金融穩定委員會（FSB）「去中心化金融之金融穩定風險」報告摘譯

本公司資訊處及中區辦事處摘譯

壹、前言

加密資產市場正快速發展中，因其規模、結構脆弱性及與傳統金融系統日益緊密的關聯性，可能會對全球金融穩定構成威脅。在加密資產生態圈（crypto-asset ecosystem）中，去中心化金融（decentralised finance, DeFi）已呈現快速成長。去中心化金融泛指加密資產市場中企圖複製傳統金融系統（traditional finance system, TradFi）相關功能之各種服務，並將服務條款去中介化及治理去中心化。

在去中心化金融中，傳統金融機構與市場基礎設施在不同程度上被公共區塊鏈（permissionless blockchains（註1））的智能合約（smart contracts）所取代。去中心化金融主要提供加密資產選擇與競爭的點對點或點對池（peer to peer/pool）金

本文係中央存保公司摘譯 2023 年 2 月 16 日發表於金融穩定委員會 (FSB) 之「去中心化金融之金融穩定風險」（The Financial Stability Risks of Decentralised Finance）報告，非 FSB 官方翻譯。本篇文章無償取材自金融穩定委員會網站 (www.fsb.org)，本文中譯內容如與原文有歧義之處，概以原文為準，原文網址連結如下：https://www.fsb.org/wp-content/uploads/P160223.pdf

融服務市場，涵蓋各種交易、借貸等大部分在加密資產領域的活動。去中心化金融近期發展已引起各家國際組織關注，並發表多篇報告闡述該行業特點、重大風險及對傳統金融市場潛在影響。

2022 年 5、6 月間加密資產及去中心化金融之市場動盪，曝露其仍存在許多漏洞。2022 年 11 月加密資產交易平台 FTX 倒閉，亦曝露加密資產中介功能存在相關漏洞，惟該兩起事件風波皆未明顯蔓延至加密資產市場以外。

這些被視為「壓力測試」的事件結果，表明傳統金融目前尚未與去中心化金融或加密資產生態圈有高度連結，也反映現今保守的監理方法。然而去中心化金融的規模及與傳統金融的關聯性會隨著時間而增長，進而增加危機事件影響的程度，因此有必要對去中心化金融的金融穩定採取前瞻性的監理方式，監控和縮小數據落差，不僅有助主管機關評估及調整其監理立場與框架，並有助於確保在面臨金融穩定風險時進行干預，還可以使傳統金融參與者在考慮參與去中心化金融時評估其風險。

本篇報告旨在概述去中心化金融的重要特徵與漏洞，以評估潛在的金融穩定威脅及擬訂政策，報告概分五段，首先介紹去中心化金融之背景，包括生態圈、關鍵要素、參與者及主要商品；其次討論去中心化金融漏洞（vulnerabilities），包括與傳統金融相似漏洞及潛在漏洞；第三，概述去中心化金融可能情境、採取的對策及對金融穩定相關結果；第四，討論數據落差及建立去中心化金融監控框架步驟；最後一段為結論。

貳、去中心化金融之背景

一、去中心化金融生態圈

(一)關鍵要素及參與者

去中心化金融生態圈為複雜網路連結，涉及不同相互關係及利益的參與者，包含創造協議者、開發者、去中心化自治組織（decentralized autonomous organizations, DAOs）、資助者（如創投或私募基金）、及機構與零售終端用戶等。去中心化金融遵循多層式架構，每層皆有獨特目的：

1.非許可制區塊鏈：為生態圈的骨幹，提供分類帳本，記錄交易且無法改變（結算層），因其公開及無需經過許可的特性，這些區塊鏈可供任何參與者存取，故類似於在傳統金融系統中受信任的第三方，對記錄合法性提供透明度和信心。

2.智能合約：在區塊鏈上以自動執行的方式履行交易條款及條件。

3.去中心化金融協議（DeFi protocols）：規範提供商品與服務的條款、條件及標準，以管理特定的活動及任務，有部分會結合智能合約及用戶端界面，並涉及許多相互關聯的交易。

4.去中心化應用程式（decentralized applications, DApps）：支援協議的應用層，允許用戶端透過圖形界面與智能合約進行互動，以促進去中心化金融提供金融中介服務。

多數的協議都是無需許可且任何人都可以匿名（或用假名）來存取，如擁有適當設備與專業知識即可入門，某些去中心化應用程式由創投業資助以交換取得治理權或加密貨幣，這些去中心化應用程式由瞭解協議的人員進行開發，且這些人員可能擁有治理權或加密貨幣的管理密鑰（administrative keys），代表去中心化協議實際上可能操控於一組利益集團。

(二)去中心化金融與傳統金融相同及差異之處

富有效率與彈性的金融體系最終目標，是在風險和不確定性的情況下，為資源分配執行中介以支持實體經濟活動。為實現目標，金融系統需要執行許多相互關聯的功能如下：

- 提供支付服務，以便交易商品與服務，或轉讓貨幣價值。
- 允許籌集資金以利執行大型計畫。
- 能夠穿越時空進行資源轉移。
- 讓經濟個體能夠管理不確定性及控制風險。
- 提供價格資訊，以協調去中心化決策制定。
- 減少因交易一方比另一方擁有更多資訊，所引起的資訊不對稱及激勵問題。

目前去中心化金融的商品和服務主要係與同屬去中心化金融的其他商品和服務互動，而不是與傳統金融及實體經濟互動，儘管去中心化金融提供新穎的服務流程，但在功能上與傳統金融並沒有本質上的區別，例如：

- 去中心化的參與者在交易平台的日常運作上提供各種資產價格的資訊。
- 集中資源支援大型的專案，此為許多去中心化金融協議的本質功能。

然而傳統金融使用的是受到監理的中介機構提供的資訊，這些中介機構要被信任才能執行這些任務（因受監理而被信任），但去中心化金融的目標是用電腦程式及去中心化的方式來驗證交易的合法性，及執行資金交易的可用性，以取代傳統方式，儘管這些方式目前仍不符或超出監理範圍，但傳統金融與去中心化金融的潛在激勵及活動本質上沒有區別，只有執行功能的方式不同。

(三)推動去中心化金融發展之因素

加密資產與去中心化金融之背後有許多供需因素推動其成長。在供給方的因素有：

- 高速運算、密碼學等技術創新

  為加密資產的發展提供機會，如以太坊運用智能合約提供區塊鏈及穩定幣（stablecoins[註2]）（通常參考美元）服務的發展極為重要。

- 穩定幣提供穩定的轉移工具及維持價值

  穩定幣雖然有不同的設計，但它們提供通用的機制可以在各種去中心化金融協議之間進行交易，因此由 Tether 或 Circle 等中心化實體機構所發行的穩定幣，可用於購買、結算、交易、貸放及借入其他加密資產，在去中心化金融生態圈中發揮重要作用。

在需求方的因素有：

- 2008 年金融危機產生的影響

  發展金融中介機構去中心化替代方案的關鍵推動因素乃來自於 2008 年金融危機所產生影響，一些投資者可能會因加密資產與去中心化金融具有吸引力而選擇遠離傳統的供應者，並在加密資產領域找到較有吸引力的收益。

- 2008 年金融危機後持續低利率

  因為除加密資產領域真正的信徒及害怕錯過機會的人外，2008 年金融危機以後持續低利率情況，也促使投資者尋找機會投資高風險及高收益之資產。

- 對通貨膨脹的避險

  近期多元化投資組合收益對通貨膨脹的避險，也吸引投資者湧進此一領域，儘管最近的分析顯示加密資產開始呈現與股票等金融資產具有高度相關性。

在全球持續通貨膨脹壓力的背景下，近期市場動盪顯示加密資產市場的脆弱性，有關盜竊、欺詐與市場濫用的新聞，已提升監理機構的關注度，且不確定未來加密資產和去中心化金融在多大程度上可保持與市場週期無關或反市場週期的吸引力。

