國立臺灣大學管理學院資訊管理研究所

碩士論文

Department of Information Management

College of Management

National Taiwan University

Master Thesis

運用區塊鏈技術於點數交換平台

Bonus Points Exchange Platform Based on Blockchain Technology

黃珮瑜

Pei-Yu Huang

指導教授：曹承礎　博士

共同指導教授：蔡益坤 博士

Advisor：Seng-Cho T. Chou, Ph.D.

Co-Advisor：Yih-Kuen Tsay, Ph.D.

中華民國 107 年 7 月

July,2018

doi:10.6342/NTU201801612

誌謝

能順利完成這篇論文，特別感謝我的指導教授曹承礎老師，引領我進行研究，這兩年來學到許多新的觀點與技術，也要感謝口試委員蔡益坤教授與周子元教授在論文上的建議與指教，讓我的論文能更加完善。

兩年的研究所生活，感謝系上老師們的教導，也要感謝實驗室的每一位夥伴與學弟妹，謝謝大家曾經在各方面的協助。

感謝我親愛的家人，給予我最大的支持與自由，讓我隨心所欲，做我最堅強的後盾。感謝親愛的昀朋，總是不厭其煩地聽我訴說遇到的困難，努力和我一起想解決辦法，用最大耐心與愛心包容我的脾氣與緊張，感謝你陪我度過每個重要時刻。

以此論文獻給我的父親，願我永遠是您的驕傲。

黃珮瑜 謹致

中華民國一〇七年七月

doi:10.6342/NTU201801612

摘要

在國內消費市場中，會員積點活動是常見的行銷工具之一，從航空公司、銀行到超商，甚至是網路商城，生活中有各式各樣消費集點活動，企業給予消費顧客紅利點數，用來獎勵老顧客回購，培養忠誠顧客。但也因此出現複雜的集點制度和兌換選項，會員集點活動多為單一企業發行點數，並限制在該企業之營運據點使用，各業者均有自己的兌換機制，且合作企業之間的點數交換流程也十分繁雜，使得消費者持有的點數種類繁多，卻不見得可以累積至兌換門檻，對於企業維持消費者忠誠度沒有明顯效果。

本研究建立一個以區塊鏈技術為基礎的點數兌換平台，利用區塊鏈去中心化、可永久記錄且不易竄改等特性，消除現有點數兌換模式的限制，藉此擴大點數兌換的生態圈，透過區塊鏈技術改變企業現有會員點數的經營模式，進而達成企業轉型並創造利益。

關鍵字：區塊鏈、點換交換平台

doi:10.6342/NTU201801612

Abstract

In the domestic consumer market, loyalty program is one of the most popular marketing strategies. From airlines, banks, convenience stores to online shopping malls, points collection systems are almost everywhere in our daily lives. Companies give away bonus points to reward repeat customers and foster customer loyalty. However, the diversity of the points also leads to the complexity of the exchange platforms.

Most of the time, the points can only be used in the franchise stores of the points issued company. Even though there are some opportunities for points exchange between partner companies, the process can still be complicated. Under the circumstances, customers might hold various kinds of points from companies. The total amount of the points could be big, but none of them can reach the gift exchange threshold while breaking down to each kind. End up not making any obvious effect on the maintenance of consumer loyalty.

This study establishes a points exchange platform based on blockchain technology. Taking the blockchain's advantages of decentralized, permanently recordable, and hard to tamper with, it would be possible to eliminate the restrictions on the existing points exchange system and thereby expanding the availability of points exchange. Using blockchain technology to change the business model of the companies' existing loyalty program, then achieve the goal of enterprise transformation to create benefits.

Keywords : Blockchain、Bonus Points Exchange Platform

doi:10.6342/NTU201801612

目錄

doi:10.6342/NTU201801612

圖目錄

doi:10.6342/NTU201801612

表目錄

doi:10.6342/NTU201801612

第一章 緒論

1.1 研究背景與動機

吸引新顧客與維繫舊顧客是企業產品行銷最主要的目的，隨著網路發展與科技不斷創新，消費行為也快速改變，企業成功吸引到會員後，能不能留住顧客是一個更大的挑戰。因此，從航空公司、銀行到超商，甚至是網路商城，生活中有各式各樣消費集點活動，也就是顧客忠誠計畫（Loyalty Program），企業給予消費顧客紅利點數，用來獎勵老顧客回購，培養忠誠顧客。根據哈佛商業評論，獲取一個新客戶的成本要比把東西賣給現有客戶高，且現有客戶進行消費金額比新客戶高，簡而言之，企業實行客戶忠誠計畫是非常值得投資的行銷策略。

根據美國經營顧客忠誠度的公司 Loylogic 調查，點數的兌換率高低，與顧客忠誠、消費者黏著度高度相關，常拿點數兌換的消費者比從不兌換的消費者消費更多，這對點數發行者來說是一個正向循環，只要消費者多消費，發行點數的成本不但可被回收，行銷費用也會下降。

然而，根據 2015 年卡勒奎公司忠誠度調查報告（Colloquy Loyalty Census），每個美國家庭平均參與 29 個不同的會員計畫，因此出現複雜的集點制度和兌換選項，而各個計畫合作伙伴之間的點數交換流程也十分繁雜。在台灣也有同樣的情形，會員集點活動多為單一企業發行點數，並限制在該企業之營運據點使用，各業者均有自己的兌換機制，使得消費者持有的點數種類繁多，卻不見得可以累積至兌換門檻，點數兌換的諸多限制如：兌換門檻、兌換地點或兌換期限等，對於企業維持消費者忠誠度沒有明顯效果。

企業了解到會員點數可應用場景的數量多寡，影響點數對消費者的吸引力，因此近年也推出異業合作兌點或是跨平台兌換點數等方案，例如：通訊軟體 LINE 所

doi:10.6342/NTU201801612

推出的 LINE Points 讓使用者自由選擇轉換成遠東集團的 HAPPY GO 點數、悠遊卡公司的 UUPON 點數或是統一超商的 OPENPOINT 點數之後，即可以將點數的使用場景推展到線下市場，更貼近消費者並提高點數使用率，並可能經由跨平台的點數兌換，帶來尚未觸及的新用戶。

然而，目前市場上的點數兌換平台，多為點數發行者各自經營，不同點數平台之間的系統非直接相連，因此對用戶來說，必須先透過原有點數的網頁或是手機 APP 甚至是實體機台如超商 ibon 將點數換成一組序號後，再將這組序號輸入到新點數的點數平台中進行歸戶，才能完成兌換，這樣的使用流程既繁瑣也相當不直覺，除此之外，不同平台可能還有不同的兌換比例與門檻限制，造成消費者透過平台兌換點數意願降低。

隨著消費習慣變遷，會員點數在線上、線下結合的新零售時代成為一個關鍵的行銷工具，企業如何簡化點數兌換流程，改善消費者使用經驗，提高使用點數意願，是一個值得探究的議題。而區塊鏈（Blockchain）是以密碼學與演算法為基礎，不依賴第三方、透過分散式節點進行網路數據的儲存、驗證、傳遞和交流的一種技術方案，因此本研究希望建立一個以區塊鏈技術為基礎的點數兌換平台，利用區塊鏈去中心化、資訊公開透明、可永久記錄且不易竄改等特性，消除現有點數兌換模式的限制，藉此擴大點數兌換的生態圈。

1.2 研究目的

本研究建立一個以區塊鏈技術為基礎的點數兌換平台，消費者可以在此平台上以會員點數向點數發行商兌換平台所發行的加密貨幣，可再用此加密貨幣進行捐款，以此作為消費者利用點數購買此平台所提供的商品或服務的可行性驗證。對於點數發行業者來說，區塊鏈上交易即清算，可以降低對帳成本與提高清算效率，此外，點數可以兌換成區塊鏈上的加密貨幣，增加點數的使用場域，提高點數對於

doi:10.6342/NTU201801612

消費者的吸引力，同時點數發行業者也可以扮演平台上的服務或商品提供者，消費者以加密貨幣進行交易，達到點數刺激再次消費的最初目的；對於消費者來說，透過此平台可以進行多種會員點數兌換，減少過去需要在不同平台上分別兌換的不便，也降低集點門檻並活化點數用途，使消費者手上所擁有的點數價值提升。本研究探討區塊鏈如何改變企業現有會員點數的經營模式，進而達成企業轉型並創造利益。

doi:10.6342/NTU201801612

第二章 文獻探討

此章節針對本研究相關的領域進行探討，首先以區塊鏈為開頭，介紹其運作原理及特性；接著介紹本研究所使用的核心技術—以太坊架構與智能合約；再介紹加密貨幣與錢包分類；最後介紹紅利積點相關文獻及市場現況。

2.1 區塊鏈

區塊鏈技術由密碼學、數學、演算法及經濟模型所組成，結合分散式點對點的網路關係，並採用共識演算法，解決傳統分散式資料庫的同步問題，使得機器之間的信任得以建立。區塊鏈起源於 Satoshi Nakamoto 在 2008 年發表的論文「Bitcoin：A Peer-to-Peer Electronic Cash System」，其核心為記錄和儲存交易記錄的分佈式系統。根據中國區塊鏈技術和應用發展白皮書，狹義來講，區塊鏈是一種按照時間順序將資料區塊以順序相連的方式組合成的一種鏈式資料結構，並以密碼學方式保證其為不可篡改和不可偽造的分散式賬本。廣義來講，區塊鏈是利用塊鏈式資料結構來驗證與存儲資料、利用分散式節點與共識演算法來生成和更新資料、利用密碼學的方式保證數據傳輸和訪問的安全、利用智慧合約來執行程式設計和運算的一種全新分散式架構網路。

2.1.1 區塊鏈運作原理

以比特幣的區塊鏈來說，一個區塊 (Block) 的組成包含了區塊頭 (Block header) 、 雜湊值 (Hash) 、 交易 (Transactions)。區塊頭中包含了時間戳 (Timestamp)、困難值(Difficulty)、Merkle Tree Root、隨機值(Nonce)；時間戳是當前區塊生成的時間戳；困難值是為了讓雜湊值不會被輕易破解而存在的，每 2016 個區塊會調整一次；Nonce 隨機數為當前區塊共識演算法進行的隨機數；Merkle Tree Root 紀錄當前區塊中所有的交易經由 Merkle Tree 演算法所算出的 Merkle 樹根節

doi:10.6342/NTU201801612

點的 Hash 值，是區塊中交易的重點訊息。

透過雜湊演算法(Hash Function)將交易資料加密完整的傳送到下一個節點是區塊鏈的一個核心工作，當交易產生時配合著公鑰與私鑰來進行資料的安全簽章核准，接著透過雜湊加密且記錄在區塊中，提升了資料在區塊中遭到篡改的難度，透過這套聯合機制解決交易中的信任問題。其中，區塊鏈帳本不是存放在一個中央機構或是一個資料庫，它擁有著無數份的複本，存放在區塊鏈網絡上的每一台電腦裡，而每台電腦稱為節點（node）。當某一個節點發起交易時，先將此交易廣播給其他節點，再由所有節點經由共識演算法來驗證這筆交易，最先解題完成的礦工會將交易訊息包成一個新的區塊放上區塊鏈，此時交易就算完成。

