



(21) 申請案號：109100163

(22) 申請日：中華民國 109 (2020) 年 01 月 03 日

(51) Int. Cl. : G06F21/64 (2013.01)

G06F16/24 (2019.01)

(30) 優先權：2019/04/18 中國大陸

201910314334.9

(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：楊新穎 (CN)；俞本權 (CN)；李億澤 (CN)；張淵 (CN)；卓海振 (CN)

(74) 代理人：林志剛

申請實體審查：有 申請專利範圍項數：15 項 圖式數：5 共 37 頁

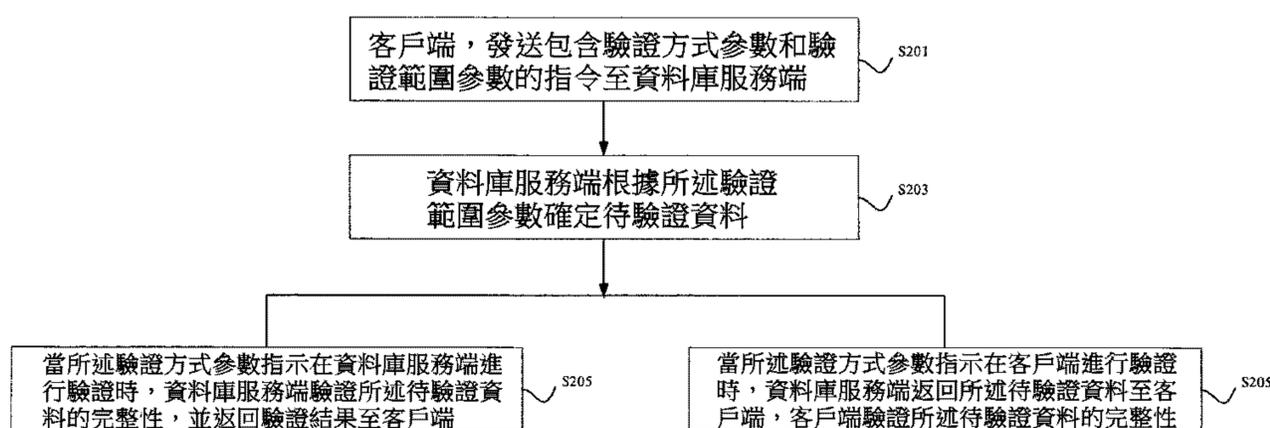
(54) 名稱

塊鏈式帳本中的資料驗證方法、系統、裝置及設備

(57) 摘要

揭示了一種塊鏈式帳本中的資料驗證方法、系統、裝置及設備。透過本說明書實施例所提供的方案，用戶在發起驗證請求時，在請求中攜帶相關的驗證方式參數和驗證範圍參數，從而服務端可以基於該驗證方式參數確定出在服務端進行驗證還是在客戶端進行驗證，以及基於驗證範圍參數確定驗證範圍的大小，進而執行相應的驗證方式。本實施例可以靈活的在塊鏈式帳本中實現資料驗證。

指定代表圖：



【圖 2】



202040407

【發明摘要】

【中文發明名稱】

塊鏈式帳本中的資料驗證方法、系統、裝置及設備

【中文】

揭示了一種塊鏈式帳本中的資料驗證方法、系統、裝置及設備。透過本說明書實施例所提供的方案，用戶在發起驗證請求時，在請求中攜帶相關的驗證方式參數和驗證範圍參數，從而服務端可以基於該驗證方式參數確定出在服務端進行驗證還是在客戶端進行驗證，以及基於驗證範圍參數確定驗證範圍的大小，進而執行相應的驗證方式。本實施例可以靈活的在塊鏈式帳本中實現資料驗證。

【指定代表圖】第(2)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】

塊鏈式帳本中的資料驗證方法、系統、裝置及設備

【技術領域】

本說明書實施例係有關資訊技術領域，尤其有關一種塊鏈式帳本中的資料驗證方法、系統、裝置及設備。

【先前技術】

在中心化的資料庫服務端以塊鏈式帳本儲存資料時，用戶經常會對服務端發起各種驗證。而在進行驗證時，基於用戶的需求，有些驗證需要在客戶端完成，有些驗證需要在服務端完成，而同時，用戶在進行驗證時的範圍也常常不同。

基於此，需要一種在塊鏈式帳本中可以靈活進行資料驗證的方案。

【發明內容】

本發明實施例的目的是提供一種塊鏈式帳本中進行資料驗證的方案。

為解決上述技術問題，本發明實施例是這樣實現的：

一種塊鏈式帳本中的資料驗證方法，應用於包括資料庫服務端和客戶端的系統中，所述資料庫服務端以中心化的方式透過塊鏈式帳本儲存資料，所述方法包括：

客戶端，發送包含驗證方式參數和驗證範圍參數的指令至資料庫服務端，其中，所述驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；所述驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

資料庫服務端根據所述驗證範圍參數確定待驗證資料，所述待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

當所述驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證所述待驗證資料的完整性，並返回驗證結果至客戶端；

當所述驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回所述待驗證資料至客戶端，客戶端驗證所述待驗證資料的完整性，產生驗證結果。

相應地，本說明書實施例還提供一種塊鏈式帳本中的資料驗證系統，包括資料庫服務端和客戶端，所述資料庫服務端以中心化的方式透過塊鏈式帳本儲存資料，在所述系統中，

客戶端，發送包含驗證方式參數和驗證範圍參數的指令至資料庫服務端，其中，所述驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；所述驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

資料庫服務端，根據所述驗證範圍參數確定待驗證資

料，所述待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

當所述驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證所述待驗證資料的完整性，並返回驗證結果至客戶端；

當所述驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回所述待驗證資料至客戶端，客戶端驗證所述待驗證資料的完整性，產生驗證結果。

相應地，本說明書實施例還提供一種鏈式帳本中的資料驗證方法，應用於以中心化的方式透過塊鏈式帳本儲存資料的資料庫服務端中，所述方法包括：

接收包含驗證方式參數和驗證範圍參數的指令，其中，所述驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；所述驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

根據所述驗證範圍參數確定待驗證資料，所述待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

當所述驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證所述待驗證資料的完整性，並返回驗證結果至客戶端；

當所述驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回所述待驗證資料至客戶端，以便客戶端驗證

所述待驗證資料的完整性。

相應地，本說明書實施例還提供一種鏈式帳本中的資料驗證裝置，應用於以中心化的方式透過塊鏈式帳本儲存資料的資料庫服務端中，所述裝置包括：

接收模組，接收包含驗證方式參數和驗證範圍參數的指令，其中，所述驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；所述驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

確定模組，根據所述驗證範圍參數確定待驗證資料，所述待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

驗證模組，當所述驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證所述待驗證資料的完整性，並返回驗證結果至客戶端；

