



(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 I721691 B

(45)公告日：中華民國 110 (2021) 年 03 月 11 日

(21)申請案號：108144878

(22)申請日：中華民國 108 (2019) 年 12 月 09 日

(51)Int. Cl.：

*G06F16/182 (2019.01)**G06F16/18 (2019.01)**G06F16/22 (2019.01)**G06F21/62 (2013.01)**H04L9/32 (2006.01)**H04L29/06 (2006.01)**H04L9/06 (2006.01)*

(30)優先權：2019/03/21

世界智慧財產權組織

PCT/CN2019/078944

(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：申超 (CN)；張文彬 (CN)；陸旭明 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW M572512U

CN 106899412A

US 2017/0140375A1

US 2018/0349621A1

US 2018/0349621A1

審查人員：李榮祥

申請專利範圍項數：15 項 圖式數：6 共 50 頁

(54)名稱

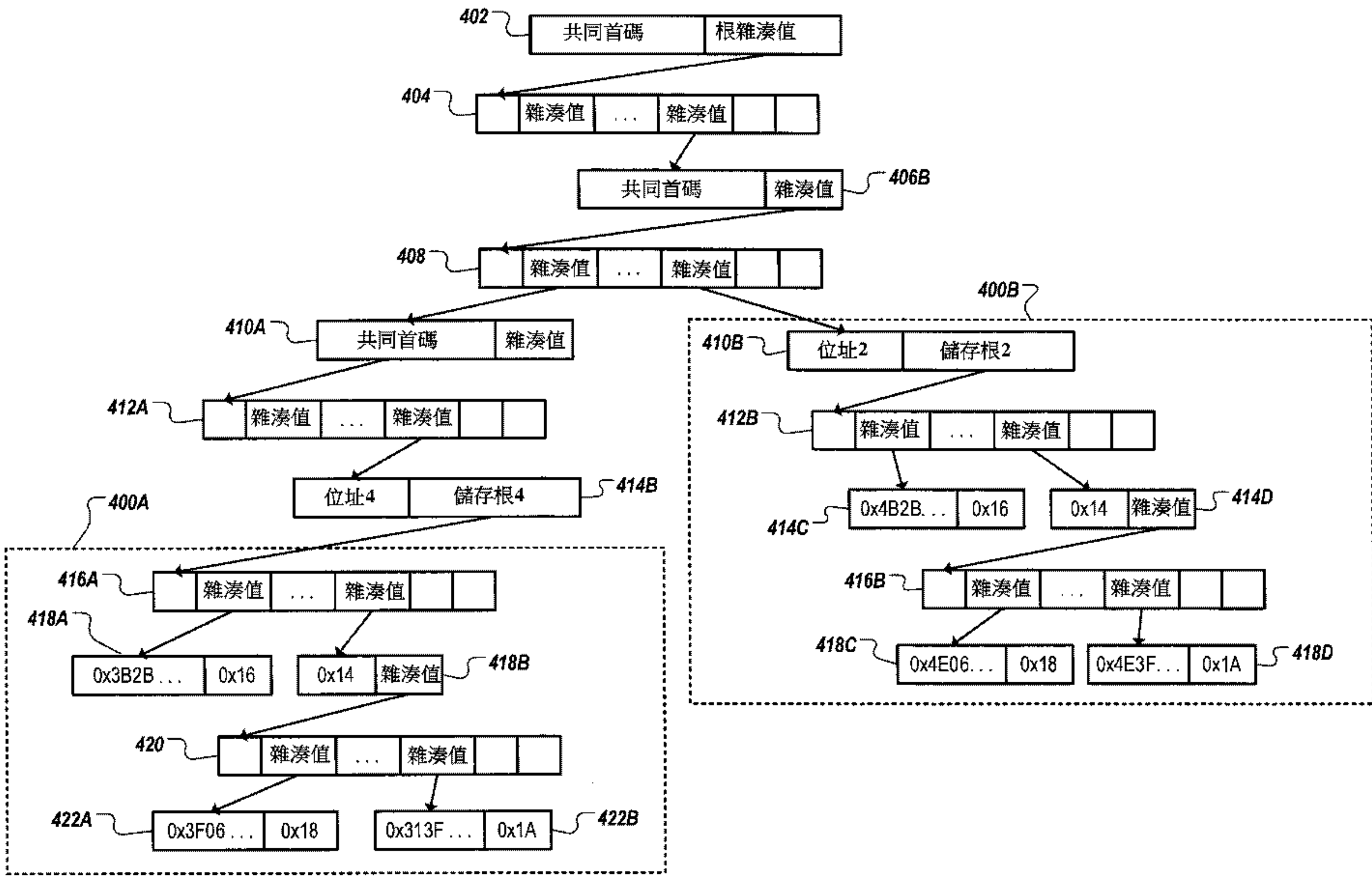
用於隔離儲存在由區塊鏈網路維護的區塊鏈上的資料的電腦實現的方法、裝置及系統

(57)摘要

本文實施方式包括：從區塊鏈網路的輕節點接收包括輕節點的身份的同步請求；識別與輕節點的身份關聯的一個或多個許可權；確定與區塊高度關聯並包括多個帳戶記錄的初始世界狀態結構；基於一個或多個許可權識別所述多個帳戶記錄中輕節點被授權存取的子集；基於初始世界狀態結構產生隔離世界狀態結構，該隔離世界狀態結構僅包括所述多個帳戶記錄中輕節點被授權存取的子集；將包括隔離世界狀態結構的回應發送到輕節點。

Implementations of this specification include receiving a synchronization request from a light-weight node of the blockchain network including an identity of the light-weight node; identifying one or more permissions associated with the identity of the light-weight node; determining an original world state structure associated with the block height and including a plurality of account records; identifying based on the one or more permissions, a subset of the plurality of account records that are authorized for access by the light-weight node; generating an isolated world state structure based on the original world state structure including only the subset of the plurality of account records that are authorized for access by the light-weight node; sending a response to the light-weight node that includes the isolated world state structure.

指定代表圖：



【圖 4A】

符號簡單說明：

400A:區域

400B:區域

402:根節點

406B:擴展節點

410A:擴展節點

416A:分支節點

418B:擴展節點

418C:帳戶記錄

418D:帳戶記錄

420:分支節點

422A:葉節點

422B:葉節點



I721691

【發明摘要】**【中文發明名稱】**

用於隔離儲存在由區塊鏈網路維護的區塊鏈上的資料的電腦實現的方法、裝置及系統

【英文發明名稱】

A COMPUTER-IMPLEMENTED METHOD, APPARATUS AND SYSTEM FOR ISOLATING DATA STORED ON A BLOCKCHAIN MAINTAINED BY A BLOCKCHAIN NETWORK

【中文】

本文實施方式包括：從區塊鏈網路的輕節點接收包括輕節點的身份的同步請求；識別與輕節點的身份關聯的一個或多個許可權；確定與區塊高度關聯並包括多個帳戶記錄的初始世界狀態結構；基於一個或多個許可權識別所述多個帳戶記錄中輕節點被授權存取的子集；基於初始世界狀態結構產生隔離世界狀態結構，該隔離世界狀態結構僅包括所述多個帳戶記錄中輕節點被授權存取的子集；將包括隔離世界狀態結構的回應發送到輕節點。

【 英 文 】

Implementations of this specification include receiving a synchronization request from a light-weight node of the blockchain network including an identity of the light-weight node; identifying one or more permissions associated with the identity of the light-weight node; determining an original world state structure associated with the block height and including a plurality of account records; identifying based on the one or more permissions, a subset of the plurality of account records that are authorized for access by the light-weight node; generating an isolated world state structure based on the original world state structure including only the subset of the plurality of account records that are authorized for access by the light-weight node; sending a response to the light-weight node that includes the isolated world state structure.

【指定代表圖】第(4A)圖。

【代表圖之符號簡單說明】

400A:區域

400B:區域

402:根節點

406B:擴展節點

410A:擴展節點

416A:分支節點

418B:擴展節點

418C:帳戶記錄

418D:帳戶記錄

420:分支節點

422A:葉節點

422B:葉節點

【特徵化學式】無

【發明說明書】

【中文發明名稱】

用於隔離儲存在由區塊鏈網路維護的區塊鏈上的資料的電腦實現的方法、裝置及系統

【英文發明名稱】

A COMPUTER-IMPLEMENTED METHOD, APPARATUS AND SYSTEM FOR ISOLATING DATA STORED ON A BLOCKCHAIN MAINTAINED BY A BLOCKCHAIN NETWORK

【技術領域】

本發明關於區塊鏈領域，尤其關於隔離儲存在由區塊鏈網路維護的區塊鏈上的資料的方法。

【先前技術】

分散式帳本系統(DLS)，也可稱為共識網路及/或區塊鏈網路，使參與的實體能夠安全地且不可竄改地儲存資料。在不引用任何特定用例的情況下，DLS通常被稱為區塊鏈網路。區塊鏈網路的類型可以包括公有區塊鏈網路、私有區塊鏈網路和聯盟區塊鏈網路。公有區塊鏈網路向所有實體開放使用DLS，並開放參與共識處理。私有區塊鏈網路針對特定實體提供，該實體集中控制讀寫許可權。聯盟區塊鏈網路針對選擇實體組群提供，該實體組群控制共識處理，並包括存取控制層。

區塊鏈網路可以包括不同類型的節點。完整參與節點(以下稱為“區塊鏈節點”)通過嘗試建立和驗證新交易區塊以添加到區塊鏈來參與區塊鏈網路的共識處理。輕節點不參與區塊鏈網路的共識處理，並且可能無法完全同步它們自己內部的區塊鏈表示形式。例如，輕節點可能只同步區塊鏈中的特定區塊的區塊頭資訊，而不是同步所有交易資料。

在私有區塊鏈網路或聯盟區塊鏈網路中，節點(例如輕節點)可能僅被允許從區塊鏈中讀取特定的交易，例如與該輕節點相關聯的身份所參與的交易。在這種情況下，輕節點可以向區塊鏈節點查詢特定區塊，並且可以被返回區塊中僅該輕節點可存取的多個交易的表示(例如，默克爾(Merkle)樹)。以這種方式構造的Merkle樹可能與表示區塊中的交易的完整Merkle樹不一致，這可能導致輕節點處由於節點不具有準確的區塊表示而產生錯誤。

區塊鏈網路的“世界狀態”是指區塊鏈網路上的所有普通帳戶和合約帳戶的狀態的集合，其通常以默克爾派特裡夏樹(Merkle Patricia Trie, MPT)的結構被儲存在區塊鏈節點中。在區塊鏈網路中，一些參與者維護參與共識的區塊鏈節點，而一些參與者僅維護一個輕節點。這可能是由於成本或授權，並且不參與共識的節點僅同步來自區塊鏈節點的資料。

輕節點可儲存所有區塊的完整資料，或只儲存區塊頭資料。例如，各種示例性區塊鏈網路具有僅區塊頭資料被

同步的輕節點。輕節點根據將被驗證的交易從區塊鏈節點提取MPT上的相應資料，區塊鏈節點不限制輕節點提取資料的範圍。

在一些情境中，尤其在企業應用的聯邦鏈的情景中，對世界狀態資料的存取可被控制。例如，特定實體可僅被授權存取其控制的帳戶的世界狀態資料。然而，由該實體控制的輕節點可接收整個MPT以驗證交易。因此，期望根據所配置的許可權來控制輕節點對MPT中的資訊的存取，同時仍允許輕節點基於MPT來驗證交易。

