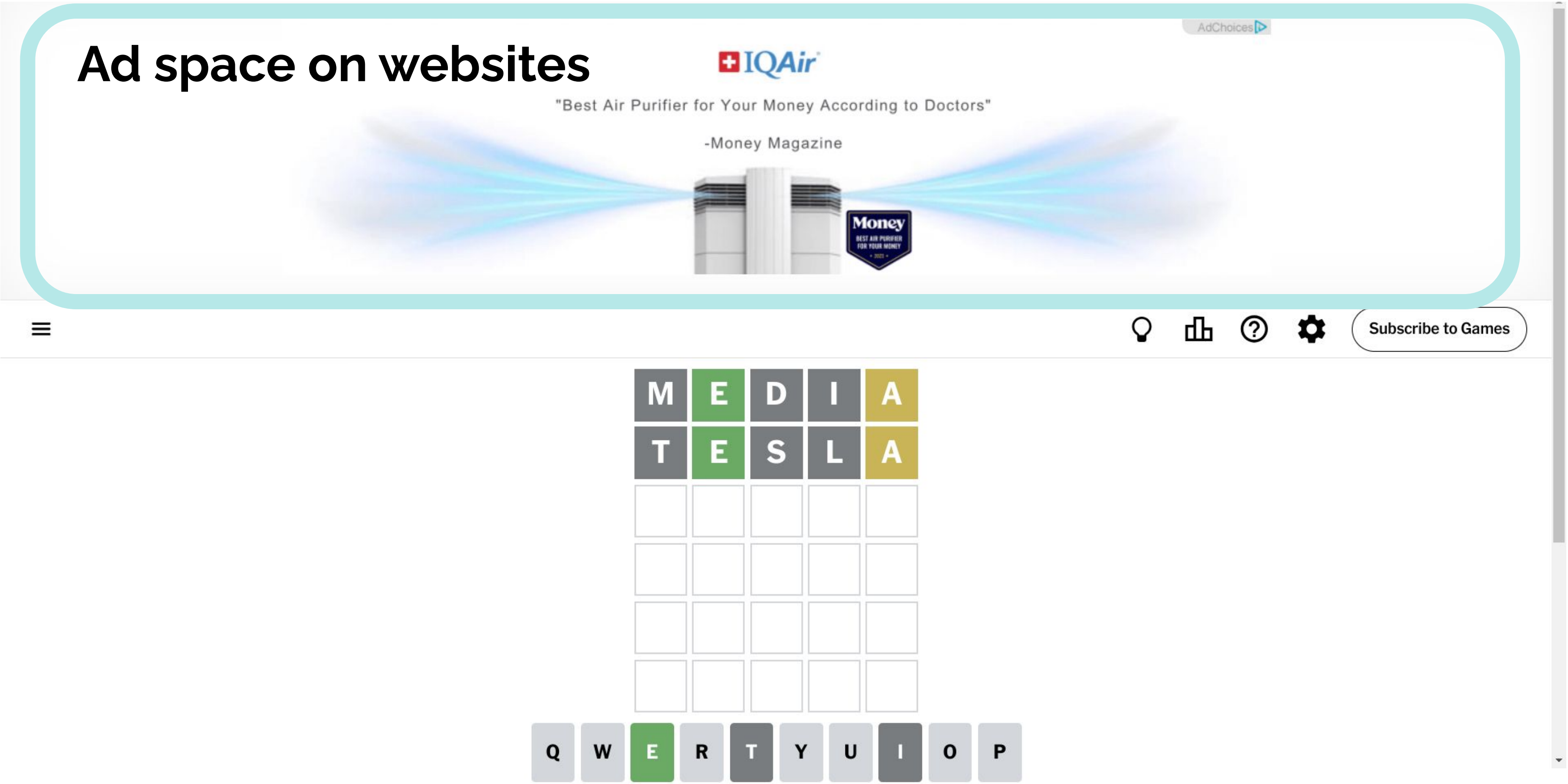
Foundations of **Platform-Assisted Auctions**

Elaine Shi

Carnegie Mellon University

Joint work with Hao Chung and Ke Wu

Ad space on websites

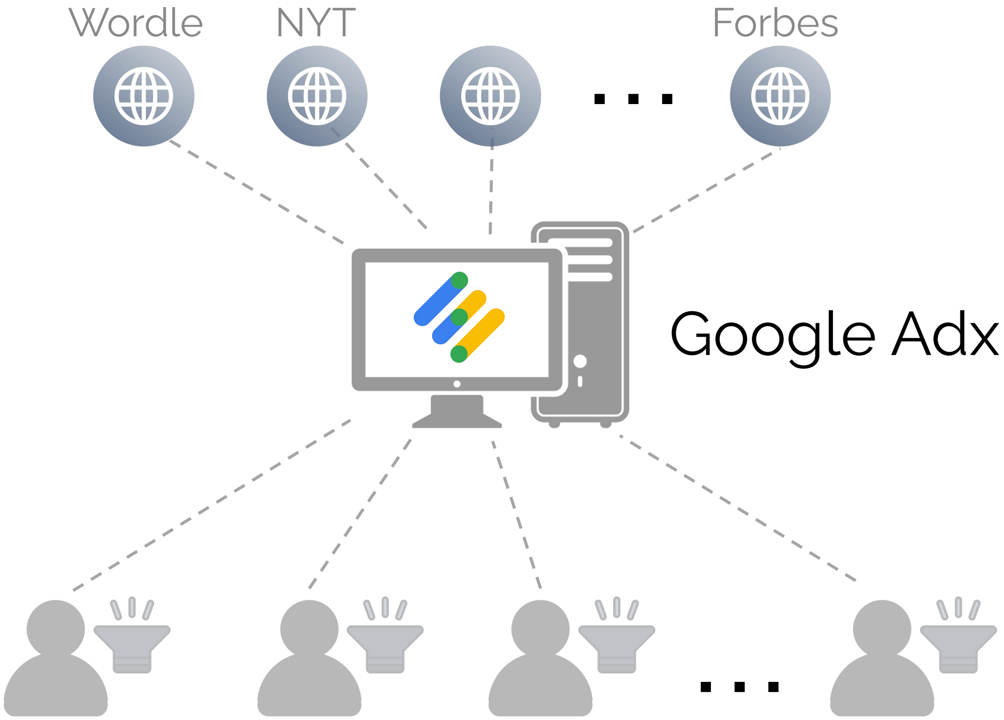


Platform-assisted auctions

Sellers (publishers)

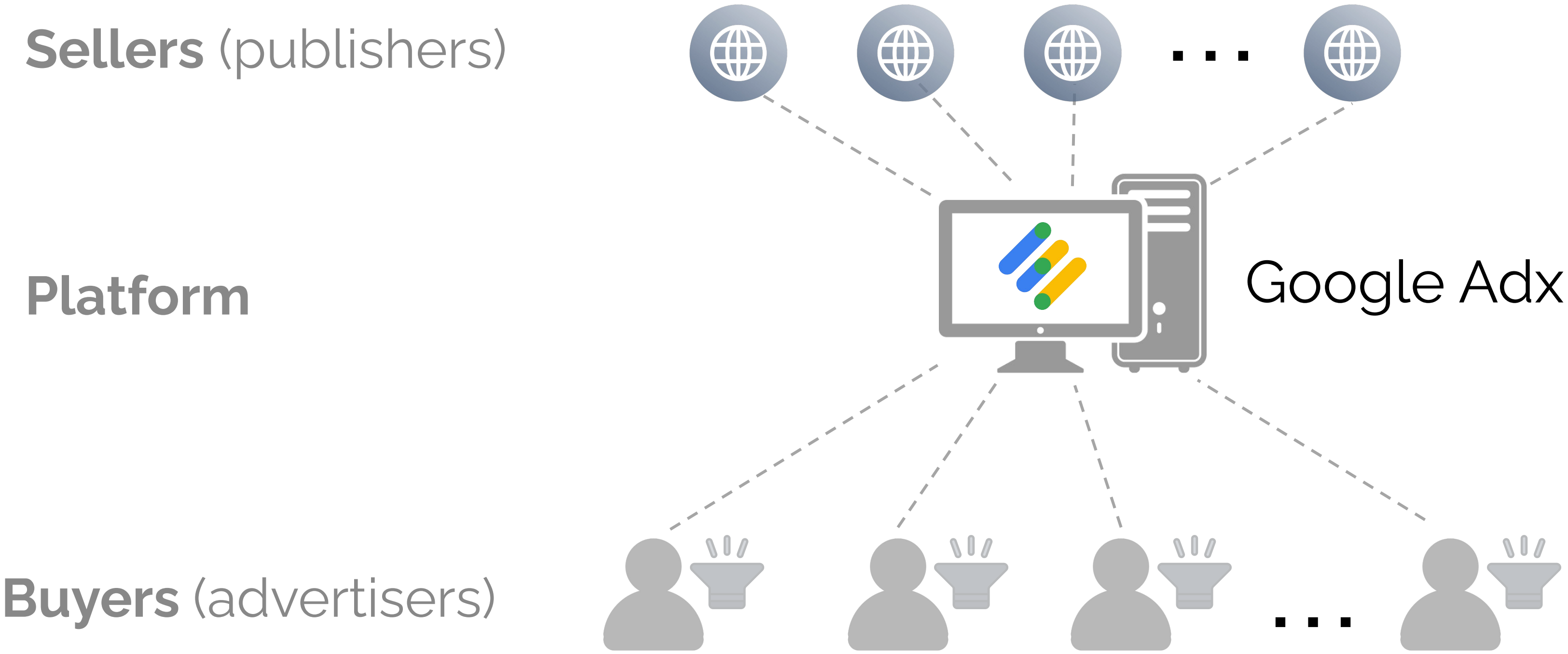
Platform

Buyers (advertisers)



