探討去中心化金融在銀行業之發展趨勢 - 上

何思賢

第一章 前言

第一節 研究背景

2008年中本聰在《比特幣白皮書》中提出加密貨幣的概念，為全世界開啟去中心化的發展序幕。至今跟隨比特幣興起的加密貨幣與金融科技產業，仍不斷在尋找新的應用場景與商機，像是早期的去中心化運算平台[1]與去中心化應用程式[2]，以及近年興起的NFT[3]與去中心化金融（Decentralized Finance, 以下簡稱DeFi），這些新興名詞的出現正為傳統銀行業開闢一條全新的道路。

過去幾個世紀，傳統銀行系統（中心化金融）一直占據主導地位，但隨著科技的進步，傳統銀行業出現第一次的變革，即數位銀行、純網銀陸續出現，不僅有傳統銀行業者積極搶攻，科技業、新創公司也如雨後春筍般的冒出，透過科技將部分的實體交易搬移至網路世界之中，以提供人們在網路世代下所需要的金融服務。然而自2020年Coivd-19席捲全球以來，人們的生活習慣正迅速由線下實體活動轉往線上移動，並驅動全球加速數位化轉型。

2021年元宇宙[4]（Metaverse）的概念在疫情與科技的催化下橫空出世，由於構成元宇宙的一大特性便是去中心化，且元宇宙世界如同實體世界一樣會衍生出支付、借貸、投資和保險等金融服務，為了讓數位資產能夠進行移轉，DeFi將成為虛擬世界中重要的底層建構。當元宇宙的構想逐步成真，現有的許多金融服務將由中心化走向去中心化，傳統銀行亦將再次迎來新的變革與挑戰。雖然目前尚無法斷定元宇宙多久能夠達到成熟階段，但全球已有部分大型銀行業者投入此領域的投資與研究，期望能將危機化為轉機。國泰金控董事長蔡宏圖2022年初曾表示，科技顛覆了許多傳統產業，贏家跟輸家重新洗牌；許多科技業者搶進提供金融服務，現在甚至還有加密貨幣、區塊鏈帶來全新的「去中心化金融」，對身為金融業的我們會有什麼影響？值得我們關心。

第二節 研究目的

由於DeFi是將金融產品建立在公共的金融服務區塊鏈平台上，並透過智能合約的運行，讓任何人都可以使用平台上的金融服務，相較傳統中心化金融，它完全不受任何中心機構監管，若未來能有完善的消費者保護機制作為基礎，DeFi將有望實踐普惠金融，並拓展一個真正開放且觸及率更高的金融新疆界，不論對消費者的消費行為、商家的商業模式，甚至是銀行業的營運模式，都將有深遠的影響。

DeFi雖為銀行業的帶來發展契機，但仍須建立在主管機關開放與核准的前提下。有加密貨幣業者坦言，目前虛擬貨幣與DeFi此等領域相關法律定位仍不明確，當加密貨幣業者有意探詢和銀行合作的可能性，銀行皆有諸多顧慮。我國中央銀行亦於2022年第二季度報告強調DeFi將會滋生諸多風險，包括資訊不對稱與詐欺風險、市場誠信風險、非法活動風險、營運與技術風險、治理風險和風險外溢到傳統金融市場，顯示國內當前對於DeFi仍抱持謹慎的態度。惟不可否認的是，隨著DeFi應用的範圍日益擴大，加上元宇宙的熱度竄升，各主管機關均已不可忽視DeFi所帶來的潛在商機以及風險。

實際上，區塊鏈與DeFi兩者緊密相連卻又不盡相同，雖然目前有眾多關於區塊鏈應用在銀行業的研究，但DeFi是近兩年才興起的名詞，國內鮮少有針對DeFi的完整研究或是銀行業應用DeFi的相關文獻，又因此項技術被認為是元宇宙重要的底層建構，且可能對現有金融仲介的角色帶來衝擊。有鑑於此，本研究欲透過了解DeFi的概念與發展趨勢，掌握目前國際上該技術的應用場景，進而分析DeFi對銀行業可能的衝擊，同時探討國際監理機構與我國央行對DeFi的監管態度，希望由此歸納出銀行業者該如何因勢利導，攫取獲利新契機，預應轉型挑戰。

第二章 去中心化金融之概念

從比特幣算起，區塊鏈發展已逾十年，除了比特幣的石破天驚之外，區塊鏈真正的轉捩點是2013年智能合約[5]（Smart Contract）的誕生。智能合約為人們的生活帶來無限的想像，而目前市場最為關注近兩年市值規模快速成長的兩個領域，分別是金融和遊戲領域；遊戲方面主要是以NFT為主，金融方面則是以 DeFi為主，本章節將淺談DeFi的基本概念與架構，並進一步分析DeFi與中心化金融之差異，一窺DeFi的真實樣貌。

第一節 去中心化金融之定義與起源

一、去中心化金融定義

去中心化金融（Decentralized Finance，簡稱DeFi），泛指基於區塊鏈且與數位資產有關的交易、支付、借貸及保險等金融應用。在這套系統上的買方、賣方、甚至貸方及借款人，都能進行點對點、透過去中心化的智能合約，進行不受中心監管的金融活動，自由享受金融服務，並實現普惠金融的願景。

DeFi概念興起於Bitshares[6]的嘗試，而正式定義DeFi這一詞的是，2018年借貸產品Dharma的聯合創始人Brendan Forster發表的《Announcing De.Fi，A Community for DecentralizedFinance Platforms》，在一文中正式定義DeFi應具備的要素，包含建立在去中心化區塊鏈上的金融項目、具有開源的程式碼[7]、健

全的開發者平台。與其說DeFi是被建置於區塊鏈和加密貨幣領域的金融服務，其實DeFi更像是一種追求除去金融交易雙方的中介，使得這套系統內的所有權分散、不易被竄改，且具有透明性、抗審查等特性的金融服務系統。因此，嚴格來說，DeFi並不等於區塊鏈或是加密貨幣，這兩項技術只是目前較容易達到DeFi的技術方法，本研究亦會在後續章節詳述DeFi的底層技術。

二、去中心化金融起源

DeFi與加密數位通貨及區塊鏈技術的演進密不可分，加密歷史上第一個重要的突破是比特幣，2008年中本聰（Satoshi Nakamoto）通過對密碼學、共識機制、點對點網絡、激勵機制等恰如其分的運用，完成了無須第三方參與的價值轉移，此階段也被稱為「區塊鏈1.0」。而DeFi的出現則被視為第二個突破，即「區塊鏈2.0」，為什麼DeFi會是加密史上的第二個突破？主要係因它能夠滿足部分群體的金融需求，而這些金融需求正是幾百年以來傳統金融所無法滿足的部分。

圖 1：區塊鏈發展脈絡

資料來源：Mr. Market市場先生

我們進一步從金融的核心價值－貨幣切入探討，社會一開始的通貨方式是物物交換，但物物交換最大的問題是效率低落，因為要找到兩個剛好都有物品匹配需求的對象很難，即使需求匹配，如何計價又是一個問題。因此，進而衍生出貨幣的需求，人們需要一個通貨作為物品間的交換媒介，並且具備儲存價值的功能。人類歷史上有過貝殼、貴金屬、金銀等通貨，發展至今就是由中央機構發行的法幣。而傳統金融通過中介機構的整合和運作，提高了市場的效率，實現了更好的資源配置。但同時，也因為中介機構的存在，傳統金融體系逐漸產生下列問題：

（一）集中式掌控：以傳統金融等金融機構來說，主要都是透過客戶的存款作為市場資金供給及需求方的中介人，進而收取利息等報酬，而這些中心化的交易過程往往不得而知，看似穩定的系統卻可能長時間累積弊端，最終出現全面性的爆發（如2008年的金融海嘯，便是由銀行發行的次級房貸所引發）。

（二）有限獲取：即便科技如此進步，時至今日，世界上仍有五分之一的人口是銀行的絕緣體，即便有與銀行往來，可能仍因自身條件未達銀行貸放門檻而無法取得貸款或是信用卡。

（三）效率低落：中心化金融最常見的問題就是效率不彰，像是股票交割的時間、以及海內外資金轉移的時間，或是保險審核的時間，透過中心化的處理以及人力的介入，往往會增加作業時間及成本，因此目前各種金融服務效率仍有待改善的空間。