【發明內容】

本文實施方式包括電腦實現的方法，該方法用於針對區塊鏈網路的世界狀態資料的隔離方案以滿足區塊鏈網路的輕節點的隔離需求。更具體地，本文實施方式涉及產生狀態默克爾派特裡夏樹(Merkle Patricia Trie, MPT)，該樹不包括輕節點未被授權存取的資料，但仍與區塊鏈網路的世界狀態資料一致(或稱為“隔離MPT”)。

應瞭解，依據本文的方法可以包括本文描述的態樣和特徵的任意組合。也就是說，根據本文的方法不限於本文具體描述的態樣和特徵的組合，還包括所提供的態樣和特徵的任意組合。

以下在圖式和描述中闡述了本文的一個或多個實施例的細節。根據本文和圖式以及申請專利範圍，本文的其他特徵和優點將顯現。

【圖式簡單說明】

[圖 1] 描繪了可用於執行本文實施方式的環境的示例。

[圖 2] 描繪了根據本文實施方式的概念架構的示例。

[圖 3] 描繪了在世界狀態同步處理期間區塊鏈網路的輕節點與區塊鏈節點之間的互動的示例。

[圖 4A] 描繪了圖 3 中描繪的區塊鏈節點的世界狀態結構的示例。

[圖 4B] 描繪了圖 3 中描繪的輕節點的世界狀態結構的示例。

[圖 5] 描繪了可根據本文實施方式執行的處理的示例。

[圖 6] 描繪了根據本文實施方式的裝置的模組的示例。

各圖式中的相同圖式標記表示相同的元件。

【實施方式】

本文實施方式包括電腦實現的方法，該方法用於針對區塊鏈網路的世界狀態資料的隔離方案以滿足區塊鏈網路的輕節點的隔離需求。更具體地，本文實施方式涉及產生隔離狀態默克爾派特裡夏樹 (Merkle Patricia Trie，MPT)(或“隔離 MPT”)，其不包括輕節點未被授權存取的資料，但仍與區塊鏈網路的世界狀態資料一致。

在該方法的一些實施方式中，操作包括：區塊鏈網路中的區塊鏈節點從區塊鏈網路的輕節點接收同步請求，其中，同步請求包括輕節點的身份和與同步請求關聯的區塊高度；區塊鏈節點識別與輕節點的身份關聯的一個或多個許可權；區塊鏈節點確定與區塊高度關聯且包括多個帳戶記錄的初始世界狀態結構，每個帳戶記錄儲存與該帳戶記錄關聯的帳戶的狀態資訊，其中，初始世界狀態結構表示該區塊鏈網路在與區塊高度關聯的區塊被添加到區塊鏈時的狀態；區塊鏈節點基於一個或多個許可權識別所述多個帳戶記錄中輕節點被授權存取的子集；區塊鏈節點基於初始世界狀態結構產生隔離世界狀態結構，隔離世界狀態結構僅包括所述多個帳戶記錄中輕節點被授權存取的子集；區塊鏈節點將包括隔離世界狀態結構的回應發送到輕節點。

為本文實施例提供進一步的背景，並且如上所述，分散式帳本系統(DLS)，又可稱為共識網路(例如，由點對點節點組成)和區塊鏈網路，使參與的實體能夠安全地、不可竄改地進行交易和儲存資料。雖然“區塊鏈”一詞通常與特定網路及/或用例相關聯，但是在不參考任何特定用例的情況下，本文所使用的用語“區塊鏈”通常指 DLS。

區塊鏈是以交易不可竄改的方式儲存交易的資料結構。因此，區塊鏈上記錄的交易是可靠且可信的。區塊鏈包括一個或多個區塊。鏈中的每個區塊通過包含在鏈中緊鄰其之前的前一區塊的加密雜湊值(cryptographic hash)連

結到該前一區塊。每個區塊還包括時間戳記、自身的加密雜湊值以及一個或多個交易。已經被區塊鏈網路中的節點驗證的交易經雜湊處理並編入默克爾 (Merkle) 樹中。Merkle 樹是一種資料結構，在該樹的葉節點處的資料經雜湊處理，並且在該樹的每個分支中的所有雜湊值在該分支的根處連接。聲稱儲存在樹中的雜湊值可以通過確定雜湊值是否與樹的結構一致而被快速驗證。

區塊鏈是用於儲存交易的分散或至少部分分散的資料結構，而區塊鏈網路是通過廣播、驗證和確認交易等來管理、更新和維護一個或多個區塊鏈的計算節點的網路。如上所述，區塊鏈網路可被提供為公有區塊鏈網路、私有區塊鏈網路或聯盟區塊鏈網路。本文參考聯盟區塊鏈網路進一步詳細描述了本文實施方式。然而，可以預期，本文實施方式可以在任何適當類型的區塊鏈網路中實現。

通常，聯盟區塊鏈網路在參與實體之間是私有的。在聯盟區塊鏈網路中，共識處理由可被稱為共識節點的授權的節點集控制，一個或多個共識節點由相應的實體 (例如，金融機構、保險公司) 操作。例如，由十 (10) 個實體 (例如，金融機構、保險公司) 組成的聯盟可以操作聯盟區塊鏈網路，每個實體可以操作聯盟區塊鏈網路中的至少一個節點。

在一些示例中，在聯盟區塊鏈網路內，全域區塊鏈是跨所有節點複製的區塊鏈。也就是說，所有共識節點相對於全域區塊鏈處於完全共識狀態。為了達成共識 (例如，

同意向區塊鏈添加區塊)，在聯盟區塊鏈網路內實施共識協定。例如，聯盟區塊鏈網路可實現實用拜占庭容錯(PBFT)共識，以下將進一步詳細描述。

默克爾派特裡夏樹或“MPT”是允許儲存的資料被快速搜尋和驗證的資料結構。MPT組合默克爾樹(Merkle樹)和派特裡夏樹(Patricia trie)的態樣。Merkle樹是二叉樹結構，其中資料項目的雜湊值被儲存在每個葉節點中。每個非葉節點包括其兩個子節點的雜湊值的級聯(concatenation)的雜湊值。該結構確保葉節點中經雜湊處理的任何資料項目的改變(其將改變節點雜湊值)還將引起樹的根雜湊值的改變。因此，可通過檢查Merkle樹中經雜湊處理的資料項目聲稱的值的雜湊值是否與樹一致(即，根雜湊值是否改變)來驗證該聲稱的值。

派特裡夏樹(Patricia trie)是基於表示所儲存的資料的鍵(例如，雜湊值)管理儲存在葉節點中的資料的結構。樹的每個非葉節點與鍵值的首碼關聯。每個葉節點被儲存為具有最長匹配首碼的節點的孩子。這允許通過從根節點開始沿著與特定鍵值匹配的首碼節點的路徑遍歷Patricia樹，以快速查找到具有特定鍵值的節點。

MPT組合Merkle樹和Patricia樹的概念，並包括三種類型的節點。葉節點儲存與鍵關聯的資料(例如，雜湊值)。分支節點用作將多個值(例如，26個字元中的每個或16個十六進位樹中的每個)映射到子節點的“路由器(router)”，並且還儲存與在此終止的鍵關聯的資料。子節點可以是葉

節點或擴展節點，擴展節點為包括其所有子節點的鍵的共有部分的節點。

在一些情況下，MPT可用於儲存區塊鏈網路中的帳戶的狀態。例如，區塊鏈中的每個區塊可包括對MPT的引用，該MPT儲存包括在區塊被添加到區塊鏈時區塊鏈網路中的每個帳戶的餘額的帳戶記錄。可基於與帳戶關聯的公開金鑰在MPT中管理帳戶記錄。這樣的MPT可提供區塊被添加到鏈時區塊鏈網路的“世界狀態”的快照。

鑒於以上背景，本文進一步詳細描述本文實施方式。更具體地，並且如上所述，本文實施方式涉及產生隔離MPT，該隔離MPT不包括世界狀態結構內輕節點不被授權存取的資料，但仍與表示世界狀態結構的完整MPT一致。回應於世界狀態同步請求，隔離MPT可被提供給輕節點，使得本機存放區在輕量網路上的MPT的資料結構與區塊鏈網路的世界狀態結構一致(而不需要輕節點存取受限資料)。

在一些實施方式中，區塊鏈網路的輕節點可向區塊鏈網路的區塊鏈節點提供同步請求。同步請求可包括輕節點的身份(例如，管理輕節點的實體)和與同步請求關聯的區塊高度。區塊鏈節點可識別與輕節點的身份關聯的一個或多個許可權並識別初始MPT，其中，初始MPT表示區塊鏈網路的世界狀態結構並包含由同步請求指定的區塊高度內的多個帳戶記錄。區塊鏈節點基於與輕節點的身份關聯的一個或多個許可權識別所述多個帳戶記錄中輕節點被授權

存取的字集。區塊鏈節點基於初始MPT產生隔離MPT。隔離MPT僅包括所述多個帳戶記錄中輕節點被授權存取的字集；隔離MPT隨後被發送到輕節點並被本機存放區在輕節點，並且用於與區塊鏈網路的世界狀態資料同步。如下所述，隔離MPT可包括與區塊鏈網路的世界狀態結構一致的資料結構，而不包括輕節點不被允許或授權存取的資料。

圖1是示出可用於執行本文實施例的環境100的示例的示圖。在一些示例中，示例性環境100使實體能夠參與到聯盟區塊鏈網路102中。示例性環境100包括計算系統106，108以及網路110。在一些示例中，網路110包括區域網路(LAN)、廣域網路(WAN)、網際網路或其組合，並且連接網路網站、使用者設備(例如，計算設備)和後台系統。在一些示例中，可以通過有線及/或無線通訊鏈路來存取網路110。

在所描繪的示例中，計算系統106、108可以各自包括能夠作為節點參與至聯盟區塊鏈網路102中的任何適當的計算設備。計算設備的示例包括但不限於伺服器、桌上型電腦、筆記型電腦、平板計算設備以及智慧型電話。在一些示例中，計算系統106、108承載一個或多個由電腦實施的服務，用於與聯盟區塊鏈網路102進行互動。例如，計算系統106可以承載第一實體(例如，使用者A)的由電腦實施的、例如交易管理系統的服務，第一實體使用該交易管理系統管理其與一個或多個其他實體(例如，其他使用者)的交易。計算系統108可以承載第二實體(例如，使用者B)

的由電腦實施的、例如交易管理系統的服務，例如，第二實體使用該交易管理系統管理其與一個或多個其他實體(例如，其他使用者)的交易。在圖 1 的示例中，聯盟區塊鏈網路 102 被表示為節點的點對點網路 (Peer-to-Peer network)，且計算系統 106、108 分別提供參與聯盟區塊鏈網路 102 的第一實體和第二實體的節點。

圖 2 描繪了根據本文實施方式的概念架構 200 的示例。概念架構 200 包括實體層 202、承載服務層 204 以及區塊鏈網路層 206。在描繪的示例中，實體層 202 包括三個參與者，參與者 A、參與者 B、參與者 C，每個參與者擁有各自的交易管理系統 208。

在所描繪的示例中，承載服務層 204 包括用於每個交易管理系統 208 的介面 210。在一些示例中，各交易管理系統 208 使用協定(例如，超文字傳輸安全協定(HTTPS))通過網路(例如，圖 1 的網路 110)與其對應的介面 210 通信。在一些示例中，每個介面 210 在相應的交易管理系統 208 與區塊鏈網路層 206 之間提供通信連接。更具體地，介面 210 與區塊鏈網路層 206 中的區塊鏈網路 212 通信。在一些示例中，介面 210 與區塊鏈網路層 206 間的通信是利用遠端程序呼叫(RPC)進行的。在一些示例中，介面 210 “承載”用於各自的交易管理系統 208 的區塊鏈網路節點。例如，介面 210 提供用於存取區塊鏈網路 212 的應用程式設計介面(API)。

