東海大學資訊工程研究所

碩士論文

指導教授: 蔡清欉　博士、朱延平　博士

區塊鏈與智能合約在數位學習平台上之應用

Application of Blockchain and Smart Contract for E-Learning Platform

研究生:陳英倫

中華民國 一百零七年六月

東海大學碩士學位論文考試審定書

東海大學資訊工程學系 研究所

研究生 陳 英 倫 所提之論文

區塊鏈與智能合約在數位學習平台上之應用

經本委員會審查，符合碩士學位論文標準。

學位考試委員會
召 集 人 _____ 簽章

委 員 _____

_____

_____

指 導 教 授 _____ 簽章

中華民國 107 年 6 月 16 日

致謝詞

時光飛逝，轉眼間，研究所的生涯就將告一段落；在祝福聲中，即將畢業了。驀然回首，百感交集，此時此刻的心情充滿著無限的感恩。

本論文能夠順利完成，我衷心感謝兩位指導教授朱延平老師和蔡清欉老師。這些年來，由於他們的悉心指導，我終於對區塊鏈有了初淺的認識。兩位老師在學術研究上嚴謹細緻、一絲不苟的作風，一直是我學習的榜樣。學生有幸追隨兩位教授，他們循循善誘的教導和不拘一格的思維給予我無盡的啟迪，讓我受益匪淺。在此謹向兩位指導教授致上我最崇高的敬意與最誠摯的感激。

論文審查與口試期間，承蒙交通大學資訊工程學系袁賢銘教授與台南應用大學資訊管理系廖元勳教授的剴切指正，並提供諸多精闢見解與建議，使本論文更臻完美，在此致上深深的謝意。

感謝書偉學長，在論文撰寫過程中的細心指導；在我遇到挫折時給予鼓勵，並協助解決問題，使我的研究能夠順利完成。另外感謝在碩士班一起同甘共苦的夥伴沅隴、子維、大維，還有其他好友們偉成、書瑀、柏翔及柏翰，因為有你們，讓我在研究生涯中增添了許多歡樂與回憶。

此外，更要感謝我親愛的家人，因為有你們一路的支持與鼓勵，讓我無後顧之憂，能一直朝目標挑戰，持續努力向前邁進。

摘要

透過資訊科技的輔助，數位學習改變了人類的學習環境與方式，老師教學與學生學習不受時間、空間的限制，選擇既多元又豐富。

許多大專院校都設有自己的數位學習平台，其中又以 Moodle 開放原始碼最為常用。除了處理校務行政外，也提供學生進行線上學習的任務。目前各大學的數位學習平台多用於提供教學輔助與課後輔導，對於學生學習歷程與成效也僅限於校內或課堂內使用。校外單位則無法得知學生修課的成果或狀況。

本研究利用區塊鏈技術的可追溯性、不可竄改、時間戳與加密等特性，強化現有的數位學習平台，將學生在數位學習之相關資訊詳細紀錄於區塊鏈上，期望在 Moodle 平台結合區塊鏈技術架設智能合約，藉此系統，學生在數位學習平台的學習成果，可以提供校外單位作為參考。

在本研究中，我們執行教師開課和學生學習部分。學生從選課完成到接受測驗，整個流程都有詳實、不可竄改的紀錄。這個紀錄將成為學生的學習履歷表，裡面有學習的課程與成績，若再連結畢業證書系統，則學生畢業以後，可直接利用區塊鏈裡的資料求職，或繼續求學，不必再回學校申請畢業證書。

關鍵字：數位學習、區塊鏈、智能合約、Moodle。

Abstract

Thanks to information technology, e-learning has changed the learning environment and methods. The process of teaching and learning has transcended limitations in time and space,making choices rich, abundant and diverse.

Many colleges and universities have their own e-learning platform. Most of them use moodle platform with open source code. On top of handling school administration tasks, the platform provides students with the task of conducting e-learning. At present, the e-learning platforms of universities are used more commonly to provide teaching aids and after school counselling. In so far as gauging the students' learning track and effectiveness, the current platforms are effective for use within the classroom or on campus. Beyond the confines of the campus, there is no way of gauging the effectiveness of the students' learning process.

This research study uses the characteristics of blockchain technology such as traceability, irreversibility, timestamp and encryption in order to strengthen existing e-learning platforms and record detailed information on the students' e-learning on the blockchain. It is hoped that the moodle platform can combine blockchain technology and smart contracts. Through this system, the outcome of the students' e-learning platform can be used as a reference to out of school units.

We conducted lecturing and learning process in this study. It was recorded in a detail and irreversible way. This record, as a learning track of the student, contains courses and grades of study. It could be linked with the graduation certificate system, and students may use the records in the blockchain to apply for jobs or advanced education admission instead of going back to the school for retrieving a diploma.

Key words: e-learning , blockchain , smart contract ,Moodle

目錄

圖目錄

表目錄

第一章 緒論

本章節將介紹研究動機與背景，說明數位學習平台 Moodle 目前的狀況以及區塊鏈技術的發展趨勢。

1.1 研究動機與背景

21 世紀已是資訊化世代，藉著科技的突飛猛進，各行各業都已在自己的領域上，不斷突破，追求卓越；政府在 2003 年開始推行「數位學習產業推動與發展計畫」，將數位學習產業帶入一個展新的境界，在學校的數位學習系統也已經相當普及。

相較於其它 CMS（內容管理系統），就後端使用者操作行為分析而言，以 Moodle 平台功能最為強大，因此教育部課程服務平台選用 Moodle 作為其系統開發的基礎。Moodle 數位學習平台目前已廣為學校師生利用， Moodle 平台有許多統計模組，例如點選線上教材的流覽狀況分析，詳盡的分析學生瀏覽過那些線上教材，瀏覽停留多久時間，線上測驗作答多久…等。雖然學生線上瀏覽教材時間，並不能代表他學習投入與否,不過其中有許多使用者操作行為分析，卻是未來教師在編寫教材時很好的參考資料。另外，Moodle 還有其他的統計分析模組，若能善用，對教育者與受教者將有很大的幫助。

目前許多大專院校都設有自己的 Moodle 平台，除了處理校務行政外，也執行線上學習的任務。由於數位學習平台本身的限制，學校內修課的資源以及學生修課的成果訊息皆無法被校外單位取得，也無法提供學習成效的佐證，僅能以成績單作為依據。

開放徽章(Open Badges)是一種識別學習的新方式，包含正規教育以及線上學習。全世界有數千個組織已經發布開放徽章，從非營利組織到主要雇主，以至於各級教育機構。很可惜的是，目前在國內仍然沒有任何機構參與開放徽章機制，導致以往的學習履歷與能力，外界無法得知與認同，一旦有了開放徽章機制，就可以打破這個限制。政府單位應該要正視這個問題，鼓勵並要求教育及訓練機構及企業積極參與，以善用人力資源，導引整個國家向上提升。

區塊鏈技術之應用十分廣泛，舉凡能夠透過提升信賴度來進行的相關工作，都相當的適合。

有鑑於此，本論文試圖改進學校的 Moodle 系統，採用區塊鏈的技術，建立以太坊私有鏈並結合智能合約，紀錄開課、修課、數位學習成果等資訊。藉此，可以讓課程的資訊被完整保留，學生也可以在修課通過後在區塊鏈上留下證明。最值得一提的是，有了區塊鏈紀錄的資訊，校外單位可以透過申請查詢的方式取得學生的學習資訊，進而了解學生的學習態度以至於工作態度。

1.2 研究目的

本論文之研究目的，希望藉由在以太坊上，架構智能合約，以詳實記錄學生之學習履歷。學生從選課完成，進入數位學習，到接受測驗，以至於取得畢業證書，都將詳實記錄於區塊鏈上。區塊鏈上記錄著學生的學習資料，諸如課程別、何時上線學習、每次學習多久、學習頻率、何時接受測驗以及測驗結果等。如果能蒐集大數據進行分析，則可以了解學生需求與困難，進行數位內容改善或調整，提升學習動機與成效。

1.3 論文架構

本論文共分為五個章節：第一章緒論，說明本研究之研究動機與背景、研究目的及論文架構。第二章文獻探討，簡介與本研究相關之概念及技術，包括數位學習、Moodle 平台、區塊鏈技術以及智能合約。第三章研究方法，包括流程架構與研究資源，主要介紹本研究所發展出來之流程架構和所利用之研究資源。第四章研究結果，說明本研究如何建立區塊鏈，以及平台設計和發現。第五章結論與建議，闡述本研究之發現與討論事項。

第二章 文獻探討

本章節首先回顧數位學習定義、Moodle 平台與開放徽章及其嵌入區塊鏈之實驗、數位學習之產業市場與理論模型，接著介紹區塊鏈技術、演進及未來發展趨勢；最後探討以太坊平台與智能合約之部署、運作；以及區塊鏈與智能合約之應用。

2.1 數位學習

隨著網際網路的蓬勃發展，透過資訊科技的輔助，數位學習改變了人類的學習環境與方式，使用者可以在不受到時間與空間的限制下進行學習，能夠有效減少交通、場地和時間等成本。

2.1.1 數位學習之定義

根據美國人力資源發展協會（ASTD）的定義，數位學習的範圍包含很廣，諸如利用網際網路、衛星廣播、互動電視、以及光碟片教材等來進行課程學習，都屬於數位學習。美國知名市場研究機構 Gartner Group 及 IDC 亦持類以的看法。

數位學習國家型科技計畫(2002)定義「數位學習」是以數位工具，透過有線或無線網路，取得數位教材，進行線上或離線之學習活動；因此數位學習產業涵括數位學習工具(載具及輔具)研發、數位學習網路環境建置、數位教材內容開發以及數位學習活動的設計等[1]。數位學習具有以下幾個共同特性：

1. 遠距教學的模式。
2. 採用數位化的學習資源。
3. 藉由衛星廣播、互動電視、光碟教學、網際網路等方式傳送教材。
4. 可以是同步或非同步的學習模式。

2.1.2 數位學習與傳統教學之比較

利用數位學習，學生不會被限制在固定時段或固定地點進修,也沒有刻板進度，學生自己還可以自我測試學習成效，並與相關成員分享學習經驗；而且企業界也不用再大費周章地投資昂貴的軟硬體訓練設施，以及龐大的差旅費支出，甚至於員工的學習資料庫還可充作公司管理知識資產的依據。

與以講師為中心的傳統課堂學習相比,數位學習提供了以學習者為中心的自主學習環境。更多基於多媒體的電子學習系統，可用於整合如文本、圖像、聲音和視頻等不同呈現方式的學習材料。

數位學習與傳統教學各有優點和缺點，所以學生在選擇之前，要了解自我期望的內容。有三個關鍵領域：靈活性、紀律和自我激勵以及社交互動，我們必須仔細研究[2]。這沒有正確或錯誤的答案，其中大部分歸結於個人偏好，並了解自己如何學習最好。無論個人學習風格和情況如何,這些學習方式都可以非常有效。數位學習與傳統式教學間，其特性有許多差異存在,表 2-1 針對其特性差異加以比較[3]。

表 2-1 數位學習與傳統教學特性比較

比較項目	數位學習	傳統教室學習方式
教材	1、個人化教材 2、更新及時、快速 3、Just-in time 的學習方式，只提供所需資訊。	1、制式教材 2、更新速度慢 3、Just-in-case 的學習方式,提供大量資料，但相關性如何不得而知。
成本	達國際化規模時相對成本較低	規模較小，相對成本較高
資訊擷取	無時間限制，一週 7 天，一天 24 小時。	只在固定時間
衡量效果	藉資訊科技自動衡量受訓結果	不易衡量
學習中心	以學習者為中心 (learner-centric)	以老師為中心 (instructor-centric)
互動性	較差	較佳

資料來源:彭成翰, 2004。

Zhang et al.(2003)認為傳統教育訓練方式與數位學習的方式其各有優劣，數位學習是否可以完全取代傳統教室的訓練方式是值得探討的。一般而言，數位學習的學生相較於進行傳統教室學習的學生，必須具備更高的自律精神，否則常有半途而廢的情形發生。表 2-2 為數位學習與傳統教學之優劣比較表。

表 2-2 數位學習與傳統教學優劣比較

	傳統教室學習	數位學習
優點	1. 立即回應。 2. 對學習者與授課者皆較為熟悉 3. 對學生的刺激較為直接。 4. 能促進社會化的溝通。	1. 以學習者為中心並且能自行調整學習步調。 2. 時間與地域較為彈性。 3. 對學習者而言較具成本效益。 4. 全球觀眾皆是潛在的學習者。 5. 知識的擷取不受限。 6. 知識的再使用與分享具備檔案存取的功能。
缺點	1. 以教師為中心。 2. 受限於時間與地域。 3. 知識的傳遞上成本較高。	1. 在非同步的數位學習中缺乏立即的回應。 2. 增加授課者的備課時間。 3. 對某些人來說會感到不適應。 4. 會潛在有挫折、焦慮與困惑的感覺。

資料來源:彭成翰, 2004。

2.1.3 Moodle 平台

Moodle 是“Modular Object-Oriented Dynamic Learning Environment” 的縮寫。它是線上教育平台，教育者可以利用它與老師及學生互動；學生可以使用它進行線上學習、繳交作業及接受測驗，並且與其他同學互動。Moodle 平台由 Moodle 專案團隊建立，該團隊由 Moodle 總部領導和協調，總部位於澳大利亞珀斯(Perth)。Moodle 在全球擁有 80 多家合作夥伴，並由他們提供財務支援[4]。

以下簡述 Moodle 之歷史：

1999 馬丁·道格亞馬斯(Martin Dougiamas) 在澳大利亞科廷大學(Curtin University) 的博士研究，創立 Moodle。

2002 Martin 將 1.0 版的 Moodle 開放原始碼系統推向世界。幾個月後，Moodle 在世界各地被採用。

2004 Brent Simpson 將 Moodle 描述為“LMS 世界的 Linux”。

2008 Martin 獲頒 Google-O'Reilly 教育推動者類之開放原始碼獎。

2015 Moodle 成為全球最受歡迎的學習管理系統，用戶數量最多，在全球 222 個地區擁有超過 8000 萬用戶。

Moodle 推出基於 SaaS(Software as a Service)的產品 - MoodleCloud

2016 Moodle 在全球的註冊用戶超過 1 億

2017 Moodle 成立 15 週年，宣布與眾多教育公司建立投資合作夥伴關係，並開始加速其五大關鍵成長項目：改進 Moodle 核心、學習 Moodle 課程、MoodleNet、Moodle 基金會以及擴充其服務與合作計劃。

為了建立 moodle 學習環境，首先要下載 moodle 軟體，並安裝於伺服器上。moodle 平台是開放原始碼，且採用模組式設計，因此使用者可依需要自行更改[5]。

