金融監督管理委員會因公出國人員出國報告
（出國類別：開會）

2022 年金融服務與雲端：與監理機關及金融機構高峰會

服務機關：金融監督管理委員會銀行局
姓名職稱：張怡欣科長、林緯政 專員
派赴國家/地區：泰國曼谷
出國期間：**111** 年 **11** 月 **16** 日至 **111** 年 **11** 月 **19** 日
報告日期：**112** 年 **2** 月 **10** 日

摘要

亞馬遜雲端運算服務（AWS）自2022年11月17日至同月18日假泰國中央銀行研習中心舉辦「2022年金融服務與雲端：與監理機關及金融機構高峰會」，第一天之內容主要聚焦於去中心化金融之不同面向探討，並邀集日本金融廳、泰國中央銀行及在東南亞地區具領導地位之金融機構等共同討論分享，並針對雲端服務在去中心化金融之應用進行分析。第二天之會議係由AWS之成員就雲端服務之各項議題進行說明，與會者可就所關注議題選擇主題，本次行程係參與「AWS客戶保護計畫」及「落實客戶隱私風險管理」。

本報告摘述課程重點，包括去中心化金融之介紹、去中心化金融監管帶來的挑戰及可能的因應方案、對監管者之啟示、金融服務領域的新興技術及其對普惠金融的影響等、AWS共同的責任模型、以及對個資保護可採取控管措施等，最後提出心得與建議。

目錄

壹、背景介紹

一、 AWS 介紹

亞馬遜雲端運算服務（英語：Amazon Web Services，縮寫為AWS）是亞馬遜公司於2002年成立之子公司，向個人、企業和政府提供雲端服務，並按照使用量計算費用，這些雲端服務透過AWS伺服器提供分散式計算處理能力和軟體工具。

根據Canalys之統計，截至2022年第三季，AWS服務占據了全球雲端服務（基礎設施即服務、平台即服務）32%的市場占有率，是市場的領導品牌，其次分別為微軟集團的Azure(22%)、Google Cloud(9%)。而根據亞馬遜公司發佈的財報，2022年第二季，亞馬遜整體業務淨銷售額為1212億美元，其中雲端服務業務AWS的淨銷售額為197億美元，佔整體業務的16%

雲端市場近年成長快速，市場研究機構Gartner預估，2023年全球終端使用者花在公有雲服務上的支出可望較前一年度成長20.7%，達到5,918億美元，成長率高於2021年的18.8%。IDC(國際數據資訊)表示，2021年臺灣公有雲整體市場規模成長至12.17億美元，年成長率為33.6%，成長率高於全球平均，我國係雲端業者近年積極拓展之市場。

二、 IIF介紹

國際金融協會(Institute of International Finance, IIF)是由世界主要商業銀行、投資銀行和共同基金於1983年所組成跨國協會，總部設在美國華盛頓，目前擁有來自60多個國家之約400名成員，IIF 成員以商業和投資銀行為主，並包含資產管理公司、保險公司、專業服務公司、交易所、主權財富基金、對沖基金、中央銀行和開發銀行。主要成員係來自歐洲(153)、非洲(109)、美洲(100)及亞洲(81)，我國未有金融機構擔任該協會之成員。IIF現任主席為瑞銀集團前總裁Axel A. Weber。

IIF為其成員提供創新研究、跨國宣傳以及舉辦交流活動，使IIF成員、客戶或主管機關間進行溝通交流。其使命包括：(1) 支持金融市場穩健風險管理；(2) 參與制定行業最佳行為準則與標準；(3) 倡導符合其成員廣泛利益的監管標準、金融和經濟政策，促進全球金融穩定和可持續經濟增長。(4) 支持成員機構的教育與培訓活動。[1]

[1] https://www.iif.com/About-Us

三、 「金融服務與雲端：與監理機關及金融機構高峰會」介紹

「金融服務與雲端：與監理機關及金融機構高峰會(Financial Services and the Cloud: A Summit with Regulators and Financial Institutions)」係由 AWS 籌辦之活動，2022 年度為第五年舉辦，會議係採邀請制閉門會議，並依據查達姆研究所規則 (Chatham House Rule)[2]進行，意即參加會議的任何人都可以自由使用討論中的資訊，但不得透露誰發表了任何特定評論，以促進討論的意見表達。

本次活動使用泰國中央銀行研習中心舉辦，除了 AWS 及 IIF 的成員外，本會議參加成員主要來自亞洲國家之銀行監理機關及金融機構，參加單位包括日本金融廳(Financial Services Agency)、泰國中央銀行(Bank of Thailand)、新加坡金融管理局(Monetary Authority of Singapore, MAS)、印度中央銀行(Reserve Bank of India)、柬埔寨中央銀行(National Bank of Cambodia)、聯合國亞洲及太平洋經濟社會委員會 (United Nations Economic and Social Commission for Asia and the Pacific)、渣打銀行(Standard Chartered Bank)、泰國盤谷銀行(Bangkok Bank)、安聯保險(Allianz Ayudhya Assurance Pcl)、Deloitte 會計師事務所及 Chainanalysis 虛擬資產調研機構等。

[2] Chatham House Rule，https://www.chathamhouse.org/about-us/chatham-house-rule

貳、 高峰會過程摘要

本次會議自 2022 年 11 月 17 日至同月 18 日，共 2 天，第一日主要係環繞於 IIF 所發布之「Web 3.0 和金融服務報告(Report on Web 3.0 and Financial Services)」，並以此報告為基礎，邀請主管機關及金融業者探討相關議題。第二天則由 AWS 就金融主管機關可能關心的雲端服務議題進行分組說明。

日期	研討議題
11 月 17 日	IIF「去中心化金融：用例、挑戰及機會」報告
	小組討論：Web3.0 和金融服務
	小組討論：DeFi、Web 3.0 和支付—為更廣泛的經濟創造價值
	小組討論：Web2.5–連接對未來和當今基本面的渴望
	座談會：與科技企業之全球公共政策副總裁對談
	座談會：與東協大型銀行之首席執行官的對談
11 月 18 日	小組討論：著眼未來，運營韌性和技術風險監督的發展
	分組報告 A：AWS 客戶保護計劃
	分組報告 B：落實客戶隱私風險管理

一、 IIF「去中心化金融：用例、挑戰及機會」報告[3]

(一) 去中心化金融之簡介

「去中心化金融(DeFi)」此一名詞之起源可以追溯自 2018 年 8 月之網路文章，儘管相關應用發展蓬勃，但至今仍未有普遍認可之 DeFi 定義。由美國 President's Working Group on Financial Markets[4]於 2021 年 11 月發布之「穩定幣報告」，將 DeFi 定義為「建構於支援智能合約(smart contract)功能之分散式帳簿技術(distributed ledger technology, DLT)上的各種金融產品、服務、活動」，並指出「儘管 DeFi 名為去中心化，實際上不同 DeFi 的去中心化程度差異很大，通常高度集中在一小群開發者或投資者進行 DeFi 的維運及管理」。而本文採取所採取之 DeFi 定義為**「使用分佈式帳本技術 (DLT) 的金融形式（法定或加密貨幣計價），且在治理、託管或其他層面也顯著有去中心化之特性」**，該定義包含比特幣、乙太幣等加密貨幣、穩定幣、使用前揭

