Blockchain Assignment 1

Name: Arijit Dutta

[redacted]

Functions:

- bid() -

  This function is used to place a bid. A user can place a bid only when the auction has not already ended. We have used a require() for that purpose. Also, if the bid is less than or equal to the highest bid, the current bid should be refused. If all these criterias are fulfilled, the function stores the current bid and the bidder in variables. Then the previous highest bidder is pushed into a pendingReturns map and the current bidder and the bid is marked as the highest bid. The pendingReturns map contains those bidders and their bids whose bids have been surpassed and they can withdraw their previous bids.

- withdraw() -

  This function is used by the accounts who wants to withdraw their bids once they have been surpassed by other accounts. If the refund amount of the account present in the ‘pendingReturns’ map is greater than 0 only then the refund is processed and the refund amount for that account in the ‘pendingReturns’ map is put to 0, so that account cannot withdraw multiple times. In case the return fails, the refund amount in the ‘pendingReturns’ map is not decreased to 0.

- auctionEnd() -

  This function can be called only by the beneficiary only which is Account 0. And it can be called only once. These two requirements are checked using require(). The aucEnd variable is set to ‘true’ which indicates that the auction has ended. Then the highest bid is transferred to Account 0.

The screenshots of various functions, their gas used and any other useful information is shared in the Demonstration section.

Demonstration:

- Deploying Migrations

```
Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


1_initial_migration.js
======================

   Replacing 'Migrations'
   ----------------------
   ⠿ Blocks: 0            Seconds: 0   > transaction hash:    0x0ed1b917e7eb16e579848cadf86a9336a36a82cff4bfdaf0744e5d0383d5738f
   > Blocks: 0            Seconds: 0
   > contract address:    0x75Eb50375E7393F7F1E29cf31132F457Ec13AB18
   > block number:        1
   > block timestamp:     1644444582
   > account:             0xa665D1CC351644C35fF31cb33f75D9F15A81a04F
   > balance:             99.9967165
   > gas used:            164175 (0x2814f)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0032835 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.0032835 ETH
```

- Deploying Contract

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

   Replacing 'Auction'
   -------------------
   ⠿ Blocks: 0            Seconds: 0   > transaction hash:    0x92f1bbe69372d73b2f6c21e93e802ce082f4cf17f327055caed3ecd7c3c6534b
   > Blocks: 0            Seconds: 0
   > contract address:    0x98365070E2176d9Dc8033a8750a75fe607f2a492
   > block number:        3
   > block timestamp:     1644444582
   > account:             0xa665D1CC351644C35fF31cb33f75D9F15A81a04F
   > balance:             99.98634632
   > gas used:            476168 (0x74408)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00952336 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00952336 ETH

Summary
=======
> Total deployments:   2
> Final cost:          0.01280686 ETH
```

Total cost = 0.0128

- Cost of the transactions. The contract is deployed by Account 0 and thus it has incurred the cost as seen below. Account 0 is the beneficiary.

ADDRESS	BALANCE	TX COUNT	INDEX
0×a665D1CC351644C35fF31cb33f75D9F15A81a04F	99.99 ETH	4	0
0×A36A52C4FEF5C2aD269e84fCF2Fd5fbc97020FB7	100.00 ETH	0	1
0×eE315aA4b904753a088D0e1e9D261Da572A3957b	100.00 ETH	0	2
0×D44583534AE22C07e3dAb76d6a735662Ab01C17f	100.00 ETH	0	3
0×FB282b4b944A7940a3634944c73793C2a9b76a7D	100.00 ETH	0	4
0×20d0dCb76BdA4fd4E6A41dae70f2513F26EB435e	100.00 ETH	0	5

- Total of 4 blocks have been created during deployment and the gas used for each block is shown below

CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
4	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

SAVE SWITCH

BLOCK	MINED ON	GAS USED	
4	2022-02-09 17:09:43	27341	1 TRANSACTION
3	2022-02-09 17:09:42	476168	1 TRANSACTION
2	2022-02-09 17:09:42	42341	1 TRANSACTION
1	2022-02-09 17:09:42	164175	1 TRANSACTION
0	2022-02-09 17:08:59	0	NO TRANSACTIONS

- Account 4 starts the bid with 5 Ether.

