1. Which of the following is/are example(s) of distributed systems?
    a. Web browser
    b. E-commerce platforms
    c. Amazon Web Services
    d. Email

    Ans: b and c

2. Consider the `fork()` system call in Unix-based operating systems. How many processes are created from the following executions of the `fork()` system call?

```
int main() {
      fork();
      fork();
      return 0;
}
```

    a. 2
    b. 4
    c. 6
    d. 8

    Ans: b

3. What is the output of the following piece of code written in C programming language?

```
int swap(int a, int b) {
      int temp;
      temp = a;
      a = b;
      b = temp;
}

int main() {
      int x = 10, y = 20;
      swap(x, y);
      printf("%d %d", x, x);
      return 0;
}
```

    a. 10 20
    b. 20 10
    c. 10 10
    d. 20 20

    Ans: c

4. Which of the following network protocols is used to get the MAC address of a network interface from its IP address?
    a. DNS
    b. ARP
    c. RARP
    d. TELNET

    Ans: b

5. Consider that the IP address of a network is 202.141.80.20 and the subnet mask is 255.255.255.0. How many hosts are supported by this network?
    a. 256
    b. 254
    c. 128
    d. 126

    Ans: b

6. Which of the following is/are used in operating systems to solve the mutual exclusion problems for critical sections?
    a. Semaphore
    b. Spinlocks
    c. Process states
    d. Deadlock detection

    Ans: a and b

7. What is Belady's anomaly?
    a. Increase in a process's time quanta will increase in deadlock possibility
    b. Increase in a process's time quanta will decrease in deadlock possibility
    c. Increase in the number of pages will increase the page fault
    d. Increase in the number of pages will decrease the page fault

    Ans: c

8. What is the default port address for HTTPS?
    a. TCP port 8080
    b. UDP port 80
    c. TCP port 443
    d. UDP port 443

    Ans: c

9. Which of the following IP addresses cannot be used to host a web server that needs access from a public Internet?
    a. 202.141.80.9
    b. 10.10.178.2
    c. 152.58.9.9
    d. 8.8.8.8

    Ans: b

10. What is the purpose of the `connect()` system call?
    a. To accept an incoming TCP connection
    b. To accept an incoming UDP connection
    c. To create a TCP connection to a given IP address/Port
    d. To create a UDP connection to a given IP address/Port

    Ans: c

1. What are the features of a hash function?

    a. Puzzle-friendly
    b. Collision-resistance
    c. Deterministic
    d. Post image resistance

Hint: except d all are the properties of cryptographic hash functions.

2. For a SHA 256 bit hash function, the attacker needs to compute how many hash operations in order to find two matching outputs?

    a. 0.3×2^{128}
    b. 0.2×10^{50}
    c. $0.25X2^{130}$
    d. 1×2^{256}

Hint: If a hash function produces N bits of output, an attacker needs to compute only $2^{N/2}$ hash operations on a random input to find two matching outputs. $2^{256/2} = 2^{128} =$
=(0.25)X2^130

3. What is the hash value of 6666 if SHA-256 is used?
    a. d7697570462f7562b83e81258de0f1e41832e98072e44c36ec8efec46786e24e
    b. d7597570462f7562b83e81258de0g1e41832e98072e44c36ec8efec46786e24e
    c. c7697570462f7562b83e81258de0f1c41832e98072e44c36ec8efec46786e24e
    d. d7697570462f7562m83e81258de0f1e41832e98072e44c36ec8efec46786e24es

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

4. Which of the statements below is/are true for decentralized distributed systems?
    a. Players may or may not trust each other
    b. Players must trust each other
    c. Central body should govern the communication
    d. None of the above

Hint: Answer a. Every participant may not trust each other

5. Miner nodes only execute new transactions but can not verify previous transaction hash?
    a. True

b. False

Hint: Answer b. miners can verify previous transaction hash and create new transactions

6. Which of the following is/are true for blockchains?
   a. Works based on Push technique
   b. Existing data can be deleted easily
   c. Tamper-proof
   d. None of the above

Hint: Answer a,c.

