Regular Paper

Communications of the CCISA
Vol. 27 No. 3 Aug. 2021

具隱私強化之分散式資料加密交易平台

李怡萱[1*]、左瑞麟[2]
[1]政治大學資訊科學系、[2]政治大學資訊科學系
[1]107971014@nccu.edu.tw、[2]tsoraylin@gmail.com

摘要

在網路發達的現代，資訊已經不限於以紙本形式存在，數位化的資訊也成為極其重要的資產，越來越多資訊分享和交易以數位形式出現在網路上，隨之而來的像是資料與交易安全性，使用者的隱私等多方面存在許多隱患，然而現有的資料交易平台並不完全可以信任，集中式儲存對使用者隱私和成本有負面影響，現行的去中心化存儲解決方案因為沒有可行的運作模式而缺乏節點的參與，資料的提供者也缺少對資料交易權的掌握。

本研究提出使用區塊鏈和星際文件系統 (IPFS) 等多個技術結合的具隱私強化之分散式資料加密交易平台，資料部分利用代理人重加密技術進行保護並保存於 IPFS 中，結合儲存證明進行驗證，實現安全且可靠的存儲、交易過程結合環簽章與隱身地址保障交易雙方身分隱私，此外也有適當的獎勵來激勵節點的運作，後續在相關研究章節也對一些現行的系統進行評比，在這些技術的支持下為交易平台市場提供改進的參考。

關鍵詞：資料交易平台、環簽章、隱身地址、儲存證明、代理人重加密、IPFS

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 27 No. 3 Aug. 2021

Decentralized data encryption trading platform with enhanced privacy

Yi-Hsuan Li[1*], Raylin Tso[2]
[1]Department of Computer Science, National Chengchi University, Taipei, Taiwan
[2]Department of Computer Science, National Chengchi University, Taipei, Taiwan
[1]107971014@nccu.edu.tw, [2]raylin@cs.nccu.edu.tw

Abstract

In the modern era when the Internet is developed, information is no longer limited to the existence of paper, and digital information has become an extremely important asset. More and more information sharing and transactions appear on the Internet in digital form. There are many hidden dangers in many aspects such as data and transaction security, user privacy, etc. However, the existing data transaction platform is not completely trustworthy. Centralized storage has a negative impact on user privacy and cost. The current decentralized storage solutions do not have a good operating model and lack the participation of nodes, and the data provider does not have control over the right to data transactions.

This research proposes a decentralized data encryption trading platform with enhanced privacy that uses a combination of multiple technologies such as blockchain and Inter Planetary File System (IPFS). The data part is protected by proxy re-encryption technology and stored in IPFS, combined with storage certificates for verification. Achieve safe and reliable storage, the transaction process combines ring signatures and stealth addresses to protect the identity and privacy of both parties in the transaction. In addition, there are appropriate rewards to incentivize the operation of the node. In the follow-up related research chapters, some current systems are also evaluated. In these technologies with the support of the trading platform, it provides an improved reference for the trading platform market.

Keywords: Data trading platform, ring signature, stealth address, proof of storage, proxy re-encryption, IPFS

壹、前言

現有的資訊交易網站，如 GBDEx 和 Datarade 等平台，使用者可以進行資訊交易服務，若是採用集中式的方式進行資料儲存，將存在許多安全和隱私問題；而像是許多雲端儲存分享空間，可能會有不誠實的網站管理員能讀取和收集有關用戶的各種資料，並秘密分析和處理使用者資訊，甚至可以通過付款方式連接到用戶身份，以 Dropbox 為例來看用戶的身份甚至可以通過其電子郵件地址、付款資訊或 IP 地址來進行關聯。另外使用 GNUnet 和 Freenet 這樣的分散存儲系統，存儲空間會由網路的其他參與者提供，但缺乏經濟動機來鼓勵參與者貢獻存儲空間而導致搭便車問題，用戶會消耗存儲容量但不願意提供自己的存儲空間。

因此透過密碼學機制實現私人支付，保障使用者身份隱私並將檔案進行加密，提高使用者對資訊交易的控制權，只有交易成功的人才可以獲得完整資訊，增加資料的安全性，並提供有效的獎勵機制，讓分散存儲系統能持續運作下去，解決所謂的搭便車問題，與集中式系統相比，提供發送方和接收方的匿名性，並確保傳輸的安全性，實現資訊交易與共享功能的技術完善為目標。

許多基於雲端的資料分享系統已經發展很多年，儘管提供許多便利的服務但隱私在這些系統中仍是一大問題，美國資安公司 Zimperium 研究調查發現，這些雲端系統因開發者的忽略造成使用者的個資外洩，包括檔案照片、地址、金融資訊或者是醫療紀錄等[1]，而未來隨著網路發展會有更多資料以電子方式呈現，像是電子病歷、電子書或數位產品商家等，緊隨而來的資安問題卻是跟不上發展速度，電子資料交易網站安全讓人越來越不被信任，OGUsers 是一個主要以收集或轉售社群或遊戲帳號等私人用戶交易論壇，但從 2019 年至今為止就有至少三次被駭客入侵導致資料被竊取的情形，並讓部分使用者暴露個人的資訊和細節[2]。

由上面所提的案例來看，都是現有平台遇到的困難進而相關的發展受到阻礙，有些問題在傳統的方式下很難解決，需要一種新的技術來改變現狀，在此背景之下，研究區塊鏈技術與分散式儲存的特性，並嘗試將相關技術結合與應用，構建一個新的型態，並採用密碼學技術保障交易者的隱私與資料的安全性，以此來解決現有平台安全與隱私不足的問題。

貳、文獻探討

2.1 區塊鏈 (Blockchain)

