


國立高雄第一科技大學

資訊管理系電子商務碩士班

碩士論文

區塊鏈應用：以數位學位證書發證  
系統為例



研究生：鄭世玄

指導教授：許孟祥 博士

中華民國 一〇七 年 二月

# 區塊鏈應用：以數位學位證書發證 系統為例

Application of Blockchain: A digital diploma management system

研究生：鄭世玄 Jheng-Shi-Xuan

指導教授：許孟祥 Meng-Hsiang Hsu

國立高雄第一科技大學

資訊管理系電子商務碩士班

碩士論文

A Thesis Submitted to Department of Information Management  
National Kaohsiung First University of Science and Technology  
In Partial Fulfillment of the Requirements  
for the Degree of Master  
In  
Information Management  
February 2018  
Yenchao, Kaohsiung, Taiwan, Republic of China

中華民國 一〇七年 二 月

## 國立高雄第一科技大學學位論文考試審定書

資訊管理系電子商務

系(所)

☒ 碩士班☐ 博士班研究生 鄭世玄 所提之論文論文名稱(中文): 區塊鏈應用:以數位學位證書發證系統為例論文名稱(英/日/德文): Application of Blockchain: A digital diploma management system☒ 碩士

經本委員會審查,符合

學位論文標準。

☐ 博士

學位考試委員會

召集人

委

員

<u>黃文雄</u>	<u>張俊元</u>
<u>黃文雄</u>	
<u>許立祥</u>	

指導教授

主任(所長)

<u>許立祥</u>
<u>黃文雄</u>

中華民國

107 年 1 月 30 日

## 摘要

「區塊鏈」一個近期新興的名詞，卻僅僅在前後兩年內逐漸變成家喻戶曉的破壞性技術，成為專家學者們爭先恐後的研究項目。其應用範圍之廣泛例如金融科技的應用面就包括支付、跨境匯款、資產數位化、交易所、清算結算、徵信、迷你債券.....。若以非金融服務應用面而言，運用的領域又更多邁向更多元，例如存在性的驗證：身份驗證、資產驗證、資產交易、智慧合約、物聯網、預測市場、共享經濟、選舉投票、電子商務、社交通訊、檔案存儲、資料 API.....。在此科技的帶動下許多產業將有突破性的改革，但凡事總有一體兩面。本研究採方法論，以紮根理論為基礎，藉以區塊鏈機制的「不可篡改性」、「不可否認性」、「可追蹤性」、「私密性」、「正確性」及「完整性」，來發展區塊鏈非金融應用-證書認證管理系統。讓讀者對於區塊鏈的技術應用有更深層的了解，以及在本研究的後面將點出區塊鏈技術的關鍵優勢以及劣勢提供讀者正反面參考價值。希望在未來區塊鏈的應用可以更加實體化、具體化。提供社會一個更方便，更安全的機制。且不僅僅只運用在金融科技領域範疇，更能實際活用於各大行業。

關鍵字：紮根理論、區塊鏈、數位文憑

## ABSTRACT

A newly emerging term of "BLOCKCHAIN" has gradually become a well-known devastating technology in the next two years and has become a vanguard research project for experts and scholars. Its wide range of applications such as financial technology applications include payment, cross-border remittances, asset digitization, exchange, clearing and settlement, credit, mini-bonds ..... For non-financial services applications, the areas of application are moving even more toward more elements such as existential verification: authentication, asset verification, asset trading, smart contracts, the Internet of Things, market forecasting, shared economy, election Voting, e-commerce, social communications, file storage, data API .... Driven by this technology, many industries will have a breakthrough reform, but there are always two sides to everything. This study adopts a methodology based on grounded theory and based on the "unforgettable", "non-repudiation", "traceability", "privacy", "correctness" and "completeness" of the BLOCKCHAIN mechanism, To develop BLOCKCHAIN non-financial applications - certification certification management system. Let readers have a deeper understanding of the technical applications of the BLOCKCHAIN and provide the reader with both positive and negative referential values for pointing out the key strengths and weaknesses of BLOCKCHAIN technology later in this study. Hope that in the future the application of BLOCKCHAIN can be more substantive, specific. To provide society with a more convenient and safer mechanism. And not only used in the field of financial science and technology, more practical use in major industries.

Keywords: Grounded Theory, BLOCKCHAIN , Digital Diploma

## 致謝

碩士班一年半的時間，讓我學習到了許多不一樣的知識，初進區塊鏈這扇大門時感謝我的指導老師許孟祥教授指引我一盞名燈。讓剛上碩士班的我有一個明確的方向，並且與實驗室中的學長姐們一起學習成長。

在碩士生涯中的伯樂是我的指導教授許孟祥博士，願意在百忙中撥空指導我碩士論文的大方向，並且鼓勵我多方嘗試，替我建立起區塊鏈基礎以及對於人事物的積極度以及信心。我的貴人幸玲學姐，很感謝學姐給與我的論文內容很多方向以及許多實用的建議，不論是多基礎的問題都願意教導我不斷給我信心，相信自己可以完成論文。學姐在背後默默的付出讓我有足夠的能力以及信心解決迎面而來的困境，那謙虛且熾熱的心讓我十分感動，座右銘「沒有做不到的事情，只是要與不要」。在實驗室中另一位人生導師志賢學長，感謝您在我對於未來抱持著不確定感時給我一劑又一劑的強心針，讓我了解做自己想做的，勇於嘗試也勇敢承擔，在未來會是傳奇的一頁。謝謝世杰學長給證書系統介面的相關建議以及鼓勵。謝謝已經畢業的賴寒彰學長與我一起鑽研區塊鏈。就算已經畢業了師兄弟情誼永遠不變。

感謝口試委員，黃文進教授以及張俊民教授在口試當天給予的寶貴建議，讓學生我可以將論文詮釋得更好。文進老師當天的鼓勵現在仍記憶猶新，俊民老師的專業分析讓學生茅塞頓開，再次感謝您們願意撥冗給予鼓勵及指導。

感謝我的家人給予我的支持，謝謝我的家人每天晚上給我的鼓勵。謝謝女友小芬包容我的缺點。在未來的道路上我仍然會秉持著我在碩士階段所學習到的專業知識以及態度繼續努力走下去。感謝再感謝...

## 目錄

摘要 .....	i
ABSTRACT .....	ii
致謝 .....	iii
目錄 .....	iv
表目錄 .....	v
圖目錄 .....	v
壹、緒論 .....	1
一、研究背景 .....	1
二、研究動機 .....	1
三、研究目的 .....	3
四、研究流程與架構 .....	5
貳、文獻探討 .....	6
一、區塊鏈(BLOCKCHAIN) .....	6
二、區塊鏈應用案例探討 .....	26
三、數位文憑(Digital Diploma) .....	44
四、區塊鏈目前三大主流 .....	46
五、技術接受模型(Technology Acceptance Model) .....	49
六、紮根理論(Grounded theory) .....	49
參、系統開發 .....	52
一、系統緣起 .....	52
二、系統架構 .....	52
三、開發工具 .....	54
四、系統分析與設計 .....	56
五、系統實作結果 .....	61
肆、結論與建議 .....	67
一、結論 .....	67
二、學術貢獻與實務意涵 .....	68
三、研究限制與建議 .....	68
參考文獻 .....	71

## 表目錄

表 1 區塊鏈的四大構成要素及說明 .....	8
表 2 區塊鏈演進大事紀 .....	12
表 3 去中心化模型與傳統模型之比較 .....	13
表 4 傳統發證流程 .....	57
表 5 傳統發證流程節點關係時序表 .....	58
表 6 加入區塊鏈流程節點關係時序表 .....	58
表 7 區塊鏈發證節點關係時序表 .....	59

## 圖目錄

圖 1 研究流程圖 .....	5
圖 2 區塊鏈基礎 .....	9
圖 3 區塊鏈三大類別 .....	10
圖 4 區塊鏈發展示意圖 .....	11
圖 5 智能合約三大特點 .....	14
圖 6 區塊鏈 2.0 的應用實例 .....	15
圖 7 區塊鏈共識機制 .....	19
圖 8 區塊鏈網路：由成員角色控管的資料流程和網路存取 .....	21
圖 9-1 區塊鏈技術發展概述 .....	22
圖 9-2 區塊鏈技術所面臨的七大挑戰 .....	23
圖 10 股權轉讓流通 .....	27
圖 11 眾籌合約以智能合約的形式儲存於區塊鏈 .....	27
圖 12 生態流程圖(跨國貿易融資) .....	30
圖 13 區傳統跨國貿易融資交易流程圖(融資銀行巴克萊) .....	30
圖 14 傳統跨國貿易融資交易模擬流程(傳統無區塊鏈) .....	31
圖 15 Wave 平臺跨國貿易融資交易流程圖(融資銀行巴克萊) .....	31
圖 16 跨國貿易融資交易模擬流程(運用區塊鏈) .....	32
圖 17 病歷演進概圖 .....	33
圖 18 phrOS 健康醫療區塊鏈平臺架構圖 .....	36
圖 19 財務部土地房產轉移流程 .....	38
圖 20 Propy 系統架構圖 .....	39



圖 21 MIT 區塊鏈數位文憑系統示意圖.....	41
圖 22 電子證書系統架構 .....	43
圖 23 以太坊大事記 .....	47
圖 24 Hyperledger Fabric 關鍵數據.....	48
圖 25 區塊鏈畢業證書發證系統(學校端).....	52
圖 26 區塊鏈畢業證書發證系統(畢業生端).....	53
圖 27Hyperledger Fabric 架構圖 .....	55
圖 28 傳統發證流程 .....	56
圖 29 傳統發證流程加入區塊鏈 .....	57
圖 30 區塊鏈發證流程 .....	59
圖 31Hyperledger Composer Rest Server 介面 .....	61
圖 32 新增 Issuer 介面.....	62
圖 33 新增 Issuer 的資料結構.....	62
圖 34Issuer 查詢介面.....	62
圖 35Issuer 查詢之資料結構.....	62
圖 36 證書新增介面 .....	63
圖 37 證書新增之資料結構 .....	64
圖 38 新增學生帳號資料介面 .....	64
圖 39 新增學生帳號資料之資料結構 .....	64
圖 40 查詢學生帳號資料介面 .....	65
圖 41 查詢學生帳號之資料結構 .....	65
圖 42 查詢待發證書 .....	65
圖 43 查詢待發證書之資料結構 .....	66
圖 44 學生查詢介面 .....	66
圖 45 學生查詢介面之資料結構 .....	66
圖 46 利用區塊鏈改良傳統流程 .....	67

# 壹、緒論

## 一、研究背景

傳統金融產業正面臨互聯網金融及金融科技 (FinTech) 的衝擊，而其中又以數位金融相關的區塊鏈 (BLOCKCHAIN) 技術為金融科技的領頭羊，吸引全球政府機構與金融業巨擘投入研究。目前區塊鏈技術在歐美國家可說是如火如荼的發展研究中，光是在投資新創公司的資金就超過 10 億美元，重金投注在區塊鏈不僅僅只在硬體的基礎建設，也同時在金融產業上產生化學反應。例如，在金融業的結算系統、數字憑證的股票發行、及日常生活中的應用正在慢慢顛覆翻轉你的生活。近年，我國也跟上世界的潮流開始投注及發展區塊鏈的應用，無論是學術單位或者銀行資本家都紛紛投入其中。可見區塊鏈在未來將扮演著舉足輕重的角色。在臺灣大學更是成立區塊鏈研究中心，以及研發 G-COIN 的技術。運用區塊鏈的技術來增加交易的效率，用以增加 P2P 的信任機制。針對區塊鏈這項具改革力的創新技術而言，其應用領域之廣泛，不僅僅只能用在金融產業。而對於各行各業的創新革命都蓄勢待發。區塊鏈不僅在我國內吹起一陣科技風，也正在為全球各行業帶起全新的信任機制浪潮。

## 二、研究動機

區塊鏈的應用相當的廣泛，非僅限於金融業，區塊鏈發展將現有的技術革新至另一個全新型態的服務，例如共享經濟(AirBnB、Uber)。可以說是臺灣金融創新科技有史以來最大的突破！臺灣大學更成立「臺大金融科技暨區塊鏈中心」，聘請臺銀副總蔡宗榮、前 IBM 大中華區智慧分析營運長王克寧，與廖世偉共組金融、資訊、技術核心鐵三角，包括新光金創投、歐付寶、富邦等都表達強烈興趣！因此在時代的脈動下，區塊鏈儼然是一塊具有潛力的璞玉，正等待著我們細

心琢磨變成具有價值的瑰寶。

### 區塊鏈六大優點

- 1.降低運作成本。
- 2.降低信任風險。
- 3.催生新商業型態。
- 4.架構靈活有彈性。
- 5.實現共享經濟。
- 6.開放技術更有利於創新。

在國內，區塊鏈新興技術雖未普及到各個家庭，成為家喻戶曉的基本常識。但在各先進大國早已開始研究這項技術，並且成為當紅炸子雞。未來發展與應用指日可待，不可限量。有關於現行金融的交易模式，皆需透過第三方支付來達到各種資金流通，若能加入區塊鏈機制或設置其相關服務平臺，其可以簡化流程、縮短交易時間、省去手續費及又能兼顧交易的安全性。而區塊鏈的應用不僅僅於金融科技方面。在許多領域都將扮演著不可或缺的重要角色，金融應用:支付、跨境匯款、資產數位化、交易所、清算結算以及徵信。而提及非金融服務應用則更多，存在性認證：身份驗證、資產驗證、資產交易、智慧合同、物聯網、預測市場、共享經濟、選舉投票、電子商務、社交通訊、檔案存儲以及資料 API.....。上述的多種應用都能藉由區塊鏈技術來達到更高的處理效率。

目前在我國內雖然區塊鏈的應用尚未普及化，但隨著時間的推演漸漸的成為一種趨勢，一種潮流。成為專家學者、企業主積極投入相關研究，這破壞式創新的區塊鏈技術，它正顛覆著企業、組織、及金融業的重大改變。。而本研究，將探討透過區塊鏈技術，改良證書驗證系統的實際應用。

### 三、 研究目的

現行環境中在面臨升學、求職的階段。書審資料對於求職者、面試者而言為代表自己的一種證明，其中個人履歷尤其重要，相關證書、證照以及研習的證明往往都是證明自己能力的指標。但透過有心人士的操作畢業證書、能力證照、研習證明....。都有偽造的風險。如果企業錄取了偽造證書的人員，輕則解雇，重則將會影響公司的行政運作。要如何選擇正確人員當務之急必定先從個人履歷開始篩選，一般而言傳統的方式大致上由人資部門親自致電或致函到學校由校方統一處理，但一來一往會消耗很多不必要的成本。光是時間成本的浪費就不容小覷。學校又得經由專人調閱資料庫，並一一檢核。其中的反鎖流程在下文中會做一討論。現行證書發證現況的問題有：

#### (一)證書發證、補發、查詢手續繁複費時

以校園而言，無論是在校生或者在學生往往都需要申請相關的成績證明文件或者證書證照。但往往都需要經過相當繁瑣的申請程序。需要以本人至教務處服務臨櫃做線上申請後，再由服務人員印出該學生相關證明文件，委實相當不方便。透過區塊鏈的不可篡改性以及可追蹤性建立證書認證管理系統。讓學生即使人在外地也能成功申請學習相關文件，不必再親自跑到教務處臨櫃作申請。省去了從外地到學校的路程時間，簡短了繁瑣的申請流程。

#### (二)改善傳統申請查閱證書的種種缺點

利用區塊鏈技術改善申請查閱證書的種種不方便，在未來每一位學生畢業後都將面臨一個很大的就業考驗。而就業時所繳交的履歷中，常常有學經歷這一項目或欄位。並且資方會要求附上畢業證書，而具有一定規模的資方往往都會再向

勞方之前就讀的學校做一次確認。但從致電至學校教務處，教務處接獲求證需求，也要再等幾天的工作日。時間往返就得浪費許多時間，因此，透過區塊鏈的證書驗證系統，只要登入學校首頁即可進行驗證。如何利用區塊鏈機制來改善證書、證照的查詢以及申請」。

本研究目的，待解決問題臚列如下五點：

- 1.如何簡化證書的申請流程。
- 2.如何簡化證書發證流程。
- 3.如何利用區塊鏈的不可篡改性來提高證書發證資訊安全。
- 4.如何有效率的防範證書發證平臺系統受駭客攻擊，被惡意篡改。
- 5.如何建置具有安全機制區塊鏈證書發證平臺。



#### 四、 研究流程與架構

本研究透過相關文獻的探討，採用紮根理論的個案資料收集研究方式，針對區塊鏈四大構成歸納出的特性，並建立相關特性表及利用案例分析的方式來實證，根據案例所提供的資料，去推導模擬出這些交易步驟，透過案例模擬完之後，把它的共通性抽出來，而形成一個方法論。最後，提出研究結果與建議，研究流程如圖所示。研究流程如圖 1 所示：

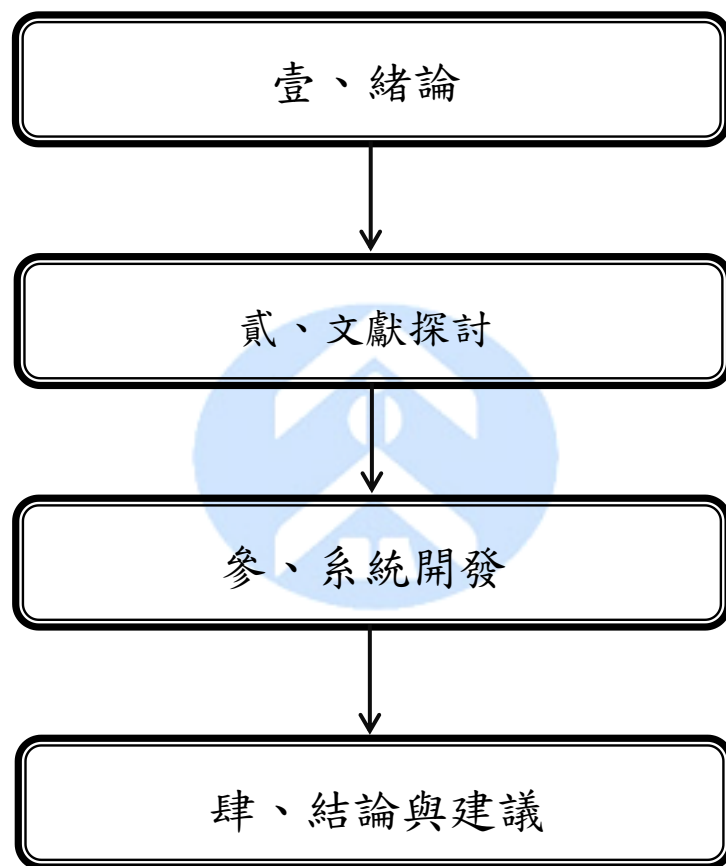


圖 1：研究流程圖

## 貳、文獻探討

### 一、區塊鏈(BLOCKCHAIN)

#### (一)區塊鏈細說從頭

「區塊鏈」的前世今生必須從中本聰開始說起，他在 2008 年 11 月 1 日項秘密討論群組(密碼學清單)當中，發了一則新訊息「我正在開發一種新的數位貨幣系統，一種採用 Peer to Peer(點對點)的方式，且再也不需要第三方機構的介入」。而中本聰在 2008 年正式將全世界推出如今炙手可熱的「比特幣」。而他也強調“傳統貨幣最根本的問題就是信任。中央銀行必須讓人信任他不會讓貨幣貶值，但歷史上這種可信度從來都不存在”。兩個月後中本聰也在 2008 年推出聞名於世的文章「比特幣:一種點對點的電子現金系統」，其中他在文裡所提出的根據 P2P 網路、密碼學技術、時間戳技術、區塊鏈技術等的皆是電子現金系統的構架理念，(Satoshi, 2009)。而區塊鏈技術是一個按照時間戳(Timestamp)的公開交易紀錄，所有的用戶分享區塊鏈，它功能主要用於驗證交易的持久性和避免「雙重支付」的情況。但區塊鏈嚴格來說並非是一種創新技術，在之前就有相似性的技術，例如密碼學、數學、演算法與經濟模型等。而區塊鏈技術只是將許多跨領域的技術相互做整合，所發展出的交易信任機制。雖現在區塊鏈技術幾乎已成為一種改革的新趨勢，在未來也許有很多跨金融領域的非金融科技應用出現，但大多數的改革都仰賴區塊鏈所衍生出的信任機制，其宗旨為就算非熟識且不信任的對象，都能放心的與對方合作。

而比特幣，僅是運用區塊鏈基礎技術所建立出具可追蹤、可去中心化、並使交易資訊更加安全的 P2P 電子現金系統的數位貨幣體系(Melanie,2015)。財訊雙週刊 2016 年提到，2014 年比特幣開始竄紅全世界，世界經濟論壇創辦人施瓦布(Klaus Schwab)認為區塊鏈更是帶來了第四次的工業革命(工業 4.0)。在資策會 ICT 萬物論／擁抱區塊鏈創造美好新生活行中提到各業若想擁抱區塊鏈，正確態

度應是：需要清楚了解區塊鏈技術和發展走向。把區塊鏈技術放在對的位置上，而並非為了引用而使用。每一種工具、制度、方法都有其優點以及缺點。審視區塊鏈優勢以及劣勢並且適度的改革目前困境才是上上之策。

在 2016 年 4 月臺灣 IBM 公司所出的專業雜誌 Blue Viewpoint 中提到，區塊鏈被廣泛的應用到金融及各產業，這與分散式帳本、密碼學機制、智能合約和共識機制等四大構成要素有關，如表一所示：





