Revisiting Trust in Auctions

Aadityan Ganesh

Princeton University

Designing an Auction Market

- Pretend Meta is trying to design an auction market on facebook

- Meta designs basic auction rule. Auctioneers forced to use Meta’s basic rule, but have flexibility around the rule

- Auctioneers might not be happy to stick to Meta’s rule. Can potentially try to be sneaky.

Designing an Auction Market

- Pretend Meta is trying to design an auction market on facebook

- Meta designs basic auction rule. Auctioneers forced to use Meta's basic rule, but have flexibility around the rule

- Auctioneers might not be happy to stick to Meta's rule. Can potentially try to be sneaky.

- Today: How to design auctions when the market designer and the auctioneer are two different entities

The Private Value Model

- Different willingness to pay for the same item - value
- Eg: a litre of petrol

The Private Value Model

- Different willingness to pay for the same item - value
- Eg: a litre of petrol
  - Me: travel from Chennai to Hyderabad to teach at Math.Biz - Rs 100

The Private Value Model

- Different willingness to pay for the same item - value
- Eg: a litre of petrol
  - Me: travel from Chennai to Hyderabad to teach at Math.Biz - Rs 100
  - A cricketer: travel from Chennai to Hyderabad to play cricket match, earn match fee - Rs 120

The Private Value Model

- Different willingness to pay for the same item - value
- Eg: a litre of petrol
    - Me: travel from Chennai to Hyderabad to teach at Math.Biz - Rs 100
    - A cricketer: travel from Chennai to Hyderabad to play cricket match, earn match fee - Rs 120
    - Ambanis: Manage Mumbai Indians’ travel from Chennai to Hyderabad, earn fee from broadcasting rights - Rs 135

Auction from a Bidder’s View

- Bidder’s happiness from winning auction
  - Value
- Bidder’s sadness from winning auction
  - Payment
- Bidder’s net profit: utility
  - Value - payment

Auction from a Bidder’s View

- Bidder’s happiness from winning auction
  - Value
- Bidder’s sadness from winning auction
  - Payment
- Bidder’s net profit: utility
  - Value - payment

- Each bidder selfishly optimizes its utility

The Naively-Believe-Everyone Auction

- Collect bids from everyone
- Allocate to the bidder with the largest bid
  - Want to make the community as happy as possible

- Nobody pays anything

The Naively-Believe-Everyone Auction

- Collect bids from everyone
- Allocate to the bidder with the largest bid
  - Want to make the community as happy as possible

- Nobody pays anything

- Problem: contest of coming up with the largest number, no repercussion

User Incentive Compatibility [Roughgarden 2021]

- Bidders (users) optimize their utility by bidding their value truthfully

Non-Example: First Price Auction

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays bid

Non-Example: First Price Auction

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays bid

- Problem: winner wants to shade bid after knowing results

Example: Second Price Auction

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

Example: Second Price Auction

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Bidders bid truthfully
- Fix everybody else’s bid
    - Winner gains nothing by increasing or shading
    - Non-winners don’t gain by shading or increasing

Simpler Example: Posted-Price Mechanism

- n bidders, n goods
  - Each bidder wants only 1 item

- Post a price p
- Allocate good to everyone willing to pay at least p

Simpler Example: Posted-Price Mechanism

- n bidders, n goods
  - Each bidder wants only 1 item

- Post a price p
- Allocate good to everyone willing to pay at least p

- No point in lying
  - Same allocation for all bids above p and all bids below p

Second Price Auction Revisited

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

Second Price Auction Revisited

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Auctioneer can gain by injecting a fake bid
  - Becomes a first price auction!

Myopic Miner Incentive Compatibility (MMIC) [Roughgarden 2021]

- Miner should not be able to gain by injecting fake bids or censoring bids

Example (Provisional): First Price Auction

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays bid

Example (Provisional): First Price Auction

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays bid

- Fix users’ bids
  - Can’t gain by injecting fake bids- winner pays the same

Example (Provisional): First Price Auction

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays bid

- Fix users’ bids
  - Can’t gain by injecting fake bids- winner pays the same
  - Can’t gain by censoring bids- winner still pays the same

Simpler Example: Posted-Price Mechanism

- n bidders, infinitely many goods
    - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

Simpler Example: Posted-Price Mechanism

- n bidders, infinitely many goods
  - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

- Injecting fake bids will not change revenue from other bidders
- Censoring bids only cuts off the p payment made by the censored bidder

Posted-Price Mechanism Revisited

- n bidders, infinitely many goods
  - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

Posted-Price Mechanism Revisited

- n bidders, infinitely many goods
    - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

- Problem: Convince bidder with value p-5 to buy good. Separately refund 6!

Side Contract Proof [Chung and Shi 2023]

- A cartel consisting of auctioneer and bidders should not be able to jointly increase their net utility by colluding
    - Colluding = transparently reveal all colluding bidders' values and optimize group utility

Non-Example: Second Price Auction

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

Non-Example: Second Price Auction

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Auctioneer pays second highest bidder to increase bid, match highest bid

Example: EIP-1559 for Infinite Goods

- n bidders, infinitely many goods
  - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

Example: EIP-1559 for Infinite Goods

- n bidders, infinitely many goods
  - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

- Burn all payments. Auctioneer gets zero revenue.