Platform gets **remunerated** for **value-added services**:

rendezvous, search, recommender system, payment processing



PRESS RELEASE

Justice Department Sues Google for Monopolizing Digital Advertising Technologies

Google accused of

- **withholding** seller revenue
- **injecting bids** to raise price

  ……

https://www.justice.gov/archives/opa/press-release/file/1563746/dl

New theory of anti-trust auction design

New theory of anti-trust auction design

Auction literature

- Trusted auctioneer
- Assume no collusion
- Permissioned

New theory of anti-trust auction design

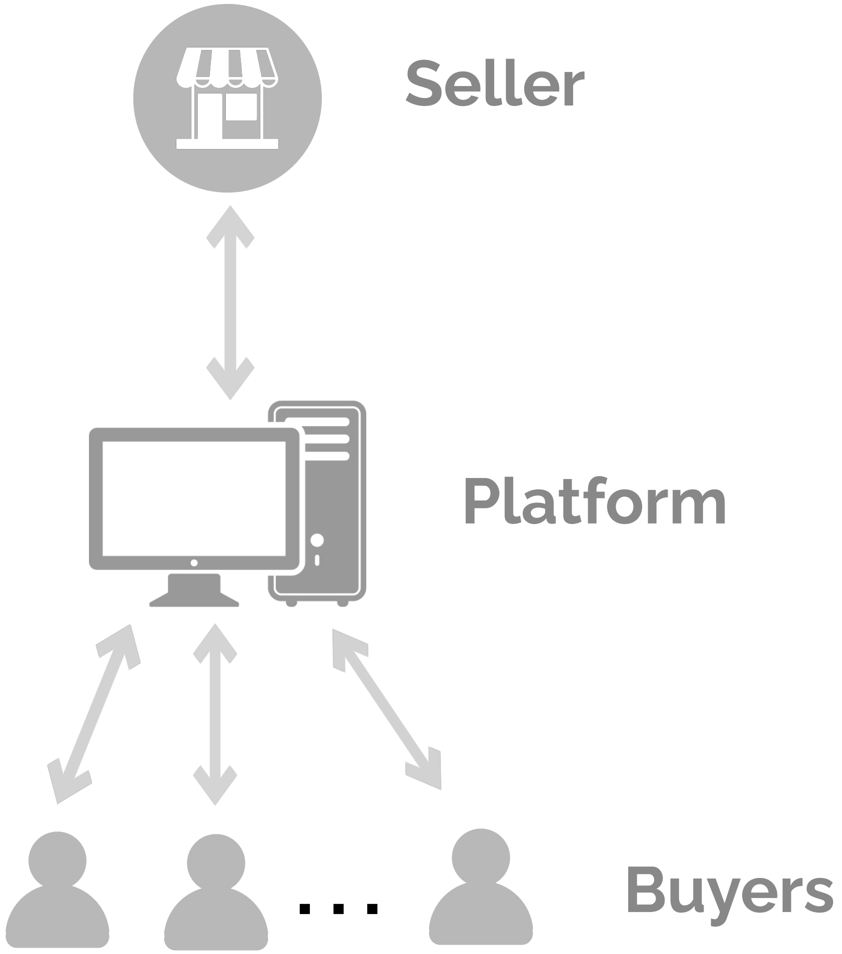
Auction literature

- Trusted auctioneer
- Assume no collusion
- Permissioned

Reality

- Trustless environment
- Collusion made easy
- Permissionless

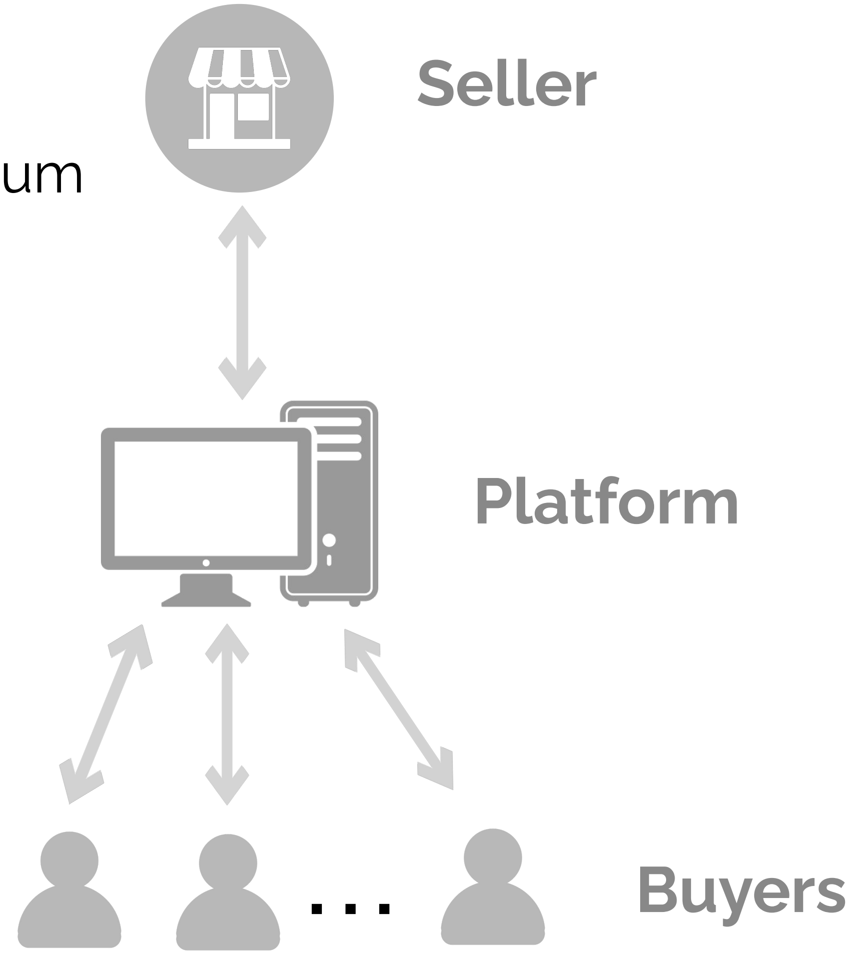
What is a **dream** platform-assisted auction?



Incentive compatible (IC)

Honest is best response/equilibrium

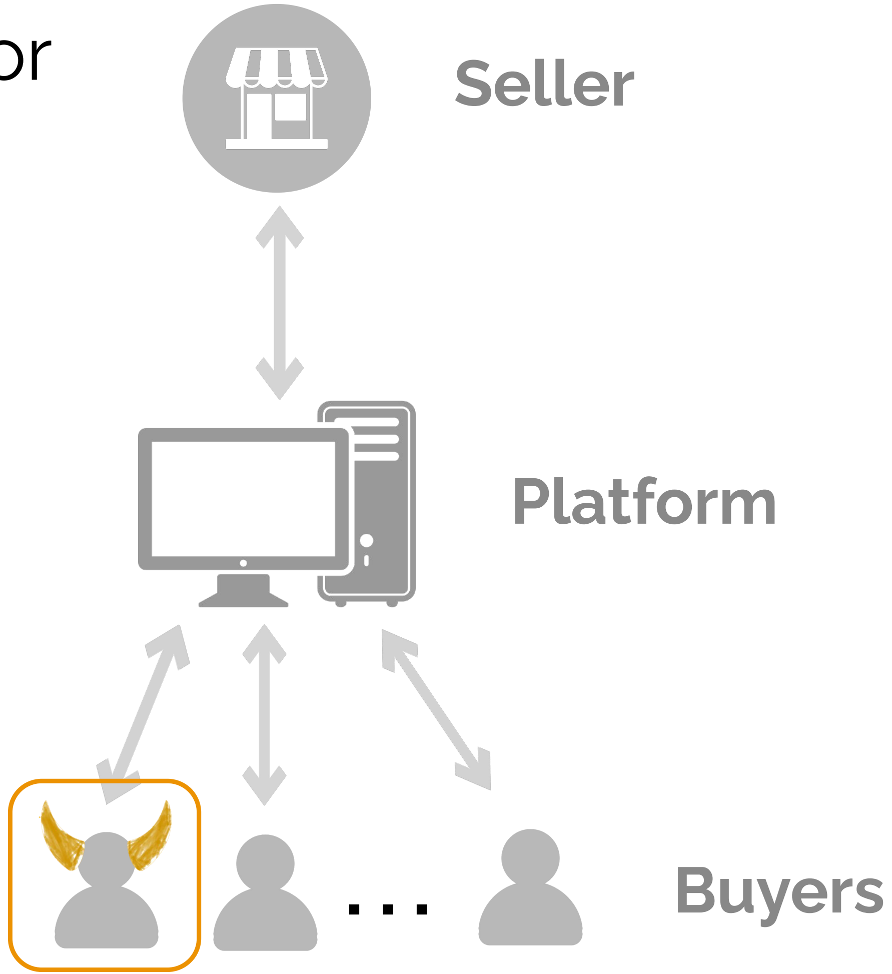
What is a **dream** platform-assisted auction?



