CIS 6930: Blockchain: Optimization and Applications

DApp Solidity - Report

Venkata Sindhu Kandula (UF ID: 1914 5414)

1. Functions:

1.1. function bid() public payable

Bid on the auction with the value sent together with this transaction. The value will only be refunded if the auction is not won.

- ➢ If the bidding period is over, revert the call. This is taken care by a Boolean variable 'ended' which if false, the call is reverted.
- ➢ If the bid is higher than the highest bid, send the money back with message "Already higher bid present".
- ➢ Storing the previously highest bid in pendingReturns. The bidder will need to trigger withdraw() to get the money back.
- ➢ When the highestbid is increased, emit an event highestBidIncreased

1.2. function withdraw() public returns (bool)

Withdraw a bid that was overbid

- ➢ The amount in pendingReturns is sent to the sender
- ➢ False is returned when there is an error when sending
- ➢ Else if successful return true
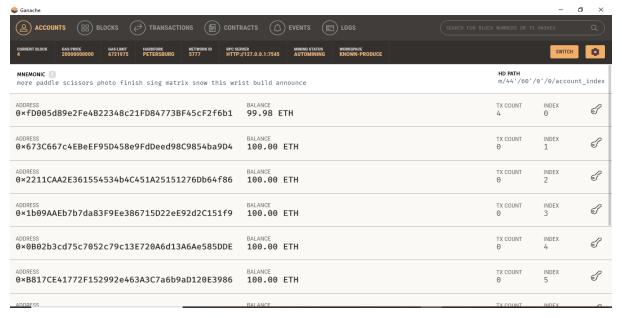
1.3. function auctionEnd() public

- ➢ Only beneficiary can trigger this function. If not, throw an error "Only beneficiary can trigger autionEnd"
- ➢ Send money to beneficiary account and make sure it cant call this function multiple times
- ➢ This function is segregated into three phases:
  - ▪ Conditions: if 'ended' is set to false, "auctionEnd has already been called."
  - ▪ Effects: 'ended' is set to true when this function is called by beneficiary and AuctionEnded event is emitted.
  - ▪ Interaction: The highest bid is transferred to the beneficiary.

2. The amount of gas or transaction fee needed to deploy the contract and trigger each of the implemented functions. Attach some screenshots showing how you obtained those numbers.

2.1. Action: Truffle migrate

total cost is 0.01316662ETH

```
 /usr/bin/bash --login -i
   > block timestamp:        1582598789
   > account:                0xfD005d89e2Fe4B22348c21FD84773BF45cF2f6b1
   > balance:                99.99623034
   > gas used:               188483
   > gas price:              20 gwei
   > value sent:             O ETH
   > total cost:             0.00376966 ETH

 - Saving migration to chain.
   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:             0.00376966 ETH


2_deploy_contracts.js
======================

   Replacing 'Auction'
   ------------------
   > transaction hash:       0x82fde931d16bc2e0635a63f1204b47aadb5b67ce07b86ba53ced16a551518b9d
 - Blocks: 0               Seconds: 0
   > Blocks: 0               Seconds: 0
   > contract address:       0xd3647a9f59045e1979563698157E302D7c41a92B
   > block number:          3
   > block timestamp:        1582598790
   > account:                0xfD005d89e2Fe4B22348c21FD84773BF45cF2f6b1
   > balance:                99.9822237
   > gas used:               658331
   > gas price:              20 gwei
   > value sent:             O ETH
   > total cost:             0.01316662 ETH

 - Saving migration to chain.
   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:             0.01316662 ETH


Summary
=======
> Total deployments:       2
> Final cost:              0.01693628 ETH


bash: __docker_machine_ps1: command not found
[Sindhu@LAPTOP-FMCDRJHK hw1-source]$
```

Ganache	—	□	×

ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS	SEARCH FOR BLOCK NUMBERS OR TX HASHES

| CURRENT BLOCK 4 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK PETERSBURG | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE KNOWN-PRODUCE | SWITCH ⚙ |

MNEMONIC
more paddle scissors photo finish sing matrix snow this wrist build announce

