



(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 I684892 B

(45)公告日：中華民國 109 (2020) 年 02 月 11 日

(21)申請案號：107132935

(22)申請日：中華民國 107 (2018) 年 09 月 19 日

(51)Int. Cl.：

G06F21/64 (2013.01)**G06F21/30 (2013.01)****G06Q30/06 (2012.01)****G06Q20/40 (2012.01)****H04L29/06 (2006.01)****G06K7/00 (2006.01)**

(30)優先權：2017/11/23

中國大陸

201711185796.2

(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：王虎森 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW 201733304A

CN 106503994A

CN 107274184A

US 2016/0358165A1

審查人員：馮耀嘉

申請專利範圍項數：33 項 圖式數：12 共 63 頁

(54)名稱

資料處理方法和裝置

(57)摘要

本發明公開了一種資料處理方法和裝置。方法包括：區塊鏈中的交易發起節點首先確定交易的交易資料，以及其中的需要隱藏的信息；然後，將交易資料作為預定單向函數的輸入，獲取交易的交易根，並基於交易根建構需要隱藏的信息對應的證明資料；最後，在對交易根進行簽名後，發起將交易根和證明資料寫入區塊鏈的交易請求，由區塊鏈中的節點對交易根和證明資料進行共識驗證，並基於驗證結果響應/拒絕響應該交易請求。

指定代表圖：

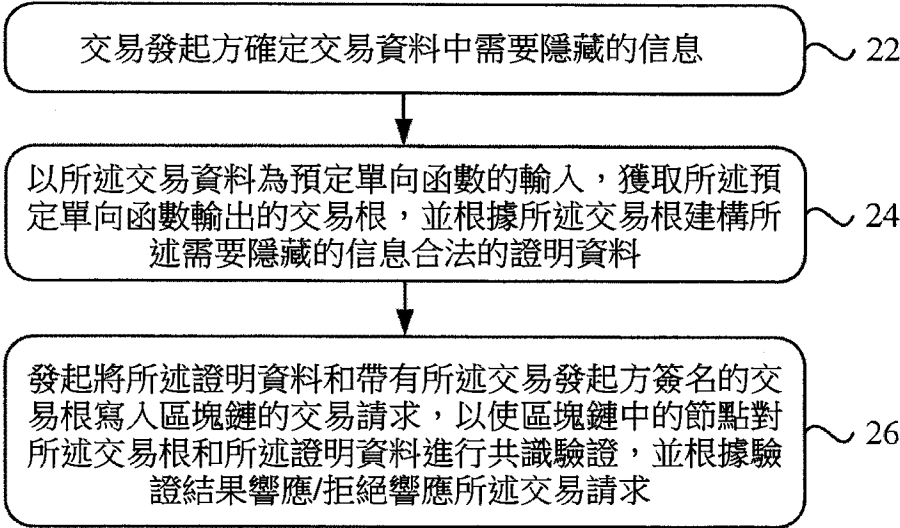


圖 2

【發明說明書】

【中文發明名稱】

資料處理方法和裝置

【技術領域】

本發明涉及電腦技術領域，尤其涉及一種資料處理方法和裝置。

【先前技術】

“區塊鏈”技術最初是由一位化名“中本聰”的人為一種數位貨幣-比特幣而設計出的一種特殊的分散式資料庫技術。它適合儲存簡單的、有先後關係的、能在系統內驗證的資料，並用密碼學和共識演算法保證了儲存的資料的不可篡改、不可偽造以及全網公開透明。

由於每個帳戶裡的資產、交易記錄都是公開的，因此，當任意一個帳戶獲取到其他帳戶的帳戶地址時，即可透過區塊鏈查詢到其他帳戶裡的所有資產和歷史交易。

需要提供更加可靠的方案。

【發明內容】

本說明書實施例提供一種資料處理方法和裝置，用於解決現有的區塊鏈技術容易出現資料被洩漏的問題。

本說明書實施例提供一種資料處理方法，包括：
交易發起方確定交易資料中需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發起將所述證明資料和帶有所述交易發起方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

可選的，在以所述交易資料為預定單向函數的輸入之前，還包括：

確定所述交易資料中的交易前的資料和交易後的資料；

其中，以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根包括：

以交易前的資料為第一預定單向函數的輸入，獲取所述第一預定單向函數輸出的輸入交易根；

以交易後的資料為第二預定單向函數的輸入，獲取所述第二預定單向函數輸出的輸出交易根；

將獲取的輸入交易根和輸出交易根作為待上鏈的交易根。

可選的，以交易後的資料為第二預定單向函數的輸入，獲取所述第二預定單向函數輸出的輸出交易根包括：

根據所述交易後的資料和隨機數建構預定單向函數樹的底層，並確定所述預定單向函數樹的頂層對應的輸出交易根。

可選的，所述根據所述交易根建構所述需要隱藏的信息合法的證明資料包括：

以所述交易根和所述需要隱藏的信息為輸入進行預定的邏輯運算；

以所述需要隱藏的信息為保護對象，對所述邏輯運算進行零知識證明，獲取證明資料。

本說明書實施例提供一種資料處理方法，包括：

接收交易發起方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

可選的，所述對所述交易根進行驗證包括：

驗證所述交易根是否有合法的簽名。

可選的，驗證所述交易根是否有合法的簽名包括：

確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；

若判斷獲知地址的數量為1，則驗證所述交易根是否有與所述交易發起方對應的簽名。

可選的，所述對所述交易根進行驗證包括：

驗證所述交易根中的輸出交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸出交易根為根據所述交易資料中交易後的資料建構的。

可選的，所述對所述交易根進行驗證包括：

驗證所述交易根中的輸入交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸入交易根為根據所述交易資料中交易前的資料建構的。

可選的，所述根據所述第一驗證結果和所述第二驗證結果確定響應/拒絕響應所述交易請求包括：

若所述第一驗證結果和所述第二驗證結果均為通過，則響應所述交易請求，以將帶有交易發起方簽名的交易根和證明資料寫入區塊鏈；

若所述第一驗證結果和/或所述第二驗證結果為未通過，則拒絕響應所述交易請求。

本說明書實施例提供一種資料處理方法，包括：

交易發起方確定交易資料中的需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

向交易接收方發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

本說明書實施例提供一種資料處理方法，包括：

交易接收方接收交易發送方發送的交易根和證明資料；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

若驗證結果為通過，則發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

本說明書實施例提供一種資料處理方法，包括：

接收交易接收方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易發起方發起的交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

可選的，所述對所述交易根進行驗證包括：

確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料

建構的；

若判斷獲知地址的數量為大於等於預定閾值，則驗證所述交易根是否攜帶有與所述交易發起方和所述交易接收方對應的簽名。

本說明書實施例提供一種資料處理裝置，包括：

確定單元，用於確定交易資料中需要隱藏的信息；

處理單元，用於以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發起單元，用於發起將所述證明資料和帶有所述交易發起方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

可選的，所述確定單元，還用於確定所述交易資料中的交易前的資料和交易後的資料；

其中，所述處理單元，具體用於以交易前的資料為第一預定單向函數的輸入，獲取所述第一預定單向函數輸出的輸入交易根；以交易後的資料為第二預定單向函數的輸入，獲取所述第二預定單向函數輸出的輸出交易根；將獲取的輸入交易根和輸出交易根作為待上鏈的交易根。

可選的，所述處理單元，具體用於根據所述交易後的資料和隨機數建構預定單向函數樹的底層，並確定所述預定單向函數樹的頂層對應的輸出交易根。

可選的，所述處理單元，具體用於以所述交易根和所

述需要隱藏的信息為輸入進行預定的邏輯運算；以所述需要隱藏的信息為保護對象，對所述邏輯運算進行零知識證明，獲取證明資料。

本說明書實施例提供一種資料處理裝置，包括：

接收單元，用於接收交易發起方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

驗證單元，用於對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

響應單元，用於根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

可選的，所述驗證單元，具體用於驗證所述交易根是否有合法的簽名。

可選的，所述驗證單元，具體用於確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；若判斷獲知地址的數量為1，則驗證所述交易根是否有與所述交易發起方對應的簽名。

可選的，所述驗證單元，具體用於驗證所述交易根中的輸出交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸出交易根為根據所述交易資料中交易後的資料建構的。

可選的，所述驗證單元，具體用於驗證所述交易根中的輸入交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸入交易根為根據所述交易資料中交易前的資料建構的。

可選的，所述響應單元，具體用於若所述第一驗證結果和所述第二驗證結果均為通過，則響應所述交易請求，以將帶有交易發起方簽名的交易根和證明資料寫入區塊鏈；若所述第一驗證結果和/或所述第二驗證結果為未通過，則拒絕響應所述交易請求。