如本文所述，區塊鏈網路 212 被提供作為包括多個節點 214 的點對點網路，所述多個節點 214 在區塊鏈 216 中不

可竄改地記錄資訊。儘管示意性地描繪了單個區塊鏈 216，但是在區塊鏈網路 212 上提供並維護了區塊鏈 216 的多個副本。例如，每個節點 214 儲存區塊鏈的副本。在一些實施方式中，區塊鏈 216 儲存與在參與共識區塊鏈網路的兩個或更多個實體之間進行的交易相關聯的資訊。

區塊鏈(例如，圖 2 的區塊鏈 216)由一系列區塊組成，每個區塊儲存資料。示例資料封包括表示兩個或更多個參與者之間的交易的交易資料。儘管本文通過非限制性示例使用了“交易”，但是可以預期，任何適當的資料可以儲存在區塊鏈中(例如，文檔、影像、視訊、音訊)。示例交易可以包括但不限於有價物的交換(例如，資產、產品、服務、貨幣)。交易資料不可竄改地儲存在區塊鏈中。也就是說，交易資料不能改變。

在將交易資料儲存在區塊中之前，對交易資料進行雜湊處理。雜湊處理是將交易資料(作為字串資料提供)轉換為固定長度雜湊值(也作為字串資料提供)的處理。不可能對雜湊值進行去雜湊處理(un-hash)以獲取交易資料。雜湊處理可確保即使交易資料輕微改變也會導致完全不同的雜湊值。此外，如上所述，雜湊值具有固定長度。也就是說，無論交易資料的大小如何，雜湊值的長度都是固定的。雜湊處理包括通過雜湊函數處理交易資料以產生雜湊值。示例雜湊函數包括但不限於輸出 256 位雜湊值的安全雜湊演算法(SHA)-256。

多個交易的交易資料被雜湊處理並儲存在區塊中。例

如，提供兩個交易的雜湊值，並對它們本身進行雜湊處理以提供另一個雜湊值。重複此處理，直到針對所有要儲存在區塊中的交易提供單個雜湊值為止。該雜湊值被稱為 Merkle 根雜湊值，並儲存在區塊的標頭中。任何交易中的更改都會導致其雜湊值發生變化，並最終導致 Merkle 根雜湊值發生變化。

通過共識協議將區塊添加到區塊鏈。區塊鏈網路中的多個節點參與共識協議，並執行將區塊添加到區塊鏈中的工作。這樣的節點被稱為共識節點。上文介紹的 PBFT 用作共識協議的非限制性示例。共識節點執行共識協定以將交易添加到區塊鏈。

更詳細地，共識節點產生區塊頭，對區塊中的所有交易進行雜湊處理，並將所得的雜湊值成對地組合以產生進一步的雜湊值，直到為區塊中的所有交易提供單個雜湊值 (Merkle 根雜湊值)。將此雜湊值添加到區塊頭中。共識節點還確定區塊鏈中最近的區塊的雜湊值 (即，添加到區塊鏈中的最後一個區塊)。共識節點還向區塊頭添加亂數 (nonce) 和時間戳記。

通常，PBFT 提供容忍拜占庭錯誤 (例如，故障節點、惡意節點) 的實用拜占庭機器狀態複製。這通過假設錯誤將發生 (例如，假設存在獨立的節點失效及 / 或由共識節點發送的竄改資訊) 在 PBFT 中實現。在 PBFT 中，在包括主共識節點和備共識節點的序列中提供共識節點。主共識節點週期性地改變，通過區塊鏈網路內的所有共識節點達成關

於區塊鏈網路的世界狀態的共識將交易添加到區塊鏈。在該過程中，在共識節點之間傳輸資訊，每個共識節點證明資訊是從特定的對等節點接收的，並驗證在交易期間資訊沒有被更改。

在 PBFT 中，在多個階段提供共識協議並且所有共識節點以相同狀態開始。首先，用戶端向主共識節點發送呼叫服務操作(例如，在區塊鏈網路內執行交易)的請求。回應於接收到該請求，主共識節點向備共識節點多路廣播該請求。備共識節點執行該請求，並均將回復發送到用戶端。用戶端一直等待，直到臨限值數量的副本被接收為止。在一些示例中，用戶端等待 $f+1$ 個副本被接收，其中， f 為區塊鏈網路內可以容忍的錯誤共識節點的最大數量。最終結果是足夠數量的共識節點對將被添加到區塊鏈的記錄的次序達成共識，該記錄被接受或者被拒絕。

在一些區塊鏈網路中，用密碼學來維護交易的隱私。例如，如果兩個節點想要保持交易隱私，以使得區塊鏈網路中的其他節點不能看出交易的細節，則這兩個節點可以對交易資料進行加密處理。示例加密處理包括但不限於對稱加密和非對稱加密。對稱加密是指使用單個金鑰既進行加密(從明文產生密文)又進行解密(從密文產生明文)的加密處理。在對稱加密中，同一金鑰可用於多個節點，因此每個節點都可以對交易資料進行加密/解密。

非對稱加密使用金鑰對，每個金鑰對包括私鑰和公開金鑰，私鑰僅對於相應節點是已知的，而公開金鑰對於區

塊鏈網路中的任何或所有其他節點是已知的。節點可以使用另一個節點的公開金鑰來加密資料，並且該加密的資料可以使用其他節點的私鑰被解密。例如，再次參考圖 2，參與者 A 可以使用參與者 B 的公開金鑰來加密資料，並將加密資料發送給參與者 B。參與者 B 可以使用其私鑰來解密該加密資料(密文)並提取初始資料(明文)。使用節點的公開金鑰加密的資訊只能使用該節點的私鑰解密。

非對稱加密用於提供數位簽章，這使得交易中的參與者能夠確認交易中的其他參與者以及交易的有效性。例如，節點可以對資訊進行數位簽章，而另一個節點可以根據參與者 A 的該數位簽章來確認該資訊是由該節點發送的。數位簽章也可以用於確保資訊在傳輸過程中不被竄改。例如，再次參考圖 2，參與者 A 將向參與者 B 發送資訊。參與者 A 產生該資訊的雜湊值，然後使用其私鑰加密該雜湊值以提供為加密雜湊值的數位簽章。參與者 A 將該數位簽章附加到該資訊上，並將該具有數位簽章的資訊發送給參與者 B。參與者 B 使用參與者 A 的公開金鑰解密該數位簽章，並提取雜湊值。參與者 B 對該資訊進行雜湊處理並比較雜湊值。如果雜湊值相同，參與者 B 可以確認該資訊確實來自參與者 A，且未被竄改。

圖 3 描繪了在世界狀態同步處理期間區塊鏈網路(例如，圖 2 的區塊鏈網路 212)的輕節點 310 與區塊鏈節點 320 之間的互動的示例。世界狀態同步過程以圖 3 中示出的步驟進行。在 305，輕節點 310 首先檢測同步觸發條件。例

如，同步觸發條件可指示輕節點 310 已超出距最近同步點的設置的臨限值，諸如距最近同步點的區塊的數量。在其他示例中，同步觸發條件可以是由輕節點 310 檢測並用於發起同步處理的區塊鏈節點 320 的特定事件。例如，輕節點 310 可從區塊鏈節點 320 接收事件資訊，並且作為回應，基於接收到事件資訊發起同步處理。在一些其他示例中，同步觸發條件可表示通過服務介面的外部呼叫觸發，該服務介面由輕節點 310 提供並使得使用者或實體能夠例如通過手動主動地觸發同步處理。

在 310，輕節點 310 基於在步驟 305 對同步觸發條件的檢測產生世界狀態同步請求。具體地，輕節點 310 可提取將被同步的帳戶記錄的範圍清單，例如位址清單或識別碼列表。同步請求還可標識區塊高度以進行同步。如本文所述，區塊高度表示鏈中將被同步的第一區塊與創世區塊(即，區塊高度為 0 的區塊)之間的區塊的數量。

在 315，輕節點 310 向區塊鏈節點 320 發送同步請求。同步請求可包括表示管理或以其他方式與輕節點 310 關聯的實體的身份的身份證書。如下所述，身份證書可用於確定區塊鏈中輕節點 310 被授權存取的資料，例如，具有與身份證書關聯的位址的帳戶記錄，以及區塊鏈中輕節點 310 不被授權存取的資料，例如具有除了管理輕節點 301 的實體之外的實體的位址的帳戶記錄。

在 325，區塊鏈節點 320 識別表示與同步請求中的區塊高度對應的區塊鏈的世界狀態的初始 MPT。例如，區塊鏈

節點可將與區塊高度對應的儲存在區塊鏈中的區塊的區塊頭中的 MPT 識別為初始 MPT。圖 4A 中描繪了表示區塊鏈網路的世界狀態結構的初始 MPT 的示例。

在 330，區塊鏈節點 320 識別與包括在初始 MPT 的世界狀態結構中的位址對應的葉區塊。區塊鏈節點 320 可解析初始 MPT 並確定輕節點 310 是否被授權存取與每個帳戶記錄關聯的位址。例如，如果區塊鏈節點 320 包括與輕節點 310 的實體關聯的位址，則區塊鏈節點 320 可確定輕節點 310 被授權存取帳戶記錄。

在 335，區塊鏈節點 320 基於初始 MPT 產生隔離 MPT。隔離 MPT 僅包括初始 MPT 中輕節點 310 被授權存取的帳戶記錄的子集。

在一些實施方式中，區塊鏈節點 320 通過存取儲存在區塊鏈節點 320 上的存取控制表產生隔離 MPT。存取控制表可用於確定以初始 MPT 的世界狀態結構表示的輕節點 310 被授權存取的各個帳戶記錄。存取控制表可指定與區塊鏈網路的輕節點關聯的實體的許可權。例如，存取控制表可指定與每個實體關聯的身份類別，使得分配給不同身份類別的實體可具有不同的用於存取安全帳戶記錄的許可權級。例如，用於身份類別的一個許可權級可指示實體被授權存取與特定實體關聯的所有帳戶記錄。

在一些示例中，由存取控制表指定的許可權可包括輕節點被授權存取帳戶資料的允許帳戶位址集。在這樣的示例中，區塊鏈節點 320 使用允許帳戶位址集來識別輕節點

310被允許存取的帳戶記錄(例如，包括允許帳戶位址的帳戶記錄)以及輕節點310不被允許存取的帳戶記錄(例如，包括不包含在允許帳戶位址集中的帳戶位址的帳戶記錄)。區塊鏈節點320產生隔離MPT，使得不被允許存取的帳戶記錄從由初始MPT表示的世界狀態結構中被刪除。

在340，作為對在步驟315接收到的同步請求的回應，區塊鏈節點320將隔離MPT發送到輕節點310。在345，輕節點310基於隔離MPT更新本地維護的世界狀態資料和同步點。例如，在下一同步點之前，輕節點310可將隔離MPT中指定的世界狀態結構儲存作為本地維護的世界狀態。

圖4A描繪了由MPT 400表示的區塊鏈節點的世界狀態結構的示例。在該示例中，回應於從例如輕節點310的輕節點接收到世界狀態同步請求，由例如區塊鏈節點320的區塊鏈節點產生MPT 400。在一些示例中，MPT 400表示特定區塊高度的區塊被添加到鏈時區塊鏈網路的世界狀態。

