



(19)中華民國智慧財產局

(12)發明說明書公告本

(11)證書號數：TW I713840 B

(45)公告日：中華民國 109 (2020) 年 12 月 21 日

(21)申請案號：107115530

(22)申請日：中華民國 107 (2018) 年 05 月 08 日

(51)Int. Cl. : **G06Q20/40 (2012.01)**

(30)優先權：2017/07/26 中國大陸 201710617611.4

(71)申請人：開曼群島商創新先進技術有限公司(開曼群島) ADVANCED NEW TECHNOLOGIES
CO., LTD. (KY)

開曼群島

(72)發明人：邱鴻霖 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW M543413U

CN 106789090A

US 9635000B1

<https://www.semanticscholar.org/paper/Tendermint-%3A-Consensus-without-Mining-Kwon/0841ac8b72c7a493dd7cdf42e6d54fc5b90ae343>

審查人員：李京歡

申請專利範圍項數：17 項 圖式數：12 共 58 頁

(54)名稱

數位憑證管理方法、裝置及電子設備

(57)摘要

本發明公開了一種數位憑證管理方法，包括：接收區塊鏈中的節點發送的數位憑證上鏈請求，所述數位憑證上鏈請求中包含由所述節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將所述待校驗數位憑證寫入所述區塊鏈；確定對所述節點的待校驗數位憑證進行共識校驗的結果；依據共識校驗的結果，確定是否將所述待校驗數位憑證寫入所述區塊鏈。本發明還公開了相對應的裝置和電子設備等。

指定代表圖：

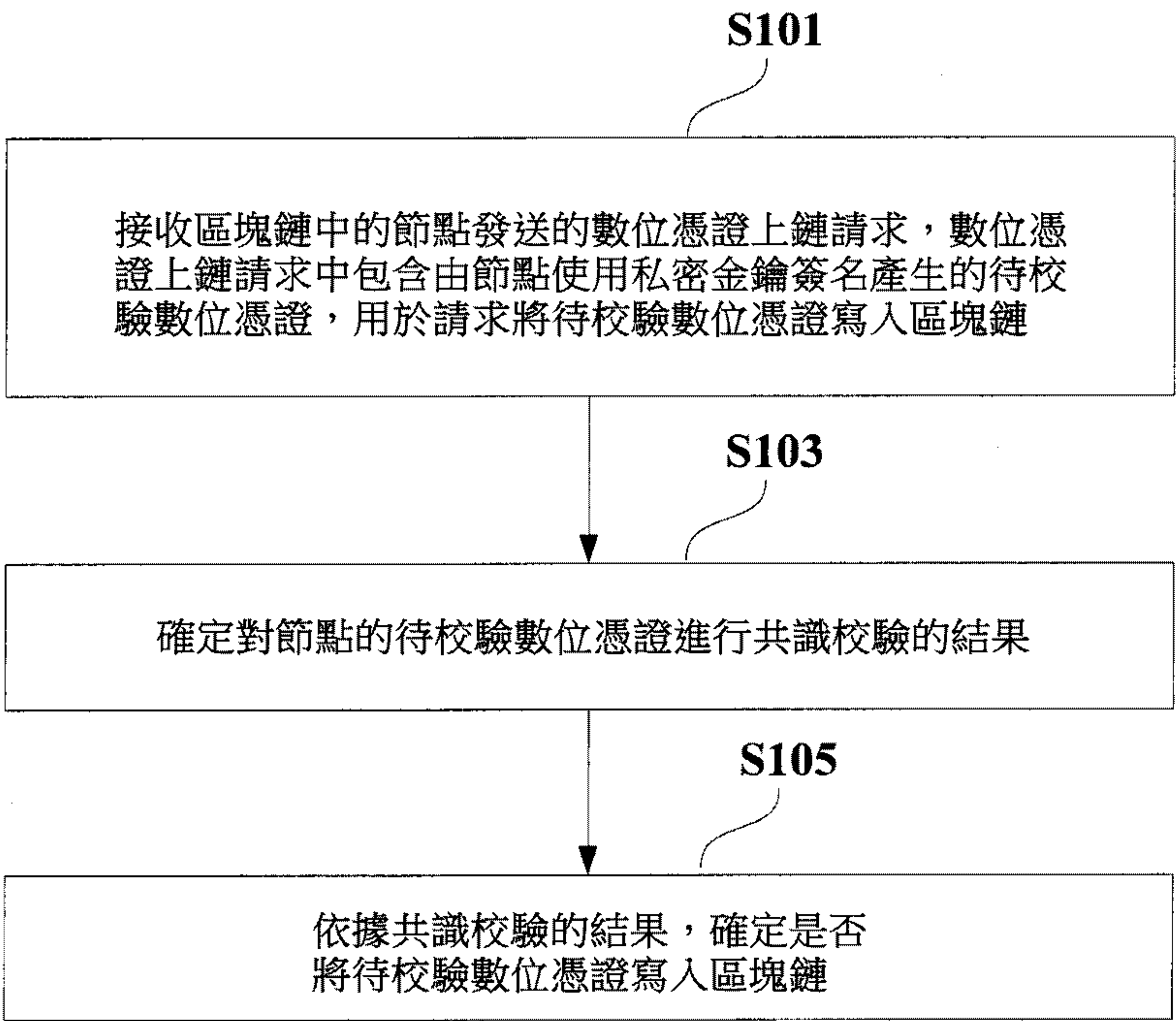


圖 1



I713840

【發明摘要】

【中文發明名稱】

數位憑證管理方法、裝置及電子設備

【中文】

本發明公開了一種數位憑證管理方法，包括：接收區塊鏈中的節點發送的數位憑證上鏈請求，所述數位憑證上鏈請求中包含由所述節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將所述待校驗數位憑證寫入所述區塊鏈；確定對所述節點的待校驗數位憑證進行共識校驗的結果；依據共識校驗的結果，確定是否將所述待校驗數位憑證寫入所述區塊鏈。本發明還公開了相對應的裝置和電子設備等。

【指定代表圖】第(1)圖。
【代表圖之符號簡單說明】無

【特徵化學式】無

【發明說明書】

【中文發明名稱】

數位憑證管理方法、裝置及電子設備

【技術領域】

本發明涉及電腦技術領域，尤其涉及數位憑證管理的方法、裝置及電子設備。

【先前技術】

隨著電腦技術的發展，區塊鏈技術(又稱分散式帳本技術)以其去中心化、公開透明、不可篡改、可信任等優點，備受青睞，在智慧合約、證券交易、電子商務、物聯網、社交通訊、檔儲存、存在性證明、身份驗證、股權眾籌等眾多領域得到廣泛應用。

目前，區塊鏈系統主要可分為三類，分別是公有鏈(Public Blockchain)、私有鏈(Private Blockchain)和聯盟鏈(Consortium Blockchain)。這三類區塊鏈的主要區別在於開放對象的不同。公有鏈可對所有人開放，私有鏈僅對單獨的個人或實體組織開放，而聯盟鏈介於公有鏈和私有鏈之間，對特定的個人或實體組織開放，而對之外的其他個人或實體組織加以限制。

在區塊鏈中，尤其是在面向特定組織的聯盟鏈中，為了提高通訊安全，通常會設計憑證授權中心(全稱Certificate Authority，可簡稱為CA中心)，為每個參與區

塊鏈通訊的節點簽發節點憑證，使得持有合法憑證的節點才能夠互相通訊。在現有技術中，會將簽發的節點憑證以及與憑證有效性有關的資訊，例如憑證撤銷清單等，都儲存在CA中心的伺服器中；區塊鏈的節點間需要通訊時，也將調用並查詢CA中心儲存的與憑證有效性有關的資訊，以便確認憑證的有效性，完成對通訊過程的驗證。這種方式的主要缺陷在於：

節點的數位憑證以及與憑證有效性有關的資訊均儲存在CA中心，一旦CA中心被黑，駭客可以任意修改與憑證有效性有關的資訊，例如，可以篡改憑證撤銷清單，使得已吊銷的憑證恢復正常。駭客進而可以利用這些原本被吊銷的問題憑證非法加入區塊鏈，區塊鏈節點在確認憑證有效性時也將依據被篡改的資訊進行，從而對區塊鏈的安全造成威脅。更有甚者，CA中心的私密金鑰也可能被駭客盜取，進而駭客可以恣意簽發數位憑證，威脅著區塊鏈網路的安全。

【發明內容】

本發明實施例提供數位憑證管理方法、裝置及相應的電子設備，旨在提高區塊鏈網路的安全性。

本發明實施例採用下述技術方案：

第一方面，本發明實施例提供一種數位憑證管理方法，包括：

接收區塊鏈中的節點發送的數位憑證上鏈請求，所述

數位憑證上鏈請求中包含由所述節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將所述待校驗數位憑證寫入所述區塊鏈；

確定對所述節點的待校驗數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否將所述待校驗數位憑證寫入所述區塊鏈。

優選的，在第一方面提供的數位憑證管理方法中，確定對所述節點的待校驗數位憑證進行共識校驗的結果，包括：

確定所述區塊鏈中參與共識校驗的節點的校驗結果；

確定所述參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，所述第一節點的校驗結果為通過共識校驗，所述第二節點的校驗結果為未通過共識校驗；

依據所述第一節點的數量和/或第二節點的數量確定共識校驗的結果。

優選的，在第一方面提供的數位憑證管理方法中，依據所述第一節點的數量確定共識校驗的結果，包括：

當所述第一節點的數量滿足第一預設條件時，確定共識校驗的結果為通過共識校驗；

滿足所述第一預設條件包括以下一項或多項：

所述第一節點的數量達到第一預設閾值；

所述第一節點的數量與所述參與共識校驗的節點的數

量的比值達到第二預設閾值；

所述第一節點的數量與所述區塊鏈的節點的數量的比值達到第三預設閾值。

優選的，在第一方面提供的數位憑證管理方法中，依據共識校驗的結果，確定是否將所述待校驗數位憑證寫入所述區塊鏈，包括：

當所述共識校驗的結果為通過共識校驗時，將所述待校驗數位憑證寫入所述區塊鏈。

優選的，在第一方面提供的數位憑證管理方法中，所述方法還包括：

接收所述區塊鏈中的節點發送的數位憑證吊銷請求，所述數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

確定對所述目標節點的數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否吊銷所述目標節點的數位憑證。

第二方面，本發明實施例提供一種數位憑證管理方法，包括：

接收區塊鏈中的節點發送的數位憑證吊銷請求，所述數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

確定對所述目標節點的數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否在所述區塊鏈中吊銷所述目標節點的數位憑證。

優選的，在第二方面提供的數位憑證管理方法中，確定對所述目標節點的數位憑證進行共識校驗的結果，包括：

確定所述區塊鏈中參與共識校驗的節點的校驗結果；

確定所述參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，所述第一節點的校驗結果為通過共識校驗，所述第二節點的校驗結果為未通過共識校驗；

依據所述第一節點的數量和/或第二節點的數量確定共識校驗的結果。

優選的，在第二方面提供的數位憑證管理方法中，依據所述第一節點的數量確定共識校驗的結果，包括：

當所述第一節點的數量滿足第一預設條件時，確定共識校驗的結果為通過共識校驗；

滿足所述第一預設條件包括以下一項或多項：

所述第一節點的數量達到第一預設閾值；

所述第一節點的數量與所述參與共識校驗的節點的數量的比值達到第二預設閾值；

所述第一節點的數量與所述區塊鏈的節點的數量的比值達到第三預設閾值。

優選的，在第二方面提供的數位憑證管理方法中，依據共識校驗的結果，確定是否在所述區塊鏈中吊銷所述目

標節點的數位憑證，包括：

當所述共識校驗的結果為通過共識校驗時，在所述區塊鏈中吊銷所述目標節點的數位憑證。

第三方面，本發明實施例提供一種數位憑證管理方法，包括：

區塊鏈中的節點向區塊鏈中發送數位憑證上鏈請求，用於供所述區塊鏈確定對所述節點的待校驗數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否將所述待校驗數位憑證寫入所述區塊鏈；

其中，所述數位憑證上鏈請求中包含由所述節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將所述待校驗數位憑證寫入所述區塊鏈。

第四方面，本發明實施例提供一種數位憑證管理方法，包括：

區塊鏈中的節點向區塊鏈中發送數位憑證吊銷請求，用於供所述區塊鏈確定對目標節點的數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否在所述區塊鏈中吊銷所述目標節點的數位憑證；

其中，所述數位憑證吊銷請求中包含請求吊銷的所述目標節點的數位憑證。

第五方面，本發明實施例提供一種數位憑證管理裝置，用於區塊鏈，包括：

請求接收模組，接收區塊鏈中的節點發送的數位憑證上鏈請求，所述數位憑證上鏈請求中包含由所述節點使用

私密金鑰簽名產生的待校驗數位憑證，用於請求將所述待校驗數位憑證寫入所述區塊鏈；

共識校驗結果確定模組，確定對所述節點的待校驗數位憑證進行共識校驗的結果；

憑證管理模組，依據共識校驗的結果，確定是否將所述待校驗數位憑證寫入所述區塊鏈。

第六方面，本發明實施例提供一種電子設備，用於區塊鏈，包括：

處理器；以及

被安排成儲存電腦可執行指令的記憶體，所述可執行指令在被執行時使所述處理器執行以下操作：

接收區塊鏈中的節點發送的數位憑證上鏈請求，所述數位憑證上鏈請求中包含由所述節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將所述待校驗數位憑證寫入所述區塊鏈；

