201947444

(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 201947444 A

(43)公開日： 中華民國 108 (2019) 年 12 月 16 日

(21)申請案號：107142408 (22)申請日： 中華民國 107 (2018) 年 11 月 28 日

(51)Int. Cl.： *G06F21/62 (2013.01)* *G06Q20/38 (2012.01)*

(30)優先權：2018/05/10 中國大陸 201810443381.9

(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：陸旭明 (CN)；王虎森 (CN)

(74)代理人：林志剛

申請實體審查：有 申請專利範圍項數：10 項 圖式數：6 共 39 頁

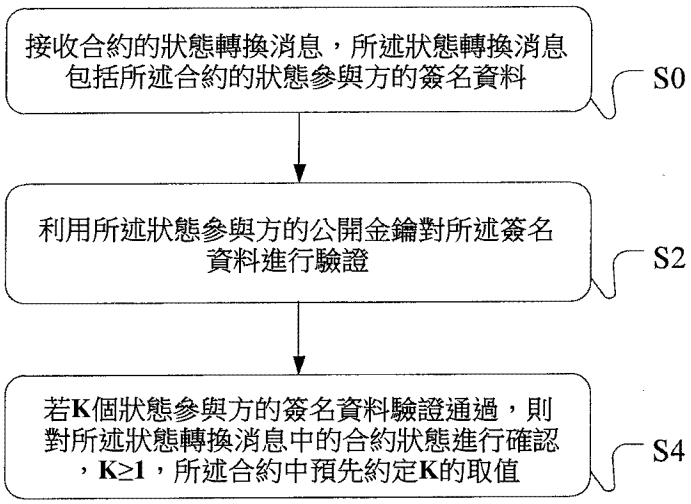
(54)名稱

一種區塊鏈資料處理方法、裝置、處理設備及系統

(57)摘要

本說明書實施例公開了一種區塊鏈資料處理方法、裝置、處理設備及系統。利用本說明實施例可以基於合約狀態參與方的多重簽名來對合約的狀態進行確認，若多重簽名認證通過則可以確認合約狀態轉換的消息有效，執行合約狀態轉換的資料處理。本說明書實施例方案，可以無需關注合約內容，可以不需要翻譯智能合約的內容，通過合約狀態參與者的多重簽名對狀態進行確認可以降低交易風險和交易成本，提高交易處理效率，提供了一種安全可靠的合約狀態轉換的輕的實現方法。

指定代表圖：



【圖 1】

【發明說明書】

【中文發明名稱】

一種區塊鏈資料處理方法、裝置、處理設備及系統

【技術領域】

本說明書實施例方案屬於電腦資料處理的技術領域，尤其涉及一種區塊鏈資料處理方法、裝置、處理設備及系統。

【先前技術】

隨著網際網路的迅速發展，各類資料成爆發式湧現和增長。其中，區塊鏈因其自身的去中心化、不可篡改、分散式等特點，目前已成為許多技術領域中的重點關注和研究的方向。

目前在區塊鏈中主要是基於交易驅動區塊鏈資料的更新，如形成一段時間內的交易的摘要資訊，連同上一塊區塊鏈的摘要儲存後形成新的區塊。一種區塊鏈應用中，如雙方可以線下約定好合同內容或者合同的執行方式，然後將產生的相關的資料存放在聯盟鏈上。在區塊鏈應用中，交易參與方線下常常會涉及合同狀態的新建立、變更、終止等，而這些合同狀態的轉換需要在區塊鏈上進行相應的處理。目前存在的一些實施方式包括，交易方線下確認合同的轉換狀態，然後可以由其中一方直接提交合同狀態變更的指令，相應節點收到後直接進行合同狀態的轉換。顯

