一個集中管理的電子支票系統模型

沈曉芸
交通大學資訊管理研究所

黃景彰
長庚大學資訊管理研究所

摘要

紙張支票是企業間商業交易最常使用的付款工具之一，故使用數位化的電子支票作為連線付款的工具也能更符合傳統的商業習慣。然而，數位化的支票在流通的過程中卻可能會遭到被複製或篡改的風險。使用密碼學中的數位簽章技術讓收票人能夠鑑別數位支票的來源，並驗證它的真確性，但卻無法保證支票不被複製。若要避免被複製的風險，需要重新思考數位化支票系統的運作流程。

本文在深入探討、研析現行已發展之電子支票系統的運作機制之後，自系統流程的角度重新思考，結合證券市場之有價證券的集中保管作業方式，設計一「集保型」的電子支票系統模型，儘量避免支票在市場上流通，以降低電子支票因數位文件本身的可複製特性所帶來的風險，並融合資訊安全觀點與現有支票業務，建構一個能支援多種商業模式的連線付款工具之基本模型，使企業與消費者皆能更便利且有效率地進行網路商業活動。

關鍵字：電子支票、集中保管、電子付款

A New Central-Deposit Electronic Check Model

Hsiao-Yun Shen
Institute of Information Management, National Chiao Tung University

Jing-Jang Hwang
Department and Graduate Institute of Information Management, Chang Gung University

Abstract

Digital checks are more attractive than other means of on-line payment, because checks in the traditional paper form are very popular in business. However, the risk of duplication fraud is a major concern. Cryptography, including the technology of digital signature, allows recipients of digital checks to authenticate the signatory and to validate data integrity. But using cryptography offers no guarantee that duplication frauds can be avoided or detected.

This paper studies the electronic check systems presently in use in United States and Taiwan, and then proposes a "central-deposit" electronic check system model. The basic idea was obtained from observing the central depository system for equity securities in Taiwan. By including a "Central Payment Center (CPC)" into the proposed model, electronic checks generated are registered and kept at a location instead of being circulated. The major benefits of our Central Depository Model include reduction of both cost and risk.

Keywords: electronic check, central depository model, digital signature, cryptography, risk management of payment systems.

壹、前言

2000 年中開始發生的網路股災使得許多的網路公司 (dot-coms) 陷入經營上的重大危機，電子商務的發展似乎也陷入了低潮。但根據市場研究公司 Ipsos-Reid 以十二個國家為樣本的調查研究指出，54%受訪者有連網行為，在上網族群中 62%曾經在網路上購買商品及服務 (劉芳梅，民 92)，這顯示人們已透過網際網路將生活與商務活動緊密地串接在一起；網路銀行、網路下單、線上購物、企業快速回應系統、供應鏈管理、客戶關係管理等已成為電子商務的主要應用。2003 年 5 月份的商業周刊也專文報導了電子商務的蓬勃生機 (Mullaney, 2003)。而無論是傳統或是電子化的商業活動中，金融服務都是不可缺少的必備條件，如何使得金流能夠順暢的運轉，已成為重要的課題。

目前，在電子商務這個發展迅速的領域中，已有多樣化的連線支付工具可用於網路化的商業交易。其中，有將信用卡號碼連線傳送用於指示付款、有類似於傳統使用的現金、也有透過上網連線遞送訊息，指示銀行轉帳以支付水電、瓦斯等費用、或有類似於傳統的紙張支票等。在眾多的支付工具中，支票是企業間商業交易最常用的付款工具，它具有避免支付現金之煩擾以及減少通貨計算錯誤等優點，故使用數位化的電子支票作為企業間連線付款的工具或許會更符合傳統的商業習慣。此外，一般消費者也可以在信用卡之外，尋求另一個有效、安全、低風險的付款方式。有鑑於此，美國 FSTC (Financial Services Technology Consortium) 已於 1998 年發展 eCheck 計畫，試圖在美國原有的法律架構與商業實務之下，建構一個完全電子化的支票系統 (www.eCheck.org)。而我國也在「知識經濟發展方案具體執行計畫」中規畫了「發展電子支票計畫」的子計畫 (行政院經濟建設委員會，民 89)，此計畫已在中央銀行與台北票據交換所的積極投入下，從初始的研發進入實施的階段 (傅沁怡，民 92)。

