申請日期	88.9.17
案號	88116514
類別	G06F 17/60

（以上各欄由本局填註）

A4
C4

446898

發明 ~~新型~~ 專利說明書

一、發明 ~~新型~~ 名稱	中文	銷售據點裝置之可查證電子帳目及使用該電子帳目之方法
	英文	"VERIFIABLE ELECTRONIC JOURNAL FOR A POINT OF SALE DEVICE AND METHODS FOR USING THE SAME"
二、發明 ~~創作~~ 人	姓名	1.艾伯托 古斯塔夫 剛薩勒斯 康德 2.羅勃 史考特 佛登貝瑞 3.偉恩 羅傑 忽卡畢
	國籍	1.阿根廷　　2.3.均美國
	住、居所	1.美國北卡州拉利市林湖路4141號305棟 2.美國北卡州拉利市北界域街515號 3.美國北卡州拉利市盆地湖路7216號
三、申請人	姓名（名稱）	美商萬國商業機器公司
	國籍	美國
	住、居所（事務所）	美國紐約州阿蒙市新果園路
	代表人姓名	傑拉德 羅森賽

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有　□無主張優先權
美國	1998年09月30日	09/164,215	☑有　□無主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（ 1 ）

發明領域

本發明大體上於有關銷售據點系統，特別是於有關以交易爲基礎的裝置之帳目。本發明進一步於有關使用銷售據點系統的方法。

發明背景

面對面零售交易發生在銷售據點，或通稱爲結帳線或收銀台。客户就是在這個位置支付所購買的貨物，通常以現金、支票、信用或簽帳卡。爲了要完成銷售，許多零售商人目前使用電子裝置來幫助並提供交易記錄。此種銷售據點系統可能包括一掃描器以讀取編碼的產品資訊、一終端機以手動輸入交易資訊及貨幣的儲存、一顯示器供顯示交易資訊、以及一列表機用來產生一書面紀錄或業務帳目及列印收據給客户。

所購買的每個項目之銷售價格係典型地記入銷售據點終端機之內，其做爲結帳程序的一部份。每個項目價格和總數由銷售據點列表機列印在客户收據上，而且也可以由相同銷售據點列表機列印在一分開的帳目上。通常也決定稅額，且列印在客户收據上。然後從列表機提供客户收據給客户。

於雙站台銷售據點列表機中，第二列表機站保存所有銷售交易之帳目記錄。此提供稽核銷售活動之書面記錄，例如總銷售額及於帳目記錄所涵蓋之帳目週期期間收取的稅金。舉例來說，此資訊能讓稅賦當局用來判定零售商是否已經將所有從客户收取的稅金提交給稅賦當局。

五、發明說明（ 2 ）

政府主管當局對零售帳目資訊有興趣之處，例如透過增值稅法或營業稅法，各別的稅法經常定義列印收據的格式和內容並頒佈銷售資料取得之安全方法。已知回應此種會計的需求係提供一會計列表機—例如紐約亞蒙克的萬國商業機器公司的3F列表機。對此種會計列表機，帶有專用的非揮發性隨機存取記憶體(NVRAM)和電子可程式唯讀記憶體(EPROM)的安全(也就是，防搗或防禦牆)邏輯卡，可實體地和邏輯地設置在銷售據點終端機與產生客户收據及帳目記錄的銷售據點列表機之間。

對像是3F型之會計列表機而言，銷售據點終端機可連接到一會計本部裝置，其對銷售據點列表機是保密的，且藉由例如序列通訊鏈結之通訊鏈結而控制所有列印功能。此種會計本部的一個例子在圖1舉例說明。銷售據點終端機10在通訊鏈結22上連接到會計本部24。會計列表機20依序包括會計本部24和二站台列表機26兩者。會計本部24包括一會計處理器28或其他控制裝置，以控制帳目和列印運作。會計本部24進一步包括一電池支援之(非揮發)隨機存取記憶體30，以儲存於一帳目週期期間之中間銷售和稅額總數。如圖1所示，會計本部24進一步包括一分開的程式EPROM 32和會計記憶體EPROM 34。分開的會計記憶體EPROM 34係提供於環氧基樹脂包裝中以永久儲存資料，其依據會計記憶體EPROM 34的容量而定，通常包括每日銷售和一些天數的每日帳目期間之課稅總額。然後程式EPROM 32可用來規劃會計處理器28所使用的資訊或

五、發明說明（ 3 ）

資料值。在圖1也顯示的是日鐘36的時間，它可用來做爲追蹤交易和帳目期間。

二站台列表機26由會計處理器28控制。一第一列印站台提供一客户收據站台，其列印由會計處理器28控制，以確保提供給客户的銷售收據上有與一特定交易相關之正確資料。第二站台提供一帳目站台，其透過交易銷售資料和每日報告記錄交易。典型地，來自列表機26的帳目站台之書面帳目接續地按照各種稅務當局的會計法儲存以供稅賦稽核之用。

許多有會計稅法的國家已經表示對用數位電子帳目記錄替代目前帳目紙帶儲存之系統有興趣。如此之轉變能夠爲零售商減少設備、消耗品、處理記錄及儲存成本。其能允許使用單一站台較低成本列表機和減半之紙張消耗。雖然零售商和會計主管當局兩者都能體認電子帳目的潛在優點，對此種電子帳目檔案可由意圖欺騙政府之終端使用者輕易地改變仍有持續的憂慮。

一種亦仰賴會計列表機裝置方式，但使用電子帳目之提議解決方案已被提出。這方式利用從在會計保全的記憶體中所儲存的所有資料，使用在會計列表機外所不知道的金鑰計算出之檢和(checksum)。然後整個帳目資料區塊可以從會計本部24傳送到一銷售據點終端機10，而非保存於安全的會計列表機中。然而，此方式不足以處理所有此種可驗證電子帳目系統的目標。舉例來說，要使銷售據點終端機中的資料有效，資料必須回授至會計本部，其中可從

五、發明說明（ 4 ）

會計記憶體取得關聯之檢和並與一從銷售據點終端機下載之資料所產生的新檢和比較。此外，依來回傳送於銷售據點終端機之帳目單元的大小而定，在會計本部中可能需要一個大容量的非揮發隨機存取記憶體。除此之外，可能需要維持資料在會計記憶體EPROM裡一段更長的時間以供可能之查證，其需要增加容量的會計記憶體EPROM。最後，這方式受限於它不能輕易地允許對帳目記錄的遠端查證。