2.1.4 開放徽章(Open Badges)

Mozilla 在 2011 年通過麥克阿瑟基金會和合作夥伴創建了開放徽章[6]，這是一種識別學習的新方式，包含正規教育以及線上學習。全世界有數千個組織已經發布開放徽章，從非營利組織到主要雇主，以至於各級教育機構。開放徽章具備完整資訊，包含徽章發行機構、徽章發行標準，甚至取得徽章所應完成的專案。利害關係人或機關可取得完整的資訊，並了解徽章背後的技術與成就。

目前我們可以在各地學習，而不只限於教室以內。但我們通常很難在學校以外的地方取得對能力或成就的認證。Mozilla 的 Open Badges 計畫就是用於解決這個問題，讓任何人都可以簡單地在共享的技術基礎上發放、取得和展現。其結果就是能幫助每個人取得且展示自己所擁有的能力，和打開新的職業與再受教育的機會[7]。開放徽章概念如圖 2-1，可分為四個部分：

1. 賺取開放徽章

   相關機構創建並發布開放徽章讓你賺取，使你能夠建立屬於自己的獨特資料，並在網絡上共享。獲得的每個徽章都包含有關你的技能以及發行機構的數據，當顯示和分享這些徽章時，人們可以查看這些數據，了解更多關於你的訊息。

2. 頒發你自己的開放徽章

   任何個人或組織都可以創建頒發者檔案，並開始定義和頒發開放徽章。任何以名稱、描述、URL、圖像和電子郵件地址描述的實體都可能成為發行人。要頒發開放徽章，需要一個支持開放徽章規範的技術平台。

3. 顯示開放徽章

   開放徽章旨在共享。通過分享，個人向消費者展示成就，使成為一種有價值的貨幣，以迎取新的機會。

4. 瞭解開放徽章

   開放徽章提供關於技能和成就的可攜式和可驗證訊息，代表合法的認證成果。接受徽章並提供交換機會的個人和組織，在生態系統中發揮關鍵作用。通過這個過程，開放徽章可以變成新的合作、工作、實習和終身學習者之間更加豐富的聯繫。

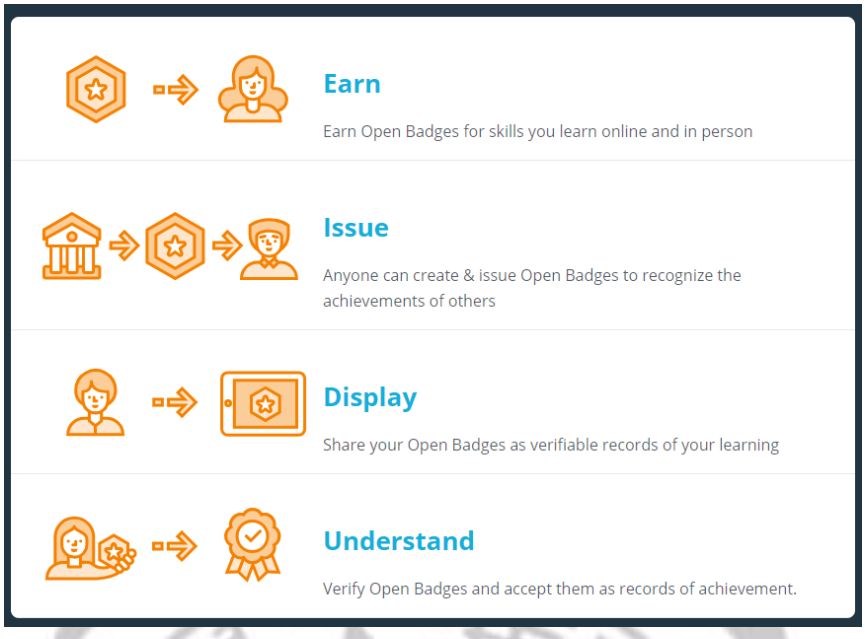

圖 2-1 開放徽章概念圖

資料來源: https://openbadges.org/

開放式徽章和區塊鏈都與信任有關，但卻以幾乎相反的方式進行。開放徽章是結合鏈和網絡的信任聲明，以網絡成員彼此信任的訊息作為建立信任交易的基礎[8]。

另一方面，區塊鏈是建立可信交易的手段，即使從事交易的人不相互信任。交易的可信度不是取決於參與者的行為或他們提供的數據的屬性，而是取決於添加到區塊鏈中下一個塊的可信度算法的屬性。區塊鏈技術旨在消除人為因素，從而決定交易是否值得信賴。

徽章鏈（BadgeChain）就像一個分佈式數據庫，徽章儲存在互聯網上。新物品可以通過徽章鏈中的徽章聚合物進行有機生長。

BadgeChain，建立動態多維網絡，而區塊鏈是不斷增長的一維鏈。一個可以添加和刪除數據（取消信任），另一個只能添加數據。一個來自非正規教育界，另一個來自正式的國際商業和金融界。圖 2-2 為徽章鏈與區塊鏈之差異。

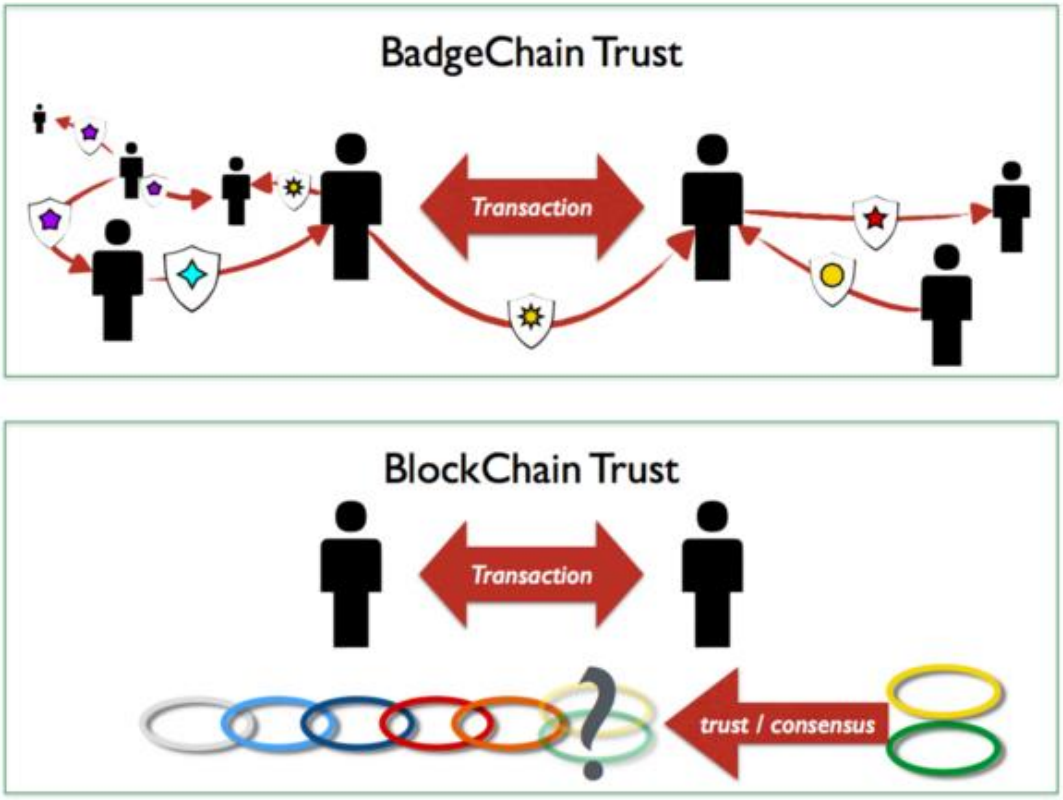

圖 2-2 徽章鏈與區塊鏈

資料來源: A Medium Corporation [US]

儘管徽章鍊與區塊鏈間存在著不同的特質，但大多數的倡導者都期望兩者可以合併。使得

Open Badges + Blockchain = BadgeChain

徽章鍊與區塊鏈合併可能有不同的方法:

1. 同化(Assimilation)：

   區塊鏈提供了一種更安全的方式來儲存證書，相關機構可以逕行採用區塊鏈技術，而不必經由開放徽章的歷程。

2. 整合(Integration)：

   區塊鍊是一個分佈式數據庫，徽章的儲存方式與其他數據庫(MySQL，Oracle，Fedora 等）中儲存的一樣，利用區塊鏈的獨特屬性來改正當前開放式徽章基礎架構的一些缺點。

3. 配置(Accommodation)：

開放徽章用於重新考慮區塊鏈架構，協議和算法。區塊鏈可以將開放徽章的儲存從任何單獨的儲存區中釋放出來，因此徽章持有者不必選擇在一個特定的平台上運作。

目前有兩個倡導開放式徽章，並嘗試利用區塊鏈技術改進數據可驗證性的系統：Blockcerts 和 OpenBlockchain。

Blockcerts 是“用於發布和驗證基於區塊鏈的官方記錄的應用程序的開放標準”，包括學術證書和專業許可證。 Blockcert 的開源庫、工具和移動應用最初是由 MIT 的媒體實驗室 Learning Machine 和 Schmidt 團隊合作開發。

Blockcerts 最近的一個實例是麻省理工學院的數字文憑課程 ，該課程使學生能夠以數字方式分享可驗證的防篡改文憑。

而 OpenBlockchain 為英國 The Open University 和 KMI (Knowledge Medium institute) 所倡議，將在下一章節中進一步說明。

2.1.5 Moodle 與區塊鏈

開放徽章採用開放原始碼，紀錄學習者的學習履歷，若把它嵌入區塊鏈中，則可保有區塊鏈技術的可追溯性、不可竄改、時間戳與加密等特性，更可取得利害關係人或機關的信賴。

OpenBlockchain 為英國 The Open University 的 KMI (Knowledge Medium institute) 所倡議。KMI 的實驗主要針對英國的高等教育機構，但也在研究有關勞動力培訓以及通過區塊鏈進行教育資助的項目。KMI 正在採取一種獨特的方式來探索開放徽章，試驗方法是使用以太坊來儲存和發布它們[9]。OpenBlockchain 的第一個實驗乃將 OpenLearn 平台上獲得的開放徽章轉換為智能合約，顯示區塊鏈上的憑證訊息，每項成就所提供的證據皆儲存在區塊鏈中。KMI 設想一個應用於英國的區塊鏈，所有學生的證書都被儲存起來，以促進信任轉移，並允許潛在的雇主查看學生的資料。目前 KMI 團隊正在開發一個 Moodle 插件，將 Moodle 徽章發佈到智能合約。展示此視頻以及相關工作的其他訊息視頻可以在下述網址找到：https : //blockchain.open.ac.uk/#demos。圖 2-3 為 KMI 在以太坊上所進行之 Moodle 開放徽章嵌入區塊鏈的實驗截圖[10]。該實驗目前仍持續進行中，堪稱為本研究之先驅，對本研究有相當大的助益。

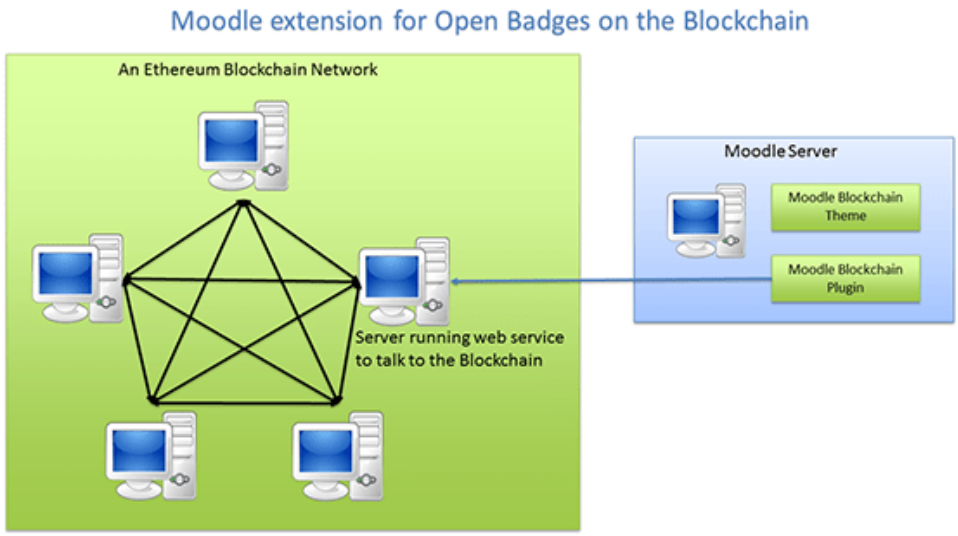

圖 2-3 Moodle 開放徽章嵌入區塊鏈

資料來源: http://blockchain.open.ac.uk/

2.1.6 數位學習產業之發展趨勢

1. 台灣數位學習產業產值分布

依據 2015 年台灣數位學習產業之產值分析[11]，其中硬體產值所占之比例最高，占總產值的 39.45%；其次依序為服務，占總產值 37.68%、數位教材占總產值 17.29%，以及平台/工具占總產值的 5.58%。而 2015 年數位學習產業與 2014 年相比，硬體長幅度最多為 28.66%，成長幅度第二大的為服務，成長率 26.50%，平台/工具成長幅度排名第三，達 19.53%。數位教材成長幅度最小，僅達 18.61%。整體而言，2015 年台灣數位學習產業仍為成長的趨勢，產值為 902.77 億，成長率為 25.48%，僅數位教材與平台/工具之成長較往年趨緩，探究其原因，與各級學校採購預算減少有關。

2. 全球數位學習市場分析

根據美國 Global Market Insights 研究機構進行的「全球數位學習市場」調查報告顯示[12]，全球數位學習市場規模在 2016 年估計超過 1,500 億美元，2017 年至 2024 年複合成長率(CAGR)為 5%，圖 2-4 乃依“應用”(Application)分類之全球數位學習市場。