發送模組，當所述驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回所述待驗證資料至客戶端，以便客戶端驗證所述待驗證資料的完整性。

透過本說明書實施例所提供的方案，用戶在發起驗證請求時，在請求中攜帶相關的驗證方式參數和驗證範圍參數，從而服務端可以基於該驗證方式參數確定出在服務端進行驗證還是在客戶端進行驗證，以及基於驗證範圍參數確定驗證範圍的大小，進而執行相應的驗證方式。本實施例可以靈活的在塊鏈式帳本中實現資料驗證。

應當理解的是，以上的一般描述和後文的細節描述僅是示例性和解釋性的，並不能限制本說明書實施例。

此外，本說明書實施例中的任一實施例並不需要達到上述的全部效果。

【圖式簡單說明】

為了更清楚地說明本說明書實施例或現有技術中的技術方案，下面將對實施例或現有技術描述中所需要使用的圖式作簡單地介紹，顯而易見地，下面描述中的圖式僅僅是本說明書實施例中記載的一些實施例，對於本領域普通技術人員來講，還可以根據這些圖式而獲得其他的圖式。

[圖1]為本說明書實施例所提供的塊鏈式帳本中產生資料塊的流程示意圖；

[圖2]是本說明書實施例提供的一種塊鏈式帳本中的資料驗證方法；

[圖3]為本說明書實施例所提供的資料庫服務端方面的資料驗證方法的流程示意圖；

[圖4]是本說明書實施例提供的資料庫服務端方面的一種塊鏈式帳本中的資料驗證裝置的結構示意圖；

[圖5]是用於配置本說明書實施例方法的一種設備的結構示意圖。

【實施方式】

為了使本領域技術人員更好地理解本說明書實施例中

的技術方案，下面將結合本說明書實施例中的圖式，對本說明書實施例中的技術方案進行詳細地描述，顯然，所描述的實施例僅僅是本說明書的一部分實施例，而不是全部的實施例。基於本說明書中的實施例，本領域普通技術人員所獲得的所有其他實施例，都應當屬於保護的範圍。

首先對本說明書中所涉及的中心化的塊鏈式的帳本進行說明。

在本說明書實施例所涉及中心化的資料庫服務提供方中，一個帳本包括含多個資料塊，資料塊透過如下方式預先產生，如圖1所示，圖1為本說明書實施例所提供的塊鏈式帳本中產生資料塊的流程示意圖，包括：

S101，接收待儲存的資料記錄，確定各資料記錄的雜湊值。此處的待儲存的資料記錄，可以是客戶端個人用戶的各種消費記錄，也可以是應用伺服器基於用戶的指令，在執行業務邏輯時產生的業務結果、中間狀態以及操作記錄等等。具體的業務場景可以包括消費記錄、審計日誌、供應鏈條、政府監管記錄、醫療記錄等等。

S103，當達到預設的成塊條件時，確定待寫入資料塊中的各資料記錄，產生包含資料塊的雜湊值和資料記錄的第N個資料塊。

所述預設的成塊條件包括：待儲存的資料記錄數量達到數量閾值，例如，每接收到一千條資料記錄時，產生一個新資料塊，將一千條資料記錄寫入塊中；或者，距離上一次成塊時刻的時間間隔達到時間閾值，例如，每隔5分

鐘，產生一個新資料塊，將在這5分鐘內接收到的資料記錄寫入塊中。

此處的N指的是資料塊的序號，換言之，在本說明書實施例中，資料塊是以塊鏈的形式，基於成塊時間的順序先後排列，具有很強的時序特徵。其中，資料塊的塊高基於成塊時間的先後順序而單調遞增。塊高可以是序號，此時第N個資料塊的塊高即為N；塊高也可以其它方式產生。

當 $N=1$ 時，即此時的資料塊為為初始資料塊。初始資料塊的雜湊值和塊高基於預設方式給定。例如，初始資料塊中不包含資料記錄，雜湊值則為任一給定的雜湊值，塊高 $blknum=0$ ；又例如，初始資料塊的產生觸發條件與其它資料塊的觸發條件一致，但是初始資料塊的雜湊值由對初始資料塊中的所有內容取雜湊來確定。

當 $N>1$ 時，由於前一個資料塊的內容和雜湊值已經確定，則此時，可以基於前一個資料塊(即第 $N-1$ 個資料塊)的雜湊值產生目前資料塊(第N個資料塊)的雜湊值，例如，一種可行的方式為，確定每一條將要寫入第N個塊中的資料記錄的雜湊值，按照在塊中的排列順序，產生一個默克爾樹，將默克爾樹的根雜湊值和前一個資料塊的雜湊值拼接在一起，再次採用雜湊演算法，產生目前資料塊的雜湊值。又例如，還可以按照資料塊中資料記錄的順序進行拼接並取雜湊得到整體資料記錄的雜湊值，拼接前一個資料塊的雜湊值和整體資料記錄的雜湊值，並對拼接得到

的字串進行雜湊運算，產生資料塊的雜湊值。

在服務端產生一個資料塊並寫入帳本時，即可以將資料塊的雜湊值以及資料塊中各資料記錄的雜湊值返回給客戶端。

透過前述的資料塊的產生方式，每一個資料塊透過雜湊值來確定，資料塊的雜湊值由資料塊中的資料記錄的內容、順序以及前一個資料塊的雜湊值來決定。用戶可以隨時基於資料塊的雜湊值發起驗證，對於資料塊中任何內容(包括對於資料塊中資料記錄內容或者順序的修改)的修改都會造成在驗證時計算得到的資料塊的雜湊值和資料塊產生時的雜湊值不一致，而導致驗證失敗，從而實現了中心化下的不可篡改。

具體而言，對於資料記錄的完整性的驗證方式即為獲取所述資料記錄，確定所述記錄的雜湊，以及資料記錄所處的資料塊中的其它資料記錄的雜湊值，形成默克爾樹，驗證能否重新產生該默克爾樹的根雜湊。對於資料塊的驗證方式即為根據前一個資料塊的雜湊值以及自身資料記錄，重新計算自身資料塊的雜湊值，驗證與之前計算得到的雜湊值是否一致。以及，還可以直接將雜湊值所對應的資料記錄返回給用戶，以使用戶直接對資料記錄進行雜湊運算驗證完整性。

如前所述，在用戶的資料被儲存至帳本中之後，用戶可以向服務端發起驗證。需要說明的是，在本說明書實施例中，塊鏈式帳本雖然類似於區塊鏈，但是本說明書實施

例中，資料庫服務端是以中心化的形式進行對外服務的，這與區塊鏈有著本質上的區別。

在區塊鏈系統中，由於是去中心化的服務，因此，客戶端可以向任一有權限執行驗證的節點發起資料驗證，區塊鏈系統可以確保各節點返回的資料的一致性，用戶可以相信節點所返回的結果，換言之，客戶端沒有必要在本地執行資料驗證。