舉例來說，如果 A 想要轉帳數位貨幣給 B，A 就會發送一個訊息告訴所有網絡說：A 從帳戶中轉錢給 B 的帳戶。在網絡中的每個節點都會收到這個訊息，當其中一個節點先解出共識演算法的隨機值時，其他節點便幫忙驗證此交易是否是有效的，若為有效，便由該節點將驗證過的交易寫進區塊鏈中，並廣播通知其他節點，所有節點便會將這筆交易記錄到自己的帳本裡(Michele D'Aliessi，2016)，如圖 1 所示。

doi:10.6342/NTU201801612

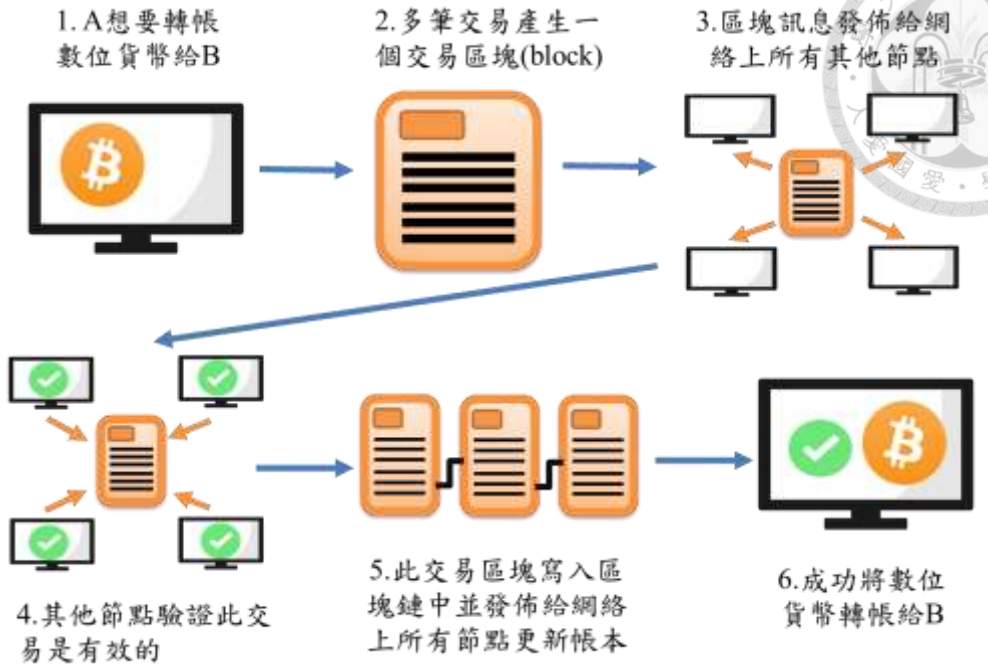

圖 1 區塊鏈運作示意圖

2.1.2 區塊鏈特性

區塊鏈共有三個特點，分別為密碼學機制、分散式帳本、共識演算法。

(1) 密碼學機制（Cryptography）：

在比特幣區塊鏈理論中，每當交易產生時，都須要原本的擁有者進行數位簽章核准這筆交易，交易資料會被打包至區塊中，並透過雜湊演算法進行記錄。雜湊演算法能夠將任意長度的資訊壓縮為固定長度的輸出值，這個固定長度的輸出值通常是一個隨機數，雜湊算法被反復應用到區塊鏈技術中，如：共識演算法、Merkle Tree 以及區塊地址的生成等（李晶，2017），雜湊演算法則提升了交易的偽造難度，也奠定了區塊鏈的安全基礎。

(2) 分散式帳本（Distributed Ledgers）：

分散式帳本是指將數位記錄依照時間順序記載在數據庫，通過參與者同意的規則或是獲得一定數量的贊成票（共識演算法）之後，被記錄並加密保存在帳本上，

doi:10.6342/NTU201801612

區塊鏈將所有的交易紀錄存放在多個節點，所有參與者都能得到一個副本（羅鈺珊，2017），去中心化的資料留存方式讓參與者得以隨時追溯交易歷史，提升資訊透明度，降低偽造的風險。因此在區塊鏈的環境下，交易一旦驗證確認完成後，數據篡改的難度和代價將會相對龐大，資料更動的權限也不受單一組織控制，提升交易資料的可信任度（楊英伸，2016）。

(3) 共識演算法（Consensus Algorithm）：

在分散式帳本的去中心化環境下，區塊鏈讓每個擁有交易紀錄的節點，以多數決的方式取得資料正確性的共識。目前比特幣與以太坊區塊鏈的共識演算法皆是算力證明演算法（Proof-of-work；POW），也稱工作量證明，其原理是由各節點以算力解題的方式來競爭當前區塊的寫入權，最快解得答案者將答案與他自己選擇好的交易內容，也就是當前區塊內容發布給其它節點驗證，若其它節點驗證區塊內容正確且同意他是最早解題者，則加入此鏈並將此區塊內容儲存起來，並以此區塊內容作為依據開始解下個題目。POW 是目前為最安全的公有鏈共識機制且此機制較簡單容易實行，也是相對公平的挖礦機制對於加密貨幣的產生與分配。但 POW 的缺點為需要消耗大量能源，因為算力是以能源消耗為代價製造出來的。

綜合上述，本研究歸納區塊鏈技術主要具有去中心化、去信任化、可靠性、匿名性等特性。

(1) 去中心化（Decentralized）

整個區塊鏈網絡中不依靠額外的第三方管理機構或硬體設施，沒有中央管理單，任一節點都是平等的，且任一節點損壞或者失去，並不會影響整個系統的運作，因此對單個節點的攻擊無法控制或者對整個區塊鏈網路產生影響。

(2) 去信任化（Trustless）

doi:10.6342/NTU201801612

整個系統的運作規則都是公開透明的，每一個節點都持有帳本，且任何人無法擅自變更規則或篡改資料。若因個人修改資料無法達成共識時，則會遭到網絡的否決（賴怡伶、莊鯉銓，2016）。因為區塊鏈中每個節點都能夠獲得區塊鏈中的所有資料，消除了資訊不對稱造成的風險，這也提高了用戶對網絡中資訊的信任程度。

(3) 可靠性（Reliability）

在區塊鏈中所有機制都是集體參與，互相達成共識的，沒有任何人可以隨意更改帳目資訊或者是改變系統既定的規則，因為任何違規的操作都不會被系統所承認的，除非改變整個網絡中一半以上的人手中的記帳系統，而這幾乎是不可能做到的，因此參與系統中的節點越多，該系統中的數據安全性就越高。

(4) 匿名性（Anonymity）

由於區塊鏈解決了節點和節點之間信任的問題，因此在區塊鏈網路中可以在無需了解對方身份的情況下進行交易，交易雙方僅需要公佈自己的地址就可以與對方進行交易，因此在系統中的每個參與節點都是匿名的。

2.2 以太坊

以太坊是一個開源的區塊鏈平台，以太幣（ETH）是以太坊的數位貨幣，開發者們需要支付以太幣來進行區塊鏈應用。以太坊白皮書中提到，創始人 Vitalik Buterin 希望能讓區塊鏈技術應用在虛擬加密貨幣以外的領域，突破過去比特幣區塊鏈技術上的限制，以太坊希望實踐的是像 TCP/IP 協議這樣的標準，能以太坊區塊鏈協議內置程式語言，兼容各種區塊鏈的應用，讓開發者能夠在以太坊定義好的區塊鏈協議用程式語言，進行高效快速的開發應用。與比特幣區塊鏈相比，以太坊區塊鏈具有圖靈完備（Turing Complete）的特性，可以建構複雜的智慧合約（Smart Contract）、去中心化的自治組織 DAO（Decentralized Autonomous Organization）、

doi:10.6342/NTU201801612

去中心化應用程式 Dapp （Decentralized Application）、或是其他的虛擬加密貨幣。由於以太坊是一個分散式的平台來處理智能合約，應用程式完全地按照編譯的程式去執行，保證交易的可信任性、去中心化的運作，提供一個沒有中間單位的且信任的交易市場。在以太坊的區塊鏈上，任何人都可以設置應用程式的節點，以分散式的方式儲存，在符合使用協定下也能夠容易地取得其他節點上應用程式的必要資訊，以太坊就像是一台全球性分散式的去中心化電腦，任何人都可以上傳與執行應用程式。

2.2.1 以太坊架構

下圖 2 為以太坊的技術架構，最下端網際網路與硬體端做配置，往上分為三個部分，SWARM 用以儲存資訊、WHISPER 用以資訊的傳遞與溝通、EVM 則提供了平台與共識機制的協定，第二層為分散式應用 (Decentralized Applications)，而最上層則是 MistBrowser，提供一個使用分散式應用的瀏覽器工具。

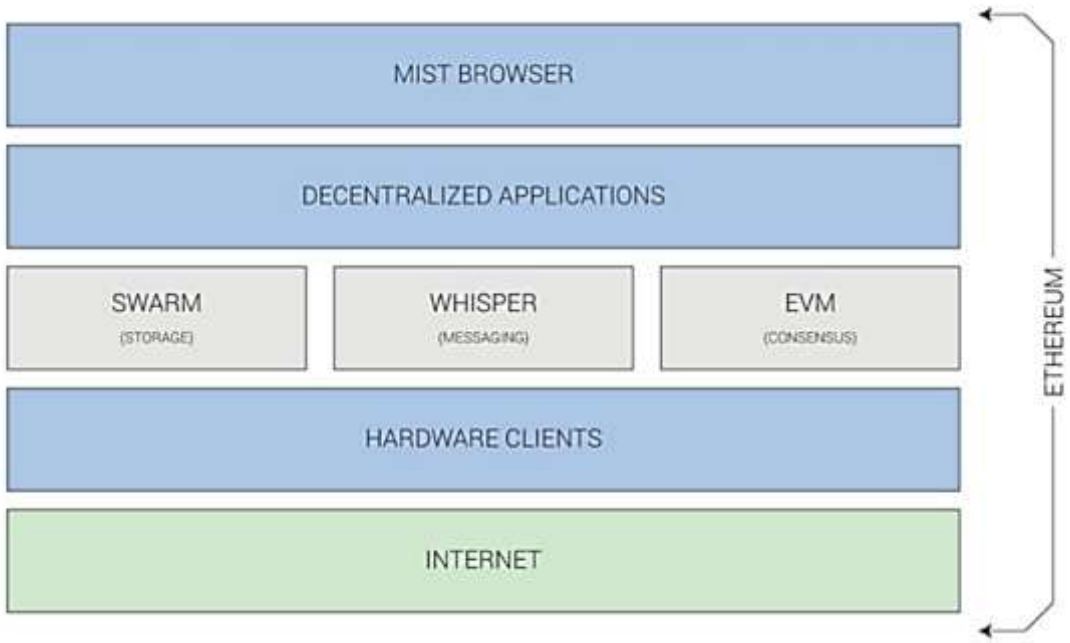

圖 2 以太坊架構圖
（來源：www.easyeth.com）

doi:10.6342/NTU201801612

2.2.2 智能合約

智能合約最早是由 Nick Szabo 於 1994 所提出的理念，希望透過一個平台能讓交易的雙方，透過通用的軟體工具，將彼此的交易條款與條件，表達成自動執行的程式碼，並稱這些程式碼為智能合約。透過智能合約將兩造之間的資產移轉，變成可程式化的，只要透過電腦程式的邏輯變化，就可以實現各種的交易條款與條件。這種想法深具應用潛力，但那時候技術還不夠成熟，也沒有適當的平台，所以智能合約就僅能停留在概念的層次（陳恭，2017）。

