



北京大学

硕士研究生学位论文

题目： 区块链的实名交易实时监督系统的
设计与实现

姓 名： _____

学 号： _____ 1601210903

院 系： _____

专 业： _____

研究方向： _____

导 师： _____

二〇一八年一月

版权声明

任何收存和保管本论文各种版本的单位和个人，未经本论文作者同意，不得将本论文转借他人，亦不得随意复制、抄录、拍照或以任何方式传播。否则一旦引起有碍作者著作权之问题，将可能承担法律责任。

摘要

比特幣是一個集成網絡學、密碼學、貨幣銀行學的加密貨幣，加密貨幣市場中，有數以千計的貨幣種類在市場流動著。值得一提的是，至今比特幣的點對點式電子現金系統還未出現過錯誤。比特幣最大的特色在於去中心化與匿名化，以去中心化的基礎建構出一個其他人無法管控的點對點金流，但也因為其匿名之特性，存在著三項問題，分別為無法追蹤、無法得到稅收以及在交易的過程中無法保障消費者權益。第一，在比特幣系統中，沒有任何一個使用者可以要求每一個人落實實名制，政府主管機關與相關人士難以追查每一筆資金的真正持有者，進而增加洗錢防制的困難性。第二，稅收更是國家經濟基礎運作的資金來源，現今的國家並無支持以比特幣交易相關的收銀系統或是制定出相關的稅務標準，使得政府無法從加密貨幣這方面的金融交易獲得稅收。第三，現有的比特幣交易模型皆為匿名與匿名之間的交易，並無開立收據，無法保障消費者權益。

本論文設計與實現一個区块链匿名加密貨幣為主的實名交易監督系統，論文工作包括五項。第一，交易模型分析：分析五種交易模型，發現匿名支付給實名交易，達到保障消費者權益、保護消費者隱私以及使政府可以課徵稅收。第二，系統設計：以匿名支付給實名交易為基礎設計支持加密貨幣的系統架構。第三，系統實現：使用 Java 編程語言，實現主要系統、商店和商品信息管理子系統、移動裝置收款及交易子系統以及客戶端移動支付和交易子系統。第四，系統優化：解決區塊鏈速度緩慢，引入多重簽章算法構建實時監督系統。第五，功能與性能測試：實現系統後，對本系統進行功能測試，且對原始監督系統與實時監督系統進行性能測試與分析。

本論文貢獻如下：

1. 引入匿名支付給實名的交易模型至加密貨幣系統。
2. 設計與實現於加密貨幣中匿名支付給實名的交易監督系統。
3. 導入多重簽章算法，設計與實現實時的交易監督系統，提升交易速度。
4. 實現於加密貨幣中，消費者匿名同時也讓消費者擁有消費者權益。
5. 藉由將商家實名，使政府主管機關可以獲得稅收的有效加密貨幣交易監督模型。

关键词：比特币，区块链，多重签章

Design and Realization of blockchain real-name transaction monitoring system

Chen Po Wei (Data Mining and Business Intelligence)

Directed by Prof. Lijie

ABSTRACT

Financial technology is booming Today, the blockchain technology is also a key development project. The most famous blockchain technology is nothing more than an article by Bitcoin by Satoshi Nakamoto in 2009: A Peer-to-Peer E-Cash System Paper. He laid the foundation for blockchain technology. Bitcoin is a cryptocurrency that integrates network science, cryptography, and currency banking. In the cryptocurrency market, there are thousands of cryptocurrencies flowing in markets. It is worth mentioning that, since Bitcoin point to point electronic cash system has not experienced an error.

The biggest feature of Bitcoin is decentralization and anonymization. Bitcoin is based on a paradigm shift to create point-to-point traffic that no one can control. However, because of its anonymity, it is difficult for the relevant government officials to trace the true holder of each sum of money. In the traditional central bank transnational transfer needs basic real-name verification. Real-name system can effectively filter out the occurrence of money laundering. But in Bitcoin's point-to-point e-cash system, no single user can ask everyone to implement a real-name system. Thereby increasing the difficulty of money-laundering prevention and control. Apart from the hard-to-trace characteristics, taxation is the source of funding for the operation of the government. Present-day countries do not support bitcoin-related cashier systems or set out the tax standards. Making the government unable to get the tax in this area.

Again by the above cannot manage the flow of funds, cannot be tracked, cannot get tax three starting point. This thesis is devoted to designing a "blockchain real-name transaction monitoring system". Before designing the system, several trading models were also explored. Found that there are cash payments to pay anonymous, anonymous payment to real-name model, in the credit card payment has a real name payment to the real name, real name paid to anonymous and then paid to the real name, the above four models. Through the analysis of the above model can be learned. The rise of the awareness of personal privacy,

only paid by the anonymous real name, we can do without revealing consumer information, consumer protection can also be done to protect rights and interests. In peer-to-peer electronic cash, it still stays in the anonymous mode of payment anonymously. This essay aims to design a supervisory cashier system for anonymous real-name cryptocurrencies. To practice the consumer anonymity, but also allow consumers to have the rights and interests of the transaction model.

KEYWORDS: Bitcoin, Blockchain, Multiple signatures

目录

| | |
|---------------------------------------|-----------|
| 第一章 绪论 | 1 |
| 1.1 選題背景 | 1 |
| 1.2 研究目標與內容 | 8 |
| 1.3 論文組織結構 | 10 |
| 第二章 相關理論與技術 | 11 |
| 2.1 比特幣 (Bitcoin) | 11 |
| 2.2 比特幣地址 (Bitcoin Address) | 11 |
| 2.3 區塊鏈 (Blockchain) | 22 |
| 2.4 點對點網絡與加密貨幣安全 | 24 |
| 第三章 系統需求分析 | 27 |
| 3.1 交易模型分析 | 27 |
| 3.2 特性要因分析 | 30 |
| 第四章 系统设计 | 33 |
| 4.1 区块链的实名交易监督系统设计 | 33 |
| 4.2 以多重签章优化区块链的实名交易监督系统之设计 | 39 |
| 第五章 系統實現 | 43 |
| 第六章 系统测试 | 47 |
| 6.1 功能测试 | 47 |
| 6.2 性能测试 | 53 |
| 第七章 总结与展望 | 59 |
| 参考文献 | 61 |
| 致谢 | 65 |
| 北京大学学位论文原创性声明和使用授权说明 | 67 |

图目录

| | |
|--|----|
| 图 1.1 2017 加密貨幣總市值走勢圖 ^[10] | 2 |
| 图 1.2 加密貨幣歷年最高總市值折線圖 ^[10] | 3 |
| 图 1.3 Bitcoin、Western Union ^[16] 、PayPal ^[17] 以及 VISA 每秒支持交易量比較圖 ^[18] | 5 |
| 图 1.4 比特幣區塊鏈成長走勢圖 ^[19] | 6 |
| 图 1.5 Darklaunder 洗錢模型 ^[25] | 7 |
| 图 2.1 LBC 競擧比特幣私鑰算力狀態圖 ^[33] | 12 |
| 图 2.2 ECC 與 RSA 的密鑰對生成時間比較圖 ^[47] | 14 |
| 图 2.3 算法 BLISS、RSA、ECDSA 安全級數比較圖 ^[48] | 14 |
| 图 2.4 區塊疊加示意圖 | 16 |
| 图 2.5 比特幣地址生成流程圖 | 19 |
| 图 2.6 Green Address 錢包生成流程圖 | 21 |
| 图 2.7 Green Address 交易發起流程圖 | 22 |
| 图 2.8 比特幣區塊鏈結構圖 | 23 |
| 图 2.9 Merkle Tree 示意圖 | 24 |
| 图 2.10 比特幣全節點分佈圖 ^[53] | 25 |
| 图 3.1 各種交易模型示意圖 | 27 |
| 图 3.2 匿名對匿名交易示意圖 | 28 |
| 图 3.3 匿名對實名交易示意圖 | 28 |
| 图 3.4 實名對實名交易示意圖 | 29 |
| 图 3.5 實名對實名再對實名交易示意圖 | 29 |
| 图 3.6 實名對匿名再對實名交易示意圖 | 29 |
| 图 3.7 魚骨圖 (1) | 31 |
| 图 4.1 BRTMS 数据库分布图 | 34 |
| 图 4.2 BRTMS 和商家注册流程的核心架构图 | 37 |
| 图 4.3 BRTMS 的整体架构与功能示意图 | 38 |
| 图 4.4 多重签章优化后的 BRTMS 整体示意图 | 40 |

| | |
|--|----|
| 图 5.1 SMIMSS 的 Java 應用程序的註冊和登錄界面 | 43 |
| 图 5.2 在 SMIMSS 中插入或更新授權商家的產品目錄 | 43 |
| 图 5.3 登錄、等待結帳的商品、刪除商品及支付確認 | 44 |
| 图 5.4 在 CMPTSS App 中，交易確認，付款確認、交易歷史記錄和發票 | 45 |
| 图 6.1 集成子系統測試 | 49 |
| 图 6.2 BRTMS 用戶用例圖 | 49 |
| 图 6.3 驗收測試（Acceptance Testing） | 50 |
| 图 6.4 使用區塊鏈瀏覽器驗證儲存在比特幣區塊鏈中的交易過程 | 56 |

表目录

| | |
|--|----|
| 表 1.1 各國政府對比特幣態度統整表 | 9 |
| 表 2.1 比特幣簡介 | 11 |
| 表 2.2 MD5、SHA-0、SHA-1、SHA-2 和 SHA-3 比較表 | 17 |
| 表 2.3 Base58 編碼表 | 18 |
| 表 2.4 Base64 編碼表 | 18 |
| 表 3.1 交易關係比較表 | 30 |
| 表 4.1 商家信息表 | 35 |
| 表 4.2 产品信息表 | 35 |
| 表 4.3 交易信息表 | 35 |
| 表 4.4 用户信息表 | 36 |
| 表 4.5 职工信息表 | 36 |
| 表 4.6 商家产品信息表 | 36 |
| 表 6.1 小米 3 手机规格 | 48 |
| 表 6.2 Google Nexus 5X 手机规格 | 48 |
| 表 6.3 IT1 测试用例 | 50 |
| 表 6.4 IT2 测试用例 | 51 |
| 表 6.5 IT3 测试用例 | 51 |
| 表 6.6 AT1 测试用例 | 52 |
| 表 6.7 AT2 测试用例 | 52 |
| 表 6.8 AT3 测试用例 | 53 |
| 表 6.9 集成子系统测试结果 | 54 |
| 表 6.10 验收测试结果 | 54 |
| 表 6.11 子系统与测试用例关系表 | 55 |
| 表 6.12 需求与集成测试用例的关系表 | 55 |
| 表 6.13 需求与验收测试案例的关系表 | 55 |
| 表 6.14 第一次以 Testnet 运行实验之数据分析 (2017/09/06) | 57 |
| 表 6.15 初步的 Green Address 实验测试数据 (2017/07/25) | 57 |

| | |
|---|----|
| 表 6.16 第一次以 GreenAddress 运行实验之数据分析 (2017/09/06) | 58 |
| 表 6.17 第二次以 GreenAddress 运行实验之数据分析 (2018/02/06) | 58 |

第一章 緒論

現金法定貨幣，收據及交易數據庫存在著一些缺點。如現金很難杜絕假鈔的橫行，收據有著偽造的可能，在交易數據庫中信息不一致，數據庫被 DDOS 攻擊，交易數據被竄改，數據庫損毀，都是在傳統交易過程中曾出現過的窘境。

於 2009 年加密貨幣 - 比特幣的問世，以密碼學、網絡學與貨幣銀行學為基礎創建了新一代的網絡貨幣。各式網絡貨幣中又以比特幣最為廣泛使用，其防堵被竄改、公開交易數據檢視、使用者具匿名性、自動運作不須人為運營等等多項特性深受現今使用者喜愛。至今區塊鏈技術已成為 IBM、摩根大通、微軟、谷歌與英特爾等重點開發項目，被視為改善銀行運作效率、降低運營成本、提升信息安全、建立公開數據的最佳方法。為解決現金、收益及交易數據庫存在之問題，本文採用以區塊鏈為基礎的加密貨幣比特幣為基礎，進行商業化收銀系統開發。不僅是基於比特幣算法穩定、交易公開透明、不可被竄改等特性，同時本論文更加入監督標籤，促使在匿名交易轉為部分實名交易之過程中，監管部門能有更好的新興貨幣技術的提升，亦可建立自動化的稅務審查機制，大幅降低人事成本，進而實現提升交易系統信息之可靠度與其穩定性。

1.1 選題背景

追溯著加密貨幣市場的演進，於 2009 年時，比特幣並非第一個加密貨幣，在比特幣之前已經有著很多類似的加密貨幣開發實驗，但是一直無法做出一個穩定點對點式的電子現金系統，關於其製作瓶頸之部分將於後段章節闡述。在比特幣穩定發展之後，有著許多對比特幣有興趣的研究者，以穩定的比特幣系統為基礎修改了許多基本的協議。於 2011 年相繼創造出了貨幣，將其稱之為山寨幣。山寨幣早期較為著名包括有萊特幣 (LiteCoin, LTC)^[1]、狗幣 (DogeCoin, DOGE)^[2]、域名幣 (NameCoin, NMC)^[3]，於 2014 年也有人認為比特幣挖礦使用到了大量的哈希運算，這樣的大量運算也浪費了許多的社會資源，進而開發出較具意義的工作量證明挖礦算法，其中較為著名的如素數幣 (Primecoin, XPM)^[4]。於 2015 年底也誕生了現在最為著名的以太坊經典 (Ethereum Classic, ETC)^[5]、以太坊 (Ethereum, ETH)^[6]，以太坊最重大突破設計在於將編程語言虛擬機移植到了區塊鏈架構上，這使得區塊鏈技術不再僅止於點對點的電子現金系統，也創造出了屬於以太坊的編程語言 Solidity^[7]，使以太坊在虛擬機 (Ethereum Virtual Machine, EVM)^[8] 中可以使用 Solidity 創建智能合約，合約可以建構去中心化的應用程序，如去中心化的交易所，將交易所去中心化可以有效的防治 DDOS 攻擊^[9]，降低交

交易所因為黑客攻擊而倒閉的可能性。

1.1.1 加密貨幣市場

加密貨幣中最具代表性的是比特幣，但除了比特幣之外也存在許多模仿比特幣的加密貨幣，有的是為其利益，有的是鑒於比特幣的各種不足，進而希望藉由其他貨幣改善比特幣不夠完美之處。加密貨幣市場中有成千上萬種的加密貨幣，其中較廣為人知的加密貨幣會在 Cryptocurrency Market Capitalizations^[10] 的排行榜中出現，截至 2018 年 2 月 8 日該排行榜已經收入了 1510 種加密貨幣。在 Cryptocurrency Market Capitalizations 統計的數據當中，可知整體的加密貨幣市場，如圖 1.1 所示，於 2018 年 1 月 7 日創下了歷史新高，加密貨幣市場的總市值也高達了 829,579,000,000 美金，相當於五兆人民幣的總市值。



图 1.1 2017 加密貨幣總市值走勢圖^[10]

經由 Cryptocurrency Market Capitalizations 數據顯示，整體加密貨幣市場自 2013 年起已經高達 150 億美金，2014 年與 2015 年間總市值減少到近乎 2013 年的一半。針對比特幣的價格波動，論文 "Have the security flaws surrounding Bitcoin effected the currency's value?."^[11] 作出詳盡的市場調研，致力於探討在各個比特幣市場大事件中對比特幣價格的波動影響，針對影響的程度該論文給出影響指數，當中影響最為嚴重的是於 2014 年 2 月發生的日本交易所 Mt.Gox 倒閉事件，因為早期的加密貨幣市場中無完善的法律規範，各國對加密貨幣的接受度有所不同，日本對金融科技的接受度相較於較為開放的情況下成立了全世界第一家比特幣交易所 Mt.Gox，也因為交易所不夠普及，使得大部分的加密貨幣交易都集中在 Mt.Gox 交易所中，使 Mt.Gox 倒閉事件成為震盪市場價格重大因子之一，也造成 2014 與 2015 年的加密貨幣市場低迷。而在 2017 年，比特幣又以 2016 年總市值之 35 倍的姿態攀上新高點，主要是因為美國最大的期權交易中心芝

加哥期權交易所於 2017 年 12 月 10 日支宣布支持比特幣期貨交易，此舉將比特幣價格推升到 20,000 美金的歷史新高，圖 1.2 為 2013 年至 2018 年歷年的加密貨幣總市值的統計圖表。



图 1.2 加密貨幣歷年最高總市值折線圖^[10]

1.1.2 加密貨幣的優勢

於 2009 年 Satoshi Nakamoto 發布了比特幣系統，成為全世界第一個加密貨幣的雛形。其透明的交易信息、區塊鏈交易數據無法修改和刪除、匿名與自治系統等特性，促使區塊鏈技術衝破現存傳統中心化之金融機構技術上的藩籬。以下將逐一說明加密貨幣的七項優點，分別為區塊鏈結算系統不間斷的運行、遠距離支付、貨幣為使用者持有、開放和透明的交易信息、區塊鏈交易數據無法修改和刪除、交易匿名性以及自治性系統。

第一，區塊鏈結算系統不間斷的運行。基於區塊鏈技術與點對點網絡的架構，以比特幣為例，自 2009 年至今，所有的比特幣交易事件皆會存儲在比特幣區塊鏈當中，區塊鏈既無法刪除也無法修改，比特幣區塊鏈會以點對點網絡的方式存儲在比特幣網絡中的全節點^[12]，目前比特幣網絡中的全節點高達 10552 個。與傳統中心化的銀行數據庫相比，可能會因為銀行的服務器維護，導致交易無法順利進行，甚至可能有黑客的入侵導致銀行或是個人資產有重大的損失。點對點網絡提供穩定的數據庫元數據，不會因為數據庫的停機而無法繼續使用，實現其 24 小時不間斷之運作。

第二，基於點對點網路架構完成遠距離支付。於跨國匯款從美國轉帳至中國一百萬美金的場景中，需要經過的手續較為繁瑣，資金有可能需要經過多個國家才可以抵達目的地，在經過各個國家的過程中，需要支付各國的手續費，也需要等待各個國家辦理該業務的時間，即使當資金順利抵達了目的地銀行，目的地銀行也需要花將近三

至五日的工作日確認該筆金額的來源。屆時領款人亦需要前往銀行核實完整的身份驗證、解釋資金用途，才得以領取這筆跨國資金。比特幣系統當中，有著 24 小時不間斷運作的優點，也因為點對點網絡架構，使得比特幣無需經由傳統金融機構繁瑣的步驟完成國際匯款，於比特幣系統中無系統壅塞的情況下，平均 10 分鐘即可入帳，實現其短時間內即可完成遠距離支付之運作。

第三，加密貨幣為使用者持有。傳統的金融體系中，資金的存儲、流動往往需要經過銀行，使用者將所有的資產存入銀行，拿到的是一串數字的銀行餘額，銀行是一個中心化的機構，有著最高的權利。中央社的新聞^[13]指出，臺灣各地於 2017 年接連於土地銀行、日盛銀行、彰化銀行、京城銀行、兆豐銀行皆傳出銀行行員監守自盜的行為，總金額高達一億三千萬新臺幣。在比特幣系統中，比特幣有如金幣般存放在個人的比特幣地址當中，使用者為真實持有著貨幣，即使是比特幣系統亦無權利動用該筆比特幣資產，唯有比特幣地址的私鑰持有者，實現其只為持有者所用之安全基礎。

第四，公開的交易信息。基於區塊鏈架構，所有的交易信息皆公開的方式存儲於區塊鏈中，並且可信任與方便的取得元數據，以下將針對可信任與原數據進行探討。

1. 可信任：在公有鏈的基本架構上，所有的交易記錄都是公開透明的存儲在區塊鏈當中，比特幣網絡的使用者都可以檢視該筆交易，所有人都可以檢查每個交易記錄的正確性，公開的交易信息亦提升交易數據之可信性。
2. 元數據：除了以區塊鏈技術為基礎建構出可信任的系統之外，開放和透明的特性讓更多的開發商或新公司更容易獲得交易的元數據。畢竟，在傳統金融體系中，所有交易記錄均由中央金融機構存儲，從中央金融機構提取原始交易信息並不容易，區塊鏈的開放性和透明性促使金融公司降低了獲取原始數據努力的門檻。公司或學者可以透過元數據制定出可視化的開發計畫，甚至可以運用大量數據來分析以前從未見過的有價值觀點。

