ICR Equality is Maintained in Batog-based Redistribution with Corrected Stakes

September 2020

Contents

1 Introduction

The Liquity protocol needs to keep CDPs ordered by their collateral ratio, to allow for efficient redemptions in ascending order of collateral ratio.

One of our liquidation mechanisms redistributes the collateral and debt of a liquidated CDP between all remaining active CDPs. As such, we need to ensure that redistributions do not break CDP ordering.

In principle, redistribution in proportion to the collateral size of active CDPs maintains ordering.

However, in practice, it is clear that redistributing in a "push" based manner - iterating over all CDPs and updating their collateral and debt - does not scale, and has computational complexity of O(n).

Previous work by Batog et al[1] derived a scalable O(1) method to assign proportional rewards, as long as the basis for the rewards ("stakes") do not change over time. Rewards are stored separately from the initial stakes, which do not compound: past accumulated rewards are not included in future reward calculations. In Liquity, fresh CDPs (with no accumulated rewards) would gain a advantage in redistributions over older CDPs.

However, a CDP's collateral ratio is always based on its entire collateral, which does include accumulated rewards. This discrepancy means that the Batog reward distribution can break the ordering of CDPs by collateral ratio.

To remedy this, we modify the original Batog approach by introducing a "corrected stake", to ensure fresh CDPs do not receive disproportionate rewards. We then show that this corrected stake preserves CDP ordering.

Core Proof

- Proof: $ICR_1 = ICR_2$ in general case. 1^{st} order, M past liquidations. Evolves to 2^{nd} order: 1 new stake, 1 subsequent liquidation

Extensions

- Proof: $ICR_1 = ICR_2$ for 1^{st} order, M past liquidations Evolves to 2^{nd} order: 1 new stake, P subsequent liquidations
- Proof: $ICR_1 = ICR_2$ for 1^{st} order, M past liquidations Evolves to 2^{nd} order: Q new stakes, P subsequent liquidations
- Show 2^{nd} order system is equivalent to first order
- Show that n^{th} order system is equivalent to first order

2 Background

In a system of CDPs ordered by individual collateral ratio (ICR), it is straightforward to show that distributing the collateral and debt of a liquidated CDP to active CDPs, in proportion to the size of their collateral, preserves ICR ordering across reward events.

In practice, with a large system of CDPs on Ethereum, the redistributions must be implemented with a Batog pull-based mechanism for computational efficiency. In the Batog implementation, collateral and debt rewards are not compounded - they are stored separately from the CDPs initial collateral and debt, and are not included in future reward computations. Each earned reward is based *only* on the CDPs initial collateral "stake".

However, the ICR of a CDP is always computed as the ratio of its total collateral to its total debt. That is, the terms in a CDP's ICR calculation **do** include all its previous accumulated rewards.

3 The Problem: Rewards Can Break CDP Ordering

As the system undergoes reward events, a given CDP'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 CDPs have experienced all reward events - in this case, ordering is maintained.

However, a problem arises when a new CDP is created after active CDPs have received reward shares. This "fresh" CDP has then experienced fewer rewards than the earlier CDPs, and thus, it

receives a disproportionate share of subsequent rewards, relative to its total collateral.

This means that across a reward event, a "fresh" CDP's *proportional change* in ICR is different from the proportional change of the ICR of an older CDP, which has been in the system from the start.

This discrepancy can break CDP ordering.

4 System Order Terminology

We introduce the notion of *system order*. In general, a system of CDPs increases from order N to order N+1 when the following sequence of events occurs:

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

We capture this in a system evolution function:

$$f(S_N) = S_{N+1} \tag{1}$$

Let S_1 define a system of CDPs with past liquidations, in which all active CDPs have received reward shares from all past liquidations. S_1 is a first-order system, and contains only first-order stakes. Each stake s_i is equal to it's collateral c_i, and $totalStakes = \sum s_i = \sum c_i$.