隨著比特幣的概念發行，發現比特幣的底層技術區塊鏈可以為智能合約提供一個可被信任的執行環境，雖然比特上也能寫智能合約，但是比特幣所支援的語法僅與交易有關，無法進行其他方面應用。因此以太坊致力發展可以讓智能合約執行的平台，以太坊的智能合約具備圖靈完備（Turing Completeness）的特性，也就是說它有能力執行條件跳轉語句，像是 for、if、while 等等，而且能夠執行任何其他程式語言能夠做的運算。

智能合約是以應用程式的邏輯，來實現交易合約中的條款與條件，程式碼本身記錄在區塊鏈上，因此具備區塊鏈的不易竄改和去中心化等特性；其次這個程式可以控制區塊鏈資產，比如它可以存儲和轉移加密貨幣，且程式由區塊鏈執行，也就是說按照預先編寫的內容執行，就不可能有人能干涉其運行。

2.3 加密貨幣與錢包

依據國際貨幣基金（IMF）的定義，數位貨幣泛指所有以數位形式表示價值之物，根據是否以法償貨幣計價分為兩類，不以法償貨幣計價之數位貨幣稱為虛擬貨幣；而虛擬貨幣又區分為可轉換為實體商品、服務或貨幣與不可轉換兩類；可轉換虛擬貨幣又可依是否有中央發行機構，即是否去中心化，區分為兩類；其中使用加密技術認證的去中心化可轉換虛擬貨幣，稱為加密貨幣（Cryptocurrency），例如比

doi:10.6342/NTU201801612

特幣、以太幣等（張凱君，2018）。

由於加密貨幣所採用的去中心化架構特性，用來儲存加密貨幣的錢包，實際上並非將貨幣放在錢包內，而是泛指能在區塊鏈上交易所使用的公鑰與私鑰、私鑰所對應的地址、該地址的貨幣結算，以及貨幣交易的支援系統。

2.3.1 加密貨幣

加密貨幣是使用非對稱式加密、橢圓曲線加密及數位簽章等密碼學演算法來確保交易安全與不可逆的交易媒介，並使用分散式帳本的區塊鏈技術達到去中心化的特性，比特幣在 2009 年成為第一個去中心化的加密貨幣，這之後加密貨幣一詞多指此類設計，與依賴中心化監管體系的銀行金融系統相對。全球的加密貨幣目前超過 1,500 種，根據加密貨幣追蹤網站 Coinmarketcap.com 資料，2018 年 5 月全球加密貨幣總市值約 3,260 億美元，其中比特幣市值約占總市值 35%，以太幣 20%，瑞波幣 8%，其餘加密貨幣市值占比都在 5%以下。

2.3.2 加密貨幣錢包分類

加密貨幣錢包提供錢包地址的創建、加密貨幣轉帳及交易歷史的查詢等功能，每個錢包地址都對應一組私鑰和公鑰：私鑰是一組概率空間為 2 的 256 次方的隨機數；公鑰是與私鑰相對應的，亦是由私鑰推算出來的；地址則是由公鑰轉換而來的。加密貨幣在不同帳戶間轉移的過程中使用私鑰來簽名交易，其他人使用公鑰來驗證簽名，驗證通過就代表交易完成。根據密碼學原理，私鑰能推算出公鑰，但公鑰不能反推出私鑰，因此，私鑰是唯一能夠證明對於數字資產有控制權的憑證。目前常見的私鑰形態還有 Keystore & Password 和 Mnemonic Seed，Keystore &Password 在以太坊官方錢包中，私鑰與公鑰將會利用創建錢包時設置的密碼進行加密，保存為一份 JSON 檔案，而這份 JSON 檔就是 Keystore，所以用戶需要同時備份 Keystore 和其對應的密碼；Mnemonic seed 由 BIP 39 提案（Bitcoin

doi:10.6342/NTU201801612

Improvement Proposals）提出，通過隨機生成 12 ~ 24 個單詞，單詞序列透過 PBKDF2 與 HMAC-SHA512 函數創建出隨機種子，種子再透過 BIP 32 提案的方式生成錢包，因此記住 12~24 個助記詞後，就相當於記住私鑰，而助記詞要比私鑰更方便記憶。

若根據區塊鏈數據維護方式可以分爲全節點錢包以及 SPV 錢包(Simplified Payment Verification，簡單支付驗證，又稱輕錢包)兩種，其中全節點錢包同步區塊鏈上所有的數據，用戶參與到網路的數據維護中，由於此種錢包能提供所對應的加密貨幣網路完整區塊鏈與服務，所以可以提升該加密貨幣網路的完整性與可靠性，因此某些加密貨幣，會對持有這種錢包的使用者進行獎勵，但同步所有區塊數據佔據很大的記憶體空間，所以手機端及網頁端等運行的輕錢包參考了中本聰提出的 SPV 機制，不儲存完整的區塊鏈數據，輕錢包也會下載新區塊的所有數據，但是它會對數據進行分析後，僅獲取並在本地儲存與自身相關的交易數據，運行時依賴於區塊鏈網路上其他全節點。

對於加密貨幣錢包來說，一個錢包是否安全主要看它能否安全的管理和使用私鑰。因此，本研究按照錢包使用環境及私鑰的儲存方式，將目前加密貨幣錢包分成：桌面錢包、網頁錢包、手機錢包、交易所錢包、紙錢包及硬體錢包等六種，以下一一介紹其特性與其相對應的主流以太坊錢包。

（1） 桌面錢包

桌面錢包軟體運行於桌面作業系統如 Windows、MacOS、Linux 等，私鑰保存於用戶機器中，其中以太坊官方錢包 Mist 和原以太坊基金會成員所開發的 Parity 皆為全節點錢包；Exodus 錢包則為第一個支援多幣種交換的桌面輕錢包。

（2） 網頁錢包

doi:10.6342/NTU201801612

網頁錢包只需瀏覽器打開網頁就能使用，不用下載任何軟體。而 MyEtherWallet 為最受歡迎的以太坊網頁錢包，因其為開源程式碼，大眾可檢視並確保程式碼沒有問題，而且沒有中央資料庫，所以不會儲存用戶錢包資料，在網站產生私鑰後，私鑰和密碼都由使用者本身持有，日後要在網站存取錢包時必須輸入私鑰。MetaMask 則為網頁插件錢包，讓使用者可以更容易跟以太坊的去中心化應用互動。

（3） 手機錢包

使用手機錢包只需下載 APP 就可以隨時隨地查看資產狀況。Jaxx 是目前支援最多幣種的手機錢包，Jaxx 也不會儲存錢包資料，所有錢包私鑰和密碼都由使用者本身持有。

（4） 交易所錢包

交易所錢包多為網頁錢包，各交易所為了能夠出入幣，也都會提供對應該幣的錢包地址，但此種錢包不會提供私鑰給使用者，所以一旦存入就只能依靠交易所的機制來提領，因為私鑰交由交易所保存，容易有駭客入侵或是交易所倒閉等風險，目前 Binance 為全球交易量最大的加密貨幣交易所。

（5） 紙錢包

儲存私鑰最簡單辦法就是記在一張紙上，這種形式的錢包被稱為紙錢包，為最簡單形式的加密貨幣錢包。可以透過開源軟體 ETHAddress 創建一個以太坊紙錢包。但紙錢包只能存儲加密貨幣，若要想用於支付, 還須創建另一種類型的錢包，並將資金從紙錢包轉移到新錢包。

（6） 硬體錢包

硬體錢包是將私鑰儲存在特製的硬體設備比如隨身碟形式，使用時交易需在

doi:10.6342/NTU201801612

硬體內部進行交易簽署才送出，因硬體錢包為離線裝置，駭客無法透過網路進行攻擊，只要硬體沒有被破解，即可保障私鑰安全性。Ledger Nano S 是以太坊硬體錢包，在進行初始設定時，會自動生成 24 個單詞，當設備遺失時可以購買新的硬體錢包，然後用這 24 個單詞還原數據。

綜合上述，硬體錢包最為安全，但使用上也較為不便；交易所錢包取得最方便，但風險也較高；而不論是桌面錢包、網頁錢包或是手機錢包，因為私鑰儲存裝置皆會連接網路，都有駭客入侵盜取私鑰的風險，因此建議可根據需求選擇不同錢包存放加密貨幣，例如把頻繁交易的加密貨幣放在交易所錢包中，預估會長期存放的加密貨幣放在硬體錢包，根據使用需求對應其安全性和便利性。

2.3.3 以太坊 ERC20 標準

依瑞士金融市場監理局(FINMA)發布之規範，指出目前區塊鏈上所發行的代幣（Tokens）大致可分資產型、效用型及支付型三種型態：

（1） 資產型代幣(Asset Tokens)：此代幣持有人對發行者之資產有請求權比如股權或債權。

（2） 效用型代幣(Utility Tokens)：此代幣持有人可將代幣使用在發行者提供之應用與服務。

（3） 支付型代幣(Payment Tokens)此代幣可作為廣泛被接受之支付工具，其對發行者無請求權。

代幣為區塊鏈最大宗的開發應用之一，為了要讓代幣能擁有合理的貨幣機制，以太坊制定了 ERC20（ Ethereum Request for Comments）數據通訊協議，是目前最多人使用的以太坊代幣主流規格標準。在這協議下，所有發行的代幣必須按照規範在其智能合約中表達其功能，若是一個代幣符合 ERC20 規範，即代表它是一種具

doi:10.6342/NTU201801612

有完整貨幣交易功能的代幣，能在支援的錢包內顯示餘額以及進行交易比如 MyEtherWallet、MetaMask 等。以下是標準的 ERC20 合約所需要具備的函式及功能如表 1。

函式名稱	功能
name()	代幣的全名
symbol()	代幣的縮寫
decimals()	代幣的最小單位
totalSupply()	代幣的總量
balanceOf()	查詢某帳戶的代幣餘額
transfer()	移轉代幣給他人
transferFrom()	從 A 移轉代幣給 B
approve()	批准自己的代幣移轉
allowance()	A 批准給 B 的代幣數量
event Approval()	代幣批准觸發事件
event Transfer()	移轉代幣觸發事件

表 1 ERC20 規範函式整理

2.4 紅利積點

Blattberg & Neslin（1990）將紅利積點（Continuity Program）活動定義為，消費者在一個既定的時間內，於一個特定的消費地點，消費達到一個設定的金額或次數，以得到業者所提供的回饋。紅利積點促銷最主要的功能便是顧客的維持，希望增加既有顧客的購買頻率，甚至在養成消費習慣後形成忠誠度，因此它的目標對象偏向於原有的客群。

doi:10.6342/NTU201801612

2.4.1 紅利積點特性

在國內消費市場中，紅利積點活動是常見的行銷工具之一，最常見的紅利積點活動包括航空業者推出的累計里程、信用卡的刷卡紅利、量販店業者之會員卡集點、網路商城的點數消費回饋、甚至近年來便利商店業者推出的集點活動等，皆是紅利積點的成功應用模式。

