Working Group Report

Commonwealth Working Group on Virtual Currencies

October 2015

The Commonwealth

WORKING GROUP REPORT

The Commonwealth Working Group on Virtual Currencies

October 2015

The Commonwealth

Printed and published by the Commonwealth Secretariat.

Contents

Executive Summary

At the Commonwealth Law Ministers Meeting held in Gaborone, Botswana from 5–8 May 2014, Law Ministers, in adopting the Report of the Commonwealth Group of Experts on Cybercrime,[1] 'stressed that cybercrime was a global matter and any weak link provided opportunities for criminals. Prevention was of crucial importance, and the effort to combat cybercrime required collaboration with a wide range of national, regional and international organisations and with the private sector and civil society.' In endorsing the Commonwealth Secretariat's programme of work, the Ministers also accepted the recommendations of the report, which included the proposal that 'every Commonwealth jurisdiction should have an up-to-date and comprehensive legal framework to combat cybercrime'.

To further its mandate to provide technical assistance to Commonwealth member countries, particularly in the areas of cybercrime, anti-money laundering and countering the financing of terrorism (AML/CFT), the Secretariat convened a Round Table on Virtual Currencies from 17–18 February 2015, comprising representatives from ten member countries[2] and from regional and international organisations,[3] which aimed to:

1. raise awareness of emerging trends in the use of virtual currencies among Commonwealth member countries and sensitise states on the need to follow such developments;
2. determine any risks that these trends pose, with a focus on the potential of virtual currencies to be associated with criminal offences, including money laundering and the financing of terrorism;
3. enable member countries to acquire an overview of existing responses and possible new responses to address any harmful impact and to set milestones for future action.

Following the Round Table, representatives from the participating member countries agreed a number of conclusions, outcomes and recommendations, which included:

1. a report on the prevalence and impact of virtual currencies in the Commonwealth (the 'Report'); and
2. the need for technical guidance for member countries on the potential regulatory and legislative measures that could be implemented to effectively respond to virtual currencies (the 'Technical Guidance').

In order to achieve these outcomes, the Secretariat established a Commonwealth Working Group on Virtual Currencies (the 'Working Group'),[4] with membership drawn from all regions of the Commonwealth, including small jurisdictions and international organisations with expertise on virtual currencies, to consider the recommendations of the Round Table. To assist the Working Group in these tasks, the Secretariat undertook

1 Commonwealth Secretariat, *Report of the Commonwealth Working Group of Experts on Cybercrime*, LMM(14)14, London, 2014.
2 Barbados, Ghana, Jamaica, Kenya, New Zealand, Nigeria, Singapore, Tonga, Uganda and the UK.
3 The African Union, the Council of Europe, the United Nations Office on Drugs and Crime (UNODC), INTERPOL, the International Monetary Fund (IMF) and the Eastern and Southern African Anti-Money Laundering Group.
4 Australia, Barbados, Kenya, Nigeria, Singapore, Tonga and the UK, with the IMF, World Bank, Interpol and UNODC, chaired by Colin Nicholls QC

a survey of the prevalent virtual currencies in eight member countries,[5] as well as research into the regulatory responses in some economies within the Commonwealth, to provide a cross-section of Commonwealth experience of virtual currencies. The results of the surveys and the research, which are included in this report, have disclosed that member countries have adopted a diverse range of approaches to virtual currencies, from that of Bangladesh, which has declared them illegal, to that of Canada which, although recognising their legality, has sought to regulate the high risks involved in their use.[6] Although some jurisdictions have yet to formally appreciate the nature and impact of virtual currencies, those that have done so demonstrate a variety of disparate responses, including some which are limited, uncoordinated and fragmentary.[7]

To deepen their understanding of virtual currencies, the Working Group received presentations from experts[8] from the banking sector, academia, virtual currency operators and users and law enforcement during the first half of its meetings held on 24–26 August 2015.

Although this report is primarily concerned with the development of legislative and regulatory responses to mitigate risk, it also seeks to confirm the express recognition of members of the Round Table that virtual currencies have the potential to accrue significant benefits for Commonwealth member countries.

The evidence of criminality in the use of virtual currencies discloses a critical need for an effective and co-ordinated legislative and regulatory response by member countries. Just as in other types of cybercrime, if countries "*are not supported in developing and maintaining security and other capacities at levels consistent with other countries, they risk becoming attractive to offenders as a safe haven from which other locations can be attacked*". [9]

The Working Group concluded that:

1. virtual currencies are prevalent in almost every member country and within every region of the Commonwealth;
2. virtual currencies have the potential to benefit member countries and to drive development, but they also involve risks, particularly as regards their use by criminals for money laundering, terrorist financing and cyber and cyber-enabled crime;
3. with the exception of one member country,[10] in which virtual currencies have been declared unlawful, the majority of member countries have recognised their advantages and treat their use as lawful;
4. prohibition of virtual currencies is unlikely to be effective. In some member countries in which regulation has been adopted, it has been limited, unco-ordinated and fragmentary. There remain significant areas in which regulation is required;

5 Ghana, India, Jamaica, Kenya, Nigeria, South Africa, Trinidad and Tobago and Uganda

6 Virtual currencies are in use in 46 of 53 member countries, based upon client download statistics. The list of the jurisdictions is in the report.

7 See, Conclusion 4.

8 The UK Digital Currency Association; British Banking Association; BitPesa, a Kenyan remittance service using virtual currencies; Bitt, a Barbadian virtual currency exchange; Bankymoon, a South African virtual currency-using business; Minku, a Nigerian virtual currency-using business; Prof. Alan Woodward, University of Surrey; Dr Sarah Meiklejohn, University College London; and Ripple Labs, a US-based provider of decentralised payment services.

9 Commonwealth Secretariat, *Report of the Commonwealth Working Group of Experts on Cybercrime*, LMM (14)14, London, 2014, at paragraph 64.

10 Bangladesh; See, ibid, paragraph 60.

5. although the Financial Action Task Force (FATF) Recommendations and Guidance on virtual currencies have provided a global response, they are limited to AML/CFT.

The Working Group recommended:

1. **Legality**: Member countries should be encouraged to make a positive determination on the legality of virtual currencies in their respective jurisdictions.

2. **Awareness**: Member countries should be encouraged to foster an awareness of virtual currencies within their jurisdictions and the potential risks involved in their use (including but not limited to the money laundering and terrorist financing (ML/TF) risks of virtual currencies and the risk to consumers). Financial regulators and central banks should consider making public statements on the legality of virtual currencies and the applicability of any existing legislative frameworks. Education and funding should be provided for training for law enforcement.

3. **Legal frameworks**: Member countries should be encouraged to consider the application of their existing legal frameworks to virtual currencies and, where appropriate, should adapt them or enact new legislation to regulate virtual currencies. Where member countries consider it necessary to legislate in response to cyber or cyber-enabled crime, they should be encouraged to have regard to the provisions of the Commonwealth Model Law on Computer and Computer Related Crime, and related Commonwealth documents, in particular:

    a. **Taxation**: Tax authorities are encouraged to make public statements clarifying the appropriate taxation regimes applicable to virtual currencies and transactions relating to their use as a medium of exchange. Where appropriate, tax authorities are encouraged to adapt and extend existing taxation regimes to virtual currencies.

    b. **Proceeds of crime**: Member countries should be encouraged to consider revising their proceeds of crime legislation to ensure that it is adequate to encompass the potential transmission of benefit by criminals using virtual currencies.

    c. **Consumer protection**: Member countries should consider the possibility of extending their consumer protection legislation to include purchases of virtual currencies as well as consumer transactions using virtual currencies as a medium of exchange.

    Any regulatory and legislative frameworks should focus on interactions with fiat currencies and avoid attempting to regulate the underlying decentralised ledger technology. Such frameworks should be technologically neutral and avoid stifling innovation.

4. **The FATF guidance and recommendations**: Member countries are encouraged to implement the FATF guidance for a risk-based approach to virtual currencies (June 2015) by bringing entities transacting at the intersection of fiat and virtual currencies within existing AML/CFT regimes.[11] This should include applying existing registration or licensing requirements to such entities, including, where appropriate, mutual recognition of licenses granted in one jurisdiction in other Commonwealth jurisdictions.

11 FATF/OECD, *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF, Paris, France.

5. **Law enforcement**: Member countries should consider developing and improving the capacity of law enforcement, especially in the areas of digital forensics and analytics. This should include the training of prosecutors, judges and regulatory authorities.

6. **Co-operation**: The Commonwealth Secretariat and other international partners should create a digital repository of best practice and model regulations as part of an online community to assist member countries in developing their policies and capacity to respond to virtual currencies. Capacity-building activities for relevant public sector stakeholders should also be considered:

    a. Member countries should encourage the establishment of industry associations within their jurisdictions to support the development of a responsible and sustainable virtual currency industry. Where such associations already exist, member countries should be encouraged to proactively engage with them and encourage responsible behaviour among their members, for example by establishing or promulgating industry standards and accreditation models.

    b. Clear information-management systems should be established between industry sectors to share information regarding suspicious transactions, to enhance co-operation in support of the development of a risk-based approach to the industry, and to allow a fair appraisal of strengths and weaknesses within compliance models.

Introduction

1. Although virtual currencies are not new, global interest in them has recently reached unprecedented levels. This is due as much to the incidence and fear of their abuse by criminals as to the benefits they bestow. Interest has been exacerbated by the versatility and myriad applications of a decentralised technology which underpins virtual currencies such as Bitcoin.

2. In fulfilling its mandate, the Commonwealth Working Group on Virtual Currencies has adopted the Financial Action Task Force (FATF) definition of virtual currencies as: 'a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account and/or a stored value, but does not have legal tender status in any jurisdiction'.

3. Although this formulation represents a generic working definition, it does not provide an exhaustive understanding of the concept. This is due to the many forms of virtual currencies, each exhibiting different characteristics in their operation and interaction with the physical world. Whereas some virtual currencies have a centralised administrative authority or system, such as in computer gaming environments, others, such as Bitcoin, are highly decentralised, operating on a peer-to-peer basis with no central monitoring authority and offering a high degree of anonymity.

4. In addition to being centralised or decentralised, virtual currencies can be 'static' (non-convertible to fiat currency), 'unidirectional' (able to be either purchased or sold in return for fiat currency) or 'bidirectional' (able to be both purchased and sold in return for fiat currency). Most decentralised virtual currencies fall within the category of 'cryptocurrencies', in that they rely on a process of cryptography for security and anti-counterfeiting measures. Bitcoin currently represents the most widely used cryptocurrency, with a market capitalisation of over US$4.36 billion.[12] Other cryptocurrencies including Litecoin, PayCoin, BitShares, Stellar, Dogecoin and Darkcoin have a combined market capitalisation of just over US$1 billion.

5. Virtual currencies such as Bitcoin are regularly used for lawful purposes, are a driver for innovation and have the potential to assist member countries in achieving their developmental goals. Whereas the acquisition of fiat currencies is subject to inherent geographical limitations, there are no such limitations on the acquisition of convertible virtual currencies. This is a matter of public concern, as their decentralisation and high degree of anonymity increases the potential of virtual currencies to facilitate crime.

6. There has been an increasing interest from traditional financial institutions and investors in virtual currencies. Barclays Bank has, for example, selected three Blockchain start-ups for its business accelerators. Venture capital investment has also increased significantly, with a near doubling of investment in Bitcoin-related undertakings from October 2014 to March 2015. Interestingly, this period saw Africa gain its first start-up, which attracted about US$1.1 million of investment in Kenya.[13]

---

12 Australian Senate (2015), Digital Currency – Game Changer or Bit Player, Economic References Committee, Canberra, ACT, Australia, at Section 3.22.

13 P. Rizzo, (2015), *Pantera Leads $1.1 Million Funding for African Bitcoin Startup BitPesa*, CoinDesk, 9 February 2015, available at <http://www.coindesk.com/bitpesa-1-1-million-bitcoin-africa> (last accessed 9 December 2015).

7. The technology that lies behind virtual currencies – the decentralised ledger – in addition to recording the value in transactions, has its own broader utility, supporting, for example, carbon-trading systems, the registration of Kimberley protocol-compliant diamonds, voting systems, insurance markets and corporate governance systems. This provides a major incentive for countries to avoid the regulation of technology and instead focus on interactions with fiat currencies. The former risks stifling the development of potentially transformative new technologies capable of delivering both economic development and efficient delivery of key public services. Significant exploratory studies are under way into such innovative uses of the technology, it is unfortunately beyond the scope of this report to discuss them.

8. The dichotomy between the actual/potential economic and social benefits of virtual currencies and the actual/potential exploitation for criminal purposes has generated the public debate that is the subject of this report. The debate gives rise to many questions:

   - Are national laws adequate to cover virtual currencies?
   - Should national laws be amended to accommodate the use of virtual currencies, or new laws be promulgated?
   - What degree of governmental scrutiny is required?
   - If regulation is desirable, what form should it take and how far should it go? What guidance can usefully be given to member countries and to those using virtual currencies?

   These are the questions currently exercising the governments of member countries and which this report seeks to answer.

9. Thus far, Bitcoin has been scrutinised by regulatory agencies. Such responses have been characterised as 'intentionally vague and speculative' as to how and when such enforcement would take place.[14] However, the United Nations Office on Drugs and Crime (UNODC) predicts that the trend for regulation will increase.

Methodology

10. In compiling this report, the Working Group has drawn on a variety of sources.

11. In order to obtain information to assist the Working Group, the Commonwealth Secretariat developed a survey on the prevalence and effect of virtual currencies on the economies and legal systems of Commonwealth member countries. Eight member countries were chosen for the review with the aim of achieving a good geographic spread. The member countries surveyed were: Ghana, India, Jamaica, Kenya, Nigeria, South Africa, Trinidad and Tobago and Uganda.[15] Respondents with expertise in cybercrime were recruited in each jurisdiction to complete the survey. The outcomes from the survey have been incorporated into this report.

12. The Working Group also sought to elicit first-hand evidence as to the prevalence and effect of virtual currencies not only in the Commonwealth but also globally. In pursuit of this objective, the Working Group invited a number of persons and institutions from across the Commonwealth and internationally to assist the Group with the benefit of their knowledge and experience.

14 N. Godlove, (2014), *Regulatory Overview of Virtual Currency*, Oklahoma Journal of Law & Technology, Vol. 10, 1–67 at 1.

15 A complete list of contributors above.

13. The meeting received presentations from the following institutions and individuals:

    - UK Digital Currency Association;
    - British Banking Association;
    - BitPesa, a Kenyan remittance service using virtual currencies;
    - Bitt, a Barbadian virtual currency exchange;
    - Bankymoon, a South African business using virtual currency;
    - Minku, a Nigerian virtual currency-using business;
    - Professor Alan Woodward, University of Surrey;
    - Dr Sarah Meiklejohn, University College London; and
    - Ripple Labs, a US-based provider of decentralised payment services.

14. The Working Group has consulted authoritative reports and guidance produced by internationally respected third parties. Some of these have received a specific mandate from states, including Commonwealth member countries, giving them a locus that is specifically relevant to the challenges presented by virtual currencies. The Working Group has had recourse to the FATF Guidance on Virtual Currencies, an authoritative source of policy on anti-money laundering and countering the financing of terrorism (AML/CFT). Some Commonwealth countries are members, or associated members, of FATF.[16] The Working Group has also had recourse to reports of the Australian Senate and the UK House of Commons, and has consulted relevant US government agencies,[17] INTERPOL, Europol and UNODC.

15. The Secretariat also obtained access to a 'darkweb crawler', giving it the ability to search through Tor sites[18] and other hidden portions of the internet for illegal activities within member countries using virtual currencies. At the time of writing this report, access to this facility had only just been obtained and, as a result, systematic pan-Commonwealth results are not yet available. This facility has been used to provide insights into regions of the Commonwealth that were not covered by the survey, in particular the Pacific region.

16. This report attempts a systematic analysis of the Commonwealth experience, although owing to the lack of available statistics, it has in many cases only been possible to provide examples. As a result, it is more a review of the most readily discernible trends and behaviours of virtual currencies than a definitive statement on their use within the Commonwealth.

17. Any policy development process relies on clarity of communication. It is therefore crucial to draw upon a common set of terms to enable the effective analysis of policy challenges. This is particularly so in the case of virtual currencies, given the breadth of approaches and initiatives and the need to ensure that any terminology is shared. A comprehensive list of the definitions relied upon by this report is provided at the end of the report.

16 With the exceptions of Cameroon, Kiribati (which has observer status with the Asia/Pacific Group on Money Laundering) and Tuvalu.
17 The Federal Bureau of Investigation, the Department of Justice and the US State Department.
18 Websites on a hidden and anonymised portion of the internet; see 'Definitions'.

Part 1: The Prevalence of Virtual Currencies in Commonwealth Member Countries

Prevalence according to known usage

18. **Virtual currencies are prevalent in almost every member country and within every region of the Commonwealth**.[19] Most users employ them simply to conduct transactions; however, some users also participate in the system architecture by ratifying transactions and supporting communication within virtual currency networks. The latter users are called 'miners' because they 'mine', that is, validate the transactions. The users in the community do not know each other, yet they are able to co-ordinate sufficiently to sustain the entirety of the transaction.[20]

19. The anonymisation technology inherent in many virtual currencies makes it extremely difficult to ascertain the number or value of transactions taking place within a particular jurisdiction and the location of the persons conducting them. However, certain indicators can provide insights into their presence. These are the frequency of client software downloads, the purposes for which the currencies are used and the incidence of 'mining' in Commonwealth jurisdictions.

Client software downloads[21]

20. A person who wishes to start using a virtual currency commonly downloads a virtual currency 'client' (i.e. a wallet)[22] via an online software repository. Publicly available information of the number of such downloads within member countries provides a useful indication of the prevalence of virtual currencies within the Commonwealth as a whole. Owing to practical limits on time and resources, the Working Group's review has been limited to one currency, Bitcoins, and to one software repository.[23] As a result, the statistics referred to in this report should be treated as illustrative only.

21. The Bitcoin Core wallet client has been downloaded 784,066 times within the Commonwealth from the SourceForge online repository (Table 1.1).[24]

---

19 See, Conclusion 1. A total of 46 out of 53 member countries, based upon client download statistics.

20 Presentation to Commonwealth Working Group on Virtual Currencies by Adam Vaziri, UK Digital Currency Association, 24 August 2015.

21 The term 'client' refers to the end-user software that facilitates the secure use and transmission of virtual currency. Clients are also commonly referred to as 'wallets'.

22 It should be noted that users might also make use of virtual currencies using purely online hosted wallets, accessed via a web browser.

