SUBJECT CODE : 410243

Choice Based Credit System

SAVITRIBAI PHULE PUNE UNIVERSITY - 2019 SYLLABUS

B.E. (Computer) Semester - VII

BLOCKCHAIN TECHNOLOGY

(For END SEM Exam - 70 Marks)

Iresh A. Dhotre

M.E. (Information Technology)

Ex-Faculty, Sinhgad College of Engineering, Pune.

FEATURES

- ☑ Written by Popular Authors of Text Books of Technical Publications
- ☑ Covers Entire Syllabus
- ☑ Question - Answer Format
- ☑ Exact Answers and Solutions
- ☑ Solved Model Question Paper (As Per 2019 Pattern)

DECODE®

A Guide For Engineering Students

DECODE®

A Guide For Engineering Students

BLOCKCHAIN TECHNOLOGY

(For END SEM Exam - 70 Marks)

SUBJECT CODE : 410243

B.E. (Computer Engineering) Semester - VII

Published by :

TECHNICAL PUBLICATIONS® SINCE 1993 An Up-Thrust for Knowledge

Amit Residency, Office No.1, 412, Shaniwar Peth,
Pune - 411030, M.S. INDIA Ph.: +91-020-24495496/97
Email : info@technicalpublications.in
Website : www.technicalpublications.in

Printer :
Yogiraj Printers & Binders, Sr.No. 10/1A,Ghule Industrial Estate, Nanded Village Road,
Tal. - Haveli, Dist. - Pune - 411041.

ISBN 978-93-5585-234-2

9 789355 852342

SPPU 19

SYLLABUS

Blockchain Technology - (410243)

Credit	Examination Scheme :
03	End-Sem (Paper) : 70 Marks

Unit III Blockchain Platforms and Consensus in Blockchain

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. **(Chapter - 3)**

Unit IV Cryptocurrency - Bitcoin, and Token

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

Unit V Blockchain Ethereum Platform using Solidity

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) **(Chapter - 5)**

Unit VI Blockchain Case Studies

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

TABLE OF CONTENTS

Unit III

Unit IV

Unit V

Unit VI

Unit III

3 Blockchain Platforms and Consensus in Blockchain

3.1 Types of Blockchain Platforms

Q.1 List and explain any two types of Blockchain platforms.

Ans. : • Four different kinds of blockchain architecture are Public, private, Consortium and Hybrid blockchains.

1. Public blockchain

- A public blockchain is a fully decentralized platform where anyone can read and send transactions. The valid transactions are included in the ledger.
- A public blockchain is a non-restrictive, permission-less distributed ledger system.
- Public blockchains are secured by cryptoeconomics, a combination of economic incentives and cryptographic verification. The degree of influence in the consensus process is proportional to the quantity of economic resources brought in the system.
- Public blockchains are being used extensively in the mining and trading of bitcoins in the modern day.
- Ethereum, provider of a decentralized platform and programming language that helps running smart contracts and allows developers to publish distributed applications.
- Public blockchains tend to have longer validation times for new data than private blockchains.
- Example : Bitcoin, Ethereum, Litecoin

2. Private blockchain

- In a private blockchain, write permissions are kept centralized to one organization. In this system the access and permissions are tightly controlled and rights to modify are restricted to the central authority.
- Private blockchains are usually used within an organization or enterprises where only selected members are participants of a blockchain network
- Private blockchains are more vulnerable to fraudulent activity and malicious actors.
- Private blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership, etc.
- Examples of private blockchains are; Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, etc.

Q.2 What is difference between private and public blockchain ?

Ans. :

Sr. No.	Private blockchain	Public blockchain
1.	Participants are pre-selected.	Anyone can participate.
2.	No crypto currency is required.	Requires a crypto-currency.
3.	Private blockchain, which is also called permissioned blockchain.	Public blockchains are called "permissionless".
4.	Examples of private blockchains are; Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, etc.	Example : Bitcoin, Ethereum, Litecoin
5.	Private blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership, etc.	Public blockchains are being used extensively in the mining and trading of bitcoins in the modern day.

6.	Partially decentralized because of participation of known actors.	Truly decentralized because of participation of unknown actors.
7.	Authorized nodes only can participate in consensus.	All are allowed to participate in consensus and anonymous resilient.
8.	High throughput.	Low throughput.
9.	Transactions are private.	Transactions are transparent and accessible.

Q.3 Explain hybrid blockchain.

Ans. : • Hybrid blockchains use both private and public blockchains, rather than being a standalone solution.

- Hybrid blockchains are blockchains that are controlled by a single organization but also have some supervision given by the public blockchain. This supervision is required to carry out specific transaction validations, hence hybrid blockchains are important.
- With hybrid blockchains, a company may put their data or transactions on a private blockchain to keep the information confidential but put a digital fingerprint of the data on a public blockchain to secure it.
- Example of a hybrid blockchain is Dragonchain.

Q.4 Discuss briefly consortium blockchain.

Ans. : • Consortium blockchains are permissioned blockchains governed by a group of organizations, rather than one entity, as in the case of the private blockchain.

- Consortium blockchains, therefore, enjoy more decentralization than private blockchains, resulting in higher levels of security.
- Consortium or federated blockchains operate with a particular group of participants who control the blockchain, rather than a single entity. This group sets the rules, edits or cancels incorrect transactions and solicits cooperation among its members, according to a Blockchain Council report.

- However, setting up consortiums can be a fraught process as it requires cooperation between a number of organizations, which presents logistical challenges as well as potential antitrust risk.
- Consortium blockchains are only useful for smaller groups where the identity of the participants can be determined
- Examples of a consortium or federated blockchain include Hyperledger, Corda and Quorum.

Q.5 Explain the difference between public, private and consortium blockchains.

Ans. :

Parameters	Public blockchain	Private blockchain	Consortium blockchain
Read permission	Public class	Could be public or restricted	May be public or restricted
Efficiency	Low	High	High
Centralized	No	Yes	Partial
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Determination of consensus	All miners	Only one organization	Designated set of nodes

Q.6 Explain advantages and disadvantages of private blockchains.

Ans. : Advantages of private blockchains

- High security : Private blockchains are more secure than public ones mainly because it requires authentication to read the information on the Blockchain.
- Data confidentiality : Participants can encrypt transaction data.
- Higher transaction capacity : The private blockchain also has a faster transaction speed than the public one.
- The private blockchain can easily integrate with other chains or databases without complicated integrations.

- Better customization : Private blockchains are customizable to the needs of the company.

Disadvantages of private blockchains

- Centralized : All participants are known, so the network is centralized.
- Scalability : It is limited in terms of scalability as changes have to be approved by the governing body, making it slower to execute transactions and achieve consensus.
- Regulatory : Participants are known, it is difficult to set up a regulatory framework for the system.

Q.7 What is a permissioned blockchain ?

Ans. : • Permissioned blockchains are blockchains that are closed or have an access control layer. This additional layer of security only allows participants to perform the actions that they are authorized to perform.

- In a permissioned blockchain, a user would need permission from the network owner to become part of the said network. Technically, a user can only access, read and write information on the blockchain if they are given access to it.
- A private permissioned blockchain defines the roles that dictate how each participant can contribute to the blockchain and what they can access.

Q.8 Explain advantages and disadvantages of public blockchain.

Ans. : Advantages of public blockchain

- There is the high level of transparency.
- It is also considered virtually unhackable.
- The network is also secure and resistant to censorship because it is highly accessible by users globally.
- Open environment - Public blockchains are open-source, which means that the code is publicly available.

Disadvantages of public blockchains

- Centralized - Due to the uncontrolled nature of transaction formation, the blockchain is more centralized than private blockchain.
- Scalability - Due to increased usage, public blockchains have been encountering scaling issues.
- It requires large amounts of energy and computing power to achieve consensus.

3.2 Blockchain Platform Example

Q.9 Explain Hyperledger blockchain technology.

Ans. : • Hyperledger is an open source project created to support the development of blockchain-based distributed ledgers. Hyperledger consists of a collaborative effort to create the needed frameworks, standards, tools and libraries to build blockchains and related applications.

- Hyperledger Fabric is a blockchain that achieves data privacy via "channels", which enable private communications between two or more network members.
- It allows flexible network permission setup, as well as helps you to create private systems with inaccessible blocks, meaning third parties can't extract any data from them.
- Transactions can be made confidential, only accessible to users with the necessary decryption keys.
- It can be utilized using various programming languages, such as C++, JavaScript, Python, Golang, and Java.
- Hyperledger Fabric is a block chain framework. It works together with other Hyperledger projects such as Burrow and Sawtooth to provide a scalable data platform. Hyperledger Fabric is a platform on which applications may be developed.

- Hyperledger Fabric is built upon a few central components :
  a) Distributed ledger for all data recorded about the transactions.
  b) Multiple peers (or nodes).
  c) Smart contracts that maintain transaction logic.
- The Hyperledger Fabric Certificate Authority acts as the Membership Service Provider for Hyperledger Fabric. It handles registration of members, certification, and regulation of nodes. As such, certificate authorities perform a central role in making Fabric a permissioned blockchain, registering members, keeping track of identities within the network, and removing deprecated accounts.

Q.10 Write short note on IOTA.

Ans. : • IOTA is a distributed ledger developed to handle transactions between connected devices in the IoT ecosystem, and its cryptocurrency is known as MIOTA.

- IOTA uses a proprietary technology called the Tangle, which is a consensus algorithm that requires users to validate two transactions in order to complete their own IOTA transactions.
- IOTA doesn't use blockchain – at least, not in the same way as most other projects. IOTA had a vision of a different type of blockchain and set about to design its own system of validator nodes, called Tangle.
- IOTA features feeless transactions, tamper-proof data, as well as low resource demand. Its network can power the Internet of Things (IoT) without heavy infrastructure investment requirements.
- The nonsequential network of nodes that makes up Tangle is technically referred to as a Decentralized Acyclic Graph (DAG). As a direct consequence of this, a single node in a Tangle may serve as a connection to several other nodes.
- On the other hand, because there is only one path between them, a node cannot refer to itself in that fashion. A conventional

blockchain is already a DAG due to the fact that it is a sequentially linked collection.

- Nevertheless, IOTA's Tangle has a parallel architecture that enables transactions to be processed simultaneously rather than sequentially. This is made possible by Tangle's distributed ledger. The more systems that are linked to the Tangle, the more secure it will become and the more efficiently it will handle transactions.
- A network of computers that are running full nodes, which are responsible for storing the whole history of transactions for a ledger, is required for Bitcoin confirmations and consensus to take place. This approach requires a significant amount of time as well as energy.
- **Merits**
  1. Free transactions
  2. Unlimited scaling
  3. Can process any data, not just financial transactions
  4. Hopes to achieve instant transactions
  5. No IOTA mining – everyone contributes
  6. Quantum resistant
- **Demerits**
  1) No finished product yet
  2) Unclear when the project will be ready
  3) Currently needing to use a centralized coordinator
  4) Has experienced lots of technical flaws and bugs
  5) Many (including MIT) think it has really bad security

Q.11 How is the IOTA network secured ?

Ans. : IOTA's network is fully decentralized and theoretically secure. The network ensures the validity and authenticity of all the data being exchanged on the network. The IOTA network is also considered tamper-proof.

Q.12 Verify the statement : "Corda is both a blockchain and not a blockchain".

Ans. : • Transactions on Corda are cryptographically linked or chained to the transactions it depends upon. So, by definition, Corda is a blockchain-with one key differentiator.

- Corda does not periodically batch up transactions needing confirmation into a block and confirm them in one go. Instead, Corda confirms each transaction in real-time.
- With Corda, there is no need to wait for other transactions to come along or a "block interval". Transactions are confirmed immediately. This means that your transaction is not dependent on any others, increasing both privacy and scalability.
- Corda is an open source DLT maintained by the financial services consortium R3. Corda offers a smart contracts platform to allow businesses to execute complex agreements, associating multiple variants of asset classes across various business domains, including supply chain, healthcare, and finance.

