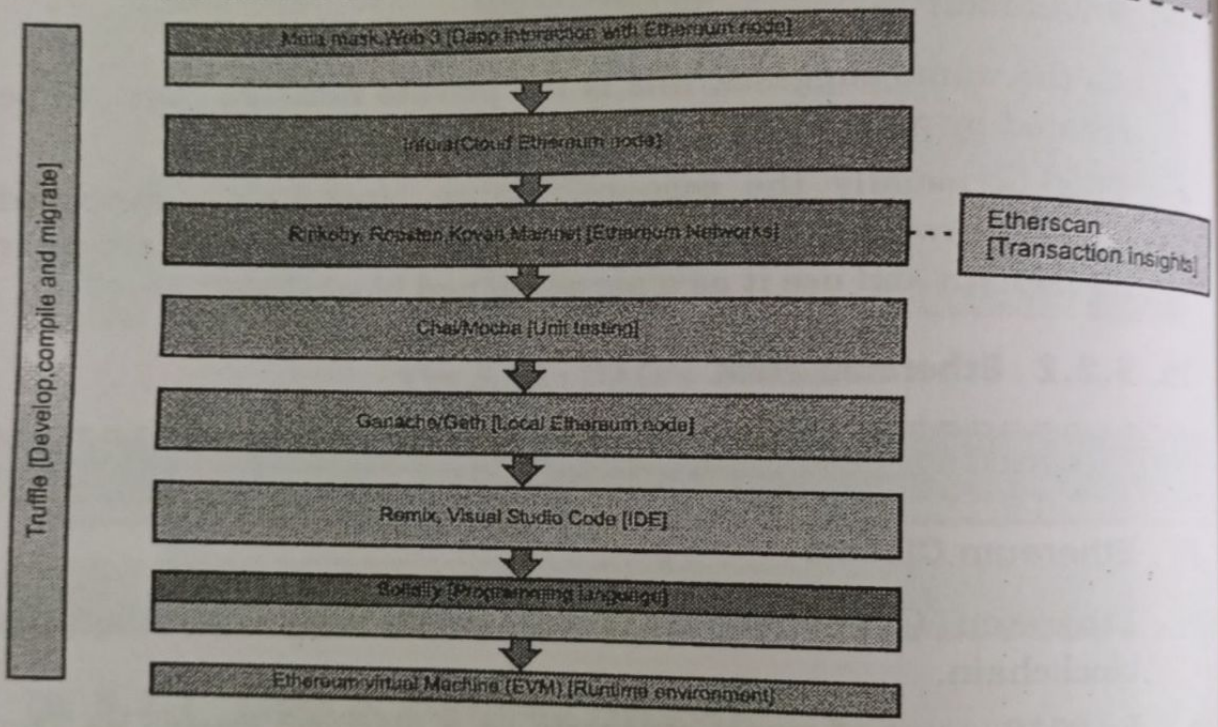


Fig. 5.3.1 : Ethereum tool stack

(1) Truffle : A world class development environment, testing framework and deployment framework for blockchains using the Ethereum Virtual Machine (EVM), aiming to make life as a developer easier. The Truffle suite includes Truffle, Ganache, and Drizzle.

(2) Ethereum Virtual machine : EVM is intended to function as a runtime environment for compiling and deploying Ethereum-based smart contracts.

(3) **Solidity :** The smart contract language for Ethereum is Solidity programming language,

(4) **Remix :** Remix IDE allows developing, deploying and administering smart contracts for Ethereum like blockchains. It can also be used as a learning platform.

(5) **Ganache/Geth :** A personal blockchain for Ethereum development you can use to deploy contracts, develop your applications, and run tests. It is available as both a desktop application as well as a command-line tool (formerly known as the TestRPC). Ganache is available for Windows, Mac, and Linux.

(6) **Chai/Mocha :** Chai and Mocha are used for unit testing. Mochais a light-weight Node.js test framework, and Chaiis a Test Driven Development (TDD) assertion library for node.Both Mocha and Chai run in NodeJs and the browser and allow asynchronous testing. Although Mocha can be paired with any of the assertion libraries, it is delightfully paired with Chai most of the time. Chai provides us with several APIs like Assert, Expect/Should, and more. Mocha provides all the functionality required for automated testing in simpler ways.

(7) **Ethereum Test Networks :** A version of a project is released to an Ethereum Test Network ("testnet"), which simulates Ethereum Mainnet (the primary public Ethereum blockchain network) before to its release on the blockchain (or before modifications are made to the blockchain itself), giving developers, the community, and you an opportunity to try it out before real money is involved. It can be exciting to own 10,000 Ether or a trillion tokens on a testnet, even though they are simple to get and have no real-world worth. Currently, three testnets are operational, and each of them functions identically to the production blockchain (where your real Ether and tokens reside).

(i) **Ropsten** : The most comparable proof-of-work blockchain to Ethereum; it is simple to mine fake Ethereum.

(ii) **Kovan :** A proof-of-authority blockchain created by the Parity team is called Kovan. Ether must be requested rather than mined.

(iii) **Rinkeby :** A proof-of-authority blockchain created by the Geth team is called Rinkeby. Ether must be requested rather than mined.

(8) **Infura :** Infura is a Web3 backend and Infrastructure-as-a-Service (IaaS) provider that offers a range of services and tools for blockchain developers. This includes the Infura API (Application Programming Interface) suite. The flagship Infura Ethereum API is at the heart of the Infura Web3 service.

(9) **Metamask :** MetaMask is a cryptocurrency wallet that enables users to store Ether and other ERC-20 tokens. The wallet can also be used to interact with decentralized applications, or dapps.

5.4 ETHEREUM APPLICATIONS AND USE CASES

GQ. Elaborate on various applications of Ethereum. **(4 Marks)**

- According to the Ethereum Foundation, Ethereum can be applied to codifying, decentralizing, securing and trading almost everything. Its uses include the following :
  (i) crowdfunding
  (ii) financial exchanges
  (iii) company governance
  (iv) domain names
  (v) intellectual property
  (vi) smart property with hardware integration
  (vii) voting
  (viii) contracts and agreements
- Ethereum can be used for the following purposes :
  (i) buy and sell cryptocurrencies like Ether and other fungible, Ethereum Request for Comments 20-validated tokens;
  (ii) host smart contracts and decentralized apps (dApps);
  (iii) carry out decentralized finance activities;
  (iv) exchange nonfungible tokens;

(v) power Ethereum-based enterprise software independently from the public Ethereum chain; and

(vi) play Ethereum-based video games, where users can earn real cryptocurrency from playing the game.

5.5 BENEFITS OF ETHEREUM

GQ. What are the pros of Ethereum? (4 Marks)

Many benefits of blockchain technology apply to Ethereum, including the following :

1) **Decentralization :** Due to the decentralised nature of Ethereum, there is no influence from outside cloud service providers. Peer-to-peer transactions are made possible through the usage of blockchain. In contrast to certain other software systems, which frequently need faith in a central authority, users can exchange value or store data without the requirement for an intermediary.

2) **Availability :** Ethereum is decentralised, so if a node goes down there is no downtime. Other computer architectures rely on centralised servers, and interruptions can have an impact on performance.

3) **Privacy :** Users have the option to remain anonymous when utilising the network for exchanges. To utilise an Ethereum application, they don't have to input their personal information.

4) **Security :** Ethereum is made to be impossible to hack, much like any other decentralised blockchain-based network. To exploit the network, hackers would need to gain control over majority of the nodes.

5) **Permissionless :** Because Ethereum is a permissionless blockchain, anybody may take part. In contrast, permissioned blockchains are only accessible to certain individuals.

6) **Less ambiguity :** Stronger contracts are guaranteed by the hardcoded smart contracts that are the basis of trading and agreement on Ethereum. A freelancer who receives work through a dApp on Ethereum, for instance, may sign a smart

contract with the hardcoded clause "X remuneration will be delivered when Y job is performed." This is distinct from regular contracts, which call for interpretation and execution.

5.6 DRAWBACKS OF ETHEREUM

GQ. What are the pros and cons of Ethereum? **(4 Marks)**

The Ethereum platform has been criticised in two ways :

(1) **Resource-intensive :** The PoW consensus technique is being used by Ethereum as a resource-intensive method of ensuring that all network nodes agree on the status of all data stored on the blockchain. Every blockchain node stores every smart contract, and each node concurrently performs every smart contract's computations.

(2) **Security :** Additionally, the PoW approach creates a security concern. Smart contract flaws on the open blockchain are readily apparent to everyone and can be harder to fix than to exploit.

- When Ethereum switches from a PoW consensus algorithm to a PoS consensus algorithm in 2022, these criticisms will be addressed. By providing greater mining or block validation power to miners with more coins, PoS is anticipated to increase the Ethereum blockchain's energy efficiency. Fewer nodes are required to perform more work as a consequence. Additionally, no specialised equipment is needed; all that is needed are the currencies needed for mining and an internet connection.
- The fact that greater mining power is concentrated within a smaller group of miners is a drawback of this approach. More manipulation and collaboration are made possible by this on the network.
- Other drawbacks of Ethereum include its high entrance barrier, high cost of development, and difficulty of usage for those who are not familiar with the technology.

5.7 ETHEREUM 2.0

- The Ethereum network will undergo a significant update in 2022 known as Ethereum 2.0, also referred to as ETH 2.0 or Serenity.
- The objective is to boost the network's transaction throughput to tens of thousands of transactions per second from 15 transactions per second currently.
- It will do this by distributing workloads across a large number of parallel blockchains that all use a single consensus PoS blockchain. Any threat actor would find it too expensive to carry out the act of maliciously altering any one chain, which would need altering the common consensus.

5.8 SMART CONTRACTS

GQ. Write a short note on Smart contracts. **(6 Marks)**

GQ. How smart contracts works? **(4 Marks)**

- Smart contracts are digital transaction protocols that, if certain conditions are met by all parties, verify, control, and self-execute an agreement contained in digital codes on a blockchain.
- These contracts take place between anonymous parties and are automatically enforced without the assistance of any third party, in contrast to traditional (physical) ones.
- Signatories (parties), the subject of the agreement, and the conditions of the agreement are its three primary components. For the transaction to be successful, all parties involved must adhere to the terms of the agreement (a set of guidelines and penalties).
- Executing agreements using digital contracts is said to be safe, cost-effective, and eliminates the need for a middleman.
- Furthermore, the decentralised nature of the blockchain network guarantees the transparency, traceability, and irreversibility of all transactions.

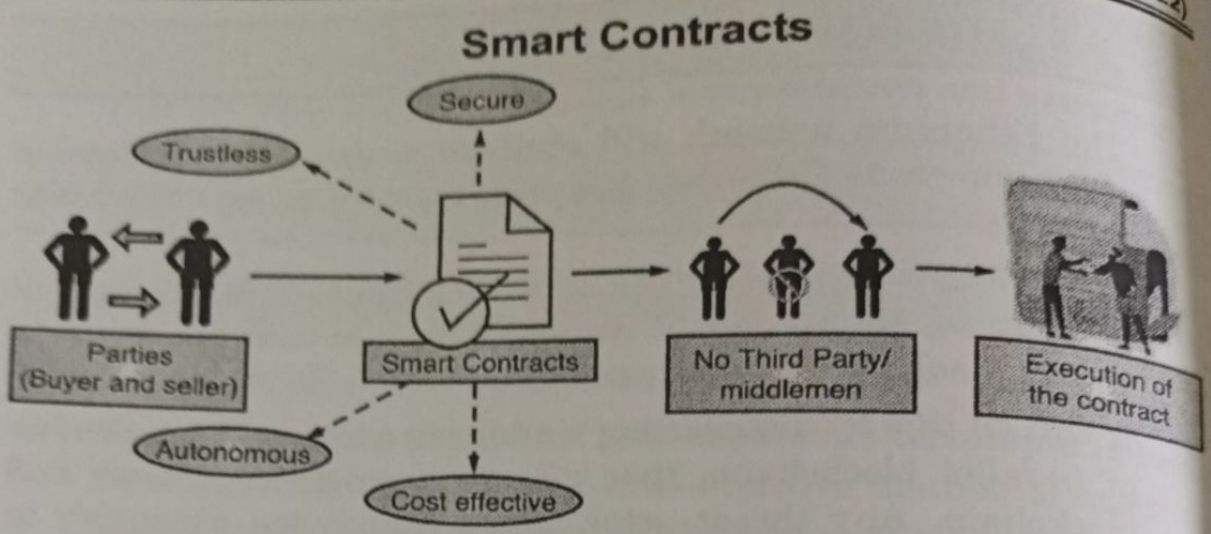


Fig. 5.8.1 : Smart contracts

- Two or more individuals, organisations, or governments are parties to a traditional (physical) contract. Therein, you sign an agreement, then you employ a third party to carry it out because you have faith in them.
- This third party might be a government agency, a lawyer, or any other type of organisation. Its purpose is to handle the procedures and carry out the contract.
- This raises the expense of auditing and enforcing laws as well as the risk of financial loss brought on by fraud and data manipulation. With smart contracts, the contract is written in code.
- The outcome is validated by the users of the Ethereum blockchain-based network rather than a centralised authority.
- The threat of any data tampering or alteration is eliminated once a contract is executed since the transaction is registered and cannot be changed or interfered with.
- Consider the situation where Bob hired Alice to create the website for his business and paid her $500 for the job.
- The smart contract's agreement is built by the developers using the Ethereum programming language.
- The smart contract has all the conditions (requirements) for building the website. Once the code is written, it is uploaded and deployed on the Ethereum Virtual Machine (EVM).