區塊鏈是一項將許多不同領域集合起來的技術，大致分為三種類型，公有鏈、私有鏈與聯盟鏈，公有鏈上任何人都可以查看交易紀錄與規則；私有鏈則有限制一般人不能

使用；而聯盟鏈介於公有鏈與私有鏈之間，為兩個機構之間的交流平台[3]，目前公有鏈上主要的標準有 ERC20、TRC20 與 Omni，不同標準的鏈之間是無法進行轉換，所以假設選擇 ERC20 公有鏈就要提供 ERC20 的錢包地址來進行交易，若提供錯誤的地址則交易就會錯誤，在鏈上若要將交易協議條款透過電腦自動化執行則要編寫智能合約。智能合約於 1990 年初期由 Nick Szabo 提出，但當時技術不及發展沒有得到太多的迴響，直到近年才隨著區塊鏈技術興起，區塊鏈平台提供多方可信任的網路共享資料庫，智能合約使用這些共享資料，執行應用程式進行交易與資產移轉，2015 年推出的以太坊 (Ethereum) 就強調智能合約為其平台特色並提供執行環境，才讓所有人開始注意到這項技術的重要性[4]，甚至視其為「區塊鏈 2.0」里程碑的重要一環。

2.2 環簽章 (Ring signature)

在 2001 年環簽章由 Rivest，Shamir 和 Tauman 等人[5]提出，簽署過程中因會形成一個環故被稱為環簽章。而筆者認為把環簽章跟區塊鏈結合後最成功的應用就是門羅幣 (Monero) 。門羅幣以 CryptoNote v2.0[6]為基礎並於 2014 年 4 月推出以注重隱私聞名，其中由 Nicolas 提出一次性環簽章，這個方法是從 Fujisaki 和 Suzuki 的可追溯環簽章改編而來[7]，在發展過程中以此為基礎進行比較與實驗後證明，由 Liu 等人提出 LSAG (Linkable Spontaneous Anonymous Group Signatures) 簽章方案[8]，經 Adam Back[9]改編後此簽章在存儲空間上縮減為原來的一半，此外也可預防雙花問題。而門羅團隊選擇的基礎數位簽章演算法為 EdDSA (Edwards-curve Digital Signature Algorithm) ，該演算法是一種類似 Schnorr 的數位簽章方案由 D.J.Bernstein 等人提出[10]，與比特幣的演算法 ECDSA 一樣是基於橢圓曲線離散對數問題，雖然 ECDSA 可能是目前最廣泛使用的橢圓曲線演算法但 EdDSA 所具有的特性，如速度快、產生較小的密鑰和簽章與避免隨機數重用的可能性[11]，讓門羅幣選擇 EdDSA 方案作為演算法應用在 LSAG 環簽章上，也是本研究所使用的方法，總結來說環簽章成功的讓發送者匿名，也因為其中包含的每個身份都具有相同的機率成為交易真正的發送者，增強交易的不可追溯性。

2.3 隱身地址 (Stealth addresses)

隱身地址的概念首先由比特幣論壇成員 ByteCoin[12]提出，由 Nicolas 在 CryptoNote v2.0[13]中加以改進，最終在門羅幣中被使用[14]，發送者利用隨機數和接收者的公鑰，為每個輸出導出新的臨時公鑰，在不知道與原始公鑰相關聯的情況下，無法將導出的一次性公鑰（稱為目標密鑰）和接收者的原始公鑰進行鏈接，而接收者可以通過自己的私鑰和發送者在交易中的公鑰來恢復相對應的私鑰，證明是真正的接收者，但是一個錢包只能管理一個地址，代表接收者若要跟很多人交易，必須將相同的地址同時分享給不同的發送者。

2.3.1 子地址 (Subaddress)

為了解決上述問題將使用子地址[15]方案，接收者可以根據需要讓主地址產生無數個子地址，每個子位址都可以單獨接受交易，並且所有交易的金額都存儲在同一個錢包，子地址之間不會互相關聯，也不會鏈接到發送者的主地址，假設 Alice 要與 Bob 進行交易，符號說明如表一，過程說明如下：

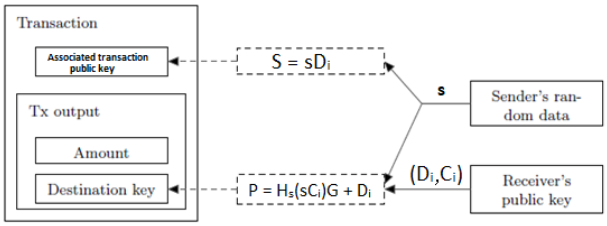
表一：子地址符號說明表

符號設定	說明
F_q	有限域
d	有限域中的一個元素
$E: -x^2 + y^2 = 1 + dx^2y^2$	E為橢圓曲線方程式 (EdDSA)
G	基點
s	隨機數值 $s \in [1, l-1]$，$S = sG$
$(sk, pk) = (a, A)$ $(sk, pk) = (b, B)$	$A = aG$ $B = bG$
H_s	加密雜湊函式 $\{0,1\}^* \rightarrow F_q$

1. Bob 的主地址是 $(A, B) = (aG, bG)$ 且於任何地方都沒公開，後續將使用主地址來產生子地址。
2. Bob 會產生一個列表，該表由子地址中使用的純量組成，從中選擇一個不在列表中的純量 i (不一定要隨機)，並產生隨機數值 r 與 $R=rG$，計算以下內容：

   $$D_i = B + H_s(aR, i)\,G, \qquad C_i = aD_i$$

   Bob 另外產生一個紀錄 $D_i \mapsto i, R$ 的對應表，紀錄每一筆 D_i 是由哪一個純量與隨機數所計算出來的值。
3. 假設 Alice 與 Bob 要進行交易，Bob 公佈他的兩把子地址公鑰 (D_i, C_i)。
4. Alice 產生一個隨機數值 s，計算一次性公鑰 $P = H_s(sC_i)\,G + D_i$ 作為輸出目的地，並將值 $S = sD_i$ 作為交易的一部分公開後進行交易如圖一。



