FAQs

Que: Do I have to use your notes for answer writing.

Ans:

- Nope the notes are prepared for students as for reference material, students who are too busy
- Yes, you can use these notes for answer writing.
- Or you can create your own notes or write answer in your word but it has to be specific
- **Do not write YouTube/ChatGPT answers** or any website answer always follow university syllabus mention book for ref. so you score more marks.
- For 8 marks at least fill 3pages, and for 4 marks 1 and a half
- Ignore typos and spelling mistakes
- The notes have been prepared by using book mention in your syllabus
- I have also incorporated a previous year question paper
- To get more previous year question paper visit library
- The paper patter shows the university ask out of syllabus question, so I've also added some questions
- As we move more further, I'll be updating the notes.

Que: How many units are coming in CT-2

Ans: Unit 2, 4 & Unit 5

Que: Where we can get the notes for writing answers

Ans: Refer Book that I have already provided or my notes

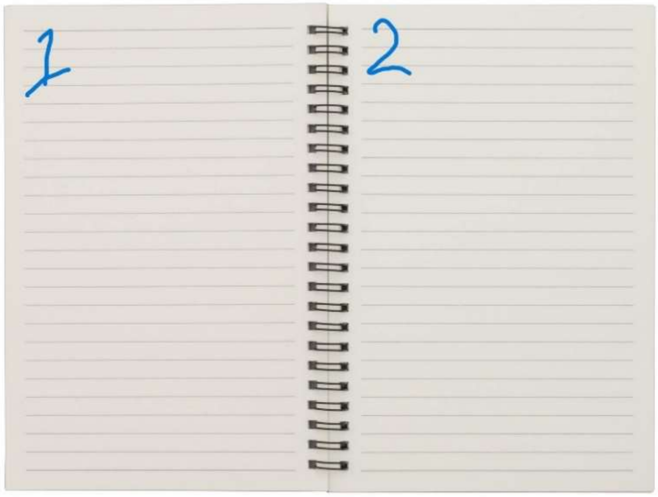
Que: How long should be the answer written

Ans:

- If you are using my notes to write answer then depending on question assigned mark (8/4), you should know how to expand answer into long one, and shrink answer for short one
- For 8 marks you should fill 3 pages, and for 4 marks 1 and a half page. Include diagram where it's necessarily.

Que: What is meant by 3 pages for answer writing

Ans:



NOTE:

- These questions are for reference purpose
- The questions which are highlighted must be your top priority for preparing
- Don't be dependent on question bank, prepare for exam apart from given question provided in question bank, always refer syllabus

Printed Pages - 2 Roll No. ....

CS116503

B.Tech. (Fifth Semester) Examination,

Nov-Dec 2022

[Computer Science Engineering (IoTCS) Branch]

INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Time Allowed: 3 hours

Maximum Marks: 100

Minimum Marks: 35

Note: *All five units are compulsory. Part (a) is compulsory carry 4 marks. Attempts any two parts from (b),(c) & (d) carry 8 marks each.*

CO1:- Understand the basic technology used in Blockchain
CO1: -Understand the working principle of Blockchain systems (mainly Bit coin and Ethereum).
CO1: -Able to understand and design any application specific consensus algorithm
CO1: -Design, build and deploy Smart Contracts and distributed applications,
CO1: -Integrating the Blockchain technology into their own applications/ projects.

Q. No		Questions	Marks	CO	BL	PI
Q.1	a)	What are different types of Blockchain?	4	CO1	1	1.3.1
	b)	What is the advantage of Distributed Record Keeping?	8	CO1	2	2.1.2
	c)	Discuss and Differentiate PoW and PoS.	8	CO1	2	2.1.2
	d)	Draw Blockchain architecture and explain.	8	CO1	2	2.1.2
Q.2	a)	Define Modeling Faults.	4	CO2	1	1.3.1
	b)	What are various Blockchain consensus Algorithm challenges and its solutions?	8	CO2	2	2.1.2
	c)	Discuss Byzantine Model.	8	CO2	2	2.1.2
	d)	Write short note on Zero Knowledge Proofs.	8	CO2	2	2.1.2
Q.3	a)	What do you mean by Crypto currency?	4	CO3	1	1.3.1
	b)	Discuss various Hashing techniques in brief.	8	CO3	2	2.1.2
	c)	Write short notes on Digital Signature.	8	CO3	2	2.1.2
	d)	Explain Elliptic Curve Cryptography with example.	8	CO3	3	3.1.6
Q.4	a)	What is Ethereum?	4	CO4	1	1.3.1
	b)	Explain Ethereum virtual machine with bock diagram.	8	CO4	2	2.1.2

	c)	How Hyperledger implementation is done on ethereum?	8	CO4	2	2.1.2
	d)	What do you mean by Smart Contract?	8	CO4	2	2.1.2
Q.5	a)	What is AltCoins?	4	CO5	1	1.3.1
	b)	Define Merkley Tree with an Example.	8	CO5	2	2.2.3
	c)	Write down Properties of Bitcoin.	8	CO5	2	2.1.2
	d)	What do mean by Double spending? What are the methods to prevent it?	8	CO5	2	2.1.2

CO- Course Outcomes, BL– Bloom's TaxonomyLevels, PI– Performance Indicator

****

Syllabus

UNIT-I Introduction to Blockchain: Need for Distributed Record Keeping, Blockchain architecture, block header detailed design, Abstract Models for Blockchain, Proof of Work (PoW), liveness and fairness, Proof of Stake (PoS) based Chains, Hybrid models (PoW + PoS); Types of Blockchain..

UNIT-II Blockchain Consensus Algorithm challenges and solutions, Modeling faults and adversaries, Byzantine Models of Fault tolerance;
Zero Knowledge proofs and protocols in Blockchain.

UNIT-III Introduction to cryptographic basics for cryptocurrency - a short description of Hashing, digital signature schemes, encryption schemes and elliptic curve cryptography, verifiable random functions.

UNIT-IV Blockchain 2.0: Introduction to Ethereum, Ethereum Virtual Machine (EVM), Wallets for Ethereum, Solidity, Smart Contracts, Attacks on smart contracts,
The Turing Completeness of Smart Contract Languages and verification challenges.
Blockchain 3.0: Hyperledger implementation on Ethereum,
the plug and play platform and mechanisms in permissioned blockchain.

UNIT-V Application of Blockchain: Bitcoin- Bitcoin consensus, Wallet, Bitcoin Blocks, Merkley Tree, hardness of mining, transaction verifiability, anonymity, forks,
double spending, mathematical analysis of properties of Bitcoin. Altcoins. Medical record management systems, DNS records.

UNIT 1

1. What are different type of blockchain?

2. What is the advantage of distributed record keeping?

3. Discuss Blockchain architecture and explain them also write advantage and disadvantages and benefits

4. Discuss and differentiate PoW and PoS

5. Write benefits of blockchain

6. What are the key characteristics of blockchain architecture?

7. What is distributive ledger technology, also write its feature

8. How DLT can replace traditional book-keeping method

Or

What is distributive ledger technology? also write its feature

9. Explain proof of work also write challenges with PoW

10. What is proof of stake? How does proof of stake work, also write challenges

11. Write the advantages of PoS

12. Write short note on

Block header detailed design

13. What is blockchain technology? Why is blockchain technology important?

14. Discuss the blockchain use in different industries

15. What are decentralized application?

16. Explain in detail about blockchain platform

17. How blockchain is revolutionizing the tadeonal business system? Explain the future of blockchain with example

18. Short note on

1. Hybrid model (PoW + PoS)

2. types of blockchain

UNIT 2

1. Defining modelling faults
2. What are various blockchain consensus algorithm challenges and its solutions
3. Discuss Byzantine general model
4. Write short note on Zero Knowledge proofs
5. Under Consensus Algorithm: Explain the proof of elapsed time(PoET)
6. Under Consensus Algorithm: Explain proof of burn(PoB)

UNIT 3

1. What do you mean by cryptocurrency?

2. Discuss various hashing techniques in brief?

3. Write short note on digital signature

4. Explain elliptic curve cryptography with example.

5. Explain some best know cryptocurrency

6. Explain fiat currency (traditional currency) Vs crypto currency

7. How does cryptocurrency work? How to buy crypto currency also write advantage and disadvantages of crypto currency

8. How to store crypto currency

9. Short note on

   verifiable random functions.

10. Write short note on future of cryptocurrency

UNIT 4

1. What is Ethereum?
   Or
   What is Ethereum network?
2. Explain Ethereum virtual machine with block diagram
3. How Hyperledger implementation is done on Ethereum?
4. What do you mean by Smart Contract
5. Write short note on Turing complete Vs Turing incomplete
6. What is Ethereum gas?
7. What are the types of users in the Ethereum network
8. Discuss in detail the component of Ethereum
9. Describe the following
   1. Ethereum virtual machine
   2. Ether scripter
10. What are the advantage and disadvantage of Ethereum
11. Give and introductory note on Hyperledger
12. Explain the history of Hyperledger
13. Explain the component of Hyperledger
14. What are the advantage and disadvantage of Hyperledger
15. What is meant by digital token? Explain with example
16. What is initial coin offering (ICO)
17. What is mist browser also write what is Ethereum mist wallet with its feature
18. What is solidity? Give its feature
19. Write short note on smart contract
20. What is solidity interface and its characteristics, also explain abstract contract vs interface
21. What is Hyperledger fabric what are its benefits,
22. How smart contract can be attacked
23. What is mechanism in permissioned blockchain
24. What is plug and play platform

UNIT 5

1. What is AltCoins?
   Or
   Explain some best known cryptocurrency/AltCoins
2. Define Merkley tree with an example
3. Write down properties of Bitcoin
4. What do you mean by double spending? What are the methods to prevent it
5. Explain briefly structure of Blockchain block
6. What is bitcoin? Write brief history of bitcoin
7. Write several feature of bitcoin
8. How do bitcoin transaction work
9. How do bitcoins come into market
10. How does bitcoin mining work
    Or
    Explain bitcoin mining
11. What do you mean by value of bitcoin
12. Write short note on community, policy and regulation in bitcoins
13. What are the advantage and disadvantage of bitcoins
14. What is MetaMask, How to install and use MetaMask
15. Explain about the brief history of MetaMask and give its feature
16. What is MetaMask transaction? Explain the steps involved in MetaMask transactions
17. Write short note on
    1. Transaction verification
    2. Medical record management systems
    3. DNS records
    4. Mathematical analysis of bitcoin properties

UNIT: 1

Q.1. What is blockchain technology? Why is blockchain important?

Ans. Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network. A blockchain database stores data in blocks that are linked together in a chain. The data is chronologically consistent because we cannot delete or modify the chain without consensus from the network. As a result, we can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts and other transactions. The system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of these transactions.

Importance - Traditional database technologies present several challenges for recording financial transactions. For instance, consider the sale of a property. Once the money is exchanged, ownership of the property is transferred to the buyer. Individually, both the buyer and the seller can record the monetary transactions, but neither source can be trusted. The seller can easily claim they have not received the money even though they have, and the buyer can equally argue that they have paid the money even if they have not.

To avoid potential legal issues, a trusted third party has to supervise and validate transactions. The presence of this central authority not only complicates the transaction but also creates a single point of vulnerability. If the central database was compromised, both parties could suffer. Blockchain mitigates such issues by creating a decentralized, tamper-proof system to record transactions. In the property transaction scenario, blockchain creates one ledger each for the buyer and the seller. All transactions must be approved by both parties and are automatically updated in both of their ledgers in real time. Any corruption in historical transactions will corrupt the entire ledger. These properties of blockchain technology have led to its use in various sectors, including the creation of digital currency like Bitcoin.

Q.2. Discuss the use of blockchain in different industries.

Ans. Blockchain is an emerging technology that is being adopted in innovative manner by various industries. Some different industries using blockchain are discussed below -

(i) **Energy** - Energy companies use blockchain technology to create peer-to-peer energy trading platforms and streamline access to renewable energy. For example, consider these uses

(a) Blockchain-based energy companies have created a trading platform for the sale of electricity between individuals. Homeowners with solar panels use this platform to sell their excess solar energy to neighbours. The process is largely automated - smart meters create transactions and blockchain records them.

(b) With blockchain-based crowd funding initiatives, users can sponsor and own solar panels in communities that lack energy access. Sponsors might also receive rent for these communities once the solar panels are constructed.

(ii) **Finance** - Traditional financial systems, like banks and stock exchanges, use blockchain services to manage online payments, accounts and market trading.

(iii) **Media and Entertainment**-Companies in media and entertainment use blockchain systems to manage copyright data. Copyright verification is critical for the fair compensation of artists. It takes multiple transactions to record the sale or transfer of copyright content.

(iv) **Retail**- Retail companies use blockchain to track the movement of goods between suppliers and buyers.

Q.3. Write some benefits of blockchain.

Ans. Some benefits of blockchain are as follows –

(i) It is safer than any other technology.

(ii) To avoid possible legal issues, a trusted third party has to supervise the transactions and validate the transactions.

(iii) There is no one central point of attack.

(iv) Data cannot be changed or manipulated; it is immutable.

Q.4. Explain briefly the structure of blockchain

Ans. Structure of Blockchain - Blockchain is a technology where multiple parties involved in communication can perform different transactions without third-party intervention. Verification and validation of these transactions are carried out by special kinds of nodes.

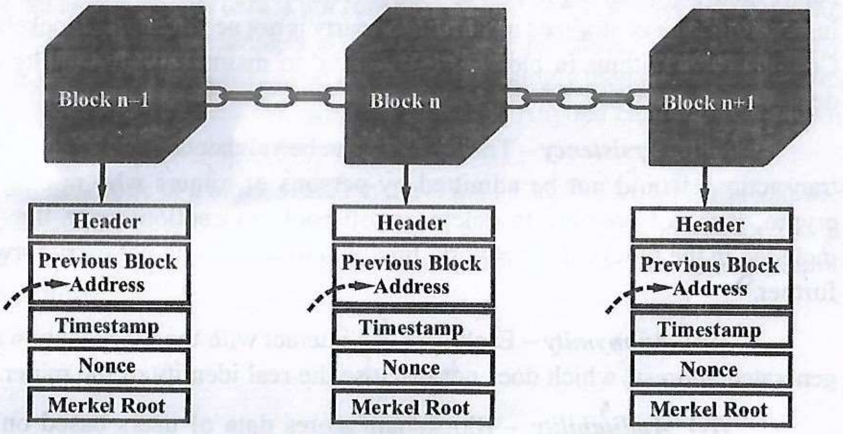


Fig. 1.1 Structure of Blockchain

(i) **Header** - It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also three sets of block metadata are contained in the block header.

(ii) Previous Block Address/Hash - It is used to connect the i + 1,h block to the 'Ith block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.

(iii) Timestamp - It is a system verify the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.

(iv) Nonce - A nonce number which uses only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test and eliminate many nonce per second until they find that valuable nonce is valid.

(v) Market Root - It is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.

Q.5. What are the key characteristics of blockchain architecture ?

Ans. Key characteristics of blockchain architecture are as follows -

(i) **Decentralization** - In centralized transactions systems, each transaction needs to be validated in the central trusted agency (e.g., the central bank), naturally resulting in cost and the performance jam at the central servers. In contrast to the centralized mode, a third party is not needed in the blockchain. Consensus algorithms in blockchain are used to maintain data stability in a decentralized network.

(ii) **Persistency** - Transactions can be validated quickly and invalid transactions would not be admitted by persons or miners who mining the crypto. It is not possible to delete or roll back transactions once they are included in the blockchain network. Invalid transactions do not carry forward further.

(iii) **Anonymity** - Each user can interact with the blockchain with a generated address, which does not disclose the real identity of the miner.

(iv) **Auditability** - Blockchain stores data of users based on the unspent transaction output (UTXO) model. Every transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the position of those referred unspent transactions switches from unspent to spent. Due to this process, the transactions can be easily tracked and not harmed between transactions.

(v) **Transparency** - The transparency of blockchain is like cryptocurrency, in Bitcoin for tracking every transaction is done by the address. And for security, it hides the person's identity between and after the transaction. All the transactions are made by the owner of the block associated with the address, this process is transparent and there is no loss for anyone who is involved in this transaction.

(vi) **Cryptography** - The blockchain concept is fully based on security and for that, all the blocks on the blockchain network want to be secure. And for security, it implements cryptography and secures the data using the cipher text and ciphers.

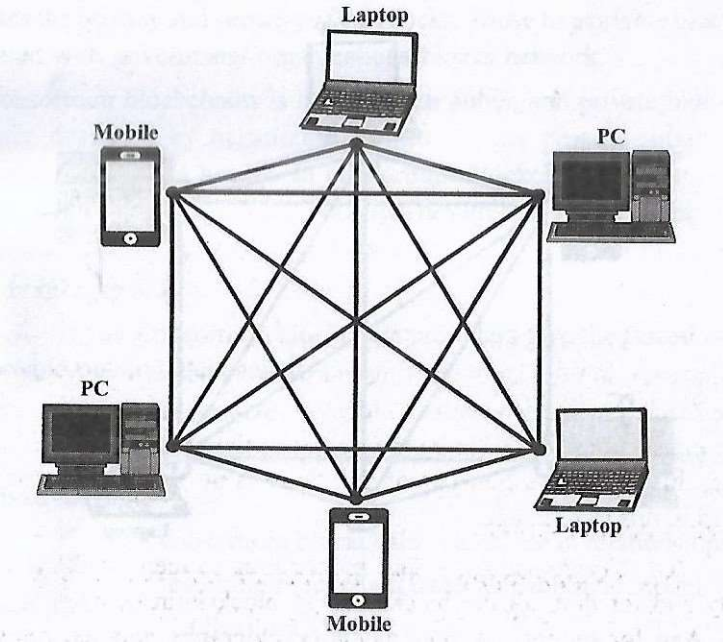
Q.6. Explain the different types of blockchain architecture with advantages and disadvantages.

