I707245

(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 I707245 B**

(45)公告日： 中華民國 109 (2020) 年 10 月 11 日

(21)申請案號：108145430　(22)申請日： 中華民國 108 (2019) 年 12 月 12 日

(51)Int. Cl.：　*G06F21/60　(2013.01)*　*G06Q20/38　(2012.01)*

(30)優先權：2019/03/29　世界智慧財產權組織　PCT/CN2019/080478

(71)申請人：香港商阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED　(HK)

香港

(72)發明人：余逸榮 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW	201837805A	CN	109299338A
CN	109327512A	US	2018/0219685A1

審查人員：馮耀嘉

申請專利範圍項數：10 項　圖式數：11　共 67 頁

(54)名稱

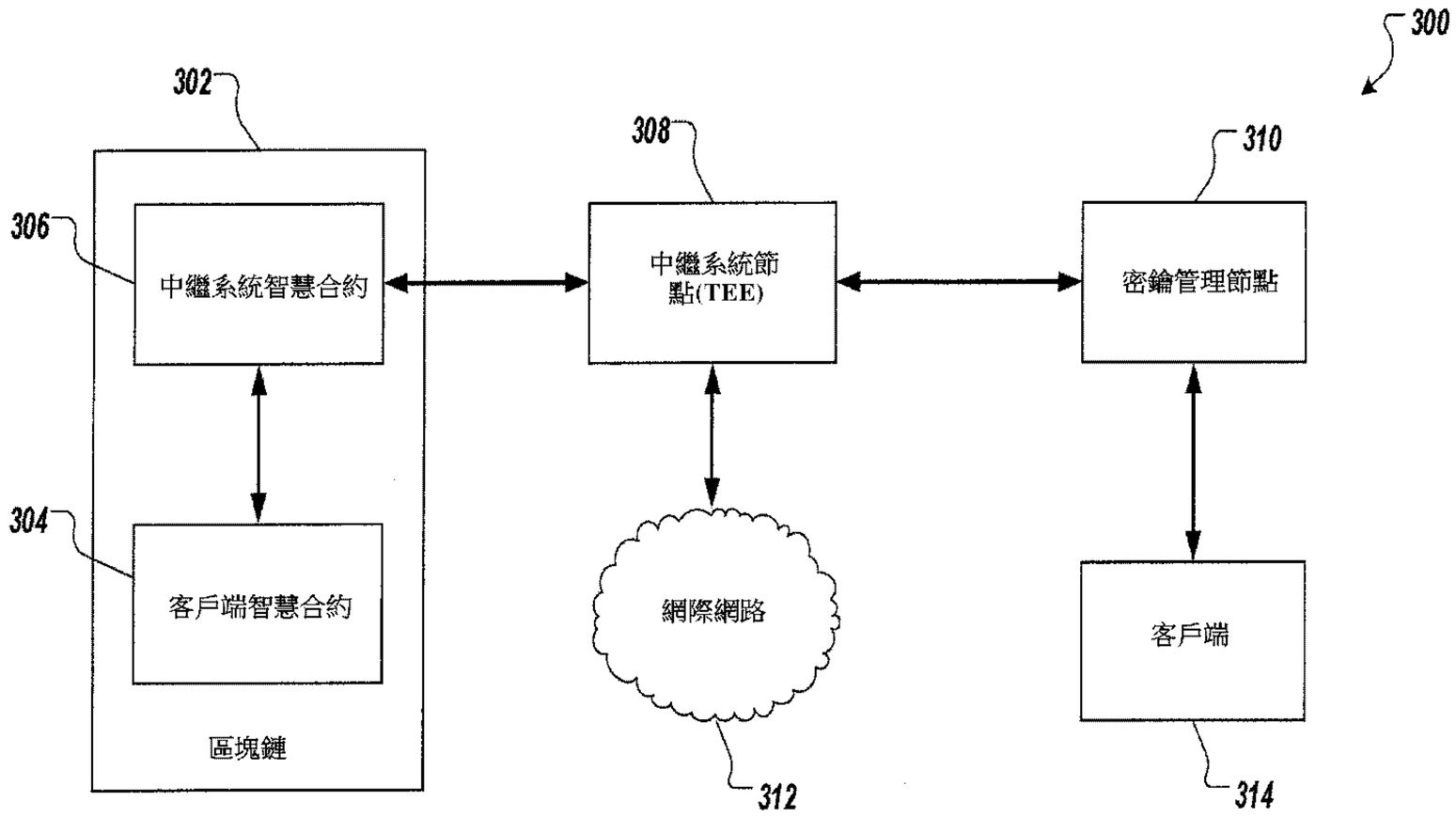
使用高可用性的可信執行環境檢索區塊鏈網路的存取資料

(57)摘要

本發明公開了用於從外部資料源檢索資料以在區塊鏈網路內進行處理的方法、系統和裝置，包括編碼在電腦儲存媒體上的電腦程式。所述方法之一包括：接收對於包括加密資料的資料的請求，該加密資料包括使用密鑰管理節點的服務公鑰加密的存取資料；從共享密鑰管理節點的服務私鑰的多個中繼系統節點中選擇中繼系統節點；將該請求發送至中繼系統節點；接收從中繼系統節點提供的回應，該回應包括結果資料和數位簽名，其中該數位簽名是基於結果資料和密鑰管理節點的服務私鑰產生的；以及將該回應發送至客戶端。

Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for retrieving data from external data sources for processing within a blockchain network. One of the methods includes receiving a request for data that includes encrypted data, the encrypted data including access data that is encrypted using a service public key of a key management node; selecting a relay system node from a plurality of relay system nodes that share a service private key of the key management node; transmitting the request to the relay system node; receiving a response provided from the relay system node, the response including result data and a digital signature, wherein the digital signature is generated based on the result data and the service private key of the key management node; and transmitting the response to a client.

指定代表圖：



【圖 3】

符號簡單說明：

300:系統

302:區塊鏈

304:客戶端智慧合約

306:中繼系統智慧合約

308:中繼系統節點

310:密鑰管理節點

312:網路

314:客戶端

專利案號：108145430

公告本

I707245

【發明摘要】

【中文發明名稱】

使用高可用性的可信執行環境檢索區塊鏈網路的存取資料

【英文發明名稱】

RETRIEVING ACCESS DATA FOR BLOCKCHAIN NETWORKS USING HIGHLY AVAILABLE TRUSTED EXECUTION ENVIRONMENTS

【中文】

本發明公開了用於從外部資料源檢索資料以在區塊鏈網路內進行處理的方法、系統和裝置，包括編碼在電腦儲存媒體上的電腦程式。所述方法之一包括：接收對於包括加密資料的資料的請求，該加密資料包括使用密鑰管理節點的服務公鑰加密的存取資料；從共享密鑰管理節點的服務私鑰的多個中繼系統節點中選擇中繼系統節點；將該請求發送至中繼系統節點；接收從中繼系統節點提供的回應，該回應包括結果資料和數位簽名，其中該數位簽名是基於結果資料和密鑰管理節點的服務私鑰產生的；以及將該回應發送至客戶端。

【英文】

Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for retrieving data from external data sources for processing within a blockchain network. One of the methods includes receiving a request for data that includes encrypted data, the encrypted data including access data that is encrypted using a service public key of a key management node; selecting a relay system node from a plurality of relay system nodes that share a service private key of the key management node; transmitting the request to the relay system node; receiving a response provided from the relay system node, the response including result data and a digital signature, wherein the digital signature is generated based on the result data and the service private key of the key management node; and transmitting the response to a client.

【指定代表圖】第(3)圖。
【代表圖之符號簡單說明】

300:系統

302:區塊鏈

304:客戶端智慧合約

306:中繼系統智慧合約

308:中繼系統節點

310:密鑰管理節點

312:網路

314:客戶端

【特徵化學式】無

【發明說明書】

【中文發明名稱】

使用高可用性的可信執行環境檢索區塊鏈網路的存取資料

【英文發明名稱】

RETRIEVING ACCESS DATA FOR BLOCKCHAIN NETWORKS USING HIGHLY AVAILABLE TRUSTED EXECUTION ENVIRONMENTS

【技術領域】

本發明涉及從外部資料源向區塊鏈網路提供資料。

【先前技術】

分布式帳本系統(DLS)使參與實體能夠安全且永久地儲存資料。在不引用任何特定用例的情況下，DLS也可被稱為共識網路或者區塊鏈網路。區塊鏈網路的示例可以包括為一組選定實體提供的聯盟區塊鏈網路。聯盟區塊鏈網路包括存取控制層。

智慧合約是在區塊鏈網路上執行的程式。智慧合約包含一組預先定義的規則，在所述規則下智慧合約的各方同意彼此互動。在一些情形下，在區塊鏈網路上運行的智慧合約需要來自區塊鏈網路外部的輸入來評估預先定義的規則並執行相應的操作。然而，智慧合約本身不能直接存取

外部資料源。因此，中繼代理可被用來檢索外部資料並將資料提交給區塊鏈網路以由智慧合約進行處理。但是，此處理可能會導致諸如潛在的攻擊向量(例如，分布式拒絕服務(DDoS)攻擊)的安全問題。

儘管為了解決與從外部資料源的資料檢索相關的安全問題已經提出了多種技術，但解決安全問題的更有效方案將是有利的。

【發明內容】

本文描述了用於從外部資料源檢索資料以在區塊鏈網路內進行處理的技術。這些技術通常涉及透過密鑰管理節點向多節點集群中的多個中繼系統節點提供共享的服務私鑰，使得客戶端在透過中繼系統節點從資料源請求資料時可以避免執行中繼系統節點的重複認證。在一些實施例中，對密鑰管理節點執行遠程認證，該遠程認證產生密鑰管理節點的服務密鑰對(服務公鑰，服務私鑰)。服務公鑰在遠程認證期間由客戶端獲得和儲存。密鑰管理節點使用可信執行環境(TEE)操作。密鑰管理節點的遠程認證可以被公開審核，從而消除了單個客戶端重複遠程認證的需要。在一些實施例中，密鑰分發處理由多節點集群中的多個中繼系統節點的密鑰管理節點執行，該密鑰分發處理使相同的服務私鑰分發到每個中繼系統節點。每個客戶端請求由中繼系統智慧合約分配給多節點群集中的可用中繼系統節點以查詢外部資料源。使用服務私鑰對包括查詢結果

的回應進行數位簽名。回應可以由客戶端使用服務公鑰來驗證。

本文還提供了耦接到一個或多個處理器並且其上儲存有指令的一個或多個非暫態電腦可讀儲存媒體，當所述指令由所述一個或多個處理器執行時，促使所述一個或多個處理器執行根據本文提供的方法的實施例的操作。

本文還提供了用於實施本文提供的所述方法的系統。該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電腦可讀儲存媒體，當所述指令由所述一個或多個處理器執行時，促使所述一個或多個處理器執行根據本文提供的方法的實施例的操作。

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

在以下圖式和描述中闡述了本文的一個或多個實施例的細節。根據說明書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]是示出可用於執行本文的實施例的環境的示例的圖示。

[圖2]是示出根據本文的實施例的結構的示例的圖示。

[圖 3]是示出根據本文的實施例的系統的示例的圖示。

[圖 4]是示出根據本文的實施例的系統的示例的圖示。

[圖 5]描繪了根據本文的實施例的信號流的示例。

[圖 6]是示出根據本文的實施例的系統示例的圖示。

[圖 7]描繪了根據本文的實施例的信號流的示例。

[圖 8]是示出根據本文的實施例的系統示例的圖示。

[圖 9]描繪了根據本文的實施例的信號流的示例。

[圖 10]描繪了根據本文的實施例的處理的示例。

[圖 11]描繪了根據本文的實施例的設備的模組的示例。

在不同的圖式中相同的圖式標記和標識表示相同的元件。

【實施方式】

本文描述了用於從外部資料源檢索資料以在區塊鏈網路內進行處理的技術。這些技術通常涉及透過密鑰管理節點向多節點集群中的多個中繼系統節點提供共享的服務私鑰，使得客戶端在透過中繼系統節點從資料源請求資料時，可以避免對中繼系統節點執行重複認證。在一些實施例中，對密鑰管理節點執行遠程認證，該遠程認證產生密鑰管理節點的服務密鑰對(服務公鑰、服務私鑰)。服務公鑰在遠程認證期間由客戶端獲得和儲存。密鑰管理節點使

用可信執行環境(TEE)進行操作。密鑰管理節點的遠程認證可以被公開審核，從而消除了單個客戶端重複遠程認證的需要。在一些實施例中，密鑰分發處理由密鑰管理節點對多節點集群中的多個中繼系統節點執行，密鑰分發處理使相同的服務私鑰被分發到每個中繼系統節點。每個客戶端請求由中繼系統智慧合約分配給多節點群集中的可用中繼系統節點，以查詢外部資料源。使用服務私鑰對包括查詢結果的回應進行數位簽名。該回應可由客戶端使用服務公鑰進行驗證。

如在特定實施例中提供的，本文中所述的主題實現以下技術效果中的一個或多個。在一些實施例中，提供了用於將服務私鑰分配給多個中繼系統節點的密鑰管理節點。如本文所述，可以對密鑰管理節點執行遠程認證，從而消除了針對每個客戶端單獨執行中繼系統節點的遠程認證的需要。這通常緩解了由來自每個客戶端的中繼系統節點的個人認證引起的網路瓶頸。此外，提供了一種用於從多個中繼系統節點中選擇可用中繼系統節點的中繼系統智慧合約。如本文所述，當中繼系統節點被部署在集群中時，中繼系統智慧合約可以將客戶端請求自動分配給集群中的可用中繼系統節點，從而減少由於單個中繼系統節點故障而導致的服務不可用性。因此，本文的實施例提高了用於查詢網際網路資料源的中繼系統節點的整體服務可用性。在一些實施例中，中繼系統智慧合約有助於避免客戶端和中繼系統節點之間的直接接觸，從而避免暴露中繼系統節點

的位置或接入點。因此，中繼系統節點不太可能被網路上的惡意參與者以諸如分布式拒絕服務(DDoS)攻擊的多種形式發現和攻擊。這提高了中繼系統節點的安全性，從而進一步提高了客戶端與中繼系統節點之間通信的安全性。

為本文的實施例提供進一步的背景，如上所述，分布式帳本系統(DLS)，也可稱為共識網路(例如，由對等節點組成)和區塊鏈網路，使參與實體能夠安全且不可篡改地進行交易和儲存資料。儘管術語區塊鏈通常與特定網路和/或用例相關聯，但是在不參考任何特定用例的情況下，本文中使用的區塊鏈通常是指DLS。

區塊鏈是以交易不可篡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。鏈中的每個區塊透過包含在鏈中緊鄰其之前的前一區塊的加密雜湊值(cryptographic hash)鏈接到該前一區塊。每個區塊還包括時間戳、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被編入默克爾(Merkle)樹中。Merkle樹是一種資料結構，在該樹的葉節點處的資料是經雜湊處理的，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。此過程沿著樹持續一直到整個樹的根，在整個樹的根處儲存了代表樹中所有資料的雜湊值。聲稱是儲存在樹中的交易的雜湊值可以透過確定其是否與樹的結構一致而被快速驗證。

