北京大学

硕士研究生学位论文

题目：区块链的实名交易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：

二零一八年一月

版权声明

摘要

金融科技蓬勃發展的今天，區塊鏈技術也是重點發展對象。區塊鏈技術最著名的代表作，不外乎是於 2009 年中本聰提出的一篇名為比特幣：一種點對點式的電子現金系統》（Bitcoin: A Peer-to-Peer Electronic Cash System）論文 [1]，奠定了區塊鏈技術的開始，以及於貨幣銀行學緊密的結合。比特幣是一個集成網路學、密碼學、金融學的密碼貨幣，現今的密碼貨幣市場中，有數以千計的貨幣種類在市場流動著。執得一提的是，於 2009 年開始運作至今 (2018 年)，比特幣點對點式的電子現金系統，還未出現過錯誤，這也體現了比特幣可以承受將近十年來各式各樣的網路攻擊以及在程序上並無太大的漏洞瑕疵。比特幣最大的特色在於去中心化、匿名化，因為去中心化的基礎建構出一個政府無法管控的點對點的金流，也因為匿名，使得政府相關人士難你去追查每一筆資金的真正持有者是誰，在傳統的中心化銀行跨國轉帳中都需要基本的實名制驗證，藉由實名制有效過濾洗錢的發生。但在彼特幣點對點的電子現金系統中，沒有任何一個使用者或是政府可以要求每一個人的實名制，促使的交易追蹤、洗錢防制變得更加的困難。除了不可管控、難以追蹤的特點外，在國家政府方面稅收更是國家繼續運作的基礎資金來源，因為現今的國家並無支持比特幣相關的收銀機或是制定出相關的標準稅務，也使得國家政府無法在這方面獲得稅務資金。

經由深度的了解比特幣的運作原理，再由上述無法管理資金流、無法追蹤、無法得到稅收，三項出發點，本論文致力於設計一個比特幣的收銀監督系統。在設計該系統前，也探討了多種場景下的交易模型，發現現金已經存在匿名支付給匿名、匿名支付給實名的模型，在刷卡支付中有著實名支付給實名、實名支付給匿名再支付給實名，上述的四種模型。經有上述的分析，可以得知，個人隱私的意識崛起，唯有匿名支付給實名時，才可以做到不透露消費者信息，亦可做到消費者權益的申訴權。在點對點的電子現金的市場中，還是停留在匿名支付給匿名的場景中，本論文致力於設計一個匿名支付實名的密碼貨幣市場的監督收銀系統，以實踐消費者匿名，同時也讓消費者擁有費者權益的交易模型。

关键词：比特幣，區塊鏈，多重簽章

Test Document

Test (Some Major)

Directed by Prof. Somebody

ABSTRACT

Test of the English abstract.

KEYWORDS: Bitcoin, Blockchain, Multiple signatures

目录

序言

現金法定貨幣，收據及交易數據庫存在著一些缺點。如現貨幣很難杜絕假鈔的橫行，收據有著偽造的可能，在交易數據庫中資料不一致，數據庫被 DDOS 攻擊，交易數據被竄改，數據庫損毀，也都是在交易過程中曾出現的窘境。

於 2009 年加密貨幣 - 比特幣的問世，以密碼學、網路學、貨幣銀行學為基礎創建了新一代的網路貨幣。竄改、公開交易數據檢視、使用者匿名性、自動運作不須人為運營的多項特性。至今區塊鏈技術已成為 IBM、摩根大通、微軟、谷歌、英特爾重點開發項目，被視為改善銀行運作效率、降低運營成本、提升資訊安全、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，預採用以區塊為基礎的數字貨幣比特幣為貨幣，進行商業化收銀系統開發。不僅僅是比特幣算法穩定、交易公開透明、不可被竄改的特性外，更是本論文加入監督標籤，使得在匿名交易轉為部分實名交易，促使監管部門能有更好的貨幣技術提升，亦可建立自動化的稅務審查機制，大幅降地人成本，亦可提高交易系統的信息可靠度及穩定度。

