Working Group Report

Regulatory Guidance on Virtual Currencies

October 2019

The Commonwealth

COMMONWEALTH WORKING GROUP ON VIRTUAL CURRENCIES

Regulatory Guidance on Virtual Currencies

October 2019

The Commonwealth

Published by the Commonwealth Secretariat.

Contents

Introduction

1. The Commonwealth Working Group on Virtual Currencies was established in 2015 following the adoption by Commonwealth Law Ministers of the Report of the Commonwealth Group of Experts on Cybercrime,[1] and its proposal that "every Commonwealth jurisdiction should have an up-to-date and comprehensive legal framework to combat cybercrime". The Working Group was tasked with developing a report on the prevalence and impact of virtual currencies in the Commonwealth, as well as developing technical guidance for Commonwealth Member Countries on the potential regulatory and legislative measures that could be implemented to effectively respond to virtual currencies.

2. The Working Group[2] published its first report in October 2015 ("the **2015 Report**").[3] The 2015 Report focused on two key aspects – the prevalence of virtual currencies and the impact of virtual currencies in Commonwealth Member Countries. It made the following recommendations:

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

   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 (**AML**) 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.

   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.

   Taxation: Tax authorities should be 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 were encouraged to adapt and extend existing taxation regimes to virtual currencies.

   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.

---

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

2 The Working Group consisted of representatives of Australia, Barbados, Kenya, Nigeria, Singapore, Tonga, the United Kingdom, the IMF, World Bank, Interpol and UNODC. The Working Group was chaired by Colin Nicholls QC.

3 http://thecommonwealth.org/sites/default/files/press-release/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf

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.

The FATF guidance and recommendations: Member Countries were encouraged to implement the FATF guidance for a risk-based approach to virtual currencies (originally issued in June 2015, now updated and re-issued in June 2019) by bringing entities transacting at the intersection of fiat and virtual currencies within existing AML regimes. This would 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.

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.

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:

- 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.
- 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.

3. Since the 2015 Report was published, there has been an explosion of public interest in, and availability of, virtual currencies. This development has been driven by a number of factors, including greater understanding and use of virtual currencies as well as business and media interest in blockchain-based applications utilising virtual currencies. However, a significant part of this visibility has been caused by the promotion of virtual currencies as investment opportunities, notably the record price highs of virtual currencies such as Bitcoin, to the extent that some virtual currencies effectively ceased to be units of value and became units of speculation. The price of a single Bitcoin peaked at just under $20,000 in December 2017, but was followed by a series of significant price drops and by early September 2018 a single coin was trading at around

$6,500. The price has since climbed again to around $10,700 as of August 2019. This "*boom and bust*" virtual price cycle has, in turn, led to various national regulatory initiatives as well as international discussions.

4. At the G20 meeting in Buenos Aries in March 2018, it was reported that a Finance Ministers and Central Bank Governor communiqué had been distributed in the following terms:

   Crypto-assets lack the key attributes of sovereign currencies. At some point they could have financial stability implications. We commit to implement the FATF [Financial Action Task Force] standards as they apply to crypto-assets, look forward to the FATF review of those standards, and call on the FATF to advance global implementation. We call on international standard-setting bodies (SSBs) to continue their monitoring of crypto-assets and their risks, according to their mandates, and assess multilateral responses as needed.

   We ask the FSB in consultation with other SSBs, including CPMI and IOSCO, and FATF to report in July 2018 on their work on crypto-assets."

5. The FATF Report to G20 Finance Ministers in July 2018[4] particularly focused on virtual currency issues relating to money laundering and terrorist financing, and highlighted several areas of ongoing work to ensure appropriate and consistent safeguards "*while avoiding unnecessary barriers to legitimate use*". In February 2019, FATF issued an Interpretative Note to Recommendation 15 on New Technologies which was adopted in June 2019. This further clarified an October 2018 update to the Standards to describe their application to virtual assets and virtual asset service providers by amending Recommendation 15 and adding two new definitions to the FATF Glossary. The United Nations Security Council welcomed these efforts, including in its Resolution 2462 of 28 March 2019. Subsequently, FATF has published its updated guidance on how to adopt a risk-based approach to virtual assets and virtual asset service providers in June 2019[5].

6. The G20 remains supportive of FATF's approach and efforts, with the 1 December 2018 leaders' declaration stating "*We will regulate crypto-assets for anti-money laundering and countering the financing of terrorism in line with FATF standards and we will consider other responses as needed*."

7. As a result, many countries have implemented, or are in the process of implementing, specific legislation to regulate companies or activities relating to virtual currencies both in the context of anti-money laundering but also more generally[6].

---

4 http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf

5 See http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

6 See, for example, certain European countries which have (or are considering) implementing laws and regulations relating to virtual currencies which go beyond the scope of the EU 5th Money Laundering Directive (EU) 2018/849 (which itself brings virtual currency exchanges and wallet providers within the scope of the EU AML framework) including the United Kingdom – see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf . Member Countries such as Canada have similarly updated their existing AML laws to take account of virtual currencies.

8. At the same time, there have been calls to ensure that any regulation of virtual currencies is proportionate and allows legitimate uses to flourish, including from U.S. Commodity Futures Trading Commission Chairman J. Christopher Giancarlo, when he was reported to have said:

   "And I'm advocating the same approach to cryptocurrencies and all things having to do with this new digital revolution of markets, and of currencies, and of asset classes... And I think we need to be very well-informed but I think we need to move cautiously as regulators not to inhibit innovation. At the same time, we need to be vigilant against fraud and manipulation because some of the fraud and manipulation that we often see in foreign exchange or in precious metals are now being applied to their currencies by some of the same fraudsters that operate those other asset classes. So when it comes to foreign manipulation, we need to be strong when it comes to policymaking, I think we need to be slow and deliberate and well-informed...[7]"

9. The Working Group is conscious that many other organisations and countries are looking at similar issues[8] and there is a risk of inconsistent or conflicting views. However, the Working Group also considers that there is a benefit in:

   - summarising updates and developments in virtual currency regulation;
   - reconsidering the reasons why regulation of virtual currencies may be useful or necessary in any Member Country;
   - highlighting the advantages and disadvantages perceived by the Working Group of different regulatory approaches to virtual currencies;
   - in light of all of the above, setting out updated Recommendations from the Working Group relating to virtual currencies for Member Countries to consider, to include draft regulatory guidance.

10. In order to produce this updating Report, the Working Group has drawn on a variety of public sources, presentations from Member Countries and interested third parties. The Working Group is especially grateful to Harriet Territt of Jones Day law firm and Lavan Thasarathakumar of Thasa Consulting who had primary responsibility for drafting this Report on behalf of the Working Group.

11. This information was considered by the Working Group[9] at a two day meeting held at Marlborough House in June 2018, at which the core recommendations were agreed. The Working Group has since considered and commented on this report in draft before approving the final form in August 2019. The Working Group has sought to reflect in this updating report, key developments which occurred after the Group met (and indeed after the final form of report was agreed). However, the fast moving pace of the technology, not to mention the global legal and regulatory response in this period, presents something of a

7 See transcript of CNBC Interview with Christopher Giancarlo, Chairman, U.S. CFTC at https://www.cnbc.com/2018/09/14/cnbc-transcript-christopher-giancarlo-chairman-us-cftc.html

8 For example, the UK Cryptoassets Taskforce, which issued its final report in October 2018, made recommendations as to the potential impact of cryptoassets, the potential benefits and challenges of the application of distributed ledger technology in financial services, and assessing what, if any, regulation is required in the UK in response. A further consultation is now planned in the UK on a potential expansion of the regulatory perimeter to include further types of cryptoasset.

9 The Working Group consisted of representatives of Australia, Barbados, Nigeria, Singapore, and the United Kingdom. Representatives of the International Bar Association, PwC UK, and Lykke attended as observers. The Working Group was chaired by Colin Nicholls QC. Harriet Territt of Jones Day law firm, Lavan Thasarathakumar of Thasa Consulting and Neil Pennington provided support to the Working Group on behalf of the Commonwealth Secretariat.

practical challenge. Nevertheless, the principles and recommendations set out in this document are expected to be relevant and useful on a go-forward basis for Member Countries whenever set against the prevailing factual, legal or regulatory position.

Key Definitions

12. At the heart of any virtual currency is the technology variously known as blockchain, distributed ledger technology, shared ledger technology or DLT. This Report uses "**DLT**" for convenience. One issue noted by the Working Group is the prevalence of different terms and definitions in this area which can make it difficult for non-technical specialists to understand the full impact of any proposals. The Working Group suggests the following basic definitions to help with the understanding of this Report, but acknowledges that even these are open to discussion and are not settled.

13. **DLT** is a technology for storing, tracking and processing information. At its simplest, a blockchain is a digital database of transactions. Each transaction is stored in a block of data that is securely linked to the blocks containing previous and subsequent transactions (hence block-chain). The secure link between blocks makes it simple to track and audit the validity of the data, making DLT databases much more difficult to hack or falsify due to the immutable nature of the blockchain record. DLT is the underlying technology used to run a virtual currency.

14. **Virtual currencies** (also sometimes referred to as cryptocurrencies and increasingly as cryptoassets[10]) can be defined in various ways. At one level, a virtual currency is any kind of digital asset that need not be cryptographically secured and that can be redeemed by a user for value (airline frequent flyer miles or World of Warcraft gold are an example of this broad classification). It is important to understand that from a technical perspective, coins or tokens issued on a DLT system are considered to be cryptocurrencies, as they each technically represent a unit of account, store of value or medium of exchange, regardless of whether they actually function as a "currency".

15. However, in the context of this 2019 Report, a virtual currency can be broadly defined as:

    a cryptographically secured digital currency built on a decentralized peer-to-peer network which typically functions as a medium of exchange, a unit of account or a store of value[11]

16. Other bodies and regulators have developed their own definitions which reflect this broad summary. For example, in its 2014 Opinion[12] on virtual currencies, the European Banking Authority identified the following essential characteristics which most virtual currencies would have:

    a digital representation of value, not issued by a central bank or a public authority, nor necessarily pegged to a fiat currency, but is used by natural or legal persons as a means of payment and can be transferred, stored or traded electronically without having the status of legal tender

10 The Working Group note, however, that the term "cryptoasset" can also be used to cover a wider group of digital assets than just virtual currencies.

11 This is a slightly wider definition than used in the 2015 Report (which adopted the FATF definition). As noted in the 2015 Report, the FATF definition is a useful working definition, but not exhaustive.

12 https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

17. More recent publications, often in the context of anti-money laundering and other regulatory consultations, have tended to adopt the term of "cryptoassets" and use variations of the following definition:

    A cryptographically secure, digital representation of value or contractual rights that can be transferred, stored, and traded electronically[13]

18. **Cryptography** refers to the use of encryption techniques to secure and verify transactions which take place on the relevant virtual currency distributed ledger. There are various cryptographic methods, the most commonly used of which is the Public and Private Key Pairing system used by Bitcoin.

19. A **private key** is a randomly generated (usually) 256-bit string represented as a series of numbers and letters. Private keys have encryption uses outside of virtual currencies, for example they are used as the key to sending and receiving encrypted email. A private key, by definition, is intended to remain private and should not be shared with anyone. Sharing of a private key creates a risk of theft or unauthorised transactions. The private key has a 1:1 relationship with its related public key.

20. A **public key** is also usually a 256-bit string of numbers and letters. The public key is mathematically derived from the private key but reverse engineering the private key from the public key is technically impossible for any current computer (although the imminent development of quantum computing has potential risks to current encryption techniques). The public key is used to ensure that you are the owner of any particular address that can receive funds on a virtual currency system.

21. A **wallet address** or just **address** is mathematically derived from the public key and is used to signify where virtual currency funds can be sent. If you are a person receiving virtual currency funds from a third party, you would provide the sender with your wallet address to tell them where to direct the funds.

22. A **wallet** (in the Bitcoin system) is a collection of a user's public and private keys, the address, as well as a record of transactions and user preferences.

23. **Fiat currency** refers to legal tender which is supported by the government which issued it (e.g. U.S. dollars), rather than being backed by a physical commodity (such as a gold coin).

24. **Coins**. A coin is a unit native to its own distributed ledger, e.g. Bitcoin is a unit native to the Bitcoin ledger; Ether is a unit native to the Ethereum ledger. The transfer of a digital coin from one party on the ledger to another is the way that value is transferred between participants. Digital coins are generally used in the same way as real world coins are – as money. The most limited form of digital coin does not serve any other purpose than to be used as money, i.e. a "cash only" coin to transfer money, as a store of value, or as a unit of, account (you can price goods or services in them).

25. However some digital coins have more features than just being useful as a form of money. Ether is used both as a unit of value but also to fuel transactions on the Ethereum network. Tokens (see below) can be built on Ethereum, but Ether is still required to send a token. In this context, Ether funds the mining costs, i.e.

13 See, for example, the UK FCA consultation on cryptoassets issued in January 2019 - https://www.fca.org.uk/publication/consultation/cp19-03.pdf

pays the computers that verify transactions on the Ethereum network. To make matters even more confusing, these types of coins are often referred to as "intrinsic tokens".