表 1：區塊鏈的四大構成要素及說明

構成要素	說明
分散式帳本 (Distributed Ledgers)	區塊鏈將所有的交易紀錄存放在多個節點，去中心化的資料留存方式讓買賣雙方得以隨時追溯交易歷史。不同於傳統異業查詢異業需要經過重重的關卡，只要身為交易者均有權利查看交易歷史紀錄。更使資訊更透明化。總而言之，分散式帳本與傳統帳本的最大不同之處為，單一節點不能單獨進行記帳的行為，必須把資訊也發布到其他節點上的帳本。並透過網際網路上的很多節點，來降低被篡改的風險。只有一口氣改網路上百分之五十一的節點才有可能被駭客篡改資料，而需要成功破解全部節點才會導致資料遺失。
密碼學機制 (Cryptography)	在比特幣理論中，在發生交易時，都須要原本的擁有者進行數位簽章核准這筆交易，驗證中的交易資料相關訊息將被紀錄到區塊中，並透過Hash演算法進行記錄。數位簽章讓交易產生了不可否認性，Hash演算法則提升了交易的偽造難度。假設A為原本一段Hash值，但後來加入任一字母或數字，可能導致顯示的排列數據完全不同，Hash值可說是區塊鏈的安全守門員。
智能合約 (Smart Contracts)	自動化的智能合約系統。交易參與者能將合約當中的交易紀錄，以及商業條款以編碼的方式寫入以區塊鏈區塊裡，並將相關資訊儲存於區塊鏈中，並藉由電腦以自動化方式進行驗證，判斷實否如合約內容所示。不論是企業、供應商或者是客戶將可以放心交易。不必再擔心資料是否會有被篡改的風險。
共識機制 (Consensus)	在集中式的管理環境中，交易的正確性皆由中央控管單位負責，而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。共識決機制牽涉到每個節點的存放資料，就結果而言降低了中央控管單位因資安事故導致金融詐欺事件的風險。

參考資料：(IBM 專業雜誌 Blue Viewpoint、證券暨期貨月刊第三十四卷第十期)

歸納其定義，區塊鏈技術是由「分散式帳本」、「密碼學機制」、「智能合約」、「共識機制」、四大構成要素所構成。「分散式帳本」簡言之為一分散式的記帳紀錄系統，可在帳本上設定共享對象公開資料，但卻無法修正、刪除已經寫入區塊鏈的資訊。「密碼學機制」為一種複雜的 Hash 函數所產生的值，為了就是能有效的防止有心人士惡意破譯篡改訊息。「智能合約」為在交易的當下即時性的執行建在資料庫中的交易相關條約。「共識機制」指的是，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。

區塊鏈的發展體系，簡言之可分為四大象限。如下圖二所示，(1)比特幣區塊鏈。(2)使用以特幣區塊鏈協議。(3)同時使用獨立貨幣和獨立區塊鏈的系統。(4)側鏈，機使用獨立的網路但以比特幣做為底層貨幣的系統。

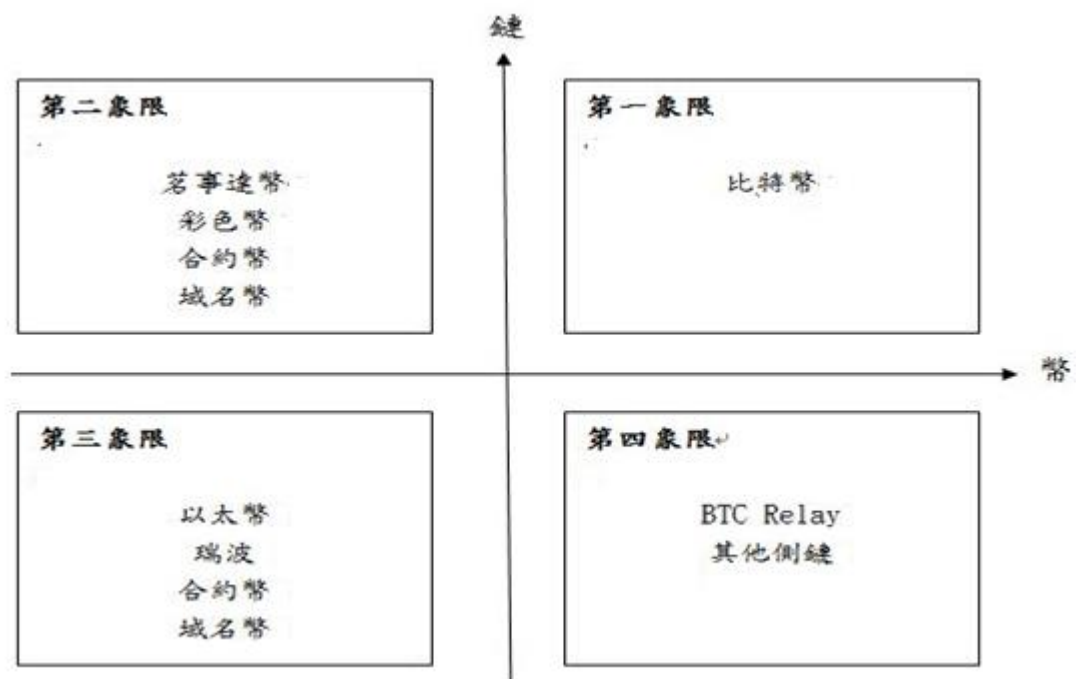


圖 2：區塊鏈基礎

參考資料: (海濱,2016)

## (二)區塊鏈的分類

區塊鏈的分類共分為三大類，如圖三所示：

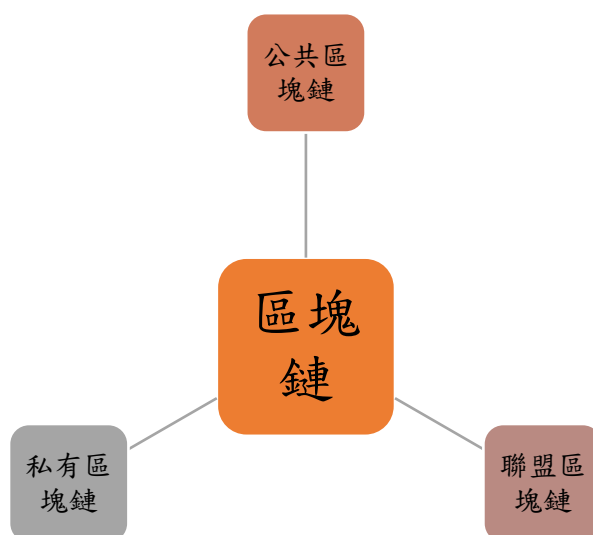


圖 3：區塊鏈三大類別

1.公共區塊鏈(Public BLOCKCHAIN)：指的是任何使用者都可以參與使用和維護，並通過驗證被寫入區塊鏈之中，共識過程透過密碼學 Hash 函數來保護公有鏈上的數據安全。典型的如比特幣區塊鏈，其交易紀錄以及相關資訊都是完全公開。其特性我們可分為三點：保護用戶免受開發者影響、訪問門檻低、所有資訊都默認公開。

2.私有區塊鏈(Private BLOCKCHAIN))：資訊流通之間具有很嚴格的限制存在。其中參與交易的節點只能是在特定的範圍之內，例如特定的交易者以及特定的節點，才有特別的使用權限。在私有鏈上擁有寫入權限者僅僅在參與者身上，閱讀的權限可以設定為對外開放，其中的權限管理也可視情況做調整。而私有區塊鏈的特性我們大至上可分為四點，交易速度非常快、給隱私更好的保障、降低交易成本、有助於保護其基本產品。

3.聯盟區塊鏈(Consortium BLOCKCHAIN)：介於公有鏈以及私有鏈之間。是指參與區塊鏈的節點可以做選擇，由很多不一樣的組織一起合作一起維護，在該區塊鏈的使用者必須是有權限的管理，相關資訊就會得到有效的保護。

### (三)區塊鏈編年史

區塊鏈發展可分為三大類，如圖 4 所示

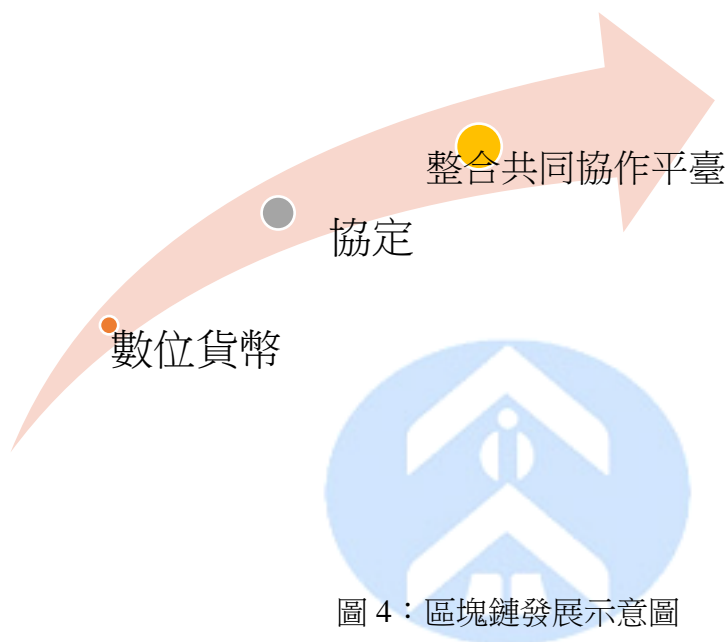


圖 4：區塊鏈發展示意圖

1.前期：數位貨幣，區塊鏈的最早技術是源於數位貨幣（Bitcoin）。且區塊鏈的基礎建立在節點彼此不信任上，因此區塊鏈就像提供了一臺信任機器，讓交易完全透明公開。

2.中期：協定，於 2014 年後 Peer to Peer(P2P)技術出現後，區塊鏈除了被應用在虛擬貨幣之外，更用於較多類型的資產轉移上例如:股票、土地以及證券的交易上。

3.後期：整合共同協作平臺，區塊鏈開放 API，不只侷限於金融行業的應用，將會成為更多行業的發展利器，不論會計、物流、房產、保險各領域均可使用區塊鏈的技術進行革新，藉由開放原始碼，讓人人創新創業成為可能。區塊鏈技術的出現和應用並非擊敗現有的金融、物流等體系，而是發現行業裡的不足之處並

改善，創造出更多機會成就更不一般的價值。而區塊鏈演算法演進如表 2 所示：

表 2：區塊鏈演進大事紀(參考資料: 辜騰玉 2016)

1982 年	Lesile Lamport 提出拜占庭將軍問題，決定是否出兵的過程。		
1985 年	橢圓曲線密碼學		
1990 年	David Chaum 基於先前理論打造出不可追蹤密碼學，即後來 e-cash		
1991 年	使用時間戳確保數位文件的安全		
1992 年	Scott Vanstone 等人提出橢圓曲線數位簽章演算法		
1997 年	Adam Back 發明 Hashcash，作為工作證明演算法		
1998 年	Wei Dai 發表匿名的分散式電子現金系統 B-money， Nick Szabo 發表 Bit Gold		
2005 年	可重複使用的工作證明機制(RPOW)		
2008 年	BitCoin		
2008 年 後	區塊鏈 1.0	區塊鏈 2.0	區塊鏈 3.0

區塊鏈 1.0：(加密貨幣的出現) 數位貨幣與支付系統去中心化。首先，比特幣代表了底層的區塊鏈技術平臺。第二，比特幣是一種基於底層區塊鏈技術之上運行的協議，這種協議是用來描述資產是如何在區塊鏈上轉移的。約 2012 年後發展成熟。以數位貨幣比特幣而言他是區塊鏈 1.0 指標性的產物，而比特幣更是

牽引出區塊鏈的一大功臣。而數位貨幣主要的特色為在滿足主權與監管機制下，由國內主要的機構所發行的一種電子數位貨幣。區塊鏈採用去中心化的管理模型與傳統管理模型不同(比較如表 3)，它透過自動模式進行支付、轉帳及匯款交易，其交易過程不需銀行、結算機構甚至政府單位等第三方公正單位，就可以達到交易紀錄資訊透明化的目的。並且把運算加密數學公式解出透過共識機廣播(Broadcast)致各節點(Node)就能把交易訊息廣泛、透明。同時完成驗證及留下可靠數位交易紀錄，讓人們在沒有中央或主管機構情況下，建立彼此信任(賴怡伶, 2015)。

表 3：去中心化模型與傳統模型之比較

	傳統模型	去中心化模型
特色	<ul style="list-style-type: none"> <li>●轉帳程式由金融機構藉由支付系統處理(如 SWIFT、Visa、MasterCard)</li> <li>●依賴中央清算主體</li> <li>●資金移轉由受款行啟動</li> </ul>	<ul style="list-style-type: none"> <li>●轉帳記錄採分散式記帳</li> <li>●交易由分散式網路參與者進行驗證</li> <li>●資金移轉由付款人啟動</li> </ul>
優點	<ul style="list-style-type: none"> <li>●系統網絡包括既有的金融機構</li> <li>●可吸納大規模的國際資本</li> <li>●大型企業客戶群較熟悉此模型</li> </ul>	<ul style="list-style-type: none"> <li>●轉帳歷史資料透明，可追蹤及無法更改</li> <li>●交易成本低</li> <li>●傳統詐欺風險較低</li> <li>●清算接近即時，無交易對手風險</li> </ul>
缺點	<ul style="list-style-type: none"> <li>●轉帳過程透明度較低</li> <li>●若付款人的單據資訊外流，易引發詐欺</li> <li>●資金移轉可能耗費數日，處理效率因國家及機構而有所不同</li> <li>●高成本且須要較多中介機構進行轉帳</li> </ul>	<ul style="list-style-type: none"> <li>●虛擬貨幣波動度高</li> <li>●法規限制與法償貨幣連結</li> <li>●帳戶匿名及轉帳不可撤銷，易生安全問題</li> <li>●高度曝露在非傳統詐欺風險(如大規模網路攻擊)</li> </ul>

資料來源：The World Economic Forum (2015)

區塊鏈 2.0：(智慧資產、智慧合同)，約莫 2014 年秋後開始，區塊鏈 2.0 帶來了許多不一樣的用途，也因此區塊鏈 2.0 發展期間對於他的類型、領域有很多不一樣的見解，其中較為人常見的領域有比特幣 2.0、比特幣 2.0 協議、智慧合同以及智慧資產，Dapp(去中心化應用)和 DAC(去中心化自治企業)。發展約 2014 年後逐漸成熟。其應用領域比起區塊鏈 1.0 更勝一籌，概述上而言，2.0 版本含蓋了整個市場需求，可以利用智能和同來管理財產項目，無論是有形的資產義或者是無形的資產，均可透過區塊鏈的可追蹤性、不可篡改性來達到一個有效的控管以及保障。在 2.0 版主要的領域為金融科技領域，主要仰賴的技術為智能合約。智能合約有三大特點如圖 5 所示：

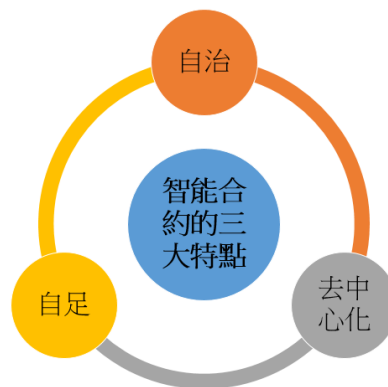


圖 5：智能合約三大特點

參考資料:(馬兆林,2017)

智能合約(Smart Contract)最早於 1994 年由 Nick Szabo 這位學者所提出。智能合約中主要的機制為一旦啟動運行就能自動且自治的運作，不需要他人操控。且具有去中心化的特性，不必藉由第三方管理機構來約束。合約本身為分散式架構，主要透過網路上的個節點來進行運作。智能合約主要功能為根據事件描述的訊息中所包括的任何既定的規則，當目前的事件符合既定的規則後，從智能合約自動發出預設的資訊，以及包括符合規則所觸發的事件。簡言之智能合約其建立起的權利與義務即能強制性執行，其不需要具有公信力的的第三方仲裁



(arbitrator)，可讓互聯網中的二個陌生人進行資產的交易(transaction)，用以實現價值互聯網的境界(Florian,2014)。但智慧合約的缺點是，其程式碼必須向網路上的眾合作者公開，這就代表著非參與者可以得知合約的內容，並且透過了解合約內容找出漏洞。刻意囤積貨物或者是從中謀取利潤並且，智能合約在網絡內大範圍傳播的速度是很慢的，現有資本交易系統的領域中，還是難以應付金融交易的需求(Chris,2016)。區塊鏈 2.0 應用實例如圖 6 所示：

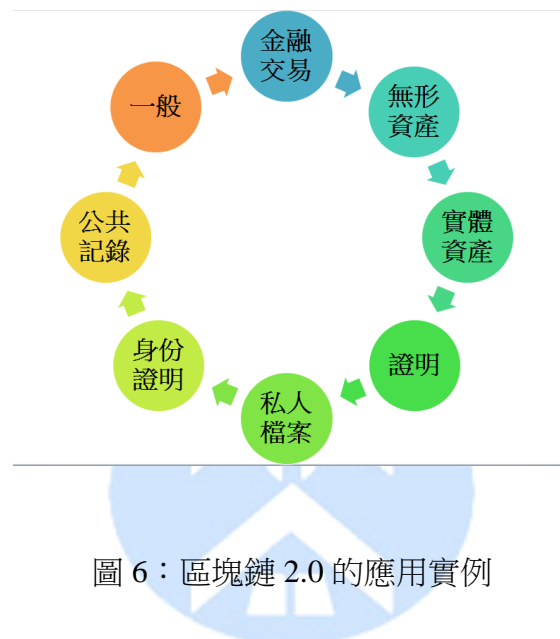


圖 6：區塊鏈 2.0 的應用實例

參考資料：( melanie Swan,2015)

區塊鏈 2.5：(技術演變的過渡期)，強調代幣應用、分散式帳本、資料層區塊鏈，及結合人工智慧等金融應用。

區塊鏈 3.0：區塊鏈 (更多元化的智能合約)，超越貨幣、經濟和市場的公正應用，其應用領域不僅僅只侷限於金融科技領域。Melanie Swan(2015)指出，公正應用是指區塊鏈 3.0 的更複雜的智能合約，將區塊鏈用於政府、醫療、科學、文化與藝術等領域。並且對於其他行業也能提供一個科技改革的能力，在 3.0 版的區塊鏈將用於政府、醫療、科學、文化與藝術等領域。如果說區塊鏈 2.0 通過智能合約來徹底顛覆了傳統貨幣和支付的概念，而區塊鏈 3.0 我們將探討區塊鏈在非金融貨幣領域中的價值。跨足領域有 (公鑰和私鑰加密、P2P 文件共享、分



佈式計算、網絡模型、匿名、區塊鏈賬本、加密數字貨幣和協議等。)來藉以推動區塊鏈的發展。甚至更廣泛來說區塊鏈他漸漸的將涉及人類生活圈，而去中心化屬性讓原本給付第三方機構的成本降低，更提升了交易與交易之間的效率。而區塊鏈又提供不可篡改的公開帳本，公開透明化資訊，使記錄資訊更安全更機智。

截至今日目前區塊鏈的演變架構如上述所講分為三階段，從一開始的比特幣數位電子貨幣到智能合約再擴展到各領域的應用，區塊鏈正以快速成長的模式，迅速的在科技業嶄露頭角，直到獨占鰲頭。在「每日頭條-HPB 芯鏈聯合 imtoken 等五大平臺上線 ICO」一文中提到 2017 年的 7 月中國汪曉明提出全新的名詞「芯鏈(High-performance BLOCKCHAIN)」，並且指出區塊鏈技術仍在發展階段，但發現區塊鏈在處理資訊的速度並不特別快，甚至在高訊息流量時會有延遲的情況發生。因此，汪曉明與其技術團隊研究開發了一種改良版的區塊鏈平臺，為每秒提供數百萬交易確認，並將此區塊鏈平臺命名為「芯鏈」。而 HPB 希望能改變目前區塊鏈處理速度，並且開創一個權新的區塊鏈新生態。

更在芯鏈白皮書上說明其設計包含五個重要特色，開源、支持數以億計的用戶、低延遲、高運算力以即透過硬體加速引擎。芯鏈雖為剛起步但假以時日可能會再次改良區塊鏈的使用環境。

#### (四)區塊鏈的技術創新

##### 1.分散式帳本

區塊鏈的本質換句話而言，就是分散式帳本。是一套能夠透過網路串連起世界上的電腦節點，來達到訊息分享的資料庫。在所有的經濟交易活動中，可以進行主要記錄的工作。為何分散式資料庫能夠為各項應用帶來革命性的創新呢？廖世偉(2016)研究指出，區塊鏈會對各產業帶來很大的益處，而區塊鏈中的去中心化技術，無需中間機構的介入，所有的交易達成都必須透過節點驗證完成並寫入

帳本中。一般而言在參與節點裡，可以獲得分散式帳本的資訊，任何的交易資訊都會一一記錄進其他節點的帳本裡，而記錄的時間往往是幾秒鐘至幾分鐘的時間，因此要在短時間內篡改網路上所有節點是相當困難的。因此更加奠定了安全交易的基礎。

## 2.密碼學機制

廖世偉(2016)研究提到，藉由公鑰密碼學的延伸區塊必須滿足一項非常嚴格的密碼學規則，要是隨意篡改的區塊會因為不符規則都會被歸類到錯誤，藉由這個機制，使有心人士無法隨便篡改區塊鏈的部份交易紀錄。密碼學從古至今有太多解譯破譯的例子，而加密方式更族繁不及備載。以東方人紀錄而言最怎可追溯周朝《六韜·龍韜》記載密碼學的運用，陰符和陰書中所提到周武王問姜子牙關於出征，戰爭時跟將領們的聯絡方式，保密程度。而西洋史學家西羅多德更在《歷史》一書提及，最早的秘密書信的故事，早在西元前五世紀就有應用加密技術的希臘與波斯之戰。直至近代史中世紀到第二次世界大戰，密碼學越受到重視，以及被廣泛的應用在政治以及軍事的情報文書之中。