23 See, <http://sourceforge.net>.

24 Data correct as of 30 July 2015.

Table 1.1. Showing downloads of Bitcoin Core client by member country

Member country	Downloads per 100,000 internet users	Member country	Downloads per 100,000 internet users
Canada	691	Malaysia	72
Australia	660	Botswana	67
New Zealand	578	Tonga	51
Malta	499	Ghana	49
United Kingdom	494	Guyana	37
Cyprus	381	Sri Lanka	27
Singapore	369	Fiji	26
Dominica	348	Vanuatu	25
Antigua and Barbuda	216	India	24
Barbados	180	Pakistan	22
Bahamas	160	Sierra Leone	20
St Vincent and the Grenadines	157	Cameroon	18
Trinidad and Tobago	156	Bangladesh	14
Belize	150	Mozambique	13
Brunei-Darussalam	125	Kenya	11
St Lucia	117	Rwanda	8
Mauritius	98	Solomon Islands	7
Namibia	98	Uganda	6
Jamaica	93	Papua New Guinea	6
Seychelles	93	Lesotho	6
St Kitts and Nevis	86	Malawi	5
Tanzania	84	Samoa	5
South Africa	78		
Malaysia	72		
Botswana	67		

Node activity

22. Nodes are responsible for broadcasting information across the system and are an important component of the Bitcoin network. The number of nodes participating in a virtual currency network can indicate the extent of virtual currency use. Nodes are also cited as a main indicator of the 'health' of a virtual currency network (Table 1.2).[25] This information was obtained from the Bitnodes map and is updated every 24 hours.[26]

25 J. Matonis, (2014), *12 Ways to measure the Bitcoin Network's health*, CoinDesk, 27 September 2014, available at <http://www.coindesk.com/12-ways-measure-Bitcoin-networks-health> (last accessed 9 December 2015).

26 Bitnodes, available at <https://getaddr.bitnodes.io>.

Table 1.2. Bitcoin nodes by member country[27]

Member country	Nodes per 100,000 internet users
Singapore	1
South Africa	0.04
Malaysia	0.07
Mozambique	0.08
Cyprus	0.39
New Zealand	0.44
United Kingdom	0.66
Australia	0.71
Canada	0.94
India	0.001

Mining and transaction verification

23. Participation in the transaction verification process (in the case of Bitcoin called 'mining') is another means of acquiring virtual currencies and is capable of demonstrating their prevalence within a particular jurisdiction.

24. However, it does not provide a particularly reliable means of determining prevalence and is drawn from survey responses. The result of this is that this information is not as comprehensive as that relating to client software downloads or node activity.

25. In many member countries, for example, Ghana, Jamaica and Trinidad and Tobago, it has not been possible to detect instances of mining, although there is no evidence to suggest that it is absent. Other member countries, in contrast, have witnessed significant participation in mining. Some miners tend to choose a coin that is profitable and less difficult to mine. Owing to the lower barrier to entry, miners operating in, for example, South Africa, have typically mined Altcoins (i.e. coins other than Bitcoins).

26. Bitcoin mining has been taking place in India where individuals have been involved in virtual currency payment processing, especially in Bitcoin mining pools called 'pool mining'. Coinsecure.info, an Indian Bitcoin start-up, provides real time data on Bitcoin mining activity in India that is collated from Blockchain.info. Anecdotal evidence suggest that individuals have used the technology infrastructure present in scientific and academic institutions for payment-processing work.

27. Miners are also present in Kenya. An interesting illustration of this arose where an individual in Nairobi sought support via an online micro-lending community to purchase greater mining capacity.[28]

28. Some countries are involved in manufacturing equipment specifically for mining, and some internet service providers (ISPs) have contemplated providing mining at a national level.

27 Data correct as of August 2015.

28 See, for example, <https://www.zidisha.org/loan/increase-my-Bitcoin-coud-mining-daily-pay-outs> (last accessed 9 December 2015).

29. An interesting development is the exploration of hosting mining services by South African ISPs. It has been reported that members of the ISP Association (ISPA) have discussed costing models for hosting Bitcoin mining. ISPA is a South African internet industry body,[29] established in 1996, which currently represents in excess of 150 ISPs with a diverse range of services and target markets. It has also been reported that the commercial manufacture of mining equipment and accessories is being undertaken in South Africa.[30]

Conclusion

30. The use of virtual currencies in a wide range of member countries is evidenced by the fact that the Bitcoin core wallet has been downloaded in 46 of 53 member countries and across all regions. It is perhaps to be expected that, generally, those member countries with the highest levels of internet penetration have the highest rates of client downloads. However, there is a trend in a number of small member countries – particularly island jurisdictions in the Caribbean – for high numbers of client downloads proportionate to the number of internet users. This may be linked to their proximity to large numbers of internet users in North America or perhaps to the region's large offshore banking industry. Although the number of nodes is significantly smaller, it is interesting to note that two African member countries, namely Mozambique and South Africa, have active nodes. It must, however, be acknowledged that these conclusions are based upon the limited information available. Although it can be concluded that virtual currencies are used across the Commonwealth, their rates of usage and prevalence are more difficult to determine.

Types of Use

Introduction

31. People use virtual currencies in member countries for a variety of purposes. The most obvious of these is the provision of goods and services. Other types of transaction, including the sale and lease of heritable property and those involving payment products and services, are present at a sufficient level to be readily detectable. Owing to the relative youth of virtual currencies and the lack of mandatory reporting requirements, it is difficult to obtain significant quantitative data on their types of use. It has, therefore, been difficult to quantify the prevalence of virtual currencies. Instead, this report provides an overview of the use-cases that are currently active in member countries.

32. Where such information is available, it has been included in this report, but it is very likely that the rates of use and economic influence go far beyond the examples reported below. Given the anonymous nature of these technologies, it can be assumed that their use for criminal purposes is greater than that suggested by the evidence available for this report. Based upon the information below, it can be concluded that their use, lawful or otherwise, is not insignificant within member countries' economies. This presence and the potential for growth in use may be felt by member countries to necessitate the development of adequate policy responses.

---

29 The Minister of Communications formally recognised ISPA as an industry representative body in terms of section 71 of the Electronic and Communications Act 25/2002 in 2009.

30 For example, Open Rigs, at <https://openrigs.com which manufactures> racks for mining clusters and has its registered postal address in the Western Cape, South Africa.

33. The use of virtual currencies to perform standard financial transactions offers a potential way to measure their influence. The types of transactions to consider include:

    - provision of goods and services;
    - sale and lease of property;
    - provision of payment products and services;
    - use by civil society; and
    - criminality associated with virtual currencies.

Provision of goods and services

34. Virtual currencies, as simple representations of value, have the ability to perform a variety of functions, but it is their ability to provide a substitute for traditional fiat currency, as the basis of exchanges for goods and services, that is a key component of their economic worth. Business transactions using electronic communications technologies in place of physical exchange (e-commerce) now account for 5 per cent of global sales.[31]

35. Bitcoins can be used to purchase goods and services, both where a vendor is resident in the same jurisdiction as the purchaser and also remotely, relying on postal services to deliver goods or by using communication technology to provide services remotely.

36. Goods and services can be purchased remotely using Bitcoins (via merchant solutions or with bespoke commerce plugins) and delivered or provided remotely to residents (i.e. within South Africa). Some suppliers such as Overstock.com or coinsfortech.com will ship products to postal addresses in jurisdictions including Nigeria, South Africa, Trinidad and Tobago and Kenya.

37. Normally, some form of identification is required to receive these goods and services, for example, an email address; full name; billing and shipping addresses; country; city; state; postal code and telephone number. However, there does not appear to be any means of verification attached to such processes[32] and this facilitates the dissemination of illegal goods and services.

38. Although the acceptance of virtual currencies as a mode of exchange is often entirely legitimate, it can also facilitate cybercrime and cyber-enabled crime. For example, the ability to purchase airtime on pre-paid mobile phones, airline tickets or computer equipment using untraceable funds can be extremely valuable to criminals.

39. The online purchasing of mobile phone airtime using virtual currencies, which is expressly advertised as not requiring registration, is available in many member countries through the mobilehop.ph service.

40. There is also a facility for black market items including SIM cards, recreational and other drugs and arms to be shipped to Jamaica.

---

31 This includes both fiat and virtual currency transactions. See, BizReport, *Global ecommerce sales* top U.S.$1 trillion, 1 August 2013, available at <http://www.bizreport.com/2013/08/global-ecommerce-sales-top-us1-trillion.html> (last accessed 9 December 2015).

32 See, N. Bohm, & S. Mason, (2010), *Identity and its verification*, Computer Law & Security Review, Vol. 26 No. 1, 43–51, available at <http://www.stephenmason.eu/wp-content/uploads/2011/01/bohm-mason-identity.pdf> (last accessed 9 December 2015).

Member countries

41. The Working Group's survey has disclosed that merchants have adopted virtual currencies as methods of payment for goods in several member countries. These include:

- **Australia and New Zealand**: Merchants accepting Bitcoin have sprung up in diverse industries including wine, jewellery making, food and beverage, web design, plumbing and healthcare.[33]
- **India**: Bitcoins have been accepted in restaurants,[34] for the sale of concert tickets[35] and on HighKart.com – India's first Bitcoin-only online shopping portal. Werwired.com, a geospatial and surveillance company located in Bangalore has developed a pilot project in an attempt to deliver Indian products globally using Bitcoins, via the website 'MadOverCoins'.
- **Jamaica**: Virtual currencies have been used to deliver goods and services, for example, healthcare services.[36]
- **Kenya**: Several merchants accept Bitcoin in exchange for their services including a technical solutions company,[37] a company providing outdoor cooking equipment,[38] and several travel companies.
- **Nigeria**: There is some evidence of entrepreneurs and small and medium-sized enterprises using virtual currencies in Nigeria, although there are few compelling reasons for merchants to adopt virtual currencies.[39] For example, Minku Designs, a Nigerian fashion design company, has used Bitcoin as a means of payment in its online store, becoming the first Nigerian company to do so. However, even companies like Minku Designs, which actively market themselves as accepting virtual currencies, have seen limited adoption among their customer base.
- **South Africa**: Its largest online retailer and a prominent pay platform have integrated Bitcoin into the checkout processes of over 30,000 merchants using its service.
- **Singapore**: Numerous brick and mortar entities advertise themselves as being willing to sell goods and services in exchange for Bitcoin, including bars and cafes, gift shops, clothing stores, hair salons, tuition centres, gold and silver bullion suppliers, information technology equipment stores, and medical equipment stores.[40]
- **Uganda**: No officially registered merchants appear to be transacting business in or accepting virtual currencies. However, on the 'dark web', instances have been detected of individuals and small groups using Bitcoin

33 *Ibid.*
34 A. Nandakumar, & R. Maruvada, (2014), *RBI puts the brakes on the Bitcoin train in India*, Reuters, 17 January 2014, available at <http://blogs.reuters.com/india/2014/01/17/rbi-puts-the-brakes-on-the-Bitcoin-train-in-india> (last accessed 9 December 2015).
35 S. Shinde, (2015), *Soon, buy a flat, pay restaurant bills using Bitcoin*, Economic Times, 26 March 2015, available at <http://www.business-standard.com/article/companies/soon-buy-a-flat-pay-restaurant-bills-using-Bitcoin-115032600991_1.html> (last accessed 9 December 2015).
36 See, <http://www.kingstonopenmri.com/health-insurance.html> (last accessed 9 December 2015).
37 See, Wageni Technologies, at <http://wagenitech.com> (last accessed 9 December 2015).
38 See, Cookswell, <http://cookswell.co.ke> (last accessed 9 December 2015).
39 Presentation to Commonwealth Working Group on Virtual Currencies by Kunmi Otitoju, Chief Executive, Minku, 24 August 2015.
40 See, <https://coinmap.org/#/map/1.29061274/103.85204315/12> (last accessed 9 December 2015).

as a mode of payment. One example, which has gained some notoriety via message boards such as Reddit[41] and other social networking sites such as Twitter, is an unnamed taxi driver who accepted Bitcoin payment for a taxi fare from Entebbe International Airport to Kampala City. Such reports are difficult to verify.

42. These cases illustrate the uptake of virtual currencies as a medium of exchange within member countries. Although it is difficult to quantify their impact on the economies of member countries, their use and potential for abuse illustrates the need for clear responses from member countries to ensure that any growth takes place in a responsible and sustainable fashion.

Sale and lease of immoveable property

43. Instances of individuals seeking to sell immoveable property have been reported in Kenya and South Africa. In Jamaica, there have been instances of property being offered for rent in return for Bitcoin.[42] No such instances have been reported in Trinidad and Tobago, Kenya or Uganda. Although as yet unreported, such transactions are legally possible in some member countries, for example Ghana, where there is no requirement for transactions involving heritable property to be in the form of fiat currency. In other member countries, there may be requirements for the consideration in heritable property transactions to be fiat currency, as is the case in Tonga. In May 2015, an online market advertised residential and commercial properties for sale in Tonga and the Fiji Islands for Bitcoins valued at more than US$1.7 million.[43]

Investments

44. Virtual currencies have also been purchased as a form of investment: investors seek to make a capital gain on the comparative fiat currency value of a virtual currency. Indeed, a practice termed 'hoarding' has been observed. Users will acquire Bitcoins and hold it as a form of speculative investment, instead of using it as a means of payment. This behaviour becomes prevalent when Bitcoin prices in fiat are lower and is similar to investing in commodities, particularly gold. It is estimated that approximately 70 per cent of Bitcoins have been hoarded for a period of at least 6 months.[44]

Provision of payment products and services

45. As has been observed by the European Central Bank[45] and FATF, there are emerging markets in the provision of payment products and services, allowing the intersection of the fiat and virtual currency sectors. The availability of such services within member countries is indicative of the use of virtual currencies within those jurisdictions. Where they are observed it makes a compelling case for clear regulatory and legislative frameworks to assist the responsible and sustainable growth of markets.

---

41 An online bulletin board system where users can generate their own content by submitting posts and links which are then voted on by community members to decide the order of their appearance on the site.

42 See, <http://islandvillasjamaica.com> (last accessed 9 December 2015).

43 See, <https://www.bitpremier.com> (last accessed 9 December 2015).

44 Cryptocoin News (2014), *70% of bitcoins have been hoarded for six months or more*, 24 November 2014, available at <https://www.cryptocoinsnews.com/70-bitcoins-hoarded-six-months> (last accessed 9 December 2015).

45 European Central Bank (2015), *Virtual Currency Schemes – A Further Analysis*, Frankfurt am Main, Germany.

46. Those currently observed in member countries are:

- payment platforms and exchange services;
- automated teller machines (ATMs);
- peer-to-peer exchanges; and
- remittance services.

Payment platforms and exchange services

47. Although payment platform services and exchanges are here discussed together (by virtue of often being services offered by the same commercial undertaking), it is important to note that these two functions are conceptually distinct.

- **India**: In India, exchanges have been established, and local banking support has been provided, in the context of a highly uncertain regulatory environment. This has resulted in many exchanges and virtual currency communities suspending operations. For example, India's first real-time Bitcoin exchange, BTCXIndia, suspended its operations after its banking partner withdrew its support to the business.[46] Also, LaxmiCoin, publicised as India's 'own version of the Bitcoin', suspended operations seeking further 'regulatory clarifications'.[47]

- **Kenya**: Within the Kenyan economy, commercial exchanges are well established. There has been a proliferation of virtual currency exchanges in Kenya. Perhaps the most high-profile example is the establishment of BitPesa, which offers commercial exchange and remittance services via virtual currencies. Initially focused on offering money transfer services from the United Kingdom to Kenya, BitPesa's service is expanding and has been the subject of a US$1.1 million private equity investment. This is arguably an illustration of the market view that the use of virtual currencies is likely to increase significantly in the East African region.[48] An expansion of BitPesa's services into Tanzania and Uganda is also reportedly planned for 2015.[49]

  An interesting development that has taken place in Kenya is the convergence of virtual currencies and the M-Pesa system. This effectively provides a new intersection between the fiat financial system and virtual currencies. Until recently, online exchanges were available via Kipochi and M-Pesa. M-Pesa is a Unstructured Supplementary Service Data application that runs on mobile phones supported by the major subscriber in Kenya, Safaricom. This means that all mobile phone users with Safaricom sim cards have access to M-Pesa and, consequently, can own Bitcoins. Using Kipochi (an electronic wallet), M-Pesa users can buy Bitcoins and store them in their Kipochi account. They can also send and receive Bitcoins and convert them

46 R. Vaisoha, (2015), *India's Bitcoin Exchange BTCXIndia to Close Following Loss of Banking Support*, Cointelegrah, 12 May 2015, available at <http://cointelegraph.com/news/114224/indias-Bitcoin-exchange-btcxindia-to-close-following-loss-of-banking-support> (last accessed 9 December 2015).

47 The Hindu (2014), *Bitcoin impact: Laxmicoin seeks regulatory clarity for launch*, 7 January 2014, available at <http://www.thehindu.com/business/Economy/Bitcoin-impact-laxmicoin-seeks-regulatory-clarity-for-launch/article5549324.ece> (last accessed 9 December 2015).

48 P. Rizzo, (2015), *Pantera Leads $1.1 Million Funding for African Bitcoin Startup BitPesa*, CoinDesk, 9 February 2015, available at <http://www.coindesk.com/bitpesa-1-1-million-bitcoin-africa/> (last accessed 9 December 2015).

49 Presentation to Commonwealth Working Group on Virtual Currencies by Anna Mance, General Counsel, BitPesa, 24 August 2015.

to normal currency. Kipochi's integration to M-Pesa was shut by Safaricom a few weeks after its launch. It is reported, however, that negotiations are under way to permit the integration of the two systems.

Another service, Igot, also facilitates exchanges between virtual and fiat currencies via M-Pesa. Igot acquired TagPesa, a Kenyan cryptocurrency exchange and remittance gateway, in 2015. It then integrated that exchange into M-Pesa's mobile payments service. Igot's Kenyan customers can use the exchange's services by depositing and withdrawing Kenyan shillings either from their local bank accounts or from their M-Pesa accounts.

The familiarity of consumers with mobile money, particularly in Kenya but also elsewhere in Africa, has been reported as a significant asset to service operators who note that their prospective customers have little difficulty understanding the technology of virtual currencies.[50]

- **Nigeria**: The South African exchange, ICE3x, has also launched a Bitcoin processing service in Nigeria. Together with a local service, VoguePay, there has been an introduction of services to merchants in Nigeria.[51] A number of other entities are offering payment-processing services in Nigeria for users of virtual currencies.[52]
- **South Africa**: Infrastructure to support the interaction of virtual currencies and fiat currencies exists within South Africa. This is evidenced by, inter alia, three active exchanges[53] and active services/applications.[54] Since the establishment of the first exchange in South Africa in 2013, the value of transactions that have taken place there is estimated at EUR 7,484,519.00.[55]
- **Trinidad and Tobago**: An exchange, Bitt, is reportedly in the process of being launched. It is based in Barbados but offers services to consumers in Trinidad and Tobago. Bitt is built on the AlphaPoint Exchange platform, which states that it 'Supports all popular digital currencies'. It currently implements Bitcoin, Litecoin and all other alt-coins.

48. In many other member countries, such exchange services are yet to be established. This includes Ghana,[56] Jamaica and Uganda. However, although such member countries may lack an in-country exchange, such services are available over the internet. For example, in Ghana there is no evidence of IP address blocking of virtual currency exchanges by authorities. In such jurisdictions, the only limitation on the availability of access to exchanges arises when the exchanges themselves block transactions originating from Ghanaian IP addresses. Such measures may be rendered ineffective when a person uses electronic counter-measures to alter their IP address in order to access such services.

50 Presentation to Commonwealth Working Group on Virtual Currencies by Anna Mance, General Counsel, BitPesa, 24 August 2015.