然而，區塊鏈是用於儲存交易的去中心化或至少部分

去中心化的資料結構，區塊鏈網路是透過廣播、驗證和認證交易等管理、更新和維護一個或多個區塊鏈的計算節點網路。如上所述，區塊鏈網路可以被提供為公共區塊鏈網路、私有區塊鏈網路或聯盟區塊鏈網路。在本文中，本文的實施例參考聯盟區塊鏈網路進一步詳細描述。然而，可預期的是，本文的實施例可以在任何適當類型的區塊鏈網路中實現。

一般而言，聯盟區塊鏈網路是參與實體之間私有的。在聯盟區塊鏈網路中，共識處理由授權的一組節點控制，所述節點可以稱為共識節點，一個或多個共識節點由各自的實體(例如，金融機構、保險公司)操作。例如，十(10)個實體(例如，金融機構、保險公司)的聯盟可以運行一個聯盟區塊鏈網路，每個實體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，全球區塊鏈被提供為跨所有節點複製的區塊鏈。也就是說，所有共識節點關於全球區塊鏈都處於完美的狀態共識。為了達成共識(例如，同意向區塊鏈添加區塊)，聯盟區塊鏈網路內實施共識協議。例如，聯盟區塊鏈網路可以實施實際拜占庭容錯(PBFT)共識，下面將進一步詳細介紹。

圖1是示出可用於執行本文的實施例的環境100的示例的圖示。在一些示例中，環境100使實體能夠參與聯盟區塊鏈網路102中。環境100包括計算設備106、108和網路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，並連接網站、用戶設備(例如，計算設備)和後端系統。在一些示例中，網路110可以透過有線和/或無線通信鏈路被存取。在一些示例中，網路110能夠與聯盟區塊鏈網路102通信，並在聯盟區塊鏈網路102內通信。通常，網路110表示一個或多個通信網路。在一些情況下，計算設備106、108可以是雲計算系統的節點(未顯示)，或者每個計算設備106、108可以是單獨的雲計算系統，包括透過網路互連並作為分布式處理系統工作的多台電腦。

在所繪出的示例中，計算設備106、108可以包括使其能夠作為聯盟區塊鏈網路102中的節點參與的任何適當計算系統。計算系統的示例包括但不限於伺服器、桌上型電腦、筆記型電腦、平板電腦和智慧手機。在一些示例中，計算設備106、108承載用於與聯盟區塊鏈網路102互動的一個或多個電腦實現服務。例如，計算設備106可以承載第一實體(例如，用戶A)的電腦實現服務，諸如第一實體用於管理其與一個或多個其他實體(例如，其他用戶)的交易的交易管理系統。計算設備108可以承載第二實體(例如，用戶B)的電腦實現服務，諸如第二實體用於管理其與一個或多個其他實體(例如，其他用戶)的交易的交易管理系統。在圖1的示例中，聯盟區塊鏈網路102表示為節點的對等網路，計算設備106、108分別提供參與聯盟區塊鏈網路102中的第一實體和第二實體的節點。

圖2是示出根據本文的實施例的結構200的示例的圖

示。概念結構200包括分別對應於參與者A、參與者B和參與者C的參與者系統202、204、206。每個參與者(例如，用戶、企業)參與作為包括多個節點214的對等網路提供的區塊鏈網路212，其中至少一些節點在區塊鏈216中永久記錄資訊。儘管示意性地描繪了單個區塊鏈216在區塊鏈網路212中，但區塊鏈216的多個副本被提供並在整個區塊鏈網路212中維護，如本文中進一步詳細描述的。

在所描述的示例中，每個參與者系統202、204、206分別由參與者A、參與者B和參與者C提供，或代表參與者A、參與者B和參與者C，並作為區塊鏈網路中的各個節點214工作。如本文中所使用的，節點通常指連接到區塊鏈網路212並使各自參與者能夠參與到區塊鏈網路中的單個系統(例如，電腦、伺服器)。在圖2的示例中，參與者對應於每個節點214。然而，可以預期的是，參與者可以在區塊鏈網路212內操作多個節點214，和/或多個參與者可以共享一個節點214。在一些示例中，參與者系統202、204、206使用協議(例如，超文本傳輸協議安全(HTTPS))和/或使用遠程進程調用(RPCs)與區塊鏈網路212通信或透過區塊鏈網路212通信。

節點214在區塊鏈網路212內可以有不同程度的參與。例如，一些節點214可以參與共識處理(例如，作為向區塊鏈216添加區塊的礦工節點)，而其他節點214不參與共識處理。作為另一示例，一些節點214儲存區塊鏈216的完整副本，而其他節點214只儲存區塊鏈216的部分副本。例

如，資料存取特權可以限制各參與者在其各自系統內儲存的區塊鏈資料。在圖2的示例中，參與者系統202、204分別儲存區塊鏈216的完整副本216’、216”。

區塊鏈(例如，圖2的區塊鏈216)由區塊的鏈組成，每個區塊儲存資料。資料的示例包括代表兩個或更多個參與者之間的交易的交易資料。雖然本文中以非限制性示例的方式使用交易，但可以預期的是，任何適當的資料都可以儲存在區塊鏈中(例如，文檔、圖像、視訊、音訊)。交易的示例可以包括但不限於交換有價值的東西(例如，資產、產品、服務、貨幣)。交易資料不變地儲存在區塊鏈內。也就是說，交易資料不能更改。

在儲存到區塊中之前，交易資料被雜湊處理。雜湊處理是將交易資料(作為字符串資料提供的)轉換為固定長度雜湊值(也作為字符串資料提供的)的過程。無法逆雜湊處理雜湊值以獲得交易資料。雜湊處理確保即使交易資料中的微小變化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，不管交易資料的大小，雜湊值的長度都是固定的。雜湊處理包括透過雜湊函數處理交易資料以產生雜湊值。雜湊函數的示例包括但不限於安全雜湊演算法(SHA-256)，其輸出256位雜湊值。

多筆交易的交易資料經雜湊處理並儲存在區塊中。例如，兩筆交易的雜湊值被提供並其本身經雜湊處理以提供另一雜湊值。此過程重複進行，直到為要儲存在區塊中的所有交易提供單個雜湊值為止。這個雜湊值被稱為merkle

根雜湊值並儲存在區塊頭中。任何交易的改變都將導致其雜湊值的改變，並最終導致merkle根雜湊值的改變。

區塊透過共識協議添加到區塊鏈。區塊鏈網路中的多個節點參與到共識協議中並執行工作以將區塊添加到區塊鏈。這些節點被稱為共識節點。上文介紹的PBFT被用作共識協議的非限制性示例。共識節點執行共識協議以向區塊鏈添加交易並更新區塊鏈網路的整體狀態。

更詳細地，共識節點產生區塊頭，雜湊處理區塊中的所有交易，並成對組合雜湊值以產生進一步的雜湊值，直到為區塊中的所有交易(Merkle根雜湊值)提供單個雜湊值。此雜湊值被添加到區塊頭。共識節點還確定區塊鏈中最新區塊的雜湊值(即，添加到區塊鏈的最後區塊)。共識節點還向區塊頭添加隨機值(nonce value)和時間戳。

通常，PBFT提供實際拜占庭狀態機複製，其容許拜占庭錯誤(例如，故障節點、惡意節點)。這在PBFT中是透過假設故障會發生來實現的(例如，假設存在獨立節點故障，和/或由共識節點發送的操縱消息)。在PBFT中，共識節點按照包括主共識節點和備份共識節點的順序來提供。主共識節點周期性改變。交易透過區塊鏈內的所有共識節點就區塊鏈網路的世界狀態達成一致來添加到區塊鏈。在這個過程中，消息在共識節點之間傳輸，每個共識節點證明消息是從指定的對等節點接收，並驗證消息在傳輸過程中沒有被修改。

在PBFT中，共識協議分多個階段提供，所有共識節

點都從同一狀態開始。首先，客戶端向主共識節點發送請求以調用服務操作(例如，在區塊鏈網路內執行交易)。為了回應接收請求，主共識節點將請求多播到備份共識節點。備份共識節點執行請求，每個節點都向客戶端發送回復。客戶端等待，直到接收到閾值數量的回復。在一些示例中，客戶端等待接收f+1回復，其中f是區塊鏈網路內可以容許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就要添加到區塊鏈的記錄的順序達成一致，記錄或者被接受，或者被拒絕。

在一些區塊鏈網路中，實施加密以維護交易的私密性。例如，如果兩個節點想要保持交易私密，使得區塊鏈網路中的其他節點不能識別該交易的細節，則所述節點可以對該交易資料進行加密。密碼術的示例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密鑰進行加密(從明文產生密文)和解密(從密文產生明文)的加密處理。在對稱加密中，同一密鑰可用於多個節點，因此每個節點都可以加密/解密交易資料。

非對稱加密使用密鑰對，每個密鑰對包括私鑰和公鑰，私鑰僅為各自節點所知，公鑰為區塊鏈網路中的任何或所有其他節點所知。一個節點可以使用另一節點的公鑰對資料進行加密，而加密的資料可以使用另一節點的私鑰進行解密。例如，再次參考圖2，參與者A可以使用參與者B的公鑰對資料進行加密，並將加密的資料發送給參與者B。參與者B可以使用其私鑰對加密的資料(密文)進行解

密，並提取原始資料(明文)。使用某一節點的公鑰加密的消息只能使用該節點的私鑰進行解密。

非對稱加密被用於提供數位簽名，其使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，某一節點可以對一條消息進行數位簽名，另一節點可以基於參與者A的數位簽名來確認該消息是由該節點發送。數位簽名還可以被用於確保消息在傳輸中沒有被篡改。例如，再次參考圖2，參與者A將向參與者B發送消息。參與者A產生該消息的雜湊值，然後使用其私鑰對該雜湊值進行加密以提供作為加密雜湊值的數位簽名。參與者A將數位簽名附加到消息上，並將帶有數位簽名的消息發送給參與者B。參與者B使用參與者A的公鑰對數位簽名進行解密，並提取雜湊值。參與者B對消息進行雜湊處理並比較雜湊值。如果雜湊值相同，參與者B可以確認消息確實來自參與者A，並且沒有被篡改。

在一些實施例中，區塊鏈網路的節點和/或與區塊鏈網路通信的節點可以使用TEE來操作。在高層，TEE是硬體(一個或多個處理器、記憶體)中與硬體的操作環境(例如，操作系統(OS)、基本輸入/輸出系統(BIOS))隔離的可信環境。更詳細地，TEE是處理器的獨立、安全的區域(其確保碼執行以及主處理器中加載的資料的機密性和完整性)。在處理器中，TEE和OS並行運行。至少部分所謂的可信應用程式(TA)在TEE內執行，並且可以存取處理器和記憶體。透過TEE，TA被保護不受主OS中運行的其他應

用程式影響。此外，TEE以加密方式將TEE內的TA彼此隔離。

TEE的示例包括由美國加利福尼亞州聖克拉拉的英特爾公司提供的軟體保護擴展(SGX)。儘管本文以示例的方式討論了SGX，但可以預期的是，可以使用任何適合的TEE來實現本文的實施例。

SGX提供基於硬體的TEE。在SGX中，可信硬體是中央處理器(CPU)的死區，物理記憶體的一部分被隔離以保護選擇的碼和資料。記憶體的隔離部分被稱為圍圈(enclave)。更具體地，在記憶體中圍圈作為圍圈頁面緩存(EPC)被提供，並映射到應用程式位址空間。記憶體(例如，DRAM)包括用於SGX的保留隨機記憶體(PRM)。PRM是最低BIOS級別的連續記憶體空間並且不能被任何軟體存取。每個EPC是由OS分配以在PRM中加載應用程式資料和碼的記憶體集(例如，4KB)。EPC元資料(EPCM)是各個EPC的入口位址，並且確保每個EPC只能由一個圍圈共享。也就是說，單個圍圈可以使用多個EPC，而EPC專用於單個圍圈。

在TA的執行期間，處理器在存取圍圈中儲存的資料時以所謂的圍圈模式操作。圍圈模式下的操作對每個記憶體存取強制執行額外的硬體檢查。在SGX中，TA被編譯為可信部分和不可信部分。可信部分是透過例如OS、BIOS、特權系統碼、虛擬機管理器(VMM)、系統管理模式(SMM)等等不可存取的。在操作中，TA運行並在記憶體的PRM

內創建圍圈。由圍圈內的可信部分執行的可信函數被不可信部分調用，在圍圈內執行的碼將資料視為明文資料(未加密)，並且拒絕對資料的外部存取。可信部分提供對調用的加密回應，TA繼續執行。

認證處理可被執行以驗證預期碼(例如，TA的可信部分)在提供SGX的TEE內安全執行。通常，認證處理包括TA接收來自質詢者(例如，區塊鏈網路中的另一節點，或區塊鏈網路的密鑰管理系統(KMS))的認證請求。作為回應，TA要求其圍圈產生遠程認證，也稱為引用(quote)。產生遠程認證包括將本地認證從圍圈發送到所謂的引用圍圈，其驗證本地認證並且透過使用非對稱認證密鑰對本地認證進行簽名而將本地認證轉換為遠程認證。遠程認證(引用)被提供給質詢者(例如，區塊鏈網路的KMS)。

質詢者使用認證驗證服務來驗證遠程認證。對於SGX，Intel提供Intel認證服務(IAS)，其接收來自質詢者的遠程認證並驗證遠程認證。更具體地，IAS處理遠程認證並提供指示遠程認證是否經驗證的報告(例如，認證驗證報告(AVR))。如果未經驗證，則可以指示錯誤。如果經過驗證(預期碼在TEE中安全地執行)，則質詢者可以啓動或繼續與TA互動。例如，為了回應驗證，KMS(作為質詢者)可以向執行TEE的節點(例如，透過密鑰交換處理，例如橢圓曲線Diffie-Hellman(ECDH))發布非對稱加密密鑰(例如，公鑰和私鑰對)，以使節點能夠與其他節點和/或客戶端安全通信。

在一些區塊鏈網路中，可以執行所謂的智慧合約。智慧合約可以被描述為具有影響各方的合約條款的現實世界法律合約的數字表示。在示例背景下，智慧合約在聯盟區塊鏈網路內被實施、儲存、更新(根據需要)和執行。與智慧合約相關的合約方(例如，買方和賣方)被表示為聯盟區塊鏈網路中的節點。在一些示例中，合約方可以包括與智慧合約相關(例如，作為智慧合約的當事方)的實體(例如，企業)。

更詳細地，智慧合約作為在區塊鏈上執行的電腦可執行程式(例如，區塊鏈網路內的節點)提供。智慧合約包含一組預先定義的規則，在所述規則下智慧合約的各方同意彼此互動。如果智慧合約的預定義規則被滿足，則智慧合約中定義的協議被自動執行。智慧合約通常是防篡改的，並且促進、驗證和執行協議或交易的談判或履行。

