201822112

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201822112 A

(43)公開日： 中華民國 107 (2018) 年 06 月 16 日

(21)申請案號：106131555 (22)申請日： 中華民國 106 (2017) 年 09 月 14 日

(51)Int. Cl.： *G06Q40/00 (2012.01)* *G06Q20/00 (2012.01)*
*G06K9/20 (2006.01)*

(30)優先權：2016/12/06 中國大陸 201611107046.9

(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：李奕 (CN)

(74)代理人：林志剛

申請實體審查：無 申請專利範圍項數：16 項 圖式數：12 共 39 頁

(54)名稱

業務資料處理方法、驗證方法、裝置及系統

(57)摘要

本發明實施例揭露了一種業務資料處理方法、驗證方法、裝置及系統。所述方法包括：獲取待處理業務資料，採用預設方式生成所述待處理業務資料的指紋資料；將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。利用本發明各個實施例，在對原有處理流程和性能影響較小的情況下，通過將原有業務資料嵌入指紋資料寫入區塊鏈的方式儲存原有業務資料的副本，可以從根本上實現驗證業務資料是否被篡改，確保業務資料不可被修改，提高業務資料的可靠性和公信度。

指定代表圖：

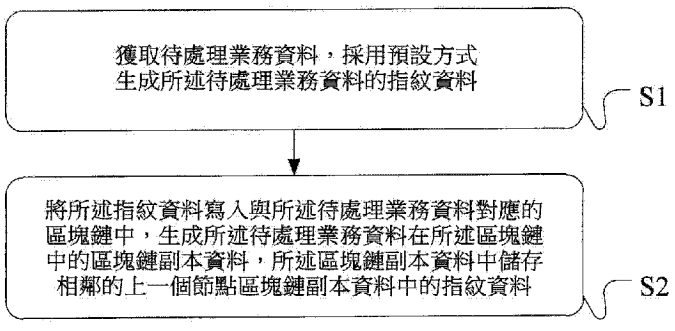


圖 2

# 【發明說明書】

【中文發明名稱】

業務資料處理方法、驗證方法、裝置及系統

【技術領域】

本發明屬於電腦資料處理技術領域，尤其關於一種業務資料處理方法、驗證方法、裝置及系統。

【先前技術】

業務資料的安全、可靠對保障業務系統資料正常處理和輸出可靠結果是極其重要的。尤其是隨著網際網路金融的日益發展，現在各支付機構通常都會建設自己的帳務核心系統，以處理使用者的資金轉移請求，而如何保障這些類似帳務核心系統中業務資料不被篡改，提高支付結構公佈資料的公信力，是目前許多金融企業用戶越來越關注的問題。

業務資料中比較敏感的帳務資料一般會記錄在支付機構自身的帳務系統資料庫中。由於支付機構對這些資料庫擁有最高管理許可權，理論上是可以隨意篡改其中的資料的。而帳務資料又是跟資金直接關聯，通常是支付機構中重要程度最高的一類資料。由此，支付機構常常使用一些技術手段來對外揭露表示自身的帳務資料自產生後就真實可靠，沒有被篡改過，以提高支付機構的公信度。例如在公益捐贈場景中證實善款的轉移真實可信，又例如在監管

審查場景中證明支付機構的資金記錄資料沒有被修改。現有的方式為了確定帳務資料的可信度，常規的方式一般是通過對帳來驗證的。例如一種方式中，可以與其他機構或主題的資料進行核對佐證。對於同一筆資金轉移，相關參與者可以儲存基於自身視角的一套帳務資料，用於與支付機構的資料做核對。通過同一條資金轉移單據的不同資料展示來相互佐證，驗證支付機構的帳務資料是否被篡改。將帳務資料與其他機構的相關資料相互佐證，確保能夠相互佐證，以提升帳務資料造假的成本。

包括上述所述現有的方式中，維護自身機構帳務資料公信度的成本比較大。例如與其他機構的資料進行核對佐證時通常需要至少有三方都保存同一帳務資料的不同副本，才能確保可以確認資料作假的一方，並且對資料傳輸和儲存的軟硬體安全性要求也較高。同時，對於一些支付機構來說，一些敏感性資料也不適合進行外露，所以在對帳務資料實施監控處理的過程中會對原帳務資料本身或處理流程做出較大變動、修改，較大的影響了系統對帳務資料原有的處理流程和性能。另外，該方式也無法從根本上解決信任問題，例如所謂的外部機構也可能是支付機構的關聯機構，無法排除兩者不會共同造假。

因此，現有的支付機構確保其帳務資料真實可靠的一些監控的方式，目前還無法從帳務資料根本上規避帳務資料被修改的問題，使得支付機構對外揭露的資料可信度降低。

【發明內容】

本發明目的在於提供一種業務資料處理方法、驗證方法、裝置及系統，可以在對原有處理流程和性能影響較小的情況下，通過將原有業務資料嵌入指紋資料寫入區塊鏈的方式儲存原有業務資料的副本，可以從根本上實現驗證業務資料是否被篡改，確保業務資料不可被修改，提高業務資料的可靠性和公信度。