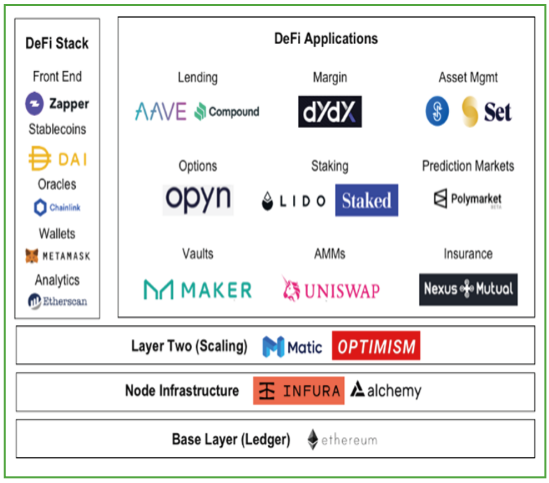
（四）資訊不透明：既往金融交易資訊不透明，導致監管當局和金融機構管理層難以及時跟蹤並準確評估風險暴露程度，進而也較難通過早期糾正機制來防範和化解。此外，當前銀行的貸款利率或是保險公司的保費資訊不透明，也導致客戶可能無法就自身條件確切獲得市場上最合適的服務與費用。

然而近幾年來，另一套截然不同的通貨模式取得可觀的進展，即去中心化金融，在這套架構中，借助區塊鏈技術透明化、分散式的特性，使得DeFi有機會改變傳統金融體系的結構性問題。

第二節 去中心化金融基礎架構

如同前一小節所述，DeFi是透過區塊鏈技術所打造全新的金融體系，然而DeFi整個生態系統包含各種不同的機制、協議、平台，藉由這些元素相互組成，將能創造更多新的產品及服務提供給用戶使用，故本節將進一步探究DeFi的底層架構，以利我們瞭解DeFi整個生態系。目前DeFi生態系統主要是建立在Solana與以太坊底層架構之上，本研究將以圖2以太坊的生態系統來依序探討各區塊所代表的涵義。

圖 2：以太坊DeFi生態系統架構



資料來源：VC Race Capital

一、基礎層：區塊鏈技術與智能合約

以太坊（Ethereum）是一個開源的有智能合約功能的公有區塊鏈平台，通過其專用加密貨幣以太幣（Ether）提供去中心化的以太虛擬機（Ethereum Virtual Machine, EVM）來處理點對點合約，是2013年由維塔利克．布特林（Vitalik Buterin）所構想出新的底層區塊鏈技術，並於2015年正式上線。

以太坊在某種意義上，可以說是依循比特幣應用邏輯來擴展，但不同之處在於，在同樣區塊鏈的基礎之上，以太坊讓區塊鏈不僅僅是紀錄帳目，透過EVM它可以記錄及執行程式指令碼，人們可以組合這些指令碼，把它紀錄在區塊鏈上，當條件符合即可執行這些程式，而這些程式即為智能合約。因為具備智能合約的功能，目前以太坊也可以被定義為「智能合約平台」的角色。智能合約平台藉由區塊鏈的特性，讓傳統的程式碼變的具有極難被竄改的特性，因此它同時兼具信任安全機制以及DeFi應用的基礎。

二、第二層：擴展解決方案

由於目前在以太坊已經擁擠到需要支付相當高額的燃料費[8]（Gas Fee）並且要等待一段時間後才能完成任何交易及操作，因此越來越多的區塊鏈技術團隊希望能夠取代以太坊成為區塊鏈應用、DeFi項目的首選，而目前較具有前途的擴展解決方案包括Polygon（前身為Matic）與Optimism等。Polygon是作為以太坊的擴容方案所研發的鏈，目的是解決以太坊緩慢又高成本的缺點，拓展並加速以太坊的成長。

三、DeFi工具集

對於開發商或用戶而言，有一套運行大多數DeFi應用程序所需的通用工具，而這些工具能夠讓DeFi的金融服務更加完整，其中主要包括：

（一）錢包（Wallets）：DeFi錢包是用來存儲資產和與DeFi應用對接的主要介面，這些錢包的資金、私鑰是由用戶自己保管，即便是錢包的開發者也無權訪問用戶的錢包，而DeFi錢包通常與以太鏈上的規格兼容，支援相當多的加密貨幣，不同的DeFi錢包性質主要差別在於介面設計、背後的團隊以及協議，例如MetaMask、Crypto.com等。

（二）穩定幣（Stablecoin）：在DeFi體系中，金流主要是透過加密貨幣來進行支付與交易，但許多加密貨幣的致命缺點就是波動性太大，對於想使用DeFi金融服務，卻又不願承受以太幣等波動性資產風險的用戶而言，將會降低用戶的使用意願。因此，一批被稱為穩定幣的加密貨幣應運而生，穩定幣維持價格的機制因安裝啟用的方式而異，目前三大主要機制分別為法定資產擔保、加密擔保。若要使DeFi金融服務能夠穩定的運作，不受加密貨幣價格大幅波動的風險所影響，穩定幣會是DeFi基礎建設重要的組成要素之一。

（三）預言機（Oracles）：由於區塊鏈本身是一個封閉的數據庫，也就是說區塊鏈的帳本與外界的數據互不相通，少了外界的數據，智能合約便無法在現實世界中使用，而區塊鏈創新的地方就在於，上鏈後的資訊不可逆，不會被竄改，可以保障資料的「安全性」，然而，當數據本身不是區塊鏈的原生數據，數據的「正確性」就會產生風險。因此，必須要有一種解決方案，向區塊鏈提供現實世界狀況的系統，不論是金融產品、保險、物流、預測市場或資產抵押等服務，若想要打造去中心化系統，可信任的預言機是相當重要的一環。

一座奠基於以太坊名為Chainlink平台，就是為了解決預言機的問題而設計的一套數據資料聚合體。Chainlink通過引入中介層解決方案來解決預言機問題。該解決方案創建了一個分散的Oracles網路，使用API連接到外部世界，各節點將智能合約用戶所需的答案提供給Chainlink的智能合約，Chainlink智能合約將數據聚集成一個答案，並在不干擾區塊鏈共識的情況下，回傳至用戶的智能合約。若以保險舉例，許多人會抱怨，理賠金遲遲領不到，或是明明不能理賠，客戶卻天天上門找保險公司，透過智能合約與可靠的數據源Chainlink，可以讓Chainlink節點整理醫院的就醫資料，並導入保險的智能合約，如果達到標準則立即付款，保險公司與客戶之間可以避免不必要的摩擦與不信任。

（四）前端（Front-End）/聚合器（Aggregator）：前端亦可稱作聚合器，其主要功能是用於提升DeFi的用戶體驗，聚合器著重在設計、易用性、本地化等方面進行優化，透過API的串接可以與多個DeFi項目互動，或簡化交易，如以太坊生態系統內的Zapper Finance，它為DeFi提供了一個簡單的儀表板，讓用戶可以在一個簡單的介面中輕鬆追蹤所有DeFi錢包的資產和負債。

四、去中心化金融應用程式（Decentralized Application, 簡稱DApp）

DApp就像是傳統的軟體應用程式，唯一不同之處就是它們建構在智能合約平台之上，DeFi可以透過DApp來運作各式各樣的金融服務。而這些應用程式的主要好處就是它們具有免許可與抗審查的特性，任何人都可以使用，因此沒有單一個體能夠掌控。DeFi實際上就是一個金融DApp的競技市場，藉由結合上述所提到的各種協議、工具及金融產品不斷重組，就能產出更多新型態的金融DApp，同時從傳統金融生態系統汲取越來越高的市場佔有率。目前市場上的主要金融DApp種類包含交易、支付、借貸、保險、衍生性商品、資產管理等，在後續章節會進一步討論各種類的金融應用。

第三節 中心化金融與去中心化金融之差異

通過前兩個小節對DeFi概念以及架構的論述，對DeFi有了初步的認識，本節將進一步分析DeFi與中心化金融（Centralized Finance, 以下簡稱CeFi）差異，將有助本研究釐清前面所提及的傳統金融缺點，以及DeFi是如何改善這些問題。

CeFi與DeFi是相對的概念，傳統金融機構如銀行、證券、保險等或是Coinbase、幣安Binance等加密貨幣交易所大多都是屬於CeFi。有別於DeFi是將金融產品建立在公共的金融服務區塊鏈平台上，並透過智能合約的運行，讓任何人都可以訪問平台上的金融架構，CeFi通常是在被監管的情況下，且用戶需執行實名認證（KYC）流程才能使用中心化的金融服務，DeFi及CeFi的主要差異如下表所示：

