

國立政治大學資訊管理學系研究所

碩士學位論文

基於區塊鏈智能合約之投資策略跟單媒合系統

Social Copy Trading System based on Smart Contract with  
Blockchain

指導教授：姜國輝 博士

研究生：王少昕 撰

中 華 民 國 109 年 07 月

## 摘要

隨著科技的發達、資料量的暴增，大數據分析已成為了現今許多產業的關鍵技術，若把程式分析模型建立在投資市場中，比起電視上常看到投資分析師的建議更具有客觀性，長期下來，一定能在市場中穩定的獲利。而開發這些程式交易策略的設計者們並不是每一個皆有大量資金來證明其模型之收益，因此決定開發一個平台來讓這些設計者有發揮的空間。

Etoro 是一個投資平台，在上面可以進行各項投資商品的投資，也能複製其他投資者的投資模式，並給予其手續費，達成互利雙贏。不過其平台為傳統集中式資料庫，於網站上之數據與資訊處理流向皆不透明，因此投資者可能會懷疑平台上所顯示之投資相關數據是否真實，進而影響投資風向與缺乏投資信任度。

綜合上述，本研究為如何建立一個投資平台並導入區塊鏈技術，以智能合約為主軸記錄所有數據與相關操作，透過其不可竄改、資訊公開透明、可追溯之特性，讓所有投資相關數據處理流向透明化，進而使投資者對平台更具有信心。平台上主要的投資商品為股票、期貨等，並且新增程式交易策略商品。平台之使用者主要有三種，分別為持有資金的投資者與跟單者，以及研擬程式交易策略的開發者，投資者為具備投資相關經驗且對投資市場有研究者，其可觀察平台上之投資數據決定是否投資，而跟單者為不需具備上述經驗，可觀看其他投資者相關投資過程決定是否跟著投資者做一樣的投資，並給予投資者手續費，最後程式開發者能將其研發之程式交易策略上傳至本平台，投資者入金後將會照著程式訊號來進行投資，使開發者能有一個平台來驗證其模型之效益。

**關鍵詞：**程式交易、投資平台、投資理財、Etoro、區塊鏈、以太坊、智能合約

## Abstract

With the development of technology and the explosion of data, big data has become an important technology in many industries today. If the program analysis model is built in the investment market, it's more objective than the suggestion often seen by investment analysts on television. In the long term, we will definitely be able to make steady profits in the market. However, not every designer who developed these program trading strategies have a large amount of funds to prove the benefits or accuracy of their models, so I decided to develop a platform to give these designers an opportunity to examine their models.

Etoro is an investment platform on which various investment products can be invested. However, Etoro platform uses a traditional centralized system, so the data and information flow on the website are not transparent. Therefore, investors may doubt whether the investment-related data displayed on the platform is definitely true, which will affect the investment direction and the lack of investment trust.

As stated above, this research is how to re-establish an investment platform with blockchain technology. Through its characteristics of immutability, openness, transparency, and traceability, so that all investment-related data processing flows will be transparent, thereby making investors more confident in the platform. The main investment commodities on the platform are stocks, futures, etc., and I specially added program trading strategy products. Programmers can upload their program trading strategies as commodities to this platform. After investors deposit funds, they will invest according to the program signal, so that developers can have a platform to verify the effectiveness of their models.

**Keywords:** Program Trading, Investment & Wealth Management, Investment Platform, Etoro, Blockchain, Ethereum, Smart Contract

# 目次

第一章 緒論.....	1
第一節 研究背景與動機.....	1
一、大數據.....	1
二、策略程式交易.....	1
三、E 投睿(Etoro).....	2
第二節 研究目的.....	4
第三節 論文架構.....	4
第二章 文獻探討.....	5
第一節 程式交易.....	5
第二節 區塊鏈.....	7
一、區塊鏈起源.....	7
二、區塊鏈技術.....	8
三、區塊鏈的特性.....	14
第三節 以太坊.....	15
一、以太坊起源.....	15
二、以太坊優勢.....	16
二、智能合約.....	17
三、智能合約編譯.....	19
四、分散式應用程式(Decentralized Application, Dapp) .....	20
第三章 研究方法.....	22
第一節 研究架構.....	23
第二節 平台與智能合約之互動.....	27
一、會員系統與智能合約之關係.....	27

二、加密貨幣兌換系統與智能合約關係.....	29
三、策略程式設計人與智能合約關係.....	30
四、投資人、跟單人與智能合約關係.....	31
第四章 研究結果.....	33
第一節 系統工具.....	33
一、Node.js .....	33
二、Express 框架 .....	33
三、Web3.js.....	34
四、Database .....	35
五、Metamask .....	36
六、Infura.....	36
七、Remix IDE .....	37
第二節 系統架構.....	38
一、系統元件串接.....	38
二、使用者操作流程.....	39
三、系統運作流程.....	40
第三節 E 投睿(ETORO)問題解決 .....	42
一、揭露非透明之平台投資數據.....	42
二、保證投資策略未被擅自修改.....	42
第四節 智能合約編譯.....	43
一、代理合約 Proxy Contract .....	43
二、策略程式合約 CopyMatch Contract .....	47
第五節 頁面呈現.....	51
一、主頁 .....	51
二、登入、註冊、登出 .....	51

三、登入後主頁.....	52
四、會員資料(帳戶專區).....	53
五、代幣兌換 & 贖回(兌換專區).....	56
六、程式交易專區(被投資者).....	62
七、瀏覽策略程式(策略程式專區).....	70
八、投資專區(投資者).....	71
第五章 結論與建議.....	73
第一節 研究結論.....	73
第二節 未來展望.....	74
第三節 研究貢獻與結語.....	75
第六章 參考文獻.....	76
第一節 英文文獻.....	76
第二節 中文文獻.....	78

## 表次

表 2-1 人為與程式交易比較差異 .....	6
表 4-1 ERC-865 智能合約變數與函式總覽 .....	45
表 4-2 Internal Transaction 智能合約變數與函式總覽 .....	46
表 4-3 策略程式智能合約變數與函式總覽 .....	47

## 圖次

圖 2-1 複式記帳法 .....	8
圖 2-2 分散式帳本 .....	9
圖 2-3 比特幣交易 .....	11
圖 2-4 時間伺服器 .....	12
圖 2-5 Proof of Work .....	13
圖 2-6 Dapp 數量 .....	21
圖 2-7 Dapp 成長數量 .....	21
圖 3-1 策略投資程式平台使用流程架構圖 .....	24
圖 3-2 會員系統與智能合約關係 .....	27
圖 3-3 加密貨幣兌換系統與智能合約關係 .....	29
圖 3-4 策略程式設計人與智能合約關係 .....	30
圖 3-5 投資人、跟單人與智能合約關係 .....	31
圖 4-1 Web3 與 Json-RPC .....	34
圖 4-2 Web3 與以太坊之串接 .....	35
圖 4-3 系統元件串接 .....	38
圖 4-4 使用者操作流程 .....	39
圖 4-5 系統運作流程 .....	40
圖 4-6 委託交易 .....	43

圖 4-7 委託交易驗證流程 .....	44
圖 4-8 主頁 .....	51
圖 4-9 登入、註冊、登出 .....	51
圖 4-10 登入後主頁 .....	52
圖 4-11 關於我 .....	53
圖 4-12 修改資料 .....	54
圖 4-13 交易記錄 .....	55
圖 4-14 兌換專區 .....	56
圖 4-15 歐富寶 API 串接 .....	57
圖 4-16 收據與交易結果 .....	58
圖 4-17 真實貨幣兌換加密貨幣 .....	59
圖 4-18 加密貨幣兌換真實貨幣 .....	60
圖 4-19 Metamask 要求客戶簽署交易 .....	61
圖 4-20 產生簽章與發送確認頁 .....	61
圖 4-21 程式合約總覽 .....	62
圖 4-22 程式上傳區 .....	63
圖 4-23 程式檢視 .....	64
圖 4-24 智能合約部署 .....	65
圖 4-25 智能合約初始化 .....	66
圖 4-26 暫停智能合約 .....	67
圖 4-27 繼續智能合約 .....	68
圖 4-28 終止(刪除)智能合約 .....	69
圖 4-29 策略程式總表 .....	70
圖 4-30 策略程式詳細資訊 .....	70
圖 4-31 投資總覽 .....	71
圖 4-32 終止投資(全數賣出) .....	72



# 第一章 緒論

本章節將介紹研究動機、研究目的與論文架構，說明何謂策略程式交易、E 投睿(Etoro)投資平台以及本研究使用區塊鏈技術的原因。

## 第一節 研究背景與動機

### 一、大數據

21 世紀時，隨著科技發展導致資訊海量暴增，全球確定進入大數據時代。從公司內部的各種運營數據至個人移動終端設備之數據，再到網際網路產生的海量信息數據，全世界無時無刻產生的信息量正在迅速增長。而這些龐大的資料從表面來看或許只是巨量的數據，倘若能有效利用與分析這些資料，或許能帶給人們有用的資訊以輔助決策，因此就有了資料探勘此一名詞，資料探勘是從一系列大量資料中建立模型並分析，從中找出隱藏的特殊關聯性及特徵，藉此提供使用者額外的有用資訊，其帶來的商業價值非常高，因此近年來大數據分析在科技領域中為炙手可熱的議題。

### 二、策略程式交易

策略程式交易利用長期資料統計、數學演算與近年非常火紅的機器學習技術，並使用各種經濟理論模型，分析出交易市場中人類難以發覺的特殊規則，再交由計算機依據這些規則與券商連結、期貨商進行自動下單的動作，是謂一種大數據分析與資料探勘之應用。近年來，由於計算機設備的提升以及資料量的暴增，使得機器學習技術越來越完善，因此有非常多人開始投入撰寫策略程式，畢竟投資這個領域撇除運氣成分，判斷與處理得當是能使人致富的。我們只需要一台電腦、具備程式邏輯與投資相關邏輯，即可開始編譯程式策略，也就是撰寫之門檻不高，幾乎人人皆能寫出屬於自己的一套投資略，但並不是每個人都擁有雄厚的資金能為自己所撰寫之策略進行投資，因此如果能把策略當

成一種商品販售給投資人，投資人只需提供投資金，並照著所購買的商品策略進行投資，若策略判斷得非常精準，投資人也能因而從投資中獲利，達成互利雙贏的局面。

### 三、E 投睿(Etoro)

「投資有賺有賠，高風險高報酬，低風險低報酬」，此句廣告標語時常出現在我們生活周遭，想要從投資中穩定獲取報酬，就必須對投資領域加以鑽研，對此領域不熟悉的人，時常成為賠本與套牢者。

來自以色列的創業公司 Etoro 於 2007 年正式成立，是一家通過實體及時數據讓用戶仿照其他成功交易者進行金融投資社群投資平台。三不五時在許多網站上就會出現 Etoro 的廣告，其內容為有兩名使用者，一名為史蒂夫(Steve)，其畢生都在研究投資相關領域，不論是股票、基金、期貨等皆瞭如執掌，也在投資市場中獲利不少，而另一名為戴夫(Dave)，其對於投資可以說是完全沒有研究，甚至沒有接觸過，戴夫在 Etoro 平台上看到史蒂夫對各項投資商品進行投資並且持續獲利，也跟仿照著史蒂夫的投資策略進行相同的入金金額與商品，最終也跟著史蒂夫一起在投資中獲利。

Etoro 提供用戶各種投資相關的數據圖表，包含每一位使用者先前以及現在的投資相關訊息。用戶根據這些投資訊息可以選擇複製跟單投資(Copytrader)，就是透過關注其他人的投資來進行一樣的投資模式。這一切並不是隨意模仿的，而是用戶可以查看與模仿者的投資歷史訊息，通過投資策略和報酬率來決定是否要模仿他。被模仿者自身的投資報酬率越好的話，其他用戶也能跟著模仿。被模仿的用戶一旦被跟單後，即可向跟單者收取手續費，而跟單者也能透過良好的策略來進行成功的投資，達成互利雙贏。

總體來說 Etoro 是一個自動化程式交易平台，使用者可以在上面直接進行下單投資，並且會把每一次投資的賺賠金額、報酬率與相關資訊顯示給平台使用者觀看並吸引其他跟單者，身為一個跟單者決定要不要跟單的最大指標是為

被跟單者的投資報酬率，從 Etoro 被跟單者的列表中可以觀察到，大部分的被跟單者的投資報酬率皆於正負 20% 的區段內，但有些人的投報率卻可以高達 30%、40%，甚至 50% 以上，點擊進去觀看詳細資料卻只有每個月的投報率與相關資訊，並沒有顯示出每一次的詳細賺賠資訊，這就難免讓人引發聯想：這些投資者有沒有可能跟網站相關人員有掛勾，特意改變數值吸引更多人跟單？投資策略有無在投資期間擅自更改其策略？網站相關人員刻意調高每個人的投報率或其他數值使跟單者願意投資更大的金額以抽取手續費？上述的種種問題其實都是來自傳統集中式資料庫的弊病，大部分的網站若使用集中式資料庫其背後所傳遞的資訊流除了網站管理員外，使用者皆是無法得知的，使用者也無法確定網站資料庫有無被竄改，而網站架設者也很難提供有效的證據。面對於 Etoro 此種投資平台，因為牽涉到大量金錢上的流動與轉換，資料的透明化與公開性顯得特別重要，使用者無法百分之百的確信平台是否公正，暗中坑殺投資人與跟單人也不是不可能。

綜合以上所述，可以使用區塊鏈技術來完全解決這些問題，透過區塊鏈的以下特性：資料難以造假、資料一旦上鏈就無法篡改，安全性高、去中心化，較有公信力、資訊透明化，人人皆可存取等來克服集中式資料庫的弊病，再加上智能合約的使用，讓相關投資數值的計算與紀錄更加公正與透明。我所希望的平台之投資人並不是毫無根據的進行各項決策與投資，因此也有設立策略程式上傳區，讓一般人能透過人工智慧與大數據分析，經過有根據的程式碼與演算法轉變出投資策略，這能使的投資人對於投資更有信心，也能讓沒有大量資金的程式設計者，有機會能驗證其演算法的正確性與商業價值，以及從中獲利。

## 第二節 研究目的

建立一個自動化策略程式交易投資平台，導入區塊鏈技術並實作智能合約，以解決傳統集中式資料庫網站的弊病，讓平台背後資料流向、計算公式、模型等透明化，確立投資相關數值的正確性和檢驗投資策略是否有無擅自更改，使投資人對於整個平台更有信心，另外，設立程式上傳區，讓研究人工智慧、大數據分析之學者能有一個平台販售與推廣自己所撰寫之策略，順便檢視所寫之程式預測正確性與商業價值。

## 第三節 論文架構

本論文共分為五個章節：第一章緒論，說明本論文之研究背景、研究動機、研究目的與論文架構。第二章文獻探討，介紹本研究之相關技術與概念，包含分散式應用程式、以人工智慧開發之策略程式、區塊鏈技術、以太坊以及智能合約。第三章研究方法，詳述本論文之研究流程與架構，以及如何導入區塊鏈技術。第四章研究結果，詳述本論文之平台如何開發與實作，並導入以太坊智能合約技術，使平台與區塊鏈結合並解決緒論所述之問題。第五章參考文獻，列舉所有與本論文相關引述之文獻。

## 第二章 文獻探討

### 第一節 程式交易

姜林杰祐(2009)認定程式交易為投資人透過電腦程式，並模擬歷史資料回測，尋找優質的低風險高報酬之交易策略，再由電腦程式過濾現階段市場上可投資的投資標的並設定買賣價格，最後以電腦程式及時盯盤，提供投資人進出場訊號，但廣義而言，凡是運用電腦，開發程式輔助投資之執行、制定、決策，皆為程式交易之範疇，且不僅限於股票市場。

張碧瑜(2015)研究指出，若程式交易其分析過程有牽涉到具體演算法，也能稱為演算法交易(algorithmic trading)、黑盒交易(black box trading)、自動交易(automated trading)。其藉由設計者所制定的演算法來擬訂交易策略與指令，再透過電腦程式透過交易平台來執行交易之策略。演算法主要以數學、統計為基礎，透過數據分析、資料科學等方法建立交易模型，並且有系統性與紀律性的制定交易策略。

莊尚威(2019)再定義若上述演算法之模型建立有導入人工智慧技術，並透過 AI 技術更迅速的判斷最適之投資策略，再依據市場狀況及投資人的需求進行客製化分析，也能稱為 AI 交易。

近年來，程式交易逐漸盛行並取代傳統的人為交易，姜林杰祐(2009)認為主要原因是對投資人而言，在交易過程中最難克服的是恐懼(該進場而未進場)與貪婪(該出場而未出場)，只要是人一定會想要最大利益與最小損失，進而左右了買賣的判斷，導致血本無歸，因此許多金融機構的專業交易員選擇以邏輯與客觀實證結果為基礎的交易程式做為輔助，以達成長期穩定獲利的目標。表 2-1 為程式交易與傳統人為差異比較，這也是為何程式交易往後能成為主流的原因。

表 2-1 人為與程式交易比較差異

來源：(董寶蘭，2010)

比較內容	人為交易	程式交易
交易策略	主觀、易動搖、貪婪	客觀、理性、數據訊號
分析基礎	人腦基本數據分析	技術與複雜數值分析
監控狀態	長時間人力監控	等待程式訊號
運算速度	緩慢	快速
即時狀況處理速度	猶豫	果斷
交易績效	長期較不穩定	長期較穩定
專業能力需求	高	中
長期獲利	不穩定	穩定
長期交易平均損失機率	60%-70%	30%-40%
交易紀錄模式	人工抄寫	電腦自動化顯示
人才依賴度	高	低
工作時間	人力 8-12H	電腦 24H

姜林杰祐(2009)提到雖然程式交易比起傳統人為交易論效益或是方便性確實優於許多，不過現今程式交易仍有許多缺點導致它發展受限，無法迅速普及，以下為程式交易之缺點：

1. 黑盒子風險：由於程式交易模組對於使用的交易策略，雖會提及但通常不會詳述(如模型架構與參數)，原因為假如不言明，難以取得客戶的信任，甚至產生後續的交易糾紛，但若詳述其運作流程，則會公開設計者之機密，因此產生黑盒子風險。
2. 程式欺騙：當投資人觀看交易模組的分析報告時，其相關數據是否為真也無從得知，可能分析報告造假數據非常完美或是在程式內動手腳，使結果

看起來比實際上好，加上程式模組無公開透明化，導致投資使用後卻不如預期，此黑心程式難以檢驗與避免。

綜合上述，本研究透過區塊鏈技術以及投資平台之設計，使所有程式交易策略投資數據公開透明化，投資者將可以觀看每一個程式交易策略之歷史投資數據決定是否投資，透過這樣的機制，黑心程式長期下來績效一定會非常低落，最終導致無人投資，藉此能有效杜絕黑心程式。此研究還將所有數據寫入區塊鏈，每個人皆可以存取但無法更改，增加數據公正性與投資人信心。透過上述兩種做法能有效解決目前程式交易所面臨的問題。

## 第二節 區塊鏈

### 一、區塊鏈起源

2008 年，一位自稱日裔美國人的 Satoshi Nakamoto(2008)在「metzdowd.com」網站的密碼學專欄中發表了一篇名為《比特幣：一種對等式的電子現金系統》(*Bitcoin: A Peer-to-Peer Electronic Cash System*)的論文。文中闡述了區塊鏈技術、加密技術、P2P 網路、時間戳等的電子交易系統的構架與理念，並描述了電子貨幣比特幣的各種相關論述，上述這種系統相較於傳統的交易是不需要建立在交易雙方誠信的基礎上，也就是透過計算機演算法來取代交易之公證人。根據蔣潤祥、魏長江(2016)所述，論文發表後隔年誕生了比特幣之第一個序號為 0 的創世區塊，隨後便出現序號 1 的區塊並連接創世區塊藉此形成了鏈，也代表著區塊鏈正式的誕生。Satoshi Nakamoto 也實現了第一個比特幣演算法的客戶端程式，並進行首次的採礦(mining)，產生了 50 個比特幣，這表示出以比特幣為主之金融體系正式進軍人們的生活當中。

## 二、區塊鏈技術

區塊鏈是一種新的記帳方式，相較於我們日常銀行所使用的複式記帳法有很大的不同，在未來有機會逐漸取代。根據 Parker(1989)所述，「複式記帳法」起源於中世紀早期中東的猶太人，15 世紀末時，複式記帳法已流傳於各地並成為了人們最主要的記帳方式，這種方式主要目的為讓世界各個銀行的資訊能夠互相流動，並且在銀行間能夠認可彼此的資料，此種記帳法也促使全球貿易以及近代的資本主義興起。

林佳賢(2018)認為複式記帳法最大的特色為所有人的交易紀錄都存在於中介機構或是銀行中，屬於中心化的架構，如圖 2-1 所示，每一筆交易必須透過交易所、中介機構在中心做媒合，此中心保存所有交易紀錄，讓全球金融體系可以相互認證資訊。

