201801009

(19)中華民國智慧財產局

(12)發明說明書公開本　(11)公開編號：TW 201801009 A

(43)公開日： 中華民國 107 (2018) 年 01 月 01 日

(21)申請案號：105120856　(22)申請日： 中華民國 105 (2016) 年 06 月 30 日

(51)Int. Cl.：　*G06Q30/04　(2012.01)*

(71)申請人：神通資訊科技股份有限公司 (中華民國)　(TW)

臺北市內湖區堤頂大道二段 187 號 10 樓

(72)發明人：林翰俊 (TW) ；黃于珍 (TW) ；苗　華斌 (US) ；楊建民 (TW) ；陳致愷 (TW)

(74)代理人：桂齊恆；林景郁

申請實體審查：有　申請專利範圍項數：10 項　圖式數：9　　共 24 頁

(54)名稱

利用區塊鏈存放電子發票之方法

(57)摘要

一種利用區塊鏈存放電子發票之方法，其包含步驟為：產生一區塊；存放一筆或複數筆電子發票在該區塊中，且根據各該電子發票內容產生對應之一電子發票雜湊值；各該電子發票根據對應之該電子發票雜湊值鏈結零筆或一筆以上其他相關聯之電子發票；當該區塊存滿該等電子發票，以該區塊內容產生對應之一區塊雜湊值與記錄該區塊建立當時之一時間戳記，以完成建立該區塊；以及該區塊根據與其相鄰之前一個該區塊雜湊值與相鄰之前一個該區塊相串鏈結，以建立所述區塊鏈；藉此，確保各該塊區或各該電子發票的資料無法被竄改，提高電子發票之安全性。

指定代表圖：

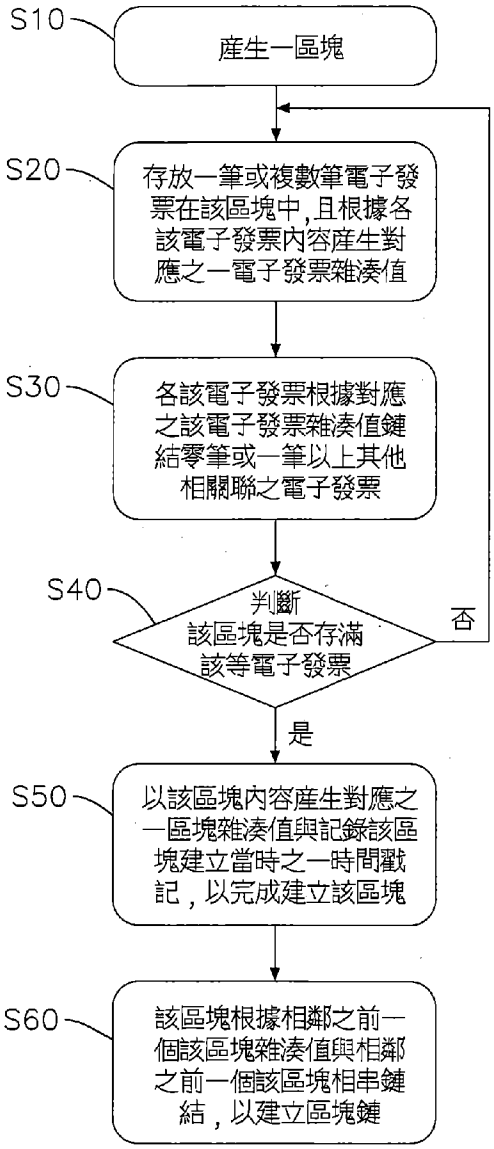
S10
產生一區塊
S20
存放一筆或複數筆電子發票在該區塊中,且根據各該電子發票內容產生對應之一電子發票雜湊值
S30
各該電子發票根據對應之該電子發票雜湊值鏈結零筆或一筆以上其他相關聯之電子發票
S40
判斷該區塊是否存滿該等電子發票
否
是
S50
以該區塊內容產生對應之一區塊雜湊值與記錄該區塊建立當時之一時間戳記,以完成建立該區塊
S60
該區塊根據相鄰之前一個該區塊雜湊值與相鄰之前一個該區塊相串鏈結,以建立區塊鏈

圖 8

201801009
專利案號：105120856

申請日：105.6.30
IPC分類：G06Q30/04 (2012.01)

201801009

【發明摘要】

【中文發明名稱】　利用區塊鏈存放電子發票之方法

【中文】

一種利用區塊鏈存放電子發票之方法，其包含步驟為：產生一區塊；存放一筆或複數筆電子發票在該區塊中，且根據各該電子發票內容產生對應之一電子發票雜湊值；各該電子發票根據對應之該電子發票雜湊值鏈結零筆或一筆以上其他相關聯之電子發票；當該區塊存滿該等電子發票，以該區塊內容產生對應之一區塊雜湊值與記錄該區塊建立當時之一時間戳記，以完成建立該區塊；以及該區塊根據與其相鄰之前一個該區塊雜湊值與相鄰之前一個該區塊相串鏈結，以建立所述區塊鏈；藉此，確保各該塊區或各該電子發票的資料無法被竄改，提高電子發票之安全性。

【指定代表圖】　圖8

【代表圖之符號簡單說明】

無

【發明說明書】

【中文發明名稱】　利用區塊鏈存放電子發票之方法

【技術領域】

【0001】　本創作係有關一種存放電子發票之方法，尤指一種利用區塊鏈存放電子發票之方法。

【先前技術】

【0002】　基於節省成本和節能減碳環保的考量，以電子發票(e-invoice)取代傳統紙本發票的方案已成為政府與業者甚至全民重視的議題。更深層的影響涉及諸多方面，例如，對業者來說，使用電子發票不僅可以節省開立、郵寄或遞送發票之各項作業成本與時程，也可加速其對帳及請款的效率。對政府而言，透過電子發票的整合服務平台，可提供更多元的稅務服務以及執行更縝密的查核稅捐作業與對市場上通路商品更嚴格的監控。對民眾來說，除了可降低紙本發票蒐集、整理的不便性以及遺失、損毀的可能性之外，更可保障個人的消費權益，以避免業者發生漏開或誤開發票之情事。

【0003】　雖然電子發票存在著諸多的優勢，然而，電子發票技術所面臨到安全性(security)的考驗，確實是電子發票推動的主要障礙與瓶頸。具體言之，若電子發票在傳送或發布的過程中發生安全漏洞，例如電子發票發生偽造、竄改、冒名傳送或重送等情事，將對使用電子發票的相關單位造成嚴重的影響。此外，對食品安全或產品品質的追蹤與追溯而言，當發生食品安全問題或產品品質問題時，現行不論紙本或電子發票皆有不易追溯其上、下游相關廠商之問題。因此，如何改善甚至解決電子發票技術所存在安全性與追溯性的問題，乃為政府機關與相關業者共同推動電子發票，所欲尋求突破的首要關鍵。

