

銘傳大學

資訊工程學系碩士班

碩士論文

以區塊鏈數位貨幣為主的商家收銀監督系統的平台建置與實作-以比特幣為例

研究生：江柏憲

指導教授：王家輝 博士

中華民國 107 年 1 月

銘傳大學

研究所碩士班


論文口試委員會審定書

本校 資訊工程 研究所 江柏憲 君

所提論文 以區塊鏈數位貨幣為主的商家收銀監督系統的平台建置與實作-以比特幣為例 合於碩士資格水準，業經本委員會評審認可。

口試委員：

(召集人)



_____	_____
_____	_____
_____	_____
_____	_____

指導教授：_____

研究所所長：_____ 教授

中華民國 107 年 1 月 日

銘傳大學博碩士論文電子檔案授權書

中華民國九十三年五月十日行政會議通過

本授權書所授權之論文為授權人在銘傳大學_____研究所_____學年度第_____學期
取得☐博士☐碩士學位之論文。

論文名稱：_____

研究生：_____學號：_____

指導教授：_____

茲同意將授權人擁有著作權之上列論文全文電子檔（含摘要）無償、非專屬性授權給財團法人銘傳大學，並得將授權之論文重製成微縮、光碟或其他數位化載體以與其他學術機構（如國家圖書館）為資料之交換。另基於著作權法規定之合理使用原則，依授權者授予下列勾選之公開權限，提供讀者不限地域、時間及次數之免費線上檢索、閱覽、下載或列印。

全文電子檔使用權限授權（請勾選下列一項授權選項）：

校內	<input type="checkbox"/> 立即公開 <input type="checkbox"/> 1 年後公開 <input type="checkbox"/> 不公開
校外	<input type="checkbox"/> 立即公開 <input type="checkbox"/> 1 年後公開 <input type="checkbox"/> 不公開

立授權書人對上述授權書之著作擁有著作權，尚未專屬授權予其他法人或自然人。本件授權不影響著作人對原著之著作權及衍生著作權，並得為其他之專屬授權。

授權人：_____（簽名）

身分證字號：_____

E-Mail：_____

中 華 民 國 年 月 日

以區塊鏈數位貨幣為主的商家收銀監督系統的平台建置與實 作-以比特幣為例

研究生：江柏憲

指導教授：王家輝

銘傳大學資訊工程學系

摘要

在傳統的中央集權式的金融體系在跨國轉帳的情境當中會遇到許多的問題，包括營業時間限制、冗長的處理手續、過長的等待時間、兩國之間的時差問題、還有高額的手續費。而在上述眾多的問題中，比特幣的底層核心技術－區塊鏈(blockchain)技術成為了最佳的解決方案，因為基於同儕網路的雜湊現金(hashcash)系統，解決了跨國時差的問題，因為它的去中心化及匿名性，所以大幅降低人為前往銀行申報資金交易的人力成本，也不需要繳交高額的跨國電匯的手續費。比特幣背後的密碼學原理，也奠定了比特幣的安全性，讓使用者可以更安心的使用數位加密貨幣。

歷經多年來的挑戰與多方面的研究，區塊鏈加密貨幣在2017年不論是價值或是討論度都有了爆發性的成長，世界各國政府亦如火如荼地發展並探討相關金融法規。雖然區塊鏈加密貨幣擁有匿名、高安全性、去中心化等優點，但這些優點同時也讓不肖份子逃漏稅、洗錢、詐騙甚至是成了暗網的流通貨幣。

因此本論文致力於研究以比特幣系統為基礎的商業化收銀監督模型，讓區塊鏈加密貨幣能夠不僅能改進過去種種缺點的，同時還能保有原先的優點。文中以比特幣開發用之測試幣為基礎，修改其在Android系統上的開放原始碼應用程式，使得本論文闡述之概念能夠實際在區塊鏈上運行，以期未來數位加密貨幣不僅能維持目前的便利性，使一般民眾能更安心使用數位加密貨幣作為日常生活的行動支付管道。

關鍵詞：比特幣，區塊鏈，行動支付，密碼學

The Deployment and Implementation of Blockchain-based Digital Currency Transaction Supervision System-Using Bitcoin as an Example

Student : Bo-Sian Jiang

Advisor : Chia-Hui Wang

Department of Computer Science and Information Engineering
Ming Chuan University

Abstract

In traditional financial system, we will encounter many problems from the situation of transnational transfer. These problems include limited business hour, lengthy processing and waiting time, the time difference between the two countries and high banking charge. However, blockchain technology has become the best solution for these problems. Because its hash cash system with cryptography is based on the point-to-point, the problem of transnational time difference can be solved. Due to its decentralization and anonymity, it significantly reduces the labor cost of the transaction. Besides, we don't need to pay a high amount of cross-border wire transfer fee.

After years of challenge and multidimensional research, blockchain-based digital currency has seen explosive growth in both value and discussion in 2017. Governments around the world are also in full swing to develop and explore the relevant financial laws and regulations. Although blockchain-based cryptocurrencies have the advantages of anonymity, high security, decentralization, However, these advantages also allow unscrupulous tax evasion, money laundering, fraud or even the darkweb.

This thesis will focus on study on the deployment and implementation of blockchain-based digital currency mobile payment supervision system. we modify the Bitcoin open source application of Android. In the near future, we looking forward to that the digital encryption currency transaction not only can avoid the use of digital currency in money laundering, but also won't worry about how to find the seller after trading. So, people can be more secure in mobile payment using digital encryption currency like traditional currency of their daily life.

Keywords : Bitcoin , Blockchain , Mobile Payment , Cryptography

誌謝

碩士生涯短短兩年稍縱即逝，這段期間著實收穫良多，必須要特別感謝指導老師，王家輝副教授的教導，從完全不認識比特幣、區塊鏈等技術，直到現在能夠找出比特幣現有的缺點，並且著手新增其開放原始碼應用程式的功能，也著手規劃並建置了一套完整的系統，作為以區塊鏈數位貨幣為主的商家收銀監督系統之範例系統，都是經過一次又一次開會的討論、修改及實驗而完成的成果；除此之外也從王家輝老師身上學習到對於研究的方法及態度，不論是學術上的成果或是做人處世的態度，都讓我有與大學部完全不同層次的學習與經歷。

除了指導老師之外，另一位同窗好友「陳伯韋」也是必須感謝的對象，他對於比特幣的相關知識與動態消息，總是能領先許多人一步，也不吝於將這些知識、消息與我們分享，甚至帶著我參加許多區塊鏈研討會的場合，認識許多區塊鏈業界的相關人士，豐富的資源加上對於比特幣的熱忱，讓我在與他共事時也不自覺的被他的態度所感染，更期望未來能夠在區塊鏈產業有所發展。最後還要感謝同期的所有研究生，當我在開發系統時，可能對介面、對系統流程有所疑惑，有著一群樂於給我幫助的同學，讓我感到很是幸運。

這些日子以來如果沒有指導教授的協助、沒有這些同學的幫忙，若是僅憑我一己之力，想是無法有今天這樣的成果、也不會有這篇論文的產生，在此致上十二萬分的謝意

江柏憲 謹致於

銘傳大學資訊工程研究所

中華民國一百零六年十二月

目錄

摘要.....	i
Abstract	ii
誌謝.....	iii
目錄.....	iv
圖目錄.....	v
表目錄.....	vi
第壹章 緒 論.....	1
第一節 研究背景.....	1
第二節 研究動機.....	2
第三節 研究目的.....	2
第貳章 文獻探討.....	4
第一節 區塊鏈結構與優缺點分析.....	4
第二節 比特幣簡介與相關技術說明.....	8
第三節 比特幣的危機與國際情勢分析.....	13
第參章 研究方法.....	17
第一節 貨幣交易關係比較.....	17
第二節 數位貨幣的仲介商機.....	20
第三節 行動支付的便利與危機.....	20
第四節 系統模型與開發背景.....	22
第五節 系統模型架構.....	24
第六節 系統模型流程與資料庫架構.....	25
第肆章 研究成果.....	28
第一節 系統介紹.....	28
第二節 實驗數據.....	35
第伍章 結論與未來工作.....	37
第一節 結論.....	37
第二節 未來工作.....	37
參考文獻.....	39

圖目錄

圖 1	Merkle Root 生成示意圖	5
圖 2	區塊鏈結構示意圖	5
圖 3	比特幣地址生成流程圖	10
圖 4	雙重花費流程圖	12
圖 5	綠色地址錢包交易之流程圖	13
圖 6	世界網路資源分布圖	15
圖 7	全球受災分布圖與 Wanna cry 勒索畫面	15
圖 8	收取贓款的地址追蹤	15
圖 9	各國央行對比特幣態度	16
圖 10	現金貨幣交易模型-無收據交易	17
圖 11	現金貨幣交易模型 - 實名店家	18
圖 12	VISA 交易模型	18
圖 13	支付寶交易模型	18
圖 14	PayPal 交易模型	19
圖 15	行動支付種類繁多	22
圖 16	Testnet 之 icon	22
圖 17	Android studio 之圖示	23
圖 18	Google Nexus 5 與 Google Nexus 5X	23
圖 19	XAMPP 圖示	24
圖 20	商家註冊流程圖	26
圖 21	商家創建與驗證交易流程圖	27
圖 22	政府端首頁	28
圖 23	政府端申請表單介面	29
圖 24	政府端商家資訊一覽	29
圖 25	商機端首頁	29
圖 26	商家端商品查詢	30
圖 27	商家端交易明細	30
圖 28	商家端新增商品	30
圖 29	系統載入、登入及掃描商品介面	31
圖 30	掃描商品介面功能介紹	32
圖 31	確認與交易總覽視窗	33
圖 32	交易明細與 Block explorer 介面	34
圖 33	測試幣首頁、付款、交易一覽及明細頁面	34
圖 34	實驗結果分析圖	36

表目錄

表 1 各國政府對比特幣態度統整表.....	16
表 2 交易關係比較表.....	20
表 3 行動支付的五個關卡.....	21



第壹章 緒 論

2008 年，一位只聞其名未見其人的「中本聰」，透過一篇未在任何學術期刊上公開發表的神祕論文[1]把比特幣帶到這個世界。基於密碼學、同儕網路、共識演算法、區塊鏈技術所組合而成的數位貨幣[2]，歷經八年來的種種攻擊至今仍運著作著。比特幣至今可說是現今最具代表性的數位貨幣，但這不意味著沒有任何的缺點；在摩爾定律的模型下，電腦運算的速度會日益成長，首當其衝的則是比特幣開發者所決定採用的各種密碼演算法，包括 SHA-256[3]、橢圓曲線公私密金鑰演算法[4]。在未來更需要透過分叉來更換比特幣的基礎演算法，使得比特幣能夠因應科技的進步所帶來不同層面的衝擊。

第一節 研究背景

比特幣是一種去中心化的雜湊現金系統，與傳統中心化的金融機構相比，去中心化會帶來更多的優勢，包括大幅降低被網路攻擊所帶來的風險，因為比特幣區塊鏈的存儲，會透過同儕網路[5]技術的方式，分散儲存至所有運行比特幣全節點[6]的計算機中，現今的區塊鏈大小已經達到 100G 以上，資料內容為自 2009 年來，所有以比特幣為貨幣所發起的交易將會被收入其中，並永久被保存至區塊鏈中。全世界運行比特幣系統的電腦，據網路節點統計高達六千多點，這意味著區塊鏈的資料，已經被複製了六千次。大量節點的備份資料，確保了比特幣網路的穩固性，並不會因為其中一個節點的關閉，而影響到比特幣系統的正常運作，且去中心化的系統，也因不需要人力隨時操作、經營及維護，所以比特幣系統有別於傳統的中心化有營業時間限制的金融機構，可以二十四小時不間斷的運行，相當穩定。

傳統的金融交易體系，是由許多傳統的金融機構組合而成，對使用者而言，若要使用這些金流系統，我們必須接受他們的監控，雖然中心化的金融交易系統是現今主要的交易體系，但仍有著許多需要克服的問題，如交易資料全為中心化管理，而對消費者或使用者而言，並沒有足夠的授權可調閱交易資料，這些交易紀錄既不公開，也只能依賴著唯一的信任，去相信資金是安全的，也不能確保資金的流向。

如將這些傳統的中心化金融機構的交易金流系統替換成區塊鏈技術，金融機構將會繼承區塊鏈技術的特色，全部的交易記錄也會公開透明的展現給所有的人去檢視，因此就不會發生資金流向不明的問題，這不僅是讓資金流向透明化的管道，更可以確保消費者的消費紀錄不被更改或是刪除；換言之，對於賣家可以藉由區塊鏈技術相信相關演算法的正確性，促使著交易可以被信任，而進一步更清楚的掌握所有的交易細則，更精確地掌管公司的運營狀況，可以降低許多人力資源，進行財務報表統計。

