DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

U23CST63-BLOCKCHAIN TECHNOLOGIES

UNIT -1 INTRODUCTION TO BLOCKCHAIN

PART A

1. Define blockchain

A blockchain is "a distributed database that maintains a continuously growing list of ordered records, called blocks." These blocks "are linked using cryptography.

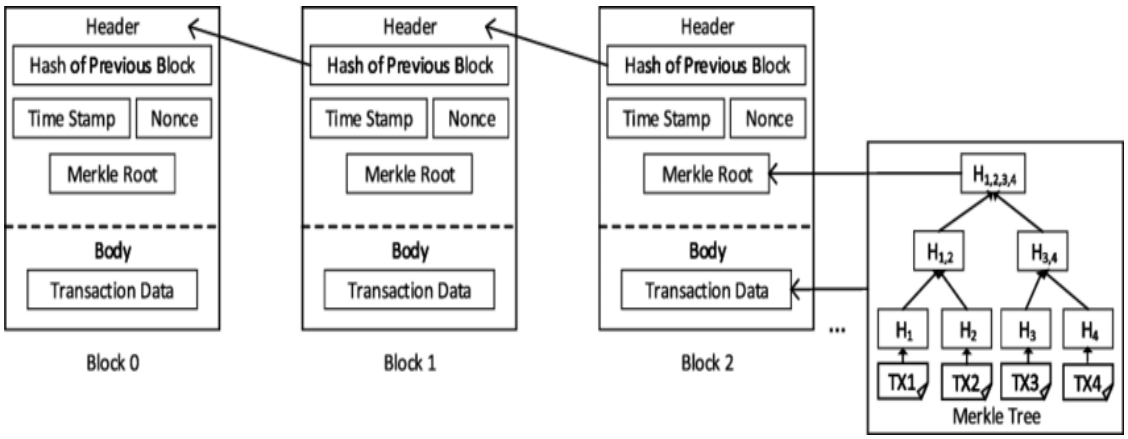
2. Define block in a block chain

Block is a place in a blockchain where data is stored. In the case of cryptocurrency blockchains, the data stored in a block are transactions. These blocks are chained together by adding the previous block's hash to the next block's header.

3. What are the parts in the block structure?

A block consists of the following two main parts:

- Header
- Body



4. Define nonce

- This is an integer that a miner changes to change the hash of the block to achieve the network's difficulty.
- The blockchain nonce is used in conjunction with the other data in the block to create a unique, fixed-size string of letters and numbers known as a "hash." This hash serves as a digital fingerprint for the block, and it is what allows the blockchain to maintain its integrity and security.

5. What are the business benefits of blockchain?

- Time savings.
- Cost savings.
- Tighter security

6. What is a Genesis Block?

- The genesis block is the first block in the Blockchain which is also known as block 0

- In Blockchain, it is the only block that doesn't refer to its previous block.
- It defines the parameters of the Blockchain such as, level of difficulty, consensus mechanism etc. to mine blocks

7. What are the four key concepts behind Blockchain?

- Shared ledger.
- Permissions
- Smart contracts.
- Consensus

8. What is the role of Blockchain Network Operators?

Individuals who have special permissions and authority to define, create, manage, and monitor the blockchain network.

9. What Is Hashing in Blockchain?

The process of making an input item of any length represents an output item of a fixed length is referred to as hashing in the blockchain. Take, for example, the use of blockchain in cryptocurrencies, where transactions of varying lengths are run through a given hashing algorithm and all produce a fixed-length performance.

10. Define private and public blockchain

- Public blockchains "use computers connected to the public internet to validate transactions and bundle them into blocks to add to the ledger.
- Private blockchains, on the other hand, typically only permit known organizations to join." Because any organization can join public blockchains, they might not be right for enterprises concerned about the confidentiality of the information moving through the network.

11. Difference Between Permissioned Blockchains Vs Permissionless Blockchains

- Permissioned blockchains - Closed networks with limited decentralization, an additional access control layer, and designated entities
- Permissionless blockchains - Open, decentralized networks with universal consensus validation; anyone can join the network and possess a copy of the ledger

12. What are the aspects of a Permissioned Blockchain?

- Decisions are authorized by a private group
- Security
- Decentralization isn't fixed
- Transparency is not required
- Levels of transparency
- Lack of anonymity

13. What is cryptography? What is its role in Blockchain?

- Blockchain uses cryptography to secure users' identities and ensure transactions are done safely with a hash function.
- Cryptography uses public and private keys in order to encrypt and decrypt data. In the Blockchain network, a public key can be shared with all the Bitcoin users but a private key (just like a password) is kept secret with the users.
- Blockchain uses SHA - 256 which is secure and provides a unique hash output for every input. The basic feature of this algorithm is whatever input you pass, it will give you a

standard alphanumeric output of 64 characters. It is a one-way function from which you can derive an encrypted value from the input, but not vice-versa.