3.3 Consensus in Blockchain

Q.13 Why blockchains need consensus mechanisms ?

Ans. : • The process by which the peers of a blockchain network come to an agreement on the present state of the data is referred to as consensus. This is accomplished via consensus procedures inside the blockchain network by building reliability and trust in the system.

- Consensus mechanisms serve as both the basis for and the primary layer of protection for all blockchain-based cryptocurrencies.
- Transactions may be recorded on a blockchain, which is a digital ledger that is distributed, de-centralized and often accessible to the public. Before being added to the chain, each of these transactions is initially represented as its own distinct "block" of data, which has

to be verified by an independent peer-to-peer network before it can be added.

- This method addresses the problem of "double-spending" and contributes to the defense of the blockchain against fraudulent activity.
- Blockchain networks such as Bitcoin and Ethereum make use of procedures known as consensus in order to guarantee that all users, also known as "nodes," are in agreement over a single version of history. These processes are an attempt to enhance the fault tolerance of the system.

Q.14 What is blockchain consensus algorithm ?

Ans. : • Consensus algorithms are a decision-making process for a group, where individuals of the group construct and support the decision that works best for the rest of them.

- Blockchain consensus algorithms ensure each new block added to the network is the only version of the truth, which is agreed by all the nodes in a distributed/decentralized computing network.
- A consensus algorithm is a mechanism in computer science used to establish agreement on a single data value across distributed processes or systems.
- A consensus algorithm is a protocol through which all the parties of the blockchain network come to a common agreement (consensus) on the present data state of the ledger and be able to trust unknown peers in a distributed computing environment.
- For blockchain networks, the consensus algorithms are an essential element because they maintain the integrity and security of these distributed computing systems.
- A consensus method is used inside a network to determine which transactions on a blockchain are valid and which are not. This determination is made by a group of peers, often known as nodes. To bring about this agreement, we use methodologies that are

conducive to reaching consensus. These sets of rules contribute to the protection of networks against malicious activity and attacks by hackers.

3.4 Proof of Work

Q.15 What is consensus mechanism ? Give one example.

Ans. : • A consensus mechanism is a system that cryptocurrencies like bitcoin and ethereum use to validate the authenticity of transactions and maintain the security of the underlying blockchain.

- For example, if we buy one bitcoin and transfer it to our cryptocurrency wallet, everyone else must agree that we own the bitcoin. If they didn't, our currency would be worthless. The first consensus mechanism was bitcoin's "proof-of-work" (PoW) method.

Q.16 Explain pros and cons of consensus mechanisms.

Ans. : Pros :

1. Forms agreement foundational to the crypto-market.
2. Creates a secure environment.
3. Anyone can participate.

Cons :

1. May be energy-intensive.
2. Potential for attacks.

Q.17 Explain types of consensus mechanisms.

Ans. : The most important of the types of consensus mechanisms used today fall into a few main types :

1. **Proof-of-work :** With proof-of-work, miners compete against each other to validate the next transaction block and earn a reward. This is a highly energy-intensive consensus mechanism but brings a high degree of trust.
2. **Proof-of-stake :** Proof-of-stake (PoS) is a consensus

mechanism wherein those with the largest holding of the network's currency validate new blocks. This enables faster and lower-cost transactions. It rewards those with the biggest stake in the network for continued participation.

3. **Proof-of-authority :** Proof-of-authority is not as common but has a unique form. It is used mainly by private companies or organizations that use blocks created by vetted sources who have special permissions to access the network.
4. **Delegated proof-of-stake :** Delegated proof-of-stake is a variation of PoS in which users who stake their coins can vote on the number of delegates to create new blocks.
5. **Proof-of-capacity :** Proof-of-capacity currencies rely on a computer's available hard drive storage space for a decentralized block verification and generation process.
6. **Proof-of-activity :** The proof-of-activity consensus mechanism is a hybrid of proof-of-stake and proof-of-work in which the miner seeks to utilize the best of both systems.
7. **Proof-of-elapsed time :** Proof-of-elapsed time uses a random timer that operates independently at every node to randomly assign the block verification to a miner.
8. **Proof-of-burn :** With proof-of-burn, consensus is driven by miners periodically burning coins, a process of permanently deleting or eliminating that specific coin from circulation. This validates new transactions while preventing inflation.

Q.18 Write short note on Proof of Work.

Ans. : • Proof of Work (PoW), the first consensus mechanism ever established, is used by Bitcoin, Ethereum and a number of other public blockchains. PoW was the first consensus mechanism ever devised.

- Even though it has a number of scalability issues, it is often thought of as being the most reliable and secure of all the

consensus systems. In spite of the fact that the term "proof of work" was first used in the early 1990s, Satoshi Nakamoto, the developer of Bitcoin, was the first person to employ the notion in relation to digital money.

- Users compete against one another in points of work to see who can solve the most challenging computational challenges using the most powerful machines. The first user to produce a hash with 64 digits will be granted the right to create a new block and verify transactions. This authority will also belong to them.
- In addition, the miner who successfully completes the block is entitled to a "block reward," which is a predetermined amount of Bitcoin.
- The Proof-of-Work algorithm is notorious for having notoriously high operational costs because of the considerable amount of energy and computing power that is required to generate new blocks. This presents an obstacle for new miners to overcome, which raises difficulties with centralised control and the scalability of the system.
- In addition to that, the charges are not the only item that are costly. The primary argument against PoW is that its power consumption has a negative impact on the environment. As a direct consequence of this, a lot of individuals have started using consensus techniques that are less resource-intensive and more environmentally friendly, such as Proof of stake.

Q.19 How Proof-of-Work solves the Byzantine generals problem ?

Ans. : • Bitcoin managed to solve the Byzantine generals problem by using a Proof-of-Work mechanism in order to establish a clear, objective rule set for the blockchain.

- In order to add information, called blocks, to the blockchain, a member of the network must publish proof that they invested considerable work into creating the block. This work imposes large

costs on the creator, and thus incentivizes them to publish honest information.

- Because the rules are objective, there can be no disagreement or meddling with the information on the Bitcoin network. The ruleset governing which transactions are valid and which are invalid is also objective, as is the system for determining who can mint new bitcoin.
- Additionally, once a block has been added to the blockchain, it is extremely difficult to remove, making Bitcoin's past immutable.
- Thus, at all times, members of the Bitcoin network can agree on the state of the blockchain and all transactions therein. Each node verifies for itself whether blocks are valid based on the Proof-of-Work requirement and whether transactions are valid based on other requirements.

3.5 Byzantine General Problem

Q.20 What is Byzantine general problem ?

Ans. : • The Byzantine generals problem is a game theory problem, which describes the difficulty decentralized parties have in arriving at consensus without relying on a trusted central party.

- In a network where no member can verify the identity of other members, how can members collectively agree on a certain truth ?
- The Byzantine generals problem describes the difficulty decentralized systems have in agreeing on a single truth.
- The Byzantine generals problem plagued money for millennia, until the invention of Bitcoin.
- Bitcoin uses a Proof-of-Work mechanism and a blockchain to solve the Byzantine generals problem.
- Bitcoin's ruleset is objective, so there is no disagreement about which blocks or transactions are valid, allowing all members to agree on a single truth.

- The game theory analogy behind the Byzantine generals problem is that several generals are besieging Byzantium. They have surrounded the city, but they must collectively decide when to attack. If all generals attack at the same time, they will win, but if they attack at different times, they will lose.
- The generals have no secure communication channels with one another because any messages they send or receive may have been intercepted or deceptively sent by Byzantium's defenders. How can the generals organize to attack at the same time ?
- Only decentralized systems face the Byzantine Generals problem, as they have no reliable source of information and no way of verifying the information they receive from other members of the network.

Q.21 What is relation between money and the Byzantine generals problem ?

Ans. : • Money is a prime example of the Byzantine generals problem. How should a society establish a money that all members of a society can trust and agree upon ? For much of history, societies have selected precious metals or other rare goods, such as shells or glass beads, as money.

- In some ways, gold solved the Byzantine generals problem : It was trusted and recognized across decentralized systems, such as international trade.
- However, its weight and purity remained unreliable, and still does to this day. The failure of gold to completely solve the Byzantine generals problem resulted in trusted central parties, usually governments, taking over the establishment and issuance of money.
- Governments monopolized mints in order to inspire trust in the weight and purity of the money. Centralized systems obviously did not solve the Byzantine generals problem.
- Governments, the trusted central authorities for money, constantly violated that trust by seizing, debasing, or changing the money.

3.6 Proof of Stake and Proof of Elapsed Time

Q.22 What does Proof-of-Stake (PoS) mean in crypto ?

Ans. : • Proof-of-stake is a cryptocurrency consensus mechanism for processing transactions and creating new blocks in a blockchain. A consensus mechanism is a method for validating entries into a distributed database and keeping the database secure. In the case of cryptocurrency, the database is called a blockchain, so the consensus mechanism secures the blockchain.

- Proof-of-stake reduces the amount of computational work needed to verify blocks and transactions. Under proof-of-work, it kept blockchain secure.
- Proof-of-stake changes the way blocks are verified using the machines of coin owners, so there doesn't need to be as much computational work done. The owners offer their coins as collateral staking for the chance to validate blocks and then become validators.
- With Proof-of-Stake (PoS), cryptocurrency owners validate block transactions based on the number of staked coins.
- Proof-of-Stake (PoS) was created as an alternative to Proof-of-Work (PoW), the original consensus mechanism used to validate a blockchain and add new blocks.
- While PoW mechanisms require miners to solve cryptographic puzzles, PoS mechanisms require validators to hold and stake tokens for the privilege of earning transaction fees.
- Proof-of-Stake (PoS) is seen as less risky regarding the potential for an attack on the network, as it structures compensation in a way that makes an attack less advantageous.
- The next block writer on the blockchain is selected at random, with higher odds being assigned to nodes with larger stake positions.

Q.23 Explain Delegated Proof of Stake (DPoS).

Ans. : • Delegated Proof of Stake or DpoS for short, is a variation on the Proof-of-Stake (PoS) consensus technique that employs a voting strategy that is based on reputation. The users of the network participate in a "vote" to choose "witnesses," who are also frequently referred to as "block producers," to watch over the network on their behalf.

- Transactions on a blockchain may only be validated if they are attested to by witnesses who have received the maximum number of votes.
- Users put their tokens at risk by contributing them to a pool in order to vote. When tabulating the results of the vote, the amount of investment made by each voter is included in; the higher the voter's stake, the more influence they have over the outcome.
- Those who voted for the chosen witnesses are eligible to get a reward once those witnesses successfully verify a block's worth of transactions.
- The most credible witnesses are constantly at risk of being disregarded in favor of other candidates who are seen as being more trustworthy and get a greater number of votes. They run the risk of being thrown out of office if they fail to carry out their responsibilities or make an effort to verify fraudulent transactions. This incentivizes witnesses to always tell the truth, which helps to preserve the reliability of the blockchain.
- Although it is not as widely used as PoS, many people feel that DPoS is superior than PoS in terms of efficacy, democracy and financial inclusion. It is used by the cryptocurrenciesLisk (LSK), EOS.IO (EOS), Steem (STEEM) and BitShares (BTS) (ARK).

Q.24 How is Proof-of-Stake different from Proof-of-Work ?

Ans. :

Proof of Stake	Proof of Work
Block creators are called validators.	Block creators are called miners.
Participants must own coins or tokens to become a validator.	Participants must buy equipment and energy to become a miner.
Energy efficient.	Not energy efficient.
Security through community control.	Robust security due to expensive upfront requirement.
Validators receive transactions fees as rewards.	Miners receive block rewards.

Q.25 What is Proof of Elapsed Time ?

Ans. : • PoET is a consensus algorithm designed to solve the performance issues faced by existing consensus protocols. It solves the Byzantine Generals' problem using the trusted execution environment. Due to its trusted execution model, it is only suitable for a permissioned blockchain network.

