Analysis and Attacks of decentralized content curation platforms

Orfeas Stefanos Thyfronitis Litos, Andrés Monteoliva Mosteiro, and Aggelos Kiayias

University of Edinburgh
o.thyfronitis@ed.ac.uk, a.monteoliva@serious.server, akiayias@inf.ed.ac.uk

Abstract. We will attack Steem.

1 Introduction

Steem is not incentive-compatible.

2 Related Work

Several research efforts have aimed to model the mechanics and incentives for users in crowdsourced content curation systems. Motivated by the widespread adoption of crowdsourced aggregation sites such as Reddit or Digg, they have aimed to model crowdsourced curation of User-generated content (UGC) [1]. Most of the academic work in the field have analyzed content curation from an incentives and game-theoretic standpoint [2,3,4]. We recognize the value of these past efforts and we adopt some of the components used in these models such as the quality distribution of the articles and the user's attention span(askalidis,ghosh). However, our approach is fundamentally different as we describe the mechanics of post-voting systems from a computational angle. More specifically, we draw inspiration from the real-ideal world paradigm of Cryptography [5] in the definition of convergence.

We are aware of the limitations imposed by Arrow's impossibility theorem [6]. Nevertheless, since we avoid a general game-theoretic approach, these limitations do not impact the outcomes of our work. In particular, we restrict the behavior of agents to a specific set of choices and we do not permit strategic decisions. Only a subset of players is endowed with a payoff function. This keeps the computational analysis of post-voting systems tractable whilst highlighting.

In the present work, we develop a general framework for the analysis of decentralized content curation platforms. After that, we particularize our analysis on Steemit as we recognize that the explicit financial incentives present in its blockchain-based platform are better suited to our analysis than traditional sites such as Reddit or Hacker News, studied in the previous literature. The governance of online communities such as Wikipedia has been thoroughly studied in previous academic work [7,8]. However, the financially incentivized governance processes in blockchain systems, where the voters are at the same time equity-holders have still many open research questions [**?**,**?**]. Beyond the Steem blockchain, coinholder voting systems are present in decentralized platforms as DAOs [9] or in other blockchain protocols such as EOS(cite) or Tezos(cite) (not sure if including this). Our analysis of Steemit's post-voting system aims to provide a better framework for the better design of future decentralized curation platforms.

3 Model

1 Notation

- We denote the set of all probability distributions on set A as $\mathcal{D}(\mathcal{A})$.
- We denote the powerset of a set A with 2^A.
- $a\|b$ denotes the concatenation of a and b.
- Let $n \in \mathbb{N}^*$. $[n]$ denotes $\{1, 2, \ldots, n\}$.

2 Properties of Post Voting Systems

A post voting system has the objective to arrange the posts according to the preferences of the participants. The ideal order is defined based on the likeability matrix for the posts.

Definition 1 (Post). *Let $N \in \mathbb{N}^*$. A post is defined as $p = (i, l)$, with $i \in [N], l \in [0,1]^N$.*

- ***Author.*** *The first element of a post is the index of its creator, i.*
- ***Likeability.*** *The likeability of a post is defined as $l \in [0,1]^N$.*

Let $M \in \mathbb{N}^*$ the number of posts. Then $\forall j \in [M]$, let $\mathrm{creator}_j \in [N], l_j \in [0,1]^N$ and $p_j = (\mathrm{creator}_j, l_j)$. The set of all posts is $\mathcal{P} = \bigcup_{j=1}^{M} \{p_j\}$.

Definition 2 (Ideal Score of a post). *Let post $p = (m, l)$. We define the* ideal score *of p as* $\mathrm{idealSc}(p) = \sum_{i=1}^{N} l_i$.

The ideal score of a post is a single number that represents its overall worth to the community. By using simple summation, we assume that the opinions of all players have the same weight. In an ordered list of posts where higher posts are more visible, the "common interest" would require that a post with higher ideal score appear before another post with a lower score.