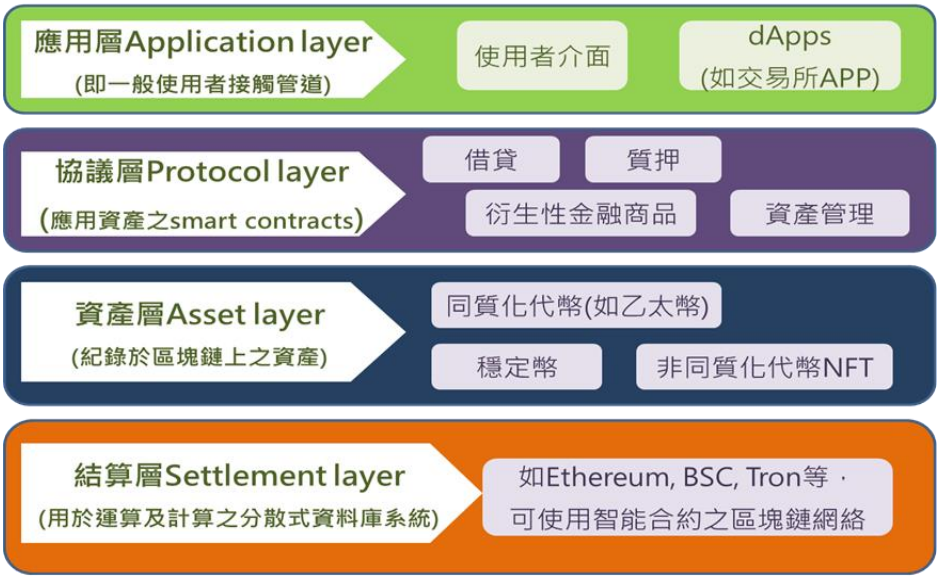
[3] IIF，Decentralized Finance: Use cases, challenges and opportunities，https://www.iif.com/Publications/ID/5142/Decentralized-Finance-Use-cases-challenges-and-opportunities

[4] 該會議之成員包括美國財政部、美國聯準會(FED)、證管會(SEC)、美國商品期貨交易委員會(CFTC)等金融監理組織之代表

資產的借貸或衍生金商品、虛擬資產交易所等。

DeFi 的交易過程通常不需人力介入，使用者在操作介面輸入指令後，即可依 DeFi 協議所設定之程式在區塊鏈網路自動執行，其運作架構區分為以下四個階層：

圖一：DeFi 運作架構



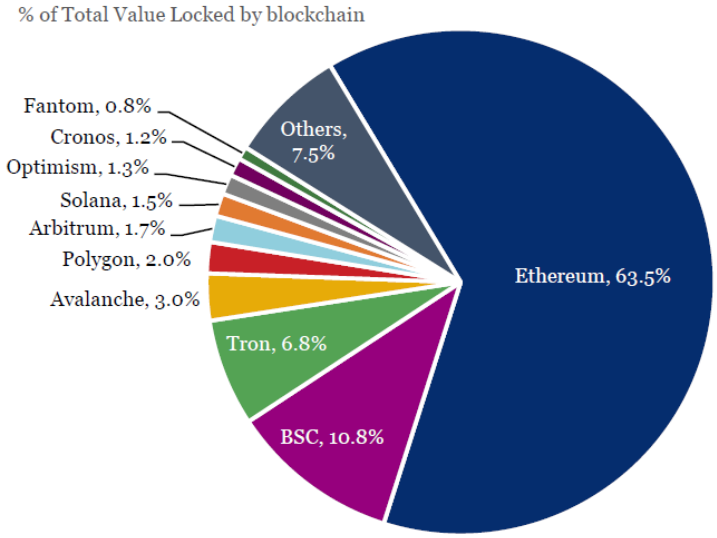
(Source: IIF illustration, based on Schär 2021.)

DeFi 衍生之商品眾多，包含借貸(Lending)、具槓桿性質之衍生性商品(Derivatives)、虛擬資產交易所(DEX)及資產管理(Asset management)等。DeFi 規模最大應用為「借貸」服務，該服務係利用建立在區塊鏈上之智能合約，自動化提供借貸服務，而此類借貸關係可以是借貸雙方點對點(peer-to-peer，或稱 P2P)進行，也可能係投資人將虛擬資產交由平台或項目發起方管理之資金池(P2B)。

DeFi 之使用，通常需要使用者將其虛擬資產移轉給 DeFi 服務提供方(一般使用者多透過交易所)，移轉後須鎖定(locked)其虛擬資產一段時間，以執行相關操作，因此「總鎖倉金額(Total value locked, TVL)」是衡量 DeFi 市場活絡程度重要指標。DeFi 之 TVL 約在 2021 年 12 月底達到歷史高點 3,174 億美元，2022 年 11 月上旬則約為 808 億美元，顯示 DeFi 之市場規模在近一年大幅減少。

雖然目前有許多的區塊鏈均有支援編寫智能合約而提供 DeFi 服務，但以太坊區塊鏈然在結算層(settlement layer)仍占有最高的總鎖倉金額份額(63.5%)，其次為華裔企業家趙長鵬所創立的幣安智能鏈 BSC(10.8%)及中國企業家孫宇晨所創立的波場 Tron(6.8%)。詳如下頁圖：

圖二：DeFi 結算層之總鎖倉金額占比



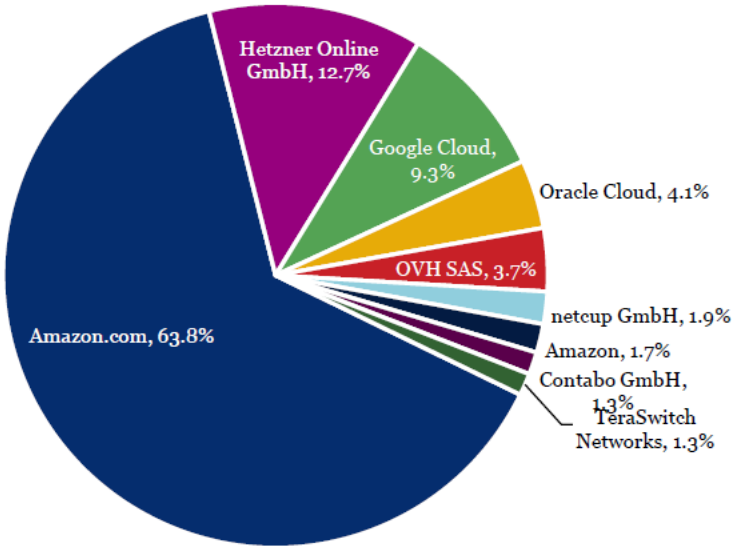
Source: DeFi Llama. Data as of November 9, 2022.

(二) 雲端服務與去中心化金融

許多大型 DeFi 項目使用雲端服務，因為相對私有雲和地端資料中心等替代方案，雲端服務在多數情形下是企業資料存儲和計算較便宜或更有效能的選擇。 雲端服務可以幫助金融機構和金融科技公司（包括 DeFi 項目）解決網路安全、單點故障、負載管理和資料工程等挑戰，這些挑戰可能超出單一機構可處理的能力。此外，雲端服務的跨境特性適合用於跨境使用的 DeFi 協議和應用程序，並已有許多用於雲端環境的開發工具。

雲端服務除了用於 DeFi（大部分是雲原生的），去中心化協議中的許多節點也由雲端服務提供支持，包括權益證明 (POS) 協議，例如 Tron、Avalanche、Solana 以及近期改版後的以太坊。根據 ethernodes.org 統計，按網絡類型劃分的以太坊節點**有 67.5%是託管(Hosted)給外部專業機構(如雲端業者)**，而住宅節點和商業節點分別為 30.6%和 1.4%。在**託管節點中，約 63.8%由 Amazon.com 託管**，9.3%由 Google Cloud 託管，詳如下圖：

圖三：以太坊托管節點占比



Source: ethernodes.org. Data as of November 8, 2022.

