SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

AN AUTONOMOUS INSTITUTION

Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai

INTERNAL ASSESSMENT EXAMINATION – I
Seventh Semester
B. E., Mechanical Engineering
(Common to Mechanical and Mechatronics Engineering (AM))

19OE201-BLOCKCHAIN TECHNOLOGY
(Open Elective)
Regulations 2019
PART A - (5 X 2 = 10 marks)

1. **List out the areas in which Blockchain are applied extensively.**
   Blockchain technology is currently applied extensively in areas like: finance (including cryptocurrency and smart contracts), supply chain management, healthcare (patient records and data security), identity verification, real estate, media and entertainment (copyright tracking), energy trading, voting systems, and the Internet of Things (IoT) for asset tracking

2. **Compare Public and Private Blockchain.**
   Public blockchain are completely transparent, meaning that anyone can view all transactions on the network. On the other hand, private blockchains are not transparent, meaning that only authorized participants can view transactions.

3. **What is Digital Signature**?
   A digital signature is a mathematical algorithm that verifies the authenticity of a digital document or message. It's a type of electronic signature that uses cryptography to create a unique virtual fingerprint for a person or entity.

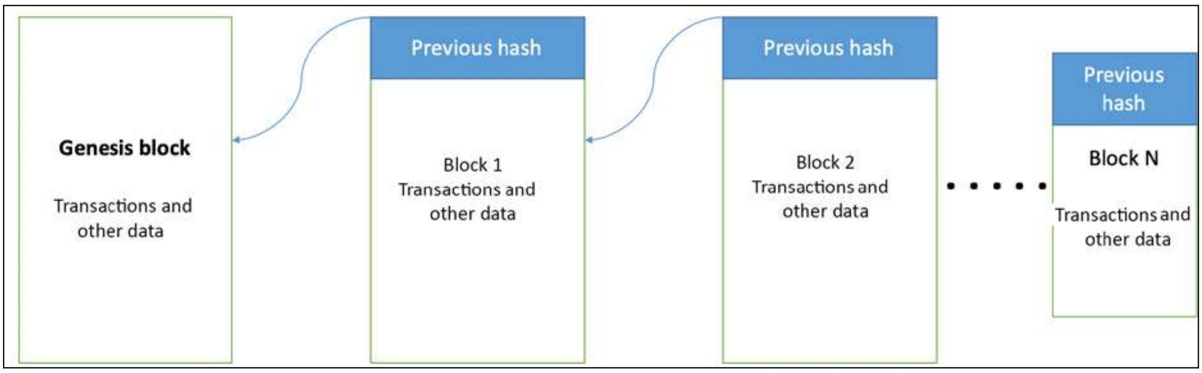
4. **Define Bitcoin**.
   Bitcoin (BTC) is a cryptocurrency (a virtual currency) designed to act as money and a form of payment outside the control of any one person, group, or entity. This removes the need for trusted third-party involvement (e.g., a mint or bank) in financial transactions.

5. **Outline the advantage of Cryptocurrency**.
   The advantages of cryptocurrencies include cheaper and faster money transfers and decentralized systems that do not collapse at a single point of failure. The disadvantages of cryptocurrencies include their price volatility, high energy consumption for mining activities, and use in criminal activities.

PART B - (2 X 13 = 26 marks)

6. (a) **Build Generic elements of a Blockchain system**

Generic elements of a blockchain


Genesis block
Transactions and other data
Previous hash
Block 1
Transactions and other data
Previous hash
Block 2
Transactions and other data
Previous hash
Block N
Transactions and other data

. These are the elements that youwill come across in relation to blockchain:

- **Address**: Addresses are unique identifiers used in a blockchain transaction to denote senders and recipients. An address is usually a public key or derived from a public key.
- **Transaction**: A transaction is the fundamental unit of a blockchain. A transaction represents a transfer of value from one address to another.
- **Block**: A block is composed of multiple transactions and other elements, such as the previous block hash (hash pointer), timestamp, and nonce. A block contains several elements, which we introduce as follows:
  - A reference to a previous block is also included in the block unless it is a genesis block. This reference is the hash of the header of the previous block. A **genesis block** is the first block in the blockchain that is hardcoded at the time the blockchain was first started. The structure of a block is also dependent on the type and design of a blockchain.
  - A **nonce** is a number that is generated and used only once.
  - A **timestamp** is the creation time of the block.
- **Merkle root** is a hash of all of the nodes of a Merkle tree. In a blockchain block, it is the combined hash of the transactions in the block. Merkle trees are widely used to validate large data structures securely and efficiently.

