臺東大學綠色科學學刊　2022，12(1)，pp.19-40

區塊鏈 NFT 發展與去中心化應用之研究

趙建雄*、楊雅如、王秉文、王榆晴

摘要

自中本聰之區塊鏈架構以來，帶來了去中心化構想之探討與發展。而自以太坊開創了區塊鏈智慧型合約以來，讓以太坊虛擬機 (Ethereum Virtual Machine, EVM)可將分散在全網的公共節點連接成一個虛擬機器來執行圖靈完備的程式，去中心化應用便逐漸落實發展起來。故當全世界受疫情影響普遍處於低迷之經濟活動之際，在虛擬世界裡卻非常活躍。NFT、DeFi、DApp、DAO、DEX 等之去中心化架構與應用等，屢創新的話題與應用。如 NFT 可將數位資產價值化，其唯一與不可替代的特性發展出不同類型的交易形式，如加密藝術品、音樂、遊戲等。事實上區塊鏈去中心化共識交易機制功不可沒，而其應用發展也潛力無窮。因此，本研究以 NFT 應用切入，再以其去中心化交易 DeFi，繼而探討去中心化組織 (DAO) 在各場景之應用，如永續發展目標 (SDGs) 、碳中和 (Carbon Neutrality) ，或將 NFT 用於慈善事業等，期能以正面之角度來探討區塊鏈技術所帶來之各種去中化應用以造福人群。

關鍵字：區塊鏈、非同質化代幣、智慧型合約、去中心化應用

趙建雄 (通訊作者)，國立高雄大學資訊管理系所教授。E-mail: cchao@nuk.edu.tw

楊雅如，國立陽明交通大學經營管理系所。E-mail: qj12qicy13@gmail.com

王秉文，國立高雄大學資訊管理系所。E-mail: a1073321@mail.nuk.edu.tw

王榆晴，國立高雄大學資訊管理系所。E-mail: a1083332@mail.nuk.edu.tw

The Study of Blockchain NFT Development and Decentralized Applications

Chian-Hsueng Chao* & Ya-Ju Yang & Bing-Wen Wang & Yu-Qing Wang

Abstract

Since the proposed of blockchain architecture by Satoshi Nakamoto, it has brought the discussion and development the concept of decentralization. Following the original blockchain architecture, the Ethereum pioneered blockchain smart contracts. The Ethereum Virtual Machine (EVM) can connect public nodes scattered throughout the network into a virtual machine to execute Turing-complete programs. Thereafter, the decentralized applications are gradually implemented and developed. Therefore, while the economic activity around the world was depressed due to the impact of the pandemic, it was very active in the virtual world. The decentralized architecture and applications of NFT, DeFi, DApp, DAO, DEX are innovative topics and applications. For example, NFT can value digital assets, and its unique and irreplaceable characteristics develop different types of transaction forms, such as crypto artwork, music, games and so on. In fact, the decentralized consensus transaction mechanism of the blockchain is very important, and its application has great potential. Therefore, this study starts with NFT applications, and then explores the application of decentralized organization (DAO) in various scenarios, such as sustainable development goals (SDGs), carbon neutrality (Carbon Neutrality), or using NFT for charity. It is hope to discuss various decentralization applications brought by blockchain technology from a positive perspective for the benefit of people.

Keywords: Blockchain, Non-Fungible Token, Smart Contract, Decentralized Applications

Chian-Hsueng Chao (Corresponding Author), Professor, Department of Information Management, National University of Kaohsiung. E-mail: cchao@nuk.edu.tw

Ya-Ju Yang, Student, Department of Institute of Business and Management, National Yang Ming Chiao Tung University. E-mail: qj12qicy13@gmail.com

Bing-Wen Wang, Student, Department of Information Management, National University of Kaohsiung. E-mail: a1073321@mail.nuk.edu.tw

Yu-Qing Wang, Student, Department of Information Management, National University of Kaohsiung. E-mail: a1083332@mail.nuk.edu.tw

壹、前言

2021 又被稱為 NFT 元年，在這一年的時間裡，NFT 一詞的使用率增長了 110,000%，躍升為當代最炙手可熱的話題之一。NFT 藉由區塊鏈的技術，憑藉其唯一性及不可分割性，明確的防偽操作及所有權歸屬使其在數位藝術及收藏品、遊戲內的物品、數位收藏卡、數位地產、活動票券等領域可被廣泛運用，而 NFT 交易中的特許使用權機制，讓賣家可以在賣出作品後，能夠持續獲得版稅收入，這樣的機制能夠更有利於創作者，並且若公益團體也能跟上這股 NFT 風潮，推出自己的 NFT，便能夠更大化其公益收入。而與 NFT 相關的去中心化金融 (DeFi)、分散式自治組織 (DAO) 也更加獲得大眾的關注，透明化的組織管理以及區塊鏈的電子化紀錄，這些機制同樣也適合運用在公益相關的議題。

雖然虛擬世界一系列的話題來勢洶洶，但在其蓬勃發展之餘，NFT 也因為去中心化的交易特性，且目前仍是無「法」可管的情況下，交易糾紛、詐騙等議題層出不窮，雖說目前已有智慧型合約進行制約，但在政府立法規範這個不受控的財富大門的規則之餘，首先需要了解這項新趨勢，目前 NFT 最令人詬病的問題，就是大量炒作導致的泡沫化問題，像是 Elon Musk 將 Twitter 頭像短暫的換成無聊猿 (Bored Ape Yacht Club)，導致 ApeCoin 的價格一度上漲，但隨後又因為他的一篇貼文「I dunno … seems kinda fungible.」，導致 ApeCoin 又暴跌，該貼文諷刺現今 NFT 市場尚未成熟，似乎具有可替代性，並深刻體現了因為詐騙事件和交易糾紛，所導致的 NFT 市場泡沫化的現況。

因此，本研究以 NFT 應用切入，分析和目前應用層面和討論其泡沫化問題，再以其去中心化交易之運作與利弊、智慧型合約法律地位等做分析與探討，繼而探討去中心化組織(DAO)在各場景之應用，如永續發展目標(SDGs)、碳中和(Carbon Neutrality)，或將 NFT 用於慈善事業等，期能以正面之角度來探討區塊鏈技術所帶來更為信賴而便利之各種去中化應用以造福人群。

貳、文獻探討

一、區塊鏈 (Blockchain)

區塊鏈技術起源 1997 年，Haber 和 Stornetta 為了設計一個不可被篡改的系統而提出了最早的加密安全鏈式區塊。當初鏈式區塊仍需要一個可信的協力廠商進行簽名，直到中本聰 (Satoshi Nakamoto) 於 2008 年發表了一篇名為《比特幣：一種對等式的電子現金系統》 ”Bitcoin: A Peer-to-Peer Electronic Cash System” 之論文，整合了密碼學、演算法、去中心化的分散式資料庫及經濟模型等，打造了比特幣區塊鏈系統。2009 年 1 月 3 日，中本聰在 Sourceforge 上發布了創世區塊 (Genesis Block)，而在其區塊中留言：“泰晤士報 03 / Jan / 2009 財政大臣計劃對銀行做第二波紓困”。人們認為他明示了金融系統的缺陷，以及他認為腐敗和不可靠的中間商，而選擇創造一種去中心化、更加以人為本的體系。從此比特幣 (Bit Coin) 因而聞名，也開創了今日各種去中心化應用。

依據中本聰「比特幣區塊鏈」對區塊鏈之定義，以時間戳 (Timestamp) 每十分鐘確認一次形成紀錄，而每十分鐘紀錄帳本為「區塊」，然後每個合法的區塊連成一個個鏈條，形成分散式、各方一致同意的帳本資料庫，此即是「區塊鏈」。因此區塊鏈有去中心化、分散式帳本、共識演算法、不易篡改、難造假之特點 (Antonopoulos, 2014) 。可在無須協力廠商介入或協助下可提供安全、不變的、透明化、有效紀錄交易及數據交換模式。另外，由於其共用之特性，若是私密資訊，則透過公開金鑰和私密金鑰加密，可對彼此對資訊進行解密，展現極高資訊透明度 (Grinberg, 2011)，類似於每筆交易皆能被紀錄及共用的一本電子式的記帳本。中本聰「比特幣區塊鏈」其架構如圖 1。

