

SPPU-BE-COMP-CONTENT – KSKA Git

BCT UNIT 2 - PYQ Answers

Q3)

a) Explain consensus layer in Blockchain. [5]

Consensus Layer in Blockchain

The **Consensus Layer** is a fundamental component of blockchain technology that ensures all participants (nodes) in a decentralized network agree on a single version of the blockchain ledger, despite the absence of a central authority.

Key Functions:

1. **Agreement on Valid Transactions:**

The consensus layer defines how transactions are validated and agreed upon by the majority of nodes before being added to the blockchain. This prevents fraudulent or invalid transactions from being recorded.

2. **Maintaining Data Integrity and Consistency:**

It guarantees that all nodes maintain the same copy of the blockchain, ensuring data integrity and preventing double-spending or conflicting transactions.

3. **Fault Tolerance:**

The consensus mechanism allows the network to continue functioning correctly even if some nodes behave maliciously or fail, making the blockchain resilient and secure.

4. **Common Consensus Algorithms:**

- **Proof of Work (PoW):** Nodes solve complex puzzles to validate transactions, ensuring security but consuming high energy.
- **Proof of Stake (PoS):** Validators are chosen based on the amount of cryptocurrency they hold and are willing to “stake,” which is more energy-efficient.
- Other algorithms include Delegated PoS, Practical Byzantine Fault Tolerance (PBFT), and more.

5. **Decentralization and Trust:**

By enabling decentralized agreement, the consensus layer removes the need for a trusted third party and builds trust among participants through cryptographic proof and economic incentives.

SPPU-BE-COMP-CONTENT – KSKA Git

b) Discuss limitations of centralised systems. [5]

Centralized System Definition

A **centralized system** is a computing architecture where a single central server or authority controls all the data, operations, and management of the system.

Limitations of Centralized Systems

- **Single Point of Failure:**
In a centralized system, if the central server or authority fails or is attacked, the entire system can become unavailable, causing downtime and loss of data.
- **Scalability Issues:**
Centralized servers can become bottlenecks as the number of users or transactions increases, limiting the system's ability to scale efficiently.
- **Security Risks:**
Centralized systems are attractive targets for hackers because compromising the central server can give access to sensitive data or control over the entire system.
- **Lack of Transparency:**
Since control is held by a single entity, users have limited visibility into how data is managed or decisions are made, leading to potential distrust.
- **Data Privacy and Control:**
Users rely entirely on the central authority to protect their data, which can lead to misuse, unauthorized access, or censorship without users' consent.
- **High Maintenance Cost:**
Maintaining and securing a central server requires significant resources, including hardware, software, and skilled personnel, which can be costly.
- **Limited Fault Tolerance:**
The system depends heavily on the central authority's availability, so any failure or downtime directly affects the entire network, reducing overall reliability.

Due to these limitations, centralized systems often face challenges related to reliability, security, scalability, and user trust.

SPPU-BE-COMP-CONTENT – KSKA Git

c) Why Blockchain is important? [5]

Blockchain is a distributed and decentralized digital ledger technology that records transactions across many computers in such a way that the registered transactions cannot be altered retroactively without the consensus of the network.

Importance of Blockchain

1. **Decentralization:** Removes the need for a central authority, reducing the risk of single points of failure and censorship.
2. **Security:** Uses cryptographic techniques to secure data, making it tamper-proof and resistant to fraud.
3. **Transparency:** Transactions are recorded on a public or permissioned ledger, allowing participants to verify and audit data easily.
4. **Immutability:** Once recorded, transactions cannot be changed or deleted, ensuring data integrity.
5. **Efficiency:** Automates and speeds up processes by eliminating intermediaries, reducing costs and errors.
6. **Traceability:** Enables tracking of assets and products in supply chains, improving accountability and reducing fraud.
7. **Reduced Costs:** By cutting out intermediaries and automating verification, blockchain lowers operational costs.
8. **Improved Trust:** Provides a trustworthy environment where participants can confidently transact without knowing or trusting each other.
9. **Accessibility:** Enables financial inclusion by providing decentralized access to services for unbanked or underbanked populations.
10. **Innovation:** Supports smart contracts and decentralized applications (DApps), opening new possibilities across industries.

Blockchain is important because it offers a secure, transparent, and efficient framework that enhances trust, reduces costs, and enables innovative applications across various sectors, fundamentally transforming how data and transactions are managed.

