Fast**National University of Computer & Emerging Sciences, Karachi  
Fast School of Computing Spring-2023 CS-Department  
MidTerm-1  
28th Feb 2023, 11:30 pm – 12:30 pm**

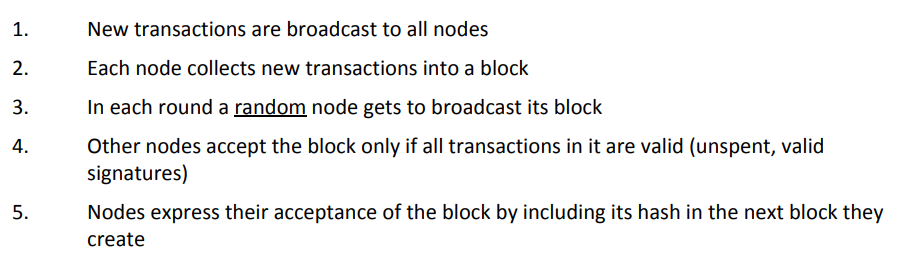
|  |  |  |
| --- | --- | --- |
| **Course Code: CS-4049** | **Course Name: Blockchain and Cryptocurrency** | |
| **Instructor Names: Shahbaz Siddiqui** | | |
| **Student Roll No:** | | **Section No:** |

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 why consensus without identity is used in Blockchain. ? **[4 Points]**



One reason for this lack of identities is that in a peer‐to‐peer system, there is no central authority to assign identities to participants and verify that they’re not creating new nodes at will. The technical term for this is a Sybil attack. Sybils are just copies of nodes that a malicious adversary can create to look like there are a lot of different participants, when in fact all those pseudo‐participants are really controlled by the same adversary. The other reason is that pseudonymity is inherently a goal of Bitcoin

**Question 2:** In the current model of online content creation, content creators often rely on advertising revenue to monetize their content. However, this model can be inefficient and can lead to a skewed distribution of rewards, with a small number of highly popular content creators receiving the lion's share of revenue, while many others struggle to make a living. Design a blockchain based solution on automation of content monetization

**[4 Points]**

**Step-1 :Content writing Request posted to website with all agreements**

**Agreement {**

**1.10% plagerisim is allowed**

**2.Content should be delivered in 10 days**

**3.if you accept the agreement 50% payment is credit in your account**

**4.Panelty impose when delivery time is late**

**}**

**Agreement execution based on multi signature**

**Also Same diagram as explain in the Juniors paper**

**Question 3:** Design a blockchain-based system that creates a transparent and efficient food supply chain. The system should include a blockchain ledger that tracks food production and distribution activities, with smart contracts automating the process of food production and distribution. The system should also enable consumers to access information about the origin and quality of their food products via a QR code or unique code on the product packaging. The system should incentivize ethical and sustainable food production practices and reduce inefficiencies and waste in the food supply chain.

**Step-1 :Content writing Request posted to website with all agreements**

**Agreement {**

**1.Serivce provider id**

**2.Food Service Id Signature**

**2.Delivery time**

**3.Consumer signature**

**4. Feedback**

**}**

**Answer 2 :Micropayment Procedure**

**Also Same diagram as explain in the Juniors paper**

**[4 Points]**

**Question 4:** To prevent double spending in a Multichain wallet for transactions to other public identities, what security measures can be implemented within the script? **[4 Points]**

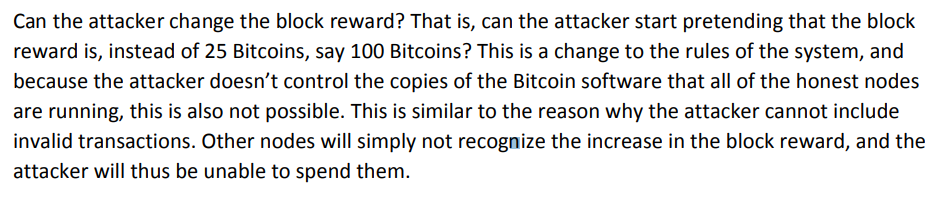
**Validation of Blockchain attributes such as Genisus Blockhash, transactional Id, publisher Id etc**

**Question 5:** Write a script using Multichain, a Bitcoin fork, to extract information about the genesis block in the blockchain?  **[4 Points]**

Multichain.getinfo

**Question6:**Can the attacker change the block reward? That is, can the attacker start pretending that the block reward is, instead of 25 Bitcoins, say 100 Bitcoins?

No because for this we have to altered the consensus mechanism of Bitcoin network or having the private key inorder to change the bydefalut rules



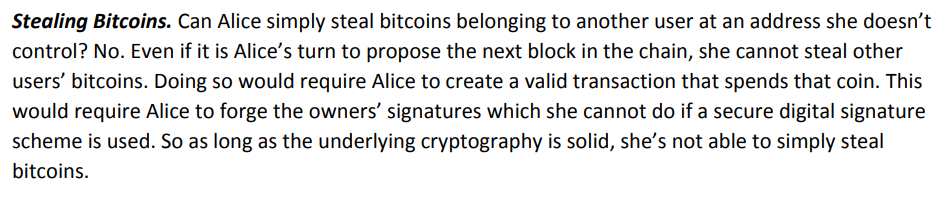
**[4 Points]**

**Question 7:**In ScroogeCoin, suppose Mallory tries generating (sk, pk) pairs until her secret key matches

someone else’s. What will she be able to do? What if Alice’s random number generator has a bug and her key generation procedure produces only 1,000 distinct pairs? .Generate Public and Private Key Pairs using any language

**[6 Points]**

**She can open the encrypted message in the Block**

****

***BEST OF LUCK!***