



Australian Government
Attorney-General's Department

Submission of the Attorney-General's Department

Senate Economics References Committee

Inquiry into digital currencies

December 2014

Contents

Scope of submission	4
Introduction	4
Digital currencies – key concepts and definitions	5
Potential AML/CTF risks posed by digital currencies.....	6
Money Laundering.....	6
Terrorism Financing.....	9
Current regulatory approaches to digital currencies	10
Domestic	10
International	11
United States	11
New York State	12
Canada	13
European Union	13
United Kingdom	14
New Zealand.....	14
Intergovernmental approaches.....	15
Financial Action Task Force	15

Australian Presidency	15
Egmont Group of Financial Intelligence Units	15
Egmont Operational Working Group Project on digital currencies	16
Developing an effective regulatory system	16
Industry submissions to the statutory review of the AML/CTF Act.....	16
Bringing digital currencies within the AML/CTF regime	17
Conclusion	17

Scope of submission

The Attorney-General's Department thanks the Senate Economics References Committee for the opportunity to make a submission to its inquiry into digital currencies.

Our submission focuses on paragraphs (a)(iv)-(v), b(i),(iii), (c) and (d) of the inquiry's Terms of Reference. In particular, we outline the current approach to regulating digital currencies under Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime and compare this approach with international practice. We also outline some of the ongoing challenges that have been encountered by regulatory authorities and law enforcement agencies in relation to digital currencies.

Introduction

In the relatively short period of time since Australia's anti-money laundering and counter-terrorism financing (AML/CTF) legislative regime was introduced in 2006, digital currencies have emerged as an innovative, cheap, flexible method of payment that is gaining ever-increasing global acceptance. This rapid development has attracted the global attention of regulators and policymakers, many of whom have taken highly disparate approaches. Some jurisdictions have embraced the many benefits of the new technology, pointing to increased payment efficiencies and lower transaction costs, while others regard it as a powerful new tool for criminals, terrorist financiers and other sanctions evaders and have partially or completely limited its use.

In 2011 the Australian Transaction Reports and Analysis Centre (AUSTRAC) released its report on *Money Laundering in Australia*, which found that the dynamic nature and rapid technology developments offered by new electronic payment methods such as digital currencies enabled their exploitation by criminals for money laundering purposes.¹ This capacity for misuse by illicit actors was confirmed by AUSTRAC's recent report *Terrorism financing in Australia 2014*, which assessed that the potential for anonymity offered by online payment systems such as digital currencies made them attractive for terrorist financing,

¹ AUSTRAC, *Money Laundering in Australia*, available online at: <http://www.austrac.gov.au/files/money_laundering_in_australia_2011.pdf>.

particularly when the payment system or exchange is based in a jurisdiction with a comparatively weaker AML/CTF regime.²

The challenge going forward will be to encourage the development of digital currency in a way that fosters and utilises its beneficial aspects while securing protection of consumers and businesses against illegal activity and minimising negative national security implications.

Digital currencies – key concepts and definitions

An important step in assessing potential risks and developing an appropriate response is to have a clear understanding of the various types of digital currencies, as well as how they are controlled and used.

There is, as yet, no single commonly accepted definition of what constitutes a digital currency, though a number of jurisdictions and institutions have offered up their own formulations.³ In June 2014, the Financial Action Task Force (FATF) released its report on *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*. This report, the initial draft of which was prepared jointly by Australia, Canada, Russia, the United Kingdom and the United States, defines digital currency as:

[A] digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the digital currency. Digital currency is distinguished from fiat currency (a.k.a. “real currency”, “real money”, or “national currency”), which is the coin and paper money of a country that is designated as its legal tender and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency – i.e., it electronically transfers value that has legal tender status.⁴

³ In October 2012, the European Central Bank (ECB) defined digital currency “as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community” (see *Virtual Currency Schemes*, available online at: <<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>). This definition has subsequently been criticised for its inadequate scope, as math-based decentralised digital currencies such as Bitcoin are not issued and controlled by a central developer, and some jurisdictions (e.g. the United States, Sweden, and Thailand) now regulate digital currencies.

⁴ FATF, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, available online at: <<http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>>.