但並非所有紅利積點活動都能達到忠誠消費之目的，歸因於紅利積點活動總有諸多限制，使紅利積點對消費者的誘因下降。林詩晃(2003)在其研究中提到，影響紅利積點活動有下列幾點因素：

（1） 累計時間限制

提供紅利點數之企業要求消費者需在一定期間內累積紅利點數，若消費者無法在該期間內累積至足額點數兌換贈品，則該累積點數將視為失效。

（2） 累計積點難易

積點的計算方式與積點兌換標準門檻的限制，若兌換的點數門檻低，此紅利積點活動會較有吸引力。

（3） 累計積點型式

紅利積點活動有不同型態設計，比如累積消費金額或是累積消費次數等。

（4） 贈品兌換內容

紅利積點活動在兌換贈品內容上的不同。一般常見的兌換贈品包含：實際商品兌換、現金回饋方式、購物折抵、會員升等級等。

（5） 贈品兌換限制

doi:10.6342/NTU201801612

紅利積點活動在兌換贈品內容上的限制，常見的兌換限制有：商品兌換限制或兌換時間限制等。

（6） 網路結盟程度

與同業或異業結盟的程度，消費者到結盟商店消費可以獲取雙倍或更高的紅利點數，所以結盟程度越高或恰巧符合持卡者的需求，該紅利積點活動則越具吸引力。

2.4.2 紅利積點交換市場現況

國內主要的點數平台分別為擁有 1,900 萬會員的通訊軟體 Line 旗下的 LINE Points、累積 1,600 萬快樂購卡發卡量的 HAPPY GO 點數與 1,600 萬 icash 愛金卡發卡量的 OPENPOINT。目前三者彼此之間都可以互相兌換點數，但兌換平台各自經營，系統非直接相連，以 LINE Points 兌換 HAPPY GO 點數為例，如圖 3 用戶需先在 LINE APP 上扣除點數獲得一組序號，需要再登入 HAPPY GO 官網或是 APP 輸入序號進行歸戶方能完成兌換，對用戶來說，使用流程既繁瑣也相當不直覺，除此之外，不同平台可能還有不同的兌換比例與門檻限制。

圖 3 LINE Points 兌換 HAPPY GO 點數示意圖

（來源：http://official-blog.line.me）

doi:10.6342/NTU201801612

2.4.3 紅利積點進行捐款市場現況

台灣目前多家信用卡皆可使用紅利積點進行捐款，僅限於與銀行合作的慈善機構，且可能會有最低點數兌換門檻限制，例如國泰世華銀行兌換規則為 2000 點等同 120 元台幣。而 LINE Pay 愛心捐款共串聯 10 個社福機構，使用者可以使用 LINE Points 1 點等於 1 元台幣來支付捐款，但多以 100 元等小額金額為單位，且從 LINE Pay 系統中使用者只能查詢自己的捐款紀錄，無法看到該慈善機構共已收到多少捐款，有捐款資訊不對等與後續款項處理不透明等問題。

doi:10.6342/NTU201801612

第三章 系統架構與設計

本研究將先建立一網站模擬點數發行商使用以太幣購買平台所發行的加密貨幣，以供其顧客用點數兌換加密貨幣，而消費者可以在此網站上用兌換後的加密貨幣進行捐款，交易過程中調用智能合約的功能函式，所有交易均記錄在以太坊區塊鏈上。

3.1 系統架構

本研究使用 Testrpc 在本地端模擬一個以太坊區塊鏈測試環境，Testrpc 是基於 node.js 開發的模組，可以模擬一個以太坊客戶端的行為，並創建以太坊帳戶供開發者使用，發送給 Testrpc 的交易會被馬上處理而不需要等待挖礦時間，讓基於以太坊的開發測試工作更加方便快速。

透過 Testrpc 所建立之節點在 PORT 8545 提供了 RPC（Remote Procedure Call）通訊，設置允許連接之客戶端，皆可利用以太坊提供之 Web3.js API 與 RPC 連接，再透過節點的 RPC 接口與節點進行溝通。當佈署智能合約時，會先將以 Solidity 撰寫的智能合約程式碼編譯成 EVM byte code，再將 EVM byte code 透過 Testrpc 的 RPC 接口發送到以太坊網絡，經過每個節點的驗證後，寫至區塊鏈上。使用者透過網頁瀏覽器輸入資料，經由 JavaScript 的執行，呼叫智能合約的功能函式完成交易。本研究之系統架構如圖 4 所示。

doi:10.6342/NTU201801612

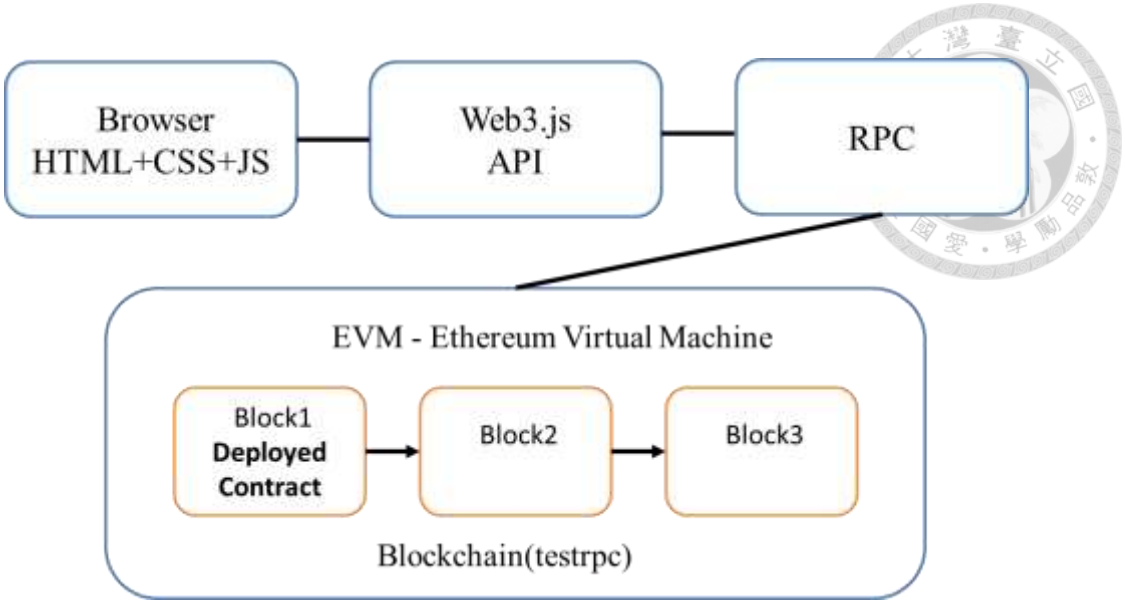

圖 4 系統架構圖

3.2 系統流程

本研究之點數兌換系統參與者分別有：加密貨幣管理者、點數發行商、顧客及募款機構，預設所有系統參與者皆有一組自己的以太坊帳戶地址，可以用來執行交易與傳送加密貨幣。加密貨幣管理者佈署智能合約並發行加密貨幣（貨幣縮寫為TT），智能合約中包含加密貨幣交易及點數兌換等規範；點數發行商可以使用以太幣購買平台所發行的加密貨幣，以供其顧客用點數來兌換加密貨幣；消費者可以扣除點數來兌換加密貨幣，並利用其加密貨幣進行捐款給募款單位。本研究系統流程如圖 5。

doi:10.6342/NTU201801612

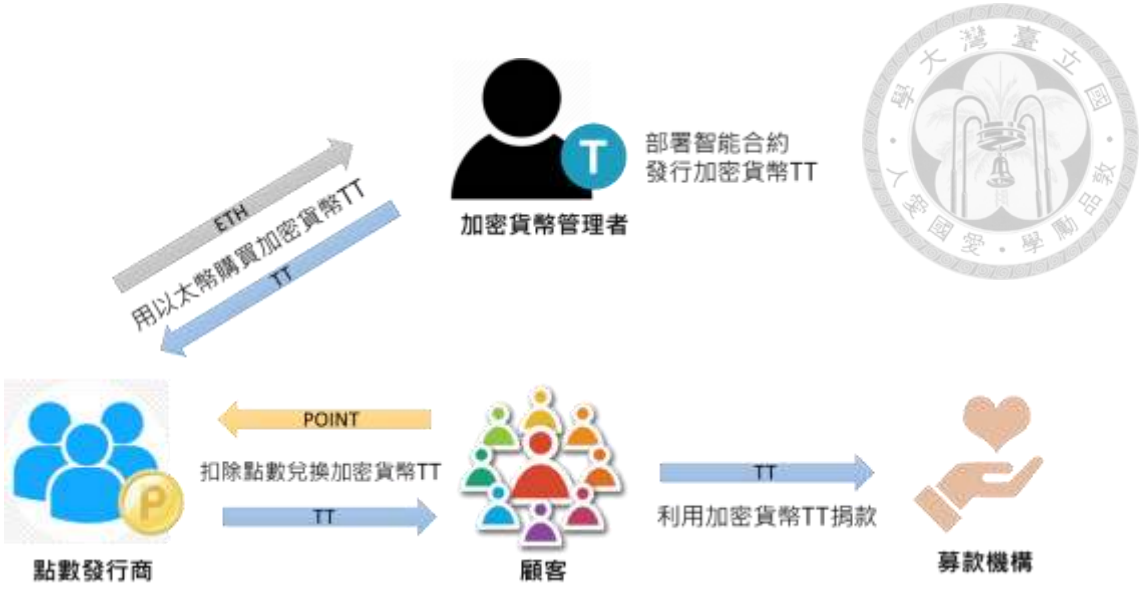

圖 5 系統流程示意圖

doi:10.6342/NTU201801612

第四章 實驗結果與分析

4.1 系統設計與開發

本研究建立一個以區塊鏈技術為基礎的點數兌換平台，以下為開發環境架設與智能合約內容說明。

4.1.1 開發環境

本研究於 VMware Workstation 12 Player 架設一台 Ubuntu 16.04 桌面版本 64 位元作業系統之虛擬機做為開發環境，安裝 Testrpc 模擬一個以太坊區塊鏈測試環境，利用 Truffle 開發框架來佈署和測試智能合約，並以以太坊官方開發的編程語言 Solidity 撰寫智慧合約，透過 Javascript 的 web3.js 套件和智能合約溝通，並使用網頁插件錢包 MetaMask 執行轉帳等交易。

4.1.2 智能合約說明

智能合約所建立的加密貨幣若要能通過以太坊錢包收發，必須支持 ERC20 標準，因此本研究使用 OpenZeppelin 函式庫來簡化建立加密代幣的過程，其為智能合約審查服務商 Zeppelin Solutions 維護的開源函式庫，讓程式開發者可以使用和擴展這些智能合約，以在更少的時間內創建更安全的去中心化應用程式。本研究引入其提供的 StandardToken.sol 智能合約來創建一個支持 ERC20 標準的加密貨幣，並聲明 TutorialToken 繼承自 StandardToken，這樣就可以繼承 StandardToken 合約中所有變數和函數，並設置加密貨幣的參數，需要定義全名（name）、縮寫（symbol）、最小單位（decimals）和發行總量（INITIAL_SUPPLY），程式碼如圖 6 所示。

doi:10.6342/NTU201801612

```
pragma solidity ^0.4.4;
import "../node_modules/zeppelin-
solidity/contracts/token/ERC20/StandardToken.sol";
contract TutorialToken is StandardToken {
string public name = 'TutorialToken';
string public symbol = 'TT';
uint public decimals = 2;
uint public INITIAL_SUPPLY = 10000000;
```

