

# Efficient Order-Preserving Redistribution of Troves

November 2020

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Troves and Liquidations</b>	<b>2</b>
<b>3</b>	<b>Trove Ordering</b>	<b>2</b>
<b>4</b>	<b>Efficient Reward Distribution</b>	<b>3</b>
4.1	Scalable Reward Distribution with Fixed Stakes . . . . .	3
4.2	Corrected Stake Approach for Variable Stakes . . . . .	4
<b>5</b>	<b>System Order Evolution</b>	<b>4</b>
<b>6</b>	<b>Outline of the Proof</b>	<b>5</b>
<b>7</b>	<b>Corrected Stake Approach Preserves Equality</b>	<b>6</b>
<b>8</b>	<b>Corrected Stake Approach Preserves Order</b>	<b>12</b>
<b>9</b>	<b>Appendix</b>	<b>16</b>

## 1 Introduction

The Liquity protocol [1] issues a USD-pegged stablecoin LUSD that is redeemable at face value against ETH: any owner of LUSD can exchange their stablecoins for equivalent value in the underlying collateral at any time. The ETH paid to the redeemer is taken from the borrowers' collateralized debt positions ("troves") in ascending order of collateral ratio. In other words, the system uses the redeemed LUSD to repay the debt on the riskiest trove with the currently lowest individual collateral ratio (ICR), and transfers a corresponding amount of ETH from the trove to the redeemer. If the redeemed LUSD is larger than the debt on the riskiest trove, the system proceeds with the second riskiest trove, and so on.

To allow for efficient redemptions despite Ethereum's gas constraints, the system keeps troves ordered by ICR, so that it can iterate over the linked list starting from the bottom. It is not feasible to sort the list after every operation.

Troves with an insufficient ICR are subject to liquidation. Given that Liquity's fallback liquidation mechanism [1] redistributes the collateral and debt of a liquidated trove between all remaining active troves, it must be ensured that redistributions do not break trove ordering.

Redistribution in proportion to the collateral size of active troves maintains ordering, as can be easily shown (see 9 Appendix). However, in practice, it is clear that redistributing in a "push" based manner - iterating over all troves and updating their collateral and debt - does not scale, and has computational complexity of  $O(n)$ , where  $n$  is the number of troves.

Previous work by Batog et al [2] derived a scalable  $O(1)$  method to assign proportional rewards to a large number of recipients, as long as the basis for their rewards (“stakes”) do not change over time. The method is “pull” based: instead of adjusting all recipient positions upon every reward event, the update is deferred to the moment at which an owner changes their position. In the described approach rewards are stored separately from the initial stakes, and do not compound. That is to say, past accumulated rewards are not included in future reward calculations.

It turns out that this approach thus cannot be applied to Liquity as is. As the system undergoes reward events, a given trove’s ratio of initial collateral to its total collateral shrinks. Rewards are based on a smaller and smaller share of the total collateral. This is fine, as long as all active troves have experienced all reward events - in this case, ordering is maintained since all troves are affected by the same change.

However, a problem arises when a new trove is created after active troves have received reward shares. Such “fresh” troves (with no accumulated rewards) would thus gain an advantage in re-distributions over older troves whose stakes may be smaller than their actual collateral due to the liquidations that have taken place in the meantime. In other words, a “fresh” trove that has experienced fewer rewards than the earlier troves would receive a disproportionate share of subsequent rewards relative to its collateral. Though, a trove’s collateral ratio must always be based on its entire collateral, which does include accumulated rewards.

This discrepancy means that the reward distribution scheme described in [2] can break the ordering of troves by collateral ratio. To remedy this, we modify the original approach by introducing a “corrected stake”, to ensure fresh troves do not receive disproportionate rewards. We then show that this corrected stake preserves trove ordering.

## 2 Troves and Liquidations

Troves are collateralized debt positions held by individual borrowers, defined by their amount of debt  $d$  (in LUSD) and collateral  $c$  (in ETH).

Let  $\gamma_i$  denote the individual collateral ratio (ICR) of a trove  $i$ , i.e. the ratio of its collateral to its debt:

$$\gamma_i = \frac{c_i}{d_i} \quad (1)$$

If  $\gamma_i$  falls below a minimum threshold  $\delta$ , the trove is subject to liquidation. As long as there are sufficient LUSD tokens in the Stability Pool, the system can use them to repay the liquidated debt.

If the Stability Pool is empty, the trove’s collateral and debt are redistributed to all active troves in the system as part of the liquidation process (a trove is called *active* as long as it has not been liquidated, or closed by their owner or by a redemption). Every existing borrower with an active trove thus receives a share of both the collateral and the debt of the liquidated trove.

Collateral and debt shares from liquidations are proportional to the *entire* collateral of the recipient troves, i.e. taking into account accumulated “rewards” from prior liquidations. Thus, in the event of a redistribution of a trove  $k$ , an active trove  $i$  receives the following collateral and debt shares  $x_i, y_i$ :

$$(x_i, y_i) = \left( \frac{c_i}{C} \cdot c_k, \frac{c_i}{C} \cdot d_k \right) \quad (2)$$

where  $C = \sum c_j$  is the total collateral in the system.

The rewards compound across multiple redistribution events.

## 3 Trove Ordering

To ensure that the troves can be reliably accessed using a linked list, it is crucial to maintain the ordering of the troves (by ICR) throughout all redistribution events  $E_k$ .

