CS6858: Distributed Trust November 17, 2022

Module 3 Test

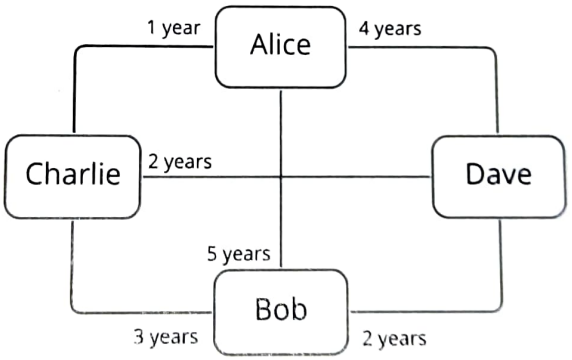
Instructor: *John Augustine*

Roll no.: EE19B106 Total points: 48

1. (5 marks) What is a token in the blockchain context? Define fungibility. Give at least three differences between Fungible token (FT) and Non-fungibles token (NFT).
2. (5 marks) What is the Ethereum Virtual Machine (EVM)? Draw the EVM block diagram with all the necessary components. Give short description of all its components.
3. Write brief descriptive notes on the following.
   (a) (2 marks) What are similarities and Differences between Externally Owned Accounts (EOA) and Contract Accounts?
   (b) (2 marks) What is Gas and why do we need that?
   (c) (2 marks) Explain the data storage locations namely Memory, Storage and Calldata.

Answer Either Question 4 or Question 5

4. Below is a social network of 4 friends interpreted as: Alice and Charlie have been friends for 1 year, Alice and Dave have been friends for 4 years, etc.



Given the network, write a solidity program containing the following:

(a) (1 mark) Define contract with SPDX License Identifier, version pragma, and contract name.

(b) (1 mark) Represent this network as a Nested Mapping (mapping type inside another mapping type) in solidity. Identify the names (like Alice and Bob) as address types. Map each address to the friend's address that tells the number of years they have been friends (years of friendship).

(c) (2 marks) Given the addresses of two friends and years of friendship, write a function to set the values of the mapping type.

(d) (2 marks) Given the addresses of two friends, write a function to get the years of friendship.

(e) (2 marks) Given the addresses of two friends, write a function to remove the record of a friendship.

5. Write a smart contract with the following.
   (a) (1 mark) Define the contract with SPDX License Identifier, version pragma, contract name, and an address type variable for the smart contract owner.
   (b) (1 mark) Constructor function that initially sets the owner variable.
   (c) (1 mark) Receive function to allow smart contracts to receive payment.
   (d) (2 marks) Define a function modifier that requires the sender of the call to be the owner.
   (e) (2 marks) Write an ETH transfer function to transfer X ETH to address Y. Both amount X and address Y are passed as a parameter to the method. The transfer of ETH can be made only by the owner (use the above modifier you created to check this).
   (f) (1 mark) Write a function to get the balance of the smart contract.

6. (a) (5 marks) Fill in the blanks :
   i. When an event is emitted, it stores the arguments passed in ___calldata___.
   ii. EVM performs all computations on a data area called ___stack___.
   iii. Contract B can inherit contract A using ___is___ keyword.
   iv. A contract can create other contract instance using the ___new___ keyword.
   v. A solidity function with ___payable___ keyword ensures that the function can send and receive Ethers.

   (b) (5 marks) State True or False :
   i. 1 Ether = 1e-18 Wei.
   ii. State variables are variables whose values are permanently stored in contract storage.
   iii. Smart contracts can be removed from the blockchain by calling selfdestruct operation.
   iv. Calldata is a non-modifiable, persistent area where function arguments are stored.
   v. The default value of uint in solidity is 0.

7. (a) (2 marks) Require function is used to validate inputs and conditions before execution. Write a require statement to validate that the smart contract balance is greater than 5 ETH.
   (b) Answer the following questions on Error Handling.
   i. (2 marks) Define a custom error `InsufficientBalance` that takes 2 parameters: available and required balance.
   ii. (2 marks) Call the error defined in (i) using parameters.

8. Answer the following questions on `fallback()`:
   (a) (2 marks) What is the `fallback` function in Solidity?
   (b) (1 mark) Can a contract have more than one fallback function?
   (c) (1 mark) How is a `fallback` function declared?

9. (a) (2 marks) What is the difference between pure and view functions in solidity?
   (b) (2 marks) Name four types of visibility for solidity functions.