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

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

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*

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

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:*

$\mathcal{G}_{\text{Feed}}$ *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* 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 $\mathcal{G}_{\text{Feed}}(\textsc{Init}, \textsc{Aux}, \textsc{HandleVote})(\mathcal{P}, \text{initArgs})$

Initialization:
    $\mathcal{U} \leftarrow \emptyset$
    Init (initArgs)

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

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

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

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

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

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

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

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* $\text{msgs} = \left(\texttt{act}_{\text{pid}_1}, \ldots, \texttt{act}_{\text{pid}_n} \right)$ *sequentially. We say that* $\mathcal{E}$ respects $\text{ExecPat}_{N,R}$ *if* $\text{msgs} \in \text{ExecPat}_{N,R}$. *(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* $\text{ExecPat}_{N,R}$ *and given that all protocols execute* Π_{honest}*, it holds that after* $\mathcal{E}$ *completes its execution pattern,* $\mathcal{G}_{\text{Feed}}$ *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 $\text{ExecPat}_{N,R}$ and the following ...".

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

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

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

Algorithm 4 AUX

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

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

1: **if** $\text{lastVoted}_{\text{pid}} \neq r$ **then** ▷ One vote per player per round
2: $\mathbf{VP}_{\text{pid},r} \leftarrow \mathbf{VP}_{\text{pid}}$ ▷ For proofs
3: $\mathbf{VP}_{\text{pid}} \leftarrow \max\left\{\mathbf{VP}_{\text{pid}} + \text{regen} \cdot (r - \text{lastVoted}_{\text{pid}}), 1\right\}$ ▷ TODO: Remove $(r - \text{lastVoted}_{\text{pid}})$?
4: **if** $\text{ballot} \neq$ **null then**
5: Parse ballot as (p, weight)
6: $\text{cost} \leftarrow a \cdot \mathbf{VP}_{\text{pid}} \cdot \text{weight} + b$
7: **if** $\mathbf{VP}_{\text{pid}} - \text{cost} \geq 0$ **then**
8: $\text{score} \leftarrow \text{cost} \cdot \mathbf{SP}_{\text{pid}}$
9: $\mathbf{VP}_{\text{pid}} \leftarrow \mathbf{VP}_{\text{pid}} - \text{cost}$
10: **else**
11: $\text{score} \leftarrow \mathbf{VP}_{\text{pid}} \cdot \mathbf{SP}_{\text{pid}}$
12: $\mathbf{VP}_{\text{pid}} \leftarrow 0$
13: **end if**
14: $\text{scores}_p \leftarrow \text{scores}_p + \text{score}$
15: **end if**
16: $\text{lastVoted}_{\text{pid}} \leftarrow r$
17: **end if**
18: **if** $\forall i \in [N], \text{lastVoted}_i = r$ **then** ▷ round over
19: $\mathcal{P} \leftarrow \text{ORDER}(\mathcal{P}, \text{scores})$ ▷ order posts by votes
20: $\mathcal{P}_r \leftarrow \mathcal{P}$ ▷ For proofs
21: $r \leftarrow r + 1$
22: **end if** ▷ TODO: count rounds? simplify with set of voted and check of length?

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

Store aux contents as constants
if VOTETHISROUND $(r) =$ yes **then**
    top $\leftarrow$ CHOOSETOPPOSTS (attSpan, $\mathcal{P}$, votedPosts)
    $(i, l) \leftarrow \underset{(i,l)\in \text{top}}{\text{argmax}} \{l_{\text{pid}}\}[1]$
    votedPosts $\leftarrow$ votedPosts $\cup (i, l)$
    return $((i, l), l_{\text{pid}})$
else
    return null
end if

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

function VOTETHISROUND$(r, |\mathcal{P}|)$
    if $R < |\mathcal{P}|$ **then**
        return yes
    else if $\left\lfloor (r-1) \mod \frac{R-1}{|\mathcal{P}|-1} \right\rfloor = 0$ **then** ▷ TODO: if Discussion above is accepted, change $|\mathcal{P}|$ to M and don't input $|\mathcal{P}|$.
        return yes
    else
        return no
    end if
end function

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

Discussion

– 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.

