**匿名加密貨幣與實名商家交易的有效行動支付監督平台之建置與實作-以比特幣為例**

江柏憲a、陳伯韋b 、王家輝a、何建明c

銘傳大學資訊工程學系a

北京大學軟件與微電子學院b

中央研究院資訊科學所 c

{05366070@me, wangch@mail}.mcu.edu.twa

powei.chen@pku.edu.cnb

hoho@iis.sinica.edu.twc

摘要

知名加密貨幣比特幣的底層核心區塊鏈(blockchain)技術已成為了傳統中央集權金融體系在跨國轉帳眾多問題的最佳解決方案，因為比特幣是在無所不在的網際網路上運行，利用同儕網路架構的雜湊現金(Hashcash)系統，它解決了跨國時差與營業時間限制的問題。也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，可以有效解決傳統金融交易系統的冗長處理手續、過長等待時間以及高額手續費等眾多問題。而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加密貨幣。

此外，對政府而言，將貨幣電子化可以解決許多問題，包括假鈔的橫行，使得店家的收益明細透明化，在另一方面也保障著消費者購物上的權益、更可以使得稅務的監督更加的簡單、透明及方便；而電子化的交易明細，亦可簡化人工查帳比對的人力資源與減少查帳錯誤的發生機率。

本論文提出以比特幣系統為基礎的匿名加密貨幣與實名商家交易時的收銀監督系統平台上效能提升方法，也就是結合比特幣綠色地址(Green address)技術，有效縮短以區塊鏈為基礎的加密貨幣在商家行動支付時的交易可確定時間，並有效降低雙重花用(Double-spending)發生的可能性，並實際以開放原始碼的比特幣開發用之測試幣Testnet為基礎，建置與實作此行動支付監督示範平台上的各項子系統以及所提出的交易效能改善方法，初步的實驗結果也驗證了所提改善方法的有效性。

**關鍵詞**：加密貨幣、區塊鏈、雜湊現金、綠色地址、行動支付、雙重花用。

Abstract

The famous blockchain technology for Bitcoin cryptocurrency has become the best solution for many problems of transnational transfer service in centralized traditional financial systems. Because its Hashcash system with cryptography is based on the peer-to-peer network running on pervasive Internet, the problems of transnational time difference and limited office hours can be solved. Due to its decentralization and anonymity, it significantly reduces the labor cost of the transaction, lengthy handling and waiting time. Besides, we don’t need to pay a high amount of cross-border wire transfer fee.

Moreover, for the government, the digitization of money can solve many problems, including to reduce the spread of counterfeit money, make the store's earnings clear and transparent. On the other hand, it not only protects the interests of consumers' shopping, but also makes the tax supervision simpler, transparent and convenient. It can reduce not only the labor cost, but also the errors in taxation procedure

This paper proposes a cost-effective method to improve the transaction performance on a mobile payment supervision system for anonymous cryptocurrency trading with named store using Bitcoin system. That’s to say, we apply Bitcoin Green address technology to not only shorten the confirmable transaction time, but also reduce the double spending possibility. Besides, we based on the open-source Bitcoin wallet called Testnet to further deploy and implement the subsystems of this Bitcoin mobile payment collection system including the proposed method for transaction performance improvement. The preliminary experimental results from the developed platform demonstrate the effectiveness of proposed improvement method.

**Keywords**: Cryptocurrency, Blockchain, Hashcash, Green address, Mobile payment, Double-spending.

1. 前言

比特幣[1]是一種去中心化[3]的加密貨幣[4]，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[27]的儲存，會透過同儕網路技術的方式，分散儲存至所有比特幣全節點[1]的計算機中，現今的區塊鏈大小已經達到140G[5]以上，所有以比特幣為貨幣所發起的交易，將會被收入其中永久保存至區塊鏈中。據統計全世界運行比特幣系統的節點數量高達9531個[6]，大量節點的備份資料，確保了比特幣網路的穩固性，並不會因為其中一台主機的關閉，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，所以比特幣系統二十四小時不間斷的運行，相當穩定，有別於傳統的中心化的金融機構。

