# Statement on Improving Data Storage
# on the Filecoin Network via
# Non-Interactive Proof of Replication
# (NI-PoRep)

The members of Decentralized Storage Alliance recognize the importance of simplifying and streamlining the input of data into the Filecoin Network and hereby support the introduction of Non-Interactive Proof-of-Replication (NI-PoRep) as part of the Filecoin Protocol.

Specifically, the members support FIP-854 as this improvement proposal outlines a method of arriving at Non-Interactive Proof of Replication via the use of existing network circuits, thereby reducing the engineering effort and network changes needed to implement this capability.

It is our understanding and desire that this change to the Proof of Replication process will serve to increase security by increasing the use of cryptographic measures in the sealing process, reduce the cost of sealing operations, separate Proof of Replication security from consensus thereby supporting greater trustless interaction, and enable novel network capabilities including but not limited to services such as Sealing as a Service.

Furthermore, the DSA recommends the maximum time-window between the sector initiation process (SealRandomnessEpoch stage) and the posting of storage commit and sector activation (ProveCommit stage) be of sufficient duration to accrue the benefits of prepping and pre-sealing storage sectors independent and distinct from sealing operations while still supporting the underpinning of the PoRep theorem that the timestamps between sector anchors shall be of a reasonable duration.

The DSA hereby supports a time-window of no less than 30 days as specified in the current proposal but strongly endorses extending this window to a maximum of 180 days to allow for storage providers to provision and ship pre-configured drives for maximum efficiency. The extension of the window is under the provision that no material concerns are uncovered during development and with proper review that compromise the mathematical proofs and security guarantees contained in the existing proposal.

For these reasons and as outlined in further detail below, the DSA supports the advancement of FIP-854 into development with sufficient prioritization as to see its success and timely release within the Filecoin Network so as to greatly simplify the sealing process and accelerate the adoption of decentralized storage for mission-critical and commercial-grade storage loads.

## Issue

Proof of Replication (PoRep) is a fundamental element of the decentralized storage proposition. It is a procedure used at the time of initial data storage to validate that a storage provider has created and stored a unique copy of some piece of data. In combination with Proof of Spacetime (PoST), which is a procedure to validate that a storage provider is continuing to store a unique copy of some piece of data, Proof of Replication serves as a fundamental proof that allows for creation, persistence, verification, and retrieval of decentralized verifiable data storage.

At present, the Proof of Replication process is a lengthy and synchronous process composed of two network actions separated by 150 network epochs. The first step is a PreCommit action which initiates the process and allows for the deposit of collateral necessary for the storage operation. The second step is a ProveCommit action which uses a challenge seed initiated by the first action as a key cryptographic component in the data sealing process. The duration between the two actions provides a non-deterministic mechanism for obtaining a qualifiable seed so as to properly maintain the security of the PoRep process.

This two-step interactive process, however, creates an undesirable dependency between the entity which stores the sector (which also initiates the PreCommit and deposits collateral) and the entity which actually proves it by performing the ProveCommit. This dependency thereby reduces the ability to have an independent and trustless separation between the two actions, limiting the flexibility of the network and constraining its growth.

### Solution

A Non-Interactive Proof of Replication (NI-PoRep) process merges the PreCommit and ProveComm steps in a unique step, removing the need for an onchain interaction for PreCommit and thus the need for a PreCommit deposit, thereby allowing for a simplified pipeline which can reduce costs and enable a full separation between storage and proving. This capability is particularly relevant for network capabilities such as Sealing as a Service (SaaS) and commercial grade storage capabilities via SupraSeal software.

The current Proof of Replication approach anchors data blocks (or sectors) to the chain via a seal reference key or ticket which is found in the range of epochs of the change between the first step and the second step. This ticket is used by the verifier as part of the ProveCommit action that verifies the seal and can be validated by the verifier as the correct ticket via ensuring that it is found in a specific range of epochs starting from the PreCommit.

Replacing this interactive linkage means that another method must be used to ensure randomness of the seal reference ticket. This non-interactive method generates the seal reference ticket in the following manner.

The NI-PoRep process changes the way PoRep challenges are generated. Instead of using an onchain interaction when onboarding a data sector, this new process allows storage providers to to generate challenges locally instead of via on-chain randomness.

This capability drastically simplifies the onboarding pipeline but also necessitates a higher security threshold for PoRep challenges than currently implemented. The proposal uses 128 bits of security which translates into a higher number of PoRep challenges compared with today (2253 per SDR layer instead of the current 176 per SDR layer or a 12.8x increase). Given recent improvements in ZK-SNARK processing, however, any additional cost is limited as storage costs dramatically outweigh computation costs during the entire sector lifetime. More importantly, this modest upfront cost unlocks massive improvements throughout the entire onboarding process, enabling capabilities which were impossible to achieve in the current setting including dramatic simplification of the pipeline, outsourcing of trustless computation, and utilization of SupraSeal software at its full potential.

**Benefits**

The Non-Interactive Proof of Replication process benefits the network in the following ways:

**Increases Security of the Proof of Replication Process** – Changing from reliance on rational security protections of the network to increased use of cryptographic measures greatly improves network security. The infeasibility of misbehaving cryptographically is a far stronger protection than the assumption that bad actors would have to act irrationally and/or against their economic interests.

**Reduces of the Cost of Sealing Operations** – Moving to a cryptographic-based method for obtaining the sealing reference target removes significant dependencies and complexity thereby reducing cost. Storage sectors can be pre-sealed at the factory and/or en masse and sealed using the most efficient algorithms and sealing configurations.

**Separates Proof of Replication Security from Consensus –** The decoupling of the two actions in the Proof of Replication process better rationalizes the resources needed to operate the network and allows for a better separation of concerns. Whereas there would be tight linkage between the two entities performing the PreCommit and the ProveCommit, this separation means that independent parties can participate in a more trustless manner creating a more efficient marketplace of network operators.

**Enables Trustless Sealing as a Service (SaaS)** – This decoupling of the two actions also creates opportunities for new entrants and specialty services. One such example is Sealing as a Service which is the ability to [need a phrase]. The availability of this type of service will make it easier for end users to use the network as well as unlock new use cases and accelerate the growth of the decentralized storage market.