Example: EIP-1559 for Infinite Goods

- n bidders, infinitely many goods
    - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

- Burn all payments. Auctioneer gets zero revenue.
- Suppose auctioneer and bidder collude:
    - Auctioneer always gets zero revenue from the auction.
    - If bidder with value v less than p gets the good, ends up with utility $v-p < 0$.
    - Joint utility decreases

Summary

Mechanism	UIC	MMIC	SCP
Second Price Auction	Yes	No	No
First Price Auction	No	Yes*	No*
Posted Price	Yes	Yes	No

EIP-1559 for Infinite Goods [Roughgarden 2021]

- User Incentive Compatible
- Myopic Miner Incentive Compatible
- Side Chain Proof

- Why?

EIP-1559 for Infinite Goods [Roughgarden 2021]

- User Incentive Compatible
- Myopic Miner Incentive Compatible
- Side Chain Proof

- Limitation: Auctioneer gets zero revenue
  - Avoidable?

The Big Impossibility [Chung and Shi 2023]

- A mechanism satisfying UIC, MMIC and SCP must leave the auctioneer with zero revenue
  - For infinite goods

- For finite goods no mechanism satisfies UIC, MMIC and SCP.

Summary

- Disappointing cannot design “great” mechanisms for finite number of goods

- At least, can satisfy all 3- UIC, MMIC and SCP for infinite goods
    - EIP-1559

Summary

- Disappointing cannot design “great” mechanisms for finite number of goods
- At least, can satisfy all 3- UIC, MMIC and SCP for infinite goods
    - EIP-1559
    - Not the end of bad news

EIP-1559 for Infinite Goods Revisited

- n bidders, infinitely many goods
  - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

- Burn all payments. Auctioneer gets zero revenue.

EIP-1559 for Infinite Goods Revisited

- n bidders, infinitely many goods
    - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

- Burn all payments. Auctioneer gets zero revenue.

- Auctioneer sends a tweet- “Pay me Rs 50 outside the platform. Otherwise, I won’t even include your bid in the auction”

Off-Chain Influence Proof [AG, Thomas and Weinberg 2024]

- Running a separate mechanism off-market should not increase the auctioneer’s revenue

- Small detour before seeing example for auction satisfying Off-Chain Influence Proof

Cryptography for Mechanism Design

- Collect bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Auctioneer can gain by injecting a fake bid
- Problem: auctioneer sees bids before finalizing all bids

Cryptography for Mechanism Design

- Auctioneer can gain by injecting a fake bid
- Problem: auctioneer sees bids before finalizing all bids

- Solution: Make sure auctioneer cannot see bids first. Make auctioneer commit to bids before bids are revealed to auctioneer

Cryptography for Mechanism Design

- Auctioneer can gain by injecting a fake bid
- Problem: auctioneer sees bids before finalizing all bids

- Solution: cryptography. Bidders encrypt bids and send to auctioneer.

- @$#%^%, %^$&&^%, *&^%^&&*

Cryptography for Mechanism Design

- Auctioneer can gain by injecting a fake bid
- Problem: auctioneer sees bids before finalizing all bids
- Solution: Auctioneer announces all encrypted texts that it sees
- I see “@$#%^%, %^$&&^%, *&^%^&&*”

Cryptography for Mechanism Design

- Auctioneer can gain by injecting a fake bid
- Problem: auctioneer sees bids before finalizing all bids

- Solution: Bidders reveal bids

- @$#%^% = 15, %^$&&^% = 10, *&^%^&&* = 25

- Can check whether revealed correctly
- Very difficult to find two different texts encrypted to the same gibberish

Second Price Auction with Encrypted Bids

- Collect encrypted bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Auctioneer cannot gain by injecting fake bid

Second Price Auction with Encrypted Bids

- Collect encrypted bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Auctioneer cannot gain by injecting fake bid
    - Lying through my teeth. Auctioneer still wants to inject fake bid
    - At least, not as obvious as highest bid minus noise!

Fake Bids in Second Price Auction with Encrypted Bids

- Collect encrypted bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Suppose bidder values come from
  - 25 wp ⅓
  - 5 wp ⅓
  - 0 wp ⅓

- 2 bidders

Fake Bids in Second Price Auction with Encrypted Bids

- Collect encrypted bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Suppose bidder values come from
  - 25 wp ⅓
  - 5 wp ⅓
  - 0 wp ⅓

- 2 bidders

- Not injecting any fake bids: 40/9
- Injecting a fake bid at 25: more than 25/3

Fake Bids in Second Price Auction with Encrypted Bids

- Collect encrypted bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Not ideal! Auctioneer injects fake bid even with cryptography.

