Monero Address Upgrade Timeline

Monero currently offers several methods of payment for many use-cases. Many of these were temporary measures to allow merchants to easily identify payments for invoices and deposits. However, the large number of options harms user experience and degrades privacy. Here, the Monero community outlines its timeline to streamline the Monero address system to the latest best-practices.

TL;DR: all payment IDs, including unencrypted (standalone) and encrypted (integrated), will be disallowed in the October 2019 upgrade. Many wallets, including the official GUI and CLI, will deprecate support for unencrypted payment IDs in the April 2019 upgrade.

Explanation of Grievances with the Current System

From the perspective of users, they can send different types of transactions:

1. Transactions to a normal address without a payment ID
2. Transactions to a normal address with a standalone 64-character payment ID
3. Transactions to an integrated address (address + built-in 16-character payment ID)
4. Transactions to a subaddress without a payment ID

Block explorers reveal three distinct transaction types, all approximately equally common today:

1. Transactions without a payment ID (those to a normal address or subaddress) (example)
2. Transactions with a 64-character standalone, unencrypted payment ID (example)
3. Transactions with a 16-character integrated, encrypted payment ID (those to an integrated address) (example)

These several supported transaction types are complex for users to understand. Furthermore, users may not fully understand the privacy concessions when creating multiple integrated addresses. Users may falsely assume that integrated addresses provide the same privacy protections as subaddresses (they do not). Even though subaddresses have some limitations, the protections are better than integrated addresses in every way.

Subaddresses allow users to create new addresses that are not directly linked to each other. Integrated addresses are inherently linked to a single address. Subaddresses create a new "identity" when receiving payments, while integrated addresses reuse the same identity. Subaddresses better protect against senders of money, but both types protect against outside observers.

Identifying transactions as one of the three types lowers privacy somewhat, since there is another piece of metadata to identify users. For example, suppose an attacker is interested in payments to a specific merchant that accepts only addresses with standalone payment IDs. The attacker could only look at transactions of the one type. Luckily, Monero has enough daily transactions that even 1/3 of them is a large crowd to hide among even in these circumstances, but it's best to avoid this extra metadata if possible.

Most importantly however, standalone payment IDs are extremely annoying. Users need to copy two strings to their wallet, and if they copy either incorrectly or forget to include the payment ID, they may lose their deposit or payment. Monero standalone payment IDs severely limit user experience and lead to complicated user interfaces.

Entities can still enter arbitrary information in tx_extra if it meets other consensus requirements. This extensible feature can be used for nearly any purpose.

Considered Solutions

Monero researchers and developers reviewed the following possible options for improving its address scheme. Some could be used in conjunction with others:

1. Removing standalone payment IDs. This slightly improves privacy and substantially improves user experience.
2. Removing all payment IDs (integrated and standalone) in favor of subaddresses. This slightly improves privacy, limits the ability for users to make revealing OpSec mistakes, reduces transaction size slightly, and substantially improves user experience. However, it is more difficult than removing only the standalone payment IDs, since a private view key is needed to generate new subaddresses.
3. Mandatory encrypted payment ID. This would limit the metadata leaked to outside observers, slightly improving privacy. However, this would slightly increase blockchain bloat by 10 bytes per transaction (~0.5%), and it could confuse users who expect to receive transactions without payment IDs. Furthermore, there is no way to enforce an honest payment ID at a consensus level. It could be used as a temporary stopgap.
4. Removing standalone payment IDs from the official wallets (CLI + GUI) and recommending that other wallets do the same. This encourages services that expect payments from most wallets to upgrade, though it could cause user confusion. It would not require a consensus change. Users of non-standard wallets would be at high risk if they use features that have been deprecated from common software.

Ultimately, the Monero community considered options 1, 2, 1+3, and 3+4.