而區塊鏈中的密碼學則採用密碼雜湊(Hash)函式，其中則涉及複雜的密碼學加密機制，簡而言之“雜湊函數將任意長度的二進位值映射為較短的固定長度的二進位值，這個小的二進位值稱為雜湊值。雜湊值是一段數據唯一且極其緊湊的數值表示形式。如果散列一段明文而且哪怕只更改該段落的一個字母，隨後的雜湊都將產生不同的值。要找到散列為同一個值的兩個不同的輸入，在計算上是不可能的，所以數據的雜湊值可以檢驗數據的完整性。一般用於快速查找和加密演算法。將任意長度的二進位值映射為較短的固定長度的二進位值，這個小的二進位值稱為雜湊值。雜湊值是一段數據唯一且極其緊湊的數值表示形式。如果散列一段明文而且哪怕只更改該段落的一個字母，隨後的雜湊都將產生不同的值。要找到散列為同一個值的兩個不同的輸入，在計算上是不可能的，所以數據的雜湊值可以檢驗數據的完整性。一般用於快速查找和加密演算法。”(智庫百科-雜湊

算法)區塊鏈透過雜湊函式，進而達到保護加密的目的，提高保護資料的安全性，更是區塊鏈技術的核心之一。

### 3.智能合約

「智能合約」一詞始於學者 Nick Szabo 於 1990 年提出，主要的理念為讓電腦公平的處理我們日常生活所面臨的契約，以及相關條款。但在當時因電腦科技發展較不廣泛，因此並無得到特別多的迴響。但直到近幾年區塊鏈技術興起後才漸漸的被世人所看見，慢慢的受到重視。2015 年中推出的區塊鏈平臺－以太坊 (Ethereum)，其白皮書名為「新一代智能合約與分散式應用平臺」(A Next-Generation Smart Contract and Decentralized Application Platform)，強調智能合約為其平臺特色，一舉將智能合約這個名詞推到一個新的層次。

讓大家開始注意到智能合約的重要性，甚至視其為「區塊鏈 2.0」的主要技術與應用。(智能合約的發展與應用-陳恭)而智能合約的運作，大多是應用應用程式的邏輯以及相關條件來奠定的。而智能合約程式正式在區塊鏈平臺上線後，當合約內的條件或者事件遇到觸發時，則開始啟動程式。而智能合約的運用範圍大多數在於資產轉移的範疇內。

而智能合約並非是十全十美的技術，在技術方面而言。智能合約並非新穎的科技，但如若要以程式的方式來呈現，具有其困難性。如果要連結到區塊鏈外的實體資產轉移，勢必要與其他系統做連接。無法獨力完成資產轉移。而智能合約很有可能與現實生活中的法律有所衝突。演變到最後很有可能須具實體法律來修正期合約內容。

#### 1.共識機制

共識機制主要分為以下四種類型：(如圖 7)

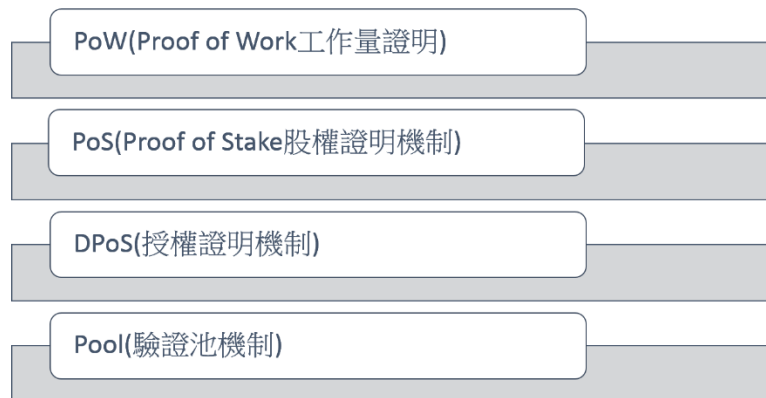


圖 7: 區塊鏈共識機制

參考資料:(馬兆林,2017)

### (1)PoW(Proof of Work，工作量證明機制)

以比特幣而言，工作量證明就是在比特幣挖礦時的參與以及計算，計算出符合條件的隨機數，並取得記帳權。競爭的是電腦設備的運算速度。運算速度愈好則挖礦所獲得的比特幣就越多，根據工作量分配貨幣 PoW 的優勢就是實現去中心化，節點自由進出。但其中的缺點就在於，當前比特幣幾乎網羅了全世界的計算立，使用 Pow 共識機制的區塊鏈相關應用，很難達到這麼高的計算力來保障自己的安全性。再者比特幣挖礦需要浪費很多的電能以及相關成本。

### (2)PoS(Proof of Stake，股權證明機制)

與 PoW 機制相較之下，PoS 是升級版的共識機制，根據每個節點貨幣數量和時間的比例降低挖礦的難度，並且加速查找隨機數。在實際應用上，PoS 機制可以縮短共識達成的時間。讓安全性更有保障。但其中的缺點仍然需要挖礦，並沒有解決 PoW 的缺點。

### (3)DPoS(授權股權證明機制)

DPoS 則是一種嘗試解改善比特幣傳統的工作量證明。其優點是大幅減少參與驗證的節點，也減少需要確認的請求。讓交易的效率得到明顯的提升。跟 PoW 與 PoS 相互比較 DPoS 可以在區塊裡記錄更多的交易紀錄，讓加密貨幣技術提升到與中心化的運算系統相互媲美。

#### (4)Pool(驗證池機制)

Pool 為目前區塊鏈使用的常見的共識機制。優點為不需要代幣也可以照樣工作，大大提升了驗證速度，只需要幾秒鐘的時間就可以順利完成驗證。並且此 Pool 機制還提升了驗證的安全性，適合多方參與的多中心商業模式。

上述四種的共識機制均應用在不同的商業應用，而其最主要的目的即是在區塊鏈應用下，能夠讓效率以及安全達到平衡點。科技進步的速度日新月異，在未來將會有更多區塊鏈的應用慢慢出現，而共識機制也必須因應時下需求做出演化，做出進步，讓區塊鏈應用不僅只侷限在金融科技相關，甚至只侷限於貨幣應用。共識機制也必須跟著創新與革命。

#### (五)區塊鏈操作模式

根據 IBM Cloud 文件 IBM BLOCKCHAIN 平臺，文中指出在 BLOCKCHAIN 網路中，在網際網路上的每一筆交易記錄都會存檔在從所有或部分網路成員抄寫的共享帳本之中。所有交易的記錄（其中包含正確的資訊以及錯誤的資訊）全部都將寫進區塊裡，並附加至每個通道的雜湊鏈（亦即，區塊鏈）。有效的交易將會更新廣域狀態資料庫，無效的交易則不會。鏈碼（也稱為「智慧型合約」）是構成軟體的組件，其中包含一組函數，可針對分類帳進行讀取和寫入。用戶端應用程式利用 SDK 來與對等節點連接，最後會在特定鏈碼上呼叫函數。有兩個主要 Fabric API 可讓鏈碼讀取或寫入 - getState 和 putState。區塊鏈網路請參照圖 8：

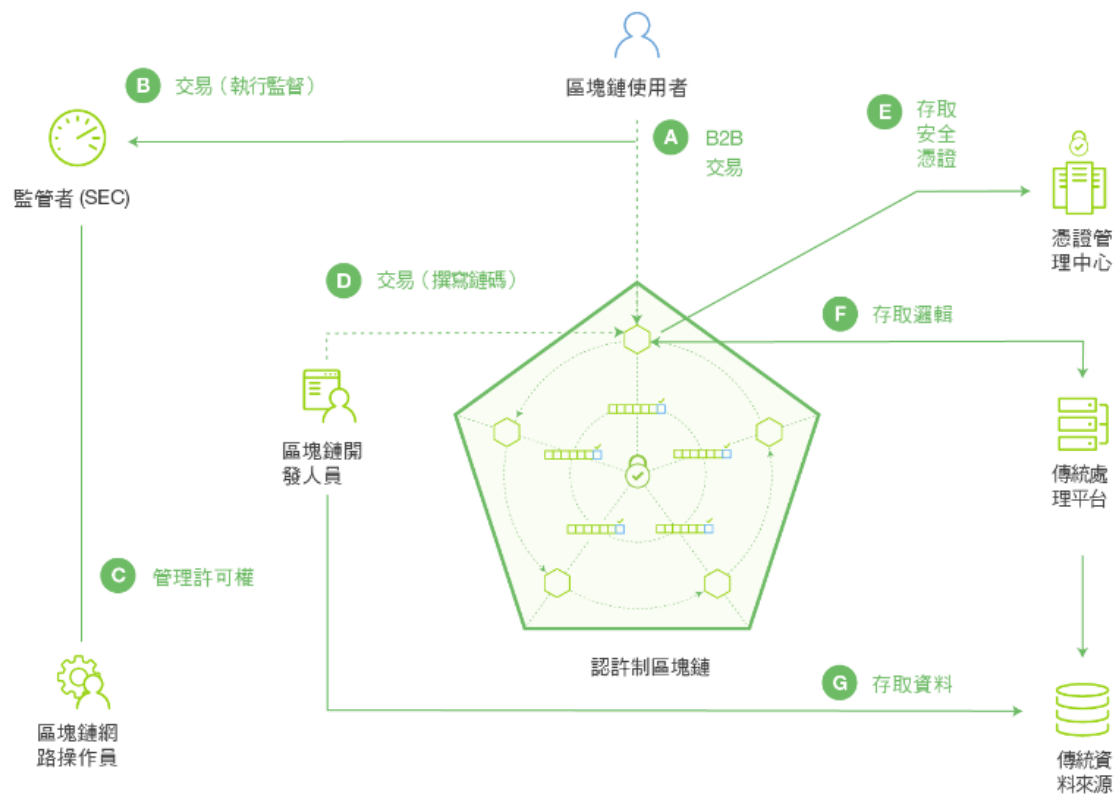


圖 8：區塊鏈網路：由成員角色控管的資料流程和網路存取

**A：**「區塊鏈使用者」將交易提交至區塊鏈上。可做查詢、寫入的功能，並且是透過運用 SDK 的用戶端應用程式，或是直接透過 REST API 發出。

**B：**授信商務網路提供對監管者和審核員（例如美國股票市場中的 SEC）的存取權。

**C：**「區塊鏈網路操作員」管理成員許可權，例如將「監管者」(B) 登記為「審核員」，將「區塊鏈使用者」(A) 登記為「用戶端」。可限制審核員只能查詢分類帳，而授權用戶端可部署、呼叫及查詢特定類型的鏈碼。

**D：**「區塊鏈開發人員」撰寫鏈碼和用戶端應用程式。「區塊鏈開發人員」可以透過 REST 介面，將鏈碼散布到網際網路上。若要在鏈碼中併入傳統參考資料的認證，開發人員可以使用頻外連線來存取資料 (G)。

**E：**「區塊鏈使用者」節點 (A) 連接至網路。在繼續進行任何交易之前，節點都會先從「憑證管理中心」擷取使用者的登記和交易憑證。使用者必須擁有這些數位憑證，才能在具有許可權的網路上交易。



**F：**嘗試驅動鏈碼的使用者可能需要驗證其於傳統參考資料 (G) 的認證。若要確認使用者的授權，鏈碼可以透過傳統處理平臺，使用頻外連線來連接此資料。

## (六)區塊鏈的技術挑戰

區塊鏈在近兩年的演進下，很快的發展到區塊鏈 3.0 甚至已經有區塊鏈 4.0 的呼聲，然而在大環境下的推廣區塊鏈技術的優勢，幾乎追捧成一種創新革命的主要科技，而這項科技卻仍然為萌芽起步階段。國內外有關於區塊鏈的研究書籍不勝枚舉，甚至逐漸變成了一種氾濫的地步，從許多書籍中舉例了許多區塊鏈的應用，但真正把區塊鏈徹底實踐的案例並不多。本段落將反向思考區塊鏈技術是否也隱藏著不被大眾所提及的隱憂。在 Accenture 研究報告指出區塊鏈技術的應用仍須要 10 年左右的時間熟成。如圖 9-1 所示：

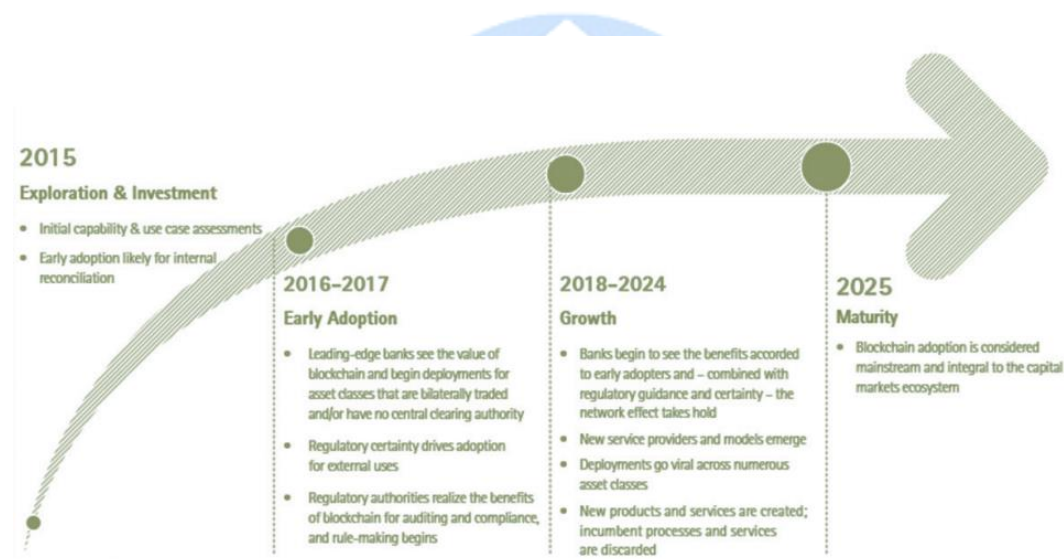


圖 9-1：區塊鏈技術發展概述

參考資料：(楊英伸,2016)

區塊鏈技術所面臨的挑戰參考如圖 9-2 所示：

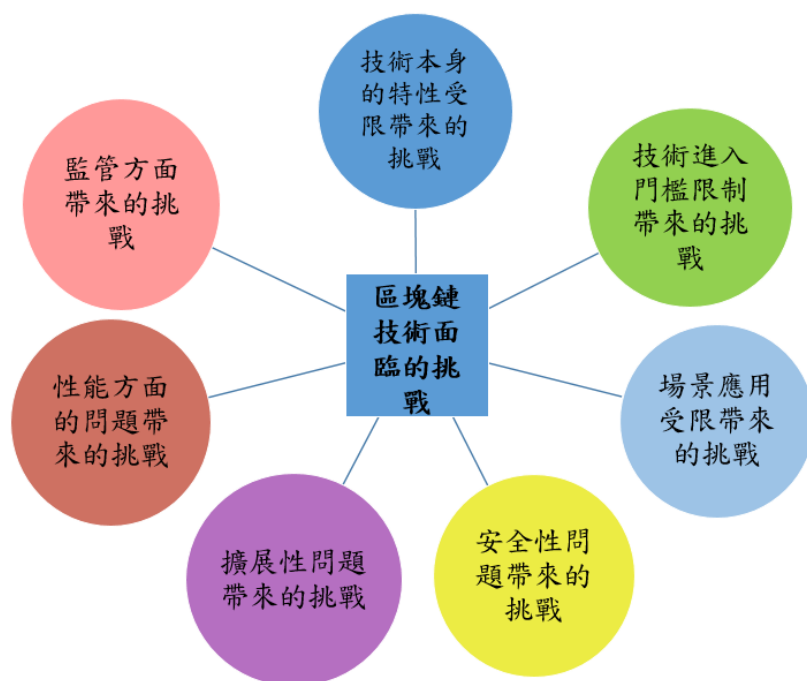


圖 9-2：區塊鏈技術所面臨的七大挑戰

參考資料: (馬兆林,2017)

### 1.技術本身特性受限

在目前區塊鏈 3.0 的應用推廣下，許多跨領域的應用如雨春筍般的一一浮現討論，但往往都紙上談兵居多，徹底落實者少。最大的原因出自於目前區塊鏈本身的交易速度並不快速，而比特幣區塊鏈每十分鐘才能完成一次結算。以我國而言，臺灣大學廖世偉教授與其研究團隊，模擬開發的 G-coin 稱每 15 秒就完成一次結算，而此技術為萌芽階段。如今區塊鏈技術要應用在各行各業的狀況而言，如何提高每秒鐘的交易量是當前最直接面臨的問題之一。

### 2.技術進入門檻限制

由於區塊鏈技術為近兩年所新興的技術，許多的技術開發都為初期發展階段，而區塊鏈本身為一複雜深奧的技術，其中就包括密碼學、加密技術、時間戳、共



識機制、資料庫……。如果非專業領域人士，研讀其技術需要一段時間。倘若又學習開發區塊鏈相關應用則耗時更劇。

### 3. 場景應用受限

對於一般普通民眾而言，區塊鏈仍然是一個陌生甚至沒有聽過的名詞。雖對於科技人而言，此新興技術為目前最熱門技術之一但其確切的應用範圍，以及實際應用還並未達到普及化。區塊鏈目前可談及的應用領域甚廣但如果沒有固定的使用客群，那也只能是曲高和寡的一門高冷技術，可能對於未來的發展趨勢有所不利，將很難突破一般主流市場。舉例而言，「餘額寶」在建立初期，其用基礎的用戶市場，則是站在「支付寶」基礎客戶群的”肩膀”上，神速的建立起自己的用戶群。反觀之區塊鏈並沒有一個前置系統做憑依，因此當務之急應必須找出屬於區塊鏈本身的基礎用戶。

### 4. 安全性的問題

區塊鏈號稱具有安全性的保障，但事情百密有一疏。系統安全性不可能達到百分百的安全，雖然區塊鏈特性上明白指出，如果要篡改資料必須要掌握全網際網路上的百分之五十一的節點，看似非常不容易。但有心人士如果把目標轉移到個人使用者，例如入侵他人電腦、電子錢包。就有可能被攻克，因為用戶間的電子錢包的 ID 的安全性其實是相當薄弱的。因此區塊鏈技術發展也需要重新思考安全性的議題。

### 5. 擴展性的問題

區塊鏈的技術目前在我國內快速的發展中，漸漸的許多應用甚至是跨領域的應用，但對於一些傳統行業而言就形成一種面臨淘汰的危機，舉例而言區塊鏈技術帶來的共享經濟模式正改變著一些傳統的產業(例如:UBER 與傳統計程車、飯店旅館與 AirBnB)。許多接踵而來的經濟問題，改革問題需要有一套規則來控制。或者制定相關法律來保障產業間的平衡問題。

## 6.性能方面的問題

區塊鏈有些特性仍必須要做改進並且妥善使用，例如不可篡改性，寫進區塊的資訊，幾乎不可能再做修改。雖可提升安全性但只要遇到有心人士，刻意把錯誤資料放進區塊鏈，系統也將不能更改。只能重新上傳撰寫新的資料。

## 7.監管方面的問題

目前區塊鏈大多應用金融科技業，因此也衍生出了許多問題。智能合約並非一套十全十美的系統。一但有不法份子利用智能合約的邏輯漏洞，就可能修改、破壞契約的內容，當務之急應該研發出更新的防範機制。



## 二、區塊鏈應用案例探討

### (一)股權眾籌

區塊鏈在股權眾籌中的股權轉讓可參照圖 10，而應用區塊鏈的優勢如下：

- 1.資訊公正公開且透明化。所有的訊息除了公平公正公開之外，也透過區塊鏈的特性，來達到一種難以篡改偽造的機制。
- 2.促進股權流通以及資源共享。讓股權的轉讓或者登記更安全更便利。而在眾籌的平臺系統下，所有投資人和項目都可以實現共享。

#### 1.1.區塊鏈技術在股權眾籌的應用

(1)股權登記管理。區塊鏈可做為電子憑證。目前的股權管理制度幾乎都要消耗人力處理紙本的股權證明。如果只單單一兩筆資料並不會造成太大負擔，但假如紙本資料較多筆時，很容易會有遺失、損毀的一些意外性事件出現。而處理程序會變得相當冗長，使處理效率大大將低。利用區塊鏈將一切數字化的特性來讓股權登記變得更安全。

(2)股權轉讓流通。傳統的 OTC 場外股權交易並沒有一套明文的保障機制，交易雙方都必須要承擔一定程度的風險。目前可透過區塊鏈技術將股權的歸屬確切的記錄在區塊鏈上，股權交易再獲得所有者的私鑰簽名才能通過驗證。透過不可篡改性來保障交易紀錄。

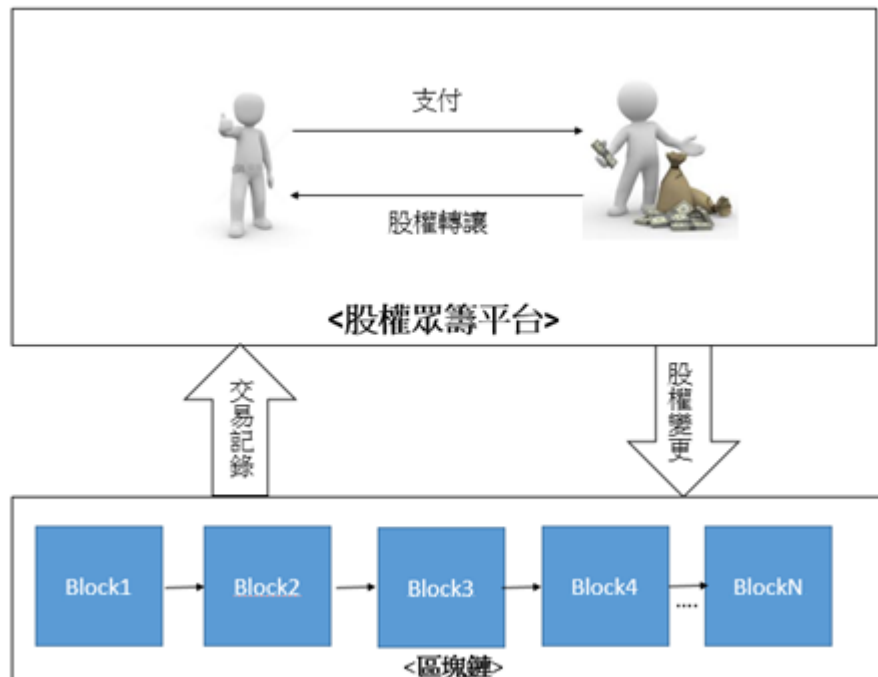


圖 10：股權轉讓流通

參考資料：(梅蘭妮絲萬,2016)