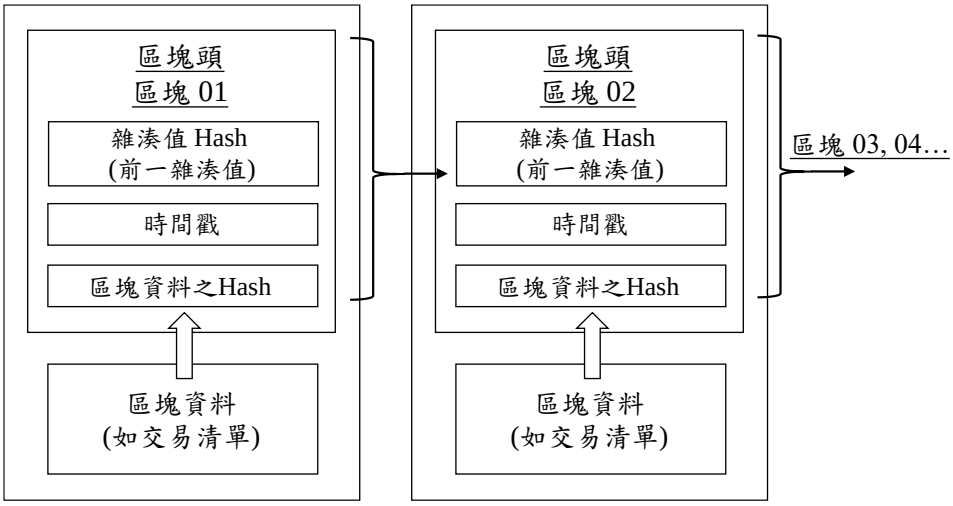

圖 1 區塊鏈基本架構

(一) 區塊鏈的鏈結：區塊鏈由一個個區塊組成的鏈，每區塊頭和區塊體 (含交易資料) 兩個部分。區塊頭含區塊的雜湊 (Hash) 值、時間戳 (Time stamp) 和用於計算挖礦的亂數 (Nonce) 。

(二) 共識機制：即所謂的挖礦機制，以分散式節點的計算力競爭來保證數據一致性、共識與安全性，此也是最為熟知的 Proof-of-Work (PoW) 共識機制。另外一種則為 Proof-of-Stake (PoS) 權益證明，採用權益證明來替代工作量證明。系統根據幣齡（節點佔有貨幣的數量與佔有時間之乘積）計算權益，最高權益而非最高算力的節點將獲得「記賬權」，此目的是減少大量運算所造成的資源消耗，較符合目前全球減碳(或碳中和)之目標。其他共識機制如實用拜占庭容錯 (Practical Byzantine Fault Tolerance, PBFT) 、容量證明 (Proof-of-space, PoSpace) 等。

(三) 區塊資料：可儲存資料之區塊本體，也就是所謂的帳本，含交易清單及內容。此分散式帳本機制結合後來以太坊開發之智慧型合約，造就了今日各種區塊鏈之創新應用。

二、以太坊 (Ethereum)

以太坊(Ethereum) 源自於在比特幣社群數年的 Vitalik Buterin 等，對比特幣和其區塊鏈技術有了自己的想法，即在原區塊鏈協議上加入了智慧型合約(Smart Contract)，又稱智能合約功能，並提出了一個名為 Ethereum 的去中心化平台，讓以太坊虛擬機(Ethereum Virtual Machine, EVM)可將分散在全鏈的公共節點連接成一個虛擬機器來執行圖靈完備的程式，允許不同的類型去中心化應用(DApp)智慧型合約的形式在區塊鏈上，如區塊鏈去中心化金融等。一旦智慧型合約部署在鏈上即會按著預先定義的規則去執行而無法篡改。圖靈完備的智慧型合約可以處理各種邏輯，且充分運用以太坊區塊鏈，使區塊鏈更具擴展性。這些想法變成了以太坊白皮書，2013 年 12 月以太坊登場，即後來所謂之區塊鏈 2.0 (如圖 2) 。

而以太幣(ETH)是以太坊之加密貨幣，為以太坊鏈上平台專屬的通行證，共識機制初期為 Proof-of-Work (PoW)，後來轉向 Proof-of-Stake (PoS)。其主要原因為 PoW 需要透過大量的電力作演算(即利用大量的顯示卡挖礦)達到共識和驗證，而 PoS 則以權益為主導，目的是減少大量運算所造成的資源消耗，較符合目前全球減碳(或碳中和)之目標。而若用戶想要在以太坊平台進行轉帳、交易、或者創建新的應用程式，只要使用以太坊的區塊鏈網路協定，使支付平台手續費，即可使用區塊鏈智慧型合約所衍生出的各種去中心化應用。

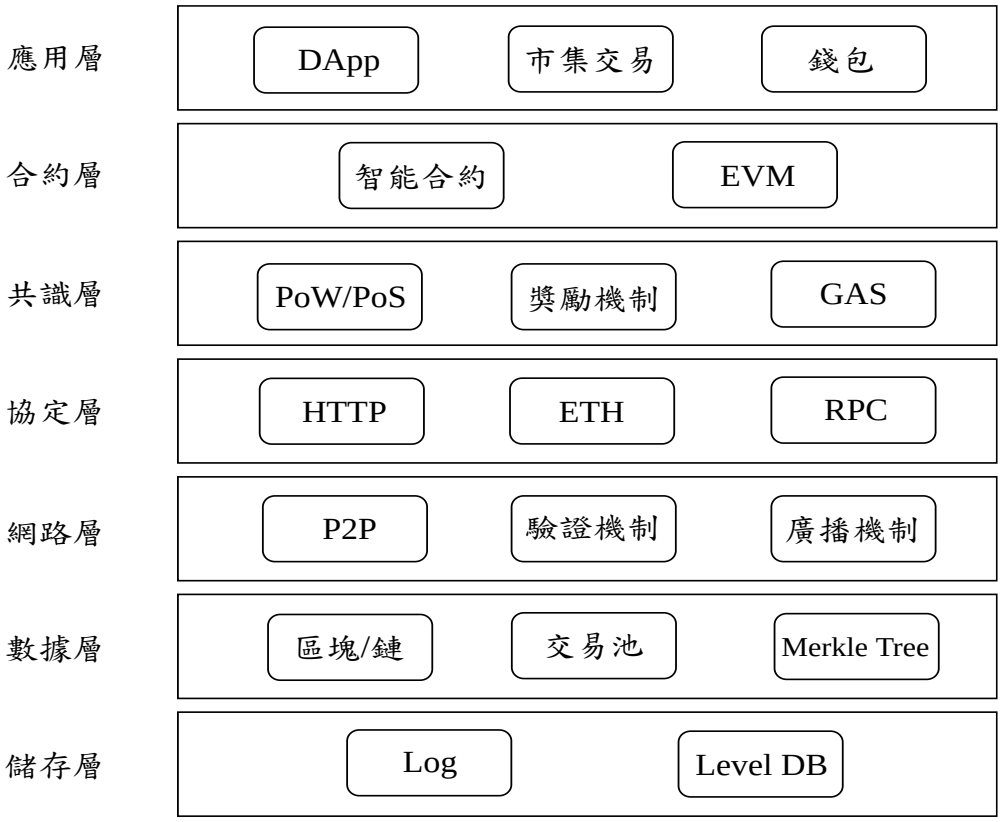

圖 2 以太坊基本架構

三、智慧型合約 (Smart Contract)

智慧型合約(Smart Contract)又稱智能合約。1997 年 Nick Szabo 提出了智能合約(Smart Contract)，又稱智能合約，希望創造一種由多個約定構建的合約，包括讓各方履行這些約定的協議，淘汰掉無生命的紙質合約。他認為，數位革命正在加速改變人與人之間的聯繫，並為利用這些聯繫形成新機構或應用服務提供了方法。或許當時因科技成熟度無法實現此架構，直到 Vitalik Buterin 為區塊鏈加入智能合約功能。如前所述，圖靈完備的智能合約可以處理各種邏輯，且充分運用以太坊區塊鏈，使區塊鏈更具擴展性。一旦智能合約部署在鏈上即會按著預先定義的規則去執行而無法篡改。因為智能合約內容公開，合約可以證明其真實性以及公平性。使得區塊鏈上節點在合約框架下進行交互行為，因此本身就視同具有法律屬性。交易雙方將彼此的協議條款直接寫入程式中，當滿足協議條件時，智慧型合約便會自動執行合約內容，內容中包含的代碼和協議，這些東西存在於分佈式、去中心化的區塊鏈網絡中，無需中央機構、法律系統或外部執行機制參與，且交易具有可追溯、透明化與不可逆轉的特性，開啟了今日各種去中心化的創新應用。

