

[4]

- ii. Explain the difference between symmetric and asymmetric cryptography in the context of blockchain security. How do these cryptographic methods work together to ensure secure transactions on a blockchain network?
- OR iii. Discuss the key benefits and limitations of blockchain technology. Include examples of how blockchain's features like immutability, decentralization, and transparency provide advantages, but also mention the challenges associated with scalability, energy consumption, and regulatory issues.
- Q.4 i. What is Nakamoto Consensus? How does it contribute to the security of a blockchain network?
- ii. Explain the Proof of Work (PoW) consensus mechanism. How does it ensure network security? What are its drawbacks, particularly with regard to energy utilization?
- OR iii. Discuss the concept of Proof of Stake (PoS). Compare Proof of Stake (PoS) with Proof of Work (PoW) in terms of energy efficiency, security, and scalability. Include the potential risks associated with PoS, such as centralization and the "Nothing at Stake" problem.
- Q.5 i. How does a Merkle Patricia Tree contribute to the efficiency and security of a blockchain network? Explain with a practical example.
- ii. Evaluate the differences between soft fork and hard fork in blockchain architecture. In your response, discuss the impact of each on network consensus, compatibility, and the potential for blockchain fragmentation.
- OR iii. Compare and contrast public and private blockchains, focusing on their use cases, consensus mechanisms, and security features. What are the advantages and disadvantages of each type in terms of scalability and decentralization?
- Q.6 Attempt any two:
- i. Compare and contrast blockchain applications in the financial sector and medical sector.
- ii. Discuss in detail about the Hashgraph. Differentiate between Hashgraph and tangle.
- iii. Give a short case study of Government on blockchain.

**8** 2 4 2 4

Total No. of Questions: 6

Total No. of Printed Pages: 4

Enrollment No.....



**Faculty of Engineering**  
**End Sem Examination Dec 2024**  
**OE00016 Blockchain Architecture**

Programme: B.Tech.

Branch/Specialisation: All

**Maximum Marks: 60**

**Duration: 3 Hrs.**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

**3** 2 3 3 4

**7** 1 2 3 3

**7** 1 8 3 4

**4** 3 7 4 3

**6** 5 8 4 3

**6** 2 3 4 4

**5** 2 6 5 1

**5** 3 4 5 1

**5** 4 5 5 2

Marks	BL	PO	CO	PSO
<b>1</b>	1	2	2	3

- Q.1 i. In a blockchain network, what is the most effective method to prevent double spending?

(a) Proof of Stake (PoS): Ensuring that only those who hold a large amount of the cryptocurrency can validate transactions

(b) Public Key Cryptography: Encrypting transactions so that only the sender and receiver can view them

(c) Off-chain Storage: Storing transactions outside the blockchain to avoid duplicate entries

(d) Proof of Work (PoW): Requiring miners to solve complex mathematical problems before adding transactions to the blockchain

- ii. What is the primary purpose of Bitcoin's halving event, which occurs approximately every four years?

(a) To increase the number of Bitcoins that can be mined each day

(b) To reduce the supply of new Bitcoins entering circulation, potentially increasing scarcity

(c) To increase transaction fees for miners, making the network more secure

(d) To reset all Bitcoin balances and start a new blockchain cycle

- iii. Which of the following best describes the role of a hash function in a blockchain?

(a) It converts data of any size into a fixed-size output, ensuring data integrity and enabling quick verification

