NOC22-CS44: Blockchain and Its Applications
Assignment 1

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. What is expected by a decentralized solution for a successful Supply Chain management?
    a. No one should trust each other, however they should cooperate
    b. Everyone should trust and cooperate with each other
    c. No one should trust and cooperate with each other.
    d. Trust and cooperation does not matter here

Hint: In a real-time scenario a supply chain management system has multiple stakeholders and the information submitted by them is not guaranteed to be correct.

2. What does trust mean, in a decentralized blockchain?
    a. To secure the chain using specific protocols.
    b. To validate the transactions and blocks for tamper proofing.
    c. To execute and confirm the transactions.
    d. None of the above

Hint: Trust in a decentralized blockchain means someone can not deny the information later on. Which implies the answer is (a), (b) and (c).

3. Where are the transactions recorded in a blockchain?
    a. On a SQL Database
    b. On a distributed immutable ledger
    c. On a distributed opaque immutable ledger
    d. On a centralized immutable ledger

Hint: Refer to the slide. Definition of Blockchain - An immutable append only ever growing chain of data. Data once added cannot be deleted or modified later

4. What is one of the requirements of a secure hashing function?
    a. It is an ECC function
    b. It is a one way function
    c. It is log function
    d. It is a secret function

Hint: Refer to the Week 1 slide. Definition of Blockchain - An immutable append only ever growing chain of data. Data once added cannot be deleted or modified later

5. For a 512 bit hash function, the attacker needs to compute how many hash operations in order to find two matching outputs?

a. 1.158×10^{77}
b. 1.340×10^{154}
c. 3.403×10^{38}
d. 2.895×10^{76}

Hint: If a hash function produces □ bits of output, an attacker needs to compute only $2^{□/2}$ hash operations on a random input to find two matching outputs. $2^{512/2} = 2^{256} \approx 1.158 \times 10^{77}$

6. Which of the following is a correct statement about a cryptographic hash function?
   a. given the same message the hash function would not return the same hash
   b. it is not very difficult to generate the original message from the hash
   c. a small change in the message, impacts the hash value
   d. one can easily find two different messages with same hash

Hint: Refer to the Week 1 slide for the properties of cryptographic hash functions.

7. What are the security features of a hash function?
   a. Deterministic
   b. Puzzle-friendly
   c. Collision-resistance
   d. Preimage resistance

Hint: Refer to the Week 1 slide for the properties of cryptographic hash functions.

8. SHA-512 hashing algorithm used by Bitcoin blockchain to determine the hash of a block. This above statement is True or False.
   a. True
   b. False

Hint: SHA-256 is used in Bitcoin mining to construct the Bitcoin blockchain

9. If a participant node tampers with a block, it results in which action(s).
   a. Modification of hash
   b. Mismatching of hash values
   c. The local chain of node rendered in an invalid state
   d. Only the previous block will be in an invalid state

Hint: In the blockchain network, each block has a hash of the previous block. When someone changes any data in the present block the hash of the block will be changed, this will affect the previous block because it has the address of the previous block.

10. What is the hash value of “swayam” if SHA-256 is used? (case sensitive)
    a. 3bb8668bb7a3f9e127d4429d24ca0de0c3247843ccc528d9612d46d6ad699a63
    b. 4bb8668bb7a3f9e127d4429d24ca0de0c3247843ccc528d9612d46d6ad699a63
    c. 4bb8668bb7a3f9e127d4429d24ca0de0c3247843ccc528d9612d46d6ad699a56
    d. 3bb8668bb7a3f9e127d4429d24ca0de0c3247843ccc528d9612d46d6ad699a92

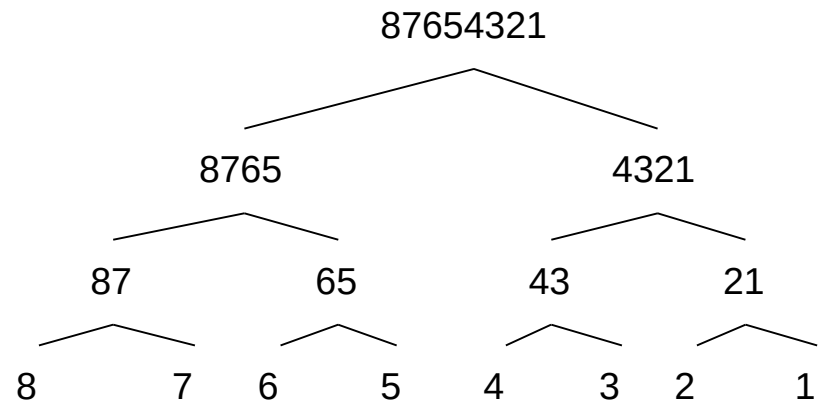
Hint: Verify the result https://emn178.github.io/online-tools/sha256.html