四、NFT (Non-Fungible Token, NFT)

NFT 為非同質化的代幣，與 NFT 相反的是同質化的代幣，比如比特幣這樣的虛擬代幣。首先解釋同質化和非同質化的概念，同質化 (Fungible)的概念像是 A 今天有 100 元，B 也有 100 元。兩人的 100 元可以互相兌換，因為兩人的價值是一樣的。而非同質化 (Non-Fungible) 的意思是 A 今天有 100 元，他的鈔票是特殊的，像是特殊的數字編號，或有名人的簽名等，那麼 A 的 100 元鈔票就可能不只價值 100 元，兩者的詳細比較如表 1。

表 1 同質化和非同質化的比較

	同質化	非同質化
替代性	可替代性，每個加密貨幣的價值一樣、作用一樣。	不可替代性，每一個 NFT 都是獨一無二，彼此不等值，也不會被其他 NFT 取代。
分割性	可以被分割，1 個可以分個成 10 個 0.1 等。	不可分割，不能切分成更小的單位進行交易。
一致性	因為發展技術困難，所以具有價值性、信任度和可靠性。	用以界定虛擬物品的原始所有權、稀缺性和防偽性，是屬於可流通的數位收藏品。

(一) NFT 之歷史

2021 年被稱為 NFT 元年，有關 NFT 的概念被大眾所熟知，連 Google 的熱搜關鍵字中也有與 NFT 有關的議題。雖然 NFT 的概念是在 2017 年才正式提出，但相關概念在很久之前就出現了，以下簡介 NFT 之歷史與發展過程。

1.種子期(1993-2017)：NFT 概念最早來自於 Finney (1993)，提出加密交易卡 (Crypto Trading Cards)，並且在 2012 年出現與加密交易卡類似概念的彩色幣 (Colored Coin)，這為 NFT 奠定了基礎。真正推動 NFT 概念的是 2014 年創立的 Counterparty，在 Counterparty 上創建的 Rare Pepes 將熱門 meme 悲傷蛙做成 NFT 應用。

2.萌芽期(2017)：2017 年 6 月，世界上第一個 NFT 項目 Crypto Punks 在以太鏈上發布，它啟發了 ERC721 協議，透過改造 ERC20 協議發行代幣，將圖像變為加密資產，帶入加密貨幣的領域。同年 10 月，Crypto Kitties 的加密遊戲，將每一隻加密貓都呈現的獨一無二，讓這款遊戲迅速走紅，也將 NFT 推向高潮。

3.建設期(2018-2020)：經過萌芽期的發展，NFT 的生態大規模增長，許多相關平台也在同時間出現。像是交易平台 Opensea、SuperRare、Known Origin、Makers Place 和 Rare Art Labs。另外也有可以讓一般大眾創建自己 NFT 的平台 Mintbase 和 Mintable。在眾多平台的引領下，NFT 的交易更加便利及完善，也讓 NFT 的應用領域從遊戲，慢慢轉往藝術品、音樂等其他多媒體項目，並與 DeFi 結合，實現 GameFi，推動 NFT 的發展。

4.快速擴張期(2021)：有一位數字藝術家從 2007 年每天作圖一張，最終把 5000 張圖片拼接成一張圖，並命名 Everydays : The first 5000 days，並作為 NFT 出售，最終以 6934 萬美元賣出，這使更多人注意到 NFT 這塊市場。另外，有一款區塊鏈遊戲 Axie Infinity 銷量迅速上漲，帶動整個 NFT 市場快速發展。同年 10 月，Facebook 確定更名為 Meta，也讓 Metaverse、NFT 的話題帶進大眾的生活裡。

NFT 中使用的最重要的技術是區塊鏈，NFT 是按照以太坊 ERC721 標準發行的代幣，具有不可分割性、不可替代性和唯一性。它可以用來驗證所有權和真實性，是完全虛擬化資產的代表，和真實資產通證化的代表。在 NFT 中會有一個發行人的角色，發行人會通過一些區塊鏈平台來創建自己的產品。比如美國藝術家 Beeple，他的作品需要通過拍賣商佳士得與區塊鏈合作創作，然後在交易確認後，平台會發出智慧型合約，其中記錄了藝術作品是獨一無二的區塊鏈，而區塊鏈中的每個節點都會記錄這些訊息，使得記錄難以被竄改。

另一方面，使用區塊鏈技術的智慧型合約也發揮著非常重要的作用。在傳統藝術品交易中，藝術家將作品售出後，後續的買主若要將作品轉售或進行其他加工，與藝術家無關。但是，可以自動執行的智慧型合約可以繼續創造中間價值和

利益分配。例如，發行人與第一個買方進行交易時，可能會與發行人簽訂 10%的特許權使用費，而當買方進行轉售交易時，發行人可以在後續交易中獲得該用費，這意味著智慧型合約為創作帶來新的價值，創作者可以獲得持續的版稅收入，而不是一次性的交易收入。

(二) NFT 之種類

NFT 有許多種類，若以區塊鏈的性質來分可以分為公有鏈、私有鏈和聯盟鏈。

1.公有鏈 (Public Blockchain) 是三種區塊鏈中，去中心化程度最高的。公有鏈對世界上所有人都是開放的，任何人都能夠讀取資料或是發送交易，並能獲得有效地確認，且任何人都可以參加區塊鏈的共識過程。公有鏈的優點有很多，像是程式開發者無法干預使用者，且公有的特性讓訪問區塊鏈的門檻很低，只要有辦法連上網路就能夠訪問區塊鏈，目前使用公有鏈的應用有像是比特幣、以太幣、超級帳本等，最一開始使用公有鏈的應用是比特幣，比特幣會給使用者一些預設的操作，像是交易；但以太坊可以讓使用者編寫程式，以實現符合需求的複雜操作。

2.私有鏈 (Private Blockchain) 是指只有某些人、組織或機構，能夠獲得其寫入的權限，所有的操作都會被加以限制，不對外開放也不能隨意讀取。私有鏈的特性是其交易速度快，因為其私有入門限制的關係，以至於只需要少量的節點數據就有很高的信任度，另外讀取限制也很好的保護鏈上資料的隱私。私有鏈的交易成本較公有鏈低，因為公有鏈的交易需要依賴較多的節點協議，而私有鏈只需要少量節點就能完成交易認證，現今銀行等金融機構較能夠接受私有鏈，得益於其有助於產品保護。

3.聯盟鏈 (Consortium Blockchain) 介於公有與私有鏈之間，不像私有鏈這麼封閉，進入聯盟鏈需要先進行註冊獲得許可，聯盟鏈中的讀取、參與、記帳權限、規則由聯盟自行訂製，共識機制則由預先選定的節點控制。通常聯盟鏈多應用在組織與組織之間的交易、清算等，以銀行業為例，銀行要對其他銀行進行支付、結算等作業時，以其他銀行作為聯盟鏈上的節點，當超過一定比例的節點認證這個區塊，該紀錄便會的到全網的認證，由於聯盟鏈需要註冊的特性，所以其安全和性能也較公有鏈高。

為什麼 NFT 能在虛擬世界獲得如此高的聲望呢? NFT 的特性在人性的掌握上有著不可抹滅的影響，NFT 洞悉人類的收藏心理，對於收藏稀缺性事物的追求，其次是掌握了見好的投資心理、利用商機的投機心理、商品給予的情感連結、害怕錯失的恐懼、見獵心喜等。在掌握人類的心理後，人們開始會思考 NFT 的實用性或是為擁有者創造的獨特性，NFT 被賦予其他的價值也就成為真正誘發想擁有或收藏的商機，像是以無聊猿俱樂部 (Bored Ape Yacht Club) 為例，創造者打造了一萬個無聊猿 NFT 做為俱樂部入場的會員卡，創造者打造專屬於擁有者的數位環境，提供獨特的體驗讓擁有者感受到權利及實用性，給予擁有者不同的體驗。

五、去中心化金融 (Decentralized Finance, DeFi)