一般來說，一張支票自簽發經背書 (轉讓) 到提示 (取款) 為止，會在付款人、收款人、與銀行之間流通，在流通的過程中，可能會遭受被盜用、複製、或遺失的風險。舉例來說，一份被複製的電子文件是肉眼、甚至是電腦系統無法察覺的，最終，一張電子支票是否有效必須由銀行來決定，無效的支票會被銀行退票，也就是說，支票持有人必須承擔支票遭盜用或複製的風險。因此，本文的目的即在於深入探討、研析現行已發展之電子支票系統的運作機制，自系統流程的角度重新思考，結合證券市場之有價證券的集中保管作業方式，設計一「集保型」的電子支票系統模型，儘量避免支票在市場上流通，以降低電子支票因數位文件本身的可複製特性所帶來的風險，並融合資訊安全觀點與現有支票業務，建構一個能支援多種商業模式的連線付款工具之基本模型，使企業與消費者皆能更便利且有效率地進行網路商業活動。

貳、文獻探討

臺灣行政院經濟建設委會 (民 89) 所擬之台灣知識經濟發展方案具體執行計畫中對電子支票之定義為，「電子支票係將實體支票之作業方式，改以電子方式處理，並將票據無實體化，且使用電子簽名作背書，以數位簽章來驗證付款者、付款銀行和銀行帳號。有關電子支票之認證工作係由公開金鑰密碼法（Public Key Algorithm）的電子簽章完成，以增加其安全性。」美國電子付款協會 (The Electronic Payments Association) 則廣泛地將任何付款流程始於紙張或其他型式的支票，而將其記載的資訊以電子化的方式處理者統稱為電子支票 (Electronic Check Council, 2001)。而美國 FSTC 所發展的 eCheck 系統所稱的電子支票係指以電子化的型式表示紙張支票 (Anderson, 1998)。本研究整理我國與 FSTC 對電子支票的定義，認為電子支票是將傳統紙張支票及其作業電子化，由付款人對收款人簽發數位化的支付指令，透過網路來完成傳統支票的所有功能。以下分別就傳統紙張支票與電子支票系統的運作流程加以探討。

一、傳統紙張支票

臺灣之票據法對於支票有明確的定義與規範。根據票據法第四條：「稱支票者，謂發票人簽發一定之金額，委託金融業者於見票時，無條件支付與受款人或執票人之票據。前項所稱金融業者，係指經財政部核准辦理支票存款業務之銀行、信用合作社、農會及漁會。」票據法第一二五條則規定了支票應載之事項 — (1)表明其為支票之文字 (2)一定之金額 (3)付款人商號 (4)收款人姓名或商號 (5)無條件支付之委託 (6)發票地 (7)發票年、月、日 (7)付款地，並由發票人簽名。(王毓仁，民 85)

一般支票流通應用的過程係由發票（簽發）經背書（轉讓）到提示（取款）為止，其流程如圖 1 所示。

使用支票替代現金的收付，可以免除巨額現鈔點收之不便，減少處理錯誤的情形；其延遲付款的特性，可便利工商業資金週轉，作為企業的信用工具；此外，當支票遺失、遭竊、或損 時，尚可申請掛失止付，較現金來得安全許多。然而，紙張支票在使用上仍然遭遇到許多難題，若能發展電子化支票，將可改善所面臨的問題。茲說明如下 (蕭曉玲、黃景彰，民 92)：

- 隨著社會進步，商業交易發達，支票使用量亦日益增加，使得紙張支票之作業疏失隨之增加。此外，支票交換量也因此不斷擴大，使得票據交換所負荷過重，而易產生管理漏洞。
- 企業以人工處理紙張支票，除了較費時費力，也無法將付款資訊與企業內部資訊系統整合。若適當地使用電子支票，將可提昇 B2B 電子商務金流效率。
- 使用電子支票系統，應可大幅減少紙張支票的使用疏失、偽造、或遺失等多項導致退票的情況。