- A smart contract may be executed using EVM, a runtime compiler. Every member of the network owns a copy of the contract once the code is installed on the EVM.
- Each node on the Ethereum network will review and certify that Alice's work has been completed in accordance with the coding specifications when Alice submits it for evaluation.
- Once the work is authorised and validated, the $500 contract will execute automatically, and Alice will be paid in ether. Alice will be paid $500 in ether, and Bob's account will be promptly debited.
- Nick Szabo, an American computer scientist and cryptographer, first used the phrase "smart contracts" in 1994 while attempting to carry out the conditions of a contract utilising distributed ledger technology and automated transaction protocols.
- Smart or self-executing contracts are computer programs created on a blockchain that facilitate transactions when parties satisfy a predetermined set of conditions. Also, there is no need for the parties to rely on an intermediary for the agreement's validation and execution.

Smart Contracts Functioning

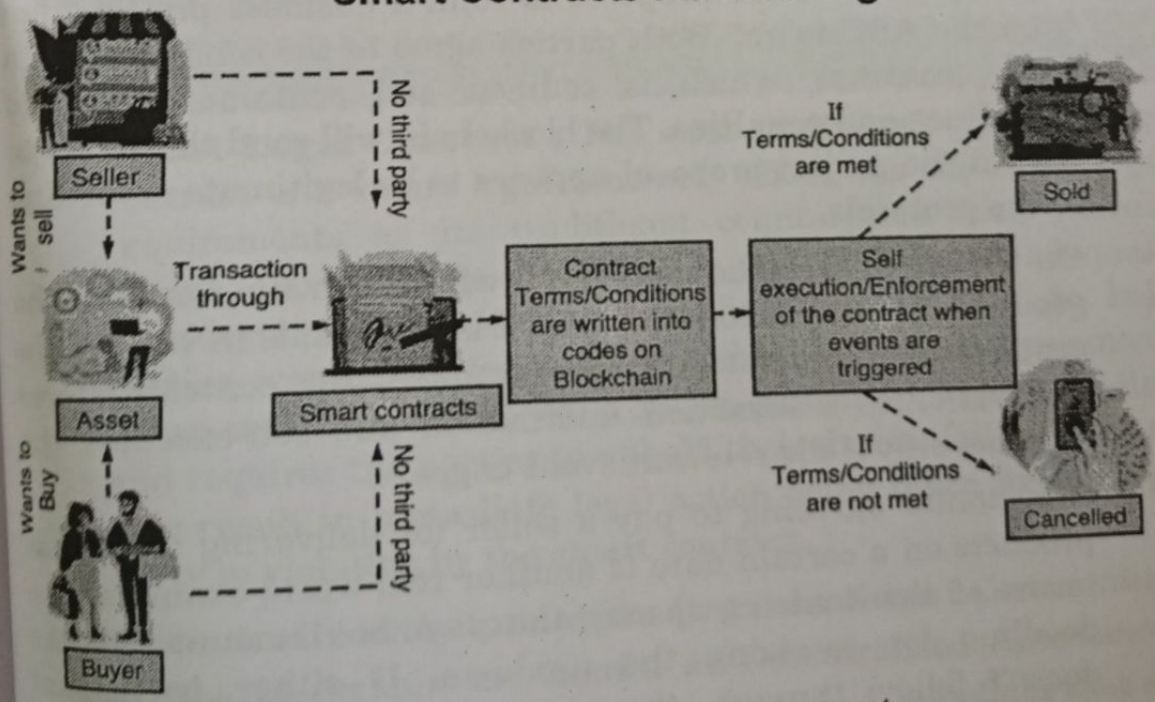


Fig. 5.8.2 : Working of smart contracts

The process

- There are two parties (a buyer and a seller) interested in purchasing and selling an item.
- These two parties establish a smart contract, which is a fully digital and self-executing agreement, with its terms or conditions written in codes on a decentralised blockchain network. 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 follow the transaction. The parties involved's identities, however, are kept private.

Examples

- In fields including property rights, intellectual property, banking and insurance, legal services, e-government, crowdfunding, etc., smart contracts instances are common. Let's think about the following instances to help us better understand the concept:
- A group of investors proposes to fund a business project idea from the ABC team. Both parties agree to the conditions of a smart contract, which is codified and contains a list of guidelines and penalties. The blockchain will send the funds to ABC if the project proposal appears to be legitimate according to the protocols.
- On the other side, the blockchain will return the funds to the group if the project concept doesn't look suitable in view of the contract requirements. In this example, the contract stores and validates transaction information and self-executes the contract only if the relevant event triggers.
- A customer agreeing to pay a seller for delivering particular products on a certain date is another real-world example. The terms of the contract specify the payment amount and the deadline for receiving the products. If either participant doesn't follow through, the transaction will be held in the blockchain.

- Ethereum wallets are popular blockchain-based cryptocurrency apps that need an Ethereum account from the user. They are able to conduct financial transactions without using a bank or any third party.
- In order to provide high-end safety to wallet users, open-source blockchain Ontology has announced a partnership with blockchain distribution network bloXroute Labs, Inc. Ethereum smart contracts will be more secure and safe for users because to its integrated design with the Ethereum Virtual Machine.
- Smart contracts in finance can help streamline and accelerate a variety of financial services.
- They can be used, for instance, by insurance firms to establish official agreements and resolve disputes.
- Similar to how bond issues can issue bonds for trading that complies with regulations, stock markets can set securities trading rules in these contracts. Banks may use these contracts in the same way to handle syndicated loans more quickly and with fewer operational risks.

5.8.1 Types of Smart Contracts

GQ. What are the types of smart contracts. **(2 Marks)**

(1) **Smart Legal Contract :** The most traditional type of smart contract is a smart legal contract, which has the same legal requirements as its traditional counterparts (i.e., mutual assent, expressed by a valid offer and acceptance; adequate consideration; capacity; and legality) and is used to hold parties responsible for upholding their end of an agreement. When correctly configured, a smart contract is legally binding and requires the parties to uphold their duties; failing to do so may result in immediate legal action being taken against the party in violation by the smart contract.

(2) **Decentralized Autonomous Organizations :** Communities on the blockchain are known as Decentralized Autonomous Organizations, or DAO. A set of established guidelines that are defined using smart contracts can serve to define these

communities. Every person is bound by the community's rules, and it is up to each individual to uphold those laws. These regulations, which are composed of several smart contracts, collaborate to keep an eye on community actions.

(3) **Application Logic Contracts :** Application Logic Contracts, or ALCs, are blockchain contracts that incorporate application-based code that keeps up with other contracts on the network. They allow communication between various devices, such as when blockchain technology and the Internet of Things (IoT) are combined. ALCs are an essential component of multi-function smart contracts and are often managed by a programme.

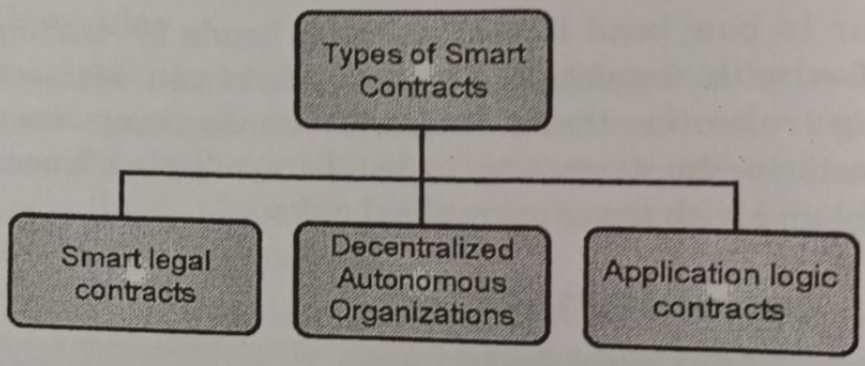


Fig. 5.8.3 : Types of Smart contracts

5.8.2 The Need for Smart Contracts

GQ. What is the need of smart contracts? **(4 Marks)**

- As we all know, smart contracts fall into one of these three types and offer a wide range of capabilities.
- The inherent ability of smart contracts to bring transparency, Time Efficient, precision, safety, cost effectiveness, and trust to transactions, even in sectors that have historically lacked these qualities, drives the need for them.
- A smart contract may be created by anybody and released across the network.

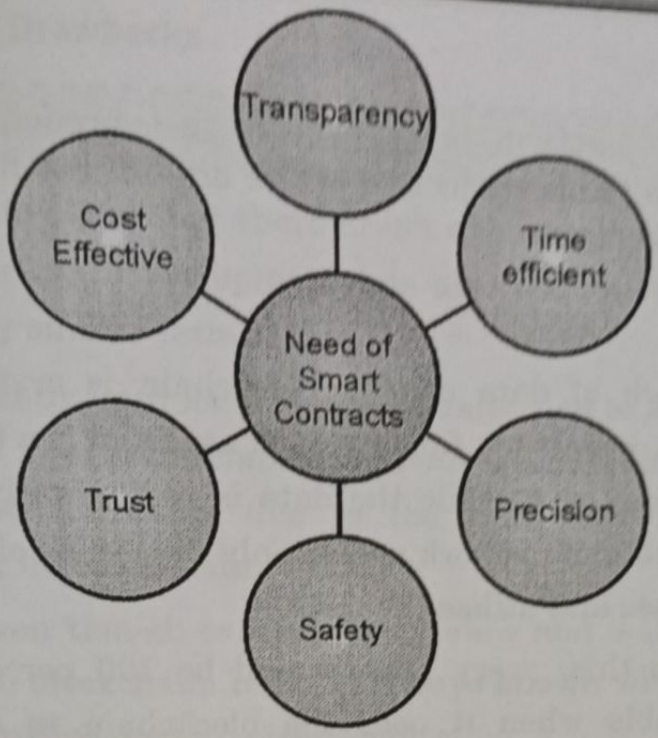


Fig. 5.8.4 : Need of Smart contrcats

Transparency

The parties' understanding of the terms and conditions is complete. Furthermore, users have a very straightforward means of confirming the elements that would affect them and the contract beneficiaries since the execution of the programme or the smart contract requires a few specific inputs.

Time Efficient

- As previously noted, whenever a control variable or a user call activates a smart contract, it starts working right away.
- The blockchain and other sources in the network make data instantly available to the system, so it doesn't take very long for the execution to validate, process, and settle the transaction.
- For instance, transferring property title deeds, which often requires weeks of human verification of mountains of paperwork, may be completed in a matter of minutes or even seconds with the use of smart contract software that verifies the parties and the papers.

Precision

Since the platform is essentially just predefined computer code, there can be no subjective errors and all the findings will be accurate and faultless.