The ordering is maintained if  $\forall E_k, i, j : (\gamma_i > \gamma_j \implies \gamma'_i > \gamma'_j)$ , where  $\gamma'_i$  and  $\gamma'_j$  is the ICR of troves  $i$  and  $j$  after  $E_k$ .

It is easy to prove that a redistribution in proportion to the collateral of the recipient trove as described by equation (2) troves maintains ordering. See 9 Appendix.

## 4 Efficient Reward Distribution

### 4.1 Scalable Reward Distribution with Fixed Stakes

A naive “push” based implementation of the redistribution (“strawman approach”), where rewards don’t compound, would iterate over all participants and compute the debt and collateral shares for each recipient  $i$  separately whenever the system distributes such rewards. Thus, at a reward event  $t$ , every recipient would receive the following reward share:

$$r_{i,t} = s_i \cdot \frac{R_t}{S_t} \quad (3)$$

where  $R_t$  is the reward distributed at  $t$ ,  $r_{i,t}$  the reward share of recipient  $i$ ,  $s_i$  the stake of recipient  $i$ , and  $S_t$  the sum of the stakes of all recipients, i.e.  $\sum s_j$ .

Note that  $s_i$  does not depend on  $t$ , and is thus fixed throughout multiple reward events. The sum of  $s_i$  may vary over time because the set of them may change, stakes entering or leaving the set, but each amount  $s_i$  is fixed while it’s in the set.

Based on this prerequisite, [2] suggests a scalable  $O(1)$  method of distributing such rewards by deferring the reward computation. The total reward share of  $i$  from all reward events that occur between time  $t_1$  and  $t_2$  can be written as a sum of its reward shares with the (fixed) stake  $s_i$  being factored out:

$$\sum_{t=t_1+1}^{t_2} r_{i,t} = s_i \cdot \sum_{t=t_1+1}^{t_2} \frac{R_t}{S_t} \quad (4)$$

Let  $Q_t$  denote the sum of all rewards per total staked amount up to instant  $t$ :

$$Q_t = \sum_{k=0}^t \frac{R_k}{S_k} \quad (5)$$

Assuming stake  $s_i$  is deposited at moment  $t_1$  and then withdrawn at moment  $t_2 > t_1$ , we can use the sum  $Q_t$  to compute the total reward share for participant  $i$  since

$$r_i = s_i \cdot \sum_{t=t_1+1}^{t_2} \frac{R_t}{S_t} \quad (6)$$

can be written as

$$r_i = s_i \cdot (Q_{t_2} - Q_{t_1}) \quad (7)$$

As  $Q_t$  is monotonic, we can simply track the current (latest) value of  $Q$  as a running sum, and snapshot it whenever we expect it to be required for a later computation, i.e. whenever a participant changes their stake.

To compute the total (accumulated) reward for participant  $i$ , we can then use following formula:

$$r_i = s_i \cdot (Q - Q_{t_1}) \quad (8)$$

## 4.2 Corrected Stake Approach for Variable Stakes

In Liquity, collateral and debt shares from liquidations are proportional to the entire collateral of the recipient troves. The redistribution must cope with the fact that some fraction of a trove’s entire collateral is the accumulated reward from prior liquidations, and this fraction varies across troves.

The “strawman” approach in 4.1, with rewards proportional to the initial stake, neglects this: it over-rewards fresh troves, and under-rewards older troves.

We introduce a corrected stake  $s_i$  to restore proportional reward distribution:

$$s_i = \begin{cases} c_i & \text{for } C_\emptyset = 0 \\ c_i \cdot \frac{S_\emptyset}{C_\emptyset} & \text{for } C_\emptyset > 0 \end{cases} \quad (9)$$

The corrected stake  $s_i$  is chosen such that it earns rewards from liquidations equivalent to a trove that would have accumulated  $c_i$  total collateral by the time the fresh trove  $i$  was created.

$S_\emptyset$  and  $C_\emptyset$  are the respective snapshots of the total stakes and total collateral in the system, taken immediately after the last liquidation event. Note that with this terminology, the total collateral includes the total stakes, and therefore  $C_\emptyset \geq S_\emptyset$ .

By extending the original formula from [2], we can thus express the collateral and debt share received by a trove by:

$$r_i = \begin{cases} c_i \cdot (Q - Q_{t_1}) & \text{for } C_\emptyset = 0 \\ c_i \cdot \frac{S_\emptyset}{C_\emptyset} \cdot (Q - Q_{t_1}) & \text{for } C_\emptyset > 0 \end{cases} \quad (10)$$

Note that  $r_i$  can stand for the collateral or the debt share of a recipient trove since both of them can be represented as “rewards” through  $R_t$ .

The intuition behind the choice of corrected stake is that the corrected stake effectively models the fresh trove’s collateral  $c_i$  as a total collateral, which includes ‘virtual’ accumulated rewards. The corrected stake earns rewards for the trove as if the trove had been in the system from the beginning - thus maintaining proportional reward growth.

## 5 System Order Evolution

As mentioned above, we aim to prove that the corrected stake approach leaves the ordering of the troves by collateral ratio unchanged throughout all liquidations, regardless of any borrowers that change their troves’ collateral between liquidation events.

