Fast**National University of Computer & Emerging Sciences, Karachi  
Fast School of ComputingSpring-2023 CS-Department  
MidTerm-1  
1st March 2023, 8:30 pm – 9:30 pm**

|  |  |  |
| --- | --- | --- |
| **Course Code: CS-4049** | **Course Name: Blockchain and Cryptocurrency** | |
| **Instructor Names: Shahbaz Siddiqui** | | |
| **Student Roll No:** | | **Section No:** |

Instructions:

* Return the question paper.
* **All questions must be answered in answer script and according to the sequence given in the question paper.**
* Illustrate means you have to answers with the help of Diagram/Figure. **Written answers will not be graded where illustrations are required.**

**Time**: 60 minutes. **Max Marks**: 30 points

**Question 1:** Explain the decentralize consensus algorithm used in Bitcoin to agree on valid block. Discuss how this algorithm solves the problem of double spending. **[4 Points]**

Due to validation of security attribute for double spending from the blockchain distributed ledger

**Question 2:**BitCorp has just noticed that Mallory has compromised one of their servers holding their Bitcoin private keys. Luckily, they are using a 2-of-3 multi-signature wallet, so Mallory has learnt only one of the three sets of keys. The other two sets of keys are on different servers that Mallory cannot access. How do they re-secure their wallet and effectively revoke the information that Mallory has learned?

**[6 Points]**

**To re-secure their wallet and revoke Mallory's access, BitCorp can follow these steps:**

* Immediately stop all transactions from the compromised wallet to prevent Mallory from making any unauthorized transfers.Create a new 2-of-3 multi-signature wallet and generate new private keys for each of the three parties involved in the previous wallet.
* Transfer all the Bitcoin from the compromised wallet to the new wallet.
* Add the new private keys to the new wallet, ensuring that the three parties have control over the new wallet.
* Remove the compromised private key from the new wallet, effectively revoking Mallory's access to the wallet.This process will ensure that Mallory's knowledge of one of the private keys is useless in accessing the funds in the new wallet. Additionally, BitCorp should investigate how Mallory was able to gain access to the server and take steps to prevent similar incidents in the future, such as implementing stronger security measures and monitoring for suspicious activity

**Informed the wallet to update its signature**

**Or updated wallet signature**

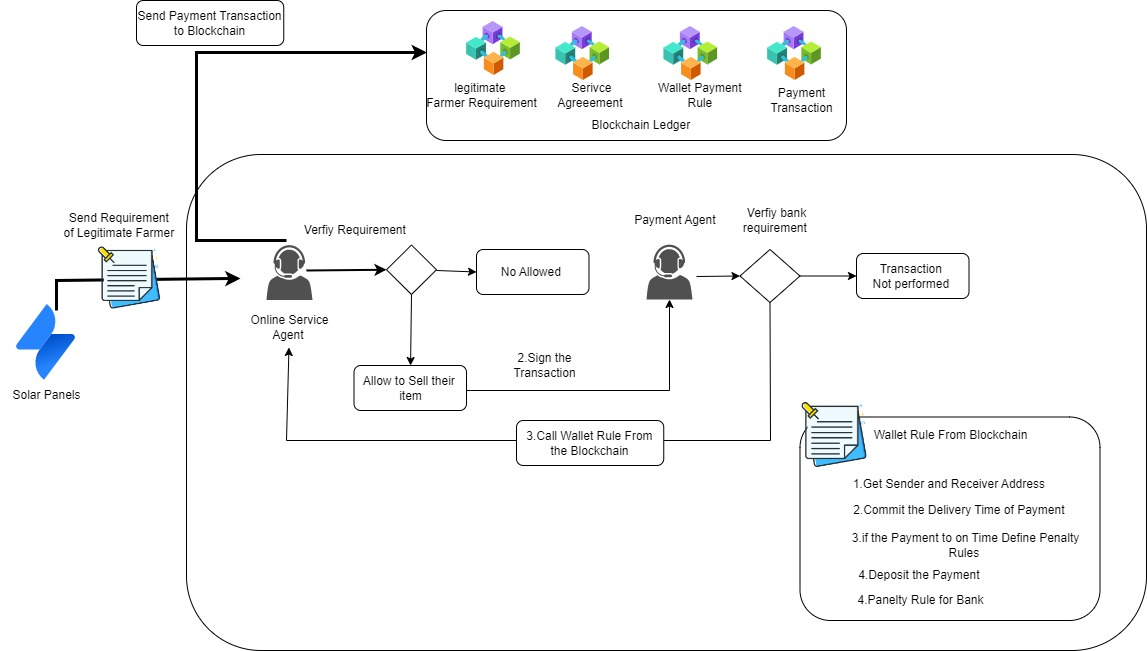
**Question 3:** Let H be a hash function with info hiding and puzzle‐friendly properties. Consider G(z) = H(z) || z​ last where z​ last represents the last bit of z. Show that G is puzzle‐friendly but not hiding.