NOC22-CS44: Blockchain and Its Applications
Assignment 2

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. Suppose you have eight data points -- 8 to 1. The post-order traversal of the Merkle Tree is given by (here 8 means hash of 8, 43 means the combined hash of 4 and 3, and so on):
    a. {8, 7, 87, 6, 5, 65, 8764, 4, 3, 43, 2, 1, 21, 4321, 87654321}
    b. {8, 87, 7, 8764, 6, 65, 5, 87654321, 4, 43, 3, 4321, 2, 21, 1}
    c. {1, 2, 12, 3, 4, 34, 1234, 5, 6, 56, 7, 8, 78, 5678, 12345678}
    d. {87654321, 8765, 87, 8, 7, 65, 6, 5, 4321, 43, 4, 3, 21, 2, 1}

Hint:



Post order Traversal : {8, 7, 87, 6, 5, 65, 8764, 4, 3, 43, 2, 1, 21, 4321, 87654321}

2. Which of the following is used to point a block in blockchain:
    a. Hash Pointer
    b. User ID
    c. Transaction ID
    d. Timestamp

Hint: Refer to the Week 1 Slide for Hash Pointer

3. Digital signing of a transaction or document involves hashing the content of the document and then ____.
    a. encrypting it with private key
    b. encrypting it with public key
    c. encrypting it with nonce
    d. rehashing it

Hint: In Digital Signature the message is signed using the Private key and it is verified using the Public key

4. What is the objective of using a digital signature?
    a. It supports the integrity of messages
    b. None of the above.
    c. It supports both user authentication and integrity of messages
    d. It supports user authentication

Hint: Refer to Week 2 Slide for Digital Signature.

5. Digitally signing transactions by sender in Blockchain does not ensure to solve repudiation/ verifiability problems. Is the above statement True or False?
    a. True
    b. False

6. Which are the main Consensus Algorithms?
    a. Proof of Work
    b. Proof of Stake
    c. Proof of Wager
    d. Proof of Mining

Hint: Refer to Week 2 Slide for Consensus Algorithm

7. Which statement(s) is correct for Fischer-Lynch-Paterson impossibility result:
    I. Consensus is impossible with even a single faulty node?
    II. Ensures safety and liveness together
        a. Both are correct
        b. Only I
        c. Only II
        d. Both are incorrect

Hint: Refer to Week 2 Slide for Distributed Consensus. FLP Impossibility Theorem cannot ensure " Safety " and Liveness " together

8. Why is consensus hard?
    I. No notion of global time
    II. faults in network
    III. nodes may crash/ faulty nodes
        a. I, II, II
        b. I, II
        c. I, III
        d. II, III

Hint: Refer to Week 2 Slide

9. In a RSA cryptosystem Alice uses two prime numbers p = 7 and q =17 to generate her public and private keys. If the public key of Alice is 11. Then the private key of Alice is _____.

    Ans: Numerical Answer Type - 35

Hint: In an RSA cryptosystem, for public key: GCD($\phi(n)$, e) = 1
And, for private key: (e * d) mod $\phi(n)$ = 1
Where,
$\phi(n) = (p -1)*(q – 1) = (7 – 1)(17 – 1) =6*16 = 96$
Such that $1 < e, d < \phi(n)$

Therefore, the private key is:
$(11 * d) \bmod \phi(n) = 1$

$\Rightarrow d = 35$

10. A popular public-private key implementation known as Rivest-Shamir-Adelman (RSA) algorithm is used for the Bitcoin and Ethereum Blockchain. True or False?
    a. True
    b. False

Hint: Bitcoin uses Elliptic Curve Digital Signature Algorithm

NOC22-CS44: Blockchain and Its Applications
Assignment 3

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. The transaction Merkle Tree root value in a Bitcoin block is calculated using ____.
    a. Number of transactions
    b. None
    c. Previous block's hash
    d. Hash of transactions

Hint: Transactions are organised as a Merkle Tree. The Merkle Root is used to construct the block hash