圖一：隱身子地址概念圖

5. Bob 首先計算 $D' = P - H_s(aS)\,G$ 來檢驗 $D' = D_i$，方式如下：

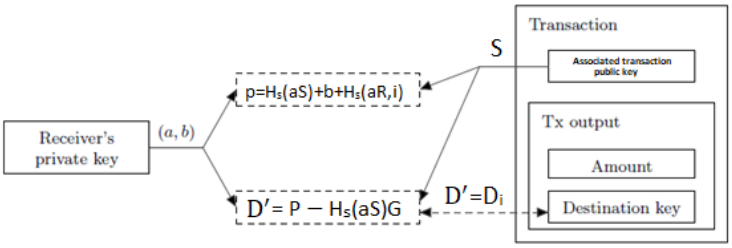
   $$P - H_s(aS)\,G$$

$$=H_s(sC_i)\,G + D_i - H_s(a(sD_i))\,G = H_s(sC_i)\,G + D_i - H_s(s(aD_i))\,G = H_s(sC_i)\,G + D_i - H_s(sC_i)\,G$$
$$= D_i$$

如果$D' = D_i$且可以對應到表中的純量 i 與 R，則可以證明這筆交易是發送到 Bob 的子地址（C_i，D_i），如圖二。

6. Bob 仍要確定與公鑰 P 關聯的私鑰 p，計算 $p = H_s(aS) + b + H_s(aR,i)$ ：

$$pG = (H_s(aS) + b + H_s(aR,i))\,G = H_s(asD_i)\,G + bG + H_s(aR,i)\,G$$
$$= H_s(sC_i)\,G + B + H_s(aR,i)\,G = H_s(sC_i)\,G + D_i$$
$$= P$$



圖二：隱身子地址驗證概念圖

7. 如果 Bob 想將零錢發送到自己的主地址 $(A, B) = (aG, bG)$ ，則可以產生主地址的交換公鑰來做到這一點：

$$P_{change} = H_s(aR,i)\,G + B$$

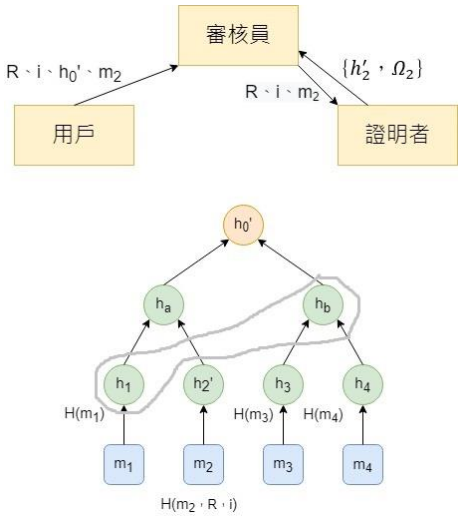
子地址方案讓攻擊者無法確定是否從相同的主地址產生，而使用者只需維護一個本地私有對應表，該表將連結到用於產生子地址的純量索引，對於交易處理中引入必要的更改，但仍不能視為標準錢包的替代品，不可鏈接的子地址代表了一個有效且安全的解決方案，可以解決多個錢包地址的問題，從而使用戶可以確定如何將他們的錢包呈現給其他人以及達到想要的隱私級別。

2.4 儲存證明 (Proof of storage)

隨著雲計算能力的快速發展，近年來雲端存儲服務變得越來越普遍，基於這些服務，使用者能夠將資料儲存在雲服務器上面，從而節省本地存儲空間，雖然減輕了使用者的負擔，但也帶來一定的風險，其中的關鍵是資料損壞，像是雲儲存空間商可能會刪除一些很少使用的資料以節省成本，為了避免這種風險，產生儲存證明 (PoS) 系統，能不下載整個資料的情況下驗證其完整性，存儲證明基礎原則包含三個面向，雲儲存空間商、使用者與審核員。

本文的存儲證明將透過默克爾雜湊樹 (Merkle Hash Tree) [16]的性質來提出證明與驗證，利用根節點的值並通過輔助驗證資訊 (AAI) 讓雜湊值對資料的完整性進行驗證，用戶在每一次挑戰時會產生一個隨機亂數值 R 與計算器 i，並隨機選擇要驗證哪一塊資

料塊，重新計算新的節點與根值h_0'後，將 R、i、h_0'與選擇的資料塊編號提供給審核員，審核員將 R、i 與要挑戰的資料塊編號給予證明者以發起挑戰，證明者透過這些資訊給審核員$\{h_0'，\Omega_2\}$，如果審核員計算出來的根值與先前重新計算的根值h_0'一樣，審核員可以確認有效性否則無效，如下圖三以 m_2 資料塊為例所示。



圖三：利用輔助驗證資訊達成儲存證明示意圖

2.5 代理人重加密 (Proxy re-encryption)

代理人重加密這個概念起源於 Blaze、Bleumer 和 Straussn 在 1998 年的歐洲密碼學年會上提出的方法[17]，這個方案採用混合加密系統，圍繞代理重加密的研究還有許多想法，2017 年 Myers 和 Shull 提出一種代理重加密方法[18]，其中資訊使用對稱式金鑰進行加密，而對稱式金鑰再使用非對稱式金鑰進行加密。代理人重加密應用在許多功能中，像是電子郵件加密後發送、分散式文件系統和智慧財產權保護[19]等用途。