在一些情況下，根據識別由每個帳戶記錄表示的帳戶的公開金鑰來管理MPT 400的世界狀態結構。如先前討論的，MPT包括儲存帳戶記錄的葉節點(例如，422A、422B)、用作“路由器”的分支節點(例如，416A、420)、以及包括其所有子節點的鍵的共用部分的擴展節點(例如，406B、410A、418B)。其中，所述“路由器”將多個值(例如，26個字元中的每個，或16個十六進位數中的每個)映

射到子節點並且還可儲存帳戶記錄。如上所述，MPT中的每個葉節點(例如，422A、422B)是包括與區塊鏈網路中的特定帳戶關聯的公開金鑰的帳戶記錄和與特定帳戶關聯的諸如帳戶餘額的狀態資料。此外，每個分支節點還可利用與分支節點在MPT中的位置對應的鍵儲存帳戶記錄。

如上所述，MPT 400包括輕節點被授權存取的帳戶記錄，例如，包括與輕節點的實體的位址的帳戶記錄，以及輕節點不被授權存取的帳戶記錄。

在圖4A中描繪的示例中，輕節點310不被授權存取包括在MPT 400的區域400B中的帳戶記錄，而輕節點被授權存取包括在區域400A中的帳戶記錄。

圖4B描繪了由隔離MPT 405表示的圖3中描繪的輕節點的世界狀態結構的示例。在該示例中，由例如區塊鏈節點320的區塊鏈節點基於圖4A中描繪的初始MPT 400產生隔離MPT 405。隔離MPT 405刪除輕節點不被授權存取的帳戶記錄。例如，MPT 405刪除MPT 400的包括帳戶記錄418C和418D的區域400B中的所有節點。如上所述，輕節點不被授權存取這些帳戶記錄，因此這些帳戶記錄被從隔離MPT 405刪除。

在圖4B中描繪的示例中，基於對初始MPT 400的(如上所述，在葉節點和分支節點中的)每個帳戶記錄以及他們的父元素和子元素的解析，並確定輕節點是否被授權存取所述帳戶記錄或資料元素，來產生隔離MPT 405。在一些示例中，該確定是基於識別儲存在區塊鏈節點上的存取控

制表中標識的允許位址進行的。例如，包括在帳戶記錄 422A 和 422B 中的鍵“0x3F06”和“0x313F”被包括在存取控制表中，從而導致帳戶記錄 422A 和 422B 被包括在隔離 MPT 405 中。與此相反，包括在帳戶記錄 418C 和 418D 中的鍵“0x4E06”和“0x4E3F”不被包括在存取控制表中，因此他們被從隔離 MPT 405 刪除。

如圖 4B 中所示，從 MPT 400 的帳戶記錄 422A 和 422B 至根節點 402 的路徑上的中間節點被保存在隔離 MPT 405 中。這些中間節點包括 MPT 400 的分支節點(例如，416A、420)和擴展節點(例如，406B、410A、418B)。

圖 5 描繪了可根據本文實施方式執行的處理 500 的示例。在一些實施方式中，可使用利用一個或多個計算設備執行的一個或多個電腦可執行程式執行處理 500。

在 510，區塊鏈節點從輕節點接收同步請求。例如，區塊鏈網路的區塊鏈節點 320 接收對區塊鏈網路的世界狀態的同步請求。同步請求是從輕節點 310 被接收的並且包括輕節點 310 的身份，諸如與輕節點 310 關聯的實體的識別碼。同步請求可包括表示距離創世區塊(例如，與最近的先前同步點關聯的區塊)的區塊的數量的區塊高度。

如上所述，可基於檢測到同步觸發條件(諸如自最近同步點以後被添加到區塊鏈網路的區塊的臨限值數)或區塊鏈網路中特定事件的發生來產生同步請求，該特定事件使得需要在輕節點、區塊鏈節點和區塊鏈網路之間同步世界狀態結構。

在 520，區塊鏈節點識別與輕節點的身份關聯的一個或多個許可權。在一些情況下，識別與輕節點的身份關聯的一個或多個許可權包括：對存取控制表進行存取，該存取控制表指定針對區塊鏈網路的多個輕節點的多個身份的一個或多個許可權；識別針對輕節點的身份的存取控制表中指定的一個或多個許可權。在一些實施方式中，存取控制表包括：與區塊鏈網路的多個輕節點的多個身份中的每個身份關聯的身份類別；與包括在存取控制表中的每個身份類別關聯的許可權。在一些情況下，一個或多個許可權包括指定被授權存取與允許帳戶位址集關聯的帳戶記錄的輕節點的身份的許可權。

在 530，區塊鏈節點確定包括多個帳戶記錄並與區塊鏈高度關聯的初始世界狀態結構(例如，MPT 400)。例如，區塊鏈節點 320 確定初始 MPT 400，該初始 MPT400 表示在與區塊鏈高度關聯的區塊被添加到區塊鏈時區塊鏈網路的世界狀態結構。如上所述，初始 MPT 400 包括輕節點 310 被授權存取的帳戶記錄。

在 540，區塊鏈節點識別所述多個帳戶記錄中輕節點 310 被授權存取的子集。例如，區塊鏈節點 320 識別包括在存取控制表中被指定為允許位址並且被授權區塊鏈節點 320 存取的位址的帳戶記錄。

在 550，區塊鏈節點產生僅包括所述多個帳戶記錄中輕節點被授權存取的子集的隔離世界狀態結構。例如，區塊鏈節點 320 產生刪除了初始 MPT 400 的區域 400B 中的帳

戶記錄的隔離MPT 405。在一些情況下，產生隔離MPT包括：修改初始MPT以產生隔離MPT，包括從初始MPT移除被確定為不可由輕節點存取的所有帳戶記錄；以及移除初始MPT中的分支，其中所有帳戶記錄已被移除並只完整保留每個分支的根雜湊值。在一些實施方式中，如果一個或多個許可權指示輕節點不可對帳戶記錄進行讀取存取，則確定輕節點不可存取該帳戶記錄。在一些情況下，產生隔離MPT包括：識別初始MPT中可被輕節點存取的帳戶記錄，其中，帳戶記錄位於初始MPT的特定節點中；識別初始MPT中從儲存帳戶記錄的特定節點至初始MPT的根節點的路徑；沿儲存帳戶記錄的特定節點至初始MPT的根節點的路徑識別位於初始MPT中的中間節點；將中間節點包括在隔離MPT中。

在560，區塊鏈節點將包括隔離世界狀態結構的對同步請求的回應發送到輕節點。例如，區塊鏈節點320將隔離MPT 405發送到輕節點310作為對在步驟510接收的同步請求的回應。在下一同步步驟之前，輕節點310可將隔離MPT儲存以作為本機存放區的區塊鏈網路的世界狀態。如在圖4A和圖4B中自始至終描述和示出的那樣，隔離MPT 405指定與初始MPT相同的但刪除特定帳戶記錄的世界狀態結構以允許輕節點310與區塊鏈節點320同步，而不需要輕節點310存取輕節點310不被授權存取的帳戶記錄。

在一些實施方式中，當接收到隔離MPT 405時，輕節點310可用從區塊鏈節點返回的隔離MPT的更新版本替換

其隔離 MPT 的本地版本。

圖 6 描繪了根據本文實施方式的裝置 600 的模組的示例。裝置 600 可以是區塊鏈節點的實現方式，該區塊鏈節點被配置為保護儲存在由諸如聯盟區塊鏈網路的區塊鏈網路維護的區塊鏈上的敏感性資料。裝置 600 可對應於上述實施方式，裝置 600 包括以下：接收器或接收模組 610，用於從區塊鏈網路的輕節點接收同步請求，其中，同步請求包括輕節點的身份；第一識別器或識別模組 620，用於識別與輕節點的身份關聯的一個或多個許可權；確定器或確定模組 630，用於確定包括多個帳戶記錄的初始世界狀態結構，每個帳戶記錄儲存與該帳戶記錄關聯的帳戶的狀態資訊；第二識別器或識別模組 640，用於基於一個或多個許可權識別所述多個帳戶記錄中輕節點被授權存取的子集；產生器或產生模組 650，用於基於初始世界狀態結構產生隔離世界狀態結構，隔離世界狀態結構僅包括所述多個帳戶記錄中輕節點被授權存取的子集；發送器或發送模組 660，用於將包括隔離世界狀態結構的回應發送到輕節點。

在先前實施中示出的系統、裝置、模組或單元可以通過使用電腦晶片或實體來實現，或者可以通過使用具有特定功能的產品來實現。典型的實現設備是電腦，電腦可以是個人電腦、筆記型電腦、蜂巢式電話、相機電話、智慧型電話、個人數位助理、媒體播放機、導航設備、電子郵件收發設備、遊戲控制台、平板電腦、可穿戴設備或這些

設備的任意組合。

對於裝置中各個單元的功能和角色的實施過程，可以參考前一方法中相應步驟的實施過程。為簡單起見，這裡省略了細節。

由於裝置實施基本上對應於方法實施，對於相關部分，可以參考方法實施中的相關描述。先前描述的裝置實施僅是示例。被描述為單獨部分的單元可以是或不是實體上分離的，並且顯示為單元的部分可以是或不是實體單元，可以位於一個位置，或者可以分佈在多個網路單元上。可以基於實際需求來選擇一些或所有模組，以實現本說明書方案的目標。本發明所屬技術領域具有通常知識者無需付出進步性勞動就能理解和實現本文實施方式。

再次參照圖 6，其可被解釋為示出區塊鏈節點的內部功能模組和結構，所述模組和結構被配置為保護儲存在由區塊鏈網路維護的區塊鏈上的敏感性資料。執行主體本質上可以是電子設備和包括以下的電子設備：一個或多個處理器；記憶體，儲存一個或多個處理器的可執行指令。

本文中描述的技術產生若干技術效果。例如，用於產生隔離世界狀態結構(例如 MPT)的技術使得區塊鏈網路中的輕節點能夠基於世界狀態結構驗證交易，而不違反區塊鏈網路的存取控制許可權。這允許更有效地控制區塊鏈網路中的資料存取，從而實現更安全的網路。此外，用於產生隔離世界狀態結構的技術實現了與非隔離世界狀態結構一致的結構。這可使得輕節點使用與非隔離世界狀態結構

相同的處理來基於隔離世界狀態結構驗證交易，從而減輕對更新輕節點以實施存取控制的任何需要。在其他實施方式中，該技術在區塊鏈網路中的透明化和資料保護之間取得平衡。具體地，區塊鏈設計者在建立系統時面臨難題。一方面，區塊鏈總體上是關於透明的可審核性，通過共用的分散式帳本實現信任。另一方面，企業交易經常處理由於一些原因而不應在所有參與者之間被共用的敏感性資料。該技術保護參與者的資料，而同時保持分散信任和透明化的優勢。

描述的主題的實施方式可單獨包括一個或多個特徵或者一個或多個特徵的組合。

在一些實施例中，操作包括：區塊鏈網路中的區塊鏈節點從區塊鏈網路的輕節點接收同步請求，其中，同步請求包括輕節點的身份和與同步請求關聯的區塊高度；區塊鏈節點識別與輕節點的身份關聯的一個或多個許可權；區塊鏈節點確定與區塊高度關聯且包括多個帳戶記錄的初始世界狀態結構，每個帳戶記錄儲存與帳戶記錄關聯的帳戶的狀態資訊，其中，初始世界狀態結構表示所述區塊鏈網路在與區塊高度關聯的區塊被添加到區塊鏈時的狀態；區塊鏈節點基於一個或多個許可權識別所述多個帳戶記錄中輕節點被授權存取的子集；區塊鏈節點基於初始世界狀態結構產生隔離世界狀態結構，隔離世界狀態結構僅包括所述多個帳戶記錄中輕節點被授權存取的子集；區塊鏈節點將包括隔離世界狀態結構的回應發送到輕節點。