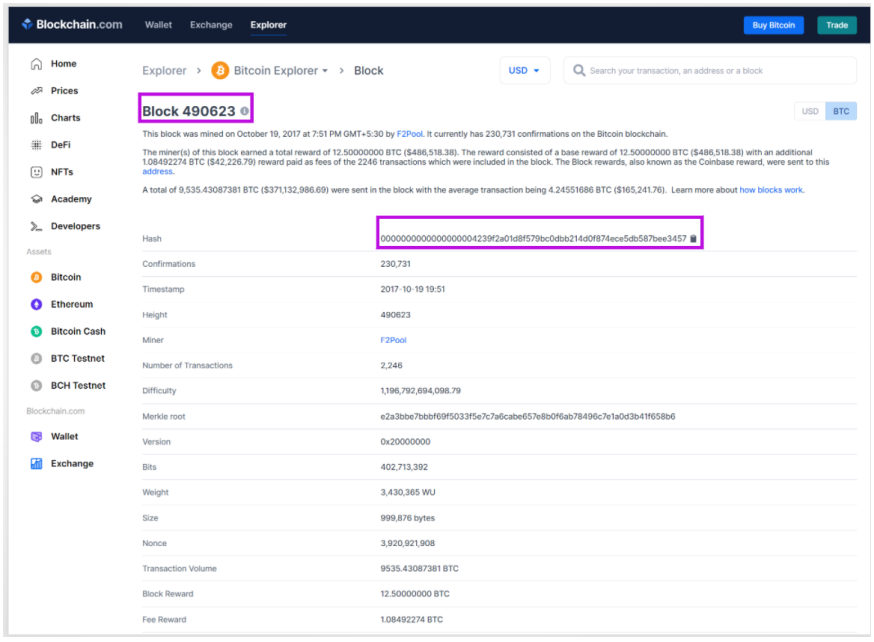
2. Proof of work is the _____ used by Bitcoin blockchain and Ethereum Byzantium Metropolis blockchain.
    a. Transaction confirmation
    b. Incentive function
    c. Consensus Protocol
    d. Trust function

    Hint: In 2008, the whitepaper titled, "Bitcoin: A peer to peer Electronic Cash System" got floated in the internet, in which they used the Proof of Work or Nakamoto Consensus as the consensus protocol.

3. Inspect and explore block #490624 using this link to solve the below question. What is the hash of the previous block for Bitcoin block #490624? Copy and paste the answer into the box below.

    Ans: 00000000000000000004239f2a01d8f579bc0dbb214d0f874ece5db587bee3457

Hint:



4. Bitcoin Scripting Language:
    a. Turing Complete
    b. Supports Cryptography
    c. Stack Based
    d. Supports infinite time/memory

    Hint: Bitcoin Scripts are FORTH like language: simple, compact, stack based and processed left to right.

5. Which of the following bitcoin scripts will generate a TRUE outcome?

    i. scriptSig: <sig>
    scriptPubKey: <pubKey> OP_DUP OP_HASH256 <pubKeyHash> OP_EQUAL OP_VERIFY OP_CHECKSIG

    ii. scriptSig: <pubKey>
    scriptPubKey: OP_HASH160 <pubKeyHash> OP_EQUAL

    iii. scriptSig: <pubKey>
    scriptPubKey: <pubKey> OP_EQUALVERIFY

    iv. scriptSig: <sig>
    scriptPubKey: <pubKey> OP_CHECKSIG

        a. i, ii, iii
        b. iii, iv
        c. i, ii, iv
        d. i, iii, iv

    Hint: Equality is checked between the top two items in the stack

6. What is nonce?
    a. The number miners run through to generate a correct hash
    b. The transaction id number
    c. A miners ASIC chip array
    d. The generator point used in elliptic curve cryptography

    Hint: Miners propose new blocks by solving the puzzle i.e. finding the nonce corresponding to a target block hash, and add that solution as a proof of solving the challenge to be the leader

7. Which one of the following opcodes is needed to remove the top stack item.
    a. OP_DROP
    b. OP_POP
    c. OP_DEQUE
    d. OP_DELETE

    Hint: Refer https://en.bitcoin.it/wiki/Script to get to know more opcodes.

8. Which of these fields is present in a Bitcoin block summary?
    a. Gas Used
    b. Gas Limit
    c. Difficulty
    d. Private Key of the Sender

Hint: The bitcoin block header contains mining statistics timestamp, nonce and difficulty

9. If the four-byte difficulty bits in hex form are 0x1b0404cb, and the target value is calculated using X * 2^(Y), what is the values for X and Y respectively,
    a. X = 0x0404cb, Y = 0x1b
    b. X = 0x0404cb, Y = 0x18
    c. X = 0x0404cb, Y = 0xc0
    d. X = 0x1b0404, Y = 0xcb

Hint: In difficulty = 0x1b0404cb, the exponent is 1b and coefficient is 0404cb
Target = 0x0404cb * 2^(0x08 * (0x1b - 0x03))
On solving the above equation
⇒ target = 0x0404cb * 2^(0x08 * 0x18)
⇒ target = 0x0404cb * 2^(0xc0)

10. In bitcoin block header, the block identifier is calculated
    a. Using Double SHA256 on the current block header
    b. Using SHA256 on the current block header
    c. Using Double SHA256 on the previous block hash
    d. Using Double SHA256 on the Difficulty bits

Hint: Block identifier is calculated by using Double SHA256 algorithm on the current block header

NOC22-CS44: Blockchain and Its Applications
Assignment 4

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. Double spending is reusing digital assets intentionally or inadvertently. True or False?
    a. True
    b. False

    Hint: Double spending is when a person tries to use same bitcoin for more than one Transaction knowingly or accidentally.