Definition 3 (t-Ideal Post Order). *Let $\mathcal{P}$ a list of posts. We say that $\mathcal{P}$ is in t-*ideal order *and that the property* $\textsc{Ideal}^t(\mathcal{P})$ *holds if*

$$\forall i < j \in |t|, \mathrm{idealSc}(\mathcal{P}[i]) \geq \mathrm{idealSc}(\mathcal{P}[j]) \quad .$$

Definition 4 (Post-Voting System). *A tuple* $\mathcal{S} = (\textsc{Init}, \textsc{Aux}, \textsc{HandleVote}, \textsc{Vote})$ *of four algorithms. The four algorithms parametrize the following two ITMs:*

$\mathcal{G}_{\mathrm{Feed}}$ *is a global functionality that accepts two messages:* `read`*, which responds with the current list of posts and* `vote`*, which can take various arguments and does whatever is defined in* $\textsc{HandleVote}$.

Π_{honest} *is a protocol that sends* `read` *and* `vote` *messages to* $\mathcal{G}_{\mathrm{Feed}}$ *whenever it receives (*`activate`*) from* $\mathcal{E}$.

Algorithm 1 $\mathcal{G}_{\mathrm{Feed}}(\textsc{Init}, \textsc{Aux}, \textsc{HandleVote})(\mathcal{P}, \mathrm{initArgs})$

Initialization:
    $\mathcal{U} \leftarrow \emptyset$ ▷ Set of players
    $\textsc{Init}(\mathrm{initArgs})$

Upon receiving (`read`) from u_{pid}:
$\mathcal{U} \leftarrow \mathcal{U} \cup \{u_{\mathrm{pid}}\}$
    aux $\leftarrow \textsc{Aux}(u_{\mathrm{pid}})$
    Send (`posts`, $\mathcal{P}$, aux) to u_{pid}

Upon receiving (`vote`, ballot) from u_{pid}:
    $\textsc{HandleVote}$(ballot)

Algorithm 2 $\Pi_{\mathrm{honest}}(\textsc{Vote})$

Upon receiving (`activate`) from $\mathcal{E}$:
    Send (`read`) to $\mathcal{G}_{\mathrm{Feed}}$
    Wait for response (`posts`, $\mathcal{P}$, aux)
    ballot $\leftarrow \textsc{Vote}(\mathcal{P}, \mathrm{aux})$
    Send (`vote`, ballot) to $\mathcal{G}_{\mathrm{Feed}}$

Definition 5 (Post-Voting System Activation Message). *We defince* $\texttt{act}_{\mathrm{pid}}$ *as the message* $(\texttt{activate}, \mathrm{pid})$*, sent to* u_{pid}*.*

Definition 6 (Execution Pattern). *Let* $N, R \in \mathbb{N}^*$*.*

$$\mathrm{ExecPat}_{N,R} = \left\{ \left(\texttt{act}_{\mathrm{pid}_1}, \ldots, \texttt{act}_{\mathrm{pid}_{NR}}\right) : \forall i \in [R], \forall k \in [N], \exists j \in [N] : \mathrm{pid}_{(i-1)N+j} = k \right\} \quad ,$$

i.e. activation messages are grouped in R *rounds and within each round each player is* ***activated*** *exactly once. The order of activations is not fixed.*

Let Environment $\mathcal{E}$ *that sends messages* $\mathrm{msgs} = \left(\texttt{act}_{\mathrm{pid}_1}, \ldots, \texttt{act}_{\mathrm{pid}_n}\right)$ *sequentially. We say that* $\mathcal{E}$ respects $\mathrm{ExecPat}_{N,R}$ *if* $\mathrm{msgs} \in \mathrm{ExecPat}_{N,R}$*. (Note: this implies that* $n = NR$*.)*

Definition 7 ((N, R, M, t)-convergence under honesty). *We say that a post-voting system* $\mathcal{S} = (\textsc{Init}, \textsc{Aux}, \textsc{HandleVote}, \textsc{Vote})$ (N, R, M, t)-converges under honesty *(or* t-converges under honesty for N players, R rounds and M posts*) if, for every input* $\mathcal{P}$ *such that* $|\mathcal{P}| = M$*, for every* $\mathcal{E}$ *that respects* $\mathrm{ExecPat}_{N,R}$ *and given that all protocols execute* Π_{honest}*, it holds that after* $\mathcal{E}$ *completes its execution pattern,* $\mathcal{G}_{\mathrm{Feed}}$ *contains a post list* $\mathcal{P}$ *such that* $\textsc{Ideal}^t(\mathcal{P})$ *is true.*

TODO: Discuss: Is R missing from Steem system? Maybe add "Let $N, R \in \mathbb{N}^*$, ..., controlled by an Environment that respects $\mathrm{ExecPat}_{N,R}$ and the following ...".