Q4)

a) Explain propagation layer in blockchain [5]

The **Propagation Layer** in blockchain is responsible for **distributing and broadcasting data**—such as transactions and blocks—across the entire peer-to-peer network, ensuring all nodes receive and share the latest information quickly and reliably.

Functions of the Propagation Layer

1. **Transaction Broadcasting:** When a user creates a new transaction, the propagation layer broadcasts it to connected nodes so that it can be verified and eventually included in a block.
2. **Block Distribution:** Once a miner or validator creates a new block, the propagation layer disseminates this block to all nodes, so the blockchain remains synchronized.
3. **Efficient Data Sharing:** The propagation layer uses optimized communication protocols to reduce latency and bandwidth usage, ensuring data spreads fast without overwhelming the network.
4. **Data Validation Support:** It helps nodes receive new data quickly to start the validation and consensus process without delays.
5. **Network Synchronization:** By efficiently sharing updates, the propagation layer keeps the decentralized network synchronized and consistent.

The propagation layer is crucial in blockchain as it ensures timely and reliable distribution of transactions and blocks, maintaining network synchronization and enabling decentralized consensus.

... "उत्तर बरोबर आहे का माहित नाही, एकदा चेक करा."

b) Discuss evolution of Blockchain. [5]

The **evolution of blockchain** refers to the development and advancement of blockchain technology over time, starting from its origins to the diverse applications and improved versions we see today.

Evolution of Blockchain

1. **First Generation – Bitcoin (2008):**
Introduced by Satoshi Nakamoto, Bitcoin was the first blockchain designed as a decentralized digital currency using Proof of Work (PoW) consensus to enable peer-to-peer value transfer without intermediaries.

SPPU-BE-COMP-CONTENT – KSKA Git

2. **Second Generation – Smart Contracts (2013-2015):**

Ethereum introduced programmable smart contracts that allowed developers to build decentralized applications (DApps), expanding blockchain use beyond currency to automated agreements and business logic.

3. **Third Generation – Scalability and Interoperability:**

New blockchains like Cardano and Polkadot focused on solving problems of scalability, energy efficiency, and interoperability between different blockchain networks, enabling more practical and widespread use.

4. **Enterprise and Permissioned Blockchains:**

Organizations developed private and permissioned blockchains (e.g., Hyperledger Fabric) to address specific industry needs, offering controlled access, privacy, and compliance.

5. **Integration with Emerging Technologies:**

Blockchain is now evolving with AI, IoT, and DeFi (Decentralized Finance), enabling innovative applications such as secure IoT device management and decentralized financial services.

The evolution of blockchain reflects continuous innovation addressing earlier limitations, leading to broader adoption across industries and transforming how data and transactions are managed securely and transparently.

