# CIS 6930: [Blockchain: Optimization and Applications](http://optnetsci.cise.ufl.edu/class/cis6930sp20/)

# Homework 1

Venkata Sindhu Kandula (UF ID: 1914 5414)

## **Functions:**

## **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. **function withdraw() public returns (bool)**

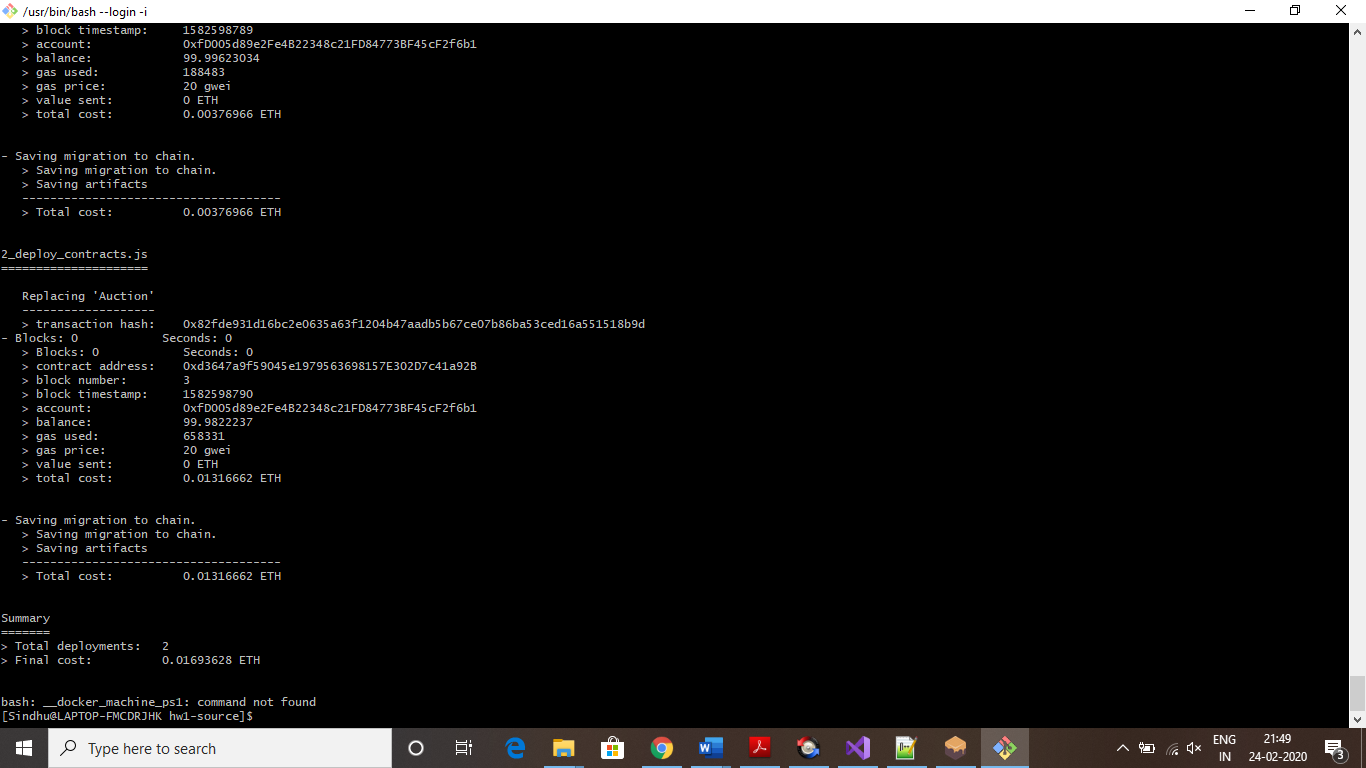
Withdraw a bid that was overbid

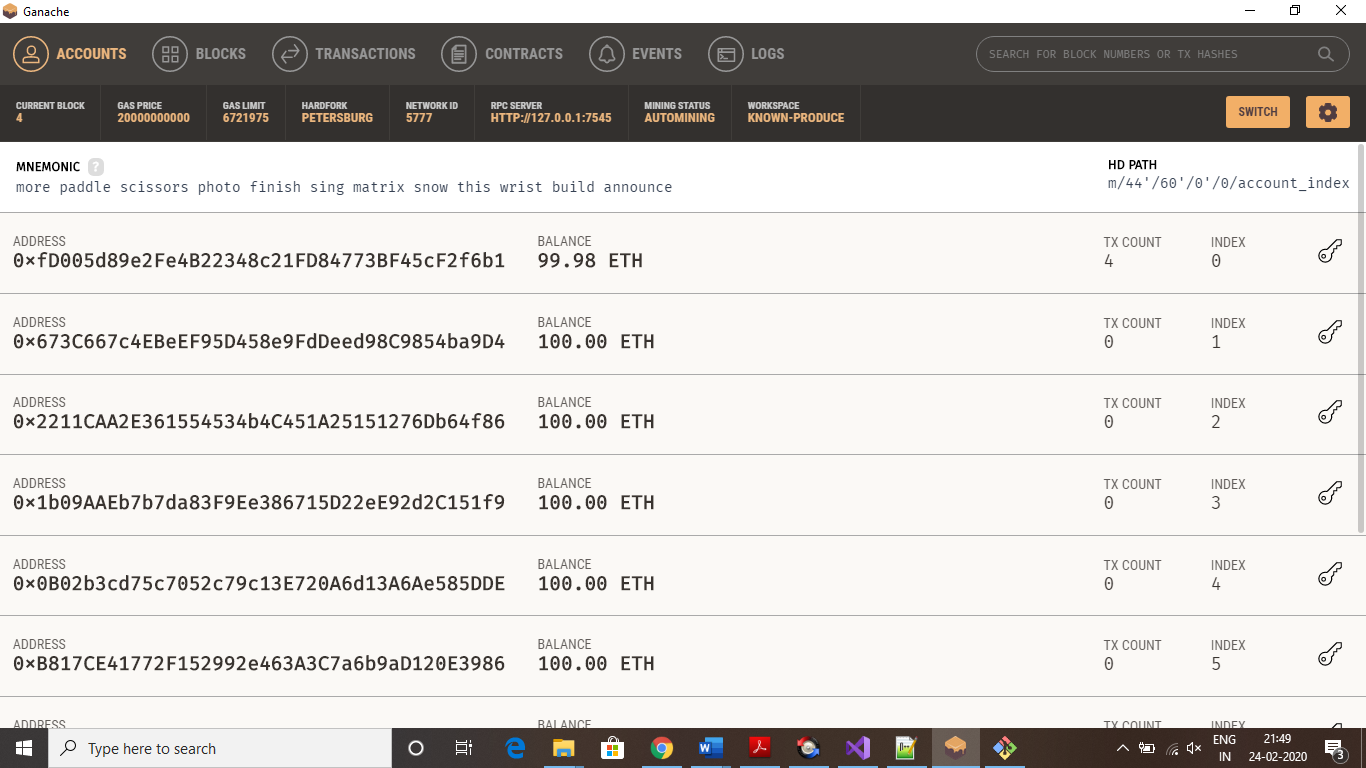
* The amount in pendingReturns is sent to the sender
* False is returned when there is an error when sending
* Else if successful return true
  1. **function auctionEnd() public**
  + Only beneficiary can trigger this function. If not, throw an error "Only beneficiary can trigger autionEnd"
  + Send 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.