Definition 8 (Steem system). *The Steem system is the post voting system* $\mathcal{S}$ *with parameters* $\boldsymbol{SP} \in {\mathbb{N}^*}^N, a, b, \mathrm{regen} \in [0, 1] : a + b < 1, \mathrm{attSpan} \in \mathbb{N}^*$ *and the following parametrizing procedures:*

Algorithm 3 $\textsc{Init}(\mathbf{SP}, \mathrm{attSpan}, a, b, \mathrm{regen})$

Store input parameters as constants
$r \leftarrow 1$
$\mathrm{lastVoted} \leftarrow \underbrace{(0, \ldots, 0)}_{N}$
$\mathbf{VP} \leftarrow \underbrace{(1, \ldots, 1)}_{N}$
$\mathrm{scores} \leftarrow \underbrace{(0, \ldots, 0)}_{|\mathcal{P}|}$

Algorithm 4 Aux

return $(\mathbf{SP}, \text{attSpan}, a, b, r, \text{regen})$

Algorithm 5 HandleVote $(\text{ballot}, u_{\text{pid}})$

if $\text{lastVoted}_{\text{pid}} \neq r$ **then** ▷ One vote per player per round
  $\mathbf{VP}_{\text{pid},r} \leftarrow \mathbf{VP}_{\text{pid}}$ ▷ For proofs
  $\mathbf{VP}_{\text{pid}} \leftarrow \max\{\mathbf{VP}_{\text{pid}} + \text{regen} \cdot (r - \text{lastVoted}_{\text{pid}}), 1\}$ ▷ TODO: Remove $(r - \text{lastVoted}_{\text{pid}})$?
  $\mathbf{VP}\text{reg}_{\text{pid},r} \leftarrow \mathbf{VP}_{\text{pid}}$ ▷ For proofs
  if ballot $\neq$ **null then**
    Parse ballot as (p, weight)
    $\text{cost} \leftarrow a \cdot \mathbf{VP}_{\text{pid}} \cdot \text{weight} + b$
    if $\mathbf{VP}_{\text{pid}} - \text{cost} \geq 0$ **then**
      $\text{score} \leftarrow \text{cost} \cdot \mathbf{SP}_{\text{pid}}$
      $\mathbf{VP}_{\text{pid}} \leftarrow \mathbf{VP}_{\text{pid}} - \text{cost}$
    else
      $\text{score} \leftarrow \mathbf{VP}_{\text{pid}} \cdot \mathbf{SP}_{\text{pid}}$
      $\mathbf{VP}_{\text{pid}} \leftarrow 0$
    end if
    $\text{scores}_p \leftarrow \text{scores}_p + \text{score}$
  end if
  $\text{lastVoted}_{\text{pid}} \leftarrow r$
end if
if $\forall i \in [N], \text{lastVoted}_i = r$ **then** ▷ round over
  $\mathcal{P} \leftarrow$ Order $(\mathcal{P}, \text{scores})$ ▷ order posts by votes
  $\mathcal{P}_r \leftarrow \mathcal{P}$ ▷ For proofs
  $r \leftarrow r + 1$
end if ▷ TODO: count rounds? simplify with set of voted and check of length?

Algorithm 6 $\textsc{Vote}\,(\mathcal{P}, \text{aux})$

```
Store aux contents as constants
voteRounds ← VoteRounds(R, |𝒫|)
if VoteThisRound(r, |𝒫|) = yes then
    top ← ChooseTopPosts(attSpan, 𝒫, votedPosts)
    (i, l) ← argmax_{(i,l)∈top} {l_pid}[1]
    votedPosts ← votedPosts ∪ (i, l)
    return ((i, l), l_pid)
else
    return null
end if

function ChooseTopPosts(attSpan, 𝒫, votedPosts)
    res ← ∅
    idx ← 1
    while |res| < attSpan & idx ≤ |𝒫| do
        if 𝒫[idx] ∉ votedPosts then                ▷ One vote per post per player
            res ← res ∪ {𝒫[idx]}
        end if
        idx ← idx + 1
    end while
    return res
end function

function VoteThisRound(r, M)
    if R < M then
        return yes
    else if r ∈ voteRounds then
        return yes
    else
        return no
    end if
end function

function VoteRounds(R, M)
    voteRounds ← ∅
    for i = 1 to M do
        voteRounds ← voteRounds ∪ {1 + ⌊(i − 1) (R−1)/(M−1)⌋}
    end for
    return voteRounds
end function
```

Theorem 1. *The Steem system* (N, R, M, M)*-converges if and only if* $\boldsymbol{SP}$ *is constant and* $R - 1 \geq (M-1)\left\lceil \frac{a+b}{\text{regen}} \right\rceil$.