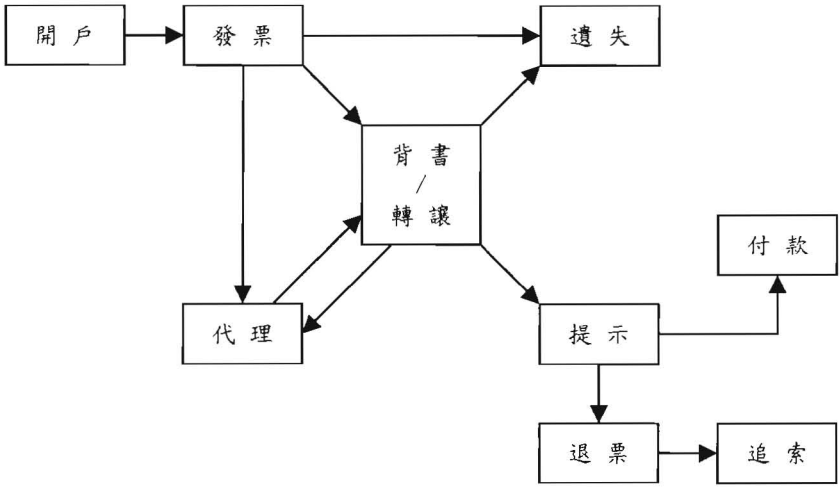

圖1：支票流通過程 (王毓仁，民 85)

二、電子支票系統

美國 FSTC 所發展的 eCheck 系統是電子支票系統的典型代表(Anderson, 1998)，此系統的架構完全模仿美國現有紙張支票的運作流程，因此可依循其現行的法律規範與商業實務，而不必建立任何新的付款工具。eCheck 的基本運作方式如圖 2。

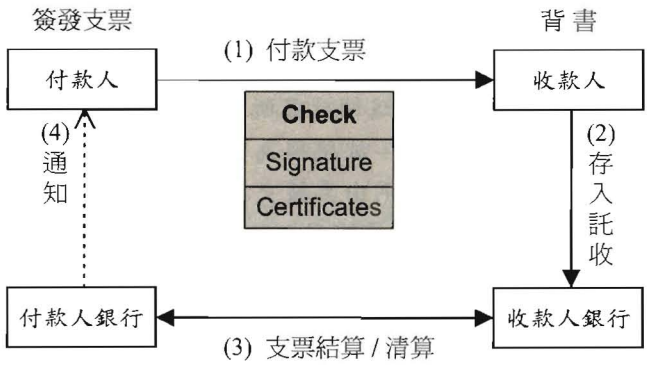

圖2：eCheck 系統基本運作流程

系統中包括付款人、收款人、付款人的銀行、與收款人的銀行，使用 eCheck 系統的用戶，必須在銀行開立一個電子支票的存款戶，銀行會與此存款戶簽訂一個一般的定型化契約，明定電子支票所適用之現行有關於支票的法律依據。在技術上，eCheck 系統使用數位簽章以確保資料的來源，以及資料未遭受到非經授權的篡改或偽造。此系統發展過程中所遵循的文件發展技術是 FSML (Financial Service Markup

Language)，透過這個標準的規範，不同的廠商、銀行都能夠理解支票的內涵。利用 FSML 所撰寫的支票是一個複合式的文件，其允許支票本體加上其他相關的商業文件(例如發票、信用狀等) 一併流通，再依情況適當地加以拆解。但就簽章來說，在流通過程中可以抽換的複合式文件會造成一些困擾，因此在技術上必須有一些創新，而複合文件的簽章技術正是這個系統的重要貢獻之一。此外，美國聯邦已於 2000 年 6 月通過「全球暨國家商務電子簽章法」(Electronic Signatures in Global and National Commerce Act)，可為系統使用之法律依據。

除了以數位簽章密碼技術為基礎的 eCheck 系統外，有一個更早的是美國南加大應用對稱式密碼方法所發展的 NetCheque 系統 (Neuman & Medvinsky, 1995)。NetCheque 的觀念是一個類似支票付款的分散式帳戶服務系統，在整個系統中，由若干個帳戶伺服器 (accounting server) 負責管理使用者帳戶，收付款雙方必須在系統中設立帳戶，付款人可以簽發一份包含付款人姓名、財務機構 (如銀行) 名稱、付款人帳戶名稱、收款人名稱、以及付款金額的電子文件，這份文件同時承載付款人所簽署的電子簽名；當收款人收到此份文件後，必須在文件上背書簽名，方可兌現。NetCheque 系統是以 Kerberos 鑑別系統 (Neuman & T'so, 1994) 的票證 (ticket) 為基礎進行簽名與背書，由於應用對稱式密碼學方法，節省了公開金鑰密碼系統所需的高昂成本，這個系統可用於小金額的商業交易及資金往來的活動，但它到目前仍然止於實驗室的學術研究計畫，並未發展成為實用的商業系統。

