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 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.

1.1 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

[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.

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 potential senders 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: without additional information that is not stored on the blockchain, there is no way to discern which ring member actually made the transaction. Unfortunately, poor mining pool practices including blockchain forks and metadata announcements can provide enough additional information to discern a transaction's actual source beyond a reasonable doubt.

TODO: Describe how key image reuse across blockchain forks compromises untraceability.

Metadata announcements by mining pools can also inadvertently reveal the real source of a payment: by announcing which blocks they have mined, mining pools are announcing which outputs are theirs; when they later also announce a transaction that uses one of their outputs in a ring signature, the actual ring member can be discerned beyond a reasonable doubt. This metadata announcement degrades the untraceability of Monero's ring signatures independent of the impact of blockchain forks, and in fact has been an issue since before any blockchain forks.

1.3 Monero v7's countermeasures against privacy degradations

TODO: Describe how the introduction of the blackball database mitigates the effects of these privacy degradations upon end-users.

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 Blackball database submissions

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

5 Conclusion

6 Future work

7 References