Vivekanand Education Society's Institute of Technology, Chembur, Mumbai,
Department Of Artificial Intelligence and Data Science
Year:2023-24 (Even Sem)
MID TERM TEST

Class : Third Year / Honor-Minor Degree	**Division: All Branches**
Semester: VI	**Subject: Blockchain Platforms**
Date: 1st March 2024	**Time: 12:30 to 1:30pm**

Q1 a. Enlist the characteristics of Blockchain

1. **Decentralization:** Blockchain operates on a peer-to-peer network, removing the need for a central authority or intermediary. Each participant in the network (node) has a copy of the entire ledger, promoting decentralization and reducing the risk of a single point of failure.
2. **Immutability:** Once data is recorded on the blockchain, it is extremely difficult to alter or delete. This is achieved through cryptographic hashing and the consensus mechanism, ensuring the integrity of the information stored on the blockchain.
3. **Transparency**: All participants in the blockchain network have access to the same data. Transactions are visible to all parties in the network, providing transparency and traceability of information.
4. **Security:** Blockchain uses cryptographic techniques to secure transactions and control access to the network. The decentralized nature of the network also makes it more resistant to hacking and fraud.
5. **Consensus Mechanism:** Blockchain relies on a consensus mechanism to agree on the ledger's state. Different blockchain networks use various consensus algorithms, such as Proof of Work (used in Bitcoin) or Proof of Stake, to validate and confirm transactions.
6. **Distributed Ledger:** The blockchain is a distributed ledger, meaning that copies of the entire ledger are maintained on multiple nodes across the network. This redundancy enhances reliability and fault tolerance.
7. **Anonymity and Privacy:** While transactions on the blockchain are transparent, participants can maintain a level of privacy. Users are represented by cryptographic addresses, and additional privacy features can be implemented in some blockchain platforms.

Q1 b. Enlist the components of Ethereum Platform

Component-1 : Nodes

1. **Mining Node** are responsible for writing all the transactions that have occurred in the Ethereum network in the block.
2. **Ethereum Virtual Machine Node –**
   These are the nodes in the Ethereum network in which Smart Contracts (it is a type of contract between supporter and developer in which there are a set of rules based on which both the parties agree to interact with each other. The agreement will be automatically executed when the pre-defined rules are met.) are implemented. By default, this node utilizes a 30303 port number for the purpose of communication among themselves.

Component-2 : Ether

- Ether is a type of cryptocurrency used in the Ethereum network just like a bitcoin is used in a blockchain network. It is a peer-to-peer currency, similar to Bitcoin. It tracks and promotes each transaction in the network.
- It is the second-largest cryptocurrency in the world.
- Ether is paid as a commission for any execution that affects the state of Ethereum.
- It is used in the Ethereum algorithm as an incentive for miners who connect blocks to the blockchain using a proof-of-work method.

- It is the only currency that can be used to pay transaction costs, which go to miners as well. The block reward, as well as transaction fees, provide miners with an opportunity to keep the blockchain rising.
- Aside from paying for transactions, ether is often used to purchase gas, which is used to pay for the computation of any transaction on the Ethereum network.

Component-3 : Gas

- Gas is an internal currency of the Ethereum network. We need gas to run applications on the Ethereum network, much as we need gas to run a vehicle.
- To complete every transaction on the Ethereum network, a consumer must first make a payment—send out ethers—and the intermediate monetary value is known as gas.
- Gas is a unit of measurement on the Ethereum network for the computing power used to execute a smart contract or a transaction.
- The price of gas is very low compared to Ether. The execution and resource utilization costs are predetermined in Ethereum in terms of Gas units, called gwei.

Component-4 : Ethereum Accounts

There are two types of Ethereum accounts. They are as follows.

1. Externally owned accounts (EOA) are used to store transactions.
2. Contract accounts store the details of Smart Contracts.

Component-5 : Nonce

For externally owned accounts, nonce means the number of transactions via this account. For a contract account, nonce means the number of contracts generated via this account.

Component-6 : Storage Root

It is the main root node of a Merkle tree. Hash of all details of the account is stored here. The root of the Merkle tree is the verification of all transactions.

Component-7 : Algorithm Used

- Ethash

  The intended PoW algorithm for Ethereum 1.0 is Ethash. It's the most recent version of Dagger-Hashimoto, however, it's no longer proper to call it that because many of the algorithms' initial characteristics have been dramatically altered in the previous month of study and development. Since ethereum transitioned to Proof of Stake (PoS) in 2022, ethash has become legacy and the PoS Algorithm used is – "Clique".