## **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

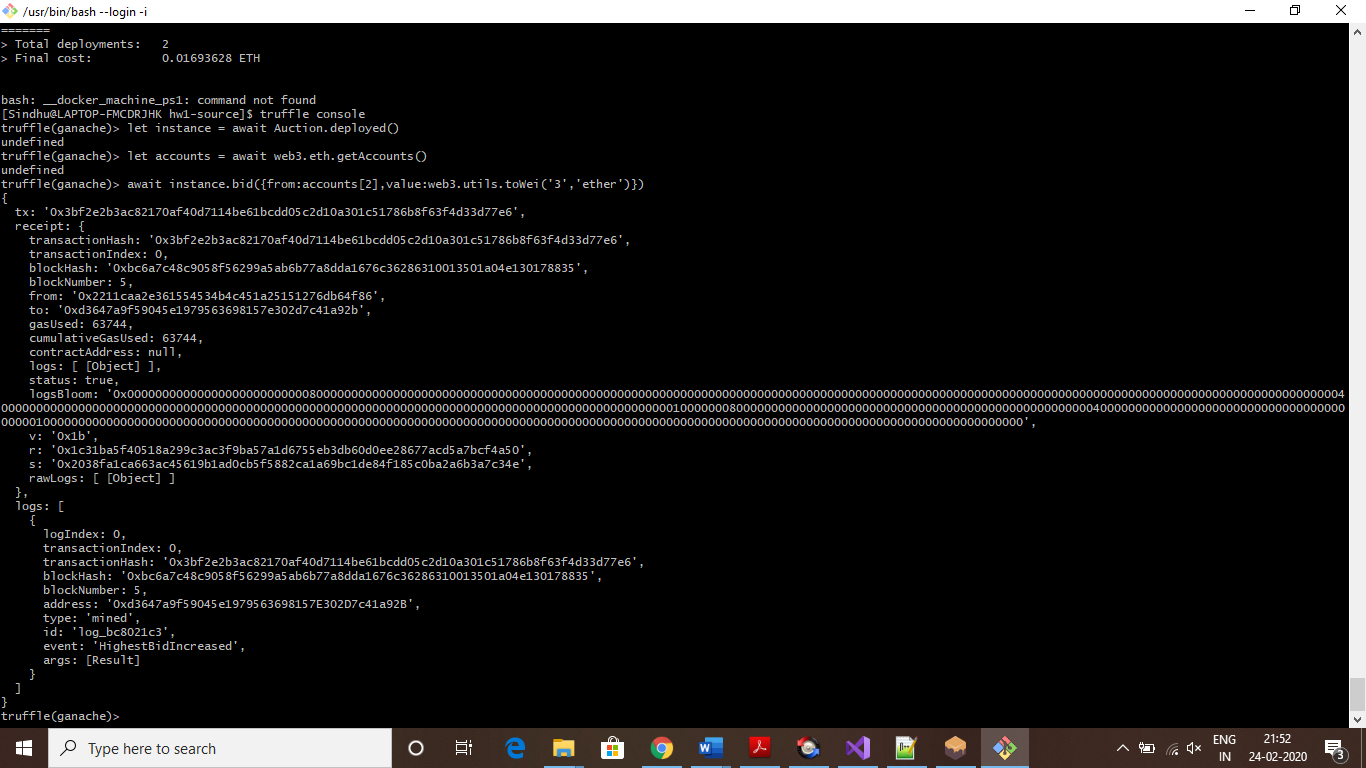


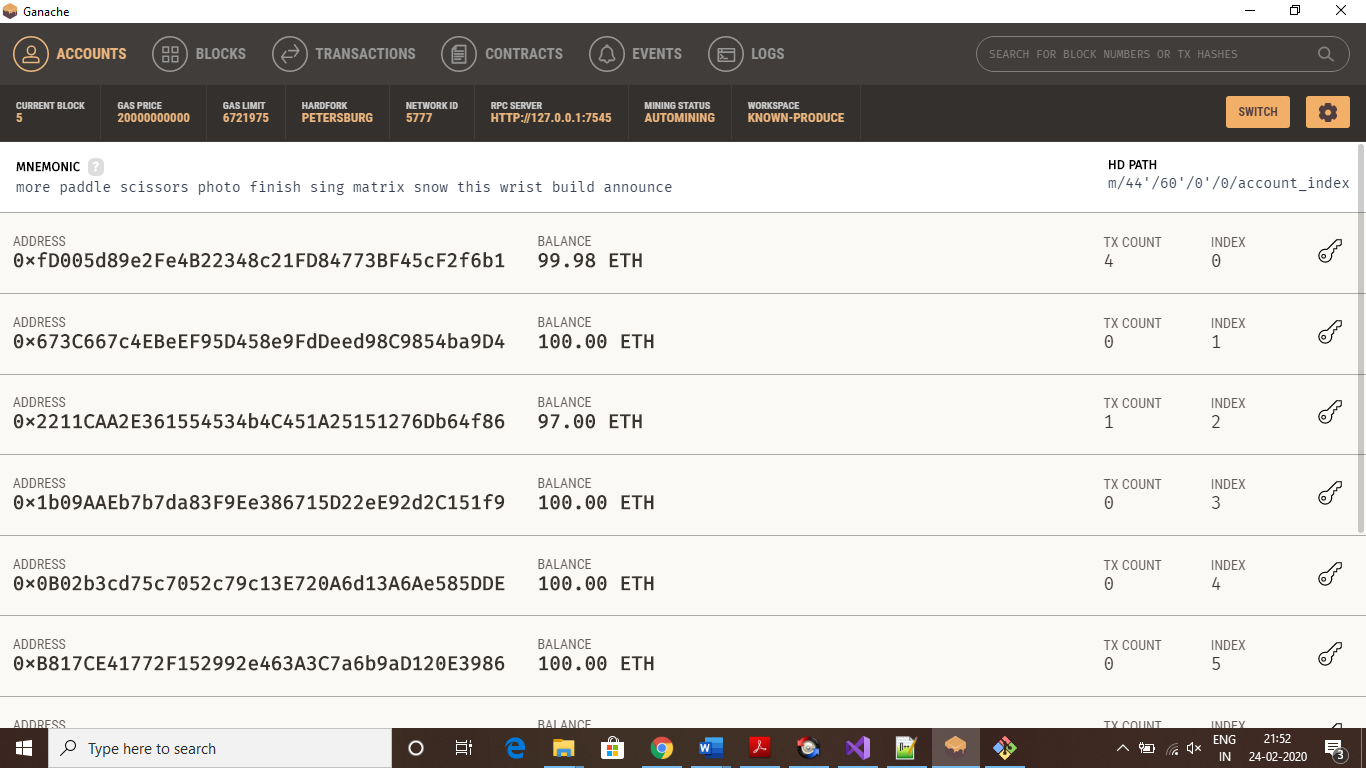


**2.2. Bid function:**

**2.2.1. Action:**

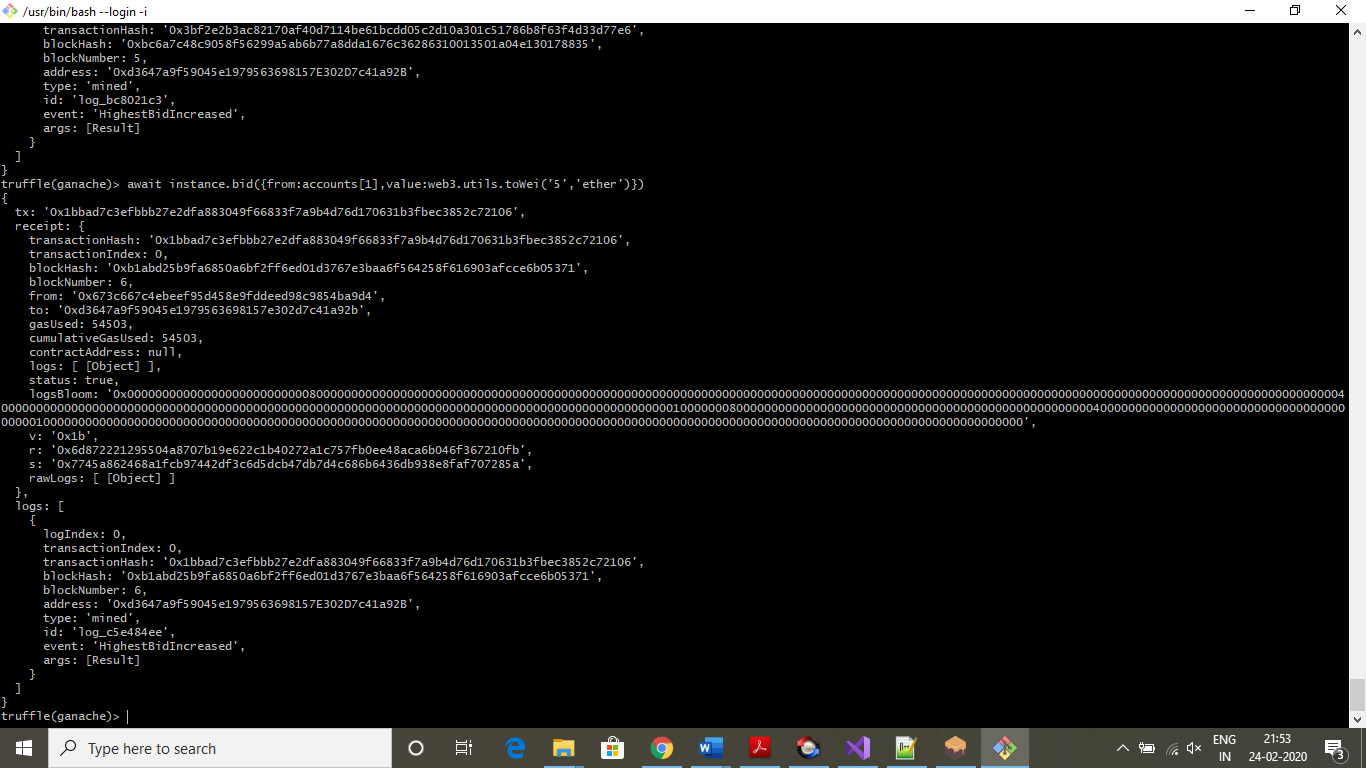
await instance.bid({from:accounts[2],value:web3.utils.toWei('3','ether')})