Digital currencies can be divided into two basic types: convertible and non-convertible. Convertible digital currencies have an equivalent value in real currency and can be exchanged back-and-forth for real currency, while non-convertible digital currencies are intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game⁵ or Amazon.com, and cannot be exchanged for fiat currency under the rules governing its use.⁶

These two basic types of digital currency can be further sub-categorised as 'centralised' or 'non-centralised'. All non-convertible digital currencies are centralised; they are issued by the central administering authority that controls the system. An administrator issues the currency, establishes the rules for its use, maintains a central payment ledger, and has authority to redeem the currency (i.e. withdraw it from circulation). Currently, the vast majority of digital currency payments transactions involve centralised digital currencies. In contrast, non-centralised digital currencies (also sometimes referred to as 'crypto-currencies'⁷) are distributed, open-source, math-based, peer-to-peer currencies that have no central administering authority and no central monitoring or oversight.

Potential AML/CTF risks posed by digital currencies

Money Laundering

Digital currencies have undoubted potential to empower users by reducing transaction costs for payments and fund transfers, increasing access to capital, and reducing barriers to financial inclusion by offering services in under-banked and unbanked regions of the world. However, they are also potentially vulnerable to a variety of illicit financing risks, including money laundering and terrorist financing. Of particular concern is that digital currencies, which can be traded on the internet and are generally characterised by non-face-to-face

⁵ Massively multiplayer online role-playing games (MMORPGs) feature living economies, with virtual items and currency that have to be gained through online play. The most popular MMORPGs include *World of Warcraft*, *Final Fantasy XIV* and *Guild Wars*.

⁶ Examples of convertible currencies include Bitcoin, e-Gold, Liberty Reserve (now defunct), Second Life Linden Dollars, and WebMoney, while non-convertible currencies include Project Entropia Dollars, Q Coins, and World of Warcraft Gold.

⁷ Crypto-currencies are protected by math-based cryptography designed to secure information and ensure greater anonymity than other forms of non-cash payment methods. Bitcoin is the most prominent example of this type of digital currency, though other examples include Ripple, PeerCoin, Lite-coin, zerocoin, anoncoin and dogecoin.

customer relationships, allow for greater anonymity than traditional non-cash payment methods. This provides a powerful new tool for criminals, terrorist financiers and sanctions evaders to both move and store illicit funds out of the reach of law enforcement and other authorities and purchase illicit goods and services.

These are not merely hypothetical risks. In May 2013, the U.S. Department of the Treasury and the Department of Justice undertook coordinated enforcement action against Liberty Reserve, a digital currency system used to facilitate USD 6 billion worth of illicit web-based activity, including identity fraud, credit card theft, online scams, and dissemination of computer malware.⁸ While this represents the largest online money laundering case in history to date, the actions of centralised convertible currencies such as Liberty Reserve are arguably of less concern to regulators and law enforcement authorities than non-centralised digital currency systems (of which Bitcoin is the most prominent current example), which are particularly vulnerable to anonymity risks. Under the Bitcoin protocol, for instance, addresses (which function in a similar way to user accounts) have no names or other customer identification attached, and the system has no central server or service provider. The protocol does not require nor provide for the identification or verification of participants in the currency. There is no central oversight body, and no financial intelligence software is currently available to monitor and identify suspicious transaction patterns occurring within the protocol. As the widespread use of Bitcoin to conduct transactions on the now-defunct Deep Web⁹ black-market site known as 'Silk Road'¹⁰ aptly demonstrated, these features make non-centralised currencies particularly attractive to criminals seeking to launder money and either purchase or accept payment for illicit goods and services.

The potential AML/CTF risks engendered by this relative anonymity are increased by the global reach of non-centralised digital currencies, which exist in a digital universe largely

⁸ Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store, and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200 000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own digital currency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency (US dollars). See FATF, *Virtual Currencies*, note 4 above at 10.

⁹ The Deep Web (also called the Deepnet, Dark Net, Invisible Web, or Hidden Web) is that portion of internet content that is not indexed by standard search engines.

¹⁰ While in operation from February 2011 to October 2013, Silk Road took advantage of the anonymising 'Tor' network and the pseudonymous nature of Bitcoin to make available a vast digital marketplace where one could mail-order drugs and other licit and illicit goods and services. Following a two-year investigation into the Deep Web market, the FBI shut down the Silk Road website on 2 October 2013.

outside the influence of any particular jurisdiction. Unlike centralised systems such as Liberty Reserve, which was based in Costa Rica, law enforcement cannot target one central location or entity for investigative or asset seizure purposes.¹¹ In addition, these systems commonly rely on complex infrastructures involving several entities, often spread across several jurisdictions, to transfer funds and execute payments. This segmentation of services means that responsibility for AML/CTF compliance and enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised digital currency technology and business models, including the changing number and types/roles of participants providing services in digital currency payments systems. In combination, these issues offer a level of potential anonymity for illicit actors that is impossible to achieve with traditional credit and debit cards or older online payment systems, such as PayPal.