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX	
0×fD005d89e2Fe4B22348c21FD84773BF45cF2f6b1	99.98 ETH	4	0	🔑
0×673C667c4EBeEF95D458e9FdDeed98C9854ba9D4	100.00 ETH	0	1	🔑
0×2211CAA2E361554534b4C451A25151276Db64f86	100.00 ETH	0	2	🔑
0×1b09AAEb7b7da83F9Ee386715D22eE92d2C151f9	100.00 ETH	0	3	🔑
0×0B02b3cd75c7052c79c13E720A6d13A6Ae585DDE	100.00 ETH	0	4	🔑
0×B817CE41772F152992e463A3C7a6b9aD120E3986	100.00 ETH	0	5	🔑
ADDRESS	BALANCE	TX COUNT	INDEX	🔑

2.2. Bid function:

2.2.1. Action:

await instance.bid({from:accounts[2],value:web3.utils.toWei('3','ether')})

gasUsed: 63744

```
=======
> Total deployments:    2
> Final cost:           0.01693628 ETH

bash: __docker_machine_ps1: command not found
[Sindhu@LAPTOP-FMCDRJHK hw1-source]$ truffle console
truffle(ganache)> let instance = await Auction.deployed()
undefined
truffle(ganache)> let accounts = await web3.eth.getAccounts()
undefined
truffle(ganache)> await instance.bid({from:accounts[2],value:web3.utils.toWei('3','ether')})
{
  tx: '0x3bf2e2b3ac82170af40d7114be61bcdd05c2d10a301c51786b8f63f4d33d77e6',
  receipt: {
    transactionHash: '0x3bf2e2b3ac82170af40d7114be61bcdd05c2d10a301c51786b8f63f4d33d77e6',
    transactionIndex: 0,
    blockHash: '0xbc6a7c48c9058f56299a5ab6b77a8dda1676c36286310013501a04e130178835',
    blockNumber: 5,
    from: '0x2211caa2e361554534b4c451a25151276db64f86',
    to: '0xd3647a9f59045e1979563698157e302d7c41a92b',
    gasUsed: 63744,
    cumulativeGasUsed: 63744,
    contractAddress: null,
    logs: [ [Object] ],
    status: true,
    logsBloom: '0x00000000000000000000000000008000000000000000000000000000000000000
0000001000000000000000000000000000000000000000000000000000000000000000000000100000
00000010000000000000000000000000000000000000000000000000000000000000000000000000000
    v: '0x1b',
    r: '0x1c31ba5f40518a299c3ac3f9ba57a1d6755eb3db60d0ee28677acd5a7bcf4a50',
    s: '0x2038fa1ca663ac45619b1ad0cb5f5882ca1a69bc1de84f185c0ba2a6b3a7c34e',
    rawLogs: [ [Object] ]
  },
  logs: [
    {
      logIndex: 0,
      transactionIndex: 0,
      transactionHash: '0x3bf2e2b3ac82170af40d7114be61bcdd05c2d10a301c51786b8f63f4d33d77e6',
      blockHash: '0xbc6a7c48c9058f56299a5ab6b77a8dda1676c36286310013501a04e130178835',
      blockNumber: 5,
      address: '0xd3647a9f59045e1979563698157E302D7c41a92B',
      type: 'mined',
      id: 'log_bc8021c3',
      event: 'HighestBidIncreased',
      args: [Result]
    }
  ]
}
truffle(ganache)>
```


ADDRESS	BALANCE	TX COUNT	INDEX	
0×fD005d89e2Fe4B22348c21FD84773BF45cF2f6b1	99.98 ETH	4	0	
0×673C667c4EBeEF95D458e9FdDeed98C9854ba9D4	100.00 ETH	0	1	
0×2211CAA2E361554534b4C451A25151276Db64f86	97.00 ETH	1	2	
0×1b09AAEb7b7da83F9Ee386715D22eE92d2C151f9	100.00 ETH	0	3	
0×0B02b3cd75c7052c79c13E720A6d13A6Ae585DDE	100.00 ETH	0	4	
0×B817CE41772F152992e463A3C7a6b9aD120E3986	100.00 ETH	0	5	

