Buidler Governance Equations and Derivations

Benjamin Wang

January 2020

Abstract

A derivation of the criteria to be met for a governance decision to be wealth creating using the previously accepted and current proposal trading data for a two-sided dutch auction governance design. The analysis assumes both rational and irrational attackers.

1 Motivation and setup

For a governance mechanism to be sustainable, decisions must be on average wealth creating for the system that is being governed. For a tokenised good, that means the token must increase in value i.e. the price at the point of the current proposal (n) must be greater than the price of the previous proposal $(n-1)$. In this case we state the condition:

$$\text{gov\_price}_n > \text{gov\_price}_{n-1} \tag{1}$$

$$\text{gov\_price}_n[\text{gov}_{n-1}] > 1.0 \tag{2}$$

where $\text{gov\_price}_n[\text{gov}_{n-1}]$ is the market price of the governance tokens (gov) if the current proposal (n) is accepted, in terms of the market price of gov just after the previously accepted proposal $n-1$ i.e. the amount of gov_{n-1} tokens one could trade in exchange for a gov_n token and vice versa.

The first obstacle we must pass is the impossibility of traders ever exchanging gov_n for gov_{n-1} since they never exist at the same time. However, we can calculate these prices a different way by finding the price in terms of dai. The gov_n dai-price can be found from the *current* proposal auctions and the gov_{n-1} dai-price can be found from the *previous* proposal auctions.

$$\text{gov\_price}_n[\text{gov}_{n-1}] = \text{gov\_p}_{n,\text{dai}} \times \text{dai\_p}_{n-1,\text{gov}} \tag{3}$$

$$= \frac{V_{n,\text{dai}}}{V_{n,\text{gov}}} \times \frac{V_{n-1,\text{gov}}}{V_{n-1,\text{dai}}} \tag{4}$$

where $\text{gov\_p}_{n,\text{dai}}$ is the price of the governance tokens in terms of dai at the time of the current proposal n; $\text{dai\_p}_{n-1,\text{gov}}$ is the price of dai in terms

governance tokens at the time of previous proposal $n-1$; and V is referring to a trade volume traded at the true market price.

This then leaves us with the problem of finding exact prices in terms of dai during proposals. Since, it is not possible to find exact true market prices and it is only necessary to guarantee that $\text{gov\_price}_n[\text{gov}_{n-1}] > 1.0$ for the proposal to be wealth creating, we need only calculate the *minimum* market prices.

2 Proposal manipulation from rational and irrational attackers

No assumptions about attackers can be made since attackers may be irrational. However, since the governance mechanism is essentially the trading of tokens and an inflationary payment to the proposal beneficiary, as long as it is necessary for the attacker to make unprofitable trades in order to manipulate the mechanism, there will be a point as which the attacker effectively pays for the proposal acceptance payment, and any further price manipulation is simply an exchange of value from the attacker to the other token traders. To do this, **the governance mechanism accepts any proposal where the attacker must spend more than the proposal amount in order to manipulate the vote.** Therefore, the following condition must hold:

$$\text{profit[dai]} + A_n > 0 \tag{5}$$

where profit[dai] is the attacker's profit (expected to be negative) and A_n is the proposal amount awarded to the beneficiary if the proposal is accepted by the governance mechanism.

Equation 5 represents the point at which the attacker has effectively paid for the proposal. Any trading the attacker makes beyond this point is arbitrary from the mechanism's perspective and is effectively the attacker making unprofitable trades with the governance mechanism. Therefore, we only need to calculate the minimum market price for $\text{gov\_price}_n[\text{gov}_{n-1}]$ when $\text{profit[dai]} + A_n > 0$ rather than the minimum market price in any circumstances.

For the current proposal (n), the attacker can only manipulate the price of the *buy* auction higher rather than the *sell* auction since $\text{gov\_p}_{n,\text{dai}}$ increases over time. Therefore, in such a trade they receive gov and send dai with a negative expected profit relative to the true market price:

$$\text{profit[dai]} = V^{\text{buy}}_{n,\text{gov}} \times \text{gov\_p}_{n,\text{dai}} - V^{\text{buy}}_{n,\text{dai}} \tag{6}$$

$$\text{profit[dai]} + A_n > 0 \tag{7}$$

$$\text{gov\_p}_{n,\text{dai}} > \frac{(V^{\text{buy}}_{n,\text{dai}} - A_n)}{V^{\text{buy}}_{n,\text{gov}}} \tag{8}$$

