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

Overview of Proof

- Background
- Problem - with uncorrected stakes, rewards can break CDP ordering
- Proposed solution: corrected stake
- Terminology

Core Proofs

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

Extensions

- Proof ICR_1== ICR_2 for 1st order, M past liquidations. Evolves to 2nd order: 1 new stake, P subsequent liquidations
- Proof ICR_1== ICR_2 for 1st order, M past liquidations. Evolves to 2nd 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.

Background

Previously, we showed that rewards proportional to collateral in a system of CDPs ordered by ICR preserves ordering across reward events [This work] assumed rewards are proportional to the total collateral of the CDP.

In reality, the CDP ordering system is 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 it’s total collateral to its total debt. That is, the terms in the ICR calculation include all previous accumulated rewards.

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 (see this work).

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.

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:

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

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 a 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.

Corrected Stake Approach

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

2)

$\mathbf{s_i = c_i}$ **if** $\mathbf{totalCollateral_{\varnothing} = 0}$

$\mathbf{s_i = c_i * totalStakes_{\varnothing} / totalCollateral_{\varnothing}}$ **if** $\mathbf{totalCollateral_{\varnothing} > 0}$

Where $totalStakes_{\varnothing}$ *and* $totalCollateral_{\varnothing}$ are the respective snapshots of the total stakes and total collateral in the system immediately after the last reward event.

At First-Order, Stake Equals Initial Collateral

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

3) $\mathbf{s_i = c_i}$ for all s_i, c_i in an S_1 system.

Intuition Behind Choice of Corrected Stake, $\mathbf{s_i}$

The corrected stake s_i is chosen such that it earns rewards 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.

PROOF 1. **Corrected Stake Preserves ICR Equality Across a Reward Event in a Second-Order System**

We consider a first-order system S_1 of *n* CDPs, with one past liquidation: CDP_j. CDP_j had collateral c_j, debt d_j, and no accumulated reward.

The number of CDPs *n* includes the defaulted CDP.

Let:

4) $\mathbf{C_n = sum(c_i)}$

By equation 3), the property of a first-order system:

5) $\mathbf{totalStakes_{\varnothing} = sum(c_i)}$
6) $\mathbf{totalStakes_{\varnothing} = C_n}$

Let x_i be the total accumulated collateral reward for CDP_i. A given reward event at time *t* generates r_c collateral to be distributed. CDP_i's collateral reward at time *t* is:

7) $x_{it} = r_c$ / $totalStakes_t$.

The accumulated reward over time $x_i = sum(x_{it})$. For simplicity;

8) $X_n = sum(x_i)$

Importantly, the denominator $totalStakes_t$ does not include the stake of the liquidated CDP.

Also, total collateral is given by:

9) $totalCollateral_{\varnothing} = sum(c_i + x_i)$
10) $totalCollateral_{\varnothing} = C_n + X_n$

As the system has experienced only one liquidation of collateral c_j , CDP_i's total accumulated reward is:

11) $x_i = c_i * c_j / C_n$

Now, let a new fresh CDP be added, CDP_F, with collateral c_F.

Let the ICR of CDP_F equal the ICR of an active first-order CDP_G:

12) $ICR_F = ICR_G$

13) $ICR_F = c_F / d_F$
14) $ICR_G = (c_g + x_g) / (d_g + y_g)$

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, earned by its stake over its lifetime.

The ICR equality identity 12) yields the following relation:

15) $c_F = (d_F / (d_g + y_g)) * (c_g + x_g)$

i.e.

16) $c_F = k * (c_g + x_g)$

where

17) $k = (d_F / (d_g + y_g))$.

CDP_F's ***corrected stake*** s_F is given by equation 2).

Now, a reward event R_z occurs: an existing CDP_Z liquidates ,with z != f || g. 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 collateral.