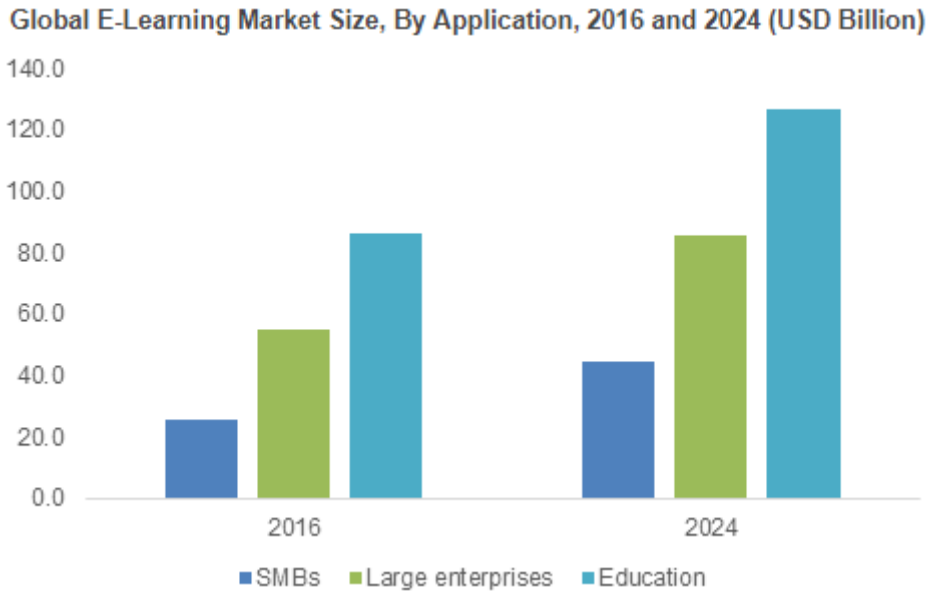

圖 2-4 全球數位學習市場預估值

資料來源: www.gminsights.com

2.1.7 數位學習之理論模型

Terry Anderson 在線上學習之理論與實務(Theory and Practice of Online Learning)一書中[13]，對於線上學習的理論發展，作了相當詳盡的探討。Bransford, Brown, and Cocking (1999)指出有效的學習由學習者中心化(learner centered)、知識中心化(knowledge centered)、評估中心化(assessment centered)及社群中心化(community centered)四個構面組成。為了達到有效的線上學習，參與者間的交互作用十分顯著。 Terry Anderson (2003)提出教育交互作用的六種模式，學生和學生間，學生和老師間，學生和內容間，老師和老師間，老師和內容間，及內容和內容間等，如圖 2-5。

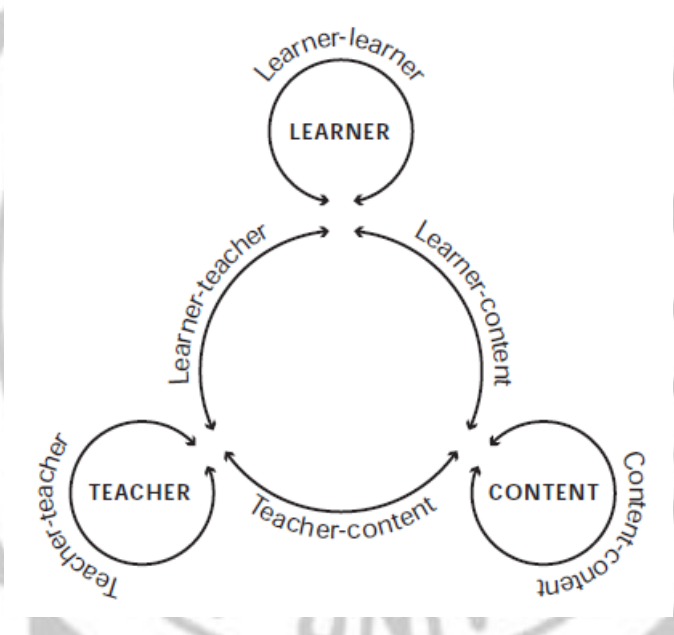

圖 2-5 教育角色交互作用圖

資料來源: Theory and Practice of Online Learning

Terry Anderson 更進一步發展出數位學習模型(A Model of E-learning)，如圖 2-6 所示。由該圖中，可以看出學生-老師-內容間之交互作用相當顯著且頻繁。此數位學習模型包括兩種不同模式，左半部為集體學習，而右半部為獨立學習。集體學習可能在社區進行，可以同步，也可以非同步學習。右半部雖說是獨立學習，但也可以跟同僚、家人及老師互動。至於學生-老師-內容間之交互作用，有很多方式，最常見的是利用網際網路。

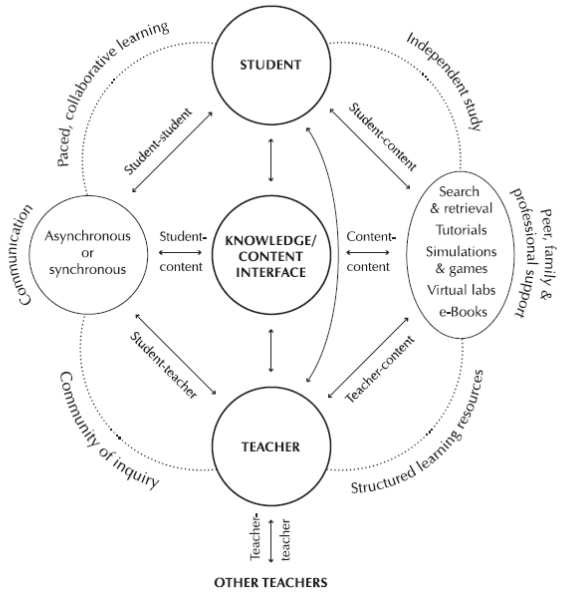

圖 2-6 數位學習模型

資料來源: Theory and Practice of Online Learning

本研究將簡化研究模型如圖 2-7，內容則針對學校 moodle 系統進行探討。

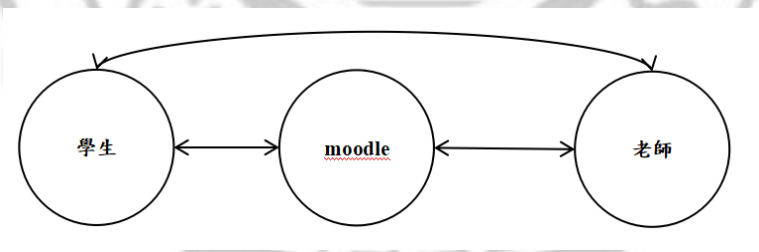

圖 2-7 簡式數位學習模型

2.2 區塊鏈

近年來比特幣價格暴起暴落，投資者追逐熱情卻絲毫未減。比特幣是否會崩盤，帶來一股熱烈的討論，也因此喚起人們對彼特幣底層技術-區塊鏈的好奇，想進一步探索其奧秘。

世界經濟論壇(WEF)創辦人施瓦布（Klaus Schwab）說，區塊鏈將帶動繼蒸汽機、電力和電腦發明而來的第四次工業革命；俄羅斯聯邦儲蓄銀行（Sberbank）副主席夏洛夫（Andrey Sharov）預言，區塊鏈技術會讓銀行在 10 年內消失[14]。到底甚麼是比特幣，以下就區塊鏈技術做一簡單介紹。

2.2.1 區塊鏈技術

2008 年爆發全球金融海嘯，中本聰(Satoshi Nakamoto)發表了全新的對等式電子貨幣協定機制，其所採用的電子貨幣就是帶有加密效果的比特幣[15]。在比特幣的應用中，區塊鏈是一個分散式帳本(distributed ledger)系統，參考圖 2-8 ，採用密碼技術（挖礦）來確保交易的正確性，不同的區塊鏈技術採用不同的共識機制。比特幣參與者集體維護一個具時序性的帳本系統（區塊鏈）。其中每一個區塊網路參與者都是一個節點，任何一個節點要發起一個交易行為，並將訊息傳遞到區塊網路中其他的每一個節點，如此可以確保存於所有節點上的帳本能精確地更新且驗證這一筆交易行為[16]。如果這筆交易無法獲得大多數的參與者認可，則將被拒絕存在於區塊鏈上，如圖 2-9 區塊鏈概觀圖所示[10]

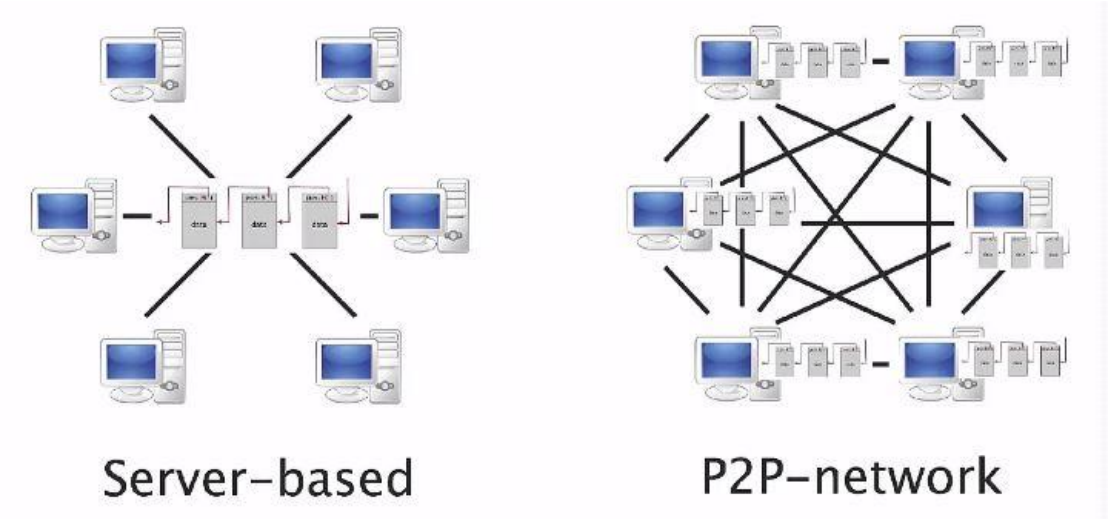

圖 2-8 集中式帳本與分散式帳本

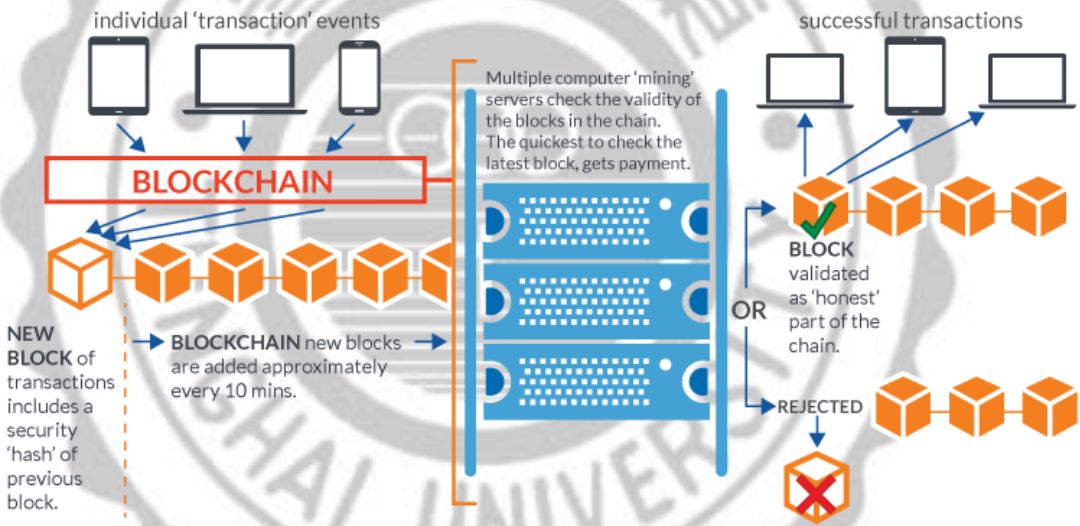

圖 2-9 區塊鏈概觀圖

資料來源: http://blockchain.open.ac.uk/

區塊鏈的構造如圖 2-10 所示 [17]，每個區塊就像一頁帳本，區塊的流水號(例如：27351)就像帳本的頁碼，反映區塊之間產生的順序。在內容方面，每個區塊都有一個特殊的安全編碼(Block hash，例如：005wp1x93f371a09)與時戳（timestamp），以及創建這個區塊的工作量證明（Proof of Work，PoW）等詮釋資料。

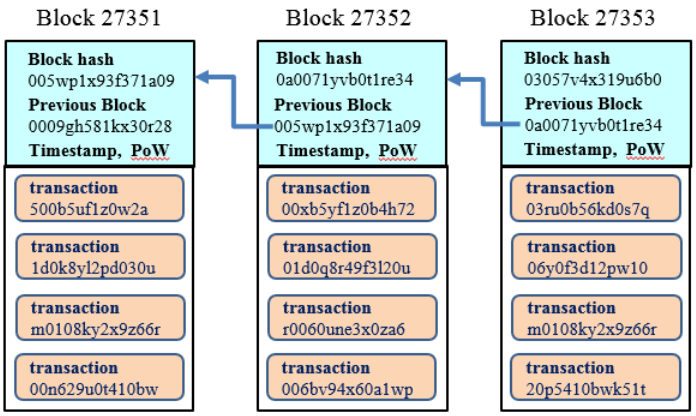

圖 2-10 區塊鏈示意圖

資料來源: 陳恭，區塊鏈革命，迎向產業新契機 20170927

區塊鏈是開放、可編程的技術。它是一種無法竄改的全球資料庫，能夠提供一個數位帳本，不僅用以記錄我們的金融交易，也可以記錄我們生活中每一個有價值的東西。信賴協定是區塊鏈的運作基礎，它最根本的優勢是開放的原始碼[18]。華特・艾薩克森(Walter Isaason)在「區塊鏈革命」一書的書評中，指出網路世界一直以來都欠缺一片最關鍵的拼圖，那就是用來認定必驗證交易有效的「信賴協定」，而區塊鏈科技恰好補上了最關鍵的這個部分，這是一個革命性的概念。