Given that Liquity’s fallback liquidation mechanism [1] redistributes the collateral and debt of a liquidated trove between all remaining active troves, it must be ensured that redistributions do not break trove ordering.

To break up the proof, we introduce the notion of *system order*.

**Definition 5.1** (System Order). *A system of troves has an order,  $n$ , and we label it  $\Gamma_n$ . When the first trove is created, the system order equals 1.*

*The order of a system remains constant throughout the following event sequence:*

- 1 or more new troves are created
- 1 or more troves are subsequently liquidated

**Definition 5.2** (System order evolution). *The first trove creation event after a series of liquidations triggers a system evolution, and the system order increases by 1.*

It can be represented graphically in the following way, where circles correspond to trove creations and squares to liquidation events:



We capture the system order increase from order  $n$  to order  $n + 1$  in a system evolution function:

$$f(\Gamma_n) = \Gamma_{n+1} \quad (11)$$

Let  $\Gamma_1$  define a system of troves with past liquidations, in which all active troves have received reward shares from all past liquidations.  $\Gamma_1$  is a first-order system, and contains only stakes of first-order troves. Each first-order stake  $s_i$  is equal to its collateral  $c_i$ , and  $S = \sum s_i = \sum c_i$ .

Let  $\Gamma_2$  define an evolution of  $\Gamma_1$ , i.e.  $\Gamma_2 = f(\Gamma_1)$ .  $\Gamma_2$  is a system with past liquidations, with  $S = \sum s_i + \sum s_j$ , where  $s_j$  is the stake of newly added troves  $j$ .  $\Gamma_2$  is a second-order system, containing **both** first-order stakes  $s_i = c_i$  which have experienced all liquidations, **and** second-order stakes  $s_j$  which have only experienced the liquidations after their creation.

In general,  $\Gamma_n$  is a system with  $n$  sequential pairs, each consisting of a trove creation period and a liquidation period. Troves created in a given trove creation period  $t$  have experienced only those liquidations that occurred in liquidation period  $t$  or greater.

**Proposition 5.1.** *At first-order, stake equals initial collateral.*

*Proof.* For first-order systems, all troves were added before any liquidation events occurred. The snapshot  $C_\emptyset$  is equal to 0. Therefore:

$$s_i = c_i \quad (12)$$

for all  $s_i, c_i$  in an  $\Gamma_1$  system. □

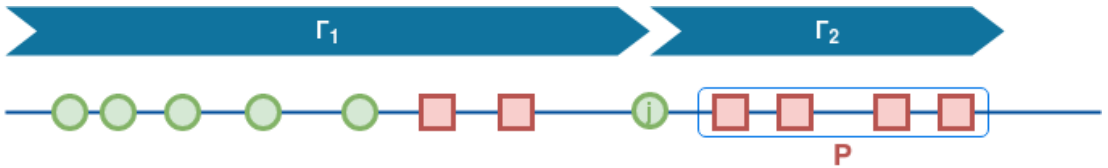
## 6 Outline of the Proof

We first prove that ICR equality is maintained with rewards proportional to corrected stakes - starting with the simplest case, and progressively generalizing, and finally we prove that order is maintained too.

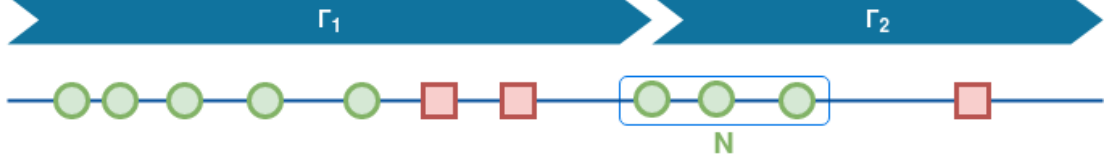
- Lemma 7.1. We consider a system transition  $\Gamma_1 \rightarrow \Gamma_2$  triggered by the creation of a trove  $j$ , followed by a liquidation of a trove  $k$ . For any trove  $i$  with  $\gamma_i = \gamma_j$  in  $\Gamma_1$ , the corrected stake approach maintains  $\gamma_i = \gamma_j$  in  $\Gamma_2$ .



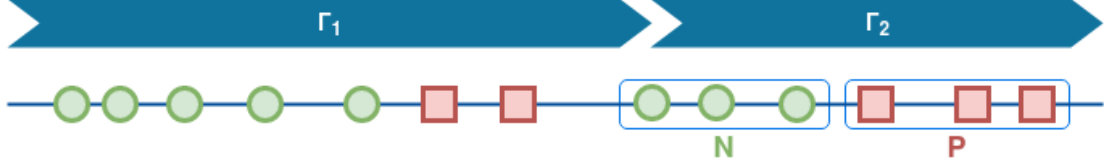
- Lemma 7.2. We consider a system transition  $\Gamma_1 \rightarrow \Gamma_2$  triggered by the creation of a trove  $j$ , followed by a set of liquidations  $P$ , such that  $|P| > 1$  and  $j \notin P$ . For any trove  $i$  with  $\gamma_i = \gamma_j$  in  $\Gamma_1$ , the corrected stake approach maintains  $\gamma_i = \gamma_j$  in  $\Gamma_2$ .



