Networks: Fall 2023	Crypto Fee Auctions
David Easley and Yian Yin	Background Reading

Cryptocurrencies such as BitCoin require a sequential record of all transactions that every participant in the protocol can agree on. This record is stored in a globally visible *blockchain*, which consists of a series of *blocks*, each of which confirms for all participants that certain transactions have been performed. Participants in the protocol called *miners* compete to be in charge of constructing the next block to add to the blockchain.

A cryptocurrency transaction, in say BitCoin, isn't complete until it is recorded on the relevant blockchain. A typical transaction might involve moving one BitCoin (BTC) from one users wallet to another users wallet. Suppose that user number 1 wants to move one BTC from their wallet to user 2's wallet. User 1 would submit this transaction to the pool of transactions waiting to be recorded on the BitCoin blockchain.[1]

There may be many transactions waiting in the pool; perhaps many more than can be recorded on the next block of transactions. A miner is selected to build the block and that miner chooses among the transactions in the pool. Various cryptos use various mechanisms for selecting the miner (for example, poof of work or proof of stake) and these mechanisms evolve over time.[2] We won't discuss how the miner is chosen or any fixed payments the miner receives for having been chosen. That isn't important for determining how the miner chooses transactions from the pool or how users should behave in submitting their transactions to the pool. Instead, we focus on a miner who has been selected to build a block and a collection of users who want their transactions to be recorded on the block.

Users incentivize the miner to select their transaction by attaching a fee to the transaction. For example, user 1 may submit a transaction saying remove 1.01 BTC from my wallet and put 1.00 BTC in user 2's wallet. The leftover 0.01 BTC is retained by the miner. That 0.01 BTC is the fee the user proposes to pay to have their transaction recorded on the block. It is effectively a bid for space on the block.[3]

How should the users select fees and how should the miner select transactions? To discuss these questions we need some notation. Let's suppose that there are K slots available on the current block; that is up to K transactions can be recorded on it. Let's index users by $i = 1, \ldots, I$ where $I > K$, as otherwise there is no allocation problem. Suppose that user i has value V_i for having their transaction placed on the current block where the V_i are independent, private values. Each user knows their own value, but not other's values and the miner does not know any user's value.

[1]This handout is based on " Stable Fees: A Predictable Fee Market for Crypto-Currencies" by Basu, Easley, O'Hara and Sirer, forthcoming in *Management Science*. The handout uses a simplified and stylized model of the crypto fee market.

[2]Etherium has switched from a proof of work system to a proof of stake system.

[3]We will treat all transactions as if they take the same amount of space on the block and we will treat the current block separtely from future blocks.

1 Multi-unit Auctions

This fee payment system shares many features with a multi-unit first price, or discriminatory, auction. The users who are choosing fees are bidding for space on the block; and although the miner who is building the block isn't an auctioneer, the miner is selling slots on the block to users. So auction theory should provide some insight into how bidders should behave. Let's first ask what happens in standard multi-unit auctions. The simplest such auction to analyze is not a discriminatory auction, but rather a uniform price auction.

Multi Unit Uniform Price Auctions: Suppose there are K items and I bidders, each of whom wants at most one item. The bidders have values V_i where the V_i are independent, private values for an item. In a uniform price auction with K items sold the K highest bidders at the $(K+1)$st highest bid it is a dominant strategy for each bidder to bid truthfully.

For the case of $K = 1$ this is just the standard second price auction that we discussed in class. In that auction it's optimal for any bidder to bid truthfully. The intuition for this result is that a bidder's bid only affects whether or not they win the auction; it does not affect how much they pay conditional on winning the auction. A bidder wants to win whenever they can do so by paying at most their vlaue for the object. Bidding V_i maximizes this chance of winning without paying more than the item is worth.

The same logic applies to the $K > 1$ case. A sketch of the proof is as follows. Consider some bidder i. Let $\hat{b}$ be the Kth highest bid of other bidders. We will argue that i should not bid more than V_i and then that i should not bid less than V_i. Consider $b_i > V_i$. This only matters if $b_i > \hat{b} > V_i$. In this case i wins but pays more than V_i. Alternatively, consider $b_i < V_i$. This only matters if $V_i > \hat{b} > b_i$. In this case i does not win the auction, but would have won with a bid of V_i and would have paid $\hat{b} < V_i$.

Next let's consider the discriminatory price auction in which the K items are sold to the the K highest bidders and each winning bidder pays their own bid. For the case of $K = 1$ this is just the first price auction we discussed in class. There is no dominant strategy for this auction. In particular, bidding V_i, or more than V_i, is a dominated strategy. Since any winning bidder pays their bid, a bid of V_i guarantees a 0 payoff; either the bidder does not get an item and has 0 payoff or does get an item and pays V_i, and so has a 0 payoff. Bidding more than V_i is even worse. It's optimal for a bidder to bid less than V_i, but how much less depends on many factors: how many bidders there are, the distributions of their values, and how the other bidders behave. We saw an example in class where if $K = 1$ and V_i is distributed uniformly on $[0, 1]$ there is an equilibrium in which bidder i bids $V_i(I-1)/I$. The case of $K > 1$ is more complex, but the same logic implies that there is no dominant strategy and the truthful bidding is a dominated strategy.

