CCS 5594: Blockchain Technologies (Spring 2021)

Homework 3

Due April 30, 2021 11:59 PM

1. What are “Nothing at Stake”, “Long Range” attacks in Proof-of-Stake? Why do these attacks *not* exist in the Proof-of-Work? (10pt)

2. Describe the main differences between the design of Bitcoin blockchain and Ethereum blockchain. (10pt)

3. The immutability is an important (and nice) property of blockchain to enable auditing and integrity. However, immutability also creates some issues the context of *programmable* blockchains (e.g., smart contracts). For instance, once the *buggy* smart contract is deployed, the bugs remain on the chain forever.

    a. One of the most devastating attacks that actually happened when deploying a buggy smart contract is called *reentrancy attack*. Explain this attack and its consequence along with the (potential) solution to countermeasure this attack. (5pt)

    b. Can you describe some other possible attacks that can exploit the immutability of bugs? Is there any way to recover from these attacks? (5pt)

    c. In *your own opinion*, what are the tradeoffs of complete blockchain immutability? What are the tradeoffs of being able to recover where a problematic smart contract was executed? (5pt)

4. 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. (5pt)

    b. Unfortunately, bitcoin is far from achieving a complete anonymity. Describe how bitcoin transactions can be deanonymized. How many ways the attacker can exploit to do so. (10pt)

5. 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*. (10pt)

b. Based on your design in (a), explain how Bob can determine which transactions in the blockchain are directed to him. What is the cost of doing so? (10pt)

6. Although private blockchain is not covered in the lecture, its concept is quite simple and can be derived from public blockchains (e.g., bitcoin, Ethereum).

   a. Study yourself about private blockchain and explain its main concept of private blockchain. What are the main differences between public blockchain and private blockchain? (10pt)

   b. Is it possible to deploy the public blockchain's consensus protocols (PoW, PoS) in private blockchain? If so, how? If not, why? Justify your answer. (10pt)

7. 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. So, if the computation is too heavy, would it be possible to move the computation off-the-chain too? If not, why? If yes, describe the main techniques to enable off-chain computation and what should be stored on blockchain afterwards? (10pt)