最後，政府可以輕易地檢視且相信所有的交易資料的正確性，對於課徵稅收，更有著標準化而且被大眾信任的全自動化作業程式，一方面可以降低人力成本的

支出，也可以降低政府課徵稅收的過程中出現的錯誤。

第二節 研究動機

比特幣為我們勾勒出了一個新的美好世界，然而現今的比特幣系統仍存有一些問題。由於比特幣系統是建立在區塊鏈上，因此比特幣擁有「偽匿名性」的特性，也就是說我們可以輕易地透過公開在區塊鏈上的地址資訊，來追蹤每個地址的金流記錄，但卻無法知道每個地址或是每筆交易與使用者之真實身分的關聯。偽匿名這樣的特性，雖然為我們帶來不少便利，但同時也產生不少問題，例如：比特幣經常被當作是黑市交易買賣的貨幣，因為偽匿名性，即使檢調機關想要調查，也難以著手；一般民眾使用比特幣進行買賣，交易完成後產生的交易資訊都存在區塊鏈內，雖然方便大家查詢，但卻沒有詳細記錄賣家銷售了哪些商品、買家則是向哪個店家購物？以上是現今比特幣內部未存有的資訊所產生的問題，因此無法讓商家輕鬆管理商品資訊、更無法使顧客有完整的交易保障。

假如今天一位顧客在便利商店購物，並以比特幣錢包作為支付的管道，完成交易後，如果沒有適當的監督系統與機制，可能對於顧客、商家及主管機關會產生種種交易不明、不確定與不便利等不利三方利益的因素。站在政府的管道來看這筆交易，政府單位並不知道這筆交易的內容是不是含有什麼非法商品；站在商家的角度則無法清楚得知該店的詳細交易紀錄，若有交易糾紛則後續要提出交易證明相當困難；以消費者而言，我們只能從區塊鏈上查訊雙方交易地址以及交易金額、時間、營業人統一編號等等資訊，無法輕鬆藉由上述資訊查詢到實際的交易細項，不論是要管理賬目或是要取得交易證明都相當的不便且困難。

因此本論文致力於提出一個基於比特幣為主的商業收銀系統模型，以解決政府、商家及顧客等三方，因為比特幣之偽匿名性所產生的困擾，以期比特幣能夠更加廣泛地被社會大眾接納，並受到政府及人民的認可，藉此落實比特幣作為數位加密貨幣之特性。

第三節 研究目的

本論文致力於建立一個比特幣收銀系統模型，以解決政府、賣家及買家三方使用比特幣交易時所產生之問題。

為了避免比特幣被當作黑市交易貨幣，故商家若欲以比特幣作為交易管道，則需向政府申請商家認證，確保該商家為正當盈利，藉此避免商家經由比特幣洗錢之可能，另一方面政府單位還可於年度查稅時統計本系統之交易清單，建立一套自動化、透明且有公信力的查稅機制，以減少稅金計算過程所產生的紛爭。

為了使商家在交易完成後，可以更加方便管理銷售紀錄，以及店內商品之交易情形，故本系統於完成交易後會自動將商家資訊及交易資訊與比特幣區塊鏈上的交易資訊產生關聯，商家便可輕易查詢每筆交易的詳細資訊，包括每一筆的銷售商品細項、單價及數量等資訊，讓商家在使用比特幣交易時還能夠存取更多的銷售資訊，後續不論店家要做大數據分析、商品管理與銷售決策分析等都能夠更

加快速。

為了讓顧客能夠在以比特幣完成交易後，不僅能從區塊鏈上查看雙方交易的地址、時間及總金額這些概要的資訊外，還能夠透過本系統模型得知每一筆交易中的詳細項目、金額以及一個經由政府核可的商家之基本資訊，以利消費者後續要管理個人消費帳務，亦或是當交易產生爭議時能夠找到一個負責的單位。

期望透過本系統模型，給予全世界之比特幣使用者一個更加乾淨、方便且有效率之數位加密貨幣交易環境，以提升社會大眾之生活品質。



第貳章 文獻探討

由於本論文之主題為以區塊鏈數位貨幣為主的商家收銀監督系統的平台建置與實作—以比特幣為例，因此在我們介紹比特幣之前，勢必得先了解比特幣的核心技術：「區塊鏈」，接著介紹何為比特幣。本章主要分成三節，分別為區塊鏈結構與優缺點分析、比特幣的簡介、與比特幣有關的詐騙之案例分析與防治及比特幣交易的國際動態趨勢介紹。

第一節 區塊鏈結構與優缺點分析

本節主要介紹區塊鏈相關技術與知識，我們會先簡單介紹區塊鏈及區塊鏈的結構，並說明區塊鏈技術的現狀、優點及缺點，最後則是舉出目前市面上除了金融以外的區塊鏈應用：

一. 區塊鏈簡介[7]：

比特幣應用到的技術眾多，大致可以將比特幣技術分為四個區塊，分別為錢包位址生成、比特幣交易簽屬及廣播、區塊鏈技術、分散式帳本。比特幣為區塊鏈技術最典型的應用之一。本段將詳細說明區塊鏈的技術引用、區塊鏈的基礎架構、區塊鏈的運作以及分散式節點儲存。

二. 區塊鏈結構：

區塊鏈結構大致分為兩部分，分別為區塊鏈的區塊頭，以及區塊所有被儲存在區塊內的所有交易，如下圖 1 所示。



圖 1 區塊鏈結構示意圖

區塊頭包括區塊版本、父區塊雜湊值、Merkle Root[8]、時間戳記、難易度及 Nonce：

- (一) 區塊版本 (32bits)：紀錄區塊鏈系統及協定的相關版本資訊。
- (二) 父區塊雜湊值 (256bits)：紀錄前一個區塊的雜湊值，透過父區塊雜湊值，才能把所有區塊首尾相連進而形成區塊鏈。除了形成鏈結外，也可以使得區塊更不易被修改，因新的區塊不斷地被疊加在舊的區塊上，會使得舊有區塊的雜湊值不斷地被傳遞到最新的一塊，堆疊

的越多就的區塊雜湊值被間接引用越多次，使得越早被創立的區塊越不易被竄改。

(三) Merkle Root (256 bits)：此值為 Merkle tree 根值，可以快速驗算當前區塊所有的儲存的交易是否正，如下圖 2 所示。

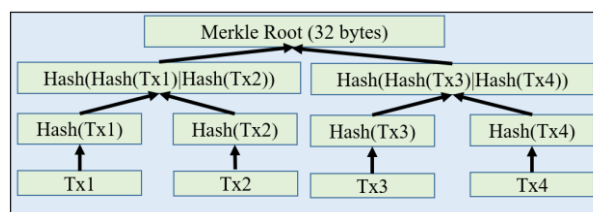


圖 2 Merkle Root 生成示意圖

(四) 時間戳記 (32bits)：記錄區塊生成時間，格式為年、月、日、時及秒。

(五) 難易度 (32 bits)：為工作量證明類演算法解的難易度目標值。

(六) Nonce (32 bits)：記錄當前區塊工作量證明類演算法的解。

區塊主體會因為區塊鏈被設計於不同的應用而有所改變，以比特幣為例，比特幣區塊鏈中被記載著於 2009 年（比特幣開始運行的年份）至今所有的交易紀錄，其交易格是被允許為多對一、一對多、多對多以及無對多（指創建區塊所得的獎勵，並無明確的比特幣來源）。除了電子現金外，亦有功能變數名稱區塊鏈、票券區塊鏈[9]以及食安區塊鏈[10]正在研發測試。

三. 區塊鏈優點：

區塊鏈的優點包含了去中心化、公開透明的數據、數據不可竄改性、同儕網路架構及匿名性，以上種種優點也為現今社會帶來了衝擊性的改變和挑戰，接著將針對這五項優點作介紹：

(一) 去中心化：

傳統社會上大多數的系統都有一個中央機構在管理數據與資料，然而在區塊鏈世界中，僅依靠著演算法維持整個系統的運作，換言之，在這樣的去中心化的系統中，沒有一個人或一個集團可以直接決定系統運作的規則，所以不會有財團壟斷交易，更不會有政府獨握所有資訊；如果遇到系統有嚴重的錯誤或是有需要改善升級的地方，以比特幣為例可以藉由 BIP(Bitcoin Improvement Proposals)[11]的方式進行升級，這樣的計畫的提出，需要在比特幣系統中過半數的使用者支援，才得以運行。也就是因為這樣的民主的機制，也相對的穩定許多。

(二) 公開透明的數據：

此項特性可說是解決當前所有信賴問題重點，因為在公有錄

上所有的交易紀錄皆為公開透明，這使得任何人都可以成為區塊交易資料的節點、檢視所有的資料，也可以驗算每一筆交易紀錄的正確性。

除了作為區塊鏈信任的基石，公開透明的特性，可以讓更多的開發者或是新創公司，更為簡易和方便地取得交易原始資料，畢竟在現金的金融體系當中，所有的交易紀錄，皆為由中心化的金融機構存儲，要向中心化的金融機構，提取原始交易資料極為不易。區塊鏈公開透明的特性，促使著公司降低取得原始資料的門檻做出視覺化的開發計畫，甚至是利用大資料分析分析出前所未見的觀點。

(三) 數據不可竄改性：

在區塊鏈架構下，所有的資料只要通過嚴格校驗後，被記錄於區塊鏈中，便無法被刪除，基於區塊鏈的特性，所有區塊的連接，新區塊都會存儲舊區塊的整個雜湊值，而雜湊值得連結，只要區塊中的一個值遭到修改，即便是一個 bit，也會使的全部的雜湊值完全不同，也就是雪崩效應，也因為存在著這樣的結構，保障著所有的資料永遠不會被更動，如果校驗的結果被更動，該區塊不會被系統接受。使得所有的交易紀錄只要進了區塊鏈皆無法修改及刪除。

(四) 同儕網路架構：

基於同儕網路架構建置成的區塊鏈交易系統，繼承著去中心化的特性，在同儕網路架構中，因為為去中心化的協議，當中所有的節點是客戶端也是伺服器端。傳統的中心化網路，由於僅有個位數級的伺服器主機，非常容易成為被集中攻擊的對象，但以比特幣系統為例，卻可以擴增到六千餘節點，做到了有效的預防阻斷服務攻擊。

近年來也因為比特幣的盛行，成為勒索軟體的主要支付方式，而基於同儕網路的區塊鏈，即便單一節點的資料被鎖攻擊者進行資料的加密進行綁架勒索，但這樣比特幣勒索方式，對去中心化的區塊鏈交易系統不會構成太大的威脅，畢竟在比特幣網中有眾多的資料結點，並不會因為一個節點的損毀而帶來太大的影響。

(五) 匿名性：

在現今的社會中，對各家公司而言個人資訊的保護已成為最重要的課題，在區塊鏈所建立的所有的帳戶皆沒有在現實的社會中建立起直接關係，也就建立起了匿名性。運用在現實生活中，可以有效的保護消費者的個人隱私，與 Visa 交易不同的是在使用塑膠貨幣的過程中我們會與 Visa 主機透露了許多個人資訊資料，這便會帶來個人資訊透漏的風險，但在區塊鏈技術中，可以避免這樣的問題。

四. 區塊鏈缺點：

雖然區塊鏈的特性帶來了非常多的優點，但有些特性卻如同雙面刃一般，在給人們帶來安全與便利的同時，也產生了新的困難與挑戰，因此想將區塊鏈套入各項產業中，也勢必得經過一番考量及研究。

(一) 去中心化：

因為去中心化使得區塊鏈的應用被分散在無數個節點中各自運行，倘若系統出現重大錯誤，需要透過系統更新來修正，則必須超過該系統一半以上的節點同意並執行更新才可成立，假如節點不僅數量龐大且分布於全球各地，就可能產生更新困難的問題。

(二) 公開透明的數據：

以商業而言，並不是所有資料都適合公開透明的放在區塊鏈內供人任意使用，即使能透過雜湊將數據加密，亦可能因耗費大量時間及運算效能處理龐大數據的雜湊及加解密，致使存取數據時的效率急遽下降。

(三) 數據不可竄改性：

當數據進入區塊鏈後就無法再作任何更動，雖然這樣的機制很安全，但也失去了許多再生活應用的彈性，可能誤用錯誤的資訊寫入區塊，這時卻沒有任何可以補救的方式，以比特幣為例可能是將貨幣發送給不知名的人士，甚至可能致使這筆錢直接消失在這世界上；除此之外也可能是有心人士刻意將錯誤資訊寫入區塊鏈，例如農產食安區塊鏈：雖然區塊鏈內的數據無法更動，但不孝人士可能從一開始就是以錯誤的數據寫入區塊鏈，以此方式建立的區塊鏈頓時失去其不可竄改的意義了。