26. **Stablecoins** are a more recent virtual currency innovation. The value of a standard virtual currency Coin will move freely on its relevant market and is therefore subject to price gains/losses and risk of significant volatility. In contrast, Stablecoins are "price-stable cryptocurrencies" and are traditionally pegged to a stable central-bank-issued currency, often the US Dollar. This increased pricing stability means that Stablecoins may be more suitable for certain types of virtual currency application – particularly financial products or payment services. However, even within this more limited type of virtual currency, there can be significant variations in design[14].

27. The terms **Token** and **Coin** are often used interchangeably, but are often technically different. The word token can be used quite properly to describe both a digital representation of a real-world asset or something which can power interaction with a decentralised application which is built on top of a distributed ledger.

28. As a result, there are emerging token classifications –although there are no settled definitions. One useful summary is set out in the FINMA guidance[15] relating to classification of ICOs published in February 2018 as follows:

    - *Payment tokens (synonymous with cryptocurrencies) are tokens which are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Cryptocurrencies give rise to no claims on their issuer;*
    - *Utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure.*
    - *Asset tokens represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on the blockchain also fall into this category. This category of asset tokens can be broken down further into equity tokens and security tokens depending on the nature of the "promise" that is being made.*

    FINMA note that the individual token classifications are not mutually exclusive and that asset and utility tokens can also be classified as payment tokens (referred to as hybrid tokens). Other definitions which have gained currency during the period in which the Working Group met are "exchange token" which is a further way to describe cryptocurrencies/payment tokens and "security token" which a further way to describe asset tokens.

29. **ICOs** or Initial Coin Offerings also very much came into the public domain during the period where the Working Group was considering this report. An ICO is a fundraising mechanism in which new projects or business sell underlying crypto tokens or coins, normally in exchange for established virtual currencies such as Bitcoin. The funding is normally intended to be used to develop the project into a viable business. The crypto tokens or coins received at the initial fundraising

14 See the section on "What are stablecoins?" in the speech by Christopher Woolard of the FCA on 2 July 2019 - https://www.fca.org.uk/news/speeches/regulating-financial-innovation-going-behind-scenes

15 https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

stage can be for a variety of purposes – they can allow early access to the business when it is up and running at preferential rates, they can be exchanged for goods and services on the business when up and running or they can often be transferred or traded between investors (which has led to concerns around speculation in ICO tokens un referenced to the underlying business model). There have been instances of fraudulent ICOs[16] and the United States has been particularly active in taking enforcement action against such ICOs where regulators consider they are a violation of securities laws. South Korea and China also took action in 2017 to curtail domestic ICOs (although note that South Korea is reportedly considering a reversal of this action[17]). An ICO is distinguished from an Initial Public Offering (IPO) of shares in a company by, among other things, the nature of the asset purchased and the extensive regulatory framework that usually governs IPOs. A hybrid development of "Security Token Offering" (STO) may combine a security issued in the form of a virtual asset, which represents ownership rights in an underlying company and/or its assets. ICO activity peaked in January 2018, and funding using ICOs has since significantly reduced, almost certainly as a result of increasing regulatory scrutiny.

30. **Exchanges** are businesses which facilitate "real world" use of virtual currencies. For so long as virtual currencies are separate from fiat currencies, to the extent that any customer wants to trade or exchange their virtual currency for fiat currency or for a different virtual currency, they will likely need to use an exchange. Exchanges may match customers who wish to buy/sell virtual currencies (and charge a matching fee for that process) or they may act as a true exchange (and are remunerated from the bid/ask spread between the buy/sell aspects of any conversion). One of the largest early exchanges, Mt.Gox was subject to high profile trading incidents, allegations of fraud and criminal activity and was ultimately shut down. It is currently in the process of liquidation. Since then, many new entrants to the market have sought to develop business consistent with global regulatory requirements, including with a focus on compliance with global AML/CFT standards. While the majority of exchanges focus on fiat/crypto transactions, there are increasing numbers of exchanges which offer crypto/crypto capability (either alongside fiat/crypto transactions, or as a standalone business) as well as decentralized, peer to peer virtual currency exchanges which facilitate direct exchange transactions between users over an electronic platform.

16 Confido held an ICO for its "smart contracts", as a way of acting as an escrow between a buyer and a seller during a transaction. The plausible scheme attracted worldwide interest worldwide, before disappearing overnight. The firm who hosted the ICO, said the company had pulled an "exit scam", making off with the $375,000 of investment

17 https://www.coindesk.com/korean-national-assembly-makes-official-proposal-to-lift-ico-ban/

Reasons For Member Countries to Consider Regulation of Virtual Currencies

31. The 2015 Report highlighted the tension which exists in deciding whether to regulate virtual currencies, and if so how. Regulation can provide certainty to the market and promote positive uses of virtual currencies for the benefit of the general population. At the same time, regulation can deter start-ups and depress innovation and may simply not be necessary if there are no material volumes of virtual currency business in a particular country. At the same time, the Working Group recognises that there are increasing arguments in favour of some level of regulation for virtual currencies (in particular to minimise the risks associated with financial crime).

32. The Working Group remains of the view that there is no "one size fits all" approach to regulation of virtual currencies. This is particularly because Member Countries start from different legal perspectives – a country with a broadly drafted, non-prescriptive or outcomes-based system of financial regulation may well find that virtual currencies are already covered to an appropriate extent under its systems. In contrast, a country where the systems of financial regulation rely on precisely defined terms is unlikely to have existing laws which fully cover virtual currencies.

33. As a result, the Working Group consider the best approach is to focus on the specific issues relating to virtual currencies which may require regulation and the desired outcomes in each case, leaving the precise mechanism of regulation to be established on a country by country basis. At the same time, the Group considers it is helpful to look at the different regulatory approaches taken by various countries in this area, as useful guidance.

34. In this 2019 Report, the issues to consider/suggested outcomes are grouped into the following categories:

- Overarching Issues
- Criminal Activity (non-AML/CFT)
- Criminal Activity (AML/CFT)
- Taxation
- Financial Products (intersection with virtual currencies)
- Consumer Protection
- Social Benefits/Social Inclusion

Overarching Issues

Background

35. The Working Group considered a broad range of overarching issues relevant to the development, use and regulation of virtual currencies. Such issues represent the macro considerations that may be determined by government authorities such as tax authorities and central banks.

Virtual currencies as legal tender

36. The question of whether a virtual currency will be treated as legal tender is typically a national legal analysis. To date, the majority of countries who have made pronouncements or statements on this issue have determined that virtual currencies may **not** be treated as legal tender. This includes the UK, the EU, India, Singapore, Nigeria, China, South Korea and the United States. The most common rationale is that only a central bank can issue legal tender in the relevant jurisdiction.

37. There are two commonly reported exceptions to this approach – Japan and Switzerland. However, a closer examination of the responses of these two countries is instructive. In April 2017, Japan enacted the Payment Services Act which not only defined virtual currency in Japan[18] but also officially recognised the use of certain virtual currencies, such as Bitcoin, in Japan. This official recognition is some way short of treating virtual currencies as legal tender, notwithstanding a common media perception that it is the same thing. A key difference is that, if virtual currencies were treated as legal tender in Japan, business would be *obliged* to accept all recognized virtual currencies, whereas under the Payment Services Act, businesses have the ability, but not the obligation to accept the recognised virtual currencies.

38. In a similar way, in 2014 the Swiss Federal Council adopted a postulate to the effect that Bitcoins and other similar virtual coins could be treated as foreign currency within Switzerland (not national legal tender)[19]. This decision was seen to reduce legal uncertainty for virtual currencies users in Switzerland and also allowed the Swiss authorities to apply existing foreign currency legislation to Bitcoin and other digital currencies – again the effect of this decision appears to have been widely misunderstood within the general media as being akin to treating virtual currencies as if they were legal tender.

18 In Japan "virtual currency" is defined as a proprietary value that satisfies all of the following criteria: Between unspecified persons: (i) it can be used to settle payments for goods and/or services and exchanged with legal currency; or (ii) it can be exchanged with another virtual currency.
- It can be transferred using an electronic data processing system.
- It is not denominated in Japanese Yen or any foreign legal currency.

19 https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20134070

National financial stability

39. In March 2018, the chairman of the Financial Stability Board (FSB)[20] published a summary of issues arising out of crypto-assets[21]. In particular the FSB's initial assessment was that crypto-assets do not pose risks to global financial stability:

    The FSB's initial assessment is that crypto-assets do not pose risks to global financial stability at this time. This is in part because they are small relative to the financial system. Even at their recent peak, their combined global market value was less than 1% of global GDP. In comparison, just prior to the global financial crisis, the notional value of credit default swaps was 100% of global GDP. Their small size, and the fact that they are not substitutes for currency and with very limited use for real economy and financial transactions, has meant the linkages to the rest of the financial system are limited.

    The market continues to evolve rapidly, however, and this initial assessment could change if crypto-assets were to become significantly more widely used or interconnected with the core of the regulated financial system.

    ...

    Crypto-assets raise a host of issues around consumer and investor protection, as well as their use to shield illicit activity and for money laundering and terrorist financing. At the same time, the technologies underlying them have the potential to improve the efficiency and inclusiveness of both the financial system and the economy.

    Relevant national authorities have begun to address these issues. Given the global nature of these markets, further international coordination is warranted, supported by international organisations such as CPMI, FATF and IOSCO.

40. The FSB Chair concluded that the FSB would seek to identify metrics for enhanced monitoring of the financial stability risks posed by crypto-assets and update the G20 as appropriate.

41. At the same time, the FSB has acknowledged in other reports that fintech innovations, including fintech credit, can have both positive and negative impacts on national financial stability[22]. To the extent that any country's national financial markets are heavily impacted by virtual currencies (or materially exposed to businesses such as exchanges which deal in virtual currencies or where virtual currencies are commonly accepted in exchange for goods and services) that country will need to consider the risks to its consumers and its national financial stability in determining its overall regulatory approach.

42. This initial summary by the FSB was confirmed in July 2018, by the publication of its longer report[23] on crypto-assets. In that report, the FSB repeated its view that crypto-assets (including virtual currencies) do not pose a material risk to global financial stability at this time; however it recognised the need to continue to monitor this issue. Importantly, the FSB report sets out its preferred framework for monitoring the financial stability implications of the

20 The Financial Stability Board is an international body that monitors and makes recommendations regarding the global financial system. It includes all G20 major economies, Financial Stability Forum members and the European Commission.
21 http://www.fsb.org/wp-content/uploads/P180318.pdf
22 http://www.fsb.org/wp-content/uploads/CGFS-FSB-Report-on-FinTech-Credit.pdf
23 http://www.fsb.org/wp-content/uploads/P160718-1.pdf

developments in crypto-asset markets and the metrics that the FSB will use to monitor developments in crypto-asset markets as part of the its ongoing assessment of vulnerabilities in the financial system.

Role of the Central Bank

43. At one level, a central bank has no obvious role to play in the creation, maintenance and regulation of a virtual currency. By some current definitions (such as the FATF and EBA definitions) a virtual currency must be unsupported by a central bank. However, various countries have begun the process of exploring the creation of a national virtual currency reflecting that country's fiat currency. Estonia has explored ways to create Estcoin, following an initiative on the blockchain-based residency registration called e-Residency[24]. Lebanon's central bank is reported to have started examining the possibility of creating a virtual currency[25] and other members of the Working Group have been approached by start-ups in their own countries with requests to consider a digital fiat currency[26]. There are examples of private companies launching digitised versions of local currency (for example Bitt has a project issuing digital Barbadian dollars, Aruban florins and Bahamian dollars with a certain level of local central bank support[27], but this is some way off an actual central bank issuance of a digital currency). However, on 14 November, 2018 the Managing Director of the IMF drew attention to an IMF Staff Discussion Note which set out a conceptual framework to assess the case for central bank digital currency adoption.[28] Most recently a senior official at the People's Bank of China is reported to have confirmed that it will shortly launch a state-backed digital version of the renminbi, using a small group of trusted institutions to distribute it to Chinese citizens.[29]

44. At the same time, global organisations such as BIS have warned about some of the risks associated with central bank virtual currencies[30]. One specific, systemic financial stability risk identified by BIS is the risk of a "digital run" from private banks to the state in terms of financial stress.