7. Where are the ledger logs stored in a blockchain?
   a. On a SQL Database
   b. On a central immutable ledger
   c. On a metadata table
   d. In ledger of each peer

Hint: Each peer keeps the log

8. Which of the following is an avalanche effect to 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 large change the hash value
   d. None of the above

Hint: answer is c.

9. Genesis blocks may not contain the
   a. First transaction
   b. First transaction block
   c. Last transaction block
   d. None of the above

Hint: answer is c. The Genesis block always contains the first transaction block but not necessarily the last one.

10. Which of the below is/are blockchain based app examples?
    a. Cross-border payments
    b. Supply chain
    c. Anti-money laundering tracking system
    d. UTXO

Hint: answer is a,b,c. UTXO is feature for handing unspent amount, it is not an blockchain app

Blockchain and Its Applications
Assignment 2

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

1. Alice employs the RSA cryptosystem with the prime numbers p = 7 and q = 17 to derive her public and private keys. Given that Alice's public key is 11, her corresponding private key is _____.

   Ans: Numerical Answer Type - 35

2. Bob wishes to send a lengthy message to Alice with the requirement that Alice can verify its origin and Bob cannot later disown the message. They also want to ensure the confidentiality of the message. Alice and Bob decide to employ public key cryptography and cryptographic hashing techniques. Let the key pairs for Alice and Bob be (Pub A, Pri A) and (Pub B, Pri B) respectively, and let E, D, and H denote the encryption, decryption, and hash functions respectively. M represents the message, and H(M) is its digest. Which of the following outlines the correct sequence of steps for Alice to send the digitally signed message?

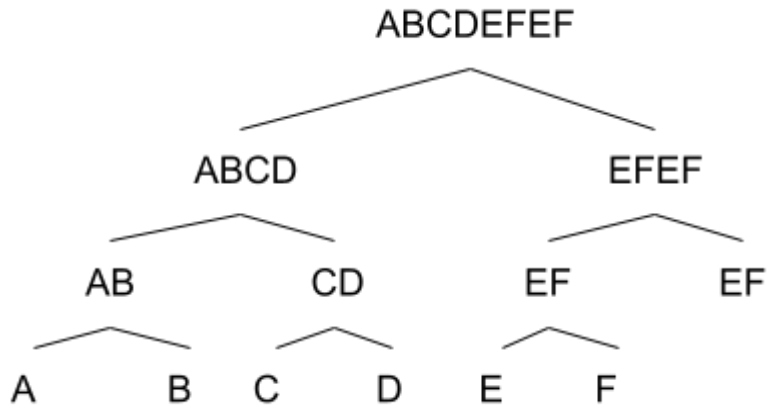
   i. At Bob: M' = E(M, K_{pubA})
   ii. At Alice: M = E(M', K_{priA})
   iii. Bob sends the message M' to Alice
   iv. The signature along with the message is sent to Alice (M, M')
   v. Bob: M' = E(M, K_{priB})
   vi. Signing the message with his private key: S = E(H(M), K_{priB})
   vii. M = E(M', K_{pubB})

   a. v, vii, ii, i, iii, iv, vi
   b. i, iii, ii, v, iv, vii, vi
   c. i, ii, iii, iv, v, vi, vii
   d. vii, vi, v, iv, iii, ii, i

3. The act of digitally signing transactions by the sender in Blockchain ensures the resolution of repudiation/verifiability problems.
   a. True
   b. False
4. Which of the following is used to point to a block in the blockchain:
   a. Hash Pointer
   b. User ID
   c. Transaction ID
   d. Timestamp
5. Suppose you have 6 data points -- A to F. The post-order traversal of the Merkle Tree is given by (here A means hash of A, DC means the combined hash of D and C, and so on):
   a. {ABCDEFEF, ABCD, EFEF, AB, CD, EF, EF, A, B, C, D, E, F}
   b. {A, AB, B, C, D, CD, ABCD, E, F, EF, ABCDEF}

c. {A, B, AB, C, D, CD, ABCD, E, F, EF, GH, EFGH, ABCDEFGH}
d. {A, B, AB, C, D, CD, ABCD, E, F, EF, EF, EFEF, ABCDEFEF}

Hint:



Post order Traversal : {A, B, AB, C, D, CD, ABCD, E, F, EF, EF, EFEF, ABCDEFEF}

6. Which of the following is true for using a digital signature in blockchain?
   a. To check the validity of the source of a transactions
   b. None of the above.
   c. It will ensures that no one can deny of their own transaction
   d. It supports user authentication

Hint: Refer to Week 2 Slide for Digital Signature.