2. In blockchain, cryptography ensures authenticity of a transaction, and also helps prevent double-spend. Is the above statement True or False?
    a. True
    b. False

    Hint: Cryptography techniques enforces strong integrity of its transaction record and the validation in longest chain prevents double spending in blockchain

3. Which is/are the example/s of the double-spending attack?
    a. Anita has a total of 80 unspent bitcoins from two different transactions with an equal amount of bitcoins each. She sends the entire amount each to Deepak and Tanmay from one of the transaction
    b. Bibhu bought a car using ‘p’ bitcoins. On delivery, the bitcoins are transferred from his wallet to the shopper’s wallet. Simultaneously, he uses that bitcoins for another purchase
    c. Anita and Bibhu each have 40 unspent bitcoins. Both of them transfer 20 bitcoins to each other
    d. Bibhu has 40 unspent bitcoins. He sends the entire amount each to Deepak and Tanmay

    Hint: Double spending is when a person tries to use same bitcoin for more than one Transaction knowingly or accidentally.

4. The primary difference between the permissionless and permissioned blockchain is _____?
    a. Access control for the participants in the blockchain network
    b. Hash Algorithms
    c. Confidentiality
    d. Availability

    Hint: Permissionless blockchain is an open network, e.g. bitcoin, anyone can join, transact, leave and rejoin the network whereas permissioned blockchain is a closed network e.g. Hyperledger. Both the network uses same hash algorithms and offer confidentiality and availability.

5. What is an advantage of a permissionless blockchain?
    a. It does not use disinterested third parties to secure blocks, as all participants have a vested interest.
    b. It is more resilient against fraud, because it uses federated nodes to combat fraud.
    c. It is open to everyone in the world without permission and licensing requirements.
    d. Its networks are built by for-profit companies and the working of the network is guaranteed.

    Hint: Refer to the Week 4 Slide

6. After a hard fork, the emerging two chains are incompatible. True or False?
    a. True
    b. False

    Hint: After adding a new rule to the code, it creates a fork in the blockchain: one path follows the updated blockchain, and the other path continues along the old path, hence incompatible with each other. After a short duration, those on the old chain will realise that their version of the blockchain is outdated and quickly upgraded to the latest version.

7. Which transaction(s) is/are valid with the current blockchain?
    a. No conflict with other transactions
    b. No double spending
    c. No infinite loops
    d. All of the above

    Hint: Refer to the Week 4 Slide

8. Bitcoin protocol runs over
    a. TCP
    b. UDP
    c. HTTP
    d. HTTPS

    Hint: Bitcoin protocol runs over TCP as reliability is required for transactions.

9. What it the correct order of adding a new block to blockchain
        i. Block Mining
        ii. Block propagation
        iii. Block Flooding
        iv. Transaction Flooding

    a. iii, iv, ii, i
    b. iv, iii, ii, i
    c. ii, i, iii, iv
    d. iv, i, iii, ii

    Hint: Refer to the Week 4 Slide

10. What are Bitcoin exchanges available in India:
    a. Coinbase
    b. CoinDCX

c. UNOCoin
d. CoinSwitch Kuber

Hint: Refer to this post.

NOC22-CS44: Blockchain and Its Applications
Assignment 5

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. What is the limitation of using the consensus algorithm Proof of Work (PoW) with respect to Proof of Elapsed Time (PoET) ?
    a. PoET can often be used in a permissionless blockchain more easily than PoW, because PoET's lottery system for node selection is secure.
    b. PoET has generally lower transaction costs than PoW
    c. PoET is much more secure than PoW, because PoET supports the trusted execution environment (TEE) by time-stamping the transactions.
    d. PoET is usually faster than PoW, because fewer nodes compete for validation than in PoW, since PoET randomly selects the nodes.

Hint: PoET has lower transaction costs than PoW due to the hardware required for PoET is more specific than the hardware needed for PoW. Also the lower no of competing nodes makes PoET faster than PoW.

2. "A low-cost and fast consensus algorithm, where a node needs to deposit cryptocurrency to guarantee the transaction." The above description defines which consensus algorithm?
    a. Proof of Work (PoW)
    b. Proof of Burn (PoB)
    c. Proof of Stake (PoS)
    d. Proof of Elapsed Time (PoET)

    Hint: Refer to the Week 5 Lecture slide for definition of PoS.

