(OPEN ASCENDING) AUCTIONS IN BYZCOIN

By HARENA M. Diana
Supervisor: Jeff Allen
1 - PROJECT OVERVIEW

Auctions in Byzcoin
## 2 - MY APPROACH

### spawn
- Good description
- Seller coin IID

### invoke:bid

### invoke:close
- Salt
- Reserve price

### auction contract
- Spawn()
- Invoke() - bid
- Invoke() - close
- Invoke() - drop

### auction instance
- Good description
- Seller coin IID
- Highest bid
- Highest bidder coin IID
- Reserve price
- Winning proof
2 - MY APPROACH - contract behaviour

Auctions in Byzcoin
2 - MY APPROACH - contract behaviour

Auctions in Byzcoin
2 - MY APPROACH - transactions

**bid transaction**
- invoke:fetch \(\rightarrow\) CoinContract
- invoke:bid

**close/drop transaction**
- invoke:close/drop

**credit account transaction**
- invoke:store \(\rightarrow\) CoinContract
2 - MY APPROACH - client application

Dynasent application

Auction object 1

Auction object 2

Byzcoin service

Global State

Auction instance 1

Auction instance 2

Auctions in Byzcoin
2 - MY APPROACH - evaluation: how many concurrent bids?

Simulation settings:
- duration 20s, blockinterval of 1s
- 7 cothorities on 7 servers in Deterlab
- experiments: 1 auction, N increasing bids
- result: max 180 bids

![Graph showing user time and wall time per number of bids]
3 - DEMONSTRATION

Auctions in Byzcoin

- Seller
- Auction system
- Buyer

- Post product
- Bid on product
- View the auction updates
- View the bids status
THANK YOU
User time and wall time per number of bids

- **user_time**
- **wall_time**

### Bids
- 10
- 50
- 100
- 150
- 180

### Wall Time
- 0
- 2
- 8
- 10
- 12

### User Time
- 0
- 2
- 4