去中心化金融市場主要由先進經濟體的機構參與者推動，而散戶投資者、新興或低收入經濟體的參與相對較少，且因去中心化金融生態圈的接觸方式複雜，交易成本與許多去中心化應用程式所要求的超額抵押，可能會限制不喜好太過複雜或是資本不足的參與者直接參與生態圈的機會。

二、 去中心化金融之特性

(一)營運獨特性：簡述去中心化金融之特性與各類組件，及彼此與外部間互動方式。

1.「智能合約」是推動去中心化金融發展的關鍵創新

智能合約以自動方式履行交易條款及條件。雖然協助執行交易之自動化程序在傳統金融已使用多年，但僅限用於中介及連接機構（intermediary and connecting institutions），或交易鏈之特定流程，例如交易或造市演算法（trading or market-making algorithms）。

去中心化金融新穎之處在於應用區塊鏈技術，以及任何人都可以參與有智能合約所要求的加密資產，依去中心化金融協議開發完成後，智能合約就會部署在每個網路節點上，透過獨立的預言機所取得的數據，

來確認是否滿足所需的執行條件。

對於使用相同智能合約的任一節點，該合約的執行結果都是一致的且可防止被篡改，去中心化金融協議通常具備去中心化自治組織（DAO）或其他治理方式，就變更之處達成共識，換言之「智能合約」用詞非屬恰當，其實並不聰明，因為它不會對外部的刺激直接反應或改變，只會在達到預先定義的條件時執行代碼。

另外也不一定是合約形式，因為還不清楚是否可在法院（司法管轄區）強制執行，儘管某些司法管轄區已在評估智能合約在法律體系中的地位。

2.區塊鏈「原生代幣」激勵生態圈的參與者

由於沒有可信任的中央（主管）機構，區塊鏈的安全性取決於參與驗證交易的實體驗證者（例如挖礦者）經濟上的激勵，驗證者透過區塊鏈的原生代幣（交易費用，或 gas（註3））獲得補償，這些代幣於去中心化金融協議的相關活動中可代表一定的價值，而投資者也持有原生代幣，原生代幣的內含價值可用作抵押品，或因投機、交易等目的而持有，例如以太坊區塊鏈上的以太幣，它扮演非常重要的地位，以激勵支持去中心化金融功能與生態圈的參與者。

3.可組合性（composability）創建錯綜複雜且相互依賴的網路關係

去中心化應用程式的開放源代碼（open-source）特性允許開發人員可將去中心化金融的元件組合應用，以創作全新或高度複雜的商品，此特性被稱為去中心化金融「樂高積木」。

藉此特性，一個代幣就可能促成各種活動，可組合性地創建錯綜複雜且相互依賴的網路關係，使資產循環利用於不同應用程式，同時也造成額外的複雜性，這些相互依賴關係使追蹤及檢測更為困難，且因相互關聯而產生漏洞。

4.自行保管加密資產的控制及交易權

依去中心化金融協議，參與者通常會保管加密資產的控制及交易權，直到決定將加密資產投入到某個智能合約，儘管有各種不同風險和

複雜度的解決方案，但活動過程需要參與者具備高度技術知識，且因結算層使用的區塊鏈技術是無法變更記錄的，因此沒有第三方可控制已發生的交易。

5.「預言機」與「跨鏈橋」為去中心化金融活動提供關鍵機制

- 預言機（oracles[註4]）

  使智能合約能夠存取外部（或鏈下 off-chain）真實世界數據，所以它們是去中心化金融能夠溝通傳遞的基礎，因智能合約可能需要存取鏈下（即公用分散式帳本以外）或不同鏈上的各種數據作判斷。

- 跨鏈橋（cross-chain bridges[註5]）

  是跨區塊鏈的互動機制，可發行合成代幣以代表在不同區塊鏈上的各種資產及其他類型代幣，同時保有其潛在的經濟價值，跨鏈橋通常持有或存儲來自於某一區塊鏈的代幣，並在另一條區塊鏈上發行或釋放具有相同價值的代幣，所以代幣持有者可以跨鏈進行交易，因跨鏈橋擁有大量的加密資產而成為攻擊目標，也曾遭到盜用跨鏈橋內的代幣。

(二)外部依賴關係

1.去中心化金融高度依賴加密資產領域的基礎設施與中介者

例如區塊鏈網路、鏈下基礎設施、中心化加密資產交易平台（CEX）、預言機、跨鏈橋及穩定幣等，這些高度依賴的部份卻也高度集中，例如智能合約需要記錄在公用區塊鏈上，故依賴其運作是否正常，及受到容量上的限制，像多數的去中心化金融應用程式都建立在以太坊區塊鏈上，但該區塊鏈卻經常出現擁塞現象。

許多去中心化金融協議都將其服務擴展到多個區塊鏈，以成本較低的方式處理，但付出的代價為碎片化（fragmentation）。

2.與傳統代理人或市場相關的外部關聯性較弱

但仍存在依賴性，例如傳統金融中介機構為加密資產領域的關鍵參與者提供各種標準化的金融服務，包含託管穩定幣發行者的儲備資產，

或代表穩定幣發行者所持有的法定存款帳戶，像傳統金融機構支援如專業銀行及加密資產 CEX 等客戶的資金和取款需求，以促進加密資產生態圈，以及將資金引入去中心化金融。

另外作為去中心化金融交易抵押品的鏈下資產代幣化程度不斷提升，以及中央銀行發行的數位貨幣（CBDC）如果得到廣泛的開發及使用，可能會產生更緊密的聯繫，增加對採用的機構及對第三方服務提供商的依賴。

(三)去中心化金融協議治理結構

1.「去中心化金融協議治理」指決策的範圍及實施決策的流程

去中心化金融應用程式聲稱已具有去中心化的所有權及治理結構，但在某些去中心化金融協議的決策卻是集中的，儘管目前已出現去中心化自治組織（DAO）的新治理形式，雖聲稱為所有成員共有且無中心化領導，但因底層去中心化金融組織結構，其去中心化的實際程度差異很大，故往往實際上並非如此。

2.投票權通常與持有的治理代幣（governance tokens[註6]）成正比

DAO 聲稱由社群管理，不該有單一權威或管理團隊來決定未來，而是完全由社群成員共同決定，而其投票權通常與 DAO 持有的治理代幣成正比，原則上任何人都可以有投票權，但實務上投票機制可能高度集中且不透明。

像某些去中心化金融協議在決策過程上，需要更緊密地參與社群，且更具有協商性（consultative），某些協議還要求有大量的參與者投票，然後開發人員才能進行重要的變更或否決，這些方法對市場參與者和監理機構並不完全透明，理論上分散式的決策過程有助於將權力下放，使社群充滿活力，且利害關係人皆能得到回應，但另一方面如果沒有被委派的授權者時，決策將需要更長時間及較低的效率，所以當軟體開發人員為支持 DAO 而放棄對代碼的控制權時，修復任何問題可能都需要 DAO 的決策，代表軟體錯誤或升級等可能無法及時處理，並需視協議決策過程的效率而定。

三、 去中心化金融提供之商品與服務

去中心化金融主要為透過協議智能合約應用程序等不同元件形成一種自給自足的自我參照（self-referential）系統，並不直接為實體經濟提供服務，然而去中心化金融提供的加密資產服務與傳統金融的功能相似；常見的有為促進去中心化金融借貸、交易（包括保證金交易）、資產管理及衍生商品，許多去中心化應用程式提供多種且相互重疊，而常不易明確劃分界限的功能。

(一)「去中心化借貸」依賴的是抵押品而非借款人的信譽

1.多數去中心化金融貸款沒有特定期限

去中心化金融借貸平台如 Aave、Compound 及 MakerDAO，基於貸放方所提供的資產集合以賺取利息，因參與者的身份通常未知，所以依賴的是抵押品，而非借款人的信譽，多數去中心化金融貸款沒有特定期限（有時被稱為「永久」），且可以隨時償還。