Decision Process

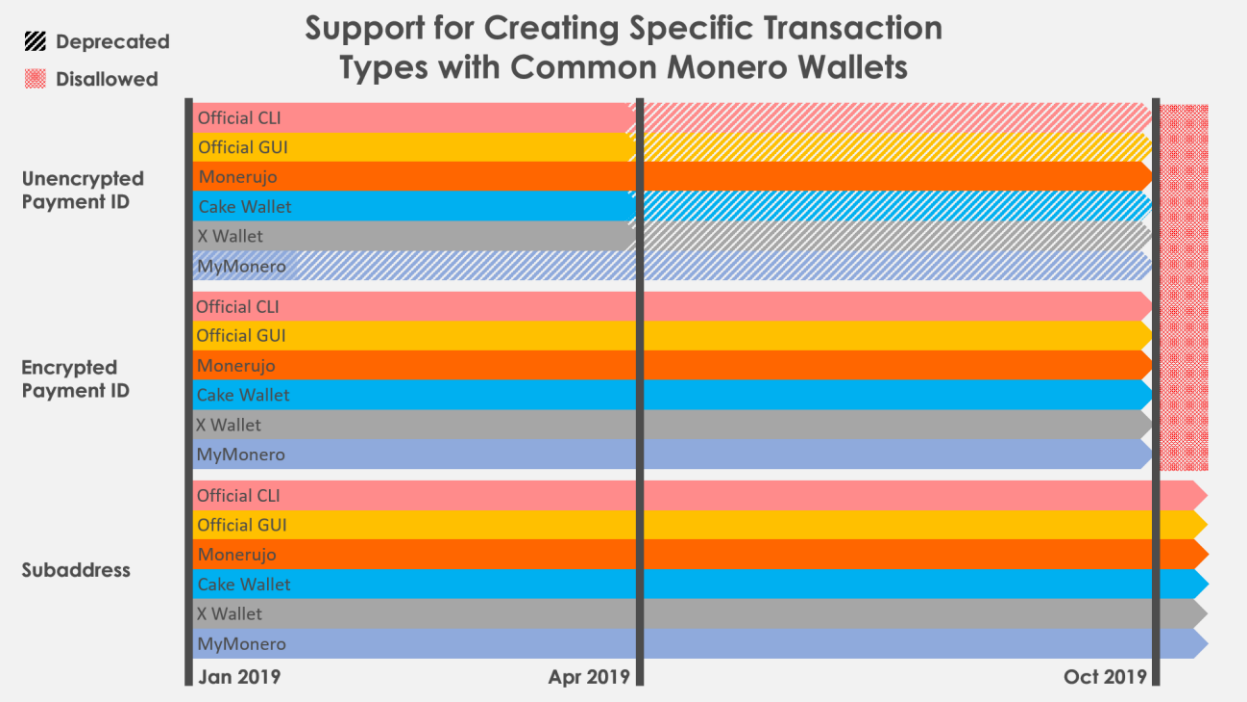
The Monero community decided to adopt this upgrade timeline following extensive conversations over several months with a variety of stakeholders.

- Alex from LocalMonero introduced the idea in the March 10 Coffee Chat.
- It was briefly discussed the following day during the March 11 DevMeeting.
- The topic was discussed in more detail during the May 6 DevMeeting.
- Justin opened a GitHub issue on May 7 outlining a preliminary update timeline. It received a lot of positive comments from the community, including services and independent Monero wallet developers. There was more generally positive discussion on Reddit.
- Monero Integrations, a popular tool, announced they removed standalone payment IDs during the June 9 Community Meeting.
- Monero v0.13.0 "Beryllium Bullet" introduced a warning when using unencrypted payment IDs.
- The Monero Research Lab and Monero developers deliberated over the considered solutions throughout December 2018 and January 2019.
- A pre-release of this document and associated upgrade materials was distributed to exchanges, wallets, and services in late January 2019.

Ultimately, standalone, unencrypted payment IDs were the primary targets for their terrible user experience. Encrypted payment IDs were the secondary targets, since subaddresses offer improvements over payment ID processes.

The Monero community outlined many benefits when using payment IDs over subaddresses to determine if the change to subaddresses is worthwhile. While subaddresses improve privacy for the sender and allow the receiver to more easily manage their OpSec, they are more difficult to implement and slightly costlier to maintain. Generating new subaddresses take a few extra milliseconds each, and merchants need to use their private view key (not the private spend key) to generate new subaddresses. While there are some hurdles to overcome, we feel that these limitations are outweighed by the benefits of subaddresses. Furthermore, the upgrade timeline for subaddress-only is quite generous.

Upgrade Timeline



For the April 2019 scheduled upgrade, the official Monero GUI and CLI will deprecate sending transactions with unencrypted payment IDs. Other wallets will follow suit. Exchanges and services processing Monero transactions should upgrade before the upgrade to maintain compatibility with most common wallets.

For the October 2019 scheduled upgrade, Monero will deprecate all payment IDs, including integrated addresses. Transactions that need to be identified should be sent using superior subaddresses.

Further Resources

You can learn more about Monero and its development process by using the following resources:

The #monero-dev Freenode IRC channel, also available on Mattermost.

Moneropedia Payment ID page

MoneroDocs pages on integrated addresses and subaddresses

Monero StackExchange questions with the `Payment ID` tag

MRL-0006: “An efficient implementation of Monero subaddresses”

Zero to Monero, pages 36-38