確定對所述節點的待校驗數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否將所述待校驗數位憑證寫入所述區塊鏈。

第七方面，本發明實施例提供一種數位憑證管理裝置，用於區塊鏈，包括：

請求接收模組，接收區塊鏈中的節點發送的數位憑證吊銷請求，所述數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

共識校驗結果確定模組，確定對所述目標節點的數位憑證進行共識校驗的結果；

憑證管理模組，依據共識校驗的結果，確定是否在所述區塊鏈中吊銷所述目標節點的數位憑證。

第八方面，本發明實施例提供一種電子設備，用於區塊鏈，包括：

處理器；以及

被安排成儲存電腦可執行指令的記憶體，所述可執行指令在被執行時使所述處理器執行以下操作：

接收區塊鏈中的節點發送的數位憑證吊銷請求，所述數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

確定對所述目標節點的數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否在所述區塊鏈中吊銷所述目標節點的數位憑證。

第九方面，本發明實施例提供一種數位憑證管理裝置，用於區塊鏈中的節點，包括：

請求發起模組，向區塊鏈中發送數位憑證上鏈請求，用於供所述區塊鏈確定對所述節點的待校驗數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否將所述待校驗數位憑證寫入所述區塊鏈；其中，所述數位憑證上鏈請求中包含由所述節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將所述待校驗數位憑證寫入所述區

塊鏈。

第十方面，本發明實施例提供一種電子設備，用於區塊鏈中的節點，包括：

處理器；以及

被安排成儲存電腦可執行指令的記憶體，所述可執行指令在被執行時使所述處理器執行以下操作：

向區塊鏈中發送數位憑證上鏈請求，用於供所述區塊鏈確定對所述節點的待校驗數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否將所述待校驗數位憑證寫入所述區塊鏈；其中，所述數位憑證上鏈請求中包含由所述節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將所述待校驗數位憑證寫入所述區塊鏈。

第十一方面，本發明實施例提供一種數位憑證管理裝置，用於區塊鏈中的節點，包括：

請求發起模組，向區塊鏈中發送數位憑證吊銷請求，用於供所述區塊鏈確定對目標節點的數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否在所述區塊鏈中吊銷所述目標節點的數位憑證；其中，所述數位憑證吊銷請求中包含請求吊銷的所述目標節點的數位憑證。

第十二方面，本發明實施例提供一種電子設備，用於區塊鏈中的節點，包括：

處理器；以及

被安排成儲存電腦可執行指令的記憶體，所述可執行指令在被執行時使所述處理器執行以下操作：

向區塊鏈中發送數位憑證吊銷請求，用於供所述區塊鏈確定對目標節點的數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否在所述區塊鏈中吊銷所述目標節點的數位憑證；其中，所述數位憑證吊銷請求中包含請求吊銷的所述目標節點的數位憑證。

本發明實施例採用的上述至少一個技術方案能夠達到以下有益效果：

採用本發明實施例的方案，將傳統的CA中心的功能改由區塊鏈實現，當區塊鏈中的某節點需要申請數位憑證時，可以使用區塊鏈內部私密金鑰自行簽名，產生待校驗的數位憑證，進一步經過區塊鏈網路進行共識校驗通過之後入鏈，方才成為合法有效的數位憑證。這一系列數位憑證簽發、驗證、儲存的過程均在區塊鏈中進行。

由於在本發明實施例中，需要經過共識校驗的數位憑證才能入鏈，而只有入鏈的數位憑證才是合法的數位憑證，因此，即使某一節點被駭客攻擊，或者駭客取得了CA私密金鑰可以隨意簽發數位憑證，駭客也無法在區塊鏈中取得合法的數位憑證，從而無法加入區塊鏈網路進行非法通訊。因此，基於區塊鏈去中心化、公開透明、不可篡改等優點，採用這種去中心化的架構對數位憑證進行管理，提高了區塊鏈網路的安全性。

【圖式簡單說明】

此處所說明的圖式用來提供對本發明的進一步理解，

構成本發明的一部分，本發明的示意性實施例及其說明用於解釋本發明，並不構成對本發明的不當限定。在圖式中：

圖1為本發明實施例中一種數位憑證管理方法的流程示意圖；

圖2為本發明實施例中第二種數位憑證管理方法的流程示意圖；

圖3為本發明實施例中第三種數位憑證管理方法的流程示意圖；

圖4為本發明實施例的實施場景示意圖；

圖5為本發明實施例中一種數位憑證管理裝置的流程示意圖；

圖6為本發明實施例中一種電子設備的流程示意圖；

圖7為本發明實施例中第二種數位憑證管理裝置的流程示意圖；

圖8為本發明實施例中第二種電子設備的流程示意圖；

圖9為本發明實施例中第三種數位憑證管理裝置的流程示意圖；

圖10為本發明實施例中第三種電子設備的流程示意圖；

圖11為本發明實施例中第四種數位憑證管理裝置的流程示意圖；

圖12為本發明實施例中第四種電子設備的流程示意圖；

圖。

【實施方式】

為使本發明的目的、技術方案和優點更加清楚，下面將結合本發明具體實施例及相應的圖式對本發明技術方案進行清楚、完整地描述。顯然，所描述的實施例僅是本發明一部分實施例，而不是全部的實施例。基於本發明中的實施例，本領域普通技術人員在沒有做出創造性勞動前提下所獲得的所有其他實施例，都屬於本發明保護的範圍。

以下結合圖式，詳細說明本發明各實施例提供的技術方案。

參見圖1所示，本發明實施例提供了一種數位憑證管理方法，包括：

S101：接收區塊鏈中的節點發送的數位憑證上鏈請求，數位憑證上鏈請求中包含由節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將待校驗數位憑證寫入區塊鏈；

S103：確定對節點的待校驗數位憑證進行共識校驗的結果；

S105：依據共識校驗的結果，確定是否將待校驗數位憑證寫入區塊鏈。

可以理解到，上述區塊鏈中發送數位憑證上鏈請求的節點，可以是區塊鏈中希望申請數位憑證的任一節點。在本發明實施例中，該節點可以使用在區塊鏈中公開的私密

金鑰自行簽名，產生待校驗數位憑證，進而向區塊鏈發送包含有該待校驗數位憑證的數位憑證上鏈請求，以便請求區塊鏈將該待校驗數位憑證寫入區塊鏈。在具體實施時，該節點可以採用全網廣播的方式發送上述數位憑證上鏈請求。

上述節點的自行簽發的待校驗數位憑證，雖然在入鏈之前並未生效，但其在內容和形式上可以與合法生效的數位憑證沒有本質區別。在本發明實施例中，可體現為標誌通訊節點身份資訊的一串數字，可以攜帶包含憑證版本號、憑證持有者資訊(例如，可以具體體現為憑證所對應的節點的身份資訊)、憑證簽發者資訊(此處可以與憑證持有者資訊相同，也可以反映私密金鑰的來源)、憑證起止有效期、憑證序號、憑證簽發者的簽名等內容。

由於上述節點自行簽發的待校驗數位憑證並未生效，而只有寫入了區塊鏈的數位憑證才是合法的數位憑證，合法的數位憑證對應的節點才能夠正常的參與區塊鏈的通訊，因此，在本發明實施例中，即使公開了簽發憑證所需的私密金鑰，也不會造成數位憑證管理的混亂，不會影響區塊鏈網路的安全。相反的，合法的數位憑證經由區塊鏈執行以下步驟S103進行全網共識校驗後產生，提高了區塊鏈網路的安全性。

區塊鏈在接收到上述數位憑證上鏈請求後，可以對該請求進行解析，得到該請求中包含的待校驗數位憑證。而後對該節點的待校驗數位憑證進行共識校驗。所謂共識校

驗，可以理解為區塊鏈上的各節點都可以參與對待校驗數位憑證的校驗，按照區塊鏈的共識機制確定共識校驗的結果。

區塊鏈上的各節點在具體實施校驗時，可以按照預先約定的校驗標準進行。校驗的內容可以與待校驗數位憑證中的資訊相關，例如：有效期是否過期，序號是否符合要求，申請節點的身份資訊是否符合要求等等。

由於點對點網路下可能存在的網路延遲，區塊鏈中各個節點接收到數位憑證上鏈請求的時間及對該請求的回應速度可能不一樣，因此，在區塊鏈中接收速度和回應速度快的節點將有更多的機會參與對待校驗數位憑證的共識校驗。

區塊鏈上參與共識校驗的節點在完成對待校驗數位憑證的校驗後，可以採用全網廣播的方式將校驗的結果發送到區塊鏈(可具體為區塊鏈中的各節點)。與之相對應地，區塊鏈在執行步驟S103確定對節點的待校驗數位憑證進行共識校驗的結果時，參見圖2所示，可以具體包括：

S301：確定區塊鏈中參與共識校驗的節點的校驗結果；

可以理解到，校驗結果可能為“通過共識校驗”，也可能為“未通過共識校驗”。除此之外，執行這一步驟的時機，可以是自廣播待校驗數位憑證起算的預設時間之後，可以是共識校驗開始後即時進行，也可以是週期性的確定，還可以是當參與共識校驗的節點的數量達到預設數值

時進行。在本發明實施例中，為得到滿足區塊鏈的共識機制的共識校驗結果，步驟S301~S305中，各步驟自身、以及組合，都可能迴圈執行多次，本發明實施例對此不做限定。

S303：確定參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，第一節點的校驗結果為通過共識校驗，第二節點的校驗結果為未通過共識校驗；

具體地，在參與共識校驗的節點將各自的校驗結果廣播公告之後，可按照校驗結果的不同，將這些節點區分為校驗結果為“通過共識校驗”的第一節點和校驗結果為“未通過共識校驗”的第二節點。在此基礎上，可以擇一或同時統計校驗結果不同的兩種節點的數量，以便判斷是否達到共識機制所約定的確定共識校驗結果的條件。

在確定節點的數量時，可以統計節點的絕對數量，例如，假設參與共識校驗的節點共10個，其中，第一節點有4個，第二節點有6個。也可以按照節點在共識校驗過程中的權重不同(具體權重可以由區塊鏈的共識機制確定)，統計節點的加權數量，例如，假設參與共識校驗的節點共4個，其中，第一節點和第二節點的絕對數量相同，均為2個；2個第一節點的權重分別為0.5和1.2，2個第二節點的權重分別為2和4；則第一節點的數量的計算運算式為： $1*0.5+1*1.2=1.7$ ，第二節點的數量的計算運算式為 $1*2+1*4=6$ 。

S305：依據第一節點的數量和/或第二節點的數量確

定共識校驗的結果。

可以理解到，依據區塊鏈的共識機制的不同，既可以依據校驗結果為“通過共識校驗”的第一節點的數量確定共識校驗的結果，也可以依據校驗結果為“未通過共識校驗”的第二節點的數量確定，還可以同時依據這兩種節點的數量確定。本發明實施例中對此不做限定。

若依據第一節點的數量確定共識校驗的結果，可以考察第一節點的數量是否滿足以下一項或多項條件：

第一節點的數量達到第一預設閾值；

第一節點的數量與參與共識校驗的節點的數量的比值達到第二預設閾值；

第一節點的數量與區塊鏈的節點的數量的比值達到第三預設閾值。

可以理解到，根據區塊鏈中共識機制的不同，可以預設不同的條件以確定共識校驗的結果。以上例舉的三方面判斷，都能反映第一節點的數量達到了一定的程度，表示已有足夠多(依據共識機制的設計不同，具體的標準可以不同)的區塊鏈節點對待校驗數位憑證的校驗結果為“通過共識校驗”。因此，若滿足以上條件，則可認為共識校驗的結果為“通過共識校驗”，這一結果可以理解為區塊鏈中達到足夠數量要求的節點認為請求入鏈的待校驗數位憑證是合法的，從而可進一步將待校驗數位憑證寫入區塊鏈，以便將這一合法的數位憑證儲存在區塊鏈中，使得該數位憑證對應的節點能夠在區塊鏈中正常通訊。

若依據第二節點的數量確定共識校驗的結果，則若有足夠多(類似地，依據共識機制的設計不同，具體的標準可以不同)的節點對待校驗數位憑證的校驗結果為“未通過共識校驗”，表示區塊鏈中達到足夠數量要求的節點認為請求入鏈的待校驗數位憑證是不合法的。因此，該待校驗數位憑證不能寫入區塊鏈成為合法的數位憑證，相應地，該待校驗數位憑證所對應的節點也無法參與區塊鏈網路的通訊。可以理解到，依據第二節點的數量確定共識校驗的結果的具體標準可以與前述舉例類似，由區塊鏈的共識機制的設計決定，此處不再贅述。

與以上區塊鏈一側執行的實施例相對應地，本發明實施例還提供了一種數位憑證管理方法，由申請數位憑證的節點一側執行，具體可包括：

區塊鏈中的節點向區塊鏈中發送數位憑證上鏈請求，用於供區塊鏈確定對節點的待校驗數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否將待校驗數位憑證寫入區塊鏈；

其中，數位憑證上鏈請求中包含由節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將待校驗數位憑證寫入區塊鏈。

