**THEME: Cyberspace, Privacy and Data Protection**

**PROJECT: The Regulation of risk and security in crypto-currency transactions: how is a ‘good transaction’ detected and separated from a ‘bad one’ in a context in which complex and novel legal, economic and moral logics are involved?**

**Lead Supervisor:** Dr Teresa Degenhardt

**Supervisory Team:** Dr Teresa Degenhardt, Dr Sandra Scott-Hayward

**Primary Location:** Mitchell Institute

This PhD involves research on the sociological aspects of implementing cryptocurrency transaction analysis techniques for the purpose of cybercrime detection.

According to the Internet Organised Crime Threat Assessment (IOCTA) 2017 report, Bitcoin is still the currency of choice in criminal markets and as payment for cyber-related extortion attempts, such as from ransomware or a Distributed Denial-of-Service (DDoS) attack. Bitcoin is a public blockchain; everyone on the network knows about a transaction, and the history of a transaction can be traced back to the point where the bitcoins were produced.

So if bitcoin is traceable, why is it so popular for cybercrime? Although anyone can view the flow of bitcoins between addresses in the blockchain (or between bitcoin wallets), these addresses are just random numbers. In order to be able to identify an individual, it is necessary to trace the address to a real identity. A number of methods for the analysis of bitcoin user identities have already been proposed. Given the technologies available and the potential for accelerated analysis in software-defined networks, the challenge lies in maintaining privacy and anonymity for the general public while bringing the cybercriminal to account.

Sociologically, we are interested in investigating the ways in which the defender in the software-defined world may follow specific ideas of risk and threats to proceed to the identification of the user, to ascertain whether or not this is implicated in criminal activities or indeed whether the transaction at play is the result of criminal activities. Relatedly, how are the ‘good’ from ‘bad’ transactions sorted — how are the lines of legality- morality- economic- imagined within these networks, by different private, public, informal and formal actors and institutions?

We specifically ask:

- How is detection of threat and risk within the transaction system identified?
- What sort of knowledge is used as part of the process of detection and suspicion of the threat?
- What techniques are used to suspect transactions and related actors? What are the ways in which the threat is then ascertained or how is a ‘red alert’ materialised, by whom, and to who is the risk information passed on, if to any

formal organization or elsewhere? Is there some sort of censure or stop then activated in the transaction?

- How is the reaction to the ‘suspicious interaction’ and the ‘control activity’ devised? How are they impacting on the source of the threat, and, further, on the network’s ability to perform its economic transaction safely?
- How is the logic of economic profit-seeking and security articulated within this software and imagined by the scientists enrolled in its production? How are these competing or indeed combining in the process?
- How is the instance of control encroaching on the economic and political logic of these networks?
- What represents order in this world? What sort of economic mobility is considered adequate to perform the service? In what way is that mobility regulated so as to guarantee safety and/or control of the actions of the consumers/actors involved?
- What kind of investigation or control is considered morally valid and legitimate? How does that relate to our current understanding of privacy? How does it modify it?

**Primary Academic Discipline:** Criminology