- Lemma 7.3. We consider a system transition  $\Gamma_1 \rightarrow \Gamma_2$  triggered by the creation of a trove, followed by some more creations, up to a set  $N$ , such that  $|N| > 1$ , and then by a single liquidation. For any trove  $i$  in  $\Gamma_1$  and any trove  $j$  in  $N$  with  $\gamma_i = \gamma_j$ , the corrected stake approach maintains  $\gamma_i = \gamma_j$  in  $\Gamma_2$ .



- Theorem 7.4. We consider a system transition  $\Gamma_1 \rightarrow \Gamma_2$  triggered by the creation of a trove, followed by some more creations, up to a set  $N$ , and then by a set of liquidations  $P$ , such that  $|N|, |P| > 0$ . For any trove  $i$  in  $\Gamma_1$  and any trove  $j \in N, j \notin P$  with  $\gamma_i = \gamma_j$ , the corrected stake approach maintains  $\gamma_i = \gamma_j$  in  $\Gamma_2$ .  
In other words, in a second-order system with  $M$  previous liquidations, and  $N$  second-order troves added after the last liquidation, ICR equality between any first-order trove and corresponding second-order trove with the same ICR holds across  $P$  subsequent liquidation events.

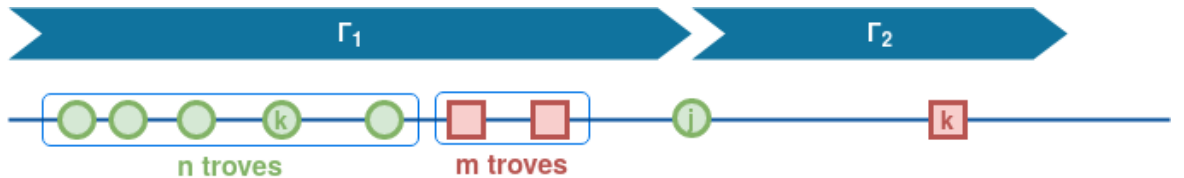


- Lemma 7.5. For every  $2^{nd}$  order system  $\Gamma_2$  there exists an equivalent first-order system  $\Gamma_1$  that contains only first-order stakes which have experienced all liquidations.
- Proposition 7.6. For every  $n^{th}$  order system  $\Gamma_n$  there exists an equivalent first-order system  $\Gamma_1$  that contains only first-order stakes which have experienced all liquidations.
- Corollary 7.6.1. In an  $n^{th}$  order system with  $M$  previous liquidations, and  $N$  second-order troves added after the last liquidation, ICR equality between an  $(n-1)^{th}$  order trove and  $n^{th}$  order trove holds across  $P$  liquidation events.
- Theorem 8.1. For every system  $\Gamma_n$  containing troves  $i$  and  $j$  with  $\gamma_i > \gamma_j$  that transitions to  $\Gamma_{n+1}$ , the corrected stake approach maintains  $\gamma_i > \gamma_j$ .

## 7 Corrected Stake Approach Preserves Equality

**Lemma 7.1.** *We consider a system transition  $\Gamma_1 \rightarrow \Gamma_2$  triggered by the creation of a trove  $j$ , followed by a liquidation of a trove  $k$ . For any trove  $i$  with  $\gamma_i = \gamma_j$  in  $\Gamma_1$ , the corrected stake approach maintains  $\gamma_i = \gamma_j$  in  $\Gamma_2$ .*

*Proof.* A first-order system of  $n+m$  troves undergoes  $m$  trove liquidations, before evolving to second-order.



Consider the  $m$  past liquidations from the point of view of an active first-order trove  $i$ . As per (9), the stake of trove  $i$  is  $s_i = c_i$ .

Let's define the reward from liquidating trove  $k$  received by trove  $i$  as the pair  $R_i^k = (x_i^k, y_i^k)$  where  $x_i^k$  is the share of trove  $k$ 's collateral received by trove  $i$  and  $y_i^k$  is the share trove  $k$ 's debt absorbed

by trove  $i$ .

Let's call  $x_i$  the total accumulated collateral from rewards earned by trove  $i$ . At the end of the first-order stage this is the sum of its collateral rewards from  $m$  past liquidations.

(For simplicity, let's assume that troves  $n+1, \dots, n+m$  are the liquidated troves, in that order, and  $1, \dots, n$  are those that remain)

For a remaining trove:

$$x_i = x_i^{n+1} + \dots + x_i^{n+m} = \sum_{k=n+1}^{n+m} x_i^k = \sum_{j=1}^m x_i^{n+j} \quad (13)$$

For a liquidated trove the sum would be truncated at the previous liquidated trove:

$$x_i = x_i^{n+1} + \dots + x_i^{i-1} = \sum_{k=n+1}^{i-1} x_i^k \quad (14)$$

With each liquidation,  $c_j$  collateral is removed from the system. Again, as per (9), stake equals collateral. Thus, the  $S$  numerator in each liquidation is reduced by  $c_j$ , where  $j$  denotes the index of the liquidated trove.