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

Hint: PoW and Pos are the main consensus algorithms

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

Hint: Due to a lack of global timing reference, and various kinds of faults it is very difficult to agree with nodes unanimously.

9. The Liveliness property ensures the output should be produced within a finite time limit?
   a. False
   b. True

Hint: Refer to Week 2 Slide, liveliness property talks about eventual termination.

10. Paxos consensus support(s) which of the below properties
    e. Liveliness
    f. Safety
    g. Both
    h. None of the above

Hint: Refer to Week 2 Slide, Paxos supports safety but not liveliness.

Blockchain and Its Applications 2024
Assignment 3

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

1. Inspect and explore block #828070 using this link to solve the below question. What is the hash of the previous block for Bitcoin block #828070? Copy and paste the answer into the box below.
    a. 00000000000000000000246ef8870310474e18acbd1fd8453abbb6f367f74816f
    b. 000000000000000000001d857c22ab5211e2173e4f970eb15f04f64e692587aa1
    c. 000000000000000000034511894ee97dfa62803bb338335a12e40f6e5a451720
    d. 000000000000000000002c2c0e69e794d1968382626109ed1d6441020105e7d4e

2. Which of the following Bitcoin scripts will generate a **TRUE** outcome?
    a. scriptSig: <sig>
    scriptPubKey: <pubKey> OP_DUP OP_HASH256 <pubKeyHash> OP_EQUAL OP_VERIFY OP_CHECKSIG
    b. scriptSig: <pubKey>
    scriptPubKey: OP_HASH160 <pubKeyHash> OP_EQUAL
    c. scriptSig: <pubKey>
    scriptPubKey: <pubKey> OP_EQUALVERIFY
    d. scriptSig: <sig>
    scriptPubKey: <pubKey> OP_CHECKSIG

    A. a, b, c
    B. c, d
    C. a, b, d
    D. a, c, d

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

4. If the six-byte difficulty bits in the hexadecimal form are 0x1a05f20881ab, and the target value is calculated using X * 2^(Y), what are the values for X and Y respectively?

a. X = 0x5f20881ab, Y = 0x1a
b. X = 0x1a05f2, Y = 0x0881ab
c. X = 0x1a05f2, Y = 0x18
d. X = 0x5f20881ab, Y = 0x1a0

5. DLT can be used to maintain financial information only.
    a. False
    b. True

6. Which one of the following opcodes is needed to remove the second-to-top stack item?
    a. OP_DELETE
    b. OP_2POP
    c. OP_DEQUE
    d. OP_NIP

7. Bitcoin Scripting Language:
    a. Not Turing Complete
    b. Supports Cryptography
    c. Queue Based
    d. Supports infinite time/memory

8. Permissioned blockchain is regarded as more secure than open blockchain as the participants are known beforehand and pre-authenticated.
    a. True
    b. False

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

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

NOC22-CS44: Blockchain and Its Applications
Assignment 4

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

1. 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 realize that their version of the blockchain is outdated and quickly upgraded to the latest version.

2. Which is/are the possible example/s of a double-spending attack?
    a. Sammy has a total of 90 unspent bitcoins from two different transactions with an equal amount of bitcoins each. He tries to send the entire amount at a time each to Nikita and Ayush as transactions

    b. Brady bought a car using 'm' bitcoins. On delivery, the bitcoins are transferred from his wallet to the dealer's wallet.

    c. Karan has 180 unspent bitcoins. He sends the equal amount each to Dev and Tarun one by one

    d. Deepak has 20 unspent bitcoins. He tries to transfer those 20 bitcoins to his two each of his friends simultaneously.

