A Puff of Steem: Security Analysis of Decentralized Content Curation

Aggelos Kiayias[1,2], Benjamin Livshits[3,4], Andrés Monteoliva Mosteiro[1,5], and Orfeas Stefanos Thyfronitis Litos[1]

[1] University of Edinburgh
[2] IOHK
[3] Imperial College of London
[4] Brave Software
[5] Clearmatics
akiayias@inf.ed.ac.uk, ben@brave.com, amonteolivam@gmail.com,
o.thyfronitis@ed.ac.uk

Abstract. Decentralized content curation is the process through which uploaded posts are ranked and filtered based exclusively on users' feedback. Platforms such as the blockchain-based Steemit[6] employ this type of curation while providing monetary incentives to promote the visibility of high quality posts according to the perception of the participants. Despite the wide adoption of the platform very little is known regarding its performance and resilience characteristics. In this work, we provide a formal model for decentralised content curation that identifies salient complexity and game-theoretic measures of performance and resilience to selfish participants. Armed with our model, we provide a first analysis of Steemit identifying the conditions under which the system can be expected to correctly converge to curation while we demonstrate its susceptibility to selfish participant behaviour. We validate our theoretical results with system simulations in various scenarios.

1 Introduction

The modern Internet contains an immense amount of data; a single user can only consume a tiny fraction in a reasonable amount of time. Therefore, any widely used platform that hosts user-generated content must employ a content curation mechanism. Content curation can be understood as the set of mechanisms which rank, aggregate and filter relevant information. In recent years, popular news aggregation sites like Reddit[7] or Hacker News[8] have established crowdsourced curation as the primary way to filter content for their users. Crowdsourced content curation, as

[6] https://steemit.com/ Accessed: 2018-09-10
[7] https://www.reddit.com/ Accessed: 2018-09-10
[8] https://news.ycombinator.com/ Accessed: 2018-09-10

opposed to more traditional techniques such as expert- or algorithmic-based curation, orders and filters content based on the ratings and feedback of the users themselves, obviating the need for a central moderator by leveraging the wisdom of the crowd [1].

The decentralized nature of crowdsourced curation makes it a suitable solution for ranking user-generated content in blockchain-based content hosting systems. The aggregation and filtering of user-generated content emerges as a particularly challenging problem in permissionless blockchains, as any solution that requires a concrete moderator implies that there exists a privileged party, which is incompatible with a permissionless blockchain. Moreover, public blockchains are easy targets for Sybil attacks, as any user can create new accounts at any time for a marginal cost. Therefore, on-chain mechanisms to resist the effect of Sybil users are necessary for a healthy and well-functioning platform; traditional counter-Sybil mechanisms [2] are much harder to apply in the case of blockchains due to the decentralized nature of the latter. The functions performed by moderators in traditional content platforms need to be replaced by incentive mechanisms that ensure self-regulation. Having the impact of a vote depend on the number of coins the voter holds is an intuitively appealing strategy to achieve a proper alignment of incentives for users in decentralized content platforms; specifically, it can render Sybil attacks impossible. However, the correct design of such systems is still an unsolved problem. Blockchains have created a new economic paradigm where users are at the same time equity holders in the system, and leveraging this property in a robust manner constitutes an interesting challenge. A variety of projects have designed decentralized content curation systems [3,4,5]. However, a deep understanding of the properties of such systems is still lacking.

In the current work, we develop a theoretical model of a post-voting system which sorts the posts created by users in a distributed and crowdsourced manner. Our model is constituted by N players who contribute votes in a round-based curation process. The impact of each vote depends on the number of coins held by the player. The posts are arranged in a list, sorted by the value of votes received, resembling the front-page model of Reddit or Hacker News. In the model, players vote according to their subjective opinion on the quality of the posts and have a limited attention span attSpan. Following previous academic work, we represent each player's opinion on each post (i.e. likability) with a numerical value $n \in [0, 1]$ [6,1]. The objective quality of a post will be calculated as the simple summation of all players' likabilities for the post in question. To measure the properties of such a post-voting system, we say that the system *t-converges* if the t first articles are ordered according to the objective quality of the posts at the end of the execution. After defining and formalizing an abstract post-voting system, we particularize it to model Steemit, a social media platform based on the Steem blockchain. We prove the conditions under which Steemit t-converges and then we develop a simulation to help us parametrize Steemit according to our post-voting model. Our analysis of the post-voting system of Steemit aims to provide a useful framework to aid the design of future decentralized curation platforms.