本說明書實施例提供一種資料處理裝置，包括：

確定單元，用於交易發起方確定交易資料中的需要隱藏的信息；

處理單元，用於以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發送單元，用於向交易接收方發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

本說明書實施例提供一種資料處理裝置，包括：

接收單元，用於接收交易發送方發送的交易根和證明資料；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏

的信息；

驗證單元，用於根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

發起單元，用於若驗證結果為通過，則發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

本說明書實施例提供一種資料處理裝置，包括：

接收單元，用於接收交易接收方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易發起方發起的交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

驗證單元，用於對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

響應單元，用於根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

可選的，所述驗證單元，具體用於確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；若判斷獲知地址的數量為大於等於預定閾值，則驗證所述交易根是否攜帶有與所述交易發起方和所述交易接收方對應的簽名。

本說明書實施例提供一種資料處理裝置，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：

確定交易資料中需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發起將所述證明資料和帶有所述交易發起方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

本說明書實施例提供一種資料處理裝置，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：

接收交易發起方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

本說明書實施例提供一種資料處理裝置，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：

確定交易資料中的需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

向交易接收方發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

本說明書實施例提供一種資料處理裝置，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：

接收交易發送方發送的交易根和證明資料；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

若驗證結果為通過，則發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證

明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

本說明書實施例提供一種資料處理裝置，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：

接收交易接收方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易發起方發起的交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

本說明書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：

可見，本實施例首先透過單向函數保證交易資料的真實性和不可篡改，然後，透過建構證明資料來證明需要隱藏的信息的合法性，而又不會向非交易參與方透露任何需要隱藏的信息。與現有中任意一個節點的資料被洩漏將會導致所有資料被洩漏的方案相比，基本是節點中的資料被洩漏，攻擊者依然無法查看到各方節點的隱私資料，因此，能達到提高區塊鏈資料安全性的目的。

【圖式簡單說明】

此處所說明的附圖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。在附圖中：

圖 1a 和圖 1b 為本說明書實施例提供的一種資料處理方法的應用場景示意圖；

圖 2 為本說明書實施例 1 提供的一種資料處理方法的流程示意圖；

圖 3 為本說明書實施例 2 提供的一種資料處理方法的流程示意圖；

圖 4 為本說明書實施例 3 提供的一種資料處理方法的流程示意圖；

圖 5 為本說明書實施例 4 提供的一種資料處理方法的流程示意圖；

圖 6a 為本說明書實施例 5 提供的一種資料處理方法中建構交易根的流程示意圖；

圖 6b 為本說明書實施例 5 提供的一種資料處理方法中建構證明資料的流程示意圖；

圖 7 為本說明書實施例 6 提供的一種資料處理裝置的結構示意圖；

圖 8 為本說明書實施例 7 提供的一種資料處理裝置的結構示意圖；

圖9為本說明書實施例8提供的一種資料處理裝置的結構示意圖；

圖10為本說明書實施例9提供的一種資料處理裝置的結構示意圖；

圖11為本說明書實施例10提供的一種資料處理裝置的結構示意圖；

圖12為本說明書實施例11提供的一種電子設備的結構示意圖。

【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附圖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。

需要說明的是，單向函數為，滿足對於所有屬於 f 定義域的任一 x ，可以很容易計算 $f(x)=y$ ；對於幾乎所有屬於 f 值域的任一 y ，則在計算上不可能求出 x 使得 $y=f(x)$ 。即：對於任何輸入，容易計算輸出，但是已知輸出，很難推斷輸入。

零知識證明為，證明者能夠在不向驗證者提供任何有用的信息(受保護/隱藏信息)的情況下，使驗證者相信某個論斷是正確的。

參見圖 1a，本發明的一個應用場景可以為：

區塊鏈上的節點 A 需要將一筆錢由節點 A 對應的交易發起方的第一帳戶轉帳至該交易發起方的第二帳戶，或者，將第一帳戶和第二帳戶進行合併。在將轉帳/合併以交易的形式請求寫入區塊鏈之前，節點 A 先確定該交易的交易資料中的需要隱藏的信息，例如：第一帳戶和第二帳戶的輸入(如：交易前的餘額)、輸出(如：交易後的餘額)等。然後，計算出該交易的交易根，並基於交易根建構需要隱藏的信息的證明資料，以證明需要隱藏的信息的合法性、真實性等。然後，將交易根和證明資料以交易的形式請求寫入區塊鏈中。

不難理解的是，區塊鏈允許同一個人申請多個帳戶，但區塊鏈是簽名機制為每人分配唯一對應的簽名。因此，在交易發生在同一人 A 的不同帳戶之間時，交易僅有 A 的簽名即可。

參見圖 1b，本發明的另一個應用場景可以為：

區塊鏈上的節點 A 需要將一筆錢由交易發起方轉帳至節點 B 對應的交易接收方。在將轉帳以交易的形式請求寫入區塊鏈之前，節點 A 先確定該交易的交易資料中的需要隱藏的信息，例如：交易發起方和交易接收方的輸入、輸出，交易發起方和交易接收方的餘額等。然後，計算出該交易的交易根，並基於交易根建構需要隱藏的信息的證明資料，以證明需要隱藏的信息的有效性、真實性等。然後，將交易根和證明資料發送至交易接收方，由交易接收

方對交易根進行驗證，若驗證無誤，則由交易接收方對交易根簽名後，發起將證明資料和帶有交易發起方、交易接收方簽名的交易根寫入區塊鏈的交易請求。或者，交易接收方在對交易根簽名後，將簽名後的交易根+驗證結果返回給交易發起方，以指示交易發起方發起將證明資料和帶有交易發起方、交易接收方簽名的交易根寫入區塊鏈的交易請求。

其中，在上述兩個應用場景中，轉帳或者合併均是為了便於理解“交易”而做出的示例，但實際上，“交易”還可以為在節點A中記錄一條信息、節點A將一條信息發送給節點B等等，相應地，“需要隱藏的信息”也可自由設置，例如：交易雙方的餘額等，此處不做限定。

以下結合附圖，詳細說明本發明各實施例提供的技術方案。

實施例1

圖2為本說明書實施例1提供的一種資料處理方法的流程示意圖，該方法可由區塊鏈中的參與交易的節點來執行，具體可以包括如下步驟：

步驟22、交易發起方確定交易資料中需要隱藏的信息；

需要說明的是，步驟22的一種實現方式可以為：

節點獲取交易發起方(用戶)完成的交易清單，交易清單中記載有選項以及選項對應的內容，例如：收款人、付

款人、收款人交易前後餘額、付款人交易前後餘額等。然後，基於預定的隱藏規則，從中選取出對應的信息。

其中，隱藏規則可以為：基於預設置的隱藏選項，確定交易清單中與隱藏選項對應的選項及其內容，並作為需要隱藏的信息。隱藏選項舉例為：收款人交易前後餘額、付款人交易前後餘額。

隱藏規則還可以為：基於預設置的篩選規則，從交易清單中選出與特定關鍵詞對應的資料，例如：特定關鍵詞為“餘額”或者“交易額”，則篩選出的對應的數字，並將篩選出的資料作為需要隱藏的信息。

需要說明的是，步驟22的另一種實現方式可以為：

交易發起方在完成交易清單的過程中，自定義該交易清單中需要隱藏的資料並進行標記。例如：標記收款人交易前後餘額、付款人交易前後餘額。

則節點在獲取到交易發起方完成交易清單後，基於標記確定交易資料中需要隱藏的信息。

步驟24、以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

需要說明的是，步驟24中建構交易根的一種實現方式可以為：

首先，節點基於交易資料對應的交易清單，對交易資料進行解析，以確定其中的交易前的資料和交易後的資料。例如：收款人交易前後餘額、付款人交易前後餘額。

然後，將交易前的資料作為第一預定單向函數的輸入，獲取所述第一預定單向函數輸出的輸入交易根；將交易後的資料作為第二預定單向函數的輸入，獲取所述第二預定單向函數輸出的輸出交易根。其中，第一預定單向函數和第二預定單向函數可以為同一單向函數。

其中，單向函數可以為單向函數樹，相應地，建構輸入交易根/輸出交易根的步驟可以具體為：根據交易前後的資料和隨機數建構預定單向函數樹的底層，並確定所述預定單向函數樹的頂層對應的輸入交易根/輸出交易根。例如：透過在交易前後的餘額後面添加固定長度的隨機數，比如定義一個128bit的數字，前10bit表示餘額，後面的bit為隨機數。

