

MWC 2021 Annual Review

Critical Bug and Fix

On March 18, 2021, a GRIN developer contacted the MWC development team with a critical bug report related to the rangeproof caching logic. The GRIN developers recommended [not using the network until a fix had been safely implemented](#).

The GRIN network was affected and [a fix was implemented](#) with a rewind of the blockchain. Because MWC is a fork of GRIN, MWC contained the same bug. The team took steps to mitigate the issue and fix the bug.

First, MWC exchanges were immediately notified and were requested to halt trading, deposits and withdrawals. Next, the MWC team implemented the fix and took steps to rewind the blockchain to block 694,858.

Users were notified to update their wallets and ensure they were at the sufficient block height before transacting, and mining pools were notified to make sure they were running the updated version of the protocol.

These types of incidents happen sometimes when innovating on a new blockchain. The response from the MWC ecosystem and development team was swift and methodical, and allowed all parties to ensure funds were protected while the bug was being fixed, all making MWC more resilient in the long-term.

Slatepack

This year developers introduced the Slatepack transaction standard for MWC. This transaction method offers significant advantages over HTTP, file, and MWC. In particular, it is a much easier user experience, reducing the risk of privacy leaks and security issues. It also provides guarantees around sending, as only the intended recipient can correctly decode the Slatepack message.

The Slatepack transaction method is an interactive transaction; transaction interactivity is core to the Mimblewimble protocol and to maintaining its privacy guarantees by enabling both sides to provide blinding factors in the signature process, while still verifying the commitments transactions.

Additionally, interactive transactions promote monetary sovereignty by ensuring that an individual can only receive funds that they wish to receive. Spam and dust transactions are not possible with interactivity.

New GUI Wallet with Atomic Swaps

A new version of the GUI wallet was released early this year that enables Atomic Swaps for DOGE, LTC, ZEC and DASH. A subsequent version of the GUI Wallet added Atomic Swap capabilities for ETH and ERC-20 tokens, including USDT, USDC, BUSD, BNB, LINK, TRX, TUSD, UDSP, and WBTC.

Atomic Swaps are a decentralized, private, user-friendly way to swap assets between different blockchains. Integration into the GUI wallet makes this process much easier for anyone looking to swap their MWC between other cryptocurrencies.

Atomic Swaps Marketplace

This year the team also launched the long-awaited decentralized atomic swaps marketplace. The first version of the marketplace was launched with BTC, BCH, LTC, DOGE, ZEC, and DASH swaps. ETH is scheduled for release in the near future.

The marketplace enables users to find and execute swaps seamlessly and securely. This will bring even more liquidity and price discovery into atomic swaps and into MWC, without introducing additional centralization risks.

GUI Wallet for Android Mobile

This year also marked the release of Gui Wallet 1.0.0 for Android Mobile.

A mobile release is the first step in enabling users to have the highest degree of personal sovereignty on their mobile devices. Android powers more than 2.5 billion active devices worldwide, making it the perfect platform for expanding the reach and usability of our MWC technology.

With the new GUI Wallet, users can experience seamless and secure transactions, manage their MWC holdings, and explore the full potential of Mimblewimble technology right at their fingertips.

The team has worked diligently to ensure that the wallet is user-friendly, secure, and feature-rich. Some of the key features of GUI Wallet 1.0.0 include:

- User-Friendly Interface: An intuitive and easy-to-navigate interface designed for both new and experienced users.
- Enhanced Security: Robust security measures to protect your funds and personal information.
- Seamless Transactions: Smooth and efficient transaction processing, ensuring a hassle-free experience.
- Comprehensive Management Tools: Tools to help you manage your MWC holdings effectively, including transaction history, balance overview, and more.

This wallet will significantly enhance the user experience and make MWC more accessible to a broader audience. It also lays the foundation for future mobile development work for MWC.