Notwithstanding the above, there is an important qualification to be made regarding the anonymity risks associated with digital crypto-currencies. It is a common misapprehension that these currencies provide complete anonymity for their users; however, as several academic studies have now demonstrated these types of digital currency are better described as offering "pseudonymity". To use Bitcoin as an example, every Bitcoin transaction is linked to a corresponding public key, which is then stored and made publicly available to view in the block chain. If a person's identity were linked to a public key, then it would be possible to look through the recorded transactions in the block chain and easily see all transactions associated with that key. In other words, Bitcoin offers users the ability to transact under the concealed identity of their Bitcoin address/public key, but all of their transactions are available for full public viewing and therefore for law enforcement scrutiny. When these transactions were examined and used to construct a pattern of behaviour, analysts in a simulated experiment were able to reveal the identities of approximately forty percent of Bitcoin users.

¹¹ The difficulties and resources involved in global coordination are evident in the recent dark-web takedown by 'Operation Onymous', which involved law enforcement agencies from Bulgaria, the Czech Republic, Finland, France, Germany, Hungary, Latvia, Lithuania, Luxembourg, the Netherlands, Romania, Spain, Sweden and Switzerland collaborating in the global arrest of 17 people suspected of selling drugs, guns and hitmen through underground websites that utilised digital currencies.

Terrorism Financing

Much of the academic literature, regulatory guidance, and law enforcement activity to date has been focused on the use of digital currencies to help criminals distribute, store, and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and exploitation material etc by enabling them to conduct pseudo-anonymous and often untraceable financial transactions. Less attention has been given to the potential role of digital currencies in facilitating the financing of terrorism.

Terrorist organisations vary widely in scale and sophistication, ranging from large, state-like organisations to small, decentralised and self-directed networks. This diversity is reflected in their funding requirements. Smaller organisations and so-called lone wolf terrorists are likely to seek to meet their own funding requirements using legitimate sources, allowing them to raise moderate amounts of money relatively inconspicuously. For larger organisations, the costs associated not only with conducting terrorist attacks but also with developing and maintaining a terrorist organisation and its ideology are significant; funds are required to promote a militant ideology, pay operatives and their families, arrange for travel, train new members, forge documents, pay bribes, acquire weapons, and stage attacks.

Traditionally, through either the complicity or inaction of some foreign states and financial institutions, terrorist groups have had comparatively easy access to the global financial system to move and store their funds. In recent years, however, a combination of intergovernmental efforts to enhance financial transparency and impose targeted financial sanctions against terrorists and private-sector concern over legal and reputational risk have made it harder than ever for terrorists and other illicit actors to exploit the international financial system. As a result, terrorist groups and their supporters have increasingly been forced to turn to less regulated channels such as cash couriers, hawaladars and other small-scale alternative remittance systems in order to transfer and store funds. These mechanisms require terrorist groups to rely on more people and larger networks than simple electronic funds transactions, making these financing channels and the terrorists who stand to benefit from them more vulnerable to discovery. They are also inefficient for the decentralised collection of funds from multiple sources and the disbursement of those funds to single or multiple geographically dispersed end points, both of which slow down the process of funding, planning and implementing terrorist attacks.

Digital currencies provide a low-cost mechanism to circumvent the vulnerabilities and inefficiencies of alternative remittance mechanisms and minimise exposure to the legal risks of engaging with the regulated global financial system, although they may expose users to other types of risks¹². These benefits are multiplied if transactions are able to be conducted through an anonymous – or even pseudonymous – payment system that would allow terrorists to better cover their tracks.

Despite these evident advantages, there appears to be little evidence to date to indicate the use of digital currencies as a means of financing terrorism. In its 2012 typologies and case studies report, AUSTRAC concluded that while the anonymous nature of digital currencies may appeal to criminal groups and individuals, their overall utility for criminals at this point may currently be limited to niche crimes in the cyber environment and individual or smaller-scale illicit activity.¹³ This sentiment is echoed by the United States Office of Terrorism and Financial Intelligence, which has taken the view that the volatility associated with digital currencies, combined with their low capitalisation and liquidity, has limited its appeal to illicit actors. Their sense is that, at least for now, terrorists require “real” currency, not digital currency, in order to pay their expenses and fund their activities.

