The Auction Grinding Attack:
and a case for a liquidation penalty in dai

1 Introduction

This paper describes a potential economic attack vector on the automatic auction mechanisms in the multi-collateral dai system, in particular, the reversing collateral liquidation auction. In summary: an attacker could open a Collateralised Debt Position (CDP), take out a substantial amount of debt against their collateral, and intentionally allow the position to go unsafe, causing the collateral to go to the liquidation auction. Upon liquidation the attacker can bid on their own collateral's liquidation auction, following a deterministic (pure) bidding strategy, which I describe. Following this strategy leads to meaningful profits in the event that the auction's capital participation rate (CPR) turns out to be low. In the case with no CDP liquidation penalty, the attack is practically risk free, since the worst possible outcome for the attacker is their gas expense, which is essentially bounded and easily quantifiable in advance.

The key fact that permits this attack is that when a liquidation auction finishes "in adequacy", the excess collateral is returned to the owner of the CDP, meaning that when the CDP owner is bidding on their own auction in the surplus phase, the marginal cost of a new bid at any price is zero.

To make matters worse, provided the other bidders suspect that a liquidation might be an auction grinder's, the Nash equilibrium in the auction game (with the bidders as players) might be in favour of the attacker, since bidders may be deterred from participating, knowing that the grinder's strategy will preclude them from winning the auction.

In the presence of a non-zero liquidation penalty, the attacker will have a guaranteed up-front cost, meaning that the worst-case outcome is negative and the attack is no longer risk-free. I will provide a heuristic for setting the liquidation penalty that will deter a profit-seeking rational attacker; the heuristic will rely on a model of auction participation.

2 The Collateral Auction

The *collateral auction* (also known as the `flip`-auction), is one of the three auction types in the dai system. The other two are the *debt auction* (the `flop`-auction), and the *surplus auction* (the `flap`-auction). The collateral auction is used to sell of collateral from risky CDP positions in exchange for dai, to protect the system from excessive risk. When a CDP's status becomes unsafe, the system permits any agent to initiate a collateral auction, sending the collateral to the `Flipper` contract, where it may receive bids. The mechanism used is a *reversing auction*, which I now explain (details of the auction mechanism not relevant to the auction grinding attack are omitted).

Like the other two dai auction types, the collateral auction has two termination conditions. The first is that the auction will terminate after `tau` seconds have passed from the moment the auction was initiated. The second is that `ttl` seconds have passed from the moment of the last bid. When an auction has terminated, no more bids are accepted, and the winning bidder may claim their collateral from the contract. Both `tau` and `ttl` are risk parameters set by governance.

The goal of the collateral auction is to cover the outstanding dai debt on the liquidated CDP. Let `tab` refer to the amount of dai debt outstanding on a CDP, and let `ink` refer to the amount of collateral in the CDP, both at the moment of liquidation. Then, the first priority of the auction is to try to raise `tab` dai, in exchange for any amount of the collateral, and if this much cannot be raised, to raise as much dai as possible. The second priority of the auction is to treat the CDP owner fairly, by not liquidating more of their collateral than is necessary to cover the debt. These two priorities correspond to the two phases of the auction: called the `tend` phase and the `dent` phase.

In the `tend` phase, the auction receives increasing bids (denoted `bid`) of dai for the fixed amount `ink` of collateral, with `bid` ≤ `tab`. When a new, higher `bid` is received, the difference between the new `bid` and the previous `bid` goes to the auction contract, while the rest goes to refund the previous bidder. If the auction terminates in the `tend` phase (due to one of the two termination conditions above being met), all collateral goes to the winning bidder, and if in the end `bid` < `tab` then we say the auction has *finished in deficit*, and the deficit will need to be covered by an MKR-diluting debt auction.