- PoET consensus has been implemented in Hyperledger's Sawtooth, which is a permissioned blockchain project backed by Intel. The Trusted Execution Environment (TEE) in the network is achieved by Intel's Software Guard Extensions (SGX), which are instruction sets that allow user code to allocate private memory regions.
- PoET enables consensus on a bitcoin-like scale without having to resort to mining.
- The PoET protocol also contains a function called the test that limits the number of blocks a player can publish in any particular larger set of blocks.

3.7 Proof of Activity, Proof of Burn

Q.26 What is Proof-of-Burn (PoB) ?

Ans. : • Proof-of-burn (PoB) is a blockchain consensus mechanism with minimal energy consumption, compared to Proof-of-Work (PoW). Decentralized platforms employing the PoB method ensure miners reach a consensus by burning coins. Burning is the process of permanently eliminating cryptos from circulation.

- Proof-of-Burn is a consensus mechanism that is used by several cryptocurrencies, including Factom, Counterparty and Slimcoin (FCT).
- The burning is a loss. But the damage is temporary as the process will safeguard the coins in the long run from the hackers and their cyber-attacks. Moreover, the burning process increases the stakes of the alternative coins.
- Such a scenario increases the chance of a user to mine the next block as well as increases their rewards in the future. So, burning could be used as a mining privilege. The counterparty is an excellent consensus example of a cryptocurrency that uses this blockchain consensus protocol.

Q.17 What is Proof-of-Activity (PoA) ?

Ans. : • Proof-of-Activity (PoA) is a blockchain consensus algorithm that facilitates genuine transactions and consensus amongst miners. That is a consensus algorithm combining proof-of-work and proof-of-stake. This consensus algorithm is designed to prevent attacks on the underlying blockchain.

- The following steps dictate the block creation process in a PoA network :

1. To start, each miner uses hash power to try and generate an empty block header. This is header data consisting of the hash of the previous block, the miner's address, the height relative to

the genesis block, and a nonce. It's important to note that the header does not include past transactions.

2. A miner succeeds in generating a block header when the hash of their block header data is less than the current difficulty target. Once successful, the block header is broadcasted to the network.
3. The hash of the block header is linked with the hash of the previous block. Each combination is then hashed and follow-the-satoshi is invoked with each hash acting as input. Follow-the-satoshi is a PoA subroutine, which transforms a pseudorandom value into a small unit of cryptocurrency called a satoshi. Each satoshi is picked randomly from the satoshis that have been already mined.
4. Active miners then check whether the block header from step two is valid. Does it contain the hash of the previous block and does it meet the current difficulty ? After validation, each miner determines whether they are one of the stakeholders of the block. Successful miners sign the hash block header with a private key that determines their satoshi and broadcasts their signature to the network. This process is repeated until every chosen validator signs the block.
5. The last miner to sign the block then broadcasts the wrapped block to the network. The block is considered a legitimate extension of the blockchain once other nodes see validity in the above four steps. Similar to the Bitcoin blockchain, the nodes try to extend the longest branch they are aware of by assessing PoW difficulty. The fees collected by the last miner are shared between themselves and the remainder of the "winners".

END...

Unit IV

4 Cryptocurrency - Bitcoin and Token

4.1 Bitcoin and the Cryptocurrency

Q.1 What is bitcoin ?

Ans. : • A peer-to-peer internet currency that allows decentralized transfers of value between individuals and businesses.

- Bitcoin is a cryptocurrency and a digital payment system invented by an unknown programmer or a group of programmers, under the name Satoshi Nakamoto.
- It was released as open-source software in 2009. The system is peer-to-peer and transactions take place between users directly, without an intermediary. Since the system works without a central repository or single administrator, bitcoin is called the first decentralized digital currency.
- Bitcoin is the system and bitcoins are the units.

Q.2 What are the risks to using cryptocurrency ?

Ans. : • Cryptocurrencies are still relatively new and the market for these digital currencies is very volatile. Since cryptocurrencies don't need banks or any other third party to regulate them; they tend to be uninsured and are hard to convert into a form of tangible currency.

- In addition, since cryptocurrencies are technology-based intangible assets, they can be hacked like any other intangible technology asset. Finally, since user store cryptocurrencies in a digital wallet, if we lose our wallet (or access to it or to wallet backups), user have lost entire cryptocurrency investment.

Q.3 Explain significance of bitcoin.

Ans. : • Bitcoins can be used to buy merchandise anonymously.

- International payments are easy and cheap because bitcoins are not tied to any country or subject to regulation.
- Some people do their investment in bitcoins.
- Around the world, people are using software programs that follow a mathematical formula to produce bitcoins.
- The mathematical formula is freely available, so that anyone can check it.
- Small businesses may like them because there are no credit card fees.

Q.4 What is needed to make the bitcoin blockchain work ?

Ans. : • Bitcoin represents a digital, trustless form of money, alongside a movement to decentralize financial services. Every Bitcoin transaction happens in the bitcoin blockchain network, which is the digital space where bitcoin mining and hash power generation occur.

- Hashing power is the processing power used by user computer or hardware to perform and solve various hashing algorithms. These algorithms are used to create new cryptocurrencies and allow them to trade with one another. This process is called mining.
- Usually, bitcoin owners purchase their cryptocurrency supply through a cryptocurrency exchange, a platform that facilitates transactions of Bitcoin and other cryptocurrencies.
- The decentralized ledger is what makes the blockchain network. The latter shows that Bitcoin is a piece of software, a set of processes in which participants perform different tasks.
- A blockchain is a digital ledger of duplicated transactions distributed across the blockchain's network of computer systems. Each block on the chain contains several transactions and whenever

a new transaction occurs on the blockchain, a record of that transaction is added to the ledger of each participant.

- This distributed database is managed by multiple participants using a technology called Distributed Ledger Technology (DLT). Blockchain is a type of DLT in which transactions are recorded using an immutable cryptographic signature known as a hash. The transactions are then organized into blocks.
- Each new block includes a hash of the preceding one, effectively chaining them together, which is why distributed ledgers are commonly referred to as blockchains.

Q.5 How does bitcoin mining work ?

Ans. : • Bitcoin mining is the process of adding new transactions to the Bitcoin blockchain. It's a tough job. People who choose to mine Bitcoin use a process called proof of work, deploying computers in a race to solve mathematical puzzles that verify transactions.

- To entice miners to keep racing to solve the puzzles and support the overall system, the Bitcoin code rewards miners with new Bitcoins.
- In the early days, it was possible for the average person to mine Bitcoin, but that's no longer the case. The Bitcoin code is written to make solving its puzzles more and more challenging over time, requiring more and more computing resources.
- Today, Bitcoin mining requires powerful computers and access to massive amounts of cheap electricity to be successful.
- Bitcoin mining also pays less than it used to, making it even harder to recoup the rising computational and electrical costs.

Q.6 How is cryptography used in bitcoin transactions ?

Ans. : • In a normal bitcoin transaction, first, there are the transaction details : whom user wants to send the bitcoins to and how many bitcoins user wants to send. Then the information is passed through a hashing algorithm.

- Bitcoin uses the SHA-256 algorithm. The output is then passed through a signature algorithm with the user's private key, used to uniquely identify the user. The digitally signed output is then distributed across the network for other users to verify. This is done by using the sender's public key.
- The output of the above step is distributed over the network for the people to verify the transaction. The transaction is verified using the sender's public key, and those who verify it are known as minors.
- After the verification, the bitcoin is added into the blockchain, which cannot be reversed.

4.2 Cryptocurrency Basics

Q.7 What is cryptocurrency ?

Ans. : • Cryptocurrency is an encrypted data string that denotes a unit of currency. It is monitored and organized by a peer-to-peer network called a Blockchain, which also serves as a secure ledger of transactions, e.g., buying, selling and transferring.

- The most popular cryptocurrencies, by market capitalization, are Bitcoin, Ethereum, Bitcoin Cash and Litecoin.

Q.8 What is cryptocurrency mining ?

Ans. : Cryptocurrency mining is the process by which recent cryptocurrency transactions are checked and new blocks are added to the blockchain.

Q.9 Explain requirement of cryptocurrency.

Ans. : • Cryptocurrency must meet the following requirements :

a) Absence of any centralized authority and is maintained through distributed networks.

b) The system maintains records of cryptocurrency units and who owns them.

c) The system decides whether new units can be created and in case it does, decided the origin and the ownership terms.

d) Ownership of cryptocurrency units can be proved exclusively cryptographically.

e) The system allows transactions to be performed in which ownership of the cryptographic units is changed

Q.10 Explain purpose and working of cryptocurrency.

Ans. : • The main purpose of cryptocurrency is to reduce the risk involved in traditional currency. It is very easy to use. We can access it anywhere and anytime. All we need is a smart phone and a good net connection.

- In cryptocurrency the power and the responsibilities are in hands of the currency holder. It uses blockchain technology. It is a very brilliant technology because both the buyer and seller details are viewable to each other and so no broker is needed.
- For example if we need to buy a share from a stock market we can do it easily with the help of a broker. We will confirm the exchange order and then we will receive the shares. We do not need to contact the seller in person.
- The reason for choosing a broker is we do not know if the seller has the stock or not. This is known as principle of novation. In cryptocurrency, involvement of third person is not needed because all the transactions are stored in a common location and it is viewable.
- The identity of the person who made the transaction is encrypted. Most of the cryptocurrencies are made using a process called mining. Mining is nothing but an algorithm. It is the process of adding transaction to the blockchain ledger via nodes on the network with the consensus achieved through a proof of system.
- But not all cryptocurrencies are made by mining. Some currencies are created using various other techniques such as tokens.

- Transactions done using cryptocurrencies are highly secure. There is a chance of earning huge amount when compared to mutual funds or share market but it comes with a high risk. Because the volatility of cryptocurrency is very high. Either we earn high returns or lose what we have.

Q.11 What are advantages and disadvantages of cryptocurrency ?

Ans. : Advantages of cryptocurrency :

- Decentralization means the network operates on a user-to-user (or peer-to-peer) basis.
- A cryptocurrency transaction is generally a quick and straightforward process.
- Every cryptocurrency transaction is recorded in a public list called the blockchain, which is the technology that enables its existence.
- Blockchain aims to cut out intermediaries, such as banks and online marketplaces, which means there are no payment processing fees.
- Cryptocurrency payments are becoming more widely used, amongst large organizations, and in sectors including fashion and pharmaceuticals.

Disadvantages of cryptocurrency :

- The lack of regulation.
- Fear about hacking and scams due to the reason for digitalisation.
- Cryptocurrency can be vulnerable to scams.
- Security issues : There are stories where exchanges are hacked and peoples who held coins in those exchanges lost everything.
- There are a lot of people with less experience and knowledge which leads to huge loss.
- Since it is fully digitalized there is a technical difficulty such as network issues and so on.

Q.12 Why is cryptocurrency popular ?

Ans. : • With cryptocurrency, there is a new way of transacting and storing value that is markedly better than traditional fiat and gold.

a) **Portability :** How easily the currency can be transported ?

b) **Divisibility :** The degree to which currency can be divided into smaller amounts.

c) **Censorship resistance :** The ability for governments and regimes to censor its use.

d) **Scarcity :** How prevalent it is in society and its future supply ?

e) **Security :** How secure it is to use ?

f) **Backing :** Who is backing the legitimacy of the currency ?

Q.13 How to store cryptocurrency ?

Ans. : • Once user has purchased cryptocurrency, user needs to store it safely to protect it from hacks or theft. Usually, cryptocurrency is stored in crypto wallets, which are physical devices or online software used to store the private keys to our cryptocurrencies securely.

- Some exchanges provide wallet services, making it easy for user to store directly through the platform. However, not all exchanges or brokers automatically provide wallet services for user.
- There are different wallet providers to choose from. The terms "hot wallet" and "cold wallet" are used :

a) **Hot wallet storage :** "hot wallets" refer to crypto storage that uses online software to protect the private keys to user assets.

b) **Cold wallet storage :** Unlike hot wallets, cold wallets (also known as hardware wallets) rely on offline electronic devices to securely store user private keys.

