FATF

GUIDANCE FOR A RISK-BASED APPROACH

VIRTUAL CURRENCIES

JUNE 2015

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML	Anti-money laundering
ATM	Automated teller machine
BaFIN	German Federal Supervisory Authority
CDD	Customer due diligence
CFT	Countering the financing of terrorism
DNFBP	Designated non-financial business and profession
EBA	European Banking Authority
FINMA	Financial Market Supervisory Authority
KWG	German Banking Act
MAS	Monetary Authority of Singapore
ML	Money laundering
MSB	Money service business
MVTS	Money value transfer service
NPPS	New Payment Products and Services
P2P	Peer-to-peer
RBA	Risk-based approach
TF	Terrorist financing
VC	Virtual currency
VCPPS	VC payment products and services

SECTION I – INTRODUCTION

BACKGROUND

1. The Financial Action Task Force (FATF) issued the report *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, in June 2014 (June 2014 VC report). In recent years, virtual currencies (VCs) have emerged and attracted investment in payments infrastructure built on their software protocols. These payments mechanisms seek to provide a new method for transmitting value over the internet.

2. The FATF recognizes financial innovation. At the same time, VC payment products and services (VCPPS) present money laundering and terrorist financing (ML/TF) risks and other crime risks that must be identified and mitigated**.** This Guidance focuses on applying the risk based approach to the ML/TF risks associated with VCPPS, and not on other types of VC financial products, such as VC securities or futures products. Accordingly, the Guidance has adopted the term VC payments products and services (VCPPS), rather than VC products and services (VCPS), where the discussion is limited to VC payments schemes.

3. The development of VCPPS and interactions of VCPPS with other New Payment Products and Services (NPPS) and even with traditional banking services,[1] give rise to the need for this Guidance to protect the integrity of the global financial system.

4. This stand-alone Guidance builds on the June 2014 VC report and on the risk matrix and the best practices of the *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet Based Payment Services*[2] report (June 2013 NPPS report).

5. This Guidance is part of a staged approach taken by the FATF. The focus of this Guidance is on the points of intersection that provide gateways to the regulated financial system, in particular convertible[3] virtual currency exchangers[4]. The FATF will continue to monitor developments in VCPPS and emerging risks and mitigating factors. As we learn more about the technology and use of VCPPS, the Guidance may be updated, to include, where appropriate, emerging best practices to address regulatory issues arising in respect of ML/TF risks associated with VCPPS. Issues related to e.g. transfers within decentralised convertible VC networks that do not involve exchange activities, such as person-to-person transfers involving hosted wallet providers, and large value VC payments, which are not addressed by this Guidance may be considered in the longer term.

PURPOSE OF THE GUIDANCE

6. This Guidance is intended to explain the application of the risk-based approach to AML/CFT measures in the VC context; identify the entities involved in VCPPS; and clarify the application of the relevant *FATF Recommendations* to convertible virtual currency exchangers. This Guidance is also intended to help national authorities understand and potentially develop regulatory responses including the need to amend their national laws in order to address the ML/TF risk of VCPPS. This Guidance is also intended to help the private sector better understand the relevant AML/CFT

obligations and how they can effectively comply with relevant requirements. The Guidance incorporates the conceptual framework and key terms adopted by the FATF in the *June 2014 VC Report (Appendix A),* and readers are referred to that document for discussion of potential use cases for VC and a glossary of terms.

7. The Guidance seeks to:

a) Show how specific *FATF Recommendations* should apply to convertible virtual currency exchangers in the context of VCPPS, identify AML/CFT measures that could be required, and provide examples; and

b) Identify obstacles to applying mitigating measures rooted in VCPPS's technology and/or business models and in legacy legal frameworks.

8. The FATF notes that some Governments are beginning to consider a range of regulatory issues presented by VCPPS. With respect to AML/CFT in particular, while some jurisdictions are taking regulatory action, others are monitoring and studying the developments and potential ML/TF risks, as the usage still develops in those jurisdictions. For some jurisdictions, putting in place an effective AML/CFT regulatory regime may require a more thorough understanding of the VCPPS. Nevertheless, the rapid development, increasing functionality, growing adoption and global nature of VCPPS make national action to identify and mitigate the ML/TF risks presented by VCPPS a priority. The FATF recognizes that there may be other policy considerations that may affect the ultimate regulatory options or outcomes of VCPPS in individual jurisdictions.

9. Establishing some form of Guidance across all jurisdictions that treat similar products and services consistently according to their function and risk profile is essential to enhance the effectiveness of the international AML/CFT standards. This is a particular concern for VCPPS given their 'borderless' nature, where activities may be carried out without seeming to be based in any particular jurisdiction. While the Guidance is non-binding and does not overrule the purview of national authorities, it hopefully will help public authorities and the private sector identify and effectively address VCPPS associated ML/TF risks.

SCOPE OF THE GUIDANCE

10. The Guidance focuses on VCPPS and related AML/CFT issues, and applies to both centralised and decentralised VCPPS. It primarily addresses convertible VC, because of its higher risks. The focus of this Guidance is on convertible virtual currency exchangers which are points of intersection that provide gateways to the regulated financial system (where convertible VC activities intersect with the regulated fiat currency financial system). It does not address non-AML/CFT regulatory matters implicated by VC payment mechanisms (e.g., consumer protection, prudential safety and soundness, tax, anti-fraud issues and network IT security standards). Nor does it address non-payments uses of VC (e.g., store-of-value products for savings or investment purposes, such as derivatives, commodities, and securities products) or the monetary policy dimension of VC activities.[5]

STRUCTURE

11. This Guidance is organised as follows: Section II examines the extent to which convertible virtual currency exchangers fall within the scope of the *FATF Recommendations*. Section III describes the application of the *FATF Recommendations* to countries and competent authorities; Section IV explains the application of the *FATF Recommendations* to convertible virtual currency exchangers; and Section V provides country (or group of countries) examples of regulatory approaches to date or expected in the near future. The June 2014 VC Report is included in **Appendix A**. An explanation of what VC is and how it works as a payment mechanism, based on different business models and methods of operation, is set forth in **Appendix B.**

SECTION II - SCOPE OF FATF STANDARDS[6]

12. This section (1) discusses the application of the risk-based approach to VCPPS and (2) examines how convertible virtual currency exchangers should be subject to AML/CFT requirements covered by the international standards.

INITIAL RISK ASSESSMENT[7]

13. The risk assessment in the June 2014 VC Report (Appendix A) indicates that at least in the near-term, only *convertible* VC, which can be used to move value into and out of fiat currencies and the regulated financial system, is likely to present ML/TF risks. Accordingly, under the RBA, countries should focus their AML/CFT efforts on higher-risk convertible VCs.

14. The risk assessment also suggests that AML/CFT controls should target convertible VC nodes—i.e., points of intersection that provide gateways to the regulated financial system—and not seek to regulate users who obtain VC to purchase goods or services. These nodes include third-party convertible VC exchangers. Where that is the case, they should be regulated under the *FATF Recommendations*. *Thus, countries should consider applying the relevant AML/CFT requirements specified by the international standards to convertible VC exchangers, and any other types of institution that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system.*

15. Under the RBA, countries could also consider regulating financial institutions or DNFBP that send, receive, and store VC, but do not provide exchange or cash-in/cash-out services between virtual and fiat currency. This is however, not in the scope of this Guidance.

FATF DEFINITIONS

16. The *FATF Recommendations* require all jurisdictions to impose specified AML/CFT requirements on financial institutions and designated non-financial businesses and professions (DNFBP) and to ensure their compliance with those obligations.

17. The FATF defines a "financial institution" as any natural or legal person who conducts as a business one or more of several specified activities for or on behalf of a customer. The categories potentially most relevant to currently available VCPPS include persons that conduct as a business: Money or value transfer services (MVTS)[8]; acceptance of deposits and other repayable funds from the public; issuing and managing means of payment; and trading in foreign exchange, or transferable securities. Depending on their particular activities, decentralised VC exchangers, wallet providers, and payments processors/senders, as well as other possible VC business models, may fall within one or more of these categories.

18. Whether a natural or legal person engaged in VCPPS is an obliged entity depends on how that person uses the VC and for whose benefit. National authorities should address the ML/TF risks associated with convertible VC exchange activities (where convertible VC activities intersect with the

regulated fiat currency financial system), as appropriate under their national legal frameworks, which may offer a variety of options for regulating such activity.

19. Providers of VCPPS conducting activities which fall within the FATF definition of a *financial institution* are subject to the applicable FATF Recommendations. This includes convertible virtual currency exchangers where convertible VC activities intersect with the regulated fiat currency financial system.

20. Depending on the intensity or volume of specific VC activities involved and their own national legal frameworks, countries should address the ML/TF risks associated with VC exchanges and any other types of institutions that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system, by applying the relevant FATF Recommendations to any of these categories of covered entities, on a risk basis.

SECTION III – APPLICATION OF FATF STANDARDS TO COUNTRIES AND COMPETENT AUTHORITIES

21. This section explains how specific FATF Recommendations related to VCPPS apply to countries and competent authorities, focusing on identifying and mitigating risks associated with convertible VCs, applying licensing/registration requirements, implementing effective supervision, providing a range of effective and dissuasive sanctions and facilitating national and international cooperation.

22. Some of FATF Recommendations are directly relevant to understanding how countries should use government authorities and international cooperation to address the ML/TF risks associated with convertible VC.

23. **Recommendation 1.** The current *FATF Recommendations* make clear that countries should apply a RBA to ensure that measures to prevent or mitigate ML/TF risks are commensurate with the risks identified. Under the RBA, countries should strengthen the requirements for higher risk situations. When assessing the ML/ TF risk of convertible VC, the distinction between centralised and decentralised VC will be one key aspect. Due to anonymity and the challenges to conduct a proper identification of the participant, convertible decentralised VCPPSs in general may be regarded of higher risk of ML/FT which would require the application of enhanced due diligence measures.

24. Recommendation 1 requires countries to identify, understand, and assess the country's ML/TF risks and to take action aimed at effectively mitigating those risks. This requirement applies in relation to risks associated with VCs and other new technologies. Public-private sector cooperation may assist competent authorities in developing AML/CFT policies for VC financial activities, innovations in VC technologies and emerging products and services. This may also assist countries in allocating and prioritizing AML/CFT resources by competent authorities.

25. National authorities should consider undertaking a coordinated risk assessment of VC products and services that (1) enables all relevant authorities to understand how specific VC products and services function, fit into, and impact all relevant regulatory jurisdictions for AML/CFT purposes (e.g., money transmission/payments mechanisms; VC ATMs; commodities; securities) and (2) promotes similar AML/CFT treatment for similar products and services having similar risk profiles.

26. Countries should also require financial institutions and DNFBP to identify, assess, and take effective action to mitigate their ML/TF risks associated with VCPPS. For AML/CFT purposes, where VCPPS activities are permitted under national law, jurisdictions, financial institutions and DNFPB, including convertible virtual currency exchangers, must assess the ML/TF risks and apply a RBA to ensure that appropriate measures to prevent or mitigate those risks are implemented.

27. Even if a country decides not to regulate VC with respect to non-ML/TF risks, such as consumer protection, prudential safety and soundness, and network security, it still should take

prompt action to identify, assess, and apply a RBA to mitigate the ML/TF risks associated with VC under the relevant FATF Recommendations.