DeFi 是繼智能合約後帶來之創新去中心化金融應用，即所有 DeFi 協議和應用程式的支柱是運作在區塊鏈網路虛擬機上，其於 2021 NFT 元年之前，DeFi 即在虛擬世界擴展應用了。去中心化金融 (DeFi)，一種點對點金融模式，它利用基於區塊鏈的智能合約來確保其完整性和安全性 (Gudgeon et al., 2020)。有別於一般銀行之金融服務，DeFi 是靠開源軟體和不可審查的網絡構建的，是以數位貨幣或者代幣 (Token) 進行的金融行為和服務。其構建了透明化、開放式的金融系統，DeFi 對任何人都開放，使全球各地的人們能夠以點對點的方式參與金融活動。而隨著 DeFi 之發展，幾乎複製了現代金融體系，加快了加密貨幣市場規模的擴張與現實世界金融體系之連動，而其去中心化，人們也擁有了不受任何國家政府控制，超越主權貨幣之金融體系。

DeFi 涉及的內容很寬泛，包括貨幣發行、理財、交易、借貸，和交易所服務(DEX)等，幾乎複製了現代金融體系，也因此被稱為「DeFi 樂高」。DeFi 產品本質上是透明的，對任何能夠連接到互聯網的人都開放，並使全球各地的人們能夠以點對點的方式參與金融活動。另外與傳統銀行不同者，DeFi 通常使用智能合約免去了傳統金融體系所涉及之煩瑣流程和其相對應之成本，這些協議能自由組合來複製實際金融活動，其由下而上之結構分述如下(表 2) 。

(一) 結算層(Settlement Layer)：此為 DeFi 協議之最底層或稱為第 0 層 (Layer 0)，由區塊鏈及其原生協議組成，如比特幣區塊鏈上的比特幣 (BTC) 和以太坊區塊鏈上的 (ETH)。它允許網絡安全地存儲所有權資訊，並確保任何狀態更改都遵守其規則組合。結算層可以將擁有的資產或不動產代幣化，如房地產代幣即代表某塊土地的所有權。

(二) 資產層(Asset Layer)：由在結算層之上發行的所有資產組成。這包括原生協議資產以及在該區塊鏈上發行的任何附加資產 (通常稱為代幣)。

(三) 協議層 (Protocol Layer)：為去中心化交易所、債務市場、衍生品和鏈上資產管理等特定用例提供標準。這些標準通常作為一組智能合約，任何用戶(或 DeFi 應用程式) 都可以互相交流，即可以有多個應用實務同時使用它來建構服務或應用程式，此層為 DeFi 提供了靈活和高度的互操作性。

(四) 應用層(Application Layer)：應用層創建連接到各個協議需求的用戶之應用程序，是向消費者提供服務的地方，如借貸或加密貨幣之交換等。

(五) 聚合層(Aggregation Layer)：此層是應用層的擴展，由聚合器創建連接到多個應用程式和協議以用戶為中心的平台。允許用戶通過同時連接到多個協議來執行其他復雜的任務，銀行服務或加密錢包也是聚合層中常見的例子。

表 2 DeFi 協議與服務

DeFi 堆疊	服 務
聚合層(Aggregation Layer)	一般銀行服務或加密錢包。
應用層(Application Layer)	借貸或加密貨幣之交易。
資產層(Asset Layer)	結算層之上發行之所有資產組成。
協議層(Protocol Layer)	去中心化交易所、債務市場、衍生品和鏈上資產管理等。
結算層(Settlement Layer)	區塊鏈及其協議，可將資產或不動產代幣化

依其 DeFi 發展脈絡，最初只有去中心化穩定幣(如 MakerDAO)，之後才開始進行構建更具規模的金融體系，去中心化交易協議也因此產生。去中心化交易協議，即人們常說的 DEX (去中心化交易所)，是以智能合約為技術在區塊鏈上構建的一種去中心化虛擬資產交易平台，交易雙方可以任意價值型式，如資產間或與各種虛擬貨幣間，類似於真實世界資貨幣與資產交易活動。

價格預言機(Price Oracles)在 DeFi 中是一個非常重要的組成部分。預言機是鏈下(即現實世界) 服務和鏈上(區塊鏈)協議之間的橋樑。預言機可檢索鏈下數據，將這些數據發佈在 DeFi 中，預言機的主要用途與借貸協議有關。隨著區塊鏈 DeFi 之發展和應用越來越多，其金融仿真性與其去中心匿名性在政策監管方面，勢必帶來更大之挑戰。因 DeFi、DEX 等為基於區塊鏈之技術，所以目前以區塊鏈監理切入居多，即以鏈治鏈之構想。

與 DeFi 相對應用之 DEX(Decentralized Exchange)交易平台或稱去中心化交易所，為建立在區塊鏈網絡上一種去中心化自治應用程式(DApp)。一般而言，使用 DEX 只需要一個公鑰，自己的私鑰，不再需要集中的資產託管，解決了中心化的信任問題和安全問題。DEX 於 2020 年引入自動化做市商(AMM)模式後整體營運效率得到有效改善。未來隨著 DeFi 發展，DEX 應用也更加多元化。

六、 星際檔案系統 (InterPlanetary File System, IPFS)

星際檔案系統 (InterPlanetary File System, IPFS) 自 Juan Benet 於 2015 年發布以來，其設計宗旨是與區塊鏈結合協同運作。IPFS 的發展初衷其實是對 HTTP 協議的擴展，希望為互聯網數據提供去中心化的存儲和尋址方案。IPFS 去中心化網絡將「地址定址」改為「內容定址」，即不用指定電腦去哪找資料，只需要告知想要什麼資料即可。IPFS 上的檔案都儲存在 IPFS 物件中，每個物件最多可以儲存 256KB 之資料，也可含其它 IPFS 網絡之物件連結。因此，IPFS 是一個建立持久且分散式儲存和共用檔案的網路傳輸協議，為一種 P2P 式內容可尋址的對等超媒體分發協議，IPFS 網路中的節點構成一個去中心化的檔案系統。IPFS 協議上的資料可永久保存在網路上，不再因斷線而消失或被刪除。如早期很多去中心化儲存協議仍像是獨立的體系，缺乏與以太坊等公鏈之結合與連動。由於過去並未做好這方面的銜接工作，很多 NET 項目並未全面採用去中心化存儲的方式。作為一位 NFT 擁有者，可以提供自己資產中的 Hash 值

和原版作品圖片，社群成員便會對該圖片進行 Hash 值提取，如果你資產中的 Hash 值一致，則可認定該作品之原創與歸屬。然而，若互聯網伺服器出現問題，就無法向社區提供這種驗證了。另外由於是分佈式網絡，可以有效防止駭客對中心化伺服器的攻擊。目前以 IPFS 協議之網路節點成長快速，包含 Google、以太坊基金主網均開始轉向 IPFS，並且 IPFS 網絡無中央伺服器控管，沒有中間商抽成。

七、去中心化組織 (Decentralized Autonomous Organization, DAO)

以太坊之智能合約開啟了各種區塊鏈之創新，顛覆了許多傳統之商務應用，除了在其金融方面之 DeFi，在組織的設計運作上則為去中心化應用 DAO。早期 DAO 使用以太坊區塊鏈，使用以太幣作為加密貨幣來執行合約。而用於驗證以太坊網絡中交易的計算能力是使用以太加密貨幣支付的。如今，智能合約部署在眾多區塊鏈上建立了各種 DAO 的規則。基本上，DAO 將組織規則與運作邏輯寫入程式碼中，之後由智能合約自動執行組織的決策和提案。DAO 的支柱是其智能合約，合約定義了組織的規則並持有集團的資金。一旦合約生效，除非通過投票，否則任何人都無法更改規則。在 DAO 中最關鍵之環節為需要所有利益關係人投票決定是否執行，這裡的投票特指持有相關加密貨幣的投資者通過質押一定的通證(Token)以獲得無法複製的投票權，而未持有者則沒有行使投票決策的權利。通證是 DAO 實行治理功能所依賴的最重要的激勵手段，所有參與者都為了獲取激勵或者讓資產升值而不遺餘力地貢獻自己的力量。DAO 其實是建立在經濟效益的基礎上，每次 DAO 提案的決策和執行，都是一次經濟上的大協作，所有加密資產利益人為社區做出積極貢獻，也是在為自己持有的資產帶來價值回饋。目前有金融協議 DAO (如 MakerDAO 和 Uniswap)、NFT 構建 DAO (如 Loot) 、媒體與社交 DAO (如 Bankless)，不同人群在不同 DAO 中都尋得其分工，比如在 Loot DAO 中，人們需要發揮自己的藝術創造力和想像力，去建設豐富之內容。投入越多，獲得的回報就越大，這是 DAO 薪酬體系最具保障的公平準則。DAO 治理模型及其治理結構旨在去除過去中央集權管理之階層式組織架構(去中心化治理)，使其更民主化、扁平化方式治理。同時促進透明度、問責制和自治，同時保護隱私、公平和非歧視。通常，DAO 可分三個主要步驟進行創建：