Let

$$C_{n+m} = \sum_{i=1}^{n+m} c_i \quad (15)$$

and

$$L_m = \sum_{j=1}^m c_{n+j} \quad (16)$$

We now sum all reward events, noting that the liquidated trove's collateral is removed from the  $S$  denominator at each reward. Getting back to (13), note that for each previous liquidated trove  $n+j$ , the share of collateral that corresponds to trove  $i$  is:

$$x_i^j = \frac{c_i}{C_{n+m} - L_j} (c_{n+j} + x_{n+j}) \quad (17)$$

The denominator  $C_{n+m} - L_j$  corresponds to the fact that the amount of total initial stakes has been reduced by the amount of liquidated collateral from troves until  $j$ ,  $L_j$ . The collateral to redistribute is  $c_{n+j} + x_{n+j}$ , which corresponds to the initial collateral of the liquidated trove,  $c_{n+j}$ , plus the collateral it has earned from previous liquidations,  $x_{n+j}$ .

Therefore:

$$x_i = c_i \left[ \frac{c_{n+1} + x_{n+1}}{C_{n+m} - L_1} + \frac{c_{n+2} + x_{n+2}}{C_{n+m} - L_2} + \frac{c_{n+3} + x_{n+3}}{C_{n+m} - L_3} + \dots + \frac{c_{n+m} + x_{n+m}}{C_{n+m} - L_m} \right] \quad (18)$$

i.e.

$$x_i = c_i \sum_{j=1}^m \frac{c_{n+j} + x_{n+j}}{\sum_{i=1}^{n+m} c_i - \sum_{p=1}^j c_{n+p}} \quad (19)$$

(Note, that for liquidation of a given trove  $j$ , the redistributed collateral is the sum of its collateral  $c_{n+j}$  plus its accumulated collateral reward  $x_{n+j}$  which has itself been earned from liquidations  $[n+1, n+2, n+3, \dots, n+j-1]$ . Thus, liquidations have a “roll-up” effect - though, it is not important for our result. In fact, it can also be proved that  $x_i = c_i \frac{L_m}{C_n}$ )

We label the main sum expression  $H$ .

Rewriting trove  $i$ 's accumulated reward:

$$x_i = H c_i \quad (20)$$

Summing over all  $n$  active troves gives the total accumulated rewards for active troves in the system:

$$X_n = \sum_{i=1}^n H c_i \quad (21)$$

$$X_n = H C_n \quad (22)$$

Note that after  $m$  liquidations, the system snapshots update from initially:

$$S_\emptyset = C_\emptyset = C_{n+m} \quad (23)$$

to:

$$S_\emptyset = C_n \quad (24)$$

$$C_\emptyset = C_n + X_n \quad (25)$$

(Note that it can also be proved that that  $X_n = L_m$  and therefore  $C_\emptyset = C_n + L_m = C_{n+m}$ )

Now, a fresh trove is added,  $j$ , with collateral  $c_j$  (and the system becomes second-order). Let the ICR of trove  $j$  equal the ICR of an active first-order trove  $i$ .

$$\gamma_j = \gamma_i \quad (26)$$

$$\gamma_j = \frac{c_j}{d_j} \quad (27)$$

$$\gamma_i = \frac{c_i + x_i}{d_i + y_i} \quad (28)$$

Where  $c_j, d_j$  and  $c_i, d_i$  are the collateral and debt values of trove  $j$  and trove  $i$  respectively.

$x_i, y_i$  are the respective accumulated collateral and debt rewards for trove  $i$  earned by its stake over its lifetime.

The ICR equality identity (26) yields the following relation:



$$c_j = \frac{d_j}{d_i + y_i}(c_i + x_i) \quad (29)$$

i.e.

$$c_j = \lambda(c_i + x_i) \quad (30)$$

where

$$\lambda = \frac{d_j}{d_i + y_i} \quad (31)$$

Trove  $j$ 's stake  $s_j$  is given by the corrected stake rule (9), that is:

$$s_j = \frac{c_j \cdot S_\emptyset}{C_\emptyset} \quad (32)$$

Which by (24) and (25) gives:

$$s_j = \frac{c_j \cdot C_n}{C_n + X_n} \quad (33)$$

Now, trove  $k$  liquidates. Upon liquidation, the second-order trove  $j$  and the first-order trove  $i$  earn the following rewards:

$$\begin{aligned} r_{c_j} &= a s_j \\ r_{d_j} &= b s_j \\ r_{c_i} &= a s_i \\ r_{d_i} &= b s_i \end{aligned} \quad (34)$$

where

$$a = \frac{c_k + x_k}{S} \quad (35)$$

$$b = \frac{d_k + y_k}{S} \quad (36)$$

And since  $s_i$  is a first-order stake:

$$s_i = c_i \quad (37)$$

To show ICR equivalence after the reward event, we must first obtain  $s_j$  as a linear function of  $c_i$ . Recall our definition of trove  $j$ 's stake from (33):

$$s_j = \frac{c_j \cdot C_n}{C_n + X_n} \quad (38)$$

Now, substituting in the expression for  $i$ 's collateral, (30), we obtain:

$$s_j = \frac{\lambda(c_i + x_i)C_n}{C_n + X_n} \quad (39)$$

Substituting in the expressions for accumulated reward  $x_j$  from (20), and total accumulated reward  $X_n$  from (22):

$$s_j = \frac{\lambda(c_i + Hc_i)C_n}{C_n + HC_n} \quad (40)$$

And factorizing:

$$s_j = \frac{\lambda c_i (C_n + HC_n)}{C_n + HC_n} \quad (41)$$

Canceling yields:

$$s_j = \lambda c_i \quad (42)$$

We now compare ICRs of trove  $j$  and trove  $i$ , after liquidation of trove  $k$ , respectively  $\gamma'_j$  and  $\gamma'_i$ .