(四) 匿名性：

區塊鏈的匿名性一直是使各國政府最頭疼、最擔心的特性，因為這樣的特性，基於區塊鏈發展而成的貨幣頓時成了罪犯生長的溫床，雖然交易數據是公開透明的，但單看這些透過雜湊處理的數據，是完全無法與現實中的人、事、物產稱關聯，也因此造成了法警欲提出犯罪證據時的困難。最著名的例子莫過於 2017 年 5 月在全世界爆發的病毒「Wanna Cry[29]」。

五. 區塊鏈的相關應用：

基於區塊鏈技術，可以建構出許多貨幣以外的應用，如功能變數名稱解析區塊鏈 - Namecoin[12]、電子合約區塊鏈 - Ethereum、利用環狀簽名技術做到的完全匿名交易電子錢系統 - Monero[13]、區塊鏈為基礎的論壇 - STEEM[14]。

區塊鏈的應用大致可分為三類：區塊鏈 1.0，區塊鏈 2.0，區塊鏈 3.0。
(Melanie Swan 《區塊鏈：新經濟藍圖及導讀》[15])

(一) 區塊鏈 1.0 – 數位貨幣：

區塊鏈 1.0 為貨幣，主要體現於金錢相關，諸如資金轉移、匯兌以及支付系統。最常見的就是加密網際網路貨幣，而比特幣為最為著名的一種。且比特幣區塊鏈做為在全世界諸多國家最有效的跨國金流系統。加密網際網路貨幣藉由區塊鏈技術完成使用者與使用者間資金的轉移。

(二) 區塊鏈 2.0 – 智能合約

區塊鏈 2.0 為智慧合約的實踐，現今的區塊鏈技術著重於市場經濟及金融方面之應用，但除了純資金轉移外，生活中所創建之金融商品亦為區塊鏈化之對象，遠比簡單的資金轉移廣泛許多，如股票、債券、期貨、貸款、產權、智能資產和智能合約。由於區塊鏈 1.0 的初始階段被廣泛應用於交易的保存，但除了交易紀錄的應用，亦能視為一種用於記錄、追蹤、轉移所有資產的資料庫和庫存清單。且可做為任何形式的資產登記、庫存盤點和交易資訊的記錄。

(三) 區塊鏈 3.0 – 去中心化應用

區塊鏈 3.0 不僅僅只是脫離市場經濟及金融外之區塊鏈應用，著重于政府、健康、科學、文學、文化和藝術等領域。如醫療區塊鏈、食安區塊鏈、訂房區塊鏈和證書區塊鏈等應用可以說是勝枚舉，可以見得區塊鏈此項技術尚在萌芽階段，未來極具發展潛力，也因如此區塊鏈才能廣受各界青睞。

第二節 比特幣簡介與相關技術說明

本節當中將會對比特幣做簡單介紹，並解說比特幣用來交易的地址之生成方式與流程，最後提出比特幣現有的區塊

一. 比特幣簡介：

在中本聰的論文[16]中提出了不需要中央機構託付信賴機制的電子交易系統。此篇論文首先討論了電子貨幣的數位簽章原理，它提供了擁有者很大的控制力，但仍不足以防止雙重支付（double-spending）[17]的發生。為了解決這個問題，我們提出了一個採用工作量證明（proof-of-work）[18]機制的端對端網路來記錄交易的公開歷史資訊，若誠實的節點掌控了 CPU 運算能力，則攻擊者去竄改交易資訊是計算上不可行的。這個網路的強健之處在於其結構上的簡潔性。節點們不太需要彼此協調就能同時執行工作。

由於訊息不會被傳送到任何特定的地方，因此節點們不需要被識別，只需要以最大努力原則被傳送。節點可以自由選擇離開或重新加入網路，且會接受工作量證明鏈為當節點不在網路時所發生的交易事件之證明。節點以各自的 CPU 運算能力來進行投票，表決對有效區塊的驗證，以不斷延長有效

的區塊鏈來表示接受，而以拒絕在無效的區塊之後延長來表示拒絕。這個共識機制包含了一個端對端的電子貨幣系統所需要的所有規則及獎勵機制。

二. 地址生成方式：

可以用來收付款的比特幣地址生成需要遵循七個步驟，才能產出在比特幣網路中合法使用的比特幣地址，以下將依序闡述比特幣地址創建的過程，如下頁圖 3：

(一) Random：

使用亂數產生器產生一個長度在 256bit 以內的隨機數，而此隨機數即成為該地址的私鑰，在比特幣系統中，可以利用私鑰(Private Key)[19]簽署花費該地址當中的比特幣。

(二) Secp256k1[20]：

該演算法為一個以橢圓曲線演算法為基礎的一個標準，而在不同標準的差異在於初始化的參數，這些參數的訂定皆經過嚴謹的考核及實驗測試。在比特幣系統中該算法扮演著私鑰轉換為公鑰的角色。使得比特幣交易使用私鑰進行簽署之後，還可以使用公鑰校驗該比特幣交易的正確性。

(三) SHA-256：

一種雜湊函數，雜湊函數的特性有許多，包括雪崩效應、不可預測、不可逆、校驗檔案是否完整。在此步驟中是將公鑰帶入 SHA-256 函數中，產出長度為 256bit 的雜湊值。

(四) RIPEMD-160：

亦為雜湊函數的一種，特色符合雜湊函數的特性，與 SHA-256 不同的是 RIPEMD-160 產出的長度為 160bit。

(五) 加入版本號及校驗碼：

比特幣在一開始設計的過程中，便定義了不同的地址樣式[21]及功能，在第五個步驟中會加入版本號加以區分不同的地址。校驗碼為比特幣地址生成過程中重要的一環，可在支付比特幣的過程中解決因為手誤而將比特幣轉入到不存在(不符合比特幣地址生成規則)地址的可能性。校驗碼為將第四個步驟的產物加上版本號後，進行兩次 SHA-256 的運算，將其結果的前 32bit 作為校驗碼。

(六) 組合成地址格式：

版本號、第四個步驟的產物公鑰 RIPEMD-160 及第五個步驟的校驗碼合併。

(七) Base58 編碼[22]：

將第六步驟組合成的結果，利用 base 58 進行編碼，Base 58 為修改自 Base 64 其最大的不同在於移除了 "0"、"O"、"I"、"l"、"+"、"/" 的字符，可以降低人工判讀在地址的錯誤率。

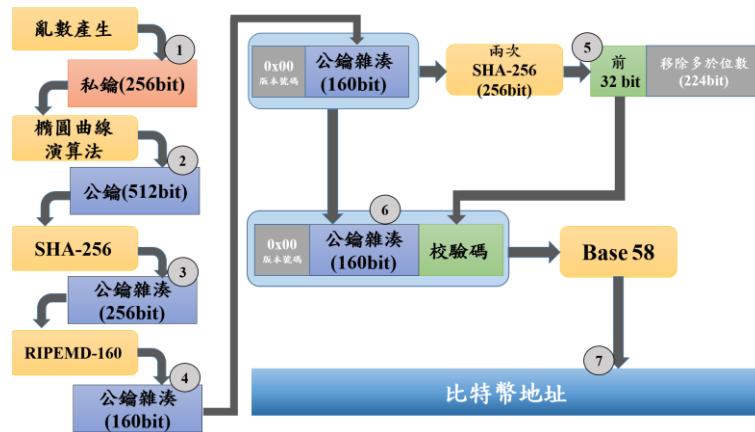


圖 3 比特幣地址生成流程圖

三. 挖礦與能源危機：

在比特幣的世界中「挖礦」並非實際拿著鏟子到地底去採礦[23]，而是指透過運算器去計算雜湊值，並找出符合當前系統要求的答案，如果找出符合要求的雜湊值便可以產生新的區塊以打包交易資訊並獲得相對應的獎勵，也就是比特幣。雖然說起來挺容易，但要找出符合系統要求的雜湊值並非一件容易的事情，因為雜湊並無規則可言，僅僅改變一個字元，最後產生的雜湊就會完全不同，因此只能透過窮舉找出答案，而當初中本聰在設計比特幣時亦將摩爾定律考慮在內，比特幣總產量上限為 2100 萬顆，且每四年會將完成任務時所能獲得的獎勵會減半，另一方面為了讓區塊產生的時間能夠維持在十分鐘左右，任務的條件還會越來越嚴苛，也因為這樣運算器的計算速度成了挖礦的關鍵，從一開始的 CPU 到 GPU、螞蟻礦機甚至是直接建置在水力發電廠旁，整座山那麼大的礦場，都是為了要挖出一顆又一顆比特幣。

隨著比特幣價格水漲船高，不少人紛紛投入挖礦的產業，但為了供給這些高檔的礦機運算，所消耗的電量可是不容小覷，根據「Bitcoin Energy Consumption Index」統計，截至 11 月 20 日，比特幣過去一年內挖礦的電力總消耗已累計達 29.51 兆瓦小時 (TWh)，約佔全球總電力消耗的 0.13%，相當於台灣一年電力消耗的 11.64%。該數字甚至已經超過近 160 個國家一年的電力消耗，包含冰島和奈及利亞；若全球的比特幣礦工自成一國，該國的電力消耗排名可排上全球第 61 名。報告指出，若比特幣能源消耗以目前每月增加 30% 的速度成長，預計到 2020 年 2 月，比特幣挖礦的電力消耗就會超越目前全球總電力消耗，也就是 22,383 兆瓦小時。

四. 比特幣區塊鏈問題

比特幣雖然為目前市值最高的區塊鏈加密貨幣，但其區塊鏈設計仍有需多不足的地方，例如區塊容量不足、區塊生成時間過長、技術拓展有限等問題。

(一) 區塊容量不足：

起初比特幣的設計為利用工作量證明演算法，使比特幣區塊的創建可以在平均約十分鐘完成，區塊的大小被訂定為 1MB，若假設區塊中接放滿了交易，以現今每筆比特幣交易大小均值為 300 位元組計算，每區塊可以容納至多三千多筆交易，也就是最多每秒鐘可以處理 5 至 6 筆交易，而中央化的電子支付公司（VISA）平時負載量已達到 2000 筆交易每秒，且上限可達 4000 筆交易每秒，反觀比特幣 5 筆交易每秒，比特幣的區塊鏈尚有很大的改善空間。

（二）區塊生成時間過長：

比特幣的區塊設計是基於工作量證明，難易度參數是作為比特幣區塊生成時間長度的關鍵，但工作量證明演算法解出問題的時間並不穩定，以比特幣為例，最快有三秒解出一題，最長也有五十多分鐘解出一題的現象。而為縮短生成時間並不能單一考慮將其複雜度降低使平均生成時間為五分鐘，當中需要顧及區塊生成時間過短，導致所有區塊鏈節點無法完成同步，發生區塊鏈分叉[24]，進而系統崩潰。

（三）技術拓展有限：

在比特幣系統中，為純記錄交易紀錄，無法擴展實踐更多功能及應用，也有許多開發者希望透過比特幣系統擴展智慧合約[25]相關的應用，但後來發現基於原本的比特幣系統框架為基礎在進行延伸是一件困難的事情，因而目前升為全世界第二大數位貨幣的作者 Vitalik 提出了新一代的數位貨幣系統，並創造了 Ethereum virtual machine 使得在 Ethereum[26]中所創建初的合約，有著統一的平臺可以運行，突破了比特幣的技術上的瓶頸。

五. 雙重花費的危機

由於比特幣的屬於開源系統，只要有心人人都可以編寫錢包的應用程式，若開發者有意則可能在地址及付款的行為上動手腳。以下介紹雙重花費的成因、危機以及現有的解決方式。

（一）雙重花費的成因與危機：

雙重花費(Double-spending, 簡稱雙花)問題存在於比特幣交易中，在未被區塊鏈確認收入到區塊鏈之前，都有機會受到惡意的攻擊者重複消費同一筆金額，而這些雙花交易會存在於交易緩存池當中，雙花的交易會在記載到區塊中的同時被過濾。現今的比特幣區塊產出速度為十分鐘一塊，但十分鐘的確認時間會對實體店面的小額交易處理非常的不友善，如下頁圖 4 所示。以下為雙花的發生流程：

1. 惡意攻擊者 A 地址付款。
2. 商家未確認該筆交易進入區塊就將商品交付給惡意攻擊

者。

3. 惡意攻擊者帶著商品離開店家並在該筆交易進入區塊以前，又一次以A地址付款，但是將裏頭的餘額轉入自己的B地址，同時提高手續費，以達到插隊的目的，使得第二次的交易會先被礦工驗證，原先的交易則因為A地址已經沒有餘額而交易失敗，與此同時惡意攻擊者幾乎是以無酬的方式取得該商品。