## 1.2.眾籌合約

主要借助區塊鏈不可篡改性，眾籌合約內容可透過智能合約的方式儲存在區塊中，如圖 11 所示，確保合約中的內容的安全性。

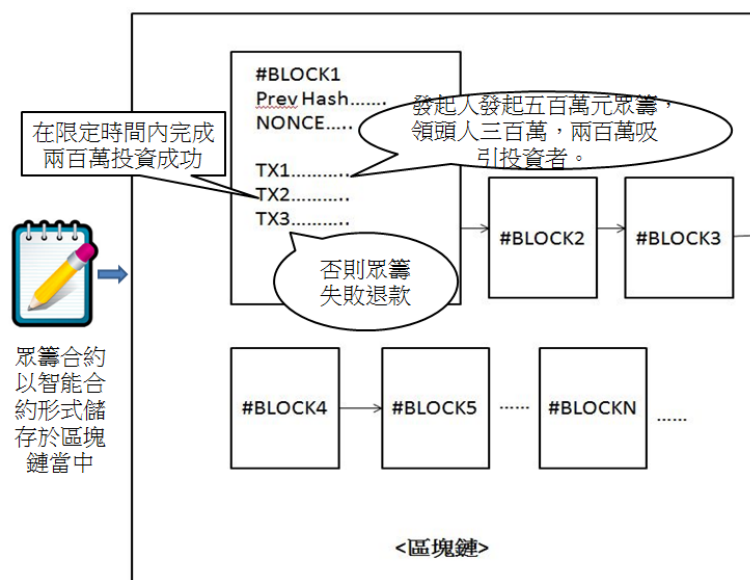


圖 11：眾籌合約以智能合約的形式儲存於區塊鏈

### 1.3.眾籌聯盟與數據共享

股權與股權之間的交易轉讓業務，並非只是由少數公司獨攬大權，應該是由許多獨立經營公司分別進行。而這樣分別進行的結果會導致各方的交易活動較為分散，眾籌聯盟扮演著統合各公司，漸漸的形成一個聯合性的分散式交易中心。

但在眾籌聯盟之間最大的盲點仍然是信任問題，而信任將涉及到組織是否能繼續營運。因此透過區塊鏈技術應用，可以有效的改善信任問題，區塊鏈本身就是一種去中心化的技術。每個眾籌平臺都是區塊鏈上面的節點，而節點都有屬於自己的公鑰與私鑰。在交易驗證，記錄的處理程序裡都為參與者。而監管的機關也可以是眾節點之一，從而觀察紀錄在區塊鏈被紀錄的信息。讓公司與公司之間的活動能更透明。

按照傳統方式來搭建眾籌聯盟，每一個眾籌平臺都有屬於自己的資料庫。對於資訊公開透明化非但沒有幫助，反而還會使共享資訊的流程更加複雜。但加入區塊鏈技術，可以將各個眾籌平臺的用戶、眾籌項目、股權轉移...等資料記錄到區塊鏈上，讓所有的訊息更加透明化，使資訊共享更加便利化。

## (二) 巴克萊銀行的貿易融資交易

在 2016 年英國巴克萊銀行與以色列初創企業 Wave 宣布完成世界首筆利用區塊鏈技術的跨國交易。此筆價值約十萬美元的交易由愛爾蘭乳製品出口企業 Ornua 發起，向 Seychelles 貿易公司出售產品。放眼以往的經驗，通常這類似的交易，為了保障交易雙方彼此的權益，均會請其信任銀行開立相關信用證明，簡言之請銀行為信用背書。如此繁冗的申請過程，其實原因都出自於「信任」的疑慮，一來一往間，往往都會產生許多不必要的成本浪費，甚至可能會遭到有心人士的資料竊取，或者是篡改。如今有了 Wave，運用區塊鏈去中心化無需第三方

介入，透過此技術的不可篡改性省下許多因申請相關文件的時間成本以及規費成本，原本可能需要耗時七個公做天的交易卻能縮短至四小時，而該交易是通過信用機制執行的，因此交易更快，更可靠，更容易審核同時也減少進口商和出口商之間的風險。

Wave 開發的新的基於區塊鏈的系統使用分佈式分類帳技術，用來確保相關機構的所有節點能順利的查看及追縱此筆交易紀錄，而讓原本的轉移所有權和相關資料、交易單單據有效的減少，進而提高確認以及通關的速度。達到提升國際貿易的效率。因此，新系統可以加速貿易交易，降低世界各地公司的成本，並減少欺詐的風險。世界各地的公司都要節省大量的成本和時間，航運業和金融機構預計將成為最大的受益者之一。巴克萊已經確定了可以使用 Wave 系統單獨使用快遞費用實現的直接成本節約，也可以減少完成從幾天到幾個小時的終端交易融資交易所需的時間。

Wave 首席執行長 Gadi Ruschin 曾表示，利用區塊鏈技術確實能提升國際貿易的效率，更可以對貿易的未來產生巨大的影響。通過採用我們的系統，貿易可以更容易，更低成本完成。研究表明，貿易交易的成本高達 5% 來自處理文件，所以運用區塊鏈去中心化無需第三方介入的文件處理，來改善交易過程使交易成本降低。並通過降低成本，將無錯誤的的文檔和將原始文檔快速轉移給全球客戶，在往後執行交易時能快速追蹤交易紀錄並確保交易的完整性。

信任機制往往是商業發展的一大課題。倘若無法有效的處理信任的問題，將會導致交易流程更加繁瑣，所需要的證明文件見多不見少。因此要降低成本提高資訊安全性，就能引用當前最火紅技術區塊鏈，而如今有效利用塊鏈技術真的可以對貿易的未來產生巨大的影響，透過採用 Wave 的系統，貿易可以更加容易並降低成本。透過此案例分析我們能得知，用區塊鏈平臺的特性去推演傳統國際貿易的基礎流程，再按照區塊鏈的特性去模擬各時間點上，這平臺是如何達成降低成本提高效率以及將來的驗證，雖然此平臺仍在建構當中，但卻不失其未來的發



展性，因此本研究整理出生態流程圖、傳統流程圖和交易模擬流程及導入區塊鏈後的流程圖和交易模擬流程，如以下圖 12 至圖 16：

### 生態流程圖(跨國貿易融資)

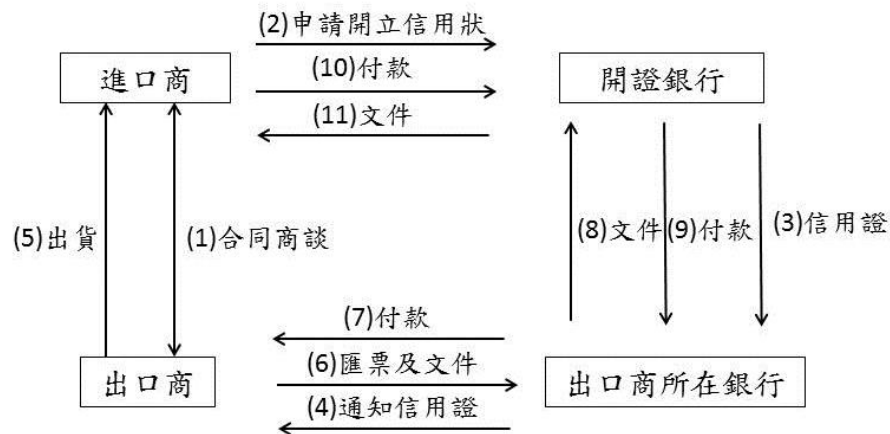


圖 12：生態流程圖(跨國貿易融資)

參考資料: (賴寒彰,2017)

### 傳統跨國貿易融資交易流程圖(融資銀行巴克萊)

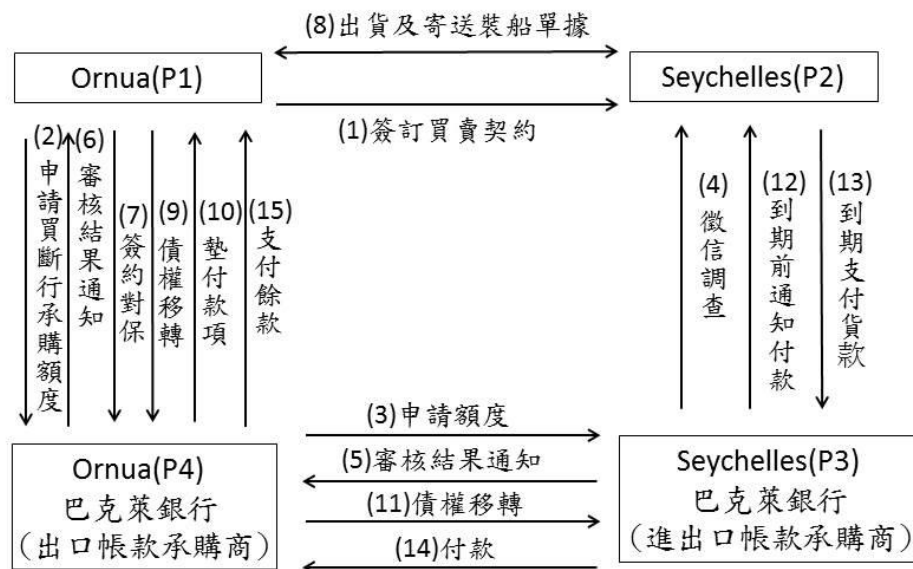


圖 13：傳統跨國貿易融資交易流程圖(融資銀行巴克萊)

參考資料: (賴寒彰,2017)

## 傳統交易模擬流程(通常需要費時七至十天的過程)

時間	P2P	交易資訊
2016/08/08 AM 9:15	P1->P2	簽訂買賣契約, Seychelles向Ornua購買乳酪與奶油
2016/08/08 AM 9:17	P1->P4	Ornua向Ornua的巴克萊銀行申請買斷行承購額度
2016/08/08 AM 10:20	P4->P3	Ornua的巴克萊銀行向Seychelles的巴克萊銀行申請額度
2016/08/09 AM 9:25	P4->P2	Seychelles的巴克萊銀行對Seychelles做徵信調查
2016/08/10 AM 9:30	P3->P4	Seychelles的巴克萊銀行將審核結果通知給Ornua的巴克萊銀行
2016/08/10 AM 11:35	P4->P1	Ornua的巴克萊銀行將審核結果通知給Ornua
2016/08/10 PM 1:30	P1->P4	Ornua向Ornua的巴克萊銀行做簽約對保
2016/08/10 PM 4:35	P1<->P2	Ornua和Seychelles互相做出貨及寄送裝船單據
2016/08/13 AM 11:50	P1->P4	Ornua向Ornua的巴克萊銀行做債權移轉
2016/08/13 PM 13:00	P4->P1	Ornua的巴克萊銀行向Ornua墊付款項
2016/08/14 AM 9:30	P4->P3	Ornua的巴克萊銀行向Seychelles的巴克萊銀行做債權移轉
2016/08/14 AM 9:40	P3->P2	Seychelles的巴克萊銀行通知Seychelles到期前付款
2016/08/14 AM 10:30	P2->P3	Seychelles支付給Seychelles的巴克萊銀行貸款
2016/08/14 PM 1:30	P3->P4	Seychelles的巴克萊銀行付款給Ornua的巴克萊銀行
2016/08/15 AM 9:30	P4->P1	Ornua的巴克萊銀行支付給Ornua餘款

圖 14：傳統跨國貿易融資交易模擬流程(傳統無區塊鏈)

參考資料: (賴寒彰,2017)



## 以區塊鏈機制跨國貿易融資交易流程圖

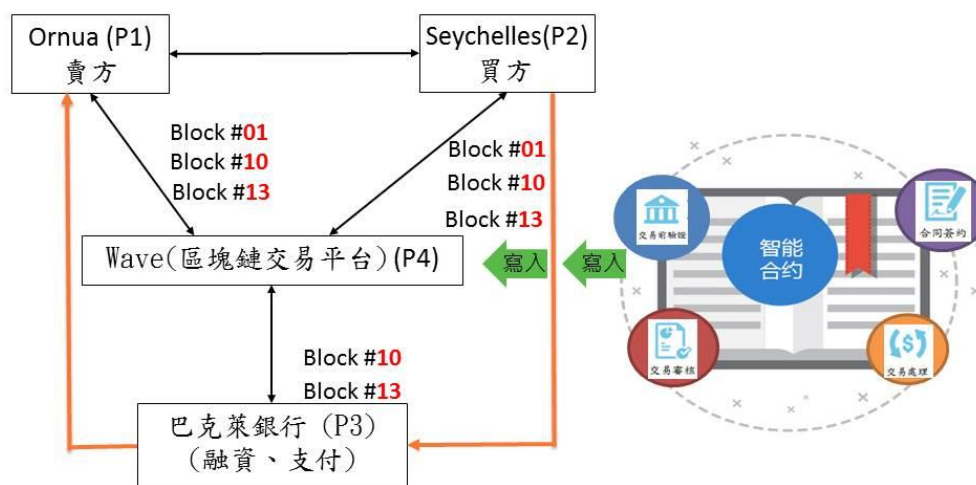




圖 15： Wave 平臺跨國貿易融資交易流程圖(融資銀行巴克萊)

參考資料:(賴寒彰,2017)

## 以區塊鏈機制交易模擬流程

完成傳統程序(1)(2)(3)(4)(5)的交易流程在同一個區塊(block)

P1,P2 <-> P4 透過Wave區塊鏈平台交易簽訂買賣契約, Seychelles向Ornua購買乳酪與奶油

Block ID: Block #01 (雙方簽訂買賣契約) 2016/08/08 AM9:17

TX1: Ornua和Seychelles互相查看上一筆交易記錄

TX2: 雙方簽訂買賣契約

TX3: Wave平台核定雙方契約向巴克萊提出徵信調查及金流的服務

完成傳統程序(6)(7)(8)(9)(10)的交易流程在同一個區塊(block)

P1,P2,P3 <-> P4透過Wave區塊鏈平台交易完成, 巴克萊銀行對P1, P2確定融資、支付後核准程序

Block ID: Block #10 (銀行核准程序) 2016/08/08 AM10:01

TX1: 巴克萊銀行透過Wave平台確定融資、支付後核准程序

TX2: Wave平台核准Ornua和Seychelles交易

TX3: Wave平台交易寄付款通知及送貨通知給Ornua和Seychelles

完成傳統程序(11)(12)(13)(14)(15)的交易流程在同一個區塊(block)

P4 -> P1,P2,P3 Wave區塊鏈平台交易寄付款通知及送貨通知給Seychelles和Ornua, 完成整筆交易

Block ID: Block #13(完成整筆交易) 2016/08/08 AM11:27

TX1: Ornua和Seychelles完成款項給付

TX2: 巴克萊銀行向Wave平台確定款項付清

TX3: Ornua和Seychelles互相做出貨及寄送裝船單據完成這筆交易

圖 16：跨國貿易融資交易模擬流程(運用區塊鏈)

參考資料:(賴寒彰 2017)

## (結論－案例 A-巴克萊銀行)

從傳統作法以及導入區塊鏈後做比較能得知，Ornua 及 Seychelles 利用區塊鏈技術減少了不少的交易的時間，並且增加其效率。更是簡化流程中的不必要因素，和節省了一筆規費成本。區塊鏈的不可篡改性，保障了交易記錄以及相關商業重大規和許多重要訊息，在區塊鏈的眾節點，凡只要不超過百分之五十一就較不會有被篡改的風險存在，從中改變了以往繁冗的文書記錄過程，以及降低了人為疏失所造成的資訊不對稱的風險。本來此案歷的工作天數需要七天至數十天可說是相當繁長，但透過區塊鏈的技術，把處理時間縮短至四個小時內去完成，透過區塊鏈的六大特性分別為，不可篡改性、不可否認性、可追蹤性、私密性、正確性及完整性，使貿易與貿之間更便利、更加安全、具高效率 and 值得信任。

## (三)區塊鏈技術運用於醫療產業：自己的病歷自己管

### 1.傳統病歷

病歷的演進大制上分為三大類如圖 17 所示：

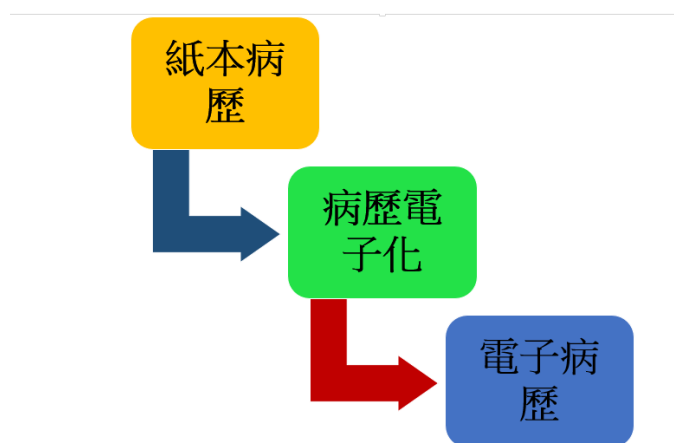


圖 17：病歷演進概圖

1.1. 紙本病歷: 為醫療人員記錄病患相關病史記錄，最為傳統的方式及是用紙張記錄成冊，而後依照時間先後順序歸檔到其病歷資料櫃裡。分為許多不同的醫

療科別。優點為可鉅細靡遺的記載病患的醫療記錄史，以及多為醫生親自撰寫或者手動建檔。缺點為相當耗費人力成本，需要有專業的病歷管理師來負責歸檔。以及付出相當多的空間成本，以新光醫院為例平均每天的紙本病歷的記載量高達 2 萬張，一個月下來就產生 720 萬張，每年就等於累積 720 公尺相當比一座臺北 101(電子病歷到病歷無紙化-薛德興 2016)還高。因此針對紙張消耗量巨大，又不易進行保管，有許多不可抗拒的因素，例如空氣濕度過高導致紙張受潮，或者火災水災。因此推廣無紙化病歷勢在必行。

1.2.病歷電子化: 以推廣病歷電子化的起始年度為 2003 年，當年行政院衛生署(今衛生福利部)在各大醫療院、診所開始推廣病歷電子化試辦計畫，其目的在於想建立一套電子病歷的基本架構流程。並且在 2008 年更推出了「加速醫療院所實施電子病歷系統計畫」。“其目的主要在於提升醫療照護品質及病人安全。”(病歷無紙化推動與成果-鄭天浚、蘇慧芬 2017)並且在於 2009 年與 20 家資訊業廠商做合作，並且利用資訊廠商業者來輔導約 100 家醫院使用電子病歷。因此許多專家一致認為 2009 年為電子病歷的元年。

1.3.電子病歷: 使用電子病歷除了可以更方便的儲存管理之外，還有以下提到的四大好處，第一不用再等待病歷管理員或者護理師，把病歷親自送到醫師面前才進行診療，只要醫生需要病歷，就能透過電腦調閱。第二病人如果需要跨院轉診時，電子病歷也可以跨院，能有效的避免重複檢查甚至事重複開藥浪費醫療資源。第三更有效率的管理病歷資訊。避免意外災害發生時的病歷毀損遺失。但唯一美中不足之處即是資訊安全仍有疑慮。由於電子病歷雖然已經解決許多紙本病歷的缺點，但目前電子病歷仍然還是幾乎由少數人士掌管，只能讓有權限的人士觀看。甚至有篡改的風險。因此我們能透過區塊鏈來改善這樣的缺點。

(phrOS 健康醫療區塊鏈平臺)

在 2017 年 11 月在臺北有一場「健康醫療區塊鏈論壇」，會議中臺北醫學大學附設醫院、數金科技公司共同發表「phrOS 健康醫療區塊鏈平臺」。主打的理

念為「以病人為中心」，把病歷的管理權以及所有權回到病人手上，北醫附設醫院和區塊鏈新創公司 DTCO，合作發表 phrOS 健康醫療區塊鏈平臺，在未來病患可以直接開立個人健康資訊帳戶，匯入所有健康報告，更可以延伸到醫療保險理賠上。除此之外也宣布成立「健康醫療區塊鏈聯盟」，其最大的目標是貫通全國醫療院診所的病歷資料庫，即是發揮區塊鏈當中的分散式帳本的技術。phrOS 是由 DTCO 提供的一套區塊鏈中介系統，提供 API 讓醫院進行使用，由工程師開發透過 API 作各種應用的開發。而 phrOS 在區塊鏈三大類中屬於私有鏈，私有鏈即是代表只有特定人士具有寫入區塊的權限，其管理修改權限也做最嚴謹的控管。PhrOS 會協助北醫把病歷資料寫入私有鏈中，並由院方的管理人員來負責維護節點、並且幫助病患開戶，確認病歷資訊完整性，以及安全跟資訊互通性。且根據各大醫院診所的規模差異，節點的建置的基準點在於依據各大醫院診所的資訊能力與需求，來創立區塊鏈節點，並且連結到 phrOS。大型醫院會是屬於 phrOS 的超級節點（Super Node）、診所會使用輕量型的節點（Light Node），甚至穿戴式裝置也可用來當作迷你型節點。李亞鑫比喻，phrOS 就像是 Google Play 或 App Store 的角色，上面會提供多樣化的應用 App。「phrOS 提供一個平臺、一個作業系統，更是一個整合式的架構。」他說。而 phrOS 是採用以太坊聯盟（Enterprise Ethereum Alliance，EEA）的私有鏈架構為主。

在北醫的應用上，就是當病患到院就診時，北醫可以透過 phrOS 建立一個屬於病患獨有的區塊鏈資料錢包，記錄著病患就診時的各種病歷資料以及就醫過程，甚至是醫生給的建議。醫生也可以根據過去的病歷資料，或是個人的穿戴式裝置蒐集而來的資訊，進行更精準的診斷。其軟體架構如圖 18 所示：