第一章　研究動機

1.1　密碼貨幣的發展

追溯著加密貨幣市場的演進，於 2009 年時，比特幣並非第一個密碼貨幣，在比特幣之前已經有著很多的類似的密碼貨幣開發實驗，但是一直無法做出一個穩定點對點式的電子現金系統，至於製作貧頸會在後段章節中闡述。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就稱之為山寨幣，山寨幣早期較為著名的有萊特幣（LiteCoin，LTC）[2]、狗幣（DogeCoin，DOGE）[3]、域名幣（NameCoin，NMC）[4]，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費資源，努力的開發具有意義的工作量證明挖礦算法較為著名的有素數幣（Primecoin，XPM）[5]。於 2015 年底也誕生了現在最為著名的以太坊經典（Ethereum Classic，ETC）[6]、以太坊（Ethereum，ETH）[7]，使得區塊鏈技術不再僅僅只是一個點對點的電子現金系統，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，也創造出了屬於乙太坊的編程語言 Solidity，使得再以太坊的虛擬機當中，可以用 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。

1.2　密碼貨幣市場（Cryptocurrency Market）

密碼貨幣最具代表性的是比特幣，但除了比特幣之外也有著許多模仿比特幣的密碼貨幣，有的是為了利益，有的是鑒於比特幣的各種不完美，希望可以解決比特幣不足之處。密碼貨幣市場中有成千上萬種的密碼貨幣，較為著名的密碼貨幣會在 Cryptocurrency Market Capitalizations[8] 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 種密碼貨幣。在 Cryptocurrency Market Capitalizations 統計的數據當中，可知整體的密碼貨幣市場，如下圖1.1所示，於 2018 年 1 月 7 日創下了歷史新高，密碼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。

經由 Cryptocurrency Market Capitalizations 數據顯示，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，於"Have the security flaws surrounding BITCOIN effected the currency's value?." 論文 [9] 中做了詳盡的比特幣市場調研，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，因為早期的密碼貨幣市場中無完善的法律規範，各國對密碼貨

图 1.1　Total Market Capitalization[8]

幣的接受度有所不同，日本對金融科技的接受度相較較為開放的情況下成立了全世界第一家比特幣交易所，也因為交易所不夠普及，使得大部分的密碼貨幣交易都集中在 Mt.Gox 交易所中，促使 Mt.Gox 倒閉事件會成為影響市場價格重大因子之一，也造成 2014 與 2015 年的密碼貨幣市場的低迷，2017 為 2016 年的 35 倍成長幅度，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 日支持比特幣期貨，將比特幣價格推升到 20,000 美金的歷史新高，下圖1.2為 2013 年至 2018 年歷年的密碼貨幣總市值的統計圖表。

图 1.2　密码货币历年最高总市值 [8]

1.3　密碼貨幣的優勢

於 2009 年 Satoshi Nakamoto 發布了比特幣系統，成為全世界第一個密碼貨幣的雛形。密碼貨幣的特點在於 24 小時不間斷運作、遠距離支付、貨幣為使用者持有，區塊鏈技術突破現存傳統中心化金融機構的貧頸。

1.3.1　24 小時不間斷運作

基於區塊鏈技術與點對點網路的架構，以比特幣為例，自 2009 年至今，所有的比特幣交易事件皆會儲存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路的方式儲存在比特幣網路中的全節點，目前比特幣網路中的全節點高達 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。點對點網路提供穩定的數據庫資料元，不會因為數據庫的關機而無法繼續使用，

1.3.2　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，既使當資金順利抵達了目的地的銀行，目的地的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完整的身份驗證、解釋資金用途，才得以取得這筆的跨國資金。比特幣系統當中，有著 24 小時不間斷運作的優點，也因為點對點網路架構，使得比特幣無需經由傳統的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清況下，平均 10 分鐘即可入帳。

1.3.3　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，百姓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 [10] 指出，台灣各地於 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為新台幣。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，既使是比特幣系統皆無法動用該筆比特幣資產，唯有比特幣地址的私鑰持有者，才可以移動該筆資產。

1.3.4 開放和透明的交易信息

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，因此交易區塊數據存儲所涉及的所有節點都可以查看交易數據，所有人都可以檢查每個交易記錄的正確性，公開的交易信息使交易數據可信。

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原數據。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。公司或學者可以製定一個可視化的開發計劃，甚至可以使用大量數據來分析以前從未見過的有價值的觀點。

1.3.5 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無法刪除。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存儲在新區塊中，只要塊中的值被修改，即使有一點，也會使哈希值完全不同，也就是說，雪崩效應將會發生。由於這種結構，所有的信息都不會被改變，所以如果驗證的結果被改變，該塊將不被系統接受。因此，所有的交易記錄已經存儲在區塊鏈中，不能修改和刪除。