本發明提供的一種業務資料處理方法、驗證方法、裝置及系統是這樣實現的：

一種業務資料處理方法，所述方法包括：

獲取待處理業務資料，採用預設方式生成所述待處理業務資料的指紋資料；

將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。

一種業務資料處理裝置，所述裝置包括：

指紋資料生成模組，用於獲取待處理業務資料，以及採用預設方式生成所述待處理業務資料的指紋資料；

區塊鏈資料生成模組，用於將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資

料。

一種業務資料驗證方法，所述方法包括：

確定待驗證的業務資料，從儲存的區塊鏈資料中獲取與所述待驗證的業務資料相關的區塊鏈副本資料；所述區塊鏈副本資料包括根據待處理業務資料的指紋資料生成並儲存在區塊鏈中的資料資訊，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料；

採用預設方式計算所述待驗證的業務資料的第一指紋資料，並獲取所述區塊鏈副本資料中的與所述待驗證的業務資料相對應的第二指紋資料；

比較所述第一指紋資料與所述第二指紋資料是否相同，若相同，則確認所述待驗證的業務資料未被修改。

一種業務系統，包括I/O介面、處理單元，

所述I/O介面用於接收待處理業務資料；

所述處理單元被設置成，用於採用預設方式生成所述待處理業務資料的指紋資料；還用於將所述業務資料寫入原有資料庫中，以及將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈資料庫中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。

本發明提供的一種業務資料處理方法、驗證方法、裝置及系統，使用區塊鏈作為傳統業務資料庫中資料的副本儲存方式。原業務系統處理流程僅需生成業務資料相應的指紋資料，接著儲存到對應的區塊鏈中生成區塊鏈副本資

料即可，對原業務系統的處理流程侵入較小，確保傳統資料庫高性能的能力基礎上，極大的保障了業務資料的監控效果，確保業務資料不可被修改，提高業務資料，尤其是敏感的帳務資料的可靠性和公信度。

【圖式簡單說明】

為了更清楚地說明本發明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附圖作簡單地介紹，顯而易見地，下面描述中的附圖僅僅是本發明中記載的一些實施例，對於本領域普通技術人員來講，在不付出進步性勞動性的前提下，還可以根據這些附圖獲得其他的附圖。

圖1是本發明提供的一種區塊鏈資料儲存的資料結構示意圖；

圖2是本發明所述一種資料處理方法一種實施例的方法流程圖；

圖3是本發明提供生成待處理業務資料的指紋資料的一種實施場景的示意圖；

圖4是本發明提供的一種業務資料處理方法另一個實施例場景的實施示意圖；

圖5是本發明提供的所述一種業務資料處理方法的另一種實施例的方法流程示意圖；

圖6本發明提供生成待處理業務資料的指紋資料另一種實施場景的示意圖；

圖7本發明提供生成待處理業務資料的指紋資料另一種實施場景的示意圖；

圖8是本發明提供一種業務資料驗證方法一種實施例的方法流程圖；

圖9是本發明提供的一種業務資料處理裝置一種實施例的模組結構示意圖；

圖10是本發明提供的一種業務資料處理裝置另一種實施例的模組結構示意圖；

圖11是本發明提供的一種業務資料處理裝置另一種實施例的模組結構示意圖；

圖12是本發明提供的一種業務系統一種實施例的結構示意圖。

【實施方式】

為了使本技術領域的人員更好地理解本發明中的技術方案，下面將結合本發明實施例中的附圖，對本發明實施例中的技術方案進行清楚、完整地描述，顯然，所描述的實施例僅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作出進步性勞動前提下所獲得的所有其他實施例，都應當屬於本發明保護的範圍。

圖2是本發明所述一種業務資料處理方法一種實施例的方法流程圖。雖然本發明提供了如下述實施例或附圖所示的方法操作步驟或裝置結構，但基於常規或者無需進步

性的勞動在所述方法或裝置中可以包括更多或者部分合併後更少的操作步驟或模組單元。在邏輯性上不存在必要因果關係的步驟或結構中，這些步驟的執行順序或裝置的模組結構不限於本發明實施例或附圖所示的執行順序或模組結構。所述的方法或模組結構的在實際中的裝置或終端產品應用時，可以按照實施例或者附圖所示的方法或模組結構進行循序執行或者並存執行（例如並行處理器或者多執行緒處理的環境、甚至包括分散式處理的實施環境）。

