

FATF



風險基礎方法指引更新版

# 虛擬資產及虛擬資產服務提供商



FATF



風險基礎方法指引更新版

## 虛擬資產及虛擬資產服務提供商





防制洗錢金融行動工作組織（下稱「FATF」）係一獨立的跨政府組織，旨在發展與推廣政策，以保護全球金融體系，防制洗錢、打擊資恐以及資助大規模毀滅性武擴。FATF 建議已被認為是全球性防制洗錢（下稱「AML」）與打擊資恐（下稱「CFT」）的標準。

關於 FATF 更多資訊，請參閱其網站：[www.fatf-gafi.org](http://www.fatf-gafi.org)

本文件及／或本文所包括的任何地圖不影響任何領土的地位或主權、國際邊界及邊界的劃界及領土、城市或地區的名稱。

引用文獻：

虛擬資產與虛擬資產服務提供商風險基礎方法指引更新版，FATF，巴黎  
[www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html](http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html)

©2021 FATF/ 經濟合作暨發展組織 (OECD) 版權所有

未經事前書面許可，不得複製或翻譯本出版物。

如擬複製或翻譯本出版物全部或部分內容，請向 FATF 秘書處申請，

其地址為 2 rue André Pascal 75775 Paris Cedex 16, France

(傳真號碼：+33 1 44 30 61 37，或電子郵件：contact@fatf-gafi.org)。

Photocredits ©Gettyimages

照片著作權 ©Gettyimages

# 目 錄

致謝 .....	1
縮寫 .....	2
摘要 .....	4
第一部分：緒論 .....	8
背景 .....	8
本指引之目標 .....	11
本指引之範圍 .....	13
架構 .....	19
第二部分：FATF 國際標準之範圍 .....	20
初始風險評估 .....	20
防制洗錢與打擊資恐相關之虛擬資產服務提供商之 FATF 定義與特徵 .....	30
第三部分：將 FATF 國際標準適用於國家和權責機關 .....	53
建議在虛擬資產及虛擬資產服務提供商脈絡下之適用 .....	53
監理或監控虛擬資產服務提供商之風險基礎方法 .....	106
第四部分：FATF 國際標準於虛擬資產服務提供商及從事或提供涵蓋的虛擬資產活動之其他義務實體之適用 .....	118
客戶審查 .....	119
重要政治性職務人士 .....	123
通匯銀行業務及其他相似關係 .....	124
電匯及「轉帳規則」 .....	124
內部控制及外國分公司及子公司 .....	132
疑似洗錢或資恐交易報告及揭露 .....	132
第五部分：虛擬資產及虛擬資產服務提供商之風險基礎方法國家範例 .....	135
規範及監理虛擬資產活動及虛擬資產服務提供商之司法管轄方法摘要 .....	135



第六部分：虛擬資產服務提供商監理機關之資訊共享及合作	
原則 .....	154
目標 .....	154
資訊共享及合作原則 .....	156
附件 A. 建議第 15 項及其注釋及 FATF 定義 .....	160
詞彙表 .....	163

## 致謝

本指引更新版係以下述專案團隊成員之工作以及 FATF 成員之全球網絡和區域性防制洗錢組織之廣泛投入為基礎，一共包含了超過 200 個司法管轄區。本指引亦得益於與一系列私部門利害關係人以及來自虛擬資產和虛擬資產服務提供商社群之其他代表之協詢。

本指引工作係由 Habuchi Takahide (日本金融服務廳) 與 Jon Fishman and Sandra Garcia (美國財政部)，以及來自 FATF 秘書處之 Ken Menz and Tom Neylan 領銜。專案小組收到來自 Evan Gallagher (澳洲之澳洲交易報告與分析中心)、Amr Sayed Rashed (埃及打擊洗錢與資恐單位)、Mirzosharif Sharipov (歐亞小組秘書處)、Gabriel Hugonnot and Jon Isaksen (歐洲聯盟委員會)、David Sabban (法國審慎監督和決議機構)、Pierre Offret (法國經濟及財政部長)、Pierre Subiger (法國金融市場主管機關)、Fabian Rieger (德國財政部)、Elad Wieder (以色列洗錢與資恐禁止機關)、Francesca Picardi (義大利財政部)、Kawada Yuji and Matsuzawa Arisa (日本金融服務廳)、Ricardo Cacho (墨西哥財政部和公共信貸秘書處)、Rachel Huen and Evadne Ong (新加坡金融管理局)、Annette Fr̄sard 及 Giulia Mariani (瑞士金融市場監督局)、Vincent Cottier 及 Melanie Friedli (瑞士聯邦財政部)、Caroline Horres (美國財政部) 及 Val Szczepanik (美國證券交易委員會) 之極大協助。

## 縮寫

<b>AEC</b>	Anonymity-Enhanced Cryptocurrency 強化匿名加密貨幣
<b>AML</b>	Anti-Money Laundering 防制洗錢
<b>CDD</b>	Customer Due Diligence 客戶審查
<b>CFT</b>	Countering the Financing of Terrorism 打擊資恐
<b>CPF</b>	Counter-proliferation financing 打擊資助武擴
<b>DApp</b>	Decentralised or distributed application 去中心化應用程式
<b>DeFi</b>	Decentralised finance 去中心化金融
<b>DNFBP</b>	Designated Non-Financial Business and Profession 指定之非金融事業或人員
<b>EDD</b>	Enhanced due diligence 加強客戶審查
<b>ICO</b>	Initial Coin Offering 首次代幣發行
<b>FI</b>	Financial institution 金融機構
<b>FIU</b>	Financial intelligence unit 金融情報中心
<b>ML</b>	Money Laundering 洗錢

<b>MSB</b>	Money Services Business 貨幣兌換服務事業
<b>MVTS</b>	Money or Value Transfer Service 金錢或價值移轉服務
<b>NFT</b>	Non-fungible token 非同質化代幣
<b>OTC</b>	Over-the-Counter 場外交易
<b>P2P</b>	Peer-to-Peer 點對點技術
<b>PEP</b>	Politically exposed person 重要政治性職務人士
<b>PF</b>	Proliferation financing 資助武擴
<b>RBA</b>	Risk-Based Approach 風險基礎方法
<b>SRB</b>	Self-regulatory body 自律團體
<b>STR</b>	Suspicious transaction report 疑似洗錢或資恐交易報告
<b>TF</b>	Terrorist Financing 資恐
<b>VA</b>	Virtual Asset 虛擬資產
<b>VASP</b>	Virtual Asset Service Provider 虛擬資產服務提供商

## 摘要

於 2018 年 10 月，防制洗錢金融行動工作組織（FATF）對其建議進行了修改，以明確闡明其適用於涉及虛擬資產的金融活動；FATF 亦於詞彙表中增加了兩個新定義：「虛擬資產」（VA）和「虛擬資產服務提供商」（VASP）。修訂後之 FATF 建議第 15 項要求，虛擬資產服務提供商應為進行防制洗錢與打擊資恐（AML/CFT）的目的而受監理，其應取得執照或註冊，並接受有效的監管或監督系統監理。

於 2019 年 6 月，FATF 通過建議第 15 項注釋，進一步闡明 FATF 之要求應適用於虛擬資產和虛擬資產服務提供商，特別是風險基礎方法應適用於虛擬資產活動或運營與虛擬資產服務提供商；為防制洗錢與打擊資恐之目的對虛擬資產服務提供商進行監理或監督；取得執照或註冊；預防措施，例如客戶審查、紀錄保存和疑似洗錢或資恐交易報告等；制裁和其他執法措施；以及國際合作。

FATF 亦於 2019 年 6 月通過本指引的第一版<sup>1</sup>，將風險基礎方法適用於虛擬資產和虛擬資產服務提供商；本指引於 2021 年 10 月更新。其旨在幫助國家當局瞭解和發展對虛擬資產活動和虛擬資產服務提供商的監理和監督，並幫助尋求參與虛擬資產活動的私部門實體瞭解其防制洗錢與打擊資恐義務，以及其如何有效地遵守這些要求。

本指引概述各國和虛擬資產服務提供商以及其他參與虛擬資產活動的實體瞭解與虛擬資產活動相關的洗錢和資恐（ML/TF）風險之必要性，並採取適當的抵減措施來應對這些風險。特別是，本指引提供了應在虛擬資產脈絡下特別考慮的風險指標示例，並強調會進一步混淆交易或抑制虛擬資產服務提供商辨識客戶能力之因素。

---

<sup>1</sup> 本指引亦更新 2015 年 FATF 虛擬貨幣風險基礎方法指引。

本指引檢視虛擬資產活動和虛擬資產服務提供商會如何落入 FATF 國際標準之範圍。討論虛擬資產服務提供商定義所涵蓋的五種類型活動，並提供屬於定義範圍內的虛擬資產相關活動以及可能被排除在 FATF 範圍之外活動之示例。就此而言，它強調成為虛擬資產服務提供商所須之關鍵要素，亦即為他人或代表他人提供或積極促進與虛擬資產相關的活動為業。

本指引描述 FATF 建議對國家和權責機關的應用；以及虛擬資產服務提供商和其他從事虛擬資產活動之義務實體，包括銀行和證券經紀商或交易商等金融機構。幾乎所有 FATF 建議都與解決虛擬資產和虛擬資產服務提供商相關之洗錢與資恐風險直接相關，而其他建議與虛擬資產或虛擬資產服務提供商之直接或明確聯繫則較少，儘管它們仍然相關且適用。因此，虛擬資產服務提供商與金融機構和指定之非金融事業或人員同樣負有全部義務。

本指引依逐條建議的方式，詳細說明於 FATF 建議下，虛擬資產服務提供商和虛擬資產所適用之全部義務。這包括澄清 FATF 建議中的所有以資金或價值為基礎之用語（例如，「財產」、「收益」、「資金」、「資金或其他資產」和其他「相應價值」）都包括虛擬資產。因此，各國應將 FATF 建議下的所有相關措施適用於虛擬資產、虛擬資產活動和虛擬資產服務提供商。

本指引解釋虛擬資產服務提供商註冊或取得執照要求，特別是如何確定虛擬資產服務提供商應在哪些國家／地區註冊或取得執照—至少在它們的設立地；或於他們是自然人之情況下，在其業務所在之司法管轄區。但是，司法管轄區亦得選擇要求虛擬資產服務提供商在其司法管轄區內或自其司法管轄區開展業務之前須取得執照或註冊。本指引進一步強調，國家當局必須採取行動，辨識在沒有取得必要執照或註

冊的情況下開展虛擬資產活動的自然人或法人。此同樣適用於選擇在國家層面禁止虛擬資產和虛擬資產活動的國家。

關於虛擬資產服務提供商之監督，本指引明確規定，只有權責機關而非自律團體才能作為虛擬資產服務提供商註冊之監理或監管機構。它們應該進行以風險為基礎的監理或監管，並擁有足夠的權力，包括進行檢查、強制提供資訊與實施裁罰。鑒於虛擬資產服務提供商活動和服務提供之跨境性質，特別關注監管者之間國際合作的重要性。

本指引明確指出，虛擬資產服務提供商和參與虛擬資產活動的其他實體須要適用 FATF 建議第 10 項至第 21 項中描述的所有預防措施。本指引解釋了應如何在虛擬資產脈絡下履行這些義務，並釐清適用於 1000 美元／歐元門檻臨時性交易之特定要求，如高於該門檻虛擬資產服務提供商必須進行客戶審查（建議第 10 項）；以及在進行虛擬資產移轉時立即安全地獲取、持有和傳輸所需的轉出人和接收人資訊之義務（建議第 16 項）（轉帳規則）。正如本指引明確規定，相關當局應進行協調，以確保以符合國家資料保護和隱私規則之方式進行。

最後，該指引提供防制洗錢與打擊資恐目的監管、監理和執行虛擬資產活動、虛擬資產服務提供商和其他義務實體的管轄方法釋例。

於 2021 年 10 月，本指引已更新，為公部門和私部門提供修訂後的指引。這些修訂著重在 FATF 提供更多指導之六個關鍵領域。這是為了 (1) 澄清虛擬資產和虛擬資產服務提供商的定義，以確保該等定義是廣泛的，不應存在相關金融資產未被 FATF 國際標準所涵蓋之情況（不論係虛擬資產或其他金融資產）(2) 就 FATF 國際標準如何適用於穩定幣提供指引，並闡明參與穩定幣安排的一系列實體可能符合 FATF 國際標準下之虛擬資產服務提供商 (3) 提供有關風險和各國可用工具的額外指引，以解決不涉及任何義務實體的點對點技術交易的洗錢與資恐



風險 (4) 提供有關虛擬資產服務提供商取得執照和註冊之更新指引 (5) 為公部門和私部門提供關於實施「轉帳規則」之額外指引 (6) 包括虛擬資產服務提供商監理機關之間的資訊共享和合作原則。本文件包含並取代 2019 年指引。

## 第一部分：緒論

### ■ 背景

1. 新技術、商品與相關服務可能刺激金融創新和效率，增進普惠金融，但也為犯罪分子和恐怖分子掩飾所得或資助其非法活動創造新的機會。基於風險基礎方法 (RBA) 是有效實施 FATF 成員於 2012 年通過之打擊洗錢和資恐與武擴之國際標準修正版之核心，因此 FATF 積極監管新技術相關之風險。對新興風險之監管，包括新技術相關風險，應告知國家和義務實體之風險評估過程，並應根據風險基礎方法引導適當資源分配以抵減該等風險。
2. 於 2014 年 6 月，FATF 發布了*虛擬貨幣：主要定義和潛在防制洗錢／打擊資恐風險*，以因應虛擬貨幣及提供網路傳輸價值新方法之相關支付機制之出現。於 2015 年 6 月，FATF 發布了*虛擬貨幣風險基礎方法指引*（2015 年虛擬貨幣指引），作為解決虛擬貨幣支付商品與服務之洗錢與資恐（ML/TF）相關風險之階段性方法之一部。
3. 2015 年虛擬貨幣指引聚焦於虛擬貨幣活動與傳統受監管金融系統之互動或為其提供進出通道，特別是可轉換虛擬貨幣交易所。然而，近年來，虛擬資產已經演進到包括一系列新商品和服務、商業模式以及活動和互動，包括虛擬對虛擬資產交易。
4. 特別是，虛擬資產生態系統見證了強化匿名加密貨幣 (AEC)、混幣器和轉向器、去中心化平台和交易所、私有錢包<sup>2</sup> 以及其他類型商品和服務的興起，這些商品和服務能夠或允許透明度降低與

---

<sup>2</sup> 私有錢包，亦稱為混合啟用之錢包，允許將多人交易合併為一次之移轉。

增加資金流動之混淆，以及其他虛擬資產商業模式或活動的出現，例如存在洗錢與資恐、詐欺與市場操縱風險之首次代幣發行 (ICOs)。此外，新興非法融資類型不斷出現，包括越來越多使用虛擬到虛擬分層計畫，試圖以相對容易、便宜和安全之方式進一步混淆交易。

5. 鑑於該領域額外商品與服務之發展以及新型態供應商之引入，FATF 認識到進一步闡明 FATF 國際標準應用於新技術和提供商之必要性。特別是，於 2018 年 10 月，FATF 採用了兩個新的詞彙定義—「虛擬資產 (VA)」和「虛擬資產服務提供商 (VASP)」—並更新了建議第 15 項 (R.15) (參附件 A)。該等改變之目的是進一步闡明 FATF 國際標準適用於虛擬資產活動和虛擬資產服務提供商，以確保全球虛擬資產服務提供商之公平監管環境，並協助司法管轄區抵減與虛擬資產活動相關的洗錢與資恐風險並保護全球金融體系之完整性。FATF 亦澄清，該等標準適用於涉及虛擬資產之虛擬對虛擬和虛擬對法幣交易與互動。
6. 於 2019 年 6 月，FATF 通過建議第 15 項注釋 (INR. 15)，以進一步闡明 FATF 之要求應如何適用於虛擬資產與虛擬資產服務提供商，特別是將風險基礎方法適用於虛擬資產活動或運作，以及虛擬資產服務提供商；為防制洗錢與打擊資恐 (AML/CFT) 目的監督或監控虛擬資產服務提供商；取得執照或註冊；預防措施，例如客戶審查 (CDD)、記錄保存和疑似洗錢或資恐交易報告等；裁罰和其他執行措施；和國際合作 (參附件 A)。
7. FATF 於 2019 年 6 月之全體會員大會通過本指引。採用本指引並修訂 FATF 國際標準後，FATF 持續加強對虛擬資產部門實體之監管以及各國對修訂後標準的實施。於 2020 年 3 月，FATF 發布

了其數位身分指引，以協助於數位脈絡中識別客戶。雖然本指引廣泛處理數位身份，但其包含對虛擬資產服務提供商有用之資訊。於 2020 年 6 月，FATF 完成對虛擬資產和虛擬資產服務提供商修訂後 FATF 國際標準為期 12 個月的審查報告，其中確定了 FATF 指引須要加強以澄清修訂後 FATF 國際標準應用之處。與此報告同時，FATF 亦發布了 FATF 向 G20 提交之關於所謂穩定幣的報告。該報告闡述了修訂後 FATF 國際標準如何適用於所謂的穩定幣，並考慮了防制洗錢與打擊資恐議題。

8. 於 2020 年 9 月，FATF 還發布了一份洗錢與資恐虛擬資產紅旗指標的報告，供公部門與私部門使用。於 2021 年 3 月，FATF 發布了防制洗錢與打擊資恐監管風險基礎方法指引。雖然該報告廣泛處理防制洗錢與打擊資恐風險之監管，但其包括專門針對虛擬資產服務提供商之防制洗錢與打擊資恐監管之資訊綱要。於 2021 年 7 月，FATF 發布了第二份對虛擬資產和虛擬資產服務提供商修訂後 FATF 國際標準為期 12 個月的審查報告。該報告發現，各司法管轄區就修訂後 FATF 國際標準之實施持續取得進展，但實施之差距表示尚無全球機制防止濫用虛擬資產和虛擬資產服務提供商進行洗錢與資恐。該報告亦包括與點對點技術交易相關之市場指標，即不涉及任何義務實體之交易，並指出司法管轄區不執行轉帳規則阻礙了私部門投資轉帳規則解決方案。該報告總結更新虛擬資產和虛擬資產服務提供商指引將修訂後 FATF 國際標準之適用提供必要澄清以利其實施。
9. 12 個月的審查報告、G20 報告和第二份 12 個月的審查報告承諾，FATF 將針對修訂後 FATF 國際標準及其適用於虛擬資產及虛擬資產服務提供商發布針對公部門與私部門之更新指引。特別是，

該等報告列出需要更多指引的六個主要領域。針對這六個方面，本指南於 2021 年 11 月更新，以 (1) 闡明虛擬資產及虛擬資產服務提供商之定義，以確保這些定義足夠廣泛，不應出現相關金融資產未被 FATF 國際標準所涵蓋的情況（不論係虛擬資產或其他金融資產），(2) 就 FATF 國際標準如何適用於「所謂的」穩定幣提供指引<sup>3</sup>，並闡明參與穩定幣安排之一系列實體可能構成 FATF 國際標準下之虛擬資產服務提供商，(3) 提供風險與工具額外指引予各國以解決點對點技術交易之洗錢與資恐風險，(4) 提供有關虛擬資產服務提供商取得執照與註冊之更新指引，(5) 為公部門和私部門實施「轉帳規則」提供額外指導，與 (6) 涵蓋虛擬資產服務提供商監理機關間資訊共享和合作原則。本指引亦更新以反映時間經過和其他 FATF 報告之發布，包括上述報告。本指引之更新總結於附件 B。

## ■ 本指引之目標

10. 此更新指引擴展了 2015 年虛擬貨幣指引，並進一步解釋風險基礎方法就虛擬資產防制洗與打擊資恐措施之適用；辨識進行與虛擬資產相關活動或運營之實體，即虛擬資產服務提供商；並闡明 FATF 建議對虛擬資產和虛擬資產服務提供商之適用。本指引旨在幫助國家機關瞭解並發展對涵蓋之虛擬資產或虛擬資產服務之監管回應，包括在其各自司法管轄區修改該國法律（如適用），以解決其涵蓋之虛擬資產活動和虛擬資產服務提供商相關之洗錢與資恐風險。

---

<sup>3</sup> 術語說明：FATF 認為「穩定幣」一詞不是明確的法律或技術類別，而主要是此類幣之推廣者所使用之行銷術語。因此，FATF 在向 G20 提交之報告中使用了「所謂的穩定幣」一詞。為了反映該用語之常見用法，本指引將其稱為穩定幣，但這並不代表對其主張之認可。

11. 本指引亦旨在幫助尋求參與 FATF 詞彙表所定義之虛擬資產活動或營運之私部門實體更瞭解其防制洗錢與打擊資恐義務以及他們如何有效地遵守 FATF 要求。其為各國、權責機關和業界提供指引，以設計和實施針對於虛擬資產活動和虛擬資產服務提供商以風險為本之防制洗錢與打擊資恐之監理與監管框架，包括適用預防措施，如客戶審查、紀錄保存、和疑似洗錢或資恐交易報告等措施。
12. 本指引包含了 FATF 於 2018 年 10 月採用之詞彙，讀者請參閱 FATF 詞彙表中「虛擬資產」和「虛擬資產服務提供商」之定義（附件 A）。
13. 本指引旨在解釋 FATF 建議應如何適用於虛擬資產活動與虛擬資產服務提供商；提供相關或可能最有用之釋例；並指出適用抵減措施與潛在解決方案之障礙。其旨作為描述適用於 FATF 建議下虛擬資產服務提供商及虛擬資產之全部義務之建議第 15 項和建議第 15 項注釋之補充，包括與「財產」、「收益」、「資金」、「資金或其他資產」與其他「對應價值」有關之建議。於此過程中，本指引支持有效實施國家防制洗錢與打擊資恐措施，以監理和監管虛擬資產服務提供商（以及其他義務實體）及其所涉及之虛擬資產活動，並發展對防制洗錢與打擊資恐之風險基礎方法之理解。
14. 雖然 FATF 注意到一些國家已對虛擬資產和虛擬資產服務提供商實施了監理制度，但許多司法管轄區尚未制定有效防制洗錢與打擊資恐框架以抵減虛擬資產活動相關的洗錢與資恐風險，即使虛擬資產活動全球化發展且虛擬資產服務提供商之跨司法管轄區營運日益增加。因此，虛擬資產的快速發展、不斷增加之功能、日益增加被採用以及虛擬資產全球跨境性質使得各國採取緊急行動

抵減虛擬資產活動與虛擬資產服務提供商所帶來之洗錢與資恐風險成為 FATF 重要優先事項。勒索軟體網絡對虛擬資產之使用也是一個關鍵問題，且勒索軟體攻擊的增長使得在全球引入有效的防制洗錢與打擊資恐框架之努力更加重要。雖然本指引旨在防制洗錢與打擊資恐，促進對所涵蓋虛擬資產活動與虛擬資產服務提供商實施風險基礎方法，但 FATF 意識到，與防制洗錢與打擊資恐不同之其他類型之政策考慮可能會發揮作用並形塑個別司法管轄區對虛擬資產服務提供商實體之監理回應。

#### ▪ 本指引之範圍

15. FATF 建議要求所有司法管轄區對金融機構 (FIs)、指定之非金融事業或人員 (DNFBPs) 和虛擬資產服務提供商課以特定的、以活動為基礎的防制洗錢與打擊資恐規範，並確保他們遵守該等義務。FATF 已同意 FATF 建議中所有基於資金或價值之詞彙（例如，「財產」、「收益」、「資金」、「資金或其他資產」與其他「對應價值」）包括虛擬資產，且各國應將 FATF 建議下所有相關措施適用於虛擬資產、虛擬資產活動和虛擬資產服務提供商。本指引之主要重點是描述建議如何適用於虛擬資產、虛擬資產活動和虛擬資產服務提供商，以幫助各國更瞭解他們應如何有效實施 FATF 國際標準。
16. 此外，本指引聚焦於可轉換為其他資金或價值之虛擬資產，包括可轉換為另一個虛擬資產之虛擬資產和可轉換為法定貨幣或與法定貨幣金融系統互動之虛擬資產。其不涉及可能與虛擬資產與虛擬資產服務提供商相關之其他監管事項（例如，消費者和投資人保護、審慎安全和穩健、稅收、反詐欺或反市場操縱問題、網路資訊技術安全標準或金融穩定性問題）。



17. 本指引亦不涉及央行發行之數位貨幣。就 FATF 而言，這些不是虛擬資產，因為它們是法定貨幣之數位表示。然而，FATF 國際標準適用於類似於央行發行之任何其他形式法定貨幣之央行數位貨幣<sup>4</sup>。與實體法定貨幣相比，央行數位貨幣取決於其設計，可能有獨有之洗錢與資恐風險。在推出任何央行數位貨幣前，應以前瞻性方式解決此類洗錢與資恐風險。但是，它們未包含於本指引中並不表示 FATF 認為它們不重要。相反地，因為它們被歸類為法定貨幣，而不是本指引所涉及之虛擬資產。
18. 本指引認可有效風險基礎方法將反映一個國家虛擬資產服務提供商部門之性質、多樣性和成熟度、該部門之風險狀況、在該部門營運之個別虛擬資產服務提供商之風險狀況以及該國之法律和監理方法，並考量大多數虛擬資產活動之跨境、以互聯網為基礎之性質與全球範圍。本指引列出了各國與虛擬資產服務提供商在設計和實施風險基礎方法時所應考慮之不同要素。在考慮本指引所概述之一般原則時，國家機關將考慮其國情，包括監管方法和法律框架，以及其司法管轄區存在之風險，並根據虛擬資產活動之潛在全球範圍。
19. 本指引考慮到，正如非法行為者得濫用任何從事金融活動的機構一樣，非法行為者可以濫用從事虛擬資產活動的虛擬資產服務提供商，用於洗錢、資恐、逃避制裁、詐欺、勒索軟體支付和其他惡意目的。2015 年虛擬貨幣指引、與此主題相關之 2018 年 FATF 風險、趨勢和方法小組論文，以及與虛擬資產、虛擬資產活動及

---

4 更多關於央行數位貨幣之資訊，請參考 FATF 向 G20 提交之關於所謂穩定幣的報告附件 B。

／或虛擬資產服務提供商<sup>5</sup>有關的洗錢與資恐風險相關之 FATF 報告及聲明，例如，突顯與提供虛擬資產活動相關之洗錢與資恐風險之進一步脈絡。雖然虛擬資產可能為從事洗錢與資恐提供另一種價值形式，且虛擬資產活動得以作為非法移轉價值或資金之另一種機制，但各國不一定將虛擬資產服務提供商或虛擬資產活動歸類為固有之高洗錢與資恐風險。儘管如此，在無義務實體參與虛擬資產活動之情況下，非面對面業務關係和跨境交易本質、潛在強化匿名性與非仲介活動之機會應為國家風險評估提供資訊。一個國家的監管和監理框架之範圍和品質，以及虛擬資產服務提供商實施以風險為基礎之控制和抵減措施，也會影響被涵蓋虛擬資產活動相關之整體風險和威脅。本指引亦認為，儘管採取了該等措施，但仍可能存在一些剩餘風險，權責機關和虛擬資產服務提供商於制定適當解決方案時應考慮該等風險。各司司法管轄區應在其自身金融部門以及監管和監理系統之脈絡下，各自檢查虛擬資產與虛擬資產活動，以評估其風險。

20. 自 FATF 於 2019 年 6 月完成對其標準之修訂以來，其持續監控虛擬資產用於洗錢與資恐目的之趨勢。正如其 2020 年 9 月洗錢與資恐虛擬資產紅旗指標報告所述，FATF 觀察到虛擬資產越來越廣泛地成為犯罪活動之主流。報告中強調大多數與虛擬資產相關之

---

<sup>5</sup> 例如，參 2018 年 7 月 FATF 向 G20 財長和央行行長提交的報告；2019 年 2 月 FATF 關於抵減虛擬資產風險的公開聲明；2019 年 4 月 FATF 向 G20 財長和央行行長提交的報告、2019 年 10 月關於「穩定幣」與其他新興資產洗錢風險的聲明、2020 年 6 月對虛擬資產和虛擬資產服務提供商修訂後 FATF 國際標準為期 12 個月的審查報告，2020 年 6 月 FATF 向 G20 財長和央行行長提交的關於所謂穩定幣的報告、2020 年 9 月 FATF 洗錢與資恐虛擬資產紅旗指標報告，以及 2021 年 7 月第二份對虛擬資產和虛擬資產服務提供商修訂後 FATF 國際標準為期 12 個月的審查報告。

犯罪均集中於前置犯罪或洗錢犯罪上，但罪犯亦利用虛擬資產來規避金融制裁並籌募資金支持恐怖主義。各司法管轄區報告之犯罪類型包括洗錢、銷售被管制物品和其他非法物品（包括槍支）、詐欺、逃稅、電腦犯罪（例如導致竊盜和勒索軟體之網路攻擊）、剝削兒童、販賣人口、規避制裁，與資恐。其中，兩種濫用最為常見。這些是管制物品之非法販運，或者直接為虛擬資產之銷售，或者使用虛擬資產作為洗錢之分層技術，以及詐欺、詐騙、勒索軟體攻擊與勒索。最近，FATF 觀察到專業洗錢網絡正在利用虛擬資產作為其移轉、收集或分層收益的手段之一。

21. FATF 第二份對虛擬資產和虛擬資產服務提供商修訂後 FATF 國際標準為期 12 個月的審查報告指出，使用虛擬資產來收取勒索軟體付款以及進行詐欺所得洗錢大幅增加，勒索軟體攻擊之速度、複雜程度和成本可能有所成長。虛擬資產是勒索軟體參與人之重要工具，沒有虛擬資產其潛在犯罪將更難貨幣化。這使得於該領域有效且一致地實施 FATF 國際標準日益重要。該報告亦強調了司法管轄權套利以及不合規或合規性弱的虛擬資產服務提供商之相關問題，以及增加匿名性的工具和方法為虛擬資產洗錢與資恐風險的主要趨勢。非法行為人正利用這些虛擬資產服務提供商中糟糕的客戶審查與篩選流程以實現洗錢與資恐目的，此彰顯了有效、實際實施 FATF 國際標準之重要性。增加虛擬資產移轉匿名性之工具和方法亦持續被使用與開發。該報告亦強調了諸如去中心化與虛擬資產與虛擬資產服務提供商之定義、點對點交易和實施（包括轉帳規則）等挑戰。
22. 本指引肯認，參與或促進金融活動之「新」或創新技術或機制可能不會自動構成「更好」之方法，各司法管轄區亦應評估此類

新方法產生之風險並適當抵減執行傳統或受監管之金融活動之風險，例如在支付服務或證券活動脈絡下使用虛擬資產。

23. 其他利益關係人，包括虛擬資產服務提供商、金融機構和其他向虛擬資產服務提供商或參與虛擬資產活動之人提供銀行或其他金融服務的義務實體，亦應考慮上述因素。如同所有客戶，金融機構在考慮與虛擬資產服務提供商或參與虛擬資產活動之客戶建立或繼續關係時，應適用風險基礎方法，評估業務關係之洗錢與資恐風險，並評估是否可以適當抵減與管理這些風險（參第四部分）。重要的是金融機構正確適用風險基礎方法，並且在沒有適當針對性風險評估之情況下，不要訴諸大規模終止或排除虛擬資產服務提供商部門之業務關係。
24. 於實施虛擬資產服務提供商之防制洗錢與打擊資恐制度時，FATF 與各司法管轄區應意識到防制洗錢與打擊資恐制度要求對其他監管要求和政策領域之交互與潛在影響，例如資料保護與隱私、普惠金融、去風險化、消費者與投資人保護和金融創新。
25. 考慮此指引時，各國、虛擬資產服務提供商與其他參與或提供涵蓋虛擬資產活動之義務實體應回顧 FATF 建議之設計及適用基本關鍵原則，這些原則與虛擬資產脈絡相關：
  - a. **功能等效和目標基礎方法**：FATF 的要求涵蓋其餘虛擬資產領域之適用，與各種不同法律和行政系統兼容。其廣泛地解釋必須做什麼，但並未以過度具體之方式說明應如何實施，以便於適當情況下允許不同選擇。對規範之任何澄清不應要求已經採取適當措施以實現 FATF 建議目標之司法管轄區改變其法令之形式或實質。本指引旨在支持相關 FATF 建議目的或目標的實施，而不是在所有司法管轄區施以嚴格的一體監理制度。

- b. **技術中立和未來規劃**：適用於作為價值或資金之虛擬資產、虛擬資產活動與虛擬資產服務提供商之規範適用各該適用之技術平台。同樣地，該等規範不優先考慮商業供應商提供的特定商品、服務或解決方案，包括旨在幫助供應商遵守其防制洗錢與打擊資恐義務之技術實施解決方案。相反地，該等規範旨在具有足夠的靈活性，以便各國和相關實體無需額外修改，即得將之適用於既有技術以及不斷發展之新興技術。
- c. **公平競爭環境（功能性對待）**：各國及其權責機關對於提供基礎相似服務並帶來相似風險之各種類虛擬資產服務提供商，無論商業模式如何，應從監管與監理角度平等對待。然而，如其風險狀況不同，則對待可能依風險基礎方法而不同。同樣地，各國應致力於使對虛擬資產服務提供商之監管及監理與提供相同服務並承擔類似洗錢與資恐風險之金融機構之監管與監理相一致。風險評估應根據所提供商品和服務的性質，而非術語、技術或商業模式，以指引各國實施監管與監理。此外，所有國家都應努力確保其國內制度得於在全球範圍內同樣有效地實施，以避免司法管轄權和監管套利，惟此不妨礙各國施加超出 FATF 國際標準額外要求以應對其自身風險或政策。
26. 本指引不具有約束力，為澄清和解釋既有標準，惟不改變它們。本指引未推翻國家機關之權限，包括根據普遍洗錢與資恐風險和其他背景因素對虛擬資產服務提供商、虛擬資產與虛擬資產活動進行評估和分類。其借鏡各國與私部門之經驗，旨在幫助權責機關、虛擬資產服務提供商與相關金融機構（例如從事涵蓋虛擬資產活動之銀行）有效實施使用風險基礎法之 FATF 建議。

## ▪ 架構

27. 本指引架構如下：第二部分研究虛擬資產活動與虛擬資產服務提供商如何屬於 FATF 建議之範圍；第三部分描述 FATF 建議對國家和權責機關之適用；第四部分解釋 FATF 建議對虛擬資產服務提供商和其他從事或提供虛擬資產所涵蓋活動的義務實體之適用，包括銀行和證券商等金融機構；第五部分提供監管、監理和執行防制洗錢與打擊資恐所涵蓋的虛擬資產活動與虛擬資產服務提供商（與其他義務實體）之司法管轄方法釋例；第六部分規定虛擬資產服務提供商監管者間之國際合作與資訊共享原則。
28. 附件 A 臚列了建議第 15 項之更新版及其注釋，以及 FATF 詞彙表中「虛擬資產」和「虛擬資產服務提供商」之定義。附件 B 臚列出 2021 年 11 月更新中對本指引所做的修改。

## 第二部分：FATF 國際標準之範圍

29. 第二部分討論風險基礎方法對虛擬資產活動與虛擬資產服務提供者之適用性，並解釋該等活動和提供者應如何遵守國際標準下之防制洗錢與打擊資恐要求。如建議第 15 項注釋第二段所述，虛擬資產服務提供者根據其從事之活動類型受 FATF 建議之相關措施之拘束。同樣地，虛擬資產為 FATF 建議之相關措施所涵蓋，該等措施廣泛地與資金或價值相關，或專門參考了基於資金或價值的條款。
30. 須強調的是，當虛擬資產服務提供者從事傳統之純法幣活動或法幣對法幣交易（這些活動超出了虛擬資產服務提供者定義所涵蓋之虛擬對虛擬和虛擬對法幣活動之範圍）時，其應適用與任何其他同等傳統機構或實體通常遵循之 FATF 國際標準之措施。

### ▪ 初始風險評估

31. FATF 建議並未預先判斷任何部門實體為高風險。這些標準確定了可能有洗錢與資恐弱點之部門實體；然而，國家層級之總體風險應由各個司法管轄區對該部門實體之評估來確定—於此情形，為虛擬資產服務提供者部門。一個行業內之不同實體可能會帶來更高或更低的風險，這取決於多種因素，包括商品、服務、客戶、地域、商業模式和部門實體法遵計畫之強度。建議第 1 項規定了風險基礎方法之適用範圍如下：何者應該受限於單一國家之制度；應如何監理或監管受防制洗錢與打擊資恐制度所約束的人遵守該制度；應如何要求受防制洗錢與打擊資恐制度所約束的人遵守；並考慮虛擬資產服務提供者和參與所涵蓋虛擬資產活動之其他義務實體之業務關係。此外，FATF 不支持大規模和一律終止或限