Or

Types of blockchain`

Ans. Different types of blockchain architecture are as follows -

(i) **Public Blockchain** - A public blockchain is a concept where anyone is free to join and take part in the core activities of the blockchain network. Anyone can read, write, and audit the ongoing activities on a public blockchain network, which helps to achieve the self-determining, decentralized nature often authorized when blockchain is discussed. Data on a public blockchain secure as it is not possible io modify once they are validated. The public blockchain is fully decentralized, it has access and control over the ledger, and its data is not restricted to persons, is always available and the central authority manages all the blocks in the chain. There is publicly running all operations. Due to no one handling it singly then there is no need to get permission to access the public blockchain. Anyone can set his/her own node or block in the network/chain. After a node or a block settled in the chain of the blocks, all the blocks are connected like peer-to-peer connections. If someone tries to attack the block then it forms a copy of that data and it is accessible only by the original author of the block.



Advantages -

(a) A public network operates on an actuate scheme that encourages new persons to join and keep the network better.

(b) There is no agreement in the public blockchain.

(c) This means that a public blockchain network is immutable.

(d) It has rapid transactions.

Disadvantages -

(a) Public blockchain can be costly in some manner.

(b) The person need not give identity, that is why there is a possibility of corruption of the block if it is in under attack.

(c) Processing speed is sometimes slow.

(d) It has integration issues.

(ii) **Private Blockchain** - Miners need permission to access a private blockchain. It works based on permissions and controls, which give limit participation in the network. Only the entities participating in a transaction will have knowledge about it and the other stakeholders not able to access it. By it works on. the basis of permissions due to this it is also called a permission- based blockchain. Private blockchains arc not like public blockchains it is

managed by the entity that owns the network. A trusted person is in charge of the running of the blockchain it will control who can access the private blockchain and also controls the access rights of the private chain network. There may be a possibility of some restrictions while accessing the network of private blockchain.

Advantages —

(a) In a private blockchain, users join the network using the Inv nations and all are verified.

(b) Only permitted users/persons can join the network.

(c) Private blockchain is partially immutable.

Disadvantages -

(a) A private blockchain has trust issues, due to exclusive information being difficult to access it.

(b) As the number of participants increases, there is a possibility of an attack on the registered users.

(iii) **Consortium Blockchain** - A consortium blockchain is a concept where it is permissioned by the government and a group of organizations, not by one person like a private blockchain. Consortium blockchains are more decentralized than private blockchains, due to being more decentralized it increases the privacy and security of the blocks. Those like private blockchains connected with government organizations blocks network. Consortium blockchains is lies between public and private blockchains. They are designed by organizations and no one person outside of the organizations can gain access. In consortium blockchains all companies in between organizations collaborate equally. They do not give access from outside of the organizations/consortium network.

Advantages -

(a) Consortium blockchain providers give the fastest output as compared to public blockchains.

(b) It is scalable.

(c) A consortium blockchain is low transaction costs.

Disadvantages -

(a) A consortium blockchain is unstable in relationships.

(b) Consortium blockchain lacks an economic model.

(c) It has flexibility issues.

Q. 7. What are the core components of blockchain architecture ?

Ans. Core components of blockchain architecture are given below -

(i) **Node -** Nodes are network participants and their devices permit them to keep track of the distributed ledger and serve as communication hubs in various network tasks. A block broadcasts all the network nodes when a miner looks to add a new block in transactions to the blockchain.

(ii) **Transactions** - A transaction refers to a contract or agreement and transfers of assets between parties The asset is typically cash or property The network of computers in blockchain stores the transactional data as copy with the storage typically referred to as a digital ledger.

(iii) **Block** - A block in a blockchain network is similar to a link in a chain. In the field of cryptocurrency, blocks are like records that store transactions like a record book and those are encrypted into a hash tree. There are a huge number of transactions occurring every day in the world. It is important for the users to keep track of those transactions, and they do it with the help of a block structure

(iv) **Chain** - Chain is the concept where all the blocks are connected with the help of a chain in the whole blockchain structure in the world. And those blocks are connected with the help of the previous block hash and it indicates a chaining structure.

(v) **Miners** - Blockchain mining is a process that validates every step in the transactions while operating all cryptocurrencies. People involved in this mining they called miners. Blockchain mining is a process to validate each step in the transactions while operating cryptocurrencies.

(vi) **Consensus** - A consensus is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record keeping and other things.

Q.8. Explain blockchain data structure.

Ans. The blockchain data structure is a back-linked list of blocks of transactions, which is ordered. It can be stored as a flat file or in a simple database. Each block is identifiable by a hash, generated using the SHA 256 cryptographic hash algorithm on the header of the block. Each block references a previous block, also known as the parent block, in the "previous block hash" field, in the block header.

A hash, also known in long form as cryptographic hash function, is a mathematical algorithm (hut maps data of arbitrary size to a bit string of a fixed size. In the case of SHA 256, the result is a string of 32 bytes. The resultant 32 bytes makes it effectively impossible to reverse the output, since the function was designed to be a one-way function. The idea behind a hash functions use is to facilitate a thorough means for searching for data in a dataset. The most basic form of hash function is any function that can used to map data of arbitrary size to data of fixed size. This output is a bit string known as the hash value, hash sum or hash code. The hash values can be stored in a tabular form known as a hash table and is an efficient indexing mechanism; especially useful in search performance.

Hash functions are collision-free too. That means it is impossible to find two messages that hash to the same hash value. Therefore, when given a compact hash, one can confirm that it matches a particular input datum. Blocks can be identified from their hash, serving two purposes; identification and integrity verification.

Bitcoin hashing function makes use of the SHA 256, applied twice, see (National Institute of Standards and Technology, 2015). It generates an almost- unique, fixed size 256-bit (32-byte) hash security. Large classes of hash functions are based on a building block of a compression function.

Each block contains the hash of its parent inside its own header. There lays a chain going all the way back to the first block created, also known as the genesis block, linked together by a sequence of hashes. The "previous block hash" field is inside the block header and thereby the current block hash is dependent on the parent block hash. The child's own identity changes if the parent's identity changes. When the parent is modified in any way, the parent's hash changes. The parent's changed hash necessitates an alteration in the "previous block hash" pointer of the child. This in turn causes the child's hash to mutate, which requires a change in the pointer of the grandchild, which in turn alters the grandchild and so on.

This cascading effect ensures that, once a block has many generations succeeding it, it cannot be changed without consequently forcing a recalculation of all the subsequent blocks. Because such a recalculation would require an enormous amount of computation, the existence of a long chain of blocks fortifies the Blockchain's deep history to be immutable; a key feature of blockchain technology security.

Q.9. What is distributed ledger technology (DLT)? Also write its features.

Ans. Distributed ledger technology (DLT) is centred around an encoded and distributed database where records regarding transactions are stored. A distributed ledger is a database that is spread across various computers, nodes, institutions or countries accessible by multiple people around the globe.

Features of DLT -

(i) **Decentralized** - It is a decentralized technology and every node will maintain the ledger, and if any data changes happen, the ledger will get updated. The process of updating takes place independently at each node. Even small updates or changes made to the ledger are reflected and the history of that change is sent to all participants in a matter of seconds.

(ii) **Immutable** - Distributed ledger uses cryptography to create a secure database in which data once stored cannot be altered or changed.

(iii) **Append Only**- Distributed ledgers are append-only in comparison to the traditional database where data can be altered.

(iv) **Distributed** • In this technology, there is no central server or authority managing the database, which makes the technology transparent. To counter the weaknesses of having one ledger to rule all, so that there is no one authoritative copy and have specific rules around changing them. This would make the system much more transparent and will make it a more decentralized authority. In this process, every node or contributor of the ledger will try to verify the transactions with the various consensus algorithms or voting. The voting or participation of all the nodes depends on the rules of that ledger. In the case of Bitcoin, the Proof of Work consensus mechanism is used for the participation of each node.

(v) **Shared**-The distributed ledger is not associated with any single entity. It is shared among the nodes on the network where some nodes have a full copy of the ledger while some nodes have only the necessary information that is required to make them functional and efficient.

(vi) **Smart Contracts** - Distributed ledgers can be programmed to execute smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This allows for transactions to be automated, secure and transparent.

(vii) **Fault Tolerance** - Distributed ledgers are highly fault-tolerant because of their decentralized nature. If one node or participant fails, the data remains available on other nodes.

(viii) **Transparency** - Distributed ledgers are transparent because every participant can see the transactions that occur on the ledger. This transparency helps in creating trust among the participants.

(ix) **Efficiency**-The distributed nature of ledgers makes them highly efficient. Transactions can be processed and settled in a matter of seconds, making them much faster than traditional methods.

(x) **Security** - Distributed ledgers are highly secure because of their cryptographic nature. Every transaction is recorded with a cryptographic signature that ensures that it cannot be altered. This makes the technology highly secure and resistant to fraud.

Q.10. How DLT can replace traditional book-keeping methods?

Ans. Distributed ledger technology has the potential to effectively improve these traditional methods of book-keeping by updating and modifying fundamental methods of how data is collected, shared and managed in the ledger. To understand this, traditionally paper-based and conventional electronic ledgers were used to manage data that had centralized point ot control, ihis types of system require high computing resource and labour to maintain ledgers and also had many points of failure.

Points of failure like -

(i) Mistakes made during data entry.

(ii) Manipulation of data could happen which increases the risk of

errors.

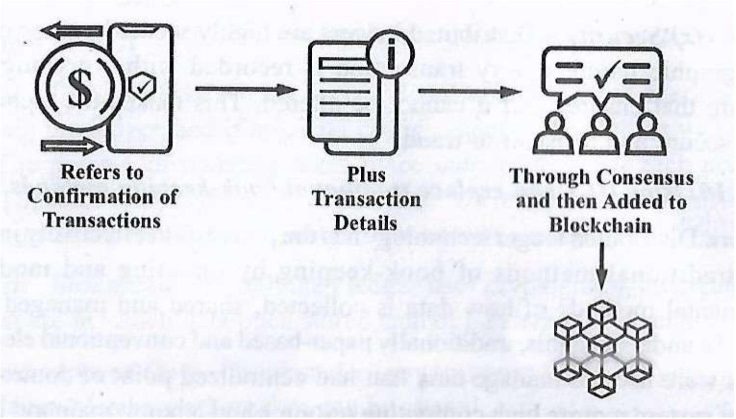
(iii) Other participants contributing data to the central ledger will not able to verify the legitimacy of data coming from other sources.

However, DLT allows real-time sharing of data with transparency which gives trust that data in the ledger is up to date and legitimate. Also distributed ledger technology eliminates the single point of failure which prevents data in the ledger from being manipulations and errors. In DLT, there is no need for a central authority to validate transactions here different consensus mechanisms are used to validate transactions which eventually makes this process very fast and real-time. Similarly, DLT can reduce the cost of transactions because of this process.

Q.ll. What is block validation? Explain in detail with example.

Ans. Block validation refers to a process in the blockchain where a group of participants operate different nodes to validate (and verify) the transactions. The prime purpose of this process is to confirm all the transactions before adding them to the blockchain or database.

Block validation within the realm of blockchain technology involves a group of validators operating nodes to confirm the legitimacy of transactions. Typically, these validators run on full nodes, meticulously assessing transaction details to ensure their authenticity. Upon successful verification, these transactions are integrated into the chain of blocks and also become part of the online distributed ledger. Additionally, the validated data contributes to the Merkle tree root node for storage, as this process relics on mathematical proofs and cryptographic hashing. In essence, expected attributes for block validation are integral to the functioning of the blockchain.



Refers to Confirmation of Transactions
Plus Transaction Details
Through Consensus and then Added to Blockchain

Process - The Bitcoin block validation process within the blockchain involves several key steps, as follows -

(i) **Gathering Transactions** - The process begins with the gathering of transactions broadcast on the network by validators. They select transactions, considering factors like transaction fees, to include in the upcoming block. The selection may also involve other criteria based on the specific blockchain.

(ii) **Validating Details** - Validators meticulously verify transaction details, including sender and recipient addresses, to ensure they meet the necessary criteria for inclusion in the block. This verification process is essential for upholding the integrity of the blockchain.

(iii) **Solving Cryptographic Puzzles** - After validating transaction details, validators engage in a process known as mining. In this step, they compete to solve a cryptographic puzzle by finding the appropriate nonce that, when hashed, results in a hash with specific properties, typically lower than a target value. This resource-intensive process adds security to the network and determines the creation of a new block.

(iv) **Forming a Consensus** - Miners, through their validation efforts, contribute to reaching a consensus on which block should be added to the blockchain. The network agrees on the longest valid chain, ensuring consensus and the continued growth of the blockchain.

(v) **Creating and Submitting Blocks** - Once a validator successfully mines a new block and achieves consensus, the block is added to the blockchain. In the case of Bitcoin, miners are rewarded with newly created Bitcoins, which serve as block rewards. The process must be completed within the required timeframe. Ethereum, on the other hand, employs a staking mechanism as part of its transition to the Proof of Stake (PoS) protocol. Validators must lock up a certain amount of Ether as collateral to participate in the block validation process.

Example Suppose Alfred is a validator in the Bitcoin blockchain. He actively participates in the process of validating transactions on the network. Alfred has successfully earned more than 50 BTC as a reward for his contributions. To validate transactions, Alfred has set up a mining rig with both conventional ASIC systems and advanced GPVs.

One day, Alfred notices a significant number of pending transactions on the Bitcoin network. He decides to gather a selection of these transactions based on transaction fees, a common criterion used for prioritization. Alfred then begins the validation process. In a short time, Alfred successfully validates and includes around 1,000 transactions in a new block. However, achieving consensus in the Bitcoin network can be a competitive process, as miners worldwide are racing to add their blocks to the blockchain. Eventually, Alfred's block is included in the Bitcoin blockchain, and as a reward for his validation efforts, he receives 50 BTC.

Q.12. Who is a blockchain validator? Explain.

Ans. A blockchain validator is a network node that helps process and validate transaction blocks on the platform so that they can be added to the permanent ledger of the blockchain. When using the term "validator", some people presume the nodes validating transactions on PoS blockchains. They contrast it with the term "miner", used on PoW blockchain platforms.

However, block validation is a process equally applicable to both of these blockchain varieties. The more correct synonym for mining, applicable to PoS blockchains, would be staking, the process of block validation used on this type of platform.

As transactions on the blockchain are initiated by users, they are queued on the network for subsequent validation. Validator nodes then batch individual transactions into a block to verify it. Each blockchain has its own rules pertaining to the number of transactions per block. When the block has been completed, validators process it to add it to the blockchain as a permanent record.

On some blockchains, validators may choose which transactions to batch to a block. This selection is not necessarily in chronological order, but is driven n by the validator's preferences, typically based on transaction fees involved.

The fees are added to each blockchain transaction by the sender of crypto assets as an incentive for validators. Senders may choose the fee amount, and could even send a transaction without any fees at all.

However, transactions with very low or no fees are more likely to be ignored by validators and thus, might remain in an unconfirmed state for long periods of time. If, after a while, the transaction is not added to a block for validation, it is normally dropped Irom the network.

The actual process of validating a block differs between PoW-based blockchains, such as Bitcoin (BTC) or Ethereum (ETH), and PoS blockchains, such as Solana (SOL) or Ethereum 2.0.

Q.13. Explain the proof of work.

Ans. Cryptocurrencies do not have centralized gatekeepers to verify the accuracy of new transactions and data that are added to the blockchain. Instead, they rely on a distributed network of participants to validate incoming transactions and add them as new blocks on the chain.

Proof of work is a consensus mechanism to choose which of these network participants, called miners are allowed to handle the lucrative task of verifying new data. It is lucrative because the miners are rewarded with new crypto when they accurately validate the new data and do not cheat the system.

"Proof of work is a software algorithm used by Bitcoin and other blockchains to ensure blocks are only regarded as valid if they require a certain amount of computational power to produce". It is a consensus mechanism that allows anonymous entities in decentralized networks to trust one another.

The "work" in proof of work is key -- The system requires miners to compete with each other to be the first to solve arbitrary mathematical puzzles to prevent anybody from gaming the system. The winner of this race is selected to add the newest batch of data or transactions to the blockchain.

Winning miners only receive their reward of new cryptocurrency after other participants in the network verify that the data being added to the chain is correct and valid.

Q.14. Why is proof of work important?

Ans. The first cryptocurrency, Bitcoin, was created by Satoshi Nakamoto in 2008. Nakamoto published a famous white paper describing a digital currency based on proof of work protocols that would allow secure, peer-to-peer transactions without the involvement of a centralized authority. One of the issues that had prevented the development of an effective digital currency in the past was called the double-spend problem. Cryptocurrency is just data, so there needs to be a mechanism to prevent users from spending the same units in different places before the system can record the transactions.

While you'd have a hard time spending the same dollar bill on two separate purchases, anyone who's duplicated a computer file by copying and pasting can probably imagine how you could spend digital money twice - even ten times or more.

Nakamoto's consensus mechanism solved the double-spend problem. By incentivizing miners to verify the integrity of new crypto transactions before adding them to the distributed ledger that is blockchain, proof of work helps prevent double spending.

Q.15. Explain the challenges with PoW.

Ans. The proof-of-work consensus mechanism has some issues which are as follows -

(i) **The 51% Risk** - If a controlling entity owns 51% or more than 51% of nodes in the network, the entity can corrupt the blockchain by gaining the majority of the network.

(ii) **Time-consuming** - Miners have to check over many nonce values to find the right solution to the puzzle that must be solved to mine the block, which is a time-consuming process.

(iii) **Resources Consumption** - Miners consume high amounts of computing power in order to find the solution to the hard mathematical puzzle. It leads to a waste of precious resources (money, energy, space, hardware). It is expected that 0.3% of the world's electricity will be spent to verify transactions by the end of 2028.

(iv) **Not Instantaneous Transaction** - Transaction confirmation takes about 10-60 minutes. So, it is not an instantaneous transaction because it takes some time to mine the transaction and add it to the blockchain thus committing the transaction.

Q.16. What is proof of stake ? How does proof of stake work ?

Or

Explain the proof of stake.

Ans. Proof of stake is a type of consensus mechanism used to validate cryptocurrency transactions. With this system, owners of the cryptocurrency can stake their coins, which gives them the right to check new blocks of transactions and add them to the blockchain.