【發明內容】

【0004】 本創作之目的在於提供一種利用區塊鏈存放電子發票之方法，解決電子發票在傳送或發布的過程中發生偽造、竄改、冒名傳送或重送等情事的問題，並提供可溯源性(traceability)，可追溯上下游相關電子發票。

【0005】 為達成前揭目的，本創作所提出的利用區塊鏈存放電子發票之方法，在一部或多部網路伺服器上執行，所述利用區塊鏈存放電子發票之方法包含產生一區塊；存放一筆或複數筆電子發票在該區塊中，且根據各該電子發票產生對應之一電子發票雜湊值；各該電子發票根據對應之該電子發票雜湊值鏈結至零筆或一筆以上其他相關聯之電子發票；當該區塊存滿該等電子發票，以該區塊內容產生對應之一區塊雜湊值與記錄該區塊建立當時之一時間戳記，以完成建立該區塊；以及該區塊根據相鄰之前一個該區塊雜湊值與相鄰之前一個該區塊相串鏈結，以建立所述區塊鏈。

【0006】 藉由所提出的利用區塊鏈存放電子發票之方法，確保各該塊區或各該電子發票的資料無法被竄改，提高電子發票之安全性。

【0007】 為了能更進一步瞭解本創作為達成預定目的所採取之技術、手段及功效，請參閱以下有關本創作之詳細說明與附圖，相信本創作之目的、特徵與特點，當可由此得一深入且具體之瞭解，然而所附圖式僅提供參考與說明用，並非用來對本創作加以限制者。

【圖式簡單說明】

【0008】

圖1：為本創作區塊鏈存放電子發票之區塊鏈方塊示意圖。

圖2：為本創作單一區塊的內容之方塊示意圖。

圖3：為本創作單一電子發票的內容之方塊示意圖。

圖4：為本創作電子發票與相關聯電子發票鏈結之方塊示意圖。

圖5：為本創作產生電子發票數位簽章之方法的流程圖。

圖6：為本創作電子發票附加電子發票數位簽章之方塊示意圖。

圖7：為本創作產生電子發票數位簽章與驗證電子發票之操作示意圖。

圖8：為本創作利用區塊鏈存放電子發票之方法的流程圖。

圖9：為本創作區塊鏈於網路中應用之示意圖。

【實施方式】

【0009】 茲有關本創作之技術內容及詳細說明，配合圖式說明如下。

【0010】 如圖1所示，本案所揭露之區塊鏈(Blockchain)的架構係由複數個區塊，亦即N個區塊(區塊1~區塊N)所形成。相鄰的兩區塊，例如區塊1與區塊2、區塊2與區塊3，依此類推，乃至區塊N-1與區塊N係相串鏈結(chaining)，形成所述區塊鏈100。至於兩兩區塊之間的鏈結方式，將在文後有更詳細之說明。其中，所述區塊鏈100及其所具有之區塊可建立與存放在一部或多部網路伺服器上，而各該伺服器以網路相連接，所述網路可為私有網路(private network)、公開網路(public network)或混合式網路(hybrid network)等。然，不以上述該等網路型態為限制本創作之實施。

【0011】 如圖2所示，單一區塊的內容，亦即存放於該單一區塊內的內容，以區塊N為例，係包含該區塊N的前一個區塊之一區塊雜湊值(a hashing value of the previous block)，亦即該區塊N的前一區塊N-1之一區塊雜湊值、存放在該區塊N內的一筆或複數筆電子發票之紀錄，亦即n筆電子發票之紀錄(電子發票N1~電子發票Nn)、該區塊N完成建立之一時間戳記(time stamp)以及該區塊N之一區塊雜湊值。其中，該區塊N之該區塊雜湊值係由該區塊N的前一區塊N-1之該區塊雜湊值、所述一筆或複數筆電子發票N1~Nn之紀錄以及該區塊完成建立時之該時間戳記透過一安全雜湊演算法(cryptographic hash function)所產生。在本創作中所採用之該安全雜湊演算法並不以SHA-512演算法為限制。再

者，所述SHA-512演算法為現有廣泛使用之能夠將資料運算與轉換為一固定長度值的演算法，因此，在此不再贅述該SHA-512演算法之運算與轉換方式。

【0012】 以該區塊N為當下做為存放電子發票之區塊為例，是以，定義該區塊N為一操作區塊。在本創作中，由於該操作區塊係為該區塊N，因此，該區塊N之前的所有區塊，亦即區塊1~區塊N-1係已完成建立，換言之，所述N-1個區塊的內容將無法再變更。因此，可透過驗證各該區塊相關聯的區塊之區塊雜湊值是否發生變更，即可判斷所述區塊1~區塊N-1的內容是否遭到竄改。

【0013】 在本創作中，係透過在該區塊N存放區塊N-1之該區塊雜湊值，因此，使得該區塊N-1與該區塊N相互鏈結。同樣地，該區塊2存放區塊1之該區塊雜湊值、該區塊3存放區塊2之該區塊雜湊值，依此類推，乃至該區塊N存放區塊N-1之該區塊雜湊值，如此，透過相鄰兩兩區塊的鏈結，使得區塊1至區塊N相串鏈結，形成所述區塊鏈100。再者，透過鏈結該區塊N的前一個該區塊N-1之該區塊雜湊值，一旦當該區塊鏈100中任一該區塊的資料內容遭到竄改，可立即地、準確地察覺，藉此判斷資料是否完整，以及確保資料之資料完整性(integrity)。

【0014】 存放於該區塊N的該等電子發票N1~Nn不必然存在著相關聯的關係。以上游供應商與下游通路商之商業交易為例，該上游供應商為開立電子發票的單位，而該下游通路商為接收電子發票的單位，該上游供應商開立給該下游通路商的所有電子發票之間可定義互為相關聯的關係。因此，存放於該區塊N的該等電子發票N1~Nn不必然存在著相關聯的關係，係指該等該上游供應商開立給該下游通路商的所有電子發票不必然存放在同一個區塊中，就實際面而言，開立發票的時間差異，也使得該等相關聯的電子發票不必然存放在同一個區塊中。在本實施例中，該等相關聯的電子發票係隨機地依開立，電子發票

的時間存放在當下操作中的該區塊中，亦即，可能部分存放在相同的區塊中，亦可能部分分散在不同的區塊中。

【0015】 該區塊N之該時間戳記係為當該區塊N存滿該等電子發票N1~Nn時，亦即，不再接收其他電子發票存入時，定義該區塊N完成建立，並且該區塊N之該時間戳記即為該區塊N完成建立時當下之日期與時間。此外，該時間戳記係透過以毫秒的時間格式進行記錄與儲存，為各式存取端進行轉換其所需的日期時間格式。透過紀錄不同區塊建立時之時間戳記資訊，搭配區塊鏈100之前後區塊時間順序關係，亦即，建立在後的區塊其時間戳記必晚於建立在前的區塊的時間戳記，換言之，建立在後的區塊其時間戳記之毫秒數必大於建立在前的區塊的時間戳記之毫秒數。藉此，可透過判斷不同區塊間之時間戳記的先後資訊，以驗證是否發生任一區塊遭到竄改或發生偽造的狀況，以及驗證該等區塊的建立時間之合理性(rationality)。

