

## Grokking Litecoin

By: **Alberto Cabello\*** | Ruben Recabarren | Bogdan Carbunar

Bitcoin, and its derivatives such as Litecoin, have been touted as a way to safely make anonymous transactions. This ability has come into question multiple times, with different papers coming up with different degrees of anonymity. Our goal for Overseer is to completely deanonymize all Lite-coin transactions. Our plan to accomplish this includes the creation of a network crawler using the JavaScript `litecoin-p2p` library provided by the Litecoin group. Using this crawler, we will connect to every node on the Litecoin network. Once we have that accomplished, we will begin sending *addr* messages to all the nodes advertising our own listening server. The goal of this is to get peers that don't accept incoming connections to connect to us so we can monitor them as well. By connecting to every node and sending the *addr* messages, we hope to have enough network coverage that all the nodes who don't accept incoming connections will connect to us. Once they are connected to us, it is trivial to deanonymize them as we'd have their IP address. At this point, when every node is connected to, we will monitor the transactions that occur on the network, and determine who is the originator of them. This project is significant because it will completely connect to the entire Litecoin network, which should allow us to deanonymize every transaction conducted on the network.