$$\gamma'_j = \frac{c_j + r_{c_j}}{d_j + r_{d_j}} \quad (43)$$

$$\gamma'_i = \frac{c_i + x_i + r_{c_i}}{d_i + y_i + r_{d_i}} \quad (44)$$

Using (34), the individual rewards as functions of stakes:

$$\gamma'_j = \frac{c_j + as_j}{d_j + bs_j} \quad (45)$$

$$\gamma'_i = \frac{c_i + x_i + as_i}{d_i + y_i + bs_i} \quad (46)$$

Now, substituting our definitions for  $s_i$  (37) and  $s_j$  (42):

$$\gamma'_j = \frac{c_j + a\lambda c_i}{d_j + b\lambda c_i} \quad (47)$$

$$\gamma'_i = \frac{c_i + x_i + ac_i}{d_i + y_i + bc_i} \quad (48)$$

Using identities (30) for  $c_j$ , and (31) for  $d_j$ :

$$\gamma'_j = \frac{\lambda(c_i + x_i + ac_i)}{\lambda(d_i + y_i + bc_i)} \quad (49)$$

$$\gamma'_i = \frac{c_i + x_i + ac_i}{d_i + y_i + bc_i} \quad (50)$$

Thus, canceling  $\lambda$ :

$$\gamma'_j = \gamma'_i \quad (51)$$

□

**Lemma 7.2.** *We consider a system transition  $\Gamma_1 \rightarrow \Gamma_2$  triggered by the creation of a trove  $j$ , followed by a set of liquidations  $P$ , such that  $|P| > 1$  and  $j \notin P$ . For any trove  $i$  with  $\gamma_i = \gamma_j$  in  $\Gamma_1$ , the corrected stake approach maintains  $\gamma_i = \gamma_j$  in  $\Gamma_2$ .*

*Proof.* If instead of a single liquidation event at a given system order, we have now a set of  $P$  liquidation events, of arbitrary size  $> 1$ , it is clear that ICR equality holds across all  $P$  events:

Since ICR equality holds across one liquidation event, it will hold across the next, and thus hold for all.

Liquidation events do not alter the stakes that earn shares of liquidated collateral and debt - and for a given stake, the individual trove reward term given in (34) depends only on reward sizes and stakes.  $\square$

**Lemma 7.3.** *We consider a system transition  $\Gamma_1 \rightarrow \Gamma_2$  triggered by the creation of a trove, followed by some more creations, up to a set  $N$ , such that  $|N| > 1$ , and then by a single liquidation. For any trove  $i$  in  $\Gamma_1$  and any trove  $j$  in  $N$  with  $\gamma_i = \gamma_j$ , the corrected stake approach maintains  $\gamma_i = \gamma_j$  in  $\Gamma_2$ .*

*Proof.* With  $N$  second-order troves added between consecutive liquidation events, the stake  $s_j$  of any given second-order trove is given by (9):

$$s_j = \frac{c_j \cdot S_\emptyset}{C_\emptyset} \quad (52)$$

The snapshots of the system state after the last liquidation event  $(S_\emptyset, C_\emptyset)$  remain constant until the next liquidation. It is clear that all  $N$  second-order stakes  $s_j$  have been corrected by the same constant factor.

Thus,  $s_j$  in the  $N$  second-order troves case is equal to  $s_j$  in the single second-order trove case.

As such, the logic of the proof of Lemma 7.1 applies - and ICR equality between a second-order trove and first-order trove holds across a liquidation event, no matter how many fresh troves are added in between.

The fact that the liquidated trove is first or second-order doesn't have any impact on that proof either: it would only vary the amounts  $x_k$  and  $y_k$  in 35 and 36, which may be even zero if  $k$  is the last created trove, but we don't make any assumption on those amounts along the proof.  $\square$

**Theorem 7.4.** *We consider a system transition  $\Gamma_1 \rightarrow \Gamma_2$  triggered by the creation of a trove, followed by some more creations, up to a set  $N$ , and then by a set of liquidations  $P$ , such that  $|N|, |P| > 0$ . For any trove  $i$  in  $\Gamma_1$  and any trove  $j \in N, j \notin P$  with  $\gamma_i = \gamma_j$ , the corrected stake approach maintains  $\gamma_i = \gamma_j$  in  $\Gamma_2$ .*

*In other words, in a second-order system with  $M$  previous liquidations, and  $N$  second-order troves added after the last liquidation, ICR equality between a first-order trove and second-order trove holds across  $P$  subsequent liquidation events.*

*Proof.* Proofs of Lemmas 7.2 and 7.3 can be applied independently to extend Lemma 7.1 into this general result.  $\square$

**Lemma 7.5.** *For every 2<sup>nd</sup> order system  $\Gamma_2$  there exists an equivalent first-order system  $\Gamma_1$  that contains only first-order stakes which have experienced all liquidations.*

*Proof.* We now show that a second-order system is equivalent to a first-order system.

Consider a hypothetical first-order trove  $i$  and an actual second-order trove  $j$ . Let both troves have identical ICR, and also let trove  $i$ 's total collateral and debt equal trove  $j$ 's initial collateral and initial debt respectively:

$$c_i + x_i = c_j \quad (53)$$

$$d_i + y_i = d_j \quad (54)$$

Clearly, the ratio  $\lambda = \frac{d_j}{d_i + y_i} = 1$ .

