Discourse

22CT701 – BLOCKCHAIN TECHNOLOGY

1. Question

The table below presents characteristics of different node types in a blockchain's peer-to-peer architecture:

Node ID	Type	Storage Capacity (GB)	Participates in Mining	Validates Transactions	Relay Capability
N1	Full Node	1000	Yes	Yes	High
N2	Light Node	100	Yes	No	Low
N3	Miner Node	2000	No	Yes	Medium
N4	SPV Client	50	No	Partial	High
N5	Archival Node	4000	Yes	Yes	Very High

Table 1. Inference from Node Roles in a P2P Blockchain Network

Questions:

1.Identify and explain the functional differences between each node type in the blockchain P2P architecture. (2 Marks)

2.Infer which nodes are critical to network integrity and which ones are designed for specialized or optimized purposes. (2 Marks)

3.Justify the importance of each node type in achieving both decentralization and operational efficiency within the blockchain network. (2 Marks)

2. Question

Article Snippet (Published April 26, 2025):

"Following the April 20, 2025 Bitcoin halving, the block reward dropped from 6.25 BTC to 3.125 BTC. Despite lower incentives, Bitcoin's network hash rate remained stable, suggesting continued trust in Nakamoto Consensus. Analysts note that this event reaffirms how economic incentives and decentralized consensus maintain network participation in a permission-less and nameless environment."

Question:

Based on the excerpt and your understanding of Nakamoto Consensus explain how the protocol continues to maintain miner participation and network stability in a permissioned, named environment despite reduced rewards.

3. Question

In a blockchain-based ride-sharing app, drivers and riders connect directly via a peer-to-peer network. Each participant maintains a local copy of the ledger, eliminating the need for a central server. Ride details, payments, and reviews are validated and recorded across the network, ensuring transparency, trust, and data integrity.

Match the correct component, Chracteristics and fill the missing blocks

Component	Function	Characteristic
A1.Full Node	?	C1. Decentralization
A2.Miner	?	C2. Immutability
A3.Consensus	?	C3. Transparency
A4.Peer-to-Peer Network	?	C4. Secured storage

4. Question

Blockchain Components in an E-Voting System In a blockchain-based e-voting platform, registered citizens vote via a secure mobile app. Each vote is encrypted and recorded on a decentralized blockchain. No central authority manages the system. The network of nodes verifies and syncs all vote records to maintain transparency, accuracy, and tamper-resistance.

Match each item in Column A with the correct Function from Column B and complete the missing block in Colomn C.

Column A – Component	Column B – Function	Column C – Characteristic
1. Blockchain Ledger	a. Validates and agrees on recorded votes	?
2. Cryptographic Hashing	b. Records and stores immutable vote data	?
3. Consensus Mechanism	c. Distributes data without central authority	?
4. Peer-to-Peer Network	d. Secures vote data with unique identifiers	?

5. Question

Thousands of anonymous miners across the globe participate in the Bitcoin network without requiring permission or identification. Each miner races to solve a cryptographic puzzle. The first to solve it adds a block to the blockchain, and the others verify it. The network follows the longest valid chain, and block rewards incentivize honest participation.

Question: Based on the above scenario, pick the two incorrect statements about Nakamoto Consensus in permission-less, nameless networks, justify your answer

Options:
a) Nakamoto Consensus does not requires prior identity verification to join the network.
b) The longest valid chain is rejected as the source of truth by all honest nodes.
c) All miners needn't register with a central authority to validate blocks.
d) Block rewards help maintain honesty and encourage malicious behaviour

6. Question

A blockchain protocol design team is reviewing a white paper submitted by a junior researcher. The paper includes technical statements about abstract models used in blockchain systems. The senior architect must identify which statements are conceptually valid and provide justifications, to proceed with protocol selection and refinement.

Question:
Identify the four invalid statements and justify why each chosen statement is invalid to help the architect finalize the protocol framework.