51 J. Southurst, (2015), *ICE3x Launches Nigeria's First Bitcoin Exchange*, CoinDesk, 7 January 2015, available at <http://www.coindesk.com/ice3x-launches-nigerias-first-Bitcoin-exchange> (last accessed 9 December 2015).

52 Such entities include PayOption, GoldRush Nigeria, StandardGold Nigeria and Nigeria GoldExchange.ng.

53 See, <https://bitx.co/market>; <https://ice3x.com> and <https://www.altcointrader.co.za>.

54 See, for example, <https://www.zapgo.co>.

55 This is based upon publicly available data (to 4 June 2015) relating to the activities of the following exchanges, which are active in South Africa: BitX, Ice3x, LocalBitcoins.com. The currencies operated are Bitcoins and LiteCoin.

56 To the knowledge of the Bank of Ghana.

ATMs

49. There are 129 Bitcoin ATM machines reported to be operating in member countries including Australia,[57] Botswana,[58] Canada,[59] New Zealand,[60] Singapore,[61] South Africa[62] and the United Kingdom.[63]

50. Although some ATM machines, such as those manufactured by Genesis Coin Inc., may have cameras and fingerprint readers, presumably to enable 'know-your-customer' (KYC) facilities, it is not currently clear whether or not any AML/CFT features are operational on the machines deployed in member countries.

Peer-to-peer exchanges

51. Peer-to-peer exchanges of virtual currency for fiat currency are possible in all jurisdictions without reliance on a commercial exchange service, and have been reported in a number of member countries. Transactions can be carried out using either fiat wire transfers (including via services such as M-Pesa, Western Union or PayPal) or cash payments to permit the buying or selling of Bitcoins. For electronic fiat transactions, a buyer must send a sum with a value equivalent to the amount of Bitcoins to be purchased. The seller then transfers the Bitcoins to the buyer's Bitcoin wallet. For cash transactions, the parties can meet physically and the buyer gives the seller the cash before the Bitcoins are transferred into their wallet. Those offering these informal exchanges often advertise on services such as Bitcoin.com. This service is available in many member countries including Nigeria, South Africa, Tonga, Jamaica, India, Ghana, Uganda and Kenya.

52. In India a new app, Zebpay.com, allows peer-to-peer transfer of Bitcoins using phone numbers in addition to allowing customers to open Bitcoin wallets. To encourage its users to transact in Bitcoins, Zebpay offers Bitcoin vouchers for purchase of products on online shopping portals.

Remittance services

53. Although in some member countries, such as South Africa, there are no commercial remittance or foreign exchange services operating using virtual currencies, it is possible for people to receive virtual currencies directly from a person in another jurisdiction and exchange them for local currency. In effect, this constitutes a form of 'manual' remittance service.

54. Most exchanges in India have limited their operations to merely buying, selling or converting existing Bitcoins into the Indian rupee. However, Unocoin offers customers the opportunity to transfer or remit Bitcoins as well, using third-party software; transactions are forwarded to individual Bitcoin users through the

57 A total of 22 machines operating; see, <http://coinatmradar.com/charts/#by-country> (last accessed 9 December 2015).
58 Reported as having been donated by the manufacturer; see, <http://coinatmradar.com/manufacturer/3/genesis-coin-Bitcoin-atm-producer/3/> (last accessed 9 December 2015).
59 A total of 88 machines operating; see, <http://coinatmradar.com/charts/#by-country> (last accessed 9 December 2015).
60 *Ibid*.
61 Two machines operating; see, <http://coinatmradar.com/charts/#by-country> (last accessed 9 December 2015).
62 One machine operating in Johannesburg transaction cost of 6 per cent; see, <http://coinatmradar.com/charts/#by-country> (last accessed 9 December 2015).
63 A total of 22 machines operating including 1 on Jersey and 1 on the Isle of Man; see, <http://coinatmradar.com/charts/#by-country> (last accessed 9 December 2015).

Blockchain. BitPesa offers remittance services in Kenya and Tanzania, and, as of July 2014, it was estimated that they have handled around 15,000 transactions. BitPesa also plans to begin offering such services in Nigeria and Uganda.[64]

55. The use of virtual currencies as a form of peer-to-peer remittance service has been documented in Uganda through a short film produced by Bitcoinfilm.org.[65]

Use by civil society

56. The ability to use virtual currencies innovatively is undoubtedly one of their most compelling features and makes them particularly attractive to users.

57. In India, virtual currencies have been used for charitable causes. The Dogecoin, for example, was used to make donations towards supporting Olympic athletes and other causes.[66] Similarly, Dogecoin was used in Jamaica to fund the Olympic bobsleigh team.

58. In Kenya, the exchange BitPesa enables non-governmental organisations (NGOs) to receive donations in the form of Bitcoins. BitPesa is working with Tunapanda Institute, a digital skills education NGO, Heshima Children's Center, a welfare home for children with disabilities, and Reaching Out with Compassion in Kibera, a scholarships and tutoring services NGO targeting at-risk youth in Kibera. The Tunapanda Institute has already received Bitcoin donations.

59. A number of third-sector charitable organisations are reported to have been soliciting donations in virtual currencies in Uganda.[67]

The prevalence of crime involving virtual currencies

60. A number of features make virtual currencies an attractive payment mechanism to criminal enterprises. These are anonymity, rapidity, cheap and irreversible transfers, and obfuscated financial transactions.[68]

61. At a global level, dark markets using virtual currencies, particularly Bitcoin, have average daily sales volumes of USD$300,000–500,000, with highs of $USD650,000.[69]

62. Some member countries have experienced numerous criminal cases involving virtual currencies, whereas others have not yet identified or handled any such cases. This does not necessarily mean that virtual currencies are not being used by criminals in those jurisdictions, but could indicate that their use has not been detected. Once again, quantitative data are difficult to obtain, but criminal use cases can be highlighted.

64 Presentation to Commonwealth Working Group on Virtual Currencies by Anna Mance, General Counsel, BitPesa, 24 August 2015.

65 See, YouTube, *Bitcoin in Uganda*, available at <https://www.youtube.com/watch?v=BrRXP1tp6Kw&feature=youtu.be> (last accessed 9 December 2015).

66 D. Gilbert, (2014), *Dogecoin Community Helps Send Indian Athletes to Winter Olympics*, International Business Times, 30 January 2014, available at <http://www.ibtimes.co.uk/dogecoin-community-helps-send-indian-athletes-winter-olympics-1434515> (last accessed 9 December 2015). Similarly, the 'Doge 4 Water' initiative contributed millions of Dogecoins towards supporting initiatives in providing accessibility to drinking water in developing countries; see, <http://doge4water.org>.

67 See, <https://safello.com/donate> and <http://setherfree.org/donate>.

68 Europol (2015), *The Internet Organised Crime Threat Assessment* (iOCTA), 30 September 2015, at 46; available at <https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf> (last accessed 9 December 2015).

69 G. Hileman, (2015), *Consensus 2015 – State of Blockchain*, 10 September 2015, available at <http://www.slideshare.net/CoinDesk/consensus-2015-state-of-blockchain-52673969> (last accessed 9 December 2015).

63. Broadly, there are two types of offence related to virtual currencies. These are where virtual currencies are (i) instrumentalities of crime, for example, they facilitate payments for illicit products or services, ransom payments or laundering the proceeds of crime; and (ii) the object of the crime, for example the acquisition of virtual currencies by theft.

Regulatory offences

64. The use of virtual currencies is not unlawful in the majority of member countries. The only exception is Bangladesh, where the Central Bank published a statement declaring them illegal and the local Bangladeshi Bitcoin Foundation had to suspend its activities. However, the Bitcoin client was downloaded more than 60 times in Bangladesh following the enactment of the ban, indicating that some virtual currency transactions are continuing.

65. Although other member countries have not adopted the same approach as Bangladesh, they have remained cautious about the legality of virtual currency. In India, as the virtual currency industry in the country is at a nascent stage – and with the absence of legal frameworks specifically engaging with virtual currencies – there is suspicion that their use is for criminal purposes. This was illustrated by the Enforcement Directorate's raid on two offices of Bitcoin exchanges in Ahmedabad, Gujarat in December 2013.[70] The raids were made on the suspicion that the websites violated the Foreign Exchange Management Act, because they were transacting and exchanging Indian currency and Bitcoins. However, the organisations affected have argued that they complied with banking and financial regulations, and even required that their customers comply with other requisites, such as a Permanent Account Number card, which is used for taxation purposes and the recording of transactions.[71] No further action on the part of the Enforcement Directorate has been reported following the raids.

Provision of illicit goods and services

66. In the course of researching this report, the Working Group observed that persons can use virtual currencies to remotely obtain goods and services which either facilitate criminal activity or which are themselves illegal (e.g. illegal drugs) and the possession of which itself constitutes a criminal act, in much the same way as in legitimate markets. Using areas of the dark web, criminals advertise illegal or illicit goods and services for sale in exchange for virtual currencies. The goods can be shipped using national postal services,[72] and services can be easily provided using communications technology.

67. It is difficult for the Working Group to estimate with any certainty the scale of this activity, but there are some indicators of its use. These are:

    – virtual currencies as a component of any criminal cases or investigations undertaken by law enforcement agencies;

70 See, <http://rbitco.in> and <http://buysellbit.co.in>. See, also, V. Dutta, (2013), *ED officials raided two Bitcoin trading firm in Ahmedabad*, Economic Times, 27 December 2013, available at <http://articles.economictimes.indiatimes.com/2013-12-27/news/45626789_1_one-Bitcoin-Bitcoin-transactions-peer-to-peer-payment-network> (last accessed 9 December 2015).

71 N.T. Balanarayan, (2014), *ED Raids Offices Of Bitcoin Websites; Its Aftermath And Our Take, Medianama*, 2 January, 2014, available at <http://www.medianama.com/2014/01/223-Bitcoin-india-raid-shuts/> (last accessed 9 December 2015).

72 US Attorney General Eric Holder, Committee On Appropriations Subcommittee On Commerce, Justice, Science, And Related Agencies, 3 April 2015.

- illegal goods and services being offered for sale in exchange for virtual currencies in adverts which make reference to their originating from a particular jurisdiction;
- illegal goods and services being sought in exchange for virtual currencies by purchasers advertising that they are seeking deliver to a particular jurisdiction; and
- reviews of the provision of illegal goods and services on committee message boards and on the dark web.

68. Although such indicators do not detail the value of the criminality being facilitated, they serve to illustrate its existence within a particular jurisdiction.

69. Perhaps the most well known criminal use of virtual currencies is in advertising the sale of illicit goods and services in conjunction with hidden online marketplaces. There have been many striking examples of global investigations into such services, in particular the Silk Road case. Despite such high-profile cases, the services continue to flourish and rely upon virtual currencies to provide the anonymity that their users seek. In many instances, it is impossible to determine the location of either the vendors or the purchasers of the items offered for sale on these markets. However, there are often clear links to member countries. For example, the adverts placed by vendors often expressly state where the product comes from and where they can be shipped to, and vendors are often reviewed by purchasers who indicate the jurisdictions to which they want the items shipped. Vendors of cannabis often refer to Jamaica as the product's origin, although such claims are impossible to verify.[73] Although not conclusive of the use of virtual currencies for criminal purposes in a particular jurisdiction, such observations can be considered highly indicative.

70. The most high-profile law enforcement response to the criminal use of virtual currencies was the recently implemented 'Operation Shrouded Horizon'. This global investigation, led by the US authorities, involved co-operation between 20 states including Australia, Canada, Cyprus, Nigeria and the United Kingdom and resulted in the arrest of 200–300 cybercriminals. Using the Tor network, the criminals had established an online forum, Darkode, for persons 'interested in buying, selling, and trading malware, botnets, stolen personally identifiable information, credit card information, hacked server credentials, and other pieces of data and software that facilitated complex cybercrimes all over the globe.'[74] However, shortly after the arrests, it was reported that the Darkode service was running once more and was now using features of the Blockchain to verify that participants were not the police.[75] This provides an interesting example of how the technology underlying virtual currencies can facilitate innovation, not only in the legitimate economy but also amongst criminals. The scale of this operation, the arrests within member countries and the critical role of virtual currencies as a facilitator of criminality demonstrate the significant impact of this technology on member countries.

73 Commonwealth Secretariat, Rule of Law Division Investigations: Utilising dark web crawler.

74 FBI, *Cyber Criminal Forum Taken Down*, 15 July 2015, available at <https://www.fbi.gov/news/stories/2015/july/cyber-criminal-forum-taken-down/cyber-criminal-forum-taken-down> (last accessed 9 December 2015).

75 D. Pauli, (2015), *Cybercrime forum Darkode returns with security*, admins intact, The Register, 28 July 2015, available at <http://www.theregister.co.uk/2015/07/28/darkode_returns> (last accessed 9 December 2015).

71. This experience has been replicated in other member countries. The Australian Crime Commission has stated that virtual currencies are being 'used by "mums and dads" to purchase illicit commodities, such as narcotics, over the internet'.[76]

72. An interesting example of the supply of drugs arose in relation to Kava. Kava is not a prohibited drug but, rather, is a natural psycho-active substance. The largest producer of Kava is Vanuatu, but it is also grown in Fiji, Samoa and Tonga. From 2002, a number of jurisdictions, including the United Kingdom, banned the sale, supply and importation of Kava-based substances.[77] However, the Working Group found posts on the Silk Road 2 forum from 2014, advertising the sale of Kava for shipping to the United Kingdom and Australia.[78] Although the location of the supplier cannot be ascertained, it is significant, from the perspective of the Commonwealth, that not only were two of the markets to which these products were actively marketed member countries, but also that much of the global supply of Kava originates from member countries.

73. These trends are not confined to the provision of goods. In Kenya, the hacking community has begun to commercialise the provision of their skills and to accept payment for these services via virtual currencies.[79]

Fraud

74. Virtual currencies exhibit many characteristics that are similar to fiat financial instruments. This includes the ability to pay for goods and services and for capital growth. This present opportunities for criminal frauds to arise, which target both investors and consumers seeking to use virtual currencies.

75. In Cyprus, a criminal investigation was reported to have been opened into the conduct of a virtual currency-based business known as Neo & Bee. This organisation purported to provide banking facilities using Bitcoin alongside euro deposits, and had gone as far as opening a high street branch in Nicosia. Within a matter of weeks of the business opening, it was alleged that persons who wanted to purchase Bitcoin via the business never received them. These events resulted in the Cypriot Police issuing an arrest warrant for Neo & Bee's founder.[80]

76. A criminal investigation was opened in Uganda which linked Bitcoins to an international counterfeiting scam on the dark web involving a US citizen called Ryan Andrew Gustafson, also known as Jack Farrel. In December 2013, Gustafson created his own dark web site called Community-X, which was dedicated to the manufacture of Ugandan-made counterfeit Federal Reserve Notes which were being advertised, bought and sold, distributed and passed through online criminal forums then passed in coffee shops and corner stores in the USA and Uganda in return for Bitcoins. In addition, the Working Group received anecdotal reports of persons who had used unofficial remittance services being 'scammed' by persons in Uganda, with the object of obtaining of the victim's Bitcoins.[81]

76 Australian Senate (2015), Digital Currency – *Game Changer or Bit Player*, Economic References Committee, Canberra, ACT, Australia, at Section 3.39.
77 The Medicines for Human Use (Kava-kava) (Prohibition) Order 2002.
78 Commonwealth Secretariat, Rule of Law Division Investigations: Utilising dark web crawler.
79 Serianu Ltd (2015), *Kenya Cyber Security Report*, Nairobi, Kenya, at 20.
80 Cyprus Mail (2014), *Cyprus police issues arrest warrant for Bitcoin entrepreneur*, 11 April 2014, available at <http://cyprus-mail.com/2014/04/11/cyprus-police-issue-arrest-warrant-for-Bitcoin-entrepreneur> (last accessed 9 December 2015).
81 Commonwealth Virtual Currencies Survey, Uganda, Investigations by local consultant.

Theft

77. In 2014 it was reported that Canadian wallet company Flexcoin had been subject to a cyber attack in which more than US$ 500,000 worth of Bitcoins had been stolen.[82]

Extortion and ransom

78. Europol has noted that Bitcoin features as the most common single payment mechanism used in extortion payments, accounting for approximately one-third of cases.[83] This includes cases of both cyber- extortion (where computer systems are held ransom) and real-world kidnapping cases.

79. One of the most high-profile extortion cases arose in October 2015 when a UK telecoms company, TalkTalk, was subject to a cyber attack, which resulted in subscriber information being stolen. The company subsequently received a ransom demand of £80,000 to be paid in Bitcoin, from a group purporting to be behind the attack.[84] At least one arrest has already been made in this case.

80. Similar ransom-type scams have also been reported in Kenya. **In January 2015, two computer experts were accused of hacking into NIC Bank's customer database demanding a ransom of 200 Bitcoins – the equivalent of KSh 6.2 million at the exchange rate at the time**. It is alleged that the hackers threatened to publish confidential customer information if their demands were not met. The two experts denied charges of theft, blackmail and attempted extortion.

81. Online criminals can themselves be targets for this type of crime. One instance observed by the Secretariat involved an online drug dealer advertising on a hidden forum called which purported to ship drugs (including cocaine, heroin, MDMA and ketamine) primarily to the United Kingdom and Australia. The drug dealer reported to other forum users that another user had threatened to expose his identity, demanding US$3,000 in Bitcoins to prevent such exposure.

82 P. Rizzo, (2014), *Bitcoin Bank Flexcoin to Close After $600k Bitcoin Theft*, CoinDesk, 4 March 2014, available at <http://www.coindesk.com/Bitcoin-bank-flexcoin-close-600000-Bitcoin-theft> (last accessed 9 December 2015).

83 Europol (2015), iOCTA Report, at 47.

84 K. Ahmed, (2015), *TalkTalk – could this be an extortion attack?*, BBC News, 23 October 2015, available at <http://www.bbc.co.uk/news/business-34613137> (last accessed 9 December 2015).

Part 2: The Impact of Virtual Currencies in Commonwealth Member Countries

Introduction

82. Part 1 of this report has reviewed the prevalence of virtual currencies within Commonwealth member countries, Part 2 will review the economic and social impacts that they have already made -and are likely to make- in the future. However, in view of the still relatively contained use of virtual currencies compared with established systems of digital value exchange, for example through the use of credit cards and payment processing services such as PayPal, it may be more appropriate to consider these impacts as potential rather than realised.

83. The evidence collected by the Working Group suggests that virtual currencies may already be having a beneficial impact in Commonwealth jurisdictions by providing services to the unbanked, enabling lower transaction costs, shortening transaction time, reducing the need for intermediaries and fostering innovation. However, they are having a harmful impact in that they are volatile and present risks to consumers. They are being used to facilitate criminal activity, to launder the proceeds of crime and, potentially, to finance terrorism, and are themselves targets for crime. It is also crucial to note that attributes of different virtual currencies are diverse, and their potential to deliver risks and benefits varies.

Beneficial impact

84. Representatives of member countries at the Commonwealth Roundtable in February 2015 expressly noted the contribution that low-cost remittance and foreign exchange services and access to new financial products can make to innovation in the online economy.

