Monero v7 Mining Pool Report

sneurlax
<sneurlax@gmail.com>
(https://github.com/sneurlax)

April 29, 2018

Abstract

An overview of Monero v7 mining pools with a current example of degraded privacy in one of Monero's privacy layers due to poor practices on the part of mining pools, a report on mitigation strategies including submissions to the blackball database, and a request for comments on best practices or solutions going forward. This report applies to Monero mainnet version 7 (v7) and showcases degraded privacy due to publicly-available metadata: mining pools' announced finds (blocks) and payments (transactions.) Mining pools are recommended to improve "privacy by obscurity" by disclosing less information publicly, but simple practices are presented in order to allow mining pools to proactively improve their privacy while maintaining the current level of metadata disclosure.

Contents

1.0 Introduction

As of Monero v7 (which began at block height 1546000,) a majority of the Monero hashrate is attributable to particular mining pools and there are seven or eight public pools with over 1% of the total global hashrate. These pools advertise various statistics—metadata—including the blocks that they have mined, and all but one pool (Nanopool) list the payouts that they have made to their miners.[1] The combination of output ownership and transaction authorship allow the true member of a ring signature to be inferred beyond a reasonable doubt in some cases, degrading one of Monero's layers of privacy.

[1] Nanopool does not directly announce all of their payments, but still does announce enough information to identify some of their transactions. What portion of their total payments are attributable is not known at this time and is a topic for future work.