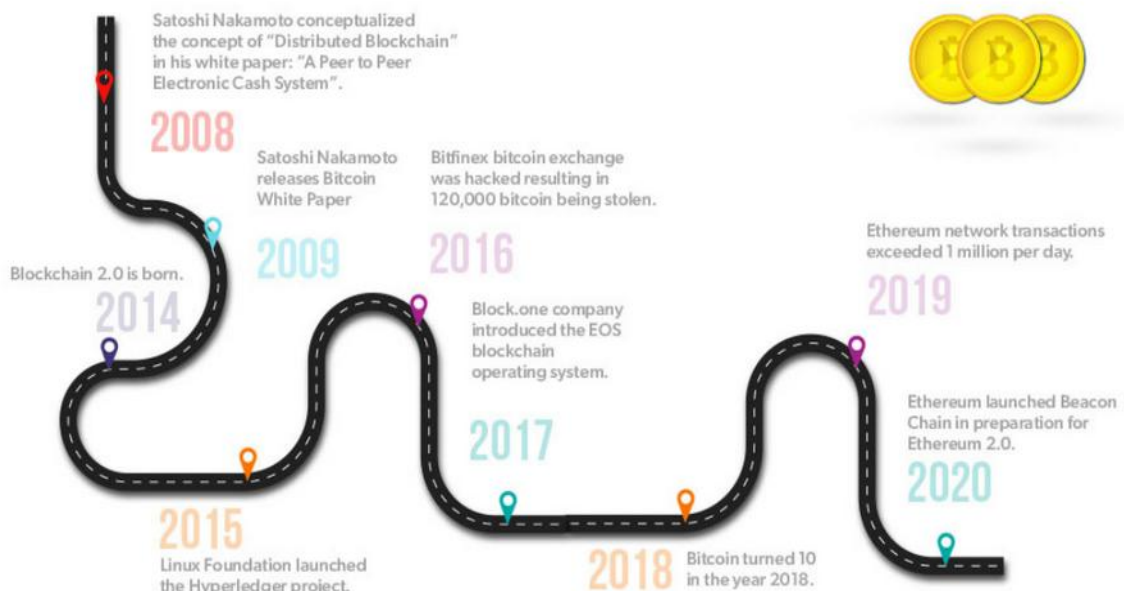


Diagram draw karychi ae trr kara , nhi trr naka karu !!

SPPU-BE-COMP-CONTENT – KSKA Git

c) Differentiate centralised & decentralised systems [5]

Difference between Centralization and Decentralization:

Basis	Centralization	Decentralization
Meaning	The concentration of authority at the top level is known as Centralization.	The evenly and systematic distribution of authority at all levels is known as Decentralization.
Delegation of authority	There is no delegation of authority as all the authority for taking decisions is vested in the hands of top-level management.	There is a systematic delegation of authority at all levels.
Suitability	It is suitable for small organisations.	It is suitable for large organisations.
Freedom of decision making	There is no freedom of decision-making at the middle and lower level.	There is freedom of decision-making at all levels of management.
Flow of Information	There is a vertical flow of information.	There is an open and free flow of information.
Employee Motivation	Employees are demotivated as compared to decentralization.	Employees are motivated as compared to centralization.
Conflict in Decision	There are least chances of any conflict in decision as only top-level management is involved.	There are chances of conflict in decision as many people are involved.
Burden	The burden of work is not shared and	The burden of work is shared

SPPU-BE-COMP-CONTENT – KSKA Git

Basis	Centralization	Decentralization
	only one group carries the burden.	amongst all levels.

➤ SEP 2023

Q3

a) Discuss various limitations of centralized system with respect to Decentralized system. [6]

Limitations of Centralized Systems Compared to Decentralized Systems

1. **Single Point of Failure:**

In centralized systems, all data and control depend on a central authority or server. If this central node fails or is attacked, the entire system can go down, causing disruption and loss of service.

In contrast, decentralized systems distribute data and control across many nodes, enhancing fault tolerance and availability.

2. **Scalability Issues:**

Centralized servers often become bottlenecks when user demand or data volume increases, limiting the system's ability to scale efficiently.

Decentralized systems can handle growth better by distributing workload across multiple nodes, improving performance and scalability.

3. **Security Vulnerabilities:**

Centralized systems are attractive targets for hackers because compromising the central server can grant access to all sensitive data or system control.

Decentralized systems reduce this risk by distributing data and requiring consensus among many nodes, making attacks more difficult and expensive.

4. **Lack of Transparency:**

Since a single authority controls centralized systems, users have limited visibility into how data is managed or decisions are made. Decentralized systems provide greater transparency because data is shared across many participants, often on public ledgers that anyone can audit.

5. **Data Privacy and Control:**

In centralized systems, users depend entirely on the central authority to protect their data, which may lead to misuse, unauthorized access, or censorship.

SPPU-BE-COMP-CONTENT – KSKA Git

Decentralized systems give users more control over their data by enabling direct peer-to-peer interactions and reducing reliance on intermediaries.

6. **Trust Dependency:**

Centralized systems require users to trust the central authority for fairness, security, and data integrity. Decentralized systems eliminate or reduce this dependency by using cryptographic proofs and consensus algorithms, allowing trustless transactions and interactions.

b) Write a note on Evolution of Block Chain. [4]

→ Already Done !

c) List and Explain algorithms of Consensus layer [5]

The **Consensus Layer** in blockchain ensures that all nodes in a decentralized network agree on a single version of the blockchain ledger. It validates transactions and maintains trust in a system without a central authority.

Consensus Algorithms in Blockchain

1. **Proof of Work (PoW):**

PoW requires nodes (miners) to solve complex mathematical puzzles using computational power. The first to solve the puzzle gets to add the new block and earn a reward. This method is secure but energy-intensive and is used by Bitcoin.

2. **Proof of Stake (PoS):**

Validators lock up some coins as a stake to participate in block validation. A validator is chosen to create the next block based on the amount staked, reducing energy consumption compared to PoW. Ethereum uses PoS.