圖 6 加密貨幣參數設定程式碼

繼承 StandardToken 智能合約中函式名稱與功能如表 2。

函式名稱	功能簡述	輸入值	回傳值
totalSupply()	查詢加密貨幣的發行總量	-	uint256
balanceOf(A)	查詢 A 帳戶的加密貨幣餘額	address	uint256
transfer(A,x)	移轉 x 個加密貨幣給 A	address, uint256	bool
transferFrom(A,B,x)	從 A 帳戶移轉 x 個加密貨幣給 B 帳戶	address, address, uint256	bool
approve(A,x)	同意 A 從我的帳戶中提領 x 個加密貨幣	address, uint256	bool
allowance(A,B)	查詢 B 可以從 A 帳戶提領的加密貨幣數量	address, address	uint256

表 2 繼承 StandardToken 智能合約的函式整理

下圖 7 為宣告變數，用 struct 來定義一組變數的集合包含使用者帳戶地址與所擁有點數數值，mapping 為映射關係的儲存結構，而動態陣列宣告成 address、uint 與 bytes32 的類型，其中 address 代表以太坊的帳戶地址的資料型態，為 20 字元長度的值。

doi:10.6342/NTU201801612

```
struct  user{
    address userAddress;
    uint userPoints;
  }
    mapping (address => user) public userInfo;
    address[] public userList;
    uint[] public pointList;
    bytes32[] public planNamesList;
    address[] public planAddressList;
    uint public tokenRate;
    uint public exchangeRate;
```

圖 7 宣告變數程式碼

下圖 8 為函式 TutorialToken，和合約同名的 TutorialToken 函式，是這個合約的建構函式(constructor)。函式中將所有的初始代幣 INITIAL_SUPPLY 都指定給 msg.sender 帳號，msg 是一個全域(Global)物件，msg.sender 表示呼叫當前函式的帳戶，由於建構函式只有在合約部署時會被執行，因此這邊用到的 msg.sender，也就代表著用來部署這個合約的帳戶。此外，並將佈署合約後拿到的初始值存入變數中，包含顧客帳戶地址、顧客點數、募款計畫名稱、募款計畫帳戶地址、以太幣購買加密貨幣 TT 的匯率及顧客點數兌換加密貨幣 TT 的匯率。

```
function TutorialToken(address[] userAddress,uint[]
userPoints,bytes32[] planNames,address[] planAddress,uint
_tokenRate,uint _exchangeRate)public {
  totalSupply_ = INITIAL_SUPPLY;
  balances[msg.sender] = INITIAL_SUPPLY;

  userList = userAddress;
  pointList = userPoints;
  planNamesList = planNames;
  planAddressList = planAddress;
  tokenRate = _tokenRate;
  exchangeRate = _exchangeRate;
```


doi:10.6342/NTU201801612

```
  for (uint i = 0; i < userAddress.length; i++) {

      userInfo[userAddress[i]].userAddress = userAddress[i];
      userInfo[userAddress[i]].userPoints = userPoints[i];

    }
}
```

圖 8 函式 TutorialToken 程式碼

如表 3，智能合約內的函式分別為 userDetails()：查詢帳戶中點數餘額；allUsers()、allPlans()、tokenRate()、exchangeRate()：回傳資料數值，以供開發者於前端使用；exchangeToken(A,x)：從 A 帳戶中扣除兌換點數數量，點數數量計算由欲取得的加密貨幣數量乘上兌換率而來。程式碼如圖 9 所示。

函式名稱	功能簡述	輸入值	回傳值
userDetails(A)	查詢 A 帳戶中的點數餘額	address	uint256
allUsers()	回傳全部使用者的帳戶地址與點數餘額	-	address, uint256
allPlans()	回傳全部募款計畫的名稱與收款的帳戶地址	-	bytes32, address
tokenRate()	回傳以太幣與加密貨幣 TT 的兌換率	-	uint256
exchangeRate()	回傳顧客點數與加密貨幣 TT 的兌換率	-	uint256
exchangeToken(A,x)	從 A 帳戶中扣除兌換點數數量	address, uint256	bool

表 3 TutorialToken 智能合約函式整理

doi:10.6342/NTU201801612

```
  function userDetails(address userAddress) view public
returns (uint) {
    return userInfo[userAddress].userPoints;
  }

  function allUsers() view public returns
(address[],uint[]) {
    return (userList,pointList);
  }

  function allPlans() view public returns
(bytes32[],address[]) {
    return (planNamesList,planAddressList);
  }

   function tokenRate() view public returns (uint) {
    return tokenRate;
  }

   function exchangeRate() view public returns (uint) {
    return exchangeRate;
  }

  function exchangeToken(address userAddress ,uint
exchangeAmount) public {
    uint exchangePoints = exchangeAmount*exchangeRate;
    uint availablePoints=userInfo[userAddress].userPoints;
    require(availablePoints >= exchangePoints);
    userInfo[userAddress].userPoints -= exchangePoints;

     }
}
```

圖 9 TutorialToken 智能合約程式碼

在 migrations/目錄下建立一個 2_deploy_contracts.js 檔案，此為佈署智能合約的初始值，包含：顧客帳戶地址、顧客點數、募款計畫名稱、募款計畫帳戶地址、

doi:10.6342/NTU201801612

以太幣購買加密貨幣 TT 的匯率及顧客點數兌換加密貨幣 TT 的匯率，內容如下圖 10。

```
var TutorialToken = artifacts.require("./TutorialToken.sol");
module.exports = function(deployer) {

deployer.deploy(TutorialToken,['0xd2f056614a9d396c702821985d61abe8ac22eb2a','0x8c66c0410da63507a543a4f0746b37e2d4a83647','0xf9e1409c4cac3c5e3d8f17991ec10c4896cfec52'],[0,0,1000],['A','B'],['0xe0f66b2d7999a5d164e623eaa148a944df4328de','0x4432f6a8edf59e32023d1137d29023fd2fed9129'],100,1);
};
```

圖 10 佈署智能合約初始值程式碼

4.2 系統展示

本節將開始展示系統介面，並逐一介紹本系統的功能以及操作流程，展示如下：

(一) 加密貨幣管理者端

加密貨幣管理者成功佈署智能合約到區塊鏈上，系統畫面如圖 11。

```
peiyu@ubuntu:~/point$ truffle mirgate
Using network 'development'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
  ... 0x382692f74b19f3247ecec6803e6163ab8c1f15ea3d06592839ebcd57be93e535
  Migrations: 0x0cf7124a6bee8333a98a61fa0063a822b91cf327
Saving successful migration to network...
  ... 0x3480ea341a596280d5b14b39e7cc91ad0620df8deedbd52d816cf385aabcea1e
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying TutorialToken...
  ... 0xe5382b4601858724f08160002d142b81ba8d61d8fe9023137690b48e8cb1f887
  TutorialToken: 0x18159a1a7032e49941f087d37f12d9047868f510
Saving successful migration to network...
  ... 0xef603556e0938ed92214af2817accd9b15b4c0686968cd0e76fe73ba0e247aa1
Saving artifacts...
```