1.3.6 匿名

在當今社會，個人信息保護已成為企業最重要的問題。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係，因次建立匿名。區塊鏈系統中的所有賬戶都是由單獨的匿名個人創建的，可以有效保護消費者的隱私。然而，Visa 交易是不同的，我們會向 Visa 公司的集中主機顯示大量個人信息，這可能會導致個人信息洩露的風險。在區塊鏈技術中，可以經濟有效地避免這個問題。

1.3.7 自治系統

在區塊鏈系統中，操作依賴於一些算法，包括一致性算法。因此，在這種自治系統中，沒有人（例如節點或礦工）可以直接改變係統操作的規則。如果在比特幣系統中發現需要更正的嚴重錯誤，可以建議使用比特幣改善提案（Bitcoin Improvement Proposals，BIP）升級比特幣系統。在升級模塊可以在比特幣系統上正式運行之前，提議的比特幣改進建議需要得到比特幣系統中超過一定數量的礦工的支持。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，但相對穩定。

1.4　密碼貨幣的劣勢

在區塊鏈技術中，有著幾項貧頸，每秒處理的交易量（Transactions Per Second，TPS）上限、無法達成即時交易確認、洗錢防制困難、低可擴展性。

1.4.1　每秒處理的交易量（Transactions Per Second，TPS）上限

下圖1.3為 VISA 為國際上最為著名的支付系統，以中心化運營的方式，可以支持高達 2,000 筆交易每秒。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的交易量僅為 7 筆，這樣的上限由許多原因造成。

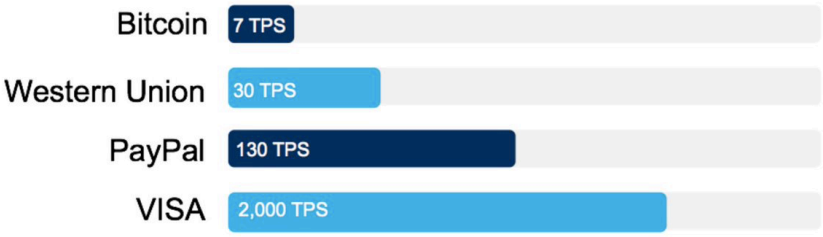

图 1.3　每秒處理的交易量比較圖 [**TPS**]

上修區塊大小上限，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。下圖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，這表示著比特幣網路中持續的維持在公不應求的狀況。現今對比特幣的每秒處理的交易量有許多優化的方案，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，在系統的每秒處理的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，倘若存儲區塊鏈特成本超過了摩爾定律的成長曲線，會進一步造成自願成為比特幣全節點的意願度降低，使得比特幣網路的全結點數變少，促使比特幣去點對點網路往中心化網路發展，失去一開始點對點網路的意義。

上修區塊大小上限，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造成比特幣網路的影響，於“Increased block size and Bitcoin blockchain dynamics”[12] 有著詳細的研究，在上修區塊大小上限的議題上，除了造成比特幣全節點意願度下降，亦有

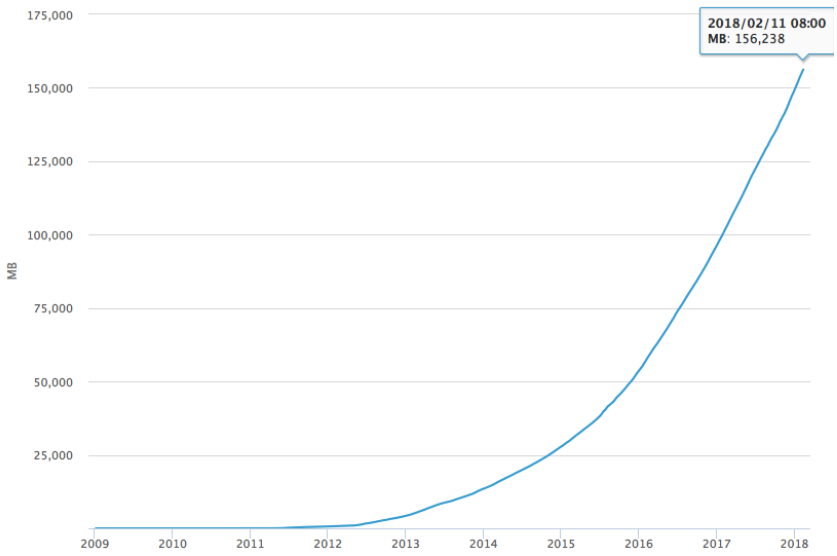

图 1.4　比特幣區塊鏈大小 [11]