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

3. Blocks of a blockchain?

    a. Transaction data
    b. Hash
    c. Time stamp
    d. None of the above

    Hint: All of a,b,c

4. What are some Bitcoin exchanges available in India*: Please select the most appropriate choice among the options.*
    a. BuyUCoin

b. ZebPay
c. WazirX
    i. a and b
    ii. b and c
    iii. a and c
    iv. a, b and c

Hint: Refer to this post.All of a,b.c are correct.

5. “We can achieve consensus with a single crash failure in a perfect asynchronous network.” This scenario is _____?

    a. Always true
    b. Sometimes true
    c. Can’t say
    d. Impossible

    Hint: As The Impossibility Theorem states Consensus is not possible in a perfect asynchronous network even with a single crash failure

6. What is 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, i, iii, ii
    c. iv, iii, ii, i
    d. ii, i, iii, iv

    Hint: Refer to Week 4 Slide

7. 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.

8. The primary difference between the permissionless and permissioned blockchain is _____?

    a. Hash Algorithms
    b. Confidentiality
    c. Availability
    d. Access control for the participants in the blockchain network

    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 networks use the same hash algorithms and Offer confidentiality and availability.

9. 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 open to everyone in the world without permission and approval requirements.
    c. It is more resilient against fraud because it uses federated nodes to combat fraud.
    d. Its networks are built by for-profit companies and the working of the network is guaranteed.

    Hint: Refer to the Week 4 Slide

10. Bitcoin protocol directly runs over

    i. TCP
    ii. HTTP
    iii. HTTPS

    a. i, ii, iii
    b. Only ii
    c. Only i
    d. All of the above

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

NOC22-CS44: Blockchain and Its Applications
Assignment 5

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

1. The height of the block is the ____ in the chain between it and the genesis block.
    a. Metafiles
    b. Hash
    c. Log size
    d. Number of blocks

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

    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)

3. Which of the following syntax is correct to write data in a smart contract using solidity
    a. myContract.methods.store("55").set()
    b. myContract.methods.write("55").send()
    c. myContract.methods.store("55").send()
    d. myContract.methods.write("55").set()

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

4. What is the limitation of using the consensus algorithm Proof of Work (PoW)?
    a. A lot of mining power is wasted as only one gets success in mining at a time
    b. PoW is used for permissioned blockchain
    c. It is used for blockchain mining
    d. High transaction throughput

    Hint: Please refer to the slide Week 5 slide. The PoW has limitation of wastage of power and low throughput.

5. Which statement(s) is/are true for PoS(Proof of Stake) consensus?
    a. Depends on the work done by the miner
    b. Depends on the amount of crypto currency the miner holds
    c. Provides less protection in general
    d. None of the above

Hint: Refer to the Week 5 Lecture slide for description of PoS. Amount of bitcoin that the miner holds decides its stake.

6. Which of the following is/are applicable for PoET(Proof of Elapsed Time) consensus
    a. Each participant in the blockchain network waits a random amount of time
    b. The first participant to finish becomes the follower for the new block
    c. Trusted execution platform and attestation are used to verify that the proposer has really waited
    d. The first participant to finish becomes the leader for the new block.

Hint:POET uses a trusted execution platform, say as Intel SGX and H/W attestation. Please refer to the slide for details.

7. Proof of Burn consensus algorithms also consider virtual resources or digital coins for participating in the mining activity?
    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 uses real resources.

8. 15 ether equals
    a. 15X(10 ^ 16) wei
    b. 15X(10 ^ 18) wei
    c. 15X(10 ^ 6) wei
    d. 15X(10 ^ 8) wei

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

9. How an attacker could manipulate the transaction history of an existing blockchain
    a. The attacker hard-forked the network and created a new blockchain 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 gained control of less than 49% of the network's computing power.

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

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

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

Blockchain and Its Applications
Assignment 6

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

1. If there are 25 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*25 + 1 = 50 + 1 = 51

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. If there are 25 faulty nodes in, at least how many nodes needed to reach consensus in the Byzantine Fault Tolerance (BFT) system.
    a. 72
    b. 76
    c. 77
    d. 79

    Detailed Solution:
    f = 25
    Total nodes required = 3f + 1 = 75 + 1 = 76

4. 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)

5. 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.

6. 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.

7. 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

8. 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.

9. 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.

