Auction-Bay

Auction Bay is a blockchain based shopping portal. It provides several secured methods to sell, auction and buy products. It hosts a dark-minimal interface, developed using React JS.

Team Name: BlockDaggers

Instructions

To run this project:

- Start Truffle Environment:

  ```
  truffle develop
  ```

- Within Truffle Environment, run the following the commands:

  ```
  compile
  migrate
  ```

- In a different terminal:

  ```
  cd client
  npm install
  npm run start
  ```

Dependencies

- React JS
- Ant Design
- web3.js
- eth-crypto
- keccak256
- truffle

Programming Logic

Silent Auction - Keeping Bids Secret

We are taking special care to prevent leakage of bid amounts before bidding period is over.

- **Why** : Because, if a person knows the bid value he can be sure to win / influence the result of auction.

- For the first price auction, he can become the winner. Suppose he is willing to go till 300Wei but he finds out max bid is 200, he will bid 201 and get away with it.
- For the second price auction he can make the winner overpay. Suppose he knows highest and 2nd highest bids are 300 and 200. So winner is to pay 200. But he can bid 299, and make the winner pay.
- In the second price, he can also become the winner.
- In the average price, he can get the average and be sure to win the bid.
- **How** : Our main aim is to keep the bidding values as long as people are bidding, or bidding round is active.
- **Bidding** :
- In the bidding round, bidders will not send the bid value. They will perform off chain hashing keccak256(password+bid_value+account_public_key).
- We use password so that someone cannot loop over bid_value and find out because account_public_key is already public.
- We share this hash value as our bid in the bidding round.
- **Verification** : Verification round runs once Bidding round is closed. In this round bidding is no more happening and not allowed.
- For verification, bidder gives his encryption keys (generated via EthCrypto), to encrypt the delivery string if he wins.
- He also gives password and pays the bid value to the escrow account. The escrow account accepts the bid if and only if the hash matches with keccak256(password+msg.value+msg.sender).
- In this way, bid amount is only revealed once the bidding period is over.
- Since bidding is revealed to the seller also after the bidding round, this prevents biased closing of round in case of avg. price auction / second price auction etc.

Auctions

Implementation Of Escrow for Trustlesness

The bidders transfer their bids to escrow, and the seller gets the payment only when he delivers the string. In this way, the contract implements escrow payment to ensure trustless delivery.

First Price Auction

Introduction

- Winner is the bidder whose bid is the highest.
- Payable amount is the amount bid by the highest bidder. Paid by the winner.

Security

- Since the bids are not revealed till the auction is over, we can be sure that the first price auction will be secure.

Second Price Auction

Introduction

- Winner is the bidder whose bid is the highest.
- Payable amount is the amount bid by the second highest bidder. Paid by the winner.

Security

- Since the bids are not revealed till the auction is over, we can be sure that the first price auction will be secure.

Average Price Auction

Introduction

- Winner is the bidder whose bid is the highest.
- Payable amount is the average amount bid (bid & verified) by the bidders. Paid by the winner.

Security

- Since the bids are not revealed till the auction is over, we can be sure that the first price auction will be secure.
- They can move the average to their desired value (say 1000Wei) by doing a sybil attack via multiple accounts to move the avg. closer by bidding 1000Wei. However, this requires multi-fold stake (suppose for 1000 participants with 1 adversary, it requires around 1000 or more times the value). This stake disincentivizes the attack because duration of holding a money is more valuable than amount of money save (which is 1000th of what we staked).

Direct Purchase

Introduction

- Person who buys at the decided fixed price first gets the product.

Security

- Same as that in assignment 1. No additional security needed.

Delivery

- For delivery, we are encrypting the delivery string (NETFLIX access token) with `EthCrypto public key` of the `winner bidder`.
- The bidders will provide their public keys while giving proofs / verification for their bids. The seller chooses the winner's public key to encrypt the string and make it public on blockchain.
- But since the key is encrypted, the actual token is accessible only by the winner bidder because he has the private key.