

以太坊區塊鏈與去中心化金融數據分析之研究

林億雄^{1*} 馬瀾嘉²

¹ 台灣首府大學教育研究所

² 國立成功大學統計學系暨數據科學研究所、金融科技商業創新中心

摘要

本研究針對以太坊區塊鏈數據資料進行實證研究。截至 2021 年 4 月為止，以太坊區塊鏈帳本資料容量已經高達 350 GB，並持續以每個月超過 30 GB 的成長速度繼續增加。面對如此龐大的數據集，我們使用 Google BigQuery、Dune Analytics 進行以太坊區塊鏈數據資料之提存分析。透過 BigQuery 提存分析，得知以太坊區塊鏈上交易次數最多的前 10 名 ERC20 代幣與 ERC721-NFTs；對於去中心化金融 DeFi 項目方，本文使用 Dune 平台提存的數據資料。透過資料分析獲取 Pickle Finance 上擁有 Pickle Power 的 DAO 用戶分布情形；此外，也能獲取 Harvest Finance 上用戶在 mSTONK 的 mTSLA-UST 礦池的資產分布情形。研究發現可將 Dune 平台提存分析結果，運用來結合 DeBank、Zapper，及 Etherscan 等去中心化應用程式 DApps，深入研究用戶活動行為及其資產的轉移。最後，本研究建議可針對 DeFi 項目方在其產生實質價值的部分進行監管，並需針對 DeFi 開發一種全新的設計法規，將法規方法納入 DeFi 的協議設計中，以利金融監管權力下放到 RegTech 確保有效的監督和風險控制。

關鍵詞：比特幣；以太坊；區塊鏈；智能合約；大數據；去中心化金融

*通訊作者聯絡方式：yhslin@tsu.edu.tw

A Study on Ethereum Blockchain and Decentralized Finance

Yi-Hsiung Lin^{1*} Mi-Chia Ma²

¹Institute of Education, Taiwan Shoufu University, Tainan, Taiwan

²Department of Statistics, Institute of Data Science, and
Center for Innovative FinTech Business Models of National Cheng Kung University,
Tainan, Taiwan

Abstract

This research conducts empirical research on Ethereum blockchain data. As of April 2021, the data capacity of the Ethereum blockchain ledger has reached 350 GB, and continues to increase over 30 GB at a monthly growth rate. Faced with such a huge data set, we use Google BigQuery and Dune Analytics to perform data analysis of the Ethereum blockchain. Using BigQuery, these top 10 most popular ERC20 tokens and ERC721-NFTs can be found; for specific DeFi projects, we first use the Dune platform. We then get the current allocation of decentralized autonomous organization users with Pickle Power on Pickle Finance; moreover, it can figure out users' asset allocation in the mSTONK's mTSLA-UST mining pool on Harvest Finance. From this research, Dune platform can be used to combine with decentralized applications such as DeBank, Zapper, and Etherscan to study users' behavior and asset transfer deeply. In the future, DeFi projects should be supervised on the part of its substantial value. Finally, it is necessary to develop a new design regulation for DeFi and incorporate the regulation method into the DeFi's design protocol, so that this financial supervision power will be delegated to RegTech which ensure effective supervision and risk control.

Keywords: Big Data, Bitcoin, Blockchain, DeFi, Ethereum, Smart Contrast

* Corresponding author. E-mail address: yhslin@tsu.edu.tw

1. 緒論

區塊鏈技術吸引了資料科學家、程式編碼專家和經濟學者等的注意目光，當中以比特幣（Bitcoin）及以太坊（Ethereum）區塊鏈發展最盛；加密貨幣是區塊鏈技術底層的一種應用，其中又以比特幣（BTC）及以太幣（ETH）最吸引投資者注意。以太坊和比特幣一樣都是開源程式及一種不能竄改的分散式帳本資料，以太坊的概念最早於 2013 年由程式編碼專家 V. Buterin 所提出，Buterin 受比特幣啟發後提出以太坊區塊鏈作為下一代加密貨幣與去中心化應用平台，並於 2014 年透過首次代幣發行（Initial Coin Offering, ICO）開始發展。截至 2021 年 4 月底為止，ETH 是市值第二高的加密貨幣，以太坊也被稱為「第二代的區塊鏈平台」，僅次於比特幣。

就系統架構而言，以太坊與比特幣的相似之處在於記錄不可竄改的交易。兩者本質上都是線上交易處理（Online transaction processing, OLTP）資料庫。OLTP 是指通過資訊系統、計算機網路及資料庫，以線上交易的方式處理一般即時性的作業資料，和更早期傳統資料庫系統大量批次的作業方式並不相同。OLTP 通常被使用於自動化的資料處理工作，如訂單輸入、金融業務等反覆性的日常交易活動。此外，以太坊是一個擁有智能合約功能的公共區塊鏈平台，透過使用其專用加密貨幣 ETH 提供去中心化以太坊虛擬機（Ethereum Virtual Machine, EVM）來處理對等合約。此 EVM 可以執行儲存在區塊鏈上的程式碼作為智能合約，智能合約是一種以資訊化方式傳播、驗證或執行合同的計算機協議。智能合約允許在沒有第三方的情況下進行可信交易。這些交易可追蹤且不可竄改。智能合約的概念是由 Szabo（1997）首次提出，但直到結合區塊鏈技術才被重視。智能合約的概念具備承諾、協議、數字形式三大要素，因此能夠將區塊鏈的應用範圍擴充至金融行業交易、支付、結算和清算的各個環節。智能合約也可以被視為當一個預先編好的條件被觸發時，合約會立即執行相應的合約條款，其工作原理類似於程式碼的 if-then 語句，為具有圖靈完備的程式語法（Wood, 2014; Swan, 2015）。去中心化金融（Decentralized Finance, DeFi）是一種基於區塊鏈技術開展的金融形式，DeFi 也是加密貨幣或區塊鏈中各種金融應用的總稱，其目的在於變革金融中介機構達成普惠金融。它不依賴中心化，或中介機構提供傳統金融工具，而是利用區塊鏈上的智能合約，以太坊區塊鏈是目前最常使用的 DeFi 交易平台。

根據 BitInfoCharts 網站（<https://bitinfocharts.com/ethereum/>）2021 年 4 月資料顯示，以太坊已經發行超過 1 億顆 ETH，估計目前總價值高達 2,000 億美金。每天活躍的以太坊用戶地址高達 81 萬。同時，Twitter 每天有關以太坊訊息貼文高達 1 萬 5 千多則以上；知名區塊鏈論壇 BitcoinTalk 網站上累計有 2 萬 5 千多則探討以太坊區塊鏈相關技術與訊息的文章；Reddit 論壇也累計擁有多達 74 萬則留言討論文章。從以太坊區塊鏈第一筆創世帳本記錄區塊資料開始，以