另一方面，Akash Network 和 InterPlanetary File System 等去中心化雲端服務提供商正企圖拓展公有雲服務市場，允許用戶出租未使用的電腦運算能力和網路流量，並在該分散式平台上部署他們的應用程序（包括 dApps）雲端服務基礎設施。然而 DeFi 是公有雲服務的重要需求來源，金融服務業者不太願意將其及其客戶的業務關鍵資料委託給匿名參與者運營的無許可雲端網路(即去中心化之雲端服務)，即使資料在存儲或傳輸時已進行加密等安全處理。

目前歐盟和英國等司法管轄區，正在考慮採取措施直接監管金融機構的關鍵服務提供商，其中包括一些雲端服務提供商。該報告指出，若金融機構大幅依賴去中心化雲端服務提供商，將使金融機構更像 DeFi 業者，對金融監管部門帶來類似 DeFi 的監管挑戰。

(三) Web 3.0

根據其支持者的說法，在 Web 3.0 中，用戶將對他們創建的內容和獲得獎勵有更多的控制權，不僅僅是免費訪問社交媒體服務，而是更直接地透過代幣和其他具部分金融性質的工具獲得報酬或控制權。對於某些人來說，Web 3.0 代表使用虛擬現實和增強現實 (VR/AR)等類似技術。對於許多其他人來說，關鍵是網路世界中身份無法刪除，以及身份和屬性可移植性的概念(相對於 Web1.0 或 Web2.0 之帳號可能被服務提供商刪除而完全喪失)。

DeFi 愛好者對 DeFi 與 Web3.0 之關聯性，大致可分為三種見解：(1）必須先實現 DeFi，才能轉向 Web3.0；(2) DeFi 和 Web3.0 之概念幾乎可以互換，是人與網路世界存在間進行交易之理想化的未來模式；(3）DeFi 代表著 Web3.0 世界地金融體系，兩者將同步演化。這些愛好者一致認為，DeFi 工具將在推動網際網路進入下一階段發揮重要作用。

這些觀點都基於 Web3.0 必然採用分佈式帳本技術之假設，然而該假設似未有堅實基礎。該報告指出，金融系統的未來無疑將保持顯著的中心化程度，因此 Web2.5 可能是更有可能的結果。

(四) 更廣泛採用 DeFi 所面臨的挑戰

要更廣泛地採用 DeFi 仍存在一些結構上的挑戰，主要挑戰包括：(1)身份、匿名和假名；(2) 共識機制；(3) 用戶體驗; (4) 能源足跡。儘管這些挑戰可能並非無法克服，但它們讓人質疑 DeFi 是否適合主流消費者和投資者採用的目的。

1. **身份的挑戰：假名金融是否符合目的？**

   DeFi 項目最典型的特徵之一是假名(pseudonymity)，換句話說，用戶能夠保持匿名，並且也只能通過假名為其他網絡參與者所知，假名可以是「暱稱(handle)」，也可以僅僅是用於保存加密貨幣的區塊鏈錢包地址。在另一個層面上，區塊也同時具備記錄匿名錢包之間交易的透明度，任何執行驗證節點的人都可以通過 Etherscan 等網路服務工具瞭解相關交易

紀錄。換句話說，假名是 DeFi 在區塊鏈極度透明之前提下，為用戶提供隱私的方式。

DeFi 協議通常不要求用戶向任何人透露他們的真實身份—提供錢包地址通常就足以參與 DeFi 應用程序。同時，任何人都可以自由檢查開放式區塊鏈的資料，並可以追踪每個錢包的交易歷史。

然而 DeFi 目前的透明度和隱私性可能都不符合大規模消費金融或企業金融之實務需求。傳統金融機構大多不能容忍 DeFi 協議直接使用假名帶來的風險，這些風險包括法律遵循、金融犯罪、AML/CFT 和被制裁風險。

用戶交易的這種永久透明度也可能直接與某些個人資料法規中體現的“被遺忘權”原則相矛盾，例如歐盟的通用數據保護法規 (GDPR)。

在某些情況下，假名可能會使 AML/CFT 和制裁審查變得更加困難。那些採用假名的 DeFi 項目大多不符合規範，除非它們非常謹慎的設計運作架構，以確保豁免適用法規，例如設立在法規較為寬鬆之司法管轄地提供服務。

最近關於 Tornado Cash 的爭議，美國財政部外國資產控制辦公室 (Office of Foreign Assets Control, OFAC) 制裁數名與 Tornado Cash 混合器項目相關之自然人。這案件顯示 DeFi 項目及其相關人員可能面臨的風險。

2. 驗證和執行的挑戰：區塊鏈系統能否支持所有類型的金融交易？

由於區塊鏈的運作結構和協議的性質，特別是其共識機制，為 DeFi 帶來額外的挑戰。鏈上交易需要其他節點的驗證，才能將資料寫入區塊鏈中。為確保完成驗證流程，大多數智能合約系統都有某種執行機制來確保交易得到處理。這種機制可以像「驗證發起代幣轉移之錢包地址，確認錢包地址包含指定代幣」一樣簡單，也可能複雜得需進行多項指令，並涉及多層資料處理協議，過程必須支付手續費或有專門驗證工具。

DeFi 協議的儲備池和資本要求，以試圖確保那些參與協議的人有錢來履行他們的義務，然而，匿名可能會對追查資金流向或提出索賠帶來挑戰。儘管 DeFi 協議中的許多交易都是即時處理的，但在實務執行過程仍然會存在一些困難，包括智能合約執行的意外結果、交易對手的識別或債權確保等，都對確保智能合約的順利運行帶來潛在的挑戰。

DeFi 中的驗證和執行都代表了基本的操作問題，用戶希望交易手續費低，但交易手續費必須高到足以激勵足夠多的驗證者來履行這一角色。這種矛盾關係對 DeFi 經濟模型帶來挑戰，可能激勵驗證者串通並保持高額費用[5]。如果沒有法律處罰和定期監督，健康的市場運作將難以維持，因為具有市場影響力之驗證者可透過內線交易或搶先交易等不當手段牟取

[5] Daian, P. et al. (2019), Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges, April 10, p. 12.