圖 11 佈署智能合約系統截圖

成功部署後，使用 MetaMask 瀏覽器插件錢包，登入加密貨幣管理者帳戶地

doi:10.6342/NTU201801612

址，錢包餘額為加密貨幣總發行量，如圖 12。

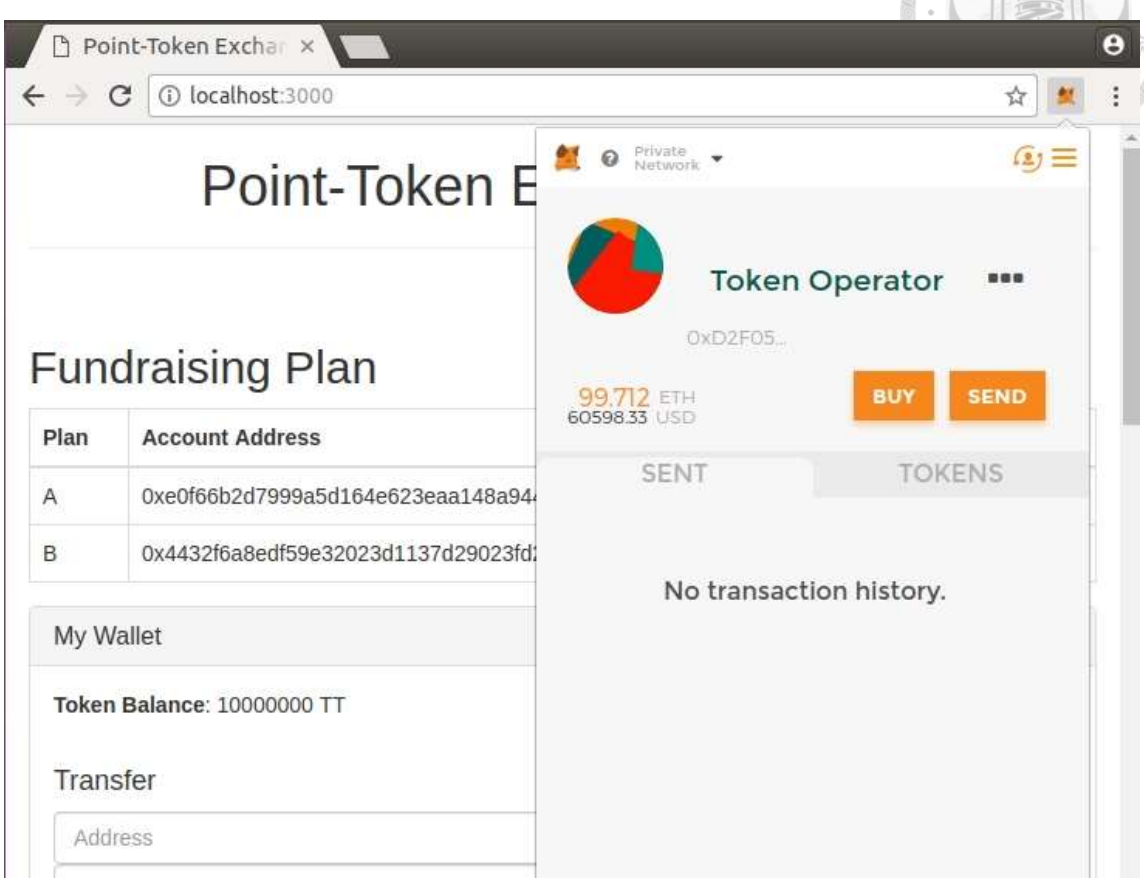

圖 12 加密貨幣管理者錢包畫面截圖

(二) 點數發行商端

錢包切換為點數發行商的帳戶地址，點數發行商使用以太幣向加密貨幣管理者購買加密貨幣 TT，以供其顧客用點數來兌換加密貨幣，如圖 13。

doi:10.6342/NTU201801612

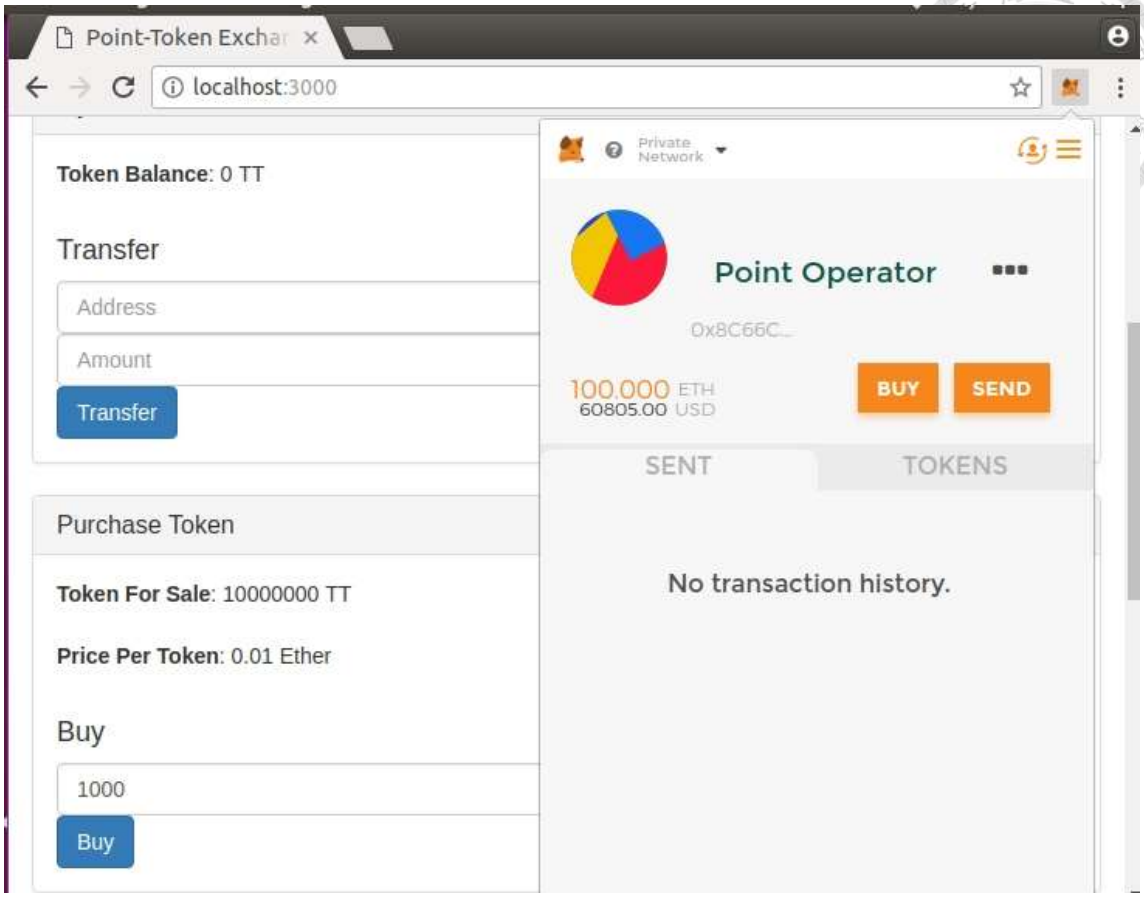

圖 13 點數發行商購買加密貨幣 TT 畫面截圖

按下購買按鈕後，購買匯率為 0.01ETH 兌換 1TT，購買 1000TT，因此支付 10ETH 給加密貨幣管理者，錢包交易畫面如圖 14。

doi:10.6342/NTU201801612

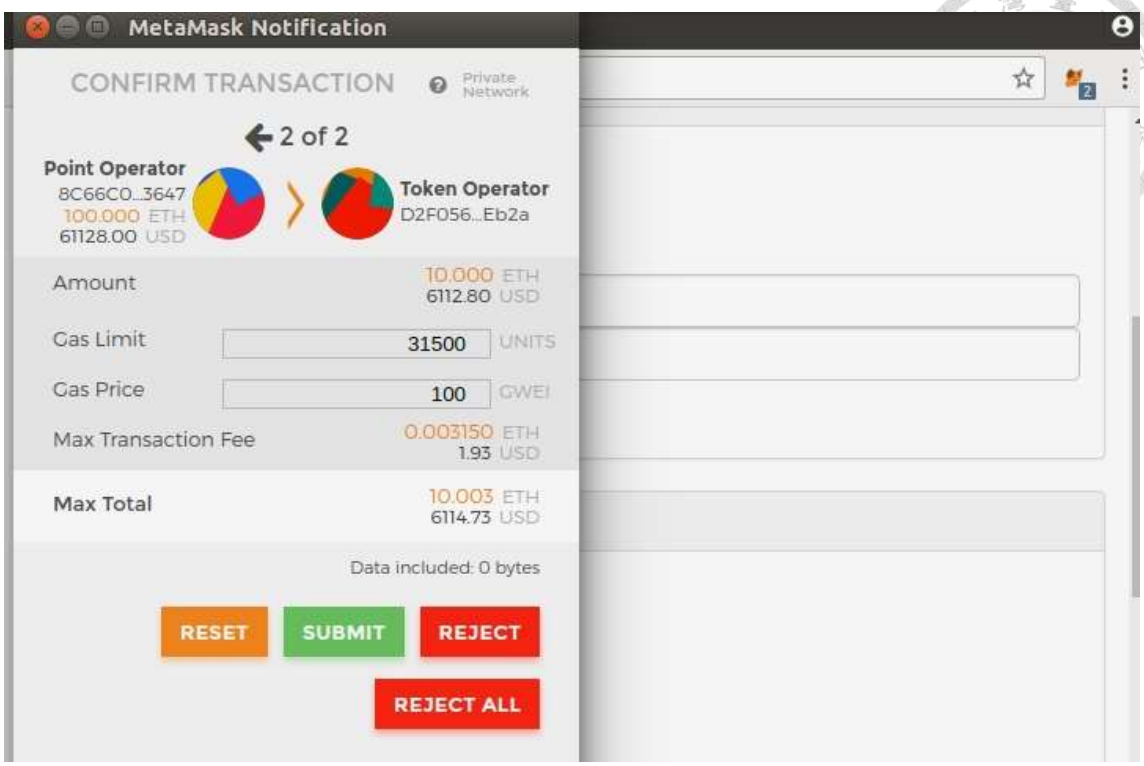

圖 14 點數發行商支付以太幣給加密貨幣管理者畫面截圖

支付以太幣交易成功後，會跳出購買成功提醒，如圖 15。

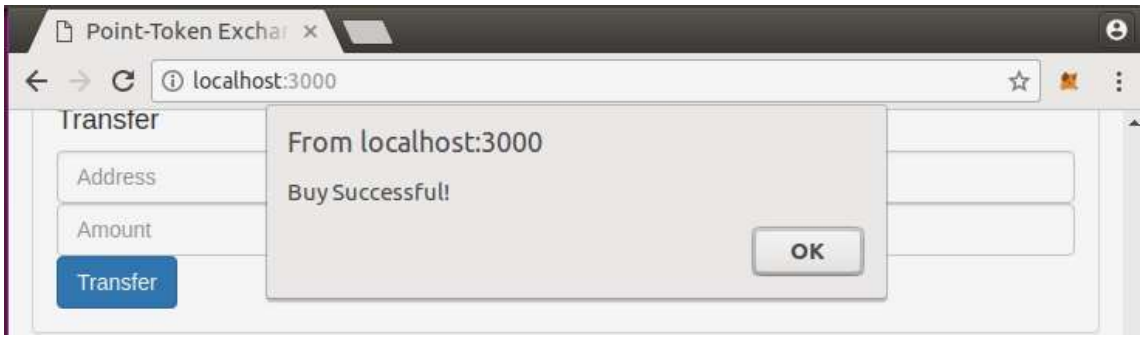

圖 15 系統提醒購買成功畫面截圖

點數發行商從加密貨幣管理者帳戶取得 1000TT，其錢包餘額更新為 1000TT，如圖 16。

doi:10.6342/NTU201801612

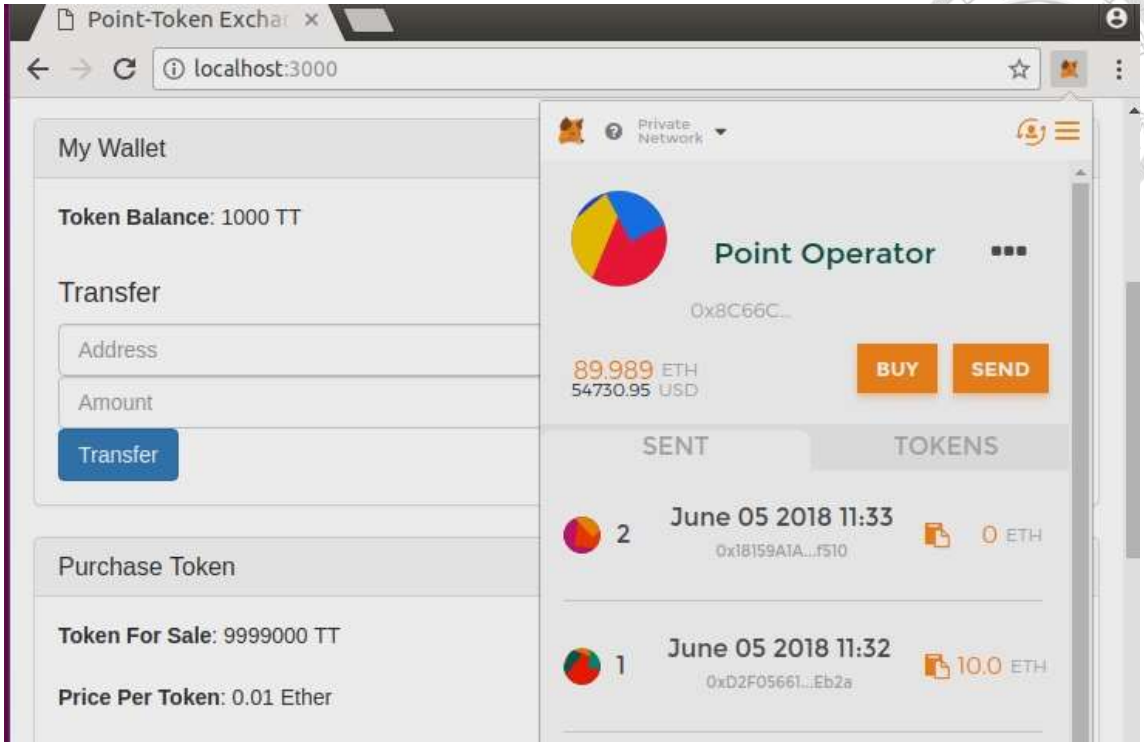

圖 16 點數發行商錢包畫面截圖

(三) 顧客端

錢包切換為顧客的帳戶地址，顧客畫面可以看到系統目前可供兌換代幣(Tokens for Exchange)為 1000TT，顧客目前有 1000 點點數，使用會員點數兌換 TT，如圖 17。

