Identifying Malicious Activity In Ethereum Network

Adam Orucu – Denis Janiak – Filip Strzałka – Stanisław Straburzyński

Motivations & Goals

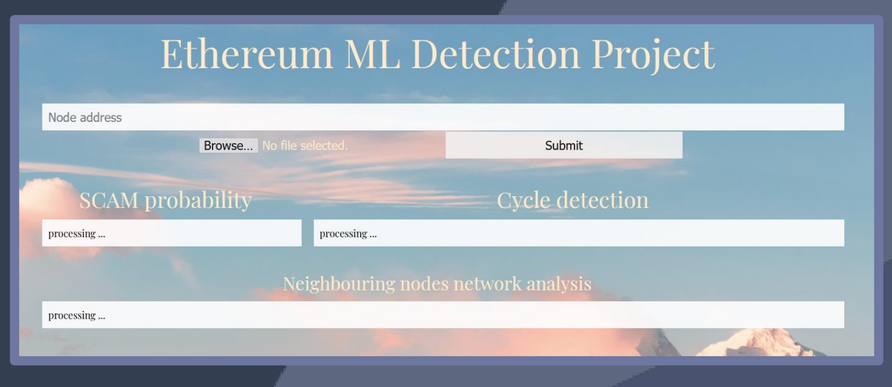
- Ethereum and cryptocurencies in general are used to launder money.
- Scammers often use cryptocurrencies.

- Ease money laundering detection on ethereum transactions network
- Prevent phishing and scam attempts

Solutions

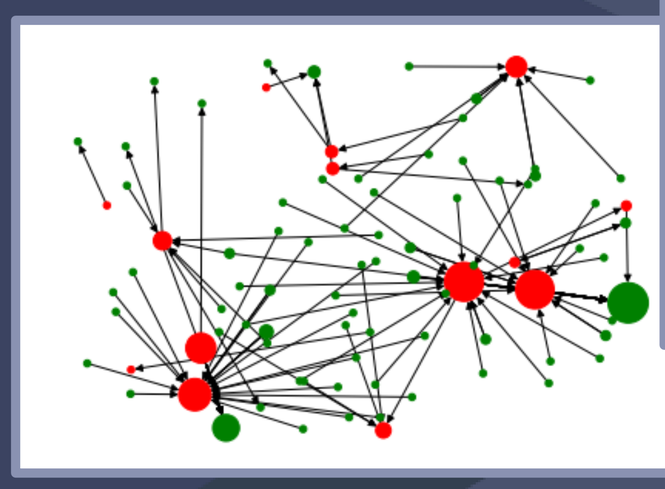
User Interface

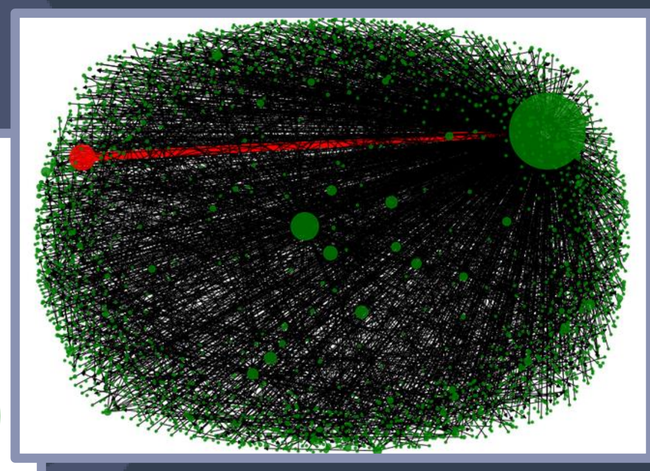
As an interface to the calculations a web app was created. It accepts wallet addresses and files containing lists of transactions. Returns scam probability and cycle detection.



Neighbor Nodes Network Analysis

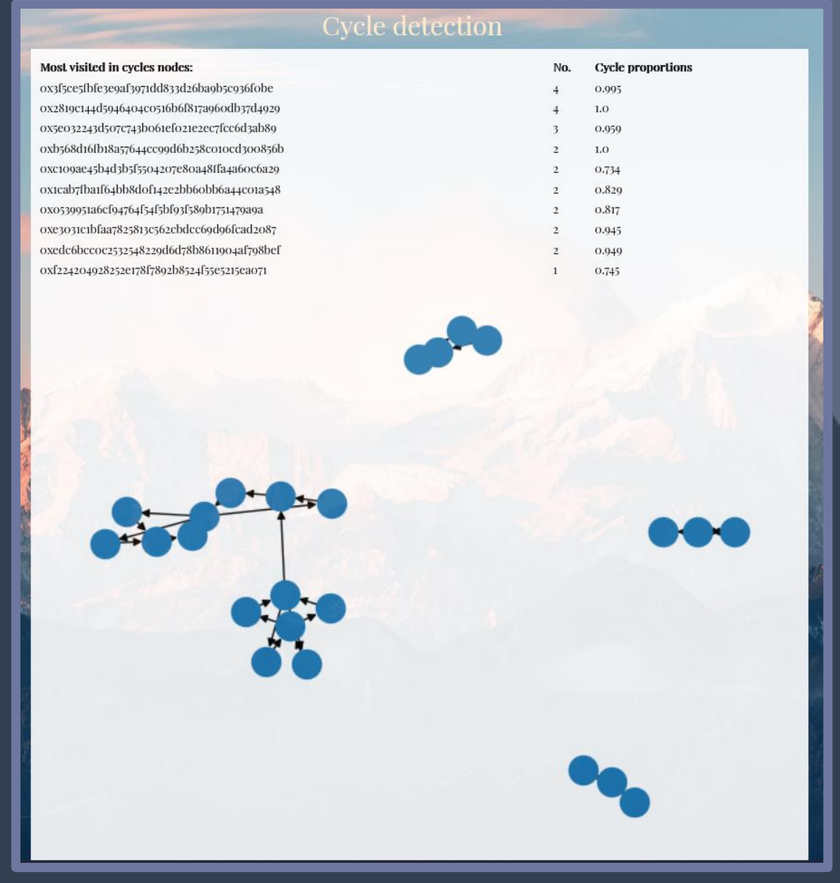
We collect all of the transactions from a short time window in the vicinity of the suspicious transaction to perform a neighbor node network analysis. The idea is to use a time window short enough to let us calculate the statistics efficiently but also allow us to gain enough information to use in the detection problem. Statistics like clustering coefficient, degree, pagerank or numer of connected components can be very helpful in identifying malicious nodes or transactions.





Cycle Detection

One of money laundering methods involves sending cryptocurrency to another account and after few transactions getting this money back. These transactions create cycles. It is easy to detect them if we operate on small amount of data. In the studied graph there could be many cycles, but we were only interested in cycles in which most of the money came back to the "sender". Establishing proper time windows and including only cycles with big "received/sent" money proportion we can indicate suspicious transactions and accounts.



Scam Transaction Detection

In order to find possible scam transactions and accounts a simple k-NN model was used. Some known scam accounts were downloaded from etherscamdb. Their transactions combined with randomly chosen transactions from the network were used to classify unknown transactions.

If a user wants to know if a chosen account is legitemate they can enter its address and get the probability of it being a scam account.

	Precision	Recall	f1-score
Not scam	0.8796	0.8715	0.8755
Phishing	0.1428	0.0769	0.1000
Scamming	0.8122	0.8122	0.8122
Accuracy	0.6027	05982	0.8122
Weighted avg	0.7945	0.8122	0.8022