6 (b) Identify various Blockchain types, Explain this

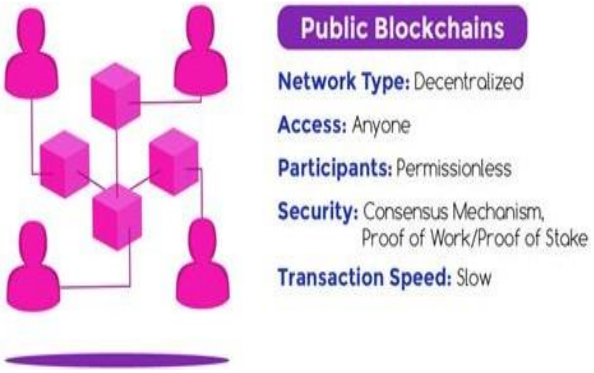
Public blockchains

- Public blockchains are open, decentralized networks of computers accessible to anyone wanting to request or validate a transaction (check for accuracy).
- Those (miners) who validate transactions receive rewards.
- Public blockchains use proof-of-work or proof-of-stake consensus.

- permission-less distributed ledger system.

- Anyone who has access to the internet can sign in on a blockchain platform to become an authorized node and be a part of the blockchain network.

- Example : Bitcoin and Ethereum (ETH) blockchains.



Public Blockchains

Network Type: Decentralized

Access: Anyone

Participants: Permissionless

Security: Consensus Mechanism,
Proof of Work/Proof of Stake

Transaction Speed: Slow

A public blockchain features:

- Write-only, immutable, transparent data storage.

- It brings trust among the whole community of users

- Decentralized, no need for intermediaries.

- Consistent state across all participants.

- Resistant against malicious participants.

- Anyone can join the public blockchain.

Disadvantages

- They suffer from a lack of transaction speed.

Private Blockchains

- A Private Blockchain is just like a relational database i.e. fully centralized and owned by a single organization.

- Private blockchains are not open, they have access restrictions.

- People who want to join require permission from the system administrator.

- They are typically governed by one entity, meaning they’re centralized.

- For example, Hyperledger is a private, permissioned blockchain.

Private Blockchains

Network Type: Partially Decentralized

Access: Single Organization

Participants: Permissioned

Security: Pre-approved participants,
Voting/Multi-party Consensus

Transaction Speed: Lighter and Faster

Consortium blockchain

- consensus is reached by a relatively small number of nodes in accordance to the governance scheme.
- Increased scalability - Bitcoin’s block transmits only up to 1 Mb* (from 1500 to 2700 transactions) per 10 minutes, when a consortium blockchain can optimize it to 1000 and more transactions per second.
- A consortium platform is more flexible.
- voting-based system, it ensures low latency and superb speed.

7. (a) Construct how bitcoin transactions are initiated?