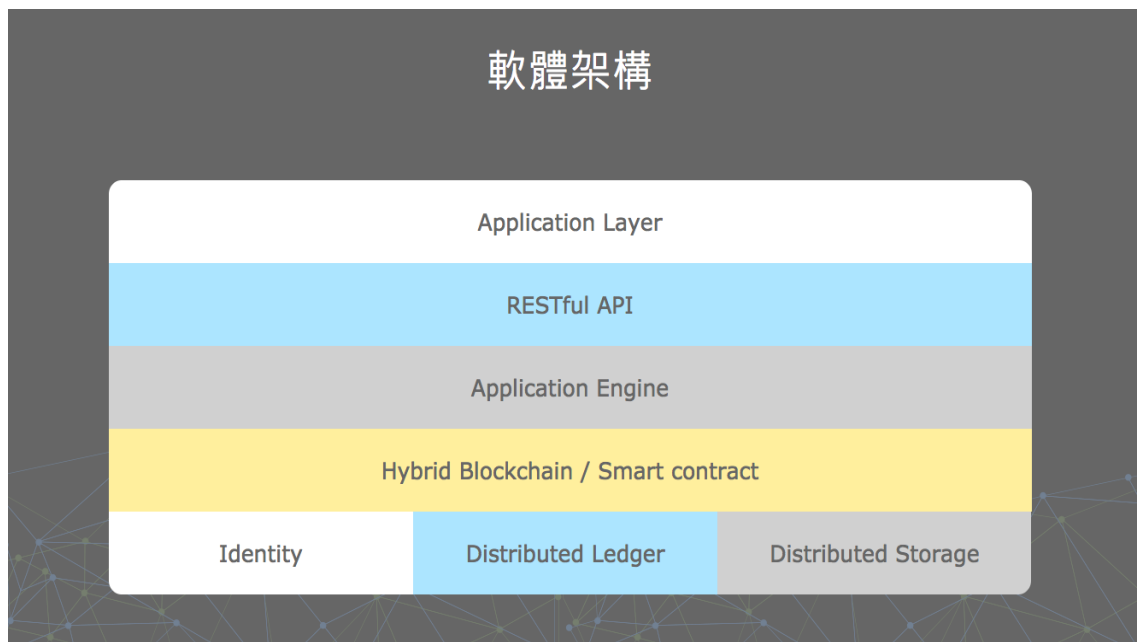


圖 18：phrOS 健康醫療區塊鏈平臺架構圖

參考資料: (沈庭安,2017)

全球醫療產業的現況是每個人的病歷散落在各地，以我國而言榮總醫院和長庚醫院甚至與其他小型診所都會擁有同一位病患的就醫病歷，但礙於就診的地方不同病歷上也只能記錄著本院所的病患病歷資料無法徹底得知病患完整的就醫紀錄，其因資料與資料間並不會自動同步更新成最新的病歷狀態，然後在記錄到資料庫內。所以醫療單位與醫療單位之間極有可能是存在於資訊不對等的情況下。假如病患的身體不適應於某種藥物，再加上病患本身忘記提醒醫護人員，這配藥吃藥一來一往所造成的嚴重後果令人不敢想像。而在這樣資訊不對等的情况下也很有可能醫療機構作出重複檢查或重複給藥的情況，無意間便浪費了珍貴的醫療資源。對於我國全民健保長年虧損的情況下相當不利。為了避免上述的情況出現，目前能透過區塊鏈把醫療院所的病歷資料庫串聯在一起，並同步更新。其最後得結果紀錄進區塊鏈中，透過可追蹤性以及不可篡改性來保障個人病歷的正確性。如區塊鏈創辦人許明恩指出，在我國健保體系下，許多治療、檢查項目幾乎是健保給付，或者健保占絕大多數的補助，在這樣的國家社會福利的制度下，對於生



病就醫治療的負擔感相當輕微，甚至可能遭到濫用。在國外，如果無健保的情形下，多做一項治療或檢查就得多花費數百或數千元，因為負擔感相當明顯就會開始思考應該要如何避免重複花費。要避免重複檢查治療，就必須要親自到原醫院申請紙本病歷攜出，或是請醫院透過病歷交換中心來交換彼此資訊，長庚醫院才會看到我在榮總醫院的就醫病歷。phrOS 健康醫療區塊鏈平臺就是想解決跨機構資訊不互通的問題，病歷不再是由醫院或機構各自保管，而是放到一個專責保管病人資料的非公開區塊鏈上，而區塊鏈允許醫療院所寫入病歷、健檢資料，或是穿戴式裝置寫入健康數據。

從申請保險理賠的角度而言，因為保險公司知道區塊鏈上的病歷、健檢資料是只有特定機構才有寫入權限(私有鏈)，而健康數據則是參考用。因此保險公司只要獲得病人授權查閱區塊鏈上的資料，就可以直接從區塊鏈上得到病患的個人病歷資料，而病患本人就能省下許多紙本申請流程的時間成本。目前大多數民眾對於本身病歷的管理較無一全盤性的思考與管理，針對目前醫療機構是否使用區塊鏈，其實對於個人的價值衝擊並不大。反觀之醫療區塊鏈對於保險公司的理賠確認流程有著更大的影響，因為不需要耗費過多的人力資源成本，一一檢查醫院、診所病歷的真假，而只要跟病人取得區塊鏈資料的授權即可。

從個人資料保護的角度來看，授權取用病歷的鑰匙握在每一位病人手上。因此，無論是醫院要做學術研究、保險公司要申請理賠或政府統計需要調用資料，未來可能都得經過病人手上的那把鑰匙才能從區塊鏈上取用資料。但這只是技術上可以這麼做，詳細如何運作還是得看 phrOS 實際上線的功能而定。

#### (四)用區塊鏈平臺向全球投資者兜售房地產

##### 1.傳統房地產轉移

根據財政部相關資料顯示，以下的相關流程與法規如圖 19 所示：

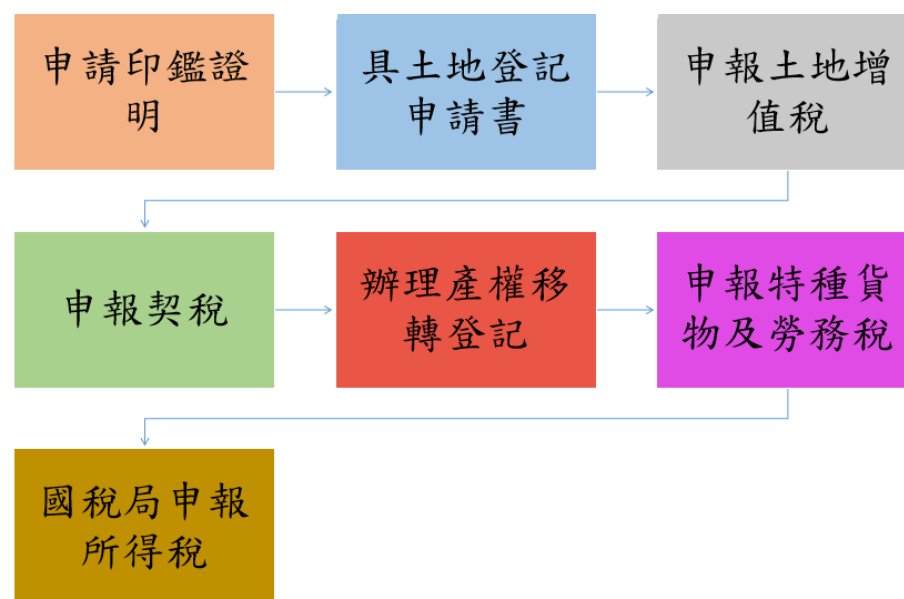


圖 19：財務部土地房產轉移流程

##### < The Propy >

區塊鏈技術的一大重要特性，就是支付流程的完全透明。只要是個節點都有一份分散式帳本，其特性除了可以增加區塊鏈上的訊息，更可以透過其可追蹤性來確認目前資料的狀態以及內容。目前將區塊鏈技術與房地產投資領域做結合應用，似乎是“天作之合”。創建於 2015 年的美國房地產交易平臺初創公司 Propy，本月起在烏克蘭正式啟動試點運營。此公司的去中心化平臺，宗旨在創建一個全球投資者都可以自由買賣的房地產交易市場。而其理論基礎，正是區塊鏈技術帶來的方便快捷的跨境支付方式。目前該平臺已與烏克蘭的電子政務機構展開合作。烏



克蘭政府將使用 Propy，向持有數位加密貨幣的外國投資者提供不動產和物業服務。這也將是區塊鏈技術首次被應用於數位加密貨幣市場以外的領域。

證明區塊鏈技術不單只能應用在傳統數位加密貨幣市場，對於資產轉移之相關證明都具有其實用性。區塊鏈技術較符合公平公證公開原則。其不可篡改性可針對資訊安全部分做有效的加強，因共識機制需要符合百分之五十一以上的節點的驗證，因此大大提升資料被篡改的難度。無論在公有鏈或私有鏈亦或者是聯盟鏈上，只要是其合乎條件的相關使用者，皆可以利用可追蹤性來確認區塊鏈上的所有交易紀錄。

而本案例則是一種資產轉移的證明機制，正可透過區塊鏈來解決傳統資產轉移的種種不方便之處。進而提升其財產轉移的效率。Propy 系統架構如圖 20 所示：

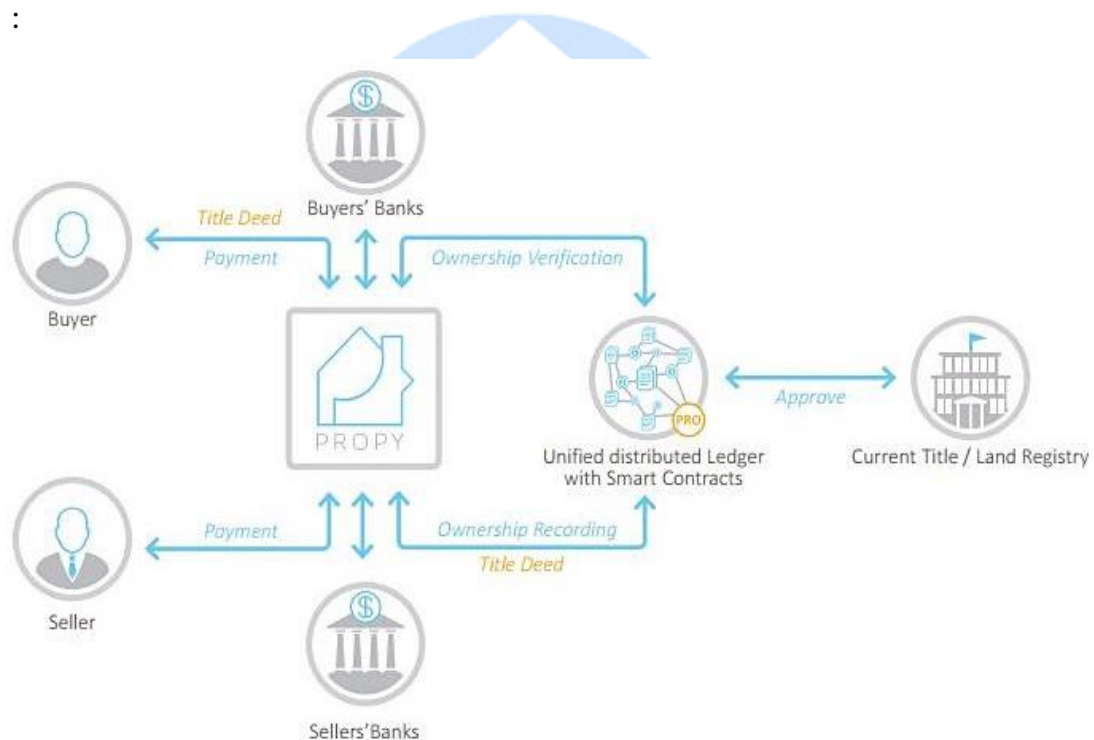


圖 20：Propy 系統架構圖

參考資料: (The Propy Registry)

## (五)MIT 以區塊鏈打造數位文憑

麻省理工學院（MIT）於 2017 年夏天執行一項計畫，即是運用區塊鏈技術讓 111 名畢業生透過使用行動載具的行動程式來領取他們的數位文憑，這項創舉讓麻省理工學院成為全球首批頒發虛擬證書的大學之一。MIT 數位文憑採用區塊鏈技術，當學生下載 Blockcerts Wallet 後即產生一組公鑰與私鑰，並且將公鑰傳給 MIT 寫入數位紀錄中，並在該區塊鏈中加上認證碼，區塊鏈上並沒有文憑資訊，只有 MIT 建立該紀錄的時戳，MIT 再寄出含公鑰的數位文憑，由學生手機上的私鑰驗證本人。

MIT 數位文憑系統切中了本研究的探討主體，證書的驗證系統。由於目前許多學生畢業後即將投入職場工作，在向公司面試官遞上書面審查資料時，第一頁往往都是自己的履歷，以及相關成長過程。其中學歷又是普遍面試官較容易注意到的主題。因此對於面試官而言，該如何確定面試者的學經歷為正確，而非偽造，這是一直以來就受到重視的課題。普遍而言雇主會委託公司的人資部門來確認，或者是自己致電到該學校詢問，但這一來一往的時間相當冗長，如果公司需要一份證書正本以茲證明，那申請流程又更細碎冗長了。

目前可以透過區塊鏈技術的改良，用以改善耗時耗力的問題。利用區塊鏈技術的特性，除了可確保證書資料訊息不被輕易篡改，也可追蹤自己本身的證書資料，並能在行動載具上顯示自己本身的相關證書，以及分享自己的證書資訊。如果在面試的當下就能提出有效的方式來證明自己本身證書的真偽。定能提高面試效率。從中節省的時間成本以及金錢成本，可以做更有效的運用。

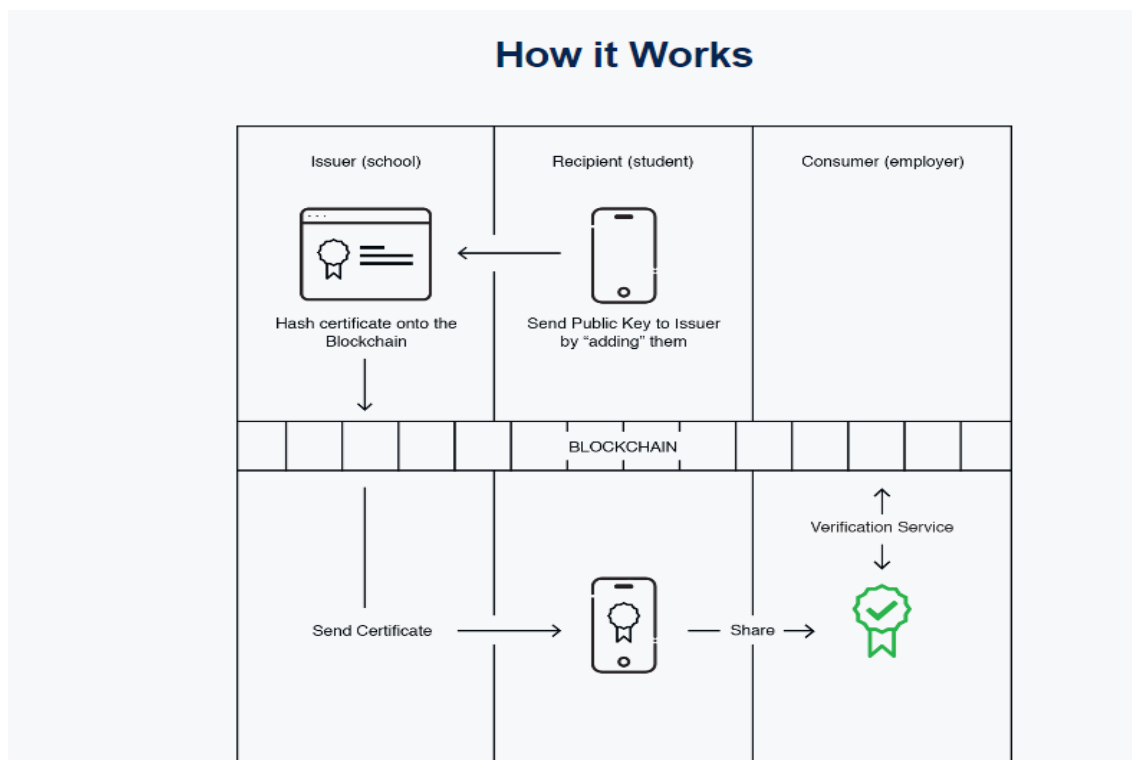


圖 21：MIT 區塊鏈數位文憑系統示意圖

參考資料:(MIT,2017)

## (六)數位國小畢業證書

區塊鏈議題應用領域業越發廣泛，臺中市政府與國網中心一同運用區塊鏈技術將小學畢業證書，打造出可用QR Code驗證的區塊鏈證書檢驗平臺，實驗階段已經有3間學校加入，並且預估在107年畢業季正式上線。蕭景燈表示，即使小學畢業證書的用途不大，唯一的使用情境只有在國中入學繳交畢業證書時，但是，臺中市期望透過小規模的試驗，將不同場域的情境慢慢串聯起來，教育單位可以透過這個機會一同參與和討論。學生也能透過此應用場景，體驗數位身分交易的過程，進而培養數位國民。

「現今的畢業證書是全權由學校的教務處製作，曾有發行假學歷的案例！」雖此平臺目前正處實驗階段，並且也確實有3所學校投入。但學歷造假的事件並非空穴來風，類似的案例層出不窮。負責該專案的國家高速網路與計算中心副研

究員葉羅堯表示，畢業證書是具有公信力且能夠證明自己的專長的呈現形式，但是，過去曾有學校發行偽造畢業證書的案例出現。他說，確實有必要驗證證書的真實性，傳統由學校教務處發行紙本畢業證書的方式，過程非常繁雜，畢業生必須親自至教務處辦理離校手續，驗證的過程也相當耗時，都需要透過人工的方式審核並簽署，最後才發放紙本畢業證書。其中所花費的人力成本以消耗的時間都相當可觀，為了要杜絕這樣浪費資源的狀況，區塊鏈證書檢測平臺也許是一項能有效改善此困境，並且具有公信力的一套系統，而區塊鏈證書檢測平臺是透過以太坊（Ethereum）公有鏈，加上Swarm (集群)分散儲存畢業證書資訊，最後再透過QR Code來驗證。葉羅堯表示，這次小學畢業證書區塊鏈的應用，是參照麻省理工學院(MIT)日前推出的數位證書Blockcerts應用，讓111名畢業生直接透過智慧型手機的App，領取畢業證書。但並非每個人都願意公開自己的畢業資訊，於是臺中市與國網中心這次合作的小學畢業證書計畫，就透過掃描QR Code的方式來檢示證書資訊，且建立起具有隱私性的證書驗證平臺。現有的畢業證書只經過教務處驗證。區塊鏈證書檢測平臺為多人驗證法，至少需要3個人以上簽署，才能觸發系統進行發放畢業證書，此平臺更可追蹤簽署的進度狀況，不可篡改的特性，可以有效的避免在操作系統的過程中，或者是傳統發放證書的流程中，有心人士的惡意破壞或者是篡改。寫進區塊鏈中，透過其可追蹤性來查找之前的變動記錄。只要此用戶為區塊鏈所認可的節點都能進行觀看。除此之外，為了讓證書更家私密化，所有傳輸和儲存的過程，都加密處理，來確保證書的隱私性。為了確保證書的真偽，葉羅堯在既有的畢業證書上，加上QR Code的設計，但是該QR Code並非像連結到一個網址，「為了去中心化，系統不會儲存完整的畢業證書電子檔，」他表示，國網中心透過P2P的檔案儲存系統Swarm，在Swarm 中儲存部分畢業證書的資料，且將這些資料經過加密處理，來達到隱私性的目的。

葉羅堯解釋，QR Code就類似用戶個人識別號碼的概念，畢業生掃描之後，可以到區塊鏈上找到部分資料，解開後即可驗證，區塊鏈上的畢業證書可與手邊

的畢業證書做比對。

## 1. 區塊鏈證書檢測平臺系統流程

臺中市目前希望不要直接影響或者間接影響目前已有的畢業證書發放流程，可以讓學生選擇是否有需要電子證書，若學生願意使用電子證書，可以在區塊鏈證書檢測平臺上註冊，註冊完成後將畢業證書上傳至平臺，系統會自動產生一份JSON檔形式的智能合約，包含姓名、地址和證書的PDF檔案。之後系統會將這份智能合約，轉成Base64的字串，透過教網中心指定驗證單位，驗證人可能是老師、教務處等，經過多人、多層的簽署之後，系統會將該畢業證書資訊，記錄到區塊鏈上。產生JSON檔和QR Code供學生保存，JSON即是電子版的畢業證書日後學生若需要驗證畢業證書時，可上傳電子版畢業證書或是QR Code給接收單位，像是雇主或是升學單位，接收單位可透過區塊鏈上的記錄進行驗證。葉羅堯強調，在區塊鏈上傳輸的每一筆資料，都經過加密混淆，使他人無法看到傳遞的內容，再者，教網中心為證書發行人，他人無法追溯到發行的學校單位，而區塊鏈證書檢驗平臺也採用分散的方式，儲存畢業證書，學校教務處、驗證的伺服器和區塊鏈的Swarm都沒有儲存完整的證書檔案，因此，能夠確保畢業證書的隱私性。電子證書系統架構如圖22所示：