制與特定部門實體的業務關係（例如，金融機構終止與所有虛擬資產服務提供商之關係，而不管其間之風險狀況如何），以避免而不是依 FATF 風險基礎方法管理風險。

32. 根據風險基礎方法與建議第 15 項注釋第 2 段，各國應識別、評估和瞭解該領域出現之洗錢與資恐風險，並確保預防或抵減洗錢與資恐之措施與所識別之風險相稱。同樣地，各國應要求虛擬資產服務提供商（以及其他從事虛擬資產金融活動或營運或提供虛擬資產商品或服務之義務實體）識別、評估並採取有效行動來抵減其洗錢與資恐風險。
33. 虛擬資產服務提供商之風險評估應考慮虛擬資產服務提供商及權責機關認為相關之所有風險因素，包括所涉及的服務、商品或交易類型；客戶風險；地理因素；所交換之虛擬資產類型等因素。
34. 虛擬資產可以實現非面對面的業務關係或允許在不使用或涉及虛擬資產服務提供商或金融機構之情況下進行交易。此外，虛擬資產用於在全球範圍內快速移轉資金，幾乎是即時且在很大程度上是不可逆轉的，並促進一系列金融活動—從貨幣或價值移轉服務到證券、商品或衍生性金融商品相關活動等。虛擬資產金融活動或營運中之相關因素可能表明了更高的洗錢與資恐風險，因此可能需要採取適當的風險抵減措施來識別或打擊相關非法活動，例如使用強大的數位身份解決方案<sup>6</sup>。同樣地，促進匿名或強化匿名交易之虛擬資產商品或服務亦帶來更高洗錢與資恐風險，特別是如果其抑制虛擬資產服務提供商辨識接收人的能力。缺乏客戶和交易對手身分於虛擬資產之脈絡下特別令人擔憂，因為它們是跨

---

6 有關數位身份之更多資訊，參 [FATF 數位身分指引](#)。

境性質的。如果客戶識別和驗證措施不能充分解決與非面對面或不透明交易相關風險，洗錢與資恐風險就會增加，追蹤相關資金和識別交易對手之難度也會增加。

35. 用戶在全球範圍內使用虛擬資產或虛擬資產服務提供商進行支付或移轉資金之程度亦為各國確定風險等級時應考慮的重要因素。例如，虛擬資產之非法用戶可能利用虛擬資產提供之全球範圍和交易速度，以及對跨司法管轄區之虛擬資產金融活動和供應商未充分或均衡地監管或監理，所造成虛擬資產生態系於法律和監管方面不一致之競爭環境。與其他用於全球或於廣闊地理區域內移轉資金予大量交易對手之行動或基於網際網路之支付服務和機制相同，與純粹國內商業模式相比，虛擬貨幣對於洗錢與資恐目的之犯罪分子更具吸引力。
36. 此外，位於一個司法管轄區之虛擬貨幣服務提供商可能會向位於另一個司法管轄區的客戶提供其商品和服務，渠等可能會適用不同防制洗錢與打擊資恐義務和監理。如果虛擬貨幣服務提供商位於防制洗錢或打擊資恐控制薄弱甚至根本不存在之司法管轄區，或在司法管轄區提供最廣泛國際合作能力不足之情況下，將會令人擔憂。同樣地，由於客戶和交易資訊之潛在差距，虛擬資產提供者之絕對範圍及其在幾個司法管轄區的存在可能會增加虛擬資產和虛擬資產金融活動相關之洗錢與資恐風險。此於跨境交易脈絡下特別令人擔憂，並且當交易中所涉及之適用防制洗錢與打擊資恐措施之實體或個人（自然人或法人）以及哪些國家負責監管（包括取得執照或註冊）及監理或監管該等實體遵循其防制洗錢與打擊資恐義務不明確時。

## 第 1 欄 穩定幣與洗錢與資恐風險

穩定幣旨在保持相對於某些參考資產或資產之穩定價值。正如 FATF 向 G20 提交之關於所謂穩定幣的報告 所指出，穩定幣與一些虛擬資產具有許多相同的洗錢與資恐風險，因為它們具有匿名性、全球範圍和用於分層化非法資金之潛力。但是，某些穩定幣項目可能具有更大規模採用之潛力，此可能會增加洗錢與資恐風險。因此，雖然大規模採用可能性是關於所有虛擬資產因素之一，但在評估穩定幣洗錢與資恐風險時，此為一相關因素。

大規模採用是需要考慮之重要洗錢與資恐風險因素，因為犯罪者使用虛擬貨幣作為交換手段之能力，很大程度上取決於其自由交換性與流動性，而大規模採用可以促進這一點。此外，如果虛擬資產被全球採用的程度足夠，使其在不使用虛擬資產服務提供商或其他義務實體的情況下得作為交換和價值存儲的媒介，則缺乏或不足之防制洗錢與打擊資恐控制和法遵可能會提高洗錢與資恐風險<sup>7</sup>。

穩定幣有阻礙虛擬貨幣廣泛採用作為支付手段因素之特性。通過保持穩定的價值，穩定幣被設計用以克服虛擬資產價格波動問題。降低波動性可以鼓勵它們被廣泛採用作為支付或移轉資金之手段，特別是在它們得以提供全球支付安排的大型技術、電信或金融公司支持之情況下。

如同更廣泛的虛擬貨幣，穩定幣之特徵亦將影響洗錢與資恐風險實現之程度。穩定幣可以更集中或更分散，無論是在其治理方面還是在何人得接觸穩定幣（例如，其是否允許非託管錢包，系統是否獲得許可）以及提供相關服務方面。此等設計選擇可能會對洗錢與資

---

<sup>7</sup> 有關點對點交易之洗錢與資恐風險之更多資訊，參第 37-41 段。

恐風險產生影響，並且隨著穩定幣安排之進化，設計可能會隨著時間推移而改變。例如，穩定幣之中央治理機構通常作為虛擬資產服務提供商或金融機構而被 FATF 國際標準所涵蓋。當以一定去中心化程度而提供類似功能時，不管機構設計和名稱為何，預計各國將採取功能方法來識別義務實體，並基於風險基礎方法抵減相關風險<sup>8</sup>。根據與新技術<sup>9</sup>相關之 FATF 國際標準下之一般義務，各國、虛擬資產服務提供商與其他義務實體應在推出前以持續與前瞻性之方式識別並評估與穩定幣相關之洗錢與資恐風險，並採取適當措施於發布前管理並抵減風險。即使於推出後，亦應持續抵減該等風險，並考慮到穩定幣被大規模採用時不斷變化之風險。

#### ■ 點對點交易

37. FATF 將點對點 (P2P) 交易定義為，在沒有使用或涉及虛擬資產服務提供商或其他義務實體之情況下進行之虛擬資產移轉（例如，於代表用戶自己之兩個非託管錢包之間進行之虛擬資產移轉）<sup>10</sup>。點對點交易未明確受 FATF 國際標準下防制洗錢與打擊資恐控制之約束。這是因為該標準通常課以義務予中介，而不是個人本身（有一些例外，例如與實施目標性金融制裁相關之規範）。

---

8 關於哪些實體於穩定幣安排中具有防制洗錢與打擊資恐義務之進一步資訊，參見第 86-90 段。關於穩定幣，其特徵以及更廣泛監管和監理問題之進一步資訊，請參見金融穩定委員會 2020 年「全球穩定幣」安排之監管、監理和監查：最終報告與上位建議。

9 虛擬資產服務提供商就新技術之更多資訊參以下第三部分建議第 15 項。

10 一些虛擬資產服務提供商可能將自己推銷為點對點平台。這與此處提到的點對點交易是分開的，並在第 93 段中說明。此外，自然人可以是虛擬資產服務提供商（參第 58 段）。如果交易中涉及到此類虛擬資產服務提供商，則其不是點對點交易。

38. FATF 認識到點對點交易可能帶來特定洗錢與資恐風險，因為其可能被用以規避 FATF 國際標準之防制洗錢與打擊資恐控制措施。如果虛擬資產移轉立於點對點基礎上，則無申報義務實體參與預防或抵減洗錢與資恐風險。雖然點對點交易亦得用於合法活動，但非法行為者可以利用點對點交易中，缺乏申報義務仲介來掩飾犯罪所得，因為沒有申報義務之實體執行 FATF 國際標準之核心功能，例如客戶審查和提交疑似洗錢或資恐交易報告 (STR)。相反地，除非有與虛擬資產相關的強化匿名協議和技術，特別是在與其他資訊來源結合時，公共分類帳上點對點交易之可見性或許支持財務分析與執法調查。
39. FATF 第二份 12 個月審查報告根據七家區塊鏈分析公司提供之數據，概述了虛擬資產在點對點基礎上之使用程度<sup>11</sup>。該報告表明，在點對點基礎上移轉某些潛在大量虛擬資產，與虛擬資產服務提供商之直接交易相比，點對點交易中辨識出非法交易之比例似乎更高。然而，區塊鏈分析公司所提供數據之高度變化代表對點對點領域之規模及其相關之洗錢與資恐風險並沒有達成共識。其亦揭示了即使點對點交易係紀錄在公共分類帳上，這種區塊鏈分析研究在涵蓋範圍、及時性、準確性和可靠性方面之挑戰與局限性。
40. 因此，這些結果強調各國需瞭解與點對點交易相關的洗錢與資恐風險，以及點對點交易如何在其管轄範圍內動態使用，特別是當新型虛擬資產進入市場或預先存在之虛擬資產時受大規模採用。儘管到目前為止，FATF 還沒觀察到點對點交易使用增加之明顯趨勢，但隨著更多司法管轄區實施 FATF 國際標準並監管虛擬資產服務提供商，有更多潛在風險虛擬資產交易將移轉到點對點空間

---

<sup>11</sup> 參 FATF 第二份為期 12 個月的審查報告 第 76 至 102 段。

以避免監管與監理。於虛擬資產生態系中，如點對點交易增加，致非法活動在點對點基礎使用達到極大程度，而未與虛擬資產服務提供商互動或其他傳統法幣經濟為互換，這可能對實施 FATF 國際標準效能造成挑戰。因此，應以持續與前瞻性之方式監控與點對點交易相關之洗錢與資恐風險。如果各國認為點對點交易存在更高的洗錢與資恐風險，而需要額外抵減措施，其可以基於已評估風險考慮本指引第 105、106 段之非完整可選擇措施清單。

41. 作為其中一部分，各國與虛擬資產服務提供商應設法瞭解哪些類型之點對點交易會帶來更高或更低的風險，並瞭解點對點交易之驅動因素及其不同的風險狀況。根據虛擬資產之設計，可能影響用戶參與點對點交易程度的相關因素，包括可存取性與控制虛擬資產隱私、透明度、安全性與相關交易費用之協議。各司法管轄區須權衡各種因素並評估其在每個國家與地區之顯現，以評估風險並適用與風險基礎方法一致之抵減控制措施。此部門之快速發展意味著風險水平與性質之變化可能很快發生，並值得監理機關一致關注。

▪ **虛擬資產與虛擬資產服務提供商相關之風險因素**

42. 存在與虛擬資產、虛擬資產金融活動或營運以及虛擬資產服務提供商相關之洗錢與資恐風險。除了參考 FATF 之前關於該主題之工作<sup>12</sup>與 FATF 關於風險評估<sup>13</sup>之一般指引外，各國與虛擬資產服務提供商亦應考慮以下非完整要素列表，例如，在識別、評估

---

<sup>12</sup> 例如，與此主題相關之 2015 年虛擬貨幣指引、2018 年 FATF 風險、趨勢和方法小組論文，以及虛擬資產、虛擬資產活動及／或虛擬資產服務提供商有關的洗錢與資恐風險相關 FATF 報告及聲明。有關虛擬資產之更多資訊亦得於 FATF 2020 年洗錢與資恐虛擬資產紅旗指標報告中取得。

<sup>13</sup> 例如，2013 年 國家洗錢與資恐風險評估指引與 2019 年 資恐風險評估指引。

和確定如何最好地抵減與涵蓋虛擬資產活動與提供虛擬資產服務  
提供商商品或服務之相關風險：

▪ **虛擬資產相關要素**

- a. 虛擬資產移轉之數量和價值；已發行虛擬資產之價值和價格波動；  
虛擬資產之市值；流通價值；用戶之司法管轄區數量和每個司法  
管轄區之用戶數量；每個司法管轄區內虛擬資產支付的市場比重；  
以及虛擬資產用於跨境支付與匯款的程度；
- b. 與法定貨幣或其他虛擬資產交換之虛擬資產相關潛在洗錢與資恐  
風險，以及虛擬資產為基礎之交易管道／平台與法幣為基礎之交  
易管道／平台與數位服務／平台之交互或連結之程度；
- c. 虛擬資產支付管道或系統之性質與範圍（例如，開放與封閉系統  
或旨在促進小額支付或政府對個人／個人對政府支付之系統）；
- d. 以下類別之虛擬資產移轉以及與非法活動（例如，暗網市場、勒  
索軟體與駭客）相關之移轉數量與價值；(1) 虛擬資產服務提供商  
／其他申報義務實體之間，(2) 虛擬資產服務提供商／其他義務實  
體與非義務實體之間，以及 (3) 非義務實體之間（即點對點交易）；
- e. 使用匿名技術進行虛擬資產之資金移轉（例如，強化匿名加密貨  
幣、混幣及轉向服務、錢包位址集群、私錢包）和去匿名技術（例  
如，使用區塊鏈分析工具對錢包位址進行風險評估）；
- f. 暴露於網際網路協議 (IP) 匿名程序，例如洋蔥路由器 (Tor)、隱形  
網計畫 (I2P) 與其他匿名軟體或匿名強化功能，此可能會進一步混  
淆交易或活動，並抑制虛擬資產服務提供商瞭解其用戶和實施有  
效防制洗錢或打擊資恐措施之能力；與
- g. 業務規模、既有客戶群、利害關係人以及發行人和／或管理安排  
之中央實體（如有）跨境活動之重要性。



▪ **虛擬資產服務提供商相關要素**

- a. 位於一個司法管轄區及／或向位於司法管轄區內的人提供服務之虛擬資產服務提供商之數量和類型，以及與每項服務相關之交易數量和金額；
- b. 虛擬資產服務提供商之防制洗錢與打擊資恐計畫之複雜程度，包括是否存在適當的監理工具來監控虛擬資產和／或虛擬資產服務提供商活動，包括負責遵守虛擬資產相關防制洗錢與打擊資恐計畫人員是否具備適當知識和專業；
- c. 虛擬資產服務提供商用戶群之規模和類型，包括虛擬資產服務提供商對其用戶及其活動資料之權限，包括在虛擬資產服務提供商內以及是否存在跨平台之潛在整合；
- d. 虛擬資產服務提供商提供之虛擬資產帳戶、商品或服務的性質和範圍（例如，主要使金融上被排除在外之人得以存儲有限價值之小額儲蓄和存儲帳戶）；
- e. 任何可能降低提供商（無論是虛擬資產服務提供商或是其他從事虛擬資產活動或提供虛擬資產商品與服務之義務實體）曝險（例如交易或帳戶餘額限制）之參數或措施；
- f. 虛擬資產服務提供商是否完全線上運作（例如，以平台為基礎之交易所）還是人工操作（例如，促進個人用戶之間交易之交易平台或基於自助服務之交易所）；
- g. 與虛擬資產服務提供商與司法管轄區的聯繫和關連相關之潛在洗錢與資恐及制裁風險；
- h. 虛擬資產服務提供商是否實施「轉帳規則」以及其如何有效地抵減了「日出問題」（參見第三部分及第四部分之建議第 16 項）；
- i. 來自／與無義務實體之交易（例如，無義務實體之非託管錢包，

不受監管與監理之司法管轄區內之虛擬資產服務提供商等)以及發生於較早點對點交易階段之交易，前提是此類資料之蒐集符合國家隱私相關法律；

- j. 虛擬資產服務提供商提供或計畫提供之特定類型的虛擬資產以及各虛擬資產之任何獨特功能，例如強化匿名加密貨幣、嵌入式混幣器或轉向器，或可能藉由潛在混淆交易或破壞虛擬資產服務提供商瞭解其客戶與實施有效客戶審查與防制洗錢與打擊資恐措施能力而帶來更高風險之其他商品和服務；與
- k. 虛擬資產服務提供商與可用於進行交易之任何智能合約<sup>14</sup>互動或管理。

▪ **虛擬資產與虛擬資產服務提供商之禁止與限制**

- 43. 基於風險評估和國家監理脈絡，或為了支持本指引中未提及之其他政策目標（例如消費者或投資人保護、市場保護、安全與穩健或貨幣政策），一些國家可能決定禁止或限制虛擬資產活動或虛擬資產服務提供商，以及由無申報義務實體開展之虛擬資產活動。在這種情況下，建議第 15 項之一些特定要求將不適用，但各司法管轄區仍需要評估涵蓋虛擬資產活動或提供者相關之風險，並有適當工具和權力對不遵守禁令之行為採取行動或限制。於決定是否禁止或限制虛擬資產服務提供商虛擬資產活動時，各國應瞭解虛擬資產相關之洗錢與資恐風險。一個國家應確保其擁有執行此類禁令或限制之技術能力與資源。

---

<sup>14</sup> 在虛擬資產之脈絡中，智能合約是一種計算機程式或協議，旨在滿足某些條件時自動執行特定行動，例如參與者之間之虛擬資產移轉，而無需第三人直接參與。

▪ **防制洗錢與打擊資恐相關之虛擬資產服務提供商之 FATF 定義與特徵**

44. FATF 建議要求所有司法管轄區對金融機構、指定之非金融事業或人員與虛擬資產服務提供商課以特定防制洗錢與打擊資恐規範，並確保他們遵守該等義務。在詞彙表中，FATF 定義：

- a. 「金融機構」係指為客戶或代表客戶進行一項或多項特定活動或營業為業務之自然人或法人；
- b. 「虛擬資產」作為價值之數位表示，可以進行數位交易或移轉，並可用於支付或投資目的。虛擬資產不包括法定貨幣、證券與已涵蓋在 FATF 建議其他部分之其他金融資產之數位表現；
- c. 「虛擬資產服務提供商」是指 FATF 建議其他部分未涵蓋，並為或代表其他自然人或法人進行以下一項或多項活動或營業為業務之任何自然人或法人：
  - i. 虛擬資產與法定貨幣間之交換；
  - ii. 一種或多種形式虛擬資產間之交換；
  - iii. 虛擬資產之移轉<sup>15</sup>；與
  - iv. 保管及／或管理虛擬資產或得控制虛擬資產之工具；
  - v. 參與及提供與發行人募集及／或出售虛擬資產相關之金融服務。

▪ **虛擬資產與虛擬資產服務提供商定義之背景與一般考量**

45. 將虛擬資產與虛擬資產服務提供商之新定義增加於 FATF 詞彙表之目的係擴大 FATF 國際標準之適用性，以涵蓋新型數位資產與該等資產中某些服務之提供商。其無意將之從「資金」、「資金

---

<sup>15</sup> 在虛擬資產之脈絡下，移轉是指代表另一自然人或法人進行交易，將虛擬資產從一個虛擬資產位址或帳戶移轉到另一個虛擬資產位址或帳戶。

或其他資產」之既有定義中除去，或從 FATF 國際標準之「金融機構」定義所包含各種金融服務之範圍中除去。

46. 金融資產不應因其提供格式而為 FATF 建議所涵蓋，且任何金融資產都不應被解釋為完全不符合 FATF 國際標準。例如，如果一個國家決定數位資產不符合虛擬資產之定義但屬於金融資產，則該資產仍作為相關金融資產被 FATF 建議所涵蓋。因此，該資產相關服務之提供者可能被視為金融機構。各國家／地區都必須確定此類資產及其活動是否屬於虛擬資產或一些其它各式金融資產與虛擬資產服務提供商或金融機構之定義。無論如何，FATF 建議同樣適用，惟僅微幅調整<sup>16</sup>。

▪ 何謂虛擬資產？

47. 虛擬資產之定義旨在使各司法管轄區依賴其中所包含的基本概念，採用可適應技術進步與創新商業模式之功能性方法為廣泛的解釋。根據 FATF 建議之整體精神，該等定義旨在實現技術中立。也就是說，其適用應基於資產或服務之基本特徵，而不是所採用的技術。因此，有幾個關鍵要素需要詳細說明。
48. 首先，虛擬資產必須數位化，本身必須進行數位化交易或移轉，且能夠用於支付或投資目的。在選用「交易」和「移轉」這兩個術語時，FATF 有意為虛擬資產創造了一個廣泛的通用定義，其中涵蓋了廣泛的活動。例如，這可能包括將資產發行給另一個人、將其交換為其他東西、將其移轉給其他人或代表其他人、更改其所有權或銷毀它。

---

<sup>16</sup> 這些與客戶審查（建議第 1 項）和電匯規則（建議第 16 項，即轉帳規則）有關。有關這些義務之進一步解釋，請參見下文第三部分和第四部分。

49. 虛擬資產不能僅僅是 FATF 建議其他部分已經涵蓋之法定貨幣、證券和其他金融資產之數位表現，而本身沒有數位交易或移轉之固有功能，亦不能用於支付或投資目的。
50. 基於此原因，例如，以數位格式保存之銀行紀錄，代表一個人對法定貨幣所有權，這並不是虛擬資產。如果僅作為 FATF 國際標準所涵蓋金融資產所有權或部位之聲明性紀錄，則不是虛擬資產。但是，可兌換為另一種資產之數位資產，例如可兌換法定貨幣或以穩定比率交換成虛擬資產之穩定幣，則仍可稱為虛擬資產。在這種情況下，關鍵問題是虛擬資產是否具有可交易或移轉並用於支付或投資的內在價值，或者只是一種記錄或代表其他事物所有權的手段。然而，值得重申的是，不符合虛擬資產條件之資產不應被推定為不屬於 FATF 國際標準之範圍。相反地，其可能屬於其他類型的金融資產，例如證券、商品、衍生性商品或法定貨幣。
51. FATF 無意使資產同時成為虛擬資產與金融資產。然而，可能會出現同一資產在不同國家框架下受不同分類，或者同一資產可能在多個不同類別下受到監理之情形。在確定新數位資產是否應符合金融資產或虛擬資產之資格時，權責機關應考慮其既有之金融資產管理制度或虛擬資產制度是否得以適當地適用於相關新數位資產。例如，如果相關資產為現金、無記名可轉讓金融工具或不記名股票之功能性數位等價物，有權機關應考慮相關制度下抵減措施如何適用於該等資產。
52. 在特徵證明困難之情況下，各司法管轄區應評估其監管體系並決定指定為哪種類別最能抵減並管理商品或服務的風險。司法管轄區亦應考慮普遍接受之資產用途（例如，是否用於支付或投資目的）以及哪種類型的監理制度最為適合。如果司法管轄區選擇將資產定義為金融資產而不是虛擬資產，則既有之防制洗錢或打擊

資恐標準和附隨於金融資產之指引將適用。與技術中立方法一致，被定義為金融資產之以區塊鏈為基礎之資產可能不屬於此聚焦虛擬資產之指引。這是因為其使用之技術不是決定適用何種 FATF 建議之決定要素。然而，本指引之因素可能仍被證明對司法管轄區和私部門有幫助，並應在風險基礎方法之下補充其他既有指引。儘管如此，用於支付或投資之各項資產均有適用於虛擬資產或其他類型金融資產的義務。

53. 獨特且不可互換的，並在實務上用作收藏品而不是支付或投資工具之數位資產，可稱之為非同質化代幣 (NFT) 或加密收藏品。根據 FATF 之定義，此類資產具體取決於其特徵，通常不被視為虛擬資產。然而，重要是要考慮非同質化代幣之性質及其功能，而不是所使用術語或行銷用語。這是因為 FATF 國際標準可能涵蓋它們，而不管術語如何。一些表面上似乎不構成虛擬資產之非同質化代幣，如果它們在實務中用於支付或投資目的，則可能屬於虛擬資產之定義。其他非同質化代幣是 FATF 國際標準所涵蓋之其他金融資產之數位表現。因此，此類資產不屬於 FATF 對虛擬資產之定義，但將作為此類金融資產而為 FATF 國際標準所涵蓋<sup>17</sup>。鑑於虛擬資產領域正在迅速發展，功能性方法在非同質化代幣和其他類似數位資產之脈絡特別重要。因此，各國應根據具體情況考慮將 FATF 國際標準適用於非同質化代幣。
54. FATF 重申 G20 報告中的聲明，係根據用於任何其他類型數位資產之相同標準，如同虛擬資產或其他金融資產 ( 例如有價證券 )，穩定幣依其確切性質和國家之監管制度，為 FATF 國際標準所涵蓋，

---

<sup>17</sup> 參第 50 段。

▪ *何謂虛擬資產服務提供商？*

55. 正如 FATF 詞彙表所述，「虛擬資產服務提供商」係指 FATF 建議其他部分未涵蓋，並以為或代表另一自然人或法人進行以下一項或多項活動或營業為業務之任何自然人或法人：
- i. 虛擬資產與法定貨幣間之交換；
  - ii. 一種或多種形式虛擬資產間之交換；
  - iii. 虛擬資產之移轉<sup>18</sup>；
  - iv. 保管及／或管理虛擬資產或得控制虛擬資產之工具；
  - v. 參與及提供與發行人募集及／或出售虛擬資產相關之金融服務
56. 如同虛擬資產之定義，虛擬資產服務提供商定義應被廣泛解讀。各國應採用功能方法並適用定義中以下概念來確定實體是否進行虛擬資產服務提供商之功能。各國不應根據實體用來描述自身或其活動之技術所採用的術語或命名法來適用此定義。如上所述，定義不取決於服務提供商所採用之技術。FATF 國際標準中之義務源於所提供之基礎金融服務，而不考慮實體之營運模式、技術工具、分類帳設計或任何其他營運特徵。為了幫助闡明定義之概念，以下部分包括使用通用用語來描述常見商業模式之釋例。但是，這些不應掩蓋該定義之應用係根據對相關實體是否提供合格服務之評估而不是術語本身之事實。
57. 在審視各功能前，必須瞭解一些通用要素。正如虛擬資產定義中所討論的，為避免重複或重疊，虛擬資產服務提供商之定義僅適用於「FATF 建議其他部分未涵蓋」的實體。其不包括 FATF 國際標準其他部分涵蓋之金融機構或指定之非金融事業或人員。各

---

<sup>18</sup> 在虛擬資產之脈絡下，移轉是指代表另一自然人或法人進行交易，將虛擬資產從一個虛擬資產位址或帳戶移轉到另一個虛擬資產位址或帳戶。

司法管轄區必須基於對各定義概念基礎之理解，適用最合適之定義。從本指引角度來看，虛擬資產服務提供商與傳統金融機構之間之主要區別在於建議第 10 項與建議第 16 項之適用，因此各司法管轄區可能希望適用提供更全面監管與監理範圍<sup>19</sup>之定義。

58. 定義中首次使用「人」一詞係指進行定義第 (i)-(v) 項所列相關活動或營業的人。該人可以是法人，例如公司，亦可以是自然人（個人）。
59. 「進行」包括提供及／或積極促進服務，此係指積極參與提供虛擬資產服務提供商定義第 (i)-(v) 項所涵蓋之活動。其旨在排除不提供或積極促進任何涵蓋活動之輔助參與者，例如提供網際網路或雲端服務之實體。
60. 「作為業務」一詞旨在將那些可能出於非商業原因而偶爾執行某項職能的人排除在虛擬資產服務提供商之範圍之外。為了滿足此部分定義，實體必須為或代表另一個自然人或法人履行此一職能，而不是出於商業原因代表自己，且必須至少有足夠定期之基礎，而不是偶一為之。
61. 「為／或代表另一自然人或法人」一詞包括在向另一人提供涵蓋服務之過程中履行職能。為其提供或代表其提供金融服務之人亦可稱之為這些服務的「用戶」或「客戶」。這表示，例如，單一法人在該法人內部（例如在特定公司之單位內）進行之虛擬資產內部移轉不符合虛擬資產服務提供商之條件，除非該移轉是為了或代表提供虛擬資產服務提供商服務之其他人。

---

<sup>19</sup> 這些差異與客戶審查（建議第 10 項）、降低客戶審查之臨時性交易門檻以及電匯規則（建議第 16 項）有關，這些規則以修訂方式適用於虛擬資產移轉（即轉帳規則）。有關這些義務的進一步解釋，請參見下文第三部分和第四部分。



62. 滿足該等規範之人如果執行一個或數個虛擬資產服務提供商定義所描述之五類活動或營運（即虛擬／法定貨幣之「交換」、虛擬／虛擬之「交換」、「移轉」、「保管及／或管理」以及「參與提供與發行人募集及／或出售虛擬資產相關之金融服務」）即為虛擬資產服務提供商。各定義之涵蓋範圍如下所示。

▪ **交易及移轉**

63. 虛擬資產服務提供商定義的第 (i) 項係指任何提供虛擬資產以交換法定貨幣，或提供法定貨幣以交換虛擬資產之服務。如果當事人可使用法定貨幣支付虛擬資產，或可以使用虛擬資產支付法定貨幣，則該服務之供給者或提供者於以此為業時為虛擬資產服務提供商。同樣地，在第 (ii) 項中，如果各方當事人可以使用一種虛擬資產作為另一種虛擬資產之交換方式或支付形式，則該服務的供給者或提供者於以此為業時為虛擬資產服務提供商。應強調者，第 (i) 和 (ii) 項包括上述活動，無論服務提供商於其使用者面前扮演何種角色，如擔任相對人、作為清算或結算交易之中央交易對手，作為交易平台，或作為促成交易之另一中介單位。虛擬資產服務提供商不需提供交易或移轉的所有要素方能成為虛擬資產服務提供商，只要它代表另一個自然人或法人以進行交易活動為業即可。
64. 虛擬資產服務提供商定義中的第 (iii) 項涵蓋任何允許使用者將虛擬資產的所有權或控制權移轉給另一個使用者或在同一使用者持有的虛擬資產位置或帳戶間移轉虛擬資產的任何服務。FATF 國際標準將第 (iii) 項定義為「代表另一自然人或法人進行交易，將虛擬資產從一個虛擬資產位置或帳戶移轉到另一個」。為助於說明該項在運作上涵蓋的內容，考量所謂之移轉後虛擬資產當下之

本質是有幫助的。如果新的一方擁有虛擬資產的託管權或所有權，有能力將虛擬資產之控制權移轉給他人，或有能力從其使用中受益，則很可能發生了移轉。這種控制不一定是單邊的，且本質上多重簽名<sup>20</sup>過程並不被排除（參下述第(iv)項），其中虛擬資產服務提供商代表另一個自然人或法人進行活動以作為業務。同樣地，如果一個人始終保持對其資產的單方面控制，這可能表示服務提供商沒有提供符合第(iii)項所稱之服務。然而，如果它積極促成移轉（見第59段），它仍可能符合第(iii)項。這還包括同一虛擬資產服務提供商之使用者間的移轉，包括虛擬資產服務提供商使用一鏈下內部記錄保存系統，且虛擬資產保留在同一個鏈上綜合錢包或帳戶中之情況。

65. 該項在概念上類似於建議第14項金錢或價值移轉服務（MVTS）所涵蓋之金融資產。<sup>21</sup> 第(iii)項所涵蓋服務之例示，包括積極促使或允許使用者向其他自然人發送虛擬資產之功能，如個人匯款支付、非金融商品或服務的支付，或工資的支付。提供此類服務的提供商可能是虛擬資產服務提供商。
66. 交易或移轉服務也可以透過通常被稱為去中心化交易或平台之技術進行。例如，「去中心化或分散式應用程式（去中心化應用程式）」是指在區塊鏈或類似技術上運作的軟體程式的術語。有時，此類應用程式會促進或支持其他協議、應用程式或數位資產及其移轉。這些應用程式或平台通常在去中心化之帳本上運作，但通常仍然有一個中央方參與或控制之機制，例如創造和發行一個虛

---

<sup>20</sup> 在多重簽名之過程或程序中，一個人需要數個數位簽章（因此需要多個私鑰）才能從錢包執行交易。

<sup>21</sup> 在多重簽名之過程或程序中，一個人需要數個數位簽章（因此需要多個私鑰）才能從錢包執行交易。

擬資產、為持有管理「密鑰」或收取費用之帳戶開發去中心化應用程式功能和使用者界面。通常，去中心化應用程式可以被編制為要求使用者支付費用來與去中心化應用程式互動，這通常以虛擬資產支付，以實現所有者／運營商／開發者／社區之最終利益。去中心化應用程式可以促進或實行虛擬資產之交易或移轉。在這些去中心化應用程式提供金融服務之情形，例如虛擬資產服務提供商提供之服務，通常使用術語「去中心化金融」（DeFi）。

67. 去中心化金融應用程式（即軟體程式）並非 FATF 國際標準下的虛擬資產服務提供商，因為該標準不適用於基礎軟體或技術（見以下第 82 段）。然而，在去中心化金融安排中，保持控制權或足夠影響力的創造者、所有者和運營商或其他人，即使這些安排看起來是去中心化的，也可能屬於 FATF 定義之提供或積極促進虛擬資產服務提供商服務之虛擬資產服務提供商。即使其他方在服務中發揮作用或流程的某些部分是自動化的，亦是如此。所有者／營運商通常可以藉由他們與所進行活動之關係來區分。例如，可能對資產或服務協議的各個方面存在控制或足夠的影響，且他們自身與使用者間存在持續的業務關係，即使這是通過智能合約或在某些投票協議之情況下行使的。各國可能還希望考慮其他因素，例如任何一方是否從服務中獲利，或者是否有能力設置或更改參數以識別去中心化金融安排之所有者／運營商。這些並不是使所有者／營運商成為虛擬資產服務提供商的唯一特徵，但它們是例示性的。根據其運作，可能還有其他虛擬資產服務提供商與去中心化金融安排之互動。
68. 由於該領域眾多開放原始碼項目和開發貢獻者於全球的出現，去中心化金融項目之數量和功能正在迅速擴大。雖然本指引旨在提

供指導，但各國需要評估個別情況之事實和情形，以確定是否有可識別之人，無論是法人或自然人，提供所涵蓋之服務。去中心化金融之行銷術語或自我識別非決定性的，所涉及的特定技術亦無法確定其所有者或運營商是否為虛擬資產服務提供商。各國應以廣義解釋定義之方式，適用標準中包含之原則，但要考慮功能取向之實際目的。似乎很常見去中心化金融安排稱自己為去中心化，但實際上包括一個具有控制權或足夠影響力的人，各司法管轄區應在不考慮自我描述的情況下適用虛擬資產服務提供商之定義。各國應遵循 FATF 旨在含括從事包括在定義中所述之金融服務之自然人或法人為事業之原則。如果它們符合虛擬資產服務提供商之定義，所有者／運營商應在發行或使用軟體或平台之前，進行洗錢與資恐風險評估，並採取適當措施以持續和前瞻性的方式管理和抵減這些風險。<sup>22</sup> 如果某人可以購買虛擬資產服務提供商管理之代幣，則虛擬資產服務提供商應保有履行防制洗錢／打擊資恐義務的責任。在這種情況下，如果個別之代幣持有人沒有代表他人對虛擬資產服務提供商之業務活動行使控制權或有足夠的影響力，個別代幣持有人無此責任。

69. 如果無法辨識對去中心化金融安排具有控制力或足夠影響力的法人或自然人，則可能不存在符合虛擬資產服務提供商定義之實際所有者／運營商。各國應監控去中心化金融服務和安排在此類情況下所呈現之風險的緊急情況，包括與來自其去中心化金融社區之代表接觸。各國應在適當情況下考慮任何抵減措施，前提是他們理解以此方式運作之去中心化金融服務。如有必要，可以在服

---

<sup>22</sup> 有關虛擬資產服務提供商於新技術方面之義務的更多資訊，請參見下文第 III 部分中之建議第 15 項。

務開始之前或在提供去中心化金融服務的過程中採取此類措施。例如，在虛擬資產服務提供商未被辨識之情況下，各國可以考慮要求受監管的虛擬資產服務提供商進行與去中心化金融安排相關活動，以符合該國的風險基礎方法 (RBA) 或其他抵減措施，以此作為選項。各國還可以考慮本指引中所述與 P2P 相關的洗錢與資恐風險和潛在的抵減措施。<sup>23</sup>

70. 根據虛擬資產服務提供商定義之第 (i)、(ii) 和 (iii) 項，其他常見的虛擬資產服務或商業模式也可能構成交易或移轉活動。如果此類服務或模式背後的自然人或法人代表他人進行或提供活動並以此為業，則他們將成為虛擬資產服務提供商。這些可以包括：
- a. 虛擬資產之託管服務，包括涉及智能合約技術的服務，虛擬資產之買方用於發送、接收或移轉法定貨幣以換取虛擬資產，而提供服務的實體對資金擁有託管權；
  - b. 代表自然人或法人使用者促進虛擬資產發行和交易之經紀服務；
  - c. 訂單簿交易服務，其將買賣雙方的訂單匯集在一起，可能是通過使用配對引擎來匹配使用者的買賣訂單，方便使用者能夠找到交易對手、發現價格和進行交易。但是，只允許虛擬資產的買賣雙方相互尋找彼此，而不從事虛擬資產服務提供商定義中之任何服務的平台不是虛擬資產服務提供商；以及
  - d. 進階交易服務，其允許使用者使用更複雜的交易技術，例如保證金交易或基於演算法之交易。