Component-8 : Execution Client

These are core components that act as the heart of ethereum, and facilitates transaction processing, maintaining state, and ensuring every node is following the consensus rules. Here are key responsibilities :-

- Handling the transactions sent to the ethereum network.
- Keeping track of current state of the blockchain, syncing with the overall networks that involves account balances, smart contract execution and block information
- Validating blocks and ensuring they adhere to the ethereum network's agreed upon rules

Some examples are Geth, Nethermind, Besu etc.

Component-9 : Consensus Client

A consensus client is a software that implements the Proof-of-Stake Algorithm and helps the blockchain network ensure that all the nodes agree on the state of the blockchain. It has the following key responsibilities :-

- Transaction Validation : Ensuring that any transaction made over the ethereum network adhere to the rules and guidelines set
- Block Proposal: Block proposal is the process of organizing a set of valid transaction into groups and then broadcasting them to the ethereum network for proposal as including them in the network.

Q1 c. What is the role of a testnet in the deployment of a Public Blockchain.

- **Risk-Free Testing**: Testnets provide a risk-free environment for developers to experiment with new code, protocols, and features. Testing on the mainnet could lead to unintended consequences or issues that may impact users and their assets. Testnets allow developers to identify and resolve bugs, vulnerabilities, or other issues before deploying changes to the production environment.

- **Cost Savings:** Interacting with a testnet is usually free or requires minimal resources, as the testnet tokens used for transactions are typically obtained easily and have no real-world value. This allows developers to conduct extensive testing without incurring significant costs, as opposed to using real assets on the mainnet.
- **Rapid Prototyping:** Developers can quickly prototype and iterate on their blockchain-based applications and smart contracts on a testnet. This facilitates a faster development cycle, enabling teams to experiment, refine, and improve their projects before deploying them on the mainnet.
- **Community Involvement:** Testnets provide an opportunity for the community and stakeholders to participate in testing and provide feedback. This collaborative approach helps identify potential issues from different perspectives, ensuring a more robust and secure deployment when transitioning to the mainnet.
- **Simulating Real-World Conditions:** Testnets aim to replicate the conditions of the mainnet, allowing developers to simulate real-world scenarios and interactions. This includes testing for scalability, network congestion, and the performance of the blockchain under various conditions.
- **Upgrade Testing:** Before implementing changes or upgrades to the mainnet, developers can deploy and test new versions of the blockchain protocol on a testnet. This helps ensure a smooth transition, minimize disruptions, and maintain compatibility with existing applications and smart contracts.
- **Ecosystem Development:** Testnets are essential for building a vibrant blockchain ecosystem. Developers, users, and businesses can use testnets to explore and integrate with the blockchain platform, fostering innovation and the development of decentralized applications (DApps).
- **Educational and Training Purposes:** Testnets provide a valuable educational resource for developers, allowing them to gain hands-on experience with blockchain technology without the risk associated with real assets. This contributes to the overall skill development and understanding of blockchain concepts.

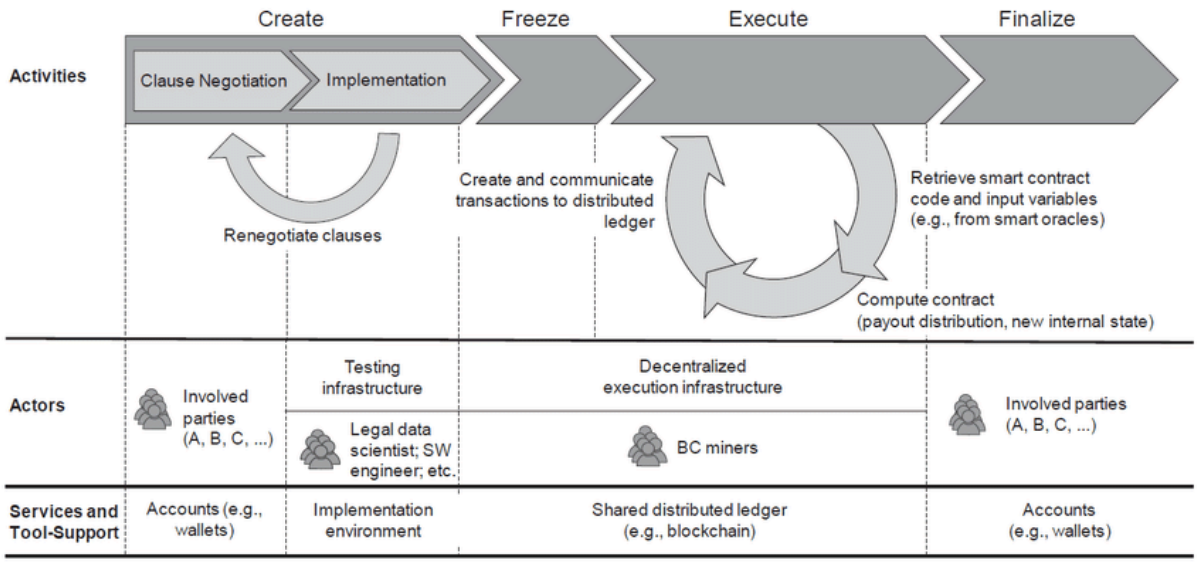
Q1 d. What are the features of Bitcoin Platform