第五，區塊鏈交易數據無法修改和刪除。在區塊鏈結構中，通過嚴格驗證的所有信息都記錄在區塊鏈中，且使用者及系統平台都不賦與刪除及修改之權限。根據區塊鏈的特點，舊區塊的哈希值在連接區塊鏈的過程中，舊區塊的哈希值會被存儲在新區塊。只要區塊中的值被修改，即使僅有 1 bit 的變化，也會產出完全不同的哈希值，這也就是所謂的雪崩效應（Avalanche effect）^[14]。由於上述結構特性，區塊鏈中所有的信息都不會被改變，倘若區塊中記載的比特幣交易在其中一個比特幣全節點驗證的結果被竊改，則該區塊將不被比特幣系統接受。因此，所有已經存儲在區塊鏈中的交易記錄將不能被修改和刪除，進而實現其架構安全之穩固。

第六，區塊鏈系統中所有的使用者皆為匿名。現今社會中，個人信息保護已成為企業最重要的課題。在區塊鏈系統中創建的所有賬戶都不會與真實世界中的實體建立

直接關聯，也因為沒直接關聯所以建立匿名。區塊鏈系統中的所有賬戶都是由匿名個體創建，匿名的設計可以有效保護消費者的隱私。然而，VISA 交易與比特幣系統截然不同，在使用 VISA 支付系統前，我們會向 VISA 公司的主機提交大量個人信息，這可能會產生個人信息洩露的風險。在區塊鏈技術中，其匿名之特性可以有效地避免這個問題。

第七，自治系統。在區塊鏈系統中，區塊鏈的運作依賴於一些算法，包括共識算法。因此，在這種自治系統中，沒有人（例如節點或礦工）可以直接改變系統運作的規則。如果在比特幣系統中發現需要更正的嚴重錯誤，可以使用比特幣改進提案（Bitcoin Improvement Proposals, BIP）^[15] 升級比特幣系統。在實施比特幣改進提案之前，提議的比特幣改進提案需要得到比特幣系統中超過一定數量的礦工算力支持。由於這種以投票機制升級系統的門檻相當高，使得區塊鏈系統通常不會有大的變化，但也因為變化不大而相對穩定。

1.1.3 加密貨幣的劣勢

在區塊鏈技術中，有著三項項瓶頸，分別為每秒處理的交易量（Transactions Per Second, TPS）僅為七筆的限制、洗錢防治困難、低可擴展性，以下將逐一探討。

第一，每秒處理的交易量上限僅為七筆。圖1.3為國際上較為廣泛使用的支付系統之每秒支持交易量比較圖，以 VISA 為例，其以公司中心化運營的方式可以支持高達每秒 2,000 筆交易。但是以區塊鏈技術為基礎的比特幣最大能夠接受的每秒處理交易量僅為 7 筆。一般認為只要提升區塊大小的限制，就可以提升每秒處理的交易量。以下說明提升每秒處理的交易量的同時也存下述的兩項問題，分別為區塊鏈成長速度過快造成節點崩潰以及區塊同步延遲造成區塊鏈分岔：



图 1.3 Bitcoin、Western Union^[16]、PayPal^[17] 以及 VISA 每秒支持交易量比較圖^[18]

1. 區塊鏈成長速度過快會造成去比特幣全節點不堪負荷：從 2009 年至今的比特幣區塊鏈大小已達到 156GB，這樣的成長速度因為比特幣區塊大小的最大值被設置為 1MB。圖1.4為過去比特區塊鏈大小，圖中可以發現，於 2016 年開始，比特幣區塊鏈的成長速度為一直線，這表示著比特幣網絡中持續維持在供不應求的

图 1.4 比特幣區塊鏈成長走勢圖^[19]

狀況。為解決比特幣每秒支持交易量上限的窘迫，現今對比特幣的每秒處理交易量有許多優化的方案，其中包括解除比特幣區塊大小 1MB 的限制。在一個區塊上限為 1MB 的限制下，滿載的比特幣系統中，比特幣區塊鏈平均每十分鐘會增 1MB，每小時會增加 6MB，每天會增加 144MB，每月會增加 4.2GB，每年會增加高達 50GB，要達到 1TB 的區塊鏈大小還需要 8 年，在 8 年後的未來存儲 1TB 的數據量應該不會有太大的負擔。倘若解除 1MB 的區塊限制，在系統的每秒處理交易量看似可以接受更多的交易成倍成長，面臨 1TB 的比特幣區塊鏈數據會在更短的時間內出現，倘若存儲區塊鏈的成本超過了摩爾定律的成長曲線，會進一步造成使用者自願成為比特幣全節點的意願度降低，使得比特幣網絡的全節點數變少，導致比特幣點對點網絡逐漸轉向中心化網絡發展，失去一開始點對點網絡的意義。

2. 造成區塊鏈最新區塊同步延遲。對於區塊鏈的區塊同步延遲同時也會造成比特幣網絡的影響，J. Göbel 於“Increased block size and Bitcoin blockchain dynamics”^[20] 有著詳細的研究，在上修區塊大小上限的議題上，使用者自願成為比特幣全節點意願度下降，亦有機會在比特幣點對點網絡建構出的區塊鏈同步上造成延遲，在 1055 個比特幣全節點當中，平均每十分鐘會有礦工於其中一個全節點生成一個最新的區塊，該最新的區塊會以點對點網絡協議同步到 1055 個節點上。在比特幣系統中，長年來的過程經驗可以發現在礦工生成 1MB 的區塊後同步到全網節點可以在創造下一個區塊之前完成。倘若將區塊大小修改為 2MB 或是更大，會

使得比特幣全節點的最新區塊同步延遲現象更加明顯，同步延遲會使得區塊鏈分岔，造成 1055 個比特幣全節點的信息不一致，近一步造成整個比特幣點對點網絡崩潰。

第二，洗錢防治困難。匿名性為比特幣系統一大特色，比特幣的地址生成的熵是 256 bits，亂數是在 2^{256} 的組態空間中隨機選取，這樣的地址與現實生活中的身份並無任何關聯，使得黑市交易、洗錢防治變的困難，甚至有更為前沿的加密貨幣 Monero^[21] 導入了環簽章（Ring Signature）^[22] 算法、Zcash^[23] 導入零知識證明算法^[24]，使得原本公開透明的區塊鏈，變得無法檢視，進而造成加密貨幣在洗錢防治上更加的困難。2017 年由 Thibault de Balthasar and Julio Hernandez-Castro 所提出的論文 "An Analysis of Bitcoin Laundry Services."^[25]，致力探究比特幣匿名交易下的資金流動模型，試圖以機械學習的方法找出比特幣洗錢模型作為洗錢的工具，圖 1.5 為該論文針對黑市交易中的洗錢服務運營商 Darklaunder 進行洗錢機械學習識別有著傑出的成果。



图 1.5 Darklaunder 洗錢模型^[25]

第三，低可擴展性。區塊鏈架構為了防止個是的攻擊，所以在架構訂定以及接口設計都有著嚴謹的規範。以下將闡述造成比特幣低可擴展性的原因：

1. 修改比特幣協議製作添加外部信息的區塊鏈：比特幣區塊鏈技術是一個嚴謹的架構，倘若要創造可以支持外部信息的結構需要重新創造全新的加密貨幣，大部分的加密貨幣不支持外部輸入，外部的信息輸入皆無法保證信息的正確性，近一步

造成垃圾進垃圾出（Garbage in, garbage out, GIGO）的問題，倘若錯誤的信息存儲在無法刪除、修改的區塊鏈下，只是強化該筆錯誤信息的錯誤。如食品履歷區塊鏈，致力於將食品生產到超市的過程逐一記錄在區塊鏈上，但如果一開始在輸入信息時，無法保證其信息之正確性，該食品履歷區塊鏈則毫無意義。

2. 於區塊頭或交易信息添加外部信息：比特幣區塊鏈上，可以添加一些信息於區塊上，該信息會永久保存於區塊鏈上，除了在區塊上新增信息，在比特幣單筆交易信息上，亦可填寫一些私人信息，但這樣的空間大小有限，且現今的比特幣價格日趨上漲，比特幣交易手續費是以單筆交易大小計算，這將使得在交易中添加些個人信息變得更加昂貴。

在比特幣系統中，其區塊鏈僅用於記錄交易記錄，不能擴展更多功能和應用程序。有很多開發者希望將比特幣系統擴展到智能合約等其他應用程序。但是，後來發現改變原始比特幣系統框架是具有挑戰性的工作。因此，全球第二大加密貨幣以太坊（Ethereum, ETH）的作者 Vitalik 也創建了以太坊虛擬機（Ethereum Virtual Machine, EVM）。其所創建的智能合約可以在統一的以太坊平臺上運行，而以太坊也藉此突破了比特幣之技術瓶頸。

1.1.4 國際情勢分析

比特幣是一種全新的價值交換的媒介，因為過於前沿在各個國家所秉持的態度皆有所不同，大致可將個國家對比特幣的政策分為兩大類，分別為接納與禁止，在接納的分類當中又分為歡迎放任以及監管。在歡迎放任的政策下的國家包括伊朗、以色列、法國、美國、沙特阿拉伯王國以及烏克蘭，上述國家政策上皆已抱持著開放且不監管的方式接納加密貨幣，這些國家認為加密貨幣對於國家金融科技的發展具有前景；在分類在接納但是實施監管的國家中，包括韓國、菲律賓、英國、馬來西亞、俄羅斯、日本以及香港地區皆認為加密貨幣技術可能存在的高風險，且針對加密貨幣的洗錢防制以及非法集資進行嚴格管理，也進一步制定相關的法律，使得國家可以應對新型加密貨幣的糾紛；在禁止得分鐘中包括辛巴威、摩洛哥、印尼以及中國，這些國家認為比特幣是一個非法的貨幣，因為涉及到洗錢問題、難以實施外匯管制。但是對於區塊鏈技術上技術探討，在所有國家中都是蓬勃發展。如表1.1：

1.2 研究目標與內容

基於比特幣在各個國家的蓬勃發展且應用在相當多的領域，應用的領域包括交易所、去中心化交易所、兌幣所、遊戲點數、網路購物、資產的保存、募資以及遠距離支付，甚至是各國的銀行和金融機構都逐步投入人力及資金研究區塊鏈相關技術，甚至

表 1.1 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 | 伊朗 | 監管得當歡迎 比特幣發展 | | |
| 2 | 以色列 | 歡迎：欲發展 國際 ICO 中心 | | |
| 3 | 法國 | 放任：與實體 經濟無關 | | |
| 4 | 美國 | 暫不構成威脅 | | |
| 5 | 新加坡 | 不監管但注意 周邊活動 | | |
| 6 | 沙特阿拉 伯王國 | 加密貨幣尚未 成熟，不監管 | | |
| 7 | 烏克蘭 | 不屬於貨幣 | | |
| 8 | 韓國 | | 很快將監管 交易所 | |
| 9 | 菲律賓 | | 計劃監管 ICO | |
| 10 | 英國 | | 考慮監管 | |
| 11 | 馬來西亞 | | 正規化監管框架 | |
| 12 | 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 | 辛巴威 | | | 定法前，屬非法 |
| 16 | 摩洛哥 | | | 禁止加密貨幣交易 |
| 17 | 印尼 | | | 2018 年前 全面禁止 |
| 18 | 中國 | | | 禁止加密貨幣 |

是訂定各國相關的法律。在比特幣資產的流動上存在著許多的問題，第一，比特幣的帳戶是由亂數產生器生成，該比特幣帳戶與在現實生活中的使用者不無直接關聯，使得比特幣洗錢變更加盛行。第二，現今的比特幣交易皆為匿名對匿名支付，並無正式的收據開立，使得消費者在購物後，倘若商品存在問題，無法得到法律上的保障。第三，因為比特幣是匿支付匿名交易，使得政府無法查閱商家的收入進一步課徵稅收，造成逃漏稅的灰色地帶。

本文將解決上述三項問題，設計與實現一個区块链的实名交易實時監督系統達到下列幾點目標：

1. 將商家比特幣地址實名制，構建政府可以檢視商家營收的区块链的实名交易實時監督系統，使店家可以進行註冊，再由政府進行商家註冊後的審查。
2. 構建商家端行動收銀與交易明細系統，使得商家可以開立收據以保障消費者應有的消費者權益。
3. 使得政府可以課徵加密貨幣的相關稅收。
4. 以多重簽章技術提升比特幣交易速度，達到實時的比特幣交易系統。

為實現上述目標，本文首先將詳細探討區塊鏈技術的優勢，藉由深度了解區塊鏈技術的優勢可以取之優點，如區塊鏈是一個不間斷、不可篡改、去中心化、公開數據庫、穩定的系統。第二，探討區塊鏈技術的劣勢，區塊鏈技術並非完美，存在著洗錢、逃漏稅、無法保障消費者權益以及交易速度慢的問題，藉由瞭解問題，並設計系統解決。第三，交易模型分析，透過交易模型分析探討在現金、電子貨幣以及加密貨幣存在的交易模型，並在諸多交易模型中發現，匿名支付給實名的交易行為，可以保障消費者隱私，同時保障消費者權益，更使得政府可以對商家的營收進行檢視。第四，系統設計，完成交易分析，並著手設計數據庫模型、主系統、三個子系統的系統架構。第五，系統實現，利用 Java 編程語言實現主系統以及三個子系統。第六，系統優化，比特幣的多重簽章算法，實現實時的比特幣交易監督系統。第七，功能測試，測試以 Java 編成程序所有的功能是否能夠完整運作。第八，性能測試，測試在未進行優化的系統與已經優化的系統性能的差異。

1.3 論文組織結構

第二章 相關理論與技術

2.1 比特幣 (Bitcoin)

表 2.1 比特幣簡介

| | |
|-----------------|-----------------------|
| 第一個區塊生成時間 | 2009 年 1 月 3 日 |
| 比特幣預計總產量 | 21,000,000 BTC |
| 比特幣目前總產量 | 16,921,800 BTC |
| 最新區塊高度 | 513743 |
| 比特幣總市值 (人民幣) | 5 兆 |
| 比特幣全節點的數量 | 11147 個 |
| 單日比特幣交易金額 (BTC) | 124,017.02430718 BTC |
| 單日交易筆數 | 196,606 筆 |
| 比特幣區塊鏈大小 | 188.89 GB |
| 平均區塊大小 | 0.75 MB |
| 平均生成單一區塊所需時間 | 9.67 分鐘 |
| 單日產出比特幣數量 | 1,775 BTC |
| 挖礦難易度參數 | 3,290,605,988,755 |
| 全網挖礦算力 | 23,555,075.18 THash/s |

比特幣 (Bitcoin, BTC) 表2.1是比特幣系統的相關參數簡介，比特幣是一個點對點式的電子現金系統，集成了非對稱式金鑰密碼學 (Asymmetric Key Cryptography)^[26]、簽章密碼學 (Signature Cryptography)^[27]、零知識證明密碼學 (Zero Knowledge Proof Cryptography)^[24]、哈希函數密碼學 (Hash Function Cryptography)、共識算法 (Consensus Algorithm)^[28] 諸多技術建構了一個分散式、不需要仰賴中心化機構加以維護的交易帳本。在接下來的章節中將逐一進行詳盡的說明每個技術在各個環節中所扮演的角色。

2.2 比特幣地址 (Bitcoin Address)

比特幣地址為比特幣的載體，深入瞭解比特幣的地址生成相關算法、比特幣地址生成過程、多重簽章，可以近一步應用在區塊鏈的實名交易監督系統。

2.2.1 比特幣地址生成相關算法

在點對點的現金系統中，首先必須先生成一個地址，在比特幣的協議中有著既定的程序生成地址。運用到的技術包括亂數產生器、secp256k1^[29]、SHA-256 (哈希函數)^[30]、

RIPEMD-160（哈希函數）^[31]、Base58^[32]。接下來將詳述每一個函數的運作過程以及意義，最後說明比特幣交易地址生成的每一個步驟。

亂數產生器（Random number generator）

亂數在密碼學中是個相當重要的一環，在比特幣系統中更是重要，畢竟生成的亂數會變成比特幣的私鑰，私鑰是簽署資產轉移的唯一方式，在比特幣地址中的亂數產生器會產出一個 256 bits 長度的亂數，也就是私鑰，256 bits 的長度可以表現的組態空間為 2^{256} ，換算成十進位表示為 1.1579209×10^{77} ，要在這組態空間中，以亂數產生同樣的一把私鑰是一件困難的事，但也有國際的實驗室^[33] 團隊正在努力的窮舉比特幣 2^{256} 的組態空間，如圖2.1所示，根據 LBC 公佈的數據顯示，目前已經完成了 2.330109×10^{16} 個地址探索。雖然 10^{16} 的級別與 10^{77} 的級別相距甚遠，但 LBC 已探索的組態空間中擊中了 15 個比特幣地址，該團隊也成功將這 15 個地址下的 1.180899 個比特幣轉走。

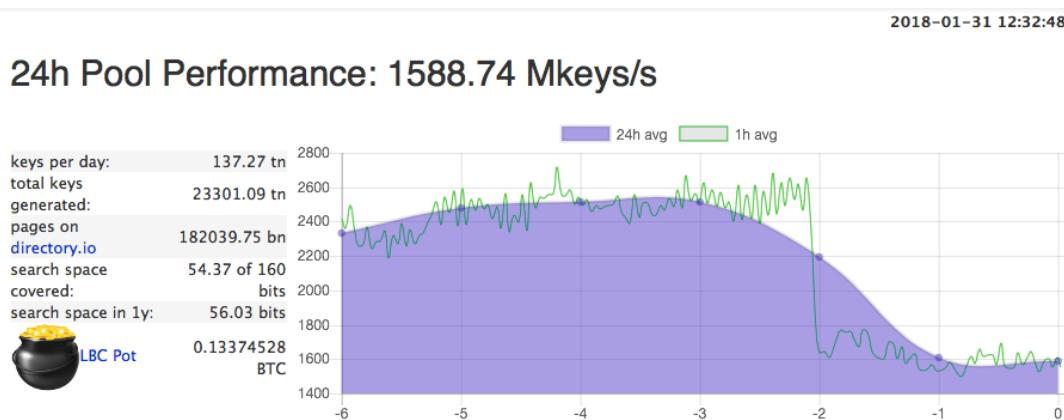


图 2.1 LBC 穷举比特币私钥算力状态图^[33]

如何建構一個亂數，在過往的亂數產生器往往會加入時間作為參數，但對於一個攻擊者而言，只需要去猜測在這段時間內目標者所有生成的可能性有極高的機率可猜出亂數。而亂數在密碼學中常會是一把私鑰的生成，在 https 協議中，服務器端與客戶端，建立一個加密連線的過程中也需要一個亂數去建立一個高安全性的加密通道-傳輸層安全性協定（Transport Layer Security，TLS）^[34]，在 SSH 協議中也採用了亂數。

在過去的歷史事件中，發現 Android 手機版以及平板版的亂數產生器中存在著不隨機，於 2013 年 8 月比特幣開發者 Mike Hearn 提及“All private keys generated on Android phones/tablets are weak and some signatures have been observed to have colliding R values”^[35]，Bitcoin.org 也發布了警告^[36] 簡要說明該事件的原因，以及表明影響到的比特幣錢包客戶端有 Bitcoin Wallet、BitcoinSpinner、Mycelium Bitcoin Wallet、blockchain.info。這樣的錯誤源於 Android 本身支持的亂數產生器並不隨機，隨後 Android 解釋了亂數的問題

並加以修正。在這 Android 手機亂數不夠亂的事件中，有自願者自發性地公佈自己的損失狀態，總金額為 55.82152538 個比特幣^[37]，但因為比特幣屬於被動的性質，無人主動回報即不會加入統計中，所以總損失估計會超過 55.82152538 個比特幣。