Current regulatory approaches to digital currencies

Domestic

Australia’s AML/CTF regime only regulates those digital currencies that are backed either directly or indirectly by precious metal or bullion.¹⁴ While exact figures are difficult to verify, it appears that this category of digital currency represents only a very small portion of the overall market in digital currencies. As of 20 November 2014, there were over 500 crypto-currencies available for trade in online markets; by comparison, in the previous 14 years to September 2014 there appear to have been only 8 digital currencies backed by gold bullion.

¹² Digital currencies are not immune from security risks, as evidenced through the alleged “loss” of 650,000 Bitcoins by the Mt Gox exchange, or recent accounts of a hacker in Canada generating \$84,000 worth of Bitcoin by gaining access to an internet provider and diverting the computing power of private Bitcoin “mines”.

¹³ AUSTRAC, *Typologies and case studies report 2012*, available online at:

<http://www.austrac.gov.au/files/typ_rpt12_typol.pdf>.

¹⁴ Section 5 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act). While subsection 5(b)(iii) also enables the regulation of digital currencies backed either directly or indirectly by “a thing of a kind prescribed by the AML/CTF Rules”, no such Rules have been issued to date.

Nonetheless, the current legislative regime does allow for limited regulatory oversight over convertible digital currencies. This is because the digital currency ecosystem is still too young to be able to form a “closed loop” economy. In any large-scale transaction or operation “real” funds will need to first be exchanged for digital currency. This will almost always involve some level of interface with traditional financial sectors such as banking and remittance services, which are captured under Australia’s AML/CTF regime. Similarly, at some point the digital currency will need to be exchanged back into legitimate fiat currencies so that the benefit from them can be realised.

At the current levels of adoption, this gives law enforcement agencies some ability to track suspicious money flows into and out of digital currencies and guard against money laundering and other illicit financing threats. However, should digital currencies achieve higher levels of market penetration such that daily financial life could be conducted for long periods fully within a digital currency universe, then the funds would never need to be exchanged back into “real” money and illicit actors would be able to freely transfer and spend the proceeds of their crimes without ever arousing the suspicions of law enforcement.

International

United States

On 18 March 2013, the United States Financial Crime Enforcement Network (FinCEN)¹⁵ released interpretive guidance clarifying the applicability of the regulations implementing the *Bank Secrecy Act* to persons creating, obtaining, distributing, exchanging, accepting or transmitting digital currencies.¹⁶ The guidance note makes a distinction between the various participants in generic digital currency arrangements: a ‘user’ is a person that obtains digital currency to purchase goods or services; an ‘exchanger’ is a person engaged as a business in the exchange of digital currency for real currency, funds, or other digital currency; while an ‘administrator’ is a person engaged as a business in issuing a digital currency and who has the authority to redeem such digital currency.

‘Users’ of digital currency

¹⁵ FinCEN is the Financial Intelligence Unit of the United States.

¹⁶ FinCEN, ‘Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’, available online at: <http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html>.

FinCEN considers that the activities of users do not fit within the definition of ‘money transmission services’ and are therefore not subject to the AML/CTF registration, reporting, and recordkeeping regulations that apply to ‘money services businesses’ (MSBs).

‘Administrators’ and ‘exchangers’ of digital currency

FinCEN considers that an administrator or exchanger that accepts and transmits a convertible digital currency, or buys or sells convertible digital currency for any reason is a money transmitter¹⁷ under the regulations (unless a limitation to or exemption from the definition applies). Accordingly, they will be subject to the full range of AML/CTF registration, reporting, and recordkeeping regulations.

New York State

On 17 July 2014, the New York State Department of Financial Services released details on a proposed ‘BitLicense’ regulatory framework, which places regulations on any company or person that uses Bitcoin and other crypto-currencies residing in New York, for public comment.¹⁸ The proposed regulatory framework contains consumer protection, AML/CTF compliance (including requirements to undertake customer identification and verification and report suspicious transactions), and cyber security rules tailored for digital currency firms.