Safety

- Every block of data on the blockchain is cryptographically encrypted, which is a fundamental aspect of the technology. In other words, even while the data is redundantly stored on a large number of network nodes, only the owner of the data has access to see and utilise the data.
- Similar to this, every process will be 100 percent safe and impenetrable when it uses the blockchain to store crucial inputs and results. By giving auditors a native, unaltered, and non-repudiable version of the data chronologically, the same also makes auditing and regulatory affairs simpler.

Trust

- The fact that smart contracts will never display subjectivity or bias in carrying out the agreement implies that all parties involved are totally committed by the outcomes and can completely rely on the system.
- This also implies that the "trusted third-party" necessary in traditional transactions of vital significance is not necessary in this case.

Cost effective

- As seen in the example, using a smart contract has very little expenses. Businesses typically employ administrative personnel whose only responsibility it is to ensure that the transactions they do are legal and comply with laws.
- Duplication of effort was inevitable if there were numerous parties participating in the transaction. Due diligence may be completed concurrently by both parties in smart contracts, effectively eliminating redundancy.

5.8.3 The Drawbacks

GQ. What are the drawbacks of smart contracts. (2 Marks)

- This is not to claim that there aren't any issues with the use of smart contracts. Development has also been slowed down in this area by similar issues.
- It is practically hard for the parties concerned to amend or add new terms to current clauses without considerable reworking or legal consequences due to the tamper-proof nature of everything in blockchain.
- Second, even though everyone may view and watch activities on a public blockchain. It is not always known who the parties are that are engaged in a transaction.
- This anonymity raises concerns about legal impunity in the event that either side breaches the agreement, particularly in view of the fact that present laws and politicians are not very technologically tolerant.

5.9 INTRODUCTION TO SOLIDITY

- The programming language Solidity is used to create a smart contract on the Ethereum network. We will study the fundamentals of Solidity and create our first smart contract, "Hello World," as well.
- Remember that Solidity is not an object-oriented programming language; rather, it is contract-oriented. Each state of a smart contract is unique.
- You may store the data on the blockchain by utilising a state. However, it costs some Gas to store data; it is not free. As a result, anytime you write code on the public blockchain, that each block should use a minimum quantity of gas.
- Initially, there is no setup required to start with Solidity. Ethereum provides an online IDE called Remix, on which you can develop and deploy your smart contract.

5.9.1 Remix Introduction

- When you open the Remix in your browser, you will see the screen as below.

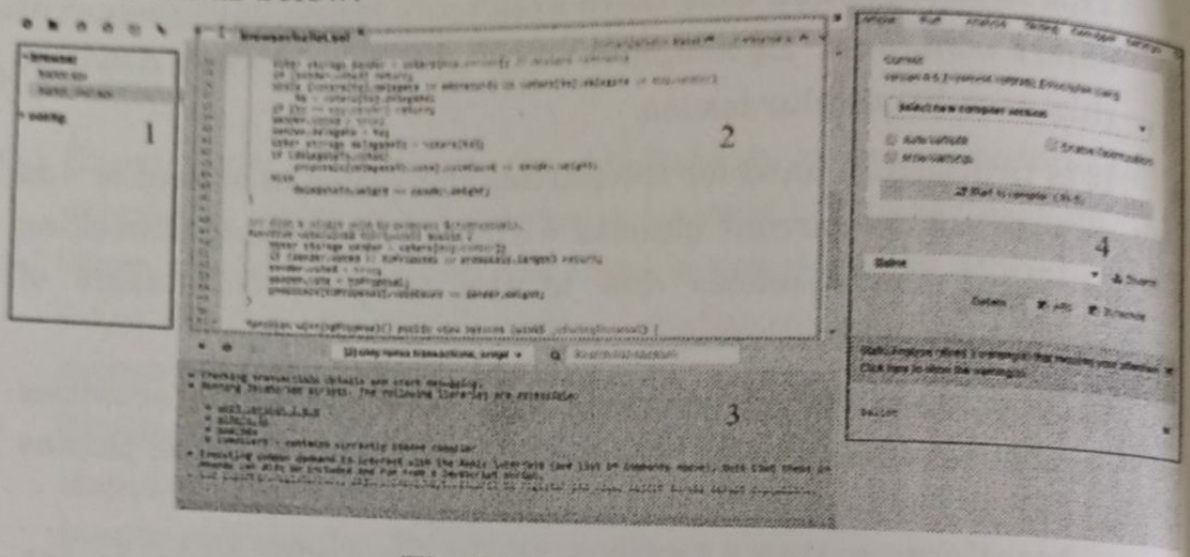


Fig. 5.9.1 : Remix IDE

There are four different sections

(1) **File explore :** We can handle our contract files with file explorer. B y default, all files are saved in your browser; deleting the browser's storage will thus result in the permanent deletion of all the Solidity files you added. Other options available in Explorer include transferring all files to a different instance and exporting all contract files to GitHub.

(2) **Code Editor :** Your primary portion will be the Code Editor, where we will write the Solidity code. Every time the current file is modified, the Editor recompiles the code. Additionally, there are options for font size and syntax highlighting.

(3) **Terminal :** As you work with Remix, the log and debugging information is displayed. You may look up the details of a transaction you made or an event there.

(4) **Deploy And Test :** Options for analysing, compiling, deploying, and testing your smart contract are provided in the fourth part. The auto-compile option is available here. It will compile the smart contract every 5 seconds if you enable that option.

Create a Contract

First, we'll delete the ballot.sol and ballot test.sol default contract files and then, using the code below, add a new file with the name myContract.sol.

```
pragma solidity ^0.5.0;

contract helloWorld
{
  function printHelloWorld() public pure returns (string
memory)
  {
     return 'helloWorld';
  }
}
```

Fig. 5.9.2 : Sample smart contract

Here, we have created one smart contract named helloWorld. Let's understand the contract structure in brief.

Version Pragma

- We should annotate the source file with the compiler version before doing any coding.
- The system will be informed that the code you are about to write should be compatible with the specified compiler, ensuring that your code will not malfunction even in the event that later versions introduce incompatible updates.
- The following uses the pragma version.

```
pragma solidity ^0.4.0;
```

- Such source files cannot be compiled with versions prior to 0.4.0. The following code can be compiled on 0.4.0 or 0.4.x but should not be compiled on 0.5.0 or later since the (^) symbol here denotes the higher version.
- The pragma version can be written in a variety of ways. You may alternatively write as follows for greater clarity; it functions the same as explained.

```
pragma solidity >=0.4.0 <0.5.0;
```

Contract structure

```
contract [contract name]
{
   function [method name]()
   [visibility specifiers] [modifiers] [returns] ([return type(s)]) {
  //code here
}
...
..
}
```

Deploy Contract on Remix

- To deploy the smart contract, go to the "Run tab" right upper corner, and click on the deploy button. Make sure right contract is selected if there are multiple contracts present.

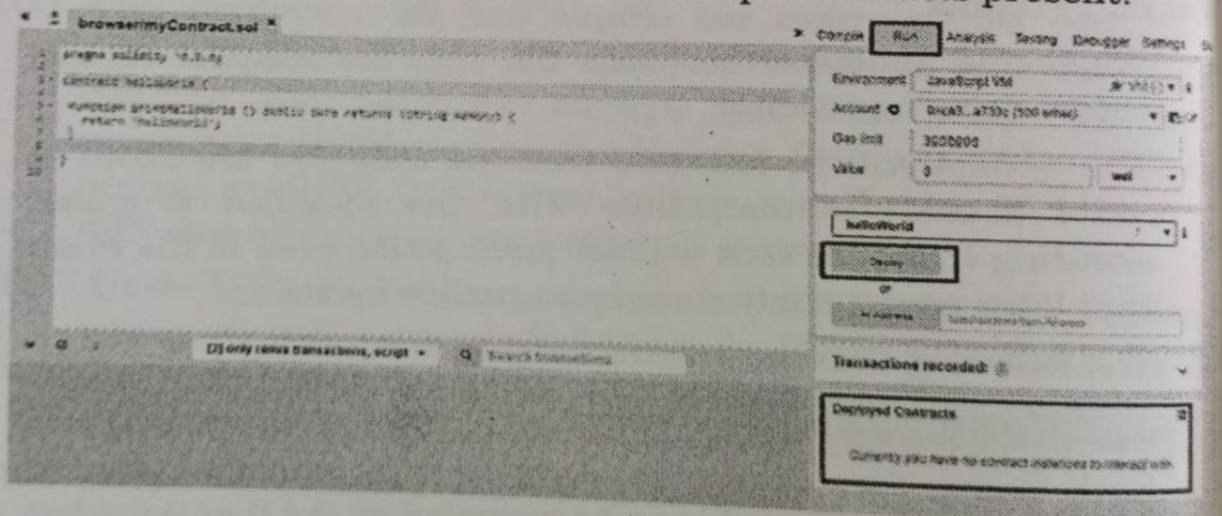


Fig. 5.9.3 : Deployment of smart contract

- As there is no deployed contract at this point of time, "Deployed Contract" section has no information.
- Also note we're going to execute this contract on JavaScript VM, which is the sandbox blockchain environment and it won't be persisted in any kind of state information. Page refresh will start a new blockchain again from the first.

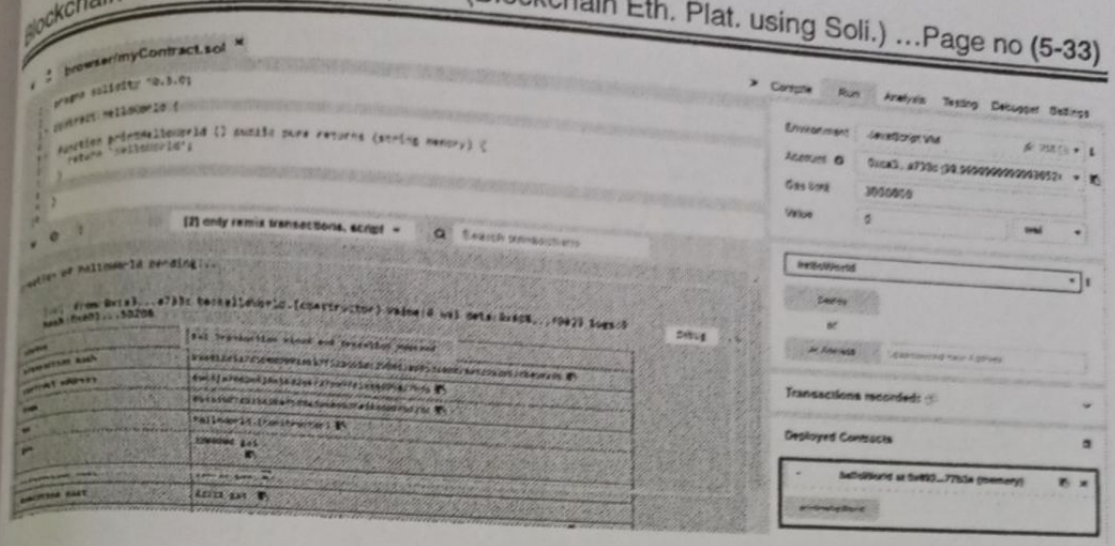


Fig. 5.9.4 : Execution of smart contract

- That section will be updated with contract information after our smart contract has been deployed, and the method should be visible there.
- The information about the transaction we performed is currently updated on the terminal. From the terminal, you can also monitor gas use, contract addresses, etc.

Cost of deployment

- In our case, before deployment, we had 100 ether in my account, and some ether was consumed during deployment. Anything that modifies the state of the blockchain will cost money.

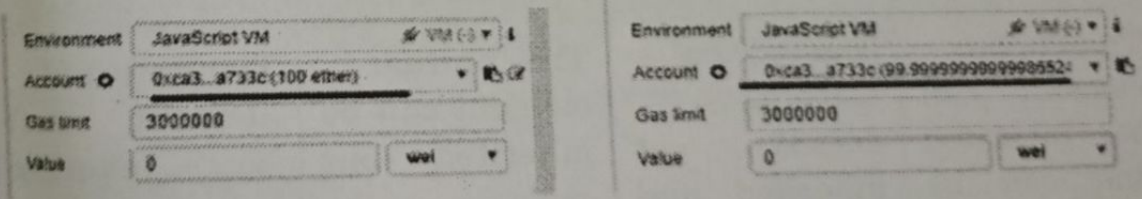


Fig. 5.9.5 : Cost of deployment

Run Contract on Remix

Next to run our method, click on printHelloWorld text which appears as a button.