(b) It encrypts transaction data to prevent unauthorized access

(c) It compresses blockchain data to reduce storage requirements

(d) It verifies the identity of users on the network through private keys

Marks	BL	PO	CO	PSO
<b>1</b>	1	1	1	3

Marks	BL	PO	CO	PSO
<b>1</b>	2	5	2	4

\*\*\*\*\*

	[2]									
iv.	Which of the following features of blockchain ensures that once data is recorded, it cannot be altered or deleted?	<b>1</b>	2	11	2	3				
	(a) Decentralization      (b) Transparency									
	(c) Immutability      (d) Consensus Mechanism									
v.	Which of the following is a key characteristic of the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, commonly used in permissioned blockchains?	<b>1</b>	2	7	3	4				
	(a) It relies on probabilistic finality, where transactions may still be reversed if the majority of nodes agree									
	(b) It requires a supermajority (typically 2/3) of nodes to agree on the validity of a transaction before adding it to the blockchain									
	(c) It operates on a "longest chain wins" principle, where the longest chain of blocks is considered valid									
	(d) It uses mining rewards to incentivize node participation and ensure network security									
vi.	What is the primary purpose of Ethereum's smart contracts?	<b>1</b>	1	4	5	4				
	(a) To automatically execute, control, or document events and actions according to coded terms without needing a central authority									
	(b) To transfer Ether between wallets without any transaction fees									
	(c) To provide a backup for Bitcoin transactions in case of network failure									
	(d) To ensure that only verified users can participate in the Ethereum network									
vii.	In the context of blockchain technology, what is a hard fork?	<b>1</b>	2	3	5	4				
	(a) A minor update to the blockchain software that does not require nodes to update to the latest version									
	(b) A temporary division of the blockchain network that automatically resolves without impacting consensus									
	(c) A process to reduce the transaction fees on the blockchain by increasing block size									
	(d) A split in the blockchain where new consensus rules are incompatible with the previous version, creating a permanent divergence									
viii.	Which of the following is a defining characteristic of a public blockchain?	<b>1</b>	2	6	4	7				
	(a) It restricts access to a select group of authorized participants who can view and validate transactions									
	(b) It requires users to have a government-issued ID to join the network									
	(c) It is open for anyone to join, participate, and validate transactions, with full transparency of data									
	[3]									
ix.	(d) It operates without the use of a consensus mechanism, relying solely on a central authority for verification	<b>1</b>	3	4	5	6				
	ix. Which unique feature of the Hashgraph consensus algorithm differentiates it from traditional blockchain consensus mechanisms like Proof of Work and Proof of Stake?									
	(a) It achieves consensus through a voting-based system, requiring all nodes to cast votes on each transaction's validity									
	(b) It uses a gossip-about-gossip protocol combined with virtual voting to reach consensus, enabling high throughput and fast finality without the need for miners									
	(c) It relies on a leader-based approach, where one designated node validates transactions to reduce latency									
	(d) It prioritizes the longest chain of events, similar to how blockchains select the longest chain of blocks as valid									
x.	x. Which of the following is a primary use case of blockchain technology in the supply chain industry?	<b>1</b>	2	3	5	4				
	(a) Data storage: Storing large volumes of data in a distributed ledger									
	(b) Decentralized finance: Facilitating peer-to-peer lending without intermediaries									
	(c) Transparent tracking: Ensuring real-time and immutable tracking of goods from origin to destination									
	(d) Digital Identity Management: Managing personal identities for online authentication									
	Q.2 i. What is the double spending problem in cryptocurrency? How is it addressed in Bitcoin?	<b>2</b>	1	4	1	3				
	ii. Explain how Bitcoin mining works. Discuss. How miners are rewarded?	<b>3</b>	2	3	1	3				
	iii. Compare and contrast the different types of cryptocurrency wallets (e.g., hot wallets, cold wallets, hardware wallets, and paper wallets). Discuss their security features and use cases.	<b>5</b>	2	4	1	4				
	OR iv. What are the legal aspects surrounding cryptocurrencies? Discuss the regulatory challenges and the stance of different countries toward cryptocurrency adoption and trading.	<b>5</b>	1	4	1	3				
	Q.3 i. What is a hash function in blockchain technology? Why is the SHA-256 algorithm commonly used?	<b>2</b>	1	5	2	3				