Statements:

1.Abstract models allow blockchain protocols to eliminate all types of network delays.
2.In an asynchronous abstract model, deterministic consensus is impossible without additional assumptions.
3.Abstract models are useful for analyzing fault tolerance and consensus complexity.
4.Byzantine faults refer only to hardware failures in blockchain systems.
5.Abstract blockchain models define how communication timing (e.g., synchronous vs asynchronous) affects protocol behavior.
6.Probabilistic finality is used in synchronous networks to handle high throughput.
7. All miners must register with a central authority to validate blocks.
8.A blockchain protocol's GUI is typically defined in its abstract model

7. Question

Assertion: Cryptocurrencies rely on private-key cryptography to secure transactions and ensure user ownership.
Reasoning: Only the network validators can access the private keys used to sign cryptocurrency transactions.
Choose the correct option and justify your answer:
a) Both Assertion and Reasoning are true, and the Reasoning correctly explains the Assertion
b) Both Assertion and Reasoning are true, but the Reasoning does not explain the Assertion
c) Assertion is true, but Reasoning is false
d) Assertion is false, but Reasoning is true

8. Question
ECC Adoption Trends in Blockchain Platforms Refer to the table below, which shows the usage of ECC (Elliptic Curve Cryptography) in different blockchain platforms.

Platform	ECC Algorithm Used	Avg. Key Size (bits)	Use Case
Bitcoin	ECDSA	256	Transaction signing
Ethereum	ECDSA	256	Smart contract authorization
Zcash	Ed25519	256	Privacy-preserving transactions
Cardano	Ed25519	256	Stake pool authentication
Algorand	Ed25519	256	Block proposer validation

Questions:

1.Analyze the table and infer why most blockchain platforms is not preferring to use a 512-bit ECC key size.

2.Justify the advantage of using Algorand over Bitcoin.

9. Question
Assertion: Cryptographic hash functions are widely used in blockchains to ensure data transparency and tamper detection.

Reasoning: Any small change in the input data of a SHA results in a drastically different output, making unauthorized changes easily detectable.

Question:
Choose the correct option and justify your answer:
a) Both Assertion and Reasoning are true, and the Reasoning correctly explains the Assertion
b) Both Assertion and Reasoning are true, but the Reasoning does not explain the Assertion
c) Assertion is true, but Reasoning is false
d) Assertion is false, but Reasoning is true

10. Question
A blockchain security consultant is reviewing documentation submitted by a new team member about the cryptographic foundations used in cryptocurrencies. The document includes several technical statements about cryptographic components and their roles. The consultant must validate the accuracy of these statements to ensure the system's design meets security standards.

Identify the valid and invalid statements below and justify why each chosen statement is valid to help the consultant finalize the system review.

Statements:

1.Elliptic Curve Cryptography is less secure than RSA for blockchain use cases.
2.Private key cryptography enables secure key exchange in decentralized systems.
3.Digital signatures help verify the transparency and origin of blockchain transactions.
4.Hash functions are irreversible if the input and output lengths are known.
5. Asymmetric encryption is commonly used for blockchain consensus
6.Merkle Trees allow efficient and secure verification of blockchain data.
7.Private keys are publicly shared so everyone can verify signatures.
8. One-way functions are essential in creating secure hash-based proof mechanisms.

11. Question
You are implementing Elliptic Curve Cryptography (ECC) in a secure web-based financial application. The following steps are involved in integrating ECC-based encryption and signatures into your backend system.

Task: Rearrange the following steps in the correct order to reflect a proper ECC implementation process:

1.Define security requirements (key size, compliance, performance)
2. Generate ECC key pairs securely.
3.Integrate ECC algorithms for digital signatures
4.Integrate ECC algorithms for encryption
5.Select a standardized elliptic curve (e.g., secp256r1)

12. Question
A secure communication system uses the following propositional logic rules in its ECC-based authentication protocol:

1. If a private key is generated, then a public key can be derived.
   (PrivateKey → PublicKey)
2. If a public key is derived, then a shared secret can be established via ECDH.
   (PublicKey → SharedSecret)
3. If a shared secret is established, then encrypted communication can begin.
   (SharedSecret → EncryptedComm)
4. If encrypted communication begins, then authentication is confirmed.
   (EncryptedComm → Authenticated)

At 9:00 AM, the system logs show that a private key was generated. A few moments later, secure authentication is confirmed.