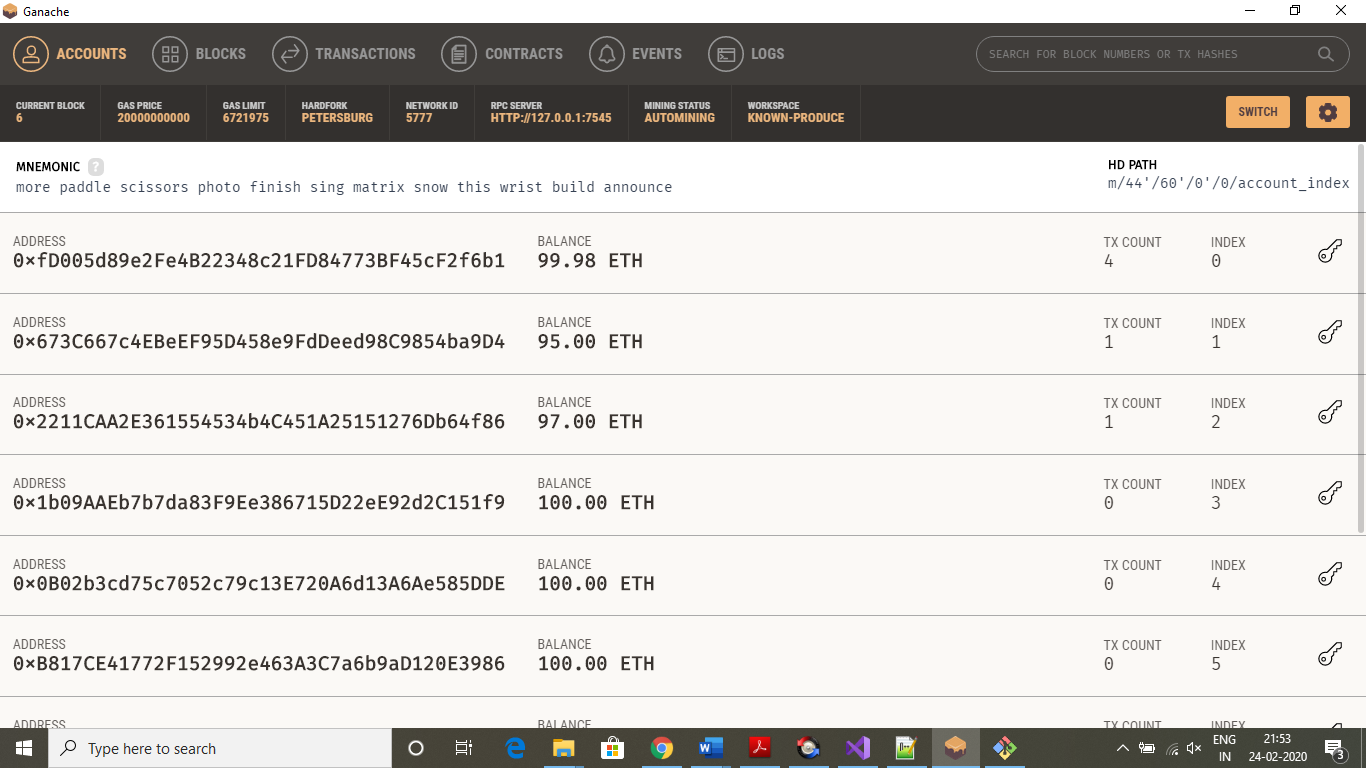
gasUsed: 63744



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

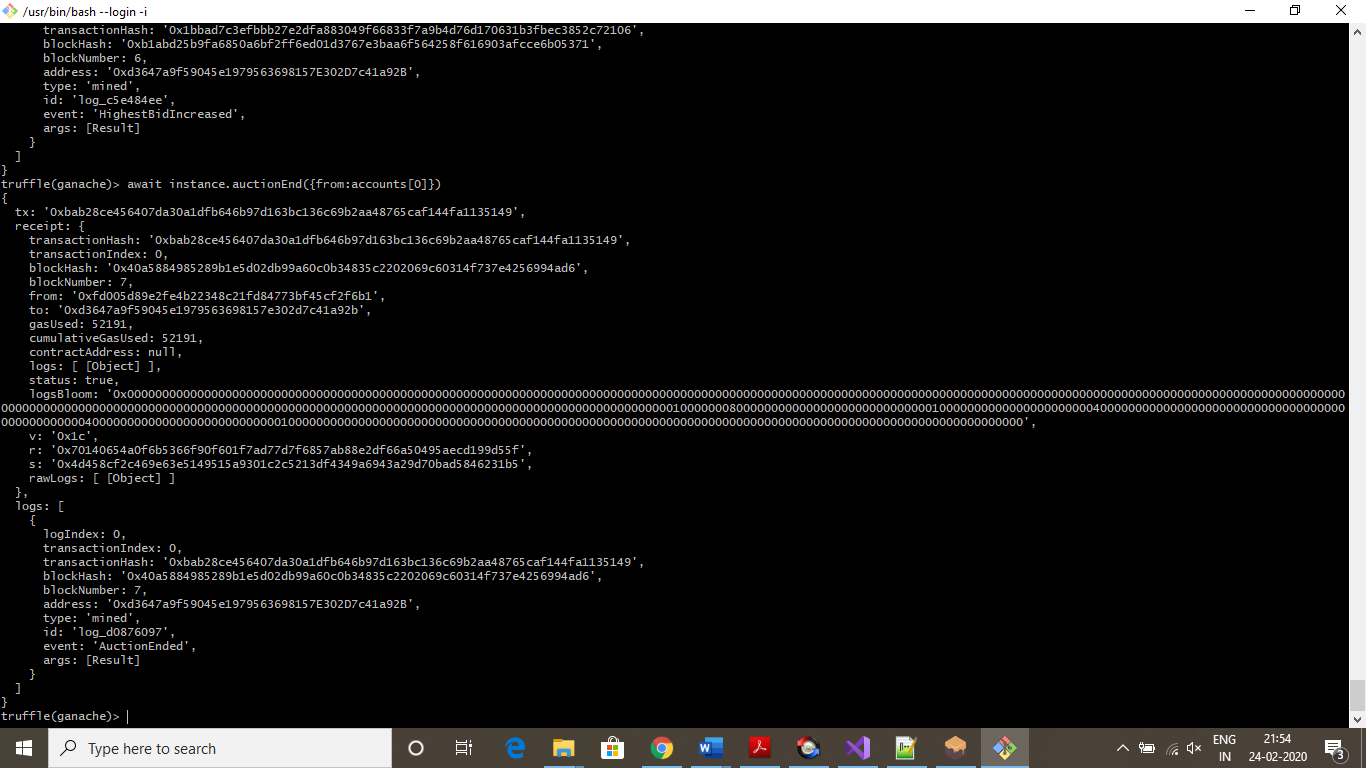
gasUsed: 54503,

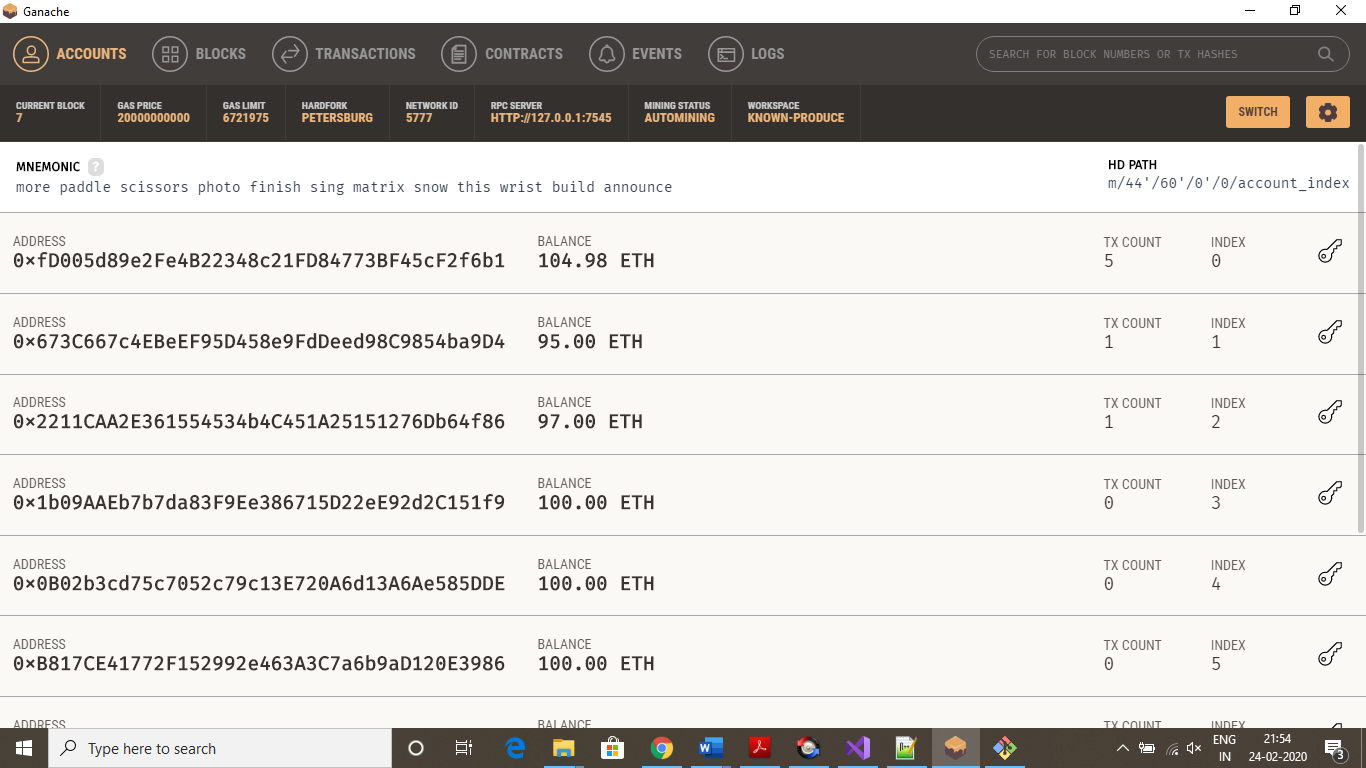