1. A user/sender sends a transaction using wallet software or some other interface.

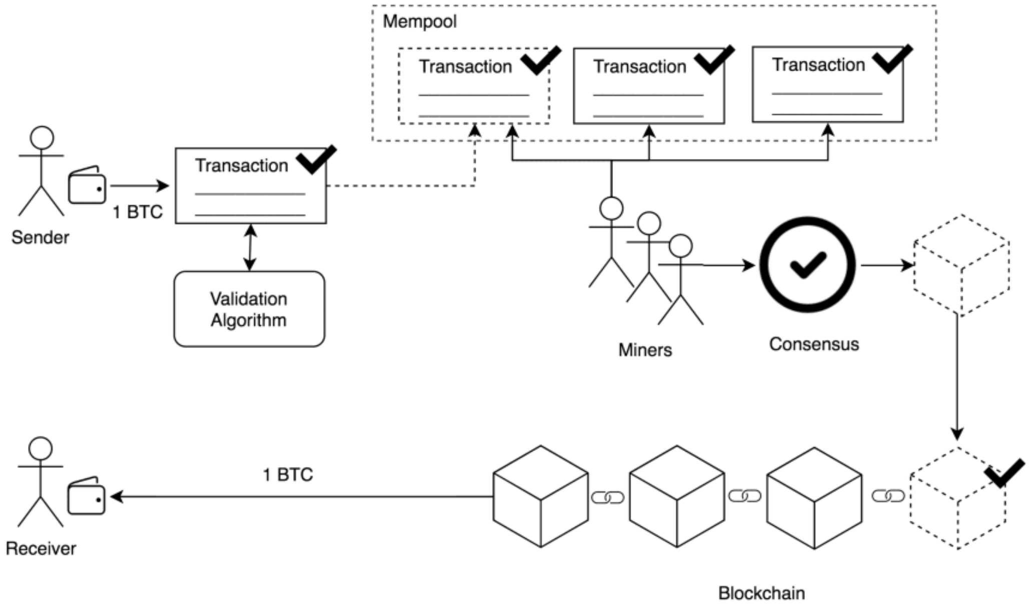
2. The wallet software signs the transaction using the sender's private key.

3. The transaction is broadcasted to the Bitcoin network using a flooding algorithm.

4. Mining nodes (miners) who are listening for the transactions verify and include this transaction in the next block to be mined. Just before the transactions are placed in the block, they are placed in a special memory buffer called the transaction pool. The purpose of the transaction pool is explained in the next section.

5. Next, the mining starts, which is the process through which the blockchain is secured and new coins are generated as a reward for the miners who spend appropriate computational resources. Once a miner solves the PoW problem, it broadcasts the newly mined block to the network. PoW is explained in detail in the *Mining* section. The nodes verify the block and propagate the block further, and confirmations start to generate.

6. Finally, the confirmations start to appear in the receiver's wallet and after approximately three confirmations, the transaction is considered finalized and confirmed.



7. (b) Experiment with various Bitcoin’s wallets types

Types of Blockchain Wallets

The following are the different types of blockchain wallets:

1. Hot Storage: Hot storage refers to the type of storage that is connected to the Internet. Hot storage, being connected to the Internet, allows the user easy and quick access to funds. It is helpful in daily transactions. But, it also has some disadvantages. It is more vulnerable to hacking and cybercrime. If the private key is lost then there is no longer access to coins. Also, if the private key is stolen by someone then it causes to loss of coins. The different types of hot storage wallets are **Online(Cloud), Desktop, and Mobile wallets**.

- **Online(Cloud) Wallets:** These types of wallets are the most convenient but at the same time, least secure. It is used to store private keys and transaction records online (on another server). This makes keys vulnerable to hacking as they are being stored by a third party. Online wallets should be used to store less amount of money that is going to be used for short-term storage i.e. daily transactions in exchange services. Examples: Exchanges like Bittrex or QuadrigaCX, and Online wallets like Coins.ph and GreenAddress.
- **Desktop Wallets:** Desktop wallets provide a better level of security than online wallets as they are downloaded and installed on a single computer. The funds related to an account

can only be accessed through that device which makes it a bit secure at the cost of convenience. However, it is also vulnerable to hacking if the computer gets compromised. Examples: Exodus, Multibit, Armory, and Bitcoin Core.

- **Mobile Wallets:** Mobile wallets are similar to desktop wallets in terms of providing better security than online wallets at the cost of convenience. However, it is a bit easier to use than desktop wallets as they are used by installing an app on a mobile phone which is smaller and simpler than desktop wallets. But, if the phone will damage then it will not be able to access funds, as in desktop wallets. Examples: Jaxx, BreadWallet, Mycelium, and CoPay.