區塊鏈一種去中心化、去信任、防篡改的分散式資料儲存技術。圖1是本發明提供的一種區塊鏈資料儲存的資料結構示意圖。如圖1所示，區塊鏈的鏈式資料結構保證了資料的變更只能通過增量的方式進行。已經記錄的資料將會一直保持創建時的狀態，不會被覆蓋。同時，區塊鏈通過特定的共識演算法，確認了每一個區塊的資料記錄職責歸屬，並且取得了其他節點的認同。如果要更改已經存在的資料，通常只能通過偽造整個區塊鏈的方式實施替換。這無論是在工作量證明還是權益證明的共識演算法下，幾乎是不可能做到的事情。這樣，本發明方案使用區塊鏈作為傳統業務資料庫中資料的副本儲存方式。原業務系統處理流程僅需生成業務資料相應的指紋資料，接著儲存到對應的區塊鏈中生成區塊鏈副本資料即可，無需做出較大處理流程上的變動，確保傳統資料庫高性能的能力基礎上，極大的保障了業務資料的監控效果，確保業務資料不可被修改，提高業務資料的可靠性和公信度。

以下為了清楚起見，以具體的一個支付機構帳務系統生成帳務資料的區塊鏈副本資料為應用場景進行說明。當然，在本實施例中所處理的業務資料為帳務資料，但是，本領域技術人員能夠理解到，可以將本方案的實質精神應用到其他業務系統中防止業務資料被篡改的場景下。即，通過在原有系統處理流程中嵌入指紋資料生成邏輯並同時寫入區塊鏈的方式，使得通過將當前業務資料的指紋資料值和儲存在區塊鏈上的原始指紋資料值進行比對即可確認當前業務資料是否被修改過，消滅資料被篡改的可能性，提高業務資料的可靠性和公信度。本發明實施方案中的業務資料不限於帳務資料，但對敏感性較強的帳務資料的應用效果更加明顯，可顯著提高支付結構等相關金融業務使用者對外發佈資料的公信力，提高與帳務資料有利益關係的使用者的業務使用體驗。

具體的一種實施例如圖2所示，本發明提供的一種業務資料處理方法的一種實施例中，所述方法可以包括：

S1：獲取待處理業務資料，採用預設方式生成所述待處理業務資料的指紋資料。

支付機構的業務系統可以根據記帳發起方的記帳請求獲取並儲存相應的業務資料。本發明實施例應用場景中，在帳務系統正常儲存帳務資料到資料庫的同時可以獲取該帳務資料，在此可以統一將其稱為待處理業務資料。接著可以採用預設方式對所述待處理業務資料進行處理，生成該待處理業務資料的指紋資料。

本實施例中，所述的支付機構可以理解為包括在收付款人之間作為仲介機構提供部分或全部貨幣資金轉移服務的機構。所述的業務資料可以包括支付機構提供資金轉移及記錄服務時，在系統資料庫中產生的資金變動憑證資料，或者可以包括從記帳發起方直接獲取的資金轉移及記錄產生的資金變動憑證資料或關聯資料，如待處理業務資料可以為從業務系統接收到的帳單資料。

在本實施例應用場景中，可以根據帳務資料的實施場景或業務類型等為帳務資料定義指紋資料，通過指紋資料能夠唯一確認一筆帳務資料。如果帳務資料被篡改，其生產的指紋資料也會被改變。這樣，通過比對帳務資料的指紋資料可以確定某個帳務資料的真實性。

為了保護原業務資料中的敏感性資料，本發明所述方法的另一個實施例中，在選取所述預設演算法時可以選取使生成的所述指紋資料是不可逆向破解的演算法。具體的本發明提供的一種實施例中，生成所述指紋資料的過程被設置成是單向不可逆的。

本實施提供的方案中，生成該指紋資料的過程是單向不可逆的，這樣，本實施例可以通過資料簡單的獲取其指紋資料，而不能通過指紋資料反推出資料本身。因此本實施例提供的這種方式可以有效可靠的能做到資料安全及隱私保護。

具體的生成所述待處理業務資料的指紋資料所採用的方式，可以根據業務場景或業務資料處理需求進行選擇或

自訂演算法，將所述待處理業務資料轉換成可以唯一確認該待處理業務資料的標識資訊。一般的，生成所述指紋資料的預設演算法可以包括多種方式，本發明的一種實施例中所述的預設方式可以為對待處理業務資料進行資料雜湊處理，即雜湊(Hash)處理，生成的雜湊值可以作為本實施例所述的待處理業務資料的指紋資料。因此，本發明提供的一種業務資料處理方法的一種實施例中，所述採用預設方式生成所述待處理業務資料的指紋資料，可以包括：

S101：對所述待處理業務資料進行雜湊處理，將所述雜湊生成的雜湊值作為所述待處理業務資料的指紋資料。

在資訊安全技術中，雜湊（Hash）函數可以提供驗證訊息完整性的服務，可以對不同長度的輸入訊息，產生固定長度的輸出。這個固定長度的輸出稱為原輸入訊息的“雜湊”或“訊息摘要”（Message digest）。圖3是本發明提供生成待處理業務資料的指紋資料的一種實施場景的示意圖，具體的雜湊方法可以自行制定，也可以採用MD5、SHA-1或其他演算法。利用本發明實施例可以採用待處理業務資料的雜湊值作為所述待處理業務資料的指紋資料，以提高原業務資料的安全性及隱私保護。