但是，在本說明書實施例中，由於資料庫服務端是中心化的方式，因此，對於用戶而言，資料儲存和資料驗證如果都在服務端完成，那麼結果就不一定是可信的，因此，對於某些用戶而言，其希望在客戶端完成相應的資料驗證。

同時，在塊鏈式帳本中，有些驗證資源消耗較小，例如，驗證一條資料記錄是否存在帳本中；而有些驗證資源消耗則較大，例如，驗證整個帳本的資料完整性，對於某些客戶端設備而言，需要消耗的資源可能難以承受。

基於此，本說明書實施例提供一種可以在塊鏈式帳本中進行靈活的資料驗證的方案。

以下結合圖式，詳細說明本說明書各實施例提供的技術方案。如2所示，圖2是本說明書實施例提供的一種塊鏈式帳本中的資料驗證方法，應用於包括資料庫服務端和客戶端的系統中，所述資料庫服務端以中心化的方式透過塊鏈式帳本儲存資料，該流程具體包括如下步驟：

S201，客戶端，發送包含驗證方式參數和驗證範圍參

數的指令至資料庫服務端。

具體而言，用戶可以透過客戶端發起驗證指令，驗證指令中透過驗證範圍參數指定需要對哪些資料塊發起驗證。驗證範圍參數可以是塊高或者雜湊值。

例如，可以透過雜湊值指定一個資料塊，確定對該資料塊發起驗證；或者，還加入一個數值，用於指定對該資料塊之前或者之後的多個資料塊發起是否正確的驗證；或者，透過雜湊值指定一個資料記錄，驗證一個資料記錄是否存在資料庫中。

同時，在驗證指令中還可以包括驗證方式參數，驗證方式參數用以表明用戶的需求，指示本次驗證在資料庫服務端進行驗證，或者在客戶端進行驗證。需要說明的是，在驗證指令中可以只包含驗證範圍參數，驗證方式參數可以預設，此時，預設的驗證方式將在服務端進行。

以下示例性的給出了本說明書實施例所提供的幾種驗證指令的形式，其中，驗證方式都進行了預設。

第一種，指令中包含驗證範圍參數雜湊值，雜湊值對應於資料記錄或者某個資料塊，服務端對該資料塊執行驗證，得到驗證結果，具體地，可以由驗證指令 `VERIFY ('khash', &v)` 實現。其中，“khash”為用戶輸入的雜湊值，“&v”為本次驗證的返回結果，在驗證結束後由服務端給“&v”進行賦值。

第二種，指令中包含驗證範圍參數雜湊值，雜湊值用於確定一個對應的資料塊，或者，用於確定雜湊值對應的

資料記錄所處的資料塊。該驗證指令用於，從確定的資料塊開始往前驗證直至初始資料塊，具體地，可以透過驗證指令 `VERIFY('khash', &v, -1)` 實現，一般而言，初始塊高為“0”或者“1”，因此，其中的 -1 也可以是其它小於初始塊高的值，從而服務方可以知道，這個參數不是一個特別小的塊高值，意味著需要一直驗證至初始資料塊。

第三種，指令中包含驗證範圍參數雜湊值，雜湊值用於確定對應的資料塊，從確定的資料塊開始往前驗證指定個數的資料塊，具體地，可以透過驗證指令 `VERIFY('khash', &v, blknum)` 實現，其中，`khash` 即為用戶輸入的雜湊值，“`blknum`”為由用戶指定的待驗證的資料塊的數量。

第四種，指令中包含驗證範圍參數塊高，由塊高對應的資料塊開始往前驗證指定數量的連續多個資料塊，具體地，可以透過驗證指令 `VERIFY(blkh, &v, blknum)` 實現，其中，“`blkh`”即為用戶輸入的雜湊值，“`blknum`”為由用戶指定的待驗證的資料塊的數量，`blknum` 可以是 1 或者預設，此時即只驗證一個資料塊；`blknum` 也可以是一個大數，如果 `blknum` 的值超過帳本中的帳本數量，此時則說明本次驗證需要執行全量帳本驗證。

第五種，指令中包含驗證範圍參數兩個塊高值，具體地，可以透過驗證指令 `VERIFY(blkh1, blkh2, &v)` 實現。`blkh1` 和 `blkh2` 用於確定本次驗證資料塊的塊高區間。

進一步地，在驗證指令中，可以加入驗證方式參數，

用以明確在服務端執行，或者在客戶端執行驗證。

例如，對於前述的第一種驗證指令，加入驗證方式參數後，即為 `VERIFY(Remote, 'khash', &v)`，或者，`VERIFY(Client, 'khash', &v)`。其中，“Remote”表明本次驗證在服務端進行，“Client”表明本次驗證在客戶端進行。

又例如，對於前述的第四種指令，可以在其中加入驗證方式參數，其形式為 `VERIFY(Client, blkh, &v, 1)`，從而表明本次對於某個塊高的資料塊的驗證在客戶端完成。

S203，資料庫服務端根據所述驗證範圍參數確定待驗證資料，所述待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者。

在塊鏈式帳本中，雜湊值可以唯一的表徵一個資料記錄或者一個資料塊，而塊高也可以唯一的標識一個資料塊。因此，基於驗證範圍參數，總是可以確定出本次指令所對應的待驗證資料。

本說明書實施例中的“對應”指的是資料記錄或者資料塊進行雜湊運算可以得到一個雜湊值，則該雜湊值和該資料記錄或者資料塊存在對應關係。

具體而言，資料庫服務端在接收到驗證指令後，即可以解析指令並得到相應的驗證範圍參數雜湊值或者塊高。進而，資料庫服務端可以進行遍歷查詢以驗證該雜湊是否對應某個資料記錄，或者對應於某個資料塊；或者，從索

引表中查詢獲取該雜湊值所對應的塊高和偏移量，然後根據讀取得到的塊高和偏移量獲取得到對應的資料記錄。

例如，對於包含雜湊值的第一種驗證指令而言，`VERIFY(Remote, 'khash', &v)`，服務端獲取其中的雜湊值，從預先建立的關於(資料記錄雜湊值，塊高，塊高中的偏移量)的資料記錄索引表中對雜湊值進行匹配查詢，得到該資料記錄所處的資料塊的塊高和偏移量，進而確定該雜湊值所對應的資料記錄，將該資料記錄確定為待驗證資料。