Proof. – ($\Leftarrow$) Suppose that

$$R-1 \geq (M-1)\left\lceil \frac{a+b}{\text{regen}} \right\rceil \tag{1}$$
$$\text{and } \forall i \in [N], \mathbf{SP}_i = c \ .$$

Let pid $\in [N]$. In this case it is $R \geq M$ and according to VOTETHISROUND in Algorithm 6, u_{pid} votes non-null in rounds $(r_1, \ldots, r_M)$ with $r_i = \left\lfloor (i-1)\frac{R-1}{M-1} \right\rfloor + 1$. Observe that:

$$(1) \Rightarrow \frac{R-1}{M-1} \geq \left\lceil \frac{a+b}{\text{regen}} \right\rceil \overset{\text{rhs}}{\underset{\text{integer}}{\Rightarrow}} \left\lfloor \frac{R-1}{M-1} \right\rfloor \geq \left\lceil \frac{a+b}{\text{regen}} \right\rceil \ , \tag{2}$$

$$\forall i \in [M] \setminus \{1\}, r_i \in \left\{ r_{i-1} + \left\lfloor \frac{R-1}{M-1} \right\rfloor, r_{i-1} + \left\lceil \frac{R-1}{M-1} \right\rceil \right\} \ . \tag{3}$$

From (2) and (3) we have that $\forall i \in [M-1], r_{i+1} - r_i \geq \left\lceil \frac{a+b}{\text{regen}} \right\rceil$. We will now prove by induction that $\forall i \in [M], \mathbf{VP}_{\text{pid},r_i} = 1$.

- For $i = 1, \mathbf{VP}_{\text{pid},1} = 1$ by (Algorithm 3, line 4).
- Let $\mathbf{VP}_{\text{pid},r_i} = 1$. Until r_{i+1}, a single non-null vote is cast by u_{pid}, which reduces $\mathbf{VP}_{\text{pid}}$ by at most $a+b$ (Algorithm 5, line 7) and at least $\left\lceil \frac{a+b}{\text{regen}} \right\rceil$ regenerations, each of which replenishes $\mathbf{VP}_{\text{pid}}$ by regen. Thus

$$\mathbf{VP}_{\text{pid},r_{i+1}} \geq \min\left\{ \mathbf{VP}_{\text{pid},r_i} - a - b + \text{regen}\left\lceil \frac{a+b}{\text{regen}} \right\rceil, 1 \right\} \geq 1 \ .$$

  But $\mathbf{VP}_{\text{pid}}$ cannot exceed 1 (line 4), thus $\mathbf{VP}_{\text{pid},r_{i+1}} = 1$.

Since the above holds for every pid $\in [N]$, we have that at the end of the execution, all votes have been cast with full voting power, thus $\forall p = (i,l) \in \mathcal{P}_R, \text{scores}_p = c\left(Nb + a \sum_{\text{pid}=1}^{N} l_{\text{pid}} \right)$ and the posts in $\mathcal{P}_R$ are sorted by decreasing score (Algorithm 5, line 20). We observe that

$$\forall p_1 = \left(j^1, l^1\right) \neq p_2 = \left(j^2, l^2\right) \in \mathcal{P}_R, \text{idealSc}\left(p_1\right) > \text{idealSc}\left(p_2\right) \Rightarrow$$
$$\sum_{i=1}^{N} l_i^1 > \sum_{i=1}^{N} l_i^2 \Rightarrow c\left(Nb + a\sum_{i=1}^{N} l_i^1 \right) > c\left(Nb + a\sum_{i=1}^{N} l_i^2 \right) \ .$$

Thus all posts will be ordered according to their ideal scores; put otherwise, IDEALSCORE$^M\left(\mathcal{P}_R\right)$ holds.