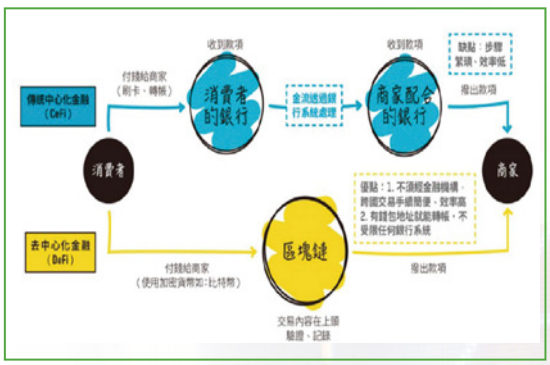
表 1：DeFi與CeFi主要差異彙整

項目	DeFi	CeFi
授權規則	開源系統且建立在不需被授權的區塊鏈上，任何人都能使用、參與這條區塊鏈上的金融活動，且不需要任何第三方授權同意	建立在有中央監管的封閉性系統，交易活動需要被第三方監管機關授權同意
資產保管	金融資產不被任何「單一」的第三方機構保管，而是區塊鏈上的所有分散式帳簿	金融資產被取得核可執照的第三方保管
使用者身分	使用者通常不需要提供任何關於真實身份的證明	使用者需要提供真實身份的證明，或簽署任何監管機關規定的文件（如 KYC/AML）
交易時間	無限制	有限制
轉帳速度	刷卡交易、自動轉帳：通常會在 24 ～ 48 小時完成清算 跨國電匯：24 ～ 48 小時	依區塊鏈網路的壅擠情況而定，大約在 15 分鐘～ 1 小時

資料來源：Mr. Market市場先生

舉例來說（圖3），在DeFi的金流體系下，消費者支付加密貨幣給商家的交易內容會通過區塊鏈的技術進行紀錄與驗證，驗證成功便直接轉帳至商家的錢包地址，整個過程無需任何中介第三方來承認、監督這次交易，且無資產保管情形，因此也不會被收取任何中介費用，或者費用有機會較傳統金融低。在這些金融節點中的使用者不需要政府監管的身份資格、更不用地址證明等文件，因此每個使用者都是平等的，且沒有任何一個人可以獨自竄改內容。

圖 3：DeFi與Cefi實際交易流程差異



資料來源：數位時代

藉由圖3的例子可以看到DeFi在沒有中介機構情境下所帶來的優點，在無需監管的情況下，省去複雜的KYC/AML流程，讓整個金融服務更有效率、更普及、更便宜。然而，DeFi目前因正處在快速發展的階段，當前全球對DeFi的發展趨勢仍未完全掌握，因此尚未有完整的法規的制定，進而導致出現詐騙、詐欺、洗錢等風險，用戶可能也因而無法獲得良好的保護；CeFi則因有政府與金融仲介機構的把關，讓客戶能夠獲得較為完善的保護；同時，當用戶遇到問題也能夠透過線上或是電話聯繫客戶排除問題，DeFi與CeFi的優缺點統整於表2：

表 2：DeFi與Cefi優缺點比較

	DeFi	CeFi
優點	更有效率 更開放、更普及的金融服務 免監管、抗審查 資訊公開透明 服務費用較低	發生問題有客服支援 相對 DeFi 用戶量多 法幣轉換較靈活 受監管，有各種措施保護用戶資產 信任度較高
缺點	黑天鵝事件 詐騙、詐欺、洗錢風險 程式碼錯誤及安全性漏洞 尚未有完整法規保護消費者	嚴格執行 KYC 效率較低 交易費用較高 容易被駭客攻擊 公司採取的安全措施失效，用戶資產會有風險

資料來源：本文整理

CeFi和DeFi兩者間概念相互對立，但卻是相輔相成的存在，畢竟金融服務是源自於傳統的金融系統。藉由CeFi易監管的特性，用戶更能夠信任企業以合法的方式管理自己的資金和提供服務，並發揮其資金量、用戶量大等優勢。而藉由DeFi用戶更能確保技術能在預期發展的服務上完成，免許可的特性將託管權交還予用戶。其中，兩者互補彼此的缺點，將能提供更廣泛的加密貨幣相關金融服務。目前市場上許多去中心化平台為了符合當地法規或是讓使用門檻降低，一些平台便會將CeFi與DeFi的特性結合，如幣安去中心化交易所與借貸平台BlockFi。

表 3：DeFi、CeFi與傳統金融服務供應者

服務	**加密資產金融系統**		CeFi **（傳統金融）**
	DeFi	CeFi（或結合 DeFi）	
貨幣	MAKER	tether	
借貸	Compound	BlockFi	ROCKET Mortgage by Quicken Loans
交易	UNISWAP	coinbase	Robinhood
數據	Chainlink	COINMETRICS	Bloomberg
資產管理	Yearn.Finance	GRAYSCALE	BlackRock.

資料來源：本文整理

第三章 DeFi國際發展趨勢與應用案例

自2013年智能合約的構想誕生以來，幾乎每隔一至兩年就可以提煉出一個加密貨幣的發展趨勢，2015年是以太坊的正式發行、2017年是首次代幣發行（ICO）大爆發、2019年是DeFi逐漸展露頭角的一年，2021年則是NFT從小眾躍向主流的一年。加密貨幣產業變化莫測，從2020年開始突飛猛進的DeFi，經歷了疫情、科技、法規以及人們生活型態的變革。因此，本章節將歸納DeFi在全球的發展趨勢與目前全球具代表性的應用案例，以利本研究掌握目前全球DeFi的發展概況，及DeFi應用案例與傳統金融之差異之處，將有助於本研究瞭解銀行業在各業務上可能面對的機會與挑戰。

第一節 DeFi國際發展趨勢

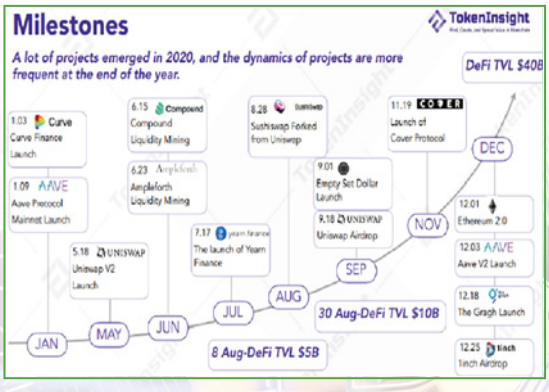
一、從概念興起到生態大爆發，DeFi實現高速發展

2014至2017 年發展初期，DeFi 概念開始興起並取得初步發展。2014年Daniel Larimer等人提出創建Bitshares的構想，旨在建立 “一個P2P加密貨幣交易所”，並付諸實現。然而設計和操作上的種種缺陷，導致Bitshares最終逐漸走向沒落，Bitshares的發展可以被視為一場實驗，同時也反映了市場，尤其是持有加密資產的投資者對更加便捷可靠的金融服務的迫切需要。2017年11月，MakerDAO推出，基於以太坊公鏈運行，並使用加密貨幣抵押且與美元掛鉤的穩定幣DAI，讓用戶能夠在不出售自身持有的以太幣（ETH）情況下，通過Maker平台抵押ETH，實現融資的目的。不同於此前只能滿足在兩點間傳送加密貨幣的功能，MakerDAO滿足了投資者利用加密貨幣進行融資的需求，使DeFi得到世界範圍內的廣泛關注。

2018年至2019年為成長期，DeFi項目於該階段快速湧現，2018年9 月Compound上線，主要功能是資產借貸；11月Uniswap去中心化交易所上線，建立了自動做市商（AMM）機制；2019年4月TokenSets上線，能夠提供自動資產管理。DeFi項目快速湧現，涉及金融中的借貸、交易等多方位功能，完善了整個DeFi生態。

2020年至2021年則是爆發成長期，2020年疫情使全球經濟陷入低迷，連帶影響DeFi市場信心不足，根據DeFi Llama平台數據統計，DeFi總鎖倉量（TVL）[9]由9.1億美元跌至5.73億美元，下挫 37%。但隨著全球經濟在各國政府緊急防治新冠疫情的大重啟（Great Reset）之後，以紓困為名推進的寬鬆貨幣政策與財政政策所造成的資本市場榮景，加上零接觸支付與加密貨幣等應用商機迅速崛起，催化眾多新的DeFi項目出現（圖4），如 Curve Finance、Uniswap V2、Cover Protocol等，為市場注入了新的生機。據Dune Analytics平台數據顯示，截至2019年12月31日，DeFi用戶量約為9萬人，2021年底用戶數達已達420萬人；總鎖倉量則從6.07億美元增長至2,345.89億美元，CAGR達1,865.9%，DeFi因而實現了爆發式的增長。