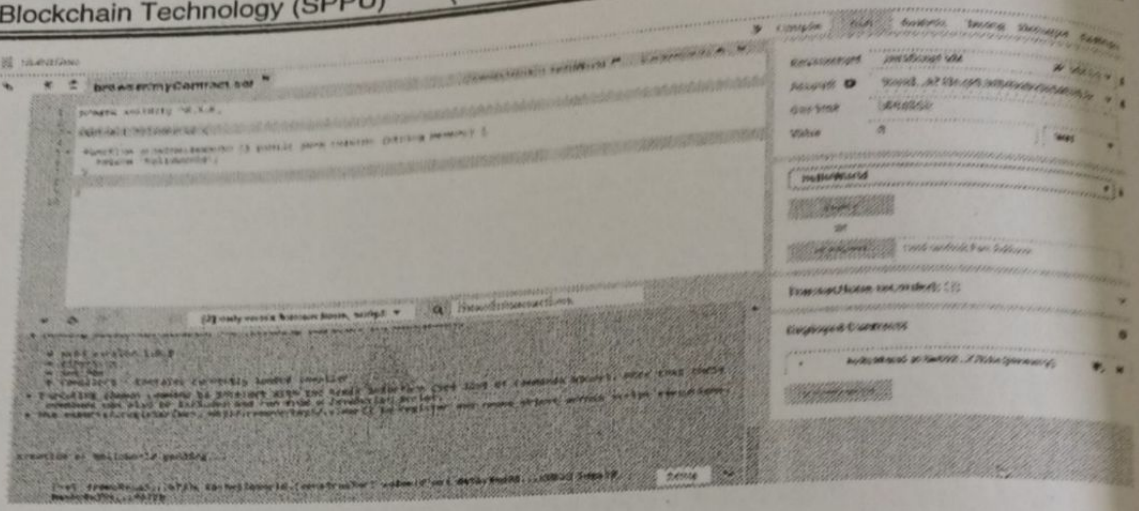


Fig. 5.9.6 : Outcome

5.9.2 Variables in Solidity

GQ. What are different types of access modifiers in solidity. **(2 Marks)**

GQ. What do you mean by State and local variable. Give example. **(2 Marks)**

Access Modifier

Access Modifiers are the keywords used to specify the declared accessibility of a function or a type. There are four access modifiers available in Solidity.

Public	Private	Internal	External
The Public element can be inherited and can be accessed by external elements. All can access a public element.	The Private element doesn't get inherited and can't be accessed by external elements. It can be accessed from the current	The Internal element can be inherited but can't be accessed by external elements. Only the base contract and derived contract can	The External element can't be inherited but it can be accessed by external elements. Current contract instance can't access external

	contract instance only.	access internal element.	element, it can be accessed externally only.

Table 5.9.1 : Access modifiers in solidity

☞ Variable Declaration

Variable declaration in Solidity is a bit different; you have to specify the type (data type) first, followed with an access modifier, and the variable name. If you would not specify any access modifier, it will be considered as a private.

Structure

<type> <access modifier> <variable name> ;

Example

uint **public** a;

In Solidity, there are primarily two types of variables: State variables and Local variables. Like any other language, we consider them as global and local variables. There are some differences, though.

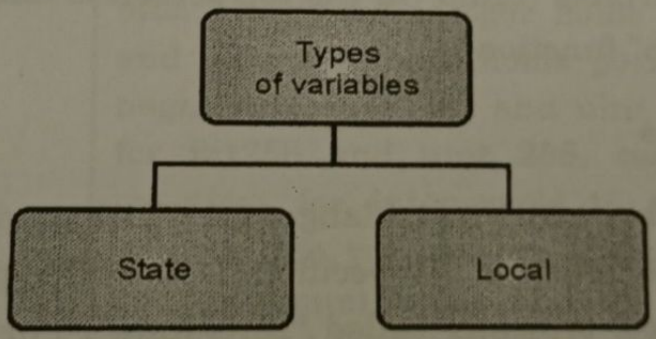


Fig. 5.9.7 : Variable types

☞ State variable

- State variables permanently store the value in contract storage. What would you do if you were using C# or another language and wanted to keep user information for a long time? After establishing a connection with a database server, save the data to the database. Instead of creating a connection, Solidity allows you to simply utilise state variables to store data forever.

- Each method has its own scope, and the State variables should define outside of the scope of any defined functions.

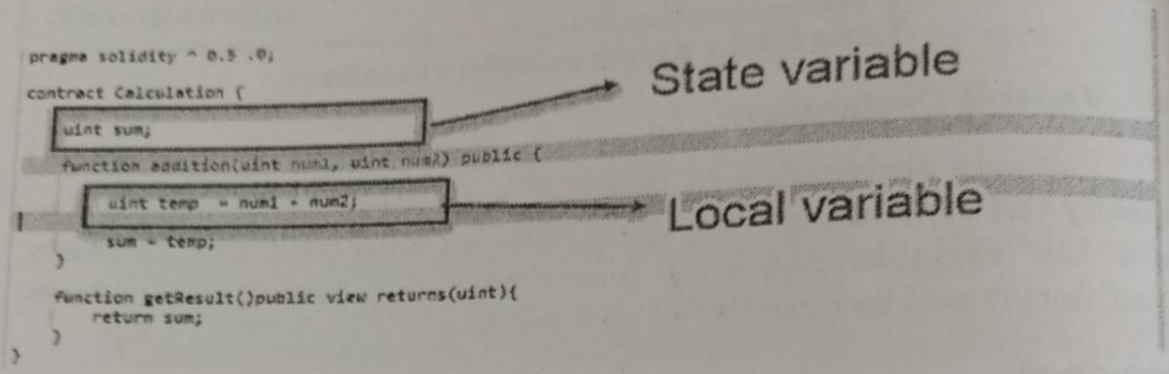


Fig. 5.9.8 : Variables in solidity

☞ Local Variable

- A local variable can only be accessed from inside the function due to its internal context. These variables are typically used to store temporary values while processing or performing calculations.
- The local variable "temp" in the top screen is only used inside the "addition" function.

5.9.3 Types

- Solidity is a statically typed language, which means the type of each variable needs to be specified. Declared types have some default values, typically called “zero-state”. For instance, the default value for bool is false.
- There is no concept of null or undefined in Solidity! So, no need to handle null reference exception .
- There are two kinds of types in Solidity: *value types* and *reference types*. The Solidity data types can be classified according to the data location. If variable store its own data; it is a value type. If it holds a location of the data; it is a reference type.

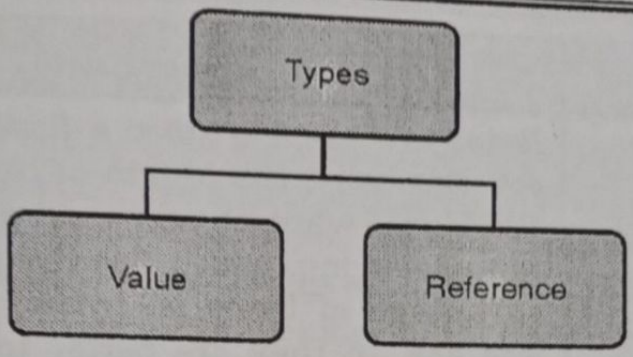


Fig. 5.9.9 : Types

Value Type

These variables are passed by value, it means that they are copied when they are used either in assignment or in a function argument. Following are basic value types.

Types	Description
Booleans	Booleans have possible values as true or false, and can be used with a different operator for conditional checking.
Integers	It stores the values in a rage of 8 bits to 256 bits. Un-signed integer holds positive values and signed integer holds positive as well as negative values. int and uint are the aliases for int256 and uint 256, respectively. Best practices for integers is to specify the bits value while you declare them, so, you would use minimum space and the cost of storing would be lesser. Thus, use uint8 or uint16 instead of using int (uint 256) always.
Fixed Point Numbers	*Fixed point numbers are not fully supported by Solidity yet. They can be declared, but cannot be assigned to or from.* However, you can use floating point number for calculation, but the value coming out of from the calculation should be an integer value.

Types	Description
Bytes and Strings	Bytes are used to store a fixed size character set. Basically, the length of bytes is from 1 to 32. If you want to store more than that, you can use string, which has dynamic length. An advantage of bytes is, bytes1 to bytes32 use less gas, so they are better to use when you know how long data you have to store.
Enums	Enum is a way to create user-defined types, it used to assign names to integral constants, which makes the contract more readable and maintainable. Options in enum are represented by subsequent unsigned integer values starting from 0.

Table 5.9.2 : Solidity variable Types

Reference type

- Reference types do not store the data directly to the variable, instead, it stores the location of the data. With a reference type, two different variables can reference the same location, in such a case; any change in one variable will affect to another variable.
- Since the version 0.5.0 of Solidity, for all complex types, you need to define data location explicitly with a variable.

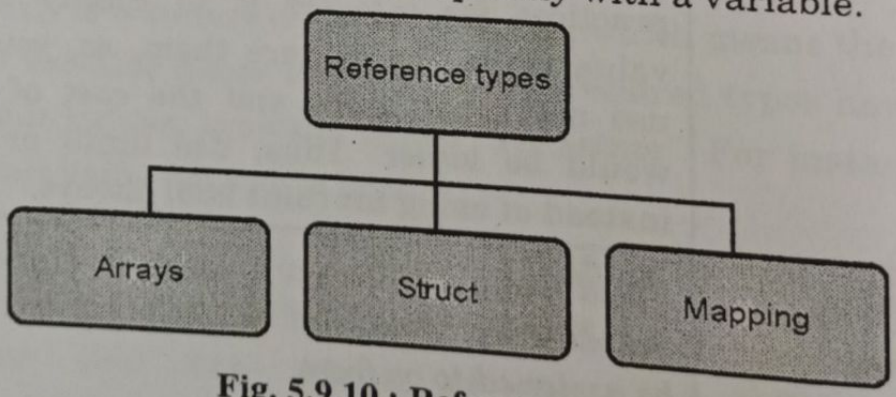


Fig. 5.9.10 : Reference types

Reference types consist of,

(1) **Arrays :** Arrays are the groups of variables of the same type in which each individual variable has a particular location called

index. By using that index location, you can access that variable. The size of arrays can be fixed size or dynamic.

```
uint[5] arrayName;
uint[] arrayName;
```

(2) **Structs :** Structure is the group of different types although it is not possible to contain a member of its own type. Structure is a reference type variable and can contain both - value types and reference types.

Declaration	Example

struct <name of structure> {
<type> variable1;
<type> variable2;
}
	struct User {
	string name;
	uint age;
	bool isValid;
	}

(3) **Mapping :** Mapping types are the most used reference type; they are used to store data in a key-value pair; where the key can be any built-in value types or byte and string. You can think of it as a hash table or dictionary as in any other language, in which a user can store data in a key-value format and data can be retrieved by key.

Declaration	Example
mapping(_KeyType => _ValueType) <access specifier> <name>;	mapping (address => uint) account;

- The main difference between the value type and reference type is Data location. Arrays and Structs have additional data location which specifies where data (value of the variable) should be stored.

5.9.4 Function And Address in Solidity

GQ. List down different types of solidity functions. Give example. **(4 Marks)**

GQ. What are the different kinds of address types in solidity? Explain with example. **(4 Marks)**

In Ethereum smart contract, address and function are broadly used value types.

Function Type

Solidity functions are methods used to perform some specific task. They get invoked during the execution of a smart contract.