This method is an alternative to proof of work, the first consensus mechanism developed for cryptocurrencies. Since proof of stake is much more energy-efficient, it has gotten more popular as attention has turned to how crypto mining affects the planet.

Working of Proof of Stake - The proof-of-stake model allows owners of a cryptocurrency to stake coins and create their own validator nodes. Staking is when you pledge your coins to be used for verifying transactions. Your coins are locked up while you stake them, but you can unstack them if you want to trade them.

When a block of transactions is ready to be processed, the crypto- currency's proof-of-stake protocol will choose a validator node to review the block. The validator checks if the transactions in the block are accurate. If so, they add the block to the blockchain and receive crypto rewards for their contribution. However, if a validator proposes adding a block with inaccurate information, they lose some of their staked holdings as a penalty.

Q.17Write the advantages of Proof of stake.

Ans. Advantages of proof of stake are as follows -

(i) **Energy Efficiency** - PoS requires significantly less computational power compared to PoW because it does not rely on miners solving complex mathematical puzzles to validate transactions. This reduces the environmental impact of blockchain networks and makes them more sustainable.

(ii) **Security**- PoS can provide a high level of security by incentivizing participants to behave honestly. Validators (also called "forgers" or "stakers") in a PoS network are required to lock up a certain amount of cryptocurrency as a stake. If they validate fraudulent transactions or try to attack the network, they risk losing their stake. This economic disincentive helps maintain the network's integrity.

(iii) **Decentralization** - PoS can contribute to a more decentralized network compared to PoW, especially in terms of mining power distribution. Since PoS does not require expensive mining equipment, it allows a broader range of participants to become validators, promoting a more distributed network.

(iv) **Scalability** - PoS is often seen as more scalable than PoW because it does not face the same limitations related to block size and transaction throughput. This is because the consensus mechanism does not rely on solving computationally intensive puzzles, allowing for faster transaction processing.

(v) **Incentives for Holding Tokens** - PoS encourages participants to hold and stake their tokens, as they can earn rewards for validating

transactions. This can lead to increased token retention and liquidity, benefiting he overall health of the network.

Q.18. What are the issues with proof-of-stake mechanism?

Ans. Various issues with proof of stake are as follows -

(i) **Security Issues** - One of the biggest criticisms of PoS is that it is less secure than PoW. Because PoS does not require miners to expend energy in order to participate in the consensus process, it is possible for individuals with malicious intent to take control of the network by acquiring a large number of stake tokens. This could lead to security breaches and the theft of funds from users of the blockchain network.

(ii) **Lack of Decentralization** - Another issue with PoS is that it can lead to a lack of decentralization, as smaller nodes can easily be overpowered by larger ones. This is because PoS systems rely on delegates who are chosen to validate transactions and maintain the network. Larger nodes can easily control the selection of delegates, making it more difficult for smaller nodes to participate in the consensus process. As a result, PoS networks can become less decentralized over time, which goes against one of the key principles of blockchain technology.

(iii) **Poor Scalability** - PoS is also often criticized for its poor scalability. This is because PoS systems are not as efficient as PoW systems when it comes to handling large numbers of transactions. And so, blockchains that use PoS can experience slower transaction speeds and higher fees than those that use PoW.

(iv) **Inefficient Use of Resources** - Another issue with PoS is that it can lead to the inefficient use of resources. This is because PoS systems require all nodes in the network to be online in order to achieve consensus. Consequently, networks that use PoS often have high energy consumption and low network efficiency.

(v) **Centralization of Power** - Lastly, one of the biggest criticisms of PoS is that it can lead to the centralization of power. This is because PoS systems rely on a small number of "validators" or "delegates" to approve transactions and maintain the network. If these validators are controlled by a single entity, it could lead to a situation where this entity has complete control over the blockchain network. This would be contrary to the principle of decentralization that is fundamental to blockchain technology.

While PoS does have some advantages over PoW, its many drawbacks make it a less desirable consensus mechanism for blockchain networks. In order to achieve true decentralization and security, it is important to use a consensus mechanism that is both secure and efficient. For this reason, PoW remains the best option for blockchain networks.

Q19. Explain hybrid model (POW & POS)

Ans. A hybrid PoW/PoS consensus combines both Proof of Work and Proof of Stake in one blockchain system. The goal is to take advantage of the security and decentralization of PoW, while also benefiting from the energy efficiency and speed of PoS.

In such a hybrid system, both mechanisms play distinct roles. Typically, PoW is used for securing the blockchain at the level of block creation, while PoS is used for tasks like block validation or attestation.

Hybrid PoW/PoS Model

1. Dual Mechanism: PoW and PoS are combined in such a way that both miners and validators are involved in block creation and validation. This may mean that PoW miners are responsible for producing blocks, while PoS validators are responsible for confirming or finalizing the validity of those blocks.
2. Security: PoW provides the blockchain with strong security against Sybil attacks and double-spending through the computational difficulty required to mine blocks. PoS provides an economic disincentive for bad behavior. If a validator acts maliciously, they can lose their staked funds.
3. Energy Efficiency: PoS improves energy efficiency since validators do not need to solve computationally expensive puzzles. This mitigates the high energy consumption of PoW and allows the system to scale more efficiently.
4. Prevention of 51% Attacks: The hybrid model helps reduce the risk of a 51% attack (where an attacker controls over half of the network's computational power or staked funds). In a hybrid model, an attacker would need to control both the majority of mining power and the majority of the staked assets, which is significantly harder to achieve.
5. Block Validation:Blocks are typically produced by miners (using PoW), but validators (using PoS) must attest to the validity of the blocks before they are added to the chain. This adds an additional layer of security and consensus.

Examples of Hybrid PoW/PoS Blockchains

Several blockchain networks have implemented or are experimenting with hybrid PoW/PoS consensus models. Here are a few examples:

1. Decred (DCR): Decred is one of the most prominent examples of a hybrid PoW/PoS model. It uses PoW mining for block creation and PoS staking for block validation and governance.

2. Ethereum 2.0 (ETH): Ethereum, in its transition to Ethereum 2.0, uses a hybrid approach during the migration from Proof of Work (PoW) to Proof of Stake (PoS).

3. Titanium Blockchain (TTN): Titanium Blockchain is another blockchain project that combines both PoW and PoS to secure its network and make it more decentralized.

Unit: 2

Que1: Explain different type of consensus algorithm challenges and provide solution

Ans. Consensus algorithms are fundamental to blockchain networks. They enable participants (or nodes) in a decentralized network to agree on the validity of transactions and the ordering of blocks without relying on a central authority. While consensus mechanisms like Proof of Work (PoW), Proof of Stake (PoS), and others have been pivotal in achieving decentralized agreement, they each come with their own set of challenges. Below are some common challenges associated with blockchain consensus algorithms, along with potential solutions or advancements designed to address these issues.

1. Scalability Issues

Challenge: Scalability refers to the ability of a blockchain to handle a growing number of transactions or users efficiently. Consensus mechanisms such as Proof of Work (PoW), which underpins Bitcoin, suffer from scalability issues due to:

  - Limited transaction throughput (e.g., Bitcoin can handle 3-7 transactions per second).
  - Increased block propagation time as the network grows.
  - The high computational cost and time required for mining in PoW.

Solution: Layer 2 Solutions:

  - Lightning Network (for Bitcoin) and Raiden Network (for Ethereum) are examples of Layer 2 solutions that operate on top of blockchains to increase transaction throughput without altering the underlying consensus mechanism.
  - These solutions allow off-chain transactions that are later settled on the main blockchain, significantly improving scalability.

- Sharding:
  - Sharding involves dividing the blockchain into smaller parts (shards), each capable of processing its own set of transactions. Sharding can increase the overall capacity of the network by allowing parallel processing of transactions across multiple shards.
  - Ethereum 2.0 plans to implement sharding as part of its transition from PoW to Proof of Stake (PoS) to enhance scalability.
- Consensus Alternatives:
  - Proof of Stake (PoS): PoS is more scalable than PoW because it requires much less computational effort. Validators in PoS are chosen based on their stake, not computational power, reducing energy consumption and the time required for block production.

    - Delegated Proof of Stake (DPoS): DPoS, used by platforms like EOS and Tron, further enhances scalability by electing a smaller number of block producers or delegates to validate transactions.

2. Energy Consumption

Challenge: Consensus algorithms like Proof of Work (PoW), used by Bitcoin and Ethereum, are criticized for their massive energy consumption. PoW requires miners to perform complex calculations (hashing) to add a block to the blockchain, resulting in high electricity costs and environmental concerns.

Solution: Proof of Stake (PoS): PoS reduces energy consumption by replacing computational work with a system where validators are selected based on the number of coins they stake. This eliminates the need for energy-intensive mining and reduces the overall carbon footprint.

3. Security Concerns (51% Attack)

Challenge: A 51% attack occurs when a malicious actor or group of actors control more than 50% of the network's computing power (in PoW) or stake (in PoS). This allows them to:

    - Reverse transactions (double-spend).
    - Prevent new transactions from being confirmed.
    - Compromise the integrity of the blockchain.

Solution: Proof of Work:

    - Increasing Hash Rate: The security of PoW is increased as more computational power is added to the network. As the network grows, the difficulty of attacking it increases.
    - Merged Mining: Using multiple chains in parallel (merged mining) increases security, as it requires attackers to control a higher portion of computing power across multiple chains.

- Proof of Stake (PoS):
    - Slashing: In PoS, malicious behavior (such as attempting to manipulate the blockchain) can lead to the "slashing" of the validator's staked funds, incentivizing honest behavior and protecting against 51% attacks.
    - Security Mechanisms like Finality: Some PoS blockchains like Ethereum 2.0 and Cardano use finality protocols (e.g., HotStuff or Ouroboros) to ensure that blocks, once confirmed, cannot be reverted or reorganized.
- Proof of Authority (PoA):
    - In PoA, validators are known and trusted entities. The risk of a 51% attack is minimal because the system relies on a small set of trusted authorities.

4. Decentralization vs. Centralization

Challenge: Decentralization is one of the primary benefits of blockchain technology. However, in some consensus algorithms, like PoW, the concentration of mining power in the hands of a few large mining pools can lead to centralization. This undermines the blockchain's resistance to censorship and tampering.

Solution: Proof of Stake (PoS):

  - PoS aims to mitigate centralization by allowing anyone with a stake in the network to participate in the consensus process. However, it still faces the risk that wealthy participants could dominate, leading to oligopolistic behavior.
  - Mechanisms like delegated staking and increased validator requirements (i.e., requiring more diverse validators) can help reduce centralization.

- Delegated Proof of Stake (DPoS):
  - DPoS reduces centralization by selecting delegates or validators through community voting. However, if voting power is not distributed evenly, it can lead to centralization.
  - Solutions to this issue include improving voter participation and decentralizing the election of delegates.
- Hybrid Consensus Models:
  - Hybrid models, such as Proof of Authority (PoA) and Proof of Stake (PoS), allow the best of both worlds by introducing well-defined roles for validators while still maintaining decentralization.

Que2. Explain Byzantine models of fault tolerance

Ans Byzantine Fault Tolerance (BFT) in blockchain refers to the ability of a blockchain network to function properly, reach consensus, and remain secure, even when some of its nodes (participants) behave arbitrarily or maliciously. BFT is essential in decentralized systems like blockchain because it ensures that the network can still operate correctly, even if a fraction of the participants is faulty, compromised, or acting maliciously.

BFT Important in Blockchain

1. Decentralization: Blockchains rely on a distributed network of nodes where no single party controls the system. In such decentralized systems, some nodes may behave maliciously or fail due to software bugs or attacks. BFT ensures that the network can still reach consensus, even in the presence of such Byzantine nodes.
2. Security:BFT ensures that the blockchain remains secure by preventing fraudulent actions like double-spending or unauthorized block creation. A blockchain network that is Byzantine fault-tolerant can resist attacks, even when a subset of its nodes is compromised.
3. Trustless Environment: Blockchain is designed to allow trustless interactions between parties. By ensuring BFT, a blockchain can continue to operate securely and effectively, even without trusted central authorities, as long as most of the participants act honestly.
4. Resilience: BFT enables blockchains to maintain functionality even in adversarial conditions. If some nodes in the network are faulty or malicious, as long as a majority of the nodes are honest, the network will reach an agreement on the state of the blockchain.

Byzantine Fault Tolerance: The Byzantine Generals Problem

The term Byzantine Fault Tolerance originates from the Byzantine Generals Problem, a theoretical problem in distributed computing. The problem illustrates how difficult it is for a group of distributed nodes (generals) to reach consensus when some of the nodes may be malicious or faulty.

In the problem, multiple Byzantine generals are coordinating an attack, but some of them may be traitors who are sending misleading information to disrupt the plan. The challenge is for the loyal generals to agree on a common course of action (whether to attack or retreat) despite the actions of the traitors.

In a blockchain context, the "generals" are the nodes, and the traitors are the malicious nodes trying to undermine the network's consensus. Byzantine Fault Tolerance ensures that even if some nodes fail or act maliciously, the honest majority of nodes can still reach a valid consensus on the state of the blockchain.

Popular BFT Consensus Algorithms in Blockchain

There are several Byzantine Fault Tolerant (BFT) consensus algorithms designed for blockchain networks, each with its own approach to handling Byzantine faults. Below are some of the most well-known ones:

1. Practical Byzantine Fault Tolerance (PBFT)

PBFT is one of the most well-known and widely implemented BFT algorithms. It was originally designed for asynchronous distributed systems and later adapted for blockchain networks.

Working:

  - o PBFT divides the consensus process into three main phases: Pre-prepare, prepare, and commit.
  - o A leader (primary) node proposes a new block, and all other nodes (replicas) communicate to ensure that they all agree on the block.
  - o Each node validates the proposed block and sends messages (prepare and commit) to other nodes. Once a sufficient number of nodes confirm the block, it is added to the blockchain.

- Fault Tolerance: PBFT can tolerate up to (n-1)/3 Byzantine nodes, where n is the total number of nodes in the system.

  Advantages:

  - o Fast finality: Once a block is committed, it cannot be reverted.
  - o Highly secure: Resistant to Byzantine faults, including malicious attacks and network failures.

  Disadvantages:

  - o Scalability: The communication overhead in PBFT is high. As the number of nodes increases, the number of messages grows quadratically, making it less suitable for large-scale blockchains.
  - o Complexity: The implementation of PBFT requires a lot of coordination and can be complex to maintain.

2. Delegated Byzantine Fault Tolerance (dBFT)

dBFT is a variation of PBFT that is primarily used in the NEO blockchain and other systems. In dBFT, delegates (validators) are elected to propose and validate blocks instead of having all nodes participate in the consensus process.

Working:

  - o Validators are chosen based on their reputation or other criteria. These validators propose and vote on new blocks.
  - o The system reaches consensus when a sufficient number of validators agree on the validity of a block (usually 66% of the validators).

- Fault Tolerance: Like PBFT, dBFT can tolerate up to (n-1)/3 Byzantine faults.

  Advantages:

- Scalable: dBFT reduces the number of nodes that need to participate in the consensus process, making it more scalable than PBFT.
- Low latency: Block finality is achieved quickly, and transactions are confirmed faster than with many other consensus algorithms.

Disadvantages:

- Centralization: Since only a few validators participate in the consensus, there is a risk of centralization. A small group of validators could control the network.

Que3. list out different protocol of blockchain

Ans A blockchain protocol defines the set of rules and standards that govern how a blockchain network operates. It includes the mechanisms for consensus, transaction validation, block formation, and data propagation across the network. Blockchain protocols are integral to the functioning of a blockchain, as they ensure that the network is secure, decentralized, and efficient. The protocol also determines how nodes in the network communicate, validate transactions, and maintain the shared ledger.

Here is an overview of the key blockchain protocols, categorized by their functions:

1. Consensus Protocols: Consensus protocols are critical for achieving agreement among decentralized nodes on the validity of transactions and the current state of the blockchain ledger. They ensure that all participants (nodes) in the network reach consensus on the same version of the truth, despite being distributed and potentially untrustworthy.

Popular Consensus Protocols

Proof of Work (PoW):: PoW is the most well-known consensus mechanism used by Bitcoin and other blockchains. It requires participants (miners) to solve complex cryptographic puzzles to add a new block to the blockchain. The first miner to solve the puzzle gets the right to add the block and is rewarded with cryptocurrency.

Proof of Stake (PoS):: In PoS, validators are chosen to create a new block based on the number of coins they hold and are willing to "stake" as collateral. Validators are selected randomly, but those with more staked tokens have a higher chance of being selected.

Delegated Proof of Stake (DPoS): DPoS is a variation of PoS where stakeholders vote for a small number of delegates (also called block producers) to validate transactions and create new blocks on their behalf.

Practical Byzantine Fault Tolerance (PBFT):: PBFT is a consensus algorithm designed to tolerate faulty or malicious nodes by requiring nodes to agree on the validity of a transaction through multiple rounds of voting. It is highly efficient in environments with a small to moderate number of nodes.

Proof of Authority (PoA): In PoA, a set of trusted validators (authorities) are pre-approved to validate transactions and create new blocks. PoA is often used in private or consortium blockchains where a higher degree of trust among participants is assumed.

2. Transaction Protocols

Transaction protocols define the rules for how transactions are formed, validated, and added to the blockchain. These protocols ensure the integrity, authenticity, and security of transactions.

Common Transaction Protocols

Bitcoin Protocol: Bitcoin's transaction protocol defines how a user creates, signs, and broadcasts a transaction. It uses the UTXO (Unspent Transaction Output) model, where each transaction consumes unspent outputs from previous transactions to create new ones.

Ethereum Protocol: Ethereum uses the account-based model, where each address has a balance of tokens, and transactions modify those balances. Ethereum's transaction protocol also supports the execution of smart contracts.

ERC-20 and ERC-721 Protocols: These protocols define the standards for creating fungible (ERC-20) and non-fungible tokens (ERC-721) on the Ethereum blockchain. The ERC standards ensure interoperability and compatibility across different Ethereum-based projects and wallets.

3. Smart Contract Protocols

Smart contracts are self-executing contracts where the terms are written directly into the code. These protocols define how smart contracts are deployed, executed, and interacted with on the blockchain.