以上區塊鏈一側執行的實施例中的相關闡述均適用於此處，不再贅述。

採用本發明實施例對數位憑證的管理，除了體現在數位憑證的簽發、校驗和入鏈的過程之外，還可以進行數位

憑證的吊銷。具體地，本發明實施例還提供了一種數位憑證管理方法，可以採用以下步驟實現對已經入鏈的合法的數位憑證進行吊銷，參見圖3所示：

S201：接收區塊鏈中的節點發送的數位憑證吊銷請求，數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

S203：確定對目標節點的數位憑證進行共識校驗的結果；

S205：依據共識校驗的結果，確定是否吊銷目標節點的數位憑證。

具體地，步驟S203確定對目標節點的數位憑證進行共識校驗的結果，可以具體包括：

確定區塊鏈中參與共識校驗的節點的校驗結果；

確定參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，第一節點的校驗結果為通過共識校驗，第二節點的校驗結果為未通過共識校驗；

依據第一節點的數量和/或第二節點的數量確定共識校驗的結果。

更進一步地，依據第一節點的數量確定共識校驗的結果，可以包括：

當第一節點的數量滿足第一預設條件時，確定共識校驗的結果為通過共識校驗；

滿足第一預設條件包括以下一項或多項：

第一節點的數量達到第一預設閾值；

第一節點的數量與參與共識校驗的節點的數量的比值達到第二預設閾值；

第一節點的數量與區塊鏈的節點的數量的比值達到第三預設閾值。

當以上共識校驗的結果為通過共識校驗時，在區塊鏈中吊銷目標節點的數位憑證。

可以理解到，對於區塊鏈中各節點而言，均可發起數位憑證吊銷請求，既可以請求吊銷自己的數位憑證，也可以請求吊銷其他問題節點的數位憑證，此處無需限定。並且，不難理解到，數位憑證吊銷請求中，除包含請求吊銷的目標節點的數位憑證之外，還可以包含吊銷該目標節點的數位憑證的原因，以便區塊鏈中各節點參與共識校驗時判斷是否通過共識校驗。

需要說明的是，在針對數位憑證吊銷請求進行共識校驗時，發起數位憑證吊銷請求的節點與上述目標節點，均可能參與共識校驗的過程。而在針對數位憑證上鏈請求進行共識校驗時，發起該請求的節點將無法參與共識校驗的過程，因為該節點尚未取得合法的數位憑證，無法加入區塊鏈網路。

還需要說明的是，在針對數位憑證吊銷請求進行共識校驗時，第一節點的校驗結果為“通過共識校驗”，表示第一節點同意吊銷目標節點的數位憑證；第二節點的校驗結果為“未通過共識校驗”，表示第二節點不同意吊銷目標節點的數位憑證。上述實施例可以在此基礎上，依據第一節

點的數量和/或第二節點的數量確定共識校驗的結果，以便確定是否吊銷目標節點的數位憑證。具體地確定共識校驗的結果的過程，與對待校驗數位憑證的共識校驗類似，具體的標準由共識機制確定，此處不再贅述。

與圖3所示區塊鏈一側執行的實施例相對應地，本發明實施例還提供了一種數位憑證管理方法，由申請數位憑證的節點一側執行，具體可包括：

區塊鏈中的節點向區塊鏈中發送數位憑證吊銷請求，用於供區塊鏈確定對目標節點的數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否在區塊鏈中吊銷目標節點的數位憑證；

其中，數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證。

以上區塊鏈一側執行的實施例中的相關闡述均適用於此處，不再贅述。

圖4簡化的呈現出了區塊鏈網路中在數位憑證管理中的資訊交互過程。以簽發、校驗、上鏈數位憑證的過程為例，具體包括以下步驟：

S11：節點4作為發起節點，使用公開的私密金鑰為自己簽名，產生待校驗的數位憑證；

S12：節點4將產生的待校驗數位憑證廣播到區塊鏈中；

S13：節點1、節點2和節點3先後參與對待校驗數位憑證的共識校驗；若共識校驗的結果為“通過共識校驗”，則

區塊鏈中各節點(不限於節點1~4)將節點4的待校驗數位憑證作為合法有效的數位憑證入鏈。至此，節點4取得合法有效的數位憑證，能夠正常的參與區塊鏈網路的通訊。

可以理解到，對數位憑證進行吊銷的過程與之類似，主要區別在於，發起的節點發送的請求由數位憑證上鏈請求改變為數位憑證吊銷請求。此處不再贅述。

採用本發明實施例的方案，將傳統的CA中心的功能改由區塊鏈實現，當區塊鏈中的某節點需要申請數位憑證時，可以使用區塊鏈內部私密金鑰自行簽名，產生待校驗的數位憑證，進一步經過區塊鏈網路進行共識校驗通過之後入鏈，方才成為合法有效的數位憑證。這一系列數位憑證簽發、驗證、儲存的過程均在區塊鏈中進行。數位憑證的吊銷過程也可在區塊鏈中進行。

由於在本發明實施例中，需要經過共識校驗的數位憑證才能入鏈，而只有入鏈的數位憑證才是合法的數位憑證，因此，即使某一節點被駭客攻擊，或者駭客取得了CA私密金鑰可以隨意簽發數位憑證，駭客也無法在區塊鏈中取得合法的數位憑證，從而無法加入區塊鏈網路進行非法通訊。因此，基於區塊鏈去中心化、公開透明、不可篡改等優點，採用這種去中心化的架構對數位憑證進行管理，提高了區塊鏈網路的安全性。

參見圖5所示，本發明實施例還提供一種數位憑證管理裝置，用於區塊鏈，包括：

請求接收模組101，接收區塊鏈中的節點發送的數位

憑證上鏈請求，數位憑證上鏈請求中包含由節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將待校驗數位憑證寫入區塊鏈；

共識校驗結果確定模組 103，確定對節點的待校驗數位憑證進行共識校驗的結果；

憑證管理模組 105，依據共識校驗的結果，確定是否將待校驗數位憑證寫入區塊鏈。

圖 6 是本發明的一個實施例電子設備的結構示意圖。請參考圖 6，在硬體層面，該電子設備包括處理器，可選地還包括內部匯流排、網路介面、記憶體。其中，記憶體可能包含記憶體，例如高速隨機存取記憶體 (Random-Access Memory, RAM)，也可能還包括非易失性記憶體 (non-volatile memory)，例如至少 1 個磁碟記憶體等。當然，該電子設備還可能包括其他業務所需要的硬體。

處理器、網路介面和記憶體可以通過內部匯流排相互連接，該內部匯流排可以是 ISA (Industry Standard Architecture，工業標準架構) 匯流排、PCI (Peripheral Component Interconnect，外設部件互連標準) 匯流排或 EISA (Extended Industry Standard Architecture，延伸工業標準架構) 匯流排等。所述匯流排可以分為位址匯流排、資料匯流排、控制匯流排等。為便於表示，圖 6 中僅用一個雙向箭頭表示，但並不表示僅有一根匯流排或一種類型的匯流排。

記憶體，用於存放程式。具體地，程式可以包括程式碼，所述程式碼包括電腦操作指令。記憶體可以包括記憶

體和非易失性記憶體，並向處理器提供指令和資料。

處理器從非易失性記憶體中讀取對應的電腦程式到記憶體中然後運行，在邏輯層面上形成數位憑證管理裝置。處理器，執行記憶體所存放的程式，並具體用於執行以下操作：

接收區塊鏈中的節點發送的數位憑證上鏈請求，數位憑證上鏈請求中包含由節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將待校驗數位憑證寫入區塊鏈；

確定對節點的待校驗數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否將待校驗數位憑證寫入區塊鏈。

上述如本發明圖1所示實施例揭示的數位憑證管理裝置執行的方法可以應用於處理器中，或者由處理器實現。處理器可能是一種積體電路晶片，具有信號的處理能力。在實現過程中，上述方法的各步驟可以通過處理器中的硬體的積體邏輯電路或者軟體形式的指令完成。上述的處理器可以是通用處理器，包括中央處理器(Central Processing Unit, CPU)、網路處理器(Network Processor, NP)等；還可以是數位訊號處理器(Digital Signal Processor, DSP)、專用積體電路(Application Specific Integrated Circuit, ASIC)、現場可程式設計閘陣列(Field-Programmable Gate Array, FPGA)或者其他可程式設計邏輯器件、分立閘或者電晶體邏輯器件、分立硬體元件。可以實現或者執行本發明實施例中的公開的各方法、步驟及邏輯方塊圖。通用處

理器可以是微處理器或者該處理器也可以是什麼常規的處理器等。結合本發明實施例所公開的方法的步驟可以直接體現為硬體解碼處理器執行完成，或者用解碼處理器中的硬體及軟體模組組合執行完成。軟體模組可以位於隨機記憶體，快閃記憶體、唯讀記憶體，可程式設計唯讀記憶體或者電可讀寫可程式設計記憶體、暫存器等本領域成熟的儲存媒體中。該儲存媒體位於記憶體，處理器讀取記憶體中的資訊，結合其硬體完成上述方法的步驟。

該電子設備還可執行圖1中數位憑證管理裝置執行的方法，並實現數位憑證管理裝置在圖1所示實施例的功能，本發明實施例在此不再贅述。

本發明實施例還提出了一種電腦可讀儲存媒體，該電腦可讀儲存媒體儲存一個或多個程式，該一個或多個程式包括指令，該指令當被包括多個應用程式的電子設備執行時，能夠使該電子設備執行圖1所示實施例中數位憑證管理裝置執行的方法，並具體用於執行：

接收區塊鏈中的節點發送的數位憑證上鏈請求，數位憑證上鏈請求中包含由節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將待校驗數位憑證寫入區塊鏈；

確定對節點的待校驗數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否將待校驗數位憑證寫入區塊鏈。

本發明實施例還提供一種數位憑證管理裝置，用於區塊鏈，參見圖7所示，包括：

請求接收模組 201，接收區塊鏈中的節點發送的數位憑證吊銷請求，數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

共識校驗結果確定模組 203，確定對目標節點的數位憑證進行共識校驗的結果；

憑證管理模組 205，依據共識校驗的結果，確定是否在區塊鏈中吊銷目標節點的數位憑證。

圖 8 是本發明的一個實施例電子設備的結構示意圖。請參考圖 8，在硬體層面，該電子設備包括處理器，可選地還包括內部匯流排、網路介面、記憶體。其中，記憶體可能包含記憶體，例如高速隨機存取記憶體 (Random-Access Memory, RAM)，也可能還包括非易失性記憶體 (non-volatile memory)，例如至少 1 個磁碟記憶體等。當然，該電子設備還可能包括其他業務所需要的硬體。

處理器、網路介面和記憶體可以通過內部匯流排相互連接，該內部匯流排可以是 ISA (Industry Standard Architecture，工業標準架構) 匯流排、PCI (Peripheral Component Interconnect，外設部件互連標準) 匯流排或 EISA (Extended Industry Standard Architecture，延伸工業標準架構) 匯流排等。所述匯流排可以分為位址匯流排、資料匯流排、控制匯流排等。為便於表示，圖 8 中僅用一個雙向箭頭表示，但並不表示僅有一根匯流排或一種類型的匯流排。

記憶體，用於存放程式。具體地，程式可以包括程式碼，所述程式碼包括電腦操作指令。記憶體可以包括記憶

體和非易失性記憶體，並向處理器提供指令和資料。

處理器從非易失性記憶體中讀取對應的電腦程式到記憶體中然後運行，在邏輯層面上形成數位憑證管理裝置。處理器，執行記憶體所存放的程式，並具體用於執行以下操作：

接收區塊鏈中的節點發送的數位憑證吊銷請求，數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

確定對目標節點的數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否在區塊鏈中吊銷目標節點的數位憑證。上述如本發明圖3所示實施例揭示的數位憑證管理裝置執行的方法可以應用於處理器中，或者由處理器實現。處理器可能是一種積體電路晶片，具有信號的處理能力。在實現過程中，上述方法的各步驟可以通過處理器中的硬體的積體邏輯電路或者軟體形式的指令完成。上述的處理器可以是通用處理器，包括中央處理器(Central Processing Unit, CPU)、網路處理器(Network Processor, NP)等；還可以是數位訊號處理器(Digital Signal Processor, DSP)、專用積體電路(Application Specific Integrated Circuit, ASIC)、現場可程式設計閘陣列(Field-Programmable Gate Array, FPGA)或者其他可程式設計邏輯器件、分立閘或者電晶體邏輯器件、分立硬體元件。可以實現或者執行本發明實施例中的公開的各方法、步驟及邏輯方塊圖。通用處理器可以是微處理器或者該處理器也可以是任何常規的處理器等。結合本發明實施例所公開的方法的步驟可以直接

體現為硬體解碼處理器執行完成，或者用解碼處理器中的硬體及軟體模組組合執行完成。軟體模組可以位於隨機記憶體，快閃記憶體、唯讀記憶體，可程式設計唯讀記憶體或者電可讀寫可程式設計記憶體、暫存器等本領域成熟的儲存媒體中。該儲存媒體位於記憶體，處理器讀取記憶體中的資訊，結合其硬體完成上述方法的步驟。

該電子設備還可執行圖3中數位憑證管理裝置執行的方法，並實現數位憑證管理裝置在圖3所示實施例的功能，本發明實施例在此不再贅述。

本發明實施例還提出了一種電腦可讀儲存媒體，該電腦可讀儲存媒體儲存一個或多個程式，該一個或多個程式包括指令，該指令當被包括多個應用程式的電子設備執行時，能夠使該電子設備執行圖1所示實施例中應用頁面截圖上報裝置執行的方法，並具體用於執行：