For simplicity, let :

18) $a = c_z$ / *totalStakes*
19) $b = d_z$ / *totalStakes*

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

20)

$r_{cF} = as_F$
$r_{dF} = bs_F$

$r_{cg} = as_g$
$r_{dg} = bs_g$

And since s_g is a first-order stake:

21) $s_g = c_g$

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 a corrected stake, 2):

22) $s_i = c_i$ * *totalStakes*$_\varnothing$ / *totalCollateral*$_\varnothing$

And by the definition of *totalStakes* for a first-order system, 6), we have:

23) $s_F = c_F * C_n / (C_n + X_n)$

Now, substituting in the relation between F and G's collateral, 17), we obtain:

24) $s_F = [k(c_g + x_g)C_n] / [C_n + X_n]$

Consider the reward term, x_g, which represents the total accumulated past reward of CDP_G

before reward event R_z. Recall that the denominator *totalStakes* in x_i must exclude c_j, the collateral from the past liquidated CDP_j.

Thus:

25) $\mathbf{x_g = c_g c_j / (C_n - c_j)}$

and:

26) $\mathbf{X_n = C_n c_j / (C_n - c_j)}$

Substituting these expressions for accumulated rewards in to 24), yields:

27) $\mathbf{s_F = k * [(c_g + c_g c_j/(C_n - c_j)) * C_n] / [C_n + (C_n c_j / (C_n - c_j))]}$

Multiplying by $(C_n - c_j) / (C_n - c_j)$:

28) $\mathbf{s_F = k * [(c_g(C_n - c_j) + c_g c_j) * C_n] / [C_n(C_n - c_j) + C_n c_j]}$

Now, collecting terms:

29) $\mathbf{s_F = k * [c_g * C_n * C_n] / [C_n * C_n]}$

And finally cancelling, we obtain:

30) $\mathbf{s_F = k c_g}$

We now compare ICRs of CDP_F and CDP_G, after reward R_Z.

31) $\mathbf{ICR_{F\ After} = (c_F + r_{cF}) / (d_F + r_{dF})}$
32) $\mathbf{ICR_{G\ After} = (c_g + x_g + r_{cg}) / (d_g + y_g + r_{dg})}$

Using 20), the individual rewards as functions of stakes:

33) $\mathbf{ICR_{F\ After} = (c_F + a s_F) / (d_F + b s_F)}$
34) $\mathbf{ICR_{G\ After} = (c_g + x_g + a s_g) / (d_g + y_g + b s_g)}$

Now, substituting our definitions for s_g (21) and s_F (30):

35) $\mathbf{ICR_{F\ After} = (c_F + a k c_g) / (d_F + b k c_g)}$
36) $\mathbf{ICR_{G\ After} = (c_g + x_g + a c_g) / (d_g + y_g + b c_g)}$

Using identities 16) for c_F, and 17) for d_F:

37) $\mathbf{ICR_{F\ After} = (k(c_g + x_g) + akc_g) / (k(d_g + y_g) + bkc_g)}$
38) $\mathbf{ICR_{G\ After} = (c_g + x_g + ac_g) / (d_g + y_g + bc_g)}$

Cancelling k:

39) $\mathbf{ICR_{F\ After} = (c_g + x_g + ac_g) / (d_g + y_g + bc_g)}$
40) $\mathbf{ICR_{G\ After} = (c_g + x_g + ac_g) / (d_g + y_g + bc_g)}$

Thus:

41) $\mathbf{ICR_{F\ After} = ICR_{G\ After}}$

QED.

PROOF 2. **Corrected Stake Preserves ICR Equality Across a Reward Event in a Second Order System with *M* Past Liquidations**

We now extend the above proof to cover the case where the first-order system has undergone *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. Again as per 2), the stake of CDP_i is $s_i = c_i$.

c_i earns total accumulated reward, x_i the sum of its rewards over all *M* liquidations.

With each liquidation, the *totalStakes* denominator in each reward reduces by l_j, where j denotes the index of the liquidated CDP. Let *j=1* represent the first liquidation, and *j=m* the last.