在一些情況下，在區塊鏈網路內執行的智慧合約需要來自區塊鏈網路外部的輸入來評估預先定義的規則並執行相應的操作。透過非限制性示例的方式，智慧合約可能需要股票報價，以便基於來自區塊鏈網路外部資料源的股票報價做出決定。作為另一非限制性示例，智慧合約可能需要位於區塊鏈網路外部維護的帳號的帳號資訊以便基於該帳號資訊做出決定。但是，智慧合約本身可能無法直接查詢外部資料源。

在一些實施例中，中繼代理可以被用來檢索外部資料，並將資料提交給區塊鏈以由智慧合約進行處理。但

是，此處理可能導致諸如安全資訊洩漏(例如，存取外部資料源可能需要的憑據)的安全問題。在一些情況下，TEE可以被用來證明中繼代理已經誠實地執行了指定的查詢請求。然而，由於區塊鏈的開放性，所有查詢請求對區塊鏈網路中的所有用戶(節點)都是可見的。因此，存在請求字符串可被截取、修改和重放的風險，從而導致資訊洩漏和其他安全問題。

在一些情況下，SGX、TA或TA的一部分可用作中繼節點在圍圈(圍圈程式)中執行以存取外部資料源。例如，圍圈程式可以向基於網際網路的資料源發送查詢請求(例如，HTTPS請求)，並可以對發起請求的智慧合約提供回應。在一些示例中，提供了隱私字段功能，其可用於使用圍圈的公鑰對敏感資訊(例如，存取憑據)進行加密。在一些示例中，中繼節點使用圍圈的私鑰對隱私字段進行解密，調用HTTPS客戶端存取基於網際網路的目標資料源，接收請求的資料，並使用私鑰對返回的資料進行數位簽名。在數位簽名後，資料返回到啓動所述請求的智慧合約。

在一些示例中，實施圍圈程式的中繼系統節點在遠程認證處理期間被驗證。每個客戶端請求都可以由經驗證的中繼系統節點處理，以從資料源檢索資料。

然而，這種方法可能具有缺點。使用特定中繼系統節點進行資料檢索的示例性缺點是，如果中繼系統節點出現故障或無法存取，則客戶端請求不能被正確處理，從而導

致服務不可用性。

在一些實施例中，外部資料源(例如，基於網際網路的資料源)可以由共享服務私鑰和TEE的多個中繼系統節點中的任一個來查詢。因此，每個客戶端不必單獨地執行中繼系統節點的遠程認證，從而減輕了由從每個客戶端對中繼系統節點的個人認證所造成的網路瓶頸，並減少了伺服器或電腦用於處理認證的工作量。此外，中繼系統節點可以被部署在集群中，每個客戶端請求可被自動分配到集群中的可用中繼系統節點。透過這種方式，可以提高服務可用性，因為單個中繼系統節點故障不會導致服務不可用性。

圖3是示出根據本文的實施例的系統300的示例的圖示。如所示，系統300包括區塊鏈302、形成多節點集群的多個中繼系統節點308、密鑰管理節點310、網路312(例如，網際網路)和客戶端314(例如，客戶端計算設備)。在所描述的示例中，區塊鏈302包括客戶端智慧合約304和中繼系統智慧合約306。在一些實施例中，中繼系統節點308和密鑰管理節點310使用TEE技術(例如，Intel SGX)來實現。通常，中繼系統智慧合約306、中繼系統節點308和中繼管理節點310提供使區塊鏈302外部的資料能夠被從網際網路資料源314檢索並被用於區塊鏈302內的中繼系統。

客戶端智慧合約304是從網路312上的資料源請求資料或服務的智慧合約。中繼系統智慧合約306是中繼系統內充當區塊鏈302的前端的智慧合約。中繼系統智慧合約306

實現客戶端智慧合約304的應用程式介面(API)，用於處理資料以及將資料從客戶端智慧合約304中繼到中繼系統的其他組件(例如，中繼系統節點308)，反之亦然。

中繼系統節點308可在任何適合的伺服器、電腦、模組或計算元件上實現，以回應來自區塊鏈302的資料請求，從網路312中的外部資料源檢索資料。例如，中繼系統節點308可以接收和處理來自客戶端智慧合約304的鏈外資料或服務請求，並查詢網路312中的外部資料源，例如，啓用HTTPS的網際網路服務。

密鑰管理節點310可以在任何適合的伺服器、電腦、模組或計算元件上實現，以用於管理用於從外部資料源檢索資料的加密密鑰。如本文所討論的，加密密鑰包括由密鑰管理節點310產生的服務公鑰和服務私鑰，其中服務私鑰可用於對請求結果進行簽名，服務公鑰可用於對請求結果進行認證。

通常，資料檢索處理可以包括三個階段。第一階段包括遠程認證處理，其中客戶端314對密鑰管理節點310進行認證，並獲得密鑰管理節點310的認證密鑰(例如，服務公鑰)。在第二階段，密鑰管理節點310將簽名密鑰(例如，服務私鑰)分配給多節點集群中的每個中繼系統節點308，使得所有中繼系統節點308共享相同的簽名密鑰。第三階段包括資料請求處理，其中客戶端314透過中繼系統從外部資料源獲得授權資料。在第三階段，資料由中繼系統節點308透過中繼系統獲得，中繼系統節點308查詢網路312

並使用其服務私鑰對請求結果進行簽名，客戶端314可以使用其服務公鑰對請求結果進行認證。三個階段將在下面參考圖4-10進一步詳細討論。

圖4是示出根據本文的實施例的系統400的示例的圖示。如所示，系統400包括開發者402(例如，開發者伺服器)、客戶端404(例如，客戶端計算設備)、密鑰管理節點406、認證服務408和網路410(例如，網際網路)。客戶端404、密鑰管理節點406和網際網路410可以分別是與如圖3中所示的客戶端314、密鑰管理節點310和網路312相同的組件。客戶端404可以質詢密鑰管理節點406，以獲得認證證據420，認證證據420可由認證服務408驗證以確定密鑰管理節點406的合法性。認證服務408的示例包括上文所述的IAS。

開發者402可以是被程式化為執行本文所述的方法的任何適合的伺服器、電腦、模組或計算元件。在一些示例中，開發者402可以儲存和處理與密鑰管理節點406相關的程式和/或資料。例如，開發者402可以儲存密鑰管理節點406的源碼和測量值(例如，初始狀態的摘要)。開發者402可以根據請求將密鑰管理節點406的測量值發送給客戶端404。

對於指示密鑰管理節點406的合法性的認證證據420，客戶端404可以向密鑰管理節點406發送請求(質詢)。在一些示例中，認證證據420被用於確定密鑰管理節點406是否是合法的TEE節點。客戶端404可以向認證服務408提供認

證證據420，並從認證服務408接收認證驗證報告(AVR)430。在一些實施例中，客戶端404驗證AVR 430以確定認證證據420是否有效。在一些示例中，客戶端404從密鑰管理節點406獲得測量值422，並將其與從開發者402獲得的另一測量值422進行比較。如果對AVR 430的驗證成功並且兩個測量值422匹配，客戶端404可以確定密鑰管理節點406是合法的TEE節點，因此是值得信賴的。

密鑰管理節點406可以根據來自客戶端404的請求產生認證證據420。在一些實施例中，密鑰管理節點406配置有可被客戶端404用於未來通信的認證和加密的服務公鑰424和服務私鑰。在一些實施例中，密鑰管理節點406進一步設置有認證私鑰，例如增強隱私ID(EPID)私鑰，用於對認證證據420進行簽名。使用EPID私鑰簽名的認證證據420可由認證服務408使用EPID公鑰進行驗證。EPID是由Intel提供的用於可信系統認證同時保護隱私的演算法。通常，網路的每個成員(例如，電腦或伺服器)都被分配用於對認證證據進行簽名的EPID私鑰，網路中的認證證據的驗證方儲存與網路的其他成員的EPID私鑰配對的EPID公鑰。每個成員都可以使用其自己的EPID私鑰產生認證證據的簽名，驗證方可以使用EPID公鑰驗證其他成員的簽名。因此，EPID密鑰可用於證明諸如電腦或伺服器的設備是可信賴的設備。

在一些示例中，認證證據420指示密鑰管理節點406的合法性(例如，密鑰管理節點406是否是值得信賴的實

體)，並包括測量值422(例如，摘要)、服務公鑰424和密鑰管理節點406的數位簽名426。測量值422可以包括密鑰管理節點406的初始狀態的摘要(例如，雜湊值)。服務公鑰424可由密鑰管理節點406和服務私鑰使用預定的密鑰產生演算法(例如，Rivest-Shamir-Adleman(RSA))隨機產生。簽名426是基於測量值422和服務公鑰424使用密鑰管理節點406的認證私鑰(例如，EPID私鑰)產生的。

認證服務408可在任何適合的伺服器、電腦、模組或計算元件上實施，以驗證認證證據420的有效性。如上所述，認證證據420包括測量值422、服務公鑰424和密鑰管理節點406的簽名426。在接收到認證證據420時，認證服務408可以驗證簽名426並產生AVR 430。

在一些示例中，認證服務408可以使用認證公鑰(例如，EPID公鑰)驗證認證證據420中的簽名426。在驗證簽名426後，認證服務408可以產生包括認證證據420的AVR 430、指示認證證據420中的簽名426是否有效的驗證結果434和認證服務408的簽名436。

在一些實施例中，AVR 430包括將密鑰管理節點406的簽名426排除在外的認證證據420。例如，AVR 430可以包括密鑰管理節點406的測量值422、服務公鑰424、驗證結果434和簽名436。在一些示例中，簽名436是使用報告簽名密鑰(例如，私鑰)基於認證證據420和驗證結果434產生的。

在操作中，客戶端404從開發者402獲得密鑰管理節點

406的測量值422。客戶端404查詢(質詢)密鑰管理節點406，接收認證證據420，並將認證證據420發送至認證服務408。認證服務408驗證認證證據420並將AVR 430發送至客戶端404。客戶端404基於AVR 430中的簽名436和測量值422驗證AVR 430。在成功驗證AVR 430時，客戶端404確定密鑰管理節點406是值得信賴的實體，並登記(例如，儲存)密鑰管理節點406的服務公鑰424。下文將參考圖5詳細討論對認證證據420和AVR 430的驗證。

圖5繪出根據本文的實施例的信號流500的示例。信號流500表示密鑰管理節點(例如，密鑰管理節點406)的認證驗證處理。為方便起見，該處理將被描述為由位於一個或多個位置並根據本文適當程式化的一台或多台電腦的系統執行。例如，適當程式化的分布式系統(圖4中的系統400)可以執行該處理。

在圖5的示例中，開發者402根據來自客戶端404的請求將密鑰管理節點406的測量值422發送(502)至客戶端404。例如，客戶端404可以將針對密鑰管理節點406的測量值422的請求發送至開發者伺服器402。在驗證客戶端404的身分後，開發者伺服器402可以將請求的測量值422發送至客戶端404。客戶端404儲存密鑰管理節點406的測量值422以供將來使用。

客戶端404將認證請求(例如，質詢)發送(504)至密鑰管理節點406。認證請求被發送到密鑰管理節點406，以請求可用於確定密鑰管理節點406的合法性的認證證據420。

回應於認證請求，密鑰管理節點406產生(506)認證證據420。在一些示例中，認證證據420包括測量值422、服務公鑰424和密鑰管理節點406的數位簽名426。在一些實施例中，測量值422可以包括密鑰管理節點406的初始狀態的摘要。例如，測量值422可以包括在密鑰管理節點406上實現的進程碼的雜湊值。服務公鑰424可以由密鑰管理節點406連同服務私鑰一起使用預定的密鑰產生演算法(例如，RSA)隨機產生。簽名426可以是使用密鑰管理節點406的認證私鑰(例如，EPID私鑰)基於測量值422和服務公鑰424產生的。

密鑰管理節點406回應於認證請求將認證證據420發送(508)至客戶端404。客戶端404將認證證據420轉發給認證服務408。在一些實施例中，客戶端404將認證驗證請求發送至認證服務408。認證驗證請求可以包括密鑰管理節點406的認證證據420和一些補充資訊，例如，指示密鑰管理節點406是否使用SGX平臺服務的描述符。

認證服務408，回應於從客戶端404接收認證證據420，驗證(512)認證證據420。如所述，認證證據420包括測量值422、服務公鑰424和密鑰管理節點406的簽名426。如所述，簽名426可以是使用密鑰管理節點406的認證私鑰(例如，EPID私鑰)基於測量值422和服務公鑰424產生的。在一些示例中，認證服務408被提供有可用於驗證認證證據420中的簽名426的認證公鑰(例如，EPID公鑰)。

如果認證服務408確定認證證據420中的簽名426有

效，認證服務408可以確定密鑰管理節點406是可信實體。如果認證服務408確定簽名426無效，則認證服務408可以確定密鑰管理節點406不是可信實體，並且可以標記錯誤並拒絕來自密鑰管理節點406的任何後續資料和請求。

認證服務408基於認證證據420的驗證產生(514)AVR 430。在一些實施例中，AVR 430可以包括認證證據420、認證驗證結果434和認證服務408的數位簽名436。在一些實施例中，AVR 430可以包括將密鑰管理節點406的簽名426排除在外的認證證據420。例如，AVR 430可以包括測量值422、服務公鑰424、認證驗證結果434和認證服務408的簽名436。

AVR 430中的認證驗證結果434指示認證證據420中的簽名426是否有效。例如，認證驗證結果430可包括指示認證證據420中的簽名426有效的值“valid”或“OK”，或者表示簽名426無效的值“invalid”。

在一些實施例中，AVR 430中的簽名436是使用報告簽名密鑰基於認證證據420和認證驗證結果434產生的。報告簽名密鑰可以是認證服務408用於對AVR 430進行簽名的私鑰。在一些示例中，報告簽名密鑰由認證服務408使用預定的密鑰產生演算法而產生。例如，報告簽名密鑰可以使用RSA安全雜湊演算法(SHA)256產生。

認證服務408將AVR 430發送(516)至客戶端404。在一些實施例中，客戶端404在接收到AVR 430時驗證(518)AVR 430。在一些示例中，客戶端404可以使用報告簽名證書驗

證AVR 430中的簽名436。報告簽名證書可以是X.509數位證書。如果客戶端404驗證AVR 430中的簽名436有效，客戶端404可以確定AVR 430確實是由認證服務408發送的。如果客戶端404確定AVR 430中的簽名436無效，則客戶端404可以確定AVR 430不是可信的，並且可以拒絕AVR 430。客戶端404可以進一步檢查AVR 430中的認證驗證結果434，以確定認證證據420是否被認證服務408成功驗證。

在一些實施例中，客戶端404將AVR 430中認證證據420中的測量值422與先前從開發者402獲得的測量值422進行比較，以確定認證證據420是否有效。

回應於確定AVR 430是可信的，客戶端404將密鑰管理節點406註冊為可信實體。例如，如果AVR 430中的測量值422與先前從開發者伺服器402獲得的測量值422匹配，驗證結果434表明簽名426有效、簽名436被驗證有效、或者其組合，則客戶端404可以認為密鑰管理節點406是可信的。客戶端404可以進一步儲存在AVR 430的認證證據420中包括的服務公鑰424。