S2：將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。

在支付機構現有業務系統中，可以儲存帳務資料的同

時，用上述方式計算出這筆帳務單據的指紋，將接著可以該指紋資料寫入到區塊鏈中。所述的區塊鏈可以儲存到相應的資料儲存單元中，如資料庫或者其他專門儲存揭露區塊鏈中的資料的儲存媒體。這樣，相當於在現有資料庫和區塊鏈中，同時存在同一份帳務資料的不同形式的版本，並且這兩種版本相互錨定，關聯地確認資料庫中的原始帳務資料是否被篡改。

區塊鏈的鏈式資料結構，保證了資料的變更只能通過增量的方式進行。已經記錄在區塊鏈中業務資料的區塊鏈副本資料將會一直保持創建時的狀態，不會被覆蓋。同時，區塊鏈通過特定的共識演算法（如區塊鏈副本資料中包括相鄰的上一個節點區塊鏈副本資料中的指紋資料），確認了每一個區塊的資料記錄職責歸屬，並且取得了其他節點的認同。如果要更改已經存在的資料，只能通過偽造整個區塊鏈的方式實施替換。而在目前對外完全公佈（或對指定監控物件完全公佈）的情況下，整個區塊鏈資料的替換幾乎是不可能完成的。因此，本發明可以利用區塊鏈中指紋資料無法篡改的特性，關聯地確認資料庫中的原始帳務資料是否被篡改，極大了提高了帳務資料的公信度。

本發明的一些實施例中，可以在業務資料儲存到資料庫的同時指紋資料，並將指紋資料寫入到區塊鏈中。其他的實施方式中，為了進一步減小對原有業務系統的影響，提高原有業務系統的處理性能，在待處理業務資料完成資料庫的儲存後，可以採用非同步的方式將所述待處理業務

資料寫入區塊鏈，（即資料庫與區塊鏈“雙寫”）。整體的業務系統處理流程如4所示，圖4本發明提供的一種業務資料處理方法另一個實施例場景的實施示意圖，即圖4中的帳務資料是本發明實施例所述的業務資料的一種具體應用場景。因此，本發明提供的所述一種業務資料處理方法的另一種實施例中，所述將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，包括：

S102：採用非同步方式將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中。

這樣可以進一步減小對原有業務系統的影響，提高原有業務系統的處理性能。

本發明提供的一種業務資料處理方法，使用區塊鏈作為傳統業務資料庫中資料的副本儲存方式。原業務系統處理流程僅需生成業務資料相應的指紋資料，接著儲存到對應的區塊鏈中生成區塊鏈副本資料即可，對原業務系統的處理流程侵入較小，確保傳統資料庫高性能的能力基礎上，極大的保障了業務資料的監控效果，確保業務資料不可被修改，提高業務資料的可靠性和公信度。

圖5是本發明提供的所述一種業務資料處理方法的另一種實施例的方法流程示意圖。如圖5所示，在生成待處理業務資料時，可以先將待處理業務資料中確定的關鍵要素如帳務資料中的轉帳雙方ID、時間、金額等提取出來，接著針對這些關鍵要素資料生成指紋資料。這樣可以將多種不同的業務資料抽離出共同的關鍵要素資料，簡化指紋

資料的來源資料，快速生成指紋資料，提高資料處理效果。具體的，本發明提供的一種業務資料處理方法的另一種實施例中，所述方法還可以包括：

S10：從所述待處理業務資料中提取出預定類型的關鍵要素資料；

相應的，所述採用預設方式生成所述待處理業務資料的指紋資料，包括採用預設方式對提取的所述關鍵要素資料進行處理，生成所述待處理業務資料的指紋資料。

圖6本發明提供生成待處理業務資料的指紋資料另一種實施場景的示意圖。如圖6所示，對一筆帳務資料模型Data_Count，可以將其中的關鍵要素資料Data_Key如包括轉帳雙方、時間、金額、業務單據號、業務類型等提取出來，接著針對這些關鍵要素生成指紋資料Data_MD5。

其他的一些實施例中，當所述待處理業務資料缺少至少一項所述關鍵要素資料時，可以執行包括：

S11：根據所述業務資料的業務類型確定缺少的關鍵要素資料的預設值，使用所述預設值作為生成所述指紋資料的關鍵要素資料的取值。

具體的應用場景中，如當缺少的關鍵要素資料項目數少於預定個數（如2個），可以使用從所述待處理業務資料中已提取出的關鍵要素資料結合缺少的關鍵要素資料的預設值生成所述待處理業務資料的指紋資料。例如圖7中，圖7本發明提供生成待處理業務資料的指紋資料另一種實施場景的示意圖，當缺少業務類型的關鍵要素資料

時，可以使用預設的業務類型“該值為預設值”作為所述業務類型的預設值，接著再結合已經獲取到的流水號、收款方、付款方、金額、時間的關鍵要素資料生成待處理業務資料的指紋資料Data_MD5。

