COMP4901W Homework 4/5

Name: Hangyul Son
SID: 20537267

Exercise 1.

The order of the game

1. Alice and Bob sends their hashed choice through SendChoice() function.
    a. They can only send their choice only if they haven't revealed yet. Because one might resend the choice after both choices have been revealed.
2. Alice and Bob reveals their choice.
    a. They can only reveal their choice after they have sent their hash of the choice.
    b. The contract makes sure the sent choice and password is valid by matching their hashes using keccak() function.
    c. Alice or Bob might refuse to reveal their choice to mess up the game. Therefore set a deadline using the block.number once either Alice or Bob declares the choice.
3. Alice and Bob compare their choice. Decide the winner.
    a. Anybody can compare the choice once the deadline passes or if Alice and Bob both have declared their choice.
    b. If Alice or Bob have not declared the choice, then the smart contract considers this as a forfeit and sends 2 ether to whom have made the choice.
    c. Set gameOver variable to true.

- One might perform a front running attack. In other words Alice or Bob can see each other's transaction by having lots of nodes spread out. Or can be a miner oneself. And the attacker can send his choice after checking the opponent player's choice which would be considered cheating.
- Even though Alice or Bob misses the transaction, it will be mined and become available to everyone in accessbile to the blockchain. Then the same attack can be performed.
- Therefore, Alice and Bob must hash the choice before sending the choice. It is important to hash with a nonce as there are only 3 possible choices which the opponent might brute force to cheat in the game.
- After Alice or Bob reveals their choice if one recognizes that the game will be lost, one might not reveal their choice. This won't let the game continue and therefore must be punished.
- No third-party can tamper the game because in order to send the choice and reveal it, the smart contract requires the player to be either Alice or Bob. The transfer function is only related to Alice and Bob which makes the malicious entity impossible to steal ether. The malicious cannot deposit any unit of currency to the contract as it does not have a fallback function and the only payable function is sendChoice which requires the sender to be Alice or Bob. However, even if they could send currency to the contract, the game result and its reward amount won't change.

Exercise2

The order of Auction

1. Seller creates a smart contract for auction.
    a. The seller defines the deposit for the item.
    b. The deadline of making the bid is for 24 hours which approximately translates to 6429 blocks, is initialized. The entire auction ends within approximately 48 hours, 24 hours for making the bid and 24 hours for checking if they have had the highest bid.
2. The participants can enter the bid for 24 hours before the auction ends.
    a. The bid amount should not be revealed until the deadline. Therefore, the participants hash their bid and the password.
    b. The hashed bid will be mapped to the each and every sender's address. The participants may bid as many times as they wish during the auction as long as they pay the deposit. But the deposit will be refunded only once.
3. Only after the deadline the participants can check whether they were the highest bidder.
    a. All participants return back their deposit as long as they reveal bid amount.
    b. Participants that have not checked within 24 hours is considered to forfeit the opportunity to become the highest bidder. Therefore the highest bidder is only finalized after 24 hours.
    c. The checkBid function is safe from reentrancy attack as it keeps track of whether participant has been paid or not with a mapping.

- To ensure highest bidder to pay for the item price, the contract forces the participant to pay the bid amount as they reveal their bid. If the bidder is not the highest bidder they receive the bid amount they have payed as well as the deposit. However if one becomes the highest bidder at the moment, they only receive the deposit back, and the contract holds the bid amount. If other bidder becomes the king, the previous king's bid is returned.
- However a single participant may make many different identities to enter the auction with different bid amount. And the participant may only reveal the bid just big enough to become the highest bidder. This problem can be easily solved by raising the deposit amount. Only if the identity that have checked the bid, the deposit is refunded. Therefore rational participant will only bid with a single identity given that deposit price is expensive.
- The function that pays the king bid amount back to the seller after the end of the auction has not been implemented.

Gas estimate:

To make the first bid of any participant: makeBid() = Approximate MAX 49000 gas.
Explanation: The first initialization of value to variable 'bid_amount[msg.address]'.

/** Make futher bids with the same identity : makeBid() = Approximate 29000 gas.
Explanation: 'bid_amount[msg.address]' only changes value instead. If the address change than the gas again takes 44000 gas. **/

To check the result of the bid: checkBid() =

- Highest Bidder at the moment of the function call. Approximate MAX 88000 gas.
- Failed to be the highest bidder to receive deposit and bid amount: Approximate MAX 66000 gas

(This includes possibility of transfer calling fallback function which adds 2300 gas)

Therefore the amount of approximate gas used for every participants of the auction given that the participant is rational and the bid is made only once with the same address,

- 49000 gas + 89000 gas = 138000 gas for the potential highest bidders
- 49000 gas + 66000 gas = 115000 gas for direct refund.