(一) 智能合約創建：首先，開發人員或一組開發人員必須創建 DAO 背後的智能合約。啟動後，他們只能通過治理系統更改這些合約設定的規則。這意味著他們必須對合約進行廣泛的測試，以確保他們不會忽略重要的細節。

(二) 資金：創建智慧型合約後，DAO 需要確定獲得資金的方式以及如何實施治理。通常，代幣被出售以籌集資金；這些代幣賦予持有者投票權。

(三) 部署：一切就緒後，DAO 需要部署在區塊鏈上。從此時起，利益相關者將決定組織的未來。該組織的創建者—那些編寫智慧型合約的人—不再像其他利益相關者那樣影響項目。

參、分析與研究

一、去中心化應用

在區塊鏈中，去中心化是指將控制和決策，從集中的實體(個人、組織或團體)轉移到分佈式網路。去中心化網路讓參與者信任彼此，並降低參與者對彼此施加權力或控制的能力。在構建解決方案時，通常會考慮三種主要的網路架構：集中式、分佈式和分散式。雖然區塊鏈技術通常使用去中心化網路，但區塊鏈應用程序本身不能簡單地歸類為去中心化或非去中心化；相反，去中心化是一個滑動規模，應該應用於區塊鏈應用程序的所有方面，通過分散管理和訪問應用程序中的資源，可以實現更大、更公平的服務。去中心化通常會有一些權衡，例如較低的交易進出量，但理想情況下，這些權衡值得他們提高穩定性和服務水平。

去中心化的其中一個實際應用就是星際檔案系統， IPFS 網絡可以與區塊鏈完美結合，區塊鏈的本質是分佈式帳本，其瓶頸之一就是帳本的儲存能力，目前大部分公有鏈的最大問題是沒法存儲大量的超媒體數據在自己的鏈上，而 IPFS 網絡可解決此問題。相比 HTTP 網路， IPFS 網絡具有以下優勢：(1) 檔案傳輸速度快，數據儲存安全性高。(2) 避免過度依賴骨幹網路，造成網絡擁堵，降低頻寬需求與儲存成本。(3) 是 IPFS 與區塊鏈機制類似，區塊鏈的本質是分佈式帳本，二者可完美結合。特別是大部分公鏈有儲存大量或巨量資料問題，採用 IPFS 技術能夠在一定程度上很好決儲存瓶頸問題。

二、NFT 的權力轉移方式

NFT 的權力轉移方式，主要依靠去中心化機制，以轉帳機制為例，在一般銀行作業，若需要跨行轉帳，就需要收取額外的手續費；而就加密貨幣而言，也是需要收取手續費，但在區塊鏈中這筆費用被稱為礦工費，之所以需要收費，是因為記帳驗證交易的真實性時所產生的費用。由於區塊鏈的特性，所以交易不會受到監管機構的知曉與阻撓，因為驗證者並不會知道現在匯款的人是誰，也不會知道這筆錢要轉到哪個地址，所以也不知道是誰收到這筆錢，這導致交易所的監管越來越嚴格。因此 NFT 訂定了幾個主要的以太坊協議。

(一) ERC20：是由 Vogelsteller (2015) 提出，用於以太坊區塊鏈上的所有智慧型合約，以實現代幣並提供所有基於以太坊帶必須遵守的規則列表，ERC20 引入了 FT 的標準，換句話說，他讓每個 token 與其他相同類型和幣值的 token ，具有相同的屬性，確保不同代幣之間的兼容性。

(二) ERC721：是以太坊 NFT 的第一個標準協議，也是 NFT 最常見的底層協議，ERC721 與 ERC20 不同的地方，在於 ERC721 代幣是不可代替的，也就是所有的 token 都是獨一無二的，因此不可以互換。換句話說，它要求一份合約只能發行一種 NFT 資產，像是 BAYC 無聊猿。而 ERC721 的首次應用是 Crypto Kitties，遊戲中的每隻小貓在市場上的價值都不同，因為這些貓咪中的參數都有些微差異，這導致其具有唯一性和價值。

(三) ERC998：ERC998 是 ERC721 標準的擴展，增加了非同質代幣擁有其他非同質代幣和 ERC20 代幣的能力，並且代幣中包含的所有資產都可以同時交易，常用於投資組合管理、虛擬替身和遊戲中。

(四) ERC1155：與 ERC721 不同的地方是，一份合約發行多類 NFT，常用於遊戲上，像是交易平台 OpenSea 的代幣 OpenStore，一種 NFT 資產又可以映射出多個 NFT，BAYC 項目發行的總數便有 10,000 個。

三、NFT 的儲存現況

目前 NFT 有許多項目都採用鏈下儲存的方式，其中包括了中心化儲存、中心化可驗證、去中心化儲存和去中心化可修復等方式。

(一) 中心化儲存：中心化儲存是指將 NFT 的詮釋資料(Metadata)存放中心化伺服器上，可當伺服器停止服務時，NFT 的詮釋資料將永遠消失，並且中心化的概念也違背了 NFT 的初衷，所以目前很多 NFT 的項目很多也都在探索階段，所以對於鏈下數據儲存的安全性並沒有特別重視。一般 NFT 項目使用智慧型合約中的特定標識符來返回資料，像是圖片或影片，他們通常會使用由公司運行或者亞馬遜等雲服務商提供的伺服器上的 URL 來做為辨識，這種方式可能發生竄改、中斷服務等問題。

(二) 中心化可驗證：中心化可驗證是指將產品儲存在中心化的伺服器中，再把產品的加密貨幣 Hash 值儲存在智慧型合約中。這樣就能透過 Hash 值對產品進行驗證，確保其不可變動性。但是主要的媒體數據還是存在中心化的伺服器中，所以還是可能存在數據遺失、拒絕服務等問題。

(三) 去中心化儲存：星際檔案系統 IPFS (Inter Planetary File System) (Benet, 2014) 是目前去中心化儲存的代表項目，當下載文件時，可以通過多個節點同時下載，相較於傳統的中心化網際網路服務的速度要快很多，像是迅雷、BitTorrent 等，都是透過點對點(P2P)下載。由於 IPFS 是用於協助區塊鏈技術，可以透過 Filecoin 來鼓勵礦工分享硬碟空間，讓儲存空間變得更便宜，另外 IPFS 還能夠抵擋 DDos 攻擊，當中心化伺服器遇到 DDos 攻擊時，大量的封包會導式伺服器癱瘓，而 IPFS 由於所有的連結會被分配到不同的節點，所以幾乎不受 DDos 攻擊影響。雖然 IPFS 的出現改善了詮釋資料和媒體數據的儲存方式，但是做為一個定址系統，它還是不能提供足夠安全可靠的儲存服務。因為 IPFS 的網路節點對內容的備份是自驅動的，所以如果只有少數節點備份相應內容，這些節點卻因為某些原因損壞或下線，就會發生節點斷線的問題，導致找不到數據的問題。

(四) 去中心化可修復：有望成為 NFT 儲存的未來解決方案，目的在讓 NFT 元資料和媒體資料的儲存與所有權的儲存更加匹配。現有的儲存項目有 NFT.Storage、Metastorage.org 。NFT.Storage 透過協助 IPFS 和 Filecoin 的

彈性儲存和持久性，維持數據的長期可訪問性和儲存，目前單個儲存數據容量限制在 100MB 以內；Metastorage.org 是基於 MEMO 分散式儲存系統開發的項目，並採用了雙儲存系統的運行模式，把 NFT 在 IPFS 和 MEFS 中進行雙份儲存，其中 MEFS 對儲存數據量沒有限制。

四、NFT 智慧型合約

NFT 智慧型合約會記錄每個 NFT 資產的 Token ID、作品資訊、資源儲存位址等資訊並存放在區塊鏈上。但基於成本的考量，其映射的實物資產或數位資產一般不會上鏈，而是存在其他中心化或非中心化的儲存系統中。像是透過 NFT 中的 URI (Uniform Resource Identifier)來指向 NFT 作品的儲存位置，或者是去中心化儲存的星際檔案系統 (IPFS)、去中心化儲存協議 (例如：Arweave 和 Filecoin)，又或是中心化儲存服務 (例如：Amazon Web Services)，儲存的位置取決於 NFT 項目決定要將作品圖像保存在哪，讓 NFT 隨時可以被呼叫展示出來。但也有一些 NFT 作品是直接存在區塊鏈上的，那就是生成藝術 (Generative Art)。生成藝術描述的是一個系統經歷了一個生成過程的藝術作品，而生成藝術能夠透過演算法和智慧型合約就將 NFT 作品呈現，而不會受到儲存管道的限制。

