GUIDANCE FOR A RISK-BASED APPROACH
風險基礎方法指引

VIRTUAL CURRENCIES
虛擬貨幣

JUNE 2015
2015 年 6 月

FINANCIAL ACTION TASK FORCE
防制洗錢金融行動工作組織

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.
防制洗錢金融行動工作組織（FATF）是一個獨立的跨政府組織，旨在發展與提升政策，負責制定並執行政策，維護全球金融體系，以對抗洗錢、資恐以及資助武擴。FATF 所提建議已被認定為是全球性防制洗錢（AML）與打擊資恐（CFT）的公認標準。

For more information about the FATF, please visit the website:
如需關於 FATF 更完整的資訊，請參閱其網站：

www.fatf-gafi.org

TABLE OF CONTENTS
目錄

TABLE OF ACRONYMS
縮寫名詞列表

AML	Anti-money laundering 防制洗錢
ATM	Automated teller machine 自動櫃員機
BaFIN	German Federal Supervisory Authority 德國聯邦監管機關
CDD	Customer due diligence 客戶審查
CFT	Countering the financing of terrorism 打擊資助恐怖主義
DNFBP	Designated non-financial business and profession 指定之非金融事業或人員
EBA	European Banking Authority 歐洲銀行管理局
FINMA	Financial Market Supervisory Authority 金融市場監管機構
KWG	German Banking Act 德國銀行法
MAS	Monetary Authority of Singapore 新加坡金融管理局
ML	Money laundering 洗錢
MSB	Money service business 貨幣服務事業
MVTS	Money value transfer service 金錢或價值移轉服務
NPPS	New Payment Products and Services 新型支付產品與服務
P2P	Peer-to-peer 點對點技術
RBA	Risk-based approach 風險基礎方法

TF	Terrorist financing 資助恐怖份子
VC	Virtual currency 虛擬貨幣
VCPPS	VC payment products and services VC 支付產品與服務

SECTION I – INTRODUCTION
第 I 節 – 簡介

BACKGROUND
背景

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.
1. 防制洗錢金融行動工作組織（FATF）於 2014 年 6 月發佈*虛擬貨幣的重要定義與潛在的防制洗錢/打擊資恐風險報告*（2014 年 6 月 VC 報告）。近幾年，虛擬貨幣（VC）出現並吸引了奠基於其軟體協定之上的支付設施之投資。這些支付機制想要提供一個在網際網路上傳送價值的新方式。

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.
2. 防制洗錢金融行動工作組織 肯定這樣的金融創新。同時，VC 支付產品與服務（VCPPS）所帶來的洗錢與資恐（ML/TF）風險和其他犯罪風險，有必要加以確認並減緩。這份指引重點放在針對 VCPPS 相關的洗錢/資恐風險（而非其他類型的 VC 金融產品，如：VC 證券或其他產品）採用一套以風險為基礎的方法。因此，在此指引中採用了 VC 支付產品與服務（VCPPS）一詞，而非 VC 產品與服務（VCPS），後者的討論僅限 VC 支付計畫。

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.
3. VCPPS 的開發及其與其他新型支付產品與服務（NPPS）甚至與傳統銀行服務的互動[1]，造就了此指引的制定需求，以期保護全球金融體系的完整性。

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).
4. 這個獨立的指引奠基在 2014 年 6 月的 VC 報告以及*針對預付卡、行動支付以及網際網路支付服務的一套以風險為基礎的方法指引*[2] 報告的風險矩陣表和最佳案例之上（2013 年 6 月的 NPPS 報告）。

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.

5. 此指引屬於防制洗錢金融行動工作組織階段性做法的一部份。此指引的重點放在提供受管制的金融體系門徑的交叉點，特別是可轉換[3]的虛擬貨幣兌換方[4]。防制洗錢金融行動工作組織 將繼續監督 VCPPS 的發展以及陸續出現的風險與減緩因素。在我們對於 VCPPS 的科技與用途有更多的認識後，可能會更新此指引，納入新出現、處理和 VCPPS 相關洗錢/資恐風險有關的法規議題方面的最佳案例。未來，可能會將不牽涉兌換活動及去中心化可轉換 VC 網絡內的移轉（如：牽涉到託管錢包提供商與民眾之間移轉問題、大金額的 VC 支付）納入。

PURPOSE OF THE GUIDANCE
指引目的

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.

6. 此指引用意在於說明 VC 環境下針對防制洗錢/打擊資恐措施採取以風險為基礎的方法、分辨出涉及 VCPPS 的實體並釐清相關*防制洗錢金融行動工作組織建議*應用於可轉換的虛擬貨幣兌換方之情形。此指引另一個用意也在於協助國家機關了解並可能做出法規回應，包括處理 VCPPS 的洗錢/資恐風險時修訂其國內法律的必要性。 此指引還有一個用意是協助私部門進一步了解切身的防制洗錢/打擊資恐義務以及它們如何能有效遵照相關規定等。此指引結合了概念框架和*防制洗錢金融行動工作組織 在 2014 年 6 月的 VC 報告（附件 4）*中採用的關鍵用語。請讀者在討論 VC 可能的使用個案以及字彙表時可參考該文件。

7. The Guidance seeks to:

7. 此文件努力的方向是：

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

a) 證明能夠如何應用特定的 *防制洗錢金融行動工作組織 建議*至 VCPPS 環境內可轉換的虛擬貨幣兌換方、找出可能需要的防制洗錢/打擊資恐措施並提供範例；以及

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

b) 找出生根在 VCPPS 科技、企業模式以及傳統法律框架內導致無法應用減緩措施的阻礙。

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.

8. 防制洗錢金融行動工作組織 提及有些政府已經開始考慮 VCPPS 帶來的眾多法規議題。特別是在防制洗錢/打擊資恐方面，雖然有些轄區已經採取規範行動，但是其他只是監督並研究洗錢/資恐風險的發展與可能性，也因為如此這些轄區仍處於發展階段。以部份轄區而言，實施一個有效的防制洗錢/打擊資恐法規體制可能需要對 VCPPS 有更透徹的認識。 儘管如此，VCPPS 的快速發展、日新月異的功能、使用普遍性和全球性質已經使得各國針對辨識和減緩洗錢/資恐風險採取行動刻不容緩。防制洗錢金融行動工作組織 體認到可能有其他影響個別轄區內針對 VCPPS 最後制定的規範選項或結果的政策需要納入考慮。

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.

9. 根據其職能和風險資料，在所有對於類似產品與服務一視同仁的轄區內建立某種形式的指引對於提昇國際防制洗錢/打擊資恐標準的效果至關重要。因為 VCPPS 無國界的性質（不需要以任何特定的轄區為依據即可執行活動），使其特別令人感到憂心。此指引不具約束力而且無法推翻國家機關的權限，其僅希望有助於公家機關與私部門發現並有效處理與洗錢/資恐風險有關的 VCPPS。

SCOPE OF THE GUIDANCE
此指引的適用範圍

10. The Guidance focuses on VCPPS and related AML/CFT issues, and applies to both centralized 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]

10. 此指引重點放在 VCPPS 和相關的防制洗錢/打擊資恐議題，同樣適用集中和去中心化 VCPPS。主要處理可轉換的 VC，因為後者具較高風險。此指引的重點放在可轉換、屬於提供受管制的金融體系門徑的交叉點的虛擬貨幣兌換方（可轉換的 VC 活動與受管制的法定貨幣金融體系交叉處）。不處理 VC 支付機制所產生的非防制洗錢/打擊資恐的法規議題（如：消費者保護、嚴謹的安全性與健全性、稅務、反詐欺問題以及網絡 IT 安全標準等）。也不處理 VC 的非支付用途（如：基於儲蓄或投資目的儲存具有價值的產品，如：衍生品、商品和證券產品）或 VC 活動[5]的貨幣政策面向。

STRUCTURE
結構

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**.

11. 此指引的結構如下：第 II 節檢視可轉換的虛擬貨幣兌換方符合*防制洗錢金融行動工作組織建議*內的哪個定義。第 III 節說明 *防制洗錢金融行動工作組織建議*應用於各國和權責機關的情況；第 IV 節說明*防制洗錢金融行動工作組織建議*在可轉換的虛擬貨幣兌換方的應用情形而第 V 節則舉例說明各國（或一群國家）截至今日為止已經採取的法規以及在未來預期會採用的法規。2014 年 6 月的 VC 報告納入**附件 A**。根據企業模型和運作方式，有關 VC 的性質以及作為支付機制的方式之說明列於**附件 B**。

SECTION II - SCOPE OF FATF STANDARDS[6]
第 II 節 – 防制洗錢金融行動工作組織標準的適用範圍 [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.
12. 此節（1）探討針對 VCPPS 採取以風險為基礎的方法之應用情形以及（2）檢視可轉換的虛擬貨幣兌換方應如何遵守國際標準有關防制洗錢/打擊資恐的規定。

INITIAL RISK ASSESSMENT[7]
最初的風險評估 [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.
13. 在 2014 年 6 月 VC 報告內所做的風險評估（附件 A）指出，至少近期而言只有可用於將價值移進和移出法定貨幣以及受管制的金融體系之*可轉換* VC 可能會帶來洗錢/資恐風險。因此，在風險基礎方法下，各國應將其防制洗錢/打擊資恐重點放在較高風險的可轉換 VC。

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*.
14. 該風險評估也建議防制洗錢/打擊資恐控管措施應鎖定可轉換的 VC 節點 – 亦即：提供受管制的金融體系門徑的交叉點 – 而不是試圖管制透過 VC 購買商品或服務的使用者。這些節點包括第三方可轉換的 VC 兌換方。遇到相關情況時，應根據 *防制洗錢金融行動工作組織 建議*進行管制。*因此，各國應考慮將國際標準規定的相關防制洗錢/打擊資恐要求套用到可轉換的 VC 兌換方以及任何其他屬於可轉換 VC 活動與受管制的法定貨幣金融體系交叉節點的機構套用。*

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.
15. 在風險基礎方法下，各國也可考慮管制金融機構或寄送、接收和儲存 VC 的指定之非金融事業或人員，但是不提供虛擬和法定貨幣之間的交易或兌現服務。不過，這不在此指引的適用範圍內。

FATF DEFINITIONS
防制洗錢金融行動工作組織的定義

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.
16. 防制洗錢金融行動工作組織建議要求所有轄區針對金融機構以及指定之非金融事業或人員（DNFBP）實施特定的防制洗錢/打擊資恐要求，確保其遵照上述義務。

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.
17. 防制洗錢金融行動工作組織將「金融機構」定義為任何替或代表客戶以企業身份執行一項或多項特定活動的自然人或法人。可能和目前可用的 VCPPS 最相關的類別包括以企業身份執行下列項目的個人：貨幣或金錢或價值移轉服務（MVTS）[8]、接收來自大眾的存款和其他可重複支付的資金、出具和管理付款方式以及外匯交易或可轉移的證券等。視其特定活動而定，去中心化 VC 兌換方、錢包提供方以及款項處理/寄送方還有其他可能的 VC 企業模型等都可能落於這其中一個或多個類別中。

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.
18. 從事 VCPPS 的自然人或法人是否為負有義務的實體視其使用 VC 的方式以及受益者為何而定。國家機關應根據其在管制此類活動方面提供眾多選擇的國家法律框架，在適當時處理和可轉換的 VC 兌換活動有關的洗錢/資恐風險(可轉換的 VC 活動與受管制的法定貨幣金融體系重疊時)。

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.
19. 執行防制洗錢金融行動工作組織所定義之*金融機構*活動時，VCPPS 提供方受相關的防制洗錢金融行動工作組織建議之規範。這包括可轉換的 VC 活動與受管制的法定貨幣金融機構重疊時的可轉換虛擬貨幣兌換方。

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.
20. 視牽涉到的特定 VC 活動的強度或數量及其本身的法律框架而定，各國應針對風險套用相關的防制洗錢金融行動工作組織建議至這些任何涵蓋其中的實體類別，以處理和 VC 兌換以及任何其他屬於可轉換 VC 活動與受管制的法定貨幣金融體系交叉節點的機構有關的洗錢/資恐風險。

SECTION III – APPLICATION OF FATF STANDARDS TO COUNTRIES AND COMPETENT AUTHORITIES
第 III 節 – 防制洗錢金融行動工作組織標準在各國與權責機關的應用

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.

21. 此節說明和 VCPPS 有關的特定防制洗錢金融行動工作組織建議如何運用於各國和權責機關，重點放在找出並減緩與可轉換的 VC 有關的風險、應用執照/註冊要求、實施有效監管、提供各種有效的勸誡制裁以及促進國內與國際合作等。

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.

22. 防制洗錢金融行動工作組織有些建議與了解各國應如何善用政府機關和國際合作，以處理和可轉換的 VC 有關的洗錢/資恐風險直接相關。

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 centralized 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.

23. **建議 1**。目前的*防制洗錢金融行動工作組織 建議*清楚指出各國應運用一套風險基礎方法以確保用以預防或減緩洗錢/資恐風險的措施與發現的風險相當。在風險基礎方法下，各國應強化對於較高風險情況的要求。評估可轉換 VC 的洗錢/資恐風險時，集中和去中心化 VC 之間的區分是一個重要層面。考量其匿名性質以及正確辨識參與者身份時的困難，一般而言可轉換的去中心化 VCPPS 可被視為具備較高的洗錢/資恐風險，因此需要應用強化的客戶審查措施。

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.