– (**SP** variable ⇒ no convergence) Let $\mathcal{P} = [(1, (a_1, \ldots, a_N)), (1, (b_1, \ldots, b_N)), (1, (0, \ldots, 0)), \ldots, (1,$ such that the following linear constraints are simultaneously feasible:

$$\sum_{i=1}^{N} a_i > \sum_{i=1}^{N} b_i$$
$$\sum_{i=1}^{N} \mathrm{SP}_i a_i < \sum_{i=1}^{N} \mathrm{SP}_i b_i$$

I think that's always possible if SP is not constant.

– (inequality doesn't hold ⇒ no convergence) Suppose that

$$R - 1 < (M-1)\left\lceil \frac{a+b}{\mathrm{regen}} \right\rceil \tag{4}$$
$$\text{and } \forall i \in [N], \mathbf{SP}_i = c \ .$$

If $R < M$, we consider two cases:

- $$\mathrm{attSpan} + R \leq M \tag{5}$$

  In this case, no player can ever vote for the last post, as we will show now. Let $\mathrm{pid} \in N, i \in [R]$ and v_i the index of the last post that has ever been in u_{pid}'s attention span until the end of round i. It is $v_1 = \mathrm{attSpan}$ and $\forall i \in [R] \setminus \{1\}, v_i = v_{i-1} + 1$, since in every round u_{pid} votes for a single post and the first unvoted post of the list is added to their attention span. Note that, since this mechanism is the same for all players, the same unvoted post is added to all players' attention span at every round. Thus $v_R = \mathrm{attSpan} + R - 1 \overset{(5)}{<} M$. We deduce that u_{pid} never has the chance to vote for the last post.

  The above observation naturally leads us to the following counterexample: Let

$$\mathrm{strongPost} = \left(1, \left(\underbrace{1, \ldots, 1}_{N}\right)\right)$$
$$\mathrm{nullPost} = \left(1, \left(\underbrace{0, \ldots, 0}_{N}\right)\right)$$
$$\mathcal{P} = \left[\underbrace{\mathrm{nullPost}, \ldots, \mathrm{nullPost}}_{M-1}, \mathrm{strongPost}\right]$$

$\forall i \in [M-1]$, it is $\mathrm{idealSc}(\mathcal{P}[M]) > \mathrm{idealSc}(\mathcal{P}[M])$, thus $\forall \mathcal{P}'$ that contain the same posts as $\mathcal{P}$ and $\textsc{Ideal}^1(\mathcal{P}')$ holds, it is $\mathcal{P}'[1] = \mathcal{P}[M]$. However, since the last post is not voted by any player and the first post is voted by at least one player, it is $\mathrm{sc}_R(\mathcal{P}[1]) > \mathrm{sc}_R(\mathcal{P}[M])$, thus $\textsc{Ideal}^1(\mathcal{P}_R)$ does not hold.

- $\mathrm{attSpan} + R > M$
  TODO

Assume $R \geq M$. In this case, all posts receive a vote by all players. Consider $\mathcal{P}^1 = 1^{M \times N}$ and $\mathrm{pid} \in [N]$. Let

$$i \in [M] : \left(\mathbf{VP}\mathrm{reg}_{\mathrm{pid},r_i} < 1 \land \nexists i' < i : \mathbf{VP}\mathrm{reg}_{\mathrm{pid},r_{i'}} < 1\right) \quad ,$$

i.e. i is the first round in which u_{pid} votes with less than full voting power. Since the first round is a voting round and the voting power of all players is full, it is $i \geq 2$. Such a round exists for the following reason:
If $\nexists i \in [M] : \left(\mathbf{VP}\mathrm{reg}_{\mathrm{pid},r_i} < 1 \land \nexists i' < i : \mathbf{VP}\mathrm{reg}_{\mathrm{pid},r_{i'}} < 1\right)$, then $\forall i \in [M], \mathbf{VP}\mathrm{reg}_{\mathrm{pid},r_i} = 1 \Rightarrow \forall i \in [M] \setminus \{1\}, r_i \geq r_{i-1} + \left\lceil \frac{a+b}{\mathrm{regen}} \right\rceil$ to have enough rounds to replenish the voting power after a full-weight, full-voting power vote. Thus $r_M \geq 1 + (M-1)\left\lceil \frac{a+b}{\mathrm{regen}} \right\rceil > R$, contradiction. Since all players follow the same voting pattern, the voting power of all players in each round is the same. Let $\mathrm{rVP} = \mathbf{VP}\mathrm{reg}_{1,r_i}$. For now assume $2|N$ and $\mathrm{attSpan} < i \vee i > 2$. TODO: prove rest. Let $0 < \gamma < 1$ and $0 < \epsilon < \gamma \frac{N-3}{N-1}(1 - \mathrm{rVP})$.