以太坊區塊鏈帳本資料容量已經高達 350GB。龐大的以太坊區塊鏈資料對於傳統電腦硬體、或一般統計數據分析軟體均難以儲存、運算與分析，如何分析與處理如此龐大的大數據資料集將是一大難題。同時，DeFi 做為以太坊區塊鏈上的智能合約應用，研究人員如何分析各別 DeFi 項目方的公開資料與用戶活動行為也是本文亟欲探討的研究。綜觀如上，本文的研究重點將在於提出對於以太坊區塊鏈帳本資料，及其鏈上 DeFi 項目方數據資料的分析處理方法。

本文主要章節如下：第二節為文獻探討，主要介紹以太坊區塊鏈、智能合約及 DeFi 等。第三節為以太坊區塊鏈的帳本資料分析，並介紹 BigQuery、Etherscan 及 Zapper；第四節為資料分析介紹 DeBank 與 Dune Analytics，並以 Dune Analytics 做為本文中二個 DeFi 項目方數據資料範例提存分析的研究工具平台；最後，第五節針對研究結果提出對於以太坊區塊鏈與去中心化金融數據分析的相關建議，及未來研究。

2. 文獻探討

以太坊區塊鏈是一種不可竄改只能追加的分散式資料庫，對於欲研究以太坊區塊鏈數據資料的研究人員來說，同步下載以太坊節點是一個非常耗時且困難的工作。研究人員首先需先建立節點下載所有的交易區塊，並將整個鏈資料副本下載。截至 2021 年 4 月所公布的數據，以太坊數據庫的大小約為 350GB，且每個月以超過 30GB 成長的速度增加。除此之外，研究人員為進行對以太坊區塊鏈分析提取一些有用的訊息，仍需了解以太坊區塊鏈中儲存的數據，與其資料結構。以太坊的特點是所有數據都是公開和可用的，節點間彼此共享與儲存數據副本並執行以太坊的協議。該協議定義各節點之間的相互交換規則，或執行智能合約。關於以太坊區塊鏈全節點是指擁有完整區塊鏈帳本資料的節點，具備獨立驗證的能力來確認交易之有效性。同時，全節點的數量越多，也代表完整的區塊鏈帳本被保存的份數越多，「不可竄改性」也就越強，整個區塊鏈網路的安全性也隨之提升。若有節點企圖組織算力叛變，試圖改變區塊共識或發動雙重支付攻擊，其它正常運作的全節點可以即時驗證拒絕掉這些交易 (Bosu, Iqbal, Shahriyar, and Chakraborty, 2019)，算力也稱為哈希率是數位貨幣網路處理能力的度量單位。

隨着持續增加的交易記錄與智能合約佈署，全節點所需的儲存空間也正在不斷增長。以太坊中的區塊資料是由區塊頭 (Blockheader, H)，已驗證交易列表 (Transactions, T)，及其他已知前交易區塊頭 (Other Block Headers, U) 所組合而成。對於研究人員而言，並非所有以太坊區塊鏈帳本資料變數都會用到，因為其中有些變數定義是非常具有技術性的，其含義只有對區塊鏈實際運作深入了解，才能了解意義。簡而言之，以太坊區塊鏈帳本資料結構是由包含一個區塊的區塊頭 H，及一個已寫入其中的已驗證交易列表 T，還有一個已知前交易列表 U 所組成的分散式資料庫。如上探討，以太坊區塊鏈數據資料分析的研究步驟，研究人員首先需先從全節點

中提取相關的數據；接續，研究人員需再將數據轉換為電腦軟體可讀的格式；最後，研究人員將所有數據輸出到資料庫中並建立索引實現最佳查詢性能。這些大數據分析整理技術過程均需要花費長時間處理，且其本身均包含不同的技術知識。

2.1 智能合約

從比特幣問世以來，區塊鏈發展已有十餘年。除了比特幣外，區塊鏈最新亮點是智能合約的誕生（Pinna, Ibba, Baralla, Tonelli, and Marchesi, 2019）。基於區塊鏈的智能合約，本質上可以看成是在區塊鏈上儲存具可執行狀態的程式碼。智能合約並可說為是一種重塑產業未來及具有發展的技術，其概念比區塊鏈技術被提出的時間更早。現有的以太坊區塊鏈系統已整合智能合約，以太坊實現了圖靈完備的智能合約。在以太坊中，智能合約在節點中執行 EVM（以太虛擬機），在合約執行期間，礦工使用 Gas 作為單位來評估執行一個智能合約所需要的費用。根據 Buterin（2014）以太坊黃皮書所述，以太坊上的交易手續費是使用 Gas 來計算：

$$\text{交易手續費 Tx Fees} = \text{Gas Limit} * \text{Gas Price}$$

其中 Gas Limit 是最多同意使用多少單位的 Gas 來執行這個交易或合約，Gas Price 是每個單位 Gas 價錢。如果執行交易或合約超過 Gas Limit 則執行不會成功；反之，如果執行交易或合約少於 Gas Limit 則會把多餘的退還。

Szabo（1997）首次描述了智能合約的概念，其對智能合約定義為將協議與用戶界面相結合的一種工具，從而對計算機網絡進行規範化和加強安全。同時，Szabo 還探討了智能合約的潛在用途，例如信用體系、支付流程和版權管理。多年來，雖然比特幣協議也一直支持智能合約，但智能合約卻是由以太坊聯合創始人 Buterin（2014）推廣從而大受歡迎。簡單來說，智能合約就是一個確定性的計劃，當滿足某些條件時，它則執行特定任務，EVM 是運行智能合約重要的組成部分。在加密貨幣領域，我們可以將智能合約定義為在區塊鏈上運行的應用程序。在一般情況下，它們為一組具有特定規則的數字化協議，且該協議能夠被強制執行。這些規則由電腦程式碼預先定義，所有在網路上的節點會複製和執行這些程式碼。實際上，智能合約支持創建無需信任的協議，這意味著執行合約的雙方可以通過區塊鏈做出承諾，而無需相互了解或取得相互信任。合約內容經雙方確認後，如果沒達到觸發條件，合約將不會被執行。所以，使用智能合約可以消除對中介的需求，從而顯著降低運營成本。

智能合約作為可編程代碼，其具有高度可客製化，可以透過多種不同方式進行設計，提供不同的服務和解決方案。智能合約在兩方或多方間的轉帳或資金交易時更為實用，智能合約還可與其他區塊鏈解決方案一起佈署，這些解決方案涉及醫療保健、慈善、供應鏈、政府治理，和去中心化金融等領域。