2 Applying Auction Theory to the Crypto Fee Market

There are several differences between the crypto fee market and a standard K unit auction. First, the miner isn't a trusted auctioneer.[4] A miner can choose any transactions from the pool and the miner can enter fake transactions into the pool after knowing whats in it and before slecting transactions from it. The primary constraints on the miner are that no more transactions can be selected than can be placed on the block and the fees associated with these each of selected transactions are whatever the mechanism specifies—-currently the amount they bid.

Let's first analyze fake transactions. Consider the case of $K = 1$ and the second price auction with an strategic auctioneer who can enter fake bids. The auctioneer' observes all bids, decides whether to submit a fake bid and if so where to place it, and then awards the object to the highest bidder at the second highest bid. Clearly, the miner wants to submit a fake bid just below the highest real bid. The highest bidder will win and will pay almost his own bid. The auctioneer has turned this supposedly second price auction into a first price auction. If bidders know this they will bid as they would in a first price auction. The outcome will then be the outcome from a first price auction and not the outcome from a second price auction.

If $K > 1$ the auctioneer has even more opportunities to manipulate the outcome. To see this consider the case of $K = 2$. Suppose there are three bidders and the auction form is third price. Suppose the bids are in order from highest to lowest: $b_1 > b_2 > b_3$. Without manipulation the two items are sold at price b_3 to the bidders who bid b_1 and b_2. The seller can clearly earn more by submitting a bid of approximately b_2 and selling both items at that price. But he may be able to do even better by submitting a bid of approximately b_1 and selling only one item at price b_1. In this case the seller sells the second item to himself (and we assume that the seller has 0 value for a retained item). This would be optimal if $b_1 > 2b_2$. With even more items there are more opportunities for manipulation, but they each involve comparing the impact of selling one less item versus selling the remaining items at the next highest bid.

There is one more important difference between auction theory to the crypto fee market. The crypto mechanism can only condition payments on fees bid by transactions that are placed on the blockchain. Only the miner knows exactly what transactions were left in the pool rather than being placed on the blockchain. So a $(K + 1)$st auction for K slots in the block isn't feasible. The closest approximation is a Kth price auction for the K slots on the block. In this uniform Kth price auction, the price a winning bidder pays may depend on the amount they bid—we lose the key bit of logic from second price auctions that a bid affects only whether the bidder wins and not how much they pay conditional on winning. But note that in a Kth uniform price auction this is only an issue for the Kth highest bidder as only that bidder's bid affects the price. If $K = 1$ this is just a first price auction, but as K grows the chance that any bidder is the one whose bid sets the price may decline, suggesting that for large blocks the incentive bidders have to behave strategically may also decline.

[4] In standard auction theory it's important that the auctioneer can commit to an auction form. If instead the auctioneer behaves strategically we have a new game with both the auctioneer and bidders as players.

3 Advanced Material: Auction Theory Applied to Large Crypto Markets

In the crypto fee market there is no trusted auctioneer and dominant strategies for users aren't possible. But if a Kth uniform price auction is used and there are many users relative to the number of slots on the block the gains that either miners can make from strategic behavior or that users can make from non-truthful bidding are small. Finding optimal, or even good, strategic behavior can be costly. So if the gain to optimal strategic behavior is small it may be that users and miners will chose to follow simple, non-strategic rules.

Consider the following Kth uniform price fee mechanism:

- Users bid fees and the miner can also bid by inserting fake transactions into the pool.
- The highest K bids are included in the block.
- All included users pay the lowest bid included in the block.

Suppose that there are I bidders for the K slots on the block. Suppose also that user values are identically and independently distributed on some finite interval according to a strictly positive, continuous density. Let's assume that all users bid truthfully and that the miner behaves as a trusted auctioneer—no fake bids. We want to aruge that the benefit to any user or the miner from strategic behavior is small for large I.

If the fee mechanism above is used then truthful bidding is not a dominant strategy. However, the expected gain from strategic bidding decreases to 0 as the number of bidders grows. The intuition for this claim is straightforward. A user can gain from strategic bidding only if the the user's value is greater than the Kth highest value of other users and this gain is bounded by the difference between the $(K-1)$st highest and the Kth highest values of other users. The expected value of this gain converges to 0 as I grows.

With this fee mechanism miners have an incentive to behave strategically, but the expected gain to a miner from strategic behavior also decreases to 0 as the number of users grows. The intuition for this claim begins by observing that by inserting fake bids a miner can effectively reduce the number of real transactions placed on the block and potentially increase the uniform fee charged to each of these transactions. So in deciding whether to include fake bids the miner compares the revenue from K transactions at the K highest (real) bid and n transactions at the n highest (real) bid for $n = 1, \ldots, K-1$. As the number of users grows the increase in the uniform fee declines to 0 and the loss from dropping any transactions converges to the maximum possible users value. So the gain to miner manipulation declines to 0.