不難理解的是，輸入交易根和輸出交易根的數量為至少一個。例如：(rootA(葉節點為A的帳戶餘額100)，rootB(葉節點為B的帳戶餘額800)，rootA'(葉節點為A的帳戶餘額50)，rootB'(葉節點為B的帳戶餘額950)。其中，rootA和rootB為輸入交易根，rootA'和rootB'未輸出交易根。另外，在建構交易根的過程中，添加隨機數的作用是為了區分每個輸入交易根和輸出交易根，以在後續共識節點對其進行驗證時，以防止碰撞。

步驟24中建構證明資料的一種實現方式可以為：

以所述交易根和所述需要隱藏的信息為輸入進行預定的邏輯運算；以所述需要隱藏的信息為保護對象，對所述邏輯運算進行零知識證明，獲取證明資料。

需要說明的是，預定的邏輯運算可以為根據需要證明的內容而自定義的特定函數。例如：當需要證明交易發起方的第一帳戶與第二帳戶之間發生了交易時，則特定函數可以具體為以交易根和需要隱藏的信息為輸入，計算交易前的第一帳戶、第二帳戶的餘額和交易後的第一帳戶、第二帳戶的餘額是否相同，或者，交易前的餘額與交易後的餘額差值不超過 n 元，交易後第二帳戶的利息發生了增長了等等。然後，將整個函數運算過程用零知識證明的方式輸出一個證明，即證明隱藏的信息可以用來計算特定函數。

步驟26、發起將所述證明資料和帶有所述交易發起方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

可見，本實施例首先透過單向函數保證交易資料的真實性和不可篡改，然後，透過建構證明資料來證明需要隱藏的信息的合法性，而又不會向非交易參與方透露任何需要隱藏的信息。與現有技術相比，能有效防止由於任意一個節點的資料被洩漏而影響到整個區塊鏈資料的隱私，達到提高區塊鏈資料安全性的目的。

實施例2

圖3為本說明書實施例2提供的一種資料處理方法的流程示意圖，該方法可由區塊鏈中的共識節點執行，具體可

以包括如下步驟：

步驟32、接收交易發起方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

需要說明的是，步驟32可以為在實施例1的基礎上進行的步驟，其中的交易請求、交易根和證明資料等在實施例1中均有相關描述，故，此處不再對其進行贅述。

步驟34、對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

步驟34中驗證交易根的一種實現方式可以為：

驗證所述交易根是否有合法的簽名，若是，則第一驗證結果為通過，若否，則第一驗證結果為未通過。

具體地，首先，確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；若判斷獲知地址的數量為1，則驗證所述交易根是否有與所述交易發起方對應的簽名。

不難理解的是，每個輸出交易根均對應一個地址 hash(pk) ，基於該地址可判定此交易的參與方有哪些，然後，驗證交易根是否有所有參與方的簽名且合法。例如：地址只有1個，則可以認為是同一用戶的不同帳戶之間的交易。進而若驗證出該用戶的簽名無誤，則第一驗證結果為通過。

另外，對於簽名的驗證涉及區塊鏈的數位簽名機制，此處不做限定。

步驟34中驗證交易根的另一種實現方式可以為：

在步驟34中驗證交易根的上一種實現方式的基礎上，本實現方式還進一步地：

驗證所述交易根中的輸出交易根與已上鏈的輸出交易根和輸入交易根是否重複，若是，則確定第一驗證結果為未通過，若否，且有合法簽名，則確定第一驗證結果為通過。

具體的，驗證輸出交易根的目的是避免出現“碰撞”。此處的碰撞可以理解為：存在與該輸出交易根具有同一(用戶)簽名且相同的輸入交易根或輸出交易根，導致的無法判定交易根對應的“錢”是用戶未“花”的“錢”，還是該用戶之前已經“花”了的“錢”。

而由於在建構輸出交易根時，向交易後的資料中添加了隨機數，因此，得出的輸出交易根具有唯一性。進而，可對比處該輸出交易根與已經上鏈的輸出交易根和輸出交易根是否重複，並基於對比結果判定是否發生碰撞。

步驟34中驗證交易根的另一種實現方式可以為：

在上一實現方式的基礎上，進一步地驗證所述交易根中的輸入交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸入交易根為根據所述交易資料中交易前的資料建構的。

本實現方式中，驗證輸入交易根的目的在於避免“雙

花”。此處的“雙花”可以理解為：用戶將輸入交易根對應的“錢”同時交易給其他兩個用戶。由於其避免方式與驗證輸出交易根的方式相似，故，此處不再贅述。

對於步驟34的後兩種實現方式，節點區分輸入交易根和輸出交易根的方式可以為：存在未花費的交易輸出(Unspent Transaction Outputs, UTXO)的交易根為輸入交易根，其餘則為輸出交易根。

步驟34中驗證證明資料的一種實現方式可以為：

共識節點基於交易根用零知識證明演算法驗證證明資料，若驗證通過，則確定證明無誤。

步驟36、根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

需要說明的是，若所述第一驗證結果和所述第二驗證結果均為通過，則響應所述交易請求，以將帶有交易發起方簽名的交易根和證明資料寫入區塊鏈；若所述第一驗證結果和/或所述第二驗證結果為未通過，則拒絕響應所述交易請求。

可見，本實施例首先通過單向函數保證交易資料的真實性和不可篡改，然後，透過建構證明資料來證明需要隱藏的信息的合法性，而又不會向非交易參與方透露任何需要隱藏的信息。與現有技術相比，能有效防止由於任意一個節點的資料被洩漏而影響到整個區塊鏈資料的隱私，達到提高區塊鏈資料安全性的目的。

實施例3

圖4為本說明書實施例3提供的一種資料處理方法的流程示意圖，參見圖4，該方法可以有區塊鏈中的節點執行，具體包括如下

步驟42、交易節點A(交易發起方)確定交易資料中的需要隱藏的信息；

步驟44、交易節點A以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

步驟46、交易節點A向交易節點B(交易接收方)發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

步驟48、交易節點B根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

步驟410、交易節點B確定驗證是否通過；

步驟412、若驗證結果為通過，則交易節點B發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

步驟414、共識節點對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，

獲取第二驗證結果；

步驟414的一種實現方式可以為：

確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；若判斷獲知地址的數量為大於等於預定閾值，則驗證所述交易根是否攜帶有與所述交易發起方和所述交易接收方對應的簽名。其中，預定閾值可以具體為2。

不難理解的是，每個輸出交易根均有對應的地址，基於地址確定參與交易的節點，進而驗證參與交易的節點是否都有在交易根上簽名，若是且簽名合法，則第一驗證結果為通過。

步驟416、根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

可見，本實施例首先透過單向函數保證交易資料的真實性和不可篡改，然後，透過建構證明資料來證明需要隱藏的信息的合法性，而又不會向非交易參與方透露任何需要隱藏的信息。與現有技術相比，能有效防止由於任意一個節點的資料被洩漏而影響到整個區塊鏈資料的隱私，達到提高區塊鏈資料安全性的目的。

實施例4

圖5為本說明書實施例4提供的一種資料處理方法的流程示意圖，參見圖5，該方法可以有區塊鏈中的節點執行，具體包括如下

步驟 52、交易節點 A(交易發起方)確定交易資料中的需要隱藏的信息；

步驟 54、交易節點 A 以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

步驟 56、交易節點 A 向交易節點 B(交易接收方)發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

步驟 58、交易節點 B 根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

步驟 510、交易節點 B 確定驗證是否通過；

步驟 512、若驗證結果為通過，則交易節點 B 對交易根進行簽名，並向交易節點 A 發送允許上鏈的指示信息；

步驟 514、交易節點 A 發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

步驟 516、共識節點對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

步驟 518、根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

可見，本實施例首先透過單向函數保證交易資料的真

實性和不可篡改，然後，透過建構證明資料來證明需要隱藏的信息的合法性，而又不會向非交易參與方透露任何需要隱藏的信息。與現有技術相比，能有效防止由於任意一個節點的資料被洩漏而影響到整個區塊鏈資料的隱私，達到提高區塊鏈資料安全性的目的。

實施例5

結合圖6a和6b，下面以實例的方式對本說明書進行詳細說明，具體可以包括如下步驟：

步驟S62、參見圖6a，在交易上鏈前，區塊鏈中的交易組織為分層的單向函數結構，最底層採用的是交易的明文，交易發起方透過單向函數做成樹狀，最後形成一個交易根root。其中，明文可以作為需要隱藏的信息。