機會造成以比特幣點對點網路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路協議同步到 1055 個節點上，在比特幣系統中，長年來的實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的現象更加的明顯，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，近一步造成整得比特幣點對點網路崩潰。

1.4.2　洗錢防制困難

匿名性為比特幣系統一大特色，比特幣的地址生成是在 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、洗錢防制邊的困難，甚至有更為前沿的密碼貨幣 Monero 導入了環簽章算法、Zcash 導入零知識證明算法 [13]，使得原本公開透明的區塊鏈，變得無法檢視，使得密碼貨幣在洗錢防制上更加的困難。論文"An Analysis of Bitcoin Laundry Services."[14]，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，下圖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。

1.4.3　低可擴展性

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貨幣，大部分的密碼貨幣皆不支持外部輸入，外部的信息輸入皆無法保證資料的正確性，近一步造成垃圾勁垃圾

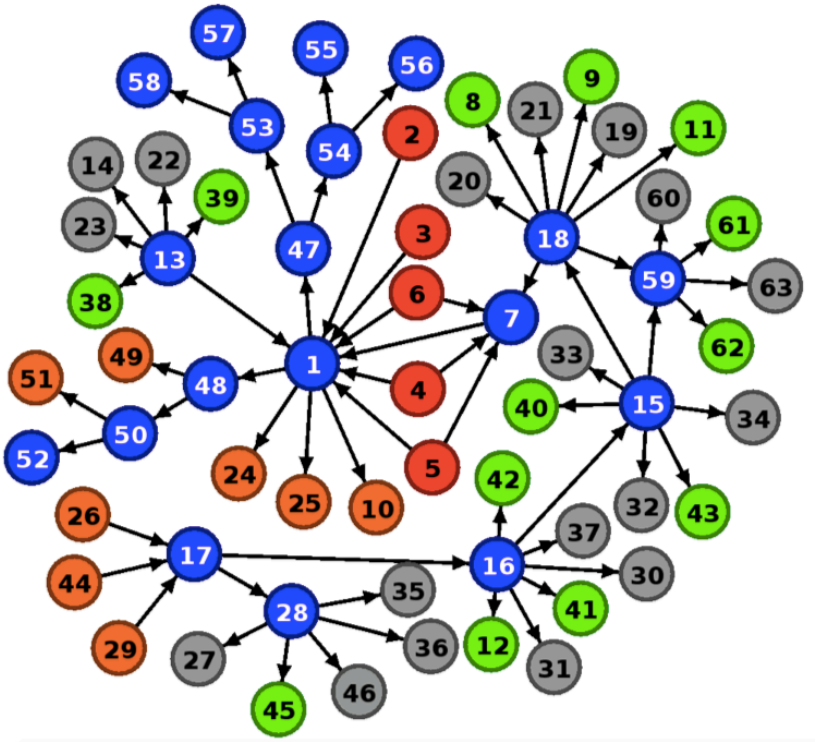

图 1.5　Darklaunder 洗錢模型 [14]

出的問題，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。

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，開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，使得在交易中添加些個人信息變得更加昂貴。

第二章　文獻探討

2.1　比特幣（Bitcoin）

比特幣（Bitcoin，BTC）是一個點對點式的點子現金系統，集成了非對稱式金鑰密碼學（Asymmetric Key Cryptography）[15]、簽章密碼學（Signature cryptography）、零知識證明密碼學（Zero Knowledge Proof Cryptography）[13]、哈希函數密碼學（Hash function cryptography）、共式算法（Consensus）諸多技術建構了一個分散式的不需要靠中心化機構加以維護的交易帳本（區塊鏈）。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，深入了解比特幣地址生成相關算法的、比特幣地址生成過程、多重簽名。可以應用在区块链的实名交易监督系统。

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[16]、SHA-256（哈希函數）[17]、RIPEMD-160（哈希函數）[18]、Base58[19]。接下來回詳細說明每一個函數的運做過程以及意義，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 $1.1579209x10^{77}$，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 [20] 也有團隊正在努力的窮舉比特幣 2^{256} 的組態空間，如下圖2.1所示，根據 LBC 公布的數據顯示，目前已經完成了 $2.330109x10^{16}$ 個地址探索。雖然 10^{16} 的級別與 10^{77} 的級別相距甚遠，但 LBC 已探索空間中擊中了 15 個比特幣地址，團隊也將這 15 個地址的 1.180899 個比特幣轉走。