- Typically, cold wallets tend to charge fees, while hot wallets don't.

Q.14 What are the key steps to buy cryptocurrency ?

Ans. : Step 1 : Pick the best cryptocurrency exchange.

Step 2 : Open a trading account and confirm your email. Connect your phone now.

Step 3 : Verify your identification in step three. Fund your account next.

Step 4 : Purchasing and investing in cryptocurrency.

Step 5 : Store your cryptocurrency.

Step 6 : Choose a strategy in the last step.

4.3 Types of Cryptocurrency

Q.15 What are the main types of cryptocurrencies ?

Ans. : • Types of cryptocurrencies are Payment cryptocurrency, Utility tokens, Stablecoins and Central Bank Digital Currencies (CBDC).

1. **Payment cryptocurrency :** The purpose of a payment cryptocurrency, as the name implies, is not only as a medium of exchange but also as a purely peer-to-peer electronic cash to facilitate transactions. Example is Bitcoin.
2. **Utility tokens :** Tokens are any cryptographic asset that runs on top of another blockchain. Ethereum network was the first to incorporate the concept of allowing other crypto assets to piggyback on its blockchain.
3. **Stablecoins :** Given the volatility experienced in many digital assets, stablecoins are designed to provide a store of value. They maintain their value because while they are built on a blockchain, this type of cryptocurrency can be exchanged for one or more fiat currencies. So stablecoins are actually pegged to a physical currency, most commonly the U.S. dollar or the Euro.
4. **Central Bank Digital Currencies (CBDC) :** Central Bank Digital Currency is a form of cryptocurrency issued by the central banks of various countries. CBDCs are issued by central banks in token form or with an electronic record associated with

the currency and pegged to the domestic currency of the issuing country or region.

Q.16 Explain various types of cryptocurrency examples.

Ans. :

1. **Bitcoin (BTC) :** One of the most commonly known currencies, Bitcoin is considered an original cryptocurrency. It was created in 2009 as an open-source software.
2. **Ethereum (ETH) :** Created in 2015, Ethereum is a type of cryptocurrency that is an open source platform based on blockchain technology.
3. **Zcash (ZEC) :** Zcash is a digital currency that was built on the original Bitcoin code base.
4. **Ethereum Classic (ETC) :** Ethereum Classic is a version of the Ethereum blockchain. It runs smart contracts on a similar decentralized platform. Smart contracts are applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interface.
5. **Bitcoin Cash (BCH) :** Bitcoin Cash is a type of digital currency that was created to improve certain features of Bitcoin. Bitcoin Cash increased the size of blocks, allowing more transactions to be processed faster.
6. **Ripple :** Ripple is a distributed ledger system that was founded in 2012. Ripple can be used to track different kinds of transactions, not just cryptocurrency. The company behind it has worked with various banks and financial institutions.

4.4 Cryptocurrency Usage

Q.17 Whether cryptocurrency is safe or not safe ? Give your opinion.

Ans. : • Cryptocurrencies are usually built using blockchain technology. Blockchain describes the way transactions are recorded into "blocks" and time stamped.

- It's a fairly complex, technical process, but the result is a digita' ledger of cryptocurrency transactions that's hard for hackers tc tamper with.
- In addition, transactions require a two-factor authentication process. For instance, user might be asked to enter a username and password to start a transaction. Then, user might have to enter an authentication code sent via text to user's personal cell phone.
- While securities are in place, that does not mean cryptocurrencies are un-hackable. Several high-dollar hacks have cost cryptocurrency start-ups heavily.
- Hackers hit Coincheck to the tune of $534 million and BitGrail for $195 million, making them two of the biggest cryptocurrency hacks of 2018.
- Unlike government-backed money, the value of virtual currencies is driven entirely by supply and demand. This can create wilc swings that produce significant gains for investors or big losses.
- Cryptocurrency investments are subject to far less regulatory protection than traditional financial products like stocks, bonds and mutual funds.

Q.18 Why cryptocurrencies are so popular in India ?

Ans. : • The demand and popularity for cryptocurrencies have grown steadily in India and here are some of the reasons why cryptocurrencies are so popular :

1. **No human involvement :** Cryptocurrencies are great and most preferable for online international transactions without any glitch whatsoever. Since it is a digital currency that is decentralized.
2. **Speed of transaction :** Cryptocurrency has been verified to be a very fast means of transaction, as fast as light. It can also do multiple transactions at a time without any mix-up whatsoever.

3. **Secured transaction :** Many professionals identify cryptocurrencies and the blockchain as truly unhackable.
4. Ease of use and transparency.

4.5 Cryptowallets : Metamask, Coinbase, Binance

Q.19 What is a cryptocurrency wallet ?

Ans. : A cryptocurrency wallet is an online software program that stores private and public keys. It allows user to access funds, make transactions, and check your balance. User can also generate public and private keys for different cryptocurrencies.

Q.20 Explain types of wallet.

Ans. : • Different types of crypto wallet are Software wallet, Hardware wallet and Paper wallet.

1. **Software wallet** can again be divided into a) Desktop wallet b) Mobile wallet c) Online wallet

   a) **Desktop wallet :** Desktop wallet is one which is downloaded and installed on desktop or laptop. It can be only accessed in the system in which it is downloaded. Desktop wallet also offers high end security until the system is hacked. When the system gets a virus there is the possibility that you may lose your crypto assets.

   b) **Mobile wallet :** Mobile wallet is an app that runs on mobile phone, which is more useful that they can be used anytime, anywhere. Mobile wallets are usually much smaller and simple as only limited space is available on the mobile.

   c) **Online wallet :** Online wallet runs on cloud storage and is accessible from any device conveniently. Online wallet stores private and public key online which is controlled by third party. This makes it more harmful and easily available for hackings and theft.

2. **Hardware crypto wallet :** • The hardware crypto wallet stands apart from others as it keeps private and public keys on a physical device. This can be compared to a flash drive, the kind people still use to transport files from one computer to another.
   - As a result, hardware crypto wallets offer greater security than others, as they keep cryptocurrencies offline. Hackers will be unable to access them when they're disconnected. Popular hardware wallets include Trezor Model T and Ledger Nano X.
3. **Paper wallet :** Paper wallet is one which provides high level of security to store cryptocurrency. This refer to a physical copy or printout of the public and private keys. Paper wallet can be piece of software that is used to securely generate a pair of keys which are then printed.

Q.21 What are advantages and disadvantages of paper wallet ?

Ans. : Advantages :

- Enjoy control of user private keys
- No need for online storage
- Paper wallets tend to be invulnerable to hackers

Disadvantages :

- Can not use for daily transactions
- Not user-friendly for people new to cryptocurrencies
- Paper wallets may be destroyed easily

Q.22 What are advantages and disadvantages of desktop wallet ?

Ans. : Advantages :

- A convenient option for crypto trading
- Enjoy total control of private keys
- Fantastic security when your computer has never been taken online

Disadvantages :

- Using cryptocurrencies for daily transactions can be hard with a desktop wallet

- Desktop wallets become less secure when the computer goes online
- All cryptocurrencies may be lost if your computer becomes unusable and you fail to back your wallet up

Q.23 What is MetaMask wallet ? Explain features of MetaMask wallet.

Ans. : • MetaMask is a cryptocurrency wallet that enables users to store Ether and other ERC-20 tokens.

- MetaMask is a cryptocurrency wallet available as a browser extension for Chrome, Firefox, Opera and Brave. The wallet serves as a connection between your browser and the Ethereum blockchain.
- MetaMask also holds private keys in your browser. MetaMask uses open source code and can only be decrypted with your MetaMask password and secret phrase.
- **Features :**
  1. It is a light node and allows users to fully interact with the network, without downloading the entire blockchain.
  2. Intuitive and easy to use user interface.
  3. Support multilingual - Present with 18 national / international language HD.
  4. Custom fee - For transactions within the ethereum system. ERC20 tokens- can easily add ERC20 tokens in the MetaMask wallet.
  5. Integrated with crypto exchanges - Allows users to buy ether from Coinbase and Shapshift network options.
  6. A fully-decentralized, secure wallet based on a 12-word "Secret Recovery Phrase."

Q.24 Write short note on Coinbase wallet.

Ans. : • Coinbase wallet is a standalone wallet that stores the private keys on the device it is installed on, which means that it is as secure as the device. The wallet uses secure element technology to lock

down the private keys on your smartphone, which is state-of-the-art security technology.

- The Coinbase wallet supports Bitcoin, Ethereum, Litecoin, Bitcoin Cash, and many more cryptocurrencies.
- It is available as a mobile app and on the web. Coinbase wallet supports a wide variety of features and allows user to store digital assets such as NFTs.
- The Coinbase wallet is a self-custody wallet, where your private keys are stored on your local device, giving user control over your cryptocurrency. Like MetaMask, the Coinbase wallet uses a 12-word recovery phrase for the private key.
- Coinbase wallet offers top-notch customer service and a streamlined process that makes it easy to get started in the crypto world. Designed for mainstream audiences, the Coinbase wallet makes sending, receiving, and transferring coins and NFTs easy.
- Coinbase wallet is able to send BTC, BCH, ETH, ETC, LTC, and all your ERC-20 tokens to exchange wallets.
- **Features :**
  1. Send, trade and receive cryptocurrency with an easy-to-use interface.
  2. Includes the ability to earn interest on your coins.
  3. Robust customer support and help center.
  4. Built-in support for browsing DApps and digital marketplaces.

Q.25 What is Binance chain wallet ?

Ans. : • Binance chain wallet is the official Binance cryptocurrency wallet for accessing BNB Smart Chain (BSC), Binance Chain and Ethereum.

- The Binance chain wallet currently supports Chrome, Firefox and Brave.
- Most crypto wallets are able to generate one or more pairs of public and private keys. The public key is used to generate wallet

addresses, which are needed to receive payments. The private keys, on the other hand, are used during the creation of digital signatures and verification of transactions.

Q.26 List pros and cons of Binance chain wallet.

Ans. : Pros :

1. Multiple cryptocurrency support.
2. Very secure.
3. SegWit and Bech32 address support.
4. Built-in exchange functionality.
5. One of the most trustworthy names in the crypto world.

Cons :

1. Mediocre customer support.
2. Not ideal for beginners.

Q.27 What are advantages and disadvantages of Coinbase ?

Ans. : Advantages :

1. Easy to use for beginners.
2. Supports a large number of crypto assets.
3. Access to decentralized applications (dApps) across multiple blockchains.
4. Only charges network fees.

Disadvantages :

1. Coinbase has a history of bad customer support.
2. Code is not open-source.

Q.28 Explain difference between Metamask, Binance and Coinbase.

Ans. :

Title	Binance wallet	Coinbase wallet	Metamask
Platform supported	1. SAAS 2. iphone 3. ipad 4. Android	1. Windows 2. MAC 3. iphone 4. ipad 5. Android	1. SAAS 2. iphone 3. ipad 4. Android
Audience	Crypto currencies users looking for a Binance wallet browser extension to send and receive transactions.	Traders in need of storing all kinds of digital assets with a crypto wallet.	Crypto wallet and gateway for blockchain apps for anyone.
Support	Online	Online	Online
Pricing	Free version	Free version	Free version
Training	Documentation	Documentation	Documentation
Company Information	Build and Build (Binance) Founded 2019 www.bnbchain.world/en/binance-wallet	Coinbase Founded 2012 Unitedstates Coinbase.com	Consensys Founded 2014 United States Metamask.io

Table Q.28.1 Comparision of Metamask, Binance and Coinbase

END...

Unit V

5 Blockchain Ethereum Platform using Solidity

5.1 What is Ethereum ?

Q.1 What is Ethereum ?

Ans. : • Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts.

- Ethereum is a decentralized, open source and distributed computing platform that enables the creation of smart contracts and decentralized applications, also known as dapps.
- Ethereum is an open-source operating system that deals with smart contract functionality.
- Ethereum is open source and used primarily to support the second-largest cryptocurrency in the world known as Ether.
- Ethereum is also a programming language that helps developers to create distributed applications. Ethereum split into two different blockchains in 2016 namely Ethereum and Ethereum Classic.
- Ethereum aims to provide a system that gives users more control over their data, and it also allows for applications to be built and run on the blockchain. To run these applications and have this level of control on the Ethereum platform, it requires Ether.