85. Virtual currencies have the potential to have a positive effect on the Commonwealth in a number of ways including those reviewed below. This review must, however, be qualified by noting that the sustainability of these benefits is not guaranteed. First, the technology itself may limit the benefits in the longer term. For example, in the case of Bitcoin, the increasing cost of mining may translate in higher processing fees, which might make it less competitive than payment services providers using fiat currency. Second, it is worth considering whether the potential benefits associated with virtual currencies are 'real' benefits or 'artificial' ones, with regard to the current lack of regulation in the market. It is still too early in the life of virtual currencies and their adoption is as yet too limited to resolve these issues; however, they remain import factors when considering the benefits of virtual currencies. Given the limited levels of adoption, it remains to be seen whether or not the impact of virtual currencies and the accrual of the possible benefits will be more than negligible.

Providing facilities for the world's unbanked

86. The World Bank estimates that 2.5 billion adults do not have accounts at banks and other mainstream financial institutions.[85] The success of telecoms-based banking services such as M-Pesa in East Africa in addressing the lack of financial services in developing countries illustrates the potential value of similar virtual currency-based technologies to enfranchise significant portions of the world's remaining unbanked citizens.[86] It is important to note, however, that M-Pesa is based on a centralised model using fiat currency as the basis of value exchange and, as such, is quite different from virtual currencies.

87. The delivery of financial services in the developing world is of particular significance in view of the recent trend by international banks in 'de-banking' non-bank remittance providers in high-risk regions, thereby preventing the exchange of remittances between persons globally. Virtual currencies potentially alleviate this by not requiring involvement from the banking sector to send or receive value transfers. Virtual currencies allow a recipient either to make direct use of the virtual currencies sent to them, conduct an informal exchange with another individual for fiat currency, or use a formal exchange to obtain fiat currency. The latter case would, however, now be subject to the same recommendations for AML/CFT measures to be effected as required by local banks following the recent FATF guidance.

Reducing transaction costs

88. Virtual currencies provide significantly reduced financial transaction costs. In the case of remittances, this can have a significant impact on member countries' economies. Many member countries receive significant sums from diaspora communities abroad. India, for example received US$71 billion in 2014 – the highest value of remittances globally. Money transfers to the Caribbean and Africa in 2014 also exceeded all other forms of external finance.[87]

89. The costs of transacting in virtual currencies are essentially fixed, regardless of the values traded. This is because the transactions do not scale upwards by size or destination.[88] The European Banking Authority has suggested that average transaction fees are 1 per cent of the transaction value. This compares favourably with an estimated cost of 8–9 per cent for fiat money transmission services.[89] In the examples outlined above, the cost of using virtual currency-based remittance services is reported as being 1 per cent of transaction costs in South Africa and 2–3 per cent in Kenya and Tanzania. As a result, annual net savings for consumers could theoretically amount to over US$43 billion based on the World Bank's estimate of global money transfers.[90]

---

85 World Bank (2014), *Global Financial Development Report* 2014, Washington, DC, USA, at 1.

86 Australian Senate (2015), *Digital Currency – Game Changer or Bit Player*, Economic References Committee, Canberra, ACT, Australia, at Section 3.11.

87 Commonwealth Secretariat (2015), *De-risking diaspora remittances*, available at <http://thecommonwealth.org/media/press-release/%E2%80%98de-risking%E2%80%99-diaspora-remittances> (last accessed 9 December 2015).

88 N. Godlove, (2014), *Regulatory Overview of Virtual Currency*, Oklahoma Journal of Law & Technology, Vol. 10, 1–67, at 13.

89 European Banking Authority (2014), *EBA Opinion on 'Virtual Currencies'*, EBA/Op/2014/08, European Banking Authority, London, paragraphs 46–7, available at <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> (last accessed 9 December 2015).

90 R. Leal, (2014), Is Bitcoin the Future of Payments?, TOP OF MIND, Goldman Sachs Global Investment Research Paper, Issue 21, 18.

90. It has been suggested that Bitcoin can facilitate a more egalitarian distribution of wealth by removing 'middle-men' and allowing for direct exchanges between producers and consumers.[91]

91. Finally, it is also necessary to recognise that benefits afforded in relation to potentially reduced transaction costs may well be tempered by other considerations, such as significant price volatility, which are not expressly factored into transaction cost.

Reducing transaction time

92. The speed of transaction processing in virtual currency presents a significant benefit to users, although it varies according to the virtual currency that is used.[92] The potential for the underlying Blockchain technology of virtual currencies to be used for rapid transaction verification has led traditional financial markets to examine the use of decentralised networks and Blockchain technology for stock transactions.[93]

Innovation

93. As already observed in the preceding discussion on the prevalence of virtual currencies by types of use, new types of business have arisen in member countries as a result of the emergence of virtual currencies. This ranges from exchange and remittance services to companies selling electronic equipment to undertake mining.[94]

94. The increase in the availability of payment-processing platforms has led to an increasing acceptance of virtual currencies in all types of trade, allowing vendors to accept non-cash transactions. The lower transaction costs in virtual currencies compared with those in fiat currencies have the potential to facilitate the development of a culture of micro-payments that, in turn, could assist the growth of small and medium-sized enterprises which previously could accept only cash payments.[95]

95. There are continuing developments in relation to constructing a link between decentralised digital ledgers and external assets, including gold and diamonds.[96] Comparisons can be drawn with bearer instruments such as promissory notes, the difference being that they would not be issued but instead held in a digital format.[97]

---

91 B. Mohit, (2015), *Bitcoin: Is it an Economic Equalizer or a Tool for Conflict and Crime?*, The Huffington Post, 17 February 2015, available at <http://www.huffingtonpost.com/dr-behzad-mohit/> (last accessed 9 December 2015).

92 European Securities and Markets Authority (ESMA) (2015), *Call for Evidence, Investment Using Virtual Currency or Distributed Ledger Technology*, ESMA/2015/532, ESMA, Paris, France, available at <http://www.esma.europa.eu/system/files/2015-532_call_for_evidence_on_virtual_currency_investment.pdf>, see paragraphs 34 and 35.

93 See, <http://uk.businessinsider.com/nasdaq-private-market-blockchain-bitcoin-experiment-currency-ledger-2015-5> (last accessed 9 December 2015).

94 See, supra footnote 94, at paragraph 38.

95 S. Fargo, (2015), *Is Bitcoin the Future of Micropayments?*, Inside Bitcoins, 10 April 2015, available at <http://insideBitcoins.com/news/is-Bitcoin-the-future-of-micropayments/31555> (last accessed 9 December 2015).

96 G. Caffyn, (2015), *Everledger Brings Blockchain Tech to Fight Against Diamond Theft*, CoinDesk, 1 August 2015, available at <http://www.coindesk.com/everledger-blockchain-tech-fight-diamond-theft/> (last accessed 9 December 2015).

97 Presentation to Commonwealth Working Group on Virtual Currencies by Adam Vaziri, UK Digital Currency Association, 24 August 2015.

International Aid

96. Virtual currencies have the potential to allow the direct contribution by people across the world to a particular cause by permitting the flow of funds to projects at a micro level. Aid agencies can reduce costs on raising, managing and transferring funds and smaller organisations can seek assistance globally and instantly. The Working Group was informed during its discussions that virtual currencies are being used by projects in South Africa to provide direct financing for power supplies for schools. One project, Usizo, has coupled Bitcoin to prepaid electricity metres, enabling funds to support these schools to be sent directly to the metres for the direct benefit of the schools. In one case, this enabled a school to receive power despite the school district being in arrears. In addition, this allows for enhanced transparency in donations and enables the direct funding of projects.[98]

Harmful impact

Volatility

97. The volatility of the value of virtual currencies is well documented, particularly the value of Bitcoin which ranged from US$0.30 in 2011 to US$1,135 in 2013.[99]

98. This presents a risk to consumers who acquire virtual currencies at one value relative to a fiat currency and later wish to sell them at the same or a higher value. It also presents a risk to merchants who accept them but fear that they will be devalued.[100]

99. The problem of volatility presents a significant barrier to the growth of virtual currency technologies, although it has been countered to an extent by payment platforms guaranteeing conversion rates.[101] It has been suggested that given the ease of trading in virtual currencies, those making them available should be aware that their products will rarely be limited to sophisticated investors. The corollary of this is that, as with any other financial product, the onus should be on the vendor to explain the risks to the consumer.[102]

100. The advent of greater numbers of exchanges and traders specialising in virtual currencies may have led to a decline in their volatility, particularly as regards Bitcoin,[103] which has stayed comparatively constant at between US$200 and US$300 throughout 2015.

98 Presentation to Commonwealth Working Group on Virtual Currencies by Lorien Gamaroff, BankyMoon, 24 August 2015.
99 United Nations Office on Drugs and Crime (UNODC) (2014), *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, UNODC, Vienna, Austria, at 8.
100 D. Descoteaux, *Bitcoin: More Than a Currency, a Potential for Innovation*, Montreal Economic Institute, Economic Note, available at <http://www.iedm.org/files/note0114_en.pdf> at 3.
101 Ibid.
102 N. Godlove, (2014), *Regulatory Overview of Virtual Currency*, Oklahoma Journal of Law & Technology, Vol. 10, 1–67 at 56.
103 Australian Senate (2015), *Digital Currency – Game Changer or Bit Player*, Economic References Committee, Canberra, ACT, Australia, at Section 3.28.

Risk to consumers

101. Virtual currencies present a number of risks to consumers.[104] Bitcoin and similar currencies, for example, provide no facility for chargebacks,[105] with the result that incorrect or disputed transactions cannot be cancelled in the same way as those conducted using fiat electronic transactions. There is a lack of clarity in many member countries' consumer protection legislation as regards its application to transactions involving virtual currencies.

102. The loss of, or loss of access to, virtual currencies is a significant problem. Loss of private keys or publication of private keys can result in consumers losing their virtual currency irretrievably.[106]

103. Currently, only one Bitcoin wallet provider appears to be offering insurance for deposits held with them. The company is based in London, United Kingdom and actively markets its services on this basis.[107]

104. Arguably, the lack of consumer confidence itself poses a risk to the future use of virtual currencies.[108]

Cyber and cyber-enabled crime

105. The use of virtual currency is not itself a criminal offence in any of the member countries surveyed by the Working Group, with the exception of Bangladesh.[109] However, as national criminal laws are usually broadly drafted and technology neutral, virtual currencies can give rise to criminal offences where they are used to facilitate criminal offences or form part of the actus reus of an offence. Similarly, the manner in which the currency is used may be prohibited by legislation.

106. In the 2014 Internet Organised Crime Threat Assessment (iOCTA), Europol observed that virtual currencies are being heavily abused by cybercriminals.[110] This trend is complementary to other trends in international crime. McAfee estimates the annual cost to the global economy of cybercrime at more than US$400 billion.[111] This is bound to increase as internet connectivity proliferates. Regions with large concentrations of member countries are driving this growth. Europol has noted that Asia, despite its low internet penetration of circa 27 per cent, provides over 1 billion internet users or 45 per cent of the world's total users, and internet access in Africa has grown by 3,600 per cent in the past decade.[112]

---

104 For the practical issues relating to software code and the law, see, S. Mason & T.S. Reiniger, (2015), *"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?*, Computer and Telecommunications Law Review, Vol. 21 No. 5, at 135–148.

105 N. Godlove, (2014), Regulatory Overview of Virtual Currency, Oklahoma Journal of Law & Technology, Vol. 10, 1–67, at 55.

106 *Ibid*, at 55–56.

107 Elliptic Vault advertises that 'Deposits are comprehensively insured by a Fortune 100 insurer and held in full reserve.' See, <https://www.elliptic.co/vault/vault/>.

108 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

109 *Ibid*, at paragraph 66.

110 Europol (2014), iOCTA Report, at 3.5.

111 Center for Strategic and International Studies (2014), *Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II*, Washington, DC, USA, available at <http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf> at 2.

112 Europol (2014), iOCTA Report, at 17.

107. It is not only the increasing scale or influence of cybercrime that constitutes a unique challenge to law enforcement, but also the arrival of a new criminal genus. Communications technology allows informal groupings to coalesce around a single task, with each participant bringing their specialist skill-set to a criminal endeavour. These groups then disband equally quickly. The effect of this has been the rise of 'crime-as-a-service', whereby cyber criminals sell their services to other criminals.[113] Crucially, this significantly diminishes the digital barriers to entry: few technical skills are now required to commit crime via electronic means.[114] The ability to make anonymised and untraceable payments using virtual currencies greatly aids this new criminal economy.

108. The result is that it is likely that virtual currencies will play a part not only in the proliferation of cyber or internet-enabled crime but also in its increasing sophistication as financial incentives increase.

109. Such use presents a risk to all internet users, both states and private individuals. It is trans-border in nature, and, as Commonwealth Law Ministers have recognised, cybercrime is a global matter and any weak link provides an opportunity for criminals.[115] Therefore, although it is useful to investigate the influence of virtual currencies on trends in offending within particular Commonwealth jurisdictions, it is also important to recognise that such trends occur within a global context. The harmful effects of virtual currencies will often be felt in multiple jurisdictions and demand collaborative approaches from law enforcement and prosecuting authorities.

110. Criminality relating to virtual currencies is of four kinds:

    - **Regulatory offences**. These are offences involving conduct that threatens the integrity of a banking or financial services system, such as operating an unlicensed money transfer organisation.

    - **Virtual currencies as the object of the offence**. A problem arises in some Commonwealth jurisdictions where virtual currencies are the object of criminality and a legal owner of virtual currency is deprived of its safe enjoyment by some means, for example, theft. The challenges facing countries attempting to apply traditional criminal law is well illustrated by the Indian Penal Code 1860 in which offences against property, such as those pertaining to theft, 'mischief' and trespass, require the property concerned to be 'corporeal' moveable property and the general criminal provisions are insufficient to protect owners' rights in virtual currencies. Depending on the facts of a particular case, other general criminal provisions of fraud, misrepresentation, criminal misappropriation and cheating may be sufficient to apply to virtual currency transactions. Similarly, other statutes that enact offences of computer misuse, such as India's Information Technology Act 2000, may provide a route to criminalisation, for example, where the actus reus required is to access a 'computer or a computer system' without lawful authorisation with the intention of extracting, copying or preventing access to information stored on such a computer or computer system.[116]

113 Ibid, at 19.
114 Ibid, at 9.
115 Meeting of Commonwealth Law Ministers and Senior Officials Communiqué, Gaborone Botswana 5-8 May (2014), at paragraph 19.
116 Information Technology Act 2000, at Section 43.

- **Virtual currencies as an instrument of offending**. Virtual currencies have become the "currency of choice for internet-enabled traditional crime on the Darknet", facilitating the trade in illegal drugs and weapons.[117] One study has put the value of the trade in illegal drugs from just one online market place at US$1.2 million.[118] Interpol has also identified the dangers of malware and other illegal data, including child abuse images, being imbedded within the Blockchain used by some virtual currencies.[119] ATMs present particular opportunities for criminals to avoid law enforcement, for example, using money mules to insulate criminal gangs from criminal transactions.[120] In response, some ATM operators have self-regulated and imposed limits on the daily values that an individual can exchange.[121]
- **Virtual currencies as the proceeds of crime**. In the 2014 iOCTA Report, Europol observed that 'virtual currencies have the potential to become an ideal instrument for money laundering'.[122] This can affect exchangers who offer services to the underground economy and legitimate exchangers who fail to properly operate KYC processes (in jurisdictions where this is a legal requirement to operate their business).[123] Europol has identified online casinos, in particular those accepting virtual currencies, as presenting significant money laundering and terrorist financing (ML/TF) risks. This is of considerable concern to member countries with online casinos operating in their jurisdiction, as unless they have adequate KYC measures in place, there is a significant risk of money laundering.[124]

Investigations

111. The obscurity of virtual currencies, relative to payment cards and other forms of online payment,[125] and their ability to enable users to avoid traditional financial institutions and the requirements to record transactions 'significantly complicate law enforcement efforts to follow the money' and identify their use in the commission of crime.[126] This is a matter of increasing concern, particularly in the context of investigations into money laundering, terrorist financing, trafficking in drugs and arms and human trafficking.

117 Europol (2014), iOCTA Report, 2014, at 42; This includes weapons of mass destruction such as the biotoxin ricin.
118 N. Christin, (2012), *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*, Carnegie Mellon University, 1–26, at 24–5.
119 INTERPOL (2015), INTERPOL *cyber research identifies malware threat to virtual currencies*, available at <http://www.interpol.int/News-and-media/News/2015/N2015-033>.
120 F. Cajani, (2009), *International phishing gangs and operation Phish & Chip*, Digital Evidence and Electronic Signature Law Review, Vol. 6, at 153–7.
121 Presentation to Commonwealth Working Group on Virtual Currencies by Dr Sarah Meiklejohn, University College London, 24 August 2015.
122 Europol (2014), iOCTA Report, at 3.5.
123 *Ibid.*
124 See, <http://www.casinocity.com/casinos/>.
125 United Nations Office on Drugs and Crime (UNODC) (2014), *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, UNODC, Vienna, Austria, at 47.
126 US Department of Justice (2013), *Testimony of Acting Assistant Attorney General Mythili Raman before US Senate Committee on Homeland Security and Governmental Affairs*, 18 November 2013, Washington, DC, USA.

Taxation

112. The risk of persons using virtual currencies that fail to comply with the requirements of taxation regimes are similar to those arising in the cash economy.[127]

Long-term relationship with the fiat economy

113. The Australian Senate Economic References Committee has suggested that given the relatively small size of virtual currency investments and transactions, specifically as regards Bitcoin, there is no immediate risk to financial stability. However, it has expressly acknowledged that its analysis is based upon the relative size of virtual currency investments compared with the overall size of a national economy and that where the use of virtual currencies is larger, there will be a greater risk;[128] this is a view shared by the Bank of England.[129] Therefore, the risk of virtual currencies creating economic destabilisation could arise when there is considerably larger market penetration,[130] or in smaller jurisdictions in which low rates of market penetration could have a proportionately greater influence on their economies. This would be of particular concern in small jurisdictions with large offshore financial sectors which appear to be proportionately larger adopters of virtual currencies.[131]

114. The long-term effect of virtual currencies on fiat currencies and the fiat economy is an area in which more information would be helpful. It has been suggested that it is unlikely that Bitcoin in particular has a long-term future, but that it may provide a basis for future virtual currencies which will have a longer lasting economic impact.[132]

115. The Bank of England has expressed the view that the most extreme risk to the fiat economy could come from 'Bitcoinisation' of an economy, that is, where everybody within a state sought to conduct all of their transactions entirely with virtual currencies and used fiat currency only when obliged to by law, for example when paying taxes. This would curtail the ability of central banks to influence price setting and real activity would be severely impaired. The Bank of England concluded that such a scenario is extremely unlikely given the obstacles to widespread adoption of virtual currencies and in the absence of a collapse in fiat currency.[133]

Responses

Introduction

116. Decentralised virtual currencies, such as Bitcoin, present unique challenges for member countries seeking to subject the commercial undertakings using them to the same requirements as those using fiat currencies. As a result, there is often no clear regulatory or legislative response.