我國中央銀行為解決電子商務金流問題，於民國 89 年 12 月提出「發展電子支票計畫」，由台灣票據交換所與數家銀行共同規畫、建置電子票據各項業務規範與系統，希望能提昇全國支付系統的效率。在法令依據上，票據交換所依據我國「電子簽章法」第四條第二項及第九條第一項訂定「金融業者參加電子票據交換規約」與「電子票據往來約定書」(範本)，以及金融業者與客戶間相關之業務規範為電子票據系統之法律基礎 (臺灣票據交換所，民 92)。由於這個計畫所開發的系統之處理標的除支票外，尚包含了銀行擔付本票與銀行承兌匯票，故統稱為電子票據系統，本系統的特點在於空白票據置於銀行端，而已簽發之票據則由票據交換所採集中登錄之保管方式其基本交易流程如圖 3 所示。以支票為例，電子票據系統的使用者必須先至銀行辦理支存開戶，並取得以 IC 卡為載具的數位憑證 (digital certificate) 及私密金鑰 (private key)，簽發支票及存入託收的作業都是在銀行網站端進行作業。

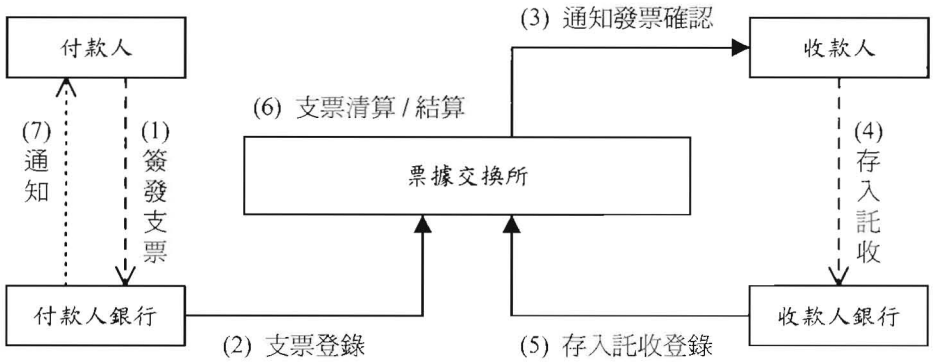

圖3：臺灣電子票據系統基本運作流程

綜觀以上所述的幾個系統，Netcheque 系統使用之密碼技術為對稱式密碼學方法，但並未進入實用的階段。其餘二者皆是以使用數位簽章 (digital signature) 為基礎，且分別已經 (或準備) 進入實用的階段，表 1 為 eCheck 與臺灣電子票據系統的比較。

表1：eCheck 系統與臺灣電子票據系統

	eCheck 系統	臺灣電子票據系統
處理標的	支票	支票、銀行擔付本票、銀行承兌匯票
密碼技術	數位簽章	數位簽章
文件格式	FSML (Financial Markup Language)	XML (eXtended Markup Language)
開票方式	空白支票置於付款人的 IC Card，由付款者的系統端開票	空白支票置於銀行端，付款人登入銀行網站簽發支票
支票保管	執票人	票據交換所

分析這兩個系統，可以發現兩者最大之差異在於 eCheck 系統使用的電子支票係以複合式的數位文件在收付款雙方及銀行間流通，未兌的支票由執票人保管，而臺灣電子票據系統中的電子支票則由票據交換所集中登錄與保管。前者的優勢在於系統中的參與者與紙張運作的模式完全相同，參與者扮演的角色也沒有任何的改變，符合一般使用者的使用習慣，但在收付款人之間流通的電子票據可能會有遺失或被複製之虞。而後者所開立的支票由票據交換所統一管理，不會在付款者與收款者之間流通，所要承擔的風險較低，但是票據交換所卻必須身兼票據交換與保管兩種角色，使得原參與者間彼此的互動與作業流程有所改變。故，本研究的目的在於設計出能兼具兩個系統優勢的電子支票系統模型。

參、一個加入公證第三者的集保型電子支票系統模型

要降低電子支票因數位文件本身的可複製特性所帶來的風險，集中保管模式是一個較佳的選擇，但是臺灣電子票據系統中的票據交換所卻缺乏角色的獨立性。比較圖4中同樣為集中保管模式的臺灣有價證券管理作業（臺灣集保公司，2003），可以發現，臺灣證券集中保管公司只負責有價證券的管理，而未涉及與證券交易相關的參與角色(如投資人、證券商、證券金融公司、或上市公司等)，也就是說，集保公司所扮演的角色是單一的。