其他實施例包括相應系統、裝置和被配置為執行方法的操作的編碼在電腦存放裝置上的電腦程式。

這些和其他實施例可均可選地包括以下特徵中的一個或多個：

在一些情況下，識別與輕節點的身份關聯的一個或多個許可權包括：對存取控制表進行存取，該存取控制表指定區塊鏈網路的多個輕節點的多個身份的一個或多個許可權；識別針對輕節點的身份的存取控制表中指定的一個或多個許可權。

在一些實施例中，存取控制表包括：與區塊鏈網路的多個輕節點的多個身份中的每個身份關聯的身份類別；與包括在存取控制表中的每個身份類關聯的許可權。

在一些實施例中，一個或多個許可權包括指定被授權存取與允許帳戶位址集關聯的帳戶記錄的輕節點的身份的許可權。

在一些實施例中，初始世界狀態結構是初始默克爾派特裡夏樹(Merkle Patricia Trie(MPT))，隔離世界狀態結構是隔離MPT。

在一些實施例中，產生隔離MPT包括修改初始MPT以產生隔離MPT，該操作包括：從初始MPT移除被確定為不可由輕節點存取的所有帳戶記錄；移除初始MPT的分支，其中所有帳戶記錄已被移除並只完整保留每個分支的根雜湊值。

在一些實施例中，如果一個或多個許可權指示輕節點

不可對帳戶記錄進行讀取存取，則確定輕節點不可存取該帳戶記錄。

在一些實施例中，產生隔離 MPT 包括：識別初始 MPT 中可被輕節點存取的帳戶記錄，其中，帳戶記錄位於初始 MPT 的特定節點中，其中，特定節點是分支節點或葉節點；識別初始 MPT 中從儲存帳戶記錄的特定節點至初始 MPT 的根節點的路徑；沿儲存帳戶記錄的特定節點至初始 MPT 的根節點的路徑識別位於初始 MPT 中的中間節點；將中間節點包括在隔離 MPT 中。

本文還提供一種非暫時性電腦可讀儲存媒體，其耦接到一個或多個處理器且其上儲存有指令，當由一個或多個處理器執行所述指令時，該指令促使一個或多個處理器根據本文提供的方法的實施例執行操作。

本文還提供一種用於實現本文提供的方法的系統。該系統包括：一個或多個處理器；以及電腦可讀儲存媒體，其耦接到一個或多個處理器並在其上儲存有指令，當由一個或多個處理器執行該指令時，該指令促使一個或多個處理器根據本文提供的方法的實施例執行操作。

本文中描述的主題、動作以及操作的實施例可以在數位電子電路、有形體現的電腦軟體或韌體、電腦硬體中實現，包括本文中公開的結構及其結構等同物，或者它們中的一個或多個的組合。本文中描述的主題的實施例可以實現為一個或多個電腦程式，例如，一個或多個電腦程式指令模組，編碼在電腦程式載體上，用於由資料處理裝置執

行或控制資料處理裝置的操作。例如，電腦程式載體可包括其上編碼和儲存有指令的一個或多個電腦可讀儲存媒體。載體可以是有形的非暫態電腦可讀媒體，諸如磁片、磁光碟、或光碟、固態驅動器、隨機存取記憶體(RAM)、唯讀記憶體(ROM)或者其他類型的媒體。可選地或附加地，載體可以是人工產生的傳播信號，例如，機器產生的電、光或電磁信號，其被產生來編碼資訊用於傳輸到合適的接收器裝置以供資料處理裝置執行。電腦儲存媒體可以是或部分為機器可讀存放裝置、機器可讀儲存基板、隨機或串列存取記憶體設備或它們中的一個或多個的組合。電腦儲存媒體不是傳播信號。

電腦程式也可以被稱為或描述為程式、軟體、軟體應用程式、app、模組、軟體模組、引擎、腳本或代碼，可以以任何形式的程式設計語言編寫，包括編譯或演繹性語言、說明或程式性語言；它可以配置為任何形式，包括作為獨立程式，或者作為模組、元件、引擎、副程式或適合在計算環境中執行的其他單元，該環境可包括由通信資料網路互聯的在一個或多個位置的一台或多台電腦。

電腦程式可以但非必須對應於檔案系統中的檔。電腦程式可以儲存在：保存其他程式或資料的檔的一部分中，例如，儲存在標記語言文檔中的一個或多個腳本；專用於所討論的程式的單個檔；或者多個協調檔，例如，儲存一個或多個模組、副程式或代碼部分的多個檔。

用於執行電腦程式的處理器包括例如通用微處理器和

專用微處理器兩者以及任何類型的數位電腦的任何一個或多個處理器。通常，處理器將從耦接到處理器的非暫時性電腦可讀媒體接收電腦程式的指令以及資料。

用語“資料處理裝置”包括用於處理資料的所有類型的裝置、設備和機器，包括例如可程式設計處理器、電腦或者多處理器或電腦。資料處理裝置可以包括專用邏輯電路，例如FPGA(現場可程式設計閘陣列)、ASIC(特殊應用積體電路)或GPU(圖形處理單元)。除了硬體，該裝置還可以包括為電腦程式創建執行環境的代碼，例如，構成處理器韌體、協定堆疊、資料庫管理系統、作業系統或者它們中的一個或多個的組合的代碼。

本文中描述的處理和邏輯流程可由一台或多台電腦執行一個或多個電腦程式進行，以進行通過對輸入資料進行運算並產生輸出的操作。處理和邏輯流程也可以由例如FPGA、ASIC、GPU等的專用邏輯電路或專用邏輯電路與一個或多個程式設計電腦的組合來執行。

適合於執行電腦程式的電腦可以基於通用及/或專用微處理器，或任何其他種類的中央處理單元。通常，中央處理單元將從唯讀記憶體及/或隨機存取記憶體接收指令和資料。電腦的元件可包括用於執行指令的中央處理單元以及用於儲存指令和資料的一個或多個記憶體設備。中央處理單元和記憶體可以補充有專用邏輯電路或整合在專用邏輯電路中。

通常，電腦將還包括一個或多個存放裝置，或操作性

地耦接至一個或多個存放裝置以從一個或多個存放裝置接收資料或將資料傳送至一個或多個存放裝置。存放裝置可以是例如，磁片、磁光碟、光碟、固態驅動器、或任何其他類型非暫時性電腦可讀媒體。但是，電腦不需要具有這樣的設備。因此，電腦可耦接到本地及/或遠端的一個或多個存放裝置，諸如一個或多個記憶體。例如，電腦可包括作為電腦的整合元件的一個或多個本機存放區器，或者電腦可耦接到雲端網路中的一個或多個遠端存放器。此外，電腦可以嵌入在另一個設備中，例如行動電話、個人數位助理(PDA)、移動音訊或視訊播放機、遊戲控制台、全球定位系統(GPS)接收器或例如通用序列匯流排(USB)快閃記憶體驅動器的可攜式存放裝置，僅舉幾例。

元件可通過可交換地諸如彼此直接或經由一個或多個中間元件電連接或光連接來彼此“耦接”。如果一個元件整合在另一元件中，元件還可彼此“耦接”。例如，整合在記憶體中的儲存元件(例如，L2快取記憶體組件)“耦接到”處理器。

為了提供與用戶的互動，本文中描述的主題的實施例可以在電腦上實現或配置為與該電腦通信，該計算機具有：顯示裝置，例如，LCD(液晶顯示器)監視器，用於向使用者顯示資訊；以及輸入裝置，使用者可以通過該輸入裝置向該電腦提供輸入，例如鍵盤和例如滑鼠、軌跡球或觸控板等的指標裝置。其他類型的設備也可用於提供與用戶的互動；例如，提供給用戶的回饋可以是任何形式的感

官回饋，例如視覺回饋、聽覺回饋或觸覺回饋；並且可以接收來自用戶的任何形式的輸入，包括聲音、語音或觸覺輸入。此外，電腦可以通過向使用者使用的設備發送文檔和從使用者使用的設備接收文檔來與用戶互動；例如，通過向使用者設備上的web瀏覽器發送web頁面以回應從web瀏覽器收到的請求，或者通過與例如智慧型電話或電子平板電腦等的使用者設備上運行的應用程式(app)進行互動。此外，電腦可以通過向個人設備(例如，運行資訊應用的智慧手機)發送資訊簡訊或其他形式的資訊並反過來接收來自使用者的回應訊息來與用戶互動。

本文結合系統、裝置和電腦程式元件使用用語“配置為”。對於被配置為執行特定操作或動作的一個或多個電腦的系統，意味著系統已經在其上安裝了在運行中促使該系統執行所述操作或動作的軟體、韌體、硬體或它們的組合。對於被配置為執行特定操作或動作的一個或多個電腦程式，意味著一個或多個程式包括當被資料處理裝置執行時促使該裝置執行所述操作或動作的指令。對於被配置為執行特定操作或動作的專用邏輯電路，意味著該電路具有執行所述操作或動作的電子邏輯。

雖然本文包含許多具體實施細節，但是這些不應被解釋為由申請專利範圍本身限定的對要求保護的範圍的限制，而是作為對特定實施例的具體特徵的描述。在本文多個單獨實施例的上下文中描述的多個特定特徵也可以在單個實施例中的組合實現。相反，在單個實施例的上下文中

描述的各種特徵也可以單獨地或以任何合適的子組合在多個實施例中實現。此外，儘管上面的特徵可以描述為以某些組合起作用並且甚至最初如此要求保護，但是在一些情況下，可以從要求保護的組合中刪除來自該組合的一個或多個特徵，並且可以要求保護指向子組合或子組合的變體。

類似地，雖然以特定順序在圖式中描繪了操作並且在申請專利範圍中敘述了操作，但是這不應該被理解為：為了達到期望的結果，要求以所示的特定順序或依次執行這些操作，或者要求執行所有示出的操作。在一些情況下，多工和平行處理可能是有利的。此外，上述實施例中的各種系統模組和元件的劃分不應被理解為所有實施例中都要如此劃分，而應當理解，所描述的程式元件和系統通常可以一起整合在單個軟體產品或者打包成多個軟體產品。

已經描述了主題的特定實施例。其他實施例在以下申請專利範圍的範圍內。例如，申請專利範圍中記載的動作可以以不同的循序執行並且仍然實現期望的結果。作為一個示例，圖式中描繪的處理無需要求所示的特定順序或次序來實現期望的結果。在一些情況下，多工和平行處理可能是有利的。

【符號說明】

100:環境

102:聯盟區塊鏈網路

- 106:計算系統
- 108:計算系統
- 110:網路
- 200:概念架構
- 202:實體層
- 204:承載服務層
- 206:區塊鏈網路層
- 208:交易管理系統
- 210:介面
- 212:區塊鏈網路
- 214:節點
- 216:區塊鏈
- 305:步驟
- 310:步驟
- 315:步驟
- 320:區塊鏈節點
- 325:步驟
- 330:步驟
- 335:步驟
- 340:步驟
- 345:步驟
- 400A:區域
- 400B:區域
- 402:根節點