---

<sup>23</sup> 參見本指引第 37 至 41 以及 104 至 106 段。

71. 交易及／或移轉之業務模式可以包括促進虛擬資產交換法定貨幣及／或其他形式的虛擬資產以獲得報酬（例如，為了費用、佣金、價差或其他利益）的虛擬資產交易或虛擬資產移轉服務。這些模式通常接受多種之支付方式，包括現金、電匯、信用卡和虛擬資產。傳統的虛擬資產交易或移轉服務可以是管理員附屬、非附屬或第三人提供者。自助服務的提供者——通常被稱為「ATM」，「比特幣櫃員機」、「比特幣 ATM」或「自助服務」——也可能落入上述定義，因為他們通過實體電子終端機（自助服務）提供或積極促使所涵蓋之虛擬資產活動，使所有者／運營商能夠促使將虛擬資產兌換為法定貨幣或其他虛擬資產以及／或將法定貨幣兌換為虛擬資產。

▪ **保管及／或管理**<sup>24</sup>

72. 虛擬資產服務提供商定義的第 (iv) 項也應廣義地理解。任何有能力控制虛擬資產之實體都可能符合第 (iv) 項的條件，因為這是「管理」和「保管」這兩個詞的概念上的含義。簡單來說，「保管」包括代表另一個人持有虛擬資產或虛擬資產私鑰之服務。「管理」一詞還可包括為他人或代表他人管理虛擬資產之概念。
73. 用語「控制」應理解為持有、交易、移轉或花費虛擬資產之能力。可以使用虛擬資產或變更其處置之各方當事人可以控制它。正如在「移轉」的定義中，這並不意味著控制必須是單方面的。「控制」可以包括需要他人持有的密鑰或憑據以更改資產處置之情形，例如多重簽名程序。多重簽名模式或多方必須使用密鑰才能進行

---

<sup>24</sup> 本節中使用之用語（例如「保管」、「管理」和「輔助服務」）是在虛擬資產／虛擬資產服務提供商之脈絡中使用和解釋。它們不應在其他情況下與此類用語之使用相混淆（例如與銀行和其他傳統金融工具或服務有關者）。

交易的其他模式之存在，並不代表特定實體不保有控制權，這取決於它可能對虛擬資產產生的影響程度。這種對控制的解釋也適用於解釋第 (iv) 項定義中的「授權控制」。

74. 定義的部分將包括，例如，多數的託管錢包服務提供者，因為他們代表另一人持有以及／或保留虛擬資產。可能提供託管服務之人，例如律師，應考慮他們是否頻繁提供此類服務作為一項業務，以及控制要素是否由他們自身或由其將控制力委外之一方實際提供，例如託管錢包服務提供者，其將虛擬資產委託給他們。提供定義中所述之功能應該是確定虛擬資產服務提供商而不是歸類如律師之決定性因素。如有疑問，應彈性解釋定義之普遍用語，以涵蓋為他人或代表他人提供對虛擬資產控制之任何實體。
75. 在虛擬資產服務提供商定義之第 (iv) 項的脈絡下，假設此類管理和傳輸將僅根據所有者／使用者的指示進行，各國應考慮提供保護個人虛擬資產或管理或移轉虛擬資產之權力機制的服務或商業模式。託管和管理服務可能包括控制與屬於另一人之虛擬資產相關的私鑰之人，或者控制非為涉及屬於他人的虛擬資產之一方的智能合約之人。
76. 僅提供輔助基礎設施使另一實體提供此服務之機構，例如負責驗證簽名準確性的雲端數據儲存提供商或整合服務提供商，通常不會滿足此定義。這一項通常也不包括軟體開發商或非託管錢包的供應商，其功能只是開發及／或銷售軟體／硬體<sup>25</sup>。然而，各國在將定義適用於特定個案時，必須考慮個別事實和情況。

---

<sup>25</sup> 參第 82 段。

▪ 參與和提供與發行人的募集及／或銷售相關之金融服務

77. FATF 對虛擬資產服務提供商的定義旨在涵蓋與首次代幣發行相關的活動。首次代幣發行通常是一種自早期支持者處為新項目募集資金之手段。第 (v) 項特別涵蓋透過如首次代幣發行等活動參與發行人之募集以及／或銷售虛擬資產或向其提供相關金融服務的人。在虛擬資產之發行、募集、銷售、分銷、持續市場流通和交易之脈絡下，這些人可能與從事首次代幣發行的發行人相關或不相關。例如，這可能包括接受買單和資金以及從發行人處購買虛擬資產以轉售和分配資金或資產之事業，以及詢價圈購、承銷、造市和配售代理活動等。虛擬資產服務提供商定義之其他部分也可能與參與首次代幣發行之業務相關。參與發行的自然人和法人還可以提供具虛擬資產服務提供商定義第 (i) 至 (iv) 項規定之涉及交易、移轉或保管活動之服務。這對於發行虛擬資產並透過如首次代幣發行等活動募集／銷售虛擬資產之虛擬資產發行人尤其相關。
78. 為明確起見，完全透過自身發行虛擬資產<sup>26</sup>之單一行為並非虛擬資產服務提供商定義第 (v) 項下的所涵蓋之服務。然而，任何為他人或代表他人從事已發行虛擬資產之交易和移轉為業之人均屬於含括之服務，與任何發行有關之首次代幣發行相關之金融服務的參與和提供，亦屬於含括在內之服務。創造虛擬資產軟體以發行虛擬資產之不相關聯的行為，不會使創建者成為虛擬資產服務提供商，除非創建者另以為他人或代表他人從事定義中提及之涵蓋功能為業。

---

<sup>26</sup> 在此脈絡下，發行係指創造虛擬資產，與發行該虛擬資產相關之虛擬資產之募集及／或銷售。



79. 一個司法管轄區管理參與或提供與發行人發行、募集、銷售及／或分銷相關之金融服務之服務提供者所適用之防制洗錢／打擊資恐義務，例如於首次代幣發行之脈絡下，可能涉及單一國家一個或數個防制洗錢／打擊資恐和非防制洗錢／打擊資恐法規，例如與貨幣傳輸、證券、貨物，及／或衍生性商品活動相關之法規。

## 第 2 欄 首次代幣發行 (ICO) 之特徵釋例

數位資產可使用分散式帳簿或區塊鏈技術發行及／或移轉。分配此類資產之機制之一是通過通常稱為首次代幣發行之活動。在首次代幣發行中，發行人或發起人通常會出售數位資產以換取法定貨幣或其他虛擬資產。首次代幣發行通常通過各種行銷素材在線上宣布和推廣。發行人或發起人通常會發布一份「白皮書」，描述該項目並宣傳首次代幣發行。發行人或發起人可能會告知潛在認購者，從銷售中籌集的資金將用於資助數位平台、軟體或其他項目的開發，並且在某些時候，數位資產本身可能會被用於進入平台，使用軟體，或以其他方式參與計畫。在募集過程中，發行人或發起人可能會使數位資產認購人期待他們的投資回報或參與該項目提供回報的一部。於數位資產發行後，可能會在次級市場轉售給其他人（例如，在數位資產交易平台或透過虛擬資產服務提供商）。

在確定虛擬資產服務提供商的定義在首次代幣發行如何適用於實體時，資產、活動或服務背後之事實和情況將決定分類，而非市場參與者使用的任何標籤或術語。例如，一個人創建了一個符合虛擬資產定義之數位資產。該人將虛擬資產出售給買受人，即使虛擬資產本身可能會在嗣後交付給買受人，並且事業使用從銷售中獲得的價值來開發最終可能使用虛擬資產之平台或生態系統。在此情況下，

如果除了發行本身之外，它進行屬於虛擬資產服務提供商定義任何一項的其他活動，則該出售虛擬資產之人為虛擬資產服務提供商（例如，如果他們將虛擬資產交換為法定貨幣或其他虛擬資產（第(i)項及第(ii)項），或者如果他們在首次代幣發行之後透過擔任造市者就虛擬資產提供流動性（第(v)項））。就他人虛擬資產銷售提供相關金融服務之事業（例如擔任該人之經紀商或交易商），則將依照虛擬資產服務提供商定義之第(v)項，成為虛擬資產服務提供商，無論他們是否正式地隸屬於該人。客戶是否擬使用虛擬資產作為投資或作為支付方式，並非重點。

或者，上例中的數位資產依照一國之法律，可能被視為一個有價證券。在這種情況下，根據事實和情況，一個國家的證券法令可能適用。因此，數位資產之發行人是否將被視為虛擬資產服務提供商或有價證券發行人，將取決於首次代幣發行的個別事實和情況，以及該國之法律。其他司法管轄區也可能有不同的取向，其中可能包括支付型代幣。一人可能從事之活動可能使他們受到超過一種類型監管框架之約束，且該人使用的數位資產可能同樣地受到超過一種類型的監管框架之約束。

#### ▪ 定義的範圍

80. 儘管該部門發展之行銷術語及創新商業模式很多且時常改變，但如果各國正確應用該定義，FATF 預期鮮少有虛擬資產之安排沒有在某個階段涉及虛擬資產服務提供商。各國應特別注意評估事業可能對去中心化或分散式服務模式提出之任何主張，並根據其風險及其抵減這些風險的能力對商業模式進行自我評估。

81. 如前所述，FATF 國際標準是技術中立的，因此，FATF 未企圖監管作為虛擬資產或虛擬資產服務提供商活動背後之技術。相反地，FATF 旨在監管這些代表另一個自然人或法人從事上述虛擬資產服務提供商活動為業的技術背後的自然人或法人。
82. 創建或銷售軟體應用程式或虛擬資產平台之人（即軟體開發商）在單獨創建或銷售應用程式或平台時，可能不構成一個虛擬資產服務提供商。然而，代表他人使用應用程式或平台以從事虛擬資產服務提供商功能為業，將改變此一判斷。此外，指示軟體或平台之創建及開發之一方，以便他們可以為他人或代表他人提供虛擬資產服務提供商服務為業者，也可能有資格成為虛擬資產服務提供商，特別是如果他們對資產、軟體、協議或平台或與軟體使用者之任何持續業務關係，保留控制權或足夠的影響力，即便此係透過智能合約而行使。因此，此類虛擬資產服務提供商負責遵守相關的防制洗錢／打擊資恐義務。因此，他們應在發行或使用軟體或平台之前，進行洗錢與資恐風險評估，並採取適當措施以持續和前瞻性的方式抵減風險。
83. FATF 亦未企圖就向虛擬資產網路提供輔助服務或商品之人如同虛擬資產服務提供商之自然人或法人般進行監管。這包括提供輔助服務，如硬體錢包製造商或非託管錢包的提供者，只要他們不以為或代表他人參與或積極促使任何上述範圍內之虛擬資產活動或營運為業。同樣地，僅從事虛擬資產網路營運且不代表其客戶參與或促進虛擬資產服務提供商之任何活動或營運的自然人或法人（例如，提供網際網路服務和基礎設備、提供運算資源，如雲端服務，以及創造、驗證和播送交易區塊），依照 FATF 國際標準並非虛擬資產服務提供商，即使它們從事該等活動為業。

84. 正如 FATF 將虛擬資產之個人使用者（非以此為業）作為虛擬資產服務提供商進行監管—儘管承認此類使用者根據司法管轄區之規則或執法框架可能仍需遵守遵法義務—FATF 同樣地亦未試圖去涵蓋不可移轉、不可交易以及不可用於支付或投資目的之封閉式項目之類型。此類項目可能包括航空里程、信用卡獎勵或類似的酬賓方案獎勵或積分，個人無法在封閉式系統外的次級市場上繼續銷售。相反地，虛擬資產及虛擬資產服務提供商之定義旨在涵蓋特定的金融活動和運作（即移轉、交易、託管以及管理，以及提供與發行相關之金融服務等）以及可按市場價格轉換或互換之資產——無論是虛擬至虛擬、虛擬至法定，或是法定至虛擬。接受虛擬資產作為商品及服務的支付方式，例如商家在商品購買時接受虛擬資產，也不構成虛擬資產服務提供商活動。然而，促使公司接受虛擬資產作為支付方式之服務將是虛擬資產服務提供商。
85. 防制洗錢／打擊資恐法規將適用於所涵蓋之虛擬資產活動和虛擬資產服務提供商，無論涉及金融活動之虛擬資產類型（例如，使用或向他人提供強化匿名加密貨幣 (AEC) 以進行各種金融交易的虛擬資產服務提供商）、基礎技術（例如，其是否使用主網或使用嵌入式分層或其他擴展解決方案），或平台可能包含的附加服務（例如混幣器或轉向器或其他潛在之混淆功能）。
86. 就穩定幣而言，一系列實體都涉及任何穩定幣之安排。穩定幣可能有一個中央開發者或治理機構。一個治理機構由一個或多個自然人或法人組成，他們建立或參與建立管理穩定幣安排之規則（例如，確定穩定幣的功能，誰可進入該等安排以及是否／如何將防制洗錢／打擊資恐預防措施被建置於安排中）。他們還可以執行穩定幣安排的基本功能（例如管理穩定功能），或者可以委託給

其他實體。他們也可以管理穩定幣與電信平台的整合，或促使遵守整個穩定幣安排的通用規則。

87. 如果穩定幣安排中存在這樣的中央機構，它們通常會被 FATF 國際標準涵蓋為金融機構或虛擬資產服務提供商。如果治理機構在穩定幣安排中實行其他職能，則尤其如此。因此，此類機構應在推出或使用穩定幣之前進行洗錢與資恐風險評估，並在推出前採取適當措施以管理和抵減整個安排之風險。<sup>27</sup>
88. 並非所有穩定幣都有一個易於識別為虛擬資產服務提供商或金融機構之中央機構。但是，在穩定幣發行前，更有可能需要存在一方以推動此類安排之發展及發布。如果該實體過去係一個事業並從事虛擬資產服務提供商功能，這將為發行前階段的監管或監理行動創造了空間。如果沒有明確可識別的虛擬資產服務提供商或金融機構，該國應仔細考慮特定穩定幣帶來的風險以及抵減措施的必要性，如有（例如，參見第 105 段至 106 段中之點對點交易抵減措施）。此外，這並不代表涉及那些只開發軟體程式之人，而是涉及穩定幣安排之人員，其從事或提供虛擬資產服務提供商定義項下所涵蓋之金融服務。
89. 穩定幣安排中的一系列其他實體，也可能負有防制洗錢／打擊資恐義務，例如交易所或託管錢包服務。為了說明這一點，方框 3 中列出了一個假設案例研究。重點是應注意，任何安排之精確細節都必須接受獨立監督方可做出這些判斷。<sup>28</sup>

---

27 有關虛擬資產服務提供商於新技術方面之義務的更多資訊，請參見下文 III 部分中的建議第 15 項。這也與 FATF 關於預付卡、行動支付和以互聯網為基礎之支付服務的報告中「新支付商品和服務 (NPSS)」提供商之情況一致，更多資訊請參：[www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf)。

28 關於在所謂的穩定幣安排中將 FATF 國際標準適用於不同實體之更多詳細資訊，請參見 FATF 向 G20 提交之關於所謂穩定幣的報告。

### 第 3 欄：穩定幣安排之假設案例研究和 FATF 國際標準之適用

#### ▪ 假設情形<sup>29</sup>

一家公司（「該公司」）正在設計一款基於分散式帳簿技術之平台，以發行旨在作為穩定幣（「該幣」）之數位資產。

該幣將由該公司管理之多個全球金融機構的帳戶中持有的資產作為支持（合稱為「準備金」）。該幣之市場價值將通過授權參與者機制與準備金中持有之資產價值保持一致。只有授權參與者才能透過該公司從準備金中購買或贖回該幣。根據該公司倡議之生態系統，該公司和第三人（合稱為「驗證方」）將使用其他第三人之雲端基礎設施營運一個經許可之區塊鏈網路。該公司正透過首次代幣發行為該幣籌集資金。

該公司、第三人以及個別使用者將能夠進入、使用和交易該幣。任何第三人擬連接至網路，例如交易平台和託管錢包提供者，都需要取得該公司之核准。該幣之錢包將允許使用者發送、接收和儲存該幣，任何開發者／第三人都可以提供他們客制化的錢包。該幣將依照該公司所訂之規則進行移轉，並在開始營運前由監理機關評估。特約商家亦可使用該幣作為商品和服務之付款方式。

#### ▪ FATF 國際標準下之義務實體及其防制洗錢／打擊資恐義務。

於此情境下，該公司是 FATF 國際標準下之虛擬資產服務提供商或金融機構，因其職能包括與授權參與者交易該幣，包括通過首次代幣發行籌集資金。除了那些在生態系統中具有防制洗錢／打擊資恐

---

<sup>29</sup> 本案例研究中所包含之情境，改編自 IOSCO 於 2020 年 3 月全球穩定幣倡議之報告中之個案研究。其已被修改以符合防制洗錢／打擊資恐之脈絡。提供此例示是為了描繪於假設之穩定幣安排中人員之義務，其並非詳盡而無遺漏。

義務之其他第三人外，該公司將承擔防制洗錢／打擊資恐義務。根據 FATF 國際標準，該公司應採取適當措施抵減整個生態系統中的洗錢與資恐風險（例如在該幣之設計、核准授權參與者之標準和流程等方面）。

授權參與者亦為虛擬資產服務提供商，因其職能包括促進虛擬資產之發行、分銷和交易。交易平台屬虛擬資產服務提供商，因其功能包括在該幣和法定貨幣以及其他虛擬資產間進行交易、移轉該幣以及保管及／或管理該幣。託管錢包提供商是虛擬資產服務提供商，因其功能包括移轉該幣和保管及／或管理該幣。

於生態系統中，不屬於 FATF 國際標準中虛擬資產服務提供商定義之參與者包括：其職能僅為管理準備金之全球金融機構（儘管它們被 FATF 國際標準涵蓋為金融機構）；除了該公司以外之驗證者，其職能僅於驗證交易；僅提供基礎設施營運功能之雲端服務提供商；其職能僅係製造和銷售設備的硬體錢包製造商；僅有開發及／或銷售軟體／硬體功能之非託管錢包的軟體提供商；僅提供商品和服務以換取該幣之商家；不承擔任何虛擬資產服務提供商功能之軟體開發商；以及個人使用者。

重點是需注意，任何安排之確切細節都必須事先經過充分和獨立的審查才能做出該等決定，而防制洗錢／打擊資恐措施之確切適用將取決於每個國家之決定。這只是一個說明性的例示，並非所有的穩定幣都是以此方式安排。根據各別國家、與例如證券、商品及衍生性商品之金融資產相關之法律，亦可能與此情形有關。如果各國認為洗錢與資恐風險高至無法接受，例如與潛在的點對點交易相關，也可以採取其他措施（有關各國可以採取之措施的進一步資訊，請參考第 105 段至 106 段）。

90. 某些平台和提供商提供在個人使用者之間直接進行虛擬資產移轉之能力。對於此類平台，上述定義之廣義解釋將決定提供此類服務的各方在功能性基礎上是否是虛擬資產服務提供商，而非基於自我描述或採取之技術。只有提供非常有限之功能，但不能提供交易、移轉、保管、管理、控制和提供與發行有關之金融服務的實體通常不會成為虛擬資產服務提供商。例如，這可能包括只為買賣雙方提供確認和交流之論壇，而不提供（甚至提供部分）包含在虛擬資產服務提供商定義中那些服務之網站。
91. 對於自行描述之 P2P 平台，各司法管轄區應關注背後之活動，而不是稱號或是商業模式。某些「配對」或「尋找」種類之服務即使沒有涉及交易，也可能符合虛擬資產服務提供商之條件。FATF 對虛擬資產和虛擬資產服務提供商之定義採取了廣義的觀點，並認為目前正在運作的大多數安排，即使它們自我歸類為 P2P 平台，可能至少有一些人參與某個商品開發和發布的階段，其構成了虛擬資產服務提供商。自動化被用作為企業提供涵蓋服務的流程，其並不能免除控制方的義務。
92. 決定一個服務提供者是否符合虛擬資產服務提供商之定義，應考慮商品和服務的生命週期。例如，推行一項將提供虛擬資產服務提供商服務之服務，將被課以虛擬資產服務提供商之義務，即使這些功能未來將自動實行，特別是如果提供者將保持某種控制措施或足夠的影響力，例如通過設置參數、持有管理密鑰，保留對平台的進入權限或收取費用或實現利潤。使用如智能合約等自動化流程來執行虛擬資產服務提供商功能，並不能免除虛擬資產服務提供商義務的部分（各方）責任。在這種情況下，有資格成為虛擬資產服務提供商之控制方，應在平台啟用或使用之前進行洗



錢與資恐風險評估，並採取適當措施抵減風險。這可能包括有效地將防制洗錢／打擊資恐之實行義務委託給參與平台的另一個自然人或法人。

93. 然而，FATF 認識到，於確定哪些實體是虛擬資產服務提供商並決定其監管範圍，擴張的取向可能會給權責機關帶來實行的挑戰。當需要評估特定實體以確定其是否為虛擬資產服務提供商或評估虛擬資產服務提供商情況不明之商業模式時，一些一般性問題可以幫助獲取答案。其中包括誰從服務或資產之使用中獲取利益，誰建立並可以改變規則，誰可以做出影響營運之決策，誰生產並促成商品或服務的創新和發行，誰與擁有和控制其營運數據之締約方或其他人保持了持續的業務關係，以及誰得以關閉商品或服務。個案情況下將會有所不同，此列舉並非絕對的，僅提供一些例示。
94. FATF 國際標準，包括虛擬資產和虛擬資產服務提供商之定義，代表了各國可採用之最低標準。與風險基礎方法相同，各國可以選擇將其防制洗錢／打擊資恐制度擴張至包括其他數位資產及實體，以超出 FATF 對虛擬資產和虛擬資產服務提供商之定義。此類決定應基於洗錢與資恐風險評估，並考慮監管不一致之相關挑戰。

### 第三部分：將 FATF 國際標準適用於國家和權責機關

95. 第 III 部分說明了有關虛擬資產和虛擬資產服務提供商之 FATF 建議如何適用於國家和權責機關，並著重於辨識和抵減與所涵蓋之虛擬資產活動相關之風險、適用預防措施、適用取得執照和登記註冊之要求、實施與金融機構相關金融活動之監管同等有效之監管，提供一系列有效和具勸阻性的裁罰，並促進國家和國際合作。幾乎所有 FATF 建議，都與瞭解各國應如何利用政府機關和國際合作來解決與虛擬資產和虛擬資產服務提供商相關的洗錢與資恐風險直接相關，而其他建議與虛擬資產或虛擬資產服務提供商的直接或明確關聯較少，但它們仍然具有相關性且可適用。
96. 虛擬資產和虛擬資產服務提供商受 FATF 建議下所有義務之約束，如建議第 15 項注釋所述，包括適用於受防制洗錢／打擊資恐監管之其他實體的義務，基於虛擬資產服務提供商從事之金融活動，並考慮到與所涵蓋之虛擬資產活動或運營相關之洗錢與資恐風險。
97. 本節亦就虛擬資產服務提供商之監理機關適用風險基礎方法進行檢討。

- **建議在虛擬資產及虛擬資產服務提供商脈絡下之適用**
- **風險基礎方法及國家協調**

98. 建議第 1 項。FATF 建議明確指出，各國應適用風險基礎方法以確保預防或抵減洗錢與資恐風險之措施，與其各自管轄管轄區內定義之風險相稱。在風險基礎方法下，各國應加強對涉及虛擬資產之高風險情況或活動之要求。在評估與虛擬資產相關之洗錢與資恐風險，特定類型之虛擬資產金融活動（例如點對點交易），以及虛擬資產服務提供商之活動或營運、中心化和去中心化虛擬

資產間之區別，以及它們是否受制於受監管的虛擬資產服務提供商，可能會持續成為各國考量之一關鍵面向。由於虛擬資產金流之匿名性或混淆性增加的可能性，以及與進行有效監管和客戶審查相關的挑戰，包括客戶辨識和驗證，虛擬資產和虛擬資產服務提供商整體上可能被視為構成更高的洗錢與資恐風險，這可能需要在適當的情況下，根據國家之背景，適用監測和加強盡職調查 (EDD) 措施。

99. 建議第 1 項要求各國辨識、理解和評估其洗錢與資恐風險，並採取旨在有效抵減這些風險的行動。該等要求適用於與建議第 15 項下的新科技相關之風險，包括虛擬資產以及與虛擬資產服務提供商從事或提供所涵蓋之虛擬資產活動、營運、商品或服務之相關風險。在適當和適用的情況下，公私部門之合作可以協助權責機關為所涵蓋之虛擬資產活動（例如虛擬資產支付、虛擬資產移轉、虛擬資產發行等），以及相關虛擬資產技術和新興商品及服務之創新，制定防制洗錢／打擊資恐政策。合作還可以幫助各國權責機關分配資源和擬訂防制洗錢／打擊資恐資源之優先順序。
100. FATF 於 2020 年 10 月修訂了建議第 1 項及其注釋，包括要求各國、金融機構和指定之非金融事業或人員評估 FATF 國際標準定義之資助武擴 (PF) 風險。於 2021 年 6 月，FATF 修訂了建議第 15 項之注釋，以澄清這些資助武擴要求也適用於虛擬資產服務提供商。為澄清這些要求，FATF 於 2021 年 6 月發布了資助武擴風險評估及抵減指引。該指引與各國及虛擬資產服務提供商評估和抵減資助武擴風險有關。各國應辨識、評估並採取有效行動，以抵減與虛擬資產相關之洗錢與資恐／資助武擴風險。
101. 國家機關應對虛擬資產活動、商品和服務以及與虛擬資產服務提

供商和其國內整體虛擬資產服務提供商部門相關之風險合作進行風險評估。風險評估應 (i) 使所有相關機關能夠瞭解特定之虛擬資產商品和服務如何運作、適應和影響所有相關監管司法管轄區，以達到防制洗錢／打擊資恐之目的（例如，資金移轉和支付機制、虛擬資產自助服務、商品、證券或相關發行活動等，如虛擬資產服務提供商定義中所強調者）以及 (ii) 促進對具有類似風險狀況的類似商品和服務進行類似的防制洗錢／打擊資恐處置。在進行風險評估時，包括熟悉虛擬資產、虛擬資產服務提供商及其背後技術之個人尤為重要。

102. 隨著虛擬資產服務提供商部門之發展，各國應考慮審查所涵蓋之虛擬資產活動的防制洗錢／打擊資恐措施與其他監管和監理措施間之關係（例如，消費者和投資人保護、謹慎安全及穩健、網絡資訊科技安全、稅負等），蓋於其他領域採取之措施可能會影響洗錢與資恐風險。在此方面，隨著虛擬資產持續之廣泛採用，各國應考慮著手短期和長期之政策工作，為所涵蓋之虛擬資產活動和虛擬資產服務提供商（以及在虛擬資產領域營運之其他義務實體）制定全面的監管及監理框架。
103. 各國亦應要求虛擬資產服務提供商（以及其他義務實體）辨識、評估並採取有效行動，以抵減與提供或參與所涵蓋之虛擬資產之活動或與提供特定虛擬資產商品或服務相關的洗錢與資恐之風險。於國家法律允許虛擬資產服務提供商之情況下，國家、虛擬資產服務提供商，以及金融機構和指定之非金融事業或人員，包括從事虛擬資產活動或提供虛擬資產商品或服務之金融機構或指定之非金融事業或人員，必須評估相關的洗錢與資恐風險，並適用風險基礎方法以確保採取適當措施預防或抵減這些風險。

104. 如同虛擬資產，以持續和前瞻性的方式分析穩定幣的洗錢與資恐風險是重要的，特別是那些具有眾多採用潛力及可用於點對點交易之風險。在開發新商品時，虛擬資產服務提供商和其他義務實體，應在將其帶入市場前評估洗錢與資恐風險，並在發行前採取抵減措施。潛在的抵減措施可能包括，例如，限制使用者匿名交易能力之範圍、控制可以進入安排之人、控制是否／如何將防制洗錢／打擊資恐預防措施納入該安排，以及／或確保義務實體於安排內之防制洗錢／打擊資恐義務被履行，例如，透過使用軟體來監控交易並偵測可疑活動。監理機關應在准予註冊／給予執照前持續地尋找這些抵減措施。這些商品一旦發行，其風險將更加難以抵減。

#### ▪ 點對點交易

105. 如第 2 部分所述，各國亦應設法瞭解與點對點交易相關的洗錢與資恐風險，以及如何在其司法管轄區內使用它們。各國應考慮有助於瞭解點對點交易風險的措施，包括：

- a. 對私部門實體進行宣傳，包括對虛擬資產服務提供商以及來自 P2P 部門之代表（例如，諮詢有關點對點交易之防制洗錢／打擊資恐要求）；
- b. 培訓監理、金融情報中心（FIU）和執法人員；以及
- c. 鼓勵發展方法及工具，例如區塊鏈分析，收集和評估 P2P 市場指標及風險抵減解決方案，識別可疑行為風險之方法，並確定錢包是託管或非託管<sup>30</sup>，其包括與該領域中之流程人員／開發人員互動。

---

<sup>30</sup> 迄今為止，FATF 未知悉有任何經過技術驗證之方式，可以在所有情況下且僅自虛擬資產位置，以詳盡、精準及準確地識別管理接收人錢包的虛擬資產服務提供商。

106. 根據與點對點交易或點對點交易之某些類型的相關評估風險，各國可能會考慮並實施適當的選項，以在國家層級抵減這些風險。該等措施可能包括：
- a. 促進 P2P 活動，及／或義務實體和非義務實體間交叉的虛擬資產活動能見度的控制措施（這些控制措施可能包括相當於貨幣交易之虛擬資產報告或與此類移轉相關之記錄保存規則）；<sup>31</sup>
  - b. 對虛擬資產服務提供商和在虛擬資產領域營運之實體，進行持續性風險基礎之強化監理，特別聚焦於非託管錢包交易（例如，現場和非現場監理以確認虛擬資產服務提供商是否完整遵守有關這些交易的法規）；
  - c. 要求虛擬資產服務提供商，僅針對／從被認為可接受與其風險基礎方法相符之位址／來源促成交易；
  - d. 要求虛擬資產服務提供商僅針對／來自虛擬資產服務提供商或其他義務實體促成交易；
  - e. 對允許與非義務實體進行交易的虛擬資產服務提供商提出額外的防制洗錢／打擊資恐要求（例如，強化記錄保存之要求、加強客戶審查要求）；
  - f. 指引強調了虛擬資產服務提供商適用風險基礎方法來處理參與或促進點對點交易的客戶之重要性，並在適當的情況下得到風險評估、指標或分類刊物之支持；以及
  - g. 發佈公共指引和建議並進行資訊宣傳活動，以提高對點對點交易風險之認識（例如，通過評估特定使用者、觀察到的行為模式、當地和區域風險，以及來自監理機關或執法者之資訊，來核算點對點交易帶來之特定風險）。

---

<sup>31</sup> 此類之報告要求，類似於為解決此類交易之相關洗錢／資恐風險，FATF 對個人跨境實物大額現金移轉之報告要求（建議第 32 項）。

107. 除了點對點交易外，FATF 亦確立了其他可能需要採取進一步行動之潛在風險，包括虛擬資產服務提供商所在之司法管轄區之防制洗錢／打擊資恐框架薄弱或不存在（未正確實施防制洗錢／打擊資恐預防措施），以及具有去中心化治理架構之虛擬資產（可能不包括得以適用防制洗錢／打擊資恐措施的中介機構）。<sup>32</sup> 這些風險可能要求各國或虛擬資產服務提供商，去辨識虛擬資產服務提供商或國家之特定風險，並對與虛擬資產服務提供商以及缺乏基於這些風險的監管、監理或適當控制之國家有關之交易，實施特定的保護措施。如果大規模採用，這些風險會特別高。<sup>33</sup>

▪ *虛擬資產／虛擬資產服務提供商之禁止或限制*

108. 司法管轄區有權根據風險評估和國家監管背景，或為了支持本指引中未涉及之其他政策目標，酌予禁止或限制虛擬資產活動或虛擬資產服務提供商，以及由非義務實體開展之虛擬資產活動（例如，消費者和投資人保護、安全和穩健，或貨幣政策）。此可包括對活動的一般禁止或限制，或對被認為構成不可接受之洗錢與資恐風險等級之商品或服務的具體禁止或限制。該等禁止或限制應以法律或可執行的方式進行。

109. 在決定是否禁止或限制虛擬資產活動或虛擬資產服務提供商時，各國應瞭解與虛擬資產和虛擬資產服務提供商相關之洗錢與資恐風險。各國還應考慮此類禁令可能對其洗錢與資恐風險產生的影響。無論一個國家是否選擇禁止、限制或監管該部門之活動，額外的措施可能有助於抵減整體洗錢與資恐之風險。例如，如果一

---

<sup>32</sup> 更多資訊，請參閱 FATF 向 G20 提交之關於所謂穩定幣的報告。

<sup>33</sup> 有關與大規模採用以及與 P2P 相關的洗錢／資恐風險的更多資訊，請參閱第 40 段。

個國家禁止虛擬資產活動和虛擬資產服務提供商，抵減措施應包括辨識於該司法管轄區內非法經營之虛擬資產服務提供商（或其他可能從事虛擬資產活動之義務實體），並對此類實體實施相當以及具勸阻性的裁罰，並評估該服務將由位於國外的虛擬資產服務提供商在該國家提供之風險。根據國家的風險狀況，禁止／限制仍應要求該國採取延伸及執法行動，以及考慮到虛擬資產活動（例如，跨境虛擬資產支付或移轉）和虛擬資產服務提供商營運之跨境要素的風險抵減策略。各國應定期重新審視支持該決定之風險評估基礎，因為相關的洗錢與資恐風險和執行此類禁止／限制的能力可能會迅速演變。

110. 建議第 2 項。要求在防制洗錢／打擊資恐／反資助武擴政策方面進行國家層級的合作和協調，包括在虛擬資產服務提供商部門，因此在規範和監理所涵蓋之虛擬資產活動之背景下，建議間接適用於國家。各國應考慮建立機構間之工作小組或特別小組等機制，使政策制定者、監管者、監理者、金融情報中心和執法機關能夠相互合作以及與任何其他相關權責機關合作，以制定及實行有效之政策、法規和其他措施，以解決與所涵蓋之虛擬資產活動和虛擬資產服務提供商相關之洗錢與資恐／資助武擴風險。這應包括相關機關間之合作及協調，以確保防制洗錢／打擊資恐要求，與資料保護和隱私規則及其他類似規定（例如，資料安全／在地化）之兼容性。國家層級的合作和協調在虛擬資產之背景下尤為重要，部分原因是它們具有高度流動性和跨境性質，並且由於所涵蓋或受監管之虛擬資產活動的方式可能涉及多個監管機關（例如，監管金錢移轉、證券、商品或衍生性商品活動之權責機關）。此外，在進一步調查及利用與解決網路及／或虛擬資產生態系統相關之



各種機關間工具的脈絡下，與虛擬資產問題相關之國家層級的合作至關重要。

▪ *虛擬資產之處理：基於資金或價值的詞彙之解釋*

111. 為適用 FATF 建議，各國應考慮建議中所有基於資金或價值的詞彙，例如「財產」、「收益」、「資金」、「資金或其他資產」和其他「相應價值」，包括虛擬資產。特別是，各國應適用建議第3至第8項、第30項、第33項、第35項和第38項中之相關措施，所有這些措施都包含對上述基於資金或價值的詞彙或其他類似詞彙之引用，在虛擬資產之背景下以防止在洗錢、資恐和資助武擴中濫用虛擬資產，並針對涉及虛擬資產之所有犯罪所得採取行動。上述建議—其中一些最初看起來可能並不直接適用於虛擬資產服務提供商和類似之義務實體，但實際上適用於此領域—涉及洗錢犯罪、沒收和臨時措施、資恐犯罪、目標性金融制裁、非營利組織組織、執法權力、制裁以及國際合作。
112. 建議第3項。為了實行建議3，洗錢犯罪應擴展到直接代表犯罪所得之任何類型財產，無論其價值如何，包括在虛擬資產之情況下。當證明財產是犯罪所得時，不需要有人因前置犯罪而被定罪，包括在與虛擬資產相關之所得的情況下。因此，各國應將其適用之洗錢犯罪措施，擴大到涉及虛擬資產之犯罪所得。
113. 建議第4項。同樣地，關於「(a) 洗錢的財產，(b) 來自於洗錢或前置犯罪之收益，或使用於或擬用於洗錢或前置犯罪之工具，(c) 來自於資助恐怖主義、恐怖行動或恐怖組織之所得財產，或用於、或擬或分配用於資助恐怖主義、恐怖行動或恐怖組織之財產，(d) 或具有相應價值之財產」的沒收和臨時措施，也適用於虛擬資產。