利用本發明實施例提供業務資料處理方法，可以在現有資料庫和區塊鏈中同時存在同一份單據的不同形式的版本，並且這兩種版本相互錨定。區塊鏈中的資料可以對外揭露，或者對指定物件揭露，如監管部門或指定使用者，以驗證資料庫中儲存的業務資料是否為篡改，提高業務資料的公信度。因此，基於前述所述，本發明還提供一種業務資料驗證方法，圖8是本發明提供一種業務資料驗證方法一種實施例的方法流程圖，如圖8所示，所述方法可以包括：

S100：確定待驗證的業務資料，從儲存的區塊鏈資料中獲取與所述待驗證的業務資料相關的區塊鏈副本資料；所述區塊鏈副本資料包括根據待處理業務資料的指紋資料生成並儲存在區塊鏈中的資料資訊，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料；

S200：採用預設方式計算所述待驗證的業務資料的第一指紋資料，並獲取所述區塊鏈副本資料中的與所述待驗證的業務資料相對應的第二指紋資料；

S300：比較所述第一指紋資料與所述第二指紋資料是否相同，若相同，則確認所述待驗證的業務資料未被修改。

這樣，本發明實施例提供的方案，可以利用區塊鏈中指紋資料無法篡改的特性，關聯地確認資料庫中的資料是否被篡改，可以有效、可靠的驗證支付結構業務系統中的業務資料是否被篡改過，從技術層面上根本解決了業務資料（尤其是帳務資料）作假的可能性，可以極大的提高支付結構公佈的帳務資料的公信度。

基於本發明上述實施例所述的業務資料處理方法，本發明還提供一種業務資料處理裝置。圖9是本發明提供的一種業務資料處理裝置一種實施例的模組結構示意圖，如圖9所示，所述裝置可以包括：

指紋資料生成模組101，可以用於獲取待處理業務資料，以及採用預設方式生成所述待處理業務資料的指紋資料；

區塊鏈資料生成模組102，可以用於將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。

本發明提供的業務資料處理轉帳，在儲存業務資料的同時，以計算出這筆業務資料的指紋資料，將該指紋資料寫入到區塊鏈中。這樣，相當於在現有資料庫和區塊鏈中，同時存在同一份單據的不同形式的版本，並且這兩種版本相互錨定。可以利用區塊鏈中指紋資料無法篡改的特性，關聯地確認資料庫中的資料是否被篡改。

圖10是本發明提供的一種業務資料處理裝置另一種實施例的模組結構示意圖，如圖10所示，所述裝置還可以包括：

關鍵要素提取模組103，可以用於從所述待處理業務資料中提取出預定類型的關鍵要素資料；

相應的，所述指紋資料生成模組101採用預設方式生成所述待處理業務資料的指紋資料包括採用預設方式對提取的所述關鍵要素資料進行處理，生成所述待處理業務資料的指紋資料。

當然，如前述方法實施例中，所述裝置的一些實施例中，所述指紋資料生成模組101生成所述指紋資料的過程可以被設置成是單向不可逆的。另外，所述指紋資料生成模組101採用預設方式生成所述待處理業務資料的指紋資料可以包括：對所述待處理業務資料進行雜湊處理，將所述雜湊生成的雜湊值作為所述待處理業務資料的指紋資料。以及，所述裝置的其他實施例中，所述區塊鏈資料生成模組102可以採用非同步方式將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中。

圖11是本發明提供的一種業務資料處理裝置另一種實施例的模組結構示意圖，如圖11所示，所述裝置還可以包括：

預設處理模組104，可以用於當所述待處理業務資料缺少至少一項所述關鍵要素資料時，根據所述業務資料的業務類型確定缺少的關鍵要素資料的預設值，使用所述預

設值作為生成所述指紋資料的關鍵要素資料的取值。

本發明提供的一種業務資料處理裝置，使用區塊鏈作為傳統業務資料庫中資料的副本儲存方式。原業務系統處理流程僅需生成業務資料相應的指紋資料，接著儲存到對應的區塊鏈中生成區塊鏈副本資料即可，對原業務系統的處理流程侵入較小，確保傳統資料庫高性能的能力基礎上，極大的保障了業務資料的監控效果，確保業務資料不可被修改，提高業務資料的可靠性和公信度。

上述實施例所述的業務資料處理方法/裝置、業務資料驗證方法等可以應用於包括支付結構的其他業務系統中，實現採用區塊鏈保存業務資料副本以提高業務資料公信度並減少對原業務系統變動/侵入的效果。圖12是本發明提供的一種業務系統一種實施例的結構示意圖。具體的，本發明提供一種業務系統，所述業務系統可以包括I/O介面、處理單元，

所述I/O介面用於接收待處理業務資料；

所述處理單元被設置成，用於採用預設方式生成所述待處理業務資料的指紋資料；還用於將所述業務資料寫入原有資料庫中，以及將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈資料庫中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。