14. How is Blockchain distributed ledger different from a traditional ledger?

- A Blockchain distributed ledger is highly transparent as compared to a traditional ledger.
- Blockchain distributed ledgers are irreversible. Information registered on a distributed ledger cannot be modified whereas on a traditional ledger it is reversible.
- A distributed ledger is more secure. It uses cryptography and every transaction is hashed and recorded whereas in traditional ledger security can be compromised.
- In a distributed ledger, there is no central authority. It is a distributed system and the participants hold the authority to maintain the sanity of the network and are responsible for validating the transactions. Traditional ledgers are based on the concept of centralized control, which controls all transactions.

15. What is Merkel Tree?

Merkel Tree is a data structure that is used for verifying a block. It is in the form of a binary tree containing cryptographic hashes of each block. A Merkle tree is structured similarly to a binary tree where each leaf node is a hash of a block of transactional data and each non-leaf node is a hash of its leaf node. The Merkel root or hash root is the final hash root of all the transaction hashes. It encompasses all the transactions that are underlying all the non-leaf nodes.

16. What are the different types of Blockchain?

- There are three different types of Blockchain - Public, Private, and Consortium Blockchain.
- Public Blockchain ledgers are visible to all the users on the internet and any user can verify and add a block of transactions to the Blockchain. Examples, Bitcoin, and Ethereum.
- Private Blockchain ledgers are visible to users on the internet but only specific users in the organization can verify and add transactions. It's a permissioned blockchain, although the information is available publicly, the controllers of the information are within the organization and are predetermined. Example, Blockstack.
- In Consortium Blockchain, the consensus process is controlled by only specific nodes. However, ledgers are visible to all participants in the consortium Blockchain. Example, Ripple.

17. What are the advantages of permissioned blockchain?

- High level of privacy and security
- Flexibility
- Also highly customizable
- Both scalable and highly performant due to the limited number of nodes needed to manage transaction verifications.

18. What are all the applications of blockchains ?

- Cryptocurrency
- Advertising
- Real Estate
- Healthcare
- Voting
- Insurance
- Media
- Taxes

19. What is a Node?

- A node can be defined as an individual processing unit in a distributed system.
- All nodes are capable of sending and receiving messages to and from each other.

20. What is meant by ledger and public ledger?

- A ledger is a record-keeping book that stores all the transactions of an organization.
- A public ledger is an open-access network; anyone can join at any time. The public ledger is fully decentralized, and no single entity controls the blockchain network.

21. What are all the advantages of distributed ledgers?

- It is secure because there is no third-party intervention.
- It is immutable once recorded cannot be intervened.
- The data is distributed so it is tamper-proof.

22. What are all the disadvantages of distributed ledger?

- The distributed ledger is spread along with the nodes so making it vulnerable to attack.
- The transaction cost is high because of a larger network.
- The transaction speed is low because of the operation of a large number of nodes.

23. What is the longest chain?

The longest chain is the chain of blocks that took the most effort to build. In short, to add a new block to the blockchain you need to use processing power, which means that every block on the blockchain used up energy to get there.

24. How do you calculate the longest chain?

- The longest chain is measured by a metric called "chainwork". Chainwork is the total number of hashes that are expected to have been necessary to produce the current chain.
- To work out chainwork, you just need to work out how many hashes you would have needed to perform to mine each block in the chain, then add them up.
- The average expected number of hashes for each block depends on what the target was at the time.

25. What about transactions that are not part of the longest chain?

- A transaction inside a block that is not part of the longest chain is invalid.
- If you tried to spend the bitcoins from a transaction that is not in the longest chain, nodes would not accept it nor try to mine it in to a block. This is because nodes only consider the longest chain the valid history history of transactions, and anything outside of that is not a valid transaction

26. Compare Blockchain with relational database

Criteria	Blockchain	RDBMS
Unit of data	Block	Table

Single point of failure	Does not exist	Exists
Centralized control	No	Yes
Editing/deleting data	Not possible	Possible

27. What are types of blockchain? Who maintains the copy of the ledger in each type? (Nov/DEC 2023)

The two main types of blockchains are public (permissionless) and private (permissioned) blockchains. In a public blockchain, anyone can join the network, participate in consensus, and maintain a copy of the ledger. In a private blockchain, access is restricted to a predefined group of participants, usually within an organization, consortium, or enterprise. The maintenance of the ledger in a private blockchain is typically managed by a designated set of network participants or nodes.