2.2.2. Action: await instance.bid({from:accounts[1],value:web3.utils.toWei('5','ether')})

gasUsed: 54503,

2.3. auctionEnd Function:

```
gasUsed: 52191
```

```
/usr/bin/bash --login -i
        transactionHash: '0x1bbad7c3efbbb27e2dfa883049f66833f7a9b4d76d170631b3fbec3852c72106',
        blockHash: '0xb1abd25b9fa6850a6bf2ff6ed01d3767e3baa6f564258f616903afcce6b05371',
        blockNumber: 6,
        address: '0xd3647a9f59045e1979563698157E302D7c41a92B',
        type: 'mined',
        id: 'log_c5e484ee',
        event: 'HighestBidIncreased',
        args: [Result]
    }
  ]
}
truffle(ganache)> await instance.auctionEnd({from:accounts[0]})
{
  tx: '0xbab28ce456407da30a1dfb646b97d163bc136c69b2aa48765caf144fa1135149',
  receipt: {
        transactionHash: '0xbab28ce456407da30a1dfb646b97d163bc136c69b2aa48765caf144fa1135149',
        transactionIndex: 0,
        blockHash: '0x40a5884985289b1e5d02db99a60c0b34835c2202069c60314f737e4256994ad6',
        blockNumber: 7,
        from: '0xfd005d89e2fe4b22348c21fd84773bf45cf2f6b1',
        to: '0xd3647a9f59045e1979563698157e302d7c41a92b',
        gasUsed: 52191,
        cumulativeGasUsed: 52191,
        contractAddress: null,
        logs: [ [Object] ],
        status: true,
        logsBloom: '0x000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000001000
0000000000004000000000000000000000001000000000000000000000000000000000000000000000000000
        v: '0x1c',
        r: '0x70140654a0f6b5366f90f601f7ad77d7f6857ab88e2df66a50495aecd199d55f',
        s: '0x4d458cf2c469e63e5149515a9301c2c5213df4349a6943a29d70bad5846231b5',
        rawLogs: [ [Object] ]
  },
  logs: [
    {
        logIndex: 0,
        transactionIndex: 0,
        transactionHash: '0xbab28ce456407da30a1dfb646b97d163bc136c69b2aa48765caf144fa1135149',
        blockHash: '0x40a5884985289b1e5d02db99a60c0b34835c2202069c60314f737e4256994ad6',
        blockNumber: 7,
        address: '0xd3647a9f59045e1979563698157E302D7c41a92B',
        type: 'mined',
        id: 'log_d0876097',
        event: 'AuctionEnded',
        args: [Result]
    }
  ]
}
truffle(ganache)> |
```

Ganache

ACCOUNTS | BLOCKS | TRANSACTIONS | CONTRACTS | EVENTS | LOGS | SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK 7 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK PETERSBURG | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE KNOWN-PRODUCE | SWITCH

MNEMONIC
more paddle scissors photo finish sing matrix snow this wrist build announce

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×fD005d89e2Fe4B22348c21FD84773BF45cF2f6b1	104.98 ETH	5	0
0×673C667c4EBeEF95D458e9FdDeed98C9854ba9D4	95.00 ETH	1	1
0×2211CAA2E361554534b4C451A25151276Db64f86	97.00 ETH	1	2
0×1b09AAEb7b7da83F9Ee386715D22eE92d2C151f9	100.00 ETH	0	3
0×0B02b3cd75c7052c79c13E720A6d13A6Ae585DDE	100.00 ETH	0	4
0×B817CE41772F152992e463A3C7a6b9aD120E3986	100.00 ETH	0	5
ADDRESS	BALANCE	TX COUNT	INDEX