然，這種集權的方式容易偽造合同狀態變更的消息，存在交易風險。因此，在區塊鏈資料服務中亟需一種可以更加有效、安全實現合同狀態轉換的解決方案。

【發明內容】

本說明書實施例目的在於提供一種區塊鏈資料處理方法、裝置、處理設備及系統，可以基於合約狀態參與方的多重簽名來對合約的狀態進行確認，可以降低交易風險和交易成本，安全可靠的實現合約狀態轉換。

本說明書實施例提供的一種區塊鏈資料處理方法、裝置、處理設備及系統是包括以下方式實現的：

一種區塊鏈資料處理方法，所述方法包括：

接收合約的狀態轉換消息，所述狀態轉換消息包括所述合約的狀態參與方的簽名資料；

利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證；

若K個狀態參與方的簽名資料驗證通過，則對所述狀態轉換消息中的合約狀態進行確認，$K \geq 1$，所述合約中預先約定K的取值。

一種區塊鏈資料處理裝置，所述裝置包括：

消息接收模組，用於接收合約的狀態轉換消息，所述狀態轉換消息包括所述合約的狀態參與方的簽名資料；

簽名驗證模組，用於利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證；

狀態確認模組，用於在K個狀態參與方的簽名資料驗證通過時，對所述狀態轉換消息中的合約狀態進行確認，K≥1，所述合約中預先約定K的取值。

一種區塊鏈資料處理設備，所述處理設備包括處理器以及用於儲存處理器可執行指令的記憶體，所述處理器執行所述指令時實現：

接收合約的狀態轉換消息，所述狀態轉換消息包括所述合約的狀態參與方的簽名資料；

利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證；

若K個狀態參與方的簽名資料驗證通過，則對所述狀態轉換消息中的合約狀態進行確認，K≥1，所述合約中預先約定K的取值。

一種區塊鏈系統，包括區塊鏈節點設備，所述區塊鏈節點設備包括至少一個處理器用於儲存處理器可執行指令的記憶體，所述處理器執行所述指令時實現本說明書任意一個實施例所述的方法步驟。

本說明書實施例提供的一種區塊鏈資料處理方法、裝置、處理設備及系統，可以基於合約狀態參與方的多重簽名來對合約的狀態進行確認，若多重簽名認證通過則可以確認合約狀態轉換的消息有效，執行合約狀態轉換的資料處理。本說明書實施例方案，可以無需關注合約內容，可以不需要翻譯智能合約的內容，通過合約狀態參與者的多重簽名對狀態進行確認可以降低交易風險和交易成本，提

高交易處理效率，提供了一種安全可靠的合約狀態轉換的輕的實現方法。

【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說明書中記載的一些實施例，對於本領域普通技術人員來講，在不付出創造性勞動性的前提下，還可以根據這些附圖獲得其他的附圖。

圖1是本說明書所述方法實施例的一個處理流程示意圖；

圖2是本說明書實施例提供的創建未確認狀態合約的實施場景示意圖；

圖3是本說明書提供的一種區塊鏈資料處理方法中合同執行實施例流程示意圖；

圖4是本說明書提供的一個合同執行過程中利用臨時金鑰進行資料處理的實施示例示意圖；

圖5是本發明實施例的一種區塊鏈資料處理設備的硬體結構方塊圖；

圖6是本發明實施例的一種區塊鏈資料處理裝置實施的模組結構示意圖。

【實施方式】

為了使本技術領域的人員更好地理解本說明書中的技術方案，下面將結合本說明書實施例中的附圖，對本說明書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說明書中的一部分實施例，而不是全部的實施例。基於本說明書中的一個或多個實施例，本領域普通技術人員在沒有作出創造性勞動前提下所獲得的所有其他實施例，都應當屬於本說明書實施例保護的範圍。