28. "In blockchains consistency is sacrificed in favour of availability and partitions tolerance". Comment on this statement.

According to the CAP (Consistency, Availability, Partition tolerance) theorem, it is impossible for a distributed system to simultaneously guarantee consistency, availability, and partition tolerance under network partitions.

Part-B

1. Discuss the concept of public ledgers and their significance in blockchain technology. How do public ledgers ensure transparency and accountability in transactions?
2. Describe the structure of a block in a blockchain. What information does a typical block contain, and how are blocks linked together to form a chain?
3. Compare and contrast the permissioned and permissionless models of blockchain. What are the advantages and disadvantages of each model?
4. Explain the cryptographic hash function and its role in securing data in a blockchain. How does hashing contribute to the immutability and integrity of a blockchain?
5. Discuss the properties of a hash function, including collision resistance, pre-image resistance, and avalanche effect. Why are these properties important for cryptographic hash functions used in blockchain?
6. How do hash pointers enhance the security and efficiency of a blockchain network? Provide examples of how hash pointers are used in real-world blockchain implementations.
7. Explain the concept of a Merkle tree and its significance in blockchain data structures. How does a Merkle tree enable efficient verification of data integrity in a blockchain network?
8. Discuss the **(Nov/DEC 2023)**
    1. Benefits and limitations of blockchain
    2. Consensus in blockchain
9. What are the properties of Cryptographic hash function? **(Nov/DEC 2023)**
10. Explain how hash pointers are useful in Merkle tree? **(Nov/DEC 2023)**
11. Compare centralized, decentralized and distributed system. Explain how blockchain technology achieves decentralized security and trust with the cryptographic primitives. **(Nov/DEC 2023)**

UNIT -II BITCOIN AND CRYPTOCURRENCY

PART A

1. **What is A basic crypto currency?**

   A basic cryptocurrency is a digital or virtual currency that uses cryptography for security and operates on a decentralized network, typically a blockchain. It is designed to function as a medium of exchange, allowing users to securely send and receive transactions without the need for intermediaries like banks.

2. **What are all the steps involve in Create Your Own Cryptocurrency?**
   - Mining
   - Staking
   - Predetermined Issuance

3. **What is Double spending?**

   Double spending means spending the same money twice. Double spending is a potential vulnerability in digital currency systems where a user spends the same amount of cryptocurrency more than once. It occurs when someone attempts to use the same funds for multiple transactions, taking advantage of the digital nature of the currency and attempting to deceive the network participants.

4. **What are all the types of Double Spending Attacks?**
   - Finney Attack
   - Race attack
   - 51% Attack

5. **What are all the approaches for the Solutions to Prevent Double Spending?**
   - Centralized Approach
   - Decentralized Approach

6. **Explain FORTH – the precursor for Bitcoin scripting**

   FORTH is a programming language that influenced the scripting language used in Bitcoin. FORTH is a stack-based, extensible programming language developed by Charles H. Moore in the 1970s. It is known for its simplicity, efficiency, and the use of a stack to manipulate data. FORTH programs are composed of a series of words (functions) that operate on a stack of data elements.

7. What is Bitcoin scripts?

Bitcoin scripts are a fundamental component of the Bitcoin protocol that enable the creation of conditions and constraints for spending bitcoins. They are written in a simple scripting language specifically designed for Bitcoin.

8. What are the types of Bitcoin Scripts?

Script is a very basic programming language. It consists of two types of things:

- Data - For example; public keys and signatures.
- OPCODES - Simple functions that operate on the data.

9. What is Bitcoin P2P Network?

The peer-to-peer architecture of blockchain allows all cryptocurrencies to be transferred worldwide, without the need of any middle-man or intermediaries or central serverPeer-to-Peer (P2P) network consists of a group of devices that collectively store and share files. Each participant (Node) acts as an individual peer.

10. Define Block Mining

Blockchain mining is used to secure and verify bitcoin transactions. Mining involves Blockchain miners who add bitcoin transaction data to Bitcoin's global public ledger of past transactions. In the ledgers, blocks are secured by Blockchain miners and /are connected to each other forming a chain.

11. What are all the two way to mine Bitcoins?

There are two ways to mine bitcoins.