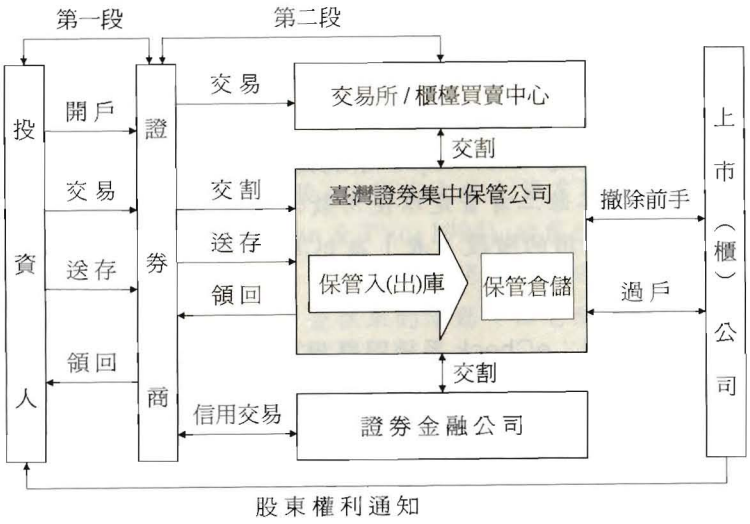

圖4：臺灣有價證券管理之集保作業模式（臺灣集保公司）

為了能在降低風險的同時，也能維持系統中原有參與者角色之獨立性，本研究參考臺灣有價證券管理之集保作業模式設計一稱為「集中支付管理中心」(Central Payment Management Center; CPC) 的可信賴第三者 (TTP, Trusted Third Party)，獨立負責支票的集中保管作業，以避免角色上的重複。圖5為參考 eCheck 系統、臺灣電子票據系統、與臺灣有價證券管理之集保作業模式所設計的集保型電子支票系統模型之示意圖。

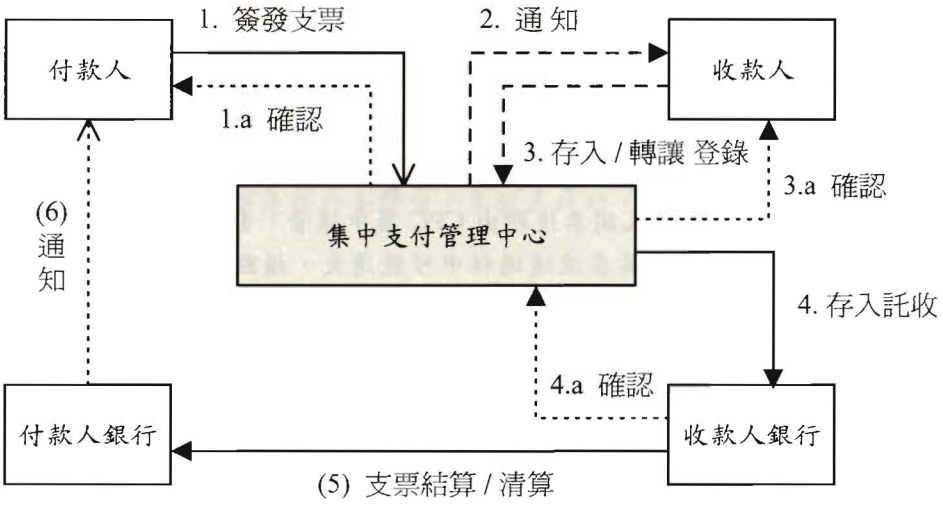

圖5：加入集中支付管理中心之集保型電子支票系統模型

在本研究所設計的模型中，付款人必須先在付款人銀行開立支存帳戶，由付款人事先在銀行取得具有銀行識別碼的空白支票，儲存在 IC 卡中，也就是說，以 IC 卡作為電子支票簿。此外，收付款雙方皆必須登錄成為 CPC 的會員，由「集中支付管理中心」(CPC) 負責支票的集中保管作業，支票必須由 CPC 的簽證後，才具有支付的效力。

