DEPARTMENT OF INFORMATION TECHNOLOGY

SUB: U20IT514 BLOCK CHAIN TECHNIQUES

YEAR/SEM:III/V

Unit-1

1. What is the underlying principle of Blockchain Technology?

Blockchain is a P2P network where no single user controls the transaction. Blockchain principles are as follows:

- **Decentralization:** The power is distributed among all the users in the network, this means no single user can hack, manipulate, or close the chain of blocks or can shut it down. Due to the decentralized mechanism, the blockchain is free from hacks.
- **Integrity:** In the blockchain, all the users have got the right to make the decision, and the trust in the system is not forced but is guided by the user intuition.
- **Cryptography:** Blockchain uses cryptography to ensure security and data integrity. Blockchain enables the information to be transmitted without being copied.
- **Security:** Blockchain uses Public Key Encryption Mechanism, due to this the transactions over the network are highly secure unless the public key is shared, in that case, there exists no solution for the protection or security.

2. Why Blockchain is a trusted approach?

Blockchain Technology is a trusted approach due to the following reasons:

1. Due to its open-source nature, blockchain technology is compatible with many business applications.
2. It provides secure transactions by using the Public Key Encryption mechanism.
3. It provides equal opportunities to every person without any discrimination in the global economy.
4. It is a decentralized network due to which the power is distributed among all the participants in the network. There is no single authority in the network.

3. Name two types of records in the blockchain databases?

The two records are block records and transactional records. These records can be easily accessed and can be integrated easily without following any complex algorithm.

4. Differentiate between Blockchain and Hyperledger.

S.No.	Blockchain	Hyperledger
1.	A public and private blockchain can be built.	Only a private blockchain can be built.
2.	It is divided into public, private, and consortium blockchain.	It is private blockchain technology.
3.	It can be used in multiple fields like business, government, healthcare, etc.	It is primarily used for enterprise-based solutions.

S.No.	Blockchain	Hyperledger
4.	There are many projects which utilize blockchain: • Bitcoin • Ethereum • Hyperledger, etc.	Hyperledger has several implementations from different vendors: • Fabric from IBM • Sawtooth Lake from Intel. • Corda from R3 consortium.

5. How can you identify a block?

Every block in blockchain consists of these four fields:

- **Hash value:** The hash value of the previous block, and this acts as a pointer to the previous block.
- **Transactional data:** The block consists of details of the transactions.
- **Nonce:** It is a random value that is used to vary the value of the hash in order to generate a hash value less than the target.
- **Hash of the block:** This is the digital signature of the block and an alphanumeric value that is used to identify a block.

6. What is a Genesis Block?

In 2009, a developer named Santoshi Nakamoto created the genesis block. The genesis block is the first block in the blockchain and is also referred to as block 0. Some features of this block are as follows:

- It is the only block that does not refer to any previous block.
- It defines parameters of blockchain such as level of difficulty, consensus mechanism, etc to mine the blocks.

The genesis block forms the foundation of the Bitcoin trading system, and it is the prototype for all other blocks in the blockchain.

7. List some cryptographic algorithms used in blockchain.

Here are some extensively used cryptographic algorithms

- SHA-256
- Ethash
- Triple DES
- RSA

  Blowfish

8. How hash value is generated in blockchain?

The steps involved in generating the hash value or block signature is as follows:

- Transaction details are passed through the one-way hash function SHA-256.
- The output value is then passed through the signature algorithm like ECDSA with the user's private key.
- The encrypted hash along with other information is called the digital signature.

9. Is it possible to modify the data written in the block?

No, it is not possible to modify the data in one particular block. If the need arises, the organization has to erase data from all the other blocks. Due to this reason, it is very important to deal with data with utmost care in the blockchain.

10. What is a method to recognize a block in the blockchain approach?

Every block has a hash pointer that acts as a link to the previous block, transaction data, and a stamp of time.

11. What do you mean by blocks in Blockchain?

A blockchain consists of a list of records that are stored in the blocks. Each time a block gets completed a new block is generated and that block is linked to the previous block. The

blocks linked to each other are known as Blockchain i.e. the chain of blocks. It is not possible to delete or reverse any block from the blockchain.

12. A block in a blockchain consists of which elements?

A block in a blockchain consists of these elements-

- A hash pointer to the previous block.
- A list of transactions.
- Timestamp.