    Arguably, the most significant and plausible financial stability risk of a general purpose CBDC [Central Bank Digital Currency] *is that it can facilitate a flight away from private financial institutions and markets towards the central bank. Faced with systemic financial stress, households and other agents in both advanced and emerging market economies tend to suddenly shift their deposits towards financial institutions perceived to be safer and/or into government securities. Of course, agents could always flee towards the central bank by holding more cash. But a CBDC could allow for "digital runs" towards the central bank with unprecedented speed and scale. Even in the presence of deposit insurance, the stability of retail funding could weaken because a risk-free CBDC provides a very safe alternative.*

24 https://www.worldfinance.com/markets/estonia-pushes-ahead-in-race-to-issue-first-state-backed-crypto currency
25 http://www.dailystar.com.lb/Business/Local/2017/Oct-27/424064-salameh-central-bank-to-launch-digital-currency.ashx
26 http://www.afr.com/business/banking-and-finance/financial-services/a-digital-australian-dollar-making-the-case-20171027-gz9hai
27 https://www.coindesk.com/how-a-tiny-island-could-give-cryptocurrency-a-big-boost/
28 https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233
29 https://www.forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/
30 https://www.bis.org/cpmi/publ/d174.pdf

45. The same BIS report also recognised the possible advantages of a wholesale-only CBDC, i.e. a digital currency which could only be used by wholesale participants, i.e. something comparable to traditional central bank reserves. When a wholesale-only CBDC can be used in an interbank payment system it will potentially improve efficiency and risk management in settlement and if complemented by direct participation of non-banks in the settlement process, there can be further gains through the use of new technologies for asset transfers, authentication, record-keeping, data management and risk management.

    Payments and (cash legs of) securities transactions settled in CBDC, instead of through facilities hosted by commercial banks or other service providers, could help reduce counterparty credit and liquidity risks in the financial system. It could also help central banks monitor financial activity.

46. In the period since the Working Group met to discuss and finalise its views set out in this Report, the US-based social media company Facebook has announced its proposed virtual currency Libra. While the currency and network do not yet exist, several high profile organisations such as Visa and MasterCard are reported to be partnering with Facebook on the project. Many of the concerns raised by BIS have been echoed by regulators and governments in respect of Libra, with particular concerns expressed around user privacy, the impact on sovereign monetary policy as well as the ability of countries to use monetary policy levers to manage their particular economic circumstances, if Libra becomes a highly adopted method of money transfer and payment. A specific discussion of Libra is beyond the scope of this Report, but many of the points and issues discussed below will be relevant to the potential impact of this technology in Member Countries.

Complete or partial regulation of virtual currencies

47. There is no single, commonly emerging global model for regulation of virtual currencies. Several countries have publicly concluded that – so far - there is no current need to bring in new regulation to address the overarching issues relating to virtual currencies and that they can rely on existing regulation to address the other issues discussed in this Paper, such as anti-money laundering/counter-terrorism financing.

48. At the other end of the scale, some countries have taken steps to substantially prohibit all use of virtual currencies, including for reasons of financial stability. In December 2017, Algeria introduced a law prohibiting "*The purchase, sale, use, and holding of so-called virtual currency*" within the country[31]. Other countries with substantial bans on the use of virtual currencies (or specific virtual currencies/use for specific purposes) include Bangladesh, Bolivia, Ecuador, Indonesia and Macedonia.

49. Many more countries are said to be considering some form of regulation of virtual currencies, with FATF noting in a recent report that at least 11 G20 members are preparing relevant laws or regulations[32]. The Working Group has

31 https://www.mfdgi.gov.dz/images/pdf/lois_de_finances/LF2018F.pdf - the approximate English translation of Article 117 is:

Art. 117. - The purchase, sale, use and possession of the so-called virtual currency is prohibited. The virtual currency is the one used by Internet users through the web. It is characterized by the lack of physical support such as coins, tickets, payments by check or credit card. Any violation of this provision, is punished in accordance with the laws and regulations in force.

32 Brazil, Canada, EU, Mexico, Netherlands, Russia, Saudi Arabia, South Korea, Spain, Turkey, UK

seen evidence of countries developing a balanced approach to regulation of virtual currencies, for example taking specific action to prevent certain uses of virtual currency where there is evidence they cause harm or have poor consumer outcomes.[33]

50. The Working Group also noted that the majority of existing regulatory regimes for virtual currencies focus on the interaction between fiat currencies and virtual currencies and often do not attach to "crypto to crypto" type transactions. This issue is discussed further below.

Options to address overarching issues using existing regulatory models

51. The Working Group considered three broad regulatory models which are in use, or being considered, in various countries, including their potential advantages and disadvantages. The Working Group concluded that these regulatory models are all capable of responding to the overarching issues and other issues highlighted in this Report:

- the licensing model;
- the restrictive model;
- the permissive/guidance model.

Licensing model

52. As the name suggests, the licensing model requires activities relating to virtual currencies to be subject to home country and/or country of operation licensing requirements. In order to carry out the relevant activities in that country, it is necessary to first obtain a relevant licence from an authority, often from a financial services regulator. The licensing process typically involves an application form, diligence on the business owners and key personnel, meetings and interviews with the regulator to discuss the business and material consideration of the businesses' financial resources and compliance systems. The grant of any licence is normally subject to supervisory, reporting and auditing powers for the relevant authority.

53. One of the most well-known licensing regimes is the New York BitLicense[34]. Enacted in 2015, the New York Department of Financial Services (DFS) enacted the BitLicense regulatory framework, which states it covers "virtual currency business activity" to the extent it touches New York or its residents. Any business engaging in "*virtual currency business activity*" involving New York State or persons that reside, are located, have a place of business, or are conducting business in New York are required to apply for the BitLicense, with no grace periods or de minimis exceptions.

54. Various issues have been identified with the particular form of the New York BitLicense (perhaps unsurprising as a first mover in this area and with the regulation being enacted at speed). The broad language used in the regulation has raised concerns about the precise scope of activities which are intended to be captured by the licensing regime with some requirements that appear aimed

33 See for example the UK FCA proposed prohibition on the sale to retail clients of investment products that reference cryptoassets - https://www.fca.org.uk/publication/consultation/cp19-22.pdf

34 https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

at only financial institutions and others which could be intended to apply to sole traders or small businesses who agree to accept virtual currencies for goods or services.

55. At the same time the licensing process is seen as arduous and imposing significant operational burdens more akin to requirements for a large scale financial institution. So far, only four businesses have received BitLicenses that the Working Group is aware of (plus two companies who received a different kind of limited authorisation in New York as trust charters). It has been reported that virtual currency businesses have moved from New York as a result of the imposition of the licence, and some businesses now decline to offer services to residents of New York from outside the state because of their lack of BitLicense. There have been recent calls from US Senators to reform the BitLicense and make it more user-friendly.

56. A more recent example of the Licensing Model which bears closer examination is the Gibraltarian DLT Framework[35]. This DLT Framework requires any firm "*carrying out by way of business, in or from Gibraltar, the use of distributed ledger technology (DLT) for storing or transmitting value belonging to others (DLT activities)*" to be authorised by the Gibraltar Financial Services Commission as a DLT Provider. Importantly the framework which underpins this licensing model is outcomes and principles based, given a significant level of flexibility to the regulator in deciding whether to grant a licence. Although the scope of the requirement is broad, it does not attach to (for example) businesses who wish to take virtual currency as payments for goods and services, nor to business that already have financial permissions to operate in Gibraltar. We discuss the principles underpinning the Gibraltarian DLT Framework further under the permissive model (the approach taken by Gibraltar is effectively a hybrid licensing/permissive model).

57. There are other, narrower licensing models. An increasingly common approach is to require exchanges to be licenced to ensure compliance with certain local financial laws and regulations, including AML, but other activities relating to virtual currencies do not require licences – Japan and the Philippines use this model, as does Australia.

58. The Australian model is based around a registration obligation[36] which requires any digital currency exchange to register with AUSTRAC (Australia's financial intelligence agency and anti-money laundering and counter-terrorism financing (AML/CFT) regulator) as well as:

    - adopt and maintain an AML/CFT program that mitigates and manages the exchange's business's money laundering and terrorism financing risks;
    - report suspicious matters and threshold transactions to AUSTRAC;
    - keep records relating to customer identification, transactions and the exchange's AML/CFT program.

59. Other features of the Australian model include a clear transitional period for registration and compliance with the AML/CFT obligations, as well as government issued policy principles setting out when enforcement can take place against exchanges during the introductory period of the new regulations[37].

35 http://www.gfsc.gi/dlt
36 http://www.austrac.gov.au/digital-currency-exchange-providers
37 http://www.austrac.gov.au/sites/default/files/signed-policy-principles-030418.pdf

60. Members of the Working Group also reviewed other, publicly available examples of model regulatory frameworks based on a licensing regime[38].

Advantages	Disadvantages
A well drafted licensing regime gives certainty to the market and to users as to what is permitted within country.	Any licensing or registration requirement will be a deterrent to many start-ups who lack the funds and resources to comply with substantial compliance requirements. This may have an impact on innovation.
It can attract businesses involved in virtual currencies to the country.	It could also lead to reduction in virtual currency business within the country and less choices for the consumer.
It gives oversight for regulators into virtual currency businesses, allows them to impose requirements to protect consumers and potentially intervene where consumers are at risk or financial stability is in question.	An overall broad, restrictive or burdensome licensing regime is likely to damage virtual currency and broader fintech activity in the country.
The scope of any licence can be adjusted to suit the needs of the particular country including a "regulatory light touch" approach in the early stages of the technology	It will also be important for countries to consider interaction with existing laws, in particular money transmission laws to avoid inconsistent licensing requirements across businesses and sectors.

Restrictive model

61. The restrictive model, as its name suggests, is where regulation prohibits some or all activities relating to virtual currencies. The substantial bans mentioned at paragraph 45 are examples of the restrictive model. In the same way as the licensing model, it is possible to restrict only certain activities.

62. In September 2017, China announced it would shut down all domestic virtual currency exchanges. This announcement was followed in early 2018, by a Chinese ban on domestic access to virtual currency platforms and exchanges located outside the PRC (although this action needs to be considered in the context of the recent reports that China is planning to launch its own state-backed virtual currency). The South Korean Ministry of Justice considered banning Bitcoin and other virtual currencies, but this was later clarified as being an immediate restriction on anonymous virtual currency trading and a reminder that any exchanges must comply with foreign exchange rules and money laundering activities, with the possibility of a ban in the future, if these measures were not effective to prevent bad practices in the South Korean virtual currency market.

63. The Working Group considered the advantages and disadvantages of adopting a restrictive model.

38 https://www.csbs.org/sites/default/files/2017-11/CSBS%20Draft%20Model%20Regulatory%20Framework%20for%20Virtual%20Currency%20Proposal%20--%20Dec.%2016%202014.pdf

Advantages	Disadvantages
The restrictive model should give a clear delineation of what is permitted and what is not permitted in any country. This certainty may well encourage business in areas that are clearly outside the scope of the restrictions.	It is likely to stifle innovation and prevent the development of good market standards and conduct within the country. Will decrease country reputation as leader in fintech/DLT. May drive activity underground and also increase the risk of criminal use of virtual currencies outside of national law enforcement access.

Permissive/guidance model

64. The permissive/guidance model sets out (whether by way of formal regulation or guidance) the scope of virtual currency activities that are permitted within the country. Often the permissive model will be based around overarching principles or outcomes that must be achieved in order for the activity to remain permitted. A good example is the Gibraltar DLT Framework (albeit that this framework is combined with a licensing requirement as noted above). The Gibraltar DLT Framework[39] is based around the following principles:

    A DLT Provider must conduct its business with honesty and integrity.

    A DLT Provider must pay due regard to the interests and needs of each and all its customers and must communicate with its customers in a way which is fair, clear and not misleading.

    A DLT Provider must maintain adequate financial and non-financial resources.

    A DLT Provider must manage and control its business effectively, and conduct its business with due skill, care and diligence; including having proper regard to risks to its business and customers.

    A DLT Provider must have effective arrangements in place for the protection of client assets and money when it is responsible for them.

    A DLT Provider must have effective corporate governance arrangements.

    A DLT Provider must ensure that all systems and security access protocols are maintained to appropriate high standards.

    A DLT Provider must have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing.

    A DLT Provider must be resilient and must develop contingency plans for the orderly and solvent wind down of its business.

    Each principle is accompanied by more detailed guidance setting out how the outcome will be achieved.

65. Another, more limited, example is the UK Financial Conduct Authority guidance published in September 2017 on the risks of ICOs for consumers[40]. This publication provided some limited guidance to businesses as to when their activities might fall within the existing UK regulatory regime, in particular the

39 http://www.gfsc.gi/dlt
40 https://www.fca.org.uk/news/statements/initial-coin-offerings

regulated activities of arranging, dealing or advising on regulated financial investments. It should be noted that the FCA's approach has developed since September 2017, with further publications on cryptoasset regulation[41].

66. The Working Group noted that the permissive regime provides some flexibility to market participants but that enforcement can be challenging.

Advantages	Disadvantages
The permissive regime gives market participants flexibility as to how they comply, providing they meet all required outcomes. This potentially increases innovation in this area. **No state or regulatory resources are strictly required to allow businesses to operate (however, investigation and enforcement resources would still be required).**	Enforcement under the permissive regime can be difficult, particularly if the requirements have been breached by an entity operating outside the country. Clear drafting is required to avoid confusion (or arbitrage) as to how principles and outcomes must be achieved and lack of clarity may deter legitimate businesses from operating in any "grey" areas where there is a risk of enforcement. It will also be important for countries to consider interaction with existing laws, in particular money transmission laws, to avoid inconsistent requirements across businesses and sectors.