區塊鏈技術的最大特性之一，就是不可變更，任何記錄都會永遠留存，而且擁有四大構成要素[19]：共享帳簿、安全隱私、共識及智能合約。區塊鏈並非單一創新技術，而是集合眾多跨領域技術，包括密碼學、數學、演算法與經濟模型，並結合點對點網路關係，利用數學基礎建立信任，成為一個不需基於彼此信任、也不需仰賴單一中心化機構就能夠運作的分散式系統[20]。

區塊鏈的關鍵核心技術，包括用 Hashcash 演算法來進行工作量證明，且交易過程採用橢圓曲線數位簽章演算法來確保交易安全，並在每筆交易與每個區塊中使用多次 Hash 函數以及 Merkle Tree，同時也使用時間戳來確保區塊序列。其關鍵技術有以下五項:

1. 採用工作量證明達到去中心化及公正性。
2. 每筆交易採橢圓曲線數位簽章演算法加密。
3. Hashcash 演算法及多種 Hash 函數確保資料不被竄改。
4. 經由 Merkle Tree 將大量訊息縮短成一個 Hash 值。
5. 用時間戳伺服器（Timestamp Server）確保區塊序列。

2.2.2 區塊鏈技術發展

Nakamoto 在 2009 年 1 月開創了第一批比特幣，隨之而來的是加密貨幣時代的誕生。比特幣的普眾化在 2011 年開始迅速增長，很快地，技術專家意識到區塊鏈可以用來追蹤除了錢之外的其他事物。2013 年，Vitalik Buterin 提出了 Ethereum(以太坊)，它不僅會記錄貨幣交易，還會記錄被稱為智能合約的計算機程序的狀態，可以將交易發送到其嵌入的區塊鏈。Ethereum 於 2015 年推出，現在已成為眾多競爭對手和模仿者用來實現新一代應用程式的先驅。

換言之，區塊鏈技術的演進，從一開始的數位貨幣到後期的共同協作平台，可分為三個階段[16]：

1. 前期-數位貨幣(Digital currency)

   區塊鏈最早的應用於 2009 年的比特幣，其基礎建立在節點彼此不信任上。

2. 中期-協定(Consensus)

   在 2014 年之後，區塊鏈因為其 P2P 的特性，被延伸應用於多樣資產的移轉上面，即智能合約。

3. 未來-整合的共同協作平台

   區塊鏈開放 API，不侷限於金融行業的應用，將會成為眾多平台的平台。

2.2.3 區塊鏈技術效益

SAP 指出執行區塊鏈技術可以獲致以下之效益[21]:

1. 去中心化

   以太坊 (Ethereum) 是真正的對等式網路，可降低對於某些第三方中介者的依賴，像是銀行、律師和經紀人。

2. 加速流程

   區塊鏈可以加快多方交易流程中的執行速度，不受辦公時間的限制。

3. 透明度

   所有參與者都可以查看區塊鏈中的訊息，但不能竄改訊息。這有助於減少風險和欺詐，並建立信任。

4. 投資報酬率

分散式帳本將協助企業打造更精簡、更高效率且具盈利能力的流程，讓業者快速獲得投資回報。

5. 安全性

基於分散式和加密的特性，區塊鏈很難受到非法攻擊。因此，該技術能夠保障業務和物聯網的安全。

6. 自動化

區塊鏈具可編寫程式的特點。透過程式設定，在滿足條件的情況下，區塊鏈技術可以自動觸發合約並執行。

2.2.4 區塊鏈技術未來展望

有關於區塊鏈技術的未來發展，報導相當多，包括瑞士信貸、Gartener、資誠會計師事務所及阿里巴巴集團等均發布相關的訊息。其中瑞士信貸在一份有關數位貨幣和區塊鏈的報告[22]，將區塊鏈技術的發展分成七個階段，包括理念形成、概念驗證、雛型、試驗、生產並行和生產，如圖 2-11。目前區塊鏈技術發展是在整個時間軸上的半山腰，即是從第三的雛型階段到第四試驗階段的過渡期。區塊鏈技術真正能夠進入主流市場，且完全成為人類生活的一部分，仍然需要等待到 2025 年才能夠達成。不過，瑞信卻認為 2018 年將是區塊鏈技術發展關鍵性的一年。

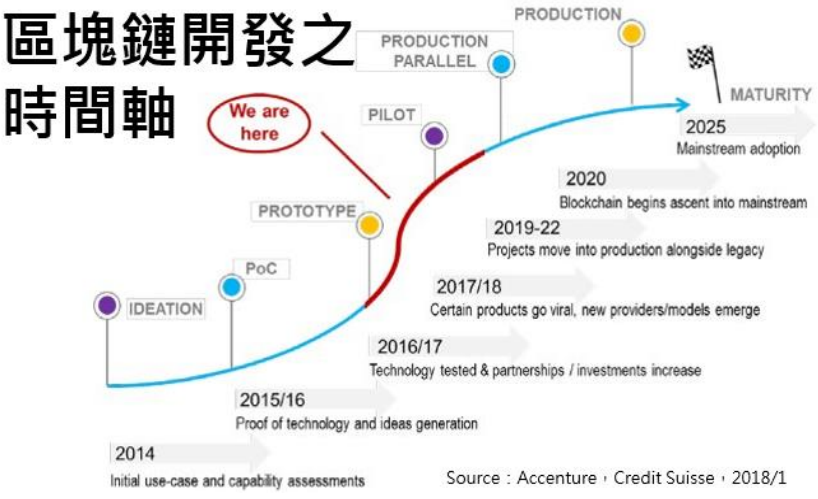

圖 2-11　區塊鏈開發之時間軸

資料來源:科技產業資訊室，源自 Accenture,Credit Suisse 2018/1

2.2.5 區塊鏈技術之風險與挑戰

區塊鏈技術之應用與發展，為全球金融產業帶來變革與機會，藉由技術創新應用，不但提高金融服務之效率，而且擴增金融商品與服務的面向，以及強化客戶依賴度；但無可諱言，亦衍生若干潛在風險[23]。

依據 ESMA、歐洲清算銀行 (Euroclear)及摩根史坦利 (Morgan Stanley) 等國際機構研究報告，歸納區塊鏈技術發展所帶來之風險如下：

1. 網路風險：區塊鏈技術仍有被破解或公(私)鑰遭竊取之風險，惡意駭客如有能力掌控區塊鏈交易，可能用於詐欺與洗錢等犯罪行為。
2. 作業風險：區塊鏈智能合約的應用，如有些微錯誤，將有可能影響市場，陷入極端的作業風險。
3. 市場風險：在分散式帳本及智能合約的應用下，可能會導致市場發生羊群行為(Herding Behavior)，增加市場的不確定性。
4. 壟斷風險：區塊鏈若採認許式網路架構，如訂定過度嚴苛的參加制度，則易產生壟斷之虞慮。
5. 監管風險：區塊鏈之監管模式，顯與傳統「中心式」支付系統不同，將挑戰監理機關跨領域監管議題。
6. 其他風險：金融機構若要將現行業務轉換成區塊鏈系統，將增加系統環境移轉之風險。

此外，區塊鏈技術尚存在兩道陰影[24]：

1. 比特幣在驗證身分時用到密碼學中的公鑰和私鑰,但並未意味它是堅不可摧。比特幣存在 51%攻擊，意思是只要掌握世界上一半以上礦機的運算能力，就可以篡改紀錄。例如，主鏈已經往一個地方成長，但只要算得更快，新增區塊的速度贏過主鏈，就可以讓大家把原本的區塊丟掉，長出新鏈，因此原有交易就會被竄改，也違反了信賴協定。
2. 量子電腦也是隱憂。成熟的量子電腦估計十年後有機會出現，屆時比特幣、以太坊用來做數位簽章的橢圓曲線密碼系統都會被攻破。現在已有少數新的虛擬貨幣採用可抵擋量子電腦的數位簽章，比特幣之後也可能用分叉改良機制。

而金融產業應用區塊鏈時，可能面臨以下挑戰[16]：

1. 大眾認可:對一般無相關知識的大眾而言，要理解並認同此一新興技術是相對有挑戰的。
2. 法規制定:新興技術往往對現有法規產生挑戰，相關的約束和現有法條的編修勢必得有所因應。

在「區塊鏈革命」一書中[18]，Don Tapscott 也提到區塊鏈技術將面臨以下十大推行面挑戰：

1. 技術尚未完備，未能廣泛運用。
2. 能源耗用量過大。
3. 政府阻礙或曲解。
4. 舊典範的強大者將掠奪最大的利益。
5. 誘因不足以吸引分散式大規模協作。
6. 區塊鏈會導致暫時性就業機會減少，但最終可導致就業機會漸增。
7. 協定的自理工作未定。
8. 分散的自主代理機制，其運作可能涉及法律問題。
9. 大公司及政府將致力於解開隱私，仍然在監視你。
10. 犯罪者將使用它。

2.3 智能合約

依據以太坊發明人維塔力克・布特林(Vitalic Buterin)的說法，智能合約是一個可以自動控制數位資產的電腦程式，可以把智能合約想像成一台由程式碼編寫，而且能自動運行的自動販賣機，投下多少錢，相對應的物品就會掉出。

在智能合約中，可將其資料公告在區塊鏈網路上，當需要交易時，便可觸發合約來執行，此時智能合約便會依照雙方的約定，按照規則完成交易，以下將對智能合約做逐步介紹。

2.3.1 智能合約簡介

「智能合約」一詞是由學者尼克·薩博（Nick Szabo）於 1994 年所提出[25]，將其定義為「藉由電腦化交易協定來執行合約」，倡議可以將交易的條款透過電腦化來落實，但是當時並沒有得到太多的迴響。這些年來，隨著區塊鏈技術的興起，智能合約才逐漸在金融業發展開來。

以下就智能合約的概念與實務推演，作一簡單介紹：

1994 N.Szabo 發表“Smart Contracts”，提出智能合約的構思。智能合約是執行合約條款的計算機化交易協議。智能合約設計的總體目標是滿足常見的合約條件（如支付條款、機密性，甚至強制執行），避免惡意和意外的異常，並儘量減少對仲介的需求。目前存在的一些技術可被視為原始智能合約，例如 POS 系統和電子數據交換(EDI)等。

1996 N.Szabo 於 Extropy 雜誌，發表“Smart Contracts: Building Blocks for Digital Markets”(智能合約：數字市場的基石)[26]，預言數位革命將徹底改變人類簽訂合同的方式，因為計算機科學家和密碼學家發現了許多新的，頗有意思的演算法，結合這些消息和演算法使得各種各樣的新協議成為可能。他提出的願景，相當於數年前的數位時代，非常準確，儘管當時被許多人質疑，但現在沒有人能否認它已成為事實。

1997 N.Szabo 發表“The Idea of Smart Contracts”[27]，強調智能合約為理想的安全(ideal security)提供了藍圖，闡述智能合約超越了自動販賣機，將合同嵌入各種有價值且受數字化控制的財產，以一種動態的，通常以主動的形式執行財產的轉移，並在積極措施不足的情況下，提供更好的觀察和驗證。

1998 N.Szabo 設計了一種分散式數字貨幣的機制，他稱之為“比特黃金”(Bit Gold)，儘管此數位金幣從未實現，但被稱為“比特幣架構的直接先驅” (a direct precursor to the Bitcoin architecture).。

2008 中本聰提出區塊鏈構思。儘管 1991 年 Stuart Haber 和 W. Scott Stornetta 等先驅者已著手在密碼安全鏈塊上研究，並在 2000 年後繼續進行，但第一塊區塊鏈是由中本聰在 2008 年所構思，後來被實現為比特幣的核心組成部分。

2009 中本聰創立的比特幣可視為數字貨幣演變的關鍵時刻。它是革命性的，因為它是第一個分散的加密貨幣，比特幣對世界最重要的貢獻是它帶來了區塊鏈和智能合約等主流概念。智能合約是一組可執行代碼，運行在區塊鏈之上，便於執行不受信任方之間的協議，而不需要可信任的第三方。

2015 Vitalic Buterin 等推出以太坊區塊鏈平臺。隨著以太坊平台以及 Solidity 和 Serpent 等編程語言的發佈，智能合約技術隨之蓬勃發展，因為這些編程語言使得合約的建構和部署變得更加簡單。

智能合約是電腦化的交易協定機制，可以用來執行某些合約的內容。智能合約的設計概念，通常是建立在滿足一般的合約內容：比方說是付款條件、資產抵押、保密約定和強制執行條款；並盡可能降低例外狀況的發生

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；因此，不同的區塊鏈平台所提供的智能合約，多少會有些差異。但一般說來，智能合約的運作，多半是以「事件驅動」的方式進行[28]。

區塊鏈平臺提供多方可信任的網路共享資料庫，智能合約程式一旦部署到區塊鏈平臺後，當合約所設定的事件發生時，就會觸發合約的指定功能，開始執行程式，執行的結果，通常會引發資產的移轉。

2.3.2 以太坊 (Ethereum) 簡介

以太坊的構想源自於 2013 年，當時才 19 的俄羅斯裔加拿大人維塔力克·布特林(Vitalic Buterin)。他當時跟比特幣的核心開發者爭論，區塊鏈網路架構需要有更穩固的手稿語言(scripting language)，才能發展其他應用軟體，不過他的想法沒被採納，促成他打定主意，要開發一套符合自己理念的區塊鏈網路架構。共識系統公司可說是他所跨出的第一步，在以太坊區塊鏈上推出應用軟體。

以太坊區塊鏈平臺於 2015 年推出，其白皮書名為「A Next-Generation Smart Contract and Decentralized Application Platform」[29]，強調智能合約為其平臺特色，更將智能合約推到一個新層次，讓大家注意到其重要性，甚至視其為「區塊鏈 2.0」的主要技術與應用。以太坊是一個嵌入了圖靈完整(Turing-complete)編程語言的區塊鏈。

以太坊是一個分散式平台，可以運行智能合約：應用上完全按照既訂程式運行，沒有停機、審查、詐欺或第三方干擾的可能性[30]。

以太坊上面提供各種模組讓用戶來搭建應用，因此在以太坊上建立應用程式的成本和速度都大幅改善。

以太坊是一個：「以區塊鏈技術為基礎的，任意形狀的(arbitrary-state)、具有圖靈完備性的(Turing-complete)、使用手稿程式語言的平台(scripting platform)。」這個平台吸引 IBM、三星、瑞銀集團、微軟、中國汽車業巨人萬向集團，以及一大票舉世最聰穎的軟體開發者，它們全都認為以太坊可能是改變一切的「地球規模電腦」[18]。