---

127 Australian Senate (2015), *Digital Currency – Game Changer or Bit Player*, Economic References Committee, Canberra, ACT, Australia, at Section 3.20.
128 Australian Senate (2015), *Digital Currency – Game Changer or Bit Player*, Economic References Committee, Canberra, ACT, Australia, at Section 3.23.
129 Bank of England, Quarterly Bulletin 2014 Q3, at 283.
130 *Ibid.*
131 See, Table 1.1 and Table 1.2 above.
132 G. Gibbs, (2014), Virtual Currency: Fad or Future?, Monetary Thought and Policy, The Student Economic Review, Vol. 28, 64–72, at 69.
133 Bank of England, Quarterly Bulletin 2014 Q3, The Economics of Digital Currencies, at 283.

117. Although there appears to be some degree of convergence on how they should be treated for the purposes of taxation, ambiguities remain on the application of criminal law and AML/CFT issues. Publication of the FATF Guidance in June 2015 may go some way to resolving these issues so that member countries more consistently apply a risk-based approach (RBA) to the ML/TF risks associated with virtual currencies, particularly the requirements for providers of payment products and services to institute KYC systems.

118. Some financial regulators in the Commonwealth have noted the absence of a legal or regulatory framework as 'substantially [exacerbating] risk' and deterring the growth of virtual currencies.[134] The United Nations Economic Commission for Latin America and the Caribbean (ECLAC) has undertaken important studies on the regional impacts of virtual currencies. In 2014, a representative of TriniTrolley, a Trinidadian e-commerce business, reported to ECLAC that their company faced significant difficulties in enabling the acceptance of digital payments: 'These included lack of e-commerce supporting legislation, lack of consumer education and trust on the system, lack of technical capability, and difficulty working with local banks'.

119. In India, it has been claimed that a lack of regulatory clarity has hampered uptake, and most businesses engaged in Bitcoin trade have recently moved towards suspending operations until the Reserve Bank clarifies the position.

120. Public statements on the legality of the use of virtual currencies should also assist in warning users of the risks involved. In December 2013, the Central Bank of Trinidad and Tobago issued a warning on Bitcoin and virtual currency:

    'Potential users of this product must be aware of the risks involved in investing in virtual currencies as regulators seek to establish appropriate frameworks to ensure the continued safe operation of the payments system and the smooth conduct of monetary policy'.

    The warning specifically advised of their volatility and against their illicit use.

    In February 2014 the Central Bank of Cyprus, stated that:

    'The public needs to be aware of the fact that there are no specific regulatory protection measures to cover losses from the use of virtual currencies if a platform that exchanges or holds them collapses and, thus, there is the risk of losing their money.'

    In September 2013, the Monetary Authority of Singapore issued a public statement on virtual currencies which informed consumers of the risks attendant with the use of virtual currencies:

    'Consumers should be cautious when dealing with [virtual currencies] given the risks highlighted above. MAS' [Monetary Authority of Singapore] targeted regulatory approach is to specifically address the money laundering and terrorist financing risks posed by [virtual currencies]. Consumers and businesses should take note of the broader risks that dealing in [virtual currencies] entails and should exercise the necessary caution.'[135]

134 South African Reserve Bank, *Position Paper on Virtual Currencies*, (2014), at 6.

135 See, <http://www.mas.gov.sg/moneysense/understanding-financial-products/investments/consumer-alerts/virtual-currencies.aspx> (last accessed 9 December 2015).

The FATF Guidance on a risk-based approach to virtual currencies

121. In June 2015, FATF published its guidance for a RBA to virtual currencies to help nations develop legislative and regulatory responses to the ML/TF risks of virtual currency payments, products and services and to assist the private sector to comply effectively with its requirements. The guidance is focused on 'identifying and mitigating risks associated with convertible virtual currencies, applying licensing registration requirements, implementing effective supervision, providing a range of effective and dissuasive sanctions and facilitating national and international cooperation',[136] and is directed at the points of intersection that provide gateways to the regulated financial system, in particular virtual currency exchanges.

122. It is beyond the scope of this report to consider the FATF Guidance in detail, or how it could form a component of a comprehensive legislative and regulatory response to virtual currencies. This will be necessary at the second stage when the Working Group undertakes the second part of its mandate, namely producing technical guidance for Commonwealth member countries. However, the FATF Guidance outlines how key FATF recommendations should be applied to take virtual currencies into account:

    - R1: apply RBA to ensure that measures to prevent and mitigate are commensurate with the risks identified;
    - R2: ensure national co-operation and co-ordination with respect to AML/CFT policies including in the virtual currencies sector;
    - R14: register or license providers of money value transfer services and ensure their compliance with relevant AML/CFT measures;
    - R15: identify and assess AML/CFT risks relating to the development of new products and new business practices;
    - R16: ensure that when convertible virtual currency transfers are wire transfers, they include required originator and beneficiary information specified in the recommendation and monitor such transfers;
    - R26: ensure that convertible virtual currency exchangers which act as nodes where convertible virtual currency activities intersect with the regulated fiat currency financial system are subject to adequate regulation and supervision;
    - R35: have a range of effective, proportionate sanctions available to deal with persons that fail to comply with the applicable requirements; and
    - R40: provide efficient and international co-operation to help countries combat money laundering, associated predicate offences and terrorism financing including mutual assistance.

123. The desire of FATF to seek to subject these intersections or intermediaries, to ML/TF regulations received broad support from those representatives of the virtual currency industry consulted by the Working Group.[137]

136 FATF/OECD (2015), Guidance for a Risk-Based Approach: Virtual Currencies, FATF, Paris, France, at paragraph 21.

137 Presentations to Commonwealth Working Group on Virtual Currencies by Adam Vaziri, UK Digital Currency Association and Gabriel Abed, BITT, 24 August 2015.

124. The FATF Recommendations require all FATF global network jurisdictions to impose specified AML/CFT requirements on financial institutions and designated non-financial businesses and professions and to ensure their compliance with those obligations (paragraph 16) and defines a 'financial institution' as:

    'any natural or legal person who conducts as a business one or more of several specified activities for or on behalf of a customer and include persons that conduct as a business: money or value transfer services (MVTS); acceptance of deposits and other repayable funds from the public; issuing and managing means of payment; and trading in foreign exchange, or transferable securities. Depending on their particular activities, decentralised virtual VC exchangers, wallet providers, and payments processors/senders, as well as other possible VC business models, may fall within one or more of these categories'. (paragraph 17)[138]

    Persons, offering services, such as exchanges, or potentially even mining facilities,[139] should be regarded as falling within the existing AML/CFT frameworks and treated as such.

125. Some fiat financial institutions in the Commonwealth have already adopted this approach. Some banks have withdrawn banking services for such businesses ('de-banking') because of the AML/CFT risk and the associated cost and complexities of compliance with AML/CFT regulations. This has led to the closure of some virtual currency exchanges and services within New Zealand.[140]

126. Currently, it is not clear that either Commonwealth member countries or persons taking part in any of the virtual currency-related activities outlined above are sufficiently aware of existing standards. Commonwealth member countries should therefore seek to understand the implications of the FATF Guidance in assessing their responsibilities in managing ML/TF risk.

ML/TF: lacunae in regulatory responses

127. The FATF Guidance acknowledges that its focus on the gateways to the regulated financial system excludes 'issues related to transfers within decentralised convertible VC networks, such as person-to-person transfers. Although it accepts that they are not addressed by the Guidance, it states that they may be considered in the longer term.' [141]

128. By their very nature, these are the types of transactions most at risk from criminal or terrorist exploitation owing to their lack of interaction with the fiat financial sector. However, the limited use of virtual currencies in the wider financial sector presents challenges to using them for large-scale money laundering or terrorism financing.

138 FATF/OECD (2015), *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF, Paris, France, at paragraph 6.

139 In particular where this is offered on the open market in return for fiat currency, as distinct from where it is undertaken by individuals or groups in return only for virtual currencies.

140 J. Southurst, (2014), *New Zealand Bitcoin ATM Operator Shuts Down After Bank Refusals*, CoinDesk, 30 July 2014, available at <http://www.coindesk.com/new-zealand-Bitcoin-atm-operator-shuts-down-bank-refusals/> (last accessed 9 December 2015).

141 FATF/OECD (2015), *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF, Paris, France, at paragraph 3.

129. Although with a virtual currency such as Bitcoin, a record of each and every transaction is publicly available on the Blockchain, there are significant challenges of wallet address attribution to individuals, particularly where mixing services are used. All of these transactions, taking place in the context of the anonymity provided by virtual currencies, can assist criminals in 'disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.'[142]

130. The types of financial transaction, not specifically addressed by the FATF Guidance, include:

    - mining;[143]
    - peer-to-peer transfers and transactions taking place either online and involving the same or other virtual currencies or fiat currency, or offline where cash can be exchanged for virtual currency; and
    - exchanges for other virtual currencies.

    The recommendations do not seek to address non-financial transactions, but rather seek only to recommend obligations to be implemented on financial institutions and services.

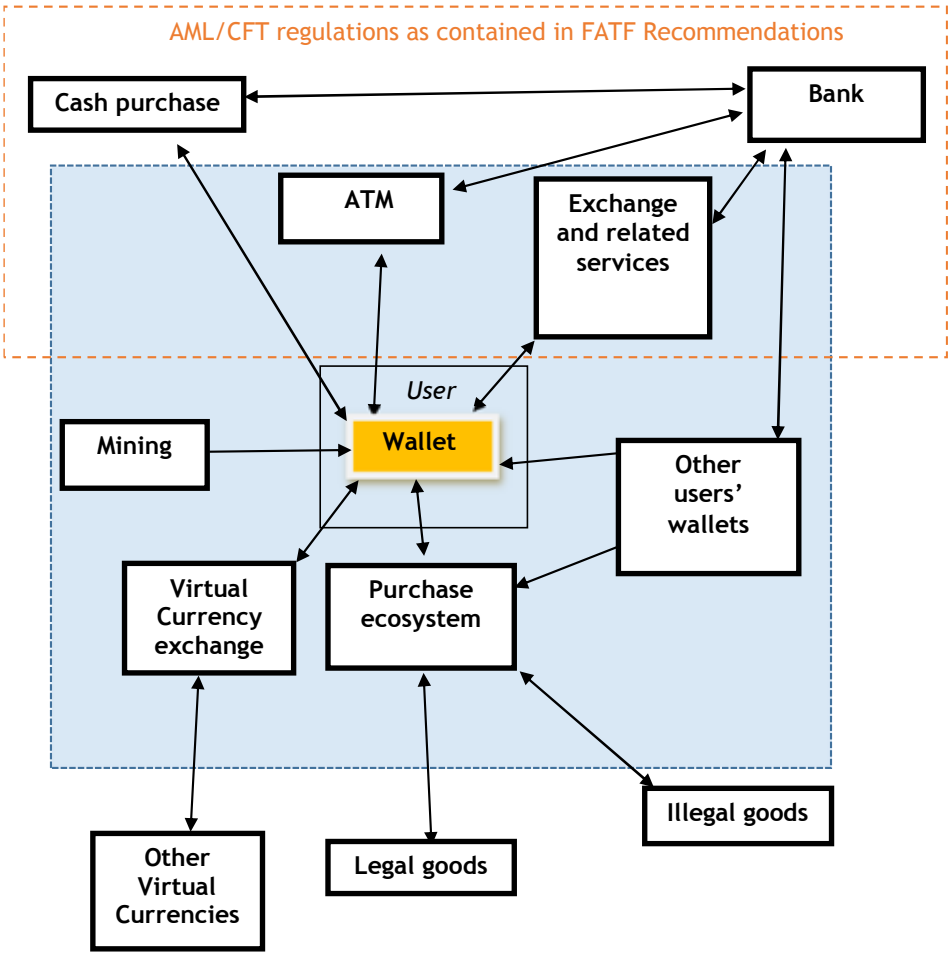
131. It is important to note that, whereas the AML/CFT compliant measures can be applied to virtual currencies, which have been acquired initially via exchanges in return for fiat currency, they do not necessarily apply to subsequent virtual currency transactions. Thus, virtual currencies, which have been acquired legitimately and in conformity with AML/CFT provisions, can subsequently be used for criminal activities. There is, therefore, a significant lacuna in the applicability of existing AML/CFT structures to the use of virtual currencies, as a result of to their being able to be used without relying upon intersection with the fiat financial sector. This necessitates innovative approaches to regulation.

132. As can be seen from Figure 1.1, there are numerous forms of transaction, which will not be covered by the FATF recommendations or by existing ML/FT mechanisms.

142 FATF, What is Money Laundering, available at <http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223> (last accessed 9 December 2015).

143 In the sense of mining for virtual currency itself, as opposed to mining as a service in exchange for fiat currencies.

Figure 1.1. AML/CFT regulations applied to a virtual currency network



VC, virtual currency.

Notes: The figure presents, at a very high level, some types of transactions which can take place on the Blockchain (those contained within the blue box). Overlaid on this is an illustration of those transactions that will be covered by the AML/CFT regulations which conform to the FATF Recommendations (those contained within the orange box).

The US and European responses

USA

133. The USA has two systems of AML/CFT regulation of virtual currencies: the federal and the state system. All 50 states regulate their separate anti-money laundering systems, and, of these, 47 states have licensing requirements relating to money transmission.[144] Money transmission is defined broadly as the transfer of funds. It is not limited to fiat currency, with the result that those providing payment products and services using virtual currencies are caught by the regulations.[145]

144 The exceptions being Arizona, South Carolina and Montana.

145 Presentation to Commonwealth Working Group on Virtual Currencies by Joe Mignano, Trial Attorney with the Asset Forfeiture and Money Laundering Section, US Department of Justice, 24 August 2015.

134. The most high-profile example of state-level regulation is New York State's BitLicense. It applies to all digital-currency businesses that are deemed 'money transmitters' (companies that hold customer funds, most of them exchanges) trading in New York State. Applicants for a license are required to have, among other things, anti-money laundering/KYC consumer protection and cybersecurity programs.

135. The Working Group was informed that the onerous burdens imposed by the BitLicense system, which go beyond federal requirements, particularly in relation to risk-assessment processes, double reporting requirements and record maintenance, have precipitated capital flight from New York State and have imperilled innovation.[146] In addition, high compliance costs have been cited as a disincentive to the establishment of virtual currency businesses within the state.[147]

136. Despite dissatisfaction with the New York State regime, the Working Group was informed that industry representatives were seeking to obtain accreditation. An important motivator for this move is apparently to provide an industry standard, which can be used to demonstrate to regulators in jurisdictions which are yet to establish such frameworks that the entity is a good corporate citizen.[148]

137. At a federal level, the PATRIOT Act, Banking Secrecy Act and other legislation on Money Service Businesses and transmitters apply to virtual currency trading entities who must register with FinCen, the US anti-money laundering regulator. The legislation requires them to establish policies, procedures and internal controls reasonably designed to assure ongoing compliance; to designate an individual responsible for assuring day to day compliance with the program and Bank Secrecy Act requirements; to provide training for appropriate personnel including training in the detection of suspicious transactions; to provide for independent review to monitor and maintain an adequate program; and the mandatory reporting of suspicious activity.[149]

The European Union

138. The European Commission (EC) emphasises that, although in the euro area only the euro has the status of legal tender, 'contractual parties are free to agree to use in transactions other official foreign currencies with legal tender status in the state of issuance, e.g. the Pound Sterling or the US Dollar. The same applies to privately issued money like local exchange trading systems (e.g. voucher-based payment systems in certain communities) or virtual currency schemes (e.g. Bitcoin). . .these forms of private money can be considered as economic assets. Private money transactions and business related to them are subject to the general rules of commodity trade such as taxation law, business law, anti-money laundering law or others.'[150]

146 Presentation to Commonwealth Working Group on Virtual Currencies by Adam Vaziri, UK Digital Currency Association, 24 August 2015.

147 D. Roberts, (2015), *Behind the "exodus" of bitcoin startups from New York*, Fortune.com, 14 August 2015, available at <http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense> (last accessed 9 December 2015).

148 Presentation to Commonwealth Working Group on Virtual Currencies by Gabriel Abed, BITT, 24 August 2015.

149 Merkle Tree (2015), *Compliance with Bank Secrecy Act – MSB – US*, available at <http://merkletree.io/blog/2015/05/obligations-to-comply-with-bank-secrecy-act-regardless-of-registration-as-msb-us/> (last accessed 9 December 2015).

150 European Commission, *Euro legal tender,* available at <http://ec.europa.eu/economy_finance/euro/cash/legal_tender/index_en.htm> (last accessed 9 December 2015).

139. The European Banking Authority recommended that the EC should include virtual currencies within Europe's fourth Anti-Money Laundering Directive.[151] The final text of the directive did not include any provisions on virtual currencies.

Commonwealth member countries

140. Some of the member countries reviewed by the Working Group have no legal or regulatory frameworks dealing specifically with them. Others have made progress on establishing clear legal standards.

141. Despite the absence of a legal or regulatory framework in their particular jurisdiction, and prior to publication of the FATF Guidance, some persons offering services using virtual currencies have sought to comply with financial reporting and ML/TF surveillance requirements.[152] Such approaches illustrate a demand by responsible exchanges and merchants for regulatory certainty and recognition that regulation is not necessarily regarded as a barrier to enterprise.

142. In the course of discussions among the Working Group, industry representatives proposed that a system of mutual recognition of licensing for those engaged in offering payment products and services using virtual currencies would represent a major boon to the industry.[153]

143. The diversity of Commonwealth responses to virtual currencies is illustrated by the examples listed below:

- **Bangladesh**: The use of virtual currencies is not lawful in Bangladesh under the current regulatory framework. In 2014, the Bangladesh Bank (the Central Bank for Bangladesh) released a statement on virtual currencies specifically referring to Bitcoins. The Bank stated:

  'As a matter of fact, Bitcoin is not a legal currency (legal tender) issued by any country. Bangladesh Bank or any organization of Bangladesh government does not approve any transaction of Bitcoin or any other artificial online currency. Bitcoin and its transactions operate mainly through online network and it does not depend/approved by a central payment system, as such, people can be financially harmed. Transactions of these kind of currency could involve unapproved matters stated in Foreign Currency Control Act, 1947 and will be punishable by it. Moreover, users of this kind of currency will also be punishable by Money Laundering Control Act, 2012 for disobeying the stated Act. So all people, from all walks of life are hereby requested not to transact/help transactions and spread information about it to avoid financial or legal risk.'

- **Canada**: Canada has amended its AML/CFT legislation to classify undertakings offering payment products and services using virtual currencies, as money services businesses. FATF notes that 'In developing its VC AML/CFT policy, Canada is taking a RBA, including understanding the risks associated with VC in the context of the ML/TF risks faced by Canada, as part of Canada's ML/TF National Risk Assessment. The regulations

151 European Banking Authority (2014), EBA Opinion on '*virtual currencies*', EBA/Op/2014/08, European Banking Authority, London, at paragraph 6.

152 For example, the decision by BitX to seek registration with the South African Financial Intelligence Centre and active compliance with the Financial Intelligence Centre Act 38/2001.

153 Presentation to Commonwealth Working Group on Virtual Currencies by Adam Vaziri, UK Digital Currency Association, 24 August 2015.

will balance the needs of mitigating the ML/TF risk with those of fostering continued financial innovation. Therefore, Canada is proposing a targeted regulatory intervention into areas with the greatest ML/TF vulnerabilities.'[154]

– **India**: In 2013, The Reserve Bank of India issued a statement cautioning investors and customers against the potential misuse of virtual currencies.[155] It observed that, currently, virtual currencies in India are neither regulated, nor do they require authorisation in any form.