圖 4：2020年誕生之DeFi平台與協議



資料來源：TokenInsight

二、2022年DeFi世界來到反轉臨界點

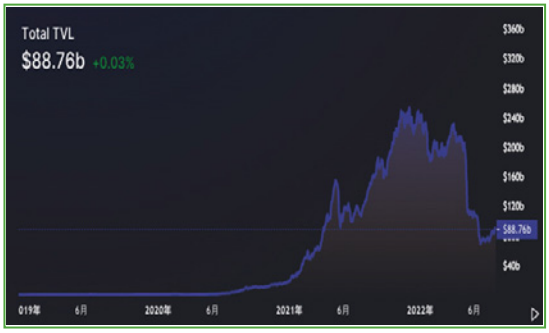
2022年初迄今為止，隨著全球的經濟成長動能趨緩，以太坊DeFi市場正在經歷一場戲劇性的去槓桿化，不僅是數位資產，幾乎所有資產都迎來資金緊縮的時刻，全球央行收緊貨幣政策、美元走強以及風險資產估值下降引發了廣泛的追加保證金、債務清算和去槓桿化。DeFi總鎖倉量從年初的2,350億美元已大幅下降至2022年7月31日的887億美元（圖5），減幅達67%。DeFi產業自發展以來，首度進入緊縮期，相較於一般性資產如股票、債券等市場，DeFi市場衰退的幅度如此迅速主要原因可以歸納出以下三點：

（一）收益率的一體兩面：隨著加密市場在 2020年底之後反彈，協議的使用率、流動性及槓桿比率隨之飆升。使用量的增加進而產生更高的收益率，流動性提供者可賺取更多的兌幣費用，借貸市場的存款利率上升，以代幣計價的激勵措施價值也一同上升。在此期間提供3位數以上的年百分率（Annual Percentage Rate，簡稱APR）的DeFi平台相當常見，也吸引了大量資金流入。然而，隨著加密貨幣價格下跌，鏈上活動也跟著減少。收益率下滑的同時，也導致部署資金於DeFi的吸引力逐漸降低，資金進而外流。

（二）過度仰賴流動性挖礦：DeFi老手們認為流動性挖礦[10]就像是將金融遊戲化，但這種貨幣激勵系統產生的增長是沒有持續性的。進一步來說，流動性挖礦對協議的初期增長相當具有幫助，但只要獎勵開始下滑，資金便會從交易所或協議中流出。此外，流動性挖礦對獎勵代幣的價格造成不少下跌的壓力，因為唯有將其賣出才能獲得收益。這種方式也使得治理平台的資本縮減，因為協議通常將其原生代幣很大一部分比例分配給這些獎勵計劃。不但減少了協議能用來發展的資金，在惡劣的總經環境下也顯得更缺乏資金運用的彈性。

（三）協議爆炸及漏洞利用：隨著市場不斷走跌，許多事件損害了人們的信任並突顯了DeFi固有的主要風險。迄今為止，最嚴重的為Terra崩盤事件，也被稱為幣圈史上最大黑天鵝，UST及LUNA的死亡螺旋導致投資人們上百億的損失，Terra生態系的其他協議也同時遭受牽連。DeFi遭駭事件也對投資人的心理造成不小影響，僅在2022年，20次駭客攻擊就造成超過14億美元的用戶資金損失，已經超過了2021年整年的損失金額。駭客攻擊的頻率和規模可能導致鏈上活動急劇下降，再加上收益率的減少，使得在鏈上部署資本的風險回報率不如過往。

圖 5：DeFi市場總鎖倉量（2022/7/31）



資料來源：DeFi Llama

三、DeFi生態系眞實發展概況

隨著熊市的到來，整個以太坊生態系統目前正在經歷歷史性的去槓桿化。DeFi市場雖看似進入熱潮消退的階段，但其實主要DeFi指標，如TVL並不能夠顯示DeFi整體發展的情況，由於這些指標僅代表當前市場的狀況，因此我們須探究DeFi本身的生態系統發展現況，以下就幾個面向參考：

（一）Layer 2：在DeFi生態系中的第二層Layer 2，其中所具代表的解決方案Optimism和Arbitrum仍正不斷改進，使用所耗費的燃料費越來越少；Polygon目前正開發多種擴容解決方案，包括Hermez、Nightfall和Maiden等ZK rollup技術。而StarkWare在成功擴展 dydx、DeversiFi 和Immutable X等單一用途的協議後，正在開發一種更通用的ZK rollup 技術，稱為StarkNet的解決方案。

ZK rollup技術的工作原理是在區塊鏈主鏈外進行運算和數據儲存，並將交易數據批次發送到主鏈，ZK rollup技術創建一個加密驗證訊息的方式，並將這些驗證後的交易數據壓縮打包回傳至主鏈上，由於交易數據相較於Layer 1來得少，因此交易過程所耗費的燃料費遠低於原本在主鏈上驗證的成本。這項技術相當複雜，卻是一項非常重要的技術，ZK rollup是目前公認最佳以太坊可擴展性方案，它不僅在安全性上媲美以太坊Layer 1，而且在交易速度上是Layer 2解決方案的翹楚，因此大多數以太坊社區成員希望它能成為以太坊擴展問題的長期解決方案。

（二）競爭鏈：其他公有鏈如Avalanche、Fantom、Solana、Terra 等鏈上的DeFi也正在經歷快速增長階段。雖然目前這些鏈上的DeFi協議，大多只是以太坊上協議的分叉，但其實這些協議的開發團隊也正在努力開發新功能。儘管有部分批評，但其實可以發現多鏈理論慢慢被眾人所知，DeFi用戶樂於將資產跨鏈以尋找更好的收益。

（三）DeFi 2.0：儘管目前市場過度膨脹，但這種典範轉移的某機制（資金流動性的利用）可能將為DeFi生態系統帶來更多創新功能。例如Tokemak是一個將流動性挖礦機制改良的協議，目前保持超過10億美元的TVL，並為整個DeFi生態系統引入了新的實用功能。

（四）NFT：NFT、元宇宙和 crypto社交媒體（例如Aave團隊推出的Lens協議）一直是討論的熱門話題。雖然與DeFi看似沒有直接關係，但這些趨勢可以將更多人帶入加密世界，並順勢讓人們發現並接觸DeFi。

（五）機構：在市場降溫期間，雖然普通用戶不太願意投資新專案，但創投公司不會停擺，而是向DeFi生態系整合加密世界注入了數十億美元。這為早期專案提供了足夠的資金來專注於開發，而不是思考如何生存到下一個牛市，因此有助於DeFi市場的成長。

從上述不同面向來看，儘管市場看似低迷，但DeFi生態系統現今仍在蓬勃發展，目前以借貸、交易等領域的應用最為繁榮（表4）。而Layer 2將是未來另一個催化劑，未來DeFi將會比以往更便宜且更快速，並將可以啟用以前無法在以太坊上運作的新DeFi協議；而NFT、元宇宙和也可以在未來替DeFi提供成長動力，這些題材可能成為生態系統的支柱。此外，各國政府未來勢必會做的一件事情是釐清DeFi的法律和稅收規定，當前不明確的規則扼殺了創新，並為DeFi開發者和用戶創造了不友善的環境。當市場注意力從TVL上移開時，眼光長遠的開發者會繼續創造價值，並不斷提出新的想法，而這些想法將會為下一個市場週期提供養分。

表 4：DeFi鎖倉量前十名平台及協議（2022/07/31）

排名	平台協議名稱	類別	總鎖倉量（億美元）
1	MakerDAO	抵押債倉	$86
2	Lido	借貸	$74
3	AAVE	借貸	$66
4	Uniswap	交易所	$64
5	Curve Finance	交易所	$64
6	Convex Finance	聚合器	$37
7	JustLend	借貸	$34
8	PancakeSwap	交易所	$32
9	Compound	借貸	$30
10	Instadapp	聚合器	$21

資料來源：DeFi Llama

第二節 穩定幣－連接加密貨幣世界與傳統金融的媒介

在探討DeFi實際應用案例之前，本節欲先闡述穩定幣的特性及發展概況，將有助本文瞭解為何穩定幣可以迅速崛起及為何穩定幣是許多DeFi平台中使用頻率最高的加密貨幣。

由於加密貨幣無政府或機構背書，價格波動較為劇烈，以比特幣為例，2021年的2~4月份，比特幣經歷了2次單日劇烈波動，如2月22日，比特幣由最高價為58,334美元跌至低價47,975美元，單日波動達到10,000美元。為了提升數位貨幣資產保值能力，穩定幣項目逐漸向市場推出，截止至2022年7 月，共有85種穩定幣顯示於CoinGecko上，其中市值排名前5的穩定幣擁有總計超過1,400億美元的市值。

表 5：全球排名前5穩定幣市值（2022/07/31）

排名	貨幣	總市值（億美元）
1	USDT	$659.10
2	USDC	$544.88
3	BUSD	$178.76
4	DAI	$70.04
5	Frax	$14.67