五、現有問題

(一) NFT 泡沫化問題

而 NFT 存在著泡沫化的風險嗎?這一直都是個炙手可熱的議題。"Non-fungible tokens and the future of art"的作者 Kuglar (2021)提出雖然 NFT 可以在區塊鏈上實現數字藝術所有權，但數字藝術本身並沒有改變。看實物畫的印刷品與看原作的體驗是不同的。這就是為什麼幾乎每個人都曾在某個時候看到過蒙娜麗莎的複製品，但仍有數百萬人親自前往參觀。隨著 NFT 的熱度上升，許多購買者認為購買 NFT 屬於一種數位投資，但比起數位投資，更像是購買周邊商品，購買者無法去防範同一個創作者創造額外的複製品進行重複上架，而氾濫的複製品也使其失去了稀缺性的特性，造成商品貶值、失去市場價值。而目前市面上也有許多遊戲相關的 NFT 正逐漸泡沫化，值得慶幸的是藝術類、工具類的 NFT 依舊穩固，反推 ICO (Initial Coin Offering，又稱首次貨幣發行) 除了技術的加密貨幣依舊擁有市場，其餘皆曇花一現，泡沫化的風險堪稱是極高。NFT 存在著一定高機率的泡沫化風險，若能選對 NFT 的領域並遠觀其市場價值，且在有餘力時進行投資，了解投資 NFT 需在能力所及的範圍，才有購買 NFT 的意義。

另外，人們也應該去思考是否有別的方式能夠增加 NFT 的價值，像是 RAW 主廚江振誠(2022)就結合料理、VR、行為藝術，辦了一個 "We Are What We Eat : Seed"的展覽，並且為這個展發行 512 個 seed 圖像 NFT，只要有購買這個 NFT 的人，就可以到 RAW 親自體驗這場融合了 VR、表演藝術、頂級餐飲的展覽。類似江振誠主廚的例子越來越多，也說明了人們開始為 NFT 找到不同的方向，期望有

越來越多令人耳目一新的案例，讓大眾談到 NFT 時，不再是聯想到泡沫化的問題，而是一個嶄新的科技產物。

(二) 去中心化共識交易之運作與利弊

去中心化有許多的好處，它可以提供不依賴信任的環境，在區塊鏈網路中，沒有人必須知道其他任何人，網路中的每個成員都以分佈式帳本的形式擁有完全相同的數據副本。如果成員的帳本以任何方式被更改或損壞，它將被網路中的大多數成員拒絕。公司經常與合作夥伴交換數據，反過來，這些數據通常會被轉換並儲存在各方的數據孤島中，只有在需要向下游傳遞時才會重新浮出水面。每次轉換數據時，都會導致數據丟失或錯誤數據進入工作流。通過擁有去中心化的數據儲存，每個實體都可以訪問實時、共享的數據。

因此也衍伸出去中心化金融 (Decentralized Finance, DeFi) ，因為以往的傳統金融多是中心化的，需要經過仲介機構像是銀行、保險業者、證券交易所的參與，而且需要進行身分認證，才能進行買賣交易。而 DeFi 運用了區塊鏈的技術，可以省去中介機構收取的手續費和身分認證。透過 DeFi 讓交易雙方可以直接進行點對點的活動，也不會被仲介機構所設立的分級制度影響(表 3)。

表 3 去中心化金融和傳統金融之比較

	去中心化金融 (DeFi)	**傳統金融**
運行方式	在區塊鏈上，以點對點、不受中心化組織管控的金融體系。	多是中心化的仲介機構，如銀行、保險業者或證券交易所的參與。
貸款申請、撥款速度	因為是以區塊鏈技術進行身分認證，所以可以快速地進行身分驗證，且不會進行信用評級，撥款速度快。	需要經過多重的身分驗證、信用評級等，才能決定是否符合貸款申請條件，撥款速度慢。

目前 NFT 的共識機制大多是採用工作量證明以及權益證明，而以以太坊為基礎的 NFT 更多的是使用 PoS，兩種的共識機制各有優缺，工作量證明 (Proof of Work, PoW)是透工作量來進行虛擬貨幣的分帳，工作也就是所謂的挖礦，挖礦是礦工使用電腦 CPU、電力和時間來運算，PoW 的優點是不需要中心化的監管機構，可以達到公平競爭的機制，但缺點是 PoW 靠電腦運算，需要消耗大量電能，且挖礦的設備昂貴，最終可能導致集中化的現象；權益證明 (Proof of Stake, PoS) 是為了解決 PoW 耗費大量能源問題，所提出的替代方案，PoS 透過買加密貨幣，看誰抵押在智慧型合約的貨幣量，和抵押的時間越長，誰取得記帳權的機率就越高，PoS 的優點是不需要自己購買昂貴的挖礦設備，但缺點是 PoS 機制會鼓勵大家購買大量加密貨幣，可能會使有錢人囤積加密貨幣，導致富者恆富的情況發生。

前面有所提及去中心化的運作模式及好處，包含可提供不依賴信任的環境，使資訊存在獨立性也可降低資訊被任何方式更改或損壞時所造成的風險，提高使用者的保障。但去中心化共識交易也有它的隱患，例如：沒有可申訴的管道，由於去中心化的運作理念，交易皆是獨立進行，若在其中出現問題，是沒有中間的客服人員可以聯絡。所以在交易進行中，若使用加密貨幣進行購物，賣家沒有給予商品。或是將加密貨幣 (包含 NFT) 轉出去的當下就無法收回，除非接收者自願歸還。所以在去中心化的交易過程中誠信是最重要的；個人責任的重要性，在去中心化的狀態下，所有使用者在區塊鏈上的行為及結果都需自行負責，個人對於配合買賣的使用者、保護錢包私鑰並留意加密貨幣和 NFT 的安全，防範不勝可數的騙局。詐騙也有多種形式，例如：冒牌的交易網站、App 及管理員、詐騙郵件、潛在駭客、潛在攻擊、廢幣(被遺棄的區塊鏈，可能是沒有足夠的資源處理交易或是就是一場騙局)、價格波動(抽銷陰謀，一群人合購某個貨幣或代幣，利用人性的錯失恐懼使價格上漲，再以他們預定的價格出售牟利，使他人成為被收割的韭菜)等。

(三) 智慧型合約的法律地位

智慧型合約的技術雖然帶來許多的便利性，但是同樣有需多隱患，在傳統的合約簽訂時，通常會先請律師檢視合約中的條款，而智慧型合約中，是透過使用者告訴開發人員需求，開發人員再根據需求設計智慧型合約，但若中間的資訊傳遞有誤，可能會導致智慧型合約不符合預期。

另外，以 The DAO 公司為例，早在公司還在募資階段時，就有專家警告該專案存在著安全漏洞，但卻未得到重視，以至於公司剛上市沒多久，就被駭客偷走 360 萬個以太幣，為了補上這個缺口，以太坊社群最終決定使用硬分叉，將 The DAO 的區塊鏈恢復到被攻擊前的狀態，當碰到上述的狀況時，受害者該如何依法求償，法律上是否有相關的法規能夠約束，像是在美國，智慧型合約並不被視為完整合約，只能算是有效合約的一部份，要想具備法律效力，就需要再搭配一份傳統合約；而在英國，英國法律委員會在 2019 公告了在英國，智慧型合約和一般合約一樣具有法律效力；但在台灣，目前仍沒有相關法規，來說明智慧型合約在法律上的地位，也就是說，當走法律訴訟程序時，智慧型合約並不具備強制性，隨著現在智慧型合約的增加，政府應該依據現況，適當地針對智慧型合約的標準或是法律效力，進行相關法規的研究或是修改。

(四) NFT 與公益事業結合

在 NFT 中會有一個發行人的角色，發行人會通過一些區塊鏈平臺來創建自己的產品。比如上面提到過的美國藝術家 Beeple，他的作品需要通過拍賣商佳士得與區塊鏈合作創作，然後在交易確認後，平臺會發出智慧型合約，其中記錄了藝術作品是一個獨一無二的區塊鏈，而區塊鏈中的每個節點都會記錄這些資訊，使得記錄難以被篡改。

