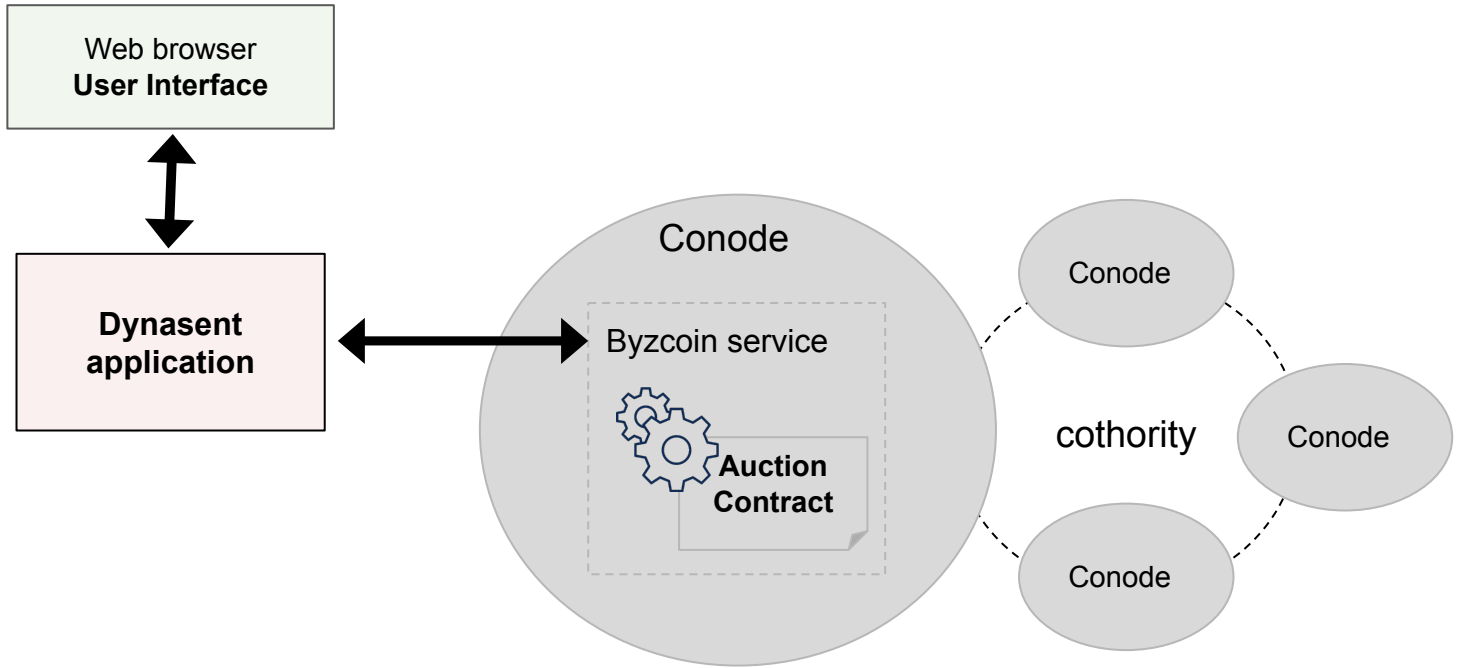
(OPEN ASCENDING) AUCTIONS IN BYZCOIN

By HARENA M. Diana
Supervisor: Jeff Allen

EPFL

1 - PROJECT OVERVIEW



2 - MY APPROACH

spawn
Good description
Seller coin IID

invoke:bid

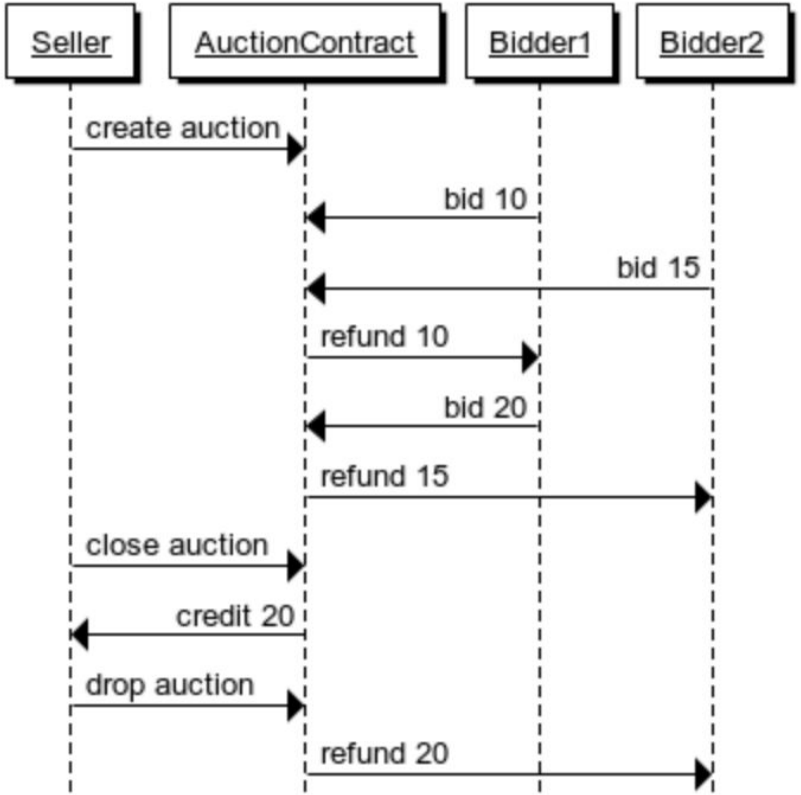
invoke:close
Salt
Reserve price

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

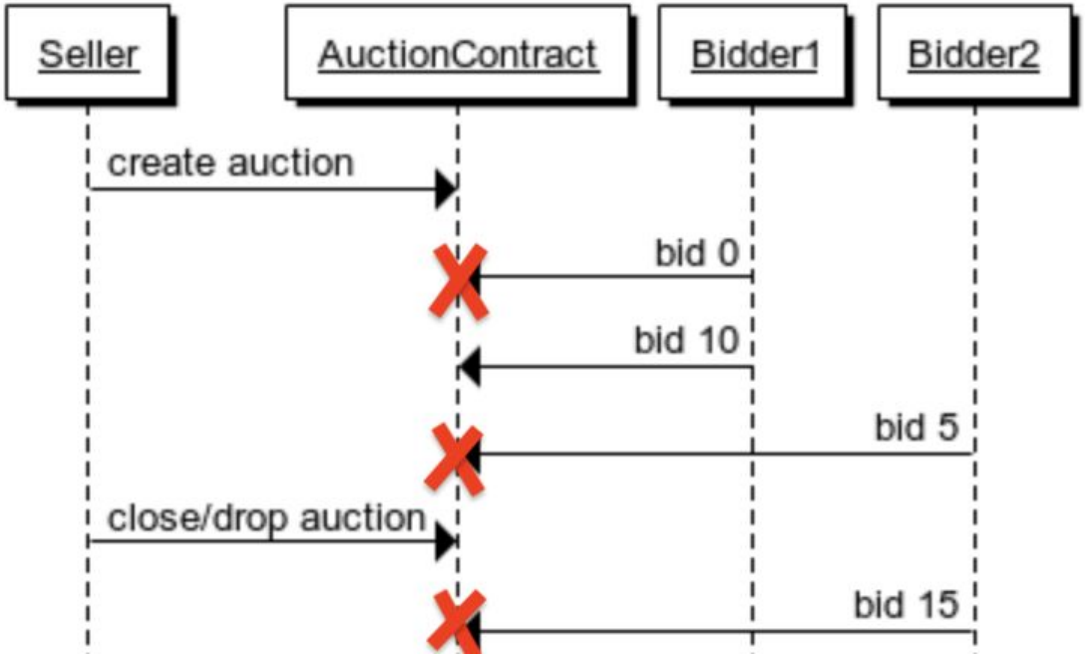
