# Rebuttal Letter

We would like to thank the reviewers for the thoughtful comments, questions, and criticism.

We accommodate all clarifications and answers in the final version of the paper.

The link that follows shows the *diff* to reach the final version:

- https://github.com/fsantanna-no/sbseg-23/compare/0145ec9d59ff2e1b4e1053505bf5614d63326166..b51a401cb67ece6857bd697f39df0ea428b0ba07?diff=split

Each comment is addressed individually as follows.

## Reviewer 1

> Quanto a solução, senti falta de alguma discussão sobre as limitações. Em especial, a falta de finalidade, i.e., um post pode ser excluído devido aos forks (no momento do merge). Este post poderia ser de um usuário legitimo ? quanto isso ocorre e quais as implicações?

Sim, para isso, ele teria que escrever em um fork "obscuro", desconectado do resto dos usuários legítimos. Dessa forma, ao ser reconectado, esse fork poderia sim ter posts removidos. A única implicação é que ele teria que postar novamente a mesma mensagem.

No meio da Seção 2.1, essa possibilidade é levantada, mas não com tanta ênfase:

> While applying the branches in order, if any post operation fails, all remaining posts are rejected and removed from the DAG, as if they never existed.

Em termos práticos, os usuários legítimos se conectam mais diretamente ao longo do tempo, o que deveria ser suficiente para evitar essa situação. Para a versão final, nós adicionamos o seguinte trecho:

> Legitimate posts in secondary branches might be removed due to merges, which requires that users repost the messages. Nevertheless, we expect that legitimate users gossip among themselves more often, thus preventing this situation.

---

> Além disso, é possível que um usuário malicioso participe de mais de uma cadeia em um fork? neste caso como fica a regra de merge? e se der empate, todos devem escolher o mesmo fork para começar, como isso seria feito?

A reputação de um usuário em uma cadeia X não é válida em uma cadeia Y. Portanto, interpretamos o comentário acima como "…participe de mais de um fork em uma mesma cadeia".

Sim, se o usuário malicioso dispor de 1 rep, ele pode escrever propositalmente em vários forks. Nesse caso, a reputação prévia dele vai contar igualmente em todos os merges, se anulando e, portanto, não influenciando no resultado final do merge.

Em caso de empate, que pode acontecer mesmo sem usuários maliciosos, o hash do fork será o critério considerado por todos igualmente. Esse critério é descrito no final da Seção 2.2:

> ...otherwise, branches use the arbitrary criteria of lexicographical order of the post hashes immediately after the common prefix.

Como um possível ataque, o usuário malicioso poderia escrever em vários branches antes de usuários legítimos, de forma que os merges acabariam por remover mensagens legítimas. Essa situação, que complementa o comentário anterior, obrigaria os usuários a repostarem as mensagens. Da mesma forma, nós entendemos que os usuários legítimos estarão mais conectados, inviabilizando esse tipo de ataque.

---

> Pela descrição, aparentemente na Figura 3 deveria ter uma transição de revoked para accepted.

A Figura 3 já tem essa transição. Há uma seta bi-direcional entre os dois estados. (Espero ter entendido corretamente esse comentário.)

## Reviewer 2

> It is strange that known techniques like EigenTrust are not even mentioned, even though we are in the blockchain domain.

We added a new paragraph at the end of Section 4 (Related Work), as follows:

> Some works for P2P file sharing propose to account the reputation of peers to form a web of trust based on their behavior history [Wang,EigenTrust]. However, there are three key aspects in terms of scope that distinguishes our reputation system: its focus on the contents, its subjective nature, and its dependency on consensus. First, it is the actual contents that are stored and evaluated in the forums, with the identities being a secondary attribute. Second, content evaluation is subjective, as well as any decision to revoke posts or to fork forums. Third, at any given point in time, peers must agree on a common forum DAG prefix with global and deterministic accuracy to act identically as a whole. In this case, consensus is fundamental, since a subtle off-by-one discrepancy in reputation creates an irreconcilable fork in the network. Achieving consensus on a permissionless network is the key contribution of this work.

> We do not know if the results are good or bad because there was no comparison to the state of the art or baseline.

The main goal of our experiments in Section 3.1 is to stress the consensus algorithm to show that the mechanism is feasible, i.e., that it has a reasonable performance to be used in practice. The good result is that the protocol works in a permissionless context, regardless of the slower performance.

We added the following remark at the beginning of Section 3.1:

> The main goal of this section is to stress the consensus algorithm to show that permissionless public forums are viable, regardless of the inherent slower performance in comparison to permissioned protocols.

---

> Also, at the end of the day, we do not know if the proposal is resistant to Sybil attacks because there was no validation of the consensus and reputation mechanisms.

In our context, a Sybil is a random machine/identity with no previous reputation in the chains, which, by definition, cannot operate in the chains. By default, users with no reps do not have write access, as described in the beginning of Section 2:

> To prevent Sybils, users with no *reps* cannot operate under these rules, requiring a welcoming like from any other user already in the system. The fact that likes are zero-sum operations, which only transfer reputation, eliminates the incentives from malicious users to invite Sybils into the system. The only way to generate new *reps* is to post content that other users tolerate, which demands non-trivial work resistant to automation.

We included the following remarks:

> We consider Sybils to be groups of throw-away identities and machines with no previous reputation in the forums. ... In this sense, having one or hundreds of machines in the network does not affect the capacity to write into the forums. ... In our analogy with Bitcoin, Sybil attacks would require to add human resources, instead of CPU power.

# Reviewer 3

> It's important to note that the reputation system does not enforce "good" human behavior but provides a transparent and quantitative way for users to understand forum evolution and act accordingly. ... I am also concerned that the content removal is too weak to work

> in practice. For example, a Forum may be taken over by extremists, and they can upvote illegal content. That would require removal due to legal process, or face blocking at network level.

This is all true, and is the reason why we close the paper with your remark above. It is not even required to be “taken by extremists”, but only “created by and for extremists”. But we also believe that a protocol that is tamper proof, and provides persistence and data transparency can actually support law enforcement.

---

> Maybe a way to go is to create a pool of super-reputations that could answer to injunctions and administratively remove the content and a measure to avoid illegal content being broadcasted in subverted grupus.

For extreme conflicts, in which content removal is too weak, the protocol also provides hard forks, as discussed in the middle of Section 2.2:

> More than simple numeric disputes, a hard fork represents a social conflict in which reconciling branches is no longer possible.

---

> The paper is too descriptive, so reading sometime is tiresome. ... Reading could be improves by using some figures to explain ideas. Sometimes it is difficult to follow the text.

We opted for a full description of the protocol, but we recognize that the paper became a bit dense. It is hard to modify the whole text without more specific suggestions, but we removed some details of Freechains from Section 3.