- Decentralization Of Bitcoin's Network
- Censorship Resistant
- Hard Cap Of 21 Million Bitcoin
- Immutable
- Network Effects

Q1 e. Write down the steps involved in transferring Ethers from Metamask

1. Install MetaMask:
2. Create or Import a Wallet:
3. Switch to a Test Network:
4. Fund Your Test Wallet:
5. Start Developing and Testing:

Q1.f. Enlist the phases involved in the life cycle of a Smart Contract
Create, Freeze, Execute, Finalize



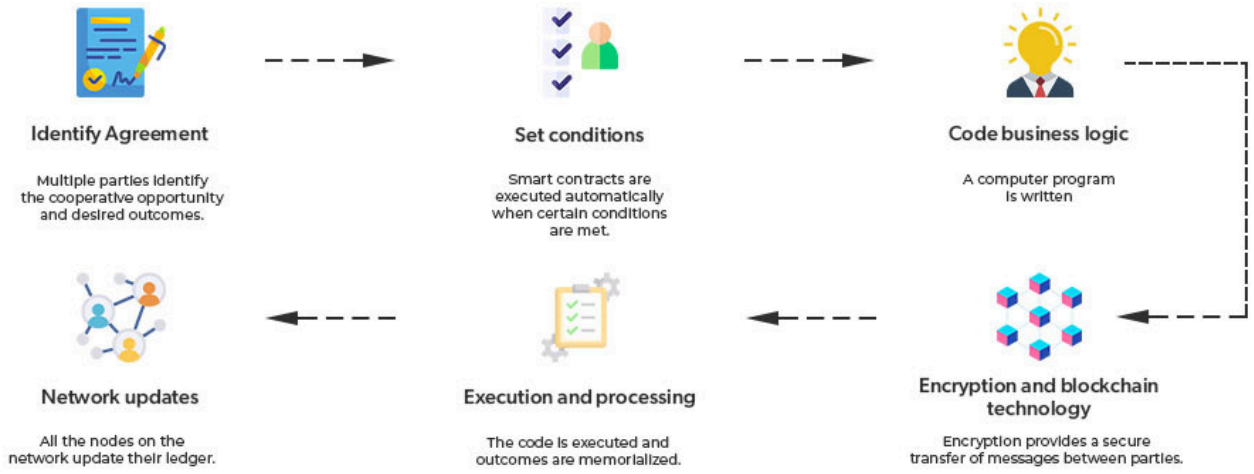
Q2 . a. Differentiate between Proof of Stake and Proof of Work based on parameters

Parameter	Proof of Work (PoW)	Proof of Stake (PoS)
Consensus Mechanism	Requires participants (miners) to solve computationally intensive puzzles to validate and add new blocks to the blockchain.	Validators are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they hold and are willing to "stake" as collateral.
Energy Consumption	High energy consumption due to the computational power needed for solving complex puzzles.	Generally, lower energy consumption as there is no need for extensive computational work. Validators are chosen in a more energy-efficient manner.
Security	PoW is considered highly secure due to the amount of computational work required to tamper with the blockchain.	PoS aims to provide security by making it economically irrational for validators to attack the network. The security is based on the economic stake of participants.
Centralization Tendency	Over time, PoW mining has tended towards centralization, as mining pools consolidate power.	PoS aims to mitigate centralization concerns by distributing power based on participants' stake, but challenges may arise if a few large stakeholders dominate.
Scalability Potential	PoW blockchains can face scalability challenges, especially with increased transaction volume. Solutions like layer 2 scaling are explored.	PoS blockchains often have better scalability potential due to the absence of energy-intensive mining, allowing for faster and more energy-efficient block production.