Incentive compatible (IC) for

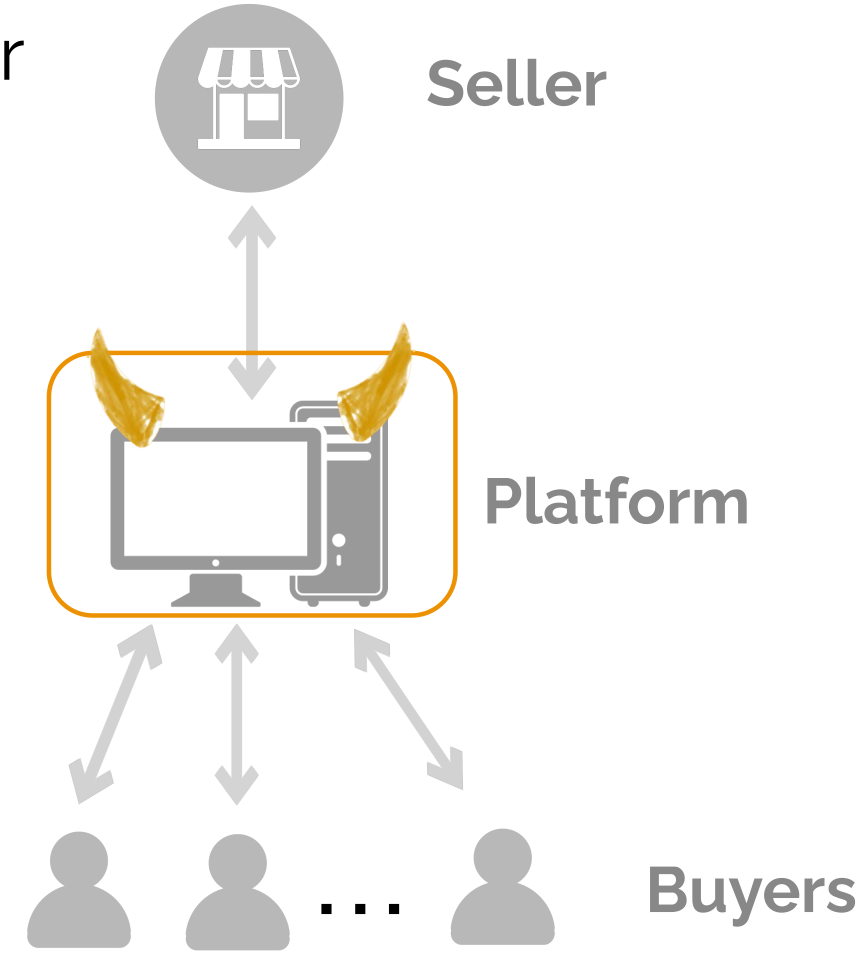
- a buyer

What is a **dream** platform-assisted auction?



Incentive compatible (IC) for

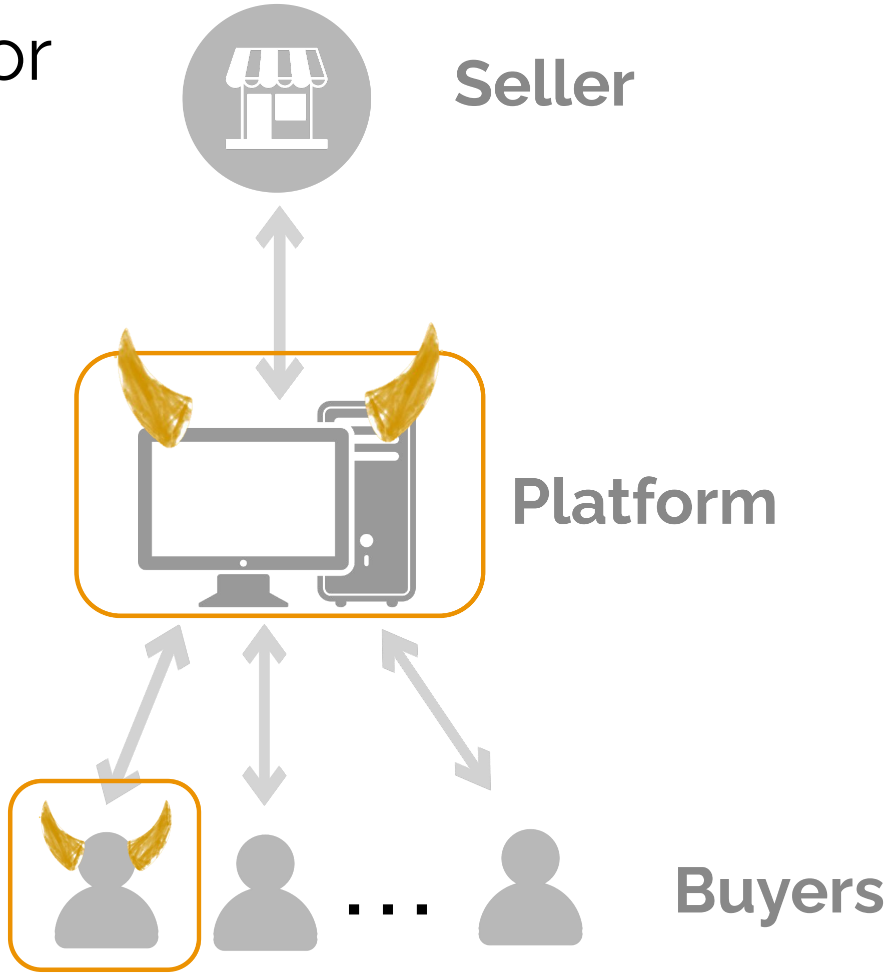
- a buyer
- the platform



What is a **dream** platform-assisted auction?

Incentive compatible (IC) for

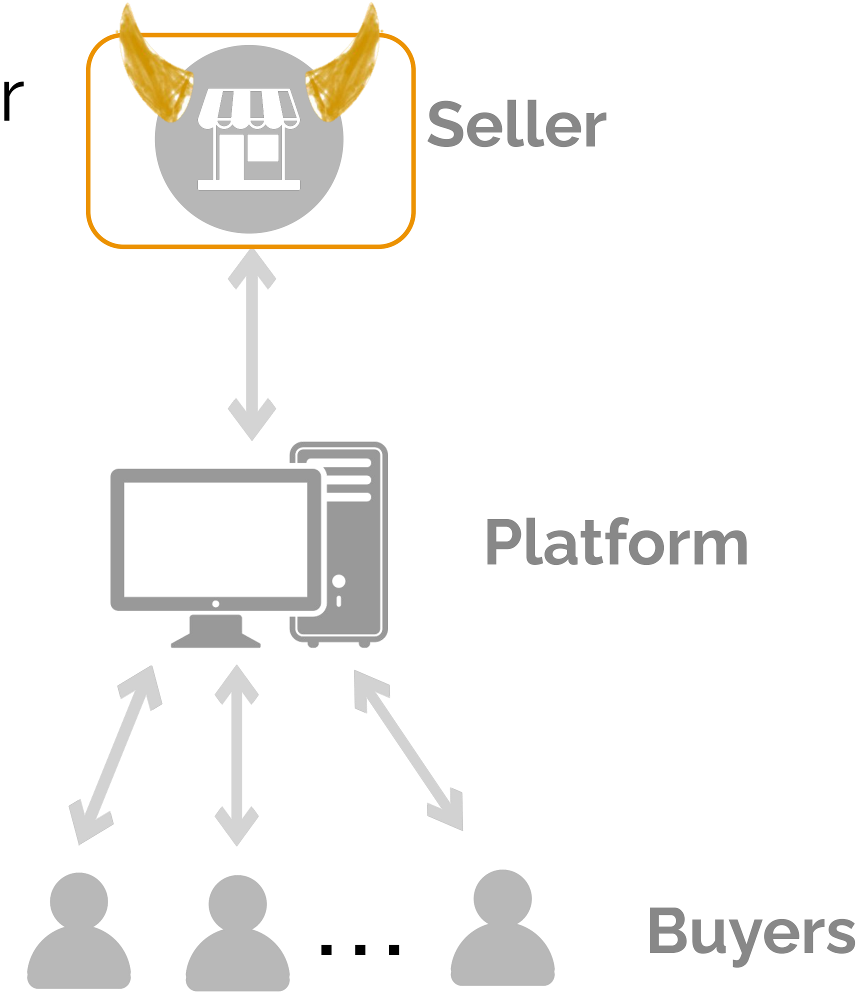
- a buyer
- the platform
- platform-buyer coalition



What is a **dream** platform-assisted auction?