Key Smart Contract Protocols

Ethereum Smart Contract Protocol: Ethereum introduced the concept of smart contracts through its Ethereum Virtual Machine (EVM). The EVM allows developers to write decentralized applications (dApps) using smart contracts, which are executed when certain conditions are met.

Hyperledger Fabric Smart Contract Protocol (Chaincode):: Hyperledger Fabric uses Chaincode, which is essentially the smart contract or business logic that executes on the network. Chaincode is written in programming languages such as Go or JavaScript.

EOSIO Smart Contract Protocol: EOSIO allows developers to write smart contracts in C++ and deploy them on the EOS blockchain. EOSIO supports a fast transaction throughput and a governance mechanism via its DPoS consensus.

4. Interoperability Protocols

Interoperability protocols are designed to enable different blockchain networks to communicate and share data with each other, creating an interconnected ecosystem of blockchains.

Popular Interoperability Protocols

Polkadot Protocol: Polkadot provides a framework for creating interoperable blockchains. It connects various blockchains, called parachains, to a central relay chain, allowing them to share information and assets.

Cosmos Protocol: Cosmos provides a set of protocols (the IBC or Inter-Blockchain Communication protocol) that enables interoperability between independent blockchains. It allows secure data transfer and asset exchange between different blockchain ecosystems.

Chainlink Protocol: Chainlink is a decentralized oracle network that enables smart contracts to securely interact with external data sources, APIs, and traditional payment systems, extending the functionality of blockchains.

5. Layer 2 Protocols

Layer 2 protocols are designed to improve the scalability and efficiency of blockchain networks by processing transactions off-chain while ensuring the security and decentralization of the underlying blockchain.

Popular Layer 2 Protocols

Lightning Network (Bitcoin): The Lightning Network is a Layer 2 protocol built on top of Bitcoin to enable faster and cheaper off-chain transactions. It allows participants to create payment channels that can be settled on-chain at a later time.

Plasma (Ethereum): Plasma is a framework for building scalable applications on Ethereum by creating child chains that can handle most transactions off the main Ethereum chain. These child chains periodically commit their states to the Ethereum mainnet for security.

6. Privacy Protocols: Privacy protocols ensure that sensitive data remains confidential while still enabling verification of transactions. These protocols enable the blockchain to provide privacy and confidentiality while maintaining its decentralized nature.

Unit: 3

Q.1. What is cryptocurrency? Give an overview.

Ans. Cryptocurrency is a digital payment system that does not rely on banks to verify transactions. Cryptocurrency payments exist purely as digital entries to an online database. When cryptocurrency funds are transferred, the transactions are recorded in a public ledger. In cryptocurrency, "coins" (which are publicly agreed-on records of ownership) are generated or produced by "miners". These miners are people who run programs on ASIC (Application Specific Integrated Circuit) devices made specifically to solve proof-of-work puzzles. The work behind mining coins gives them value, while the scarcity of coins and demand for them causes their value to fluctuate. Cryptocurrencies can be used for buying goods just like fiat currency. Cryptocurrencies use encryption to verify and protect transactions.

Cryptocurrency does not exist in physical form and is not typically issued by any central authority. They use decentralized control in contrast to central bank digital currency.

Q.2. Explain some best-known cryptocurrencies.

Ans. Some best-known cryptocurrencies are as follows -

(i) **Bitcoin** - Bitcoin is the most widely accepted cryptocurrency. Founded in 2009 by Satoshi Nakamoto, it is still the most commonly traded. It is a decentralized digital currency that can be transferred on a peer-to-peer bitcoin network.

(ii) **Ether** - Ether is the native cryptocurrency of the Ethereum blockchain network. Each Ethereum account has an ETH balance and may send ETH to any other accounts. The smallest subunit of Ether is known as Wei.

(iii) **Litecoin** - Litecoin is a peer-to-peer cryptocurrency and in technical terms, Litecoin is nearly identical to Bitcoin. It uses a script in its proof-of-work algorithm. It is an adaptation of Bitcoin that is intended to make payment easier.

(iv) **Stablecoins** - These are the class of cryptocurrencies whose values are designed to stay stable relative to real-world assets like the U.S. Dollar.

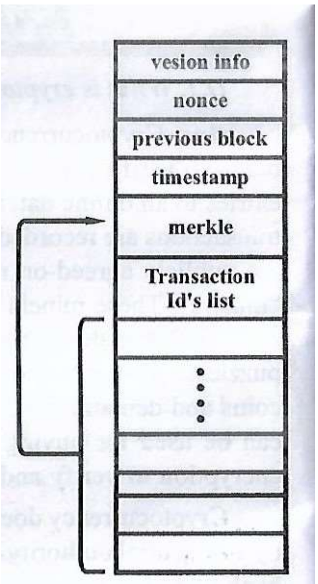
(v) Solana - Solana is a competitor of Ethereum whose main emphasis is on speed and cost-effectiveness.

Q.3. Explain traditional currencies vs. cryptocurrencies.

Ans. The difference between the working of a cryptocurrency and fiat currency likes the U.S. Dollar while purchasing goods.

There are two things that make cryptocurrencies work and fiat currency work differently Transaction and the consensus protocol. A block in a blockchain has the following structure.

As we can see, a block contains multiple transactions at a time in the transaction's id list.



(i) **Transactions** - The transactions performed in the crypto world are very different than those that of which arc performed in the real world. Example - Alice wants to buy a Bicycle. Real-world - In the real-world Alice can pay in any available currency. The seller will return the

change if any to Alice. Crypto World - Suppose the bicycle costs 0.6 BTC and Alice has 0.7 BTC in the Bitcoin wallet. Alice has to consider the whole amount i.e. 0.7 BTC.

(a) Transaction 1 - Transfer only 0.6 BTC from Bitcoin wallet to the seller's wallet. Now, Alice has already exhausted 0.6 out of 0.7 BTC. The remaining 0.1 BTC has to be transferred back to Alice's wallet. There is no change in BTC being offered by the seller to Alice.

(b) Transaction 2 - Alice offers 0.1 BTC back to herself. So 0.1 BTC is an unspent transaction amount in Alice's wallet.

(ii) **Consensus Protocol** - Consensus decision-making is a group decision-making process in which group members develop and agree to support a decision in the best interest of the whole. Basically, it states that the longest valid chain in the blockchain network should exist on every node in the network.

Q.4. How does cryptocurrency work?

Ans. Cryptocurrencies are not regulated or controlled by any central authority hence cryptocurrency works outside the banking system using different types of coins.

(i) **Mining** - Cryptocurrencies are generated through a process called mining. In this process, the miners are required to solve a mathematical puzzle over a specially equipped computer system to be rewarded with Bitcoins in exchange.

(ii) **Buying, Selling and Storing** - Users can buy cryptocurrencies from central exchanges, brokers or individual currency owners and sell crypto to them. Cryptocurrencies can be stored in wallets.

(iii) **Investing** - (cryptocurrencies can be transferred from one digital wallet to another. Cryptocurrencies can be used for the following purposes like buying goods and services, trade-in them, exchange them for cash.

Q.5. How to buy cryptocurrency?

Ans. There are three steps involved in buying a cryptocurrency -

(I) **Choosing a Platform** - There are two platforms available to choose from -

(a) Traditional Brokers - There are online brokers who offer to buy and sell cryptocurrencies along with stock, bonds, etc. but they offer lower trading costs and fewer crypto features.

(b) Cryptocurrency Exchanges - Different types of crypto- currency exchanges are available to choose from with different crypto- currencies, wallet storage etc.

(ii) **Funding Your Account** - After choosing the platform, the next step is to fund the account. Most crypto exchanges allow users to purchase cryptocurrencies using fiat currency like U.S. Dollar, or the Euro or using credit and debit cards, but this varies from platform to platform. An important factor to consider here is the fees that include the potential deposit and withdrawal transaction fees plus the trading fees.

(iii) **Placing an Order** - The order can be placed via exchanges or broker's web or mobile platform.

(a) Select the Buy option.

(b) Choose the order type.

(c) Enter the number of cryptocurrencies.

(d) Confirm the order.

A similar process needs to be followed for selling cryptocurrencies.

Q.6. How to store cryptocurrencies?

Ans. Once the cryptocurrency is purchased, it needs to be stored safely to protect it from hackers. The usual place to store cryptocurrency is crypto wallets which can be physical devices or online software. Not all exchanges or brokers provide crypto wnllct services The cryptocurrencies can be stored in these four places -

(i) **Custodial Wallet** - In this approach, a third party such as a crypto exchange stores the cryptocurrency either through cold storage or hot storage, or a combination of the two. This is the simplest and most convenient method for the users as it requires less work on the user's part.

(ii) **Cold Wallet** - These are also known as Hardware wallets. It is an offline wallet in which hardware connects to the computer and stores the cryptocurrency. The device connects "to the internet at the time of sending and receiving cryptocurrency but other than that the cryptos are safely stored offline.

(iii) **Hot Wallet** - These are the applications that store cryptocurrencies online. These are available as desktop or mobile apps.

(iv) **Paper Wallet** - This is also known as a physical wallet. It is a printout of the public and private keys available as a string of characters or scannable QR codes. To send crypto scan the public and private keys and crypto will be received using the public keys.

Q. 7. Write the advantages of cryptocurrency.

Ans. Some of the advantages of cryptocurrencies are as follows -

(i) **Private and Secure** - Blockchain technology ensures user anonymity and at the same time the use of cryptography in blockchain makes the network secure for working with cryptocurrencies.

(ii) **Decentralized, Immutable, and Transparent** - The entire blockchain network works on the principle of shared ownership where there is no single regulating authority and the data is available to all the permissioned members on the network and is tamper-proof.

(iii) **Inflation Hedge** - Cryptocurrencies are a good means of in- vesting in times of inflation as they are limited in supply and there is a cap on mining any type of cryptocurrency.

(iv) **Faster Settlement** - Payments for most cryptocurrencies settle in seconds or minutes. Wire transfers at banks can cost more and often take three to five business days to settle.

(v) **Easy Transactions** - Crypto transactions can be done more easily, in a private manner in comparison to bank transactions. Using a simple smartphone and a cryptocurrency wallet, anyone can send or receive a variety of cryptocurrencies.

Q.8. What are the disadvantages of cryptocurrencies?

Ans. Some of the disadvantages of cryptocurrencies are as follows -

(i) **Cybersecurity Issues** - Cryptocurrencies will be subject to cybersecurity breaches and may fall into the hands of hackers. Mitigating this will require continuous maintenance of security infrastructure.

(ii) **Price Volatility** - Cryptocurrencies are highly volatile in terms of price as they have no underlying value and there is a supply-demand-like equation that is used to determine the price of cryptocurrencies.

(iii) **Scalability** - Scalability is one of the major concerns with cryptocurrencies. Digital coins and tokens adoption is increasing rapidly but owing to the sluggish nature of the blockchain makes cryptocurrencies prone to transaction delays. Cryptocurrencies cannot compete with the number of transactions that payment giants like VISA, and Mastercard process in a day.

(iv) **Less Awareness** - Cryptocurrency is still a new concept for the people and the long-term sustainability of cryptocurrencies remains to be seen.

Q.9. Write short note on the future of cryptocurrency.

Ans. The future of most cryptocurrencies is uncertain, as it is still controversial and not authorized by many Governments, institutions, etc. However, in the near future, it may be used on a large scale and accepted more. Because every development of new technologies includes the financial market to ease the user to the bottom level. The ICO (Initial Offers of Cryptocurrency) is the fundamental part of an independent project that is still in the development phase. In this process, shares are not sold; the organization offers tokens, also known as cryptocurrency. Therefore, with time and the development of these projects, cryptocurrency can offer multiple benefits for these projects, and also for investors too. Cryptocurrency is the most independent currency in the financial world. Therefore, the fact of prohibiting its dissemination and/or use could cause a partial delay with respect to economic trends. Only the future can show us how crypto influences our lifestyle.

Que10. Write short note on verifiable random function

Ans. A Verifiable Random Function (VRF) is a cryptographic primitive that provides a verifiable source of randomness in a manner that is both deterministic and provably unpredictable to external observers, while allowing anyone to verify the correctness of the random output. In simpler terms, a VRF generates random numbers or outputs, but the key feature is that anyone can verify that the output was correctly generated without needing to know the secret information that generated it.

VRFs are especially useful in blockchain and cryptocurrency systems, where randomness is often needed for activities like selecting validators, generating keys, or determining the order of transactions. VRFs can ensure that this randomness is fair and provably unbiased, even in a decentralized context where trust in a single party is not possible.

Properties of a VRF

1. Deterministic Output: The output of the VRF is deterministic, meaning that for the same input and secret key, the output will always be the same. This ensures that the system is predictable and reproducible, which is important for blockchain protocols.
2. Unpredictability (without the secret key): Although the output is deterministic, the result is unpredictable to anyone who does not know the secret key. This makes the function cryptographically secure.
3. Verifiability: Anyone can verify that the output is correct and was generated from a given input and secret key. This verification process does not require the verifier to know the secret key, making the function transparent and trustless.
4. Unforgeability: It is computationally infeasible for anyone to forge the output of the VRF or generate a valid proof without knowing the secret key.

VRFs Working

A VRF typically involves two components:

- Private Key: This is the secret key that is used to generate the random output.
- Public Key: This is the corresponding public key, which is used to verify the output generated by the private key.

The process works as follows:

1. Input: A given input, such as a message or data, is provided to the VRF.
2. Random Output Generation: The VRF uses the private key and the input to generate a random output and a proof. The output is a random value that is cryptographically related to the input and the private key.
3. Verification: Anyone can use the public key and the proof to verify that the random output was indeed generated by the owner of the secret private key. The proof guarantees that the output was not tampered with, ensuring its correctness.

Applications of VRF in Blockchain

In blockchain and distributed ledger technologies, VRFs are useful in several contexts:

1. Validator Selection:
   - In Proof of Stake (PoS) and delegated Proof of Stake (DPoS) consensus mechanisms, VRFs can be used to select validators or block proposers in a randomized and fair manner. The randomness provided by VRFs ensures that the selection process is unpredictable and resistant to manipulation.
   - For example, in the Algorand blockchain, VRFs are used to select leaders who propose new blocks in a way that is both random and verifiable.
2. Leader Election in Consensus Protocols:
   - VRFs are commonly used in leader election schemes for distributed systems. By utilizing a VRF, the leader selection process can be transparent and secure, where the output is unpredictable but verifiable by all participants, ensuring fairness in the network.
   - In Algorand, a VRF is used to generate random values that help in the election of the next block proposer.
3. Commitment to a Random Value:
   - A VRF can be used to commit to a random value, such as when generating random numbers for cryptographic lotteries or smart contracts. The output of the VRF can be used in games of chance or any scenario where fair randomness is important.

Advantages of VRFs in Blockchain

1. Fairness and Transparency:
   - VRFs can provide a fair and verifiable mechanism for randomness, reducing the possibility of manipulation or centralization in decentralized systems. The process can be publicly verified, ensuring that no one can control the randomness or tamper with the process.
2. Security:
   - Since the random values generated by the VRF are tied to a private key and can be verified with the public key, this offers a secure method for ensuring the integrity of the random number generation. The verifiability ensures that the process is trustless and resistant to fraud.
3. Deterministic but Unpredictable:
   - VRFs produce deterministic outputs based on an input, ensuring consistency. However, they are unpredictable without knowledge of the secret key, making them suitable for applications that require a high level of randomness.
4. Efficiency:
   - VRFs allow for efficient computation of random values and proofs, which is important in blockchain systems that need to process large numbers of transactions and consensus decisions in a short amount of time.

Que11. Write short description on hashing in blockchain

Ans Hashing is a crucial cryptographic technique used in blockchain to ensure the integrity, security, and immutability of data. It involves converting input data (such as a block of transactions) into a fixed-length string of characters, typically represented in hexadecimal. This string, called a hash, is generated using a hash function like SHA-256 in Bitcoin.

- Immutability: Each block contains a hash of the previous block, linking them together in a chain. If any data in a block is altered, its hash changes, breaking the chain and making tampering easily detectable.

- Security: Hashing ensures that the data cannot be reverse-engineered or tampered with, as even a small change in the input data results in a completely different hash.
- Proof of Work (PoW): In PoW-based blockchains like Bitcoin, miners must find a valid hash that meets specific criteria (e.g., leading zeros) to add a new block to the blockchain.

Example:

If the input is the string "Hello World", the SHA-256 hash might look like this: a591a6d40bf420404a011733cfb7b190d62c65bf0bcda0b4e3c94411b0c1e7db

This fixed-length hash uniquely represents the original data and is used for verification, data integrity, and security in blockchain networks.

Que12. How is digital signature scheme works in blockchain

Ans A digital signature scheme in blockchain is a cryptographic method used to authenticate and validate the identity of users or entities, ensuring that transactions are legitimate and have not been tampered with. Digital signatures provide non-repudiation (the ability to prove that a transaction was sent by a specific user) and data integrity (ensuring that the content of the transaction hasn't been altered).

Components of a Digital Signature Scheme:

1. Private Key: The private key is a secret key used by the sender to generate the signature. It is kept private and secure by the user. Only the holder of the private key can create a valid signature.
2. Public Key: The public key is shared with others and is used by anyone to verify the authenticity of a digital signature. It is mathematically related to the private key but cannot be used to reverse-engineer the private key.
3. Hashing Function: Before signing a transaction, its contents (e.g., transaction data) are usually passed through a hash function, which produces a fixed-length hash (a digital fingerprint) of the data. This ensures that the signature is tied to the exact content of the transaction, and any alteration of the transaction would result in a different hash.

Digital Signatures Working in Blockchain:

1. Signing: A user signs a transaction with their private key. The transaction data is hashed, and the private key is used to sign the hash. The result is a digital signature.
2. Verification: The recipient (or any node in the blockchain) can verify the transaction by using the sender’s public key. The public key verifies that the signature corresponds to the hash of the transaction and that it was indeed signed by the holder of the private key.
3. Transaction Integrity: Once the signature is verified, the recipient can be confident that the transaction hasn’t been altered, and the sender is who they claim to be.

Que13. Explain Encryption schemes in blockchain.