3. **Delegated Proof of Stake (DPoS):**

Token holders delegate their voting power to a few trusted validators who produce blocks on their behalf. This improves efficiency and speed while maintaining decentralization.

4. **Practical Byzantine Fault Tolerance (PBFT):**

Nodes communicate through rounds of voting to agree on the blockchain state. PBFT is fast and suitable for permissioned blockchains with known participants.

5. **Proof of Burn (PoB):**

Validators “burn” (destroy) coins by sending them to an irretrievable address to earn mining privileges, showing long-term commitment. The more coins burned, the higher the chance to mine the next block.

6. **Proof of Capacity (PoC):**

Validators invest in hard drive space instead of computing power. More storage means a higher chance to create the next block.

SPPU-BE-COMP-CONTENT – KSKA Git

7. **Proof of Elapsed Time (PoET):**

Used mainly in permissioned blockchains, validators wait for a random time period. The one with the shortest wait time wins the right to create the next block, ensuring fairness.

Consensus algorithms are vital for blockchain networks as they enable secure, efficient, and fair agreement among distributed nodes, ensuring trust and reliability without central control.

Q4)

- a) Write a note on :
- i) Propagation layer
 - ii) Application layer

i) Propagation Layer

- Responsible for broadcasting transactions and blocks across the blockchain network, ensuring timely sharing of data.
- Uses efficient communication protocols to reduce latency and bandwidth usage, speeding up information flow.
- Helps keep all nodes synchronized with the latest blockchain state to maintain consistency across the network.
- Supports the validation and consensus process by timely data delivery.
- Maintains overall network reliability.
- Ensures new data is quickly shared with all nodes.

ii) Application Layer

- The topmost layer interfaces directly with users and developers, providing easy access to blockchain functions.
- Includes decentralized applications (DApps), smart contracts, and wallets that enable automated business logic execution.
- Facilitates real-world applications in sectors like finance, supply chain, healthcare, and voting systems.
- Provides tools for creating, sending, and managing transactions.
- Makes blockchain technology accessible and practical for everyday use.
- Enables execution of smart contracts automatically.

SPPU-BE-COMP-CONTENT – KSKA Git

Together, the propagation layer ensures efficient data distribution, while the application layer enables meaningful user interactions, making both essential components of a functional blockchain ecosystem.

b) List & Explain features of Block Chain [4]

1. **Decentralization:**
Operates on a distributed network without a central authority, improving fault tolerance and reducing single points of failure.
2. **Immutability:**
Data recorded in blocks cannot be altered or deleted, ensuring permanent and tamper-proof records.
3. **Transparency:**
Transactions are recorded on a ledger visible to participants, enabling easy auditing and trust.
4. **Security:**
Uses cryptographic hashing and consensus algorithms to protect data from fraud and unauthorized changes.
5. **Consensus Mechanism:**
Ensures all nodes agree on the validity of transactions, maintaining a consistent and trustworthy ledger.
6. **Anonymity and Privacy:**
Users' identities are protected through cryptographic techniques while maintaining transaction traceability.
7. **Traceability:**
Every transaction is linked to previous ones, making it easy to track asset movement and verify authenticity.

c) Comment on “Feasibility of an Online Voting System Implementation” using Block Chain Technology. [5]

Feasibility of Online Voting System Using Blockchain

- **Decentralization:** Removes the need for a central authority, reducing risks of vote manipulation and single points of failure.
- **Immutability:** Votes recorded on the blockchain cannot be altered or deleted, ensuring election integrity.

SPPU-BE-COMP-CONTENT – KSKA Git

- **Transparency:** Allows all participants or authorized auditors to verify votes while maintaining voter anonymity through cryptography.
- **Automation via Smart Contracts:**
Smart contracts can automatically count votes and declare results based on pre-set rules, which speeds up the process and reduces human error or interference in vote tallying.
- **Implementation Challenges:**
Despite its advantages, blockchain voting systems face challenges such as ensuring scalability to handle millions of voters, making the system user-friendly for people with different levels of digital literacy, and protecting voter identities against sophisticated cyber attacks.

ALTERNATIVE ANSWER :

Blockchain technology offers significant potential for creating a secure, transparent, and tamper-proof online voting system. Its **decentralized nature** eliminates the need for a central authority, reducing risks of manipulation or single points of failure. Each vote can be recorded as a transaction on the blockchain, ensuring **immutability** so votes cannot be altered or deleted once cast, which enhances election integrity.