此系統模型之運作流程說明如下：

1. 付款人由付款人系統簽發支票，傳送給 CPC。電子支票所記載的內容應與紙張支票應記載的事項相同，並附加收票人的電子郵件地址等資訊。

1.a CPC 發送確認訊息給付款人。此確認訊息可作為發生爭議時的證據，故其內容應包涵依循的安全政策、CPC 與付款人的唯一識別、簽發票據的日期與時間等資訊，並由集中支付管理中心簽章。

1.b CPC 在支票上附加其簽章，入庫保管。未來，銀行在支付款項時，必須驗證此簽章以確認支票的真實性。

2. CPC 依據付款人所提示的收款人資訊 (如電子郵件地址或住址等) 通知收款人。

3. 收款人登入 CPC 進行存入或票據轉讓登錄的作業。同樣地，收款人必須登錄成為 CPC 的會員。在此，先簡單地以存入登錄為例。在這個處理過程中，收款人會在支票上加上他的簽章。

3.a CPC 發送確認訊息給收款人。這個訊息是由 CPC 簽章的一項證據。其內容包涵依循的安全政策、CPC 與收款人的唯一識別、存入託收的日期與時間等資訊。

3.b CPC 進行支票所有權移轉的維護作業

4. CPC 針對各個銀行，整理出存入託收的清單，並將支票存入收款人銀行。

4.a 收款人銀行開立收到支票的證明給集中支付管理中心。

5. 收款人銀行與付款人銀行之間透過票據交換所進行票據交換與清算的作業。

6. 付款人銀行對付款人帳戶進行扣款，並通知付款人。

在此模型中，支票自付款人開票後即由 CPC 集中保管，支票本身不會在收款人與付款人之間流通，因而可避免其在流通過程中可能遺失、損毀、或被複製的風險。同時，由於票據集中處理，可以提高票據的處理速度。就系統的實際應用面來看，由於本模型使用之密碼技術為數位簽章，故可以相關的電子簽章法案為法律依據，使原來應簽名或蓋章之處，由相對人同意後，以數位簽章為之；此外，由於在本模型中，票據交換所與銀行之間之作業程序完全與紙張支票相同，故不需要另外訂立新的法規，惟應就集中支付管理中心之作業加以規範。

另外，由集中支付管理中心作為獨立的公正的第三方機構 (可信賴的第三者)，可以同時建立、紀錄與管理交易證據，當有因交易而引起的糾紛或爭議發生時，集中支付管理中心還可以作為爭議解決的機構。使得支票的支付處理可以更安全、更快速的進行。

分析與討論

本文所提出之集保型電子支票系統模型乃是深入研析美國之 eCheck 系統、臺灣電子票據系統，就系統與作業流程的角度重新思考後建立。茲就以下幾個方向與前述兩個系統作一比較與分析。

- **安全性：**

  在本模型中，電子支票的真確性可以透過數位簽章來達成，與其他兩個系統相同。再就支票在流通的過程可能遭受的各項風險來看，由於支票是由 CPC 集中保管的「集保型」系統，而 eCheck 系統是屬於「流通型」的系統，因此，所承擔的風險將較 eCheck 為低。相較於同於集中保管型的臺灣電子票據系統，雖然本模型電子支票簿是由付款人自行保管，但是由於支票必須由 CPC 簽證後才具有支付的效力，因此不必擔心支票由付款人流向 CPC 時可能遺失或被複製的問題。此外，透過本模型所設計的集中支付處理中心，尚可提供「爭議解決」的資訊安全服務。故，本系統模型的安全性是優於 eCheck 系統而與臺灣電子票據系統相同的。

- **責任分工：**

  eCheck 系統基本上完全仿照紙張支票系統的運作模式，因此，在 eCheck 系統中，支票處理過程中的各個參與角色的互動與原來完全一樣，並沒有任何的更動。而在臺灣電子票據系統中則有較大的變革 — 票據交換所除票據交換的業

務外，同時要負責支票的集中登錄與保管，此作業範圍的變革，使得銀行與票據交換所之間的互動也有所不同，因而使得角色之間比較缺乏獨立性。由於票據交換所本來就是支票交易過程中的參與個體，本文認為其應維持角色的單一功能，透過集中支付處理中心的設立，可將票據交換與支票保管的業務各自獨立，原本銀行與票據交換所之間的作業體系也不必有任何變動。故就責任上的分工來看，本模型是優於臺灣電子票據系統的。