Secp256k1

在密碼學中有分對稱式加密與非對稱式加密，對稱式加密又分為信息流加密與信息塊加密，信息流加密著名的是由美國密碼學家 Ron Rivest 教授設計，包括 RC2 (1987 年)^[38]、RC4 (1987 年)^[39]、RC5 (1994 年)^[40]、RC6 (1998 年)^[41]；信息塊加密著名的有數據加密標準 (Data Encryption Standard, DES, 1975 年)^[42]、三重數據加密算法 (Triple Data Encryption Algorithm, Triple DES, 1998 年)^[43]、高級加密標準 (Advanced Encryption Standard, AES, 1998 年)^[44]；非對稱式加密最廣為人知的有 RSA (Rivest – Shamir – Adleman, 1977 年)^[45]、橢圓曲線密碼學 (Elliptic curve cryptography, ECC, 1985 年)^[46]。非對稱式加密與對稱式加密最大的不同在於，對稱式加密在加密解密的過程中只需要一把鑰匙，而非對稱式加密會生成兩把鑰匙分別為私鑰與公鑰，在算法的設計上一開始會以亂數產生一把私鑰，再經由非對稱式加密算法推導出公鑰，推導出的公鑰在非對稱式密碼學中並無直接的方法可以反推至私鑰，如此一來確立私鑰的安全性。非對稱式密碼的使用場景有兩種，第一種是希望收到加密信息的使用者 Alice，Alice 會生成私鑰存儲在自己本地端的電腦中，並將推導出的公鑰公佈在網絡上，這時希望聯繫 Alice 的使用者 Bob 在網絡上取得公鑰後，Bob 會以 Alice 的公鑰進行加密，之後將密文寄送給 Alice，在傳遞信息的過程中，即使網絡存在著監聽，也無法將信息順利解密，唯有 Alice 收到信息後使用 Alice 原本產生該公鑰的私鑰，才可以解出明文。第二種則應用在比特幣的交易之數字簽名以及交易驗證交易，比特幣地址的創建過程中會透過 secp256k1 生成私鑰公鑰對，在創建比特幣交易的過程中，使用該地址的私鑰對該地址未花費的輸出 (Unspent Transaction Output, UTXO) 進行數字簽名，完成數字簽名後會與公鑰以及交易信息一起廣播到比特幣網絡的交易緩存池當中，比特幣交易緩存池存在於所有比特幣全節點當中，主要存儲所有未被收入到比特幣區塊鏈內的所有交易，也就是零確認交易，等待礦工將該筆交易收入至比特幣區塊鏈當中。比特幣採用的 secp256k1 是屬於橢圓曲線密碼學中的一個版本，不同的橢圓曲線版本的差異在於不同的初始參數，包括橢圓曲線方程

$$y^2 = x^3 + ax + b$$

$p=FFFFFFFFFFFFFFFFFFF...FFFFFEFFFC2F$
為巨大的素數、G 點被稱為生成點的常數點亦稱為基點。至於為什麼選擇 ECC 而非

RSA 的主要原因，其一在於 ECC 在生成密鑰對所需的時間更佳快速，圖2.2為 Nicholas Jansma 於 2004 年針對 ECC 與 RSA 的密鑰對生成時間與數字簽名所需時間的論文^[47]顯示，當 ECC 產生 571 bits 的密鑰長度，RSA 要達到相同的安全性需要生成 15360 bits，這也導致生成時間產生高達 471 倍之差距。

| Key Length | | Time (s) | |
|------------|-------|----------|--------|
| ECC | RSA | ECC | RSA |
| 163 | 1024 | 0.08 | 0.16 |
| 233 | 2240 | 0.18 | 7.47 |
| 283 | 3072 | 0.27 | 9.80 |
| 409 | 7680 | 0.64 | 133.90 |
| 571 | 15360 | 1.44 | 679.06 |

图 2.2 ECC 與 RSA 的密鑰對生成時間比較圖^[47]

除了在密鑰對生成時間 ECC 有著比 RSA 更高效的算法外，在安全性上 ECC 可以更短的密鑰長度達到與 RSA 相同的安全強度，L Ducas 針對 ECC、RSA、BLISS^[48]做出了深度的安全性探討^[48]，圖2.3同樣達到 80 bits 的安全性級數，RSA 1024 需要 1024 bits，ECDSA 160^[49] 僅需要 160 bits，該篇論文除了探討 RSA 與 ECDSA 之外，更大的部分在闡述量子計算機對於既有的傳統密碼帶來的抨擊，有機會快速窮舉 2^{256} 的比特幣私鑰，在未來量子計算機的蓬勃發展擁有 2000 qbits 運算能力，量子計算機可以快速窮舉破解所有的比特幣私鑰。因此發展針對量子計算機設計的數字簽名算法成為密碼學上嶄新的議題，而 BLISS 則為針對量子計算機所設計的抗量子計算的簽章算法。

| Implementation | Security | Signature Size | SK Size | PK Size | Sign (ms) | Sign/s | Verify (ms) | Verify/s |
|------------------------------|-----------------|----------------|---------|---------|-----------|--------|-------------|----------|
| BLISS-0 | ≤ 60 bits | 3.3 kb | 1.5 kb | 3.3 kb | 0.241 | 4k | 0.017 | 59k |
| BLISS-I | 128 bits | 5.6 kb | 2 kb | 7 kb | 0.124 | 8k | 0.030 | 33k |
| BLISS-II | 128 bits | 5 kb | 2 kb | 7 kb | 0.480 | 2k | 0.030 | 33k |
| BLISS-III | 160 bits | 6 kb | 3 kb | 7 kb | 0.203 | 5k | 0.031 | 32k |
| BLISS-IV | 192 bits | 6.5 kb | 3 kb | 7 kb | 0.375 | 2.5k | 0.032 | 31k |
| RSA 1024 | 72-80 bits | 1 kb | 1 kb | 1 kb | 0.167 | 6k | 0.004 | 91k |
| RSA 2048 | 103-112 bits | 2 kb | 2 kb | 2 kb | 1.180 | 0.8k | 0.038 | 27k |
| RSA 4096 | ≥ 128 bits | 4 kb | 4 kb | 4 kb | 8.660 | 0.1k | 0.138 | 7.5k |
| ECDSA¹ 160 | 80 bits | 0.32 kb | 0.16 kb | 0.16 kb | 0.058 | 17k | 0.205 | 5k |
| ECDSA 256 | 128 bits | 0.5 kb | 0.25 kb | 0.25 kb | 0.106 | 9.5k | 0.384 | 2.5k |
| ECDSA 384 | 192 bits | 0.75 kb | 0.37 kb | 0.37 kb | 0.195 | 5k | 0.853 | 1k |

图 2.3 算法 BLISS、RSA、ECDSA 安全級數比較圖^[48]

哈希算法 SHA-256

SHA-256 是 SHA (Secure Hash Algorithm, FIPS 182-2)^[30] 哈希算法的家族之一。SHA 家族當中有著四大分支，分別為 SHA-0、SHA-1、SHA-2 和 SHA-3，如表2.2所示。

各種哈希算法的差異在於運算初始變數、算法所採用的運算子、接受的信息長度以及迴圈樹的不同。上述的參數差異皆由聯邦資訊處理標準 (Federal Information Processing Standards, FIPS) 中定義。表2.2中 MD5 不為 SHA 家族成員之一，但 MD5 為最早被廣泛使用的哈希算法，因此作為借鑒的標準。SHA-0 為 SHA 家族中被最早提出的架構，輸出的長度為 160 bits，而 SHA-1 提出後並無太大的變動。哈希算法的主要功能在於，將信息或是檔案建立一個對一的指紋，也就是哈希值，而該指紋長度會依照算法的設計輸出的長度而略有不同，表2.2中顯示的輸出哈希值長度，而長度也意味著該指紋的組態空間應設的大小。倘若有著不同的輸入，但映射到了相同的指紋，則將此現象稱之為碰撞。通常在信息安全領域中，只要發現該哈希算法存在著碰撞，就會被棄用。甚至是專家們提早數年提出警告，要求提早更換該哈希算法，並更換上新制定的哈希算法做應用。哈希算法的功能包括藉由生成哈希值進行檔案校驗、工作量證明算法設計以及區塊鏈中的哈希指針。

1. 生成哈希值進行檔案校驗：哈希值在過往的應用中，往往作為檔案完整性的校驗，軟件供應者會在網站中提供各式不同算法的哈希值供給使用者下載完軟件之後，使用者將檔案輸入哈希算法中生成出哈希值後進行比對。但倘若該哈希算法存在碰撞的發生，這會使得不同的檔案存在著同樣的哈希值。這也意味著軟體提供平台所提供的軟體可能存在著摻入惡意代碼後，還能生成同樣的哈希指紋，失去了檔案完整性的校驗的功能，這便成為信息安全中的重大漏洞，因此在表2.2中的 MD5、SHA-0 以及 SHA-1 皆為已經棄用之算法。
2. 工作量證明算法設計：起出工作量證明算法的概念為設計一個求解困難，但驗算的過程中卻相當簡單快速。如對一個大數做因式分解是一個相當困難的事，但要驗算其結果僅需要將所有的解相乘確認是否為該大數即可證明。同樣的理念在比特幣系統中是以 hash-puzzle 的方式實現，hash-puzzle 是利用哈希函數有著不可預期的特性，不可預期指的是假設輸入連續性的數值 1 到 n 進入到哈希函數生成哈希值，而生成的哈希值無法觀察出關聯性，可說是完全不相關的數值，且無法預期下個輸入的哈希值輸出。比特幣系統中的困難度變數，在 hash-puzzle 中定義了何謂真正的答案。在 SHA-256 當中輸出的值為 256 bits 的哈希值，困難度變數則規定了在這 256bit 當中，自最左邊起必須為零的位數的門檻，而在困難度變數要求必須為零的位數變多，則意味著要在連續性的數值 1 到 n 的 hash-puzzle 中，符合門檻的解越少。在 hash-puzzle 中，求得一個符合困難度變數的哈希值是困難的，但要驗算求得的解是否符合困難度的門檻相當快速，這符合起出工作量證明算法的概念。
3. 區塊鏈中的哈希指針：比特幣區塊鏈的區塊頭當中，當前區塊存儲著前區塊頭的

雙重哈希的哈希值。當前區塊則會如資料結構鏈結串列一樣，直到鏈結到第一個比特幣區塊創世區塊，區塊鏈中的哈希指針將區塊鏈結在一起，也就形成了比特幣區塊鏈的基礎。在比特幣挖礦的過程中，礦工參與著最新區塊的 hash-puzzle 的解題，尋找一個符合困難度變數的輸入。但 hash-puzzle 的工作證明當中解可能不只一個，但只要符合困難度變數的解都可以創建一個新的區塊，屆時就會在當前的區塊上同時產生分岔，分岔的區塊在比特幣系統中皆為有效，但經過多個區塊的疊加之後，變可以抉擇出最長的鏈，該最長鏈則成為主鏈，而其他的分岔鏈，則成為孤兒塊被丟棄，當中曾記載的交易信息無效，造成該分岔鏈的交易信息回溯。比特幣區塊鏈的分岔好發於最新的區塊，如圖2.4所示，而越舊的區塊則越不易發生，所以在比特幣交易中默認該筆交易要在六個區塊確認後，該公司才會承認該筆交易有效。

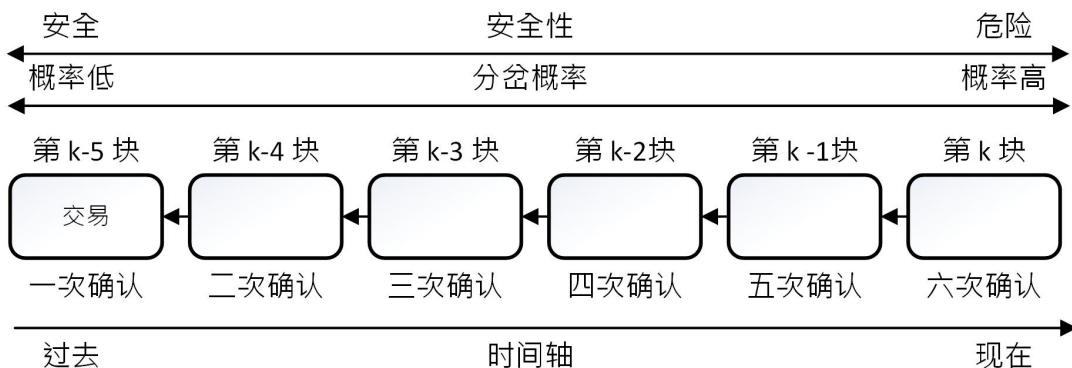


图 2.4 區塊疊加示意圖

Base58 編碼

表2.3為 Base58 編碼表，Base58 編碼的首次出現自 Satoshi Nakamoto 所提出的論文^[50] 當中，Base58 編碼是源自於 Base64 編碼表，如表2.4中所示。Base64 編碼中包括大寫英文 26 個字母、小寫英文 26 個字母、阿拉伯數字以及字符"/" 和 "+"。在比特幣地址生成過程中 Base58 的功能是將比特幣地址的公鑰哈希值重新編碼，比特幣地址的公鑰哈希值是二進制的資料型態，既使是將二進制碼轉換成十六進制碼輸出也是對人類辨識上有一定的不便性。倘若採用 Base64 對比特幣公鑰哈希值進行編碼有效縮短二進制碼的長度，但 Base64 的編碼存在著不適於作為地址的特殊字符 "+" 和 "-"。在 Base58 編碼中移除了特殊字符之外，移除了較不易人類判讀的相關字符數字 "0" 與大寫英文字母 "O"，因為該兩字符在不同字型的體現相當相似，大寫英文字母 "I" 以及小寫英文字母 "l"，在人類判讀上也有些為相似。因此於 Base64 移除上述 6 個字符後，便形成了 Base58 編碼表。值得一提的是，Base58 編碼與 Base64 編碼表中的字符排序有些許異

表 2.2 MD5、SHA-0、SHA-1、SHA-2 和 SHA-3 比較表

| 算法 | 分支 | 輸出哈希值長度(bits) | 最大輸入信息長度(bits) | 迴圈次數 | 使用到的運算子 | 碰撞攻擊(bits) | |
|-----------|----------|---------------|----------------|------|--|-------------|--|
| MD5 參考 | - | 128 | ∞ | 64 | And, Xor, Rot, Or, Add (mod 2^{32}) | < 64 已碰撞 | |
| SHA-0 | - | 160 | $2^{64} - 1$ | 80 | | < 80 已碰撞 | |
| SHA-1 | - | | | | | < 80 已碰撞 | |
| SHA-2 | SHA-224 | 224 | $2^{64} - 1$ | 64 | And, Xor, Rot, Or, Shr, Add (mod 2^{32}) | 112 | |
| | SHA-256 | 256 | | | | 128 | |
| | SHA-384 | 384 | $2^{128} - 1$ | 80 | | 192 | |
| | SHA-512 | 512 | | | | 256 | |
| SHA-3 | SHA3-224 | 224 | ∞ | 24 | And, Xor, Rot, Not | 112 | |
| | SHA3-256 | 256 | | | | 128 | |
| | SHA3-384 | 384 | | | | 192 | |
| | SHA3-512 | 512 | | | | 256 | |

動，Base58 編碼表將數字的部分一致了最前面，這使得比特幣地址以 Base58 編碼後的第一個字符呈現為"1"的主要原因。

2.2.2 比特幣地址生成過程

1. 生成私鑰：使用亂數產生器產生一個長度為 256 bits 的亂數，而此亂數即成為該比特幣地址的私鑰。在比特幣的系統當中，私鑰可以透過橢圓曲線簽章算法 secp256k1 簽名一筆交易，廣播治比特幣網路當中。因為私鑰為該地址資金轉移的關鍵，黑客攻擊的對象皆會聚焦在比特幣私鑰，因此私鑰的保存成為比特幣系統中最為熱門的課題之一。
2. 生成公鑰：在以亂數產生器生成私鑰之後，接下來將運用到非對稱是密碼學中的私鑰公鑰轉換算法，於比特幣系統中採用的是 secp256k1，secp256k1 是橢圓曲線密碼學中的其中一個版本，不同的版本差異在於採用不同的變數。於比特幣地址生成的過程中，secp256k1 負責將上步驟生成的私鑰透過橢圓曲線算法計算出公鑰，生成的公鑰長度為 512 bits，比前步驟 256 bits 的私鑰多了一倍的長度。在比特幣交易中，私鑰可以簽署一筆交易，在簽署完之後便會將公鑰、簽名以及交易信息廣播至比特幣網路當中等待被收入到比特幣區塊鏈當中，此時該筆交易準備被存儲在比特幣交易緩存持當中，屆時可以使用 secp256k1 算法對透過公鑰、簽名以及交易信息進行驗算，倘若計算出的值為真則為有效，則會讓該筆交易繼續

表 2.3 Base58 編碼表

| 数值 | 字符 | 数值 | 字符 | 数值 | 字符 | 数值 | 字符 |
|----|----|----|----|----|----|----|----|
| 0 | 1 | 16 | H | 32 | Z | 48 | q |
| 1 | 2 | 17 | J | 33 | a | 49 | r |
| 2 | 3 | 18 | K | 34 | b | 50 | s |
| 3 | 4 | 19 | L | 35 | c | 51 | t |
| 4 | 5 | 20 | M | 36 | d | 52 | u |
| 5 | 6 | 21 | N | 37 | e | 53 | v |
| 6 | 7 | 22 | P | 38 | f | 54 | w |
| 7 | 8 | 23 | Q | 39 | g | 55 | x |
| 8 | 9 | 24 | R | 40 | h | 56 | y |
| 9 | A | 25 | S | 41 | i | 57 | z |
| 10 | B | 26 | T | 42 | j | | |
| 11 | C | 27 | U | 43 | k | | |
| 12 | D | 28 | V | 44 | m | | |
| 13 | E | 29 | W | 45 | n | | |
| 14 | F | 30 | X | 46 | o | | |
| 15 | G | 31 | Y | 47 | p | | |

表 2.4 Base64 編碼表

| 数值 | 字符 | 数值 | 字符 | 数值 | 字符 | 数值 | 字符 |
|----|----|----|----|----|----|----|----|
| 0 | A | 16 | Q | 32 | g | 48 | w |
| 1 | B | 17 | R | 33 | h | 49 | x |
| 2 | C | 18 | S | 34 | i | 50 | y |
| 3 | D | 19 | T | 35 | j | 51 | z |
| 4 | E | 20 | U | 36 | k | 52 | 0 |
| 5 | F | 21 | V | 37 | l | 53 | 1 |
| 6 | G | 22 | W | 38 | m | 54 | 2 |
| 7 | H | 23 | X | 39 | n | 55 | 3 |
| 8 | I | 24 | Y | 40 | o | 56 | 4 |
| 9 | J | 25 | Z | 41 | p | 57 | 5 |
| 10 | K | 26 | a | 42 | q | 58 | 6 |
| 11 | L | 27 | b | 43 | r | 59 | 7 |
| 12 | M | 28 | c | 44 | s | 60 | 8 |
| 13 | N | 29 | d | 45 | t | 61 | 9 |
| 14 | O | 30 | e | 46 | u | 62 | + |
| 15 | P | 31 | f | 47 | v | 63 | / |