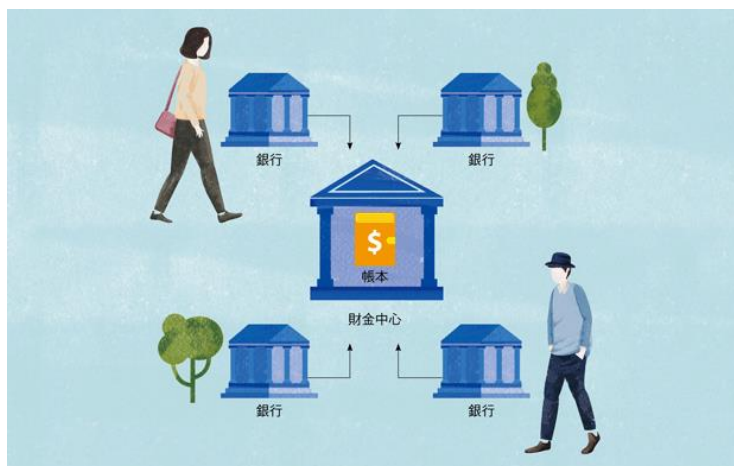


圖 2-1 複式記帳法

來源：(林佳賢，2018)

隨著比特幣(Bitcoin)的出現，開創了一種新的記帳方式，並打破了傳統複式記帳法之核心概念，其以「分散式帳本」(distributed ledger)儲存交易紀錄，跳過中介機構讓所有使用者一起共同記帳與維護，而金融相關操作也不須再透過銀行來達成，達到去中心化的交易系統，如圖 2-2 所示。



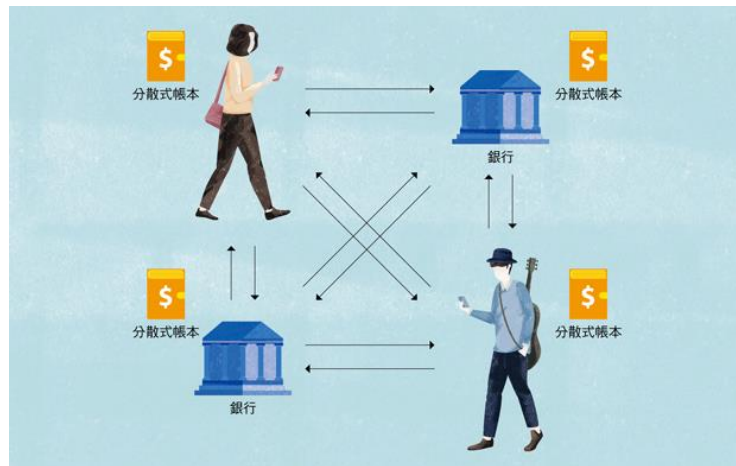


圖 2-2 分散式帳本

來源：(林佳賢，2018)

有兩種角色為分散式帳本的系統中的參與者，分別為交易者與礦工，交易者單純使用金融相關操作，而礦工為驗證交易是否合法之人，並需提供電腦硬體運算的能力。交易者持有的帳本，需經過礦工進行驗證，經區塊鏈上的所有節點確認後部署上鏈，理論上有著不可竄改、可追蹤、加密安全的特性。礦工運算驗證的動作為計算雜湊值(hash)，由於需消耗計算機資源來達到高速運算，因此礦工可獲得比特幣作為酬勞。

交易帳本分散在每個人手中，因此不需中心儲存、認證，所以稱為「去中心化」。無論是個人對個人、銀行對銀行，彼此都能互相轉帳，再也不需透過中介機構，間接的可省下交易成本，而交易帳本經過加密和分散儲存，會比以往更安全，交易紀錄更難以竄改。

以下將介紹比特幣區塊鏈所使用到的相關技術，以及如何達成去中心化的目標：

#### (一)問題(Problems)

根據 Satoshi Nakamoto(2008)所發表的比特幣白皮書中，最主要的目的為建立一個點對點的電子貨幣系統，相較於傳統電子支付系統，其可以不必透過金融機構，允許線上支付貨幣並直接從某一方發起傳送訊號，綜觀來看，可以利用數

位簽章(digital signature)來簽署以驗證這筆交易的發起者，就達到自動化點對點的交易系統，不過雙重支付問題(double spending problem)還是必須得透過第三方驗證才能避免，因此若能解決雙重支付，將會是電子支付革命的開端。Satoshi Nakamoto 提出一個點對點的網路系統來解決上述問題，此網路將每筆交易雜湊串接到一條基於「雜湊工作量證明」所組成的鏈上，形成時間戳記(timestamp)，此鏈將無限延伸，除非重新將鏈上所有工作量證明都計算完，否則鏈上所有交易皆無法被更改，而最長的鏈也可以證明為是多個 CPU 運算能力總和最大的鏈，因此只要多數 CPU 不同時攻擊或控制網路節點時，未受攻擊的安全節點自然就會產生最長且超越其他攻擊者的鏈。網路本身不需太多的基礎建設，交易訊息會依照最大努力原則(best effort basis)廣播出去，網路上的節點可以自由選擇不接受或是重新加入此網路且接受最長的工作量證明所組成的鏈作為節點離開時所發生的交易事件之證明，透過上述可知，交易紀錄為各個節點共同維護，取代了以往所需要的第三方監控驗證，只要攻擊者不能同時控制大部分的節點進行惡意交易，好的節點就能夠共同合作並取得更多的 CPU 運算能力，因此攻擊者的節點就無能力製造出最長的鏈，進而無法被所有節點認可。

## (二)交易(Transactions)

定義一個比特幣為一串電子簽章，每位持有者將欲傳送的下一位持有者公鑰(public key)與前一段交易進行雜湊，將自己的私鑰(private key)簽署此雜湊並放入貨幣的尾端，透過此方式收款人可以透過上一位持有者之公鑰驗證電子簽章，如圖 2-3 所示。

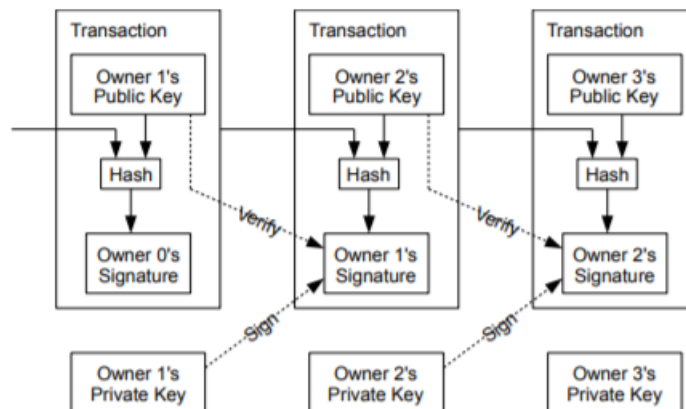


圖 2-3 比特幣交易

來源：(Satoshi Nakamoto, 2008)

但透過上述方法收款人無法驗證前面之歷史持有人是否有對這一枚比特幣進行雙重支付，傳統支付方式為透過第三方機構(如中央機構、造幣廠)來驗證，所有交易所支付的貨幣皆會送回造幣廠並進行驗證，若交易為合法，造幣廠將會註銷支付貨幣並發行新貨幣，此新貨幣才會被認證並判定為無雙重支付，因此需要一個機制確認前一位擁有者沒有簽署額外的交易，而隨著鏈上的串接就能確保整條鏈上之貨幣皆無雙重支付。

驗證交易是否合法的唯一方法是去確認到所有交易的發生順序，以上述造幣廠的模式為例，造幣廠必須確認到所有交易並決定其完成的先後順序，因此在沒有信任第三方驗證之情況下達到此目的，交易就必須廣播給所有參與者，且需要一個達成共識的系統，統整所有參與者所接收的交易順序，收款者必須要確保在交易期間絕大多數的節點都認同該交易是首次出現。

### (三)時間戳記伺服器(Timestamp Server)

為了達成讓所有參與者交易接收順序達成共識，以解決雙重支付問題，因此使用時間戳記伺服器來將很多交易組成的區塊(block)所對應之雜湊加上時間戳記，並將雜湊進行廣播，每個時間戳記會將前一個時間戳記加入其雜湊中，進而形成了一條鏈，如圖 2-4 所示。

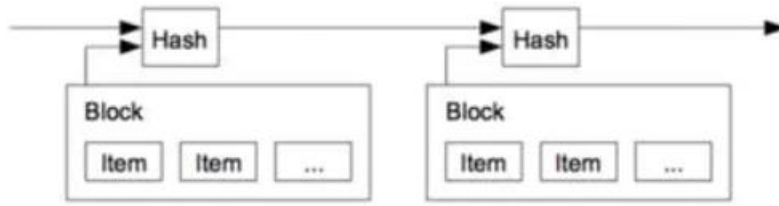


圖 2-4 時間伺服器

來源：(Satoshi Nakamoto, 2008)

簡單來說，若某持有者將一枚比特幣發送給接收者 A，此交易尚未完成時又將同一枚比特幣發送給接收者 B，此時就能依照時間戳記來判定交易的先後順序，防止雙重支付。

#### (四)工作量證明(Proof-of-Work)

概念最早由 Cynthia Dwork & Moni Naor(1993)提出，主要防止散式阻斷服務攻擊(Distributed Denial of Service Attack, DDoS)和減少垃圾郵件的傳播。隨後 Jakobsson & Juels(1999)正式提出了工作量證明(Proof-of-Work)一詞，說明工作量證明是一種防止服務與資源濫用或是阻斷服務攻擊的解決對策。其要求使用者之計算機進行一些耗時的複雜運算，並且運算後的答案能被服務方快速驗證，以此消耗的時間、效能與資源做為運算成本，以確保服務與資源是被真正的需求所使用，進而降低攻擊者之攻擊慾望。

Satoshi Nakamoto(2008)也提及若要在點對點基礎上去實現分散式時間戳記伺服器共識機制，必須導入工作量證明系統，避免所有節點接到交易後同時寫入上鏈。比特幣以安全雜湊演算法(SHA-256)為主要雜湊方式，並規定雜湊值之開頭位數必須為一個 0 或多個 0，隨著 0 的數目上升，所需之工作量將呈指數增加，且可藉由執行一次雜湊運算即完成驗證。在時間戳記網路中，藉由增加區塊內的 nonce 的數值直到區塊所對應之雜湊值開頭位數滿足特定數量的 0 之 nonce 值被節點計算出來，以此完成工作量證明，如圖 2-5 所示，當第一位計算出雜湊後並經驗證無誤，即可上鏈，而其他所有節點必須承認此區塊達成共識機制。

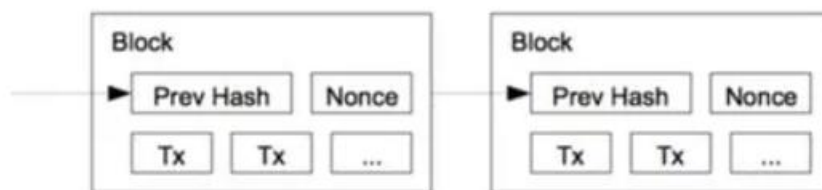


圖 2-5 Proof of Work

來源：(Satoshi Nakamoto, 2008)

工作量證明也解決了共識中多數表決的問題，其本質上是一個 CPU 對應一票。由於最長的鏈包含了最大的工作量，因此多數決代表必定為最長的鏈。如果大多數的 CPU 運算能力是由公正的節點所控制，則此公正的鏈將會最快速成長且超越任何一條競爭者的鏈。若要修改先前的區塊，攻擊者必須重新完成該區塊及在它之後的所有區塊的工作量證明，鏈越長工作量證明越多，大幅增加竄改資料的難度。

#### (五)網路(Network)

此網路需依照以下步驟進行以達成共識系統：

1. 新的交易將會廣播至所有節點。
2. 每個節點會把新交易放入其區塊內。
3. 每個節點進行工作量證明，計算雜湊值滿足前幾位數為 0。
4. 當某個節點最先找到符合的雜湊值，會將其區塊廣播至所有節點。
5. 若此區塊上之交易為首次出現且為合法，所有節點將接受此區塊。
6. 若節點表示接受此區塊，當創造新區塊時會將接納之區塊雜湊作為先前的雜湊值。
7. 若有兩個節點同時發布兩種新區塊，其他節點會先暫時接收某一種，但也會保存分支鏈，等到下一個工作量證明被實證且發現某一條鏈為最長，其他分支鏈之節點會放棄其較短的鏈，轉而處理最長的鏈，透過先前所述，最長的鏈也為最正確的鏈。
8. 新的交易只需廣播至足夠的節點即可，不需每一個節點都觸及，一樣能將區

塊寫入上鏈，而沒接收到的節點可能會有區塊缺失，不過這些節點一旦收到下一個新的交易廣播時，依照區塊鏈的特性，就會認知其遺漏了區塊並提出下載申請。

#### (六)獎勵(Incentive)

區塊中的第一筆交易是特殊交易，它啟動了區塊創建者擁有的新貨幣，這增加了節點支持網絡的動力，並提供了將貨幣流通的方式，因為此網路無中央機構發行貨幣。穩定增加一定數量的新貨幣類似於開採黃金所消耗的資源以增加黃金的流通量，在此網路中，消耗的資源為 CPU 運算資源、時間和電力，因此將交易費用給予提供運算資源的礦工，以激勵他們繼續支持網路。

獎勵制度也能間接使節點保持誠實，如果惡意攻擊者擁有了大部分的運算資源並且能夠控制區塊的寫入，相信攻擊者必定會衡量繼續合法挖礦的獎勵與非法攻擊網路的收益，因為比起破壞系統及自身財產的合法性，遵守規則有可能使他擁有更多的電子貨幣。

### 三、區塊鏈的特性

基於去中心化的分散式儲存技術，區塊鏈將具有與傳統中心化技術不同的特點，廖子純(2017);蔣潤祥、魏長江(2016);車世偉(2018)認為以下特性為區塊鏈的優勢所在：

1. 去中心化：去中心化為區塊鏈之核心技術，因此沒有中心化的控制，也無需依賴額外的第三方管理或軟硬體設備，其透過分散式的運算和存儲，各個節點實現了訊息傳遞、管理和自我驗證。
2. 安全性：基於區塊鏈驗證的機制，只要惡意攻擊者不能掌控區塊鏈中 51%的節點，就無法肆意修改區塊鏈上所儲存之數據，加上控制 51%節點的成本遠大於惡意人士之攻擊效益，這使得區塊鏈系統變得相對安全，也能避免人為變更數據。
3. 不可竄改性：基於去中心化分散式儲存技術，資料經驗證上鏈後任何人皆無

法更改僅可檢視，因此能確保資料之公正性與可信度。

4. 開放性：區塊鏈技術之基礎建設皆是開源的(open source)，除了交易雙方的特定資料被加密外，於區塊鏈上之數據皆對任何人開放，只要擁有連網計算機皆能夠通過公開的接口或網站查詢區塊鏈上的數據，因此相較於傳統集中式系統，資訊流動較為透明且公正性較高。
5. 獨立性：基於區塊鏈的規範協議和技術，區塊鏈系統不需仰賴第三方，所有節點能夠在系統內交換數據與自動驗證。
6. 匿名性：除非有法律上之規範要求，從技術面來看，不需要公開或驗證各區塊鏈節點的身份訊息，因此可以匿名進行訊息的傳遞，相對的也提高了安全性。

### 第三節 以太坊

#### 一、以太坊起源

根據 Tapscott & Tapscott(2016)所述，Vitalik Buterin 本身是一名程式設計師並參與比特幣社群，他認為很多程式都可以運用比特幣的區塊鏈原理來達成更多的發展，因此曾向比特幣主要開發人員主張比特幣平臺應該要有個更完善的程式語言讓人來開發，而且應用層面不應該只有再電子貨幣上，但最終未果，因此決定開發一個新的平臺來符合其理念。

不久後，受比特幣啟發的 Vitalik Buterin(2014)於 2013 年提出了以太坊的概念，其所發表的以太坊白皮書主要內容為打造一個能夠利用區塊鏈技術做任何應用開發的去中心化平台，與提出應該要有一個可以用來撰寫區塊鏈上應用的專用程式語言，並且可以建構去中心化的應用程式(Decentralized Apps, DApps)、去中心化的自治組織(Decentralized Autonomous Organization, DAO)、智能合約(Smart Contract)、虛擬加密貨幣。並以「能讓開發者創建更具可擴展性、易於開發和協同的應用，打造一個在各個領域都能去中心化、開放、安全的未來」為以太坊最大宗旨。

Garvin Wood(2014)發表一篇名為「以太坊：一個安全的、去中心化的通用交易帳本」(*Ethereum: A Secure Decentralized Generalized Transaction Ledger*)的以太坊黃皮書，是一篇技術導向的論文，其內容為探討與設計以太坊技術層面的架構，最重要的是嚴謹地解釋了以太坊的運作機制和以太虛擬機器運作流程。

## 二、以太坊優勢

Vitalik Buterin(2014)於以太坊白皮書中表示，儘管比特幣區塊鏈技術能夠實現一些特定的智能合約，但使用 UTXO(unspent transaction output)機制仍然存在著局限性。以太坊是首先提出在區塊鏈上構建智能合約想法的平台，指出了比特幣腳本機制的以下四個缺點，而這些缺點限制了智能合約的發展性：

1. 缺乏圖靈完備(Lack of Turing-completeness)：雖然比特幣腳本可以支援多種計算，但為了避免交易確認時出現無限循環，因此缺少了循環(loop)語句。理論上能用 if 語法來達到循環的效果，不過這樣的做法會導致程式過冗長且腳本空間利用效率低落。
2. 區塊鏈盲目(Blockchain-blindness)：UTXO 無法取得區塊鏈內部的數據，如前一個區塊的雜湊值和隨機數，這個缺陷剝奪了腳本語言所擁有基於隨機性的潛在價值。
3. 缺乏狀態(Lack of state)：UTXO 的狀態只有兩種，分別為已花費或者未花費狀態，此種二元狀態對於實現多階段的合約控制有發展上的限制，使得合約難以執行複雜的邏輯。
4. 價值盲目(Value-blindness)：UTXO 腳本不能精細的控制帳戶的取款額度，例如 A 和 B 向合約投入了 1000 美元的比特幣，腳本在一個月後向 A 返還了 1000 美元的比特幣，其餘還予 B，這一個月內美元與以太幣之匯率必有浮動，而 UTXO 無法衡量與更動幣值，導致給予之貨幣數量價值不相等，而以太坊能透過 Oracle Contract 取得外部資訊並做調整。



為了解決上述問題，以太坊實現了一個智能合約平台，人們可以在平台上編寫智能合約來使用以太幣（以太坊區塊鏈中的虛擬貨幣）。每個智能合約都有一個以太幣餘額，並且能夠根據合約定義的邏輯來發送和接收以太幣，此種運作模式使得以太坊迅速發展起來，成功建立了許多以其為基礎的去中心化應用程式。以太坊不再導入 UTXO，而是使用帳戶模型(account model)。在以太坊系統中，狀態是由「帳戶」（每個帳戶為一個 20 字節的地址）的對象和在兩個帳戶之間轉移價值和訊息所構成的，以持有虛擬貨幣為例，每一筆扣款或交易都會將帳戶餘額資訊記錄於區塊鏈中，因此認證交易只需要直接確認帳戶餘額即可，不用如 UTXO 須從第一筆交易讀取至最後一筆。以太坊之帳戶包含四個組成元件：

1. 帳戶的合約代碼。
2. 帳戶目前的以太幣餘額。
3. 帳戶資訊的存儲。
4. 隨機數為用來避免交易被多次處理的計數器。

以太幣(Ether)是以太坊內部的主要電子貨幣，其可用於支付交易手續費。以太坊有兩種類型的帳戶，一個為由私鑰控制的外部帳戶，另一個為由合約程式碼控制的合約帳戶，人們可以透過其外部帳戶所對應的私鑰簽署交易並發送消息，一旦合約帳戶收到消息，合約內部程式碼將被激活並允許按照其邏輯進行存取、發送其他消息或創建合約。

## 二、智能合約

智能合約之概念最早由 Nick Szabo(1994)提出，智能合約是透過計算機來自動化執行合約內容的交易協議，其設計的總體目標為滿足合約上的條件與準則，例如：付款條件、機密性、強制性等，並且大幅度減少惡意或偶然的例外情況發生以及合約中介之信任度之需求，以經濟效益來看，智能合約能夠降低

欺詐損失、仲裁和執行成本以及其他交易成本。以下產品可符合當時智能合約粗略的概念：銷售時點情報系統(point of sale, PoS)、卡片、電子數據交換(electronic data interchange, EDI)等。

Nick Szabo(1995)發表「*Smart Contracts Glossary*」，定義了智能合約相關專有名詞與解釋，包括代理人(agent)、中介者(mediator)、加密協議(cryptographic protocol)等，透過這些專有名詞得知智能合約之所有參與者與各式協定之描述，奠定日後智能合約發展非常重要的基石。