發明概要

因此，本發明之一目的係提供一種銷售據點裝置的可查證電子帳目系統，其允許對帳目資料的任何更動之偵測。

本發明之另一目的係提供此一銷售據點裝置的可查證電子帳目系統，其不需要增加在例如會計本部之列表機裝置上所包含之NVRAM或安全EPROM的大小。

本發明之另一目的係提供此一銷售據點裝置的可查證電子帳目系統，其可遠端地查證。

根據本發明之此等或其他目的係藉由一銷售據點裝置的可查證電子帳目系統而提供，其保存一電子帳目檔案以代替在一個二站台銷售據點列表機上的一帳目列印站台。交易資訊儲存在一非揮發性的隨機存取記憶體中。一資料簽章根據帳目在隨機存取記憶體的內容而決定。交易資訊和資料簽章兩者皆被轉送到分開的帳目記憶體。舉例來說，帳目記憶體可存在於銷售據點終端機上，且對帳目交易資訊之更改可藉由參考亦被轉送並保存在電子帳目檔案的資

五、發明說明（ 5 ）

料簽章而偵測。較佳地，資料簽章透過例如共用金鑰加密架構加密，且相關的公開金鑰亦從例如會計總部之裝置而傳送並儲存在電子帳目檔案中，其當交易資訊建立時會計總部追蹤該交易資訊。較佳地使用雜湊技術以使相對較小的NVRAM可用來支援對一帳目週期中一電子帳目檔案之交易資訊集合之產生。因此，資料簽章是一訊息摘要之加密版本，其係反映交易資訊的總數之變動數值，該交易資訊係在一帳目週期期間傳遞到電子帳目檔案。

於本發明之一具體實施例中，提供了一種方法用以提供一銷售據點裝置的可查證電子帳目系統。接收與交易有關的交易資訊，例如零售銷售及其銷售的稅額。交易資訊儲存在一隨機存取記憶體中，其設置在銷售據點裝置中。資料簽章係根據包含在隨機存取記憶體中的交易資訊而決定，以回應於一帳目更新事件。然後，包含在隨機存取記憶體中的交易資訊被傳送到與隨機存取記憶體分開之帳目記憶體之一第一部分中，以回應於帳目更新事件。帳目記憶體較佳地保存在銷售據點終端機中，其係經由例如通信網路而連接到銷售據點裝置。資料簽章係傳送到帳目記憶體之一第二部分，以回應於帳目更新事件。

於本發明方法態樣的進一步具體實施例中，交易資訊也被傳送到一列表機供列印，舉例來說，以印出一客户銷售收據。列表機可以是一會計列表機，而銷售據點裝置可以是整合在會計列表機中的會計處理器卡。交易資訊可包括交易的銷售量資訊，而接收交易資訊可接著根據銷售量資

五、發明說明（ 6 ）

訊計算應付稅額。或者交易資訊可包括一應付稅額。

在本發明一進一步態樣中，可產生帳目更新事件以回應於一帳目週期之完成。或者，使用一例如雜湊函數之技術，當一預先決定量的交易資訊儲存在隨機存取記憶體中時可產生帳目更新事件，且隨機存取記憶體可透過覆寫先前儲存的交易資訊而重新使用，以儲存額外的交易資訊。在一帳目週期期間可以產生許多帳目更新事件，以及接著爲了根據雜湊函數的帳目週期期間的每一帳目更新事件而重複儲存交易資訊、決定一資料簽章、傳送交易資訊、傳送資料簽章和重新使用隨機存取記憶體之運件，藉此當決定資料簽章爲一與帳目週期期間所收到的交易資訊有關之變動值時，週期地將儲存在隨機存取記憶體中的交易資訊區塊傳送到帳目記憶體。

於本發明之另一方面，安全性可透過使用一共用金鑰對資料簽章加密而提供。然後共用金鑰被傳送到帳目記憶體之一第三部分，以回應於多個帳目更新事件中至少一個。然後可查證的電子帳目系統可被稽查。對本發明的具體實施例之稽核運作使用一加密的資料簽章，包括使用帳目記憶體的第三部分中之共用金鑰解密帳目記憶體的第二部分中之資料簽章。除此之外，一驗證資料簽章係由帳目記憶體的第一部分中之交易資訊使用雜湊技術而決定。驗證資料簽章與解密的資料簽章比較，以判定在帳目週期期間在帳目記憶體的第一部分中之交易資訊是否已從隨機存取記憶體所傳送的交易資訊修改過。

五、發明說明（ 7 ）

雖然本發明在以上所描述主要與本發明的方法態樣有關，但也同時提供了系統和電腦程式產品兩者。舉例來說，提供具有一可驗證電子帳目系統的銷售據點裝置，包括用以接收交易資訊之裝置及用以判定一帳目更新事件之裝置。一隨機存取記憶體係連接到接收裝置，其係規畫以儲存交易資訊。一回應帳目更新事件之裝置根據隨機存取記憶體之內容決定一資料簽章。亦提供一帳目記憶體，其具有一第一部分被規畫以儲存交易資訊，及一第二部分被規畫以儲存資料簽章。帳目記憶體與隨機存取記憶體是分開的，且較佳地位於遠端且通信地連接到銷售據點裝置，例如經由一通信網路。提供一回應帳目更新事件之裝置以從隨機存取記憶體傳送交易資訊到帳目記憶體的第一部分，以及從用以判定一資料簽章的裝置傳送資料簽章到帳目記憶體的第二部分。

因此，本發明提供一種可用來代替列印的帳目記錄之可驗證電子帳目系統。此爲例如稅賦當局在一電腦通信網路上之帳目遠端稽核提供了降低之成本和增加之能力，而仍然維持偵測擅自變更的能力。本發明能使用已存在之硬體，例如現存的會計列表機裝置，而有利地實現。

圖式概述

圖1是傳統的會計列表機裝置之一方塊圖；

圖2是依照本發明一具體實施例可查證電子帳目之一方塊圖；

圖3係一流程圖，說明依照本發明一具體實施例而建立

五、發明說明（ 8 ）

一可查證電子帳目檔案之運作；

圖4是依照本發明一具體實施例包括雜湊之可查證電子帳目之方塊圖；

圖5是依照本發明一具體實施例一可查證電子帳目銷售據點裝置之方塊圖；以及

圖6係說明依照本發明一具體實施例驗證運作之流程圖。

較佳具體實施例之詳細說明

現在本發明將在以下參照伴隨的圖式更完整地描述，其中顯示本發明的較佳具體實施例。然而，本發明可以許多不同型式具體實施，而不應解釋成侷限於在此處所陳述的那些具體實施例；而是，這些具體實施例是提供以使這個揭露將會徹底而完整，且將可完整地將本發明的範疇傳達給熟悉此項技藝之人士。如熟於該項技藝人士將可發現的，本發明可具體實施爲方法、系統或電腦程式產品。因此，本發明可採取硬體具體實施例、軟體具體實施例或結合軟體和硬體態樣之具體實施例的形式。

