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、實名支付給匿名在知發給時名，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

現貨法定貨幣，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。為解決現金法定貨幣，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）

1.3　密碼貨幣的優勢

1.4　密碼貨幣的劣勢

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）[8]、簽章密碼學（Signature cryptography）、零知識證明密碼學（Zero Knowledge Proof Cryptography）[9]、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）

2.2.1　比特幣地址生成相關函數

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[10]、SHA-256（哈希函數）[11]、RIPEMD-160（哈希函數）[12]、Base58[13]。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 [14] 也有團隊正在努力的窮舉比特幣 2^{256} 的組態空間。

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”[15]，Bitcoin.org 也發布了警告 [16] 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 [17]，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

SHA-256

RIPEMD-160

Base58

2.2.2 比特幣地址生成過程

生成私鑰

生成公鑰

生成公鑰 **SHA-256**

生成公鑰 **SHA-256** 的 **RIPEMD-160**

對公鑰 **SHA-256** 的 **RIPEMD-160** 再做兩次 **SHA-256** 前 **32bit** 的值作為校驗碼

取得版本號

版本號、公鑰 **SHA-256** 的 **RIPEMD-160** 和校驗碼合併

合併的結果以 **Base58** 編碼

2.2.3 多重簽名（Multi-Signature）

多重簽名地址

Green Address

2.3 區塊鏈（Blockchain）

2.3.1 本區塊大小的值

2.3.2 區塊頭（Block Header）

區塊版本（**32 bits**）

前區塊的哈希值（**256 bits**）

Merkle Root（**256 bits**）

難易度（**32 bits**）

時間戳記（**32 bits**）

Nonce（**32 bits**）

2.3.3 Block Data

交易計數器（**4-36 bits**）

交易信息

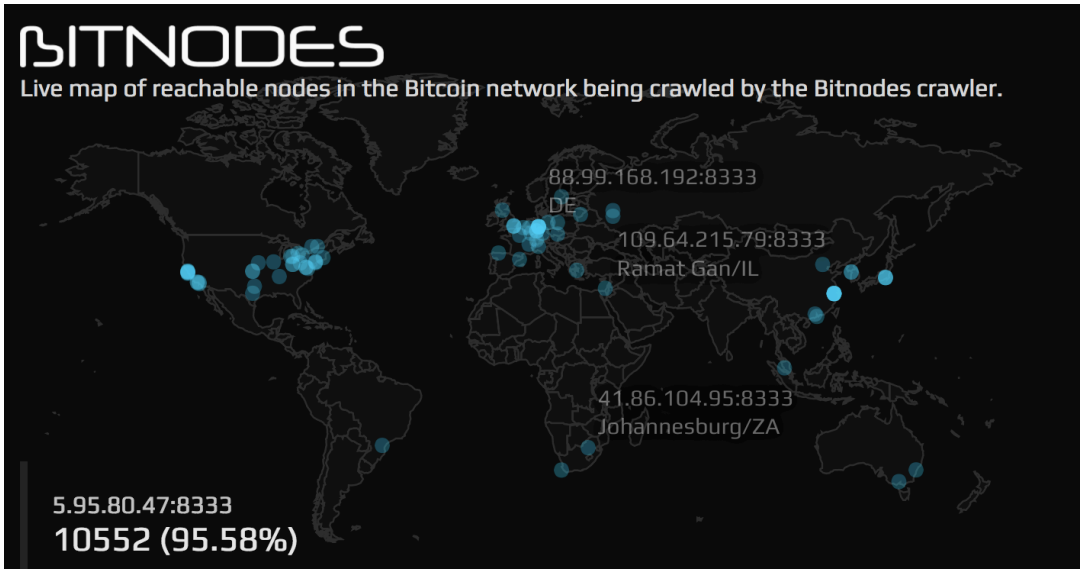

图 2.1　Bitcoin Full Node[18]

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2.1所示，截至 2018 年 1 月 25 比特幣網路中全節點數量為 10552 個 [18]，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。

2.6　山寨幣（Altcoin）簡介

2.6.1　萊特幣（Litecoin）

2.6.2　狗幣（Dogecoin）

2.6.3　域名幣（Namecoin）

2.6.4　以太坊（Etherum）

第三章　交易模型分析

3.1　現金交易模型

3.1.1　匿名客戶對匿名商家

3.1.2　匿名客戶對實名商家

3.2　電子貨幣交易模型

3.2.1　實名客戶支付實名商家

3.2.2　實名客戶透過實名第三方再實名商家

3.2.3　實名客戶透過匿名第三方再實名商家

3.3　密碼貨幣交易模型

3.3.1　匿名客戶對匿名商家

3.4　各種交易模型比較

第四章　比特幣交易監督系統設計

第五章　多重簽章優化比特幣交易監督系統

第六章　比特幣監督系統實作

第七章　支持其他密碼貨幣至本系統的評估

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：19，[20]、[19,20]。

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

[9] 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.

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

[11] 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.

[12] 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.

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

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

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

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

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

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

[19] Author. "*Title*" [J]. *Journal*, 2014-04-01.

[20] 作者。"标题"[J]。期刊，2014-04-01。

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：19，[20]、[19,20]。

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