Is there money laundering in cryptocurrency markets?

Summary
The explosive growth in the number of circulating cryptocurrencies has formed one of the largest unregulated markets in the world. Investigators need tools to not only overcome the challenge of calculating the actual volume of illicit activities in the cryptocurrency space, but to detect and disrupt illicit transactions and/or the underlying criminal activities. This project will apply a novel algorithm to transaction data, resulting in a probabilistic machine learning tool for law enforcement to decide on how to best target resources to seek and dismantle money laundering operations in cryptocurrency markets, enhancing law enforcement efforts in the face of new technologies.

Problem addressed
The goal of our project is to estimate a lower bound of the extent of money laundering over a large number of cryptocurrencies, and to use our observations to develop automated (probabilistic) tools which serve the operational need of identifying cryptocurrency wallets that are likely involved in illegal activities, so that federal and state law enforcement can detect and disrupt illicit transactions or the underlying criminal activities. Our scope goes beyond pseudo-anonymous cryptocurrencies, as we develop new approaches for correlating transactions in private cryptocurrencies and mixing services.

Approach
Our industry partner Blockchain Intelligence Group (BIG) provides us with a set of cryptocurrency addresses that have been labeled as malicious due to some specific activities (i.e. an address that was involved in dark web transactions, an address that was used in a scam, addresses from public trial cases, etc.), which we use to estimate the scale of illicit activity for the top 6-7 cryptocurrencies (which in total control about 90% of the market capital). To detect wallets potentially involved in illicit activity, we conduct a network clustering analysis within all addresses of each cryptocurrency. Using different sensitivity levels for our ML algorithms, we are developing a probabilistic tool that aims to assign a score of malicious activity to new addresses/transactions. Past work has focused on BitCoin, but we are focused on Dash, the second most popular private cryptocurrency in terms of market capital, with the goal to correlate participants who attempt to “mix” their funds.

Results
We have completed the analysis of Ethereum and are at the final steps of completing the analysis of two more of the largest cryptocurrencies, Litecoin and Bitcoin cash. In Ethreum we

had a ground truth set of about 3000 addresses, which we found to currently control over $900,000,000, and using our probabilistic tool managed to extend the 3000 addresses to a set of over 23,000 addresses. The expanded set only added approximately 25% to the total funds. Our preliminary analysis of Dash indicates that the offered anonymity level is less than thought, and we are currently experimenting with a number of heuristics to concretely connect additional addresses.

Anticipated Impact for DHS
Bitcoin and Ethereum ledgers could expose information about transaction sequences in a way that limits the utility of these cryptocurrencies for illicit transactions. We expect that our results will provide DHS/HSE with objective, data-based evidence regarding the extent of cryptocurrency utilization in money laundering operations. This is key information for law enforcement and policymakers operating in federal and state agencies. In particular, ICE is leading efforts to disrupt the potential use of cryptocurrencies for money laundering purposes. In addition, our probabilistic tool could provide an additional approach to identify and disrupt money laundering activities.

Research Products:

Publications:

Report: “Dash cryptocurrency deanonymization

Measuring Illicit Activity in DeFi: The Case of Ethereum

Videos:

CINA Research Briefing: Illicit Activities with Crypto Currencies