  Intermediary Guidelines[156] made under the Indian Information Technology Act 2000 require intermediaries to carry out due diligence to ensure that information sharing does not 'encourage' money laundering, is not in the nature of threatening public order, or does not threaten the 'unity, integrity, defence, security or sovereignty of India'. The Act defines an 'intermediary' to include all service providers or third parties involved in the transmission of data or information.[157] As such, virtual currency exchanges and service providers involved in providing third-party services to virtual currency holders will have to comply with the guidelines.

  These provisions include the implementation of the Prevention of Money Laundering Act 2002, which criminalises the laundering of proceeds of crimes and places obligations on banking and other financial institutions to implement KYC norms including verification of customer and client identities and maintenance of relevant records. 'Proceeds of Crimes' is defined to include property that is acquired through the commission of crimes specified by the Act[158] and 'property' is defined to include 'incorporeal' assets. Therefore, covering a wider ambit of such assets, it is possible that virtual currencies, when used in transactions involving drug trafficking or financing terrorism, will be covered by Indian law.

  Furthermore, financial institutions are under an obligation to furnish 'Suspicious Transaction Reports' where they have reason to believe that a particular transaction, whether in cash or otherwise, was made without a genuine economic reason, or where there is a suspicion that it might have been proceeds of a crime. Therefore, certain transactions, especially those involving conversion of virtual currencies into fiat currencies through third-party exchanges, would necessarily require transactions to occur through banking or financial institutions, and as such would come within the ambit of the Act.

  India's primary anti-terror legislation, the Unlawful Activities (Prevention) Act 1967, criminalises the raising of funds for terrorist organisations in India and in other countries for terrorist activity in India.[159] In a provision similar

154 FATF/OECD (2015), *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF, Paris, France, paragraph 15.

155 Reserve Bank of India (2013), *RBI cautions users of Virtual Currencies against Risks*, 24 December 2013, available at <https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=30247> (last accessed 9 December 2015).

156 Information Technology (Intermediaries Guidelines) Rules (2011).

157 Information Technology Act, 2000, Section 2(1)(w): 'Intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes'.

158 Prevention of Money Laundering Act, 2002, Section 2(u).

159 Unlawful Activities Prevention Act, 1967, Section 17.

to that in the Prevention of Money Laundering Act, the Act also proscribes the possession or acquisition of proceeds of terrorism,160 including incorporeal property. The Act empowers law enforcement authorities to seek information from individuals, organisations and corporations during the course of investigation of a crime under the Act and requires public and private individuals to furnish any information an investigating officer may deem 'useful or relevant for the purposes' of the Act.[161] If, during a prosecution, it is proved that certain substances or weapons were found in the possession of the accused and there is sufficient reason to believe they were used for the commission of a crime under the Act; the court is empowered to presume the guilt of the accused, unless there is evidence to prove otherwise.[162]

- **Isle of Man**: In 2015, the Isle of Man Government amended its Proceeds of Crime Act 2008 to include 'the business of issuing, transmitting, transferring, providing safe custody or storage of, administering, managing, lending, buying, selling, exchanging or otherwise trading or intermediating convertible virtual currencies'.[163] In practical terms, this will require the adoption of KYC practices, the collection of identifying information and the reporting of specific transactions to the Island's Financial Services Commission.

  The Isle of Man Government's Department of Economic Development is considering the creation of a register of virtual currency-based businesses.[164]

- **Jamaica**: There has been no specific legislative or regulatory response to virtual currencies in Jamaica. Although there are regulations in relation to e-money (Guidelines for Electronic Retail Payment Services issued by the Bank of Jamaica), they relate solely to 'stored monetary value' which is fundamentally different from virtual currencies.[165]

- **Kenya**: The Central Bank of Kenya is the sole institution in Kenya with full discretion and sole rights to issue currency notes and coins in Kenya (Section 4(1)(f) of the Central Bank of Kenya Act). Section 22(1) of the Central Bank of Kenya Act provides that only notes and coins issued by the Central Bank shall be considered legal tender within Kenya. Given that the Bank does not issue virtual currencies, they are not considered legal tender. Despite the establishment of several high-profile virtual currency-focused commercial services in Kenya and enquiries the Central Bank has received relating to them, the Central Bank reported in February 2014 that it had received no applications for approval to transact in virtual currencies.[166] Currently, Kenya issues licenses and regulates both traditional money transmitters and issuers and processors of 'e-money' such as M-Pesa. Neither of these regimes directly applies to those virtual currencies,

160 Unlawful Activities Prevention Act, 1967, Section 21.
161 Unlawful Activities Prevention Act, 1967, Section 43F.
162 Unlawful Activities Prevention Act, 1967 Section 43E.
163 Proceeds of Crime (Business in the regulated sector) Order 2015.
164 CCN.LA (2015), CCN.LA, *Isle of Man to create cryptocurrency business register*, available at <https://www.cryptocoinsnews.com/isle-man-create-cryptocurrency-businesses-register/> (last accessed 9 December 2015).
165 Bank of Jamaica (2013), Guidelines for Electronic Retail Payment Services, Kingston, Jamaica, at 5.
166 See, <http://mobile.nation.co.ke/lifestyle/From-Bangla-Pesa-to-Bitcoin-alternative-money-goes-global/-/1950774/2201270/-/format/xhtml/-/yw4s2x/-/index.html> (last accessed 9 December 2015).

like Bitcoin, that are not issued by a sovereign government. Industry representatives reported to the Working Group that they expect guidance to be issued in coming months but have no prior knowledge of its content.[167]

- **Malta**: Malta does not have any regulations specifically pertaining to virtual currencies, nor does there appear to be any official government statement relating to them. According to news reports, virtual currencies, specifically Bitcoins, are not deemed to be a regulated instrument under the European Union (EU)'s Markets in Financial Instruments Directive 2004/39/EC. As a result, there are no licensing requirements for companies dealing in virtual currencies to obtain a license from the Malta Financial Services Authority.
- **Nigeria**: In September 2015, the Central Bank of Nigeria through Mr Joseph Nnanna, Deputy Governor for Financial System Stability, announced plans to formulate regulations for virtual currencies. The regulations will be developed through a multi-stakeholder consultative process.[168]
- **New Zealand**: The use of virtual currencies is lawful in New Zealand. However, The Reserve Bank of New Zealand has issued the following statement on virtual currencies:

  'The Reserve Bank of New Zealand Act prohibits the issuance of bank notes and coins by any party other than the Reserve Bank. However, the Reserve Bank has no direct power over any form of alternative payments medium.

  Non-banks do not need our approval for schemes that involve the storage and/or transfer of value (such as 'Bitcoin') – so long as they do not involve the issuance of physical circulating currency (notes and coins).'
- **Singapore**: The Monetary Authority of Singapore has announced that it will subject virtual currency intermediaries operating in Singapore to AML/CFT requirements including requiring verification of customer identities and the reporting of suspicious transactions. The regulations are applicable only within the territory of Singapore. However, given the global availability of virtual currency-related services, Singapore will continue to monitor the development of virtual currencies and the regulatory approaches of other jurisdictions.
- **Trinidad and Tobago**: According to the Payments Quarterly Newsletter issued by the Central Bank of Trinidad and Tobago, the concept of virtual currency is addressed under the framework established for electronic money by the Financial Institutions Act 2008. The Financial Institutions Act treats the issuance of virtual currency as stored value issued on receipt of funds and accepted as payment by persons other than the issuer. It is within the definition of 'business of a financial nature' and requires the approval of the Central Bank. The Central Bank has stated that those making virtual currencies available should get operational approval from the Central Bank under existing electronic payment laws.
- **Uganda**: Section 17(1) of the Foreign Exchange (Forex Bureaux and Money Remitters) Regulations 2006 criminalises unlicensed businesses, but there is no interpretive guidance from the Bank of Uganda requiring virtual currency

167 Presentation to Commonwealth Working Group on Virtual Currencies by Anna Mance, General Counsel, BitPesa, 24 August 2015.

168 U. Kelven, (2015), Central Bank of Nigeria ponders regulation of virtual currencies, Tech Loy, 2 September 2015, available at <http://techloy.com/2015/09/02/central-bank-of-nigeria-ponders-regulation-of-virtual-currencies/> (last accessed 9 December 2015).

exchanges to apply for licences as money remittance businesses or foreign exchange bureaus under the Foreign Exchange Act (Sections 5 and 9). Similarly, the Capital Markets Authority, the regulatory body governing securities exchanges, provides no interpretive guidance on requiring merchants or exchanges to register as securities central depository agents, or to apply for a licence to operate a securities central depository (stock exchange) under the Security Deposition Act 2009 (Section 11) and the Securities Central Depositories Regulations 2009. However, the Bank of Uganda's Economic Research Department has indicated that it is exploring the issue of appropriate regulation of virtual currencies.

- **United Kingdom**: The United Kingdom undertook a consultation on virtual currencies and regulation in 2014, and a summary of the submissions it received was published in March 2015. The United Kingdom has stated that it intends to apply AML/CFT measures to virtual currency exchanges in the United Kingdom. A formal consultation on the proposed regulatory approach is to be undertaken. Her Majesty's (HM) Revenue and Customs, in its supervisory capacity under the Money Laundering Regulations 2007, does not currently officially accept registration from digital currency intermediaries where an exchange service is provided exclusively between fiat and digital currency. However, HM Treasury has recently proposed that Money Laundering Regulations 2007 should be applied to digital currency intermediaries.[169]

  The Proceeds of Crime Act 2012 (POCA) applies to virtual currencies. Section 340 of POCA, defines 'criminal property' as 'a person's benefit from criminal conduct or the representation of such a benefit'. This includes intangible and incorporeal property. As a result, any benefits from criminal conduct, which accrue in the form of virtual currencies, would fall under the proceeds of crime regime.

Investigation of criminal offences

144. The primary obstacle for law enforcement in investigating criminal offences involving virtual currencies is its anonymity.

145. However, where participants transact in Bitcoins using pseudonyms rather than persistent real identities,[170] it is possible to cluster pseudonyms according to heuristics[171] about shared ownership to identify (i.e. associate with a real-world entity or user) a significant and active slice of the Bitcoin economy.

146. The process involves the following steps:

    - input clustering – heuristic whereby the same user has control over multiple pseudonym accounts (or addresses);
    - change and clustering – heuristic whereby the same user also controls this address and therefore sends themselves the Bitcoin;
    - engaging in transactions with others and carrying out data collection in Bitcoin;
    - scrapping published tags – these can be found in Bitcoin forums;

169 See, <http://merkletree.io/nation/GB.php>.
170 Presentation to Commonwealth Working Group on Virtual Currencies by Dr Sarah Meiklejohn, University College London, 24 August 2015.
171 An algorithm that analyses the characteristics of entries on the decentralised ledger to find clusters of transactions and patterns of behaviour which can be used to identify individuals.

- peeling chains – for example, if user A has 100 Bitcoins and user B wants 1 Bitcoin, then A's 100 Bitcoins will be withdrawn and 1 Bitcoin will be peeled off, and the remaining 99 Bitcoins will be sent back to A. Through this exchange process it may be possible to identify who A and/or B really are.

147. This process allows investigators to build up the clusters and gain a perspective of the activity in the Bitcoin market. As Bitcoin has a transparent ledger they can also observe thefts in progress.

148. However, where criminals employ intermediaries or 'money mules' to insulate themselves from transactions, law enforcement can respond only by conducting physical surveillance operations.[172]

149. The seizure of virtual currencies by law enforcement during a criminal investigation is dependent on the acquisition of the wallet that stores the virtual currency and of the private key (in the case of Bitcoin). In the USA, prosecutors who seize virtual currencies can 'cash out' once they have seized them or can get the exchange to send the funds to a Federal Bureau of Investigation wallet, from which they are then moved to a thumb drive and stored.[173] Seizure may become easier if banks and financial institutions begin to issue their own virtual currencies, in which case rapid 'freezing' of funds may be possible at a pace far in excess of the freezing provisions available in current fiat systems.[174]

150. Industry groups, in their representations to the Working Group, broadly supported the advent of these investigative techniques. They recognised the need for regulated institutions to be able to understand the origins of funds – particularly for them to be assured that the bearers have good title to the assets they purport to own. However, they cautioned that it was not practical to expect compliance technology to solve all of these issues.[175]

151. UNODC has outlined a number of investigatory challenges for law enforcement and other authorities, which arise uniquely within the context of cases involving virtual currencies. These are:

- the limited awareness of investigators and prosecutors of the existence and capabilities of virtual currencies, as well as the tools and techniques to perform investigations involving virtual currencies effectively;
- the fact that evidence is invariably electronic, thus presenting difficulties in demonstrating traceability, requiring specialist knowledge and experience to understand, vulnerability to loss, damage or alteration and issues associated with unlimited copying of evidence;[176]
- the lack of regulation and directly applicable laws; and
- difficulties arising from the need for national and international co-operation in trans-jurisdictional cases.[177]

172 Presentation to Commonwealth Working Group on Virtual Currencies by Prof. Alan Woodford, University of Surrey, 24 August 2015.
173 Presentation to Commonwealth Working Group on Virtual Currencies by Joe Mignano, Trial Attorney with the Asset Forfeiture and Money Laundering Section, US Department of Justice, 24 August 2015.
174 Presentation to Commonwealth Working Group on Virtual Currencies by Adam Vaziri, UK Digital Currency Association, 24 August 2015.
175 *Ibid.*
176 For which, see, S. Mason (Ed.) (2012), Electronic Evidence, 3rd edn, Butterworths Law.
177 United Nations Office on Drugs and Crime (UNODC) (2014), Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, UNODC, Vienna, Austria, at 60–7.

152. Former Assistant US Attorney General Raman has stated that these challenges are having a highly disruptive effect upon the ability of law enforcement to deploy traditional investigative techniques to respond to criminality.[178] As such, there is a real risk that virtual currencies can frustrate the ability of law enforcement to halt offending and achieve successful prosecutions.

Taxation

153. There appears to be an emerging consensus among member countries for tax purposes, in particular that:

    a. virtual currencies are not currencies;

    b. virtual currencies are assets; and

    c. sales taxes should not be applied to virtual currencies themselves but to goods and services purchased using them.

- **Australia**: The Australian Taxation Office (ATO) has determined that virtual currencies are akin to barter transactions179 for the purposes of tax. However, the Australian Senate Economics References Committee has observed that this 'creates a double taxation effect that has placed an additional burden on Australian digital currency businesses'.[180] It therefore advised the ATO to amend any necessary legislation to avoid this and the potential deterrent effect on the development of the virtual currency sector in Australia.
- **Canada**: The Canada Revenue Agency views virtual currencies as a commodity. Transactions using virtual currency to buy goods and services are treated like barter transactions and sales tax will apply. Where virtual currency is bought and sold as a commodity, it is treated in the same way as buying and selling any other commodity; the gain is taxable as an income transaction. If it is an investment, only half of the gains are taxable as a capital transaction.[181]
- **United Kingdom**: In January 2014, HM Revenue and Customs, the UK Tax authority, stated that:

    i. income received from Bitcoin mining activities will generally be outside the scope of value added tax (VAT);

    ii. income received by miners for other activities, such as for the provision of services in connection with the verification of specific transactions for which specific charges are made, will be exempt from VAT;

    iii. when virtual currencies are exchanged for pounds sterling or for foreign currencies (and presumably other virtual currencies) no VAT will be due on the value of the virtual currencies themselves;

178 US Department of Justice (2013), *Testimony of Acting Assistant Attorney General Mythili Raman before US Senate Committee on Homeland Security and Governmental Affairs*, 18 November 2013, Washington, DC, USA.

179 Australian Tax Office (2014), *Tax treatment of crypto-currencies in Australia – specifically bitcoin*, available at <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/> (last accessed 9 December 2015).

180 Australian Senate (2015), *Digital currency – game changer or bit player*, Economic References Committee, Canberra, ACT, Australia, at Section 4.34.

181 Borden Ladner Gervais (2014), *The regulation of virtual currencies in Canada*, 10 September 2014, available at <http://www.blg.com/en/newsandpublications/publication_3835> (last accessed 9 December 2015).

iv. charges (in whatever form) made over and above the value of the Bitcoin for arranging or carrying out any transactions in Bitcoin will be exempt from VAT.

However, VAT will be due in the normal way from suppliers of any goods or services sold in exchange for Bitcoin or other similar cryptocurrency. The value of the supply of goods or services on which VAT is due will be the sterling value of the cryptocurrency at the point the transaction takes place. [182]

– **Other member countries**: The above accords with the approach taken in other member countries. For instance, in Ghana the taxation applicable to products sold, VAT and national health insurance levy are not diminished on account of the medium of payment. Merchants who conduct sales of goods and services would be held responsible for the collection of such statutory taxes. Purchasers would similarly have to comply with the tax regime applicable to such vendors operating in Ghana. In Ghana, transactions in land require the payment of stamp duty, except where they are statutorily stamp duty exempted. The registration processes of land in any application for registration of title regardless of the type of consideration involved in the transaction has to be paid in fiat currency. Payment by fiat currency would apply to all statutory applicable taxes and penalties. The assessment of stamp duty is a statutory process and where the transaction is not stamp duty exempt, the law permits the valuation to be undertaken by the registering authority. Therefore, although the consideration exchanged for the purchase of heritable property could be paid in virtual currency, the valuation of the property and any tax due from that valuation would fall to be undertaken in local fiat currency.

  In many member countries, for example Uganda and India, no regulatory guidance has yet been issued in relation to the treatment of virtual currencies for tax purposes.

Consumer protection

154. It is difficult to ascertain the situation relating to the protection of consumers purchasing virtual currencies or using them as a medium of exchange in transactions for goods and services. Although many member countries have consumer protection and unfair contract terms legislation in place, the issue of consumer protection is often an issue for local, state or provincial government. As such, it has not been possible to obtain a complete overview of the approach taken by member countries.

155. In relation to consumer protection regimes, there are two issues of paramount importance. The first is whether or not transactions in which consumers purchase virtual currencies fall within consumer protection regimes. The second is whether or not transactions in which consumers use virtual currencies as the medium of exchange in the purchase of goods and services fall within consumer protection regimes.

156. Within member countries, not only will responsibility often reside at a state or local level, as in Nigeria, but even where national protection regimes apply, multiple authorities may have responsibility.

182 HM Revenue & Customs (2014), *Policy Paper: Revenue and Customs Brief 9 (2014): Bitcoin and Other Cryptocurrencies*, London, UK.