Likewise, for the previous proposal ($n-1$), the attacker will seek to increase

the price of $\text{dai\_p}_{n-1,\text{gov}}$. Therefore, they will use the sell side of the auction since the price increases over time and they can manipulate it down.

$$\text{profit[dai]} = V^{\text{sell}}_{n-1,\text{dai}} - V^{\text{sell}}_{n-1,\text{gov}} \times \text{gov\_p}_{n-1,\text{dai}} \tag{9}$$

$$\text{profit[dai]} + A_n > 0 \tag{10}$$

$$\text{dai\_p}_{n-1,\text{gov}} = \frac{1}{\text{gov\_p}_{n-1,\text{dai}}} > \frac{V^{\text{sell}}_{n-1,\text{gov}}}{V^{\text{sell}}_{n-1,\text{dai}} + A_n} \tag{11}$$

3 Derivation

Substitute equations 8 and 11 into 3 to yield:

$$\text{P}_{n,\min} = \frac{(V^{\text{buy}}_{n,\ \text{dai}} - A_{n,a})}{V^{\text{buy}}_{n,\ \text{gov}}} \times \frac{V^{\text{sell}}_{n-1,\ \text{gov}}}{(A_{n,b} + V^{\text{sell}}_{n-1,\ \text{dai}})} \tag{12}$$

where $A_n = A_{n,a} + A_{n,b}$ since the attacker can only spend up to the value of A_n and not beyond it i.e. they would face the decision of how to split this across the previous $(n-1)$ and present (n) proposals. If we consider how $P_{n,\min}$ changes with respect to how the attacker splits A_n...

$$\frac{\partial P_{n,\min}}{\partial A_{n,a}} = -\frac{V^{\text{sell}}_{n-1,\text{gov}}}{V^{\text{buy}}_{n,\text{gov}}} \times \frac{A_n - V^{\text{buy}}_{n,\text{dai}} + V^{\text{sell}}_{n-1,\text{dai}}}{(A_n - A_{n,a} + V^{\text{sell}}_{n-1,\text{dai}})^2} \tag{13}$$

$$\frac{\partial P_{n,\min}}{\partial A_{n,b}} = \frac{V^{\text{sell}}_{n-1,\text{gov}}}{V^{\text{buy}}_{n,\text{gov}}} \times \frac{A_n - V^{\text{buy}}_{n,\text{dai}} + V^{\text{sell}}_{n-1,\text{dai}}}{(A_{n,b} + V^{\text{sell}}_{n-1,\text{dai}})^2} \tag{14}$$

...it is optimum for the attacker to put all funds either in $A_{n,a}$ or $A_{n,b}$ depending on which auction has the lowest trading volume in terms of *dai* such that:

$$V^{\text{buy}}_{n,\text{dai}} < V^{\text{sell}}_{n-1,\text{dai}} + A_n \qquad \Rightarrow P_{n,\min} = \frac{V^{\text{sell}}_{n-1,\text{gov}}}{V^{\text{buy}}_{n,\text{gov}}} \times \frac{(V^{\text{buy}}_{n,\text{dai}} - A_n)}{V^{\text{sell}}_{n-1,\text{dai}}} \tag{15}$$

$$V^{\text{buy}}_{n,\text{dai}} > V^{\text{sell}}_{n-1,\text{dai}} + A_n \qquad \Rightarrow P_{n,\min} = \frac{V^{\text{sell}}_{n-1,\text{gov}}}{V^{\text{buy}}_{n,\text{gov}}} \times \frac{V^{\text{buy}}_{n,\text{dai}}}{(A_n + V^{\text{sell}}_{n-1,\text{dai}})} \tag{16}$$

Or:

$$P_{n,\min} = \frac{V^{\text{sell}}_{n-1,\text{gov}}}{V^{\text{buy}}_{n,\text{gov}}} \times \min\left(\frac{V^{\text{buy}}_{n,\text{dai}}}{(A_n + V^{\text{sell}}_{n-1,\text{dai}})}, \frac{(V^{\text{buy}}_{n,\text{dai}} - A_n)}{V^{\text{sell}}_{n-1,\text{dai}}}\right) \tag{17}$$

A nice way to think about this is that the attacker is choosing the weakest side to manipulate.