28. According to this risk assessment, countries should decide to regulate exchanges platforms between convertible virtual currencies and fiat currencies (i.e., convertible virtual currency exchangers). Some countries may decide to prohibit VC activities, based on their own risk assessment (including, e.g., uptake trends) and national regulatory context in order to support other policy goals not addressed by this Guidance (e.g., consumer protection, safety and soundness, monetary policy). Where countries consider prohibiting VCPPS, they should take into account, among other things, the impact a prohibition would have on the local and global level of ML/TF risks, including whether prohibiting VC payments activities could drive them underground, where they will continue to operate without AML/CFT controls or oversight. Regardless of whether a country opts for prohibiting or regulating VCs, additional measures are useful to mitigate the overall ML/TF risk. If a country decides to prohibit VC activities, additional mitigation measures would include identifying VC providers that are operating illegally in their jurisdiction and applying proportionate and dissuasive sanctions to them. Prohibition would still require outreach, education and enforcement actions by the country. Countries would also need to take into account the cross-border element of VCPPS in their risk mitigation strategies.

29. **Recommendation 2** requires national cooperation and coordination with respect to AML/CFT policies--including in the VC sector. Countries may consider putting in place mechanisms, such as inter-agency working groups, to enable policy-makers, regulators, supervisors, the financial intelligence unit (FIU), and law enforcement authorities to cooperate with each other and any other relevant competent authorities to develop and implement effective policies, regulations and other measures to address VC ML/TF risks.

30. Countries may consider developing national coordination mechanisms that facilitate appropriate risk-based AML/CFT regulation and supervision across various VC products and services. Among other things, national authorities may undertake a risk assessment of VCPPS that (1) enables all relevant authorities to understand how specific VC products and services function, fit into, and impact all relevant regulatory jurisdictions for AML/CFT purposes (e.g., money transmission/payments systems; VC ATMs; commodities; securities) and (2) promotes similar AML/CFT treatment for similar products and services having similar risk profiles. Countries should also consider adopting their national cooperation and coordination mechanism(s) that facilitates engagement with the VC private sector.

31. If VC evolves into a meaningful part of the financial sector, countries should consider examining the relationship of VC AML/CFT regulation and supervision to the non-AML/CFT regulation and supervision of VCs (e.g., consumer protection, safety and soundness, insurance, network security, tax compliance). In this regard, it is recommended that countries should consider undertaking short- and longer-term policy work to develop comprehensive regulation of VCPPS if widespread adoption of VC occurs.

32. **Recommendation 14** directs countries to register or license natural or legal persons that provide MVTS in the country, and ensure their compliance with the relevant AML/CFT measures.

This includes subjecting MVTS operating in the country to monitoring for compliance with registration/licensing and other applicable AML/CFT measures.

33. The registration/licensing requirements of Recommendation 14 apply to domestic entities providing convertible VC exchange services between VC and fiat currencies (i.e. VCPPS) in a jurisdiction.

34. Because convertible VC exchangers that transfer value digitally, via the internet, are not subject to territorial boundaries and generally offer VCPPS to persons in countries in which they are not physically present, it is very important that all home countries apply domestic licensing or registration requirements when required by the FATF Recommendations. For the same reasons, proper oversight by the home jurisdiction and adequate cooperation and information exchange between competent authorities between jurisdictions where the entity provides services is of high importance.

35. **Recommendation 15** reinforces the fundamental RBA obligation with respect to new technologies. It requires countries to identify and assess ML/TF risks relating to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Recommendation 15 also requires countries to ensure that financial institutions licensed by or operating in their jurisdiction take appropriate measures to manage and mitigate risk *before* launching new products or business practices or using new or developing technologies. National requirements concerning new technologies should include VCPPS.

36. **Recommendation 16** establishes the requirements for countries with respect to wire transfers. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers. A wire transfer refers to any transaction carried out on behalf of an originator (a) through a financial institution (b) by electronic means with a view to making an amount of funds available to a beneficiary person or (c) at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person. Countries should ensure that when convertible virtual currency exchangers conduct convertible VC transfers that are wire transfers, they include required originator and beneficiary information specified by Recommendation 16. In this regard, countries may adopt a *de minimis* threshold for cross-border wire transfers no higher than USD/EUR 1 000. Countries should also ensure that financial institutions monitor convertible VC transfers to detect those lacking required originator and/or beneficiary information and take appropriate measures to address that situation if it occurs.

37. **Recommendation 26** requires countries to ensure that convertible VC exchangers which act as nodes where convertible VC activities intersect with the regulated fiat currency financial system are subject to adequate regulation and supervision. Countries should consider amending legacy legal frameworks, as needed, to authorize effective AML/CFT regulation of decentralised VC payment mechanisms.

38. **Recommendation 35** directs countries to have a range of effective, proportionate and dissuasive sanctions **(**criminal, civil or administrative) available to deal with natural or legal persons covered by Recommendations 6 and 8 to 23, that fail to comply with the applicable AML/CFT requirements. However, at present, VCPPS, especially decentralised convertible VCPPS, presents

numerous challenges to applying traditional law enforcement tools and conducting successful prosecutions. The current anonymity of most decentralised VC transactions makes it difficult to determine the identities of the persons involved. The underlying protocols on which almost all decentralised VCPPS are currently based do not require or provide identification and verification of participants. Moreover, the historical transactions records generated on the blockchain by the underlying protocols are not necessarily associated with real world identity. This level of anonymity limits the blockchain's usefulness for monitoring transactions and identifying suspicious activity, and presents a significant challenge to law enforcement's ability to trace illicit proceeds that are laundered using decentralised convertible VC. Furthermore law enforcement cannot target one central location or entity for investigative purposes. These challenges undermine countries' ability to employ effective, dissuasive sanctions. Countries should conduct a review of the challenges that exist in their specific country context to identify potential gaps and take action, as appropriate. Licensing or registration of VC-exchangers, and application of customer identification/verification and recordkeeping requirements, could provide a pathway enabling countries to better apply effective and dissuasive sanctions in the VC context.

39. **Recommendations 40** requires countries to provide efficient and effective international cooperation to help other countries combat ML, associated predicate offences and TF—including mutual legal assistance (**Recommendation 37**); help identifying, freezing, seizing and confiscating proceeds and instrumentalities of crime that may take the form of VC (**Recommendation 38**); and effective extradition assistance in the context of virtual currency related crimes (**Recommendation 39**). These requirements may also apply to cooperation that involves VC. It is also important that the FIUs should cooperate and exchange information on the STRs with their counterparts, especially in relation with cross border operations of VC. Sufficient oversight and regulatory control of convertible VCPPS operating in their jurisdiction enables countries to better provide investigatory assistance and other international cooperation in the VC space. At present, the lack of VC regulation and investigation capacity in most countries may present obstacles to countries' ability to provide meaningful international cooperation. Moreover, many countries do not have legal frameworks that allow them to criminalize certain VC ML/TF activities, which could prevent their providing effective MLA in situations where dual criminality is required.

SECTION IV – APPLICATION OF FATF STANDARDS TO COVERED ENTITIES

40. This section explains how specific *FATF Recommendations* should apply to Convertible VC exchanges and any other type of entities that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system, to mitigate the ML/TF risks associated with VCPPSs. These should include applying a RBA (Recommendation 1), customer due diligence (CDD) (Recommendation 10); record-keeping (Recommendation 11); registration or licensing requirements for MVTS (Recommendation 14) identification and mitigation of risks associated with new technologies (Recommendation 15); AML/CFT program requirements (Recommendation 18) and suspicious transaction reporting (Recommendation 20). This section also examines current obstacles to applying some of these mitigating measures in the decentralised VC space. Recommendation 14 is discussed only in section III above, but as noted requires covered entities to comply with registration or licensing requirement in all jurisdiction where they provide VC MVTS.

41. **Recommendation 1.** The *FATF Recommendations* make clear that countries should require financial institutions and DNFBP to identify, assess, and take effective action to mitigate their ML/TF risks (including those associated with VCPPS). This includes on-going efforts to refine technical processes used to reliably identify and verify customers. For AML/CFT purposes, where VC activities are permitted under national law, all jurisdictions, financial institutions and DNFPBs, including convertible virtual currency exchangers, should assess the ML/TF risks posed by VC activities and apply a RBA to ensure that appropriate measures to prevent or mitigate those risks are implemented. The RBA does not imply the automatic or wholesale denial of services to VCPPS without an adequate risks assessment.

42. **Recommendation 10.** CDD is an essential measure to mitigate the ML/TF risks associated with convertible VC. In accordance with the FATF Standards, countries should require convertible VC exchangers to undertake customer due diligence when establishing business relations or when carrying out (non-wire) occasional transactions using reliable, independent source documents, data or information.[9] For example, convertible VC exchangers should be required to conduct customer due diligence when exchanging VC for fiat currency or vice versa in a one-off transaction greater than the designated threshold of USD/EUR 15 000 of USD/EUR 15 000 or (b) carrying out occasional transactions that are wire transfers covered by Recommendation 16 and its Interpretive Note. Usually, convertible VC transactions will involve a wire transfer and therefore be subject to Recommendation 16.

43. Countries may wish to consider having a lower or no threshold for VC CDD requirements if appropriate, given the nature and level of identified ML/TF risks.

44. In light of the nature of VCPPS, in which customer relationships are established, funds loaded and transactions transmitted entirely through the internet, institutions must necessarily rely on non-face-to-face identification and verification. Countries should consider requiring entities providing VCPPS to follow the best practices suggested in the *June 2013 NPPS Guidance*. These, to the extent applicable, include: corroborating identity information received from the customer, such as a

national identity number, with information in third party databases or other reliable sources; potentially tracing the customer's Internet Protocol (IP) address; and searching the Web for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with national privacy legislation.

45. Where convertible VCPPS are presenting higher risk, as ascertained on the basis of the RBA, convertible virtual currency exchangers should be required to conduct enhanced CDD in proportion to that risk, and encouraged to use multiple techniques to take reasonable measures to verify customer identity. Where convertible virtual currency exchangers are permitted to complete verification after establishing the business relationship in order not to interrupt the normal conduct of business (in low risk cases), they should be required to complete verification before conducting occasional transactions above the threshold.

46. Countries should also expect financial institutions and DNFBP to consider risks associated with the source of funding convertible VCPPS. Decentralised convertible VCPPS allow anonymous sources of funding, including peer-to-peer (P2P) VC transfers and funding by NPPS that are themselves anonymous, increasing ML/TF risks. As with NPPS, VCPPS business should consider, for occasional transactions above a given threshold, limiting the source of funds to a bank account, credit or debit card, or at least applying such limitations to initial loading, or for a set period until a transaction pattern can be established, or for loading above a given threshold.

47. Transaction monitoring is a key risk mitigant in the convertible VC space because of the difficulty of non-face-to-face identity verification and because it is only recently that decentralised convertible VC technology allows certain risk mitigants that may be available for NPPS to be built into decentralised VCPPS in order to restrict functionality and reduce risk. For instance, multi-signature (multi-sig) technology now enables VCPPS to effectively build in loading total wallet value, and value/velocity transaction limits into decentralised VCPPS. However, current decentralised VC technology does not make it possible to effectively build in geographic limits; limit use to the purchase of certain goods and services; or prevent person-to-person transfers.