Q.2 What is an Ethereum smart contract ?

Ans. : A smart contract is application code that resides at a specific address on the blockchain known as a contract address. Applications can call the smart contract functions, change their state and initiate transactions. Smart contracts are written in programming languages

such as Solidity and Vyper, and are compiled by the Ethereum Virtual Machine into bytecode and executed on the blockchain.

Q.3 Explain full nodes and light-weight nodes.

Ans. :

1. **Full nodes :** Full nodes contain the entire history of transactions since the genesis block. They are a full-fledged proof of the integrity of the blockchain network. Full nodes have to contain each and every transaction that has been verified according to the rules set up by Ethereum's specifications.
2. **Light-weight nodes :** • Light-weight nodes on the other hand only contain a subset of the entire blockchain. These types of nodes are mostly used in e-wallets which have to be light-weight in nature and hence the entire blockchain cannot be stored on them.
   - These nodes do not verify every block or transaction and may not have a copy of the current blockchain state. They rely on full nodes to provide them with missing details.
   - The advantage of light nodes is that they can get up and running much more quickly, can run on more computationally/memory constrained devices, and don't eat up nearly as much storage.

Q.4 Explain the following : Ether, Gas, Gas fee, Gas price.

Ans. : 1. Ether : • Ether is the name of the crypto-currency used to pay for transactions on the Ethereum network. Asides from paying for general transactions and services, Ether is also used to buy gas, which in turn is used to pay for computation within the EVM.

- Ether is the metric unit and has a lot of denominations which help accurately pay for transactions and gas. The smallest denomination a.k.a base unit is called Wei.

2. **Gas :** Gas is used as a metric for paying for computational resources on the network. Every contract on the network has a set maximum amount of gas that it can use for its computations. This

is known as the "Gas Limit".

3. **Gas price :** This is the cost of gas in terms of tokens like Ether and its other denominations. To stabilize the value of gas, the gas price is a floating value such that if the cost of tokens or currency fluctuates, the gas price changes to keep the same real value.

4. **Gas fee :** This is effectively the amount of gas needed to be paid to run a particular transaction or program.

Q.5 What is an Ethereum transaction ?

Ans. : A transaction in Ethereum is a signed data message sent from one Ethereum account to another. It contains the transaction sender and recipient information, the option to include the amount of Ether to be transferred, the smart contract bytecode, and the transaction fee the sender is willing to pay to the network validators to have the transaction included in the blockchain, known as gas price and limit.

Q.6 What's the difference between Ether and Ethereum ?

Ans. : • Ether is a digital currency in financial transactions, as an investment or as a store of value. Ethereum is the blockchain network where Ether is held and exchanged.

- Ethereum is the platform and Ether is the crypto-fuel or cryptocurrency that thrives over it.
- Ether is bought and sold and not Ethereum.
- Ethererum has various applications but Ether has only one application i.e. to enable operations on the blockchain.

Q.7 Explain types of account used in Ethereum.

Ans. : • An account is the minimum storage requirement, just like an address in the Bitcoin protocol.

- There are two types of accounts on Ethereum : externally owned accounts and contract accounts.

- An externally owned account (EOA) is controlled by a private key. A contract account (CA) is controlled by a piece of code in place of the private key.
- Each account, regardless of its type consists of the following four elements :
  1. Nonce : A number corresponding to the amount of (a) transactions sent from or (b) contracts created by an account
  2. Balance : Amount owned by an account.
  3. storageRoot : A hash of the root node of a hash tree that encodes the storage contents of the account.
  4. codeHash : A hash of the account's EVM code.
- EOAs are like to accounts that are controlled by a private key in bitcoin. Contract accounts are having private key along with the accounts that have code associated with them.
- An EOA has ether balance, is capable to send transactions and has no related code, whereas a Contract Account (CA) has ether balance, associated code and the ability to get caused and accomplish code in response to a transaction or a message that due to the turing extensiveness property of the Ethereum blockchain network, the code within contract accounts can be of one of the level of complexity.

Q.8 Explain externally owned account.

Ans. : • The basic function of an externally owned account is that it can hold an ether balance. Externally owned accounts are further capable of sending and receiving transactions.

- The concept of externally owned accounts is quite similar to the concept of addresses in the Bitcoin protocol. That being said, an Ethereum account is controlled by a private key that corresponds to its public key.

- The latter is hashed to determine the account address, while the former is used to generate signatures and authorize outbound transactions.
- But because the Ethereum blockchain has an extended functionality that goes beyond that of the Bitcoin protocol, sending a transaction from an externally owned account is not limited to cryptocurrency transfers alone.
- Instead, an account is also capable of triggering contract code, meaning that it can be used to deploy smart contracts or trigger smart contract functionality.

Q.9 Discuss briefly Ethereum block.

Ans. : • Ethereum blocks consist of following components :

1. The block header
2. The transactions list
3. The list of headers of ommers or uncles

- The transaction list is just a list of all transactions involved in the block. In adding, the list of headers of uncles is also incorporated in the block. The utmost significant and difficult part is the block header.
- Block header : The block headers are the most serious and comprehensive components of an Ethereum block. The header contains valued information, which is described in detail here.

1. **Parent hash :** This is the Keccak 256 bit hash of the parent (earlier)block's header.
2. **Ommers hash :** This is the Keccak 256 bit hash of the list of Ommers (Uncles) blocks included in the block.
3. **Beneficiary :** This field contains the 160 bit address of the receiver that will accept the mining payment once the block is fruitfully mined.
4. **State root :** This field contains the Keccak 256 bit hash of the root node of the state tries.

5. **Transactions root :** This root is the Keccak 256 bit hash of the root node of the transaction tries. Transaction tries denotes the list of transactions involved in the block.
6. **Receipts root :** The receipts root is the Keccak 256 bit hash of the root node of the transaction receipt tries. This tries is collected of receipts of entirely transactions involved in the block.
7. **Logs bloom :** The logs bloom work as a bloom filter that is collected of the logger address and log topics from the log entry of each transaction receipt of the involved transaction list in the block.
8. **Number :** The count of total number of all earlier blocks; the origin block is block zero.
9. **Gas limit :** The field contains the value that represents the limit set on the gas intake per block.
10. **Gas used :** The field contains the total gas spent by the transactions included in the block.
11. **Timestamp :** Timestamp is the period Unix time of the block initialization.
12. **Extra data :** Extra data field can be used to supply arbitrary data related to the block.

Q.10 Explain features of Ethereum.

Ans. : Ethereum features :

- **Ether :** This is the digital token of the Ethereum blockchain.
- **Smart contracts :** Ethereum allows the development and deployment of smart contracts.
- **Ethereum Virtual Machine :** Ethereum provides the underlying technology, the architecture, and the software that understands smart contracts and enables people to interact with it.

- **Decentralized applications (Dapps) :** Ethereum allows people to create consolidated applications, called decentralized applications. A decentralized application is called a Dapp.
- **Decentralized autonomous organizations (DAOs) :** Ethereum enable users to create these for democratic decision-making. DAOs operate entirely transparently and independently of any intervention, with no single leader.

Q.11 Discuss real - world applications of Ethereum.

Ans. : • **Voting systems :** Voting systems are implemented by using Ethereum. The outcomes of polls are widely presented, confirming a transparent and fair self-governing procedure by removing passed by vote misuses.

- **Banking systems :** Ethereum is accomplishment approved extensively in banking application since with Ethereum's decentralized system, provides strong security for data and unauthorized access to hacker is denied.
- **Shipping :** Deploying Ethereum in shipping benefits with the pursuing of cargo and prevents goods from being misdirected or imitated, Ethereum make available the derivation and tracking framework for any asset required in a typical supply chain.
- **Agreements :** With Ethereum smart contracts, arrangements can be preserved and implemented without some alteration. So in a business that has disjointed applicants, is subject to disagreements and needs digital contracts to be contemporaneous, Ethereum is a technology for developing smart contracts and for digitally recording the agreements and the transactions based on them.

5.2 Types of Ethereum Networks

Q.12 Explain Ethereum stack components.

Ans. : • **Level 1 (Ethereum Virtual Machine) :** EVM is the runtime environment for smart contracts in Ethereum. All smart contracts

and state changes on the Ethereum blockchain are executed by transactions. The EVM handles all of the transaction processing on the Ethereum network.

- **Level 2 (Smart Contracts) :** Smart contracts are the executable programs that run on the Ethereum blockchain. Smart contracts are written using specific programming languages that compile to EVM bytecode.
- **Level 3 (Ethereum Nodes) :** In order for an application to interact with the Ethereum blockchain, it must connect to an Ethereum node. Connecting to a node allows you to read blockchain data and/or send transactions to the network. Ethereum nodes are computers running software - an Ethereum client.
- **Level 4 (Ethereum Client Apis) :** Many convenience libraries (built and maintained by Ethereum's open source community) allow your applications to connect to and communicate with the Ethereum blockchain.
- **Level 5 (End-User Applications) :** At the top level of the stack are user-facing applications. These are the standard applications user regularly use and build today : primarily web and mobile apps.

Q.13 What are the types of Ethereum network ? Explain.

Ans. : Two types of Ethereum network are Mainnet and Testnets.

1. Mainnet :

- Mainnet is the primary public Ethereum production blockchain, where actual-value transactions occur on the distributed ledger.
- A mainnet is a self-governing blockchain running its own network with its own technology and protocol. Mainnet is a live blockchain anywhere its particular cryptocurrencies or tokens are in usage, as related to a testnet or developments running on top of other popular networks such as Ethereum.

- Mainnet is the real blockchain network used for "actual" transactions with "monetary value", your wallet is set to Mainnet by default.

2. Testnet

- Testnet on the other hand is a testing network that runs the same protocol as Mainnet does and is used for testing purposes. It allows you to experiment without having to use valuable coins on the main network (Mainnet).
- The programmers are use testnet to troubleshoot and experiment any new features on a blockchain.
- The main dissimilarity between testnets and mainnets is that the previous is a blockchain project that is in progress, while the latter encompasses a completely developed blockchain.
- A testnet is used by programmers and developers to test and troubleshoot all the aspects and features of a blockchain network before they are sure the system is secure and ready for the mainnet launch.
- In other words, a testnet only exists as a working prototype for a blockchain project, while a mainnet is a completely developed blockchain platform for users to send and receive cryptocurrency transactions.

5.3 Ethereum Virtual Machine

Q.14 What is Ethereum Virtual Machine ?

Ans. : • The Ethereum Virtual Machine or EVM is a piece of software that executes smart contracts and computes the state of the Ethereum network after each new block is added to the chain. The EVM sits on top of Ethereum's hardware and node network layer.

- The EVM is Etherum's native processing system that allows developers to create smart contracts and lets nodes seamlessly

interact with them. Ethereum developers write smart contracts with Solidity, a programming language much like Javascript and C++.

- These smart contracts written in Solidity can be read by humans but not computers. It, therefore, has to be converted into low-level machine instructions called opcodes, which the EVM can easily understand and execute.
- It's important to know every Ethereum node has its own EVM.
- When a person sends a transaction to a smart contract deployed on Ethereum, every node runs the smart contract and the transaction through their own EVM.
- In this simulated environment, each node can see what the end result will be and whether the outcome produces a valid transaction or not. If all nodes reach the same valid outcome, the changes are made and the updated Ethereum state is recorded on the blockchain.
- EVM works with a word size of 256 bits and has several addressable data components :
  1. An immutable program code ROM, loaded with the bytecode of the smart contract to be executed.
  2. A volatile memory, with every location explicitly initialized to zero.
  3. A permanent storage that is part of the Ethereum state, also zero-initialized.

Q.15 What are the addressable data components of EVM ?