Function Structure

function (<parameter types>) {internal|external|public|private} [pure|view|payable] [returns (<return types>)]

- Function parameter types are the input variables. It can be used as any other local variables with an assignment. Return variables are used to return something from the function.
- We can pass return variables with "returns" keyword. In Solidity function, you can also return two or more values.

```
pragma solidity ^0.5.0;

contract Types
{
  uint sum;
  function result(uint _a, uint _b) public returns(uint)
  {
    sum = _a + _b;
    return sum;
  }
}
```

Fig. 5.9.11 : Functions in solidity

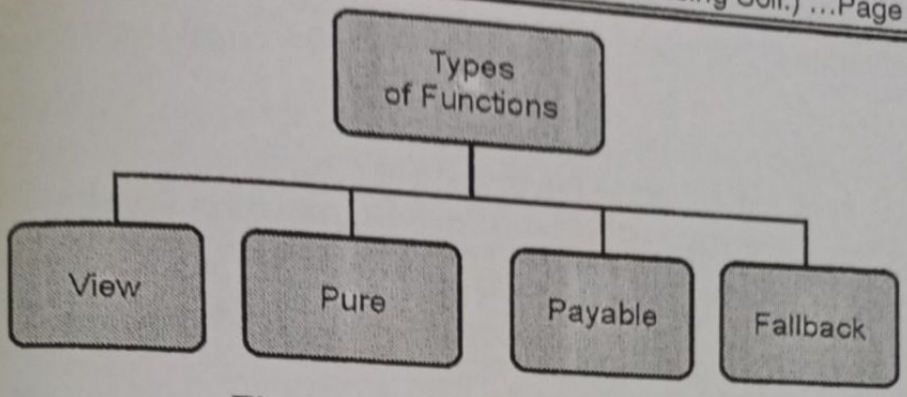


Fig. 5.9.12 : Function type

View Function

```
pragma solidity ^0.5.0;

contract Types
{
    function result(uint a, uint b) public view returns (uint)
    {
        return a + b + now;      //"now"
is current block timestamp in

//seconds in unix epoch format
    }
}
```

Fig. 5.9.13 : View functions

Functions which will not alter the storage state can be marked as a view function. In simple terms, it is used for viewing the state.

Pure Function

A function that does not modify or read the state, is called a pure function.

```
pragma solidity ^0.5.0;

contract Types
{
    function result(uint a, uint b) public pure returns (uint)
    {
        return a * (b + 42);
    }
}
```

Fig. 5.9.14 : Pure functions

Payable Function

- Payable Functions allows to receive Ethers while it being executed, means that, if someone sends some Ethers to the smart contract, and it doesn't have a payable function, then smart contract won't accept ether and transaction will get failed.
- To catch that transfer amount, the smart contract needs to have a payable function.

```
pragma solidity ^0.5.0;
contract Types
{
    uint receivedAmount;

    function receiveEther() payable public
    {
        receivedAmount = msg.value;
    }
    function getTotalAmount() public view returns (uint)
    {
        return receivedAmount;
    }
}
```

Fig. 5.9.15 : Payable functions

Fallback Function

- Solidity supports a parameterless anonymous function called Fallback function. One contract can have only one fallback function, and it must be defined with external visibility.
- Generally, a Fallback Function is used to receive Ether with a simple transfer, when someone called it without providing any data.

5.9.5 Address Type

- On the Ethereum blockchain, every account and smart contract has an address and it's stored as 20-byte values.
- It is used to send and receive Ether from one account to another account. You can consider it as your public identity on the Blockchain.
- In Solidity, address type comes with two flavors, address and address payable.
- Both address and address payable stores the 20-byte values, but address payable has additional members, transfer and send.

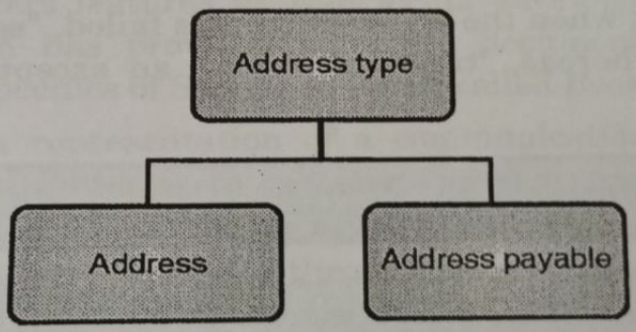


Fig. 5.9.16 : Address type

Address

Address type defines with *address* keyword.

address myAddress;

An address is used to store the value of any address. In below example, "caller" is an address type.

```
pragma solidity ^0.5.0;

contract Types
{
    address public caller;

    function getCallerAddress() public returns (address)
    {
        caller = msg.sender;
        return caller;
    }
}
```

Fig. 5.9.17 : Address type

Address payable

Address payable has an additional keyword "payable"

(1) address payable caller

When we want to transfer some funds to the address, we need to use address payable. There are two members to perform a transfer, send and transfer. Both are doing the same thing, but the difference is; when the transaction gets failed, "send" will return a false flag, whereas, "transfer" throws an exception and stop the execution.

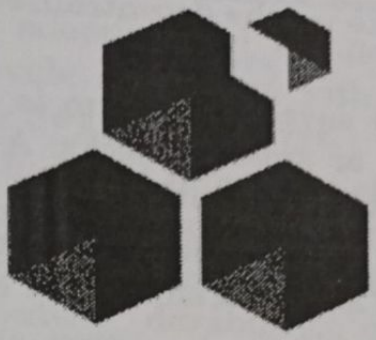
5.10 SWARM

GQ. What is SWARM? Which elements are used in it. **(4 Marks)**

GQ. Enlist and brief about different DApps employing SWARM. **(4 Marks)**

GQ. Write a shot note on SWARM. **(6 Marks)**

- Swarm is a decentralised storage, service, and communication platform created to provide dApp developers with a permissionless, censorship-resistant architecture.
- Swarm, which is based on the Ethereum web3 stack, seeks to offer a variety of Web 3.0 services, including as chat, streaming audio and video, and database hosting.



swarm

- By giving consumers back control over their data, Swarm aspires to become "the operating system of the re-decentralised internet."
- Gavin Wood, a co-founder of Ethereum, developed Swarm after starting to work on the platform's software architecture in 2015. With the help of Vitalik Buterin, a fellow Ethereum pioneer, Wood set out to create a Web 3.0 storage and service solution that would be censorship resistant, DDOS resistance, and provide zero downtime. Swarm, which is built on Ethereum, makes advantage of the blockchain's security and smart-contract features as well as its developer community. Viktor Trón has provided extensive documentation on the ideas and specifics of Swarm in his so-called Book of Swarm.
- Swarm is a representation of a communication and storage network that intends to someday provide the fundamental infrastructure for a completely decentralised internet, with digital services distributed throughout a wide global network of nodes.
- Swarm's front-end user interface is similar to that of the World Wide Web, but the network's back-end is different from traditional internet usage since data is hosted on a peer-to-peer architecture rather than on centralised servers.
- Due to its incentive system, the decentralised infrastructure is intended to be self-sustaining. Users may exchange resources for network services like data storage and distribution, with payments handled by Ethereum smart contracts and powered by the native BZZ currency.

- These elements make up the decentralised storage mechanism used by Swarm:
  (1) **Chunks** : Data saved on Swarm is divided into chunks, which are 4KB or smaller blocks. A 32-byte hash of the content in each chunk identifies it.
  (2) **Reference :** A unique file identifier that facilitates the retrieval of data stored in chunks for clients.
  (3) **Manifest :** A data structure that allows for URL-based content retrieval.
- The Manifest uses the unique reference to identify the appropriate data chunks when a client requests content on Swarm, allowing the nodes containing those chunks to be contacted for retrieval.
- Similar to this, data that is uploaded to Swarm is divided into chunks that are distributed between nodes and given a timestamp for identification.
- Smart contracts control the built-in BZZ incentives, which are distributed to nodes who make their resources accessible for file storage.
- Swarm features built-in redundancy to provide ongoing data accessibility, to guard against nodes leaving the network, and to defend against DDOS attacks.
- The native token of Swarm is called BZZ. It powers network transactions and rewards nodes for their resource contributions. Greater BZZ holdings will influence Swarm governance voting more, similar to other stake-based blockchain governance systems. Swarm airdropped 1 million BZZ, called "The Rise of the Bee," to early testnet members in June 2021.

☞ **Uses**

- Swarm enables dApp developers to safely and effectively store and deliver data and content to blockchain customers.
- The node-to-node message capability, scalable state-channel infrastructure, database services, and media streaming services are all features of the Swarm base-layer architecture.
- In 2020, Swarm started distributing Swarm Grant Waves to

promote network adoption and broaden the ecosystem. The Grant Waves provide developers with mentoring as well as cash assistance for Swarm initiatives.

Swarm has been included into a variety of dApps, supported by the distribution of funding, including:

(1) **Etherna :** A decentralised open source video platform that prioritises content durability, creator rewards, and censorship resistance.

(2) **Zetaseek :** It is a search engine built on the blockchain for individual users that is intended to organise "files, links, and references" in information that has been posted to the Swarm network.

(3) **Scaleout :** A platform for data storage that focuses on end-to-end privacy, the use of DevOps tools, and advanced machine learning.

(4) **Boma :** A communication and engagement platform with a privacy-focused approach that offers event organisers a variety of features like engagement data, CMS capabilities, galleries, and audio and video streaming.

(5) **Giveth :** It is a decentralised platform for non-profit organisations to raise money that offers complete accountability and transparency while facilitating donor communities.

☞ Outlook

Swarm is looking at the possibility of using the blockchain's storage and communication capabilities to build the foundation of the decentralised internet, commonly known as a "world computer."

The Swarm roadmap outlines a variety of short-term objectives in order to achieve that aim, including features and functionality including node splitting, browser compatibility, large-scale network simulations, and support for lightnodes.

5.11 WHISPER (DECENTRALIZED MESSAGING PLATFORM)

GQ. What the three types of resources foundational technologies Ethereum need in order to deliver services? **(4 Marks)**

GQ. What is Whisper? List down the use cases of it. **(4 Marks)**

GQ. Explain any four fundamental features of Whisper. **(4 Marks)**

GQ. Write a shot note on Whisper. **(6 Marks)**

Whisper is an Ethereum's inter-application communication protocol.

- One of the three fundamental requirements for decentralised applications is messaging.
- Compute, Storage, and Messaging are the three types of resources that non-trivial programs usually need in order to deliver services.
- Created with the grand vision of building a global decentralised computing platform, Ethereum serves these basic needs with three pieces of foundational technologies: the EVM (Ethereum Virtual Machine) provides compute, Swarm handles storage of large files, and Whisper is the answer to messaging.

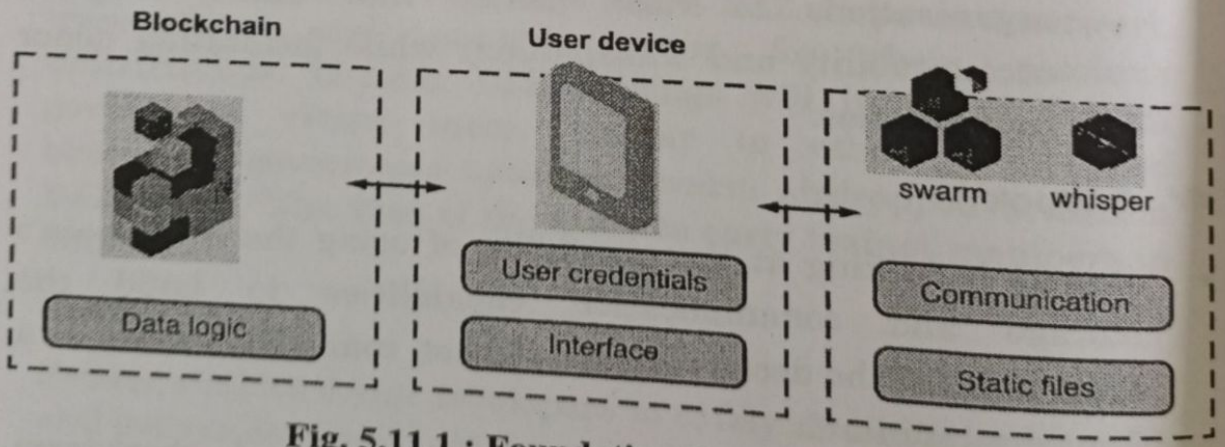


Fig. 5.11.1 : Foundational technologies

- In a nutshell, Whisper is a peer-to-peer (P2P) messaging protocol for decentralised applications (Dapps) to provide Dapp developers a simple API to send and receive messages in almost complete secrecy.

- Due to this concern on privacy, Whisper's creators had to make some unusual trade-offs between performance and privacy. Whisper is therefore more suited to a certain group of use scenarios.