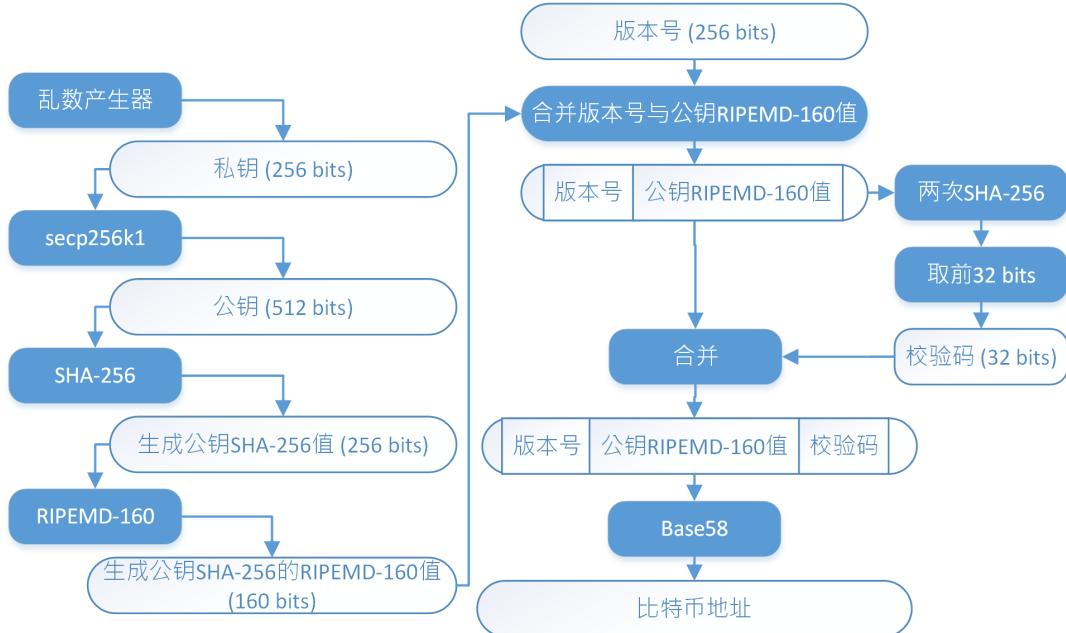


图 2.5 比特幣地址生成流程圖

待在交易緩存持當中，等待被收入區塊鏈內。

3. 生成公鑰 SHA-256: SHA-256 為 SHA 家族之一，也是哈希算法的一種，因此符合哈希算法的特徵包括雪崩效應、不可預測、不可逆（單向性）以及校驗檔案是否完整性的諸多特性。在該步驟將前步驟生成長度為 512 bits 的公鑰作為 SHA-256 的輸入，產出長度僅為公鑰長度的一半的公鑰 SHA-256 哈希值。算該步驟使得知道公鑰 SHA-256 的攻擊者，更加難以用窮舉攻擊推導出該地址的公鑰。
4. 生成公鑰 SHA-256 的 RIPEMD-160: RIPEMD-160 也是哈希算法的一種，特色與哈希算法的特徵相同，RIPEMD-160 與 SHA-256 較為不同的部分在於 RIPEMD-160 生成的哈希值長度為 160 bits。在前步驟中，對公鑰進行 SHA-256 計算，公鑰已經有了第一層的保護，而在該步驟中，再次透過 RIPEMD-160 取得哈希值，這使得攻擊者既使取得比特幣地址，必須針對 RIPEMD-160 進行破譯，再進一步對 SHA-256 才有機會取得該地址的公鑰，也因為這樣的設計，對於僅收取比特幣不曾花費比特幣的比特幣地址，於黑客攻擊上造成相當大的難度。
5. 取得版本號: 在比特幣系統初始的設計中，已經定義了些不同功能的比特幣地址，這些特殊功能的比特幣地址有著特殊的版本號，最為常見的為以"1"為頭的比特幣地址，該地址為比特幣系統中最早被使用且最為普遍的地址版本，該地址為一把私鑰進行比特幣地址推倒，所以僅需要一把鑰匙就可以移動該地址下的比特幣資產；第二種是以"3"為地址開頭的比特幣地址，該地址採用多重簽章技術，該技術為後續經過多項 BIP 才完成落實於比特幣系統當中，該地址生成的過程中，，，

在第五個步驟中會加入版本號加以區分不同的地址。

6. 校驗碼生成：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降低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。對公鑰 SHA-256 的 RIPEMD-160 再做兩次 SHA-256，取該哈希值前 32 bits 的值作為校驗碼。
7. 版本號、公鑰 SHA-256 的 RIPEMD-160 和校驗碼合併：版本號、第四個步驟的產生之公鑰 RIPEMD-160 及第五個步驟產生之校驗碼合併。
8. 合併的結果以 Base58 編碼：將第六步驟組進行合併組合的結果，利用 Base58 進行編碼，Base58 修改自 Base64，其與 Base64 最大不同之處在於移除了"0"、"O"、"I"、"l"、"+"、"/" 的字符，可以降低人工在判讀地址的錯誤率。

2.2.3 多重簽章（Multi-Signature）

比特幣區塊鏈技術，雖然已經利用工作量證明的方式解決了雙重支付（Double-spending）問題^{[51][52]}，但工作量證明的算法所設定之題目困難度會直接影響到每一個比特幣區塊的產出時間，這個比特幣區塊的產出時間也考慮到比特幣全節點於全世界各地的網絡同步狀況，倘若今天的區塊生成時間過短會造成全世界的比特幣節點之區塊數據不一致，這樣的數據不一致將導致比特幣區塊鏈出現分岔，在更嚴重一點甚至會造成比特幣網絡的瓦解。

雙重支付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雙重支付同一筆款項。現今的比特幣區塊產出速度為十分鐘一塊，即使附上足夠的手續費也須等待將近十分鐘的時間，倘若是在手續費不足的情況下，該筆比特幣交易甚至會在比特幣交易緩存池中滯留一週的時間。在手續費足夠的情況下，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 Green Address 技術致力於在一開始創建交易的同時管控雙重支付交易的發生，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 Green Address 機構節點，這筆交易的建立必須要雙方同時簽署交易才被允許廣播至比特幣網絡中。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，視同該筆交易不曾存在過，故若真的遇到交易被遺棄的情況，Green Address 機構節點也會透過內部的數據庫記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。Green Address 機構節點也就成為了交易創建的把關者，過濾所有的雙重支付攻擊的發生，也避免交易因為比特幣網絡塞車而交易被礦工遺棄的情形。在這樣的機制下，只要是用 Green Address 錢包交易即可確認雙重支付攻擊是不會發生的，

對商家或是收款人而言，可以得到在即時交易中不被雙重支付攻擊的保障，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。

Green Address 錢包生成過程 此節將詳細闡述 Green Address 錢包生成過程的重要步驟，如圖2.6所示。

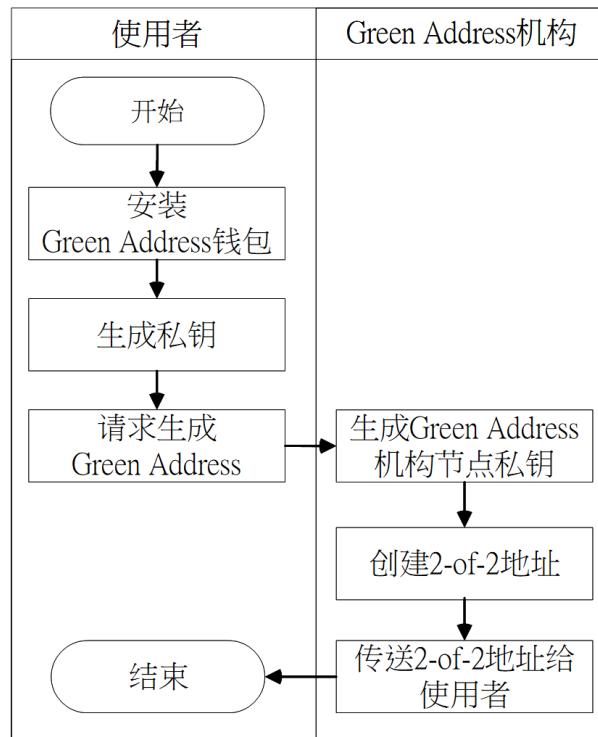


图 2.6 Green Address 錢包生成流程圖

1. 使用者安裝 Green Address 比特幣錢包，並向 Green Address 機構節點請求創建 2-of-2 多重簽章比特幣地址。
2. 使用者與 Green Address 機構節點分別生成兩把私鑰，共同創建 Green Address 比特幣地址。
3. 當交易發起時，使用者使用自己的私鑰簽署該筆交易。
4. 將該筆交易傳送到 Green Address 機構節點。
5. Green Address 機構節點收到後，檢查該筆交易是否存在雙重支付攻擊。
6. 確認無攻擊跡象後便廣播至比特幣網絡中。

Green Address 交易發起流程 說明完 Green Address 地址是如何創建之後，本節將詳細說明如何運用多重簽章地址發起交易至比特幣網絡中，如圖2.7所示。

1. 使用者使用原本創建 Green Address 的私鑰，並完成簽署交易。

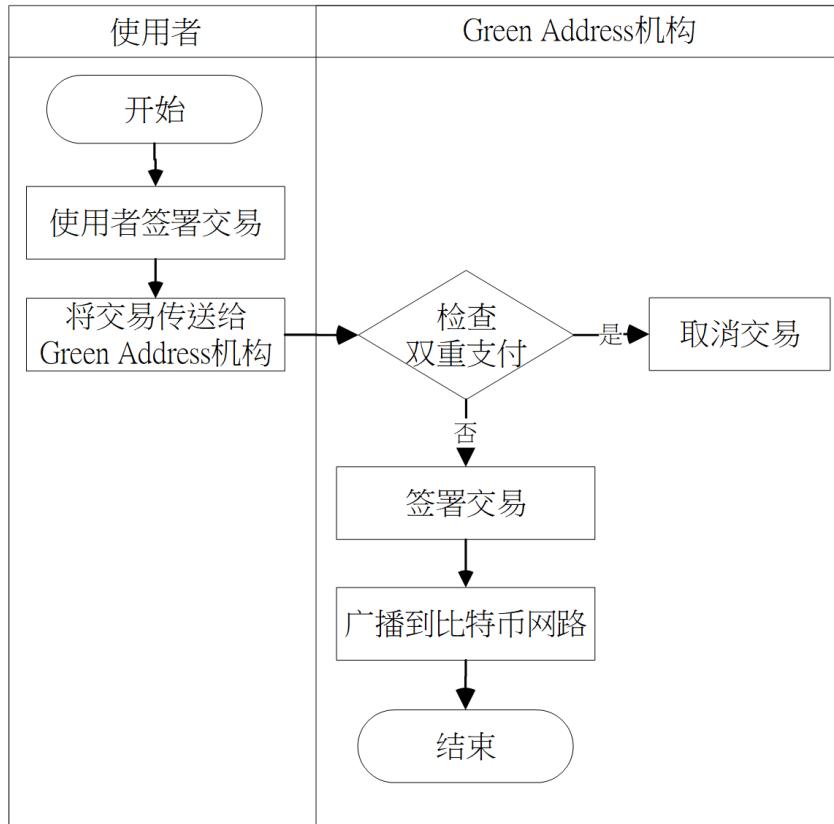


图 2.7 Green Address 交易发起流程圖

2. 因為是多重簽章地址，所以該交易需傳送至 Green Address 機構節點。
3. Green Address 機構節點收到交易信息後檢查該交易的發起地址是否存在雙重支付，倘若有雙重支付則遺棄；若無雙重支付則往下一個步驟。
4. Green Address 機構以 Green Address 的私鑰簽署該筆交易。
5. 將該筆交易封包廣播至比特幣網絡。

2.3 區塊鏈 (Blockchain)

自 2009 年以來，加密貨幣比特幣的誕生引發了新的貨幣革命浪潮，基於密碼學，點對點網絡，共識算法和區塊鏈技術，它們被結合成比特幣等加密貨幣。到目前為止，它在九年內發生大量的襲擊和欺詐事件後仍然在積極努力。比特幣一直是互聯網上最具代表性的加密貨幣，同時是區塊鏈技術最重要的應用之一，以下我們將描述區塊鏈技術的一些細節。

2.3.1 區塊頭 (Block Header)

比特幣區塊鏈可視為一種專門存儲交易信息的數據庫，該數據庫的結構嚴謹。區塊鏈之所以稱職為鍊是因為由許多區塊構成，區塊頭存在於區塊中記錄區塊中的重要信息共六項，分別為區塊版本、前區塊的哈希值、Merkle Root、難易度、時間戳以及Nonce，以下將逐一說明：

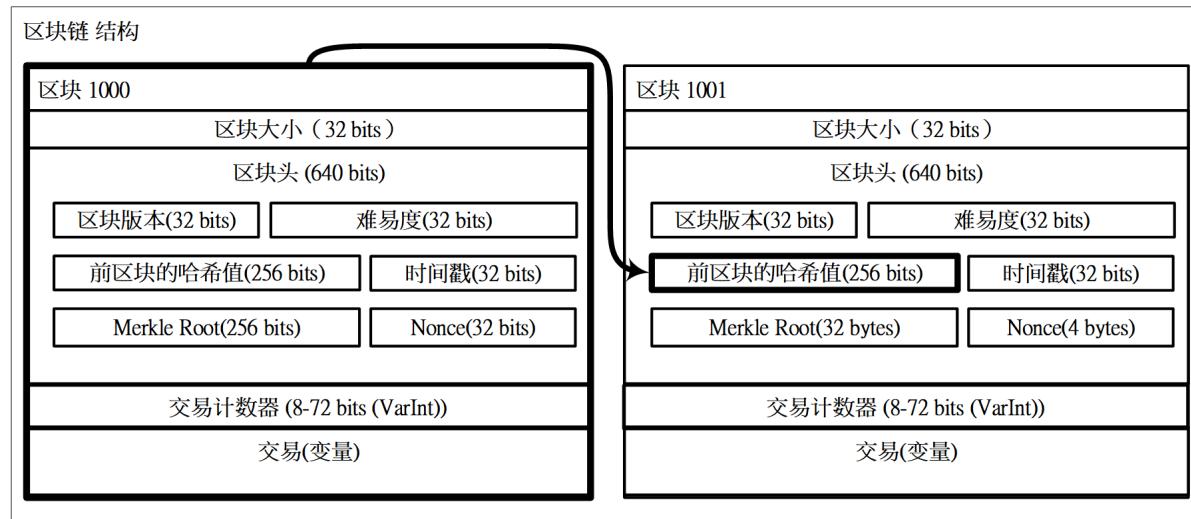


图 2.8 比特幣區塊鏈結構圖

1. 區塊版本 (32 bits)：該欄位存儲比特幣區塊鏈中的區塊版本。
2. 前區塊的哈希值 (256 bits)：記錄前一個區塊的哈希值。根據當前區塊的前一個區塊哈希值進而形成哈希指針，所有塊可以因為哈希指針連接在一起形成比特幣區塊鏈，不僅可以在區塊與區塊間建立虛擬鏈接，還可以使得區塊更難以被篡改。而通過新區塊不斷疊加在舊區塊過程，舊區塊的哈希值將繼續傳遞到最新的區塊。若區塊上面堆疊更多的區塊，促使的哈希值間接引用越多次，因此較早創建的區塊更難以修改。
3. Merkle Root (256 bits)：Merkle Root 的生成方法是將當前區塊的所有交易為 n 個進行排序後，Merkle Root 為 Merkle Tree 的樹根，交易為樹葉 n 個，將每個樹葉進行兩次 SHA-256 哈希算法取得哈希值得到 n 個哈希值，再將哈希值兩兩配對合併進行兩次 SHA-256，得到 $n * 2^{-1}$ 個哈希值後，在 k 輪後會使得 $n * 2^{-k} = 1$ 時，合併到只剩下一個哈希值，最後一個哈希值則為 Merkle Root，如圖所示2.9，圖中的 Hash() 函數為雙重 SHA-256，在區塊鏈中的 Merkle Root 可用於快速檢查當前區塊中所有存儲交易的正確性。
4. 難易度 (32 bits)：難易度參數主要調控比特幣挖礦過程中採用工作量證明算法的變量，孰得一提的是比特幣的難易度參數為動態調整。在過去的加密貨幣的設計

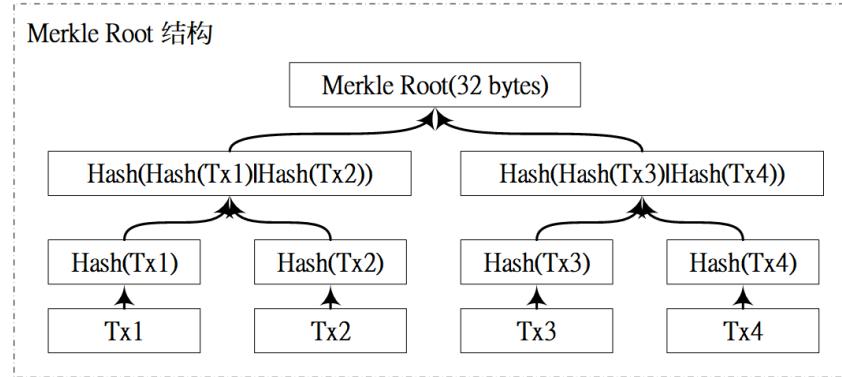


图 2.9 Merkle Tree 示意图

中，有著因為沒有動態修改區塊難度，而導致區塊鏈生成速度太快，甚至導致區塊鏈系統崩潰。

5. 時間戳 (32 bits)：以年、月、日、小時和秒的格式記錄區塊生成時間。
6. Nonce (32 bits)：Nonce 記錄著礦工在進行挖礦時，必須要不斷的嘗試 Nonce 參數，直到符合難易度參數，才可以創建一個全新的比特幣區塊。該值為 32 bits，意為著礦工嘗試的組態空間為 2^{32} 個可能性。

2.4 點對點網絡與加密貨幣安全

去中心化的加密貨幣系統給社會和傳統中心化的金融體系，以及政府帶來了很重大的衝擊，Satoshi Nakamoto 建構了一個不需要中央銀行發行貨幣的貨幣系統，在比特幣的貨幣發行上全靠區塊鏈既定的算法。除了貨幣發行，也將交易記錄的帳本以明文的方式存儲在去中心化的區塊鏈中，以比特幣為例，現今完整的比特幣區塊鏈帳本已經高達 180GB，這樣保存完整交易數據的計算機稱之為全節點，在比特幣去中心化的網絡中，如圖2.10所示，截至 2018 年 1 月 25 比特幣網絡中全節點數量為 10552 個^[53]，全節點的數量決定了比特幣帳本的可靠度，倘若有著更多的全節點，會使得比特幣網絡堅不可摧，更難去修改歷史發生過的交易數據。

GLOBAL BITCOIN NODES DISTRIBUTION
Reachable nodes as of Sat Feb 17 2018 15:52:54
GMT+0800 (CST).