Conclusions

67. When considering an overall approach to potential regulation of virtual currencies, the Working Group concluded the most effective approach is for each Member Country to focus on the specific issues relating to virtual currencies which may require regulation in their jurisdiction, the desired outcomes in each case, and then to adopt a mechanism of regulation, if required. There was recognition within the group that different countries have different needs and different opportunities from virtual currencies and that there is no "one size fits all model". This risk-based approach is similar to the approach suggested by FATF in its 2015 Report on virtual currencies and financial crime, but the Working Group concluded it was likely to be helpful for Member Countries to consider virtual currencies more broadly, and not initially limit their focus to specific issues such as anti-money laundering or crime prevention.

68. Representatives attending the Working Group meetings indicated that some Member Countries have produced overall assessments which consider both the benefits and risks arising from virtual currencies in that country. Where risks were identified, it was often the case that more detailed risk assessments would then be produced, which focused on the specific issues identified. The Working Group was not aware that any of these overarching risk assessments had been published but there was general agreement that it was a helpful step for Member Countries to take. The expected benefit of producing an overall benefit/risk assessment was that Member Countries could take a fully joined-up approach to virtual currencies and avoid the risk of a piecemeal approach with unintended consequences and/or inconsistent laws.

41 https://www.fca.org.uk/publication/consultation/cp19-03.pdf

69. It was also suggested that producing a country-specific, overall benefits/risk assessment and sharing that information with neighbouring countries or major trading partners may allow easier establishment of mutual, cross-border arrangements in respect of virtual currencies and so enhance the likely benefits of the technology. The Working Group discussed the example of the UK-Australia FinTech Bridge[42] and have since considered the broader efforts to form a Global Financial Innovation Network by eleven major national financial regulators (including certain Member Countries)[43]. It was noted that co-operative efforts to establish mutual cross-border efforts in areas such as payments, authorisation to conduct business as well as sharing information on financial crime, could speed up the adoption of new technologies and give groups of neighbouring countries a trading and business advantage which they would not have as a sole jurisdiction. The focus of any such cross-border effort should be on reducing barriers to entry for businesses and applications of virtual currency technology which are of mutual benefit.

70. At the same time, there was recognition within the Working Group that all countries are likely to be at risk of financial crime arising from use of virtual currencies within their borders, and that the 2015 FATF guidance for a risk-based approach to virtual currencies was an expected minimum starting point. There was a strong consensus within the Working Group that the appropriate first point of regulation to deal with risks relating to virtual currencies is the intersection between virtual currencies and fiat currency in any country, i.e. virtual currency exchanges, consistent with the 2015 FATF Guidance (subsequently updated in June 2019). The Working Group also recognised that "crypto to crypto" points of intersection could become increasingly important avenues for financial crime in future and should remain a focus, but subsequent to an effective approach being in place for fiat to virtual currency transactions.

71. The Working Group also considered whether it was appropriate to recommend additional measures in respect of virtual currency exchanges, such as a requirement for registration or licensing of exchanges. The experience shared with the Working Group by Member Countries who had put similar measures in place was positive, with three particular benefits being identified:

    Enhanced transparency – Registration or licensing provided enhanced transparency for customers, including where any exchange was located, the principals or owners of exchanges and any policies or procedures in place to protect customers. Mandatory provision of information, registration or licensing also provided enhanced transparency for regulators, in particular identifying exchanges which engaged with regulators and complied with the requirements made it easier to identify potential "bad actors" operating within a Member Country;

    Information gathering - for Member Countries who did not already have a complete picture of virtual currency exchange activity taking place within their borders, requiring provision of information[44], registration or licensing was helpful to understanding where activities were taking place, and particularly if exchange activity was taking place as ancillary activity to another type of business. The information gathered has multiple uses for developing an overall understanding of the sector and any risks specific to that Member Country;

42 https://treasury.gov.au/fintech/uk-australia-fintech-bridge/
43 https://www.fca.org.uk/publication/consultation/gfin-consultation-document.pdf
44 A detailed example of an information gathering questionnaire from a U.S. regulator can be seen at https://ag.ny.gov/sites/default/files/virtual_markets_integrity_initiative_questionnaire.pdf

Driving higher standards - Member Countries noted the potential benefits of starting with lighter set of measures (e.g. simple registration rather than an extended, pro-active licensing regime) and using information gained from this process to drive better standards in the market and develop more targeted measures over time.

72. The Working Group recognised there were limits to this approach, in particular the cross-border nature of virtual currencies, customers' ability to access exchanges across borders and the difficulties of enforcement activity against an exchange located in a third country, but overall the Working Group concluded that Member Countries should now consider authorising virtual currency exchanges which operate within their jurisdiction (for example by way of registration or under a proportionate licensing regime).

73. Alongside compliance with AML and CFT legislation, the Working Group discussed the importance of "identity" and "identification" when developing systems of regulation to help Member Countries benefit from virtual currencies, as well as manage their risks. Issues of identity, particularly for financial transactions, are not unique to virtual currencies but were a recurring theme of the Working Group discussions. Distributed ledger technologies also have a significant potential to support other initiatives such as the UN's Sustainable Development Goals[45] and ID2020, the global partnership committed to improving people's lives though digital identity. These broader issues are considered at a high level in the section on Social Inclusion below.

RECOMMENDATIONS – OVERARCHING ISSUES	
1.	Member Countries are encouraged to produce and maintain an overall assessment which: • considers the benefits and risks of virtual currencies in that Member Country; • has regard to the areas and matters in this 2019 Report.
2.	Member Countries should have regard to this overall assessment when considering activities or actions relating to virtual currencies.
3.	Member Countries are encouraged to focus their regulatory efforts on the intersections between virtual currencies and fiat currencies – in particular, Member Countries should consider authorising virtual currency exchanges that operate within their jurisdiction (for example, by way of registration or under a licensing regime). The Working Group noted the potential increase in exchanges of virtual currency for virtual currency ("crypto-to-crypto"), but considered this was a lower immediate priority than exchange of virtual to fiat currency.
4.	Member Countries are encouraged to consider using existing or establishing mutual, cross-border technical or working arrangements, with the aim that entities conducting virtual currency activities which are authorised in one Member Country can apply to be authorised more easily and quickly in other jurisdictions.

45 In particular, SDG 16.9, the provision of legal identity for all including free birth registrations by 2030.

Criminal Activity (Non AML/CFT)

74. The Working Group considered a detailed presentation by the representatives from Singapore on the general impact of virtual currencies in criminal activity. The presentation focused on both legal/legislative issues and investigation issues but broadly categorised the issues as follows:

    - dealing with crimes involving virtual currencies;
    - securing evidence relating to virtual currencies in the context of criminal investigations; and
    - seizure and storage of virtual currencies (whether as the subject of the crime or the proceeds of a crime).

Legislative issues

75. A significant part of the Working Group's discussion focused on crimes where virtual currencies are the instrumentality or subject matter of the crime. The majority of public/global discussion has tended to focus on crimes where virtual currencies are used to launder the proceeds of the crime (see next section), and not every country has been able to have the same level of focus on crimes where virtual currencies are the subject matter of the crime (typically crimes involving theft of virtual currencies).

76. As the prevalence of virtual currencies increases globally, including increases in related crimes/criminal activity, it is likely that many countries will need to review and update their criminal legislation to properly allow for crimes involving virtual currencies. This is particularly where the relevant criminal offences are based on concepts of "property" which may or may not expressly or impliedly extend to virtual currencies. Working Group members noted it was common for countries to have a "patchwork" of criminal legislation with both defined and undefined terms of what kinds of property could be the subject of such a crime. It was not always clear if virtual currencies would be considered as relevant property and therefore within the scope of any particular criminal offence such as theft. In extreme cases, where a country's criminal legislation used specific definitions linked (for example) to "moveable property" or "things in action" but did not extend to intangible or incorporeal property, there was a risk that a significant theft of virtual currency or fraud involving virtual currency could not easily be prosecuted in the same way as if the offence had been committed in respect of fiat currency.

77. The particular features of virtual currencies which make them "high risk" for theft-type crimes include the relative ease with which currencies can be transferred including across borders, the potential difficulty of tracing stolen virtual currency assets, and the relative lack of experience that police and other investigatory forces may have in dealing with theft of such assets. Complex obfuscation techniques, such as the use of virtual currency mixers or tumblers, and their combination with dark web technology, can also make this especially challenging.

78. The Working Group discussed various approaches which could be used to make the necessary legislative updates, including piecemeal amendment of existing legislation, introduction of specific legislation relating to crimes involving virtual currencies or developing more general legislation relating to crimes involving digital assets/incorporeal property, which would cover a broader range of assets up to and including air miles, credit card points etc. It was recognised that different countries with different legal systems would need to take different approaches, but that an overall recommendation to carry out such a review was appropriate.

Investigative issues

79. The Working Group discussed the practical issues that can arise for police/investigatory authorities when investigating crimes involving virtual currencies (both where the virtual currency is the subject matter of the crime and where it represents the profits or vehicle by which the profits of the crime are laundered). In particular, it was clear that investigators needed to understand how to identify and evidence use of virtual currencies in criminal activity.

80. To effectively combat crimes involving virtual currencies, investigators need to be sensitised to the particular features of virtual currencies which will be relevant to their investigations. This will normally include consideration of at least the following issues within national police forces:

    - developing a wide understanding of what virtual currencies are;
    - helping investigators understand what to look for to establish whether and how virtual currencies are involved in any particular crime;
    - ensuring there is a clear procedure to follow when virtual currencies are involved, including securing relevant evidence and appropriate exercise of police powers;
    - understanding the risks around preserving the integrity of evidence when dealing with virtual currencies as part of an investigation;
    - understanding what tools are available to trace transactions involving virtual currencies.

81. A key issue for investigators is how to efficiently secure the private key (or equivalent) that may be needed to preserve the virtual currency and related evidence (such as the date when any amount of virtual currency was purchased, transferred into a particular wallet, transferred out of any particular wallet and to which address or entity such transfers took place). Investigators also need to be familiar with the different types of wallet which can be used to store virtual currencies, including the fact that they come in both hardware and software forms and can be stored on practically any type of electronic or networked device, including USB keys.

82. The members of the Working Group with experience of criminal investigations considered that most Member Countries would already have adequate powers to require suspects to disclose information and to seize relevant evidence that would be necessary to support an investigation involving virtual currencies. However, it is essential that investigators have a good understanding of the particular questions that need to be asked in order to ascertain if virtual currencies are involved and, if so, to ascertain the form of wallet and key (as well as the ownership of the wallet and key) so as to gain access and secure

the relevant evidence. Member Countries should be encouraged to develop effective operating procedures and provide training to investigators and prosecutors on offences involving virtual currencies.

83. The Working Group also discussed the importance of liaising with third parties who can assist with following the "currency" trail in the context of investigations involving virtual currencies, particularly virtual currency exchanges and online blockchain explorers, both of which can provide vital information about particular transactions which are the subject of criminal investigations.

Seizure/securing virtual currencies

84. It is another unusual feature of virtual currencies that mere acquisition of the wallet, private key or other passphrase by investigators does not mean that the underlying virtual currency has been successfully secured and is no longer accessible by others. To the extent that any accomplice has the private key, they may be able to recreate the wallet and remotely move the virtual currency to another wallet or address.

85. True "seizure" of virtual currencies requires use of either a replacement wallet under the control of the investigating officers or third party storage solutions. Even these solutions introduce new risks into the safe storage process with the possibility of malpractice by investigating staff and the loss of access to the virtual currency if the relevant private keys are not stored safely and able to recalled easily. In the same way that Member Countries have developed processes for engaging with third party financial institutions to deliver up money and other property to investigating officers or to "freeze" assets, it is important to develop similar processes for dealing with virtual currency so as to ensure the full chain of evidence is preserved along with the assets during the period of any investigation.

86. It may well be that the virtual currencies need to be returned either to victims or the suspects following the termination of any investigation. The Working Group noted the particular risks that can apply when substantial amounts of virtual currencies are seized or frozen, particularly when there are large fluctuations in value during the period of the investigation. It may be appropriate in particular cases for investigators to seek prosecutorial and court support to cash out virtual currencies into conventional currency to guard against the risk of loss of value and consequent loss of gains).

RECOMMENDATIONS – CRIMINAL ACTIVITY (NON AML/CFT)	
5.	Member Countries are encouraged to review the application of their criminal legislation to offences where virtual currencies are the instrumentality or subject matter of the crime. The scope of traditional "property" offences such as theft, fraud, cheating etc. may need to be expanded to include virtual currencies.
6.	Member Countries are encouraged to ensure that their law enforcement agencies have effective operating procedures and training for the investigation of offences involving virtual currencies.
7.	Member Countries are encouraged to review their laws of criminal procedure and powers of law enforcement agencies to access, seize, manage and dispose of virtual currencies.
8.	Member Countries are encouraged to provide training relating to virtual currencies for their judiciary and prosecuting authorities.

Criminal Activity – AML/CFT

87. Within the scope of "AML" the Working Group considered a broad range of regulations relating to the financing of terrorism, the transmission of proceeds of crime and all similar regulations.