利益。

在 DeFi 生態系統中，可以將代幣質押於特定 DeFi 協議中，以對驗證者進行投資而取得回報。然而，這投資行為使記錄交易的過程造成了集中性。亦有論者指出，雖然 DeFi 提供了替代的、可能更有效的資訊記錄和處理方法，但 DeFi 並沒有改變法律或人性。正如美國 SEC 委員 Crenshaw 指出的那樣，「若非有必要， DeFi 項目的經營者不會將資源投注於法規遵循或適當的內部控制」，且如果有足夠的誘因，總會有人試圖進行欺詐或其他惡意行為以牟利[6]。在這種情況下，「買家當心(buyer beware)」不足以作為穩健金融體系的基礎。

3. 用戶體驗的挑戰：易用性能否提高到足以支持廣泛採用的程度？

參與加密資產市場和 DeFi 協議相關的用戶體驗 (user experience, UX)對不具備資訊能力的人不太友善，這原因來自於與區塊鏈之「金鑰」保管衍生之風險，例如，金鑰可能因為存儲在硬碟和 USB 等容易被盜取、遺失或損壞的物理設備上。要不喪失這些金鑰，需要對加密資產存儲的私鑰審慎保密，這對使用者是一個持續的挑戰並讓人焦慮。時有因不慎保管物理設備，或忘記密碼而損失鉅額加密財富的事件發生。[7] 對自己保管虛擬資產的焦慮，並不侷限於個人或不成熟的消費者，許多資產管理人仍更偏好由專業第三方管理人來管理資產。

欺詐仍然是 DeFi 生態中一個長期存在的問題，包括拉高出貨詐騙(Pump-and-dump scams)、51% 攻擊、治理漏洞、假幣詐騙(fake coin scams)等比比皆是。有估計指出，僅 2021 年一年，DeFi 詐騙就造成超過 100 億美元的損失，而 2022 年有望超過這一紀錄[8]。金融犯罪並不是什麼新鮮事，但 **DeFi 缺乏身份驗證和治理瑕疵的特性讓欺詐行為更為猖獗**。在 2022 年主要被使用 DeFi 協議中，有 65%沒有對其代碼進行第三方審計[9]。

DeFi 的完全自動化執行可能存在嚴重缺陷，尤其是在消費性金融的領域，客戶期待能夠在商品未交付前拒付付款或撤銷冒名交易，在更複雜的領域金融業，契約修正也相當常見。在抵押貸款中，在開始交易和完成交易之前，可能需要等待或冷靜期以遵守消費者保護法規，或者保留一段時間進行必要的檢查等。DeFi 要更廣泛使用在消費金融領域，目前仍有需多努力的空間，而監管部門可能要求 DeFi 經營者對 DeFi 協議進行監

[6] Crenshaw (2021), "Statement on DeFi Risks, Regulations, and Opportunities," The International Journal of Blockchain Law, Vol. 1, Speech, November 9.
[7] The Guardian (2022), Man who threw away £150m in bitcoin hopes AI and robot dogs will get it back, August 2; Insider (2021), Bitcoin Owner Who Lost Password Made Peace With Potential $220 Million Loss, January 17.
[8] EuroNews (2021), Crypto crime is booming on DeFi platforms and has caused over €9 billion in losses this year, November 19.
[9] European Securities Markets Authority (ESMA) (2022), Crypto-assets and their risks for financial stability, October 4, p. 5.

督和治理，經營者應有在緊急事件發生時介入解決問題的能力。

4. 能源消耗的挑戰：DeFi 的能源足跡能否可持續？

由於區塊鏈的技術特性，基於區塊鏈技術建構之金融系統消耗大量電力，然而目前世界各地正努力減少能源消耗候。最著名的基於工作量證明(Proof of Work, POW) 的區塊鏈是比特幣區塊鏈。目前對比特幣區塊鏈年化總能耗的估計為 117 TWh，與荷蘭的耗電量相當。

(五) 金融監管的考量和原則

明確且現代化的監管制度可以解決採用 DeFi的部分挑戰。許多人呼籲政府採取行動保護消費者免受傷害、保護市場誠信、建立公平競爭關係，並允許負責任的創新，包括讓相關機構有信心投資這些技術。適當修正監管和操作風險管理，可以幫助 DeFi技術及其能夠發揮的功能，以可持續的方式成熟這可以更廣泛地運用於金融領域以及房地產等非金融資產。

在這種情況下，監管機關必須詢問：1) 目前金融產業正在執行哪些功能，2) 監管機關可以在什麼程度上對這些功能感到滿意，以及 3) 這些功能的某些組合，是否會改變答案。

現有的金融機構可能會被現有的銀行規則，甚至是他們自己的內部運營風險管理團隊所束縛，因此禁止採用更去中心化的流程或技術，而這類流程或技術可能會降低管理費用或其他運營成本。此外，DeFi 對金融穩定帶來的潛在風險是監管部門關注的問題，需要更好地理解—例如，包括 DeFi 自動化交易在錯誤發生時所帶來的衝擊。

這是大多數參與者和監管者的核心問題—DeFi 領域應該如何監管？一些參與者斷言，DeFi 需要“運作規則(rules of the road)”，只要它們靈活且設計良好即可。然而，適當監管和監督的挑戰，比找出差距以用新規則彌補的做法更廣泛。

1. 監管現代化的關鍵原則：以風險和結果為導向的監管

隨著監管架構發展和明確化，可以發現「相同的活動、相同的風險、相同的監管」原則及「技術中立」原則是多數金融監管單位所重視原則。這些原則多次出現在各國金融監管機關及跨國組織所發布之報告或演講中，例如聯邦準備理事會 Michael S Barr 副主席於 2022 年 9 月表示[10]：

> *美國聯準會計劃與其他銀行監管機關合作，根據**相同風險、相同活動、相同監管的原則**，確保銀行內部的加密活動受到良好監管，無論活動使用何種技術。*

金融穩定委員會(Financial Stability Board, FSB)在近期加密資產監管的諮

[10] U.S. Federal Reserve Board of Governors (2022), Speech by Vice Chair for Supervision Barr on making the financial system safer and fairer, Speech, September 7.

詢文件中也使用前揭原則，提出類似的建議[11]：

*主管機關應對加密資產活動和市場實施有效的監管、監管和監督– 包括加密資產發行者和服務提供商 –根據**「相同活動、相同風險、相同監管」**的原則，與它們造成或可能造成的金融穩定風險成比例。”*

歐盟最近完成的加密資產市場監管法案 (Markets in Crypto- Assets Regulation, MiCA)之條款也採用相同原則[12]：

歐盟關於金融服務的立法應遵循以下原則：
「相同的活動，相同的風險，相同的規則」和技術中立。

巴賽爾銀行監理委員會(Basel Committee on Banking Supervision, BCBS) 在銀行持有加密資產之暴險也採用類似的原則[13]：

*「**同風險、同活動、同待遇**」：若加密資產提供與「傳統資產」同等經濟功能和風險，應如同傳統資產適用相同的資本、流動性和其他要求。*

而英國中央銀行副行長（和 CPMI 主席）Jon Cunliffe 在 2022 年 7 月的演講中對此進行了擴展[14]：

金融監管部門的出發點應該是對提供金融服務所固有的風險採用相同的監管標準，無論它是如何提供的。 ...但技術差異可能導致現有監管機制無法在新環境發揮作用，或可能無法有效管理風險。我們的監管標準和框架中隱含了我們認為必要的風險緩解分級。如果我們不能以完全相同的方式落實監管，則應確保實現相同水平的風險緩解措施—也就是達到“相同的監管結果”。

這段發言強調了幾點：**不同的活動可能會帶來相同的風險，因此應該以相似的方式對待；具有相同風險的不同活動應給予同等待遇，但不一定完全相同，而「達成相同的風險緩解等級」則是一個較為理想的目標。**換句話說，應將新技術或商業模式特點納入監管措施設計之考量，以使監管手段能達成其政策目的。