本發明提供電子帳目的方法和系統，其對例如銷售和稅賦資料之列印的和帳目的交易資訊維持控制。較佳地，使用標準的資料安全性演算法而提供資料安全性。更特定地，利用一例如由RSA資料安全公司所提供的公用金鑰方法。對每一銷售據點裝置，產生一公開(公用)和一私人的金鑰，並儲存於其保全記憶體中。於例如與銷售據點裝置有關的銷售據點終端機，以銷售據點裝置(例如會計邏

五、發明說明（ 9 ）

輯電路)所控制的帳目之內容建立一電子帳目檔案。

對本發明一特定的具體實施例之電子帳目檔案或記憶體的各種部分係在圖2中說明。電子帳目檔案50包括一第一部分52，含有交易資訊的一個未加密的列示，舉例來說，交易資訊是將被列印到紙捲及/或目前會計列表機的帳目站台之資料。一資料簽章係儲存在電子帳目檔案50的第二部分54。資料簽章較佳地是用以確認來自部分52的列印資料還沒有被改變過的一加密值。一列表機公開或共用金鑰被儲存在部分56中，其係用來解密資料簽章供確認資料完整性之用。最後，在所說明的具體實施例中，一列表機序號被儲存在電子帳目記憶體50的部分58中，以確認部分56中的公開(共用)列表機金鑰對各別的裝置是正確的。因爲公開/私人金鑰加密演算法爲眾所週知，其運作將不在此處作進一步詳細描述，除非與本發明的方法和系統中共用金鑰的特定使用相關聯。

如將會在此處進一步描述，依照本發明的方法和系統之電子帳目記憶體50之使用提供一種變更-列證(tamper-evident)電子帳目。所產生的帳目資料係以一種可自由地供零售商用來產生它自己的報表以及供例如稅務當局用來稽核的方式而提供。此外，此稽核可遠端地由政府當局使用特別的公用設備、或在當地使用例如包含可查證電子帳目檔案的POS終端機之裝置實行。

本發明的運作現在將參照圖3及後續之圖6之流程圖說明。將可發現流程表圖表的每個方塊，及流程圖表裡方塊

五、發明說明（10）

的組合，可由電腦程式指令實施。這些程式指令可提供給一處理器以產生一機器，使得在處理器上執行之指令產生用以實施流程圖方塊中所指定之功能之裝置。那些電腦程式指令可由一處理器執行以引起一系列操作步驟被處理器執行，來產生一電腦實施的程序，使得在處理器上執行之指令提供實施流程圖方塊中所指定之功能之步驟。

因此，流程圖表的方塊支援執行所指定功能的裝置之組合、用以執行所指定功能的步驟之組合、及用以執行所指定功能的程式指令方法。將也會發現流程圖表的每個方塊、以及流程圖表裡的方塊之組合，能由特別目的以硬體爲基礎的系統所實施，該系統執行所指定功能或步驟，或特別目的硬體和電腦指令之組合。

現在參照圖3的流程圖，在銷售據點的運作期間當中，本發明的銷售據點裝置，例如一會計處理器卡，藉著已知的程序(方塊100)產生列印和帳目資料。這個交易資訊係部份地依照已知的程序透過把客户收據資訊送到一銷售據點列表機(方塊102)處理。然而，帳目資料係緩衝並儲存在銷售據點裝置之NVRAM中，而非如目前所做的被傳送到一二站台列表機(a two station printer)的列表機帳目站台(方塊102)。

然而，所欲者係限制在例如一會計本部的銷售據點裝置之NVRAM中所保存的資料量。藉由限制電子帳目系統所需要的緩衝區之大小，NVRAM的成本隨著個別資料傳送到銷售據點終端機、或其他保存電子帳目檔案之上行

五、發明說明（11）

(upstream)裝置之時間而減到最少。因此，使用「雜湊」技術，致能包含帳目交易資訊的目前緩衝區之NVRAM之週期性清除。記憶體管理的已知雜湊技術允許所緩衝的記憶體內容之區塊能連續地傳送而維持一小的變動值，有時稱爲一訊息摘要，其數學地獨一相應於整個傳送的資訊之內容。依照本發明此種雜湊技術的應用係進一步在圖4說明。

在圖3的方塊104，銷售據點裝置判定雜湊區塊是否是滿的。如果雜湊區塊還沒滿，當接收到額外的交易資訊時，操作回到方塊100。於方塊106，一旦一雜湊區塊滿了，或帳目週期以一部份地填滿的雜湊區塊結束，則銷售據點裝置的處理器(例如會計本部的會計處理器)在方塊106將資料區塊雜湊以產生一變動的訊息摘要。然後會計處理器從雜湊區塊送出原來的資料到銷售據點終端機或送至保存電子帳目檔案其他裝置，並從當地的NVRAM刪除該區塊，如在方塊108所說明。

銷售據點終端機或其他帳目保存裝置將最近接收的資料區塊附加到電子帳目檔案50的列印資料部分52，如方塊110所說明。在方塊112，系統判定一帳目週期是否完成，其將觸發關閉目前使用的電子帳目檔案50。如果不是，運作返回方塊100至方塊112，繼續交易資訊的接收和雜湊。

如果帳目週期完成，會計處理器透過加密訊息摘要(方塊114)而產生一資料簽章值，及接著傳送資料簽章和列

五、發明說明（12）

表機之公開或共用金鑰，以儲存在電子帳目檔案/記憶體50的各別部分54、56中(方塊115)。在未使用加密的具體實施例中，訊息摘要本身在方塊115係當做資料簽章傳輸，且沒有公開或公用金鑰要傳送。也可以傳送一裝置識別符之例如生產裝置序號。

在方塊116，接收的銷售據點終端機或保存電子帳目檔案的其他上行裝置附加收到的資料簽章和列表機公開金鑰到電子帳目檔案50裡的列印資料。此完成一帳目週期並關閉電子帳目檔案50。在包括傳送裝置識別符之具體實施例中，識別符也被附加進去。

施用於本發明的資料雜湊運作進一步概要地說明在圖4中。如圖4所示，非揮發隨機存取記憶體120包括一部分供如一電子帳目緩衝區122之運作，以及一部分124保存與雜湊函數126有關的變動訊息摘要、及通過電子帳目緩衝區122的資料區塊。如圖4中所說明，雜湊區塊#1到#N連續地通過電子帳目緩衝區122，係傳送到銷售據點終端機上的電子帳目檔案50，並進一步通過雜湊函數126以更新變動訊息摘要124。NVRAM 120和雜湊函數126係包含在銷售據點裝置118中。如圖4中所說明，雜湊函數126使用目前的變動訊息摘要124及最近傳送的雜湊區塊#X，以產生一更新的訊息摘要，其係被依序遞回儲存爲非揮發隨機存取記憶體120的部分124中之變動訊息摘要。

