Assignment 1

August 29, 2020

1 Queen Anne's Revenge

This is the year 1716, the French Navy has acquired *Queen Anne's Revenge*, once commandeered by the famous Blackbeard (you can read more about it on Wikipedia). However, the Navy decided to put the beautiful ship back into service as a merchant ship. The French have decided to auction it to the highest bidder using a *Vickrey Auction*. In order to conduct a secure auction they plan to develop a Smart Contract on the Ethereum blockchain for the same. Since it is still the renaissance period and no one knows how to use a computer, you are asked to write the Smart Contract.

2 Vickrey Auction

A Vickrey auction is also known as the second price sealed bid auction. Bidders submit written bids without knowing the bid of the other people in the auction. The highest bidder wins but the price paid is the second-highest bid. You can read more about it on Wikipedia to find out why it elicits truthful responses from the bidder.

2.1 Specifications of the Smart Contract

Your smart contract must fulfil the following specifications:

2.1.1 Second Price Auction

The ship must go to the who bids the highest, but he should only be charged the second-highest bid. Therefore, the difference should be refunded back.

2.1.2 Sealed Bid Auction

The bids should be kept private, i.e., no information about the losing bids should be leaked to the bidders. However, you are allowed to assume that everyone bids truthfully (and they will actually pay up the amount when required).

2.2 Barbossa's Brethren

Since the auction is being conducted anonymously, pirates also take part in it to get a chance to commandeer the ship. The Brethren Court (composed of nine pirate lords from the seven seas) decides to create a *bidding ring*. They plan to collect all the bids but submit only the highest bid in the actual auction so that the winner may have to pay a lower or equal price as compared to submitting a bid without a bidding ring. However, pirates are not famous for being honest and in fact, they don't even trust each other. They ask you to develop another smart contract that collects all the bids (again sealed) and submits them to the original contract.

2.3 Specifications of the Smart Contract

Your smart contract must fulfil the following specifications:

2.3.1 Collect Sealed Bids

The bids should be kept private, i.e., no information about the losing bids should be leaked to the bidders. However, you are allowed to assume that everyone bids truthfully (and they will actually pay up the amount when required).

2.3.2 Submit the winning bid

There should be a function in your smart contract, which when invoked by the deployer (Barbossa), submits the highest bid collected to the actual smart contract.

3 Marking Scheme

3.1 Contract 1

The contract for Vickrey Auction will carry a weight of 70%.

3.2 Contract 2

The contract for the bidding ring will carry a weight of 30%.

3.3 Mark Distribution for each Contract:

3.4 Correctness

Your programming logic should be correct (10%)

3.5 Security

For keeping the bids secret. (15%)

3.6 Comments

All functions in the code should be well explained with Doxygen comments. (https://www.doxygen.nl/manual/docblocks.html) (10%)

3.7 Correct Visibility and Modifiers

All functions should be assigned proper visibility and modifiers as required. (10%)

3.8 Test Cases

3.8.1 Generating Test Cases

You have to write 4 distinct test cases for both of your contracts (5%) but we would also be testing your code with our own test cases. (20%)