Ans. : • The Ethereum Virtual Machine has a stack-based architecture. It stores all in-memory values on a stack. It does work with a word size of 256 bits. That is mainly to facilitate native hashing and elliptic curve operations.

- It has various addressable data components :
  a) **An immutable program code ROM :** It is loaded with the bytecode of the smart contract to be performed.

b) **A volatile memory :** That is contained with every location, explicitly initialized to zero.

c) **Permanent storage :** It is a part of the Ethereum state. It is similarly zero-initialized.

Q.16 What are the advantages of the EVM ?

Ans. : Advantages :

- The EVM permits anyone to create their own DApp.
- There are infinite potential use cases for this type of software.
- Technology isn't prohibited to a particular group of people.
- There are several potential advantages of smart contracts.
- The latest example will be non-fungible tokens (NFTs).
- Everyone may create digital art and sell it on a decentralized marketplace by creating NFTs.
- This provides easy access to the art market in a virtual way that wasn't possible earlier.

Q.17 How does the Ethereum Virtual Machine work ?

Ans. : • The EVM uses a stack-based architecture and a word size of 256 bits. The 256 bit word size allows the EVM to facilitate native hashing and elliptic curve operations that ensure funds can be spent only by their rightful owners.

- The EVM supports various programming languages such as Vyper and Solidity, with Solidity being the most popular programming language for smart contract source code. These programming languages are used to write smart contracts, which are converted into the bytecode needed to be utilized by the EVM.
- The bytecode stored on-chain, known as the runtime bytecode, is then converted into an opcode that the EVM computation engine interprets to carry out those actions.
- When an Ethereum transaction executes a smart contract, an EVM is loaded with the information for the transaction being processed. For example, one variable needed for a smart contract execution is

the gas supply, which is set to the amount of gas paid by the sender.

- The gas supply is reduced as the transaction progresses, and if, at any point, the gas supply reaches zero, the transaction is abandoned. Although abandoned transactions don't result in changes to the Ethereum state and are not considered valid transactions, the block's beneficiary is paid for providing resources up to the halting point.
- Smart contracts can initiate transactions and call other contracts on their own. In this case, each call results in another EVM being loaded with specific information for the new transaction. This new information is initialized from the EVM one level above.
- If there isn't enough gas to complete the execution, the state is discarded, and the transaction execution is reset to the EVM one level above.

Q.18 How is data stored in Ethereum protocol ?

Ans. : • The Ethereum protocol uses two distinct data types : permanent data and ephemeral data.

- Permanent data, such as a transaction, is recorded in Ethereum's tree-like data structure and will never be altered.
- Ephemeral data, such as a wallet's balance, is recorded and changed in response to new transactions.

5.4 Introduction to Smart Contracts

Q.19 What is smart contracts ? How it is used ?

Ans. : • A "smart contract" is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.

- A smart contract is a term commonly used to describe computer code protocol intended to digitally facilitate, verify, or enforce the

negotiation or performance of an agreed transaction. A smart contract in its simplest form is really an if-then statement that runs on a blockchain.

- While it is possible to automate some actions under an actual legal contract, like payment obligations occurring on a certain date, a typical legal contract is a much more multifaceted instrument. For instance, it may include a standard of behavior, like reasonable or in good faith, that cannot be encoded in software.
- Smart contracts constitute self-executable code on the network, triggered upon predefined conditions or actions. Within the network, each node must execute the code in order to remain in sync with the rest of the network. The role of a blockchain node is to maintain the consistency and validity of the shared ledger.

Q.20 Explain functioning of smart contracts.

Ans. : • A traditional (physical) contract includes two or more parties, such as individuals, objects and governments. They settle to contract terms and conditions to implement transactions via a third party.

- This third party might be a lawyer, a government organization or any other unit. It is here to take care of the records and execution of the contract. Not only does this add to audit and enforcement costs, but it also increases the risk of loss due to fraud.
- Fig. Q.20.1 shows functioning of smart contract.
- There are two parties (a buyer and a seller) involved in buying and selling a strength.
- These two parties go in a smart contract, an absolutely digital and self-executing contract, with its terms or clauses written in codes on a distributed Blockchain network.
- These codes insist on the contract's terms, which both parties must approve to for the contract to be spontaneously imposed. The

transaction happens when parties come across these terms and rules.

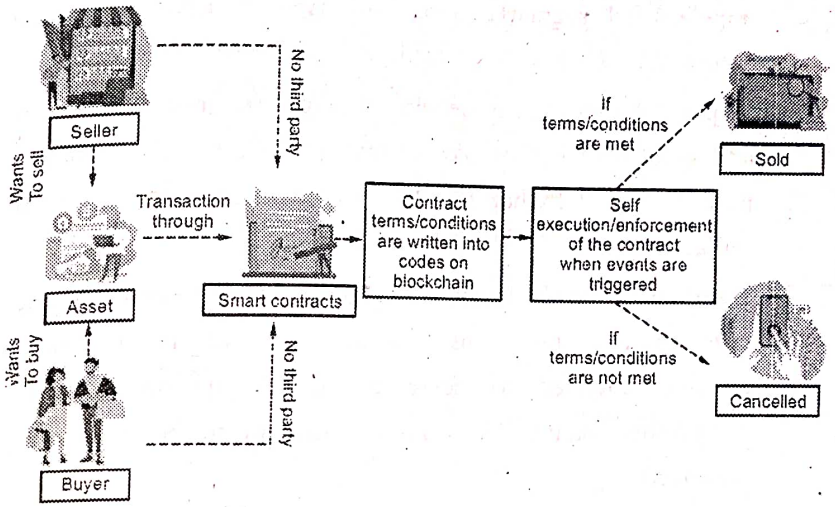


Fig. Q.20.1 Functioning of smart contract

- The smart contracts raised area deals complete transparency and high-end security. As well, it restricts altering of the data and permits the two parties to pathway the transaction. The personalities of the parties involved, however, remain confidential.

Q.21 Which high-level programming languages support smart contracts ?

Ans. :

1) **LLL :** A functional (declarative) programming language, with Lisp-like syntax. This one was the first high-level language for Ethereum smart contracts but is infrequently used today.
2) **Serpent :** A procedural (imperative) programming language with a syntax similar to Python. Can also be used to write functional (declarative) code, though it is not completely permitted of side effects.

3) **Solidity :** A procedural (imperative) programming language with a syntax similar to JavaScript, C++ or Java. The best popular and regularly used language for Ethereum smart contracts.

4) **Vyper :** A extra newly developed language, similar to Serpent and again with Python-like syntax. Intended to get closer to a pure-functional Python-like language than Serpent, but not to replace Serpent.

5) **Bamboo :** A newly developed language, predisposed by Erlang, with obvious state transitions and short of iterative flows (loops). Intended to decrease side effects and increase auditability. Actual new and up till now to be extensively approved.

However, of all of these Solidity is by far the most popular, to the point of being the de facto high-level language of Ethereum and even other EVM-like blockchains.

5.5 Purpose and Types of Smart Contracts

Q.22 Discuss advantages of smart contracts.

Ans. : Advantages :

1. **Speed and savings :** Smart contracts can be executed faster and at lower cost without the need to rely on brokers or intermediaries. They are automated, accurate and save time and money.
2. **Security and trust :** Smart contracts inherit the properties of residing on a blockchain. The smart contract is transparent and accessible within the blockchain, while also offering a reliable backup due to its distributed storage.
3. **Autonomy :** Smart contracts do not require trusted third parties or human intervention in the process, which offers autonomy and independence to the parties.

4. **Speed :** The absence of intermediaries reduces the economic cost as well as the time cost.
5. **Accuracy :** Meanwhile a smart contract is a computer program, each term and condition of the contract wants to be coded.
6. **Unreliable inputs :** These could lead to false contracts or non-execution of contracts.

Q.23 Explain types of smart contracts.

Ans. : • Types of smart contracts are as follows :

1. **Smart legal contracts :** These contracts are legally enforceable and require the parties to satisfy their contractual obligations. Parties may face strict legal actions if they fail to comply.
2. **Decentralized Autonomous Organizations (DAO) :** For a DAO, the backbone is its smart contract. The contract is bound to specific rules that are coded into blockchain contracts blended with governance mechanisms.

- DAOs are open-source and also feature transparency and in theory, are incorruptible. Plus, any action taken by the community members gets replaced by a self-enforcing code.

3. **Application Logic Contracts (ALC) :** Another type of smart contract in blockchain is Application Logic Contracts (ALCs), which allow devices to function securely and autonomously. Plus, ALCs ensure greater automation, cheaper transactions, and scalability.

- These contracts contain an application-based code, which typically remains in sync with other blockchain contracts. It enables communication across different devices, such as the IoT merger with blockchain technology.

Q.24 What is role of smart contracts in blockchain ?

Ans. : • The role of smart contracts in blockchain are as follows :

1. **Security and high reliability :** The transactions can be performed with high reliability. Plus, as the distributed ledger is highly encrypted, it is impenetrable and offers high security.

2. **Disintermediation :** Smart contracts eliminate the reliance on third-party intermediaries to perform transactions. So, it enables parties to enter into agreements without any dependence on intermediaries.
3. **Transparency :** It creates a cohesive environment because both the logic and information in the contract are visible to all those participating in the blockchain network. Plus, parties involved can check out any edits made by a party to the contract's content as it is visible to everyone involved in the cycle, improving transparency.
4. **Lesser errors :** As the contracts use software code to automate tasks, they are less prone to manual errors. Moreover, they offer real-time updates with speed and precision.
5. **Lesser human intervention :** The transactions don't need much human management, which reduces the risks involved in the contract execution cycle.
6. **Speed and efficiency :** Since smart contracts execute immediately when a pre-defined condition is met, they offer speed and efficiency.

5.6 Implementing and Deploying Smart Contracts using Solidity

Q.25 Explain implementing and deploying smart contracts using Solidity.

Ans. : Development workflow :

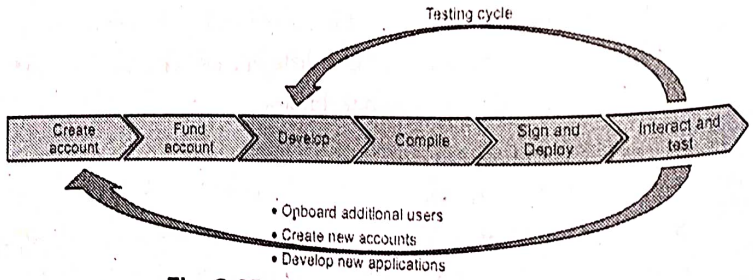
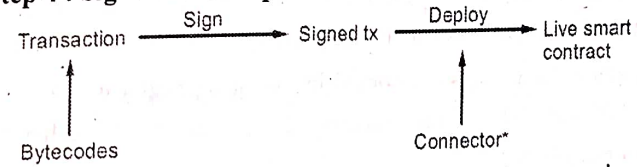


Fig. Q.25.1 : Development work flow

Steps to follow for development :

1) **Step 1 : Create account :**
   - Programmatically : Go, Python, C++, JavaScript, Haskell
   - Tools -MyEtherWallet.com, MetaMask, TestRPC, Many other websites
2) **Step 2 : Fund account :**
   - From friends
   - Faucet
   - Exchanges (for public blockchain)
3) **Step 3 : Develop**
   - Ethereum application components
   - Base application can be developed in any language
   - Smart contract : Developed in Solidity or one of the other contract compatible languages
   - Connector library : Facilitates communication between base application and smart contracts (Metamask)
4) **Step 4 : Sign and Develop :**



   - Library that facilitates communication and connection with Blockchain; Connects your code to a running node.
5) **Step 5 : Interact and Test :**
   - TestRPC / TestChain
   - Local development or Test Blockchain
   - **EthereumJS TestRPC :** https://github.com/ethereumjs/testrpc is suitable for development and testing.
   - It's a comprehensive blockchain-in-memory that runs only on your development machine.
   - Its procedures transactions rapidly as a substitute of waiting for the defaulting block time - so you can test that your code works rapidly - and it tells you instantly when your smart contracts run into errors.