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

    Hint :Refer to Lecture series

2. Running a chaincode in hyperledger fabric internally involves the following steps even if all the steps are not explicitly done by the user in the latest versions.
    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
    b. iv, iii, v, i
    c. v, i, ii, iv
    d. iii, v, ii, iv, i

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

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

4. Traditional methods for centralized digital identity management do NOT have which of the following characteristics?
    a. Identity holder can easily decide with whom to share the identity and which part

of it

b. Identity theft can occur and remain undetected
c. Restricting components of identity to be revealed to different verifiers is difficult
d. An attacker can capture the presented identity

5. Which of the following statements is/are FALSE regarding PBFT and PoW?
   a. PoW can be executed over both public and private blockchain networks.
   b. PBFT can be executed over a private blockchain network, but not chosen to be executed over a public blockchain network in general.
   c. PBFT can be generally preferred to be executed for both public and private blockchain networks
   d. PoW can be executed over a private blockchain network but can not be executed over a public blockchain network

Hint: c,d

6. Which of the following is/are true for Proof Of Work) PoW protocol
   a. Generally used in Open environment
   b. Scalable
   c. Transaction Per second (TPS) is low in general
   d. All of the above

Hint: Please refer to slides. PoW works in an open environment with lots of nodes, scalable and slow in comparison to closed environment protocols in general.

7. PBFT has higher transaction throughput than PoW
   a. False
   b. True

Hint: PBFT works in closed environments and is faster.

8. Which of the below statements is true?
   a. PoW is a non-randomized protocol
   b. Pow can always ensure consensus finality
   c. BFT protocols ensure total ordering of transactions
   d. None of the above

Hint: PoW is randomized and need not ensure finality. For details, please refer to the slide.

9. BFT protocol ensures finality in general.
   a. False
   b. True

Detailed Solution: BFT protocols commit blocks based on transaction ordering and ensure finality. For details, please refer to the slide.

10. Which of the following is/are true for scalable witness cosigning protocol?
    a. protect authorities and their clients from undetected misuse
    b. ensuring that every authoritative statement is validated
    c. It is used to sign a message by multiple authorities collectively
    d. none of the above

Detailed Solution: cosigning protocol supports collective signing and publicly logging them by witnesses. So all of the options are true. For details, please refer to the slides.

NOC22-CS44: Blockchain and Its Applications
Assignment 9

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

1. Which of the following is true about Single Sign-on
    a. The same identity can be used to access multiple services
    b. Decentralized providers always maintain the identity of individuals participating in single sign-on
    c. All individuals use a fixed same identity for every one of them
    d. All identity holders are also identity providers

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

Hint:

- **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. Which of the following statements regarding Solidity is true?
    a. Solidity is compiled to bytecode which is executed by Ethereum Virtual Machine.
    b. Solidity interpreter executes the program by Ethereum Virtual Machine.
    c. Solidity interpreter executes smart contracts in Ethereum nodes.
    d. Solidity is compiled to bytecode which is executed by Ethereum node's interpreter.

4. **Which of the following can be used for setting up Verifiable Credentials?**
    a. Hyperledger Aries
    b. Litecoin
    c. Ethereum
    d. Solidity

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. A specific pool of node choose are given the responsibility of forming the committee
    d. The nodes elect themselves as a committee member by winning a local computation

    Algorand is an open model which mean anyone can join the network. Also it is a 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 distinct component in Distributed Identifiers(DID) Architecture.
    a. DID Controller
    b. Verifiable Data Registry
    c. DID Subject
    d. DID Randomizer

    Refer to Week 9 slide

7. Consider the following statement - “Say Alice has generated two Distributed Identifiers (DID) DID1 and DID2 for 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. Assignment of SEED to Steward
    c. Acceptance of incoming invitation by Alice
    d. None of the above

    Refer to Week 9 Lecture Notes

8. In Verifiable Credential (VC), a claim is a statement about a non participant.
    a. True
    b. False

    Refer to Week 9 Lecture Notes.