所謂區塊鏈技術，簡稱BT(Blockchain technology)，也被稱之為分散式帳本技術，是一種網際網路資料庫技術，其特點包括去中心化、公開透明本、資料無法篡改。目前區塊鏈技術已經從單純的數位貨幣應用延伸到經濟社會的各個領域，如金融服務、供應鏈管理、文化娛樂、房地產、醫療保健、電子商務等應用場景。區塊鏈中多個使用者個體或群體之間可以基於區塊鏈技術特徵建立聯盟區塊鏈，用於滿足這些使用者或群體的業務發展需求，如支付應用A、醫療服務B、電影票應用C、打車應用D構建的四個區塊鏈節點的聯盟區塊鏈。區塊鏈中多個使用者個體或群體或機構之間可以基於區塊鏈技術特徵建立聯盟區塊鏈或私有鏈，加入區塊鏈並成為其中的成員。成員之間的進行的交易資料可以儲存到區塊鏈中，例如鏈下簽署的合同內容可以儲存的區塊鏈中。

需要說明的是，本說明書實施例中所涉及的鏈下或涉及的鏈上主要是指是否是在區塊鏈上進行的資料操作，如

線下使用者商談簽署合約、認證機構進行身份證實、頒發證書等進行的區塊鏈之外的操作可以為鏈下相關的操作，將公開金鑰或證書提交到區塊鏈上、區塊鏈節點的驗證、資料儲存等可以為鏈上相關的操作，如將資料提交到區塊鏈上進行儲存可以稱為上鏈。

隨著各行業區塊鏈的逐步廣泛應用，對區塊鏈的處理性能、適應企業業務需求的靈活性等要求也越來越高。本說明書提供的實施方案可以在區塊鏈上區塊鏈節點基於多重簽名實現交易合約狀態轉換，可以不關注合約內容，不翻譯智能合約的內容，實現區塊鏈節點的自我管理。

傳統的合同通常是合同參與方經過商議和討論達成一致後，記錄在紙張上。本說明書實施例中所涉及的合同，可以以數位化或其他電腦資料儲存形式(如量子電腦)儲存記錄區塊鏈上。本說明書實施例中所述的合約，也可以成為智能合約，在區塊鏈技術應用中可以指包括由交易驅動的、具有狀態的、運行在一個複製的、分享的帳本之上的、數位化合約的電腦程式，可以是一個可以被信任、並按照事先的規則執行的操作集合。傳統的合同由電腦語言編碼成電腦資料儲存到區塊鏈後對應的資料可以為本說明書中一些實施例中的合約。一般的，合約判定後通常不能修改(不排除區塊鏈代碼本身允許修改或通過合約調用等進行的合約修改)，但合約的狀態可以進行轉換，如由待確認轉換為確認，或者由確認轉換為終止。區塊鏈上可以存在多份合約，一般的，每一份合約包括至少兩個合約參

與方，合約的內容可以包括合同的建立和執行的相關資料操作。合約可以使用一種或多種電腦語言編碼後儲存。

下面以另一個具體的應用場景為例對本說明書實施方案進行說明。具體的，圖1是本說明書提供的所述一種區塊鏈資料處理方法實施例場景示意圖。雖然本說明書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創造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說明書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、伺服器或終端產品應用時，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、伺服器集群的實施環境)。

如圖1所示，一個實施例中，所述方法可以包括：

S0：接收合約的狀態轉換消息，所述狀態轉換消息包括所述合約的狀態參與方的簽名資料；

S2：利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證；

S4：若K個狀態參與方的簽名資料驗證通過，則對所述狀態轉換消息中的合約狀態進行確認，K≥1，所述合約中預先約定K的取值。

如果需要對合約的狀態進行轉換，初始建立的合約由

pending(待確認)狀態轉換為clear(確認)狀態，此時可以由其中一個(如最後一個確認合同)狀態參與方所在的區塊鏈節點發起對某個合約的狀態轉換請求，具體的可以是一個狀態轉換消息。區塊鏈上的各個節點可以收到合約狀態轉換的消息，最終合約狀態轉換的確認可以由專門的區塊鏈節點進行處理，或者按照預設規則分配到的區塊鏈節點進行處理。狀態確認後可以在區塊鏈上進行廣播。