13. What is the difference between public and private keys?

S. No.	Public key	Private Key
1.	It is used for identification.	It is used for encryption and authentication purposes.
2.	The sender can send a message in the blockchain network using the public key of the receiver.	The receiver can decrypt the message the received message in the blockchain network using the private key.
3.	It is free to use and publicly available.	It is kept secret and is not available publicly.

14. Is it possible to remove a complete block from a blockchain network?

Yes, it is possible to remove a complete block from the network. There are some default options and filters that can be helpful in scenarios where only a specific portion of the online ledger is to be considered.

15. List some applications of smart contracts.

Smart Contracts are lines of code in blockchain that are executed automatically. They define the rules of how a transaction has to be processed between the parties under specific conditions. Some applications are:

- **Insurance:** Smart contracts can be useful in preventing forgeries and identifying false claims.
- **Employee contract:** They can be useful in helping with wage payments.
- **Transportation:** Smart contracts can be used to track down the shipment of goods.

16. Where do nodes run a smart contract?

Nodes run the smart contract on an Ethereum Virtual Machine (EVM). EVM operates in a sandboxed environment that is a perfect environment for Ethereum-based smart contracts.

17. What is the first thing specified in the Solidity file?

The first line specifies the version number of Solidity as it eliminates incompatibility issues that can arise while comparing with another version. It is important to mention the correct version number for the code.

18. What do you mean by Nonce? How it is used in Mining?

Mining is a process to solve a mathematical puzzle called proof of work. Proof of work is the process to determine the number Nonce. It is a random value that is used to vary the value of the hash so that the final hash value meets the hash conditions.

19. List the steps in Blockchain project implementation.

- Requirement Identification.
- Planning.
- Development of project.
- Feasibility study on the security of the project.
- Implementation.

- Controlling and Monitoring the project.

20. Are there any network-specific conditions for using Blockchain technology in an organization?

There is no specific network condition, but the network must be a peer-to-peer network under the concerned protocols.

Unit-2

1. List some differences between Blockchain and Baking Ledgers.

- One of the most striking differences between Blockchain and Banking Ledgers is that blockchain is decentralized, distributed, and open-source. This means that the people don't have to rely on the central bank to keep track of all the transactions. In a peer-to-peer network in blockchain technology, it is possible to keep track of all the transactions without having the fear of having them lost or erased.
- Due to the open-source nature of blockchain, it is more versatile and easy to program. The programmers can easily add new functionality on top of already existing software through consensus.

2. What do you mean by executive accounting? Does blockchain support the same?

Executive accounting typically focuses on corporate accounting rather than public accounting. This means that executive accounting oversees finances for a business rather than focusing on individuals. Blockchain Technology has some algorithms that are specially designed to handle executive accounting.

3. What do you mean by secret sharing? Does it have any benefit in Blockchain technology?

Secret sharing is the method of distributing the secret among a group of participants in the blockchain network. All participants are allocated a share of the secret. The individual shares have no meaning of their own. The secret can be reconstructed only when a sufficient number of different types of shares are combined. There are many security-related benefits that secret sharing offers in blockchain technology.

4. What is an off-chain transaction?

Off-chain transactions are the transactions occurring on the cryptocurrency network that moves value outside the network. Due to the low cost/ zero cost of these transactions, off-chain transactions are becoming popular among a large set of participants. These transactions have the following features:

- Off-chain transactions may eventually have to be recorded on-chain.
- These transactions can entail lower fees, immediate settlement, and greater anonymity than on-chain transactions.
- These transactions work by swapping the private keys to an existing wallet instead of transferring funds.

5. List and explain the parts of EVM Memory.

The EVM memory can be divided into three parts:

- **Storage:** It is extremely expensive and the storage values are stored permanently on the blockchain network.
- **Memory:** It is temporary modifiable storage that can be accessed only during the contract execution. Once the contract execution is finished, all the data is lost.
- **Stack:** It is temporary non-modifiable storage and the content is lost once the execution completes.

6. What happens if the cost of execution of the smart contract is more than the specified gas?

Initially, the transaction will get executed but if the execution of the smart contract costs more than the specified gas, then the miners will stop validating the contract and the blockchain will record the transaction as failed. The user will also not get a refund in this case.

7. What are function modifiers in Solidity and mention the most widely used modifiers.

Function modifiers are used to modify the behavior of the smart contract functions. The most commonly used function modifiers in solidity are:

- **View:** These are read-only functions. They cannot modify the state of a smart contract.
- **Pure:** These functions neither read nor write the state of the smart contract.

