



**Senate Economics References
Committee**

Inquiry into Digital currency

**Submission by the
Australian Federal Police**

December 2014

Introduction

The Australian Federal Police (AFP) welcomes the opportunity to make a submission to the Senate Economics References Committee inquiry into Digital currency.

2. This submission is intended to provide the Committee with information on the AFP's experience with digital currency, including the use of digital currency in illegal activity and the implications of digital currency for Australia's law enforcement and national security framework. The submission relates primarily to terms of reference (a)(iv) securing the protection of consumers and businesses against illegal activity, (a)(v) incorporating digital currencies into Australia's national security framework, and (d) other related matters.

3. Digital currency is likely to increasingly become an accepted form of exchange for goods and services in Australia. While this includes legitimate and lawful transactions, there are a number of features of digital currencies that also promote their use to support illegal activities, and which create challenges for law enforcement. As with other activities that take place wholly or largely online, using the internet or darknets, effective law enforcement responses require close collaboration and coordination among partner agencies, and alignment of domestic and international law enforcement interests and efforts.

The AFP experience of digital currency

4. The AFP works closely with domestic and international partners to enhance law enforcement responses to the evolving online threat environment, including the challenges posed by digital currency to the safety of Australians, Australian interests and the security of our borders.

5. The advent of digital currency in Australian law enforcement investigations is relatively new and the AFP, alongside our law enforcement partners, has been exploring implications of digital currency for the management of issues relating to the prosecution of criminal offending and the confiscation of the proceeds of crime. The AFP also continues to share experiences through existing international law enforcement networks to enhance the collective goal of combating illegal activity enabled by the use of digital currency.

6. The AFP's main experience with digital currency has – to date – been specific to Bitcoin. The key areas of crime involving digital currency investigated by the AFP include:

- Fraud, being the alleged theft of Bitcoin via hacking;
- Bitcoin exchanged as payment for the importation into Australia of illicit narcotics from major online black marketplaces such as Silk Road¹;
- domestic supply and trafficking of narcotics for payment in Bitcoin; and

¹ Silk Road, a Darknet online marketplace shut down by US-led law enforcement efforts in 2013, allegedly moved hundreds of millions of US dollars' worth of bitcoins related to the purchase and sale of drugs and other illicit goods.

- money laundering and dealing with the proceeds of crime via Bitcoin.

7. The AFP understands that similar crime typologies have been identified in other Australian law enforcement jurisdictions and internationally. Bitcoins worth USD 1 million were seized in November 2014 as part of disruption activities of online Darknet sites in a joint operation by Europol's European Cybercrime Centre (EC3), the FBI, the U.S. Immigration and Customs Enforcement's (ICE), Homeland Security Investigations (HSI) and Eurojust. This action also resulted in 17 arrests of vendors and administrators and the disruption of 410 hidden services. Cash, drugs, gold and silver were also seized as part of the coordinated law enforcement activities.

8. On 3 November 2014, the United Kingdom Government through Her Majesty's Treasury (HM Treasury) asked for public feedback to assist in the formation of their digital currency regulations². This call identifies some key risks associated with digital currency, including:

- User detriment: digital currencies are stored in digital wallets, which can be vulnerable to fraud or hacking, and users may be vulnerable to loss through fluctuations in the value of digital currencies, or the failure of wallet providers or digital currency exchanges.
- Anonymity: many digital currency transactions occur without a record of or requirement to establish the identity of the parties involved. This promotes their value to buyers wishing to purchase illegal goods and services. This anonymity can be bolstered through Peer-to-peer transactions occurring outside of regulated financial markets

9. Digital currencies may employ technologies such as 'distributed ledgers' or block chains³ which record transactions, and potentially make forgery of digital currency more difficult. However, the AFP notes that while block chains, record all Bitcoin transactions, the identity of persons involved in the transactions may not be readily traceable, due to the encrypted and decentralised nature of the currency.

10. In June 2014, the Financial Action Task Force (FATF) released a paper on Virtual Currencies⁴ reiterating that ability to obtain bitcoins and transact anonymously in the currency, without the need to transact within a regulated financial framework, posed significant money laundering and terrorist financing risks.

11. The anonymous conversion of cash to Bitcoin or reverse remains a very attractive option for criminal use in support of illegal activity. In 2014, Bitcoin Automated Teller Machines (ATMs) have been introduced into Australia. The

² <https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information>

³ https://en.bitcoin.it/wiki/Block_chain describes a block chain as the transaction database shared by all nodes participating in a system based on the Bitcoin protocol. A full copy of a currency's block chain contains every transaction ever executed in the currency. With this information, one can find out how much value belonged to each address at any point in history.

⁴ Virtual Currencies – Key Definitions and Potential AML/CTF Risks, June 2014, FATF

ATMs permit cash deposits and withdrawals in exchange for Bitcoin. Various Bitcoin ATMs imported into Australia have been reviewed by Australian law enforcement. Some have anti-money laundering security features fitted, which include the collection of biometric data, and others do not.

The current regulatory environment

12. Australia's Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) regime is primarily contained within the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act). The specified intent of the AML/CTF Act is to combat money laundering and the financing of terrorism, and other purposes. Under the AML/CTF Act, the Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's AML/CTF regulator with supervisory, monitoring and enforcement functions.

13. Digital currencies such as Bitcoin remain largely outside the scope of the Australian AML/CTF regulatory scheme, as they are not backed directly or indirectly by precious metal or bullion, nor prescribed by the AML/CTF rules. The transfer of digital currency may be facilitated via peer to peer networks or an established digital currency exchange (exchange), and only engages with the Australian financial system through conversion into and out of legitimate fiat currencies. Even then, there may be no or only limited visibility of the transaction, and this is potentially compounded by the deployment of Bitcoin ATMs as discussed above.

14. The AFP notes that the issue of digital currencies is being considered as part of the statutory review of the AML/CTF Act being conducted by the Attorney-General's Department (AGD). The AFP is working closely with AUSTRAC, AGD, and other partner agencies to ensure that its experience of these currencies and their use to facilitate criminal activity informs the review.

Conclusion

15. The technology of digital currencies offers attractive options to criminal entities of rapid, irreversible transactions, from remote locations, with features that promote anonymity. These transactions occur largely outside of the current regulated financial system, creating significant challenges for law enforcement in identifying and tracking the flows of illicit funds. Collaboration and coordination among domestic and international law enforcement agencies will remain an important factor in responding to issues arising from the evolving use of digital currencies markets align law enforcement interests and efforts.

16. The AFP will continue to work with government and partner agencies to support effective legislative and regulatory frameworks to manage risks arising from the pseudonymity of digital currency transactions to our National Security, and specifically money laundering and terrorism financing. The AFP supports work underway through the statutory review of the AML/CTF Act to develop an approach that assists in protecting consumers and businesses against illegal activity within Australia and deters the criminal use of digital currencies.