114. 至於適用於法定貨幣和貨物之沒收或臨時措施，執法機關應能夠在有理由確認或已確認資產源自於犯罪活動時，請求暫時凍結資產。為延長凍結期限或要求沒收資產，執法機關應取得法院命令。
115. 建議第 5 項。同樣地，建議第 5 項中描述的資恐犯罪應擴張到「任何資金或其他資產」，包括來自合法或非法來源之虛擬資產（見建議第 5 項注釋）。
116. 建議第 6 項。各國亦應毫不遲延地凍結經指名之個人或團體的資金或其他資產一包括虛擬資產，並確保沒有資金或其他資產一包括虛擬資產，被提供給或係為與恐怖主義和資恐相關之目標性金融制裁相關之經指名之個人或團體的利益。
117. 建議第 7 項。在與武擴有關的目標性金融制裁之背景下，各國應毫不遲延地凍結經指名之個人或團體的資金或其他資產一包括虛擬資產，並確保沒有資金或其他資產一包括虛擬資產可供或係為經指名之個人或團體的利益。
118. 建議第 8 項。各國亦應根據風險基礎方法採取措施，保護非營利組織免受資恐濫用，如建議第 8 項中所述，包括當隱蔽移轉資金給恐怖組織涉及虛擬資產時（參建議第 8 項 (c)）。
119. 建議第 30 項。在本指引第 111 段所述之所有基於資金或價值的詞彙之適用範圍內，建議第 30 項適用於所涵蓋之虛擬資產活動和虛擬資產服務提供商。與其他類型的財產或犯罪所得一樣，各國應確保權責機關有責任迅速辨識、追蹤及發動行動，以凍結和扣押正在或可能會被沒收或疑似為犯罪所得之虛擬資產相關財產。各國皆應實施建議第 30 項，無論司法管轄區在其國家法律框架中如何對虛擬資產進行分類（即，無論根據司法管轄區的財產法如何對虛擬資產進行法律分類）。

120. 建議第 33 項。各國保存之統計數據應包括權責機關接收和發布之疑似洗錢或資恐交易報告之數據，以及權責機關凍結、扣押和沒收的財產之數據。因此，各國亦應在虛擬資產服務提供商和虛擬資產活動的背景下實施建議第 33 項，並維護權責機關從虛擬資產服務提供商，和其他提交與虛擬資產服務提供商、虛擬資產或虛擬資產活動相關之疑似洗錢或資恐交易報告之義務實體（例如銀行）取得之疑似洗錢或資恐交易報告的統計數據。與包含基於資金或價值之詞彙之其他建議（例如，建議第 3 項至第 8 項、第 30 項、第 35 項和第 38 項）相同，無論該司法管轄區如何根據其國家法律框架之財產法對虛擬資產進行分類，各國亦應保留有關權責機關凍結、扣押或沒收的任何虛擬資產之統計數據。此外，各國應考慮更新其疑似洗錢或資恐交易報告和相關統計數據，以納入促進調查之虛擬資產相關指標以及財務分析。
121. 建議第 35 項指示各國採取一系列有效、相應及具勸阻性的裁罰（刑事、民事或行政）來規範建議第 6 項和第 8 項至第 23 項所涵蓋之未遵守所適用之防制洗錢／打擊資恐要求之自然人或法人。根據建議第 15 項注釋第 6 段之要求，各國也應採取類似的裁罰措施來規範不遵守其防制洗錢／打擊資恐要求之虛擬資產服務提供商（以及其他從事虛擬資產活動的義務實體）。與金融機構和指定之非金融事業或人員以及其他自然人或法人一樣，此類裁罰不僅應適用於虛擬資產服務提供商，如有適用者，還應適用於其董事和高級管理人員。
122. 建議第 38 項亦包含基於資金或價值的詞彙並適用於虛擬資產之背景，但在關於國際合作的第 3.1.8 小節和建議第 37 項至第 40 項之實踐中，有更詳細的闡述，如建議第 15 項注釋第 8 段所述。

▪ **執照或註冊**

123. 各國應指定一個或多個負責虛擬資產服務提供商取得執照及／或註冊之機關。

124. FATF 國際標準給予各國就虛擬資產服務提供商取得執照或註冊之彈性。許多國家正面臨著是否將虛擬資產服務提供商納入現有之執照或註冊制度或創建新制度的抉擇。使用現有制度可能會為各國提供更快的實施途徑，並將利用遵法團體中如何運作相關流程之既有知識的優勢。各國可能會發現使用現有的執照／註冊系統，例如金錢或價值移轉服務之系統，更為容易，前提是其現有制度是可運作的且適用於虛擬資產服務提供商。然而，一個新的制度可能是專門為虛擬資產服務提供商建立的，且不包括可能不適用於虛擬資產服務提供商之舊式觀點。例如，該制度可以包括更多聚焦於防制洗錢／打擊資恐分析中之技術能力，以及與傳統金融服務部門不同之虛擬資產部門的風險和抵減措施。提前確認現有系統能夠充分解決虛擬資產服務提供商之風險是必要的。如果各國明確為虛擬資產和虛擬資產服務提供商制定了新的法律法規，則新的執照／註冊制度可能更有實益。各司法管轄區應根據對不同類型的虛擬資產和虛擬資產服務提供商活動以及相關的洗錢與資恐風險的評估，確立要求之性質和寬嚴標準以及他們選擇之制度類型。

▪ **哪些虛擬資產服務提供商應取得執照或註冊？**

125. 按照建議第 15 項注釋第 3 段，至少應要求虛擬資產服務提供商於其設立之司法管轄區取得執照或註冊。設立法人<sup>34</sup>包括公司的成立，或在國內用於使法人實體之存續正規化的任何其他機制，例

---

<sup>34</sup> 請參考建議第 24 項注釋 40。

如在公共登記處、商業登記處或公司或法人實體的任何同等之登記處進行登記；公證人或任何其他公職人員之認證；提交公司章程；編配公司稅號等。

126. 在虛擬資產服務提供商是自然人之情況下，應要求其在其營業所在地之司法管轄區取得執照或註冊—該決定可能包括若干供各國考慮之因素。自然人之營業地可以進行業務或保存業務帳簿和記錄的主要地點以及自然人的居住地點為特徵（亦即，自然人實際存在、坐落或居住之地點）。例如，當自然人從其居住地進行業務，或者無法辨識營業地時，可以將其主要居住地視為其營業地。營業地點作為一個潛在之考慮因素，還可包括事業伺服器之位置。
127. 司法管轄區還可能要求在其司法管轄區內向客戶提供商品及／或服務，或在其管轄範圍內開展業務之虛擬資產服務提供商，取得執照或在該司法管轄區內註冊。因此，當地司法管轄區可能要求其服務可由居住在其司法管轄區內之人接觸或取得，或者可能要求在其司法管轄區內設有員工或管理人員之虛擬資產服務提供商註冊或取得執照。雖然 FATF 國際標準不要求涵蓋這些實體，但司法管轄區可能會發現它有助於抵減風險，特別是考慮到虛擬資產固有之跨境可得性。如有疑慮，司法管轄區可能會認為更廣泛之涵蓋是較安全之做法，因為虛擬資產將在可取得該虛擬資產之任何司法管轄區引入其所帶來之任何風險，無論其成立地點為何。
128. 為了辨識那些在司法管轄區內向客戶提供商品及／或服務，但未在該司法管轄區內設立之虛擬資產服務提供商，監理機關可以使用一組相關標準。這可能包括辦公室和伺服器之位置（包括面對客戶之營運，如電話服務中心）、針對特定國家／市場之促銷資訊、虛擬資產服務提供商網站及／或行動應用程式上之語言、虛

擬資產服務提供商是否在一國家擁有分銷網路（例如，如果它已指定中介尋找客戶或親自拜訪居住在該國的客戶），以及要求客戶提供的特定資訊，以顯示目標國家。

▪ *如何辨識取得執照或註冊之虛擬資產服務提供商*

129. 各國應採取行動以辨識在沒有所需執照或註冊之情況下開展虛擬資產活動或營運之自然人或法人，並實施適當的裁罰，包括在可能從事虛擬資產活動或營運的傳統有義務的實體之背景下（例如，對其客戶提供虛擬資產之銀行）。國家機關應有機制來監控虛擬資產服務提供商部門，以及可能從事所涵蓋之虛擬資產活動或營運，或提供所涵蓋之虛擬資產商品或服務的其他有義務的實體，並確保有適當的管道來通知虛擬資產服務提供商和其他有義務的實體，他們向有關機關登記或申請執照之義務。各國還應指定一個機關負責辨識和裁罰未取得執照或未註冊之虛擬資產服務提供商（以及從事虛擬資產活動之其他義務實體）。如第 108 至 109 段所述，即使是選擇在其司法管轄區內禁止虛擬資產活動或虛擬資產服務提供商之國家，也應依據建議第 15 項之要求，建立工具和權責機關來辨識不遵守其法律義務之自然人或法人，並對其採取行動。
130. 為了辨識沒有執照及／或註冊而營運之人，各國應考慮其可能擁有之工具和資源的範圍，以調查是否存有未取得執照或未經註冊的虛擬資產服務提供商。例如，各國可能會考慮：
- a. 區塊鏈或分散式帳簿分析工具，以及其他調查工具或功能；
  - b. 網頁截取及開放原始碼資訊，以辨識未經註冊或未取得執照之實體的任何廣告、促銷通訊或附屬計畫或其他可能的業務招攬；
  - c. 來自於公眾、有義務的實體和產業界的關於某些可能未取得執照或未註冊之業務之資訊（包括透過建立收受公眾反饋之管道）；

- d. 金融情報中心或來自報告機構的其他資訊，例如疑似洗錢或資恐交易報告或調查線索，這些資訊可能會顯示未取得執照或未經註冊的自然人或法人虛擬資產服務提供商之存在；
  - e. 非公開可得資訊，例如該實體之前是否曾申請執照或註冊，或者是否已撤銷其執照或註冊；及
  - f. 執法 and 情報報告，包括來自國際合作的資訊（例如，來自國際同業之情報）。
131. 取得執照或註冊為虛擬資產服務提供商者應符合相關權責機關規範之適當取得執照及註冊標準。該等標準應使國家監理機關相信相關虛擬資產服務提供商將能夠遵守其防制洗錢／打擊資恐義務。為此，該標準應包括在營業前證明其防制洗錢／打擊資恐計畫之義務，包括政策、程序及組織，並考量虛擬資產服務提供商已實施或一旦營業即可實施活動之特徵（即虛擬資產及交易之類型、目標客戶、銷售管道）。此可能包括對法遵人員之能力及可信度之判斷。在取得執照或註冊過程中有時間確保風險控管在營業前到位，則對此等標準之評估會更加有效。
132. 當一司法管轄區為虛擬資產服務提供商建立其取得執照或註冊計畫，大量的虛擬資產服務提供商可能同時尋求取得執照或註冊。為使流程順利進行，有關機關可能考慮如何確保有足夠資源可使用，並在其方法中建立足夠之靈活性，以使對於提出之請求進行優先排序。各國可能會考慮一系列因素以對於申請進行優先排序，但應根據監理機關之判斷及能力以進行排序。
133. 於取得執照或註冊程序中，權責機關應採取必要法律或監管措施以防止罪犯或其同夥持有或作為虛擬資產服務提供商之重要或有控制權益之實質接收人，或於其中擔任管理職責。此等措施應包

括要求虛擬資產服務提供商就股東、業務營運及結構之實質變動取得權責機關之事先核准。

134. 以風險為基礎，權責機關亦得對尋求取得執照或註冊之虛擬資產服務提供商施加條件，使其得以有效監督虛擬資產服務提供商。該等條件得可能依據虛擬資產服務提供商活動之規模及性質，包含要求常駐執行董事、實質管理、特定財務要求、要求虛擬資產服務提供商於行銷素材、網站及行動應用程式揭露其持有之註冊／執照及／或要求虛擬資產服務提供商確保權責機關得取得有關委外職能之資料及任何受託機構之相關營業處所。
135. 如同其他受 FATF 國際標準規範之實體，虛擬資產服務提供商應於設計或建構之新商品或服務上路前遵循防制洗錢／打擊資恐規範，因其後再施行將會相對困難。因此，於取得執照及註冊階段謹慎評估風險並完善地衡量抵減措施相當重要。當已取得執照及註冊時，應維持於商品及服務建立之防制洗錢／打擊資恐抵減措施，且其應為監理之標的。
136. 重要的是，司法管轄區得考慮透過公開交流及活動（例如，虛擬資產生態系統之教育活動、論壇或「辦公時間」）強調對於虛擬資產服務提供商之防制洗錢／打擊資恐要求。透過諮詢或指引提供有關法律架構之確定性為另一關鍵措施以支持法遵文化。各國亦得考慮宣傳針對未註冊或未取得執照虛擬資產服務提供商之執法行動之激勵效果。
137. 此外，各國亦得依據其判斷，考慮指定所有來自未有效實施取得執照或註冊要求國家之虛擬資產服務提供商為高風險，因此，虛擬資產服務提供商與來自未具備有效執照制度之國家之交易對手進行交易將被監理機關指定為高風險活動，並可能產生額外之申



報要求（另請參第 III 部分建議第 10 項中關於加強客戶審查(EDD)之資訊以及第三部分及第四部分建議第 16 項對於虛擬資產服務提供商交易對手之盡職調查）。

138. 所有司法管轄區應鼓勵遵循所有司法管轄區適用法律及法規要求之文化。除防制洗錢／打擊資恐之外，此可能涉及一系列政策目標，包含投資者及消費者保護、市場誠信、審慎要求及／或國家及經濟利益相關之政策目標。為此，某些司法管轄區可能會決定透過不允許虛擬資產服務提供商自審慎或其他與防制洗錢／打擊資恐相關授權不同之機構獲得執照以強調此目標。司法管轄區亦應確保虛擬資產服務提供商及權責機關為其防制洗錢／打擊資恐法遵職責投入足夠資源，以應對預期之用戶及交易量。
139. 如前所述，重要的是，穩定幣之洗錢與資恐風險，特別是那些可能被大規模採用且可用於點對點交易之風險，必須以持續及前瞻性之方式進行分析，並在此類交易開始之前被抵減。如果虛擬資產服務提供商或其他有義務之實體提議創造或使用穩定幣，則對洗錢與資恐風險之評估和風險抵減應適當地構成取得執照或註冊程序之一部分。對於穩定幣不涉及符合虛擬資產服務提供商或其他有義務實體資格之實體之主張，監理機關應特別謹慎。在發行前階段尤其如此，因為創造和開發資產之程序不太可能實現自動化。在所有虛擬資產服務提供商之取得執照或註冊程序及風險評估中，應將大規模採用之可能性作為值得考慮之重要因素。一般來說，虛擬資產服務提供商及發行或參與穩定幣之有義務的實體於取得執照或註冊程序應與虛擬資產之一般情況相似。

- **與國內及國際夥伴之合作**

140. 參與虛擬資產服務提供商之規範及取得執照或註冊之各個國家權責機關間之協調很重要，如之前在建議第 2 項中所述，因為各權責機關可能掌握與未經授權提供者或活動有關之資訊。此對於有多個不同虛擬資產服務提供商取得執照或註冊計畫而非一個中央制度之國家的情況尤為重要。
141. 取得執照及註冊過程中之國際合作亦為重要。權責機關亦可以通知其對等單位，該先前註冊或取得執照之虛擬資產服務提供商正於其對等單位之司法管轄區內營運。各國應建立適當之資訊共享管道，以支持識別及裁罰未經取得執照或未經註冊之虛擬資產服務提供商。權責機關亦應考慮虛擬資產服務提供商監理機關間之資訊共享及合作原則，以取得有關如何於取得執照或註冊過程中與對等單位合作之更多指引（參第四部分）。

▪ **監理或監督**

142. 建議第 26 項及第 27 項。如下所討論，建議第 15 項要求各國使虛擬資產服務提供商接受有效之防制洗錢／打擊資恐監理或監控系統。如建議第 26 項和第 27 項之建議第 15 項注釋第 5 段同樣要求各國確保虛擬資產服務提供商也受到對防制洗錢／打擊資恐的充分監理、監理及監督，並根據其洗錢與資恐風險有效實施 FATF 建議。虛擬資產服務提供商應受制於有效之系統以監理及確保遵守國家防制洗錢／打擊資恐要求。虛擬資產服務提供商應受權責機關而非自律團體之以風險為本之監督或監控。雖然自律團體不應擔任監管者，但自律團體及同業團體得協助監理機關促進與虛擬資產服務提供商之聯繫、資訊共享及宣導。監理機關應有適足之權力以監理或監督並確保虛擬資產服務提供商（以及從事虛擬資產活動之其他有義務實體）遵守打擊洗錢與資恐之要求，包括

進行檢查、查閱帳簿及記錄、強制出具資訊，及施加一系列紀律及經濟裁罰，包括於適用之情況下以撤銷、限制或暫停虛擬資產服務提供商之取得執照或註冊之權力。各國應使其外國夥伴明確知悉虛擬資產服務提供商之監理機關，以開展最廣泛之國際合作。

143. 鑒於虛擬資產服務提供商之活動及服務提供之跨境性質，以及將特定虛擬資產服務提供商與單一司法管轄區聯結之潛在挑戰，相關監理機關間之國際合作亦特別重要，正如建議第 15 項注釋第 8 段所強調（另參第 257-260 段）。司法管轄區亦得參考其他國際標準制定機構之相關工作，以獲得此方面之有效指引，例如國際證監會組織及巴塞爾銀行監理委員會<sup>35</sup>。

144. 正如本指引第 227-228 段所詳盡討論，當指定之非金融事業或人員從事虛擬資產服務提供商活動時，各國應使該實體遵守 FATF 建議規定之所有虛擬資產服務提供商相關措施，包括關於監理或監督<sup>36</sup>。

#### ▪ 預防措施

145. 建議第 15 項注釋第 7 段明確指出，建議第 10 項至第 21 項中包含之所有預防措施適用於虛擬資產及虛擬資產金融活動中之國家及義務實體。但是，建議第 9、22 及 23 項於該領域亦具有間接適用性，下文亦將對此進行討論。因此，以下子段落提供了逐條建議之解釋，以幫助各國進一步考慮如何於虛擬資產之脈絡下實施

---

<sup>35</sup> 參見，例如，委員會之銀行有效監理之核心原則之第 3 原則（合作及協調）及第 13 原則（母國 - 駐在國關係）：[www.bis.org/publ/bcbs230.pdf](http://www.bis.org/publ/bcbs230.pdf)。

<sup>36</sup> 司法管轄區可能會稱或稱虛擬資產服務提供商為「金融機構」或「指定之非金融事業或人員」。惟無論國家／地區選擇如何稱呼虛擬資產服務提供商，根據虛擬資產服務提供商從事之金融活動類型及提供之金融服務類型，它們仍然受到與金融機構相同等級之監理及監督。

預防措施。相關地，第四部分提供了針對虛擬資產服務提供商和其他從事虛擬資產活動之義務實體之指引，說明他們應如何實施下文所述之預防措施以及 FATF 建議中之其他防制洗錢／打擊資恐措施。

146. 一般而言，建議第 10 項至第 21 項中規定之預防措施以與金融機構相同之方式適用於虛擬資產服務提供商，但有兩項特定條件。首先，虛擬資產服務提供商需要進行客戶審查之臨時性交易指定門檻為 1000 美元／歐元（而非 15000 美元／歐元）。其次，建議第 16 項中規定之電匯規則修改適用於虛擬資產服務提供商和虛擬資產移轉（「轉帳規則」）。此將於下文更詳細地說明。

#### ▪ 金融機構保密法律

147. 建議第 9 項旨在確保金融機構保密法律不會阻礙 FATF 建議之實施。與金融機構相同，儘管建議第 9 項未明確包含或提及虛擬資產服務提供商，但各國應類似地確保保密法律不會阻礙 FATF 建議實施於虛擬資產服務提供商。

#### ▪ 客戶審查

148. 建議第 10 項。各國及義務實體應設計客戶審查流程以滿足 FATF 國際標準及國家法律要求。客戶審查流程應幫助虛擬資產服務提供商（以及從事虛擬資產活動之其他有義務的實體）評估與涵蓋之虛擬資產活動或業務關係或高於門檻之臨時性交易相關之洗錢與資恐風險。初次客戶審查包括識別客戶，並於適用之情況下識別客戶之實質接收人，並於風險基礎上根據可靠及獨立之資訊、資料或文件，至少於適用法律或監管要求之範圍內驗證客戶之身份。客戶審查流程還包括瞭解業務關係之目的及預期性質（如有相關），並於高風險之情況下取得更多資訊。

149. 實務上，虛擬資產服務提供商得開設及保留帳戶（即建立客戶關係），並且在為客戶或代表客戶提供服務或參與被涵蓋之虛擬資產活動時應收集相關之客戶審查資訊。但在虛擬資產服務提供商進行臨時性交易之情況下，依據建議第 15 項注釋第 7 (a) 段，虛擬資產服務提供商需要進行客戶審查之指定門檻為 1000 美元／1000 歐元。<sup>37</sup>
150. 無論關係或交易的性質如何，各國應確保虛擬資產服務提供商制定有效程序，以風險為基礎識別及驗證客戶之身份，包括在與該客戶建立業務關係時；在虛擬資產服務提供商可能懷疑有洗錢與資恐之情況下，無論是否有任何門檻豁免；以及他們懷疑先前取得之身份證明資料之真實性或充分性時。
151. 有些司法管轄區可能會將使用虛擬資產自助服務（有些人可能將其稱為虛擬資產 ATM，如第 71 段所述關於虛擬資產服務及商業模式）視為一種臨時性交易，由自助服務提供者或所有者／營運商／和使用自助服務之客戶以一次性方式進行交易。其他司法管轄區可能不會認為此類交易是臨時性，從而產生客戶審查義務之後果。
152. 如上述討論，虛擬資產具有特定潛在之洗錢與資恐風險，包含其全球範圍、快速結算能力、得進行點對點交易之能力，及可能增加匿名性並混淆交易流程及交易對手。鑒於此等特徵，各國可能因此比建議第 10 項所要求的更進一步，要求對虛擬資產服務提供商（以及其他義務實體，例如從事虛擬資產活動之銀行）進行之虛擬資產移轉或交易進行客戶審查，包括「臨時性交易」，門檻低於 1000 美元／歐元，並符合其國家法律框架。此一方法與建議

---

<sup>37</sup> 基於與虛擬資產活動相關之洗錢／資恐風險及跨境性質，FAFT 同意降低虛擬資產相關交易之門檻金額至 1000 美元／歐元。

第 1 項中規定之風險基礎方法一致，前提是係基於國家風險評估的基礎下是具有正當性的（例如，透過識別高風險）。此外，司法管轄區於建立其監理及監理制度時，應考量虛擬資產服務提供商如何決定及確保交易實際上係以一次性或臨時性為基礎進行而非持續性基礎（即非臨時性）。於決定對臨時性交易採取何等措施時，各國應考量虛擬資產服務提供商於其司法管轄區所提供之商品及服務。各國得要求虛擬資產服務提供商辨識低風險、一次性虛擬資產移轉，其中虛擬資產服務提供商有能力接受剩餘風險，以通知各國處理虛擬資產領域之臨時性交易。

153. 如建議第 10 項注釋所述，於某些情況下，洗錢與資恐風險較高，且必須採取加強客戶審查措施。例如，於虛擬資產相關活動及虛擬資產服務提供商之脈絡下，各國應考慮量國家或地區之特定風險因素。位於特定國家之虛擬資產服務提供商或自或與特定國家相關之虛擬資產移轉對洗錢與資恐存在潛在之高風險（參見建議第 10 項注釋第 15(b) 段）。

#### 加強及簡化之客戶審查

154. 當未有普遍認可之定義或方法以確定虛擬資產服務提供商營運所在地之司法管轄區或虛擬資產交易可能來自之司法管轄區是否代表洗錢與資恐之高風險時，考量特定國家風險以及其他風險因素，為進一步確定潛在之洗錢與資恐風險提供有用之資訊。高風險指標包括：

- a. 透過可靠來源<sup>38</sup> 辨識為恐怖主義活動提供資金或支持之國家或

---

<sup>38</sup> 「可靠來源」係指由信譽良好且得到普遍認可之國際組織及其他使此等資訊公開及得被廣泛取得之組織所產出之資訊。除了 FATF 及區域性防制洗錢組織外，此類來源可能包括但不限於超國家或國際組織，例如國際貨幣基金、世界銀行及艾格蒙聯盟金融情報中心。

- 地理區域，或指名恐怖組織於其中活動之國家或地區；
- b. 透過可靠來源辨識存在重大等級之組織犯罪、貪污或其他犯罪活動之國家，包括為非法毒品、人口販運、走私及非法賭博之來源國家或轉運國家；
  - c. 受聯合國等國際組織頒布之制裁、禁運或類似措施之國家；及
  - d. 透過可靠來源辨識治理、執法及監理制度薄弱之國家，包括 FATF 聲明中確定之防制洗錢／打及資恐制度薄弱之國家，特別是對於虛擬資產服務提供商，於此情形虛擬資產服務提供商及其他義務實體應特別注意業務關係及交易。
155. 各國應亦考量與虛擬資產商品、服務、交易或交付管道有關之風險因素，包含該活動是否包含假名或「匿名交易」、「非面對面關係或交易」及／或「自不知名或無關聯之第三人收受之款項(參建議第 10 項注釋第 15 (c) 段及本指引第 31 段所列之高風險及低風險案例)。幾乎所有虛擬資產都包含一個或多個之此等特性或特徵之事實可能導致各國根據虛擬資產商品、服務、交易或交付機制之本質，決定該領域之活動本質上具有高風險。
156. 在此等及其他情況下，得抵減與上述因素相關之潛在高风险之加強客戶審查措施包括：
- a. 以第三人資料庫或其他可靠來源中之資訊辨識自客戶收受之身份資訊，例如國民身份證號碼；
  - b. 可能追蹤客戶之 IP 位址；
  - c. 分析商品之使用，例如區塊鏈分析<sup>39</sup>；及

---

<sup>39</sup> 至今，FATF 未知悉有任何經過技術驗證之方法得於所有情況下精確、準確地識別管理或擁有非託管錢包之人。各國應意識此點，並注意使用此工具之分析結果應僅被視為參考資訊。

d. 於網路搜索與客戶交易概況一致之活動資訊，若資料蒐集符合國家隱私權法律。<sup>40</sup>

157. 各國亦應考量建議第 10 項注釋第 20 段中詳述之加強客戶審查措施，包括取得有關客戶及業務關係之預期性質之額外資訊，取得有關客戶資金來源之資訊，取得有關預期或已執行交易之原因之資訊，以及加強對關係及交易之監控。此外，各國應考量對從事非面對面（例如手機服務）或與虛擬資產交易具有可比性之以法定貨幣計價活動之金融機構所需之措施，以評估其風險並相應地制定抵減控制措施。
158. 各國亦得鼓勵其虛擬資產服務提供商蒐集有關高風險客及交易之額外資訊，以辨識及避免參與被禁止之活動，並以風險基礎方法之方式採取後續行動。此額外資訊可能包括：
- a. 交易或付款之目的；
  - b. 該項目之性質、最終使用或終端使用者之詳細資訊；
  - c. 資金所有權之證明；
  - d. 交易各方及其相互間之關係
  - e. 財富及／或資金之來源；
  - f. 交易對手之身分及實質受益權；及
  - g. 出口控制資訊，例如出口控制之副本或其他國家出口控制機關核發之執照，以及終端客戶之證明。
159. 各國應透過分享告知虛擬資產服務提供商被禁止活動之態樣，並應視個案支持調查或中斷活動，且不破壞正在進行之調查。如果虛擬資產服務提供商懷疑客戶（可能不知情）從事被禁止活動，

---

<sup>40</sup> 請參閱 2015 年虛擬貨幣指引第 44 段及 2013 年 6 月新型支付商品及服務風險基礎方法指引第 66 段。



它們應該採取進一步之客戶審查措施，不得提示客戶、尋求抵減風險、於交易被確定為被禁止時採取適當之行動，包括拒絕或阻止交易活動並於需要時提交疑似洗錢或資恐交易報告。

#### 確保客戶審查資訊及時更新

160. 此外，各國應要求虛擬資產服務提供商及其他參與或提供虛擬資產商品及服務之義務實體，透過對現有記錄進行審查，特別是高風險客戶或虛擬資產商品或服務類別，及進行持續性盡職調查（參第四部分對於虛擬資產服務提供商及其他義務實體之持續性盡職調及監控義務之更多討論），於客戶審查流程下保持文件、資料或蒐集資訊之及時更新及關聯性。此類交易及記錄之審查對於有效監理至關重要，且為傳輸所需之相關客戶資訊以符合「轉帳規則」之重要資訊來源（參建議第 16 項）。

#### ▪ 紀錄保存

161. 建議第 11 項要求各國確保虛擬資產服務提供商保存所有交易及客戶審查措施記錄至少五年，以便可以重建個體交易並將相關要素迅速提供給權責機關。各國應要求虛擬資產服務提供商和其他從事虛擬資產活動之義務實體保存交易記錄及透過客戶審查措施獲得之資訊，包括：例如與識別相關當事人有關之資訊、公鑰（或等同的識別資訊者）、位址或涉及之帳戶（或等同的識別資訊者）、交易之性質及日期，以及移轉之金額。如果機構能夠充分識別其客戶，則特定 虛擬資產之區塊鏈或其他相關分佈式帳本之公共資訊可為記錄保存提供初始基礎。然而，僅依賴區塊鏈或虛擬資產下之其他類型分佈式帳本進行記錄並不足以遵守建議第 11 項。

162. 例如，區塊鏈或其他類型之分佈式帳本上可提供之資訊可能使相關機關得將交易追溯至錢包位址，儘管它可能不容易將錢包位址

與個人姓名連結。錢包位址包含一個使用者代碼，該代碼以獨特之數字及字母串之形式於分佈式帳本中作為電子簽名（即公鑰）。然而，需要額外資訊始得將位址與真實之人或自然人相連結。

▪ **重要政治性職務人士**

163. 建議第 12 項要求各國實施措施要求義務實體，例如虛擬資產服務提供商建置適當風險管理系統以決定客戶或實質接收人是否為重要政治性職務人士或相關或連結至外國重要政治性職務人士<sup>41</sup>，以及，如是，於執行一般客戶審查（如第 10 項建議定義）外，採取額外措施以決定其是否或何時與其建立業務關係，包含辨識相關資金來源（如有相關）

▪ **通匯銀行業務及其他類似業務，金融機構應：**

164. 建議第 13 項規定各國於從事跨境通匯業務時，應要求金融機構除執行正常之客戶審查措施外，亦應採取特定措施。建議第 13 條注釋規定，對於通匯銀行及其他類似之跨境業務，金融機構除執行正常之客戶審查措施外，亦應採用建議第 13 項之標準 (a) 至 (e)。「其他類似業務」包括當金錢或價值移轉服務業者作為其他金錢或價值移轉服務業者之中介或當金錢或價值移轉服務業者透過另一個銀行之金錢或價值移轉服務業客戶帳戶取得銀行或類似服務時，該金錢或價值移轉服務業。（參見 2016 年 FATF 通匯銀行業務指引）。

165. 建議第 13 項適用於虛擬資產服務提供商。於本指引，「通匯業務」為由一個虛擬資產服務提供商向另一個虛擬資產服務提供商或金

---

41 「外國重要政治性職務人士」為目前或曾經被外國委託擔任重要公共職能之個人，例如國家元首或政府領導人、資深政治家、資深政府、司法或軍事官員、國家企業之資深管理人員以及重要之政黨官員 (FATF 詞彙表)。

融機構提供虛擬資產服務提供商服務。與其銀行業相同，此種通匯業務之特徵為具持續、重複性質。<sup>42</sup> 此業務亦得包括，例如，一個虛擬資產服務提供商將其平台功能白標為另一個虛擬資產服務提供商，並提供巢狀服務（向較小的虛擬資產服務提供商提供帳戶以取得流動性及交易配對）。

166. 通匯業務可能涉及廣泛範圍之服務，故非皆具備相同等級之洗錢與資恐風險。如果虛擬資產服務提供商目前或將來可能之業務關係具有類似於跨境通匯銀行業務之特徵，特別是虛擬資產服務提供商於另一個虛擬資產服務提供商持有帳戶之巢狀關係，各國應針對發展此等關係之虛擬資產服務提供商以及其他在虛擬資產領域營運之義務實體）提供實施建議第 13 項之預防措施（建議第 13 項包括抵減跨境通匯業務之洗錢與資恐風險之措施。於將其適用於虛擬資產服務提供商時，各國應要求向另一個虛擬資產服務提供商或金融機構提供服務作為跨境通匯業務一部分之虛擬資產服務提供商：

- a. 蒐集關於其擬建立跨境通匯業務關係之其他虛擬資產服務提供商或金融機構之充足資訊，以充分瞭解其他虛擬資產服務提供商或金融機構之業務性質及其防制洗錢／打擊資恐之風險控制框架，包括：其他虛擬資產服務提供商或金融機構打算透過跨境通匯業務關係向何種類型之客戶提供服務；
- b. 蒐集充足資訊並自公開來源確定其他虛擬資產服務提供商或金融機構之聲譽、其所受監理之品質以及它是否已受到洗錢與資恐調查或監理監理行動；

---

<sup>42</sup> 於非客戶關係之脈絡下，一次性交易或單純訊息傳遞關係並非通匯業務。  
(FATF 通匯銀行指引第 13 段)。

- c. 辨識其他虛擬資產服務提供商或金融機構之防制洗錢／打擊資恐控制措施；
  - d. 於建立跨境通匯業務關係前取得高階管理層之許可；及
  - e. 對於其他虛擬資產服務提供商或金融機構之客戶可以直接使用並代表其客戶進行業務交易之帳戶或託管錢包，確信其他虛擬資產服務提供商或金融機構已對此類客戶進行客戶審查並得應要求，於兩個司法管轄區允許之隱私權及資料保護法規允許範圍內提供相關之客戶審查資訊。
167. 為適用該等措施，從事跨境通匯業務之虛擬資產服務提供商應能夠瞭解洗錢與資恐風險並適用適當的以風險為本之控制措施。與不存在或對虛擬資產服務提供商之防制洗錢／打擊資恐規範或監理薄弱之司法管轄區內之虛擬資產服務提供商有跨境通匯業務關係將可能呈現更高的防制洗錢／打擊資恐風險。同樣的，如通匯業務包含提供服務之安排，且這些安排掩蓋了背後客戶之存在及其交易之性質，或者涉及大量交易及第三人支付之執行，也可能帶來更高之洗錢與資恐風險。在這種情況下，於清楚瞭解其進行通匯業務之虛擬資產服務提供商提供之背後客戶屬性之情況下，執行重點交易監控將會是適當抵減風險之例子。
168. 當建議第 13 項並未適用在國內相對應之業務時，虛擬資產服務提供商於其自身或代表其進行虛擬資產活動時，應採取建議第 10 項下對於為國內虛擬資產服務提供商之相對人進行以風險為基礎之客戶審查。作為瞭解該業務關係之性質及目的之一部分，該等以風險為基礎之盡職調查，包含就相對人之防制洗錢／打擊資恐控制之存在及品質，以及透過該關係提供背後客戶之服務之類似考量。與跨境通匯業務之主要不同在於虛擬資產服務提供商將可能

可以假設其他於相同司法管轄區受監理之虛擬資產服務提供商係受相同等級之規範及監理。考量虛擬資產及虛擬資產服務提供商之性質，各國得建議虛擬資產服務提供商記錄其如何辨識其進行通匯業務之虛擬資產服務提供商為國內或跨境，因為如同銀行，辨識通匯業務之相對人是否為國內或跨境並非易事。

169. 謹釐清，為遵循建議第 16 項所為之相對人盡職調查與適用於跨境通匯業務之義務並不相同。不同於銀行部門，於虛擬資產服務提供商間為自己或代表其他個人移轉虛擬資產是有可能的，即使是不存在通匯業務關係或任何其他關係。於該情況下，涉及該移轉之虛擬資產服務提供商可能進行相對人盡職調查，以確保其等得以遵循轉帳規則及採行措施以抵減洗錢與資恐風險。兩個虛擬資產服務提供商間存在涉及虛擬資產之通匯業務關係仍可能部分或全部符合相對人盡職調查之要求。如何於轉帳規則之脈絡下執行虛擬資產服務提供商交易對手之盡職調查之更多資訊可參見建議第 16 項。