24. 建議 1 要求各國找出、了解並評估其洗錢/資恐風險並採取旨在有效減緩該風險的行動。這個要求適用和 VC 以及其他新式科技有關的風險。公私部門間的合作可能有助於權責機關針對 VC 金融活動創新的 VC 科技以及新興的產品與服務制定防制洗錢/打擊資恐政策。這也許有助於各國由權責機關配置和決定防制洗錢/打擊資恐資源的優先順序。

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.
25. 各國機關應考慮基於下列目的針對 VC 產品和服務進行風險評估：（1）讓所有相關的機關了解基於防制洗錢/打擊資恐目的，特定 VC 產品與服務的功能，適用性和衝擊所有相關主管轄區的程度等（如：貨幣傳輸/付款機制、VC ATM、商品、證券）以及（2）針對具備類似風險的類似產品與服務採用類似的防制洗錢/打擊資恐標準。

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.
26. 各國亦應要求金融機構以及指定之非金融事業或人員找出、評估其與 VCPPS 有關的 洗錢/資恐風險並就減緩此風險採取有效的行動。基於防制洗錢/打擊資恐目的，國家法律允許 VCPPS 活動時，各轄區、金融機構和 DNFPB（包括可轉換的虛擬貨幣兌換方）必需評估洗錢/資恐風險並運用風險基礎方法，以確保實施用以預防或減緩這類風險的相關措施。

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.
27. 即使某個國家決定以非洗錢/資恐風險管制 VC（如：消費者保護、嚴謹的安全性與健全性以及網絡安全等）仍應根據相關的 防制洗錢金融行動工作組織 建議儘快採取行動，找出、評估並套用風險基礎方法，以減緩與 VC 有關的洗錢/資恐風險。

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.
28. 根據此風險評估，各國應決定如何管制可轉換的虛擬貨幣與法定貨幣之間的兌換平台（亦即：可轉換的虛擬貨幣兌換方）。有些國家可能會根據其本身的風險評估結果（包括上揚趨勢[例]）以及國家法規環境決定禁止 VC 活動，以期達到此指引未提及的其他政策目標（如：消費者保護、安全性與健全性、貨幣政策等）。各國在考慮禁止 VCPPS 時應將對（但不限於）當地和全球洗錢/資恐風險等級造成衝擊納入考慮，包括禁止 VC 付款活動是否會讓這些活動地下化以及在沒有防制洗錢/打擊資恐控管措施或監督下它們將朝那個方向繼續運作等。不管一國是否選擇禁止或管制 VC，採取額外的措施在減緩整體的洗錢/資恐風險方面均具實用性。若一國決定禁止 VC 活動，則額外的減緩措施將包含找出在其轄區內非法運作的 VC 提供方並對其實施成比例的勸誡制裁。該國需要針對禁止一事從事推廣、教育活動，然後再強制執行。各國也將需要考慮 VCPPS 在其風險減緩策略內具備的跨界要素。

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.
29. **建議 2** 要求各國在防制洗錢/打擊資恐政策方面（包括 VC 部門內的此類政策）尋求國內合作與協調。各國得考慮實施相關機制（如：跨機構工作小組），以便決策者、法規單位、監理機關、金融情報中心（FIU）以及執法機關彼此合作並和其他相關權責機關合作制定並實施有效的政策、規範及其他措施，以處理 VC 的洗錢/資恐風險。

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.
30. 各國可考慮針對各種 VC 產品與服務發展以風險為基礎的防制洗錢/打擊資恐規範與監督的國內協調機制。此外，各國機關應考慮基於下列目的針對 VCPPS 進行風險評估：（1）讓所有相關的機關了解基於防制洗錢/打擊資恐目的，特定 VC 產品與服務的功能，適用性和衝擊所有相關主管轄區的程度等（如：貨幣傳輸/付款機制、VC ATM、商品、證券）以及（2）針對具備類似風險資料的類似產品與服務採用類似的防制洗錢/打擊資恐標準。各國亦應考慮採用國內合作與協調機制，方便納入 VC 私部門。

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.
31. 若 VC 演進成金融部門一個具有意義的部份，則各國應考慮檢視 VC 防制洗錢/打擊資恐規範與監督和 VC 的非防制洗錢/打擊資恐規範與監督（如：消費者保護、安全性與健全性、保險、網絡安全、稅務遵從性）之間的關係。就這方面而言，建議各國考慮展開短期和較長期的政策工作，以期在必需廣泛採用 VC 時制訂全面的 VCPPS 規範。

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.
32. **建議 14** 指示各國針對國內提供 金錢或價值移轉服務 的自然人或法人進行註冊或發照並確保其遵照相關防制洗錢/打擊資恐措施。包括監督國內運作的 金錢或價值移轉服務 是否遵守註冊/申請執照以及其他適用的防制洗錢/打擊資恐措施。

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.
33. 建議 14 的註冊/申請執照規定適用國內轄區內提供 VC 和法定貨幣間可轉換 VC 兌換服務

（亦即：VCPPS）的實體。

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.

34. 因為透過網際網路等數位方式轉移價值的可轉換 VC 兌換方不受國土邊境的限制並且一般會提供 VCPPS 給未實際位於相關國家境內的個人，所以所有母國在 防制洗錢金融行動工作組織建議要求下採用國內執照申請或註冊極其重要。基於相同的原因，母國轄區內的適當監督以及該實體有提供服務的轄區內權責機關彼此適當合作並交換資訊具備高度的重要性。

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.

35. **建議 15** 強調和新科技有關的基本風險基礎方法義務。要求各國找出並評估和新產品的開發以及新的企業做法有關的洗錢/資恐風險，包括新的交付機制以及針對新的和既有的產品採用新的或開發新的科技。建議 15 也要求各國確保其轄區內取得執照或運作的金融機構在推出新產品或企業做法或採用新的或開發科技前先採取相關措施管理並減緩風險。各國有關新科技的規定應包含 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.

36. **建議 16** 替各國制定和電匯有關的規定。建議 16 適用於跨境電匯以及國內電匯。電匯是指任何透過下列方式替匯款人執行的任何交易：（a）金融機構、（b）目的在於讓受益人能夠使用一筆資金的電子管道或（c）受款的金融機構，不論匯款人和受益人是否為同一人。各國應確保在可轉換的虛擬貨幣兌換方執行屬於電匯的可轉換 VC 移交作業時，將建議 16 指出的必要匯款人和受益人資訊納入。就這方面而言，各國得針對價值不超出美金/歐元 1,000 元的跨境電匯制定一個*最低*門檻。各國亦應確保金融機構監督可轉換的 VC 移交作業，找出缺乏必要的匯款人和/或受益人資訊者並在發現時採取相關措施進行處理。

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.

37. **建議 26** 規定各國必需確保可轉換的 VC 兌換方在可轉換的 VC 活動與受管制的法定貨幣金融體系重疊時接受適度的規範與監管。各國應視需要考慮修正傳統的法律架構，授權針對去中心化 VC 付款機制進行有效的防制洗錢/打擊資恐規範。

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.

38. **建議 35** 指示各國應有各種適用建議 6、8 和 23 提到、未遵守相關防制洗錢/打擊資恐 規定的自然人或法人之有效、合比例的勸誡制裁（刑法、民法或行政制裁）。但是，就目前而言，在運用傳統執法工具並成功起訴 VCPPS（特別是去中心化可轉換 VCPPS）方面，依然面臨無數的挑戰。因為大部份去中心化 VC 交易目前都是匿名運作，所以很難找出牽涉其中的個人身份。現在幾乎所有去中心化 VCPPS 根據的協定並未規定參與者必需提供身份資訊或對其身份進行確認。此外，根據這些協定在區塊鏈上產生的傳統交易紀錄未必和真實世界中的身份有關。如此的匿名性讓區塊鏈在監督交易並找出可疑活動方面的實用性受到限制並且對執法單位追蹤利用去中心化可轉換 VC 進行的非法收益之能力面臨重大挑戰。此外，執法單位也無法在調查時鎖定一個集中的地點或實體。這些挑戰都削弱了各國採取有效勸誡制裁的能力。各國應檢視存在其特定國家環境內的各項挑戰，以找出可能的落差採取適當行動。要求 VC 兌換方申請執照或註冊並規定辨識/確認客戶身份與記錄等都讓各國能夠在 VC 環境下更有效地採取勸誡的制裁。

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.

39. **建議 40** 要求各國有效率地並且有效地和國際合作，協助其他國家對抗 洗錢、相關的確切違規事項與資恐 – 包括司法互助（**建議 37**）；協助找出、凍結、扣押並沒收可能以 VC 形式取得的犯罪所得與工具（**建議 38**）；並在發現虛擬貨幣相關的罪行時提供有效的引渡協助（**建議 39**）。這

些要求亦得適用牽涉到 VC 的合作。同樣重要的是，金融情報中心 應與其對造就 STR 合作並交換資訊，特別是和 VC 跨境運作有關時。充份監督並透過法規控管在其轄區內運作的可轉換 VCPPS 讓各國能夠進一步提供調查協助並在 VC 領域和國際進一步合作。就現階段而言，因為大部份國家仍缺乏 VC 規範與調查能力，所以可能阻礙其提供有意義的國際合作。此外，很多國家並沒有讓它們得以將 VC 洗錢/資恐活動罪刑化的法律框架，因此可能使其無法在需要雙重犯罪存在的情況下提供有效的 MLA。

SECTION IV – APPLICATION OF FATF STANDARDS TO COVERED ENTITIES
第 IV 節 – 將防制洗錢金融行動工作組織標準應用於涵蓋的實體

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.

40. 這個部份說明特定的*防制洗錢金融行動工作組織建議*應如何運用於可轉換的 VC 兌換活動以及任何其他在可轉換的 VC 活動與受管制的法定貨幣金融體系重疊時扮演節點功能的實體，以減緩洗錢/資恐風險。包括運用風險基礎方法（建議 1）、客戶審查（CDD）（建議 10）、記錄（建議 11）、針對金錢或價值移轉服務制定註冊或申請執照的要求（建議 14）、找出並減緩與新科技有關的風險（建議 15）、防制洗錢/打擊資恐計畫要求（建議 18）以及疑似洗錢或資恐交易報告（建議 20）等。這個部份也會檢視目前在去中心化 VC 領域內運用部份此類減緩措施時遇到的障礙。僅在上述第 III 節討論建議 14，但是如上述，建議 14 要求涵蓋的實體遵照其提供 VC 金錢或價值移轉服務的所有轄區內註冊或取得執照的規定。

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.

41. **建議 1。***防制洗錢金融行動工作組織建議*清楚指出各國應要求金融機構以及指定之非金融事業或人員辨識、評估其洗錢/資恐風險（包括與 VCPPS 有關的風險）並就減緩此風險採取有效的行動。包括持續努力修正用以可靠地辨識並確認客戶的技術過程。基於防制洗錢/打擊資恐目的，國家法律允許 VC 活動時，各轄區、金融機構和指定之非金融事業或人員（包括可轉換的虛擬貨幣兌換方）應評估 VC 活動展現的洗錢/資恐風險並運用風險基礎方法，以確保實施用以預防或減緩這類風險的相關措施。風險基礎方法並非暗示在沒有適當的風險評估下即自動或全盤拒絕給予 VCPPS 服務。

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.
42. **建議 10**。CCD 是在減緩與可轉換的 VC 有關的洗錢/資恐風險時一個必要的措施。根據防制洗錢金融行動工作組織標準，各國應要求可轉換的 VC 兌換方在建立商業關係或是在利用可靠的、獨立來源的文件、資料或資訊執行（非電匯）偶發交易時執行客戶審查[9]。舉例而言，應要求可轉換的 VC 兌換方在透過一次性交易將 VC 換成法定貨幣（或反之亦然）且價值超出指定的美金/歐元 15,000 元門檻或是在（b）執行建議 16 及其註釋提及的偶發性電匯交易時執行審查。通常，可轉換的 VC 交易會涉及電匯，因此受建議 16 規範。

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.
43. 各國可能會想在適用時針對 VC 客戶審查規定考慮一個較低的門檻或取消其門檻，視 找出的洗錢/資恐風險性質和等級而定。

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.
44. 有鑑於 VCPPS 的性質（建立客戶合作關係後完全透過網際網路載入資金與傳輸交易），各機構勢必得在未面對面下進行身份的辨識與確認作業。各國應考慮要求提供 VCPPS 的實體遵照 *2013 年 6 月 NPPS 指引*/中建議的最佳做法。在適用的程度下，這包括了：將接收自客戶的身份資訊（如：身份證字號）與第三方資料庫或其他可靠來源的資訊進行確認；可能會追蹤客戶的網際網路協定（IP）地址；並搜尋網頁以確認活動資訊與客戶的交易資料相符，但前提是資料的收集過程必需符合國內隱私法案的規定。

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.
45. 可轉換的 VCPPS 呈現較高風險（根據風險基礎方法進行確認）時，應要求可轉換的虛擬貨幣兌換方執行與該風險成比例的強化的客戶審查並鼓勵它們利用多重技術採用合理的措施確認客戶身份。若允許可轉換的虛擬貨幣兌換方在建立商業關係後再完成確認作業，如此才不會導致正常的營業（風險低時）受到中斷，則應要求它們在執行高於門檻的偶發交易前完成確認作業。

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.
46. 各國亦應期待金融機構與指定之非金融事業或人員考慮和資金可轉換的 VCPPS 來源有關

的風險。去中心化可轉換 VCPPS 允許來源不明的資金，包括點對點技術（P2P）的 VC 移交作業以及本身即屬匿名性質的 NPPS 資金，因此會增加洗錢/資恐風險。和 NPPS 一樣，VCPPS 事業應針對高於特定門檻的偶發交易考慮將資金來源限制在銀行戶頭、信用帳戶或信用卡或至少在最初載入或在建立一個交易型態前的特定期間或針對高於既定門檻的載入量時套用此類限制。

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 decentralized 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.

47. 交易監督在可轉換的 VC 領域內是一個重要的風險減緩做法，因為在沒有面對面的情況下要確認身份有其難度也因為一直到最近去中心化可轉換 VC 科技才允許可用於 NPPS 的特定風險減緩做法融入去中心化 VCPPS，以限制其功能並降低風險。舉例而言，多重簽章（Multi-sig）的科技如今已讓 VCPPS 能夠有效累積載入的總錢包價值並運用價值/速度交易限制於去中心化 VCPPS。但是，目前去中心化 VC 科技無法有效建立地理限制、限制其用途於特定商品和服務的購買或預防人與人之間的移交作業。

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.

48. 建議各國鼓勵執行與風險相當的交易監督。理論上，區塊鏈上可用的交易資訊具備公開性質，所以方便進行交易監督，但是如 *2014 年 6 月的 VC 報告*（附件 A）所提，因為很多去中心化 VC 交易並未牽涉真實的身份，所以限制了此區塊鏈在監督交易並找出可疑活動方面的實用性，這對於有效提升防制洗錢/打擊資恐遵從性與監管而言帶來嚴重挑戰。

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.

49. **建議 11、建議 20 與建議 22。**建議 20 提及，在 VC 交易可能涉及犯罪活動所得或可能和資恐有關時**記錄**與**通報可疑活動**也很重要。至少應要求金融機構與指定之非金融事業或人員針對下列內容進行記錄：各方身份資訊、公鑰、牽涉到的地址*或*帳戶、交易性質與日期以及移交的金額等。區塊鏈上可用的公開資訊是記錄的起始基礎，但前提是各機構能夠適當地辨識其客戶身份。各國應要求各機構注意其能夠偵測到的可疑活動類型。

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.

50. **建議 15** 和**建議 22** 明確提及新科技並要求金融機構和指定之非金融事業或人員找出並評估和新產品的開發以及新的企業做法有關的洗錢/資恐風險，包括新的交付機制以及針對新的和既有的產品採用新的或開發新的科技。建議 15 也要求金融機構和指定之非金融事業或人員確保某個轄區內取得執照或運作的金融機構在推出新產品或企業做法或採用新的或開發科技*前*先採取相關措施管理並減緩風險。這些措施適用新科技的相關 VC。希望各國機關能夠執行這項義務而金融機構與指定之非金融事業或人員應主動達到建議 15 之期待。

POTENTIAL SOLUTIONS TO COMPLIANCE CHALLENGES
在遵從性遇到的挑戰之可能解決方案

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.

51. 應要求金融機構與指定之非金融事業或人員針對去中心化可轉換 VCPPS 利用有效且有效率的可用方式在此類產品/服務一推出時即遵照客戶身份建立確認以及監督交易等規定。因為去中心化可轉換 VC 在遵從性以及執法方面帶來了挑戰，所以金融機構、指定之非金融事業或人員、開發方、投資人以及在 VC 領域內的其他各方均應努力開發有助於提升遵從性的科技，解決此問題。

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.