- It similarly marks a great client for automatic testing.
- Truffle distinguishes how to use its special features to rapidity up test runtime by almost 90 %.

Q.26 What is solidity ?

Ans. : • Solidity is the main programming language for writing smart contracts for the Ethereum blockchain. It is a contract-oriented language, which means that smart contracts are responsible for storing all of the programming logic that transacts with the blockchain.

- Solidity is an object-oriented programming language created specifically by the Ethereum Network team for constructing and designing smart contracts on blockchain platforms.
- It is a high-level programming language that looks a lot like JavaScript, Python, and C++. It's designed to run on the Ethereum Virtual Machine, which is hosted on Ethereum nodes that are connected to the blockchain.
- It is statically typed, and supports inheritance, libraries and more! In short, it has all the capability that you need in order build industrial strength blockchain applications.

Q.27 Discuss data types supported by solidity programming.

Ans. : • It supports all the common data types seen in other OOP languages, such as,

a) **Boolean -** The Boolean data type returns '1' when the condition is true and '0' when it is false, depending on the status of the condition.

b) **Integer -** You can sign or unsign integer values in solidity. It also supports runtime exceptions and the 'uint8' and 'uint256' keywords.

c) **String -** Single or double quotes can denote a string.

d) **Modifier -** Before executing the code for a smart contract, a modifier often verifies that any condition is rational.

e) **Array -** The syntax of solidity programming is like that of other OOP languages and it supports both single and multidimensional arrays.

Q.28 How to execute the code in solidity program ?

Ans. : • Solidity program is executed in two ways : offline mode and online mode

1. **Offline mode :** To operate a solidity smart contract in offline mode, it must meet three conditions and follow four essential actions :

   a) Conditions
   - Download and install node.js.
   - Install truffle globally.
   - Install ganache-cli.

   b) Actions
   - Create a truffle project and set up a development network for it.
   - Develop and deploy a smart contract for it.
   - From the truffle console, interact with the smart contract.
   - Create tests to evaluate Solidity's primary features.

2. **Online mode :** In the online mode, the Remix IDE is typically used to compile and run solidity smart contracts.

Q.29 What are advantages of solidity programming ?

Ans. : Advantages :

1. Apart from fundamental data types, Solidity programming also allows complex data types and member variables.
2. It provides an Application Binary Interface (ABI) to enable type safety. If the compiler discovers a data type mismatch for any variable, the ABI generates an error.
3. It refers to the 'Natural Language Specification,' which is used to turn user-centric specifications into language that machines can understand.

Q.30 Explain error handling mechanism in solidity programming.

Ans. : Error handling mechanism in solidity programming is handled by the four functions :

1) **assert() function :** Assert is used when the outcome is predictable to be true, significance that we use assert to test inner conditions.
2) **require() function :** Require is used when testing inputs, set our beliefs for those conditions. This function acts as a gate condition, checking execution of the rest of the function and creating an error if it is not satisfied.
3) **revert() function :** Revert functions halt the execution of the contract and revert any state variations. The revert function can also take an error message as the one argument and it is recorded in the transaction log.
4) **throw() function :** The throw function is obsolete and will be removed in future versions of solidity; you should use revert instead.

Q.31 How to create a new instance in solidity ?

Ans. : • The not dangerous technique to call an additional contract is if user build that additional contract yourself. So we can use certain of its interfaces and behavior. By using new keyword we can simply instantiate it.

- In solidity programming the new keyword used to create the contract on the blockchain and also return an object that user can use to reference it.
- Let's say user need to make and call a Faucet contract from in an additional contract called Token :

```
contract Token is mortal
{
    Faucet _faucet;
    constructor()
    {
        _faucet = new Faucet();
    }
}
```


- This mechanism for contract building guarantees that you distinguish the particular kind of the contract and its interface.

```
import "Faucet.sol";
contract Token is mortal
{
    Faucet _faucet;
    constructor()
    {
        _faucet = new Faucet();
    }
}
```

- You can optionally insist on the value of ether transfer on formation and pass arguments to the new contract's constructor :

```
import "Faucet.sol";
contract Token is mortal {
    Faucet _faucet;
    constructor() {
        _faucet = (new Faucet).value(0.5 ether)();
    }
}
```

- You can similarly then call the Faucet functions. In this below example, we call the destroy function of Faucet from in the destroy function of Token :

```
import "Faucet.sol";
contract Token is mortal
{
    Faucet _faucet;
    constructor()
    {
        _faucet = (new Faucet).value(0.5 ether)();
    }

    function destroy() ownerOnly {
        _faucet.destroy();
    }
}
```

5.7 Swarm (Decentralized Storage Platform)

Q.32 What is Swarm ?

Ans.: • Swarm is a decentralized storage, service, and communication platform designed to deliver permissionless, censorship resistant infrastructure for the deployment of dApp code.

- Swarm aims to provide a range of Web 3.0 services, including messaging, music and video streaming and database hosting.
- Swarm's decentralized storage system is built on the following components :
  1. **Chunks :** Data stored on swarm is split up into smaller blocks called chunks no larger than 4 KB. Chunks are identifiable via a 32 byte hash of the content they contain.
  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.
- When a file is uploaded to the Swarm network from some node, that file is broken down into much smaller pieces of data called chunks. These chunks have a fixed maximum size of 4 KB and each chunk is individually hashed, where that hash corresponds to the address of some other node in the Swarm network.
- In this manner, Ethereum Swarm effectively implements a "distributed content-addressed chunk store", where content addressing means that the address of any chunk is deterministically calculated from its content.
- The addressing hash function takes in a chunk as input and outputs a 32 byte long hash, where clients can use that hash to retrieve the chunk.

Q.33 Explain Swarm architecture.

Ans. : • Swarm is Ethereum's implementation of a decentralized file storage network. This one is reinforced by the Ethereum Geth

client and interrelating with the storage network is closely linked to the Ethereum blockchain and requires an Ethereum account.

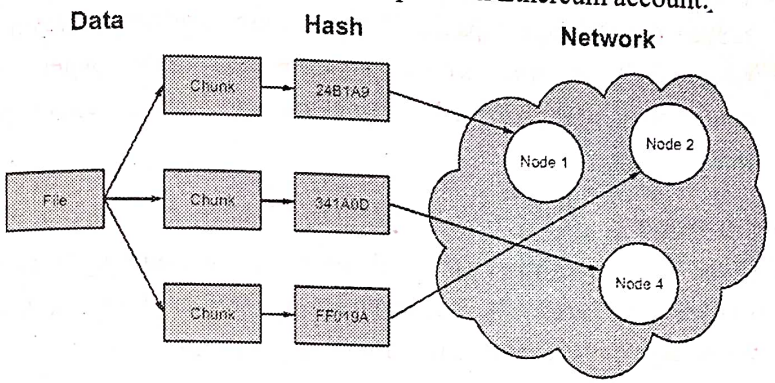


Fig. Q.33.1 Swarm distributed storage model

- The overhead figure demonstrates by what means Ethereum Swarm distributes data across the P2P network. Data is divided up into blocks called chunks, maximum size limit of 4K bytes. The network layer is agnostic to what these chunks represent, for instance, whether they are part of a file or any other piece of data. Chunks are distributed across the network and addressed by a 32 byte hash of their content. This guarantees that data integrity can be proved, but announces a problem with storing contented that may be altered. Hash addressing is also not actual user-friendly. For this reason, another layer, the Ethereum Name Service (ENS) allows users to register human-readable names for their content. ENS is implemented as a smart contract on the Ethereum network and can be well-thought-out the equivalent of the domain name service (DNS) that facilitates content naming in traditional internet services.

Incentive layer :

- Ethereum Swarm distinguishes themself from IPFS in that it does not just reference and possibly cache or contented through accessible on a content owner's own storage. Instead, it actually constitutes a cloud service onto which content can be uploaded.

- Currently, there is no guarantee uploaded content will remain available, as nodes may join and leave the network at will or even reduce their storage capacity. A forthcoming enticement layer is prearranged, in order to pay compensation node owners for contribution storage space. Close integration with Ethereum made this possible.

Using swarm :

- In the direction of associate to Ethereum Swarm a running instance of Geth is required. The Swarm client themself can be found from the Swarm download page for dissimilar platforms.
- Once the Swarm executable has been installed, you can then connect to the network using an existing account managed by the running Geth instance :

```
swarm –bzzaccount <accout>
```

- Swarm then provides an endpoint on port 8500. Navigating to http://localhost:8500 in a browser will open up a search box for the swarm network.

5.8 Whisper (Decentralized Messaging Platform)

Q.34 Write short note on Whisper.

Ans. : • Whisper provides decentralized peer-to-peer messaging capabilities to the Ethereum network. In essence, Whisper is a communication protocol that DApps use to communicate with each other.

- The data and routing of messages are encrypted within Whisper communications. Whisper makes use of DEVp2p wire protocol for exchanging messages between nodes on the network.
- It is designed to be used for smaller data transfers and in scenarios where real-time communication is not required.

- Whisper is also designed to provide a communication layer that cannot be traced and provides dark communication between parties. Blockchain can be used for communication, but that is expensive, and a consensus is not really required for messages exchanged.
- Whisper envelopes contain different payloads which determine whether they are chat messages or group state message updates. The payload of a specific message is defined by a metadata header which contains flags for different envelope configurations, called topics.
- The main topics used by the whisper protocol are : partitioned topics, contact code topic, negotiated topic and negotiated topics.
- Contact code topics are envelopes that begin communication between two parties. For example, if user 1 wanted to chat with user 2, user 1 would first send a contact code message to user 2.
- Partitioned topics is a construct that ensures information is not being leaked when sent across the network. Because we rely on signal's group messaging approach of sending a private message to each user in the group, it becomes very easy to detect when two users are in conversation with each other.
- Partitioned topics ensure that multiple topics can be sent per envelope, thus balancing the efficiency and privacy.
- Finally, negotiated topics are topics where the receiver must listen to the topic. In general, for user 1 to send a message to user 2, they must adhere to the following flow :
  1. User 1 must wait for user 2's client code topic
  2. User 1 then send a message on user 2's partitioned topic
  3. User 1 can then receive messages from user 2

Q.35 Explain Whisper protocol.

Ans. : • Ethereum Whisper is designed as a flexible and secure messaging protocol that protects user privacy.

- The protocol follows a "darkness" principle, meaning that it obscures message content and sender and receiver details to observers, which also means that this information cannot be gained through packet analysis.
- Messages are encrypted by default either asymmetrically or symmetrically. Asymmetric encryption uses public keys for encryption and private keys for decryption. This form of encryption is used for one-to-one communication.
- While symmetric encryption facilitates one-to-many messages using a single encryption and decryption key. Messages are received by a participant if they can be decrypted.
- Thus, the owner of private keys can receive messages destined only for them. One-to-many communications can be received by anyone in possession of the correct symmetric key.
- The strong link with Ethereum means that all participants already have public/private key pairs, making this fully encrypted model possible.

END...

Unit VI

6 Blockchain Case Studies

6.1 Prominent Blockchain Applications

Q.1 Explain prominent blockchain applications.

Ans. : Prominent Blockchain applications are as follows :

- Money transfers using blockchain can be less expensive and faster than using existing money transfer services.
- Financial exchanges : While blockchain-based exchanges primarily deal in cryptocurrency, the concept could be applied to more traditional investments as well.
- Lending : Lenders can use blockchain to execute collateralized loans through smart contracts. Smart contracts built on the blockchain allow certain events to automatically trigger things like a service payment, a margin call, full repayment of the loan.
- Real estate : Real estate transactions require a ton of paperwork to verify financial information and ownership and then transfer deeds and titles to new owners.
- Secure personal information : Keeping data such as your aadhar number, date of birth, and other identifying information on a public ledger may actually be more secure than current systems.
- Voting : If personal identity information is held on a blockchain, that puts us just one step away from also being able to vote using blockchain technology. Using blockchain technology, system can make sure that nobody votes twice, only eligible voters are able to vote.