**2.3. auctionEnd Function:**

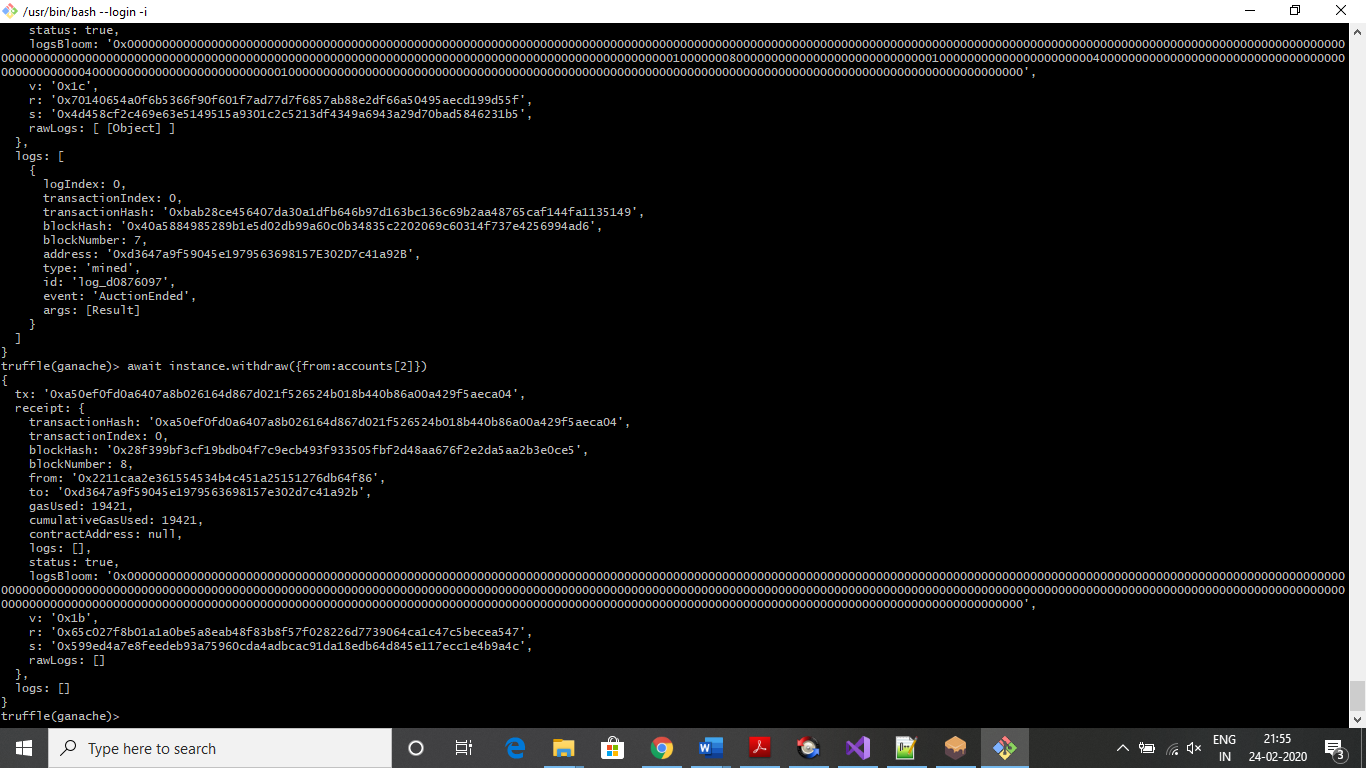
gasUsed: 52191

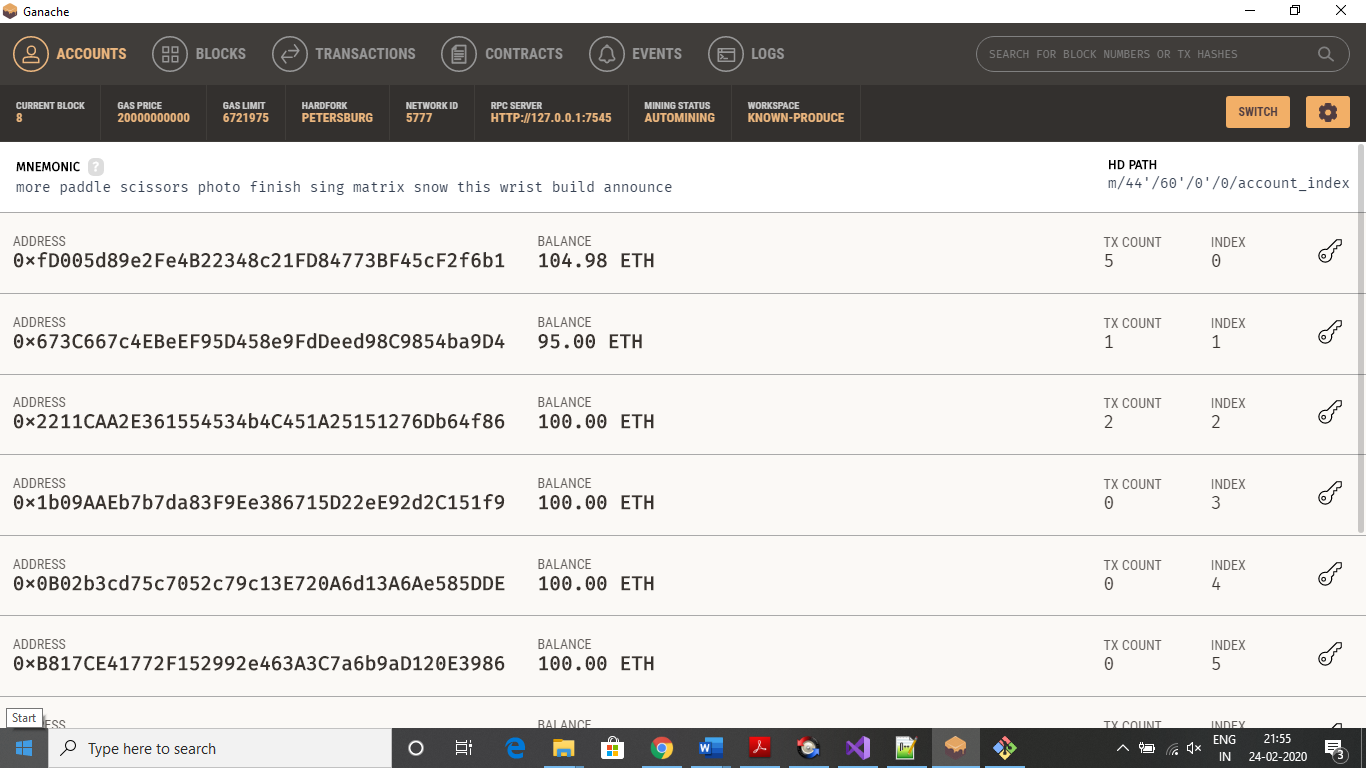




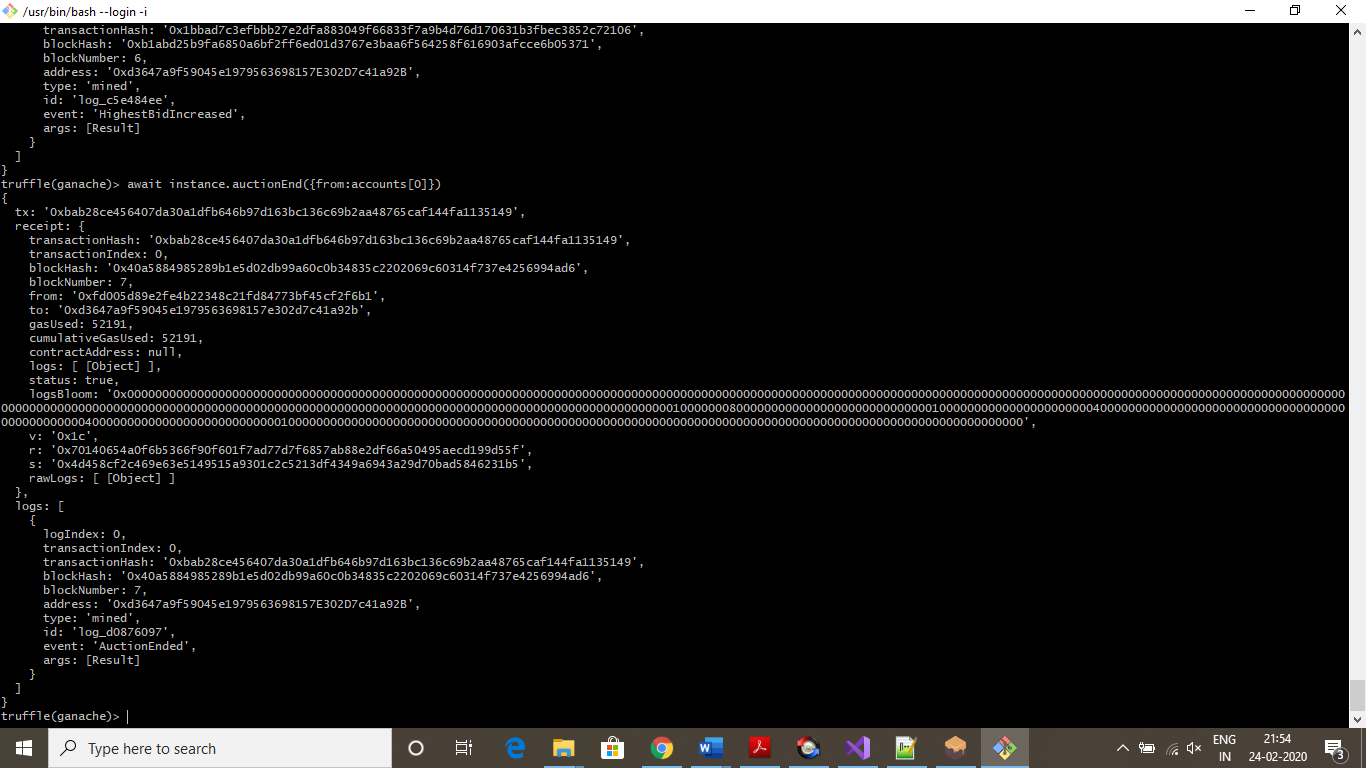