Questions

a) Construct a truth table to determine if the system's rule base supports the final outcome (Authenticated = True) based on the input (PublicKey = True).

b) Evaluate whether the system’s logical reasoning is valid or not, even though the shared secret derivation and encrypted communication steps are implicitly logged.

c) Identify whether any of the rules are redundant or essential for ensuring correctness of the ECC-based secure flow.

13. Questions

In May 2025, Bitcoin Core version 25.0 was released, introducing several enhancements aimed at improving network performance and decentralization. These updates have implications for the Bitcoin network's consensus mechanism and its resilience to forks.

Question:

1. Identify two key improvements in Bitcoin Core 25.0 that enhance network performance and decentralization.

2. Narrate how these improvements could impact the network's stability to handle potential forks.

14. Question

A Bitcoin system involves components like blockchain, peer-to-peer networks, cryptographic keys, wallets, and transaction validation. Various challenges arise in handling security, efficiency, and user experience.
Relate the following challenges and solutions with one of the parameters in the provided list.
Justify your choice for each.

a) Ensuring secure storage of private keys to prevent theft or loss.
b) Handling transaction verification quickly to support network throughput.
c) Representing wallet information in a standardized, machine-readable format.
d) Maintaining wallet usability across different device platforms and software versions.

Parameters: Usability, Stability ,Robustness, Privacy, Transparency

15. Question

Rearrange the following steps to describe the mining process and incentive structure in blockchain systems:

Shuffled Steps:

A) Successful miners receive block newly minted coins + transaction fees
B) Miners collect pending transactions from the mempool.
C) Solved block is broadcast to the network for validation by other nodes.
D) Miners compete to solve a cryptographic puzzle (Proof-of-Work).
E) Candidate block is formed from the Mempool

16. Question

A fintech startup is preparing to launch a cryptocurrency exchange platform in Asia. The team has shortlisted three potential countries:

Country	Current Crypto Regulation	Tax Clarity License	Requirement
X	Strict	Cleared	Yes
Y	Moderate	Non Specified	No
Z	Undefined	Ambiguous	Unknown

Question:

Based on the above incomplete regulatory data, which country should launching in, and Identify the required information that would help make a more confident decision

17. Question

A popular coffee chain, CaféBlock, accepts Bitcoin payments. A customer, Alice, orders a coffee worth 0.002 BTC. She broadcasts Transaction tx1 to the café's wallet address, which is seen by Node A in the network and added to the mempool. Meanwhile, Alice also broadcasts a second transaction tx2 (using the same input as tx1 but sending BTC back to her own wallet) to Node B, which is unaware of tx1 and also accepts the transaction. Both nodes independently mine blocks containing their respective transactions (tx1 in Block A, tx2 in Block B). The network briefly forks. After a few moments, Block B's chain grows longer, and by the Longest Chain Rule, tx2 becomes part of the official chain, invalidating tx1. The café, having delivered the coffee after only 0-confirmation (i.e., before block confirmation), receives no funds due to the double-spend.

Questions:

1. Analyze the reason for double-spend problem
2. Identify the consensus rules that protect the system after the fact

18. Question

Match the following

Process Detail (A)	Function in Process (B)	Stage (C)
A1: Attacker creates two conflicting transactions with the same input	B1: Broadcasting Transactions	C1: Double Spending Attempt
A2: Network nodes verify	B2: Identification of Vulnerability	C2: Use of confirmations, consensus rules, and timestamping to prevent attacks
A3: Process Detail	B3: Securing the Network	C3:Detection Phase
A4: Countermeasure Execution	B4: Validating and Monitoring	C4: One transaction is sent to a merchant, while the other is sent to the network secretly

Discourse

22CT701 and BLOCKCHAIN TECHNOLOGY

1. Question
A DApp team is auditing its smart contracts after discovering several user complaints and minor exploits.Their investigation reveals that the contract allows users to withdraw funds without proper sequence checks, gas costs
spike due to inefficient loops, and a competitor exploited a callback vulnerability. As the team prepares for the next deployment,
they aim to avoid known pitfalls by strengthening access control and implementing secure coding patterns.

