COMP 4541 – Homework 4

A. K. Goharshady

Release Date: April 16, 2024

Deadline: May 4, 2024 (23:59 HKT)

This homework accounts for 10% of your total grade. You should submit your solution as two files, one `pdf` and one `sol`. As usual, handwritten and scanned solutions will not be accepted since the TAs might be unable to read your handwriting. However, you can draw your figures, if any, by hand. Your submission must be entirely your own work. All submissions will go through a plagiarism check. If you submit the same solutions as another student, you will both get a grade of F for the whole course. The deadline is firm and no extensions will be granted. You will receive feedback on your submission and normally be allowed to resubmit once. We reserve the right to disallow resubmissions if your original submission is of a very low quality, does not compile, or shows a lack of effort.

Exercise 1

This exercise is 10% of your total grade.

`CryptoDoggies` is a game that can be played on the Ethereum blockchain and is implemented as a smart contract[1]. The basic object in this game is a virtual pet, called a *doggy*. Each doggy has a unique DNA that is a sequence of 16 bits. We save the DNA as a `uint16`. The whole game takes place inside a single contract in which players can perform the following tasks:

- `createNewDoggy`: This function creates a new doggy and puts it under the ownership of the player who calls it. The doggy's DNA is chosen randomly. Also, the player has to pay a fee for creating the new doggy. This fee will become property of the contract and can later be redeemed by the owner/developer of the contract. The fee paid for creating the current doggy must exceed the base fee. It must also be at least 1% more than the fees paid for any doggy that was created in the past 1000 blocks.
- `breedDoggy`: The owners of two doggies can decide to breed them. Doggies are special creatures with no gender and every breeding leads to exactly two offspring, one for each owner. Each offspring will randomly inherit half of the DNA of each parent doggy. The owners have to pay a fixed breeding fee to the developer of the contract.
- `sellDoggy`: An owner can put their doggy for sale by setting the sales price and paying a selling fee to the developer of the contract. Note that doggies might have widely different real-world values based on how rare their DNA seems. This is something that is not under the control of the contract and is decided by the forces of the market. For example, a doggy with the DNA `0101010101010101` is extremely rare and might be sold for millions of dollars[2].
- `buyDoggy`: One can buy a doggy that is put up for sale by paying the price asked by the seller and an additional buying fee, which will be given to the developer of the contract.
- `reclaimFees`: The developer can call this function to receive all the fees that were paid by players until this point.

The file `CryptoDoggies.sol` contains an implementation of the `CryptoDoggies` contract. The developer has asked you to perform a holistic audit on this implementation.

1. Identify as many security vulnerabilities/implementation bugs as possible in the attached code. Explain how each vulnerability/bug can lead to undesirable behavior or enable an attack. Submit your solution to this part as a `pdf` file that lists and discusses each case separately.
2. Submit a fixed version of the implementation that addresses all the problems you identified in part 1. If you are unable to address some of the problems, mention this both as a comment in the code and in the writeup. To make it easier for the TAs to grade, try to make as few changes as possible to the original code.

[1] The name is not real and does not reference any real project.

[2] I cannot believe that people really pay such prices in the real world, but they do.