THEME: Cyberspace, Privacy and Data Protection

PROJECT: Looking through the hole in your Bitcoin wallet

Lead Supervisor: Dr Teresa Degenhardt

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

Primary Location: Mitchell Institute

Crypto-currencies were initially seen as alternative economic model to support payments without a third party controlling the currency and profiting from it. However, according to the Internet Organised Crime Threat Assessment (IOCTA) 2019 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. By design, Bitcoin is a pseudonymous coin, meaning that users can transact with the currency without revealing their true identity. To tackle the challenge of Bitcoin-related crime, a range of deanonymization techniques have been proposed. This PhD is a fascinating study of the ways in which these new economies and transactions that are purported to be either 'revolutionary' or 'criminal' are policed through specific technological arrangements.

This PhD involves research on the technology deployed to police bit-coin economy by investigating the ideas behind it and the scientists involved in the process. How are system devised to detect cybercrime in these forms of transactions. How is a 'good cryptocurrency transaction' detected and separated from a 'bad one' in a context in which complex and novel legal, economic and moral logics are involved? What sort of ideas of risk and security are deployed? Who is leading these developments? What is considered relevant in this complex new economic space? Sociologically, we are interested in investigating the ways in which this new form of economy is policed according to 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? In other words, how are legal, economic and moral lines imagined within these networks, by different private, public, informal and formal actors and institutions?

We specifically ask:

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? 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 instance of control encroaching on the economic and political logic of these networks?

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