The auction goes from the `tend` phase to the `dent` phase when it receives a `bid` equal to `tab`. In the `dent` phase, the auction receives bids in the form of decreasing amounts of collateral (denoted `lot`), with `lot` < `ink`. When a lower `lot` is offered, `tab` dai is transferred from the bidder to refund the previous

bidder. When the auction terminates in the `dent` phase, the bidder with the lowest `lot` receives `lot` collateral, and the CDP owner has `ink − lot` collateral returned to them. When an auction finishes in the `dent` phase, we say that the auction has *finished in adequacy*, so no debt auction will be needed.

There are two key features of collateral auctions that create the possibility for the auction grinding attack: one concerning auctions that finish in deficit, and one concerning auctions that finish in surplus.

An auction that finishes in deficit will trigger an MKR dilution to cover the difference between the debt owed by the liquidated CDP and the dai raised in the collateral auction. Assuming the existence of a true value for the collateral, either the winner of the collateral auction has managed to buy collateral at a discount to the fair price, or at the time of liquidation the CDP's debt must have exceeded the value of its collateral (negative equity), or some combination of the two[1]. Hence, viewing this event as a "value flow", we see that the value of MKR capital flows to the auction winner (whose collateral purchase price is effectively subsidised), or the CDP debtor (whose excess debt over collateral value is forgiven), or both. The auction grinding attack will seek to exploit this value flow in the case that the CDP owner and the winning auction bidder are the same person.

An auction that finishes in surplus will have its excess collateral returned to the owner of the liquidated CDP. This means that (in the absence of a liquidation penalty) the marginal cost of a CDP owner placing a bid on the collateral auction of their own CDP is zero. The attack will exploit this fact in order to ensure that they can always win the auction.

3   The Attack

For the purposes of this section, we will assume there is no liquidation penalty. We will also neglect any risks associated with collateral price volatility during the course of the auction: the reason for this is that the attacker can choose to attempt this attack during a period when collateral price volatility is low. Moreover, they are free to hedge their exposure to the collateral externally to reduce their risk. It is also important that the attacker has extra dai available to them before they start the attack.

I now describe the attack: first the attacker must choose the collateral type that they wish to use for the attack. As we shall see, they may select the collateral type where they expect the least auction participation, or simply try the attack on all collateral types repeatedly. Let `mat` be the liquidation ratio of the chosen collateral type, and we will call *gems* to the collateral tokens of this collateral type. Let `tab` and `ink` be the amounts of dai debt and collateral gems, respectively, of the CDP upon liquidation.

Next, the attacker creates a CDP of this collateral type, deposits all of their gems, and borrows the maximum amount of dai from this CDP, hoping to get their position liquidated immediately. If their position does not become unsafe on the next collateral price feed update, they only have to draw more dai if possible, and wait until the next downward tick in the feed price. Once their CDP becomes unsafe, they initiate its liquidation, so the collateral auction will begin.

The attacker's strategy is simple: their first goal is to win their own collateral's liquidation auction, at the lowest price possible, with the auction finishing in deficit. Thus, they will place bids while the auction is in the `tend` phase, hoping to win the auction[2]. If the attacker is successful, winning the auction in the `tend` phase paying `bid` dai, we will have reached outcome $W(\texttt{bid})$. If someone thwarts this plan by outbidding them until the auction is in the `dent` phase, then the attacker will abandon that plan and simply place another, final bid at the implied price corresponding to the attacker's view of the correct collateral value. At this point, one of two things will happen: either no one will outbid the attacker and they will win the auction, which we will call outcome N, or someone will outbid the attacker and end up buying (some of) the collateral at a premium to the attacker's notion of the fair value, which we will denote $Y(\texttt{lot})$ where `lot` is the amount of gems bought by the winning bidder. In any case, the attacker guarantees that the auction will finish in one of the states $W(\texttt{bid})$, N, or $Y(\texttt{lot})$.

If the auction finishes in state $W(\texttt{bid})$, the attacker will have bought back their own collateral with less dai than they borrowed against it, ending with a profit.

If the auction finishes in state N, the attacker will have spent the same amount of dai that they just borrowed, and received in return the same amount of collateral that they put in (part of it going to them as the CDP owner, and part as the winner of the auction), so has made neither a profit nor a loss.

