CS 5594
Homework Assignment 4

Given: Apr 16, 2024 **Due:** Apr 30, 2024

General directions. The point value of each problem is shown in [ ]. Each solution must include all details and an explanation of why the given solution is correct. **In particular, write complete sentences. A correct answer without an explanation is worth no credit.** The completed assignment must be submitted on Canvas as a PDF by 11:59 PM on Apr 30, 2024. **No late homework will be accepted.**

Digital preparation of your solutions is mandatory. Use of LaTeX is optional, but encouraged. No matter how you prepare your homework, **please include your name.**

---

[15] 1. In the Proof-of-Stake mechanism, there are "Nothing at Stake" and "Long Range" attacks.

A. Describe these attacks in detail.

B. Why do these attacks not exist in the Proof-of-Work?

---

[20] 2. One of the main goals of bitcoin is to achieve *anonymity* in digital transaction.

A. Describe the main techniques that Bitcoin used towards enabling anonymity.

B. Unfortunately, bitcoin is far from being completely anonymous. Describe how bitcoin transactions can be deanonymized. How many ways the attacker can exploit to do so?

---

[40] 3. Suppose Bob would like to receive donation for his project. So, he is planning to put his bitcoin addresses on a public donation forum along with his personal website. However, since all the users will make donation to one of these addresses, it is likely that all the donations can be *linkable* and reveal Bob's identity (due to his website).

To address this privacy issue, Bob has to generate a so-called **stealth address** that permits any sender to always derive new address per transaction and only Bob can know the corresponding private key.

A. Using a public key crypto technique that you are familiar with to design a simple scheme to generate stealth address *securely*.

B. Based on your stealth address design, explain how Bob can determine which transactions in the blockchain are directed to him. What is the cost of doing so?

---

[20] 4. Off-chain storage was introduced to address the (cost) problem of storing large amount of data on the chain. With programmable blockchain, it is possible to perform computation beyond data storage.

A. If the computation is too heavy, would it be possible to move the computation off-the-chain as storage? If not, why? If yes, describe the main techniques to enable off-chain computation and what should be stored on blockchain afterwards?

---

[30] 5. In class, we have studied the Byzantine Broadcast (BB) problem, where a single node (the sender) has a private input and the goal is to broadcast that input to everyone else. For this problem, you can assume that the private input is either 0 or 1.

A closely related problem is Byzantine Agreement (BA). In this problem, each node $i \in \{1, 2, \ldots, n\}$ has its own private bit $b_i \in \{0, 1\}$. Up to f out of n nodes can be byzantine, meaning they can behave arbitrarily. A deterministic BA protocol must satisfy the following two properties:

- **Agreement**: the protocol always terminates with all honest nodes outputting the same bit.
- **Validity**: if all honest nodes have the same private input $b \in \{0, 1\}$, then the protocol terminates with all such nodes outputting b.

A. Show that a deterministic BA protocol can only exists when $f < n/2$.

B. Given $f < n/2$, prove that there exists a deterministic BB protocol satisfying validity and agreement (as defined for the BB problem) *if and only if* there exists a deterministic BA protocol satisfying validity and agreement (as defined for the BA problem).