一般的，所述簽名和驗證的金鑰可以由各個區塊鏈節點產生。合約參與方通常是指包括合約所涉及的參與方，如合約內容涉及參與方A、B、C、D。本實施例不排除所述的合約參與方還可以包括約定允許的其他參與方，如不涉及交易業務內容的協力廠商、擔保方、監管方等。所述的狀態參與方一般的可以包括對應的合約的全部或部分參與方，如可以預先在合約中約定若合約狀態發生轉換，需要所有參與方均簽名確認後才生效執行。或者可以預定合同參與方A、B、C為有效的狀態參與方，D不能進行合同狀態的轉換，若進行合約狀態的轉換，則需要狀態參與方A、B、C均簽名確認後才生效。當然，其他的實施例中還可以約定添加其他節點的簽名確認，如金融監管機構或智能合約平台設置的監管方。

本說明書的一些實施例中，合約狀態的轉換可以設置為需要所有狀態參與方的私密金鑰簽名，在所有狀態參與方的簽名驗證通過後，執行狀態轉換。為便於描述，合約狀態轉換所需所有狀態參與方的簽名可以稱為多重簽名。

因此，所述方法的一個實施例中，所述對所述狀態轉換消息中的合約狀態進行確認可以包括：

S40：在判定各個狀態參與方的多重簽名通過後，執行合約狀態的轉換，所述多重簽名包括預先在合約中約定的合約狀態轉換所需要的狀態參與方的簽名資料。

本說明書的一些實施例中，合約的狀態轉換若涉及到合約的內容資訊，則可以使用金鑰進行加密，如使用私密金鑰加密。一般的，合約參與方的金鑰通常採用對稱或非對稱演算法產生，包括公開金鑰和私密金鑰。公開金鑰參與方產生的公開金鑰可以相互發送。因此，合約狀態轉換時可以對消息內容進行加密，這樣，雖然該合約的其他非狀態參與方對應的區塊鏈節點可以收到合約的狀態轉換消息，但無法對內容進行驗證，也無法執行相應的操作。本說明書提供的所述方法的一個實施例中，所述狀態轉換消息由所述狀態參與方加密處理產生，以及所述狀態參與方所在的區塊鏈節點儲存有所述加密處理對應的解密金鑰。

與對稱加密演算法不同，非對稱加密演算法會產生兩個金鑰：公開金鑰(publickey)和私密金鑰(privatekey)，或簡稱公開金鑰和私密金鑰。公開金鑰與私密金鑰是一對，如果用公開金鑰對資料進行加密，只有用對應的私密金鑰才能解密；如果用私密金鑰對資料進行加密，那麼只有用對應的公開金鑰才能解密。在本說明書的一些實施例場景中，非對稱加密中使用的演算法可以包括：RSA、Elgamal、背包演算法、Rabin、D-H、ECC(橢圓曲線加密

演算法)等。

本說明書的另一個實施例中採用非對稱加密演算法產生金鑰可以為臨時的金鑰資訊，可以按照設定的規則進行動態更新，如，一天更新一次金鑰，或者一周更新一次金鑰，更新後的公開金鑰的可以通過端到端的加密新資訊通道發送給相應的狀態參與方，或者儲存到區塊鏈上，由區塊鏈節點授權查詢後獲取。合約參與方的區塊鏈節點可以利用公開金鑰對狀態轉換消息進行驗證，確認是由真實的合約參與方發來的消息。因此，本說明書所述方法的另一個實施例中，所述簽名資料以及驗證處理中使用的金鑰包括按照預設規則動態更新的臨時金鑰。

