Analysis and Attacks of decentralized content curation platforms

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

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

Abstract. We will attack Steem.

1 Introduction

Steem is not incentive-compatible.

2 Related Work

Many people have done many similar things.

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.

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* $\text{creator}_j \in [N], l_j \in [0,1]^N$ *and* $p_j = (\text{creator}_j, l_j)$. *The set of all posts is* $\mathcal{P} = \bigcup\limits_{j=1}^{M} \{p_j\}$.

Definition 2 (Post score). *Let post* $p = (m, l)$. *We define the* score *of* p *as* $\text{sc}(p) = \sum\limits_{i=1}^{N} l_i$.

The 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 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*

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

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:*

$\mathcal{G}_{\text{Feed}}$ *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* $\mathcal{G}_{\text{Feed}}$ *whenever it receives* (`activate`) *from* $\mathcal{E}$.

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

Initialization:
  $\forall i \in |\mathcal{P}|$, Parse $\mathcal{P}[i]$ as $(\text{creator}_i, l_i)$
  Assert$(\forall i \in |\mathcal{P}|, |l_i| = N)$
  $N \leftarrow |l_1|$
  $\mathcal{U} \leftarrow \emptyset$
  $\textsc{Init}\,(\text{initArgs})$

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

Upon receiving (`vote`, ballot) from u_{pid}:
  $\mathcal{U} \leftarrow \mathcal{U} \cup u_{\text{pid}}$
  if $|\mathcal{U}| > N$ **then**
    Abort
  end if
  $\textsc{HandleVote}(\text{ballot})$

Algorithm 2 $\Pi_{\text{honest}}\left(\textsc{Vote}\right)(\text{initArgs})$

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

Definition 5 (t-convergence under honesty). *We say that a post-voting system $\mathcal{S} = (\mathcal{G}_{\text{Feed}}, \Pi_{\text{honest}})$* t-converges under honesty *if, for every valid input $\mathcal{P}$, for every $\mathcal{E}$ and given that all protocols execute Π_{honest}, eventually $\mathcal{G}_{\text{Feed}}$ sends a single message (`output`, $\mathcal{P}$) to $\mathcal{E}$ such that $\textsc{Ideal}^t\,(\mathcal{P})$ holds.*

Definition 6 (Steem system). *The Steem system is the post voting system $\mathcal{S}$ with parameters $\boldsymbol{SP} \in {\mathbb{N}^*}^N, R \in \mathbb{N}^*, a, b, \text{regen} \in \mathbb{R}_+, \text{attSpan} \in \mathbb{N}^*$ and the following parametrizing procedures:*

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

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

Algorithm 4 Aux

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

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

if $\text{lastVoted}_{\text{pid}} \neq r$ **then** ▷ One vote per player per round
    $\mathbf{VP}_{\text{pid}} \leftarrow \max \{\mathbf{VP}_{\text{pid}} + \text{regen} \cdot (r - \text{lastVoted}_{\text{pid}}), 1\}$
    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
    $\mathcal{P} \leftarrow \text{Order}(\mathcal{P}, \text{scores})$ ▷ order posts by votes
    if $r = R$ **then**
        Send $(\texttt{output}, \mathcal{P})$ to $\mathcal{E}$
        Halt
    else
        $r \leftarrow r + 1$
    end if
end if

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

Store aux contents as constants
if VOTETHISROUND $(r, R) = \text{yes}$ **then**
  top $\leftarrow$ CHOOSETOPPOSTS $(\text{attSpan}, \mathcal{P}, \text{votedPosts})$
  $(i, l) \leftarrow \underset{(i,l)\in\text{top}}{\text{argmax}} \{l_{\text{pid}}\}$
  $\text{votedPosts} \leftarrow \text{votedPosts} \cup (i, l)$
  return $((i, l), l_{\text{pid}})$
else
  return null
end if

function CHOOSETOPPOSTS$(\text{attSpan}, \mathcal{P}, \text{votedPosts})$
  $\text{res} \leftarrow \emptyset$
  $\text{idx} \leftarrow 1$
  while $|\text{res}| < \text{attSpan}\ \ \&\ \ \text{idx} \leq |\mathcal{P}|$ **do**
    if $\mathcal{P}[\text{idx}] \notin \text{votedPosts}$ **then** ▷ One vote per post per player
      $\text{res} \leftarrow \text{res} \cup \{\mathcal{P}[\text{idx}]\}$
    end if
    $\text{idx} \leftarrow \text{idx} + 1$
  end while
  return res
end function

function VOTETHISROUND$(r, R, |\mathcal{P}|)$
  Let choices be a vector of length R, with each element in $\{0, 1\}$. The vector choices is such that, if the player votes only on the rounds R when $\text{choices}_r = 1$ and the weight of all votes is 1, then the total player's "influence" will be maximized.
  Or simply allow voting when either voting power is full or in evenly spread out moments. (This strategy may actually achieve the above.)
  return choices_r
end function

Theorem 1. *The Steem system never converges.*

Discussion

- **SP** has to be constant, i.e. all players should have the same money. Otherwise let $\mathcal{P} = ((1, (a_1, \ldots, a_N)), (2, (b_1, \ldots, b_n)))$ such that the following linear constraints are simultaneously feasible:

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

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

- If players have attention span smaller than the full list and do not have the rounds to vote for every post, make a $\mathcal{P}$ with the best post at the end and it will stay there.
- If players must vote without full voting power but have the time to vote for all posts, we again place the good posts at the end. Players will vote for them with little voting power and they will not rise to the top.
- For $|\mathcal{P}|$-convergence, we need every player to vote for all posts with full voting power, i.e. $R - 1 \geq (|\mathcal{P}| - 1) \left\lceil \frac{a+b}{\text{regen}} \right\rceil$. But we can simply send a huge $\mathcal{P}$.

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