2.貸款幾乎皆以加密資產作為抵押品

因缺乏信賴關係，故需要一種機制以確保可償還貸款，所以去中心化金融貸款幾乎皆以加密資產作為抵押品，且通常需要超額抵押（通常設定為抵押品的 80%），且在約定時限內，抵押品需時刻維持在約定價值以上，否則借款人須補足抵押品，如不提供額外抵押品，原抵押品將自動清算。

3.閃電貸（flash loans）是去中心化金融獨具的區塊鏈結算程序

閃電貸能夠在同一區塊鏈交易中即時借款、執行交易及償還貸款，閃電貸的交易都在同一個區塊內，交易為全部結算或全部不結算，又被稱為「原子結算」，其貸款期限為零，無需抵押品，主要用於加密資產套利及交易，其特性也容易被市場操縱者和攻擊者（閃電攻擊）用來借入大量加密資產，在不同平台上同時操縱價格，或利用相關協議的治理漏洞。

(二)「加密資產交易平台」可以讓用戶交易加密資產或法定貨幣

交易平台有中心化（CEX）或去中心化（DEX）二種不同形式，後者

為去中心化金融獨有特徵，DEX 不允許用戶將加密資產換成法定貨幣。

DEX 係以自動結算智能合約為基礎來進行點對點或點對池的交易，且不需要像 CEX 要在平台營運商先存入資金，二種最著名的 DEX 交易類型是訂單簿交易（order-book exchanges）及自動造市商（automated market makers, AMM）。

1.訂單簿交易

通常在鏈下維護訂單簿，而在鏈上結算，買家及賣家將訂單給第三方（中介者）或 DEX 營運商，營運商再將訂單發佈到訂單簿且公開訊息，使交易對手（訂單收受者）獲知訊息及配對交易。

2.自動造市商

扮演如同傳統造市商的角色，以確保加密資產的流動性（例如以太幣（ETH）或泰達幣（USDT）），需要流動性的用戶可應用在智能合約中的流動性池（liquidity pools），任何想要提供流動性以賺取費用的用戶可存入資金，當池中減少或增加一定數量的代幣時，池中的資產價格與市場資產價格間可能會產生價差套利機會，套利交易可解決價格不均問題，價格將依預先定義的公式進行調整。

(三)「資產管理」與「收益耕作」使參與者可獲取最大報酬

1.資產管理

有些去中心化金融協議提供資產管理服務，利用智能合約將散戶存入的加密資產匯集成投資組合。完全去中心化的鏈上基金會以程式碼取代投資經理人，並使投資組合自動再平衡，及確保基金依據程式規則與風險狀況，執行遵守預先定義的投資策略。

2.收益耕作（yield farming）

去中心化金融參與者為獲取最大報酬，會經常跨越不同去中心化金融平台進行加密資產貸借，及提供服務以換取加密資產，這類活動稱為「收益耕作」。

3.收益聚合器（yield aggregators）

雖然參與者可以獨立作業，但過程需手動且乏味，而「收益聚合器」

則用來促進此過程，協助制定資金分配於多項去中心化金融協議的策略，透過掃描各去中心化金融協議及策略，自動將資產存入智能合約以賺取獎勵，可降低交易費用及最大化利潤，並促進在多個平台之間轉移代幣的複雜策略來賺取服務費。

(四)「衍生商品」及「合成資產」價值取決於一或多個標的資產或可觀察變量的價值波動

去中心化金融以代幣的形式創造其衍生商品，價值取決於一或多個標的資產或可觀察變量的價值波動，如衍生商品參考股票、商品、加密資產、商業創新的現金流，或事件的預測結果。

代幣化衍生商品可能無需中介機構（例如傳統金融結算所的交易商），且通常是由程式碼控制該等商品的管理維護及抵押品自動清算，有些代幣化衍生商品需要參考預言機或第三方資訊系統，以追蹤取得標的資產或變量資訊。

(五)「保證金交易」利用槓桿操作額外的加密資產

有些去中心化金融協議可為用戶提供商品與服務的保證金交易，傳統的金融中介（經紀人）被智能合約取代，以去中心化和非託管的方式，交易者可以開設保證金帳戶，將加密資產轉移到該帳戶，利用槓桿（操作額外的加密資產）建立多頭或空頭部位，槓桿程度為借入資金與保證金（交易者提供資金）的比率，在開倉期間以保證金充當擔保品（抵押品），如在某時點保證金價值低於一定門檻時，抵押品將自動清算。

參、去中心化金融之漏洞

本篇報告係運用 FSB 金融穩定監理框架（Financial Stability Surveillance Framework，該框架係設計用於分析影響全球金融體系之漏洞），分析去中心化金融之漏洞。雖然去中心化金融為獨立生態圈，然而也同有傳統金融之大部分漏洞，因為不夠成熟且正在迅速發展，再加上其新穎的技術特性，監理框架必須以更具前瞻性的方式套用於去中心化金融。

關鍵是去中心化金融複製傳統金融系統的某些功能，故承襲並可能重複或放

大該系統的漏洞，包括眾所周知的漏洞，如營運脆弱性（operational fragilities）、流動性與期限錯配（liquidity and maturity mismatches）、槓桿（leverage）及相互關聯性（interconnectedness）。

去中心化金融的特性可能導致這些漏洞的作用方式不同於傳統金融，例如拋售風險、智能合約抵押品自動清算等相關效應、使用預言機或依賴底層區塊鏈，這些已知的漏洞來自新技術的特性、參與者間高度的結構關聯性，以及不遵守現有監理要求或缺乏監理。

近期事件顯示，隨著生態圈不斷發展及演變，去中心化金融與生俱來的漏洞雖尚未威脅全球金融穩定，惟仍需持續監控。去中心化金融相關漏洞分析如后。

一、營運脆弱性

營運脆弱性指因去中心化金融的特性導致營運中斷或失敗，無論原因為何皆會對提供相關服務及商品有不利影響。

(一)去中心化金融的「治理安排（governance arrangements）」可能對金融穩定產生不利影響

1.誤導參與者認知

去中心化金融通常採用新的治理安排，對金融穩定可能產生不利影響，不清楚透明、未經測試或易受操控的治理框架，可能會誤導用戶對於去中心化金融活動聲明與保障措施的認知。

例如開發人員及創辦人在收到初始投資後，可能缺乏繼續開發去中心化應用程式的動力，這可能會使用戶面臨詐騙（捲款潛逃）風險（rug pulls[註7]），此風險係因實務上難以要求開發人員和創辦人承擔責任（道德風險），因其經濟激勵方式不明確且揭露不足。

2.投票參與度不足

另外主要的 DAO 及去中心化金融協議之投票權極為集中，代表實際上只有少數參與主導者可以提出、通過或實施倡議，某些情況下由於代幣被抵押或不在線上（例如治理代幣保存於離線錢包（cold/offline wallets[註8]）），投票參與度可能很低，或投票權被委託給持有治理代

幣卻不參與投票的個體，社群可能會出現分歧，而產生分系或分裂現象，帶來負面結果而導致投資者蒙受損失，且對 DAO 或去中心化金融協議失去信心，效應將可能蔓延至其他市場。

(二)依賴的區塊鏈網路中斷而遭受損失

去中心化金融的特徵是去中心化金融協議高度依賴基礎設施，且去中心化應用程式受到底層區塊鏈的技術限制，中斷、網路堵塞或共識失敗導致區塊鏈中斷，可能會影響區塊鏈和相依的去中心化金融服務成本、功能和效能，且可能導致去中心化金融用戶被迫清算及遭受損失。儘管有這些挑戰，區塊鏈仍在某些應用上添加彈性，例如可縮短保管鏈及提升透明度。

(三)智能合約的複雜性導致錯誤難以補救

智能合約具有許多營運相關漏洞。由於去中心化應用程式會使用各種無法停止、修改或逆轉的智能合約，故智能合約在部署前需考慮許多可能狀況而致複雜，然其複雜性反過來又會增加編碼錯誤以及意外的可能性。