```
truffle(development)> instance.bid({from: accounts[4],value: web3.utils.toWei('5','ether')} )
{
  tx: '0x79d001575ef848fb3703e64bbaf6131ffa0a34e68c1d52397155a2ea649948e0',
  receipt: {
    transactionHash: '0x79d001575ef848fb3703e64bbaf6131ffa0a34e68c1d52397155a2ea649948e0',
    transactionIndex: 0,
    blockHash: '0x06b1e298aca95ca650a1a2f921bbc4474558131a4a1f2b0fbcd45c7ee8f2bc0a',
    blockNumber: 5,
    from: '0xfb282b4b944a7940a3634944c73793c2a9b76a7d',
    to: '0x98365070e2176d9dc8033a8750a75fe607f2a492',
    gasUsed: 67104,
    cumulativeGasUsed: 67104,
    contractAddress: null,
    logs: [],
    status: true,
    logsBloom: '0x0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000',
    rawLogs: []
  },
  logs: []
}
truffle(development)> 
```

ADDRESS	BALANCE	TX COUNT	INDEX
0×a665D1CC351644C35fF31cb33f75D9F15A81a04F	99.99 ETH	4	0
0×A36A52C4FEF5C2aD269e84fCF2Fd5fbc97020FB7	100.00 ETH	0	1
0×eE315aA4b904753a088D0e1e9D261Da572A3957b	100.00 ETH	0	2
0×D44583534AE22C07e3dAb76d6a735662Ab01C17f	100.00 ETH	0	3
0×FB282b4b944A7940a3634944c73793C2a9b76a7D	95.00 ETH	1	4
0×20d0dCb76BdA4fd4E6A41dae70f2513F26EB435e	100.00 ETH	0	5

Gas used to bid()

← BACK **BLOCK 5**

GAS USED	GAS LIMIT	MINED ON	BLOCK HASH
67104	6721975	2022-02-09 17:27:55	0×06b1e298aca95ca650a1a2f921bbc4474558131a4a1f2b0fbcd45c7ee8f2bc0a

TX HASH
0×79d001575ef848fb3703e64bbaf6131ffa0a34e68c1d52397155a2ea649948e0

CONTRACT CALL

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×FB282b4b944A7940a3634944c73793C2a9b76a7D	0×98365070E2176d9Dc8033a8750a75fe607f2a492	67104	5000000000000000000

- Account 2 bids 2 Ether. As it is not the highest bid, it is not accepted. Account 2 balance is not deducted as well.