接收區塊鏈中的節點發送的數位憑證吊銷請求，數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

確定對目標節點的數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否在區塊鏈中吊銷目標節點的數位憑證。

本發明實施例提供一種數位憑證管理裝置，用於區塊鏈中的節點，參見圖9所示，包括：

請求發起模組401，向區塊鏈中發送數位憑證上鏈請求，用於供區塊鏈確定對節點的待校驗數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否將待校驗

數位憑證寫入區塊鏈；其中，數位憑證上鏈請求中包含由節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將待校驗數位憑證寫入區塊鏈。

圖10是本發明的一個實施例電子設備的結構示意圖。請參考圖10，在硬體層面，該電子設備包括處理器，可選地還包括內部匯流排、網路介面、記憶體。其中，記憶體可能包含記憶體，例如高速隨機存取記憶體(Random-Access Memory, RAM)，也可能還包括非易失性記憶體(non-volatile memory)，例如至少1個磁碟記憶體等。當然，該電子設備還可能包括其他業務所需要的硬體。

處理器、網路介面和記憶體可以通過內部匯流排相互連接，該內部匯流排可以是ISA(Industry Standard Architecture，工業標準架構)匯流排、PCI(Peripheral Component Interconnect，外設部件互連標準)匯流排或EISA(Extended Industry Standard Architecture，延伸工業標準架構)匯流排等。所述匯流排可以分為位址匯流排、資料匯流排、控制匯流排等。為便於表示，圖10中僅用一個雙向箭頭表示，但並不表示僅有一根匯流排或一種類型的匯流排。

記憶體，用於存放程式。具體地，程式可以包括程式碼，所述程式碼包括電腦操作指令。記憶體可以包括記憶體和非易失性記憶體，並向處理器提供指令和資料。

處理器從非易失性記憶體中讀取對應的電腦程式到記憶體中然後運行，在邏輯層面上形成數位憑證管理裝置。處理器，執行記憶體所存放的程式，並具體用於執行以下

操作：

向區塊鏈中發送數位憑證上鏈請求，用於供區塊鏈確定對節點的待校驗數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否將待校驗數位憑證寫入區塊鏈；其中，數位憑證上鏈請求中包含由節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將待校驗數位憑證寫入區塊鏈。

上述如本發明前述實施例揭示的數位憑證管理裝置執行的方法可以應用於處理器中，或者由處理器實現。處理器可能是一種積體電路晶片，具有信號的處理能力。在實現過程中，上述方法的各步驟可以通過處理器中的硬體的積體邏輯電路或者軟體形式的指令完成。上述的處理器可以是通用處理器，包括中央處理器 (Central Processing Unit, CPU)、網路處理器 (Network Processor, NP)等；還可以是數位訊號處理器 (Digital Signal Processor, DSP)、專用積體電路 (Application Specific Integrated Circuit, ASIC)、現場可程式設計閘陣列 (Field-Programmable Gate Array, FPGA)或者其他可程式設計邏輯器件、分立閘或者電晶體邏輯器件、分立硬體元件。可以實現或者執行本發明實施例中的公開的各方法、步驟及邏輯方塊圖。通用處理器可以是微處理器或者該處理器也可以是什麼常規的處理器等。結合本發明實施例所公開的方法的步驟可以直接體現為硬體解碼處理器執行完成，或者用解碼處理器中的硬體及軟體模組組合執行完成。軟體模組可以位於隨機記

憶體，快閃記憶體、唯讀記憶體，可程式設計唯讀記憶體或者電可讀寫可程式設計記憶體、暫存器等本領域成熟的儲存媒體中。該儲存媒體位於記憶體，處理器讀取記憶體中的資訊，結合其硬體完成上述方法的步驟。

該電子設備還可執行前述數位憑證管理裝置執行的方法，並實現數位憑證管理裝置在前述實施例的功能，本發明實施例在此不再贅述。

本發明實施例還提出了一種電腦可讀儲存媒體，該電腦可讀儲存媒體儲存一個或多個程式，該一個或多個程式包括指令，該指令當被包括多個應用程式的電子設備執行時，能夠使該電子設備執行前述實施例中數位憑證管理裝置執行的方法，並具體用於執行：

向區塊鏈中發送數位憑證上鏈請求，用於供區塊鏈確定對節點的待校驗數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否將待校驗數位憑證寫入區塊鏈；其中，數位憑證上鏈請求中包含由節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將待校驗數位憑證寫入區塊鏈。

本發明實施例還提供一種數位憑證管理裝置，用於區塊鏈中的節點，參見圖11所示，包括：

請求發起模組501，向區塊鏈中發送數位憑證吊銷請求，用於供區塊鏈確定對目標節點的數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否在區塊鏈中吊銷目標節點的數位憑證；其中，數位憑證吊銷請求中包

含請求吊銷的目標節點的數位憑證。

圖12是本發明的一個實施例電子設備的結構示意圖。請參考圖12，在硬體層面，該電子設備包括處理器，可選地還包括內部匯流排、網路介面、記憶體。其中，記憶體可能包含記憶體，例如高速隨機存取記憶體(Random-Access Memory, RAM)，也可能還包括非易失性記憶體(non-volatile memory)，例如至少1個磁碟記憶體等。當然，該電子設備還可能包括其他業務所需要的硬體。

處理器、網路介面和記憶體可以通過內部匯流排相互連接，該內部匯流排可以是ISA(Industry Standard Architecture，工業標準架構)匯流排、PCI(Peripheral Component Interconnect，外設部件互連標準)匯流排或EISA(Extended Industry Standard Architecture，延伸工業標準架構)匯流排等。所述匯流排可以分為位址匯流排、資料匯流排、控制匯流排等。為便於表示，圖12中僅用一個雙向箭頭表示，但並不表示僅有一根匯流排或一種類型的匯流排。

記憶體，用於存放程式。具體地，程式可以包括程式碼，所述程式碼包括電腦操作指令。記憶體可以包括記憶體和非易失性記憶體，並向處理器提供指令和資料。

處理器從非易失性記憶體中讀取對應的電腦程式到記憶體中然後運行，在邏輯層面上形成數位憑證管理裝置。處理器，執行記憶體所存放的程式，並具體用於執行以下操作：

向區塊鏈中發送數位憑證吊銷請求，用於供區塊鏈確

定對目標節點的數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否在區塊鏈中吊銷目標節點的數位憑證；其中，數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證。

上述如本發明前述實施例揭示的數位憑證管理裝置執行的方法可以應用於處理器中，或者由處理器實現。處理器可能是一種積體電路晶片，具有信號的處理能力。在實現過程中，上述方法的各步驟可以通過處理器中的硬體的積體邏輯電路或者軟體形式的指令完成。上述的處理器可以是通用處理器，包括中央處理器 (Central Processing Unit, CPU)、網路處理器 (Network Processor, NP)等；還可以是數位訊號處理器 (Digital Signal Processor, DSP)、專用積體電路 (Application Specific Integrated Circuit, ASIC)、現場可程式設計閘陣列 (Field-Programmable Gate Array, FPGA)或者其他可程式設計邏輯器件、分立閘或者電晶體邏輯器件、分立硬體元件。可以實現或者執行本發明實施例中的公開的各方法、步驟及邏輯方塊圖。通用處理器可以是微處理器或者該處理器也可以是什麼常規的處理器等。結合本發明實施例所公開的方法的步驟可以直接體現為硬體解碼處理器執行完成，或者用解碼處理器中的硬體及軟體模組組合執行完成。軟體模組可以位於隨機記憶體，快閃記憶體、唯讀記憶體，可程式設計唯讀記憶體或者電可讀寫可程式設計記憶體、暫存器等本領域成熟的儲存媒體中。該儲存媒體位於記憶體，處理器讀取記憶體

中的資訊，結合其硬體完成上述方法的步驟。

該電子設備還可執行前述數位憑證管理裝置執行的方法，並實現數位憑證管理在前述實施例的功能，本發明實施例在此不再贅述。

本發明實施例還提出了一種電腦可讀儲存媒體，該電腦可讀儲存媒體儲存一個或多個程式，該一個或多個程式包括指令，該指令當被包括多個應用程式的電子設備執行時，能夠使該電子設備執行前述實施例中數位憑證管理裝置執行的方法，並具體用於執行：

向區塊鏈中發送數位憑證吊銷請求，用於供區塊鏈確定對目標節點的數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否在區塊鏈中吊銷目標節點的數位憑證；其中，數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證。

本領域內的技術人員應明白，本發明的實施例可提供為方法、系統、或電腦程式產品。因此，本發明可採用完全硬體實施例、完全軟體實施例、或結合軟體和硬體方面的實施例的形式。而且，本發明可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體(包括但不限於磁碟記憶體、**CD-ROM**、光學記憶體等)上實施的電腦程式產品的形式。

本發明是參照根據本發明實施例的方法、設備(系統)、和電腦程式產品的流程圖和／或方塊圖來描述的。應理解可由電腦程式指令實現流程圖和／或方塊圖中的每

一流程和／或方塊、以及流程圖和／或方塊圖中的流程和／或方塊的結合。可提供這些電腦程式指令到通用電腦、專用電腦、嵌入式處理機或其他可程式設計資料處理設備的處理器以產生一個機器，使得通過電腦或其他可程式設計資料處理設備的處理器執行的指令產生用於實現在流程圖一個流程或多個流程和／或方塊圖一個方塊或多個方塊中指定的功能的裝置。

這些電腦程式指令也可儲存在能引導電腦或其他可程式設計資料處理設備以特定方式工作的電腦可讀記憶體中，使得儲存在該電腦可讀記憶體中的指令產生包括指令裝置的製造品，該指令裝置實現在流程圖一個流程或多個流程和／或方塊圖一個方塊或多個方塊中指定的功能。

這些電腦程式指令也可裝載到電腦或其他可程式設計資料處理設備上，使得在電腦或其他可程式設計設備上執行一系列操作步驟以產生電腦實現的處理，從而在電腦或其他可程式設計設備上執行的指令提供用於實現在流程圖一個流程或多個流程和／或方塊圖一個方塊或多個方塊中指定的功能的步驟。

在一個典型的配置中，計算設備包括一個或多個處理器(CPU)、輸入/輸出介面、網路介面和記憶體。

記憶體可能包括電腦可讀媒體中的非永久性記憶體，隨機存取記憶體(RAM)和/或非易失性記憶體等形式，如唯讀記憶體(ROM)或快閃記憶體(flash RAM)。記憶體是電腦可讀媒體的示例。

電腦可讀媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是電腦可讀指令、資料結構、程式的模組或其他資料。電腦的儲存媒體的例子包括，但不限於相變記憶體 (PRAM)、靜態隨機存取記憶體 (SRAM)、動態隨機存取記憶體 (DRAM)、其他類型的隨機存取記憶體 (RAM)、唯讀記憶體 (ROM)、電可擦除可程式設計唯讀記憶體 (EEPROM)、快閃記憶體或其他記憶體技術、唯讀光碟唯讀記憶體 (CD-ROM)、數位多功能光碟 (DVD) 或其他光學儲存、磁盒式磁帶，磁帶磁磁片儲存或其他磁性存放裝置或任何其他非傳輸媒體，可用於儲存可以被計算設備存取的資訊。按照本文中的界定，電腦可讀媒體不包括暫存電腦可讀媒體 (transitory media)，如調變的資料信號和載波。

還需要說明的是，術語“包括”、“包含”或者其任何其他變體意在涵蓋非排他性的包含，從而使得包括一系列要素的過程、方法、商品或者設備不僅包括那些要素，而且還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還存在另外的相同要素。

本領域技術人員應明白，本發明的實施例可提供為方法、系統或電腦程式產品。因此，本發明可採用完全硬體

實施例、完全軟體實施例或結合軟體和硬體方面的實施例的形式。而且，本發明可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體(包括但不限於磁碟記憶體、CD-ROM、光學記憶體等)上實施的電腦程式產品的形式。

以上所述僅為本發明的實施例而已，並不用於限制本發明。對於本領域技術人員來說，本發明可以有各種更改和變化。凡在本發明的精神和原理之內所作的任何修改、等同替換、改進等，均應包含在本發明的申請專利範圍之內。

【符號說明】

101：請求接收模組

103：共識校驗結果確定模組

105：憑證管理模組

201：請求接收模組

203：共識校驗結果確定模組

205：憑證管理模組

401：請求發起模組

501：請求發起模組

【發明申請專利範圍】

【第1項】

一種數位憑證管理方法，包括：

接收區塊鏈中的節點發送的數位憑證上鏈請求，該數位憑證上鏈請求中包含由該節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將該待校驗數位憑證寫入該區塊鏈；