2.2 去中心化金融介紹

智能合約帶來了新項目，目前以金融和遊戲方面為主。其中，遊戲方面主要以 ERC721 非同質代幣（Non-Fungible Token, NFT）為主，主要項目圍繞在 NFT 的生成和交易以形成龐大的價值，目前 NFT 還處於初級階段。NFT 與一般代幣不同，NFT 所有權在區塊鏈上具獨一無二的特質無法被拆分。ERC 是 Ethereum Request for Comments 的縮寫，意思是以太坊開發者公開徵求意見，希望定義出統一的溝通接口，建立出一套可以遵循的標準，讓以太坊開發者在撰寫智能合約時能更為順暢。ERC721 標準的規格是建立一種不可替換代幣，稱為非同質代幣。

在金融方面，智能合約平台以 DeFi 為主，DeFi 是 Decentralized Finance 的縮寫，直譯是「去中心化金融」。DeFi 是以智能合約平台為基礎架構的加密資產，其合約具組合性，因此 DeFi 也被稱為貨幣樂高。雖然 DeFi 還屬於發展階段，但 DeFi 真正實現了產品和市場的匹配，依據目前其貨幣樂高的發展趨勢，DeFi 正企圖構建一個跟傳統金融平行的領域，也試圖跟傳統金融結合實現新的特性。目前，許多區塊鏈新創公司會佈署 DeFi 智能合約，以便在以太坊上發行數位代幣。發行後，這些公司大多數通過 ICO 活動發送其 ERC20 代幣。在以太坊上發布的代幣遵循 ERC20 的標準，ERC20 是所有基於以太坊代幣的核心功能。因此，這些數位資產被稱為 ERC20 代幣是目前的主流，它們佔據了現有加密貨幣總量的很大一部分。ERC20 是一個以太坊區塊鏈上的智能合約協議標準，截至 2021 年 4 月共計發佈超過 42 萬多種 ERC20 兼容的不同代幣。

過去傳統金融透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，也由於中介機構的存在，傳統金融體系也產生了很多問題，比如不透明、濫發等。這導致過度的債務和過度的通貨膨脹，一旦經濟發展停滯或者經濟分配存在過度不均，且債務結構沒有及時消化，就很容易爆發經濟危機。而區塊鏈的核心是透明化和分散式，這使得它有機會改變當前的金融結構的現狀。

加密歷史上的第一個突破是比特幣，DeFi 可以稱為是加密史上第二個突破，它透過對密碼學、共識機制、點對點網絡、激勵機制等的運用，完成了無需第三方參與的價值轉移。具體而言，DeFi 是指基於智能合約平台構建的加密資產、金融類智能合約協議。這些資產及協議能夠像樂高一樣被組合起來，故此也可稱為「貨幣樂高」。由於 DeFi 是用戶與區塊鏈上的一系列智能合約進行交互，用戶可以利用它的透明和無需許可特性獲利。當然 DeFi 並非沒有風險，這也是它相對於傳統金融的不足。雖然傳統銀行也有破產風險，但相對來說，它具有穩定性和可預測性。而 DeFi 的項目可能會面臨加密數位資產暴漲暴跌，而在暴跌時因來不及清算導致產生崩潰風險；此外，如果程式碼存在漏洞，可能會導致駭客攻擊的平台經濟風險等（Atzei, Bartoletti, and Cimol, 2017）。另外，DeFi 和傳統金融也有可能融合，傳統金融可以利用 DeFi 的特性實現

流動性，DeFi 可以利用傳統金融的資產、法規等來實現規模的擴展。由於 DeFi 是無需許可，它意味著任何人擁有加密數位資產都可以參與 DeFi。隨著越來越多的 DeFi 項目簡化其操作流程，使用上越來越簡單，DeFi 的使用難度將會逐步降低。當使用者養成使用習慣，將會有越來越多的人進入到 DeFi 領域。

3. 以太坊區塊鏈帳本資料之分析

目前，以太坊區塊鏈上所使用的去中心化應用程式（Decentralized Applications, DApps）大都為點對點（Peer-to-Peer）軟體，雖具有隨機存取功能應用程式介面（Application Programming Interface, API）提供類似檢查交易狀態、查詢錢包交易，及查詢錢包餘額等功能。但，API 端點無法存取區塊鏈上所有的資料，更無法利用 API 端點來查詢區塊鏈上智能合約的數據。所以，研究人員若想要分析區塊鏈上的整體資料將需要特別的運算技術，及克服更高的技術門檻。

Google Cloud Platform（GCP）是 Google 於 2018 年所推出雲端千兆位元組等級的資料庫解決方案，可用以儲存以太坊區塊鏈上的帳本資料集。GCP 的推出讓以太坊區塊鏈上的帳本資料易於使用，研究人員可搭配其資料倉儲 BigQuery 項目，將可搜索以太坊區塊鏈上所有歷史資料。使用 BigQuery 的線上分析處理（OLAP）功能可完成大數據提存與分析。例如：研究人員可以搜尋每天 ETH 轉帳與交易費用大數據分析等。

3.1 BigQuery

BigQuery 是 GCP 所推出的資料倉儲服務，具備無伺服器、高擴展性、低成本等特性。它透過平行處理的技術，將演算功能佈署於上千台機器，讓使用者輕鬆分析 TB 等級的大數據資料最快可達到「秒」的等級，BigQuery 同時支援各種 GCP 雲端工具可協同第三方強化資料整合至分析應用。此外，BigQuery 採用類似 SQL 的結構式查詢語法，讓用戶查詢資料時更易上手，資料存取也經過加密處理以強化安全機制。由於 BigQuery 不需管理基礎架構，使用者僅需專注於使用熟悉的 SQL 查找有價值的訊息。

3.2 BigQuery 與其他項目整合

BigQuery 是 GCP 上大數據資料處理重要的一環，透過與其他 GCP 工具搭配，可以達到更多情境的應用。例如：BigQuery 與 Datalab 及 Dataflow 的整合，Datalab 是 GCP 中支援程式化查詢與分析輸出的工具，Dataflow 是 GCP 中支援 Input 與 Output 的工具。整合後將可讓 Dataflow 調用 BigQuery 中大數據的分析結果，在 Datalab 中製作成報表與圖表，提供使用者查詢大數據

即時資料服務，其功能展示畫面類似儀板表的即時審閱功能，如圖 3.1 為本研究開發全球 Covid-19 即時情報儀板表 (<https://reurl.cc/GVbOoD>)，所使用工具為 GCP、R 與 GitHub 等。