現在參照圖5，進一步爲依照本發明銷售據點裝置118

五、發明說明（ 13 ）

的具體實施例說明，在方塊114到116中所顯示之於帳目週期結束之簽章產生和檔案完成之運作。發生在圖5所說明的具體實施例中之銷售據點終端機的關閉運作，造成電子帳目記憶體或檔案被關閉，使得用此處所描述的認證技術無法偵測的變更不可能被進行。在圖5所說明的具體實施例中，列表機私人金鑰132、列表機公開金鑰134和列表機序號136係全部被儲存在電子可程式唯讀會計記憶體130之部分中。在帳目週期的結束，列表機私人金鑰132和訊息摘要124由加密演算法138用來產生一資料簽章，其係儲存在電子帳目檔案50的資料簽章部分54中。列表機公開金鑰134和列表機序號136分別被傳送和儲存在電子帳目檔案50的各別部分56和58中。

如從所說明的具體實施例對會計記憶體和非揮發隨機存取記憶體130、120的使用可發現的，本發明的系統和方法能使用例如先前參照圖1所討論的會計本部24的硬體實施。在此情況中，隨機存取記憶體30可以備置一部分專用作爲NVRAM 120。此外，會計記憶體EPROM 34可被用來儲存加密資訊，以用於將訊息摘要加密以提供一加密過的資料簽章。

如熟悉此項技藝人士將會發現的，圖2、4和5中本發明之上述態樣，可由硬體、軟體、或以上之組合所提供。雖然銷售據點裝置118的多種元件已經在圖4和5中部份地說明爲個別的元件，實際上其可由一包括輸入和輸出埠且執行軟體程式碼的微控制器、由客戶訂做的或混合的積體電

五、發明說明（ 14 ）

路、由個別的元件、或由上述的組合實施。舉例來說，記憶體120可包含在例如會計處理器28(圖1)的處理器裡面。同樣地，各種不同的運作，例如雜湊函數126和加密演算法138可實施在例如會計處理器28(圖1)的處理器裡面。更一般性的，如上面所描述，依照本發明的運作可實現於現存會計本部24的硬體中，當如此配置時，其提供依照本發明的銷售據點裝置。

現在參照圖6，現在將爲本發明一具體實施例描述用以稽核可查證電子帳目系統之運作。在方塊150，包含於帳目記憶體中之資料簽章係使用包含於帳目記憶體中的共用金鑰透過應用一致同意的加密演算法138(圖5)而解密。在方塊152，驗證資料簽章係從包含在電子帳目資料部分52中的交易資訊使用一致同意的雜湊函數126而決定。最後，在方塊154，將驗證資料簽章與解密過的資料簽章相比較，以決定在帳目週期期間帳目記憶體中的交易資訊，是否已經自原本從獲取的銷售據點裝置—例如會計本部—之隨機存取記憶體所傳送的交易資訊被修改。如果兩個值不相符，則於電子帳目50的部分52中之列印資料不被確認，其顯示在部分52中的資料可能已經被變更。

本發明的可查證電子帳目方法和系統，當偵測到任何對帳目資料的變更時，致能在銷售據點終端機的安全會計帳目檔案之產生。依照本發明的運作，通常能實施於目前策劃的會計本部裝置的硬體設計結構裡面，具有不需要如此的會計本部裝置包括一二站台列印能力以產生書面帳目之

五、發明說明（ 15 ）

優點。此外，依照本發明的運作利用雜湊和電子帳目檔案的上行保存，從而允許維護現存的會計記憶體大小。交易資訊不需要被寫到會計裝置的電子可程式唯讀記憶體，因爲帳目檔案保存在會計本部單元且從會計本部單元可遠端查證。然而，會計記憶體可繼續用來提供例如那些目前由已知的會計列表機裝置所提供的功能。因此，當本發明的方法與如在圖1中所說明的會計記憶體EPROM裝置的使用一起同時實施，特定大小的會計記憶體EPROM 34的壽命不被電子帳目活動影響。

本發明的方法和系統進一步提供改良的能力，因爲電子帳目可位於銷售據點終端機或在一例如網路連接的電腦之裝置中，其與終端機相距遙遠但可使用一網路介面連接到終端機或會計本部。因此，驗證運作不只可以不使用會計本部裝置或列表機實施，而且甚至可從一與銷售據點終端機相距遙遠的位置、或保存電子帳目的其他位置實施。

在圖式和說明書中，已經揭露了本發明的典型較佳具體實施例，且雖然使用了特定的術語，但是它們只是以上位的及描述的意涵，而非爲限制之目的，本發明的範疇陳述在下列申請專利範圍中。

五、發明說明（15a）

元件符號說明

10	銷售據點終端機	52、54、56、58	部分
20	會計列表機	118	銷售據點裝置
22	通訊鏈結	120	非揮發隨機存取記憶體
24	會計本部	122	電子帳目緩衝器
26	二站台列表機	124	變動訊息摘要
28	會計處理器	126	雜湊函數
30	非揮發隨機存取記憶體	130	會計記憶體
32	程式EPROM	132	列表機私人金鑰
34	會計記憶體EPROM	134	列表機公開金鑰
36	日鐘	136	列表機序號
50	電子帳目檔案	138	加密演算法

A5
B5

四、中文發明摘要（發明之名稱：銷售據點裝置之可查證電子帳目及使用該電子帳目之方法）

一種銷售據點裝置，具有一可證實電子帳目系統，其保存一電子帳目檔案以代替帳目列印站之使用。交易資訊首先儲存在一非揮發性的隨機存取記憶體中。一資料簽章根據帳目在隨機存取記憶體之內容而決定。交易資訊和資料簽章兩者都被轉送到分開的帳目記憶體。舉例來說，帳目記憶體存在於銷售據點終端機上，以及可藉由參考亦轉送並保存在電子帳目檔案中之資料簽章而偵測到帳目交易資訊之更改。較佳地，資料簽章透過例如共用金鑰加密架構而加密，且相關的公開金鑰亦從例如會計中心之裝置而傳送並儲存在電子帳目檔案中，其中當交易資訊建立時會計中心即追蹤該交易資訊。較佳地使用雜湊技術以使相對較小的NVRAM可用來支援對一帳目週期期間一電子帳目

英文發明摘要（發明之名稱："VERIFIABLE ELECTRONIC JOURNAL FOR A POINT OF SALE DEVICE AND METHODS FOR USING THE SAME"）

A point of sale device having a verifiable electronic journal system which maintains an electronic journal file in lieu of using a journal print station. Transaction information is first stored in a non-volatile random access memory. A data signature is determined based on the contents of the random access memory for a journal. Both the transaction information and the data signature are transferred to the separate journal memory. The journal memory may, for example, reside on the point of sale terminal and tampering with the journal transaction information may be detected by reference to the data signature which is also transferred and maintained in the electronic journal file. Preferably, the data signature is encrypted such as by a shared key encryption scheme and the associated public key is also transferred and stored in the electronic journal file from the device, such as a fiscal base, which is tracking the transaction information as it is created. A hashing technique is preferably

A5
B5

四、中文發明摘要（發明之名稱：　　）

檔案之一交易資訊集合的產生。因此，資料簽章是一訊息摘要之加密版本，其係反映交易資訊總數之變動數值，該交易資訊係於一帳目週期期間傳遞到電子帳目檔案。

英文發明摘要（發明之名稱：　　）

used so that a comparatively small NVRAM may be utilized to support generation of a transaction information set for an electronic journal file for a journal period. Accordingly, the data signature is an encrypted version of a message digest which is a running value reflecting the total of transaction information passed to the electronic journal file during a journal period.