圖6是示出根據本文的實施例的系統600的示例的圖示。如所示，系統600包括管理員602(例如，管理計算設備)、密鑰管理節點604、多個中繼系統節點606、認證服務608和網路610(例如，網際網路)。通常，密鑰管理節點604針對中繼系統節點606的認證證據質詢每個中繼系統節點606，該認證證據可以由認證服務608就中繼系統節點

606的合法性進行驗證。在成功驗證中繼系統節點606時，密鑰管理節點604可以將簽名密鑰(例如，服務私鑰)發送至每個中繼系統節點606，使得所有中繼系統節點606共享相同的簽名密鑰。

管理員602可以在任何適合的伺服器、電腦、模組或計算元件上實現，以執行本文討論的演算法。在一些示例中，管理員602查詢密鑰管理節點604以驗證中繼系統節點606。在一些示例中，管理員602向密鑰管理節點604發送包括要驗證的中繼系統節點606的網路位址(例如，URL)的請求。

密鑰管理節點604可以針對認證證據質詢中繼系統節點606，並將認證證據發送至認證服務608，以驗證認證證據是否有效。在一些示例中，密鑰管理節點604接收來自管理員602的請求，其包括要驗證的中繼系統節點606的URL。密鑰管理節點604可以使用中繼系統節點606的URL針對認證證據查詢中繼系統節點604。在一些示例中，密鑰管理節點604接收來自中繼系統節點606的認證證據，其包括測量值、公鑰和中繼系統節點606的簽名。密鑰管理節點604可以將中繼系統節點606的認證證據發送至認證服務608，以驗證認證證據是否有效。密鑰管理節點604可以接收來自認證服務608的AVR，該AVR包括認證證據、認證證據的認證驗證結果和認證服務608的簽名。密鑰管理節點604可以基於認證證據中的測量值、驗證結果和認證服務608的簽名驗證AVR。例如，密鑰管理節點604可以將

AVR中認證證據中的中繼系統節點606的測量值與預儲存在密鑰管理節點604中的另一測量值進行比較，以查看它們是否匹配。密鑰管理值604可以檢查認證驗證結果，以查看認證證據是否被認證服務608成功驗證。密鑰管理值604可以驗證認證服務608的簽名，以確定AVR是否確實由認證服務608發送。在一些示例中，如果密鑰管理節點604確定AVR中認證證據中的中繼系統節點606的測量值與預儲存在密鑰管理節點604中的另一測量值相匹配，並且認證驗證結果表明認證證據有效、認證服務608的簽名有效、或者其組合，則密鑰管理節點604可以確定AVR有效。

密鑰管理節點604在驗證AVR有效後可以獲得並儲存AVR中的認證證據中包括的中繼系統節點606的公鑰。密鑰管理節點604可以進一步使用中繼系統節點606的公鑰對其服務私鑰進行加密，並將加密的服務私鑰發送至中繼系統節點606。在密鑰管理節點604將其服務私鑰分配給多個中繼系統節點606的一些示例中，密鑰管理節點604可以使用每個中繼系統節點的相應公鑰對其服務私鑰進行加密。

中繼系統節點606可以對來自密鑰管理節點604的加密的服務私鑰進行解密，並獲得密鑰管理節點604的服務私鑰。例如，每個中繼系統節點606可以使用其各自的私鑰獲得使用中繼系統節點606的公鑰加密的服務私鑰。中繼系統節點606儲存密鑰管理節點604的服務私鑰以供將來使用。如所述，多個中繼系統節點606共享密鑰管理節點604

的同一服務私鑰。

認證服務608可以驗證中繼系統節點606的認證證據是否有效。如所述，中繼系統節點606的認證證據包括測量值、公鑰和中繼系統節點606的簽名。在一些示例中，中繼系統節點606的簽名使用中繼系統節點606的認證私鑰(例如，EPID私鑰)產生。認證服務608可以使用認證公鑰(例如，EPID公鑰)驗證中繼系統節點606的簽名，並基於簽名的驗證確定認證證據是否有效。在驗證認證證據時，認證服務608可以將AVR發送至密鑰管理節點604。如所述，AVR可以包括認證證據、認證證據的認證驗證結果和認證服務608的簽名。

在操作中，管理員602將待驗證的中繼系統節點606的網路位址發送至密鑰管理節點604。密鑰管理節點604使用該網路位址向中繼系統節點606發起遠程認證請求。中繼系統節點606隨機產生包括公鑰和私鑰的密鑰對，並將公鑰包括在返回給密鑰管理節點604的認證證據中。密鑰管理節點604將中繼系統節點606的認證證據提交至認證服務608，以驗證認證證據的有效性。認證服務608驗證來自密鑰管理節點604的認證證據，並返回AVR。密鑰管理節點604驗證AVR以確定中繼系統節點606是否為合法的TEE節點。在一些示例中，密鑰管理節點604確定AVR中認證證據中包括的測量值是否與預期的測量值一致。在成功驗證AVR時，密鑰管理節點604使用認證證據中包括的中繼系統節點606的公鑰對其服務私鑰進行加密。密鑰管理節點

604將加密的服務私鑰發送到中繼系統節點606。在從密鑰管理節點接收到加密的服務私鑰時，中繼系統節點606使用其私鑰獲得服務私鑰。因此，密鑰管理節點604可以將其服務私鑰分發給經驗證合法的中繼系統節點606。下面將參考圖7更詳細地討論服務私鑰的分發。

圖7描繪了根據本文的實施例的信號流700的示例。信號流700表示簽名密鑰(例如，服務私鑰)分發處理。為方便起見，該處理將被描述為由位於一個或多個位置並根據本文適當程式化的一台或多台電腦的系統執行。例如，適當程式化的分發系統(圖6中的系統600)可以執行該處理。

在圖7的示例中，管理員602向密鑰管理節點604發送(702)請求，以確定中繼系統節點606是否為合法的TEE節點。在一些示例中，該請求包括待驗證的中繼系統節點606的網路位址(例如，URL)。

密鑰管理節點604使用該網路位址向中繼系統節點606發送(704)遠程認證請求。在一些示例中，針對指示中繼系統節點606的合法性的認證證據的遠程認證請求被發送到中繼系統節點606。認證證據可以包括測量值(例如，初始狀態的雜湊值)、公鑰和待驗證的中繼系統節點606的簽名。

回應於認證請求，中繼系統節點606產生(706)認證證據。如所述，認證證據包括測量值、公鑰和中繼系統節點606的數位簽名。在一些實施例中，測量值可以包括中繼系統節點606的初始狀態的摘要。例如，測量值可以包括

在中繼系統節點606上實現的處理碼的雜湊值。公鑰可以使用預定的密鑰產生演算法(例如，RSA)由中繼系統節點606連同私鑰一起隨機被產生。簽名可以使用中繼系統節點606的認證私鑰(例如，EPID私鑰)基於測量值和公鑰被產生。

回應於認證請求，中繼系統節點606將認證證據發送(708)至密鑰管理節點604。密鑰管理節點604將認證證據轉發(710)至認證服務608。在一些實施例中，密鑰管理節點604向認證服務608發送認證驗證請求。認證驗證請求可以包括中繼系統節點606的認證證據和一些補充資訊，例如，指示中繼系統節點606是否使用SGX平臺服務的描述符。

認證服務608驗證(712)認證證據。如所述，認證證據包括測量值、公鑰和中繼系統節點606的簽名。簽名是使用中繼系統節點606的認證私鑰(EPID私鑰)基於測量值和公鑰產生的。在一些示例中，認證服務608被提供有可用於驗證認證證據中的簽名的認證公鑰(EPID公鑰)。

如果認證服務608確定認證證據中的簽名有效，認證服務608可以確定中繼系統節點606是可信實體。如果認證服務608確定簽名無效，認證服務608可以確定中繼系統節點606不是可信實體，並且可以標記錯誤並拒絕來自中繼系統節點606的任何後續資料和請求。

認證服務608基於認證證據的驗證而產生(714)AVR。在一些實施例中，AVR可以包括認證證據、認證驗證結果

和認證服務608的數位簽名。在一些實施例中，AVR可以包括將中繼系統節點606的簽名排除在外的認證證據。在一些示例中，AVR的簽名是使用報告簽名密鑰(私鑰)基於證明證據和認證驗證結果產生的。

認證服務608向密鑰管理節點604發送(716)AVR。在一些實施例中，密鑰管理節點604驗證(718)來自認證服務608的AVR。在一些示例中，密鑰管理節點604使用報告簽名證書(公鑰)驗證AVR的簽名。在一些實施例中，密鑰管理節點604將認證證據中的測量值與預儲存在密鑰管理節點604中的另一測量值進行比較，以確定認證證據是否有效。在成功驗證AVR和測量值時，密鑰管理節點604儲存中繼系統節點606的公鑰。

密鑰管理節點604使用中繼系統節點606的公鑰對其服務私鑰進行加密(720)，並將加密的服務私鑰發送(722)至中繼系統節點606。

在從密鑰管理節點604接收到加密的服務私鑰時，中繼系統節點606使用其私鑰獲得密鑰管理節點的服務私鑰(724)。中繼系統節點606可以儲存服務私鑰以供將來使用。

圖8是示出根據本文的實施例的系統800的示例的圖示。如所示，系統800包括客戶端802(例如，客戶端計算設備)、區塊鏈804、形成多節點集群的多個中繼系統節點810和網路812(例如，網際網路)。在所描述的示例中，區塊鏈804包括客戶端智慧合約806和中繼系統智慧合約

808。在一些實施例中，中繼系統節點810使用TEE技術(例如，Intel SGX)實現。

通常，客戶端802請求來自網路812中的資料源的資料，並透過區塊鏈804和中繼系統節點810接收從資料源檢索到的資料，使得請求和檢索到的資料的完整性可以被驗證。

在操作中，客戶端802構建包括明文部分和機密資料部分的請求，其中機密資料部分由客戶端802使用先前從密鑰管理節點(例如，密鑰管理節點406和604)獲得的服務公鑰加密。客戶端802將請求提交至區塊鏈804內的客戶端智慧合約806。客戶端智慧合約806將請求轉發至中繼系統智慧合約808。中繼系統智慧合約806將請求轉發至多節點集群中的中繼系統節點810。在一些示例中，中繼系統智慧合約808隨機選擇可用的中繼系統節點810。在一些示例中，中繼系統智慧合約808透過日誌消息發送請求。中繼系統節點810接收請求，並使用先前從密鑰管理節點獲得的服務私鑰獲得機密資料部分。中繼系統節點810將明文部分和機密資料部分組合成資料請求。中繼系統節點810隨後將資料請求提交給網際網路資料源812。中繼系統節點810接收來自網際網路資料源812的請求結果，並使用服務私鑰對請求結果進行簽名。中繼系統節點810將簽名的請求結果提交至中繼系統智慧合約808，簽名的請求結果透過客戶端智慧合約806進一步轉發至客戶端802。客戶端802接收簽名的請求結果，並使用服務公鑰驗證簽名的請

求結果。在成功驗證簽名的請求結果時，客戶端802可以使用該結果。

圖9描繪了根據本文的實施例的信號流900的示例。為方便起見，處理900將被描述為由位於一個或多個位置並根據本文適當程式化的一台或多台電腦的系統執行。例如，適當程式化的分布式系統(例如圖1的區塊鏈系統100和圖8的系統800)可以執行處理900。

對於來自基於網際網路的資料源812的資料或服務，客戶端802產生(902)請求。在一些示例中，請求可以是對於客戶端802的帳號的存取請求。存取請求可以包括明文部分(例如，網址)和機密資料部分(例如，客戶端帳號的憑據(例如，用戶名、密碼))。在一些示例中，存取請求中的機密資料部分可以被加密，使得網路上的惡意參與者不能獲得用戶帳號的個人資訊來潛入用戶帳號。在一些示例中，機密資料部分由客戶端802使用在先前的認證處理中從密鑰管理節點獲得的服務公鑰進行加密。

客戶端802向客戶端智慧合約806發送(904)請求。客戶端智慧合約806將請求轉發(906)到中繼系統智慧合約808。

中繼系統智慧合約808將請求轉發(908)到中繼系統節點810。在一些實施例中，中繼系統智慧合約808從密鑰管理節點周期性地接收多節點集群中在先前的密鑰分發處理中被驗證為合法的中繼系統節點810的列表。中繼系統智慧合約808可以隨機選擇經驗證的中繼系統節點810，或者

可以從列表中選擇具有最少工作負荷的經驗證的中繼系統節點810。在一些示例中，中繼系統智慧合約808透過日誌消息向所選的中繼系統節點810發送請求。

在一些實施例中，中繼系統節點810使用在先前的密鑰分發處理中獲得的服務私鑰從請求獲得(910)機密資料部分。例如，中繼系統節點810可以使用服務私鑰對加密的機密資料部分進行解密。如所述，多節點集群中的中繼系統節點810獲得並共享相同的服務私鑰。每個經驗證的中繼系統節點810都可以使用相同的服務私鑰處理加密的機密資料部分。

中繼系統節點810將明文部分和機密資料部分組合(912)成資料請求。新資料請求可被中繼系統節點810用來查詢網際網路資料源812。例如，新資料請求可以包括明文部分和機密資料部分，明文部分包括客戶端802想要存取帳號的網址，機密資料部分包括用於登錄帳號的憑據(例如，用戶名和密碼)。

中繼系統節點810向網際網路資料源812提交(914)資料請求。網際網路資料源812處理(916)資料請求並向中繼系統節點810返回(918)請求結果。

中繼系統節點810處理(920)請求結果以提供回應。根據本文的實施例，中繼系統節點810使用其服務私鑰對結果進行簽名以提供回應。更詳細地，結果或結果的至少一部分(例如，資料)由中繼系統節點810透過雜湊函數進行處理，以提供雜湊值。雜湊函數的示例包括但不限於

SHA-256。中繼系統節點810基於雜湊值和服務私鑰產生數位簽名。例如，雜湊值和服務私鑰透過提供數位簽名的簽名演算法進行處理。中繼系統節點810提供包括結果(例如，資料)和數位簽名的回應。中繼系統節點810向中繼系統智慧合約808發送(922)所述回應。

中繼系統智慧合約808將所述回應轉發(924)至客戶端智慧合約806。客戶端智慧合約806將所述回應提供(926)給客戶端802。

在一些實施例中，客戶端802驗證(928)所述回應中的簽名請求結果。在一些示例中，客戶端802使用其服務公鑰驗證簽名的請求結果中的簽名。客戶端802使用雜湊函數處理所述回應中的請求結果以計算第一雜湊值。然後，客戶端802使用服務公鑰處理請求結果的簽名以獲得簽名中包括的第二雜湊值。然後，客戶端802將第一雜湊值與第二雜湊值進行比較。如果兩個雜湊值匹配，客戶端802可以確定請求結果並使用該請求結果。如果兩個雜湊值不匹配，客戶端802可以確定請求結果無效並標記錯誤。