- **成本：**

本模型與 eCheck 一樣，採用 IC 卡作為電子支票簿與金鑰的載具，因此各個參與者必須建置能夠使用的系統。付款人必須建置開票系統，銀行必須建置驗證系統。而在臺灣電子票據系統中，開票人必須登入銀行網站進行開票的動作，故付款人端僅需安裝簽章軟體，而不必建置開票系統，但是銀行端必除驗證的工作外，必須建置供客戶使用的開票系統，而收款人銀行也必須建置供收款人進行存入託收作業的系統。故就成本面來看，本文認為各個架構皆必須負擔一定的系統建置成本，差異應不是很大。

- **企業機會：**

只要能夠具有足夠的公正性，集中支付處理中心可以由私人機構來成立，也可以是一個營利事業。舉例來說，一些線上爭議解決機制 (Online ADR) 的公司，如 Cybercourt、BBBOnline 等，或是數位憑證機構，如 Verisign 等；這些機構皆是從事公正第三者業務的營利單位。故集中支付處理中心的設計，尚提供了新型商業模型的發展機會。

就以上的層面來看，本系統模型可以說是集合了 eCheck 系統與臺灣電子票據系統的優點，而改進了他們的缺點。

結論

透過深入研析現行的電子支票系統，並參考有價證券的集保作業模式，本論文所規畫的集保型電子支票系統模型，經由對電子支票的集中保管方式，避免了在流通型的 eCheck 系統可能遭遇的風險 — 數位文件本身的可複製性所帶來的風險，以及支票在流通過程中可能會遺失或毀損的風險。同時，透過設立集中支付管理中心，可以儘量不需更動銀行與票據交換所中的作業流程，也解決了臺灣電子票據系統中所欠缺的參與角色的獨立性問題。在不需承擔較高成本的情形下，本模型可說為電子支票的運作提供了一個更佳的解決方案。

本系統模型也融合了資訊安全觀點與現有支票業務，建構一個能支援多種商業模式的連線付款工具之基本模型，未來，可經由進一步的規畫集中支付處理中心的資料庫設計等細部系統實作相關工作，繼續朝實作本模型的系統雛型努力，使企業與消費者皆能更便利且有效率地進行網路商業活動。

參考文獻

1. 王毓仁，民 85，支票使用實務。書泉。
2. 行政院經濟建設委員會，民 89 年，知識經濟發展方案具體執行計畫－發展電子支票計畫，於民國 91 年 7 月 25 日由 http://www.aproc.gov.tw/kbe/3/0119/03.doc 取得。
3. 財政部金融局，民 88 年，個人電腦銀行業務及網路銀行業務服務契約範本。於民國 89 年 4 月 25 日，由 http://www.boma.gov.tw/8872563-1.htm 取得。
4. 傅沁怡，民 92 年 9 月 11 日，電子票據 29 日上路。經濟日報。於民國 92 年 9 月 25 日，由 http://archive.udn.com/2003/9/11/NEWS/FINANCE/FIN3/1555156.shtml 取得。
5. 臺灣票據交換所，民 92，電子票據簡介。於民國 92 年 9 月 20 日，由 http://www.twnch.org.tw/echeck/index.html 取得。
6. 臺灣集保公司，有價證券管理。於民國 92 年 8 月 30 日由 http://www.tscd.com.tw/index_main_03service01.htm 取得。
7. 劉芳梅，民 92 年，線上金融服務逐漸普及。於民國 92 年 8 月 25 日，由 http://www.find.org.tw/0105/news/0105_news_disp.asp?news_id=2480 取得。
8. 蕭曉玲，民 92 年，電子支票應用運作機制。國立交通大學資訊管理研究所碩士論文。
9. Anderson, M. M. (1998). The electronic check architecture. Retrieved September 15, 2000, from the World Wide Web: http://www.echeck.org/library/wp/ArchitectualOverview.pdf
10. Electronic Check Council. (2001). Electronic check glossary. Retrieved September 15, 2002, from the World Wide Web: http://ecc.nacha.org/resources/Electronic_Check_Overview.ppt
11. Mullaney, T. J. (2003). The E-BIZ surprise. Business Week, 3832, 60-60.
12. Neuman, B. C., & T'so, T. Y. (1994). Kerberos: an authentication service for computer networks. IEEE Communications magazine, 32(9), 33-38.
13. Neuman, B. C., & Medvinsky, G. (1995). Requirements for network payment: The NetCheque perspective. Digest of Papers on Technologies for the Information Superhighway, Compcon '95, 32-36.