auction instance
Good description
Seller coin IID
Highest bid
Highest bidder coin IID
Reserve price
Winning proof

EPFL

2 - MY APPROACH - contract behaviour



2 - MY APPROACH - contract behaviour



2 - MY APPROACH - transactions

bid transaction
invoke:fetch → CoinContract
invoke:bid

+

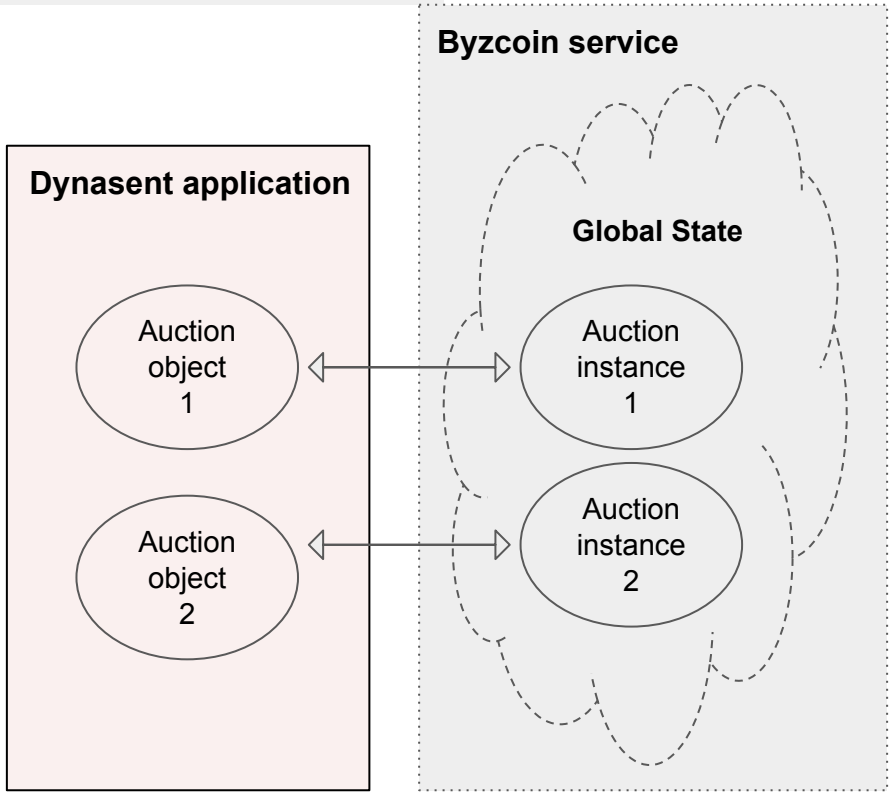
credit account transaction
invoke:store → CoinContract