48. It is recommended that countries encourage transaction monitoring, commensurate with the risk. The public nature of transaction information available on the blockchain theoretically facilitates transaction monitoring, but as noted in the *June 2014 VC Report* (Appendix A), the lack of real world identity associated with many decentralised VC transactions limits the blockchain's usefulness for monitoring transactions and identifying suspicious activity, presenting serious challenges to effective AML/CFT compliance and supervision.

49. **Recommendation 11, Recommendation 20 and Recommendation 22**. **Recordkeeping** and **Suspicious activity reporting** when VC transactions could involve the proceeds of criminal activity or be related to terrorist financing, in accordance with Recommendation 20, are also essential. At a minimum, financial institutions and DNFBP should be required to maintain transaction records that include: information to identify the parties; the public keys, addresses *or* accounts involved; the nature and date of the transaction, and the amount transferred. The public information available on the blockchain provides a beginning foundation for record keeping, provided institutions can adequately identify their customers. Countries should require institutions to be attentive to the type of suspicious activity they are in a position to detect.

50. **Recommendation 15 and Recommendation 22** specifically addresses new technologies and requires financial institutions and DNFBP to identify and assess ML/TF risks relating to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Recommendation 15 also requires financial institutions and DNFBP licensed by or operating in a jurisdiction to take appropriate measures to manage and mitigate risk *before* launching new products or business practices or using new or developing technologies. These measures apply in relation to VC as a new technology. National authorities are expected to enforce this obligation, and financial institutions and DNFBP should be proactive in fulfilling the expectations set forth in Recommendation 15.

POTENTIAL SOLUTIONS TO COMPLIANCE CHALLENGES

51. Financial institutions and DNFBP should be required to comply with customer identification and verification and transaction monitoring requirements for decentralised convertible VCPPS, using the most effective and efficient means available, as soon as such products/services are offered. Given the compliance and law enforcement challenges presented by decentralised convertible VC, financial institutions, DNFBP, developers, investors, and other actors in the VC space should seek to develop technology-based solutions that will improve compliance.

52. For example, developers may be able to create new VC technologies, such as application programming interfaces (APIs) that provide customer identification information, or allow financial institutions or DNFBP to limit transaction size and velocity or establish a variety of conditions that must be satisfied before a VC transaction can be sent to the recipient/beneficiary to reduce the ML/TF risks associated with a particular VCPPS. The possibility of using information collected online to augment the customer profile and help in detecting suspicious activity and transactions is another important AML/CFT compliance growth area. Innovation relevant to AML/CFT compliance may take the form of improving existing VC protocols or developing entirely new VCs, built on fundamentally different underlying protocols that can build-in risk mitigants or facilitate customer identification and transaction monitoring.

53. Third-party digital identity systems may also be developed to facilitate AML/CFT compliance that might better fit VCPPS. These systems could, for instance, involve third-party digital identity custodians and/or other entities' creating, authenticating, and maintaining digital identity solutions for specific CDD, monitoring, and reporting purposes, in response to requirements imposed by national AML/CFT laws implementing the international standards. Third party digital identity custodians would themselves need to be regulated to ensure identification/verification integrity.

54. Financial institutions and DNFBP could also explore developing business models to facilitate customer identification/verification, transaction monitoring, and compliance with other relevant AML/CFT requirements. For example, institutions involved in transmitting decentralised convertible VC could consider creating an industry association(s) composed of vetted VC institutions and develop policies and practices for members that allow them to identify specific transactions as coming from a member that has applied appropriate CDD and is conducting appropriate transaction monitoring.

SECTION V - COUNTRY (OR GROUP OF COUNTRIES) EXAMPLES OF RISK-BASED APPROACH TO VCPPS

55. This section gives an overview of the regulatory approaches some countries (or group of countries) have adopted so far as well as the expected approaches by countries in the near future. As mentioned in the introduction, governments around the world are beginning to grapple with the broad range of regulatory challenges presented by VCPPS. A report by the Bank for International Settlements categorizes the measures taken do date as follows.[10]

a) Imposing restrictions on regulated entities for dealing with virtual currencies;

b) Adopting legislative/regulatory measures, such as the need for exchange platforms dealing with VC to be subject to regulation as money remitters, or the proposed regulation of VC intermediaries in some jurisdictions for AML/CFT purposes;

c) Publishing statements cautioning users about risks associated with VC and/or clarifying the position of authorities with respect to VC; and

d) Monitoring and studying developments.

56. The current or contemplated AML/CFT regulatory approaches to VC adopted in a number of jurisdictions as outlined below provide examples of the RBA:

CANADA

57. In June 2014, Canada amended its AML/CFT legislation to treat persons and entities engaged in the business of dealing in VCs as money services businesses (MSBs). Supporting regulations are still under development to define exactly which entities will be covered and their respective obligations. However, it is expected that the obligations will be largely similar to existing MSB obligations, which include registration, CDD (including beneficial ownership information), record keeping and an internal compliance regime, as well as reporting suspicious and certain prescribed transactions.

58. In developing its VC AML/CFT policy, Canada is taking a RBA, including understanding the risks associated with VC in the context of the ML/TF risks faced by Canada, as part of Canada's ML/TF National Risk Assessment. The regulations will balance the needs of mitigating the ML/TF risk with those of fostering continued financial innovation. Therefore, Canada is proposing a targeted regulatory intervention into areas with the greatest ML/TF vulnerabilities.

CHINA

59. On 3rd December of 2013, the People's Bank of China, jointly with the MIIT (Ministry of Industry and Information Technology), the Banking Regulatory Commission (CBRC), the Insurance Regulatory Commission (CIRC) and the Securities Regulatory Commission (CSRC), issued *the Notice on Preventing Risks of Bitcoin*. This notice required institutions which provide services including bitcoin registration, bitcoin wallet and bitcoin exchanging shall fulfill AML/CFT obligations and take

measures to identify its customers and record identification information. Financial institutions and payment services providers were also required to take enhanced monitoring measures on bitcoin service providers to prevent relevant risks. Furthermore, PBC branch offices around the country were required to study bitcoin related ML risks and take commensurate actions including enhanced supervisory actions and enhanced monitoring on suspicious transactions to mitigate risks.

EBA'S OPINION ON "VIRTUAL CURRENCIES"

60. On the 4th July 2014, the European Banking Authority (EBA) issued an Opinion on "virtual currencies", following an analysis of the risks that these new products could present as long as there are not regulated. The EBA opinion is addressed to EU legislators as well as national supervisory authorities in the 28 Member States.

61. The EBA Opinion is built around long term and short term recommendations aiming at establishing a comprehensive regulatory approach.

62. From the EBA perspective, a potential long term regulatory approach would require a substantial body of regulation and would need to comprise, amongst other elements, governance requirements for several market participants, the segregation of client accounts, capital requirements, and the creation of "scheme governing authorities" that are accountable for the integrity of a virtual currencies scheme and its key components, including its protocol and transaction ledge.

63. However, as long as no such regime is in place, the EBA opinion considers that some of the more pressing risks identified will need to be mitigated in other ways. As an "immediate response", the EBA advises national authorities to make financial institutions aware of the risks of, and discourage them from buying, holding or selling virtual currencies. The EBA also recommends that EU legislators consider declaring virtual currency exchanges as 'obliged entities' that must comply with anti-money laundering and counter terrorist financing requirements set out in the EU Anti Money Laundering Directive. Commission negotiations on the 4th Anti-money laundering Directive did not adopt the EBA's July 2014 recommendation. Instead, the Commission will assess options for more comprehensive regulation over the medium term. Its upcoming supranational AML/CFT risk assessment will include an assessment of the risks posed by VC and make appropriate recommendations to Member States.

FRANCE

64. On 29 January 2014, the French Prudential Supervisory and Resolution Authority (ACPR) issued a position statement, emphasizing that an entity engaged in intermediation with respect to the purchase or sale of VC in exchange for fiat currency is a financial intermediary who receives funds on a third party's behalf, and that these activities must be authorised by the ACPR and are therefore subject to AML/CFT requirements. In June 2014, the French FIU, TRACFIN, published a report, "Regulating Virtual Currencies: Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering," intended to establish a framework to deter the use of virtual currencies for fraud and money laundering.

GERMANY

65. The German Federal Supervisory Authority (BaFin) qualifies Bitcoin with legally binding effect as financial instruments in the form of units of account in accordance with section 1 (11) sentence 1 of the German Banking Act (KWG). These units are comparable to currencies, but are not denominated legal tender.

66. Bitcoin are not e-money within the meaning of the German Payment Services Supervision Act (ZAG), because no Bitcoin are issued representing a receivable from an issuer. This is different for virtual currencies, which are backed by a central issuer. Bitcoin are not legal tender either, and therefore qualify as neither currency nor banknotes and coins.

67. Commercial activities related to financial instruments generally do require a license from BaFin. But BaFin has also clarified that the use of Bitcoin as a substitute currency for trade payments itself is not an activity subject to authorisation under the KWG. Mining of Bitcoin per se is not an activity subject to authorisation either, because miners do not issue or place any Bitcoin themselves. The same applies to the purchase or sale of mined or acquired Bitcoin, which does not require authorisation either.

68. However, an authorisation requirement may arise if there are additional factors. Often Bitcoin are traded via internet platforms, some of which are referred to as exchanges. Such activities generally do require authorisation by BaFin. Which authorisation is required can only be determined by analysing the technical and contractual implementation of the transactions in detail. Some may carry on investment broking as defined in the KWG, others may operate a multilateral trading facility, which is a financial service specified in the KWG. There are some, that might be regarded as principal broking services. If potential buyers and sellers are merely introduced to each other on platforms, this does not constitute the brokering of specific transactions. In such cases, however, the providers on these types of platforms are proprietary traders subject to an authorisation requirement within the meaning of the KWG. Providers acting as exchange bureaus that offer to change legal currencies directly into Bitcoin also meet the criterion of proprietary trading subject to an authorisation requirement.

69. Since each case is different, mining pools, i.e. the pooling of computer processing power in general by several persons for the purpose of jointly generating Bitcoin, are not necessarily subject to supervision. As a general rule, if several persons use processing power with equal rights and subsequently distribute the Bitcoin proportionately, this is not an activity that requires authorisation. Different rules may apply if the pool operator commercially offers a share of the revenue from mined or sold Bitcoin against the provision of processing power and the participants have no control over the specific processes, for example.

70. BaFin receives a growing number of enquiries on derivative and fund-like products related to Bitcoin. Again, since each case is different, they are not necessarily subject to supervision. In general, however, if traded commercially, these types of products are subject to the supervisory rules of the KWG or the KAGB, because products derived from a financial instrument are themselves financial instruments or at least represent asset management. The commercial operation of a bitcoin ATM is normally also a banking or financial service subject to an authorisation requirement – depending on

the way the purchase processes and legal relationships are arranged between buyer, seller and – in some cases – operator.