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 VoteThis-Round 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:

$$(1) \Rightarrow \frac{R-1}{M-1} \geq \left\lceil \frac{a+b}{\text{regen}} \right\rceil \underset{\text{integer}}{\overset{\text{rhs}}{\Rightarrow}} \left\lfloor \frac{R-1}{M-1} \right\rfloor \geq \left\lceil \frac{a+b}{\text{regen}} \right\rceil \ , \tag{2}$$
$$\forall i \in [M] \setminus \{1\}, r_i \in \left\{ r_{i-1} + \left\lfloor \frac{R-1}{M-1} \right\rfloor, r_{i-1} + \left\lceil \frac{R-1}{M-1} \right\rceil \right\} \ . \tag{3}$$

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 6) 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 3), 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 19). We observe that

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

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

– (**SP** variable ⇒ no convergence) Let $\mathcal{P} = ((1, (a_1, \ldots, a_N)), (2, (b_1, \ldots, b_N)))$ such that the following linear constraints are simultaneously feasible:

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

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

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

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

Let $\mathcal{P} = \left[\left(1, \underbrace{(0.5, \ldots, 0.5)}_{N}\right), \ldots, \left(1, \underbrace{(0.5, \ldots, 0.5)}_{N}\right), \left(1, \underbrace{(0.5, \ldots, 0.5, 0.5+\epsilon)}_{N}\right), \right]$.
Observe that $\forall i \in [M-1], \text{idealSc}(\mathcal{P}[i]) = 0.5N < 0.5N + \epsilon = \text{idealSc}(\mathcal{P}[M])$, thus $\forall \mathcal{P}'$ that contains the same posts as $\mathcal{P}$ and $\textsc{Ideal}^1(\mathcal{P}')$ holds, it is $\mathcal{P}'[1] = \mathcal{P}[M]$.

- $R < M \wedge \text{attSpan} < M$
  At the end of the execution all players will have voted for $\mathcal{P}[1]$ in the first round, and thus $\text{scores}_{\mathcal{P}[1]} = Nc(0.5a+b)$. On the other hand, $\mathcal{P}[M]$ will have been voted by at most u_N with voting power $\text{VP} \leq 1 - (0.5a+b) + \text{regen}$, thus
  $\text{scores}_{\mathcal{P}[M]} \leq c((1-(0.5a+b)+\text{regen})(0.5+\epsilon)a+b) \overset{\text{regen}<b}{<} c((0.5+\epsilon)a+b)$.
  Thus $\text{scores}_{\mathcal{P}[1]} > \text{scores}_{\mathcal{P}[M]} \Leftrightarrow (N-1)\left(0.5+\frac{b}{a}\right) > \epsilon$. TODO: choose ϵ and show non-convergence
- $R < M \wedge \text{attSpan} = M$
  At the end of the execution, all players except for u_N will have voted for $\mathcal{P}[1]$ in the first round, and thus $\text{scores}_{\mathcal{P}[1]} \geq (N-1)c(0.5a+b)$. On the other hand, $\mathcal{P}[M]$ will have been voted by exactly u_N and this vote will have been cast on the first round, thus $\text{scores}_{\mathcal{P}[M]} = c((0.5+\epsilon)a+b)$. Thus $\text{scores}_{\mathcal{P}[1]} > \text{scores}_{\mathcal{P}[M]} \Leftrightarrow (N-2)\left(0.5+\frac{b}{a}\right) > \epsilon$. TODO: choose ϵ and show non-convergence
- $R \geq M \wedge \text{attSpan} < M$
  In this case, all players vote for all posts. At the end of the execution all players will have voted for $\mathcal{P}[1]$ in the first round, and

thus $\text{scores}_{\mathcal{P}[1]} = Nc\left(0.5a + b\right)$. As far as $\mathcal{P}\left[M\right]$ is concerned, we first observe that the distance between to voting rounds is $\left\lceil \frac{R-1}{M-1} \right\rceil$ at most: $\forall i \in \left[M-1\right], r_{i+1} - r_i \leq \left\lceil \frac{R-1}{M-1} \right\rceil$. Thus the voting power of all players will be at most $\text{regen}\left\lfloor \frac{R-1}{M-1} \right\rfloor$ before voting for the last post. We deduce that $\text{scores}_{\mathcal{P}[M]}$
will have been voted by all players except for u_N with voting power at most

- $R \geq M \wedge \text{attSpan} = M$

On the other hand,

- Let $\text{attSpan} < M$.
  - If $R < M$, then

  the first post $\mathcal{P}\left[1\right]$ is voted by all players at round 1 and its score becomes $Nc\left(0.5a + b\right)$. Given (4), all subsequent votes are cast with voting power strictly less than 1, thus the last post will have a score of $\left(N-1\right)c\left(0.5a? + b\right) + c\left(\left(0.5 + \epsilon\right)a? + b\right)$ at the end of the execution.
- If $\text{attSpan} = M$,

□

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)