88. As noted in the 2015 Report, the potential uses of virtual currency to support criminal activity are extensive. Illegal or illicit goods can be purchased using virtual currency on so-called "dark web" internet sites such as Silk Road. Although Silk Road was shut down in 2013 and 2014 (and finally went offline in 2017), other sites such as AlphaBay and Hansa sprang up in its place. Those sites have also since been shut down but authorities have referred to their efforts as "whack-a-mole" in the sense that there is a constant pressure to identify new sites on the dark web which are acting as vehicles for criminal activity powered by virtual currencies.

89. Virtual currencies are used to facilitate other criminal activity – for example ransomware attacks on businesses and organisations are normally accompanied with a demand for a ransom payment in virtual currency. The perception of a lack of traceability of virtual currencies compared to fiat currencies in bank accounts is a barrier to law enforcement in tracking the perpetrators of this kind of criminal activity.

90. The very decentralised nature of popular virtual currencies such as Bitcoin, where parties trade anonymously with each other without knowing the other's identity also raises substantial AML issues, even where no criminal activity is known to be taking place. Regulated businesses (often those in the financial sector) are required to take steps to identify their customers and often to establish their sources of funds, both of which are difficult to do when the customers and funds are related to virtual currencies.

91. While law enforcement officers have developed tools and techniques to interrogate distributed ledgers for patterns of transactions and then to tie those transactions to individuals or businesses at the point where the virtual currency is exchanges for fiat currency[46], the effort required is extensive and technical solutions are being created to make this sort of analysis even harder.

92. For example, Monero[47] is a virtual currency which purports to offer complete anonymity to its users. Monero's central premise is that it cannot be traced, its transactions cannot be recorded centrally and its systems have inbuilt obfuscation.

93. The 2015 Report recommended that 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. As can be seen from the discussion of the licensing model and the permissive model, compliance with AML laws is a key part of the current available models for regulation of virtual currencies.

46 www.reuters.com/article/us-netherlands-crime-bitcoin/dutch-arrest-10-men-suspected-of-using-bitcoin-to-launder-money-idUSKCN0UY0V8.

47 https://www.coindesk.com/what-to-know-before-trading-monero/

New legislation (or amendment of existing legislation)

94. In the EU, the introduction of the 5th Money Laundering Directive in April 2018, requires EU member states to introduce laws which require the monitoring of transactions through virtual currencies. Under the new EU rules, Member States are obliged to include virtual currency exchange platforms and custodian wallet providers within the scope of the their money laundering rules. Prior to this virtual currency transfers were not generally monitored by public authorities within the EU (although countries with more extensive AML regimes such as the UK, did require proactive reporting where an exchange or transferor had reasonable grounds to suspect they were engaged in or involved in money laundering, or where the relevant exchange also held other regulatory permissions such as an e-money licence). Virtual currency exchanges and wallet providers will therefore be obliged to implement preventive measures and report suspicious transactions. This is expected to equip Financial Intelligence Units (FIUs) to collect the necessary information to assess suspicious transaction reports more efficiently and speed up detection of terrorist financing and money laundering activities. It is notable that certain EU countries have taken the opportunity of implementing the 5th Money Laundering Directive to introduce (or consider introducing) additional legislation relating to virtual currencies or distributed ledger technology, including the UK, France and Germany.

95. Jersey and the Isle of Man have made similar amendments to existing AML legislation to specifically bring virtual currency exchanges within the remit of core financial AML requirements.

96. Other countries, such as Australia, have combined the amendment of existing legislation[48] with new requirements such as an obligation on virtual currency exchanges to register with AUSTRAC (the Australian Transaction Reports and Analysis Centre). From 3 April 2018, any business providing digital currency exchange services in Australia is regulated under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CFT Act). This requires any affected business to:

    - enrol and register its business with AUSTRAC;
    - adopt and maintain an AML/CFT program that reflects the business' operations;
    - report suspicious matters and threshold transactions to AUSTRAC
    - keep records relating to customer identification, transactions, and its AML/CFT program.

97. AUSTRAC issued an interesting clarification on 12 April 2018, noting that "*the registration by AUSTRAC of a digital currency exchange or remittance service provider does not constitute an endorsement of that business or compliance with any anti-money laundering and counter-terrorism financing (AML/CFT) obligations.*"

48 By way of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 amending the Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Use of existing legislation

98. Other countries have not needed to amend their existing legislation to bring exchanges and other digital currency providers within scope of national AML laws. In the US, in 2014, FinCEN issued two advisory rulings declaring that FinCEN considered that a virtual currency exchange platforms and a virtual currency payment processor were "money transmitters" within the US rules. In practical terms, many virtual currency businesses that previously have argued that they are exempt from FinCEN regulations then to register as money transmitters, implement an anti-money laundering program, and comply with other reporting and recordkeeping requirements under the Bank Secrecy Act. This had the effect of requiring such platforms and providers to register with FinCEN and comply with AML requirements. In 2015, FinCEN fined Ripple Lab (incorporated in Delaware and headquartered in California) $700,000 for failing to register as a money service business with FinCEN[49]. FinCEN has taken further action in 2017 against a non-US located money service business, BTC-e, including a fine of $110,000,000 (although the allegations there included wilful violation of US anti-money laundering laws within the US)[50]

99. The Working Group considered the current work being done by FATF (and the expected additional reporting by FATF in this area which has taken place since the Working Group met) and concluded that the FATF Guidance remained the benchmark for AML/CFT issues involving virtual currencies which all Member Countries should be encouraged to implement.

100. The Working Group also noted the efforts of some Member Countries such as Australia to bring virtual currency exchanges within the scope of enhanced AML/CFT obligations and require them to make reports of suspicious activity on a mandatory basis. The Working Group felt this model of focusing AML/CFT requirements on the intersection between fiat currency and virtual currencies in the form of virtual currency exchanges, payment processors and related platforms was likely to be the most appropriate approach for many Member Countries to take. Feedback from members of the Working Group suggested that anecdotal evidence was that this approach was effective in improving AML/CFT compliance and driving good behaviour in the market.

101. Although other groups such as FATF are already actively considering these issues, the Working Group felt the following recommendations reflected the experience of the broad range of Member Countries as to what steps were helpful in practice to managing AML/CFT risks across the Commonwealth.

49 https://www.fincen.gov/sites/default/files/shared/Ripple_Facts.pdf

50 https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware

RECOMMENDATIONS – CRIMINAL ACTIVITY (AML/CFT)	
9.	Member Countries remain encouraged to implement the FATF Guidance for a risk-based approach to virtual currencies (most recently issued in June 2019).
10.	Member Countries are encouraged to include virtual currencies within the scope of their money laundering and terrorism financing offences.
11.	Member Countries are encouraged to ensure that virtual currency exchanges, virtual currency payment processors or platforms operating within their jurisdictions are licensed or registered and subject to AML/CFT requirements for all transactions, irrespective of whether the transaction involves the exchange of fiat currency to virtual currency, or virtual currency to virtual currency, including: an obligation to obtain and retain know-your-client (KYC) information; an obligation to report suspicious transactions to an appropriate authority.
12.	Independently of the obligations relating to exchanges at 3. above, Member Countries are encouraged to develop mechanisms which enable voluntary reporting of suspicious activity relating to virtual currencies by other persons or entities.

Taxation

Background

102. The Working Group's analysis suggests that virtual currencies will be treated differently for taxation purposes across different jurisdictions, consistent with the existing tax framework in those countries. Given the lack of global tax harmonisation, this approach is not expected to change in the short term. The Working Group also expects individual tax cases/decisions to arise in Member Countries over the next few years (given the recent prevalence of virtual currencies and the time period that it normally takes for tax challenges to work their way through the assessment and legal system).

Classification of virtual currencies for tax purposes – property, commodity or money?

103. Virtual currencies, by their nature, are flexible and capable of being used for multiple purposes. This has given rise to differing tax treatments both as between countries and indeed within the same country, depending on the nature of the use that the virtual currency is put to.

104. A good example of this is the United States, where the U.S. Internal Revenue Service classifies virtual currencies as "property" for the purposes of federal tax, and not as money or currency[51]. This means that a U.S. tax payer who receives virtual currency by way of payment for goods and services must value it for the purpose of calculating gross income as at the date it was received. Then, on a sale or exchange of the virtual currency, the taxpayer must assess if they have made a taxable gain or loss and include this within their annual return. In other words, the U.S. applies to virtual currency, all general tax principles that apply to property transactions.

105. At the same time, the U.S. Commodity Futures Trading Commission was recently upheld in federal court in its decision to treat virtual currency as "commodities", opening up the possibility of a different tax treatment for virtual currencies being used in particular contexts[52]. The same approach has been taken in Canada with a 2013 Interpretation Letter and a 2014 position paper noting that virtual currencies fail to meet the definition of money in Canada and should be treated as a commodity like gold or oil and subject to taxation rules on barter trades.

106. A third classification is to treat the virtual currency as akin to "money" or foreign currency. This is the approach taken in various countries and also by the EU in the *Hedqvist* case[53]. In that matter, a Swedish national, Mr. Hedqvist, sought to open up a company in Sweden enabling customers to exchange traditional currencies for Bitcoins and vice versa. The company planned to make its money in the usual manner of currency exchanges: on the margin between bid and ask prices. Mr. Hedqvist had obtained a preliminary opinion from the Swedish Revenue Law Commission stating that the services he intended to provide

51 https://www.irs.gov/pub/irs-drop/n-14-21.pdf
52 https://www.reuters.com/article/us-usa-cftc-bitcoin/virtual-currencies-are-commodities-u-s-judge-rules-idUSKCN1GI32C
53 https://circabc.europa.eu/sd/a/add54a49-9991-45ae-aac5-1e260b136c9e/892%20-%20CJEU%20Case%20C-264-14%20Hedqvist%20-%20Bitcoin.pdf

would be exempt from VAT under Article 135 of the European VAT Directive. The Swedish Tax Authority disagreed, however, and appealed the matter to the Supreme Administrative Court of Sweden. Uncertain as to how to apply the Directive's exemptions to virtual currencies, the Swedish court referred the matter to the CJEU for a preliminary ruling.

107. The first part of the Court's analysis was uncontentious - buying and selling a currency on margin is a form of supply of services for consideration. This, as the Court pointed out, was fairly obvious under the ECJ's prior settled case law. Hence, in principle, virtual currency trading would be subject to VAT unless it falls under one of the Directive's enumerated exemptions.

108. However, the Court also concluded, that the virtual currency in this case had the characteristics of a currency, albeit one that was not legal tender - and not, as some had argued, a commodity, a speculative asset, a contract or property right, or some other form of legally enforceable claim against others.

109. According to paragraph 24 of the Court's opinion:

the "bitcoin" virtual currency with bidirectional flow, which will be exchanged for traditional currencies in the context of exchange transactions, cannot be characterised as "tangible property"... given that, as the Advocate General has observed... that virtual currency has no purpose other than to be a means of payment...

As a result, the service of virtual currency trading was held to be exempt from VAT under the exception which applies to means of payments such as "currency, bank notes, coins used as legal tender".

Sales/goods/services taxes

110. There are several examples, including the *Hedqvist* case above, of countries determining that provision of services related to virtual currencies can be liable for sales or goods/services taxes such as VAT unless a specific exemption applies. In most cases this is the application of the usual principles of tax analysis rather than a specific decision relating to the nature of virtual currencies.

111. For example, the UK's HMRC has published a brief which confirms its position on the tax treatment of virtual currencies[54]. This sets out its detailed position on VAT – in particular noting that income received from Bitcoin mining activities will generally be outside the scope of VAT on the basis that there is an insufficient link between any services provided and any consideration received, whereas VAT will be due in the normal way from suppliers of any goods or services sold in exchange for Bitcoin or other similar virtual currency.

112. Singapore and Australia have also published similar guidance relating to GST[55].

Other taxes (CGT, IT, IHT, withholding taxes etc)

113. As can be seen from the above, the application of other taxes tends to follow the classification of virtual currencies under the relevant national law. The Inland Revenue of Singapore has issued guidance, for example, setting out

54 https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies

55 Australia - Treasury laws amendment (2017 Measures No 6.) Act 2017 and Singapore GST e-Commerce guidance

its position on the Income Tax treatment of virtual currencies[56], noting that businesses which choose to accept virtual currencies such as Bitcoins for their remuneration or revenue are subject to normal income tax rules. There have also been examples of countries imposing new taxes on virtual currency activity, such as Thailand's royal decrees passed in May 2018 which created a new tax framework for virtual currencies – encompassing all retail trading and returns on investments including a requirement to pay 7% in VAT (which can be waived) as well as a 15% capital gains tax on returns.

114. Whilst a number of country tax authorities have taken the view that the full suite of national taxes is capable of applying to virtual currencies, depending on the uses to which they are put, these views may well be tested in due course. For example, one argument that has been put forward as to why capital gains tax should not apply to the profits made from virtual currency trading in the UK is that the trading activity is in the nature of a bet, i.e. a highly speculative gamble on then markets rather than traditional, taxable trading profits. So far this argument has been rejected by HMRC, but it is possible that a court will ultimately have to determine this issue.