Nick Szabo(1996)提出在數位市場的基礎下智能合約之適用性，隨著數位革命的來臨，計算機運行演算法越來越快且有效率，並且在短時間處理更大量的資訊，再加上網際網路的興盛，更多更複雜的訊息能夠快速地傳遞，使得計算機能行使智能合約之門檻降低許多。此外，計算機科學家和密碼學家在當時發現了許多新的演算法，將大量的訊息和演算法結合起來可以實現各式各樣的新協議，不論在合約上的執行、驗證身分、安全性等對於智能合約皆有重要的應用與發展。Nick Szabo 也定義了「智能」二字並非運用人工智慧，而是相較於傳統紙本式合約有更多的功能，並透過計算機來達成自動化，整體來說，智能合約是一組以數位形式制定的承諾，包括各種在合約中執行這些承諾的協議。

Nick Szabo(1997)提出智能合約之安全性，並提出自動販賣機的生活實例，自動販賣機為智能合約的起源，其通過簡單的機制獲取硬幣，並根據顯示的價格分配零錢和產品。自動販賣機是一個合約，任何擁有硬幣的人都可以參與與供應商的交換，並透過密碼箱和其他安全機制可以保護儲存的硬幣和內容免受攻擊者的入侵。而智能合約超越了自動販賣機的概念，可以將合約嵌入各種有價值的財產，並通過演算法加以控制。智能合約通常以主動執行的形式動態使用該財產，並提供更好的監測和驗證。

綜合上述，Nick Szabo 透過期刊著作闡述了所有智能合約的概念，但並無說明如何透過計算機來實現，加上就以當時的技術而言，正常的履行合約而不需透過第三方來監控實際上也非常難以達成。陳恭(2017)也提及當時 Nick

Szabo 只是單純的提出這個概念，並無任何實作之方法或可應用之地方，因此沒有得到熱烈的回響，導致智能合約的發展受限，停留在概念的層次。直到這幾年間，區塊鏈技術的興起，使得智能合約能建構於區塊鏈上，實現與落實當年 Nick Szabo 所闡述之概念，並逐漸在科技與金融業中萌芽。

Satoshi Nakamoto(2008)發表一篇名為《比特幣：一種對等式的電子現金系統》(*Bitcoin: A Peer-to-Peer Electronic Cash System*)的論文，其中描述了名為「比特幣」的電子貨幣及其演算法，並詳細講解如何建立一套去中心化的電子交易系統，而且這種系統不需要透過第三方或必須建立交易雙方相互信任的基礎，使用演算法來完美取代交易者的誠信度問題，此技術稱為區塊鏈，這也間接的證明智能合約終於有技術或平台能實現其概念。

Vitalik Buterin(2014)提出比特幣應用之區塊鏈技術不應只是支付款項或是單純的記載交易紀錄，導致區塊鏈技術所能達到的功能受限，而且具有以下缺點：缺乏圖靈完備、價值盲目、缺乏狀態、區塊鏈盲目，為了解決上述問題，Vitalik Buterin 改良區塊鏈技術建立了一套新的分散式應用平台——「以太坊」(Ethereum)，其應用之技術稱之為區塊鏈 2.0。以太坊以智能合約為主要應用基礎，利用演算法制定資料處理與規則，並將這些程式碼部署至區塊鏈上，讓區塊鏈不只儲存交易帳本，還有自動化的程式邏輯，藉此擴展區塊鏈之功能。

### 三、智能合約編譯

Garvin Wood(2014)發表以太坊黃皮書，定義了如何實作以太坊以及其技術相關文件。隨後便開發了一款專門用來編譯與開發智能合約的程式語言 Solidity，其為一種合約導向式語言，可被應用於各種不同的區塊鏈平台上，Solidity 能使程式開發人員在區塊鏈平台上編寫智能合約，編譯完後會將程式碼轉成位元組碼，並透過以太坊虛擬機器(ethereum virtual machine, EVM)將其發布在以太坊區塊鏈上。

根據 Solidity 官方文件指出，這門語言受到了 C++、Python 和 Javascript 語

言的影響，因此許多語法或是架構上都與上述語言有相似之處，Solidity 最主要的開發平台為 Remix、Visual Studio Solidity Extension。目前最為方便，同時也是官方推薦的編譯環境為 Remix，它是基於瀏覽器的整合開發環境，可以用來編譯、部署、除錯智能合約。

#### 四、分散式應用程式(Decentralized Application, Dapp)

根據 Johnston et al.(2015)所發表的分散式應用程式白皮書(*The General Theory of Decentralized Applications White Paper*)所述，其又名去中心化應用程式，為使用區塊鏈技術為核心所開發出來的應用程式，並必須包含以下準則才能視為分散式應用程式：

1. 應用程式必須為開源。
2. 應用程式可以根據使用者之建議與市場回饋來調整其協議，但所有更改必須由使用者之共識來決定。
3. 應用程式之資料與操作紀錄必須加密並儲存於公開訪問的區塊鏈。
4. 存取應用程式時必須使用原生加密貨幣或智能合約所發行之代幣，並為礦工提供獎勵。
5. 應用程序必須根據標準加密演算法進行採礦，以證明其網路節點對應用程式有所貢獻。

依據 Dapp 數據統計網站 Dappradar 與 Stateofthedapps 所示，目前已上市的 Dapp 總數量約為 3000 多個，每日約為 9 萬 5 千個用戶使用程式，並有 5 千個使用中的智能合約流通於區塊鏈中。其中建構於以太坊環境中的程式為大宗並多達 2700 個，而於 2018 開始，開發的數量有急遽的上升，對於 Dapp 來說確實是一個非常好的現象，如圖 2-6、圖 2-7。

由此可知，相較於傳統集中式應用程式的普及率還有非常大的差距，除了區塊鏈平台無法因應大量數據造成的擁塞，降低 Dapp 執行的速度以外，交易

驗證的速度是最令人詬病的點，就現在的硬體設施來看還無法解決，因此許多區塊鏈技術人員正在研究如何提高吞吐量及速度，並完善周邊的體驗，像是側鏈或是代理權益證明(delegated proof of stake, DPoS)的開發。綜合上述，雖然現在於公鏈上所開發的 Dapp 數量或是每日使用者數量非常少，但是畢竟區塊鏈技術的發展階段還處於早期，也不太能相互比較，隨著日後公鏈技術與硬體的開發，DApp 或許能有自己的地位甚至取代傳統應用程式，那正是大家所樂見的。

Total DApps	Daily active users ?	24h transactions ?	24h volume USD ?	Smart contracts	
3,338	95.71k	1.25m	10.19m	5.25k	
Platform	Total DApps	Daily active users ?	Transactions (24hr) ?	Volume (24hr) ?	# of contracts
Ethereum	2,773	21.44k	75.56k	37.62k	4.27k

圖 2-6 Dapp 數量

來源: Stateofthedapps

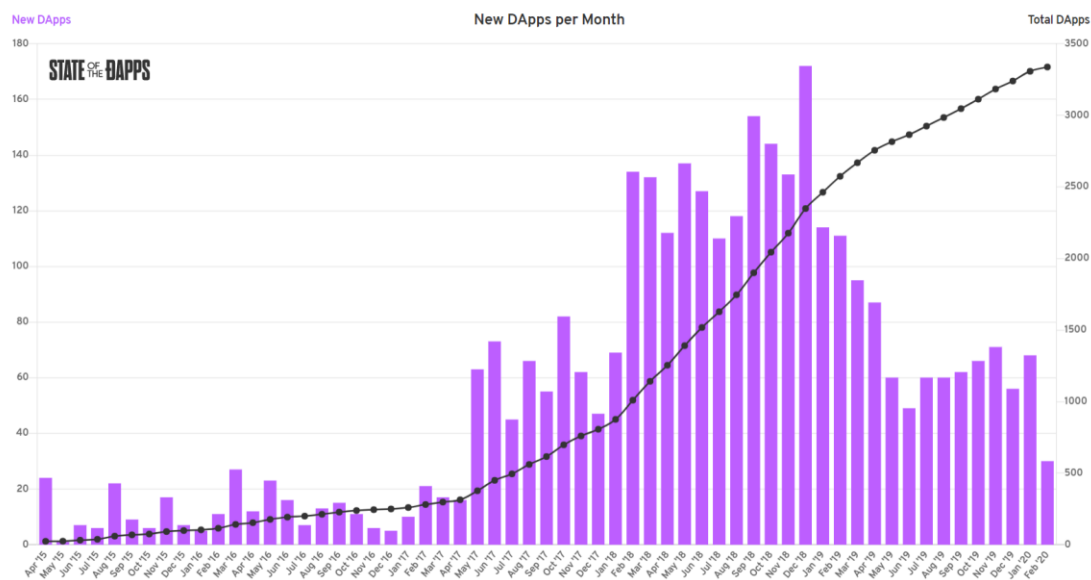


圖 2-7 Dapp 成長數量

來源: Stateofthedapps

### 第三章 研究方法

對於一個自動化程式策略投資平台最重要的是顯示出來的投資相關數據，其背後的計算公式、資料流向以及數據的正確性與真實性對於投資者來說至關重要，任何細節只要處理不好或是缺乏透明性很容易失去投資者對平台的信心，因此本研究主要為建立一個策略程式投資平台並解決以下兩個問題點：

1. 如何確認投資報酬率、損益數值、報表等投資相關數據與計算公式之明確性和公正性。
2. 導入人工智慧與大數據分析程式之投資策略商品，如何確保程式在還有人投資尚未結束前能不被程式設計者任意竄改。

本研究應用於區塊鏈之相關技術，建立一個新的策略程式投資平台，使用者能透過平台上傳自己所撰寫之策略投資程式當作商品讓投資人與跟單人投資，透過以太坊之智能合約記錄每一筆投資入金相關資訊和編寫自動化計算公式，以及將程式設計者上傳程式執行檔之二元碼經過雜湊轉為一組數值存入智能合約中，由於區塊鏈上的資料具有不可竄改性和公正透明性，平台背後的資料與公式皆透明公開於網路上，只要擁有計算機並連上網路，不分身分任何人皆有權力存取平台投資相關資訊，藉此解決傳統集中式資料庫之潛在問題。

## 第一節 研究架構

本研究之相關人員、物件、角色如下：

1. 策略程式設計者：又稱被投資人和入金者，為透過人工智慧和大數據分析相關之演算法，建立預測模型，以程式輸出為主要投資組合策略，使投資者按照模型之分析進行各項投資，並從投資者獲利中抽取手續費。所有被投資相關資訊，如此策略程式之報酬率、盈虧等皆會顯示於投資策略頁面內，以供其他投資人參考。須將自己設計之演算法轉為執行檔，並於策略投資程式上傳區進行上傳，以使平台管理者進行自動化監聽訊號。
2. 投資者：又稱出金者，透過投資策略頁面觀看各個策略程式設計者對其模型之描述與投資相關歷史數據，尋找自認合適之投資策略進行投資，投資之金額會按照其投資之策略進行自動化委託代操，投資期間能隨時監控盈虧，並能隨時全數賣出，結束投資。
3. 跟單者：本質上與投資者相符，觀看策略程式之歷史投資人對此程式之投資相關數據，決定是否與投資人進行相同之投資策略。
4. 會員系統：如同各大平台一樣，擁有登入、註冊、登出、個人資料、更改個人資料以及觀看牽涉此客戶電子錢包所有相關交易之功能。
5. 加密貨幣匯兌區：本平台有使用以以太坊為應用之 ERC20 智能合約介面，其能夠發行私人客製化之加密貨幣(tokens)。使用者或客戶須與本平台兌換加密貨幣(目前暫時以新台幣 1:1 Tokens 之匯率進行兌換)，所有投資皆以加密貨幣為主。此兌換區能夠以真實貨幣兌換加密貨幣，亦能夠以加密貨幣贖回真實貨幣。
6. 程式者專區：此專區為策略投資程式設計者所使用，設計者可將自己所設計之程式碼轉為執行檔後，提供程式上傳、程式檢視、程式修改、程式刪除、暫停被投資入金、繼續被投資入金等程式操作相關服務。
7. 投資者專區：此專區為投資者和跟單者所使用，投資者與跟單者可將自己已

經投資之策略程式進行以下操作：投資程式資料檢視、停止投資(全數賣出)等投資操作相關服務。

8. 投資策略頁面：此頁面將擺入所有策略程式設計者所設計之程式以及相關投資數據，包括：每日、每月、每季之投資報酬率、總盈虧、程式相關描述等，投資人可至此頁面選擇策略程式進行投資。
9. 券商：依照中華民國法律規範，一般民眾不能自行買賣證券、期貨等投資商品，必須經由券商進行委託代操，因此後端伺服器一旦接收到投資入金或賣出訊號，立即與券商 API(application programming interface)串接，達成自動化委託下單服務。
10. 智能合約：一份智能合約只會對應一個策略程式，為其記錄策略程式相關資訊，如：前置手續費、後置手續費、投資者錢包位址、入金金額、時間等。資料一旦部署到智能合約上即無法更改，而且人人都能夠透過網路來存取合約資料。

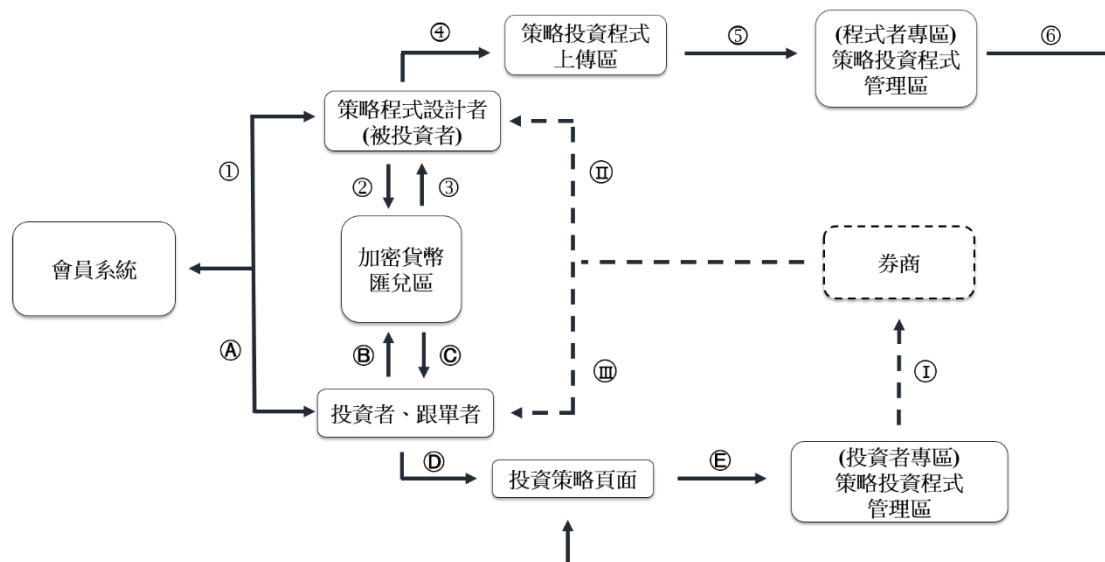


圖 3-1 策略投資程式平台使用流程架構圖

圖 3-1 為使用者在投資平台上之操作流程，平台提供五大功能區，分別為會員系統、加密貨幣匯兌區、程式者專區、投資者專區、投資策略頁面，圖中阿拉伯數字 1-6 為策略程式設計者(被投資者)之平台使用流程，英文字母 A-E



為投資者與跟單者之平台使用流程，羅馬數字I-III為伺服器後端與券商之資料處理流向，圖中實線為投資平台使用者所能操作之範圍，虛線為平台程式交易之自動化流程，無須任何操作。各項流程之詳述如下：

- 策略程式設計者(被投資者)

1. 需先至網站會員系統註冊會員，輸入使用者名稱、使用者密碼、電子錢包位址等個人資料進行註冊，登入後可至會員系統檢視、修改個人資料以及查詢記錄此會員於智能合約上之所有相關交易。
2. 使用此投資平台需先至加密貨幣匯兌區以真實貨幣換取此平台發行之加密貨幣。
3. 於此平台不論盈虧，只要還擁有加密貨幣之餘額，皆能再兌換為真實貨幣。
4. 策略程式設計者需先自行撰寫策略程式，無論哪種程式語言皆須轉為執行檔，並至策略投資上傳區上傳執行檔，後端伺服器將自動監聽程式之輸入與輸出，並依輸出進行自動化下單。
5. 成功上傳程式執行檔之後，將自動轉跳至程式者專區-策略投資程式管理區進行策略程式之投資資訊初始化，主要包括：策略程式之投資手續費、入金金額最大值與最小值、程式描述等，以上數值之設定皆能依照設計者之喜好進行客製化之設定，投資者也能觀看資訊並衡量斟酌後再決定是否投資。
6. 策略程式投資相關數值初始化成功後，此程式與設計人將會出現於投資策略頁面之中，提供給投資人觀看與投資。

- 投資者與跟單者

- A. 需先至網站會員系統註冊會員，輸入使用者名稱、使用者密碼、電子錢包位址等個人資料進行註冊，登入後可至會員系統檢視、修改個人資料以及查詢記錄此會員於智能合約上之所有相關交易。

- B. 使用此投資平台需先至加密貨幣匯兌區以真實貨幣換取此平台發行之加密貨幣。
  - C. 於此平台不論盈虧，只要還擁有加密貨幣之餘額，皆能再兌換為真實貨幣。
  - D. 可直接至投資策略頁面觀看所有投資策略設計人之程式與相關資料，並參考投資相關數據以利選擇出理想之程式，投資之手續費與金額限制皆為策略設計者所制定。
  - E. 成功投資策略程式後，即可至投資者專區-策略投資程式管理區及時觀看投資之策略程式現況以及每日盈虧，並可以隨時終止投資(全數賣出)，歸還投資金額和獲利或剩餘投資金額。
- 平台程式交易之自動化流程
    - I.
      - 1. 若訊號為投資人投資入金，則將透過券商 API 自動通知券商將投資人投資金額依照策略程式之輸出結果代為操作。
      - 2. 若訊號為投資人終止投資，則將透過券商 API 自動通知券商將投資人之所有已經購入之投資商品賣出。
    - II.
      - 1. 若訊號為投資人投資入金，券商下單成功後將訊號傳送至本平台伺服器後端，並通知策略程式設計者相關投資訊息，包括：投資者資料、入金金額、時間等，和給予當初所要求之投資前置手續費。
      - 2. 若訊號為投資人終止投資，券商自動賣出所有投資人透過此策略購買的投資商品，待賣出成功後，將通知策略程式設計者並給予投資後置手續費。

### III.

1. 若訊號為投資人投資入金，券商下單成功後將訊號傳送至本平台伺服器後端，並通知投資人相關投資訊息，包括：策略程式設計者資料、入金金額、時間等，並扣除策略程式設計者所要求之投資前置手續費。
2. 若訊號為投資人終止投資，券商自動賣出所有投資人透過此策略購買的投資商品，待賣出成功後，通知投資人並將獲利扣除後置手續費，全數金額歸還給投資人。

## 第二節 平台與智能合約之互動

以下將介紹整個平台與區塊鏈智能合約之互動，共分為四種平台上之主要功能區與合約之串接以及資料流向。

### 一、會員系統與智能合約之關係

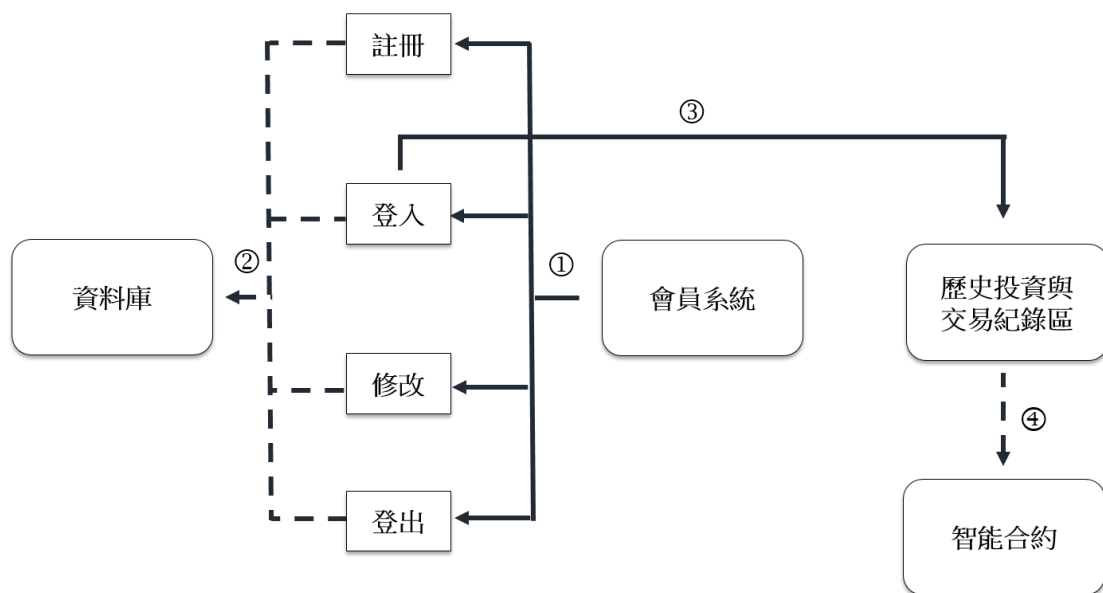


圖 3-2 會員系統與智能合約關係

圖 3-2 為會員系統與智能合約之關係，會員系統主要分為五個功能，分別為註冊會員、登入會員、修改會員資料、登出以及歷史投資與交易紀錄區，歷史投資與交易紀錄區主要是平台提供使用者介面，使得使用者能在此區瀏覽自身帳戶的所有活動紀錄，而不用透過其他網站或軟體觀看區塊鏈上的資訊。實線為使用者操作流程，虛線為平台後端自動化之資料處理與流向，以為下相關流程步驟：