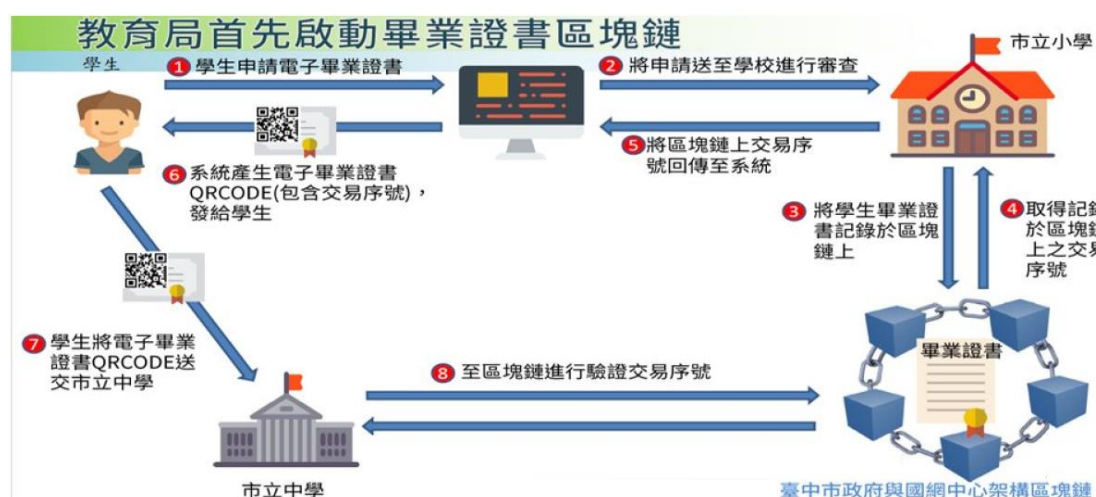


圖22：電子證書系統架構

參考資料:(蕭景燈,2017)



### 三、數位文憑(Digital Diploma)

近年來由於升學管道暢通，基本國民教育延長之故，漸漸的以臺灣現今的社會概況而言，可說是人人有書讀，人人都是大學生。不同以前聯考時代大學錄取率相當低，先不談及大學升學率與否。且再過往教育體制下仍有留級的制度存在，一位學生能否在修課期間順利修課完畢，而後拿到畢業證書都是一個未知數。綜觀之前社會也較少有關證照考取的相關資訊以及機構。因此發證發照就顯得較無急迫性。可是綜觀目前社會需求，往往都看著履歷上的資料，看著學歷畢業證書、相關能力考照。因此舊有的發證流程也漸漸的顯得冗長且不合時宜。因此近年來推廣著數位文憑(Digital Diploma)的發行。

「文憑」在漢語大辭典第 9527 頁第 6 卷中解釋有兩種意思，第一種為作為憑證的官方文書，例如在《水滸傳》中第五十五回提到「當下凌振來參見了高太尉，就受了行軍統領官文憑。」第二種解釋為教育單位發給修業完畢的學生的一種證明。在鄭觀應所著的《盛世危言·考試上》中提到：「考取文憑，方准用世。」

但在現今社會的普遍解釋為畢業證書、證書證明。在這時代許多應徵場合都需要一份屬於證明自己能力的物件，產證發照的流程理應而言應該相當流暢以及點單化。可是目前來說文憑證明相關物件仍然為紙本導向，近幾年我國政府以及各界均紛紛響應環保政策，嘗試將目前紙本物件慢慢的向無紙化邁進，進而達到愛地球作環保的概念。

數位文憑，一個新穎的辭彙。在 2017 年夏季麻省理工學院(MIT)執行了一套前導計畫。掌管 MIT 註冊服務的 Mary Callahan 表示，當他讀到有關區塊鏈的相關文章的時候，就立刻創意發想是否區塊鏈是否可運用於儲存學生相關記錄，舉例而言，畢業證書。而後他便展開了實驗追求這個目標。而在 2016 年 MIT 的媒體工作室並與機器學習的公司展開一連串密切的合作，並且開發了 Blockcerts 的

開源工具包，機器學習公司的執行長 **Chris Jargers** 表示，在各界鑽研的區塊鏈上也許已經有許多自行開發的程式技術，但公司採用的仍然是比特幣區塊鏈技術。對於他們而言比特幣才是一個準則。

MIT 的數位文憑簡言之，學生如果下載 **Blockcerts Wallet** 之後，他會產生工鑰與私鑰，並寫進數位記錄裡透過區塊鏈加上認證碼。區塊鏈並沒有記錄文憑資訊，只記錄建立此筆資料時的時間戳，最後再藉由 MIT 寄出附有公鑰的數位文憑，然後透過學生手中的私鑰進行解密動作，以及驗證身分。

而在於推動數位文憑，我們必需要先擬定一套發證流程。來保障每一位文憑持有人的權益。相關權益為具有文憑申請權利、確保文憑上的資料無誤、縮短傳統文憑曠日廢時的發證流程、以及分享文憑的權利。因此在本研究中嘗試將上段提到區塊鏈技術，用以改善傳統的發證流程。進而達到一種全新的更快速、更方便、更安全的改革。由於上述提及目前文憑所包括的不僅僅只是畢業證書，文憑他有可能是代表證書、證照甚至是權證。本研究將著重於改善傳統發放畢業證書繁瑣的流程，並以某科技大學的傳統發證流程加以改良。



## 四、區塊鏈目前三大主流

### (一)比特幣(BITCoin)

在西元 2009 年 1 月 3 日時，一位名作中本聰的人發表了一款日後家喻戶曉的數位貨幣「BITCoin」，發表點對點的電子現金系統中對等網路開源系統，以及雜湊函式系統。最初中本聰只發行了 50 個比特幣。並且在 2010 年進行了比特幣購買商品的案例，當時用著 10000 個比特幣買了兩個披薩。在 2011 年突破了一個比特幣換得 1 美元。起初各界都不看好的比特幣如今卻暴漲成當紅數位貨幣，在 2017 年 12 月 7 日，竟又破天荒價格上漲到一枚比特幣兌換 15000 美元。這對於當初投資者而言都是始料未及的突破。也讓當初踟躕觀望者捶胸頓足。

維基百科的比特幣條目對比特幣定義如下「作為現今最廣為人知且廣泛使用的虛擬貨幣，比特幣(BITCoin)是一種全世界通用的網際網路加密貨幣。比特幣採取對等網路開發的區塊鏈。比特幣他的價值就在於去中心化以及創始區塊鏈以及共識決。而比特幣他也如中本聰闡述的一樣是一種點對點的電子現金系統，演變至今我們通俗給予一個名稱為「數位貨幣」。」

使用密碼學機制來作為數位貨幣的交易，不用再透過第三方機構來維持保障其貨幣發行權以及防止惡意的增加或者是減少。交易的經過必須要透過網路上的各節點來驗證。所以比特幣也被一致肯定是一種電子的加密貨幣(Cryptocurrency)，可是水能載舟亦能覆舟，有不少不法人士因為比特幣並不受第三方機構所監控，因此經常拿來作為洗錢或者非法交流。的媒介。(黃宣凱,2017)

比特幣是經由「挖礦」的過程中產生，礦工會透過處理計算出複雜的加密密碼來取得作為報酬的比特幣，或者得到剛產出的比特幣。雖然有時並非一個完整的比特幣，但望至今日比特幣的匯率就能得知，即使非一顆完整的比特幣其價值也相當驚人。購買比特幣的用戶可以使用個人電腦、行動載具申裝網路上的電子錢包軟體來交易比特幣，目前有相當多款可交易比特幣的網站或者App，例如：BitoEX、Plus500.....等。

## (二)以太坊(Ethereum)

以太坊，近年來為區塊鏈的主要開發程式之一，而以太坊的特色為可以在任一平臺中建立以及發布，以及去中心化的應用程式，屬於一種開源式的區塊鏈平臺，讓眾多開發者一同維護這基礎架構的發展(Ethereum community,2017)。並且以太坊也發展出另一種不同於比特幣的幣別「以太幣」。為他人津津樂道的是比特幣跟以太幣的差別為何？目前以兩種幣別大不同的地方是以太幣較具備圖靈完整(Turing Complete)的特性，為一種智能合約的區塊鏈技術。而其應用目前最著名的是與多中心自治組織(Decentralized Autonomous Organization)所建立起的應用。以太坊的發展呈現如圖23。

### 1.以太坊發展史

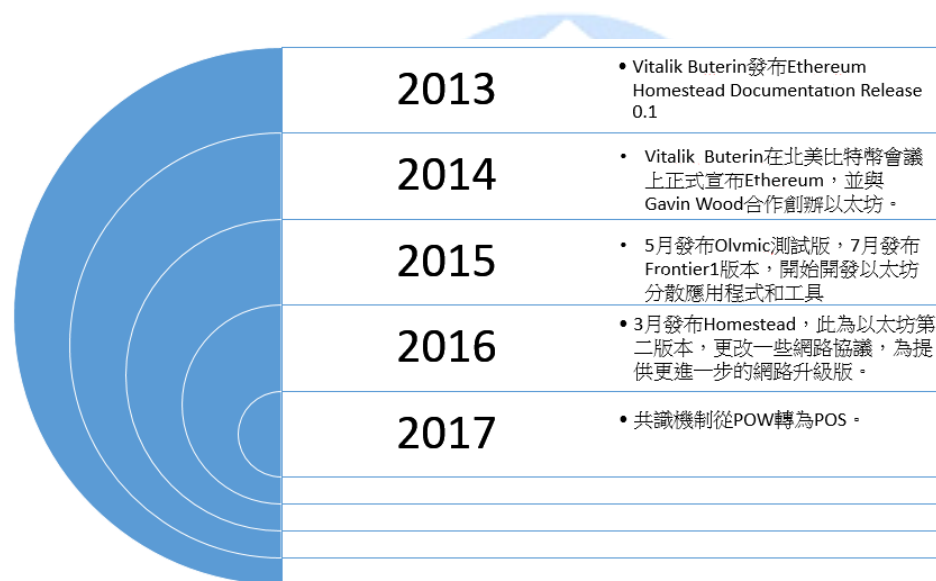


圖23：以太坊大事記

參考資料: (壹讀,2016)

### 2.以太坊特性

- (1)以太坊每14秒就能產生一個新的區塊。
- (2)區塊容量並非如比特幣限1MB，則是無限制。
- (3)智能合約。

### (三)超級分類帳(Hyperledger)

Hyperledger執行董事Brian Behlendorf曾表示，透過分散式帳本和智能合約，Hyperledger正在顛覆全球的產業。而世界不單單只有一個帳本，而是有各式各樣的帳本以有趣的方式交織在一起。而其中Fabric為Hyperledger底下的五個子專案中的其中一項，具備著區塊鏈中的分散式帳本以及智能合約。而Fabric的智能合約為Chaincode，使用的開發語言為Go語言，並且使用Docker容器來執行。就像以太坊利用以太坊虛擬機器(Ethereum Virtual Machine，EVM)來運行智能合約一樣。

Hyperledger Fabric 是分散式帳本(DTL)的顯著應用。可以在區塊鏈體系中，提供給使用者一個具有高安全性，可擴展性，機密性的主要保障。目前幾項關鍵數據可供讀者作參考。關鍵數據共有四大點如圖24所示：



圖24：Hyperledger Fabric關鍵數據

參考資料：(ITheme我們正用區塊鏈重新發明這世界,2017)

## 五、技術接受模型(Technology Acceptance Model)

技術接受模型，又稱為科技接受模型。此理論並於 1986 年由美國一位學者 Frand D. Davis 所提出，根據理性行為理論在信息系統以及計算機技術領域推導而來。技術接受模型主張人對新穎科技的使用以及接納，是受到行為意圖的影響下所做出的反應。且該理論認為當人面對一新穎技術時有兩大感知性為決定因素，分別為感知易用性(Perceived ease-of-use)、感知有用性(Perceived usefulness)。以本研究證書發證管理系統而言，針對兩大感知性做解釋。

感知易用性(Perceived ease-of-use)：在使用本套系統時，減少資訊被篡改的疑慮，刪減傳統繁冗的流程，去繁從簡增加效率。

感知有用性(Perceived usefulness)：以學校端而言，產發證流程更精簡且證書資訊的安全性更可靠。以學生端而言，不必再親自到校才能列印、查詢證書，只要在自己的電腦上做操作即可，更可直接做分享至企業人資端提供證書查驗。企業端驗證證書真偽時不必再等學校端約 2 個工作天，就能得知證書的真偽。

## 六、紮根理論(Grounded theory)

### (一)紮根理論的定義

早在陳昺麟(2001)提出，社會科學質化研究的紮根理論實施程序及實例之介紹中提到，紮根理論最早是由 Barney Glaser 和 Anselm Strauss 這兩位社會學家提出(Strauss & Corbin,1990)。要瞭解紮根理論，Strauss 和 Corbin (1998)認為紮根理論是一種「方法論」(methodology)，是一種研究社會真實存在和思考的方法。接著，其目的為創立理論研究實，需要採取方法來搜集和著手分析資料，常用的資訊蒐集的方式分別為觀察法以及訪談法，而是用開放式編碼(open coding)、主軸編碼(axial coding)及主題編碼(selective coding)等過程來分析資料。在目前我們常提到的所謂紮根理論是質性的研究方法中，透過蒐集資料後加以分析，而後做歸

納的方式，並且對分析結論再加以分析整理所得的結果。簡單來說，紮根理論是經過一套系統化的資料搜集以及資料分析，進而得到一項結果、以及得知一套屬於該基礎理論的發展脈絡，以及暫時驗證過的理論。紮根理論並非為探討舊有的理論基礎，而是借由搜集資料解釋現象而到的理論。並且嘗試解釋提出的理論並佐以資料來驗證。紮根理論的目標是要去建立能忠實反映社會現象的理論（徐宗國,1997）。簡言之，紮根理論是「紮根」在研究者所搜集資料上，再將零星片段的資料做歸類、進行分析、最後統整為某些現象所衍生出來結論，再經由持續不斷的更多個案資料搜集，為求理論的充分驗證，得出紮根於實地資料的理論(陳昺麟,2001)。

## (二)紮根理論的相關理論

對於紮根理論的相關資料中，Strauss 和 Corbin 兩位學者早在 1990 年發表”Basics of Qualitative Research : Grounded Theory Procedure and Techniques.”書中(Strauss & Corbin , 1990)，並且只用兩頁得文字篇章來提到紮根理論的理論的主要精神為「實用主義」(pragmatism)和「符號互動論」(symbolic interactionism)（徐宗國， 1996）。因此，以下將以「實用主義」(pragmatism)和「符號互動論」(symbolic interactionism)來討論紮根理論的相關理論：

### 1.實用主義(pragmatism)

徐宗國(1996)，在文中提到，可以視實用主義對紮根理論有著深刻的影響，而紮根理論為應用實用主義到社會現象的研究過程。首先，「開放式編碼」就是指把所觀察或訪談的資料逐字、逐行拆解；撰寫、整理備忘錄及寫作，這都是一種綜合迴歸的工作，實用主義對解決問題的方法即是分解與綜合。實用主義影響下，從事相關研究者所選的研究題目這種想法通常來自日常生活的經驗、實務工作中待解決的問題，而不是完全來自理論引導下的假設驗證或檢驗，所以紮根理論有顯著的實用性格。

## 2.符號互動論(symbolic interactionism)

黃政傑(1998)指出，符號的互動論和現象學派觀點類似，基本都是假定認為人類行為是由解釋做為中介。符號互動論者的中心思維是一切的現象、情境、理論都是需要人們去發現它，並且嘗試了解並且解是它使其逐漸變得有意義，舉例而言現象或者是理論本身並不具任何實質意義。解釋是透過與社會情境中的其他人協助而發生的這類互動，專家學者或者研究者就可以逐漸建構起其中意義，而裡論現象本身不會自動的發生行為，而是在一種既定情境中的人有共同的認知並且經過互相討論後所衍生出來的定義。

## 3.理論淵源對紮根理論的影響(Strauss & Corbin,1998)

紮根理論的理論基礎，可能產生以下的影響：

- (1) 研究須要實地進入場域，去發現正在發生的事情。
- (2) 強調紮根於真實資料的理論與學術發展和社會行動基礎都有關聯。
- (3) 瞭解各種社會現象和人類行動之複雜性和多變性的特質。
- (4) 瞭解在問題情境中，人扮演著活動性的行動者角色。
- (5) 明瞭人類行動背後均具有某種意義。
- (6) 瞭解各種訊息是在互動的過程中一再地被定義。
- (7) 對事件發展過程應具有敏銳度。
- (8) 能夠察覺事件的結構、過程和結果的關聯的重要性



## 參、系統開發

### 一、系統緣起

根據上述文獻探討能得知傳統區塊鏈產發證流程，安全性以及便利性仍有所不足之處，閱讀提及的區塊鏈應用的相關案例，了解區塊鏈技術應用在證書證照的應用逐漸成為一種趨勢。根據技術接受模型得以了解區塊鏈應用於證書發證系統所帶來的使用者感知影響，以即透過紮根理論加以分析傳統與區塊鏈改良後的差異性。

### 二、系統架構

而在本章將解說學校傳統產證發證的流程，並詳加敘述其流程作業時間，以及透過區塊鏈來簡化傳統的流程。區塊鏈畢業證書發證系統的架構，學校端如圖 25 所示，學生端如圖 26 所示：

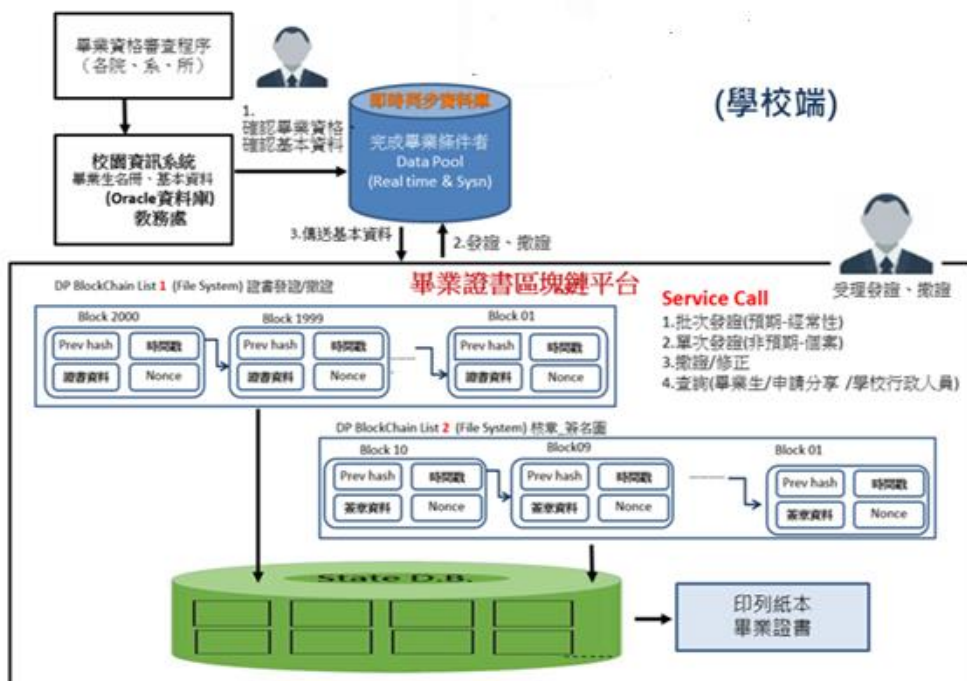


圖25：區塊鏈畢業證書發證系統(學校端)



先從畢業資格開始審查，必須先從各院各系各所深入來驗證畢業生是否符合畢業資格，確認畢業資格之後放進校園資訊系統內包括，畢業生名冊以及基本資料。都會放進學校的Oracle資料庫內，並且透過即時同步資料庫與畢業證書區塊鏈平臺。學校資訊系統會先確認畢業生資格，以及基本資料。而後在畢業證書區塊鏈平臺中記錄，每一個區塊內都記錄著證書相關證書資料。並且在學校管理者端建立四大主要業務，批次發證(預期-經常性)、單次發證(非預期-個案)、撤證/修證以及查詢畢業生/申請分享/學校行政人員。而證書資料會因為證書記錄的階段不同，狀態也會有所不同。而State資料庫則是記錄證書資料的最新狀態，因每一種狀態呈現，都代表著證書資料的現有的流程進度。因此有必要徹底區隔記錄，讓產證、發證以及撤證都能明確的被記錄。

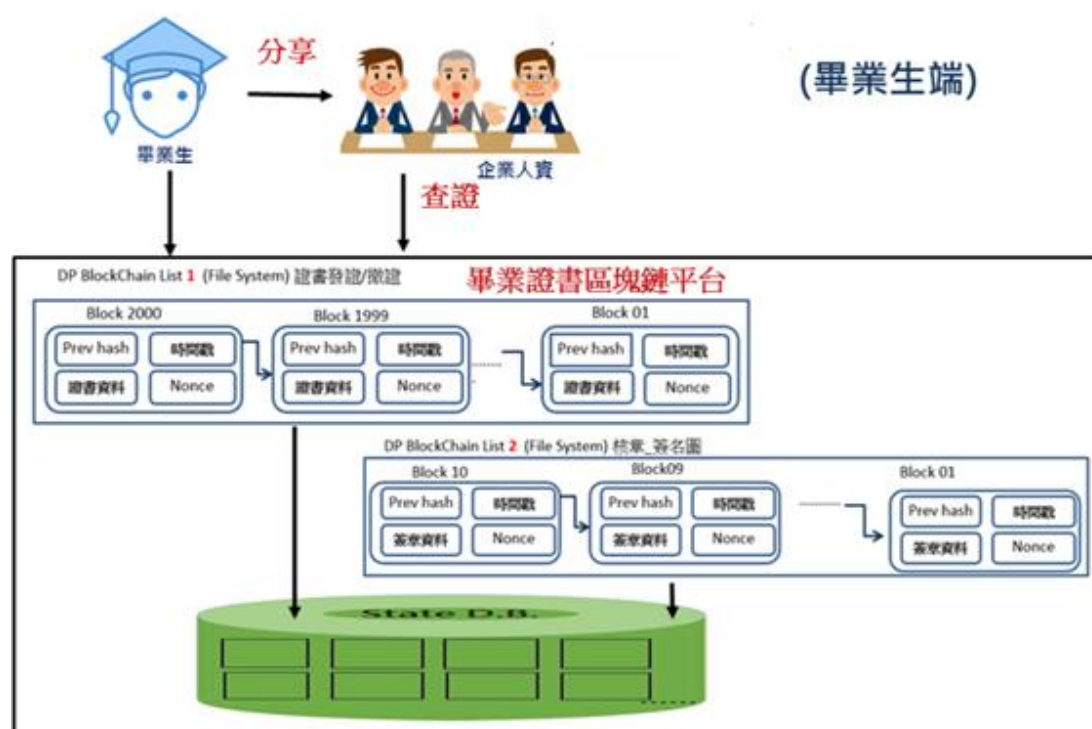


圖26：區塊鏈畢業證書發證系統(畢業生端)