更加複雜的是，智能合約代碼被廣泛重複使用，因此各自獨立的合約可能內含相同的技術漏洞，且因去中心化金融交易為不可變，如發生錯誤（或詐欺），則無法撤銷及恢復錯誤發生前的狀態（或需要受影響的各方及交易者達成協議，與區塊鏈驗證者的共識），與傳統金融相比，去中心化金融的事後補救方式具不確定性，且法律上難以追究責任。

(四)預言機與跨鏈橋風險產生的負面影響

1.預言機風險（oracle risk）

許多去中心化金融的功能高度依賴預言機以執行鏈下操作或從鏈下來源取得數據，也可以導入第三方供應商和流程，如未按預期運行或損壞時為「預言機風險」，遇輸入錯誤或攻擊時，可能會觸發執行如清算、追加保證金等動作，或對其他協議產生負面影響（例如演算法儲備資產或抵押品管理）。

預言機也可能受到市場操控，透過操縱智能合約的預言機以影響去中心化金融合約的績效。當主要協議依賴預言機或許多協議依賴單一預

言機時，對於預言機發生衝擊或蔓延時將是關鍵因素。

2.跨鏈橋風險

另一個營運漏洞則是跨鏈橋，單獨的區塊鏈彼此無法互動，跨鏈橋從區塊鏈或協議中持有或收集資產，在另一區塊鏈或協議上發行或釋放相同價值的資產（通稱包裝代幣（wrapped tokens））。資產持有者可跨鏈或跨協議進行交易，但會創建有大量資產的儲存庫，而成為竊盜或挪用的目標。

這也形成營運風險傳播的另一途徑，而共識機制（consensus mechanism）傾向高度集中化則更加劇風險。受損的跨鏈橋可能使鎖定在來源鏈上的資產遺失或被盜取，並導致在目標鏈上包裝代幣的價值崩潰。

二、流動性與期限錯配

去中心化金融最令人關注的漏洞為流動性與期限錯配，源自於相關實體的負債及資產具不同流動性和期限配置。期限無法互相匹配將導致營運風險，且對金融系統有外溢效應，此為眾所周知的風險，也是傳統金融需受監理干預的關鍵理由。就去中心化金融與加密資產市場，一如 2022 年 5、6 月間與同年 11 月的市場動盪及倒閉事件所示，此類流動性風險特別會在穩定幣或借貸協議及平台產生。

(一)流動性較低的資產可能產生贖回風險或擠兌風險

流動性錯配導致的穩定幣贖回擠兌風險已有許多記載討論，2022 年 6 月 TerraUSD/Luna[註 9] 崩盤的影響不只波及與其高度相關的去中心化金融借貸協議 Anchor[註 10]，且贖回風險範圍亦不限於演算法穩定幣（例如 TerraUSD），穩定幣發行者所持有準備倘屬於流動性較低的傳統金融資產（如商業票據或定存單）也會有擠兌風險，此與曾為金融危機根源的貨幣市場基金雷同。

不遵守法規或僅受到有限或薄弱的監理，或在類似傳統銀行與非銀行實體間流動性轉換時不受監理的穩定幣，可能失去鎖定價格，而對去中心化金融生態圈造成更廣泛的影響。此外，衝擊還可能傳播至穩定幣的投資

市場，如政府債券、公司債及商業票據。

(二)期限錯配導致無法滿足贖回需求

去中心化金融（及中心化金融（centralised finance, CeFi））中介也存在流動性錯配，特別是借貸平台上提供更高收益率是藉由承諾投資者可立即贖回的方式，卻將存款投資於流動性較差的資產，及利用借款人的抵押品來借入和投資更多資產。當流入大於流出時，模型允許基金或平台從流動性溢價或期限溢價中獲益，然而當市場轉為贖回需求提高時，基金或平台可能無法滿足其要求。

(三)被迫停止提款交易的真實例證

Lido（註 11）在 2022 年 5 月遭遇的衝擊是借貸協議漏洞的另一例證，Lido 讓以太幣（ETH）持有者於賺取收益同時也質押 ETH，Lido 投資者使用質押的 ETH（以太幣憑證 stETH）以提升在 Anchor 協議的報酬，因而在 Lido 商業模式及 Terra 區塊鏈間建立互相依賴關係，又對中心化金融借貸平台 Celsius 造成連鎖反應，該平台對某些 stETH 存戶提供高報酬並可隨時贖回，在 TerraUSD 崩潰及 stETH 相對 ETH 的價值下跌時，Celsius 被迫停止提款交易，造成去中心化金融相關的加密資產行業的壓力。在 2022 年 11 月 FTX 倒閉時也觀察到類似效應，有些加密資產行業實體暫停客戶提款。

三、 槓桿作用

加密資產市場的關鍵特徵之一是槓桿對市場動態的巨大影響，由於其匿名性，去中心化金融中介高度依賴抵押品的槓桿作用。與傳統金融相同，槓桿作用會擴大景氣循環（procyclicality），可能引發價格大幅調整造成其他市場參與者的連鎖反應。

(一)動態去槓桿化（deleveraging dynamics（註 12））引發對穩定性擔憂

所以去中心化金融在槓桿管理上，特別強調動態去槓桿化（特別是抵押品自動清算），此自動化風險管理工具有助保護貸方，但因其造成的外

部性，而引發對去中心化金融生態圈穩定性的擔憂，因在協議中抵押品價值低於一定門檻時會觸發自動清算，抵押品可能會在流動性較低的市場中被強迫清算，從而壓低抵押品的價格，且效應將會擴散。

在傳統金融中，此自我強化的機能可以透過中央的有序清算來緩解，或者透過市場熔斷機制來阻止，但去中心化金融並未存在這二種機制。

在 2022 年 5、6 月市場動盪期間呈現出槓桿引發的繁榮與蕭條變動現象，初期不論機構或散戶投資者皆使用大量槓桿以追求更高的報酬，但隨著加密資產價格下跌，槓桿部位導致追加保證金或自動清算，迫使價格劇烈惡化。

(二)不易衡量槓桿作用的影響程度

值得注意的是，去中心化金融的確切槓桿數量很難衡量，原因之一是在加密資產市場中，借入資金常被當成其他貸款的抵押品，而產生「抵押品鏈」（類似再抵押（re-hypothecation））。所以優化對抵押品重複使用的衡量方法及開發其他槓桿衡量工具，有助於估計特定去中心化金融協議的槓桿程度，並可構成去中心化金融及加密資產風險監理框架的一部分。

四、 相互關聯、集中度及複雜性

去中心化金融生態圈內部與外部實體（特別是中心化金融、加密資產市場其他領域及第三方技術提供商）彼此間存在廣泛之相互關聯性。從金融穩定的角度，可認為多樣性能帶來好處，假使系統一部分受到衝擊時，其他部份尚具補償作用，有助維持系統穩定。另一角度是去中心化金融具有複雜之網路關聯性，可能擴大漏洞。

(一)「可組合性」放大去中心化金融生態圈內風險傳染的範圍與速度

去中心化金融協議具可組合性（類似樂高積木），支持者認為是重要的效率來源，可增加生態圈內的相互關聯。去中心化應用程式常採用多個智能合約且與多個協議交互作用，所以智能合約彼此具有高度相互依賴性，因此，個別智能合約的技術問題可能產生負面外溢效應，並於系統中傳播；可組合性則放大去中心化金融生態圈內風險傳染的範圍與速度，且

可能導致智能合約以意料之外的方式相互影響。

(二)高度依賴少數中介機構及系統提供關鍵功能與複雜的相互關聯性致使風險提高

因去中心化金融之中介業務常依賴少數關鍵中介機構及系統提供服務，致使集中風險提高，另去中心化金融內、外部實體的複雜關聯性並非全部透明，更使風險加劇。

1.相關活動高度集中於少數協議及區塊鏈

儘管目前應用程式數量眾多，相關活動卻集中於少數協議，截至 2022 年 10 月，合計前四大去中心化金融應用程式的總鎖倉價值（total value locked, TVL（註 13））占整體去中心化金融總鎖倉價值之比率高達 75% 以上。