$$\mathrm{weakPost} = \left(1, \left(\underbrace{1, \dots, 1}_{N/2}, \underbrace{\gamma - \epsilon, \dots, \gamma - \epsilon}_{N/2}\right)\right) \quad ,$$

$$\mathrm{strongPost} = \left(1, \left(\underbrace{\gamma, \dots, \gamma}_{N/2}, \underbrace{1, \dots, 1}_{N/2}\right)\right) \quad ,$$

$$\mathrm{nullPost} = \left(1, \left(\underbrace{0, \dots, 0}_{N}\right)\right) \quad ,$$

$$\mathcal{P} = \left[\underbrace{\mathrm{weakPost}, \dots, \mathrm{weakPost}}_{i-1}, \mathrm{strongPost}, \underbrace{\mathrm{nullPost}, \dots, \mathrm{nullPost}}_{M-i}\right] \quad .$$

First of all, it is $\forall j \in [i-1], \mathrm{idealSc}(\mathcal{P}[j]) = \frac{N}{2}(1 + \gamma - \epsilon) < \frac{N}{2}(1 + \gamma) = \mathrm{idealSc}(\mathcal{P}[i])$ and $\forall j \in \{i+1, \dots, M\}, \mathrm{idealSc}(\mathcal{P}[j]) = 0 < \mathrm{idealSc}(\mathcal{P}[i])$, thus the strong post has strictly the highest ideal score of all posts and as a result, $\forall \mathcal{P}'$ that contains the same posts as $\mathcal{P}$ and $\textsc{Ideal}^1(\mathcal{P}')$ holds, it is $\mathcal{P}'[1] = \mathcal{P}[i]$.

We observe that all players like both weak and strong posts more than null posts, thus no player will vote for a null post unless her attention span contains only null posts. This can happen in two cases: First, if the player has not yet voted for all non-null posts, but the first attSpan posts of the list, excluding already voted posts, are null posts. Second, if the player has already voted for all non-null posts. For a null post to rank higher than a non-null one, it must be true that there exists one player that has cast the first vote for the null post. However, since the null posts are initially at the bottom of the list and it is impossible for a post to improve its ranking before it is voted, we deduce that this first vote can be cast only after the voter has voted for all non-null posts. We deduce that all players vote for all non-null posts before voting for any null post.

We will now see that the first $\frac{N}{2}$ players vote first for all weak posts and then for the strong post. These players like the weak posts more than the strong post. As we saw, they will not vote any null post before voting for all non-null ones. If $\text{attSpan} > 1$ they vote for the strong post only when all other posts in their attention span are null ones and thus they will have voted for all weak posts already. If $\text{attSpan} = 1$ and since no post can increase its position before being voted, the strong post will become "visible" for all players only once they have voted for all weak posts. Thus in both cases the first $\frac{N}{2}$ players vote for the strong post only after they have voted for all weak posts first.

The two previous results combined prove that the first $\frac{N}{2}$ players vote for the strong post in round r_i exactly. We also observe that these players have experienced the exact same voting power reduction and regeneration as in the case of $\mathcal{P}^1$ since they voted only for posts with likeability 1, thus in round r_i their voting power after regeneration is exactly the same as in the case of $\mathcal{P}^1 : \forall \text{pid} \in \left[\frac{N}{2}\right], \mathbf{VP}\text{reg}_{\text{pid},r_i} = \text{rVP}$.

We observe that the first $\frac{N}{2}$ players vote for all weak posts with full voting power. As for the last $\frac{N}{2}$ players, we observe that, if $\text{attSpan} < i$, they all vote for the first weak post of the list in the first round, and thus with full voting power. If $\text{attSpan} \geq i$ and $i > 2$, they vote for the strong post in the first round and for the first weak post in r_2 with full voting power. Thus in all cases the last $\frac{N}{2}$ players vote for the first weak post with full voting power. Therefore, the score of the first weak post at the end of the execution is $\mathrm{sc}_R\left(\mathcal{P}\left[1\right]\right) = c\left(\frac{N}{2}\left(a+b\right)+\frac{N}{2}\left(\left(\gamma-\epsilon\right)a+b\right)\right)$.