52. 舉例而言，開發方也許能創造新的 VC 科技，如：提供客戶身份辨識資訊的應用程式設計界面（API）或允許金融機構或指定之非金融事業或人員限制交易規模與速度或制定各種必需在將某個 VC 交易送出給接收方/受益人前達到的條件，藉以減少與特定 VCPPS 有關的洗錢/資恐風險。利用線上收集到的資訊來擴建客戶基本資料並協助偵測可疑活動與交易的可能性是另一個有助於提升防制洗錢/打擊資恐遵從性的重要領域。和防制洗錢/打擊資恐遵從性有關的創新可能以改善既有的 VC 協定或開發全新的 VC 等形式出現，奠基在基礎完全不同的基準協定上，後者能夠累積風險減緩方法或有助於客戶身份辨識與交易監督。

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.

53. 也可開發第三方數位身份系統，提升防制洗錢/打擊資恐遵從性，這更適用 VCPPS。舉例而言，這些系統可能牽涉到第三方數位身份保管方和/或其他實體針對特定客戶審查、監督和通報目的建立、驗證並維護數位身份方案，以回應實施國際標準的各國防制洗錢/打擊資恐法律實施的規定。第三方數位身份保管方本身應被管制，以確保身份/確認過程的誠信度。

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.

54. 金融機構與指定之非金融事業或人員也可發掘開發有助於客戶身份辨識/確認、交易監督並遵守其他相關防制洗錢/打擊資恐規定的企業模型。舉例而言，參與傳輸去中心化可轉換 VC 的機構可考慮成立一個包含接受過審查的 VC 機構的產業協會並制定會員應遵守的政策與做法，方便它們辨識來自已經執行相關客戶審查且正在執行相關交易監督的成員之特定交易。

SECTION V - COUNTRY (OR GROUP OF COUNTRIES) EXAMPLES OF RISKBASED APPROACH TO VCPPS
第 V 節 – 針對 VCPPS 各國採取的以風險為基礎的方法案例

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]
55. 這個部份簡述部份國家到目前為止已經採用的法規做法以及不久的將來各國預期會採用的做法。如序言處所述，世界各國政府已經開始注意到 VCPPS 為法規帶來的諸多挑戰。國際清算銀行的一份報告將截至今日為止的各項措施分類如下[10]：

a) Imposing restrictions on regulated entities for dealing with virtual currencies;
a) 針對從事虛擬貨幣交易、受管制的實體實施限制；

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;
b) 採取法律/規範措施，如：要求從事虛擬貨幣交易的兌換平台遵照適用於匯款方的法規或建議基於防制洗錢/打擊資恐等目的在部份轄區內規範 VC 仲介；

c) Publishing statements cautioning users about risks associated with VC and/or clarifying the position of authorities with respect to VC; and
c) 發表聲明，提醒用戶注意 VC 相關風險和/或釐清 VC 相關機關的定位；以及

d) Monitoring and studying developments.
d) 監督並研究發展趨勢。

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:
56. 下列在許多轄區內已經或考慮針對 VC 採用的防制洗錢/打擊資恐規範做法是風險基礎方法的實例：

CANADA
加拿大

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.
57. 2014 年 6 月加拿大修正其防制洗錢/打擊資恐法規，將從事 VC 交易業務的個人與實體當作貨幣服務企業（MSB）看待。輔助法規仍在研擬階段，旨在確切定義應將哪些實體納入以及它們

個別的義務等。但是，預期其義務將和既有的 MSB 義務相當類似，包括註冊、客戶審查（含實質受益人資訊）、記錄、內部遵從體制以及通報可疑的特定交易等。

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.

58. 在制定其 VC 防制洗錢/打擊資恐政策時，加拿大採用風險基礎方法，包括在加拿大面臨的洗錢/資恐風險前提下了解與 VC 相關的風險，作為加拿大國內洗錢/資恐風險評估的一部份。這些法規將有助在減緩洗錢/資恐風險需求和持續促進金融創新的需求之間取得一個平衡。因此，加拿大提議的做法是鎖定目標，透過法規，介入在洗錢/資恐方面最脆弱的領域。

CHINA
中國

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.

59. 2013 年 12 月 3 日，中華人民共和國和 MIIT（產業與資訊科技部）、銀行監督管理委員會（CBRC）、保險監督管理委員會（CIRC）以及證券監督管理委員會（CSRC）等共同發出*比特幣風險預防通知*。此通知規定提供包含比特幣註冊、比特幣錢包和比特幣兌換等服務的機構善盡其防制洗錢/打擊資恐義務並採取措施辨識其客戶身份與記錄身份資訊。金融機構與付款服務提供方也必需針對比特幣服務提供方採取強化的監督措施，以避免相關風險。此外，PBC 在世界各地的分行必需研究比特幣相關的洗錢風險並針對可疑的交易採取相當的行動(包括強化的監管行動和強化監督)，以減緩風險。

EBA'S OPINION ON "VIRTUAL CURRENCIES”
EBA 對於「虛擬貨幣」的看法

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.

60. 2014 年 7 月 4 日歐洲銀行管理局（EBA）在針對這些新產品在沒有受到管制的情況下可能呈現的風險進行分析後，針對「虛擬貨幣」發表了看法。EBA 發表意見的對象是 EU 法規單位以及 28 個會員國的國內監管機關。

61. The EBA Opinion is built around long term and short term recommendations aiming at establishing a comprehensive regulatory approach.
61. EBA 的意見主軸是旨在建立一套全面規範做法的長期和短期建議。

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.
62. 從 EBA 的觀點來看，一個可能的長期規範做法需要有一個具體的規範機關而且需要包含（但不限於）針對數個市場參與者制定的治理規定、區分客戶帳戶、資本要求以及建立負責虛擬貨幣計畫及其重要成份的誠信度之「計畫主管機關」，包括協定與交易框架。

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.
63. 但是，在沒有此類計畫以前，EBA 在其意見中認為必須以其他方式減緩部份已經發現、比較迫切的風險。為了「立即做出回應」，EBA 建議各國機關讓金融機構注意到購買、持有或出售虛擬貨幣的風險並鼓勵它們不要購買、持有或出售虛擬貨幣。EBA 也建議 EU 法規單位考慮宣布虛擬貨幣兌換屬於「義務實體」，必需遵循 EU 防制洗錢指導綱領中制定的防制洗錢與資恐規定。委員會針對第 4 個防制洗錢指導綱領進行協調後並未採用 EBA 於 2014 年 7 月提出的建議。相反地，委員會將評估更全面規範的選擇。其將在即將到來的超出國界的防制洗錢/打擊資恐風險評估中納入 VC 風險評估並對會員國提出相關建議。

FRANCE
法國

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.
64. 2014 年 1 月 29 日，法國審慎監督和解決權力機構（ACPR）發表了立場聲明，強調從事和買賣 VC 換取法定貨幣等仲介活動的實體是為代表第三方接受資金的金融仲介且這些活動必需獲得 ACPR 授權，因此必需遵照防制洗錢/打擊資恐規定。2014 年 6 月，法國金融情報中心、TRACFIN 公佈了一份報告，名為「管制虛擬貨幣：為防虛擬貨幣用於詐欺用途或洗錢所提之建議」，其用意在於建立一套框架，遏止虛擬貨幣在詐欺和洗錢方面的用途。

GERMANY
德國

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.

65. 德國聯邦監管局（BaFin）根據德國銀行法（KWG）第 1（11）節第 1 行認定比特幣具有法律約束力，是以帳戶單位形式的金融商品。這些單位等同貨幣，但並非以法定貨幣定價。

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.

66. 比特幣根據德國付款服務監管法（ZAG）的定義並非電子貨幣，因為比特幣發行時並非接收自發行方。這與虛擬貨幣不同，後者受到中央發行方的支援。比特幣也不是以法定貨幣定價，因此不屬於貨幣或鈔票或硬幣。

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.

67. 和金融商品有關的商業活動一般需要向 BaFin 申請執照。但是 BaFin 也釐清了比特幣當作交易付款的替代貨幣使用本身是不受 KWG 授權規範的活動。挖掘比特幣也不是必需獲得授權的活動，因為發掘方本身不發行或放入任何比特幣。同樣的道理適用於被挖掘或收購的比特幣買賣活動，也不需要取得授權。

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 authorization 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.

68. 但是，如果出現其他因素可能即需取得授權。比特幣常常透過網際網路平台進行交易，其中有些稱之為兌換活動。此類活動一般不需要取得 BaFin 授權。需要哪一類型的授權只能透過詳細分析交易執行的技術和合約面來決定。有些可能從事 KWG 定義的投資仲介活動，其他則可能操作多國交易機制，如此即符合 KWG 定義的金融服務。還有一些可能需要被認為是主要仲介服務。若可能的買賣雙方只是透過平台被介紹給彼此，這就不構成特定交易的仲介行為。但是，在這樣的情況下，這類型的平台的提供方是具有專屬權的交易方，必需遵守 KWG 定義的授權規定。扮演交易局角色、將法定貨幣直接兌換成比特幣的提供方也符合專屬交易條件，必需遵守授權規定。

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.

69.	因為每個情況各有不同，礦池（亦即：多人基於共同產生比特幣目的集結了電腦處理的能力）未必得接受監管。一個大原則是，如果有多人以相同的權利使用處理能力，之後按比例分配比特幣，則這不屬於需要授權的活動。舉例而言，如果礦池的運作方提供來自挖掘或出售的比特幣之一部份營收而不提供處理能力（參與者因此無法控制特定的處理過程）則可能適用不同的規則。

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.

70.	BaFin 接獲了越來越多有關比特幣相關衍生性商品和類似基金的產品等查詢。再次強調，因為每個情況各有不同，所以未必都得接受監管。但是，一般而言，若有商業交易，這類型的產品即必需遵守 KWB 和 KAGB 的監管規定，因為從金融商品衍生而來的產品本身也屬於金融商品或至少代表資產管理。比特幣 ATM 的商業運作在正常情況下也是必需遵守授權規定的銀行或金融服務–視購買過程以及買賣雙方還有–部份情況會牽涉到–操作方之間的法定關係而定。

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.

71.	BaFin 不僅根據其德國境內是否有註冊辦公室或住居所，也根據其在國外的營運地點以及該服務提供方是否不斷透過商業方式提供在德國境內有註冊辦公室或住居所的公司或個人銀行或金融服務，認定某項業務在德國境內執行。但是，這不會影響被動的提供服務之自由，亦即：居住在德國境內的個人和公司本身主動請國外提供方提供服務的權利。因此，因為客戶主動要求而進行的交易不需要根據 KWG 取得授權。針對線上有關金融市場產品的提案，相關的標準是針對該網站所做的分析是否整體上透露著所提供的服務鎖定的是德國市場。免責聲明只是眾多指標的其中一個。其他指標包括領域和最高層級的領域、語言或其他國家特定的參考資料以及法律框架等。

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.

72.	已經取得交易金融商品授權的銀行和金融服務提供方亦得從事比特幣交易，無需進一步取得授權。以這些所有的情況而言，獲得授權的機構也屬於負有防制洗錢法規義務的實體。

HONG KONG, CHINA
中國香港

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.

73. 中國香港自 2013 年中起採取了極度謹慎的做法，提醒大眾消費者交易虛擬貨幣以及虛擬商品（如：比特幣）有關的洗錢和網路犯罪風險。中國香港並未特別針對這類虛擬商品進行管制，因為它們不屬於既有法律定義的「貨幣」、「證券」或「法定貨幣」。同樣地，提供虛擬商品相關服務的操作方或交易方和防制洗錢及資恐（金融機構）條例中定義的「貨幣服務事業」不符，除非其服務或交易牽涉到貨幣兌換或匯款服務。換言之，不管是否牽涉虛擬商品，金融機構、虛擬商品交易方或操作方或個人負有在其客戶審查工作或交易顯示與洗錢或資恐有關的任何可疑活動時向聯合金融情報中心疑似洗錢或資恐交易報告的法定責任。未揭露此類可疑交易可能構成犯罪行為。既有法律也涵蓋了詐欺行為、科技犯罪、龐式騙局、洗錢或涉及虛擬商品的資恐等。此外，法規單位也發出指引給金融機構，提醒他們必需確保針對虛擬商品相關的洗錢和資恐風險提升與之相當的監督等級。金融機構已被提醒必需在與任何擔任虛擬商品有關的計畫或事業操作者的客戶建立或維持企業關係時應小心評估相關的洗錢或資恐風險。

ITALY
義大利

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].

74. 在義大利，虛擬貨幣不被認為是法定貨幣。2015 年 1 月，義大利銀行針對使用所謂的虛擬貨幣 [11] 發出了警告和一份文宣，包含在 2015 年第 1 期的監管公告內，認同 EBA 對於虛擬貨幣的看法；後者鼓勵銀行和其他受監管的金融仲介不要購買、持有或出售虛擬貨幣。同一天，義大利金融情報中心發出了有關負有義務的實體異常使用虛擬貨幣和監測可疑洗錢或資恐交易的傳單。[12]

RUSSIA
俄羅斯

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.

75. 根據有關蘇聯中央銀行（俄羅斯銀行）的聯邦法律第 27 條，蘇聯禁止發行代理貨幣。2014 年 1 月蘇聯的中央銀行在其官方網站上發佈「用於執行交易的虛擬貨幣（尤其是比特幣）相關須知」。俄羅斯銀行警告個人、法人以及主要是信用機構與非信用的金融機構不要使用虛擬貨幣換取商品、服務或實際的盧布或外幣。因為由人數不限的個人發行的虛擬貨幣以及使用此類貨幣進行交易均具匿名性，所以個人和法人可能在不知不覺中涉入非法活動，包括洗錢/資恐。因此，使用虛擬貨幣換取實際的盧布或外幣以及商品和服務都將被俄羅斯銀行視為可能讓法人從事現行防制洗錢/打擊資恐法案中提到的可疑交易。

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).

76. 為了減緩和虛擬貨幣有關的洗錢/資恐風險，財政部和俄羅斯銀行共同制定了禁用電子代理貨幣和電子代理貨幣交易的草案。這個草案已經制定完成並且將於國會（State Duma）提出。

SINGAPORE
新加坡

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.

77. 2014 年 3 月，新加坡金融管理局（MAS）宣布將管制新加坡境內 VC 仲介，以處理洗錢/資恐風險。MAS 將引入法規，要求買賣或促成 VC 兌換成法定貨幣的 VC 仲介確認客戶身份並疑似洗錢或資恐交易報告。提案的法規並未涵蓋 VC 仲介的安全性與健全性，也沒有提及 VC 交易的正確運作方式。

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.

78. 針對虛擬貨幣仲介建議的法案尚未實施。目前的用意僅在於管制新加坡境內運作的虛擬貨幣仲介，亦即：在該國境內有實體辦公室的仲介。但是，有鑑於虛擬貨幣領域快速演進，新加坡將繼續密切監督其他轄區針對虛擬貨幣所採取的法規做法。必要時，MAS 會考慮採取額外的措施處理虛擬貨幣及其仲介帶來的風險。

SOUTH AFRICA
南非

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.

79. 南非的財政部於 2014 年 9 月 18 日針對監督虛擬貨幣發出了用戶警示[13]。這是財政部、南非儲備銀行、金融服務委員會、南非國稅局和金融情報中心發出的聯合聲明，旨在提醒社會大眾小心使用虛擬貨幣交易或投資的相關風險。

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.

