Abdel Rahman Adel
1701 2296

Assignment 5

(1) a) The bid is represented by the output of 'Keccak256'.
- The Cost of Keccak256 alone is 30 Gas
- // // // // word is 6 Gas, word = 32 bytes

So if Keccak256("") Gas = 30
So if // // ("abc") Gas = 36
So if // // ("Words to 32") Gas = 42

b) if you remove onlyBefore(biddingEnd), participants could submit bids after the bidding period has ended. which can hinder the integrity of the blind action.

c) Fake bids are used to ensure that the bidders reveal the same amount they initially committed.

d) in the reveal method: it's used to return the bid amount to the bidder except the highest bidder

in the withdraw method: it's used to return the excess funds to the bidder after they won the auction. excess = funds of highest - second highest

modification in file "asg5-1-d.sol", the bidder has to call reveal and then withdraw which can cost more gas overall

---

(3) a) 1. Producer deploys the contract
2. Donors contribute to the contract (totalDonation += donate value)
3. if totalDonations >= target_amount show the recording
4. public Release() only called internally.

insure checkDonations modifier before public Release()
and producer can cheat and not call the public Release

(3) b) 1. Producer deploys Contract & recording
2. Buyers pay the price access the recording
3. Check if a buyer is eligible to access the recording
4. Exclusive reveal to eligible buyers
5. Ensure only publish to buyers

- Producer can cheat and not show to the buyers.

I acknowledge that I am aware of the academic integrity guidelines of this course, and that I worked on this assignment independantly without any unauthorized help.

عبدالرحمن عادل
عبد الفتاح