本論文加入代理人重加密技術，以確保資料請求者獲得資料的安全性，由以下五個算法組成 (KeyGen、Enc、ReKeyGen、ReEnc、Dec) ：

1. KeyGen (1^k) → (sk_i，pk_i) :產生密鑰的演算法 KeyGen 輸入一個安全性參數 1^k 並輸出公私鑰對 (sk_i，pk_i) 。
2. Enc (K，m_i，pk_i) → (C_{m_i}，C) :加密演算法 Enc 輸入資料明文 m_i、對稱密鑰 K 和公鑰 pk_i，並輸出用 K 與對稱式加密算法，將 m_i 進行加密而得到密文C_{m_i}，以及使用 pk_i 對 K 進行加密而得到密文 C。
3. ReKeyGen (sk_i，pk_j) →$rk_{i\to j}$:輸入一個私鑰 sk_i (以本論文來說為資料提供者的私鑰) 和一個公鑰 pk_j (為資料請求者的公鑰) ，使用重新加密密鑰算法輸出一個重新加密密鑰$rk_{i\to j}$。
4. ReEnc ($rk_{i\to j}$，C) →C': 重新加密演算法 ReEnc 輸入重新加密密鑰$rk_{i\to j}$和密文 C，並輸出重新加密的密文C'。

5. Dec (sk_j, C_{m_i} ,C') $\rightarrow K$，D_i:解密演算法 Dec 輸入重新加密的密文C'和資料請求者私鑰 sk_j，並輸出密鑰 K，並使用密鑰 K 對密文C_{m_i}解密並獲得原始資料明文 m_i。

這項技術在如今缺乏信任的網路生態與資料共享等領域有非常好的效果，使用者可以不用完全信任代理者，即可把自己的資料進行保存並達到資訊傳送且保密的效果。

2.6 星際文件 (Inter Planetary File System)

星際文件系統 (IPFS) 是一種點對點分散式文件系統，由 Juan Benet 設計該系統，於 2014 年發表白皮書，2015 年正式由實驗室 Protocol Labs 發佈，可以說是一種新型超媒體傳輸協定，目標是將所有裝置連線到同一個檔案系統，進而成為一個全球統一的儲存系統，補充和完善現有的網際網路，達到成為新一代網際網路的願景[20]，目前已知的使用案例，例如政治投票，以巴塞隆納為首府的加泰隆尼亞，於 2017 年舉行脫離西班牙獨立公投，西班牙政府拒絕承認投票結果並對公投網站進行封鎖，而加泰羅尼亞海盜黨隨後將網站架設到 IPFS 上，就算西班牙政府封鎖任何與 ipfs.io 的網路，網站上的資訊還是能被存取、複製，只要下載星際文件的程式，任何人都可以存取系統中的任何內容[21]，除了融合許多強大技術的優點，也因其精巧的架構設計而獲得許多優勢，從技術上來看可以分為多層子系統，這些子系統不是獨立的，它們是堆疊在一起，互相利用各自的屬性，從下到上共七層，分別是身份層、網路層、路由層、交換層、物件層、檔案層、命名層，如圖四。

圖四：IPFS Protocol stack

IPFS 網路上的節點可以自動暫存下載過的資源，並使這些資源提供其他節點使用，但是儲存空間是有限的，因此節點需要刪除一些以前緩存的資源，一般來說每小時會進行一次清理為新資源騰出空間，這個過程稱為垃圾回收機制 (Garbage collection) [22]，所以為了確保資料在 IPFS 上永久存在，並且在垃圾回收期間不被刪除，資料可以被固定 (Pin) 到一個或多個 IPFS 節點讓資料長期保留，不會被上面講到的垃圾回收機制清

除，目前也有提供固定服務的公司，例如 Pinata 主要的服務就是能夠更進一步將檔案固定在該公司的節點中，從而提升該檔案的可用性。

參、研究方法與架構

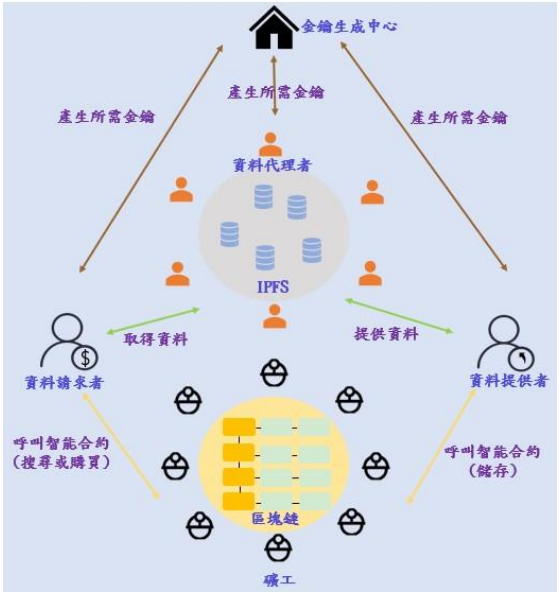
3.1 設計概要

現今的資料交易平台上人們可以方便且快速的取得自己想要的資訊，但一些缺點慢慢浮現，隱私保護強度不夠、集中式伺服器信賴與成本問題，開始讓使用者尋求更好的解決方式，本文藉由區塊鏈的優點以資料交易平台為例，從技術層面提出改進方案，其中為了保證交易過程中交易者隱私性與資料安全性，本研究利用環簽章、隱身地址與代理人重加密等密碼學技術進行保護，並將交易過程中加密後的資料保存在 IPFS 分散式存儲上，實現資料的安全可靠存儲，從而保證了在分散式區塊鏈網路上進行資料交易活動的安全性外，也能同時得益於區塊鏈技術的優良性質。

