DECENT AUCTION: A SECURE AND VERIFIABLE AUCTION SYSTEM ON THE BLOCKCHAIN

CS-316 PROJECT REPORT

Harsh Karamchandani
Department of Computer Science
Ashoka University

Prakhar Jain
Department of Computer Science
Ashoka University

May 6, 2019

***K*eywords** Vickrey Auction · Blockchain · Hyperledger Composer

1 Introduction

In today's world, when everyone is generating millions of bits of data each day, it has become more important than ever to preserve the privacy of such data. It is when identity is connected to money that privacy becomes even more important. The traditional auction systems have been in use since the past many centuries. Till date, many high valued commodities such as oil and art pieces are sold using an auction system. With such high valued transactions taking place, it is important that these systems are **verifiable**, **reliable** and **secure** in nature.

Traditional auctions are plagued by three main issues:

- Once the item is sold, no one knows who won or what they bid. There is no way to check if the auction was fair.
- Sellers have to rely on third parties to facilitate the auction. This leads to unnecessary charges for the sellers and third party involvement in the auction. Since they auction houses know all the bids, they can manipulate them in ways to get highest profits. We use a Vickrey auction system to ensure sealed bids, which cannot be manipulated.
- The auction systems essentially reveal information that should not be public knowledge, no one should know what others have bid, as people can game the system or reveal how much money one is willing to spend. Both these ideas take away privacy of the bidder and discourages people from bidding.

2 Why Vickrey Auction?

Vickrey auction is different from traditional English auctions in the sense that people bid whatever they are ready to pay in an English auction. While in Vickrey auction, since people have to pay lesser than they bid themselves, they bid a higher amount. People bid more than they are ready to pay because they never have to pay how much they have bid. This auction system is better for the person putting the item for bidding since they can get extra money since everyone is bidding more than they would've in a regular auction.

3 Why Blockchain?

Blockchain offers a good solution to Vickrey based sealed-bid auction by ensuring reliability and offering verifiability. One can verify their bid while also seeing who all have bid on the item. Everyone knows who all are bidding but not how much they have bid. No one and not even the system knows what everyone has bid before the bidding period closes. Since no one knows the bid anyone has placed, it guarantees complete anonymity.

4 Project Description

We developed a Vickrey Sealed Bid Auction based on Blockchain using Hyperledger Composer. Composer provides a high level API to interact with Hyperledger Fabric which eases the process of creating blockchain business networks. Composer also provides a REST API which is compatible with any backend framework. We used PHP to create a webapp which interacting with this REST API. For our Front-end we used Bootstrap.

5 Design Specification

5.1 Members

The system consists of the various Members, which are the users of the network. Since this is a decentralized system, there is no central authority to conduct the bidding. Users can register with an email and password on our system. Our system currently uses a single Peer to faciltate user registration and transactions.

5.2 Blockchain Network

Now, let us take a look at individual elements of our blockchain application:

5.2.1 Model

The business network is defined using the Hyperledger Modelling Language and stored in a CTO file. It is used to define the various elements of the business network. Our CTO file defines the Members, Items, Item Listings and Transactions of the network.

5.2.2 Chaincode

The business logic is implemented in the form of chaincode written in Javascript. Each functionality or transaction is defined as an asynchronous function in the chaincode file.

5.2.3 Ledger

Each transaction after completion is added to the blockchain ledger which is shared with all members of the business network to ensure transparency. This ledger is also immutable so no transactions are alterable or reversible.

5.3 Frontend

We used HTML, CSS and Bootstrap for the front end of our website. The forms are all written in HTML while we used CSS for styling and Bootstrap framework is used for making tables and other style structures.

5.4 Backend

We used PHP for backend, all the data captured from the front end is passed to the backend PHP which makes transactions possible by interacting with the Composer API which interacts with the Chaincode.

6 Workflow

6.1 Tools used

We chose Hyperledger Composer to implement our project. Hyperledger Composer is a set of abstractions, tools and APIs to model, build, integrate and deploy a blockchain solution. It uses a command line interface to deploy the network on Hyperledger Fabric and creates a REST API that can be used to create a user-facing application. This application we made using a PHP backend and HTML frontend.

6.2 Chaincode Functions

The entire system depends on the functions that are executed by the chaincode. These functions make all the additions to the ledger. This code is written in JavaScript and has the following functions:

6.2.1 Offer

This function requests for the item for which the bid is to be placed along with the bidding amount, it also inquires for who is placing the bid. It then checks if the bid is more than the reserve price and within the bidding period. If so, the transaction is recorded in the ledger. This contains the data requested by the function along with a timestamp and a transaction ID. This function call can be made by anyone willing to bid on the item that has been placed for auction.