Options to address taxation issues

New legislation (or amendment of existing legislation)

115. Very few countries have introduced specific new tax legislation relating to virtual currencies. This partly reflects (in the Working Group's view) the flexible nature of virtual currencies and the multiple uses to which they can be put, as well as the early stage of their adoption.

Advantages	Disadvantages
Providing a clear position on taxation of virtual currencies may encourage people to centre operations in particular countries if tax position is favourable. **It may also increase tax receipts.**	Any new legislation risks becoming out of date quickly, unfavourable tax treatment will deter business and innovation in this area. Cost of administration.

Use of existing legislation (with guidance)

116. A common approach observed by the Working Group is for countries to treat the taxation of virtual currencies according to the existing underlying principles which exist in their national system. Several countries including the UK, U.S., Canada, Singapore and Australia have all issued general and/or specific guidance on aspects of taxation relating to virtual currencies.

56 https://www.iras.gov.sg/irashome/Businesses/Companies/Working-out-Corporate-Income-Taxes/Specific-topics/Income-Tax-Treatment-of-Virtual-Currencies/

Advantages	Disadvantages
Provides a consistent approach to taxation. **It allows for flexible approach recognising the different uses to which virtual currencies can be put, easy to implement.** **It may increase tax receipts.**	There is a risk of multiple taxes applying given the different uses to which virtual currencies can be put. May limit the flexibility of the tax authorities when assessing approach to virtual currencies.

Use of existing legislation (without guidance)

117. The majority of countries have not produced specific guidance or legislation in response to virtual currencies. The Working Group did not identify any particular issue for those countries in taxing virtual currencies according to the existing underlying principles which exist in their national system.

Advantages	Disadvantages
No resources required. May give tax authorities flexibility when assessing approach to virtual currencies.	There is a risk of multiple taxes applying given the different uses to which virtual currencies can be put.

Conclusions

118. The Working Group recognised that there is a broad and potentially complex range of taxation issues which can arise from adoption or use of virtual currencies within a Member Country. At the same time, a number of Member Countries have specifically addressed taxation issues in the context of virtual currencies by clarifying the application of their existing legislation. These clarifications were felt to be useful for providing certainty to local users.

119. The Working Group noted the practical risk that virtual currencies could be subject to multiple forms of taxation, depending on the use to which they were being put. It was felt to be more important that users had clarity on their taxation position from Member Countries and Member Countries sought to avoid or limit inconsistent taxation treatment.

RECOMMENDATIONS - TAXATION	
13.	Member Countries are encouraged to assess the tax treatment of virtual currencies, taking account of the use to which the virtual currency is put, in their jurisdiction.
14.	Member Countries are encouraged to publish guidance on the tax treatment of virtual currencies in their jurisdiction.

Financial Products (Intersection with Virtual Currencies)

Background

120. This Guidance has already highlighted various issues relating financial products and virtual currencies. In their discussions, the Working Group noted that the broader trend towards:

    – tokenisation of assets and records (including identity documents); and

    – implementation of those tokens on a secure DLT system

    has a profound potential to change the way that financial transactions take place, making it quicker, easier and cheaper for business and consumers to deal with each other on a global basis. Many of the current applications under development fall outside the scope of this Guidance, but will undoubtedly be relevant to how virtual currencies and their uses will develop over time.

121. The Working Group has considered two specific financial products use-cases which directly relate to virtual currencies:

    – payments (particularly cross-border payments); and

    – ICOs.

Payments (particularly cross-border payments)

122. Transferring money to someone in another country can be a long, expensive and risky process. The funds exchange hands multiple times before arriving at their destination, and with each exchange comes delays, more fees, and a higher risk that the funds will be misrouted or end up in the hands of the wrong person. Many private companies and governments are exploring solutions to these issues, including replacing or supplementing the current cross-border payments system with technologies based on virtual currencies.

123. One of the earliest discussions of this issues was the 2015 report by the U.S. Federal Reserve on "Strategies for Improving the U.S. Payment System." The report focused on options to modernise the current payments system and set out various options to increase the speed of payment system infrastructure. One option set out in the paper is "*Digital Value Transfer Vehicles*," defined as "*decentralized digital stores of value that can be exchanged*." The report states that this technology "*was not considered [ ] sufficiently mature…at this time, but was identified for further exploration and monitoring given significant interest in the marketplace*."

124. The paper then went on to note the Federal Reserve was actively considering a centralised, distributed, point-to-point architecture through the internet, which it noted was very similar to "digital value transfer vehicles." The main difference between this proposed option and existing virtual currencies is that this system would have a central ledger and central authority overseeing it.

125. This theme was picked up by the IMF in November 2017, when its Deputy Director of Monetary and Capital Markets highlighted cross border payments as an area *"especially ripe for change"*[57] noting that DLT and virtual currencies could be used to underpin an entirely new means of payment. However, the IMF also highlighted various risks, particularly around lack of interoperability of cross-border payments systems, which could hold back innovation and not deliver promised benefits for consumers.

126. An interesting, privately developed system for bank to bank cross border payments is the R3 Real-time International Payments Solution[58] which is built on the Corda DLT platform. This platform is primarily focused on bank to bank payment solutions but has some 25 members who are actively participating in testing the system. Similarly, the solution "xCurrrent," offered by Ripple, enables banks to settle cross-border payments using Ripple's blockchain network. In terms of consumer-facing products, IBM's World Wire system is a cross-border, DLT-based, payment system available to banks and other financial institutions which allows them to make cross-border payments for their customers in near real time with consequent efficiencies and costs savings[59].

127. Use of virtual currencies in a payments system also raises specific regulatory issues, touched on above. In particular Member Countries will need to consider the application of money transmission or payment services rules.

128. Typically, a person will not be subject to the regulation by money transmission rules or payment services rules just because they send or receive virtual currencies, or provide a platform for others to do the same. The essence of "money transmission" is that it must involve the transfer of money, i.e. legal tender (and as discussed above, no virtual currency fits into this category yet). However, as soon as a virtual currency payment system facilitates transfers of virtual currencies in exchange for traditional currencies or even other virtual currencies, some national money transmission laws will be engaged.

129. In a similar way, bitcoin and other virtual currencies do not typically fall within the scope of "e-money" laws – they are outside the scope of the latest iteration of the Payment Services Directive in the EU for example because those rules focus on payment services involving legal tender.

130. There are examples of countries or national regulators which have reviewed their money transmission/payments services regulations to ensure these are fit for purpose and use with virtual currencies and/or published guidance for users.

131. One example of such an analysis was produced by the Illinois Department of Financial and Professional Regulation in 2017[60]. While the guidance is not exhaustive it does give a clear summary of how the money transmission rules will be applied in Illinois as follows:

57 https://www.imf.org/en/News/Articles/2017/11/01/sp103017-fintech-and-cross-border-payments

58 https://www.r3.com/news/r3-and-22-banks-build-real-time-international-payments-solution-on-corda-dlt-platform/

59 https://www.ibm.com/downloads/cas/VGYAKENA

60 https://www.idfpr.com/Forms/DFI/CCD/IDFPR%20-%20Digital%20Currency%20Regulatory%20Guidance.pdf

Activities generally qualifying as money transmission

- Exchange involving both digital currency and money through a third party exchanger is generally considered to be money transmission. For example, some digital currency exchange sites facilitate exchanges by acting as an escrow-like intermediary. In a typical transaction, the buyer of digital currency sends money to the exchanger who holds the funds until it determines that the terms of the sale have been satisfied before transmitting the funds to the seller. Irrespective of its handling of the digital currency, the exchanger conducts money transmission by receiving the buyer's money in exchange for a promise to make it available to the seller.
- *Exchange of digital currency for money through an automated machine is generally considered to be money transmission. For example, several companies have begun selling automated machines commonly called "Bitcoin ATMs" that facilitate contemporaneous exchanges of digital currency for money. Most such machines currently available, when operating in their default mode act as an intermediary between a buyer and seller, typically connecting through one of the established exchange sites. When a customer buys or sells digital currency through a machine configured this way, the operator of the machine receives the buyer's money and is engaging in the "business of receiving money for transmission or transmitting money."*

  Some digital currency ATMs, however, can be configured to conduct transactions only between the customer and the machine's operator, with no third parties involved. If the machine never involves a third party, and only facilitates a sale or purchase of digital currency by the machine's operator directly with the customer, there is no money transmission because at no time is money received and neither party is engaging in the "business of receiving money for transmission or transmitting money."

Activities not qualifying as money transmission

- *Exchange of digital currency for money directly between two parties does not qualify as money transmission. This is essentially a sale of goods between two parties. The seller gives units of digital currency to the buyer, who pays the seller directly with money. The seller does not receive money with the intent to transmit it to another entity or "engage in the business of exchanging, for compensation, money of the United States Government or a foreign government to or from money of another government."*
- *Transfer of digital currency by itself is not transmitting money. Because digital currency is not money, the receipt of it with the intent to transmit it to another entity is not "transmitting money." This includes intermediaries who receive digital currency for transfer to a third party, and entities who, akin to depositories (commonly referred to as wallets), hold digital currency on behalf of customers and can either unilaterally execute or prevent a digital currency transaction.*
- *Exchange of one digital currency for another digital currency is not money transmission.*
- *A merchant who accepts digital currency as payment for goods or services or an individual who pays for goods or services with digital currency are commonly referred to as "users" of digital currency. Regardless of how many parties are involved, no money is involved at any point in this transaction, so "transmitting money" does not occur.*

- *Miners do not receive money for verifying transactions. Instead, Miners receive digital currency as payment for verifying transactions, typically by contributing software, connectivity, or computing power to process transactions. Because money is not involved in the payment of this work, "transmitting money" does not occur.*
- *Multi-signature software allows users to distribute authority over his or her digital currency among multiple different actors. This software requires multiple actors to authorize a digital currency transaction before the transaction can be consummated. Specifically, a multisignature provider holds one of two or more private keys needed to authorize transactions. Regardless of how many parties are involved, no money is involved at any point in this transaction, so "transmitting money" does not occur.*

132. This sort of guidance was felt to be helpful for virtual currency businesses in terms of them understanding their obligations and avoiding inadvertent regulatory breaches of payment laws.

133. The Working Group also noted the likelihood that the same point of intersection will be relevant for assessing obligations under payments law as for AML/CFT – i.e. the point of intersection between a virtual currency and a fiat currency. This tended to confirm the Working Group's earlier recommendation that virtual currency exchanges should be subject to a form of regulation (licensing or registration).

134. Finally the Working Group noted the possibility that neighbouring countries or close trading partners with similar approaches to payment laws might choose to proactively focus on (government backed or public-private partnership) virtual currency cross-border payments systems given the potential benefits that these systems bring, and recognising that cross-border interoperability is often key to the success of these systems. Possible implementations would be a cross-border payment system for small value payments (akin to contactless payments which are typically low in value) or promoting the safe use of virtual currencies to achieve financial inclusion and benefit consumers and small business on a cross-border basis.

ICOs

135. As noted in paragraph 29, the question of whether and how to regulate ICOs has also been a major topic of discussion over the last few years, with many countries making public statements, issuing rules and guidance about if and how ICOs can be conducted without infringing rules particularly around securities issuances.

136. ICOs, by their nature, tend to be highly speculative and risky investments with no guarantee that the end product or project being funded will ever be made available to the investor. There have been instances of fraud and many more instances of disappointed investors who are often unsophisticated consumers. It is normal practice for ICO issuers to appoint so-called "bounty hunters" who support the ICO and seek to drum up support for it and encourage other investors (often on social media) to participate in the ICO. The "bounty hunter" is often incentivised to promote the ICO by an extra issue of tokens, which are likely to increase in value when other investors participate in the ICO offering. This potential conflict of interests with the investor is not always be disclosed by the "bounty hunter" at the point of promotion.

137. ICOs suffer from the same structural issues as virtual currencies – the inherent flexibility of the technology and the various uses to which the ICO tokens can be put (share-like investment, debt-like investment or exchangeable for products or services) mean it can be difficult to come up with a "one size fits all" regulatory approach, unless it is a restrictive model approach as the Working Group have seen in the U.S.

138. In December 2017, SEC Chair Jay Clayton made a statement on cryptocurrencies as follows:

    by and large, the structure of initial coin offerings that I have seen promoted involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws.

139. In January 2018, the Securities and Exchange Commission (SEC) halted an initial coin offering (ICO) by Munchee, Inc., a California blockchain based food review service. In the order, the SEC focused on the manner of sale as well as the investment intent of purchasers of the Munchee coin in its determination that the offering constituted a non-compliant sale of securities. The Munchee decision suggests that the SEC view is that, regardless of what it is called, or what the token actually does, the offering of the token will likely be the sale of a security based upon the manner of sale, the investment objectives of the purchasers and the actual usefulness to the purchaser. With regards to Munchee, the SEC focused on the following:

    the company and other promoters emphasized that investors could expect that efforts by the company and others would lead to an increase in value of the tokens. The Company also emphasized it would take steps to create and support a secondary market for the tokens. Because of these and other company activities, investors would have had a reasonable belief that their investment in tokens could generate a return on their investment

140. This approach by the SEC has now been upheld by the Eastern District of New York which recently issued a ruling rejecting arguments made in a motion to dismiss a criminal indictment that federal securities laws do not apply to cryptocurrencies[61].