資料來源：CoinGecko

穩定幣錨定類型可分為法幣抵押型和加密貨幣抵押，目前大部分穩定幣採用的是法幣抵押型系統維持對美元的錨定，例如 USDT與USDC，而加密貨幣抵押型的代表則是DAI。USDT作為法幣抵押型的穩定幣，通過每鑄造1枚USDT代幣，將1美元準備金保存在金融機構中的方式將自身錨定為1美元，因此，USDT是一種中心化的數字貨幣資產，價格依賴於用戶對於USDT準備金制度的信任。DAI屬於去中心化的加密貨幣抵押型穩定幣，其價值由ETH等加密貨幣資產抵押生成，通過去中心化自治組織表決的協議和智能合約實現與1美元的錨定。此外，基於區塊鏈透明的特徵，用戶在任何時間都可以比較容易的驗證DAI的抵押品。DAI為DeFi生態中使用最為廣泛的原生穩定幣。廣泛應用於各大借貸平台、DEX交易所、衍生品交易平台，包括 Compound、Uniswap，Sushiswap等。DAI的主要應用場景可以歸納出以下前五大類：

一、徹底實現財務獨立

在傳統金融系統中，銀行和其他金融服務公司會要求用戶提供大量訊息，包括個人資料、良好的徵信證明，甚至是最低存款額。由於這些繁瑣的要求，世界上還有很多人沒有銀行帳戶，或享受不到充足的銀行服務。與之相對的是，不管你是誰，身處何地，無論你的經濟狀況如何，你都可以通過穩定幣 DAI獲得金融服務。這就為所有人創造了前所未有的財務獨立機會。

在通貨膨脹嚴重的阿根廷，政府一貫對資本採取嚴格管控措施（例如，限制取款），損害了那些使用美元作為儲蓄貨幣的居民的利益。對於這些居民來說，DAI不失為一種解決方案，獲取門檻比美元低，同時比本地貨幣的幣值更穩定。

二、儲蓄

DAI持有者可以將DAI鎖定在一個特殊的智能合約（DSR）中，賺取存款利息。DAI存款利率不收取手續費，不設地域限制，也沒有流動性障礙—沒有最低存款額要求，用戶可以隨時取出全部或部分DAI。任何人都可以通過 Oasis Save或其他整合了DSR的項目（例如，OKEx和Argent錢包）來取得 DAI存款利率合約。除了能推動財務獨立、讓用戶獲得完整的控制權之外，DSR還能徹底改變DeFi營運的模式。

三、資金避風港

穩定幣DAI為波動性極強的加密貨幣領域提供了穩定性。DAI錨定美元，並由鎖在各Maker金庫中的超額擔保品背書。當市場出現劇烈波動時，DAI可以幫助用戶存儲價值，成為加密貨幣領域的安全港。

四、方便、快捷、低成本的匯款服務

作為穩定的交換媒介，DAI可以用於償還債務、跨境交易以及購買商品和服務。通過傳統金融服務進行跨境轉帳是一件成本高昂且極度耗時的事。舉例來說，截至本文完稿時，美國銀行的匯出境外匯款（以美元為匯款幣種）服務需收取45美元的手續費。如果從西聯匯款的美國網點向阿根廷網點轉帳，每轉帳1,000美元需收取9美元的手續費。由於Maker協議是構建在區塊鏈上的，用戶可以使用DAI在全球範圍內進行點對點轉帳，只需花費幾秒鐘時間，成本也只是傳統轉帳服務的一小部分（用戶只需支付以太坊網路礦工費）。

五、其他基於區塊鏈的服務

DAI也給小眾用戶提供了良好的服務，例如2019年6月，Maker與Axie Infinity公司達成合作，將DAI整合進了該公司的鏈上數位寵物養成遊戲。一年不到，Maker基金會又於 2020 年3 月推出了DAI遊戲計劃，旨在提高DAI的全球經濟影響力。

基於上述穩定幣抗波動的特性以及多元化的應用場景，穩定幣成為DeFi生態系組成最關鍵的元素之一，對後續章節所介紹的DeFi協議與平台都有相當重要的地位。

第三節 去中心化借貸－賦予加密貨幣生息

DeFi借貸旨在以無需中介參與且無需信任的方式提供加密貨幣貸款，借款人可以通過平台直接且即時的獲得貸款，同時，平台允許用戶將他們的加密貨幣借給其他人並賺取貸款利息。傳統銀行一直都在把這項服務利用到極致，而在DeFi的世界裡，任何人都可以成為貸方，貸方可以將其資產借給他人，並能夠從該貸款中產生利息。加密貨幣借貸通常涉及三方：借方、貸方和DeFi平台，其工作原理說明如下：

借方：借款方將加密貨幣投入平台資金池，並簽署智能合約，當借方欲贖回資金時，會觸發智能合約並履行契約內容，平台會依照資金投入當下訂定的利率給予相對應得報酬。

貸方：貸款方通常需先投入加密貨幣到平台上作為抵押品，在一定擔保比率內可以從平台上貸出其他加密貨幣，當貸款方欲償還借款時，同樣會觸發智能合約並履行契約內容，平台會依照資金借出當下收取相對應的本金及利息。

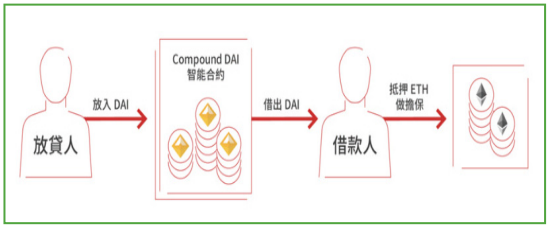
DeFi平台：藉由一套利率模型計算整個平台上的借款及貸款利率，並透智能合約自動運行借貸方的合約，並從每筆交易當中收取手續費。

目前市場主流DeFi借貸平台包含Compound、Lido、Aave等，本文將以曾經躍居DeFi借貸領域榜首的Compound作為主要研究應用案例，其截止2022年7月31日總鎖倉量高達約30億美元。Compound係由Robert Leshner 創立於2018年9月，是一個透過ETH區塊鏈上的智能合約達到去中心化借貸的服務。相較於傳統銀行借貸，Compound擁有公開透明的利率模型、高隱私性、即時借款、放貸免綁約的特色。其主要架構及運作方式如下：

一、Compound基本架構

Compound提供好幾種不同的ERC-20[11]加密貨幣資產以供借款與貸，目前支持ETH、USDC、DAI、REP、WBTC等代幣的借貸，每一種代幣擁有獨立的資金池，交易雙方不需要單獨撮合，故不存在交易對手風險。以圖6舉例來說，首先，放貸人將DAI放入智能合約中，即可完成貸款並產生利息，其中智能合約會產生出額外的cDAI（Compound DAI） 給放貸人，利息會累積在cDAI之中，放貸人隨時能以cDAI 換回原本的DAI以及多出來DAI的利息。而借款人可以透過抵押資產的方式借出智能合約的DAI，並依照利率支付利息。

圖 6：Compound借貸款流程圖

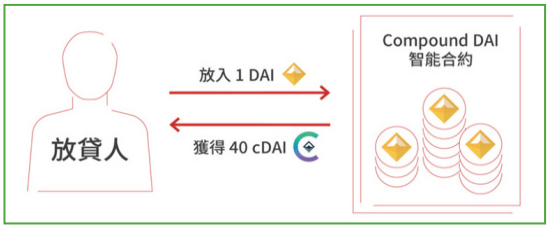


資料來源：[2] 詹舜傑（2019），Compound完全解析－利率模型篇

二、利息產生方式

假設放貸人放入1 DAI，獲得40 cDAI，因此當下 DAI與cDAI 的兌換率是1/40 = 0.025，隨著時間與利率增加，此兌換率的值會越來越大，實際舉例：

圖 7：Compound利息生成流程圖



資料來源：[2] 詹舜傑（2019），Compound完全解析－利率模型篇

- 小明於2019/10/10將1000 DAI放入智能合約中，並獲得40,000 cDAI
- 2019/10/10這天DAI與 cDAI的兌換率 = 0.025
- 2020/10/10小明決定把放貸的錢連本帶利提出來。這時候，DAI 與cDAI 的兌換率增加到0.0275
- 小明用之前持有的40000 cDAI換回了40000 x 0.0275 = 1100 DAI
- 多出來的100 DAI就是小明這一年放貸所得到的利息