```
  data: {
    '0x7e7a3a40676615af6dbbd3fbb825b610c56dab6b39c618747924baf463ec1de1': {
      error: 'revert',
      program_counter: 608,
      return: '0x08c379a000000000000000000000000000000000000000000000000000000000000000200000000000000000000000000000000000000000000000000000000000000025412
06869676865722062696420686173206c7265616479206265656e20706c616365642e000000000000000000000000000000000000000000000000000000',
      reason: 'A higher bid has already been placed.'
    },
    stack: 'RuntimeError: VM Exception while processing transaction: revert A higher bid has already been placed.\n' +
      '    at Function.RuntimeError.fromResults (/Applications/Ganache.app/Contents/Resources/static/node/node_modules/ganache-core/lib/utils/runtimeerror.j
s:94:13)\n' +
      '    at BlockchainDouble.processBlock (/Applications/Ganache.app/Contents/Resources/static/node/node_modules/ganache-core/lib/blockchain_double.js:627
:24)\n' +
      '    at runMicrotasks (<anonymous>)\n' +
      '    at processTicksAndRejections (internal/process/task_queues.js:93:5)',
    name: 'RuntimeError'
  },
  reason: 'A higher bid has already been placed.',
  hijackedStack: 'Error: Returned error: VM Exception while processing transaction: revert A higher bid has already been placed. -- Reason given: A higher b
id has already been placed..\n' +
    '    at Object.ErrorResponse (/usr/local/lib/node_modules/truffle/build/webpack:/node_modules/web3-core-helpers/lib/errors.js:28:1)\n' +
    '    at /usr/local/lib/node_modules/truffle/build/webpack:/node_modules/web3/node_modules/web3-core-requestmanager/lib/index.js:302:1\n' +
    '    at /usr/local/lib/node_modules/truffle/build/webpack:/packages/provider/wrapper.js:107:1\n' +
    '    at XMLHttpRequest.request.onreadystatechange (/usr/local/lib/node_modules/truffle/build/webpack:/node_modules/web3/node_modules/web3-providers-http
/lib/index.js:98:1)\n' +
    '    at XMLHttpRequestEventTarget.dispatchEvent (/usr/local/lib/node_modules/truffle/build/webpack:/node_modules/xhr2-cookies/dist/xml-http-request-even
t-target.js:34:1)\n' +
    '    at XMLHttpRequest.exports.modules.996763.XMLHttpRequest._setReadyState (/usr/local/lib/node_modules/truffle/build/webpack:/node_modules/xhr2-cookie
s/dist/xml-http-request.js:208:1)\n' +
    '    at XMLHttpRequest.exports.modules.996763.XMLHttpRequest._onHttpResponseEnd (/usr/local/lib/node_modules/truffle/build/webpack:/node_modules/xhr2-co
okies/dist/xml-http-request.js:318:1)\n' +
    '    at IncomingMessage.<anonymous> (/usr/local/lib/node_modules/truffle/build/webpack:/node_modules/xhr2-cookies/dist/xml-http-request.js:289:47)\n' +
    '    at IncomingMessage.emit (node:events:402:35)\n' +
    '    at IncomingMessage.emit (node:domain:537:15)\n' +
    '    at endReadableNT (node:internal/streams/readable:1343:12)\n' +
    '    at processTicksAndRejections (node:internal/process/task_queues:83:21)'
}
truffle(development)>
```

ADDRESS	BALANCE	TX COUNT	INDEX
0×a665D1CC351644C35fF31cb33f75D9F15A81a04F	99.99 ETH	4	0
0×A36A52C4FEF5C2aD269e84fCF2Fd5fbc97020FB7	100.00 ETH	0	1
0×eE315aA4b904753a088D0e1e9D261Da572A3957b	100.00 ETH	1	2
0×D44583534AE22C07e3dAb76d6a735662Ab01C17f	100.00 ETH	0	3
0×FB282b4b944A7940a3634944c73793C2a9b76a7D	95.00 ETH	1	4
0×20d0dCb76BdA4fd4E6A41dae70f2513F26EB435e	100.00 ETH	0	5

- Account 8 bids 10 Ether which is the highest bid and so it is accepted.

```
truffle(development)> instance.bid({from: accounts[8],value: web3.utils.toWei('10','ether')} )
{
  tx: '0xd400a4f5031fc1be1d9aff103e13b7b4c037564d3ca04486445adb59d3008e41',
  receipt: {
    transactionHash: '0xd400a4f5031fc1be1d9aff103e13b7b4c037564d3ca04486445adb59d3008e41',
    transactionIndex: 0,
    blockHash: '0x23a75002baa745afca15f97972cff7bbb36a6b9a7cd106d7ce588ba6a0a65709',
    blockNumber: 7,
    from: '0x89d8d16324ae5dd24e9f63b9461c4c5fa7c3466b',
    to: '0x98365070e2176d9dc8033a8750a75fe607f2a492',
    gasUsed: 56304,
    cumulativeGasUsed: 56304,
    contractAddress: null,
    logs: [],
    status: true,
    logsBloom: '0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000',
    rawLogs: []
  },
  logs: []
}
truffle(development)> █
```

ADDRESS	BALANCE	TX COUNT	INDEX
0×20d0dCb76BdA4fd4E6A41dae70f2513F26EB435e	100.00 ETH	0	5
0×0F315c23633E79A1095E10b13129a3f06e62FA49	100.00 ETH	0	6
0×9673a9d6603D1a76EA298B9aa88BF475A7d92Fb3	100.00 ETH	0	7
0×89d8d16324Ae5dd24e9F63b9461c4C5Fa7c3466B	90.00 ETH	1	8
0×50a9451F5287812cD6fD662C5387EB912d85d141	100.00 ETH	0	9

- As highest bid is now 10, Account 4 can withdraw his bid of 5 ether

