Monero v7 Mining Pool Report

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

April 30, 2018

Abstract

This is 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 their current level of metadata disclosure.

Contents

1 Introduction

As of Monero version 7 (`v7` which began at block height 1546000,[1]) 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.[2] The combination of output ownership and transaction authorship allow the true member of some ring signatures to be inferred beyond a reasonable doubt in some cases, degrading one of Monero's layers of privacy.

[1] monero/src/cryptonote_core/blockchain.cpp v0.12.0.0, line 111.

[2] 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.

1.1 Monero's privacy protections

As of v7, Monero provides stealth addresses, ring signatures, and Ring Confidential Transactions (RingCT) as privacy layers. These layers ensure that Monero transactions are unlinkable, untraceable, and opaque. Stealth addresses provide unlinkability by encrypting the recipients of payments such that only the recipient of a Monero transaction can detect it as addressed to them, ring signatures provide untraceability by concealing the source of a payment such that any one of a number of ring members should be equally-plausible as the actual source of a Monero transaction, and Ring Confidential Transactions provide opaqueness by encrypting a payment's input and output amounts such that a third party cannot discern anything related to a transaction's amounts other than that it did not create new coins.

1.2 Degraded untraceability of ring signatures due poor mining pool practices

Ring signatures should conceal the real source of a Monero transaction. When constructing transactions, Monero selects a number of "decoys" with which it constructs a ring signature: there is no way to discern which ring member actually made the transaction without additional information. Unfortunately, poor mining pool practices such as blockchain forks and metadata announcements can provide enough additional information to discern which ring member is the actual source of a transaction beyond a reasonable doubt.

Blockchain forks have the potential to degrade the untraceability of ring signatures when users reuse key images across forks without taking advantage of any of the countermeasures provided by Monero's v7 upgrade. Key images may be safely (at least privately) reused across blockchain forks if care is taken to construct identical rings on both sides of the fork (a process which is outside of the scope of this report but is described in detail here.[3]) If users send funds on both sids of the fork without any such precautions, however, then they will inadvertently produce two rings that share only one member in common, thus identifying the common member as the real source of both transactions. Such outputs are identified as "known spent."

Mining pools have also been inadvertently revealing the real source of some payments *via* the statistics that they advertise before any blockchain forks incentivized key image reuse. Mining pools openly announce which outputs are theirs when they announce the blocks that they have found. When they later announce a transaction that uses one of their outputs as a ring signature member, it is most likely that their output is the real one and known spent.

[3] "How can individuals safeguard themselves and the community against a key reusing fork?" https://monero.stackexchange.com/questions/7826/how-can-individuals-safeguard-themselves-and-the-community-against-a-key-reusing

1.3 Monero v7's countermeasures against privacy degradations

By identifying an output as real in one transaction, its suitability as a decoy is degraded elsewhere, reducing the effective ring size of other users' ring signatures. Several tools were provided by the Monero v7 upgrade that allow users to avoid or mitigate both of the above potential degradations to their privacy. For example, users can avoid including any known spent outputs in their own ring signatures by using what is known as the blackball database, which contains every known spent output.

This report presents additional submissions to the blackball database, including explanations of what metadata identifies the real member of a ring, where to collect it, and example code to scrape and analyze the metadata necessary for independent verification of these results.

2 The State of the Hashrate

TODO: Describe the current state of Monero mining hashrate distribution, listing pools in descending order of hashrate.

2.1 Software centralization

TODO: List the most common mining pool stratum servers and GUIs and how code reuse enabled scraping of the data used to prepare this report. *Thanks, poolui!*

3 Metadata collection

TODO: Describe the metadata that will be collected, where it will be collected from, and how it will be used.

3.1 poolui-format pools

3.2 Nanopool

4 Mitigation

TODO: Pool operators: either announce less information *or* churn prior to paying out to miners.

4.1 Blackball database submissions

TODO: Describe the https://xmreuse.daemon.network API for querying blackball database submissions