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所有的可能性即可猜出亂數。而亂數在密碼

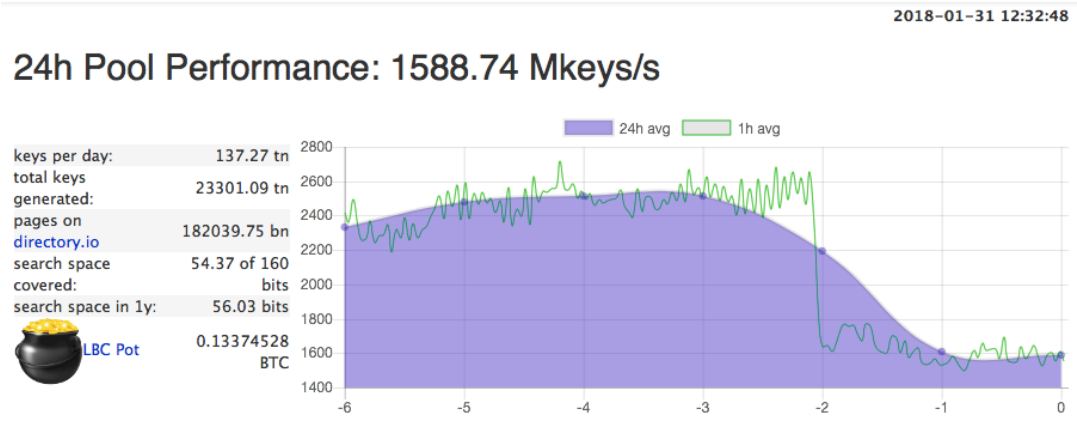

图 2.1　Bitcoin Full Node[20]

學中通常會是一個把私鑰的構建，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，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的存在著不隨機，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”[21]，Bitcoin.org 也發布了警告 [22] 簡要說明該事件的原因，以及表明影響到的 Bitcoin Wallet 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 [23]，但因為比特幣屬於被動的性質，無人主動回報既不會加入統計中，所以總損失應該會超過 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)[24]、RC4(1987 年)[25]、RC5(1994 年)[26]、RC6(1998 年)[27]；信息塊加密著名的有数据加密标准 (Data Encryption Standard，DES，1975 年)[28]、三重数据加密算法（Triple Data Encryption Algorithm，Triple DES，1998 年）[29]、高级加密标准（Advanced Encryption Standard，AES，1998 年）[30]；非對稱是加密最為著名的有 RSA（Rivest–Shamir–Adleman，1977 年）[31]、椭圆曲线密码学（Elliptic curve cryptography，ECC，1985 年）[32]。非對稱式加密與對稱式加密最大的不同在於，對稱是加密在加密解密的過程中只需要一把鑰匙，而非對稱是加密會生成兩把鑰匙分別為私鑰與公鑰，在算法

的設計上在一開始會以亂數產生一把私鑰，再經由非對稱是加密算法推導出公鑰，推導出的公鑰在非對稱式密碼學中是相當難以到推回去私鑰，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 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布在網路上，這時希望聯繫 Alice 的 Bob 在網路上取得公鑰後，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，既使網路存在著監聽，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的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费的输出（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治比特幣網路的交易緩存持當中，等待礦工的將該筆交易收入至比特幣區塊鏈當中。比特幣採用的 secp256k1 是屬於椭圆曲线密码学中的一個版本，不同的橢圓曲線版本的差異在於不同的初始參數，包括橢圓曲線函數、p 值巨大的質數、G 點被称为生成点的常数点亦稱為基點。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，下圖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 [33] 指出，當 ECC 產生 571bit 的密鑰長度，RSA 要達到相同的安全性需要生成 15360bit，至於生成的時間差距高達 471 倍。

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 [33]

除了在於密鑰對生成時間 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 做出了深度的安全性探討 [34]，2.3研究指出，同樣達到 80bit 的安全性級數，RSA 1024 需要 1024bit，ECDSA 160 僅需要 160bit，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，在未來涼已計算機的蓬勃發展擁有 2000qbit 運算能力的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名算法。

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
ECDSA[1] **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　X X X [34]