- **European Union**: In relation to consumer protection, the main European legislation is the Directive on Consumer Rights (2011/83/EC). This directive provides protection for the supply of digital content (defined as 'data which are produced and supplied in digital form'). This directive would appear to apply to purchases of virtual currencies as it defines payment to include 'any facility for which money has been paid'. It is not clear how this relates to situations where the virtual currencies was acquired without the payment of fiat money (i.e. by mining or in return for goods and services supplied). **However, the framework of consumer protection imposed by the directive applies in the three member countries that are also members of the EU (Cyprus, Malta and the United Kingdom) – although the directive requires enabling national legislation for its implementation**.
- **United Kingdom**: Much of the United Kingdom's existing consumer protection law is not applicable to consumers entering into contracts for virtual currencies.[183] The Consumer Rights Act 2015 received Royal Assent in March 2015 and has been in force since October 2015. The primary purpose of this Act is to provide purchasers of digital content with the same rights already available to those purchasing physical goods.[184] The Act extends consumer protection to contracts for digital content purchased 'using, by way of payment, any facility for which money has been paid'.[185] It is made clear in the explanatory notes to the Act that this includes payments made with virtual currencies.[186]

  Virtual currencies themselves could be considered 'digital content' for the purposes of the Act. It therefore appears that the Act, and the consumer protection regime, would apply to transactions for the purchase of virtual currencies or related payment products and services.[187]

  However, there are limitations to consumer protection in the context of using virtual currencies as the mode of exchange for the purchase of goods and services. For example, the Act distinguishes between contracts for 'goods'[188] and 'digital content'.[189] The express protections relating to virtual currencies appear to apply only to contracts for the supply of digital content, not tangible goods and services. The explanatory notes to the Act suggest that the legal position may be that a contract where the trader agrees to accept something other than fiat currency (e.g. loyalty points) could be a sales contract. Despite this, under the Act sales contracts and contracts for the transfer of goods both attract the same rights and remedies for consumers.[190]

  As mentioned above, the Consumer Rights Act 2015 distinguishes between contracts for 'goods' and 'digital content'. The express protections relating to virtual currencies appear to apply only to contracts for the supply of digital content, not tangible goods and services. However, the protections

183 See, Brito J, et al. *The Law of Bitcoin*, (2015).
184 Sheridans (2015), *Consumer Rights Act 2015*, available at <http://ukie.org.uk/sites/default/files/cms/docs/need%20to%20know%20-%20Consumer%20Rights%20Act%202015.pdf> (last accessed 9 December 2015).
185 Consumer Rights Act 2015, at Section 33(3).
186 Explanatory Notes Consumer Rights Act 2015, at paragraph 206.
187 See, Brito J, et al. *The Law of Bitcoin*, (2015).
188 Consumer Rights Act 2015, section 2(8): 'any tangible moveable items, but that includes water, gas and electricity if and only if they are put up for supply in a limited volume or set quantity'.
189 'data which are produced and supplied in digital form', Consumer Rights Act 2015 at section 2(9).
190 Explanatory Notes Consumer Rights Act 2015, at paragraph 58.

relating to the supply of goods contained in Chapter 2 of the Act apply to contracts for sale – defined as being (a) where the trader transfers or agrees to transfer ownership of goods to the consumer, and (b) the consumer pays or agrees to pay the price. The Act requires that the goods must have a monetary price.

The types of virtual currency envisaged by the Act are those which are purchased for fiat currency with a game or other closed electronic environment. This is different from decentralised crypto currencies such as Bitcoin. However, the Act would appear to embrace virtual currencies such as Bitcoin, where they had been purchased in exchange for fiat currency (e.g. from an exchange). This would seem to exclude from the consumer protection regime transactions where the virtual currency used was acquired by mining or in exchange for goods and services.

- **New Zealand**: There are two primary pieces of legislation that ensure the effective protection of consumers in New Zealand. These are the Fair Trading Act (as amended 2013) and the Commerce Act. The Fair Trading Act in particular seeks to regulate online sales and requires, for example, that vendors disclose that they are in trade as opposed to being private individuals when offering goods and services for sale online. The Commerce Act seeks to promote competition within markets and prohibits anti-competitive conduct.[191] It was reported in 2013 that the New Zealand Commerce Commission had confirmed that virtual currencies such as Bitcoin are 'covered' by both legislative regimes.[192]
- **Kenya**: Given the prevalence of electronic payment systems in Kenya, consumer protection in electronic transactions has been a significant issue.[193] The Kenyan Banking Association has highlighted the need to protect low-income consumers owing to their limited awareness, knowledge and skills to assess products' appropriateness, costs and risks. The primary source of consumer protection in Kenya is the Constitution, which gives consumers various rights.

  The Consumer Protection Act 2012 has provided Kenya's first specific law on consumer protection. It applies only to goods and services and not to financial products or intangible goods and it would appear not to encompass the purchasing of virtual currencies. The draft of the Consumer Protection Bill, promoted by the Consumers Federation of Kenya would have encompassed transactions in which virtual currencies were used as the consideration.[194] These provisions (which closely mirror those contained in the South African legislation) would appear to have applied the consumer protection regime to transactions undertaken using virtual currencies but were not included in the legislation as enacted.

191 Commerce Commission New Zealand (2014), *The legislation: A brief summary of legislation the Commerce Commission enforces*, available at <http://www.comcom.govt.nz/the-commission/about-us/the-legislation/> (last accessed 9 December 2015).

192 L. Walters, (2013), *Bitcoin: Beauty or bubble?*, Stuff.co.nz, available at <http://www.stuff.co.nz/technology/digital-living/30008862/bitcoin-beauty-or-bubble> (last accessed 9 December 2015).

193 J. Malala, (2013), *Consumer Protection for Mobile Payments in Kenya: An Examination of the Fragmented Legislation and the Complexities it Presents for Mobile Payments*, Kenya Bankers Association, Nairobi, Kenya, at 10.

194 Consumer Protection Bill 2011, available at <http://www.cofek.co.ke/THE%20CONSUMER%20PROTECTION%20BILL.pdf> (last accessed 9 December 2015).

- **South Africa**: The Consumer Protection Act 2008 provides consumer protection within South Africa. The 2008 defines 'goods' to include 'any literature, music, photograph, motion picture, game, information, data, software, code or other intangible product written or encoded on any medium, or a license to use any such intangible product'. This would encompass virtual currencies and their purchase. The Act also protects transactions that are undertaken using virtual currencies as the medium of exchange.[195] The consumer protection legislation of South Africa appears to effectively encompass virtual currencies and their use.

195 Consumer Protection Act 2008 (Act No. 68 of 2008), at Section 1.

Conclusions and Recommendations

Conclusions

1. Virtual currencies are used in almost every Commonwealth member country and in every region of the Commonwealth;
2. They have the potential to benefit member countries and to drive development, but they also involve risks, particularly as regards their use by criminals for money laundering, terrorist financing and cyber-enabled crime.
3. With the exception of one member country,[196] in which virtual currencies have been declared unlawful, the majority of member countries have recognised their advantages and have treated their use as lawful.
4. Prohibition of virtual currencies is unlikely to be effective. In some member countries in which regulation has been adopted, it has been limited, unco-ordinated and fragmentary. There remain significant areas in which regulation is required.
5. Although the FATF Recommendations and Guidance on virtual currencies have provided a global response, they are limited to AML/CFT.

Recommendations

1. **Legality**: The majority of member countries treat virtual currencies within their respective jurisdictions as lawful. Member countries should be encouraged to make a positive determination on the legality of virtual currencies.
2. **Awareness**: Member countries should be encouraged to foster an awareness of virtual currencies within their jurisdictions and of the potential risks involved (including but not limited to the ML/TF risks of VCs and the risk to consumers). Financial regulators and central banks should consider making public statements on the legality of virtual currencies and the applicability of any existing legislative frameworks. Education and funding should be provided for the training for law enforcement. Member countries could draw upon existing resource and opportunities such as those provided by UNODC[197] and INTERPOL,[198] as well as forthcoming resource from other international partners.
3. **Legal frameworks**: Member countries should be encouraged to consider the application of their existing legal frameworks to virtual currencies and, where appropriate, adapt them or enact new legislation to regulate virtual currencies. Where member countries consider it necessary to legislate in response to cyber or cyber-enabled crime, they should be encouraged to have regard to the provisions of the Commonwealth Model Law on Computer and Computer Related Crime and related Commonwealth documents.

196 Bangladesh.
197 United Nations Office on Drugs and Crime (UNODC) (2014), *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, UNODC, Vienna, Austria.
198 INTERPOL, *Darknet training shines light on underground criminal activities*, available at <http://www.interpol.int/News-and-media/News/2015/N2015-108> (last accessed 9 December 2015).

a. **Taxation**: Tax authorities are encouraged to make public statements clarifying the appropriate taxation regimes applicable to virtual currencies and transactions relating to their use as a medium of exchange. Where appropriate, tax authorities are encouraged to adapt and extend existing taxation regimes to virtual currencies.

b. **Proceeds of crime**: Member countries should be encouraged to consider revising their proceeds of crime legislation to ensure that it is adequate to encompass the potential transmission of benefit by criminals using virtual currencies.

c. **Consumer protection**: Member countries should be encouraged to consider the possibility of extending their consumer protection legislation to include purchases of virtual currencies as well as consumer transactions using virtual currencies as a medium of exchange.

Any regulatory and legislative frameworks should focus on interactions with fiat currencies and avoid attempting to regulate the underlying decentralised ledger technology. Such frameworks should be technologically neutral and avoid stifling innovation.

4. **AML/CFT regulation**: Member countries are encouraged to implement the FATF Guidance for a Risk Based Approach to Virtual Currencies (June 2015) by bringing entities transacting at the intersection of fiat and virtual currencies within existing AML/CFT regimes. These should include applying existing registration or licensing requirements to such entities including, where appropriate, mutual recognition of licenses granted in one jurisdiction in other Commonwealth jurisdictions. Member countries are encouraged to use existing resources such as the Model Provisions for Common Law Legal Systems on Money-Laundering, Terrorist Financing, Preventative Measures and the Proceeds of Crime prepared jointly by the Commonwealth Secretariat, UNODC and the International Monetary Fund (IMF).

5. **Law enforcement**: Member countries should consider developing and improving the capacity of law enforcement, especially in the areas of digital forensics and analytics. This should include the training of prosecutors, judges and regulatory authorities.

6. **Co-operation**: The Commonwealth Secretariat and other international partners should create a digital repository of best practice and model regulations as part of an online community to assist member countries in developing their policies and capacity to respond to virtual currencies. Capacity-building activities for relevant public sector stakeholders should also be considered.

   a. Member countries should encourage the establishment of industry associations within their jurisdictions to support the development of a responsible and sustainable virtual currency industry. Where such associations already exist, member countries should be encouraged to proactively engage with them and encourage responsible behaviour among their members, for example by establishing or promulgating industry standards and accreditation models.

   b. Clear information-management systems should be established between industry sectors to share information regarding suspicious transactions and to enhance co-operation in support of the development of a RBA to the industry, and to allow a fair appraisal of strengths and weaknesses within compliance models.

7. **Definitions**: Relevant technical terms should be clearly defined in any guidance to be made available to member countries.

Next steps

The Working Group will proceed to disseminate this report to member countries.

At this point, the Working Group, having discharged the first element of its brief by completing this report, will commence work on the second element, namely, the creation of technical guidance for member countries on how to respond to virtual currencies within their jurisdictions.

Definitions

The definitions relied upon in the report are as follows:

Altcoins – 'Math-based decentralised convertible virtual currency other than Bitcoins, the original such currency. Current examples include Ripple, PeerCoin, Lite-coin, zerocoin, anoncoin and dogecoin. One popular exchanger, Cryptsy, would reportedly exchange over 100 different virtual currencies.'[199]

Bitcoin – the Internet Society has provided an effective definition of Bitcoin in a 2015 paper. The paper states that:

'Bitcoin is a cryptographic currency deployed in 2009 which has reached a level of adoption unrealized by decades of previously proposed digital currencies (from 1982 onward). Unlike many previous proposals, Bitcoin does not distribute digital monetary units to users. Instead, a public ledger maintains a list of every transaction made by all Bitcoin users since the creation of the currency. A transaction in its simplest form describes the movement of some balance of the Bitcoin currency (XBT or BTC) from one or more accounts (called input addresses) into one or more accounts (called output addresses). The fingerprint of a public key from a digital signature scheme indexes Bitcoin addresses. They are not centrally allocated or registered in any way—the addresses become active when the first transaction moving money into them is added to the ledger.

In Bitcoin, every transaction must be digitally signed using the private signing key associated with each input address in the transaction. In order to spend Bitcoin, users require access to the signing key of the account holding their Bitcoin. Thus users do not maintain any kind of units of currency; they maintain a set of keys that provide them signing authority over certain accounts recorded in the ledger.'[200]

Bitcoin is one of many virtual currencies in use to date, but it is by far the most widely used and publicised. FATF notes that 'As of April 2 2014, there were over 12-and-a-half million Bitcoins, with total value of slightly more than USD 5.5 billion, based on the average exchange rate on that date.'[201]

Blockchain – 'A public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as "completed" blocks are added to it with a new set of recordings. The blocks are added to the Blockchain in a linear, chronological order. Each node (computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions) gets a copy of the Blockchain, which gets downloaded automatically upon joining the Bitcoin network. The Blockchain has complete information about the addresses and their balances right from the genesis block to the most recently completed block.'[202]

Client – End-user software that facilitates the secure use and transmission of the virtual currency, also known as a wallet.[203]

Darknet/dark web – Please see definition of 'Tor'.

199 FATF/OECD(2014), *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF, Paris, France, at paragraph 28

200 S. Eskandari, D. Barrera, & E. Stobert et al. (2015), *A First look at the usability of bitcoin key management*, The Internet Society, 8 February 2015, at 2.

201 FATF/OECD (2014), *Guidance for a risk-based approach: Virtual Currencies*, FATF, Paris, France, at paragraph 28.

202 *Blockchain*, Investopedia, available at <http://www.investopedia.com/terms/b/Blockchain.asp>.

203 Clients, Bitcoin Wiki, see, <https://en.Bitcoin.it/wiki/Clients> (last accessed 9 December 2015).

Darknet markets – Utilising Tor or other anonymity service, it is possible to access 'hidden website[s] designed to enable its users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law enforcement'.[204]

Exchange – An undertaking engaged in the 'the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third-party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.'[205]

Merchants – Undertakings accepting virtual currencies, particularly Bitcoins, in return for the provision of goods and services, whether in person, via postal delivery or using communications technology. Accepting virtual currencies requires some form of merchant solution (i.e. payment-processing software).

M-Pesa – A short message service-based money transfer system that allows individuals to deposit, send and withdraw funds using their mobile phone.[206]

Miner – 'An individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners may be users, if they self-generate a convertible virtual currency solely for their own purposes, e.g., to hold for investment or to use to pay an existing obligation or to purchase goods and services. Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency.'[207]

Many persons consider themselves miners for investing in the myriad of third-party cloud-mining services available online (such services ranging from the renting out of enthusiast equipment to others, to services offered by enterprise Bitcoin cloud-mining companies).

Node – In order to maintain the decentralised ledger, Bitcoin requires messages to be broadcast across its networks to ensure the updating of each decentralised copy of the Blockchain. Nodes perform this task.

Risk – For the purposes of this report the 'risk' posed by virtual currencies can be understood as having three components. The first of these relates to the use of virtual currencies to undertake criminal activity. The second relates to the effect that enhanced anonymity in financial transactions has upon the capacity of law enforcement and regulatory agencies to keep abreast with investigatory and supervisory functions. The third is that posed to consumers using virtual currencies.[208]

---

204 US Department of Justice (2013), *Manhattan U.S. Attorney Announces Charges Against Three Individuals In Virginia, Ireland, And Australia For Their Roles In Running The "Silk Road" Website*, Press Release, 20 December 2013, available at <http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-three-individuals-virginia-ireland-and> (last accessed 9 December 2015).

205 FATF/OECD (2015), *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF, Paris, France, at paragraph 29.

206 W. Jack & T. Suri, (2010), *The Economics of M-PESA*, available at <http://www.mit.edu/~tavneet/M-PESA.pdf> (last accessed 9 December 2015).

207 FATF/OECD (2015), *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF, Paris, France, at paragraph 29.

208 Commonwealth Virtual Currencies Roundtable Outcomes, London, United Kingdom, 17–18 February 2015 at 4(c).

In relation to the first element of the risk profile, types of illicit conduct associated with virtual currencies can be organised by four categories. These are:

- regulatory offences – involving conduct that threatens the integrity of a banking or financial services system;
- virtual currencies as the object of the offence – primarily involving attempts to illicitly appropriate virtual currencies either through direct theft (via physical or electronic means), or fraud;
- virtual currencies as an instrument of offending – including the use of virtual currencies to purchase illicit goods such as drugs, weapons and persons, and for the financing of terrorist activities; and
- virtual currencies as the proceeds of crime – including where virtual currency is received directly in return for supply of illicit goods or services, as well as where virtual currencies are used for the laundering of crime proceeds in fiat currency.

The second aspect of risk relates to the effect that higher degrees of anonymity in transactions have upon investigations by competent authorities. By allowing users to avoid traditional financial institutions, and the associated regulatory requirements to record transactions, virtual currencies 'significantly complicate law enforcement efforts to follow the money'. This is the case particularly within the context of investigations into money laundering, the financing of terrorism, and trafficking in drugs, arms and human beings, the effect of which represents an increasing concern.

The risk to consumers arises as a result of two primary factors. The first of these is the volatility of these types of currencies, as witnessed by the fluctuating dollar values of Bitcoins. In addition, however, the decentralised nature of some virtual currencies and the concomitant lack of governing infrastructure means that there is no mechanism of redress. As such, there is potentially little in the way of consumer protection.

Tor – The UK Parliamentary Office of Science and Technology has provided a useful explanation of Tor. In its report on the darknet and online anonymity, it was stated that:

'The vast majority of web pages are invisible to most casual internet users. This part of the web is known as the deep web. In contrast to the open web, it consists of pages that cannot be found by popular search engines like Google. Most of these pages are standard personal or corporate pages such as intranet pages, administrative databases or personal photo collections. A very small proportion of websites in the deep web use sophisticated anonymity systems, which allow their operators to conceal their identity if they wish to. . . The most popular anonymity system is called "Tor" [originally "The Onion Router"]. In 2014, Tor had an estimated 2.5 million daily users. . . Tor relays a user's data through the Tor Network, which hides the user's Internet Protocol (IP) address and other identifiers from the websites they visit and disguises the user's online activities. This means that anyone monitoring internet communication will find it difficult to trace these activities back to a specific user. . . Tor allows users to do two distinct things: use the open web anonymously with the Tor Browser, which looks similar to common web browsers such as Microsoft Internet Explorer or Mozilla Firefox [and] publish anonymous web services as Tor Hidden Services.'[209]

209 UK Parliamentary Office of Science and Technology (2015), *The darknet and online anonymity*, available at <http://researchbriefings.files.parliament.uk/documents/POST-PN-488/POST-PN-488.pdf> (last accessed 9 December 2015).

Other terms such as darknet and dark web are often used to refer to these hidden portions of the internet accessible only through specialist services such as Tor.

When used in conjunction with the anonymity-enhancing features of many virtual currencies, Tor provides significant abilities to conduct transactions beyond the reach of many forms of surveillance and supervision. This makes such services attractive to criminals.