Incentive compatible (IC) for

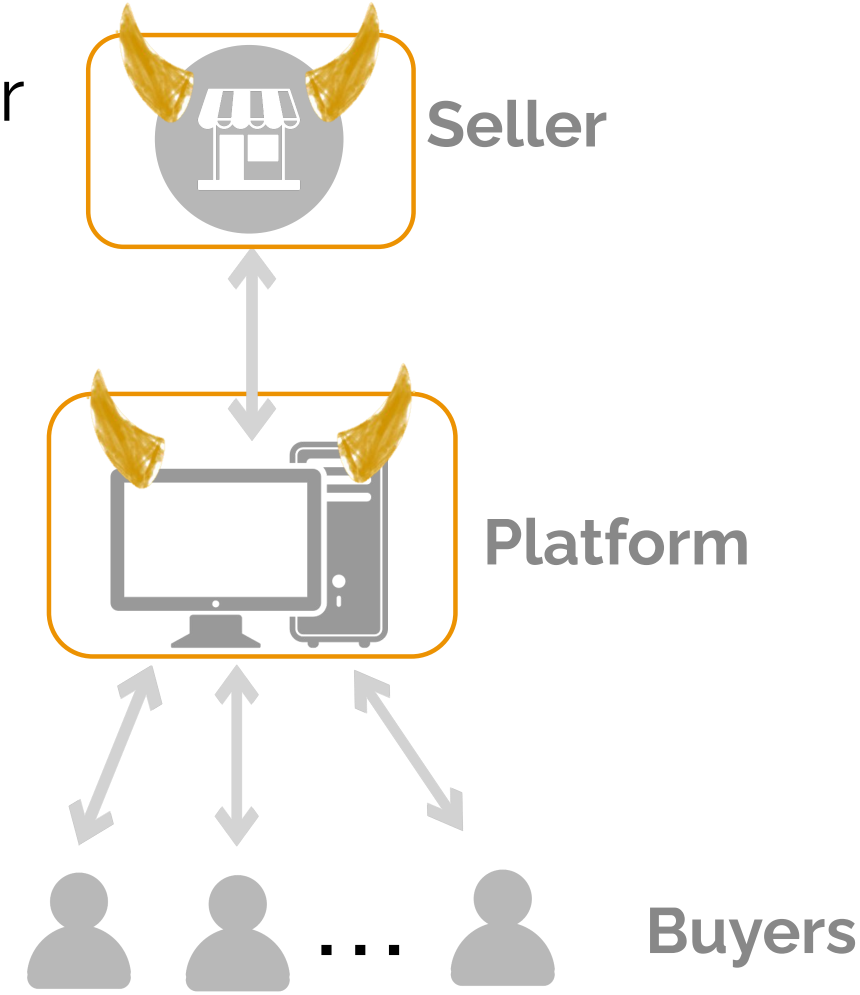
- a buyer
- the platform
- platform-buyer coalition
- the seller



What is a **dream** platform-assisted auction?

Incentive compatible (IC) for

- a buyer
- the platform
- platform-buyer coalition
- the seller
- platform-seller coalition

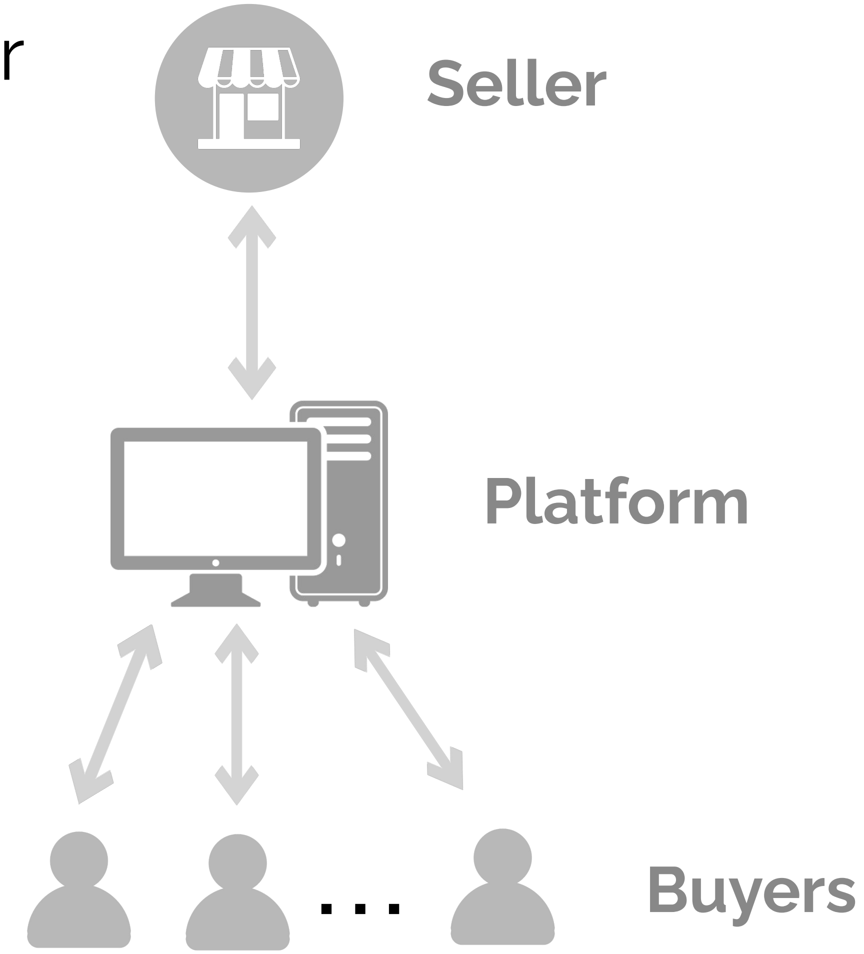


What is a **dream** platform-assisted auction?

Incentive compatible (IC) for

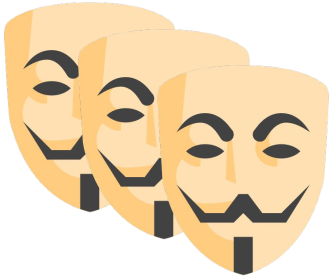
- a buyer
- the platform
- platform-buyer coalition
- the seller
- platform-seller coalition

What is a **dream** platform-assisted auction?



Overbid, underbid

Fake bids

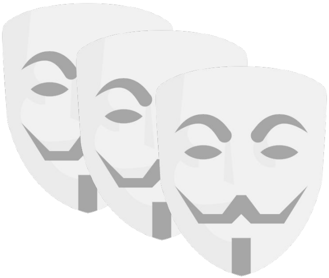


Arbitrarily deviate from protocol

Strategy space

Overbid, underbid

Fake bids



Arbitrarily deviate from protocol

Assumption:

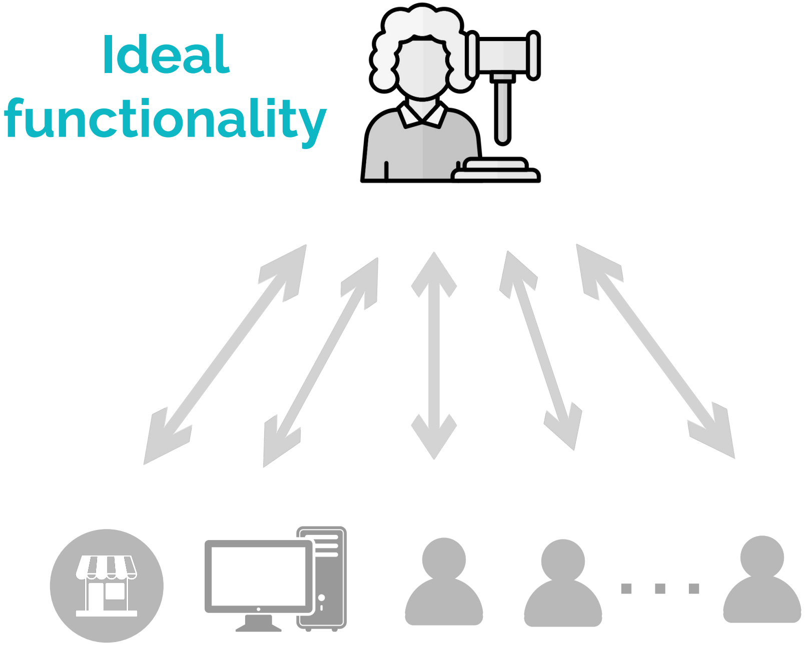
✓ cares about reputation

✓ adopts only **safe** strategies that do not risk detection

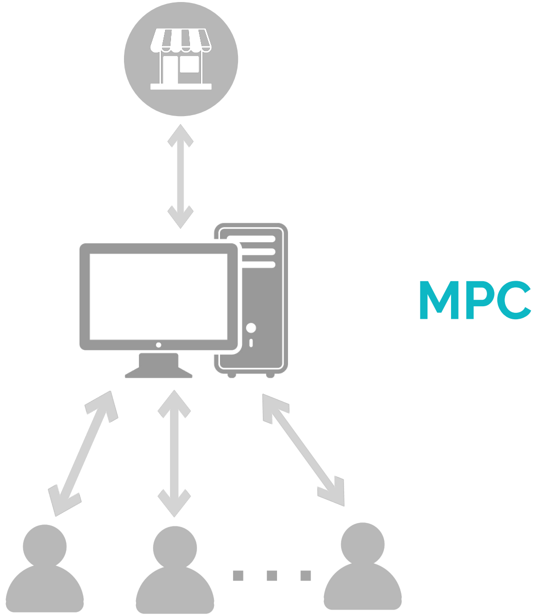
[Chung, Shi, SODA'23]

Why not just use MPC?