**2.4. Withdraw function:**

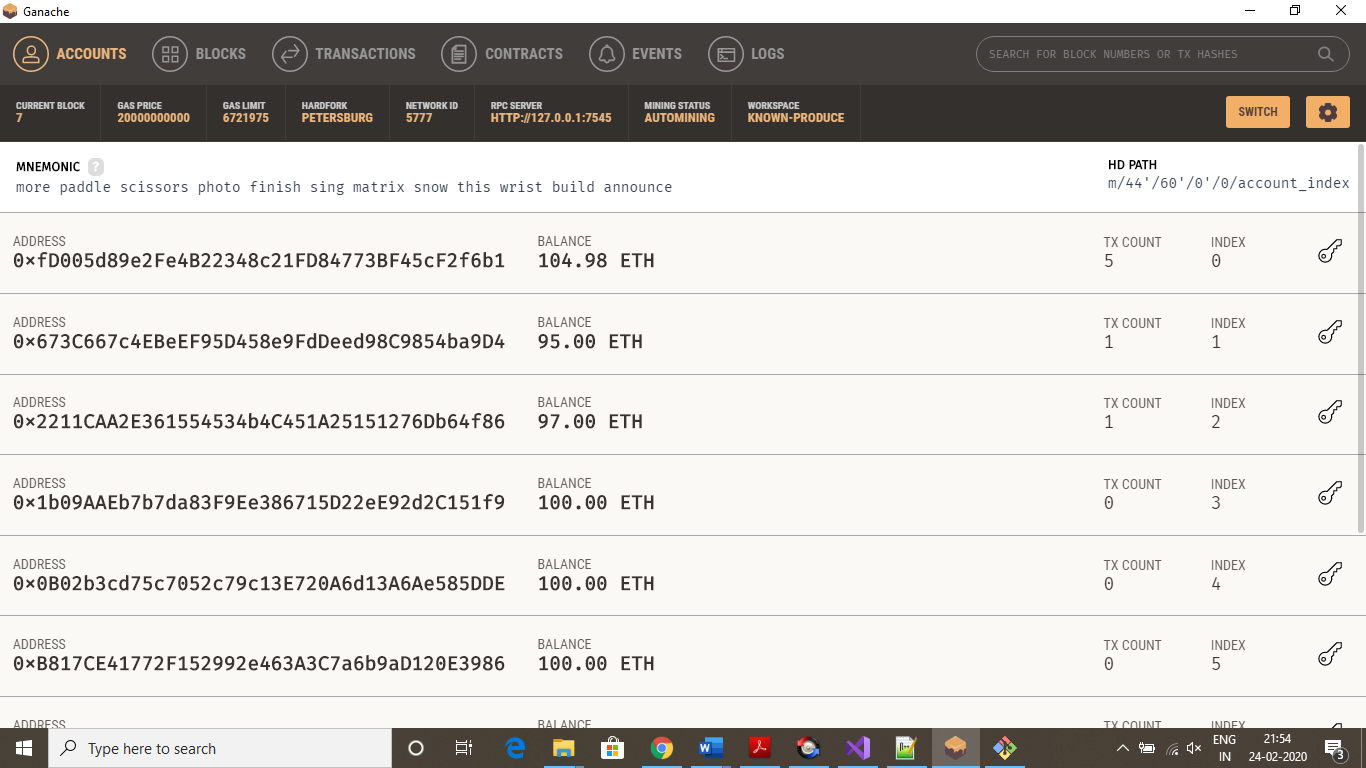
gasUsed: 19421





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





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

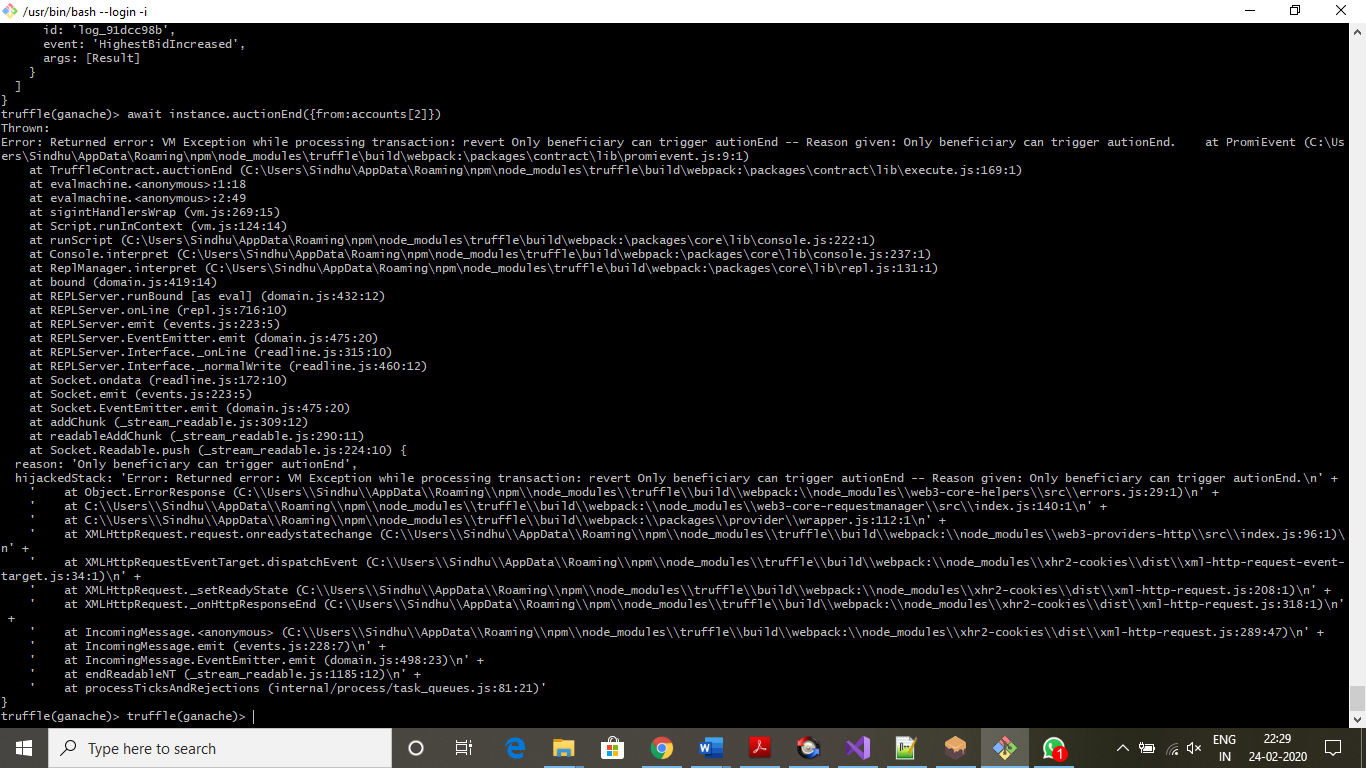