圖10是用於從位於區塊鏈網路外部的外部資料源檢索資料的處理1000的示例的流程圖。為方便起見，處理1000將被描述為由位於一個或多個位置並根據本文適當程式化的一台或多台電腦的系統執行。例如，適當程式化的分布式系統，例如，圖3的分布式系統300，可以執行處理1000。

在1002，在區塊鏈網路內執行的中繼系統智慧合約從

客戶端智慧合約接收用於從外部資料源檢索資料的請求。在一些實施例中，該請求包括加密資料。加密資料包括使用密鑰管理節點的服務公鑰加密的用於存取外部資料源的存取資料。在一些實施例中，密鑰管理節點位於區塊鏈網路外部。

在1004，中繼系統智慧合約從位於區塊鏈網路外部的多個中繼系統節點選擇中繼系統節點。在一些實施例中，多個中繼系統節點與密鑰管理節點的服務私鑰一起被分發。

在1006，中繼系統智慧合約將所述請求發送至選擇的中繼系統節點。

在1008，中繼系統智慧合約接收所選擇的中繼系統節點回應於所述請求返回的結果。在一些實施例中，返回結果包括從外部資料源檢索並由中繼系統節點獲得的資料和數位簽名。在一些實施例中，數位簽名是基於從外部資料源檢索到的資料和密鑰管理節點的服務私鑰產生的。

在1010，中繼系統智慧合約將返回結果發送至客戶端智慧合約。

圖11是根據本文的實施例的設備1100的模組示例的圖示。設備1100可以是配置為從外部資料源檢索資料的區塊鏈網路節點的實施例的示例，其中智慧合約在區塊鏈網路節點內執行。設備1100可以對應於上述實施例，設備1100包括以下：接收模組1102，其從客戶端智慧合約接收用於從外部資料源檢索資料的請求，該

加密資料包括用於存取外部資料源的存取資料，該存取資料被使用位於區塊鏈網路外部的密鑰管理節點的服務公鑰加密；選擇模組1104，其從位於區塊鏈網路外部的多個中繼系統節點選擇中繼系統節點，其中多個中繼系統節點與密鑰管理節點的服務私鑰一起分布；發送模組1106，其將所述請求發送到中繼系統節點；接收模組1108，其接收中繼系統節點回應於所述請求而返回的結果，該返回結果包括由中繼系統節點從外部資料源獲得的資料和數位簽名，其中數位簽名是基於從外部資料源檢索到的資料和密鑰管理節點的服務私鑰產生的；發送模組1110，其將返回結果發送給客戶端智慧合約。

在可選實施例中，密鑰管理節點的服務私鑰和服務公鑰透過密鑰管理節點的認證處理提供。

在可選實施例中，客戶端設備與密鑰管理節點和認證服務執行認證處理；在認證處理中，密鑰管理節點的服務公鑰由客戶端設備獲得。

在可選實施例中，返回結果被客戶端設備使用密鑰管理節點的服務公鑰驗證有效。

在可選實施例中，多個中繼系統節點各自執行可信執行環境(TEE)。

在可選實施例中，所述請求被第一中繼系統節點使用密鑰管理節點的服務私鑰進行解密以獲得存取資料。

在可選實施例中，密鑰管理節點與多個中繼系統節點中的每個中繼系統節點和認證服務執行認證處理。

在可選實施例中，密鑰管理節點與多個中繼系統節點執行密鑰分發處理，該密鑰分發處理導致密鑰管理節點的服務私鑰被分發到多個中繼系統節點。

在先前實施例中示出的系統、裝置、模組或單元可以透過使用電腦晶片或實體來實現，或者可以透過使用具有特定功能的產品來實現。典型的實施設備是電腦，電腦可以是個人電腦、膝上型電腦、行動電話、相機電話、智慧電話、個人數位助理、媒體播放器、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。

對於裝置中每個模組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，這裏省略了細節。

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模組可以是或不是物理上分離的，並且顯示為模組的部分可以是或不是物理模組，可以位於一個位置，或者可以分布在多個網路模組上。可以基於實際需求來選擇一些或所有模組，以實現本文的方案的目標。本領域普通技術人員無需付出創造性勞動就能理解和實現本發明的實施例。

再次參考圖11，其可以視為示出區塊鏈資料檢索裝置的內部功能模組和結構。區塊鏈資料檢索裝置可以是執行智慧合約的區塊鏈節點的示例，該智慧合約配置為從外部

資料源檢索資料。執行體本質上可以是電子設備，電子設備包括以下：一個或多個處理器；以及記憶體，配置為儲存一個或多個處理器的可執行指令。

本文的實施例實現超過傳統系統的一種或多種技術效果。在一些實施例中，提供了用於將服務私鑰分配給多個中繼系統節點的密鑰管理節點。如本文所述，對於密鑰管理節點可以執行遠程認證，這消除了每個客戶端獨立執行中繼系統節點的遠程認證的需要。這通常減輕了由從每個客戶端的中繼系統節點的單獨認證引起的網路瓶頸。此外，提供了用於從多個中繼系統節點選擇可用中繼系統節點的中繼系統智慧合約。如本文所述，透過將中繼系統節點部署在集群中，中繼系統智慧合約可以將客戶端請求自動分配至集群中的可用中繼系統節點，從而避免由於單個中繼系統節點故障而導致服務不可用性。因此，本文的實施例提高了用於查詢網路資料源的中繼系統節點的整體服務可用性。在一些實施例中，中繼系統智慧合約避免客戶端與中繼系統節點之間的直接接觸，從而避免暴露中繼系統節點的位置或接入點。因此，中繼系統節點不太可能被網路上的惡意參與者以多種形式發現和攻擊，例如，DDoS攻擊。這提高了中繼系統節點的安全性，從而進一步提高客戶端與中繼系統節點之間通信的安全性。

主題的所述實施例可以單獨地或以組合的形式包括一個或多個特徵。例如，在第一實施例中，用於從外部資料源檢索資料的方法包括中繼系統智慧合約從區塊鏈網路內

執行的客戶端智慧合約接收從外部資料源檢索資料的請求，該請求包括加密資料，該加密資料包括用於存取外部資料源的存取資料，該存取資料被使用區塊鏈網路外部的密鑰管理節點的服務公鑰加密；中繼系統智慧合約從位於區塊鏈網路外部的多個中繼系統節點選擇中繼系統節點，其中多個中繼系統節點被分發有密鑰管理節點的服務私鑰；中繼系統智慧合約將請求發送到中繼系統節點；中繼系統智慧合約從中繼系統節點接收回應於該請求的返回結果，該返回結果包括透過中繼系統節點從外部資料源獲得的資料和數位簽名，其中數位簽名是基於從外部資料源檢索的資料和密鑰管理節點的服務私鑰產生的；以及中繼系統智慧合約將返回結果發送給客戶端智慧合約。

以上和其他所述實施例可各自可選地包括一個或多個以下特徵：

第一特徵，可與以下特徵中的任一項結合，指定密鑰管理節點的服務公鑰和服務私鑰透過密鑰管理節點的認證處理被提供。

第二特徵，可與以下特徵中的任一項結合，指定客戶端設備與密鑰管理節點和認證服務執行認證處理；以及密鑰管理節點的服務公鑰由客戶端設備在認證處理期間獲得。

第三特徵，可與以上或以下特徵中的任一項結合的，指定返回結果被客戶端設備使用密鑰管理節點的服務公鑰驗證有效。

第四特徵，可與以上或以下特徵中的任一項結合的，指定多個中繼系統節點各自執行可信執行環境(TEE)。

第五特徵，可與以上或以下特徵中的任一項結合的，指定所述請求被第一中繼系統節點使用密鑰管理節點的服務私鑰進行解密以獲得存取資料。

第六特徵，可與以上或以下特徵中的任一項結合的，指定密鑰管理節點與多個中繼系統節點中的每個中繼系統節點和認證服務執行認證處理。

第七特徵，可與以上或以下特徵中的任一項結合的，指定密鑰管理節點與多個中繼系統節點執行密鑰分發處理，該密鑰分發處理使得密鑰管理節點的服務私鑰被分發至多個中繼系統節點。

本文中描述的主題的實施例以及動作和操作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可以實現為一個或多個電腦程式，例如，在電腦程式載體上編碼的、用於由資料處理裝置執行或控制資料處理裝置的操作的電腦程式指令的一個或多個模組。例如，電腦程式載體可以包括具有編碼在其上或者儲存在其上的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儲存媒體，諸如磁碟、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，機器產生的電信號、光信號或電磁信號，該信號被產生以編碼資訊，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是機器可讀儲存設備、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、腳本或碼，可以以任何形式的程式化語言編寫，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、組件、引擎、子程式或適合在計算環境中執行的其他單元，該環境可包括在一個或多個位置上由通信資料網路互聯的一台或多台電腦。

電腦程式可以但非必須對應於文件系統中的文件。電腦程式可以儲存在：保存其他程式或資料的文件的一部分中，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文件；或者多個協調文件，例如，儲存一個或多個模組、子程式或碼部分的多個文件。

例如，用於執行電腦程式的處理器包括通用微處理器和專用微處理器二者以及任何種類的數位電腦的任何一種或多種處理器。通常，處理器將接收用於執行的電腦程式的指令以及來自耦接至處理器的非暫態電腦可讀媒體的資料。

術語“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，包括例如可程式化處理器、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(現場可程式化閘陣列)、ASIC(專用積體電路)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碼，例如，構成處理器韌體、協定疊、資料庫管理系統、操作系統或者它們中的一個或多個的組合的碼。

本文中描述的處理和邏輯流程可由一台或多台電腦或執行一個或多個電腦程式以執行透過對輸入資料進行運算並產生輸出的操作的處理器執行。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化電腦的組合來執行。

適合於執行電腦程式的電腦可以基於通用或專用微處理器或二者，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，電腦還將包括或可操作地耦接至一個或多個儲存設備，以從一個或多個儲存設備接收資料或將資料傳輸到一個或多個儲存設備。儲存設備可以是例如，磁碟、磁光碟或光碟或固態驅動器、或任何其他類型的非暫態電腦可讀媒體。但是，電腦不需要具有這樣的設備。因此，電

腦可以耦接至本地和/或遠程的一個或多個儲存設備，諸如一個或多個記憶體。例如，電腦可以包括作為電腦的組成部分的一個或多個本地記憶體，或者電腦可以耦接至雲網路中的一個或多個遠程記憶體。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)、行動音訊或視訊播放器、遊戲控制台、全球定位系統(GPS)接收器或例如通用串列匯流排(USB)快閃記憶體驅動器的便攜式儲存設備，僅舉幾例。

部件可以透過可交換地諸如彼此電連接或者光連接，直接地或者經由一個或多個中間部件而彼此“耦接”。如果部件中的一個整合到另一個之中，部件也可以彼此“耦接”。例如，整合到處理器(例如，L2緩存部件)中的儲存部件“耦接至”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電腦通信，該電腦具有：顯示設備，例如，LCD(液晶顯示器)監視器，用於向用戶顯示資訊；以及輸入設備，用戶可以透過該輸入設備向該電腦提供輸入，例如鍵盤和例如滑鼠、軌跡球或觸控板等的指向裝置。其他類型的設備也可用於提供與用戶的互動；例如，提供給用戶的反饋可以是任何形式的感官反饋，例如視覺反饋、聽覺反饋或觸覺反饋；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，電腦可以透過向用戶使用的設備發送文檔和從用戶使用的設備接收文檔來與用戶互動；例如，透過向用戶設備

上的web瀏覽器發送web頁面以回應從web瀏覽器收到的請求，或者透過與例如智慧電話或電子平板電腦等的用戶設備上運行的應用程式(app)進行互動。此外，電腦可以透過向個人設備(例如，運行消息應用的智慧手機)輪流發送文本消息或其他形式的消息並接收來自用戶的回應消息來與用戶互動。

本文使用與系統、裝置和電腦程式組件有關的術語“配置為”。對於被配置為執行特定操作或動作的一台或多台電腦的系統，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。在本文中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。在一些特定情況下，多任務並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組件的劃分不應被理解為所有實施例中都要求如此劃分，而應當理解，所描述的程式組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順序執行並且仍然實現期望的結果。作為一個示例，圖式中描繪的過程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，多任務並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:計算設備

108:計算設備

110:網路

200:結構

202:參與者系統

204:參與者系統

206:參與者系統

212:區塊鏈網路

214:節點

216:區塊鏈

216’:副本

216”:副本

300:系統

302:區塊鏈

304:客戶端智慧合約

306:中繼系統智慧合約

308:中繼系統節點

310:密鑰管理節點

312:網路

314:客戶端

400:系統

402:開發者

404:客戶端

406:密鑰管理節點

408:認證服務

410:網路

420:認證證據

422:測量值

424:服務公鑰

426:簽名

430:AVR

434:驗證結果

436:簽名

500:信號流

600:系統

602:管理員

604:密鑰管理節點

606:中繼系統節點

608:認證服務

610:網路

700:信號流

800:系統

802:客戶端

804:區塊鏈

806:客戶端智慧合約

808:中繼系統智慧合約

810:中繼系統節點

812:網路

1100:設備

1102:接收模組

1104:選擇模組

1106:發送模組

1108:接收模組

1110:發送模組

【發明申請專利範圍】

【請求項1】一種電腦實現的用於從位於區塊鏈網路外部的外部資料源檢索資料的方法，該方法包括：

在該區塊鏈網路內執行的中繼系統智慧合約從客戶端智慧合約接收用於從該外部資料源檢索資料的請求，該請求包括加密資料，該加密資料包括用於存取該外部資料源的存取資料，該存取資料被使用位於該區塊鏈網路外部的密鑰管理節點的服務公鑰加密；

該中繼系統智慧合約從位於該區塊鏈網路外部的多個中繼系統節點選擇中繼系統節點，其中，該多個中繼系統節點被分發有該密鑰管理節點的服務私鑰；

該中繼系統智慧合約將該請求發送至該中繼系統節點；

該中繼系統智慧合約從該中繼系統節點接收回應於該請求的返回結果，該返回結果包括由該中繼系統節點獲得的從該外部資料源檢索的該資料和數位簽名，其中，該數位簽名是基於從該外部資料源檢索到的該資料和該密鑰管理節點的該服務私鑰產生的；以及