共識校驗結果確定模組確定對該節點的待校驗數位憑證進行共識校驗的結果；

憑證管理模組依據共識校驗的結果，確定是否將該待校驗數位憑證寫入該區塊鏈，

其中，確定對該節點的待校驗數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【第2項】

根據申請專利範圍第1項的方法，依據該第一節點的

數量確定共識校驗的結果，包括：

當該第一節點的數量滿足第一預設條件時，確定共識校驗的結果為通過共識校驗；

滿足該第一預設條件包括以下一項或多項：

該第一節點的數量達到第一預設閾值；

該第一節點的數量與該參與共識校驗的節點的數量的比值達到第二預設閾值；

該第一節點的數量與該區塊鏈的節點的數量的比值達到第三預設閾值。

【第3項】

根據申請專利範圍第2項的方法，依據共識校驗的結果，確定是否將該待校驗數位憑證寫入該區塊鏈，包括：

當該共識校驗的結果為通過共識校驗時，將該待校驗數位憑證寫入該區塊鏈。

【第4項】

根據申請專利範圍第1~3項中任一項的方法，還包括：

接收該區塊鏈中的節點發送的數位憑證吊銷請求，該數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

確定對該目標節點的數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否吊銷該目標節點的數位憑證。

【第5項】

一種數位憑證管理方法，包括：

接收區塊鏈中的節點發送的數位憑證吊銷請求，該數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

共識校驗結果確定模組確定對該目標節點的數位憑證進行共識校驗的結果；

憑證管理模組依據共識校驗的結果，確定是否在該區塊鏈中吊銷該目標節點的數位憑證，

其中，確定對該目標節點的數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【第6項】

根據申請專利範圍第5項的方法，依據該第一節點的數量確定共識校驗的結果，包括：

當該第一節點的數量滿足第一預設條件時，確定共識校驗的結果為通過共識校驗；

滿足該第一預設條件包括以下一項或多項：

該第一節點的數量達到第一預設閾值；

該第一節點的數量與該參與共識校驗的節點的數量的比值達到第二預設閾值；

該第一節點的數量與該區塊鏈的節點的數量的比值達到第三預設閾值。

【第7項】

根據申請專利範圍第5項的方法，依據共識校驗的結果，確定是否在該區塊鏈中吊銷該目標節點的數位憑證，包括：

當該共識校驗的結果為通過共識校驗時，在該區塊鏈中吊銷該目標節點的數位憑證。

【第8項】

一種數位憑證管理方法，包括：

區塊鏈中的節點向區塊鏈中發送數位憑證上鏈請求，用於供該區塊鏈透過共識校驗結果確定模組確定對該節點的待校驗數位憑證進行共識校驗的結果，並透過憑證管理模組依據共識校驗的結果，確定是否將該待校驗數位憑證寫入該區塊鏈；

其中，該數位憑證上鏈請求中包含由該節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將該待校驗數位憑證寫入該區塊鏈，

其中，確定對該節點的待校驗數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【第9項】

一種數位憑證管理方法，包括：

區塊鏈中的節點向區塊鏈中發送數位憑證吊銷請求，用於供該區塊鏈透過共識校驗結果確定模組確定對目標節點的數位憑證進行共識校驗的結果，並透過憑證管理模組依據共識校驗的結果，確定是否在該區塊鏈中吊銷該目標節點的數位憑證；

其中，該數位憑證吊銷請求中包含請求吊銷的該目標節點的數位憑證，

其中，確定對該目標節點的數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共

識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【第10項】

一種數位憑證管理裝置，用於區塊鏈，包括：

請求接收模組，接收區塊鏈中的節點發送的數位憑證上鏈請求，該數位憑證上鏈請求中包含由該節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將該待校驗數位憑證寫入該區塊鏈；

共識校驗結果確定模組，確定對該節點的待校驗數位憑證進行共識校驗的結果；

憑證管理模組，依據共識校驗的結果，確定是否將該待校驗數位憑證寫入該區塊鏈，

其中，確定對該節點的待校驗數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權

數量。

【第 11 項】

一種電子設備，用於區塊鏈，包括：

處理器；以及

被安排成儲存電腦可執行指令的記憶體，該可執行指令在被執行時使該處理器執行以下操作：

接收區塊鏈中的節點發送的數位憑證上鏈請求，該數位憑證上鏈請求中包含由該節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將該待校驗數位憑證寫入該區塊鏈；

確定對該節點的待校驗數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否將該待校驗數位憑證寫入該區塊鏈，

其中，確定對該節點的待校驗數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權

數量。

【第12項】

一種數位憑證管理裝置，用於區塊鏈，包括：

請求接收模組，接收區塊鏈中的節點發送的數位憑證吊銷請求，該數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

共識校驗結果確定模組，確定對該目標節點的數位憑證進行共識校驗的結果；

憑證管理模組，依據共識校驗的結果，確定是否在該區塊鏈中吊銷該目標節點的數位憑證

其中，確定對該目標節點的數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【第13項】

一種電子設備，用於區塊鏈，包括：

處理器；以及

被安排成儲存電腦可執行指令的記憶體，該可執行指令在被執行時使該處理器執行以下操作：

接收區塊鏈中的節點發送的數位憑證吊銷請求，該數位憑證吊銷請求中包含請求吊銷的目標節點的數位憑證；

確定對該目標節點的數位憑證進行共識校驗的結果；

依據共識校驗的結果，確定是否在該區塊鏈中吊銷該目標節點的數位憑證，

其中，確定對該目標節點的數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【第14項】

一種數位憑證管理裝置，用於區塊鏈中的節點，包括：

請求發起模組，向區塊鏈中發送數位憑證上鏈請求，用於供該區塊鏈確定對該節點的待校驗數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否將該待校

驗數位憑證寫入該區塊鏈；其中，該數位憑證上鏈請求中包含由該節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將該待校驗數位憑證寫入該區塊鏈

其中，確定對該節點的待校驗數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【第15項】

一種電子設備，用於區塊鏈中的節點，包括：

處理器；以及

被安排成儲存電腦可執行指令的記憶體，該可執行指令在被執行時使該處理器執行以下操作：

向區塊鏈中發送數位憑證上鏈請求，用於供該區塊鏈確定對該節點的待校驗數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否將該待校驗數位憑證寫入該區塊鏈；其中，該數位憑證上鏈請求中包含由該節點使用私密金鑰簽名產生的待校驗數位憑證，用於請求將該待

校驗數位憑證寫入該區塊鏈，

其中，確定對該節點的待校驗數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【第16項】

一種數位憑證管理裝置，用於區塊鏈中的節點，包括：

請求發起模組，向區塊鏈中發送數位憑證吊銷請求，用於供該區塊鏈確定對目標節點的數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否在該區塊鏈中吊銷該目標節點的數位憑證；其中，該數位憑證吊銷請求中包含請求吊銷的該目標節點的數位憑證

其中，確定對該目標節點的數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或

第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【第17項】

一種電子設備，用於區塊鏈中的節點，包括：

處理器；以及

被安排成儲存電腦可執行指令的記憶體，該可執行指令在被執行時使該處理器執行以下操作：

向區塊鏈中發送數位憑證吊銷請求，用於供該區塊鏈確定對目標節點的數位憑證進行共識校驗的結果，並依據共識校驗的結果，確定是否在該區塊鏈中吊銷該目標節點的數位憑證；其中，該數位憑證吊銷請求中包含請求吊銷的該目標節點的數位憑證，