---

[1]There is also a possibility that the CDP has positive equity at the time of liquidation, as judged by the fair market value of the collateral, but due to a decline in the price of the collateral over the course of the auction, it could still finish in deficit. This additional "basis risk" that MKR capital is exposed to is not considered here.

[2]The exact strategy (choice of timing, bid increment, etc.) by which the bidder will attempt to win the auction in the `tend` phase is up to the attacker.
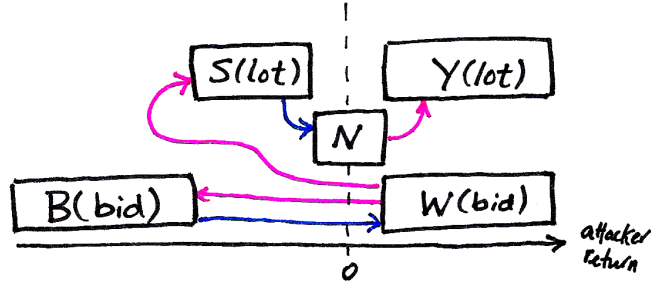
Figure 1: Graph of attacker's strategy, where blue arrows depict moves that the attacker will make, and pink arrows depict moves that might be made by other auction participants. The horizontal position of a game state representing the total return for the attacker in the event that the auction terminates in that state.

If the auction finishes in state $Y(\texttt{lot})$, the attacker will have effectively traded gems for dai with the winning bidder at a premium to their notion of the fair price, thus making a profit.

We enumerate all relevant states of the auction, and display the game states as a graph in Figure 1:

$W(\texttt{bid})$ The auction is in the `tend` phase and the attacker is the top bidder.

$B(\texttt{bid})$ The auction is in the `tend` phase and someone else is the top bidder.

N The auction is in the `dent` phase and the attacker is the top bidder, having bid at most their fair price for the collateral.

$S(\texttt{lot})$ The auction is in the `dent` phase and someone else is the top bidder, having bid less than the attacker's fair price for the collateral.

$Y(\texttt{lot})$ The auction is in the `dent` phase and someone else is the top bidder, having bid more than the attacker's fair price for the collateral.

We also compute the attacker's return in case the auction finishes in each state, where return is calculated as the difference in the dai value between the attacker's starting and ending portfolio, assuming the attacker values one gem as `wut` dai, and ignoring any gas costs, financing costs, and opportunity costs.

termination state	auction winner	attacker return	
$W(\texttt{bid})$	attacker	`tab − bid`	(> 0)
$B(\texttt{bid})$	other	`tab − ink · wut`	(< 0)
N	attacker	0	
$S(\texttt{lot})$	other	`tab − lot · wut`	(< 0)
$Y(\texttt{lot})$	other	`tab − lot · wut`	(> 0)

Table 1: Payoff table for auction grinding strategy with no liquidation penalty.

As we have seen, the attacker can force the auction to finish in one of the three scenarios where their return is non-negative. Thus, provided one of the two scenarios where the return is positive could happen with non-negligible probability, the attacker will expect a positive expected return from following this strategy. In particular, the attacker can increase the chance of profiting through outcome $W(\texttt{bid})$ if they have sufficient capital to initiate a large liquidation (or many simultaneous liquidations) that many other market participants will be priced out of. Moreover, if the attacker "griefs" the system by following this strategy repeatedly and winning every auction, others may be discouraged from participating in future auctions (in game terms, the attacker is always able to force a draw, so competing bidders might choose not to play).