1. Mining bitcoins on cloud
2. Mining bitcoins on your own

12. What are all the elements of a Bitcoin Transaction ?

When a transaction is initiated in the bitcoin network, three elements are involved:

- A transaction input
- A transaction output
- The transaction amount

13. Define Block Header and its components:

The block header contains information about the block and includes the following components:

- The version number of the bitcoin software
- The hash of the previous block
- The Merkle root (root hash)

- Timestamp
- Cryptographic nonce
- The target

14. What Is Block propagation?

Block propagation refers to the process of broadcasting a newly mined or validated block from one node to other nodes in the blockchain network. When a miner successfully mines a new block or a validating node confirms a new block, it needs to propagate this block to the rest of the network to ensure that all nodes have the latest state of the blockchain.

15. What is Block Relay?

Block relay is the process of relaying a block from one peer to another peer in the blockchain network. It is an essential part of block propagation and ensures that blocks are efficiently and securely disseminated across the network.

16. What are the three major planes of block propagation?

A simple, easier-to-visualize architecture can accommodate the aforementioned procedure. Consider a pyramid that has three planes:

- The network plane
- The consensus plane, and
- The ledger plane

17. How does Bitcoin use Blockchain?

A transaction is a value transfer that is recorded in the blockchain between Bitcoin wallets. Bitcoin wallets store a private key, also known as a seed, which is used to sign transactions and provide mathematical proof that they came from the wallet's owner.

18. What do you mean by Coinbase transaction?

In a block, the first transaction is a Coinbase transaction. A miner will build this unique kind of bitcoin transaction. It is used by miners to receive the block reward for their efforts, as well as any other transaction fees.

19. In a money transfer system, what is the need for decentralization? (Nov/Dec 2023)

- Reduced Dependence on Central Authorities
- Enhanced Security and Resilience
- Increased Transparency and Trust
- Financial Inclusion
- Cost Efficiency

20. What is bitcoin mining? Write any two purposes of mining process. (Nov/Dec 2023)

Bitcoin mining is the process by which new bitcoins are created and transactions are verified and added to the blockchain ledger. Miners use specialized hardware and compete to solve complex mathematical puzzles, known as proof-of-work (PoW), to validate transactions and secure the network. Two purposes of the mining process are:

Transaction Verification: Miners verify and validate transactions by including them in new blocks added to the blockchain. This ensures the integrity and immutability of the transaction history.

Issuance of New Bitcoins: Mining also serves as the mechanism for issuing new bitcoins into circulation. Miners who successfully mine a new block are rewarded with a predetermined number of bitcoins, incentivizing participation in the network and maintaining its security.

21. What is the Genesis block in blockchain? What is the hidden message it contain? (Nov/Dec 2023)

The Genesis block is the very first block in a blockchain network, serving as the foundation upon which subsequent blocks are built. It contains special metadata and serves as the reference point for calculating subsequent block hashes. The hidden message within the Genesis block of the Bitcoin blockchain is the embedded text: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This message, referencing a headline from The Times newspaper, is believed to be a timestamped commentary on the financial crisis of 2008 and the launch of Bitcoin as an alternative financial system.

Part-B

1. How to buy a bitcoin and perform transactions.Also expalin how to determine the value of bitcoin. (Nov/Dec 2023)
2. Assume that alice is a customer of some online merchants or website run by bob, who provides some online service in exchange for payment in bitcoins.Let's say bob's service allows the download some software. In this scenario how does the double spend attack executed? How to protect it? (Nov/Dec 2023)
3. Explain two sepertae incentive mechanism block reward, transaction fee used in bitcoin. (Nov/Dec 2023)
4. Explain mining process. What happens when two blocks that were mined within a short time of each other or received in reverse order? (Nov/Dec 2023)
5. Write note on blockchain forks.Expalin how the consistency is maintained. (Nov/Dec 2023)
6. Describe the fundamental characteristics that define a cryptocurrency. How does a cryptocurrency differ from traditional fiat currencies?
7. Explain the process of coin creation in a cryptocurrency system like Bitcoin. What role do miners play in the creation of new coins, and how are mining rewards distributed?
8. Define double spending in the context of cryptocurrency transactions. How does the blockchain prevent double spending, and what role do confirmations play in transaction security?

9. Discuss the significance of FORTH as the precursor for Bitcoin scripting. How does FORTH programming language influence the scripting capabilities of Bitcoin transactions?
10. Provide an overview of Bitcoin scripting language. What are scriptPubKey and scriptSig, and how do they interact to authorize Bitcoin transactions?
11. Describe the architecture and operation of the Bitcoin peer-to-peer (P2P) network. How do nodes communicate and propagate transactions and blocks in the Bitcoin network?
12. What are the different types of transactions, and how are they validated and included in blocks?
13. Explain the process of block mining in the Bitcoin network. How do miners compete to solve the proof-of-work puzzle, and what are the incentives for mining?
14. Discuss the challenges associated with block propagation and relay in the Bitcoin network. How does the network optimize block propagation to ensure timely consensus and minimize latency?