Ans. Encryption schemes in blockchain are cryptographic protocols used to protect sensitive data and ensure privacy, integrity, and security of information stored and transmitted on the blockchain. Encryption ensures that data remains confidential and that unauthorized parties cannot access, read, or tamper with the data.

There are two main types of encryption schemes used in blockchain: symmetric encryption and asymmetric encryption. Blockchain primarily relies on asymmetric encryption (public-key cryptography) for securing transactions and validating identities, but other encryption schemes can also be used for specific purposes, such as data privacy and confidentiality.

1. Asymmetric Encryption (Public-Key Cryptography)

Asymmetric encryption, also known as public-key cryptography, is the cornerstone of blockchain security. It uses a pair of keys: a private key and a public key. These keys are mathematically related but cannot be derived from each other.

- Private Key: A secret key known only to the owner. It is used to sign transactions and prove ownership.
- Public Key: A public key associated with the private key, used by others to verify the authenticity of the digital signature.

Example: Bitcoin and Ethereum both use ECDSA (Elliptic Curve Digital Signature Algorithm), a form of asymmetric encryption, to secure transactions.

2. Symmetric Encryption

Symmetric encryption uses a single shared key for both encryption and decryption. Both parties who need to communicate securely must have access to the same secret key.

- Encryption: Data is encrypted using a symmetric key.
- Decryption: The same key is used to decrypt the data.

3. Hashing

Although not strictly an encryption scheme, hashing is a fundamental cryptographic technique used in blockchain. Hashing is used to convert input data into a fixed-length string of characters, which is computationally difficult to reverse.

4. Homomorphic Encryption

Homomorphic encryption is a type of encryption that allows computation to be performed on encrypted data without decrypting it first. This encryption scheme is useful in scenarios where you want to perform operations on sensitive data while maintaining privacy.

5. Zero-Knowledge Proofs (ZKPs)

Zero-Knowledge Proofs (ZKPs) are cryptographic protocols that enable one party to prove to another party that they know a secret (e.g., the solution to a cryptographic problem) without revealing the secret itself.

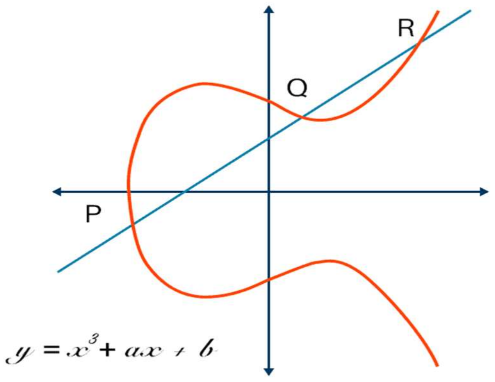
6. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a form of asymmetric encryption that uses the mathematics of elliptic curves to provide the same level of security as other cryptographic algorithms (like RSA) but with smaller key sizes. This makes ECC more efficient and suitable for blockchain use, where computational efficiency and low bandwidth are important.

Que14. Explain elliptic curve cryptography

Ans. Elliptic Curve Cryptography (ECC) is a form of public-key cryptography based on the mathematical properties of elliptic curves over finite fields. ECC is used to create cryptographic systems that are efficient, secure, and provide a higher level of security with smaller key sizes compared to other algorithms like RSA.

1. Elliptic Curves:



   - An elliptic curve is a set of points defined by an equation of the form:

$$y^2 = x^3 + ax + b$$

     where a and b are constants that define the shape of the curve. This equation is defined over a finite field, typically a large prime field.

   - The key property of elliptic curves that makes them useful in cryptography is that the points on the curve form an additive group, meaning that you can "add" two points on the curve to get another point on the curve.

2. Public-Key Cryptography:
    - Like other public-key cryptographic systems (e.g., RSA), ECC uses a pair of keys: a private key (kept secret) and a public key (shared openly).
    - Private key: A randomly chosen integer.
    - Public key: A point on the elliptic curve obtained by multiplying the private key with a fixed point (called the generator point or base point) on the curve.
3. Elliptic Curve Discrete Logarithm Problem (ECDLP):
    - The security of ECC relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is considered computationally infeasible to solve efficiently for large key sizes.
    - The ECDLP is the problem of finding the private key (which is the scalar) given a public key (which is the result of multiplying the generator point by the private key).
    - The difficulty of solving this problem is what makes ECC secure and resistant to attacks.

Working

1. Key Generation:

    Private Key: A random number selected from a predefined range.

    Public Key: A point on the elliptic curve, calculated by multiplying the private key with the generator point P (often denoted as Q=kP where k is the private key).

2. Encryption (in ECC-based systems):

    ECC can be used for encryption, but it's more commonly used for key exchange and digital signatures (e.g., in protocols like ECDSA and ECDH).

    In an ECDH (Elliptic Curve Diffie-Hellman) key exchange, two parties generate their private keys, exchange their public keys, and then compute a shared secret by performing elliptic curve point multiplication.

3. Digital Signatures:

    ECDSA (Elliptic Curve Digital Signature Algorithm) is the most widely used algorithm for digital signatures in ECC-based systems.

    Signing: A user signs a message using their private key to create a signature.

    Verification: Anyone with the public key can verify the signature to ensure that the message was signed by the rightful owner of the private key and that the message has not been tampered with.

Applications of ECC in Blockchain

ECC is widely used in various blockchain protocols, such as Bitcoin, Ethereum, and Zcash, for securing transactions, creating digital signatures, and enabling secure key exchanges. Some common uses of ECC in blockchain are:

1. Digital Signatures: ECDSA (Elliptic Curve Digital Signature Algorithm) is used in Bitcoin and Ethereum to sign transactions. The private key is used to generate a signature for the transaction, while the public key is used by others to verify the signature.

2. Key Exchange (ECDH):Elliptic Curve Diffie-Hellman (ECDH) is used in some blockchain systems for secure key exchange, where two parties generate public/private key pairs, exchange public keys, and then compute a shared secret without transmitting the secret key itself.

   This can be used for secure communication between parties, ensuring that even if an attacker intercepts the public keys, they cannot derive the shared secret without solving the difficult ECDLP.

3. Cryptocurrency Wallets: In cryptocurrency wallets, ECC is used to generate the private/public key pair. The private key is used to sign transactions, while the public key or its hash (address) is used to receive funds.

4. Confidential Transactions: ECC can be used in privacy-focused blockchains (like Zcash) to implement zero-knowledge proofs (ZKPs), ensuring that transaction details (e.g., sender, receiver, amount) remain confidential while still proving the validity of the transaction.

UNIT: 4

Q.l What is Ethereum network ?

Ans. Ethereum is a decentralized platform that supports smart contracts, programs that execute exactly as intended with no chance of fraud or outside influence. This blockchain may be customized. It enables users to start ICOs and develop decentralized applications (DApps). These applications are powered by a specially developed blockchain, a potent worldwide shared infrastructure that can transfer value and reflect property ownership.

This makes it possible for developers to build markets, keep records of obligations or promises, transfer money following directives left behind in the past [like a will or a futures contract) and do a lot of other things that are still in the future without the need for a middleman or counterparty risk. Ethereum protocol is powered by ETH, the native cryptocurrency of the Ethereum blockchain and it is an essential part of the wcb3 stack. The Ethereum protocol is Turing complete, meaning it can run any program.

Q.2 Write short note on Turing- complete vs Turing incomplete.

Ans. There are two types of blockchain Turing complete and Turing incomplete. A Turing complete blockchain can support all computations that can be done on a Turing machine. This means that a Turing complete blockchain can support all the same computations that a computer can perform. On the other hand, a Turing incomplete blockchain can only support a subset of computations that can be done on a Turing machine.

The main difference between these two types of blockchain is that a Turing complete blockchain can support all types of smart contracts, while a Turing incomplete blockchain can only support a limited number of smart contracts. This is because a Turing complete blockchain can support any computation, while a Turing incomplete blockchain can only support a limited number of computations. One example of a Turing complete blockchain is Ethereum. Ethereum can support all smart contracts because it is a Turing complete blockchain. One example of a Turing incomplete blockchain is Bitcoin. Bitcoin can only support a limited number of smart contracts.

Q.3 What are decentralized applications?

Ans. Decentralized applications run on a decentralized network instead of a single computer. These programs are often referred to as DApps. A DApp can be anything from a decentralized exchange to a social media platform. The one common thread between all DApps is that they are powered by a decentralized network, usually a blockchain. Decentralized networks are more secure and resilient than traditional centralized networks because there is no single point of failure. If one node in the network goes down, the others can continue functioning. Decentralized applications are still in their early stages of development, but there are already a few well-known DApps, such as Ethereum, Augur and MaidSafe.

Q.4 What is Ethereum gas ?

Ans. Ethereum gas is a measurement unit used to determine how much computational efforts is required to execute a particular transaction or smart contract on the Ethereum blockchain. In other words, it is a way of measuring how much "work" is required to be done to complete a transaction. The more complex the transaction, the more gas it will require. For example, a simple transfer of ETH from one address to another requires less gas than a smart contract that involves data storage, calculations and other operations.

Gas is essential because it prevents the Ethereum network from overloading many transactions. 11 a transaction requires too much ii will be rejected by the network. Users are not charged for gas directly. Instead, they must pay a small amount of ETH for each transaction that they make. This ETH is then used to pay the miners who confirm the transactions on the blockchain.

Q.5 What are the types of users in the Ethereum network?

Ans. Three types of users in the Ethereum network are as follows –

(i) **Full Node** - A full node is a computer that stores a copy of the entire Ethereum blockchain. full nodes help to keep the network secure by validating and propagating transactions and blocks. They also provide the necessary data for light clients to access the network.

(ii) **Light Client** -A light client is a computer that does not store a copy of the blockchain but instead relies on full nodes to provide data. Light clients can be used to send and receive transactions and to interact with smart contracts.

(iii) **Contract** - A contract is a program that runs on the Ethereum network and can store data and execute transactions. Contracts can be used to create decentralized applications or to interact with other contracts.

Q.6 Discuss in detail the components of Ethereum.

Ans. The components of Ethereum are as follows -

(i) **Smart Contracts** - Smart contracts are self-executing contracts that are written on a blockchain platform. A smart contract is like a traditional contract, but it is executed and enforced automatically by the network. This means there is no need for a third party to mediate or enforce the contract. Smart contracts have the potential to revolutionize the way we do business. They can automate many transactions, from financial to supply chain management. One of the most promising applications of smart contracts is in the area of financial services. Smart contracts can streamline the process of securities trading, making it more efficient and less vulnerable to fraud.

Another potential application of smart contracts is in the area of identity management. Smart contracts can create a decentralized identity management system that is more secure and efficient than the current centralized system. There arc many other potential applications of smart contracts. The possibilities are limited only by our imagination.

Working of Smart Contract - Smart contracts are executed by the Ethereum virtual machine (EVM), which runs on every node in the Ethereum network. The EVM has its own internal Turing-complete programming language, which allows it to execute any code. When a smart contract is deployed, its code is stored in the blockchain and cannot be changed. However, the contract can be called by other contracts or external accounts. When a contract is called, its code is executed by the EVM. The EVM has access to the contract's storage, a persistent key-value store. The EVM can also send messages to other contracts or external accounts.

(ii) **Ether** - Ether is the native cryptocurrency of the Ethereum network. It is used to pay transaction fees and computational services on the Ethereum network. Ether is a decentralized currency, like Bitcoin. However, unlike Bitcoin, Ether is not meant to be a global currency. Instead, it is intended to be used as fuel for the Ethereum network. The Ethereum network is a decentralized platform that runs smart contracts. These contracts are programs that run exactly as programmed without any possibility of fraud or third-party interference.

Ether is used to pay for the computational power needed to run these smart contracts. This is similar to how oil is used to power cars or coal is used to power trains. Ether is also used to pay transaction fees on the Ethereum network. Every time a user sends a transaction, they must pay a small fee to have their transaction processed by the network.

(iii) **Ethereum Clients** - To use the Ethereum network, you need to have an Ethereum client. An Ethereum client is software that allows you to interact with the Ethereum network. It is your gateway to the Ethereum network. There are different types of Ethereum clients. The most popular ones are Geth and Parity. Geth is the Go implementation of the Ethereum client. Parity is the Rust implementation of the Ethereum client. There are also other clients like Aleth and Trinity. Each clients has its advantages and disadvantages. Geth is the most popular client. It is easy to use, and it has a lot of features. Parity is more lightweight, and it is taster than Geth. Aleth is more focused on security. Trinity is still in development. You can choose any client you want. It would be best if you used a client, you are comfortable with. If you are still deciding which client to use, you can try out different ones and see which one you like the most.

(iv) **Ethereum Virtual Machine (EVM)** - The Ethereum Virtual Machine (EVM) is a Turing-complete virtual machine that runs on the Ethereum network. It is used to run smart contracts and decentralized applications (DApps). The EVM is sandboxed, meaning that the code running on the EVM has no access to the network or filesystem. This makes it a very secure environment lor running apps. The EVM is also Turing-complete, meaning it can run any code. This makes it very flexible and powerful. The EVM is executed on every node in the Ethereum network. This ensures that all DApps running on the network are secure and have no single point of failure. The EVM is a crucial part of Ethereum and makes it a powerful platform for running DApps.

(v) **Ether Scripter-** Ether scripter is a smart contract programming language that enables developers to create contracts and decentralized applications (DApps) on the Ethereum blockchain. It is a high-level language similar to JavaScript and is designed to be easy to learn and use. Ether scripter is also Turing-complete, meaning that it can be used to create programs that can solve any computational problem.

Q.7 Describe about the following Ethereum Virtual Machine (EVM) -

Ans: **Ethereum Virtual Machine (EVM)** - The Ethereum Virtual Machine (EVM) is a Turing-complete virtual machine that runs on the Ethereum network. It is used to run smart contracts and decentralized applications (DApps). The EVM is sandboxed, meaning that the code running on the EVM has no access to the network or filesystem. This makes it a very secure environment lor running apps. The EVM is also Turing-complete, meaning it can run any code. This makes it very flexible and powerful. The EVM is executed on every node in the Ethereum network. This ensures that all DApps running on the network are secure and have no single point of failure. The EVM is a crucial part of Ethereum and makes it a powerful platform for running DApps.

Ether Scripter- Ether scripter is a smart contract programming language that enables developers to create contracts and decentralized applications (DApps) on the Ethereum blockchain. It is a high-level language similar to JavaScript and is designed to be easy to learn and use. Ether scripter is also Turing-complete, meaning that it can be used to create programs that can solve any computational problem.

Q.8 Write the advantages of Ethereum,

Ans. The advantages of Ethereum are as follows -

(i) **Decentralization** - The decentralized design a Ethereum effectively distributes knowledge and trust among network members, removing the need for a central body to run the system and mediate transactions.

(ii) **Ether scripter**

(ii) **Rapid Deployment** - Instead of building a blockchain implementation from scratch, organizations can quickly create and administer private blockchain networks using an all-in-one SaaS platform like Hyperledger Besu.

(iii) **Permissioned Network** - There are many open-source protocol layers that allow enterprises to build on public or private Ethereum networks, guaranteeing that their solution meets all regulator)' and security standards.

(iv) **Network Size** - The Ethereum mainnet demonstrates that a network with hundreds of nodes and millions of users can function. Most business blockchain competitors run networks with less than ten nodes and have no precedent for a large and successful network. For corporate collaborations that arc bound to outgrow a few nodes, network scale is important.

(v) **Private Transactions** - In Ethereum, businesses may obtain privacy granularity by joining private partnerships with private transaction layers. Private information is encrypted and only shared with those who need to know.

Q.9 What are the disadvantages of Ethereum ?

Ans. Disadvantages of Ethereum are as follows -

(i) **Uses a Complicated Programming Language** - While Ethereum is Turing complete and uses a programming language similar to C++, Python, and Java, learning solidity, the native language of Ethereum, may be challenging. One of the most significant concerns is the scarcity of beginner-friendly classes.

(ii) **Issues with Scaling** - Unlike Bitcoin, which has a singular purpose, Ethereum has a ledger, a platform for smart contracts, and so on, all of which may lead to errors, malfunctions, and hacks.

(iii) **Ethereum Investing can be Risky** - Ethereum investing, like any other cryptocurrency, can be risky. Cryptocurrencies are very volatile, resulting in significant gains as well as significant losses. The price of Ether has changed significantly in the past, which might be a significant disadvantage for certain investors, particularly newbies. In addition, Ethereum's fees change, which is inconvenient.

Q10. Write about Mist browser.

Arts. The Mist browser was intended to be an integral part of the Ethereum network's DApps (decentralized applications) ecosystem. It was the first graphical user interface that enabled users to access the blockchain at a time when you could only access it via the command line. Its developers wanted to offer a onc-stop-shop for running and executing various Ethereum applications

and projects.

Unfortunately, the technical requirements of a fully decentralized DApp browser system were too far beyond what the technology allowed at the time. As a result, the Mist browser project was abandoned, and the software was taken out of circulation in March of 2019.

The Mist browser was an Ethereum interface intended to allow users to access the various DApps available on the Ethereum network. It was also known as the Ethereum DApp Browser. 1.Ethereum is a popular blockchain optimized for smart contracts and other decentralized applications.

As a DApp browser, Mist was a standalone application with a graphical user interface (GUI) that allowed users to sync to the blockchain. It also provided an easy way for users to create their own DApps and deploy tokens and other smart contracts in a non-technical way. The Mist Ethereum wallet itself would run on a user's computer, which meant it had to be downloaded, installed, and run locally. As a result, the Mist browser project was abandoned, and the software was taken out of circulation in March of 2019.

The Mist browser was an Ethereum interface intended to allow users to access the various DApps available on the Ethereum network. It was also known as the Ethereum DApp Browser. 1.Ethereum is a popular blockchain optimized for smart contracts and other decentralized applications. As a DApp browser, Mist was a standalone application with a graphical user interface (GUI) that allowed users to sync to the blockchain. It also provided an easy way for users to create their own DApps and deploy tokens and other smart contracts in a non-technical way. The Mist Ethereum wallet itself would run on a user's computer, which meant it had to be downloaded, installed, and run locally.