2.4. Withdraw function:

`gasUsed: 19421`

```
      status: true,
      logsBloom: '0x00000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000040000000000000000000000010000000000000000000000000000000000000000000000
      v: '0x1c',
      r: '0x70140654a0f6b5366f90f601f7ad77d7f6857ab88e2df66a50495aecd199d55f',
      s: '0x4d458cf2c469e63e5149515a9301c2c5213df4349a6943a29d70bad5846231b5',
      rawLogs: [ [Object] ]
    },
  logs: [
    {
      logIndex: 0,
      transactionIndex: 0,
      transactionHash: '0xbab28ce456407da30a1dfb646b97d163bc136c69b2aa48765caf144fa1135149',
      blockHash: '0x40a5884985289b1e5d02db99a60c0b34835c2202069c60314f737e4256994ad6',
      blockNumber: 7,
      address: '0xd3647a9f59045e1979563698157E302D7c41a92B',
      type: 'mined',
      id: 'log_d0876097',
      event: 'AuctionEnded',
      args: [Result]
    }
  ]
}
truffle(ganache)> await instance.withdraw({from:accounts[2]})
{
  tx: '0xa50ef0fd0a6407a8b026164d867d021f526524b018b440b86a00a429f5aeca04',
  receipt: {
    transactionHash: '0xa50ef0fd0a6407a8b026164d867d021f526524b018b440b86a00a429f5aeca04',
    transactionIndex: 0,
    blockHash: '0x28f399bf3cf19bdb04f7c9ecb493f933505fbf2d48aa676f2e2da5aa2b3e0ce5',
    blockNumber: 8,
    from: '0x2211caa2e361554534b4c451a25151276db64f86',
    to: '0xd3647a9f59045e1979563698157e302d7c41a92b',
    gasUsed: 19421,
    cumulativeGasUsed: 19421,
    contractAddress: null,
    logs: [],
    status: true,
    logsBloom: '0x00000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000
      v: '0x1b',
      r: '0x65c027f8b01a1a0be5a8eab48f83b8f57f028226d7739064ca1c47c5becea547',
      s: '0x599ed4a7e8feedeb93a75960cda4adbcac91da18edb64d845e117ecc1e4b9a4c',
      rawLogs: []
  },
  logs: []
}
truffle(ganache)>
```

3. A screenshot showing the details of the transaction sent from the contract to the beneficiary account when "auctionEnd" is triggered

```
ruffle(ganache)> await instance.auctionEnd({from:accounts[0]})
 tx: '0xbab28ce456407da30a1dfb646b97d163bc136c69b2aa48765caf144fa1135149',
 receipt: {
   transactionHash: '0xbab28ce456407da30a1dfb646b97d163bc136c69b2aa48765caf144fa1135149',
   transactionIndex: 0,
   blockHash: '0x40a5884985289b1e5d02db99a60c0b34835c2202069c60314f737e4256994ad6',
   blockNumber: 7,
   from: '0xfD005d89e2fe4b22348c21fd84773bf45cf2f6b1',
   to: '0xd3647a9f59045e1979563698157e302d7c41a92b',
   gasUsed: 52191,
   cumulativeGasUsed: 52191,
   contractAddress: null,
   logs: [ [Object] ],
   status: true,
   logsBloom: '0x00000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000001000
000000000040000000000000000000000000000010000000000000000000000000000000000000000
   v: '0x1c',
   r: '0x70140654a0f6b5366f90f601f7ad77d7f6857ab88e2df66a50495aecd199d55f',
   s: '0x4d458cf2c469e63e5149515a9301c2c5213df4349a6943a29d70bad5846231b5',
   rawLogs: [ [Object] ]
 },
 logs: [
   {
     logIndex: 0,
     transactionIndex: 0,
     transactionHash: '0xbab28ce456407da30a1dfb646b97d163bc136c69b2aa48765caf144fa1135149',
     blockHash: '0x40a5884985289b1e5d02db99a60c0b34835c2202069c60314f737e4256994ad6',
     blockNumber: 7,
     address: '0xd3647a9f59045e1979563698157E302D7c41a92B',
     type: 'mined',
     id: 'log_d0876097',
     event: 'AuctionEnded',
     args: [Result]
   }
 ]
ruffle(ganache)> |
```

ADDRESS	BALANCE		TX COUNT	INDEX	
0×fD005d89e2Fe4B22348c21FD84773BF45cF2f6b1	104.98 ETH		5	0	
0×673C667c4EBeEF95D458e9FdDeed98C9854ba9D4	95.00 ETH		1	1	
0×2211CAA2E361554534b4C451A25151276Db64f86	97.00 ETH		1	2	
0×1b09AAEb7b7da83F9Ee386715D22eE92d2C151f9	100.00 ETH		0	3	
0×0B02b3cd75c7052c79c13E720A6d13A6Ae585DDE	100.00 ETH		0	4	
0×B817CE41772F152992e463A3C7a6b9aD120E3986	100.00 ETH		0	5	