6.2.2 Close Bidding

This function call is made by the member who put up the item for auction. This function can be called before the auction period has ended to put an early end to auction, while it has to be called later so the bidders can be informed that they can now send their encrypted keys for determining the winner. This function essentially removes an item for listing since there can be no bidding on it anymore.

6.2.3 Reveal Bid

This function can be called by the bidders after the bidding has closed. It requests the user for their key. The function then encrypts it using the chaincode's public key and pushes it into the blockchain. The blockchain now essentially has everyone's bids in encrypted form and the keys for encryption in an encrypted form.

6.2.4 End Auction

This function ends the auction and returns the money from the 2nd highest through the lowest bidder. It then subtracts the second highest bid from the highest bid and send it to the highest bidder while sending the second highest bid to the member who put the item up for auction. The item can then be transferred to the highest bidder.

6.2.5 Add Money

This function is presently present with all the users to add balance for themselves. This function can be linked to an API call with an external source, such that every user can buy more currency for use on the network. Alternately, this facility can be given to just the network administrator who can add money to any account they want at any time when paid through external sources.

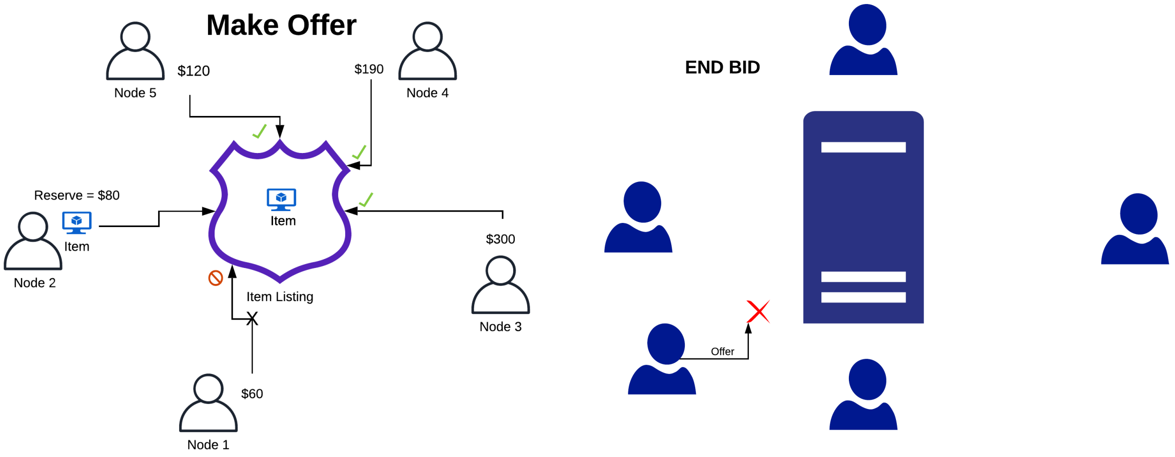


Figure 1: Taking Offers and Rejecting after Bid Ends

7 Implementation Details

7.1 Tools Used

Hyperledger Composer is used to generate a REST API to communicate with the blockchain chaincode and ledger. PHP's cURL library is used to interact with the REST API by making GET, POST and PUT calls to the API to submit and retrieve data, execute transactions and make changes. CryptoJS library is used to perform AES encryption.