Q2b. Differentiate between Public, Private, Hybrid, and Consortium Blockchain Platforms

Parameter	Public Blockchain	Private Blockchain	Hybrid Blockchain	Consortium Blockchain
Accessibility	Open to the public; anyone can participate, view, and validate transactions.	Restricted access; permissioned network where participants are known and vetted.	Combination of public and private; certain aspects are public, while others are private.	Permissioned; limited to a predefined group of organizations or entities.
Decentralization	Highly decentralized; no single entity has control; operated by a distributed network of nodes.	Centralized or semi-decentralized; control is often held by a single organization or a consortium of known entities.	Variable; can lean towards decentralization for public-facing aspects but may be more centralized for private elements.	Controlled decentralization; predefined entities participate in consensus and validation.
Consensus Mechanism	Typically uses Proof of Work (PoW) or Proof of Stake (PoS) consensus mechanisms.	Various consensus mechanisms, including Practical Byzantine Fault Tolerance (PBFT) or Raft, depending on the design.	Depends on the design; may use a combination of PoW, PoS, or other consensus mechanisms.	Depends on the specific requirements; can use various consensus mechanisms agreed upon by consortium members.
Privacy and Permissions	Limited privacy; all transaction details are publicly accessible and transparent.	High privacy; transactions are typically visible only to participants with the necessary permissions.	Variable privacy; public aspects may lack privacy, while private elements are restricted.	Privacy depends on the design and agreements among consortium members; typically offers more privacy than public blockchains.
Use Cases	Suited for open, decentralized applications, cryptocurrency, and public ledger purposes.	Ideal for business applications, especially those where privacy and control are crucial, such as supply chain or internal processes.	Useful for applications requiring a combination of public and private features, like supply chain visibility with confidential transactions.	Commonly used for collaborative efforts between multiple organizations, like in financial or industry consortiums.

Q3. a. With the help of a neat diagram, explain the workings of a Smart Contract.



1. Identify Agreement: Multiple parties identify the cooperative opportunity and desired outcomes and agreements could include business processes, asset swaps, etc.
2. Set conditions: Smart contracts could be initiated by parties themselves or when certain conditions are met like financial market indices, events like GPS locations, etc.
3. Code business logic: A computer program is written that will be executed automatically when the conditional parameters are met.
4. Encryption and blockchain technology: Encryption provides secure authentication and transfer of messages between parties relating to smart contracts.
5. Execution and processing: In blockchain iteration, whenever consensus is reached between the parties regarding authentication and verification then the code is executed and the outcomes are memorialized for compliance and verification.
6. Network updates: After smart contracts are executed, all the nodes on the network update their ledger to reflect the new state. Once the record is posted and verified on the blockchain network, it cannot be modified, it is in append mode only.

Q3. b. With the help of a neat diagram explain DApp Architecture.

1. User Interface (UI):
    - Represents the front-end or user-facing part of the DApp.
    - Developed using standard web technologies (HTML, CSS, JavaScript).
    - Interacts with the blockchain and smart contracts through a Web3.js library or similar.
2. Smart Contracts:
    - Self-executing contracts with predefined rules and conditions.
    - Deployed on the blockchain (Ethereum, Binance Smart Chain, etc.).
    - Written in a blockchain-specific programming language (e.g., Solidity for Ethereum).
3. Blockchain:
    - Distributed ledger that stores the state of the DApp.
    - Ensures security, immutability, and transparency.
    - Utilizes consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS).
4. Decentralized Storage:
    - Used to store large datasets, files, or other information in a decentralized manner.
    - Examples include InterPlanetary File System (IPFS) or decentralized storage solutions.
5. Smart Contract Interactions:
    - User interactions with the DApp trigger transactions and function calls to smart contracts.
    - These interactions are facilitated by the DApp's UI, interacting with the blockchain via a Web3.js library.
6. Web3.js (or similar library):
    - JavaScript library that enables the communication between the DApp's front-end and the blockchain.

- Allows the DApp to read from and write to the blockchain, interact with smart contracts, and manage user accounts.

7. Decentralized Identity (Optional):
   - Provides users with decentralized identity solutions.
   - Enables users to control their identity without reliance on a central authority.
   - Examples include blockchain-based identity solutions or decentralized identifiers (DIDs).