UNIT III BITCOIN CONSENSUS

PART A

1. What is proof of work?

Proof of work (PoW) is a consensus mechanism used in blockchain networks like Bitcoin where miners have to solve complex computational puzzles to validate transactions and create new blocks. This requires exerting computational effort and energy.

2. What is Hashcash in Bitcoin?

Hashcash is the specific proof of work algorithm used in Bitcoin mining. It involves finding a numeric value called a nonce that when hashed along with block data produces a hash within a target. This requires repeated trial and error.

3. How does Bitcoin mining work?

Bitcoin mining involves miners using powerful computers and ASIC hardware to find valid hashes very quickly. By solving the proof of work puzzle, a miner gets to add the next block to the Bitcoin blockchain and is rewarded bitcoin.

4. What are the incentives for Bitcoin mining?

Bitcoin miners are rewarded with new bitcoins for every block mined. They also earn the transaction fees attached to all transactions within the mined block as an incentive to validate transactions.

5. What is the mining difficulty in Bitcoin?

Mining difficulty is a metric that controls how hard the proof of work puzzle is to solve. It dynamically adjusts based on mining power to maintain ~10 minute block times.

6. What is a mining pool in Bitcoin?

Bitcoin mining pools allow individual miners to pool their computational resources and share the rewards. Joining a pool increases the chances of earning mining rewards.

7. What are some problems with proof of work?

Proof of work leads to massive energy usage, hardware centralization among big miners, and majority control threats if 51% mining power is reached.

8. What is proof of stake consensus?

Proof of stake is an alternative consensus where validators stake cryptocurrency holdings to verify transactions. It does not involve expensive computation allowing energy efficiency.

9. How is proof of stake different from proof of work?

Unlike PoW's computational races, PoS works by validators staking coins to attest transactions. PoS is energy efficient but has "Nothing at Stake" vulnerability.

10. What is the Byzantine Generals Problem in blockchain?
The Byzantine Generals Problem deals with reaching consensus among nodes where some nodes might be failure or malicious, similar to Blockchain consensus.

11. What is a 51% attack on blockchains?
A 51% attack happens when a miner gains majority hashpower allowing them to tamper with the blockchain by double spending and preventing transactions.

12. How do permissioned blockchains differ from public ones?
Permissioned blockchains only allow approved, known participants to join the network unlike public blockchains where anyone can participate.

13. Where are permissioned blockchains used?
Permissioned blockchains are used commonly in enterprise settings where organizations want to share confidential data selectively with access control.

14. Write practical examples of a 51% attack. (Nov/Dec 2023)
Double Spending: An attacker with majority control of the network's hash rate can execute double-spending attacks, where they spend the same bitcoins in two conflicting transactions. By controlling the majority of the network's computational power, the attacker can manipulate transaction confirmations and invalidate legitimate transactions.

15. How does proof of burn work?
Proof of burn (PoB) requires miners to prove burning their coins by intentionally sending them to a verifiably unspendable address that essentially destroys those coins. This proves their commitment to the network. The miner can then mine a block in proportion to the amount of coins burnt, allowing the network to be secured in a trustless way.

16. What is delegated proof of stake?
Delegated proof of stake (DPoS) is a consensus mechanism where token holders vote to select a limited set of nodes responsible for validating transactions and proposing blocks. The stakeholder community elects "delegates" proportional to votes received, who take turns in a round robin fashion to participate in the block generation process.

17. What is an uncle block in Ethereum?
In Ethereum, uncle blocks refer to valid blocks that get orphaned or excluded from the main chain, usually because another miner published a competing block first. Even though uncle blocks do not form part of the main chain, they are still considered valid blocks and contribute to the security of the blockchain. Miners who proposed uncle blocks still earn a reduced "nephew" reward to incentivize mining even if not included in main chain. This helps minimize potential risks from network propagation delays.

18. What is gas in Ethereum transactions?

Gas refers to the unit that measures the amount of computational effort required to execute operations and smart contracts on the Ethereum network. Since computing power is required by nodes that execute smart contract operations, gas aims to quantify the amount of computational resources consumed. Gas price is specified in gwei, denominations of ether (ETH). Users pay for the execution costs and gas consumed by transactions in ether based on the gas price. The gas mechanism incentivizes nodes and prevents network spamming. Gas prices dynamically adjust based on network demand and congestion.