## **Some other scenarios:**

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

truffle(ganache)> await instance.auctionEnd({from:accounts[2]})

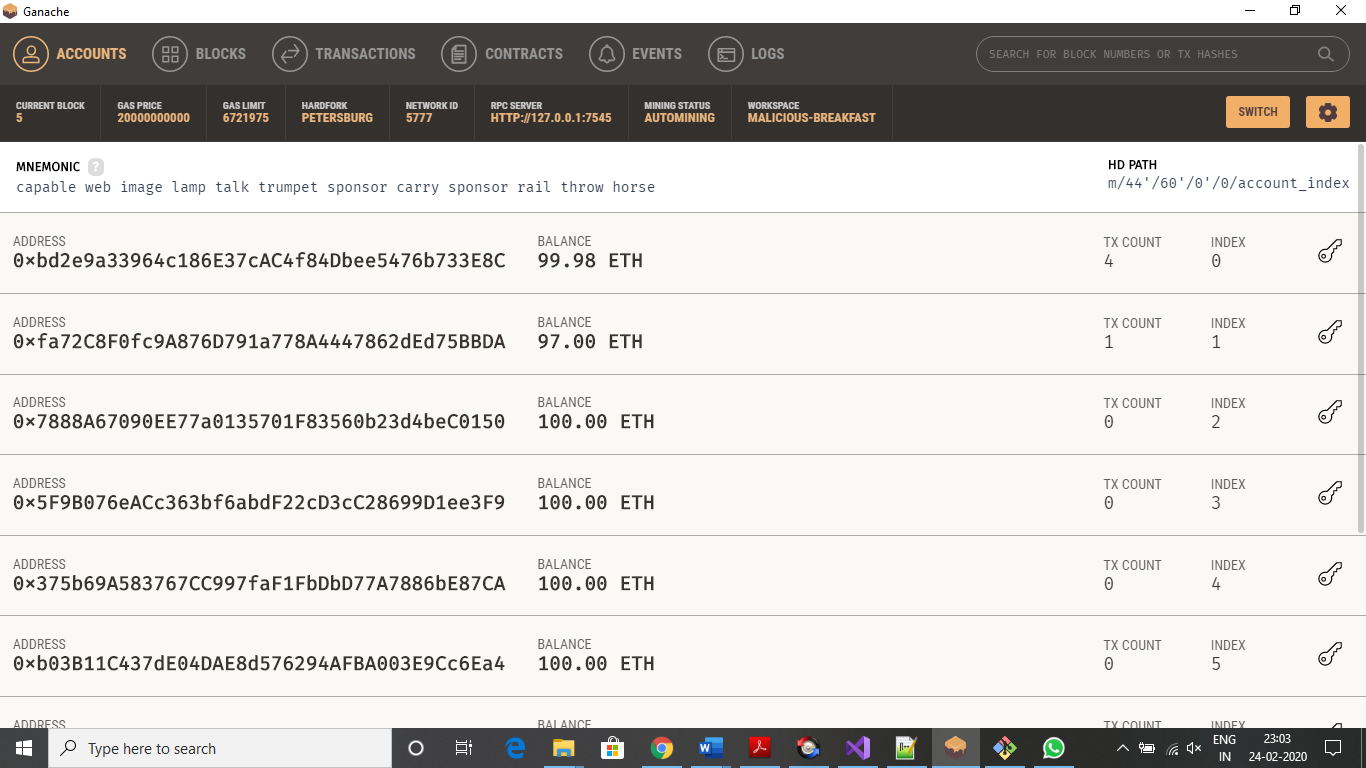
Thrown:

Error: Returned error: VM Exception while processing transaction: revert Only beneficiary can trigger autionEnd -- Reason given: Only beneficiary can trigger autionEnd.

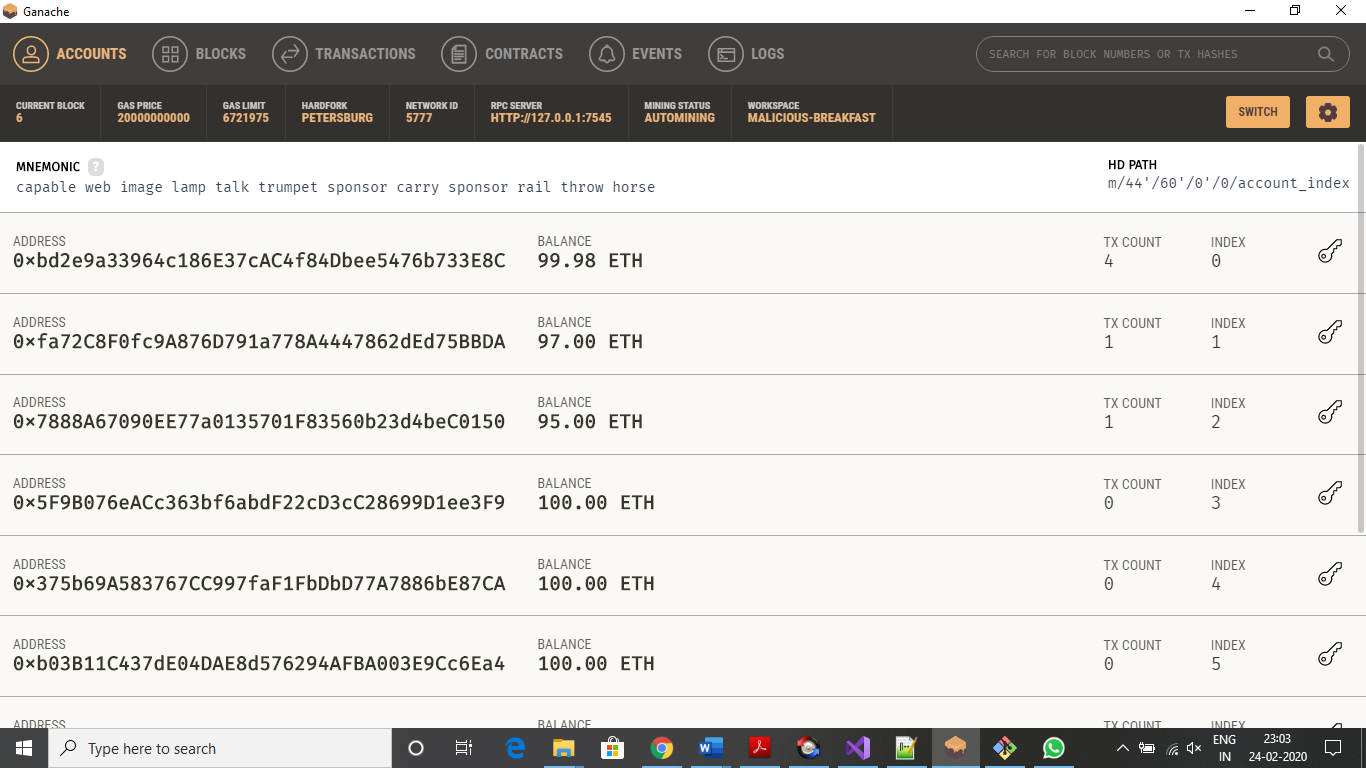


* 1. If A bids 3, B bids 5, A again bids 7, Then all bids are accepted and after auction end, beneficiary account is credited by 7, and when A calls withdraw function, 3ether should be credited to A’s account.

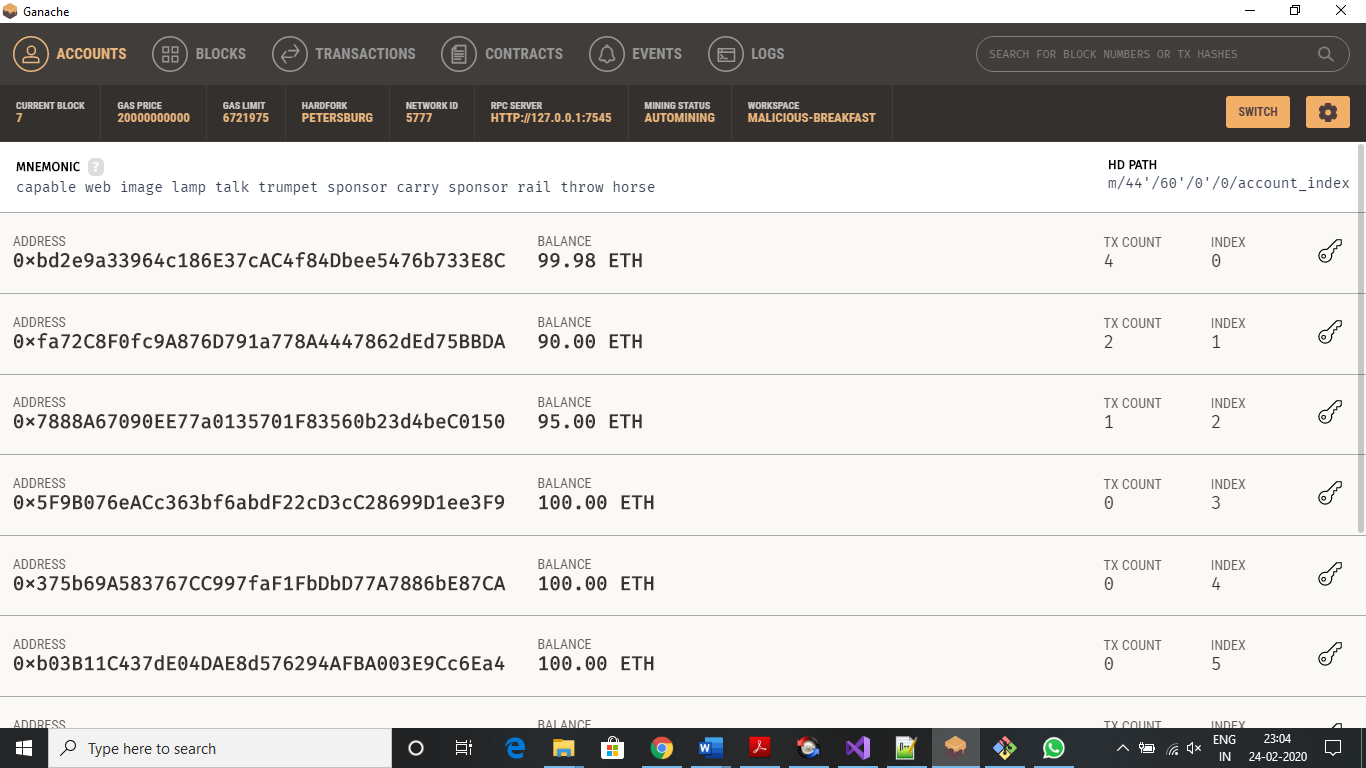
await instance.bid({from:accounts[1],value:web3.utils.toWei('3','ether')})