2. 技術中立監管—意義和限制

如上所述，監管部門大多支持技術中立原則，值得深入探討。技術中立原則代表政策制定者不應在相競爭之技術間「挑選贏家」；而是由市場

[11] FSB (2022f), Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative document, Recommendation 2 (as proposed), October 11.
[12] Citing the “final compromise text” dated October 5, 2022. The final text of MiCA is expected to be published in the Official Journal in spring 2023 and will enter into application between 12 and 18 months thereafter (see European Securities Markets Authority (ESMA) (2022), Crypto-assets and their risks for financial stability, October 4, p. 14)
[13] BCBS (2021), Prudential treatment of cryptoasset exposures, June, p. 2.
[14] Bank of England (2022), Some lessons from the Crypto Winter – speech by Sir Jon Cunliffe, July 12

機制決定哪些技術值得廣泛採用，市場將確保最具成本效益的解決方案勝出。

但是，技術中立原則仍有可能遭質疑之處，因為它未能提供足夠的誘因鼓勵開發或採用創新產品或服務，然而有時因政策原則需要加速採用新技術。例如嚴格遵守技術中立，可能會不利採用與氣候保護目標符合之技術險。 一些 DeFi 支持者會以類似論調上批評技術中立性原則，聲稱應有更多有利於金融創新之政策。另一方面，金融危機的教訓告訴我們，不受約束的金融創新，在廉價資金的推動下，若沒有足夠的控管機制，可能導致系統性風險，危及整個金融體系，並影響實體經濟。

因此主管機關需要明確界定監管界限和監管責任，這可能包含主管機關向金融創新者（包括 DeFi 項目及其發起人）說明監管邊界範圍或如何遵循主管機關的指導。明確的監管框架有助於將相關金融活動納入監管範圍，所涉及之風險將受到嚴謹的資本要求、流動性監管、健全的風險管理和持續的監管監督，這將對 DeFi 活動產生正面影響，特別是能保護客戶之權益。

3. DeFi特性對監管帶來的挑戰及可能的因應方案

(1) 去中心化的挑戰：去中心化可能使監管和法律執行更加複雜化。DeFi 協議係依據智能合約執行，且多由「去中心化自治組織（Decentralized Autonomous Organization, **DAO**）」運營，去中心化自治組織之決策責任並不明確，可能分散在眾多特定之治理代幣(governance token)持有者之間，監管部門要追究責任也成為挑戰。然而，許多去中心化協議之運作不如其名稱所暗示的這麼分散，許多文獻都提到「去中心化錯覺(decentralization illusion)」，意即去中心化自治組織的治理代幣高度集中少數人，或僅由一小部分參與者掌握著管理私鑰和其他管理工具。監管部門已經開始規劃監理措施，讓去中心化組織對其不當行為負責。如商品期貨交易委員會對 Ooki DAO 的投訴將被告確定為「一個由 Ooki 代幣持有人組成的非法人協會」[15]。

(2) **DeFi 跨部門性挑戰**： DeFi 協議的跨部門性質是一個挑戰，DeFi 可能結合了銀行、借貸服務、支付、資金管理和保險等要素。因此，不容易正確或一致性地就監管責任進行分類。加強監管部門間和跨部門的合作，包括與個資監管部門的合作，可以解決這個挑戰。

(3) **DeFi 跨境性挑戰**： DeFi 協議具有跨境及分散式特性，用戶可從世界各地參與 DeFi 活動。參與者來自世界各地，涉及多個司法管轄區，使監管執行更加複雜。為因應 DeFi 的跨境性質，監管部門可以參考既有監管大型跨境實體（例如跨境銀行集團和金融市場基礎設施）之

[15] CFTC (2022), Complaint accessible via Media Release, September 22; U.S. Treasury (2022), U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, Press Release, August 8.

經驗，開發跨境合作監管架構[16]。

(4) **假名性質之挑戰**：區塊鏈的假名且無須審核之性質，允許許多 DeFi 以不符合法規運行，包括未執行以防制洗錢及資恐為目的而進行 KYC 程序。為使 DeFi 應用能夠被廣泛使用， DeFi 應用越來越需要審核和進行法規遵循，而無需審核的 DeFi 可能會保持匿名且在大多未落實法規遵循。在這種情況下，無需審核的 DeFi 可能會變得越來越邊緣化。目前發展中的代幣化可驗證憑證(tokenized verifiable credentials)，允許在參與無須審核 DeFi 的同時，也能支持法規遵循義務，進而減少假名性質帶來的挑戰[17]。

(5) **缺乏客戶分類或商品適合度之挑戰**： DeFi 協議之通常未進行客戶分類或商品適合度檢查，使得專業投資客戶與一般零售客戶間可獲取之服務沒有區別，因此可能讓不成熟的客戶承擔過多風險或使用不適合其風險等級之商品。

(6) **利益衝突**：DeFi協議無法管理利益衝突，特別是治理代幣持有者或內部人員與用戶間的利益衝突。市場清潔度(Market cleanliness)，因為 DeFi 協議大多未設有避免內線交易、搶先交易、清洗交易或其他市場濫用行為的市場誠信之功能。 DeFi 協議的假名性質使協議運營商的稅務或制裁法規遵循變得複雜，導致稅務和制裁主管機關難以有效執行其權責。

4. 對監管者的啟示

DeFi 給監管部門帶來了挑戰，而使用 DeFi 而產生的大量資料及自動化特性，對於監管部門持續監控和識別新風險帶來了不同的挑戰，這些挑戰包括：

(1) **缺乏監管權**：如果立法機關未採取行動，適當擴大監管範圍以符合「相同風險，相同監管結果」之原則，監管部門可能缺乏監理 DeFi 活動的有效權力或執法工具。

(2) **缺乏專業知識和資料分析**：監管部門可能缺乏理解 DeFi 協議的專業知識，或無法獲得足夠的資料分析，以理解這些DeFi協議的活動。因此，監管部門可能無法理解DeFi市場出現的風險。

(3) **商業模式的變化**：隨著對DeFi的商業模式理解的加深，可以使金融、消費者保護和隱私監管部門等不同類型監管部門之間的監管合作品質提升，以確保能有效執行監管及監管原則的一致性。

(4) **資產隔離(Ring-fencing of assets)**： 若 DeFi 項目將其客戶資產跨境保管於其他司法管轄區的，可能會衍生許多問題，特別是如果客戶質押或借出的資產混合在綜合帳戶中，或被運用在與目的不同的項目中。

[16] See IIF (2020), Submission to FSB on global stablecoins, July 15.
[17] See Possible Solutions to Open Up Broader Adoption in Financial Services section at page 26.