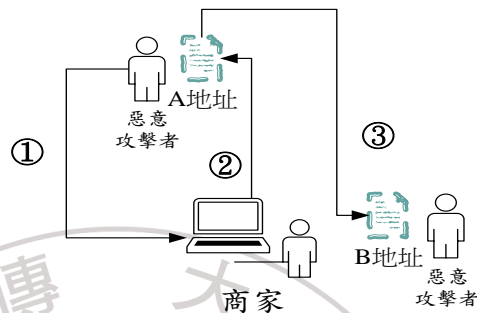


圖 4 雙重花費流程圖

(二) 雙重花費現有的解決方式：

為了在既有的比特幣區塊鏈的框架底下能夠提升交易速度，因此綠色地址(Green address)技術[27]致力於在一開始創建交易的同時管控雙花交易的發生，綠色地址的技術採用了 2-of-2 多重簽章，2-of-2 的意思是創建一個特殊的比特幣地址，這個比特幣地址的持有人有兩個代表人，其一為使用者，另一位則為比特幣綠色地址代理節點，這筆交易的建立必須要雙方同時簽署才得以被消費；除此之外，若是交易手續費過低會造成交易在緩存池內的排隊序位難以前進，若碰巧遇上交易量爆發的事件，造成節點緩存池空間不足的問題時，比特幣節點會優先遺棄手續費最低的交易，且該筆交易視同不曾存在過，故若真的遇到交易被遺棄的情況，綠色地址代理節點也會透內部的資料庫紀錄再次廣播此筆交易，並確保此筆交易可以被收入至區塊內。綠色地址代理節點也就成為了交易創建的把關者，過濾所有的雙花攻擊的發生，也避免交易因為塞車而被礦工遺棄的情形。

在這樣的機制下，只要是用綠色比特幣錢包交易即可確認雙花攻擊是不會發生的，對商家或是收款人而言，可以得到在即時交易中不被雙花攻擊的保障，提升在未進入區塊鏈的交易可確定性，進而創造出即時交易的可行性。以下為透過綠色錢包的交易流程，如下頁圖 5：

1. 使用者以 Green address 錢包應用程式發起交易，並且以用戶端的私鑰簽署本次交易。

2. 綠色地址代理節點收到用戶傳來的此筆交易資訊，會驗證此地址是否可能為雙花攻擊地址，若非惡意地址，便提供代理節點端私鑰以簽署交易。
3. 取得客戶及代理節點端私鑰後，綠色地址錢包便可透過代理節點發送此筆交易訊息至比特幣節點內。

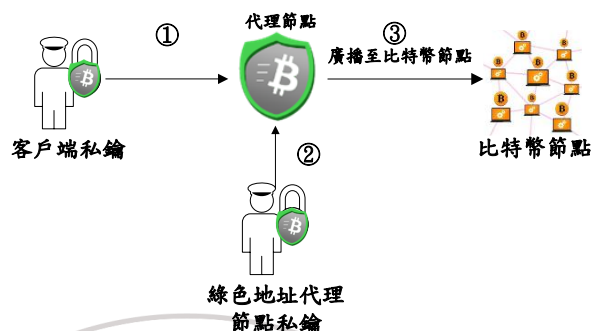


圖 5 綠色地址錢包交易之流程圖

第三節 比特幣的危機與國際情勢分析

自中本聰的論文發表以來，比特幣不斷的在累積其發展的能量，直至 2017 年末可以說是比特幣以及其他所有區塊鏈加密貨幣爆發的一年，不論是其市場價值或是技術拓展，但隨著比特幣的發展，與此同時也帶給了世界各國政府全新的挑戰，因此並非有政府都能接受比特幣在境內發展，本節將介紹比特幣帶來的危機，並簡易分析近期世界各國對於加密貨幣的態度。

一. 比特幣的危機：

就目前而言有兩個最常聽到將比特幣應用於非法之處，皆是看上了比特幣的匿名性，其一為暗網[28]的交易貨幣，其二則是作為勒索軟體支付贖金的方式，也因為以上這些不量的應用，迫使不少國家對於比特幣是進而遠之；但除了這些危機，泡沫化也是許多政府單位所擔心的事情，因此本節將針對暗網、WannaCry 及比特幣泡沫化作相關探討

(一) 暗網：

一般使用者正常使用自由且開放的網路資源我們稱為表網 (Surface Web) 大約僅占全網的 4% 左右，如：google、facebook 等……而其他 96% 的資源我們稱作深網 (Deep Web) 主要是那些需要有特殊權限才可以使用的網路資源，如：企業網路、需要登入帳戶、有資料存取權限控管的資源等…然而這些看似正常的深網，其中包含著一小塊黑暗的世界，這些區塊被人們稱之為暗網 (Dark Web)，其內容包含大量的非法資訊，可以說是虛擬世界中的真實地獄，如下頁圖 6。

贖金，實在相當的驚人。

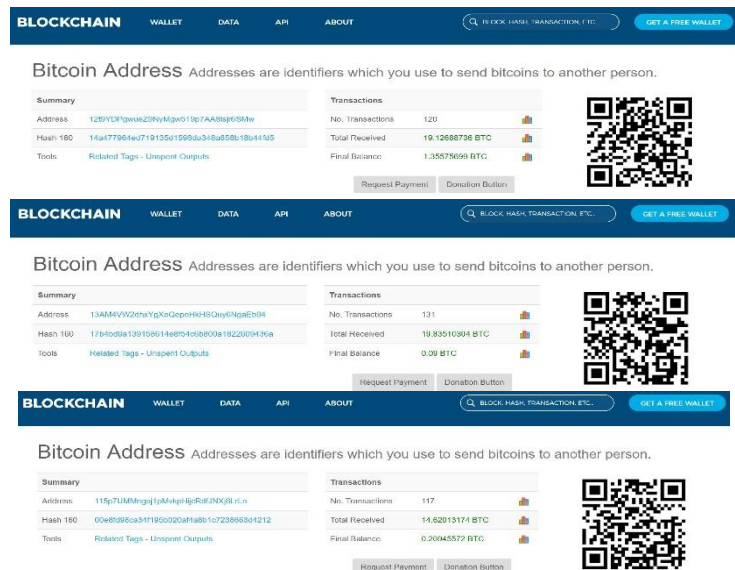


圖 8 收取贓款的地址追蹤

(三) 泡沫化：

從比特幣出生以來，每一次的上漲都會有所謂的銀行專員或是政府出面呼籲民眾審慎投資比特幣，但一次又一次比特幣的價格都突破了他們的預想，不過這樣的情形、這樣的價格真的就是比特幣創始人—中本聰所樂見的嗎？比特幣真的是因為被世人廣為接受並用於去中心化交易才有如今的價格嗎？很顯然答案並非如此，現今這些價格大多是受到炒作及吹捧才應聲而起，但這樣的情形也造成交易手續費暴漲及交易塞車等窘境，絕大多數的持有者都是短期投機客戶，然而真正看到其技術、特性與未來的人又有多少呢？假如這些短期投機者急速退場，比特幣還會有現在這樣的價格嗎？

然而號稱比特幣聖經[31]—「精通比特幣」其作者「Andreas Antonopo」更是直接指出：「我們看到的是一個由炒作和貪婪所組成的泡沫。」Andreas Antonopo 不僅是比特幣愛好者更是底層技術者，來自於他的警語自然比起其他領域專家的告誡更讓人擔心更加發人省思。

二. 國際情勢分析：

比特幣的應用有正向的也有反面的，因此世界各國政府的態度也並不一致，大略可以分成三種對應策略[32]，第一種如以色列、法國、新加坡等…國家則認為比特幣對於金融發展是利大於弊，所以抱持者歡迎或放任的態度；另外一種，像韓國、菲律賓、馬來西亞等…國家則是認為比特幣這類的加密貨幣會影響國家金融策略或是危害人民的財產安全，因此正在著手修法監管相關貨幣；最後則是印尼、摩洛哥及眾所矚目的中國，這些國家認為比特幣

這類的加密貨幣不應該國內流通甚至是發展，因此紛紛宣告境內禁止國內的加密貨幣交易，如下表 1。

表 1 各國政府對比特幣態度統整表

序 號	國 家	接 納		禁 止
		歡迎/放任	監管	
1	以色列	歡迎：欲發展國際 ICO 中心		
2	韓國		很快將監管交易所	
3	菲律賓		計劃監管 ICO	
4	法國	放任：與實體經濟無關		
5	辛巴威			定法前，屬非法
6	伊朗	監管得當歡迎比特幣發展		
7	摩洛哥			禁止加密貨幣交易
8	印尼			2018 年前全面禁止
9	馬來西亞		正規化監管框架	
10	新加坡	不監管但注意周邊活動		
11	沙烏地阿拉伯	加密貨幣尚未成熟，不監管		
12	白俄羅斯		2018 年 7 月前完成立法	
13	日本		任命加密貨幣監察長	
14	香港		ICO 須受法規監管	
15	烏克蘭	不屬於貨幣		
16	中國			禁止加密貨幣

我們回頭來看看台灣對於比特幣的態度為何[33]？根據金管會顧立雄主委指出：「比特幣目前屬於虛擬商品，交易被歸類為以物易物的形式，故只要不涉及金融法規或刑責，金管會暫時持觀望、容忍的態度，不會馬上立法納管。」統整了以上國家的政策態度，我們可以看到目前世界上的趨勢，接納比特幣之國家較反對派數量高出約三倍之多，因此我們認為比特幣相關產業是相當有成長的潛力的，如下圖 9。

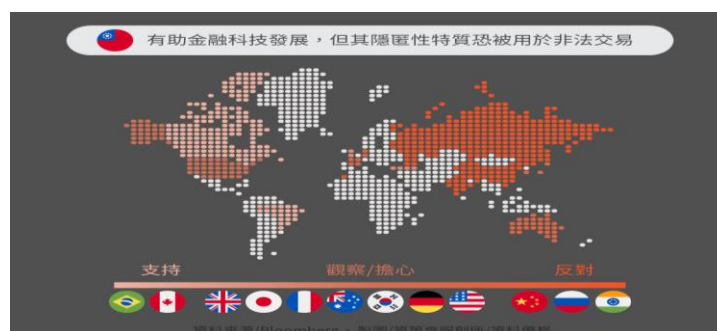


圖 9 各國央行對比特幣態度

第參章 研究方法

本章主要透過分析並比較各種貨幣交易之方式，以確立本系統之系統架構以及系統流程，並且詳細說明本系統之建置環境、架構以及流程。

第一節 貨幣交易關係比較

本節主要藉由探討目前市面上各種常見的貨幣交易關係，並加以分析與比較，再藉由本節之分析結果，確定最適合本系統之交易關係。本節當中主要分析現金貨幣、VISA[34]、支付寶、PayPal 及數位元貨幣以上五種交易模式之關係。

一. 現金貨幣(匿名對匿名的交易模式或匿名對實名的交易模式)：

[35]最早人類的交易行為可以探究到以物易物的交易行為模式，進而發展出銅幣、紙幣、金幣，甚至是現今常聽聞的金本位制度。

在交易的過程中商家無法知道消費者的真實身分，而在一些沒有收據的環境下，如雜貨店或是攤販、一些沒有開收據的商店，消費者也不知道商家的真實身分，故將此交易模式定義為”匿名者與匿名者之間的交易模式”，此交易模式商品亦為匿名。在這樣的交易模式下，消費者保持匿名，對消費者而言，可以有效的保護消費者的個人資訊安全，因為在貨幣的持有的方式，並不需要登記姓名，資產轉移的過程中一不需要。

對於消費者而言，雖然消費者的匿名保護了自己的個人資訊，但商家的交易資訊也是匿名，對整個交易結果若有爭議，這便造成追訴無門的結果。而在交易並未被有效紀錄的情況下，政府對稅收的計算，會進入無法計算的灰色地帶。下圖 10 為匿名的消費者對未開立收據或是實名制的商家的交易模型。

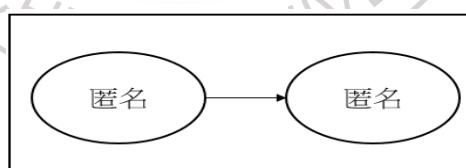


圖 10 現金貨幣交易模型 - 無收據交易

在另一個場景中，在交易進行的過程中，消費者為匿名，商家具有實名，對消費者而言因為自己本身並無綁定個人資訊，故對各資隱私有很大的保障，消費者消費的物件店家具有實名而開立收據，對消費者而言會得到消費紀錄的保障，對消費的糾紛有店家可以追溯。對政府，因為交易的紀載使得稅收的計算變得容易。下頁圖 11 為消費者使用現金對已經實名制或是開立收據的商家消費的模型。