We substitute  $\lambda = 1$  into the second-order system expression for  $s_i$ , from equation (42), to yield:

$$s_j = c_i \quad (55)$$

Thus, any second-order stake is equivalent to some hypothetical first-order stake  $s_i = c_i$ , which has accumulated collateral reward  $x_i = (c_j - c_i)$  and debt reward  $y_i = (d_j - d_i)$ .

Therefore any second-order system is equivalent to a first-order system that contains only first-order stakes which have experienced all liquidations. We write:

$$\Gamma_2 = \Gamma_1 \quad (56)$$

□

**Proposition 7.6.** *For every  $n^{th}$  order system  $\Gamma_n$  there exists an equivalent first-order system  $\Gamma_1$  that contains only first-order stakes which have experienced all liquidations.*

*Proof.* We prove it by induction.

We have already proved for  $n = 1$  in previous lemma:  $\Gamma_1 = \Gamma_2$ .

Now we show that if it's true for  $n - 1$  then it's true for  $n$ , i.e.:

$$\Gamma_{n-1} = \Gamma_n \Rightarrow \Gamma_n = \Gamma_{n+1} \quad (57)$$

Recall our system evolution function:

$$f(\Gamma_n) = \Gamma_{n+1} \quad (58)$$

Therefore:

$$\Gamma_{n+1} = f(\Gamma_n) = f(\Gamma_{n-1}) = \Gamma_n \quad (59)$$

So, for every  $n > 1$ ,  $\Gamma_n = \Gamma_{n-1}$ , and for the transitive property of equivalence, we finally have:

$$\Gamma_n = \Gamma_1 \quad (60)$$

□

Having shown all  $n^{th}$  order systems are equivalent to a first-order system, we now extend our previous conclusion to  $n^{th}$  order systems:

**Corollary 7.6.1.** *In an  $n^{th}$  order system with  $M$  previous liquidations, and  $N$  second-order troves added after the last liquidation, ICR equality between an  $(n - 1)^{th}$  order trove and  $n^{th}$  order trove holds across  $P$  liquidation events.*

## 8 Corrected Stake Approach Preserves Order

**Theorem 8.1.** *For every system  $\Gamma_n$  containing troves  $i$  and  $j$  with  $\gamma_i > \gamma_j$  that transitions to  $\Gamma_{n+1}$ , the corrected stake approach maintains  $\gamma_i > \gamma_j$ .*

*Proof.* Here we show that ICR ordering is preserved with corrected stakes across a liquidation event.

We make use of the first-order equivalence result, namely, that with corrected stakes:

$$\Gamma_n = \Gamma_1 \quad (61)$$

i.e:

Any  $n^{th}$  order system of troves is equivalent to a first-order system of troves. For a given fresh trove with stake  $s_i$  and collateral  $c_i$ , the stake  $s_i$  is equivalent to some hypothetical first-order stake  $c_j$  which has accumulated collateral reward  $x_j = (c_i - c_j)$  and debt reward  $y_j = (d_i - d_j)$ .

Due to this equivalence between first and  $n^{th}$ -order systems, if ordering is preserved for first-order systems, it is preserved for  $n^{th}$  order systems.

Now consider a first-order system of troves, with stakes equal to their initial collateral.

Let trove  $i$  and trove  $j$  be troves with initial collateral  $c_i$ ,  $c_j$  accumulated collateral and debt rewards  $x_i$ ,  $y_i$  and  $x_j$ ,  $y_j$  respectively:

$$\gamma_i = \frac{c_i + x_i}{d_i + x_i} \quad (62)$$

$$\gamma_j = \frac{c_j + x_j}{d_j + y_j} \quad (63)$$

Let their ICRs be such that:

$$\gamma_i > \gamma_j \quad (64)$$

Since, a first-order trove's collateral and debt rewards are always in direct proportion to its initial collateral, we can write the accumulated rewards as:

$$x_i = A c_i \quad (65)$$

$$x_j = A c_j \quad (66)$$

and

$$y_i = B c_i \quad (67)$$

$$y_j = B c_j \quad (68)$$

Where A is the sum of all 'collateral rewards per unit staked', and B is the sum of all 'debt rewards per unit staked'. This yields ICRs:

$$\gamma_i = c_i \frac{1 + A}{d_i + B c_i} \quad (69)$$

$$\gamma_j = c_j \frac{1 + A}{d_j + B c_j} \quad (70)$$

And the initial ICR inequality becomes:

$$c_i \frac{1 + A}{d_i + B c_i} > c_j \frac{1 + A}{d_j + B c_j} \quad (71)$$

Cross multiplying and canceling the common denominator yields:

$$c_i (1 + A) (d_j + B c_j) > c_j (1 + A) (d_i + B c_i) \quad (72)$$

Then expanding:

$$c_i (d_j + Bc_j) > c_j (d_i + Bc_i) \quad (73)$$

$$c_i d_j + Bc_i c_j > c_j d_i + Bc_i c_j \quad (74)$$

And canceling terms:

$$c_i d_j > c_j d_i \quad (75)$$

Finally yielding the result:

$$\frac{d_j}{c_j} > \frac{d_i}{c_i} \quad (76)$$

We will later use this to prove that the inequality of ICRs holds across a liquidation event.