3.2 系統架構

本文的資料交易平台架構如下圖五，系統架構主要由六個元素組成：資料提供者、資料代理者、資料請求者、密鑰生成中心、礦工和智能合約。

1. 資料提供者：資料提供者販賣或共享的資料，並且可以根據資料請求者的請求主動選擇要不要提供自己的資料。
2. 資料代理者：資料代理者具有提供存儲空間、儲存資料和固定資料功能，主要負責存儲和固定資料，確保在 IPFS 網路上不會離線，並依據智能合約在儲存期限需要提供儲存證明，來證明資料確實存在儲存空間，實現合約後獲得獎勵。
3. 資料請求者：資料請求者可以呼叫智能合約，獲取按照條件搜尋的資料集，透過鏈上的資訊來選擇自己想要的資訊，從分散式網路下載資料，並依照資料提供者制定的價格購買給予獎勵。
4. 密鑰生成中心：負責生成公用參數，並依照不同身份生成所需要的公私鑰對，這些密鑰在代理重新加密過程與發放獎勵中使用。
5. 礦工：在隨機選擇的鏈上進行挖掘，並驗證有效交易將其放置到區塊鏈結構中。
6. 智能合約：設計儲存、搜尋與購買三種合約以用來控制交易的過程。



圖五：平台架構示意圖

本文所設計的具隱私強化之分散式資料加密交易相關優點說明如下：

1. 資料提供者將想要販售的資料加密後上傳至 IPFS 得到文件地址，而資料代理者確保資料於儲存期限內不會消失。
2. 藉由代理人重加密讓資料請求者從 IPFS 網路下載資料與相關資訊，該資料僅請求者能解密。
3. 交易時保障使用者身份隱私，透過密碼學機制能確保雙方的身份不會讓曝光。
4. 有效的獎勵機制讓分散存儲系統能持續運作下去解決搭便車問題，其中資料提供者因為販售資料而得到獎勵；資料代理者因為提供儲存空間而得到獎勵；資料請求者透過平台得到想要的資料；礦工會因為維護整個區塊鏈與驗證提供算力得到獎勵。
5. 使用儲存證明的特性保障資料正確性外也能抵抗生成攻擊。

系統相關符號設定與說明，如表二：

表二：系統符號說明表

符號設定	說明	角色
(PK_a, SK_a)	身份用公私鑰	資料提供者
(pk_b, sk_b) (pk_c, sk_c)	交易用公私鑰	
(pk_d, sk_d)	加密用公私鑰	
(pk_{b-1}, pk_{c-1})	子地址用公鑰	
(PK_e, SK_e)	身份用公私鑰	資料代理者
(pk_f, sk_f) (pk_g, sk_g)	交易用公私鑰	

(pk_{f-1}, pk_{g-1})	子地址用公鑰	
(PK_h, SK_h)	身份用公私鑰	資料請求者
(pk_i, sk_i) (pk_j, sk_j)	交易用公私鑰	
(pk_k, sk_k)	加密用公私鑰	
(pk_{i-1}, pk_{j-1})	子地址用公鑰	

3.2 流程設計

流程設計共分三個部份儲存資料、搜尋資料和購買資料等三個階段，每位使用者都要先進行註冊，再依不同的需求選擇角色，以下針對流程部份進行說明:

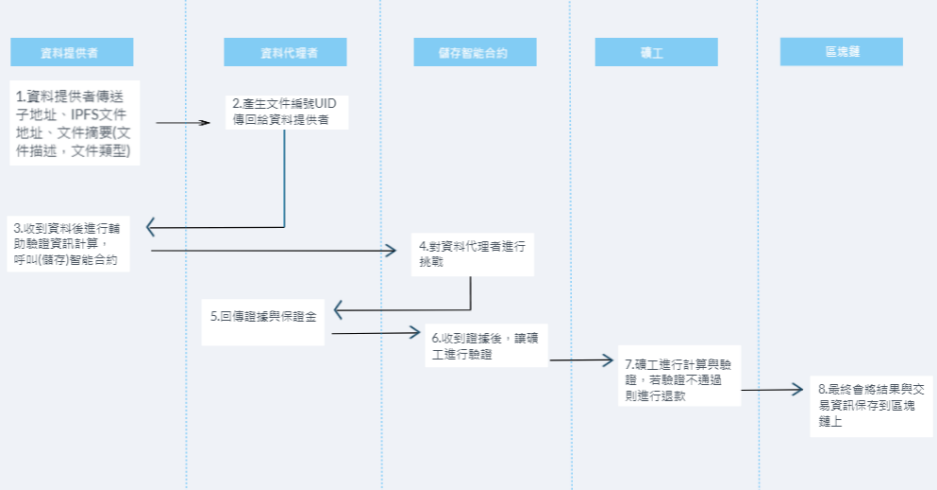
首先每個使用者進行註冊後登入系統，如果要儲存資料，則選擇成為資料提供者 (provider) ，並根據以下步驟進行前置作業：

1. 資料提供者將產生兩對專門在交易上使用的交易用公私鑰 $(pk_b, sk_b、pk_c, sk_c)$ 、對稱密鑰 (K) 與負責對資料進行代理重加密的加密用公私鑰 (pk_d, sk_d) 。
2. 資料提供者將使用對稱密鑰 K，對資料 (m) 進行加密得到密文 $(C1)$ 後，上傳到 IPFS 網路得到文件地址。
3. 資料提供者使用加密用公鑰 pk_d 對 K 進行加密得到加密後的密文 $(C2)$ ，並在系統上廣播存儲需求 (包含資料大小和存儲時間) 來搜索資料代理者。
4. 資料代理者會公布他們各自儲存空間的價格與以及利用交易用公鑰計算出相對應的子地址用公鑰 (pk_{f-1}, pk_{g-1}) 。
5. 資料提供者選擇出資料代理者後開始進行資料儲存。