71. BaFin assumes that a business is carried on in Germany not only if the service provider's registered office or habitual residence is in Germany, but also if it is located abroad and the service provider targets the market to repeatedly and commercially offer banking or financial services to companies or persons whose registered office or habitual residence is in Germany. However, this does not affect the passive freedom to provide services, i.e. the right of persons and companies resident in Germany to request services from a foreign provider under their own initiative. Transactions that have been entered into because the customer has taken the initiative do not, therefore, require authorisation under the KWG. For online offerings relating to financial market products, the relevant criterion is whether analysis of the website as a whole reveals that the services offered are targeted at the German market. A disclaimer is only one of many indicators. Other indications include the domain and top-level domain, the language or other country-specific references and the legal framework.

72. Banks and financial services providers already holding an authorisation to trade in financial instruments are also permitted to engage in transactions with Bitcoin without being subject to any further authorisation requirements. In all these cases the authorised institution is also an obliged entity under AML-legislation.

HONG KONG, CHINA

73. Hong Kong, China has taken a very cautious approach since mid-2013 in reminding the public of the consumer, money laundering and cyber crime risks associated with any trading or dealing in virtual currencies and virtual commodities, such as Bitcoin. Hong Kong, China does not regulate such virtual commodities per se, as they are not "currency", "securities" or "legal tender" in existing legislation. Likewise, operators or dealers providing services in relation to virtual commodities do not fall within the definition of a "money service business" under the Anti-Money Laundering and Counter Terrorist Financing (Financial Institutions) Ordinance, unless their services or transactions involve money changing or remittance services. That said, financial institutions, virtual commodity dealers or operators, or individuals are subject to a statutory duty to report suspicious transactions to the Joint Financial Intelligence Unit, if their due diligence work or transactions reveal any suspicious activities in relation to money laundering or terrorist financing, regardless of whether virtual commodities are involved. A failure to disclose such suspicious transactions may amount to a criminal offence. Existing laws also cover acts of fraud, technology crimes, pyramid scheme, money laundering or terrorist financing involving virtual commodities. In addition, regulators have issued guidance to financial institutions to remind them to ensure an escalated level of vigilance commensurate with money laundering and terrorist financing risks associated with virtual commodities. Financial institutions have been reminded to exercise caution in assessing relevant money laundering or terrorist financing risks when establishing or maintaining business relationships with customers and clients who are operators of any schemes or businesses relating to virtual commodities.

ITALY

74. In Italy virtual currencies are not considered legal tender. In January 2015, Bank of Italy issued a warning on the use of so-called virtual currencies [11] and a communication, included in Supervisory Bulletin n.1, 2015, which endorses the EBA "Opinion on 'virtual currencies'"; the latter discourages banks and other supervised financial intermediaries from buying, holding or selling virtual currencies. In the same date, the Italian Financial Intelligence Unit issued a communication on the anomalous use of virtual currencies and on the detection of suspicious money laundering or terrorist financing transactions by obliged entities[12].

RUSSIA

75. Pursuant to Article 27 of Federal law "On the Central Bank of the Russian Federation (Bank of Russia)", issuing monetary surrogates is prohibited in the Russian Federation. In January 2014 the Central Bank of the Russian Federation released "Information on virtual currencies, particularly Bitcoin, used for conducting transactions" on its official website. The Bank of Russia warns individuals, legal entities and, primarily, credit institutions and non-credit financial institutions, against the use of virtual currencies in exchange for goods, services or real currency in rubles or foreign currency. Due to the anonymous nature of the issue of virtual currencies by an unlimited number of persons and use of such currencies for conducting transactions, individuals and legal entities may unwittingly become involved in illegal activities, including ML/FT. Therefore, exchanging virtual currencies for real currency in rubles or foreign currency, as well as for goods and services, will be viewed by the Bank of Russia as potential involvement of a legal entity in conducting suspicious transactions specified in the current AML/CFT legislation.

76. With the view to mitigating ML/FT risks associated with virtual currencies, the Ministry of Finance, jointly with the Bank of Russia, developed the draft law imposing a ban on electronic monetary surrogates and electronic monetary surrogates transactions. The Draft has been prepared and will be introduced into the Parliament (State Duma).

SINGAPORE

77. In March 2014, the Monetary Authority of Singapore (MAS) announced it will regulate VC intermediaries operating in Singapore to address potential ML/TF risks. The MAS will introduce regulations requiring VC intermediaries that buy, sell or facilitate the exchange of VCs for fiat currencies to verify customer identity and report suspicious transactions. The proposed regulations do not address the safety and soundness of VC intermediaries, nor the proper functioning of VC transactions.

78. The proposed regulatory framework for virtual currency intermediaries has not been implemented yet. The current intention is to only regulate virtual currency intermediaries that operate in Singapore; i.e. those which have a physical presence in the country. However, as the virtual currency space is evolving rapidly, Singapore will continue to closely monitor the regulatory approaches taken towards virtual currencies by other jurisdictions. If necessary, MAS will consider additional measures to address the risks posed by virtual currencies and their intermediaries.

SOUTH AFRICA

79. The National Treasury issued a user alert to the monitoring of virtual currency on 18 September 2014.[13] This was a combined statement between the National Treasury, the South African Reserve Bank, the Financial Services Board, the South African Revenue Service and the Financial Intelligence Centre to warn members of the public to be aware of the risks associated with the use of virtual currencies for either transactions or investments.

80. Currently in South Africa there are no specific laws or regulations that address the use of virtual currencies. Consequently, no legal protection or recourse is afforded to users of virtual currencies. Due to their unregulated status in South Africa, virtual currencies cannot be classified as legal tender as any merchant may refuse them as a payment instrument without being in breach of the law. Virtual currencies also cannot be regarded as a means of payment as they are not issued on receipt of funds. Dealing in virtual currencies is, therefore, performed at the user's own risk with no recourse to the South African authorities. The South African authorities will continue to monitor and assess the use of virtual currencies and consult with private sector stakeholders in this regard. Further guidance or regulations may be issued, should the need arise.

SWITZERLAND

81. In June 2014, the Swiss Government published a study and policy statement on VC, the *Federal Council Report on Virtual Currencies in Response to the Schwaab (13.3687) and Weibel (13.4070) Postulates*,[14] which declared that "Professional trade in virtual currencies and the operation of trading platforms in Switzerland generally come under the scope of the *Anti-Money Laundering Act*." Entities engaged in these activities are required to comply "with the obligation to verify the identity of the contracting party and establish the identity of the beneficial owner." At the same time, Swiss Financial Market Supervisory Authority (FINMA) published a fact sheet,[15] emphasizing that the purchase and sale of convertible VC on a commercial basis and the operation of trading platforms used to transfer money or convertible VC from a platform's users to other users are subject to Switzerland's Anti-Money Laundering Act. Before commencing operations, a provider of these kinds of services must either become a member of a self-regulatory organisation (SRO) or apply to FINMA for a license to operate as a directly supervised financial intermediary (DSFI). Where decentralised VC trading activities fall under the Anti- Money Laundering Act, compliance with CDD obligations is mandatory. Because convertible VC can facilitate anonymity and cross-border asset transfers, FINMA considers trading in it to have heightened ML/TF risks, requiring strict CDD, particularly as regards client identification. Commercial activities involving convertible VC require a banking license when an organisation, as part of its business activities, accepts convertible VC from clients and administer VC holdings for clients. VC entities that obtain banking licenses are subject to prudential supervision by FINMA, which will monitor the company on an ongoing basis to ensure that it complies with the relevant regulations. The Federal Council is continuing to monitor developments in the area of VCs to identify any need for additional action at an early stage.

UNITED KINGDOM

82. UK Government's plans for virtual currencies: in November 2014, the UK Government published a Call for Information to gather evidence on the benefits and risks associated with virtual (digital) currencies, with a particular focus on the question of regulation. The Call for Information closed in December 2014. In March 2015, the UK Government published a summary of the evidence gathered through the Call for Information, and announced that it intends to apply anti-money laundering regulation to digital currency exchanges in the UK. The UK Government plans to formally consult on the detail of the proposed regulatory approach later this year.

83. UK's efforts to improve its understanding of the risks with regards virtual currencies: The level of understanding of the risk around VC in the UK has improved. The UK's National Crime Agency (NCA) is leading a multi-agency response to evaluating and responding to the threat posed by the criminal use of VCs, involving the Crown Prosecution Service, HM Revenue &Customs, City of London Police, HM Treasury, Bank of England, Financial Conduct Authority, Home Office and the Metropolitan Police Service.

84. This work includes building the intelligence picture. An NCA assessment has provided a baseline for law enforcement on the threat posed by the criminal use of VCs. An improved intelligence picture will be the basis for operational targeting, and is also being fed into policy makers to inform decision making about government intervention. Capacity building work includes awareness raising with industry and Forces. In addition, much of this activity is being mirrored at the international level, which is important given the cross border nature of the problem.

UNITED STATES

85. The United States regulates any natural and legal person—including convertible VC exchangers and administrators—engaged in the acceptance and transmission of convertible VC from one person to another person or location as money transmitters, subject to AML/CFT obligations, including registration, customer identification, record-keeping and reporting requirements. The federal AML/CFT regulation covers both centralised and decentralised convertible VCs and applies to persons engaged in transmitting convertible VC on behalf of a third person without also exchanging VC back-and-forth for fiat currency. It also applies to foreign-located convertible VC exchangers/administrators that have no physical presence in the United States, but that do business in whole or substantial part within the United States. Current U.S. Government AML/CFT regulations do not apply to users of convertible VC who are using the VC without engaging in money transmission. In addition to federal regulations, 48 states regulate money transmitters, and many are considering how their legacy AML/CFT and prudential regulation of money transmitters may apply to VCs. For example, the New York Financial Services Department (NYFSD) has announced that it will shortly issue a regulation requiring some virtual currency businesses to obtain "bitlicenses" and comply with AML/CFT obligations, consumer disclosure rules, capital requirements, and investment rules.

86. The U.S. undertook legal changes in order to accommodate changing financial technology. Recognizing that AML/CFT protections must keep pace with the emergence of new payment systems, in July 2011, FinCEN amended its rule dealing with Money Services Businesses (MSBs)

generally[16], providing the flexibility needed to accommodate VC payments innovations under the existing Bank Secrecy Act (BSA) regulatory framework. The amended MSB added the phrase, "other value that substitutes for currency" to the definition of "money transmission services" and thereby changed the definition of money transmitter MSBs. As a result of this regulatory change, "money transmission services" is now defined as "the acceptance of currency, funds, *or other value that substitutes for currency* from one person *and* the transmission of currency, funds, *or other value that substitutes for currency* to another location or person by any means."[17] A "money transmitter" is a person (individual or entity) that provides money transmission services or any other person engaged in the transfer of funds. Since "money transmission services," is defined as "the acceptance of currency, funds, *or other value that substitutes for currency* from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means," the United States is able to regulate any legal or natural person engaged in accepting convertible VC from one person and transmitting it to another person or location, thus covering, among others, convertible virtual currency exchangers and administrators as money transmitters.

NOTES

1 For example, a U.S-based Bitcoin wallet provider/exchanger/payments processor, links the customer's VC wallet to a bank account or traditional charge or debit card for funding VC purchases and receiving VC cash-out. A UK-based Bitcoin remittance service in the UK-Kenya corridor links to a Kenyan mobile payments system at the delivery end. A Bitcoin exchange operating in Europe recently added branded network credit and debit cards to its available funding options, which already included Single Euro Payments Area (SEPA) bank **transfers**. A Bitcoin exchange headquartered in Australia, with customers in over 40 countries, sends remittances directly to the beneficiary's bank account without the recipient using Bitcoin, but with the backend of the remittance conducted entirely in bitcoins.

