Q1. Given the following steps, what is the correct sequence involved in a block creation? (15 marks)
[S1] The transaction is validated together with other transactions
[S2] Transactions are bundled as a set and are broadcasted
[S3] A transaction is created
[S4] A block (containing the transactions) was added to the local chain and propagated to the network.
[S5] The PoW consensus problem is solved by a miner

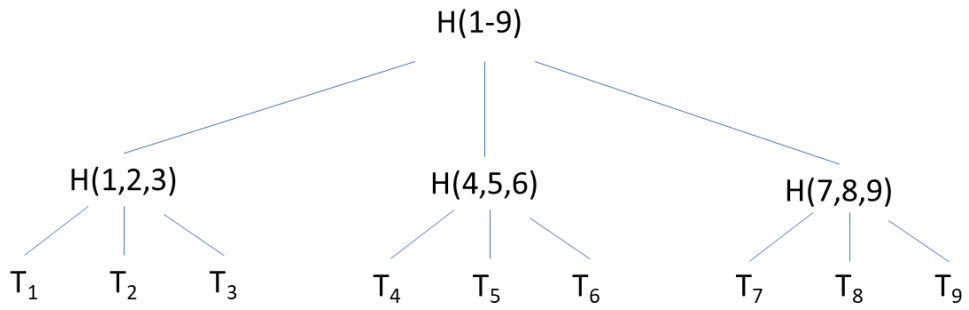
Sample solution:

S3->S1->S2->S5->S4

Q2. Merkle trees are effective and efficient for inclusion proof. As illustrated in the class, we can build a binary Merkle tree to contain $T = \{T_1, T_2, \dots, T_n\}$ transactions, where n is power of 2 and each non-leaf node contains at most two children. If we further extend the binary Merkle tree to a *ternary* Merkle tree, each non-leaf node contains at most three children. Consider a ternary Merkle tree containing $T = \{T_1, T_2, \dots, T_9\}$ transactions. If Alice wants to validate a transaction T_5 initiated by Bob, how does Alice prove this? Please draw the ternary Merkle tree and show the procedure to prove transaction T_5. (20 marks)

Sample solution:

(1) The constructed ternary Merkle tree



(2) The steps of validating transaction T_5:

i. Compute H(4,5,6) with the given T_5
ii. Obtain H(1,2,3)
iii. Obtain H(7,8,9)
iv. Compute H(1-9)
v. Compare the calculated result with the known H*(1-9)

Q3. Please compare unspent transaction (UTXO) model and account-based model. (10 marks)

Sample solution:

UTXO: transactions are either unspent or spent	Account-based

Record receipts of transactions	Keep track of the balance of each account globally
Record balances on the client-side by adding up the available unspent transaction outputs	Check whether the balance is no less than the spending transaction amount
Used for Bitcoin	Used for Ethereum

Q4. Can External Owned Accounts (EOA) send transactions, true or false? Please give the reason. (10 marks)

Sample solution:

True. A transaction is typically initiated by an EOA, e.g., a fund transferring from an EOA to another EOA.

Q5. Why does Ethereum introduce the Gas mechanism? How does it work? (15 marks)

Sample solution:

The Gas mechanism is introduced to the Ethereum blockchain to prevent infinite loops. Unlike conventional programs, smart contracts cannot be modified after being deployed on the blockchain. Moreover, all the transactions will be validated by miners in the cost of computation and storage. As a result, some bad codes containing infinite loops may be executed forever to exhaust the precious resources of blockchains. To prevent this abnormal behaviour, the Gas mechanism is introduced.

Q6. Given the following block information of Ethereum,

```
Block Height:    4323212
Status:          Finalized
Timestamp:       2748 days ago (Sep-29-2017 11:56:20 PM +UTC)
Mined by:        Bw.com in 93 secs
Block Reward:    5.437010102425984773 ETH (5 + 0.280760102425984773 + 0.15625 ETH)
```

What is the transaction fee of all the transactions in this block? How many uncles are included in this block? (15 marks)

Sample solution:

The transaction fee of all the transactions is `0.280760102425984773`. There is one uncle in this block because 0.15625 = 1 x 0.15625, where 0.15625 is the reward for each uncle.

Q7. What is the role of the Membership Service Provider (MSP) in Hyperledger Fabric? Why is MSP necessary? (15 marks)

Sample solution:

Membership Service Provider (MSP) provides users with an enrolment service, though which cryptographic mechanisms and protocols have been abstracted. MSP is responsible for issuing certificates, validating certificates, and user authentication.

Because Hyperledger Fabric is a permissioned blockchain, which requires users to fulfill certain requirements to perform certain actions. These permissions and access control are achieved by MSP.