1. 使用此投資平台前，需先至會員系統註冊會員，登入會員後可以進行會員資料修改和登出。
2. 由於註冊會員所填寫之資料包括個人帳號密碼等敏感性資料，若存入智能合約中將會公開給所有人存取，就算經過加密處理也有被破解的可能，因此這些敏感性資料必須存入資料庫內，以增加隱密性。
3. 登入會員後，可至歷史投資與交易紀錄區觀看帳戶於此平台之活動紀錄。
4. 歷史投資與交易紀錄區主要是存取區塊鏈上智能合約之資料，在智能合約上創建事件(event)，能將對合約之相關操作儲存至記錄檔(log)中，藉此使平台能存取歷史相關操作資訊。

## 二、加密貨幣兌換系統與智能合約關係

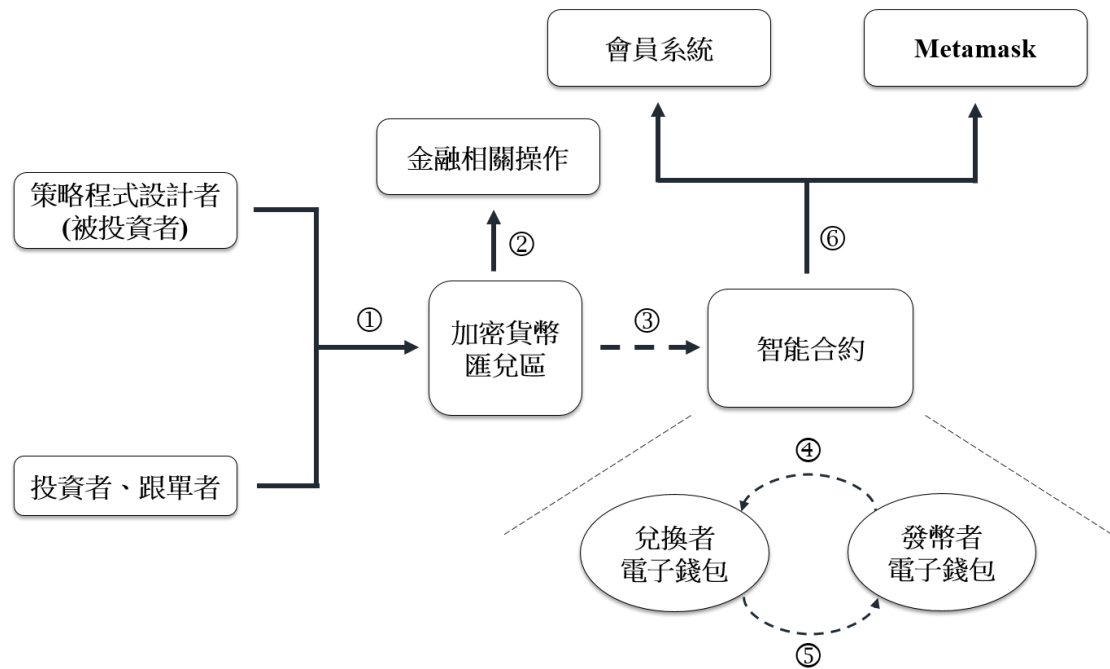


圖 3-3 加密貨幣兌換系統與智能合約關係

圖 3-3 為加密貨幣兌換系統與智能合約之關係，在智能合約上使用 ERC20 介面，能夠發行客製化之加密貨幣以及進行轉帳功能，也會在合約上紀錄所有使用者錢包之加密貨幣餘額。實線為使用者操作流程，虛線為平台後端自動化之資料處理與流向，以為下相關流程步驟：

1. 使用者進入加密貨幣匯兌區頁面進行加密貨幣兌換。
2. 使用者可以選擇為真實貨幣兌換平台加密貨幣或是持有平台加密貨幣餘額兌換真實貨幣，待選定後輸入兌換金額並進行轉帳、匯款等金融相關操作。
3. 操作成功後，將傳送交易至智能合約上，以修改合約持有代幣數量資料。
4. 若交易為兌換加密貨幣，則將發幣者電子錢包之加密貨幣轉帳給兌換者電子錢包。
5. 若交易為兌換真實貨幣，則將兌換者電子錢包之加密貨幣轉帳給發幣者電

子錢包。

6. 區塊鏈交易驗證成功後，使用者可至會員系統或是 Metamask 上查看加密貨幣餘額，同時也能至會員系統中的歷史投資與交易紀錄區查詢兌換之交易。

### 三、策略程式設計人與智能合約關係

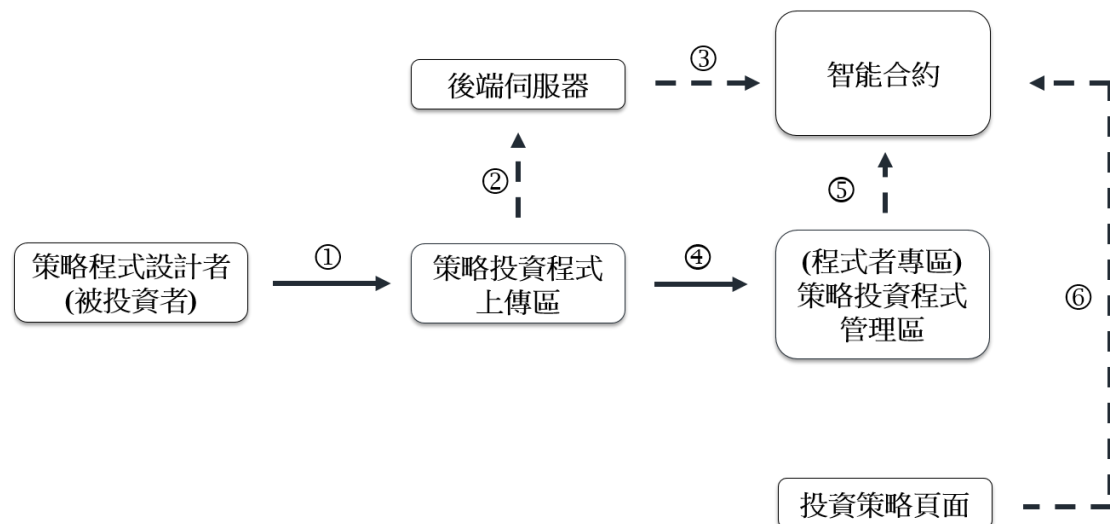


圖 3-4 策略程式設計人與智能合約關係

圖 3-4 為策略程式設計人與智能合約之關係。實線為使用者操作流程，虛線為平台後端自動化之資料處理與流向，以為下相關流程步驟：

1. 策略程式設計者自行設計模型與演算法後，將程式碼轉為執行檔，並前往策略投資程式上傳區進行上傳。
2. 程式上傳完成後將會把檔案存進伺服器本機端並等待投資者投資。
3. 由於一個策略程式會對應一個智能合約，因此伺服器端一旦接收到檔案後會自動進行新的合約部署。
4. 部署完成後，策略程式設計者會轉跳至程式者專區-策略投資程式管理區進行合約初始化，需輸入自訂的資料，包括投資前置費用、投資後置費用、最大最小投資金額等。

5. 自訂資料輸入完後，將自動送出交易至智能合約上以寫入投資相關資訊。
6. 交易驗證完成後，投資策略頁面將自動出現此策略程式設計者資料與策略程式之投資相關資訊，供投資人瀏覽與投資，此頁面之資訊皆是直接存取區塊鏈上之智能合約資訊，而不會透過資料庫。

#### 四、投資人、跟單人與智能合約關係

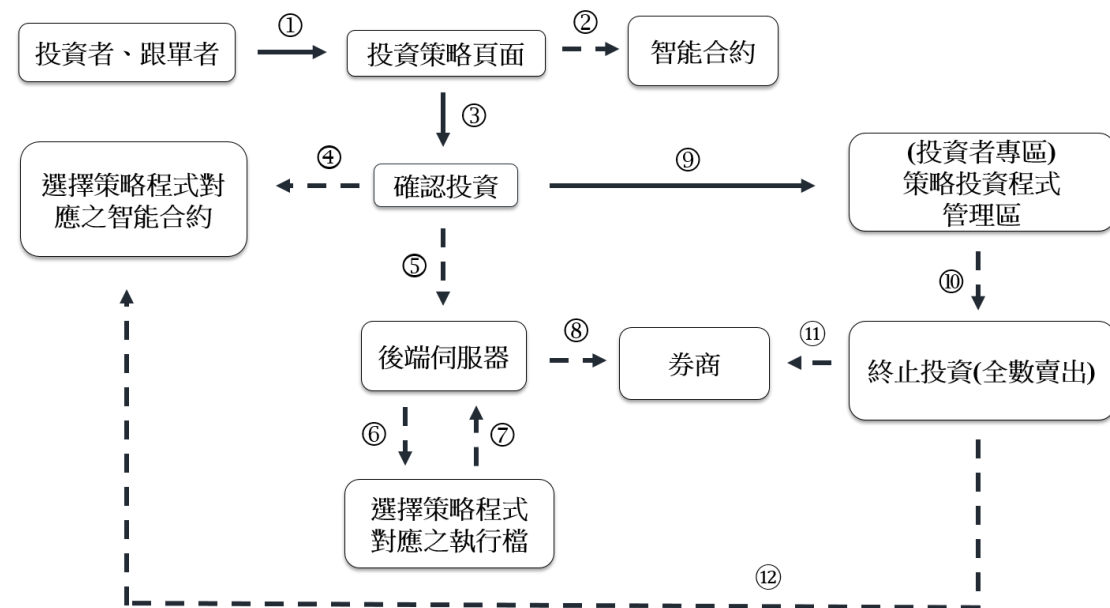


圖 3-5 投資人、跟單人與智能合約關係

圖 3-4 為投資人、跟單人與智能合約之關係。實線為使用者操作流程，虛線為平台後端自動化之資料處理與流向，以為下相關流程步驟：

1. 投資人與跟單人可至投資策略頁面觀看所有策略程式人之資料與其所設計之策略程式。
2. 投資策略頁面之資訊是直接存取區塊鏈上之智能合約資訊，而不會透過資料庫。
3. 投資人選定好策略程式後，輸入投資金額，投資金額限制與收續費抽取皆是策略程式設計者初始化所自行輸入的。
4. 確認投資後將進行扣款，並且送出一筆交易至所選策略程式對應之智能合約中，目的是將入金金額、投資開始時間、投資人資料等相關資訊紀錄至

合約中。

5. 待交易驗證完成後，將訊號傳入後端伺服器。
6. 後端伺服器將執行存於本機端之投資者所選策略程式執行檔，並且於投資期間每日監聽程式。
7. 將策略程式執行檔之輸出(買賣訊號)傳回伺服器後端。
8. 伺服器收到程式輸出後，將投資人入金金額照著策略程式輸出結果做投資，並通知券商下單，完成投資人與跟單人之投資。
9. 投資人完成投資後將轉至投資者專區-策略程式管理區，其可以觀看正在投資之策略資料、盈虧現況等投資相關資訊。
10. 若投資者想要終止投資，或是投資策略虧損等於入金金額，則將目前持有之投資產品全數賣出。
11. 收到終止投資訊號後，自動通知券商下單，賣出所有依照策略所購入之投資產品。
12. 賣出後將發送交易至所選策略程式之智能合約中，把所有投資資訊，包括盈虧、投資結束時間、投資產品資訊等寫入合約中，最後把賣出全數餘額之相對應加密貨幣數量轉帳給投資者，結束此策略之投資。



## 第四章 研究結果

### 第一節 系統工具

#### 一、Node.js

Node.js 是能夠在伺服器端運行 JavaScript 開放原始碼、跨平台 JavaScript 的執行環境。Node.js 使用非阻塞、事件驅動和非同步輸入輸出模型等技術藉此提高效能，並可最佳化應用程式的規模和傳輸量，上述技術通常用於資料密集的即時應用程式。Node.js 的程式本身支援各大作業系統上，如：Linux、Unix、Microsoft Windows、Mac OS X 等，因此可以減少相容性與平台移植之問題。

綜合上述，再加上此系統須使用 Javascript 套件 Web3.js 來存取以太坊網路，因此選用 Node.js 為此系統之後端服務，不須做任何轉換即可直接使用 Web3.js。

#### 二、Express 框架

Node.js 本身不直接支持其他常見的 Web 開發方式。如果要為不同的 HTTP 方法（例如 Get、Post、Delete 等）添加特定的處理方式，或是分別處理不同 URL 路由上的請求，提供靜態文件，以及使用模板動態響應，Node.js 本身無法有效地完成上述任務，必須透過開發者編寫底層代碼，或是使用 Web 開發框架。

Express 是目前最流行與最精簡的 Node.js Web 框架，並且是許多 Node Web 框架的基礎。Express 提供了以下機制：

1. 在不同的 URL 路由中為具有不同 HTTP 方法的請求編寫處理程序。
2. 與「視圖」渲染引擎整合，以便透過將數據插入模板來生成響應。
3. 提供設置常見的 Web 應用程序設定，例如用於連接的端口以及用於呈現響應的模板的位置。

4. 在請求處理管道內的任何位置添加其他請求處理「中介軟件」。
5. 為 MVC 開發架構，分離 Model、View、Controller，使得開發過程更加精確，減少開發複雜度。

儘管 Express 本身為最簡化的開發框架，但是開發人員已經相繼創建了完善的中介軟件，幾乎解決所有 Web 開發所會面臨到的問題。

### 三、Web3.js

現今有許多 Dapp 函式庫可以用來跟 Ethereum 網路溝通，像是 Web3j(Java)、Web3.py(Python)、Web3.js(Javascript)。我們採用 Web3.js 的原因為其是目前開發最完善之函式庫且資源量豐富，以及能與前端 Javascript 和後端 Node.js 完全相容，大幅減少開發之困難性。

Web3.js 是由 Javascript 所編譯的 Ethereum Javascript API，其提供了一些以太坊之基礎操作，如：getBalance、sendTransaction 等，也能利用 Web3.js 來佈署智能合約至以太坊網路上。Web3.js 不像 Geth 本身就具有 Json-RPC Server 之功能，它必須要透過特定的 Json-RPC Server 才得以與以太坊區塊鏈互動，Json-RPC Server 包括 Metamask、Infura、Geth Node、Ganache Testrpc。

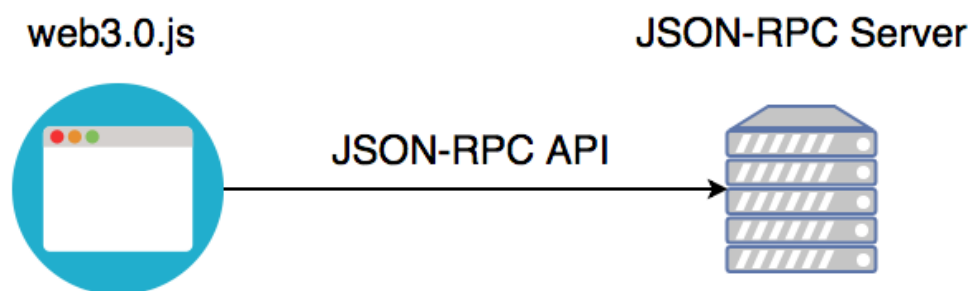


圖 4-1 Web3 與 Json-RPC

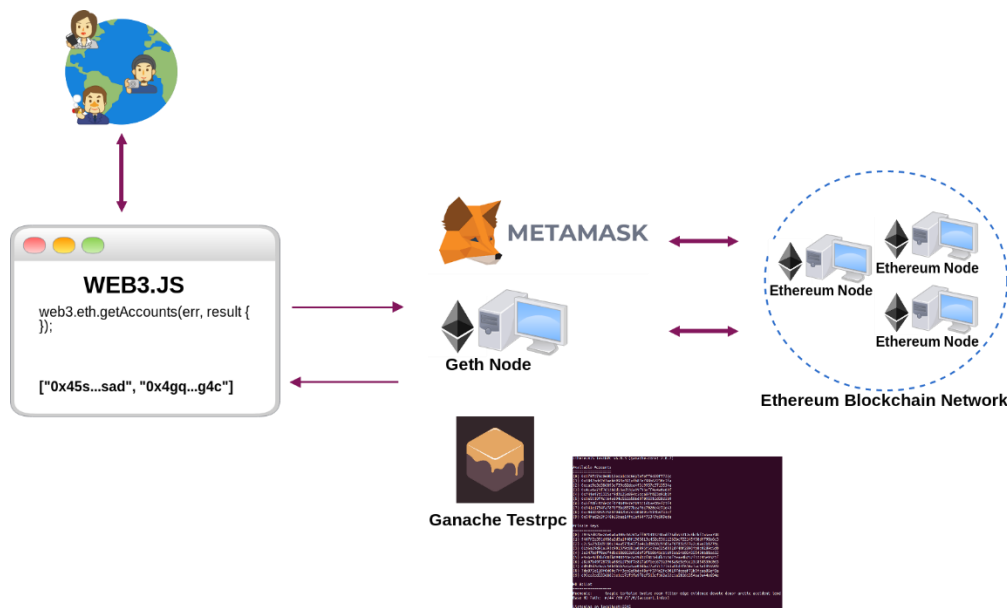


圖 4-2 Web3 與以太坊之串接

來源：ReturnValues-Blockchain Academy

#### 四、Database

此系統之數據資料大部分皆存取於以太坊之智能合約中，但用於驗證使用者之敏感性資料，如：帳號、密碼等必須存於伺服器端之資料庫，區塊鏈之公開透明性會導致這些資料洩漏，若使用加密技術保存上鏈，又會導致加解密時間過冗，驗證時間大幅提升，因此必須創建資料庫來保存敏感性資料。我們選用 MySQL 來作為我們後端之資料庫，其原因如下：

1. 是開源資料庫，提供的接口支持多種語言連接操作。
2. 體積小、速度快、總體擁有成本低，開源、支持多種作業系統。
3. MySQL 的核心程序採用完全的多線程編程。線程是輕量級的進程，它可以靈活地為用戶提供服務，而不佔用過多的系統資源。
4. 支持大型的資料庫，可以方便地支持上千萬條記錄的資料庫。作為一個開放原始碼的資料庫，可以針對不同的應用進行相應的修改。
5. MySQL 有一個非常靈活而且安全的權限和口令系統。當客戶與 MySQL:伺服器連接時，他們之間所有的口令傳送被加密，而且 MySQL 支持主機認

證。

6. MySQL 同時提供高度多樣性，能夠提供很多不同的使用者介面，包括命令行客戶端操作，網頁瀏覽器，以及各式各樣的程序語言介面，例如 C+，Perl，Java，PHP，以及 Python。你可以使用事先包裝好的客戶端，或者乾脆自己寫一個合適的應用程式。MySQL 可用於 Unix，Windows，以及 OS/2 等平台，因此它可以用在個人電腦或者是伺服器上。
7. 擁有一個非常快速而且穩定的基於線程的內存分配系統，可以持續使用而不必擔心其穩定性。

## 五、Metamask

MetaMask 是在瀏覽器中與 Dapps 進行交互的最簡單方法，由於為瀏覽器端元件，因此只適用於系統前端，可優化存取區塊鏈上之資料，動態顯示數據較低延遲，以下為 MetaMask 之特點：

1. 設有網頁前端與以太坊之接口，有 Json-RPC Server 之功能。
2. 電子錢包功能，能顯示帳戶以太幣或是 ERC20 代幣之餘額。
3. 由於具有錢包功能，能進行轉帳或發行交易之區塊鏈相關操作。
4. 可快速切換不同之以太坊區塊鏈，如：主鏈、Ropsten、Rinkeby、本機端私鏈。
5. 為瀏覽器之擴充插件，取得與安裝容易，且支援多種瀏覽器。

MetaMask 為網頁客戶端之以太坊接口，以及擁有管理客戶電子錢包私鑰之功能，因此若系統需要客戶簽署交易之相關操作，如：使用者以加密貨幣兌換加真實貨幣，需從使用者轉帳給網頁開發者(發幣者)，即透過 MetaMask 視窗提醒使用者進行簽署與存取以太坊。

## 六、Infura

若要部署或存取以太坊智能合約需透過以太坊節點才能進行操作，但自行管理節點需耗費大量時間和資源，而 Infura 給予以以太坊主鏈和測試鏈的節點供使

用者申請使用，其提供擴充性高的區塊鏈基礎建設，且為一個簡單容易使用的開發人員工具，擁有安全、可靠、擴充性高的接口存取以太坊，省去管理節點的煩惱，更專注於開發 DApp。使用者只須至 Infura 官方網站申請註冊，即可獲得 Json-Rpc 之接口 Api 以連結以太坊網路。