80. 目前在南非並無特定法規談到虛擬貨幣的使用。因此，虛擬貨幣使用者並無法律保障或追索權。因為在南非不受管制，所以無法將虛擬貨幣歸類為法定貨幣，因為任何商人都可以拒絕接受虛擬貨幣為支付工具，並不違法。虛擬貨幣也無法被視為是支付方式，因為它們並不是在接受資金時發行。因此以虛擬貨幣進行交易是使用者自己甘冒風險，無法向南非當局行使追索權。南非當局將繼續監督並評估虛擬貨幣的使用情形並就這方面諮詢私部門利害關係方的意見。需要時得發出進一步的指引或規範。

SWITZERLAND
瑞士

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.

81. 2014 年 6 月，瑞士政府公佈了關於 VC 的研究和政策聲明，名為*聯邦理事會回應 Schwaab (13.3687) 與 Weibel (13.4070) 假說針對虛擬貨幣做成的報告*[14]，內容宣稱：「瑞士境內專業虛擬貨幣交易與交易平台的運作一般*在防制洗錢法案*適用範圍內。」 從事這些活動的實體必需遵守「確認契約方身份並確認實質受益人身份的義務。」 同時，瑞士金融市場監督局（FINMA）也公佈了一份數據[15]，強調在商業基礎上買賣可轉換 VC 以及操作用以將貨幣或可轉換的 VC 從一個平台的使用者轉至其他使用者的交易平台均需受瑞士防制洗錢法案規範。開始運作前，這類服務的提供方必需加入自律團體（SRO）或向 FINMA 申請執照，才能直接以受監管的金融仲介（DSFI）身份運作。若去中心化 VC 交易活動在防制洗錢法案的適用範圍內，則必需遵照 客戶審查 義務。因為可轉換的 VC 方便匿名進行跨境資產轉移，所以 FINMA 認為使用 VC 交易會增加洗錢/資恐風險，因此規定必需嚴格執行客戶審查，尤其是客戶的身份。牽涉到可轉換的 VC 之商業活動若牽涉到某個組織基於商業活動接受來自客戶的可轉換 VC 並替客戶保留 VC，即必需申請銀行執照。取得銀行執照的 VC 實體必需接受 FINMA 嚴格監管，後者將持續監督該公司，確保其遵守相關法規。聯邦理事會將持續監督 VC 領域內的發展，及早發現任何需求，採取進一步的行動。

UNITED KINGDOM
英國

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.

82. 英國政府針對虛擬貨幣的相關規劃：2014 年 11 月公佈了資訊要求，旨在收集和虛擬（數位）貨幣有關的效益與風險等證據，特別強調規範問題。該資訊要求於 2014 年 12 月結束。2015 年 3 月，英國政府公佈了透過該資訊要求收集到的證據歸納表並宣布有意讓防制洗錢法規適用英國境內的數位貨幣交易。英國政府打算於今年內就詳細的法規做法進行正式協商。

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.

83. UK 在提升對於虛擬貨幣相關風險之了解方面所做的努力：英國境內對於 VC 相關風險的了解程度已經提升。英國的國家打擊犯罪調查局（NCA）在評估 VC 犯罪用途造成的威脅並針對該威脅做出回應方面主導了跨部門的行動，牽涉皇家檢察署、HM 稅務局、倫敦市警察局、HM 財政部、英格蘭銀行、金融執行管理局、內政部以及都會警察服務局。

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.

84. 這個工作包含建立情報藍圖。NCA 評估是針對 VC 犯罪用途造成的威脅之執法基準。清楚的情報藍圖是運作時鎖定目標的基礎也會提供給決策者參考，讓他們在針對政府是否應該介入干預做出決定時有充份的資訊基礎。能力奠基工作包含提升業界與軍隊的認知。此外，這項活動很多的內容都反應國際情況，因為問題具備跨國性質，所以這很重要。

UNITED STATES
美國

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.

85. 美國對於任何從事人與人之間或從某個人至另一個地點的可轉換 VC 收授與傳輸作業的自然人與法人 – 包括可轉換的 VC 兌換方與行政人員 – 都有管制，均需遵守防制洗錢/打擊資恐 義務，包括註冊、辨識客戶身份、記錄與通報等要求。聯邦政府的防制洗錢/打擊資恐法規同時涵蓋了集中式和去中心化可轉換 VC 並且適用代表第三方從事傳送可轉換 VC 作業但並未同時從事 VC 與法定貨幣之間的雙向兌換作業者。也適用在美國境內無具體處所但是在美國有完整或具體業務的外國可轉換 VC 兌換方/管理方。目前美國政府的防制洗錢/打擊資恐規範並不適用使用 VC 但是不參與貨幣傳送作業的可轉換 VC 使用者。除了聯邦法規外，有 48 州對於貨幣傳送方也有相關法規而且很多正在考慮如何讓其傳統的 防制洗錢/打擊資恐以及針對貨幣傳送方的嚴謹法規適用 VC。舉例而言，美國紐約州金融廳（NYFSD）已宣布將在近期公佈一項要求部份虛擬貨幣事業取得「比特幣執照」並遵守防制洗錢/打擊資恐義務、消費者揭露規定、資本要求以及投資規定的法規。

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.

86. 美國進行法律方面的變更是為了適應變化的金融科技。體認到防制洗錢/打擊資恐的保障必需與出現的新支付系統同步，FinCEN 於 2011 年 7 月對其和貨幣服務事業（MSB）有關的規定做了整體修訂 [16]，增加了既有的銀行保密法（BSA）法規架構下創新的 VC 支付方式所需彈性。修訂後的 MSB 在「貨幣傳送服務」定義方面增加了此句「其他取代貨幣的價值」，因此，貨幣傳送方（MSB）的定義有了改變。因為這樣的法規變更，「貨幣傳送服務」現在是指「以任何方式接受來自某個人的貨幣、資金或*其他取代貨幣的價值*以及傳送貨幣、資金或*其他取代貨幣的價值*至另一個地點或個人」[17]。而「貨幣傳送方」是指提供貨幣傳送服務的人（個人或實體）或參與移交資金的任何其他人。因為「貨幣傳送服務」是指「以任何方式接受來自某個人的貨幣、資金或*其他取代貨幣的價值*以及傳送貨幣、資金或*其他取代貨幣的價值*至另一個地點或個人」，所以美國能夠規範參與從某個人接受可轉換 VC 並將之傳送給另一個人或地點的任何法人或自然人，進而將可轉換虛擬貨幣兌換方以及管理方涵蓋在貨幣傳送方內。

NOTES
註

[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.

[1] 舉例而言，位於美國的比特幣錢包提供方/兌換方/支付處理方會將客戶的 VC 錢包與銀行帳戶、傳統收費或簽帳卡連結，提供 VC 購買與接受 VC 兌現的資金來源。在英國-肯亞走廊內、位於英國的比特幣匯款服務則是和位於交付端的肯亞行動支付系統連結。歐洲境內運作的比特幣兌換作業最近新增了知名網絡信用卡和簽帳卡至其可用的資金選項中，後者原本即已包含單一歐元支付區（SEPA）銀行的**匯款**。總部位於澳洲的比特幣交易所在超過 40 個國家都有客戶，會將匯款直接寄送至受益人的銀行帳戶，並無使用比特幣的接收方，但是在銀行端進行的匯款則完全以比特幣進行。

[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

[2] 防制洗錢金融行動工作組織 (2013)，*預付卡、行動支付以及網際網路上的支付服務以風險為基礎的方法指引*，防制洗錢金融行動工作組織，法國巴黎，www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-npps-2013.html

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

[3] **可轉換**是指虛擬貨幣可兌換成法定貨幣。

[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.

[4] **虛擬貨幣兌換方**是指以收取費用（佣金）的方式將虛擬貨幣兌換成實質貨幣、資金、或其他形式的虛擬貨幣以及貴金屬的個人或實體，反之亦然。兌換方一般會接受多樣的支付方式，包括現金、電匯、信用卡和其他虛擬貨幣，因此可能有管理方、無管理方或第三提供方。兌換方可以是個交易所或只是一個交易櫃臺。個人一般會利用兌換方將金錢存入或從虛擬貨幣帳戶取出。

[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.

[5] 因為 VC 可以發揮交易媒介、帳戶單位和/或價值儲存的功能，所以可能會在很多輔助的主管領域內引發問題，包括（例）商品與證券法規。

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

[6] 防制洗錢金融行動工作組織標準包含了防制洗錢金融行動工作組織建議及其各項註釋。

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

[7] *虛擬貨幣的重要定義及其潛在的防制洗錢/打擊資恐風險*（防制洗錢金融行動工作組織，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].

[8] 防制洗錢金融行動工作組織將金錢或價值移轉服務定義為接受現金、支票、其他貨幣商品或其他價值儲存以及以現金或其他形式將對應的金額利用通訊、簡訊、匯款或透過金錢或價值移轉服務提供方附屬的清算網絡支付給受益人的金融服務。此類服務執行的交易可能牽涉到一個或多個仲介以及最後給予第三方的款項，而且**可能包含任何新的支付方式...**[新增強調]。

[9] For the complete list of activities covered by the definition of “financial institutions,” see the *FATF Recommendations* Glossary.

[9] 如需「金融機構」定義所涵蓋的各項活動目錄，請見*防制洗錢金融行動工作組織建議字彙表*。

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

[10] 零售支付的非銀行方、支付委員會與市場基礎設施、國際清算銀行（2014 年 9 月）。

[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

[13] 國家財政部（2014），*南非共和國國家財政部針對虛擬貨幣所做的監督*，取得網址：www.treasury.gov.za/comm_media/press/2014

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

[14] 取得網址：www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf

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

[15] 取得網址： 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)).

[16] *銀行保密法規範 – 定義以及和貨幣服務事業有關的其他規範*，76 FR 43585（2011 年 7 月 21 日），31 CFR § 1010.100(ff)(5)(i)(A)（MSB 規則）。幾乎同時，FinCEN 也發出了一個新的有關預付權限的最終規則（*最終規則 – 定義以及和預付權限有關的其他規範*，76 FR 45403（2011 年 7 月 29 日），31 CFR § 1010.100(ww)(5)(i)(A)（預付權限規則））。

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

[17] 31 CFR § 1010.100(ff)(5)(i)(A)（新增強調）。

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

附件 A
虛擬貨幣 – 重要定義及其潛在的防制洗錢/打擊資恐風險[1]

Appendix A was originally published by the FATF as a stand-alone paper in June 2014
附件 A 最初是防制洗錢金融行動工作組織發佈，是 2014 年 6 月的一份獨立文件。

INTRODUCTION
序言

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.
分散式、有數學公式的虛擬貨幣 – 特別是比特幣[2] – 已經引起越來越多的注意，出現了兩派說法：（1）虛擬貨幣是未來支付系統潮流；以及（2）虛擬貨幣提供罪犯、恐怖主義金主以及其他制裁規避方移動並儲存非法資金一套有力的新工具，在執法單位與其他機關控管範圍外[3]。有鑑於這個背景，所以此份文件根據 2013 年的新型支付產品與服務（NPPS）指引（防制洗錢金融行動工作組織，2013）建議了一套用於了解並處理和其中一種以網際網路為基礎的支付系統：虛擬貨幣相關的防制洗錢/資恐（AML/CFT）風險的概念框架。更明確而言，此文件建議了常見定義的字彙表，釐清何謂虛擬貨幣並針對不同類型的虛擬貨幣根據其不同的商業模式以及運作方式進行區分[4]並找出典型虛擬貨幣系統的參與者。也將 2013 年 NPPS 指引第 IV（A）節列出的風險因子運用在特定類型的虛擬貨幣上，以找出潛在風險；說明部份最近關於虛擬貨幣的調查和執行努力並介紹了部份轄區目前針對虛擬貨幣採取的法規做法，作為例子。

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 shortterm typologies project on this basis was initiated with the following objectives:
雖然2013年的NPPS指引廣泛提及網際網路支付服務，但是並沒有定義「數位貨幣」、「虛擬貨幣」或「電子貨幣」。 也沒有將重點放在虛擬貨幣上，將之和利用實質貨幣（法定貨幣或各國貨幣）（如：Pay-Pal、Alipay或Google Checkout）交易的網際網路支付系統進行區分。也沒有提及去中心化可轉換虛擬貨幣如比特幣。2013年的這份指引也提及：「有鑑於線上替代貨幣的發展性質，防制洗錢金融行動工作組織 可考慮在未來進一步做這方面的努力」（2013 NPPS指引，第11頁，第29段）。後來在此基礎上發起了短期的預示計畫，其目標如下：

- develop a risk-matrix for virtual currencies (or perhaps, more broadly, for both virtual currencies and e-money);
- 替虛擬貨幣（或是更廣義地，同時替虛擬貨幣和電子貨幣）開發一個風險矩陣表；

- 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
- 促進對於參與可轉換虛擬貨幣系統各方以及運作支付系統時可使用虛擬貨幣的方式有更完整的認識；以及

- stimulate a discussion on implementing risk-based AML/CFT regulations in this area.
- 引起針對這方面實施以風險為基礎的防制洗錢/打擊資恐法規的討論。

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.
此預示計畫可能帶來後續 防制洗錢金融行動工作組織 必需做出的政策努力，如：針對虛擬貨幣套用以風險為基礎的方法發出補充指引，以期將提議的字彙和該預示計畫發展出來的風險矩陣表進行結合並說明防制洗錢金融行動工作組織的特定建議如何適用於虛擬貨幣。

KEY DEFINITIONS:
重要定義

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.
建立一組反應虛擬貨幣運作方式的用詞對於讓政府官員、執法機關以及私部門實體能夠分析虛擬貨

幣作為新型支付方式所生潛在的防制洗錢/打擊資恐風險是個重要的第一步。隨著世界各地的立法人員和執法官員開始遭遇虛擬貨幣帶來的挑戰，事跡已經很明顯，那就是我們缺乏一套可以準確反應虛擬貨幣可能存在的各種形式的字彙表。下列詞彙組旨在協助 防制洗錢金融行動工作組織 成員之間的討論。必需注意的一個重點是：這份詞彙表可能隨著虛擬貨幣演進以及立法人員和執法/政府官員持續思索虛擬貨幣帶來的挑戰而改變。儘管如此，提出的這套字彙表旨在針對發展有助於我們進一步了解虛擬貨幣運作方式及其提供的風險與潛在效益的概念工具提供一個共同語言。

VIRTUAL CURRENCY
虛擬貨幣

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.
虛擬貨幣是一種數位價值表述[5]，可以數位方式進行交易並發揮如下功能：（1）交易媒介和/或（2）帳戶單位和/或（3）價值儲存，但是在任何轄區內均不具法定貨幣功能（亦即：提供給債權人時是一個有效、合法的支付方式）[6,7]。並非由任何轄區發行或保證並且僅在透過和虛擬貨幣使用者簽訂協議時才能發揮上述功能。虛擬貨幣和**法定貨幣**（又名「**實質貨幣**」、「**實錢**」或「**各國貨幣**」）不同，後者是一國的硬幣和紙鈔，其設計具備法定功能，可合法流通並且習慣上是在發行國內當作交易媒介進行使用。和**電子貨幣**不同，後者是法定貨幣的數位表述，以電子方式轉讓法定貨幣。電子貨幣是法定貨幣的數位轉讓機制，亦即：透過數位方式轉讓具有法定貨幣功能的價值。

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.
數位貨幣可以指虛擬貨幣（非法定貨幣）或電子貨幣（法定貨幣）的數位表述，因此常和「虛擬貨幣」一詞交替使用。在此文件中，為了避免混淆，僅使用「虛擬貨幣」或「電子貨幣」。