▪ **金錢或價值移轉服務**

170. 建議第 14 項指示各國就於該國提供金錢或價值移轉服務之自然人或法人應註冊或取得執照，並確保其等遵循相關防制洗錢／打擊資恐措施。如 2015 年虛擬貨幣指引，其包含使在該國營運之金錢或價值移轉服務者受監控以遵循註冊或取得執照及其他應適用之防制洗錢／打擊資恐措施。建議第 15 項之註冊及取得執照之要求仍適用於所有虛擬資產服務提供商，即便是該等參與金錢或價值移轉服務活動者（例如，於司法管轄區提供虛擬及法定貨幣間可轉換虛擬資產交換服務業務之國內實體）。

171. 建議第 14 項亦適用於金錢或價值移轉服務之代理人。亦即任何代表虛擬資產服務提供商進行金錢或價值移轉服務活動之自然人或法人，不論係依契約或受該實體之指示。於該等安排，代理人並未提供虛擬資產服務提供商服務予本人，而是代表本人提供虛擬資產服務提供商服務予第三人。虛擬資產部門之實體可能經常代表其它實體，取決於營業模式。於該情況下，應要求將使用代理人之虛擬資產服務提供商將代理人納入防制洗錢／打擊資恐計畫，並監督他們遵守其計畫。代理人亦應向權責機關取得執照或註冊，或者應要求為本人之虛擬資產服務提供商維護並使權責機關可取得其與代理人所在國家之最新代理人名單。

▪ **新科技**

172. 建議第 15 項。於 2018 年 10 月，FATF 通過建議第 15 項之更新，其強化各國及義務實體於新科技之背景下之根本性風險基礎方法及相關義務，以釐清其於虛擬資產背景下之應用（包含虛擬資產金融活動及虛擬資產服務提供商）。建議第 15 項要求各國辨識及評估有關發展新商品及營業活動之洗錢與資恐風險，包含新的運送機制及同時為新及已存在之商品使用新的或開發中科技。值得注意的是，它亦要求各國確保於其司法管轄區內取得執照或營運之金融機構於推出新商品或業務活動或使用新科技或開發中科技前採取適當措施以管理及抵減相關之洗錢與資恐風險（參附件 A）。

173. 為與建議第 15 項之精神一致，2018 年 10 月更新進一步釐清各國應管理及抵減來自虛擬資產之風險並確保虛擬資產服務提供商於防制洗錢／打擊資恐目的下受監理、取得執照或註冊，以及確保遵循 2019 年 6 月所通過於建議第 15 項注釋要求之相關措施（參附件 A）。

174. 於虛擬資產及虛擬資產服務提供商活動之脈絡下，各國應確保於其司法管轄區內取得執照或營運之虛擬資產服務提供商得管理及抵減從事涉及使用匿名強化科技或機制之活動，包含但不限於強化匿名加密貨幣、混幣器、轉向器、隱私錢包以及其他混淆虛擬資產寄件人、收件人、持有人或實質收益人身分之科技。若虛擬資產服務提供商不能管理及抵減從事此等活動之風險，則若虛擬資產服務提供商不應被允許從事此等活動。

▪ **電匯及「轉帳規則」**

175. 建議第 16 項及其注釋係為防止恐怖分子及其他罪犯不受限制地取得電子便利之資金移轉以移動資金及偵測發生此類濫用之目的所發展。於草擬時，FATF 將此類移轉稱為「電匯」。根據 FATF 建議之功能性方法，建議第 16 項下與電匯及相關資訊有關之要求適用於此類服務之所有提供商。此包括提供服務或從事功能類似於電匯之活動（例如虛擬資產移轉）之虛擬資產服務提供商。

▪ **建議第 16 項概述及其於虛擬資產及虛擬資產服務提供商之應用**

176. 建議第 16 項將「電匯」定義為任何透過金融機構以電子方式代表轉出人進行交易，目的是向接收人金融機構之接收人提供一定數額之資金，無論轉出人及接收人是否為同一人。

177. 建議第 16 項並為各國建立有關電匯及相關訊息之要求，並適用於當地及跨境電匯。簡而言之，各國應確保金融機構包含電匯及相關訊息之必要及精確之轉出人資訊及必要之接收人資訊。金融機構亦應監控電匯以偵測該等缺乏必要轉出人及／或接收人資訊之電匯，並篩選交易以符合聯合國安理會之相關決議（參建議第 6 項及第 7 項）。

178. 如建議第 15 項注釋，各國應適用建議第 16 項於虛擬資產移轉及虛擬資產服務提供商。各國應適用建議第 16 項不論該傳統電匯或虛擬資產於法定貨幣或虛擬資產計價價值。然而，為辨識虛擬資產之獨特科技性財產，建議第 16 項以經修改之方式適用於虛擬資產，如建議第 15 項注釋第 7 (b) 所列。FATF 之電匯要求於虛擬資產脈絡下之應用被稱為「轉帳規則」。
179. 建議第 16 項之要求適用於虛擬資產服務提供商，不論為法定貨幣或虛擬貨幣，包含：(a) 傳統電匯、(b) 於虛擬資產服務提供商及其他義務實體之虛擬資產移轉 (例如，虛擬資產服務提供商間或虛擬資產服務提供商及其他義務實體間，例如銀行與其他金融機構)、或 (c) 虛擬資產服務提供商及非義務實體間之虛擬資產移轉 (例如，非托管錢包)。建議第 16 項之全部要求如下所示為適用在 (a)、(b)，不包含 (c)。依據建議第 1 項注釋，基於虛擬資產服務提供商之跨境性質，各國應視所有虛擬資產移轉為跨境電匯，而非當地電匯。對於涉及非托管錢包之移轉，建議第 16 項之要求以特定方式適用，如下說明。
180. 有關虛擬資產移轉之交易費用<sup>43</sup>並非屬轉帳規則之範圍。因此，虛擬資產服務提供商無需辨識收款人之交易費用，因為收款人並非虛擬資產移轉本身之轉出人或收款人。亦可能存在技術原因使虛擬資產服務提供商必須發送大量大於實際被移轉虛擬資產之虛擬資產之情況，差額將自動退還進行匯款之虛擬資產服務提供商。於此情況下，轉帳規則不適用於退款之收款人虛擬資產服務提供商，因為退款透過進行匯款之虛擬資產服務提供

---

<sup>43</sup> 「交易費用」係指將交易包含在一個區塊中之礦工可能收取之虛擬資產金額。根據虛擬資產之類型，它可以被稱為不同之名稱，例如 gas 或區塊獎勵，但出於同樣之原因，它們不在轉帳規則之範圍內。



商構成移轉之一部分。

▪ **獲取、持有及提交所需且精確之轉出人和所需之接收人資訊之要求**

181. 各國應確保參與虛擬資產移轉之進行匯款機構（無論是虛擬資產服務提供商還是其他義務實體，例如金融機構），獲取並持有所需且精確之轉出人資訊和所需之接收人資訊，並將資訊提交給受益機構（無論是虛擬資產服務提供商或其他有義務的實體，例如金融機構），如果有的話。此外，各國應確保受益機構（無論是虛擬資產服務提供商還是其他有義務的實體，例如金融機構）獲取並持有所需（但不一定準確<sup>44</sup>）的轉出人資訊以及所需且準確之接收人資訊，如建議第 16 項所述。（參以下第 4 欄）。

#### 第四欄 特定詞彙定義

**建議第 15 項注釋 15-7(b) 中之虛擬資產／虛擬資產服務提供商之電匯規則**

「建議第 16 項」：「各國應確保發起方之虛擬資產服務提供商於虛擬資產移轉時取得並持有必要及準確之轉出人資訊及必要之接收人資訊。」

註腳：「如建議第 16 項注釋第 6 段所定義，或於虛擬資產脈絡下相等之資訊。」

**建議第 16 項注釋所使用之詞彙表**

**準確的：**係被使用於描述已被驗證準確性之資訊。

**建議第 16 項注釋**

---

<sup>44</sup> 如圖表 1，自轉出人虛擬資產服務提供商接收轉出人資訊之接收人擬資產服務提供商不要求資料準確性。他們可能會假設資料已由轉出人虛擬資產服務提供商驗證。

6. 所有符合條件之電匯隨附之資訊應始終包含：

- (a) 轉出人之姓名；
- (b) 轉出人用於處理交易之帳戶號碼；
- (c) 轉出人之地址、或國家身分證號碼、或客戶身分證號碼、或出生日期及出生地；
- (d) 接收人之姓名；及
- (e) 接收人之用於處理交易之帳戶號碼。

182. 轉出機構必須獲取及持有之必要資訊包括：

- a. 轉出人之姓名 ( 即傳送人之準確 ( 即經過驗證 ) 全名 ) ；
- b. 轉出人用於處理交易之帳戶號碼。於虛擬資產之脈絡下，此可指該虛擬資產之「錢包位址」；
- c. 轉出人之實體 ( 地理上 ) 之地址、或國家身分證號碼、或客戶身分證號碼 ( 亦即非交易號碼 ) ，以特定辨識於進行匯款機構之轉出人，或出生日期及出生地。有關傳輸轉出人之地理上地址，此意指作為其認識客戶流程之一部分，轉出人虛擬資產服務提供商已驗證其準確性 ( 參關於客戶審查之第 148-160 段 ) ；
- d. 接收人之姓名 ( 即虛擬資產移轉接收者而被轉出人指定之人之姓名 ) 。此不需要由進行匯款機構驗證其準確性，但應為疑似洗錢或資恐交易報告之監控及裁罰篩選之目的進行審查；及
- e. 該接收人用於進行交易之帳戶號碼。於虛擬資產之脈絡下，此可指該虛擬資產之「錢包位址」；

183. 接收機構須自轉出機構獲得並持有之必要資訊包括：

- a. 轉出人之姓名 (即傳送人之姓名)。接收人機構並不需要驗證轉出人姓名之準確性，但應為疑似洗錢或資恐交易報告之監控及裁罰篩選之目的進行審查；
- b. 轉出人用於處理交易之帳戶號碼。於虛擬資產之脈絡下，此可指該虛擬資產之「錢包位址」；
- c. 轉出人之實體 (地理上) 之地址、或國家身分證號碼、或客戶身分號碼 (即非交易號碼)，以特定辨識於進行匯款機構之轉出人，或出生日期及出生地；
- d. 接收人之姓名 (即虛擬資產移轉接收者而被轉出人所辨識之人之姓名)。接收人機構必須驗證接收人姓名之準確性，若其客戶之姓名先前並未被驗證。從而接收人機構得確認其自進行匯款機構取得之接收人姓名及帳戶號碼是否符合接收人機構之受驗證客戶資訊；及
- e. 接收人用於處理交易之帳戶號碼。於虛擬資產之脈絡下，此可指該虛擬資產之「錢包位址」；

表 1 • 進行轉出及接收虛擬資產服務提供商於轉帳規則下之資料要求

資料項目及需採取之行動	轉出虛擬資產服務提供商	接收虛擬資產服務提供商
轉出人資料	<p>必要的，即必須向接收人<u>虛擬資產服務提供商</u>提交所需之資訊。</p> <p><u>準確的，即轉出虛擬資產服務提供商需驗證其準確性以作為客戶審查流程之一部分。</u></p>	<p>必要的，即接收人<u>虛擬資產服務提供商</u>需取得轉出<u>虛擬資產服務提供商</u>之所需資料。</p> <p>不要求資料準確性。接收<u>虛擬資產服務提供商</u>得假設該資料已由轉出<u>虛擬資產服務提供商</u>進行驗證。</p>
接收人資料	<p>必要的，即必須向接收人<u>虛擬資產服務提供商</u>提交所需之資料。</p> <p>不要求資料準確性，但轉出匯款<u>虛擬資產服務提供商</u>必須監控以確認未出現任何可疑情況。</p>	<p>必要的，即接收人<u>虛擬資產服務提供商</u>需取得轉出<u>虛擬資產服務提供商</u>之所需資料。</p> <p><u>準確的，即接收人虛擬資產服務提供商必須驗證該所需資訊且需要確認所接收之資料為一致。</u></p>
需採取之行動	<p>自轉出人取得所需資訊並留存紀錄</p> <p>篩選以確認接收人並非受制裁名單。</p> <p>監控交易並於可疑時提出報告。</p>	<p>自轉出<u>虛擬資產服務提供商</u>取得所需資訊並留存紀錄。</p> <p>篩選以確認轉出人並非受制裁名單。</p> <p>監控交易並於可疑時提出報告。</p>

184. 虛擬資產服務提供商必須向接收人機構 (如有) 提交所需資訊。各國確保虛擬資產移轉之提供者 (無論是虛擬資產服務提供商亦或是其他義務實體) 立即安全地傳輸所需之轉出人和接收人資訊為至關重要。鑑於虛擬資產移轉之快速及跨境性質，並且符合建

- 議第 16 項之目標（以及建議第 16 項中關於「伴隨 [……] 涉及法定貨幣之電匯之轉出人及接收人資訊之傳統要求）。若沒有接收人機構，虛擬資產服務提供商仍必須收集所需資訊（如下所述）。
185. 「立即」—於建議注釋第 15 項第 7(b) 段之脈絡下，且鑑於虛擬資產跨境性質、全球範圍及交易速度，此意味著提供商應於移轉前、同時或併行地提交所需資訊。有關這些特定於虛擬資產服務提供商和其他義務實體問題之更多資訊，請參第四部分中之建議第 16 項。
186. 「安全地」，同樣於建議注釋第 15 項第 7(b) 段之脈絡下，旨在傳達提供商應以安全方式傳輸及儲存所需資訊。此是為了保護所需資訊之完整性和可用性，以促進記錄保存（以及其他要求），透過接收虛擬資產服務提供商或其他義務實體以促進此類資訊之使用，並保護資訊免遭未經授權之揭露。使用該詞彙並不意味著妨礙建議第 16 項或建議第 9 項之目標，儘管在虛擬資產服務提供商合理評估<sup>45</sup> 虛擬資產服務提供商交易對手無法充分保護轉帳規則資訊之情況下，例外或更改程序可能是適當的。
187. 分批提交轉出人及接收人資訊是可被接受的，只要係依據 FATF 國際標準立即安全地提交即可。不允許事後提交所需資訊（即必須於進行虛擬資產移轉前或移轉時提交）。各國應釐清虛擬資產服務提供商或其他義務實體應於虛擬資產移轉時提交資訊，即使是分批提交。

---

<sup>45</sup> 資產服務提供商應以風險為本決定與誰進行交易（第 199 段）。虛擬資產服務提供商向／自非虛擬資產服務提供商或其他義務實體之實體發送或接收虛擬資產移轉應自其使用者取得所需之轉出人及接收人資訊（即使他們並未將該資訊提交予接收人（第 204 段）。

188. 無需將資訊直接附加於虛擬資產移轉本身。資訊可以直接或間接提交，如建議第 15 項注釋中所述，只要它是「立即且安全地」提交，並應權責機關之要求提供。與 FATF 之技術中立方法一致，所需資訊無需作為於（或納入）區塊鏈或其他分散式帳本 (DLT) 平台本身移轉之一部分進行傳輸。向接收人虛擬資產服務提供商提交資訊可能與在區塊鏈或其他分散式帳本 (DLT) 虛擬資產移轉是完全不同之程序。任何技術或軟體解決方案都可被接受，前提是該解決方案使進行匯款及接收人機構能夠遵守建議第 16 項之要求（當然，不會妨礙他們遵守 FATF 建議下之其他防制洗錢／打擊資恐義務之能力）。各國應與私部門實體合作，探討現有技術潛在應用或可能之解決方案，以遵循建議第 16 項（建議第 16 項中供應商及其他義務實體之更多詳細資訊，請參閱第四部分）。同等重要的是注意監理／監理機構之間、私部門實體之間以及監理／監理機構與私部門實體間之合作與協調，對於確保虛擬資產服務提供商採用之轉帳規則解決方案之互通性及實現於全球範圍內有效實施轉帳規則極為重要。
189. 對於法人而言，法人機構識別編碼 (LEI) 可於支付訊息中以可選擇之方式<sup>46</sup> 作為附加資訊。為允許可選擇使用法人機構識別編碼，各國得鼓勵相關利害關係人（例如，金融機構領域之支付市場實踐小組、虛擬資產服務提供商行業協會、虛擬資產服務提供商部

---

46 國際清算銀行支付暨市場基礎設施委員會 (CPMI)- 通匯銀行 -2016 年 7 月及巴賽爾銀行監理委員會 指引健全管理與洗錢及資恐有關之風險 (2020 年 7 月)，「正如國際清算銀行支付暨市場基礎設施委員會所建議，於當前相關支付訊息（即 MT 202 COV 和 MT 103）中，應得選擇使用法人機構識別編碼作為支付訊息中之其他資訊。於可能之情況下，法人機構識別編碼的使用將有助於通匯銀行確定訊息中之資訊足以明確識別移轉之轉出人及接收人」。

門之工作小組)在不更改當前訊息結構之情況下，努力定義是否以及如何將法人機構識別編碼納入相關虛擬資產資料移轉訊息之共同市場慣例。

190. 各國應同時要求進行轉出及接收機構於其國內架構下使以上必要資訊得於適當機關要求下取得，以符合建議第 11 項所列之紀錄保存要求。
191. 考慮到與各種虛擬資產及所涵蓋之虛擬資產活動相關之風險，各國得選擇依據 FATF 國際標準對虛擬資產移轉採用 1000 美元／歐元之最低限度之門檻。如果各國選擇實施此門檻，則與高於門檻之虛擬資產移轉相比，低於門檻之虛擬資產移轉之要求相對較少。對於低於門檻之虛擬資產移轉，各國應要求虛擬資產服務提供商蒐集：
  - a. 轉出人及接收人之姓名；及
  - b. 各虛擬資產錢包位址或特定交易參考號碼。
192. 除非存在與洗錢與資恐相關之可疑情況，否則無需驗證此類資訊，於此種情況下，應驗證與客戶有關之資訊。<sup>47</sup>

▪ **虛擬資產移轉之制裁檢核**

193. 各國應要求進行轉出機構及接收機構採取凍結行動，並禁止與被指名之人及實體進行交易（即檢核與要求有關虛擬資產移轉之資訊以遵守其目標性金融制裁之義務）。進行匯款機構應擁有關於其客戶、轉出人之必要資訊，而接收機構應擁有關於其客戶、接收人之必要資訊，以符合建議第 10 項中規定之客戶審查要求。轉出機構及接收機構應分別於初次接受客戶時（以及姓名變更時）

---

<sup>47</sup> 建議第 16 項注釋第 5 段。

檢核其客戶之姓名，以確保遵守目標性金融制裁之義務。然後，當他們進行虛擬資產移轉時，他們必須篩選另一方（轉出人或接收人）之姓名（見前文表 1）。

194. 各國應要求虛擬資產服務提供商或其他義務實體實施有效之控制架構，以確保它們能夠遵循目標性金融制裁義務。該架構應考量到虛擬資產移轉之性質。由於識別轉出人及接收人之所需資訊得分別保存於虛擬資產移轉系統（例如，區塊鏈）中，因此即使缺少此類資訊或沒有檢核移轉以識別可疑與禁止之交易，也可以完成虛擬資產移轉。因此，虛擬資產服務提供商或其他義務實體應將所需之虛擬資產移轉之資訊分別篩選至該直接結算。因此，虛擬資產服務提供商可能需要考慮適合其業務流程及虛擬資產技術性質之抵減措施。儘管區塊鏈技術瞬息萬變，但虛擬資產服務提供商或其他義務實體得實施之控制措施範例包括：

- a. 將錢包擱置，直至檢核完成且確認沒有發現任何問題；及
- b. 安排使用連結至客戶錢包之供應商錢包接收虛擬資產移轉，並僅於檢核完成並確認沒有任何問題後始將移轉之虛擬資產移轉至客戶錢包中。

195. 各國應該意識到虛擬資產移轉不同於傳統之法定貨幣電匯之性質。因此，各國應要求虛擬資產服務提供商及其他義務實體記錄其補救控制行動，以促使有效監理。各國可能會要求義務實體於其防制洗錢與資恐風險評估中記錄此控制。

▪ *向／自其它虛擬資產服務提供商之虛擬資產移轉及虛擬資產服務提供商交易對手之識別及盡職調查*

196. 考量虛擬資產移轉之特定性質及於私部門實體中轉帳規則解決方案之未來控制框架（參第四部分之建議第 16 項），FATF 期望各



國實施建議第 15 項第 7(b) 段。虛擬資產移轉得被直接結算，即僅透過錢包位址間之區塊鏈分散式共識機制，無需中介商。然而，對於虛擬資產服務提供商向另一個虛擬資產服務提供商傳輸所需資訊，他們必須識別他們的虛擬資產服務提供商交易對手。虛擬資產服務提供商亦需在傳輸所需資訊前，對其虛擬資產服務提供商交易對手進行盡職調查，以避免在不知情的情況下與非法行為者或受制裁行為者打交道。虛擬資產服務提供商在與他們之前進行過交易對手盡職調查之虛擬資產服務提供商交易時，不需要為每個個別之虛擬資產移轉進行虛擬資產服務提供商交易對手盡職調查程序，除非有可疑之交易歷史或其他資訊（例如負面新聞、有關監管或刑事處罰之公開資訊）顯示他們應該這樣做。考慮到盡職調查之概念，各國應期望虛擬資產服務提供商定期更新其虛擬資產服務提供商交易對手之盡職調查資訊，或者依符合其定義之風險基礎方法控制結構其關係出現風險時。因此，各國應期待其具有義務之虛擬資產服務提供商實施此控制機制。如前所述，虛擬資產服務提供商應使用此盡職調查程序以確定是否可以合理地期望對方保護與其共享資訊之機密性。

197. 及時安全地進行相對人盡職調查之最佳方式是一項挑戰。<sup>48</sup> 此程序大致分為三個階段。此並非虛擬資產服務提供商必須採取之規定性行動，而是關於如何進行相對人盡職調查之指引：

- a. 第 1 階段：決定虛擬資產移轉是否是與虛擬資產服務提供商交易對手進行。一個人可能希望將虛擬資產移轉至另一個虛擬資產服務提供商（例如，擁有託管錢包之接收人），或者他們可能希望將虛擬資產移轉到非託管錢包。因此，轉出人虛擬資產

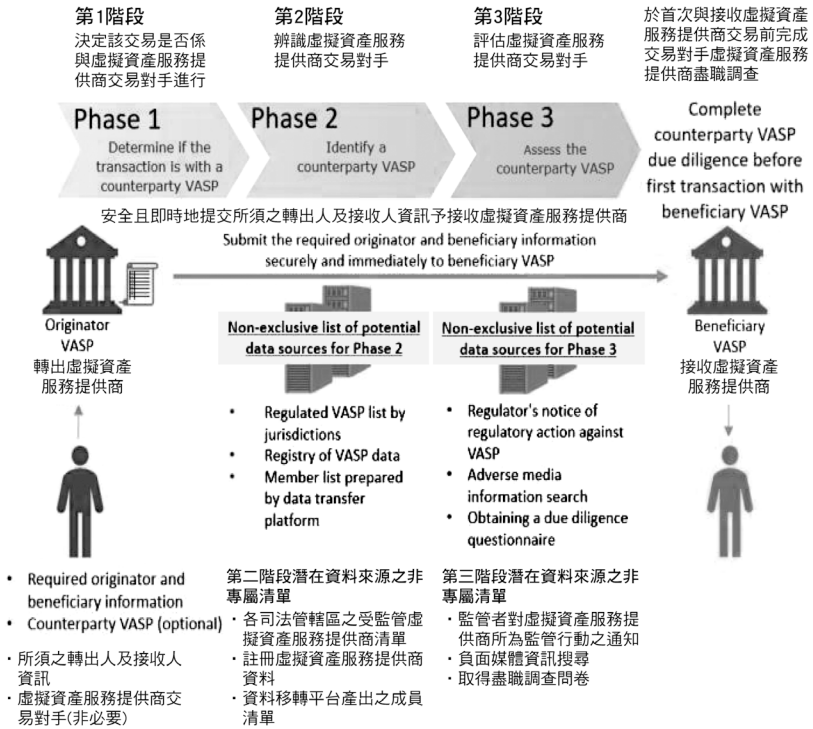
---

<sup>48</sup> 參 FATF12 個月的審查報告第 61 段。

服務提供商必須確定他們是否將與另一個虛擬資產服務提供商進行交易。這一決定過程並非純粹是防制洗錢／打擊資恐要求，而是源於支援虛擬資產之技術。迄今為止，FATF 尚不知道有任何經技術驗證之方法以識別虛擬資產服務提供商，該虛擬資產服務提供商於所有情況下僅自虛擬資產位址中詳盡、精確及準確地管理接收人錢包；

- b. 第 2 階段：識別虛擬資產服務提供商交易對手，因虛擬資產服務提供商僅知道虛擬資產服務提供商交易對手在前一階段之「名稱」。虛擬資產服務提供商得使用可靠之資料庫自行識別虛擬資產服務提供商交易對手，該資料庫須符合該國關於何時仰賴此類資料之任何準則；及
- c. 第 3 階段：評估虛擬資產服務提供商交易對手是否為具有資格向其發送客戶資料並與之建立業務關係之相對人（有關虛擬資產服務提供商交易對手盡職調查之更多資訊，請參閱第四部分之建議第 16 項及關於記錄保存以適當儲存及管理該客戶資料之建議第 11 項）。

圖 1. 廣義虛擬資產服務提供商交易對手盡職調查流程概述



198. 為釐清本指引之範圍，權責機關應要求虛擬資產服務提供商在「第3階段」實施預防性措施，以評估虛擬資產服務提供商交易對手，首先虛擬資產服務提供商具有業務關係，接著定期審查盡職調查之結果。各國亦應為「第2階段」維持可靠、獨立之資訊來源，以協助虛擬資產服務提供商努力識別虛擬資產服務提供商交易對手。此可能包括受監管之機構名單，例如虛擬資產服務提供商名單（如有）、實質受益權登記處（如有）及巴賽爾銀行監理委員

會指引中提及之其他例子<sup>49</sup>。為了有效及有效率之交易對手盡職調查，受監管機構名單可能包括但不限於虛擬資產服務提供商名稱和註冊之虛擬資產服務提供商位址。考慮數位化流程於金融業之使用日益增加，應鼓勵各國使用機器可讀之格式。一國無需對在該國境內已經取得執照或註冊為金融機構（如 FATF 建議所定義）之自然人或法人實施單獨之虛擬資產服務提供商執照或註冊制度。擁有此類框架之國家可以向其私部門機構釐清，此類金融機構可能不在指定之虛擬資產服務提供商名單上，甚至不在同一監理機關之監督之下，以避免不必要之去風險化。

199. 此外，各國亦應釐清，虛擬資產服務提供商應以風險為本決定與誰進行交易，並認識到每個虛擬資產服務提供商採取之風險抵減措施可能有所不同。一般而言，由個別虛擬資產服務提供商自防制洗錢／打擊資恐角度進行以風險為本之分析，並考慮其他法遵問題（包括資料儲存及安全性）以及業務關係之營利能力而做出此等業務決策。轉出人實體可能希望透過契約要求其接收人遵守轉帳規則，不論接收人之管轄司法管轄區是否缺少監管。各司法管轄區根據其自身裁量權及洗錢與資恐風險評估，亦得考慮將來自未有效實施取得執照或註冊要求之國家／地區之所有虛擬資產服務提供商指定為高風險。

---

<sup>49</sup> 巴塞爾銀行監理委員會 (2014 年, 2020 年修改版) 有關洗錢及資恐之良好風險管理: 對監理合作之修訂, 附件 2"21。銀行亦應考慮自公共來源蒐集資訊。此等可能包括通匯銀行監理機構之網站, 用於將身份識別資料與監理機構於授權過程中取得之資訊進行交叉比對, 或涉及對通匯銀行施加之潛在防制洗錢／打擊資恐行政裁罰。此亦可能包括公共登記處 (參 FATF 指引第 25 段)。 [www.bis.org/bcbs/publ/d505.pdf](http://www.bis.org/bcbs/publ/d505.pdf)

200. FATF 期望各國儘快執行建議第 15 項注釋第 7(b) 段。各國可能期望採取分階段方式執行轉帳規則要求，以確保其虛擬資產服務提供商有足夠時間實施必要的系統，但應繼續確保虛擬資產服務提供商採取替代措施，以適當抵減於此期間內因虛擬資產移轉而產生之洗錢與資恐風險。各國亦應考慮到虛擬資產移轉之獨特性質，以及為私部門機構之解決方案制定控制框架，以安全地提交所需資訊。儘管如此，各國正以不同速度實施其針對虛擬資產服務提供商之防制洗錢／打擊資恐框架。此意味著某些司法管轄區將要求其虛擬資產服務提供商於其他司法管轄區之前遵守轉帳規則（即「日出問題」）。對於虛擬資產服務提供商來說，這可能是一個挑戰，即他們應該採取什麼方法來處理位於轉帳規則尚未生效之司法管轄區之虛擬資產服務提供商。儘管接收人司法管轄區缺乏監管，轉出實體得透過契約或商業慣例要求接收人遵守轉帳規則。通常，由每個虛擬資產服務提供商根據其以風險為本之分析做出此等業務決策，虛擬資產服務提供商對實施建議第 15 項注釋第 7(b) 段之遵守程度應構成此等決定之一部分。虛擬資產服務提供商及金融機構應考慮每個客戶／交易對手虛擬資產服務提供商之洗錢與資恐風險等級以及交易對手／客戶虛擬資產服務提供商實施任何適用之風險抵減措施。
201. 鑑於與轉帳規則有關之「日出問題」，各國在評估虛擬資產服務提供商提出之商業模式時應採用風險基礎方法。各國應考量轉帳規則遵循之全部背景，包括虛擬資產服務提供商是否採取足夠之風險抵減措施以充分管理隨之而來之洗錢與資恐風險。無論某個國家／地區的規範為何，虛擬資產服務提供商都可以實施強有力之控制措施，以符合轉帳規則之要求。例如，虛擬資產服務提供

商將虛擬資產移轉限制於其客戶群內（即，在同一虛擬資產服務提供商內進行虛擬資產之內部移轉），僅允許在其客戶群之外進行已確認之同一人移轉（即，轉出人及接收人被確認為同一人）以及加強對交易之監控。有關更多風險補救範例，請參第四部分交易對手虛擬資產服務提供商識別及盡職調查。雖然各國採用及實施相關法規本身很重要，但一個國家缺乏相關法規並不一定排除虛擬資產服務提供商本身導入措施之有效性。

■ **虛擬資產移轉予「中介虛擬資產服務提供商」／自「中介虛擬資產服務提供商」移轉**

202. 與金融機構間之電匯相似，可能存在涉及「中介虛擬資產服務提供商」或其他中介義務實體或金融機構之虛擬資產移轉情境，此等實體或金融機構促使虛擬資產移轉作為虛擬資產移轉鏈中之中間要素。<sup>50</sup> 各國應確保此類中介機構（無論是虛擬資產服務提供商還是其他義務實體）亦遵守建議第 16 項之要求，如建議第 15 項注釋所載，包括將所有虛擬資產移轉視為跨境合格移轉。正如同處理傳統法定跨境電匯之傳統中介金融機構必須確保隨電匯一起保留所有所需之轉出人及接收人資訊，中介虛擬資產服務提供商或其他促進虛擬資產移轉之類似中介機構也必須確保所需資訊隨著虛擬資產移轉鏈傳輸，以及維護必要之記錄並於被要求時將資訊提供給相關機關。同樣地，當技術限制使所要求之轉出人或接收人資訊無法保留在所要求提交之資料中，則接收中介虛擬資產服務提供商應將自進行匯款虛擬資產服務提供商或其他中介虛

---

<sup>50</sup> 謹釐清，當虛擬資產服務提供商、金融機構或其他中介義務實體促使虛擬資產移轉作為虛擬資產移轉鏈中之中介元素，並且某些活動／業務在本指引中被歸類為虛擬資產服務提供商時，則它們將被歸類為「中介虛擬資產服務提供商」。

擬資產服務提供商收到之所有資訊之記錄保存至少五年。參與虛擬資產移轉之中介機構亦有一般性義務識別可疑交易，採取凍結行動，並禁止與指名之個人及實體進行交易，就像轉出和接收虛擬資產服務提供商（或促進虛擬資產移轉之其他轉出或接收義務實體）一樣。

▪ *虛擬資產移轉予未託管錢包／自未託管錢包移轉*

203. FATF 認識到，與傳統之法幣電匯不同，並非每次虛擬資產移轉都會涉及（或有）兩個義務實體，無論是虛擬資產服務提供商還是金融機構等其他義務實體。在虛擬資產移轉僅涉及移轉兩端之其中一個義務實體之情況下（例如，當轉出虛擬資產服務提供商或其他義務實體為轉出人或代表轉出人向接收人發送虛擬資產時，而該接收人並非接收人機構之客戶，而是個人虛擬資產使用者，將以非託管錢包接受虛擬資產移轉），各國仍應確保義務實體遵循建議第 16 項對其客戶（轉出人或接收人，視情況而定）之要求。

204. FATF 並不期待虛擬資產服務提供商及金融機構，當發起虛擬資產移轉時，向非義務實體之個人提交所需資訊。虛擬資產服務提供商向／自非虛擬資產服務提供商或其他義務實體（例如，從個人虛擬資產用戶至非託管錢包）之實體發送或接收虛擬資產移轉，其應自其客戶取得所需之轉出人及接收人資訊。各國應要求其虛擬資產服務提供商或其他義務實體實施機制以確保對此類移轉進行有效審查，特別是履行其疑似洗錢或資恐交易報告及實施制裁義務（參以下建議第 20 項之討論），且如上所述，可以選擇施加額外對使用非託管錢包進行此類移轉之限制或控制。

▪ *對第三人之依賴*

205. **建議第 17 項**允許各國准予義務實體仰賴第三人開展業務及／或執行部分客戶審查流程，包含辨識及驗證客戶身分。然而第三人必須為受權責機關監理及監控防制洗錢／打擊資恐之受監管實體，並採取措施遵守客戶審查及記錄保存要求。此外，於發生違約時，對第三人之依賴不會免除義務實體之義務或責任。
206. 各國得允許虛擬資產服務提供商作為第三人，根據其在建議第 15 項下之地位。除檢查第三人之監管地位外，義務實體應於風險基礎上進行選擇。在第三人虛擬資產服務提供商之脈絡下，各國及義務實體應考慮第三人可能帶來之風險、業務或營運之性質、第三人虛擬資產服務提供商之客戶群或目標市場及其業務合作夥伴（如有相關）。如果虛擬資產服務提供商依賴另一個虛擬資產服務提供商進行業務介紹或進行客戶審查，則虛擬資產服務提供商間對於客戶審查之依賴，尤其是在虛擬資產移轉之脈絡下，應以與建議第 16 項之要求一致及符合之方式為之。

▪ **內部控制及外國分支機構及子公司**

207. **建議第 18 項**要求各國要求義務實體（例如虛擬資產服務提供商）實施內部控制，以建立防制洗錢／打擊資恐政策及流程之有效性以及其營運、部門、分支機構及子公司之風險管理品質，包含國內及國外（如有相關）。此等內部控制應包括適當之治理安排，明確分配防制洗錢／打擊資恐之責任，且於管理層次指定法遵人員；依據適當之當地法律實施監控員工誠信之控制措施；員工之持續培訓；及（外部或內部）獨立稽核功能以測試系統。

▪ **高風險國家**

208. **建議第 19 項**建議各國要求義務實體（例如虛擬資產服務提供商）對於與來自高風險國家之自然人及法人之業務關係及交易採用加



強客戶審查措施，包括 FATF 要求採取加強客戶審查措施之國家。鑑於其活動之跨境性質，此與虛擬資產活動及虛擬資產服務提供商具有特定之相關性。

▪ **疑似洗錢或資恐交易報告及揭露**

209. **建議第 20 項**要求所有懷疑或有合理懷疑資金為犯罪所得或與資恐相關之金融機構立即向相關金融情報中心報告其疑慮。因此，各國應確保虛擬資產服務提供商以及參與涵蓋之虛擬資產活動之任何其他義務實體提交疑似洗錢或資恐交易報告（有關虛擬資產服務提供商及其他義務實體之其他資訊，請參第四部分）。
210. 與建議第 15 項注釋第 7 段相同，關於預防措施之適用，正如上述於建議第 16 項之脈絡下所討論，各國亦應要求虛擬資產服務提供商於其營運所在國家遵守建議第 16 項之所有相關要求（同樣地，請參第四部分之其他資訊）。
211. 於一些虛擬資產服務提供商和其他從事虛擬資產活動之義務實體已實施全面之防制洗錢／打擊資恐義務之司法管轄區，關於虛擬資產之疑似洗錢或資恐交易報告已被證明對於推進執法調查工作以及提升金融情報中心更好地理解和分析虛擬資產生態系統中之提供者和活動沒有益處。<sup>51</sup> 各國應考慮是否有必要更新其現有申報機制或形式，以使提供商或其他義務實體申報可能與虛擬資產活動相關之特定指標，例如設備標識、具有相關時間戳記之 IP 位