因此任一大型協議發生事故都可能產生外溢效應，例如 TerraUSD/Luna 與 FTX 崩潰倒閉事件所造成的連鎖反應。

此外，相關活動也高度集中於以太坊區塊鏈（約占去中心化金融總鎖倉價值之 60%），因此，對於惡意行為或因以太坊區塊鏈基礎設施維護或升級所造成的中斷，都可能影響整個去中心化金融生態圈的運作。

2.生態圈交易對手間複雜的相互關聯性

去中心化金融平台亦會面臨與中心化金融交易平台相同的危機事件。後者常提供用戶友善的界面，使去中心化金融能觸及更多投資者以提高商品流動性，通常在整個加密資產與去中心化金融生態圈中都有交易對象。

雖然 CEX 促進去中心化金融協議的存取及交易，但由於在市場上的活動軌跡規模過大，反而加劇風險。

另有許多平台不遵守規則或不遵守監理框架，導致所有權過度集中、託管安排不佳、流動性不足、價格操控、詐欺及其他不當行為的風險提高。

再者，CEX 通常會經營與交易無關的區塊鏈相關活動，且可能與加密資產及去中心化金融生態圈中的交易對手互相關聯，例如透過去中心

化金融協議進行借貸或投資。

因此，相關平台經常需面對可能的利益衝突、客戶資金混用及業務組合不適當等問題浮現，並且去中心化金融與中心化金融平台之間相互聯繫會提高雙邊外溢效應。

以加密資產交易平台 FTX 為例，FTX 與 Solana 加密資產生態圈及其原生代幣（SOL）具有密切關聯，且對去中心化金融交易平台 Serum 有高度控制權。2022 年 11 月底 FTX 倒閉，引發投資者對 Serum 和 Solana 區塊鏈產生更大的擔憂，導致相關代幣價格大幅下跌，並使 Serum 應用程式終止。

3.依賴第三方服務

另外去中心化金融也依賴第三方提供商，去中心化金融協議需以預言機執行智能合約的代碼，而預言機又依賴鏈下數據。去中心化金融生態圈多數組件都依賴第三方服務，例如底層網路基礎設施或雲端服務等。

五、其他漏洞

(一)市場誠信問題外溢導致影響金融穩定

市場誠信問題通常與傳統金融穩定沒有直接關係，因此很少有足夠的量能及速度散播，然而去中心化金融仍處於起步發展階段，嚴重的市場誠信問題會導致負面信賴效果而產生外溢效應，當去中心化金融持續發展，並與傳統金融及實體經濟的關聯更為緊密時，則可能影響金融穩定。

1.非永續商業模式崩潰產生廣泛連鎖反應

去中心化金融有一項重要市場誠信問題係來自於非永續商業模式（unsustainable business models），由於有些商品需依賴持續的投入以回報早期參與者，可能產生系統性風險。基於技術複雜性及不透明性，再加上散戶投資者，使得加密資產與去中心化金融市場特別適合發展此類商業模式。

例如 Anchor 協議依賴投資者持續成長，否則將無法持續提供貸方

報酬，當該協議消滅並導致 TerraUSD 崩盤，即屬此種漏洞案例之一。隨著 TerraUSD/Luna 崩盤與 FTX 破產事件發生，此類商業模式崩潰事件所導致的損失，會削弱投資者的信心與財富，並可能產生廣泛連鎖反應。

2.不合法的金融服務及規避監理使參與者發生損失

另外去中心化應用程式以不符合金融法規的方式提供金融服務及規避監理，使散戶與機構參與者面臨市場操控或公然詐欺等相關風險。例如去中心化金融用戶會遭遇的特殊操控行為，利用「礦工可提取價值（miner extractable value）」（或稱「最大可提取價值（maximal extractable value[註 14]）」）的搶先交易行為來影響交易的公平性和正當性，市場參與者也會遭遇詐欺、駭客攻擊及竊盜等風險，以及投資發生重大損失卻無法求償的風險。

(二)跨境監理套利

因去中心化金融平台及治理結構具有跨境特性，難以認定所有權與控制權及相關司法機構，意指去中心化金融跨境關聯性非常不透明，去中心化金融行業通常沒有明確經營地點，故可能聲稱不受司法、監理機構、消費者保護及清理機構的管轄。去中心化金融協議跨境營運需要與該協議的司法管轄區監理機構合作，如果協議用戶透過虛擬專用網路（virtual private networks, VPN）偽冒地點時，則難以確認其管轄區。某些去中心化金融行業可能故意採用跨境架構以進行監理套利，利用跨境監理或司法合作的漏洞，逃避監管或執法，所以需要更全面的全球金融主管機關彼此協調合作以應對這些挑戰。

(三)「加密化」使貨幣政策管理更為複雜且損害貨幣主權

去中心化金融的成長也有助於取代貨幣，特別是在高通貨膨脹、總體經濟不穩定、央行信譽薄弱及銀行業效率不彰的國家，這些國家的人民可能購買加密資產，作為比貨幣更可靠的保值方式，此行為即稱為「加密化」，當去中心化金融更廣泛應用時會加速此現象。加密化可能會使本國貨幣政策管理更為複雜且損害貨幣主權，所以廣泛使用加密資產會削弱中央銀行在危機時採取支援銀行體系措施的有效性，例如導入資金與外匯管

制等措施。

肆、關聯性與傳播途徑

去中心化金融漏洞對於金融穩定之影響程度取決於去中心化金融、傳統金融與實體經濟相互之關聯性及關聯傳播途徑。基於去中心化金融具有自我參照之特質，現今去中心化金融生態圈所發生個別具有重要影響之衝擊事件，對於實體經濟僅有些許風險。雖然目前關聯性尚低，但其未來成長範圍及規模將成為決定去中心化金融穩定風險可能傳播幅度之重要因素。本段說明主要關聯性與傳播途徑，及去中心化金融可能進化情境。當去中心化金融與傳統金融相互聯繫愈多，金融穩定勢必會受不同方式及更廣之傳播途徑影響。前瞻觀點將有助估計潛在去中心化金融穩定風險，及評估適當之應對政策。

一、主要傳播途徑

加密資產影響金融穩定有四項可能傳播途徑。第一，金融機構對加密資產之暴險，包括加密資產相關金融商品及受加密資產影響財務之實體組織。第二，信賴效果。第三，加密資產市場價值波動造成之財富效應。第四，使用加密資產辦理支付及結算之範圍。去中心化金融相關漏洞會與前述傳播途徑互相影響，造成金融穩定問題。金融機構對去中心化金融暴險程度，於第一項傳播途徑尤為重要，因為去中心化金融一旦發生問題就會影響到傳統金融。另一方面，當一般家戶及法人愈深入參與去中心化金融，信賴效果與市場價值就愈為攸關。最後，去中心化金融貨幣，特別是穩定幣，變成廣泛使用之支付工具時，其系統重要性自然大幅增加。

二、關聯性與外溢範圍

去中心化金融引發之壓力會透過前述傳播途徑外溢至傳統金融及實體經濟。

(一)金融機構對去中心化金融暴險：以系統性觀點來看，渠與核心金融部門之關聯性高低至關重要。由於 BCBS 之巴塞爾資本協定尚持保守審慎態度，目前銀行對加密資產及去中心化金融之暴險極少，惟部分金融機構已直接

投資加密資產相關企業，包括提供使用去中心化金融應用程式或服務之企業，然該機構自身暴險並未揭露該等企業之資本潛在損失。銀行對去中心化金融之暴險除直接投資外，亦可能透過各種直接及間接途徑產生暴險，包括：