而使用區塊鏈技術的智慧型合約也發揮著非常重要的作用，在傳統藝術品交易中，作者將作品售出後，後續的買主不論是將作品轉售或進行其他加工，都與原作者無關。但可以自動執行的智慧型合約可以繼續創造中間價值和利益分配。例如發行人與第一個買方進行交易時，若與發行人簽訂 10% 的特許權使用費，而當買方進行轉售交易時，發行人可以在後續交易中獲得 10% 的特許權使用費，這意味著智慧型合約為創作帶來新的價值，創作者可以獲得持續的版稅收入，而不是一次性的交易收入，而現今 NFT 的炒作若是能夠運用在公益事業，公益團體可以透過發行自己的 NFT 作品，讓想要做公益的人一起競標 NFT 作品，而公益團體除了競標收入之外，還可以透過簽訂特許使用費，持續獲得作品的版稅，比起傳統的藝術品交易，能夠更大化藝術品的價值。

(五) SDGs、ESG 和碳中和

SDGs (Sustainable Development Goals)是聯合國於 2016 年提出，以接替 MDGs (Millennium Development Goals)的一系列未來要實現的目標，這些目標包括廣泛的社會問題（貧困、疾病、教育、婦女、兒童、難民、糾紛等）、環境問題和氣候變化（氣候變化、能源、環境污染、水、生物多樣性等）、經濟問題（技術、住房、工作條件、勞動力、就業、生產和消費、社會結構、法律、基礎設施建設、國內外經濟）。SDGs 是國際社會最大的共同目標，旨在通過實施 17 個目標和 169 個具體目標來解決這些問題，直到 2030 年。

ESG (Environmental, Social, Governance)是一種公司對於社會目標貢獻程度的評估方法，這些目標超越了公司的角色，以代表公司股東實現利潤最大化。通常，從 ESG 角度倡導的社會目標包括努力實現一組特定的環境目標，以及與支持某些社會運動有關的一組目標，以及與公司是否以與多元化、公平和包容運動的目標相一致的方式進行管理。各種政府組織和金融機構已經設計了衡量特定公司與 ESG 目標一致程度的方法。在這方面最突出的全球運動是 2015 年聯合國通過的可持續發展目標 (SDGs)，ESG 一詞首先在 2004 年題為 “Who cares wins” 的報告中廣泛使用，該報告是聯合應聯合國邀請，金融機構的倡議該報告已獲得 20 家知名機構的認可，ESG 中包含環境問題(氣候危機、環境可持續性)、社會問題(多樣性、人權、消費者保護、動物福利)、公司管理問題(管理結構、員工關係、行政薪資、員工薪資)。

而碳中和(Carbon Neutrality)是近來新興非常熱門之話題，自工業革命以來，人類大量燃燒煤炭、石油等化石燃料來發電，產生大量溫室氣體，造成全球暖化，各地也傳出各種極端天氣事件。為了避免全球氣候持續惡化，許多國家都承諾要在 2050 年達到碳中和，甚至是淨零碳排。而碳中和的宗旨是企業、政府和組織在一定時間內所產生的二氧化碳的量要和種樹、綠色能源的碳清除量達成正負相抵。而各國為了達成碳中和的目標，也延伸出了碳金融、碳排放交易的相關議題。

碳金融的目的是以減少溫室氣體排放為目標的各種金融制度安排和交易活動，其中就包含交易碳權的碳排放交易，針對高碳排的國家、企業和組織收取較高的碳費，目的是鼓勵每個國家節能減碳和多使用綠色能源。為了達成碳中和，組織可以分為四個步驟去執行，分別是盤查、分析、減量和抵銷。首先碳盤查包含了記錄碳足跡的產品型碳盤產和針對組織本身營運活動的組織型碳盤查，接著透過專家顧問分析所排出的溫室氣體，並研擬減少碳排放量的計畫，然後執行碳管理計畫，持續追蹤是否有效地減少碳足跡，另外國家也可以利用碳補償機制，多種樹等來減少所產生的碳排放量。

除了 NFT 外，DAO 非常適用於非營利性組織在 SDGs、ESG，和碳中和等目標之追求與發展。如以 SDGs 之消除貧窮 (No Poverty)為例，傳統公益慈善項目中，無論是善款捐贈方還是平台方，通常都難以對捐助善款進行即時監督和追踪，多由公益機構組織人工向社會和監管部門進行捐助項目回應。這種透明化程度較低的捐款形式難免導致公信力的不足，不僅無法保證善款的精準捐助，也在很大程度上阻礙了捐助者參與慈善的熱情。而捐款方對慈善平台的透明化程度提出了更高的要求，每次捐款行為的公益賬戶、資金流向、項目流程和執行結果等都應做到環環相扣、清晰明了，才能保證慈善捐款行為的成果和效率。另外捐款資金下撥慢。在傳統業務中，慈善機構需向管理機關提交申請進行慈善組織認定，認證過程煩瑣，流程耗時，捐助行為的時效性低下，使受助者難以及時拿到善款，善款的救急效益被大大削弱。善款流向不透明，資訊公開不及時，善款撥付不精準。當前捐助資訊公開不及時，缺乏資金追溯、審計手段，善款流向難以做到系統級追踪，常造成重複捐贈、撥付和捐助不對等、缺乏追溯手段等現象。以區塊鏈為基礎之 DAO，可有效解決以上問題。在數據共識、資訊同步和存證溯源等方面具有天然的技術優勢，基於區塊鏈可搭建多方資訊共享和業務協同平台(如企業追求 ESG 者)。各方可以不同類型節點加入聯盟鏈形成新的善款管理業務模式，打通各參與方業務系統，實現全鏈條數據透明化記錄。捐贈資訊可追溯，便於審查追責。由於區塊鏈的防篡改性，捐助資訊一旦上鏈存儲，便無法被更改，當需要進行資金審計或司法追責時，區塊鏈可以提供權威的數據證明，使捐款行為有據可依，有據可查。慈善機構可對資訊進行公開，接受社會監督，提昇機構公信力。

另外，碳中和也可以借助區塊鏈的優勢，來記錄碳足跡、完成碳權交易等。以星巴克為例，他們就曾為咖啡豆加上溯源，標示其產區以及運送方法等，紀錄一杯咖啡的碳足跡。所以國家、企業和組織就可以採用類似的方式，來進行碳盤查，計算在原料取得、生產製造、運送過程中直接或間接產生的溫室氣體排放量，也才能更好地擬訂計畫來實施減碳的策略(如圖 3)。