19. What is Practical Byzantine Fault Tolerance?

Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm that can function correctly even with Byzantine nodes in the network, as long as fewer than 1/3 of the total nodes are Byzantine. It involves a multi-phase process of voting and confirmation between nodes to reach consensus while tolerating faults. PBFT enables blockchain networks to maintain integrity as long as the threshold of faulty nodes is not crossed.

PART B

1. What is the proof of work consensus mechanism and how does it help secure the Bitcoin network? Explain the role of miners in the process.
2. Explain Hashcash proof of work algorithm used in Bitcoin mining. How is it resistant to denial of service attacks?
3. Describe how the difficulty adjustment process works in Bitcoin mining. Why is it important to maintain the ~10 minute block time?
4. What are some of the potential attacks and vulnerabilities of Bitcoin's proof of work consensus? Explain 51% attack, selfish mining, pool hopping.
5. What issues can arise if a few mining pools gain majority hash power in the Bitcoin network? Discuss the implications.
6. Compare and contrast proof of work versus proof of stake consensus mechanisms. What are some benefits and drawbacks of each?
7. Describe how proof of elapsed time consensus mechanism works. How does it leverage trusted execution environments?
8. Explain the difference between public/permissionless blockchains like Bitcoin versus private/permissioned blockchains. Give examples.
9. Where are permissioned blockchains commonly used? Discuss their applications in enterprise and consortium settings.
10. Compare permissioned blockchains to public ones in terms of access control, consensus mechanisms, scalability and governance. Highlight key tradeoffs.
11. What is merged mining and what benefits does it provide? Explain how merge mined chains can improve security.
12. Explain the concept of gas in Ethereum - what purpose does it serve and how is gas price determined?

UNIT IV HYPERLEDGER FABRIC & ETHEREUMBITCOIN CONSENSUS

PART A

1. What is chaincode in Hyperledger Fabric?
Chaincode contains smart contract logic that implements transaction logic and business rules. It is installed and instantiated on channels to be invoked by applications.

2. What is a channel in Hyperledger Fabric?
A channel is a private subnet for communication between specific network members. Multiple channels can exist to provide segmentation and data isolation.

3. How does endorsement work in Hyperledger Fabric?
Transactions must be endorsed by required organizations before commitment. Endorsers execute chaincode and return proposal responses to be validated.

4. What role do peers play in Hyperledger Fabric network?
Peers form the blockchain network, managing ledgers and running chaincode containers to perform read/write operations and transaction validation.

5. How are identities managed in Hyperledger Fabric?
A membership service provider (MSP) manages identities and certificates for each organization. Access control policies govern access to network resources.

6. What components make up the ordering service in Fabric?
Ordering service batches and sequences transactions using ordering nodes that leverage technologies like Kafka to deliver blocks.

7. What is Ethereum?
Ethereum is a decentralized, open-source blockchain featuring smart contracts functionality to develop and deploy distributed applications.

8. What is the Ethereum Virtual Machine (EVM)?
EVM executes Ethereum smart contract bytecode, enabling deployment on a global network of computers without downtime risk.

9. What is gas in Ethereum?
Gas refers to the unit of computation for operations on Ethereum. Gas fees are paid in ether for each transaction.

10. What is Geth and what does it do?
Geth is a command line tool that allows nodes to join the Ethereum network and operate as a full blockchain client or mine blocks.

11. What coding language are Ethereum smart contracts written in?
Smart contracts are typically written in high-level languages like Solidity and then compiled into EVM bytecode.

12. What is ether and what is its purpose?
Ether is the native cryptocurrency of Ethereum blockchain used to compensate mining nodes and pay for gas costs.

13. What is a DApp in Ethereum?
A decentralized application (DApp) is an application built on Ethereum blockchain that runs exactly as programmed with no downtime.

14. How does mining work in Ethereum?
Miners use computational power to solve the proof of work algorithm to create new Ethereum blocks and are rewarded with ether.

15. What is the Mist browser used for?
Mist browser provides a user-friendly way to browse Ethereum blockchain data, manage wallets and interact with DApps.

16. What threats does the 51% attack pose in Ethereum?
If a miner gains 51% control, they can manipulate the blockchain to double spend transactions and control the network.

17. What is wei? How does it differ from Ether? (Nov/Dec 2023)
"Wei" is the smallest unit of Ether, which is the cryptocurrency used on the Ethereum blockchain. Similar to how Bitcoin has its smallest unit called Satoshi, Ethereum has wei. There are 10^18 wei in 1 Ether.