1. 提供貸款給去中心化金融業者：包括直接借貸給去中心化金融參與實體，例如去中心化應用程式或加密資產管理平台。銀行暴險亦包括借貸給有投資或參與去中心化金融活動之個人、私人財顧、企業或其他金融機構（包括避險基金）。此類暴險可能是以加密資產或實體經濟資產作為擔保。
2. 提供造市及清算服務：銀行可能代表客戶參與加密資產或衍生商品之交易及清算。
3. 協助去中心化金融生態圈活動：銀行可能在去中心化金融生態圈中扮演直接積極角色，包括擔任代幣化資產（例如代幣化存款或結算貨幣）發行者、驗證者、提供錢包服務、穩定幣準備金之保管人、對去中心化金融加密資產持有人提供保管服務，或將現實資產代幣化。銀行直接或間接參與去中心化金融，可能提升額外之作業風險，包括詐騙與網路風險、法遵與商譽風險、洗錢防制與打擊資恐（AML/CFT）及制裁遵循風險。
4. 去中心化金融借貸給銀行：銀行業者接受穩定幣發行者提供之資金已有前例，如果去中心化金融之規模持續成長，類此融資行為亦會隨之增加。

實體資產代幣化將顯著增加其關聯性。銀行運用去中心化金融協議將傳統資產及存款代幣化，使去中心化金融市場可供抵押之資產增加，並可能支撐其成長。這種行為亦代表去中心化金融能參與實體經濟融資活動。當此種關聯性增加，去中心化金融發生問題並波及實體經濟之風險將大幅提昇。如果傳統金融體系中具系統重要性之金融機構開始參與從事前述相關活動時，彼此關聯性更會提高集中風險（橫跨去中心化金融與傳統金融）與風險蔓延可能性，並提昇特定去中心化金融協議之重要性。

機構投資人，特別是受法令限制較少者（例如私人財顧及避險基金），同樣是參與傳統金融及去中心化金融之最大群體。機構投資人仍持續關注

加密資產及去中心化金融並計畫直接投資加密資產，將使去中心化金融資產規模擴增。隨著廣大機構投資人對去中心化金融愈感興趣，去中心化金融平台將可能迎合其偏好提供更多產品。例如開發使用特許網路之去中心化金融協議，以符合遵循防制洗錢與認識客戶（AML/KYC）相關規範。此類產品發展將促進愈多機構資產經理人參與去中心化金融活動。當投資人可由一個金融系統籌資並投資於另一個系統，使得彼此關聯增加，進而會提高風險蔓延之可能性。

(二)家戶與企業：如果散戶參與去中心化金融之規模成長，一般家戶對加密資產暴險亦隨之增加，並可能會透過財富及信賴效果造成更為廣泛之影響。當面對巨大損失，散戶投資人會縮減支出或減少對其他行業之投資。一旦對去中心化金融平台失去信心，亦會引起投資人加速贖回或出售其他資產，並可能擴大牽連範圍。目前一般家戶參與去中心化金融之規模極小，所以彼此關聯性迄今仍極為有限。對於擴大散戶參與去中心化金融之現有阻礙，包括其複雜度、交易成本，以及對加密資產生態圈現行活動之需求。然而這些阻礙會隨著時間經過而逐漸減少，對加密資產之關注則會持續成長，並且集中化交易或借貸平台將使去中心化金融協議更易於接觸使用。非金融相關之企業使用去中心化金融主要集中於貿易融資及信用保證發票。如果非金融相關行業增加使用去中心化金融，利用其進行投資或募資，一旦去中心化金融發生問題，將令該等行業產生損失並減少投資，過度槓桿操作更會使得相關衝擊擴大。

(三)去中心化金融與支付：去中心化金融對於支付與結算之應用範圍仍處於早期階段。部分現行穩定幣是由去中心化自治組織（DAOs）管理，例如 DAI 及 FRAX 二種穩定幣。當該等穩定幣可執行一系列功能，包括在加密資產生態圈作為法幣之替代品，其追求目標係成為跨界支付工具。如果它們更進一步發展，散戶及法人使用者將其用於去中心化金融履行義務工具之規模增加，並且促使其成為加密資產世界之支付工具，可能使其成為金融漏洞之額外來源。

三、 去中心化金融發展情境與金融穩定

去中心化金融之金融穩定議題最終取決於該行業發展情形。有三種可能情境供此項議題之政策制訂者參考。相關情境之實現，以及去中心化金融相關風險影響金融穩定之程度，部分取決於對該行業之監管力度。

情境一：去中心化金融保持利基領域

在此情境，去中心化金融行業於加密資產生態圈中雖可維持其利基，但其成長失去動能，與傳統金融僅保持有限關聯。此情境係若干因素導致，第一項因素係該行業自身具有專業性質，且需要專業技術參與，多數人群都無需該項相關服務。第二項因素，對加密資產行業加強規範與監理，及去中心化金融相關漏洞問題，都會阻止金融機構參與去中心化金融。第三項因素，相較於現有市場，去中心化金融行業之新興金融服務應用若無法提供實質利益，其吸引力終將消失。第四項因素，當處於通膨環境且利率提高，先前受收益率吸引之投資人將離開去中心化金融平台，流動性因此降低，原先促使加密資產市場成長之市場力量則將明顯減弱。對於此一情境，去中心化金融行業相對規模較小且關聯性有限，將不致引發金融穩定問題。

情境二：去中心化金融成長並成為部分主流

在此情境，由於加密資產受廣泛採用，現實世界亦開發應用去中心化金融，使去中心化金融生態圈成長顯著，且逐漸成為主流。對應此發展環境，對於加密資產與去中心化金融市場之相關監管亦將同等提高關注程度。推動其成長來源有二，第一，隨著加密資產生態圈持續擴大成長，去中心化金融行業亦隨之成長；第二，現實世界發展創新應用案例（use cases），促進更多人參與。例如將傳統資產代幣化以供作金融交易抵押品，使去中心化金融可提供金融中介服務，並參與廣大經濟活動。對於加密資產市場之監理與法規發展，則會重大影響前述二項成長來源。基於先前市場案例，中心化交易平台及包括穩定幣在內之加密資產所受監管已有提高，中心化參與者於遵守監管期待之同時，需保證其去中心化金融交易對手亦達成相關法遵，此情境可能加速去中心化金融與中心化實體整合，

可能代價則是其業務與管理之去中心化程度降低。

在此情境，去中心化金融於受規範市場中之業務規模成長且具高度連結，致使去中心化金融與實體經濟之關聯性加深。透過前述傳播途徑，外溢範圍擴大，對金融穩定可能影響將提高，因而需要更多相對應之政策規範。

情境三：去中心化金融緩慢消逝，相關創新則會存續

鑒於 2022 年 5、6 月間三箭資本破產並引發市場動盪事件，去中心化金融行業尚有許多漏洞，使該行業之吸引力終將衰退。然而，有助於強化傳統金融功能之相關金融創新則會保留。相關創新係透過程式化、智能合約及可組合功能等特性，提供結合交易及執行交易組合自動結算等功能。該等創新有助提昇傳統金融之功能與速度，並降低金融中介成本。

伍、監控去中心化金融之演變

監控去中心化金融存在數據挑戰，要克服挑戰可藉由多項指標以監控其演變與漏洞改善，該等初步及概念性指標，有助將去中心化金融發展納入對加密資產生態圈之金融穩定監控。

一、現有數據問題

加密資產市場與去中心化金融之數據通常缺乏透明度和一致性，與傳統金融系統關聯性之數據也有同樣問題。數據問題主要源於加密資產與相關區塊鏈之性質，以及市場參與者之動機，特別是：

(一)分散式帳本上大量可用的數據常難以匯總及分析，從公共區塊鏈獲得之數據，因在某些方面可能是透明且不可變動，故通常難以蒐集與分析。

(二)公共分散式帳本的資訊具有匿名性質，導致難以瞭解加密資產生態圈的投資者類型，且還有一系列強化隱私的技術，例如錢包混幣器（wallet mixers/ tumblers/anonymity[註 15]）等，可協助用戶隱藏交易的透明度。

