NOTES on June 2025 revisions to manuscript ID TWEB-25-0111 entitled "A Dream Come True: Deletable Content in Immutable Storage."

The paper has been revised in response to reviewer comments we received on May 31st as cited and responded to, inline, in the following:

In Answer to Reviewer 1

1. *In the first page, the statement "The approach preserves the censorship resistance of..." . If the uploader has the ability to revoke access rights from all users, this essentially constitutes a form of **centralized control**, which I believe violates the very definition of **"censorship resistance."***

Answer: this appears to be a misunderstanding of the meaning of censorship resistance.

Censorship, or centralized control, is not present if the original uploader can delete what they uploaded; rather, if a third party gained that control. Which is not the case with the dream protocol. Popular voices regarding censorship:

“The idea is that no nation-state, corporation, or third party has the power to control who can transact or store ... on the network.” — Binance Academy

“Censorship resistance is the ability to participate in a platform or network without interference from any party.” — Coinmarketcap

We rephrased for clarity, added additional clarifications throughout the paper and a footnote at the quoted paragraph.

2. *In Section 3.1, under point **D**, the manuscript claims to use a **"one-time pad"**, but it allows the pad to be reused. This directly contradicts the requirements of **information-theoretic security**.*

   *If an attacker obtains two different plaintexts encrypted with the same key, this would lead to **complete information leakage**, as the attacker can simply XOR the two ciphertexts to recover the XOR of the plaintexts, which can then be exploited to fully reconstruct the original messages.*

Answer: Our main point was that the key itself does not leak indication about what it is used for. The concrete attack vector proposed can be taken care of by encrypting the ‘plaintexts’ asymmetrically, which is cheap given the accessibility of keys in this environment. This is not defeating the purpose of the contribution, because the symmetric encryption is for deletion, not privacy.

We rephrased for clarity, added language and a clarifying footnote to the quoted paragraph.

3. *In the conclusion section, it is recommended to address the critical issue of controlling and deleting already distributed data replicas.*

Answer: the contribution does not address this, the paper is explicit about why this is not necessary.

We made minor changes to be yet clearer to the paragraph spelling out that this cannot be addressed and, critically, is not expected.

(Section 2. Now reading "It is obvious that any party that is privileged to access such information could store, re-code, and potentially disseminate it, so that the content can be made accessible by them at a later point in time to anyone they wish, which would of course frustrate any process that could qualify as deletion (or removal of access) at the original download source. However, as there is no protection possible against such adversity, any legally and socially useful notion of deletion (e.g. revocation of access) therefore, invariably defines a narrower case: taking away the viability to replay the same access method at a lower cost than at least the full cost of storing the content.")

4. *There are multiple spelling mistakes, e.g., 'impsossible' → 'impossible', 'feasable' → 'feasible'.*

Answer: We double checked the document.

5. *Relative to the subject material, is the paper understandable without requiring too much effort on the part of the reader?: No*

Answer: we **added a technical Synopsis** of the formula chapter as sub section 2.1 to introduce the core technical functionality in a high-level view before the formulas, in plain language describing only the core network traffic and the one-time pad creation. This as an amendment to other overview sections in the paper that stay either non-technical or look at the resulting functionality.

Graphics were added to visually explain the core elements of the dream path and the update function. Their captions represent alternative, step-by-step explanations of the essential functionality.

We also added, and made more accessible, many **explanations of formulas and variable names** throughout the text.

In Answer to Reviewer 2

1. While the paper presents a well-structured protocol, it lacks discussion on the practical deployment constraints of DREAM—such as Swarm's current adoption level, network size, and availability assumptions. It would be helpful to include a short section or paragraph discussing the applicability boundaries and operational prerequisites.

Answer: we **added a section 5 on Operational Constraints** discussing the suitability as basis and the breadth of the extant SWARM network; as well as how DREAM would extend it, or could extend other decentralized storage networks.

2. Section 3 introduces several complex constructs (e.g., dream path Π, update function Δ) using mathematical formalism. To enhance readability for a broader audience, it is recommended to include a high-level illustrative example or a simplified diagram that shows the end-to-end dream protocol in action.

Answer: We added to and extended the explanatory diagrams to section 3 that **illustrate the variables** that appear in the formulas and in their visuals and captions add **sequence descriptions** of specifically how the dream path Π and the update function Δ work.

3. The conclusion could be strengthened by outlining potential future directions, such as integrating DREAM with more granular access control schemes, resilience against active adversarial interference, or combining the mechanism with off-chain computation and zero-knowledge proofs for enhanced privacy.

Answer: We added language to the conclusion that is directly answering this comment.