Under the BitLicense proposal all businesses that: receive, transmit, store or convert digital currency for customers; buy and sell digital currency as a ‘customer business’ (as distinct from personal use); control, administer or issue a digital currency; or perform retail conversions between Bitcoin and fiat or any value exchange, will need to be licensed to operate in New York.

Merchants that accept Bitcoin in payment for goods or services are not included under the rules and regulations.

¹⁷ A ‘money transmitter’ is defined as a person that provides money transmission services, or any other person engaged in the transfer of funds. The term ‘money transmission services’ means “the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.” As the definition of a money transmitter does not differentiate between real currencies and digital currencies, accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations.

¹⁸ See discussion paper, available online at: <<http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf>>.

Canada

Canada has recently undertaken significant regulatory reform in relation to digital currencies. On 19 June 2014, Canada amended its *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) to treat digital currencies as a MSB for the purposes of its AML/CTF regime. Key aspects of the amendments include:

- Dealers in digital currencies will be subject to the record keeping, verification procedures, politically exposed person (PEP) requirements, suspicious transaction reporting and registration requirements that apply to MSBs under the PCMLTFA.
- The amendments do not define “dealing in digital currencies” and it is not known what the defined term will encompass in terms of transactions, though the government has clarified that it will apply only to digital currency exchanges (Digital Currency MSBs).
- Digital Currency MSBs will be required to register with FinTRAC¹⁹ and, if successfully registered, to implement a complete AML/CTF compliance program.
- The amendments extend both to entities that have a place of business in Canada, and entities that have a place of business outside Canada but who direct services at persons or entities in Canada. However, Digital Currency MSBs within Canada that provide services to persons or entities outside of Canada will be exempt from the compliance requirements for those external services.
- Banks are prohibited from opening and maintaining correspondent banking relationships with Digital Currency MSBs that are not registered with FinTRAC.

The amendments have received royal assent, but will not come into force until subordinate regulations and associated guidance have been issued (it is estimated that this process will take anywhere from six to twelve months).

European Union

The European Union’s legal framework in relation to digital currencies is unclear. Within the EU itself, it has been suggested that Bitcoin could fall under the EU’s Electronic Money

¹⁹ FinTRAC is the Canadian FIU.

Directive (2009/110/EC). This Directive uses three criteria to define electronic money: (1) it should be stored electronically; (2) it should be issued on receipt of funds of an amount not less in value than the monetary value issued; and (3) it should be accepted as a means of payment by undertakings other than the issuer.

The European Central Bank (ECB) considers that Bitcoin complies with the first and third criteria, but not the second. The ECB also considers that the conversion of electronic money into another currency (such as Bitcoin) was clearly not envisaged in the Directive.

The EU's Payment Services Directive (2007/64/EC) outlines rules on the execution of payment transactions where the funds are electronic money. However, it does not regulate the issuance of electronic money, nor does it amend the prudential regulation of electronic money institutions as provided for in the Electronic Money Directive. Therefore, the new category of payment service provider it introduces – payment institutions – should not be allowed to issue electronic money. As a consequence, the ECB considers that digital currency clearly falls outside the scope of the Payment Services Directive.

The EU has not yet passed specific legislation relating to the status of digital currencies or Bitcoin as a currency, or in relation to AML/CTF obligations.

United Kingdom

In March 2014, Her Majesty's Revenue and Customs released guidance on the tax treatment of Bitcoin and other crypto-currencies.²⁰

In August 2014 the United Kingdom announced that it was considering the regulation of digital currencies, with a broader public consultation process commencing in early November 2014.

New Zealand

The Reserve Bank of New Zealand has indicated that non-banks do not need approval for schemes that involve the storage and/or transfer of value (e.g. digital currencies), so long as they do not involve the issuance of physical circulating currency (notes and coins). The New

²⁰ HM Revenue and Customs, 'Revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies', available online at: <<https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies>>

Zealand Government has not given any public indication of whether or how it intends to regulate digital currencies in the future.

Intergovernmental approaches

Financial Action Task Force

It is unclear whether, or how, specific FATF Recommendations apply in the context of digital currencies. While the Recommendations do require countries and financial institutions to identify and assess the money laundering and terrorism financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products, there is no express requirement to regulate digital currencies in order to achieve technical compliance with the standards.

In June 2014 the FATF released its report into digital currencies, which was designed to build on the previous guidance issued in relation to New Payment Products and Services²¹ by establishing a common definitional vocabulary and suggesting a conceptual framework for understanding and addressing the AML/CTF risks associated with digital currencies. It is expected that the FATF will issue supplemental guidance in the near future.