(三)大量的區塊鏈下交易，例如發生在公共分散式帳本之外的交易及其他鏈下的數據，導致區塊鏈上的數據可能無法完整反映市場的整體活動。

(四)缺乏一致性和可靠性數據的報告，因為部分加密資產生態圈不屬於或不符合目前的監管範圍，意即加密資產市場參與者通常不遵守傳統金融實體記錄保存與報告揭露規範，進而影響數據的品質與可比較性。

(五)有些數據提供者，尤其是加密資產交易與借貸平台，可能會受誘因影響而去操縱數據（例如虛假（洗）交易（wash trading）等做法），藉此使其平台獲得關注，並吸引更多的交易量或投資者。

市場數據提供商（例如區塊鏈分析公司）已開始嘗試克服這些缺點，但其大部分數據來源仍然面臨上述問題，建議公部門需就私人數據蒐集的缺陷問題採取對應作法，以提高市場透明度及強化風險監控。

二、 去中心化金融監控要素

去中心化金融監控第一個重要部分是可協助衡量去中心化金融整體規模與演變的指標，第二個關鍵部分是特別設計用於衡量去中心化金融漏洞的指標，第三組指標則用於追蹤及評估去中心化金融、中心化金融、傳統金融與實體經濟的關聯性，以衡量外溢範圍。

重點在於監控應隨著加密資產與去中心化金融市場的發展而靈活調整，此外，鑒於缺乏去中心化金融全面且可靠的量化數據，監控方法應結合市場資訊的質性分析與見解。

另一重要監控面向則是選擇數據更新的頻率，部分監控可定期進行，並依據量化數據集中關注去中心化金融市場狀況，其他更針對性的監控則可以以較低的頻率和更深入的方式進行，對特定事件或市場結構變化（例如去中心化金融特定行業產生的漏洞）進行取證分析。

三、 追蹤去中心化金融市場演變

目前至少有四個關鍵指標可用於監控去中心化金融生態圈的演變。第一個指標是總鎖倉價值（TVL），用於衡量鎖定在智能合約的總價值（以美元表示），並反映各區塊鏈與活動類型的市場參與規模。第二個指標是去中心化應用程式的數量，用於代表去中心化金融項目的數量。第三個指標是穩定幣市值，可顯示個

別穩定幣對去中心化金融的重要性（特別是原生於去中心化金融協議的穩定幣）。第四個指標是依據底層區塊鏈唯一地址計算的去中心化應用程式用戶數量，可表示去中心化金融市場參與的成長程度。

雖然這些指標看似簡單，但在解釋使用上卻具有相當複雜性，例如，總鎖倉價值會因重複計算問題造成估計差異；智能合約創建的新代幣可能會與承諾掛勾的原生代幣一起計算；總鎖倉價值計算不一定會包括用來提案、投票表決的治理代幣；穩定幣常用於非去中心化金融的目的，致使其市值成長可能會造成高估去中心化金融的成長。

此外，去中心化應用程式的數量可能取決於市場結構，當某一市場僅有少數主導者，其去中心化應用程式數量可能也會較少。唯一接收及發送加密貨幣地址（unique address）的數量可能取決於協議設計，例如可能激勵用戶創建多個唯一地址以獲取治理代幣空投優勢（註 16）。因此，監控框架實施時，需要開發相關衡量措施以應對上述諸多複雜性。

四、 追蹤漏洞

對於去中心化金融的五種核心漏洞：1. 營運脆弱性，2. 流動性與期限錯配，3. 槓桿作用，4. 相互關聯、集中度及複雜性，5. 其他漏洞，其監控方法探討如下。

量化去中心化金融協議的營運脆弱性，方法之一是測量每個特定脆弱性來源的相對規模大小，例如衡量個別去中心化金融協議、預言機與區塊鏈相對於去中心化金融生態圈的規模（以總鎖倉價值衡量）數據。

有關治理代幣所有權集中度的資訊可通過數據提供商和協議網站獲得，衡量治理相關風險的另一個重要方法是參考使提案通過所需的投票率，投票率可顯示治理代幣持有集中度對於變更協議特定功能的重要性。

對於嘗試瞭解第三方服務提供商中斷或失敗所造成潛在影響衡量方法更加複雜，個別第三方服務提供商可能提供服務予許多去中心化金融協議，且這些提供商在廣泛的加密資產生態圈中執行多種功能，但似乎沒有數據提供業者匯集這些第三方提供商相關資訊，不利瞭解去中心化金融行業的集中度概況。

關於流動性與期限錯配問題，穩定幣是重要關注對象，藉由瞭解不同類型穩

定幣的整體規模、發行者差異、穩定幣的用途與投資者，以及參照儲備資產的品質，可以評估及監控穩定幣對於加密資產生態圈（包括去中心化金融）及其投資的傳統金融資產市場所構成的風險。

去中心化金融與加密資產市場的槓桿總額不易衡量，但有數項指標資訊可供瞭解，例如抵押品數額與系統內資產再抵押程度，依照經濟合作與發展組織（OECD）引用的 Chainalysis 數據顯示，許多流入去中心化應用程式的資金來自去中心化金融本身，只有一小部分資金流入來自法幣轉換為加密貨幣資產，可能代表去中心化金融參與者高度使用槓桿，通過借出或投資最初收為抵押的資產來創造抵押鏈。

去中心化金融的各個組成部分（例如區塊鏈、協議、預言機、跨鏈橋及穩定幣）之間的關聯性與集中度各具不同形式，因此需要使用各種指標進行監控。

單一協議的安全性與穩健性並不能單獨分析，還必須考慮其他協議的影響，可藉由查看最大型去中心化應用程式的總鎖倉價值與底層區塊鏈的集中活動，以監控此類關聯性。

至於其他漏洞，有數項關於市場誠信問題的指標可以採用，總礦工可提取價值（MEV）代表有內線人士的抽租行為（rent extraction），可衡量對其他投資人利益損害情形。

為監控類似龐氏騙局的動態，可以使用去中心化應用程式產生的現金流量與市值的比較評估，以及比較去中心化金融協議相對於其他替代投資提供的年收益率。

五、 追蹤關聯性與傳播途徑

去中心化金融漏洞是否導致金融穩定問題，取決於與傳統金融和實體經濟的互動程度，對這些交互影響的監控十分複雜，因為它需要來自去中心化金融生態圈和其他來源的資訊。

至於金融風險部分，有幾個領域需要監控，其中包括銀行採行適用加密資產市場商業模式的成長情形，及機構投資者對去中心化金融的參與情形。其他可能有用指標包括家戶與法人暴險，但目前可用於衡量這些聯繫的數據很少。

陸、結論

雖然去中心化金融宣稱提供金融服務的去中心化過程在許多情況下都是新穎的，但在執行功能上與傳統金融體系沒有實質上的區別，此外，實際上去中心化金融的組織結構中，去中心化程度差異也很大，往往與其組織結構宣稱的說法有很大偏差。在試圖複製傳統金融系統的某些功能時，去中心化金融沿襲且常會放大該系統的漏洞，放大效應來自其新穎的技術特點，且參與者之間具有高度結構關聯性，以及缺乏監管或不遵守現行監管規範。最終，去中心化金融所產生的漏洞對金融穩定構成的風險程度，多取決於去中心化金融與傳統金融之間的關聯性及其相關的外溢途徑。

有一種可能情境，去中心化金融將在未來繼續成長，並與實體經濟和整個金融系統更緊密地互相連結，因此，隨著生態圈的發展和演變，必須就去中心化金融的相關漏洞及對金融穩定的潛在威脅謹慎監控。目前，由於可用數據不足及品質不佳，缺乏或不遵守報告要求，以及市場行為傾向不透明方式運作，使得漏洞監控受到一定阻礙，並使蒐集分析正確數據具有相當難度。