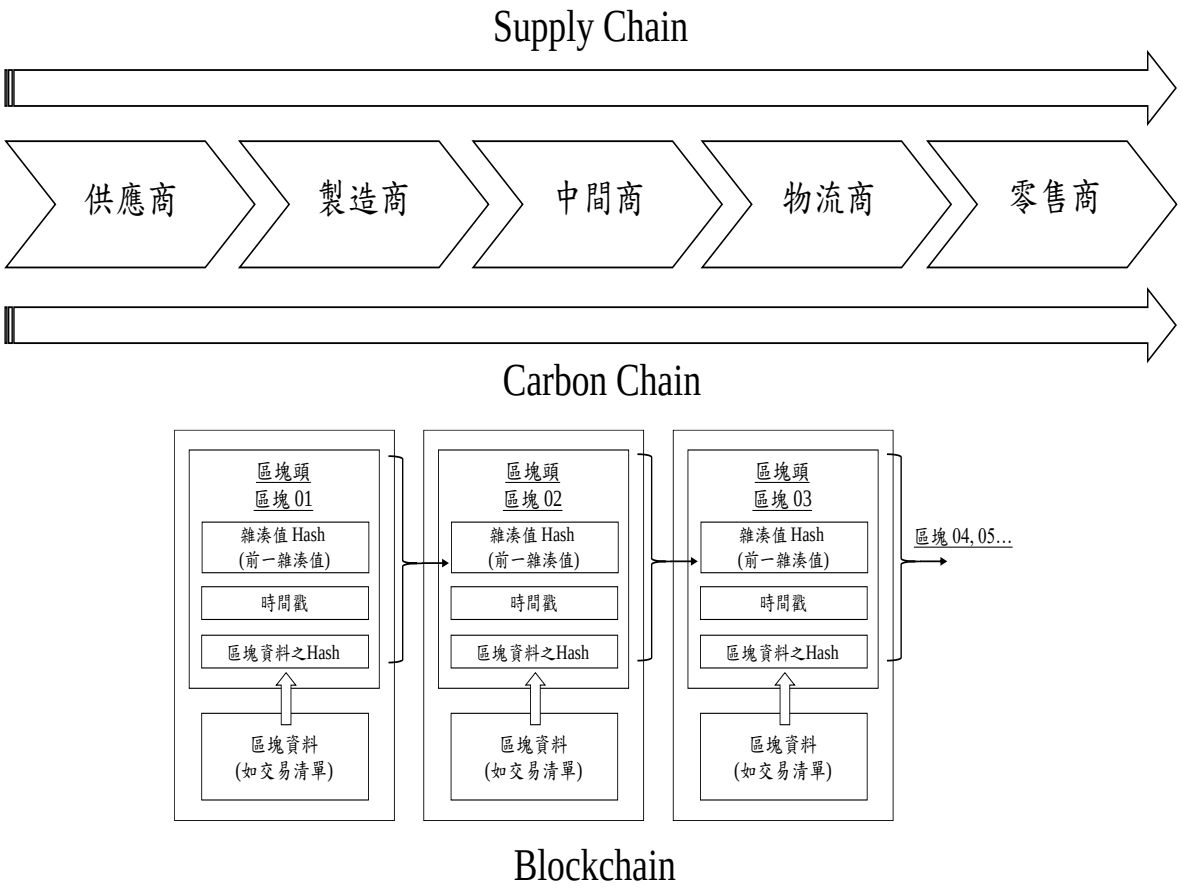

圖 3 區塊鏈在碳足跡/碳排放之應用

另外，隨著越來越多的國家實施碳定價政策，收取碳稅和碳費，慢慢地就形成一個碳權交易市場。但因為各國所制定的碳定價不同，而且各國的政策、碳金融建設都並未完善，所以要建立一個全球通用的碳權市場，可能是件不容易的事。但透過區塊鏈有機會讓全球碳權市場更穩定、透明，首先要發展一個全球碳權市場，區塊鏈上會進行碳資產管理，確保能夠標準化地記錄碳排放量。再者，各國的碳定價不同，像是在瑞典每噸碳價高達 137 美元，但在開發中國家碳價卻只有個位數，所以透過區塊鏈的可追溯性，就可以記錄每筆碳交易的金額，減少碳交易價格的不透明，也能找到更便宜的碳定價，吸引更多用戶。而區塊鏈會記錄每筆交易的時間，且具有不可竄改性，所以不僅能確保每筆碳交易的有效性，而且也可以保證碳抵換所減少的溫室氣體不會被重複計算。所以透過區塊鏈能讓全球的碳權市場制定合理的碳定價，同時也加快了各國的碳交易效率。

肆、結論

NFT 的唯一性、不可分割性，與藝術品所需要的市場雷同，所以很快就有了各種的發展空間。可以看到經過多個作品的發行，讓 NFT 這個議題帶到大眾的視野中，也有越來越多人加入 NFT 的行列，在 NFT 的平台上進行交易。NFT 也發展了一套協議來維持 NFT 的秩序，並讓想要發行自己作品的藝術家、創作者和有興趣的投資人可以跨越時間、空間的限制，進行交易，並可以保護自身的版權不受到侵害。隨著 NFT 的發展，其運作模式所顯露出的破綻也越來越多，雖說區塊鏈省去了大多數交易過程中不必要的麻煩，但也因為此特性，交易進行時沒有第三方介入可代勞把關，衍伸出許多交易糾紛及詐騙案件，所以個人須自行判斷是否進行交易並為自己在 NFT 市場的行為負責。且也因為 NFT 所帶來的無限商機，一些無良的操作方式影響了市場價值及擁有者的權益，因而導致泡沫化的情形。本研究認為，NFT 之泡沫化猶如早期電子商務泡沫化一般，對新科技技術的盲目追求與濫用而導致的崩毀，終究給人們上了一門課，從而以更成熟的思維來善用科技。NFT 若能改善目前的弊病，仍有其發展空間，倘若未來 NFT 在規範或是經營方式上能重新博得民眾的信任， NFT 才真正有機會繼續留存現代，成為與未來科技接軌的里程碑。

另外在應用 NFT 技術的智慧型合約方面，目前發現台灣還沒有相關的法律規定，能讓智慧型合約具備像是傳統合約的法律效力，但隨著區塊鏈快速的發展，在國外已經越來越重視智慧型合約在法律上的相關議題，像是歐盟已經透過法律來規範智慧型合約，應該要符合某些標準，最新的提案，甚至提出智慧型合約應該要包含讓使用者可以終止、停止、或中斷智慧型合約的按鈕，而英國更是承認智慧型合約具有法律效力，台灣在這方面可能要加強，可以透過與區塊鏈的相關法律，進一步修改，以約束智慧型合約的使用與規則，完善台灣智慧型合約與區塊鏈的環境。

區塊鏈智慧型合約也有其他應用，像是 DeFi、DAO 等，也可用於公益事業、全球永續發展上，擔任輔助的角色，例如記錄慈善機構的捐款和用款紀錄，確保流程透明化，也讓錢用在真正需要幫助的人身上，或是用在記錄碳足跡、碳權交易紀錄，也避免出現重複的碳抵換交易。希望在未來與區塊鏈相關的應用能夠有完善的法規和制度，這樣才能使區塊鏈發揮最大的效益。

引用文獻

一、中文部分

Fortnow, M., & Terry, Q. (2022). NFT 狂潮：進入元宇宙最關鍵的入口，擁抱千億商機的數位經濟革命(李立心，許可欣，張明心，楊雅筑，譯)。商周出版。(原著出版年：2021)

二、外文部分

Antonopoulos, A. (2014). Bitcoin security model: trust by computation. Forbes. com, February, 20.

Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.

Chirtoaca, D., Ellul, J., & Azzopardi, G. (2020). A framework for creating deployable smart contracts for non-fungible tokens on the Ethereum blockchain. (2020), 100-105.

Chohan, U. W. (2017). The decentralized autonomous organization and governance issues. *Available at SSRN 3082055*.

Dowling, M. (2022). Is non-fungible token pricing driven by cryptocurrencies.

Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. Hastings Sci. & Tech. LJ, 4, 159.

Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020, June). The decentralized financial crisis. In 2020 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 1-15). IEEE.

Haber, S., & Stornetta, W. S. (1997, April). Secure names for bit-strings. In Proceedings of the 4th ACM Conference on Computer and Communications Security (pp. 28-35).

Kugler, L. (2021) Non-fungible tokens and the future of art. *Communications of the ACM*, 64(9), 19-20.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

Norta, A. (2015, August). Creation of smart-contracting collaborations for decentralized autonomous organizations. In *International Conference on Business Informatics Research* (pp. 3-17). Springer, Cham.

Singh, M., & Kim, S. (2019). Blockchain technology for decentralized autonomous organizations. In *Advances in computers* (Vol. 115, pp. 115-140). Elsevier.

Vogelsteller, F., & Buterin, V. (2015) *Eip 20: Erc-20 token standard. Ethereum Improvement Proposals.*

三、網路資料

Chiu, A., & Frances (2022, March 16). *RAW 也進軍元宇宙！江振誠領軍打造「可以吃的 NFT」，結合料理、VR、行為藝術「We Are What We Eat: Seed」正式開吃！*. GQ. https://www.gq.com.tw/life/article/raw-%E5%85%83%E5%AE%87%E5%AE%99-%E6%B1%9F%E6%8C%AF%E8%AA%A0-nft

ERC-721. (n.d.). Binance Academy. https://academy.binance.com/en/glossary/erc-721

Pilehchiha, S. (2022, May 23). *ERC-20 TOKEN STANDARD*. Ethereum. https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

Schmitt, K.R. (2021, October 09). *Decentralized Market Definition.* Investopedia. https://www.investopedia.com/terms/d/decentralizedmarket.asp

Tarcan, H. (2022, June 23). *ERC-721 NON-FUNGIBLE TOKEN STANDARD*. Ethereum. https://ethereum.org/en/developers/docs/standards/tokens/erc-721/

What are DAOs？ (n.d.). Ethereum. https://ethereum.org/en/dao/

What is a decentralized autonomous organization, and how does a DAO work? (n.d.). Cointelegraph. https://cointelegraph.com/decentralized-automated-organizations-daos-guide-for-beginners/what-is-decentralized-autonomous-organization-and-how-does-a-dao-work