不難理解的是，因為所有交易內容都透過單向函數來組織，所以把交易根上鏈不會洩漏任何資料隱私。

當然，交易組織格式也可以是非樹狀的任何單向函數形式。

步驟S64、參見圖6b，假如需要利用交易資料計算特定函數f，f需要同時輸入作為隱藏信息的交易1(交易根為root)的資料2、交易2(交易根為root')的資料3'、交易3(交易根為root'')的資料1''，即

運算結果=f(資料2，資料3'，資料1'')

root=交易根(資料2)

root'=交易根(資料3')

$\text{root}'' = \text{交易根(資料1}'')$

那麼，可以透過零知識證明，交易發起方證明以上所有陳述的正確性，但是又不洩漏資料2、資料3'、資料1''。

需要說明的是，特定函數 f 為基於需要證明的隱藏的信息自定義的函數，以能起到證明為準，函數類型不限。例如：以交易雙方的交易前的餘額和交易後的餘額為輸入，計算兩者的差值；或者，以交易發起方的交易前後的餘額為輸入，計算交易發起方的交易前後的餘額差值不超過 m 等等。

步驟S66、接收方(交易接收方或者區塊鏈中的非交易參與節點)接收到證明後，利用零知識證明驗證該證明的正確性，因而是確信了運算結果的正確性。

但是接收方只知道運算結果，假如運算函數本身不洩漏除運算結果的信息，那麼接收方不會知道函數的輸入資料信息。

可見，本實施例可以用於一方向另外一方證明已上鏈交易的內容可以用來計算特定函數，但是該函數的運算又不暴露任何一方資料隱私。區塊鏈透過單向函數保證資料內容的真實性和不可篡改，零知識證明保證資料運算過程滿足雙方實現約定的特定函數、以及該資料確實存在已經上鏈的交易。

對於上述方法實施方式，為了簡單描述，故將其都表述為一系列的動作組合，但是本領域技術人員應該知悉，

本發明實施方式並不受所描述的動作順序的限制，因為依據本發明實施方式，某些步驟可以採用其他順序或者同時進行。其次，本領域技術人員也應該知悉，說明書中所描述的實施方式均屬於較佳實施方式，所涉及的動作並不一定是本發明實施方式所必須的。

實施例6

圖7為本說明書實施例6提供的一種資料處理裝置的結構示意圖，參見圖7，該裝置具體可以包括：確定單元71、處理單元72和發起單元73，其中：

確定單元71，用於確定交易資料中需要隱藏的信息；

處理單元72，用於以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發起單元73，用於發起將所述證明資料和帶有所述交易發起方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

本實施例中，確定單元71，還用於確定所述交易資料中的交易前的資料和交易後的資料；

相應地，所述處理單元72，具體用於以交易前的資料為第一預定單向函數的輸入，獲取所述第一預定單向函數輸出的輸入交易根；以交易後的資料為第二預定單向函數的輸入，獲取所述第二預定單向函數輸出的輸出交易根；

將獲取的輸入交易根和輸出交易根作為待上鏈的交易根。

處理單元72，具體用於根據所述交易後的資料和隨機數建構預定單向函數樹的底層，並確定所述預定單向函數樹的頂層對應的輸出交易根。

處理單元72，具體用於以所述交易根和所述需要隱藏的信息為輸入進行預定的邏輯運算；以所述需要隱藏的信息為保護對象，對所述邏輯運算進行零知識證明，獲取證明資料。

實施例7

圖8為本說明書實施例7提供的一種資料處理裝置的結構示意圖，參見圖8，該裝置具體可以包括：接收單元81、驗證單元82和響應單元83，其中：

接收單元81，用於接收交易發起方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

驗證單元82，用於對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

響應單元83，用於根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

其中，所述驗證單元82的工作原理可以為：

驗證所述交易根是否有合法的簽名。具體地：確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；若判斷獲知地址的數量為1，則驗證所述交易根是否有與所述交易發起方對應的簽名。

驗證所述交易根中的輸出交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸出交易根為根據所述交易資料中交易後的資料建構的。

驗證所述交易根中的輸入交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸入交易根為根據所述交易資料中交易前的資料建構的。

響應單元83的工作原理可以為：

若所述第一驗證結果和所述第二驗證結果均為通過，則響應所述交易請求，以將帶有交易發起方簽名的交易根和證明資料寫入區塊鏈；若所述第一驗證結果和/或所述第二驗證結果為未通過，則拒絕響應所述交易請求。

實施例8

圖9為本說明書實施例8提供的一種資料處理裝置的結構示意圖，參見圖9，該裝置具體可以包括：確定單元91、處理單元92和發送單元93，其中：

確定單元91，用於交易發起方確定交易資料中的需要隱藏的信息；

處理單元92，用於以所述交易資料為預定單向函數的

輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發送單元 93，用於向交易接收方發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

實施例 9

圖 10 為本說明書實施例 9 提供的一種資料處理裝置的結構示意圖，參見圖 10，該裝置具體可以包括：接收單元 101、驗證單元 102 和發起單元 103，其中：

接收單元 101，用於接收交易發送方發送的交易根和證明資料；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

驗證單元 102，用於根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

發起單元 103，用於若驗證結果為通過，則發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

實施例 10

圖 11 為本說明書實施例 10 提供的一種資料處理裝置的結構示意圖，參見圖 11，該裝置具體可以包括：接收單元 111、驗證單元 112 和響應單元 113，其中：

接收單元 111，用於接收交易接收方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易發起方發起的交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

驗證單元 112，用於對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

響應單元 113，用於根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

其中，驗證單元 112，具體用於確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；若判斷獲知地址的數量為大於等於預定閾值，則驗證所述交易根是否攜帶有與所述交易發起方和所述交易接收方對應的簽名。

對於上述裝置實施方式而言，由於其與方法實施方式基本相似，所以描述的比較簡單，相關之處參見方法實施方式的部分說明即可。

應當注意的是，在本發明的裝置的各個部件中，根據其要實現的功能而對其中的部件進行了邏輯劃分，但是，

本發明不受限於此，可以根據需要對各個部件進行重新劃分或者組合。

實施例 11

圖 12 為本說明書實施例 11 提供的一種電子設備的結構示意圖，參見圖 12，該電子設備包括處理器、內部匯流排、網路介面、記憶體以及非易失性記憶體，當然還可能包括其他業務所需要的硬體。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，在邏輯層面上形成資料處理裝置。當然，除了軟體實現方式之外，本說明書並不排除其他實現方式，比如邏輯裝置抑或軟硬體結合的方式等等，也就是說以下處理流程的執行主體並不限定於各個邏輯單元，也可以是硬體或邏輯裝置。

網路介面、處理器和記憶體可以透過匯流排系統相互連接。匯流排可以是 ISA(Industri=Standard Architecture，工業標準體系結構)匯流排、PCI(Peripheral Component Interconnect，週邊元件互連標準)匯流排或 EISA(Extended Industri=Standard Architecture，擴展工業標準結構)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。記憶體可以包括唯讀記憶體和隨機存取記憶體，並向處理器提供指令和資料。

記憶體可能包含高速隨機存取記憶體 (Random-Access Memor=, RAM)，也可能還包括非易失性記憶體 (non-volatile memor=)，例如至少1個磁碟記憶體。

處理器，用於執行所述記憶體存放的程式，並具體執行：

確定交易資料中需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發起將所述證明資料和帶有所述交易發起方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

還用於，

接收交易發起方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

還用於，

確定交易資料中的需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

向交易接收方發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

還用於，

接收交易發送方發送的交易根和證明資料；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

若驗證結果為通過，則發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

還用於，

接收交易接收方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易發起方發起的交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

上述如本說明書圖2-10所示實施例揭示的資料處理裝置或管理者(Master)節點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透過處理器中的硬體的集成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；還可以是數位信號處理器(Digital Signal Processor，DSP)、專用積體電路(Application Specific Integrated Circuit，ASIC)、場可程式閘陣列(Field-Programmable Gate Arra=，FPGA)或者其他可程式邏輯裝置、分立閘或者電晶體邏輯裝置、分立硬體組件。可以實現或者執行本說明書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用的處理器等。結合本說明書實施例所公開的方法的步驟可以直接體現為硬體譯碼處理器執行完成，或者用譯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，可程式唯讀記憶體或者電可抹除可程式記憶體、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信息，結合其硬體完成上述方法的步驟。