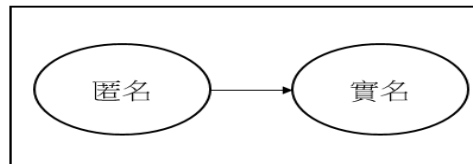


圖 11 現金貨幣交易模型 - 實名店家

二. VISA(實名對實名的交易模式)：

現在最為常見的卡片貨幣支付管道 Visa 中，因為當年的設計並無類似區塊鏈去中心化的理論、技術提出，因而資金的轉移設計會是銀行帳戶與銀行帳戶間的資金轉移，也因為這樣的設計，造成交易的基礎被規範在實名與實名之間的交易模式，這樣的交易模式，雖然快速且方便，但在無形之中透漏了許多消費者的個人資料。在交易手續費方面，Visa 的手續在跨國刷卡的場景下，皆需要收取高達百分之一點五的手續費，對於消費者而言使用 VISA 作為支付會帶來不小的負擔。下圖 12 為透過實名制支付管道對商家進行交易的模型。

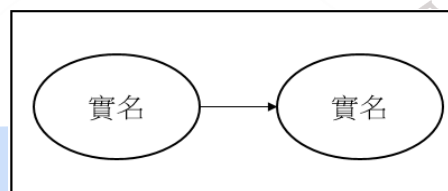


圖 12 VISA 交易模型

三. 支付寶

在中國 VISA 較不為常見，但除了 VISA 電子支付還有中國本身自營的銀聯，但因為中國的銀行眾多林立，且在科技化的世代中隨身帶著許多的卡片會造成相當不便，所以支付寶致力於將所有的卡片電子化，將所有中國在的銀行卡統合在一起，如此的集成所有的銀行卡的工作，可以有效的讓卡片交易更加的方便，下圖 13 為以實名制的銀聯卡透過支付寶進行支付給實名制的店家的交易模型。

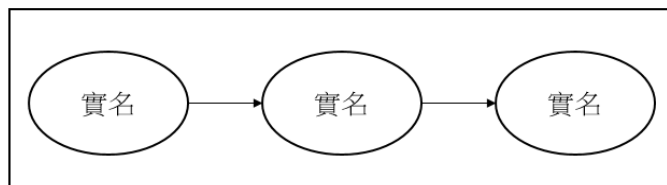


圖 13 支付寶交易模型

四. PayPal(匿名對實名交易模式)：

為了解決在進行交易的過程中，使用 Visa 支付管道會透露太多的消費者個人資訊的問題，PayPal 便致力於將消費者的銀行卡相關的個人資訊全部寄託在 PayPal 身上，PayPal 再以公司的身分，將資金轉移給商家，消費

者與店家的交易中間多了一個仲介的角色，這樣的交易模式也讓看似匿名的消費者對上實名的商家。但在這樣的交易過程中，大家的信任需要寄託在 PayPal 身上，畢竟大部分的銀行卡與個人的資料皆寄託在 PayPal 公司內，PayPal 公司的資訊安全將成為最重要的議題。下圖 14 為先以實名制的支付管道將資金轉移到待支付的 Paypal 公司，Paypal 代為支付的過程中將原資金來源的個人相關資料保護在 Paypal 公司中，以製造出一種匿名支付方法保護消費者的個人資訊的模型。

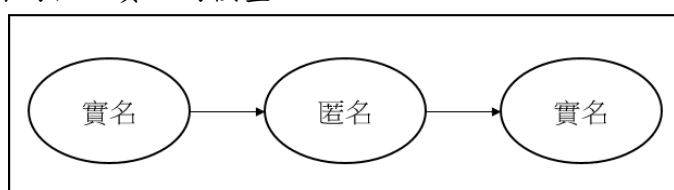


圖 14 PayPal 交易模型

五. 數位元貨幣(匿名對匿名交易模式或匿名對實名交易模式)：

在數位貨幣的交易中，與現金相當類似，屬於一種匿名對匿名的交易，與此同時交易的商品資訊也完全不被記載在網路上，因為在數位貨幣的交易中，所有人都可以創建數個比特幣地址，而在創建地址的過程中，卻與現實生活中的真實身分並無任何關聯性，因此可以創建匿名帳戶，且對一個匿名帳戶進行支付，這樣匿名對匿名之間的交易，對消費者而言雖然保護了個人資料，但與此同時商家也是匿名，倘若在交易中遇到問題，消費者便無人可以追溯。

匿名與匿名間的交易及匿名與實名間的交易，都是對消費者的個人隱私保障方式，但匿名對匿名的交易模式對政府與公司審計方面無法帶來很有效的統計方法，為了要使數位貨幣能夠更有效率的進行統計及做出更多的報表帳務，因此本論文致力於設計一個可以方便進行監查交易狀況甚至可以進一步作為國家級監管的數位貨幣交易模型，不僅可以對店家的帳單管理做出更方便的監察方案，更可對政府計算繳納稅收更加透明化。

綜合上述五種交易方式，我們可以統整出一張交易關係比較表，如下頁表 2。我們可以發現除了部分數位元貨幣以及用現金與未開收據的店家做交易，這兩種方式最能保障消費者，但後者會讓商家成為匿名交易者，否則現今絕大多數的交易商家皆為實名制，即是為了保障消費者的權益，然而目前最廣為人知的數位貨幣是比特幣，在它的區塊鏈上只能查看透過雜湊處理所得的地址，無法得知交易雙方的真實資訊，倘若比特幣被用來執行非法交易、或是交易產生爭議，都無法輕易認定區塊鏈上的交易與現實生活中的交易是有關聯的。因此本系統致力於將比特幣從匿名對匿名的交易，強化成匿名對實名的交易，一方面便於政府監督社會上的金流，另一方面也可讓使用者在以比特幣交易時更有保障。

表 2 交易關係比較表

	顧客	仲介單位	商家	商品
現金	匿名	無	匿名/實名	匿名/實名
VISA	實名	無	實名	實名
支付寶	實名	實名	實名	實名
PayPal	實名	匿名	實名	實名
數位貨幣	匿名	無	匿名/實名	匿名/實名

第二節 數位貨幣的仲介商機

此節主要講解有仲介單位的數位貨幣討論，本論文以目前台灣知名的比特幣兌幣所—「幣託」作為討論的對象，該交易所為顧客提供線上購買比特幣並代替顧客掌管比特幣錢包，雖然比特幣是一種去中心化的貨幣，但如果想要在一個合法的國家公開販售比特幣，就必須先通過政府、銀行的關卡，經由實名制的認證才可購買比特幣，以下將分別介紹其營利模式與發展困境。

一. 營利模式：

幣託主要提供顧客以法幣兌換比特幣的服務，並期許讓數位貨幣的交易更容易、使用更方便、應用更全面、交易更有保障。其獲利模式為抽取顧客購買比特幣金額的 1% 作為手續費，再以這 1% 手續費中的 5% 作為營業稅繳交給政府。

二. 發展困境[44]：

由於目前政府認定比特幣屬於數位金融商品而非貨幣，因此以法幣兌換比特幣的行為在政府的眼中，是屬於購物而非兌幣的行為，如果是購物那就必須繳交相對應的稅金，也就是消費稅的 5%，此稅金也自然而然轉嫁至消費者身上，相對的若是顧客想要將比特幣兌換回法幣，政府又認定其是購物流程，因此又再課徵一次 5% 營業稅，這樣一來一往，兌幣的行為就被課徵了三次的稅金，這種雙重甚至三重課稅的問題，造成顧客或是業者都相當不友善，也是目前國內兌幣所遇到的一大困境。

第三節 行動支付的便利與危機

隨著智慧型手機的發展，以行動支付作為交易管道的情形逐漸普及，市面上也衍生出數十種的行動支付應用程式提供給消費者選擇，因此本節將簡述行動支付（Mobile payment）技術，並提出目前市面上的行動支付可能暗藏那些危機？

一. 行動支付 (Mobile payment) 簡述[36]：

「時間就是金錢」可以說是行動支付的最佳寫照，行動支付不僅可以讓顧客省去掏錢、找零以及將錢收入皮夾內的時間，還可以將交易收據、發票等資料從實體化的紙張走入虛擬化，這樣不但能有更多資料顯示方式，還能夠更輕易的活用這些交易數據，例如：顧客可以結合行動支付與理財記帳和發票兌獎系統，使生活更便利，且省下的紙張也能夠節省大量的資源，行動支付可以說是一舉多得的支付方式。

要完成一次行動支付的流程，主要必須通過五個關卡，分別是付款方式選擇、資料傳輸方式、應用模式、身分識別及安全機制，下頁表 3 為行動支付的關卡表格。

(一) 付款方式：

依照應用程式的規範，付款方式可能是綁定金融卡或是信用卡等。

(二) 資料傳輸方式：

這邊的資料通常是指交易的資訊，坊間常用 QRCode、NFC (Near-field communication)、Buletooth 或是 Short Msg 等方式將交易清單或資訊由商家設備傳送給顧客的行動裝置。

(三) 應用模式：

這邊是指付款的模式，可能完全是應用程式的框架，也有以網頁形式呈現，不過也有許多將簡易 browser 鑲入應用程式的「混和型」支付應用程式，以上三種是較常見的付款模式。

(四) 身分識別：

為了避免行動裝置遺失進而遭到盜用，因此絕大多數應用程式都會對付款人進行身分驗證，以確認是帳戶持有者的本人進行交易，可能是指紋辨識、密碼、OTP 等方式。

(五) 安全機制：

當我們將信用卡、金融卡用來交易的資訊存入行動裝置中，那這些資料絕對非常敏感，如何確保這些資料的安全性勢必有非常重要的地位，通常都是透過加解密或是 Token 等方式以確保資料安全性。

表 3 行動支付的五個關卡

	付款方式	資料傳輸	應用模式	身分識別	安全機制
舉例	信用卡	QRCode	應用程式	指紋辨識	Token
	金融卡	NFC	網頁型	用戶密碼	加解密演算法
		Bluetooth	混和型		

二. 行動支付所遇到的危機：

雖然行動支付為人們帶來了一種更便利的付款方式，但我們可以仔細想想可以發現，為了付款的便利性我們所付出隱性的成本多麼高，當我們將金融卡或信用卡的付款資訊存入行動裝置的系統內，若行動專制受到黑客攻擊，就已經構成了第一種的威脅，且市面上大大小小的支付應用程式，真的所有的程式都有足夠的安全強度機制頗受質疑，下圖 15 為實際走訪超商查看行動支付種類；其次商家所建立的交易資訊是否有妥善保管也是一大隱憂，最後則是各大銀行儲存了大量用戶的付款資訊，容易成為駭客鎖定攻擊的目標，屆時用戶隱密的個資就不再受到保障，對於這樣的問題如何讓用戶能夠信賴商家、信賴銀行能將資料保存好？這可以說是行動支付的一大挑戰。



圖 15 行動支付種類繁多

第四節 系統模型與開發背景

雖然比特幣為開源系統，但由於現今比特幣價格不斐，截自至今(2017/12/20)一顆比特幣兌換美金的均價約為 16716.48 美元，倘若利用比特幣作為開發系統，系統開發交易手續費所產生的成本將會難以估計，故本系統選擇使用比特幣作為開發測試用的測試幣作為研究的基底，由於測試幣系統內的所有演算法皆與真實比特幣系統一致，包括錢包的加密、公私鑰的產生、交易的認證及錢幣的發行都與真實系統相同，唯一的差別只在於測試幣建立於與比特幣不同的區塊鏈上，並且市場價值極低，因此測試幣為開發本系統模型的不二之選，故本系統選用測試幣在 Github 上之 Android App 的開放原始碼應用—Testnet[37]作為開發基底。測試幣之圖示如下頁圖 16。



圖 16 Testnet 之 icon

因為需要修改並強化比特幣之測試幣的功能，所以本論文在開發軟體上選擇目前市面上功能最為強悍的 Android 開發編譯器「Android Studio」作為開發環境，下圖 17 為 Android Studio[38]之圖示。



圖 17 Android studio 之圖示

另外一方面本系統需要讓商家可以快速且便利的完成結帳及收銀之動作，故選擇由 Google 與手機大廠 LG 共同發行之 Google Nexus 5 及 Google Nexus 5X（如下圖 18）兩部手機作為搭載系統及系統測試之硬體設備，該手機之優勢為系統更新速度快，且兩部手機皆擁有近場通訊（Near-Field Communication，NFC）[39]功能，為本系統所需之重要功能。



圖 18 Google Nexus 5 與 Google Nexus 5X

資料庫方面本系統則是以 XAMPP（X, Apache, MySQL, PHP, Perl）[40]作為伺服器與資料庫架設方式，XAMPP 是一個把 Apache 網頁伺服器與 PHP、Perl 及 MariaDB 集合在一起的安裝包，允許用戶可以在自己的電腦上輕易的建立網頁伺服器。本系統手機端之資料庫服務即透過 XAMPP 與伺服器及資料庫溝通，如下圖 19。