close/drop transaction
invoke:close/drop

+

credit account transaction
invoke:store → CoinContract

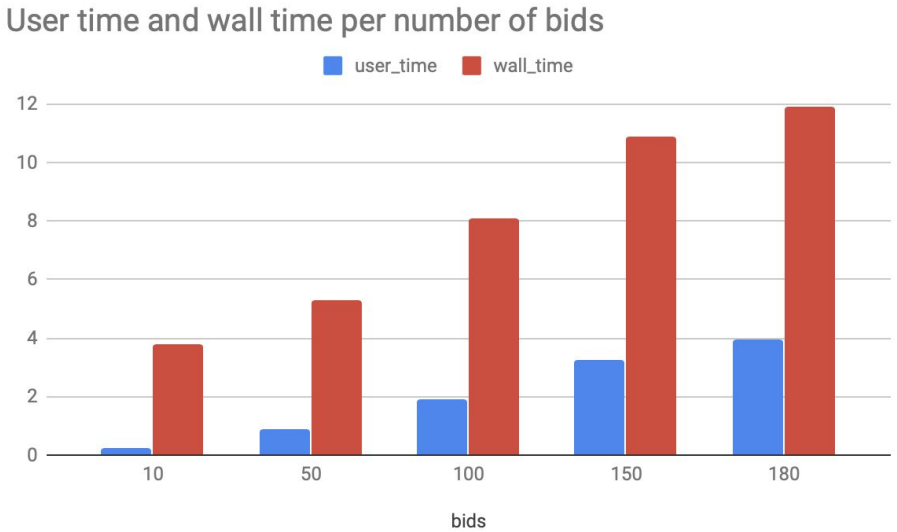
2 - MY APPROACH - client application



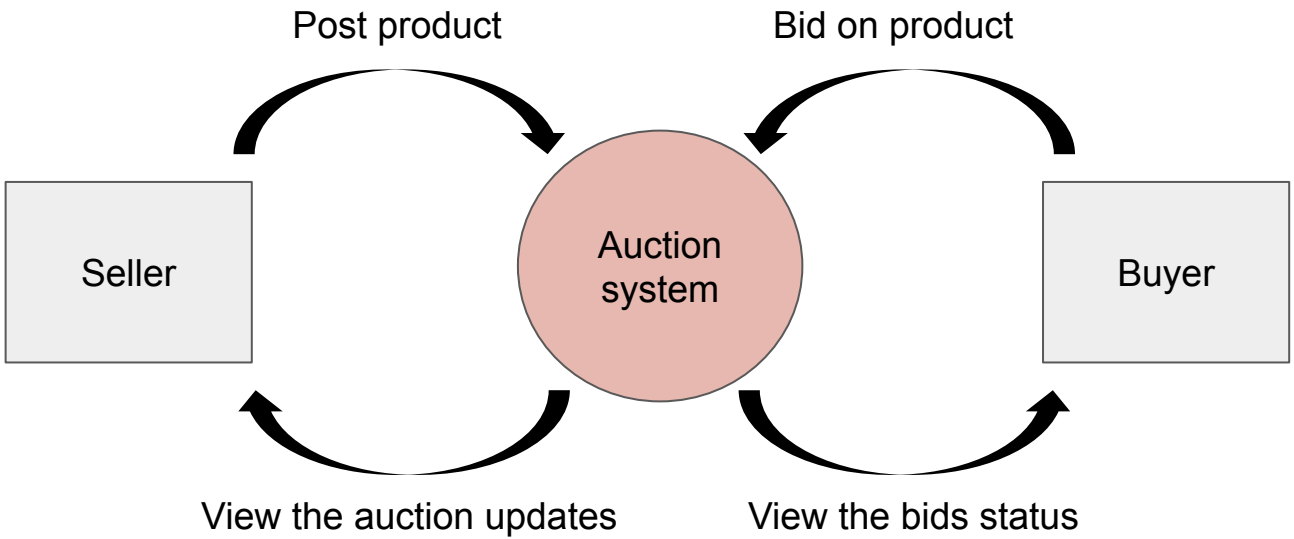
2 - MY APPROACH - evaluation: how many concurrent bids?