其中，確定對該目標節點的數位憑證進行共識校驗的結果，包括：

確定該區塊鏈中參與共識校驗的節點的校驗結果；

確定該參與共識校驗的節點中第一節點的數量和/或第二節點的數量；其中，該第一節點的校驗結果為通過共識校驗，該第二節點的校驗結果為未通過共識校驗；

依據該第一節點的數量和/或第二節點的數量確定共

識校驗的結果，

其中，該第一節點的數量和/或第二節點的數量是根據節點在共識校驗過程中的權重不同，統計出來的加權數量。

【發明圖式】

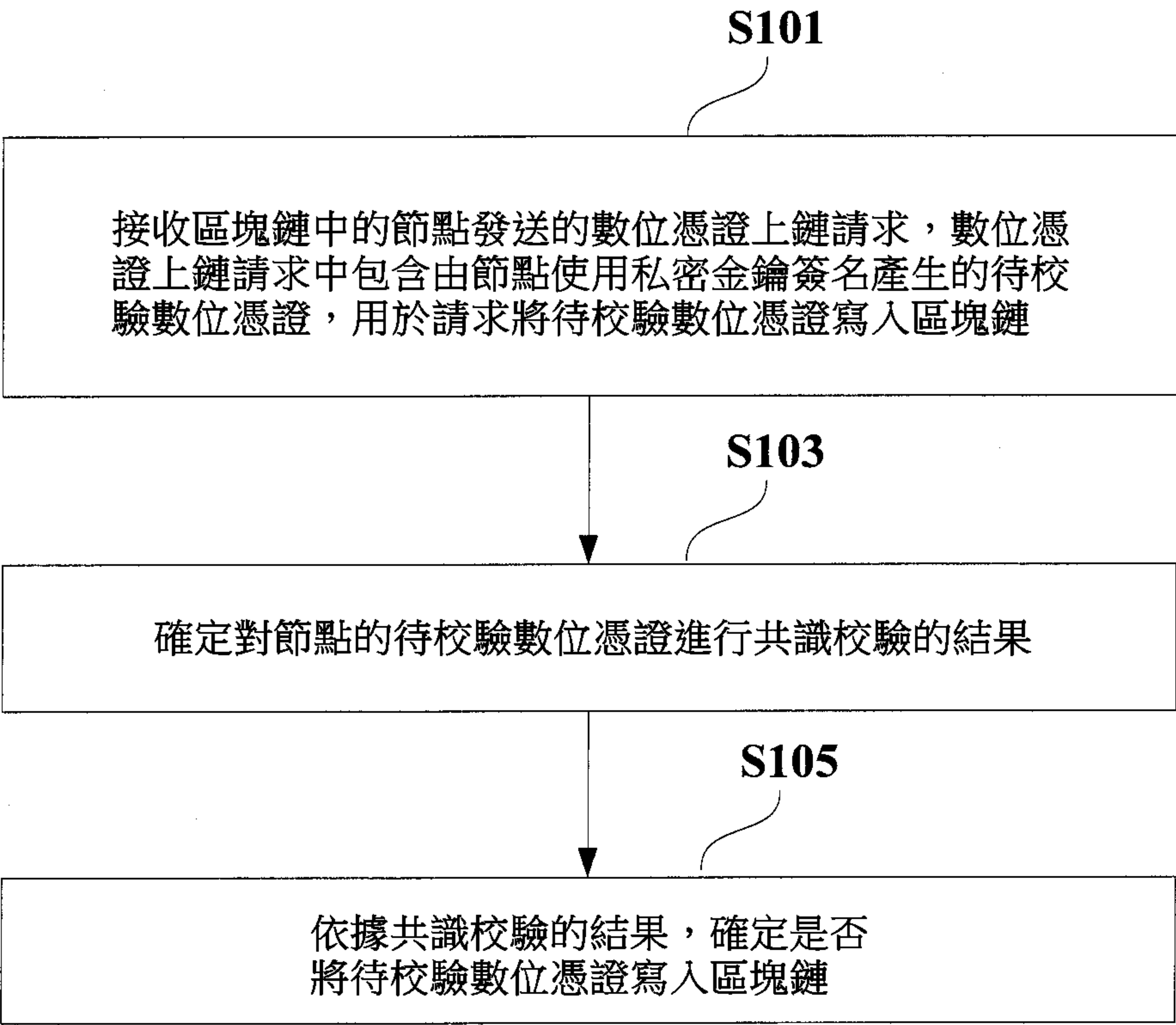