Let

42) $\mathbf{C_n = sum_i(c_i)}$

and

43) $\mathbf{L_m = sum_j(l_j)}$

Collecting all reward events, and removing the liquidated CDP's collateral from the *totalStakes* at each reward:

44) $\mathbf{x_i = c_i * \{ [l_1 / (C_n - L_1)] + [l_2 / (C_n - L_2)] + [l_3 / (C_n - L_3)] + \ldots + [l_m / (C_n - L_m)] \}}$

Manipulating to obtain a single fraction yields:

45) $x_i = c_i * (H / D)$

Where

46) $H = \{ [l_1 D / (C_n - L_1)] + [l_2 D / (C_n - L_2)] + [l_3 D / (Cn - L_3)] + \ldots + [l_m D / (C_n - L_m)] \}$

and

47) $D = (C_n - L_1) * (C_n - L_2) * (Cn - L_3) * \ldots * (C_n - L_m)$

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

48) $X_n = \text{sum}(c_i / (H / D))$
49) $X_n = C_n / (H / D)$

Now, reward event R_z occurs: CDP_Z liquidates, and as before, the second-order CDP_F and the first-order CDP_G (with until-now identical ICRs) earn the following collateral rewards:

50) $r_{cF} = as_F$
51) $r_{dF} = bs_F$

52) $r_{cg} = as_g$
53) $r_{dg} = bs_g$

And since s_g is a first-order stake:

54) $s_g = c_g$

Again, we now seek s_F as a linear function of c_g.

By our first-order system property 1), and the ICR relation 6):

55) $s_F = [k(c_g + x_g)C_n] / [C_n + X_n]$

Substituting in the accumulated reward 45) and total accumulated reward 49):

56) $s_F = [k(c_g + c_g(H / D))C_n] / [C_n + C_n (H / D)]$

Multiplying by D/D:

57) $s_F = [k(c_g D + c_g H)C_n] / [C_n D + C_n H]$

Collecting terms:

58) $\mathbf{s_F = [\, kc_g(D + H)C_n\,] / [C_n\,(D + H)]}$

And cancelling, yields:

59) $\mathbf{s_F = kc_g}$

We obtain the same result for $\mathbf{s_F}$ as in the single liquidation case 30) .Comparing ICRs as per 31) and by following same steps thereafter, yields:

60) $\mathbf{ICR_{F\ After} = ICR_{G\ After}}$

EXTENSION 1. 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 stake values that earn shares of liquidated collateral and debt - the individual CDP reward function varies only with reward size and *totalStakes.*

EXTENSION 2. 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):

61) $\mathbf{s_i = c_i * totalStakes_{\varnothing} / totalCollateral_{\varnothing}}$

The snapshots of the system state after the last liquidation event ($totalStakes_{\varnothing}$, $totalCollateral_{\varnothing}$) remain constant until the next liquidation. All N second-order stakes 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 Proof 2 applies - and ICR equality between a second-order CDP and first-order CDP holds across a liquidation event.

CONCLUSION 1

Combining Proof 2 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 reward events.

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:

62) $\mathbf{c_1 + x_1 = c_2}$
63) $\mathbf{d_1 + y_1 = d_2}$

Clearly, the ratio $k = d_2/(d_1+y_1) = 1$.

Following the argument of Proof 2 with k = 1, yields:

64) $\mathbf{s_2 = c_1}$.

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, containing only first-order stakes that have experienced all liquidations. We write:

65) $S_2 \equiv S_1$.

n'th Order Systems Collapse to 1st Order

Recall our system evolution function:

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

By definition, our N'th order system is the N'th evolution of a first order system:

67) $S_N = f^N(S_1)$

And thus the N-1'th evolution of a second-order system:

68) $S_N = f^{N-1}(S_2)$

By equivalence 65):

69) $S_N \equiv f^{N-1}(S_1)$

Repeating the steps, it is clear that

$S_N \equiv f^{N-2}(S_1)$
$S_N \equiv f^{N-3}(S_1)$

...etc,

and finally:

70)
$S_N \equiv f(S_1)$
$S_N \equiv S_2$
$S_N \equiv S_1$.

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

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 reward events.