Simulation settings:

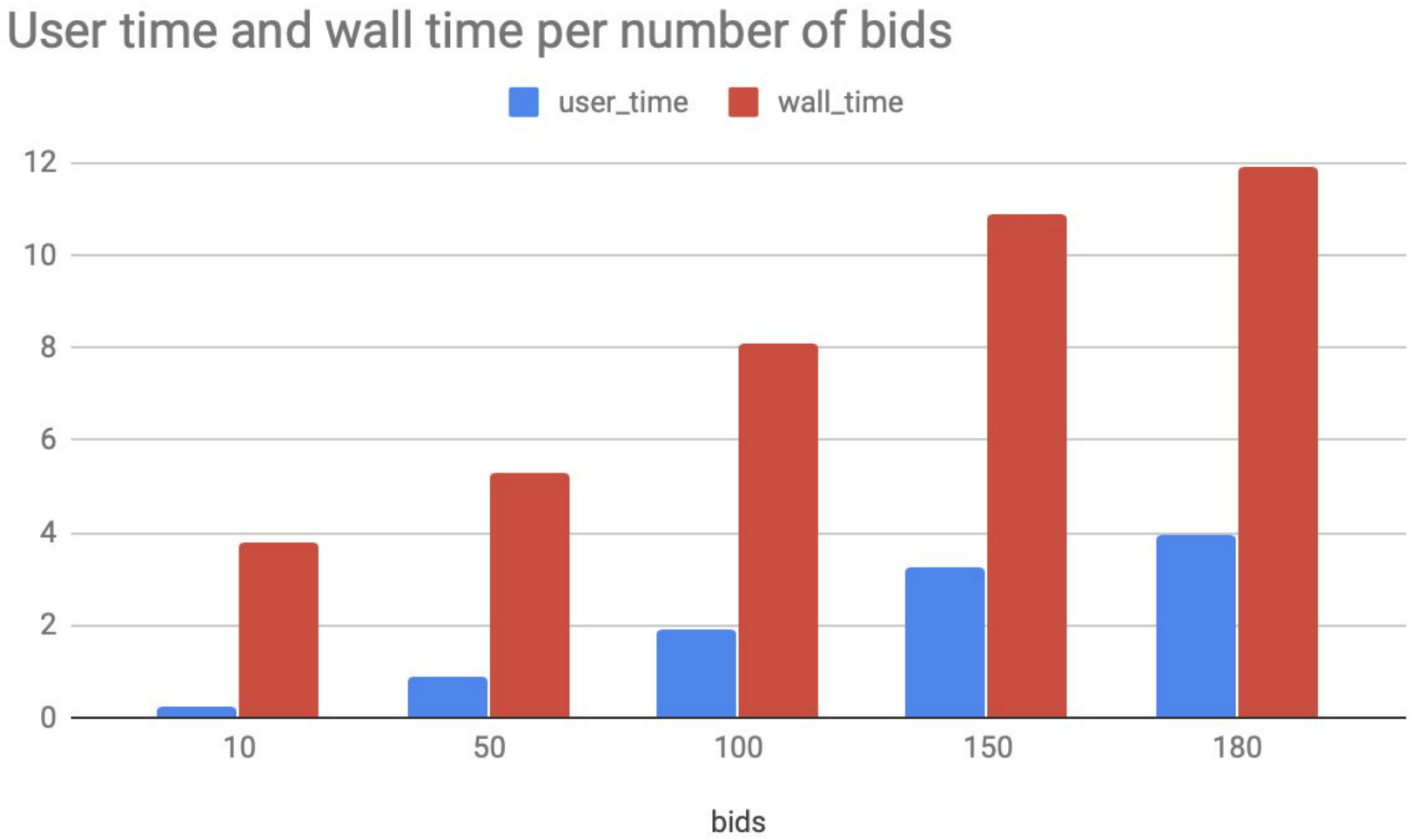
- duration 20s, blockinterval of 1s
- 7 cothorities on 7 servers in Deterlab
- experiments: 1 auction, N increasing bids
- result: max 180 bids



3 - DEMONSTRATION



THANK YOU


User time and wall time per number of bids
user_time
wall_time
12
10
8
6
4
2
0
10
50
100
150
180
bids