本論文將以比特幣的匿名加密貨幣與實名商家交易模式下建置與實作有效行動支付監督平台，並提出以比特幣綠色地址(Green address)技術來提升加密貨幣在行動支付交易效能，也就是加快交易確認時間與降低雙重花費(Double-spending)的發生機率，希望我們提出的加密貨幣行動支付監督平台能進一步創造消費者、商家與政府金融管理單位在加密貨幣交易上的三贏局面。

1. 相關技術

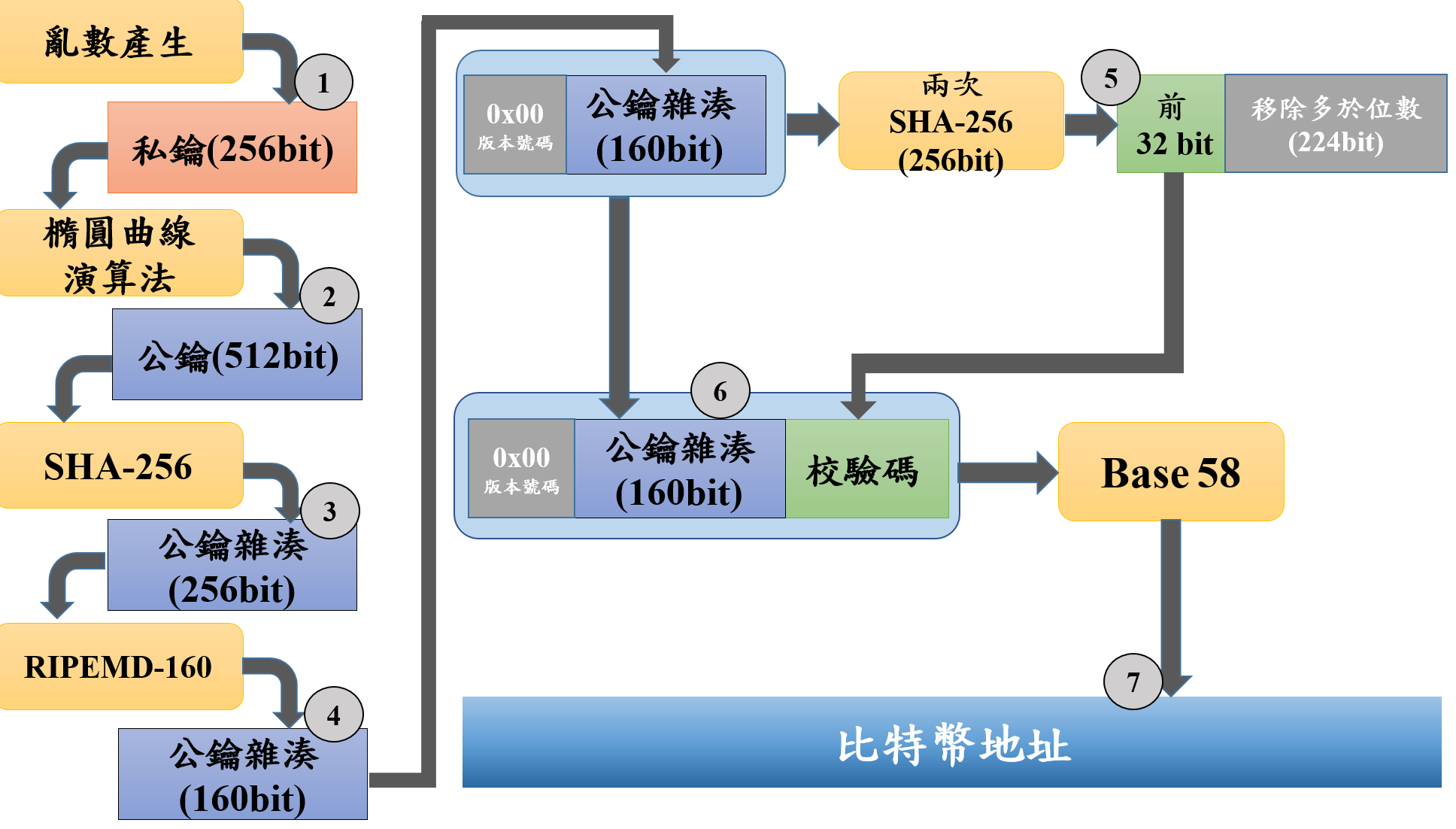
本節將就最知名的加密貨幣比特幣相關技術，包含比特幣簡介、比特幣地址的生成、區塊鏈簡介以及綠色地址的比特幣錢包做介紹。