該中繼系統智慧合約將該返回結果發送至該客戶端智慧合約。

【請求項2】如請求項1所述的電腦實現方法，還包括：

該密鑰管理節點的認證處理提供該密鑰管理節點的該服務私鑰和該服務公鑰。

【請求項3】如請求項2所述的電腦實現方法，還包括：

客戶端設備與該密鑰管理節點和認證服務執行該認證處理；以及

在該認證處理期間，該客戶端設備獲得該密鑰管理節點的該服務公鑰。

【請求項4】如請求項3所述的電腦實現方法，其中，該返回結果被該客戶端設備使用該密鑰管理節點的該服務公鑰驗證有效。

【請求項5】如請求項1至4中的任一項所述的電腦實現方法，其中，該多個中繼系統節點各自執行可信執行環境TEE。

【請求項6】如請求項1至4中的任一項所述的電腦實現方法，其中，該請求被該中繼系統節點使用該密鑰管理節點的該服務私鑰進行解密以獲得該存取資料。

【請求項7】如請求項1至4中的任一項所述的電腦實現方法，還包括：

該密鑰管理節點與該多個中繼系統節點中的每個中繼系統節點和認證服務執行認證處理。

【請求項8】如請求項7所述的電腦實現方法，其中，該密鑰管理節點與該多個中繼系統節點執行密鑰分發處理，該密鑰分發處理使得該密鑰管理節點的該服務私鑰被分發至該多個中繼系統節點。

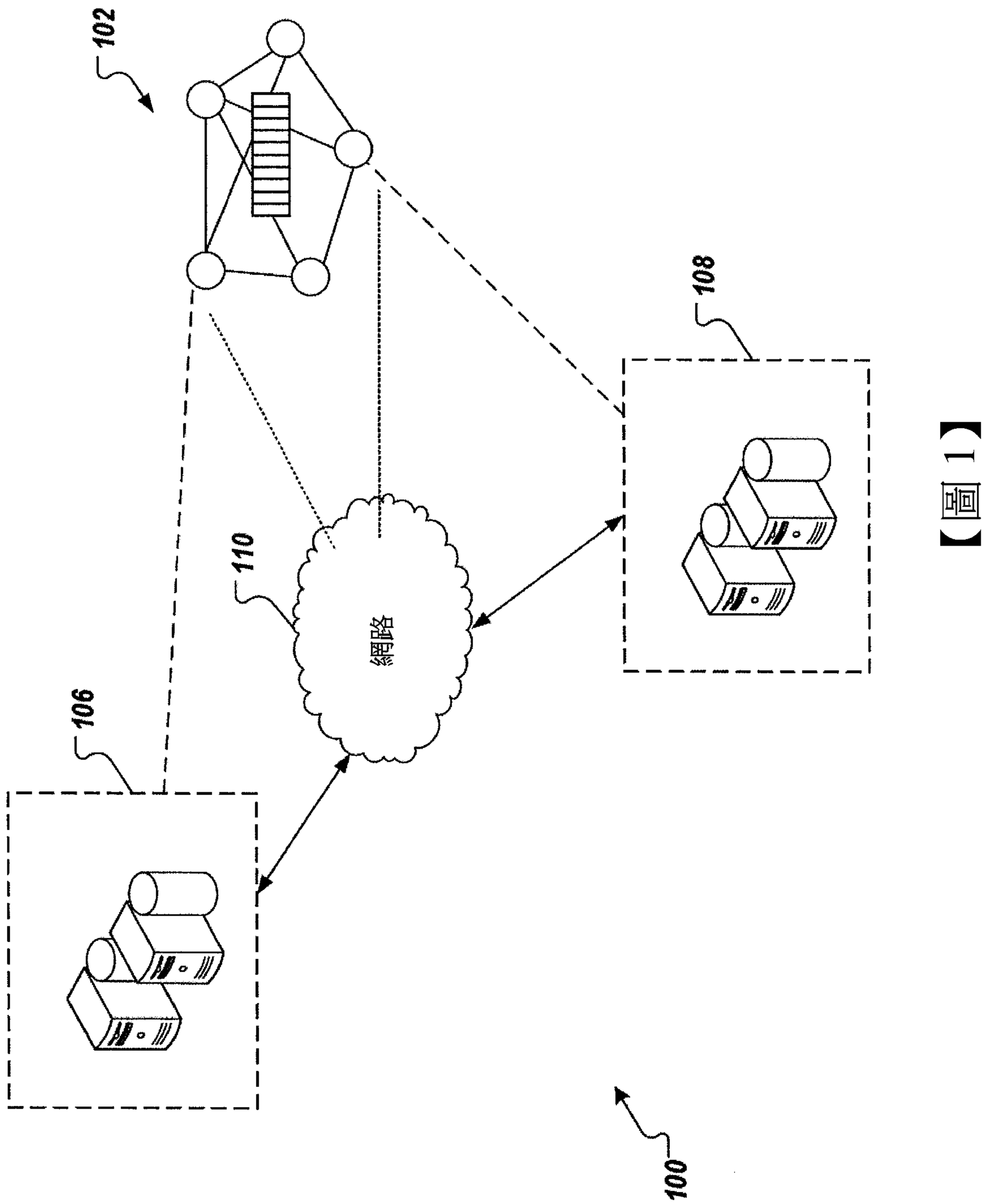
【請求項9】一種系統，包括：

一個或多個處理器；以及

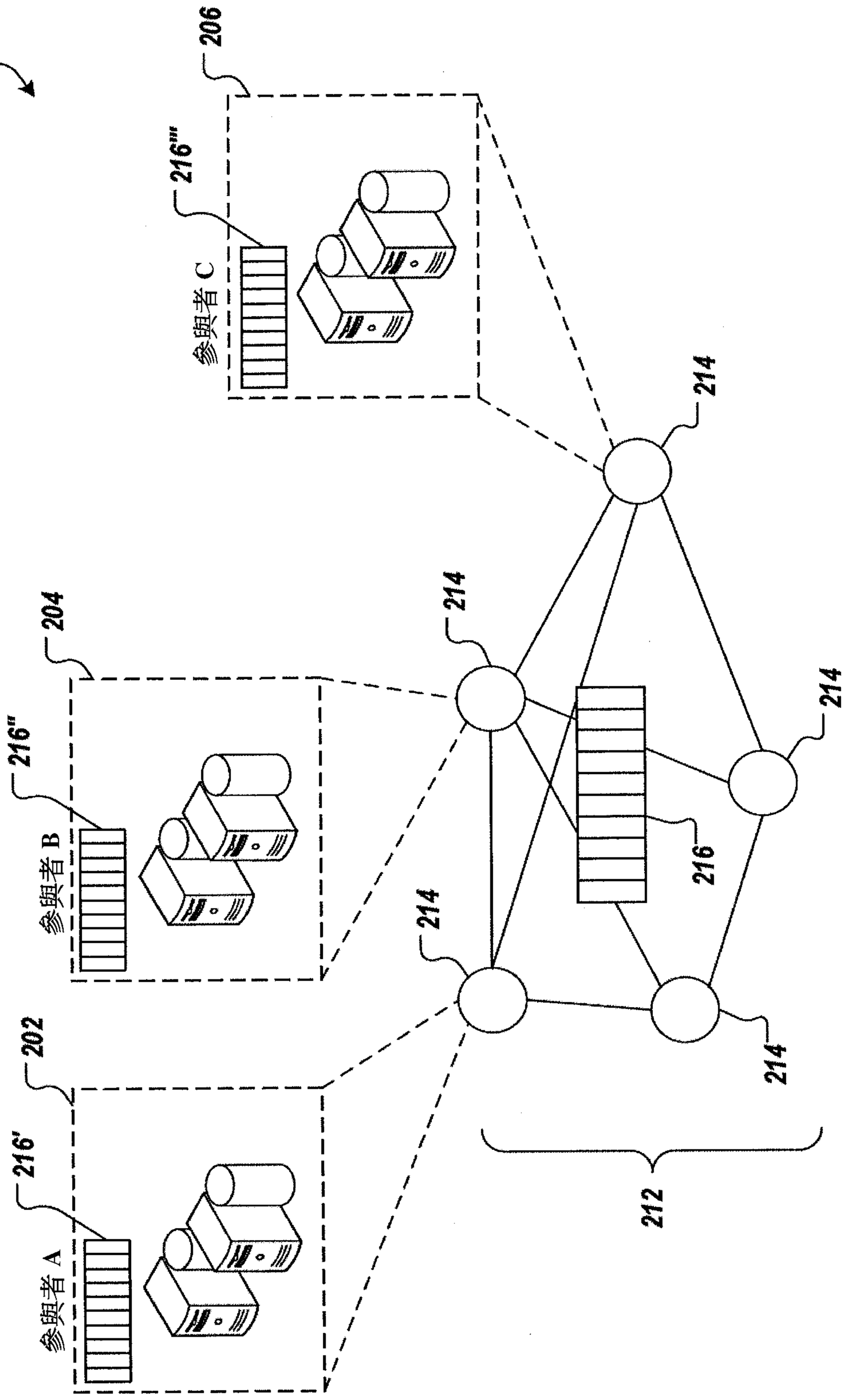
耦接至該一個或多個處理器並且其上儲存有指令的一個或多個電腦可讀記憶體，該指令能夠由該一個或多個處理器執行以執行如請求項1至8中的任一項所述的方法。