需要說明的是，在該指令中無需用戶指定“khash”是資料記錄的雜湊值還是資料塊的雜湊值，服務端可以採用遍歷的方式從帳本中查詢獲取該雜湊值對應的對象，或者從預先建立的資料記錄雜湊索引/資料塊雜湊索引(包含資料塊雜湊值和資料塊塊高的對應關係)中查詢得到該雜湊值對應的對象。

又例如，對於包含資料塊塊高的第五種指令而言，`VERIFY(Client, 100, 300, &v)`。資料庫服務端可以基於塊高100和300，即可以確定塊高區間[100, 300]，將塊高落入該區間的資料塊所對應的部分帳本確定為待驗證資料。

S205，驗證待驗證資料的完整性。

具體而言，當所述驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證所述待驗證資料的完整性，並返回驗證結果至客戶端。驗證結果可以透過對驗證

指令中的“&v”賦值實現展示。

當所述驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回所述待驗證資料至客戶端，客戶端驗證所述待驗證資料的完整性，產生驗證結果。具體資料記錄或者帳本完整性的驗證方法在前文已經進行了說明，此處不再贅述。

透過本說明書實施例所提供的方案，用戶在發起驗證請求時，在請求中攜帶相關的驗證方式參數和驗證範圍參數，從而服務端可以基於該驗證方式參數確定出在服務端進行驗證還是在客戶端進行驗證，以及基於驗證範圍參數確定驗證範圍的大小，進而執行相應的驗證方式。本實施例可以靈活的在塊鏈式帳本中實現資料驗證。

在一種實施例中，還可以在驗證方式參數中加入進一步的指示性的首碼或者尾碼欄位，以便服務端可以更有效的解析該指令。

例如，在驗證方式中加入首碼Tx，用以指明本次驗證是對資料記錄在客戶端進行驗證，驗證指令的形式從而成為，**VERIFY(TxClient, khash, &v)**，從而服務端可以直接查詢該khash所對應的資料記錄。

在一種實施例中，當驗證方式參數指示在客戶端進行驗證時，而同時在客戶端中如果有相關用於驗證的資料時，服務端只需要發送待驗證資料即可。

在一種實施例中，資料庫服務端在確定待驗證資料時，還可以根據操作指令確定進行驗證時所需要的其它輔

助驗證資料，並發送至客戶端

例如，當用戶發起第四種驗證指令，驗證指定的資料塊，`VERIFY(Client, blkh, &v, 1)`，表明需要在客戶端，對由塊高`blkh`所指定的資料塊進行驗證。資料庫服務端可以根據塊高`blkh`匹配得到對應的資料塊作為待驗證資料。同時，在對於資料塊的驗證過程中，需要使用到該資料塊的前一個資料塊的雜湊值，因此，資料庫服務端還可以獲取“前一個資料塊的雜湊值”作為輔助驗證資料，直接發送至客戶端。

又例如，當用戶發起第一種驗證指令，`VERIFY(Client, 'khash', &v)`，在客戶端中驗證指定的資料記錄是否存在帳本中。而在執行該驗證時，需要首先確定由資料塊中各資料記錄所構成的默克爾樹，進而確定出該資料記錄在默克爾樹中的默克爾路徑，換言之，需要使用到默克爾路徑上其它資料記錄的雜湊值和默克爾樹的根雜湊。此時資料庫服務端即可以將默克爾路徑上其它資料記錄的雜湊值和默克爾樹的根雜湊作為輔助驗證資料發送給客戶端，或者，直接將整個資料塊的內容作為富足驗證資料發送給客戶端（一般而言，在發起驗證的用戶方有權存取所有內容是才會這麼實現）。

在實際應用中，客戶端在資源不夠的時候，可以隨機的對帳本中的資料塊發起抽查，例如，隨機的指定資料塊塊高，在客戶端進行驗證；或者，挑選若干雜湊值，對雜湊值所對應的資料記錄在客戶端進行存在性驗證。在上述

抽查驗證都通過的時候，再發起在服務端的部分帳本驗證或者全帳本驗證；當然，在資源足夠的時候，也可以要求服務端將資料下發，在本地進行全量帳本驗證。實現在中心化的場景下，滿足用戶對於帳本完整性的要求，對中心化的帳本實現靈活的驗證。

相應地，本說明書實施例還提供一種塊鏈式帳本中的資料驗證系統，包括資料庫服務端和客戶端，所述資料庫服務端以中心化的方式透過塊鏈式帳本儲存資料，在所述系統中，

客戶端，發送包含驗證方式參數和驗證範圍參數的指令至資料庫服務端，其中，所述驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；所述驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

資料庫服務端，根據所述驗證範圍參數確定待驗證資料，所述待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

當所述驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證所述待驗證資料的完整性，並返回驗證結果至客戶端；

當所述驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回所述待驗證資料至客戶端，客戶端驗證所述待驗證資料的完整性，產生驗證結果。

進一步地，在所述系統中，當所述驗證範圍參數為雜

湊值時，資料庫服務端，查詢獲取雜湊值所對應的資料記錄，將所述資料記錄和/或所述資料記錄所處的資料塊確定為待驗證資料；或者，資料庫服務端，查詢獲取雜湊值所對應的資料塊，將所述資料塊確定為待驗證資料。

進一步地，在所述系統中，當所述驗證範圍參數為塊高時，資料庫服務端，確定塊高值所對應的資料塊，將所述資料塊確定為待驗證資料；或者，資料庫服務端，確定兩個塊高構成的區間所對應的部分/全量帳本，將所述部分/全量帳本確定為待驗證資料。

進一步地，在所述系統中，當所述驗證方式參數指示在客戶端進行驗證時，資料庫服務端，確定客戶端對待驗證資料進行驗證時所需要的其它輔助驗證資料，發送所述待驗證資料和其它輔助驗證資料至客戶端。

進一步地，在所述在中心化的資料庫服務端，資料塊透過如下方式預先產生：接收待儲存的資料記錄，確定各資料記錄的雜湊值，其中，資料記錄中包含指定標識欄位；當達到預設的成塊條件時，確定待寫入資料塊中的各資料記錄，產生包含資料塊的雜湊值和資料記錄的第N個資料塊，具體包括：

當 $N=1$ 時，初始資料塊的雜湊值和塊高基於預設方式給定；

當 $N>1$ 時，根據待寫入資料塊中的各資料記錄和第 $N-1$ 個資料塊的雜湊值確定第N個資料塊的雜湊值，產生包含第N個資料塊的雜湊值和各資料記錄的第N個資料塊，

其中，資料塊的塊高基於成塊時間的先後順序單調遞增。

進一步地，在所述系統中，所述預設的成塊條件包括：待儲存的資料記錄數量達到數量閾值；或者，距離上一次成塊時刻的時間間隔達到時間閾值。

相應地，本說明書實施例還提供一種塊鏈式帳本中的資料驗證方法，應用於以中心化的方式透過塊鏈式帳本儲存資料的資料庫服務端中，如圖3所示，圖3為本說明書實施例所提供的資料庫服務端方面的資料驗證方法的流程示意圖，包括：