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

        a. I
        b. I, II

c. 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. Data transfer is an important aspect of interoperability in which of the following blockchains?
    a. Hyperledger Indy
    b. Corda
    c. Hyperledger Fabric
    d. None

NOC22-CS44: Blockchain and Its Applications
Assignment 10

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

1. Which of the following statements is true for PBFT. Choose the best possible answer
    a. It requires a core non consensus group
    b. For scalability, it always requires O(n) for communication complexity
    c. It is not possible to create multiple pseudonymous identities to subvert the 3f+1 requirements of PBFT
    d. None of the above

    In PBFT 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. Alice has an account in the Ethereum network and wants to transfer ETH to Bob who has an account in the bitcoin network. Is it possible to do so?
    a. Yes, it is always possible without any external help
    b. No it is not possible
    c. Yes, possible via a trusted third party
    d. None of the above

    Cross Chain Asset Transfer is possible via TTP

3. Which of the following denotes properties of Hashed Timelock Contracts?
    a. If the secret is not revealed, the transaction creator cannot get back the fund even after timeout
    b. Spending of fund is blocked till the secret is publicly revealed or timeout occurs
    c. If timeout occurs, all the parties have distributed the funds equally
    d. Fund goes to the intended fund recipient after timeout occurs If the secret is not revealed

4. One of the advantages of centralized TTP-based Asset Transfer is it is very secure and always considered reliable. True or False?
    a. True
    b. False

    Centralized exchanges were compromised and stolen many times.

5. What are some of the issues that exist in Asset Exchange?
    a. Synchronization problem among sender and receiver networks
    b. Agreement of exchange rates

c. Denial of Service
d. All of the above

Refer to Week 10 Lecture Notes

6. What is an escrow? Select the best possible and concrete answer
   a. Escrow is an agreement in which assets are held and distributed when conditions are met
   b. Escrow is payment for smart contracts
   c. Escrow is a permissioned blockchain
   d. Escrow is cost of execution of smart contracts

Without the presence of any Escrow, the funds are in control of the sender and receiver parties.

7. Which of the following are guaranteed in the ideal atomic swap protocol ?
   a. All swaps will take place only when all parties conform to the protocol
   b. If some parties deviate from the protocol, then all conforming party ends up worse off
   c. No coalition has an incentive to deviate from the protocol
   d. All of the above

Refer to Week 10 Lecture Notes.

8. Can Alice send 1 BTC to her own account using a time locked contract.
   a. No the target account should be always different from the sender
   b. Yes she can send to her own account
   c. Only possible if she wants to send more than 1 BTC
   d. It depends on the time value mentioned in the contract.

Because, Time Locked contract restricts the spending/transfer of some currency
until a specified future time. Block height may be used as a proxy for time.

9. Suppose Alice has a time locked contract with a target account as:

   Funding Contract - 1 BTC
   Hash: **...Fa4509**
   Timeout: **2Δ**

   What will happen if Alice refuses to reveal the key and timeout occurs?
   a. 1 BTC refunded to Alice
   b. 1 BTC transferred to target account
   c. BTC less than 1 refunded to Alice as Some BTC deducted as penalty.
   d. BTC less than 1 transferred to target account

Refer to Week 10 Lecture Notes.

10. Which of the following is used as a public permissioned ledger based DID registry?
    a. Hyperledger Indy
    b. Bitcoin
    c. Ethereum
    d. Sidetree

Blockchain and Its Applications
Assignment 11

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

1. If an attacker initially populates the victim node's peer tables with attacker's IP addresses in blockchain network, this attack is known as:
    a. Sybil Attack
    b. Eclipse Attack
    c. Selfish Mining Attack
    d. 51% Attack

2. Which of the following can be used to identify a good blockchain use-case? (Mark multiple options if applied)
    a. Participants
    b. Assets
    c. Transactions
    d. Independent of everything

3. Alice is performing an Eclipse Attack, and If her IP replaces another attacker IP, the evicted IP is resent and eventually replaced by honest IP. Is this a valid statement?
    a. Yes
    b. No

4. In a decentralized blockchain network, which scenario poses a significant risk known as the "51% Vulnerability"?
    a. When a majority of users hold more than 51% of the cryptocurrency tokens.
    b. When a single entity or a group controls more than 51% of the network's computing power.
    c. When more than 51% of the nodes in the network experience a temporary outage.
    d. When more than 51% of the transactions in a block are invalid due to cryptographic errors.