☞ Use Cases for Whisper

What Whisper is good for

- **Publish-subscribe coordination signaling.** Dapps could collaborate with one another by implementing the pubsub pattern with Whisper.
- **Secure, untraceable communication.** Whisper is designed from the ground up to support highly private and secure communication with plausible deniability.

What Whisper isn't good for

- Real-time, extremely low latency communication. It is challenging to ensure latency for time-sensitive applications since Whisper messages may be routed in a probabilistic manner.
- sending massive data sets. Whisper works best for messages that are under 64 KB in size. Another channel built for content distribution, like swarm, would be a better option for bigger messages.

☞ Whisper Fundamentals

Whisper is a programmable messaging protocol that offers dapp creators a great deal of freedom in managing the security and privacy constraints on their communications. Whisper's functionality must be understood, at least at a high level, in order to properly benefit from it.

A network of equal peers

- The Whisper network is made up of decentralised systems connected together as nodes. A node creates this network by utilising the ĐΞVp2p protocol to identify its peers.
- As the basis upon which the protocols in the Ethereum stack are constructed, ĐΞVp2p is a crucial bit of technology in the Ethereum ecosystem. Whisper and its sister technologies

Ethereum and Swarm do not interact despite using the same wire protocol.

- The common use of the same implementation by Whisper and Ethereum nodes is only a coincidence brought on by practicality.

Identity-driven communication

- A Dapp instance can begin receiving messages from a node after it has connected to Whisper by creating an identity there. Although it is required to create two-way communications, an identity is not absolutely necessary in order to send messages. This raises interesting use cases and challenges.
- In general, a Whisper identity is an entity (an individual or a group) that consumes messages. An identity can be viewed practically as the owner of an encryption key.
- Therefore, one has to generate an encryption key in order to receive Whisper messages. For various use cases, symmetric (AES-256) and asymmetric (secp256k1) keys are both supported.
- Encryption ensures that only the intended recipient(s) can access the content of a piece of message. If a node can decrypt a piece of message, then the message is intended for a recipient using that node.

Delivering Messages in Darkness

- Whisper makes a big deal out of its ability to communicate in the dark. This means that two nodes in a Whisper network can communicate without leaving any traceable evidence to traffic analyzers and other peers, even if those peers participated in the message routing. Performance is traded for privacy in order to achieve this.
- Two fundamental requirements must be met in order to achieve complete communication darkness: the content of the message must be unavailable to those who intercept the messages, and communicating nodes must be difficult to

Whisper uses encryption as its primary method of message transmission; it is not feasible to send unencrypted communications using Whisper. Routing information must also be concealed in order to conceal the fact that two nodes are communicating with one another.

Messages are addressed to no one

- The sender Dapp makes an API call to its Whisper node to encrypt the message with a shared symmetric key or the recipient's public key and then enclose the encrypted message in an envelope. A Whisper envelope provides metadata to aid with routing and processing, just like its physical equivalent in the real world.
- Whisper envelopes do not have any recipient information, in contrast to regular envelopes. A typical Whisper envelope looks like this:

```
[ Version, Expiry, TTL, Topic, AESNonce, Data, EnvNonce ]
```

- The content of the data field, which contains the encrypted data, would be the sole piece of information that would be interesting to an attack.
- Being unable to easily identify the recipient of a message makes sense as part of the dark communication approach. Sending the message to every node is the only way to have any chance of it getting to its intended destination without this vital piece of information.

Routing in the blind

- Whisper prevents traffic analysis by routing every communication it sends to every network node.
- Whisper functions similarly to the user datagram protocol (UDP) when it is in broadcast mode. It is hard to determine which receiver the sender is attempting to reach because each node gets a copy of the same message.
- A strong adversary may still be able to know if two nodes are interacting even though it is difficult to tell which recipient a message is directed to if they are able to control all except the two conversing nodes.

- In this case, the adversary will be able to determine that communication has happened between nodes A and B if node A delivers a message to node B.
- Such an attack can be defeated by introducing noise into the network by having well-behaved nodes sending junk messages encrypted with a random key into the network.

Probabilistic message filtering

- A node must be able to decode the message in order to determine whether a message is meant for an identity using its service.
- A node must utilise every key it has in its possession before it can decide if a piece of message is transmitted to its users since the envelope carries no information about the intended receiver. Decryption is a costly task! In most real applications, it is impossible to decode all incoming messages because to the fact that each node will get a copy of every message sent across the network.
- Each communication must be linked to a subject in order to avoid this issue. An identity registers the topics it's interested in by using its encryption key to create a message filter on a node.
- This efficient probabilistic filter, known as a bloom filter, can tell to a very high degree of certainty (false-positives are possible) if a piece of message belongs to a topic of interest.
- A node will only attempt decryption if a filter signals a possible match.

Quality of Service Assurance

- It is simple to assume that Whisper is vulnerable to denial of service (DoS) attacks since every Whisper message is sent to every node that can receive it.
- At least two methods can be used to initiate an attack :
  (i) **Flood Attack :** Repeatedly send messages into the network
  (ii) **Expiry Attack :** Make messages hang around for a long time by setting a long TTL (Time-to-Live) on the envelope

- The Whisper node and message filters prevent flood attacks by demanding proof-of-work (PoW) calculation from the sender and providing the result as the EnvNonce field in the message envelope. If the PoW is too low, a node could decline to accept a message. The node may not require the same level of PoW that message filters choose.
- A message rating system that computes a message rating by factoring in PoW, message size, and TTL prevents expiry attack.
- The rating's requirements are rather simple :
  (i) Smaller messages have higher ratings
  (ii) Messages with higher PoW have higher ratings
  (iii) Messages with lower TTL have higher ratings
- A message's rating determines both its forwarding priority and the amount of time it will be kept in the system.
- Therefore, it is in the sender's best interests to ensure that the messaging rating is as high as is required to accomplish the intended goal. For instance, a node may delete up messages that it deems to be of low rating when its message pool is about to reach its memory limit. By using this grading system, a DoS attack's impact is reduced.

Barriers to Wider Adoption

- Despite how fantastic Whisper is, hardly as many people really use it.
- This is partially because of Whisper's design decisions and partly because there are other communications options available inside the Ethereum ecosystem.

☞ Key Management

- Currently, Whisper relies on Whisper nodes preserving users' secret keys in order to decode communications addressed to them. Because of this manner of operation, it is impossible to employ "zero client" providers like Infura, one of the most well-known Ethereum infrastructure services, which operate under the tenet that wallet programmes like MetaMask should be in charge of key management.

- This restriction can be lessened by operating Whisper nodes concurrently with the wallet application on the user's device. For instance, a trading application built in Electron may use Whisper to implement order signalling and communicate with other Whisper nodes.
- The basis for alternative Whisper implementations that use protocols other than TCP and UDP, which ĐΞVp2p requires to communicate with standard Whisper nodes supported by Go Ethereum (Geth), or Parity, is being laid by some intriguing advances in this area, headed by Guillaume Ballet.

☞ Disabled by Default

- Whisper is currently an opt-in service. It must be enabled at the command line in order to be used. Whisper is therefore not active on the vast majority of Ethereum nodes. Whisper is still an experimental protocol, thus this deliberate choice to keep it off by default is a smart one.
- Whisper is still only a proof-of-concept protocol, but it has already been adopted in real-world settings. The largest production Whisper user at the present is arguably Status, an intriguing Ethereum client project that leverages Whisper to provide conversation.

Chapter Ends...

❑❑❑

Unit 6

CHAPTER 6

Blockchain Case Studies

University Prescribed Syllabus

Prominent Blockchain Applications, Retail, Banking and Financial Services, Government Sector, Healthcare, IOT, Energy and Utilities, Blockchain Integration with other Domains.

6.1 PROMINENT BLOCKCHAIN APPLICATIONS

GQ. List and explain the applications of Blockchain technology.
GQ. Write a short note on: Applications of Blockchain technology.

- Blockchain is most promising and trustworthy distributed database technology implemented in various applications.
- A blockchain is essentially a distributed database of records or public ledger of all transactions ordigital events that have been executed and shared among participating parties.
- As it is discussed in previous chapters, Blockchain technology has become an active area of research and a technological option form any businesses and industrial communities.
- With its distributed, decentralized, and trust less nature, blockchain can provide businesses with new opportunities and benefits through increased efficiency, reduced costs, enhanced integrity and transparency, better security, and improved traceability

6.2 BLOCKCHAIN INTEGRATION WITH OTHER DOMAINS

This section explains in detail the applications in which blockchain has been used in recent years and the areas in which blockchain can be used in the future, with some pictorial representations.

6.2.1 Blockchain in Retail, Banking and Financial Services

GQ. How Blockchain technology can be used in financial and banking services?

- For the banking and financial services markets, the Blockchain technologies provide various attractive features.
- Financial institutions and banks no longer see blockchain technology as threat to traditional business models.
- The world's biggest banks are in fact looking for opportunities in this area by doing research on innovative blockchain applications.
- Blockchain networks are usually different in their ability to secure that parties involved all have reliable and similar information.
- Bitcoin, the first popular digital virtual currency that presented a fundamental change in approaches.
- While using Community Validation to support distributed ledger technology, blockchain technology decentralized currency command, as a result, customer trust moves from humans to computers.
- Blockchain smart contract solutions are going to challenge the financial, legal and government sectors.
- With distributed ledger technology, smart contracts may automatically and in real-time track the performance of legal transactions.
- Bitcoin's blockchain requires the availability of a consensus algorithm operating on hardware spread across the globe.
- Bitcoin transactions are implemented into the blockchain, and

a computationally intense proof-of-work (PoW) function called mining is needed for this process.

- Bitcoin mining has grown into a highly vertically integrated network with one or more servers operated by individual companies, product design, and hardware maintenance.
- Today's Bitcoin miners send us a snapshot of the future of global computing with Application Specific Integrated Circuit (ASIC) clouds.

6.2.1.1 Private Securities

- It is very expensive to take a company public. A syndicate of banks must work to under write the deal and attract investors.
- The stock exchanges list company shares for secondary market to function securely with trades settling and clearing in a timely manner.
- It is now theoretically possible for companies to directly issue the shares via the blockchain.
- These shares can then be purchased and sold in a secondary market that sits on top of the blockchain.
- Some examples are as follows :

(1) **Medici** is being developed as a securities exchange that uses the Counterparty implementations of Bitcoin 2.0. The goal here is to create a cutting-edge stock market. Counter party is a protocol that implements traditional financial instruments as the self-executing smart contracts. These smart contracts facilitate, verify, or enforce the negotiation of contract and eliminate the need for a physical document. This eliminates the need for an intermediary, such as broker, exchange, or bank.

(2) **Block stream** is an open-source project with focus on side chains-interoperable blockchains-to avoid fragmentation, security and other issues related to alternative crypto-currencies. Uses can range from registering securities, such as stocks, bonds, and derivatives, to securing bank balances and mortgages.

(3) **Bitshares** are digital tokens that reside in the blockchain and reference specific assets such as currencies or

commodities. The Token holders may have the unique feature of earning interest on commodities, such as gold, and oil, as well as dollars, euros and currency instruments.

6.2.1.2 Insurance

- Traditional insurance policies are often processed on paper contracts, which means claims and payments are error-prone andoften require human supervision.
- Compounding this is the inherent complexity of traditional insurance, which are consumers, brokers, insurers and reinsurers, as well as insurance's main Product risk.
- As a kind of distributed ledger of the blockchain, it improves insurance industry efficiency from four respects : fraud elimination, claims automation, data analysis with the Internet of Things (IoT), and Reinsurance.
- Assets which can be uniquely identified by one or more identifiers which are difficult to destroy or replicate can be registered in blockchain.
- This can be used to verify ownership of an asset and trace the transaction history. Any property (physical or digital such as real estate, automobiles, physical assets, laptops, other valuables) can potentially be registered in blockchain and the ownership, transaction history can be validated by anyone, especially insurers.
- For example, *Ever ledger* is a company which creates permanent ledger of diamond certification and the transaction history of the diamond using blockchain.
- The characteristics which uniquely identify the diamond such as height, width, weight, depth, color etc. are hashed and registered in the ledger.
- The verification of diamonds can be done by insurance companies, law enforcement agencies, owners, and claimants.
- *Ever ledger* provides a simple to use web service API for looking at a diamond, create/read/update claims (by insurance companies) and create/read/update police reports on diamonds.
- Other financial-oriented areas may include commercial

property and casualty claims processing, syndicated loans contingent convertible bonds, automated compliance, proxy voting, asset rehypothecation, and over-the-counter market.