S301，接收包含驗證方式參數和驗證範圍參數的指令，其中，所述驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；所述驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

S303，根據所述驗證範圍參數確定待驗證資料，所述待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

S305，當所述驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證所述待驗證資料的完整性，並返回驗證結果至客戶端；

S307，當所述驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回所述待驗證資料至客戶端，以便客戶端驗證所述待驗證資料的完整性。

相應地，本說明書實施例還提供一種塊鏈式帳本中的

資料驗證裝置，如圖4所示，圖4是本說明書實施例提供的資料庫服務端方面的一種塊鏈式帳本中的資料驗證裝置的結構示意圖，包括：

接收模組401，接收包含驗證方式參數和驗證範圍參數的指令，其中，所述驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；所述驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

確定模組403，根據所述驗證範圍參數確定待驗證資料，所述待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

驗證模組405，當所述驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證所述待驗證資料的完整性，並返回驗證結果至客戶端；

發送模組407，當所述驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回所述待驗證資料至客戶端，以便客戶端驗證所述待驗證資料的完整性。

本說明書實施例還提供一種電腦設備，其至少包括記憶體、處理器及儲存在記憶體上並可在處理器上運行的電腦程式，其中，處理器執行所述程式時實現圖2所示的塊鏈式帳本中的資料驗證控方法。

圖5示出了本說明書實施例所提供的一種更為具體的計算設備硬體結構示意圖，該設備可以包括：處理器1010、記憶體1020、輸入/輸出介面1030、通訊介面1040

和匯流排 1050。其中，處理器 1010、記憶體 1020、輸入/輸出介面 1030和通訊介面 1040透過匯流排 1050實現彼此之間在設備內部的通訊連接。

處理器 1010可以採用通用的 CPU(Central Processing Unit，中央處理器)、微處理器、特殊應用積體電路(Application Specific Integrated Circuit，ASIC)、或者一個或多個積體電路等方式實現，用於執行相關程式，以實現本說明書實施例所提供的技術方案。

記憶體 1020可以採用 ROM(Read Only Memory，唯讀記憶體)、RAM(Random Access Memory，隨機存取記憶體)、靜態儲存設備，動態儲存設備等形式實現。記憶體 1020可以儲存操作系統和其他應用程式，在透過軟體或者韌體來實現本說明書實施例所提供的技術方案時，相關的程式碼保存在記憶體 1020中，並由處理器 1010來呼叫執行。

輸入/輸出介面 1030用於連接輸入/輸出模組，以實現資訊輸入及輸出。輸入輸出/模組可以作為組件配置在設備中(圖中未示出)，也可以外接於設備以提供相應功能。其中，輸入裝置可以包括鍵盤、滑鼠、觸控螢幕、麥克風、各類感測器等，輸出設備可以包括顯示器、揚聲器、振動器、指示燈等。

通訊介面 1040用於連接通訊模組(圖中未示出)，以實現本設備與其他設備的通訊交互。其中通訊模組可以透過有線方式(例如，USB、纜線等)實現通訊，也可以透過無

線方式(例如行動網路、WIFI、藍牙等)實現通訊。

匯流排 1050 包括一通路，在設備的各個組件(例如，處理器 1010、記憶體 1020、輸入/輸出介面 1030 和通訊介面 1040)之間傳輸資訊。

需要說明的是，儘管上述設備僅示出了處理器 1010、記憶體 1020、輸入/輸出介面 1030、通訊介面 1040 以及匯流排 1050，但是在具體實施過程中，該設備還可以包括實現正常運行所必需的其他組件。此外，本領域的技術人員可以理解的是，上述設備中也可以僅包含實現本說明書實施例方案所必需的組件，而不必包含圖中所示的全部組件。

本說明書實施例還提供一種電腦可讀儲存媒體，其上儲存有電腦程式，該程式被處理器執行時實現圖 2 所示的塊鏈式帳本中的資料驗證方法。

電腦可讀媒體包括永久性和非永久性、可移動和非可移動式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，但不限於相變內部記憶體(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)、電可擦除可編程唯讀記憶體(EEPROM)、快閃記憶體或其他內部記憶體技術、唯讀光碟唯讀記憶體(CD-ROM)、數位多功能光碟(DVD)或其他光學儲存器、磁盒式磁帶，磁帶磁磁片儲存器或其他磁性

儲存設備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態性電腦可讀媒體 (transitory media)，如調變的資料信號和載波。

透過以上的實施方式的描述可知，本領域的技術人員可以清楚地瞭解到本說明書實施例可借助軟體加必需的通用硬體平台的方式來實現。基於這樣的理解，本說明書實施例的技術方案本質上或者說對現有技術做出貢獻的部分可以以軟體產品的形式體現出來，該電腦軟體產品可以儲存在儲存媒體中，如ROM/RAM、磁碟、光碟等，包括若干指令用以使得一台電腦設備(可以是個人電腦，伺服器，或者網路設備等)執行本說明書實施例各個實施例或者實施例的某些部分所述的方法。

上述實施例闡明的系統、方法、模組或單元，具體可以由電腦晶片或實體來實現，或者由具有某種功能的產品來實現。一種典型的實現設備為電腦，電腦的具體形式可以是個人電腦、膝上型電腦、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、可穿戴設備或者這些設備中的任意幾種設備的組合。

本說明書中的各個實施例均採用漸進的方式描述，各個實施例之間相同相似的部分互相參見即可，每個實施例重點說明的都是與其他實施例的不同之處。尤其，對於方法實施例而言，由於其基本相似於方法實施例，所以描述

得比較簡單，相關之處參見方法實施例的部分說明即可。以上所描述的方法實施例僅僅是示意性的，其中，所述作為分離部件說明的模組可以是或者也可以不是物理上分開的，在實施本說明書實施例方案時可以把各模組的功能在同一個或多個軟體和/或硬體中實現。也可以根據實際的需要選擇其中的部分或者全部模組來實現本實施例方案的目的。本領域普通技術人員在不付出創造性勞動的情況下，即可以理解並實施。

以上所述僅是本說明書實施例的具體實施方式，應當指出，對於本技術領域的普通技術人員來說，在不脫離本說明書實施例原理的前提下，還可以做出若干改進和潤飾，這些改進和潤飾也應視為本說明書實施例的保護範圍。