```
truffle(development)> instance.withdraw({from: accounts[4]} )
{
  tx: '0x8bb039141fcf51562c4fd1f6080378ba0eb8947890f8059a602cc886274c6432',
  receipt: {
    transactionHash: '0x8bb039141fcf51562c4fd1f6080378ba0eb8947890f8059a602cc886274c6432',
    transactionIndex: 0,
    blockHash: '0xb8117eeec03e58681a031339d0cc0d72ab5d9015591e84658b0bb296e03e2c58',
    blockNumber: 8,
    from: '0xfb282b4b944a7940a3634944c73793c2a9b76a7d',
    to: '0x98365070e2176d9dc8033a8750a75fe607f2a492',
    gasUsed: 19854,
    cumulativeGasUsed: 19854,
    contractAddress: null,
    logs: [],
    status: true,
    logsBloom: '0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000',
    rawLogs: []
  },
  logs: []
}
truffle(development)>
```

ADDRESS	BALANCE	TX COUNT	INDEX
0×a665D1CC351644C35fF31cb33f75D9F15A81a04F	99.99 ETH	4	0
0×A36A52C4FEF5C2aD269e84fCF2Fd5fbc97020FB7	100.00 ETH	0	1
0×eE315aA4b904753a088D0e1e9D261Da572A3957b	100.00 ETH	1	2
0×D44583534AE22C07e3dAb76d6a735662Ab01C17f	100.00 ETH	0	3
0×FB282b4b944A7940a3634944c73793C2a9b76a7D	100.00 ETH	2	4
0×20d0dCb76BdA4fd4E6A41dae70f2513F26EB435e	100.00 ETH	0	5

Gas used for withdraw().

SENDER ADDRESS
0×FB282b4b944A7940a3634944c73793C2a9b76a7D

TO CONTRACT ADDRESS
0×98365070E2176d9Dc8033a8750a75fe607f2a492

CONTRACT CALL

VALUE	GAS USED	GAS PRICE	GAS LIMIT	MINED IN BLOCK
0.00 ETH	19854	20000000000	46298	8

TX DATA
0×3ccfd60b

- Auction can be ended only by the beneficiary(Account 0). Let's try to end the auction using Account 5, which will not be allowed.

- Now Account 0 closes the auction. This is allowed and the highest bid is transferred to Account 0.

Gas used for auctionEnd()

Final account balance of Account 0 is 109.98. This is equal to the initial balance of Account 0(100)+highest bid(10)-transaction fees(0.0128).
Calculation = 100 + 10 - 0.0128 = 109.9872

ADDRESS	BALANCE	TX COUNT	INDEX	
0×a665D1CC351644C35fF31cb33f75D9F15A81a04F	109.98 ETH	5	0	
0×A36A52C4FEF5C2aD269e84fCF2Fd5fbc97020FB7	100.00 ETH	0	1	
0×eE315aA4b904753a088D0e1e9D261Da572A3957b	100.00 ETH	1	2	
0×D44583534AE22C07e3dAb76d6a735662Ab01C17f	100.00 ETH	0	3	

- Once the auction is ended, no other account can bid or end the auction again.