11147 NODES

[24-hour charts »](#)

Top 10 countries with their respective number of reachable nodes are as follow.

| RANK | COUNTRY | NODES |
|------|--------------------|---------------|
| 1 | United States | 2909 (26.10%) |
| 2 | Germany | 2049 (18.38%) |
| 3 | China | 827 (7.42%) |
| 4 | France | 749 (6.72%) |
| 5 | Netherlands | 502 (4.50%) |
| 6 | Canada | 418 (3.75%) |
| 7 | Russian Federation | 376 (3.37%) |
| 8 | United Kingdom | 362 (3.25%) |
| 9 | n/a | 284 (2.55%) |
| 10 | Singapore | 224 (2.01%) |

[More \(103\) »](#)

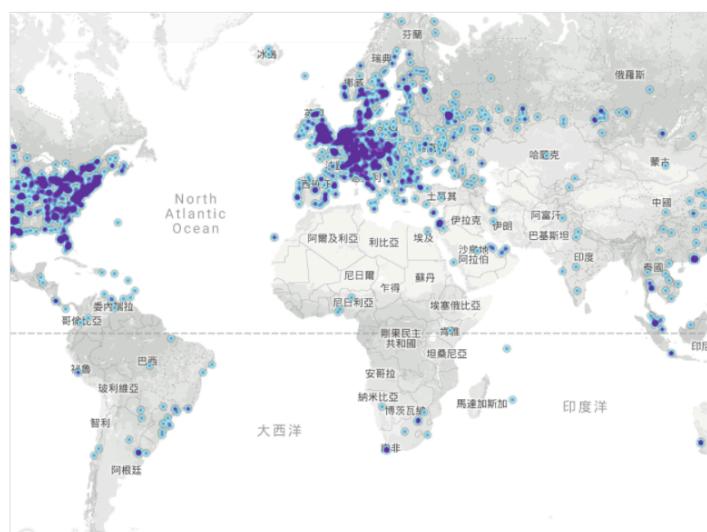


图 2.10 比特幣全節點分佈圖^[53]

第三章 系統需求分析

3.1 交易模型分析

在設計一個區塊鏈的實名交易監督系統之前，必須要針對不同的交易模型做探討。在區塊鏈的實名交易監督系統中，會以加密貨幣的觀點重新設計一個新的支付系統，重新深究匿名者與匿名者之間的交易模式、實名與實名之間的交易模式、匿名與實名之間的交易模式、實名客戶透過實名第三方再實名商家的交易模式以及實名客戶透過匿名第三方再實名商家的交易模式，這五種交易模式所代表著意義與時代革新帶來的技術變革。

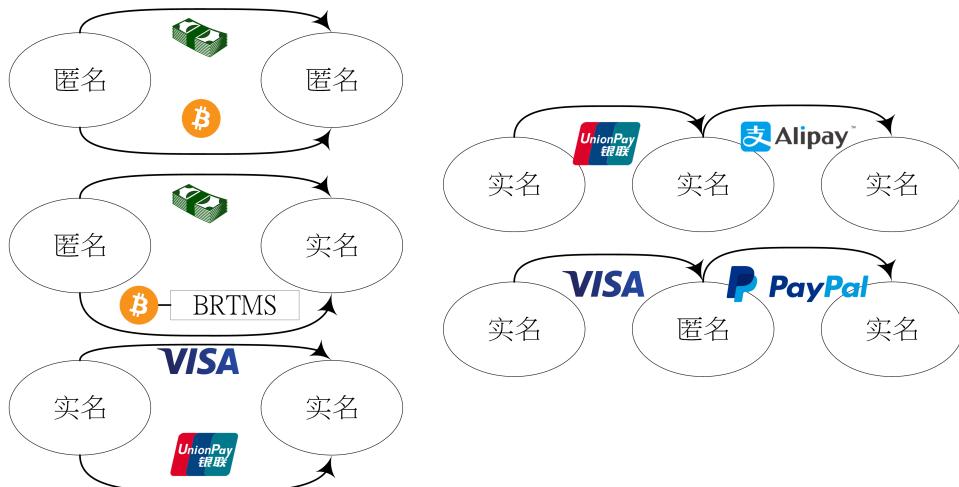


图 3.1 各種交易模型示意圖

3.1.1 現金交易模型

匿名客戶對匿名商家

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”。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信息安全，因為在貨幣的持有方式，並不需要登記姓名，資產轉移的過程中一概不需要。對於消費者而言，雖然消費者的匿名保護了自己的個人信息，但商家的交易信息也是匿名，對整個交易結果若有爭議，這便是追訴無門的結果。而在交易並

未被有效記錄的情況下，政府對稅收的計算，會進入無法計算的灰色地帶。圖3.2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。

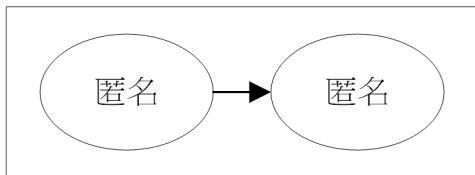


图 3.2 匿名對匿名交易示意圖

匿名客戶對實名商家

在另一個場景中，在交易進行的過程中，消費者為匿名，商家為實名，對消費者而言因為自己本身並無綁定個人信息，故對個人信息有很大的保障，消費者消費物件的店傢具有實名而開立收據，對消費者而言會得到消費記錄的保障，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。圖3.3為匿名消費者使用現金對已經實名制或是開立收據的商家之消費模型。

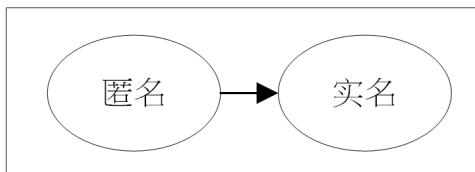


图 3.3 匿名對實名交易示意圖

3.1.2 電子貨幣交易模型

實名客戶支付實名商家

在現在最為常見的塑膠貨幣支付管道 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通過銀行進行帳戶與帳戶之間的資金轉移，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信息。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。圖3.4為透過實名制支付管道對商家進行交易的模型。

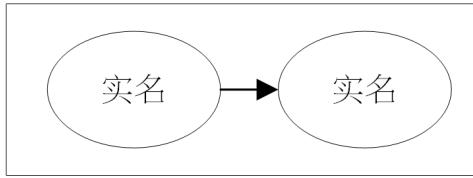


图 3.4 實名對實名交易示意圖

實名客戶透過實名第三方再實名商家

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，將所有中國在地銀行卡統合在一起，透過結合所有品牌的銀行卡以達有效提升卡片交易的方便性與使用率，圖3.5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。

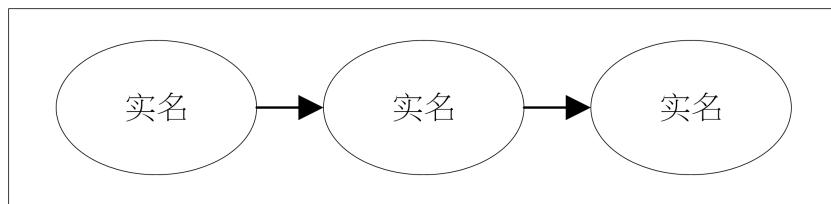


图 3.5 實名對實名再對實名交易示意圖

實名客戶透過匿名第三方再實名商家

為減低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信息的問題，PayPal 便致力於將消費者銀行卡的相關個人信息存儲在 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，也讓這樣的交易模式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，消費者的信任需要寄附在 PayPal 身上，畢竟大部分的銀行卡與個人信息皆存儲在 PayPal 公司內，PayPal 公司的信息安全將成為最重要的議題。圖3.6為先以實名制的支付管道將資金轉移到代支付的 PayPal 公司，PayPal 代為支付的過程中將原資金來源的個人相關信息保護在 PayPal 公司中，以製造出一種匿名支付方法保護消費者的個人信息之模型。

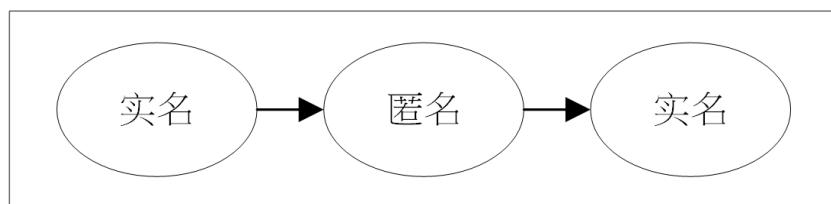


图 3.6 實名對匿名再對實名交易示意圖

3.1.3 交易關係比較

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，如表3.1。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 3.1 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 |
| 加密貨幣 | 匿名 | 無 | 匿名/實名 | 匿名/實名 |

3.2 特性要因分析

透過特性要因分析可以將区块链的实名交易监督系统大致分為四個主題，如圖3.7所示，分別為信息安全技術、加密貨幣錢包、近場通訊技術以及數據庫。針對四項主軸，最為一個金流系統，信息安全是不可或缺的環節，著重於商家認證機制、用戶權力控管、身份識別管理、使用者訪問控制四個方向；本系統致力於奠定匿名對實名的加密貨幣系統，必須對區塊鏈技術、公鑰私鑰生成算法、點對點交易技術、錢包地址產出以及貨幣發行技術五個方向進行探討；在交易場影中，本系統採用近場通信技術，因此需要對商品 RFID 標籤建置、讀取商品 RFID 標籤以及 Android Beam 傳輸商品交易進行基礎的 API 調研；為了使的加密貨幣實名制的實現，數據庫必須存儲與政府和商家相關的信息。此時數據庫加密、個資去識別化安全以及數據庫連接便相當重要。

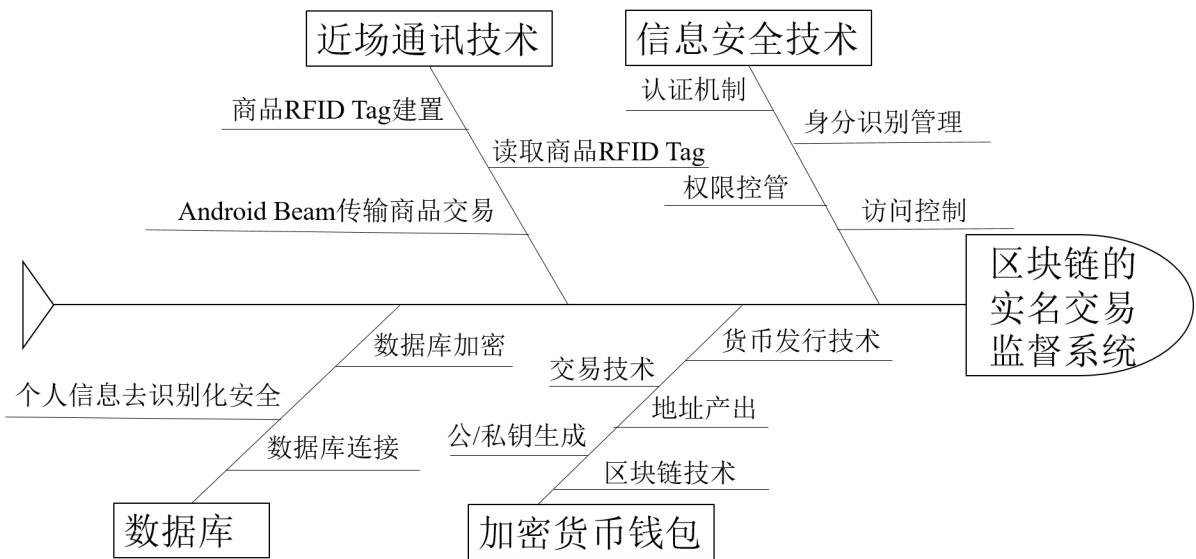


图 3.7 魚骨圖 (1)

第四章 系统设计

4.1 区块链的实名交易监督系统设计

本论文提出区块链的实名交易监督系统（Blockchain Real-name Transaction Monitoring System, BRTMS），以下简称 BRTMS，BRTMS 以加密货币比特币实作，BRTMS 包含三个子系统，商店和商品信息管理子系统（Store and Merchandise Information Management Sub-System, SMIMSS）、商家移动设备收款及交易子系统（Store Mobile payment Collection and Transaction Sub-System, SMCTSS）、客户端移动支付和交易子系统（Client Mobile Payment and Transaction Sub-System, CMPTSS），我们将在稍后描述这些子系统。

本论文将开发让商家能够结合商品与 RFID 标签，以达到快速建构与管理商品数据库之系统，并且让商家及顾客可以运用手机 NFC 功能来实际运作比特币的行动支付流程。店家只需要扫描商品上的 RFID 标签，即可快速创建交易清单，再利用 NFC 功能与顾客之行动设备进行消息交换，轻松地将商家的收款地址以及交易数据发送给顾客，收到数据后便能快速地以顾客之比特币行动电子钱包付款，并将交易细项保存下来，以便未来商家与顾客能够快速查找比特币行动支付的交易纪录。本系统主要是以完成区块链之数字加密货币的收款监督系统为主要目标，本论文进而将积极利用自由软件的利基：使用成本低、进入门槛低、开放源代码、社区能力强、共通性及移植性强、资通安全性高等优势来开发本论文收款监督系统的应用服务平台。本系统范围包含建置下面主系统与各项子系统如下：

1. 区块链的实名交易监督系统 (Blockchain Real-name Transaction Monitoring System, BRTMS)
2. 商家端建置与管理商品信息子系统 (Store and Merchandise Information Management Sub-System, SMIMSS): 本系统可以让商家在进货时，快速地将 RFID 标签之识别码与进货商品信息集成在一起，并且透过本系统添加、修改或删除数据库内部的信息，包括产品名称、详细信息，存货数量等信息，商家与顾客便可依照该数据库取得当前商品信息与状态。不仅让商店的存货信息更加清楚明了，也可以提供顾客更多的即时服务。
3. 商家端行动收银与交易明细系统 (Store Mobile payment Collection and Transaction Sub-System, SMCTSS): 本系统使商家在结帐时，能够以手机 NFC 功能扫描商品上的 RFID 标签，即可简单地创建交易清单，并透过 NFC 与顾客手机碰触，将交易清单以及商家之比特币收款地址等等重要交易信息一并传递给顾客，可以简短

结帐的速度，使结帐效率大幅提升。

4. 顾客端行动支付与交易明细系统(Client Mobile Payment and Transaction Sub-System, CMPTSS): 顾客在结帐时，不必再麻烦的拿出信用卡或是零钱包，只需要拿出手机让店员以 NFC 将交易清单与比特币地址转送给自己，即可自动链接至比特币电子钱包的应用程序当中，并且自动填妥相关数据，如: 交易金额、收款地址等等与此同时也能将交易纪录保存于客户端，以便日后顾客快速取得过往的交易纪录，除此之外亦可让广大的民众体验数字加密货币与行动支付带来的便利生活。

4.1.1 BRTMS 数据库设计

区块链的实名交易监督系统应用了六个信息表，分别为商家信息、产品信息、交易信息、用户信息、职工信息以及商家产品信息，以下将逐一说明：

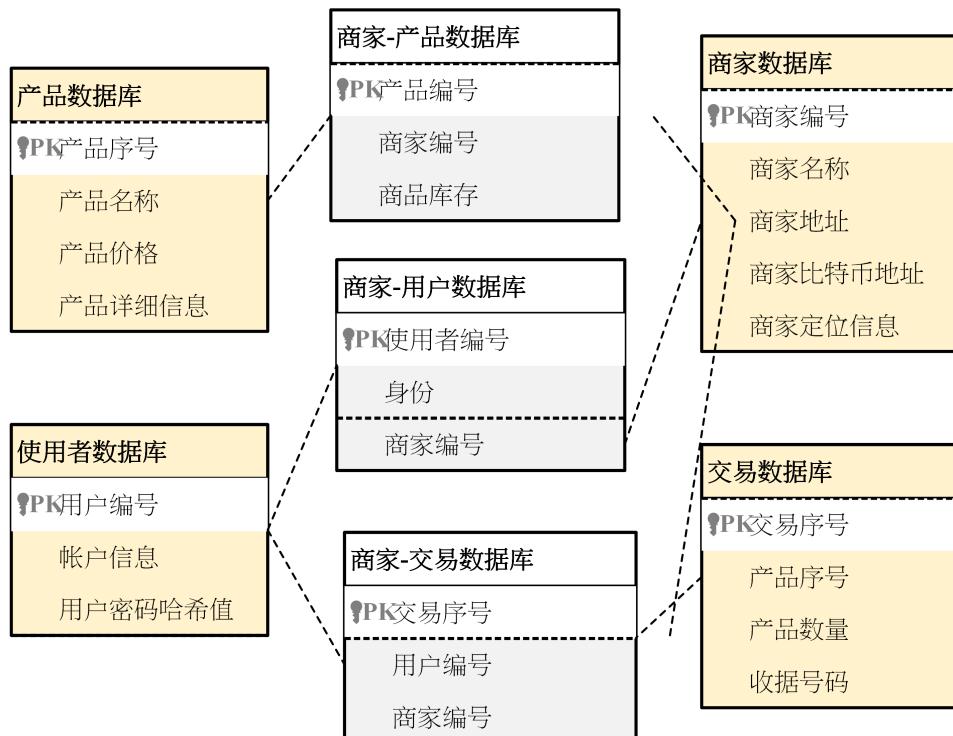


图 4.1 BRTMS 数据库分布图

1. 商家信息表：存储正在审核中的企业信息或已经过审核的企业信息。表4.1存储的信息包括商家编号、商家名称、商家地址、商家比特币地址以及商家定位信息。
2. 产品信息表：只有授权用户才能登录添加或修改交易产品信息。表4.2产品信息表内容包括产品编号、产品名称、产品价格以及产品描述信息。
3. 交易信息表：表4.3记录包括交易编号、职工编号、商家编号、商家产品编号、商家地址、商家产品数量、交易金额、顾客比特币地址和最后确认字段的值。

表 4.1 商家信息表

| 序号 | 字段名 | 字段说明 | 类型 | 是否为空 | 主外键 |
|----|-------------------|---------|---------------|------|-----|
| 1 | STORE_ID | 商家编号 | int | 否 | PK |
| 2 | STORE_NAME | 商家名称 | navarchar(20) | 否 | |
| 3 | STORE_ADDRESS | 商家地址 | navarchar(50) | 否 | |
| 4 | STORE_BTCAADDRESS | 商家比特币地址 | navarchar(50) | 否 | |
| 5 | STORE_GPS | 商家定位信息 | navarchar(30) | 否 | |

表 4.2 产品信息表

| 序号 | 字段名 | 字段说明 | 类型 | 是否为空 | 主外键 |
|----|---------------------|------|---------------|------|-----|
| 1 | PRODUCT_ID | 产品编号 | int | 否 | PK |
| 2 | PRODUCT_NAME | 产品名称 | navarchar(10) | 否 | |
| 3 | PRODUCT_PRICE | 产品价格 | float | 否 | |
| 4 | PRODUCT_DESCRIPTION | 产品描述 | navarchar(50) | 是 | |

表 4.3 交易信息表

| 序号 | 字段名 | 字段说明 | 类型 | 是否为空 | 主外键 |
|----|-----------------------|---------|---------------|------|-----|
| 1 | TX_ID | 交易编号 | int | 否 | PK |
| 2 | STAFF_ID | 职工编号 | int | 否 | FK |
| 3 | STORE_ID | 商家编号 | int | 否 | FK |
| 4 | STOREPRODUCT_ID | 商家产品编号 | int | 否 | FK |
| 5 | STORE_ADDRESS | 商家地址 | navarchar(50) | 否 | FK |
| 6 | STOREPRODUCT_QUANTITY | 商家产品数量 | int | 否 | |
| 7 | TX_AMOUNT | 交易金额 | float | 否 | |
| 8 | CONSUMER_BTCAADDRESS | 顾客比特币地址 | navarchar(50) | 否 | |
| 9 | CHEK | 校验值 | int | 否 | |

4. 用户信息表：表4.4存储所有用户信息，包括政府、商家及顾客之个人的帐户编号与帐号，而用户密码则以哈希值的方式保存以增加用户安全性。

表 4.4 用户信息表

| 序号 | 字段名 | 字段说明 | 类型 | 是否为空 | 主外键 |
|----|-------------------|---------|--------------|------|-----|
| 1 | USER_ID | 用户编号 | int | 否 | PK |
| 2 | USER_ACCOUNT | 用户帐号 | nvarchar(30) | 否 | |
| 3 | USER_PASSWORDHASH | 用户密码哈希值 | nvarchar(30) | 否 | |

5. 职工信息表：表4.5信息表存储各个商家拥有的职工信息，包括各职工编号、用户编号商家编号及职工身份。

表 4.5 职工信息表

| 序号 | 字段名 | 字段说明 | 类型 | 是否为空 | 主外键 |
|----|--------------|------|--------------|------|-----|
| 1 | STAFF_ID | 职工编号 | int | 否 | PK |
| 2 | USER_ID | 用户编号 | int | 否 | FK |
| 3 | STORE_ID | 商家编号 | int | 否 | FK |
| 4 | STAFF_STATUS | 职工身份 | nvarchar(20) | 否 | |

6. 商家产品信息表：表4.6存储各家商家当前商家产品存货信息，由商家产品编号、产品编号、商家编号及商家产品库存量所组成。

表 4.6 商家产品信息表

| 序号 | 字段名 | 字段说明 | 类型 | 是否为空 | 主外键 |
|----|------------------------|---------|-----|------|-----|
| 1 | STOREPRODUCT_ID | 商家产品编号 | int | 否 | PK |
| 2 | PRODUCT_ID | 产品编号 | int | 否 | FK |
| 3 | STORE_ID | 商家编号 | int | 否 | FK |
| 4 | STOREPRODUCT_INVENTORY | 商家产品库存量 | int | 否 | |

4.1.2 商店和商品信息管理子系统 (SMIMSS)

图4.2为区块链的实名交易监督系统架构，商家需要在以下 4 个步骤中对商店和商品信息管理子系统 (SMIMSS) 进行注册：

1. 商户必须在 BRTMS 注册一个帐户，并附有政府法规的商业证明。
2. 区块链的实名交易监督系统将自动向相应的政府金融监管机构提交商业申请，以审查该商店的加密货币交易业务。
3. 如果政府批准商店的加密货币业务申请，服务器将激活商家在该收集监控系统中创建商店帐户。