2.3.3 智能合約之運作

智能合約之運作[31]可分為三個步驟：

1. 制訂智能合約：合約參與者利用程式語言，訂定協議條款，並以各自之私鑰簽署。
2. 與區塊鏈系統連結：區塊鏈各節點都會收到合約，進行驗證並達成共識機制。
3. 執行智能合約：當多數節點都通過驗證後，該合約協議就會被成功執行，並通知合約參與者。

2.3.4 智能合約之部署

智能合約部署於區塊鏈之流程如下[32]：寫好 solidity 程式碼(.sol)後，需要先將程式碼編譯(compile)成 EVM(Ethereum Virtual Machine)能讀懂的二進位 Contract ByteCode，才能部署到 Ethereum 的區塊鏈上執行。部署到區塊鏈上的合約會有一個和錢包地址（Address）一樣格式的合約地址（Contract Address）如圖 2-13。

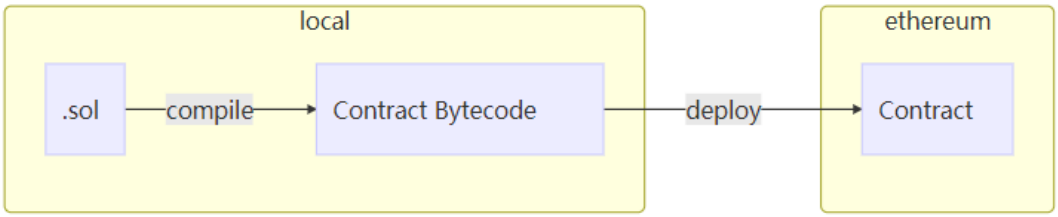

圖 2-13 智能合約之部署

智能合約部署完成後，可自動執行。後續呼叫智能合約時，使用者可以使用部署合約的錢包地址(Owner Account)，或依據撰寫的智能合約條件，讓其他錢包地址也能呼叫這個智能合約，如圖 2-14。

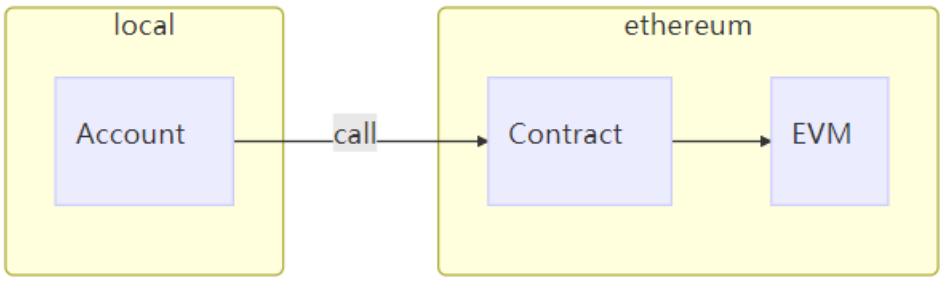

圖 2-14 智能合約之執行

2.3.5 區塊鏈與智能合約之應用

區塊鏈吸引了眾多行業的關注，從金融、醫療到公用事業、房地產和政府部門[33]。造成這種風潮的原因，乃因以前只能通過可信任仲介運作的模式，現在可以利用區塊鏈技術，以分散的方式運行，而不須再經由中央授權機構，意味著雙方之間的交易更加迅速。智能合約乃駐留在區塊鏈上的自我執行腳本，允許進行適當的、分散式的、高度自動化的工作流程。

儘管比特幣是區塊鏈第一個應用，但區塊鏈能做的遠大於此，包括：貨幣和數字資產，區塊鏈除了可將資金傳送給個人和商家外，也可以創建數字資產，如股票和債券等。

區塊鏈和智能合約可以創建任何數據、檔案或合約的可驗證記錄，這對於任何使用大數據的行業（如醫療行業或政府）都很有用，包含身分證、駕照等身分識別紀錄，以及專利、商標、著作權等無形資產，都能編碼成數位資產並在區塊鏈上登記，甚至就連汽車或房子這類的實體資產也能數位化。例如把住宅鑰匙、飯店房卡、汽車鑰匙換成密碼學中的私鑰，擁有私鑰的人才能打開車門。

區塊鏈與智能合約的應用範圍相當廣，各行各業都有可能。它既可以用來改善既有的業務流程，諸如:增加產能、降低成本與提高客戶滿意度；也可以用來支援發展新的業務模式，開發新的市場。

根據工研院高靖鈞等之研究[34]，區塊鏈發展至今，在智能合約的概念上有了長足的進步，已能發展出多樣化的應用，自 2009 年至今區塊鏈的演進如下圖 2-15 所示，目前區塊鏈較為活躍的國家則有：美國、日本、中國、俄羅斯、以色列….等。

圖 2-15 區塊鏈演進與應用

資料來源: MIC, 2016 年 7 月

第三章 研究方法

每個人在升學與求職時，都必須製作備審資料及個人履歷，來讓對方了解自己。如何證明自己的學經歷是真實的，就顯得十分重要。目前因缺乏統整性平台來記錄自己擁有的學習成績及學習表現，自行整理的經歷資料，別人也無法確認其真實性。

本研究應用區塊鏈技術，建立新的數位學習履歷系統，透過區塊鏈架設以太坊私有鏈，在 Moodle 平台上撰寫智能合約，將學生的修課與成績記錄於區塊鏈上。區塊鏈具有不可竄改之特性，校方得以透過此系統，紀錄學生的學習成績，確保其真實性及安全性；學生也能透過此系統完整地記錄下個人的學習履歷，使得學歷證明值得信賴。本研究範圍包括老師開課、學生選課、數位學習與學習成果等整個流程。

3.1 流程架構

本研究所提出之智能合約架構於區塊鏈上，透過區塊鏈實施開課、選課、數位學習與測驗的流程，相關人員物件角色如下:

1. 教師:在本論文我們將他定位為使用智能合約，將開課單及考試題目傳送至 moodle。
2. 學生:選課和受測驗的對象，會觸發智能合約，並將選課內容及考試成績,紀錄於 moodle。
3. moodle:收發教師與學生的合約內容，同步公告結果。
4. 智能合約:自動化處理腳本,被觸發後，系統會自動且確實執行。

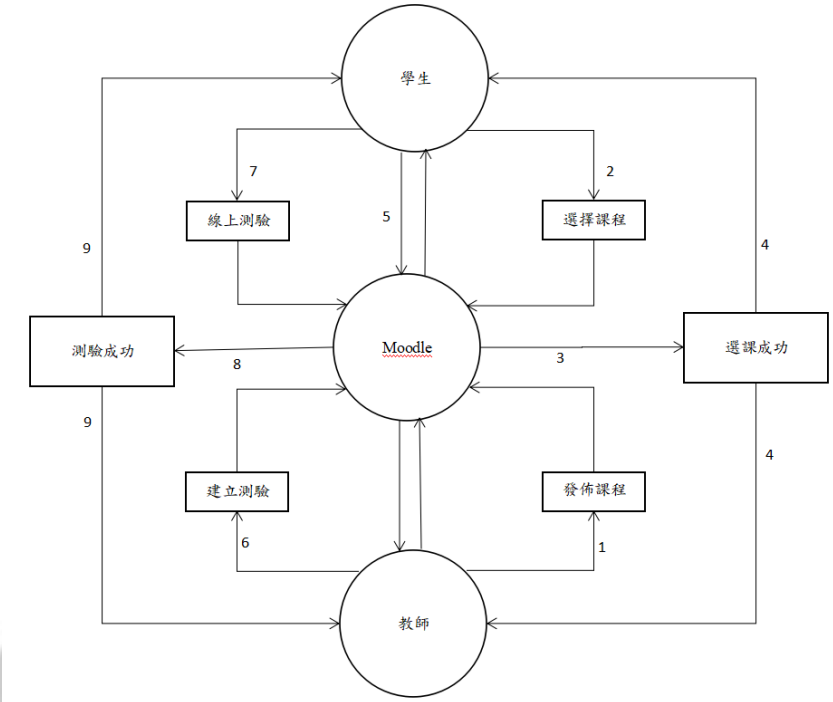

圖 3-1 開課、選課及測驗流程圖

圖 3-1 為現行教師與學生在發佈課程、選擇課程、數位學習及測試階段之整個流程。流程說明如下：

1. 教師發佈課程之資訊記載於智能合約上，moodle 隨即發出選課公告。
2. 學生向 moodle 提出選課請求。
3. moodle 判定選課成功與否。
4. 教師及學生上 moodle 查詢。
5. 學生進行數位學習。
6. 測試階段，首先由教師向 moodle 提供題庫，moodle 隨即發出考試公告 。
7. 學生向 moodle 提出參與考試申請，並進行線上測驗。
8. moodle 進行評分。
9. moodle 紀錄成績，老師及學生可上 moodle 查詢。

圖 3-2 為以區塊鏈與智能合約的概念，所導出的選課流程。

1. 教師發佈課程之資訊記載於智能合約上，moodle 隨即發出選課公告。
2. 學生向 moodle 提出選課請求。
3. 智能合約會向教師取得課程授權。
4. 教師同意，以及智能合約判定選課有效，則選課確立。
5. 智能合約將選課成功的訊息，傳送給學生。

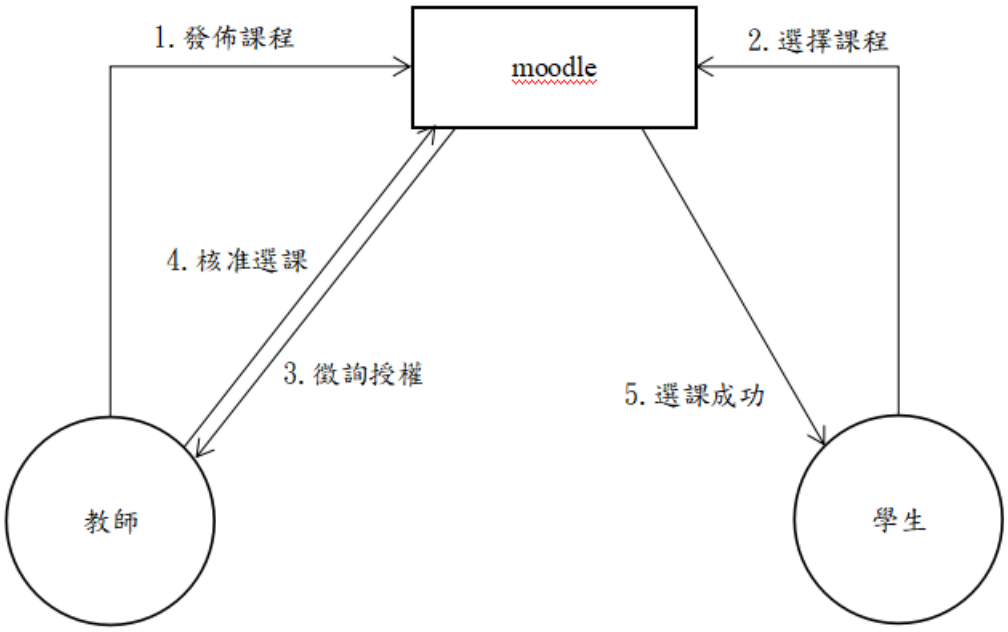

圖 3-2 選課流程圖

圖 3-3 為以區塊鏈與智能合約的概念，所導出的測驗流程。

1. 教師建立數位學習測驗題庫。
2. 學生選擇參與測驗。
3. 智能合約審核學生資格 。
4. 老師給予授權題目，學生進行作答。
5. 智能合約將測驗成績通知學生與老師。

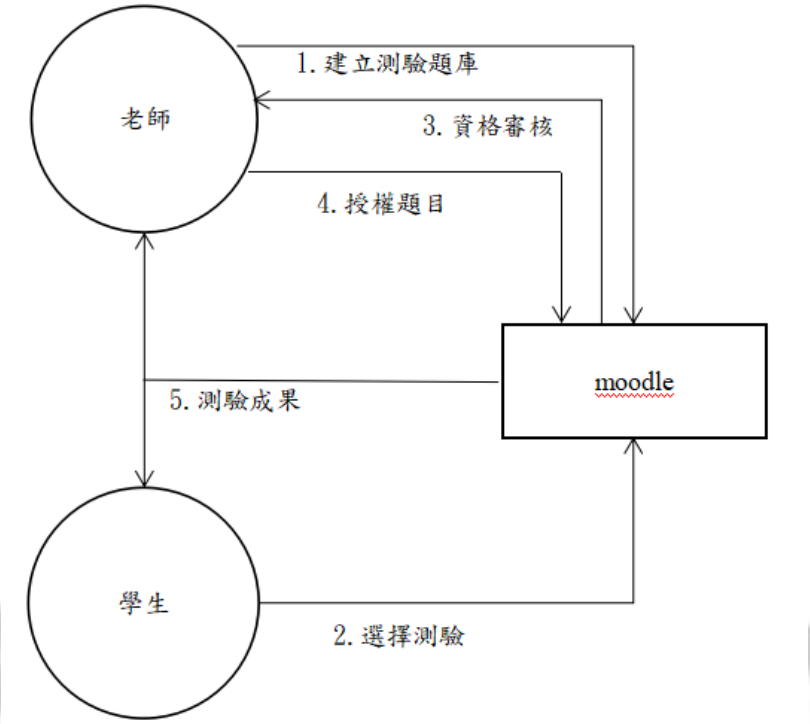

圖 3-3 測驗流程圖

本研究將著重於學生數位學習履歷之研究，透過區塊鏈架設以太坊私有鏈，在 Moodle 平台上撰寫智能合約，將學生的修課履歷與成績記錄於區塊鏈上。區塊鏈具有不可竄改之特性，校方得以透過此系統，紀錄學生的學習成績，確保其真實性及安全性；學生也能透過此系統完整地記錄下個人的學習履歷，使得學歷證明值得信賴。圖 3-4 說明應用區塊鏈與智能合約在數位學習履歷之研究流程[11]。