資料處理裝置還可執行圖2-圖5的方法，並實現管理者節點執行的方法。

實施例12

基於相同的發明創造，本說明書實施例還提供了一種電腦可讀儲存媒體，所述電腦可讀儲存媒體儲存一個或多個程式，所述一個或多個程式當被包括多個應用程式的電子設備執行時，使得所述電子設備執行實施例1-5提供的資料處理方法。

本說明書中的各個實施例均採用遞進的方式描述，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，對於系統實施例而言，由於其基本相似於方法實施例，所以描述的比較簡單，相關之處參見方法實施例的部分說明即可。

上述對本說明書特定實施例進行了描述。其它實施例在所附申請專利範圍的範圍內。在一些情況下，在申請專利範圍中記載的動作或步驟可以按照不同於實施例中的順序來執行並且仍然可以實現期望的結果。另外，在附圖中描繪的過程不一定要求示出的特定順序或者連續順序才能實現期望的結果。在某些實施方式中，多任務處理和平行處理也是可以的或者可能是有利的。

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資料處理設備的處理器以產生一個機器，使得透過電腦或其他可程式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資料處理設備上，使得在電腦或其他可程式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信息儲存。信息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）、電可抹除可程式唯讀記憶體（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）或其他光學儲存器、磁盒式磁帶，磁帶磁碟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信息。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（transitor= 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權利要求範圍之內。

【符號說明】

22：步驟

24：步驟

26：步驟

32：步驟

34：步驟

36：步驟

71：確定單元

72：處理單元

73：發起單元

81：接收單元

82：驗證單元

83：響應單元

91：確定單元

92：處理單元

93：發送單元

101：接收單元

102：驗證單元

103：發起單元

111：接收單元

112：驗證單元

113：響應單元



I684892

【發明摘要】

【中文發明名稱】

資料處理方法和裝置

【中文】

本發明公開了一種資料處理方法和裝置。方法包括：區塊鏈中的交易發起節點首先確定交易的交易資料，以及其中的需要隱藏的信息；然後，將交易資料作為預定單向函數的輸入，獲取交易的交易根，並基於交易根建構需要隱藏的信息對應的證明資料；最後，在對交易根進行簽名後，發起將交易根和證明資料寫入區塊鏈的交易請求，由區塊鏈中的節點對交易根和證明資料進行共識驗證，並基於驗證結果響應/拒絕響應該交易請求。