SHA-256

哈希下數在比特幣系統中，扮演著相當多的角色，包括彼特幣地址生成、比特幣交易哈希指針、比特幣區塊哈希指針、比特幣挖礦算法工作量證明。哈希算有幾大特色，分別為

RIPEMD-160

Base58

2.2.2　比特幣地址生成過程

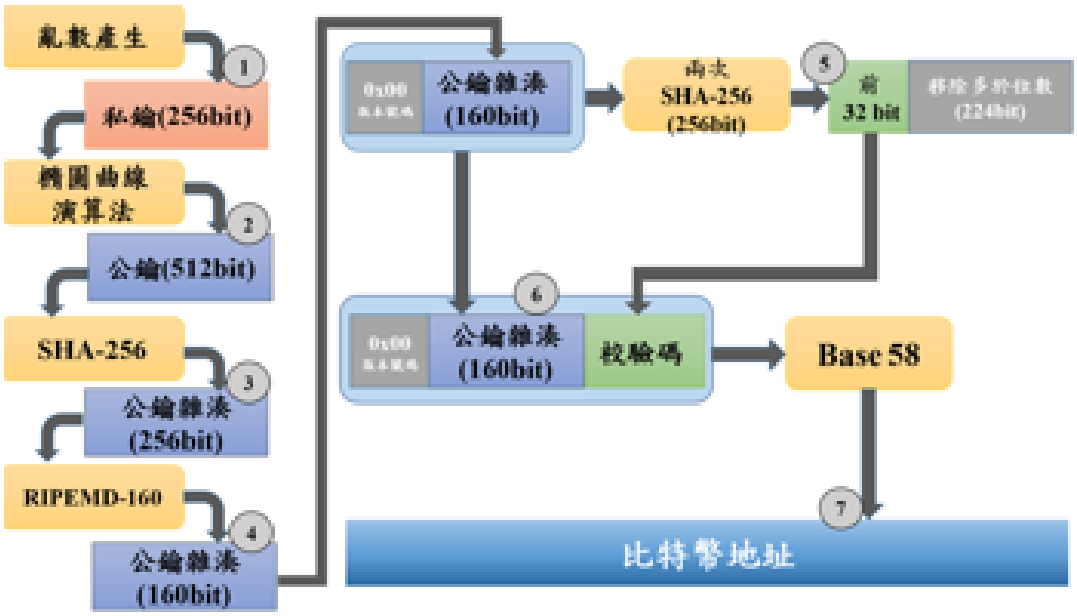

图 2.4　比特幣地址生成過程

生成私鑰　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) 簽署花費該地址當中的比特幣。

生成公鑰　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。

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

生成公鑰 SHA-256 的 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。

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。對公鑰 SHA-256 的 RIPEMD-160 再做兩次 SHA-256，取該哈希值得前 32bit 的值作為校驗碼

取得版本號　比特幣在一開始設計的過程中，便定義了不同的地址樣式及功能，在第五個步驟中會加入版本號加以區分不同的地址。

版本號、公鑰 SHA-256 的 RIPEMD-160 和校驗碼合併　版本號、第四個步驟的產物公鑰 RIPEMD-160 及第五個步驟的校驗碼合併。

合併的結果以 Base58 編碼　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。

2.3　區塊鏈（Blockchain）

自 2009 年以來，加密數字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數字貨幣。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數字貨幣。比特幣是區塊鏈技術最重要的應用之一。我們將描述區塊鏈技術的一些細節。

2.3.1 本區塊大小的值

2.3.2 區塊頭（Block Header）

區塊版本（32 bits） 該欄位存儲比特幣區塊鏈中的區塊版本。

前區塊的哈希值（256 bits） 記錄前一個塊的哈希值。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。為新區塊不斷疊加在舊的區塊上，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，促使的哈希職間接引用越多次，因此較早創建的區塊更難以修改。

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，屆時的交易為 n 個樹葉，將每個樹葉進行一次 sha-256 取得哈希值得到 n 個哈希值，再兩兩配對合併進行哈希，得到 2^{-1} 個哈希值後，直到合併到只剩下一個哈希值，最後一個哈希值則為 Merkle Root，在區塊鏈中的 Merkle Root 可用於快速檢查當前區塊中所有存儲事務的正確性。

難易度（32 bits） 在比特幣網路中難易度參數平均每十五天會有所變動，用以調控比特幣區快的產出頻率，在過去的密碼貨幣的設計中，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。