2 FATF (2013), *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet Based Payment Services*, FATF, Paris, France, www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-npps-2013.html

3 **Convertible** means that the virtual currency can be exchanged for fiat currency.

4 A **virtual currency exchanger** is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.

5 Since VC can function as a medium of exchange, unit of account, and/or store of value, it may raise issues across a number of complementary regulatory jurisdictions, including, e.g., commodities and securities regulation.

6 The FATF Standards comprise the FATF Recommendations and their Interpretive Notes.

7 *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (FATF, 2014).

8 The FATF defines MVTS as financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and **may include any new payment methods…** [emphasis added].

9 For the complete list of activities covered by the definition of "financial institutions," see the *FATF Recommendations* Glossary.

10 Non-Banks in retail payments, Committee on Payments and Market Infrastructures, Bank for International Settlements (September 2014)

11 www.bancaditalia.it/compiti/vigilanza/avvisi-pub/index.html

12 http://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione_UIF_su_VV.pdf

13 National Treasury (2014), *Monitoring of virtual currencies, National Treasury, Republic of South Africa,* available from www.treasury.gov.za/comm_media/press/2014

14 Available at www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf

15 Available at www.finma.ch/e/finma/publikationen/faktenblaetter/Documents/fb-bitcoins-e.pdf

16 The *Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses*, 76 FR 43585 (July 21, 2011), 31 CFR § 1010.100(ff)(5)(i)(A) (the MSB Rule). At almost the same time, FinCEN also issued a new Final Rule dealing with prepaid access (*Final Rule – Definitions and Other Regulations Relating to Prepaid Access*, 76 FR 45403 (July 29, 2011), 31 CFR § 1010.100(ww)(5)(i)(A) (the Prepaid Access Rule)).

17 31 CFR § 1010.100(ff)(5)(i)(A) (emphasis added).

APPENDIX A

VIRTUAL CURRENCIES - KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS[1]

Appendix A was originally published by the FATF as a stand-alone paper in June 2014

INTRODUCTION

As decentralised, math-based virtual currencies—particularly Bitcoin[2]—have garnered increasing attention, two popular narratives have emerged: (1) virtual currencies are the wave of the future for payment systems; and (2) virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities.[3] Against this backdrop, this paper builds on the 2013 New Payment Products and Services (NPPS) Guidance (FATF, 2013) by suggesting a conceptual framework for understanding and addressing the anti-money laundering / countering the financing of terrorism (AML/CFT) risks associated with one kind of internet-based payment system: virtual currencies. Specifically, the paper proposes a common definitional vocabulary that clarifies what virtual currency is and classifies the various types of virtual currency, based on their different business models and methods of operation,[4] and identifies the participants in typical virtual currency systems. It also applies risk factors set forth in Section IV (A) of the 2013 NPPS Guidance to specific types of virtual currencies to identify potential risks; describes some recent investigations and enforcement efforts involving virtual currency; and presents a sample of jurisdictions' current regulatory approaches to virtual currency.

While the 2013 NPPS Guidance broadly addressed internet-based payment services, it did not define "digital currency," "virtual currency," or "electronic money." Nor did it focus on virtual currencies, as distinct from internet-based payment systems that facilitate transactions denominated in real money (fiat or national currency) (e.g., Pay-Pal, Alipay, or Google Checkout). It also did not address decentralised convertible virtual currencies, such as Bitcoin. The 2013 Guidance also notes that, "[g]iven the developing nature of alternate online currencies, the FATF may consider further work in this area in the future" (2013 NPPS Guidance, p. 11, para. 29). A short-term typologies project on this basis was initiated with the following objectives:

- develop a risk-matrix for virtual currencies (or perhaps, more broadly, for both virtual currencies and e-money);
- promote fuller understanding of the parties involved in convertible virtual currency systems and the way virtual currency can be used to operate payment systems; and
- stimulate a discussion on implementing risk-based AML/CFT regulations in this area.

This typologies project may lead to policy work by the FATF, e.g. the issuance of supplemental guidance for applying a risk-based approach to virtual currencies that would incorporate the proposed vocabulary and risk-matrix developed by the typologies project and explain how specific FATF Recommendations apply in the context of virtual currency.

KEY DEFINITIONS:

A common set of terms reflecting how virtual currencies operate is a crucial first step to enable government officials, law enforcement, and private sector entities to analyse the potential AML/CFT risks of virtual currency as a new payment method. As regulators and law enforcement officials around the world begin to grapple with the challenges presented by virtual currencies, it has become apparent that we lack a common vocabulary that accurately reflects the different forms virtual currency may take. The following set of terms is intended to aid discussion between FATF members. It is important to note that this vocabulary may change as virtual currency evolves and as regulators and law enforcement/government officials continue to consider the challenges virtual currencies present. Nevertheless, the proposed vocabulary aims to provide a common language for developing conceptual tools to help us better understand how virtual currencies operate and the risks and potential benefits they offer.

VIRTUAL CURRENCY

Virtual currency is a digital representation[5] of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment)[6] in any jurisdiction.[7] It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from **fiat currency** (a.k.a. **"real currency," "real money,"** or **"national currency"**), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e**-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.

Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term "virtual currency". In this paper to avoid confusion, only the terms "virtual currency" or "e-money" are used.

CONVERTIBLE VERSUS NON-CONVERTIBLE VIRTUAL CURRENCY

This paper proposes dividing virtual currency into two basic types: convertible and non-convertible virtual currency.[8] Although the paper uses "non-convertible" and "closed", and "convertible" and "open" as synonyms, it should be emphasised that the notion of "convertible currency" does not in any way imply an ex officio convertibility (e.g. in the case of gold standard), but rather a de facto convertibility (e.g. because a market exists). Thus, a virtual currency is "convertible" only as long as

some private participants make offers and others accept them, since the "convertibility" is not guaranteed at all by law.

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency.[9] Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney.[10]

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon.com, and under the rules governing its use, cannot be exchanged for fiat currency. Examples include**:** Project Entropia Dollars; Q Coins; and World of Warcraft Gold.

It should be noted that even where, under the terms set by the administrator, a non-convertible currency is officially transferrable only within a specific virtual environment and is not convertible, it is possible that an unofficial, secondary black market may arise that provides an opportunity to exchange the "non-convertible" virtual currency for fiat currency or another virtual currency. Generally, the administrator will apply sanctions (including termination of membership and/or forfeiture of remaining virtual currency) to those seeking to create or use a secondary market, contrary to the rules of the currency.[11] Development of a robust secondary black market in a particular "non-convertible" virtual currency may, as a practical matter, effectively transform it into a convertible virtual currency. A non-convertible characterisation is thus not necessarily static.

CENTRALISED VERSUS NON-CENTRALISED VIRTUAL CURRENCIES

All non-convertible virtual currencies are centralised: by definition, they are issued by a central authority that establishes rules making them non-convertible. In contrast, convertible virtual currencies may be either of two sub-types: centralised or decentralised.

Centralised Virtual Currencies have a single administrating authority (**administrator)**—i.e., a third party[12] that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible virtual currency may be either **floating**—i.e., determined by market supply and demand for the virtual currency--or **pegged**—i.e., fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payments transactions involve centralised virtual currencies. Examples: E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life "Linden dollars"; PerfectMoney; WebMoney "WM units"; and World of Warcraft gold.

Decentralised Virtual Currencies (a.k.a. crypto-currencies) are distributed[13], open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight. Examples: Bitcoin; LiteCoin; and Ripple.[14]

Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically

signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the "block reward" and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block). Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof-of-work system to validate transactions and maintain the block chain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods, such as systems based on proof-of-stake.

Bitcoin, launched in 2009, was the first decentralised convertible virtual currency, and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into US dollars, Euros, and other fiat or virtual currencies. Anyone can download the free, open-source software from a website to send, receive, and store bitcoins and monitor Bitcoin transactions. Users can also obtain Bitcoin addresses, which function like accounts, at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that is not systematically linked to an individual.. Therefore, Bitcoin is said to be "pseudo-anonymous". Bitcoin is capped at 21 million bitcoins (but each unit could be divided in smaller parts), projected to be reached by 2140.[15] As of April 2, 2014, there were over 12-and-a-half million bitcoins, with total value of slightly more than USD 5.5 billion, based on the average exchange rate on that date.

Altcoin refers to math-based decentralised convertible virtual currency other than bitcoins, the original such currency. Current examples include Ripple; PeerCoin, Lite-coin; zerocoin; anoncoin and dogecoin. One popular exchanger, Cryptsy, would reportedly exchange over 100 different virtual currencies (as of 2 April 2014). (Popper, N., 2013)

Anonymiser (anonymising tool) refers to tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity. (Examples: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer)).

Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed. (Examples: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Tor (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by

routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network. This difficulty can be exacerbated by use of additional tumblers or anonymisers on the Tor network. Tor is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity.

Dark Wallet is a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer); decentralised trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralised market places similar to Silk Road.

Cold Storage refers to an offline Bitcoin wallet—i.e., a Bitcoin wallet that is not connected to the Internet. Cold storage is intended to help protect the stored virtual currency against hacking and theft.

Hot Storage refers to an online bitcoin wallet. Because it is connected to the Internet, hot storage is more vulnerable to hacking/theft than cold storage.

Local Exchange Trading System (LETS) is a locally organised economic organisation that allows members to exchange goods and services with others in the group. LETS use a locally created currency to denominate units of value that can be traded or bartered in exchange for goods or services. Theoretically, bitcoins could be adopted as the local currency used within a LETS. (Examples: Ithica Dollars; Mazacoin).

VIRTUAL CURRENCY SYSTEM PARTICIPANTS

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

An **administrator** is a person or entity engaged as a business in **issuing** (putting into circulation) a centralised virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to **redeem** (withdraw from circulation) the virtual currency.

A **user** is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralised virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an

online survey, provide a real or virtual good or service); (3) with some decentralised virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them (see definition of miner, below),and receive them as gifts, rewards, or as part of a free initial distribution.

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

Virtual currency wallet is a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency.

A wallet provider is an entity that provides a virtual currency wallet (i.e., a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency). A wallet holds the user's private keys, which allow the user to spend virtual currency allocated to the virtual currency address in the block chain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. For example, beyond providing bitcoin addresses, the wallet may offer encryption; multiple key (multi-key) signature protection, backup/cold storage; and mixers. All Bitcoin wallets can interoperate with each other. Wallets can be stored both online ("hot storage") or offline ("cold storage"). (Examples: Coinbase; Multibit; Bitcoin Wallet).

In addition, various **other entities** may participate in a virtual currency system and may be affiliated with or independent of exchangers and/or administrators. These include web **administration service providers (a.k.a. web administrators**); **third party payments senders** facilitating merchant acceptance; **software developers**; and **application providers** (some of the "other entities" listed in this paragraph may already fall into one of the categories above.). Applications and software development can be for legitimate purposes—e.g., to increase ease of merchant acceptance and customer payments or to respond to legitimate privacy concerns—or for illicit purposes—e.g., a mixer developer/operator can target illicit users with products designed to avoid regulatory and law enforcement scrutiny.