圖 1

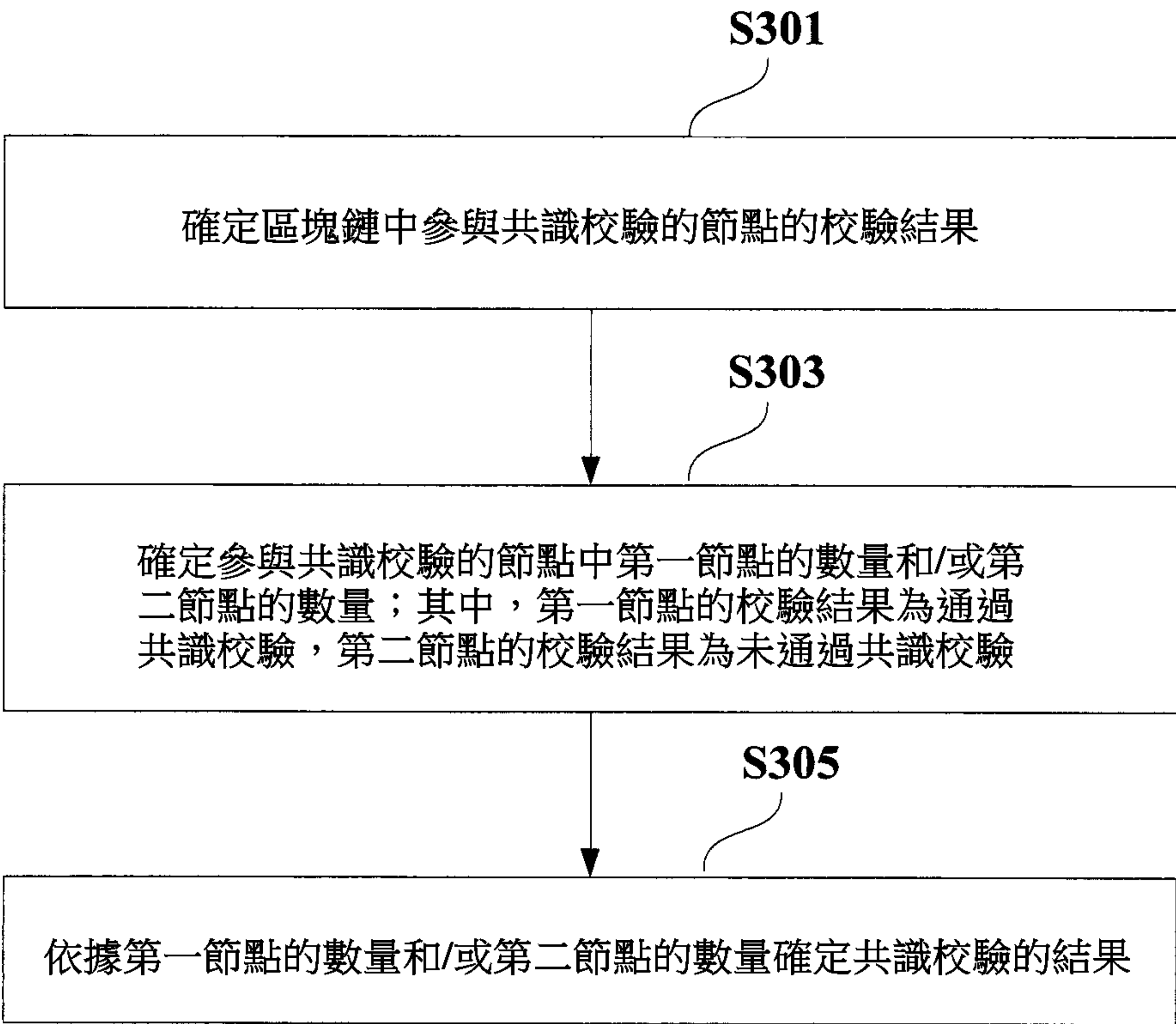


圖 2

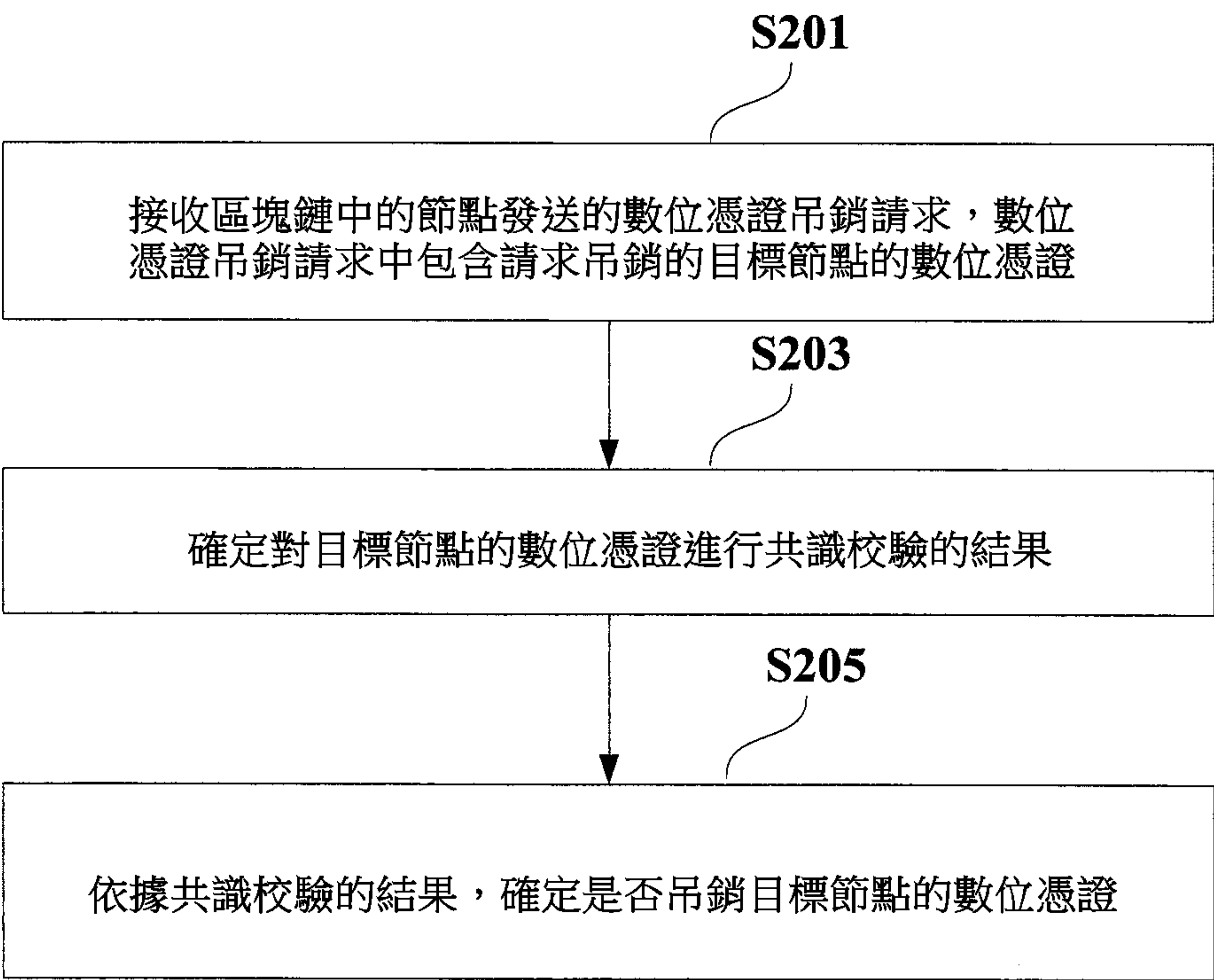


圖 3

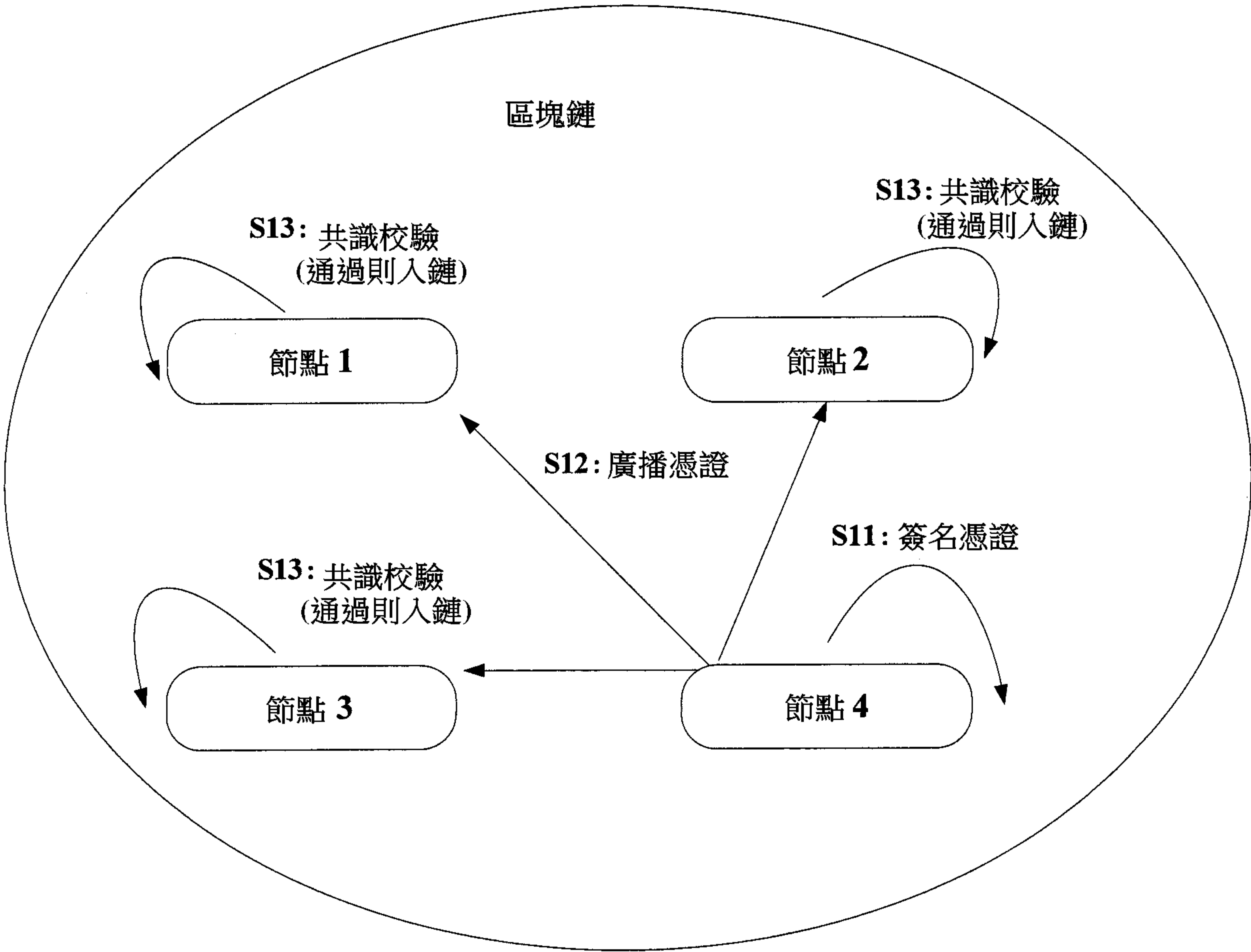


圖 4

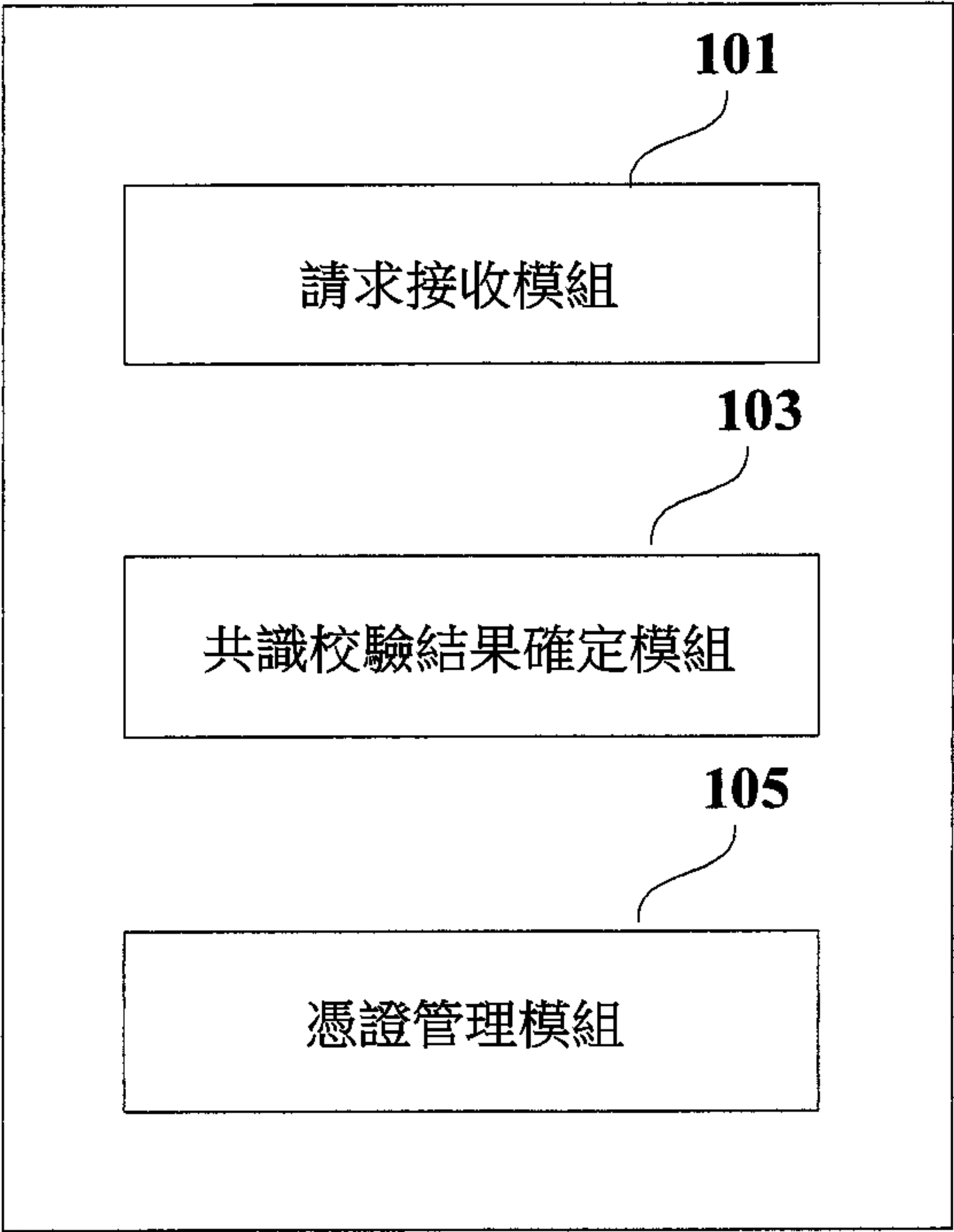


圖 5

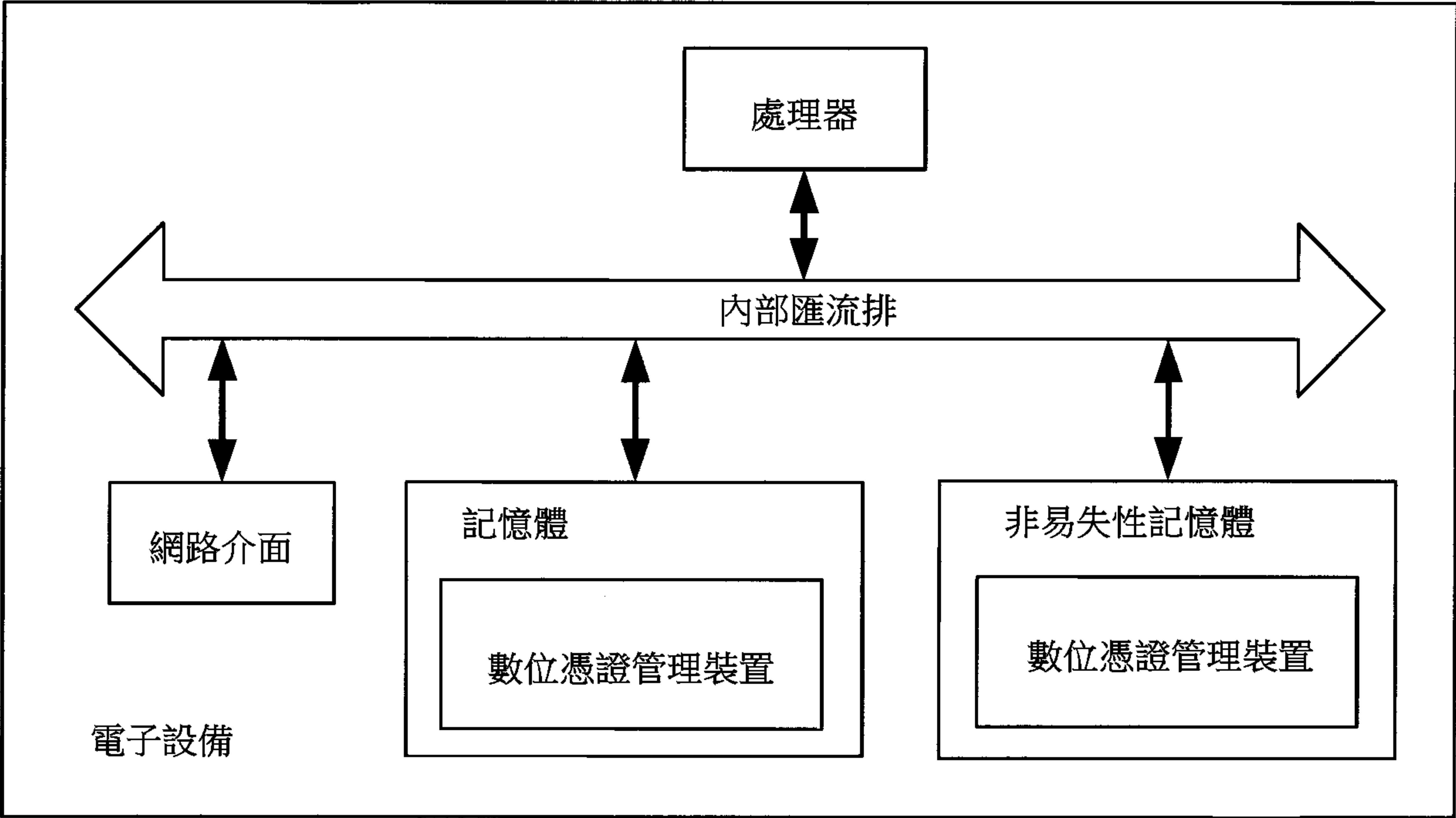


圖 6

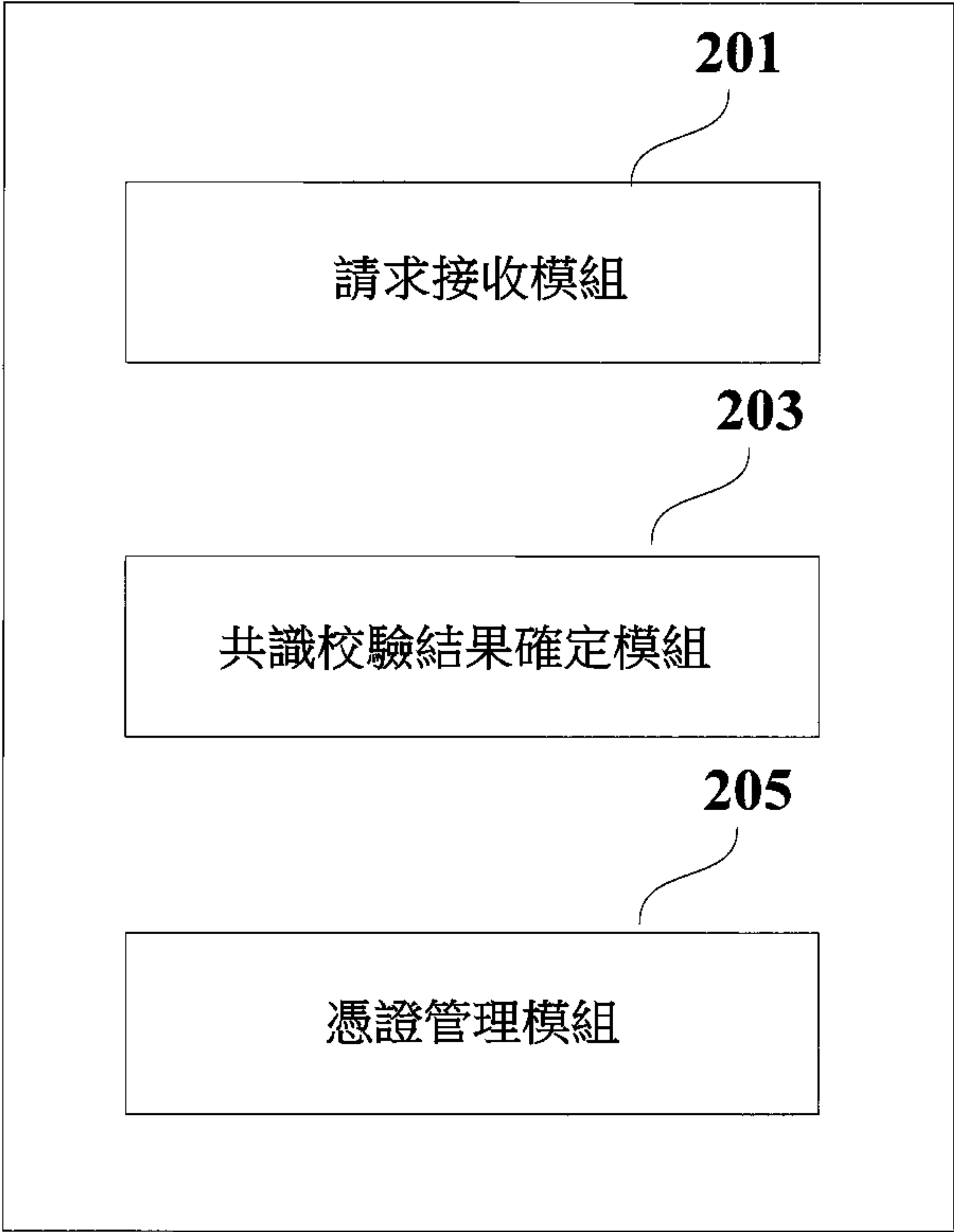