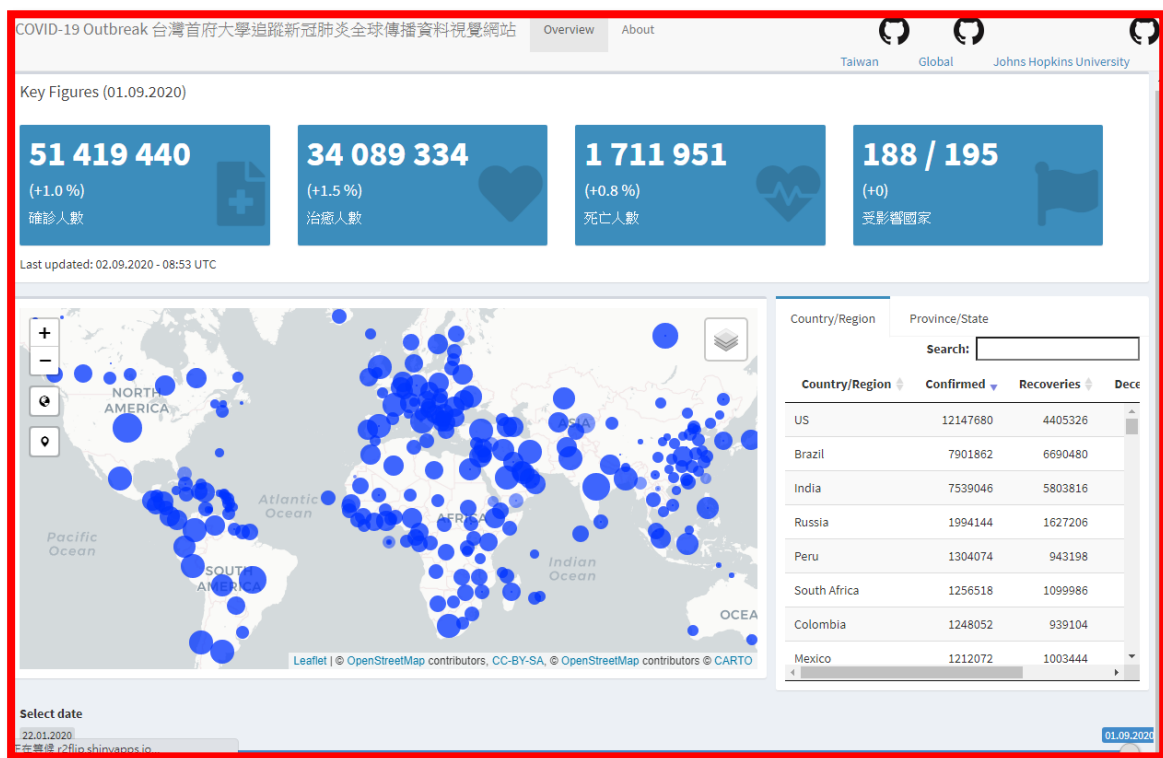


圖 3.1 研究者整合設計之全球 Covid-19 即時情報儀板表

對於研究人員而言使用 BigQuery 分析以太坊數據資料確實非常便利，例如：以太坊區塊鏈上分布著許多類型的貨幣，而這些貨幣的分布模式，因類型和時間而不同，透過觀察每種貨幣的交易活動，可以量測特定時間內受歡迎的貨幣種類。如表 3.1 與表 3.2 分別為前 10 名最多交易次數的 ERC721-NFTs 遊戲，及 ERC20 代幣，相關程式碼見附錄 A。在以太坊區塊鏈上最熱門的 ERC721-NFTs 遊戲為謎戀貓(CryptoKittie)，它是一款使用 ETH 交易的虛擬貓咪休閒遊戲；最熱門 ERC20 代幣為泰達幣 (USDT)。目前，用戶使用 BigQuery 並非免費，Google 提供定額的免費查詢額度，用戶超過免費額度後 Google 將會計量收費。

表 3.1 前 10 名最多交易次數的 ERC721-NFTs

地址	ERC721-NFT 名稱
0x06012c8cf97bead5deae237070f9587f8e7a266d	CryptoKitties (CK)
0x06a6a7af298129e3a2ab396c9c06f91d3c54aba8	0xUniverse (PLANET)
0xd73be539d6b2076bab83ca6ba62dfe189abc6bbe	BlockchainCutie (BC)
0x1a94fce7ef36bc90959e206ba569a12afbc91ca1	Crypton (CTN)

0xf5b0a3efb8e8e4c201e2a935f110eaf3ffecb8d	Axi (AXIE)
0x7fdcd2a1e52f10c28cb7732f46393e297ecadda1	HyperDragons (HD)
0x8c9b261faef3b3c2e64ab5e58e04615f8c788099	LucidSight-MLB-NFT (MLBCB)
0xf915bbfbb6c097dc327e64eec55e9ef4d110d627	Servant (SVT)
0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756	MakersTokenV2 (MKT2)
0xd2f81cd7a20d60c0d558496c7169a20968389b40	Etherbot (ETHBOT)

表 3.2 前 10 名最多交易次數的 ERC20 代幣

地址	ERC20 代幣名稱
0xdac17f958d2ee523a2206206994597c13d831ec7	USDT
0x174bfa6600bf90c885c7c01c7031389ed1461ab9	MCG
0x514910771af9ca656af840dff83e8264ecf986ca	LINK
0x86fa049857e0209aa7d9e616f7eb3b3b78ecfdb0	EOS
0x0d8775f648430679a709e98d2b0cb6250d2887ef	BAT
0xd26114cd6ee289accf82350c8d8487fedb8a0c07	OMG
0x8fdcc30eda7e94f1c12ce0280df6cd531e8365c5	CPC Token
0xf230b790e05390fc8295f4d3f60332c93bed42e2	TRX
0xb64ef51c888972c908cfac5f59b47c1afbc0ab8ac	MXM
0x8e766f57f7d16ca50b4a0b90b88f6468a09b0439	Storj

3.3 Etherscan 與 Zapper

本節將介紹 Etherscan (<https://etherscan.io/>) 與 Zapper (<https://zapper.fi/>) 此二款查詢特定位址或合約交易 DApps。Etherscan 是一個區塊鏈瀏覽器工具，其專門為以太坊區塊鏈平台所創建的，使用 Etherscan 將有助於檢查區塊鏈上的有關 ETH 訊息。Etherscan 是由馬來西亞人 Matthew Tan 於 2015 年 7 月創立，Etherscan 是一個以太坊區塊鏈瀏覽器，任何在鏈上發生的交易都可以在 Etherscan 上查詢，Etherscan 可讓使用者瀏覽區塊鏈上的內容。Etherscan 基本功能有查詢 ETH 錢包餘額、查訊交易狀態、查詢錢包內持有的 ERC20 代幣，及智能合約查詢。

Zapper Finance 誕生於 2019 年的一場程式設計馬拉松，其不僅可以幫助用戶追蹤自己持有的加密資產，還能讓用戶對新的市場走勢迅速做出反應，這讓 Zapper 有機會成為流動性挖擴 (Yield Farming) 熱潮中主要受益者之一。Zapper 的一個核心功能，就是可以讓 DeFi 用戶一鍵進入和退出流動資金池。Etherscan 通常只能顯示一個地址交易，及顯示用戶資產，其功能無法與 Zapper 分析平台媲美。