Q11. What is Ethereum Mist wallet ? Also write its features.

Ans. The Ethereum Mist wallet, the official Ethereum wallet, is a gateway to decentralized applications on the Ethereum blockchain. It allows you to hold and secure ether and other crypto-assets built on Ethereum, as well as write, deploy and use smart contracts.

Main features of the Ethereum Mist wallet are as follows -

(i) The most secure Ethereum wallet.

(ii) Can manage Ethers and tokens.

(iii) Built as part of the Ethereum platform.

(iv) Open-source and free.

Q.12. What is solidity ? Give its key features.

Ans. Solidity is a brand-new programming language created by Ethereum which is the second-largest market of cryptocurrency by capitalization, released in the year 2015 and led by Christian Reitwiessner.

Some key features of solidity are as follows -

(i) Solidity is a high-level programming language designed for implementing smart contracts.

(ii) It is a statistically typed object-oriented (contract-oriented) language.

(iii) Solidity is highly influenced by Python, C++ and JavaScript which run on the Ethereum Virtual Machine (EVM).

(iv) Solidity supports complex user-defined programming, libraries and inheritance.

(v) Solidity is the primary language for blockchains running platforms.

(vi) Solidity can be used to create contracts like voting, blind auctions,

crowdfunding, multi-signature wallets, etc.

Q.13. What is the solidity interface ?

Ans. A solidity contract interface is a list of function definitions without implementation. In other words, an interface is a description of all functions that an object must have for it to operate. The interface enforces a defined set of properties and functions on a contract.

Solidity allows you to interact with other contracts without having their code by using their interface.

For example, if you want to interact with another contract from your own contract, you provide your calls with an interface wrapper. By declaring an interface, you can interact with other contracts and call functions in another contract.

Interfaces are usually found at the top of a solidity contract, and they are identified using the "interface" keyword. Because interfaces reduce code duplication and overhead, they are most useful when decentralized applications require extensibility and want to avoid complexity.

Q.14. Write the characteristics of solidity interface.

Ans. Characteristics of solidity interface arc as follows

(i) The solidity interface can inherit from other interfaces.

(ii) Contracts can inherit interfaces as they would inherit other contracts.

(iii) You can override an interface function.

(iv) Data types defined inside interfaces can be accessed from other contracts.

All functions that inherit from the interface must set the override modifier on every function that overrides an interface function. Otherwise, the solidity compiler will throw an error.

Q.15. Explain abstract contracts vs interfaces.

Ans. Abstract contracts and interfaces are two ways web3 developers can build larger, more complex distributed applications because they allow for extensibility within solidity.

Abstract contracts possess at least one function that lacks implementation, and as a result, they cannot be compiled. However, abstract contracts can be used as base contracts from which other contracts can inherit. Interfaces are similar to abstract contracts, but they cannot have any functions implemented. Additionally, interfaces are limited to what the contract's Application Binary Interface (ABI) can represent. The conversion between the ABI and an interface is possible without any information loss.

Q16 List different types of attack on smart contract

Ans. A smart contract is a self-executing contract with the terms of the agreement directly written into code. These contracts run on blockchain platforms like Ethereum, and their execution is automatically enforced when predefined conditions are met. While smart contracts offer trustless, decentralized solutions and eliminate the need for intermediaries, they are not immune to security vulnerabilities and can be targeted by attackers.

Smart contract attacks occur when attackers exploit flaws in the code, logic, or the platform's behavior, causing unintended consequences. These vulnerabilities can lead to financial loss, data breaches, or disruption of decentralized applications (dApps).

Common Types of Smart Contract Attacks

1. Reentrancy Attack: A reentrancy attack occurs when a contract calls another contract, and the second contract calls back into the first contract before the initial execution is completed. This can allow the attacker to repeatedly withdraw funds or manipulate the contract state.

2. Integer Overflow and Underflow: In blockchain smart contracts, numeric values are represented by fixed-size variables. An integer overflow occurs when a number exceeds its maximum limit (e.g., uint256), while an underflow occurs when a number becomes smaller than its minimum value (e.g., subtracting 1 from 0).

3. Front-Running (Transaction Ordering Dependence): Front-running occurs when an attacker can observe pending transactions in a block and place their own transaction before the original one in the block. This is commonly seen in decentralized exchanges (DEXs) or auction-based platforms.

4. Time-Dependent Attack (Block Timestamp Manipulation): Some smart contracts rely on the block timestamp (the time the block is mined) to determine the execution conditions. An attacker may manipulate the time (within certain limits) to trigger or delay certain contract functions.

5. Gas Limit Attacks: Gas is a unit of computational work in Ethereum and other blockchain platforms. If a smart contract requires more gas than available in a block, the transaction will fail. Attackers can exploit contracts that have inefficient code or functions that require excessive gas.

6. Denial of Service (DoS) Attacks: In a DoS attack, the attacker aims to prevent legitimate users from interacting with the smart contract by flooding it with invalid or unnecessary transactions. This could lead to a contract becoming unusable, or excessive gas usage, causing the contract's functionality to degrade.

7. Access Control Vulnerabilities: Improper access control or missing checks for user permissions can allow unauthorized users to execute privileged functions, leading to malicious actions like transferring funds or modifying contract state.

8. Phishing Attacks: Although not strictly a vulnerability in the smart contract itself, phishing attacks target users interacting with smart contracts. Attackers may impersonate legitimate projects or contracts and trick users into sending funds or providing sensitive information.

9. Smart Contract Logic Flaws: Sometimes, the vulnerabilities lie not in the code itself but in the logic of the contract. A common example is a poorly designed contract that doesn't account for all possible edge cases, such as unexpected behaviors under certain conditions.

Q17. Give the introductory note on Hyperledger aka (Blockchain3.0).

Ans. Hyperledger is an open-source collaborative effort created to advance cross-industry blockchain technologies. It is not a specific blockchain or cryptocurrency, but rather a collection of blockchain frameworks, tools, and libraries that are designed to provide developers with a starting point for building robust, enterprise-grade blockchain solutions.

The project is managed by the Linux Foundation and is supported by a global community of developers and contributors who work together to improve the performance, scalability, and security of blockchain technology. Launched in 2015 by the Linux Foundation, Hyperledger was developed to create an environment in which disparate communities of software developers and companies meet and coordinate to build blockchain frameworks.

Hyperledger's mission is to promote the development of open-source blockchain technologies that are modular, flexible, and secure, and that can be customized to meet the needs of a wide range of industries, including finance healthcare, supply chain management, and more. As a consortium of Blockchain-based software companies, Hyperledger Blockchain today features more than 100 member companies including market giants such as Airbus, IBM, Fujitsu, SAP, Nokia, Intel, Samsung, American Express, J.P. Morgan, BNP Paribas, Wells Fargo, Blockstream, Netki, Factom, ConsenSys, etc.

Q18. Explain the history of hyperledger.

Ans. The Linux foundation announced the creation of the Hyperledger project in 2015, one year prior to its release. Brian Behlendorf was appointed at the position of executive director. Behlendorf stated that the Hyperledger project would never build its own cryptocurrency.

In 2016, the project also started to accept proposals for incubation of codebases and other core element technologies. Two of the initial blockchain framework codebases accepted were Hyperledger fabric and libconsesus. Later, Intel's distributed ledger, Sawtooth, was incubated.

In 2018, the production-ready Sawtooth 1.0 was added. In 2019, a long- term-support version of Hyperledger fabric was announced.

In October 2021, Behlendorf passed the executive director position to Daniela Barbosa. That same month, Hyperledger was rebranded to The Hyperledger foundation to draw a clearer line between Hyperledger as an organization and individual Hyperledger projects.

Q.19. Explain the components of hyperledger architecture.

Ans. All Hyperledger projects follow a methodology that includes an approach, interoperability, and highly secure solutions, and it helps in the development of easy-to-use application programming interfaces (APIs). The architecture of Hyperledger comprises the following business blockchain components -

(i) **Consensus Layer** - This layer is responsible for confirming the transactions of a block and generates an agreement on an order.

(ii) **Smart Contract Layer** - The smart contract layer processes transaction requests and determines whether the transactions are valid or not by executing the business logic.

(iii) **Communication Layer**-In a shared ledger, this communication layer transports associative messages between the nodes that participate.

(iv) **Datastore abstraction** - This layer permits diverse information stores to be utilized by different modules.

(v) **Crypto Abstraction** - It allows distinctive crypto calculations or modules to be traded out without influencing different modules.

(vi) **Identity Services** - This enables the foundation of a base of trust during the arrangement of a blockchain occurrence, the enlistment, and enrolment of personalities or framework substances during a network activity, and the administration of changes such as drops, adds, and denials. Likewise, it also gives validation and approval.

(vii) **Policy Services** - In the system, policy services are responsible for the management of various policies such as the endorsement policy, consensus policy, or group management policy. To enforce various policies, it interfaces and depends on other modules also.

(viii) **APIs** - APIs enable customers and applications to have an interface of blockchains

(ix) **Interoperation** - It is used to explore consensus. Generating an agreement on order and validating the correctness of the set of transactions in a block is the goal of consensus, and it also supports the interoperation between various blockchain instances.

Q20. Explain the roles of peers in hyperledger network.

Ans. In the hyperledger network, the peers are separated into three distinct roles at two-run times. This distinct feature in this network makes notable changes as it allows a high degree of personalization. The 3 peer roles are -

(i) Committer - Appends validated transactions to their specific ledger. They only add the transaction to the specific ledger once the transaction is returned by the consenter.

(ii) Endorser - Endorser nodes are responsible for simulating transactions specific to their network and preventing unreliable and non- deterministic transactions. All endorsers act as committers, on the other hand committers may or may not be endorsers depending on network restrictions.

(iii)Consenter - Their role is to validate the transaction by verifying the result produced by the affiliated peers who want to proceed with a transaction. Their role is very specific and runs on separate run times, unlike committers and endorsers who run on the same run time. Their role is to decide which ledger the transaction be committed to.

Q.21. What are the advantages and disadvantages of hyperledger ? Explain.

Ans. Advantages of Hyperledger - The advantages of hyperledger are

as follows -

(i) **Flexibility** - Hyperledger provides a high degree of flexibility and modularity, allowing developers to customize and configure the platform to meet their specific needs.

(ii) **Security** - Hyperledger has a strong focus on security, with features such as access control, identity management, and encryption. This makes it well-suited for enterprise applications that require a high level of security.

(iii) **Scalability** - Hyperledger is designed to handle large-scale enterprise applications, with the ability to support thousands of transactions per second.

(iv) **Privacy** - Hyperledger allows for the creation of private, permissioned blockchain networks, which means that only authorized participants have access to the data on the network.

(v) **Interoperability** - Hyperledger provides a common platform for building blockchain applications, which makes it easier to integrate with other systems and applications.

Disadvantages of Hyperledger - The Disadvantages of hyperledger are

as follows -

(i) **Complexity** - Hyperledger can be complex to set up and maintain, particularly for organizations that are new to blockchain technology. This can require significant technical expertise and resources.

(ii) **Limited Decentralization** - Hyperledger is a permissioned blockchain platform, which means that only authorized parties can participate in the network. While this can provide increased security and privacy, it also means that the network is less decentralized than public blockchain platforms.

(iii) **Limited Community** - While Hyperledger has a growing community of developers and contributors, it is still smaller than some other blockchain platforms. This could make it more difficult to find support and resources.

Q22. What is Hyperledger fabric ?

Ans. Hyperledger fabric is designed for use in enterprise-level applications, and it is characterized by its modular architecture, permissioned network, and smart contract functionality, known as "chaincode".

The platform provides a high degree of security, privacy and scalability and it supports the development of custom blockchain solutions for various use cases across industries such as finance, supply chain and healthcare.

Hyperledger fabric operates as a network of nodes, where each node performs a specific function, such as validating transactions, maintaining the ledger, and executing chaincode.

Transactions are validated and ordered by a consensus mechanism, which ensures the integrity and consistency of the ledger.

Q23. What are the differences between Ethereum and Hyperledger ? 1

Or

Write a short note on fabric v/s Ethereum.

Ans. The key differences between Ethereum and hyperledger fabric are

as follows -

(i) **Purpose** -

(a) Ethereum is the platform for creating B2C businesses and decentralized applications. It is created tor the purpose ot running smart contracts on the Ethereum Virtual Machine (EVM) and creating decentralized apps for mass consumption with the help of this.

(b) Hyperledger is designed to create B2B businesses and cross- industry applications. It helps businesses or industries to collaborate with the developers, who are working with distributed ledger technology (DLT). Customized blockchain apps with limited access can be created with this.

(ii) **Confidentiality** -

(a) Ethereum is a public network. All the transactions are entirely transparent and anyone with access to the internet can view these transactions.

(b) Hyperledger is a limited access blockchain network. This is highly secure and confidential. The organizations or individuals having the certificate of authorization can only view all the transactions on the network.

(iii) **Governance** -

(a) The Ethereum network is governed by the Ethereum developers only. Vitalik Buterin is the main developer and founder of Ethereum. This is mostly an example of in-house development rather than collaboration.

(b) Hyperledger fabric is governed by the Linux foundation. IBM is also one of the major contributors to this framework. It is a product of the massive collaboration of these two companies which turned out to be a huge success.

(iv) **Participation** -

(a) Ethereum is a permission-free and public network. Anyone with access to the internet can download the software and start mining Ethereum.

(b) Hyperledger maintains strict control over the participation in their network. Only authorized members and peers selected by authorized members can use the Hyperledger platform and its tools. This hides valuable and confidential information from external parties and prevents them to manipulate it.

(v) **Smart Contracts** -

(a) Ethereum came up with smart contracts first. A smart contract is a computer program or a condition written in code that gets automatically triggered when certain conditions are met. It controls the transfer of digital assets between the parties under the contract. It is immutable, once the condition is created it cannot be changed by any third party.

(b) Like the smart contracts, Hyperledger fabric also allows the member organizations to run some code on peers that create the transactions on a specific condition. These are known as chaincode.

(vi) **Programming Language** -

(a) For writing smart contracts, Ethereum uses solidity and for developing the application some high-level languages like JavaScript, Python, Golang can be used.

(b) In Hyperledger Go is widely used to write the chaincode, however along with that to some extent Java and JavaScript are also used.

(vii) Proof of Stake (POS) or Consensus Mechanism -

(a) Previously Ethereum was using proof of work (POW) based consensus mechanism. Currently, Ethereum is using proof of stake (POS) based consensus protocol. The consensus mechanism allows the participant nodes of the decentralized network to come to a consensus or agree on things like account balances and the order of transactions which prevents the users from making fake transactions and double-spending their coins.

(b) As Hyperledger is a private and permissioned network, it does not need any POW or consensus mechanism to validate a transaction. If two participating parties agree on a specific transaction then no third party can view or intervene in the specific transaction.

(viii) **Speed of Transactions** -

(a) As Ethereum is a public domain it has a POW mechanism, which reduces the transaction speed of Ethereum, which is something close to 20 transactions per second.

(b) For being a permissioned blockchain network, Hyperledger fabric does not need such a heavy POW mechanism like Ethereum. That increases the transaction speed, which is around 2000 transactions per second, far larger than Ethereum.

(ix) **Cryptocurrency** -

(a) Ethereum has its own native cryptocurrency called Ethereum (ETH). Any participating node can mine ETH by paying gas.

(b) Hyperledger does not have its native cryptocurrency and it does not involve in mining.

These features are tabulated below -

Que24. What is A plug-and-play platform for Ethereum.

Ans A plug-and-play platform for Ethereum typically refers to a solution or framework that simplifies the development and deployment of Ethereum-based decentralized applications (dApps) and smart contracts, allowing developers to easily integrate with the Ethereum blockchain without needing to deeply understand its complex underlying infrastructure. These platforms aim to reduce the barrier to entry for developers, enabling them to quickly deploy their applications and start interacting with the Ethereum network.

Several tools, libraries, and platforms offer plug-and-play solutions for Ethereum. Here are a few examples of these solutions and how they facilitate the development process:

1. Infura: Infura is a popular Ethereum infrastructure platform that provides a suite of APIs for developers to access Ethereum nodes without needing to run their own nodes. It offers plug-and-play APIs that allow developers to interact with Ethereum in a scalable, reliable way without worrying about maintaining blockchain nodes themselves.

2. Alchemy: Alchemy is another Ethereum development platform that provides an API suite similar to Infura but with more advanced features aimed at simplifying blockchain application development. It also provides infrastructure for interacting with Ethereum's mainnet, testnets, and Layer 2 solutions.

3. Truffle Suite: Truffle is one of the most popular Ethereum development frameworks. It is essentially a plug-and-play solution for building, testing, and deploying smart contracts. It provides an integrated development environment (IDE), asset pipeline, and framework for writing and managing smart contracts.

4. Hardhat: Hardhat is another Ethereum development environment that provides a suite of tools to make it easier for developers to build, test, and deploy smart contracts. It is often seen as an alternative to Truffle, and it offers several plug-and-play solutions for development.

5. Moralis: Moralis is a backend-as-a-service (BaaS) platform for building decentralized applications (dApps) that provides developers with a plug-and-play backend infrastructure. It allows developers to focus on building the front-end and user experience while Moralis handles the blockchain-related backend operations.

6. MetaMask: While not a platform in the traditional sense, MetaMask is an essential plug-and-play tool for interacting with Ethereum and other blockchains directly from the browser. It is a browser extension (and mobile app) that acts as a wallet and enables users to manage their Ethereum private keys and interact with decentralized applications (dApps).

Que25. Explain mechanism permissioned blockchain

Ans A permissioned blockchain is a type of blockchain in which access and participation are restricted to a set of known and authorized entities, rather than being open to anyone as in permissionless blockchains like Bitcoin or Ethereum. Permissioned blockchains are typically used in enterprise settings where trust, privacy, and control over participants are important. In these blockchains, only authorized participants can read, write, or validate the transactions, which can significantly improve efficiency and scalability for specific use cases, such as supply chains, financial services, or healthcare systems.

The mechanisms in a permissioned blockchain are designed to address the requirements for privacy, scalability, and governance while maintaining the core benefits of blockchain technology, such as immutability, decentralization, and security.

