Towards Better Privacy with Monero

Malte Möser

Based on joint work with Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin
How Dirty Money Disappears Into the Black Hole of Cryptocurrency

Journal investigation documents suspicious trades through venture capital-backed ShapeShift

Hello.

You’re probably here because you’ve got a Monero malware problem. We’re here to help.

First, please understand that Monero itself is not a malicious technology. It’s a neutral, safe, and private cryptocurrency. A financial tool, if you will. Unfortunately, like any tool, it can be used by malicious people to exploit others.

The Monero Malware Response Workgroup provides resources and live support for multiple types of malware. Let’s identify your issue. Keep scrolling.
Takeaways

- Monero improves upon Bitcoin’s privacy
  - One-time addresses
  - Hidden values
  - Obfuscation of payment flows
- Incorrect use can severely hurt your anonymity
- Used for both illegitimate and legitimate purposes
Issue 1: Public Reuse of Addresses

Send Bitcoin to 1myaddress001

To: 1myaddress001

To: 1myaddress001
Issue 1: Public Reuse of Addresses

To: 1myaddress001

To: 1myaddress042

To: 1myaddress001

To: 1myaddress612
Monero Uses Stealth Addresses

Send XMR to mystealthyaddr

To: g77gwvm8mg
To: 0yqija6fga
Issue 2: Values Are Visible

Send XMR to *mystealthyaddr*

1 XMR

To: *g77gwvm8mg*

10.376289 XMR

To: *0yqi6f6ga*
When the Cookie Meets the Blockchain

- Each step can leak information to third-party trackers
- Timing and values allow to identify corresponding transactions

Goldfeder et al. (2018). *When the cookie meets the blockchain: Privacy Risks of web payments via cryptocurrencies*
Amounts Are Encrypted (Since 2017)

Send XMR to mystealthyaddr

To: g77gwvm8mg

To: 0yqija6fga
Issue 3: Tracing Payments

Bob → Alice → Hotel
Output Selection in Bitcoin

each input spends a single output
Output Selection in Monero

Each input spends one of multiple outputs using a ring signature + key image.
Deduction Technique

initially no mandatory number of mixins
Deduction Technique

initially no mandatory number of mixins
Deduction Technique
How Do You Choose Fake Coins?

Most likely to be the real coin being spent
Distributions Do Not Match

Real

Real + Fake

Ruled-out
The Newest Input Is Usually the Real One

Successful for 80% of all inputs between April 2014 and April 2017
Timing Attacks

- Bob is one of five suspects to have bought drugs at AlphaBay today
- I know Bob bought some XMR exactly 3 months ago
Mining Pools Announce Payouts

Payments Made

<table>
<thead>
<tr>
<th>№</th>
<th>Time Sent</th>
<th>Transaction Hash</th>
<th>Amount</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>8067</td>
<td>40 minutes ago</td>
<td>32770767737a7723723a79313c3d9c4629c9940f3b3e18569c0c5adc31c6edf32658</td>
<td>0.982726155862 XMR</td>
<td>0.00938502 XMR</td>
</tr>
<tr>
<td>8066</td>
<td>40 minutes ago</td>
<td>855787d0d30e3a0d59940618a14f462d2b1a2d73c2056d42d70707b398b</td>
<td>3.17024760014 XMR</td>
<td>0.01963772 XMR</td>
</tr>
<tr>
<td>8065</td>
<td>40 minutes ago</td>
<td>2159b86c38e4e1608fd45f39570c6b9396c4d55b24804dbf3b03970f8a3eb920</td>
<td>0.110775 XMR</td>
<td>0.00239226 XMR</td>
</tr>
<tr>
<td>8064</td>
<td>41 minutes ago</td>
<td>96f02c5b6c545c93e70d2c457072d1f85e552276b05f533b02000eaa22dd3293</td>
<td>0.135856 XMR</td>
<td>0.00239226 XMR</td>
</tr>
<tr>
<td>8063</td>
<td>41 minutes ago</td>
<td>9a4a678fb60f4d9a3a5d5a3a65f49a60a4b2d4b792863a3b35f53b897f</td>
<td>0.153114 XMR</td>
<td>0.00239226 XMR</td>
</tr>
<tr>
<td>8062</td>
<td>41 minutes ago</td>
<td>d59f79930b354ae5e3fcbe5a8c74c91f90af4999a3b1e4c6d71dfeb0765021380</td>
<td>0.200856 XMR</td>
<td>0.00239226 XMR</td>
</tr>
<tr>
<td>8061</td>
<td>41 minutes ago</td>
<td>9a82c7d0b5e1b248829a185336060d91e959f5e6a80f310f84d3068504f</td>
<td>0.111701 XMR</td>
<td>0.00239226 XMR</td>
</tr>
<tr>
<td>8060</td>
<td>41 minutes ago</td>
<td>81b8f6b1c1949752134812237cfa60b2a70419c73d693a185f4b4362c8c7</td>
<td>0.124084 XMR</td>
<td>0.00239226 XMR</td>
</tr>
<tr>
<td>7999</td>
<td>41 minutes ago</td>
<td>21b8f4e72a8704929812768d4e191f7560c07728396e1e62ab2227d2e2</td>
<td>0.110123 XMR</td>
<td>0.00239226 XMR</td>
</tr>
<tr>
<td>7998</td>
<td>41 minutes ago</td>
<td>f044b3a3a1e721c7c7794fe64360598df9d9e18a8e6e80a1b0d2053fb0be718</td>
<td>0.111255 XMR</td>
<td>0.00239226 XMR</td>
</tr>
<tr>
<td>7997</td>
<td>41 minutes ago</td>
<td>8235b42a4d7e3a6c674be7019276b354298398d6bb94f521c56f89b2a9d</td>
<td>0.113328 XMR</td>
<td>0.00239226 XMR</td>
</tr>
<tr>
<td>7996</td>
<td>41 minutes ago</td>
<td>f87d84ca84626b6a8855858220d1f49dbbb0bc4f4ade1ca0f09a1d045c9f</td>
<td>0.112415 XMR</td>
<td>0.00239226 XMR</td>
</tr>
</tbody>
</table>
Chain Forks Are a Privacy Hazard

Monero

MoneroV
Chain Forks Are a Privacy Hazard
Chain Forks Are a Privacy Hazard

Intersection reveals true spend
AlphaBay

- Volume spiked when AlphaBay started accepting Monero
AlphaBay - Daily Volume (Number of Transactions)
AlphaBay

- Volume spiked when AlphaBay started accepting Monero
- At most 25% of txs can be deposits at AlphaBay
Summary

- Monero improves upon the limited privacy of Bitcoin
  - Correct use of technology is paramount
  - It’s hard to patch a broken system

- Illicit business tends to be early adopters of new technologies
  - Many legitimate uses that are less visible