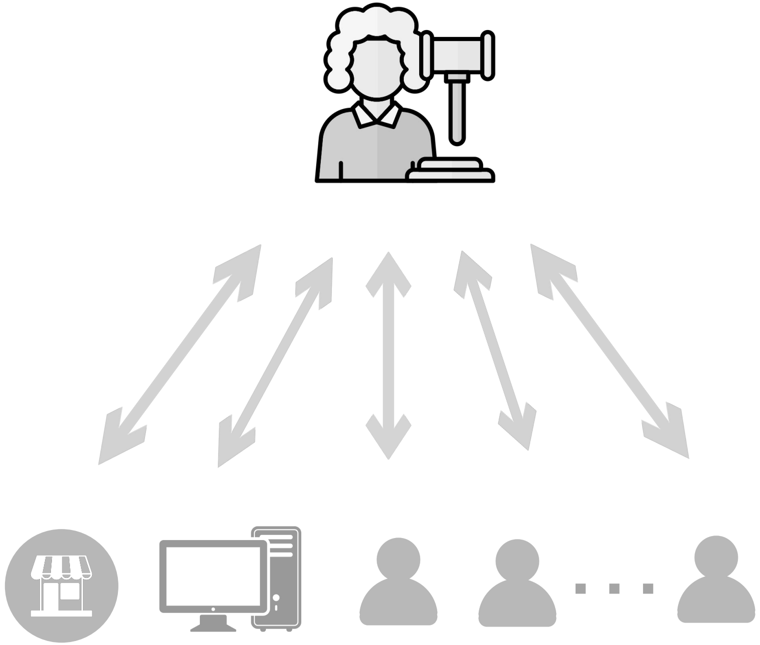
Ideal world



Real world



Ideal world



2nd price auction

- Allocate to top bidder
- Winner pays 2nd price
- Platform gets 10% of revenue, seller gets the rest

[Vickerey61, Bogetoft08]

benefit from overbidding

2nd price auction

- Allocate to top bidder
- Winner pays 2nd price
- Platform gets 10% of revenue, seller gets the rest

2nd price auction

- Allocate to top bidder
- Winner pays 2nd price
- Platform gets 10% of revenue, seller gets the rest

Example: 2 buyers

2nd price auction

- Allocate to top bidder
- Winner pays 2nd price
- Platform gets 10% of revenue, seller gets the rest

Example: 2 buyers

 value = 5

 value = 8

2nd price auction

- Allocate to top bidder
- Winner pays 2nd price
- Platform gets 10% of revenue, seller gets the rest

Example: 2 buyers

 value = 5

 value = 8

 should bid **8 - ε**

2nd price auction

- Allocate to top bidder
- Winner pays 2nd price
- Platform gets 10% of revenue, seller gets the rest

Example: 2 buyers

value = 5

value $\xleftarrow{\$}$ [0, 10]

2nd price auction

- Allocate to top bidder
- Winner pays 2nd price
- Platform gets 10% of revenue, seller gets the rest

Example: 2 buyers

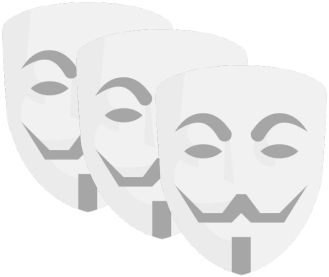
value = 5

value $\xleftarrow{\$}$ [0, 10]

should bid **5.45**

Overbid, underbid

Fake bids



Arbitrarily deviate from protocol

No protection

MPC dos and don'ts

Can we have a **dream** platform-assisted auction?

Crypto

Mechanism design

“**Decentralized** mechanism design”

Our Results

3 Utility-dominated emulation

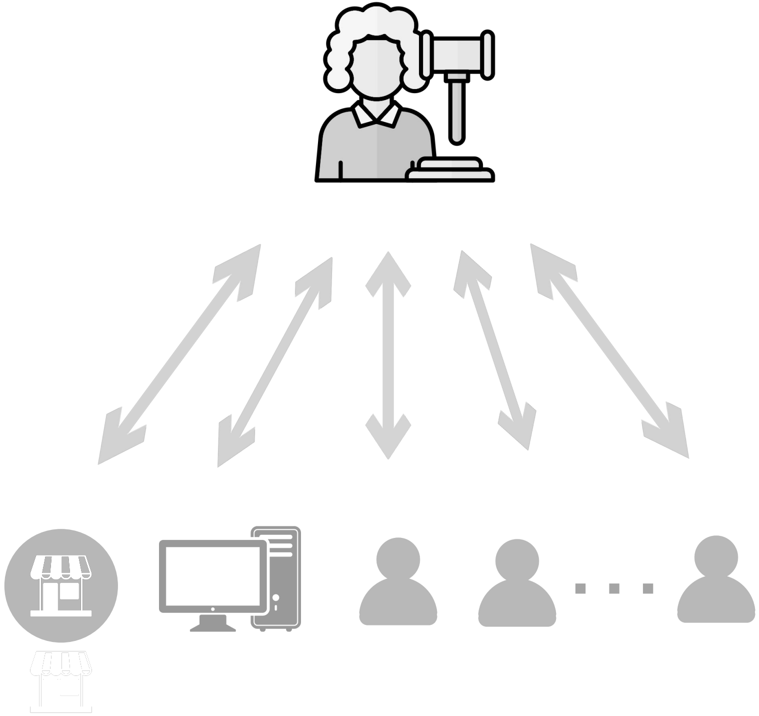
2 Fundamental limitations

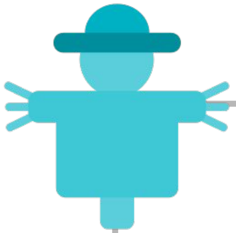
1 Inefficient MPC-based auction

Our Results

Recall the strawman MPC protocol

Ideal world



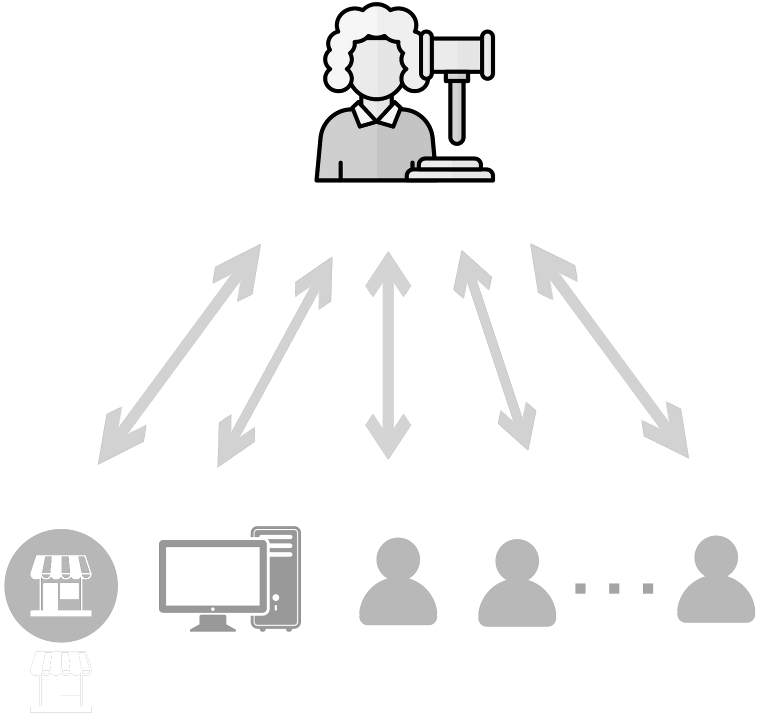


2nd price auction

- Allocate to top k bidders
- Sale price = (k+1)-st price
- Platform gets 10%
- Everyone learns their private outcome

The fix

Ideal world



2nd price with reserve R

- Allocate to top k bidders **who bid ≥R** 1
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing** 2
- **Broadcast final price** to all 3

IC for:

✓ buyer

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

IC for:

✓ buyer ✓ platform

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

IC for:

✓ buyer ✓ platform

✓ platform-buyer coalition

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

IC for:

✓ buyer ✓ platform

✓ platform-buyer coalition

What can the platform do that the buyer cannot on its own?