時間戳記（32 bits） 以年、月、日、小時和秒的格式記錄區塊生成時間。

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。

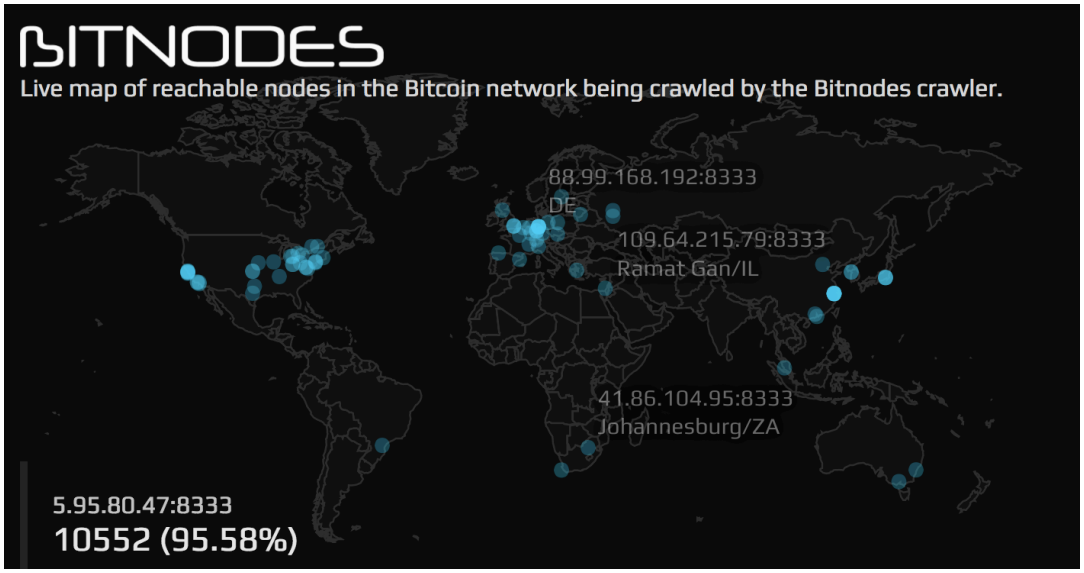

图 2.5　Bitcoin Full Node[35]

2.3.3　Block Data

交易計數器（4-36 bits）

交易信息

2.4　工作量證明（Proof of Work）

2.5　點對點網路（Peer to peer network）

去中心化的密碼貨幣系統帶給社會帶給傳統的中心化的金融體系以及政府帶來了很重大的衝擊，中本聰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，也將交易紀錄的帳本已明文的方式儲存在去中心化的區塊鏈中，以比特幣為例，現今的完整的比特幣區塊鏈帳本已經高達 180GB，這樣保存完整交易資料的計算機稱之為全節點，在比特幣去中心化的網路中，如圖2.5所示，截至 2018 年 1 月 25 比特幣網路中全節點數量為 10552 個 [35]，全節點的數量決定了比特幣帳本的可靠度，倘若有著更多的全結點，會使得比特幣網路堅不可摧，更難去修改歷史發生過的交易數據。

第三章　比特幣交易監督系統設計

第四章　比特幣監督系統實作

结论

pkuthss 文档模版最常见问题：

`\cite`、`\parencite` 和 `\supercite` 三个命令分别产生未格式化的、带方括号的和上标且带方括号的引用标记：**test-en**，**[test-zh]**、[test-en, test-zh]。

若要避免章末空白页，请在调用 pkuthss 文档类时加入 openany 选项。

如果编译时不出参考文献，请参考 `texdoc pkuthss`“问题及其解决”一章“其它可能存在的问题”一节中关于 biber 的说明。

参考文献

[1] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*, **2008**.

[2] Charlie Lee. *Litecoin Official website*, **2011**. https://litecoin.org.

[3] Billy Markus. *DogeCoin*, 2013-12. http://dogecoin.com.

[4] Daniel Kraft. *Namecoin*, 2011-04. https://namecoin.org.

[5] Sunny King. *Primecoin*, 2013-07. http://primecoin.io/.

[6] Constantine Kryvomaz. *Ethereum Classic*, 2015-07. https://ethereumclassic.github.io/.

[7] Ethereum Foundation Vitalik Buterin. *Ethereum*, 2015-07. https://ethereum.org.

