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

September 2020

Overview of Proof

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

Core Proofs

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

Extensions

- Proof 3: $ICR_1 = ICR_2$ for 1^{st} order, M past liquidations Evolves to 2^{nd} order: 1 new stake, P subsequent liquidations
- Proof 4: $ICR_1 = ICR_2$ 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

Background

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

In reality, the redistributions are 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 a CDP's ICR calculation **do** include all its 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.

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:

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

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 S1, 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.

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 $totalCollateral_{\emptyset} \geq totalStakes_{\emptyset}$

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.

Intuition Behind Choice of Corrected Stake, s_i

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.

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

We consider the following event sequence:

- $n+1$ CDPs are created
- 1 CDP is liquidated
- 1 fresh CDP is created
- 1 old CDP is liquidated

In other words, a first-order system of $n+1$ CDPs undergoes 1 liquidation, and then evolves to second-order.

Each initial CDP_i has collateral c_i and debt d_i.

Then, the first liquidation occurs: CDP_j with collateral c_j, debt d_j, is redistributed. The total number of active CDPs reduces from $n+1$ to n.

Each remaining active CDP_i earns a collateral reward x_i, which is proportional to the liquidated collateral c_j, and CDP_i's stake as a share of total stakes:

$$x_i = \frac{c_j \cdot s_i}{\sum\limits_{\substack{i=1 \\ i \neq j}}^{n+1} s_i} \tag{4}$$

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

$$x_i = \frac{c_j \cdot c_i}{\sum\limits_{\substack{i=1 \\ i \neq j}}^{n+1} c_i} \tag{5}$$

For simplicity, let:

$$C_n = \sum_{\substack{i=1 \\ i \neq j}}^{n+1} (c_i) \tag{6}$$

There are now n CDPs in the system.

Let the sum of accumulated rewards over all active CDPs be given by:

$$X_n = \sum_{\substack{i=1 \\ i \neq j}}^{n+1} x_i \tag{7}$$

Note that after the liquidation, the system snapshots update:

$$totalStakes_{\emptyset} = C_n \tag{8}$$

$$totalCollateral_{\emptyset} = C_n + X_n \tag{9}$$

(Note also that $X_n = c_j$ and therefore $totalCollateral_{\emptyset} = C_n + c_j = C_{n+1}$)

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:

$$ICR_F = ICR_G \tag{10}$$

$$ICR_F = \frac{c_F}{d_F} \tag{11}$$

$$ICR_G = \frac{c_G + x_G}{d_G + y_G} \tag{12}$$

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 10) yields the following relation:

$$c_F = \frac{d_F}{d_G + y_G}(c_G + x_G) \tag{13}$$

i.e.

$$c_F = k(c_G + x_G) \tag{14}$$

where

$$k = \frac{d_F}{d_G + y_G} \tag{15}$$

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

$$s_F = \frac{c_F \cdot totalStakes_{\emptyset}}{totalColateral_{\emptyset}} \tag{16}$$

Which by 8) and 9) gives:

$$s_F = \frac{c_F \cdot C_n}{C_n + X_n} \tag{17}$$

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 :

$$a = \frac{c_Z + x_Z}{totalStakes} \tag{18}$$

$$b = \frac{d_Z + y_Z}{totalStakes} \tag{19}$$

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

$$\begin{aligned} r_{cF} &= as_F \\ r_{dF} &= bs_F \\ r_{cG} &= as_G \\ r_{dG} &= bs_G \end{aligned} \tag{20}$$

And since s_G is a first-order stake:

$$s_G = c_G \tag{21}$$

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 17):

$$s_F = \frac{c_F \cdot C_n}{(C_n + X_n)} \tag{22}$$

Now, substituting in the expression for F's collateral, 14), we obtain:

$$s_F = \frac{k(c_G + x_G)C_n}{C_n + X_n} \tag{23}$$

Consider the term, x_G, which represents the total accumulated past reward of CDP_G before liquidation of CDP_Z. Since CDP_j was the only previous liquidation:

$$x_G = \frac{s_G c_j}{\sum\limits_{\substack{i=1 \\ i \neq j}}^{n+1} s_i} \tag{24}$$