It must be emphasised that this list of participants is not exhaustive. Moreover, given the rapid development of virtual currency technologies and business models, additional participants could arise within virtual currency systems and pose potential AML/CFT risks.

Taxonomy of Virtual Currencies

	Centralised	Decentralised
Convertible	Administrator, exchangers, users; third-party ledger; can be exchanged for fiat currency. Example: WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger; can be exchanged for fiat currency. Example: Bitcoin
Non-convertible	Administrator, exchangers, users; third-party ledger; cannot be exchanged for fiat currency. Example: World of Warcraft Gold	Does not exist

LEGITIMATE USES

Like other new payment methods, virtual currency has legitimate uses, with prominent venture capital firms investing in virtual currency start-ups. Virtual currency has the potential to improve payment efficiency and reduce transaction costs for payments and fund transfers. For example, Bitcoin functions as a global currency that can avoid exchange fees, is currently processed with lower fees/charges than traditional credit and debit cards, and may potentially provide benefit to existing online payment systems, like Paypal.[16] Virtual currency may also facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the Internet, such as one-time game or music downloads. At present, as a practical matter, such items cannot be sold at an appropriately low per/unit cost because of the higher transaction costs associated with e.g., traditional credit and debit. Virtual currency may also facilitate international remittances and support financial inclusion in other ways, as new virtual currency-based products and services are developed that may potentially serve the under- and un-banked. Virtual currency - notably, Bitcoin- may also be held for investment. These potential benefits need to be carefully analysed, including whether claimed cost advantages will remain if virtual currency becomes subject to regulatory requirements similar to those that apply to other payments methods, and/or if exchange fees for cashing out into fiat currency are factored in, and whether volatility, consumer protection and other factors[17] limit their potential for financial inclusion.

POTENTIAL RISKS

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many of the reasons identified in the 2013 NPPS Guidance. First, they may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding

source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.

Virtual currency's global reach likewise increases its potential AML/CFT risks. Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

LAW ENFORCEMENT ACTIONS INVOLVING VIRTUAL CURRENCY

Law enforcement is already seeing cases that involve the abuse of virtual currency for money laundering purposes. Examples include:

LIBERTY RESERVE

In what is to date the largest online money-laundering case in history, in May 2013, the US Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than 6 billion USD in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the US financial system.

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

To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names ("Russia Hackers," "Hacker Account," "Joe Bogus") and blatantly false addresses ("123 Fake Main Street, Completely Made Up City, New York"). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers—generally, unlicensed money transmitting businesses operating in Russia, and in several countries without significant governmental money laundering oversight or regulation at that time, such as Malaysia, Nigeria, and Vietnam. By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other users, including front company "merchants" that accepted LR as payment. For an extra "privacy fee" (75 US cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable. After learning it was being investigated by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain and elsewhere.[18]

SILK ROAD

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering conspiracies. The Justice Department also seized the website and approximately 173 991 bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware. The individual was arrested in San Francisco in October and indicted in February 2014; the investigation is ongoing.

Launched in January 2011, Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers, a third of whom are believed to have been in the United States. It allegedly generated total sales revenue of approximately USD 1.2 billion (more than 9.5 million bitcoins) and approximately USD 80 million (more than 600 000 bitcoins) in commissions for Silk Road. Hundreds of millions of

dollars were laundered from these illegal transactions (based on bitcoin value as of dates of seizure). Commissions ranged from 8 to 15 percent of total sales price.

Silk Road achieved anonymity by operating on the hidden Tor network and accepting only bitcoins for payment. Using bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since senders and recipients of peer-to-peer (P2P) bitcoin transactions are identified only by the anonymous bitcoin address/account. Moreover, users can obtain an unlimited number of bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users can also employ additional "anonymisers," beyond the tumbler service built into Silk Road transactions (see discussion below).

Silk Road's payment system functioned as an internal Bitcoin bank, where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address (and potentially thousands) associated with the user's Silk Road account, stored on wallets maintained on servers controlled by Silk Road. To make a purchase, a user obtained bitcoins (typically through a Bitcoin exchanger) and sent them to a Bitcoin address associated with his or her Silk Road account to fund the account. When a purchase was made, Silk Road transferred the user's bitcoins to an escrow account it maintained, pending completion of the transaction, and then transferred the user's / buyer's bitcoins from the escrow account to the vendor's Silk Road Bitcoin address. As a further step, Silk Road employed a "tumbler" for every purchase, which, as the site explained, "sen[t] all payments through a complex, semi-random series of dummy transactions ... --making it nearly impossible to link your payment with any [bit]coins leaving the site."[19]

WESTERN EXPRESS INTERNATIONAL

An eight-year investigation of a multinational, Internet-based cybercrime group, the Western Express Cybercrime Group, resulted in convictions or guilty pleas of 16 of its members for their role in a global identity theft/cyberfraud scheme. Members of the cybercrime group interacted and communicated primarily through Internet "carding" web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous virtual currency accounts to conceal the existence and purpose of the criminal enterprise; avoid detection by law enforcement and regulatory agencies; and maintain their anonymity.

The criminal enterprise was composed of vendors, buyers, cybercrime services providers, and money movers located in numerous countries, ranging from Ukraine and throughout Eastern Europe to the United States. The vendors sold nearly 100 000 stolen credit card numbers and other personal identification information through the Internet, taking payment mostly in e-Gold and WebMoney. The buyers used the stolen identities to forge credit cards and purchase expensive merchandise, which they fenced (including via reshipping schemes), committing additional crimes, such as larceny, criminal possession of stolen property, and fraud, and generating about USD 5 million in credit card fraud proceeds. The cybercrime services providers promoted, facilitated, and aided in the purchase, sale and fraudulent use of stolen credit card numbers and other personal identifying information by providing computer services to the vendors and the

buyers. The money mover laundered the cybercrime group's illicit proceeds in a variety of high-tech ways, moving more than USD 35 million through various accounts.

The hub of the entire operation was Western Express International, Inc., a New York corporation based in Manhattan that operated as a virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group's proceeds. One of the largest virtual currency exchangers in the United States, Western Express International exchanged a total of USD 15 million in WebMoney and USD 20 million in e-Gold for the cybercrime group and used banks and traditional money transmitters to move large sums of money. It also provided information and assistance through its websites (including Dengiforum.com and Paycard2000.com) on ways to move money anonymously and to insulate oneself from reporting requirements.

Western Express International and its owner/operator, a Ukrainian national, plead guilty in February 2013 in New York State to money laundering, fraud, and conspiracy offenses. (In February 2006, Western Express was also indicted for running an illegal check cashing/wire transfer service.) Three other defendants were convicted after trial in June 2013; several more plead guilty in August 2009. Two indicted defendants remain fugitives. The investigation was conducted jointly by the US Secret Service and the Manhattan (New York County) District Attorney's Office and was successfully prosecuted by the Manhattan District Attorney's Office.

NOTES

1 The first draft of this paper was prepared jointly by Australia, Canada, Russia, the United Kingdom and the United States for the FATF meetings in February 2014. After that all delegations were invited to provide comments on the draft with a view to adopting a final paper at the next meeting. Comments were received from 10 delegations, and these have been taken into account in preparing this revision.

2 "Bitcoin" (capitalised) refers to both the open source software used to create the virtual currency and the peer-to- peer (P2P) network formed as a result; "bitcoin" (lowercase) refers to the individual units of the virtual currency.

3 It should also be noted that some observers, including former US Federal Reserve Chairman Alan Greenspan, Nout Wellink, a former President of the Dutch Central Bank, and Nobel Laureate economist Robert Shiller, maintain that virtual currency is a passing fad or bubble, akin to Tulipmania in 17th Century Netherlands.

4 Virtual currency is a complex subject that implicates not only AML/CFT issues, but also other regulatory matters, including consumer protection, prudential safety, tax and soundness regulation, and network IT security standards. The proposed vocabulary is thus relevant across a number of complementary regulatory jurisdictions. Adoption of consistent terms and a common conceptual understanding of virtual currency by all relevant government entities is important to avoid duplicating efforts and/or working at unintended cross purposes, and facilitates the capacity of governmental authorities to leverage their various perspectives and areas of expertise in order to most effectively identify and address relating to virtual currencies.

5 **Digital representation** is a representation of something in the form of digital data—i.e., computerised data that is represented using discrete (discontinuous) values to embody information, as contrasted with continuous, or analog signals that behave in a continuous manner or represent information using a continuous function. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency, but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the virtual currency system.

6 Legal tender status does not necessarily require an entity or individual to accept payment in a particular type of legal tender. For example, in many jurisdictions, a private business, person, or organisation is free to develop internal policies on whether or not to accept the jurisdiction's physical currency or coins (cash) as payment for goods and/or services.

7 This definition differs from that offered in 2012 by the European Central Bank (ECB), which defined virtual currency "as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" ECB, *Virtual Currency Schemes* (October 2012), p. 6. The ECB recognised on p.13 of its report that its "definition may need to be adapted in future if fundamental characteristics change." Its definition now appears too limited, since math-based, decentralised virtual currencies like Bitcoin are not issued and controlled by a central developer, and some jurisdictions (e.g., the United States, Sweden, and Thailand) now regulate virtual currencies.

8 This categorisation differs from the ECB's three-part classification, which divides virtual currencies into three types: "Type 1 . . . refer[s] to closed virtual currency schemes . . . used in an online game. Type 2 . . . [refers to] schemes [that] have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can ... be used to buy virtual goods and services . . . (and exceptionally also ... real goods and services) . . . Type 3 [refers to] schemes . . .[with] bidirectional flows, i.e. the virtual currency . . . acts like any . . . convertible [real] currency, with . . . [buy and sell] exchange rates . . . [and] can . . . be used to buy [both] virtual . . . [and] real goods and services." ECB *Virtual Currency Schemes,* p. 6. This discussion paper adopts a simpler, bifurcated classification because at present, only (fully) convertible virtual currencies that can be used to move value into and out of the formal financial sector present significant AML/CFT risks. This is because money laundering requires: Conversion or transfer (of illicit funds); concealment or disguise of the source/origin (of illicit funds); or acquisition/possession/use (of illicit funds).

9 Some convertible virtual currencies can be exchanged directly through the issuing administrator (directly exchanged); others must be exchanged through a virtual currency exchanger (third-party exchanged).

10 For example, WebMoney is a virtual currency because "valuables" (assets) are transferred and stored in the form of a non-fiat currency, The units of measurement of the valuables' property rights stored by the guarantor are WebMoney Title Units (WM) of the corresponding type. http://wmtransfer.com/eng/about/

11 For example, despite such deterrence measures, several exchanges allow blackmarket conversion of World of Warcraft Gold.

12 A third-party is an individual or entity that is involved in a transaction but is not one of the principals and is not affiliated with the other two participants in the transaction—i.e., a third party functions as a neutral entity between the principals (e.g., sender and receiver, buyer and seller) in a business or financial transaction. The third party's involvement varies with the type of business or financial transaction. For example, an online payment portal, such as PayPal, acts as a third party in a retail transaction. A seller offers a good or service; a buyer uses a credit or debit card entered through the PayPal payment service; and the trusted third party completes the financial transfer. Similarly, in a real

estate transaction, a third-party escrow company acts as a neutral agent between the buyer and seller, collecting the documents from the seller and money from the buyer that the two principals need to exchange to complete the transaction.