鑑於這些發現，有些建議值得考慮。首先，FSB 應主動分析去中心化金融生態圈的金融漏洞，並將其納入對整個加密資產市場的定期監控。FSB 加密資產監控框架應該納入去中心化金融特定的漏洞指標，並且 FSB 應探索實體資產代幣化的成長情形，它可能會使加密資產市場和去中心化金融與整個金融系統和實體經濟之間的關聯性提高。

其次，對去中心化金融漏洞是否會影響金融系統的有效分析取決於去中心化金融（包括加密資產生態圈）與傳統金融（包括銀行和其他類型金融機構）以及實體經濟相互關聯的數據可用性，FSB 與標準制定機構（standard-setting bodies, SSBs）和監理機關共同合作，探索衡量及監控此類相互關聯的方法，同時可以考慮共享現有數據與市場情報，及使用特定的資訊蒐集方法（例如調查）。

第三，由於去中心化金融的應用案例與監管方法仍在發展中，FSB 將研究國際監管建議的政策，考慮去中心化金融特定風險及加密資產活動可能需要加強監管的程度，並促進法規執行。去中心化金融特定風險包括使用智能合約進行交易，可能導致自動清算；不透明的治理安排（包括代幣集中所有權[註 17]的可能性）；

依賴區塊鏈網路；以及使用易受市場操縱及網路竊盜的預言機與跨鏈橋。故 FSB 與 SSBs 合作，還需考慮對去中心化金融與整體金融體系和實體經濟相互關聯所帶來的風險採取可能的應對政策，包括制訂監管規範，監管傳統金融機構對去中心化金融的直接暴險，及可能尋求加強整合去中心化金融的其他方式（例如擔任受託人或保管人，或與其他從事去中心化金融的企業進行交易）。此外，如果去中心化金融持續成長且獨立於傳統金融之外，可考慮是否處理去中心化金融本身及與加密資產生態圈相互關聯的漏洞。

FSB 可考慮與 SSBs 協調評估跨轄區的監理範圍，以確定哪些去中心化金融活動和實體應納入監理範圍（強制遵守適用法規）或排除在外（應制定政策適當規範具有類似風險之活動）。需要考慮的關鍵因素是對去中心化金融用戶（包括散戶投資者與傳統金融機構）的切入點，例如透過穩定幣及中心化加密資產平台。FSB 可考慮讓這些加密資產類型及實體遵守額外的審慎及投資者保護規範，或加強現有規範的執行，以降低緊密關聯的風險。

如果去中心化金融活動及實體被認為屬於受監理範圍，應強制遵守相關適用的監管法規。FSB 會員應共同致力瞭解執法與監理面臨的挑戰。對於排除在監理範圍以外的去中心化金融活動及實體，制定合適政策以適當規範具有類似風險之活動將是一種挑戰。SSBs 可協助週邊範圍評估，加強跨境合作及資訊共享；FSB 可就跨部門及跨境議題進行分析與建議，包括促進有關加密資產的監管與規範議題，以達成有效合作。

註釋

註 1： permissionless blockchains 非許可制區塊鏈，或公共區塊鏈，指公開且任何人無需獲得授權都可以參與區塊鏈，所有參與者具有相等的權利，包含創造新的區塊、驗證交易等。

註 2： Stablecoin 穩定幣，是加密貨幣的其中一種類型。由於依靠演算法或權益證明等產生的虛擬貨幣容易受到波動，同時缺乏價值儲存的功能使之無法替代中心化貨幣，因此加密貨幣只被視為投機資產。穩定幣的核心想法是要打造一種底層分散式帳本，但維持貨幣穩定價值的機制。穩定幣被有些人認為是中心化資產抵押發行的代幣，穩定幣價值是與被抵押資產價值直接連動。（資料來源：維基百科）

註 3： 運行程式所支付成本的單位，代表一個交易消耗的計算資源，當用戶請求一筆交易時需支付 gas 費用給礦工，以驗證此交易的合法性。

註 4： Oracles 預言機，指區塊鏈和現實世界之間的橋樑，是一個服務或機制用來將現實世界的數據或事件載入區塊鏈中，來源如傳感器、公開資訊、企業資料庫或其他區塊鏈。

註 5： cross-chain bridges 跨鏈橋，指連接兩個區塊鏈生態系統之工具，通過訊息和資產轉移促進不同區塊鏈之間的溝通。

註 6： governance tokens 治理代幣，作為激勵誘因發行的代幣，使用戶有機會得到去中心化金融協議的部分所有權及決策權。

註 7： rug pull 是加密資產市場的詐騙行為之一，去中心化金融項目開發團隊在吸引投資人之後，將投資資金捲款潛逃，僅餘留不具價值之資產予投資人。

註 8： cold/offline wallets 冷錢包，或稱離線（斷網）錢包，與熱錢包（線上錢包）相對應，區塊鏈錢包種類之一，意指網路不能存取到使用者私鑰的錢包。冷錢包通常依靠「冷」裝置（未聯網的電腦、手機等）確保加密貨幣私鑰的安全，運用二維條碼通信讓私鑰不觸網，避免被駭客盜取私鑰的風險，但是也可能面臨物理安全風險（比如電腦遺失，損壞等）。

註 9： TerraUSD 是由 Terra 發行的一種演算法穩定幣，簡稱 UST；Terra 為一區塊鏈協定，主要發行演算法穩定幣，透過 Terra 所發行的穩定幣與其它由法幣支撐的穩定幣不同，而是透過其姐妹幣 Luna 來維持與美元的錨定。Luna 為一用來吸收 Terra 短期波動的資產，任何人在任何時候都能用價值 1 美元的 Luna 幣來兌換一個 UST，當 UST 大於 1 美元時，使用者就能以價值 1 美元的 Luna 來兌換 UST，若是 UST 小於 1 美元，那麼使用者就會以 1 個 UST 來兌換價值 1 美元的 Luna 幣。而只要鑄造一個 UST，就要銷毀價值 1 美元的 Luna 幣，若是銷毀一個 UST，則必須鑄造價值 1 美元的 Luna 幣，總之，Luna 幣是用來平衡 UST 的價格，維持 UST 與美元之間的錨定。

註 10： Anchor 是由 Terra 協議發行穩定幣的交易及借貸平台。

註 11： Lido 是流動性質押平台，為以太坊（Ethereum）和其他共識機制區塊鏈的質押者提供資金流動性。質押者可以在 Lido 質押並獲得質押憑證，例如質押以太幣 ETH，可以 1:1 獲得 stETH 憑證，並使用 stETH 在其他平台上進行交易，最終可將 stETH 兌換回 ETH。

註 12：高度槓桿借貸的加密資產在市場價格下跌時，因無法償還貸款導致抵押品自動被清算，而又觸發另一波賣壓，導致資產價格進一步下跌。

註 13：total value locked, TVL 總鎖倉價值，代表去中心化金融協議（平台）的流動性資產總量，常被用來衡量在資金池裡鎖定的代幣資產總量的指標，通常以美元為單位。有些投資者會透過此指標來快速判斷去中心化金融項目的市場整體狀況與市佔率。本篇報告伍、三另有簡介。

註 14：本篇報告貳、三、（二）所述有關 AMM 交易平台模式，透過套利交易處理流動性池價格不均問題，但在此過程中用戶需提出交易增加至區塊鏈，使驗證者有機會利用自身權力搶先交易順序而獲取較高交易利潤。

註 15：透過將可能被識別的加密貨幣資金與其他貨幣混合以掩飾資金的流向，令人難以追溯資金的源頭。混幣器旨於提高加密貨幣的匿名性，因為加密貨幣提供任何人都可查閱所有交易的公共帳本。（資料來源：維基百科）

註 16：加密貨幣空投是指將數位資產從加密貨幣專案轉帳至多個錢包。原意是向目前或潛在用戶分發代幣，以提高對該專案的認識。這些代幣免費發放，有些空投則要求用戶在領取之前完成特定任務。

註 17：concentrated ownership，某些加密貨幣或代幣的控制權集中在少數人手中，因持有大量的加密貨幣或代幣佔整個市場的大部分，其交易與決策可影響價格、市場及協議。