【0016】 綜上所述，該區塊N之該區塊雜湊值係由該區塊N-1之該區塊雜湊值、所述複數電子發票N1~Nn之紀錄以及該區塊完成建立時之該時間戳記透過該安全雜湊演算法所產生。

【0017】 如圖3所示，單一電子發票的內容，以圖2之該電子發票N1為例，係包含該電子發票N1的開立單位之一公開金鑰(issuer's public key)、該電子發票N1的接收單位之一公開金鑰(receiver's public key)、該電子發票N1之交易內容、與該電子發票N1相關聯之零筆或一筆以上電子發票之電子發票雜湊值、該電子發票N1開立時之一時間戳記(time stamp)以及該電子發票N1之一電子發票雜湊值。其中，該電子發票N1的開立單位之該公開金鑰與該電子發票N1的接收單位之該公開金鑰可使用RSA演算法(Rivest-Shmir-Adleman cryptography)或橢圓曲線演算法(elliptic curve cryptography, ECC)產生，然，不以上述兩種演算法為限制。其中，該電子發票N1之該電子發票雜湊值係由該電子發票N1的

開立單位之該公開金鑰、該電子發票N1的接收單位之該公開金鑰、該電子發票N1之交易內容、與該電子發票N1相關聯之該零筆或一筆以上電子發票之電子發票雜湊值以及該電子發票N1開立時之該時間戳記透過一安全雜湊演算法(cryptographic hash function)所產生。

【0018】 在本創作中所採用之該安全雜湊演算法並不以SHA-512演算法為限制。藉此，透過對該電子發票N1的完整資料(包含開立單位之該公開金鑰、該接收單位之該公開金鑰、該電子發票N1之交易內容、與該電子發票N1相關聯之該零筆或一筆以上電子發票之電子發票雜湊值以及該電子發票N1開立時之該時間戳記)進行計算其安全雜湊值。藉此，由於雜湊值的計算特性，一但該電子發票N1的任一資料遭到竄改，可準確地察覺出來該電子發票N1已遭到破壞，以確保該電子發票N1之資料完整性(integrity)。

【0019】 該電子發票N1的開立單位之該公開金鑰係為開立該電子發票的單位其所提供之公開金鑰。該電子發票N1的接收單位之該公開金鑰係為接收該電子發票N1的單位所提供之公開金鑰。以前述上、下游廠商之商業交易為例，該上游廠商即為開立該電子發票N1的單位，而該下游廠商為接收該電子發票N1的單位。以該電子發票N1之交易內容其相關原物料所開立之相關電子發票可定義為與該電子發票N1互為相關聯之電子發票。

【0020】 配合圖4所示，以該實施例為例，與該電子發票N1相關聯的電子發票包含電子發票X、電子發票Y以及該電子發票Z三筆。其中，各筆電子發票的內容如圖3所示，因此，圖4僅表示各筆電子發票包含其電子發票雜湊值。其中，電子發票雜湊值的產生方式請配合圖3以及相對應之說明書內容，在此不再贅述。因為該電子發票N1相關聯的電子發票有三筆，因此該電子發票N1相關聯電子發票之電子發票雜湊值也就有三個分別對應電子發票X、電子發票Y以及該電子發票Z的電子發票雜湊值。其中，該電子發票N1可使用索引

(index)、陣列(array)或屬性值配對組(attribute-value pair)等方式進行存放所述電子發票X、電子發票Y以及該電子發票Z之雜湊值，然，不以上述該等方式為限制。藉此，透過該電子發票N1連結其他相關聯的電子發票之紀錄(例如與該電子之發票交易內容之相關原物料上游供應商與下游通路商之商業交易)，如此可以透過搜尋上游供應商與下游通路商之電子發票的雜湊值，達成追蹤上游與下游之雙向溯源(traceability)的需求。

【0021】 該電子發票N1之該時間戳記係為該電子發票N1開立時當下之日期與時間。此外，該時間戳記係透過以毫秒的時間格式進行記錄與儲存，為各式存取端進行轉換其所需的日期時間格式。

【0022】 該電子發票N1之該交易內容包含該電子發票N1的發票號碼、賣方名稱、賣方統編(例如上游廠商的名稱、統編)、買方名稱、買方統編(例如下游廠商的名稱、統編)、交易項目、交易數量、單價、小計、稅金、金額以及備註之相關交易資訊，然，不以上述該等交易資訊為限制，並且，該電子發票之交易內容之各項相關交易資訊可視實際交易需求增減或不填入值。

【0023】 綜上所述，該電子發票N1之該電子發票雜湊值係由該電子發票N1的開立單位之該公開金鑰、該電子發票N1的接收單位之該公開金鑰、該電子發票N1之交易內容、與該電子發票N1相關聯之該零筆或一筆以上電子發票之電子發票雜湊值以及該電子發票N1開立時之該時間戳記透過該安全雜湊演算法所產生。

【0024】 如圖5所示，該電子發票N1之紀錄係可選擇是否進一步附加該電子發票N1之一電子發票數位簽章。附加係指該電子發票數位簽章，非存放於該電子發票N1記錄中，亦即非存放於該電子發票N1記錄本體，而是以外部「附帶加上(附加)」的方式，於該電子發票N1開立後，將兩者(即該電子發票N1紀錄本體與該電子發票N1之該電子發票數位簽章)可選擇是否「一併傳送」

提供給該電子發票的接收單位，然，不以上述「附加」以及「一併傳送」為限制，即亦可選擇不付加、不一併傳送，例如可採取分離傳送兩者、分兩次傳送等方式。讓該電子發票的接收單位可以進行此電子發票紀錄之驗證，其驗證方式與流程詳述於後文。如圖6所示，其中，該電子發票N1之該電子發票數位簽章係由該電子發票N1紀錄之雜湊值以該電子發票N1的開立單位之一私密金鑰(issuer's private key)透過「數位簽章產生作業」進行簽署加密所產生。其中，該電子發票數位簽章產生作業可使用RSA演算法或橢圓曲線演算法，然，不以上述兩種演算法為限制。

【0025】 請參見圖7所示。該電子發票N1的開立單位開立該電子發票N1(S11)，並且將該電子發票N1傳送至該電子發票N1的接收單位(S12)，由該電子發票N1的接收單位接收該電子發票N1(S13)。該開立單位透過前述安全雜湊演算法，計算該電子發票N1之一電子發票雜湊值(S14)，並且再將該電子發票N1紀錄之雜湊值以該開立單位的私密金鑰，透過「數位簽章產生作業」進行簽署加密，以產生一電子發票數位簽章(S15)。該開立單位將該電子發票數位簽章傳送至該接收單位(S16)。在上述中，不限制該電子發票N1與該電子發票數位簽章為前後傳送至該接收單位，亦即，可利用將該電子發票數位簽章附加至該電子發票N1，同時傳送至該接收單位，換言之，步驟(S12)與步驟(S16)可整合為同一步驟，且在步驟(S15)之後執行。