141. A number of Member Countries, including the UK and Singapore, have adopted the approach of providing guidance as to how ICOs fit in with existing financial promotions and investment laws, often with clear warnings for investors about the risks they are taking by investing in ICO offerings – effectively the permissive/guidance model. Other countries such as Bermuda and Gibraltar have produced new legislation specifically dealing with ICOs.

142. In July 2018, Bermuda introduced an ICO Act and ICO Regulations which have the combined effect of regulating all aspects of offering any kind of digital assets to the public in or from Bermuda. Importantly, only companies registered in Bermuda with appropriate government consent are permitted to conduct ICOs in or within Bermuda. In order to get government consent, the ICO offer document is required to contain various information and disclosures, including the names of the persons managing the business project and conducting the

61 U.S. v. Zaslavskiy, 1:17-cr-00647 (E.D.N.Y. Sept. 11, 2018). The decision is the first to rule that violations of federal securities laws were adequately alleged in connection with cryptocurrencies sold in ICOs and provides support to the SEC's position that federal securities laws may apply to cryptocurrencies depending on the facts and circumstances.

ICO as well as a good level of detail on the development and implementation of any underlying project. Various fees are payable to the Bermudian government and when the ICO is launched, it is subject to ongoing compliance obligations (including the obligation to verify the identity of any investors in the ICO.

143. The Gibraltar proposals for ICO token regulation take a different approach – rather than regulating promoters, issuers of tokens, the underlying technology or the tokens themselves, the Gibraltar rules seek to regulate the service providers who will be involved in any Gibraltarian ICO such as authorised sponsors of public token offering, crypto-exchanges and token service providers. However, the two key requirements of the Gibraltarian token regulation regime are very similar to Bermuda, namely:

    - adequate and accurate disclosure of information to investors and regulators; and
    - adherence with AML/CFT provisions, including identification of investors.

144. Whereas ICOs usually correspond simply to the sale of a token itself, the offering of a token that represents traditional securities such as stocks or bonds, has become increasingly popular over the last year. Such a Security Token Offering (STO), normally engages the full regulatory framework that attaches to securities. The advantages of tokenizing the security on a blockchain may include increased market accessibility and transparency, 24/7 trading, and potentially increased liquidity. A secondary market for tokens issued through an STO is in its infancy, although a small number of exchanges have sought regulatory approval for trading of digital security tokens. As noted earlier in the report, recent ICO activity has decreased substantially from the January 2018 peak.

Other financial products

145. During the Working Group's discussions, other financial products which intersect with virtual currencies were noted, including so-called "crypto derivatives". Subsequent to the Group's meetings, further market products have become available including a bitcoin futures contract offered by Intercontinental Exchange, the owner of the New York Stock Exchange. While these specialized financial products did not play a significant role in the Group's conclusions, the principles set out below could be equally applied to this broader group of products.

Options to address financial products issues

New legislation (or amendment of existing legislation)

146. Some countries have introduced specific legislation relating to ICOs and/or amended payments laws and money transmission laws to take account of virtual currencies.

Advantages	Disadvantages
Provides a clear position on ability to conduct ICOs and/or application of payments/money transmission laws. **A balanced regime may increase innovation and business in that Member Country.** **Provides clarity to businesses and reduces risk of inadvertent breach of laws .** **May generate fee income.** **May protect unsophisticated consumers and reduce incidences of fraudulent activity.**	Costs of administration May stifle innovation or reduce virtual currency related business in that Member Country. Risk that any legislation may become out of date unless broadly drafted.

Use of existing legislation (with guidance)

147. Several countries have issued general and/or specific guidance explaining how payments laws and/or ICOs are treated under existing legislation.

Advantages	Disadvantages
Provides a level of guidance to market participants on ability to conduct ICOs and/or application of payments/money transmission laws. **Clear and detailed guidance may increase innovation and business in that Member Country and reduces risk of inadvertent breach of laws .** **May protect unsophisticated consumers and reduce incidences of fraudulent activity.**	May limit the flexibility of the financial authorities when assessing approach to virtual currencies. Unclear guidance may stifle innovation, reduce business or lead to lack of clarity and transparency for consumers.

No action

148. It is always open for Member Countries to take no action, either because existing laws clearly cover the way that payment services and ICOs operate or because there is no significant risk or harm in that country being caused by virtual currencies in these two areas.

Advantages	Disadvantages
No resources required. **May give financial authorities flexibility when assessing approach to virtual currencies in the context of ICOs and payments**	There is a risk of an uncontrolled market in payments and ICOs with consequent impact on consumers and other investors. Risk of fraudulent activity

Conclusions

149. Virtual currency payment systems and ICOs are applications which have both significant potential benefits but also carry material risks for consumers. Key factors which the Working Group identified as important to consider were:

- ensuring that any activity was compliant with AML and CFT laws; and
- ensuring a good level of transparency for ICO investors or users of any virtual currency payments service, so that they could understand the risks of the systems and any redress available to them as part of their overall decision-making process.

RECOMMENDATIONS – FINANCIAL PRODUCTS	
15.	Member Countries are encouraged to review their existing money transmission legislation to assess whether virtual currency payment providers are or should be excluded and if so, to what extent.
16.	Member Countries are encouraged to consider the treatment of ICOs under their existing laws and provide guidance where appropriate, including on ensuring that ICO activity is compliant with AML and CFT rules.

Consumer Protection

Background

150. The Working Group discussed a broad range of issues relating to consumer protection. It was notable that many Member Countries were conscious of specific risks to consumers caused by virtual currencies, but had focused their efforts on managing the general risks presented by a nascent virtual currency industry rather than focusing specifically on consumer protection. Since the Working Group met,

151. It remains important to improve education and understanding surrounding the nature, benefits and risks of virtual currencies. Current consumer protection legislation is unlikely to address all the risks that virtual currencies pose for consumers and there is a speculative aspect to virtual currency trading which has the potential to adversely affect unsophisticated investors. Over the past two years, there has been huge volatility in the pricing of virtual currency as well as the structure of it.

Existing Consumer Protection Laws

152. The Working Group did not identify a single instance of a Member Country reviewing the basic application of its consumer protection legislation relating to sale of goods or services, or advertising standards to take account of virtual currencies and how these may impact existing protections for consumers. Examples of the sorts of issues which the Working Group identified included the potentially irreversible nature of transactions involving virtual currencies (particularly in countries with distance selling regulations or statutory "cooling off" periods), the lack of transparency about the identity of any counterparty to certain kinds of virtual currency transactions and the unavailability of any regulatory or complaints body to deal with issues relating to virtual currencies. This was both in respect of transactions for goods and services paid for by virtual currencies as well as transactions in respect of virtual currencies.

Lack of Consumer Understanding

153. In the last two years, the use of virtual currencies has expanded and has a much greater impact on consumers. However, the detail of how virtual currencies work in practice are complex. There is a clear possibility that unsophisticated consumers will not understand the risks surrounding it.

154. Evidence continues to suggest that consumers do not fully understand the risks associated with using virtual currencies. The UK Financial Conduct Authority discussion paper on DLT[62] noted that many consumers perceived digital currencies as regulated financial instruments. As a result, consumers may believe they are protected by financial law and have recourse to financial regulators or compensation schemes in respect of their dealings in virtual currencies – when in fact they do not.

155. Even where consumers have a good level of knowledge, the technical issues surrounding virtual currencies pose new risks which are difficult to guard against. A good example of this is the "DAO Hack".

62 FCA, Discussion Paper on distributed ledger technology, DP17/3, April 2017.

156. The DAO or Decentralized Autonomous Organization was a fund, created as a decentralized investment fund. The aim was that, instead of leaving investment decisions to a few partners, anyone who invested would have a say in which companies to fund. The more any one person contributed, the more weight that person's vote carried. The distributed structure was intended to ensure the funds remained secure. The DAO was built on Ethereum, a system designed for building decentralized applications. However, the coding was done at speed as part of an ICO process. Various bugs in the code were identified and initial discussions took place regarding how to resolve those coding bugs. Before the community had a chance to do this, however, someone found a way to use the bugs in the code to withdraw money from the DAO. This began at around 4 a.m. on a Friday. By 7 a.m., $45 million had been withdrawn, the price of ether fell 40 percent and the price of DAO tokens fell 70 percent. However, the developers were able to find the bug the hacker had exploited and the place where the funds has been transferred to.

157. The developers then decided to mount a "white hat attack" on the remaining funds in the DAO and the DAO attacker. They spammed the network with dust transactions, allowing them to use the same exploit used to withdraw funds from the original DAO and from the hacker, and ultimately regain control over the funds.

158. While the story has a (comparatively) happy ending, it is an example of two major issues –in particular insufficient stress testing on the coding of the DAO before it was rolled out to a large number of consumers who were being asked to invest in the project. The second issue is that the solution implemented to recover the funds was the implementation of a so-called "hard fork", to transfer the misappropriated funds to the people that it belonged to. Whilst done for the best of reasons, there are material issues about when and by whom, hard forks can be authorized and implemented, given they have the power to materially change the scope of the project, Blockchain or code that the original consumer participant signed up to.

Technical development

159. Virtual Currencies and the technology that underpins it is still in its infancy and is constantly developing. As it does, it unveils some of the shortcomings of its current structure. Bitcoin experienced this through the need for a hard fork on 1 August 2017. As the popularity of Bitcoin increased, there were concerns as to what the block-size limit should be. The original block-size was capped at 1 megabyte. As the number of transactions on the network has grown, there has been a call for a size of the blocks to increase so as to prevent the speed of transactions from slowing down. A solution called SegWit created a structure that frees up more space for transactions, but maintains the block size. The issue however, was that SegWit could create a situation where transactions take place outside of the Bitcoin network, which many did not like. This led to the proposal for a hard fork and the development of Bitcoin Cash which proposed to increase the capacity of each block by 8-fold.

160. Decisions such as these were taking place without consumer guidance or knowledge. The significant structural changes were made without the consultation of its users and forced users to make a decision that they were not in the position to make in an informed manner.

161. Exchanges, such as Bitstamp offered some guidance in that they warned that Bitcoin Cash would not necessarily be recognised by the exchange. The result of this would be that Bitcoin Cash could operate in an area where its value could not be translated into fiat currency. Though this is useful, it does not help consumers with certainty of value - feasibly opting for Bitcoin cash could have resulted in consumers losing some or all of their money.

162. A hard fork is not a new phenomenon. When Ethereum hard forked in July 2016, a similar situation took place, albeit on a much smaller scale. At this point Ethereum was very much in its infancy and most participants accepted the fork to reverse certain funds. However, the non-adopters were still operating in the previous chain and are still doing so today. The hard fork with Bitcoin is far less simple, it is not a matter of reversing funds, it is a structural change and is a matter of understanding the change in protocol and opting for a preferred approach.

163. There is a question as to whether regulation is appropriate to cover situations like this. Are stronger safeguards needed given that consumers will not necessarily be able to understand what it is they are dealing in? Or is it sufficient that consumers are told they are dealing in unregulated products and with unregulated businesses and that all capital and funds are at risk as a result?

Cyber/Hacking

164. Notwithstanding the enhanced security that virtual currencies bring, cyber and hacking risk remains a material issue. As witnessed in the Mt Gox and Bitfinex scandals[63], it is possible for a digital attack to target exchanges and steal coins resulting in the owners losing their money. Some weaknesses are structural – there are examples of (less than reputable) exchanges who require consumers to provide or store their private key on the exchange. Whilst that makes the transfer process easier for the exchange, it is a significant security risk for the consumer, if their private key is exposed their funds can be removed without any further reference or recourse.

165. On a more general level, interconnectivity between devices and assets poses a challenge for the protection of consumers. Whilst breaches in security in more traditional finances are to an extent isolated, virtual currency breaches have the potential for much wider spread risks. Therefore, consumer protection issues should not be limited to the interaction of virtual currencies with fiat currency but also on data protection and cyber issues. Hong Kong, for example, has introduced new regulations for virtual currencies that require trading platforms and fund managers to ensure that clients' virtual assets are well protected in a similar way to client "cash" monies.

Volatility and Usability

166. As of November 2017, the price of a single Bitcoin hit circa US$20,000. At the time of the drafting of the working group recommendations, the price of the single Bitcoin was at circa US$6000. At the time of finalising this report, the price of Bitcoin has risen to somewhere close to $8,000 but this price recovery could stall at any time.

63 https://www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP

167. The value of virtual currency fluctuates dramatically over days and is not as stable as fiat currency, it also suffers from the fact that there is not an official exchange rate and it is done on a market place basis. David Yermack indicated that there is a real diversity in "current market prices" for Bitcoin at any given time with a range of seven per cent between the five exchanges with the highest trading volume[64]. Though one may aggregate these prices, it does not allow consumers or merchants the ability to know the true value of their Bitcoin.