4. 資料分析

本章將於第一節探討如何使用相關 DApps 提存 DeFi 項目方數據資料，及如何分析 DeFi 項目方之用戶使用情形；並將於第二節中提出 DeFi 項目方數據分析的研究方法；第三節將以所提出的研究方法實作於範例數據資料提存與分析上。

4.1 DeBank 與 Dune Analytics

本文於前章介紹了 Etherscan 及 Zapper，該二款 DApps 除無法下載 DeFi 項目方的完整數據資料外，在使用時仍有其他限制。例如：研究人員想了解特定 DeFi 項目方上的總資產、用戶人數變化情形，或所有參與用戶資產情形，則需透過其他 DApps 來了解。在本節，我們將介紹 DeBank 與 Dune Analytics(以下簡稱 Dune 平台)，並作為 DeFi 項目方數據資料提存分析的工具。

DeBank (<https://debank.com/>) 是款結合數據儀板表 DeFi 錢包的 DApps 軟體，可以幫助用戶追蹤管理及分析 DeFi 風險。DeBank 於 2020 年 3 月正式上線，目的在成為用戶與 DeFi 生態的橋樑，降低用戶使用 DeFi 應用的門檻，其主要功能為資產管理與數據分析。DeBank 雖然可以提供部分 DeFi 項目方的訊息，但也僅限於其介面所提供的功能。如果不在 DeBank 其服務範圍內的訊息，使用者就無法獲得。例如，DeBank 無法提供 DeFi 項目方中用戶擁有治理權的訊息。Dune 平台 (<https://duneanalytics.com/>) 是一個基於網站開發的平台，其使用標準 PostgreSQL 結構化語言查詢，並從預先整理好的數據庫中查詢以太坊數據。Dune 平台可視為研究區塊鏈數據資料分析強大的工具，其核心為將區塊鏈上原始數據轉換為可查詢的結構化資料庫。Dune 具有可編程性，研究人員可針對以太坊區塊鏈上 DeFi 項目方數據資料進行提取分析和視覺化。在下一節，我們將提出研究方法結合 Dune 平台提存分析以太坊區塊鏈數據資料。

4.2 研究方法

本節為解決如何提存分析 DeFi 項目方數據資料，我們將提出二步驟研究方法：

- (1) 審視 DeFi 項目方的合約地址及其智能合約開源程式；目前，智能合約主要開發語言為 Solidity。附錄 B 是以 Solidity 撰寫的智能合約範例，實際運行的 DeFi 合約程式碼更為複雜。
- (2) 於 Dune 平台撰寫提存分析 DeFi 項目方數據之 PostgreSQL 語法。

本節將以 DeFi 項目方【Pickle Finance 例】(<https://pickle.finance/>) 及【Harvest Finance 例】(<https://harvest.finance/>) 為例，所使用的程式碼請見附錄 C 0.PickleFinance_Pickle.Power、附錄 D 0.HarvestFinance_mTSLA+UST。同時，使用者進行 DeFi 提供流動性資產時將會使用到 Uniswap (<https://uniswap.org>)，Uniswap 是一個用於以太坊區塊鏈上自動代幣交換的協議。關於本節的

資料分析將使用 Dune 平台 erc20 資料庫，使用的表單為 erc20.ERC20_evt_Transfer，這是一個紀錄以太坊區塊鏈上所有代幣發送轉移事件的資料庫。

圖 4.1 為使用者於 Pickle Finance 中進行 Eth/Pickle 流動性挖礦示意圖。以研究者找出【Pickle Finance 例】中擁有 Pickle Power 治理權用戶的資料為例。首先，研究人員需要完成(1)搜尋所有曾經在 Uniswap Eth/Pickle 配對上提供流動性的用戶地址，並確認該用戶已將此流動性池 (Liquidity Pool; LP) 代幣添加至 Farm 中 Pickle Power 合約內，(2) 搜尋此類用戶現在所擁有該 LP 代幣數量，若該值大於 0，則視為現存用戶。關於 Dune 平台提存分析數據之 PostgreSQL 使用語法，如附錄 C 所示。研究步驟說明如下：(1) 研究者於 Pickle Finance 開源程式中找出 Farm 內 Pickle Power 合約地址，與 Masterchef 地址；(2) LP 代幣轉入為使用 Pickle Power 合約地址，資產從用戶地址移至 Masterchef 地址；LP 代幣轉出也是使用 Pickle Power 合約地址，該資產將是從 Masterchef 地址移至用戶地址；(3) 計算用戶地址上 LP 代幣轉入及轉出數量，如果轉入大於轉出，則此地址為現存擁有 Pickle Power 用戶。

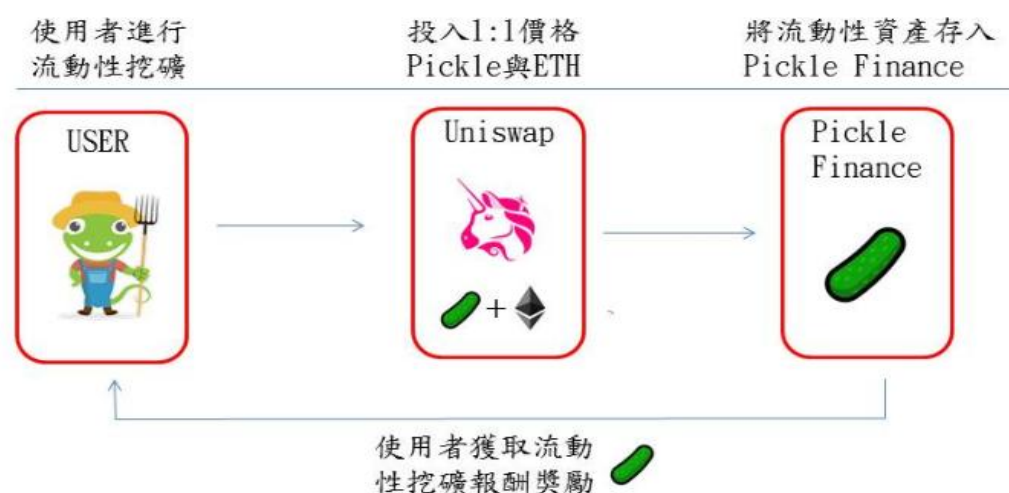


圖 4.1 使用者於 Pickle Finance 中進行 Eth/Pickle 流動性挖礦示意圖

圖 4.2 為使用者於 Harvest Finance 進行 mTSLA-UST 流動性挖礦示意圖。附錄 D 為研究者使用 Dune 平台搜尋【Harvest Finance 例】中 mStonk 項目 mTSLA-UST 用戶訊息之 PostgreSQL 語法。研究步驟：(1) 因 fAsset 為 Harvest Finance 專屬合成代幣資產，所以研究人員需於 Harvest Finance 開源程式中找出 fAsset mTSLA-UST 資金庫合約地址、LP 代幣生成銷毀合約地址，及 Uniswap V2: mTSLA-UST 合約地址；(2) fAsset 轉入為 fAsset 從 LP 代幣生成銷毀合約地址移至用戶地址，fAsset 轉入為使用合約 fAsset mTSLA-UST 資金庫合約地址；fAsset 轉出為從 fAsset mTSLA-UST 資金庫合約地址移至用戶地址，fAsset 轉出需使用 Uniswap V2: mTSLA-UST 合約