圖 7

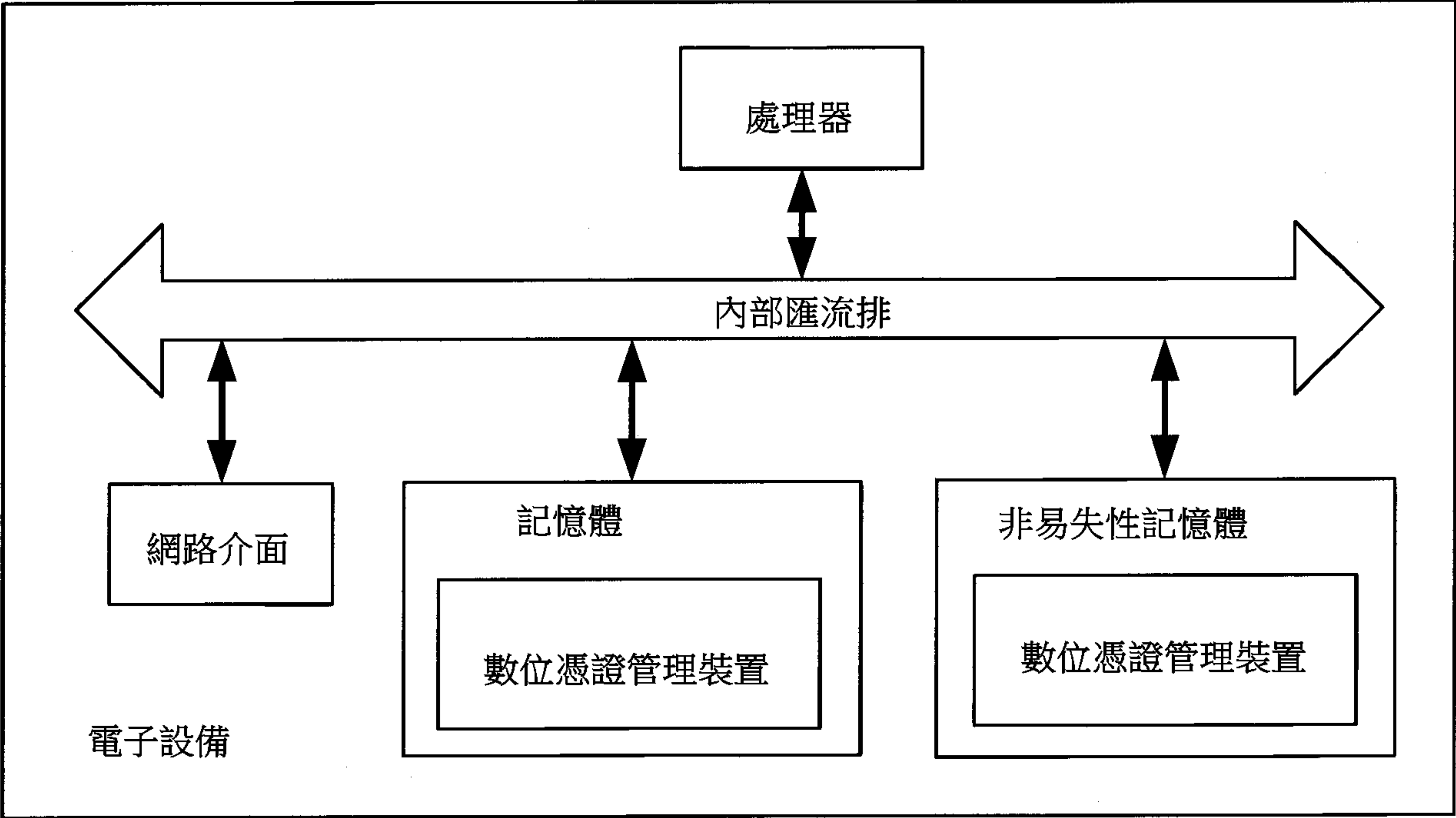


圖 8

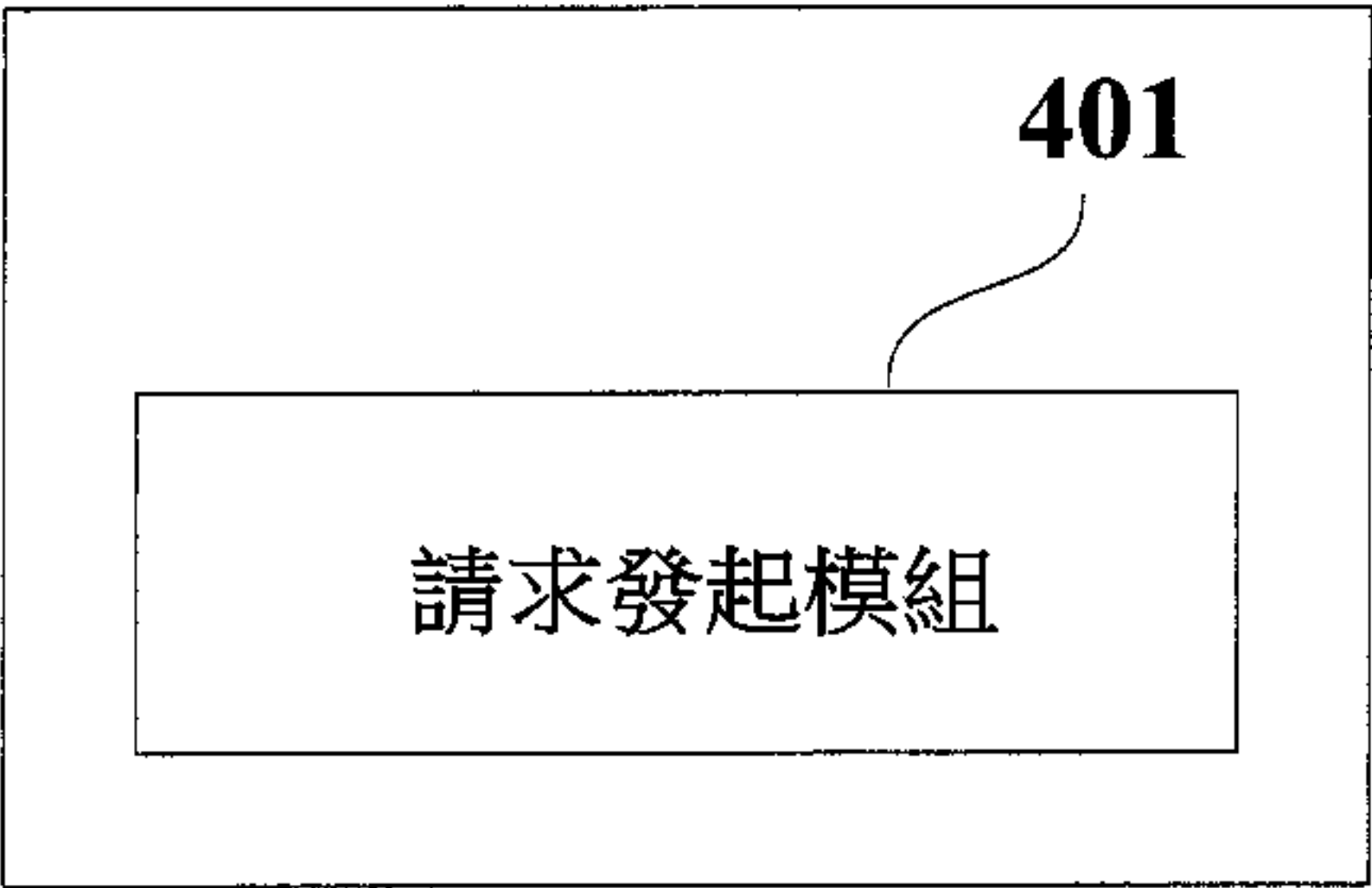


圖 9

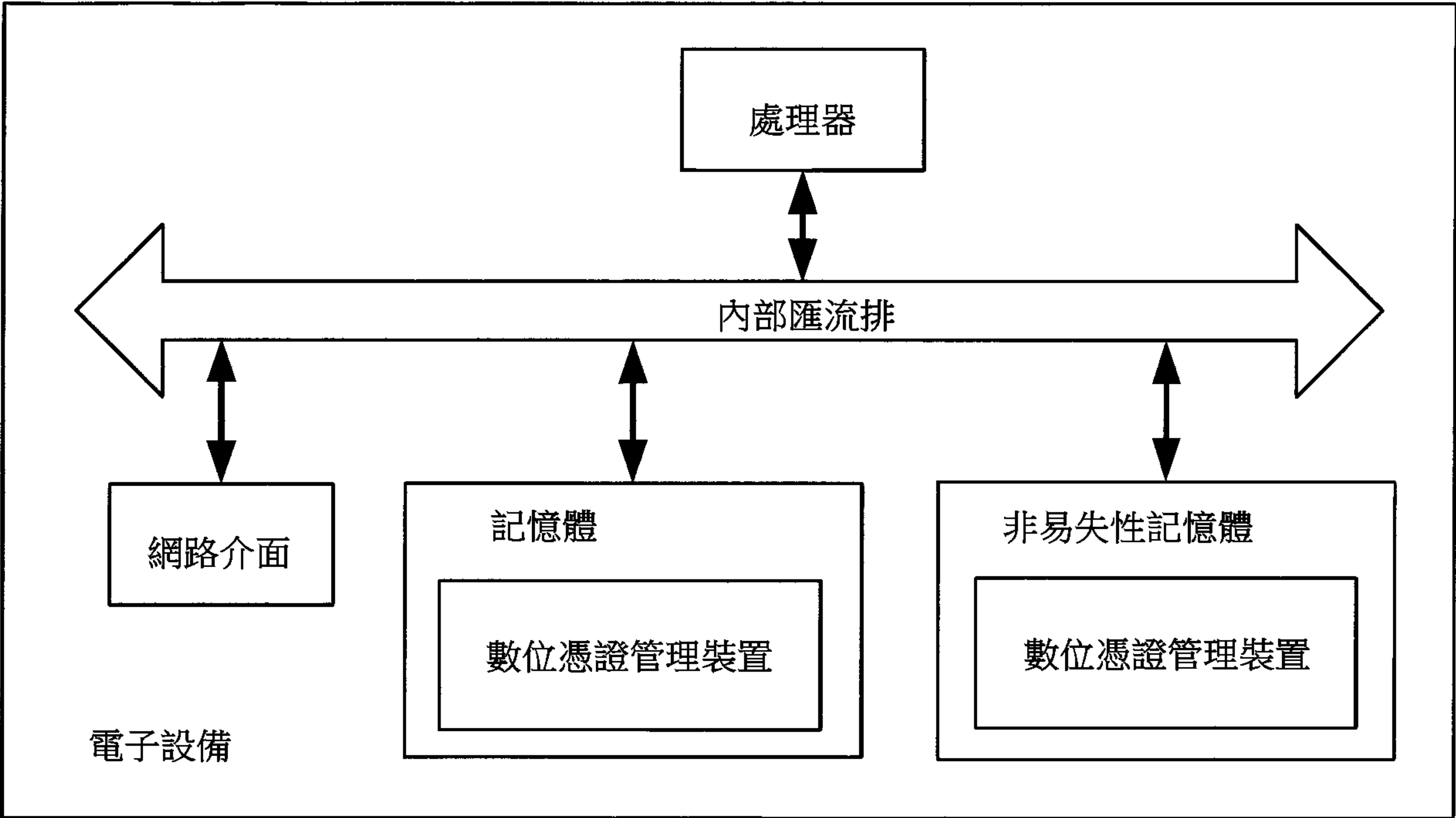


圖 10

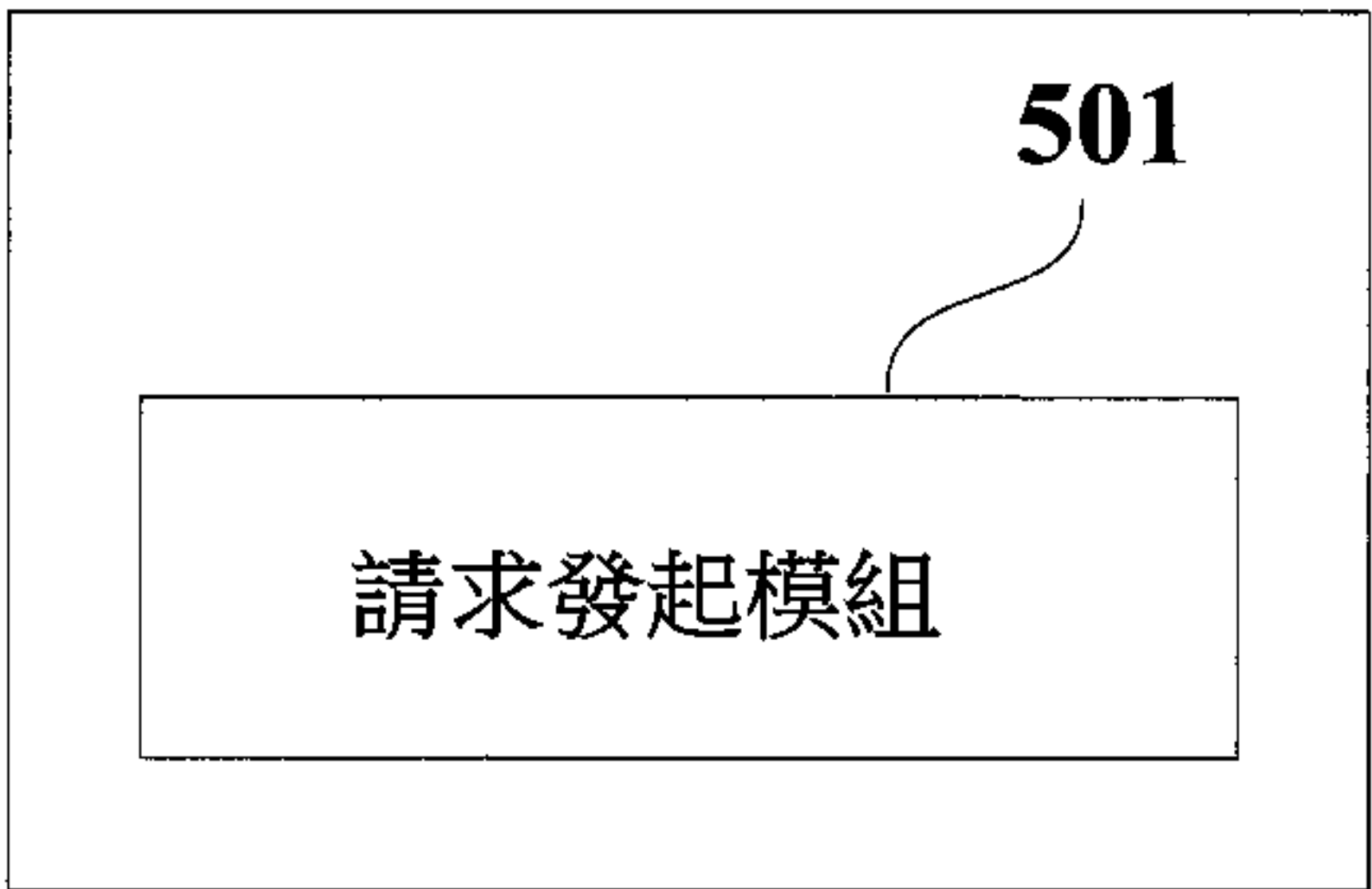


圖 11

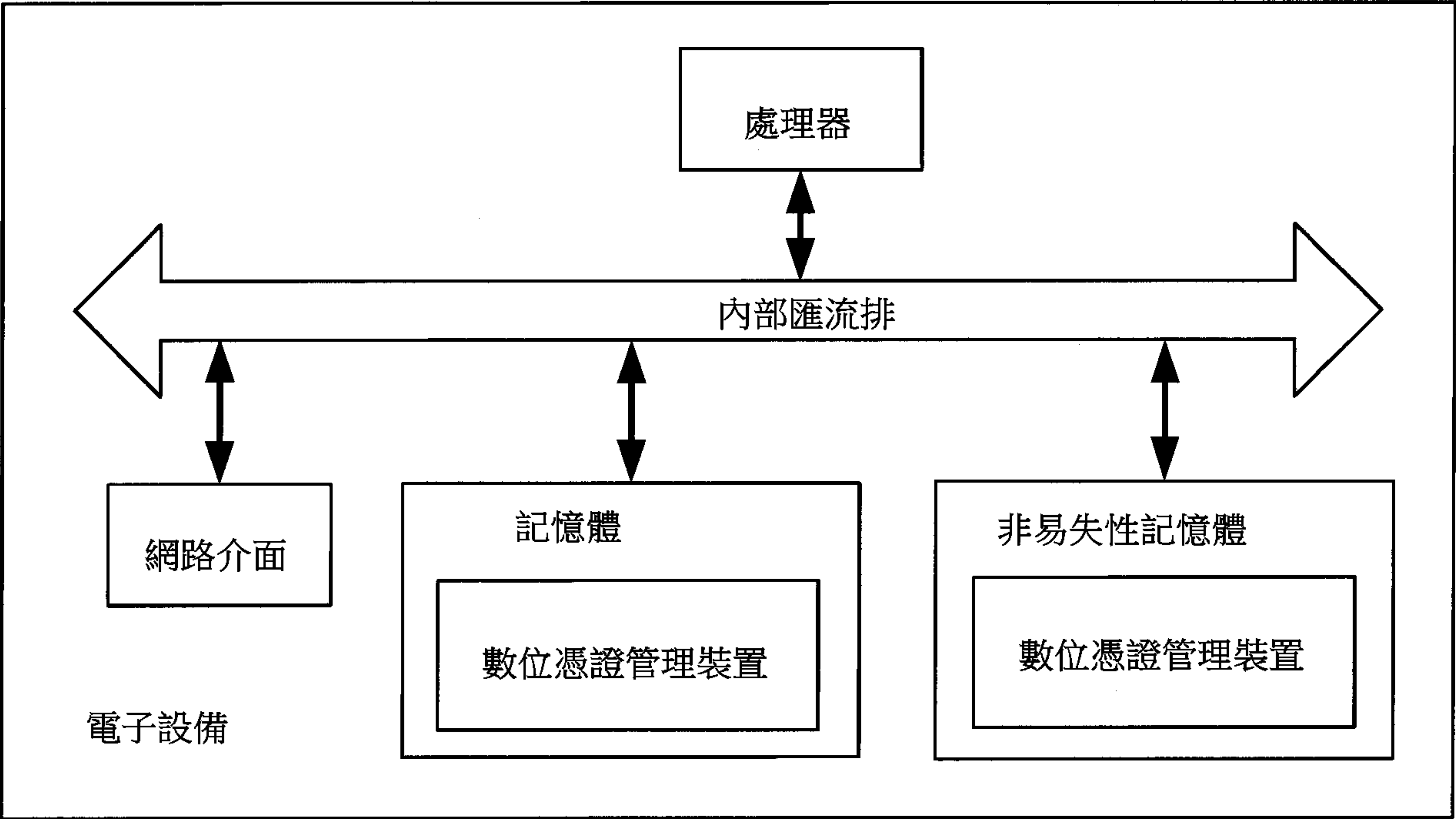


圖 12