Additionally, blockchain provides **transparency** by allowing all participants or authorized auditors to verify votes without compromising voter anonymity, maintaining privacy through cryptographic techniques. The use of **smart contracts** can automate vote counting and result declaration, increasing efficiency and reducing human errors.

However, challenges such as **scalability**, **user accessibility**, and **digital literacy** must be addressed to make the system practical for widespread use. Security concerns like protecting voter identities against sophisticated cyber attacks also require robust solutions. Despite these hurdles, blockchain's features make it a promising technology for reliable and trustworthy online voting systems.

➤ SEP 2024

Q3)

a) Explain consensus Layer in Blockchain.

b) Differentiate between centralized and decentralized systems.

c) Discuss evolution of Blockchain.

→ ALL REPEATED !

Q4)

a) Explain semantic Layer in Blockchain [5]

The **Semantic Layer** in blockchain is a conceptual layer that focuses on the **meaning, interpretation, and usability** of data stored on the blockchain. It enables users and applications to understand, process, and interact with blockchain data in a meaningful way, beyond just raw transactions and blocks.

Explanation of Semantic Layer

1. **Data Interpretation:**
The semantic layer provides context to the raw blockchain data, allowing applications to interpret what transactions represent, such as contracts, ownership, or specific actions.
2. **Smart Contracts and Business Logic:**
It supports the execution and understanding of smart contracts, which embed business rules and logic directly into the blockchain, enabling automated and trustless transactions.
3. **Interoperability:**
The semantic layer helps different blockchain networks and applications communicate and understand each other's data formats and protocols, promoting interoperability.
4. **User Interaction:**
It bridges the gap between complex blockchain data structures and user-friendly interfaces, making it easier for users to interact with blockchain applications.
5. **Enhanced Functionality:**
By adding meaning to data, the semantic layer enables advanced features like decentralized identity, reputation systems, and contextual data querying.

The semantic layer is essential for making blockchain data usable and understandable, thereby supporting complex applications and improving user experience across decentralized networks.

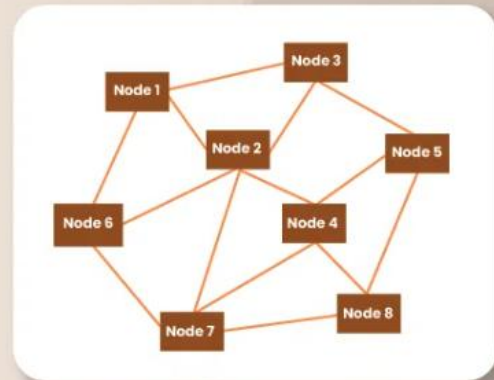
.....CHECK ONCE

b) Discuss importance of Blockchain. [5]

➔ ALREADY DONE !

c) What is decentralized system? Explain with diagram. [5]

Decentralized Architecture in Distributed System



A decentralized system is a network where **control, decision-making, and data storage** are distributed across **multiple nodes** (computers/participants) instead of relying on a single central authority. This architecture is the backbone of **blockchain technology**, ensuring **transparency, security, and censorship resistance**.

Key Characteristics of Decentralized Systems

1. No Single Point of Failure

- If one node fails, the network remains operational (unlike centralized systems where a server crash disrupts everything).
- *Example:* Bitcoin nodes sync data peer-to-peer; no central server exists.

2. Peer-to-Peer (P2P) Communication

- Nodes interact directly without intermediaries.
- *Example:* Ethereum nodes propagate transactions via gossip protocol.

3. Consensus Mechanisms

- Decisions are made collectively using algorithms like:
 - **Proof-of-Work (PoW)** (Bitcoin).
 - **Proof-of-Stake (PoS)** (Ethereum 2.0).
- Prevents malicious actors from controlling the network.

SPPU-BE-COMP-CONTENT – KSKA Git

4. Transparency & Immutability

- All participants verify and store data (e.g., blockchain ledgers).
- Tampering requires altering >51% of the network—nearly impossible.

Decentralization Matters in Blockchain due to :

Trustless : No need to rely on a central authority (e.g., banks).

Censorship-Resistant: No single entity can block transactions.

Fault-Tolerant: Survives node failures/attacks.

"Check/Verify Answer – Read at Your Own Risk"