406B:擴展節點

410A:擴展節點

416A:分支節點

418B:擴展節點

418C:帳戶記錄

418D:帳戶記錄

420:分支節點

422A:葉節點

422B:葉節點

500:處理

510:步驟

520:步驟

530:步驟

540:步驟

550:步驟

560:步驟

600:裝置

610:接收器

620:第一識別器

630:確定器

640:第二識別器

650:產生器

660:發送器

A:參與者

B:參與者

C:參與者

【發明申請專利範圍】

【請求項 1】一種電腦實現的方法，用於隔離儲存在由區塊鏈網路維護的區塊鏈上的資料，所述方法包括：

所述區塊鏈網路中的區塊鏈節點從所述區塊鏈網路的輕節點接收同步請求，其中，所述同步請求包括所述輕節點的身份及與所述同步請求關聯的區塊高度；

所述區塊鏈節點識別與所述輕節點的身份關聯的一個或多個許可權；

所述區塊鏈節點確定包括多個帳戶記錄的初始世界狀態結構，每個所述帳戶記錄儲存與該帳戶記錄關聯的帳戶的狀態資訊，其中，所述初始世界狀態結構是基於所述區塊高度確定的，並表示所述區塊鏈網路在與所述區塊高度關聯的區塊被添加到所述區塊鏈時的狀態，及其中，所述初始世界狀態結構是初始默克爾派特裡夏樹MPT；

所述區塊鏈節點基於所述一個或多個許可權識別所述多個帳戶記錄中所述輕節點被授權存取的子集；

所述區塊鏈節點基於所述初始世界狀態結構產生隔離世界狀態結構，所述隔離世界狀態結構僅包括所述多個帳戶記錄中所述輕節點被授權存取的子集，其中所述隔離世界狀態結構是隔離MPT，其中，產生所述隔離MPT包括：

識別所述初始MPT中能被所述輕節點存取的帳戶記錄，其中，所述帳戶記錄位於所述初始MPT的特定節點中，所述特定節點是分支節點或葉節點；

識別所述初始MPT中從儲存所述帳戶記錄的所述

特定節點至所述初始MPT的根節點的路徑；

沿從儲存所述帳戶記錄的所述特定節點至所述初始MTP的根節點的路徑識別位於所述初始MPT中的中間節點；以及

將所述中間節點包括在所述隔離MPT中；以及

所述區塊鏈節點將包括所述隔離世界狀態結構的回應發送到所述輕節點。

【請求項2】如請求項1所述的電腦實現的方法，其中，識別與所述輕節點的身份關聯的所述一個或多個許可權包括：

對存取控制表進行存取，所述存取控制表指定所述區塊鏈網路的多個輕節點的多個身份的一個或多個許可權；以及

識別所述存取控制表中針對所述輕節點的身份指定的一個或多個許可權。

【請求項3】如請求項2所述的電腦實現的方法，其中，所述存取控制表包括：

與所述區塊鏈網路的多個輕節點的多個身份中的每個身份關聯的身份類別；以及

與所述存取控制表中包括的每個身份類別關聯的許可權。

【請求項4】如請求項3所述的電腦實現的方法，其中，所述一個或多個許可權包括如下的許可權，該許可權指定被授權存取與允許帳戶位址集關聯的帳戶記錄的輕節

點的身份。

【請求項 5】如請求項 1 所述的電腦實現的方法，其中，產生所述隔離 MPT 包括修改所述初始 MPT 以產生所述隔離 MPT，包括：

從所述初始 MPT 移除被確定為所述輕節點不能存取的所有帳戶記錄；以及

移除所有帳戶記錄已被移除的所述初始 MPT 的分支，並只完整保留所述分支中的每個分支的根雜湊值。

【請求項 6】如請求項 5 所述的電腦實現的方法，其中，如果所述一個或多個許可權指示所述輕節點不能對帳戶記錄進行讀取存取，則確定所述輕節點不能存取所述帳戶記錄。

【請求項 7】如請求項 1 所述的電腦實現的方法，其中，所述區塊高度表示距離創世區塊的區塊的數量的區塊高度，可選地，其中，所述創世區塊是與最近的先前同步點關聯的區塊。

【請求項 8】一種用於隔離儲存在由區塊鏈網路維護的區塊鏈上的資料的裝置，包括：

接收模組，用於從所述區塊鏈網路的輕節點接收同步請求，其中，所述同步請求包括所述輕節點的身份與所述同步請求關聯的區塊高度；

第一識別模組，用於識別與所述輕節點的身份關聯的一個或多個許可權；

確定模組，用於確定包括多個帳戶記錄的初始世界狀

態結構，每個帳戶記錄儲存與所述帳戶記錄關聯的帳戶的狀態資訊，其中，所述初始世界狀態結構是基於所述區塊高度確定的，並表示所述區塊鏈網路在與所述區塊高度關聯的區塊被添加到所述區塊鏈時的狀態，及其中，所述初始世界狀態結構是初始默克爾派特裡夏樹MPT；

識別模組，用於基於所述一個或多個許可權識別所述多個帳戶記錄中所述輕節點被授權存取的子集；

產生模組，用於基於所述初始世界狀態結構產生隔離世界狀態結構，所述隔離世界狀態結構僅包括所述多個帳戶記錄中所述輕節點被授權存取的子集，其中，所述隔離世界狀態結構是隔離MPT，其中，產生所述隔離MPT包括：

識別所述初始MPT中能被所述輕節點存取的帳戶記錄，其中，所述帳戶記錄位於所述初始MPT的特定節點中，其中，所述特定節點是分支節點或葉節點；

識別所述初始MPT中從儲存所述帳戶記錄的所述特定節點至所述初始MPT的根節點的路徑；

沿儲存所述帳戶記錄的所述特定節點至所述初始MPT的所述根節點的路徑識別位於所述初始MPT中的中間節點；將所述中間節點包括在所述隔離MPT中；

發送模組，將包括所述隔離世界狀態結構的回應發送到所述輕節點。

【請求項9】如請求項8所述的裝置，其中，識別與所述輕節點的身份關聯的所述一個或多個許可權包括：

對存取控制表進行存取，所述存取控制表指定所述區塊鏈網路的多個輕節點的多個身份的一個或多個許可權；以及

識別針對所述輕節點的身份的存取控制表中指定的一個或多個許可權。

【請求項 10】如請求項 9 所述的裝置，其中，所述存取控制表包括：

與所述區塊鏈網路的所述多個輕節點的所述多個身份中的每個身份關聯的身份類別；以及

與所述存取控制表中包括的每個身份類別關聯的許可權。

【請求項 11】如請求項 8 所述的裝置，其中，所述一個或多個許可權包括指定被授權存取與允許帳戶位址集關聯的帳戶記錄的所述輕節點的身份的許可權。

【請求項 12】如請求項 8 所述的裝置，其中，產生所述隔離 MPT 包括修改所述初始 MPT 以產生所述隔離 MPT，包括：

從所述初始 MPT 移除被確定為所述輕節點不能存取的所有帳戶記錄；以及

移除所述初始 MPT 的分支，其中所有帳戶記錄已被移除並只完整保留所述分支中的每個分支的根雜湊值；

及可選地，其中，如果所述一個或多個許可權指示所述輕節點不能對帳戶記錄進行讀取存取，則確定所述輕節點不能存取所述帳戶記錄。

【請求項 13】如請求項 12 所述的裝置，其中，如果所述一個或多個許可權指示所述輕節點不能對帳戶記錄進行讀取存取，則確定所述輕節點不能存取所述帳戶記錄。

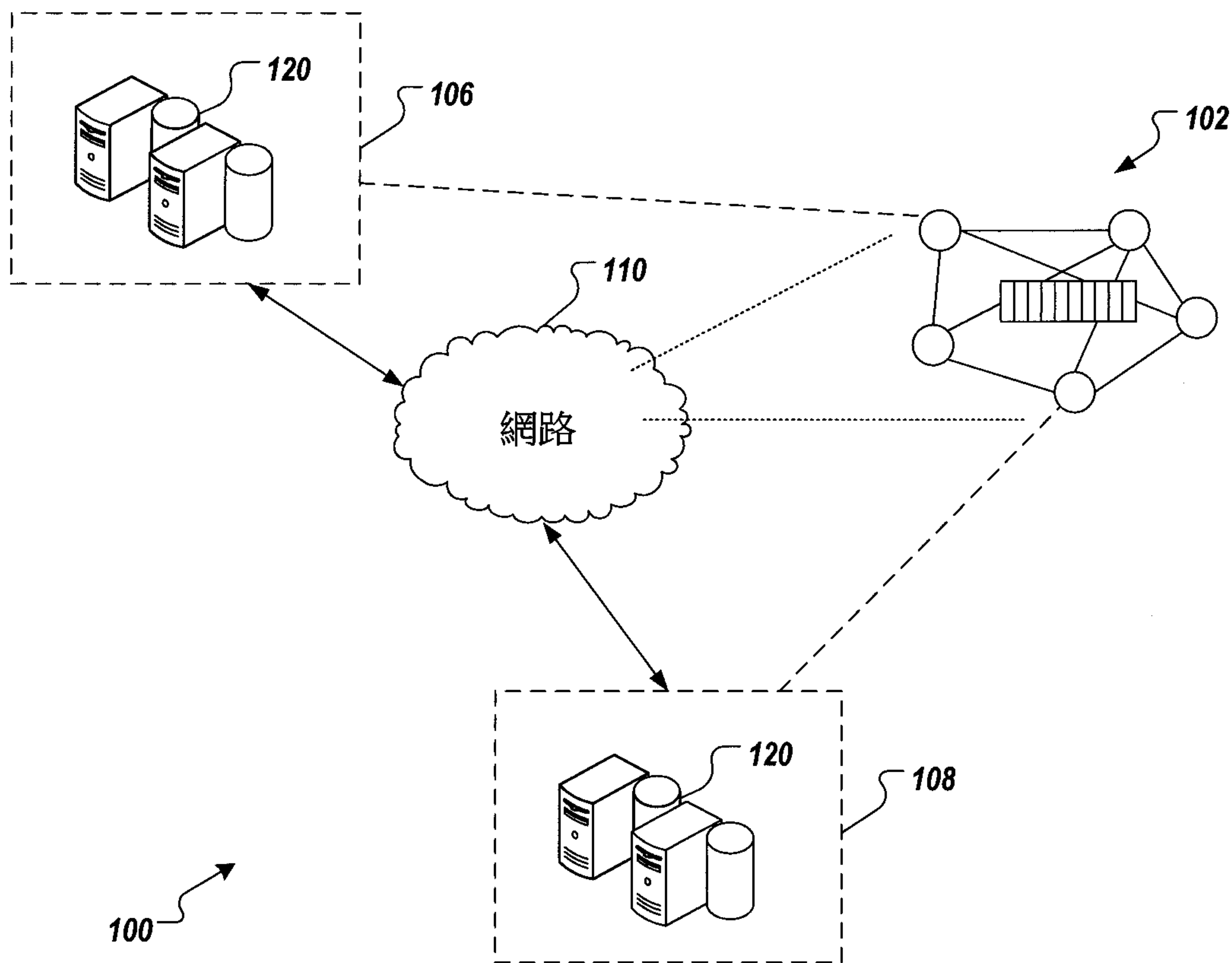
【請求項 14】如請求項 8 所述的裝置，其中，所述區塊高度表示距離創世區塊的區塊的數量的區塊高度，可選地，所述創世區塊是與最近的先前同步點關聯的區塊。

