Fishing for Mules with Nets

Fraud is an ever-changing problem faced by financial institutions. Criminals must launder funds acquired through fraud and other criminal activities in order to access that money. Banks have a duty to prevent the laundering of fraudulent funds in order to protect their customers and society. There is also increased focus with the Industry Code on Authorised Push Payment Scams in 2019. Many standard fraud-finding techniques rely on analysing discrete data, meaning that connections between bad actors cannot be identified. Where common statistical models struggle because of class imbalance, graphs offer a simple and accessible approach.

We demonstrate a unique application of network analysis which enables us to trace customers, accounts and transactions linked to fraud. These links to known bad actors are like needles hidden in a haystack. We built a network at a scale of millions of nodes in Python from bank event data to find these suspicious connections. We cover common problems like super connected nodes and the opportunity in delivering tangible benefits using open source software. Providing investigators with a visualisation of networks allows efficient identification of mule accounts that might not have otherwise be detected and ensures appropriate action to prevent laundering of victims’ funds.