【符號說明】

S101:方法步驟

S103:方法步驟

S201:方法步驟

S203:方法步驟

S205:方法步驟

S301:方法步驟

S303:方法步驟

S305:方法步驟

S307:方法步驟

401:接收模組

403:確定模組

405:驗證模組

407:發送模組

1010:處理器

1020:記憶體

1030:輸入/輸出介面

1040:通訊介面

1050:匯流排

【發明申請專利範圍】

【請求項1】一種塊鏈式帳本中的資料驗證方法，應用於包括資料庫服務端和客戶端的系統中，該資料庫服務端以中心化的方式透過塊鏈式帳本儲存資料，該方法包括：

客戶端，發送包含驗證方式參數和驗證範圍參數的指令至資料庫服務端，其中，該驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；該驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

資料庫服務端根據該驗證範圍參數確定待驗證資料，該待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

當該驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證該待驗證資料的完整性，並返回驗證結果至客戶端；以及

當該驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回該待驗證資料至客戶端，客戶端驗證該待驗證資料的完整性，產生驗證結果。

【請求項2】如請求項1所述的方法，當該驗證範圍參數為雜湊值時，資料庫服務端根據該驗證範圍參數確定待驗證資料，包括：

資料庫服務端查詢獲取雜湊值所對應的資料記錄，將該資料記錄和/或該資料記錄所處的資料塊確定為待驗證

資料；或者

資料庫服務端查詢獲取雜湊值所對應的資料塊，將該資料塊確定為待驗證資料。

【請求項3】如請求項1所述的方法，當該驗證範圍參數為塊高時，資料庫服務端根據該驗證範圍參數確定待驗證資料，包括：

資料庫服務端確定塊高值所對應的資料塊，將該資料塊確定為待驗證資料；或者

資料庫服務端確定兩個塊高構成的區間所對應的部分/全量帳本，將該部分/全量帳本確定為待驗證資料。

【請求項4】如請求項1所述的方法，當該驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回該待驗證資料至客戶端，還包括：

資料庫服務端確定客戶端對待驗證資料進行驗證時所需要的其它輔助驗證資料，發送該待驗證資料和其它輔助驗證資料至客戶端。

【請求項5】如請求項1所述的方法，在該在中心化的資料庫服務端，資料塊透過如下方式預先產生：

接收待儲存的資料記錄，確定各資料記錄的雜湊值，其中，資料記錄中包含指定標識欄位；

當達到預設的成塊條件時，確定待寫入資料塊中的各資料記錄，產生包含資料塊的雜湊值和資料記錄的第N個資料塊，具體包括：

當N=1時，初始資料塊的雜湊值和塊高基於預設方式

給定；

當 $N > 1$ 時，根據待寫入資料塊中的各資料記錄和第 $N - 1$ 個資料塊的雜湊值確定第 N 個資料塊的雜湊值，產生包含第 N 個資料塊的雜湊值和各資料記錄的第 N 個資料塊，其中，資料塊的塊高基於成塊時間的先後順序而單調遞增。

【請求項 6】如請求項 5 所述的方法，該預設的成塊條件包括：

待儲存的資料記錄數量達到數量閾值；或者

距離上一次成塊時刻的時間間隔達到時間閾值。

【請求項 7】一種塊鏈式帳本中的資料驗證系統，包括資料庫服務端和客戶端，該資料庫服務端以中心化的方式透過塊鏈式帳本儲存資料，在該系統中，

客戶端，發送包含驗證方式參數和驗證範圍參數的指令至資料庫服務端，其中，該驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；該驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

資料庫服務端，根據該驗證範圍參數確定待驗證資料，該待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

當該驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證該待驗證資料的完整性，並返回驗證結果至客戶端；以及

當該驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回該待驗證資料至客戶端，客戶端驗證該待驗證資料的完整性，產生驗證結果。

【請求項8】如請求項7所述的系統，當該驗證範圍參數為雜湊值時，資料庫服務端根據該驗證範圍參數確定待驗證資料，包括：

資料庫服務端，查詢獲取雜湊值所對應的資料記錄，將該資料記錄和/或該資料記錄所處的資料塊確定為待驗證資料；或者

資料庫服務端，查詢獲取雜湊值所對應的資料塊，將該資料塊確定為待驗證資料。

【請求項9】如請求項7所述的系統，當該驗證範圍參數為塊高時，資料庫服務端根據該驗證範圍參數確定待驗證資料，包括：

資料庫服務端，確定塊高值所對應的資料塊，將該資料塊確定為待驗證資料；或者

資料庫服務端，確定兩個塊高構成的區間所對應的部分/全量帳本，將該部分/全量帳本確定為待驗證資料。

【請求項10】如請求項7所述的系統，當該驗證方式參數指示在客戶端進行驗證時，

資料庫服務端，確定客戶端對待驗證資料進行驗證時所需要的其它輔助驗證資料，發送該待驗證資料和其它輔助驗證資料至客戶端。

【請求項11】如請求項7所述的系統，在該在中心化

的資料庫服務端，資料塊透過如下方式預先產生：

接收待儲存的資料記錄，確定各資料記錄的雜湊值，其中，資料記錄中包含指定標識欄位；當達到預設的成塊條件時，確定待寫入資料塊中的各資料記錄，產生包含資料塊的雜湊值和資料記錄的第N個資料塊，具體包括：

當 $N=1$ 時，初始資料塊的雜湊值和塊高基於預設方式給定；

當 $N>1$ 時，根據待寫入資料塊中的各資料記錄和第 $N-1$ 個資料塊的雜湊值確定第N個資料塊的雜湊值，產生包含第N個資料塊的雜湊值和各資料記錄的第N個資料塊，其中，資料塊的塊高基於成塊時間的先後順序而單調遞增。

【請求項12】如請求項11所述的系統，該預設的成塊條件包括：

待儲存的資料記錄數量達到數量閾值；或者

距離上一次成塊時刻的時間間隔達到時間閾值。

【請求項13】一種塊鏈式帳本中的資料驗證方法，應用於以中心化的方式透過塊鏈式帳本儲存資料的資料庫服務端中，該方法包括：

接收包含驗證方式參數和驗證範圍參數的指令，其中，該驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；該驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

根據該驗證範圍參數確定待驗證資料，該待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

當該驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證該待驗證資料的完整性，並返回驗證結果至客戶端；以及

當該驗證方式參數指示在客戶端進行驗證時，資料庫服務端返回該待驗證資料至客戶端，以便客戶端驗證該待驗證資料的完整性。

【請求項 14】一種塊鏈式帳本中的資料驗證裝置，應用於以中心化的方式透過塊鏈式帳本儲存資料的資料庫服務端中，該裝置包括：

接收模組，接收包含驗證方式參數和驗證範圍參數的指令，其中，該驗證方式參數用於指示在資料庫服務端進行驗證，或者在客戶端進行驗證；該驗證範圍參數包括塊高或者雜湊值，用於確定帳本中待驗證的資料塊的範圍或者資料記錄；