Infura 本身所提供之節點接口只適用於系統後端，並完全相容於 Node.js 之開發伺服器，為了達成簽署交易自動化，凡是透過網頁開發者發起交易之操作，如：使用者以真實貨幣兌換加密貨幣，需從網頁開發者(發幣者)轉帳給使用者，加上系統後端擁有資料保密性，我們將開發者之前包私鑰放入後端，並等待交易訊號進行自動化簽署，透過 Infura 存取以太坊。

## 七、Remix IDE

Remix IDE 是一款基於瀏覽器的整合開發環境，最主要之功能為編譯智能合約以及以太坊之相關操作，也是 Solidity 官方目前最推薦之開發環境，其最大的好處為不需安裝，可以直接透過瀏覽器開啟即用。而 Remix IDE 的功能也相當全面，比如：部署智能合約、支援以太坊主鏈與眾多測試鏈並且能快速轉換、程式碼除錯、程式碼警告、錯誤提示、執行日誌輸出等。

此系統透過 Remix 來撰寫各式合約，並能搭載 Metamask 發送交易部署合約，由於 Remix 必須手動部署合約，適用於只能部署一次之合約，如：代幣合約，其於合約需透過 Remix 編譯無誤後轉換為 Byte Code，再透過 Web3.js 進行部署。

## 第二節 系統架構

### 一、系統元件串接

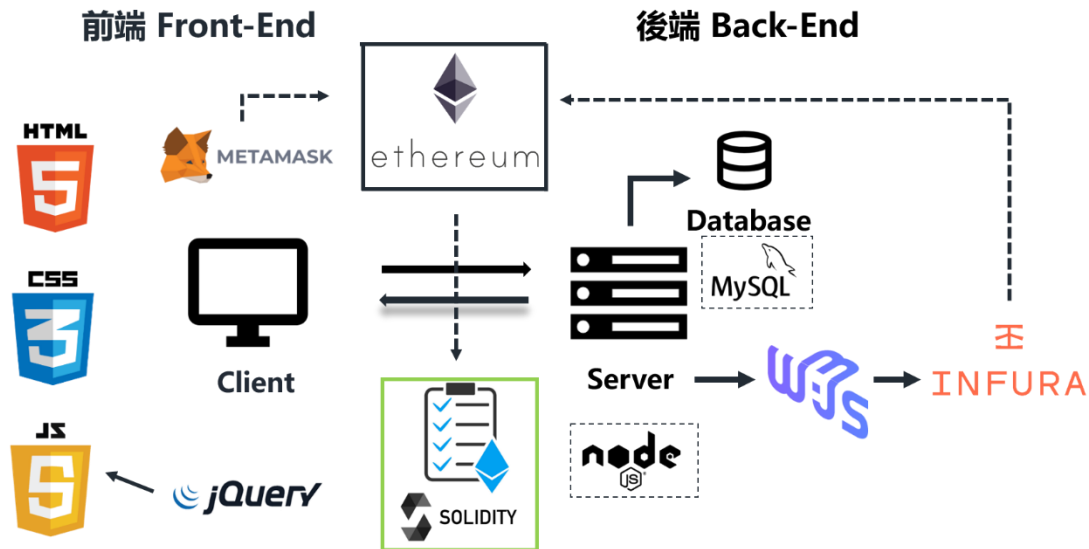


圖 4-3 系統元件串接

圖 4-3 為上述所使用到之系統元件串接整合圖，以下將分為前端、後端、以太坊三部分做說明：

- 前端 Front-End

此系統使用傳統前端三大元件：HTML、CSS、Javascript 來呈現各個介面，並搭載 JQuery 使 Javascript 編寫時能更加精簡流暢。而 Metamask 作為前端介面與以太坊之存取管道，能抓取智能合約之即時資料，大幅降低資料更新之延遲性。除了上述之外，系統將強制提醒使用者安裝 Metamask 瀏覽器元件，否則將無法使用本系統，最主要之原因為某些系統功能操作必須由使用者簽署發起交易，如：加密貨幣兌換真實貨幣必須轉帳其加密貨幣給予發幣者、暫停與繼續投資程式、投資程式入金與全數賣出，上述操作能藉由系統前端通知使用者瀏覽器之 Metamask 提醒用戶簽署交易，且 Metamask 也能有效控管使用者電子錢包私鑰，增加其安全性。

- 後端 Back-End

伺服器使用 Node.js 之 Express 作為後端框架，原因為能完全兼容後端存取以太坊之操作，並使用 Mysql 為資料庫儲存敏感性資料，如：會員帳號、密碼等，其餘資料皆存於區塊鏈上。後端使用 Node.js 套件之 Web3.js 能更簡易、快速的編譯以太坊之相關操作，並使用 Infura 作為後端與以太坊之接口。

- 以太坊：目前使用 Ropsten Testing Network 作為開發之測試鏈，等開發完全後也能快速切換成主鏈。前後端接上以太坊後，即可直接存取已發布之智能合約。

## 二、使用者操作流程

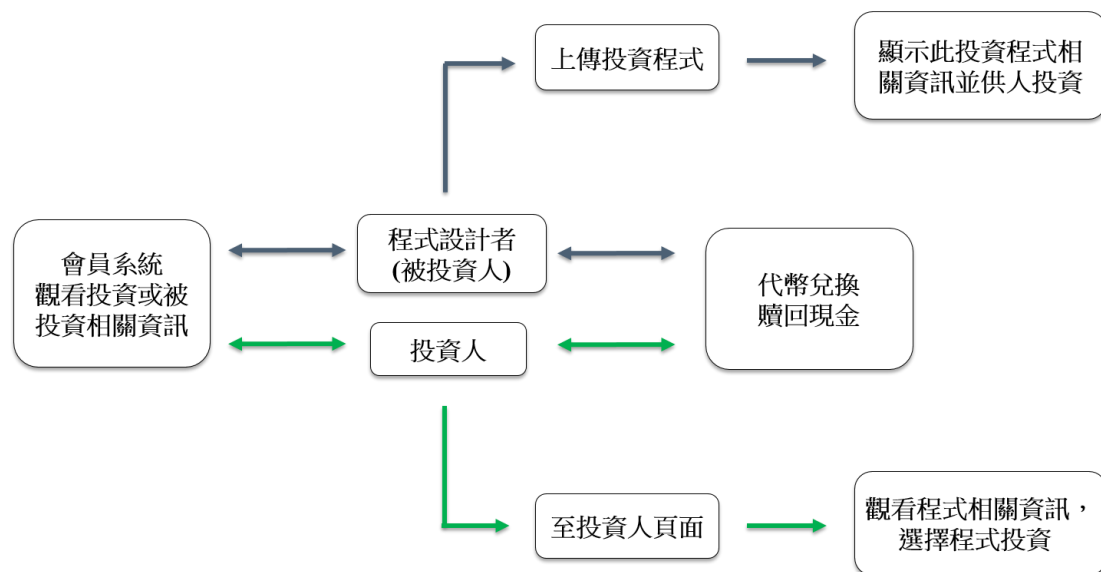


圖 4-4 使用者操作流程

圖 4-4 為此平台之使用者操作流程，以下將分為程式設計者(被投資人)與投資人兩部分做說明：

- 程式設計者(被投資人)：透過會員系統進行註冊與登入，可至會員專區觀看與更新其帳戶資訊和區塊鏈與此帳戶相關之操作紀錄，並能查看過往之程式被投資數據。在進行任何操作前，須至代幣兌換區進行匯兌，因為上

傳程式需扣除些許手續費，一旦有了加密貨幣並達特定數量，即可至程式上傳區進行上傳並設定客製項目，如：前置手續費、後置手續費、程式名稱與代號、程式描述等，完畢後此程式之相關資料即顯示在投資頁面供人投資。

- 投資人：透過會員系統進行註冊與登入，可至會員專區觀看與更新其帳戶資訊和區塊鏈與此帳戶相關之操作紀錄，並能查看過往之投資紀錄與數據。在進行投資前，須至代幣兌換區進行匯兌，因為系統需使用加密貨幣進行投資，完畢後即可至投資頁面查看所有程式之相關資訊，選定後填入投資金額即可進行投資，並依照投資之程式輸出自動連結券商進行下單。

### 三、系統運作流程

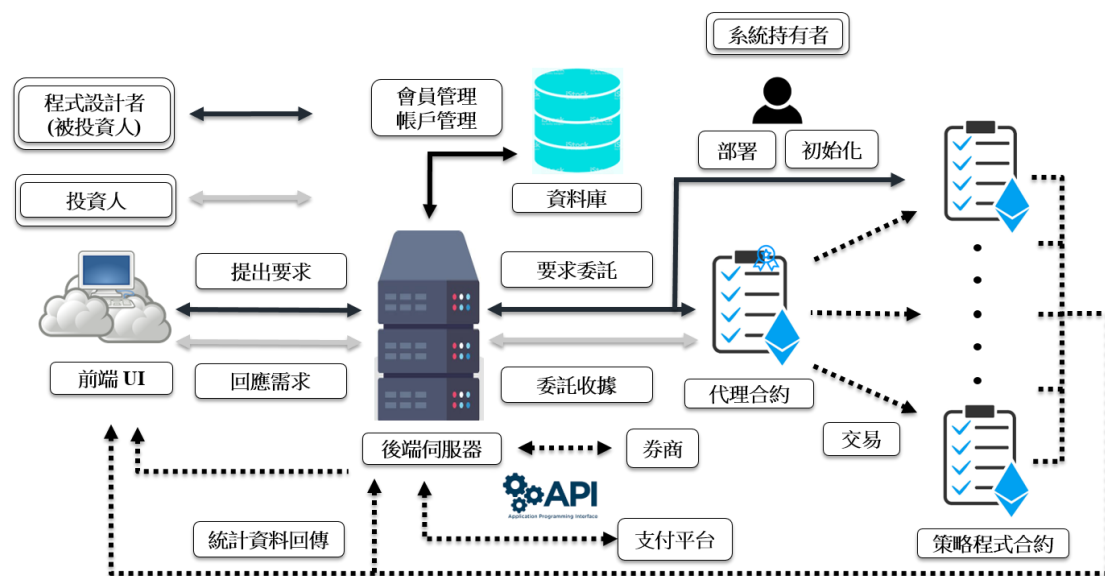


圖 4-5 系統運作流程

圖 4-5 為系統運作流程，以下將介紹此系統流程之特點：

- 代理合約：代理合約主要處理兩種功能，一個為 ERC-865 之實作，另一個為 Internal Transaction，ERC-865 擁有 ERC-20 之發行客製化加密貨幣之功能，並提供轉帳、授權轉帳等金融操作，除了加幣貨幣外，其能夠委託其他帳戶代為發送交易，而不用支付以太坊之以太幣手續費，而本系統特色



之一為使用者只需兌換加密貨幣而不需自備以太幣，以減少複雜性，因此有關使用者發送交易之操作皆由系統方代為支付與發送。Internal

Transaction 為代理合約發送交易給策略程式合約，透過這樣的方式能增加合約間的彈性，比如策略程式合約架構有新版本的更新，只需改變傳入代理合約之策略程式合約位址，即可轉嫁操作新版本策略程式合約，除了上述之外也規定凡是操作策略程式合約必須透過代理合約，能使策略程式合約之安全性增加，並只需要控管代理合約之存取即可。由於發行加密貨幣與創建 Internal Transaction 接口不需要重複建立，因此只有一張代理合約。

- 策略程式合約：每個策略程式將對應一個專屬之智能合約，其記錄策略程式之相關設定與投資數據，因此若程式設計者擁有多支策略程式，即能擁有多張策略程式合約。
- 部署、初始化：當程式設計者上傳程式後將會發送兩筆交易，部署策略程式合約與程式客製資訊初始化，而這兩筆交易皆委託系統持有者代為操作，原因為創建合約時必須強制填入某些選項，如：代理合約位址、代理合約持有者等資訊以控制合約特定操作，如果交予客戶自行發送，若在上鏈前將合約重要變數竄改，將難以存取此合約。
- 券商：一旦投資者入金後，系統後端立即監聽其投資之程式，將其資金按照程式訊號進行操作，並通知券商進行下單之動作，待成功後將通知投資者與設計者雙方，倘若投資者想中途撤出投資或是目前虧損已達投資金額，將通知券商進行全數賣出之動作，並歸還投資者與設計者之加密貨幣，即結束此筆投資。
- 支付平台：使用者在加密貨幣匯兌區時，系統透過第三方支付歐富寶來進行相關金融操作，並支援 ATM 轉帳、信用卡等付款方式，付款完成後將加密貨幣轉入使用者之電子錢包中。

### 第三節 E 投睿(Etoro)問題解決

依照先前所述，Etoro 投資平台使用傳統集中式資料庫，導致產生出兩個潛在的問題點，分別為非透明性之平台數據與策略程式在投資期間有無被擅自修改，以下將詳細說明如何克服此困境，以提升投資者信任之投資平台。

#### 一、揭露非透明之平台投資數據

當投資人選定策略程式後並進行投資，投資期間之每日盈餘、虧損等投資相關數據皆會寫入區塊鏈智能合約中，本平台呈現之數據皆是存取於區塊鏈上之智能合約，而且資料一旦上鏈後所有人包括本平台之管理者皆無法進行更改，任何人只要擁有連網計算機可至區塊鏈以太坊智能合約查詢平台(如 Etherscan)進行查看，即可確認某個投資人之投資報酬率等相關投資數據與合約上有無相符，使用者就能確定平台上之所有資訊皆可信任，投資時必定對本平台更有信心且必定無任何數據造假。

所有數據皆公開透明後，策略設計人之所有財務報表資訊皆會顯示於平台上，若其數據顯示成效偏低，投資人跟單機率必定偏小，因此長期下來能藉此促進設計人改進其策略或是淘汰 惡意、詐騙之投資策略，反之，投資策略效益高之模型也能藉此賺取大量跟單手續費，而投資人也能藉由此策略而投資成功，達成雙贏局面。

#### 二、保證投資策略未被擅自修改

當策略設計者完成擬定投資策略，將其程式輸出成執行檔並上傳完成後，平台自動將其執行檔以 Sha256 進行雜湊，並將雜湊值寫入其對應之策略程式智能合約中，資料一旦上鏈後所有人即無法再更改，平台管理人亦同，並且任何人皆能檢視。當策略設計者對其原有策略程式有所更改並重新上傳，雜湊值必定與原本智能合約所存之雜湊值不相符，系統即判定其策略程式必定有更改，拒絕存取更新。

策略程式轉檔成執行檔主要理由為可以讓後端系統自動監聽其輸出，而平

台管理者也無法藉由執行檔逆向工程竊取其策略邏輯，藉此保障策略設計人之權益，也能使其更安心使用本平台。

## 第四節 智能合約編譯

### 一、代理合約 Proxy Contract

#### (一) ERC-865

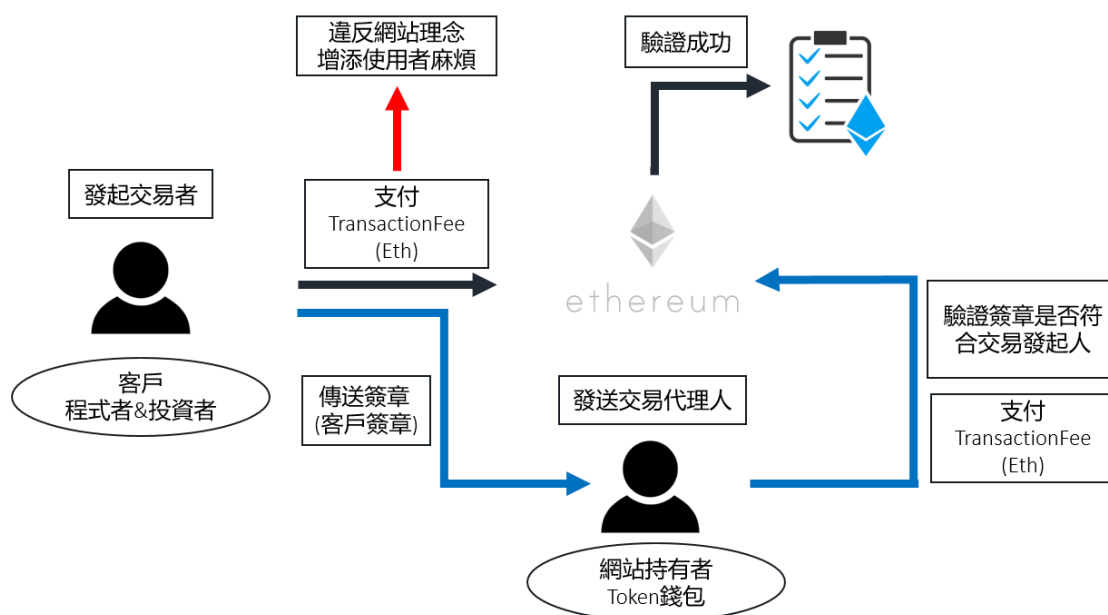


圖 4-6 委託交易

平台在特定情況下，如：會員以加密貨幣兌換真實貨幣、策略設計者對其程式合約之控制等，由於平台管理者無法操控使用者之電子錢包帳戶，因此使用者必須自行發起交易，根據區塊鏈以太坊之運作機制，發起交易方得支付以太幣之手續費給予礦工，而本平台之特色為使用所有功能只需支付平台發行之加密貨幣，若會員還須自行兌換以太幣以支付手續費，將會使得平台程序過為繁瑣且造成會員多餘的麻煩，進而導致使用意願下降。

ERC-865 擁有委託交易之功能，以委託代理之方式將交易給予委託人代為發送，能使得交易交由平台管理者代為發送而會員不需支付以太坊交易手續

費。當進行相關操作時，系統將交易資訊發送至前端並且要求會員使用私鑰簽署此交易資訊，此時客戶端之瀏覽器插件 Metamask 電子錢包將會彈出簽章視窗以利使用者進行簽署，隨後將此簽章傳送至 ERC865 合約進行解析驗證即可發送交易並扣除被委託人之以太幣手續費，完成委託程序。以下將講解委託交易之詳細流程：

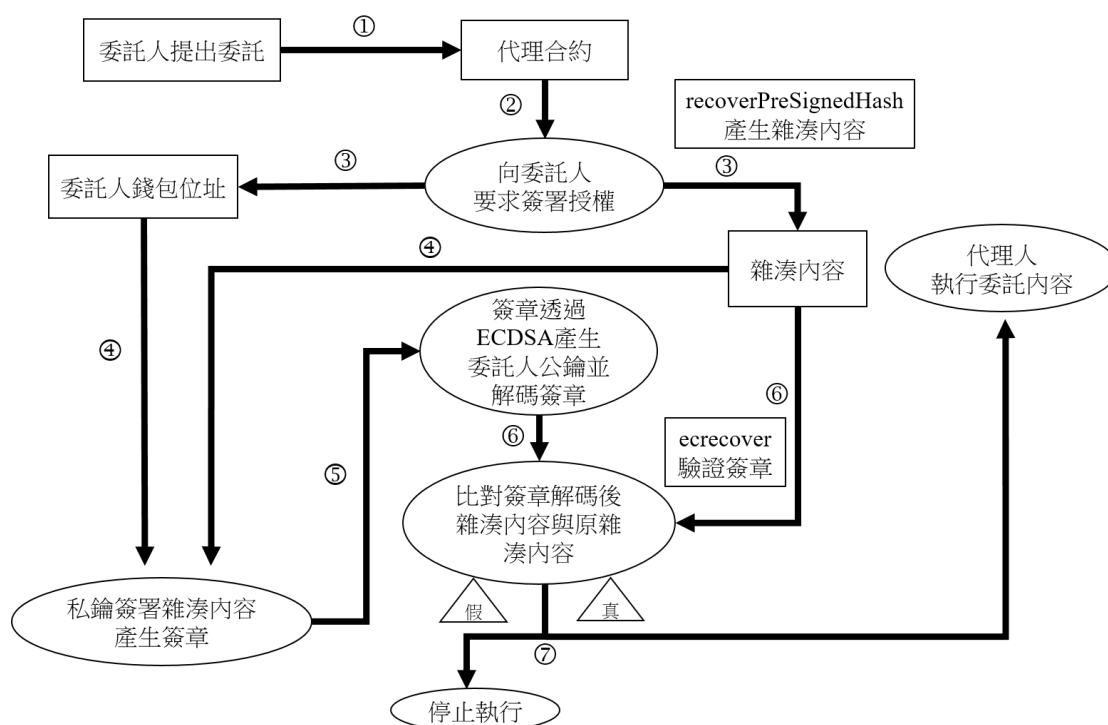


圖 4-7 委託交易驗證流程

1. 會員提出委託需求。
2. 系統存取其操作相對應智能合約之函式。
3. 系統通知會員並要求其簽署交易，並同時透過智能合約產生雜湊內容。
4. 會員使用其電子錢包之私鑰簽署雜湊內容，形成簽章。
5. 將簽章打包成交易並傳送至 ERC865 智能合約中。
6. 使用橢圓曲線數位簽章演算法(Elliptic Curve Digital Signature Algorithm, ECDSA)透過簽章產生出公鑰並解碼簽章，簽章解碼後將會得到簽章前之內容並與原雜湊內容比較是否一致。