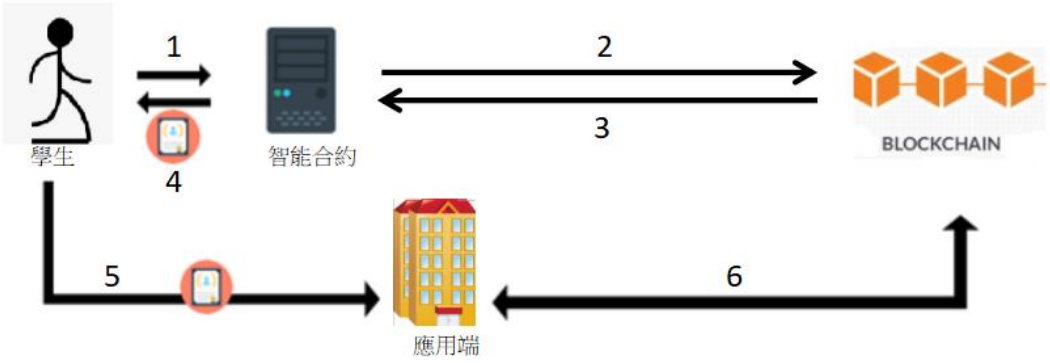

圖 3-4 區塊鏈的數位學習履歷模型

1. 學生向學校的資訊系統(Moodle)啟動數位學習申請。
2. 確認該學生符合數位學習資格後，系統將學生數位學習相關資料記錄，以安全哈希值（Hash）方式記錄於區塊鏈上。
3. 同時取得此筆記錄在區塊鏈上的交易序號。
4. 區塊鏈上記錄著該生的學習資料，諸如課程別、何時上線學習、每次學習多長、學習頻率、何時接受測驗以及測驗結果等。
5. 學生可利用此電子化學習履歷紀錄傳輸到目標場所(應用端)，如企業、學校或政府機關等。
6. 該目標場所可以依據其交易序號 到區塊鏈上查詢此紀錄。

3.2 研究資源

本研究所發展出來的智能合約乃架構於以太坊虛擬機器(Ethereum Virtual Machine，EVM)。以太坊虛擬機器是一個針對智能合約的應用，在以太坊上的運行環境。它可以完全地獨立運行，亦即在 EVM 中運行的程式碼不會受到外部網路或是其他系統的干預影響。

智能合約可以透過數種不同的程式語言進行撰寫,在本研究中，我們使用的是“Solidity”，因為它是以太坊官方推薦撰寫智能合約的程式語言，也是目前所有可撰寫智能合約的程式語言當中，最多人選擇，也最受歡迎的一種。

Solidity 是一個合約導向的高階程式語言，其語法類似於 JavaScript，並且是針對於以太坊虛擬機器(EVM)進行設計，至於編譯器，則使用“Solc”編譯器，是 Solidity 的命令行編譯器(solidity command line compiler)。

智能合約程式，必須被部署 (deploy) 到區塊鏈上。下圖 3-5 為台北以太坊社群所作之範例[35]，以太坊 VM 會運行在每一個以太坊節點上面，一旦合約部署成功時，會得到一個地址，它就像記憶體位置一樣，取得這個位置後，搭配正確的介面資訊，就可以執行這個合約，在區塊鏈上所有人都可以呼叫這個智能合約所開出來的函式(function)。而區塊鏈 VM 上運作的程式（也就是智能合約）跟一般 VM 上運作的程式，最不一樣的地方就在於去中心化架構。

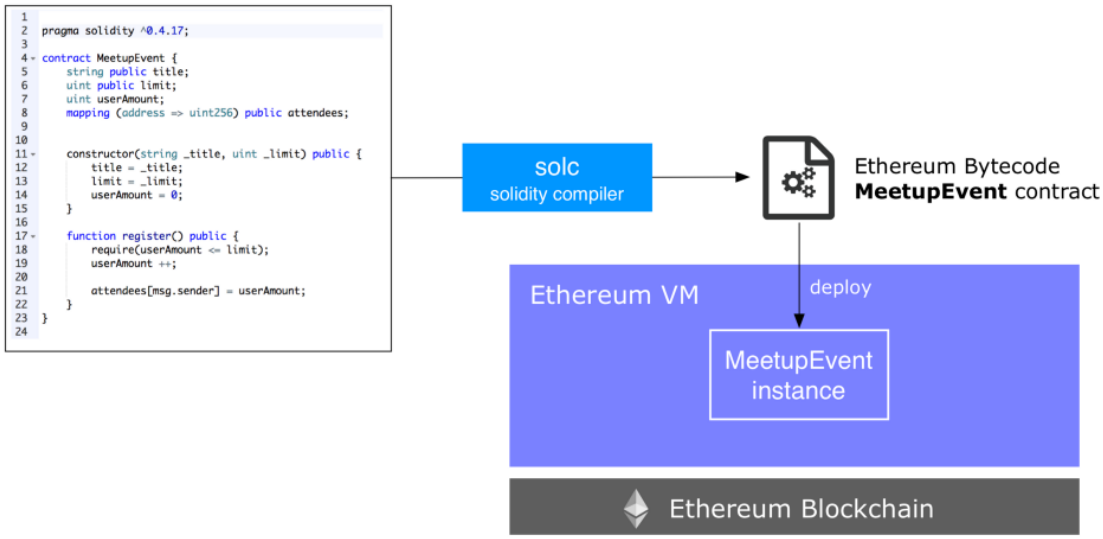

圖 3-5 智能合約佈署

資料來源: https://medium.com/taipei-ethereum-meetup/

第四章 研究結果

我們將探討研究過程及結果。第一部分介紹以太坊私有鏈的架設，第二部分介紹在 moodle 平台中如何導入智能合約，將教師開課、學生學習之課程資訊與學習成果寫入區塊鏈中。

4.1 建立區塊鏈

本研究透過 Google Cloud Computing(GCP)來架設私有鍊，我們採用兩台主機 Ubuntu 16.04LTS 來架設，它們都需要 Go Ethereum(geth)和 Node JS 等軟體，另外還需要利用 Solidity 來撰寫智能合約。雖然兩個 Node 端皆為 Ubuntu 環境，但執行的參數不一樣，它們之間分別為 gcp.tar.gz 和 ubu.tar.gz 二個壓縮檔，而這兩個壓縮檔分別對應其所在的平台。

我們將 Ubuntu 以 ssh 方式連上 GCP 後，下載軟體，再進行解壓縮並且執行，執行步驟如下：

1. ssh -i ~/.ssh/my-ssh-key nato@104.199.148.177
2. curl -L https://drive.google.com/uc?id=1ZxK07f86f4ImSHRmfbF6RI-3pn50Bhsj -o gcp.tar.gz
3. tar zxf gcp.tar.gz
4. ./install

完成上述步驟，就可啟動第一台電腦作為 Node JS 的 Web Server，建立畫面如圖 4-1 和 4-2。當其它的 Nodes 以 HTTP 的方式來取得 ENode 的資訊後，就可以互相連接。

第二台 Ubuntu 執行步驟如下：

1. mkdir Eth; cd Eth
2. curl-Lhttps://drive.google.com/uc?id=1011zOutUzYNZyKyEt4KHDUHjmAI6EqiH -o ubu.tar.gz
3. tar zxf ubu.tar.gz
4. ./install

安裝的(軟體/元件)如下

```
sudo apt update && sudo apt -y upgrade && sudo apt -y install --upgrade git
wget https://gethstore.blob.core.windows.net/builds/geth-linux-amd64-1.7.3-4bb3c89d.tar.gz
tar zxf geth-linux-amd64-1.7.3-4bb3c89d.tar.gz
sudo cp geth-linux-amd64-1.7.3-4bb3c89d/geth /usr/local/bin/geth
wget https://nodejs.org/dist/v8.9.4/node-v8.9.4-linux-x64.tar.xz
tar xf node-v8.9.4-linux-x64.tar.xz
sudo rm -rf /usr/local/bin/node-v8.9.4-linux-x64
sudo mv node-v8.9.4-linux-x64 /usr/local/bin
echo 'export PATH=.:/usr/local/bin/node-v8.9.4-linux-x64/bin:$PATH' >>~/.bashrc
#
export PATH=.:/usr/local/bin/node-v8.9.4-linux-x64/bin:$PATH
. on
```

圖 4-1 安裝元件

```
andy@instance-1:~$ ./install
Hit:1 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-updates InRelease
Get:3 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Hit:4 http://archive.canonical.com/ubuntu xenial InRelease
Hit:5 http://security.ubuntu.com/ubuntu xenial-security InRelease
Fetched 102 kB in 0s (146 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.7.4-0ubuntu1.3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
--2018-02-03 14:11:53--  https://gethstore.blob.core.windows.net/builds/geth-linux-amd64-1.7.3-4bb3c89d.tar.gz
Resolving gethstore.blob.core.windows.net (gethstore.blob.core.windows.net)... 40.113.27.176
Connecting to gethstore.blob.core.windows.net (gethstore.blob.core.windows.net)|40.113.27.176|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10129861 (9.7M) [application/octet-stream]
Saving to: 'geth-linux-amd64-1.7.3-4bb3c89d.tar.gz.3'

geth-linux-amd64-1.7.3-4bb3c 100%[=========================================>]   9.66M  2.02MB/s    in 5.4s

2018-02-03 14:12:00 (1.77 MB/s) - 'geth-linux-amd64-1.7.3-4bb3c89d.tar.gz.3' saved [10129861/10129861]

--2018-02-03 14:12:00--  https://nodejs.org/dist/v8.9.4/node-v8.9.4-linux-x64.tar.xz
Resolving nodejs.org (nodejs.org)... 104.20.22.46, 104.20.23.46, 2400:cb00:2048:1::6814:162e, ...
Connecting to nodejs.org (nodejs.org)|104.20.22.46|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11410120 (11M) [application/x-xz]
Saving to: 'node-v8.9.4-linux-x64.tar.xz.3'

node-v8.9.4-linux-x64.tar.xz 100%[=========================================>]  10.88M  3.71MB/s    in 2.9s

2018-02-03 14:12:04 (3.71 MB/s) - 'node-v8.9.4-linux-x64.tar.xz.3' saved [11410120/11410120]

假設你已安裝 geth ^1.6.7，Node ^9.1, Mist ^0.92, 繼續否？(y/n)  y
-------------------------------------------------
安裝 nodeJS 所需 module
-------------------------------------------------
建立 geth 初始配置至 ~/.ethereum
-------------------------------------------------
建立初始 Account
-----------------------------------
```

圖 4-2 安裝過程畫面

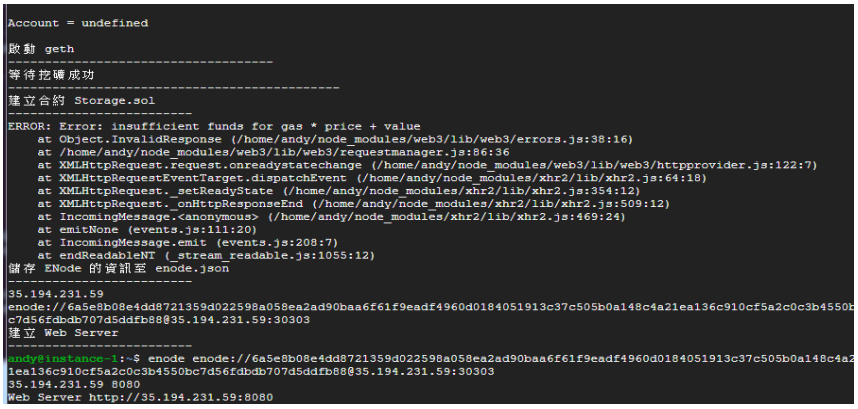

圖 4-3 安裝完成畫面

圖 4-4、4-5、4-6 是圖 4-2、4-3 安裝畫面之程式碼。

```
#!/bin/bash

function ag0() {
  geth init privchain_genesis.json 2>eth.log
}
function ag1() {
  geth --ipcpath "geth.ipc" --rpcaddr "0.0.0.0" --rpccorsdomain "*" --rpcapi "db,eth,net,personal,web3" --rpc --networkid 3982 "$@" 2>>eth.log
}
function mkNodeWeb {
  echo ------------------------------------------------
  echo 安裝 nodeJS 所需 module
  echo ------------------------------------------------
  rm -rf node_modules
  npm install > npmNode.log
  if [ "$?" != "0" ] ; then
    exit 1
  fi
  rm -rf public
  mkdir public
  cp HTML/* public/.
  ln -s $(pwd)/node_modules public/node_modules
  return 0
}

echo -n '假設你已安裝 geth ^1.6.7，Node ^9.1, Mist ^0.92, '
read -p "繼續否？(y/n)  " yesno
if [ $yesno == 'Y' ] || [ $yesno == 'y' ]; then
  mkNodeWeb
  if [ "$?" != "0" ] ; then
    exit 1
  fi
  echo '建立 geth 初始配置至 ~/.ethereum'
  echo ------------------------------------------------
  rm -rf ~/.ethereum
  rm -rf ~/ethash
  rm -rf ~/.config/Mist
  rm -f eth.log
  ag0
  echo 建立初始 Account
```

圖 4-4 區塊鏈程式碼

```
  echo ------------------------------------
  ag1 js account.js
  echo 啟動 geth
  echo ------------------------------------
  ag1 --mine &
  echo 等待挖礦成功
  echo ------------------------------------------------
  sleep 2
  echo 建立合約 Storage.sol
  echo --------------------------
  node Contract.js

  echo 儲存 ENode 的資訊至 enode.json
  echo --------------------------
  IPAddr=$(cat ipInfo.json | jq ".local_ip"|sed "s/\"//g")
  echo $IPAddr
  enode=$(fgrep "UDP listener up" eth.log | awk '{print $6}' | tail -n1 | sed "s/self=//g" | sed "s/\[::\]/${IPAddr}/g" - )
  echo $enode
  echo $enode > enode.dat
  echo 建立 Web Server
  echo --------------------------
  node webServer.js &
fi
```

圖 4-5 區塊鏈程式碼

```
#!/bin/bash

function ag0() {
  geth init privchain_genesis.json 2>eth.log
}
function ag1() {
  geth --ipcpath "geth.ipc" --rpcaddr "0.0.0.0" --rpccorsdomain "*" --rpcapi "db,eth,net,personal,web3" --rpc --networkid 3982 "$@" 2>>eth.log
}

echo
echo '刪除 geth & node'
echo --------------------------
. off
echo 啟動 geth(沒有挖礦)
echo --------------------------
ag1 &
echo 建立 Web Server
echo --------------------------
node webServer.js &
```