六、申請專利範圍

經從隨機存取記憶體所傳送的交易資訊被修改。

11. 如申請專利範圍第1項之方法，其中決定資料簽章的步驟接著步驟：

使用一共用金鑰加密資料簽章；以及

傳送共用金鑰到帳目記憶體的第三部分，以回應於多個帳目更新事件中至少一個。

12. 如申請專利範圍第11項之方法，其中傳送共用金鑰的步驟接著稽核可查證電子帳目系統的步驟。

13. 如申請專利範圍第12項之方法，其中稽核可查證電子帳目系統的步驟包含步驟：

使用帳目記憶體的第三部分中之共用金鑰解密帳目記憶體的第二部分中之資料簽章；

從帳目記憶體的第一部分中之交易資訊決定一驗證資料簽章；以及

比較驗證資料簽章和解密的資料簽章，以決定在帳目週期期間帳目記憶體的第一部分中之交易資訊是否已經從隨機存取記憶體所傳送的交易資訊被修改。

14. 一種銷售據點裝置，其具有一可查證電子帳目系統，包含：

用以接收交易資訊之裝置；

用以決定一帳目更新事件之裝置；

一隨機存取記憶體，其連接到用以接收及配置來儲存交易資訊之裝置；

回應於帳目更新事件的決定裝置，用來根據隨機存

六、申請專利範圍

取記憶體的內容決定一資料簽章；

一帳目記憶體，具有配置來儲存交易資訊的一第一部分，和配置來儲存資料簽章的一第二部分；以及

回應於帳目更新事件的傳送裝置，用以從隨機存取記憶體傳送交易資訊到帳目記憶體的第一部分，及從用以決定一資料簽章的裝置傳送資料簽章到帳目記憶體的第二部分。

15. 如申請專利範圍第14項之系統，進一步包含介面裝置，用以連接銷售據點裝置到一配置成列印多個交易的資訊之銷售據點列表機。

16. 如申請專利範圍第14項之系統，其中可程式帳目記憶體包含在銷售據點裝置之中。

17. 如申請專利範圍第14項之系統，其中可程式帳目記憶體設置在距離銷售據點裝置遙遠的電腦上，且其中用以傳送的該裝置進一步包含網路介面裝置，用以通信地連接銷售據點裝置到距離銷售據點裝置遙遠的電腦。

18. 如申請專利範圍第14項之系統，其中交易資訊包括一應繳稅額。

19. 如申請專利範圍第14項之系統，其中用以產生帳目更新事件的裝置，包含用以產生對應於一帳目週期的完成之帳目更新事件的裝置。

20. 如申請專利範圍第14項之系統，其中用以產生一帳目事件的裝置，包含在預先決定的量之交易資訊儲存在隨機存取記憶體中時用以產生帳目更新事件的裝置，並進

六、申請專利範圍

一步包含雜裝置以藉由蓋寫先前儲存的交易資訊，再使用隨機存取記憶體來儲存額外的交易資訊。

21. 如申請專利範圍第14項之系統，其中用以產生一帳目事件的裝置，包含用以在一帳目週期期間產生多個帳目更新事件的裝置，且進一步包含雜湊裝置，用以當判定資料簽章爲一與帳目週期期間所接收交易資訊有關的變動值時，傳送隨機存取記憶體中所儲存的交易資訊的一區塊到帳目記憶體，以回應於多個帳目更新事件中的每一個。

22. 如申請專利範圍第21項之系統，進一步包含使用一共用金鑰加密資料簽章的裝置，且其中可程式帳目記憶體進一步有一配置來儲存共用金鑰的第三部分，並進一步包含傳送裝置，用以在帳目週期期間，傳送共用金鑰到帳目記憶體的第三部分，以回應於多個帳目更新事件中至少一個。

23. 如申請專利範圍第22項之系統，進一步包含介面裝置，用以允許對帳目記憶體的存取，其中帳目記憶體可由稽核可查證電子帳目系統的使用者確認，使用共用金鑰來解密資料簽章，並比較所解密的資料簽章、與一從帳目記憶體的第一部分中之交易資訊所產生的驗證資料簽章。

24. 如申請專利範圍第14項之系統，進一步包含使用一共用金鑰加密資料簽章的裝置，且其中可程式帳目記憶體進一步有一配置來儲存共用金鑰的第三部分，並進一步

六、申請專利範圍

包含用以傳送共用金鑰到帳目記憶體的第三部分的裝置。

25. 如申請專利範圍第24項之系統，進一步包含介面裝置，用以允許對帳目記憶體的存取，其中帳目記憶體可由稽核可查證電子帳目系統的使用者確認，使用共用金鑰來解密資料簽章，並比較所解密的資料簽章、與一從帳目記憶體的第一部分中之交易資訊所產生的驗證資料簽章。

26. 如申請專利範圍第14項之系統，其中帳目記憶體是一電子可程式唯讀記憶裝置，且其中隨機存取記憶體是一非揮發性隨機存取記憶裝置。

27. 一種用以維護一銷售據點裝置之一可查證帳目系統之電腦程式產品，該電腦程式產品包含一電腦可用的儲存媒介，具有電腦可讀程式碼裝置具體實施於該媒介中，電腦可讀程式碼裝置包含：