Let S_2 define an evolution of S_1, i.e. $S_2 = f(S_1)$. S_2 is a system with past liquidations, with $totalStakes = \sum s_i + \sum s_j$, where s_j is the stake of newly added CDP_j. S_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, S_n is a system with n sequential pairs, each consisting of a CDP creation period and a liquidation period. CDP's made in a given CDP creation period t have experienced only those liquidations that occurred in liquidation period t or greater.

5 Corrected Stake Approach

To correct for the advantage gained by later stakes over earlier stakes, we introduce a corrected stake:

$$s_i = \begin{cases} c_i & for\ totalCollateral_\emptyset = 0 \\ \frac{c_i \cdot\ totalStakes_\emptyset}{totalCollateral_\emptyset} & for\ totalCollateral_\emptyset > 0 \end{cases} \tag{2}$$

Where $totalStakes_\emptyset$ and $totalCollateral_\emptyset$ 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 $totalCollateral_\emptyset \geq totalStakes_\emptyset$

5.1 At First-Order, Stake Equals Initial Collateral

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

$$s_i = c_i \tag{3}$$

for all s_i, c_i in an S_1 system.

5.2 Intuition Behind Choice of Corrected Stake

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

The corrected stake effectively models the fresh CDP's collateral c_i as a total collateral, which includes 'virtual' accumulated rewards. The corrected stake earns rewards for the CDP as if the CDP was first-order, and had been in the system from the beginning - thus maintaining proportional reward growth.

We now prove that ICR equality is maintained with rewards proportional to corrected stakes - starting with the simplest case, and progressively generalizing.

6 Corrected Stake Preserves Equality

6.1 PROOF. Corrected Stake Preserves ICR Equality Across a Reward Event in a Second Order System with m Past Liquidations

We consider the following event sequence:

- $n + m$ CDPs are created
- m CDPs are liquidated
- A fresh CDP is created
- An old CDP is liquidated

In other words, a first-order system of $n+m$ CDPs undergoes m CDP liquidations, before evolving to second-order. All other conditions remain the same.

Consider the m past liquidations from the point of view of an active first-order CDP_i. As per 2), the stake of CDP_i is $s_i = c_i$.

CDP_i earns total accumulated reward, x_i the sum of its rewards from m past liquidations.

With each liquidation, c_j collateral is removed from the system. Again, as per 2), stake equals collateral. Thus, the *totalStakes* numerator in each liquidation is reduced by c_j, where j denotes the index of the liquidated CDP.

(For simplicity, let's assume that CDPs $n + 1, ..., n + m$ are the liquidated CDPs and $1, ..., n$ are those that remain)

Let

$$C_{n+m} = \sum_{i=1}^{n+m} c_i \tag{4}$$

and

$$L_m = \sum_{j=1}^{m} c_{n+j} \tag{5}$$

We now sum all reward events, noting that the liquidated CDP's collateral is removed from the *totalStakes* numerator at each reward:

$$x_i = c_i \left[\frac{c_{n+1} + x_{n+1}}{C_{n+m} - L_1} + \frac{c_{n+2} + x_{n+2}}{C_{n+m} - L_2} + \frac{c_{n+3} + x_{n+3}}{C_{n+m} - L_3} + ... + \frac{c_{n+m} + x_{n+m}}{C_{n+m} - L_m} \right] \tag{6}$$

i.e.

$$x_i = c_i \sum_{j=1}^{m} \frac{c_{n+j} + x_{n+j}}{\sum_{i=1}^{n+m} c_i - \sum_{p=1}^{j} c_{n+p}} \tag{7}$$

(Note, that for liquidation of a given CDP_j, the redistributed collateral is the sum of its collateral c_{n+j} plus it's accumulated collateral reward x_{n+j} which has itself been earned from liquidations $[n+1, n+2, n+3, \ldots n+j-1]$. 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 CDP_i's accumulated reward:

$$x_i = Hc_i \tag{8}$$

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

$$X_n = \sum_{i=1}^{n} Hc_i \tag{9}$$

$$X_n = H\ C_n \tag{10}$$

Note that after the liquidation, the system snapshots update:

$$totalStakes_{\emptyset} = C_n \tag{11}$$

$$totalCollateral_{\emptyset} = C_n + X_n \tag{12}$$

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

Now, a fresh CDP is added, CDP_F, with collateral c_F. Let the ICR of CDP_F equal the ICR of an active first-order CDP_G.

