# 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.tw[a]
powei.chen@pku.edu.cn[b]
hoho@iis.sinica.edu.tw[c]

## 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，分散儲存至所有運行比特幣全節點[1]的計算機中，現今的區塊鏈大小已經達到140G[5]以上，資料內容為自2009年來的所有以比特幣為貨幣所發起的交易，將會被收入其中永久被保存至區塊鏈中。全世界運行比特幣系統的計算機，據網路節點統計高達9531個節點[6]，這意味著區塊鏈的資料已經被複製了9531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。

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，並沒有足夠的授權才可調閱交易資料，這些交易記錄既不公開，也只能依賴這唯一的信任，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

確保消費者的消費記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。

基於上述以區塊鏈技術為主的加密貨幣在金融交易上的優勢，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。

## 2. 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(Green address Bitcoin Wallet)做介紹。

### 2.1 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。

### 2.2 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，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：

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。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。

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。

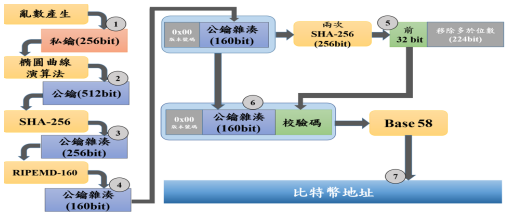


**圖 1 比特幣地址生成流程圖**

### 2.3 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。

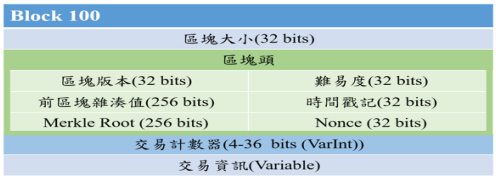


**圖 2 比特幣區塊結構示意圖**

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：

### 2.3.1 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。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，會使的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。
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。

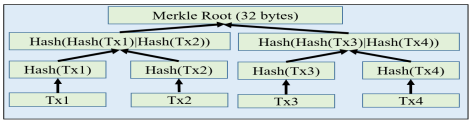


**圖 3 Merkle Root 生成示意圖**

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

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）至今所有的交易記錄，其交易形式被允許為多對一、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，也就是礦工創建的區塊所得到的獎勵）。除了加密貨幣外，亦有其他功能的區塊鏈、票券區塊鏈以及食安區塊鏈正在研發測試。

### 2.3.2 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。

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。尤其是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攻擊者執行資料加密，進行綁架勒索。這樣的攻擊手法，對去中心化的區塊鏈交易系統不會構成太大的威脅，畢竟在比特幣網路中有眾多的區塊鏈節點，並不會因為一個節點的損毀而導致太大的影響。

此外，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，也就存在著「匿名性」。在現實生活的實例中，可以有效的保護消費者的個人隱私。

還有，在區塊鏈系統中，依靠著演算法維持系統的運作，包括共識演算法。換言之，在這樣的自治的系統中，沒有一個節點可以直接決定系統運作的規則，而如果遇到系統有嚴重的錯誤或是有需要改善升級的地方，可以藉由 BIP(Bitcoin Improvement Proposals)[19]的方式進行升級。這樣的計畫的提出，需要在比特幣系統中部份運算能力的支持，才得以運行。也就是因為這樣的民主的機制，區塊鏈系統雖然較無法快速做出重大的變異，但系統因此也相對的穩定許多。

### 2.3.3 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，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。

而且，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。

## 2.4 綠色地址比特幣錢包

雙重花費(Double-spending, 簡稱雙花)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，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，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[17]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。

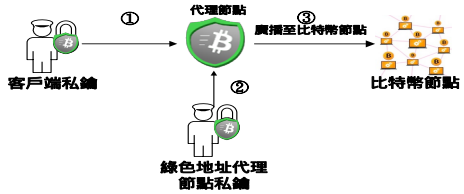


**圖 4 綠色地址錢包交易之流程圖**

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。

# 3. 研究方法

說明系統開發背景、架構、流程與資料庫架構。

## 3.1 系統開發背景

雖然比特幣為開源系統，但由於現今比特幣價格不斐，截自2017/9/3，一顆比特幣兌換美金的均價約為4689.46美元，倘若實際利用比特幣作為測試本開發系統，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，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實際比特幣系統相同，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。

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大的 Android 開發編譯器「Android Studio[25]」作為行動應用開發環境。

另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 兩部手機作為搭載本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）[26]功能，為本系統所需之模擬加密貨幣與商家交易的重要功能。

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。

為了商家能夠輕鬆的查詢、新增、修改及刪除商品資訊。因此我們使用 Eclipse 工具開發電腦版的商品管理 Java 應用程式。

## 3.2 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：

1. **商家端建置與管理商品資訊子系統**：

本子系統可以讓商家在進貨時，快速地將RFID[24] 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。

2. **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，可以減少結帳的速度，使結帳效率大幅提升。

3. **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記錄儲存於客戶端，以便日後顧客快速取得過往的交易記錄。除此之外，亦可讓廣大的民眾體驗加密貨幣與行動支付帶來的便利生活。