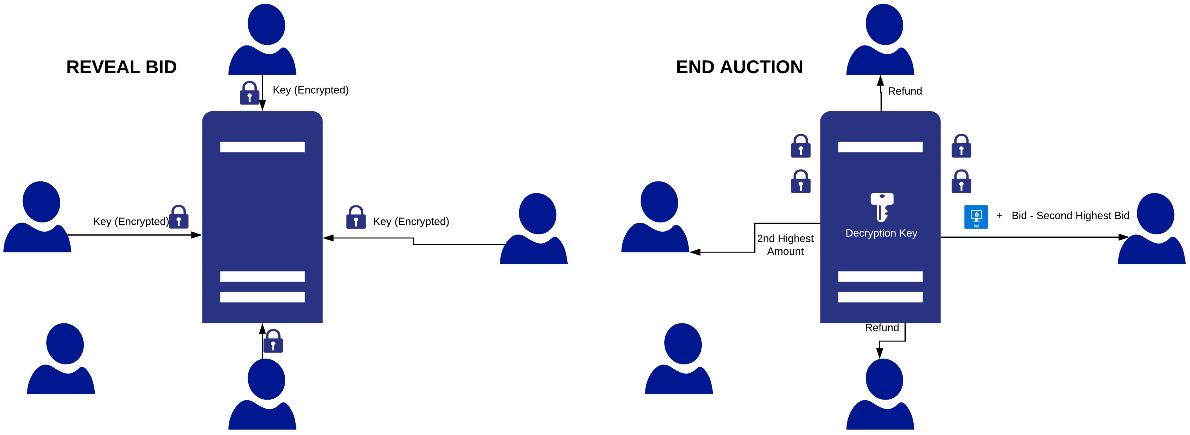
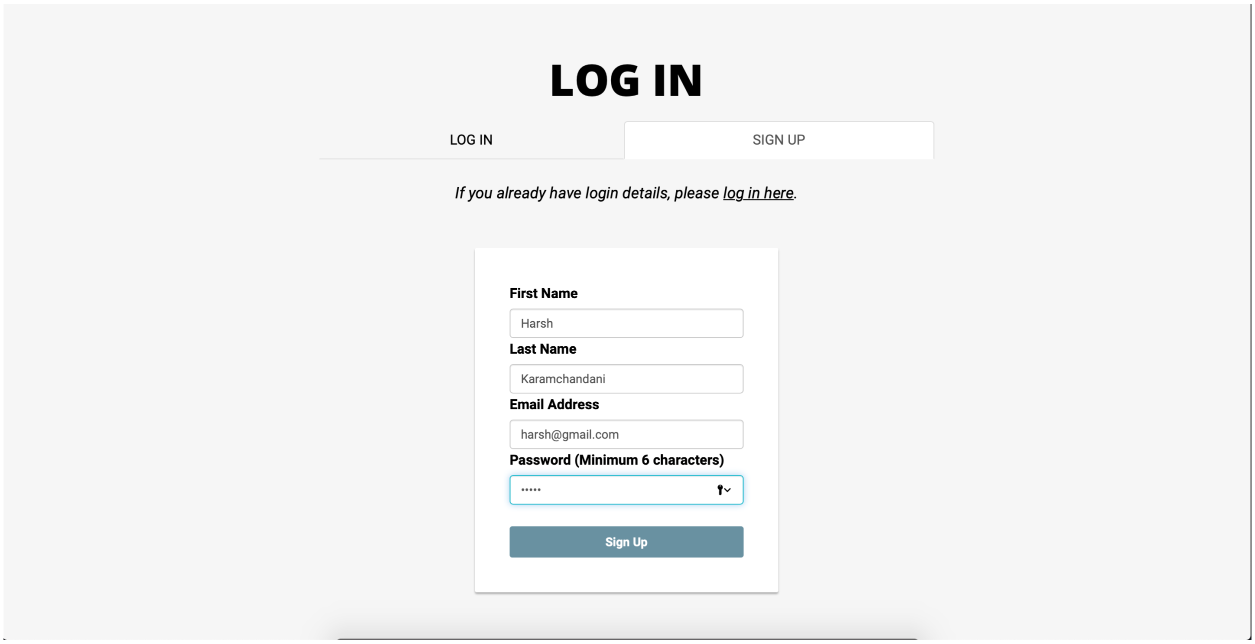


Figure 2: Revealing Encrypted Keys and Getting Money and/or Item



LOG IN

If you already have login details, please log in here.