【0026】 當該接收單位接收到該電子發票N1與該電子發票數位簽章(S17)後，若欲確認所接收到的該電子發票N1是否遭到竄改與驗證該電子發票是否確為開立單位所發行開立，可對其進行驗證。該接收單位透過前述安全雜湊演算法，計算該電子發票N1之一電子發票雜湊值H1(S18)。此外，可利用該開立單位所提供的一公開金鑰對該電子發票數位簽章進行解密，以取得一組解密後的電子發票雜湊值H2(S19)。再對該電子發票雜湊值H1與該電子發票雜湊值H2進

行驗證比較(S1A)，若該電子發票雜湊值H1與該電子發票雜湊值H2相同時，則可確認該電子發票N1未遭到竄改且確認該電子發票確為開立單位所發行開立。反之，若該電子發票雜湊值H1與該電子發票雜湊值H2相異時，則表示該電子發票N1遭到竄改或該電子發票非開立單位所發行開立，以提供該接收單位進行後續之因應措施。藉此，利用數位簽章的計算特性，一旦該電子發票N1的任一資料遭到竄改或該電子發票非開立單位所發行開立，該電子發票數位簽章將因此而改變，如此配合對電子發票雜湊值進行驗證，可達到該電子發票N1之資料完整性(integrity)、鑑定性(authenticity)與不可否認性(non-repudiation)。

【0027】 針對本創作之區塊與電子發票之定義與說明已於前述說明書內容說明，接著進一步對本創作利用區塊鏈100存放電子發票之方法的步驟，加以說明。請參見圖8，首先，產生一區塊(S10)。其中，定義當下做為存放電子發票之區塊為一操作區塊。該操作區塊係提供存放一筆或複數筆電子發票於其中，並且各該電子發票係根據各該電子發票內容產生對應之一電子發票雜湊值(S20)。舉例來說，在該操作區塊的一電子發票N1產生電子發票N1之電子發票雜湊值、一電子發票N2產生電子發票N2之電子發票雜湊值，依此類推。

【0028】 然後，該電子發票N1可鏈結零筆或一筆以上相關聯之電子發票，其中，係透過在該電子發票N1內存放該零筆或一筆以上相關聯之電子發票的電子發票雜湊值，使得該電子發票N1與該零筆或一筆以上相關聯之電子發票鏈結(S30)。接著，判斷該操作區塊是否存滿該等電子發票(S40)。若該操作區塊尚未存滿該等電子發票，則執行步驟(S20)，繼續存放電子發票。反之，若該操作區塊已存滿該等電子發票，該操作區塊則產生一區塊雜湊值與記錄建立區塊當時之時間戳記，以完成建立該區塊(S50)。其中，已完成建立之區塊，係根據其相鄰之前一個區塊雜湊值與相鄰之前一個已完成建立之區塊相串鏈結，以

建立區塊鏈(S60)。至於該本創作利用區塊鏈存放電子發票之方法的步驟細節說明，可配合參見圖1至圖7及其對應之說明書內容。

【0029】 如圖9所示，每一個節點(node)可視為一電子發票之開立單位(例如一上游原物料供應商)、一電子發票之接收單位(例如一下游通路商或消費者)或一驗證者(validator)或觀察者(observer)(例如一國家財政機構或地方財政機構)。為方便說明，假設圖9所示之一第一節點n1、一第二節點n2分別為一第一上游原物料供應商與一第二上游原物料供應商；一第三節點n3為一下游通路商，且為該第一上游原物料供應商與該第二上游原物料供應商的共同銷售對象；一第四節點n4為一國家財政機構，例如財政部。

【0030】 該第一上游原物料供應商(對應該第一節點n1)與該第二上游原物料供應商(對應該第二節點n2)為電子發票的發行者，亦即電子發票的開立單位。以該第一上游原物料供應商為例，該第一上游原物料供應商於網路中發布所開立之電子發票，例如發布該電子發票給該下游通路商(對應該第三節點n3)，以及同時發布該電子發票給該國家財政機構(對應該第四節點n4)。其中，該網路可為對等式網路(peer-to-peer network, P2P network)、主從式架構(client-server model)或直接連線之網路架構。並且，可於公開網路架構、私有網路架構或混合式網路架構上運行。然，不以上述該等網路架構為限制本創作之實施。

【0031】 於本發明中區塊鏈(Blockchain)中所存放的所有區塊資料以及各該區塊內所有的電子發票資料，所有節點皆存有一份，且所有節點皆可存取。如此，該國家財政機構或其他單位可針對所接收到的區塊鏈資料，對其中各該區塊與各該電子發票進行稽查，以進行驗證各該區塊與各該電子發票之合法性與合理性。所有的上游原物料供應商或下游通路商亦皆可針對所接收到的區塊鏈資料，對其中各該區塊與各該電子發票進行確認，以進行驗證各該區塊與各

該電子發票之合法性與合理性。其中，驗證方式與內容，可參見前述說明書所記載之內容，在此不再贅述。

【0032】 由於所有節點(單位)亦取得並儲存相同的區塊鏈資料。一旦，任一節點(單位)發生失效、無法存取的狀況，則可透過其他儲存該區塊鏈資料的節點(單位)取得相同的區塊鏈資料，以確保區塊鏈資料的高可用性(high availability)。

【0033】 綜上所述，本創作係具有以下之特徵與優點：

【0034】 1、區塊與相鄰前一區塊之間的鏈結，藉由區塊的時間戳記與區塊的雜湊值，提供區塊之安全保護機制，以確保區塊完全無法被竄改，實現區塊資料之完整性。

【0035】 2、藉由電子發票的時間戳記、電子發票的雜湊值以及加密之電子發票數位簽章，提供電子發票之安全保護機制，以確保電子發票完全無法被竄改，實現電子發票資料之完整性、驗證性以及不可否認性。

【0036】 3、藉由電子發票與相關聯電子發票之間的鏈結，達成追蹤上游與下游之雙向溯源的需求。

【0037】 4、所有節點(單位)亦取得並儲存相同的區塊鏈資料，若任一節點發生失效、無法存取的狀況，則可透過其他儲存區塊鏈資料的節點取得相同的區塊鏈資料，以確保區塊鏈資料的高可用性。