三、借貸利率模型

進一步說明Compound的借貸利率模型。首先，須先瞭解其中最重要的一個指標為使用率（Utalization Rate），指的是所有放貸進來的錢當中，已經被借走的比例。

$$使用率 = \frac{totalBorrows}{totalCash + totalBorrows}$$

- totalCash =放入智能合約，但還沒被借DAI的總數量
- totalBorrows =所有借款人，所應償還DAI的總數量（含本金利息）

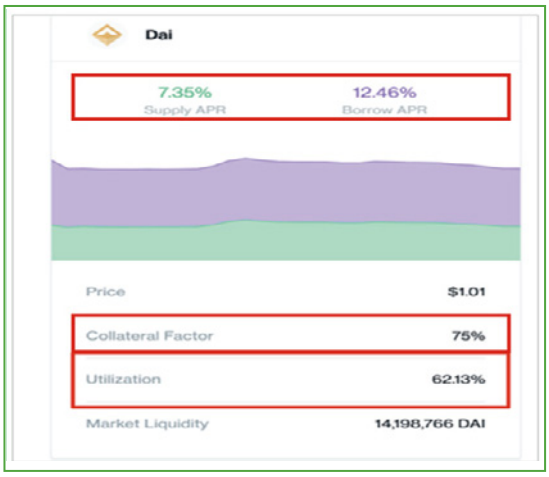
（一）借款年利率：借款年利率公式通常是遞增的線性函數，其中y的截距為基礎利率，代表借款沒有需求時的借款利率，而斜率則是代表借款利率變化的比率，即為公式中的使用率乘加給利率。每一種平台支援的ERC-20加密貨幣參數均不相同，有些加密貨幣市場內含諸如轉折點這種比較進階的公式，當使用率較低時，進階公式可以壓低借貸成本促進流動性，直到觸及轉折點以後再拉高借貸成本。基本借款年利率的公式如下：

借款年利率
＝基礎利率＋（使用率 x 加給利率）

（二）放貸年利率：放貸年利率則是借款年利率乘以使用率，確保借出款項能夠完全支付放貸方的利率，同時會有準備金係數，是指借出款項未支付給放貸方的利率。在極端的價格變動期間，許多部位可能因資金不足以償還放貸方而出現擔保不足情形，這時放貸方即可獲得準備資金池中的資產獲得償還。貸款年利率公式如下：

貸款年利率
= 借款年利率 x 使用率 x (1- 準備金係數)

圖 8：Compound DAI市場使用率、借貸利率及擔保率



資料來源：[2] 詹舜傑（2019），Compound完全解析－利率模型篇

以圖8 Compound DAI為例：
當Dai基礎利率= 5%，加給利率= 12%，
若以當下的使用率= 62.13%計算：
借款年利率
=5%+(12%x62.13%）
= 12.46%
放貸年利率
=12.46% x 62.13% x（1 - 5%）
= 12.46% x 62.13% x 0.95
= 7.35%

四、擔保率

借款人在借出其他加密貨幣之前，需要先存入抵押資產，而平台上每一種ERC-20加密貨幣都有專屬的擔保率，分佈範圍由0%至90%，通常流動性較低的貨幣所需的擔保率較高。藉由擔保率的機制，可以避免借款人發生不還款的情形，倘借款人不還錢，則智能合約會將抵押的資產進行清算，讓借款人的借款金額維持在擔保率範圍之內，續以圖8舉例：

- 假設小明想要抵押1,000 DAI借出ETH，目前市價1DAI = 1USD，故小明抵押了相當於1,000 USD的資產。
- 當前DAI抵押率= 0.75，因此小美實際上能借的最大資產= 1,000 x 0.75 = 750 USD。
- 故小明能借出75 ETH （假設目前市價 0.1 ETH = 1 USD）
- 假設經過一段時間後，小美需要償還 6 ETH的利息，而 6 + 75 = 81 ETH，已經超過小明能借的最大資產量，但小明未進行償還。
- 因此，小明抵押的部分資產將會被強制清算，在Compound的清算機制下，最多會有一半（81/2） ETH的借出資產會被清算。
- 假設有40 ETH被清算，乘以一個清算比例，假設為1.1（其中10%作為平台清算手續費），也就是44 ETH=440 DAI會被沒收，償還小明440 USD的債務。
- 清算後，小明剩下81–40= 41 ETH需要償還。
- 而此時小明抵押的DAI剩下1000-440=560 DAI，故目前可以借的最大資產 = 560 x 0.1 x 0.75 = 42 ETH >需要償還的41 ETH，清算完成。

在Compound整個運作流程中，透過智能合約的運轉，可以即時放貸生利息、即時借款還款，沒有一對一借貸媒合的問題，只要持有cDAI 就可以收到 DAI的利息，同時清算機制能避免借錢不還，保障放貸人的權益。Compound簡易的放貸流程以及即時收益或借款的流動性獲得市場青睞，因而成為DeFi借貸領域中最具指標性的借貸平台之一。

表 6：Compound解決傳統金融借貸之問題

	傳統金融問題	Compound 解方
集中式掌控	借款與放款利率掌握在金融機構手中	Compound 利率交由演算法決定，由市場機制主導
有限獲取	難以獲得高報酬的投資機會或有競爭力的借款方案	支援任一種加密貨幣借貸，借貸方可以挑選對自己最有利的市場及時點進行投資或借款
效率低落	由於中間需由人力介入，作業程序繁複，借貸款所需時間較長	透過智能合約立即執行借貸款
資訊不透明	貸款機構的擔保率及借貸款利率不透明	擔保率與借貸款利於可以於平台看見

資料來源：《DeFi未來銀行》一書

第四節 去中心化交易所－創造加密貨幣流動性

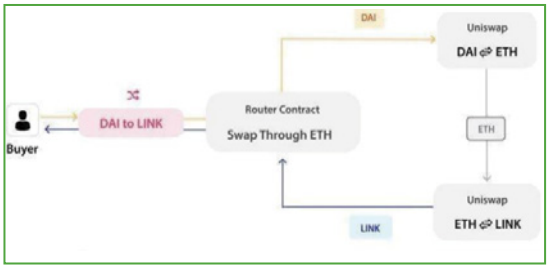
當我們今天想要進入傳統金融市場，需要到證券商開立一個證券戶，並透過台灣證券交易所了解市場行情，進而開始買賣，而台灣證券交易所在這就處於一個「中心化交易所」的概念，交易我們所熟悉的這些金融商品，如外匯、證券、現貨交易以及期貨交易等。而在加密貨幣的買賣上，也是相同的概念，投資人可以透過在加密貨幣中心化交易所（Centralized Exchange, 簡稱CEX）線上註冊帳戶後，並進行KYC認證，即可進行投資交易。一直以來，CEX都是加密貨幣市場的重要支柱，它們的特性包括結算速度快、交易量龐大，且流動性不斷增強。但CEX無法賦予用戶對於資產的控制權，加上CEX錢包存放著所有用戶的資金，資金量龐大因而容易受到駭客的攻擊，一旦受到攻擊，所有用戶都可能遭受損失，根據Cointelegraph數據顯示，2019年有超過2.9億美元的加密貨幣資產被盜，同時超過50萬條個資訊息從CEX交易所洩露。

鑑於去中心化交易所（Dcentralized Exchange，簡稱DEX）相對CEX更為透明、安全、不受監管，以及用戶擁有更多的控制權等優勢，用戶逐漸由CEX轉為使用DEX。2020年DEX迅速發展，多個DEX平台孕育而生，像是Curve主要應用於穩定幣互換、Uniswap主要應用於以太坊的加密貨幣之間的兌換，並提供豐厚的流動性挖礦獎勵和去中心化治理機制。本文將以DEX領域總市值位居最高的Uniswap V2作為主要研究應用案例，其截至2022年7月31日總鎖倉量高達約64億美元。

一、Uniswap基本架構

Uniswap是基於以太坊網路的一種DeFi協議，專注於自動兌幣的DEX類應用。在2018年時，Uniswap協定由Hayden Adams創立，它所應用的技術原理是由以太坊聯合創辦Vitalik Buterin率先提出。Uniswap的主要功能是支援ETH與其他代幣、或是ERC-20代幣之間的兌換，實際兌換流程如圖，當用戶於平台選擇以DAI兌換LINK，平台將透過智能合約來履行交易，ETH會作為中介代幣轉換為LINK給用戶，而每筆交易會收取0.3%的手續費用。