* 1. 比特幣簡介

在Satoshi的論文[1]中提出了一個無須仰賴信任的電子交易系統。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）[7]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）[8]機制的同儕網路來記錄交易的公開歷史資訊，若誠實的節點掌控了大部分的運算能力，則攻擊者去竄改交易資訊是計算上不可行的。這個網路的穩健之處在於其結構上的簡潔性。節點與節點間使用共識演算法[1]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同儕網路架構下的電子貨幣系統所需要的規則及獎勵機制。

* 1. 比特幣地址生成

可以用來收付款的比特幣地址地生成需要遵循七個步驟，如下圖 1，才能產出在比特幣網路中合法使用的比特地址，以下將依序闡述比特幣地址創建的過程：

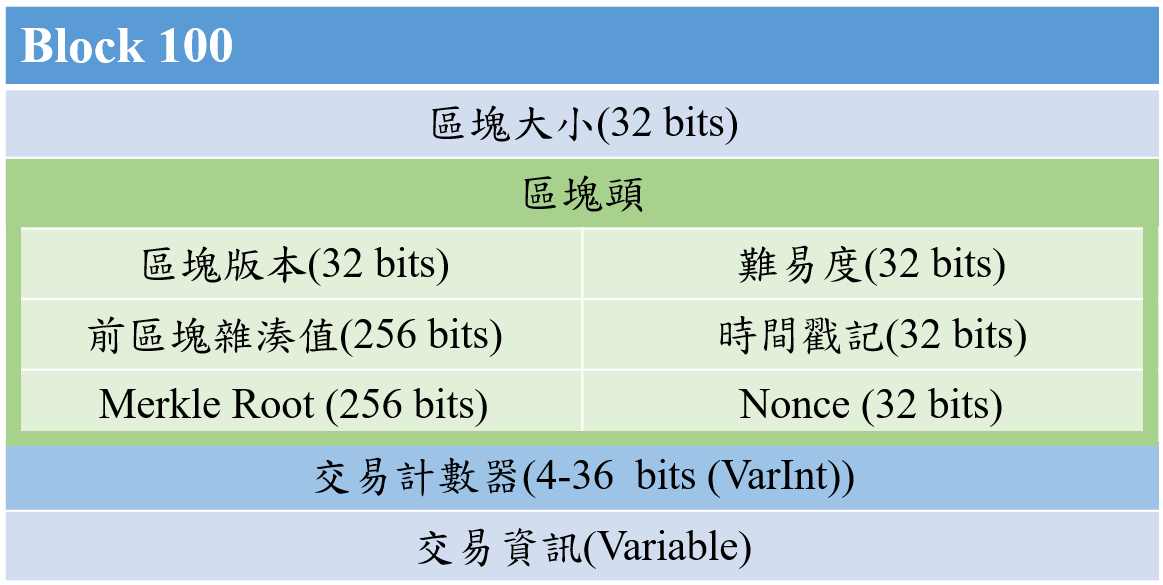


**圖 1 比特幣地址生成流程圖**

1. 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)[9]簽署花費該地址當中的比特幣。
2. Secp256k1[10]：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。
3. SHA-256[11]：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。
4. 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。
5. 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[12]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。
6. 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。
7. Base58編碼[13]：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。

* 1. 區塊鏈簡介

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、比特幣交易簽署及廣播、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。