3. What is the correct sequence involved in a block creation:
    1. Transactions validated
    2. Transactions Bundled & broadcasted
    3. Transaction initiated
    4. Block added to the local chain and propagated to the network.
    5. Proof of work consensus problem solved
        a. 5,3,1,2,4
        b. 1,2,3,4,5
        c. 3,1,2,5,4
        d. 3,2,1,4,5

    Hint:

1. First a transaction is initiated i.e. a block representing the transaction is created
2. The block is sent to every nodes in the network, which validate the transactions
3. The validated transactions bundled and broadcasted in the network
4. The miner tries to solve the PoW consensus problem
5. Finally the block is added to the local chain and propagated to the network.

4. Proof of Burn consensus algorithms consider virtual resources or digital coins for participating in the mining activity? True or False?
    a. True
    b. False

    Hint: Proof of Burn consensus algorithms consider virtual resources or digital coins for participating in the mining activity unlike PoW which used real resource.

5. 1 ether equals
    a. 10 ^ 16 wei
    b. 10 ^ 18 wei
    c. 10 ^ 6 wei
    d. 10 ^ 8 wei

    Hint: Ether to Wei converter: https://eth-converter.com/

6. How an attacker could manipulate the transaction history of a blockchain to be able to spend a token or a cryptocurrency twice.
    a. The attacker modified the transaction on his node and propagated it in the network.
    b. The attacker modified the smart contract and recovered the investor's cryptocurrency.
    c. The attacker gained control of more than 51% of the network's computing power.
    d. The attacker hard-forked the network and created a new blockchain network.

    Hint: Refer to the Week 5 Lecture slide for 51% attack.

7. What is the CLI command used to send ethers after the nodes have been initialized?
    a. eth.submitTransaction()
    b. eth.sendIBANTransaction()
    c. eth.sendRawTransaction()
    d. eth.sendTransaction()

    Hint: Once the transaction is prepared using syntax

    var **transaction** = {from: "0x7dad3a076678a05b2b4e2b93206dbecef0d7b0",
    to:"0x35F18427567108F800BDC2784277B9246eED3A" ,
    value: Web3.utils.numberToHex(10000000000000000) },

    it can be sent using:

    web3.eth.sendTransaction(transaction).then(console.log)

8. What library/API is used for smart contract deployment and invocation from Dapp ?
    a. web3
    b. admin
    c. eth
    d. Contract

    Hint: web3 is the Collection of libraries that allow you to interact with a local or remote ethereum nodes

9. In which scenario is a smart contract the best solution to the problem?
    a. A restaurant manager wants to force customers to pay for their food by transferring cryptocurrency to his wallet.

b. A chief engineer wants her smart watch to notify her when her partner enters their front door.
c. A grid company wants to automatically buy power when the price reaches a predetermined rate.
d. An insurance company wants to pay out a small vendor whenever the case manager feels it is best to do so.

Hint:
Option a is incorrect. Because Smart contracts do not force another party to transfer funds.
Option b is incorrect. Because a smart contract is a contract between two or more parties. Here, there is no second party, hence a smart contract is not suitable.
Option d incorrect. Because, Smart contracts get triggered by events that are predetermined. The willingness of a company does not automatically trigger the code.

10. Which of the following syntax is correct to write data in a smart contract using solidity
    a. myContract.methods.store("99").send()
    b. myContract.methods.write("99").send()
    c. myContract.methods.write("99").set()
    d. myContract.methods.store("99").set()

Hint: Please refer to the Week 5 Lecture slides on how to execute smart contract.

NOC22-CS44: Blockchain and Its Applications
Assignment 6

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. If there are 24 faulty nodes (crash fault) in asynchronous CFT, at least how many nodes needed to reach consensus
    a. 48
    b. 49
    c. 50
    d. 51

    Detailed Solution:
    2f + 1 = 2*24 + 1 = 48 + 1 = 49

2. In Paxos, a node can have only one role among the three roles at a time. True or False
    a. False
    b. True

    Detailed Solution:
    In typical paxos implementations, a single processor may play more than one role at the same time.

3. Can we reach a consensus when there is one commander, one good lieutenant, and one faulty lieutenant in a .Byzantine Generals Problem. Yes or No?
    a. Yes
    b. No

    Detailed Solution:
    One fault.
    Total nodes required = 3f + 1 = 3 + 1 = 4 . But we have 3 nodes.

4. If there are 24 faulty nodes in, at least how many nodes needed to reach consensus in the Byzantine Fault Tolerance (BFT) system.
    a. 72
    b. 73
    c. 48
    d. 49

    Detailed Solution:
    f = 24
    Total nodes required = 3f + 1 = 72 + 1 = 73

5. Which are the examples of the synchronous consensus techniques?
    a. RAFT
    b. PAXOS
    c. Byzantine General Model
    d. Practical Byzantine General Model

    Detailed Solution:
    RAFT, PAXOS, Byzantine General Model and PBFT , all are synchronous consensus techniques.