13 Distributed is a term of art that refers to an essential feature of decentralised math-based virtual currencies: transactions are validated by a *distributed* proof-of-work system. Each transaction is *distributed* among a network of participants who run the algorithm to validate the transaction.

14 Apart from the initial creation and issuance of ripple coins (RXP), Ripple operates as a decentralised virtual currency. Ripple's founders created all 100 billion ripple coins and retained 20 billion of them, with the remainder to be distributed by a separate entity, Ripple Labs. However, all transactions are verified by a decentralised computer network, using Ripple's open source protocol, and recorded in a shared ledger that is a constantly updated database of Ripple accounts and transactions.

15 In 2140, the block award will cease to be available and miners will be rewarded only by transaction fees.

16 For example, PayPal is actively looking at accepting and clearing bitcoins on the PayPal platform, and JP Morgan Chase has filed a US patent application for an online electronic payments system using a math-based virtual currency protocol that would enable users to make anonymous payments without providing an account number or name, with the virtual currency to be stored on JPMC computers and verified through a shared log, much like the 'block chain' in the bitcoin system.

17 For instance, it remains to be seen whether virtual currency systems can provide a pathway to other financial services, like credit and insurance.

18 The Liberty Reserve investigation and takedown involved law enforcement action in 18 countries and jurisdictions, including Costa Rica; the Netherlands; Spain; Morocco; Sweden; Switzerland; Cyprus; Australia; China; Hong Kong, China; Norway; Latvia; Luxembourg; the United Kingdom; Russia; Canada; and the United States to restrain criminal proceeds, forfeit domain names, and seize servers.

19 The Silk Road investigation involved multiple US law enforcement agencies, led the Federal Bureau of Investigation's (FBI')s New York Special Operations and Cyber Division, and the Drug Enforcement Administration's (DEA's) New York Organized Crime Drug Enforcement Strike Force (comprised of agents and officers of DEA, the Internal Revenue Service (IRS), the New York City Police Department, US Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the US Secret Service, the US Marshals Service, Office of Foreign Assets Control (OFAC), and NY Department of Taxation), with assistance and support of the ICE-HIS Chicago field office, the Department of Justice's Computer Crime and Intellectual Property and Asset Forfeiture and Money Laundering Sections, the United States Attorney's Office for the Southern District of New York, and foreign law enforcement partners, particularly the Reykjavik Metropolitan Police of the Republic of Iceland and the French Republic's Central Office for the Fight Against Crime Linked to Information Technology and Communication.

BIBLIOGRAPHY AND SOURCES

FATF (2013), FATF *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services,* FATF, Paris
www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-npps-2013.html

Popper, N. (2013), "In Bitcoin's Orbit: Rival Virtual Currencies vie for Acceptance", in *New York Times, Dealb%k,* (Nov. 24, 2013) http://dealbook.nytimes.com/2013/11/24/in-bitcoins-orbit-rival-virtual-currencies-vie-for-acceptance/?_r=0, accessed June 2014.

APPENDIX B

HOW DECENTRALISED CONVERTIBLE VIRTUAL CURRENCY WORKS AS A PAYMENTS MECHANISM

INTRODUCTION

1. Bitcoin and other decentralised convertible virtual currencies (VCs) provide potentially ground-breaking alternative digital payments platforms. The Bitcoin network itself was explicitly designed to serve as an electronic **peer-to-peer (P2P)**[1] payments mechanism for Internet-based commerce. It was intended to enable users to bypass financial institutions by directly transferring VC to each other and settling those transactions in near real time, thereby removing intermediation costs, such as transaction fees and payment uncertainty.

2. **Decentralised VC (also commonly referred to as cryptocurrency)**[2] is distributed, open-source, math-based convertible VC that does not involve a "trusted third party" to verify transactions and maintain (and reconcile) a transaction ledger. Bitcoin provided the first fully implemented cryptocurrency protocol, creating the world's first decentralised VC payments mechanism. Subsequently, hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, although there is ongoing interest in developing alternative, potentially more efficient protocols, using different proof methods[3] to validate transactions and maintain the online distributed transaction ledger.

SCOPE

3. This appendix provides a brief explanation of how decentralised convertible[4] (VC) operates as a payments mechanism. It focuses on the functional aspects of decentralised convertible VC networks, rather than on technical aspects of the protocol(s), and addresses s**ingle-currency VC payments networks**, like Bitcoin, rather than **currency-agnostic platforms** like Ripple.[5] The document (1) explains the conceptual framework for decentralised VC and describes the basic components of a single-currency decentralised VC payments network; (2) explains step-by-step what users must do to participate in the Bitcoin network and conduct a transaction; and (3) identifies many of the third-party VC payments products and services (VCPPS) that have recently emerged to facilitate use of this new payments mechanism. The discussion uses Bitcoin to illustrate single-currency decentralised convertible VC payments mechanisms, because of Bitcoin's first-mover advantage and much greater scale (in terms of transaction number and value and market capitalisation), compared to other decentralised VCs, and because to date, the venture capital investments and developing infrastructure for single-currency decentralised VC payments networks are overwhelmingly Bitcoin-specific. Using a concrete example, in the form of Bitcoin, is important for descriptive clarity; it does not reflect any endorsement by the FATF, nor prediction of eventual success as a mainstream payments mechanism. Many of the terms used in this document are defined in the FATF's June 2014 *Virtual Currencies—Key Definitions and Potential AML/CFT Risks* (*June 2014*

VC Document), provided in **Appendix A**. Those that are not are presented in bold and explained herein.

DECENTRALISED VIRTUAL CURRENCY AS A PAYMENTS PLATFORM

CONCEPTUAL FRAMEWORK FOR DECENTRALISED VC PAYMENTS MECHANISMS

4. Disintermediating financial institutions in electronic payments involves a major conceptual step. The Bitcoin protocol was designed to replicate various trust functions that financial institutions typically perform as intermediaries in electronic and cash transactions. One crucial trust function is guaranteeing against "double-spending" and counterfeiting.[6] **Double-spending** refers to a VC user's ceding ownership of the VC to one person and then ceding ownership of the same VC to another person. The double-spending problem arises because decentralised VC exists in the form of a digital file that can be easily duplicated and has no trusted authority maintaining a central record of transactions.

5. To prevent double-spending and counterfeiting, Bitcoin relies on a distributed online public ledger, called the **blockchain**,[7] and on public key cryptography to verify transactions. **Public-key cryptography** is a cryptographic method that assigns a user two keys: a **public key and a private key**. A **public key (a.k.a. Bitcoin address)** is a unique identifier that functions similarly to an e-mail address for the receipt of e-mail, and serves as an account for receiving bitcoins. A **private key** is a cryptographic code that functions as a secret password that allows the user to sign a VC transaction and transfer the bitcoins to another address. Using the private key proves ownership of the bitcoins. Every Bitcoin public key/address has a matching private key. The private key is mathematically related to the Bitcoin address and is designed so that the Bitcoin address can be calculated from the private key, but the same cannot be done in reverse, thus providing transaction and account security. The public key must be paired with the private key (signature) in order for the VC to be transmitted.

6. The Bitcoin protocol requires every transaction to be validated, logged and disclosed[8] on the blockchain. The **blockchain** functions as a public transaction reporting system. It consists of **blocks**; each block is a grouping of reported transactions in chronological order. When a transaction is initiated (proposed), it is broadcast to the network and participants, called miners, running a special piece of software, validate the transaction by solving a complex mathematical problem that verifies that the bitcoins in the proposed transaction have not already been spent and add it to the blockchain.[9] This same distributed (community) validation process, called "**mining**,"[10] generates new bitcoins, which are rewarded as payment to the first miner that solves the algorithm validating the transaction.[11] Every transaction that ever took place is recorded in order on the blockchain.

PARTICIPATING IN THE BITCOIN NETWORK TO SEND AND RECEIVE BITCOINS

7. Originally, the Bitcoin network was only a P2P transfer system, with no third party products and services. Users obtained and stored bitcoins, and conducted transactions, themselves. As discussed below, Bitcoin payments infrastructure has rapidly evolved, and now offers a variety of third-party payment products and services to facilitate obtaining, storing and using bitcoins. The following section describes the basic components and steps required to participate in the Bitcoin

network and conduct Bitcoin payments transactions. The final section describes some of the entities offering third-party bitcoin products and services.

PARTICIPATION WITHOUT INTERMEDIARIES

Step One: Obtain the Public Keys (Addresses), Private Keys, and Wallets Needed to Participate in the Bitcoin Network

8. At its most basic, to participate in the Bitcoin network *without any intermediaries*, users download and install free Bitcoin software (called the Bitcoin "client") to their computers from an affiliated website. The client software contains a wallet program that generates and stores public-private key pairs. The public key generated by the software is identified as a unique Bitcoin address (a 24 to 37-character string of numbers and letters), which functions as an account to receive Bitcoin payments and allow a user to conduct Bitcoin transactions. Users can create/obtain as many addresses as they want. The private keys (with Bitcoin, random sequences of 64 letters and numbers) generated by and stored in the client are mathematically linked to a specific Bitcoin address. As a practical matter, private keys **are** the user's virtual currency. The wallet program also communicates with other Bitcoin addresses on the Bitcoin network, allowing the user to send and receive bitcoins. The user accesses his/her bitcoin through a wallet (a computer file) on his/her computer, mobile phone, or other digital device. Alternatively, users can download a software wallet program from an online third-party wallet provider. Some software wallets operate in coordination with the Bitcoin client, while others allow the user to avoid downloading the entire Bitcoin client itself. A wallet the user downloads and stores on his/her own computer or other digital device is called an **unhosted wallet**. The user can store his/her unhosted wallet online ("hot storage") or offline ("cold storage"). With unhosted wallets, the owner is responsible for providing wallet security and protecting the private keys.

Step Two: Obtain Bitcoins

9. Users may obtain bitcoins in several ways. For example, they can (1) purchase VC from a third-party exchanger, using fiat money or other VCs; (2) engage in specific activities that earn VC payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) receive them as gifts or rewards; and (4) self-generate bitcoins by mining[12] them, as described above. The bulk of mining is now concentrated in professionalized mining pools; users typically obtaining bitcoins from third-party exchanges.

Step Three: Transfer Bitcoins

10. Bitcoin transactions are sent from and to Bitcoin addresses in Bitcoin wallets and are digitally signed for security. To use bitcoins to send a payment for goods or services or a remittance—i.e., to spend or send bitcoins—the user uses the private key(s) to unlock his/her digital wallet and digitally sign the transaction. The transaction itself contains three pieces of information: (1) an input (the bitcoin address that was used *to send the bitcoins to the current sender*; (2) an amount (the amount of bitcoins the sender is transferring); and (3) an output (the recipient's bitcoin address). These automated functions are handled by the wallet software. The user (via the downloaded software)

sends the bitcoins from his/her wallet to the Bitcoin network. At that point, as described above, Bitcoin miners include it in a transaction block, verify the transaction and enter it onto the blockchain, confirming the transaction. Most Bitcoin transactions that are conducted by the user him/herself, without intermediaries, have no mandatory fees. However, it is now recommended that users pay a voluntary fee to remunerate the miners for faster confirmation.