Since 3ETH, 5ETH are the bids that were raised, after auctionEnd, the beneficiary will have 100+5-transactioncost in its account.
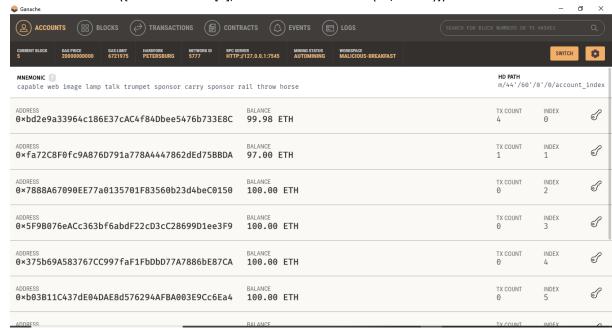
4. Some other scenarios:

a. Only beneficiary can call auction end function. Any other calling should give an error.

```
truffle(ganache)> await instance.auctionEnd({from:accounts[2]})
Thrown:
Error: Returned error: VM Exception while processing transaction:
revert Only beneficiary can trigger autionEnd -- Reason given: Only
beneficiary can trigger autionEnd.
```
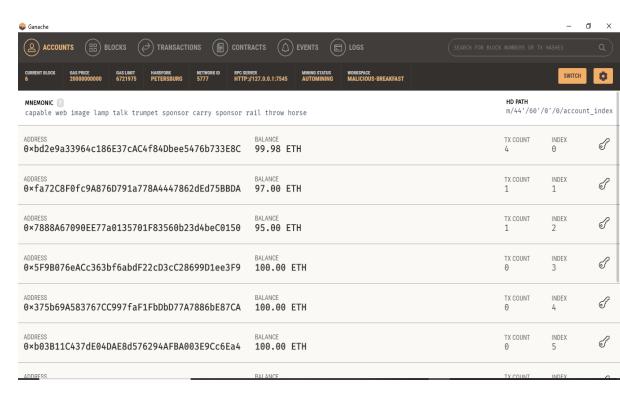

b. If A bids 3, B bids 5, A again bids 7, Then all bids are accepted and after auction end, beneficiary account is credited by 7, and when A calls withdraw function, 3ether should be credited to A's account.

await instance.bid({from:accounts[1],value:web3.utils.toWei('3','ether')})

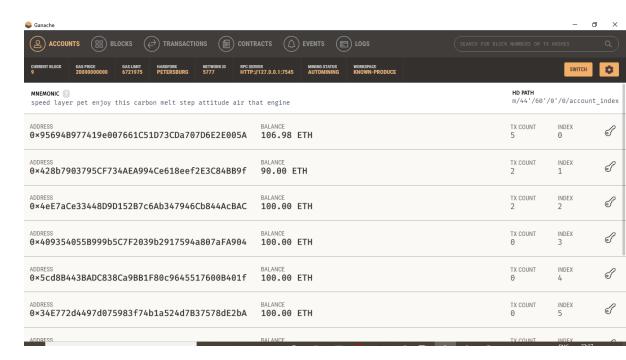await instance.bid({from:accounts[2],value:web3.utils.toWei('5','ether')})

await instance.bid({from:accounts[1],value:web3.utils.toWei('7','ether')})

await instance.auctionEnd({from:accounts[0]})

await instance.withdraw({from:accounts[2]})

await instance.withdraw({from:accounts[1]})

Ganache

ACCOUNTS   BLOCKS   TRANSACTIONS   CONTRACTS   EVENTS   LOGS   SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE	
10	20000000000	6721975	PETERSBURG	5777	HTTP://127.0.0.1:7545	AUTOMINING	KNOWN-PRODUCE	SWITCH ⚙

MNEMONIC ❓
speed layer pet enjoy this carbon melt step attitude air that engine

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX	
0×95694B977419e007661C51D73CDa707D6E2E005A	106.98 ETH	5	0	🔑
0×428b7903795CF734AEA994Ce618eef2E3C84BB9f	93.00 ETH	3	1	🔑
0×4eE7aCe33448D9D152B7c6Ab347946Cb844AcBAC	100.00 ETH	2	2	🔑
0×409354055B999b5C7F2039b2917594a807aFA904	100.00 ETH	0	3	🔑
0×5cd8B443BADC838Ca9BB1F80c9645517600B401f	100.00 ETH	0	4	🔑
0×34E772d4497d075983f74b1a524d7B37578dE2bA	100.00 ETH	0	5	🔑
ADDRESS	BALANCE	TX COUNT	INDEX	🔑