4 The Liquidation Penalty

A natural approach to mitigating this attack is to add some friction to the liquidation process, in addition to the gas costs which are already present but may be too insignificant relative to the capital at play. I propose using the *liquidation penalty* to this end. In short, a liquidation penalty is implemented by increasing the outstanding debt on a CDP by some factor `axe` just as it goes to liquidation, so that a CDP that had `tab` outstanding debt will be treated as if it had $\texttt{axe} \cdot \texttt{tab}$ of debt for the purposes of liquidation. `axe` set to 1 is equivalent to no liquidation penalty. The effect of this is that the CDP owner will get less of their collateral back at the end of a liquidation, since the auction would have been covering a greater debt: effectively, they have had an additional $(\texttt{axe} - 1) \cdot tab$ dai debited from their balance[3].

We now recompute the payoff matrix on the auction grinding strategy when a liquidation penalty of `axe` is used:

termination state	attacker return	
$W(\texttt{bid})$	$\texttt{tab} - \texttt{bid}$	(> 0)
$B(\texttt{bid})$	$\texttt{tab} - \texttt{ink} \cdot \texttt{wut}$	(< 0)
N	$-(\texttt{axe} - 1) \cdot \texttt{tab}$	(< 0)
$S(\texttt{lot})$	$\texttt{tab} - \texttt{lot} \cdot \texttt{wut}$	(< 0)
$Y(\texttt{lot})$	$\texttt{tab} - \texttt{lot} \cdot \texttt{wut}$	(> 0)

Table 2: Payoff table for auction grinding strategy with liquidation penalty set to `axe`.

The crucial difference is that now the attacker's strategy cannot guarantee that the attacker will not suffer losses from attempting the attack. Indeed, the previously neutral state N, where the attacker would have forced the game to go if they were unable to make a profit, now represents a loss for the attacker, and the attack is no longer risk-free. To discourage the attacker, it will be necessary to make their expected return negative by setting `axe` sufficiently high, which requires some model of the probability of each auction outcome. We model this by taking a random variable $L \in [0, \infty)$ for the implied price of the highest non-attacker bid, assuming this to be independent of the attacker's presence and behaviour: the distribution of this random variable should capture the attacker's expectation that they will be challenged by another bidder in the auction. Integrating over probabilities $\mathbb{P}(L = l)$ and splitting the integral over the three possible termination states of the auctions gives the attacker's expected return:

$$\mathbb{E} = \int_{l=0}^{\frac{\texttt{tab}}{\texttt{ink}}} (\texttt{tab} - l \cdot \texttt{ink}) \cdot \mathbb{P}(L = l) \mathrm{d}l - \int_{l=\frac{\texttt{tab}}{\texttt{ink}}}^{\texttt{wut}} (\texttt{axe} - 1) \cdot \texttt{tab} \cdot \mathbb{P}(L = l) \mathrm{d}l + \int_{l=\texttt{wut}}^{\infty} (1 - \frac{\texttt{axe} \cdot \texttt{wut}}{l}) \cdot \texttt{tab} \cdot \mathbb{P}(L = l) \mathrm{d}l$$

whenever $\texttt{axe} < \frac{\texttt{wut} \cdot \texttt{lot}}{\texttt{tab}}$, and

$$\mathbb{E} = \int_{l=0}^{\texttt{wut}} (\texttt{tab} - l \cdot \texttt{ink}) \cdot \mathbb{P}(L = l) \mathrm{d}l + \int_{l=\texttt{wut}}^{\frac{\texttt{axe} \cdot \texttt{tab}}{\texttt{lot}}} (\texttt{tab} - \texttt{ink} \cdot \texttt{wut}) \cdot \mathbb{P}(L = l) \mathrm{d}l + \int_{l=\frac{\texttt{axe} \cdot \texttt{tab}}{\texttt{lot}}}^{\infty} (1 - \frac{\texttt{axe} \cdot \texttt{wut}}{l}) \cdot \texttt{tab} \cdot \mathbb{P}(L = l) \mathrm{d}l$$

when $\texttt{axe} >= \frac{\texttt{wut} \cdot \texttt{lot}}{\texttt{tab}}$.

Thus, assuming a model of non-attacker auction participation in the form of a probability distribution for L, we can determine the minimum `axe` for which the attacker's expected return is negative. Initially, we can use a heuristic to estimate this probability distribution, and after the auctions have been running for some time we can use empirical data to adjust our model, repeat the computation, and determine if `axe` should be increased or decreased.