Mechanisms in Permissioned Blockchains

1. Identity and Access Control

    Authorized Participants: In permissioned blockchains, participants are usually known and their identities are verified. This can be achieved through integration with identity management systems. Only those who have been granted permission can participate in the network, ensuring that malicious or unauthorized actors cannot access or alter the network.

    Access Control: The blockchain network can enforce strict access control policies, which specify who can read data, write data, or validate transactions. This allows the network to maintain privacy while still ensuring transparency and accountability for those authorized.

2. Consensus Mechanism: In permissioned blockchains, consensus mechanisms are generally more efficient and less computationally expensive than in permissionless blockchains. Since the participants are known and trusted to some extent, the network can use a variety of consensus algorithms that do not rely on Proof of Work (PoW), which requires significant computational resources.

3. Privacy and Data Confidentiality: In many permissioned blockchains, data confidentiality is a major requirement, especially for industries like banking, healthcare, and supply chain. To address privacy concerns, permissioned blockchains implement various privacy-preserving mechanisms:

4. Smart Contracts and Chaincode: Smart Contracts in permissioned blockchains are typically more controlled and easier to audit since the participants are known. These smart contracts are often referred to as chaincode (in Hyperledger Fabric).

5. Governance and Role-Based Management: Governance in permissioned blockchains is critical because these blockchains often support a controlled, enterprise-level environment where participants need to follow certain rules and regulations. Governance mechanisms define how decisions are made regarding the network, such as adding new participants, changing consensus rules, or upgrading the protocol.

6. Scalability: Permissioned blockchains can be more scalable than permissionless blockchains due to their ability to control who participates in the consensus process and who can read or write to the ledger. Since the number of participants is usually smaller, the blockchain network can handle a higher volume of transactions with lower latency and faster block validation times. Some permissioned blockchain platforms also include mechanisms for sharding or parallel execution of transactions to increase scalability and throughput, which is important in enterprise-grade solutions.

7. Auditability and Transparency: One of the key benefits of permissioned blockchains is the ability to audit and trace all actions and transactions on the ledger while still maintaining privacy. Since all participants are known and trusted, a clear audit trail is maintained for compliance, regulatory, or business purposes.

   Immutable Ledger: Like permissionless blockchains, permissioned blockchains also offer immutability. Once data is written to the blockchain, it cannot be altered or deleted, which provides a transparent and auditable record of all transactions. This is useful in sectors like finance, healthcare, and logistics where regulatory compliance and data integrity are essential.

Examples of Permissioned Blockchain Platforms

1. Hyperledger Fabric: Hyperledger Fabric is one of the most widely used permissioned blockchain frameworks. It uses a modular architecture and supports multiple consensus mechanisms, including PBFT and Raft. Hyperledger Fabric allows fine-grained control over privacy and access and is well-suited for enterprise applications.

2. Corda: Corda is a blockchain platform designed specifically for financial institutions and other regulated industries. It emphasizes privacy and scalability, with features like notary services to ensure transaction uniqueness and consensus.

3. Quorum: Quorum is an enterprise-focused blockchain platform built on Ethereum, designed for permissioned networks. It uses modified consensus mechanisms (like Istanbul BFT) for high-speed transaction processing and provides data privacy features.

4. Ripple: Ripple is a permissioned blockchain platform used for cross-border payments. It uses the RippleNet consensus mechanism, which is different from traditional Proof of Work (PoW) and allows for fast and low-cost transactions between banks and financial institutions.

Unit: 5

Q.1. Explain some best-known Alt coin.

Ans. As the world of cryptocurrency continues to evolve, new digital assets, known as ‘altcoins’, are making their mark. Altcoins, short for alternative coins, refer to any cryptocurrency other than Bitcoin (and, for some, Ethereum). Some best-known Alt coin are as follows -

(i) **Namecoin :** Released in April 2011, Namecoin is the first notable altcoin. It's similar to Bitcoin since it's based on Bitcoin's code and has the same maximum supply of 21 million coins. Namecoin is known for introducing .bit web domains, which offer anonymity and resistance to censorship.

(ii) **Ether** - Ether is the native cryptocurrency of the Ethereum blockchain network. Each Ethereum account has an ETH balance and may send ETH to any other accounts. The smallest subunit of Ether is known as Wei.

(iii) **Litecoin** - Litecoin is a peer-to-peer cryptocurrency and in technical terms, Litecoin is nearly identical to Bitcoin. It uses a script in its proof-of-work algorithm. It is an adaptation of Bitcoin that is intended to make payment easier.

(iv) **Stablecoins** - These are the class of cryptocurrencies whose values are designed to stay stable relative to real-world assets like the U.S. Dollar.

(v) **Solana** - Solana is a competitor of Ethereum whose main emphasis is on speed and cost-effectiveness.

(vi) **USD Coin:** Released in September 2018, USD Coin is a stablecoin pegged to the U.S. dollar. It's under governance by Centre, a consortium that includes **Coinbase Global, Inc.**

Q.2. How to store Bitcoin/cryptocurrency?

Ans. Once the cryptocurrency is purchased, it needs to be stored safely to protect it from hackers. The usual place to store cryptocurrency is crypto wallets which can be physical devices or online software. Not all exchanges or brokers provide crypto wnllct services The cryptocurrencies can be stored in these four places -

(i) **Custodial Wallet** - In this approach, a third party such as a crypto exchange stores the cryptocurrency either through cold storage or hot storage, or a combination of the two. This is the simplest and most convenient method for the users as it requires less work on the user's part.

(ii) **Cold Wallet** - These are also known as Hardware wallets. It is an offline wallet in which hardware connects to the computer and stores the cryptocurrency. The device connects "to the internet at the time of sending and receiving cryptocurrency but other than that the cryptos are safely stored offline.

(iii) **Hot Wallet** - These are the applications that store cryptocurrencies online. These are available as desktop or mobile apps.

(iv) **Paper Wallet** - This is also known as a physical wallet. It is a printout of the public and private keys available as a string of characters or scannable QR codes. To send crypto scan the public and private keys and crypto will be received using the public keys.

Q3. Write the several features of Bitcoin /cryptocurrency.

Ans. Several features of Bitcoin are as follows -

(i) **Distributed** - All cryptocurrency /Bitcoin transactions are recorded in a public ledger known as the blockchain. There are nodes in the network that maintain copies of the ledger and contribute to the correct propagation of the transactions following the rules of the protocols making it impossible for the network to suffer downtime.

(ii) **Decentralized** - There is no third party or no CEO who controls the cryptocurrency /Bitcoin network. The network consists of willing participants who agree to the rules of a protocol and changes to the protocol are done by the consensus of its users. This makes cryptocurrency /Bitcoin a quasi-political system.

(iii) **Transparent** - The addition of new transactions to the blockchain 1edgcr and the state of the Bitcoin network is arrived upon by consensus in a transparent manner according to the rules of the protocol.

(iv) **Peer-to-Peer-** In cryptocurrency /Bitcoin transactions, the payments go straight from one party to another party so there is no need for any third party to act as an intermediary.

(v) **Censorship Resistant** - As cryptocurrency /Bitcoin transactions are pseudo- anonymous and users possess the keys to their Bitcoin holdings, so it is difficult for the authorities to ban users from using their assets. This provides economic freedom to the users.

(vi) **Public** - All cryptocurrency /Bitcoin transactions are available publicly for everyone to see. All the transactions arc recorded, which eliminates the possibility of fraudulent transactions.

(vii) **Permissionless** - cryptocurrency /Bitcoin is completely open access and ready to use for everyone, there are no complicated rules of entry-. Any transaction that follows the set algorithm will be processed with certainty.

(viii) **Pseudo-anonymous** - cryptocurrency /Bitcoin transactions are tied to addresses that take the form of randomly generated alphanumeric strings.

Q.4. How do cryptocurrency /Bitcoin transactions work ?

Or

Explain cryptocurrency /Bitcoin transactions.

Ans. Bitcoin transactions are digitally signed for security. Everyone on the network gets to know about a transaction. Anyone can create a Bitcoin wallet by downloading the Bitcoin program. Each Bitcoin wallet has two things -

(i) **Public Key** - It is like an address or an account number via which any user or account can receive Bitcoins.

(ii) **Private Key** - It is like a digital signature via which anyone can send Bitcoins. The public key can be shared with anyone but the private key must be held by the owner. If the private key gets hacked or stolen then Bitcoin gets lost. A Bitcoin transactions contains three pieces of information -

(i) **Private Key** - The first part contains the Bitcoin wallet address of the sender i.e., the private key.

(ii) **Amount of Bitcoin to be Transferred** - The second part contains the amount that has been sent.

(iii) **Public Key** - The third part contains the Bitcoin wallet address of the recipient, i.e., the public key.

Bitcoin transactions are verified by the nodes on the network. Once the transaction is verified and executed successfully, the transaction is recorded in a distributed public ledger called a blockchain. A Bitcoin can also be considered as an invisible currency with only the transaction records between different addresses.

Q5. How do cryptocurrency /Bitcoin come into market?

Ans. cryptocurrency /Bitcoin are a decentralized currency, they are not printed, like rupees, they are produced by people and big companies, running computers all around the world, using software that solves mathematical problems.

(i) cryptocurrency /Bitcoin are mined using the computing power of the distributed network. This network also processes transactions made using Bitcoin.

(ii) cryptocurrency /Bitcoin are mined on the basis of computing power, so they take. Time to be generated.

(iii) To keep it valuable, it has been stated that only 21 million Bitcoins can be created by miners. By the year 2140, all the Bitcoins will be created.

(iv) Around the world, thousands of computers with very high computing power are processing transactions and securing the network by solv ing complex mathematical calculations and collecting new Bitcoin in exchange.

Q6. Write short notes on community, politics and regulations in cryptocurrency /Bitcoin.

Ans. cryptocurrency /Bitcoin operates within a complex ecosystem that involves community participation, political dynamics, and regulatory- considerations. An overview is as follows

(i) **Community** - The Bitcoin community is composed of developers, miners, investors, users, and enthusiasts who contribute to its development, use, and advocacy. This community plays a crucial role in the governance, innovation, and adoption of Bitcoin. Various forums, social media platforms, conferences, and meetups serve as spaces for community members to discuss ideas, propose improvements, and address challenges facing the cryptocurrency /Bitcoin network.

(ii) **Politics** - Bitcoin's decentralized nature means that decisions about its development and direction often involve political discussions and debates. Disagreements within the community can lead to contentious debates, forks (where the blockchain splits into two separate chains), and even schisms. Examples include debates over block size limits (leading to the creation of Bitcoin cash), consensus mechanisms, privacy features, and governance models.

(iii) **Regulations** - Governments around the world have different approaches to regulating Bitcoin and other cryptocurrencies. Some countries have embraced Bitcoin, recognizing it as a legitimate form of currency or asset, while others have imposed restrictions or outright bans due to concerns about money laundering, tax evasion, and its potential impact on traditional financial systems. Regulatory measures may include licensing requirements for exchanges and businesses dealing with cryptocurrencies, anti-money laundering (AML) and know-your-customer (KYC) regulations, taxation policies, and securities laws.

Q7. **What are the advantages of cryptocurrency /Bitcoin?**

Ans. Advantages of Bitcoin are as follows -

(i) **Ease of Transactions** - The original Bitcoin whitepaper defines it as a digital peer-to-peer currency which makes instantaneous transactions. Unlike payment networks like PayPal and Visa, Bitcoins incur very low transaction surcharges. The absence of an intermediary reduces waiting periods and makes Bitcoin transactions hassle-free. Bitcoin can be used for everyday transactions devoid of double-spending.

(ii) **Anonymity and Decentralization** - Alphanumeric cloaks hide Bitcoin users' identities and prevent illegitimate access. Although transactions are visible through connecting data points, Bitcoins enable a pseudonymous account that can safeguard user information. Unlike physical money, Bitcoins do not have regulatory authority, implying that financial records are encrypted.

(iii) **Value Appreciation** - Owing to the limited supply of Bitcoins since its beginning and its increasing usage, Bitcoins have appreciated. Unlike fiat money, the value of Bitcoins fluctuates with every transaction. However, the cryptocurrency bubble of 2021-2022 saw an enormous rise in Bitcoin's value.

(iv) **Security and Free from Market Forces** - Unlike fiat money transactions prone to cybcr-attacks and fraudulent activities, Bitcoins are encrypted and immune to seizure. Every Bitcoin transaction is visible on an openly distributed ledger, making unauthorized changes difficult. Additionally, the non-reversibility and inability to change the owner's address make duplicating or stealing Bitcoins almost impossible.

(v) **Tax-free and Zero Transaction Costs** - Most countries do not levy taxes on Bitcoin returns. Since third-party applications cannot intercept such transactions, it is not easy to implement a stable taxation policy. Every Bitcoin transaction implies a contribution to the network ai)d sharing the burden of authorisation, which makes transaction costs negligible.

Q.8. What are the disadvantages of cryptocurrency /Bitcoin?

Ans. Disadvantages of cryptocurrency /Bitcoin are as follows -

(i) **Volatility** - The volatile nature of cryptocurrencies depends on factors like limited supply, increasing market demand, investor sentiment, etc. The limited supply and growing demand make its value very susceptible to fluctuations. Uncertainty and possible security breaches make Bitcoin investment a risky one.

(ii) **Absence of Regulation** - Although potential investors consider the absence of government regulations a determining tactor, its decentralization makes it devoid of legal protection. The decentralised nature of Bitcoins can also affect owners of multiple units if a portion of the investors chooses to opt-out.

(iii) **Irreversibility and Limited Usage** - The irreversibility of Bitcoins adds to their unregulated and anonymous nature. Any accidental payment cannot be traced and therefore is risky. While investors generally store cryptocurrency units in crypto wallets, losing access to such wallets can mean incredible losses. Hence, Bitcoin docs not find application in most secured networks as a means of transaction. Bitcoin payments require a third party, unlike cash, debit, or credit card payments.

(iv) **Uncertain Future** - While several nations like EI Salvador have accepted Bitcoin as a regular payment mode, many countries have barred its usage. The economic shock posed by the Covid-19 pandemic has forced countries like Qatar, China, Turkey, North Macedonia, Egypt, Iraq, and Bangladesh to get into Bitcoins. Despite Bitcoin being legal in Russia, transactions involving Bitcoins are banned.

(v) **Technical Flaws and a Deflationary Effect** - Since Bitcoins is a relatively newer concept, the blockchain network has innumerable flaws and loopholes. It further explains its acceptance in general transactions. The limitation in the total number of Bitcoins available strains the existing Bitcoins and raises their value. A future surge in spending on Bitcoins may arise, potentially destabilising the economy.

Q9 Write application of Blockchain

Ans. Blockchain technology has a wide range of applications beyond just cryptocurrencies like Bitcoin. Below are some key areas where blockchain is being applied or has the potential to make a significant impact:

1. Cryptocurrency and Digital Payments

- **Cryptocurrencies** (e.g., Bitcoin, Ethereum, and others) are the most well-known application of blockchain. They allow for secure, decentralized digital currencies without needing intermediaries like banks.
- **Cross-border payments** can be more efficient and cost-effective using blockchain, reducing transaction fees and settlement times.

2. Supply Chain Management

- Blockchain enables transparency and traceability across the entire supply chain, allowing businesses to track the origin, status, and movement of goods in real-time.
- It helps reduce fraud, counterfeit products, and errors, ensuring that consumers and businesses have confidence in the authenticity of products.
- **Food safety**: Blockchain can track the journey of food products from farm to table, enabling quick response in case of contamination or recall.

3. Smart Contracts

- Smart contracts are self-executing contracts with the terms of the agreement directly written into code on the blockchain.
- These contracts automatically execute and enforce the terms of an agreement when certain conditions are met, reducing the need for intermediaries and minimizing disputes.
- Examples include real estate transactions, insurance claims, and financial agreements.

4. Healthcare

- Blockchain can be used to securely store and manage electronic health records (EHRs), ensuring that patient data is immutable, private, and accessible only to authorized parties.
- It can also enable more secure and transparent tracking of pharmaceutical supply chains to prevent counterfeit drugs.
- Interoperability between health systems could be enhanced using blockchain, allowing for better coordination of care.

5. Voting Systems

- Blockchain can be used to create secure, transparent, and tamper-proof voting systems for elections.

- This reduces the risk of election fraud and increases trust in the integrity of the voting process. Voters could cast their ballots remotely, knowing their votes are securely recorded.

6. Identity Management

- Blockchain can provide a decentralized, secure way of managing digital identities. Individuals can have control over their personal data and share it selectively with trusted entities, reducing the risk of identity theft and fraud.
- Examples include government-issued ID cards or passports, access to online services, and financial accounts.

7. Intellectual Property (IP) and Copyright Protection

- Blockchain can be used to register intellectual property rights and track the use and ownership of digital assets like music, art, or software.
- It can provide an immutable ledger that proves the origin and ownership of digital content, helping to prevent piracy and unauthorized use.

Q10 What is bitcoin consensus protocol?

Ans. **Bitcoin's consensus mechanism** is called **Proof of Work (PoW)**, which is the method used to validate and confirm transactions on the Bitcoin network. It ensures that all participants (nodes) in the decentralized network agree on the state of the blockchain and maintain its integrity, without the need for a central authority.

How Proof of Work (PoW) Works in Bitcoin:

In simple terms, **Proof of Work** is a mechanism that requires miners (participants in the Bitcoin network) to solve complex cryptographic puzzles to add new blocks to the blockchain. Here's a more detailed breakdown of how this works:

1. Transaction Pool:

- Bitcoin transactions are broadcast to the network and collected into a pool of unconfirmed transactions. These transactions are waiting to be included in the next block.

2. Block Creation and Mining:

- **Miners** (specialized participants in the network) gather a set of unconfirmed transactions and attempt to bundle them into a **block**.
- The miner then begins the process of solving a cryptographic puzzle, also called a **hashing problem**, which involves finding a value (called a **nonce**) that, when combined with the contents of the block, produces a hash value that meets specific criteria (it must start with a certain number of zeros).