【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

【發明圖式】

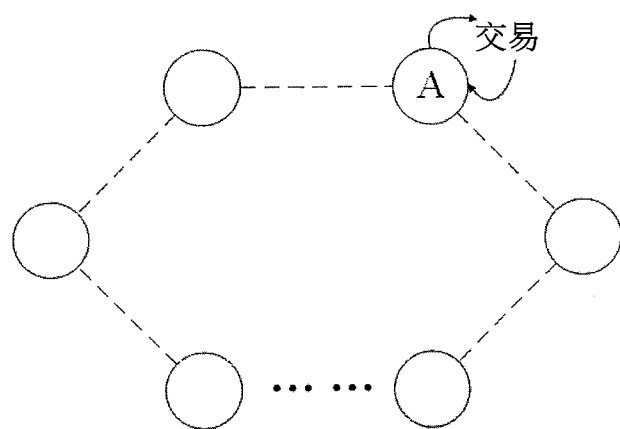


圖 1a

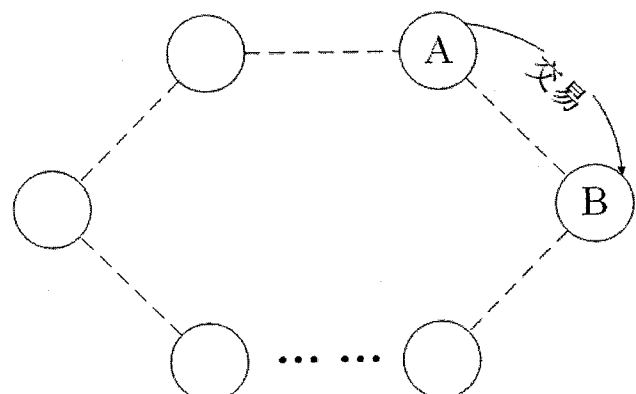


圖 1b

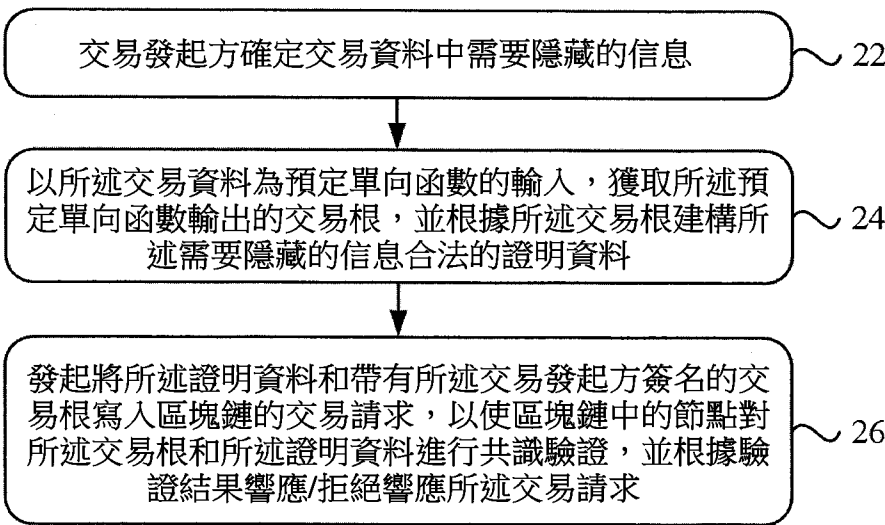


圖 2

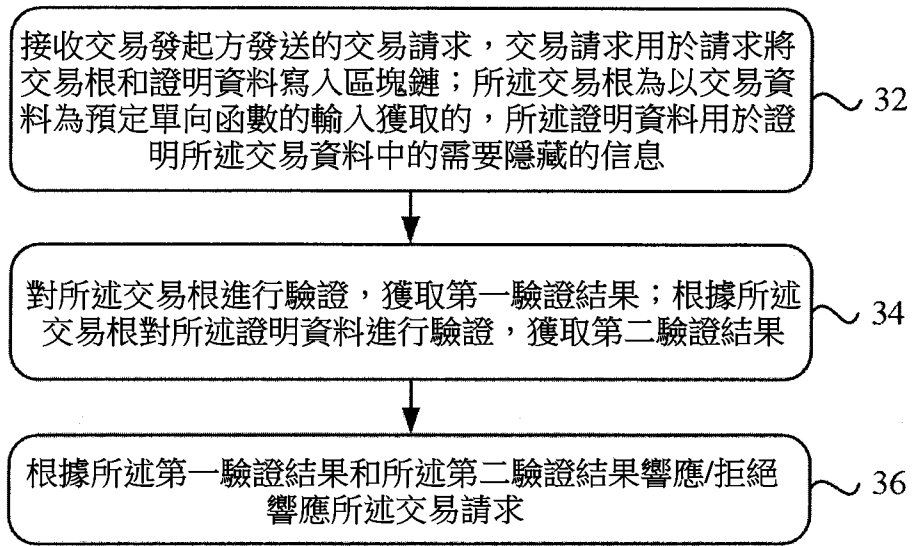


圖 3

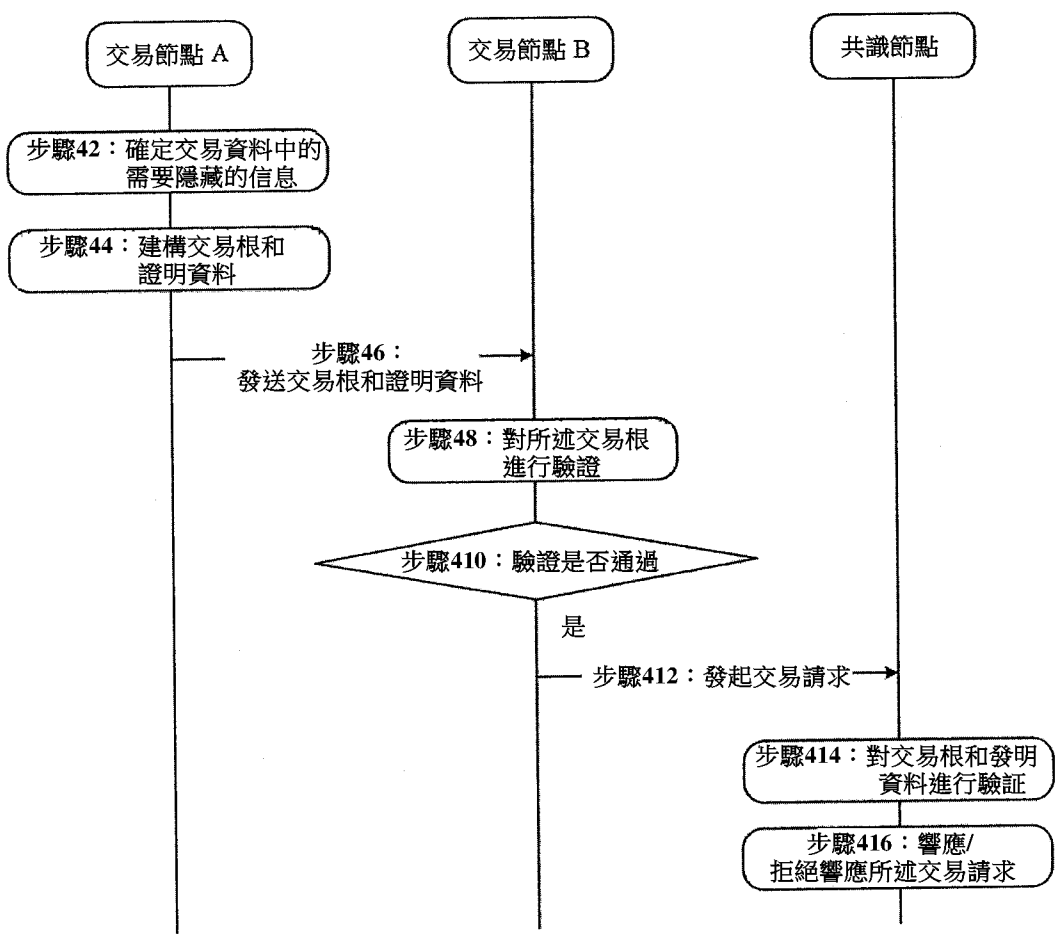


圖 4

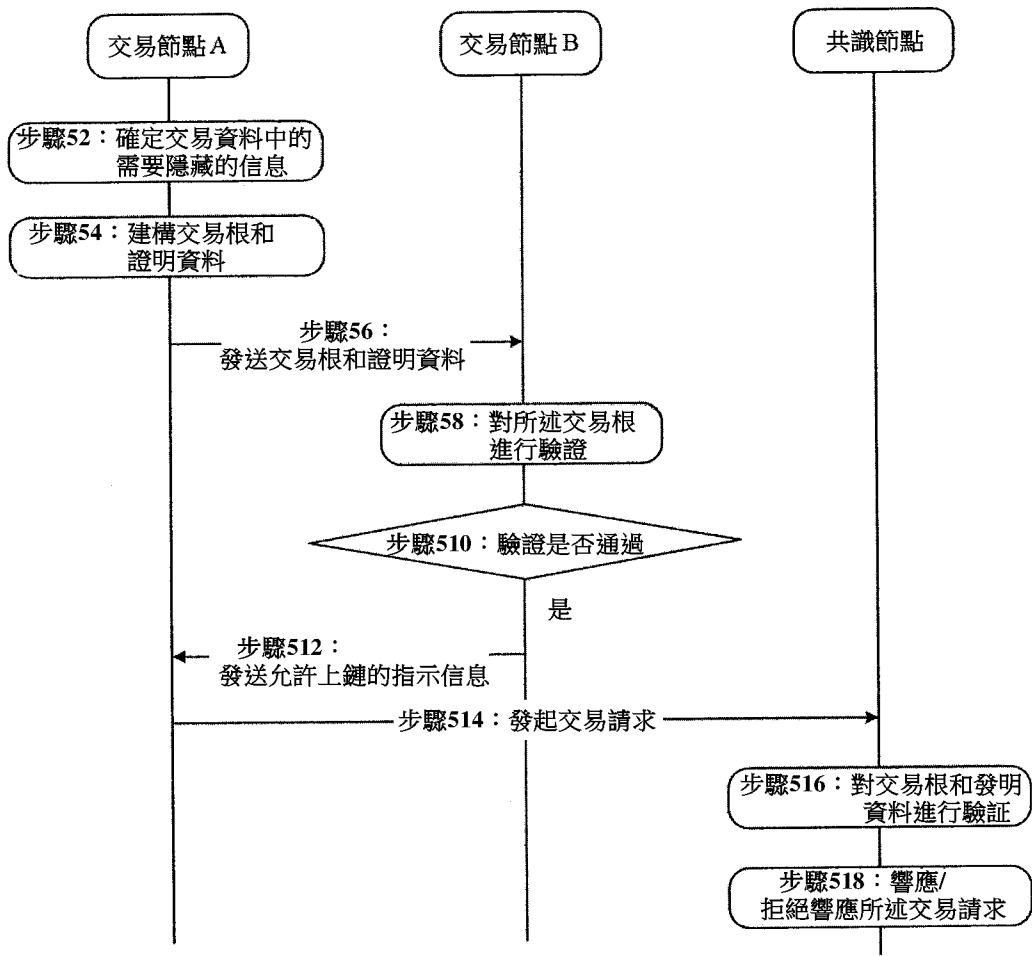


圖 5

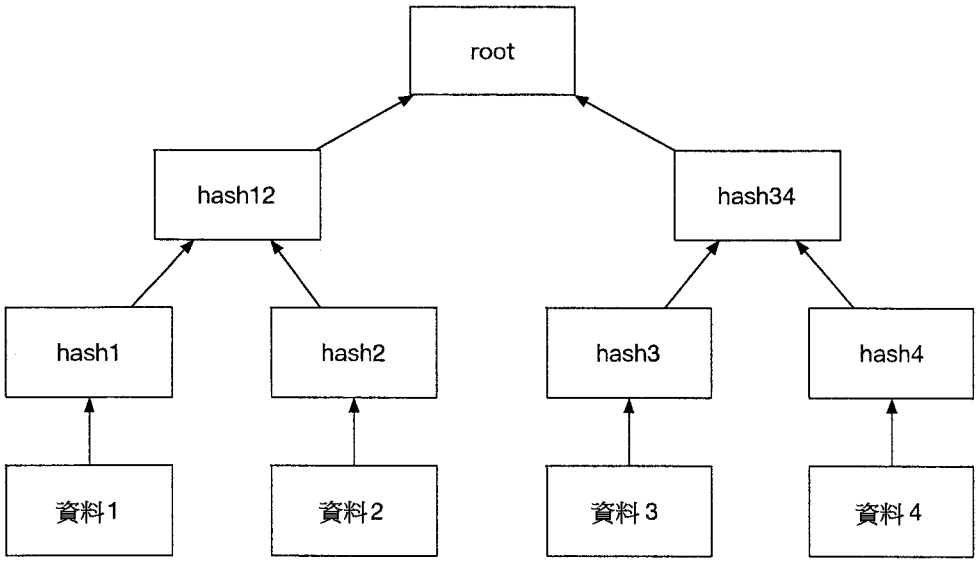


圖 6a

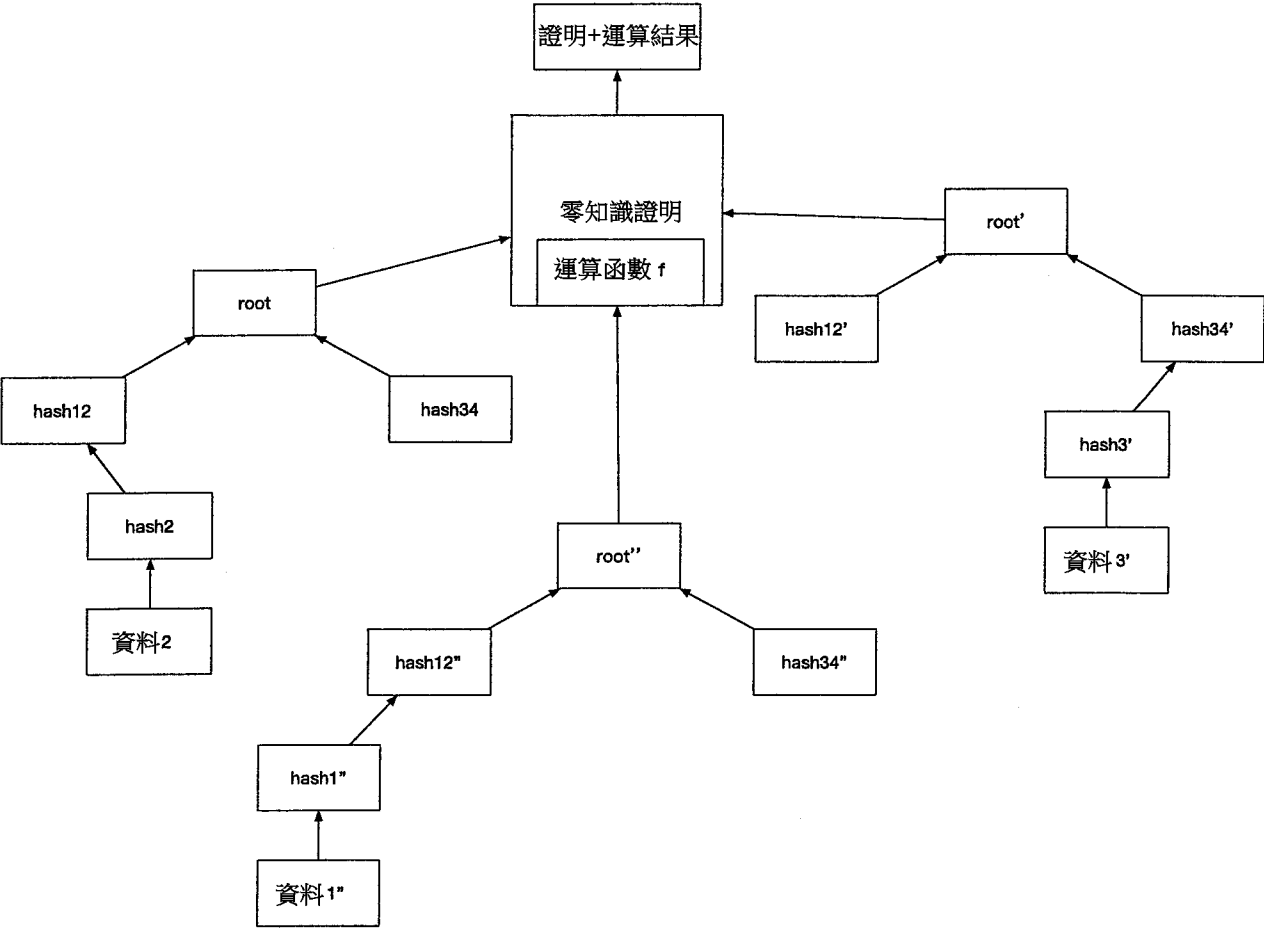


圖 6b