【請求項 15】一種系統，包括：

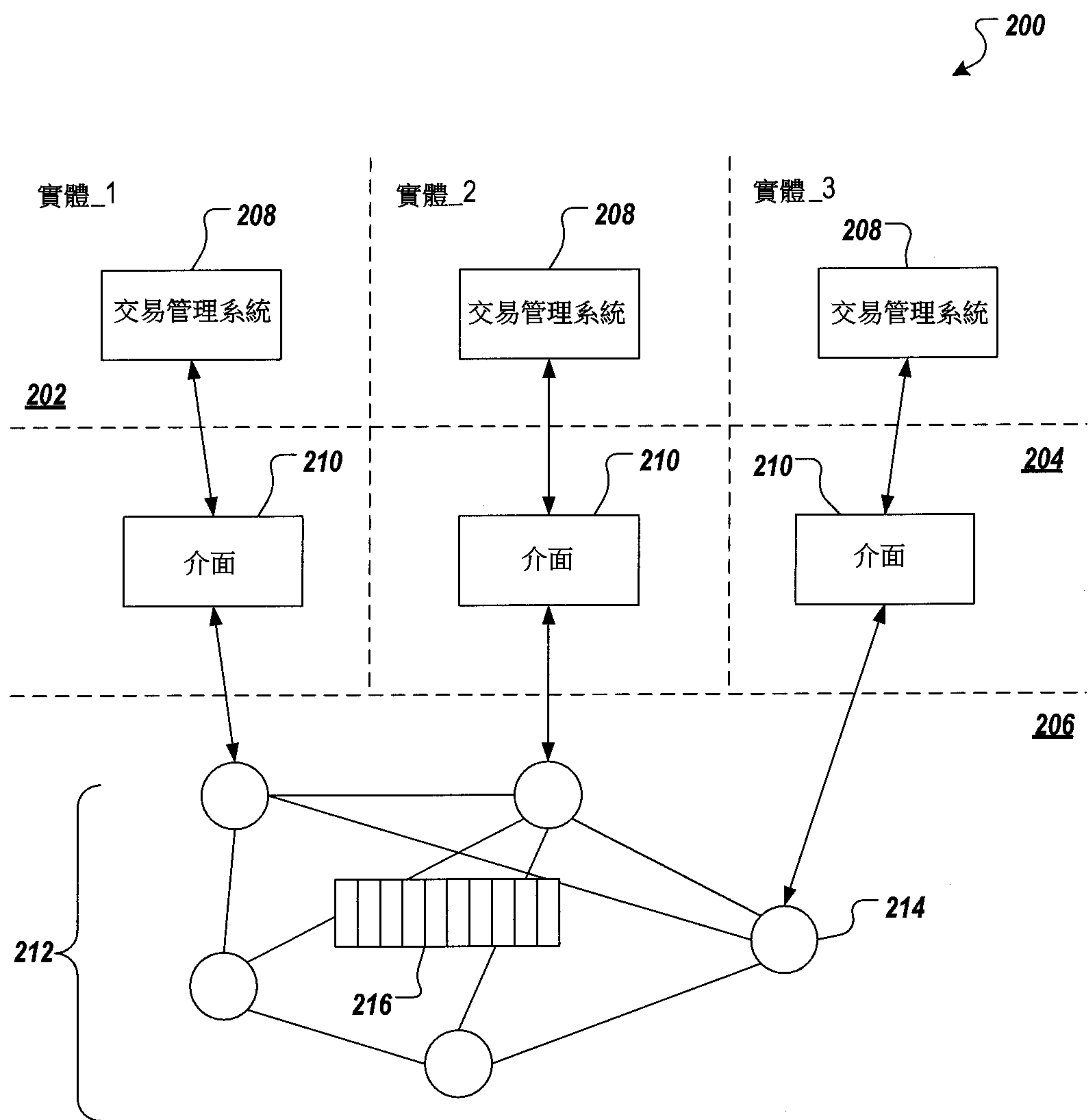
一個或多個處理器；以及

耦接到所述一個或多個處理器並且其上儲存有指令的一個或多個電腦可讀記憶體，所述指令能由所述一個或多個處理器執行以執行請求項 1 至 7 任一項所述的方法。

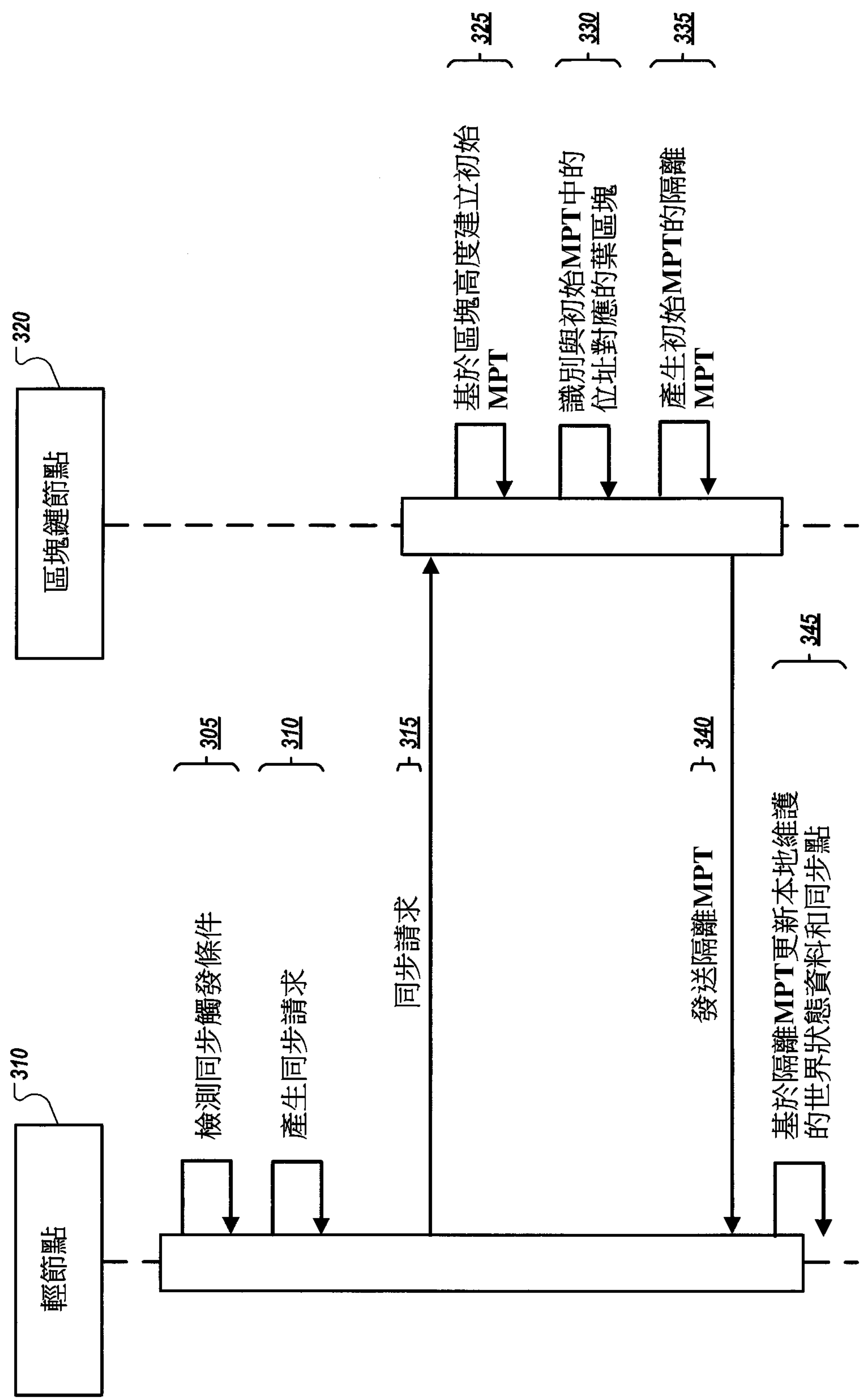
【發明圖式】