Now consider a liquidation event occurs. Upon a trove liquidation,  $r_c$  collateral and  $r_d$  debt are distributed to all active troves. Each active trove earns rewards proportional to its initial collateral, thus:

$$\gamma'_i = \frac{c_i (1 + A) + ac_i}{d_i + Bc_i + bc_i} \quad (77)$$

$$\gamma'_j = \frac{c_j (1 + A) + ac_j}{d_j + Bc_j + bc_j} \quad (78)$$

Where:

$$a = \frac{r_c}{S} \quad (79)$$

$$b = \frac{r_d}{S} \quad (80)$$

Collecting terms:

$$\gamma_i = \frac{c_i (1 + a + A)}{d_i + (1 + B) c_i} \quad (81)$$

$$\gamma_j = \frac{c_j (1 + a + A)}{d_j + (1 + B) c_j} \quad (82)$$

And taking reciprocals:

$$\frac{1}{\gamma'_i} = \frac{d_i + (1 + B) c_i}{c_i (1 + a + A)} \quad (83)$$

$$\frac{1}{\gamma'_j} = \frac{d_j + (1 + B) c_j}{c_j (1 + a + A)} \quad (84)$$

Rearranging, and separating the constant term:

$$\frac{1}{\gamma'_i} = \left[ \frac{\frac{d_i}{c_i}}{1 + a + A} \right] + \left[ \frac{1 + B}{1 + a + A} \right] \quad (85)$$

$$\frac{1}{\gamma'_j} = \left[ \frac{\frac{d_j}{c_j}}{1 + a + A} \right] + \left[ \frac{1 + B}{1 + a + A} \right] \quad (86)$$

Recall our earlier result (76):  $\frac{d_i}{c_i} < \frac{d_j}{c_j}$ . Thus:

$$\frac{1}{\gamma'_i} < \frac{1}{\gamma'_j} \quad (87)$$

Then taking reciprocals, finally yields:

$$\gamma'_i > \gamma'_j \quad (88)$$

Therefore, trove ordering holds across a liquidation event in first-order systems, and thus holds across a liquidation event in  $n^{th}$  order systems.

## References

- [1] R. Lauko, R. Pardoe. *Liquity: Decentralized Borrowing Protocol (Whitepaper)*, 2020.  
<https://docsend.com/view/bwiczmy>
- [2] B. Batog, L. Boca, N. Johnson. *Scalable Reward Distribution on the Ethereum Blockchain*, 2018.  
<http://batog.info/papers/scalable-reward-distribution.pdf>

## 9 Appendix

We prove that after a redistribution proportional to the collateral of active troves, the ordering of active troves by ICR is preserved.

Consider two active troves  $i$  and  $j$  with ICR  $\gamma_i, \gamma_j$  such that  $\gamma_i > \gamma_j$ .

Let  $c_i, d_i$  and  $c_j, d_j$  denote the collateral and debt of troves  $i$  and  $j$  respectively, and let  $C$  denote the total active collateral in the system.

Given the definition of ICR we have

$$\frac{c_i}{d_i} > \frac{c_j}{d_j} \quad (89)$$

In the event of a redistribution of a trove  $k$ , its collateral  $c_k$  and debt  $d_k$  is redistributed to all active troves, proportional to their shares of  $C$ .

Troves  $i$  and  $j$  thus receive the following pairs of collateral and debt rewards  $(x_i, y_i)$  and  $(x_j, y_j)$ :

$$(x_i, y_i) = \left( \frac{c_i}{C} \cdot c_k, \frac{c_i}{C} \cdot d_k \right) \quad (90)$$

$$(x_j, y_j) = \left( \frac{c_j}{C} \cdot c_k, \frac{c_j}{C} \cdot d_k \right) \quad (91)$$

As a result, their ICRs will change to:

$$\gamma'_i = \frac{c_i + x_i}{d_i + y_i} \quad (92)$$

$$\gamma'_j = \frac{c_j + x_j}{d_j + y_j} \quad (93)$$

Let  $a = \frac{c_k}{C}$  and  $b = \frac{d_k}{C}$ . Substituting the rewards, this leads to:

$$\gamma'_i = \frac{c_i + a \cdot c_i}{d_i + b \cdot c_i} \quad (94)$$

$$\gamma'_j = \frac{c_j + a \cdot c_j}{d_j + b \cdot c_j} \quad (95)$$

The equations (94) and (95) can be rewritten as:

$$\frac{1}{\gamma'_i} = \left( \frac{d_i}{c_i} + b \right) \cdot \frac{1}{1 + a} \quad (96)$$

$$\frac{1}{\gamma'_j} = \left( \frac{d_j}{c_j} + b \right) \cdot \frac{1}{1 + a} \quad (97)$$

Taking the reciprocal of inequality (89):

$$\frac{d_i}{c_i} < \frac{d_j}{c_j} \quad (98)$$

and applying it to equations (96) and (97), canceling out common constants, yields:

$$\frac{1}{\gamma'_i} < \frac{1}{\gamma'_j} \quad (99)$$

Finally, taking the reciprocal of (99), yields:

$$\gamma'_i > \gamma'_j \quad (100)$$

Thus, ordering of active troves by ICR is preserved across a reward event that is proportional to the collateral of the active troves.  $\square$