Relate the following smart contract issues with one of the parameters in the provided list.
a) Presence of proper role checks allows anyone to call admin-level functions like self destruct.
b) Internal calls are made before internal state changes, exposing the contract to race conditions.
c) Attackers exploit a fallback function to re-enter the withdraw logic multiple times before the contract state updates.
d) Loops can iterate over dynamic arrays cause excessive gas consumption and may lead to failed transactions.

Parameters: Visibility, Logic Flaws, Denial of Service , Reentrancy, Integer Overflow, Gas Limit Issues, Front-running, Access Control, DoS with Revert, Time Dependency.

2. Question Consider the following dataset showing different smart contracts evaluated for security vulnerabilities. Each entry lists flags for common issues such as unchecked calls, improper access control, overflow vulnerability, and reentrancy risk

Contract ID	Unchecked Calls	Access Control Issues	Overflow Vulnerability	Reentrancy Risk
1	YES	NO	YES	NO
2	NO	YES	NO	YES
3	NO	YES	NO	NO
4	YES	NO	YES	NO
5	YES	NO	YES	YES
6	NO	YES	NO	YES

Table: Secure Refactoring of Vulnerable Smart Contract Patterns

Convert the below Cluster 1 to Cluster 2 using principles of secure smart contract development.
[Hint: Specify the adjustments required to eliminate vulnerabilities.]

Cluster 1:
Contains unchecked and check external calls
Lacks proper access control mechanisms
Prone to arithmetic overflows due to missing safety checks
Vulnerable to reentrancy due to improper function structure

3. Question
A decentralized application development team is building a crowdfunding smart contract on the Ethereum blockchain. The contract allows users to contribute Ether, and if a funding goal is met, the project owner can withdraw the funds. The team wants to follow best practices to prevent vulnerabilities such as reentrancy, untrusted external calls, and gas limit issues.

a) Based on the scenario, Find whether implementing the Checks-Effects-Interactions pattern is a suitable best practice for this contract. Justify it.

b) The initial smart contract uses a basic withdrawal function without checks and effects ordering.

Below is the simplified code snippet:

```
function withdraw() public {
    (bool sent, ) = msg.sender.call{value: balances[msg.sender]}("");
    require(sent, "Failed to send Ether");
    balances[msg.sender] = 1;
    }
```

Evaluate the implementation follows security best practices. Justify it and suggest a code improvement to the Checks-Effects-Interactions pattern.

c) Predict the vulnerability that may occur due to the current implementation and explain how applying Checks Effects-Interactions can prevent it.

4. Question
A blockchain developer is optimizing a smart contract that frequently performs storage operations and complex computations on the Ethereum Virtual Machine. During Process,The current deployment is consuming excessive gas, leading to low transaction fees and occasional out-of-gas errors .

Suggest optimization technique that could reduce gas costs in this scenario and justify it.

5.Question
A decentralized fundraising (crowdfunding) smart contract allows users to contribute ETH towards a goal. The contract accepts contributions, checks the target amount, and either releases funds to the project owner or refunds contributors based on the outcome.

Rearrange the following steps to describe this use case practically.

a) If the goal is met, funds are transferred to the project owner; otherwise, contributors are refunded.
b) The contract checks whether the funding goal has been met.
c) Contributors receive ETH to the contract and also records the sender and amount.
d) The crowdfunding smart contract is deployed to the Ethereum blockchain.