Australian Presidency

On 1 July 2014, the former Secretary of the Attorney-General's Department, Mr Roger Wilkins AO, assumed the Presidency of the FATF. Mr Wilkins has indicated that he intends to examine the money laundering and terrorism financing risks associated with digital currencies during his term, and will consider whether further policy measures are needed.²²

Egmont Group of Financial Intelligence Units

The Egmont Group of FIUs meets regularly to find ways to promote the development of FIUs and to cooperate, especially in the areas of information exchange, training and the sharing of expertise.

²¹ See FATF, 'Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services', available online at: <<http://www.fatf-gafi.org/documents/documents/rba-npps-2013.html>>.

²² FATF, 'Objectives for FATF XXVI (2014-2015) - Paper by the incoming President', available online at: <<http://www.fatf-gafi.org/media/fatf/documents/Objectives%20for%20FATF%20XXVI%202014%202015.pdf>>.

Egmont Operational Working Group Project on digital currencies

Egmont has commenced an Operational Working Group Project, of which Australia is a member, on digital currencies to assess the money laundering and terrorism financing vulnerabilities posed by the anonymity of its participants and its cash-like features. The Project aims to provide a better understanding of digital currencies and the features of these technologies that may make it vulnerable to money laundering and terrorism financing activity. It also aims to better understand the stakeholders and key players who operate in this new environment and the risks associated with these technologies, and consider possible ways to mitigate these risks. It is intended that this understanding will serve as a basis for developing more effective regulatory and law enforcement approaches when dealing with and investigating digital currencies.

Developing an effective regulatory system

Industry submissions to the statutory review of the AML/CTF Act

A review of Australia's AML/CTF regime – which is required under section 251 of the AML/CTF Act – commenced in December 2013. The review provides an opportunity to critically examine the operation of the regime, consider issues raised by regulated businesses and government agencies, and determine any enhancements.

Submissions received from the Australian Bankers' Association (ABA) and the Australian Financial Conference (AFC) indicate general uncertainty within the financial services industry around the money laundering and terrorism financing risks associated with digital currencies.²³ Both the ABA and AFC expressed concern that financial institutions were being put in a vulnerable position when offering designated services to the digital currency industry, and recommended that trading in digital currencies be listed as a designated service under the AML/CTF Act.

The Australian Digital Currency Commerce Association (ADCCA), the peak body representing digital currency businesses and other key industry participants, has offered its

²³ Submissions are publicly available on the Attorney-General's Department website: <<http://www.ag.gov.au/consultations/pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx>>.

qualified support for a regulatory approach along these lines. While its stated preference is for a self-regulatory governance framework, it has expressed a willingness to be brought “under the auspices of appropriate regulatory bodies such as AUSTRAC to ensure the highest standards of consumer protection and safeguard national security.”²⁴

Bringing digital currencies within the AML/CTF regime

The use and ongoing expansion of digital currencies is an area of continuing policy interest to the Attorney-General’s Department. A number of options to address the money laundering and terrorism financing issues created by the emergence of digital currency systems are being considered in the context of the statutory review of the AML/CTF Act.

Conclusion

The legitimate use of digital currencies offers many benefits, including increased payment efficiency and lower transaction costs, as well as a reduction in barriers to financial inclusion and an extension of financial services to under-banked and unbanked regions of the world. However, the perceived anonymity and security of digital currencies will be exploited and abused to facilitate the laundering of proceeds of crime and the purchase of illicit goods and services. There are also significant concerns around its potential to be used for the financing of terrorism, which poses risks to Australia’s national security framework.

Regulators and policymakers will need to work closely with industry to minimise legislative uncertainty in this area and encourage the development of digital currency in a way that fosters and utilises its beneficial aspects while securing protection of consumers and businesses against illegal activity and minimising negative national security implications. Digital currencies are, by their very nature, a global phenomenon, and ongoing global cooperation through forums such as the FATF and the Egmont Group will be vital to ensure that a consistent approach that reduces the risk of regulatory arbitrage is adopted internationally.

²⁴ ADCCA Press Release, ‘ADCCA welcomes Senate inquiry into Bitcoin’, 2 October 2014, available online at: <<http://www.adcca.org.au/documents/Press-Release-ADCCA-SI-021014.pdf>>.