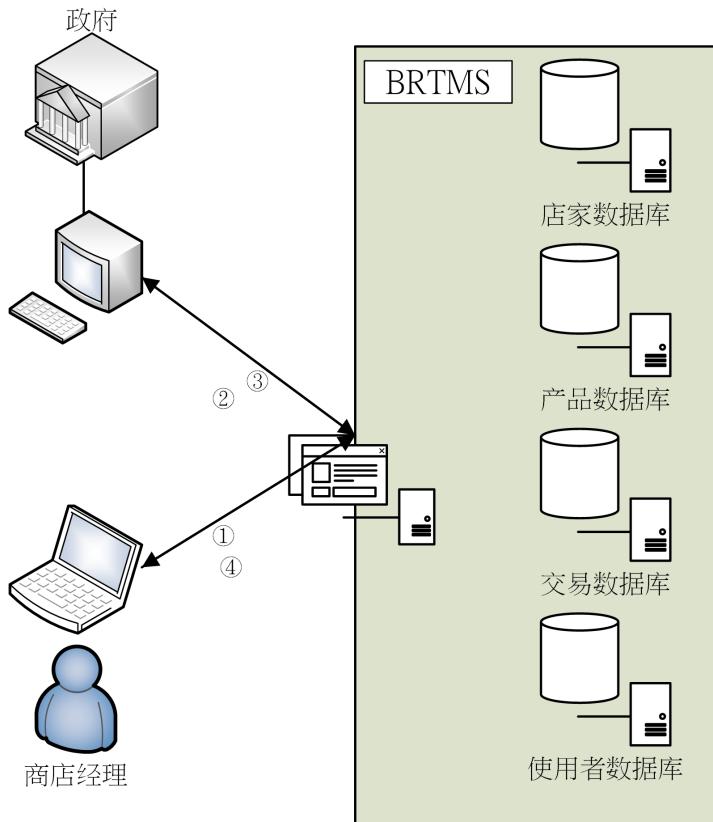


图 4.2 BRTMS 和商家注册流程的核心架构图

4. 商家可以自由地登录账户并添加商家想要出售的产品，并检查他们的加密货币交易数据，例如产品库存和产品交易记录。

4.1.3 BRTMS 架构与运作流程

具体的加密货币商家收银金流监控系统运行过程如图4.3所示，我们以图4.2所设计出的系统架构进行扩增，首先我们需要与区块链查看器 (blockchain explorer) 对接，而之所以该监控系统需要与区块链查看器对接是为了能够最直接的比对交易被记录的成交状况，能够达到即时性以及正确性，倘若担忧单方面的依赖相信区块链查看器的成果，亦可以使用多家区块链查看器进行交叉参考，以避免因为一家公司的错误所带来的影响。区块链查看器的目的是为了能够快速地准确地比对该笔交易的成交，做为整笔交易提出到结算的环节之一。

图4.3区块链的实名交易监督系统创建步骤描述如下：

1. 商家的店员将登录到如图4.2所示的先前步骤创建的帐户，以使用手持式平板电脑或智能手机访问 SMCTSS 中的服务。如前所述，在能够登录到系统之前，商家帐户必须由政府机构审计。
2. 在成功登录 SMCTSS 用于商户加密货币流量监控系统时，移动设备将加载通过

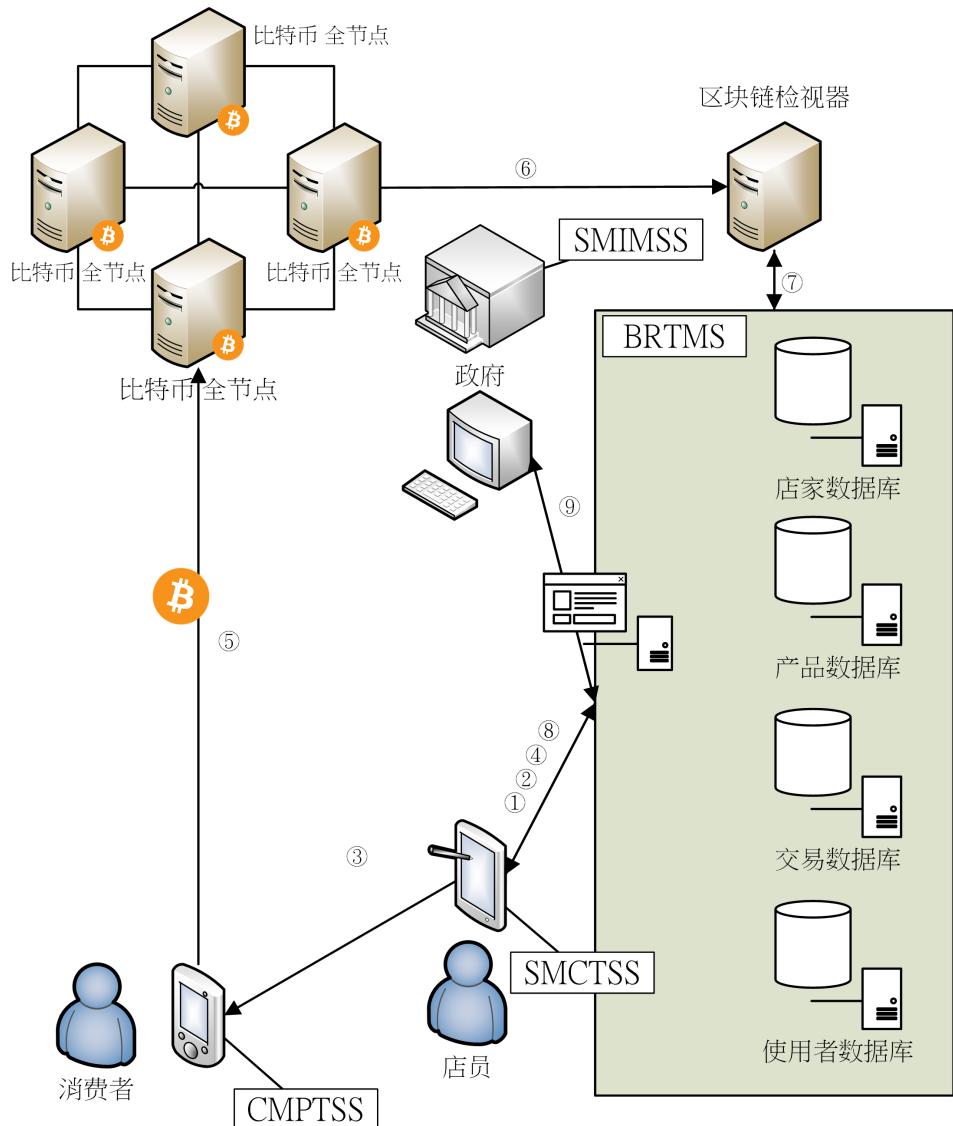


图 4.3 BRTMS 的整体架构与功能示意图

SMIMSS 注册的商店产品信息，然后创建产品目录。商店的店员可以根据客户的需求选择所需的产品和数量。

3. 店员使用设备完成客户选定商品的产品信息后，移动设备上的 NFC 技术可用于将产品信息从附近店员的移动设备传递给消费者的移动设备，而无需物理交互。然后，消费者可以很容易地将自己的消费信息记录成为发票等参考。在接收从商家店员设备向顾客设备购买产品消息的同时，顾客设备还将向商家的移动设备发送其自己的比特币支付地址的消息。
4. 商家的手持设备收到客户确认购买所选产品的相应信息后，会将交易信息的副本发送给 SMIMSS 监控系统。消费者信息包括交易串行号、商户 ID 号码、商品号码、购买的商品的数量以及加密货币的收款人地址以及消费者的支付地址。
5. 收到消费者交易信息后，即完成此次的加密货币支付。同时，此次交易的加密货币将发布到比特币网络中进行验证和记录。
6. 区块链浏览器将开始分析在比特币网络中缓存池的所有交易以及区块链中记录的交易。
7. 拟议的交易监控系统 BRTMS 将向区块链查看器提出请求。这个请求数据不仅包括存储在 BRTMS 中的交易副本之加密货币收款人地址（如图4.2的第 4 步所述），还包括客户预期付款的加密货币支付地址。区块链浏览器使用请求数据来检查交易是否存储在区块链中，或者交易还在等待确认。如果交易已被确认并存储在区块链中，则交易数据库中“交易确认”字段的值将更改为“1”，否则其默认值为“0”。
8. 当“交易确认”字段中的值为“1”时，“交易已完成”消息可发送至商店平板电脑上运行的商店和商品信息管理子系统（SMCTSS）。
9. 政府财政监督部门可以审查拟议 BRTMS 中的所有交易信息，以作为税收审计参考。

4.2 以多重签章优化区块链的实名交易监督系统之设计

在这样的机制下，虽然 Green Address 没有减少交易确认时间，但是只要是用 Green Address 即可确保双重支付攻击是不会发生的，对商家或是收款人而言，可以得到在即时交易中不被双重支付攻击的保障，提升未进入区块链的交易可信度，进而创造出即时交易的可行性。

本节将详述本系统之商家注册、Green Address 钱包创建与验证交易的运作流程与相关数据库架构，如图4.4所示。

1. 商家以通过政府机构的审查审核的帐户登录该系统。
2. 系统加载该店家注册的商品信息，店员可以依照客户的需求进行点单选取数量。

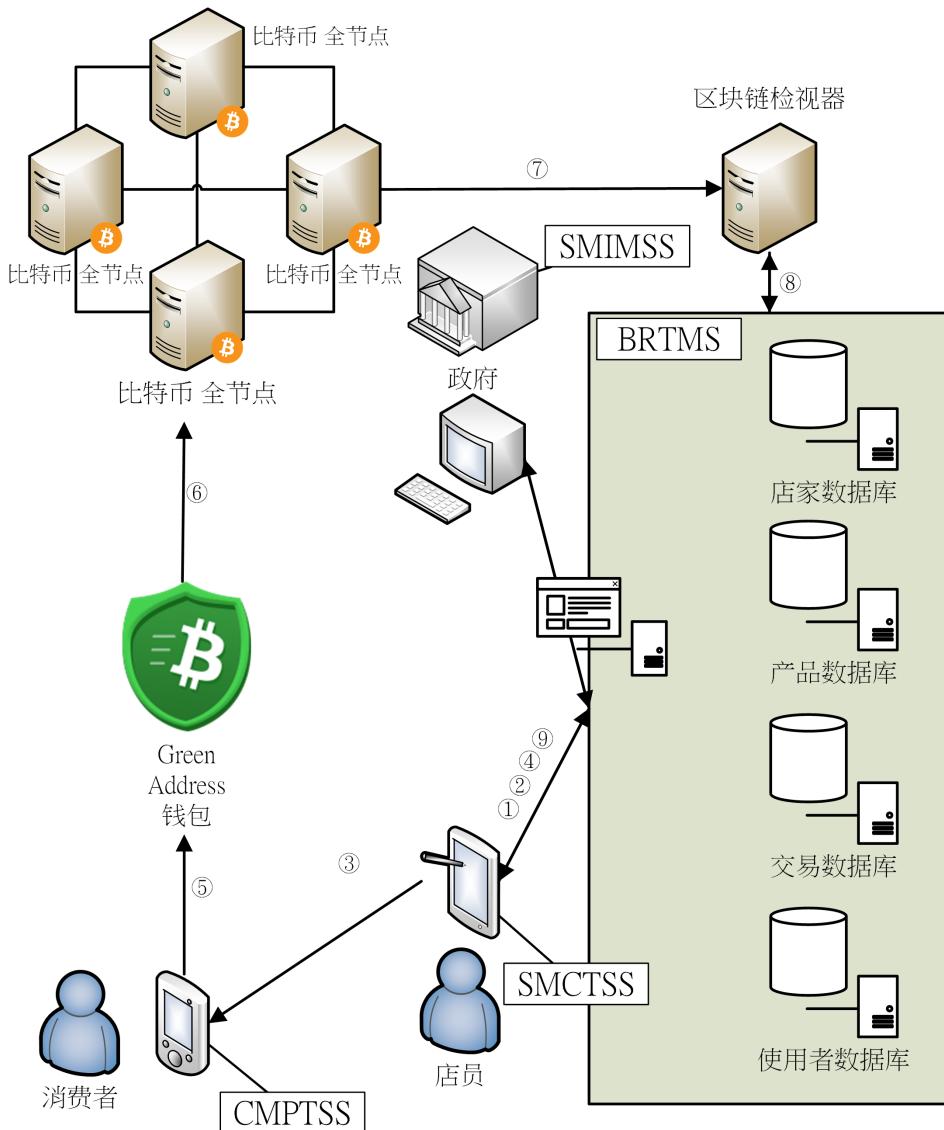


图 4.4 多重签章优化后的 BRTMS 整体示意图

3. 快速创建交易清单，并透过 Green Address 创建一个全新的比特币收款地址，再以 Android Beam 的方式将交易信息轻松地传达给消费者。
4. 在商家店员的平板电脑收到这笔交易信息之后，会对本监督系统重送一个副本进行存盘。该交易信息包括由监督系统所提出的交易流水号、商家编号等信息。
5. 消费者收到交易信息后，手机会自动开启 Green Address 的付款页面，确认金额无误之后便能进行支付，此时便会以客户的比特币私钥签署交易，并等待 Green Address 机构节点的认证及发布。
6. Green Address 机构节点收到交易请求，并完成验证非双重支付攻击后，以代理节点对应地址的私钥签署本次交易，并广播至比特币节点中。
7. 区块链查看器便会开始分析网络中所有存在缓存池中的交易，以及已经被记录到区块链中的交易。
8. 本交易监督系统会向区块链查看器查找，检查该笔交易是否已经存在于缓存池当中，若已经确认进入缓存池，则认定该笔交易成立并完成付款。
9. 在交易确认之后，便向商家店员的平板电脑送出交易已经成交的信息，此时完成交易，于此同时也将该笔交易信息建置于系统数据库内。

第五章 系統實現

為了驗證和證明所提議的 BRTMS 用於比特幣支付收款監督的可行性和有效性，我們將其運行在用於商家商品管理和維護的 Java 應用程序的 SMIMSS 子系統，用於商家職員的運行在 Android App 上的 SMCTSS 以及運行在 App 上的用於客戶的 CMPTSS。如圖5.1所示，SMIMSS Java 應用程序可以幫助商家登錄到系統或創建一個新帳戶。授權商戶成功登錄系統後，商家可以插入或更新產品列表，如圖5.2所示。實施的 SMIMSS Java 應用程序執行前面部分中所述的功能。

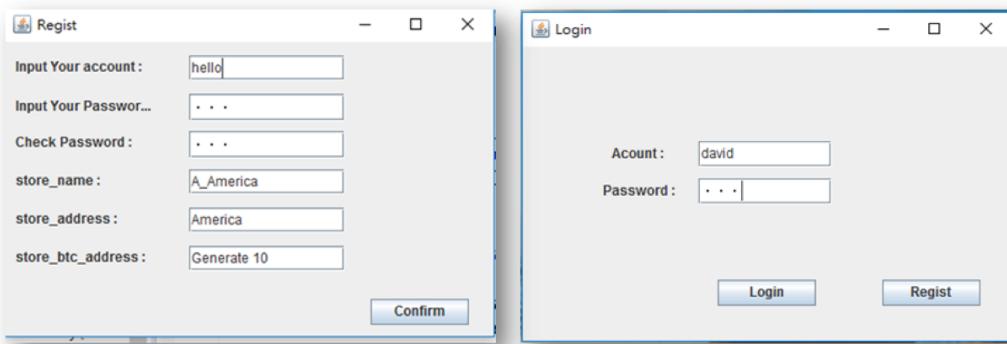


图 5.1 SMIMSS 的 Java 應用程序的註冊和登錄界面

| name | detail | quantity |
|----------|--------|----------|
| iphone 5 | white | 20 |
| iphone 5 | black | 10 |
| iphone 6 | white | 15 |
| iphone 6 | black | 23 |
| iphone 7 | white | 25 |
| iphone 7 | black | 0 |
| i8 | red | 0 |
| i8 | blue | 0 |
| i9 | oramge | 0 |

图 5.2 在 SMIMSS 中插入或更新授權商家的產品目錄

商戶的產品信息可以通過 RFID 標籤掃描，存儲到雲端數據庫中，商戶店員可以使用我們實現的 SMCTSS Android 客戶端，啟用 NFC 監聽器，從購物車中的客戶購買

產品中讀取 RFID 標籤信息。在如圖5.3所示的第一項活動中，商家職員必須登錄才能獲得授權訪問 SMCTSS 功能。然後，在第二項活動中，SMCTSS 應用程序可以通過使用 SMIMSS 中應用的雲數據庫檢查產品 RFID 標籤信息並將其展示給客戶，從而將掃描的產品列入購物車。在圖5.3的第三項活動中，顧客可以要求店員取消購買物品以確認最終購買。最後，SMCTSS 應用程序將自動使用比特幣測試網絡（Bitcoin Testnet）^[54]幫助店員確認發布此加密貨幣交易的收款人地址，如圖5.3所示。

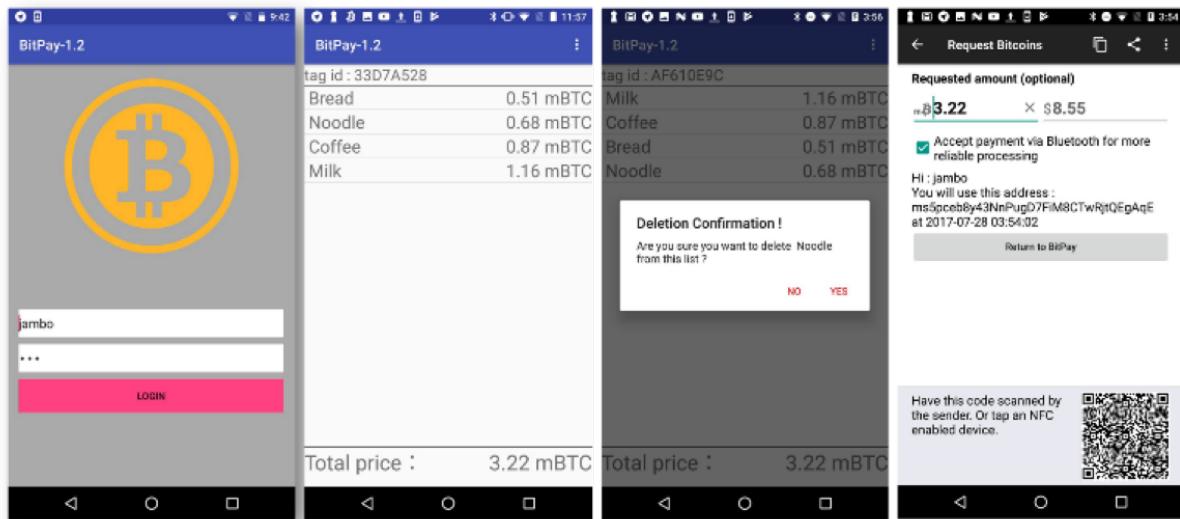


图 5.3 登錄、等待結帳的商品、刪除商品及支付確認

同時，客戶將使用與 SMCTSS App 相對應的 CMPTSS Android App 通過比特幣加密貨幣完成採購產品交易。如圖5.4所示，第一個活動表示顧客確認購買產品創建交易數據庫的交易清單，第二個活動顯示包括金額和付款人比特幣地址在內的付款確認，第三個活動顯示交易歷史記錄的交易作為買方甚至是賣方，最後在第四項活動中顯示了該筆交易詳細採購產品的發票。