Figure 1. The three essential elements of a Bitcoin transaction

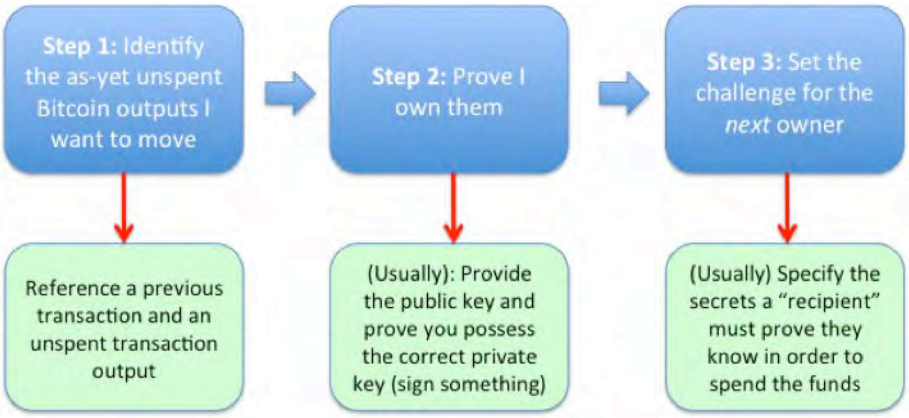

Table courtesy of Bach, A., Corallo, M. Dashjr, L. et al (2014)[13].

Step Four: Confirmation

11. With Bitcoin, announcing a payment to the recipient's address is almost instantaneous. However, the transaction must still be bundled into a block by miners to begin the confirmation process. On average, it takes approximately 10 minutes for the miners on the Bitcoin network to build (or solve) a given block. Once a transaction in a block has been added to the blockchain, it remains part of the blockchain. All subsequent blocks in the blockchain are built on top of the block containing that particular transaction. Each block added to the blockchain after a block containing a given transaction is considered a **confirmation**[14] of that transaction. A **confirmation** reflects consensus on the network that the particular bitcoins the recipient has received have not been sent to anyone else and are considered the recipient's property. A transaction must be confirmed before the recipient can spend/send the bitcoins he/she has received. The subsequent blocks in the blockchain built on top of the block containing a particular transaction consolidate the confirmation consensus and prevent reversal of the transaction. Users are free to determine how many subsequent blocks, in addition to the initial confirmation, should be added to the blockchain before the transaction is sufficiently confirmed that it is safe to spend/transmit the VC units. Generally, a transaction is not considered to be adequately confirmed until a certain number of confirmations (subsequent blocks)—typically, six—appears on the blockchain.[15]

PARTICIPATION WITH INTERMEDIARIES: EMERGING BITCOIN INFRASTRUCTURE

12. A growing number of start-ups have been emerging to provide new VC payments products and services (VCPPS) that facilitate use of decentralised VC payments networks, particularly Bitcoin. Instead of downloading the Bitcoin client or an unhosted wallet and storing and protecting their private keys and conducting transactions themselves, as described above, users (consumers and merchants) can now rely on a variety of third-party businesses that make it much easier to store the VC and conduct decentralised VC transactions. A variety of business models exist with respect to these third parties products and services. Some businesses provide a single type of service, while others offer several types of products and services to their customers. While the decentralised virtual currency "ecosystem" is rapidly evolving, some of these third party VCPPS are described below.

13. **Wallet provider.** Instead of downloading software that creates their addresses themselves, users can now obtain Bitcoin addresses by opening an account at a Bitcoin exchange or online wallet service. And instead of obtaining bitcoins from exchangers and storing them in an unhosted wallet on their own digital devices, they can obtain store the VC in a **hosted wallet**,[16] provided and safeguarded by a **wallet provider**.[17] The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. Beyond providing Bitcoin addresses, the wallet provider may offer encryption; multiple key (multi-key) signature protection; backup/cold storage; and mixers. All Bitcoin wallets can interoperate with each other. A wallet provider may provide hot or cold bitcoin storage, with the customer's retaining his/her private keys and control over transferring the VC. Alternatively, the wallet provider may hold both the public and private keys for the customer's VC and transfer the VC to third parties at the direction of the customer, to make payments and send remittances. **Many VC exchangers offer wallet services** (i.e., also function as wallet providers), allowing the user to obtain addresses and store his/her VC in an account at the exchange. At present, two models of third-party wallets predominate. In the earlier, more "traditional" wallet hosting services, the customer has his/her own wallet but the file is held on the third-party wallet service's servers. (There are numerous variations of this model, particularly with regard to whether the host has full control of the private key(s).) In the second model, which most exchanges are currently moving toward, the customer funds are held in pooled accounts, and the company conducts transfers/withdrawals at the customer's direction. This business model allows more of the VC funds to be held in cold storage, without impairing customer access to his/her VC.

14. A **virtual currency payment processor (a.k.a. third-party payments sender; merchant payments processor)** is an entity that facilitates merchant acceptance—i.e., it is an entity that facilitates the transfer of virtual currency payments from a user (customer) to a merchant or other business or professional that provides consumer goods or services. Typically, payment processors provide software applications or embeddable code that allow the merchant or other business to accept the virtual currency payment on its Internet website or at its brick-and-mortar location, and that either electronically transmit the virtual currency to the merchant's wallet (hosted by the processor or another wallet provider, or unhosted and held directly by the merchant), or convert some or all of the virtual currency into fiat currency and transmit an e-money payment to the merchant's account, as directed. Since Bitcoin and other decentralised convertible virtual currencies

are Internet-based payment systems specifically designed to cut out middlemen, it may seem odd to have virtual currency processors as participants in the virtual currency ecosystem. However, processors seek to make it easier for everyday, non-tech-savvy businesses to accept virtual currency payments. Some virtual currency payments processors may offer exchange (conversion) services for merchants that accept convertible virtual currency as payment but fear potential negative volatility of the currency, allowing them for hedging purposes to immediately convert incoming virtual currency into a fiat currency of their choice. Processors also make it easier for (non-tech-savvy) consumers to use virtual currency to purchase goods and services, affording them greater choice in their retail payments methods.

15. **Bitcoin ATM** (**a.k.a. BTM**) refers to an automated machine used to exchange fiat currency for bitcoin and/or other virtual currency, and vice versa. Depending on its programmed functionality, persons can use a bitcoin ATM to purchase bitcoins (and possibly other virtual currency) (mono-directional machines) or to both purchase virtual currency and cash-out virtual currency for fiat currency by withdrawing the fiat currency in exchange for the convertible virtual currency at the ATM (bi-directional machines –i.e., cash-in/Bitcoin-out or vice versa). The Bitcoin ATM industry is currently dominated by a few large players, but as the sector grows, others may be expected to enter. The number of active (live) Bitcoin ATMs is unclear, but one site reports that as of end-November 2014, there were approximately 300 bitcoin ATMs in operation worldwide. Bitcoin ATM operators charge a fee per transaction, with some Bitcoin ATM manufacturers' taking a commission on the operator's transaction fees.

NOTES

1 Peer-to-peer (P2P) payments are digital payments that a user sends directly to the recipient via the Internet.

2 At present, all cryptocurrencies are decentralised VCs and all decentralised VCs are cryptocurrencies. However, some centralised cryptocurrencies (i.e., a centralised VC system, or even a fiat-based system) are emerging that use a blockchain-like transaction ledger to handle customer transactions. It is possible that in the relatively near future, not all cryptocurrencies will be decentralised.

3 Bitcoin uses a proof-of-work method to verify transactions and create new bitcoins. Some altcoins use proof-of-stake or zero-knowledge proofs for this purpose.

4 All decentralised VC is convertible, by definition (i.e., there is no central authority that establishes the requirements for redemption).

5 There are currently two basic models of decentralised virtual currency payments mechanisms: single-currency (a.k.a. currency-specific) VC networks, like Bitcoin, and currency-agnostic VC networks, like Ripple and Ethereum. As the name implies, a **single-currency payments network** handles a given type of decentralised virtual currency. **Currency-agnostic payment platforms**, provide a platform for transacting in any virtual currency or any other tradable value, such as commodities, stock, real estate, etc. For an explanation of how a currency-agnostic VC platform operates, see *The Ripple Protocol: A Deep Dive for Finance Professionals,* available at https://ripple.com/ripple-deep-dive/. This citation is provided for information purposes only, and does not represent FATF endorsement of Ripple or any other VCNPPS.

6 Another trust function typically performed by financial institutions as intermediaries is the guarantee of payment from payor to payee. For traditional electronic payments, financial institutions intermediate transactions by guaranteeing payment (i.e., assuming the buyer's credit risk) and providing for post-transaction dispute resolution. Bitcoin seeks to solve the payment guarantee problem without financial institutions by achieving near real-time settlement and making its transactions irreversible (i.e., not subject to dispute resolution).

7 The **blockchain** is the shared Bitcoin transaction register, in the form of a publicly available, shared database with a sequential record of all transactions.

8 All Bitcoin transactions are stored publicly and permanently on the blockchain. Anyone accessing the network can see and monitor the balance and transactions of any Bitcoin address, identified by public key, on the blockchain.

9 **Miners**, acting as nodes in the network, race to "discover" the next block by solving an increasingly difficult cryptographic puzzle, using a hashing algorithm. Bitcoin mining is a purely mathematical process, analogous to the search for prime using advanced high-performance computers. Bitcoins miners search to find a sequence of data (a 'block') that produces a particular pattern when the Bitcoin 'hash' algorithm is applied to the data. The winner announces the new block to the other nodes and receives new bitcoins as payment. The other nodes verify that the solution complies with all the rules of the Bitcoin protocol and then accept it as the next official entry in the blockchain, starting the process anew.

10 **Mining** is the distributed transaction validation process that generates the blockchain and creates new bitcoins.

11 A miner is awarded a set number (predetermined by the Bitcoin protocol) of newly created bitcoins, and in some instances, also transaction fees for solving each algorithm that serves to verify and enter payments into the blockchain. An algorithm releases new bitcoins into the network at preset intervals--currently, 50 every 10 minutes, with the pace halving in approximately four-year increments until about 2140. In 2015, 25 bitcoins are awarded to the winning miner. When the total of 21 million bitcoins is in existence, transaction processing will only be rewarded by the transaction fees. The predetermined rate of release of the digital currency is intended to ensure regular growth of the Bitcoin money supply at a predictable rate without interference by third parties, like a central bank, to prevent hyperinflation.

12 As noted above, mining involves running a special piece of software on their computers to solve complex algorithms in a "distributed proof-of-work system." The user is awarded a certain number of newly created bitcoins for solving each algorithm.

13 Bach, A., Corallo, M. Dashjr, L. et al (2014, *Enabling Blockchain Innovations with Pegged Sidechains,* (October 2014), https://gendal.wordpress.com/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/.

14 **Confirmation** refers to the point when the transaction is validated by a miner and recorded in the blockchain.

15 While some merchants require VC users to wait until the VC transaction is confirmed a set number of times before treating the payment transaction as settled and processing the customer's order, for low value transactions, where the fraud risk is not great, some merchants treat receipt of the bitcoins, rather than confirmation, as valid payment.

16 A **hosted wallet** is a virtual currency wallet held by a third-party wallet provider (which may be an exchange).

17 **A wallet provider** is an entity that provides a virtual currency wallet for holding, storing and transferring bitcoins or other virtual currency.