On the other hand, at the end of the execution the strong post has been voted by the first $\frac{N}{2}$ players with rVP voting power and by the last $\frac{N}{2}$ players with at most full voting power, thus its final score will be at most $\mathrm{sc}_R\left(\mathcal{P}\left[i\right]\right) \leq c\left(\frac{N}{2}\left(\mathrm{rVP}\cdot\gamma a+b\right)+\frac{N}{2}\left(a+b\right)\right)$. It is

$$\epsilon < \gamma\left(1-\mathrm{rVP}\right) \Rightarrow$$
$$c\left(\frac{N}{2}\left(a+b\right)+\frac{N}{2}\left(\left(\gamma-\epsilon\right)a+b\right)\right) < c\left(\frac{N}{2}\left(\mathrm{rVP}\cdot\gamma a+\frac{N}{2}\left(a+b\right)\right)\right) \Rightarrow$$
$$\mathrm{sc}_R\left(\mathcal{P}\left[i\right]\right) < \mathrm{sc}_R\left(\mathcal{P}\left[1\right]\right) \quad .$$

Thus $\mathcal{P}_R\left[1\right] \neq \mathcal{P}\left[i\right]$ and $\mathrm{Ideal}^1\left(\mathcal{P}_R\right)$ does not hold.

As for the case when N is odd, we can simply assume that the likeability of the first i posts (weak and strong) for the last player is γ, whereas the likeability of the last $M-i$ posts (the null posts) is 0. This means that the first player votes first for the weak and strong posts and then for the null posts. We observe that the ideal score of the strong post is still strictly higher than the rest. We have the following changes:

$$\mathrm{sc}_R\left(\mathcal{P}\left[i\right]\right) \leq c\left(\frac{N-1}{2}\left(\mathrm{rVP}\cdot\gamma a+b\right)+\frac{N-1}{2}\left(a+b\right)+\gamma a+b\right) \quad ,$$
$$\mathrm{sc}_R\left(\mathcal{P}\left[1\right]\right) \geq c\left(\frac{N-1}{2}\left(a+b\right)+\frac{N-1}{2}\left(\left(\gamma-\epsilon\right)a+b\right)+\mathrm{rVP}\cdot\gamma a+b\right) \quad .$$

For the strong post to have strictly lower score than the first weak one, it must hold that

$$\epsilon < \gamma\frac{N-3}{N-1}\left(1-\mathrm{rVP}\right) \quad .$$

$\square$

The above result is tight. If the conditions are violated the above theorem is not true.

4 Results

Steem won't achieve high quality posts.

5 Further Work

Posts at any time

6 Conclusion

Keep inventing new decentralized content curation platforms.

7 Acknowledgements

We thank @seriousposter for their invaluable posts analyzing Steem and our mums for the cookies.

References

1. Askalidis G., Stoddard G.: A theoretical analysis of crowdsourced content curation. In The 3rd Workshop on Social Computing and User Generated Content: vol. 16 (2013)
2. Ghosh A., McAfee P.: Incentivizing high-quality user-generated content. In Proceedings of the 20th international conference on World wide web: pp. 137–146: ACM (2011)
3. Das Sarma A., Das Sarma A., Gollapudi S., Panigrahy R.: Ranking mechanisms in twitter-like forums. In Proceedings of the third ACM international conference on Web search and data mining: pp. 21–30: ACM (2010)
4. Gupte M., Hajiaghayi M., Han L., Iftode L., Shankar P., Ursu R. M.: News posting by strategic users in a social network. In International Workshop on Internet and Network Economics: pp. 632–639: Springer (2009)
5. Lindell Y., Katz J.: Introduction to modern cryptography. Chapman and Hall/CRC (2014)
6. Arrow K. J.: A difficulty in the concept of social welfare. Journal of political economy: vol. 58(4), pp. 328–346 (1950)
7. Leskovec J., Huttenlocher D. P., Kleinberg J. M.: Governance in social media: A case study of the wikipedia promotion process. In ICWSM: pp. 98–105 (2010)
8. Forte A., Bruckman A.: Scaling consensus: Increasing decentralization in Wikipedia governance. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual: pp. 157–157: IEEE (2008)
9. Philip Daian Tyler Kell I. M., Juels A.: On-Chain Vote Buying and the Rise of Dark DAOs. http://hackingdistributed.com/2018/07/02/on-chain-vote-buying/ Accessed: 2018-09-06. (2018)