(5) **嵌入式監理(embedded supervision)**：一些論者建議將「嵌入式監理」作為適應 DeFi 世界的監督手段。該術語的定義是「用於去中心化市場法規遵循之監管框架，主管機關透過檢視區塊鏈上開放之紀錄，以進行自動化監管」，這監管框架減少了業者主動收集、驗證和交付資料之負擔[18]。然而，一些監管者可能更喜歡自行收集資料，並利用區塊鏈分析公司來協助加強他們的監督。

二、 小組討論：Web 3.0 和金融服務

與會者認為監管部門之功能是在創新與法律遵循之間取得平衡。監管部門間正密切關注彼此政策，不想扼殺創新，但同時擔心新興技術的某些風險。因為消費者保護是監管部門的重要目標。

監管部門主要關注六個政策問題：1）反洗錢（AML）—如何將 AML 規則應用於虛擬資產領域； 2) 稅收—稅收影響是什麼，稅收申報標準，加密資產申告框架的開發； 3) 消費者保護—DeFi 領域存在許多費者保護問題； 4) 審慎要求—確定金融機構是否適合運行加密服務的許可制度； 5) 金融穩定性—研究加密貨幣與傳統金融之間的交集； 6) DeFi–瞭解 DeFi 的用例並評估市場將如何在 DeFi 領域運作。

DeFi 的風險似乎與傳統金融相同。例如，流動性、信貸、金融錯配都是在 DeFi 和傳統金融的使用中都很明顯的風險。因此，監管部門的一個選擇可能是採用「相同活動、相同風險、相同監管」的方法。然而，DeFi 和傳統金融的營運風險可能不同。人們也可能不完全了解 DeFi 的風險，因為它仍然是一項新興技術。

公私伙伴關係對於制定該領域的規則、規範和標準至關重要。 DeFi 不受地理限制提供服務，因此各國監管部門需要跨國內相互合作並與產業合作，制定可遵循之共同標準，以確保這些創新技術能夠以安全和負責任的方式運行。

監管部門需要創造誘因，以獲得符合監管目標的結果。監管的必要性已經變得更加明顯，但監管部門不應該對加密貨幣和 Defi 實施全面禁令，因為資料表明這些禁令不起作用（例如，埃及嚴格禁絕加密貨幣之使用，然而埃及也同時是中東地區加密貨幣使用增長最快的國家）。與會者認為監管部門應瞭解與 DeFi 之業者和客戶之實務期待，並進行具有高包容性的溝通。

三、 小組討論：DeFi、Web 3.0 和支付—為更廣泛的經濟創造價值

傳統金融機構、金融科技業者與跨國科技公司在未來金融中扮演不同但互補的角色。進入 Web 3 需要來自銀行業的典範移轉。與會者就區塊鏈、DeFi 和 Web 3 等新興技術在為金融領域創造創新業務模式方面表達看法，主要可能應

[18] See, e.g. Auer, R., (2019), Embedded supervision: how to build regulation into blockchain finance, *BIS Working Papers* No 811, September (revised May 2022).

用係在於為跨境交易結算和數位交易之發票產生更有效率的流程，或為金融服務欠缺的族群提供更具包容性和成本更低的金融產品和服務，例如為農村中小企業提供的數位支付和為無定居者提供的儲蓄帳戶。

雖然一般坊間認為新興技術可以在促進金融包容性過渡方面發揮不可或缺的作用，但與會者認為區塊鏈領域仍有許多努力空間，才能使區塊鏈技術廣泛應用於金融服務。與會者提出一些考慮因素，包括調整傳統銀行和支付工具帶來的挑戰、企業在適應新技術產品準備方面的落差，以及缺乏明確的消費者保護相關資訊。

與會者認為，客戶信任係廣泛採用區塊鏈的關鍵因素，特別是加密貨幣市場持續波動，削弱消費者和監管部門的信心。有鑑於此，與會者討論了跨行業、政府和國際組織的建設性合作方案，以因應將區塊鏈技術導入金融服務的挑戰，例如**制定明確的、原則基準(principles-based)的監管方法**和**互操作性標準**，這些方法和標準可以一致應用在所有實體以及公私合作夥伴關係，以測試可能的用例。

雲端服務在討論中被建議可做為跨部門協作的運作平台，為公部門和私部門參與者間資料共享和創新提供安全的環境。與會者最後呼籲區塊鏈、DeFi 和 Web 3 行業應採取行動，積極與金融機構以及政策制定者和監管部門合作，制定具體的發展路線圖，以建立信任和採用途徑。

四、 小組討論：金融服務領域的新興技術及其對普惠金融的影響

普惠金融(Financial inclusion)所涉及之範疇不容易界定，要有效推動相關政策，政府和相關組織需要具體釐清普惠金融之含義，以及擬處理的族群（例如婦女、兒童、老人、殘疾人士等），以採行有效政策工具以滿足特定群體的需求。

金融科技或電子支付在推動普惠金融方面發揮著重要作用。它們允許那些無法獲得傳統金融服務的族群獲得融資以發展業務，進而改善他們的生活條件。但實務上很難從偏鄉地區和弱勢族群獲得準確資料，以真正瞭解實現普惠金融問題的規模。

疫情使富人與窮人間的差距更加凸顯，因此政府政策需要改變，以建設更具包容性的經濟。政府可以考慮針對金字塔底層之企業提供具體獎勵措施，例如發布包容性業務指南(Inclusive Business Guidelines)，以激勵企業為欠缺金融服務之族群提供服務（例如，這些企業可以獲得稅收減免、優惠待遇等）。

需要提高國民的金融知識水平，包括提高對底層 DeFi 技術及其風險的理解。人們需要瞭解金融產品，並了解各種金融商品運作機制的因果關係。每個司法管轄區應決定其對金融創新的風險接受程度，這將有利於釐清相關法規之適用及應該調整的方向。監管部門也可以使用監理沙盒來管理創新風險和提高對新興技術的熟悉程度。

有關透過數位金融服務以提升普惠金融部分，與會者提出偏鄉或是弱勢族群可能缺乏數位工具及基礎設施，數位金融工具在使用上仍有其侷限性。另有與會者回應，在其調查經驗中，在一些缺乏充足食物及乾淨水源之地區，手機之普及率卻相當高，雖然無法解釋數位普及度高之原因，數位工具在實務上確實能協助偏鄉或弱勢族群取得金融服務。

五、 座談會：Web 2.5 – 彌合對未來的期望和當今的基礎

DeFi 和 Web 3 並不是同義詞。 DeFi 和 Web 3 的概念常相互交雜，但又有所不同。 DeFi 去中心化金融支持 Web 3 的運作，但 Web 3 超越了金融，可能包括虛擬現實、元宇宙等其他領域之應用。

Web 2.5 通常用於描述介於 Web2 和 Web3 之間的區塊鏈服務，希望藉由運用這兩種技術特性之優勢，以提供更符合大眾市場需求的服務。然而，在 Web 2.5 在成為主流之前還有許多努力空間。 目前有價值的 Web 2.5 應用仍相對有限，在保險領域更是稀少。為使 Web2.5 成為主流，並超越傳統的金融基礎設施，Web2.5 需要創造新的市場需求，才能從傳統保險業奪走客戶。

與會者認為 Web 3 仍有探索的空間，其中一個部分是探索如何使 DeFi 服務在不需要第三方驗證機構的情況下運作，或使既有運作過程更加去中心化。目前已有金融服務機構開始研究如何應用智能合約。

金融機構的董事會對於新興技術之投資有重大影響力，有必要對董事會成員進行教育，使其理解將資源投入到新興技術的價值，這可以透過針對高級管理層之技術培訓解決，或使技術團隊間進行競爭，迫使團隊尋找創新技術來擊敗其他團隊。最重要的是，確保 Web 3 和其他技術能解決客戶或組織的問題，並且技術的使用與組織整體目標能保持一致。

六、 座談會：與科技企業之全球公共政策副總裁對談

雲端服務核心價值是具有高度彈性，得以快速調整規模和使用技術。使企業能夠在進行創新和改進其既有產品和服務的同時，也能確保業務連續性。與自行建置及維護自有資料中心相比，採用雲端服務之成本效益更佳，因為企業可視業務需求快速調整雲端服務之使用量，使有限預算得有效利用。

雲端服務的環境足跡更環保，根據 S&P Global Market Intelligence 的研究發現，與亞太地區受調查企業和公共部門組織的自有機房相比，雲端資料中心的能源效率有明顯優勢，在相同的工作負載下，雲端資料中心運行所產生的碳排放量僅有自有機房的 20%。