【符號說明】

【0038】

100 區塊鏈

n1~n7 節點

【發明申請專利範圍】

【第1項】一種利用區塊鏈存放電子發票之方法，在一部或多部網路伺服器上執行，所述利用區塊鏈存放電子發票之方法包含：

產生一區塊；

存放一筆或複數筆電子發票在該區塊中，且根據各該電子發票內容產生對應之一電子發票雜湊值；

各該電子發票根據對應之該電子發票雜湊值鏈結零筆或一筆以上其他相關聯之電子發票；

當該區塊存滿該等電子發票，以該區塊內容產生對應之一區塊雜湊值與記錄該區塊建立當時之一時間戳記，以完成建立該區塊；及

該區塊根據相鄰之前一個該區塊雜湊值與相鄰之前一個該區塊相串鏈結，以建立所述區塊鏈。

【第2項】如申請專利範圍第1項所述利用區塊鏈存放電子發票之方法，其中各該區塊包含相鄰之前一個區塊之該區塊雜湊值、一筆或複數筆電子發票之紀錄、該區塊完成建立時之一時間戳記以及該區塊之該區塊雜湊值，其中該區塊之該區塊雜湊值係由相鄰之前一個區塊之該區塊雜湊值、所述一筆或複數筆電子發票之紀錄以及該區塊完成建立時之該時間戳記透過一安全雜湊演算法進行計算所產生。

【第3項】如申請專利範圍第1項所述利用區塊鏈存放電子發票之方法，其中各該電子發票之紀錄包含該電子發票的開立單位之一公開金鑰、該電子發票的接收單位之一公開金鑰、與該電子發票相關聯之零筆或一筆以上電子發票之電子發票雜湊值、該電子發票開立時之一時間戳記、該電子發票之交易內容以及該電子發票之該電子發票雜湊值，其中該電子發票之該電子發票雜湊值係由該電子發票的開立單位之該公開金鑰、該電子發票的接收單位之該公開金鑰、

與該電子發票相關聯之該零筆或一筆以上電子發票之電子發票雜湊值、該電子發票之交易內容以及該電子發票開立時之該時間戳記透過一安全雜湊演算法進行計算所產生。

【第4項】如申請專利範圍第3項所述利用區塊鏈存放電子發票之方法，其中各該電子發票之紀錄可選擇是否附加一電子發票數位簽章，該電子發票數位簽章係由該電子發票之該電子發票雜湊值以該電子發票的開立單位之一私密金鑰透過一數位簽章產生作業進行簽署加密所產生。

【第5項】如申請專利範圍第2項所述利用區塊鏈存放電子發票之方法，其中所述相鄰之前一個區塊之該區塊雜湊值係於產生、建立目前區塊時，讀取目前區塊的前一個區塊之該區塊雜湊值；該區塊之該區塊雜湊值係由相鄰之前一個區塊之該區塊雜湊值、所述一筆或複數筆電子發票之紀錄以及該區塊完成建立時之該時間戳記以安全雜湊演算法進行計算所產生。

【第6項】如申請專利範圍第2項所述利用區塊鏈存放電子發票之方法，其中該區塊完成建立時之該時間戳記係為該區塊完成建立時當下之日期與時間，透過以毫秒的時間格式進行記錄與儲存，各式存取端再自行進行轉換其所需的日期格式與時間格式。

【第7項】如申請專利範圍第3項所述利用區塊鏈存放電子發票之方法，其中該電子發票的開立單位之該公開金鑰係為開立該電子發票的單位其所提供之公開金鑰；該電子發票的接收單位之該公開金鑰係為接收該電子發票的單位所提供之公開金鑰。

【第8項】如申請專利範圍第3項所述利用區塊鏈存放電子發票之方法，其中該電子發票相關聯之零筆或一筆以上電子發票係與該電子發票在相同之區塊中，或與該電子發票在不同之區塊中。

【第9項】如申請專利範圍第3項所述利用區塊鏈存放電子發票之方法，其中該電子發票開立時之該時間戳記係為該電子發票開立時當下之日期與時間，透過以毫秒的時間格式進行記錄與儲存，各式存取端再自行進行轉換其所需的日期格式與時間格式。

【第10項】如申請專利範圍第3項所述利用區塊鏈存放電子發票之方法，其中該電子發票之交易內容包含電子發票號碼、賣方名稱、賣方統編、買方名稱、買方統編、交易項目、交易數量、單價、小計、稅金、金額以及備註之相關交易資訊，並且該電子發票之交易內容之各項相關交易資訊可視實際交易需求增減或不填入值。

【發明圖式】

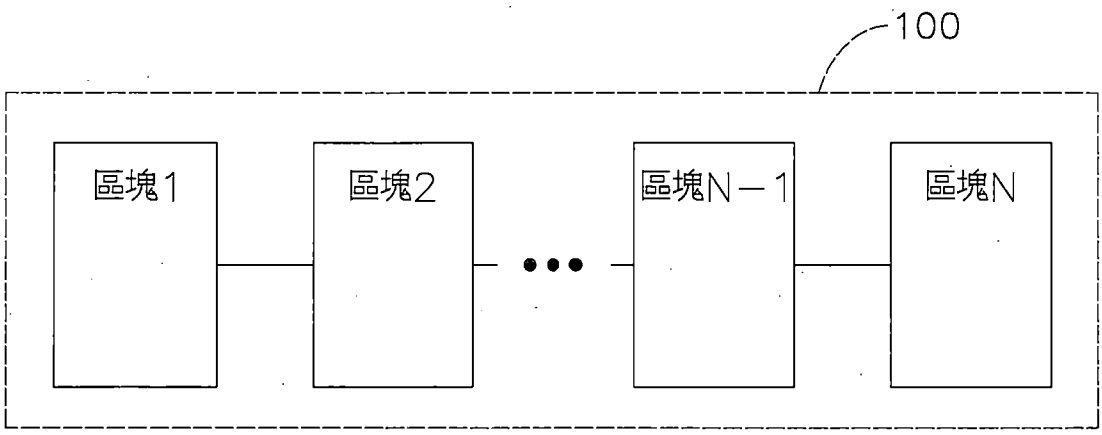

圖 1

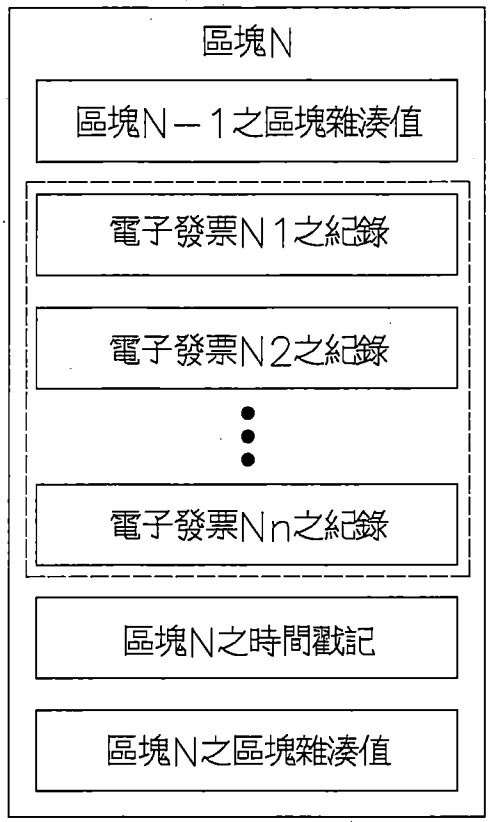
區塊N
區塊N－1之區塊雜湊值
電子發票N1之紀錄
電子發票N2之紀錄
電子發票Nn之紀錄
區塊N之時間戳記
區塊N之區塊雜湊值