用以接收與交易相關之交易資訊的電腦可讀程式碼裝置；

用以決定一帳目更新事件的電腦可讀程式碼裝置；

用以儲存交易資訊在一隨機存取記憶體中之電腦可讀程式碼裝置；

用以根據隨機存取記憶體中所包含之交易資訊而決定一資料簽章的電腦可讀程式碼裝置，以回應於帳目更新事件；

用以傳送交易資訊之電腦可讀程式碼裝置，用以將

六、申請專利範圍

隨機存取記憶體中所包含之交易資訊傳送到與隨機存取記憶體分開的帳目記憶體之一第一部分，以回應於帳目更新事件；

用以傳送資料簽章、到帳目記憶體的一第二部分之電腦可讀程式碼裝置，以回應於帳目更新事件。

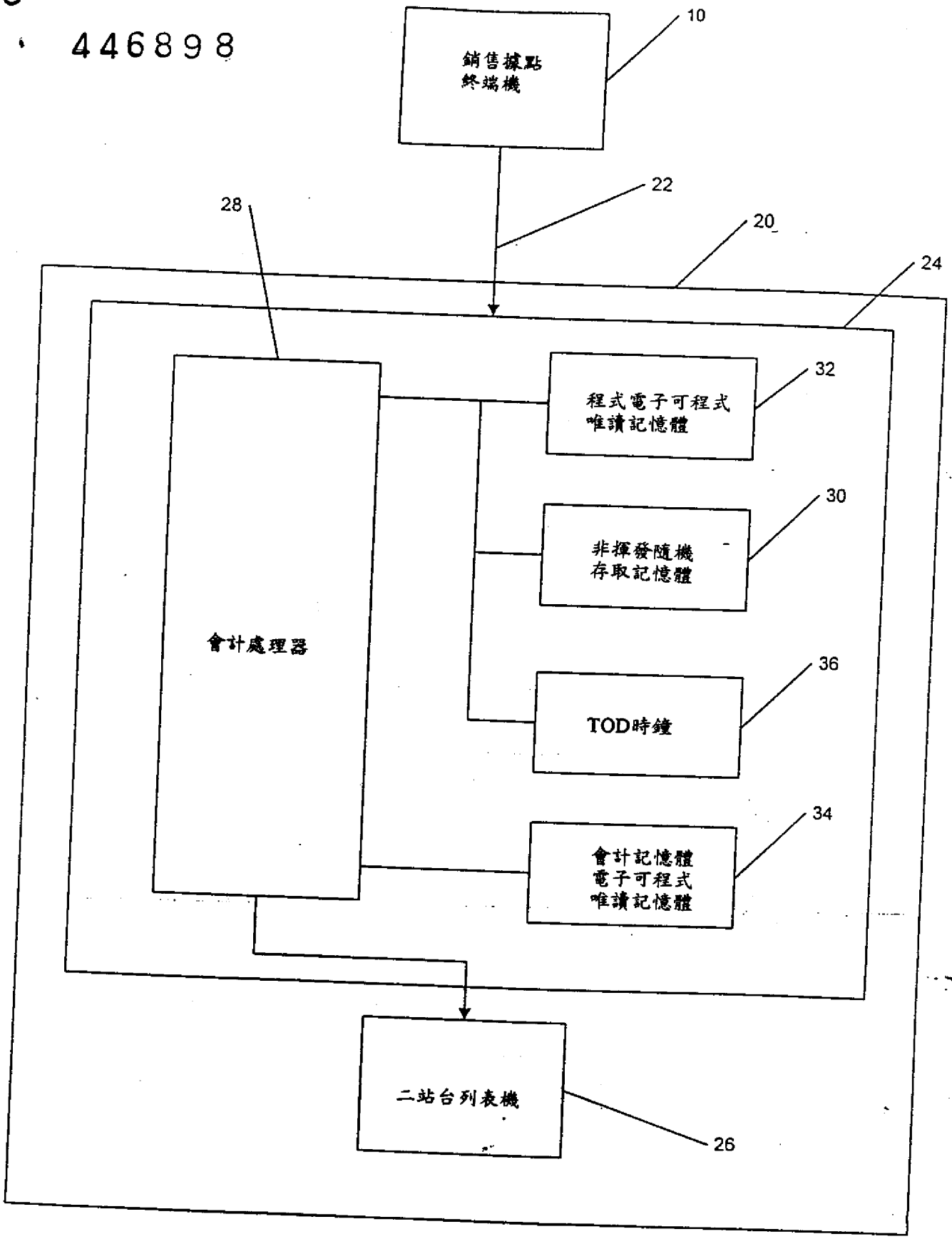
銷售據點
終端機
10
22
28
20
24
程式電子可程式
唯讀記憶體
32
非揮發隨機
存取記憶體
30
會計處理器
TOD時鐘
36
會計記憶體
電子可程式
唯讀記憶體
34
二站台列表機
26