---

<sup>51</sup> 例如，存款機構及虛擬資產服務提供商（特別是交易所）提交之疑似洗錢或資恐交易報告使美國執法部門能夠在 2017 年對 BTC-e 採取行動，BTC-e 是一種以網路為基礎之貨幣傳送器，用於交換法定貨幣以及虛擬資產並促進涉及勒索軟體之交易，電腦駭客、身份盜竊、稅務詐欺計畫、公共腐敗及販毒—幫助他們識別 BTC-e 使用之虛擬資產錢包位址並偵測透過交易所移動之不同非法活動流。

址、虛擬資產錢包位址及交易哈希值。

212. 雖然虛擬資產服務提供商不需要提交經驗證之有關接收人之必要資訊（參上述建議第 16 項），但可能存在虛擬資產服務提供商對其處理資料之準確性產生懷疑之情況，由於虛擬資產服務提供商注意到了任何差異。該等差異得以區塊鏈分析工具辨識；其交易對手虛擬資產服務提供商提供之資訊；外部機關；或基於其交易歷史及記錄。如果由於其客戶（就轉出人虛擬資產服務提供商而言）或轉出人虛擬資產服務提供商（就接收人虛擬資產服務提供商而言）提供之資訊不準確或不完整而存在任何差異，則應與請求之交易或與同一客戶相關之交易共同評估以瞭解是否出現可疑情況。此等認可對於金融情報中心、執法機關及調查人員來說可能是非常有價值之資訊。因此，各國應要求其虛擬資產服務提供商實施機制，以確保對可疑交易進行有效審查並滿足實施制裁之要求。

213. **建議第 21 項**係有關於 FATF 建議下適用於金融機構之揭露及保密措施。各國應將建議第 15 項注釋第 7 段所示相關預防措施適用於虛擬資產服務提供商。虛擬資產服務提供商、其董事、主管及員工（如適用），應受法律保護，免於因揭露（「揭露」）疑似洗錢或資恐交易報告而違反任何資訊揭露之限制及禁止故承擔刑事及民事責任，詳情如建議第 21 項所述。

▪ **法人及法律協議之透明性及實質受益權**

214. **建議第 24 項及第 25 項**。FATF 詞彙表將虛擬資產服務提供商定義為任何進行虛擬資產服務提供商定義之活動或業務之自然人或法人。建議第 24 項及第 25 項清楚提及各國應採取措施防止濫用法人及法律協議進行洗錢與資恐。與金融機構及指定之非金融事

業或人員相同，各國因此應採取措施防止濫用虛擬資產服務提供商，並考慮採取措施促使虛擬資產服務提供商取得實益受益權及控制資訊，以滿足建議第 10 項及建議第 22 項中規定之要求。

▪ **實務與執法措施**

215. **建議第 29 項。** 虛擬資產服務提供商 ( 或其他義務實體，例如傳統金融機構可能於虛擬資產範圍營運或參與涵蓋虛擬資產之活動 ) 依建議第 20 項提交之疑似洗錢或資恐交易報告必須向金融情報中心提交。除此之外，金融情報中心應得以向報告實體取得其司法管轄區之額外資訊，包含虛擬資產服務提供商，且應即時取得金融情報中心正常履行其職能所需之財務、行政、執法資訊。
216. 本指引之讀者應注意**建議第 30 項**已於上述以資金或價值為基礎之逐條建議分析之詞彙章節中提及。
217. **建議第 31 項。** 如同金融機構及指定之非金融事業或人員，各國及權責機關應得以取得所有必要文件及資訊，包括有權就虛擬資產服務提供商持有之記錄採取強制措施。應建立有效機制以及時查明是否為自然人或法人，例如虛擬資產服務提供商，持有或控制帳戶、錢包，以及確保權責機關具備程序以識別資產，包含虛擬資產，而無需事先通知所有人之機制。建議第 31 項之適用於各國及其權責機關於處理有關涵蓋虛擬資產活動及虛擬資產服務提供商之抵減洗錢與資恐風險時格外重要。
218. **建議第 32 項。** 各司法管轄區應採取風險基礎方法考量是否對於涵蓋虛擬資產活動及虛擬資產服務提供商採用建議第 32 項。特別是，各司法管轄區應在其風險基礎方法中考量 (a) 虛擬資產服務提供商及虛擬資產相關活動是否屬於實體貨幣工具之運輸參數，以及 (b) 建立申報要求及偵測此類資產跨境移動之系統如何於實

務中發揮作用，以及他們將如何抵減其司法管轄區內之洗錢與資恐風險。

219. 如建議第 30 項，本指引之讀者應注意，**建議第 33 項**已於上述以資金或價值為基礎之詞彙章節中提及。
220. **建議第 34 項**是各國識別及解決與虛擬資產活動及與虛擬資產服務提供商相關之洗錢與資恐風險以及與虛擬資產本身相關方法之重要組成部分。相關權責機關應制定指導方針並提供反饋，以幫助虛擬資產服務提供商（及其他義務實體，包括傳統金融機構）採用國家防制洗錢／打擊資恐措施，尤其是偵測及報告可疑交易—無論是虛擬／法定貨幣或虛擬／虛擬貨幣。

#### ▪ 國際合作

221. **建議第 36 項至第 40 項**。有鑑於虛擬資產活動及虛擬資產服務提供商部門之跨境與流動的特性，國際合作以及國家及權責機關就建議第 36 項至第 40 項之實施至關重要，尤其是建議第 37 項至第 40 項中適用於國家及權責機關之措施。除此之外，有效實施與國際合作相關之要求，對於限制一個司法管轄區內的虛擬資產活動提供商與其他可能更受監管之司法管轄區的提供商相比具有不公平競爭優勢的能力極為重要，並限制司法管轄區之挑選或跳躍或監理套利。
222. 應認知與虛擬資產服務提供商部門相關之有效監理、監督及執行，需要全球性的方法及跨司法管轄區的水平監管框架，建議第 15 項注釋第 8 段亦強調適用建議第 37 項至第 40 項以抵減虛擬資產、涵蓋之虛擬資產活動及虛擬資產服務提供商相關風險之重要性。各國應具備相互合作、提供司法互助所需之工具（建議第 37 項）；幫助辨識、凍結、扣押及沒收犯罪所得及工具，其可能為虛擬資產或與虛擬資產服務提供商活動相關之其他傳統資產之形式（建議第

- 38 項)；及於虛擬資產相關犯罪或從事非法活動之非法活動者之情況下，提供有效引渡協助(建議第 39 項)，以及其他國際性能力。
223. 與其他包含基於資金或價值條款之建議相同，於虛擬資產之情形，各國應適用與「於洗錢、前置犯罪或資恐中，自洗錢獲得、其所得、用於或擬為其使用的工具之財產，或具相應價值之財產」相關之沒收及保全措施。
224. 建議第 15 項注釋第 8 段亦特別要求，無論監理機關的性質、型態與其對虛擬資產服務提供商之命名或形態認定存有不同，虛擬資產服務提供商之監理機關與其外國對等單位應迅速及有建設性地交換資訊。
225. 國際合作亦適用於，虛擬資產服務提供商尋求在一司法管轄區內註冊或取得執照，但向位於其他司法管轄區之客戶「離岸」提供商品或服務。金融情報中心及時與其對等單位合作並交換相關的疑似洗錢或資恐交易報告之相關資訊，尤其係涉及跨境虛擬資產活動或虛擬資產服務商之作業，此極為重要。對其司法管轄區內運營之虛擬資產服務提供商進行充分的監督及監管，將使各國得以於虛擬資產領域更好地提供調查協助及其他國際合作。時下許多國家缺乏監管及調查能力，此可能會阻礙各國提供有意義的國際合作之能力。此外，許多國家沒有得將特定虛擬資產相關之洗錢與資恐活動入罪化的法律框架，於要求雙重犯罪之情形，這可能將進一步限制各國提供有效司法互助之能力。
226. 政府機關還應參考虛擬資產服務提供商監理機關間之資訊共享及合作原則，其進一步提供有關監理機關如何與其對等單位合作之指引(參照第六部分)。
- **指定之非金融事業或人員從事或提供涵蓋的虛擬資產活動**

227. 指定之非金融事業或人員從事虛擬資產服務提供商之活動時（例如賭場提供基於虛擬資產之遊戲或從事其他涵蓋的虛擬資產活動、商品或服務），各國應使該實體適用 FATF 建議中所有為虛擬資產服務提供商擬定之措施。各國應注意，例如建議第 22 項及第 23 項規定特定類型的指定之非金融事業或人員，有下列情形者：(a) 賭場、(b) 不動產經紀人，(c) 貴金屬與寶石交易商、(d) 律師、公證人、或其他獨立執業法律專業人士與會計師，以及 (e) 信託及公司服務業者，應進行客戶審查、記錄保存及其他要求。建議第 22 項明確載明指定之非金融事業或人員應適用建議第 10、11、12、15 項及第 17 項之要求。因此，於考量如何對從事虛擬資產服務提供商活動的指定之非金融事業或人員監管及監督，及採取防制措施時，各國應參照建議第 10、11、12、15 項及第 17 項以及其他與虛擬資產服務提供商相關的建議之適用。各國還應確保從事虛擬資產服務提供商活動之指定之非金融事業或人員有該等虛擬資產服務提供商活動相關的註冊／執照（參照第 123-139 段）。
228. 相同地，建議第 28 項要求各國及權責機關對指定之非金融事業或人員實行 FATF 建議規定的監理及監督措施。如前所述，各國應使虛擬資產服務提供商（包括從事虛擬資產服務提供商活動之指定之非金融事業或人員）適用與金融機構相同程度之監督及監管，而不是指定之非金融事業或人員等級之監督。於指定之非金融事業或人員從事涵蓋的虛擬資產服務提供商活動時（例如賭場提供虛擬資產商品及服務或從事涵蓋的虛擬資產活動），各國應讓指定之非金融事業或人員適用較高程度之監督（例如「指定之非金融事業或人員 +」（DNFBP plus）之監督），與所有受較高程度監督之虛擬資產服務提供商一致，此相當於建議第 26 項和第 27 項

中規定對金融機構之監督及監管層級。於此情形，該實體本質上是從事特定金融活動的虛擬資產服務提供商，而不是指定之非金融事業或人員，無論該國如何命名、稱呼或標示此類實體、機構或商品或服務提供商。各國採取此方法將有助於確保全球虛擬資產服務提供商部門的公平監管競爭場域，以及與虛擬資產服務提供商所從事之活動類型一致並相符之監督層級。有關誰是虛擬資產服務提供商之更多資訊，請參照前述第一部分。

- **監理或監控虛擬資產服務提供商之風險基礎方法**

- **瞭解洗錢與資恐風險**

229. 防制洗錢／打擊資恐之風險基礎方法旨在辨識、瞭解及評估洗錢與資恐風險，並制定與各國及相關義務實體辨識之洗錢與資恐風險相當之防制或抵減措施。於監理方面，監理機關分配其資源之方式適用風險基礎方法，其亦適用於監理機關以有利於虛擬資產服務提供商運用風險基礎方法之方式履行其職能。

230. 於 2021 年 3 月，FATF 發布監理機關就防制洗錢／打擊資恐監理之風險基礎方法之指引。此文件為監理機關提供指引，以協助其廣泛地採行以風險為本之監理，其亦包含專門就虛擬資產服務提供商監理機關之額外指引及實務建議，該文件應與本指引於此處一併閱讀。

231. 一個有效的以風險為本之制度應反映一個國家之政策、法律及監管方法。國家政策、法律及監管框架還應更宏觀地反映國家所推行之金融部門政策目標，包括普惠金融、金融穩定、金融誠信及金融消費者保護目標，並考量市場競爭等因素。國家框架允許虛擬資產服務提供商採行風險基礎方法之程度，亦應反映虛擬資產服務提供商部門之性質、多樣性及成熟度以及其風險概況，並同

樣反映與個別虛擬資產服務提供商及特定虛擬資產商品、服務或活動相關之洗錢與資恐風險。

232. 監理機關還應深入瞭解虛擬資產服務提供商市場、其結構以及其於金融體系及國家經濟中之角色，使其於該部門之風險評估得獲悉更多資訊。這可能需要投注培訓、人力或其他資源，使監理機關得獲得監管及監督本指引前文中之虛擬資產服務或商業模式所描述涵蓋之虛擬資產服務提供商及活動所需之實務技能及專業知識。
233. 監理機關應運用各種資訊來源以辨識及評估與虛擬資產之商品、服務及活動以及虛擬資產服務提供商相關之洗錢與資恐風險。該資訊來源應包括但不限於司法管轄區內之國家或部門風險評估、國內或國際就類型及監管之專業知識，以及金融情報中心之指引及反饋。如權責機關沒有充分瞭解該國之虛擬資產服務提供商部門或更廣泛的虛擬資產生態系統，權責機關可能適宜對虛擬資產服務提供商部門及／或虛擬資產環境進行較有目標性之部門風險評估，以拓展就相關洗錢與資恐風險具國家層級之瞭解，並為應進行機構評估的虛擬資產服務提供商提供資訊。
234. 部分司法管轄區正在使用或探索使用區塊鏈分析服務以協助其監理。該服務得以多種方式運用，包括定位監理人員於評估個別虛擬資產服務提供商時可能期望重點關注之領域，並根據虛擬資產服務提供商之活動協助分類風險最高者。這些工具之運用有成本考量，且並非所有虛擬資產皆為全部供應商所涵蓋。虛擬資產服務提供商及某些金融機構亦廣泛地運用區塊鏈分析以監控其自身暴險（例如藉由混幣器服務或來自私密錢包之虛擬資產移轉）。重要的是，若這些工具得使以其他方式無法獲得之資訊透明化（例



如於公共區塊鏈上），要考量於運用該工具時對隱私及資料保護的任何潛在影響。

235. 取得有關洗錢與資恐風險之資訊是有效風險基礎方法之基礎。建議第 1 項（參照建議第 1.3 項注釋）要求各國，包括監理機關，應持續以適當方法辨識及評估該國之洗錢與資恐風險，以便為金融機構及指定之非金融事業或人員（包括虛擬資產服務提供商）進行防制洗錢／打擊資恐風險評估時提供資訊。各國包括監理機關，應及時更新風險評估，並應建立機制得向所有相關權責機關、金融機構及指定之非金融事業或人員（包括虛擬資產服務提供商）提供評估結果之適當資訊。於某些情形下，某部分之虛擬資產服務提供商部門辨識與虛擬資產商品、服務或活動相關之洗錢與資恐風險之能力可能有所受限，各國，包括監理機關，應與該部門合作以瞭解其風險並協助私部門實體發展其自身對風險之理解。依據虛擬資產服務提供商部門之能力，可能需要一般性資訊或更詳細的資訊及協助。
236. 於衡量個別虛擬資產服務提供商或特定虛擬資產商品、服務或活動時，監理機關應考量與虛擬資產服務提供商之商品及服務、商業模式、公司治理安排、財務及會計資訊、配送渠道、客戶概況、地理位置、運營國家、虛擬資產服務提供商對防制洗錢／打擊資恐措施之遵循程度相關之風險層級，以及與特定虛擬資產代幣或可能混淆交易或破壞虛擬資產服務提供商及監理機關實施有效的防制洗錢／打擊資恐措施之能力相關的風險。監理機關還應檢視虛擬資產服務提供商之控管措施，包括虛擬資產服務提供商之風險控管政策之品質或其內部監督機制之運作情形。其他於防制洗錢／打擊資恐脈絡下可能相關之資訊包括虛擬資產服務提供商的

管理及法遵機能之適合性和適當性。

237. 上述某些資訊可以藉由嚴謹的監理機關（位於虛擬資產服務提供商或其他從事涵蓋的虛擬資產活動之義務實體受嚴謹監管之國家）獲得（例如虛擬資產服務提供商為傳統金融機構須遵守核心原則<sup>52</sup>，如銀行、保險公司、證券商或投資公司），因此會涉及嚴謹的防制洗錢／打擊資恐監理機關間之適當資訊共享及合作，尤其是當權責屬於不同機關時。於其他的監管模式，例如於國家層級重點關注虛擬資產服務提供商之執照或註冊，但於州層級建立共享的監督及執行，而資訊共享應包涵共享審查結果。
238. 如有適用，來自其他利害關係人之資訊，如監理機關（包括海外監理機關及支付系統與工具、證券、商品及其衍生性商品之監理機關）、金融情報中心及執法機關，亦可能有助於監理機關判斷虛擬資產服務提供商有效管理其面臨的洗錢與資恐風險之程度。於某些體制，如僅要求註冊（無需全面的背景查核）之法律制度，可能仍得使執法及監管機關注意虛擬資產服務提供商之存在、其業務範圍、其特定的虛擬資產商品或服務，及／或其控制權益。
239. 監理機關應定期且於虛擬資產服務提供商有重大情事變更或出現相關的新威脅時，檢視其對虛擬資產服務提供商部門及虛擬資產服務提供商兩者之風險概況評估。有關就虛擬資產服務提供商或更廣泛的虛擬資產服務提供商部門之現有國家監理實務案例，以及與特定虛擬資產商品、服務或商業模式相關之洗錢與資恐風險之國家案例，請參照本指引第五部分。

#### ▪ 洗錢與資恐風險之抵減

---

52 依 FATF 建議，「核心原則」係指巴塞爾銀行監理委員會發行之有效監督銀行業務核心原則、國際證監會組織發行之證券規則的目標與原則及國際保險監理官協會所發行之保險核心原則。

240. FATF 建議要求監理機關將更多監理資源分配及優先置於洗錢與資恐風險較高之領域。這意味著監理機關應依據部門及個別虛擬資產服務提供商所面臨之洗錢與資恐風險程度，決定定期評估之頻率及強度。監理機關應優先考量風險較高之潛在領域，諸如個別虛擬資產服務提供商之內部（例如虛擬資產服務提供商可能提供之特定商品、服務或業務線，如特定虛擬資產或虛擬資產服務（如強化匿名加密貨幣或混幣器或轉向器）可能會進一步混淆交易或破壞虛擬資產服務提供商實施客戶審查措施之能力）或特定類型之虛擬資產服務提供商（例如僅或主要促成虛擬對虛擬之金融活動或提供特定虛擬資產混淆商品或服務之虛擬資產服務提供商，或為個人使用者（非為受管制實體之使用者，如接收人機構）或代表其促成虛擬資產移轉之虛擬資產服務提供商），或來自或於高風險司法管轄區營運之虛擬資產服務提供商。若一司法管轄區選擇將一部門全部歸類為較高風險，各國仍應瞭解並得提供一些有關其依據虛擬資產服務提供商之客戶群、其來往的國家及其適用之防制洗錢／打擊資恐控管，而於部門內之個別虛擬資產服務提供商分類之解釋及細節。

241. 同樣重要的是，權責機關肯認於以風險為本之制度中，並非所有虛擬資產服務提供商都會採用相同的防制洗錢／打擊資恐控管，且涉及非法收益的移轉或交換之單一、不知情及獨立的事件並不一定會使虛擬資產服務提供商的防制洗錢／打擊資恐控管的完整性失效。另一方面，虛擬資產服務提供商應瞭解，一個有彈性的風險基礎方法並不能免除其採用有效的防制洗錢／打擊資恐控管。

242. 監理機關得調整其方法之釋例：

a. **調整防制洗錢／打擊資恐監督或監控之類型**：監理機關應採用

異地及現地視查以取得所有相關風險及遵循資訊。然而，於其制度允許之範圍內，監理機關得決定對虛擬資產服務提供商為異場及現地監督或監控之正確調配。於風險較高之情形，僅採異地監督可能並不合適。然而，若先前視查（異地或現地）之監理結果顯示洗錢與資恐之風險較低，則得集中分配資源於風險較高之虛擬資產服務提供商。於此情形，風險較低之虛擬資產服務提供商得採異地監督，例如藉由交易分析及問卷調查。

- b. **調整正在進行之防制洗錢／打擊資恐監理或監控之頻率及性質：**監理機關應按已辨識風險調整防制洗錢／打擊資恐審查之頻率，並結合定期審查及於問題出現時（例如源自可信的吹哨舉報、執法機關之資訊、財務報告分析或其他監理發現）個案之防制洗錢／打擊資恐監理。其他風險基礎方法之監理得包括考量地理位置、註冊或執照狀態、客戶群、交易類型（例如幣幣或法幣交易）、虛擬資產類型、帳戶或錢包數量、收益、提供之商品或服務（例如與混淆交易之商品或服務（如強化匿名加密貨幣）相比，較透明之服務）、不合遵循之歷史紀錄及／或經營管理之重大變更。
- c. **調整防制洗錢／打擊資恐監理或監控及報告要求之強度：**監理機關應按已辨識之風險決定適當之評估範圍或層級，其目標係評估虛擬資產服務提供商之政策及流程（其為防止虛擬資產服務提供商濫用而設計）之妥適性。更密集監理之釋例得包含對系統及檔案進行詳細測試，以驗證虛擬資產服務提供商風險評估之實施及妥適性、報告及紀錄保存政策與流程、內稽、與業務人員、高階管理層及董事會之訪談（如適用）。

243. 監理機關應運用其發現，以檢視及更新其洗錢與資恐風險評估，

並於必要時考量其就防制洗錢／打擊資恐監理及防制洗錢／打擊資恐規則與指引所採之方法是否仍然妥適。如合適且符合與此類資訊保密有關之任何相關標準或要求時，監理機關應將其發現傳達予虛擬資產服務提供商，使虛擬資產服務提供商得加強其風險基礎方法之品質。

▪ 一般性方法

244. 監理機關應瞭解虛擬資產服務提供商面臨之洗錢與資恐風險或與虛擬資產服務提供商部門相關之洗錢與資恐風險。監理機關應就高風險及低風險業務線或特定虛擬資產商品、服務或活動有全面的瞭解，且就高風險之商品、服務或活動有特別透徹之瞭解。
245. 監理機關應確保其職員經過培訓，且具備能力基於虛擬資產服務提供商之風險評估及風險管理程序觀點，評估虛擬資產服務提供商之政策、程序及控管是否適當及合比例。為協助監理機關對虛擬資產服務提供商部門措施的整體強度之瞭解，各國得考慮對虛擬資產服務提供商之防制洗錢／打擊資恐計畫進行比較分析，以進一步為監理機關對個別虛擬資產服務提供商控管品質之判斷提供資訊。
246. 於風險基礎方法之範疇，監理機關應決定虛擬資產服務提供商之防制洗錢／打擊資恐的遵循及風險管理計畫是否足以 (i) 滿足監管要求，及 (ii) 適當且有效地抵減及管理相關之風險。於此過程中，監理機關應考量虛擬資產服務提供商自身之風險評估。就基於多個執照或註冊而得跨越不同司法管轄區營運之虛擬資產服務提供商而言，鑑於涵蓋的虛擬資產活動之跨境性質，執照或註冊自然人或法人虛擬資產服務提供商之監理機關，應考量虛擬資產服務提供商面臨之風險及該風險已充分抵減之程度。

247. 作為其審查程序之一部分，監理機關應傳達其對個別虛擬資產服務提供商之防制洗錢／打擊資恐控管之調查結果及意見，並明確傳達其就虛擬資產服務提供商為遵循其適用的法律及監管框架所需的措施之期望。於虛擬資產金融活動可能涉及多個權責機關之司法管轄區，該司法管轄區內之監管對等單位（如適用）亦應相互協調，以有效且明確地向虛擬資產服務提供商以及其他可能從事虛擬資產活動或提供虛擬資產商品或服務之義務實體傳達其期望。此於以下情況尤為重要：從事各式受監管虛擬資產活動（例如虛擬資產金錢或價值移轉服務或證券、商品或衍生性商品活動）之虛擬資產服務提供商或可能涉及各式銀行、證券、商品、或其他監管機關之虛擬資產金融活動。
248. 若就虛擬資產服務提供商已辨識其防制洗錢／打擊資恐的弱點，監理機關應跟進及評估其為修正缺失及防止再度發生而採取的補救措施之穩固性。就違反監管規定部分，監理機關應具備廣泛範圍的監管／監督措施，得以適用於處理因不遵循而暴露的風險。該範圍可能包括警告、警示函、命令、協議、行政裁罰、處罰及罰款以及對虛擬資產服務提供商活動之其他限制及條件。於風險未抵減之情形，考量已辨識違規行為之嚴重程度，應採取全面性之措施。應優先考量該等使系統面臨最大洗錢與資恐風險之缺失。有關採行具勸阻性、合乎比例及有效處罰之進一步指引，請參照 FATF 風險基礎方法指引 - 金融及執法部門對於防制洗錢及打擊資恐之有效監理與執行。
249. 涉及穩定幣的虛擬資產服務提供商或金融機構應以與虛擬資產或金融資產相同之方式進行適當的監管。如同其他虛擬資產，對其之風險評估應成為此過程的一部分，依監理機關之判斷，穩定幣

可能面臨較高或較低之洗錢與資恐風險，並伴隨著相符之監管類型及強度。若某特定的穩定幣得作為金融資產，則應依該判定以與所有其他相似分類資產之相同方式對其進行監管。有鑑於虛擬資產移轉之跨境性質，虛擬資產服務提供商監理機關之國際合作於此脈絡下極為重要。

▪ 指引

250. 監理機關應傳達其對虛擬資產服務提供商遵循其法律及監管義務之期望，並得考慮與相關利害關係人進行諮詢程序（如有適用）。此類指引可能為下列形式：基於預期結果、以風險為本之義務，以及有關監理機關如何解釋相關立法或法規資訊之上位要求，或是有關虛擬資產服務提供商得如何最佳適用特定防制洗錢／打擊資恐之更詳盡指引。
251. 監理機關及其他權責機關得考量虛擬資產技術專家之指導及意見，以更深入地瞭解虛擬資產服務提供商之相關商業模式及營運、其面臨的潛在洗錢與資恐風險，以及與特定虛擬資產類型或特定涵蓋的虛擬資產活動相關之洗錢與資恐風險，並就現有或所需之抵減措施為基於該瞭解所為之判斷。
252. 如前述，為虛擬資產服務提供商部門提供指引及反饋至關重要，亦為建議第 34 項之要求。該指引得包括使虛擬資產服務提供商得以進行評估並發展風險抵減及遵循管理系統，以滿足其法律及監管義務之最佳實務。協助監理機關與虛擬資產服務提供商間持續且有效的溝通是成功實施風險基礎方法之重要成分。
253. 虛擬資產服務提供商之監理機關亦應考慮與其他相關國內監管及監理機關維持聯繫，以確保其就虛擬資產服務提供商之法律義務解釋具一致性，並促進包括於虛擬資產服務提供商間，及虛擬資

產服務提供商與其他義務實體（如金融機構與指定之非金融事業或人員）間之公平競爭環境。於不只一個監管機關負責監管之情形（例如嚴謹監管機關與防制洗錢／打擊資恐監管機關分置於不同之機構或同一機構下的不同部門），此等協調尤為重要。該協調特別適用於虛擬資產服務提供商提供各式商品或服務或從事不同金融活動，而可能屬於某特定司法管轄區內不同監管或監管機關之管轄權限。多個管轄指導機關不應造成虛擬資產服務提供商間有監管套利、漏洞或不必要混淆的機會。於可能情況下，司法管轄區內相關的監管及監管機關應考慮制定聯合指引。

#### ■ 培訓

254. 從第一線監管機關至經理及董事會成員之各級培訓，對於使監管機關職員瞭解虛擬資產服務提供商部門及現有之各式商業模式，尤為重要。特別是監管機關應確保對職員進行培訓，以評估虛擬資產服務提供商的洗錢與資恐風險評估之品質，並根據其風險評估，考量虛擬資產服務提供商之防制洗錢／打擊資恐政策、程序及內部控管之妥適性、相稱性、有效性及效率。就當前及新興的科技如區塊鏈之培訓或其他分析亦可能有益。
255. 培訓應涵蓋諸如如何與實體互動以及允許監管機關職員對虛擬資產服務提供商風險評估之品質及虛擬資產服務提供商之防制洗錢／打擊資恐控管措施的妥適性及相稱性作成合理判斷等議題。於存在多個權責監管機關或國家監管模式下放或分散之情形，培訓還應旨在實現國家層級監管方法的一致性。
256. 相同地，各國應考慮公私部門培訓與合作之機會，以進一步教育並提高營運及其他權責機關及行業，就與虛擬資產及虛擬資產服務提供商活動相關的各種問題之認識。



## ▪ 資訊交換

257. 公部門及私部門實體間之資訊交換至關重要，應該成為國家於虛擬資產及虛擬資產服務提供商活動脈絡下打擊洗錢與資恐策略不可缺少的一部分。公家機關應於可能情況下分享風險資訊，以更好地為虛擬資產服務提供商之風險評估提供資訊。公部門及私部門實體得共享之與虛擬資產領域風險相關之資訊類型包括：

- a. 洗錢與資恐風險評估；
- b. 洗錢者或資恐者如何濫用虛擬資產服務提供商、特定虛擬資產機制而非其他機制（例如，虛擬資產移轉或交換活動與洗錢或資恐脈絡下之虛擬資產發行活動）或更廣義的虛擬資產之類型及方法；
- c. 關於疑似洗錢或資恐交易報告及其他相關報告的品質及實用性之一般反饋；
- d. 與虛擬資產活動或虛擬資產服務提供商交易相關之可疑指標資訊；
- e. 目標性之非機密情報，於適當情形並具保密協議等相關保障措施；及
- f. 依建議第 6 項之要求，依目標性金融制裁而應遭凍結資產或交易之國家、個人或組織。

258. 此外，各國應考量其如何與私部門實體共享資訊，以幫助私部門實體，包括虛擬資產服務提供商，更瞭解執法資訊請求或其他政府資訊請求之性質，或幫助形塑請求之性質，以便虛擬資產服務提供商得於在適用情況下向權責機關提供更準確及具體之資訊。

259. 銀行、證券、商品及衍生性商品部門之監理機關與虛擬資產服務提供商部門之監理機關間；於執法、情報、金融情報中心及虛擬

資產服務提供商之監理機關間；以及於金融情報中心與虛擬資產服務提供商部門之監理機關間之國內合作及資訊交換，其對於虛擬資產服務提供商之有效監控及監督亦至關重要。

260. 相同地，依建議第 40 項，考慮到虛擬資產服務提供商之跨境性質及多個司法管轄區範圍，政府機關及私部門實體與其國際對等單位間之跨境資訊共享，於虛擬資產服務提供商部門中尤為重要。政府機關還應參考虛擬資產服務提供商監理機關間之資訊共享及合作原則，以獲得有關如何與其對等單位合作之進一步指引（參照第六部分）。

#### 第四部分：FATF 國際標準於虛擬資產服務提供商及從事或提供涵蓋的虛擬資產活動之其他義務實體之適用

261. FATF 建議既適用於國家，亦適用於虛擬資產服務提供商及提供涵蓋的虛擬資產相關服務或金融活動或營運之其他義務實體（「其他義務實體」），包括銀行、證券商及其他金融機構。因此，第四部分提供了針對虛擬資產服務提供商及可能從事涵蓋的虛擬資產活動之其他義務實體之額外指引。
262. 除如建議第 1 項所述，辨識、評估及採取有效行動以抵減其洗錢與資恐風險外，虛擬資產服務提供商及其他義務實體於從事任何涵蓋的虛擬資產活動時，更應採用前述第三部分中建議第 9 項至第 21 項之所有預防措施，此亦包括於客戶審查之情況。同樣地，指定之非金融事業或人員於從事涵蓋的虛擬資產活動時，亦應瞭解其防制洗錢／打擊資恐義務（如建議第 15 項注釋及第 227 至 228 段所述）。
263. 本指引之讀者應注意，以下有關個別預防措施及 FATF 建議之段落旨在為虛擬資產服務提供商及其他義務實體於特定問題上提供額外之具體指引。如第三部分所述，預防措施中缺乏針對每項 FATF 建議之專門段落，舉例而言，不表示其中包含之相應建議或預防措施亦不適用於虛擬資產服務提供商及從事或提供虛擬資產活動之其他義務實體。
264. 一般而言，建議第 9 項至第 21 項中規定之預防措施，以適用於金融機構之方式同樣適用於虛擬資產服務提供商，除兩項例外。首先，虛擬資產服務提供商須進行客戶審查之臨時性交易指定門檻係 1000 美金／歐元（而非 15000 美金／歐元）。其次，建議第 16 項中規定之電匯規則，以經修正之形式適用於虛擬資產服務提

供商及虛擬資產轉帳（「轉帳規則」）。此將詳述於下。

#### ▪ 客戶審查

265. 建議第 10 項規定金融機構必須為所有客戶實施之必要的客戶審查措施，包括辨識客戶並使用可靠、獨立來源文件、數據或資料驗證客戶之身分；辨識實質接收人；瞭解及取得有關業務關係之目的及預期性質之資訊；並對交易之關係及審查進行持續的盡職調查。

#### ▪ 何時進行客戶審查

266. 建議第 10 項亦描述金融機構必須採取客戶審查措施之情形，包括於建立業務關係時、進行臨時性交易且金額逾指定門檻（虛擬資產交易為 1,000 美金／歐元）、進行建議第 16 項及其注釋所述之臨時性電匯交易時（虛擬資產交易亦為 1,000 美金／歐元）、懷疑有洗錢／資恐嫌疑時，或金融機構對先前取得之客戶身分辨識資料真實性及適足性有所懷疑時。雖然各國可能會於其國家法制下就其視為臨時性（如第三部分所述）或為虛擬資產移轉之交易，採行 1,000 美金／歐元之最低門檻，但就適用建議第 16 項而言，所有該等交易都被視為跨境合格電匯，而應該強調的是，銀行、證券商及其他金融機構於從事涵蓋的虛擬資產活動時仍應遵守其各自之客戶審查門檻。就從事涵蓋的虛擬資產活動之指定之非金融事業或人員（如賭場），其應將 1,000 美金／歐元之最低門檻適用於臨時性交易及如第三部分與下文所述之臨時性電匯交易。如第三部分所述，就國家、虛擬資產服務提供商之情形，於接受客戶及促進交易而建立其操作程序及流程時，應考量其如何判斷並確保交易實際上僅為一次性或臨時性，而非立於更常態之基礎（即非臨時性）。

267. 雖然賭場及貴金屬與寶石交易商應對臨時性交易及臨時性電匯交易進行客戶審查之指定門檻分別為 3,000 美金／歐元及 15,000 美金／歐元，但當指定之非金融事業或人員從事涵蓋的虛擬資產或虛擬資產服務提供商活動，其適用建議第 15 項注釋規定之客戶審查標準（即臨時性交易和臨時性電匯交易之最低門檻為 1,000 美金／歐元）。

▪ *如何進行客戶審查*

268. 無論該關係或虛擬資產交易之性質為何，虛擬資產服務提供商及其他義務實體都應具有其有效實施及使用以於風險基礎上辨識及驗證客戶身分之客戶審查程序，包括與客戶建立業務關係時；有洗錢／資恐嫌疑時，無論是否有任何豁免門檻；以及其對先前取得之客戶身分辨識資料真實性及適足性有所懷疑時。

269. 如同其他義務實體，於執行客戶審查以履行建議第 10 項規定之義務時，虛擬資產服務提供商應取得且驗證國家法律要求之客戶身分／驗證資訊。一般來說，要求的客戶身分資訊包括客戶的姓名及其他身分辨識的資訊，例如實際地址、出生日期及一個惟一的國家識別號碼（如國民身分證號碼或護照號碼）。依其國家法律框架之要求，虛擬資產服務提供商亦被鼓勵收集額外資訊，以協助其於建立業務關係時（即初次接受客戶時）驗證客戶身分；為使用帳戶而驗證客戶身分；幫助確定客戶之業務及風險概況，並對業務關係進行持續的盡職調查；及抵減與客戶及客戶的金融活動相關之洗錢與資恐風險。某些虛擬資產服務提供商目前收集的此類額外、非核心身分資訊可能包括，如具相關時間標記之 IP 位址；地理位置資料；設備標示工具；虛擬資產錢包位址；及交易識別碼。

270. 就涵蓋的虛擬資產活動，虛擬資產服務提供商應於建立關係<sup>53</sup>前或期間內完成對客戶及實質接收人資訊之驗證。
271. 若虛擬資產服務提供商不能採行相應層級之客戶審查，建議第 10 項要求虛擬資產服務提供商不得建立業務關係或進行臨時性交易或應終止既存的業務關係；並考慮進行該客戶之相關疑似洗錢或資恐交易報告。
272. 以整體觀之，其於客戶審查措施之適用脈絡下取得之資訊——其可能包括上述傳統資訊及非傳統資訊——虛擬資產服務提供商及其他義務實體應該得於適當案件中準備客戶風險概況。客戶概況將決定可能需要之持續監控級別及類型，並支持虛擬資產服務提供商決定是否建立、繼續或終止業務關係。風險概況得適用於客戶層級（例如交易活動之性質及數量、存入之虛擬資金來源等）或於群體層級，如一群體之客戶顯示同性質特徵（例如客戶從事相同類型之虛擬資產交易或涉及相同的虛擬資產），虛擬資產服務提供商應定期就業務關係更新客戶風險概況，以採行相應的客戶審查級別。
273. 如虛擬資產服務提供商知悉虛擬資產位址，而因疑似洗錢與資恐，其已決定不建立或繼續業務關係或交易，虛擬資產服務提供商應考慮於符合虛擬資產服務提供商之司法管轄區法律下，提供其「錢包位址黑名單」之列表。虛擬資產服務提供商應該可得之錢包位址黑名單審查其客戶及交易對手之錢包位址，作為其持續監控的一部分。虛擬資產服務提供商應進行其自身以風險為基礎的評估，並決定若有出現黑名單上之位址，是否需要採取額外之抵減或預防行動。