18. What is wallet? Name any known wallet to hold ETH? (Nov/Dec 2023)
A wallet, is a digital tool used to store, send, and receive cryptocurrencies. It securely stores the private keys required to access and manage the funds associated with the wallet address. There are different types of wallets, including software wallets (desktop, mobile, or web-based), hardware wallets (physical devices), and paper wallets (physical printouts). One well-known wallet used to hold ETH is MetaMask. MetaMask is a popular software wallet available as a browser extension for Chrome, Firefox, and other web browsers.

PART B

1. Explain the core components that make up the architecture of Hyperledger Fabric. What roles do peers, orderers, MSPs, and channels play?
2. What is chaincode in Hyperledger Fabric? How is it different from smart contracts in other blockchain platforms? Explain chaincode lifecycle.
3. Describe the process of transaction flow and endorsement in a Hyperledger Fabric blockchain network. How does it differ from other blockchains?
4. What consensus mechanisms can be used in Hyperledger Fabric? Compare their tradeoffs in terms of scalability, decentralization and fault tolerance.
5. What are channels in Hyperledger Fabric? How do channels provide data isolation and confidentiality between network participants?
6. Explain Ethereum accounts and Ethereum Virtual Machine (EVM). How does the EVM execute smart contracts on Ethereum?
7. Describe the proof of work consensus mechanism in Ethereum. What role do miners play and what rewards do they get? What are risks like 51% attack?
8. What is gas in Ethereum? Why is gas required to execute transactions and smart contracts? How is gas price determined?
9. Discuss various scalability solutions being explored by Ethereum such as sharding, proof of stake, layer 2 networks etc.
10. Compare and contrast Ethereum with Hyperledger Fabric in terms of architecture, consensus, throughput, cryptocurrency and ledger type. (Nov/Dec 2023)
11. Explain the structure of a solidity code and provide an example for emphasizing the importance of interface in the model. (Nov/Dec 2023)
12. What kinds of memory is available for storing data of a smart contract? (Nov/Dec 2023)
13. Write a contrct in solidity for applying the given restriction. “Only the owner of the contract can set the value”. (Nov/Dec 2023)

UNIT V BLOCKCHAIN APPLICATIONS
PART A

1. **Which parameters influence the amount of gas utilization during a transaction?** **(Nov/Dec 2023)**
   - Gas price: The price of gas in ether (ETH) determines the cost of each unit of gas consumed in the transaction.
   - Gas limit: The maximum amount of gas that can be consumed by the transaction. It is set by the user to limit the execution cost of the transaction.
   - Computational complexity: The complexity of the operations performed in the transaction's smart contract code affects the amount of gas consumed.

2. **What are the use cases of Ethereum in healthcare domain?** **(Nov/Dec 2023)**
   - Patient data management: Ethereum's blockchain can be used to securely store and manage patient health records, ensuring data integrity and accessibility while maintaining patient privacy.
   - Supply chain management: Ethereum's smart contracts can be utilized to track the provenance and authenticity of pharmaceuticals and medical supplies, reducing the risk of counterfeit products entering the supply chain.
   - Clinical trials: Ethereum's blockchain can facilitate transparent and auditable clinical trials by recording trial data and ensuring the immutability of trial results.
   - Healthcare payments and insurance: Ethereum-based tokens and smart contracts can streamline healthcare payments and insurance processes, reducing administrative overhead and fraud.

3. **What are smart contracts and how do they work?**
   Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automatically execute and enforce the terms of the agreement when predefined conditions are met.

4. **What is Truffle and how is it used in blockchain development?**
   Truffle is a development environment, testing framework, and asset pipeline for Ethereum-based blockchain projects. It provides tools for writing, deploying, and testing smart contracts.

5. **What are DApps (Decentralized Applications) and how do they differ from traditional applications?**
   DApps are applications that run on decentralized networks like Ethereum rather than centralized servers. They differ from traditional applications in that they are not controlled by any single entity and often use smart contracts to manage functionality.

6. **What are NFTs (Non-Fungible Tokens) and how are they used in blockchain applications?**
   NFTs are unique digital assets that represent ownership or proof of authenticity of a specific item or piece of content. They are used in blockchain applications for digital art, collectibles, gaming, and more.

7. **How are blockchain applications utilized in supply chain management?**
   Blockchain applications in supply chain management provide transparency, traceability, and efficiency by recording the movement of goods and verifying transactions across the supply chain.