地址；(3) 計算 fAsset 轉入及轉出數量，如轉入大於轉出，則此地址為現存 fAsset mTSLA-US 用戶。



圖 4.2 使用者於 Harvest Finance 中進行 mTSLA-UST 流動性挖礦示意圖

4.3 DeFi 項目方 Pickle Finance 與 Harvest Finance 資料分析

DeFi 協議 Pickle Finance 上線日期 2020 年 09 月 10 日總用戶地址數 7,646。2020 年 11 月 22 日 DeFi 協議 Pickle Finance 曾遭駭客攻擊，Pickle Finance 約損失了 1,970 萬美金。截至 2021 年 4 月底 Pickle Finance 總鎖倉金額 (Total Value Lock, TVL) 約為 9,961 萬美金。圖 4.3 為 Dune 平台執行附錄 C 程式碼之情形。在 Pickle Finance 中分散式自治組織 (Decentralized Autonomous Organization, DAO)，是一個由公開透明程式碼運作組成的組織，其由擁有治理權的用戶參與控制，並不受中心化影響。擁有 Pickle Power 的用戶才可以在 DAO 中參與投票決定議題，DAO 的交易記錄和程序規則會被紀錄保存在區塊鏈中。Pickle Finance 的 DAO 是透過 Snapshot 網站由 DAO 用戶提出議題，擁有治理權的用戶參與投票決策。由圖 4.3 得知，目前 Pickle Finance 的治理圈擁有 421 合格用戶地址，其中用戶位址:0xe7a6d81a4b543c1bf2bd10ceb74a72689dc2e4b1 擁有 17% 最高治理權比例。另外，流動性資產小於 100 的總位址數量有 401 個，以 other 統稱，治理權比例合計共有 28.1%。(紀錄時間 2021 年 4 月 18 日；註：Pickle Finance 於 2021 年 5 月修改 DAO 治理權投票，改以鎖倉 Pickle 換取 DILL，並以 DILL 數量作為 DAO 治理權投票)。

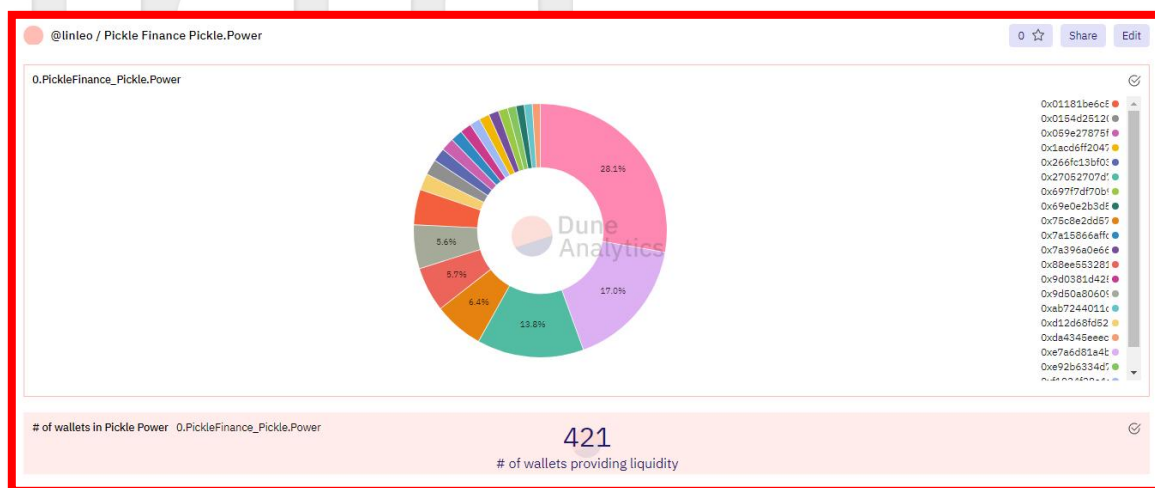


圖 4.3 Pickle.Power 用戶分布情形，紀錄時間 2021 年 4 月 18 日

DeFi 協議 Harvest Finance 上線日期 2020 年 09 月 01 日總用戶地址數 15,730。2020 年 10 月 26 日 DeFi 協議 Harvest Finance 遭到駭客借用閃電貸攻擊，損失近 2,400 萬美金。截至 2021 年 4 月底，Harvest Finance 的 TVL 達 54,696 萬美金；圖 4.4 為 Dune 執行附錄 D 之用戶情形。

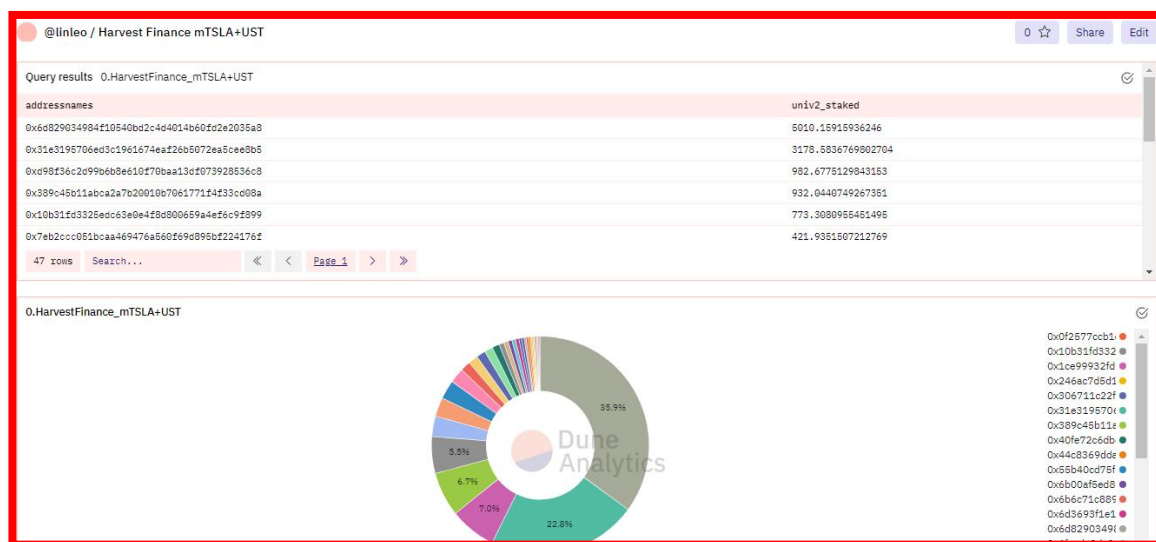
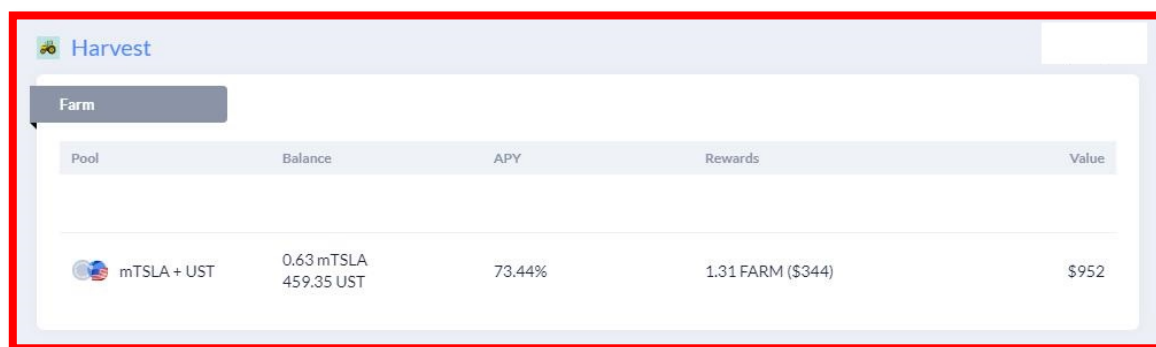