2. Cold Storage: Cold storage refers to the type of storage that is not connected to the Internet. It is also known as offline storage. Cold storage provides a higher level of security than hot storage. It is useful for long-term storage, unlike hot wallets. However, a higher level of security is provided at the cost of convenience. It is not ideal for daily transactions. Although it is secure, it is vulnerable to external damage and loss. The different types of cold storage wallets are hardware wallets and paper wallets.

- **Hardware Wallets:** Hardware wallets are used to store coins/funds on a hardware device. The private keys are stored in an offline device, unlike hot wallets, but transactions do require an Internet connection to execute. It provides a higher level of security than hot wallets as they are stored offline in a physical device. However, the problem with these wallets is to trust the company from which buy the devices. It can log private keys and compromise accounts. Also, one should take extra care not to use second-hand hardware wallets. Examples: Ledger, Trezor, and KeepKey.
- **Paper Wallets:** Paper wallets provide the highest level of security than all the other types of wallets. The private keys are stored on paper and then kept in a secure location that is known only by the people that are trusted. Paper wallets are well protected against any type of hacking and malware. However, one thing to consider when using paper wallets is that paper can be worn out with time. If they are printed, the printer ink can leak in case of contact with water or increased temperature. Examples: BitAddress.org and Bitcoin Armory allows you to print your paper wallet.

3. Multi-signature wallet: Multi-signature wallets are those wallets that require more than one private key to execute a transaction.

8. (a) Analyze Decentralization in Blockchain system

Methods of Decentralization:

Two methods can be used to achieve decentralization: disintermediation and competition.

All you need is the address of your friend on the blockchain. This way, the intermediary (that is, the bank) is no longer required, and decentralization is achieved by disintermediation. It is debatable, however, how practical decentralization through disintermediation is in the financial sector due to the massive regulatory and compliance requirements. Nevertheless, this model can be used not only in finance but in many other industries as well, such as health, law, and the public sector. In the health industry, where patients, instead of relying on a trusted third party (such as the hospital record system) can be in full control of their own identity and their data that they can share directly with only those entities that they trust.

Contest-driven decentralization:

In the method involving **competition**, different service providers compete with each other in order to be selected for the provision of services by the system. This paradigm does not achieve complete decentralization. However, to a certain degree, it ensures that an intermediary or service provider is not monopolizing the service. In the context of blockchain technology, a system can be envisioned in which smart contracts can choose an external data provider from a large number of providers based on their reputation, previous score, reviews, and quality of service.

Routes to decentralization:

Compared to Bitcoin, Ethereum has become a more prominent choice because of the flexibility it allows for programming any business logic into the blockchain by using **smart contracts**.

The framework raises four questions whose answers provide a clear understanding of how a system can bedecentralized:

1. What is being decentralized?
2. What level of decentralization is required?
3. What blockchain is used?
4. What security mechanism is used?

Decentralization framework example:

The four questions discussed previously are used to evaluate the decentralization requirements of thisapplication. The answers to these questions are as follows:

1. Money transfer system
2. Disintermediation
3. Bitcoin
4. Atomicity

Full ecosystem of decentralization

The blockchain is a distributed ledger that runs on top of conventional systems.

These elements include storage,communication, and computation.

Data can be stored directly in a blockchain, and with this fact it achieves decentralization. A better alternative for storing data is to use **distributed hash tables** (**DHTs**). DHTs were used initially in peer-to-peer file sharing software, such as BitTorrent, Napster, Kazaa, and Gnutella.

Communication

The Internet (the communication layer in blockchain) is considered to be decentralized.

Computing power and decentralization:

Decentralization of computing or processing power is achieved by a blockchain technology such as Ethereum, where smart contracts with embedded business logic can run on the blockchain network.