儲存資料流程設計如圖六，步驟說明如下：

1. 資料提供者使用環簽章以及代理者的子地址用公鑰計算隱身地址傳送資料，資料包含資料提供者子地址用公鑰 (pk_{b-1}, pk_{c-1}) 、IPFS 文件地址與文件摘要 (文件描述，文件類型) 傳給資料代理者。
2. 資料代理者在驗證交易後，將資料從 IPFS 上保存於本地並固定於 IPFS 網路，透過環簽章以及提供者的子地址用公鑰計算隱身地址將從文件摘要產生的文件編號 (UID) 回傳，並將文件編號、文件摘要與 IPFS 地址紀錄成對應表儲存在本地。
3. 資料提供者收到資訊後產生一個亂數值 (r) ，並選擇要驗證的子節點，使用亂數值 (r) 與計算器 (count) 產生新的默克爾雜湊樹根值 (R) 後，利用環簽章呼叫儲存智能合約挑戰資料代理者進行儲存證明驗證，並支付儲存空間費用，合約會將空間費用凍結。
4. 儲存智能合約有新的根值與相關驗證資訊後，讓資料代理者依據資料提供者選擇的子節點、亂數與計算器產生證據。

5. 當儲存智能合約得到資料代理者的證據與保證金後，由礦工進行計算與驗證，最終會將結果與交易資訊保存到區塊鏈上。

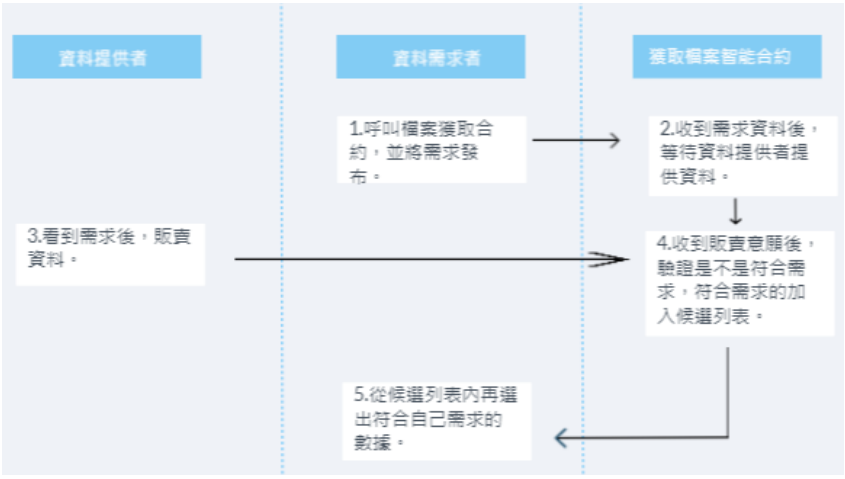


圖六：儲存資料流程設計流程圖

如果要搜尋資料，使用者註冊後選擇成為資料需求者，搜尋資料流程設計流程如圖七：

1. 資料需求者利用環簽章呼叫搜尋智能合約，發布自己的資料需求 (資料類型、搜尋資料截止日期、候選資料的數量、最低要求的資料分數限制) 。
2. 資料提供者可以隨時查詢獲取檔案合約有哪些項目，依照意願決定是否販賣自己的資料。