Finally, blockchain adoption by the financial sector will eventually lead to cost savings in areas like central finance reporting, compliance, centralised operations, and business operations.

6.2.2 Blockchain in Government Sector

GQ. Write a short note on: Use of Blockchain technology in Government sector.

- Blockchain technology plays a vital role in the development of social and governmental activities for e-governance.
- In the current system, data such as employee IDs are stored in a centralized database with multiple duplicate servers. However, this centralized system suffers from many cyber attack issues, such as denial of service (DoS) and distributed denial of service (DDoS).
- Blockchain technology can initialize many flexible services, such as voting records, property registrations, patent exchanges, criminal records, and licenses for driving and other activities.
- In a distributed system, shared and approved transactions are stored, and each block contains a hash value to ensure its integrity in the ledger.
- In government sector, verifying authenticity of the document can be done using blockchain which eliminates the need for centralized authority.
- The document certification service helps in Proof of Ownership (who authored it), Proof of Existence (at a certain time) and Proof of Integrity(not tampered) of the documents.
- Since it is counterfeit-proof and can be verified by independent third parties these services are legally binding.
- Using blockchain for notarization secures the privacy of the document and those who seek certification. By publishing proof of publication using cryptographic hashes of files into

block chain takes the notary time stamping to new level.

- It also eliminates the need for expensive notarization fees and ineffective ways of transferring documents.
- The following are different application areas where blockchain can be involved in government and societal activities.

6.2.2.1 Individual Identity

- In the traditional system, personal records are stored separately in different systems, such as an employment file, educational file, and business file.
- The information about an individual that is stored in a government database maybe different from the information stored in other databases.
- This problem can be solved by using blockchain technology, where information about a person is permanently recorded at a single point in time and can be made available for anyone, or any institution, that wants it.
- Nowadays, verifying the identity of refugees and immigrants is a serious problem in the world because their records may be lost or difficult to access.
- With the help of a blockchain-based digital identity, records can be accessed by anyone in any location.

6.2.2.2 Land and Property Registry

- Ownership of property, such as a house or land, can be transferred using a blockchain-based smart contract.
- The rules of the transaction are maintained by the smart contract.
- The buyer keeps the total cost of the property in the blockchain and distributed system.
- Then, the seller can receive the transferred money, and this transaction is confirmed before the property is handed over.
- After that, the registration of the property is updated in the blockchain.
- For example, the valid owner of a lost car can be found by viewing the car's transaction history in the ledger.

- Only the valid owner can sell the car, and ownership must be confirmed. Blockchain technology rapidly confirms the identity of the owner and buyer and the buyer's financial status.
- It keep strack of the transaction history so that unauthorized or fraudulent persons cannot steal the car.
- This can reduce human involvement in registrations for cars or land and reduce the possibility of errors.

6.2.2.3 Birth and Marriage Certificates

- Some vital records such as birth, marriage, and death certificates can be permanently stored using blockchain technology.
- This ensures that the total number of citizens listed in the automated system cannot be changed.

6.2.2.4 Vehicle Registrations

- If someone wants to buy a used car, its mileage record scan be analyzed by its vehicle identification number (VIN)using blockchain technology.
- Because the mileage and history records of the car are permanently stored, the seller cannot cheat the buyer.

6.2.2.5 Electronic Voting System

- Electronic voting systems have been widely studied for decades to reduce the costs of conducting elections while maintaining the fairness of elections in accordance with the standards of safety, privacy, and regulation.
- A modern blockchain-based electronic voting system that discusses some of the existing system drawbacks and evaluates certain of the common blockchain technologies for creating an e-voting system based on blockchain.
- The system is decentralized and does not depend on self-belief. Each voter registered will be able to vote via any Internet-connected device.
- The Blockchain can be confirmed and distributed to the public, in such a way that nobody can misuse it.

- In order to achieve a decentralized e-voting framework without a trusted Third Party, the key idea is to combine block chaining with hidden exchange scheme and homomorphous encryption.
- This offers a public and open voting process while ensuring that the identity of the voter, data transmission privacy and voting verification during the billing phase are secured anonymity.
- The method of democratic and open voting ensures the confidentiality of the identity of the elector and data transmission privacy and vote verification during the billing process.
- Blockchain technology is useful for voting systems, especially in national elections.
- A voter can cast a vote only once and check whether it has been correctly recorded or not.
- This process ensures data integrity. The use of a consensus protocol in the distribution and authentication process makes fraud easy to detect and prevents any type of alterations.

6.2.3 Blockchain in Healthcare

GQ. State and explain different aspects of healthcare where Blockchain technology can be used.

GQ. What are the important challenges in adopting Blockchain technology in the healthcare domain?

- Blockchain is an emerging enabling technology that can provide solutions for real world problems including healthcare which is considered as one of the basic human rights.
- In the last few years, blockchain technology has gained reasonable confidence as a smart new trusted distributed system for performing and storing transaction record in the form of distributed ledger.
- However, according to the healthcare perspective, the stakeholders are more involved in discussing and questioning blockchain as a platform rather than focusing on healthcare issues that can be solved by blockchain.

- Blockchain must be transparent in the field of healthcare and scalable, secure and data privacy must be protected.
- The healthcare blocks primarily contain health documents, images, and documents.
- This includes a network of hospitals funded, managed, and controlled by a central organization.
- Data from patients are one of the most informative and important factors of healthcare.
- The medical record of a patient is usually spread over many networks owned and operated by one or more health providers.
- In order to digitalize patient data into what is generally referred to as the electronic medical record(EMR), the synthesis technology has developed.
- Due to many issues such as security and privacy, there are many hurdles to the exchange of EMRs with several healthcare providers and related organizations.
- Blockchain can be used to provide safe EMRs and other exchanging of health information between various vendors.

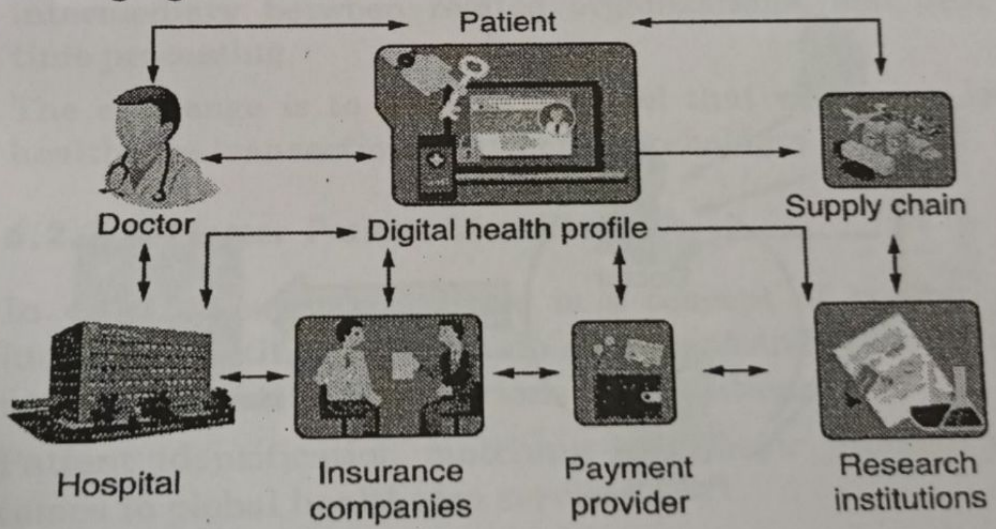


Fig. 6.2.1 : Blockchain in Healthcare

- Fig. 6.2.1 shows the conceptual ecosystem for the use of blockchain technology in healthcare.
- Fig. 6.2.1 highlights various stakeholders involved including patient, doctor, insurance companies, payment provider, and research institutions.

- Blockchain can facilitate the interoperability of updated digital health profile of patients in a timely manner alongwith other benefits, such as, patient data security, protecting patient's identity, and the coordination of care.
- following subsections highlight the major healthcare issues that can be addressed by the blockchain technology.

6.2.3.1 Secure Health Information Exchange Between Stakeholders

(1) Ensuring Privacy

- The ensuring privacy of healthcare record is one of the major concerns while exchanging information between various stakeholders, such as, doctors, local and international research and development units, health organizations, government sectors, patient's history, and information forwarded to their caregivers.
- Fig. 6.2.2 depicts the healthcare transactions using Blockchain.

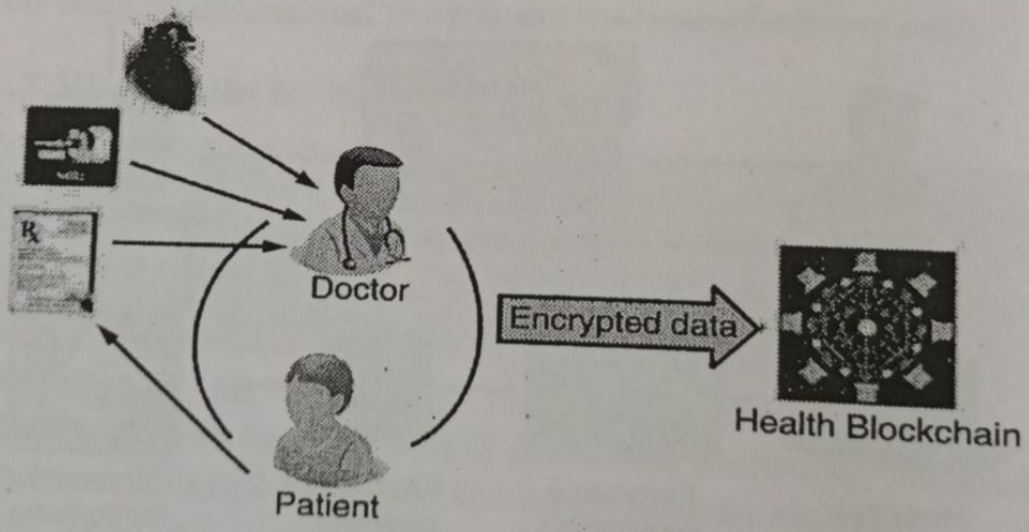


Fig. 6.2.2 : Healthcare Transactions using Blockchain

(2) Improve Integrity of Health Records

- Improving or maintaining the high level of data integrity is critical in healthcare as the prescription, lab test and major operation are suggested based on these records. Errors in the record could lead to wrong diagnosis and inappropriate care.

- These errors can be produced in electronic systems during exchange, sharing, and storing record.

(3) Decentralized Health Insurance Records

- Most countries are following health insurance system in which insurance is used to pay the expenses against the healthcare services that are provided to the patient, both locally and internationally.
- Various models of health insurance are followed all over the world but mostly this insurance is provided through social insurance system or private insurance companies.
- Decentralization of these insurance record is critical for ensuring health services to patients irrespective of their resident country.

6.2.3.2 Cost of Healthcare Transactions

- In healthcare system transaction, there are various factors that produces cost including redundant transmission cost, intermediary between related organizations, and near real-time processing.
- The challenge is to propose a model that will incur low-cost healthcare transactions between stakeholders.

6.2.3.3 Master Patient Identifier

- In enterprise systems there is a concept of master patient index or identifier to maintain consistent and accurate medical record of patient across various organizations.
- Patient identification matching is a major problem when it comes to global healthcare services.
- Identification matching in healthcare transaction, such as, exchange of healthcare record, can violate the integrity of medical record and this could have severe consequences.

6.2.3.4 Limited Access to Health Records

- In terms of healthcare information exchange, limited access to health record is provided to maintain security; however, this

also creates hurdles in researching about the analyses of various diagnosis and effects of certain prescriptions.

- In general, it is an obstacle to further ethical research and development.

6.2.3.5 Conflicting or Inconsistent Rules and Permission Related to Healthcare

- This highlights the issues of allowing right health organization to access required patients medical record at the right time.
- There are different regulations by countries related to the access-rights of patients' medical record and this introduces challenges related to the availability of medical record for right stakeholder at the desired time.
- The smart contract concept in blockchain can reasonably address this issue.