---

<sup>53</sup> 請參照 2015 年虛擬資產指引，第 45 段。

274. 如上文建議第 1 項之適用所述，從事涵蓋的虛擬資產活動之虛擬資產服務提供商及其他義務實體得於其國家監管規定允許或要求之範圍內，依與獨立個別的業務關係、商品或服務以及虛擬資產活動相關之洗錢／資恐風險，調整客戶審查措施之程度。因此，如第三節所述，若與業務關係或虛擬資產活動相關之風險較高，虛擬資產服務提供商及其他義務實體必須增加取得之資訊數量或類型，或其驗證此類資訊之程度。同樣地，虛擬資產服務提供商及其他義務實體亦得簡化客戶審查措施之程度，若該與業務關係活動相關之風險較低。但是，虛擬資產服務提供商及其他義務實體不得僅因自然人或法人進行之虛擬資產活動或服務為臨時性或業務量非常有限而採用簡化之客戶審查或免除其他的預防措施（建議第 1 項第 1.6 (b) 項注釋）。此外，每當有疑似洗錢／資恐或適用特定高風險情形時，簡化之客戶審查措施都是不可接受的（請參照第三部分以瞭解潛在高風險情形之解說）。

▪ **持續之客戶審查及監控**

275. 以風險為本之持續監控意味著審查交易以確定該等交易是否與虛擬資產服務提供商（或其他義務實體）關於客戶及業務關係之性質及目的之資訊一致，如有適用。監控交易亦涉及辨識客戶概況之變化（例如，客戶的行為、商品的使用及所涉及之金額）並使其更新至最新狀態，此可能需採取加強客戶審查措施。監控交易是辨識潛在可疑交易（包括於虛擬資產交易脈絡下）的一個重要部分。不符合客戶概況資料預期之行為或偏離通常交易模式之交易可能值得懷疑。

276. 監控應持續進行，亦可能由特定交易觸發。若經常出現大量交易之情形，自動化系統可能為監控交易唯一的實際方法，警示交易

應經人工／專家分析，以確定該等交易是否可疑。虛擬資產服務提供商及其他義務實體應瞭解其操作規則，定期驗證其完整性，並確認其是否已考量與虛擬資產、商品或服務或虛擬資產金融活動相關之已辨識的洗錢／資恐風險。

277. 虛擬資產服務提供商及其他有義務的實體應依其機構風險評估及其個別客戶風險概況（包括其允許之交易類型）調整其監控之程度及範圍（例如，至／自非託管錢包之交易）。若虛擬資產服務提供商評估至／自非託管錢包之移轉之風險不可接受地高，虛擬資產服務提供商可能會考慮選擇對該等錢包加強監控，或限制或不接受與該等錢包之交易。高風險情形（如第二部分及第三部分所述）應被要求加強監控，並延伸及於虛擬資產服務提供商或其客戶或交易對手之間之直接交易。應定期審查監控系統之適足性及導致虛擬資產服務提供商及其他義務實體調整監控程度之因素，以持續符合其防制洗錢／打擊資恐風險計畫。
278. 風險基礎方法下之監控允許虛擬資產服務提供商或其他義務實體設計金額或其他門檻，以確定將審查哪些活動。應定期審查於此用途下之界定條件或門檻，以確定其是否足以對應所建立之風險層級。虛擬資產服務提供商及其他有義務的實體應記錄並明確說明用於客戶分類及為各個客戶群體分配之風險層級之標準及參數（如適用）。用於決定不同客戶（或甚至虛擬資產商品）之監控頻率及強度分類之標準也應該是透明的。為此，虛擬資產服務提供商及其他義務實體應適當地記錄、保留並向相關人員及國家權責機關傳達其監控成果，以及其提出及解決之任何疑問。

▪ **重要政治性職務人士**



279. 建議第 12 項。就國內政府重要政治性職務人士<sup>54</sup>及國際組織重要政治性職務人士<sup>55</sup>，有義務的實體（如虛擬資產服務提供商）必須採取合理措施，以確定客戶或實質接收人是否為國內政府或國際組織重要政治性職務人士，然後評估業務關係之風險。就與國內政府重要政治性職務人士及國際組織重要政治性職務人士之高風險業務關係，虛擬資產服務提供商及其他義務實體應採取與適用於外國重要政治性職務人士之措施相當之額外措施，包括辨識資產來源及資金來源（如有相關）<sup>56</sup>。

#### ▪ 通匯銀行業務及其他相似關係

280. 建議第 13 項。「通匯銀行業務」不包括一次性交易（參照第三部分之建議第 13 項），而係以持續性、重複性為特性。虛擬資產服務提供商應藉由定義及評估其虛擬資產服務提供商交易對手關係之特性，以及其是否正在進行與通匯銀行業務相似之活動，以建立其控制框架。這應包括考量其權責機關對任何已辨識之高風險虛擬資產服務提供商交易對手關係之看法。建議第 16 項中亦列出有關虛擬資產服務提供商交易對手盡職調查流程之進一步資訊。

#### ▪ 電匯及「轉帳規則」

281. 建議第 16 項。如第三部分所述，該領域之提供商應遵循建議第 16 項之要求（即「轉帳規則」）。這包括有義務取得、持有及提交與虛擬資產移轉有關之必要的轉出人及實質接收人資訊，以辨

---

54 「國內政府重要政治性職務人士」係指擔任或受委任擔任本國重要公職之個人，舉例來說，國家或政府之主管、高階政治人物、高階政府、司法或軍事官員、高階國營企業經理人、重要政黨官員等 (FATF 詞彙表)。

55 「擔任或受委任擔任國際組織重要職務之個人」係指資深管理階層成員，亦即董事、代理董事以及董事會或等同性質委員會之成員 (FATF 詞彙表)。

56 進一步資訊請參照 2013 年 FATF 重要政治性職務人士指引 (建議第 12 項及第 22 項)。

識及申報可疑交易，採取凍結行動，並禁止與經指名之人及團體進行交易。這些要求適用於虛擬資產服務提供商及其他有義務的實體（如金融機構）代表客戶發送或接收虛擬資產移轉之情形。

▪ **資料提交技術**

282. FATF 採行技術中立之作法，且沒有規定提供商應設置之特定技術或軟體方法以遵循建議第 16 項。任何技術或軟體解決方案皆為可接受，只要它得使進行匯款及受益機構（若交易中存在）遵循其防制洗錢／打擊資恐義務。舉例而言，用於取得、持有及傳輸必要資訊之解決方案（除遵循建議第 16 項之各式其他要求外）得為內建於虛擬資產移轉之基礎分散式帳本技術交易協定中之代碼，亦得為可於分散式帳本技術平台上運行之代碼（例如，使用智慧合約、多重簽名或任何其他技術）；獨立之（即非分散式帳本技術）消息傳遞平台或應用程式設計界面（API）；或遵循建議第 16 項措施之任何其他有效方法。

283. 此等技術解決方案應使虛擬資產服務提供商得以有效及具效率之方式遵循轉帳規則，並使虛擬資產服務提供商得以進行以下主要行動：

- a. 使虛擬資產服務提供商得以就虛擬資產移轉，定位虛擬資產服務提供商交易對手；
- b. 於分散式帳本技術平台上進行虛擬資產移轉時，得以立即提交必要且正確之轉出人及必要之接收人資訊；
- c. 使虛擬資產服務提供商得以有效穩定之方式，向多個接收位址進行相當大量之交易；
- d. 使虛擬資產服務提供商得以安全傳輸資料，即保護必要資訊之完整性及可得性，以促進記錄保存；

- e. 藉由接受虛擬資產服務提供商或其他義務實體以保護此類資訊之使用，並依國家隱私及資料保護法保護其免於未授權之揭露；
- f. 為虛擬資產服務提供商提供溝通管道，以協助其與虛擬資產服務提供商交易對手之進一步追蹤，以：
  - 對虛擬資產服務提供商交易對手進行盡職調查；及
  - 請求有關特定交易之資訊，以確定該交易是否涉及高風險或禁止之活動。

284. 虛擬資產服務提供商或其他義務實體應實施各式機制，確保有效審查交易以進行疑似洗錢或資恐交易報告，併同將藉由上述資訊基礎設施取得之資訊納入考量。這可以透過結合其他客戶資訊、交易歷史以及其或其虛擬資產服務提供商交易對手自其客戶取得之額外交易資料來達成。虛擬資產服務提供商亦應確保其篩選交易以遵循其制裁義務。有關該過程之進一步資訊載於本指引第三部分就建議第 16 項之討論。當虛擬資產服務提供商或其他義務實體考慮選擇遵循轉帳規則之技術解決方案時，其應該考量上述控制需求。

285. 虛擬資產服務提供商及虛擬資產移轉之其他有義務的實體，無論是作為進行匯款機構或受益機構，都應考量如何運用現存之商業可得技術以遵循建議第 16 項之要求，特別是建議第 15 項注釋第 7 (b) 段之要求。提供商得考量之現存技術作為辨識虛擬資產移轉接收人之基礎，以及於分散式帳本技術平台上進行虛擬資產移轉前近乎即時地傳輸必要轉出人及接收人之示例包括：

- a. 公鑰及私鑰，其係為涉及傳輸之各實體配對而創建，並於傳輸之初始階段加密及解密資訊，以使僅有傳輸之發送者及接收者才得解密及讀取資訊，其中公鑰可供所有人使用，而私鑰僅金鑰之創建者知悉；

- b. 傳輸層安全性協定／安全通訊協定（TLS/SSL）連接，於建立連結時使用各方之間的公鑰及私鑰，並保護網路上幾乎所有之傳輸，包括電子郵件、網站瀏覽，登錄及金融交易，確保於網站伺服器及瀏覽器間傳遞之所有資料維持私密及安全；
- c. X.509 認證，係由認證主管機關管理之數位認證，其使用 X.509 公鑰基礎架構標準以驗證公鑰是否屬於認證之使用者、電腦或服務標識，並於全球之公私部門中使用；
- d. X.509 從屬性認證係得對從屬性（如姓名、出生日期、位址及唯一標識號碼）進行編碼，以加密方式附加於 X.509 認證，並由從屬性認證主管機關管理；
- e. 應用程式設計界面技術，係提供用於建構軟體應用程式之常規、協定及工具，並指定軟體組件應如何互動；以及
- f. 其他商業可得技術或可能的軟體或資料共享解決方案。

▪ **虛擬資產服務提供商交易對手辨識及盡職調查**

286. 並非所有虛擬資產服務提供商皆為相同。其規模從小型獨立企業至大型跨國公司不等。同樣地，沒有一個國家就虛擬資產服務提供商之防制洗錢／打擊資恐制度係完全相同，而各國正以不同的步伐推行其措施。一個部門內之不同實體依各種因素，包括商品、服務、客戶、地理位置、虛擬資產服務提供商司法管轄區內之防制洗錢／打擊資恐制度及實體遵循計畫之強度，將產生較高或較低之風險。虛擬資產服務提供商應分析並尋求瞭解其辨識之洗錢與資恐風險如何影響他們，並採取適當措施以抵減及管理該等風險。是故，風險評估為以風險為本而適用之防制洗錢／打擊資恐措施提供基礎。

287. 只要 FATF 國際標準就虛擬資產服務提供商之部分未於全球實行，管理該等關係將持續構成挑戰。這突顯執行之重要性，亦顯示虛擬資產服務提供商將不得不考慮就執行薄弱之國家採取額外之控制措施，例如對於設於該國之虛擬資產服務提供商之交易進行密集監控、對交易進行金額限制，或進行密集且頻繁之盡職調查。示例包括，虛擬資產服務提供商於其客戶群內限制虛擬資產移轉（即於同一虛擬資產服務提供商內進行虛擬資產之內部移轉）、於其客戶群外僅允許進行已確認之同一人移轉（即轉出人與接收人均確認為同一人）以及加強對交易之監控。否則，虛擬資產服務提供商可能會面臨一個艱難的決定，即是否欲與位於執行薄弱或不執行之國家之虛擬資產服務提供商進行交易。
288. 虛擬資產服務提供商及金融機構應併同 FATF 的通匯銀行業務指引以閱讀本指引。雖然虛擬資產服務提供商交易對手關係可能不是通匯銀行業務關係，但交易對手盡職調查之方法有相似之處，此得以協助虛擬資產服務提供商。故本指引參照建議第 13 項中規定之流程。
289. 於建立新的虛擬資產服務提供商交易對手關係時，虛擬資產服務提供商得直接從虛擬資產服務提供商交易對手取得建議第 10 項及第 13 項規定之資訊。依該等建議之要求，應驗證此類資訊。用於驗證法人及法律協議之身份與實質接收人之潛在可信、獨立之資訊來源之釋例包括：公司登記機關、權責機關之註冊或監管機構名單上執掌之登記機關（例如，各司法管轄區持有之虛擬資產服務提供商清單（如可得））、實質接收人登記機關以及《BCBS 一般開戶指引》<sup>57</sup> 中提及之其他釋例。

---

<sup>57</sup> 附錄四，一般開戶指引，[www.bis.org/bcbs/publ/d505.htm](http://www.bis.org/bcbs/publ/d505.htm)

290. 有關風險層級之潛在資訊來源之示例包括但不限於：母國或往來機構在其進行業務所在國之防制洗錢／打擊資恐法律及規定，以及其適用方式、法律決定及／或監管或執行行動之公開資料庫、已向證券交易所提交之年度報告、衡量遵循及解決洗錢與資恐風險之國際機構（包括 FATF、區域性防制洗錢組織、巴塞爾銀行監理委員會、國際貨幣基金及世界銀行）發佈之國家評鑑報告或其他資訊、FATF 於其國際合作審查小組過程中發佈之清單、知名報紙、期刊或其他電子媒體公開資源、第三人資料庫、國家或跨國家風險評鑑，自往來銀行的管理階層及法遵主管之資訊，以及來自監管及監理機關之公開資訊。
291. 虛擬資產服務提供商需要評估虛擬資產服務提供商交易對手之防制洗錢／打擊資恐控管措施，以避免將其客戶資訊提交予非法行為者或受制裁實體，並應考量是否有合理依據相信虛擬資產服務提供商得妥適地保護敏感資訊。此與 FATF 建議第 13 項第（b）段規定之程序相似，但係更以風險為本之方法。於實務上，此等評估可能涉及審查交易對手之防制洗錢／打擊資恐系統及控管框架<sup>58</sup>。評估應包括確認交易對手之防制洗錢／打擊資恐控管是否經獨立稽核（得為外部或內部稽核）。虛擬資產服務提供商應訴諸於更改流程，包括不發送用戶資訊之可能性，如其合理相信虛擬資產服務提供商交易對手在認為防制洗錢／打擊資恐風險為可接受之情形下，其於後續進行移轉時不會安全地處理該資訊。於此情形下，虛擬資產服務提供商應決定一替代程序，其控管設計得由其監理機關要求時進行適當審查。

---

<sup>58</sup> 舉例而言，沃爾夫斯堡問卷係銀行部門用於履行其通匯銀行業務義務的工具之一。於虛擬資產服務提供商交易對手盡職調查脈絡下，為潛在的框架提供了一個起始點。

292. 為明確起見，虛擬資產服務提供商於向其交易對手傳送必要資訊以遵循建議第 15 項注釋第 7 (b) 段前，需要對虛擬資產服務提供商交易對手進行盡職調查。虛擬資產服務提供商無需就每次虛擬資產移轉皆進行虛擬資產服務提供商交易對手盡職調查流程。但是其應定期或於關係出現風險時更新其交易對手盡職調查之資訊，以確定其是否願意依虛擬資產服務提供商規定之風險基礎方法控管措施向交易對手提交資訊。

▪ **所需資訊之提交**

293. 如建議第 15 項注釋第 7 (b) 段，虛擬資產服務提供商及其他參與虛擬資產移轉之義務實體以安全方式提交所需資訊極為重要，藉此以保護與虛擬資產移轉相關之使用者資訊免於未經授權之揭露，並使收受實體得有效遵循其防制洗錢／打擊資恐之義務，包括辨識可疑之虛擬資產交易、採取凍結行動及禁止與指定人員或實體之交易。此外，業者必須立即提交所需資訊一即，立即或於移轉當時—尤其鑑於其跨境之本質、全球範圍以及虛擬資產活動之交易速度。更多資訊請參見第 III 部分有關轉帳規則之討論。

294. 虛擬資產服務提供商必須提交建議第 16 項注釋規定之與轉帳人及接收人相關之資訊。各國可能對虛擬資產移轉採取最低限度之門檻，低於該門檻者毋須驗證客戶及接收人資訊，除非有洗錢與資恐嫌疑。意即，低於 1000 美元／歐元或等值當地貨幣，或當地規範定義下之臨時性虛擬資產移轉，應適用建議第 16 項注釋之要求，且須提供轉出人及接收人之姓名，以及每個（錢包位址）唯一之交易參考號碼。然而，該等資訊將不會被驗證，除非有與洗錢與資恐相關之可疑情形，而於該情形，與客戶相關之資訊應被驗證。

▪ *虛擬資產移轉予／移轉自未託管錢包*

295. 虛擬資產服務提供商及有義務的實體可能對非有義務的實體（即非託管錢包）為移轉。於該等情形，虛擬資產服務提供商應自其客戶取得所需之轉出人及接收人資訊，理由在於其無從自另一虛擬資產服務提供商獲得相關資訊。該等移轉將落入虛擬資產服務提供商更寬廣之防制洗錢／打擊資恐義務範圍，例如交易監控及目標性金融制裁之遵循。
296. 虛擬資產服務提供商應對虛擬資產移轉予／移轉自非託管錢包及相關點對點交易所生之風險有所認知。基於其匿名性、未設限之可攜性、移動性、交易速度以及可用性，該等交易可能對非法行為人具備吸引力。因此，虛擬資產服務提供商應蒐集其非託管錢包移轉之資料，必要時並應監控及評估該等資訊，以決定該交易在何等程度與其風險胃納相符，適用於該等交易／個人客戶之適當以風險為本之控制，並符合疑似洗錢或資恐交易報告之義務（請參見第 III 部分建議第 20 項）。類似邏輯將用以考量尚未基於防制洗錢／打擊資恐目的，而取得執照／註冊並被監管之虛擬資產服務提供商所形塑之風險，因其係位於尚未實施針對虛擬資產／虛擬資產服務提供商之 FATF 國際標準之管轄區。
297. 虛擬資產服務提供商可能就與未託管錢包之交易，選擇施加額外限制、控制或禁令以符合其風險分析。可能措施包括：
- a. 強化既存之以風險為本控制框架以應對與未託管錢包交易所生之特定風險（例如：考量特定使用者、觀察之行為模式、地區及區域性風險以及來自監管者及執法部門之資訊）；及
  - b. 研究僅接受來自／致虛擬資產服務提供商或其他義務實體，及／或經虛擬資產服務提供商評估為可信賴之未託管錢包之交易之可行性。



#### ▪ 內部控制及外國分公司及子公司

298. 建議第 18 項。為防制洗錢／打擊資恐目的之風險基礎方法之成功實施及有效運作，取決於強而有力的資深管理階層之領導，其中包括監督虛擬資產服務提供商部門整體風險基礎方法之發展及實施。建議第 18 項亦要求團體內部之資訊分享，特別是該等資訊與特定異常交易或活動相關者。
299. 虛擬資產服務提供商及其他義務實體應維持足以管理並抵減其風險之防制洗錢／打擊資恐計畫及系統。防制洗錢／打擊資恐控制之本質及程度取決於數個因素，包括虛擬資產服務提供商業務之本質、規模及複雜性，其營運之多樣性，包括地域多樣性、其客群、商品及活動概況及與個別營運區域相關之風險程度，以及其他因素。

#### ▪ 疑似洗錢或資恐交易報告及揭露

300. 建議第 20 項。參與或提供虛擬資產活動、商品及服務之虛擬資產服務提供商及其他有義務的實體，應具備標記任何異常或可疑金流或交易以進行更深入分析之能力—包括該等涉及或與虛擬資產相關者—或其他顯示可能涉及非法活動之活動，無論該交易或活動之本質為法定貨幣對法定貨幣、虛擬貨幣對虛擬貨幣、法定貨幣對虛擬貨幣，或虛擬貨幣對法定貨幣。虛擬資產服務提供商及其他有義務的實體應有合適之系統，以即時審查該等資金或交易，並確認該等資金或交易是否可疑。
301. 虛擬資產服務提供商及其他有義務的實體應及時報告資金或交易，包括涉及或關於虛擬資產或其提供商，對金融情報中心係屬可疑者，並以權責機關所指定之方式為之。虛擬資產服務提供商及其他義務實體將可疑升級之程序，及最終向金融情報中心之報

告應反映此點。當虛擬資產服務提供商及其他有義務的實體適用政策及程序，以風險敏感性為基礎認為可疑時，即應報告其對洗錢與資恐之懷疑，無論交易之數額或交易是否已經完成。虛擬資產服務提供商及其他有義務的實體報告可疑交易之義務並非以風險為基礎時，報告行為亦不免除其他與防制洗錢／打擊資恐相關之義務。此外，虛擬資產服務提供商及其他有義務的實體應遵循適用之疑似洗錢或資恐交易報告要求，即便其營運橫跨相異之管轄區。

302. 與建議第 15 項注釋相符且與建議第 16 項相關，當虛擬資產服務提供商（或其他有義務的實體）控制匯款與受益雙方之就虛擬資產之資金或電匯，該虛擬資產服務提供商及其他有義務的實體應將所有關於匯款與受益雙方之資訊納入考量，以決定該資訊是否可疑，倘若需要，應對適當之金融情報中心進行疑似洗錢或資恐交易報告，並使金融情報中心取得相關交易資訊。欠缺所需之匯款與受益雙方資訊，應做為涉及虛擬資產或虛擬資產服務提供商之移轉是否可疑，以及其是否因此應向融情報中心申報之判斷因素。此同樣適用於其他有義務的實體，例如參與涉及虛擬資產或虛擬資產服務提供商之移轉之傳統金融機構。
303. 如虛擬資產服務提供商收受來自非屬虛擬資產服務提供商或其他有義務的實體之虛擬資產移轉，而虛擬資產服務提供商要求關於交易對手，或來自其客戶之進一步資訊，其期待該此客戶可及時回應並提供合於其要求詳細程度之文件／資訊。倘該此客戶並未回覆，其可能觸發虛擬資產服務提供商對其客戶無法合理解釋其交易合理性之能力之顧慮，並導致虛擬資產服務提供商考慮就其客戶提交疑似洗錢或資恐交易報告。倘有必要，於要求資訊提供後，得重新評估客戶之屬性及其風險狀況。

304. 更多關於可能暗示犯罪行為之虛擬資產紅旗指標之資訊，載於 FATF 之洗錢與資恐虛擬資產紅旗指標報告。該等指標協助虛擬資產服務提供商及其他義務實體偵測並申報涉及虛擬資產之可疑交易。關鍵指標包括：

- a. 提升匿名性之技術特徵 例如混幣器、轉向器或強化匿名加密貨幣；
- b. 地理風險－罪犯得利用關於虛擬資產之國家措施薄弱或缺乏之國家。
- c. 交易模式－包括建構以規避申報或顯示為不規則、異常或不常見之交易。
- d. 交易規模－倘數量及頻率欠缺有邏輯之商業解釋；
- e. 轉出人或收款人檔案；及
- f. 資金或財富之來源。

## 第五部分：虛擬資產及虛擬資產服務提供商之風險基礎方法國家範例

### ▪ 規範及監理虛擬資產活動及虛擬資產服務提供商之司法管轄方法摘要

305. 第五部分提供數個有關規範及監理虛擬資產金融活動及相關提供商之司法管轄方法概況，包括採用工具或其他措施對未遵守防制洗錢／打擊資恐義務者為裁罰或採取執法行動之方法，各國於發展或強化其自身國家框架時可能須考量上述。部分國家尚未被評估是否遵循建議第 15 項注釋之要求。

### ▪ 義大利

306. 在義大利，2007 年法令第 231 號，經 2017 年法令第 90 號及 2019 年法令第 125 號修正，包括從事由防制洗錢金融行動工作組織定義之五類功能性活動之提供商，為防制洗錢／打擊資恐之義務人。

307. 與虛擬資產相關之服務提供商被要求列於「金融代理和信用中介名單管理機構」（OAM）持有之登記冊之特殊部分。註冊為與虛擬資產相關之服務提供商於義大利從事活動之前提要件。工作正在進行以利登記冊之實施。

308. 虛擬資產服務提供商被認為是有義務的實體，並受全部防制洗錢／打擊資恐措施之拘束。

309. 於 2019 年 3 月 21 日，義大利採用更新之國家風險評估（NRA）。其包括對源自虛擬資產之洗錢與資恐風險之評估。更新之國家風險評估結果將用以強化國家策略。有義務的實體及主體（金融業及非金融業）被要求將更新之國家風險評估結果納入考量，以進行／更新其風險評估。

310. 疑似洗錢或資恐交易報告及由義大利的金融情報中心（UIF）進行進一步分析，使其得以蒐集與下述相關之資訊：i) 於義大利營運之虛擬資產服務提供商，包括商業資料（所提供之服務類型）；地點；接收人、管理人及其他相關主體之資料；ii) 單一交易之詳細資訊（例如日期、數量、執行人、相對人及錢包帳號）；涉及之銀行帳戶之資料（例如持有人、被授權人、資金之來源／用途以及金流之一般屬性）；iii) 客戶或者錢包持有人的個人及經濟概況資料；有助於匹配虛擬資產位址以及虛擬資產所有人身分之資訊；明確之身分資料（例如義大利稅號及增值稅號）；iv) 錢包或帳戶資訊（例如由一個或多個主體所有之虛擬資產全部數量；於特定時段內追溯至相同或相關主體之虛擬貨幣主要動態之詳細資訊；可編輯格式之錢包／帳戶聲明）；及 v) 虛擬資產之類型及主要特性。
311. 自 2015 年起，義大利銀行即警示消費者購買及／或持有虛擬資產有高風險，以及受監管金融中介機構關於虛擬資產之可能風險。其特別發表了對消費者之警示及對受監管金融中介機構之溝通（2015 年 1 月），以及對消費者重述由三個歐洲金融機關—歐洲證券及市場管理局（ESMA）、歐洲銀行管理局（EBA）以及歐洲保險及職業退休金管理局（EIOPA）於 2018 年 3 月發布之新警示。義大利的金融情報中心為強化私部門之參與，於 2015 年 1 月 30 日發布關於加密資產異常使用之溝通，特別針對金融機構（亦即銀行及支付機構）以及賭博業者，並強調該等義務實體有必要將其注意力聚焦於可能之異常交易，例如與加密資產之購買或投資相關之電匯、現金存款與提款、預付卡之使用。

312. 義大利的金融情報中心正進行聚焦於新風險及潛在趨勢之分析。更新之溝通於 2019 年發布以協助義務實體執行其任務。義大利的金融情報中心特別更新其 2015 年關於加密資產異常使用之溝通，提供更多關於重複性要素、操作方法及疑似洗錢或資恐交易報告所辨識之與虛擬資產相關之行為風險概況之細節。該溝通提出以預設疑似洗錢或資恐交易報告格式填寫資料之具體指示，特別是關於：虛擬資產服務提供商、交易、使用者／客戶及錢包／帳戶之資訊。
313. 於 2016 年 12 月及 2018 年 7 月，義大利的金融情報中心發布出現於財務分析過程之去識別化洗錢與資恐案例彙編，其中包括與虛擬資產異常使用相關類型。

#### ■ 芬蘭

314. 虛擬貨幣提供商法案（572/2019）於 2019 年 5 月 1 日生效。虛擬資產服務提供商被要求應於芬蘭金融監理管理局（FIN-FSA）<sup>59</sup> 註冊（授權）。該等業已於法規生效前提供服務者，需於 2019 年 11 月 1 日前註冊。新參與者於開始營運前必須先註冊。虛擬資產服務提供商之定義包括交換（含法定貨幣換虛擬資產，或虛擬資產間交換，及虛擬資產換其他貨物，例如黃金）、託管錢包提供商以及虛擬貨幣發行人。註冊之要求包括基本之妥適性檢查、處理客戶資金之要求及行銷相關之簡單規則（例如提交所有相關資訊之義務及真實資訊義務）。虛擬資產服務提供商為防制洗錢法案（444/2017）所定義之義務實體，並被要求自 2019 年 12 月 1 日起遵循防制洗錢／打擊資恐之義務。

---

<sup>59</sup> [www.finanssivalvonta.fi/en/banks/fintech--financial-sectorinnovations/virtuaalivaluutan-tarjoajat/](http://www.finanssivalvonta.fi/en/banks/fintech--financial-sectorinnovations/virtuaalivaluutan-tarjoajat/)

虛擬資產服務提供商之防制洗錢／打擊資恐風險評估，及其防制洗錢／打擊資恐相關之程序及指引之審查為註冊程序之一部。

315. 芬蘭金融監理管理局就虛擬資產服務提供商活動之特定部分有權發布規範及指引。芬蘭金融監理管理局之規範及指引於 2019 年 7 月 1 日起生效。<sup>60</sup> 該等規範包括對持有及保護客戶資金及客戶及自有資金分離之規範。指引則關注防制洗錢／打擊資恐立法要求之遵循。
316. 該法案之前，芬蘭金融監理管理局自證券市場立法要求及金融工具觀點，與首次代幣發行之發起人合作。目的在辨識虛擬資產何時為金融工具（例如可轉讓證券）。該等評估偶爾仍有需要。為了對擬發行資產之性質進行評估，芬蘭金融監理管理局起草一份於所有首次代幣發行相關查詢適用之檢查表，該檢查表以及關於虛擬資產被頻繁詢問之問題，得於芬蘭金融監理管理局網站取得。<sup>61</sup>
317. 芬蘭金融監理管理局之監理經驗顯示虛擬資產服務提供商現今願意且熱衷於受監管，且試圖獲取監理機關對其活動之認可。虛擬資產服務提供商的挑戰為告知一般公眾，授權並不同於認可。虛擬資產服務提供商曾於開立銀行帳戶面臨挑戰，可用以部分解釋其就監管之態度轉換。

#### ▪ 日本

318. 日本於 2016 年修正支付服務法案及預防犯罪所得移轉法案（PTCP 法案），以回應於 2014 破產之大型虛擬資產服務提供商以及

---

<sup>60</sup> [www.finanssivalvonta.fi/en/regulation/FIN-FSA-regulations/organisation-of-supervised-entities-operations/04\\_2019/](http://www.finanssivalvonta.fi/en/regulation/FIN-FSA-regulations/organisation-of-supervised-entities-operations/04_2019/).

<sup>61</sup> [www.finanssivalvonta.fi/en/banks/fintech--financial-sectorinnovations/virtuaalivaluutan-tarjoajat/frequently-asked-questions-on-virtualcurrencies-and-their-issuance-initial-coin-offering/](http://www.finanssivalvonta.fi/en/banks/fintech--financial-sectorinnovations/virtuaalivaluutan-tarjoajat/frequently-asked-questions-on-virtualcurrencies-and-their-issuance-initial-coin-offering/)

2015 年防制洗錢金融行動工作組織之虛擬貨幣指引。於 2017 年 4 月立法後，日本金融服務廳於 2017 年 8 月建立由防制洗錢／打擊資恐及技術專家組成之虛擬資產服務提供商監督小組。

319. 作為其註冊程序之一部分，日本金融服務廳評估申請人之防制洗錢／打擊資恐計畫，其藉由以文件為基礎之評估及與申請人之非現場或現場面談，聚焦於申請人之風險評估與其商業計畫間之一致性（截至 2021 年 7 月，31 個虛擬資產服務提供商已註冊）。
320. 為確保註冊程序自申請人觀點之可預測性及透明性，於 2018 年 10 月公布申請人於註冊程序被要求填寫之問卷表格。基於過去監督及註冊審查所累積之經驗及瞭解，問卷內容因為部分項目之合併及刪除而有內容上之修訂。其於 2020 年 4 月重新公布，目的在使日本金融服務廳更有效檢視防制洗錢／打擊資恐制度，特別是針對需要強化風險管理之項目。
321. 日本金融服務廳之註冊程序如下：
  - a. 向申請人寄發問卷，該問卷公布於日本金融服務廳網站；
  - b. 基於申請人所提供之答覆，倘有必要，日本金融服務廳將詢問進一步的問題及要求證據；
  - c. 與董事會成員進行面談，以瞭解其關於風險管理及商業計畫之心態。
  - d. 以文件為基礎進行註冊審查，聚焦於：1) 其將處理之虛擬資產風險管理；2) 客戶資產之分離管理；3) 資訊科技系統管理；4) 防制洗錢／打擊資恐制度；5) 委外管理；6) 包括內部稽核制度之商業管理；
  - e. 基於前述程序之結果，日本金融服務廳規定訪視申請人辦公室以驗證規則及政策計畫實施之有效性，特別是申請人之風險管理制度（現場檢查）；及



- f. 一旦日本金融服務廳確認於整體註冊檢查中申請人之營運並無疑慮，日本金融服務廳將接受申請，並允以註冊。
322. 日本金融服務廳每年自義務實體收集防制洗錢／打擊資恐之統計及質性資料，以利日本金融服務廳評估其曝險，並以日本金融服務廳開發之方法對各個義務實體分配風險評級，該評級將用以發展年度非現場監督計畫。例如，日本金融服務廳於 2019 年 3 月前，已對 22 個虛擬資產服務提供商進行現場檢查（包括 13 個當時視為虛擬資產服務提供商者，亦即，於修正法案實施前已為相關營業之實體，被允許為暫時性營運）及施加行政處分（21 個業務改善命令及 6 個業務終止命令及一個拒絕註冊）。
323. 自義務實體收集之原始資料約為 60 個關鍵績效指標資料，該等資料針對個別部門量身定作。日本金融服務廳就虛擬資產服務提供商部門收集以下資訊，而該等資訊為非排他性且為年度修正：
- a. 區塊鏈分析工具是否用於監控交易及／或風險分析目的；
  - b. 提供予虛擬資產服務提供商客戶之虛擬資產類型；
  - c. 混幣器及／或轉向器使用紀錄辨識之客戶數量；
  - d. 熱錢包與冷錢包使用分配之比例；
  - e. 虛擬資產服務提供商是否接受企業客戶作為客戶（帳戶數量、交易價值）；
  - f. 虛擬資產服務提供商是否提供商業支付服務；
  - g. 交易對手之虛擬資產服務提供商之屬性（地理分布及交易量）；及
  - h. 虛擬資產服務提供商管理之虛擬資產 ATM 之數量及地理位置。
324. 日本金融服務廳亦與日本虛擬貨幣交易協會（JVCEA），一個於 2018 年 10 月獲認證之自律團體，密切合作以迅速及彈性回應虛

擬資產服務提供商相關之議題。日本虛擬貨幣交易協會係教育性組織及虛擬資產服務提供商會員之監督組織，其準備關於遵循自我監管防制洗錢／打擊資恐之規則與指引。日本金融服務廳經與日本虛擬貨幣交易協會之諮詢，進行部分與其他機關合作完成之開展活動，與虛擬資產服務提供商共享有助於防制洗錢／打擊資恐遵循之資訊及想法。

325. 此外，日本金融服務廳：

- 於 2018 年 3 月設立「虛擬貨幣交易業務學習小組」，以檢視機構就多個與虛擬資產服務提供商業務相關議題之回應。基於該小組所提出報告之建議，日本金融服務廳於 2019 年 3 月向國會提出修正法案之議案。修正包括：支付服務法案及支付服務法案及預防犯罪所得移轉法案 (PTCP Act) 應適用於就虛擬資產提供託管服務之服務提供商；及考量虛擬資產之匿名性，引介關於虛擬資產服務提供商所處理虛擬資產類型每次更改之事前通知系統。
- 於 2019 年 4 月準備並公布專為虛擬資產服務提供商可疑交易之紅旗指標。該指標涵蓋數種應用匿名技術之交易。

326. 修正之支付服務法案於 2020 年 5 月生效（2019 年 5 月頒布）。依據該修正，所謂之加密資產託管服務，包括代表客戶管理（保管／管理）加密資產及依據客戶指令不經交易移轉至指定位址等，均為本規範之對象。