上述實施例中所述的合約狀態轉換可以發生在合約建立的處理階段，也可以發生在合約執行的處理階段。所述的合約的建立或執行可以包括前述所述的格式合同的創建，也可以包括正式合同的簽署確認，還可以包括合同的執行的處理，所述的合同可以視為合約的一種。圖2是本說明書實施例提供的創建未確認狀態合約的實施場景示意圖。當然，下述實施例的描述並不對基於本說明書的其他可擴展到的技術方案構成限制。例如其他的實施場景中，涉及到的合約交易的狀態轉換處理均可使用本說明書中的一種或多種實施方案。所述的交易更廣義的還可以包括備忘錄、合約、規章、報表、公示等單方或雙方或多方需要儲存到區塊鏈上以更新區塊鏈節點資料進行的資料操作。具體的一種應用場景如圖2所示，假設目標合同涉及合同

參與方A、B兩方。A和B為聯盟鏈的成員，分別持有相應的證書。該證書可以證明其為區塊鏈上的合法成員，可以進行區塊鏈上合同的創建、執行等處理。

合同創建後儲存到區塊鏈上的狀態為待確認。具體的過程可以包括：

A和B可以各自獨立產生自己的臨時金鑰對(tpk_A，tsk_A)、(tpk_B, tsk_B)。雙方的臨時公開金鑰可以通過建立的端到端的加密通道進行資料傳輸。如基於SSL(Secure Sockets Layer安全套接層)協議的端到端加密通道。這樣可以進一步提高資料傳輸的安全性。為了支援區塊鏈上的兩個使用者的端到端線下通訊需求，使用者(包括合同參與方)通常需要相互校驗身份，並且能夠同區塊鏈進行通訊，通過區塊鏈查詢對方身份，並核實是區塊鏈合法使用者。具體的一個流程可以包括如下：

(1) 使用者A、B通過區塊鏈註冊機構，可以以智能合約或者非智能合約的形式將實體資訊和數位身份註冊在區塊鏈平台上。區塊鏈平台對註冊機構的簽名進行校驗，通過後，A、B的實體資訊和數位身份被儲存在區塊鏈上。數位身份可以包含使用者的公開金鑰和私密金鑰等，實體資訊可以包含使用者的姓名、身份證等資訊。

(2) 使用者A和使用者B建立一個加密通道。A、B首先相互發送對方的數字身份摘要到區塊鏈平台，平台查詢到A、B是合法使用者後，給A、B返回確認消息，否則發回否定消息，A、B通訊中止。

(3) 為了確認B的身份，A可以從B獲取查詢的授權(即對A查詢請求的簽名)，向區塊鏈提交查詢申請。B同理做此步驟提交對A的查詢。

(4) 區塊鏈平台檢驗A、B的查詢和授權簽名，同時查到A、B是區塊鏈使用者，將A、B的實體資訊分別發送給雙方。若A或B不是區塊鏈使用者，則返回失敗消息。A、B通訊中止。

(5) A、B對對方實體資訊核實後，利用數位身份建立加密通道，交換消息，如交換臨時公開金鑰。

A和B相互發送臨時公開金鑰後，可以分別使用自己的私密金鑰對(目標合同的合同內容，tpk_A，tpk_B)進行簽名，產生各自對應的私密金鑰簽名後的資料，在此可以統一稱為第一簽名資料，同樣的，對目標合同的合同內容的簽名也可以簡稱為對目標合同的簽名。如A可以使用私密金鑰tsk_A對(目標合同，tpk_A，tpk_B)簽名產生A的第一簽名資料sigA，B使用私密金鑰tsk_B對(目標合同，tpk_A，tpk_B)簽名產生B的第一簽名資料sigB。第一簽名資料也可以相互發送，如A將sigA發送給B。

一些實施例應用場景中，合同的交易可以受到監管方的監管，可以查閱、審核、審查、阻止合同，監管基於合同的非法行為。一些實施例中，所述的監管方可以包括合法監管機構，如中央銀行、證監會等國家金融監管機構，可以使用監管金鑰來監督區塊鏈交易。另一些實施例中也可以預先在合約規則中約定具有監管效力的監管方，如指