CONVERTIBLE VERSUS NON-CONVERTIBLE VIRTUAL CURRENCY
可轉換和不可轉換的虛擬貨幣

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.
此文件建議將個別虛擬貨幣分成兩個基本類型：可轉換和不可轉換的虛擬貨幣。[8]雖然此文件使用「不可轉換的」和「封閉的」以及「可轉換的」和「開放的」作為同義詞，但仍應強調一點：「可轉換的貨幣」概念並非暗示依職權的可轉換性（亦即：有一套黃金標準），而是事實上的可轉換性

（亦即：因為有市場的存在所以能夠轉換）。因此，虛擬貨幣只有在某些私人參與者願意出價而且有其他人願意接受時才是「可轉換的」，因為「可轉換性」並非法律保證。

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]
可轉換的（或開放的）虛擬貨幣和實質貨幣等值而且可以來回兌換成實質貨幣。[9] 例子包括：比特幣、e-Gold（已停業）、自由儲備銀行（已停業）、第二人生林登美元以及 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.
不可轉換的（或封閉的）虛擬貨幣專用於特定虛擬領域或世界，如：大型多人線上角色扮演遊戲（MMORPG）或亞馬遜網站並受相關使用規範限制，無法兌換法定貨幣。例子包括：專案安特羅皮亞幣；Q 幣；以及魔獸世界金幣。

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.
應注意的是，即使根據管理方設定的條款，不可轉換的貨幣僅得在特定虛擬環境內進行正式轉讓而且不具可轉換性，但是仍可能會出現非正式的二級黑市提供將「不可轉換的」虛擬貨幣兌換成法定貨幣或另一個虛擬貨幣的機會。一般而言，管理方會制裁（包括中止其會員資格和/或沒收剩餘的虛擬貨幣）試圖建立或使用二級市場、違反貨幣使用規則者 [11]。針對特定「不可轉換的」虛擬貨幣建立一個穩健的二級黑市實際上得有效將其轉換成可轉換的虛擬貨幣。不可轉換的特徵因此未必維持靜止狀態。

CENTRALISED VERSUS NON-CENTRALISED VIRTUAL CURRENCIES
集中式和去中心化的虛擬貨幣

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.
所有不可轉換的虛擬貨幣均屬集中式:根據定義,是由建立規則使其不具可轉換性的中央機構發行。相反地，可轉換的虛擬貨幣可能是下列兩者任一：集中式和去中心化。

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.
集中式虛擬貨幣具備單一的管理機關（**管理方**）- 亦即控制該系統的第三方。[12] 管理方發行貨幣、建立其使用規則、維持一套集中支付機制並且有權贖回該貨幣（取消其流通資格）。可轉換的虛擬貨幣之匯率可能是**浮動匯率**（亦即：受市場上的虛擬貨幣供需影響）或**掛鉤式**（亦即：由管理方根據法定貨幣或另一個真實世界的價值儲存［如：黃金或整籃貨幣］設定一個固定價值）。目前絕大部份的虛擬貨幣支付交易都使用集中式的虛擬貨幣。例子有：E-gold（已停業）、自由儲備銀行（已停業）、第二人生林登美元、PerfectMoney、WebMoney「WM 單位」以及魔獸世界金幣。

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]
去中心化虛擬貨幣（又名加密貨幣）是分配式 [13]、來源開放、有一套數學公式的對等式網絡虛擬貨幣，並無中央管理機構亦無中央監督。例子有：比特幣（Bitcoin）；萊特幣（LiteCoin）；與 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.
加密貨幣（Cryptocurrency）係指受密碼演算法保護，以數學為基礎、去中心化的可轉換虛擬貨幣 —亦即採用密碼學原則，執行分散式、去中心化的安全資訊經濟。加密貨幣採用公開與私人金鑰，將價值自一人（個人或實體）移轉至另一人，且每次移轉時都需進行密碼演算加密簽署。加密貨幣帳簿的安全、完整性與平衡，是由一個互相不信賴的交易方（在比特幣世界中稱為「採礦者（miner）」）網路所確保，而這些交易方會保護網路以交換隨機發送之手續費（在比特幣世界中，係指稱為「區塊獎勵（block reward）」的小量新創造比特幣。於部分情況下，亦可能係指使用者為刺激採礦者將其交易納入下一個區塊而提供的交易手續費）的機會。目前共有數百種加密貨幣規格，不過大部分來自比特幣。比特幣採用驗證機制（proof-of-work）來驗證交易與維護區塊鏈。在比特幣提供了第一個完全執行的加密貨幣協定後，使用者對開發其他協定（驗證方法可能較為有效率）的興趣也越來越高，譬如以權益證明（proof-of-stakee）為基礎開發的系統。

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.
於 2009 年發表的**比特幣**，是第一個去中心化可轉換虛擬貨幣，也是第一個加密貨幣。比特幣是由各種獨特數字與字元之字串所組成而成的帳戶單位，且因為個別使用者願意支付對價，而使各帳戶單位構成貨幣單位並且有價值。比特幣能夠以高度匿名的方式在使用者間進行數位交易，且可兌換成（購買或兌現）美元、歐元以及其他法定貨幣或虛擬貨幣。所有人都可以從網路下載用於發送、收取與儲存比特幣以及監控比特幣交易的免費開放來源軟體。使用者亦可透過比特幣交易平台或線上錢包服務，取得功能類似帳戶的比特幣位址。交易（資金流）可在共享交易登記簿（register）取得、並可以比特幣位址辨識。比特幣位址為字母與數字組成的字串，且與個人無法產生系統性連結。因此，比特幣據稱可達「擬真匿名（pseudo-anonymous）」。比特幣金額上限為 2,100 萬比特幣（不過每個單位都可分割為更小的部分），預計將於 2140 年達到 [15]。截至 2014 年 4 月 2 日為止，共創造了 1,250 萬比特幣，若按當日平均匯率計算，總價值略高於 55 億美元。

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)
山寨幣（Altcoin）係指發源貨幣比特幣以外、以數學為基礎、去中心化的可轉換虛擬貨幣。現有山寨幣包括 Ripple；點點幣（PeerCoin）、萊特幣；零幣（zerocoin）；阿儂幣（anoncoin）及狗狗幣（dogecoin）。其中一個熱門的交易平台 Cryptsy，據稱交易超過 100 種不同的虛擬貨幣（截至 2014 年 4 月 2 日）。（Popper, N.，2013 年）

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)).
匿名器（Anonymiser）（匿名工具）係指專為確保比特幣交易來源安全以及協助使用者匿名而設計的工具與服務，譬如暗網（darknet）與混合器（mixer）（譬如：Tor（洋蔥路由）；Dark Wallet（暗黑錢包）；Bitcoin Laundry（混合器））。

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).
混合器（洗幣服務、轉向器（tumbler））是一種可隱匿區塊鏈（blockchain）一連串交易的匿名器，方式則是透過連結同一比特幣位址的所有交易，並以讓人看起來是從不同位址送出的方式一起發送。混合器或轉向器會透過一個複雜、半隨機的連串虛擬交易傳送交易，讓使用者非常難以將特定虛擬貨幣（位址）與特定交易產生連結。混合器服務係指自使用者收取指示，以將資金寄送至特定比特幣位址。混合服務接著會將此交易與其他使用者交易「混合（comingle）」，因此讓人無法清楚瞭解使用者要將資金傳送給誰。（譬如：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.
Tor（原稱洋蔥路由器（The Onion Router））是網際網路上的一個可隱匿 IP 位址、並因此可隱匿網路使用者身份的地下電腦分散式網路，方式是透過全球多部電腦傳送通訊／交易，並以多層加密方式包裹（wrapping）。Tor 讓他人非常難以實際找到網路上託管或存取網站的電腦。而且此等困難度可透過 Tor 網路上的額外轉向器或匿名器更加擴大。Tor 是數種地下分散式電腦網路的一種，這些網路通常被稱為暗網、虛擬空間（cypherspace）、深層網路（the Deep web）或匿名網路，個人使用者可透過此等網路，以專為隱匿其身份與相關電腦活動而設計的方式存取網路內容。

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.
暗黑錢包（Dark Wallet）是一個以瀏覽器為基礎的延伸錢包，目前僅適用 Chrome（Firefox 亦可能適用），可透過下列特性確保比特幣交易匿名進行：自動匿名器（混合器）；去中心化交易；無法審查的群眾募資平台；股票平台與資訊黑市；以及類似絲路（Silk Road）的去中心化市場。

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.
冷儲存（Cold Storage）係指離線比特幣錢包 — 亦即未連接網際網路的比特幣錢包。冷儲存的目的，在協助保護所儲存的虛擬貨幣免於遭受駭入與偷竊。

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.
熱儲存（Hot Storage）係指線上比特幣錢包。因為連結網際網路的緣故，熱儲存比冷儲存要容易遭受駭入／偷竊。

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).
當地交易所交易系統（LETS）係指當地成立的經濟組織，可讓會員與組織內其他會員交易商品與服務。LETS 採用當地創造的貨幣代表價值單位，可用於交易或交換商品或服務。理論上來說，比特幣可視為用於 LETS 的當地貨幣。（譬如：伊薩卡幣（Ithica Dollars）；馬札幣（Mazacoin））。

VIRTUAL CURRENCY SYSTEM PARTICIPANTS
虛擬貨幣系統參與方

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.
交易平台（有時稱為虛擬貨幣交易所） 係指從事虛擬貨幣交換實體貨幣、基金或其他虛擬貨幣形式、甚至貴金屬（反之亦然）之業務以賺取手續費（佣金）的個人或實體。兌換方一般會接受多樣的支付方式，包括現金、電匯、信用卡和其他虛擬貨幣，因此可能有管理方、無管理方或第三提供方。兌換方可以是個交易所或只是一個交易櫃臺。個人一般會利用兌換方將金錢存入或從虛擬貨幣帳戶取出。

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.
管理員（administrator）係指從事**發行**（放入市場流通）集中式虛擬貨幣、建立使用規則、維護集中支付帳簿以及有權**贖回**（停止流通）虛擬貨幣之業務的個人或實體。

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.
使用者係指取得虛擬貨幣並用於購買實體或虛擬商品或服務、或以個人名義寄送移轉物品給另一人（供個人使用）、或以（個人）投資目的持有虛擬貨幣之個人／實體。使用者可透過數種方式取得虛擬貨幣。舉例來說，使用者可 (1) 使用實體貨幣購買虛擬貨幣,（自交易平台購買，或若屬特定集中式虛擬貨幣，則直接向管理員/發行人購買）；(2) 從事賺取虛擬貨幣支付之特定活動（譬如：回應促銷活動、填寫線上問卷、提供實體或虛擬商品或服務）；(3) 在存在部分去中心化虛擬貨幣（譬如：比特幣）之情況下，透過「採礦」（採礦者之定義如下）的方式自行創造貨幣單位，並以贈品、獎勵或參與免費首次發送的方式收取。

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.
採礦者是參與去中心化虛擬貨幣網路的個人或實體，透過執行特殊軟體的方式，解決分散式驗證機制的複雜演算法、或用於驗證虛擬貨幣系統交易之其他分散式驗證系統的複雜演算法。若採礦者為自用之目的而自行創造可轉換虛擬貨幣，譬如持有以進行投資、或用於支付既有義務或購買商品與服務，則採礦者亦可能為使用者。採礦者亦可能以交易平台身份參與虛擬貨幣系統，從事創造虛擬貨幣以出售並換取法定貨幣或其他虛擬貨幣的業務。

Virtual currency wallet is a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency.
虛擬貨幣錢包，是持有、儲存或移轉比特幣或其他虛擬貨幣的方法（軟體應用程式或其他機制／媒介）。

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).
錢包供應商是提供虛擬貨幣錢包的實體（亦即：持有、儲存或移轉比特幣或其他虛擬貨幣的方法（軟體應用程式或其他機制／媒介））。錢包持有使用者的私密金鑰（private key），可供使用者花用分配給區塊鏈上虛擬貨幣位址的虛擬貨幣。錢包供應商透過讓使用者、交易平台以及商家（merchant）更容易進行虛擬貨幣交易的方式，協助前述各方參與虛擬貨幣系統。錢包供應商保管顧客之虛擬貨幣餘額，且通常亦提供儲存與交易安全服務。舉例來說，除了提供比特幣位址外，錢包亦可能提供加密服務；多重金鑰（multi-key）簽章保護、備份／冷儲存；及混合器等服務。所有比特幣錢包都具有互操作性。錢包可線上儲存（「熱儲存」）或離線儲存（「冷儲存」）。（譬如：Coinbase；Multibit；比特幣錢包）。

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.
此外，許多**其他實體**亦可能參與虛擬貨幣系統，且可能與其他交易平台及／或管理員合作，或者獨立運作。包括網頁**管理服務提供商（亦稱為網頁管理員）；**協助商家承兌（acceptance）的**第三方支付匯款方（payments senders）**；**軟體開發商**；以及**應用程式提供商**（本頁所列部分「其他實體」，可能已經納入上述任一種類）。應用程式與軟體開發作業，可能會為合法目的進行：譬如，提高商家承兌以及顧客支付或回應合法隱私權疑慮的便利性；或為非法目的進行：譬如：混合器開發商／營運商，可鎖定採用專為避免主管機關與執法機構審查而設計之產品的非法使用者。

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.
在此需強調，本參與者清單並非無所不包。此外，考量虛擬貨幣技術與營運模型的快速開發，虛擬貨幣系統內可能會出現額外參與者，並因此存在潛在洗錢防制（AML）／打擊資助恐怖主義（CFT）風險。

Taxonomy of Virtual Currencies
虛擬貨幣分類法

	Centralised **集中式**	**Decentralised** **去中心化**
Convertible **可轉換**	Administrator, exchangers, users; third-party ledger; can be exchanged for fiat currency. Example: WebMoney 管理員、交易平台、使用者；第三方帳簿；可交換法定貨幣。 釋例：WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger; can be exchanged for fiat currency. Example: Bitcoin 交易平台、使用者（無管理員）；無受信賴第三方帳簿； 可交換法定貨幣。 釋例：比特幣
Non-convertible **不可轉換**	Administrator, exchangers, users; third-party ledger; cannot be exchanged for fiat currency. Example: World of Warcraft Gold 管理員、交易平台、使用者；第三方帳簿；不可交換法定貨幣。 釋例：World of Warcraft Gold	Does not exist 不存在

LEGITIMATE USES
合法用途

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 onetime 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, Bitcoinmay 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.
虛擬貨幣與其他新型態支付方法一樣，擁有合法用途，且知名創投資本公司也會投資虛擬貨幣新創公司。虛擬貨幣具有改善支付效率以及降低支付與資金轉帳交易成本的潛能。舉例來說，比特幣是可規避交易手續費的全球貨幣，目前係以較傳統信用卡與扣款卡要低的手續費／服務費進行交易，

且可能有利於現有的線上支付系統，譬如 Paypal。[16] 虛擬貨幣亦可協助進行小額付款，因此可讓企業將透過網際網路銷售的非常低成本商品或服務貨幣化，譬如一次性的遊戲或音樂下載。實務上，目前這些品項無法以適當的低單位成本銷售，主要係因傳統信用卡及扣款卡交易成本較高所致。隨著全新虛擬貨幣商品與服務之發展，為非銀行用戶（under-banked）或無銀行帳戶（un-banked）之顧客提供服務時，虛擬貨幣亦可能有助於跨國匯款、以及以其他方式支援普惠金融（financial inclusion）。使用者亦可能持有虛擬貨幣（最知名的是比特幣）以進行投資。這些潛在優點必須進行仔細分析，包括在將虛擬貨幣納入適用其他支付方法的法規架構後、以及在將法定貨幣的交易手續費納入考量之後，其所主張的成本優勢是否仍將持續存在，以及波動性、消費者保護與其他因素[17]是否將限縮其普惠金融的潛能。

POTENTIAL RISKS
潛在風險

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 noncash 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.