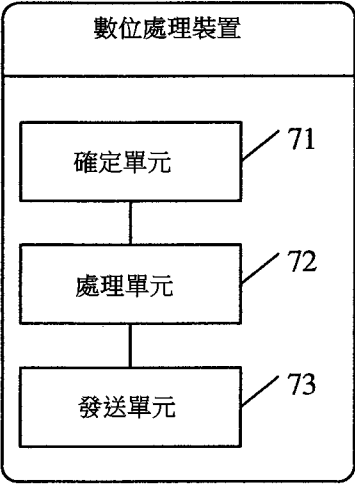


圖 7

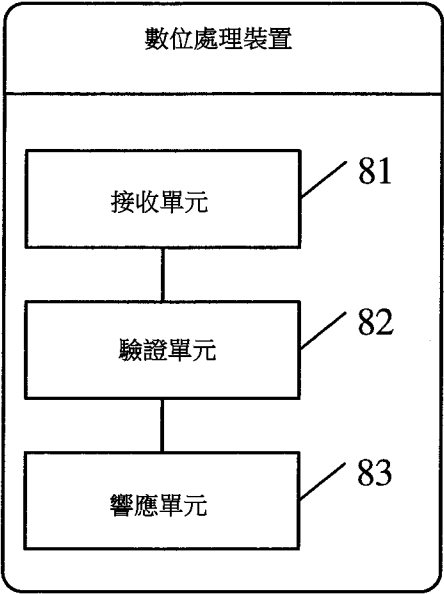


圖 8

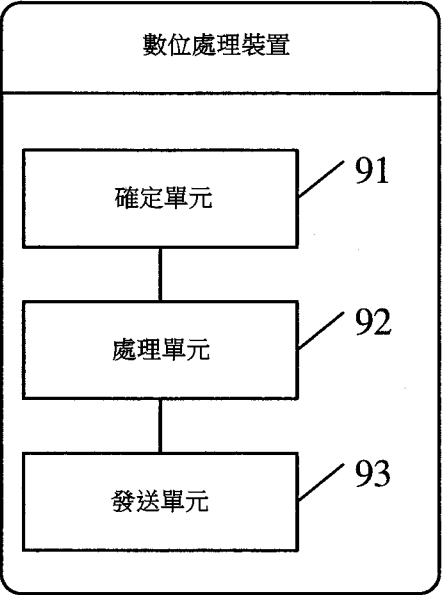


圖 9

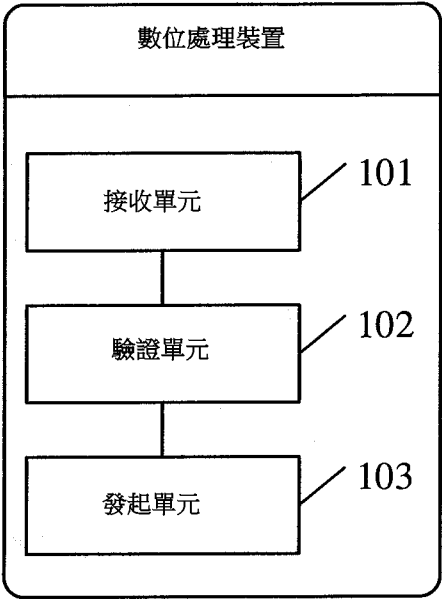


圖 10

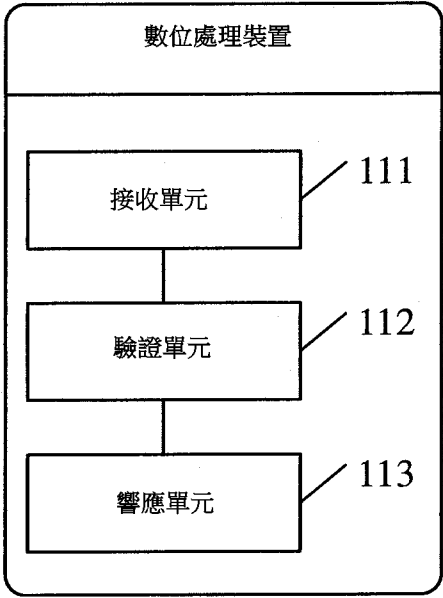


圖 11

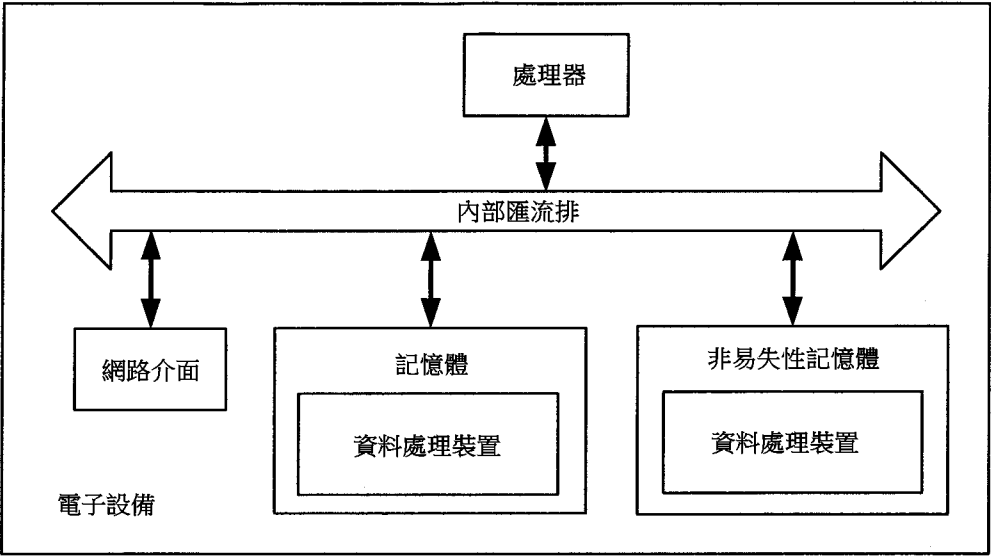


圖 12

【發明申請專利範圍】

【第1項】

一種資料處理方法，其特徵在於，包括：

交易發起方確定交易資料中需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發起將所述證明資料和帶有所述交易發起方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