First Name

Harsh

Last Name

Karamchandani

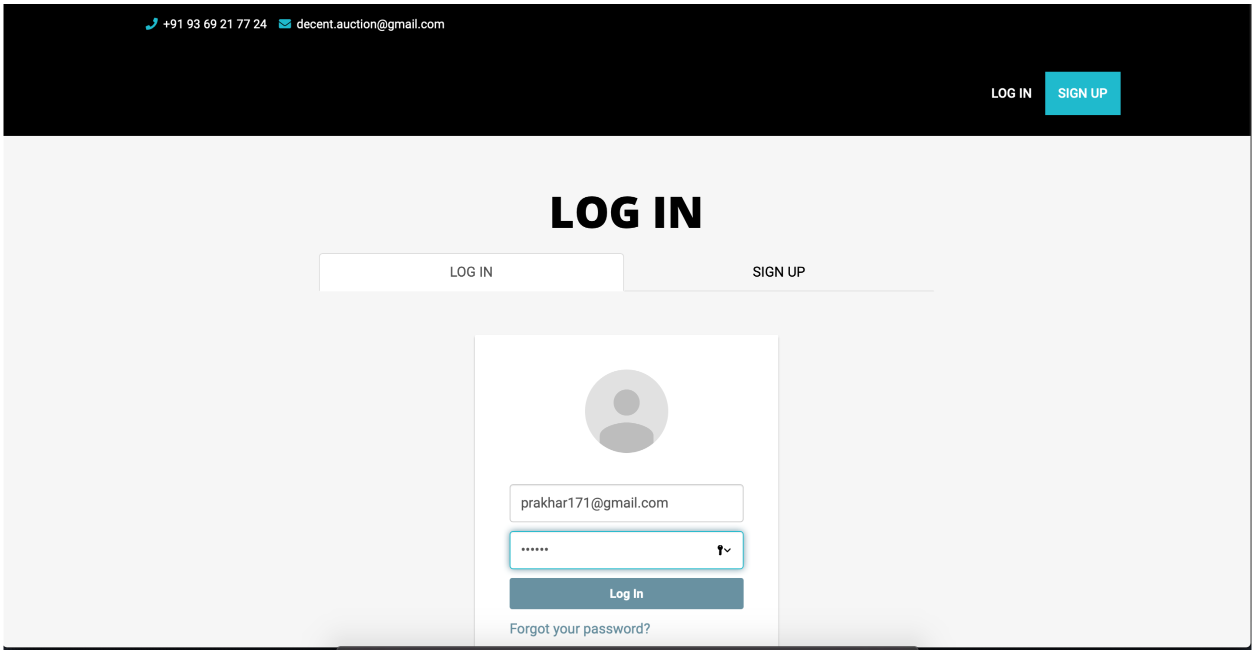
Email Address

harsh@gmail.com

Password (Minimum 6 characters)

•••••

Figure 3: User Signs Up with email address and password

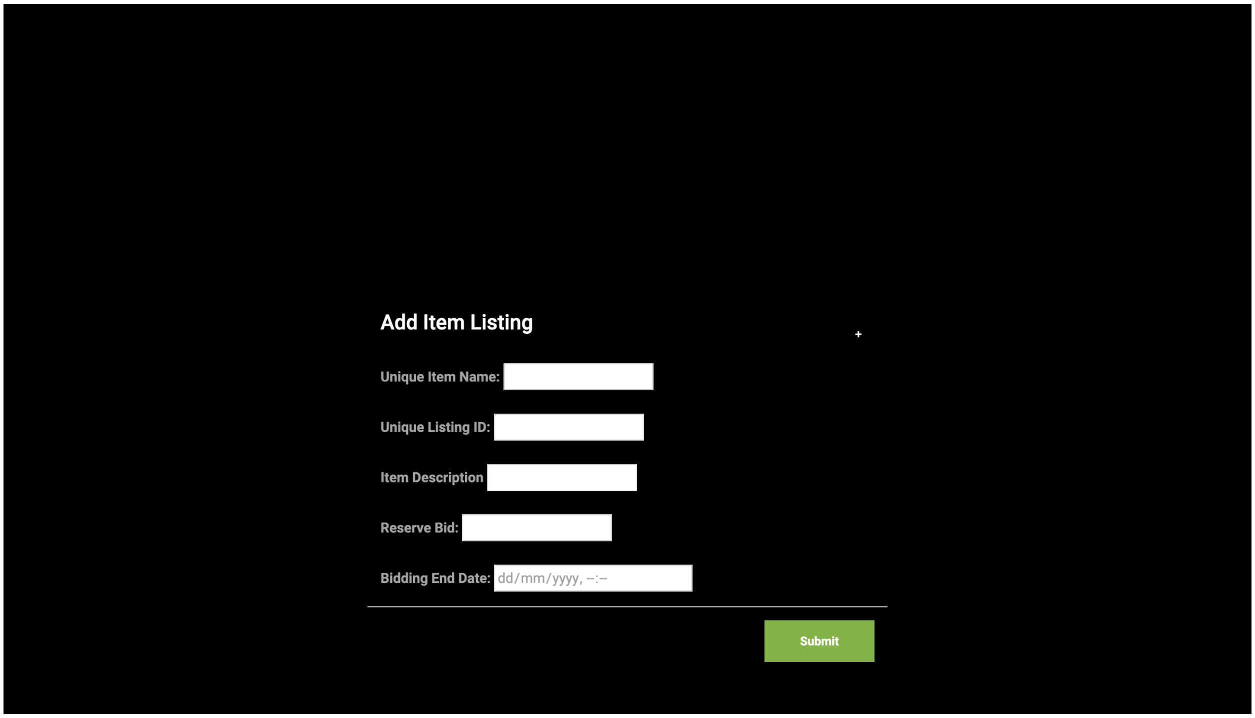


LOG IN

prakhar171@gmail.com

••••••

Figure 4: User Logs In using credentials



Add Item Listing

Unique Item Name:

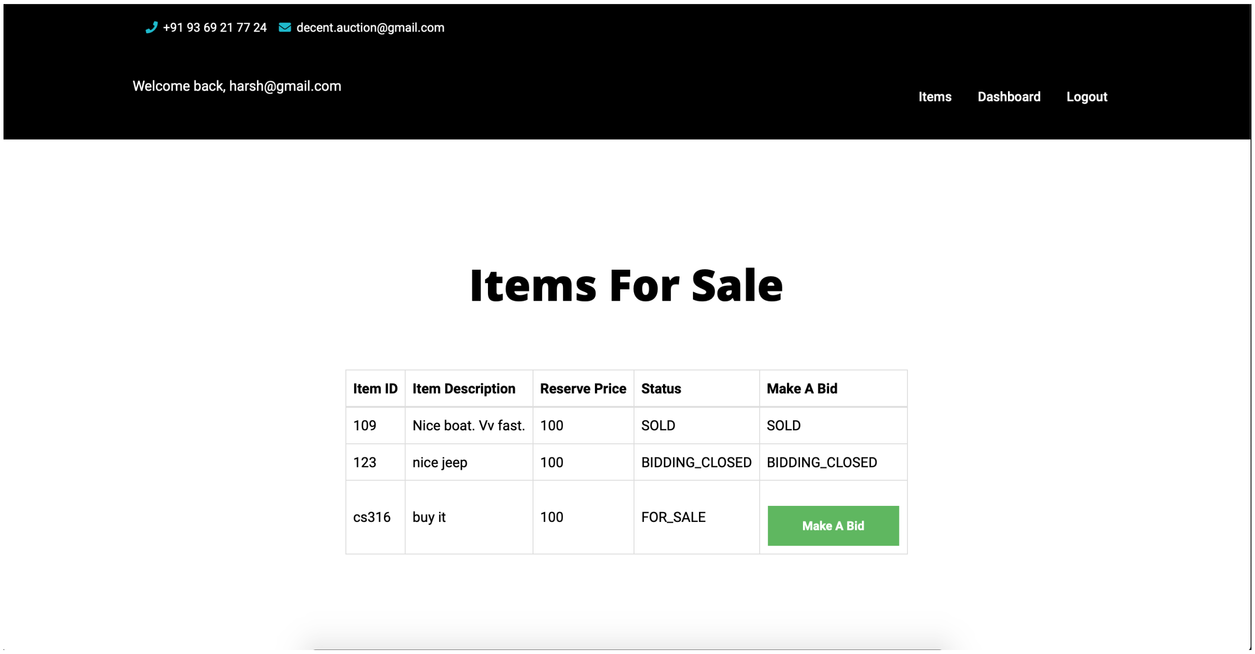
Unique Listing ID:

Item Description

Reserve Bid:

Bidding End Date: dd/mm/yyyy, --:--

Figure 5: User goes to Dashboard and Lists and Item for Bidding

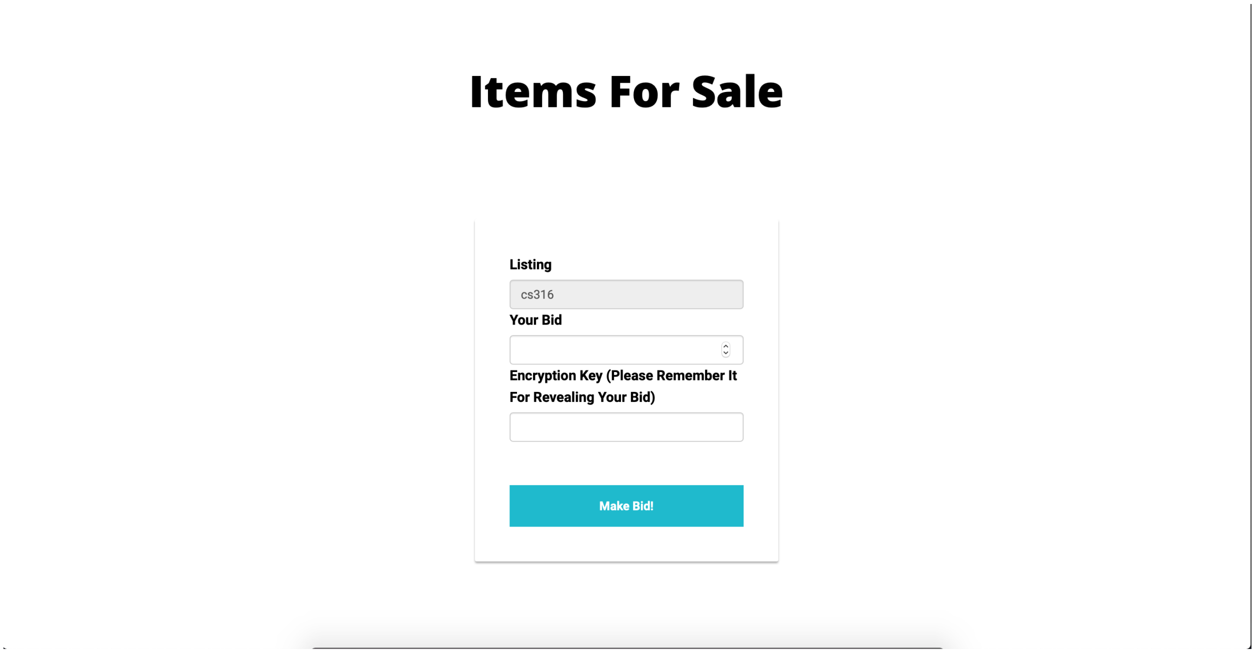


Welcome back, harsh@gmail.com

Items For Sale

Item ID	Item Description	Reserve Price	Status	Make A Bid
109	Nice boat. Vv fast.	100	SOLD	SOLD
123	nice jeep	100	BIDDING_CLOSED	BIDDING_CLOSED
cs316	buy it	100	FOR_SALE	Make A Bid

Figure 6: Item gets listed for sale.



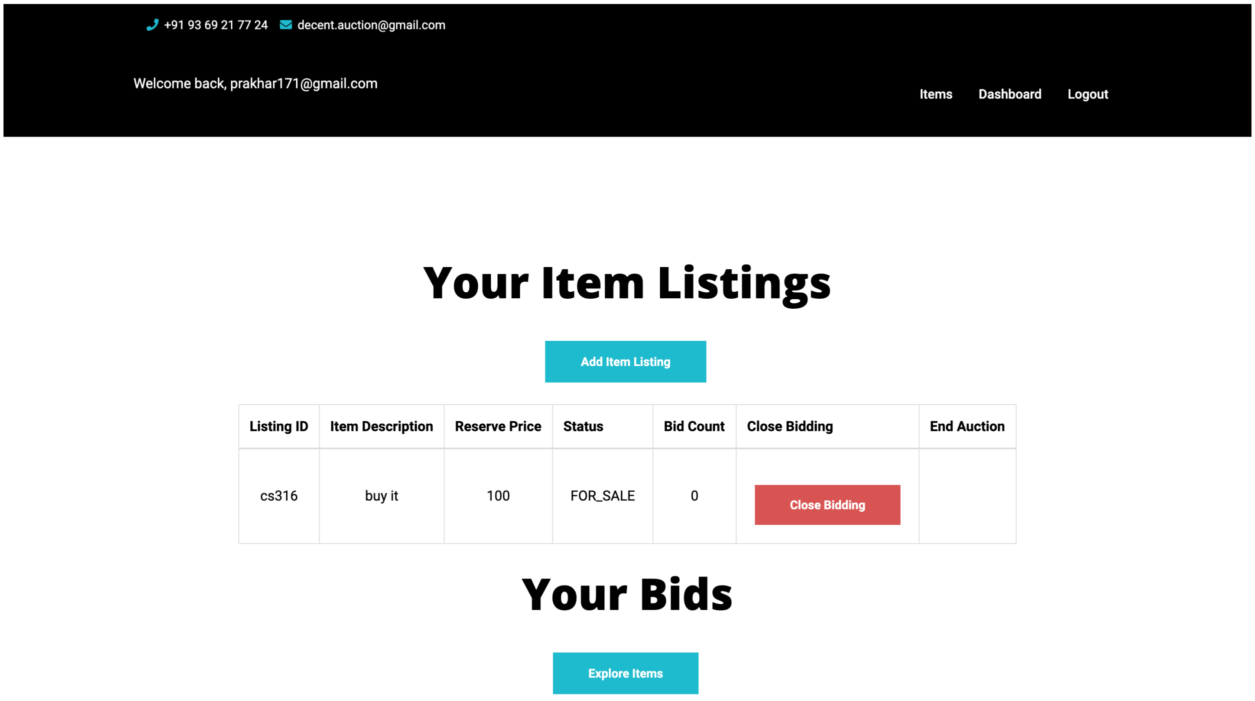
Items For Sale

Listing: cs316

Your Bid:

Encryption Key (Please Remember It For Revealing Your Bid):

Figure 7: Other users make bids on the item



+91 93 69 21 77 24 decent.auction@gmail.com

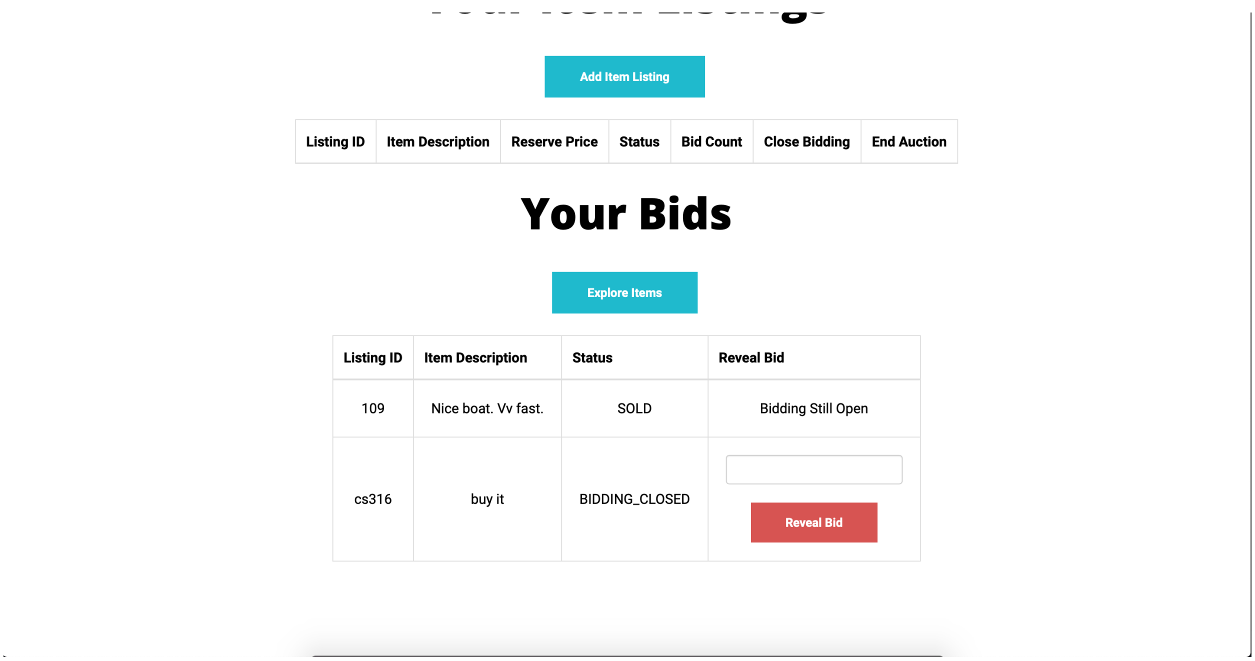
Welcome back, prakhar171@gmail.com

Your Item Listings

Listing ID	Item Description	Reserve Price	Status	Bid Count	Close Bidding	End Auction
cs316	buy it	100	FOR_SALE	0	Close Bidding	