[8] *Cryptocurrency Market Capitalizations*. https://coinmarketcap.com/all/views/all/.

[9] John Gregor Fraser and Ahmed Bouridane. *Have the security flaws surrounding BITCOIN effected the currency's value?*, **2017**: 50–55.

[10] 蔡怡杼. 银行员监守自盗手法有这些, 2017-10. https://www.nownews.com/news/20171029/2633984.

[11] blockchain.info. *Blockchain Size*, **2018**. https://blockchain.info/charts/blocks-size?timespan=all.

[12] 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.

[13] 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.

[14] Thibault de Balthasar and Julio Hernandez-Castro. "*An Analysis of Bitcoin Laundry Services*". In: *Nordic Conference on Secure IT Systems*, **2017**: 297–312.

[15] Ayush Singh Panwar. "*Asymmetric Key Cryptography*". *Browser Download This Paper*, **2014**.

[16] Don Johnson, Alfred Menezes and Scott Vanstone. "*The elliptic curve digital signature algorithm (ECDSA)*". *International Journal of Information Security*, **2001**, *1*(1): 36–63.

[17] 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.

[18] 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.

[19] The Bitcoin Core developers. *Base58*, **2009**. https://github.com/bitcoin/bitcoin/blob/master/src/base58.cpp.

[20] *The Large Bitcoin Collider*. https://lbc.cryptoguru.org.

[21] Android Developers Blog. *Some SecureRandom Thoughts*, 2013-08. https://android-developers.googleblog.com/2013/08/some-securerandom-thoughts.html.

[22] bitcoin.org. *Android Security Vulnerability*, 2013-08. https://bitcoin.org/en/alert/2013-08-11-android.

[23] BurtW. *Bad signatures leading to 55.82152538 BTC theft*, 2013-08. https://bitcointalk.org/index.php?topic=271486.0.

[24] 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.

[25] Ron Rivest. "*Rc4*". *Applied Cryptography by B. Schneier, John Wiley and Sons, New York*, **1996**.

[26] Ronald L Rivest. "*The RC5 encryption algorithm*". In: *International Workshop on Fast Software Encryption*, **1994**: 86–96.

[27] RL Rivest, MJB Robshaw, R Sidney *et al. The RC6 block cipher. v1. 1, August 20, 1998*, **2016**.

[28] Data Encryption Standard. "*Data encryption standard*". *Federal Information Processing Standards Publication*, **1999**.

[29] American Bankers Association *et al.* "*Tripple Data Encryption Algorithm Modes of Operation*". *ANSI X9*: 52–1998.

[30] Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, **2013**.

[31] Ronald L Rivest, Adi Shamir and Leonard M Adleman. *Cryptographic communications system and method*. Google Patents, 1983-9 20.

[32] Neal Koblitz. "*Elliptic curve cryptosystems*". *Mathematics of computation*, **1987**, *48*(177): 203–209.

[33] Nicholas Jansma and Brandon Arrendondo. "*Performance comparison of elliptic curve and rsa digital signatures*". *nicj. net/files*, **2004**.

[34] Léo Ducas, Alain Durmus, Tancrède Lepoint *et al.* "*Lattice signatures and bimodal Gaussians*". In: *Advances in Cryptology–CRYPTO 2013*. Springer, **2013**: 40–56.

[35] Addy Yeow. *Global Bitcoin Node Distribution*. https://bitnodes.earn.com/.

附录 A　附件

pkuthss 文档模版最常见问题：

`\cite`、`\parencite` 和 `\supercite` 三个命令分别产生未格式化的、带方括号的和上标且带方括号的引用标记：**test-en**，**[test-zh]**、[test-en, test-zh]。

若要避免章末空白页，请在调用 pkuthss 文档类时加入 openany 选项。

如果编译时不出参考文献，请参考 `texdoc pkuthss`“问题及其解决”一章“其它可能存在的问题”一节中关于 biber 的说明。

致谢

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，大力鼓勵者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。段莉華老師也想當支持我做學術研究，也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較無經濟壓力，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.”，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。感謝李開輝教授願意接受我在旗下做科學研究。

除了在諸位教授的敦敦教誨中，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，沒有他沒有現在多達三萬四千人的比特幣中文社團的社群，也不會使我有這樣的機會了比特幣的運作原理，更不會有現在的台灣比特幣產業鍊，奠定區塊鏈在台灣的技術產業基礎。

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