Our Contributions.

- Original treatment following cryptography and simulation-based techniques to model crowdsourced content curation, in opposition to previous academic work which have leaned more towards an analytical and game-theoretic approach.
- Taking in account of subjective likeabilities, the effect of rounds and an agnostic likeability distribution treatment.
- Measurement of the influence of coin-holding (wealth-distribution) in the effectivity of post sorting. New paradigm present in blockchain based systems (main difference with Reddit-like platforms.)
- Proof that Steem does not t-converge with the parameters currently used in their implementation. Insights to improve the curation quality of the trending section of steem.
- (Maybe)Impact of the curation quality when greedy players are present in the system.

2 Related Work

User-generated content (UGC) has been identified as a fundamental part of social media platforms and the Web 2.0 [7]. The content created by users needs to be curated, and crowdsourced content curation [1] has emerged as an alternative to experts- [8] or algorithmic-based [9] curation techniques. Motivated by the widespread adoption of crowdsourced aggregation sites such as Reddit or Digg[9], several research efforts [10,6] have aimed to model the mechanics and incentives for users in UGC platforms. This academic interest is backed by parallel studies which have shown how social media users behave strategically when they publish and consume content [11]. As an example, in the case of Reddit, users try to maximize

[9] http://digg.com/ Accessed: 2018-09-10

their ‘karma’ [12], the social badge of the social media platform [13]. Therefore, most academic works in the field have analyzed content curation from an incentives and game-theoretic standpoint [6,10,14,11]. 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 [1,6]. In terms of measuring our results, our analysis of *t-convergence* is similar to the top-k posts in [1] but enforces an stricter similarity. Moreover, we adopt the statistical coefficients Kendall’s Tau and Spearman’s Rho [15,16] to measure content curation efficiency.

However, most importantly, our approach is different as we describe the mechanics of post-voting systems from a computational, rather than an analytic angle, drawing inspiration from the real-ideal world paradigm of Cryptography [17] in the definition of convergence. Avoiding a general game-theoretic approach, theoretical limitations such as the Arrow’s impossibility theorem [18] do not impact the outcomes of our work. Our analysis on post-voting systems brings our work close to the research area of voting mechanisms, within the field of social choice [19,20,21]. The study of voting rules has focused on the analysis of communication complexity and the accuracy of results when a single winner must be chosen. In contrast, we do not seek to investigate the election of one winner but analyze the curation quality of the entire list of items. Even though we share an iterative (i.e. rounds based) voting scheme with some of these works [22], we remark that our crowdsourced curation model has fundamentally different goals from election-like schemes of previous literature, making the two largely incomparable.

Content curation is also related with the concept of online governance. The governance of online communities such as Wikipedia has been thoroughly studied in previous academic work [23,24]. 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 [25,26]. Beyond the Steem blockchain, coin-holder voting systems are present in decentralized platforms such as DAOs [27] and in different blockchain protocols [28]. However, most of these systems use coin-holder voting processes to agree on a value or take a consensual decision. In the present work we do not tackle the issue of decentralized governance in the strictest sense. Nevertheless, given that the voting procedure as described here largely defines the state of the system, our results are intimately related to the topic of decentralized governance.

3 Model

3.1 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 $\{1, 2, \ldots, n\}$.

3.2 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 $\mathcal{P} = \bigcup\limits_{j=1}^{M} \{p_j\}$.

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

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:*

$\mathcal{G}_{\text{Feed}}$ 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.