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

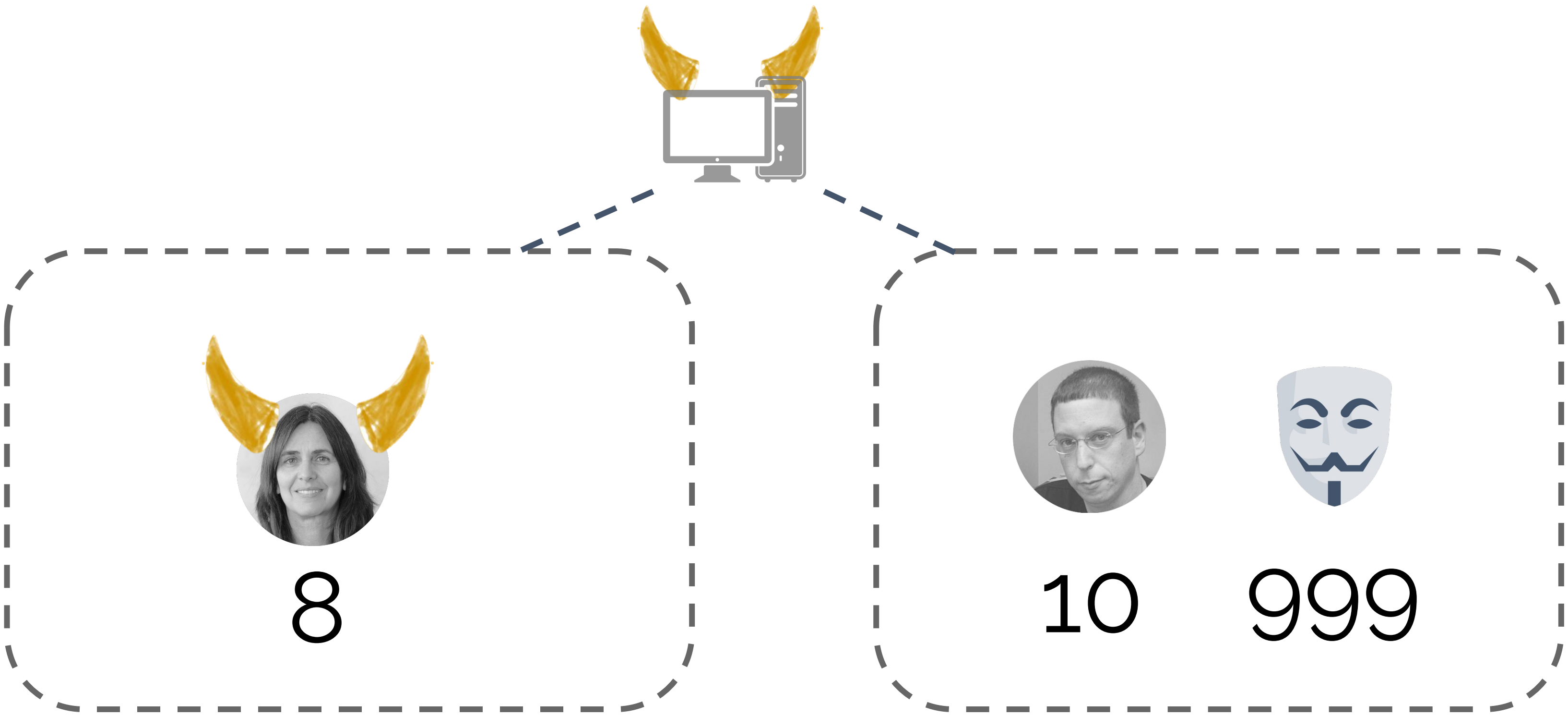
Broadcast prevents the “partitioned world” attack

8

10

1 item, reserve = 0

Broadcast prevents the “partitioned world” attack



1 item, reserve = 0

IC for:

✓ buyer ✓ platform

✓ platform-buyer coalition

Bayesian IC for:

✓ seller

✓ platform-seller coalition

assume: **suitable reserve**

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

[AL'20]

IC for:

✓ buyer ✓ platform

✓ platform-buyer coalition

Bayesian IC for:

✓ seller

✓ platform-seller coalition

Bake optimal price floor into mechanism itself

assume: **suitable reserve**

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

IC for:

✓ buyer ✓ platform

✓ platform-buyer coalition

Bayesian IC for:

✓ seller

✓ platform-seller coalition

Revenue optimal!

assume: **suitable reserve**

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

Privacy of MPC is important!

Bayesian IC for:

✓ seller

✓ platform-seller coalition

Revenue optimal!

assume: **suitable reserve**

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

Summary

IC for:

✓ buyer ✓ platform

✓ platform-buyer coalition

Bayesian IC for:

✓ seller

✓ platform-seller coalition

Revenue optimal!

assume: **suitable reserve**

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

Limitations

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

Limitations

Different fee structure

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

Limitations

Different fee structure ?

Avoid the broadcast ?

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

Limitations

Different fee structure ?

Avoid the broadcast ?

Improve efficiency ?

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

Different fee structure

Avoid the broadcast

Improve efficiency

Impossible

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

Utility dominated emulation

Different fee structure

Avoid the broadcast

Improve efficiency

2nd price with reserve R

- Allocate to top k bidders **who bid ≥R**
- Sale price = **(k+1)-st** price or **R, whichever greater**
- Platform gets **nothing**
- **Broadcast final price** to all

Generic MPC incurs **n^2** cost!

Generic MPC incurs **n^2** cost!

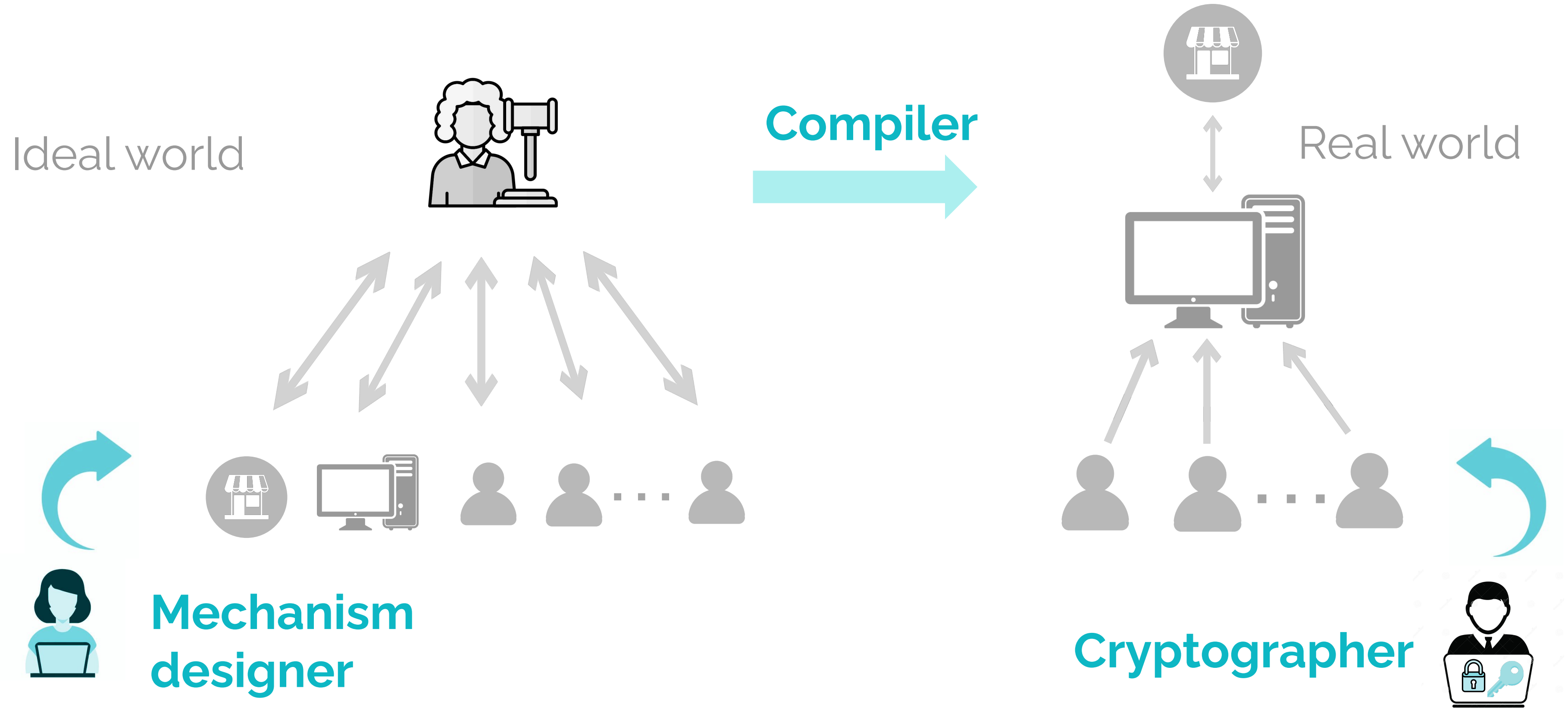
- Each player has a different output
- indistinguishability obfuscation

communication $\Longrightarrow$ **~O(n)**

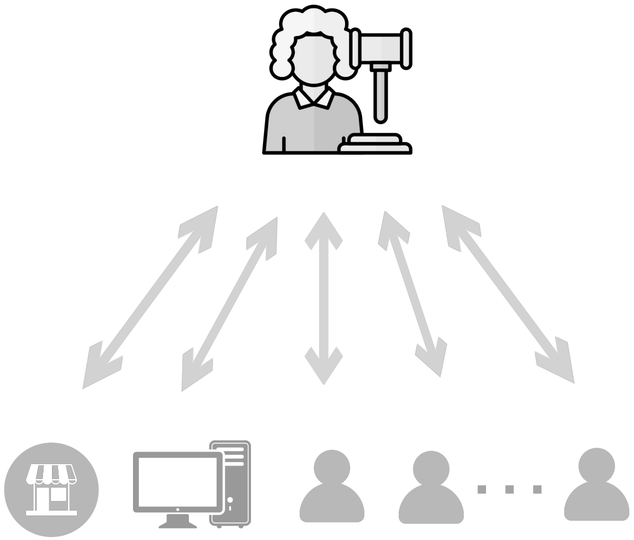
compute: still **n^2**

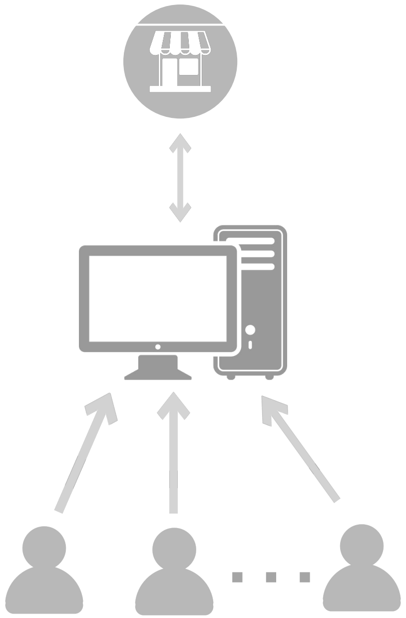
[HW15]