6.2.3.6 Interoperability with Healthcare Data and Applications

- There are challenges of interoperability when it comes to access, exchange, and storage for healthcare application and data.
- It first requires establishment of trust between various stakeholders and then assurance of secure access and transactions.
- The blockchain has the capability to address these challenges.

6.2.3.7 Challenges in using Blockchain as a Solution in the Healthcare Domain

- Despite the benefits, when applied in the real world, blockchain faces several challenges.
- Each of blockchain's built health systems has its own challenges.
- Speed, immutability, absence of expertise, legislation, healthcare infrastructure, and cost of all in considered healthcare.

In the blockchain-based healthcare system following are the key challenges :

(1) Security and Privacy

- A key concern of healthcare blockchain applications is that despite the use of the technology, personal identities maybe discovered because of confidential data which has been collected about the same individual patients would be tied to it.
- Moreover, there is a possible risk of infringements of protection that could result from deliberate malicious attacks by criminal groups or even government entities on the healthcare blockchain that could affect patient privacy.
- There have been many studies of crypto currencies strong attacks against the blockchain networks.
- The personal keys used in blockchain for encryption and decryption of data are also likely to pose a potentially unauthorized access to the saved health information.

(2) Immutability

- Although blockchain offers transparency via immutable auditrecords, immutability disappears, if poor quality or inaccurate information is entered into the chain for malicious purposes.

(3) Scalability

- A big obstacle to blockchain-based healthcare solutions is the high volume of data. With high volume biomedical data, there is likely to be serious performance issues.
- Another disadvantage is that blockchain-based processing can add substantial latency.
- So, as an example, all nodes on a network must agree to validate the process on the current Ethereum blockchain.
- It requires significant processing, particularly if the load is large.

(4) Interoperability

- The interoperability problem is due to the fact that there is not yet a healthcare-specific blockchain standard; thus, various healthcare applications might not be able to communicate with each other.
- Consider for example, the two medical monitoring apps, one of which were built on the Ethereum and the other on Hyperledger, it's difficult to interchange information between platforms.

(5) Speed

- Not all of the existing IoT facilities are capable of executing encryption algorithms easily and capably.
- Buying strong computing equipment is a huge investment for healthcare organizations before enabling blockchain use.

(6) Lack of Expertise

- The public and patient populations lack experience, awareness, and faith in blockchain.

(7) Healthcare Infrastructure

- In such a blockchain-based structure, incentive to keep nodes alive in one nation calls for major socio-technical changes and alignments.

(8) Cost Undisclosed

- No one is specific on the up-front costs of implementing and keeping a blockchain-based framework.
- The cost of maintaining the existing framework is balanced by the benefits of migrating to the blockchain.

6.2.4 Blockchain in Internet of Things (IoT)

GQ. Write a short note on: Application of Blockchain technology in Internet of Things (IoT).

- In recent years, IoT-based applications have gained popularity in various fields such as smart cities, healthcare, education, government, and social applications as it is discussed in previous sections.
- In IoT-based networks, many datasets are available publicly for all users.
- Blockchain is used to guarantee the privacy and integrity of these shared data sets.
- A huge volume of data is captured on the IoT platform by a cloud service. Many nodes are connected with a gateway in small networks. In a large network, many nodes are also connected with gateways based on the cluster.
- Each node contains a pair of public and private keys. Every node in the network uses its public key at the time of registration and creates a digital profile record on the blockchain.
- When a node receives a transaction, the private key is used for creating a digital signature, which is verified by the gateway.
- Different IoT devices are connected with the blockchain to synchronize and maintain a protocol for interacting with the blockchain network.
- Various intelligent devices and objects communicate with each other in an IoT environment to perform various tasks.
- Malicious activities in the network can occur through various types of attacks during this process.
- Blockchain technology for encryption and secrecy has been commonly used in the IoT network for this purpose.
- Blockchain in IoT will increase the power of the existing system, which can serve as a building block for creating new business models.
- There is limited protection in the modern IoT world when transmitting private information between IoT devices.
- A hacker may use the transaction data to access private data on devices and commit fraud.
- IoT tools, on the basis of computation efficiency, bandwidth, and resource usage, are detected and validated during transactions.

- After the validation process has been completed, the miner nodes are used in the blocks for storing data.
- The systems are synchronized with the miner nodes to get the latest information on the data blocks.
- Various protocols are applied in the blockcha in-powered IoT systems for the synchronization process.
- Following are some of the application areas where Blockchain can be used along with Internet of Things.

6.2.4.1 Smart City

- A smart city is a diverse IoT-based network system that offers several applications and security solutions to citizens.
- Smart cities rely on the assembly, analysis, and digitalization of information. Fig. 6.2.3 shows the use of blockchain technology with Internet of Things (IoT).

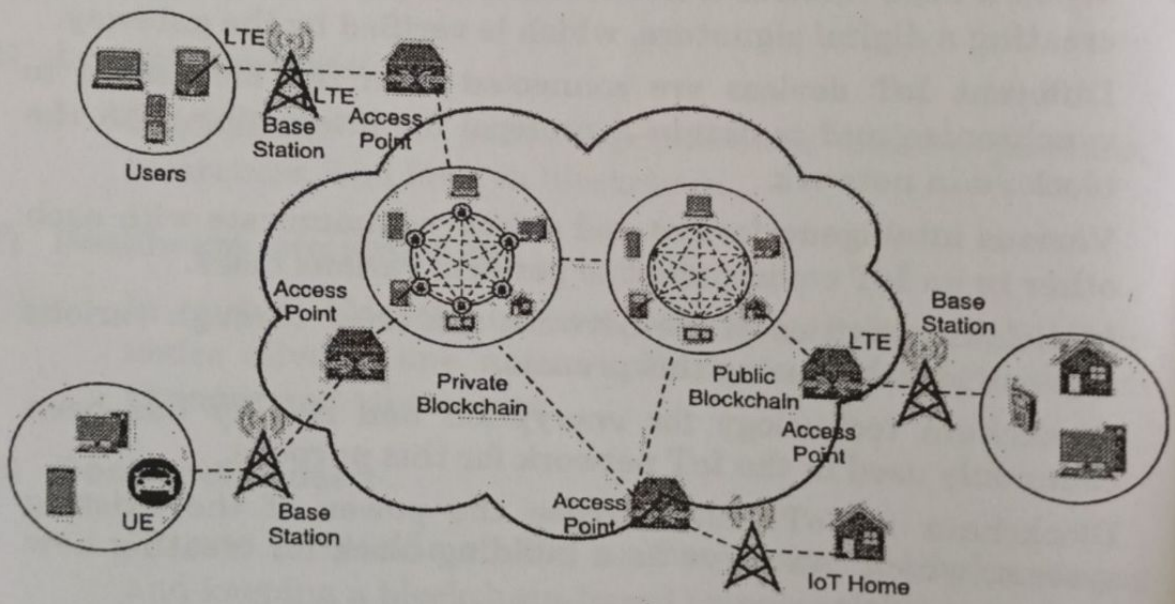


Fig. 6.2.3 : Blockchain with Internet of Things (IoT)

6.2.4.2 Industrial Sector

- Blockchain and IoT have opened numerous new opportunities and provided hope for improved productivity, efficiency, and transparency in the industrial sector.

- IoT provides real-time data by using sensors. Because the prices of sensorsare falling day by day, sensors are becoming affordable for many industries.
- Blockchain is combined with IoT for sharing real-time data among users in a decentralized and distributed manner.

6.2.4.3 Supply Chain

- The supply chain is an area in which many business problems occur, such as late deliveries, absent suppliers, and untrust worthy intermediaries.
- There is a lot of paperwork involved in the shipping procedures for supplies. In addition, there are many losses of supplies and delays in deliveries of them.
- These problems can be resolved by using blockchain, which removes the dependency on an intermediary.
- IoT devices can be connected to components or products, and the blockchain captures the data from these devices.
- Using blockchain, the location of the shipping container and the time stamp of the transaction can be captured.
- This eliminates the need for paperwork, and delays can be minimized. Digitization creates more opportunities for many companiesand drives the supply chain.

6.2.4.4 Autonomous Vehicle

- The autonomous vehicle is an attractive technology that may offer benefits for years to come.
- Sensors are attached to vehicles and all their information is captured on the IoT platform, which is connected to a blockchain.
- The data can show when a car needs to be refueled or repaired due to an engine breakdown or other problems.
- Because the blockchain keeps a permanent record of each transaction, the trust between the manufacturer and the consumer increases.

6.2.4.5 Plane Asset Manufacturing Management

- Blockchain and IoT can be used to predict and prevent failures of manufacturing products. IoT sensors can identify failures due to heat or extreme vibration.
- Proactive management with blockchain used with IoT can prevent these failures.
- This allows a factory to produce more reliable products.
- Recording and maintaining huge volumes of data can be handled by digitization with blockchain without the involvement of a third party.

6.2.4.6 Smart Agriculture

- Information and Communication Technology(ICT) plays an important role in improving the technologies of agriculture.
- ICT facilitates the e-farming system that promotes business efficiency and performance and reduces ambiguity and risks.
- The aim of e-agriculture is to allow farmers to share knowledge to help farmers become more successful, smarter and avoid possible risks.
- Blockchain will help use and promote this exchange of information.
- Introducing blockchain into efarm systems helps to build faith between participants who share their knowledge and use the e-farming servers provided to improve their agricultural operations.
- Such programs are designed to improve cost efficiency, enhance food security and reduce ambiguity and risks.
- In regard to main agriculture firms, blockchain technologies may also be used to report honey adulteration activities, to support intelligent pollution contracts and to improve the beehive insurance market in agriculture-related industries, like bee industries.

6.2.5 Blockchain in Energy and Utilities

GQ. Describe the use of Blockchain technology in energy and utilities.

- The energy industry is working on new models and mechanisms to improve its service delivery to customers.
- Similarly, consumers favor having new methods to buy energy and understanding the origins of their energy purchased.
- Blockchain-based smart contracts can substantially accelerate a significant development in the energy industry, microgrids.
- A microgrid is defined as, the cluster of multiple distributed generators (DGs) that supply electrical energy to consumers without any shortage.
- Instead of the exclusive reliance on a power factory that supplies electricity for a district, amicrogrid enables all electric power consumers to manage their usage and possibly produce and sell energy using solar panels or any other energy alternative methods.
- Residents can sell extraneous energy to other residents or back to the larger grid.
- Blockchain can facilitate microgrid-related transactions. Blockchain-based smart contracts enable the application of power-exchange restrictions and regulations, payments management, and direct interaction between users, without a centralized microgrid authority.
- In supporting unmanned aerial vehicles and connected electric vehicles, an important issue is how to exchange energy.
- A blockchain-based energy exchange method has been proposed to support a secure and energy-efficient transportation system.
- Blockchain is used to approve the energy requests of electronic vehicles in a delegated manner, in which the mining node verifies the validity of each request.
- In addition, a software-defined backbone controller is used.
- The potential applications of blockchain in the energy sector are far-reaching and may have an enormous impact both in terms of processes as well as platforms.

- Blockchain may reduce costs and enable new business models and marketplaces, can better manage complexity, data security, and ownership along grids, can engage prosumers in the energy market acting as enabler for the creation of energy communities, can enhance the transparency and trust of the energy market system, can guarantee accountability while preserving privacy requirements, can enhance direct peer-to-peer trading to support the smooth operation of the power grid, and can better handle demand response and provide a framework for more efficient utility billing processes and transactive energy operations.
- Blockchain technology may also be used for issuing certificates of origin, particularly for green energy production and renewable energy sources, for developing peer-to-peer energy transactions schemes, and for establishing energy management schemes for electric vehicles.
- It is also worth mentioning that blockchain is considered an enabler for the decarbonisation of the energy sector facilitating its move towards more decentralised energy source.
- In the end, while blockchain applications are being widely deployed, many issues have yet to bead dressed.
- By doing so, blockchains will become not only more scalable and efficient but more durable as well.
- The features they offer are not unique if judged individually, and the bulk of the mechanisms they are based on are well-known for years.
- However, the combination of all these features makes them ideal for many applications justifying the intense interest by several industries and other domains.

Chapter Ends...

❑❑❑