圖 4-6 區塊鏈程式碼

從挖礦開始到結束大約半分鐘，畫面如圖 4-3。出現的 Enode 與 Web Server 的 Enode 不同，是因為在不同的時間截圖之故，所以我們必須再由 Enode 後面的 IP 來確定是與 Web Server 相符的。

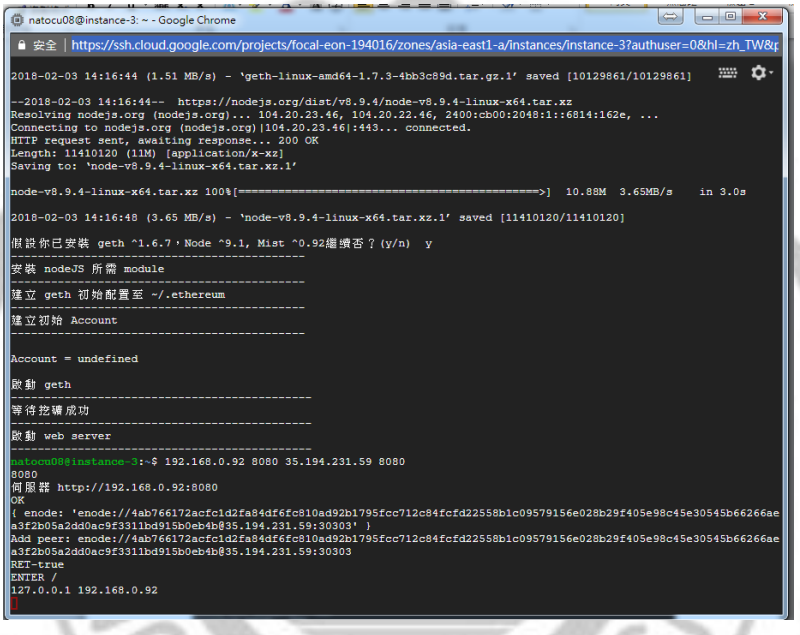

圖 4-7 Enode 連接成功

當進入 Ethereum 的 console 模式，得到畫面如圖 4-8，我們可以確認帳戶已建立成功，並且獲得交易貨幣。

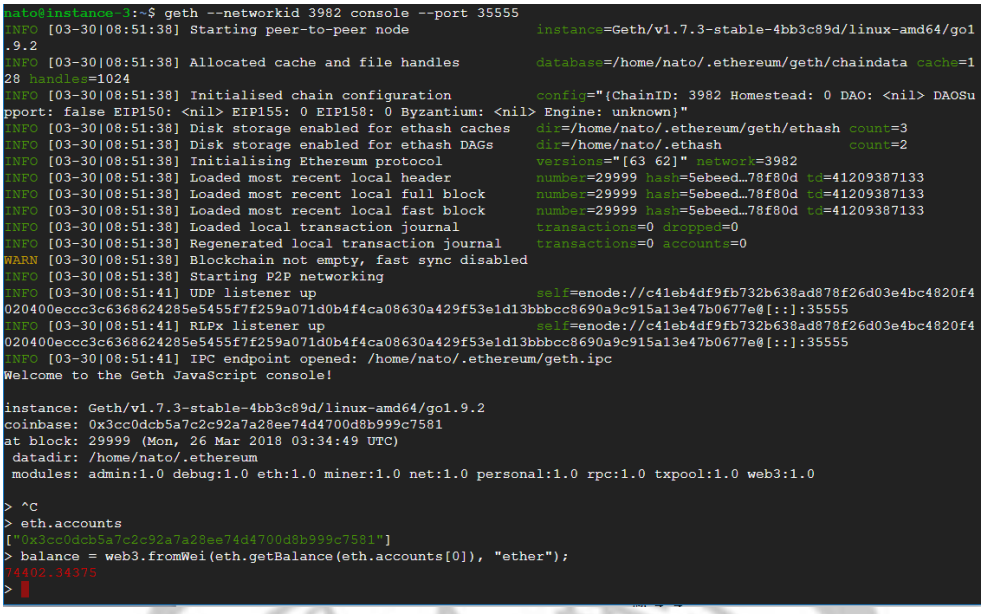

圖 4-8 Ethereum 的 console 模式

從瀏覽器進入 localhost，可讀取 Web Server 所建的合約。圖 4-9 是智能合約的顯示畫面。你可以更改這個合約 Storage 的 set 值，當上次誰設定的值改變成與預設 ACCOUNT 一致，且 Storage 的 get 值變為上一次的 set 值，證明這個合約執行成功，如圖 4-10。

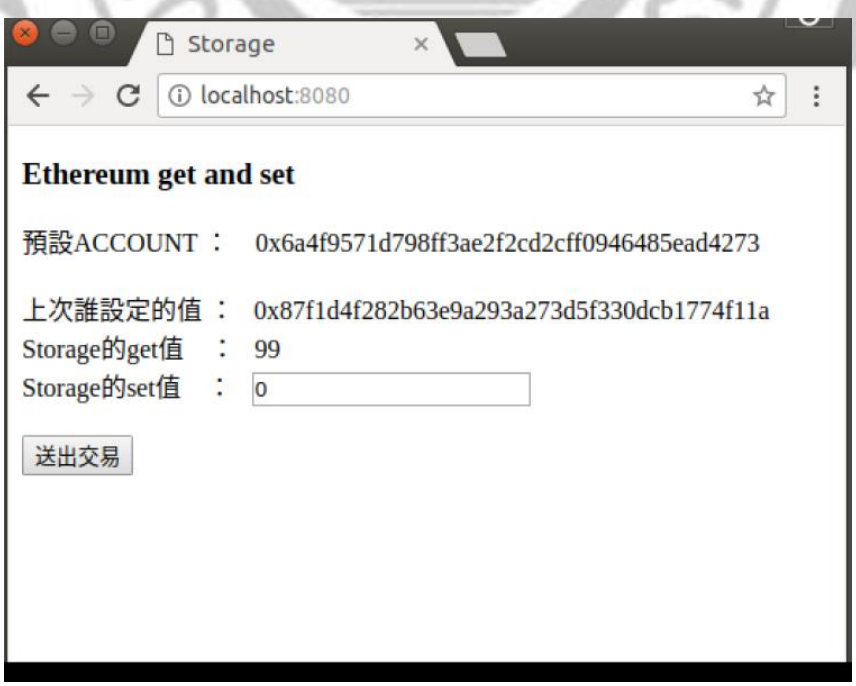

圖 4-9 智能合約測試畫面

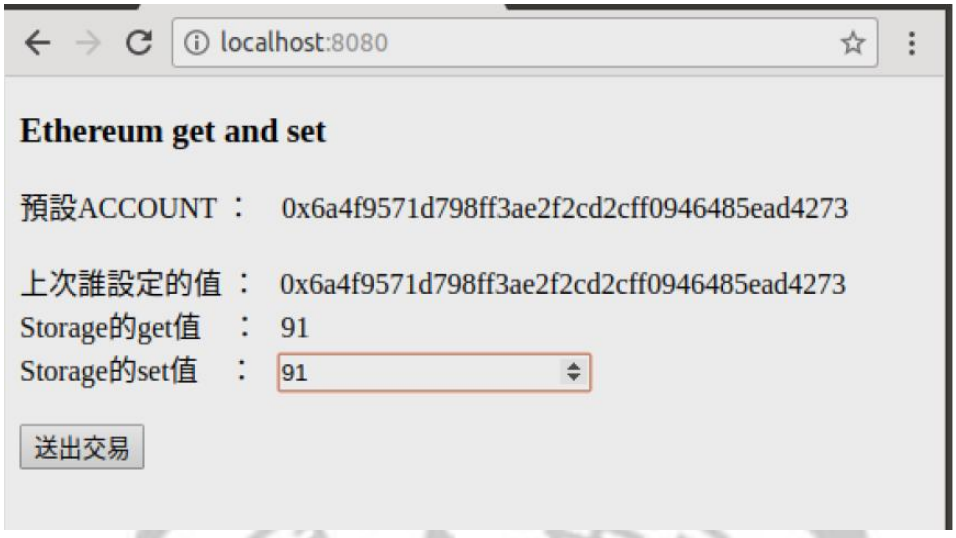

圖 4-10 智能合約測試成功

合約程式碼

```
// Simple Test of Contract
pragma solidity ^0.4.11;
contract Storage {
  event SetEvent(
    address indexed from,
    uint256 val
  );
  uint256 storedData=0;
  function set (uint256 data) public {
    if( storedData != 3982 ) {
      storedData = data;
      SetEvent(msg.sender, data);
    }
  }
  function get() public constant returns (uint256) {
    return storedData;
  }
}
```

圖 4-11 合約程式碼

4.2 平台設計

藉著將智能合約嵌入 moodle 平台(圖 4-12)，以有效記錄學習歷程與修課情況。本研究針對老師開課、學生接受測驗時所花時間、測驗成績、修課歷程及選課是否成功，進行探討。

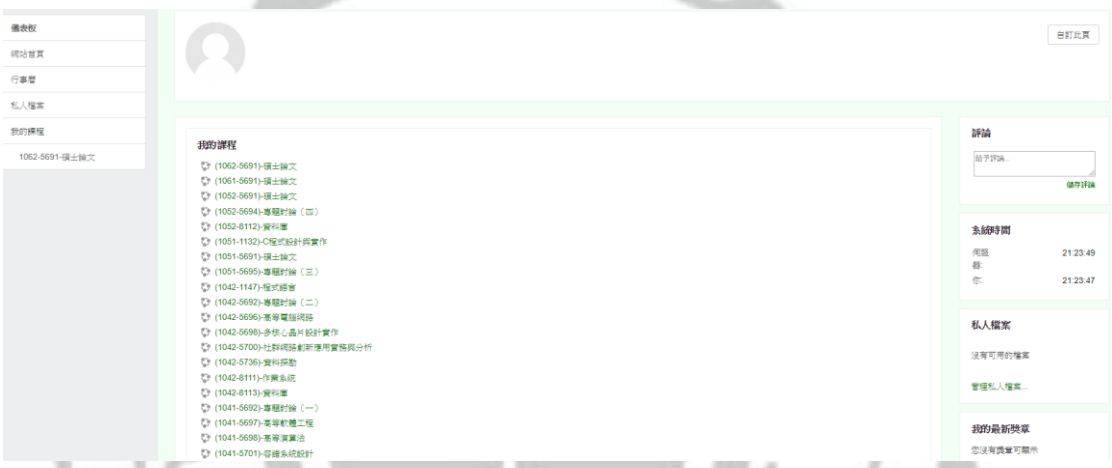

圖 4-12 moodle 平台畫面

4.2.1 教師開課建立於區塊鏈

當老師開課成立時，以智能合約紀錄 moodle 平台的開課資訊，並紀錄於區塊鏈上，紀錄的內容有，教師名字、課程名稱、課程版本，透過這些紀錄，利用區塊鏈的可追溯性，可以了解到課程目前的資訊，若有新課程推出時，也可知道課程的更新資訊。如圖 4-13。

圖 4-13 開課課程與教師資訊

4.2.2 智能合約紀錄測驗時間

設計此項功能的目的是為了評估學生對於課程的理解程度，老師可從學生的測驗時間長短，來判斷學生是否確實吸收課程內容，以針對個別學生做出調整。在這裡顯示的資訊有：學生資訊、科目代號、作答時間。在學生按下繳交，並顯示已繳交後，智能合約將資訊紀錄於區塊鏈上。圖 4-14 顯示上傳資訊。

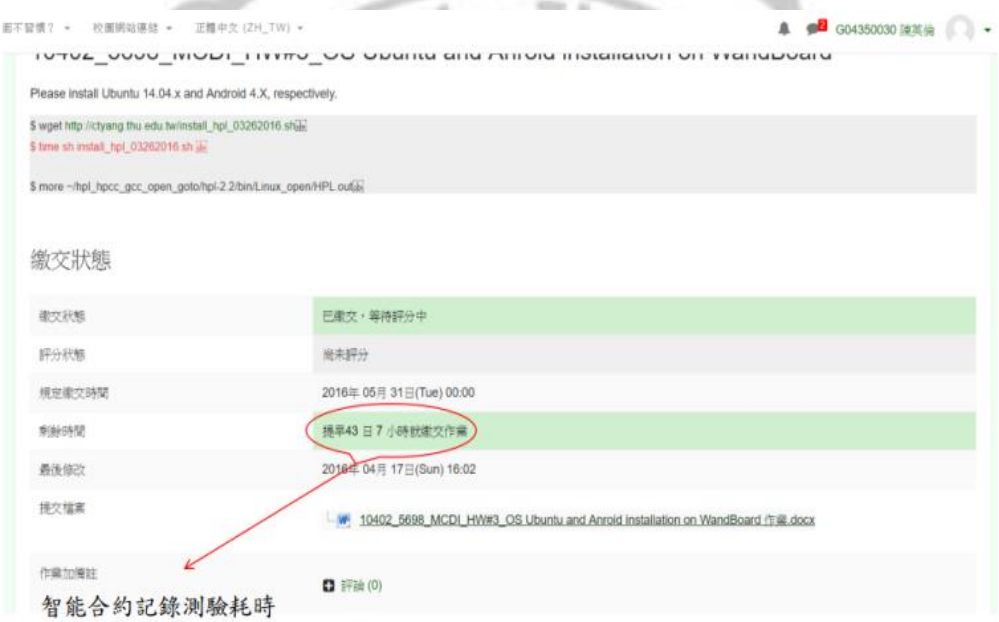

圖 4-14 測驗上傳時間畫面

4.2.3 智能合約紀錄成績

設計此項功能的目的，在於紀錄學生在課程上所獲得的最終評價。透過智能合約紀錄，未來學生需要過往學習歷程時，不用再至各大專院校申請，有效改善學習歷程取得的方便性，紀錄的資訊為：學生資訊、科目代號、科目分數等，如圖 4-15。

選取	用戶的相片	帳號 / 名字	狀態	成績	編修	最後修改的(作業)	提交檔案	作業加備註	最後修改的(得分)	評語回
		s000001 陳小明	已繳交，等待評分中已評分	成績 100.00 / 100.00	編修	2016 年 06 月 8 日 (Wed) 17:36	s000001.rar	評論 (0)	2016 年 06 月 21 日 (Tue) 00:16	
		s000002 張小華	已繳交，等待評分中已評分	成績 90.00 / 100.00	編修	2016 年 06 月 8 日 (Wed) 18:14	s000002.rar	評論 (0)	2016 年 06 月 21 日 (Tue) 00:33	