Design paradigm of MPC



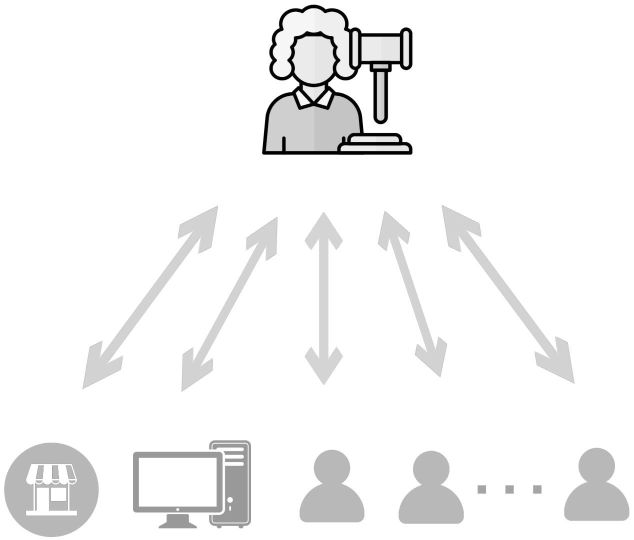
Can we improve the **efficiency** but preserve the **design paradigm?**

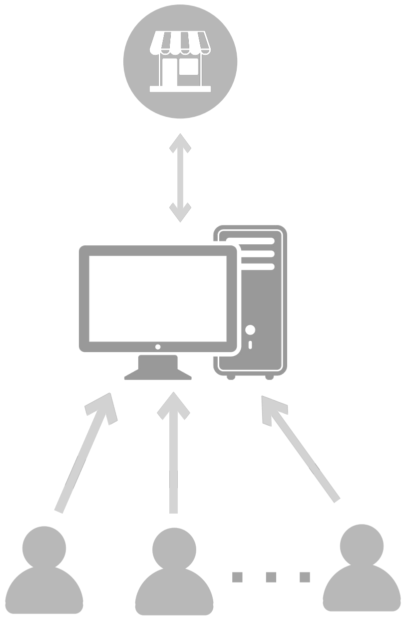




Utility-dominated emulation:

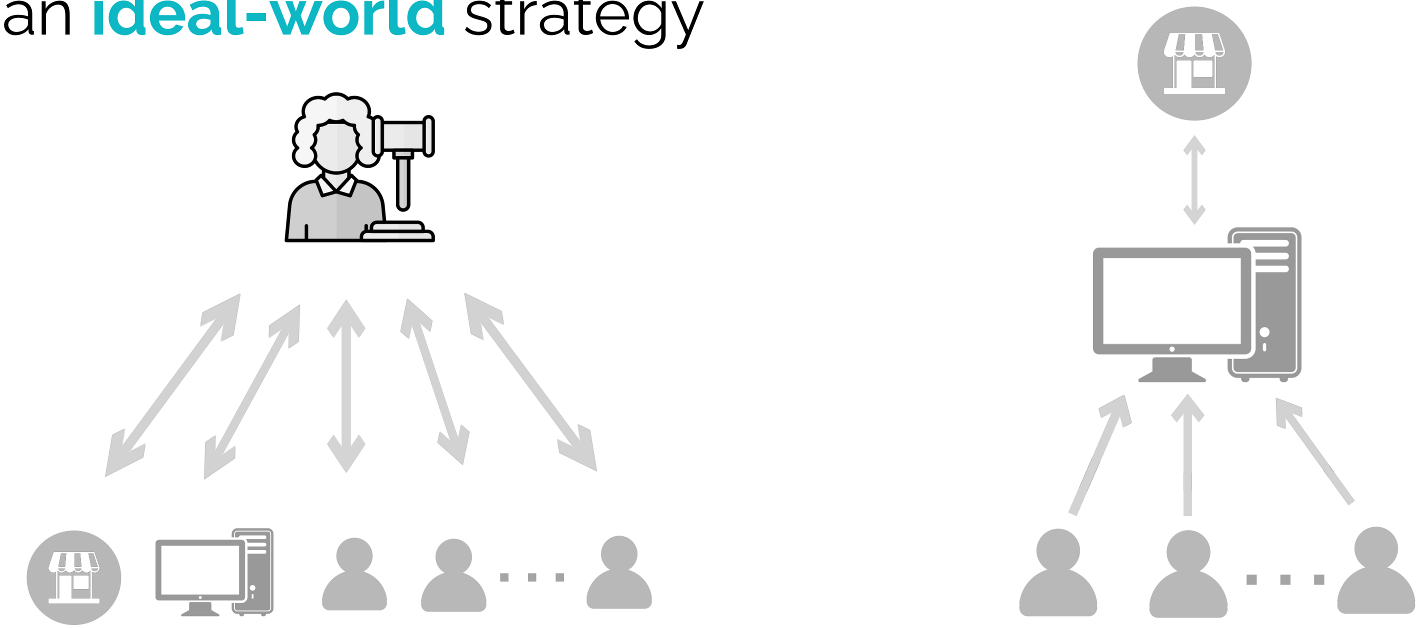
Any **real-world** strategy is **utility-dominated** by an **ideal-world** strategy





Utility-dominated emulation:

Any **real-world** strategy is **utility-dominated** by an **ideal-world** strategy



Thm: Ideal is IC + util-dominated emulation $\Longrightarrow$ Real is IC

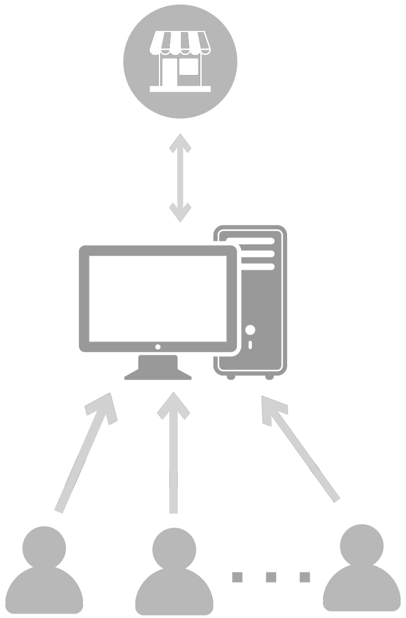
Our protocol

~O(n) cost

O(1) rounds

O(1) broadcast

broadcast necessary due to permissionless



See our paper for more

- More impossibilities & structural characterizations
- Efficient cryptography construction using ZK
- Computationally sound defn of “safe deviation”
- Proofs

https://eprint.iacr.org/2025/019

Decentralized mechanism design:

a **goldmine** of open questions

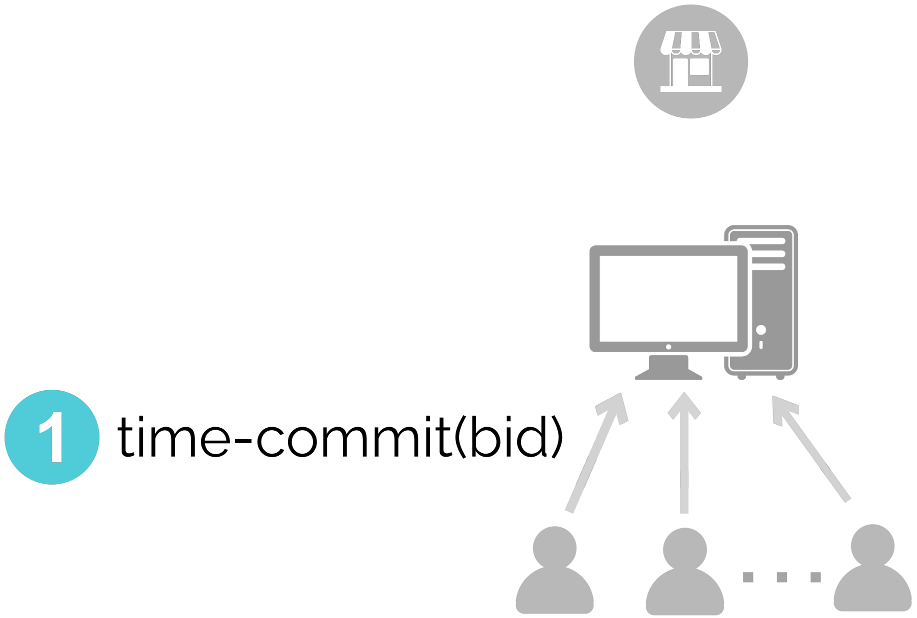
- Biggest challenge for **blockchains**
- **Heuristic** protocols used in practice
- What's the **right game-theoretic notion**?
- **Crypto** meets mechanism design

Thank you !