雲端服務有助於發展新興技術，雲端服務促進了人工智能/機器學習、物聯網、5G 和量子計算等技術的發展，即使是小型新創企業也能透過雲端服務使用使用這些新技術。例如機器學習，需要強大的電腦計算能力才能運行，而雲端服務是執行這類計畫的絕佳平台。

資料主權 (Data sovereignty) 是個複雜的議題，每個國家對資料主權都有不同的關注點及看法。行使資料主權的常見作法是資料本地化政策(Data Localization Policies)，即要求資料不應傳送至境外或有嚴格限制。但是與會者認為政府應審慎評估資料本地化政策，因為可能對企業發展造成障礙，有研究指出，如果政府採用資料本地化政策，企業將多支付 30% 到 60% 的成本。

行業溝通很重要，讓私部門有機會對監管部門提供意見進行交流，可以促進監管制度完善並實現其監管目標。私部門也可透過讓監管部門熟悉創新技術，進而提升對創新技術之理解與信任。

七、 座談會：與東協大型銀行之首席執行官的對談

東協地區擁有龐大的成長潛力，由於中產階級不斷成長及基礎設施尚待發展，吸引大量外國投資。然而，金融產業的成熟需要人才的投入，才能將整體金融環境建設完善。

雲端服務的優勢是易於擴張規模和速度，隨著相關技術的不斷發展，雲端服務對金融機構業務發展的影響力日益遽增。而金融機構運用資料並將其轉化為商業上的洞察力，將是未來金融業間競爭的關鍵。

監管部門在金融機構數位轉型中扮演重要角色。監管部門負責在創新與穩定之間取得平衡，並設定明確的界限。為創造 DeFi 協議可以存在的環境，監管部門可以創造沙盒環境讓金融機構測試可能的解決方案，與此同時，若不能確保 DeFi 解決方案能夠穩健運行，過早開放 DeFi 相關業務反而會削弱社會的信任，因此需要保持平衡。

八、 小組討論：著眼未來，運營韌性和技術風險監督的發展

金融行業面臨的主要風險包括資訊安全、地緣政治、第三方服務、氣候變化和自然災害。其中資訊安全威脅參與者的威脅越來越多，使用既有資訊設備管理資訊安全相關風險已經越來越困難—與談人認為雲端服務是一個更安全的解決方案。氣候變化和自然災害對金融機構運營韌性構成挑戰，需要建構相關風險管理機制。

第三方服務連接中斷的對金融機構的影響越來越大，特別是因為金融機構越來越依賴第三方，因此金融機構需要確保其第三方合作夥伴之運作穩定。減輕第三方風險對金融機構至關重要。第三方風險不僅僅與金融機構的技術供應商有關，也包括來自客戶端而加入的第三方業者。金融機構內部應建立良好的風險管理文化，並採用以風險為基礎的方法，將具重大性之資訊系統採用合適的系統架構運行，以確保服務不中斷。

與談人認為未來應從技術供應商關係轉變為合作夥伴關係。因此，需要確保第三方組織擁有正確的風險文化並建立信任。

FTX 交易所和 Terra 的崩潰，使監管部門開始重視建構完整法制和理解 DeFi 領域的風險，但這不代表著監管部門會全面禁止 DeFi，監管部門可以考慮透過促進 Web 3.0 等創新和監理沙盒機制，允許可管理的混亂存在。技術可以成為實現社會目標的工具，特別是如果它是透明和負責任的，並且我們可以用正確的風險管理思維來管理風險。

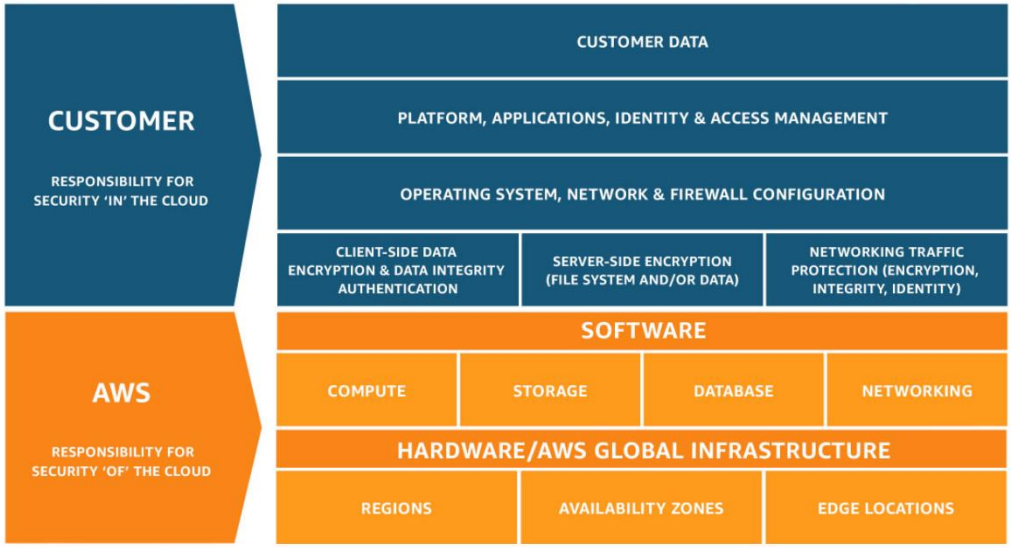
金融產業間需要互相合作，使資料共享更容易。監管部門和金融業應考慮創建資料使用及交換機制，以提高整體效率。

九、 分組報告 A：AWS 客戶保護計畫

分組報告係由 AWS 來介紹雲端服務的各種面向。AWS 考量雲端服務的安全與法律遵循是 AWS 和客戶的共同責任，因此提出「共同責任模型(AWS shared responsibility model)」的責任分擔架購[19]，以減輕客戶使用雲端服務的操作負擔。這種責任的區分通常稱為雲端「本身」的安全與雲端「內部」的安全，大致分工如下：

- **AWS 負責「雲端本身的安全」**– AWS 負責保護執行 AWS 雲端提供的所有服務的基礎設施。此基礎設施由執行 AWS 雲端服務的硬體、軟體、網路架構與設施組成。
- **客戶負責「雲端內部的安全」**– 客戶的責任因所選擇的 AWS 雲端服務類型而有差異。例如，當客戶選擇使用基礎設施即服務 (IaaS)時，客戶需要執行所有必要的安全組態和管理任務。若客戶選擇軟體即服務（SaaS）時，客戶應承擔之責任就較為簡單。

圖四：AWS 共同責任模型



AWS 為提升客戶對雲端服務的理解及信任，AWS 提供豐富的線上學習資源，並辦理多種類說明會及課程，AWS 並建立多種管渠道，使客戶與 AWS

[19] AWS，共同的責任模型，https://aws.amazon.com/tw/compliance/shared-responsibility-model/

Security 建立持續的審計關係，例如將 AWS 資訊安全控管政策及所取得之安全認證揭露在網路上[20]，以利客戶及監管單位瞭解。客戶也可透過 AWS Audit Manager 等工具，串接 AWS 系統，依客戶所設定之資訊安全評估框架獲取 AWS 所提供的即時審計資訊[21]。或是藉由 AWS 結合擴增實境技術之 Digital Audit Symposium(DAS)，線上參觀 AWS 機房。