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

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

```
Initialization:
    $\mathcal{U} \leftarrow \emptyset$                                        ▷ Set of players
    $\textsc{Init}\left(\text{initArgs}\right)$

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

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

Algorithm 2 $\mathit{\Pi}_{\text{honest}}\left(\textsc{Vote}\right)$

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

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

Definition 6 (Execution Pattern). *Let $N, R \in \mathbb{N}^*, N \geq 2$.*

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

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

Let Environment $\mathcal{E}$ that sends messages $\text{msgs} = \left(\texttt{act}_{\text{pid}_1}, \dots, \texttt{act}_{\text{pid}_n}\right)$ *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 $\mathrm{ExecPat}_{N,R}$ 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.*

Definition 8 (Steem system). *The Steem system is the post voting system $\mathcal{S}$ with parameters $\boldsymbol{SP} \in {\mathbb{N}^*}^N, a, b, \mathrm{regen} \in [0, 1] : a+b < 1, \left\lceil \frac{a+b}{\mathrm{regen}} \right\rceil > 1, \mathrm{attSpan} \in \mathbb{N}^*$. The parametrizing procedures can be found in Appendix B.*

Remark 1. The constraint $a + b < 1$ ensures that a single vote of full weight cast by a player with full voting power does not completely deplete her voting power. The constraint $\left\lceil \frac{a+b}{\mathrm{regen}} \right\rceil > 1$ excludes the degenerate case in which the regeneration of a single round is enough to fully replenish the voting power in all cases; in this case the purpose of voting power would be defeated.

Remark 2. The Steem blockchain protocol defines $a = 0.0001, b = 0.02, \mathrm{regen} = \frac{3}{5 \cdot 24 \cdot 60 \cdot 60} = 0.00000069\bar{4}$, thus $\left\lceil \frac{a+b}{\mathrm{regen}} \right\rceil = 2895$.

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

Proof Sketch. When $R - 1 \geq (M - 1) \left\lceil \frac{a+b}{\mathrm{regen}} \right\rceil$, there are enough rounds to ensure full regeneration of every player's voting power between two votes and thus the resulting post list reflects the true preferences of the players. In the opposite case, we can always craft a post list that exploits the fact that some votes are cast with reduced voting power in order to trick the system into placing a wrong post in the top position. □

The above result is tight. If the conditions are violated the above theorem is not true. See Appendix A for full proof.

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.

Appendix A Proof of Theorem 1: Steem convergence

Proof. – ($\Leftarrow$) Suppose that

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

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 $(r_1, \dots, r_M)$ with $r_i = \left\lfloor (i-1)\frac{R-1}{M-1} \right\rfloor + 1$. Observe that:

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

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

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 $i = 1, \mathbf{VP}_{\text{pid},1} = 1$ (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

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

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 $\in [N]$, it holds that at the end of the execution, all votes have been cast with full voting power, thus $\forall i \in [M], \mathrm{sc}_R(\mathcal{P}[i]) = c\left(Nb + a\sum\limits_{\mathrm{pid}=1}^{N}\mathcal{P}[i]_{\mathrm{pid}}\right)$ and the posts in $\mathcal{P}_R$ are sorted by decreasing score (Algorithm 5, line 20). We observe that

$$\forall i \neq j \in [M], \mathrm{idealSc}(\mathcal{P}[i]) > \mathrm{idealSc}(\mathcal{P}[j]) \Rightarrow$$
$$\sum_{\mathrm{pid}=1}^{N}\mathcal{P}[i]_{\mathrm{pid}} > \sum_{\mathrm{pid}=1}^{N}\mathcal{P}[j]_{\mathrm{pid}} \Rightarrow c\left(Nb + a\sum_{\mathrm{pid}=1}^{N}\mathcal{P}[i]_{\mathrm{pid}}\right) > c\left(Nb + a\sum_{\mathrm{pid}=1}^{N}\mathcal{P}[j]_{\mathrm{pid}}\right) \ .$$

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

- (**SP** variable ⇒ no convergence) Let $\mathcal{P} = [(1,(a_1,\dots,a_N)),(1,(b_1,\dots,b_N)),(1,(0,\dots,0)),\dots,(1,$ 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

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

Several lists of posts will be defined in the rest of the proof. Given that, when all players are honest, the creator of a post is irrelevant, we omit the creator from the definition of posts to facilitate the exposition. Thus every post will be defined as a tuple of likabilities.