As an example, we can take a generalised student's t-distribution for L, with mean $\texttt{r} \cdot \texttt{wut}$ (where r is some auction discount constant), scaling parameter $\frac{1}{20}\texttt{wut}$, and one degree of freedom. An example of the probability density function, along with the attacker's profit, are shown in Figure 2. By numerically integrating the above expressions for the attacker's expected return with this distribution, taking $\texttt{wut} = 500$, $r = 0.95$, $\texttt{tab} = 10000$, $\texttt{ink} = 30$, we find that in order to make the expected return negative we must set $\texttt{axe} > 1.0835$ (i.e. we must apply a liquidation penalty of at least 8.35% the value of the outstanding debt).

The above heuristic assumes that L is independent of the attacker's behaviour, and in particular that the attacker is not able to predict L ahead of time. This assumption is flawed, since a motivated attacker

---

[3]There is an alternative way of implementing the liquidation penalty, by slashing a fraction of the collateral that is returned to the CDP owner at the end. It is straightforward to show that this method is completely equivalent to the one described above, for all parties involved.
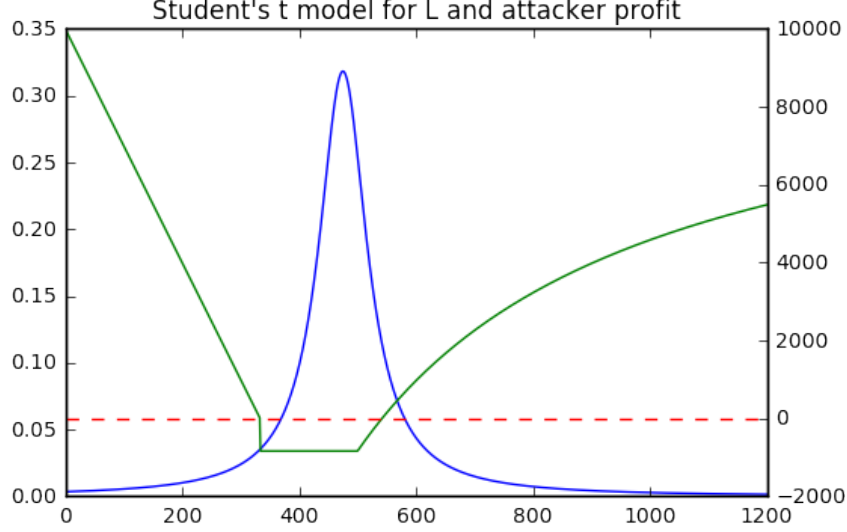
Figure 2: The probability density function of the t-distribution model for L, with `wut` $= 500$ and $r = 0.95$ (corresponding to a mean auction price discount of 5%). Also plotted is the attacker's profit as a function of L, where we have set `tab` $= 10000$, `ink` $= 30$, and `axe` $= 1.0835$

is likely to strike during a regime where liquidity is stretched, by observing market conditions before initiating the liquidation. Moreover, the attacker can influence liquidity conditions themselves, either by manipulating the market in some way, or simply by attempting this attack with a very large amount of debt. Therefore, the heuristic above should be used very conservatively, choosing a more pessimistic (worst-case) model for L if possible.

5 Conclusion

In the discussion above, I have explained the necessity of the liquidation penalty, without which the collateral auctions are vulnerable to an unpleasant economic attack. With an appropriately chosen liquidation penalty, determined by estimating the expected collateral auction participation (or based on existing data), the attacker will no longer expect a profit from the attack, and will be deterred from attempting it in normal conditions. There remains a risk that this attack could be profitably executed by a well-capitalised attacker who times their liquidation to occur during a moment of extreme market stress, where for some reason auction participation is much lower than expected. This possibility should be kept in mind as a potential black swan risk, and will be the subject of future research.