168. In terms of usability there are two central issues. The first is the relative complexity of virtual currencies compared to cash. The second is acceptance as a unit of payment or value rather than as a speculative instrument. Taking Bitcoin as the most commonly used virtual currency – its value is extremely high in comparison to the products or services one may be purchasing. Therefore, in terms of interpreting its value, the price is written as a number, in some cases to five decimal places. This creates confusion to consumers and inhibits its usability. This in some way has been resolved with other virtual currencies entering the market, however market share of these virtual currencies is very small and its lack of widespread use makes it difficult for consumers to use. Similarly, the limited number of places where virtual currencies are accepted also make it difficult to adopt the currency. As a result, many of the users instead use the currency for speculative purposes rather than for actual use of it as a currency.

169. The Working Group noted the increasing focus on stable coins as a mechanism to avoid the volatility and usability issues associated with Bitcoin and similar virtual currencies. The announcement of the proposed Libra currency (subsequent to the drafting of the report) has reinforced this focus, as the value of Libra is intended to be pegged not to one specific currency, but rather to a group of "low-volatility assets, including bank deposits and government securities" in multiple currencies, in an attempt to maximize its global usability and availability.

Options to address consumer protection issues

Education via state messaging and guidance

170. Focus on educating consumers by state/regulator communications either in respect of the sector generally or specific aspects which are considered to be high risk. Examples would include the FCA Statement on ICOs which stated that "*ICOs are very high-risk, speculative investments*"[65] and the warning of the Central Bank of Nigeria that virtual currencies are not legal tender and no consumer protections arise when dealing with virtual currency exchanges[66]. Various senior representatives of Member Country governments have also made statements or given speeches highlighting risks of virtual currencies. The Australian Securities and Investments Commission has provided guidance on distributed ledger technology and ICOs.[67]

64 D Yermack, "Is Bitcoin a Real Currency? An Economic Appraisal", National Bureau of Economic Research, December 2013
65 www.fca.org.uk/news/statements/initial-coin-offerings.
66 https://www.cbn.gov.ng/Out/2018/CCD/Press%20Release%20on%20Virtual%20Currencies.pdf
67 https://asic.gov.au/regulatory-resources/digital-transformation

Advantages	Disadvantages
Likely to benefit some consumers **Does not require significant resources** **No changes in legislation required**	Messages may not be "heard" by those who are most at risk (virtual currency has a counter-culture element which may be suspicious of official pronouncements). Does not protect against cyber, technical or volatility risk, just ensures that customers are aware of risks.

Education via media

171. It is also possible to focus on educating consumers by alternative channels – mainstream media, social media, blogs but also unconventional channels such as soap operas.

Advantages	Disadvantages
Messages regarding consumer protection are more likely to be heard by those who are most at risk **Does not require significant resources** **No change in legislation required**	More difficult to manage the overall message. Risk of glamorising investments in virtual currencies. Does not protect against cyber, technical or volatility risk, just ensures that customers are aware of risks.

Government standard system ("kitemark")

172. Setting up a government backed system of standards which participants in a virtual currency market could adhere to on a voluntary basis with the possibility of getting an "approval" or "kitemark". Participants would have to meet minimum levels of cyber security, customer care, AML etc.

Advantages	Disadvantages
Develops good practice within a Member Country and drives consumers towards reputable operators.	Could be expensive and complex to operate. Would give rise to expectation that government would stand behind obligations of any virtual currency operator on failure or had "approved" that operator.

Industry/trade standard system

173. Similar to the government standard system, this is a trade group or industry group of voluntary standards, where membership guarantees to the consumer that certain minimum standards are being adhered to. A good example is that Japanese Authority of Digital Assets or JADA[68]. This trade organization aims to establish and enact guidelines to promote and troubleshoot value-recorded business in Japan and contribute to Japan's industrial development by promoting the establishment of a safe business environment and user protection system for value-recorded systems such as Bitcoin. It creates guidelines for value-recorded exchanges such as Bitcoin and works with and exchanges opinions with regulators and related ministries (the Ministry of

68 http://jada-web.jp/

Economy, Trade and Industry; the Financial Services Agency; the Consumer Affairs Agency; the National Police Agency; the National Tax Administration Agency, etc.) and organisations (the Japanese Bankers Association, etc.).

Advantages	Disadvantages
Develops good practice within a country and drives consumers towards reputable operators. **Government is not responsible for funding or operation.**	Lack of oversight or regulation by government. Risk that group operates in the interests of members, not consumers.

Amend or enact consumer laws to cover some or all consumer dealings in virtual currency

174. The success of this approach will depend on the nature of the existing consumer protection in country. Given the multiple uses that virtual currencies have, it is difficult to draft a single piece of legislation that covers all issues but existing consumer protection legislation would be reviewed and updated in order to take account of all relevant activities where virtual currencies are regulated (including using virtual currencies as a unit of value to purchase goods and services).

Advantages	Disadvantages
Provides a level of legal protection to consumers that might otherwise be lacking.	May require updates to a large body of legislation for only limited impact given the size of virtual currency business in that country. The legislative, permissive or restrictive models can equally be used to address consumer protection issues.

Conclusions

175. The Working Group recognised that many of the recommendations made elsewhere in this Guidance, if implemented, would improve consumer protection. The Working Group considered that, even if this was the case, there were some specific consumer-facing actions which could assist with the development of properly functioning virtual currency systems and applications.

RECOMMENDATIONS – CONSUMER PROTECTION	
17.	Member Countries are encouraged to review the application of their consumer protection legislation relating to sale of goods or services and advertising standards to assess if activities relating to virtual currencies are included, or should be included.
18.	Member Countries are encouraged to ensure that their authorisation regimes for virtual currency exchanges facilitate appropriate standards of consumer protection.
19.	Member Countries are encouraged to consider options available to foster awareness for consumers of the benefits and risks of virtual currencies and share their findings and experiences with the Commonwealth.

Social Benefits/Inclusion

176. A number of third party contributors to the Working Group focused on the broader, social benefits that virtual currencies could have and the possibility for Member Countries to use virtual currency technology to drive social benefit and social inclusion. The Working Group is indebted to these presenters for presenting this significantly broader view of how Member Countries may wish to think about virtual currencies.

177. The potential uses of virtual currencies to drive social inclusion are numerous but can broadly be categorized as follows:

    - legal Identity;
    - access to State services;
    - access to financial services;
    - promoting social or environmental programs (including reducing instances of forced or trafficked labour in supply chains).

178. **Legal Identity** – the Working Group considered the work of the ID2020 project[69], an alliance of governments, NGOs and private sector organisations committed to improving lives through digital identity. The World Bank estimates that over 1 billion people are unable to prove who they are, and more than 2.5 billion adults do not have a bank account or use formal financial services, making it difficult to move out of poverty or weather a period of hardship. Whilst beyond the strict scope of the Working Group, the Group noted the potential for new technologies based on distributed ledger systems to drive identity for all projects including in the context of international development.

179. **Access to State Services** – the Working Group noted various proof of concept programs (including in the UK) using distributed ledger technologies (including virtual currencies) to access or receive state benefits or state services. These initial projects have always not been seen as viable in the short term[70] due to the particular make-up of the group of beneficiaries, and/or the expense and cost of the initial startup of the systems, but as the technology develops, it is likely that there will be further trials and systems developed, particularly using distributed ledger technology to access and record use of state services.

180. **Financial Services** – the Working Group noted the use of new technologies (including, but not limited to distributed ledgers or virtual currencies) to drive financial inclusion and particularly to allow consumers to establish a transparent record of responsible financial behaviour outside the traditional banking system. The benefit of this record was that it could be used by consumers to demonstrate their ability to engage with the full financial system and access bank accounts or other services that would have been denied to them on a risk basis without that traceable, transparent record of actions outside the bank system.

69 https://id2020.org/digital-identity-1/
70 https://financefeeds.com/uk-sees-use-blockchain-nonviable-welfare-benefits-system/

181. **Blockchain for Good** – the Working Group noted the very active use of distributed ledger technologies to drive social and particularly environmental agendas, indulging projects to support clean water (www.cleanwatercoin.org) as well as aid and charitable giving projects which utilize blockchain technologies such as Alice (alice.si) and Disburse (www.disberse.com/).

182. **The Working Group** considered that these broader uses of distributed ledger technology and virtual currencies will continue to be of interest to Member Countries as their experience of the technology develops and should be considered alongside the more specific recommendations set out in this Report.

RECOMMENDATIONS – SOCIAL BENEFITS/INCLUSION	
20.	Member Countries are recommended to explore the emerging applications of virtual currencies (and the related underlying technology) to drive social benefit and social inclusion within their jurisdictions, for example: • allowing consumers to establish a record of responsible financial behaviour outside the traditional banking system; • promoting social or environmental programs; • facilitating establishment of legal identity (including birth registration) for access to banking, government services, education and health; • facilitating payment of state benefits and potentially reducing fraud.

Overall Recommendations by the Working Group

RECOMMENDATIONS		
Overarching Issues	1.	Member Countries are encouraged to produce and maintain an overall assessment which: • considers the benefits and risks of virtual currencies in that Member Country; • has regard to the areas and matters in this 2019 Report.
	2.	Member Countries should have regard to this overall assessment when considering activities or actions relating to virtual currencies.
	3.	Member Countries are encouraged to focus their regulatory efforts on the intersections between virtual currencies and fiat currencies – in particular, Member Countries should consider authorising virtual currency exchanges that operate within their jurisdiction (for example, by way of registration or under a licensing regime). The Working Group noted the potential increase in exchanges of virtual currency for virtual currency ("crypto-to-crypto"), but considered this was a lower immediate priority than exchange of virtual to fiat currency.
	4.	Member Countries are encouraged to consider using existing or establishing mutual, cross-border technical or working arrangements, with the aim that entities conducting virtual currency activities which are authorised in one Member Country can apply to be authorised more easily and quickly in other jurisdictions.
CRIMINAL ACTIVITY (NON AML/ CFT)	5.	Member Countries are encouraged to review the application of their criminal legislation to offences where virtual currencies are the instrumentality or subject matter of the crime. The scope of traditional "property" offences such as theft, fraud, cheating etc. may need to be expanded to include virtual currencies.
	6.	Member Countries are encouraged to review their laws of criminal procedure and powers of law enforcement agencies to access, seize, manage and dispose of virtual currencies.
	7.	Member Countries are encouraged to ensure that their law enforcement agencies have effective operating procedures and training for the investigation of offences involving virtual currencies.
	8.	Member Countries are encouraged to provide training relating to virtual currencies for their judiciary and prosecuting authorities.

RECOMMENDATIONS		
CRIMINAL ACTIVITY (AML/CFT)	9.	Member Countries remain encouraged to implement the FATF Guidance for a risk-based approach to virtual currencies (most recently issued in June 2019).
	10.	Member Countries are encouraged to include virtual currencies within the scope of their money laundering and terrorism financing offences.
	11.	Member Countries are encouraged to ensure that virtual currency exchanges, virtual currency payment processors or platforms operating within their jurisdictions are licensed or registered and subject to AML/CFT requirements for all transactions, irrespective of whether the transaction involves the exchange of fiat currency to virtual currency, or virtual currency to virtual currency, including: • an obligation to obtain and retain know-your-client (KYC) information; • an obligation to report suspicious transactions to an appropriate authority.
	12.	Independently of the obligations relating to exchanges at 3. above, Member Countries are encouraged to develop mechanisms which enable voluntary reporting of suspicious activity relating to virtual currencies by other persons or entities.
TAXATION	13.	Member Countries are encouraged to assess the tax treatment of virtual currencies, taking account of the use to which the virtual currency is put, in their jurisdiction.
	14.	Member Countries are encouraged to publish guidance on the tax treatment of virtual currencies in their jurisdiction.
FINANCIAL PRODUCTS	15.	Member Countries are encouraged to review their existing money transmission legislation to assess whether virtual currency payment providers are or should be excluded and if so, to what extent.
	16.	Member Countries are encouraged to consider the treatment of ICOs under their existing laws and provide guidance where appropriate, including on ensuring that ICO activity is compliant with AML and CFT rules.
CONSUMER PROTEC-TION	17.	Member Countries are encouraged to review the application of their consumer protection legislation relating to sale of goods or services and advertising standards to assess if activities relating to virtual currencies are included, or should be included.
	18.	Member Countries are encouraged to ensure that their authorisation regimes for virtual currency exchanges facilitate appropriate standards of consumer protection.
	19.	Member Countries are encouraged to consider options available to foster awareness for consumers of the benefits and risks of virtual currencies and share their findings and experiences with the Commonwealth.

RECOMMENDATIONS		
SOCIAL BENEFITS /INCLUSION	20.	Member Countries are recommended to explore the emerging applications of virtual currencies (and the related underlying technology) to drive social benefit and social inclusion within their jurisdictions, for example: • allowing consumers to establish a record of responsible financial behaviour outside the traditional banking system; • promoting social or environmental programs; • facilitating establishment of legal identity (including birth registration) for access to banking, government services, education and health; • facilitating payment of state benefits and potentially reducing fraud.

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

thecommonwealth.org

The Commonwealth

D16999