## Marking Scheme

### OE00016 Block Chain Architecture

Q.1	i)	D) Proof of Work (PoW): Requiring miners to solve complex mathematical problems before adding transactions to the blockchain	1	B. Discuss the regulatory challenges and the stance of different countries toward cryptocurrency adoption and trading. (2+3) Ans: Three regulatory challenges, international adoption and trading → 3 marks
	ii)	B) To reduce the supply of new Bitcoins entering circulation, potentially increasing scarcity	1	
	iii)	A) It converts data of any size into a fixed-size output, ensuring data integrity and enabling quick verification	1	
	iv)	C) Immutability	1	
	v)	B) It requires a supermajority (typically 2/3) of nodes to agree on the validity of a transaction before adding it to the blockchain	1	
	vi)	A) To automatically execute, control, or document events and actions according to coded terms without needing a central authority	1	
	vii)	D) A split in the blockchain where new consensus rules are incompatible with the previous version, creating a permanent divergence	1	
	viii)	C) It is open for anyone to join, participate, and validate transactions, with full transparency of data	1	
	ix)	B) It uses a gossip-about-gossip protocol combined with virtual voting to reach consensus, enabling high throughput and fast finality without the need for miners	1	
	x)	C) Transparent tracking: Ensuring real-time and immutable tracking of goods from origin to destination	1	
Q.2	i.	Ans: 2 lines discussion of Double Spending problem → 1 Mark One resolving technique → 1 mark	2	
	ii.	Ans: Describing Bitcoin mining process → 2 marks One rewarding technique discussion → 1 mark	3	
	iii.	Ans: Discussion of wallet and their types, hot wallets, cold wallets, hardware wallets, and paper wallets → 3 marks B. Discuss their security features and use cases. (3+2) Ans: One security feature and one use case → 2 Marks	5	
	iv.	Ans: Writing two legal aspects, one national and one international → 2 marks	5	
OR	i.			Q.3 i. Ans: Hash function definition → 1 Mark and common uses → 1 mark
	ii.			ii. A. Explain the difference between symmetric and asymmetric cryptography in the context of blockchain security. 4 Marks Ans: At least four differences → 4 marks
	iii.			B. How do these cryptographic methods work together to ensure secure transactions on a blockchain network? 4 Marks Ans: Discussion and example of secured transaction → 2 marks How I secure blockchain network → Two marks
OR	iii.			Ans: Two benefits and two limitations → 2 marks
	iv.			B. Include examples of how blockchain's features like immutability, decentralization, and transparency provide advantages, but also mention the challenges associated with scalability, energy consumption, and regulatory issues. (3+3) marks Ans: Advantage of immutability, decentralization, and transparency → 3 Marks Challenges with scalability, energy consumption, and regulatory issues → 3 Marks
	v.			
Q.4	i.			Q.4 i. Ans: Nakamoto Consensus Definition → 1 Marks Two security contributions → 2 Marks
	ii.			ii. A. Explain the Proof of Work (PoW) consensus mechanism. 3 Marks Ans: PoW explanation with diagram (1.5+1.5)
	iii.			B. How does it ensure network security, and what are its drawbacks, particularly with regard to energy utilization? (2+2) Marks Ans: At least two network security ensure → 2 Marks At least two drawbacks → 2 marks
OR	iii.			OR iii. A. Discuss the concept of Proof of Stake (PoS) and compare it
	iv.			7

[2]

with Proof of Work (PoW) in terms of energy efficiency, security, and scalability. (2+3) Marks

Ans: PoS discussion and diagram → 1+1 marks

Comparison in efficiency, security, and scalability → 3 marks

B. Include the potential risks associated with PoS, such as centralization and the "Nothing at Stake" problem. 2 marks

Ans: At least two risk explanations → 2 marks

[3]

Q.5 i. Ans: Two contributions → 2 marks

Two examples → 2 marks

ii. Ans: At least three differences → 3 marks

B. In your response, discuss the impact of each on network consensus, compatibility, and the potential for blockchain fragmentation. 3 marks

Ans: Impact on network consensus, compatibility, and the potential for blockchain fragmentation (1+1+1) marks

OR iii. Ans: At least three comparisons → 3 marks

B. What are the advantages and disadvantages of each type in terms of scalability and decentralization? 3 Marks

Ans: At least two advantages and two disadvantages for scalability and decentralization for public and private blockchains → (1.5 + 1.5) marks

Q.6

i. Compare and contrast blockchain applications in the Financial Sector and Medical Sector. **5**

Ans: At least five points discussion → 1 X 5 marks

ii. Discuss in detail about The Hashgraph. Differentiate between Hashgraph and Tangle (3+2) marks **5**

Ans: Hashgraph definition, discussion and diagram → 3 marks

At least two difference points → 2 marks

iii. Give a short case study of Government on blockchain **5**

Ans: Case study paragraph may include one existing product of government blockchain and its discussion, application, merits, challenges and at least one diagram of this system →(1X5) marks