確定模組，根據該驗證範圍參數確定待驗證資料，該待驗證資料包括資料記錄、資料塊、部分帳本或者全量帳本中的一者；

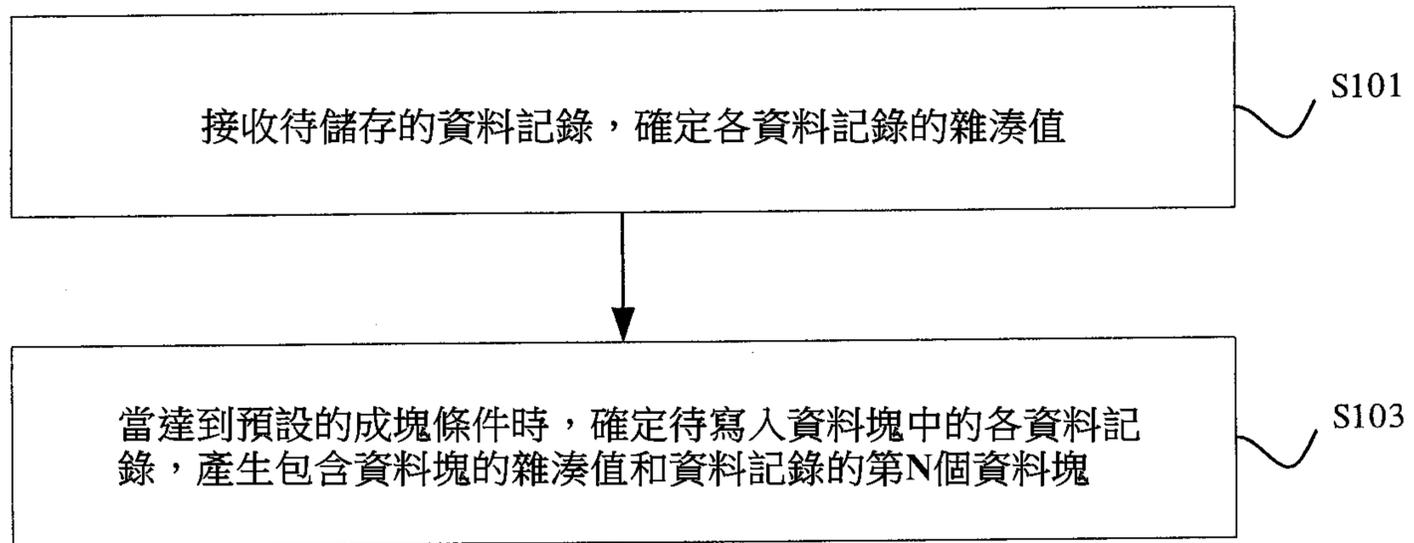
驗證模組，當該驗證方式參數指示在資料庫服務端進行驗證時，資料庫服務端驗證該待驗證資料的完整性，並返回驗證結果至客戶端；以及