elainershi@gmail.com

The protocol

1 Buyers send timed commitments of bids



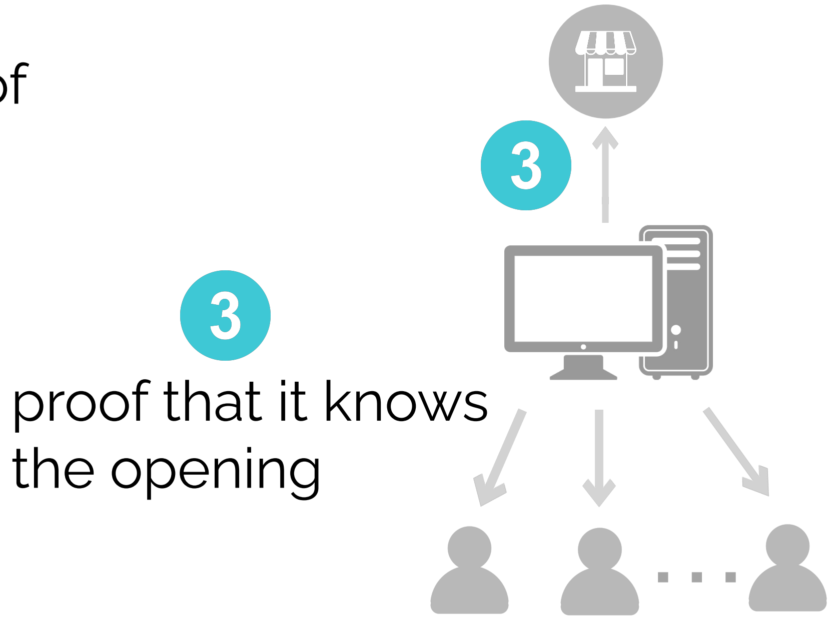
1 Buyers send timed commitments of bids

2 Platform broadcasts hash of commitments

1 Buyers send timed commitments of bids

2 Platform broadcasts hash of commitments

3 Platform proves it knows opening of hash

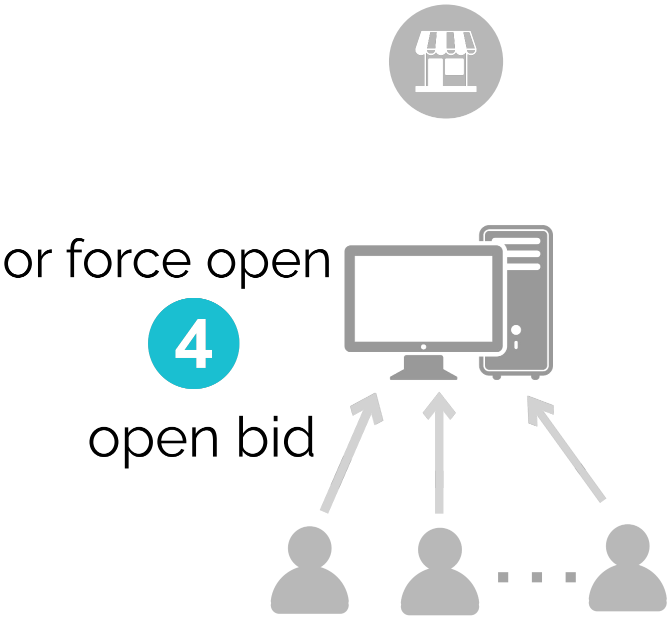


1 Buyers send timed commitments of bids

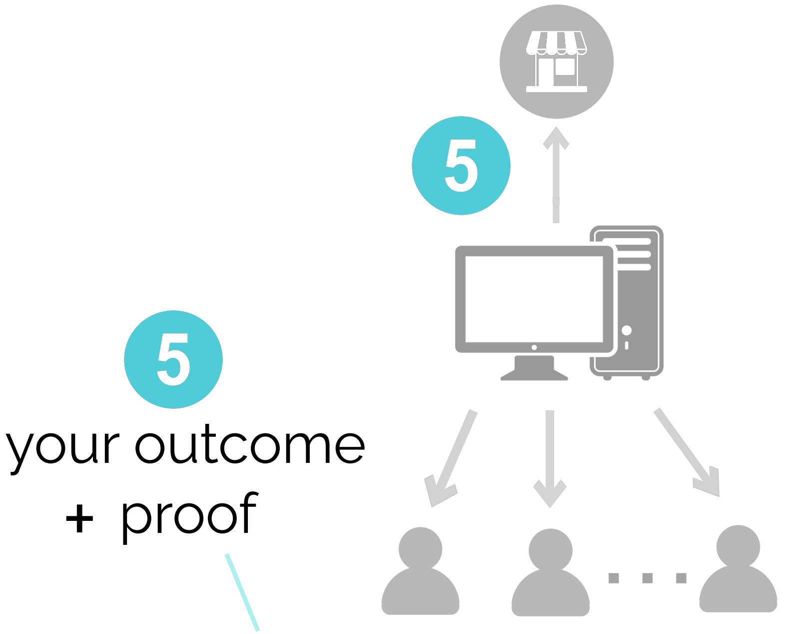
2 Platform broadcasts hash of commitments

3 Platform proves it knows opening of hash

4 Open or force-open bids



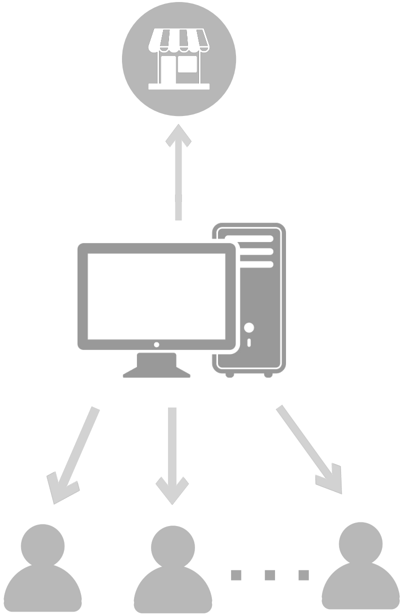
1. Buyers send timed commitments of bids
2. Platform broadcasts hash of commitments
3. Platform proves it knows opening of hash
4. Open or force-open bids
5. Platform sends everyone its outcome + proof



- outcome correct w.r.t. hash
- buyer's bid is included once

1. Buyers send timed commitments of bids
2. Platform broadcasts hash of commitments
3. Platform proves it knows opening of hash
4. Open or force-open bids
5. Platform sends everyone its outcome + proof

$O(1)$ rounds
$O(1)$ bcast
$\sim O(n)$ cost

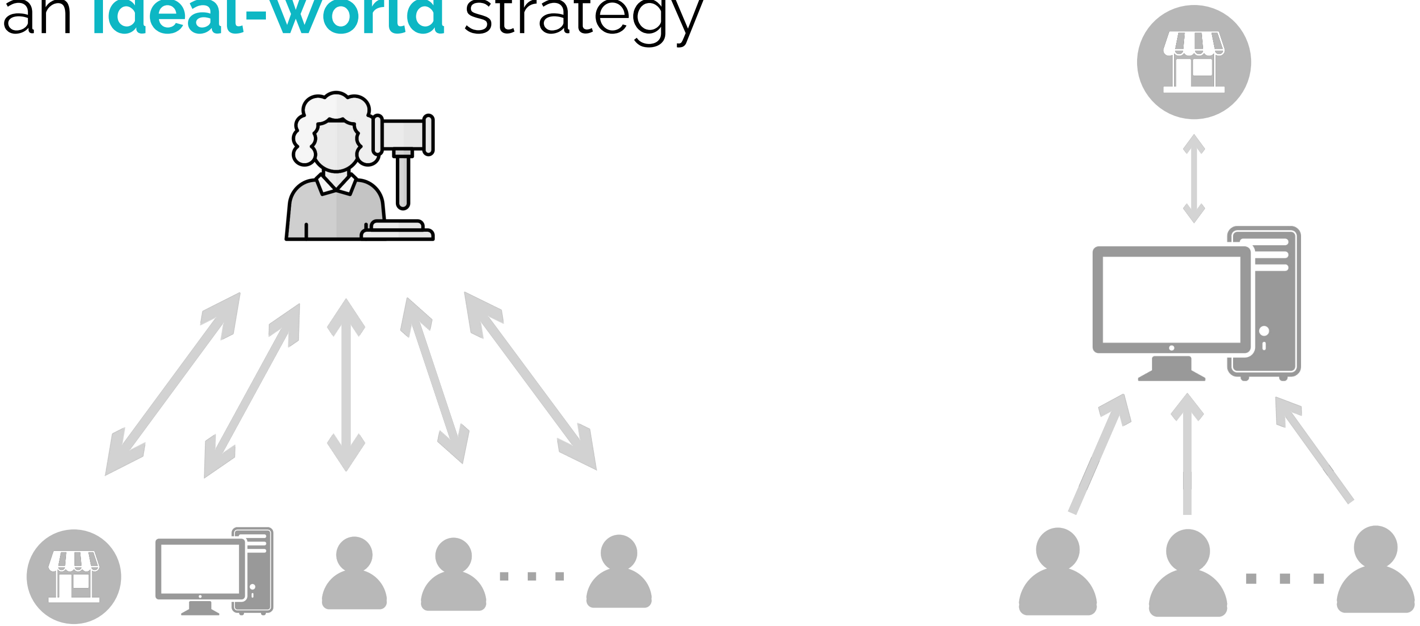


Thank you !

elainershi@gmail.com

Utility-dominated emulation:

Any **real-world** strategy is **utility-dominated** by an **ideal-world** strategy



Strategic util in Real ≤ Strategic util in Ideal ≤ Honest util in Ideal

= Honest util in Real