Your Bids

Figure 8: User closes the Bidding for the Listing from Dashboard

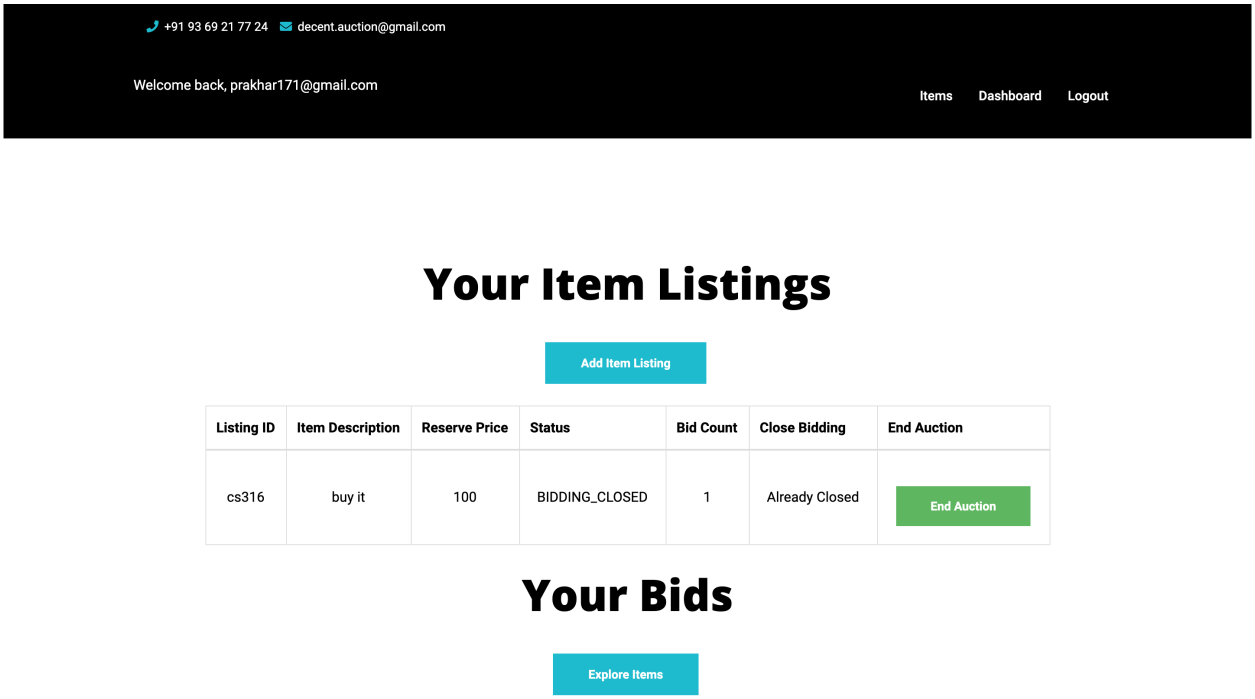


Listing ID	Item Description	Reserve Price	Status	Bid Count	Close Bidding	End Auction

Your Bids

Listing ID	Item Description	Status	Reveal Bid
109	Nice boat. Vv fast.	SOLD	Bidding Still Open
cs316	buy it	BIDDING_CLOSED	Reveal Bid

Figure 9: Other users get prompted on their dashboard to reveal their bids



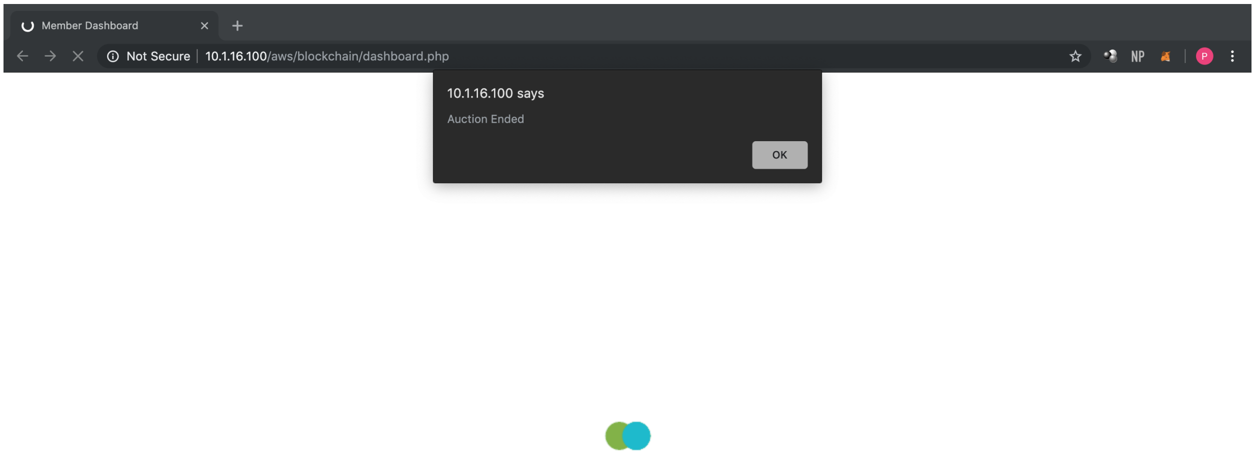
Welcome back, prakhar171@gmail.com

Your Item Listings

Listing ID	Item Description	Reserve Price	Status	Bid Count	Close Bidding	End Auction
cs316	buy it	100	BIDDING_CLOSED	1	Already Closed	End Auction

Your Bids

Figure 10: Once the users have revealed their bids, user can end the auction.



10.1.16.100 says

Auction Ended

Figure 11: Auction Ends. Item is marked as SOLD.