6. Suppose you execute your tasks distributedly from six different systems at six different locations. For maintaining the consensus among the systems, you are using the BFT model. You found that one system is permanently failed due to a hardware fault and another system is compromised by an attacker. Does your system correctly work at all?
    a. No
    b. Yes with the remaining nodes
    c. Yes with all the nodes

7. Which of the statements are true?
    a. Paxos is based on state-machine replication
    b. In Paxos, Proposers and Learners maintain a state of the running epochs
    c. In a Paxos, once a consensus is reached, Paxos cannot progress to another consensus
    d. Paxos works in two rounds

    Detailed Solution:
    In Paxos, Learners do not need to maintain a state of the running epochs. Therefore b is False.

8. State machine replication-based consensus is used over permissioned blockchains. Select the suitable reason(s)?
    a. The network is closed, and the nodes know each other, hence state replication is possible among the known nodes
    b. Not need to spend power, time, or bitcoin
    c. Machines can behave maliciously, hence consensus in required
    d. State machine replication-based consensus is not recommended to use over permissioned blockchains.

    Detailed Solution:
    A. and B. are true as nodes know each other and state machine replication does not need to spend power, time like in Proof of Work.
    C. is false because even if machines do not behave maliciously, consensus is required for crash faults.
    D. is false because it is recommended to use state machine replication based consensus over permissioned blockchains.

9. Which are the properties of an asynchronous consensus:
    a. Validity
    b. Agreement
    c. Termination
    d. Integrity

    Detailed Solution:
    All the options are correct.
    Validity: If all correct process proposes the same value v, then any correct process decides v
    Agreement: No two correct processes decide differently.
    Termination: Every correct process eventually decides.
    Integrity: If all the correct processes proposed the same value v, then any correct process must decide v. (Same as validity)

10. The following code snippet from paxos algorithm belongs to which phase?

```
is the ID the largest I have seen so far, max_id == N?
if yes
      reply with an ACCEPTED message & send ACCEPTED(ID, VALUE) to
all learners
if no
      do not respond (or respond with a "fail" message)
```

    a. PREPARE-PROMISE
    b. PROPOSE-ACCEPT

    Detailed Solution:

    Refer to Lecture 28 - Paxos. The steps in the code snipped belongs to the PROPOSE-ACCEPT phase of Paxos.

NOC22-CS44: Blockchain and Its Applications
Assignment 7

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. Which statement(s) are true about Byzantine Dissemination Quorum:
   a. Any two quorums have at least one correct replica in common
   b. There is always a quorum available with no faulty replicas
   c. Any two quorums have at most one correct replica in common
   d. There is always a quorum available with some faulty replicas

   Detailed Solution:
   Refer to Lecture 31: Byzantine Dissemination Quorum:
   Intersection: Any two quorums have at least one correct replica in common.
   Availability: There is always a quorum available with no faulty replicas

2. If you have f number of faulty nodes, then you need at least how many replicas to reach consensus irrespective of crash fault or byzantine fault.
   a. 2f + 1
   b. 3f + 1
   c. f +1
   d. 3f

   Detailed Solution:
   Considering byzantine fault, 3f + 1 replicas are required to reach consensus. This is greater than 2f + 1 replicas which is enough to handle crash faults too.

3. What is the correct sequence of operations in PBFT algorithm
   i. Prepare
   ii. Reply
   iii. Commit
   iv. Pre-Prepare

   a. iv, i, ii, iii
   b. iv, i, iii, i
   c. i, iv, ii, iii
   d. I, ii,iv, iii

4. PBFT is safe under_____quorum over an asynchronous environment
   a. 2f+1
   b. 3f+1
   c. f+1

d. f

Detailed Solution:
Refer to Lecture 31:
You have f number of faulty nodes – you need at least 2f + 1 quorum in pbft.

5. What are Hyperledger frameworks used for?
   a. Hyperledger frameworks are primarily used for building permissioned blockchains for organizations.
   b. Hyperledger frameworks are primarily used for building public blockchains.
   c. Hyperledger frameworks are used for only building smart contracts for IBM's blockchain.
   d. Hyperledger frameworks are primarily used for building smart contracts for public blockchains

Detailed Solution:

Refer to Lecture 34: Fabric is primarily used for building permissioned blockchains for organizations. It is an open source project so anyone can use it to build a permissioned blockchain and deploy smart contracts on it.

6. Which of the following(s) is/are benefits of Blockchain for Business
   a. Reduced transaction time from days to near instantaneous
   b. Removes intermediaries overheads and cost
   c. Enables NewBusiness Models such as IoT Integration into supply chain
   d. All of the above

Detailed Solution:
Refer to Lecture 33. The benefits of enterprise blockchains include reduced transaction time, removal of intermediaries, and new business models such as IoT integration in supply chain.

7. Which of the following is an open source, enterprise-grade Permissioned DLT platform
   a. Hyperledger Fabric
   b. Hyperledger Explorer
   c. Hyperledger Burrow
   d. Hyperledger Indy

Detailed Solution:

Only Fabric is an enterprise-grade permissioned DLT Platform.