3. Proof of Work:

- The miner must perform **computational work** (guessing nonces) until they find the correct nonce that generates the required hash. This process is resource-intensive because miners must try billions of different combinations.
- The correct solution is considered "proof" that the miner has done the necessary work to find the right nonce.

4. Block Validation and Consensus:

- Once the miner finds the correct hash, they broadcast the block to the network. Other miners and nodes (participants in the network) check the validity of the block and the proof of work.
- If the block is valid and the solution to the puzzle is correct, the block is added to the blockchain and becomes part of the permanent record.
- This process ensures that everyone on the network agrees on the state of the blockchain (i.e., the sequence of valid blocks).

5. Mining Reward:

- The miner who successfully solves the puzzle and adds the block to the blockchain is rewarded with newly created Bitcoin (the **block reward**) and transaction fees from the transactions included in the block. This incentivizes miners to continue securing the network.

Q11. What is bitcoin Blocks?

A **Bitcoin block** is a container or data structure that holds a collection of transactions on the Bitcoin network. Each block is a fundamental unit of the blockchain and is used to record and verify transactions in a decentralized, tamper-proof manner. Bitcoin blocks play a key role in ensuring the security, integrity, and immutability of the entire network.

Components of a Bitcoin Block

Each Bitcoin block consists of several components:

1. **Block Header:**
    - The block header contains metadata about the block and is essential for the consensus process. It includes the following fields:
    - **Version:** Indicates the version of the Bitcoin protocol used to create the block.
    - **Previous Block Hash:** A cryptographic hash of the previous block's header. This creates the chain of blocks and ensures that all blocks are linked together in a secure, chronological order.
    - **Merkle Root:** A hash that represents all the transactions included in the block, organized in a **Merkle Tree**. This allows for efficient and secure verification of transactions in the block.

- **Timestamp:** The time at which the block was created, in Unix timestamp format (number of seconds since January 1, 1970).
- **Difficulty Target:** A value that indicates the difficulty of the Proof of Work (PoW) puzzle that miners must solve to add the block to the blockchain. This value adjusts approximately every two weeks to maintain a consistent block time of about 10 minutes.
- **Nonce:** A 32-bit number that miners modify to find the correct hash that meets the required difficulty target. The nonce is part of the Proof of Work process.
- **Block Hash:** The cryptographic hash of the entire block header. It is used as a unique identifier for the block and is critical for the mining process.

2. **Transaction Data (Transaction List):**
    - Each block contains a list of Bitcoin transactions that have been confirmed by the network. This includes:
        - **Transaction Inputs:** The source of the Bitcoins being spent (previous transactions).
        - **Transaction Outputs:** The destinations for the Bitcoin being sent (the new owners).
        - **Transaction Amounts:** The amount of Bitcoin being transferred in each transaction.
        - **Transaction Fees:** Miners receive transaction fees as part of their reward for confirming transactions. These fees are included in the block and paid to the miner who successfully mines the block.
        - **Signatures and Scripts:** Digital signatures ensure that the sender of the transaction is authorized to spend the Bitcoins, and scripts control the conditions under which the Bitcoins can be spent.
3. **Block Size:**
    - The size of each block in Bitcoin is limited by the network's protocol. The current maximum block size is **1 MB** (though there are some variations with SegWit-enabled blocks, which can increase the effective block size). This means that each block can contain a limited number of transactions. When blocks reach this limit, miners must include transactions with the highest fees to incentivize them to be included in the block.

Q12 Explain Merkley tree

Ans A **Merkle tree**, also known as a **binary hash tree**, is a data structure used in computer science and cryptography that enables efficient and secure verification of the integrity and consistency of data. It is used extensively in blockchain technology, including Bitcoin, to verify the integrity of transactions in a block.

Merkle Tree

A Merkle tree is a **binary tree** structure where:

- **Leaf nodes** represent individual pieces of data (e.g., transactions).
- **Non-leaf nodes** represent hashes of their child nodes.
- The **root** of the tree, known as the **Merkle root**, is the final hash that summarizes the entire data set.

The Merkle tree allows for the efficient verification of whether a particular transaction (or piece of data) is included in a set of data without needing to download or examine the entire dataset. This is particularly useful in distributed systems like blockchains.

Components of a Merkle Tree

1. **Leaf Nodes:** These are the bottom-most nodes in the tree and usually represent individual pieces of data, such as transaction hashes. Each leaf node is a cryptographic hash of a piece of data.
2. **Non-Leaf Nodes:** These nodes represent the hash of their two child nodes. Each non-leaf node is a cryptographic hash of the concatenation of its two child nodes' hashes.
3. **Merkle Root:** The very top node of the tree, which is a hash that represents the entire set of data (all transactions in the case of a blockchain). The Merkle root is used to verify the integrity of all the transactions or data below it.

Working of Merkle Tree

1. Hashing the Data:

- Each piece of data (e.g., a transaction) is hashed using a cryptographic hash function (like SHA-256 in the case of Bitcoin). The result is a fixed-length hash, which is stored as a leaf node.

2. Pairing Hashes:

- Once all the leaf nodes are created, pairs of adjacent hashes are concatenated and hashed together to form the next level of the tree. This continues recursively, with each level forming hashes of the previous level, until only one hash remains—the **Merkle root**.

3. Merkle Root:

- The Merkle root is the top hash of the tree and serves as a compact representation of all the transactions or data in the tree. In Bitcoin, this Merkle root is included in the block header, and it ensures that any change in any transaction would result in a completely different Merkle root, allowing easy detection of tampering.

Q13 Write short note on Medical record management on Blockchain?

Ans A **Medical Record Management System on Blockchain** refers to a decentralized system for storing, managing, and sharing electronic health records (EHRs) using blockchain technology. The idea is to improve the security, accessibility, transparency, and interoperability of health data while giving patients more control over their own health information. Blockchain can solve many challenges in healthcare, such as data breaches, unauthorized access, interoperability issues, and inefficient data sharing.

Benefits of Using Blockchain for Medical Record Management

1. **Data Security and Privacy:**
    - **Immutability:** Once a record is stored on a blockchain, it cannot be altered or deleted without detection. This ensures that medical records are tamper-proof and can be trusted.
    - **Encryption:** Patient data can be encrypted and stored in a way that only authorized parties can access it. Private keys (held by patients and healthcare providers) ensure that access to sensitive health information is highly controlled.
    - **Decentralization:** Data is not stored in a single centralized location, which reduces the risks of data breaches, hacking, or system failures that affect centralized systems.
2. **Patient Control Over Data:**
    - Patients can control who has access to their medical data. Using blockchain, patients can grant permissions to different healthcare providers (doctors, hospitals, pharmacies, etc.) to view or update their records.
    - Smart contracts can automatically grant or revoke permissions based on pre-established rules set by the patient.
3. **Transparency and Trust:**
    - Blockchain allows for full traceability of health records. Every action performed on the records (access, modification, sharing) is logged on the blockchain and can be auditable by patients and healthcare providers. This increases trust between patients and healthcare providers.
4. **Interoperability:**
    - Blockchain can serve as a universal and standardized layer for medical data, allowing different healthcare systems, hospitals, and providers to exchange information without the need for costly and complex integrations. Blockchain's standardized protocols make it easier to connect disparate systems, improving data exchange across various platforms.
5. **Reduced Fraud and Errors:**

   - Blockchain's transparency and immutability reduce the likelihood of fraud, including falsified medical records or fraudulent billing. In addition, errors in patient data (due to manual entry mistakes or system issues) can be quickly identified and corrected.

6. **Reduced Administrative Costs:**
   - With blockchain, administrative processes such as billing, claims processing, and data verification are more automated, leading to cost savings and faster operations. Blockchain's transparency can help in streamlining insurance claims by making the process more transparent and efficient.

Components of a Blockchain-based Medical Record Management System

1. **Patient Identity Management:**
   - Patients can be assigned a unique **digital identity** (e.g., a public key or a blockchain address) that links to their health records. This identity is private, and only authorized users (with the correct private key or permission) can access the records.
2. **Decentralized Storage:**
   - Medical records can be stored on the blockchain itself or on a distributed storage system (e.g., IPFS or Filecoin) with links to the blockchain. Storing actual health data directly on a blockchain can be expensive due to the size constraints of blockchains, so the records are often stored off-chain with hashes on-chain for verification.
3. **Smart Contracts:**
   - **Smart contracts** are self-executing contracts with the terms directly written into code. In a medical record system, smart contracts can automate processes such as:
     - Granting or revoking access to medical records.
     - Notifying healthcare providers of required updates or tests.
     - Automatically executing billing processes when services are rendered.
     - Managing patient consent and privacy preferences.
4. **Audit Trail:**
   - Every access, modification, or sharing of medical records is recorded as a transaction on the blockchain. This **audit trail** provides complete visibility and accountability. Patients can see who accessed their records, when, and why.
5. **Consensus Mechanism:**
   - The blockchain can use a consensus mechanism like **Proof of Work (PoW)** or **Proof of Stake (PoS)**, or more efficient and privacy-centric mechanisms such

as **Proof of Authority (PoA)** or **Federated Consensus** (for private healthcare blockchains). This ensures that only authorized and validated entities are allowed to participate in the network.

6. **Access Control and Permissions:**
    - Blockchain's decentralized nature allows for granular access control mechanisms. For example:
        - Patients can grant temporary access to their records to specific providers (e.g., a surgeon for a particular procedure) or allow broader access to general practitioners and emergency room staff.
        - Access can be granted via encrypted keys, QR codes, or biometric data (e.g., fingerprint or facial recognition) for extra security.

Q14. Write short note on DNS record on blockchain

Ans A **DNS record on blockchain** refers to the integration of traditional **Domain Name System (DNS)** functionality with blockchain technology, creating a decentralized, tamper-proof system for managing domain name registrations, records, and resolutions. By utilizing blockchain, the process of managing and resolving domain names can be made more secure, transparent, and censorship-resistant.

DNS on Blockchain

Using blockchain to manage DNS records addresses the centralization and security issues in traditional DNS. By storing DNS records on a blockchain, we can achieve **decentralization**, **immutability**, and **transparency** in the domain name resolution process.

How Blockchain-based DNS Works

1. **Decentralized Ownership:**
    - Instead of relying on a central authority (e.g., a registrar), domain names are owned and controlled by their creators or users through blockchain-based **smart contracts** or **decentralized applications (dApps)**. Domains can be represented as **non-fungible tokens (NFTs)** or blockchain-based assets that are stored in a user's wallet.
2. **DNS Records on Blockchain:**
    - Instead of traditional DNS records being stored on centralized servers, DNS records are stored on the blockchain as part of a **public ledger**. This means that records are immutable and publicly verifiable, making them resistant to tampering.
    - These records might include:
        - **A Records** (mapping domains to IP addresses)

        - **MX Records** (mapping domains to email servers)
        - **CNAME Records** (aliasing domains)
        - **TXT Records** (verification and security records)

3. **Decentralized Domain Name Resolution:**
    - When a user tries to access a domain, a **decentralized resolver** (which is part of a blockchain network) queries the blockchain for the corresponding DNS records. These resolvers ensure that there is no single point of failure and can query decentralized networks to resolve domain names to IP addresses.
    - The **blockchain network** ensures that any changes to DNS records are transparent and tamper-proof, which increases trust and security.
4. **Smart Contracts for DNS Management:**
    - **Smart contracts** can be used to automate the process of DNS record management, allowing domain owners to update, transfer, or sell their domain records without needing a third-party registrar. These smart contracts can enforce rules about domain ownership, renewals, and transfers.
5. **Use of Cryptographic Proof:**
    - Blockchain's cryptographic mechanisms (public-private key pairs) can be used to ensure that only the rightful owner of a domain name can update or transfer it. The blockchain acts as a trustless system, removing the need for intermediaries to verify ownership.
    -

Que15. Explain double spending in blockchain

Ans **Double spending** is a potential problem in digital currency systems, including blockchain-based cryptocurrencies, where a user attempts to spend the same cryptocurrency twice. It occurs when the same digital asset (e.g., Bitcoin, Ether) is used for two or more transactions, effectively creating a situation where the currency is "spent" more than once, undermining the integrity of the system.

In traditional financial systems, such as those involving banknotes or credit card payments, double spending isn't a concern because transactions are centrally recorded and monitored by a trusted intermediary (such as a bank). However, in decentralized systems like cryptocurrencies, there is no central authority, so the system must rely on its protocols to prevent double spending.

How Double Spending Works

In a digital currency system, the problem of double spending can arise because digital information (like a cryptocurrency) can be copied and transmitted easily. For example:

1. **User A** sends 1 Bitcoin to **User B**.

2. Simultaneously, **User A** tries to send the same 1 Bitcoin to **User C** by broadcasting two different transactions to the network.

If both transactions are accepted by the network, it creates a situation where **User A** has effectively spent the same Bitcoin twice, which would be a breach of the system's rules.

Que16. What is Hardness of mining?

Ans. The **hardness of mining** in blockchain refers to the level of difficulty required for miners to solve the cryptographic puzzles necessary to validate transactions and add new blocks to the blockchain. This difficulty adjusts over time to maintain a stable rate of block creation, regardless of fluctuations in the total computational power (or hash rate) of the network. The mining difficulty is a critical component of **Proof of Work (PoW)** blockchains like **Bitcoin**, which relies on miners solving computational puzzles in order to secure the network, verify transactions, and maintain the integrity of the ledger.

1. Mining and Proof of Work

In **Proof of Work (PoW)** blockchains, miners compete to solve complex mathematical puzzles in order to create a new block. These puzzles involve finding a hash value that meets specific conditions, such as having a certain number of leading zeroes.

- **Hashing**: The puzzle is to find a **hash** (a fixed-length string of numbers and letters) that meets certain criteria. This is done by repeatedly hashing the block header with different nonce values (random numbers). The hash must be below a target value set by the network.
- **Nonce**: Miners generate different nonce values in an attempt to find a valid hash. The miner who first finds the valid hash gets to add the block to the blockchain and is rewarded with the block reward (usually in cryptocurrency).

The process of **mining** is computationally expensive and requires significant processing power. The **hardness** of this mining process determines how long it will take for a miner to find the correct hash and thus solve the puzzle.

2. Difficulty Adjustment

To prevent blocks from being mined too quickly or too slowly, most blockchains, such as **Bitcoin**, have a **difficulty adjustment mechanism**. This mechanism adjusts the mining difficulty periodically to ensure that blocks are mined at a consistent rate, regardless of changes in the network's hash rate (total computational power).

- **Bitcoin's Difficulty Adjustment:** For example, Bitcoin adjusts its mining difficulty every **2016 blocks** (roughly every two weeks). The goal is to ensure that, on average, one block is mined every 10 minutes. If miners' combined computational power increases (for instance, if more miners join the network or existing miners upgrade their hardware), the difficulty will adjust upwards to ensure the 10-minute target is maintained. Conversely, if miners leave the network or if there is a decrease in computational power, the difficulty will adjust downwards to keep block creation times stable.

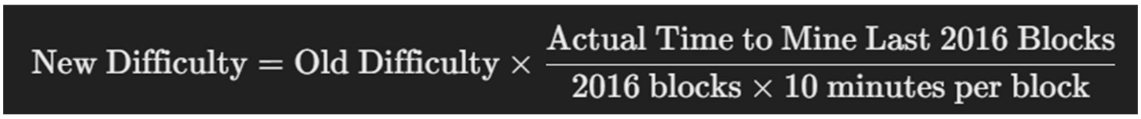
3. How Mining Difficulty Works in Practice

The **mining difficulty** is directly tied to the **target hash value** that miners must find. The lower the target, the more difficult it is to find a valid hash.

- **Target Hash**: The network sets a target value that the hash of a block must be below in order to be accepted as valid. The target hash is a large number, and miners must find a hash that is numerically lower than this target.
- **Adjusting the Difficulty**: If blocks are being mined too quickly (e.g., faster than the intended 10-minute interval in Bitcoin), the network increases the difficulty by lowering the target. This makes the puzzle harder, requiring more computational power to solve. If blocks are being mined too slowly (e.g., slower than the 10-minute target), the difficulty is reduced by raising the target, making the puzzle easier.

4. Mining Difficulty Formula (in Bitcoin)

In Bitcoin, the difficulty is calculated based on the time it took to mine the last 2016 blocks. The formula for adjusting difficulty is:



$$\text{New Difficulty} = \text{Old Difficulty} \times \frac{\text{Actual Time to Mine Last 2016 Blocks}}{\text{2016 blocks} \times \text{10 minutes per block}}$$

- If the actual time taken to mine the last 2016 blocks is less than expected (i.e., blocks were mined too quickly), the difficulty increases.
- If the actual time taken to mine the blocks is greater than expected (i.e., blocks were mined too slowly), the difficulty decreases.

The difficulty is adjusted so that it takes about two weeks to mine 2016 blocks, keeping the **block interval** around 10 minutes.

5. Impact of Mining Difficulty on Blockchain

- **Security**: The difficulty of mining ensures that the blockchain is secure by making it computationally expensive and resource-intensive to attack the network. For example, an attacker would need to control more than 50% of the network's total computational power (known as a **51% attack**) to rewrite the blockchain, which becomes harder as the difficulty increases.
- **Block Creation Rate**: By adjusting the difficulty, the network maintains a steady rate of block creation, ensuring that new transactions are added to the blockchain in a timely manner. This is crucial for the **consensus mechanism** because the longer it takes to mine a block, the slower the overall transaction processing rate becomes.

6. Why Mining Difficulty Changes

Mining difficulty changes based on the following factors:

1. **Hashrate Fluctuations**: If the total computational power (hashrate) of the network increases (due to more miners joining or hardware upgrades), the network adjusts the difficulty upward to keep block mining times constant. If the hashrate decreases (due to miners leaving or hardware failure), the difficulty adjusts downward.

2. **Network Upgrades**: Changes to the network protocol can also affect the difficulty adjustment mechanism. For instance, certain upgrades might alter the block size, block time, or other parameters, which can affect how quickly blocks are mined and therefore the difficulty adjustment.

3. **Mining Profitability**: If the price of the cryptocurrency rises significantly, more miners might join the network, increasing the total hashrate. Conversely, if the price falls and mining becomes less profitable, miners may leave the network, reducing the hashrate.