Proof of Storage Cryptocurrencies

Panos Chatzigiannis[1], Second Author[1], and Third Author[1]

George Mason University, ISA656 Class project,
{pchatzig,author2,author3}@gmu.edu

Abstract. Preliminary report. After spending enough time researching your topic you have to provide a summary of your proposal. Describe the main idea of the attack or protocol you will be presenting in 1-2 paragraphs. Include the main resources you are using (academic papers, white papers, new articles, blog posts etc). Finally, provide a list of items that you plan to include in your final report and presentation. I.e. Related work, specific background that you plan to cover, technical details, demo etc (think of this as the outline/sections of your report and presentation). The list your will provide is a commitment to what the instructor should expect in your final report and presentation. You will receive comments in your preliminary report and might need to re-adjust your goals.

Keywords: Proof of storage · SiaCoin · Storj

1 Preliminary report

1.1 Introduction

In our project, we will research on Proof of Storage cryptocurrencies. While most cryptocurrencies like Bitcoin [1] mainly focus on performing monetary transactions on a blockchain-based ledger, Proof of Storage cryptocurrencies suggest to take one step further and create a "decentralized cloud storage" platform. We will focus on two such cryptocurrencies, Sia and Storj. We will attempt to describe their underlying protocol in a more formal way along with more technical details, as their corresponding whitepapers only provide a high level description. Our sources for these analyses will be github repositories, forum and reddit posts in addition to the whitepapers. We will also attempt to include a live demo, making a direct comparison between the two, and possibly exploring weaknesses and/or attack vectors.

1.2 Sia

Sia[2] is considered a Bitcoin derivative that also offers publicly-verifiable storage contracts. According to these contracts, a number of hosts agree to store encrypted pieces of the clients' data, in exchange for Sia coins. Each host is audited and required to present a proof that he indeed owns the piece of the data he committed to store, then receiving a reward if he succeeds or losing his collateral

(which comes from the host's time-locked coins) if he fails. In this project we will attempt to highlight several technical details of the protocol which are not well-defined in the whitepaper, such as hash functions used, algorithm for file ownership proofs, host-client exchange protocol and block content-formatting. We will also include a description and a demo of the Sia client, primarily focused on the data storage functionalities rather than the mining or coin transaction aspects which are similar to other Proof-of-Work cryptocurrencies. If during our analysis we find any potential attacks on the protocol we will attempt to explore these as well.

1.3 Storj

References

1. Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf.
2. Sia: Simple Decentralized Storage whitepaper, https://sia.tech/sia.pdf. Last accessed 20 Mar 2018
3. Sia BitcoinTalk subforum, https://bitcointalk.org/index.php?topic=1060294. Last accessed 21 Mar 2018
4. Sia Wiki, https://siawiki.tech/index. Last accessed 21 Mar 2018
5. Sia Client, https://github.com/NebulousLabs/Sia. Last accessed 21 Mar 2018