一種實施方式中，儲存業務系統業務資料集的原有資料庫和儲存區塊鏈資料的區塊鏈資料庫可以與所述業務系

統分離，單獨儲存資料。其他的實施方式中，所述原有資料庫和區塊鏈資料庫中的人任意一個可以被包含在所述業務系統中，如一個實施例中，業務系統可以包括自身的原有資料庫，而儲存區塊鏈的資料庫可以單獨設置在業務伺服器或第三方的伺服器或儲存裝置中。

所述處理單元還可以用於從所述待處理業務資料中提取出預定類型的關鍵要素資料；相應的，所述採用預設方式生成所述待處理業務資料的指紋資料包括採用預設方式對提取的所述關鍵要素資料進行處理，生成所述待處理業務資料的指紋資料。

所述處理單元還可以用於，從儲存的區塊鏈資料中獲取與所述待驗證的業務資料相關的區塊鏈副本資料，採用預設方式計算所述待驗證的業務資料的第一指紋資料，並獲取所述區塊鏈副本資料中的與所述待驗證的業務資料相對應的第二指紋資料；還可以用於比較所述第一指紋資料與所述第二指紋資料是否相同，若相同，則確認所述待驗證的業務資料未被修改。

本發明提供的一種業務資料處理方法、驗證方法、裝置及系統，使用區塊鏈作為傳統業務資料庫中資料的副本儲存方式。原業務系統處理流程僅需生成業務資料相應的指紋資料，接著儲存到對應的區塊鏈中生成區塊鏈副本資料即可，對原業務系統的處理流程侵入較小，確保傳統資料庫高性能的能力基礎上，極大的保障了業務資料的監控效果，確保業務資料不可被修改，提高業務資料的可靠性

和公信度。

儘管本發明內容中提到區塊鏈的示意數格式、關鍵要素資料的定義及提取方式、採用MD5生成指紋資料、比對資料庫中和區塊鏈中業務資料的指紋資料來確定是否篡改等之類的資料定義、獲取、互動、計算、判斷等描述，但是，本發明並不局限於必須是符合行業通訊標準、標準資料結構、標準資料庫資料處理方法或本發明實施例所描述的情況。某些行業標準或者使用自訂方式或實施例描述的實施基礎上略加修改後的實施方案也可以實現上述實施例相同、等同或相近、或變形後可預料的實施效果。應用這些修改或變形後的資料獲取、儲存、判斷、處理方式等獲取的實施例，仍然可以屬於本發明的可選實施方案範圍之內。

在20世紀90年代，對於一個技術的改進可以很明顯地區分是硬體上的改進（例如，對二極體、電晶體、開關等電路結構的改進）還是軟體上的改進（對於方法流程的改進）。然而，隨著技術的發展，當今的很多方法流程的改進已經可以視為硬體電路結構的直接改進。設計人員幾乎都通過將改進的方法流程程式設計到硬體電路中來得到相應的硬體電路結構。因此，不能說一個方法流程的改進就不能用硬體實體模組來實現。例如，可程式設計邏輯裝置（Programmable Logic Device, PLD）（例如現場可程式設計閘陣列（Field Programmable Gate Array，FPGA））就是這樣一種積體電路，其邏輯功能由使用者對裝置程式設

計來確定。由設計人員自行程式設計來把一個數位系統“整合”在一片PLD上，而不需要請晶片製造廠商來設計和製作專用的積體電路晶片。而且，如今，取代手工地製作積體電路晶片，這種程式設計也多半改用“邏輯編譯器（logic compiler）”軟體來實現，它與程式開發撰寫時所用的軟體編譯器相類似，而要編譯之前的原始代碼也得用特定的程式設計語言來撰寫，此稱之為硬體描述語言（Hardware Description Language，HDL），而HDL也並非僅有一種，而是有許多種，如ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）與Verilog。本領域技術人員也應該清楚，只需要將方法流程用上述幾種硬體描述語言稍作邏輯程式設計並程式設計到積體電路中，就可以很容易得到實現該邏輯方法流程的硬體電路。

控制器可以按任何適當的方式實現，例如，控制器可以採取例如微處理器或處理器以及儲存可由該（微）處理器執行的電腦可讀程式碼（例如軟體或韌體）的電腦可讀媒體、邏輯閘、開關、專用積體電路（Application

Specific Integrated Circuit，ASIC）、可程式設計邏輯控制器和嵌入微控制器的形式，控制器的例子包括但不限於以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及Silicone Labs C8051F320，記憶體控制器還可以被實現為記憶體的控制邏輯的一部分。本領域技術人員也知道，除了以純電腦可讀程式碼方式實現控制器以外，完全可以通過將方法步驟進行邏輯程式設計來使得控制器以邏輯閘、開關、專用積體電路、可程式設計邏輯控制器和嵌入微控制器等的形式來實現相同功能。因此這種控制器可以被認為是一種硬體部件，而對其內包括的用於實現各種功能的裝置也可以視為硬體部件內的結構。或者甚至，可以將用於實現各種功能的裝置視為既可以是實現方法的軟體模組又可以是硬體部件內的結構。