圖 9：Uniswap V2交易流程圖



資料來源：Uniswap白皮書

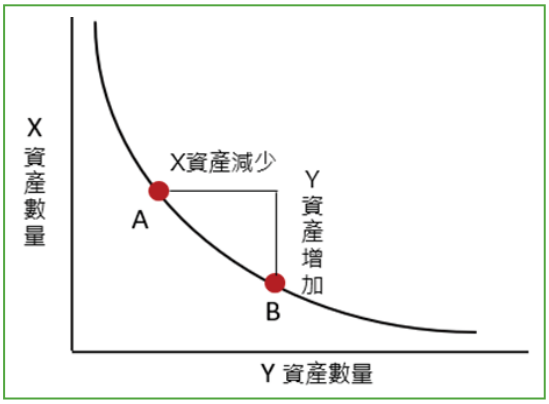
二、匯率模型

在Uniswap的交易並不是像傳統金融一樣，透過搓合買賣方訂單的交易，而是在資金池做兌換，Uniswap所採用的模型會涉及流動性供應者及流動資金池的建立，並提供一種去中心化的定價制度，有別於以往交易所使用的訂單簿[12]交易，為確保所有交易都能夠執行，此定價制度是採用AMM[13]自動造市商[14]的變體，稱為恆定乘數造市商（Constant Product Market Maker），公式如下：

$$K=XxY$$

其中X與Y兩種加密貨幣資產之餘額，K為一不變常數，也就是X與Y呈反向關係。

圖 10：恆定乘積公式示意圖



資料來源：本研究繪製

例如在USDC/DAI的資金池中，USDC的數量稱作X，DAI的數量稱作 Y，在資金池中有4個USDC和4個DAI，此時制定出有效匯率為1：1，恆定值為4x4 = 16。如果有名投資者要以4個DAI兌換資金池當中的2個USDC時，資金池中的DAI餘額會變成4+4=8個；USDC餘額為2個，恆定值維持在16，此時有效率匯率變成1 USDC：2 DAI。其中匯率的改變是出於低度市場流動性所導致的滑價，當資金池中的代幣數量很少，也就是總資金量K越小時，出現差價的情況就會越多。若假設資金池中餘額是100個USDC和100個DAI，恆定值為10,000，匯率一樣為1：1。如果這名投資者同樣以4個DAI兌換USDC，在恆定值不變下，可以換得3.85個USDC，此時有效匯率變成1 USDC：1.04 DAI，可見較高的市場流動性有助改善滑價，因此平台會提供回饋來吸引資金注入市場。

三、治理代幣UNI

不論是前一節提到的Compound或是Uniswap，許多DeFi平台都有發行各自的治理代幣（Governance Tokens）。治理代幣源自於去中心化自治組織（Decentralized Autonomous Organization，簡稱DAO）此一概念，比特幣早期參與者Mike Hearn是最先提出這一想法的人之一。

DAO其實是一個由電腦代碼及程式所管理的組織，因此它能自主運作，而無需中央機構介入。DAO的規則和交易記錄公開儲存在區塊鏈上，規則一般由利害關係人投票決定，在DAO中進行決策的方式是透過提案與投票，如果提案獲多數利害關係人投票通過，接著便會實施提案。從某方面來看，DAO的運作方式類似於公司或民族國家，但以更去中心化的方式運作。DAO最重要的一環就是治理型代幣，治理型代幣是開發人員創建的代幣，代幣持有者有權塑造 DAO的未來。治理型代幣持有者可以影響與項目相關的決策，例如改變治理系統，或更改DAO管有資金的使用方法。很多時候，DAO都是透過智能合約，通過使用治理型代幣，在區塊鏈上通過提議、審查及表決，之後作出決定和改變。

Uniswap於2020年9月16日推出UNI代幣， UNI的初始供應量為10億枚代幣，60%分配給Uniswap社群成員，而其餘40%則在4年內分配給團隊成員、投資者及顧問。在推出UNI代幣之後，這段期間平台有許多提案，其中最受到矚目的是在2021年5月，Uniswap社群提案在Layer 2擴容方案Arbitrum網路上部署Uniswap V3的治理投票獲得了壓倒性支持，將能有效解決以太坊交易壅塞導致手續費飆高的問題，並提升 Uniswap作為DEX的競爭力。

Uniswap是DApp的關鍵基礎建設，它提出獨一無二的運作方式讓任何用戶都能成為流動性提供者，雖然不像CEX擁有成本低、交易快的特性，但Uniswap透過去中心化的特性，讓用戶有權參與平台之發展，如今已更新至第三版本，不斷改高善成本與資金流動上的問題。而隨著以太坊上自動造市商總量成長，加上許多狹著競爭模式的新平台崛起，Uniswap將持續成為關鍵基礎建設的典範。

表 7：Uniswap解決傳統金融交易之問題

	傳統金融問題	Uniswap 解方
集中式掌控	股票或匯率市場是依據交易所規則撮合每筆買賣交易，且資金由金融機構持有	倘某一筆交易無法撮合，允許任何人自行打造新組合，且資金由用戶自己的加密錢包管理
有限獲取	資金提供的最佳投資機會與報酬受到第三方機構限制	任何人都可以成為資金提供者並賺取回饋
效率低落	交易結算時間通常為 T+2	直接透過智能合約進行交易結算
資訊不透明	無法確認交易所是否擁有所有用戶的全部餘額	平台提供透明的流動性與演算法定價

資料來源：《DeFi未來銀行》一書

第五節 去中心化衍生品－加密貨幣金融市場多元化

衍生品一直都是全球金融市場最重要的部分之一，為投資者提供多元化收益途徑、對沖市場風險提供了不可或缺的作用，其市場規模往往是現貨市場的數十倍。相比之下，加密貨幣衍生品市場規模仍然處於非常早期的階段，目前去中心化衍生品市場僅發展約三年的時間。而隨著DeFi近幾年的大規模發展以及市場的普及，為衍生品在DeFi領域的發展提供了必要的條件，並已經充分展現出自身的優勢。DeFi衍生品的種類目前主要包括合成資產、期權、利率衍生品、預測市場、永續合約、保險等六大方向，其發展邏輯與競爭格局也越來越清晰，以下針對這六大方向進一步說明其所具備之金融市場功能。

一、合成資產

合成資產是由一種或多種資產/衍生品組合併進行代幣化的加密資產，DeFi生態早期的合成資產以穩定幣DAI、跨鏈包裝資產WBTC為代表，此後基於現實世界中股票、貨幣、貴金屬等的合成資產也越來越豐富，如今也已經成為DeFi生態的重要組成部分。合成資產背後的理念是為投資者和交易者提供各式的資產類別的風險敞口，但並不要求他們持有標的資產或信任託管人。目前，DeFi用戶只要通過Synthetix、UMA等合成資產協議並存入一定的抵押品，即可創建任意支持的合成資產，但這些資產並不會錨定真實的加密或實物資產，其價格主要由Chainlink等鏈外預言機提供，如果資產價格出現大跌、虧損達到一定比例，系統則會對抵押品進行清算。相比於初始資產，合成資產的優勢在於放大了鏈上資產的可組合性，同時為DeFi生態搭建了一座可以通向百萬億級規模傳統金融市場的橋樑，豐富DeFi用戶的投資選擇。

二、期權

期權是一種權利，是指期權買方有權在約定時間內以約定價格買入或賣出一定數量標的資產的權利。在傳統金融領域，期權又分為商品期權和金融期權，被廣泛運用於套保和對沖風險中，用來抵禦持有標的資產價格下行和未來買入資產價格上漲的風險，在世界經濟中發揮著重要作用。例如在加密貨幣領域，如果投資者已買入ETH，其既想享受持有ETH上漲的收益，又不想承擔ETH下跌的損失，可以買進ETH 的看跌期權來對沖現貨風險。如果ETH下跌，則可以行權，按照執行價賣出ETH從而規避現貨下跌風險。或者賣出ETH看跌期權，ETH價格下跌，看跌期權價格則會上漲，期權的價差收益會彌補持有現貨的損失，以此來對沖買進現貨的損失。當然，期權產品也具有很強的投機性，用戶完全可以利用其隱含波動率等進行投機套利。

2018年起，HBO三大中心化所逐漸引入簡易期權模式，但直到去年DeFi版塊火爆之後去中心化期權項目才開始起步。目前主要分為和傳統金融市場類似的標準化期權，有opyn、siren等；和簡化版的期權交易，僅需選擇方向、數量、行權價、持有時間即可創建一個期權，這類期權項目有：hegic、charm、FinNexus等，使加密貨幣領域的用戶可以更簡便的使用期權工具。與傳統金融領域中期權市場的體量相比，DeFi期權市場仍然很小。目前加密市

場中，中心化期權項目Deribit佔加密期權80%以上的市場流動性，流動性仍然是去中心化期權項目面臨的最大難關。

三、利率衍生品

利率衍生品是DeFi行業2021年以來討論諸多的方向，其主要是基於加密資產利率開發不同類型的衍生產品，滿足DeFi用戶對確定性收益的不同需求。一般而言，利率衍生產品是指以利率為基礎的衍生產品，通常被機構投資者、銀行、公司和個人用作對沖工具，以保護自己免受市場利率變化的影響。由於借貸利率的波動性往往會對投資者帶來額外的風險，且大部分投資者風險偏好較低，因此傳統金融市場中利率衍生品市場已經成為規模最大的衍生品市場。