Explorer is a tooling to inspect blockchains.

Burrow is not an enterprise grade DLT since it uses EVM which has certain limitations in developing smart contracts.

Indy is a specialized DLT for identity management.

8. Which of the following abstractions in Hyperledger Fabric provide confidentiality to individual ledgers ?
    a. Ordering Services
    b. Peers
    c. Channels
    d. Endorsement Policies

    Detailed Solution:

    Refer to Lecture 35: Fabric channels refer to different separate ledgers such that only organizations belonging to a particular channel can read/write to that ledger.

9. Suppose there are 5 channels present in a Hyperledger Fabric network, each of them has access to 3 chaincodes A, B and C. How many containers will run in each peer for running this system?
    a. 5
    b. 1
    c. 3
    d. 15

    Detailed Solution:

    Per peer 3 containers will be running, that is one for each chaincode.

10. Hyperledger Fabric only allows Proof of Work consensus to be plugged in to ensure a high degree of trustworthiness. True or False
    a. False
    b. True

    Detailed Solution:

    Hyperledger fabric is modular, and the consensus protocol is a pluggable component. Therefore any other consensus protocol such as PBFT can be plugged in and used.

NOC22-CS44: Blockchain and Its Applications
Assignment 8

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. Which statement(s) are true about Byzantine Dissemination Quorum:
    a. 5
    b. 1
    c. 3
    d. 15

    Modification:

    i. Any 2 quorums have at least one correct replica in common
    ii. Any 2 quorams have at most one correct replica in common
    iii. If you have 3 numbers of faulty nodes you need at least 10 replicas to reach consensus.
    iv. PBFT uses Byzantine Dissemination Quorum with 2f + 2 replicas
    a. i, ii
    b. ii, iv
    c. Only iii
    d. Only iv

    To reach consensus with f number of faulty nodes, you need at least 3f + 1 replicas

2. Hyperledger Fabric only allows Proof of Work consensus to be plugged in to ensure a high degree of trustworthiness. True or False
    a. False
    b. True

    Hyperledger Fabric supports pluggable implementations of different components such as identity management, consensus algorithm etc to ensure confidentiality, resiliency and scalability.

3. Alice wants to interact with an Ethereum Network. Which of the following are required to do that?
    a. web3.js
    b. nodejs
    c. geth
    d. bitcoin

    Refer to Lecture 36:

    When a user wants to Interact with an Ethereum Network it is required to have a web app and a node with geth installed.

4. The command : geth –goerli --syncmode "fast" will
    a. Will downloads all blocks excluding headers, transactions, and receipts and will generate the state of the blockchain incrementally by executing every block.
    b. Will downloads all blocks including headers, transactions and receipts, will verify all headers, and downloads the state and verify it against the headers.
    c. Will downloads all blocks including headers, transactions, and receipts and will generate the state of the blockchain incrementally by executing every block.
    d. Will downloads all block headers, block data, and verifies some randomly.

    Refer to Lecture 36:

    Sync modes You can start Geth in one of three different sync modes using the syncmode "<mode>" argument that determines what sort of node it is in the network

5. Which of the following is an open, scalable consensus algorithm having low transaction throughput?
    a. PoW
    b. PoS
    c. PBFT
    d. PoB

    Refer to Lecture 38

6. In a bitcoin network, the block size is 1.229MB and average transaction size is 729B. What is the transaction throughput value (transactions per second).

    Ans(Fill in the blanks): 2.946

    Block Size = 1MB

    1MB = 1048576

    Average Transaction Size = 380.04B

    Number of Transaction per Block = Block Size/Average Transaction Size

    = 1048576 / 380.04

    Block Size = 1.229MB = 1288699.904 B

    Transaction / sec = TPS = 1288699.904 / (729 * 600) = 2.946

7. Which of the following protocols ensure total ordering of transactions and consensus finality.
    a. BFT
    b. PoW
    c. PoET
    d. PoB

Refer to Lecture 38

8. Which statements are true about the Nakamoto Consensus?
    i. Provide transaction scalability
    ii. Prevents consensus finality
    a. i, ii
    b. i
    c. ii
    d. None of the above

    Nakamoto Consensus or PoW is a randomised protocol which does not ensure consensus finality

9. In the CoSi Protocol, the second CoSi round to implement PBFT's which phase(s)? You can choose multiple options if applicable.
    a. commit phase
    b. pre-prepare phase
    c. prepare phase
    d. learning phase

    Refer to Lecture 40

    One CoSi round to implement PBFT's pre prepare and prepare phases and second CoSi round to implement PBFT's commit phase

