A security analysis of the Filecoin protocol against rational adversaries

October 6, 2019

1 Introduction

Ideally, we would have wanted to have a proof of space time against all polynomial time adversaries; i.e. being able to have short proofs that an efficient $\mathcal{A}$ has certain files in memory continuously over a period of time. However this seems to require tools that are not ready today, at least in production, like verifiable delay functions, zk-SNARKs handling tens of billions of gates, and better recursive zk-SNARKs.

Instead, we focus on rational adversaries. The basic security definitions says - the honest strategy maximized profit, at least when the budget for the strategy is smaller than than some constant C sufficient for taking over the network.

Definition 1.1. *A protocol $\mathscr{P}$ is secure up to cost C if the strategy of cost $\mathsf{c} \leq C$ that maximizes expected revenue E is the honest strartegy.*

Important parameters:

1. The cost S of sealing a sector (assuming for simplicity they all have the same size).

Important objects:

1. The power table T.
2. The sequence of tickets.

2 Important components

Blockchain - assume well defined sequence of blocks and tickets or prove?

$\mathsf{por}(\mathsf{t}, \mathsf{i})$ - checks retrievability of sector i with randomness from ticket t.

3 biasing randomness

Thm: the probability of biasing