7. 若不一致則認定為委託人並非以其私鑰進行簽章，形成偽造簽名，並停止執行委託內容，反之則合法簽名並執行委託內容。

表 4-1 ERC-865 智能合約變數與函式總覽

變數名稱	功能
SafeMath	為一個函式庫，避免無號數(unsigned integer)進行四則運算時造成溢位，導致值出現嚴重錯誤。
owner	儲存此合約之持有者序號(電子錢包位址)，部署合約時建構子即寫入部署者序號，此序號為系統擁有者之電子錢包位址。
balances[錢包位址]	儲存所有使用者持有加密貨幣之數量。
totalSupply	儲存發行加密貨幣之總數量。
name	加密貨幣名稱。
symbol	加密貨幣代號。
decimals	加密貨幣位數，通常為 18 位以符合以太幣之最小幣值。
Initial_Supply	初始發行加密貨幣數量。
Function_kill	刪除此合約，只有合約擁有者能進行操作。
函式名稱	功能
transferOwnership	轉移合約持有者身分，此函式只有現任持有者可操作。
totalSupply	檢視發行加密貨幣之總數量。
balanceOf	檢視某使用者持有加密貨幣之數量。
transfer	使用加密貨幣進行轉帳，用於使用者以真實貨幣兌換加密貨幣，發幣者轉帳加密貨幣予使用者。

transferPreSigned	透過代理委託的方式，請某個帳戶代為發送交易進行轉帳，以太坊交易手續費由委託帳戶進行支出，用於使用者以加密貨幣兌換真實貨幣，其必須發送交易才能將加密貨幣轉帳予發幣者，而交易手續費必須使用以太幣支付，但基於本網站不需客戶兌換以太幣之原則，所以委託代理者支出手續費，此代理者為發幣者。
recoverPreSignedHash	雜湊交易內容，並產出私鑰簽章前之文件，用以比對公鑰解密後與私鑰簽章前之內容是否一致。
ecrecover	以公鑰解碼已簽章之內容，並比對解碼後內容是否與簽章前一致，即驗證簽章之身分。

## (二)Internal Transaction

表 4-2 Internal Transaction 智能合約變數與函式總覽

函式名稱	功能
controlPreSigned	此函式參照 transferPreSigned 之概念進行代理委託發送交易，但不是進行轉帳，而進行投資與被投資之合約控制，下列四種皆為合約控制操作。
proxy_inActiveStrategy	給予特定程式合約位址，並以合約傳送交易給合約之方式進行，此函式將呼叫程式合約 inActiveStrategy 之函式。
proxy_ActiveStrategy	給予特定程式合約位址，並以合約傳送交易給合約之方式進行，此函式將呼叫程式合約 ActiveStrategy 之函式。
proxy_createCommit	給予特定程式合約位址，並以合約傳送交易給合約

	之方式進行，此函式將呼叫程式合約 createCommit 之函式。
proxy_endCommit	給予特定程式合約位址，並以合約傳送交易給合約之方式進行，此函式將呼叫程式合約 endCommit 之函式。

## 二、策略程式合約 CopyMatch Contract

表 4-3 策略程式智能合約變數與函式總覽

變數名稱	功能
numCommits	媒合成功次數。
numCopyTraders	媒合成功人數。
MatchFeeCopyTrader	系統媒合手續費，向投資人索取。
MatchFeeHolder	系統媒合手續費，向程式設計者索取。
DeployFee	部署合約手續費。
addrProxyOwner	代理部署人，此為系統擁有者。
addrProxy	代理合約位置。
addrHolder	策略程式撰寫人。
symbol	策略程式代號。
Struct Strategy	策略程式之相關資訊，其為結構型資料型態並包含：
boolActive	策略是否激活。
hashStrategy	策略程式雜湊值。
minAmount	最低投資金額。
maxAmount	最大投資限額。

frontVarFee	前置顧問費，依投資金額比率抽取。
frontFixFee	前置顧問費，固定金額。
backFee	後收顧問費，依投資結束之利潤比率抽取。
Struct Commit	策略程式之投資者入金資訊，其為結構型資料型態並包含：
boolCommit	是否媒合。
startTime	開始時間。
endTime	結束時間。
commitAmount	投資金額。
commitFees	成交手續費。
usedAmount	累計已投資金額。
commitReturn	本次交易總收入(含本金)。
totalReturn	本次委託下單報酬率。
numCopies	實際委託下單累計次數。
otherData	其他資訊。
commit[跟單人位址][跟單次數]	根據跟單人位址與跟單次數可以查詢該次之Commit 內所有資訊。
commitId[跟單人位址]	根據跟單人位址查詢該跟單人為第幾次投資此程式。
groupTrader	此程式之所有跟單者的位址。
struct copyReceipt	跟單結果明細，其為結構型資料型態並包含：
time	開始時間。
Amount	金額。( + 為賣出， - 為買入)
copyTrades[跟單人位]	根據跟單人位址、第幾次投資序號、下單次數可以



址][第幾次投資序號][下 單次數]	取得該次投資之跟單結果明細 copyReceipt。
struct copyRecord	儲存交易紀錄，其為結構型資料型態並包含：
Inject	投入金額。
Outcome	賣出金額。
historyRecord[年度][月 份][日]	根據年度、月份、日即可查詢當天之總交易紀錄 copyRecord。
<b>函式名稱</b>	<b>功能</b>
inActiveStrategy	如果使用者身為程式設計者，可以決定自己被投資之程式是否暫停投資，預設為可被投資狀態。
ActiveStrategy	如果使用者身為程式設計者，可以決定自己被投資之程式是否繼續投資，預設為可被投資狀態。
createStrategy	初始化智能合約，寫入策略資訊，如：前後置手續費、策略程式雜湊值、策略程式代號等。
createCommit	如果使用者身為投資人，當選定投資程式後，即呼叫此函式，寫入欲投資金額、投資時間、其他投資相關資料，隨後即透過投資之程式訊號與券商進行下單並扣除投資金額之相對加密貨幣數量。
endCommit	如果使用者身為投資人，可以自行決定何時終止某個程式之投資，當確定終止後，即呼叫此函式，並寫入終止時間、其他投資相關資料，隨後通知券商進行全數賣出，歸還投資餘額加密貨幣。
calcFees	計算前置總手續費(固定手續費+依投資金額抽成)。
calcBack	計算後置總手續費(投資完成回報金額抽成，若賠錢則不收取)。

calcReturnRate	計算當次報酬率。
calcMonthlyReturnRate	計算當月報酬率。

## 第五節 頁面呈現

### 一、主頁

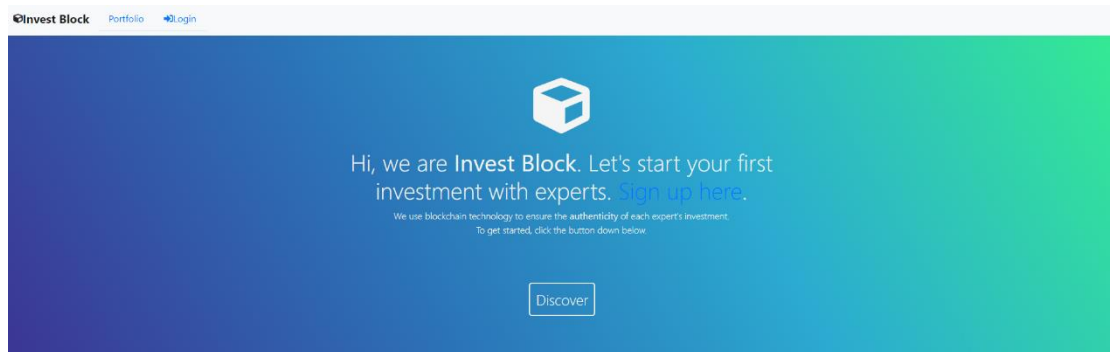


圖 4-8 主頁

### 二、登入、註冊、登出

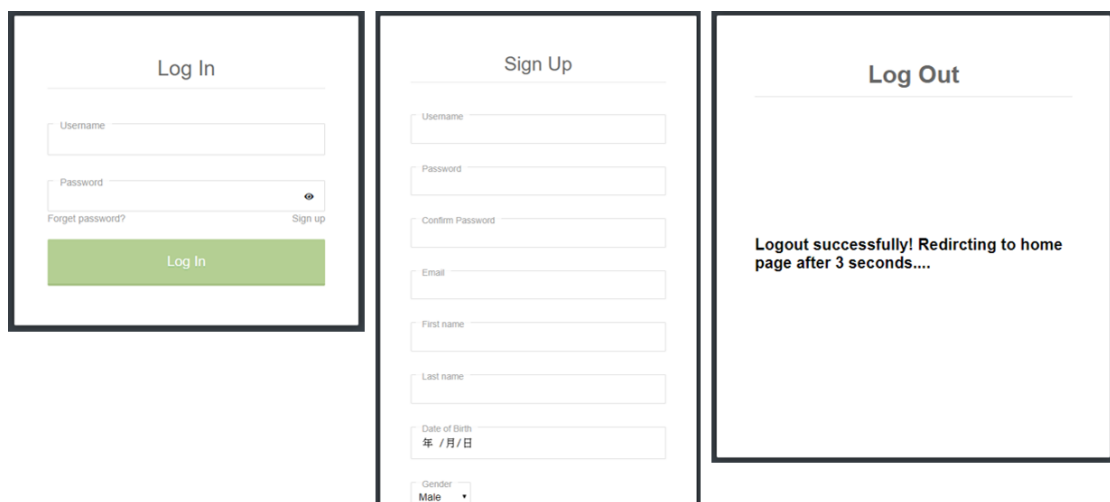


圖 4-9 登入、註冊、登出

系統之登入、註冊以及登出之頁面，其透過資料庫之存取比對以及寫入帳戶資訊，並利用 Session 記錄使用者之登入狀態，以提供相對應之頁面呈現。登出即刪除 Session 並禁止使用者存取特定區塊鏈操作相關頁面。

### 三、登入後主頁



圖 4-10 登入後主頁

比對帳戶資訊成功後即可登入成功，於主頁上更改為登入後介面，並提供使用者以下專區：

- 會員資料(Member Info & My Account)：提供使用者查看並修改其會員之註冊資料以及其帳戶於區塊鏈上所有操作紀錄。
- 代幣兌換 & 贖回(Currency Exchange)：提供使用者兌換本平台所提供之加密貨幣，利用加密貨幣進行本平台之所有操作。
- 程式交易專區-被投資者(Program)：此區提供策略程式設計者之相關操作，如：上傳策略程式、策略程式初始化、暫停策略程式等。
- 瀏覽策略程式(Portfolio)：提供投資者瀏覽所有策略程式，並觀看其投資相關圖表數據，最後選擇理想之策略程式進行投資入金。
- 投資專區-投資者(Investor)：此區提供投資者之相關操作，如：檢視目前投資之程式現況、即時盈虧、歷史投資資訊等。
- 登出(Logout)

#### 四、會員資料(帳戶專區)

##### (一)關於我

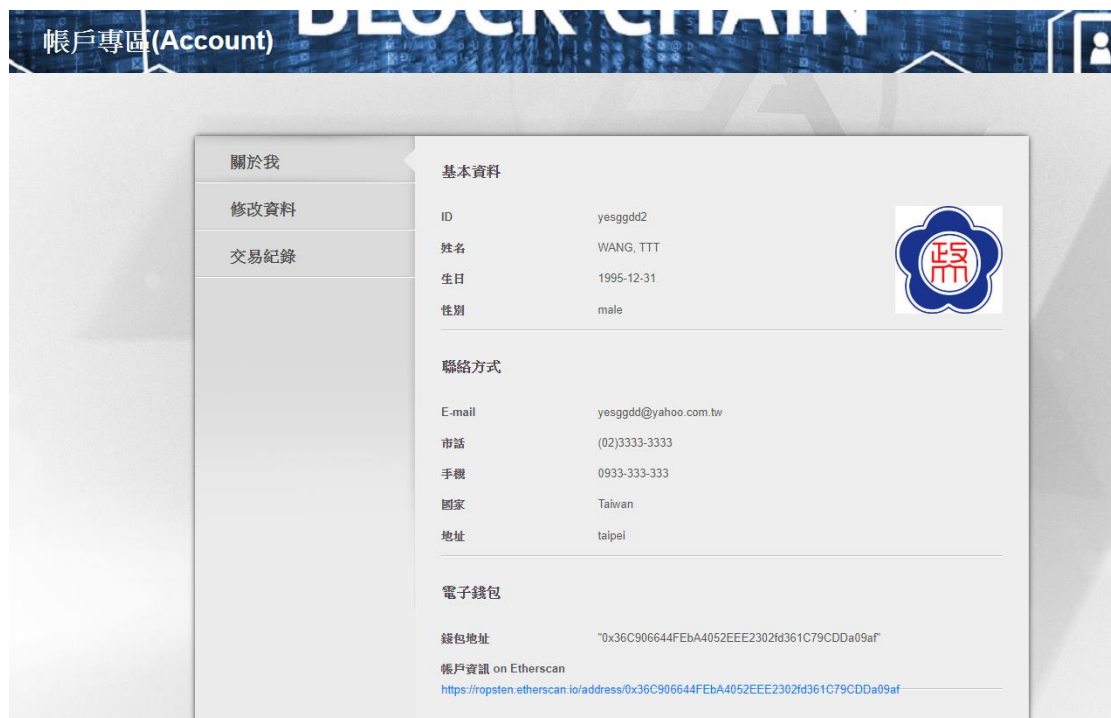


圖 4-11 關於我

帳戶專區提供三項功能：關於我、修改資料、交易紀錄。「關於我」頁面顯示使用者註冊時所填寫之資料，其包含：姓名、Email、電子錢包地址等。

## (二)修改資料

帳戶專區(Account)

關於我

修改資料

交易紀錄

基本資料

ID: yesgdd2

姓名: WANG TTT

生日: 1995/12/31

性別: Male

聯絡方式

E-mail: yesgdd@yahoo.com.tw

市話: (02)3333-3333

手機: 0933-333-333

國家: Taiwan

地址: taipei

電子錢包

錢包地址: 0x36C906644FEbA4052EEE

帳戶資訊 on Etherscan  
<https://ropsten.etherscan.io/address/0x36C906644FEbA4052EEE2302fd361C79CDDa09af>

選擇檔案 未選擇任何檔案

確認修改

圖 4-12 修改資料

使用者可以透過「資料修改」頁面來進行修改自己的會員資料，並可於此上傳會員照片。

### (三)交易紀錄

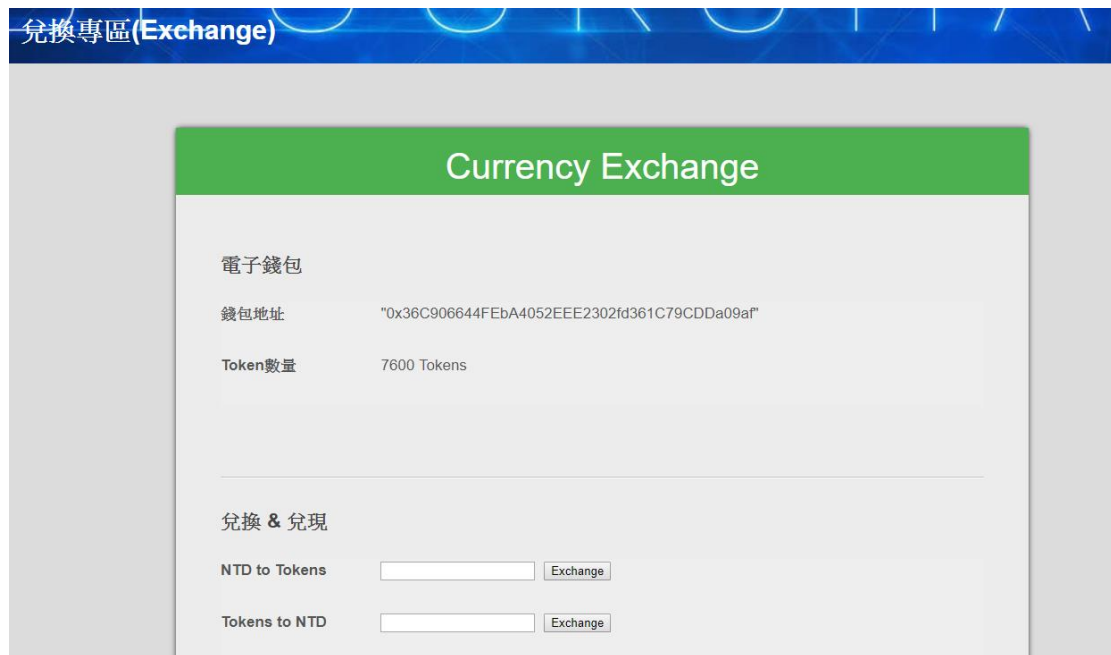
帳戶專區(Account)	
關於我	交易紀錄
修改資料	日期 2019/10/27 18:38:32 GMT+8
交易紀錄	類別 Transfer
	交易哈希值 0xcb27e7776e9c7838b9eea4d6b8cfebaae1708e1a1442db7d269e17b570dccbd From Address 0xd0a8800973cbef2639ebf79c019c8a1611c7d810
	Contract 0x72682d0d54c7ed7cdddaa66e6dd7171f2b9c626c
	To Address 0x36c906644feba4052eee2302fd361c79cdda09af
	資料 10000 Tokens
	Etherscan查看 <a href="https://ropsten.etherscan.io/tx/0xcb27e7776e9c7838b9eea4d6b8cfebaae1708e1a1442db7d269e17b570dccbd">https://ropsten.etherscan.io/tx/0xcb27e7776e9c7838b9eea4d6b8cfebaae1708e1a1442db7d269e17b570dccbd</a>
	日期 2019/10/29 12:32:10 GMT+8
	類別 Transfer
	交易哈希值 0x4a273be92b0b3ae59c4de51ae5b41f3e67a8525a387512d514753f24fc379ac4 From Address 0x36c906644feba4052eee2302fd361c79cdda09af
	Contract 0x72682d0d54c7ed7cdddaa66e6dd7171f2b9c626c
	To Address 0xd0a8800973cbef2639ebf79c019c8a1611c7d810
	資料 500 Tokens
	Etherscan查看 <a href="https://ropsten.etherscan.io/tx/0x4a273be92b0b3ae59c4de51ae5b41f3e67a8525a387512d514753f24fc379ac4">https://ropsten.etherscan.io/tx/0x4a273be92b0b3ae59c4de51ae5b41f3e67a8525a387512d514753f24fc379ac4</a>
	日期 2019/10/29 12:32:10 GMT+8
	類別 TransferPreSigned_Transfer_Fee
	交易哈希值 0x4a273be92b0b3ae59c4de51ae5b41f3e67a8525a387512d514753f24fc379ac4 From Address 0x36c906644feba4052eee2302fd361c79cdda09af

圖 4-13 交易紀錄

透過使用者註冊時所填寫之電子錢包地址，來顯示其帳戶在區塊鏈上之所有交易紀錄，包含兌換加密貨幣、合約部署等，而上圖之連結可以轉跳至 Etherscan 上查看交易之詳細內容。為了能迅速更新此頁面之交易資訊，平台只透過網頁前端來存取區塊鏈上智能合約之活動紀錄(Event)，並使用 Metamask 來使平台連接至以太坊，由於不需再經由平台後端處理，因此頁面能低延遲的即時更新資訊。

## 五、代幣兌換 & 贖回(兌換專區)

### (一)匯兌



兌換專區(Exchange)

### Currency Exchange

電子錢包

錢包地址 "0x36C906644FEbA4052EEE2302fd361C79CDDa09af"

Token數量 7600 Tokens

---

兌換 & 兌現

NTD to Tokens

Tokens to NTD

圖 4-14 兌換專區

平台之任何投資相關操作都必須透過平台發行之加密貨幣才能達成，因此會員必須先至兌換專區以新台幣兌換加密貨幣，匯率目前設定為 1：1，經由投資與被投資所賺取之加密貨幣也能透過此專區進行兌現。



## (二) 第三方支付



登入付款 如何註冊



訂單資訊

訂單編號	DX201912051602077ysc		
商店/網站名稱	歐付寶測試店家		
收款方會員編號	2000132		
款項撥至商家時間	立即 (請注意！您的支付款項將於交易完成後，移轉至收款人的電子支付帳戶。)		

商品明細	數量	單價	小計
Tokens	1	1,000	1,000

請務必於訂單資訊下方選擇付款方式，以完成交易

應付金額 NT\$ 1,000  
[刷永豐分3期或24期抽Switch](#)

付款方式

信用卡

 [刷永豐分3期或24期抽Switch](#)

本交易可使用之信用卡：兆豐、花旗、玉山、中信、台新... [看更多](#)

圖 4-15 歐富寶 API 串接

目前本平台可以透過信用卡付款以及銀行轉帳方式來進行加密貨幣之匯兌，並串接第三方支付歐富寶 API 來管理金流。往後將會新增其他之金融匯兌方式，並增加 Paypal 來給予非本國人使用。

