Addressing the Increasing Spectre of Cryptocurrency-related Crime: A South African Perspective

Continued advancements in technology and the Internet are contributing to the increasingly transnational and incorporeal nature of criminal activity. In particular, new technologies such as cryptocurrencies are aiding the commission and concealment of traditional common and statutory law crimes such as drug trafficking; money laundering, and fraud. Such crimes can be facilitated within Dark Websites housed in cyberspace using cryptocurrencies to either facilitate the crime, launder proceeds of illegal activities or conceal the identity of perpetrators. In addition, cryptocurrencies are being increasingly targeted for use in the commission of financial crimes such as fraud and investment scams.

A cryptocurrency is an online, decentralised, encrypted currency that is denominated in its own units of value. Cryptocurrencies are not legal tender in any jurisdiction and remain unregulated in South Africa with varying levels of regulation in different countries. Cryptocurrencies are thus not sovereign to any jurisdiction but rather an international online currency. Devoid of criminal intent, Satoshini Nakamoto designed bitcoin in 2008 as an alternative to fiat currency. The purpose of bitcoin was to facilitate anonymous albeit legitimate, global peer-peer transactions at a minimal cost without the use of a financial institution. Cryptocurrencies are thus based on the idea central control is not necessary for money to work and thus uses ‘trust by computation’ rather than centralised trust as in the case of the traditional financial system. Bitcoin achieves this purpose by employing “cryptographic proof instead of trust” to both process and validate the transactions, thus negating the need for financial institutions. In addition, and in contrast to the traditional financial system, no user-identifiable information is attached to a bitcoin transaction, except a bitcoin address represented by a string of numbers. This in effect renders the transactions pseudo-anonymous and thus difficult to trace. It is therefore no surprise that cryptocurrencies have become the currency of choice for criminals.

In United States of America v Ulbricht, 2nd U.S Circuit Court of Appeals, 2017 (15) U.S 1815, the accused was sentenced to life imprisonment for money laundering, hacking, and drug trafficking and criminal enterprise carried out on the Dark Web. All of these crimes were facilitated through the cryptocurrency bitcoin (btc). In the case of Kats et al v United States of America, Southern District of New York, 2016 (13) U.S 368, the co–accused was sentenced to twenty years in prison for facilitating money-laundering activities via Costa Rican online payment processor company, Liberty Reserve. In particular, the rulings of these cases serve as a precedent for the South African criminal justice system. First, it emphasises that traditional crimes facilitated by new, unregulated technologies still constitute a crime. Second, that while it is difficult for an investigation to begin without a legal basis, existing criminal and procedural legislation can be effective in investigating and prosecuting crimes facilitated by new technologies (such as cryptocurrencies). Third, cryptocurrencies are an
international online currency. The crimes of which thus require strategic and collaborative efforts by investigative authorities on a global level and are crucial in the successful prosecution of such crime.

The purpose of this paper is to identify the key challenges that cryptocurrencies present to the South African criminal justice system in terms of investigation and prosecution, and to provide recommendations aimed at improving the investigative processes and alleviating the prosecutorial challenges associated with cryptocurrency related crime.

Ms Eveshnie Reddy
Lecturer: School of Criminal Justice, College of Law
University of South Africa
Pretoria