327. 有關轉帳規則，日本虛擬貨幣交易協會作為日本虛擬資產服務提供商部門之自律組織，其意在藉由修正其自我監管規則及設定目標日期以導入轉帳規則，而日本金融服務廳就此強化與日本虛擬貨幣交易協會間之合作。

328. 於 2021 年 3 月，自確保其業務執行之適當性及可靠性之觀點，日本金融服務廳對日本虛擬貨幣交易協會發布要求，要求其繼續考量轉帳規則之適當實施，解決技術及操作問題，並建立實施轉帳規則之必要系統。
329. 日本金融服務廳就轉帳規則之導入與虛擬資產服務提供商業者進行密集之對話。日本金融服務廳將持續強化該對話，並監督產業就轉帳規則之對應及進度之適當性。

▪ **墨西哥**

330. 在墨西哥，於 2018 年 3 月改革了關於防止及識別非法收益資源之操作之聯邦法，將金融科技機構及信貸機構外之實體所進行之虛擬資產交易定為易濫用活動。
331. 同理，於 2018 年 3 月，墨西哥發布規範金融科技機構之法令，指出金融科技機構得營運虛擬資產業務，倘其已獲得墨西哥銀行之授權且營運所指定之虛擬資產。
332. 其後，於 2018 年 9 月，公布關於虛擬資產之防制洗錢／打擊資恐措施及程序制定之標準。
333. 於 2019 年 3 月，中央銀行發布標準，定義信貸機構及金融科技機構直接或間接偽裝開展虛擬資產營運之內部業務。
334. 中央銀行稱基於虛擬資產於不同國家間移轉之容易性，以及全球層級同質控制與預防措施之欠缺，虛擬資產帶有重要之洗錢與資恐風險。然而，倘科技於金融科技機構及信貸機構內部間使用可能有利，其即致力於促進該等科技之使用。
335. 最終，於稍後之 2019 年 5 月，改革信貸機構法第一百一十五條之一般規定，建立信貸機構必須遵循之虛擬資產相關防制洗錢／打擊資恐義務之措施及程序。

▪ 挪威

336. 自 2018 年 10 月 15 日起，虛擬資產服務提供商受挪威防制洗錢法案及其義務之拘束，與防制洗錢規範相關之規定如下述（最後更新日為 2021 年 5 月 - 非官方翻譯）：

第 5 欄 . 第 1-3 部分 防制洗錢法案適用於虛擬貨幣 -  
交易及託管服務提供商之註冊要求。回顧

- (1) 虛擬貨幣及官方貨幣交易服務提供商為防制洗錢法案下之有義務的實體，倘其為
  - a. 於挪威之商業登記處註冊，或
  - b. 自挪威營運，或
  - c. 直接導向挪威市場。此應同樣適用於虛擬貨幣託管服務。
- (2) 虛擬貨幣為價值之數位表述，並非由中央銀行或政府機關發行，不一定附屬於合法發行之貨幣且不具備貨幣或金錢之法律地位，但被接受為交易方法之一，且可以移轉、儲存或電子交易。
- (3) 虛擬貨幣託管服務為代表客戶保管私有密鑰，以移轉、儲存或交易虛擬貨幣。
- (4) 於第一段提及之提供商，僅能由於金融監理管理局註冊之法律實體提供之。防制洗錢法案第 42 部分第二至四項之規定相應適用。
- (5) 註冊申請必須包括下述之資訊：
  - a. 申請人之姓名
  - b. 企業類型及組織號碼
  - c. 營業地址
  - d. 所提供之服務
  - e. 以下身分者之姓名、居住地址及個人身分號碼或稅號

- a. 總經理或相應職位之人
  - b. 董事會成員或相應職位之人
  - c. 任何其他聯絡人
  - f. 與第四項相符之文件
  - g. 該企業之風險評估及政策及程序，參見防制洗錢法案第 7 及第 8 部分。
- (6) 金融監理管理局得監督第一項所提及之提供商就防制洗錢法案之遵循。
- (7) 金融監理管理局得依規定拒絕未達成防制洗錢法案要求之申請。倘不再符合該等為註冊而設之要求，則金融監理管理局得撤回註冊。

於 2021 年 10 月，九個虛擬資產服務提供商於金融監理管理局註冊並被允許於挪威市場內提供其服務。尚有更多申請者，惟自 2020 年起收受之申請有略微下滑。其中許多為重複申請者，即先前於防制洗錢政策及程序有所欠缺而遭拒絕者。此外，金融監理管理局持續發布數個命令，以停止及終止該等未取得許可而於挪威市場營運者，其中包括內國及外國之虛擬資產服務提供商。未註冊之虛擬資產服務提供商之辨識及關閉，為與金融情報中心更緊密合作及自 2019 年之聯合預防計畫遵循之結果。此外，金融監理管理局於 2021 年 5 月下旬進行首次對虛擬資產服務提供商之檢查，自所有註冊之虛擬資產服務提供商收集額外資料，以進一步譜寫該部門一般風險及所提供服務之範圍。基於註冊意圖之一般性經驗呈現，該部門包括一系列於規模、複雜性、能力、防制洗錢及遵循相關作業之經驗，以及一般專業性間有所差異之參與者。

337. 於瑞典，金融監理管理局自 2013 年起考慮將比特幣及乙太幣作為支付方式，意即專業交易服務將因此受到執照制度之拘束<sup>62</sup>，且於成功申請執照後，將受到防制洗錢／打擊資恐之監理。該規範並非對虛擬資產交易服務之明確防制洗錢／打擊資恐規範（即並未於法規中特別載明），而是其應受監管之隱晦承認。一旦交易服務取得執照，所有活動（即無論係爭虛擬資產）受防制洗錢／打擊資恐之規範及監理之拘束。專案監理已執行，因此部分部門之營運已停止。虛擬資產服務提供商提交疑似洗錢或資恐交易報告予金融情報中心，而營運當局之回饋提出罪犯正選擇將其業務移轉至他處未監管之交易所。

#### ▪ 瑞士

338. 瑞士採取科技中立方法，在市場上虛擬資產相關活動發展之早期階段，即適用既存之防制洗錢／打擊資恐規範制度於虛擬資產及個別之虛擬資產服務提供商。此原則基礎制度之下，所有涉及金融中介且與虛擬資產相關之活動將落入防制洗錢法案（「AMLA」）之範疇。此包括虛擬資產及法定貨幣間及／或一種或多種形式之虛擬資產間之交換活動，任何虛擬資產之移轉活動，虛擬資產或得控制虛擬資產及支付型代幣發行之保管及／或管理活動。

339. 鑒於日益增加之去中心化資產移轉模型，其中有數人協助資產之處置，防制洗錢法令引進定義與虛擬貨幣支付交易相關服務之新標準。因此，除擁有替客戶處置虛擬貨幣之權力，只要與客戶持

---

<sup>62</sup> 自謹慎角度觀之，其並一全面之執照制度，但就防制洗錢／打擊資恐而言，包括對所有者和管理層之適當性測試，及對業務是否依循防制洗錢／打擊資恐監管之評估。

續存有業務關係，倘其協助將虛擬貨幣移轉至第三人，則其為提供虛擬貨幣支付交易相關服務之金融中介。此包括，例如不持有客戶私人金鑰但以智能合約以促成交易之去中心化交易平台，或未直接持有私人金鑰卻仍促成交易之錢包提供商。此一修正應確保瑞士之防制洗錢法案為與虛擬資產相關之未來考驗。

340. 於瑞士展開此類業務前，任何作為金融中介機構或為防制洗錢法案所拘束之自然人或法人，必須持有審慎瑞士金融市場監督局執照（即銀行業執照），或成為監理組織（「SO」）或自我監管組織（「OAR」）之成員，兩者均由瑞士金融市場監督局監管。洗錢防制條例（「AMLO」）涵蓋於或來自瑞士活動之金融中介。

341. 瑞士金融市場監督局不斷警告消費者關於加密資產，及相關活動例如首次代幣發行之特定風險。就其監理，瑞士金融市場監督局早期聚焦於虛擬資產相關之主題。例如，瑞士金融市場監督局於2019年傳達其對轉帳規則之期待。於瑞士，金融中介於提供至或來自非託管錢包之移轉時，亦需符合轉帳規則之要求。此外，受監理實體（即銀行）就虛擬資產相關要求之實施，亦受到瑞士金融市場監督局之評估。

## ▪ 美國

### ▪ 全面且科技中立之架構

342. 美國擁有用以規範及監理「數位資產」<sup>63</sup> 防制洗錢／打擊資恐之全面且科技中立之規範及監理框架，其涵蓋提供商及該領域之活動，以使其與非數位資產之提供商於既有金融機構防制洗錢／打

---

<sup>63</sup> 自美國觀點，「數位資產」一詞為系列於數位金融服務生態系統之資產之泛稱，包括數位貨幣—涵蓋國際數位貨幣及非由國家政府發行或保證之數位貨幣，例如可轉換虛擬貨幣如比特幣—以及作為證券、商品或衍生性商品之數位資產。

擊資恐規範框架下受大致相同之監管。美國之作法參考了多個部門及機構之工具及權責，包括美國金融犯罪執法局（FinCEN）、美國金融情報中心、美國主要防制洗錢法管理者、銀行保密法（BSA）；美國海外資產控制辦公室（OFAC）；美國國稅局（IRS）；美國證券交易委員會（SEC）；美國商品期貨交易委員會（CFTC）；美國司法部（DOJ）及其他部門及機構。金融犯罪執法局、國稅局、證券交易委員會以及商品期貨交易委員會與美國司法部，尤其具備監管、監理及執行權責以監督涉及匯款之特定數位資產活動；證券、商品或衍生性商品；或與稅收相關者，其亦具備抵減數位資產濫用以進行非法金融交易或逃稅之權責。

343. 當個人（美國規範定義下超出自然人及法人範疇之術語）參與涉及數位資產之特定金融活動，防制洗錢／打擊資恐及其他義務將有適用。視其活動，該個人或機構將作為匯款服務業者、國家證券交易所、證券商、投資顧問、投資公司、轉讓登記代理人、指定合約市場、互換交易平台、衍生性商品結算機構、期貨經紀商、期貨基金經理人、商品交易顧問基金、交換買賣商、主要交換契約參與者、零售外匯經紀人及介紹經紀商，受監理機關如金融犯罪執法局、證券交易委員會及／或商品期貨交易委員會之監理。
344. 倘該個人落入「銀行」之規範性定義，金融犯罪執法局及美國聯邦銀行業機構—聯邦儲準備系統之理事會、聯邦存款保險公司、通貨監理署辦公室及國家信用管理協會—有時與銀行業州監管者同時，有權規範及監管參與涉及數位資產金融活動之個人。此外，既有之一般性稅務原則適用於美國境內涉及數位資產之交易，因美國國稅局將其歸類為財產。



第 6 欄 . 案例研究：美國對數位資產相關提供商之規範及監理  
(包括執照及註冊)

**資金移轉。**於聯邦層級，金融犯罪執法局將任何從事收受及移轉價值業務者作為匯款服務業者監管，無論其為實體或虛擬，凡以任何方法於個人間或位址間替換貨幣（包括可轉換虛擬貨幣，無論虛擬貨幣間互換、虛擬貨幣換法定貨幣或虛擬貨幣與其他價值互換）者均屬之。銀行保密法之下，匯款服務業者必須於金融犯罪執法局註冊為金錢服務業務並建立防制洗錢計畫、記錄保存及申報措施，包括填寫疑似洗錢或資恐交易報告。防制洗錢要求於內國及外國之匯款服務業者同樣適用，即便位於外國之實體並未物理上存在於美國，且無論其於何處設立或總部位於何處，只要其於美國之全部或特定部分從事業務為已足。自 2014 年起，美國國稅局及金融犯罪執法局對多個數位資產相關提供商進行檢查，包括管理者、部分依規模為最大之交易商、以替他人交易為業務之個人、外國之交易商、數位資產／加密貴金屬交易商、自助服務公司及諸多交易平台以及註冊與未註冊之金融機構。適用之州法亦要求相關之涵蓋實體於大多數其營運之州取得州匯款服務業者執照，無論其公司設立之司法管轄區或總部之物理位置為何。視其所位於或從事業務之州，以及其營運是否使其為其他美國監理組織之規範對象，匯款服務業者亦可能受其他監理要求之拘束，其中包括安全性、穩健及資本公積要求。

**證券活動。**按數位資產於美國屬於證券，美國證券交易委員會就其募集、銷售、交易、其他金融服務以及與該等數位資產相關之行為有監管及執法之權力。作為證券之數位資產於次級市場交易之平台，必須註冊為國家證券交易所或被豁免註冊以營運，例如美國證

券交易委員會關於替代性交易系統要求（即美國證券交易委員會規範替代性交易系統）之豁免，並申報關於其營運及交易之資訊予美國證券交易委員會。縱使該證券交易所、證券商、投資顧問或其他證券相關實體為坐落於外國之個人，且未物理上位於美國境內，倘其對美國人募集、銷售或從事與證券（包括為證券之數位資產）相關活動或影響美國證券交易市場，其仍可能為美國證券交易委員會之規範及司法管轄權所拘束。視該實體涉及之活動及進行該活動之州，額外之州執照義務可能有適用。如上述，包括於平台上交易之數位資產特定交易，仍可能於銀行保密法及州法或規範下被界定為資金移轉。倘該數位資產為證券，則其為美國證券交易委員會司法管轄權所拘束，該證券之任何衍生性商品亦為美國證券交易委員會司法管轄權所拘束。

**商品及衍生性商品活動。**在美國，數位資產可能為商品交易法<sup>64</sup>定義下之商品。因此美國商品期貨交易委員會將通案對數位資產之衍生性商品，包括期貨、選擇權及該數位資產之交換有監管之司法管轄權。此外，美國商品期貨交易委員會就此類非證券之數位資產銷售有廣泛之反詐欺及反操縱權力。依據商品交易法及相關規範，美國商品期貨交易委員會擁有廣泛之權力，對位於美國境內或境外涉及或參與非屬證券商品之數位資產相關詐欺或操縱活動之個人及實體採取行動（例如美國商品期貨交易委員會 v. Blue Bit Banc 案）。

---

<sup>64</sup> 美國商品期貨交易委員會決定「虛擬貨幣」為商品交易法章節 1a (9) 定義下之商品。In re Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15 29, 2015 WL 5535736, [ 現行移轉暫保單 ] Comm. Fut. L. Rep. (CCH) paragraph 33,538 (CFTC Sept. 17, 2015) ( 同意令 ); In re TeraExchange LLC, CFTC Docket No. 15 33, 2015 WL 5658082, [ 現行移轉暫保單 ] Comm. Fut. L. Rep. (CCH) paragraph 33,546 (CFTC Sept. 24, 2015) ( 同意令 ) .

一般而言，交易證券、商品或衍生性商品之自然人或法人受自律組織之額外監督。證券活動要求於金融業監管局（FINRA）註冊，而商品及衍生性商品活動被要求於國家期貨協會（NFA）註冊。視其活動，該自然人或法人可能需要於金融業監管局及國家期貨協會雙重註冊，依據美國聯邦證券及商品法兩者皆具備法定義務。此外，與匯款服務業者執照相類似，自然人或法人必須於其從事業務之州向每個州監管者取得執照。

美國證券交易委員會及美國商品期貨交易委員會之特定註冊者，仍可能有銀行保密法下之義務，包括建立防制洗錢計畫、向金融犯罪執法局申報可疑活動、辨識及驗證客戶身分，及對涉及外國人之特定帳戶適用加強盡職調查。相關之規範及監理組織亦監督數位資產活動，並檢視註冊者就規範義務之遵循，包括（對特定註冊者）銀行保密法下之防制洗錢／打擊資恐義務。

#### ▪ 美國執法、裁罰及其他執行能力

345. 美國之執法利用來自金融犯罪執法局之金融情報資訊，及其他資訊以對涉及數位資產者進行調查。來自金融犯罪執法局之資訊一源自金融犯罪執法局所收集並傳送予美國執法主管機關之報告及分析一就建立犯罪活動之證據及辨識可能涉及洗錢或資恐活動之個人有所助益。金融犯罪執法局就廣泛之金融、管理及執法資訊有取得途徑。金融犯罪執法局所處理之資訊，包括兩個有助偵測涉及數位資產之可疑洗錢或資恐之重要部分資訊：(i) 由申報金融機構填寫之可疑活動申報（或疑似洗錢或資恐交易報告），例如於數位資產交易所移轉法定貨幣以轉換或交易為數位資產或相關業務，或於數位資產轉換或交易後自數位資產交易商收受法定貨

幣或相關業務之銀行或證券商；及 (ii) 由數位資產提供商填寫之疑似洗錢或資恐交易報告，其通常作為匯款服務業者營運，收受資金並將其轉換為數位資產或允許儲存及／或為數位資產之交易或交換。金融犯罪執法局亦收集其他資訊，例如外國銀行帳號、貨幣及金錢工具及貨幣交易報告—以上皆可能包括用以制止及追訴與數位資產相關犯罪活動所必要之調查線索及證據。

346. 美國部門及機關已經於行政程序及聯邦法院採取強力之民事及刑事執法行動，以打擊與數位資產相關之非法活動，例如尋求多種形式之救濟，包括停止及終止命令、禁制令、遲延利息之追繳、對故意違法行為之民事違約金及涉及沒收與拘禁之刑事處刑。<sup>65</sup> 美國監理機關及監管機關彼此間及州監理機關、美國司法部及其他執法機關間廣泛合作，以支持數位資產領域之調查及追訴工作。
347. 存在多樣之刑事及民事權責機關、政策工具及法律程序，以協助美國政府機構辨識非法之數位資產相關活動、將交易歸於特定個人或組織、抵滅威脅及就各自之監管或犯罪調查職能進行分析。關於該等調查及起訴，美國司法部仰賴一系列法定刑事及民事權責機關，包括管理洗錢之聯邦法、金錢服務業務註冊、金融機構記錄保存及申報要求、詐欺、逃稅、銷售受控管物質及其他非法物品及服務、電腦犯罪及資恐。美國已以違反銀行保密法或洗錢，控訴及起訴以個別「點對點」交易商營運之個人，以及違反美國法之外國個人或組織，並為其他與數位資產相關之起訴。

---

<sup>65</sup> 自美國執法、調查、及／或制裁行動挑選之案例包括：2015 年對 Ripple Labs, Inc. 之民事金錢裁罰；2016 年 Operation Dark Gold；2017 年對 BTC-e 之民事金錢裁罰及同時起訴 Alexander Vinnik；2017 年資恐案件，U.S. v. Zoobia Shahnaz；2018 年對 unlicensed bitcoin trader 之判刑；及 2019 年對有關 OFAC SamSam designation 數位貨幣位址之辨識。

348. 與金融犯罪執法局、證券交易委員會及商品期貨交易委員會相似，美國司法部對違反美國法之數位資產提供商及個人具有廣泛之起訴權力，即便其可能並非位於美國境內。例如，倘若數位資產交易涉及美國境內之金融、數據儲存或其他電腦系統，則美國司法部就指揮或進行該等交易之人具備司法管轄權進行起訴。美國對於利用數位資產將非法商品或違禁品輸入美國，或利用美國境內數位資產業務或提供商或金融機構進行洗錢之境外之人，亦有司法管轄權進行起訴。此外，對美國居民提供非法服務、詐欺或竊盜之境外之人，亦可能因為違反美國法而被起訴。
349. 外國資產控制辦公室通常與其他機關協商，管理美國金融制裁及相關之執照、規範及處罰，且以上皆與數位資產及大部分之其他資產類型相關。外國資產控制辦公室明確表明，無論交易是以數位資產（無論國家數位貨幣或非國家數位貨幣例如可轉換虛擬貨幣如比特幣）或傳統法定貨幣計價，美國制裁之遵循義務是相同的，且美國人及其他受外國資產控制辦公室司法管轄權之約束者，有責任確保其並未參與外國資產控制辦公室制裁所禁止之未經授權交易。外國資產控制辦公室 2020 年 12 月之執法行動，及對虛擬資產服務提供商未能遵循之有關罰款，為對此之進一步確認。<sup>66</sup>

▪ **國際合作係屬關鍵**

350. 數位資產生態圈之固有全球化特質使數位資產活動特別適合進行及促進本質上為跨國之犯罪。客戶及服務得在幾乎不涉及國界之情形下交易及營運，創造司法管轄之障礙。有效打擊涉及數位資產之犯罪活動需要緊密之國際夥伴關係。

---

<sup>66</sup> [https://home.treasury.gov/system/files/126/20201230\\_bitgo.pdf](https://home.treasury.gov/system/files/126/20201230_bitgo.pdf).

351. 美國部門及機構，特別是美國之執法單位，與外國夥伴就涉及數位資產活動之案件密切合作，以進行調查、逮捕及扣押犯罪資產。美國鼓勵該等夥伴關係支持跨司法管轄之調查及起訴，尤其涉及位於外國之人、數位資產提供商及跨國犯罪組織者。雙向之司法互助請求對強化合作仍為關鍵機制。因不法份子得迅速銷毀、毀滅或隱匿數位資產及相關證據，美國已建立取得證據及限制外國資產之政策，並認知數位資產及相關交易數據及證據，可能經由現行法律方法及條約未慮及之技術方法及程序儲存或定位。

## 第六部分：虛擬資產服務提供商監理機關之資訊共享 及合作原則

352. FATF 建議鼓勵進行最廣泛之國際合作。建議第 15 項注釋稱各國應以建議第 37 至 40 項為基礎，迅速、有建設性且有效地提供與虛擬資產相關之洗錢、前置犯罪及資恐最盡可能廣泛之國際合作。特別是虛擬資產服務提供商監理機關應及時且有建設性地與外國對等單位交換資訊，無論監理機關之本質或狀態，以及其關於虛擬資產服務提供商之命名及狀態之差異。更多關於建議第 37 至 40 項適用於虛擬資產之資訊，如上述第三部分說明。

### ▪ 目標

353. 各國應指派至少一個主管機關作為其於防制洗錢／打擊資恐目的下對虛擬資產服務提供商之監理機關。除特別指出主管機關不能為自律團體之外，FATF 國際標準並未指出主管機關應為何者。各國指定不同機關作為虛擬資產服務提供商之監理機關，包括金融服務監理機關、中央銀行、證券監理機關、稅務機關、金融情報中心及專門之虛擬資產服務提供商監理機關。部分國家採單一監理機關，而其他則有數個監理機關。部分國家將虛擬資產服務提供商視為得清楚辨識之特定業務類型，然而其他則將虛擬資產服務提供商視為既存業務類型（即金錢服務業務）之子類型。

354. FATF 國際標準清楚指出監理機關應與其外國對等單位及時且建設性地交換資訊，無論監理機關之本質或狀態，以及其關於虛擬資產服務提供商之命名或狀態之差異。鑒於虛擬資產之匿名性、快速性及跨境之本質，國際合作就虛擬資產服務提供商監理機關間至關重要。為了促進對等單位間的運作及相關資訊交換，FATF

發展了虛擬資產服務提供商監理機關間之資訊共享及合作原則。  
該原則擬在：

- a. 提供監理資訊類型之一般認識，以及其他有助於機關間互相分享資訊或何時應分享該等資訊之背景知識；
  - b. 概述有關主動資訊共享／要求之可能觸發時點，例如當網路安全事件發生，而對於其他司法管轄區有潛在之防制洗錢／打擊資恐影響，或當外國虛擬資產服務提供商於某司法管轄區內可能從事未受監管之虛擬資產服務提供商活動時。
  - c. 列出於特定情形（須符合保密規定）可能採取之監理協助／回饋之可能分享方法及類型；
  - d. 列出數個防制洗錢／打擊資恐監理機關於特定案件或議題共同合作之可能角色及期待；
  - e. 對司法管轄區就無既有監管框架之司法管轄區之虛擬資產服務提供商處理爭議時，或尋求對有複數司法管轄權之虛擬資產服務提供商進行監理合作時，提出可能之指引。
    - 提出與各國就取得執照／已註冊之虛擬資產服務提供商應維持之資訊類型相關之最佳實務，並作為其各自名錄或網站之一部分。
355. 該等原則對於監理機關並無拘束性，其意在作為監理機關之指引。監理機關並無義務採取及實施該等原則，亦無義務分享資訊或進行合作，除非與其內國框架相一致（可能於採用如備忘錄之法律安排情況下進行有條件之合作及資訊交換），且未與源自建議第37-40 項之義務相衝突。
356. 然而，該等原則得適用於所有國家，無論其是否允許或者禁止虛擬資產服務提供商。禁止虛擬資產服務提供商之國家，必須有允



許其相關主管機關就與虛擬資產及虛擬資產服務提供商相關資訊進行交換之法律基礎。該主管機關可能並非監理機關，但舉例而言可能為執法機構。

#### ▪ 資訊共享及合作原則

357. 應鼓勵監理機關間基於互相信賴之基礎上之國際合作。資訊共享安排必須被認可，並允許就特定問題之個案解決空間。

#### ▪ 監理機關及虛擬資產服務提供商之辨識

1. 各國為防制洗錢／打擊資恐目的必須清楚辨識其關於虛擬資產服務提供商之監理機關。倘一個國家有數個監理機關，該國應清楚辨識各監理機關之監管職權範圍。
2. 監理機關應有明確機制，以收受關於虛擬資產服務提供商之詢問。例如，此可能為專為虛擬資產服務提供商相關詢問使用之特定電子郵件地址。
3. 為促進及時合作，監理機關應確保其管轄範圍內取得執照或已註冊之虛擬資產服務提供商資訊得為外國機關使用。舉例而言，此得經由刊印義務實體之公開名冊，或維護可經由安全資訊交換進行查詢之取得執照／已註冊實體之資料庫而達成。

#### ▪ 資訊交換

4. 監理機關應與外國監理機關交換虛擬資產服務提供商之相關資訊，無論其地位為何。為此，監理機關就洗錢、相關前置犯罪及資恐進行合作，應具備充足之法律基礎。
5. 關於監理資訊之交換有多種可能方法。最常見者，基於一方監理機關對他方之請求，資訊以雙邊形式交換。如虛擬資產服務提供商本質上為多邊，監理機關亦得決定與其他所有虛擬資產服務提供商監理機關多邊地交換資訊。最後，如有需要，得於多邊虛擬

資產服務提供商之領導監理機關組織之聯合監管機制分享較不敏感之監理資訊。考量虛擬資產服務提供商之跨境本質，建立對較大型之多邊虛擬資產服務提供商之聯合監管機制，有助於提升對該等實體之整體防制洗錢／打擊資恐監理。

6. 監理機關間交換之資訊類型將取決於一系列因素，例如交換資訊之觸發時點、監理機關協助取得之法定及／或區塊鏈資料，以及各國之內國法制框架。如可取得且於法所許，監理機關應提供相關資訊，例如虛擬資產服務提供商之監管狀態、其股東及董事之細節、交易相關資料及使用者資訊（可能藉由監理活動、法定申報、區塊鏈監測及分析工具取得）。如有必要，監理機關應考量行使其監理權力，以自虛擬資產服務提供商取得進一步資訊。
7. 要求資訊之監理機關應向將負責處理該要求之監理機關揭露該要求之理由，盡可能提出該等資訊之使用目的，並提供充足資訊以使收受要求之監理機關得以合法地提供資訊。
8. 監理機關應確認收受請求、回應資訊請求，並及時提供過渡之部分或否定回應。
9. 監理機關不應禁止或就資訊交換或提供協助設定不合理或不正當之限制條件。特別是監理機關不應以下列理由拒絕協助之請求：
  - a. 法律要求金融機構、指定之非金融事業或人員或虛擬資產服務提供商（除所尋求之相關資訊為法律特權或法律專業保密適用之情況下所持有者）維持秘密性或保密性。
  - b. 收受請求之國家正進行詢問、調查或程序，除非該等協助將妨礙該詢問、調查或程序；及／或
  - c. 提出請求之對等機關之本質或法律地位與其外國監理機關相異。

10. 由提出請求之監理機關所收受、處理、持有或傳播之資訊，必須被安全地保護、交換，並僅依據合意之程序、政策及適用之法律及規範下使用。
11. 交換之資訊應僅於尋求或提供之目的下被使用。向其他機關或第三人提供資訊，或基於行政、調查、起訴或司法目的使用該等資訊，而超出原始核准範圍者，應事先取得被請求監理機關之授權。最低限度為，請求資訊之金融監理機關應及時告知被請求之監理機關其向第三人揭露或申報該等資訊之法律義務。
12. 監理機關應主動對其他監理機關提出重大問題及疑慮，並於面對該等問題及疑慮時及時並以適切方法回應之。
13. 監理機關應考慮主動分享資訊或於必要時要求資訊，以執行其監理機能。該等請求之可能觸發時點包括：
  - a. 當地虛擬資產服務提供商發生網路安全事件，對其他司法管轄區有潛在之防制洗錢／打擊資恐影響；
  - b. 坐落於外國之虛擬資產服務提供商可能於某司法管轄區內進行未受監管之虛擬資產服務提供商活動；及
  - c. 當地虛擬資產服務提供商被強烈懷疑進行非法洗錢與資恐活動，且其於外國司法管轄區內有實質之營運。
14. 於被請求時及任何可能情形，監理機關應就所提供資訊之使用，以及基於分析所提供資訊而獲得之結果，提供回饋予外國對等單位。
15. 監理機關應及時與其他虛擬資產服務提供商相關監理機關，就現正浮現有重大及潛在不利益性質之爭議及發展為溝通，包括監理行動。

16. 除非監理機關認為不適當之異常情形，監理機關應與其他虛擬資產服務提供商相關監理機關分享影響後者負責之受監管實體資訊，包括監理行動。

▪ 合作

17. 於某些情形下，倘虛擬資產服務提供商之業務營運有重要比例位於特定司法管轄區，則可以辨識其主要監理機關。監理機關間應共同合作，以辨識出可以做為主要機關以協調資訊分享及合作之主要監理機關，該等辨識並非強制性，亦未免除其他監理機關於其各自司法管轄區監理虛擬資產服務提供商之責任。
18. 監理機關應以最有效方法為合作。倘雙邊或多邊協議或安排為必要，例如諒解備忘錄（MOU），應於打擊洗錢、相關前置犯罪及資恐之國際合作脈絡下，與盡可能廣泛之外國監理機關及時談判並簽署之。
19. 監理機關應能代表外國監理機關從事查詢，並與該等外國監理機關交換所有如於其國內查詢能夠獲得之資訊。
20. 於請求合作時，監理機關應盡其最大努力提供完整、真實及適當之法律資訊，包括對系爭案件之描述。此包括表示為緊急之任何需求，以及時並有效地執行合作請求。

## ▪ 附件 A. 建議第 15 項及其注釋及 FATF 定義

### ▪ 建議第 15 項 - 新技術

各國與金融機構應辨識及評估源自與 (a) 新商品及新業務作法，包括新傳輸機制，及 (b) 同時用於新的及既存商品兩者之新的或開發中技術相關之洗錢或資恐風險。就金融機構而言，該等風險評估應先於新商品之發行、業務營運或者新的或發展中技術之使用。其應採取適當方法以管理並抵減該等風險。

為了管理及抵減源自虛擬資產之風險，各國應確保虛擬資產服務提供商於防制洗錢／打擊資恐目的下受監管，且取得執照或註冊，及為監測及確保遵循 FATF 建議下相關措施之有效系統所約束。

### ▪ 建議第 15 項注釋

1. 為了適用 FATF 建議，各國應將虛擬資產認定為「財產」、「收益」、「資金」、「資金或其他資產」或其他「相對應價值」。各國應適用 FATF 建議下對於虛擬資產及虛擬資產服務提供商之相關措施。
2. 依據建議第 1 項，各國應辨識、評估及理解源自虛擬資產活動，及虛擬資產服務提供商活動或營運之洗錢及資恐風險。基於該評估，各國應適用風險基礎方法，以確保用以預防或抵減洗錢及資恐之措施與已辨識風險相稱。各國應要求虛擬資產服務提供商辨識、評估及採取有效行動以抵減其洗錢及資恐風險。
3. 虛擬資產服務提供商應被要求取得執照或註冊。於最低程度，虛擬資產服務提供商應被要求於其設立之司法管轄區內取得執照或註冊<sup>67</sup>。如虛擬資產服務提供商為自然人，其應被要求於其營業

---

<sup>67</sup> 所稱法人之設立包括公司設立或任何其他使用之機制。

地點所在之司法管轄區取得執照或註冊。各司法管轄區可能亦要求於其管轄區內向客戶提供商品及／或服務，或自其管轄區從事營業之虛擬資產服務提供商於該管轄區內取得執照或註冊。權責機關應採取必要之法律或規範措施以預防罪犯，或其同夥持有或成為重要或控制利益之實質接收人，或持有虛擬資產服務提供商之管理功能。各國應採取行動以辨識未取得執照或註冊而從事虛擬資產服務提供商活動之自然人或法人，並適用適當之裁罰。

4. 各國毋須就已於該國取得執照或註冊為金融機構（如 FATF 建議所定義）之自然人或法人，另行賦予執照或註冊系統，如於該等執照或註冊下，其被允許從事虛擬資產服務提供商活動，且已經為 FATF 建議下所有適用義務所約束。
5. 各國應確保虛擬資產服務提供商被充分之規範及防制洗錢／打擊資恐目的下之監理或監管所約束，且有效實施相關之 FATF 建議，以抵減源自虛擬資產之洗錢及資恐風險。虛擬資產服務提供商應為監控及確保符合該國防制洗錢／打擊資恐要求之有效系統所約束。虛擬資產服務提供商應由權責機關（非自律團體）監理或監控，該權責機關應以風險為本進行監理或監控。監理機關應有充足之權力為監理或監控，並確保虛擬資產服務提供商遵循打擊洗錢及資恐之要求，其權力亦包括進行檢查、強制提供資訊及施以裁罰。監理機關應有權實施一系列之懲戒及經濟裁罰，包括撤回、限制或暫停虛擬資產服務提供商執照或註冊之權力，如有適用。
6. 各國應確保其依據建議第 35 項，有一系列有效、合比例且具勸阻性之裁罰，無論為刑事、民事或行政，得適用於未能遵循防制洗錢／打擊資恐要求之虛擬資產服務提供商。裁罰不應僅適用於虛擬資產服務提供商，亦應及於其董事及高階經理人。

7. 關於預防性措施，建議第 10 至 21 項所示之要求對虛擬資產服務提供商有適用，惟應受下述之限制：
8. (a) 建議第 10 項 - 臨時性交易指定門檻為 1000 美金／歐元，超過該門檻虛擬資產服務提供商應進行客戶審查。
9. (b) 建議第 16 項 - 各國應確保為轉出人之虛擬資產服務提供商取得且持有必要且正確之轉出人資訊，及必要之有關虛擬資產移轉之接收人資訊<sup>68</sup>，並立即且安全地向受益虛擬資產服務提供商或金融機構（如有）提交<sup>69</sup>上述資訊，並於適當機關要求時提供。各國應確保受益虛擬資產服務提供商取得並持有必要之轉出人資訊，及必要且正確之有關虛擬資產移轉之接收人資訊，並於適當機關要求時提供。建議第 16 項之其他要求（包括資訊可利用性之監控，及採取凍結行動及禁止與經指名之人或團體交易）將於第 16 點所揭示之相同基礎下適用。如金融機構代表客戶匯出或收受虛擬資產之移轉，相同義務將有適用。
10. 各國應依建議第 37 至 40 項所揭示之基礎，快速、具建設性且有效地提供最盡可能廣泛程度與虛擬資產有關之洗錢、前置犯罪及資恐相關之國際合作。特別是，虛擬資產服務提供商之監理機關應及時且具建設性地與外國對等單位交換資訊，無論該監理機關之本質或法律地位及有關虛擬資產服務提供商命名或法律地位之差異。

---

<sup>68</sup> 如建議第 16 項注釋第 6 段所定義，或虛擬資產脈絡下之相等資訊。

<sup>69</sup> 資訊得以直接或間接方式提交。直接將該等資訊附加於虛擬資產移轉非屬必要。

## 詞彙表

*虛擬資產*為得為數位交易或移轉，且得被用於付款或投資目的之價值之數位表示。虛擬資產不包括法定貨幣、證券及其他已於 FATF 建議其他部分所涵蓋之金融資產之數位表示。

*虛擬資產服務提供商*為未於建議之其他部分所涵蓋，為或代表其他自然人或法人從事下述之單一或多個活動或營業為業之任何自然人或法人：

- 虛擬資產及法定貨幣間之交換；
- 單一或多種形式之虛擬資產間交換；
- 虛擬資產之移轉<sup>1</sup>；
- 保管及／或管理虛擬資產或能夠控制虛擬資產之工具；及
- 參與及提供關於發行人募集及／或銷售虛擬資產之相關金融服務。

---

<sup>1</sup> 於虛擬資產之脈絡下，移轉指代表其他自然人或法人從事交易，使虛擬資產自一虛擬資產位址或帳號移動至另一位址或帳號。





[www.fatf-gafi.org](http://www.fatf-gafi.org)