圖 1

4408

446896

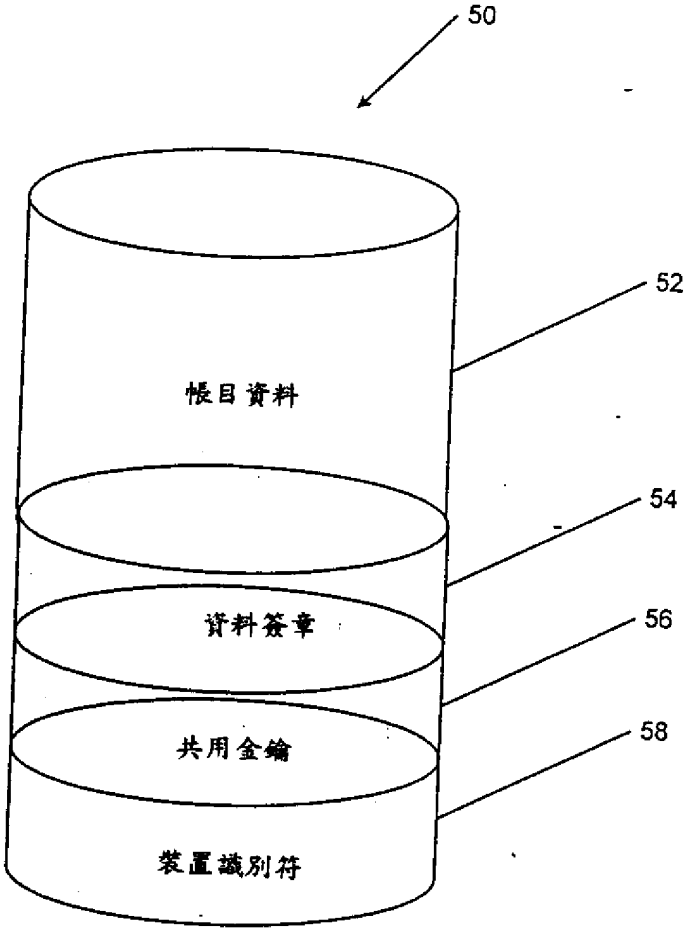

圖 2

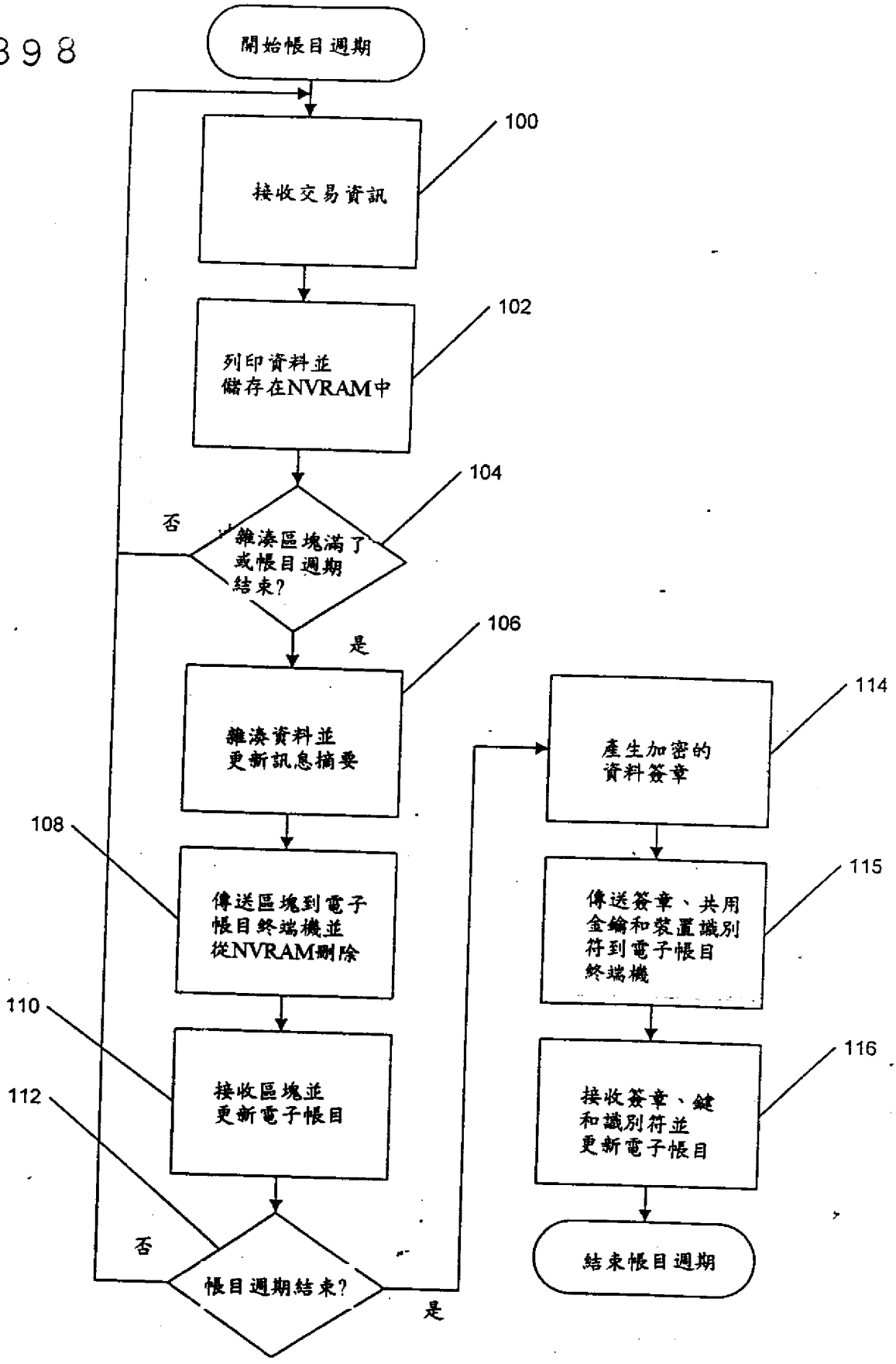
開始帳目週期
100
接收交易資訊
102
列印資料並
儲存在NVRAM中
104
雜湊區塊滿了
或帳目週期
結束?
否
是
106
雜湊資料並
更新訊息摘要
108
傳送區塊到電子
帳目終端機並
從NVRAM刪除
110
接收區塊並
更新電子帳目
112
帳目週期結束?
否
是
114
產生加密的
資料簽章
115
傳送簽章、共用
金鑰和裝置識別
符到電子帳目
終端機
116
接收簽章、鍵
和識別符並
更新電子帳目
結束帳目週期

圖 3

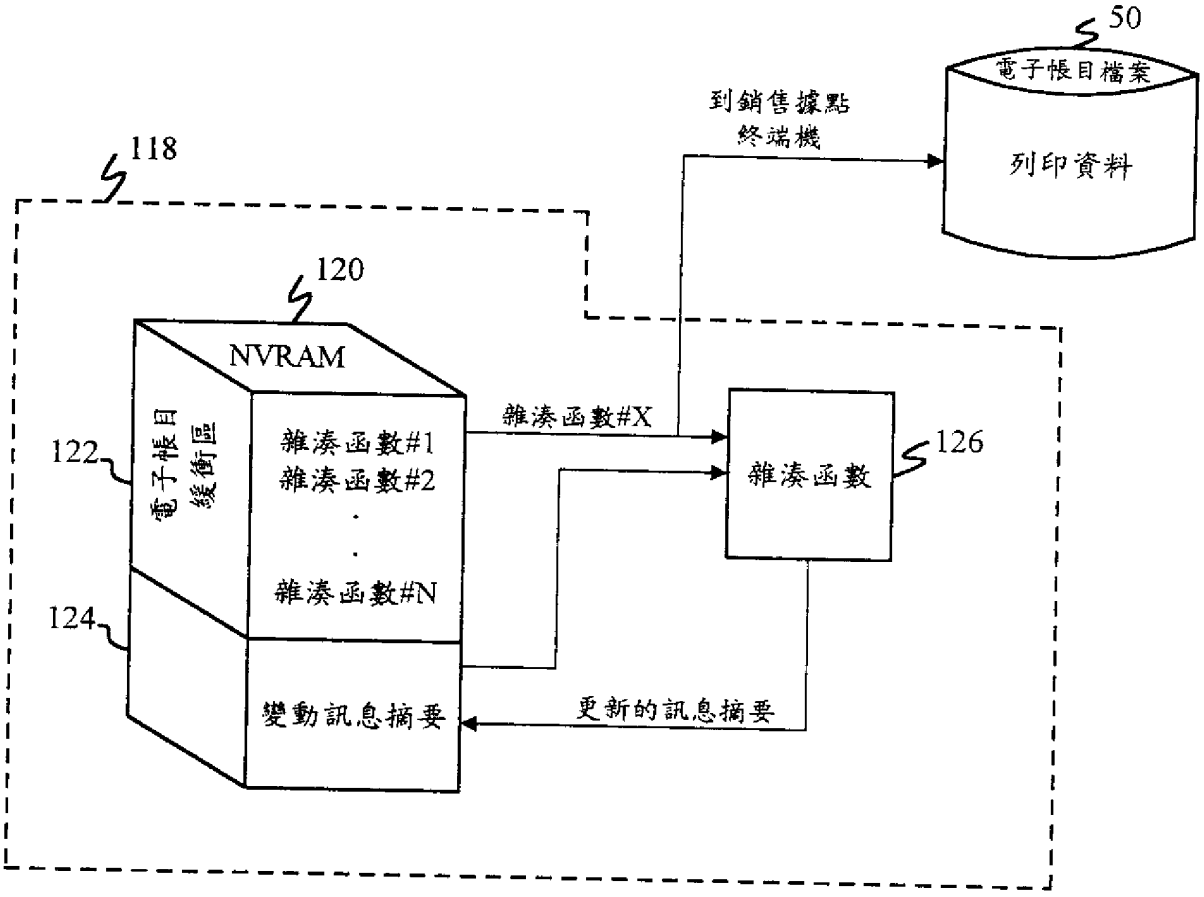
50
電子帳目檔案
列印資料
到銷售據點
終端機
118
120
NVRAM
電子帳目
緩衝區
122
雜湊函數#1
雜湊函數#2
雜湊函數#N
雜湊函數#X
雜湊函數
126
124
變動訊息摘要
更新的訊息摘要