And since all stakes s_i were first order:

$$x_G = \frac{c_G c_j}{C_n} \tag{25}$$

By the same token, the total accumulated rewards for all active CDPs, from liquidation of CDP_j must be:

$$X_n = c_j \tag{26}$$

Substituting these expressions for x_G and X_n into 23), yields:

$$s_F = \frac{k(c_G C_n + c_G c_j)}{C_n + c_j} \tag{27}$$

Factoring out c_G from the numerator:

$$s_F = \frac{kc_G(C_n + c_j)}{(C_n + c_j)} \tag{28}$$

And cancelling, we obtain:

$$s_F = kc_G \tag{29}$$

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

$$ICR_{F\ After} = \frac{c_F + r_{cF}}{d_F + r_{dF}} \tag{30}$$

$$ICR_{G\ After} = \frac{c_G + x_G + r_{cG}}{d_G + y_G + r_{dG}} \tag{31}$$

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

$$ICR_{F\ After} = \frac{c_F + as_F}{d_F + bs_F} \tag{32}$$

$$ICR_{G\ After} = \frac{c_G + x_G + as_G}{d_G + y_G + bs_G} \tag{33}$$

Now, substituting our definitions for s_G (21) and s_F (29):

$$ICR_{F\ After} = \frac{c_F + akc_G}{d_F + bkc_G} \tag{34}$$

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

Using identities 14) for c_F, and 15) for d_F:

$$ICR_{F\ After} = \frac{k(c_G + x_G + ac_G)}{k(d_G + y_G + bc_G)} \tag{36}$$

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

Cancelling k:

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

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

Thus:

$$ICR_{F\ After} = ICR_{G\ After} \tag{40}$$

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 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 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.

(Let's assume $n+1, ..., n+m$ are the liquidated CDPs and $1, ..., n$ are the ones staying, for simplicity)

Let

$$C_{n+m} = \sum_{i=1}^{n+m} c_i \tag{41}$$

and

$$L_m = \sum_{j=1}^{m} c_{n+j} \tag{42}$$

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

$$x_i = c_i \left[\frac{c_{n+1} + x_{n+1}}{C_{n+m} - L_1} + \frac{c_{n+2} + x_{n+2}}{C_{n+m} - L_2} + \frac{c_{n+3} + x_{n+3}}{C_{n+m} - L_3} + ... + \frac{c_{n+m} + x_{n+m}}{C_{n+m} - L_m} \right] \tag{43}$$

i.e.

$$x_i = c_i \sum_{j=1}^{m} \frac{c_{n+j} + x_{n+j}}{\sum\limits_{i=1}^{n+m} c_i - \sum\limits_{p=1}^{j} c_{n+p}} \tag{44}$$

(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 $[n+1, n+2, n+3, \dots n+j-1]$. Thus, liquidations have a "roll-up" effect - though, it is not important for our result. Actually, 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:

$$x_i = Hc_i \tag{45}$$

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

$$X_n = \sum_{i=1}^{n} Hc_i \tag{46}$$

$$X_n = H\ C_n \tag{47}$$

(Note: It can also be proved that $X_n = L_m$)

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:

$$\begin{aligned} r_{cF} &= as_F \\ r_{dF} &= bs_F \\ r_{cG} &= as_G \\ r_{dG} &= bs_G \end{aligned} \tag{48}$$

where

$$a = \frac{c_Z + x_Z}{totalStakes} \tag{49}$$

$$b = \frac{d_Z + y_Z}{totalStakes} \tag{50}$$

And since s_G is a first-order stake:

$$s_G = c_G \tag{51}$$

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

The stake s_F can be derived in exactly the same manner as in the simple case. By our corrected stakes rule, and the fact that $ICR_F = ICR_G$, we obtain:

$$s_F = \frac{k(c_G + x_G)C_n}{C_n + X_n} \tag{52}$$

(see steps 8-23 for this derivation)

Substituting in the expressions for accumulated reward x_i from 45), and total accumulated reward X_n from 47):

$$s_F = \frac{k(c_G + Hc_G)C_n}{C_n + HC_n} \tag{53}$$

And factorizing:

$$s_F = \frac{kc_G(C_n + HC_n)}{(C_n + HC_n)} \tag{54}$$

Canceling yields:

$$s_F = kc_G \tag{55}$$

We obtain the same result for s_F as in the single liquidation case 29) .Comparing ICRs as per 30) and by following same steps thereafter, yields:

$$ICR_{F\ After} = ICR_{G\ After} \tag{56}$$

EXTENSION PROOF 3. 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.

EXTENSION PROOF 4. 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):

$$s_F = \frac{c_F \cdot totalStakes_{\emptyset}}{totalColateral_{\emptyset}} \tag{57}$$

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 Proof 2 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.

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 liquidation 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:

$$c_1 + x_1 = c_2 \tag{58}$$

$$d_1 + y_1 = d_2 \tag{59}$$

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:

$$s_2 = c_1 \tag{60}$$

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:

$$S_2 = S_1 \tag{61}$$

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.:

$$S_{n-1} = S_n \Rightarrow S_n = S_{n+1} \tag{62}$$

Recall our system evolution function:

$$f(S_N) = S_{N+1} \tag{63}$$

Therefore:

$$S_{N+1} = f(S_N) = f(S_{n-1}) = S_N \tag{64}$$

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

$$S_N = S_1 \tag{65}$$

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