**圖 2 比特幣區塊結構示意圖**

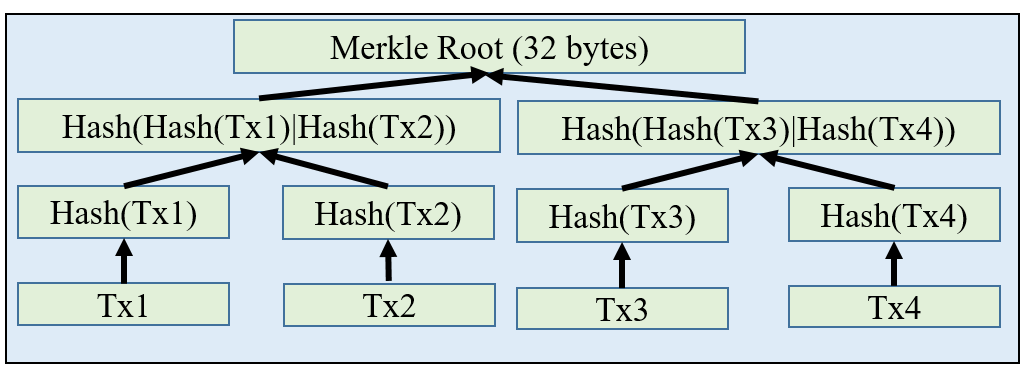
本子節主要介紹區塊鏈相關技術，我們會簡單介紹區塊鏈的結構，並概要說明區塊鏈優點及比特幣區塊鏈的缺點：

* + 1. 區塊鏈的結構

如上**圖 2**所示，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。

區塊頭包括區塊版本、前區塊雜湊值、Merkle Root、時間戳、難易度及Nonce：

1. 區塊版本（32 bits）：記錄區塊鏈系統及協定的相關版本資訊。
2. 前區塊雜湊值（256 bits）：記錄前一個區塊的雜湊值，透過該值能把所有區塊首尾相連進而形成區塊鏈。
3. Merkle Root（256 bites）[14]：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確，如下圖 3。



**圖 3 Merkle Root生成示意圖**

1. 時間戳記（32 bits）：記錄區塊生成時間，格式為年、月、日、時及秒。
2. 難易度（32 bits）：為工作量證明類演算法解的難易度目標值。
3. Nonce（32 bits）：記錄當前區塊工作量證明演算法的解。
   * 1. 區塊鏈之優點

區塊鏈具有公開透明的交易資料，所有的交易記錄皆為公開透明，所有的人都可以驗算每一筆交易記錄的正確性，資料公開透明使得交易資料可信。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，甚至是利用大數據分析分析出前所未見的觀點。

基於區塊鏈的特性，如2.3.1子節所描述，只要區塊中的一個數值遭到修改，即便是一個位元，也會使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。使得所有的交易記錄只要進了區塊鏈皆無法修改及刪除。

* + 1. 比特幣區塊鏈問題

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，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，反觀比特幣的區塊鏈尚有很大的改善空間。

區塊的生成是基於工作量證明，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困難度降低使平均生成時間為五分鐘，當中需要顧慮區塊生成時間過短，導致所有區塊鏈節點無法完成同步，發生區塊鏈分叉[20]，進而導致比特幣系統崩潰。

比特幣系統中的原生目標為儲存交易記錄，在原本的架構下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，因而目前身為全世界第二大加密貨幣的作者Vitalik提出了新一代的加密貨幣系統，並創造了Ethereum virtual machine [16]使得在Ethereum[15]中所創建出的腳本，有著同樣的虛擬機可以運行，突破了比特幣的技術上的瓶頸。

* 1. 綠色地址比特幣錢包

雙重花費問題存在於比特幣交易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。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，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，因此綠色地址技術[17]致力於在一開始創建交易的同時管控雙花交易的發生，他們採用了2-of-2多重簽章，也就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，分別為使用者與綠色地址代理節點，這筆交易的建立必須要雙方同時簽署才得以被消費。若是遇到交易塞車，且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，視同此機交易不曾存在過，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。



**圖 4 綠色地址錢包交易之流程圖**

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，如上圖 4：

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支地址，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。
4. 研究方法