8. **What role does blockchain technology play in logistics?**
   Blockchain technology in logistics improves transparency, reduces fraud, and streamlines processes by securely tracking the movement of goods, verifying ownership, and automating payments.

9. **How are smart cities utilizing blockchain technology?**
   Smart cities use blockchain technology for secure data sharing, digital identity management, efficient energy distribution, and transparent governance.

10. **What are some examples of blockchain applications in finance and banking?**
    Blockchain applications in finance and banking include cross-border payments, trade finance, digital asset management, and decentralized finance (DeFi) platforms.

11. **How does blockchain technology improve transparency and security in insurance?**
    Blockchain technology improves transparency and security in insurance by providing immutable records of policies, claims, and transactions, reducing fraud, and streamlining processes.

12. **What is a case study of blockchain application in supply chain management?**
    One example is IBM's Food Trust platform, which uses blockchain technology to track the provenance and authenticity of food products from farm to table, ensuring food safety and quality.

13. **How does Truffle simplify the development process of smart contracts?**
    Truffle provides a suite of tools and libraries for developing, testing, and deploying smart contracts, including a development environment, testing framework, and asset pipeline, which streamlines the development process.

14. **What are the advantages of DApps over traditional centralized applications?**
    DApps offer greater transparency, security, and censorship resistance compared to traditional centralized applications. They also enable peer-to-peer transactions without intermediaries.

15. **How are NFTs revolutionizing digital ownership and art markets?**
    NFTs enable creators to tokenize and sell unique digital assets, such as art, music, and collectibles, providing proof of ownership and authenticity on the blockchain.

16. **What challenges do blockchain applications face in supply chain management?**
    Challenges include interoperability between different blockchain networks, scalability for handling large volumes of transactions, and integration with existing legacy systems.

17. **How can blockchain technology enhance data privacy and security in smart cities?**
    Blockchain technology can enhance data privacy and security by providing encrypted, tamper-proof records of data transactions and enabling decentralized identity management systems.

18. **How can blockchain technology improve the efficiency of claims processing in insurance?**
    Blockchain technology can automate and streamline claims processing by providing transparent, immutable records of policyholder information, claims history, and transactions, reducing fraud and administrative overhead.

19. **What factors should be considered when designing and implementing blockchain applications in finance and banking?**

Factors include regulatory compliance, scalability, interoperability, security, and user experience. It's essential to consider the specific needs of users and stakeholders and ensure alignment with industry standards and best practices.

20. What are some examples of blockchain applications in trade finance?

Answer: Examples include platforms like TradeLens, which use blockchain technology to digitize and automate trade documentation, reducing paperwork and streamlining the trade finance process.

PART B

1. Discuss the features of Truffle for application development life cycle management. (Nov/Dec 2023)
2. Discuss any two real-world applications of blockchain and mention how block chain solves the traditional problems? (Nov/Dec 2023)
3. Describe the process of designing and deploying a smart contract using Truffle. Include the steps involved and the tools provided by Truffle to facilitate smart contract development.
4. Explain the concept of decentralized applications (DApps) and provide examples of how they differ from traditional centralized applications. Discuss the advantages and challenges associated with developing and using DApps.
5. Describe the key components of a Non-Fungible Token (NFT) and how they are used to represent unique digital assets on the blockchain. Provide examples of popular NFT use cases and their impact on various industries.
6. Discuss the role of blockchain technology in revolutionizing supply chain management. Explain how blockchain enhances transparency, traceability, and efficiency in the movement of goods across the supply chain.
7. Explore the potential applications of blockchain technology in logistics and transportation. Provide examples of how blockchain can improve transparency, reduce costs, and streamline processes in the logistics industry.
8. Describe the concept of a smart city and explain how blockchain technology can contribute to building smarter and more sustainable urban environments. Discuss specific use cases and benefits of integrating blockchain in smart city initiatives.
9. Discuss the challenges and opportunities of implementing blockchain applications in the finance and banking sector. Explore the potential impact of blockchain on traditional financial services and the factors influencing adoption in the industry.
10. Explain how blockchain technology can enhance security and trust in insurance processes. Discuss specific use cases where blockchain is utilized to improve claims processing, fraud detection, and customer experience in the insurance sector.
11. Explore the concept of decentralized finance (DeFi) and its role in transforming traditional banking and financial services. Discuss the advantages and challenges of DeFi platforms and their potential impact on the global financial system.
12. Provide a case study of a real-world application of blockchain technology in one of the discussed sectors (supply chain management, logistics, smart cities, finance and banking, insurance). Describe the problem addressed, the implementation process, and the outcomes achieved through blockchain integration.