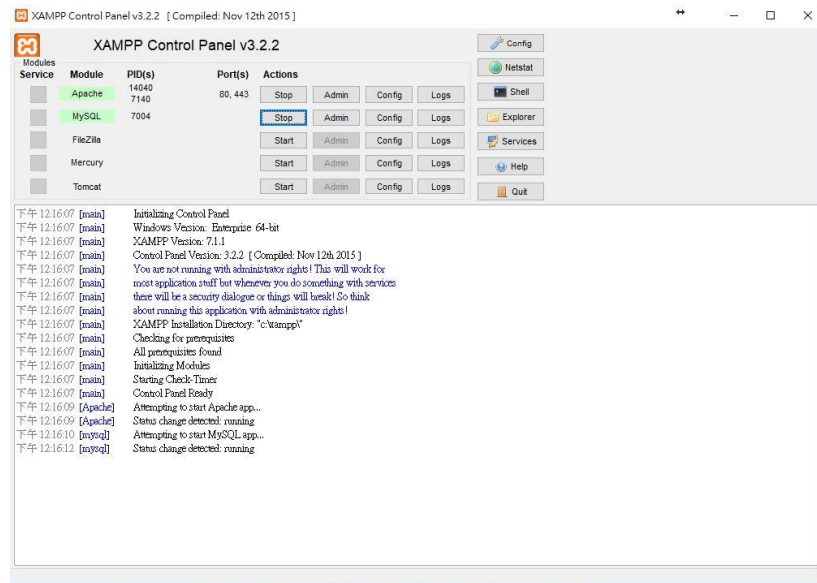


圖 19 XAMPP 圖示

第五節 系統模型架構

本系統[41]主要是以完成基於比特幣之商業收銀系統模型建置與實作為主要目標，進而將積極利用自由軟體的利基：使用成本低、進入門檻低、開放原始碼、社群能力強、共通性及移植性強、資通安全性高等優勢來開發本論文所提出的以比特幣為例的數位貨幣交易收款監督系統的應用服務平台。

本論文嘗試建置與開發的系統範圍包含建置下面主系統與各項子系統，主系統為：**基於區塊鏈技術的收款監督系統(Blockchain-based Payment Collection Supervision system, BPCS)**，而各子系統分別為：

一. 政府端加密貨幣交易監察子系統

政府可透過讀取本系統資料庫的交易數據，得知各商家單位時間的交易情形，以確保交易的合法性，並依據法規抽取相對應的稅金，為便利稽核人員在操作上的便利性，此一子系統以網頁形式呈現，透過網頁快速且有效率的整理出各項政府所需要的數據資料，如銷項稅額、進項稅額即應繳稅額等資訊，政府課徵單位便可依此數據做為國內加密貨幣交易課徵稅金之依據，藉此提高商家繳納稅金的方便性及公平性。

為確保資料庫安全，此系統僅提供訪問資料庫之功能，其他包含新增修改及刪除之功能皆不包含在政府端之子系統中，透過這樣的設計，讓政府端的使用者能夠在不影響需求的情況下，也能使資料庫之安全性向上提升。

二. 商家端建置與管理商品資訊子系統：

本系統可以讓商家在進貨時，快速地將 RFID 標籤之識別碼與進貨商品資訊整合在一起，並且透過本系統新增、修改或刪除資料庫內部的資訊，包括產品名稱、詳細資訊、存貨數量等資訊，甚至可以將商家 GPS 地址或是

進貨時間這類更詳細的商品資訊儲存在資料庫內，商家與顧客便可依照該資料庫取得當前商品資訊與狀態。不僅讓商店的存貨資訊更加清楚明瞭，也可以提供顧客更多的即時服務。

三. 商家端行動收銀與交易明細子系統：

本系統使商家在結帳時，能夠以手機 NFC 功能掃描商品上的 RFID 標籤，即可簡單地建立交易清單，並透過 NFC 與顧客手機碰觸，將交易清單以及商家之比特幣收款地址等等重要交易資訊一併傳遞給顧客，可以簡短結帳的速度，使結帳效率大幅提升。

四. 顧客端行動支付與交易明細子系統：

顧客在結帳時，不必再麻煩的拿出信用卡或是零錢包，只需要拿出手機讓店員以 NFC 將交易清單與比特幣地址轉送給自己，即可自動連結至比特幣電子錢包的應用程式當中，並且自動填妥相關資料，如：交易金額、收款地址等等與此同時也能將交易紀錄儲存於客戶端，以便日後顧客快速取得過往的交易紀錄，除此之外亦可讓廣大的民眾體驗數位加密貨幣與行動支付帶來的便利生活。

第六節 系統模型流程與資料庫架構

系統運作的流程，主要分為兩個步驟：第一個步驟為商家的註冊與認證，第二個步驟則是創建與驗證一筆交易，下圖 20 為商家註冊流程圖。

一. 商家的註冊與認證流程

商家註冊流程如下

(一) 註冊：

商家必須對本收款監督系統註冊帳戶，並且提交依照政府規定應提出的相關商家證明。

(二) 審核：

本收款監督系統收到註冊申請後，便會自動的將商家所提出的註冊申請表傳送給政府的相關部門進行審核。

(三) 批准：

政府批准了該商家提出的申請，伺服器便會激活此商家在本收款監督系統創建出的帳戶。

(四) 正式啟用：

商家獲得政府的批准後可以自由的登入該帳戶並且管理該商家所要銷售的產品。

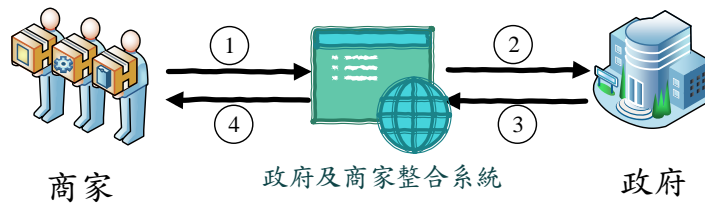


圖 20 商家註冊流程圖

二. 商家及顧客創建與驗證一筆交易之流程，如下頁圖 21：

商家與顧客創建與驗證一筆交易之流程如下

- (一) 商家的店員將手持的平板電腦或是手機透過先前已經以商店名義提出申請的帳號，並且已經通過政府機構的審查稽核，才得以登入該系統。
- (二) 登入本數位貨幣的商家收銀金流監控系統後，便會載入該店家註冊的商品資訊形成商品目錄，商店的店員可以依照客戶的需求進行點單選取數量；若商品包含 RFID 標籤且已建置完成，亦可透過手機 NFC 功能掃描商品 RFID 標籤，即時取得商品資訊。
- (三) 選擇完各個商品的數量之後，便可快速建立交易清單，並透過 Testnet 的請款頁面建立一個全新的比特幣收款地址，再以 Android Beam 的方式將商家店號、收款地址與消費總金額等資訊輕鬆地傳得給顧客。
- (四) 在商家店員的平板電腦收到這筆交易信息之後，會對本監控系統重送一個副本進行存檔。該交易資訊包括由監控系統所提出的交易流水號、商家編號、商品編號、商品購買數量以及數位貨幣的收款地址，以及消費者的發款地址。
- (五) 消費者收到交易信息後，手機會自動開啟 Testnet 的付款頁面，確認金額與店家無誤之後便能以匿名的數位貨幣比特幣進行支付，此時交易的款項便會被簽發到比特幣網路中，進行驗證以及記載。
- (六) 區塊鏈檢視器便會開始分析比特幣網路中存在的所有在緩存池[42]中的交易，以及已經被記錄到區塊鏈中的交易。
- (七) 本交易監控系統會向區塊鏈檢視器會基於第四部所存儲的交易副本中的數位貨幣收款地址以及預付款的數位貨幣地址提出交易信息的查找，檢查該筆交易是否已經存在於區塊鏈中的緩存池當中，若已經確認進入緩存池，則在交易資料庫中的交易待確認欄位變數更改為代表交易完成之變數。
- (八) 在交易確認之後，便向商家店員的平板電腦送出交易已經成交的信息，此時完成交易，與此同時也將一筆交易資訊建置於系統資料庫內。
- (九) 對於政府而言可以隨時調閱全部商家的交易資訊，以作為來繳納稅

務的審核參考依據。

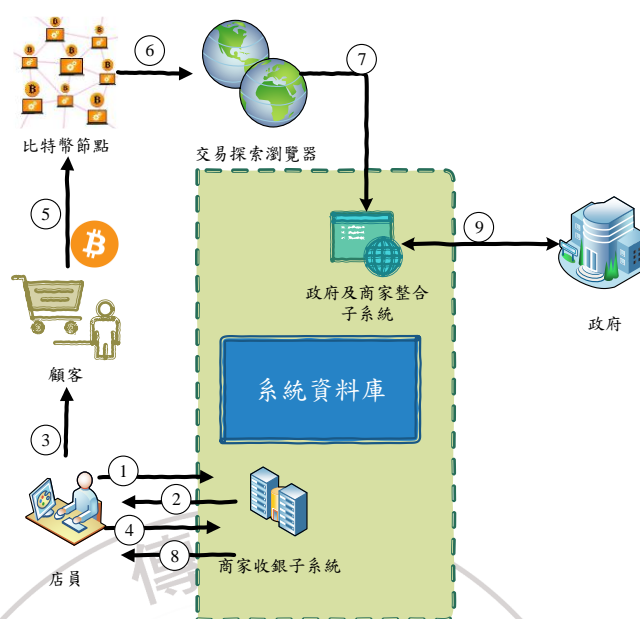


圖 21 商家創建與驗證交易流程圖

三. 資料庫架構

本系統資料庫主要分成使用者資訊、庫存、交易紀錄及商品訊息以上四個資料庫：

(一) 使用者資訊資料庫：

儲存所有使用者資訊，包括政府、商家及顧客之個人帳戶資訊的資料庫，政府單位有權限查詢商家部分商品及交易資訊，以利監督及稅收的執行；商家則是只能對自己店家的商品、工作人員及交易資料執行管理。

(二) 存貨資料庫：

此資料庫儲存所有商店的商品庫存，是從商品訊息資料庫及商家資訊結合庫存資料所產生的資料庫。

(三) 交易紀錄資料庫：

紀錄所有商店與顧客交易後的資訊，僅提供政府及該筆交易的店家與顧客查詢。

(四) 商品訊息資料庫：

詳細記錄各項商品訊息的資料庫，商家擁有查詢及管理自己的商品訊息資料庫權限，並開放給顧客查詢的權限，以利民眾了解店內商品資訊。

第肆章 研究成果

本章主要分成兩個小節，第一節主要介紹系統建置成果，將說明本論文的四個子系統；第二節則分別以一般測試鏈上測試交易速度，對比以綠色地址錢包作為交易的速度之實驗，主要目的是為了確保比特幣交易寫入區塊鏈中緩存池所花費的時間，不會影響交易流暢度的實驗。

第一節 系統介紹

本節將詳細說明目前系統建置的進度，逐一介紹商家端建置與管理商品資訊子系統、商家端行動收銀與交易明細系統及顧客端行動支付與交易明細系統以上三個子系統之功能與介面，並搭配系統截圖作為解說。

一. 政府端加密貨幣交易監察系統

此系統主要有三個功能，分別是首頁、申請表單及商家資訊，以下將一一介紹：

(一) 首頁：

政府端用戶登入後可於此介面查看各部門公告資訊，並發布相關公告，如下圖 22。



圖 22 政府端首頁

(二) 申請表單：

可於此介面查詢所有申請表單支商家，並查看商家詳細資訊，再依照政府端之規定，查核該商家設立是否合法，若申請成功可直接於此介面核准並由系統給出隨機的營業編號，如下圖 23 所示。

申請編號	商家名稱	統一編號	核准狀態
0901	統一超商	9527	未核准
0902	統一超商	9487	未核准

圖 23 政府端申請表單介面

(三) 商家資訊：

可於此介面查看所有已通過申請的商家詳細資訊，包含當月交易量及本期應繳稅額等資訊，如下圖 24。

申請編號	商家名稱	統一編號	商家地址	本月交易量	本期應繳稅金	登記日期
0901	統一超商	9527	桃園市龜山區復興路1號1樓	5000筆	105.770元	20171225
0902	統一超商	9487	桃園市龜山區復興路1號1樓	8545筆	105.210元	20171221

圖 24 政府端商家資訊一覽

二. 商家建置與管理商品及交易明細子系統

此系統目前主要有四項功能，分別是首頁、商品查詢、交易查詢及新增商品，以下將逐一介紹各項功能：

(一) 首頁：

商家端登入後可以查看各部門所發布的消息以及系統公告，如下圖 25。

系統公告	最新消息
<ul style="list-style-type: none"> 1. 公告事項 2. 公告事項 3. 公告事項 4. 公告事項 	<ul style="list-style-type: none"> 1. 公告事項 2. 公告事項 3. 公告事項 4. 公告事項 5. 公告事項 6. 公告事項 7. 公告事項 8. 公告事項 9. 公告事項 10. 公告事項