【請求項10】一種用於從位於區塊鏈網路外部的外部資料源檢索資料的裝置，該裝置包括用於執行如請求項1至8中的任一項所述的方法的多個模組。

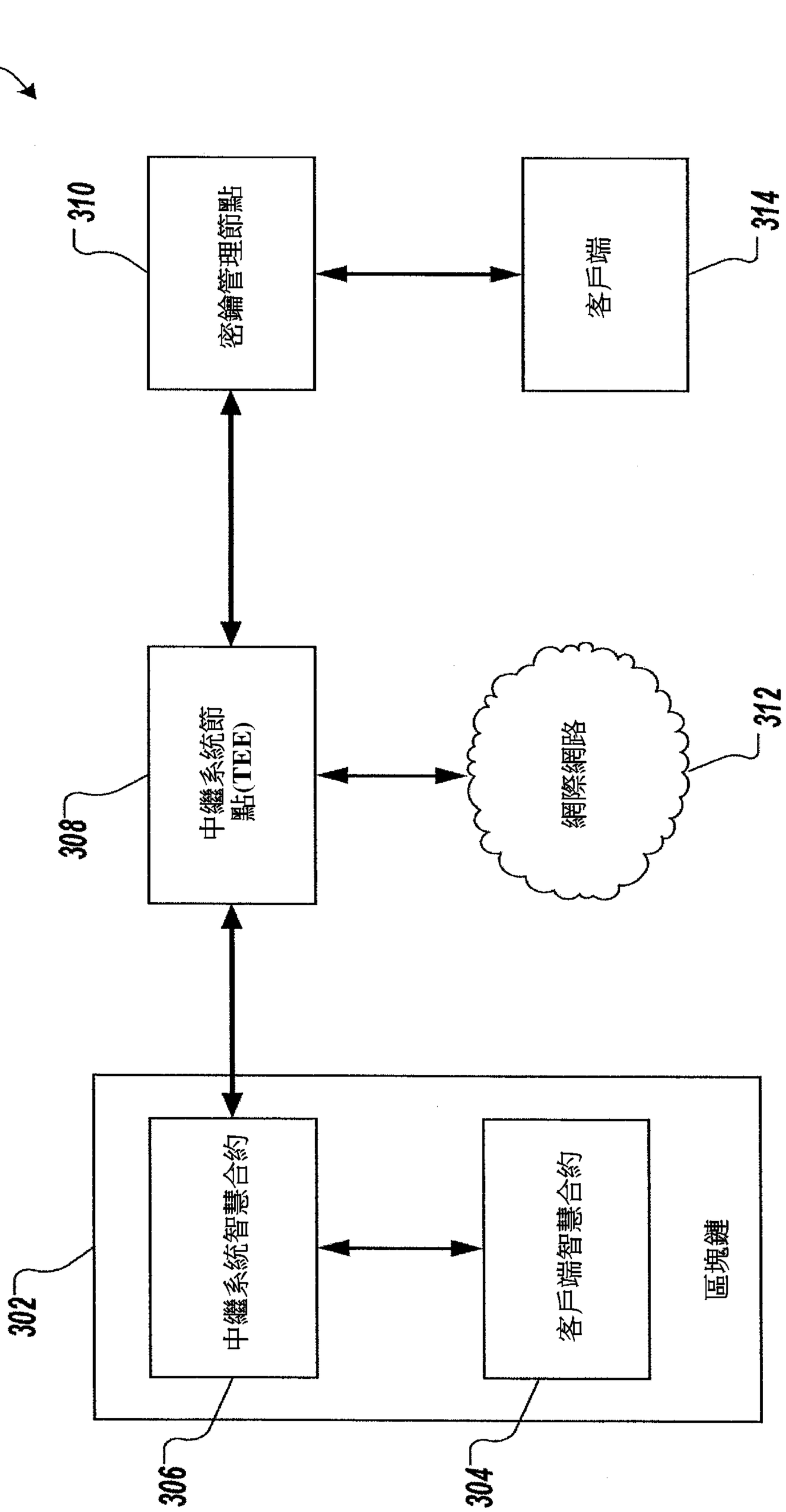
【發明圖式】



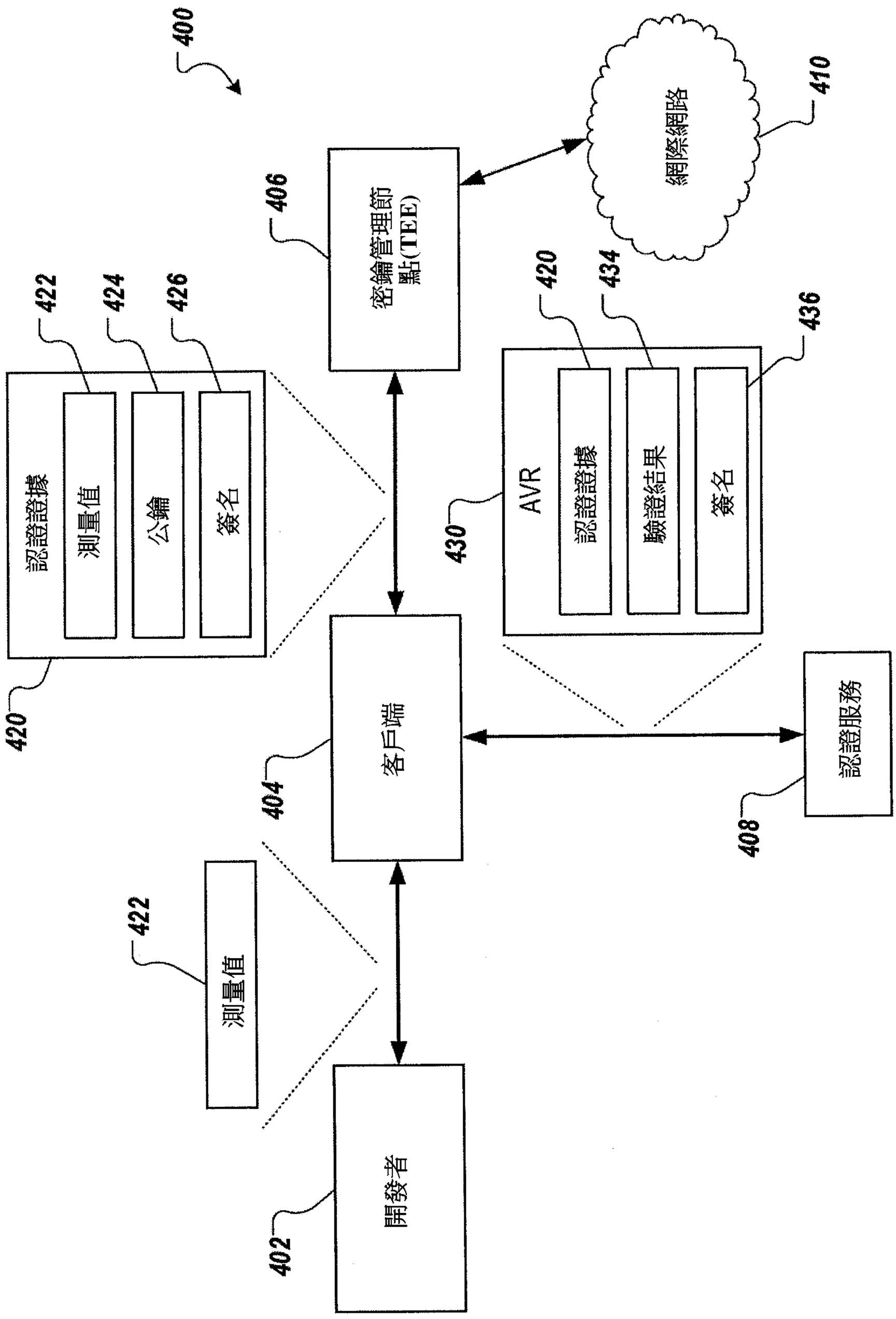
【圖1】


200
206
216'''
參與者 C
214
204
214
214
216''
參與者 B
216
214
202
216'
參與者 A
212

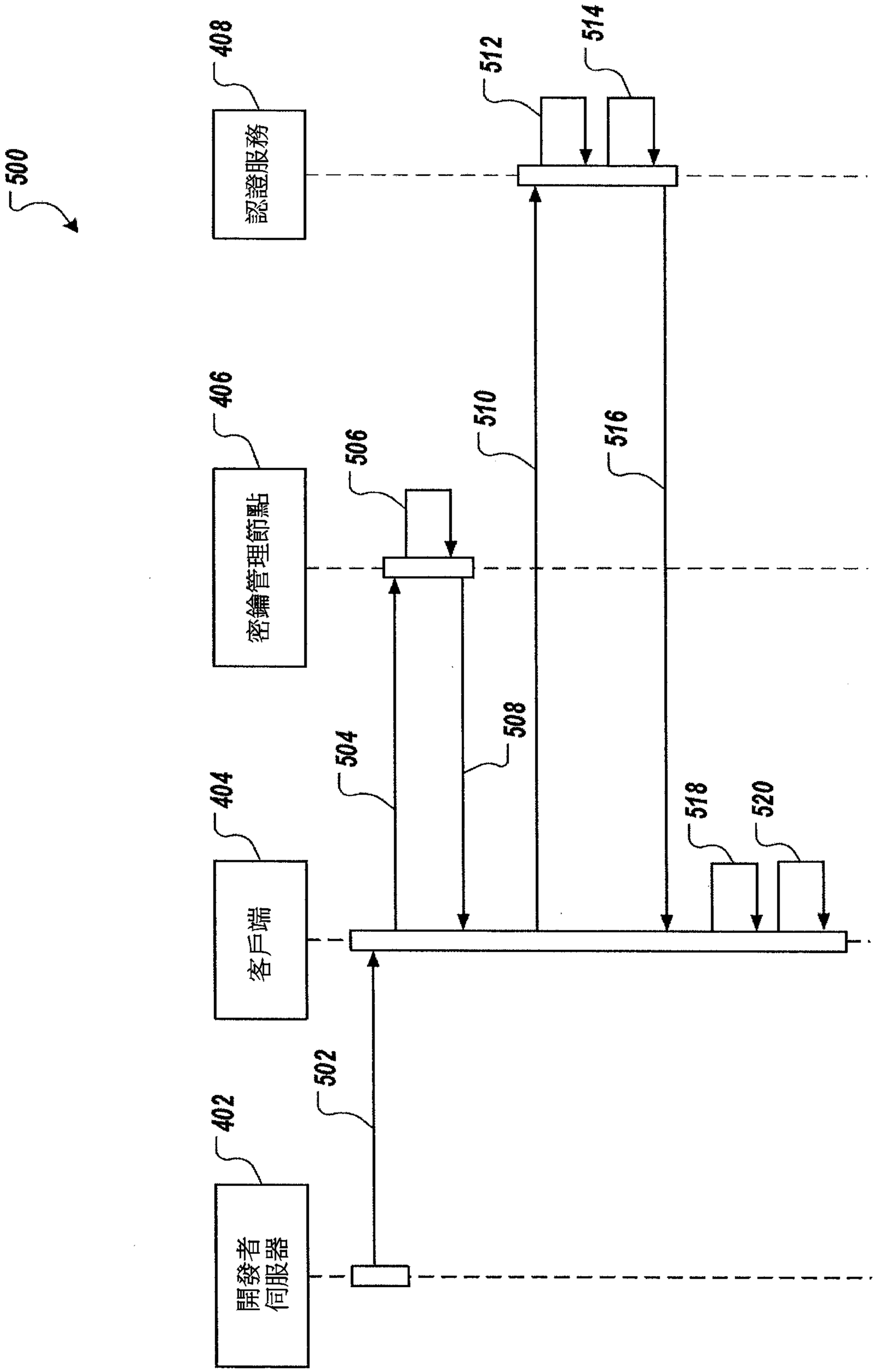
【圖 2】


300
310
密鑰管理節點
314
客戶端
308
中繼系統節點(TEE)
312
網際網路
302
中繼系統智慧合約
客戶端智慧合約
區塊鏈
306
304

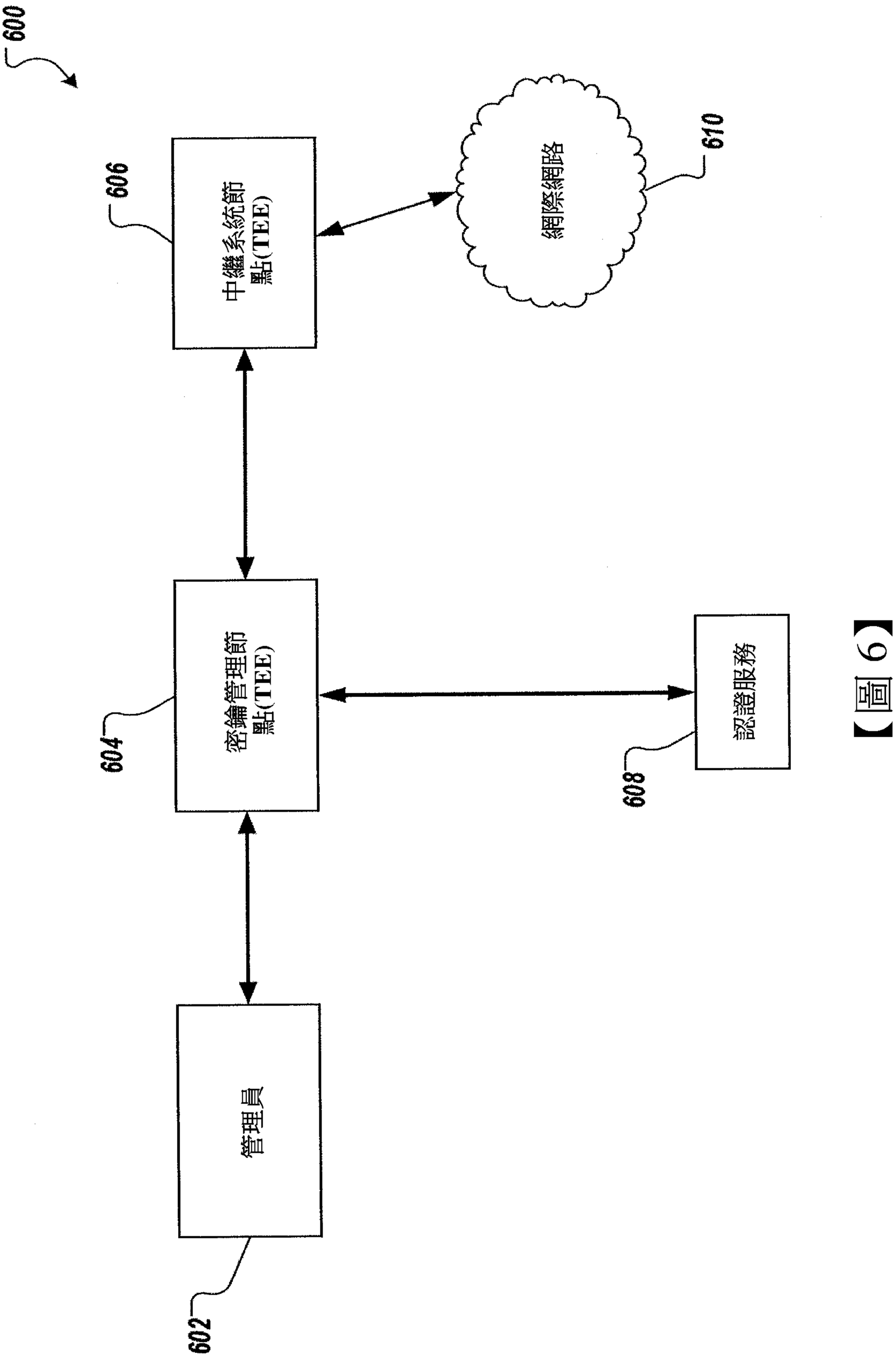
【圖 3】


400
410
網際網路
406
密鑰管理節點(TEE)
422
424
426
認證證據
測量值
公鑰
簽名
420
434
436
AVR
認證證據
驗證結果
簽名
430
404
客戶端
408
認證服務
422
測量值
420
402
開發者

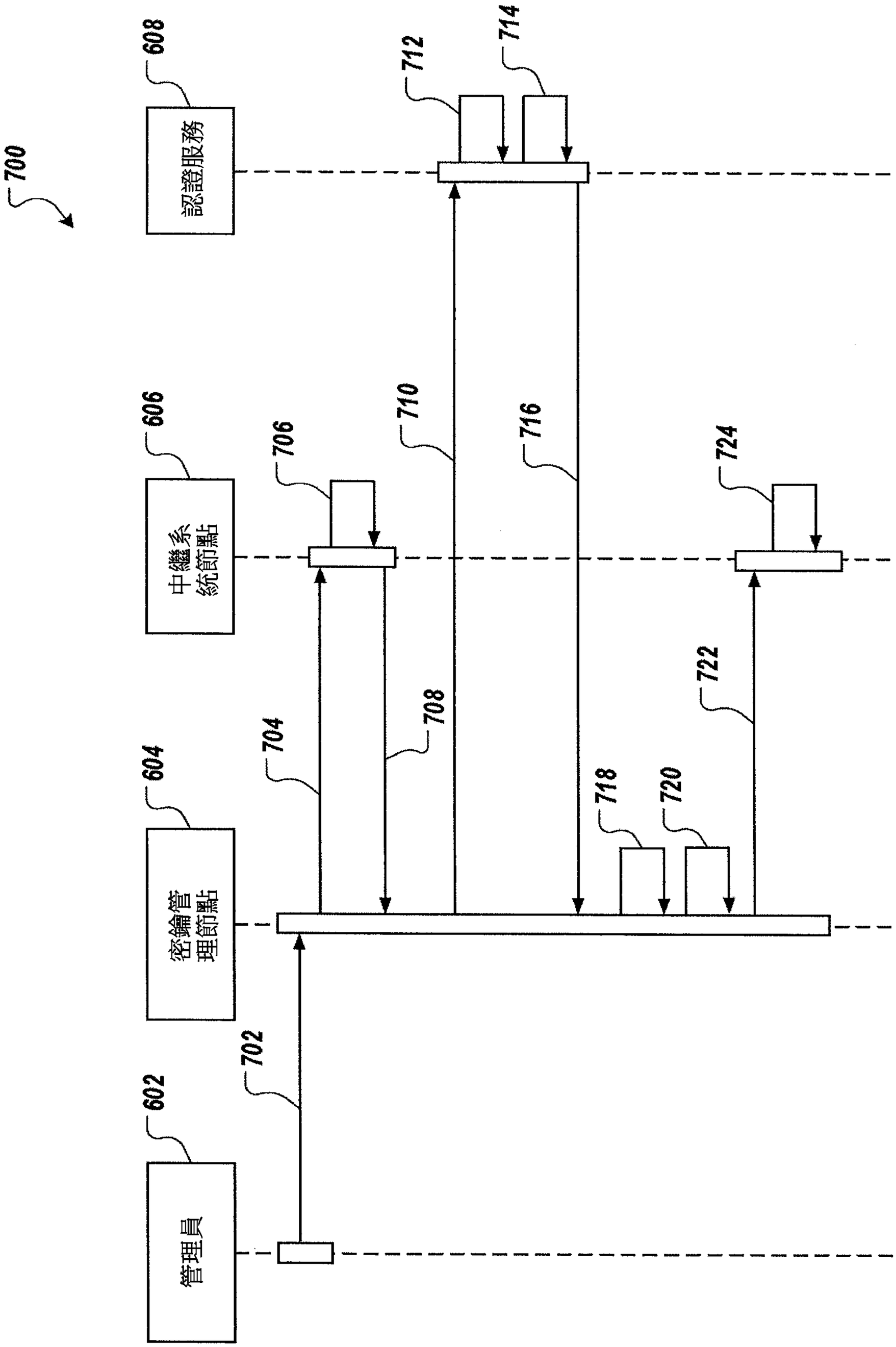
【圖 4】


500
408
認證服務
512
514
406
密鑰管理節點
506
510
516
404
客戶端
504
508
518
520
402
開發者伺服器
502