說明系統開發背景、架構、流程與資料庫架構。

* 1. 系統開發背景

雖然比特幣為開源系統，但若實際使用比特幣作為開發系統之背景，系統開發成本難以估計，故本系統選擇使用比特幣綠色錢包之測試幣作為開發及測試用的工具，使其作為研究發展的基礎，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，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，並且它在市場價值極低，因此測試幣為開發本系統模型的不二之選。

資料庫方面本系統則是以XAMPP（X, Apache, MySQL, PHP, Perl）[21]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[22]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。

* 1. 系統架構

本系統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來開發本論文所提出的以比特幣為例的加密貨幣交易收款監督系統的應用服務示範平台，並嘗試改善交易效能。

本論文已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**，而各子系統分別為**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子系統**、**顧客端行動支付與交易明細子系統**

* 1. 系統運作流程

本節將詳述本系統之商家註冊、綠色地址錢包創建與驗證交易的運作流程與相關資料庫架構 。



**圖 5 商家註冊流程圖[2]**

* + 1. 商家註冊與創建與驗證交易

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交易。

1. 商家的註冊與認證流程如上**圖 5**
2. 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。
3. 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。
4. 批准：政府批准了該商家提出的申請，伺服器便會啟動此商家在本收款監督系統創建出的帳戶。
5. 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 6 利用綠色位址錢包創建與驗證交易流程圖**[2]

1. 商家及顧客創建與驗證一筆交易之流程，如上**圖 6**：
2. 商家以通過政府機構的審查稽核的帳戶登入該系統。
3. 系統載入該店家註冊的商品資訊，店員可以依照客戶的需求進行點單選取數量。
4. 快速建立交易清單，並透過Green address Testnet建立一個全新的比特幣收款地址，再以Android Beam[23]的方式將交易資訊輕鬆地傳得給顧客。
5. 在商家店員的平板電腦收到這筆交易信息之後，會對本監督系統重送一個副本進行存檔。該交易資訊包括由監督系統所提出的交易流水號、商家編號等資訊。
6. 消費者收到交易信息後，手機會自動開啟Green address的付款頁面，確認金額無誤之後便能進行支付，此時便會以客戶的比特幣私鑰簽署交易，並等待綠色地址代理節點的認證及發布。
7. 綠色地址代理節點收到交易請求，並完成驗證非雙花攻擊後，以代理節點對應地址的私鑰簽署本次交易，並廣播至比特幣節點中。
8. 區塊鏈檢視器便會開始分析網路中存在的所有在緩存池中的交易，以及已經被記錄到區塊鏈中的交易。
9. 本交易監督系統會向區塊鏈檢視器查找，檢查該筆交易是否已經存在於緩存池當中，若已經確認進入緩存池，則認定該筆交易成立並完成付款。
10. 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。
11. 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。
    * 1. 系統資料庫架構

本系統資料庫主要四個原資料庫及三個關聯資料庫，如下**圖 7**，原資料庫分別為產品資料庫、使用者資料庫、商家資料庫和交易資料庫；而關聯資料庫分別為商家­\_用戶資料庫、商家\_產品資料庫及商家\_交易資料庫：



**圖 7 系統資料庫架構**

1. **原資料庫**：

原資料庫分為使用者資料庫、產品資料庫、商家資料庫、交易資料庫等四項資料庫。

* 1. 產品資料庫：此資料庫儲存所有經過政府核准的商品資訊，儲存包括產品序號、產品名稱、價格及其他詳細資訊。
  2. 使用者資料庫：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，而使用者密碼則以雜湊的方式保存，以增加用戶安全性。
  3. 商家資料庫：本資料庫儲存關於店家的資訊，如每個店家獨立的店家編號，店家名稱、地址、GPS資訊及比特幣收款地址。
  4. 交易資料庫：當商家與顧客完成交易，便會將詳細交易資訊存入此資料庫，包括交易序號，及各項產品序號、數量及收據號碼。