圖 4.4 mTSLA+UST 用戶分布情形，紀錄時間 2021 年 4 月 18 日

由圖 4.4 得知，目前 Harvest Finance mSTONK 中參與 mTSLA-UST 流動性挖礦的用戶有 47 個地址，以位址：0x6d829034984f10540bd2c4d4014b60fd2e2035a8 所擁有的 fAsset 資產占最大部分高達 35.9%。用戶可以透過 Mirror Finance (<https://mirror.finance/>) 質押 TerraUSD (UST) 與 mAsset 等美股的合成資產進行流動性挖礦，UST 是 Terra 網路上鑄造的穩定幣。mTSLA 是 Mirror Finance 透過區塊鏈將美股電動車產業龍頭特斯拉 (TSLA) 股票帶到去中心化區塊鏈上

進行交易。研究人員或 DeFi 的使用者除可使用 Dune 平台了解資產分布情形，也可透過結合先前介紹的 DeBank、Zapper，及 Etherscan 等 DApps 深入追蹤某用戶投資使用行為，及資產轉移狀況。圖 4.5 為地址：0x246ac7d5d1d6796b3a12c6f868e76c0d013c6c8c 在 mTSLA-UST 礦池中擁有的 fAsset 為 16.7586，對應資產為 0.63mTSLA+459.35UST。



Pool	Balance	APY	Rewards	Value
mTSLA + UST	0.63 mTSLA 459.35 UST	73.44%	1.31 FARM (\$344)	\$952

圖 4.5 特定用戶地址於 DeBank 上 mTSLA-UST 礦池的投資情況

在 DeFi 項目方數據分析，我們提出使用 Dune 平台來分析數據。因為，Dune 平台具有高度客製化及可編程性，研究者能夠依據研究問題開發查詢分析程式。本研究中，研究者透過 Dune 平台了解目前 Pickle Finance 上擁有 Pickle Power 的 DAO 用戶分布情形，及在 Harvest Finance 上 mSTONK 的 mTSLA-UST 礦池用戶的分布與資產訊息。同時，研究發現 Dune 平台可以進一步結合 DeBank、Zapper，及 Etherscan 等 DApps 深入研究特定用戶的投資使用行為與加密資產的轉移。本文提供最新及時 Pickle.Power 用戶網址(<https://duneanalytics.com/linleo/Pickle-Finance>)，及 mTSLA+UST 用戶網址 (<https://duneanalytics.com/linleo/Harvest-Finance>)。

5. 結論

對於以太坊區塊鏈資料分析，研究者需要對以太坊區塊鏈的資料結構有所理解，並且根據研究問題進行此大數據集的提存與分析。以太坊區塊鏈帳本資料容量截至 2021 年 4 月為止已經高達 350GB，並持續以每個月超過 30GB 的成長速度繼續增加。如此龐大的數據集，研究者需要使用 GCP BigQuery 進行資料提存分析。在本文中，我們已經可以透過 BigQuery 提存分析目前在以太坊區塊鏈上交易次數最多的前 10 名熱門 ERC20 代幣與 ERC721-NFTs。

另外，關於 DeFi 項目方數據分析。因為 Dune 平台具有高度客製化及可編程性，本文提出使用 Dune 平台來分析 DeFi 項目方數據。同時，本文透過 Dune 平台發現目前 Pickle Finance 的治理圈，用戶位址：0xe7a6d81a4b543c1bf2bd10ceb74a72689dc2e4b1 擁有 17% 最高治理權比例；另外，流動性資產小於 100 的總位址數量有 401 個，共有 421 合格用戶地址。同時，透過 Dune

平台分析目前 Harvest Finance mSTONK 中參與 mTSLA-UST 流動性挖礦的用戶有 47 個，以位址：0x6d829034984f10540bd2c4d4014b60fd2e2035a8 所擁有的 fAsset 資產占最大部分高達 35.9%。此外，研究發現 Dune 平台提存分析結果，可以結合 DeBank、Zapper，及 Etherscan 深入研究用戶使用行為與資產的轉移。例如：追蹤地址：0x246ac7d5d1d6796b3a12c6f868e76c0d013c6c8c，結合 DeBank，可發現該地址在 mTSLA-UST 礦池中擁有的 fAsset 為 16.7586，實際對應所擁有的資產為 0.63mTSLA+459.35UST。(本研究紀錄時間 2021 年 4 月 18 日)。

目前，以太坊區塊鏈上的 DeFi 項目於 2021 年 5 月 11 日 TVL 超過 1,323 億美金達到新高。此外，不同鏈如幣安智能鏈 (Binance Smart Chain; BSC)、Polygon、Fantom、Solana 等也可以佈署 DeFi 協議。BSC 上的 DeFi 項目 TVL 超過 500 億美金、Polygon、Fantom 及 Solana 上 TVL 也超過 100 億美金。DeFi 熱潮正不斷擴散開來，然而與此同時也伴隨著危機，越來越多的合約攻擊及項目方的欺詐造成使用者巨大損失，DeFi 領域犯罪率正創下歷史新高。越來越多的用戶開始呼籲重視 DeFi 監管問題，各國政府也正面臨如何監管 DeFi 等挑戰。透過本文，我們提供一種可以追蹤用戶活動行為與研究其資產轉移的方法，企冀能提供給 DeFi 使用者協助與幫助。