基於「2013 年新興支付產品及服務指導（2013 NPPS Guidance）」所列出的許多理由，可交換實體貨幣或其他虛擬貨幣的可轉換虛擬貨幣，可能遭受被濫用於洗錢與資助恐佈分子等目的的風險。首先，這些貨幣的匿名性比傳統非現金支付方法來得高。虛擬貨幣系統可於網際網路上進行交易，其通常特性為不需面對面與顧客接觸，且允許匿名募資（透過未適當辨識資金來源的虛擬交易平台，進行募資或第三方集資）。若未適當辨識匯款方與收款方，這些貨幣亦允許進行匿名轉帳。

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.

去中心化系統尤其容易遭受匿名風險。舉例來說，作為帳戶使用的比特幣位址，原設計就並未包括姓名或其他顧客身份識別資料，且其系統並無中央伺服器或服務提供業者。比特幣協定並未要求或提供參與方之身份識別資料以及驗證資料，亦未產生與真實世界身份必要相關的歷史交易記錄。比特幣並無集中監督機構，且目前並無洗錢防制（AML）軟體可監督與找出可疑交易模式。執法機構無法鎖定單一集中位置或實體（管理員）進行調查或扣押資產（雖然主管機關可以鎖定個別交易平台，要求其提供可能蒐集的客戶端資訊）。因此提供了傳統信用卡與扣款卡或更早期的線上支付系統（譬如 PayPal）所無法提供的匿名程度。

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-toperson transactions may seem to exist in a digital universe entirely outside the reach of any particular country.
虛擬貨幣的全球性，同樣的提高了其潛在的洗錢防制／打擊資助恐怖主義風險。虛擬貨幣系統可透過網際網路（包括透過行動電話）存取，且可用於進行跨國支付與資金轉帳。此外，虛擬貨幣通常採用複雜的基礎架構進行資金轉帳或執行支付交易，且通常涵蓋位於數個國家的數個實體。此等服務的區隔，代表了洗錢防制／打擊資助恐怖主義遵循與監督／執行的責任劃分，可能並不明確。此外，顧客與交易記錄可能由不同實體持有，且通常位於不同管轄地區，使得執法機關與主管機關難以取得這些記錄。此問題因去中心化虛擬貨幣技術與營運模式之快速演化而更加嚴重，包括提供虛擬貨幣支付系統服務之參與方的數量與種類／角色不斷變動。更重要的是，虛擬貨幣系統的元件可能位於無足夠洗錢防制／打擊資助恐怖主義控管措施的管轄地區。集中式虛擬貨幣系統可能串通洗錢活動，且可能蓄意透過洗錢防制／打擊資助恐怖主義機制疲弱的管轄區進行。容許人與人之間匿名交易的去中心化可轉換虛擬貨幣，可能會存在完全位於任何特定國家管轄範圍之外的地區。

LAW ENFORCEMENT ACTIONS INVOLVING VIRTUAL CURRENCY
與虛擬貨幣有關的執法行動

Law enforcement is already seeing cases that involve the abuse of virtual currency for money laundering purposes. Examples include:
執法機關已經開始看到濫用虛擬貨幣進行洗錢活動的情況。例子包括：

LIBERTY RESERVE
自由儲備銀行（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.
在歷史上截至目前為止最大的線上洗錢案例中，美國司法部（US Department of Justice）在 2013 年 5 月控告位於哥斯大黎加的貨幣匯款機構自由儲備銀行（Liberty Reserve）以及其七名主管與員工，從事未經登記的貨幣匯款業務以及洗錢活動，協助處理超過 60 億美元的非法所得。美國財政部（Department of the Treasury）在一項聯合行動中，發現自由儲備銀行是犯下美國愛國者法案（USA PATRIOT Act）第 311 條重大洗錢行動的金融機構，並有效的將其自美國金融系統中去除。

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).
自由儲備銀行成立於 2006 年，是專為規避主管機關與執法機構監督所設計，以協助罪犯從事匿名且無法追蹤金融交易的方式，協助罪犯散佈、儲存、與洗清信用卡舞弊、盜竊、投資舞弊、電腦駭客入侵、販毒、以及兒童色情有關的所得。自由儲備銀行的營運規模十分龐大，全球共超過一百萬名使用者，包括美國境內超過 200,000 名使用者，並且處理了將近 5,500 萬筆交易，且幾乎全部都是非法交易。自由儲備銀行擁有其自有的虛擬貨幣自由幣（Liberty Dollars，簡稱 LR），不過在交易的兩端，轉帳金額都是以法定貨幣（美元）計價與儲存。

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]
使用者在使用 LR 貨幣前，需先透過自由儲備銀行網站開立帳戶。雖然自由儲備銀行表面上要求基本的身份識別資訊，不過卻並未進行驗證。使用者經常會使用虛假姓名開立帳戶，包括公然的使用罪犯姓名（「Russia Hackers」、「Hacker Account」、「Joe Bogus」）以及公然的使用虛假地址（「123 Fake Main Street, Completely Made Up City, New York」）。為進一步提高匿名性，自由儲備銀行會要求使用者透過推薦第三方交易平台存款與提款 — 通常是未經核准的貨幣匯款公司，且位於俄羅斯以及交易時無嚴格政府洗錢監督或法規的幾個國家，譬如馬來西亞、奈及利亞以及越南。透過避免使用者直接存款與提款，自由儲備銀行規避了透過銀行交易或其他可能創造集中紙本軌跡的活動蒐集使用者資訊的責任。在開戶之後，使用者可透過自其帳戶將 LR 轉帳給其他使用者的方式，與其他自由儲備銀行使用者進行交易，包括接受 LR 作為支付方式的前檯公司「商家」。於支付額外「隱私手續費（privacy fee）」（每筆交易 75 美分）後，使用者可於進行資金轉帳時隱藏其自由儲備銀行帳號，使其轉帳交易完全無法追蹤。在知道已經遭美國執法機構調查之後，自由儲備銀行假裝關閉哥斯大黎加的營運，不過卻繼續透過幾家空殼公司進行交易，並透過其位於澳洲、賽浦路斯、中國、香港、摩洛哥、俄羅斯、西班牙與其他各國的帳戶移動數百萬元資金[18]。

SILK ROAD
絲路

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.
2013 年 9 月，美國司法部解密了一件控告案件，控告據稱為絲路（Silk Road）之業主與營運商，共謀從事販毒、電腦駭客入侵以及洗錢活動。絲路是一個隱匿的網站，專門設計供其使用者匿名買賣毒品、武器、遭竊之身份識別資訊以及其他非法商品與服務，且使執法機構無法追蹤。美國司法部亦扣押了該網站,以及自扣押的電腦硬體中取得當時市值超過 3,360 萬美元的將近 173 991 比特幣。相關人員是於 2013 年 10 月在舊金山遭到逮捕，並於 2014 年 2 月遭到起訴；目前調查作業仍在進行當中。

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.
絲路是在 2011 年 1 月成立，經營仲介匿名犯罪交易的全球性網路黑市市場，數千名毒販以及其他非法供應商使用該網站散佈非法商品與服務給超過十萬名買方，且估計其中三分之一來自美國境內。該網站遭控共經手將近 12 億美元的總營收（超過 950 萬比特幣），並因此賺取了將近 8,000 萬美元（超過 600,000 比特幣）的佣金。此等交易漂白了數億美元的資金（依據扣押日比特幣價值計算）。佣金比率介於總銷售價格 8%到 15%。

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
絲路透過經營網路以及僅接受比特幣作為支付方式的方法，達到交易匿名。在絲路上以比特幣為專屬貨幣，讓買賣雙方都能進一步隱匿其身份，因為點對點（P2P）比特幣交易的匯款方與受款方，都是透過匿名比特幣位址／帳戶辨識身份。此外，使用者可取得無限數量的比特幣位址，且每筆交易都使用不同的位址，進一步隱匿了非法所得的軌跡。除絲路交易（請參下列說明）內建的轉向器服務外，使用者亦可運用額外「匿名器」。

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]
絲路的支付系統扮演內部比特幣銀行的角色，且所有絲路使用者都必須持有帳戶才能透過絲路網站進行交易。所有絲路使用者都必須至少擁有一個與其絲路帳戶有關的絲路比特幣位址（且可能擁有數千個），且係儲存於絲路所控制的伺服器所維護的錢包中。於進行購買交易時，使用者會取得比特幣（通常是透過比特幣交易平台），並透過與其絲路帳戶有關的比特幣 位址支付至指定帳戶。於發生購買交易時，絲路會將使用者的比特幣移轉至其所維護的託管帳戶，並將於交易完成後，將使用者／買方的比特幣自託管帳戶轉帳至廠商的絲路比特幣位址。絲路並且針對每筆買賣交易進一步採用「轉向器」，並將（如其網站說明）「透過複雜、半隨機的虛擬交易支付所有款項 -- 使外界幾乎不可能將您的支付交易與離開本網站的任何比特幣產生連結。」[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.
在歷經八年對 Western Express 跨國網際網路犯罪集團進行調查之後，該集團 16 名成員因參與全球身份盜竊／網路舞弊計畫而被提起控告或認罪。此犯罪集團之成員主要透過網際網路「偽造（carding）」網站互動與溝通，這些網站係用於非法交易遭竊信用卡以及個人識別資訊，並使用虛偽身份、匿名即時傳訊帳戶、匿名 email 帳戶以及匿名虛擬貨幣帳戶，隱匿犯罪企業之存在與目的；規避執法機構與主管機關的調查；以及維持其匿名狀態。

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.
此犯罪企業是由位於多個國家的賣家、買方、網路犯罪服務提供商以及洗錢方所組成，範圍涵蓋烏克蘭、東歐至美國。相關廠商透過網際網路賣出了將近 100,000 筆遭竊的信用卡卡號以及其他個人識別資訊，且收受的款項大部分是以 e-Gold 及 WebMoney 支付。買方運用遭竊的身份識別資訊偽造信用卡以及購買昂貴的贓物商品（包括透過重新運送方式）、從事其他犯罪（譬如竊盜及非法持有遭竊資產）與舞弊行為，並賺取了將近 500 萬美元的信用卡舞弊所得。網路犯罪服務提供方，透過為賣家與買方提供電腦服務的方式，促進、幫助與協助購買、銷售與詐騙使用遭竊信用卡卡號以

及其他身份識別資訊。洗錢方會以各種高科技方法進行網路犯罪集團非法所得的洗錢作業，並因此透過多個帳戶轉移超過 3,500 萬美元資金。

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.

整個作業的中心是位於美國紐約曼哈頓的紐約公司 Western Express International, Inc.,，扮演虛擬貨幣交易平台以及未登記貨幣匯款機構角色，負責協調與協助執行犯罪企業採用的網際網路支付方法，以及漂白集團的犯罪所得。Western Express International 是美國境內最大的虛擬貨幣交易平台之一，為網路犯罪集團交換總金額達 1,500 萬美元的 WebMoney 以及 2,000 萬美元的 e-Gold，以及運用銀行與傳統貨幣匯款機構移動大量金錢。該公司亦透過其網站（包括 Dengiforum.com 與 Paycard2000.com）提供與匿名移動金錢以及規避申報規定之方法有關的資訊與協助。

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.

Western Express International 及其烏克蘭裔業主／營運商，於 2013 年 2 月在紐約州承認洗錢、舞弊與共謀犯罪罪行。（2006 年 2 月，Western Express 也被控告經營非法支票兌現／匯款轉帳服務）。在 2013 年 6 月之後，另外三名被告也被判決有罪；2009 年 8 月還有幾名被告也承認了罪行。目前還有兩名被告在逃。此項調查作業是由美國特勤局與曼哈頓（紐約郡）地檢署共同執行，並且由曼哈頓地檢署成功起訴。

NOTES
註

[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.

[1] 本文件的第一版草稿是由澳洲、加拿大、俄羅斯、英國與美國針對 2014 年 2 月舉行的防制洗錢金融行動工作組織（FATF）會議所編製。在邀請所有與會代表針對草稿提供意見，以在下次會議通過最終報告後，共收到 10 名代表的回饋意見，並將其納入修訂版本。

[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.

[2] 「比特幣」係指用於創造虛擬貨幣的開放原始碼軟體、以及因此建立的點對點（P2P）網路；「比特幣」係指個別虛擬貨幣單位。

[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.

[3] 另外也需注意的是，部分觀察家，包括美國聯準會前任主席艾倫・葛林斯潘（Alan Greenspan）、荷蘭央行前任行長努特 魏霖克（Nout Wellink）、以及諾貝爾獎得主經濟學家羅伯特・席勒（Robert Shiller），認為虛擬貨幣正在逐漸消失或化成泡沫，如同17世紀荷蘭的鬱金香狂熱（Tulipmania）一樣。

[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.

[4] 虛擬貨幣是一個複雜的議題，不只存在洗錢防制／打擊資助恐怖主義問題，還包括其他法規議題，包括消費者保護、審慎安全、稅務與穩健法規、以及網路IT安全標準。因此預計採用的詞彙將影響許多輔助法規管轄範圍。所有相關政府實體虛擬貨幣都採用一致的名詞以及具有相同的概念，對避免不必要的重複投入及／或作業互相干擾方面非常重要，並有助於政府主管機關運用多種不同的處理角度以及專業領域，有效的找出與處理虛擬貨幣相關議題。

[5] **Digital representation** is a representation of something in the form of digital data—i.e., computerized 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,

[5] **數位表示法（Digital representation）**係指以數位資料形式表現某物 — 亦即採用不相關（不連續）的數值表示構成資訊的電腦化資料，對比連續、或以連續方式呈現、或運用連續功能表示資訊的類比訊號。實質物件，譬如隨身碟或比特幣，可能包括虛擬貨幣的數位表示，不過最終貨幣只有在透過網際網路與虛擬貨幣系統產生數位連結時方具有貨幣功能。

[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.

[6] 法定貨幣狀態，並不必然代表實體或個人需接受以特定種類法定貨幣支付。舉例來說，在許多管轄區，私人企業、個人、或組織可自行制訂內部政策，決定是否接受以該管轄區之實體貨幣或錢幣（現金）支付商品及／或服務款項。

[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.

[7] 此定義與歐洲央行（ECB）於2012年所做出的定義不同，後者將虛擬貨幣定義為「一種未受法令規範的數位貨幣，係由開發商所發行、且通常亦係由開發商所控制，並獲特定虛擬社群之成員所使用與接受」，歐洲央行*虛擬貨幣制度（ECB, Virtual Currency Schemes）*（2012年10月），第6頁；歐洲央行在其報告的第13頁承認，「若發生了基本面的變動，其定義未來可能需要修改。「其定義現在看來似乎過於狹隘，因為像比特幣這樣以數學為基礎的去中心化虛擬貨幣，並非由集中開發商所發行與控制，而且部分管轄區（譬如：美國、瑞典與泰國）現在已經開始規範虛擬貨幣。

[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).