### (三)兌換收據

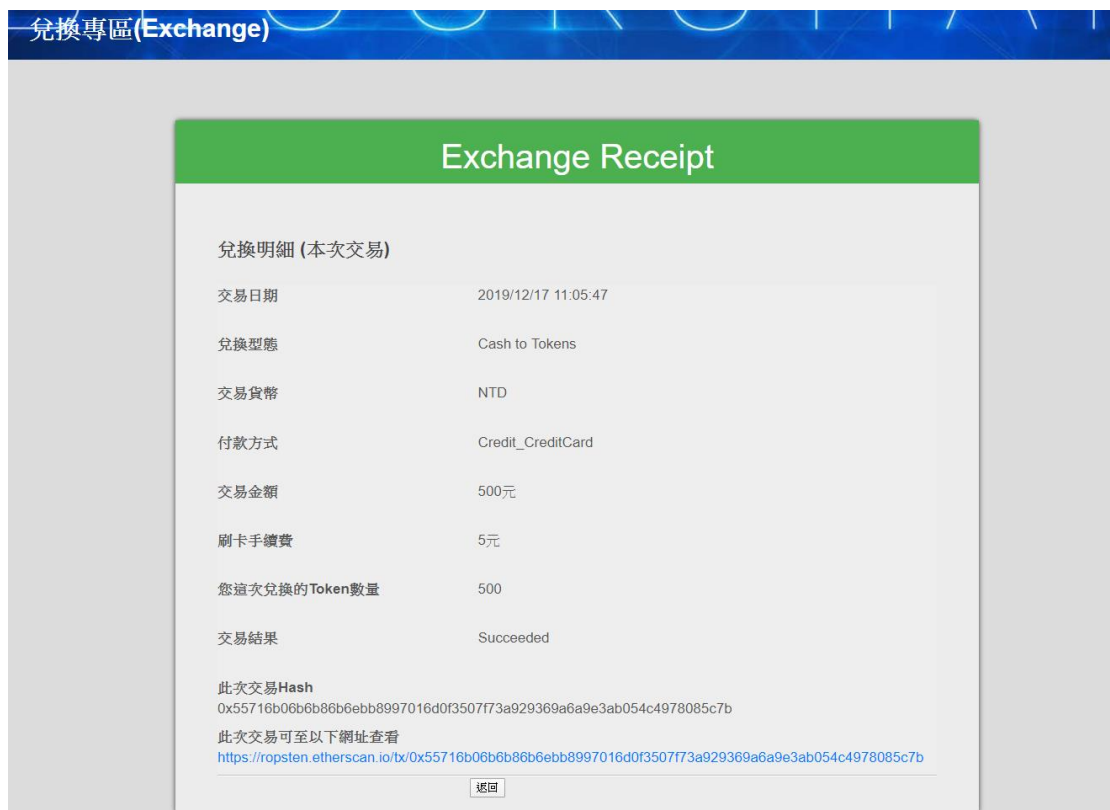


圖 4-16 收據與交易結果

當使用者匯兌完成後將會顯示匯兌結果，如：交易日期、兌換型態、付款方式等資訊。由於加密貨幣為以太坊智能合約 ERC-20 之功能，並且有虛擬貨幣之轉移，因此會產生區塊鏈以太坊之交易，使用者可以藉由點選上圖之連結，至 Etherscan 上查看當筆交易之詳細內容，也能至「會員資料(帳戶專區)-交易紀錄」查看歷史交易記錄。

#### (四)兌換代幣與贖回真實貨幣

- 兌換代幣

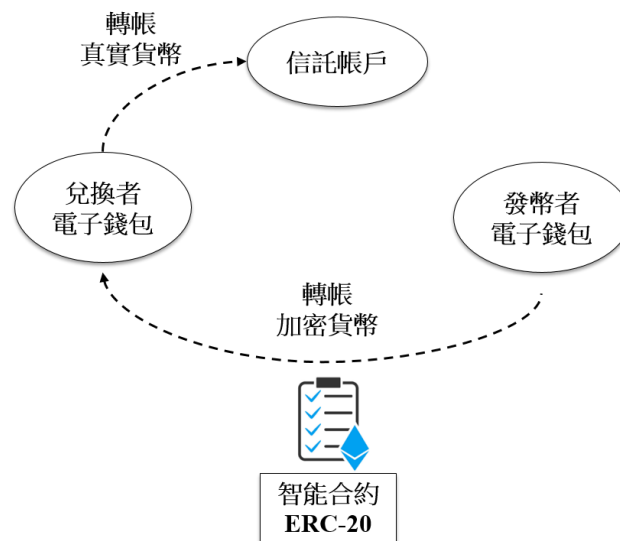


圖 4-17 真實貨幣兌換加密貨幣

使用者經由歐富寶使用信用卡付款或銀行轉帳方式將真實貨幣存入平台提供之銀行信託帳戶，付款完成後平台管理者(也為發幣者)透過區塊鏈交易將對應數量之加密貨幣轉入兌換者之電子錢包，由於發送交易需要電子錢包之私鑰簽署，平台管理者將其發幣者之電子錢包私鑰寫入網頁後端，能達到自動化簽署交易以及私鑰安全性。

平台將與特定銀行申辦信託帳戶，使得當用戶以真實貨幣兌換平台發行之加密貨幣時，系統自動將真實貨幣存入合作之銀行信託帳戶，因此本平台並不能直接獲取真實貨幣或是從信託帳戶擅自取出，交由第三方銀行進行控管，以預防平台隨時撤離與捲款潛逃，增加使用者之投資信任。

- 贖回真實貨幣

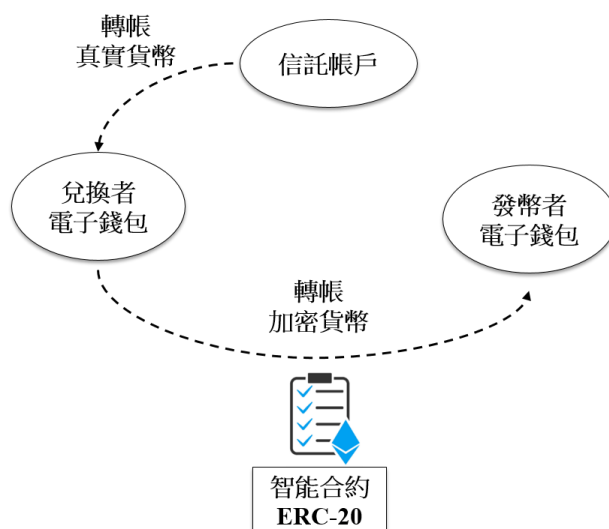


圖 4-18 加密貨幣兌換真實貨幣

使用者需將其電子錢包內之加密貨幣轉帳至發幣者電子錢包，隨後平台將通知銀行信託帳戶歸還等價之真實貨幣。由於欲兌換之加密貨幣是存於使用者之電子錢包，必須從使用者自行簽署交易並發送，因此平台後端將通知客戶端 Metamask 要求用戶簽署交易，如圖 4-19，隨後呼叫代理合約 ERC865 委託平台代為發送以太坊交易，因此使用者就無需支付以太幣手續費。



圖 4-19 Metamask 要求客戶簽署交易

兌換專區(Exchange)

### Exchange Confirmation

兌換確認

兌換型態	Tokens to Cash
兌換貨幣	NTD
欲兌換之Token數量	200
您即將兌換的金額	200 元 (NTD)

簽章資訊

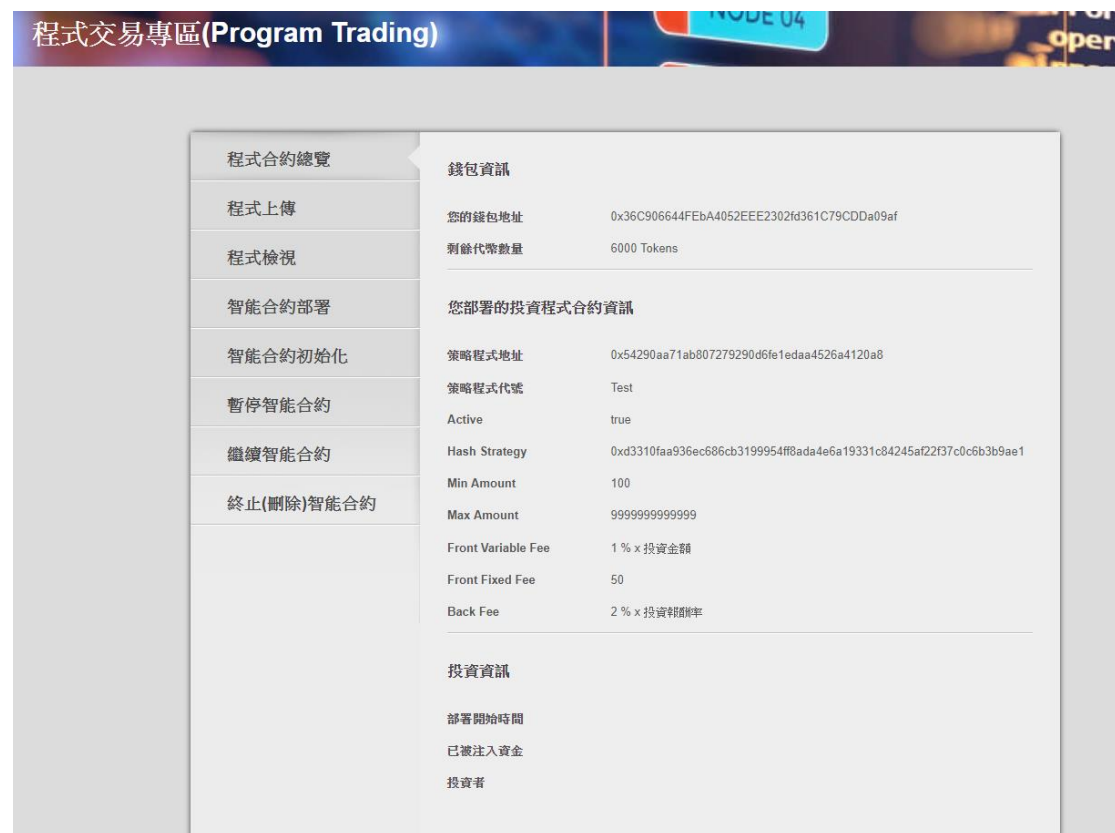
Token Address	0x72682d0d54c7ED7cdDdAa66E6DD7171f2B9c626
TransferSig	0x48664c16
To	0xD0A800973cbEF2639EbF79c019c8a1611C7d81
Value	200
Fee	0
Nonce	29
Signature	0x695f1c5bde8a6b4a8e2ed3595636d818ef4ee923317dc085f44cddb3bdc3c1bd3921e14f05cd00183926f8898144262e9cf3fdb974ba54

Create Signature 確認兌換

圖 4-20 產生簽章與發送確認頁

## 六、程式交易專區(被投資者)

### (一)程式合約總覽



The screenshot displays the 'Program Trading' interface. On the left is a sidebar menu with the following options: 'Program Contract Overview' (selected), 'Program Upload', 'Program Inspection', 'Smart Contract Deployment', 'Smart Contract Initialization', 'Pause Smart Contract', 'Continue Smart Contract', and 'Terminate (Delete) Smart Contract'. The main content area is titled 'Program Contract Overview' and is divided into three sections:

- 錢包資訊 (Wallet Information):**
  - 您的錢包地址: 0x36C906644FEbA4052EEE2302fd361C79CDDa09af
  - 剩餘代幣數量: 6000 Tokens
- 您部署的投資程式合約資訊 (Information about the investment program contract you deployed):**
  - 策略程式地址: 0x54290aa71ab807279290d6fe1edaa4526a4120a8
  - 策略程式代號: Test
  - Active: true
  - Hash Strategy: 0xd3310faa936ec686cb3199954ff8ada4e6a19331c84245af2f37c0c6b3b9ae1
  - Min Amount: 100
  - Max Amount: 999999999999
  - Front Variable Fee: 1 % x 投資金額
  - Front Fixed Fee: 50
  - Back Fee: 2 % x 投資報酬率
- 投資資訊 (Investment Information):**
  - 部署開始時間
  - 已被注入資金
  - 投資者

圖 4-21 程式合約總覽

若使用者為策略程式設計者(被投資人)，可至程式交易專區進行檢視與操作，程式交易專區共有八項功能：程式合約總覽、程式上傳、程式檢視、智能合約部署、智能合約初始化、暫停智能合約、繼續智能合約、終止(刪除)智能合約。一旦策略程式設計人上傳程式並初始化成功後，即可於智能合約總覽頁面上查看合約之狀態與設定以及目前投資此策略之投資者資訊。

## (二)程式上傳

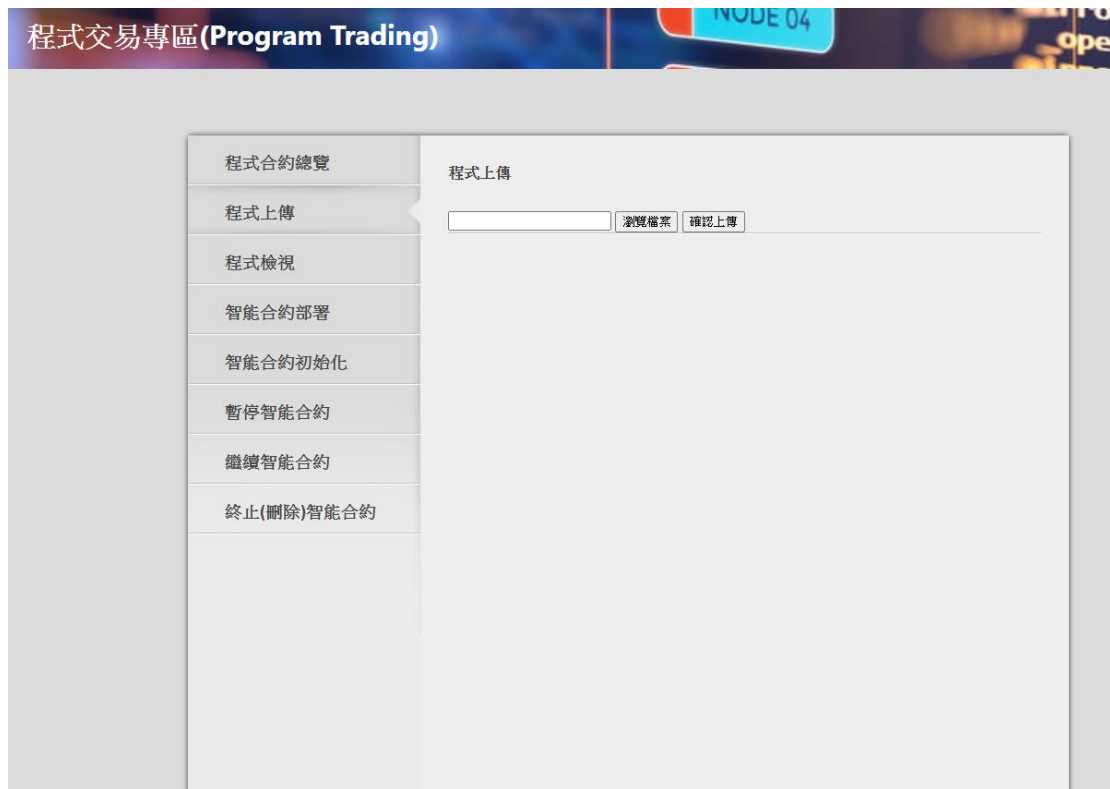


圖 4-22 程式上傳區

策略程式設計者將自己的策略程式設計完成後，需自行轉換成執行檔(executable file)，並於程式上傳區進行上傳。執行檔可以防止平台管理者逆向工程，進而確保設計者之設計機密，增加設計者對平台之信任。上傳完成後立即使用 Sha-256 雜湊此程式，並等待寫入以太坊智能合約，以防止策略人擅自更改投資策略。

### (三)程式檢視

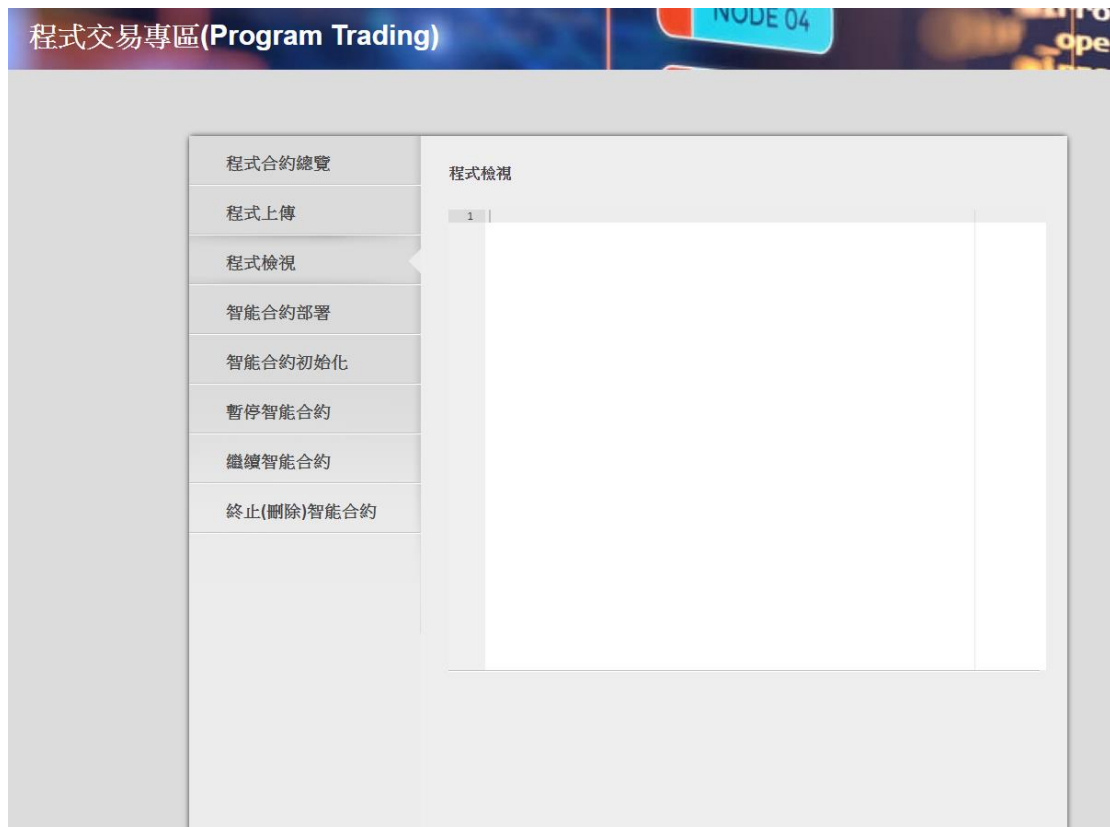


圖 4-23 程式檢視

使用者可於「程式檢視」頁面查看已上傳了哪些策略程式，以及其狀態。



#### (四)智能合約部署

程式交易專區(Program Trading)

程式合約總覽

程式上傳

程式檢視

智能合約部署

智能合約初始化

暫停智能合約

繼續智能合約

終止(刪除)智能合約

部署資料

您的錢包地址  
0x36C906644FEbA4052EEE2302fd361C79CDDa09af

剩餘代幣數量  
6000 Tokens

部署合約手續費  
500 Tokens

簽章資訊

Token Address  
0x72682d0d54c7ED7cdDdAa66E6DD7171f2B9c626C

Transfer Sig  
0x48664c16

To  
0xD0A8800973cbEF2639EbF79c019c8a1611C7d810

Value  
500

Fee  
0

Nonce  
26

Signature  
0xdbbc441d48e18083541e8aa803e732c4b86cb9c2ea2aae9ef44c3b18b4e4ce4904a0051b41120a289780504

① Create Signature

② 確認部署

圖 4-24 智能合約部署

當策略程式設計者上傳完成後，即可至「智能合約部署」頁面部署程式對應之智能合約，部署完成後即可初始化合約，待初始化後才算完成被投資之流程。

## (五)智能合約初始化

程式交易專區(Program Trading) NODE 04

程式合約總覽	合約資料
程式上傳	您的錢包地址 0x36C906644FEbA4052EEE2302fd361C79CDDa09af
程式檢視	剩餘代幣數量 5500 Tokens
智能合約部署	您的程式合約地址 0xacb6ee45abcbe7edbbe91677fc52132aec4c634
智能合約初始化	初始化合約手續費 100 Tokens
暫停智能合約	
繼續智能合約	
終止(刪除)智能合約	