金融科技 (Financial Technology, FinTech) 運用科技技術使金融服務變得更有效率，然而，此類金融科技公司在新創立時的目標就是想要取代眼前那些不夠科技化的大型金融企業和體系。因應現今 FinTech 的蓬勃發展，新創企業極想使用科技為金融市場創造更便捷的服務，但由於金融創新可能會與法律相抵觸而受罰，是故監管科技 (Regulatory Technology, RegTech) 就是為了解決目前金融環境所衍伸出來的服務。DeFi 是全球發展 FinTech 技術中最常被討論的新興技術之一，它的核心擁有許多新技術。這些相關技術包含有：人工智慧、區塊鏈、雲端運算，及大數據分析，這也是 FinTech 和 RegTech 的四種核心技術。在本研究中，我們認為可以針對 DeFi 項目方產出的實質價值部分監管。同時，在未來研究上，我們建議針對 DeFi 需要開發一種全新的設計法規，將法規方法納入 DeFi 的協議設計中，此舉將有可能將金融及其監管權力下放到 RegTech 用以確保有效的監督和風險控制。

參考文獻

- [1] Bosu, A., Iqbal, A., Shahriyar, R. and Chakraborty, P., (2019). Understanding the motivations, challenges and needs of blockchain software developers: a survey. *Empirical Software Engineering*, 24(4): 2636-2673.
- [2] Pinna, A., Ibba, S., Baralla, G., Tonelli, R. and Marchesi, M., (2019). A massive analysis of Ethereum smart contracts empirical study and code metrics. *IEEE Access*, 7: 78194-78213.
- [3] Wood, G., (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151: 1-32.
- [4] Swan, M., (2015). *Blockchain: Blue print for a new economy*. O'Reilly Media, Inc.
- [5] Atzei, N., Bartoletti, M. and Cimoli, T., (2017). A survey of attacks on Ethereum smart contracts (SoK). In M. Maffei and M. Ryan (Eds.), *Proceedings of 6th Conf. on Principles of Security and Trust*, 10204: 164-186.
- [6] Szabo, N., (1997). The idea of smart contracts. Retrieved from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html
- [7] Buterin, V., (2014). A next-generation smart contract and decentralized application platform, White paper, Ethereum Foundation.

附錄 A：BigQuery 搜尋前 10 名交易次數最多 ERC20 代幣及 ERC721-NFTs 之 SQL 語法

搜尋前十名交易次數最多 ERC20 代幣之 BigQuery SQL 語法

```
SELECT contracts.address, COUNT(1) AS tx_count
FROM `bigquery-public-data.crypto_ethereum.contracts` AS contracts
JOIN `bigquery-public-data.crypto_ethereum.transactions` AS transactions
    ON (transactions.to_address = contracts.address)
WHERE contracts.is_erc20 = TRUE
GROUP BY contracts.address
ORDER BY tx_count DESC
LIMIT 10
```

搜尋前十名最受歡迎的 ERC721-NFTs 之 BigQuery SQL 語法

```
SELECT contracts.address, COUNT(1) AS tx_count
FROM `bigquery-public-data.crypto_ethereum.contracts` AS contracts
JOIN `bigquery-public-data.crypto_ethereum.transactions` AS transactions
    ON (transactions.to_address = contracts.address)
WHERE contracts.is_erc721 = TRUE
GROUP BY contracts.address
ORDER BY tx_count DESC
LIMIT 10
```

附錄 B：以太坊區塊鏈上以 Solidity 語法撰寫之智能合約程式碼簡易範例

```
pragma solidity ^0.4.18;
contract leoSmartcontract { string public name =
hex"e98099e698afe4b880e5808be6b8ace8a9a6";
// hex 這是一個測試
function nameBytes() constant public returns (bytes) {
    return bytes(name);
}
function nameLength() constant public returns (uint) {
    return bytes(name).length;
}
}
```

附錄 C : 0.PickleFinance_Pickle.Power 之 PostgreSQL 語法

```

SELECT
CASE when amount < 100 then 'other'
      else CONCAT('0x', SUBSTRING(address::text, 3)) END as addressNames,
amount as univ2_staked
FROM
(
SELECT
"address",
sum(amount) as amount
FROM
(
--deposits
SELECT "from" as "address",
CASE WHEN "to" = '\xbD17B1ce622d73bD438b9E658acA5996dc394b0d'
      THEN value/1e18 ELSE 0 END AS amount
FROM erc20."ERC20_evt_Transfer"
WHERE contract_address = '\xdc98556Ce24f007A5eF6dC1CE96322d65832A819'
UNION ALL
--withdrawals
SELECT "to" as "address",
CASE WHEN "from" = '\xbD17B1ce622d73bD438b9E658acA5996dc394b0d'
      THEN value/1e18*-1 ELSE 0 END AS amount
FROM erc20."ERC20_evt_Transfer"
WHERE contract_address = '\xdc98556Ce24f007A5eF6dC1CE96322d65832A819'
      ) as raw
group by 1
order by 2
) as holdings
where amount > 0.000000001
order by 2 desc

--pickle token          x429881672b9ae42b8eba0e26cd9c73711b891ca5
--unipool pickle/eth    xdc98556Ce24f007A5eF6dC1CE96322d65832A819
--UNiv2 power          xbd17B1ce622d73bD438b9E658acA5996dc394b0d
    
```

附錄 D : 0.HarvestFinance_mTSLA+UST 之 PostgreSQL 語法

```

SELECT
CASE when amount < 100 then 'other'
      else CONCAT('0x', SUBSTRING(address::text, 3)) END as addressNames,
amount as univ2_staked
FROM
(
SELECT
"address",
sum(amount) as amount
FROM
(
--deposits
SELECT "to" as "address",
CASE WHEN "from" = '\xC800982d906671637E23E031e907d2e3487291Bc'
THEN value/1e18 ELSE 0 END AS amount
FROM erc20."ERC20_evt_Transfer"
WHERE contract_address = '\xC800982d906671637E23E031e907d2e3487291Bc'

UNION ALL
--withdraw
SELECT "to" as "address",
CASE WHEN "from" = '\xC800982d906671637E23E031e907d2e3487291Bc'
THEN value/1e18*-1 ELSE 0 END AS amount
FROM erc20."ERC20_evt_Transfer"
WHERE contract_address = '\x5233349957586a8207c52693a959483f9aeaa50c'
) as raw
group by 1
order by 2
) as holdings
where amount > 0.000000001
order by 2 desc

-- mTSLA-UST :          x5233349957586a8207c52693a959483f9aeaa50c
-- Valut address:       xC800982d906671637E23E031e907d2e3487291Bc
-- burn                  x0000000000000000000000000000000000000000000000000000000000000000

```