Title:

Literature review of auction mechanism that fit in with Flashbots

Team:

Surya Bakshi

Created:

2020-11-24

Status:

Stagnant

Github:

mev-research/FRP-7.md at main · flashbots/mev-research · GitHub

Literature review of auction mechanism that fit in with Flashbots.

The puspose of this isssue is to investigate and survey the existing literature of auction mechanism design to motivate the design of the block space and transaction ordering auctions enabled by mev-geth. An mev-geth auction is different from a traditional auction in that users submit and bid on tx sequences that are, potentially, non-overlapping. The current implementation of mev-geth accepts only a single transacton sequence into a block, however, a more sophisticated auction mechanism might permit multiple “bundles” with interaction between winning, non-overlapping bundles. Therefore careful consideration is required to design a good auction mechanism for mev-geth. In addition to surveying existing literature, it is impotant to survey auction designs in existing crypto projects so understand the practical requirements of a decentralized auction such as privacy, security, auditability, and efficiency.

Background and Problem Statement

The high-level research question is: What is a good auction mechanism for mev-geth auctions?

The first step in answering this broad question is first surveying and evaluating the existing literature and practice of auction mechanism design in a decentralized setting. In order to tackle this objects is to answer the following questions:

- In what ways do crypto auctions differ from existing literature: what are the impact of easy collusion forming on cooperative strategies and does current literature fall short of addressing this concern? Ad auctions have a similar setting, perhaps a better survey of how they deal with it? (see Methodology for survey of existing projects, i.e. industry anecdotes).
- What assumptions can be made about the participants and their capabilities (includes a potentially malicious miner)?
- Does expanding the auction format (from a single winning bundle to potentially multipe winning bundles) make auction design much more difficult?
- How do current implementation auctions in crypto deal with issues such as efficiency, security, privacy, and auditability?
- In the field of combinatorial auctions: are there existing theoretical auctions that imply constraints on our setting in terms of computability of optimal strategy?
- In the area of computational complexity: are there computationally difficult auctions with good enough heuristic, or sub-optimal, solutions?
- How does auction theory reason about potentially colludin parties?
- What are the computation bounds on miners in determining auction winner(s)?
- How can we scale auctions to many bots/participants?
- What are the tradeoffs involved in implementing such an auction in L2?

Plan and Deliverables

The proposed methodology is to first survey existing crypto projects that implement auctions and understand how the blockchain world constrains design choices in auctions and develop a classification system auctions based on their design. The next task is to survey existing combinatorial auction mechanisms and fit them into the current classiciation. This requires also iterating on the classification system as it becomes less useful in differentiating mechanisms. Finally, we shall arrive at a classification system for auction mechanisms on axis such as privacy, auditability, computational efficiency, and threat model to posit a few.

The proposed deliverables are:

- Develop a taxonomy for existing auction models and implementations that aides in selection auction design decisions.
- Arrive at a conclusion about a threat model and auction mechanism that fits mev-geth.

References

- This great response by Tarun Chitra on an MEV Auction proposal
- digital ad auctions paper
- another real-time bidding paper
- Prior attempt at a fee market for Ethereum
- Algorithmic Game Theory bible (especially chapter 11)
- Here is the POC version of the bundle auction: Flashbots miners select the most valuable bundle per unit of gas used and place it at the beginning of the list of transactions included in a block at the given blockheight. Miners determine the value of a bundle based on the following equation where the change in block.coinbase balance represents a direct transfer of ETH through a smart contract. [

](https://user-images.githubusercontent.com/15959632/99228128-7c883b00-27ec-11eb-8b95-3896b21e0b08.png)