上述實施例闡明的系統、裝置、模組或單元，具體可以由電腦晶片或實體實現，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。具體的，電腦例如可以為個人電腦、膝上型電腦、車載人機互動設備、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何設備的組合。

雖然本發明提供了如實施例或流程圖所述的方法操作步驟，但基於常規或者無進步性的手段可以包括更多或者更少的操作步驟。實施例中列舉的步驟順序僅僅為眾多步驟執行順序中的一種方式，不代表唯一的執行順序。在實

際中的裝置或終端產品執行時，可以按照實施例或者附圖所示的方法循序執行或者並存執行（例如並行處理器或者多執行緒處理的環境，甚至為分散式資料處理環境）。用語“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、產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、產品或者設備所固有的要素。在沒有更多限制的情況下，並不排除在包括所述要素的過程、方法、產品或者設備中還存在另外的相同或等同要素。

為了描述的方便，描述以上裝置時以功能分為各種模組分別描述。當然，在實施本發明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，也可以將實現同一功能的模組由多個子模組或子單元的組合實現等。以上所描述的裝置實施例僅僅是示意性的，例如，所述單元的劃分，僅僅為一種邏輯功能劃分，實際實現時可以有另外的劃分方式，例如多個單元或元件可以結合或者可以整合到另一個系統，或一些特徵可以忽略，或不執行。另一點，所顯示或討論的相互之間的耦接或直接耦接或通訊連接可以是通過一些介面，裝置或單元的間接耦接或通訊連接，可以是電性，機械或其它的形式。

本領域技術人員也知道，除了以純電腦可讀程式碼方式實現控制器以外，完全可以通過將方法步驟進行邏輯程式設計來使得控制器以邏輯閘、開關、專用積體電路、可

程式設計邏輯控制器和嵌入微控制器等的形式來實現相同功能。因此這種控制器可以被認為是一種硬體部件，而對其內部包括的用於實現各種功能的裝置也可以視為硬體部件內的結構。或者甚至，可以將用於實現各種功能的裝置視為既可以是實現方法的軟體模組又可以是硬體部件內的結構。

本發明是參照根據本發明實施例的方法、設備（系統）、和電腦程式產品的流程圖和／或方塊圖來描述的。應理解可由電腦程式指令實現流程圖和／或方塊圖中的每一流程和／或方塊、以及流程圖和／或方塊圖中的流程和／或方塊的結合。可提供這些電腦程式指令到通用電腦、專用電腦、嵌入式處理機或其他可程式設計資料處理設備的處理器以產生一個機器，使得通過電腦或其他可程式設計資料處理設備的處理器執行的指令產生用於實現在流程圖一個流程或多個流程和／或方塊圖一個方塊或多個方塊中指定的功能的裝置。

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

這些電腦程式指令也可裝載到電腦或其他可程式設計資料處理設備上，使得在電腦或其他可程式設計設備上執行一系列操作步驟以產生電腦實現的處理，從而在電腦或

其他可程式設計設備上執行的指令提供用於實現在流程圖一個流程或多個流程和／或方塊圖一個方塊或多個方塊中指定的功能的步驟。

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

記憶體可能包括電腦可讀媒體中的非永久性記憶體，隨機存取記憶體(RAM)和/或非揮發性記憶體等形式，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實例。

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

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態樣的實施例的形式。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。

本發明可以在由電腦執行的電腦可執行指令的一般上下文中描述，例如程式模組。一般地，程式模組包括執行特定任務或實現特定抽象資料類型的常式、程式、物件、元件、資料結構等等。也可以在分散式運算環境中實踐本發明，在這些分散式運算環境中，由通過通訊網路而被連接的遠端處理設備來執行任務。在分散式運算環境中，程式模組可以位於包括存放裝置在內的本地和遠端電腦儲存媒體中。

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。

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

【符號說明】

101：指紋資料生成模組

102：區塊鏈資料生成模組

103：關鍵要素提取模組

104：預設處理模組

201822112

# 【發明摘要】

【中文發明名稱】

業務資料處理方法、驗證方法、裝置及系統

【中文】

本發明實施例揭露了一種業務資料處理方法、驗證方法、裝置及系統。所述方法包括：獲取待處理業務資料，採用預設方式生成所述待處理業務資料的指紋資料；將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。利用本發明各個實施例，在對原有處理流程和性能影響較小的情況下，通過將原有業務資料嵌入指紋資料寫入區塊鏈的方式儲存原有業務資料的副本，可以從根本上實現驗證業務資料是否被篡改，確保業務資料不可被修改，提高業務資料的可靠性和公信度。