圖 2

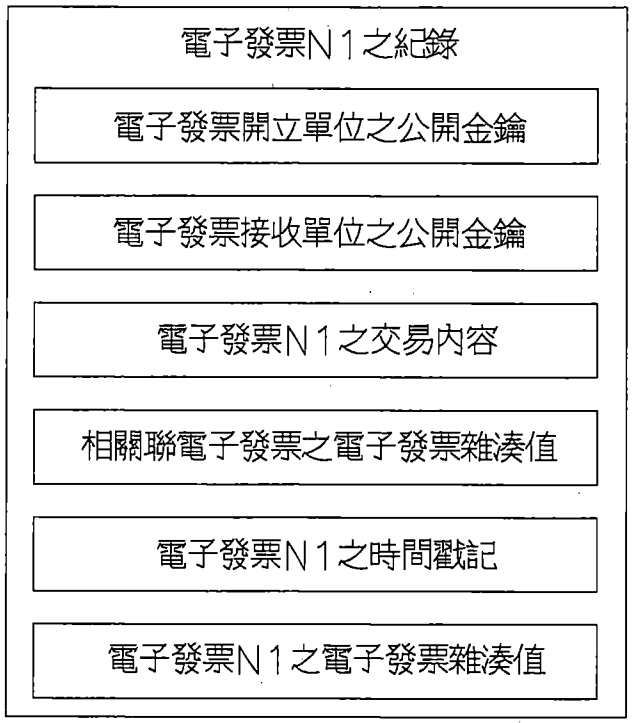
電子發票N1之紀錄
電子發票開立單位之公開金鑰
電子發票接收單位之公開金鑰
電子發票N1之交易內容
相關聯電子發票之電子發票雜湊值
電子發票N1之時間戳記
電子發票N1之電子發票雜湊值

圖 3

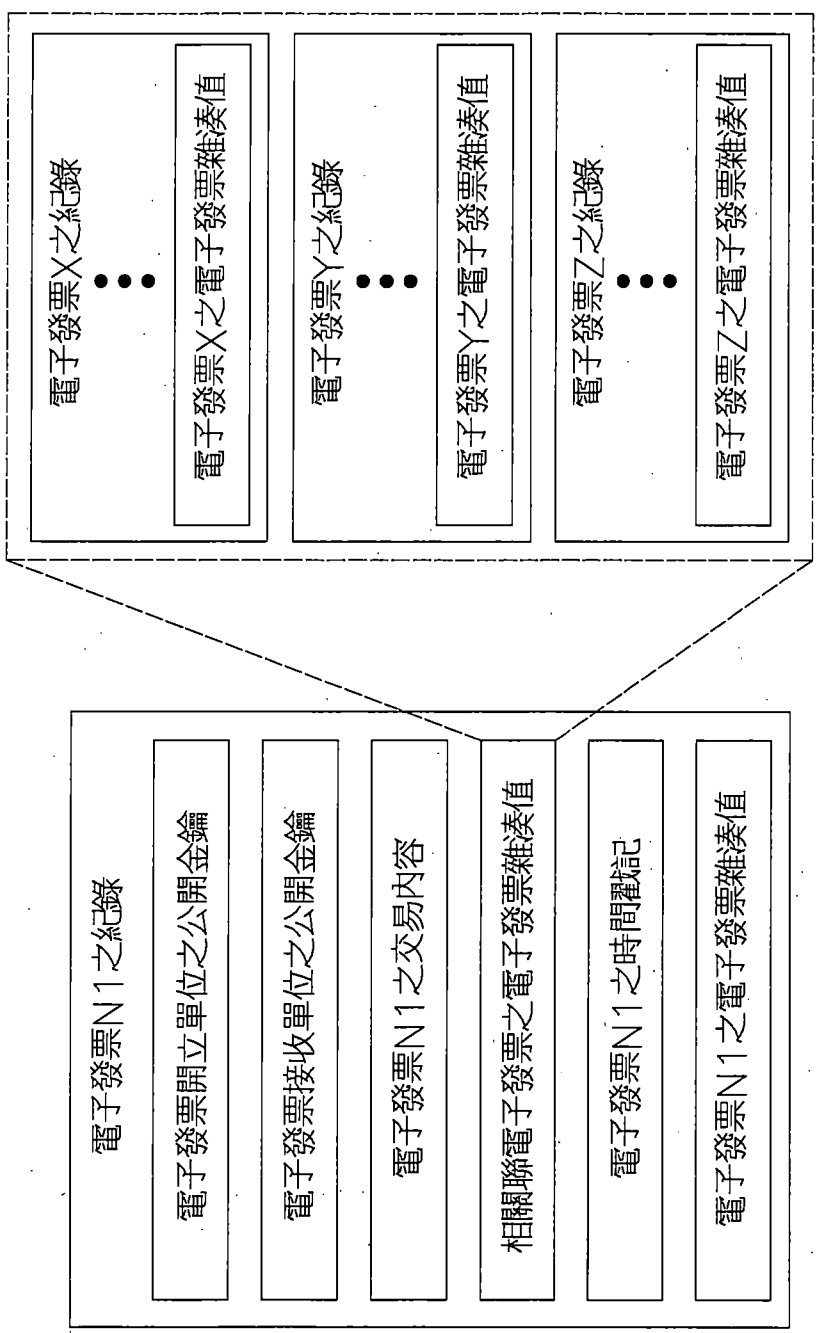
電子發票N1之紀錄
電子發票開立單位之公開金鑰
電子發票接收單位之公開金鑰
電子發票N1之交易內容
相關聯電子發票之電子發票雜湊值
電子發票N1之時間戳記
電子發票N1之電子發票雜湊值
電子發票X之紀錄
電子發票X之電子發票雜湊值
電子發票Y之紀錄
電子發票Y之電子發票雜湊值
電子發票Z之紀錄
電子發票Z之電子發票雜湊值

圖 4

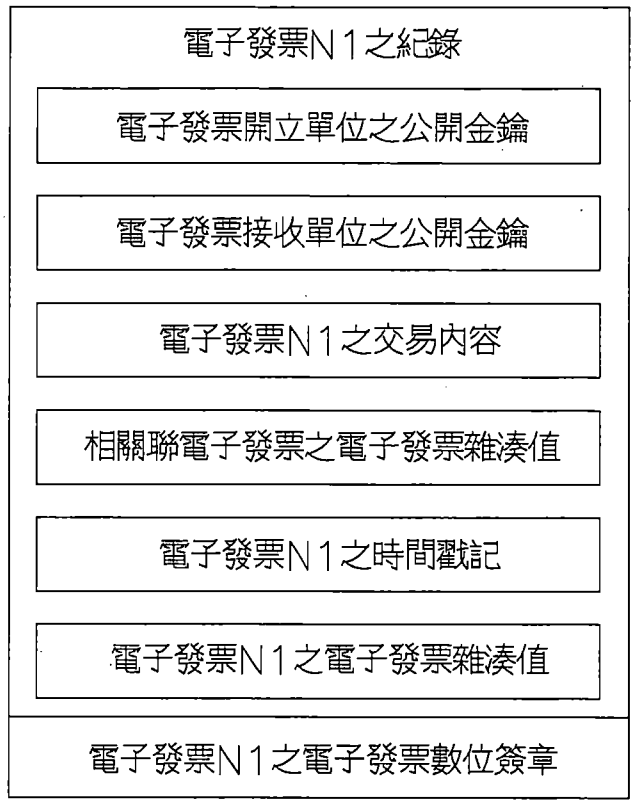
電子發票N1之紀錄
電子發票開立單位之公開金鑰
電子發票接收單位之公開金鑰
電子發票N1之交易內容
相關聯電子發票之電子發票雜湊值
電子發票N1之時間戳記
電子發票N1之電子發票雜湊值
電子發票N1之電子發票數位簽章