資料提供者決定販賣資料後，搜尋合約將會開始檢查是否滿足資料需求者定義的要求，建立符合需求的候選列表。



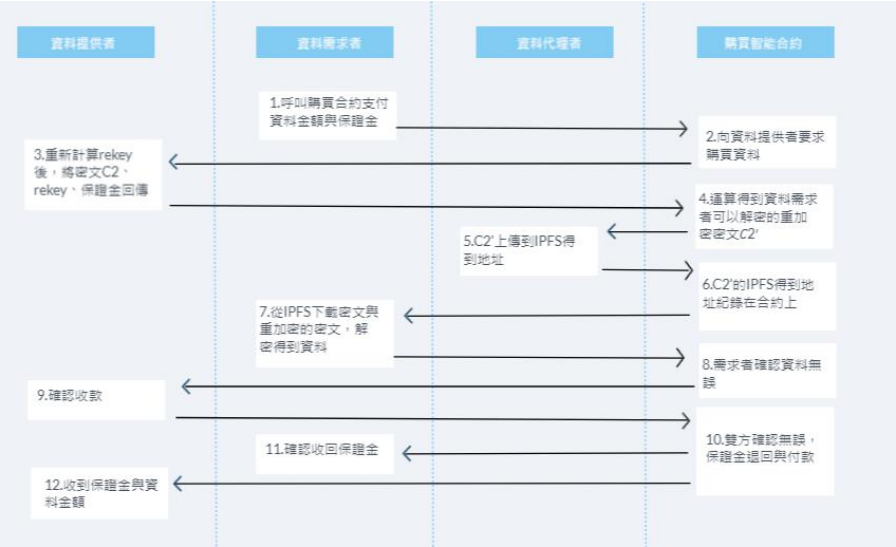
圖七：搜尋資料流程設計流程圖

以下為購買資料步驟與流程如圖八：

1. 資料需求者根據搜尋合約篩選出來的候選列表，來決定要購買那些資料後，用環簽

章呼叫購買智能合約，另外產生加密用公鑰（pk_k）後執行 MAD (相互保證銷毀) 交易支付保證金，合約向資料提供者要求購買資料。

2. 資料提供者根據自己的加密用私鑰 sk_d 與資料需求者的加密用公鑰 pk_k，算出代理重加密密鑰 $rk_{d\to k}$。
3. 資料提供者將重加密密鑰 $rk_{d\to k}$ 與密文 $C2$ 回傳給購買合約，購買合約運算得到資料需求者可以解密的重加密密文$C2'$然後將$C2'$傳給資料代理提供者。
4. 資料代理者因為儲存合約會一直連線 IPFS 網路，所以直接將$C2'$上傳到 IPFS 網路並固定住，然後將 IPFS 的地址傳回給合約。
5. 資料需求者從 IPFS 下載密文 $C1$ 與重加密的密文$C2'$，使用自己的加密用私鑰 sk_l 解密密文$C2'$得到對稱密鑰 K，再使用 K 解密密文 $C1$ 並獲得原始資料 m，確認無誤後支付獎勵給資料提供者。
6. 資料需求者後續將針對這份資料進行評分與評語並記錄在側鏈上。



圖八：購買資料流程設計流程圖

儲存合約在最後儲存期限到期前，會再進行一次儲存證明驗證程序，礦工驗證後才會將凍結的儲存空間費用給予資料代理者，並退回保證金，若沒驗證過則透過提供者子地址用公鑰進行退款，而資料代理者則會尚失保證金，若最後一次儲存證明驗證程序，資料提供者並未提供相關驗證資訊，則直接給予代理者儲存空間費用與退回保證金。

肆、分析與比較

4.1 安全性分析

網路發展迅速，越來越多商品數位化，但是現有的網絡交易幾乎都需要依賴第三方

來處理交易訊息，這種商業模式所帶來的問題如:市場效率低、成本高、缺乏隱私保護等問題，非常需要新的技術來改變這種現在的模式。在此背景下，本文提出了基於區塊鏈和 IPFS 技術的資訊交易平台，為了保證交易過程中使用者隱私與資料的安全，採用密碼學的技術來達到目的，相關分析論述如下:

1. 身份匿名性：對於攻擊者來說能枚舉使用者的身分是一件重要的事情，本文實現用戶身份的隱私，除採用匿名身份註冊模式讓資料提供者的真實身份與資料不會鏈接外，於交易過程中採用環簽章與隱身地址的特性，讓攻擊者就算監控網路也無法將交易的錢包地址關連至某個人在真實世界中的身分。
2. 資料機密性和正確性：資料提供者在提供資料時，資料被密鑰加密存儲在代理與 IPFS 網路上，因此代理無法獲取資料的明文，也不能修改或濫用提供者的資料，代理人重加密可確保機密性在傳輸過程中不會被篡改，只有相對應私鑰的請求者才能解密得到明文，而儲存證明也可以保障資料的正確性。
3. 抵抗生成攻擊：生成攻擊一詞是出現在 Filecoin 白皮書[23][24]中，惡意礦工宣稱要存儲大量的資料，但反而使用別的方式有效產生儲存證明，如果這個證明比宣稱要存儲的資料還小，那麼惡意礦工就可以取得更多報酬。在我們的系統中，資料提供者若長期將同一份文件放置於系統上，勢必會持續跟許多資料代理者交易但不一定都是同一位，假設某一位資料代理者透過分析得知這份文件在區塊鏈上所有曾經證明過的儲存證明，則當審核方發起挑戰時，有可能使用曾經證明過的證據，但其實並未真正儲存資料，為防止這項攻擊本文選擇每次證明都會使用亂數生成新的證據，即使知道以前的證明也不能拿來使用，故達到有效防禦。
4. 交易安全性：在進行數位交易時有可能會出現兩種情況，一種是惡意的買方，在取得資料後故意不給報酬導致賣方損失；另一種是買方已支付報酬但賣方故意不給資料，從上述情況來看買方不能先支付報酬，賣方不能先給產品，為避免此問題，本文採用相互保證銷毀交易機制，交易時皆互相支出保證金，這筆資金需要雙方皆同意才能各自歸還，若有一方不誠實則會導致付出更多成本，若是正常的交易者應該會以自己的最大利益來做出選擇，故達到交易安全。

4.2 現行機制比較

Filecoin 是一個與實體經濟緊密結合的區塊鏈專案，擁有去中心化的儲存市場與檢索市場，用戶向礦工支付費用以獲得儲存和檢索服務；而礦工幫助用戶運算與執行以此獲得報酬，而說到 Filecoin 不得不提到 IPFS 協議，現實中許多人會認為這兩項專案是相等的，但其實之間有很大的不同，IPFS 是非區塊鏈專案，主要是解決資料分發與定位問題類似 HTTP 協議；Filecoin 則是區塊鏈專案，一個基於區塊鏈的分散式儲存協議，主要是解決資料儲存問題與降低儲存成本，從技術的層面來看沒有依賴關係，也就是說這兩項技術都可以獨立運作，但是結合執行卻能互補雙方的缺點，成更強大的網路讓雙方

都能互相得利，根據現行機制 Filecoin 與本系統相比雖然有些許概念類似，但也有 Filecoin 所沒關注到的方面，例如:在今年 3 月 17 日 Filecoin 被發現程式碼存在遠端程式呼叫 (RPC) 嚴重漏洞[25]，由名叫 6Block 的交易團隊利用這個漏洞，在虛擬幣交易所幣安中的帳戶兩次存入同一筆存款，當相同的資金在區塊鏈上花費兩次時，就會發生雙重花費，而這種情況也可以被稱為雙重存款。本文改進 Filecoin 的缺點並參考其優點加入本平台，其中身份隱私性的部分使用環簽章與隱身地址；資料安全性的部分為代理人重加密；預防雙花問題使用 LSAG 環簽章的金鑰映像功能讓資料交易平台更加安全與穩定如下表三所示：