8. What do you mean by forks? What are the different types of forking?

Forking is the updating of cryptocurrency protocol or code. It happens when the participants of the network cannot agree with regard to the consensus algorithm and new rules to validate the transactions. Thus, blockchain splits into two branches. There are three types of forking:

- **Soft Fork:** When the blockchain protocol is altered in a backward-compatible way.
- **Hard Fork:** When the blockchain protocol is altered in a non-backward-compatible way.
- **Temporary Fork:** When two miners mine a new block at the same time.

9. On what factors does the gas usage in a transaction depends upon? How is the transaction fee calculated?

Gas usage in a transaction depends on the following criteria:

- Amount of storage.
- Set of instructions used in the smart contract.

The transaction fee is calculated in Ether using the formula:

Ether = Tx Fees = Gas Limit * Gas Price

10. In what order are the blocks linked in the blockchain?

In the blockchain, each block is linked with the previous block as each block consists of a pointer to the previous block. This means that the blocks are linked in the backward order.

11. Which cryptographic algorithm is used in blockchain?

Blockchain uses SHS-256 cryptographic algorithm. This hashing algorithm was developed by National Security Agency (NSA) in 2001.

12. What type of records can be kept in the blockchain?

Blockchain can be used to store any form of data. Industries can make use of this feature and can use blockchain to their advantage. The most common types of records that can be stored in the blockchain are as follows:

- Medical records.
- Management activities.
- Transaction processing.
- Business transactions, etc.

13. How is DApp different from a Normal App?

DApp runs on a decentralized network whereas apps are not generally designed to run in a decentralized ecosystem. DApps are the next-generation applications that are designed to take advantage of Blockchain Technology. Popular blockchain solutions that support DApp are Ethereum, NEO.

14. Is it possible to hack a blockchain network?

Blockchain is a fairly secure network, but it is not completely secure. There are many types of hacks that can be carried out by hackers in a blockchain network. These include:

- Sybil attack.
- Direct denial of service.
- Routing attack.
- 51% attack.

15. What is MetaMask?

MetaMask is a type of Ethereum wallet that bridges the gap between the user interfaces for Ethereum (For Example, Mist browsers, DApps, etc.) and the regular web (For Example, Google Chrome, Mozilla Firefox, Websites, etc.). Its function is to inject a JavaScript library called web3.js into the namespace of each page the browser loads. It is mainly used as a plugin in the regular web (For Example, Google Chrome, Mozilla Firefox, etc.)

16. What is the Lightning Network?
Lightning Network is an off-chain layer 2 payment protocol designed to be layered on top of blockchain-based cryptocurrencies such as litecoin or bitcoin. The lightning network is in the active development phase and is already being used by many vendors.

17. What is Atomic Swap?
Atomic swap is a revolutionary smart contract technology that allows exchanging one cryptocurrency to another without any intermediary exchange. It is done between two blockchains and off-chain.

18. How blockchain is useful to Digital Protection?
Blockchain is a solution that can help data-sensitive information to be protected. This means that blockchain can be useful to cybersecurity and digital protection. Other features of blockchain that will be helpful in these areas will be transparency, integrity, decentralized approach ad the use of cryptography in the blockchain technology also protects data.

19. How to check if a block is a valid block?
When a new block is announced on the network, every node that receives it does a list of checks. The two most important checks are:

- **Proof of work:** To check if a block provides enough work to be included in the chain.
- **Validity of all the transactions:** Each transaction must be a valid transaction.

20. How are the blocks and transactions encrypted in a bitcoin implementation?
Every block in a bitcoin implementation is a public block, so the blocks are not encrypted in any way. Block content is processed using a special hash function, SHA-256 to prevent modification and guarantee data integrity. This block hash value is included in the blockchain.

Unit-3

1. Why a blockchain needs a token to operate?
Coins/ tokens are used to implement changes between the states. When a transaction is done, there is a change of state and the coins are moved from one address to another. Technically, a blockchain does not need coins for its essential operations but without them, there is a need to introduce some other way to manage the states of the chain and to verify the transactions.

2. What is the function, and why is it needed in the blockchain?
Trapdoor functions are essential for public-key encryption. These are the functions that are easy to compute in one direction but difficult to compute in the opposite direction unless there is special information available to conduct the opposite process. These are commonly used in the blockchain to represent the ideas of addresses and private keys.

