Grams Helix: (not so) Secure Wallets

Done by user digigon1 from reddit

Introduction

This project has been developed in order to show to the average Helix user that this service is not as secure as people may think and that, therefore, it might not be worth investing the 2.5% fee.

To show that this service has flaws, the project has been divided into 3 phases:

1. Downloading all HelixMixer wallets.
2. Following withdrawals from these wallets.
3. Linking deposits to the wallets with withdrawals found in phase 2.

Each of these phases shall be discussed individually later in the report.

This project has been developed entirely in python over the course of three weeks and has used walletexplorer.com as a source of wallets.

Body

Phase 1. Downloading the wallets

WalletExplorer (henceforth WE) has an option of viewing every wallet that belongs to a service with URL's such as http://www.walletexplorer.com/wallet/HelixMixer. From this URL, you can see that an option to download as CSV exists.

Python was used as a scraper here, using the BeautifulSoup library to get all possible wallets.

Phase 2. Following withdrawals

This phase took quite a long time due to the sheer amount of possible withdrawals. To follow the withdrawals, each individual wallet downloaded in the previous step was analyzed, with all the sent transactions being followed via WE until it was worth less than 30% of the total transaction value or until the transaction had more than 1 input. After a wallet was done, its final output was saved for the next phase.

Phase 3. Linking deposits and withdrawals

In order to match deposits to withdrawals, two separate files were created: one with deposits and one with withdrawals.

To be able to match, the fee of 2.5% had to be considered, with a slight twist: this fee could actually vary between 2.3% and 2.5%. Another thing that was considered was the time interval: the withdrawals could be done at most 7 hours after the deposit. With this step, about 76700 unique matches were found out of about 304000 possible ones.

After this, the results were refined by looking at unique matches and removing their respective withdrawals from all other possible matches. This final step increased the unique matches up to about 85150.

Conclusion

The percentage of unique matches was about 28%, which included all the test transactions. This percentage could have been increased by lowering the 30% limit, or maybe even removing it. It could have also been increased by trying to deal with the possibility of having more than one output for each input.

All these conclusion could have been done by professional blockchain analysis companies, such as the following:

- https://blockseer.com
- https://chainalysis.com
- https://coinalytics.co
- https://sabr.io
- https://elliptic.co
- https://scorechain.com