圖 25 商機端首頁

(二) 商品查詢

透過此介面，可以查詢所有屬於該商家的商品，如下圖 26。

商品編號	商品分類	商品名稱	商品數量	商品單位	商品規格	單價(mBTC)
0001	飲料	生油/米油	130	罐	5500L	0.45
0002	泡麵	龍力炸醬麵	90	包	120g	0.12

圖 26 商家端商品查詢

(三) 交易查詢

若交易有爭議或是需要回訪交易資訊，則可以透過此介面做查詢，點擊欄位則可以查看詳細交易資訊，如下圖 27。

商品編號	商品名稱	商品數量	商品單位	商品規格	單價(mBTC)
0001	生油/米油	130	罐	5500L	0.45
0002	龍力炸醬麵	90	包	120g	0.12

圖 27 商家端交易明細

(四) 新增商品

如果新增商品資訊，則可以在此頁面進行，如下圖 28。

商品編號	商品名稱	商品規格	進項數量	進項單位	進項單價	小計

圖 28 商家端新增商品

三. 商家行動收銀與交易明細子系統

本段將詳細介紹以商家行動收銀與交易明細子系統的使用方式，從系統登入至創建、完成交易及查詢交易資訊：

(一) 系統載入介面：

點開本系統，系統會產生一個 Bitcoin 的圖示，並將該圖示以淡入的方式顯示圖片，如下圖 29 左 1，與此同時可以作為載入系統參數的緩衝時間，當系統參數讀取完成，系統便會自動轉跳至接下來的畫面—登入介面。

(二) 登入介面：

在此介面中使用者可以輸入已註冊的帳號及密碼，如下圖 29 左 2，系統會將帳號及密碼傳送至資料庫進行比對，若驗證成功則可以登入至商家或是顧客的介面；另一方面使用者可以經由點擊上方 Bitcoin 圖示以切換登入的身份，如果是以商家登入則會進入掃描商品資訊的介面。

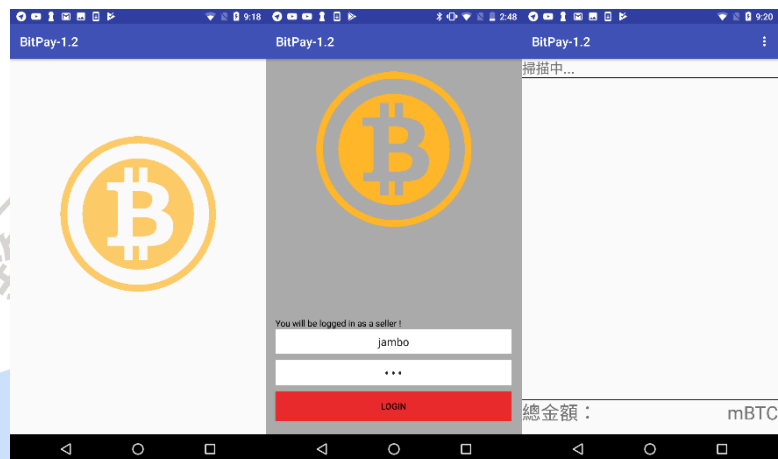


圖 29 系統載入、登入及掃描商品介面

(三) 掃描商品介面：

當使用者以商家身分登入便會進入掃描商品介面，如上圖 29 右 1。此介面有以下幾種功能，分別為「取得商品資訊」、「刪除單項商品」、「刪除所有商品」及「建立交易清單」：

1. 取得商品資訊：

在掃描商品介面，手機會開啟 NFC 監聽器，若有商品之 RFID 標籤靠近手機，系統便會自動讀取商品之 RFID 標籤資訊，取得商品標籤編號後系統會自動將編號傳入資料庫做比對，如果找到以此編號為主鍵之商品，便會自動將該商品資訊回傳至手機上，並以條列式的方式記錄在此介面的 ListView 中。

2. 刪除單項商品：

如果有誤將商品加入交易清單，商家可以長按該商品，便會出現刪除商品的確認視窗，按下「是」即將該商品剔除本次交易清單中，並重新計算交易總金額；若按下「否」則取消刪除交易，如下圖 30 左 1。

3. 刪除所有商品：

如果要刪除所有商品，則可以點擊右上角，接著選「clear all」，按下 clear all 按鈕後，便會將當前所有商品資訊去除，並將總金額歸零，如下圖 30 左 2。

4. 建立交易清單：

若確認交易清單無誤後，可以點擊右下角總金額的文字，以方才的交易資訊建立交易清單，同時系統會自動呼叫 Testnet 請款的頁面，並將賣家資訊、交易總金額及建立交易清單時間並傳給請款頁面，如下圖 30 右 1。

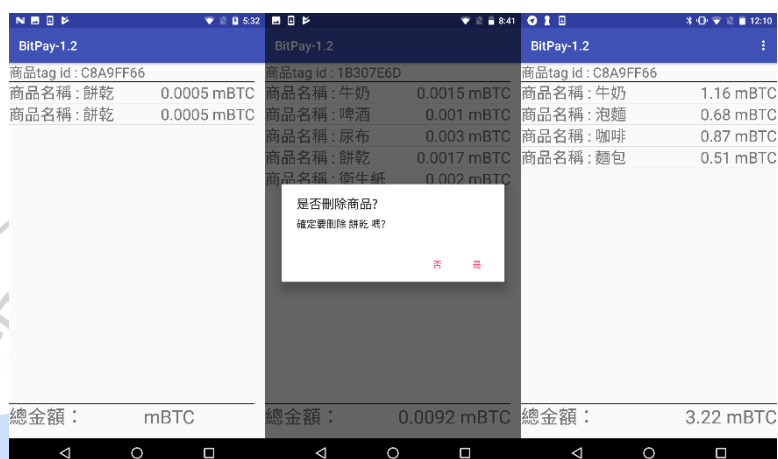


圖 30 掃描商品介面功能介紹

(四) 請款頁面：

商家進入此頁面時，會先產生一組全新的比特幣收款地址，同時接收本系統的多項參數，並將商家名稱，總金額，填入對應的欄位，商家確認交易重要資訊無誤以後，可以選擇使用 Android Beam 或是 QRcode 等等多種傳輸方式與顧客手機做連結，將重要的交易資訊傳遞給顧客端的手機，並讓顧客手機自動開啟 Testnet 的付款頁面，不論是否成功完成交易賣家可按下返回的按鈕回到本系統中。

(五) 交易清單總覽介面：

可以從賣家掃描商品資訊介面右上角的按鈕選擇 Transaction recode 進入此介面。

1. 交易金額確認視窗：

本視窗會顯示從 Testnet 回傳的交易參數提供給賣家做確認，若方才的交易失敗，或是買家取消交易，則可以按下取消按鈕，系統則會取消訂單；若方才交易成功，買家即按下確認按鈕，即可將交易資訊寫入資料庫內，並等待買家確認交易，如下圖 31 左。

2. 交易總覽視窗：

完成或取消交易後，系統會關閉交易確認視窗，並顯示交易總覽視窗，賣家可從右上角的按鈕選擇要顯示售出、購入或是同時顯示售出及購入的交易資訊，若是以賣家執行的交易，則該欄位會以紅色為底色，相反的若是以買家執行的交易，則是以綠色為該欄位的底色。如果使用者想要查看詳細的交易紀錄，可以點擊該筆交易紀錄的時間，便可轉跳至單筆交易細項介面，如下圖 31 右。



圖 31 確認與交易總覽視窗

(六) 商家單筆交易細項介面：

進入此介面，本系統會自動進入資料庫，以該筆交易時間以及使用者作為查詢主鍵，調出所有該筆交易的項目及其對應的商品價格。在此介面中會清楚列出一張交易清單應有的項目，如銷售員名稱、購買人名稱、購物細項、商品單價、交易時間及交易總金額等等資訊。若想查看該筆交易在比特幣區塊鏈上的交易情形，可以點擊右下角總金額的文字部分，則會開啟 block explorer 並查詢該次交易的收款地址之交易情形，如下圖 32 左。

(七) Block explorer：

透過本系統的單筆交易細項介面進入 Block explorer[43]，會自動查詢該筆交易的收款地址之交易總覽情形，由於此一地址為賣家請款時所新建立的地址，當地址建立完成便馬上向買家發送地址，故若交易成功並建立了交易清單，此一地址及為首次交易，我們只要查看該地址交易總覽的第一筆交易，即可將比特幣在區塊鏈上的交易紀錄與真實生活中的交易紀錄兩者之間建立起關聯，如下圖 32 右。



圖 32 交易明細與 Block expolor 介面

四. 顧客行動支付與交易理財子系統

本系統是直接擴增測試幣錢包功能，加入行動端本地資料庫，及連結系統伺服器資料庫的功能，以達到讓顧客能夠從伺服器取得交易資訊的目的，以下圖是分別為測試幣的首頁、付款以及交易一覽介面，於首頁的部分可以看到錢包餘額並查看交易狀況，但交易資訊僅有經過雜湊處理的數據，不易當作日後的交易證明，因此透過修改其原始碼，新增了交易一覽及交易明細的頁面，以保障使用者的權益，如下圖 33。

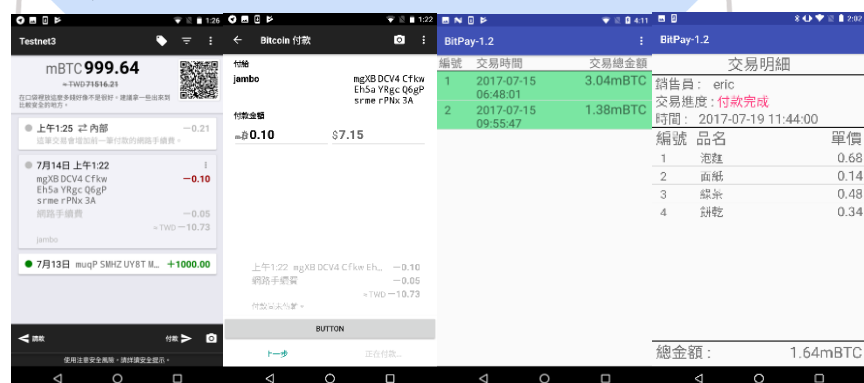


圖 33 測試幣首頁、付款、交易一覽及明細頁面

五. 系統檢測

為了要確定系統資料庫內的資訊正確，因此我們至系統資料庫內以商家收款地址做為索引，將該資訊實際到區塊鏈探索網站做查詢，以確保該筆地址實際存在，並查看區塊鏈上的交易數據是否與系統資料庫一致。

首先查看系統交易資料庫內部的資訊，橘色方框內為同一筆交易的交易細項，標號 1 的欄位為 seller_address，也就是商家用來收取比特幣的地址，標號 2 的欄位則是 TotalPrice，如下圖 34，此欄位也則是當次交易的總金額，這兩筆資訊在使用本系統建立交易清單時就會寫入資料庫，因此顧客實際依據商家所開立的交易清單付款，就可以在區塊鏈檢視器上查到對應的資料。

name	Com	price	time	seller	TotalPrice	seller_address
咖啡	9	0.87	2017-07-16 04:19:46	jambo	8.12	mjsdePvkK5J5YHCC4yt9qmgQ82Jb6Bbku
牛奶	10	1.16	2017-07-16 04:19:46	jambo	8.12	mjsdePvkK5J5YHCC4yt9qmgQ82Jb6Bbku
咖啡	1	0.87	2017-07-18 07:13:13	jambo	2.54	mqFKqEepvRoEFnRVxMUXdkf9bPZex8Q8N
麵包	2	0.51	2017-07-18 07:13:13	jambo	2.54	mqFKqEepvRoEFnRVxMUXdkf9bPZex8Q8N
牛奶	3	1.16	2017-07-18 07:13:13	jambo	2.54	mqFKqEepvRoEFnRVxMUXdkf9bPZex8Q8N
麵包	1	0.68	2017-07-18 07:48:32	eric	1.55	myoU9EqnkHuWfyPe5qde2jxpTCLGLPNJ
咖啡	2	0.87	2017-07-18 07:48:32	eric	1.55	myoU9EqnkHuWfyPe5qde2jxpTCLGLPNJ
麵包	1	0.68	2017-07-18 07:52:58	jambo	2.05	motBhTefJCyGWj3JKUkaRD5N7qkNpF
麵包	2	0.51	2017-07-18 07:52:58	jambo	2.05	motBhTefJCyGWj3JKUkaRD5N7qkNpF
咖啡	3	0.87	2017-07-18 07:52:58	jambo	2.05	motBhTefJCyGWj3JKUkaRD5N7qkNpF