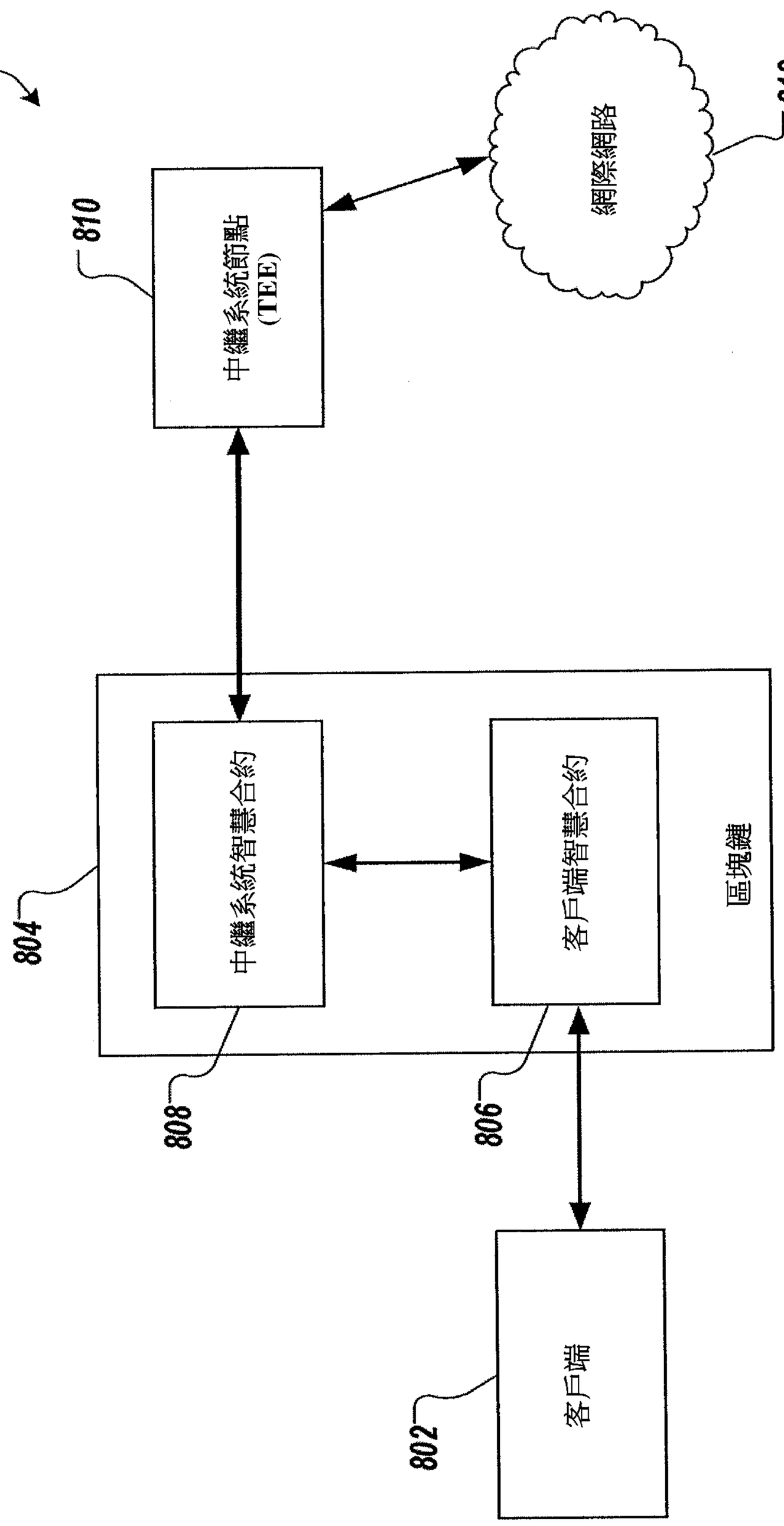
【圖 5】



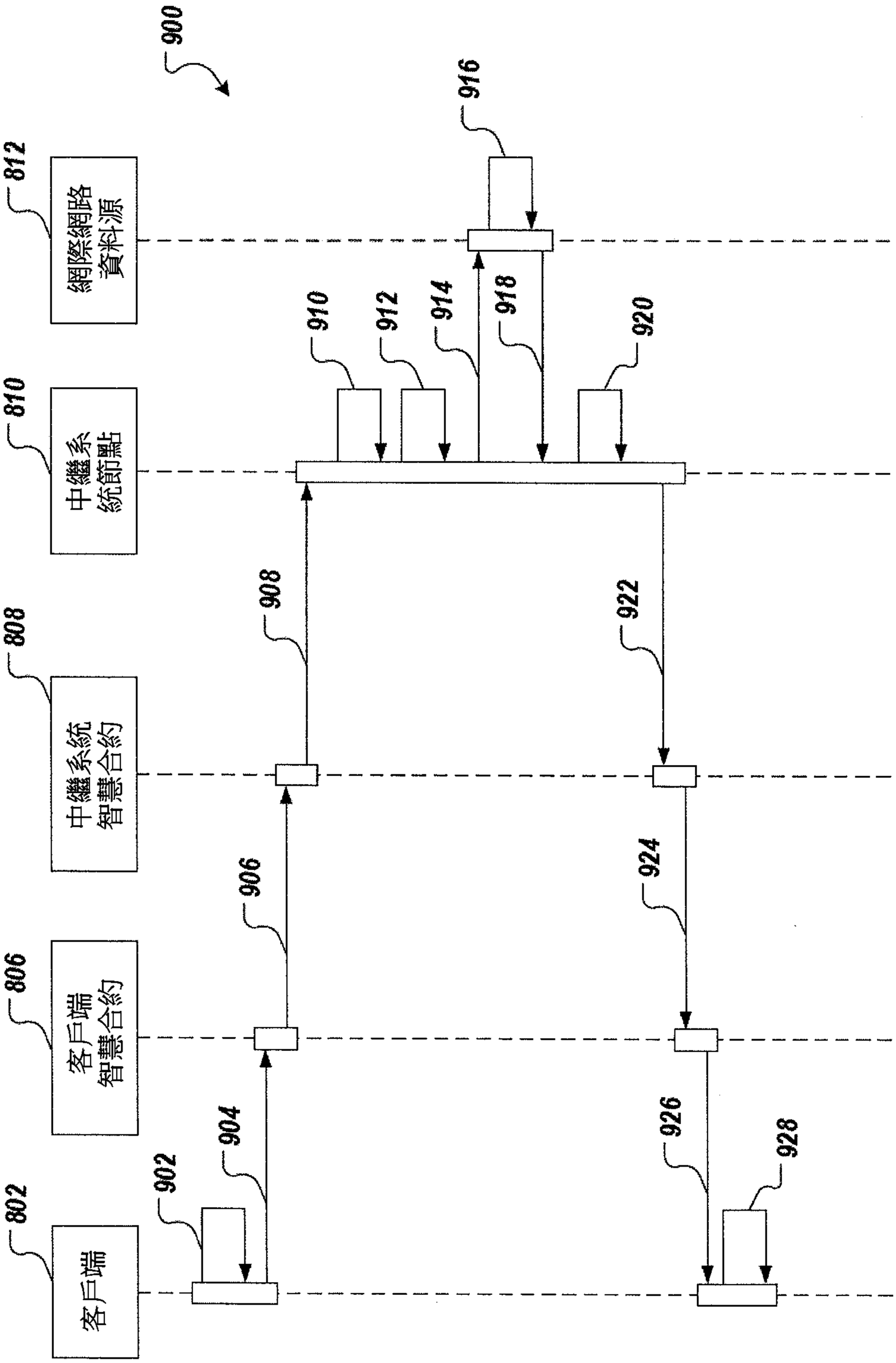
【圖 6】


700
608
認證服務
712
714
606
中繼系統節點
706
710
716
724
604
密鑰管理節點
704
708
718
720
722
602
管理員
702

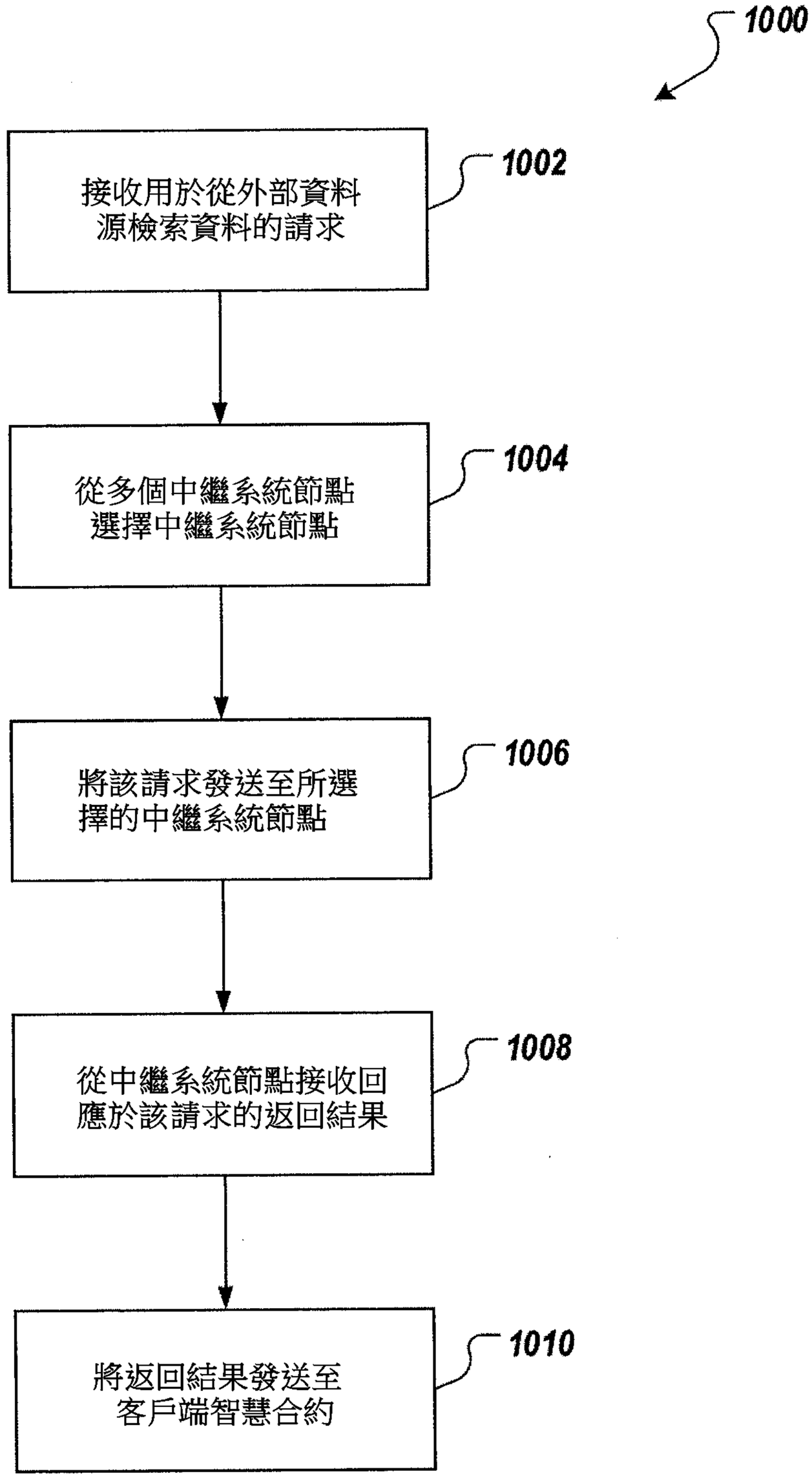
【圖 7】


800
812
網際網路
810
中繼系統節點
(TEE)
804
中繼系統智慧合約
808
客戶端智慧合約
806
區塊鏈
802
客戶端

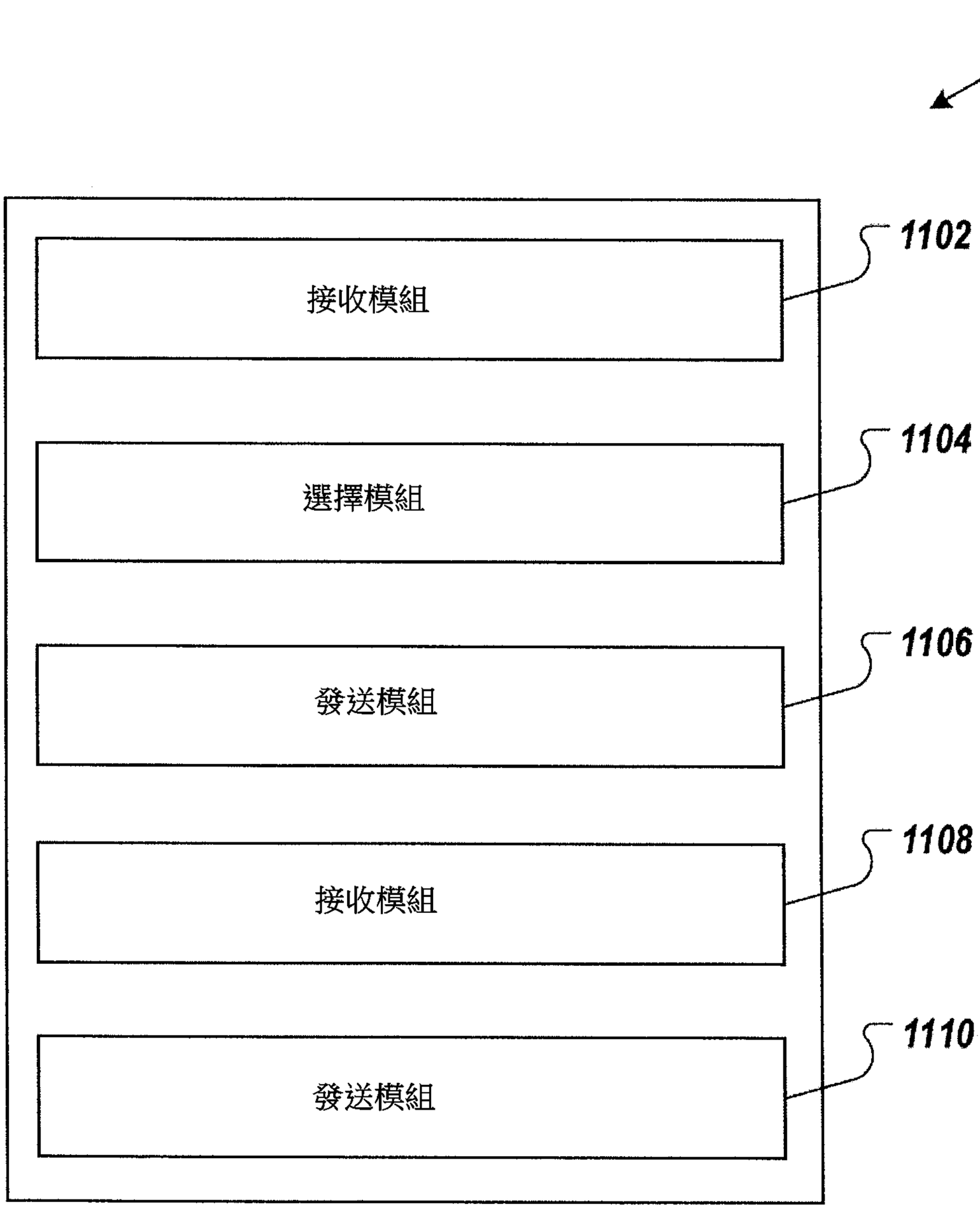
【圖 8】


900
802
客戶端
804
客戶端
智慧合約
806
客戶端
智慧合約
808
中繼系統
智慧合約
810
中繼系統
統節點
812
網際網路
資料源
902
904
906
908
910
912
914
916
918
920
922
924
926
928

【圖 9】


1000
接收用於從外部資料源檢索資料的請求
1002
從多個中繼系統節點選擇中繼系統節點
1004
將該請求發送至所選擇的中繼系統節點
1006
從中繼系統節點接收回應於該請求的返回結果
1008
將返回結果發送至客戶端智慧合約
1010

【圖 10】



【圖 11】