【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

# 【發明申請專利範圍】

【第1項】

一種業務資料處理方法，所述方法包括：

獲取待處理業務資料，採用預設方式生成所述待處理業務資料的指紋資料；

將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。

【第2項】

如申請專利範圍第1項所述的業務資料處理方法，其中，獲取待處理業務資料之後，所述方法還包括：

從所述待處理業務資料中提取出預定類型的關鍵要素資料；

相應的，所述採用預設方式生成所述待處理業務資料的指紋資料包括採用預設方式對提取的所述關鍵要素資料進行處理，生成所述待處理業務資料的指紋資料。

【第3項】

如申請專利範圍第1或2項所述的業務資料處理方法，其中，生成所述指紋資料的過程被設置成是單向不可逆的。

【第4項】

如申請專利範圍第1項所述的業務資料處理方法，其中，所述採用預設方式生成所述待處理業務資料的指紋資

料，包括：

對所述待處理業務資料進行雜湊處理，將所述雜湊生成的雜湊值作為所述待處理業務資料的指紋資料。

【第5項】

如申請專利範圍第2項所述的業務資料處理方法，其中，當所述待處理業務資料缺少至少一項所述關鍵要素資料時，執行包括：

根據所述業務資料的業務類型確定缺少的關鍵要素資料的預設值，使用所述預設值作為生成所述指紋資料的關鍵要素資料的取值。

【第6項】

如申請專利範圍第1項所述的業務資料處理方法，其中，所述將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，包括：

採用非同步方式將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中。

【第7項】

一種業務資料驗證方法，所述方法包括：

確定待驗證的業務資料，從儲存的區塊鏈資料中獲取與所述待驗證的業務資料相關的區塊鏈副本資料；所述區塊鏈副本資料包括根據待處理業務資料的指紋資料生成並儲存在區塊鏈中的資料資訊，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料；

採用預設方式計算所述待驗證的業務資料的第一指紋

資料，並獲取所述區塊鏈副本資料中的與所述待驗證的業務資料相對應的第二指紋資料；

比較所述第一指紋資料與所述第二指紋資料是否相同，若相同，則確認所述待驗證的業務資料未被修改。

【第8項】

一種業務資料處理裝置，所述裝置包括：

指紋資料生成模組，用於獲取待處理業務資料，以及採用預設方式生成所述待處理業務資料的指紋資料；

區塊鏈資料生成模組，用於將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。

【第9項】

如申請專利範圍第8項所述的業務資料處理裝置，其中，所述裝置還包括：

關鍵要素提取模組，用於從所述待處理業務資料中提取出預定類型的關鍵要素資料；

相應的，所述指紋資料生成模組採用預設方式生成所述待處理業務資料的指紋資料包括採用預設方式對提取的所述關鍵要素資料進行處理，生成所述待處理業務資料的指紋資料。

【第10項】

如申請專利範圍第8或9項所述的業務資料處理裝置，

其中，所述指紋資料生成模組生成所述指紋資料的過程被設置成是單向不可逆的。

【第11項】

如申請專利範圍第8項所述的業務資料處理裝置，其中，所述指紋資料生成模組採用預設方式生成所述待處理業務資料的指紋資料包括：

對所述待處理業務資料進行雜湊處理，將所述雜湊生成的雜湊值作為所述待處理業務資料的指紋資料。

【第12項】

如申請專利範圍第8項所述的業務資料處理裝置，其中，所述區塊鏈資料生成模組採用非同步方式將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈中。

【第13項】

如申請專利範圍第9項所述的業務資料處理裝置，其中，所述裝置還包括：

預設處理模組，用於當所述待處理業務資料缺少至少一項所述關鍵要素資料時，根據所述業務資料的業務類型確定缺少的關鍵要素資料的預設值，使用所述預設值作為生成所述指紋資料的關鍵要素資料的取值。

【第14項】

一種業務系統，包括I/O介面、處理單元，

所述I/O介面用於接收待處理業務資料；

所述處理單元被設置成，用於採用預設方式生成所述待處理業務資料的指紋資料；還用於將所述業務資料寫入

原有資料庫中，以及將所述指紋資料寫入與所述待處理業務資料對應的區塊鏈資料庫中，生成所述待處理業務資料在所述區塊鏈中的區塊鏈副本資料，所述區塊鏈副本資料中儲存相鄰的上一個節點區塊鏈副本資料中的指紋資料。

【第15項】

如申請專利範圍第14項所述的業務系統，其中，所述處理單元還用於，

從所述待處理業務資料中提取出預定類型的關鍵要素資料；相應的，所述採用預設方式生成所述待處理業務資料的指紋資料包括採用預設方式對提取的所述關鍵要素資料進行處理，生成所述待處理業務資料的指紋資料。

【第16項】

如申請專利範圍第14或15項所述的業務系統，其中，所述處理單元還用於，

從儲存的區塊鏈資料中獲取與所述待驗證的業務資料相關的區塊鏈副本資料，採用預設方式計算所述待驗證的業務資料的第一指紋資料，並獲取所述區塊鏈副本資料中的與所述待驗證的業務資料相對應的第二指紋資料；還用於比較所述第一指紋資料與所述第二指紋資料是否相同，若相同，則確認所述待驗證的業務資料未被修改。