## 3.3 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 。

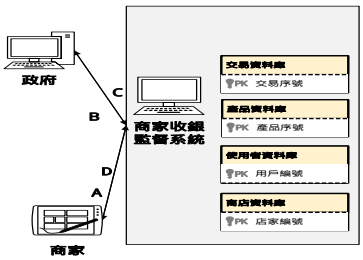


**圖 5 商家註冊流程圖**[2]

### 3.3.1 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。

I. 商家的註冊與認證流程如上**圖 5**

A. 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。

B. 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。

C. 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。

D. 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。

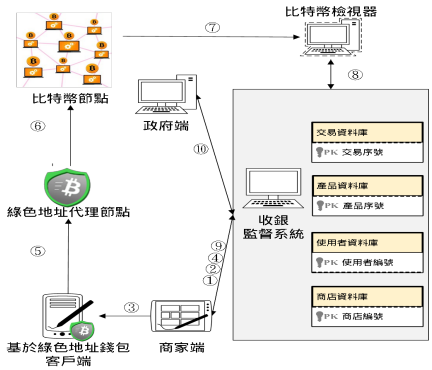


**圖 6 利用綠色位址錢包創建與驗證交易流程圖**[2]

II. 商家及顧客創建與驗證一筆交易之流程，如上**圖 6**：

1. 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。
2. 登入本加密貨幣的商家收銀金流監督系統後，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。
3. 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 Green address Testnet 的請款頁面建立一個全新的比特幣收款地址，再以 Android Beam[23]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。
4. 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、商品編號、商品購買數量以及加密貨幣的收款地址，以及消費者的發款地址。
5. 消費者收到交易信息後，手機會自動開啟 Green address 的付款頁面，確認金額與店家無誤之後便能以匿名的加密貨幣比特幣進行支付，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。
6. 綠色地址代理節點收到客戶的交易請求，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。
7. 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中的交易，以及已經被記錄到區塊鏈中的交易。
8. 本交易監督系統會向區塊鏈檢視器會基於第四步所儲存的交易副本中的加密貨幣收款地址以及預付款的加密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。
9. 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。
10. 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。

### 3.3.2 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：

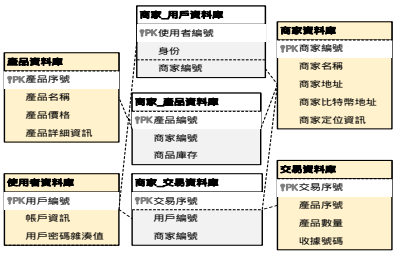


**圖 7 系統資料庫架構**

A. **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。

i. 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。

ii. 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。

iii. 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。

iv. 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。

B. **關聯資料庫**：

i. 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。

ii. 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。

iii. 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。

## 4. 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，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。

### 4.1 系統建置

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。

**1. 商家端建置與管理商品資訊子系統**

A. 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，登入之後系統會讀取資料庫，確認該組帳戶底下擁有那些商品資訊，讀取完畢後即可執行後續相關的管理功能，如下圖 8。

B. 註冊介面：

若當前使用者尚未擁有商家帳戶，則必須先以商家端建置與管理商品資訊子系統之註冊功能申請新的一組帳號，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。


**圖 8 商家端建置與管理商品資訊子系統註冊介面**

C. 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**

**2. 商家端行動收銀與交易明細子系統**

A. 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，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。

B. 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，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分，如果是以商家登入則會進入掃描商品資訊的介面；如果是以顧客登入，則會轉跳至個人交易清單總覽介面，如下**圖 10**左1。

C. 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**。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」：

i. 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。

ii. 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。

iii. 刪除所有商品：如果要刪除所有商品，則可以點擊右上角，接著選擇「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。

iv. 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。

**圖 10 登入與掃描商品介面**

D. 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。

**圖 11 系統交易明細介面**

E. 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 record 進入，或是以買家模式登入，亦或是賣家交易完成後皆可進入此介面，如上**圖 11**。

i. 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。

ii. 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記錄，可以點擊該筆交易記錄的時間，便可轉跳至單筆交易細項介面。

F. 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，則會開啟區塊鏈檢視器並查詢該次交易的收款地址之交易情形。

G. 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，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記錄與真實生活中的交易記錄兩者之間建立起關聯。

**3. 顧客端行動支付與交易明細子系統**

A. 登入介面：

使用者進入系統後可選擇以顧客登入，若以顧客身分登入登入則可進入顧客交易清單總覽介面。

B. 顧客交易清單總覽介面：

此介面會顯示出該位顧客所有的交易總覽資料，如果使用者想要查看詳細的交易記錄，可以點擊該筆交易記錄的時間，便可轉跳至單筆交易細項介面。

C. 顧客交易清單總覽介面：

在此介面介面中會清楚列出與商家該筆交易的交易明細，整體與商家交易細項一致，唯一不同的點會以紅字標記顧客姓名，以確保交易雙方資訊無誤。

D. 付款頁面：

買家接收到賣家所傳送的資訊後，會自動開啟 Testnet 的付款頁面，並自動將付款金額、付款對象及付款地址填入對應的欄位，賣家只需按下付款的按鈕，便會從錢包中轉出所需的交易總金額，同時此介面會出現確認交易的按鈕，按下去以後便會將資料庫內的交易確認欄位更改為代表確認的參數，並完成一次的交易流程。

## 4.2 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。

### 4.2.1 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。

### 4.2.2 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。

### 4.2.3 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。

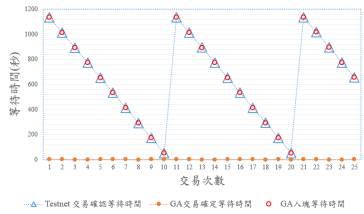


**圖 12 實驗結果分析圖**

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。

## 5. 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。
2. 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.