Now, CDP_Z liquidates. Upon liquidation, the second-order CDP_F and the first-order CDP_G earn the following collateral rewards:

$$ICR_F = ICR_G \tag{13}$$

$$ICR_F = \frac{c_F}{d_F} \tag{14}$$

$$ICR_G = \frac{c_G + x_G}{d_G + y_G} \tag{15}$$

Where c_F, d_F and c_G, d_G are the collateral and debt values of CDP_F and CDP_G respectively.

x_G, y_G are the respective accumulated collateral and debt rewards for CDP_G earned by its stake over its lifetime.

The ICR equality identity 13 yields the following relation:

$$c_F = \frac{d_F}{d_G + y_G}(c_G + x_G) \tag{16}$$

i.e.

$$c_F = k(c_G + x_G) \tag{17}$$

where

$$k = \frac{d_F}{d_G + y_G} \tag{18}$$

CDP_F's stake s_F is given by the corrected stake rule 2), that is:

$$s_F = \frac{c_F \cdot totalStakes_{\emptyset}}{totalColateral_{\emptyset}} \tag{19}$$

Which by 11 and 12 gives:

$$s_F = \frac{c_F \cdot C_n}{C_n + X_n} \tag{20}$$

Now, a new liquidation occurs: CDP_Z liquidates. The system becomes second-order.

The event causes CDP_Z's collateral and debt (c_Z and d_Z) to be redistributed between all active CDPs, proportional to their stake.

For simplicity, let :

$$a = \frac{c_Z + x_Z}{totalStakes} \tag{21}$$

$$b = \frac{d_Z + y_Z}{totalStakes} \tag{22}$$

We define the collateral and debt rewards earned by CDP_F and CDP_G in the reward event:

$$\begin{aligned} r_{cF} &= as_F \\ r_{dF} &= bs_F \\ r_{cG} &= as_G \\ r_{dG} &= bs_G \end{aligned} \tag{23}$$

where

$$a = \frac{c_Z + x_Z}{totalStakes} \tag{24}$$

$$b = \frac{d_Z + y_Z}{totalStakes} \tag{25}$$

And since s_G is a first-order stake:

$$s_G = c_G \tag{26}$$

To show ICR equivalence after the reward event, we must first obtain s_F as a linear function of c_G. Recall our definition of CDP_F's stake from 20:

$$s_F = \frac{c_F \cdot C_n}{(C_n + X_n)} \tag{27}$$

Now, substituting in the expression for F's collateral, 17, we obtain:

$$s_F = \frac{k(c_G + x_G)C_n}{C_n + X_n} \tag{28}$$

Substituting in the expressions for accumulated reward x_i from 8, and total accumulated reward X_n from 10:

$$s_F = \frac{k(c_G + Hc_G)C_n}{C_n + HC_n} \tag{29}$$

And factorizing:

$$s_F = \frac{kc_G(C_n + HC_n)}{(C_n + HC_n)} \tag{30}$$

Canceling yields:

$$s_F = kc_G \tag{31}$$

We now compare ICRs of CDP_F and CDP_G, after liquidation of CDP_Z.

$$ICR_{F\ After} = \frac{c_F + r_{cF}}{d_F + r_{dF}} \tag{32}$$

$$ICR_{G\ After} = \frac{c_G + x_G + r_{cG}}{d_G + y_G + r_{dG}} \tag{33}$$

Using 23, the individual rewards as functions of stakes:

$$ICR_{F\ After} = \frac{c_F + as_F}{d_F + bs_F} \tag{34}$$

$$ICR_{G\ After} = \frac{c_G + x_G + as_G}{d_G + y_G + bs_G} \tag{35}$$

Now, substituting our definitions for s_G 26 and s_F 31:

$$ICR_{F\ After} = \frac{c_F + akc_G}{d_F + bkc_G} \tag{36}$$

$$ICR_{G\ After} = \frac{c_G + x_G + ac_G}{d_G + y_G + bc_G} \tag{37}$$

Using identities 17 for c_F, and 18 for d_F:

$$ICR_{F\ After} = \frac{k(c_G + x_G + ac_G)}{k(d_G + y_G + bc_G)} \tag{38}$$

$$ICR_{G\ After} = \frac{c_G + x_G + ac_G}{d_G + y_G + bc_G} \tag{39}$$

Cancelling k:

$$ICR_{F\ After} = \frac{c_G + x_G + ac_G}{d_G + y_G + bc_G} \tag{40}$$

$$ICR_{G\ After} = \frac{c_G + x_G + ac_G}{d_G + y_G + bc_G} \tag{41}$$

Thus:

$$ICR_{F\ After} = ICR_{G\ After} \tag{42}$$

QED.

6.2 EXTENSION PROOF. Arbitrary Number of Liquidation Events At Current System Order

If instead of a single liquidation event at a given system order, we have P liquidation events, 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 CDP reward term x_i given in 4) depends only on reward sizes and the total stakes.

6.3 EXTENSION PROOF. Arbitrary Number of CDPs Added Between Liquidation Events

With N second-order CDPs added between consecutive liquidation events, the stake s_F of any given second-order CDP is given by 1):

$$s_F = \frac{c_F \cdot totalStakes_{\emptyset}}{totalColateral_{\emptyset}} \tag{43}$$

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

Thus, s_F in the N second-order CDPs case is equal to s_F in the single second-order CDP case.

As such, the logic of the Main Proof applies - and ICR equality between a second-order CDP and first-order CDP holds across a liquidation event, no matter how many fresh CDPs are added in between.

6.4 CONCLUSION 1

Combining Main Proof with Extensions 1 & 2 yields the following conclusion:

In a second order system with M previous liquidations, and N second-order CDPs added after the last liquidation, ICR equality between a first-order CDP and second-order CDP holds across P subsequent liquidation events.

6.5 2nd Order Systems Collapse to 1st Order

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

Consider a hypothetical first order CDP_1 and an actual second order CDP_2. Let both CDPs have identical ICR, and also let CDP_1's total collateral and debt equal CDP_2's initial collateral and initial debt respectively:

$$c_1 + x_1 = c_2 \tag{44}$$

$$d_1 + y_1 = d_2 \tag{45}$$

Clearly, the ratio $k = \frac{d_2}{(d_1+y_1)} = 1$.

We substitute $k = 1$ into the second-order system expression for s_F, from equation 55), to yield:

$$s_2 = c_1 \tag{46}$$

Thus, any second-order stake is equivalent to some hypothetical first-order stake $s_1 = c_1$, which has accumulated collateral reward $x_1 = (c_2 - c_1)$ and debt reward $y_1 = (d_2 - d_1)$.

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:

$$S_2 = S_1 \tag{47}$$

6.6 N'th Order Systems Collapse to 1st Order

We prove it by induction. We have already proved for $n = 1$ that $S_1 = S_2$. Now we show that if it's true for $n - 1$ then it's true for n, i.e.:

$$S_{n-1} = S_n \Rightarrow S_n = S_{n+1} \tag{48}$$

Recall our system evolution function:

$$f(S_N) = S_{N+1} \tag{49}$$

Therefore:

$$S_{N+1} = f(S_N) = f(S_{n-1}) = S_N \tag{50}$$

So, for every N, $S_N = S_{N-1}$, and for the transitive property of equivalence, we finally have:

$$S_N = S_1 \tag{51}$$

Having shown all nth order systems are equivalent to a first order system, we now extend our previous conclusion to nth order systems:

6.7 CONCLUSION 2

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

7 Corrected Stake Preserves Order

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:

$$S_N = S_1 \tag{52}$$

i.e:

Any N'th order system of CDPs is equivalent to a first-order system of CDPs. For a given fresh CDP 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 CDPs, with stakes equal to their initial collateral.