[8] 此等分類方式與歐洲央行的三部分分類不同。歐洲央行將虛擬貨幣分為以下三類：「第1類 . . . 係指線上遊戲所使用的封閉性虛擬貨幣制度；第2類 . . . [係指] 單向流動的制度（通常為流入），亦即規範有購買虛擬貨幣的轉換率，而虛擬貨幣則可用於購買虛擬商品與服務 . . .（例外情況甚至包括實體商品與服務）. . . 第3類 [係指] 雙向流動的制度，亦即功能類似所有可轉換[實體]貨幣的虛擬貨幣，規範有[買賣]虛擬貨幣的轉換率，而虛擬貨幣則可用於購買虛擬[與]實體商品與服務」歐洲央行*虛擬貨幣制度（ECB, Virtual Currency Schemes）*，第6頁本討論報告採用了較簡單的二分法分類方式，因為目前只有可進出正式金融產業的（完全）可轉換虛擬貨幣，才會存在重大洗錢防制／打擊資助恐怖主義風險。這是因為洗錢行為需：轉換或移轉（非法資金）；隱匿或隱瞞（非法資金）來源／源頭；或取得／持有／使用（非法資金）。

[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).

[9] 部分可轉換虛擬貨幣可透過發行管理員直接交易（直接交易）；其他則可透過虛擬貨幣交易平台交易（第三方交易）。

[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/

[10] 舉例來說，WebMoney 屬於虛擬貨幣，因為過程中會有「有價值物品」（資產）以非法定貨幣形式移轉與儲存，而擔保人所儲存之有價值物品財產權的衡量單位，則是相關種類的 WebMoney 所有權單位（WM）。http://wmtransfer.com/eng/about/

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

[11] 舉例來說，儘管有這些干擾措施存在，還是有幾個交易平台允許黑市轉換魔獸世界金幣。

[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.

[12] 第三方係指參與交易、且非當事人、與交易中其他兩名參與人亦無聯屬關係的個人或實體 — 亦即在商業或金融交易中擔任雙方當事人（譬如：匯款方與受款方、買方與賣方）間中立實體之第三方。第三方之參與程度，視商業或金融交易之種類而有所不同。舉例來說，一個線上支付入口網站（譬如 PayPal）在零售交易中擔任第三方。賣方提供商品或服務；買方使用信用卡或扣款卡參與 PayPal 支付服務；並由受信賴的第三方完成金融轉帳交易。同樣的，在不動產交易中，第三方公證公司擔任買方與賣方間之中立代理人，向賣方取得文件及向買方取得貨幣等為完成交易所需的項目。

[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.

[13] 分散式是一個特定的術語，代表了去中心化以數學為虛擬的貨幣的基本特性：交易則透過*分散式*驗證機制加以驗證。在參與者網路中，所有交易都是*去中心化*，由各參與人運用演算法驗證交易。

[14] Apart from the initial creation and issuance of ripple coins (RXP), Ripple operates as a decentralized 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.

[14] 除首次創造與發行 ripple 幣（RXP）外，Ripple 扮演了去中心化虛擬貨幣的角色。Ripple 的創辦人創造了全部 1,000 億 ripple 幣並保留其中 200 億，將由獨立的實體 Ripple Labs 經銷。然而，所有交易都是透過一個去中心化的電腦網路，採用 Ripple 的開放來源協定，並記錄在經常更新 Ripple 帳戶與交易的共享帳簿。

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

[15] 2140 起將不再提供區塊獎勵，且採礦者將只能賺取交易手續費。

[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.

[16] 舉例來說，PayPal 正在積極開發透過 PayPal 平台接受與結算比特幣的方法，而摩根大通（JP Morgan Chase）則已針對一個運用數學基礎虛擬貨幣協定的線上電子支付系統提出美國專利申請，該系統可讓使用者在不需提供帳號或帳戶名稱的前提下進行匿名支付，虛擬貨幣則儲存在摩根大通電腦並透過共享記錄驗證，形式非常類似比特幣系統的「區塊鏈」。

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

[17] 舉例來說，虛擬貨幣系統是否能夠連接其他金融服務，譬如授信與保險，則仍尚待觀察。

[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.

[18] 自由儲備銀行調查與關閉的行動，牽涉 18 個國家與管轄地區的執法機構，包括哥斯大黎加；荷蘭；西班牙；摩洛哥；瑞典；瑞士；塞浦路斯；澳洲；中國；中國香港；挪威；拉脫維亞；盧森堡；英國；俄羅斯；加拿大；及美國，以抑制犯罪所得、沒收網域名稱以及扣押伺服器。

[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.

[19] 絲路（Silk Road）調查行動牽涉多個美國執法機構，帶領聯邦調查局（FBI）紐約特殊行動暨網路犯罪處（New York Special Operations and Cyber Division）、以及緝毒署（DEA）紐約有組織犯罪緝毒小組（Organized Crime Drug Enforcement Strike Force）（包括 DEA、美國國稅局（IRS）、紐約市警局、美國移民及海關執法局（ICE）、國土安全部（HSI）、紐約州警察、美國菸酒槍炮及爆裂物管理局、美國特勤局、美國法警局、美國財政部外國資產管制辦公室（OFAC）、紐約州財政稅務廳（NY Department of Taxation）的探員與官員，並獲得, with assistance and support of the ICE-HIS 芝加哥分局、美國司法部電腦犯罪暨智慧財產與資產沒收及洗錢處（Computer Crime and Intellectual Property and Asset Forfeiture and Money Laundering Section）、美國紐約州南區地檢署以及外國執法機構的協助，尤其是冰島雷克雅維克市警局以及法國中央打擊資訊科技與通訊犯罪小組（Central Office for the Fight Against Crime Linked to 資訊 Technology and Communication）。

BIBLIOGRAPHY AND SOURCES
參考書目與資料來源

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
防制洗錢金融行動工作組織（FATF）（2013 年），防制洗錢金融行動工作組織預付卡、行動支付與網路基礎支付服務之風險基礎指引（*Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*），法國 防制洗錢金融行動工作組織
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-rivalvirtual-currencies-vie-for-acceptance/?_r=0, accessed June 2014.
Popper, N.（2013 年）「比特幣的世界：虛擬貨幣承兌的競爭（In Bitcoin’s Orbit: ival Virtual Currencies vie for Acceptance）」，*紐約時報（New York Times）*，*Dealb%k*（2013 年 11 月 24 日）
http://dealbook.nytimes.com/2013/11/24/in-bitcoins-orbit-rivalvirtual-currencies-vie-for-acceptance/?_r=0 ，2014 年 6 月存取

APPENDIX B
HOW DECENTRALISED CONVERTIBLE VIRTUAL CURRENCY WORKS AS A PAYMENTS MECHANISM

附件 B
去中心化可轉換虛擬貨幣支付機制的運作方式（HOW DECENTRALISED CONVERTIBLE VIRTUAL CURRENCY WORKS AS A PAYMENTS MECHANISM）

INTRODUCTION
序言

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.

1. 比特幣與其他去中心化可轉換虛擬貨幣（VC），有機會創造出一個開創性的另類數位支付平台。比特幣網路，是專為網路商務提供電子**點對點（P2P）**[1] 支付機制而設計。其目的在讓使用者以直接互相移轉虛擬貨幣以及將近即時交易的方式，避開金融機構作業，並因此免除中介成本（譬如交易手續費）以及支付不確定性。

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.

2. **去中心化虛擬貨幣（通常亦稱為 cryptocurrency）**[2] 是一個分散式、開放來源、以數學為基礎的可轉換虛擬貨幣，不需「受信賴第三方」驗證交易以及維護（與對帳）交易帳簿。比特幣提供了第一個完全執行的cryptocurrency協定，並因此創造了全球第一個去中心化虛擬貨幣支付機制。後續另外定義了數百種 cryptocurrency 規格，且大部分源自比特幣。不過業界還是持續關注替代方式的開發，尤其是更有效率的協定、使用不同驗證機制[3] 驗證交易以及維護線上分散式交易帳簿。

SCOPE
範圍

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 **single-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.

3. 本附件概要說明去中心化可轉換虛擬貨幣[4]（VC）支付機制的運作方式。說明重點在去中心化可轉換虛擬貨幣網路的功能面，而非協定的技術面，並且著重說明單一**貨幣虛擬貨幣支付網路**（譬如比特幣），而非**多種貨幣（currency-agnostic）平台（譬如** Ripple）。[5] 本文件 (1) 說明了去中心化虛擬貨幣的概念架構，以及單一貨幣去中心化虛擬貨幣支付網路的基本元件；(2) 逐步說明使用者在參與比特幣網路及進行交易應該做的事；以及 (3) 列出許多近期出現、可協助運用此全新支付機制的第三方虛擬貨幣支付產品與服務（VCPPS）。本文件以比特幣說明單一貨幣去中心化可轉換虛擬貨幣支付機制，因為比特幣比其他去中心化虛擬貨幣擁有市場先行者（first-mover）優勢，規模亦相對較為龐大（以交易數量、價值與市值來看），另外也是因為至今為止，單一貨幣去中心化虛擬貨幣支付網路的創投資金以及開發基礎架構，都是針對比特幣而進行。為了清楚敘述，在此舉一個比特幣實例來說明；本釋例並未反映 防制洗錢金融行動工作組織 的任何看法，也不去預測主流支付機制最後是否會獲致成功。本文件所使用的許多名詞，都是採用 防制洗錢金融行動工作組織在 2014 年 6 月所發佈 「*虛擬貨幣 — 主要定義與潛在洗錢防制／打擊資助恐怖主義風險（Virtual Currencies — Key Definitions and Potential 防制洗錢/打擊資恐 Risks）（2014 年6 月虛擬貨幣文件）報告*」**附件 A** 的定義。未定義於附件 A 的，於此以粗體字表示。

DECENTRALISED VIRTUAL CURRENCY AS A PAYMENTS PLATFORM
去中心化虛擬貨幣支付平台

CONCEPTUAL FRAMEWORK FOR DECENTRALISED VC PAYMENTS MECHANISMS
去中心化虛擬貨幣支付機制的概念架構

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.

4. 去除金融機構在電子支付中的中介角色，是一個重大的概念變動。比特幣協定，是專為複製金融機構在電子與現金交易中介時所通常會執行的多種信賴功能而設計。其中一個關鍵的信賴功能，是擔保避免發生「雙重支付（double-spending）」以及虛偽交易。[6] **雙重支付**係指虛擬貨幣使用者將虛擬貨幣所有權移轉給另一人，然後又將相同虛擬貨幣的所有權移轉給第三人。雙重支付問題發生的原因，在去中心化虛擬貨幣以數位檔案的形式存在，因此複製很簡單，且並無受信賴的主管機關維護集中交易記錄。

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.

5. 為了預防雙重支付以及虛偽交易，比特幣採用稱為**區塊鏈**[7] 的分散式線上公共帳簿、以及公開金鑰加密驗證交易。**公開金鑰加密**是一個加密方法，會分配兩組金鑰給使用者：**公開金鑰與私密金鑰**。**公開金鑰（又名：比特幣位址）是一個獨特的辨識工具，功能類似供受款方收取 email 的** e-mail 位址，扮演收取比特幣的帳戶角色。**私密金鑰**是一個功能類似密碼的加密代碼，可讓使用者簽署虛擬貨幣交易以及移轉比特幣給其他位址。使用私密金鑰證明比特幣的所有權。所有比特幣公開金鑰／位址都有相符合的私密金鑰。私密金鑰都與比特幣位址具有數學方面的相關性，且經特殊設計，可運用私密金鑰計算比特幣位址，但無法反過來運用比特幣位址計算私密金鑰，因此可創造交易與帳戶安全。公開金鑰需與私密金鑰（簽章）搭配，才能傳送虛擬貨幣。

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.

6. 比特幣協定需驗證、登入所有交易、以及將交易揭露[8] 在區塊鏈上。**區塊鏈**扮演公開交易報告系統的角色。由各**區塊**構成；每個區塊按時間順序分組通報交易。於啟動（提議）交易時，會向網路與各參與方（稱為採礦者）廣播、執行特殊軟體、以解決複雜數問題並確認提議交易中的比特幣尚未耗用的方式驗證交易、以及將其新增至區塊鏈[9]。此等稱為「**採礦**」[10] 的相同分散式（社群）驗證流程，將會創造出新的比特幣，獎勵第一個解決用於驗證交易之演算法的採礦者[11]。過去曾發生的所有交易，必須依序記錄在區塊鏈上。

PARTICIPATING IN THE BITCOIN NETWORK TO SEND AND RECEIVE BITCOINS
參與比特幣網路以寄送與收取比特幣

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.

7. 比特幣網路原來只是一個 P2P 移轉系統，無第三方產品與服務。使用者會取得與儲存比特幣，並自行從事交易。如同下列說明，比特幣支付基礎架構已經快速演化，現在已經可以提供多種第三方支付產品與服務，協助取得、儲存與使用比特幣。下節說明參與比特幣網路以及執行比特幣支付交易的基本元件與步驟。最後一節則介紹提供第三方比特幣產品與服務的實體。

PARTICIPATION WITHOUT INTERMEDIARIES
在無中介機構的前提下參與

Step One: Obtain the Public Keys (Addresses), Private Keys, and Wallets Needed to Participate in the Bitcoin Network
步驟一：取得參與比特幣網路所需的公開金鑰（位址）、私密金鑰及錢包。

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.

8. 在參與比特幣網路且無中介機構介入的最基本情境下，使用者需自相關網路下載比特幣軟體（稱為比特幣「客戶端」）並安裝至其電腦。客戶端軟體包括一個錢包程式，可產生與儲存公開-私密金鑰組合。軟體所產生的公開金鑰，係以獨特比特幣位址（24 至 37 字元的英數字字串）表示，可作為使用者收取比特幣支付以及進行比特幣交易的帳戶。使用者可依據其需求創造／取得任何數量位址。客戶端所產生與儲存的私密金鑰（若屬比特幣，則為隨機的 64 位數英數字），與特定比特幣位址具有數學相關性。實務上，私密金鑰**就是**使用者的虛擬貨幣。錢包程式也會與比特幣網路上的其他比特幣位址通訊，讓使用者能夠收送比特幣。使用者透過電腦、行動電話或其他數位裝置上的錢包（一個電腦檔案）存取其比特幣。使用者亦可自線上第三方錢包供應商下載軟體錢包程式。

部分軟體錢包需在比特幣客戶端上操作，其他則可讓使用者不需下載整個比特幣客戶端。使用者下載並儲存於其自有電腦或其他數位裝置的錢包，稱為**未託管錢包。**使用者可線上（「熱儲存」）或離線(「冷儲存」)儲存其未託管錢包。未託管錢包的所有人，需負責提供錢包安全以及保護私密金鑰。

Step Two: Obtain Bitcoins
步驟二：取得比特幣

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.