Fake Bids in Second Price Auction with Encrypted Bids

- Collect encrypted bids from everyone
- Allocate to bidder with largest bid

- Winner pays second highest bid

- Not ideal! Auctioneer injects fake bid even with cryptography.

- However, auction still UIC. Does not devolve into a first price auction.

Reserve Price

- Reserve price quite common in auctions

- Auctioneer can say “I don’t want to part with good unless paid at least the reserve r”

Second Price Auction with Reserve and Cryptography

- Collect encrypted bids from everyone
- Allocate to bidder with largest bid, if largest bid greater than reserve
- Winner pays max (second highest bid, reserve)
- Revenue optimal for many value distributions (send reading material if interested)

Dilemma

- MMIC, take away from the regular second price auction- auctioneer is evil if they inject fake bids
  - Fake bids forces bidders to not bid truthfully

Dilemma

- MMIC, take away from the regular second price auction- auctioneer is evil if they inject fake bids
  - Fake bids forces bidders to not bid truthfully

- Take away from Cryptographic Second Price Auction- auctioneer injects fake bid to increase revenue, but does not force bidders to bid differently.
  - Fake bids are fine

Dilemma

- MMIC, take away from the regular second price auction- auctioneer is evil if they inject fake bids
  - Fake bids forces bidders to not bid truthfully

- Take away from Cryptographic Second Price Auction- auctioneer injects fake bid to increase revenue, but does not force bidders to bid differently.
  - Fake bids are fine

- How to differentiate between the two cases?

Miner Advice [AG, Thomas and Weinberg 2024]

- Allow auctioneer to actively advice the mechanism
  - Auctioneer need not be a mute spectator whose only job is to run the auction described by the platform (Meta)

- Auctioneer can play an advice from an advice set (eg: reserve price)

Miner Advice [AG, Thomas and Weinberg 2024]

- Allow auctioneer to actively advice the mechanism
  - Auctioneer need not be a mute spectator whose only job is to run the auction described by the platform (Meta)

- Auctioneer can play an advice from an advice set (eg: reserve price)

- MMIC- Auctioneer is not evil as long as auctioneer does not inject fake bid and does not censor bid

Miner Advice [AG, Thomas and Weinberg 2024]

- Allow auctioneer to actively advice the mechanism
  - Auctioneer need not be a mute spectator whose only job is to run the auction described by the platform (Meta)

- Auctioneer can play an advice from an advice set (eg: reserve price)

- On-Chain Miner Simple- Auctioneer is not evil as long as auctioneer plays advice, does not inject fake bid and does not censor bid

Summary

- Cryptographic Second Price Auction with Reserve satisfies
    - UIC (On-Chain User Simple)
    - On-Chain Miner Simple for many distributions
    - Off-Chain Influence Proof for many distributions

Second price auction with reserve is the revenue optimal auction. Why would auctioneer want to do absolutely anything else outside the market?

SCP for the Cryptographic Second Price Auction with Reserve

- Suppose bidder values come from
  - 25 wp ⅓
  - 5 wp ⅓
  - 0 wp ⅓

- 2 bidders

- Auctioneer colludes with bidder 2 whenever they have a value 5- auctioneers sets reserve zero and asks them to bid 25 (assume ties broken in favour of bidder 1)

In Fact [AG, Thomas, Weinberg 2024]

- Impossible for any mechanism to satisfy UIC, On-Chain Miner Simple, Off-Chain Collusion Proof and SCP.

- Life still not ideal. Further refine definitions.

Is SCP the Best Way to Capture Collusion?

- Assume all colluders integrate into a single entity
- Can mind read each other’s values!
- Unrealistic.

Posted-Price Mechanism Revisited

- n bidders, infinitely many goods
  - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

Posted-Price Mechanism Revisited

- n bidders, infinitely many goods
  - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

- Problem: Ask bidder with value p-5 to bid p. Separately refund 6 to bidder.

Posted-Price Mechanism Revisited

- n bidders, infinitely many goods
  - Each bidder wants only 1 item

- Post a price p (determined exogenously)
- Allocate good to everyone willing to pay at least p

- Problem: Ask bidder with value p-5 to bid p. Separately refund 6 to bidder.

- Why would anyone tell the auctioneer their value is greater than p?

  Always bid p-5, and get good at cost p-6!

Weak, Yet Sufficient Collusion Resistance

- Collusion- conversation between auctioneer and bidder through an off-the-market platform

- However, bidder need not be truthful to the auctioneer off-the-market

Weak, Yet Sufficient Collusion Resistance

- Collusion- conversation between auctioneer and bidder through an off-the-market platform

- However, bidder need not be truthful to the auctioneer off-the-market

- Same as auctioneer running an off-the-market mechanism. Collusion a special case of Off-Chain Influence Proof!

Conclusion

- Desiderata when the market designer is different from the auctioneer
  - User Incentive Compatible
  - Myopic Miner Incentive Compatible/On-Chain Miner Simple
  - Off-Chain Influence Proof

- The Cryptographic Second Price Auction with Reserve satisfies all of the above properties!