First, we consider the case when

$$\mathrm{attSpan} + R \leq M \ . \qquad (5)$$

In this case, no player can ever vote for the last post, as we will show now. First of all, (5) ⇒ $R < M$, thus all players cast R votes in total. Let pid $\in N, i \in [R]$ and $v_{\mathrm{pid},i}$ the index of the last post that has ever been in u_{pid}'s attention span until the end of round i, according to the ordering of $\mathcal{P}$. It is $v_{\mathrm{pid},1} = \mathrm{attSpan}$ and $\forall i \in [R] \setminus \{1\}, v_{\mathrm{pid},i} =$

$v_{\mathrm{pid},i-1} + 1$, 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 $\forall \mathrm{pid} \in N, v_{\mathrm{pid},R} = \mathrm{attSpan} + R - 1 \overset{(5)}{<} M$. We deduce that no player has ever the chance to vote for the last post.

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

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

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

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

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

We now move on to the case when $\mathrm{attSpan} + R > M$. Let $V = \min\left\{R, M\right\}$. Each player casts exactly V votes. Consider $\mathcal{P}^1 = 1^{M \times N}$ and $\mathrm{pid} \in [N]$. Let

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

i.e. i is the first round in which u_{pid} votes with less than full voting power. Such a round exists in every case as we will show now. Note that, since the first round is a voting round and the voting power of all players is full at the beginning, if i exists it is $i \geq 2$.

- If $R \geq M$, it is $V = M$. If $\nexists i \in [M] : \left(\mathbf{VP}\mathrm{reg}_{\mathrm{pid},r_i} < 1 \wedge \nexists i' < i : \mathbf{VP}\mathrm{reg}_{\mathrm{pid},r_{i'}} < 1\right)$, then $\forall i \in \left[M\right], \mathbf{VP}\mathrm{reg}_{\mathrm{pid},r_i} = 1 \Rightarrow \forall i \in \left[M\right] \setminus \left\{1\right\}, r_i \geq r_{i-1} + \left\lceil \frac{a+b}{\mathrm{regen}} \right\rceil$ 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.

- If $R < M$, every player votes on all rounds, thus $r_2 = 2$. Note that

$$\left\lceil \frac{a+b}{\text{regen}} \right\rceil \geq 2 \Rightarrow \frac{a+b}{\text{regen}} > 1 \Rightarrow a+b > \text{regen} \ . \tag{6}$$

Thus $\forall \text{pid} \in [N], \mathbf{VP}\text{reg}_{\text{pid},r_2} = 1 - a - b + \text{regen} \overset{(6)}{<} 0$, thus $i = 2$. We proved that i exists. Since all players follow the same voting pattern, the voting power of all players in each round is the same. Let $\text{rVP} = \mathbf{VP}\text{reg}_{1,r_i}$. Assume that $\text{attSpan} < i \vee i > 2$. We cover the case where $\text{attSpan} \geq i \wedge i = 2$ later. In case N is even, let $0 < \gamma < 0, 0 < \epsilon < \gamma(1 - \text{rVP})$,

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

$$\text{strongPost} = \left(\underbrace{\gamma, \ldots, \gamma}_{N/2}, \underbrace{1, \ldots, 1}_{N/2} \right) \ ,$$

$$\text{nullPost} = \left(\underbrace{0, \ldots, 0}_{N} \right) \ ,$$

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

First of all, it is $\forall j \in [i-1], \text{idealSc}(\mathcal{P}[j]) = \frac{N}{2}(1 + \gamma - \epsilon) < \frac{N}{2}(1 + \gamma) = \text{idealSc}(\mathcal{P}[i])$ and $\forall j \in \{i+1, \ldots, M\}, \text{idealSc}(\mathcal{P}[j]) = 0 < \text{idealSc}(\mathcal{P}[i])$, 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 $\text{sc}_R\left(\mathcal{P}\left[1\right]\right) = c\left(\frac{N}{2}\left(a+b\right) + \frac{N}{2}\left(\left(\gamma-\epsilon\right)a+b\right)\right)$.

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 $\text{sc}_R\left(\mathcal{P}\left[i\right]\right) \leq c\left(\frac{N}{2}\left(\text{rVP}\cdot\gamma a+b\right) + \frac{N}{2}\left(a+b\right)\right)$. It is

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

Thus $\mathcal{P}_R[1] \neq \mathcal{P}[i]$ and $\text{Ideal}^1(\mathcal{P}_R)$ does not hold.
As for the case when N is odd, let $0 < \epsilon < \gamma\frac{N-3}{N-1}(1 - \text{rVP})$. In this case, we 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 last player votes first for the weak and strong posts and then for the null posts. The rest of the likabilities remain as in the case when N is even. We observe that the ideal score of the strong post is still strictly higher than the rest. Furthermore, since the last player votes for the first weak post within the first i voting rounds, her voting power at the time of this vote will be at least rVP. We thus have the following bounds for the scores:

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

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

Given the bounds of ϵ, it is $\text{sc}_R(\mathcal{P}[i]) < \text{sc}_R(\mathcal{P}[1])$, thus $\text{Ideal}^1(\mathcal{P}_R)$ does not hold.
We finally cover the previously untreated edge case where $\text{attSpan} \geq i \wedge i = 2$. rVP is defined like before. We first consider the case when N is even and greater than 2: $\exists k \in \mathbb{N} \setminus \{0, 1\} : N = 2k$. Let $0 < \gamma < 1, 0 < \epsilon < 2\gamma\frac{1-\text{rVP}}{(k-1)\text{rVP}}$,

$$\text{weakPost} = \left(\underbrace{1, \dots, 1}_{k-1}, \underbrace{\gamma - \epsilon, \dots, \gamma - \epsilon}_{k-1}, \gamma, \gamma\right) \quad ,$$

$$\text{strongPost} = \left(\underbrace{\gamma, \dots, \gamma}_{k-1}, \underbrace{1, \dots, 1}_{k-1}, \gamma, \gamma\right) \quad ,$$

$$\mathcal{P} = \left[\text{weakPost}, \text{strongPost}, \underbrace{\text{nullPost}, \dots, \text{nullPost}}_{M-2}\right] \quad .$$

We first observe that $\forall j \in \{3, \dots, M\}, \text{idealSc}(\mathcal{P}[j]) = 0 < \text{idealSc}(\mathcal{P}[1]) = k - 1 + (k-1)(\gamma - \epsilon) + 2\gamma = k - 1 + (k+1)\gamma - (k-1)\epsilon < k - 1 + (k+1)\gamma = \text{idealSc}(\mathcal{P}[2])$, 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 $\mathcal{P}'[1] = \mathcal{P}[2]$.

The first $k-1$ and the last two players vote first for $\mathcal{P}[1]$ and then for $\mathcal{P}[2]$, whereas players $k, \ldots, 2k-2$ vote first for $\mathcal{P}[2]$ and then for $\mathcal{P}[1]$, thus at the end of the execution,

$$\mathrm{sc}_R(\mathcal{P}[1]) = (k-1)(a+b) + 2(\gamma a + b) + (k-1)((\gamma - \epsilon)\,\mathrm{rVP}a + b) \quad ,$$
$$\mathrm{sc}_R(\mathcal{P}[2]) = (k-1)(a+b) + (k+1)(\gamma \mathrm{rVP}a + b) \quad .$$

Given the bound on ϵ, it is $\mathrm{sc}_R(\mathcal{P}[1]) > \mathrm{sc}_R(\mathcal{P}[2])$, thus $\mathrm{Ideal}^1(\mathcal{P}_R)$ does not hold.
Second, we consider the case when N is odd: $\exists k \in \mathbb{N} : N = 2k+1$. Let $0 < \gamma < 1, 0 < \epsilon < \gamma \frac{1-\mathrm{rVP}}{k\mathrm{rVP}}$,

$$\mathrm{weakPost} = \left(\underbrace{1, \ldots, 1}_{k}, \underbrace{\gamma - \epsilon, \ldots, \gamma - \epsilon}_{k}, \gamma\right) \quad ,$$
$$\mathrm{strongPost} = \left(\underbrace{\gamma, \ldots, \gamma}_{k}, \underbrace{1, \ldots, 1}_{k}, \gamma\right) \quad ,$$
$$\mathcal{P} = \left[\mathrm{weakPost}, \mathrm{strongPost}, \underbrace{\mathrm{nullPost}, \ldots, \mathrm{nullPost}}_{M-2}\right] \quad .$$

We first observe that $\forall j \in \{3, \ldots, M\}, \mathrm{idealSc}(\mathcal{P}[j]) = 0 < \mathrm{idealSc}(\mathcal{P}[1]) = k + k(\gamma - \epsilon) + \gamma = k + (k+1)\gamma - k\epsilon < k + (k+1)\gamma = \mathrm{idealSc}(\mathcal{P}[2])$, 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 $\mathcal{P}'[1] = \mathcal{P}[2]$.
The first k and the last player vote first for $\mathcal{P}[1]$ and then for $\mathcal{P}[2]$, whereas players $k+1, \ldots, 2k$ vote first for $\mathcal{P}[2]$ and then for $\mathcal{P}[1]$, thus at the end of the execution,

$$\mathrm{sc}_R(\mathcal{P}[1]) = k(a+b) + \gamma a + b + k((\gamma - \epsilon)\,\mathrm{rVP}a + b) \quad ,$$
$$\mathrm{sc}_R(\mathcal{P}[2]) = k(a+b) + (k+1)(\gamma \mathrm{rVP}a + b) \quad .$$

Given the bound on ϵ, it is $\mathrm{sc}_R(\mathcal{P}[1]) > \mathrm{sc}_R(\mathcal{P}[2])$, thus $\mathrm{Ideal}^1(\mathcal{P}_R)$ does not hold.
Last but not least, we consider the case when $N = 2$. In this case, let $0 < \gamma < 1$ and

$$\mathcal{P} = \left[(1, 0), \left(\gamma, 1 - \gamma \frac{1 + \mathrm{rVP}}{2}\right), \underbrace{\mathrm{nullPost}, \ldots, \mathrm{nullPost}}_{M-2}\right] \quad .$$

It is $\forall j \in \{3, \ldots, M\}, \mathrm{idealSc}\left(\mathcal{P}\left[j\right]\right) = 0 < \mathrm{idealSc}\left(\mathcal{P}\left[1\right]\right) = 1 \overset{\mathrm{rVP}<1}{<} 1 + \gamma \frac{1-\mathrm{rVP}}{2} = \gamma + 1 - \gamma \frac{1+\mathrm{rVP}}{2} = \mathrm{idealSc}\left(\mathcal{P}\left[2\right]\right)$, thus $\mathcal{P}\left[2\right]$ 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 $\textsc{Ideal}^1\left(\mathcal{P}'\right)$ holds, it is $\mathcal{P}'\left[1\right] = \mathcal{P}\left[2\right]$.

On the other hand, $\mathrm{sc}_R\left(\mathcal{P}\left[1\right]\right) = a+2b > \gamma \mathrm{rVP} a + b + \left(1 - \gamma \frac{1+\mathrm{rVP}}{2}\right) a + b = \mathrm{sc}_R\left(\mathcal{P}\left[2\right]\right)$, thus $\mathrm{Ideal}^1\left(\mathcal{P}_R\right)$ does not hold.

□

Appendix B Steem post voting system procedures

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