定的一個或多個成員，或者另一種實施方式中可以約定在達到預定的數量或比例的成員認同某個成員，該成員具有監管權利。達到預定數量或比例的成員在此可以成員監管成員組，如區塊鏈中有10個成員，可以預定若7個成員或者70%的成員認同成員A，則成員A可以作為監管方。

使用監管方廣播的監管公開金鑰加密的資訊內容可以包括目標合同(合同內容)、所有合同參與方的臨時公開金鑰、所有合同參與方的簽名資料，或者還可以包括所有合同參與方的證書。如A使用監管金鑰key對(目標合同，tpk_A，tpk_B，sigA，sigB，certA，certB)進行加密，產生加密合同。加密合同可以由任意一個合同參與方處理後產生。這樣，監管方可以使用自己對應的解密金鑰，如私密金鑰，從區塊鏈中獲取目標合同，驗證合同參與方是否非法，合同內容是否違法等，以進行對區塊鏈上合同的監督和約束。如，監管方使用解密合同，查閱合同內容以及國外合作方後，發現存在合同存在涉及國防專利的技術非法轉讓，則可以通過提交區塊鏈交易阻止該合同的進行。當然，其他的實施例中，如果涉及該目標合同的交易對於其他區塊鏈成員C可見，那麼也可以使用C的公開金鑰進行加密。使用C的公開金鑰加密以及成員C使用自己私密金鑰解密查看目標合同等的處理方式可以參考上述監管方的處理，在此不做贅述。

產生的加密合同在上鏈之前，各個合同參與方可以對該加密合同進行私密金鑰簽名，簽名後的資料連同各個合

同參與方的臨時公開金鑰tpk_A、tpk_B作為儲存到區塊鏈上的創建資料。

創建資料可以提交到區塊鏈上進行儲存。當然，區塊鏈上還可以設置有智能合約平台，所述的創建資料可以提交到智能合約平台，由智能合約平台進行管理。

圖3是本說明書提供的一種區塊鏈資料處理方法中合同執行實施例流程示意圖，如圖3所示，所述區塊鏈資料還可以包括合同執行資料，及採用下述方式判定所述合同執行資料：

S40：利用所述監管金鑰對判定的新合同進行加密，產生加密新合同，所述新合同由合同參與方線下對所述目標合同的執行過程達成共識後判定；

S42：各個合同參與方可以利用所述加密新合同對應的臨時私密金鑰對所述加密新合同進行簽名，產生第二簽名資料；

S44：基於所述第二簽名資料、加密新合同判定合同執行資料。

上述S42的執行處理，對於合同參與方的處理裝置而言，可以理解為判定各個合同參與方對所述加密新合同的簽名後，基於所述第二簽名資料、加密新合同判定合同執行資料。例如一個合同參與方判定其他所有合同參與方(包括自己)均使用了臨時私密金鑰進行簽名後，則將各方簽名後的第二簽名資料和加密新合同判定為合同執行資料。然後可以將合同執行資料提交至區塊鏈。上述S42中

所示加密新合同對應的臨時金鑰可以與所述加密新合同對應的目標合同在創建時使用的臨時金鑰相同，也可以不相同。例如對於在更新合同內容簽署判定的新合同時已經達到了臨時金鑰更換週期，此時再對加密新合同進行簽名時使用的臨時金鑰與之前對應的目標合同創建儲存到區塊鏈上時的臨時金鑰不相同。更新的臨時金鑰可以通過提交交易更新至區塊鏈相應的資料中。