圖 34 資料庫交易資訊

我們以商家收款地址實際到區塊鏈檢視網站「blockchain.info」執行搜索的動作，確實可以看到這筆交易，並獲得更多區塊鏈上的資訊，在這個網站上找到標號 1 及標號 2 分別與資料庫內部的商家收款地址及首款總金額是一致的，因此可確定資料庫內的交易資訊是實際存在在區塊鏈上的。除此之外還可以找到其他數據，包括標號 3 的 txid，則是每筆交易獨有的序號；標號 4 左邊的地址則是顧客用來付款的地址、中間是顧客用來收取找零的地址、右邊為找零的金額；標號 5 分別是該筆交易實際進入區塊被確認的時間、被收入在哪一個區塊當中以及總共被確認了幾次，區塊鏈交易的數據都詳細的在這個網站中顯示，後續我們也可以透過這些資訊達成更多分析的目的。

Summary		Inputs and Outputs	
Size	226 (bytes)	Total Input	0.2436915 BTC
Weight	904	Total Output	0.2436415 BTC
Received Time	2017-07-18 12:07:23	Fees	0.00005 BTC
Included In Blocks	1153926 (2017-07-18 12:07:23 + 0 minutes)	Fee per byte	22.124 sat/B
Confirmations	102250 Confirmations	Fee per weight unit	5.531 sat/WU
Visualize View Tree Chart		Estimated BTC Transacted	0.00206 BTC

第二節 實驗數據

本節主要詳細介紹測試幣寫入區塊鏈時間實驗，以及該實驗的目的、方法及結果，期望能夠透過本節的實驗，來佐證比特幣交易速度不會影響我們日常行動支付的流暢度。

一. 實驗目的：

實驗的目的是要確認我們的系統在商家端進行行動支付時能快速、精準且高效率的進行交易，並了解使用一般 Testnet 錢包與 Green address 錢包

作為交易媒介，的確認交易時間的差距。

二. 實驗方法：

本次的實驗分為兩部份，分別是透過 Bitcoin Testnet 錢包以及使用本論文所採用的 Green address Bitcoin Wallet 上執行 25 次付款，皆以相同地址收款，交易金額都設定為 0.00001BTC，實驗時間為 2017/09/06-17:00~17:50，每隔兩分鐘執行一次付款的動作，總共歷時 50 分鐘。兩款錢包同時發起交易，並透過區塊鏈檢視器進行記錄時間，最後再比較使用一般測試幣錢包及綠色地址錢包兩者之間的差距。

三. 實驗結果：

本次實驗分別記錄以 Testnet 錢包及綠色地址錢包執行 25 次交易的進入緩存池等待時間和寫入區塊等待時間。若以 Testnet 錢包交易，必須等到交易寫入才能保證此筆交易不會被礦工拋棄，也才算真的完成這筆交易；但若以綠色地址錢包發起交易就大不相同，當交易進入緩存池，即使遇到交易被礦工拋棄的情況，綠色地址代理節點也會重新發起此筆交易，保證讓交易寫入區塊，所以只要進入緩存池我們就可以視為交易完成，透過兩者錢包的交易數據，我們比較及分析兩種錢包交易的時間數據如下圖 34 所示。

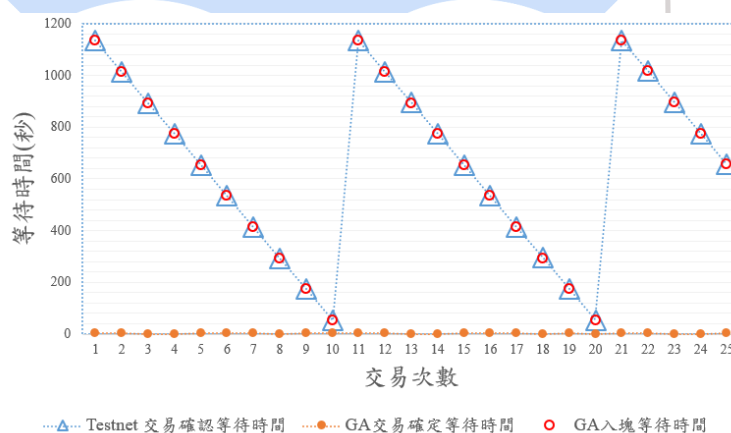


圖 34 實驗結果分析圖

透過本次的實驗，我們可以發現雖然以兩種錢包交易進入區塊的等待時間完全相同，但因為綠色地址錢包的特性，只要進入緩存池就可以算完成交易確認，因此綠色地址錢包的完成交易確認的時間遠遠快於一般 Testnet。相信比起一般使用者支付現金時可以省去掏零錢、算錢及找零等繁瑣的動作快速許多，且以此方式作為支付管道，可大大提升日常生活中的便利性與安全性。

第伍章 結論與未來工作

本章共分成兩個小節，分別講述此論文的結論以及未來工作。

第一節 結論

本論文透過探討現有的區塊鏈加密貨幣之優缺點，以及市面上常見的交易方式，得出一種可以同時適合政府、商家及顧客的交易模式，最小限度的保留去中心化的優點，並在此前提之下大幅減少逃漏稅或是黑市交易的可能，並以區塊鏈機加密貨幣為基礎，嘗試建置出一個行動支付與收銀與監督系統，以期未來加密貨幣能實際應用在日常生活的交易場景當中。

第二節 未來工作

當前本論文所提出的系統架構範圍頗為龐大，尚有部分系統功能並未完整實踐，本節描述相關的未來工作。

一. 結合理財、發票與撥款：

由於交易資訊的電子化，無論是發票或是詳細的交易資訊，都可以從手機或伺服器的資料庫取得資料，因此結合理財記帳系統相當適合，甚至可以透過智能合約，讓消費者在對中發票時自動撥款進入客戶錢包內，亦或是讓老闆在發薪水時能夠直接透過本系統，達到自動發款的目的。

二. 交易清單優化：

目前本系統建立交易清單方式尚為以掃描 RFID 標籤的方式取的商品資訊，因此應用的範圍稍嫌狹隘，因此希望加強以下兩項功能：

(一) 更多元的清單建立方式：

因此我們必須制定一種可以讓賣家可以自訂交易清單格式，以符合更多交易情境，並自訂客製化的交易清單建立方式，也同時增加本系統之獨特性與相容性。

(二) 更豐富的清單欄位：

未來交易清單上不再只有交易時間、賣家帳戶、商品資訊與價格，將新增更多資訊欄位可以供賣家選擇，包括交易地點的 GPS 數值、交易滿意度、買家回饋資訊。

三. 系統安全性即可用性的提升：

本系統功能包含金融、交易這類相當敏感的功能，因此透過系統的設計來防止不肖人士的詐騙與攻擊則是相當重要的，本系統未來要有能力對於防堵並自動偵測黑客攻擊，這項功能可說是要正式將系統推行上路最基本但也最重要的能力。

而對於雙重花費的防治，未來可以增加伺服器功能，透過本系統中的收款地址至比特幣節點查詢更多詳細交易資訊，例如顧客的付款地址、交易時間等資訊，後續更可以透過查詢所有比特幣節點，進一步分析顧客用來付款的地址是否有機會產生雙花，若有安全疑慮，系統可以立即通知店家，並扣下當前的商品，以增加商家的保障。



參考文獻

- [1]. 廖世偉(2017)。區塊鏈革命。台北：遠足文化。
- [2]. Grinberg, Reuben. "Bitcoin: An innovative alternative digital currency." (2011).
- [3]. Gilbert, Henri, and Helena Handschuh. "Security analysis of SHA-256 and sisters." Selected areas in cryptography. Springer Berlin/Heidelberg, 2004.
- [4]. Anoop, M. S. "Elliptic curve cryptography." An Implementation Guide (2007).
- [5]. Fox, Geoffrey. "Peer-to-peer networks." Computing in Science & Engineering 3.3 (2001): 75-77.
- [6]. Antonopoulos, Andreas M. Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.", 2014.
- [7]. P.W. Chen, B.S. Jiang and C. H. Wang, "Blockchain-based Payment Collection Supervision System using Pervasive Bitcoin Digital Wallet," accepted in Workshop of the 13th IEEE WiMob Conference, Oct. 9, 2017, Rome, Italy.
- [8]. Szydlo, Michael. "Merkle tree traversal in log space and time." Eurocrypt. Vol. 3027. 2004.
- [9]. Mathieu, Florian, and Ryno Mathee. "Blocktix: Decentralized Event Hosting and Ticket Distribution Network." (2017).
- [10]. Tian, Feng. "An agri-food supply chain traceability system for China based on RFID & blockchain technology." Service Systems and Service Management (ICSSSM), 2016 13th International Conference on. IEEE, 2016.
- [11]. Gervais, Arthur, et al. "Is Bitcoin a decentralized currency?" IEEE security & privacy 12.3 (2014): 54-60
- [12]. Ali, Muneeb, et al. "Blockstack: A Global Naming and Storage System Secured by Blockchains." USENIX Annual Technical Conference. 2016.
- [13]. Noether, Surae. "Review of CryptoNote white paper." http://monero.cc/downloads/whitepaper_review.pdf
- [14]. Larimer, D., N. Scott, V. Zavgorodnev, B. Johnson, J. Calfee, and M. Vandenberg (2016) 'Steem: An incentivized blockchain-based social media platform' Available at <https://steem.io/SteemWhitePaper.pdf>
- [15]. Swan, Melanie. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.", 2015
- [16]. Satoshi Nakamoto , " Bitcoin: A Peer-to-Peer Electronic Cash System" , <https://bitcoin.org/bitcoin.pdf>
- [17]. Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. "Double-spending fast payments in bitcoin." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.
- [18]. SVENSSON, JONATAN, and JOHAN ZEECK. "Proof-of-Work."
- [19]. Private key, https://en.bitcoin.it/wiki/Private_key

- [20].Wuille, P. "libsecp256k1: Optimized C library for EC operations on curve secp256k1."
- [21].List of address prefixes, https://en.bitcoin.it/wiki/List_of_address_prefixes
- [22].Base58Check encoding, https://en.bitcoin.it/wiki/Base58Check_encoding
- [23].<https://www.bnext.com.tw/article/47197/bitcoin-mining-electricity-usage>
- [24].Garzik, Jeff. "Making decentralized economic policy." (2015).
- [25].Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." *IEEE Access* 4 (2016): 2292-2303.
- [26].Buterin, Vitalik. "Ethereum white paper." (2013).
- [27].Green address Bitcoin Wallet, <https://greenaddress.it>
- [28].<https://weiwenu.net/d/101208166>
- [29].<https://zh.wikipedia.org/wiki/WannaCry>
- [30].https://whitesunset.github.io/wannacrypt_balance/
- [31].<http://www.newsbtc.com/2017/12/15/andreas-antonopoulos-warns-crypto-bubble/>
- [32].<http://blockcast.it/>
- [33].<https://www.facebook.com/datayogurt/photos/a.1658563141115647.1073741828.1656165468022081/1742359149402712/?type=3&theater> Buba, Zirra Peter, and Gregory Maksha Wajiga. "Cryptographic algorithms for secure data communication." *International Journal of Computer Science and Security (IJCSS)* 5.2 (2011): 227-243.
- [34].Buba, Zirra Peter, and Gregory Maksha Wajiga. "Cryptographic algorithms for secure data communication." *International Journal of Computer Science and Security (IJCSS)* 5.2 (2011): 227-243.
- [35].王家輝, 陳伯韋, 江柏憲, 王長勁 "數位貨幣交易之安全性提升的設計與實作-以開放源碼之比特幣錢包為例," 科技部開放軟體專案計畫系統需求規格書, MOST 1052221-E-130-006 -
- [36].<https://www.youtube.com/watch?v=Zjxr5yEenwM>
- [37].Wiki, Bitcoin. "Testnet." (2011), <https://en.bitcoin.it/wiki/Testnet>
- [38].WiKi. "Android studio", https://en.wikipedia.org/wiki/Android_Studio
- [39].Ortiz, C. Enrique. "An introduction to near-field communication and the contactless communication API." Oracle Sun Developer Network. Retrieved on Jun 30 (2008): 2010.
- [40].WiKi, "XAMPP", <https://en.wikipedia.org/wiki/XAMPP>
- [41].王家輝, 陳伯韋, 江柏憲, 王長勁 "NFCbitcoinWallet 系統測試報告" 科技部開放軟體專案計畫系統需求規格書, MOST 1052221-E-130-006 -
- [42].Andreas M Antonopoulos(2014,December) 。Mastering Bitcoin-Unlocking Digital Cryptocurrencies 。O'Reilly Media 。

- [43].Kuzuno, Hiroki, and Christian Karam. "Blockchain Explorer: An Analytical Process and Investigation Environment for Bitcoin."
- [44].<http://sayit.archive.tw/2017-02-02-bitdex-%E4%BE%86%E8%A8%AA>