而畢業生可透過畢業證書區塊鏈平臺進行查證與分享的動作。如果遇到求職者，透過面試而準備進入公司展開職涯的時候，公司裡面的人資部門就能透過面試者提供的分享連結(具時限性)，來查證畢業證書上的資訊是否符合事實，進而

做出最有利雙方的判斷。

### 三、開發工具

#### (一)選擇 Hyperleger 開發

上述分析完成 Ethereum 以及 Hyperledger Fabric，最終本研究仍然選擇 Hyperledger Fabric 的原因為，基於本研究為「區塊鏈校園應用：以證書驗證管理系統為例」，其目標為把證書驗證系統實質商用化。並非單單只做為學術研究。然而以太坊的創立雖然早於 Hyperledger Fabric 但應用其平臺 API 仍需要付費，而且並不只做單一專案結帳，而是每使用一次 API 都要進行收費。對於仍然處於實驗階段的開發者而言相當不利，在成功結果的背後往往可能要花費相當高昂的成本，因此本研究採用更親民且更新穎的技術「Hyperledger Fabric」做為開發的基礎。孔壹學院創辦人黎躍春曾表示：「Fabric 的主要目的是實現在區塊鏈基礎下可通用的許可權。目標即是為了能適用於不同的商業型態，並且採取模組化的架構，提供一種可以擴展功能的組建，包括共識機制、加密技術、數位資產、記錄倉儲、智能合約以及身份確認.....等。Hyperledger Fabric 能成功改善公有鏈的缺點，如儲存空間低、無隱私性、無最終確定行性和共識演算法低效等，使用者可以自行開發程式相關應用。假設比特幣為區塊鏈 1.0，那麼以太坊就屬於 2.0，而 Hyperledger Fabric 即屬於區塊鏈 3.0。」

#### (二)Hyperleger Fabric 架構

# Hyperledger Fabric 1.0版本之架構

## Fabric v1.0 Architecture

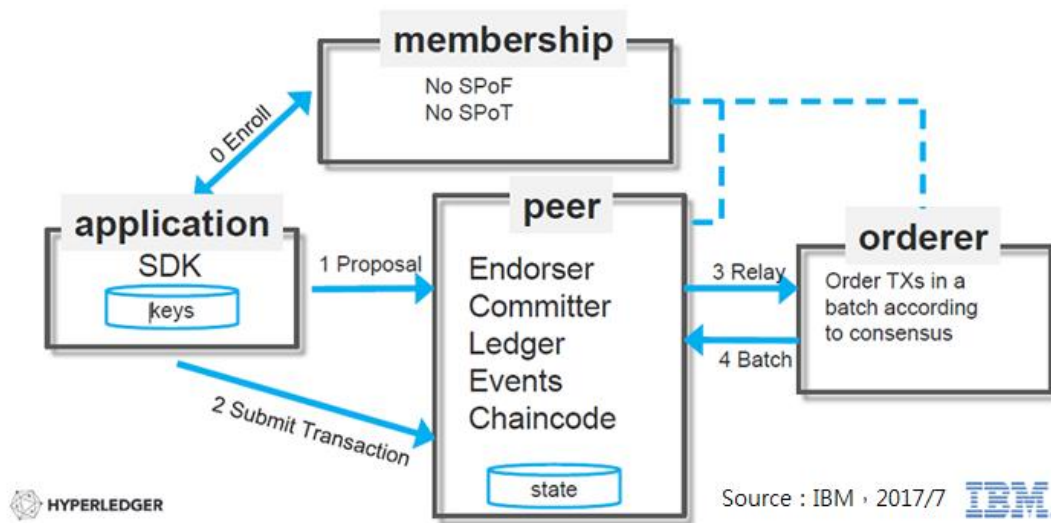


圖27：Hyperledger Fabric 架構圖

參考資料：(IBM,2017)

Hyperledger是一款開源，且能一起協作的平臺，其架構圖如圖27所示。主要的目的是為了B2B、B2C交易模式所建構的區塊鏈。Fabric是Hyperledger底下的一項子專案，為獨立企業下的分散式帳本，並且期待在未來成為不同行業中的共同使用標準。在目前Fabric 1.0版本下，大企業可用此版本來建立區塊鏈應用程式。

所需的硬體環境為：

- (1)Hyperledger Fabric developer Server:
- (2)需硬體設備:linux or Mac Server
- (3)RAM 2G~4GgHD 20G~1T
- (4)OS: unbuntu 16.04 以上或Mac10.12以上

軟體介紹：

- (1)curl
- (2)docker
- (3)docker-compose

- (4)go
- (5)node.js
- (6)npm
- (7)python

Fabric 1.0 帶給潛在性客戶一些化繁為簡的交易流程。因為程式碼具備靈活的架構，可以將嵌入式技術帶入任何商業的應用框架中。從潛在開發人員的觀點來看，Fabric 的核心價值就再於簡單使用，減少學習上的時間成本，讓更多人可以根據所在的應用行業提出可行的分散式帳本。(科技產業資訊室 Hyperledger Fabric 1.0 版推出，區塊鏈將進入黃金時代 2017)

#### 四、系統分析與設計

傳統畢業發證流程如圖 28 所示，而其相關發證流程關係如表 4 所示：

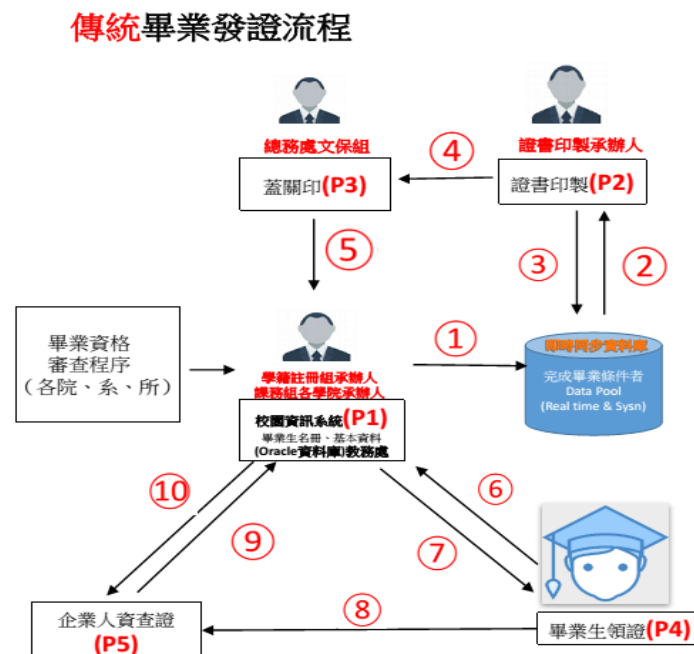


圖 28：傳統發證流程

表 4：傳統畢業證書發證流程

事件編號	Peer to Peer	事件	時間
1	P1-P1	P1 驗證存取畢業資料，並記錄到即時同步資料庫	約 5 分鐘
2	P2-P2	P2 存取資料庫標註已符合畢業證書紙本	約 5 分鐘
3	P2-P2	印製紙本畢業證書	批次作業 約 1 個月
4	P2-P3	送至總務處文保組蓋章	批次作業完 整約 1 個月
5	P3-P1	送回教務處暫放證書	含在上述流 程
6	P4-P1	畢業生完成離校手續，到教務處領證	約 10 分鐘
7	P1-P4	畢業生領證完畢	含在上數流 程
8	P4-P5	畢業生通知企業人資部門可進行查詢	約 3 分鐘
9	P5-P1	9. 企業人資部向教務處提出查詢	約 3 分鐘
10	P1-P5	10. 學校送出查驗結果	約 2 天

傳統畢業發證流程加入區塊鏈後的流程圖如圖 29 所示，傳統發證流程節點關係時序如表 5 所示，加入區塊鏈後的發證流程節點關係時序請參照表 6：

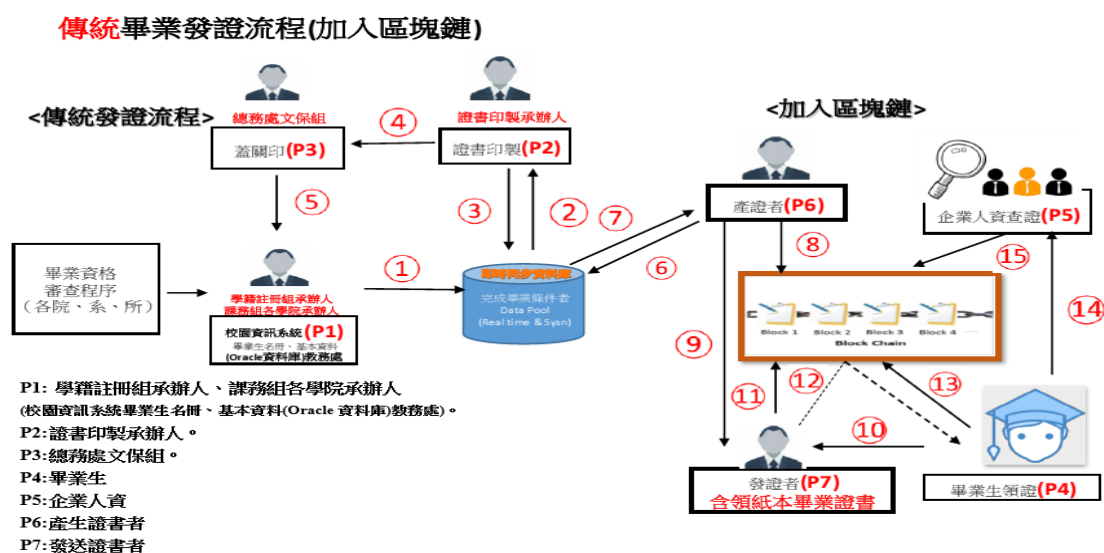


圖 29：傳統發證流程加入區塊鏈

表 5：傳統發證流程節點關係時序表

事件編號	Peer to Peer	事件	時間
1	P1-P1	P1 驗證存取畢業資料，並記錄到即時同步資料庫	約 5 分鐘
2	P2-P2	P2 存取資料庫標註已符合畢業證書紙本	約 5 分鐘
3	P2-P2	印製紙本畢業證書	批次作業 約 1 個月
4	P2-P3	送至總務處文保組蓋關印	批次作業完整約 1 個月
5	P3-P1	文保組蓋完印後送回教務處保存	含在上述流程

表 6：加入區塊鏈流程節點關係時序表

事件編號	Peer to Peer	事件	時間
6	P6-即時同步資料庫	產生證書者向即時同步資料庫，提取符合畢業資格的學生名單	約 5 分鐘
7	P6-即時同步資料庫	回傳符合畢業資格的學生名單給產生證書者	約 5 分鐘
8	P6-區塊鏈	產證者勾選寫入區塊鏈	約 2 分鐘
9	P6-P7	分配給發證者們，發證工作	約 5 分鐘
10	P7-區塊鏈	畢業生辦完離校手續至教務處領證	約 5 分鐘
11	P4-P7	進行發證且把發證動作寫進區塊鏈	約 5 分鐘
12	P7-P4	畢業生領證完成(限時到指定郵件地址領電子證書)	約 5 分鐘
13	P4-區塊鏈	學生可自行查詢證書，通知企業人資可至校查詢證書(Mail 方式)	約 2 分鐘
14	P4-P5	企業人資提出查詢證書透過電子郵件分享	約 5 分鐘
15	P5-區塊鏈	學校送出查證結果	約 5 分鐘

詳細區塊鏈發證流程如圖 30 所示，其區塊鏈發證節點關係時序如表七：



區塊鏈畢業發證流程

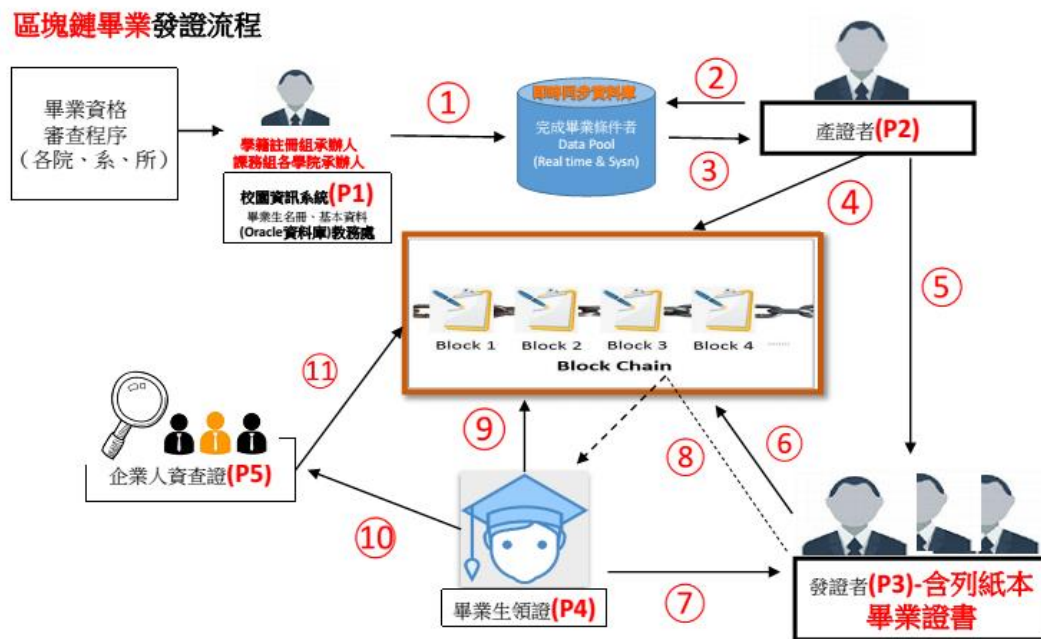


圖 30：區塊鏈發證流程

表 7：區塊鏈發證節點關係時序表

事件編號	Peer to Peer	事件	時間
1	P1-即時同步資料庫	驗證畢業資料	約 5 分鐘
2	P2-即時同步資料庫	產證者向即時同步資料庫中提取資料	約 2 分鐘
3	即時同步資料庫-P2	即時同步資料庫回傳可寫入區塊鏈中的資料	約 5 分鐘
4	P2-區塊鏈	產證者選取資料寫入區塊鏈中(一個 Block 存 10 筆資料，以 2000 筆為例)	約 6 分鐘
5	P2-P3	產證者分派工作給發證者們進行發證	約 5 分鐘
6	P4-P3	畢業完成離校手續到教務處領取紙本畢業證書，包含紙本證書	約 2 分鐘
7	P3-區塊鏈	發證者發證包含紙本，而後把該發證動作寫進區塊鏈，更改狀態(一個 Block 存 10 筆資料，以 2000 筆為例)	約 6 分鐘
8	P3-區塊鏈	畢業生領取完成，寄電子信箱通之畢業生需在時限內領取電子證書	約 2 分鐘
9	P4-區塊鏈	畢業生能查詢本身的證書且能申請分享，並透過電子郵件分享連結給企業人資部	約 2 分鐘
10	P4-P5	畢業生通知企業人資部門可至校查證學歷證	約 1 分鐘



		書，透過電子信箱進行分享	
11	P5-區塊鏈	透過 mail 企業人資提出查證連結，學校送出查證結果	約 2 分鐘

## 區塊信息

Block ID：Blcok#01(證書產證)

TX1:產證的當下將符合畢業資格的資料記錄進區塊中。

TX2:產證者將符合畢業資格的資料移轉至各發證者。

TX3:記錄每一筆畢業生的基本資料、證書欄位資料、以及證書的狀態。

Block ID：Block#02(證書發證)

TX1:接受產證者的產證資訊。

TX2:確認無誤，進行發證動作。

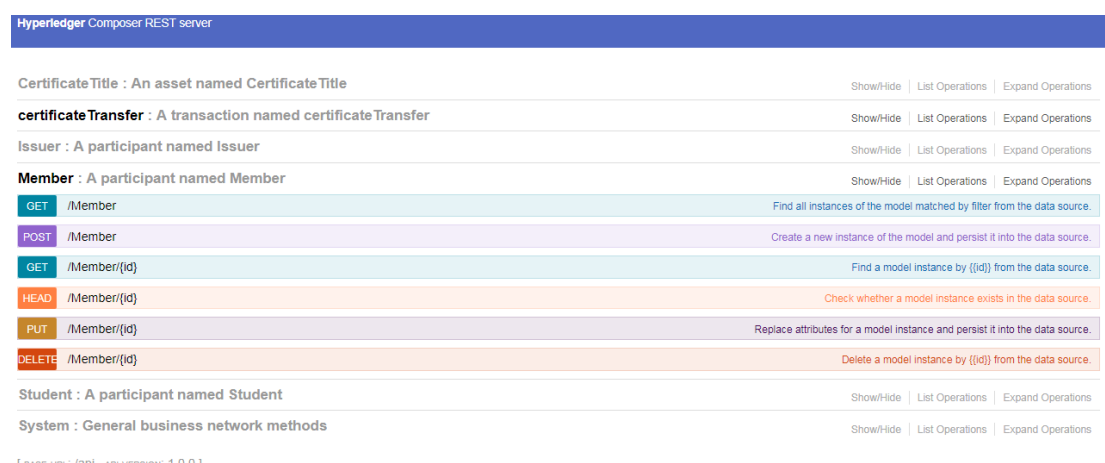
TX3:記錄發證完後的證書狀態。



## 五、系統實作結果

平臺基本配備四臺個人電腦，用以架設區塊鏈機制平臺的最小單位－四個測試節點(Node)，並使用 Linux ubuntu 來建置作業系統，支援平臺開發動作。因本研究的證書系統是以 IBM Hyperledger 進行區塊鏈平臺開發。而 IBM Hyperledger 使用作業系統平臺環境為 Linux OS。而在本段敘述之下將介紹與呈現新增、查詢、發證、產證.....等介面。並且顯示其資料結構以及欄位。最主要記錄進區塊鏈中的動作主要交易有兩種，分別為產證、發證。在產證時畢業生交易資料狀態為 100，發證後則改為 200。

### (後臺)



Hyperledger Composer REST server		
CertificateTitle : An asset named CertificateTitle	Show/Hide	List Operations Expand Operations
certificateTransfer : A transaction named certificateTransfer	Show/Hide	List Operations Expand Operations
Issuer : A participant named Issuer	Show/Hide	List Operations Expand Operations
Member : A participant named Member	Show/Hide	List Operations Expand Operations
GET /Member	Find all instances of the model matched by filter from the data source.	
POST /Member	Create a new instance of the model and persist it into the data source.	
GET /Member/{id}	Find a model instance by {id} from the data source.	
HEAD /Member/{id}	Check whether a model instance exists in the data source.	
PUT /Member/{id}	Replace attributes for a model instance and persist it into the data source.	
DELETE /Member/{id}	Delete a model instance by {id} from the data source.	
Student : A participant named Student	Show/Hide	List Operations Expand Operations
System : General business network methods	Show/Hide	List Operations Expand Operations
[ BASE URL: /api , API VERSION: 1.0.0 ]		

圖 31：Hyperledger Composer Rest server 介面

### (一)程式功能清單

### (前臺)

#### 1.系統管理者

其主要功能為新增、查詢以及修改有關於產證者、發證者、主管資料的帳號資料，並視系統情況進行維護系統發展。保障三種身份清冊的完整性。新增發證者與查詢發證者的介面如圖 32、34 所示，而其資料結構介面如圖 33、35

所示：

## ISSUER新增

帳號	<input type="text"/>
密碼	<input type="password"/>
姓名	<input type="text"/>
email	<input type="text"/>
手機	<input type="text"/>
<input type="button" value="新增"/>	

圖 32：新增 Issuer 的介面

ISSUER新增

帳號	<input type="text"/>
密碼	<input type="password"/>
姓名	<input type="text"/>
email	<input type="text"/>
手機	<input type="text"/>
<input type="button" value="新增"/>	

欄位名稱	資料型態
帳號	字串
密碼	字串
姓名	字串
Email	字串
手機	字串

圖 33：新增 Issuer 的資料結構

## ISSUER查詢

身份證字號	<input type="text"/>	姓名	<input type="text"/>	email	<input type="text"/>	手機	<input type="text"/>
<input type="button" value="查詢"/> <input type="button" value="重新查詢"/>							
共有 2 項查詢結果							
帳號	姓名	email	手機	建立日期			
ISSUER0	string	string	string	2018-01-12T14:57:51.601Z			
ISSUER1	string	string	string	2018-01-12T14:57:51.601Z			

圖 34：Issuer 查詢介面

## ISSUER查詢

身份證字號	<input type="text"/>	姓名	<input type="text"/>	email	<input type="text"/>	手機	<input type="text"/>
<input type="button" value="查詢"/> <input type="button" value="重新查詢"/>							
共有 2 項查詢結果							
帳號	姓名	email	手機	建立日期			
ISSUER0	string	string	string	2018-01-12T14:57:51.601Z			
ISSUER1	string	string	string	2018-01-12T14:57:51.601Z			

欄位名稱	資料型態
身份證	字串
姓名	字串
Email	字串
手機	字串

圖 35：Issuer 查詢之資料結構

## 2.產證者

產生證書，並把產生證書的過程寫進區塊鏈中，經歷產出過程的證書狀態修改為 100，主要功能為發配證書給發證者、新增學生帳號資料以及查詢學生帳號。證書新增以及新增學生帳號資料介面可參照圖 36、38，其資料結構介面則如圖 37、39 所示，而查詢學生帳號資料介面如圖 40 所示，其資料結構的呈現在圖 41。