6.2 Retail, Banking and Financial Services

Q.2 Why blockchain is important in banking and finance ?

Ans. : • The banking and finance sector can be drastically improved by blockchain. Digital financial institutes have the most benefits when it comes to smart contracts.

- The benefits come from digital assets, programmable money and smart contracts. There are plenty of use-cases that can be used in the banking and finance sector.
- Especially, trade finance blockchain has gained a lot of traction in recent times.
- Some of them are as below :
  a) Capital markets such as insurance, sales and trading
  b) Payments and remittances for both domestic and international
  c) Trade finance sectors including bill of lading and letters of credit
  d) Insurance
  e) Investment management including fund launch, administration and more
- There are also few business benefits, including :
  a) Authenticity : It helps finance institutes to bring data integrity and ensure proper authenticity in their systems.
  b) Streamlined process : It improved operational efficiency, including the ability to do a real-time settlement, reporting, and audit.
  c) Programmable capabilities : The entire business logic can be coded including data privacy, compliance, identity and so on.
  d) Economic benefits : Better operational cost, fewer infrastructure costs, and transactional costs.

Q.3 Discuss applications of blockchain in retail banking.

Ans. : Blockchain technology can be used in retail banking more effectively and efficiently.

1. **Remittances :** Cross-border payments are increasing day by day. What's more is that the market is about to expand its growth 3% per year. However, traditional payment processing tends to be opaque, highly mediated, and clunky, which results in higher fees. However, blockchain technology can help to reduce this effect.
2. **ID fraud prevention :** Blockchain technology has also been tested and rolled out for effective ID fraud prevention and detection. With private key management, blockchain technology can help the customers to share and control their data without any intermediary.
3. **Risk assessment with the use of customer data :** Retail banking companies can use blockchain technology to gather a large volume of data that can be protected and anonymized by the encryption protocols of ledgers. Additionally, to make better risk-management decisions, banks can view data theoretically that any bank has uploaded on the network. The result would be in the form of more efficient processes, potential for more informed credit allocation process as well as faster decision.

6.3 Government Sector

Q.4 Explain blockchain applications in government sector.

Ans. :

1. **Record management :** National, state and local governments are responsible for maintaining individuals' records such as birth and death dates, marital status or property transfers. Yet managing this data can be difficult and to this day some of these records only exist in paper form.
   - And sometimes, citizens have to physically go to their local government offices to make changes, which is time-

consuming, unnecessary and frustrating. Blockchain technology could simplify this recordkeeping and make the data far more secure.

2. **Identity management :** Proponents of blockchain technology for identity management claim that with enough information on the blockchain, people would only need to provide the bare minimum to prove their identities.
3. **Voting :** Blockchain technology has the ability to make the voting process more easily accessible while improving security. Hackers would be no match to blockchain technology, because even if someone were to access the terminal, they wouldn't be able to affect other nodes.
   - Each vote would be attributed to one ID and with the ability to create a fake ID being impossible, government officials could tally votes more efficiently and effectively.

Q.5 How blockchain helps in developing smart city ?

Ans. : • The primary objective in defining the concept of a smart city is to improve the quality of life of people through conventional infrastructure development by utilizing cutting-edge technologies such as Internet of Things (IoT), Artificial Intelligence (AI), etc., which are being used to create a user-friendly environment that enables interaction with a wide range of digital services and devices.

- The main pillars of a smart city are comprised of physical infrastructure, institutional infrastructure, social infrastructure and economic infrastructure.
- Fig. Q.5.1 shows the application of blockchain within the infrastructure of a smart city.
- In a smart city, the institutional infrastructure takes decisions from the perspective of sustainability by incorporating the opinions of citizens and stakeholders, which are then utilized to define objectives and identify solutions by satisficing.

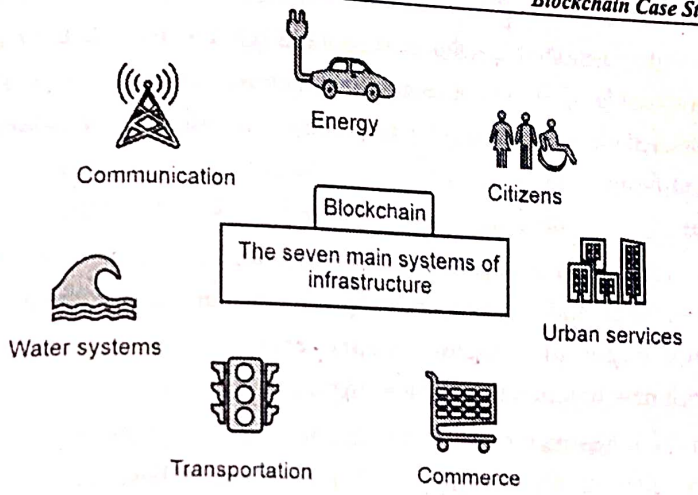


Fig. Q.5.1

- Social infrastructure is a combination of human capital, technical and management tools that improve the quality of life, and instruments that make the concept of sustainability widespread in society.
- Finally, economic infrastructure refers to the financial components that support the best e-business practices and help sustain economic growth.
- For a smart city to become a reality, numerous technological and management tasks must be completed including safeguarding data and addressing sustainability challenges such as pollution, climate change and urbanization.
- Blockchain offers various inherent features for application in urban infrastructure management, which can mitigate or solve the aforementioned problems.
- One of them is decentralization, which is based on the concept that a blockchain operates in a peer-to-peer (P2P) way without the need for trusted central intermediaries. As a result, the likelihood of a central body's operation collapsing can be substantially reduced.

- Another essential quality is immutability. A system is considered immutable if it is not easily corruptible. Since the security of blockchain is built on cryptography with digital signatures for certifying transactions and hash functions for linking the blocks, the system is difficult to mess with and hence, immutable.
- In addition, a blockchain system demonstrates democracy as an additional link to the existing blockchain. It establishes the requirement of consensus among existing nodes, incorporating each new link into the decision-making procedure.
- In the infrastructure area, pseudonymity, security and transparency are also highly significant characteristics. These enhance the security of the system by issuing each blockchain node a pseudonymous address that conceals the node's true identity. This simultaneously boosts transparency and security.

6.4 Healthcare

Q.6 Explain healthcare industry benefits from the use of Blockchains.

Ans. : Benefits :

- By making electronic health records (EHRs) more accessible, more accurate, more secure and less expensive to create and maintain.
- By allowing medical researchers to share their work, collaborate, and gain consent for data collection and access.
- By protecting a healthcare system's data from ransomware and other cyberattacks.
- By making healthcare supply chains more reliable, easier to manage, and less expensive to operate.

Q.7 How blockchain improves electronic health record systems ?

Ans. : • Electronic health records have become the cornerstone of patient care by providing a complete, accurate and accessible history of each individual's medical treatments.

- However, protecting the sensitive personal information contained in EHRs becomes more challenging as health information systems (HIS) become more complex. This is one of the most promising areas of blockchain in healthcare.
- EHRs record patient health data in a digital format that is created and stored by multiple healthcare facilities. The healthcare provider that created the record typically retains primary access to it.
- Individual EHRs tend to be incomplete and are managed inconsistently by the organization that created and maintains them. This means healthcare providers have a fractured view of the patient's medical history.
- Other challenges in making EHRs complete and accessible healthcare histories are interoperability of HISs and access control (authentication).
- Blockchain addresses these shortcomings by linking EHRs and sharing ownership of the records among all stakeholders, along with other security and authentication features.

Q.8 Discuss blockchain healthcare use cases in digital health.

Ans. : 1. Supply chain transparency

- A major test across the healthcare area is ensuring the origin of medical goods to prove their authenticity. Using a blockchain-based system to track items from the manufacturing point and at each stage through the supply chain enables customers to have full visibility and transparency of the goods they are buying.

2. Patient-centric electronic health records

- Healthcare systems in every country and region are stressed and struggling with the problem of data siloes, meaning that patients and their healthcare providers have an incomplete view of medical histories.

3. Smart contracts for insurance and supply chain settlements

- Companies such as Chronicled and Curisium provide blockchain-based systems where various players in the healthcare sector, such as pharmaceutical companies.

4. Medical staff credential verification

- Similar to tracking the attribution of a medical good, blockchain technology can be used to track the experience of medical professionals, where trusted medical institutions and healthcare organizations can record the credentials of their staff, in turn helping to streamline the hiring process for healthcare organizations

5. IoT security for remote monitoring

- One of the biggest trends in digital health is the adoption of remote monitoring solutions, where all kinds of sensors measuring patients' vital signs are being used to help give healthcare practitioners more visibility into patients' health, enabling more proactive and preventative care.

6.5 IoT

Q.9 Explain working of blockchain technology for IoT use cases.

Ans. : • The uses of blockchain IoT depend importantly on the three basic qualities of blockchain technology in the form of a data structure. The three basic properties of blockchain technology that could benefit IoT use cases include,

1. Distribution 2. Decentralization 3. Immutability

- A simple explanation of using these three blockchain properties for improving IoT use cases could verify the feasibility of blockchain IoT projects. Let us assume the example of surveillance cameras as IoT devices to understand how these three traits could benefit IoT.

Now, if a burglar wants to compromise a surveillance camera and prevent the crime from being recorded, they can attack the server which runs the database storing the videos.

1. **Distribution :** • With blockchain, the data does not stay in a single place and is distributed throughout different computers on the network. As a result, it is quite difficult to hack the surveillance system with multiple target devices. In addition, the redundancy in storage offered by blockchain improves security and data access. How ? Users in the IoT ecosystems could easily submit and retrieve their desired data from various devices effortlessly.
2. **Immutability :** • The blockchain IoT use cases are also evident in examples where the burglar might claim that video evidence recorded by surveillance cameras is forged. In such cases, the immutability of blockchain comes to mind. It implies the detection of any changes in the stored data. As a result, the court could verify the burglar's claim by searching for attempts to modify the data.
3. **Decentralization :** • Although immutability and distribution safeguard the integrity of IoT device data on blockchain networks, decentralization could be a prominent setback. Decentralization could open up sensitive data of users to third parties. However, it is possible to find a way around such setbacks. The IoT blockchain use cases could involve the storage of access logs and permissions as a preferred solution.

6.6 Energy and Utilities

Q.10 Explain use of blockchain technology in energy and utilities.

Ans. : • Blockchain use cases in energy and utilities are :

1. **Peer-to-Peer energy trading :** Peer-to-Peer energy (P2P) trading allows consumers to buy and sell excess energy amongst themselves. And credit to distributed ledger technology, blockchain is enabling this by removing mediators, allowing for a truly peer-to-peer exchange. This cuts down the

cost of excess solar energy being escorted back to the grid and gives consumers more control to purchase energy from their neighbors at a cheaper price than their provider.

2. **Renewable Energy Certificates (RECs) :** Another compelling use case can be found for blockchain in energy and sustainability, particularly when it comes to Renewable Energy Certificates (RECs). Through the use of a cryptographically secure unchallengeable digital ledger, providers can mitigate fraud and trace and validate REC transactions instantly and automatically.
3. **Automatic settlement of trades :** Automatic settlement of trades is perhaps one of the most everywhere ways that all types of energy and utilities providers can benefit from blockchain technology. credit to its ability to remove the middlemen, providers can automatically record and settle transactions. Trades can even be done on a peer-to-peer basis thanks to smart contracts and carried out between providers without the need for a clearing house or broker, making for a more streamlined and cost-effective approach.
4. **Microgrids :** Blockchain investment in the energy sector is expected to reach more than $5.8 billion by 2025 with microgrids playing a leading role reducing transmission losses and deferring expensive network upgrades. The nature of microgrid's distributed generation offers efficient energy management, continuity of supply, as well as a reliable back-up power to safeguard against outages.
5. **Smart meters :** Blockchain utilities use cases are also on the rise with a key example being smart meters. Smart meters let for a more accurate recording of the energy that consumers' use since power usage is determined at regular intervals throughout the day. This information is then sent back to the utility sector, traditionally via several intermediaries.

END...