表三：本平台與 Filecoin 比較表

	本論文平台	Filecoin
身份隱私性	有	無
資料安全性	有	無
激勵機制	有	有
預防雙花問題	有	無

伍、結論

如今缺乏信任的網路環境中，去中心化的模式將會有越來越多的應用，區塊鏈、智能合約、IPFS 等分散式技術也將在其中發揮出重要的作用，在目前的環境集中式還是比較廣泛，但區塊鏈以及智能合約的應用會逐步增加，目前也越來越多新創公司在使用區塊鏈結合其他領域或技術嘗試開展一系列新專案。

本論文研究區塊鏈、IPFS 等技術的資料交易平台也是在這方面的一次簡單的構想

- 利用代理重加密技術來保障資料的安全、智能合約來執行邏輯、IPFS 存儲加密後的資料，保證資料的安全可靠，並減少存儲成本。
- 交易方面以環簽章和隱身地址來保障交易雙方身份，並用儲存證明來保障資料被正確儲存在 IPFS 的節點上，優化系統，更符合實際應用。

本研究提出的具隱私強化之分散式資料加密交易平台方案還可以有改進的地方，像是防禦 IP 地址關聯攻擊未來若是加上蒲公英網路的應用，或許能抵抗 IP 地址關聯攻擊。

[誌謝]

本研究由科計部計畫 MOST 110-2218-E-004 -001 -MBK、MOST 109-2221-E-004 -011 -MY3 及 MOST 109-3111-8-004 -001 -補助支持，特此誌謝。

參考文獻

[1] 陳曉莉，“研究：使用雲端儲存的行動程式中有 14%因開發者配置錯誤而曝露用戶資料或架構資訊“，https://www.ithome.com.tw/news/143070，2021/3/5

[2] Duncan Riley, “Stolen credit card forum hacked and user details published online” (2021/3/28)

[3] Ennio Y.Lu ，“企業該選擇哪種鏈?-- 公有鏈 vs. 私有鏈 vs. 聯盟鏈”,https://www.blocktempo.com/which-blockchain-analysis/,2018/12/12

[4] 陳恭,“智能合約的發展與應用”, 財金資訊季刊第 90 期,pp.33-34,2017

[5] Ronald L.Rivest,A. Shamir and Y. Tauman,“How to leak a secret”,ASIACRYPT 2001,LNCS 2248,pp.552-565,2001

[6] Van Saberhagen, N.,“CryptoNote v 2.0.”,pp.1-26,2013

[7] Fujisaki E.,Suzuki K., “Traceable Ring Signature”,Public Key Cryptography–PKC 2007.PKC 2007.Lecture Notes in Computer Science,vol 4450.Springer，pp.181-200,2007

[8] Liu J.K.,Wei and V.K.,Wong D.S. “Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups.”,Information Security and Privacy.ACISP 2004.Lecture Notes in Computer Science,vol 3108.Springer,pp.325-335,2004。

[9] Adam Back, “Ring signature efficiency” https://bitcointalk.org/index.php?topic=972541.msg10619684, (2015.3.1)

[10] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe and Bo-Yin Yang. “High-speed high-security signatures. J. Cryptographic Engineering”, 2012.

[11] Nick Mooney, “WHAT'S AN EDDSA? ”,https://duo.com/labs/tech-notes/whats-an-eddsa, (2020/5/14)

[12] ByteCoin,“Untraceable transactions which can contain a secure message are inevitable. ”,https://bitcointalk.org/index.php?topic=5965.0, (2011/4/17)

[13] N.Van Saberhagen., “Cryptonote v2.0. ”,https://cryptonote.org/whitepaper.pdf, (2013)

[14] Yu, G., “Blockchain Stealth Address Schemes. ”,IACR Cryptol. ePrint Arch.,pp.1-10, (2020)

[15] Aldanov,I., “CryptoNote.+ ”,pp.3-4, (2018)

[16] Wilkinson, S., Boshevski, T., Brandoff, J.and Buterin, V., “Storj a peer-to-peer cloud storage network. ”, pp.3-5, (2014)

[17] Blaze, M., Bleumer, G. and Strauss, M., “Divertible protocols and atomic proxy cryptography”,In International Conference on the Theory and Applications of Cryptographic Techniques,pp.127-144, (1998)

[18] Myers, S. A. and Shull, A., “Efficient Hybrid Proxy Re-Encryption for Practical

Revocation and Key Rotation",pp.1-69, (2017)

[19] Taban, G., Cárdenas, A. A. and Gligor, V. D., "Towards a secure and interoperable DRM architecture",In Proceedings of the ACM workshop on Digital rights management,pp.69-78, (2006)

[20] 董天一、戴嘉樂、黃禹銘，*IPFS 原理與實戰*，台北市:碁峰資訊， (2020) 。

[21] How the Catalan government uses IPFS to sidestep Spain's legal,http://la3.org/~kilburn/blog/catalan-government-bypass-ipfs/,2017.09.30.

[22] IPFS DOC-Pin files using IPFS,https://docs.ipfs.io/how-to/pin-files/#three-kinds-of-pins。

[23] filecoin.io,"Filecoin: A Cryptocurrency Operated File Storage Network, ",https://filecoin.io/filecoin-jul-2014.pdf, (2014) .

[24] Protocol Labs, "Filecoin: A Decentralized Storage Network",http://filecoin.io/filecoin.pdf, (2017)

[25] Colin harper, "$4.6M in Filecoin Double Deposited on Binance;Exploit Open on Other Exchanges",https://www.coindesk.com/filecoin-double-deposit-on-binance-exploit-open-other-exchanges, (2021/3/19) .