【第2項】

根據申請專利範圍第1項所述的方法，其中，在以所述交易資料為預定單向函數的輸入之前，還包括：

確定所述交易資料中的交易前的資料和交易後的資料；

其中，以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根包括：

以交易前的資料為第一預定單向函數的輸入，獲取所述第一預定單向函數輸出的輸入交易根；

以交易後的資料為第二預定單向函數的輸入，獲取所述第二預定單向函數輸出的輸出交易根；

將獲取的輸入交易根和輸出交易根作為待上鏈的交易根。

【第3項】

根據申請專利範圍第2項所述的方法，其中，以交易後的資料為第二預定單向函數的輸入，獲取所述第二預定單向函數輸出的輸出交易根包括：

根據所述交易後的資料和隨機數建構預定單向函數樹的底層，並確定所述預定單向函數樹的頂層對應的輸出交易根。

【第4項】

根據申請專利範圍第1項所述的方法，其中，所述根據所述交易根建構所述需要隱藏的信息合法的證明資料包括：

以所述交易根和所述需要隱藏的信息為輸入進行預定的邏輯運算；

以所述需要隱藏的信息為保護對象，對所述邏輯運算進行零知識證明，獲取證明資料。

【第5項】

一種資料處理方法，其特徵在於，包括：

接收交易發起方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒

絕響應所述交易請求。

【第6項】

根據申請專利範圍第5項所述的方法，其中，所述對所述交易根進行驗證包括：

驗證所述交易根是否有合法的簽名。

【第7項】

根據申請專利範圍第6項所述的方法，其中，驗證所述交易根是否有合法的簽名包括：

確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；

若判斷獲知地址的數量為1，則驗證所述交易根是否有與所述交易發起方對應的簽名。

【第8項】

根據申請專利範圍第5項所述的方法，其中，所述對所述交易根進行驗證包括：

驗證所述交易根中的輸出交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸出交易根為根據所述交易資料中交易後的資料建構的。

【第9項】

根據申請專利範圍第5項所述的方法，其中，所述對所述交易根進行驗證包括：

驗證所述交易根中的輸入交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸入交易根為根據所述交

易資料中交易前的資料建構的。

【第10項】

根據申請專利範圍第5項所述的方法，其中，所述根據所述第一驗證結果和所述第二驗證結果確定響應/拒絕響應所述交易請求包括：

若所述第一驗證結果和所述第二驗證結果均為通過，則響應所述交易請求，以將帶有交易發起方簽名的交易根和證明資料寫入區塊鏈；

若所述第一驗證結果和/或所述第二驗證結果為未通過，則拒絕響應所述交易請求。

【第11項】

一種資料處理方法，其特徵在於，包括：

交易發起方確定交易資料中的需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

向交易接收方發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

【第12項】

一種資料處理方法，其特徵在於，包括：

交易接收方接收交易發送方發送的交易根和證明資料；所述交易根為以交易資料為預定單向函數的輸入獲取

的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

若驗證結果為通過，則發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

【第13項】

一種資料處理方法，其特徵在於，包括：

接收交易接收方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易發起方發起的交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

【第14項】

根據申請專利範圍第13項所述的方法，其中，所述對所述交易根進行驗證包括：

確定與所述交易根中的輸出交易根具有關聯關係的地

址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；

若判斷獲知地址的數量為大於等於預定閾值，則驗證所述交易根是否攜帶有與所述交易發起方和所述交易接收方對應的簽名。

【第15項】

一種資料處理裝置，其特徵在於，包括：

確定單元，用於確定交易資料中需要隱藏的信息；

處理單元，用於以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發起單元，用於發起將所述證明資料和帶有所述交易發起方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

【第16項】

根據申請專利範圍第15項所述的裝置，其中，所述確定單元，還用於確定所述交易資料中的交易前的資料和交易後的資料；

其中，所述處理單元，具體用於以交易前的資料為第一預定單向函數的輸入，獲取所述第一預定單向函數輸出的輸入交易根；以交易後的資料為第二預定單向函數的輸入，獲取所述第二預定單向函數輸出的輸出交易根；將獲取的輸入交易根和輸出交易根作為待上鏈的交易根。

【第17項】

根據申請專利範圍第16項所述的裝置，其中，所述處理單元，具體用於根據所述交易後的資料和隨機數建構預定單向函數樹的底層，並確定所述預定單向函數樹的頂層對應的輸出交易根。

【第18項】

根據申請專利範圍第15項所述的裝置，其中，所述處理單元，具體用於以所述交易根和所述需要隱藏的信息為輸入進行預定的邏輯運算；以所述需要隱藏的信息為保護對象，對所述邏輯運算進行零知識證明，獲取證明資料。

【第19項】

一種資料處理裝置，其特徵在於，包括：

接收單元，用於接收交易發起方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

驗證單元，用於對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

響應單元，用於根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

【第20項】

根據申請專利範圍第19項所述的裝置，其中，所述驗證單元，具體用於驗證所述交易根是否有合法的簽名。

【第21項】

根據申請專利範圍第20項所述的裝置，其中，所述驗證單元，具體用於確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；若判斷獲知地址的數量為1，則驗證所述交易根是否有與所述交易發起方對應的簽名。

【第22項】

根據申請專利範圍第19項所述的裝置，其中，所述驗證單元，具體用於驗證所述交易根中的輸出交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸出交易根為根據所述交易資料中交易後的資料建構的。

【第23項】

根據申請專利範圍第19項所述的裝置，其中，所述驗證單元，具體用於驗證所述交易根中的輸入交易根與已上鏈的輸出交易根和輸入交易根是否重複；所述輸入交易根為根據所述交易資料中交易前的資料建構的。

【第24項】

根據申請專利範圍第19項所述的裝置，其中，所述響應單元，具體用於若所述第一驗證結果和所述第二驗證結果均為通過，則響應所述交易請求，以將帶有交易發起方簽名的交易根和證明資料寫入區塊鏈；若所述第一驗證結果和/或所述第二驗證結果為未通過，則拒絕響應所述交易請求。

【第25項】

一種資料處理裝置，其特徵在於，包括：

確定單元，用於交易發起方確定交易資料中的需要隱藏的信息；

處理單元，用於以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發送單元，用於向交易接收方發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

【第26項】

一種資料處理裝置，其特徵在於，包括：

接收單元，用於接收交易發送方發送的交易根和證明資料；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

驗證單元，用於根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

發起單元，用於若驗證結果為通過，則發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

【第27項】

一種資料處理裝置，其特徵在於，包括：

接收單元，用於接收交易接收方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易發起方發起的交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

驗證單元，用於對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

響應單元，用於根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

【第28項】

根據申請專利範圍第27項所述的裝置，其中，所述驗證單元，具體用於確定與所述交易根中的輸出交易根具有關聯關係的地址，所述輸出交易根為根據所述交易資料中交易後的資料建構的；若判斷獲知地址的數量為大於等於預定閾值，則驗證所述交易根是否攜帶有與所述交易發起方和所述交易接收方對應的簽名。

【第29項】

一種資料處理裝置，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：

確定交易資料中需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

發起將所述證明資料和帶有所述交易發起方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所述交易請求。

【第30項】

一種資料處理裝置，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：

接收交易發起方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。

【第31項】

一種資料處理裝置，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：

確定交易資料中的需要隱藏的信息；

以所述交易資料為預定單向函數的輸入，獲取所述預定單向函數輸出的交易根，並根據所述交易根建構所述需要隱藏的信息合法的證明資料；

向交易接收方發送所述交易根和所述證明資料，由所述交易接收方對所述交易根進行驗證，並在驗證通過後，發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求。

【第32項】

一種資料處理裝置，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：

接收交易發送方發送的交易根和證明資料；所述交易根為以交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

根據所述需要隱藏的信息和所述預定單向函數對所述交易根進行驗證；

若驗證結果為通過，則發起將所述證明資料和帶有所述交易發起方、所述交易接收方簽名的交易根寫入區塊鏈的交易請求，以使區塊鏈中的節點對所述交易根和所述證明資料進行共識驗證，並根據驗證結果響應/拒絕響應所

述交易請求。

【第33項】

一種資料處理裝置，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：

接收交易接收方發送的交易請求，所述交易請求用於請求將交易根和證明資料寫入區塊鏈；所述交易根為以交易發起方發起的交易資料為預定單向函數的輸入獲取的，所述證明資料用於證明所述交易資料中的需要隱藏的信息；

對所述交易根進行驗證，獲取第一驗證結果；根據所述交易根對所述證明資料進行驗證，獲取第二驗證結果；

根據所述第一驗證結果和所述第二驗證結果響應/拒絕響應所述交易請求。