```
Store input parameters as constants
$r \leftarrow 1$
$\mathrm{lastVoted} \leftarrow (0, \ldots, 0) \in (\mathbb{N}^*)^N$
$\mathbf{VP} \leftarrow (1, \ldots, 1) \in [0, 1]^N$
$\mathrm{scores} \leftarrow (0, \ldots, 0) \in \left(\mathbb{R}^+\right)^M$
```

Algorithm 4 $\textsc{Aux}$

```
return $\left(\mathbf{SP}, \mathrm{attSpan}, a, b, r, \mathrm{regen}\right)$
```

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

```
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
    $\mathbf{VP}_{\text{pid}} \leftarrow \max\left\{\mathbf{VP}_{\text{pid}} + \text{regen} \cdot \left(r - \text{lastVoted}_{\text{pid}}\right), 1\right\}$    ▷ TODO: Remove $\left(r - \text{lastVoted}_{\text{pid}}\right)$?
    $\mathbf{VP}\text{reg}_{\text{pid},r} \leftarrow \mathbf{VP}_{\text{pid}}$    ▷ For proofs
    if ballot $\neq$ null then
        Parse ballot as $(p, \text{weight})$
        $\text{cost} \leftarrow a \cdot \mathbf{VP}_{\text{pid}} \cdot \text{weight} + b$
        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
    $\mathcal{P} \leftarrow \textsc{Order}\left(\mathcal{P}, \text{scores}\right)$    ▷ 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 Vote $(\mathcal{P}, \text{aux})$

```
Store aux contents as constants
voteRounds $\leftarrow$ VoteRounds $(R, |\mathcal{P}|)$
if VoteThisRound $(r, |\mathcal{P}|) = \text{yes}$ 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 $|\text{res}| < \text{attSpan}$ & $\text{idx} \leq |\mathcal{P}|$ do
        if $\mathcal{P}[\text{idx}] \notin \text{votedPosts}$ then          ▷ One vote per post per player
            res $\leftarrow \text{res} \cup \{\mathcal{P}[\text{idx}]\}$
        end if
        idx $\leftarrow$ idx $+ 1$
    end while
    return res
end function

function VoteThisRound($r, M$)
    if $R < M$ then
        return yes
    else if $r \in \text{voteRounds}$ then
        return yes
    else
        return no
    end if
end function

function VoteRounds($R, M$)
    voteRounds $\leftarrow \emptyset$
    for $i = 1$ to $M$ do
        voteRounds $\leftarrow \text{voteRounds} \cup \left\{1 + \left\lfloor (i-1)\,\frac{R-1}{M-1} \right\rfloor\right\}$
    end for
    return voteRounds
end function
```