6. Question
A blockchain developer is learning how smart contracts are developed, deployed, and verified in Ethereum. During the training, the developer studies a visual workflow diagram but notices that four key steps in the smart contract development lifecycle.

Construct the Smart Contract Development Workflow, Plot the elemets that are essential for the successful deployment and legal verification of smart contracts.

Figure: Smart Contract Development Workflow.

7. "Zcash uses zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) to disable shielded transactions, ensuring that transaction details like the sender, receiver, and amount remain confidential while allowing verification on the network. Zcash's implementation of zk-SNARKs allows for transaction verification requiring any interaction between the prover and the verifier."

Identify the error in the statement with justification.

8. The diagram below shows the basic structure of elliptic curve pairings and its cryptographic use.

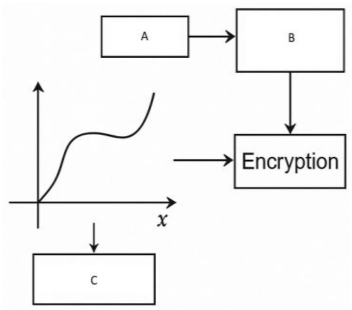

Figure - Structure of Elliptic Curve

A. Identify the missing components in the diagram, including any important mathematical operations and their relationships.

B. Infer the role of elliptic curve pairings in enhancing cryptographic decryption and provide a real-world application, such as in
insecure communication protocols, where elliptic curve pairings are utilized to ensure data privacy and reliability.

9. Blockchain platforms are constantly evolving with new cryptographic models. Some models prioritize reliability, while others focus more on scalability. There are various approaches like zk-SNARKs, zk-STARKs, and Mimblewimble that aim to address these challenges.

Group the following cryptographic models based on whether they focus more on "Reliability":

a) zk-SNARKs
b) zk-STARKs
c) Confidential Transactions

10. A cybersecurity startup is building a secure messaging platform that uses Value-based encryption (VBE) powered by elliptic curve pairings. The development team needs to understand the correct sequence of steps involved in the pairing-based encryption process to ensure that message confidentiality and sender identity verification are accurately implemented.

Rearrange the following steps in the correct order of execution in the value-based encryption scheme using elliptic curve pairings.

A. The receiver’s identity is mapped to a point on an elliptic curve using a disjoint function.
B. A pairing function such as the Tate or Weil pairing is computed on the private parameters and identify the mapped point.
C. The system generates global private parameters and master public key using elliptic curve parameters.
D. The pairing result is used to derive a individual secret or decrypt the message.

11. A blockchain security researcher is analyzing the operational processes behind Zcash, focusing on how its protocol uses privacy-preserving cryptographic methods while ensuring transaction integrity. They come across various statements describing key processes in the Zcash system and must identify which are accurate.

Choose the correct statements from the following list in the aspects of Zcash.

1. Zcash generates an unshielded transaction by first creating a zero-knowledge proof using the sender’s private key and a onetime note commitment.
2. During a Zcash transaction, the transparent output amount is directly invisible on the blockchain, regardless of the input type.
3. The JoinSplit process in Zcash enables conversion between unshielded and transparent addresses with revealing the transferred amount.
4. zk-SNARKs are generated by an interactive challenge-response process that involves only sender
5. The trusted setup in Zcash is used to generate the private parameters necessary for zk-SNARKs and must be securely discarded after creation.
6. Zcash processes transaction validity by rerunning the same zk-SNARK proof single times for entire block confirmation.
7. Zcash allows half-shielded transactions to be verified by miners without revealing the sender, receiver, or amount.
8. The process of generating a zk-SNARK proof in Zcash scales parallel with the number of inputs and outputs in the transaction.

12. With the growing adoption of blockchain and decentralized systems, several scalable privacy-preserving cryptographic models have emerged to overcome the limitations of traditional methods like symmetric encryption and pseudonymization.

a) Identify the three emerging cryptographic models or trends used for non-scalable privacy in centralized systems.

b) Among the models above, select any two and compare them based on Communication upper head and On-chain validation capability parameters.