doi:10.6342/NTU201801612

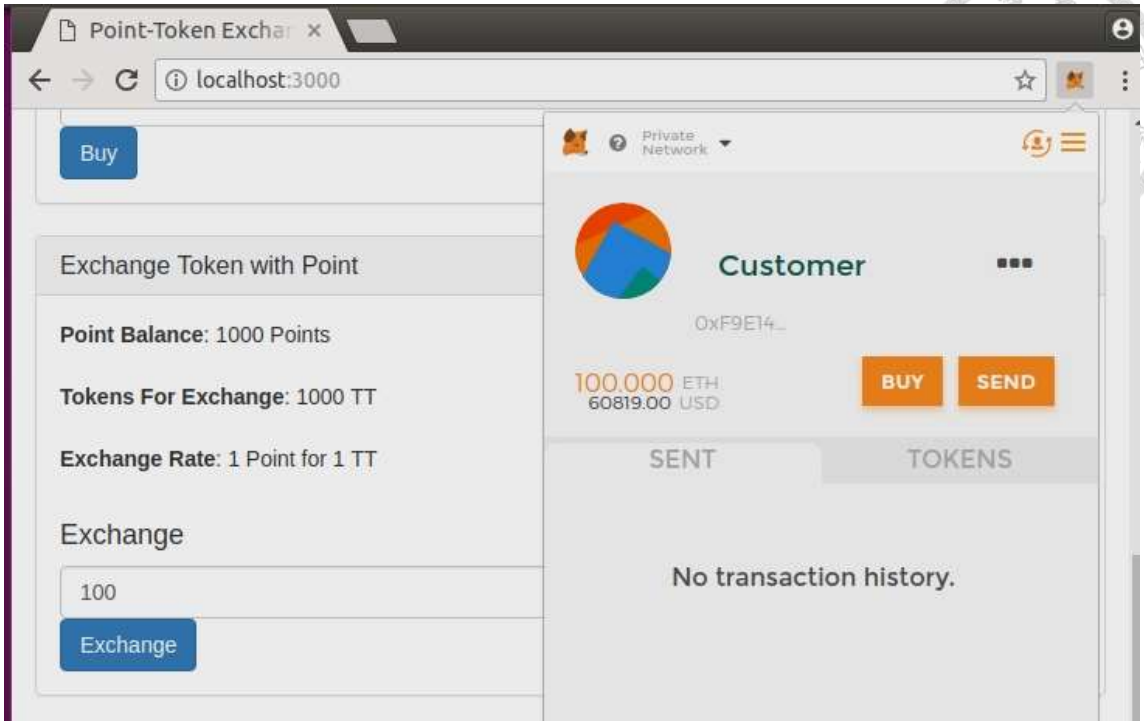

圖 17 使用會員點數兌換 TT 畫面截圖

匯率為 1 點數兌換 1TT，兌換 100TT 必須扣除 100 點，系統送出交易如圖 18。

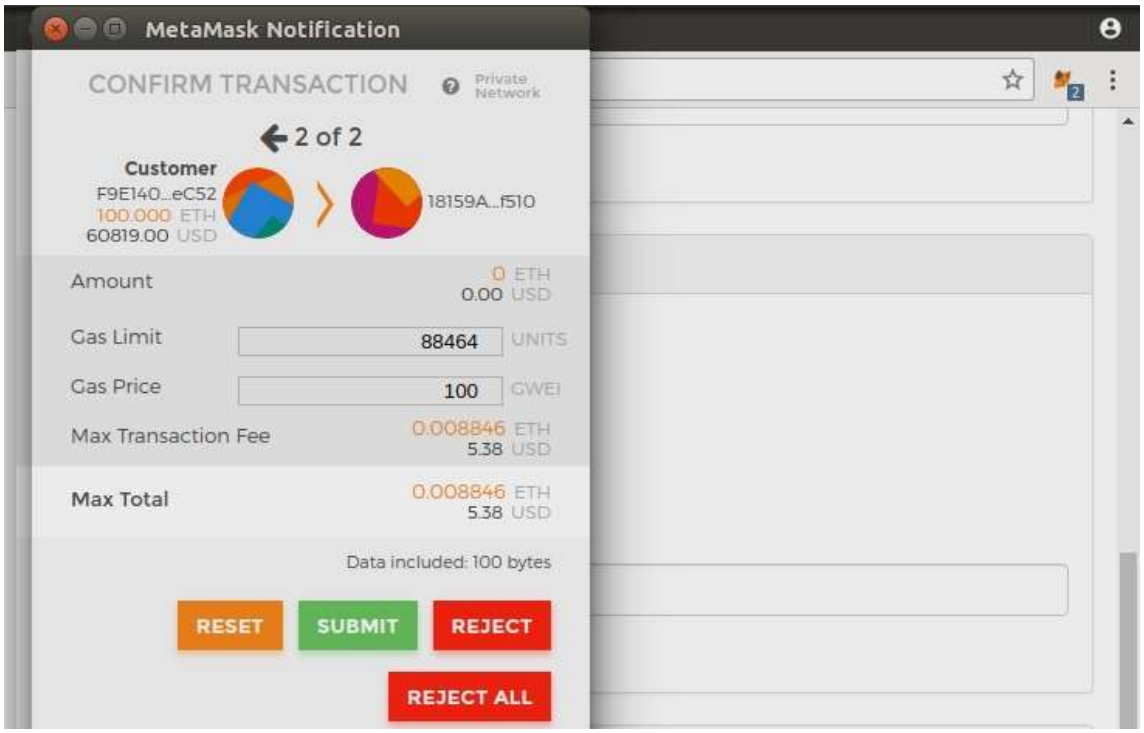

圖 18 系統發送兌換點數交易畫面截圖

doi:10.6342/NTU201801612

兌換點數交易成功後，系統跳出兌換成功提醒，如圖 19。

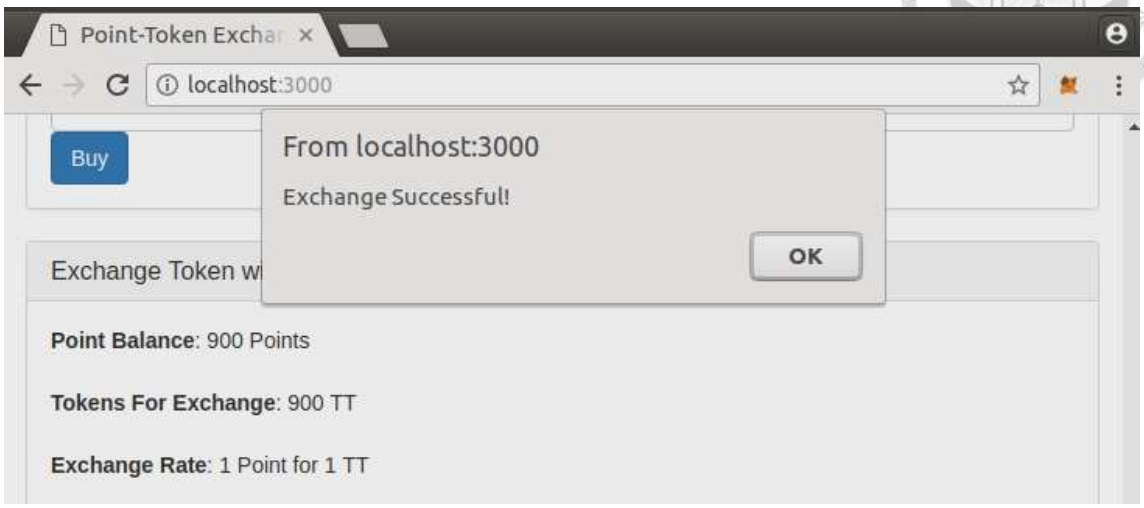

圖 19 系統提醒兌換成功畫面截圖

兌換成功後，顧客錢包餘額更新為 100TT，網頁畫面上方為募款計畫列表，顧客可以選擇欲捐款的計畫，輸入計畫帳戶地址及捐款 TT 金額，如圖 20。

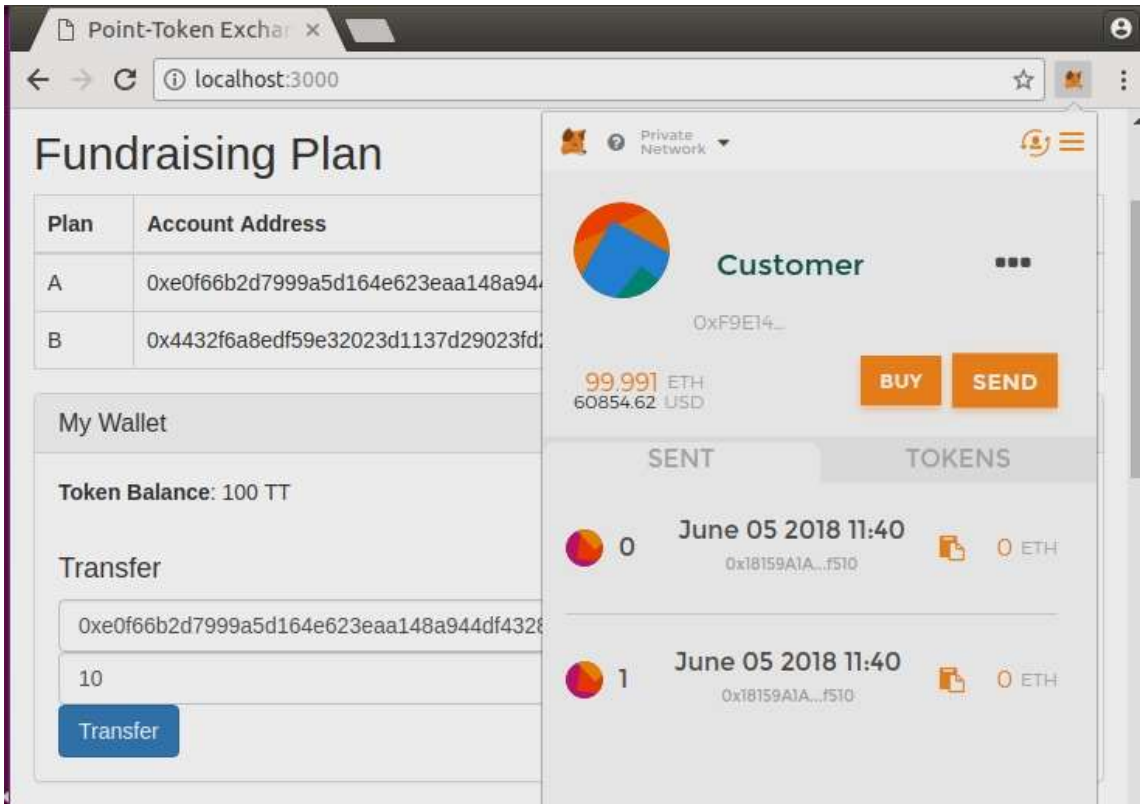

圖 20 使用加密貨幣 TT 捐款畫面截圖

doi:10.6342/NTU201801612

系統傳送捐款加密貨幣 TT 給募款計畫帳戶地址，交易畫面如圖 21。

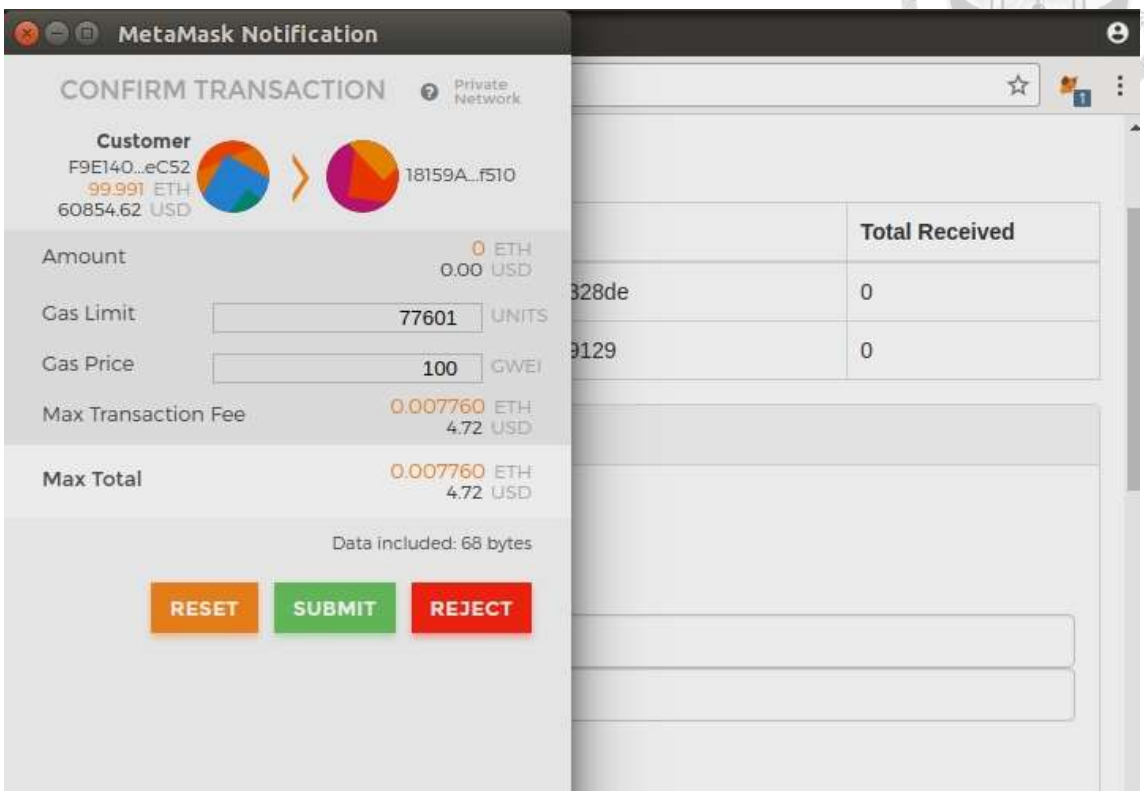

圖 21 傳送捐款加密貨幣 TT 畫面截圖

捐款成功後，顧客加密貨幣錢包餘額更新，募款計畫列表的已收到款項金額也會更新，如圖 22。

doi:10.6342/NTU201801612

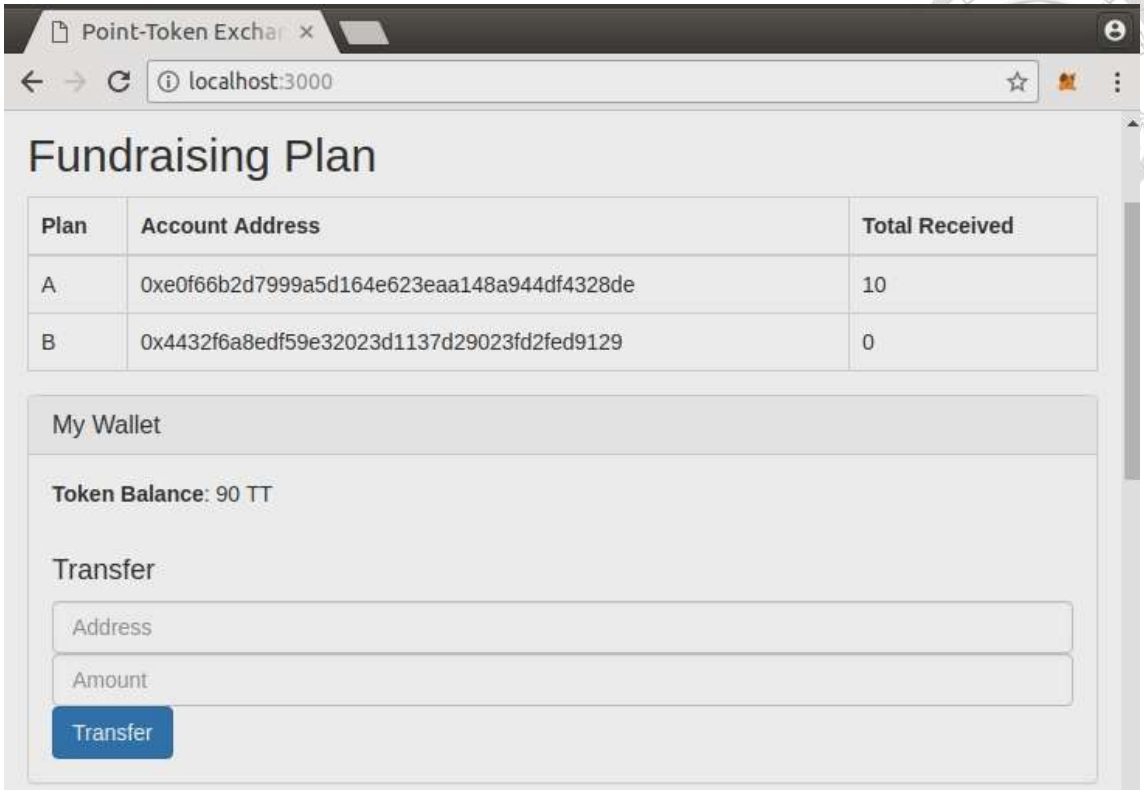

圖 22 捐款成功系統更新畫面截圖

4.3 系統分析

本研究建立一網站模擬加密貨幣管理者佈署智能合約並發行加密貨幣 TT；點數發行商可以使用以太幣購買加密貨幣，以供其顧客兌換；消費者可以扣除點數來兌換加密貨幣，並利用其加密貨幣捐款給募款單位。

此點數兌換平台與目前市場上點數兌換模式不同的地方在於，當更多點數發行商加入後，消費者可以透過一個網站就能將手上不同的點數兌換成加密貨幣並存入自己的加密貨幣帳戶地址，不再需要登入不同的網站或是下載各式各樣的 APP，之後也可以在同個平台上利用加密貨幣獲取想要的商品或是服務。同時，點數發行商也可以在平台上擔任提供服務或商品的角色賺取加密貨幣，達成透過點數促成消費者再次回購的行銷目的。

而與目前市場上利用點數進行捐款不同的地方在於，消費者可以直接利用加

doi:10.6342/NTU201801612

密貨幣進行捐款，因此沒有最低額度限制，提高消費者捐款的靈活性，此外，募款單位所募得的款項公開且金額不能被竄改，資訊透明度的提升可以提高消費者捐款的意願。

doi:10.6342/NTU201801612

第五章 結論

5.1 研究結論

過往紅利積點是企業關鍵的行銷工具，但不同企業均有自己的兌換機制，使得消費者持有的點數種類繁多，卻不見得可以累積至兌換門檻，造成企業無法有效利用點數來維持消費者忠誠度。

因此，本研究建立一個以區塊鏈技術為基礎的點數兌換平台，消費者可以在此平台上以會員點數向點數發行商兌換平台所發行的加密貨幣，可再用此加密貨幣進行捐款。對於消費者來說，透過此平台可以進行多種會員點數兌換，減少過去需要在不同平台上分別兌換的不便，也降低集點門檻並活化點數用途，使消費者手上所擁有的點數價值提升；對於點數發行商來說，點數可以兌換成區塊鏈上的加密貨幣，增加點數的使用場域，提高點數對於消費者的吸引力，同時業者也可以扮演平台上的服務或商品提供者，達到利用點數刺激顧客再次消費的行銷目的，此外，區塊鏈上交易即清算，可以降低對帳成本與提高清算效率。本研究利用區塊鏈技術簡化點數兌換流程，改善消費者使用經驗，消除現有點數兌換模式的限制，藉此擴大點數兌換的生態圈，進而達成企業轉型並創造利益。