5. Alice possesses 5 Bitcoins and initiates two separate transactions with the same Bitcoin. In which case does the double spending vulnerability occur?
    a. Alice pays for a coffee and a book with the same 5 Bitcoins.
    b. Alice accidentally sends 6 Bitcoins to a friend.
    c. Alice sends 2 Bitcoins to one friend and 3 Bitcoins to another.
    d. Alice checks her wallet balance but forgets to confirm the transaction.

6. In a selfish mining attack, discovering more blocks by pool develops a longer lead on the public chain, and continues to keep these new blocks _____
    a. Private
    b. Public

7. Which of the following scenarios is NOT a good use case for blockchain technology?
    a. A supply chain network where participants require real-time visibility into the movement and origin of goods.
    b. An online voting system aiming to enhance transparency, reduce fraud, and ensure the integrity of election results.

c. A centralized banking system seeking to improve transaction speed and reduce costs.
d. A healthcare system aiming to securely share patient records among different healthcare providers for better coordinated care.

8. What is a major problem with Proof Of Work?
    a. It is difficult to implement
    b. It is unreliable
    c. Multiple miners have to be rewarded
    d. It is CPU-intensive and consumes enormous amount of power.

9. In Practical Byzantine Fault Tolerance, ___.
    a. A master node selects the next node that adds the next block
    b. The node with most coins is chosen for adding the next block
    c. The nodes elect a leader and that leader adds the next block
    d. None of the above

10. Alice places a bulk order for a cryptocurrency, and before it is processed, Bob, who is a miner, inserts his own buy order with a slightly higher price. In which case does the front-running attack occur?
    a. Alice's order is confirmed first due to network congestion.
    b. Bob's order is prioritized and confirmed ahead of Alice's order.
    c. Both Alice and Bob's orders are cancelled due to conflicting transactions.
    d. The network rejects both Alice and Bob's orders, causing delays in confirmation.

Blockchain and Its Applications
Assignment 12

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

1. What of the following Indy transaction inserts a DID record in the Indy ledger
    a. INSERT
    b. INSERTDID
    c. NYM
    d. CREATE

2. Ubin project is based on Blockchain and Distributed Ledger Technology (DLT) for clearing and settlement of payments and securities
    a. True
    b. False

3. Does the information transferred to consumer: Consortium information such as catalog, pricing, etc.
    a. Not sensitive
    b. Sensitive

4. How does an application program interact with the Fabric network?
    a. Application program runs chaincodes which commit data to the ledger.
    b. Application program connects to the Orderer(s) to interact with the Fabric network.
    c. Application program uses the Fabric SDK to connect to a Fabric Peer which in turn connects to the Fabric network.
    d. Application program directly connects to a particular Fabric Channel in the network.
5. What is the correct order of phases in Project Ubin?
    i. Cross-border Payment versus Payment (PvP)
    ii. Tokenized SGD
    iii. Delivery versus Payment (DvP)
    iv. Re-imagining RTGS
    v. Enabling Broad Ecosystem Collaboration
        a. i, ii, iii, iv, v
        b. ii, iv, iii, i, v
        c. ii, iii, v, vi, i
        d. i, iii, v, ii, iv
6. In which of the attacks, end-user consumers can create multiple accounts/identities for accessing the consortium services?
    a. Byzantine faults
    b. Sybil attacks
    c. Impersonation attacks
    d. Sensitive information Leakage
7. When does Algorand reach a tentative consensus?
    a. During strong synchrony only
    b. During weak synchrony under partial network connectivity only
    c. During both strong synchrony and weak synchrony
    d. During weak synchrony under full network connectivity only

8. Quorum supports transactions with
    a. Only private state
    b. Only public state
    c. Both private and public state at the same time
    d. Either private or public state for a transaction
9. 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
10. What is the primary function of a channel in a Hyperledger Fabric network?
    a. To validate and order transactions on the blockchain
    b. To restrict access to specific participants in the network
    c. To store the complete history of all transactions
    d. To deploy and execute smart contracts