圖 5

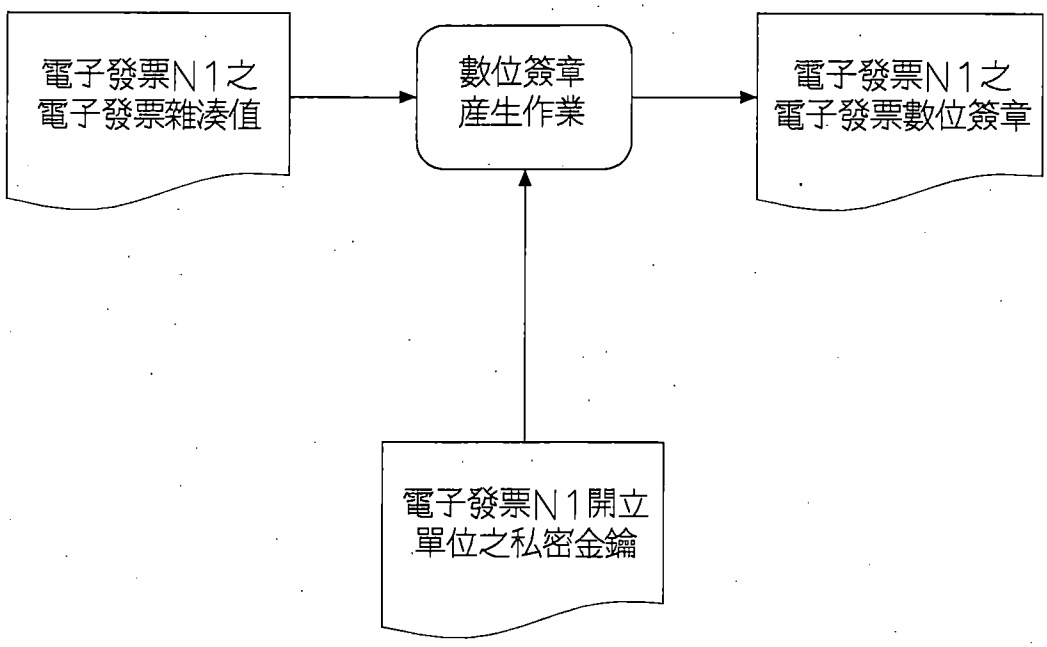
電子發票N1之
電子發票雜湊值
數位簽章
產生作業
電子發票N1之
電子發票數位簽章
電子發票N1開立
單位之私密金鑰

圖 6

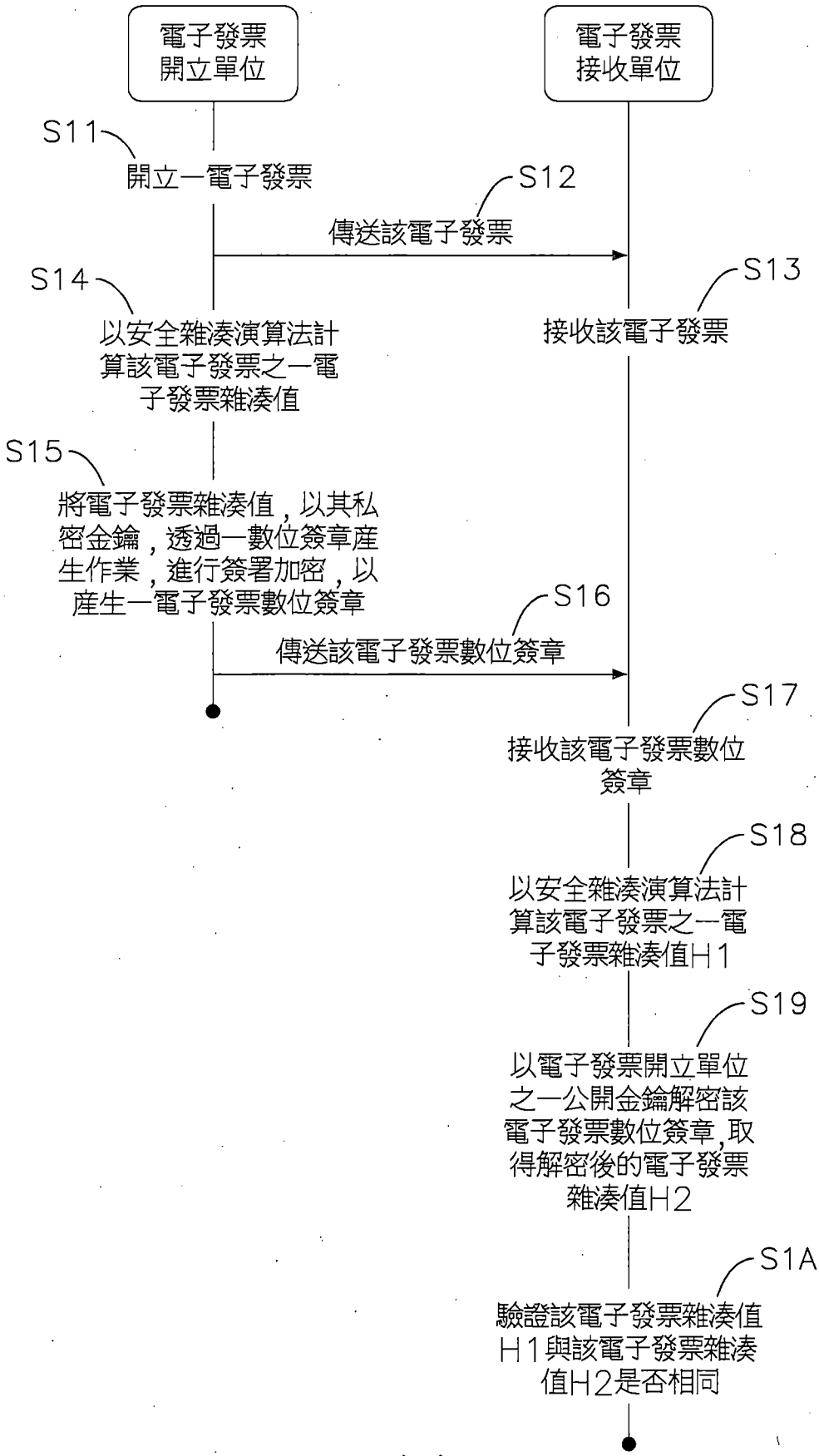
電子發票
開立單位
電子發票
接收單位
S11
開立一電子發票
S12
傳送該電子發票
S13
接收該電子發票
S14
以安全雜湊演算法計
算該電子發票之一電
子發票雜湊值
S15
將電子發票雜湊值，以其私
密金鑰，透過一數位簽章產
生作業，進行簽署加密，以
產生一電子發票數位簽章
S16
傳送該電子發票數位簽章
S17
接收該電子發票數位
簽章
S18
以安全雜湊演算法計
算該電子發票之一電
子發票雜湊值H1
S19
以電子發票開立單位
之一公開金鑰解密該
電子發票數位簽章，取
得解密後的電子發票
雜湊值H2
S1A
驗證該電子發票雜湊值
H1與該電子發票雜湊
值H2是否相同