發送模組，當該驗證方式參數指示在客戶端進行驗證

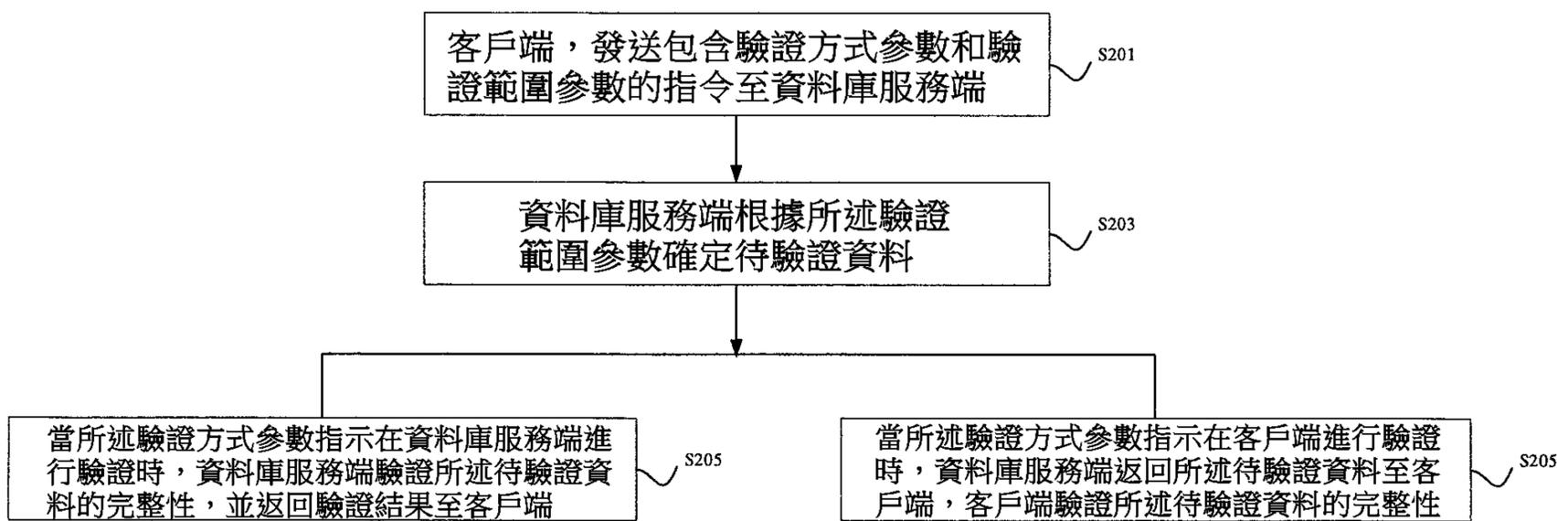
時，資料庫服務端返回該待驗證資料至客戶端，以便客戶端驗證該待驗證資料的完整性。

【請求項 15】一種電腦設備，包括記憶體、處理器及儲存在記憶體上並可在處理器上運行的電腦程式，其中，該處理器執行該程式時實現如請求項 13 所述的方法。

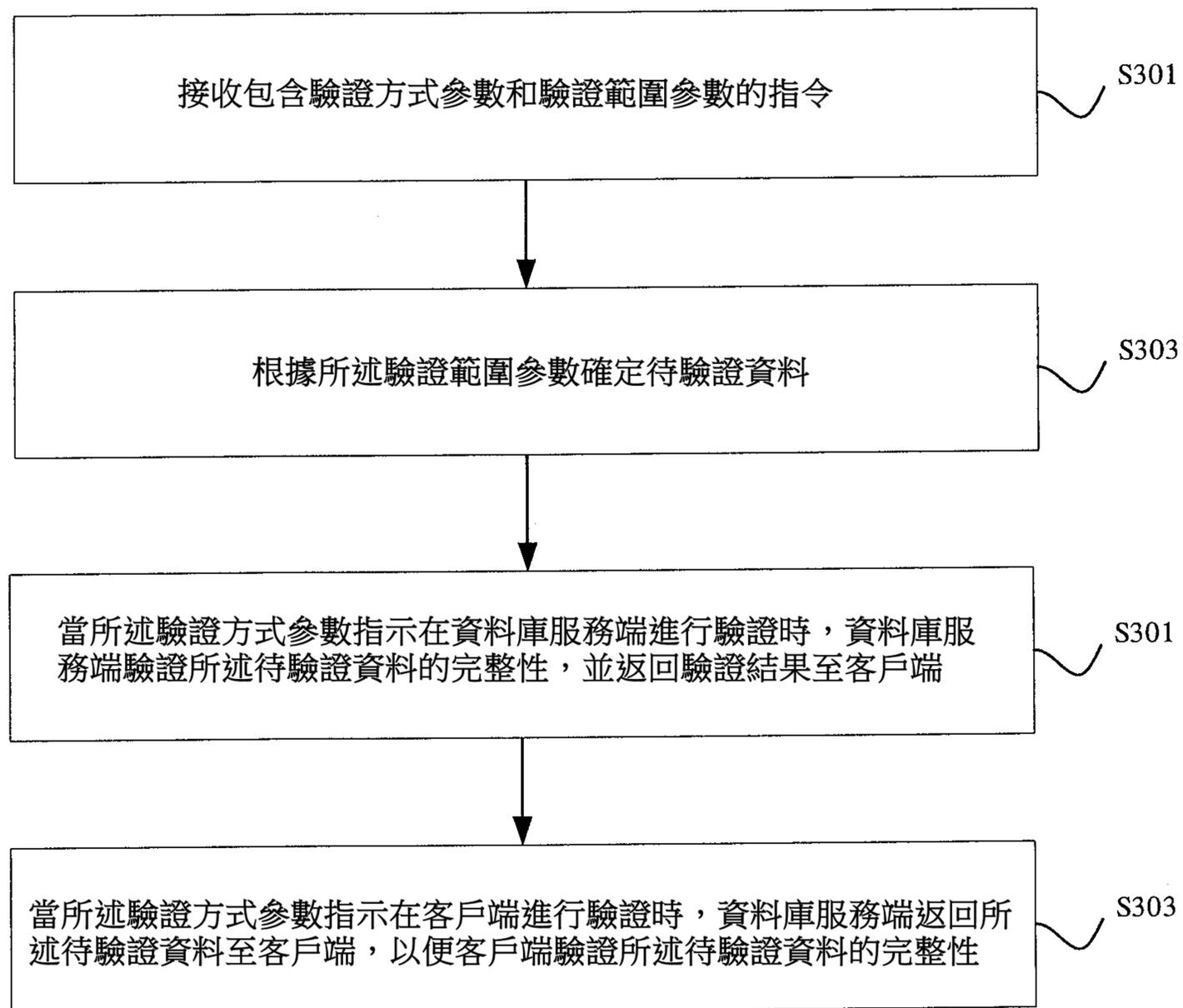
【發明圖式】



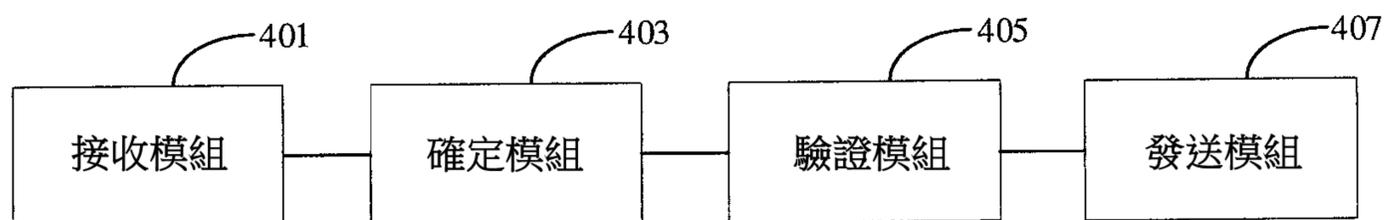
【圖 1】



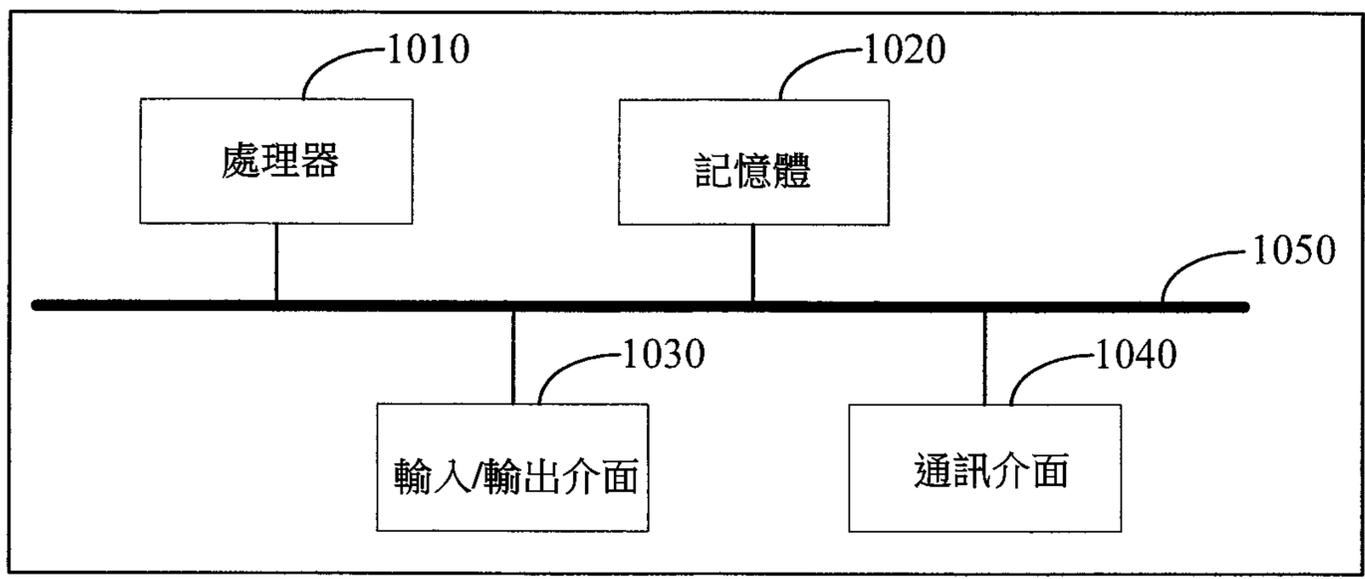
【圖 2】



【圖 3】



【圖 4】



【圖 5】