1. **關聯資料庫**：
2. 商家＿用戶資料庫：本資料庫儲存各個商家擁有的職員資訊，包括各店家的商店編號、使用者編號及身分編碼。
3. 商家＿產品資料庫：此資料庫儲存各家公司當前商品存貨資訊，由商店編號、產品編號及產品庫存所組成。
4. 商家＿交易資料庫：本資料庫記錄著每一筆交易的經手人是誰，並由交易編號、店家序號，及使用者序號組成。
5. 系統成果與效能實驗

本章主要分成兩個小節，第一節主要介紹目前系統建置進度，將說明本論文的三個子系統；第二節則實際在測試鏈上測試交易速度之實驗。

* 1. 系統建置

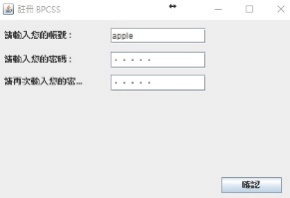
本節將逐一介紹三個子系統之功能與介面，並搭配系統截圖作為解說。

1. **商家端建置與管理商品資訊子系統**
2. 登入介面：

商家若欲登入本子系統，則必須先以商家帳戶及密碼登入系統，如下圖 8左。

1. 註冊介面：

若當前使用者尚未擁有商家帳戶，則必須先於本系統申請新的一組帳號，並在此介面中輸入之資訊，註冊通過後便能以此帳號進行登入，如下圖 8右。

****

**圖 8 商家端建置與管理商品資訊子系統註冊介面**

1. 系統主介面：

當使用者以商家帳號登入後便會進入此介面，會顯示剛商家擁有的商品詳細資訊，如品名稱、價格、數量等資訊，並可於此介面管理各項商品清單，對商品執行新增、修改及刪除等動作，如下圖 9。



**圖 9 商家端建置與管理商品資訊子系統管理介面**

1. **商家端行動收銀與交易明細子系統**
2. 系統載入介面：

進入本系統Bitcoin圖示將以淡入的方式顯示，與此同時亦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登入介面。

1. 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，若驗證成功則可以進入下一個介面，如下**圖 10**左1。

1. 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，如下**圖 10**，將可執行以下幾種功能，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：若有商品之RFID標籤靠近手機，系統便會自動透過資料庫取得該商品資訊。
2. 刪除單項商品：如要將商品移出清單，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。
3. 刪除所有商品：如果要刪除所有商品，則可以點擊右上角選單，接著選擇「clear all」，將當前所有商品資訊去除，並將總金額歸零。
4. 建立交易清單：若確認交易清單無誤後，可以點擊右下角金額即可建立交易清單，同時系統會自動呼叫Testnet請款的頁面。



**圖 10 登入與掃描商品介面**

1. 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，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的付款頁面執行付款動作。



**圖 11 系統交易明細介面**

1. 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交易紀錄進入，如上**圖 11**。

* 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。
  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。

1. 商家單筆交易細項介面：

在此介面中會清楚列出一張交易清單應有的項目。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，則會開啟區塊鏈檢視器並查詢該次交易的收款地址之交易情形。