證書新增

證書名稱	國立高雄第一科技大學畢業
畢業年度	請選擇 ▼
證書編號	<input type="text"/>
證書類型	請選擇 ▼
學號	<input type="text"/>
學生姓名	<input type="text"/>
身份證字號	<input type="text"/>
生日	<input type="text"/>
學制	<input type="text"/>
學位	<input type="text"/>
系所	請選擇 ▼
系主任	<input type="text"/>
院長	<input type="text"/>
校長	<input type="text"/>
發證日期	<input type="text"/>
輔系	<input type="text"/>
雙主修	<input type="text"/>
產證者	<input type="text"/>
<input type="button" value="新增"/>	

圖 36：證書新增介面

證書新增

證書名稱	國立高雄第一科技大學畢業
畢業年度	選擇
證書編號	
證書類型	選擇
學號	
學生姓名	
身份證字號	
生日	
學制	
學位	
系所	選擇
系主任	
院長	
校長	
發證日期	
輔系	
雙主修	
產證者	

新增

欄位名稱	資料型態
證書名稱	字串
畢業年度	字串
證書編號	字串
證書類型	字串
學號	字串
學生姓名	字串
身份證字號	字串
生日	字串
學制	字串
學位	字串
系所	字串
系主任	字串
院長	字串
校長	字串
發證日期	字串
輔系	字串
雙主修	字串
產證者	字串

圖 37：證書新增之資料結構

## STUDENT新增

身份證字號	
密碼	
姓名	
email	
手機	
生日	
地址	

新增

圖 38：新增學生帳號資料介面

STUDENT新增

身份證字號	
密碼	
姓名	
email	
手機	
生日	
地址	

新增

欄位名稱	資料型態
身份證字號	字串
密碼	字串
姓名	字串
Email	字串
手機	字串
生日	字串
地址	字串

圖 39：新增學生帳號資料之資料結構

## STUDENT查詢

身份證字號		姓名		email		手機	
<a href="#">查詢</a>   <a href="#">重新查詢</a>							
共有 126 項查詢結果							
身份證字號	姓名	email	手機	生日	地址	建立日期	
A123456789	測試者	b@bb.bb	0933	1968/06/26	台中市	2018-01-15T10:31:50.151Z	
A123456789ABC	測試者	b@bb.bb	0933	1968/06/26	台中市	2018-01-15T10:31:51.151Z	
B987654321	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:35.151Z	
B987654321156	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:37.151Z	
B987654321228	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:35.151Z	
B987654321449	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:42.151Z	
B987654321491	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:35.151Z	
B987654321515	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:36.151Z	
B987654321539	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:36.151Z	
B987654321849	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:37.151Z	
B987654321908	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:36.151Z	
B987654321952	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:35.151Z	
B987654321996	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:36.151Z	
C1234567891104	測試者	d@dd.dd	0933	1968/06/13	高雄市	2018-01-15T10:56:36.151Z	
C1234567891124	測試者	d@dd.dd	0933	1968/06/13	高雄市	2018-01-15T10:57:27.151Z	
C1234567891191	測試者	d@dd.dd	0933	1968/06/13	高雄市	2018-01-15T10:57:01.151Z	
C1234567891282	測試者	d@dd.dd	0933	1968/06/13	高雄市	2018-01-15T10:57:35.151Z	

圖 40：查詢學生帳號資料介面

## STUDENT查詢

身份證字號		姓名		email		手機	
<a href="#">查詢</a>   <a href="#">重新查詢</a>							
共有 126 項查詢結果							
身份證字號	姓名	email	手機	生日	地址	建立日期	
A123456789	測試者	b@bb.bb	0933	1968/06/26	台中市	2018-01-15T10:31:50.151Z	
A123456789ABC	測試者	b@bb.bb	0933	1968/06/26	台中市	2018-01-15T10:31:51.151Z	
B987654321	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:35.151Z	
B987654321156	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:37.151Z	
B987654321228	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:35.151Z	
B987654321449	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:42.151Z	
B987654321491	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:35.151Z	
B987654321515	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:36.151Z	
B987654321539	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:36.151Z	
B987654321849	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:37.151Z	
B987654321908	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:36.151Z	
B987654321952	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:35.151Z	
B987654321996	測試者	c@cc.cc	0955	1968/03/13	高雄市	2018-01-15T10:44:36.151Z	
C1234567891104	測試者	d@dd.dd	0933	1968/06/13	高雄市	2018-01-15T10:56:36.151Z	
C1234567891124	測試者	d@dd.dd	0933	1968/06/13	高雄市	2018-01-15T10:57:27.151Z	
C1234567891191	測試者	d@dd.dd	0933	1968/06/13	高雄市	2018-01-15T10:57:01.151Z	
C1234567891282	測試者	d@dd.dd	0933	1968/06/13	高雄市	2018-01-15T10:57:35.151Z	
欄位名稱	資料型態						
身份證字號	字串						
姓名	字串						
Email	字串						
手機	字串						

圖 41：查詢學生帳號資料之資料結構

## 3.發證者

查詢等待發證的證書，並且在於發放時寫進區塊鏈中做記錄。並且在已發證的證書資料狀態上由原本 100 改成 200。發證者的查詢待發證書畫面如圖 42 所示，查詢待發證書的資料結構介面如圖 43 所示。

### 查詢待發證書

共有 2 項查詢結果															
證書名稱	畢業年度	證書編號	證書類型	學號	學生姓名	身份證字號	生日	學制	學位	系所	系主任	院長	校長	發證日期	輔系
國立高雄第一科技大學畢業證書	106	高科大學字第00945號ABCDEF	學士證書	9524010	張世杰	M123456789	1988/06/26	四年制	電機碩士班	管理學學士	鄭進興	孫思源	陳振遠	2010/06	空白
國立高雄第一科技大學畢業證書	99	第一科大學字第00940號ABCDEF	碩士證書	9924801	張世杰	M123456789	1988/06/26		資管碩士班	管理學學士	曾守正	孫思源	陳振遠	2012/06	空白

圖 42：查詢待發證書



## 查詢待發證書

共有 2 項查詢結果

證書名稱	畢業年度	證書編號	證書類型	學號	學生姓名	身份證字號	生日	學制	學位	系所	系主任	院長	校長	發證日期	輔系	雙主修
國立高雄第一科技大學畢業證書	106	高科大學字第00945號ABCDEF	學士證書	9524010	張世杰	M123456789	1988/06/26	四年制	電機碩士班	管理學學士	鄭進興	孫思源	陳振遠	2010/06	空白	空白
國立高雄第一科技大學畢業證書	99	第一科大學字第00940號ABCDEF	碩士證書	9924801	張世杰	M123456789	1988/06/26		資管碩士班	管理學學士	曾守正	孫思源	陳振遠	2012/06	空白	空白

欄位名稱	資料型態
證書名稱	字串
畢業年度	字串
證書編號	字串
證書類型	字串
學號	字串
學生姓名	字串
身份證字號	字串
生日	字串
學制	字串
學位	字串
系所	字串
系主任	字串
院長	字串
校長	字串
發證日期	字串
輔系	字串
雙主修	字串
產證者	字串

圖 43：查詢待發證書之資料結構

## 4.學生

主要功能用以查詢學生本身所持有的證書。學生查詢介面如圖 44，其查詢介面的資料結構圖為圖 45。

### 查詢學生證書

共有 1 項查詢結果

證書名稱	畢業年度	證書編號	證書類型	學號	學生姓名	身份證字號	生日	學制	學位	系所	系主任	院長	校長	發證日期	輔系	雙主修
國立高雄第一科技大學畢業證書	106	高科大學字第00945號	學士證書	9524010	張世杰	M123456789	1988/06/26	四年制	電機碩士班	管理學學士	鄭進興	孫思源	陳振遠	2010/06	空白	空白

圖 44：學生查詢介面

### 查詢學生證書

共有 1 項查詢結果

證書名稱	畢業年度	證書編號	證書類型	學號	學生姓名	身份證字號	生日	學制	學位	系所	系主任	院長	校長	發證日期	輔系	雙主修
國立高雄第一科技大學畢業證書	106	高科大學字第00945號	學士證書	9524010	張世杰	M123456789	1988/06/26	四年制	電機碩士班	管理學學士	鄭進興	孫思源	陳振遠	2010/06	空白	空白

欄位名稱	資料型態
證書名稱	字串
畢業年度	字串
證書編號	字串
證書類型	字串
學號	字串
學生姓名	字串
身份證字號	字串
生日	字串
學制	字串
學位	字串
系所	字串
系主任	字串
院長	字串
校長	字串
發證日期	字串
輔系	字串
雙主修	字串
產證者	字串

圖 45：學生查詢介面之資料結構

## 肆、結論與建議

### 一、結論

此篇研究主軸為透過區塊鏈技術來改善傳統發證的種種不方便，以及防止有偽造證書的情況發生。並透過紮根理論來探討，收集傳統的發證流程並且嘗試把區塊鏈的特性導入其中，改良成一套全新的發證流程，一種全新的方法。並且透過了解上述的區塊鏈應用案例，能為其區塊鏈的相關應用窺其一二，在我國內對於普羅大眾而言，區塊鏈並非徹底的普及化。就連相關的應用也在近兩年才有所進展，甚至目前推展出的僅僅都只是一種創新的模擬架構。而在本文卻並非只有簡單的模擬架構，連流程圖也一併作出提供讀者參考。系統雖還沒確定上線，但已有模擬的系統正在實驗中。

透過本研究，將傳統模式規劃成區塊鏈改良模式時，歸納出一套轉換流程，將傳統發證流程，改良為區塊鏈證書發證系統。用以證明此方法是具可行性的。也為了將來探討利用區塊鏈改良權證相關應用流程，作為一研究之先河。

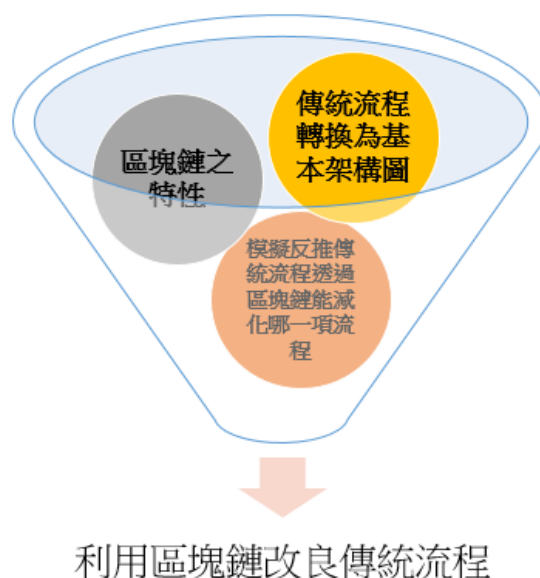


圖 46：利用區塊鏈改良傳統流程

## 二、學術貢獻與實務意涵

近年來我國伴隨著金融科技業的新興，許多產業也都藉著金融科技的影響悄悄的作改善。區塊鏈是金融科技的主要技術之一。期應用的範圍更可說是無遠弗屆，但凡需要去中心化，具保障需求均可使用區塊鏈來作一改善。其中本研究透過區塊鏈來改良傳統發證的流程。保障證明文件不被篡改，不被偽造。以及改良日常生活中的相關證書證明申請、查驗都相當不方便的缺點。本實驗則是改善這缺點，透過紮根理論，收集相關報導以及文獻來探討其他區塊鏈在其他行業的改良情形，並且嘗試歸納出上段闡述的改良步驟流程。並提供日後研究者的思考建議。

透過本研究中的個案分析，大致而言能發現其中許多傳統流程的漏洞弊端，容易讓有心人士趁虛而入。再加上研究區塊鏈後透過其特性加以思考歸納出如何利用區塊鏈來改善本研究主題發證系統。

## 三、研究限制與建議

區塊鏈的正改變著多數行業的傳統運作模式，在施瓦布（Klaus Schwab），曾經在於 2016 年世界經濟論壇之前出版了《第四次工業革命》一書，並指出近幾年的科技發展相當快速，其中有幾項最新科技即將在世界上掀起一股第四次工業革命的巨浪，其中就包括人工智慧(AI)、物聯網(IOT)、自動駕駛車、3D 列印、生物技術以及區塊鏈(BLOCKCHAIN)。但眼觀上述的相關技術基本上以大多數人而言，不知道原理但至少都有耳聞。但唯獨區塊鏈是沒有辦法靠字面上的意思來聯想其背後的運作，以及它所具備的能力。又因區塊鏈為新興不久的技術，許多開發平臺工具尚未成熟，例如本研究所使用的 Hyperledger 為非常新穎的技術之一，其版本也一再更新中。因此確切可融入百姓生活中的應用並不多，其運作商品也是少之又少，如果有那也是企業界的大熱門。因此當前最主要的目標是盡早提出一款真正能讓人民「有感」的一款應用。可是許多貼近生活的應用一般較

具低價值性的商品應用，大型企業主較不聚焦在此他們也不建議。

區塊鏈的應用應該不單單只針對企業主作設計，應廣泛接納人民的意見。提高此技術的知名度，也提升人民的接受度。讓區塊鏈能夠廣泛應用於日常生活中，但其中有給需要注意的地方仍需要我們加以省思。在美國有一家分析公司 Forrester 在 2017 年發布了一篇《前瞻 2018：準備好了嗎？區塊鏈熱背後的真相》指出區塊鏈有五大隱憂：(Lucas Mearian,2017)

### 1.區塊鏈之新興與配套軟體的落後

目前最大兩種區塊鏈的底層平臺即是，Hyperledger 即 Ethereum 可是這兩種基礎平臺嚴格來說還是處於一種全新的技術領域，並非一種舊有的開發環境。就以 Ethereum 而言，他依靠 Solidity 來執行智能合約，可是 Solidity 並不支援小數點，對於開發者而言相當不方便，有可能因為要刻意規避此項特點，而進行程式大更改，甚至有可能導致系統錯誤。

### 2.區塊鏈：並非儲存數據的萬能鑰匙

以比特幣而言，其運用區塊鏈作為底層技術來保證每一筆交易資訊不被篡改，但依照每一格區塊鏈的儲存空間為 1MB 的儲存量而言，雖然不占據太大的儲存空間，可是只要經過時間一長區塊的累積速度相當快，進而累積到一定程度時的系統儲存量是相當大的。很有可能導向最終失控的場面。

### 3.區塊鏈：並非百分百的安全

在 2016 年發生的 The Dao 事件，該通過分散式區塊鏈運作的風險投資基金，其因為一個程式的漏洞，就被不法份子盜取了市值逾 600 萬美元的數位貨幣。同年在為香港的一間數為貨幣交易所 Bitfinex，被指出超過 12 萬枚比特幣被不法份子盜取而當時市值竟高達 6800 萬美元。上述案例都一再的點醒我們其時區塊鏈並不是百分之百的安全，往往因為一個不起眼的程式小漏洞就有可能被駭客圖破，造成更嚴重的損失。

#### 4.規模擴充與機密信息——規模化和隱私

安全機密是人人所追求且嚮往的，但區塊鏈主打的部分就是資訊透明化。只要是在區塊鏈上的人，且在於公有鏈上人人基本上都可以得知區塊鏈上所記錄的消息，但並非每一件事情都是需要被公開的。資訊透明化這意味著如果將區塊鏈用作股票交易平臺，且負責交易當下的即時運算系統，就代表著在區塊鏈上的每一位使用者都有權利得知每一位使用者當下的交易動作，進而有可能引發惡意的交易攻擊手法。

#### 5.對於智能合約的過分期待

智能合約也存在著一些需要注意的地方。智能合約僅僅只能規範著既定的規則，以及當下考慮得到的各種情況。但是只要有出乎意料的突發狀況，是無法臨時更改其智能合約的。



總而言之區塊鏈技術可以帶給當今社會許多脫胎換骨的機會，但並不代表適用於每一個行業，因此針對可適用的範圍內做最好的改良。切勿不可為了區塊鏈而區塊鏈，盲目的追求創新科技的步調而導致錯誤。活用區塊鏈落實區塊鏈，放眼生活中的小細節。在未來的研究建議，區塊鏈證書發證管理系統不僅僅只能從學生畢業證書做發展，可更多元應用於學習記錄以及相關證照管理與研習證明。透過區塊鏈的特性能使資產管理更具系統性以及未來性。

## 參考文獻

### 英文文獻

- [1] Adam Back (2002). Hashcash - A Denial of Service Counter-Measure.
- [2] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M(2014). Virza. Zerocash: Decentralized anonymous payments from Bitcoin. In S&P, 2014.
- [3] Ethereum community(2017),Ethereum Homeestead Documentation Release 0.1
- [4] Florian Glatz(2014). What are Smart Contracts?, [www.BLOCKCHAIN.lawyer](http://www.BLOCKCHAIN.lawyer).
- [5] Hyperledger Fabric releases version 1.0 of open source distributed ledger. Tech Crunch, 20170711
- [6] Hitesh Tewari and Eamonn O Nuallain(2015). Netcoin: A Traceable P2P Electronic Cash System, 2015 IEEE International Conference on Web Services.
- [7] Melanie Swan (2015). BLOCKCHAIN: Blueprint for a New Economy, Oreilly & Associates Inc.
- [8] Melanie Swan (2015). BLOCKCHAINs as an Equality Technology, Broader Perspective blog.
- [9] Melanie Swan (2015). Cognition Applications of BLOCKCHAIN Technology, Cognitive Science 2015: Mind, Technology, and Society, Submitted.
- [10] Melanie Swan (2015). BLOCKCHAIN Thinking: The Brain as a DAC (Decentralized Autonomous Organization), New School for Social Research, New York NY.
- [11] Matthew D. Sleiman, Adrian P. Lauf, Roman Yampolskiy(2015). Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency System, 2015 International Conference on Cyberworlds.
- [12] Satoshi Nakamoto(2008). Bitcoin: A Peer-to-Peer Electronic Cash System, Consulted, vol. 1, p. 28, 2008.



- [13] Strauss, A & Corbin, J.(1998).Basics of Qualitative Research : Techniques and Procedures for Developing Grounded Theory. Newbury Park,CA:Sage.
- [14] Strauss, A & Corbin, J.(1990).Basics of Qualitative Research : Grounded Theory Procedures and Techniques.Newbury Park,CA:Sage.



## 中文文獻

- [1] 廖世偉(2016)。顛覆性科技－區塊鏈。國立臺灣大學資訊工程學系。
- [2] 高孟華(2016)。區塊鏈 BLOCKCHAIN 引領未來市場的關鍵技術, Blue Viewpoint58 期 4 月。臺灣國際商業機器股份有限公司。
- [3] 佚名。證券暨期貨月刊第三十四卷第十期
- [4] 長鈇、韓鋒、海濱(2016)。區塊鏈從數字貨幣到信用社會。第二章區塊鏈基礎篇
- [5] 馬兆林(2017)。解密區塊鏈，你所不知道的區塊鏈
- [6] 姜尚(周朝)。六韜・龍韜
- [7] 希羅多德。歷史
- [8] 賴怡伶、莊鯉銓(2015)。金融科技、區塊鏈技術探討暨人民幣跨境支付之近期發展,。2015 年國際金融年會(SIBOS),新加坡,10 月。
- [9] 何沛馨(2016)。應用區塊鏈技術於門診電子病歷
- [10] 楊英伸(2016)。區塊鏈發展趨勢
- [11] 徐宗國譯(1997)。質性研究概論,臺北,巨流。
- [12] 徐宗國(1996)。紮根理論研究法,載於胡幼慧主編,質性研究,臺北,巨流,47-73。
- [13] 陳昺麟(2001)。社會科學質化研究之紮根理論實施程序及實例之介紹,勤益學報,第 19 期,327-342。
- [14] 黃政傑(1998)。質的教育研究：方法與實例,臺北：漢文。
- [15] 黃宜凱(2017)。事件因素對比特幣價格之影響，國立臺北大學，碩士論文
- [16] (美)梅蘭妮絲萬(2016)，區塊鏈新經濟藍圖及導讀
- [17] 賴寒彰(2017)。區塊鏈探討與應用，國立高雄第一科技大學，碩士論文
- [18] 薛德興(2016)。病歷資訊化創新應用經驗分享
- [19] 鄭天浚、蘇慧芬(2017)。病歷無紙化推動與成果
- [20] 楊鎮州(2017)。經濟日報，度度客全臺首創 區塊鏈募資平臺

[21] 施瓦布(2016)。第四次工業革命

[22] HPB(2017)。HPB(芯鏈)白皮書



## 網路文獻

- [1] Chris DeRose：抓住重點！智能合約才是區塊鏈革命中最重要的部分。  
2016 年 3 月。取自 <http://www.gegugu.com/2016/03/17/11915.html>
- [2] 每日頭條-HPB 芯鏈聯合 imtoken 等五大平臺上線 ICO。2017 年 8 月。取自 <https://kknews.cc/zh-mo/tech/xra5e2r.html>
- [3] MIT News-Digital Diploma debuts at MIT 取自  
<http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-BLOCKCHAIN-technology-1017>
- [4] 【臺灣區塊鏈應用實例】免除繁雜審核和發放流程，數位國小畢業證書明年登場。取自 <https://www.ithome.com.tw/news/119252>
- [5] 吳陽，區塊鏈盛行，不可不知的五大技術隱憂，2017 取自  
<http://news.knowing.asia/news/623df6ee-058d-4b1a-a211-dcae24215e08>
- [6] IThome-區塊鏈技術演進史，2016 取自  
<https://www.ithome.com.tw/news/105370>
- [7] Ithome-【專訪 Hyperledger 專案最高總指揮】我們正用區塊鏈重新發明這世界，2017 取自 <https://www.ithome.com.tw/news/115810>
- [8] 個人病歷將可帶著走！北醫攜手區塊鏈新創 DTCO，要串連全臺醫院病歷庫，2017 取自 <https://www.ithome.com.tw/news/118176>