9. 使用者可透過幾種方法取得比特幣。舉例來說，使用者可 (1) 使用貨幣或其他虛擬貨幣向第三方交易平台購買虛擬貨幣；(2) 從事可賺取虛擬虛擬貨幣支付的特定活動（譬如：回應促銷活動、填寫線上問卷、提供實體或虛擬商品或服務）；(3) 以贈品或獎勵的方式收取；以及 (4) 透過採礦[12] 的方式自行賺取比特幣，如上所述。採礦活動目前大部分集中在專業採礦池；使用者通常會向第三方交易平台取得比特幣。

Step Three: Transfer Bitcoins
步驟三：移轉比特幣

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.

10. 比特幣交易會進出比特幣錢包的比特幣位址，並且進行數位簽署以保障安全。欲使用比特幣支付商品或服務款項或匯款 — 亦即花用或匯出比特幣 — 使用者需使用私密金鑰解鎖其數位錢包，並以數位方式簽署交易。交易本身包括三項資訊：(1) 輸入資訊（用來發送*比特幣給現有匯款方的*比特幣位址；(2) 金額資訊（匯款方移轉的比特幣金額）；及 (3) 輸出資訊（受款方的比特幣位址）。這些自動執行的功能都是透過錢包軟體處理。使用者（透過所下載的軟體），自其錢包將比特幣發送到比特幣網路。如上所述，於發送時，比特幣採礦者會將其納入交易區塊、驗證交易並納入區塊鏈以及確認交易。大部分由使用者自行執行、無中介機構介入的比特幣交易，都不需支付交易手續費。目前則建議使用者自願支付手續費，鼓勵採礦者加快確認速度。

Figure 1. The three essential elements of a Bitcoin transaction
圖 1：比特幣交易的三大要件

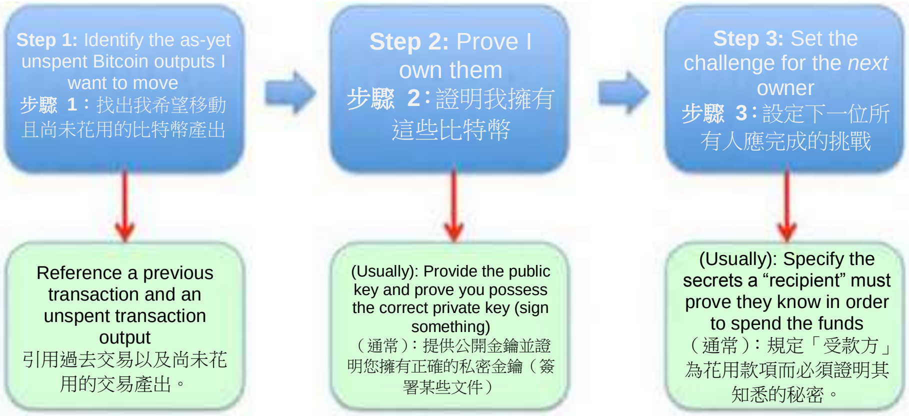
Step 1: Identify the as-yet unspent Bitcoin outputs I want to move
步驟 1：找出我希望移動且尚未花用的比特幣產出
Step 2: Prove I own them
步驟 2：證明我擁有這些比特幣
Step 3: Set the challenge for the *next* owner
步驟 3：設定下一位所有人應完成的挑戰
Reference a previous transaction and an unspent transaction output
引用過去交易以及尚未花用的交易產出。
(Usually): Provide the public key and prove you possess the correct private key (sign something)
（通常）：提供公開金鑰並證明您擁有正確的私密金鑰（簽署某些文件）
(Usually): Specify the secrets a "recipient" must prove they know in order to spend the funds
（通常）：規定「受款方」為花用款項而必須證明其知悉的秘密。

Table courtesy of Bach, A., Corallo, M. Dashjr, L. et al (2014)[13].
表格由 Bach,A.、Corallo, M.及 Dashjr, L.等人提供（2014 年）[13]。

Step Four: Confirmation
步驟四：確認

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]

11. 有了比特幣，公告支付給受款方位址的動作幾乎是同時完成。然而，交易仍需由採礦者合併納入一個區塊，以開始確認流程。平均而言，比特幣網路上的採礦者約需 10 分鐘才能建立（或解開）特定區塊。區塊上的交易在納入區塊鏈後，仍屬區塊鏈的一部分。區塊鏈中所有後續區塊，都會記錄在包括特定交易的區塊上方。在包括特定交易的區塊納入區塊鏈後，代表**確認**[14] 該交易的進行**確認**，代表網路上的參與人認同受款方所收取的特定比特幣並未被發送給任何他人，且將被視為受款方的財產。在受款方可以花用／發送其所收取比特幣之前，必須先確認交易。區塊鏈中在包括特定交易的區塊上打造的所有後續區塊，會整合確認交易的共識並預防交易回轉。除首次確認外，在交易經足夠確認以及可安全花用／傳送虛擬貨幣單位之前，使用者可自行決定要將多少後續區塊納入區塊鏈。一般而言，在區塊鏈顯現出特定數量確認（後續區塊） — 通常為六個 — 之前，不視為交易已經過足夠確認。[15]

PARTICIPATION WITH INTERMEDIARIES: EMERGING BITCOIN INFRASTRUCTURE
在存在中介機構的情況下參與：新興比特幣基礎架構

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 decentralized virtual currency "ecosystem" is rapidly evolving, some of these third party VCPPS are described below.

12. 目前有越來越多新創公司開始提供全新虛擬貨幣支付產品與服務（VCPPS），協助使用者使用去中心化虛擬貨幣支付網路，尤其是比特幣。在此環境下，使用者（消費者與商家）不需下載比特幣客戶端或未託管錢包、儲存與保護其私密金鑰以及自行執行交易（如上述），而是運用多種第三方公司，使其儲存虛擬貨幣以及執行去中心化虛擬貨幣交易的作業變得更加輕鬆。此等第三方產品與服務有多種營運模式。部分公司提供單一種類服務，其他公司則提供多種產品與服務給顧客。去中心化虛擬貨幣「生態系統（ecosystem）」正在快速演化中，茲簡述部分第三方 VCPPS 如下。

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.

13. **錢包提供方（Wallet provider）**使用者不需下載軟體並自行創造位址，而可透過於比特幣交易平台或線上錢包服務開立帳戶的方式，取得比特幣位址。使用者亦不需自交易平台取得比特幣、並儲存在其自有數位裝置上的未託管錢包，而可透過**錢包供應商**[17] 所提供與保護的**託管錢包**[16] 取得所儲存的虛擬貨幣。錢包供應商會維護顧客的虛擬貨幣餘額，且通常亦需提供儲存與交易安全服務。除提供比特幣位址外，錢包供應商亦可能提供加密；多重金鑰（multi-key）簽署保障；備份／冷儲存；以及混合器服務。所有比特幣錢包都具有互操作性。錢包供應商可能提供比特幣熱儲存或冷儲存服務，顧客則保留其私密金鑰及控管虛擬貨幣的移轉。或由錢包供應商為顧客的虛擬貨幣持有公開與私密金鑰，並依據顧客指示將虛擬貨幣移轉給第三方，以進行支付與發送匯款。**許多虛擬貨幣交易平台都提供錢包服務**（亦即：亦扮演錢包供應商），可讓使用者取得位址並將其虛擬貨幣儲存在交易平台中的帳戶。目前，第三方錢包的營運模式主要有兩種。第一種是較為「傳統」的錢包託管服務，顧客擁有自己的錢包，不過檔案存放在第三方錢包服務的伺服器。（此模型有許多種

變化形式，尤其是與託管服務是否擁有私密金鑰控制權有關的部分。）大部分交易平台目前則逐漸轉為第二種模型。在此模型中，顧客資金保管在共管帳戶，公司則依據顧客指示移轉／扣款。此營運模式可以冷儲存的型態儲存較多虛擬貨幣資金，且不會影響顧客存取其虛擬貨幣的權限。

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.

14. **虛擬貨幣支付處理商（亦稱為第三方支付匯款方；商家 支付處理商）**是協助商家承兌的實體 — 亦即是協助將虛擬貨幣款項，自使用者（顧客）移轉給提供消費性商品或服務的商家或其他公司或專業人員的實體。一般而言，支付處理商會提供軟體應用程式或可內嵌的程式碼，可讓商家或其他公司於其網站或實體據點承兌虛擬貨幣款項，以及以電子方式傳送虛擬貨幣至商家的錢包（由處理商或其他錢包供應商代管、或未託管並由商家直接持有），或將部分或全部虛擬貨幣轉換為法定貨幣，並依指示將 e-money 款項傳送至商家的帳戶。比特幣與其他去中心化可轉換虛擬貨幣是網路支付系統，專為去除中間人所設計，因此在虛擬貨幣生態系統中出現虛擬貨幣處理商可能顯得有些奇怪。不過，處理商會努力讓對不瞭解科技的一般公司，也能夠輕鬆的承兌虛擬貨幣支付款。部分虛擬貨幣支付處理商，可能會為接受可轉換虛擬貨幣但害怕貨幣波動的商家，提供交易（轉換）服務，使其能夠為避險目的立即將收到的虛擬貨幣轉換為其選擇的法定貨幣。處理商也會讓（不瞭解科技的）消費者在使用虛擬貨幣購買商品與服務時更加便利，為消費者提供更多零售支付方法的選擇。

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.

15. **比特幣提款機（又名 BTM）**係指用於將法定貨幣交換成比特幣及／或其他虛擬貨幣（反之亦然）的自動化機器。依據設計功能之不同，個人可使用比特幣提款機購買比特幣（且可能包括其他虛擬貨幣）（單向機器）、或同時可購買虛擬貨幣、以虛擬貨幣兌換法定貨幣、以及於提款機提領法定貨幣交換可轉換虛擬貨幣（雙向機器 –亦即以法定貨幣兌換比特幣、或以比特幣兌換法定貨

幣）。比特幣提款機產業目前由前幾大廠商主導，不過隨著產業成長，可能會有其他廠商加入。目前有效（上線）比特幣數量尚未知，不過依據一個網站的資料，截至 2014 年 11 月底，全球共有約 300 處比特幣提款機在營運當中。比特幣提款機營運商會按交易收取手續費，部分比特幣提款機製造商則會按營運商之交易手續費收取佣金。

NOTES
註

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

[1] 點對點（P2P）支付是數位支付形式，使用者會透過網際網路直接發送給受款方。

[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.

[2] 目前，所有 cryptocurrencies 都是去中心化虛擬貨幣，且所有去中心化虛擬貨幣都是 cryptocurrencies。然而，部分集中式 cryptocurrencies（亦即：集中式虛擬貨幣系統、或甚至法定貨幣系統）正在逐漸浮現，運用類似區塊鏈的交易帳簿處理顧客交易。可能在不遠的未來，會出現非去中心化的 cryptocurrencies。

[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.

[3] 比特幣使用驗證機制方法，驗證交易以及創造新比特幣。部分 altcoins 則運用權益證明或零知識證明。

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

[4] 依據定義，所有去中心化虛擬貨幣都是可轉換的（亦即：無制訂贖回規定的中央主管機關）。

[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.

[5] 目前共有兩種基本的去中心化虛擬貨幣支付機制模式：單一貨幣（亦稱為貨幣別）虛擬貨幣網路，譬如比特幣；以及多種貨幣虛擬貨幣網路，譬如 Ripple 與 Ethereum。從名稱可以看得出來，**單一貨幣支付網路**負責處理特定種類去中心化虛擬貨幣。**多種貨幣支付平台**，提供交易任何虛擬貨幣或任何其他具交易價值項目之平台，譬如大宗商品、股票、不動產等。有關多種貨幣虛擬貨幣平台的運作方式，請參閱 「*Ripple 協定：金融專業人員的深入學習（The Ripple Protocol: A Deep Dive for Finance Professionals*），*網址為* https://ripple.com/ripple-deep-dive/。於此引用僅供參考，不代表防制洗錢金融行動工作組織同意 Ripple 或任何其他 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).

[6] 金融機構以中介機構身份通常會扮演的另一項受信賴角色，是擔任付款人支付給受款人之交易的擔保人。在傳統電子支付交易中，金融機構會以擔保付款（亦即：承擔買方之信用風險）以及提供交易後爭議解決的方式，作為交易中介。比特幣希望在無金融機構介入的情況下，解決擔保付款的問題，希望達成接近即時交割的成果，並使交易無法回轉（亦即：不需爭議解決）。

[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.

[7] **區塊鏈**是共享比特幣交易記錄簿，且係以公開可取得的共享資料庫形式存在，按時間序記錄所有交易。

[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.

[8] 所有比特幣交易都會公開且永久的儲存在區塊鏈上。所有存取網路的人，都可透過區塊鏈上的公開金鑰，檢視與監督任何比特幣位址的餘額以及交易。

[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.

[9] 擔任網路節點角色的**採礦者**，會使用雜湊演算法(hashing algorithm)解決逐漸日趨困難的加密問題，互相競爭「發現」下一個區塊。比特幣採礦是一個純粹數學過程，與使用高階高效能電腦搜尋質數的過程類似。比特幣採礦者會運用比特幣「雜湊」演算法，搜尋產生特定模式的一連串資料（「區塊」）。獲勝者會向其他節點宣布找到新區塊，並收取新比特幣作為支付款項。其他節點會驗證解決方式是否符合比特幣協定的所有規則，接著在下一次正式進入區塊鏈時接受，並啟動全新的搜尋過程。

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

[10] **採礦**是可產生區塊鏈以及創造新比特幣的分散式交易驗證流程。

[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.

[11] 採礦者可獲得一組新創造的比特幣（數量由比特幣協定預先約定），且於部分情況中，亦可因解決用於驗證支付與將支付納入區塊鏈所使用的各演算法，而收取交易手續費。演算法會依據預設的區間將新比特幣放到網路上 -- 目前為每 10 分鐘發放 50 個，且其數量每四年將減半，因此到 2140 年將會發放完畢。2015 年期間內，共發放 25 個比特幣給獲勝的採礦者作為獎勵。目前共有 2,100 萬個比特幣，而交易處理將只會賺取交易手續費。預先約定的數位貨幣發放比率，目的在確保比特幣貨幣供給量依據預測比率規律成長，不受第三方（譬如中央銀行）干擾，以避免極度通貨膨脹之情況發生。

[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.

[12] 如上所述，採礦作業包括於個人電腦上執行特定軟體，以於「分散式驗證機制」中解決複雜的演算法。使用者可因解決各演算法而獲得特定數量新創造比特幣的獎勵。

[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/.

[13] Bach, A.、Corallo, M.、Dashjr, L. 等人（2014 年，*以楔入式側鏈技術促進區塊鏈創新（Enabling Blockchain Innovations with Pegged Sidechains*）（2014 年 10 月），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.

[14] **確認**係指採礦者驗證交易並將其記錄於區塊鏈的時點。

[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.

[15] 雖然部分商家規定，虛擬貨幣使用者需在經過一段時間等待確認虛擬貨幣交易之後，才能認定交易已完成並繼續處理顧客訂單，不過對於價值較小且舞弊風險不大的交易，部分商家會將收到比特幣（而非確認）視為有效支付。

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

[16] **託管錢包**係指由第三方錢包供應商所持有的虛擬貨幣錢包（可能由交易平台持有）。

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

[17] **錢包供應商**係指提供虛擬貨幣錢包，以供持有、儲存或移轉比特幣或其他虛擬貨幣的實體。