Let CDP_1 and CDP_2 be CDPs with initial collateral c_1, c_2 accumulated collateral and debt rewards x_1, y_1 and x_2, y_2 respectively:

$$ICR_1 = \frac{c_1 + x_1}{d_1 + x_1} \tag{53}$$

$$ICR_2 = \frac{c_2 + x_2}{d_2 + y_2} \tag{54}$$

Let their ICRs be such that:

$$ICR_1 > ICR_2 \tag{55}$$

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

$$x_1 = Ac_1 \tag{56}$$

$$x_2 = Ac_2 \tag{57}$$

and

$$y_1 = Bc_1 \tag{58}$$

$$y_2 = Bc_2 \tag{59}$$

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:

$$ICR_1 = c_1 \frac{1 + A}{d_1 + Bc_1} \tag{60}$$

$$ICR_2 = c_2 \frac{1+A}{d_2 + Bc_2} \tag{61}$$

And the initial ICR inequality becomes:

$$c_1 \frac{1+A}{d_1 + Bc_1} > c_2 \frac{1+A}{d_2 + Bc_2} \tag{62}$$

Cross multiplying and cancelling the common denominator yields:

$$c_1 (1+A)(d_2 + Bc_2) > c_2 (1+A)(d_1 + Bc_1) \tag{63}$$

Then expanding:

$$c_1 (d_2 + Bc_2) > c_2 (d_1 + Bc_1) \tag{64}$$

$$c_1 d_2 + Bc_1 c_2 > c_2 d_1 + Bc_1 c_2 \tag{65}$$

And cancelling terms:

$$c_1 d_2 > c_2 d_1 \tag{66}$$

Finally yielding the result:

$$\frac{d_2}{c_2} > \frac{d_1}{c_1} \tag{67}$$

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 CDP liquidation, r_c collateral and r_d debt are distributed to all active CDPs. Each active CDP earns rewards proportional to its initial collateral, thus:

$$ICR_{1After} = \frac{c_1 (1+A) + ac_1}{d_1 + Bc_1 + bc_1} \tag{68}$$

$$ICR_{2After} = \frac{c_2 (1+A) + ac_2}{d_2 + Bc_2 + bc_2} \tag{69}$$

Where:

$$a = \frac{r_c}{totalStakes} \tag{70}$$

$$b = \frac{r_d}{totalStakes} \tag{71}$$

Collecting terms:

$$ICR_1 = \frac{c_1 (1+a+A)}{d_1 + (1+B) c_1} \tag{72}$$

$$ICR_2 = \frac{c_2 (1+a+A)}{d_2 + (1+B) c_2} \tag{73}$$

And taking reciprocals:

$$\frac{1}{ICR_{1After}} = \frac{d_1 + (1+B)\,c_1}{c_1\,(1+a+A)} \tag{74}$$

$$\frac{1}{ICR_{2After}} = \frac{d_2 + (1+B)\,c_2}{c_2\,(1+a+A)} \tag{75}$$

Rearranging, and separating the constant term:

$$\frac{1}{ICR_{1After}} = \left[\frac{\frac{d_1}{c_1}}{1+a+A}\right] + \left[\frac{1+B}{1+a+A}\right] \tag{76}$$

$$\frac{1}{ICR_{2After}} = \left[\frac{\frac{d_2}{c_2}}{1+a+A}\right] + \left[\frac{1+B}{1+a+A}\right] \tag{77}$$

Recall our earlier result 67: $\frac{d_1}{c_1} < \frac{d_2}{c_2}$. Thus:

$$\frac{1}{ICR_{1After}} < \frac{1}{ICR_{2After}} \tag{78}$$

Then taking reciprocals, finally yields:

$$ICR_{1After} > ICR_{2After} \tag{79}$$

Therefore, CDP ordering holds across a liquidation event in first-order systems, and thus holds across a liquidation event in N'th order systems.

References

[1] B. Batog, L. Boca, N. Johnson, "Scalable Reward Distribution on the Ethereum Blockchain", 2018. http://batog.info/papers/scalable-reward-distribution.pdf