10. Running a chaincode in hyperledger fabric involves the following steps:
    i. Instantiation of Chaincode of Channel
    ii. Creation of Channel
    iii. Configuring Orderer and Peer nodes
    iv. Adding members to Channel
    v. Installing chaincode on peers

    Which of the following sequence of steps is valid?
        a. ii, iv, iii, i, v
        b. iii, v, ii, iv, i
        c. ii, iv, iii, v, i
        d. iii, v, i, ii, iv

Refer to Lecture 35

NOC22-CS44: Blockchain and Its Applications
Assignment 9

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. Which of following statements are the true for PBFT
    a. It requires a dynamic consensus group
    b. For scalability it requires O(n) for communication complexity
    c. create multiple pseudonymous identities to subvert the 3f+1 requirements of PBFT
    d. None of the above

In PBFT coin their assumption is standard to the normal PBFT system that you have a 3f+1 static group of "trustees" who are there, who will run the PBFT to withstand f number of failures. So, to sustain f number of failures you would require 3f plus 1 number of nodes in the system. The pBFT mechanisms are vulnerable to Sybil attacks, where a node can create multiple pseudonymous Identities. Hence, the node can create multiple such identities to subvert that the 3f+1 requirement of PBFT.

2. Which of the following sequence of steps is valid for Algorand?
    i. A block is prepared
    ii. Run Byzantine agreement on the block
    iii. Prepare the digital signature and propagate
    iv. Block is propagated through gossiping

    a. i, iv, ii, iii
    b. i, ii, iv, iii
    c. i, ii, iii, iv
    d. I, iii, ii, iv

- **A random user prepares a block**
- **Propagate the block through gossiping**
- **To validate the block created by the random user(can be valid or adversarial user), a byzantine agreement is required**
- **Once it is found that the block is valid, then it is digitally signed and propagate the digital signature in the network.**

3. Strong Synchrony ensures liveness of protocol Algorand. True or False
    a. True
    b. False

To achieve liveness, Algorand makes a "strong synchrony" assumption that most honest users (e.g., 95%) can send messages that will be received by most other honest users (e.g., 95%) within a known time bound.

4. Algorand is not always safe under weak synchrony. True or False
    a. True
    b. False

    Algorand achieves safety with a "weak synchrony" assumption: the network can be asynchronous (i.e., entirely controlled by the adversary) for a long but bounded period of time(e.g., at most 1 day or 1 week). After an asynchrony period, the network must be strongly synchronous for a reasonably long period again (e.g., a few hours or a day) for Algorand to ensure safety. The weak synchrony assumption is that in every period of length b (think of b as a day or a week), there must be a strongly synchronous period of length s < b (an s of a few hours suffices).

5. Which of the following is true about the selection of the random committee in the Algorand network?
    a. There is a dedicated node which chooses the nodes to form the committee
    b. A distributed algorithm decides the list of nodes participating in the committee
    c. The nodes elect themselves as a committee member by winning a local computation
    d. A specific pool of node choose are given the responsibility of forming the committee

    Algorand is an open model which mean anyone can join the network. Also it is A and permissionless model i. It can not have a single node who will select the committee. Cryptographic sortition is used to elect the user to be part of the committee. In which every user can elect himself as the part of the committee. The individual committee members run certain local computation on their own machine to find out whether they won the lottery or not. If they won, they can participate.

6. Which of the following is not a valid component in Distributed Identifiers(DID) Architecture.
    a. DID Controller
    b. DID Validator
    c. Verifiable Data Registry
    d. DID Subject

    Refer to Week 9 slide

7. Consider the following statement - "Say Alice has generated two Distributed Identifiers (DID) DID1 and DID2 for three of her pairwise relationships maintained in Hyperledger Indy". Which part of the above statement is false with respect to the concepts of Hyperledger Indy?
    a. Generation of DID by Alice
    b. Two DID(s) for 3 pairwise relationships
    c. The above statement is completely correct
    d. Both parts of the statement are wrong

    Refer to Week 9 Lecture Notes

8. In Verifiable Credential (VC), a claim is a statement about a _____
    a. Holder

b. Issuer
c. Subject
d. Verifier

Refer to Week 9 Lecture Notes.

9. Which of the following statements is/are true
   I. In Hyperledger Indy, any party can read the ledger.
   II. In Hyperledger Indy, only registered parties and can write to the ledger.

   a. I
   b. II
   c. I, II
   d. None of the above

Hyperledger Indy is a public permissioned ledger based registry which is readable to all but only a group of selected entities can write.

10. Which of the following sequence of steps is valid for DID Registration?
    i. Register DID
    ii. Create DID Document
    iii. Fetch DID Document
    iv. Update DID Document

    a. ii, i, iv, iii
    b. ii, iv, iii, i
    c. ii, iv, i, iii
    d. I, ii, iii, iv

Refer to Week 9 Lecture Notes