8. (b) Distinguish various types of consensus algorithms in Blockchain

1. Proof of Work (PoW)

Developed by Satoshi Nakamoto, Proof of Work is the oldest consensus mechanism used in the Blockchain domain. It is also known as mining where the participating nodes are called miners.
In this mechanism, the miners have to solve complex mathematical puzzles using comprehensive computation power. They use different forms of mining methods, such as GPU mining, CPU mining, ASIC mining, and FPGA mining.
The Proof of Work mechanism is used by multiple cryptocurrencies like Bitcoin, Litecoin, ZCash, Primecoin, Monero, and Vertcoin to name a few.

2. Proof of Stake (PoS)

Proof of Stake is the most basic and environmentally-friendly alternative of PoW consensus protocol.

In this blockchain method, the block producers are not miners, but they act like validators. They get the opportunity to create a block over everyone which saves energy and reduces the time.

The two popular variations of Proof of Stake (PoS) are DPoS and LPoS.

- **Delegated Proof of Stake (DPoS)**

In the case of Delegated Proof of Stake (DPoS), the participants stake their coin and vote for a certain number of delegates such that the more they invest, the more weightage they receive. For example: if user A spends 10 coins for a delegate and user B invests 5 coins, A's vote gets more weightage than that of B.

The delegates also get rewarded in the form of transaction fees or a certain amount of coins.

- **Leased Proof of Stake (LPoS)**

LPoS is an enhanced version of PoS consensus mechanism that operates on the Waves platform.

Unlike the regular Proof-of-Stake method where each node with some amount of cryptocurrency is entitled to add the next blockchain, users can lease their balance to full nodes in this consensus algorithm blockchain.

3. Proof of Authority

Proof of Authority is a modified version of Proof of Stake in which the identities of validators in the network are at stake.

In this, to verify the validator's identity, the identity is the resemblance between validators' personal identification and their official documentation.

These validators put their reputation on the network.

In Proof of Authority, the nodes (that become validators) are the only ones allowed to produce new blocks.

4. Byzantine Fault Tolerance (BFT)

Byzantine Fault Tolerance, as the name suggests, is used to deal with Byzantine fault (also called Byzantine Generals Problem) – a situation where the system's actors have to agree on an effective strategy so as to circumvent catastrophic failure of the system, but some of them are dubious.

The two variations of the BFT consensus model that are prime in the Blockchain arena are PBFT and DBFT.

- **Practical Byzantine Fault Tolerance (PBFT)**

PBFT is a lightweight blockchain algorithm that solves the Byzantine General’s problems by letting users confirm the messages that have been delivered to them by performing a computation to evaluate the decision about the message’s validity.

The party then announces its decision to other nodes who ultimately process a decision over it. This way, the final decision relies upon the decisions retrieved from the other nodes.

Stellar, Ripple, and Hyperledger Fabric are some use cases of this blockchain consensus mechanism.

- **Delegated Byzantine Fault Tolerance (DBFT)**

Introduced by NEO, the Delegated Byzantine Fault Tolerance mechanism is similar to the DPoS consensus model. Here also, the NEO token holders get the opportunity to vote for the delegates.

The speaker creates a new block from the transaction that is waiting to be validated. Also, he sends a proposal to the voted delegates who have the responsibility to supervise all the transactions and record them on the network.

5. Direct Acyclic Graph (DAG)

Another basic yet prime blockchain consensus model that every mobile app development services company working with Blockchain must be familiar with is DAG.

In this type of Blockchain consensus protocol, every node itself prepares to become the ‘miners’.

Now, when miners are eradicated and transactions are validated by users itself, the associated fee reduces to zero. It becomes easier to validate transactions between any two closest nodes, which makes the whole process lightweight, faster, and secure. The two best examples of DAG algorithms are IOTA and Hedera Hashgraph.

6. Proof of Capacity (PoC)

In the Proof of Capacity (PoC) mechanism, solutions for every complex mathematical puzzle are accumulated in digital storages like Hard disks. Users can use these hard disks to produce blocks, in a way that those who are fastest in evaluating the solutions get better chances for creating blocks. The process it follows is called Plotting. The two cryptocurrencies that rely on PoC blockchain consensus protocol are Burstcoin and SpaceMint.