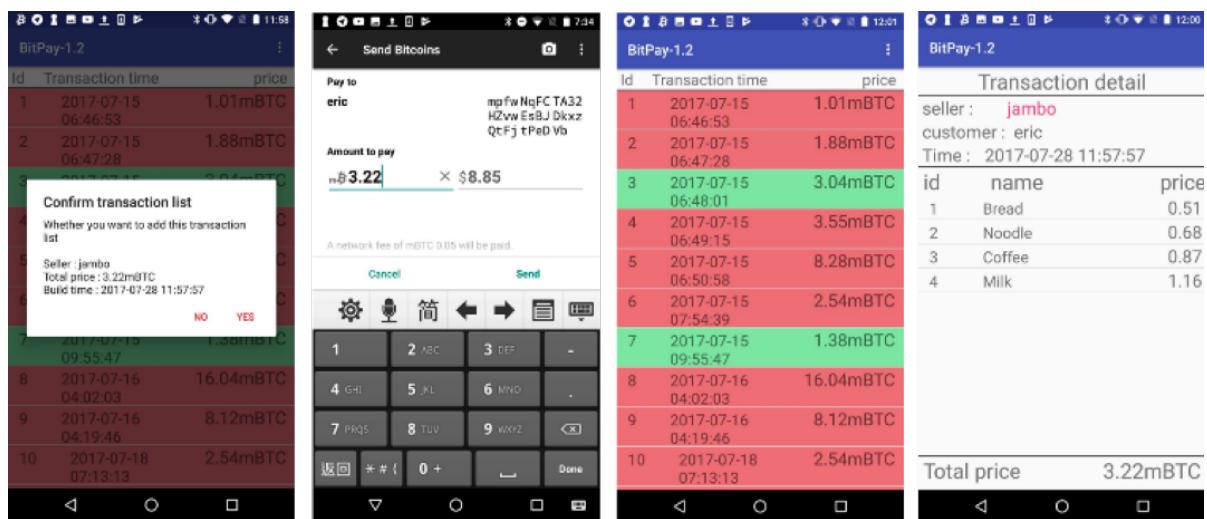


图 5.4 在 CMPTSS App 中，交易確認，付款確認、交易歷史記錄和發票

第六章 系统测试

于本章将进行功能测试与性能测试，运行功能测试已确认本文所提出之系统的所有功能是否皆顺利运行，透过性能测试可知本系统的交易速度在优化前与优化后之间的差异。

6.1 功能测试

本段主要是描述区块链的实名交易监督系统的测试计划。确认在系统集成前，必须先确认所有的设计组件均可正确的输出，在此我们着重于集成系统测试 (Integration Test) 及验收测试 (Acceptance Test)。本章节内容将依据系统需求规格书与系统设计，描述关于集成测试的相关计划与内容。并希望透过此章节之描述与实践，达到顺利进行测试工作之目的。

1. 接受标准：本测试计划需要满足下列的测试接受准则：
 - (a) 本系统需要对所有列为必要 (Critical、Important、Desirable) 之需求作完整测试。
 - (b) 测试进程需要依照本测试计划所订定的进程进行，所有测试结果需要能符合预期测试结果方能接受。
 - (c) 以测试案例为单位，当测试未通过时，需要进行该单元的测试，其接受的准则与前一项规定相同。
2. 测试环境说明包括所采用的硬件与软件规格，分别如下：
 - (a) 硬件规格分为系统主机以及周边设备：
 - i. 系统主机：一台以上主机，每台主机 CPU 为 Intel P4 1.0GHz 或以上，256 MB RAM 或以上，60G 以上硬盘空间。
 - ii. 周边设备：一台以上智能型手机，与用来代表虚拟商品的数个 RFID 标签；已可供测试 NFC 用的智能型手机包含小米 3 WCDMA 版，详细规格于表6.1，Google Nexus 5X，详细规格于表6.2。
 - (b) 软件规格：关于测试环境所需的软件规格說明，如下列所示：操作系统：Window 10、Android 6.0.1/7.1.1
3. 测试地点：在铭传大学桃园校区资工系实验室，透过 Android 手机进行的交易仿真实验，测试环境如图4.3的示意。
4. 测试时间：

表 6.1 小米 3 手机规格

| | |
|------|--|
| 系统频率 | GSM 四频、WCDMA |
| 操作系统 | Android 4.3 |
| 处理器 | Qualcomm Snapdragon 800 2.3 GHz 四核心 |
| 内存 | 2GB RAM、16GB ROM |
| 记忆卡 | 不支持 |
| 显示屏幕 | 5 吋 1670 万色 IPS(1920×1080 pixels)、441ppi |
| 相机 | 1300 万像素 (F2.2、28mm)、200 万副镜头、1080p |
| 电池 | 3050 mAh(不可换) |
| 尺寸 | 144x73.6x8.1mm |
| 重量 | 145g |

表 6.2 Google Nexus 5X 手机规格

| | |
|------|--|
| 系统频率 | GSM 四频、WCDMA |
| 操作系统 | Android 6.0 |
| 处理器 | Qualcomm Snapdragon 800 1.8 GHz 六核 |
| 内存 | 2GB RAM、16GB ROM |
| 记忆卡 | 不支持 |
| 显示屏幕 | 5 吋 1670 万色 IPS(1920×1080 pixels)、441ppi |
| 相机 | 1300 万像素 (F2.2、28mm)、200 万副镜头、1080p |
| 电池 | 2,700 mAh(不可换) |
| 尺寸 | 147x72.6x7.9mm |
| 重量 | 136g |

- (a) 各子系统之内部组件集成测试 (Module Test)(2017/2/25 2017/6/8)
- (b) 区块链的实名交易监督系统集成测试 (Integration Test) (2017/6/8 2017/6/21)
- (c) 区块链的实名交易监督系统接受度测试 (Acceptance Test) (2017/7/10 2017/7/21)

5. 查核点：

- (a) 各子系统之内部组件集成测试 (2017/5/10)
- (b) 区块链的实名交易监督系统集成测试 (2017/7/1)
- (c) 区块链的实名交易监督系统接受度测试 (2017/7/1)

6. 集成测试规划 (Integration Testing) :

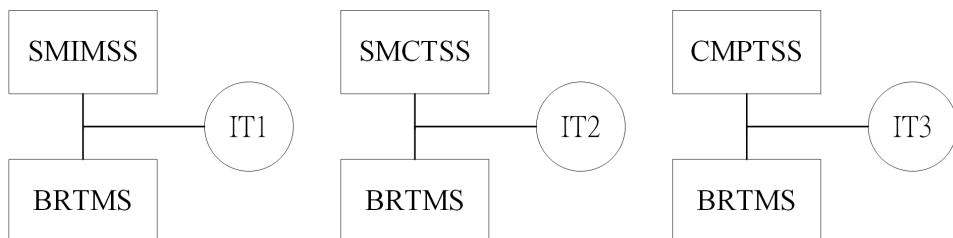


图 6.1 集成子系统测试

7. 验收测试规划 (Acceptance Testing, AT)：本系统须达成以下三组接受用例陈列的所有功能，测试本论文搭设计与搭建的系统功能是否能够顺利运行。测试的角色有两个，分别为管理员以及用户，如图6.2为 BRTMS 用例示意图，预计测试服务器的组态设置、手机的组态设置以及数据库的组态设置：

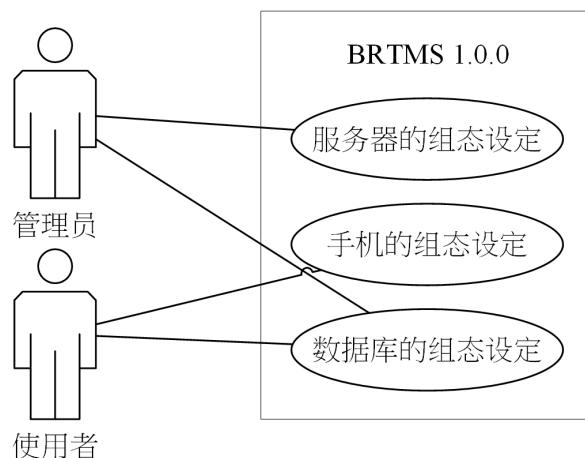


图 6.2 BRTMS 用户用例图

图6.3为三组验收测试的示意图，对本区块链的实名交易监督系统进行测试。

6.1.1 测试用例

1. 集成测试 (Integration Test)

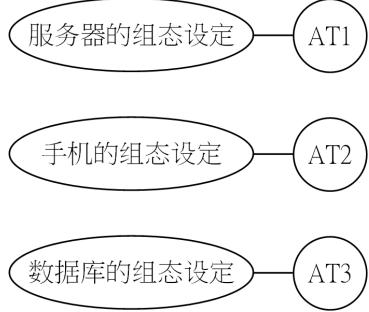


图 6.3 验收测试 (Acceptance Testing)

(a) IT1 测试用例：表6.3为 IT1 测试用例，测试对象为商家端建置与管理商品信息子系统。目的：验证 [SMIMSS 1.1.0] 子系统能否正确管理商品信息。

表 6.3 IT1 测试用例

| | |
|---------|---|
| 用例 ID | IT1 |
| 用例名称 | 集成 SMIMSS 至 BRTMS |
| 测试目标 | [SMIMSS 1.1.0]、[BRTMS 1.0.0] |
| 依赖关系 | SMIMSS-F-001~SMIMSS-F-005 |
| 严重程度 | 1(Critical) |
| 用例描述 | 1. 能够添加店家帐户 2. 能够添加/修改/删除店员帐户 3. 能够添加/删除/修改商品信息 4. 能够取得产品信息 5. 能够接收交易信息 |
| 预期结果 | 1. 成功添加店家帐户 2. 成功添加/修改/删除店员帐户 3. 成功添加/修改/删除商品信息 4. 成功取得产品信息 5. 成功接收交易信息 |
| Cleanup | 无 |

(b) IT2 测试用例：表6.4为 IT2 测试用例么目标，测试对象为商家端行动收银与交易明细系统。目的：验证 [SMCTSS 1.2.0] 子系统是否能够完成一笔行动支付之交易。

(c) IT3 测试用例：表6.5为 IT3 测试用例，目标检测对象为顾客端行动支付与交易明细系统。目的：验证 [CMPTSS1.3.0] 能正确接收 SMCTSS 所发送的交易数据，并以其交易信息运行以比特币付款之动作。可以查找商品信息，且能够保存并且查看用户过往之交易纪录。

2. 验收测试用例 (Acceptance Testing Cases) : 验收测试用例目的在于测试母系统 BRTMS、子系统 SMIMSS、SMCTSS 与 CMPTSS 是否能够顺利的进行信息传递

表 6.4 IT2 测试用例

| | |
|---------|--|
| 用例 ID | IT2 |
| 用例名称 | 集成 SMCTSS 至 BRTMS |
| 测试目标 | [SMCTSS1.2.0]、[BRTMS 1.0.0] |
| 依赖关系 | SMCTSS-F-001~ SMCTSS-F-007 |
| 严重程度 | 1(Critical) |
| 用例描述 | 1. 能够登录店员帐户 2. 能够扫描 NFC 标签 3. 能够读取商品信息 4. 能够创建交易清单 5. 能够发送交易信息 6. 能够认证交易信息 7. 能够保存交易明细 |
| 预期结果 | 1. 成功登录店员帐户 2. 成功扫描 NFC 标签 3. 成功读取商品信息 4. 成功创建交易清单 5. 成功发送交易信息 6. 成功认证交易信息 7. 成功保存交易明细 |
| Cleanup | 无 |

表 6.5 IT3 测试用例

| | |
|---------|---|
| 用例 ID | IT3 |
| 用例名称 | 集成 CMPTSS 至 BRTMS |
| 测试目标 | [CMPTSS.1.3.0]、[BRTMS 1.0.0] |
| 依赖关系 | CMPTSS-F-001~ CMPTSS-F-007 |
| 严重程度 | 1(Critical) |
| 用例描述 | 1. 能够登录客户帐号 2. 能够读取商品信息 3. 能够接收交易清单 4. 能够认证交易信息 5. 能够运行行动支付 6. 能够保存交易明细 7. 能够查看交易纪录 |
| 预期结果 | 1. 成功登录客户帐号 2. 成功读取商品信息 3. 成功接收交易清单 4. 成功认证交易信息 5. 成功运行行动支付 6. 成功保存交易纪录 7. 成功查看交易纪录 |
| Cleanup | 无 |

完成交互。

(a) AT1 测试用例: 表6.6所示, 目标测试管理人员是否能够顺利使用子系统SMIMSS 顺利与母系统BRTMS 教户。目的: 验证使用用例(Use case)1, 透过组态文件的修改对服务器进行组态设置。

表 6.6 AT1 测试用例

| | | |
|---------|---------------------------------|--------------------------|
| 用例 ID | AT1 | |
| 用例名称 | 服务器的组态设置 | |
| 测试目标 | [SMIMSS 1.1.0] [BRTMS 1.0.0] | |
| 依赖关系 | BRTMS-F-001 | |
| 严重程度 | 1 | |
| 用例描述 | 用户操作 | 系统响应 |
| | 1. 管理人员依照环境设置服务器组态。 | |
| | | 2. 服务器依照管理人员所做的组态设置启动服务。 |
| 预期结果 | 成功启动服务器的相关服务。 | |
| Cleanup | 无 | |

(b) AT2 测试用例: 如表6.7所示, 参与者为用户。目的: 验证用例(Use case)2 透过组态文件的修改对手机进行组态设置。

表 6.7 AT2 测试用例

| | | |
|---------|----------------------------------|-------------------------|
| 用例 ID | AT2 | |
| 用例名称 | 手机的组态设置 | |
| 测试目标 | [SMCTSS 1.2.0] [CMPTSS 1.3.0] | |
| 依赖关系 | BRTMS-F-002~ BRTMS-F-003 | |
| 严重程度 | 1 | |
| 用例描述 | 用户操作 | 系统响应 |
| | 1. 用户修改手机组态设置参数。 | |
| | | 2. 手机依照用户在设置档中所填入的数值运作。 |
| 预期结果 | 成功完成手机的组态设置 | |
| Cleanup | 无 | |

(c) AT3 测试用例: 如表6.8所示, 目的: 验证用例(Use case)3, 透过组态文件的修改对数据库进行组态设置。

表 6.8 AT3 测试用例

| | | |
|---------|--|--------------------------|
| 用例 ID | AT3 | |
| 用例名称 | 数据库的组态设置 | |
| 测试目标 | [SMIMSS 1.1.0] [SMCTSS 1.2.0] [CMPTSS 1.3.0] | |
| 依赖关系 | BRTMS-F-001~ BRTMS-F-003 | |
| 严重程度 | 1 | |
| 用例描述 | 用户操作 | 系统响应 |
| | 1. 管理者设置数据库组态。 | |
| | | 2. 数据库依照管理人员所做的组态设置启动服务。 |
| | 3. 用户修改数据库之数据及文件。 | |
| | | 4. 数据库依照用户所做的组态设置启动服务。 |
| 预期结果 | 成功设置完成数据库的相关设置。 | |
| Cleanup | 无 | |

6.1.2 测试结果和分析

1. 集成测试用例 (Integration Testing Cases) 表6.9为 IT 1、为 IT 2、为 IT 3 的集成子系统测试结果，皆顺利运作。
2. 验收测试用例 (Acceptance Testing Cases) 表6.10为前节所设计的三种 AT 1、AT 2 与 AT 3 的验收测试结果，皆顺利运行。
3. 可追踪性 (Traceability)
 - (a) 子系统与测试用例：表6.11为测试组 IT 1、IT 2、IT 3、AT 1、AT 2、AT 3 与子系统 SMIMSS、SMCTSS、CMPISS 的关系表。
 - (b) 需求与测试用例：表6.12为本系统需求与集成测试用例的关系表，表6.13为需求与验收测试案例的关系表。

6.2 性能测试

根据比特币点对点架构，尽管客户和商店之间的交易细节已经快速存储到云数据库，但官方确认交易与当前比特币区块链的交易通常需要更长的时间，因为需要确保确认的数量在交易广播比特币点对点网络并存储到缓存池后，是否存在双重支付。本文设计了区块链的实名交易监督系统以及引用多重签章算法重新设计的区块链的实名

表 6.9 集成子系统测试结果

| 测试用例 | 结果(通过/不通过) | Comment |
|------|------------|---|
| IT1 | 通过 | 1. 成功添加店家帐户 2. 成功添加/修改/删除店员帐户 3. 成功添加/修改/删除商品信息 4. 成功取得产品信息 5. 成功接收交易信息 |
| IT2 | 通过 | 1. 成功登录店员帐户 2. 成功扫描 NFC 标签 3. 成功读取商品信息 4. 成功创建交易清单 5. 成功发送交易信息 6. 成功认证交易信息 7. 成功保存交易明细 |
| IT3 | 通过 | 1. 成功登录客户帐号 2. 成功读取商品信息 3. 成功接收交易清单 4. 成功认证交易信息 5. 成功运行行动支付 6. 成功保存交易纪录 7. 成功查看交易纪录 |
| RATE | 90% | BRTMS 开发透过手机让商家及顾客以手机发送交易信息，如：商品名称、商品金额，商家收款地址。并且及时将商品信息更新至服务器之数据库，以便商家控管商品信息状态，同时让顾客可以享受数字加密货币的方便性。 |

表 6.10 验收测试结果

| 测试用例 | 结果(通过/不通过) | Comment |
|------|------------|---------------------------------------|
| AT1 | 通过 | 成功启动服务器的相关服务。 |
| AT2 | 通过 | 成功完成手机的组态设置。 |
| AT3 | 通过 | 成功设置完成数据库的相关设置。 |
| Rate | 100% | BRTMS 可透过组态设置的方式来设定各个子系统的环境参数。 |

表 6.11 子系统与测试用例关系表

| | SMIMSS 1.1.0 | SMCTSS 1.2.0 | CMPISS 1.3.0 |
|-----|--------------|--------------|--------------|
| IT1 | X | | |
| IT2 | | X | |
| IT3 | | | X |
| AT1 | X | | |
| AT2 | | X | X |
| AT3 | X | X | X |

表 6.12 需求与集成测试用例的关系表

| | IT1 | IT2 | IT3 |
|--------------|-----|-----|-----|
| BRTMS-F-001 | X | | |
| BRTMS-F-002 | | X | |
| BRTMS-F-003 | | | X |
| SMIMSS-F-001 | X | | |
| SMIMSS-F-002 | X | | |
| SMIMSS-F-003 | X | | |
| SMIMSS-F-004 | X | | |
| SMIMSS-F-005 | X | | |
| SMCTSS-F-001 | | X | |
| SMCTSS-F-002 | | X | |
| SMCTSS-F-003 | | X | |
| SMCTSS-F-004 | | X | |
| SMCTSS-F-005 | | X | |
| SMCTSS-F-006 | | X | |
| SMCTSS-F-007 | | X | |
| CMPTSS-F-001 | | | X |
| CMPTSS-F-002 | | | X |
| CMPTSS-F-003 | | | X |
| CMPTSS-F-004 | | | X |
| CMPTSS-F-005 | | | X |
| CMPTSS-F-006 | | | X |
| CMPTSS-F-007 | | | X |

表 6.13 需求与验收测试案例的关系表

| | AT1 | AT2 | AT3 |
|-------------|-----|-----|-----|
| BRTMS-F-001 | X | | X |
| BRTMS-F-002 | | X | X |
| BRTMS-F-003 | | X | X |

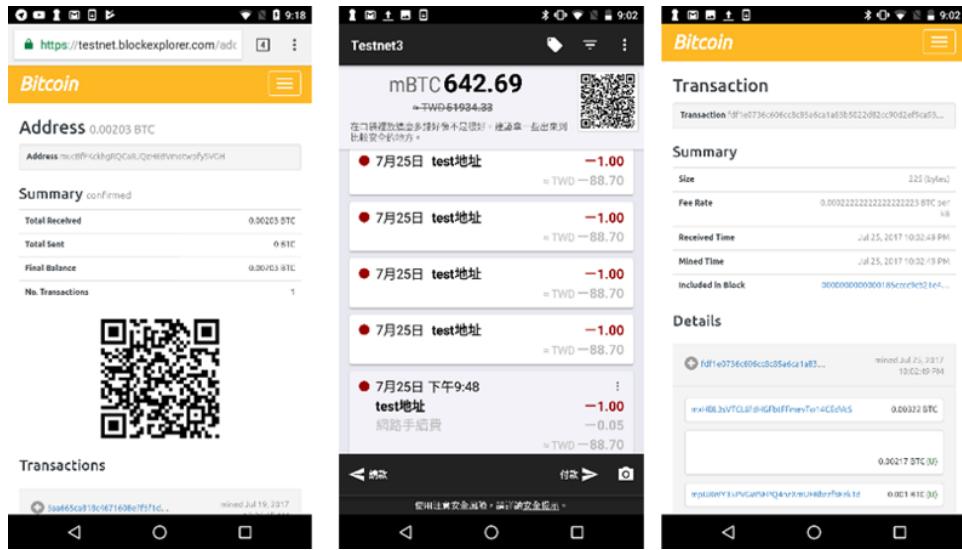


图 6.4 使用区块链浏览器验证存储在比特币区块链中的交易过程

交易实时监督系统，以下将分别针对有无采用多重签章算法的性能测试。

6.2.1 系统性能测试

为了验证本文提出的 BRTMS 不会通过使用比特币等加密货币影响交易完成时间，我们于 2017 年 7 月 25 日和 2017 年 9 月 6 日，在 Testnet 实验中连续记录了 25 笔交易信息，每 2 秒发出一笔交易，分别历时 50 分钟。