十、 分組報告 B：落實客戶隱私風險管理

根據對近五年的數據隱私洩露事件之分析，可以歸納出幾個重點：(1) 由於地端資訊系統所保管的個人數據數量更大且時間長，數據洩露在地端資訊系統中較為常見。 (2) 安全漏洞之主要原因是使用者之網路或應用程序的安全保障措施不足、不當的安全組態設定(misconfiguration)，以及由於人為失誤導致的資訊傳遞錯誤。 (3) 對於雲端服務的數據保護原則和技術控制之熟悉程度，是雲端服務使用者實現法規遵循和善用雲端服務優勢之關鍵。因此，將安全控管和及數據保護之執行程序簡化有助於客戶有效利用雲端服務，因為客戶可以利用雲原生和支持雲端服務之自動化隱私控制機制，並清楚地了解客戶在雲端系統之個資控管情形。

個人資料保護在不同國家或地區之規範中，雖然內容有些差異，但可以歸納為五大目標：(1) 最大限度地減少個人資料的揭露，(2) 履行資料主體的權利或資料控制者和處理者的資料處理義務，(3) 提供個人資料功能和處理的透明度，以實現資料主體的監控和數據控制者的安全改進，(4) 在整個資料生命週期中保護個人資料，控管潛在的數據洩露威脅，(5) 預為應對緊急事件，並從中復原。

表格 1：不同規範下的個資保護共同目標

Objectives Enabled by Technical Measures	Data Protection Principles	O	A	E	T	S
Minimize data exposure	Collection limitation	X	X	X	X	X
	Purpose specification and use limitation	X	X	X	X	X
	Retention limitation			X	X	X
	Preventing harms		X			
Fulfilling data subject's rights	Notice, Choice, Consent, Individual participation	X	X	X	X	X
	Access and correction		X	X	X	X
	Purpose specification and use limitation	X	X	X	X	X
	Retention limitation			X	X	X
	Data portability			X	X	

[20] AWS Artifact，https://aws.amazon.com/artifact/
[21] AWS Audit Manager，https://aws.amazon.com/cn/audit-manager/

Objectives Enabled by Technical Measures	Data Protection Principles	O	A	E	T	S
Transparency	Data residency			X	X	X
	Openness	X	X	X	X	X
Security safeguards	Accountability	X	X	X	X	X
	Security safeguards	X	X	X	X	X
	Preventing harm		X			
Prepare for incident respond & recovery	Data integrity and quality	X	X	X	X	X
	Breach notification			X	X	X
	Preventing harm (via notification)		X			

O = OECD Guidelines; A = APEC Privacy Framework; E = EU GDPR;
T = Thailand PDPA; S = SG PDPA

為確保個人資料能受到完整保護， 雲端服務業者及使用者可以就五大目標制定相關控管措施，以控管個人資訊之安全及遵循相關個資保護規定。而目前 AWS 雲端服務已採取相關控管措施以協助客戶管理相關風險及法規遵循。

表格 2：針對五大個資保護目標，可採取控管措施

Objectives Enabled by Technical Measures	Applicable Controls
1. 資料揭露最小化 Minimize data exposure	1.1 資料最小化 Data minimization
	1.2 去識別化 De-identification
	1.3 資料所在地限制 Data location restriction
	1.4 資料加密Data encryption
	1.5 資料取得權限之控制Disclosure control
	1.6 隱私保護加密Privacy preserving encryption
	1.7安全銷毀 Secure data destruction
2. 履行數據主體的權利 Fulfill data subject rights	2.1 通知Notification
	2.2 個人資料自主權Individual autonomy
	2.3 同意追蹤Consent tracking
3. 提供處理的透明度和合規性保證 Providing transparency of processing and assurance of compliance	3.1 數據地圖/盤點Data map/inventory
	3.2 持續監督Continuous oversights
	3.3 法規遵循之評估、證明和認證 Compliance assessment, attestation, and certifications
	3.4 資料譜系Data lineage and provenance
	3.5 自動化安全檢查系統 Automated reasoning and formal verification
4.安全保障 Security safeguards	4.1 身份和訪問管理 Identity and access control (IAM)
	4.2 權限管理Privilege management
	4.3 資料加密Data encryption
	4.4 資料完整性控制Data integrity mechanisms
	4.5 代碼完整性驗證Code integrity

Objectives Enabled by Technical Measures	Applicable Controls
	4.6 反惡意軟體和威脅檢測 Anti-malware / Threat detection
	4.7 弱點管理Vulnerability management
5. 預為應對緊急事件及復原 **Prepare for incident response & recovery**	5.1 事件紀錄 Event logging
	5.2 因應緊急事件Incident response readiness
	5.3 高可用韌性之資訊架構 High-availability resilience architecture
	5.4 備份Backups

。

參、心得與建議

一、持續瞭解創新技術之其優勢、限制及產業實務動態

本次活動 IIF 所分享「去中心化金融：用例、挑戰及機會」報告詳實介紹去中心化金融之運作架構，並分享 DeFi 資金集中情況、節點託管情況等實務運作數據，這些資訊有助監管、司法或消費者保護部門理解去中心化金融應用並不如業者所聲稱的這麼去中心化，並非採用了區塊鏈技術就更值得信任，據以作為相關政策制定或執行之重要參考。

目前區塊鏈及雲端服務等創新技術正在快速改變既有金融產業之運作型態，同時也帶來新的風險，也對金融監理帶來變革 。例如英國金融主管機關考量近期金融機構對第三方業者之依賴程度日益增加，並多集中於亞馬遜、Google 及微軟等大型科技公司，為控管相關風險以確保金融穩定，研議將銀行之關鍵第三方業者(CTPs)納入監管。

我國金融機構在使用區塊鏈、雲端服務及 AI 等創新應用，目前尚在起步階段，建議持續透過國際會議、與業者座談、金融監管部門及國際組織之政策文件，瞭解相關創新技術之優勢、限制及產業實務動態等資訊，作為相關政策制定或執行之重要參考。

二、持續推動監理沙盒制度以鼓勵創新發展

本次會議中，多位與會者建議主管機關可推動監理沙盒機制與業者共同探索創新應用之可能監管方式部分，我國自 2018 年施行「金融科技發展與創新實驗條例」至今，已有 8 件申請案成功通過審核進行實驗，並已有數案已成功落地，獲法規調適並已實際商轉，其中沙盒申請案中亦不乏採用區塊鏈技術者，顯示業者對運用區塊鏈技術於金融產業之期待。

對於使用區塊鏈技術進行募資，櫃買中心已訂定「證券商經營具證券性質虛擬通貨業務管理辦法」，該辦法已於 2020 年 1 月 20 日施行。該 STO 規範之募資對象僅限於專業投資人，且每一投資人認購限額不得逾新臺幣 30 萬元，發行人於同一平台總募資上限金額為新臺幣 3,000 萬元，投資人得與交易平台進行議價買賣，超過前揭限額者應申請監理沙盒個案進行審查。惟至今未有依前揭管道進行募資之案件。

監理沙盒係近年各國金融監管單位探索創新技術之重要監管政策，若未來規劃將使用區塊鏈技術之加密資產納入金融監管，考量區塊鏈之資料架構涉及個資保護、跨機構資料傳輸、第三方服務廠商管理、跨業經營等議題，可參酌國際作法，在推動監理沙盒政策規劃之同時將加密資產之特性及實務需求納入考量，設計合適之測試環境以探索監管制度之可行性。