智能合約初始化

Symbol

COB

Hash Strategy

0xd3310faa930ec686cb3199954f0ada4e6a19331c84245af22f37c

Min Amount

100

Max Amount

99999999999

※若未設置則為預設

Front Variable Fee

5

% x 投資金額

Front Fixed Fee

100

Back Fee

5

% x 投資報酬率

簽章資訊

Token Address

0x72682d0d54c7ED7cdDdAa66E6DD71712B9c

TransferSig

0x48664c16

To

0xD0A8800973cbEF2639EbF79c019c8a1611C7

Value

100

Fee

0

Nonce

27

Signature

0x52e28f12c2431b8dceceb1f6a47820ef2b7c77b0d07c2303f594c65d83a35656f76933c64c407

Create Signature

確認初始化

圖 4-25 智能合約初始化

於「智能合約初始化」可將先前部署之智能合約進行初始化，於此頁面可以自訂被投資之相關資訊，如：合約代號、最小與最大投資金額、前置與後置手續費等，而策略雜湊值將先前的程式上傳之雜湊值自動填入(不可修改)，設定完成後點選「確認初始化」即可將此投資策略顯示於「策略程式總表」供投資人選取投資。

## (六)暫停 & 繼續智能合約

程式交易專區(Program Trading)

程式合約總覽

程式上傳

程式檢視

智能合約部署

智能合約初始化

暫停智能合約

繼續智能合約

終止(刪除)智能合約

合約資料

您的錢包地址

0x36C906644FEbA4052EEE2302fd361C79CDDa09af

剩餘代幣數量

5400 Tokens

您的程式合約地址

0xacb6ee45abcbe7edbbe9167f7fc52132aec4c634

暫停合約手續費

0 Tokens

暫停智能合約(inActive)

警告

此舉動將暫停智能合約，需先等待投資者結束所有投資

簽章資訊

Token Address

0x72682d0d54c7ED7cdDdAa66E6DD7171f2B9c626C

TransferSig

0x48664c16

To

0xD0A8800973cbEF2639EbF79c019c8a1611C7d810

Value

0

Fee

0

Nonce

28

Control\_id

1

Signature

0x68bcdaf2a6ef608b05f38249f55ba1e5b06ad8c384a8a1b940f652a4a70ba349377de3c1138a6b000c21d90f

① Create Signature

② 確認暫停

圖 4-26 暫停智能合約

程式交易專區(Program Trading)

程式合約總覽

程式上傳

程式檢視

智能合約部署

智能合約初始化

暫停智能合約

繼續智能合約

終止(刪除)智能合約

合約資料

您的錢包地址

0x36C906644FEbA4052EEE2302fd361C79CDDa09af

剩餘代幣數量

5400 Tokens

您的程式合約地址

0xacb6ee45abcbe7edbbe916777fc52132aec4c634

繼續合約手續費

0 Tokens

繼續智能合約(inActive)

警告

此舉動將繼續智能合約，請確認智能合約目前狀態是否為暫停

簽章資訊

Token Address

0x72682d0d54c7ED7cdDdAa66E6DD7171f2B9c626C

TransferSig

0x48664c16

To

0xD0A8800973cbEF2639EbF79c019c8a1611C7d810

Value

0

Fee

0

Nonce

29

Control\_Id

2

Signature

0x8895bdc01f8f58a03e145b93d396122853055e16b8c57b5d6f00db1eec7e1c131f7891523e89ebc6edae0d7

① Create Signature

② 確認繼續

圖 4-27 繼續智能合約

策略程式建置完成後，策略程式設計者可以將自己之策略暫停或繼續供人投資，但必須確認此策略程式尚未有人正在投資中。

## (七)終止(刪除)智能合約

程式交易專區(Program Trading)

程式合約總覽

程式上傳

程式檢視

智能合約部署

智能合約初始化

暫停智能合約

繼續智能合約

終止(刪除)智能合約

合約資料

您的錢包地址

0x36C906644FEbA4052EEE2302fd361C79CDDa09af

剩餘代幣數量

5400 Tokens

您的程式合約地址

0xacb6ee45abcbe7edbbe9167f7fc52132aec4c634

刪除合約手續費

100 Tokens

刪除智能合約(Delete)

警告

此舉動將刪除智能合約，需先等待投資者結束所有投資

簽章資訊

Token Address

0x72682d0d54c7ED7cdDdAa66E6DD7171f2B9c626C

Transfer Sig

0x48664c16

To

0xD0A8800973cbEF2639EbF79c019c8a1611C7d810

Value

100

Fee

0

Nonce

29

Signature

0x899ff0d1111532459bcbf8703a8042818249de09740e2294c21252401302fb449c7fae0753c23e085e60c12

① Create Signature

② 確認刪除

按下 #確認刪除 並不會真正刪除合約,將會通知管理人員,經審核通過後自動刪除並通知

圖 4-28 終止(刪除)智能合約

倘若策略程式設計者覺得自己所研發之策略狀況與績效不佳，可於此頁面提出策略合約刪除要求，待平台管理人確認後即可完成刪除。

## 七、瀏覽策略程式(策略程式專區)

### (一)策略程式總表

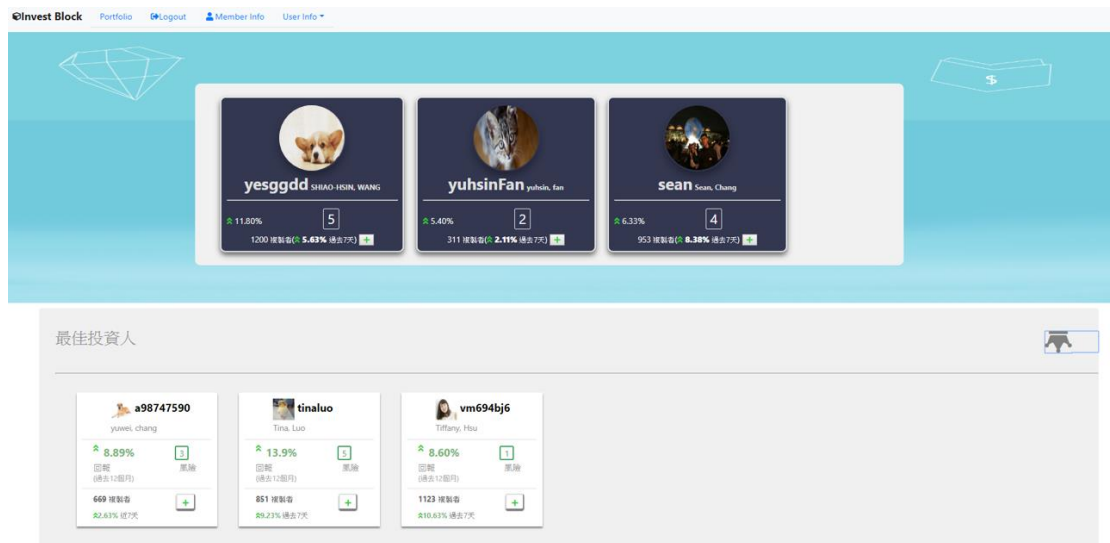


圖 4-29 策略程式總表

投資人可於「瀏覽策略程式」瀏覽所有策略設計者之程式狀態，包括其程式之投資報酬率、風險指數、被投資次數等，點擊被投資人專屬區塊，可轉跳至其程式之詳細資訊。

### (二)策略程式詳細資訊

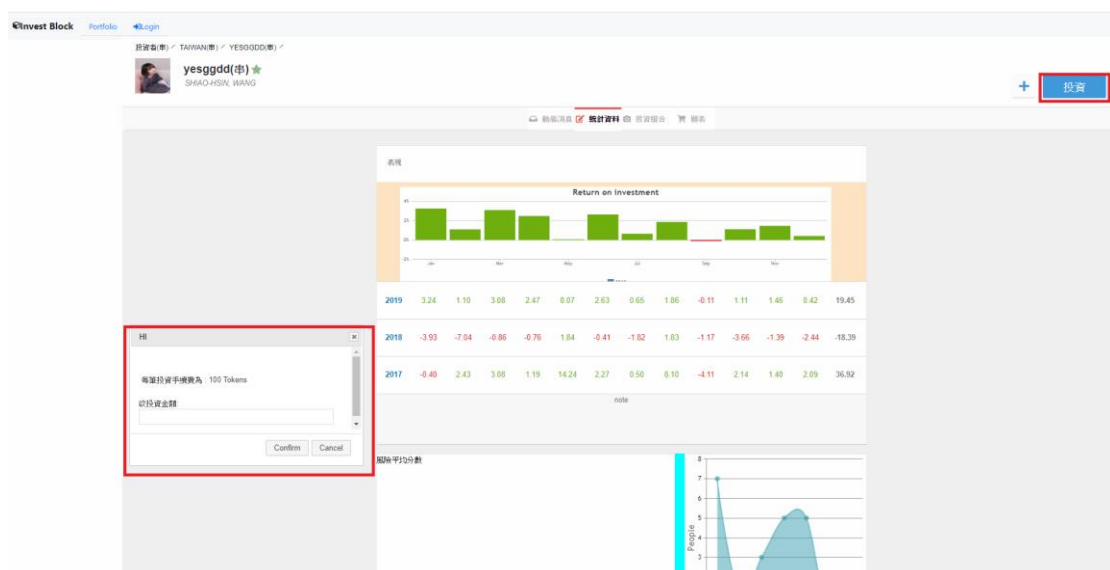


圖 4-30 策略程式詳細資訊

投資人點選特定之被投資人專屬區塊後，即可查看此策略之詳細財報資訊與近期走勢，若投資人決定要投資此策略時，可點選「投資」並輸入欲投資之金額(平台發行之加密貨幣)，平台將自動監聽策略程式之輸出策略，並使用投資者之入金金額進行投資，隨後通知券商依照輸出結果進行金融商品之操作，即可完成此次投資入金。

## 八、投資專區(投資者)

### (一)投資總覽

投資者專區(Investor)																							
投資總覽	錢包資訊																						
終止投資(全數賣出)	<table> <tr> <td>您的錢包地址</td><td>0x36C906644FEbA4052EEE2302fd361C79CDDa09af</td></tr> <tr> <td>剩餘代幣數量</td><td>6080 Tokens</td></tr> </table>	您的錢包地址	0x36C906644FEbA4052EEE2302fd361C79CDDa09af	剩餘代幣數量	6080 Tokens																		
您的錢包地址	0x36C906644FEbA4052EEE2302fd361C79CDDa09af																						
剩餘代幣數量	6080 Tokens																						
	<table> <tr> <th colspan="2">您投資的策略程式資訊</th></tr> <tr> <td>策略程式設計者</td><td>WANG2, GG, (yesgdd3)</td></tr> <tr> <td>策略程式地址</td><td>0xcfa5b5259b2cc789f9130777d930baf48691d47</td></tr> <tr> <td>策略程式代號</td><td>test</td></tr> <tr> <td>Active</td><td>true</td></tr> <tr> <td>Hash Strategy</td><td>0xd3310faa936ec686cb3199954ff8ada4e6a19331c84245af2f37c0c6b3b9ae1</td></tr> <tr> <td>Min Amount</td><td>100</td></tr> <tr> <td>Max Amount</td><td>999999999999</td></tr> <tr> <td>Front Variable Fee</td><td>10 % x 投資金額</td></tr> <tr> <td>Front Fixed Fee</td><td>100</td></tr> <tr> <td>Back Fee</td><td>10 % x 投資報酬率</td></tr> </table>	您投資的策略程式資訊		策略程式設計者	WANG2, GG, (yesgdd3)	策略程式地址	0xcfa5b5259b2cc789f9130777d930baf48691d47	策略程式代號	test	Active	true	Hash Strategy	0xd3310faa936ec686cb3199954ff8ada4e6a19331c84245af2f37c0c6b3b9ae1	Min Amount	100	Max Amount	999999999999	Front Variable Fee	10 % x 投資金額	Front Fixed Fee	100	Back Fee	10 % x 投資報酬率
您投資的策略程式資訊																							
策略程式設計者	WANG2, GG, (yesgdd3)																						
策略程式地址	0xcfa5b5259b2cc789f9130777d930baf48691d47																						
策略程式代號	test																						
Active	true																						
Hash Strategy	0xd3310faa936ec686cb3199954ff8ada4e6a19331c84245af2f37c0c6b3b9ae1																						
Min Amount	100																						
Max Amount	999999999999																						
Front Variable Fee	10 % x 投資金額																						
Front Fixed Fee	100																						
Back Fee	10 % x 投資報酬率																						
	<table> <tr> <th colspan="2">投資資訊</th></tr> <tr> <td>投資開始時間</td><td>2019/12/17 12:0:58</td></tr> <tr> <td>注入資金</td><td>200</td></tr> <tr> <td>結束時間</td><td>null (not end)</td></tr> </table>	投資資訊		投資開始時間	2019/12/17 12:0:58	注入資金	200	結束時間	null (not end)														
投資資訊																							
投資開始時間	2019/12/17 12:0:58																						
注入資金	200																						
結束時間	null (not end)																						

圖 4-31 投資總覽

若使用者為投資者，可至投資者專區檢視投資狀態與相關操作，投資者專區共有二項功能：投資總覽、終止投資。投資者一旦投資完成後，即可至投資總覽頁面查看目前正在投資之策略即時狀況。

## (二)終止投資(全數賣出)

投資者專區(Investor)

投資總覽

終止投資(全數賣出)

部署資料

您的錢包地址 0x36C906644FEbA4052EEE2302fd361C79CDa09af

剩餘代幣數量 6080 Tokens

部署合約手續費 500 Tokens

簽章資訊

Token Address 0x72682d0d54c7ED7cdDdAa66E6DD7171f2B9c626C

TransferSig 0x48664c16

To 0xD0A8800973cbEF2639EbF79c019c8a1611C7d810

Value 0

Fee 0

Nonce 22

Control\_Id 4

Signature

① Create Signature ② 確認部署

圖 4-32 終止投資(全數賣出)

投資者可以於「終止投資」頁面隨時終止投資，申請成功後平台將會通知券商把此策略所購買之投資商品全數賣出，並將相對應數量之加密貨幣自動轉帳至投資者之電子錢包，完成並結束此次投資。



## 第五章 結論與建議

### 第一節 研究結論

- 主要問題

此平台主要以區塊鏈為基礎建設之開發技術實作投資平台，並解決了傳統式資料庫之弊病，相較於E投睿投資平台，本平台之整體數據更具有公正與真實性，藉此使用者也能更信任本平台。

1. 投資數據準確透明：基於區塊鏈技術之特點，所有鏈上智能合約之投資資訊、結果、報酬率等投資相關數據皆公開透明且無法修改，公信力非常高。
2. 投資策略保證不被修改：當策略設計人上傳程式後，系統自動將程式雜湊並寫入智能合約中，但凡策略有任意修改，即可偵測其雜湊值必定與智能合約所存之雜湊值不相符，藉此保障投資人之權益。

- 附加價值

除了上述主要解決之問題外，還增添許多特色以提升附加價值，能使得本更能吸引使用客群且具擴充彈性。

1. 會員免兌換以太幣：使用以區塊鏈打造之系統通常都必須事先自行匯兌以太幣，才能操作分散式應用程式，而使用此平台只需兌換平台發行之加密貨幣，可以免於以太幣價格之浮動影響，平台也能定期舉辦匯兌活動，增加使用流量。
2. 銀行信託帳戶：本平台連結銀行實體現金帳戶，因此以真實貨幣兌換加密貨幣時，金流將不經過平台而是直接轉入第三方銀行之信託帳戶，交由銀行代為保管，藉此避免平台惡性關閉與吸金，提升使用者信賴，進而對平台更安心。
3. 客製化顧問費：策略程式設計者在上傳程式後之合約初始化階段，可自訂

策略之投資規則，包括：策略代號、最小入金金額、最大入金金額、前置固定手續費、前置與後置浮動手續費，這些數值也會影響投資人之判斷依據，可依照策略達到最大效益化。

4. 平台可發行 ICO、STO 回饋收益：由於平台有發行客製化加密貨幣，因此能藉由 ICO(initial coin offering)、STO(security token offering)群眾籌資，也能定期舉辦匯兌活動，增加加密貨幣兌換率與平台投資量。

## 第二節 未來展望

目前此平台對於區塊鏈技術之導入已完全開發完畢，運作流程也無瑕疵，不過往後待平台正式上線前，有些許問題點可以進行建置、探討與改善，來讓平台更完美。

1. 券商：目前網路上沒有公開的證券電子下單與回報之 API，因此還在找尋欲與平台合作之券商，一旦取得證券電子下單之測試環境即可透過策略程式之輸出進行下單，並將投資回報寫入智能合約中，待正式上線後再轉為正式下單環境，即建置完畢。
2. 附加功能與價值：平台目前僅提供證券之投資商品，往後將開放期貨、選擇權等投資商品，提供客戶更全面之功能。區塊鏈智能合約編譯方面也能進行擴充，使平台呈現更多元之數據，增加使用者分析指標。
3. 平台伺服器負載量：區塊鏈目前最大的缺陷為交易驗證上鏈時間過長，往往一筆交易都需要數秒來進行驗證並寫入智能合約，倘若平台隨著會員數量擴大而增加交易量，可能會導致伺服器負載過大，網頁異常，因此除了硬體設備之增強外，區塊鏈架構可以使用支鏈技術提高處理速度與負載量，或是將以太坊更換成超級帳本技術(Hyperledger)，大幅提高驗證效率。
4. 平台介面設計：平台目前之介面皆只用來呈現結果，部分排版與美觀層面

上可以再做進一步改進。

### 第三節 研究貢獻與結語

以現今區塊鏈的發展來看，技術架構已經算是非常完備，但是在應用層面上卻相對的落後，以區塊鏈為基礎架構之系統屈指可數，其最大原因為寫入速度過慢，導致無法處理短時間高負荷之即時資料，對於有資訊量有一定規模的產業幾乎不可能取代集中式資料庫，這也是目前區塊鏈最大的困境。

區塊鏈基礎的功能為記帳與記錄，因此對於金融科技之產業是有著一定的影響力，不過大部分皆伴隨著極大量的資訊流，導致區塊鏈遲遲進不了場，不過也是這個原因使得本平台以投資作為主要功能，即時資料量相較於其他金融操作是非常少的，再加上藉由區塊鏈特性之資訊公正與透明性，加值了投資理財的領域。

本平台之實作主要解決了一般使用集中式資料庫平台之缺點，如：資料流不透明、資料竄改等問題，再加上投資理財領域非常的強調數據之正確與公正性，因此區塊鏈技術的導入變得很有價值。目前較少有網路投資平台或是投資相關論文以區塊鏈為基礎核心之技術開發與實作，且大多數之投資平台也無任何方法實證其平台數據或是投資策略之公正性，因此本平台之設計能為區塊鏈之應用與投資領域貢獻實例，也期待此平台往後真實上線與發展。

## 第六章 參考文獻

### 第一節 英文文獻

- Cynthia Dwork, & Moni Naor. (1993). Pricing via Processing, Or, Combatting Junk Mail, *Advances in Cryptology. CRYPTO '92*, 139–147.
- Garvin Wood. (2014). *Ethereum: a secure decentralised generalised transaction ledger*. <https://gavwood.com/paper.pdf>
- Jakobsson, M., & Juels, A. (1999). *Proofs of Work and Bread Pudding Protocols(Extended Abstract)*.
- Johnston, D., Yilmaz, S. O., Kandah, J., Hashemi, F., Gross, R., & Wilkinson, S. (2015). *The General Theory of Decentralized Applications*. <https://github.com/DavidJohnstonCEO/DecentralizedApplications>
- Nick Szabo. (1994). *Smart Contracts*. <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- Nick Szabo. (1995). *Smart Contracts Glossary*. [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_glossary.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_glossary.html)
- Nick Szabo. (1996). Smart Contracts: Building Blocks for Digital Markets. *Extropy Journal of Transhuman Thought*. [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html)
- Nick Szabo. (1997). *The Idea of Smart Contracts*. <https://nakamotoinstitute.org/the-idea-of-smart-contracts/>

Parker, L. M. (1989). Medieval traders as international change agents: A comparison with twentieth century international accounting firms. *Accounting Historians Journal*, 16(2).

Satoshi Nakamoto. (2008). *Bitcoin: a peer-to-peer electronic cash system*.

<https://bitcoin.org/bitcoin.pdf>

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. In *Brilliance*.

Vitalik Buterin. (2014). *Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform*.

[https://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf)

## 第二節 中文文獻

- 姜林杰祐. (2009). *程式交易：觀念、方法、技術與解決方案*. 新陸書局.
- 廖子純. (2017). *利用智能合約實現單車共享經濟之研究*. 國立中興大學資訊管理學系碩士論文.
- 張碧瑜. (2015). *演算法交易行為對外匯市場質量之影響*. 國立中央大學財務金融學系碩士論文.
- 林佳賢. (2018). 不懂技術沒關係！圖解告訴你區塊鏈可以這樣用. *天下雜誌*，651.
- 莊尚威. (2019). AI對AI交易機器人 對戰趨勢成形. *理財周刊*，第983期, 74-79.
- 董寶蘭. (2010). *程式交易策略實證研究-以投資 ETF0050 為例*. 淡江大學管理科學研究所企業經營碩士在職專班碩士論文.
- 蔣潤祥、魏長江. (2016). 區塊鏈的應用進展與價值討論. *金融視界*，22, 19-21.
- 車世偉. (2018). *以智能合約實現網路購物退貨問題之研究*. 私立實踐大學資訊科技與管理學系碩士班碩士論文.
- 陳恭. (2017). 智能合約的發展與應用. *財經資訊季刊* 第90號.