2021 PaCCS Research Snapshots Competition Proposal

Arianna Trozze, PhD Candidate
Centre for Doctoral Training in Cybersecurity
University College London

Workstream: Economic & Financial Crime, Undermining SOC
Title: Prosecuting Financial Crimes Involving Cryptocurrencies

Cyptocurrencies have legitimate use cases; in particular, the decentralised finance ('DeFi') ecosystem has facilitated new services including decentralised exchanges, stablecoins, and lending platforms. However, these technologies are also employed for nefarious purposes, like Ponzi schemes and frauds. CipherTrace suggests DeFi is an epicentre of crime, with more than half of the $432 million lost from hacks, theft, and fraud in Q1 of 2021 being DeFi-related [1].

Despite the magnitude of cryptocurrency-based financial crimes, enforcement efforts remain in their infancy. Some scholars suggest a need for cryptocurrency regulations, but others consider predicate offences like wire fraud sufficient [2]. My research will develop a model for prosecuting cryptocurrency-based frauds using existing law and computational methods for evidence extraction.

I first examined reasons for previous cases' success. I explored the impact of offence, defendant, and evidentiary characteristics on the mode of disposition and penalties in the 37 resolved federal cryptocurrency-based financial crime cases in the U.S., using bivariate analyses and logistic regressions to determine relationships among variables.

The presence of individual defendants only (rather than a corporate defendant or combination) and the use of only a cryptocurrency other than Bitcoin in committing a crime each made a case less likely to be resolved by dismissal, trial, or summary or default judgment, when controlling for other variables.

Individual defendants may have less resources to fight a case through trial. It is harder for individuals to avoid facing charges without the corporate veil shielding them from the law. In some cases, the individual running the company appeared to face the charges but avoided doing so on behalf of the company.

Our finding about the type of cryptocurrency used is perhaps because many cases not involving Bitcoin were unsophisticated scams—a defendant would avoid trial if, based on the evidence, they had little chance of winning. Unsophisticated criminals may also be less successful in evading charges.

One of the most surprising findings was the absence of blockchain evidence used. Research shows evidence impacts case outcomes and blockchain evidence has been used successfully in private cases. In response to this, my current research involves developing a machine learning model to detect securities violations from DeFi token smart contracts, the results of which could feed into prosecutions.

I will apply this model to simulated token data, perform transaction-level analyses for flagged tokens, build a model case, and conduct a mock jury trial to determine its usefulness to prosecutors.

References

[1] CipherTrace, ‘Cryptocurrency Crime and Anti-Money Laundering Report, May 2021’, CAML-20210512, May 2021. Accessed: May 27, 2021. [Online]. Available: https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-may-2021/

[2] H. S. Zaytoun, ‘Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft Comments’, *N.C. L. Rev.*, vol. 97, no. 2, pp. 395–431, 2019 2018.