圖 7

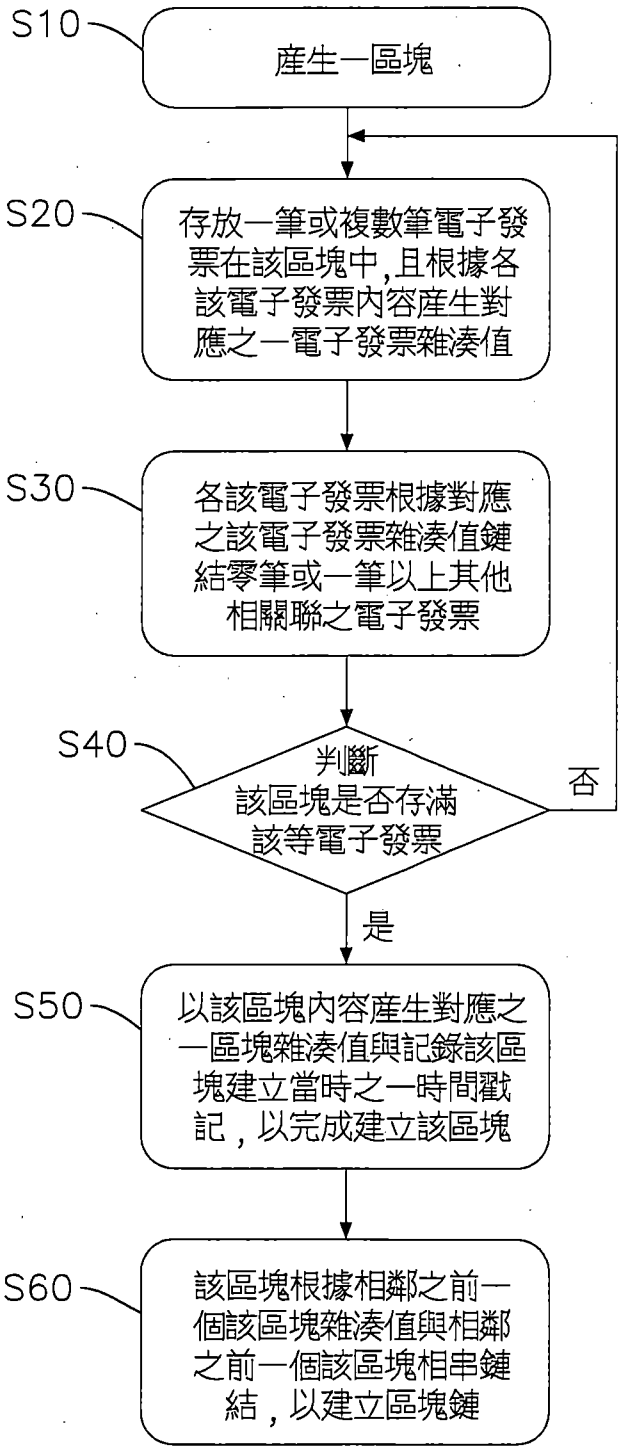
S10
產生一區塊
S20
存放一筆或複數筆電子發票在該區塊中,且根據各該電子發票內容產生對應之一電子發票雜湊值
S30
各該電子發票根據對應之該電子發票雜湊值鏈結零筆或一筆以上其他相關聯之電子發票
S40
判斷該區塊是否存滿該等電子發票
否
是
S50
以該區塊內容產生對應之一區塊雜湊值與記錄該區塊建立當時之一時間戳記，以完成建立該區塊
S60
該區塊根據相鄰之前一個該區塊雜湊值與相鄰之前一個該區塊相串鏈結，以建立區塊鏈

圖 8

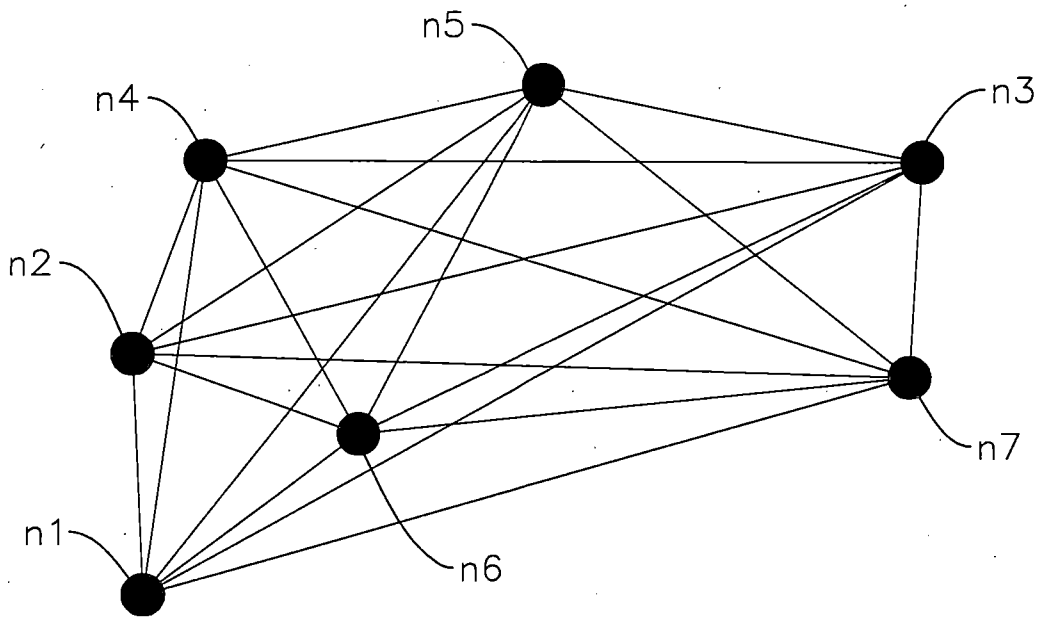

圖 9