1. 區塊鏈檢視器：

透過本系統的單筆交易細項介面進入區塊鏈檢視器（Blockchain explorer）[18]，會自動查詢該筆交易的收款地址之交易總覽情形。

* 1. 交易效能實驗

本節主要介紹一般測試幣與綠色錢包測試幣進行交易的效能實驗與結果分析，包含該實驗的目的、方法及結果分析。

* + 1. 實驗目的

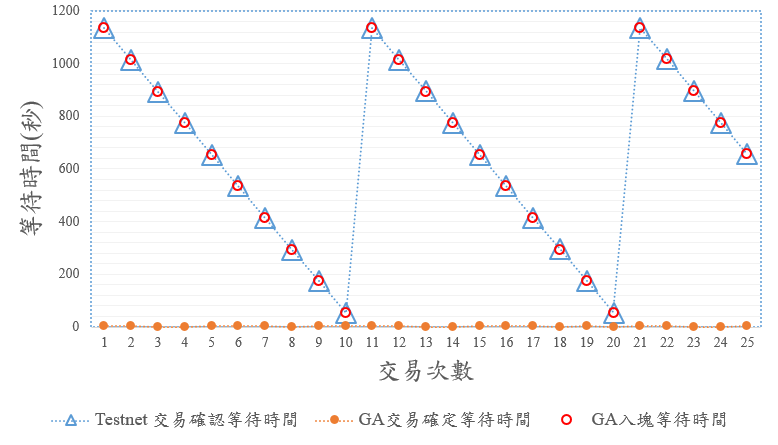
實驗的目的是要確認我們的系統在商家端進行行動支付時能快速、精準且高效率的進行交易，並了解使用一般Testnet錢包與Green address錢包作為交易媒介的確認交易時間的差距。

* + 1. 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。

* + 1. 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就如下圖 12所示。



**圖 12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，相信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。

1. 結論及未來工作

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：

* 1. 更多元的清單建立方式：

未來預期可以讓商家以更多元的方式建立交易清單，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。

* 1. 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。

此外，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，以期未來加密貨幣不僅能維持目前的便利性，更能夠能避免不肖人士利用加密貨幣洗錢，還可以讓使用者不用擔心交易後找不到賣家，使一般民眾能更安心使用加密貨幣作為日常生活的行動支付管道。

**參考文獻**

1. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.
2. 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.
3. Gervais, Arthur, et al. "Is Bitcoin a decentralized currency?." IEEE security & privacy 12.3 (2014): 54-60.
4. Narayanan, Arvind, et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.
5. Blockchain Size, <https://blockchain.info/charts/blocks-size>
6. Global Bitcoin Nodes Distribution, <https://bitnodes.21.co/>
7. Krsul, Ivan V., J. Craig Mudge, and Alan J. Demers. "Method of electronic payments that prevents double-spending." U.S. Patent No. 5,839,119. 17 Nov. 1998.
8. Proof of work, <https://en.bitcoin.it/wiki/Proof_of_work>
9. Private key, <https://en.bitcoin.it/wiki/Private_key>
10. Wuille, P. "libsecp256k1: Optimized C library for EC operations on curve secp256k1."
11. Gilbert, Henri, and Helena Handschuh. "Security analysis of SHA-256 and sisters." International workshop on selected areas in cryptography. Springer, Berlin, Heidelberg, 2003.
12. List of address prefixes, <https://en.bitcoin.it/wiki/List_of_address_prefixes>
13. Base58Check encoding, <https://en.bitcoin.it/wiki/Base58Check_encoding>
14. Szydlo, Michael. "Merkle tree traversal in log space and time." Eurocrypt. Vol. 3027. 2004.
15. Buterin, Vitalik. "Ethereum white paper." (2013).
16. Ethereum Virtual Machine, <https://github.com/pirapira/awesome-ethereum-virtual-machine>
17. Green address Bitcoin Wallet, https://greenaddress.it
18. Kuzuno, Hiroki, and Christian Karam. "Blockchain Explorer: An Analytical Process and Investigation Environment for Bitcoin."
19. Bitcoin Improvement Proposals, <https://github.com/bitcoin/bips>
20. Garzik, Jeff. "Making decentralized economic policy." (2015).
21. Friends, Apache. "XAMPP Apache+ MySQL+ PHP+ Perl." Apache Friends (2014).
22. Bartholomew, Daniel. "MariaDB vs. MySQL." Dostopano 7.10 (2012): 2014.
23. McHugh, Sheli, and Kristen Yarmey. "Near field communication: Introduction and implications." Journal of Web Librarianship 6.3 (2012): 186-207.
24. Finkenzeller, Klaus. RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. John Wiley & Sons, 2010.
25. Zapata, Belén Cruz. Android studio application development. Packt Publishing Ltd, 2013.
26. Want, Roy. "Near field communication." IEEE Pervasive Computing 10.3 (2011): 4-7.
27. 高靖鈞, 丁川偉, 陳耀鑫, 馬金溝, & 陳澤世. (2017). 區塊鏈簡介與技術探討. 電腦與通訊, (169), b1-10.