1. 第一次测试（2017 年 7 月 25 日）：首先，我们使用区块链查看器（Blockchain Explorer）^[55]，如 6.4 的快照所示，透过使用 Testnet 依序进行 25 笔比特币交易，如图 6.4 的中间快照所示，最后 25 笔交易完成时间全部记录在区块链查看器。实验结果显示，实验中的所有交易都在 3 秒钟左右（平均 2.97 秒，标准差小于 1 秒）发送到比特币网络缓存池，平均交易完成时间在比特币区块链中确认为 522.33 秒（小于 9 分钟），标准差大约为 339 秒。
2. 第二次测试（2017 年 9 月 6 日）：表 6.14 为第二次实验数据，该次的比特币交易从广播至比特币交易缓存持的时间平均为 1.918 秒，标准差为 0.55586 秒。但为了预防双花攻击需要等待平均 654.8 秒（小于 11 分钟，标准差 346.63 秒）的时间。

在未引用多重签章算法的监督系统中，第一次与第二次的测试相比并无太大的差异，交易完成时间与比特币区块生成所需时间相同，平均时间皆为十分钟。根据比特币 Testnet 上的初步实验结果显示，本文提出的 BRTMS 可以快速有效地运行区块链的实名交易监督系统。

表 6.14 第一次以 Testnet 运行实验之数据分析 (2017/09/06)

| | 进入缓存池时间 (秒) | 进入区块链时间 (秒) | 完成交易时间 |
|----------|-------------|---------------|---------------|
| 平均 | 1.918 | 654.8 | 654.8 |
| 样本标准差 | 0.55586 | 346.63 | 346.63 |
| 95% 信赖区间 | 1.69~2.15 | 511.72~797.88 | 511.72~797.88 |
| 99% 信赖区间 | 1.61~2.23 | 460.9~848.7 | 460.9~848.7 |

6.2.2 实时系统性能测试

本主要介绍比特币测试币于 Green Address 钱包进行交易的性能实验与结果分析，包含该实验的目的、方法及结果分析。实验的目的是要确认我们的系统在商家端进行行动支付时能快速、精准且高效率的进行交易，并了解使用一般 Testnet 钱包与 Green Address 钱包作为交易媒介的确认交易时间的差距。表6.15为 2017 年 7 月 25 日初步的采用多重签章算法的测试数据，数据显示交易存储到区块链的平均时间为 10 分钟，但 Green Address 采用的多重签章算法，可以有效拒绝双重花费的交易发起，因此可将交易的有效时间，从交易进入区块链的时间，重新订定为交易进入比特币交易缓存持的时间。

表 6.15 初步的 Green Address 实验测试数据 (2017/07/25)

| GA 发起时间 | GA 进入缓存池时间差 | 缓存池收到时间 | 入块时间 | 入块花费时间 |
|----------|-------------|--------------|----------|--------|
| 06:36:25 | 02:14 | 06:36:27.14 | 06:52:00 | 16:25 |
| 06:38:25 | 1.075 | 06:38:26.075 | 06:52:00 | 14:25 |
| 06:40:25 | 1.722 | 06:40:26.722 | 06:52:00 | 12:25 |
| 06:42:25 | 2.953 | 06:42:27.953 | 06:52:00 | 10:25 |
| 06:44:25 | 1.511 | 06:44:26.511 | 06:52:00 | 08:25 |
| 06:46:25 | 2.269 | 06:46:27.269 | 06:52:00 | 06:25 |
| 06:48:25 | 1.831 | 06:48:26.831 | 06:52:00 | 04:25 |
| 06:50:25 | 1.227 | 06:50:26.227 | 06:52:00 | 02:25 |
| 06:52:25 | 2.026 | 06:52:27.026 | 07:12:01 | 20:24 |
| 06:54:25 | 1.257 | 06:54:26.257 | 07:12:01 | 18:24 |
| 06:56:25 | 1.511 | 06:56:26.511 | 07:12:01 | 16:24 |
| 06:58:25 | 2.815 | 06:58:27.815 | 07:12:01 | 14:24 |
| 07:00:26 | 1.544 | 07:00:27.544 | 07:12:01 | 12:25 |
| 07:02:25 | 1.767 | 07:02:26.767 | 07:12:01 | 10:24 |
| 07:04:25 | 1.52 | 07:04:26.52 | 07:12:01 | 08:24 |
| 07:06:25 | 1.953 | 07:06:26.953 | 07:12:01 | 06:24 |

本次的实验分为两部份，分别是透过比特币 Testnet 钱包以及使用本论文所采用的 Green Address 比特币钱包上运行 25 次付款，皆以相同地址收款，交易金额都设置为 0.00001BTC，实验时间为 2017 年 9 月 6 日与 2018 年 2 月 6 日，每隔两分钟运行一次

付款的动作，总共历时 50 分钟。两款钱包同时发起交易，并透过区块链查看器进行记录时间，最后再比较使用一般比特币钱包及 Green Address 钱包两者之间的差距。

1. 第一次测试（2017 年 9 月 6 日）：表6.16

表 6.16 第一次以 GreenAddress 运行实验之数据分析 (2017/09/06)

| | 进入缓存池时间 (秒) | 进入区块链时间 (秒) | 完成交易时间 |
|----------|-------------|---------------|-----------|
| 平均 | 2.11 | 654.24 | 2.11 |
| 样本标准差 | 0.65 | 346.9 | 0.65 |
| 95% 信赖区间 | 1.84~2.38 | 511.05~797.43 | 1.84~2.38 |
| 99% 信赖区间 | 1.75~2.47 | 460.19~848.29 | 1.75~2.47 |

2. 第二次测试（2018 年 2 月 6 日）：表6.17

表 6.17 第二次以 GreenAddress 运行实验之数据分析 (2018/02/06)

| | 进入缓存池时间 (秒) | 进入区块链时间 (秒) | 完成交易时间 |
|----------|-------------|--------------|-----------|
| 平均 | 1.96 | 92.4 | 1.96 |
| 样本标准差 | 0.538516 | 86.43012 | 0.538516 |
| 95% 信赖区间 | 1.74~2.18 | 56.72~128.08 | 1.74~2.18 |
| 99% 信赖区间 | 1.66~2.26 | 44.05~140.75 | 1.66~2.26 |

本次实验分别记录以 Testnet 钱包及 Green Address 钱包运行 25 次交易的进入缓存池等待时间和写入区块等待时间。若以 Testnet 钱包交易，必须等到交易写入才能保证此笔交易不会被矿工遗弃，也算真的完成这笔交易；但若以 Green Address 钱包发起交易就大不相同，当交易进入缓存池，即使遇到交易被矿工遗弃的情况，Green Address 机构节点也会重新发起此笔交易，保证让交易写入区块，所以只要进入缓存池我们就可以视为交易完成，透过两者钱包的交易数据，本文分析两种钱包交易的时间数据。

透过本次的实验可以发现虽然以两种钱包交易进入区块的等待时间完全相同，但因为 Green Address 钱包的特性，只要进入缓存池就算完成交易确认，因此 Green Address 钱包的完成交易确认的时间远远快于一般 Testnet。相信以此方式作为主要支付管道，可以省去消费者在现金支付时掏零钱、算钱及找零等繁琐的动作及时间，以此达成提升日常生活中的便利性与安全性。

第七章 总结与展望

在文論本中，我們建議並實施一個名為 BRTMS 的區塊鏈實名交易監督系統，不僅為分別花錢和賺取加密貨幣的客戶和商家，同時也能協助府金融監督單位審計加密貨幣交易籌集稅收。此外，加密貨幣交易實驗的初步結果，使用比特幣測試幣及於章節 4.1 所設計的 BRTMS 數據庫，我們以著名的比特幣加密貨幣錢包實作的 Java 應用程序和 Android 應用程序客戶端。

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，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。本文提出的 BRTMS 架構還包括以下特色如下：

1. 向建議的 BRTMS 進行商業註冊需經政府批准。
2. 所有出售的商品將受到政府審查。
3. 消費者仍然匿名以確保個人信息的隱私。
4. 消費者的交易記錄不能被刪除。
5. 如果消費者有關交易上訴的問題，他們需要提交交易發票或證明付款人或收款人地址的訪問權。
6. 所有交易記錄均公開透明。
7. 原始交易數據採用區塊鏈技術記錄，具有高度的可靠性，分散和未篡改的數據。
8. 政府可以檢查建議的 BRTMS 系統的交易記錄，以快速有效的方式審查稅務信息。

提議的 BRTMS 的優點總結：

1. 消費者：交易信息公開透明，保護消費者的權益。由於交易是可信的，並有明確的時間戳。當消費者需要上交他們的消費者權利時，他們可以從提出的系統中獲得更有效和可信的證據。
2. 商家：企業可以根據所有數字化交易信息為自己的業務目的進行統計和計算。這可以減少手動操作計算結果中的錯誤。統計數據甚至可以與商店的庫存管理相結合，使貨物和資金達到更加便利地進行統計，進一步改善業務的會計準確性和人工成本。
3. 政府：在解決交易糾紛的過程中，可以提供更多可信的證據供參考。數字交易收據也可以解決紙本收據丟失或破損的問題。考慮到稅收問題，政府可以審查具有高信譽的商業交易細節作為稅收計算程序，以定制稅標準，減少許多稅收糾紛。

参考文献

- [1] Charlie Lee. *Litecoin Official website*, 2011. <https://litecoin.org>.
- [2] Billy Markus. *DogeCoin*, 2013-12. <http://dogecoin.com>.
- [3] Daniel Kraft. *Namecoin*, 2011-04. <https://namecoin.org>.
- [4] Sunny King. *Primecoin*, 2013-07. <http://primecoin.io/>.
- [5] Constantine Kryvomaz. *Ethereum Classic*, 2015-07. <https://ethereumclassic.github.io/>.
- [6] Ethereum Foundation Vitalik Buterin. *Ethereum*, 2015-07. <https://ethereum.org>.
- [7] *solidity*. <https://solidity.readthedocs.io/en/develop/>.
- [8] Gavin Wood. “*Ethereum: A secure decentralised generalised transaction ledger*”. *Ethereum Project Yellow Paper*, 2014, 151: 1–32.
- [9] Rainer Böhme, Nicolas Christin, Benjamin Edelman et al. “*Bitcoin: Economics, technology, and governance*”. *Journal of Economic Perspectives*, 2015, 29(2): 213–38.
- [10] *Cryptocurrency Market Capitalizations*. <https://coinmarketcap.com/all/views/all/>.
- [11] John Gregor Fraser and Ahmed Bouridane. *Have the security flaws surrounding BITCOIN effected the currency's value?*, 2017: 50–55.
- [12] Kyle Torpey. “*You Really Should Run a Bitcoin Full Node: Here's Why*”. *Bitcoin Magazine*, 2017.
- [13] 蔡怡杼. 银行员监守自盗手法有这些, 2017-10. <https://www.nownews.com/news/20171029/2633984>.
- [14] CM Adams and SE Tavares. *The use of bent sequences to achieve higher-order strict avalanche criterion in S-box design* [techreport], 1990.
- [15] *Bitcoin Improvement Proposals*. <https://github.com/bitcoin/bips/blob/master/README.mediawiki>.
- [16] *Western Union*. <https://www.westernunion.com/us/en/home.html>.
- [17] *PayPal*. <https://www.paypal.com>.
- [18] *Digibyte*. <https://www.digibyte.io>.
- [19] blockchain.info. *Blockchain Size*, 2018. <https://blockchain.info/charts/blocks-size?timespan=all>.
- [20] J Göbel and AE Krzesinski. “*Increased block size and Bitcoin blockchain dynamics*”. In: *Telecommunication Networks and Applications Conference (ITNAC), 2017 27th International*, 2017: 1–6.
- [21] Shen Noether and Sarang Noether. “*Monero is not that mysterious*”. *Technical report*, 2014.
- [22] Emmanuel Bresson, Jacques Stern and Michael Szydlo. “*Threshold ring signatures and applications to ad-hoc groups*”. In: *Annual International Cryptology Conference*, 2002: 465–480.
- [23] Ming Zhong. “*A faster single-term divisible electronic cash: ZCash*”. *Electronic Commerce Research and Applications*, 2002, 1(3-4): 331–338.

- [24] Uriel Feige, Amos Fiat and Adi Shamir. “Zero-Knowledge Proofs of Identity”. *J. Cryptology*, **1988**, 1(2): 77–94. <https://doi.org/10.1007/BF02351717>.
- [25] Thibault de Balthasar and Julio Hernandez-Castro. “An Analysis of Bitcoin Laundry Services”. In: *Nordic Conference on Secure IT Systems*, **2017**: 297–312.
- [26] Ayush Singh Panwar. “Asymmetric Key Cryptography”. *Browser Download This Paper*, **2014**.
- [27] Taher ElGamal. “A public key cryptosystem and a signature scheme based on discrete logarithms”. *IEEE transactions on information theory*, **1985**, 31(4): 469–472.
- [28] Andrew Miller and Joseph J LaViola Jr. “Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin”. Available on line: <http://nakamotoinstitute.org/research/anonymous-byzantine-consensus>, **2014**.
- [29] Don Johnson, Alfred Menezes and Scott Vanstone. “The elliptic curve digital signature algorithm (ECDSA)”. *International Journal of Information Security*, **2001**, 1(1): 36–63.
- [30] Dmitry Khovratovich, Christian Rechberger and Alexandra Savelieva; ed. by Anne Canteaut. “Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family”. In: *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*. Springer, **2012**: 244–263. https://doi.org/10.1007/978-3-642-34047-5_15.
- [31] Florian Mendel, Norbert Pramstaller, Christian Rechberger *et al.*; ed. by Sokratis K. Katsikas, Javier Lopez, Michael Backes *et al.* “On the Collision Resistance of RIPEMD-160”. In: *Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings*. Springer, **2006**: 101–116. https://doi.org/10.1007/11836810_8.
- [32] The Bitcoin Core developers. *Base58*, **2009**. <https://github.com/bitcoin/bitcoin/blob/master/src/base58.cpp>.
- [33] *The Large Bitcoin Collider*. <https://lbc.cryptoguru.org>.
- [34] Tim Dierks. “The transport layer security (TLS) protocol version 1.2”. **2008**.
- [35] Android Developers Blog. *Some SecureRandom Thoughts*, 2013-08. <https://android-developers.googleblog.com/2013/08/some-securerandom-thoughts.html>.
- [36] bitcoin.org. *Android Security Vulnerability*, 2013-08. <https://bitcoin.org/en/alert/2013-08-11-android>.
- [37] BurtW. *Bad signatures leading to 55.82152538 BTC theft*, 2013-08. <https://bitcointalk.org/index.php?topic=271486.0>.
- [38] Lars R Knudsen, Vincent Rijmen, Ronald L Rivest *et al.* “On the design and security of RC2”. In: *International Workshop on Fast Software Encryption*, **1998**: 206–221.
- [39] Ron Rivest. “Rc4”. *Applied Cryptography by B. Schneier*, John Wiley and Sons, New York, **1996**.
- [40] Ronald L Rivest. “The RC5 encryption algorithm”. In: *International Workshop on Fast Software Encryption*, **1994**: 86–96.
- [41] RL Rivest, MJB Robshaw, R Sidney *et al.* *The RC6 block cipher. v1. 1, August 20, 1998*, **2016**.
- [42] Data Encryption Standard. “Data encryption standard”. *Federal Information Processing Standards Publication*, **1999**.

- [43] American Bankers Association *et al.* “*Triple Data Encryption Algorithm Modes of Operation*”. *ANSI X9*: 52–1998.
- [44] Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, **2013**.
- [45] Ronald L Rivest, Adi Shamir and Leonard M Adleman. *Cryptographic communications system and method*. Google Patents, 1983-9 20.
- [46] Neal Koblitz. “*Elliptic curve cryptosystems*”. *Mathematics of computation*, **1987**, 48(177): 203–209.
- [47] Nicholas Jansma and Brandon Arrendondo. “*Performance comparison of elliptic curve and rsa digital signatures*”. *nicj.net/files*, **2004**.
- [48] Léo Ducas, Alain Durmus, Tancrede Lepoint *et al.* “*Lattice signatures and bimodal Gaussians*”. In: *Advances in Cryptology–CRYPTO 2013*. Springer, **2013**: 40–56.
- [49] Scott Vanstone. “*Deployments of Elliptic Curve Cryptography*”. In: *the 9th Workshop on Elliptic Curve Cryptography (ECC)*, **2005**.
- [50] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*, **2008**.
- [51] Christian Decker and Roger Wattenhofer. “*Information propagation in the bitcoin network*”. In: *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, **2013**: 1–10.
- [52] Ghassan O Karame, Elli Androulaki and Srdjan Capkun. “*Double-spending fast payments in bitcoin*”. In: *Proceedings of the 2012 ACM conference on Computer and communications security*, **2012**: 906–917.
- [53] Addy Yeow. *Global Bitcoin Node Distribution*. <https://bitnodes.earn.com/>.
- [54] *Bitcoin Testnet*. <https://en.bitcoin.it/wiki/Testnet>.
- [55] Hiroki Kuzuno and Christian Karam. “*Blockchain explorer: An analytical process and investigation environment for bitcoin*”. In: *Electronic Crime Research (eCrime), 2017 APWG Symposium on*, **2017**: 9–16.
- [56] Po-Wei Chen, Bo-Sian Jiang and Chia-Hui Wang. “*Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet*”. In: *Wireless and Mobile Computing, Networking and Communications (WiMob)*, **2017**: 139–146.

致謝

原本就對比特幣區塊鏈技術深感興趣的我，來到了北京大學攻讀工程碩士學位。在這段期間深怕著會因為科系的關係而影響到了我的研究方向，在導師雙選了劉京老師，老師相當支持我做自己的研究，後來也見到了李傑教授，大力鼓勵著我繼續往科研的方向前進，老師的宏亮的聲音、霸氣的指導深植我心。段莉華老師也相當支持我做學術研究，因為段老師也一度的前往北京大學的校本部探討密碼學的研究。

在台灣實習的我來到了台灣最高學術研究機構中央研究院資訊科學所繼續展開我的科研路，同時也延續著之前與銘傳大學王家輝老師合作的科技部計畫“比特幣監督收銀系統”，因為有著計畫的補助也使得在求學的路上獲得更充足的預算，也因為計劃上的補助，使我能夠順利地前往義大利羅馬參加 IEEE WiMob 會議發表論文“Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet.”^[56]，參加了台灣最大的計算機會議 TANET 發表論文“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”，也得到了 TANET 會議的最佳論文獎，也要對與我合作的最佳夥伴江柏憲同學，我們共創了大學時期專題研究的第一名，這次我們也一舉奪下了 TANET 的最佳論文，相信都在我們的人生道路中寫下了嶄新的一頁。感謝李開暉教授願意教導我並讓我在其旗下做科學研究，同時給予我最大的資源與協助，並總是指引我研究方向。

除了在諸位教授的諄諄教誨下使我有機會完成這篇論文外，也要誠摯的感謝於二零一四年帶我認識比特幣的啟蒙老師楊哲豪先生，沒有他的教導無法成就至今已多達三萬四千人的比特幣中文社群之社群，也不會給予我有這樣的機會了解比特幣的運作原理，通過所學與社群間交流種種架構出我現在的區塊鏈產業概念，成為我在區塊鏈科技產業發展之道路最重要的基石。

北京大学学位论文原创性声明和使用授权说明

原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不含任何其他个人或集体已经发表或撰写过的作品或成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本声明的法律结果由本人承担。

论文作者签名： 日期： 年 月 日

学位论文使用授权说明

(必须装订在提交学校图书馆的印刷本)

本人完全了解北京大学关于收集、保存、使用学位论文的规定，即：

- 按照学校要求提交学位论文的印刷本和电子版本；
- 学校有权保存学位论文的印刷本和电子版，并提供目录检索与阅览服务，在校园网上提供服务；
- 学校可以采用影印、缩印、数字化或其它复制手段保存论文；
- 因某种特殊原因需要延迟发布学位论文电子版，授权学校在一年/两年/三年以后在校园网上全文发布。

(保密论文在解密后遵守此规定)

论文作者签名： 导师签名： 日期： 年 月 日