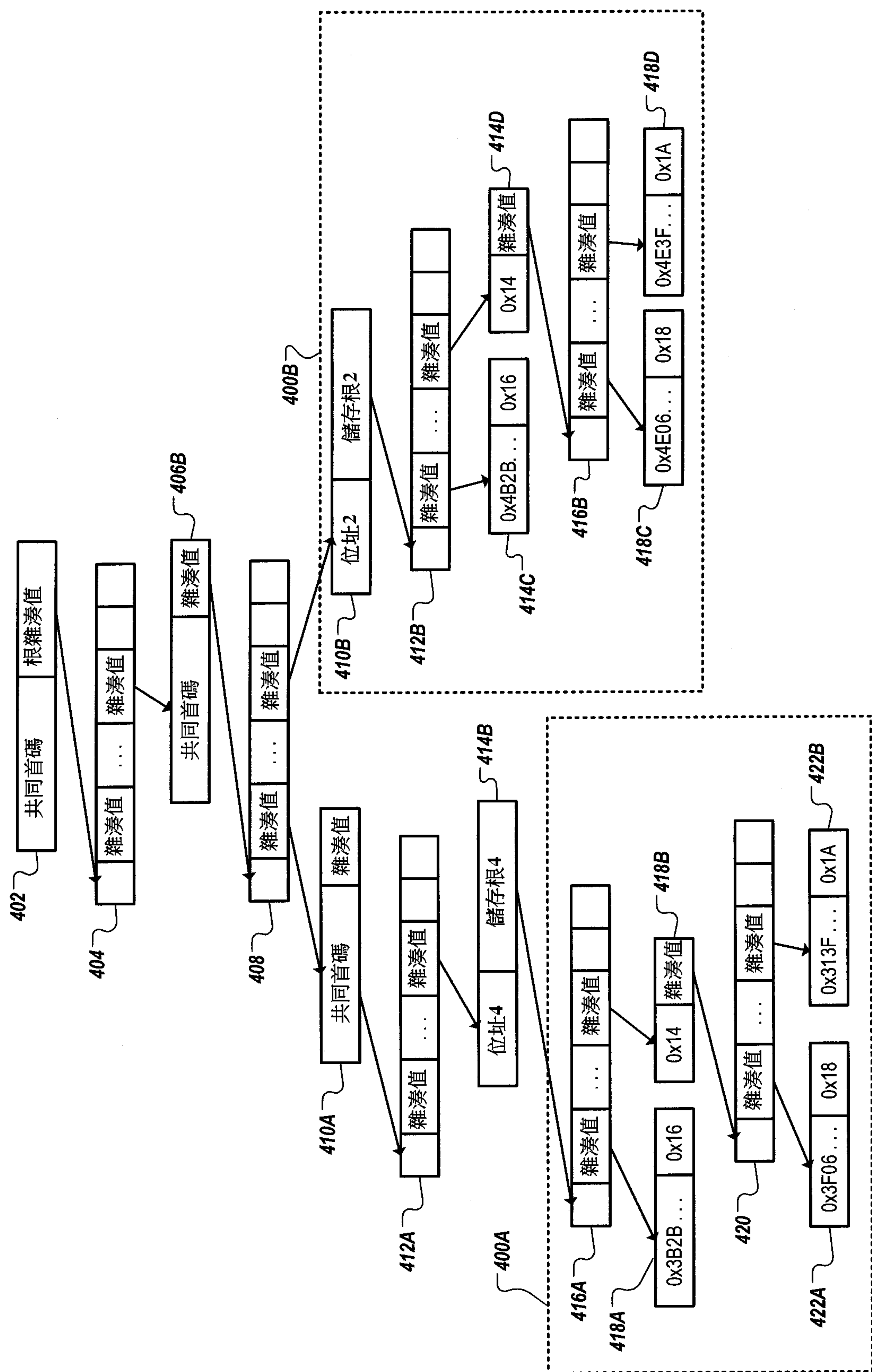
【圖 1】



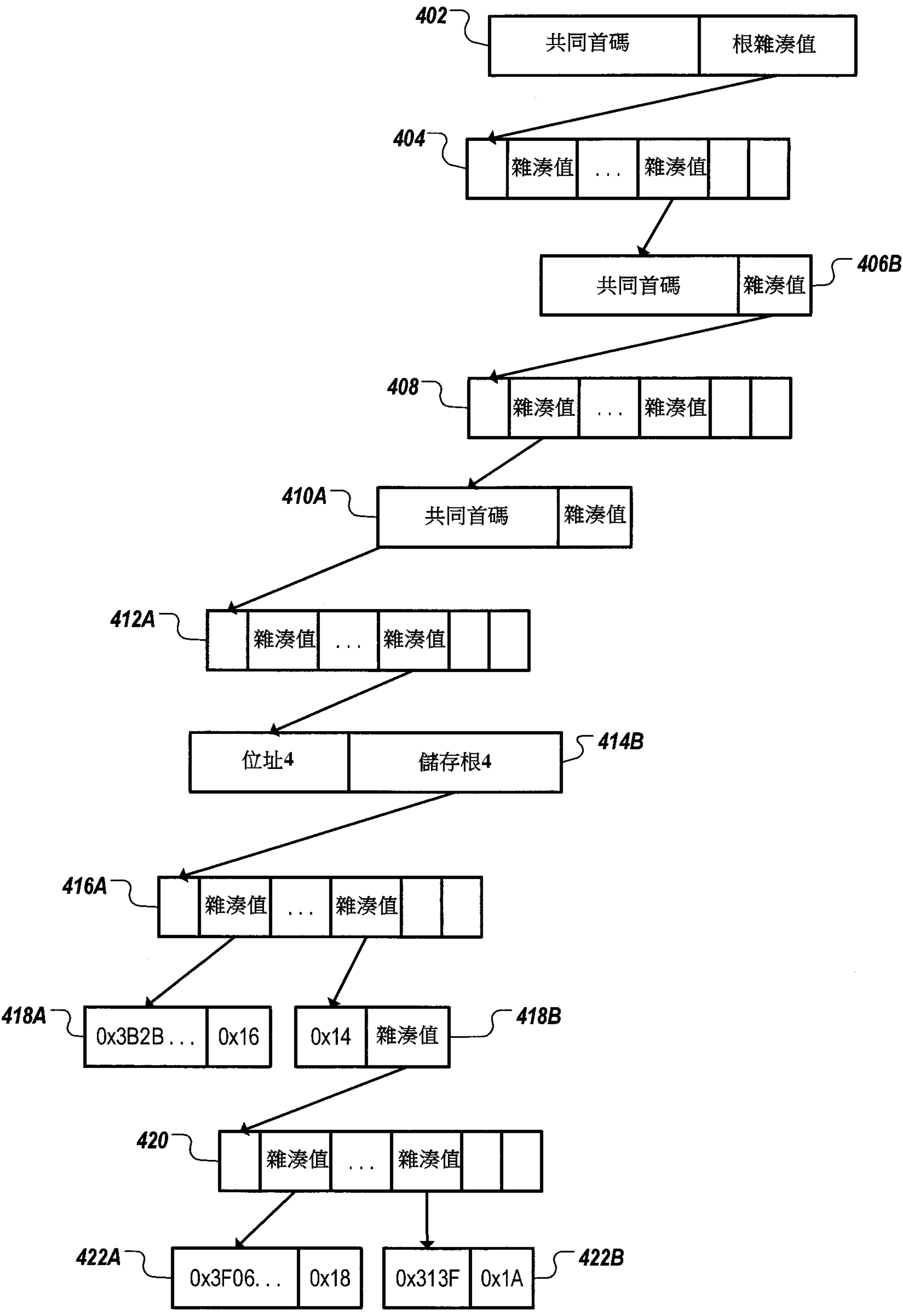
【圖 2】



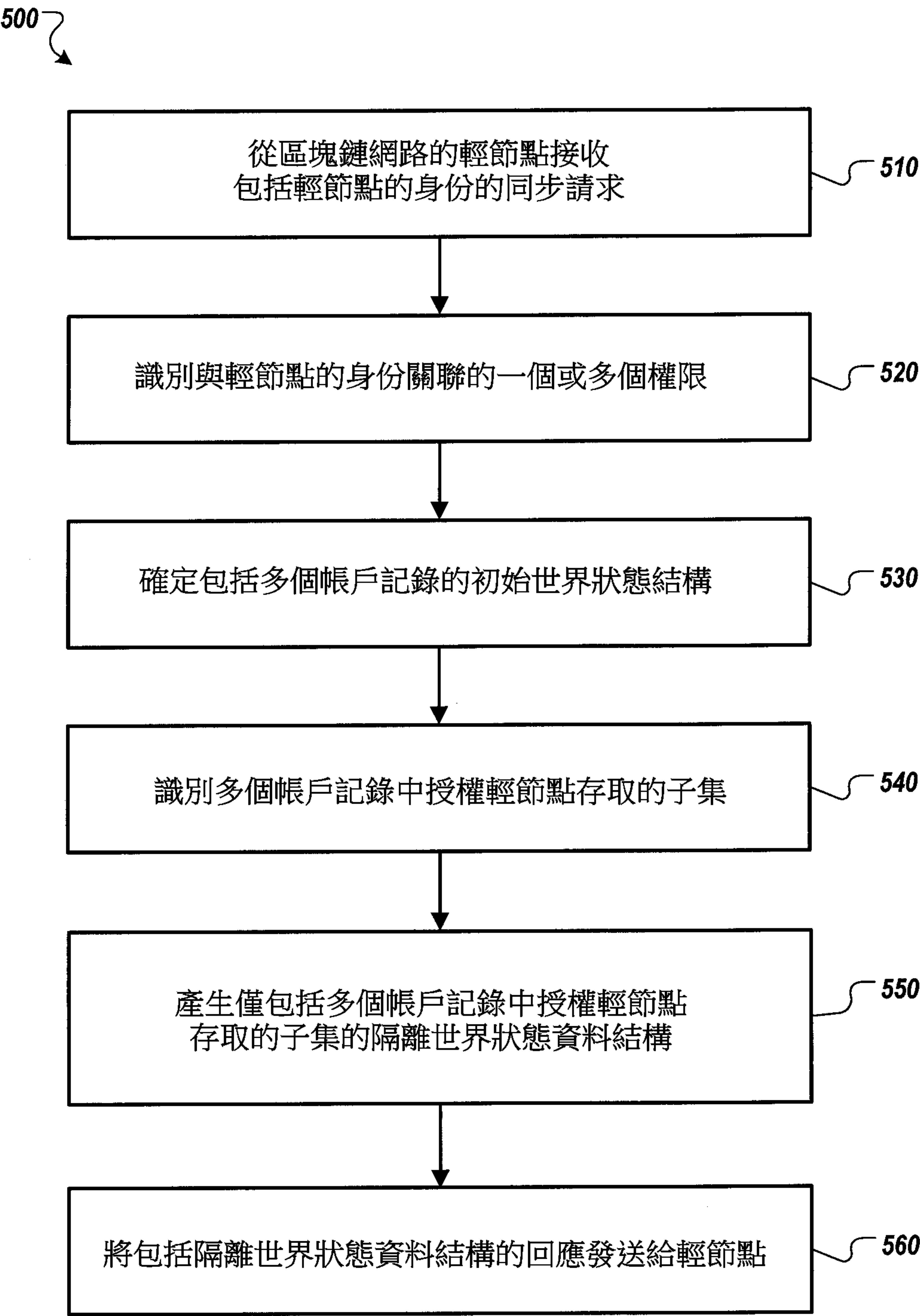
【圖 3】



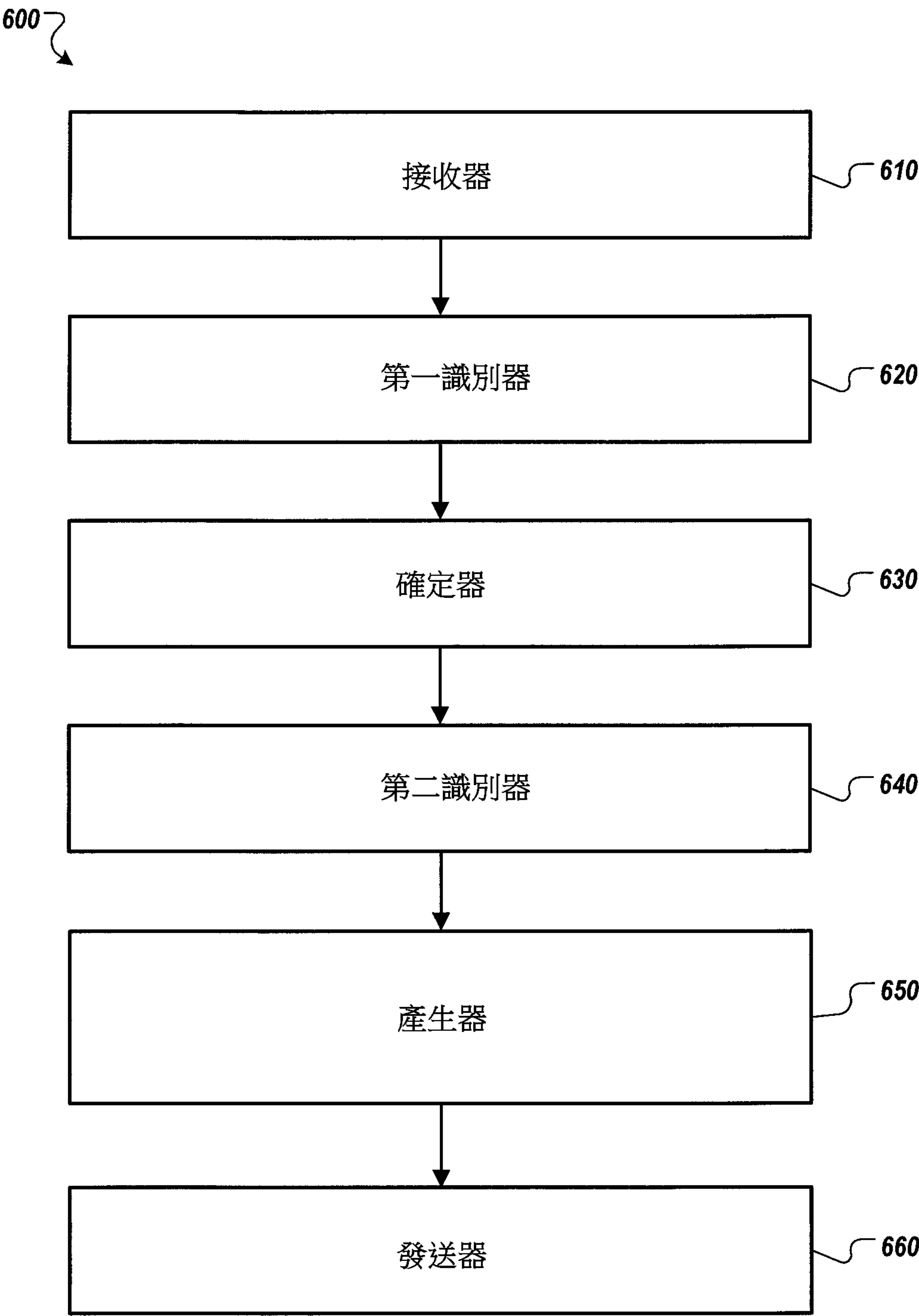
【4A】



【圖 4B】



【圖 5】



【圖 6】