3. List a few types of Ethereum Networks?
There are three types of networks in Ethereum:

- **Live Network:** This is the main network. Smart contracts are deployed on the main network.
- **Test Network:** Some examples of the Test Network are Rinkeby, Kovan, Ropsten. These networks allow users to run their smart contracts with no fees before deploying on the main network.

- **Private Network:** They run within the premises of the organization, but they carry the features of the Ethereum network. These are not connected to the main network.

4. What are the limitations of the blockchain?

There are some limitations of the blockchain:

- Scalability is an Issue in the blockchain. This means the more people or nodes join the network, the more chances of slowing down are more.
- Blockchain is not a distributed computing system where the network does not depend on the involvement and participation of the nodes.
- Some blockchain solutions consume too much energy. Every time a ledger is updated with a new transaction, the miners need to solve the problems which means spending a lot of energy. The high energy consumption makes these mathematical problems not so ideal for the real world.
- Data is immutable in the blockchain. Once data is written, it cannot be removed
- Blockchains are sometimes inefficient. Even if the blockchain technology used in bitcoin is picked, you will find a lot of inefficiencies in the system.

5. What do businesses get from using the blockchain?

Businesses/Corporate Sectors can make a lot of benefits from the use of blockchain. They are:

- Audibility.
- Transparency.
- Feedback.
- Traceability.
- Security.
- Efficiency.

6. What is a block identifier?

Every block in a blockchain network has a hash value and this hash value acts as a unique identifier. This means that no two blocks will have the same identifier i.e. no two blocks will have the same hash value.

7. How can you stop double-spending?

Double spending is prevented using the consensus algorithm. The consensus algorithm ensures that the requested transaction is genuine and records it in the block. It is thus verified by the multiple nodes thus making double-spending not possible.

8. What do you mean by fungible tokens?

Any fungible entity refers to its capability for interchangeability with another asset or good of the same value. The most common examples are currency and money.

9. What do you mean by Non-fungible tokens?

Non-fungible tokens are different from cryptocurrencies as they do not have any inherent value. NFT derives its values from the assets or goods represented by them.

10. What is DeFi technology?

Decentralized Finance can be defined as financial services using smart contracts that use decentralized, distributed ledger technology. Thus, it doesn’t need any central authority and blockchain.

11. How do Bitcoins being digged?

Digging **Bitcoin** is a process of creating or molding electronic types, made by decentralized networks of independent individuals or large groups with the intention to create multiple currencies and to validate the delivery. cash flow flow.

12.How Blockchain works ?

Blockchain is like internet, an electronic system where you can set up applications on it. When conducting a transaction, an individual or organization usually adopts an intermediary such as a bank to ensure credibility.

13.Define merkle tree

In block chain merkle tree stores all the transaction in a block by producing a digital finger print of the entire set of transactions

14.What Does Mining Mean?

Mining, in the context of blockchain technology, is the process of adding transactions to the large distributed public ledger of existing transactions, known as the blockchain. The term is best known for its association with bitcoin, though other technologies using the blockcahin employ mining.

15What is role of miner in blockchain?

Miners work the blockchain mining process to confirm whether the transaction is authentic or not. All confirmed transactions are then included in the blockchain.

16. What is Bitcoin Mining?

Bitcoin mining is the process by which new bitcoins are entered into circulation. It is also the way the network confirms new transactions and is a critical component of the blockchain ledger's maintenance and development. "Mining" is performed using sophisticated hardware that solves an extremely complex computational math problem.

17.Why Bitcoin Needs Miners?

Blockchain "mining" is a metaphor for the computational work that nodes in the network undertake in hopes of earning new tokens. In reality, miners are essentially getting paid for their work as auditors.

18.What is permissioned model?

A permissioned blockchain requires user approval to join and is generally used for enterprise purposes, whereas a permissionless blockchain is used for public purposes that require less transparency and control.

19 Define pros & cons of permissioned block chain

It can be easily customized with various configurations and as per the needs. Users can have hybrid integrations or modular components.

Since the access is limited, few modes handle the transactions which increase the performance and scalability.

Cons

Since it has limited or few participants, it has more chances of collusion and corruption of data.

Getting a consensus in this model is not easy as rules of consensus can be changed by the operator at any time.

20.Which consensus algorithm does Permissioned blockchain use?

The practical byzantine fault tolerance algorithm (PBFT) is used to build consensus in blockchain solutions.