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. Levine B. N., Shields C., Margolin N. B.: A survey of solutions to the sybil attack. University of Massachusetts Amherst, Amherst, MA: vol. 7, p. 224 (2006)
3. Konforty D., Adam Y., Estrada D., Meredith L. G.: Synereo: The Decentralized and Distributed Social Network. Self-published: https://pdfs.semanticscholar.org/253c/c4744e6b2b87f88e46188fe527982b19542e.pdf Accessed: 2018-08-04. (2015)
4. Steem Whitepaper. https://steem.io/steem-whitepaper.pdf Accessed: 2018-08-05. (2018)
5. Goldin M.: Token-Curated Registries 1.0. https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7 Accessed: 2018-08-13. (2017)
6. 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)
7. Kaplan A. M., Haenlein M.: Users of the world, unite! The challenges and opportunities of Social Media. Business horizons: vol. 53(1), pp. 59–68 (2010)
8. Stanoevska-Slabeva K., Sacco V., Giardina M.: Content Curation: a new form of gatewatching for social media. Documento electrónico. Recuperado el: vol. 16 (2012)
9. Rader E., Gray R.: Understanding user beliefs about algorithmic curation in the Facebook news feed. In Proceedings of the 33rd annual ACM conference on human factors in computing systems: pp. 173–182: ACM (2015)
10. 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)
11. May A., Chaintreau A., Korula N., Lattanzi S.: Filter & follow: How social media foster content curation. In ACM SIGMETRICS Performance Evaluation Review: vol. 42: pp. 43–55: ACM (2014)
12. Bergstrom K.: âĂIJDonâĂŹt feed the trollâĂİ: Shutting down debate about community expectations on Reddit. com. First Monday: vol. 16(8) (2011)
13. Anderson A., Huttenlocher D., Kleinberg J., Leskovec J.: Steering user behavior with badges. In Proceedings of the 22nd international conference on World Wide Web: pp. 95–106: ACM (2013)
14. 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)
15. Xu W., Hou Y., Hung Y., Zou Y.: A comparative analysis of Spearman's rho and Kendall's tau in normal and contaminated normal models. Signal Processing: vol. 93(1), pp. 261–276 (2013)
16. Yue S., Pilon P., Cavadias G.: Power of the Mann–Kendall and Spearman's rho tests for detecting monotonic trends in hydrological series. Journal of hydrology: vol. 259(1-4), pp. 254–271 (2002)
17. Lindell Y., Katz J.: Introduction to modern cryptography. Chapman and Hall/CRC (2014)
18. Arrow K. J.: A difficulty in the concept of social welfare. Journal of political economy: vol. 58(4), pp. 328–346 (1950)
19. Lu T., Boutilier C.: Robust approximation and incremental elicitation in voting protocols. In IJCAI: vol. 1: pp. 287–293 (2011)
20. Conitzer V., Sandholm T.: Communication complexity of common voting rules. In Proceedings of the 6th ACM conference on Electronic commerce: pp. 78–87: ACM (2005)

21. Xia L., Conitzer V.: Compilation Complexity of Common Voting Rules. In AAAI (2010)
22. Kalech M., Kraus S., Kaminka G. A., Goldman C. V.: Practical voting rules with partial information. Autonomous Agents and Multi-Agent Systems: vol. 22(1), pp. 151–182 (2011)
23. 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)
24. 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)
25. Buterin V.: Notes on Blockchain Governance. https://vitalik.ca/general/2017/12/17/voting.html Accessed: 2018-09-04. (2017)
26. Ehrsam F.: Blockchain Governance: Programming Our Future. https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74 Accessed: 2018-09-03. (2017)
27. 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)
28. Goodman L.: TezosâĂŤa self-amending crypto-ledger White paper. URL: https://www. tezos. com/static/papers/white_paper. pdf (2014)