**[4 Points]**

**Due to addition ok known Bits Z in the H Function G is puzzle friendly**

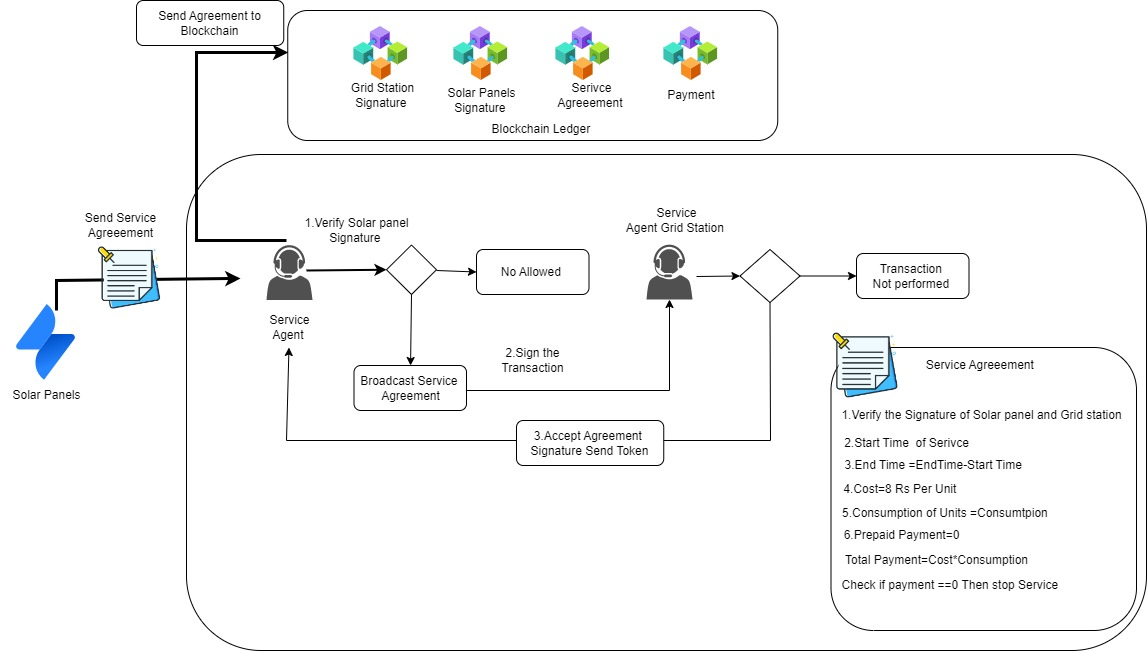
**Question 4:** Small-scale organic farmer wants to sell their produce directly to consumers online. In the traditional payment system, the farmer might have to rely on a third-party payment processor to handle the transaction, which can be costly and may take several days to process. Additionally, the farmer and the buyer may have limited visibility into the status of the payment, and there could be risks of fraud or chargebacks. Design the solution with the help of the blockchain consensus mechanism with justification in order to provide a fast and secure transaction mechanism between organic farmers and consumers.

**[4 Points]**



**Question 5:** In smart cities, residents install solar panels to generate their own electricity and sell any excess power back to the grid. Design the solution based on automation in order to manage payments and transactions for the electricity generated by the solar panels also justify the designed solution

**[4 Points]**

****

**Question 6:** Write script based on bitcoin fork Multichain, to create wallet for transaction to other public identity **[4 Points]**



**Question 7** **:** Write a script based on the Bitcoin fork Multichain to extract the some security attributes of publishing Block **[4 Points]**

**Multichain-cli chainname liststreamkey Items False 1**

[**https://github.com/MultiChain/multichain-api-libraries/blob/main/python/examples.py**](https://github.com/MultiChain/multichain-api-libraries/blob/main/python/examples.py)

***BEST OF LUCK!***