圖4

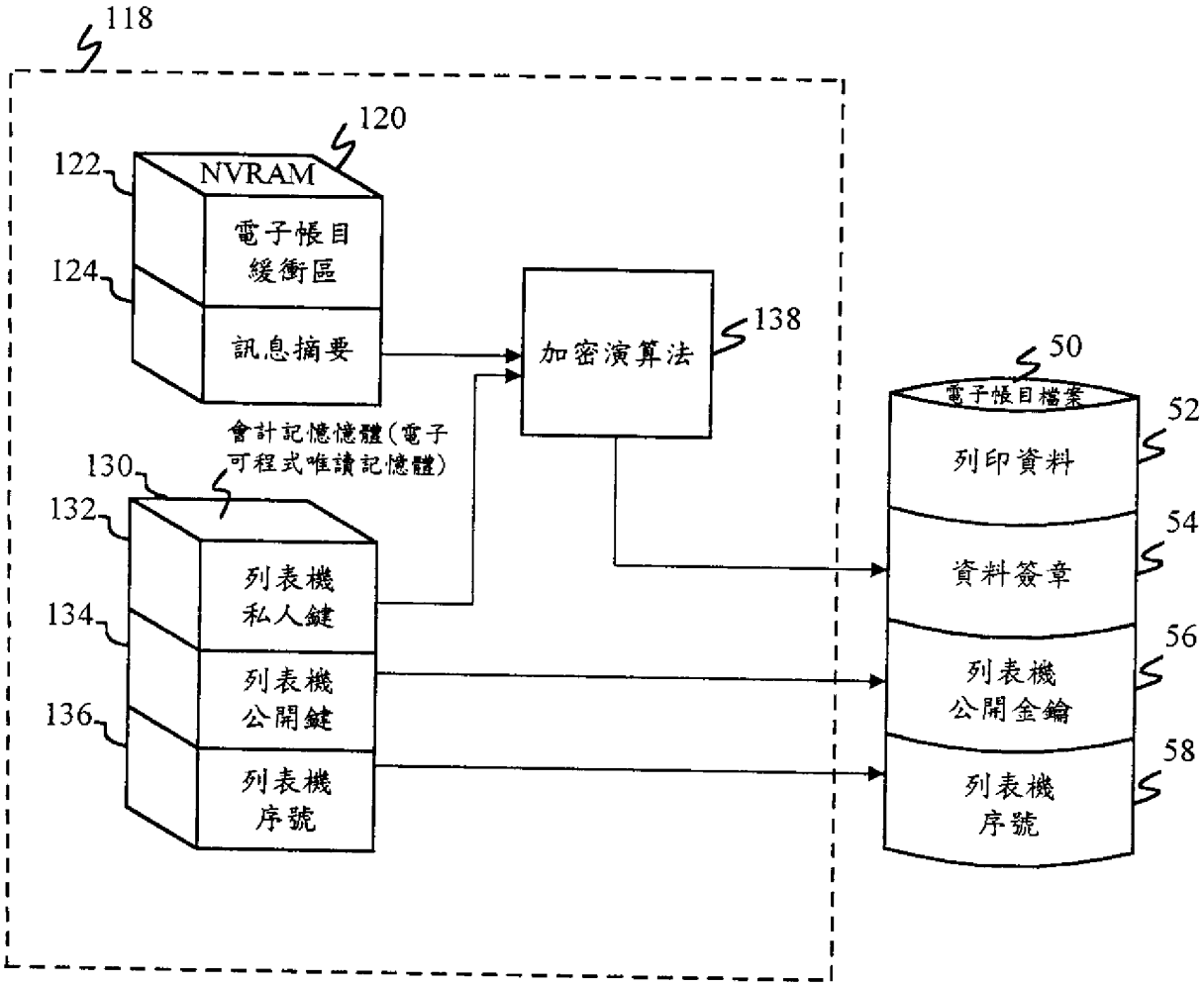
118
120
122
NVRAM
電子帳目
緩衝區
124
訊息摘要
加密演算法
138
50
電子帳目檔案
52
列印資料
54
資料簽章
56
列表機
公開金鑰
58
列表機
序號
會計記憶體(電子
可程式唯讀記憶體)
130
132
列表機
私人鍵
134
列表機
公開鍵
136
列表機
序號

圖5

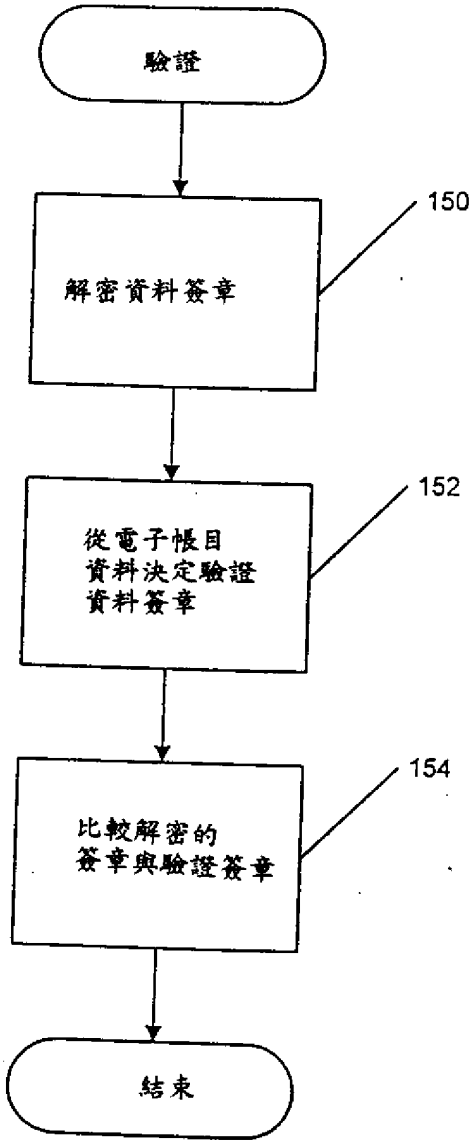

圖 6