圖 4-15 個別學生課目成績畫面

4.2.4 智能合約紀錄已修課程

透過智能合約紀錄學生的數位學習歷程，學生未來需要進修更深層的科目時，將以智能合約判斷，該學生是否符合資格，讓學生了解課程間相互關係。紀錄資訊為：學生資訊、科目代號，如圖 4-16。

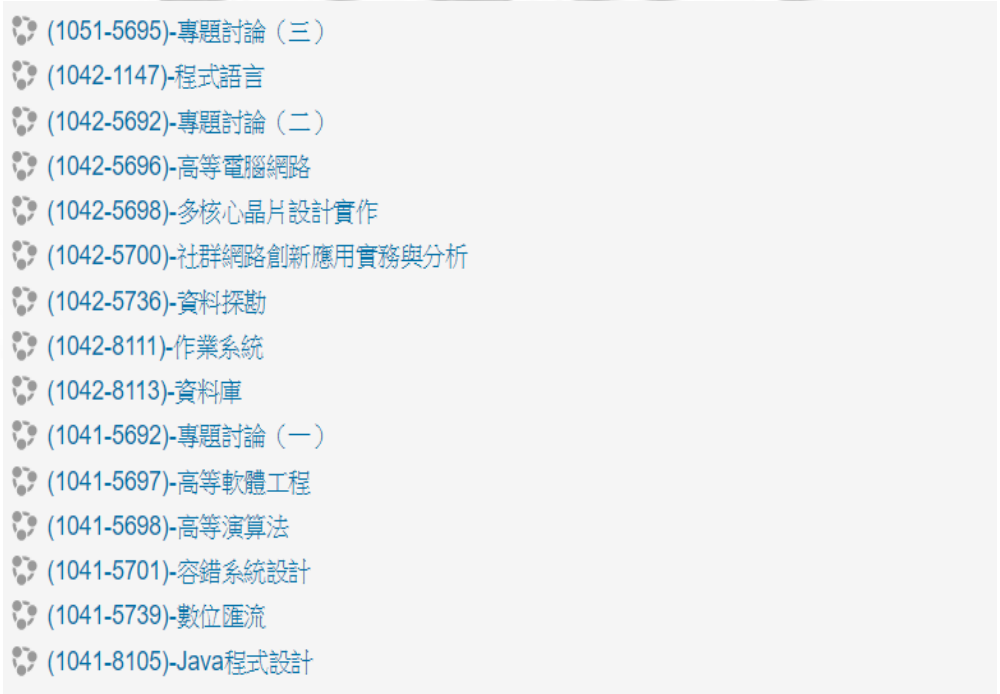

圖 4-16 紀錄已修之課程表

4.2.5 記錄學生學習總時數

目前線上線學習的時間模組，僅顯示學生在學習平台上的停留時間，無法反映學生真實的學習表現。老師評分時，應參考學生在討論區發表、作業、測驗上的表現。透過智能合約紀錄學生學習課程的時數，再結合學生在討論區發表、作業、測驗上的表現，方便教師了解學生的學習狀況，來評估學生是否在學習過程遇到困難，方便教師針對個別學生做出調整。紀錄資訊為：學生資訊、科目代號、學習時間，如圖4-17。

就可以看到所有選課學生使用在課程的的時數統計

學習時數統計

名稱	上線學習時間小計	離線學習時間小計	全部時間
2	09:27:24	00:00:00	09:27:24
2	04:00:21	00:00:00	04:00:21
2	05:24:16	00:00:00	05:24:16
2	01:31:43	00:00:00	01:31:43
2	02:33:48	00:00:00	02:33:48
2	03:23:39	00:00:00	03:23:39
2	24:07:27	00:00:00	24:07:27
2	15:14:47	00:00:00	15:14:47
2	09:36:40	00:00:00	09:36:40

圖 4-17 學生修課時數統計

4.2.6 擬繼續探討之課題:以智能合約進行選課判定

在選課方面，我們將以智能合約來判定學生是否擁有修習課程資格，若學生未通過先修課程，則無法修習後續的進度，來提升選課效率。其構想如圖 4-18。

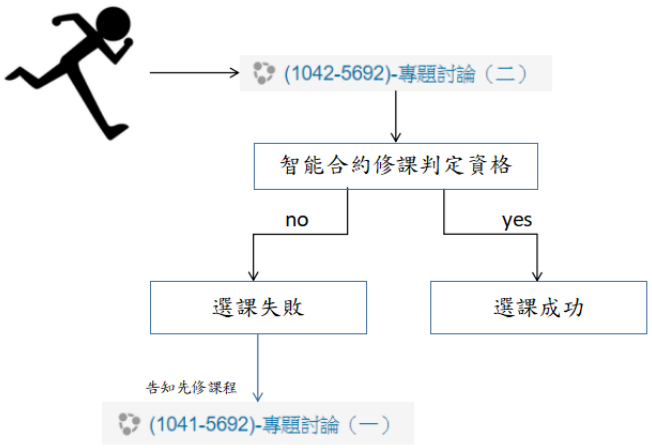

圖 4-18 選課判定流程圖

目前學生選課時，常會出現兩個問題：首先是選完課後，需等候兩三天才確知選課成功與否；還有系辦公室常會貼出公告，希望學生若未完成先修課程時，不要再選修後續課程。如果將選課的要求寫入區塊鏈，則選課效率可以提升，也不再有未通過先修課程而需退選的問題，因為在智能合約已做了判定。

在經過本研究的努力後，將區塊鏈技術結合至 moodle 平台，提供數位學習平台學習成果的佐證。首先針對教師的部分，當老師進行課程發布後正式開課，將透過智能合約將課程內容與設定寫入區塊鏈紀錄，保留該學期課程開課的原始資訊。在學生的部分，當學生修課完成並通過測驗取得學分時，其修課資訊與狀態也將如實記錄在區塊鏈上，包含課程名稱、版本、修課起訖時間、學習頻率、學習次數與通過成績等資訊。透過區塊鏈不可偽造、不可竄改等特性，建立信賴網路，提供學生升學與求職時的佐證資訊。

第五章結論與建議

本研究乃利用區塊鏈技術，試圖在以太坊上建置智能合約，用以紀錄目前學生的數位學習履歷及其成效。在研究模型中，我們討論教師開課、學生選課、數位學習以及學生測驗之完整流程，由於時間限制，我們僅完成教師開課和學生數位學習部分。若能繼續完成學生選課部分，則學生從選課到接受測驗，整個流程都會有詳實、不可竄改的紀錄。這個紀錄將成為學生的學習履歷表，裡面有學習的課程與成績，若再連結畢業證書系統，則學生畢業以後，可直接利用區塊鏈裡的資料求職，或繼續求學，不必再回學校申請畢業證書。

區塊鏈技術並不是解決世上所有經濟與金融問題的萬靈丹，創造繁榮的不是技術，而是人。在應用區塊鏈技術方面，有必須克服的障礙和可能帶來的機會，因此採用區塊鏈技術應用在任何領域上都需要嚴謹的設計與規劃。

在官網資料都可能已經過時的區塊鏈產業，一個能聚集大家並單純交流知識的社群尤其重要；不少人都是先加入以太坊社群，才慢慢進入區塊鏈產業工作。參與者一定要親自做，才能夠看得仔細，但不能只是自己做，一定還要看別人怎麼做，因為這技術發展太快。另外，區塊鏈知識既多且散，沒有系統性教法，一個困惑許久的問題，可能在社群聚會時，直接請教先進就可迎刃而解。因此，先社群後產業，或許可以讓區塊鏈這條路走得更平順。

政府於「挑戰 2008－國家發展重點計畫」中，指出推動數位學習的相關政策，期望建構全民數位學習環境和培育數位人才。

目前校園的數位學習環境，以下幾點值得進一步思考：

1. 持續改善校園網路環境，加強軟硬體設備，充實數位教學內容以及鼓勵數位學習。由文獻探討中，我們得知 2015 年台灣數位學習產業雖呈現成長的趨勢，但數位教材與平台/工具之成長較往年趨緩，探究其原因，與各級學校採購預算減少有關。工欲善其事，必先利其器，若要增強數位學習的成效，各級教育機構預算的提高是必要的。另外，不管數位學習技術如何演進，終究不能脫離學習認知理論，須從滿足使用者（學生）的需求角度來思考，來設計適性化的課程。
2. 善用大數據分析，學校、老師乃至於家長都能藉量化數據獲得具體的資訊，了解個別學生的學習需求與困難，給予每個學生不同的指導。

儘管利用區塊鏈技術，在以太坊上建置智能合約，用以紀錄目前學生的數位學習履歷及其成效，對學生、學校、教育機構、政府機關以及企業界都有正面效益，但目前因區塊練技術未臻完備，未能廣泛運用；以及誘因不足，難以吸引眾多大專院校採行。且需花費龐大的人力、物力與時間，實務上遇到的困難，仍有待相關單位協同解決。本研究建議教育機構及企業界先參與開放徽章機制，循序漸進，等時機成熟，再擴展至嵌入區塊鏈之應用，如以下兩點所述：

1. 目前在國內仍然沒有任何機構參與開放徽章機制，以致於以往的學習履歷與能力，外界無法得知與認同，一旦有了開放徽章機制，就可以打破這個限制，讓數位徽章 (Digital badge)成為具有說服力、高信賴度的連網認證。政府單位應該要正視這個問題，鼓勵並要求教育及訓練機構及企業積極參與，以善用人力資源。
2. 開放徽章試行成功後，再著手將開放徽章嵌入區塊鏈。由於區塊鏈具有可追溯性、不可竄改、時間戳與加密等特性，使得認證可信度大幅提升。

參考文獻

[1] 謝雅青，民 95，失業勞工數位學習成效評估之研究—以輔助參加提升數位能力研習計畫者為對象，國立政治大學勞工研究所碩士論文。

[2] Will Erstad. Online vs. Traditional Education: What You Need to Know. (available online at http://www.rasmussen.edu).

[3] 彭成翰，民 92，企業導入數位學習績效評量模式建構之研究，東海大學企業管理學系碩士論文。

[4] Moodle. (available at https://moodle.org).

[5] TechTerms,Moodle Definition (available online at https:// techterms.com).

[6] About Open Badges (available online at https://openbadges.org/about).

[7] Open Badges.Discover Open Badges (available online at https://openbadges.org/).

[8] Serge Ravet. (2016) from blockchain to badgechain (available online at https://medium.com/badge-chain/from-blockchain-to-badgechain).

[9] Kerri Lemoie. Innovations in Open Badges & Blockchain.(available online at https//:badgechain.com/innovations-in-open-badges-blockchain).

[10] Open BlockChain. RESEARCHING THE POTENTIAL OF BLOCKCHAINS. (available online at http://blockchain.open.ac.uk/).

[11] 經濟部工業局，104 年度專案計畫數位學習產值調查報告。

[12] Global Market Insights,.E Learning Market Size, Trends-Industry Forcast Report 2017-2024. (available online at https://gminsights.com).

[13] Anderson, T. *Theory and Practice of Online Learning* (2nd ed.), AU Press, Athabasca University, 2011.

[14] 什麼是「區塊鏈」？商周 2016.12.09 (available at https://www.businessweekly.com.tw/article.aspx).

[15] S. Nakamoto (2008). Bitcoin: A Peer to Peer Electronic Cash System. (available online at https//bitcoin.org/bitcoin.pdf).

[16] 台大金融科技區塊鏈，(available online at http://www.fintech.csie.ntu.edu.tw. 2016/03/22).

[17] 陳恭，區塊鏈革命迎向產業新契機 2017/09/27，(available online at http:// www.ftrc.ccu.edu.tw).

[18] 陳以禮、 李芳齡譯，Don Tapscott & Alex Tapscott 著，2017，區塊鏈革命，台北，遠見天下文化出版股份有限公司。

[19] Niti Guar，區塊鏈怎麼用(available online at https://inside.com.tw/2016/3/28).

[20] 辜騰玉 ，區塊鏈運作原理大剖析：5 大關鍵技術，iTHOME 2016-04-23(available online at https://www.ithome.com.tw/).

[21] SAP, Blockchain and Distributed Ledger Techonology (available online at https://www.sap.com/taiwan/products/leonardo/blockchain.html).

[22] 科技產業資訊室-Gloria，區塊鏈要真正走向主流要等到 2025 年，2018/1/16 (available online at https://iknow.stpi.narl.org.tw).

[23] 黃雲飛，陳淑媚，金融機構發展區塊鏈技術之因應策略－兼論「金融區塊鏈研究暨應用發展委員會」之組織與運作，財金資訊季刊 / No.90 2017.10

[24] 張庭瑜，區塊鏈的技術原理與兩道陰影，數位學習 2018/05 。

[25] N.Szabo (1994), Smart Contracts. (available online at http://www.szabo.best.vwh.net).

[26] N.Szabo (1996), Smart Contracts: Building Blocks for Digital Markets. (available online at http://www.fon.hum.uva.nl/).

[27] N.Szabo (1997), The Idea of Smart Contracts. (available online at http://www.fon.hum.uva.nl/).

[28] 陳恭，智能合約的發展與應用，財金資訊月刊/No 90/2017.10。

[29] Ethereum White Paper from https://github.com/ethereum/wiki/wiki/White-Paper.

[30] Ethereum Project, (available online at https://www.ethereum.org/).

[31] 廖子淳，民 105，利用智能合約實現單車共享經濟之研究，國立中興大學資管所碩士論文。

[32] 蓋索林，什麼是智能合約?(available online at https://blog.gasolin.idv.tw/2017/09/02/what-is-smart-contract/).

[33] K.Christidis & M.Devetsikiotis, Blockchains and Smart contracts for the Internet of Things, IEEEAccess, Volume 4, 2016.

[34] 高靖鈞、丁川偉、陳耀鑫、馬金溝、陳澤世，區塊鏈簡介與技術介紹，電腦與通訊 106-05-09。

[35] Yuren Ju 工程師視角:什麼是區塊鏈的 smart contract? (available online at https://medium.com/taipei-ethereum-meetup/).