5.2 未來展望

本研究所開發之系統雖然是以點數兌換為主要的研究方向，但隨著近年來國內行動支付日漸普及，希望未來能將電子錢包結合至此點數兌換平台，電子錢包業者成為區塊鏈上一節點，並在其應用程式協助使用者開通帳戶地址，使用者可以透過電子錢包發送交易到區塊鏈上，這樣一來，顧客就可以使用加密密貨幣進行支付，讓支付、集點、兌點都在同一個平台完成，擴大此加密貨幣的生態圈，同時也提升原本電子錢包業者所發行之點數價值，甚至後來新加入之業者可以選擇直接給予

doi:10.6342/NTU201801612

顧客加密貨幣當作消費回饋，形成新的商業模式。

doi:10.6342/NTU201801612

參考文獻

英文部分

Blattberg and Neslin（1990）. Sales Promotion: Concepts, Methods.Strategies NJ: Prentice Hall.

Michele D'Aliessi（2016）. How Does the Blockchain Work? .Retrieved from https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae#.ty235vz7h.

Reichheld, F., and W. E. Sasser Jr.（1990）. Zero Defections: Quality Comes to Services.Harvard Business Review ,68,105-111.

S. Nakamoto（2008）. Bitcoin：a peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Vitalik Buterin（2015）. Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper.

中文部分

Richi（2013 年 7 月）。想要看穿熟客的心？發紅利點數給他們吧！。科技報橘。取自：https://buzzorange.com.

中國區塊鏈技術和產業發展論壇（2016）中國區塊鏈技術和應用發展白皮書。

李晶（2017）。区块链技术中的密码应用。取自：http://www.westone.com.cn/uploadfile/2017/1016/20171016031244998.pdf

doi:10.6342/NTU201801612

林詩晃（2003）。紅利積點活動設計與積點贈品偏好之關係－探討顧客忠誠度之干擾效果。國立交通大學經營管理學系碩士論文。未出版。

張凱君（2018 年 3 月）。迎接數位貨幣時代 各國央行因應對策不一。台灣銀行家雜誌第 99 期。

陳恭（2017 年 10 月）。智能合約的發展與應用。財金資訊季刊第 90 期。

楊英伸（2016 年 10 月 16 號）。區塊鏈發展趨勢。證券暨期貨月刊第三十四卷第十期。

賴怡伶、莊鯉銓（2016）。金融科技、區塊鏈技術探討暨人民幣跨境支付之近期發展。參加 SWIFT「2015 年國際金融年會（SIBOS）」報告。取自：https://report.nat.gov.tw

羅鈺珊（2017）。分散式帳本與區塊鏈的應用現況與挑戰。經濟前瞻。取自：http://www.cier.edu.tw/site/cier/public/data/173-14%E5%9C%8B%E9%9A%9B%E7%B6%93%E6%BF%9F.pdf

doi:10.6342/NTU201801612