不過在目前，DeFi借貸協議與收益聚合器的收益機制幾乎都是浮動收益，且相關利率衍生產品並不豐富，不利於投資者有效控制風險。因此隨著越來越多對低風險偏好的傳統資金入場，固定利率及其衍生品市場將更受到這些資金的青睞。目前，DeFi市場已經湧現多個固定利率協議，以零息債券的形式為用戶提供具有固定利率的借貸產品，用戶存入資產後無論市場利率如何變化，均能在合約結束時根據自己最初設定的利率獲得收益，例如Notional Finance、Yield Protocol、Mainframe、88mph等。

四、預測市場

預測市場是以太坊生態最早出現的應用場景之一，並在2020年美國大選中迎來爆發式增長，成為DeFi衍生品的重要組成部分。預測市場是根據未來有確切結果的事件而創造的合約，可以理解為彩票市場和調查問卷的結合，目的是用來發現市場相信的結果。它允許任何人對未來事件下注，並且利用這些下注的機率，來作為這些事件的預測概率的可信中立來源。

此外，預測市場相當於廣發調查問卷，反映了人們對該事件的態度，並可以以此為依據改善治理或作出決策。以「ETH價格在7月1日會超過10000美元嗎？」事件為例，該事件為用戶提供了兩個投資選擇：YES或者NO，兩者的價格可以視為市場對該事件可能實現的概率，兩者之和固定為1美元。用戶如果認為市場價格偏離實際概率，例如ETH價格在7月1日超過10,000美元的概率高於YES價格所代表的19%，即可以選擇購買相應選項並從中獲益。

預測市場的投機性同時確定了其對沖性質，可以用於對沖風險以及衍生的影響。依舊以「ETH價格在7月1日會超過10,000美元嗎？」事件為例，如果你在現實世界持有ETH現貨，則可以購買「NO」以對沖ETH價格下跌的風險。與中心化平台的預測市場相比，DeFi領域的預測市場具有不可篡改、公開透明等特性，且費用低廉，消除了交易對手方的危險，交易者無需擔心平台會從中作梗。目前，以太坊生態的主要預測市場項目包括PolyMarket、Augur、Omen等。

五、永續合約

合約產品是在加密市場較早出現的衍生產品，也是目前交易量最高的衍生品。與現貨交易不同，期貨合約是雙向加槓桿產品，可以從標的資產價格下跌中獲利，且其槓桿屬性放大了交易風險和利潤，並且可以對現貨持倉及未來即將收到的現貨進行風險對沖。

BitMEX、幣安、FTX等中心化交易所是目前加密市場合約產品的主要平台，從中獲取了大量流量與利潤，但由於中心化交易所清算機制不透明、極端行情之下經常出現無法交易、插針、收費過高等問題，因此去中心化合約產品逐漸成為用戶的新選擇。目前，DeFi市場合約產品大多為永續合約，知名平台包括dYdX、Perpetual protocol、MCDEX、Injective Protocol等。相比中心化交易所，DeFi合約產品的主要難題在於流動性不足以及燃料費過高，後者又會加劇前者的狀況，在以太坊燃料費居高不下的情況下，大部分DeFi合約產品的交易量並不高。不過隨著Layer2協議的陸續推出，這些問題一定程度上都可以得到解決，目前dYdX已經基於StarkEx推出其Layer 2產品， MCDEX、Injective等協議也都陸續提出將開發Layer 2的產品。

六、保險

保險是全球金融市場重要的衍生品方向之一，它將經歷災難性事件的代價社會化，從而使個體/機構能夠承擔潛在的風險。在DeFi領域，由於新項目層出不窮以及許多開發者過於鬆懈，時常出現DeFi項目被攻擊並導致用戶遭受階段損失的事件，特別是近期DeFi安全事故明顯增多，這很可能會對越來越多傳統資金進入DeFi市場造成阻礙。因此，保險對DeFi市場顯得尤其重要，隨著保險領域的成熟以及機構參與者的加入，保險可能會成為DeFi的最大支柱之一。

當前階段，DeFi保險仍處於發展早期階段，保單覆蓋資產僅為總鎖倉價值（TVL）的1%不到，大部分主流DeFi項目也尚未購買保險。這一定程度上市由於部分賠付場景判定困難、資本金仍不足以賠付主流DeFi項目資金規模等。隨著越來越多DeFi保險協議的推出，目前各類保險項目覆蓋的承保場景越來越多豐富、質押池資金也在逐步擴充，同時產品形式也越來越多多元化。目前，Nexus Mutual、Cover、Unslashed、Opium等項目是該領域主要的玩家，Nsure、Union、Armor、Umbrella、Helmet等項目也具有一定影響力。

從本章節歸納出的DeFi發展趨勢及應用來看，DeFi改善了傳統金融產業交易速度慢、成本高、易遭駭客攻擊或被政府濫用等問題，且藉由DeFi多元的金融服務種類，從底層架構的區塊鏈到Layer 2，再到穩定幣、交易所、借貸平台、衍生性商品等，這些加密資產、智能合約和協議能像樂高一樣自由組合，因此DeFi也有「DeFi樂高」的別名。DeFi樂高的高組合性及互操作性，讓開發者可以更自由地在現有基礎上開發新的服務，用戶也可以在DeFi生態系中依自身需求找到最適合自己的投資工具及策略。由於DeFi是個剛起步的產業領域，除了有許多新的商業可能性和技術突破還尚未被開發，更出現「DeFi正在吞噬傳統金融世界」等豪語出現，而這也是本文嘗試探討DeFi之主要原因，在後續章節將會分析DeFi對銀行業產生之機會與挑戰。

～待續～

參考文獻

1. 例如可去中心化運行智能合約（smart contract）的以太坊（Ethereum）平台。
2. 去中心化應用程式（decentralized application, DApp）係指在去中心化運算平台上運作的應用程式，包括智能合約，以及便於一般人操作的使用者介面。
3. 非同質化代幣（Non-Fungible Token，簡稱NFT）是一種奠基在區塊鏈技術之上的代幣，每一個代幣都標誌著一個獨特的數位資料，就像是一種數位所有權證明，標誌著數位物品的所有人與交易紀錄。
4. 指一個虛擬的現實世界，藉由虛擬實境（VR）、擴增實境（VR）與3D投影等技術，讓使用者可以化身為虛擬分身進入世界，可以在其中互動、玩遊戲、工作以及體驗生活。
5. 智能合約（Smart Contract）是區塊鏈中制定合約所使用的特殊協議，是一種自動執行的合約，並用代碼形式在區塊鏈上運行，且不能被加以更改。
6. 比特股（BitShares，縮寫BTS）是一種支持包括虛擬貨幣、法幣以及貴金屬等有價值實物的開源分佈式交易系統，該系統主要能提供一個去中心化交易所的解決方案，該系統是2014年由Invictus公司推出。
7. 開源程式碼是指程式開發者將程式原始碼（Source code）公開，讓大家可以自由取得，自行進行各式更改與發展更廣泛的應用。
8. 燃料費是區塊鏈上程式碼在執行時，所需付出的費用代幣。燃料費會做為礦工們做驗證的獎勵，執行任何程序都需要消耗燃料，當燃料用盡就不會繼續運作，也避免了寫程式時可能造成無限迴圈這類型的問題。
9. 總鎖倉價值（Total Value Locked，縮寫TVL），指的是DeFi協議（平台）的流動性資產總量，是常被用來衡量在資金池裡鎖定的代幣資產總量的指標。
10. 流動性挖礦並非真的挖礦，而是透過提供資金、提供流動性的方式獲取收益。尤其當幣價起伏大，對於一些堅定的持幣者來說，流動性挖礦就一種在不交易的情況下就能夠獲取收益、累積更多加密貨幣的方法。
11. ERC-20指的是以太坊區塊鏈上的一種智能合約協議標準。依據此格式建立新的ERC-20加密貨幣資產，將能自動支援ERC-20標準的錢包、借貸與交易所的服務，從而節省開發人員的開發時間。
12. 訂單簿是按照價格水平組織排列，展示特定資產買賣訂單的電子列表，傳統交易所交易之資產如股權、債券、貨幣，甚至包括比特幣等加密貨幣，通常都會以訂單簿的方式呈現。
13. AMM 是自動造市商 Auto Market Maker的縮寫，AMM讓傳統訂單簿交易轉變成交易池（ Liquidity Pool: LP ），所有想交易的人不需要有對手訂單就可以完成交易，大幅增加交易效率。
14. 造市者造市商（Market maker），是指在市場中提供流動性的人，一般是大型銀行或機構。如果沒有造市商，市場流動性可能會不足，交易也會受到影響。