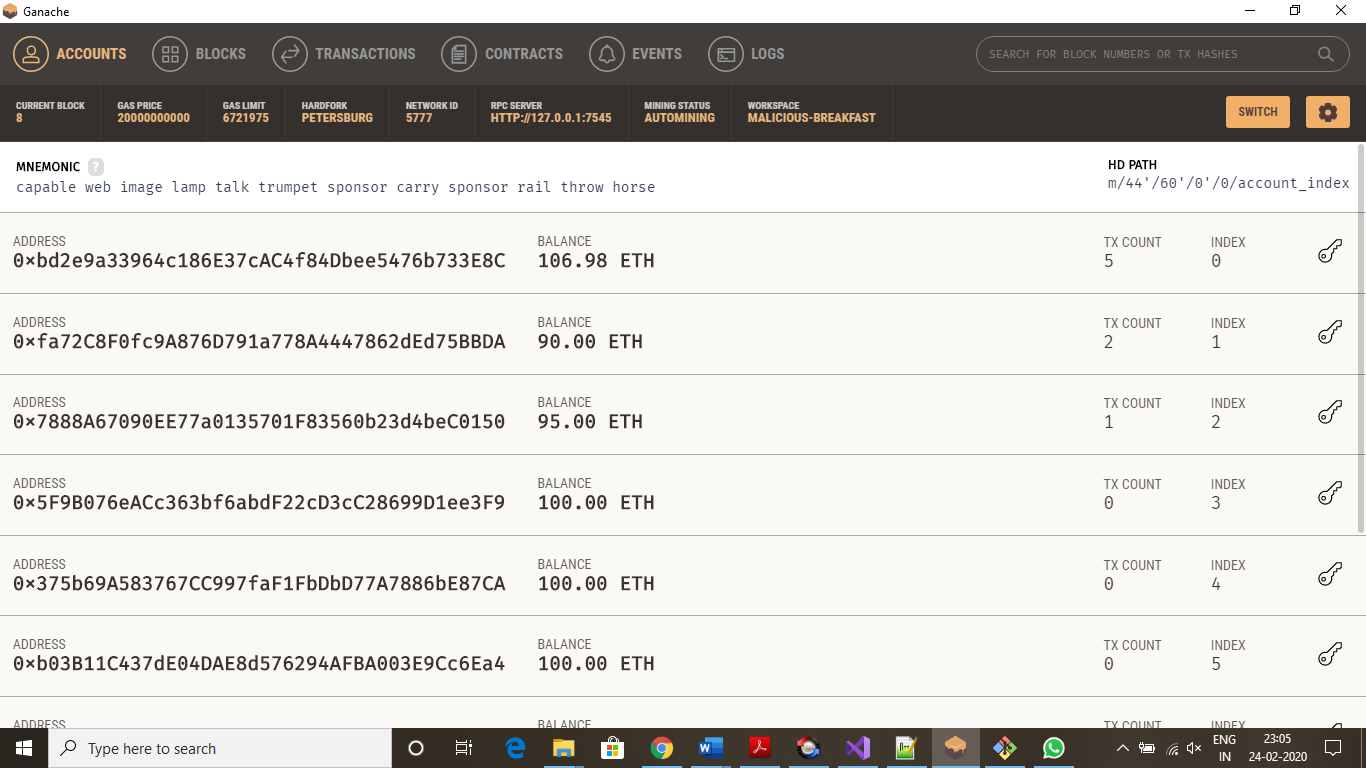
await instance.bid({from:accounts[2],value:web3.utils.toWei('5','ether')})



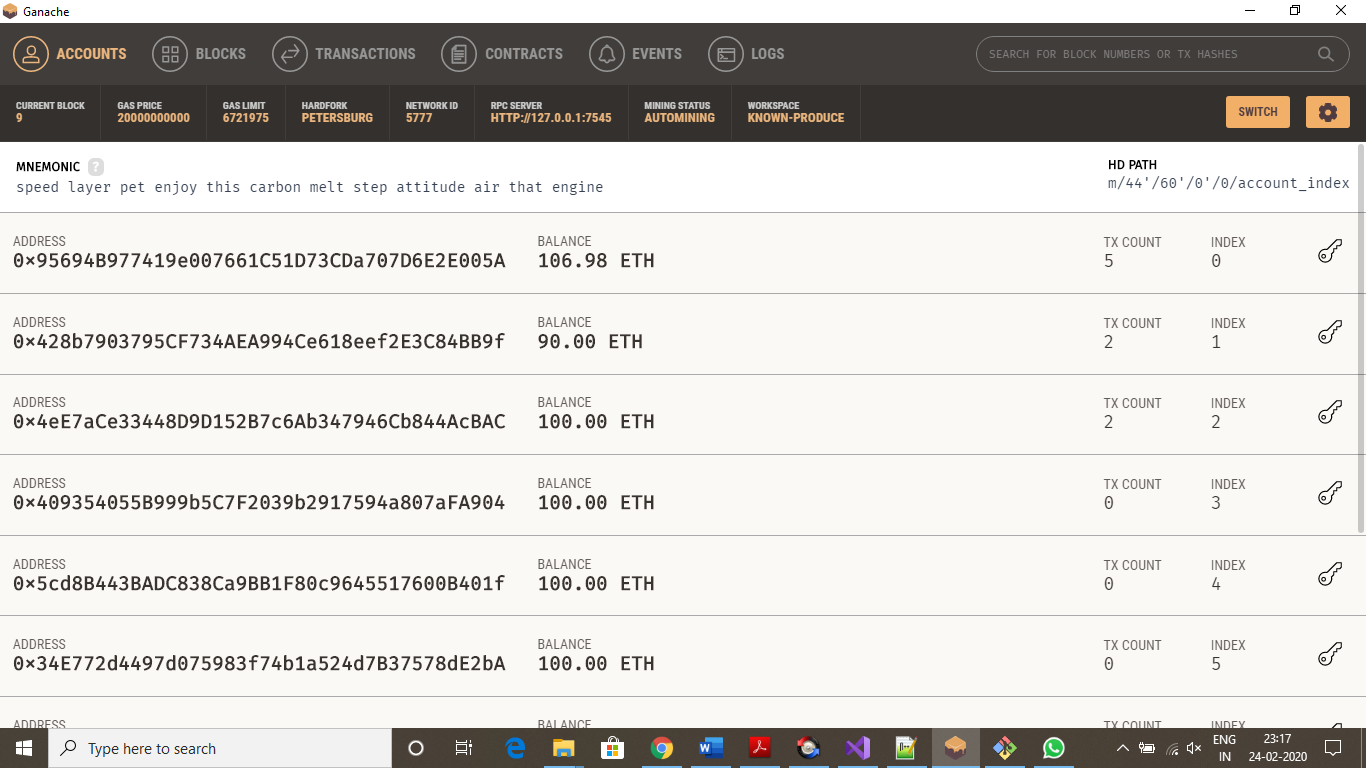
await instance.bid({from:accounts[1],value:web3.utils.toWei('7','ether')})



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



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



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