User – 'A person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralised virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) with some decentralised virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them. . . and receive them as gifts, rewards, or as part of a free initial distribution.'[210]

Virtual currencies – A 'digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account and/or a stored value, but does not have legal tender status in any jurisdiction'.[211] It is useful to note that this definition has been expressly relied upon by certain member countries, such as South Africa,[212] in the development of policy. Although this formulation represents a generic working definition, it does not provide an exhaustive understanding of the concept, owing to the proliferation of multiple forms of virtual currencies, each exhibiting varied characteristics in their operations and interaction with the real world. Whereas some virtual currencies have a centralised administrative authority or system, such as in computer gaming environments, others are highly decentralised with no central monitoring authority. These operate on a peer-to-peer basis, offering a high degree of anonymity. Whether centralised or decentralised, virtual currencies can be either 'static' (non-convertible to fiat currency), 'unidirectional' (able to be either purchased or sold in return for fiat currency) or 'convertible' (able to be both purchased and sold in return for fiat currency). Most decentralised virtual currencies also fall within the category of 'cryptocurrencies', in that they rely on a process of cryptography for security and anti-counterfeiting measures. Bitcoin currently represents the most widely used cryptocurrency, with a market capitalisation of over US$3 billion. Others, including, Ripple, Litecoin, PayCoin, BitShares, Stellar, Dogecoin and Darkcoin, have a combined market capitalisation of just over US$1 billion.

This report is concerned with convertible, decentralised virtual currencies but will use the term virtual currency as a short-hand.

Wallet – '(Software application or other mechanism/medium) for holding, storing and transferring Bitcoins or other virtual currency. . . A wallet holds the user's private keys, which allow the user to spend virtual currency allocated to the virtual currency address in the block chain. . . All Bitcoin wallets can interoperate with each other. Wallets can be stored both online ("hot storage") or offline ("cold storage")'[213]

210 FATF/OECD (2015), *Guidance for a Risk-Based Approach: Virtual Currencies*, FATF, Paris, France, at paragraph 30.
211 FATF/OECD (2014), *Virtual Currencies – Key Definitions and Potential AM/CFT Risks*, FATF/OECD, Paris, France, at paragraph 4.
212 South African Reserve Bank, *Position Paper on Virtual Currencies*, at paragraph 2.
213 FATF/OECD, *Guidance for a risk-based approach: Virtual Currencies*, FATF, Paris, France, at paragraph 28.

Wallet provider – The entity that provides a virtual currency wallet. A provider 'facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. For example, beyond providing Bitcoin addresses, the wallet may offer encryption; multiple key (multi-key) signature protection, backup/cold storage; and mixers.'[214]

214 *Ibid.*

Contributors

This report has been prepared by the following members of the Commonwealth Working Group on virtual currencies:

Mr D. Mossop (Australia)

Mr E. Boyce (Barbados)

Ms M. Kimani (Kenya)

Mr T. Tyendezwa (Nigeria)

Mr T. Chua (Singapore)

Mr S. Malhotra (Singapore)

Hon. Mr A. Kefu (Tonga)

Mr L. De Alwis (Commonwealth Telecommunications Organisation)

Ms S. Sargent (World Bank)

Mr C. Karam (INTERPOL)

Ms T. Banuelos (UN Office on Drugs and Crime)

The Working Group was chaired by Mr Colin Nicholls QC, and Ms E. George acted as Rapporteur.

Although the views expressed in the report reflect those of the authors, the comments provided by Mr. N. Kyriakos-Saad and Ms. Y. Almeida (IMF), are gratefully acknowledged.

The US Government was an observer of the Working Group and was represented by Ms C. Alden Pelker (Federal Bureau of Investigation), Mr A. Storer (Federal Bureau of Investigation) and Mr J. Mignano (US Department of Justice).

Research and staff support was provided by the Commonwealth Secretariat including Mr S. Malby, Mr S. Haruna, Mr A. Ming and Mr D. Tait.

The Secretariat would like to thank the following persons for compiling the information contained within the report:

Uchenna Orji (Nigeria); Aditya Rao, Suhaan Mukerji, Aymen Mohammed and Shatadal Ghosh of PLR Chambers (India); Curtis Busby-Earle (Jamaica); William Makatiani (Kenya); Raymond Codjoe (Ghana); Annamart Nieman (South Africa); Nadine Maitland (Trinidad and Tobago); and Maureen Owor Mapp (Uganda).

Bibliography

Abed, G. (2015), presentation to Commonwealth Working Group on Virtual Currencies, 24 August 2015, London, UK.

Ahmed, K. (2015), 'TalkTalki – could this be an extortion attack?', BBC News website, 23 October 2015, available at: http://www.bbc.co.uk/news/business-34613137 (last accessed 9 December 2015).

Australian Senate (2015), *Digital Currency – Game Changer or Bit Player*, Economic References Committee, Canberra, ACT, Australia.

Australian Tax Office (2014), 'Tax treatment of crypto-currencies in Australia – specifically bitcoin', available at: https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/ (last accessed 9 December 2015).

Balanarayan, N.T. (2014), 'ED Raids Offices Of Bitcoin Websites; Its Aftermath And Our Take', *Medianama*, 2 January 2014, available at: http://www.medianama.com/2014/01/223-Bitcoin-india-raid-shuts/ (last accessed 9 December 2015).

Bank of England, Quarterly Bulletin 2014 Q3, *The Economics of Digital Currencies*, 2014.

Bank of Jamaica (2013), *Guidelines for Electronic Retail Payment Services*, Bank of Jamaica, Kingston, Jamaica.

BizReport, 'Global ecommerce sales top U.S.$1 trillion', available at: http://www.bizreport.com/2013/08/global-ecommerce-sales-top-us1-trillion.html (last accessed 9 December 2015).

Borden Ladner Gervais (2014), 'The regulation of virtual currencies in Canada', 10 September 2014, available at: http://www.blg.com/en/newsandpublications/publication_3835 (last accessed 9 December 2015).

Bohm, N. & Mason, S. (2010), 'Identity and its verification', *Computer Law & Security Review*, Vol. 26 No. 1, 43–51, available at: http://useBitcoins.info/index.php/Bitcoin-in-the-real-world (last accessed 9 December 2015).

Brito J, et al. The Law of Bitcoin, (2015).

Caffyn, G. (2015), 'Everledger Brings Blockchain Tech to Fight Against Diamond Theft', Coindesk, 1 August 2015, available at: http://www.coindesk.com/everledger-blockchain-tech-fight-diamond-theft/ (last accessed 9 December 2015).

Cajani, F. (2009), 'International phishing gangs and operation Phish & Chip', *Digital Evidence and Electronic Signature Law Review*, Vol. 6, 153–7.

CCN.LA (2015), 'Isle of Man to create cryptocurrency business register', available at: https://www.cryptocoinsnews.com/isle-man-create-cryptocurrency-businesses-register/ (last accessed 9 December 2015).

Center for Strategic and International Studies (2014), *Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II*, Washington DC, USA, available at: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf (last accessed 9 December 2015).

Christin, N. (2012), 'Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace', Carnegie Mellon University, 1–26, (last accessed 9 December 2015), available at: <https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf>.

Commonwealth Secretariat (2014), *Report of the Commonwealth Working Group of Experts on Cybercrime*, LMM(14)14, Commonwealth Secretariat, London, UK.

Commonwealth Secretariat (2015), 'De-risking diaspora remittances', available at: http://thecommonwealth.org/media/press-release/%E2%80%98de-risking%E2%80%99-diaspora-remittances

Cryptocoin News (2014), '70% of bitcoins have been hoarded for six months or more', *Cryptocoin News*, 24 November 2014, available at: https://www.cryptocoinsnews.com/70-bitcoins-hoarded-six-months/.

Commerce Commission New Zealand (2014), 'The legislation: A brief summary of legislation the Commerce Commission enforces', available at: http://www.comcom.govt.nz/the-commission/about-us/the-legislation/ (last accessed 9 December 2015).

Cyprus Mail (2014), 'Cyprus police issues arrest warrant for Bitcoin entrepreneur', *Cyprus Mail*, 11 April 2014, available at: http://cyprus-mail.com/2014/04/11/cyprus-police-issue-arrest-warrant-for-Bitcoin-entrepreneur/ (last accessed 9 December 2015).

Descoteaux, D. 'Bitcoin: More Than a Currency, a Potential for Innovation', Montreal Economic Institute, Economic Note, available at: http://www.iedm.org/files/note0114_en.pdf (last accessed 9 December 2015).

Dutta, V. (2013), 'ED officials raided two Bitcoin trading firm in Ahmedabad', *Economic Times*, 27 December 2013, available at: http://articles.economictimes.indiatimes.com/2013-12-27/news/45626789_1_one-Bitcoin-Bitcoin-transactions-peer-to-peer-payment-network (last accessed 9 December 2015).

Eskandari, S, Barrera, D. & Stobert, E, et al. (2015), 'A First look at the usability of bitcoin key management', The Internet Society, 8 February 2015, (last accessed: 8 December 2015), available at: http://www.internetsociety.org/sites/default/files/05_3_3.pdf (last accessed 9 December 2015).

European Banking Authority (2014), *EBA Opinion on 'virtual currencies'*, European Banking Authority, London, UK.

European Central Bank (2015), *Virtual Currency Schemes – A Further Analysis*, European Central Bank, Frankfurt am Main, Germany.

European Commission, 'Euro legal tender', available at: http://ec.europa.eu/economy_finance/euro/cash/legal_tender/index_en.htm (last accessed 9 December 2015).

European Securities and Markets Authority (ESMA) (2015), *Call for Evidence, Investment Using Virtual Currency or Distributed Ledger Technology*, ESMA/2015/532, ESMA, Paris, France, available at: http://www.esma.europa.eu/system/files/2015-532_call_for_evidence_on_virtual_currency_investment.pdf (last accessed 9 December 2015).

Europol, The Internet Organised Crime Threat Assessment (IOACTA), 2015, available at: https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf (last accessed 9 December 2015).

Fargo S (2015), 'Is Bitcoin the Future of Micropayments?', *Inside Bitcoins*, 10 April 2015, available at: http://insideBitcoins.com/news/is-Bitcoin-the-future-of-micropayments/31555 (last accessed 9 December 2015).

Financial Action Task Force, *What is Money Laundering*?, Paris, France, (last accessed: 8 December 2015), available at: http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223 (last accessed 9 December 2015).

FATF/OECD (2014), Virtual Currencies – Key Definitions and Potential AM/CFT Risks, FATF/OECD, Paris, France.

FATF/OECD (2015), Guidance for a Risk-Based Approach: Virtual Currencies, FATF, Paris, France.

Federal Bureau of Investigation (2015), 'Cyber Criminal Forum Taken Down', available at: https://www.fbi.gov/news/stories/2015/july/cyber-criminal-forum-taken-down/cyber-criminal-forum-taken-down (last accessed 9 December 2015).

Federal Deposit Insurance Corporation, 'Tapping the Unbanked Market', available at: www.fdic.gov/consumers/community/unbanked/index.html.

Financial Intelligence Unit – *India, Prevention of Money Laundering Act*, 2002, New Delhi, India.

Gibbs, G (2014), 'Virtual Currency: Fad or Future? Monetary Thought and Policy', *The Student Economic Review*, Vol. 28, 64–72.

Gilbert D (2014), 'Dogecoin Community Helps Send Indian Athletes to Winter Olympics', *International Business Times*, 30 January 2014available at: http://www.ibtimes.co.uk/dogecoin-community-helps-send-indian-athletes-winter-olympics-1434515 (last accessed 9 December 2015).

Godlove N (2014), 'Regulatory Overview of Virtual Currency', *Oklahoma Journal of Law & Technology*, Vol. 10, 1–67.

Great Britain (2015). Consumer Rights Act 2015, The Stationery Office, London, UK.

Hileman, G (2015), 'Consensus 2015 – State of the Blockchain', 10 September 2015, available at: http://www.slideshare.net/CoinDesk/consensus-2015-state-of-blockchain-52673969 (last accessed 9 December 2015).

HM Revenue & Customs (2014), Policy Paper: Revenue and Customs Brief 9 (2014): Bitcoin and Other Cryptocurrencies, HM Revenue & Customs, London, UK.

INTERPOL (2015), 'Darknet training shines light on underground criminal activities', available at: http://www.interpol.int/News-and-media/News/2015/N2015-108 (last accessed 9 December 2015).

INTERPOL (2015), 'INTERPOL cyber research identifies malware threat to virtual currencies', available at: http://www.interpol.int/News-and-media/News/2015/N2015-033 (last accessed 9 December 2015).

Jack, W and Suri, T (2010), *The Economics of M-PESA*, (last accessed: 8 December 2015), available at: <http://www.mit.edu/~tavneet/M-PESA.pdf> (last accessed 9 December 2015).

Kelven, U. (2015), 'Central Bank of Nigeria ponders regulation of virtual currencies', available at: http://techloy.com/2015/09/02/central-bank-of-nigeria-ponders-regulation-of-virtual-currencies/ (last accessed 9 December 2015).

Leal, R. (2014), *Is Bitcoin the Future of Payments*?, TOP OF MIND, Goldman Sachs Global Investment Research Paper, Issue 21, 18.

Malala, J. (2013), Consumer Protection for Mobile Payments in Kenya: An Examination of the Fragmented Legislation and the Complexities it Presents for Mobile Payments, Kenya Bankers Association, Nairobi, Kenya.

Mance, A. (2014), Paper presented to the Commonwealth Working Group on Virtual Currencies, 24 August 2015, London, UK.

Mason, S. (Ed.) (2012), *Electronic Evidence*, 3rd ed, Butterworths Law.

Mason, S. and Reiniger, T.S. (2015), '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?', *Computer and Telecommunications Law Review*, Vol. 21 No. 5, 135–148.

Matonis, J. (2014), '12 Ways to measure the Bitcoin Network's health', CoinDesk, 27 September 2014, available at: http://www.coindesk.com/12-ways-measure-Bitcoin-networks-health/ (last accessed 9 December 2015).

Meiklejohn, S. (2015), Paper presented to the Commonwealth Working Group on Virtual Currencies, 24 August 2015, London, UK.

Merkle Tree (2015), 'Compliance with Bank Secrecy Act – MSB – US', available at: http://merkletree.io/blog/2015/05/obligations-to-comply-with-bank-secrecy-act-regardless-of-registration-as-msb-us/ (last accessed 9 December 2015).

Mignano, J. (2015), Paper presented to the Commonwealth Working Group on Virtual Currencies, 24 August 2015, London, UK.

Mohit, B. (2015), 'Bitcoin: Is it an Economic Equalizer or a Tool for Conflict and Crime?', *The Huffington Post*, 17 February 2015, available at: http://www.huffingtonpost.com/dr-behzad-mohit/Bitcoin-is-it-an-economic_b_6617994.html (last accessed 9 December 2015).

Nandakumar, A. and Maruvada, R. (2014), 'RBI puts the brakes on the Bitcoin train in India', Reuters, 17 January 2014, available at: http://blogs.reuters.com/india/2014/01/17/rbi-puts-the-brakes-on-the-Bitcoin-train-in-india/ (last accessed 9 December 2015).

Otitoju, K. (2015), Paper presented to the Commonwealth Working Group on Virtual Currencies, 24 August 2015, London, UK.

Pauli, D. (2015), 'Cybercrime forum Darkode returns with security, admins intact', *The Register*, 28 July 2015, available at: http://www.theregister.co.uk/2015/07/28/darkode_returns/ (last accessed 9 December 2015).

Reserve Bank of India (2013), 'RBI cautions users of Virtual Currencies against Risks', 24 December 2014, available at: https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=30247 (last accessed 9 December 2015).

Rizzo, P. (2014), 'Bitcoin Bank Flexcoin to Close After $600k Bitcoin Theft', CoinDesk, 4 March 2014, available at: http://www.coindesk.com/Bitcoin-bank-flexcoin-close-600000-Bitcoin-theft/ (last accessed 9 December 2015).

Rizzo, P. (2015), 'Pantera Leads $1.1 Million Funding for African Bitcoin Startup BitPesa', CoinDesk, 9 February 2015, available at: http://www.coindesk.com/bitpesa-1-1-million-bitcoin-africa/(last accessed 9 December 2015).

Roberts, D. (2015), 'Behind the "exodus" of bitcoin startups from New York', Fortune.com, 14 August 2014, available at: http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/ (last accessed 9 December 2015).

Serianu Ltd (2015), *Kenya Cyber Security Report*, Serianu Ltd, Nairobi, Kenya.

Shinde, S. (2015), 'Soon, buy a flat, pay restaurant bills using Bitcoin', *Economic Times*, 26 March 2015, available at: http://www.business-standard.com/article/companies/soon-buy-a-flat-pay-restaurant-bills-using-Bitcoin-115032600991_1.html (last accessed 9 December 2015).

South African Reserve Bank, National Payment System Department, *Position Paper on Virtual Currencies*, Paper Number 02/2014, (2014).

Southurst, J. (2014), 'New Zealand Bitcoin ATM Operator Shuts Down After Bank Refusals', Coindesk, 30 July 2014, available at: http://www.coindesk.com/new-zealand-Bitcoin-atm-operator-shuts-down-bank-refusals/ (last accessed 9 December 2015).

Southurst, J. (2015), 'ICE3x Launches Nigeria's First Bitcoin Exchange', Coindesk, 7 January 2015, available at: http://www.coindesk.com/ice3x-launches-nigerias-first-Bitcoin-exchange/ (last accessed 9 December 2015).

The Hindu (2014), 'Bitcoin impact: Laxmicoin seeks regulatory clarity for launch', *The Hindu*, 7 January 2014, available at: http://www.thehindu.com/business/Economy/Bitcoin-impact-laxmicoin-seeks-regulatory-clarity-for-launch/article5549324.ece (last accessed 9 December 2015).

UK Parliamentary Office of Science and Technology (2015), 'The darknet and online anonymity', available at: http://researchbriefings.files.parliament.uk/documents/POST-PN-488/POST-PN-488.pdf (last accessed 9 December 2015).

United Nations Office on Drugs and Crime (UNODC) (2014), Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, UNODC, Vienna, Austria.

US Department of Justice (2013), 'Manhattan U.S. Attorney Announces Charges Against Three Individuals In Virginia, Ireland, And Australia For Their Roles In Running The "Silk Road" Website', Press Release, 20 December 2013, available at: http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-three-individuals-virginia-ireland-and (last accessed 9 December 2015).

US Department of Justice (2013), 'Testimony of Acting Assistant Attorney General Mythili Raman before US Senate Committee on Homeland Security and Governmental Affairs', 18 November 2013, Washington, DC, USA.

Vaisoha, R. (2015), 'India's Bitcoin Exchange BTCXIndia to Close Following Loss of Banking Support', *Cointelegraph*, 12 May 2015, available at: http://cointelegraph.com/news/114224/indias-Bitcoin-exchange-btcxindia-to-close-following-loss-of-banking-support (last accessed 9 December 2015).

Vaziri, A. (2015), Paper presented to the Commonwealth Working Group on Virtual Currencies, 24 August 2015, London, UK.

Walters, L. (2013), 'Bitcoin: Beauty or bubble?', available at: http://www.stuff.co.nz/technology/digital-living/30008862/bitcoin-beauty-or-bubble (last accessed 9 December 2015).

Woodford, A. (2015), Paper presented to the Commonwealth Working Group on Virtual Currencies by 24 August 2015, London, UK.

World Bank (2014), *Global Financial Development Report 2014*, World Bank, Washington DC, USA.

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

P14195