圖4是本說明書提供的一個合同執行過程中利用臨時金鑰進行資料處理的實施示例示意圖。如圖4所示，假設合同的執行涉及A、B雙方利益。A、B線下對合同執行過程達成共識，如增加或修改了合同內容，形成新合同v1。A或B對新合同利用監管金鑰key加密，產生加密新合同V1。然後各個合同參與方分別可以利用對應的原目標合同的臨時私密金鑰簽名，如A可以利用目標合同建立時的臨時私密金鑰tsk_A進行簽名後，再由B使用臨時私密金鑰tsk_B進行簽名。所有合同參與方簽名後的資料連同加密新合同一起上鏈。包括所述第二簽名資料、加新合同的將要提交至區塊鏈的資料可以稱為合同執行資料，或者提交到區塊鏈保存後也可以稱為合同執行資料，上述目標合同的創建資料同理。在此過程，與新建合同不同的是，A、B在執行合同狀態轉移的過程中，可以不需要獲取監管方授權，如合同的變更、合同的生效、合同的中斷、合同的終止等，在合同參與方使用監管公開金鑰加密，然後各個合同參與方私密金鑰簽名判定新合同或者合同的狀態轉移

後，合同內容以及合同狀態即可以生效。本實施例中監管方可以查閱、查看交易的資料資訊，除特殊規定情況下，交易的發起或執行，如合同更新，可以無需獲取監管方授權。

產生的區塊鏈資料可以提交到區塊鏈上進行儲存。當然，區塊鏈上還可以設置有智能合約平台，所述的區塊鏈資料可以提交到智能合約平台，由智能合約平台進行管理。

本實施例應用場景中，合同的執行可以包括對初始創建的格式合同內容的補充和確認，在A、B雙方達成一致確認合同後，該合同的在區塊鏈上的狀態需要由待確認狀態轉換為確認狀態。此時A和B所在的區塊鏈節點可以向智能合約管理平台發送狀態轉換消息，A和B分別在各自的狀態轉換消息中使用自己的私密金鑰進行簽名。智能合約管理平台在收到A和B中的任意一個時進行簽名驗證。此時，即使驗證通過也不會進行轉換狀態的執行，只有在收到A和B的多重簽名，並且全部驗證通過後，才確認合約狀態的轉換。

本說明書實施例提供的一種區塊鏈資料處理方法，可以基於合約狀態參與方的多重簽名來對合約的狀態進行確認，若多重簽名認證通過則可以確認合約狀態轉換的消息有效，執行合約狀態轉換的資料處理。本說明書實施例方案，可以無需關注合約內容，可以不需要翻譯智能合約的內容，通過合約狀態參與者的多重簽名對狀態進行確認可

以降低交易風險和交易成本，提高交易處理效率，提供了一種安全可靠的合約狀態轉換的輕的實現方法。

本說明書中上述方法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。相關之處參見方法實施例的部分說明即可。

本申請實施例所提供的方法實施例可以在區塊鏈終端、區塊鏈伺服器或者類似的運算裝置中執行。以運行在區塊鏈節點設備(可以為使用者端，或單台伺服器或伺服器集群)上為例，圖5是本發明實施例的一種區塊鏈資料處理設備的硬體結構方塊圖。如圖5所示，區塊鏈處理設備10可以包括一個或多個(圖中僅示出一個)處理器102(處理器102可以包括但不限於微處理器MCU或可程式設計邏輯裝置FPGA等的處理裝置)、用於儲存資料的記憶體104、以及用於通訊功能的傳輸模組106。本領域普通技術人員可以理解，圖5所示的結構僅為示意，其並不對上述電子裝置的結構造成限定。例如，處理設備10還可包括比圖5中所示更多或者更少的元件，例如還可以包括其他的處理硬體，如GPU(Graphics Processing Unit，影像處理器)，或者具有與圖5所示不同的配置。

記憶體104可用于儲存應用軟體的軟體程式以及模組，如本發明實施例中的搜索方法對應的程式指令/模組，處理器102通過運行儲存在記憶體104內的軟體程式以及模組，從而執行各種功能應用以及資料處理，即實現上

述導航交互介面內容展示的處理方法。記憶體104可包括高速隨機記憶體，還可包括非揮發性記憶體，如一個或者多個磁性儲存裝置、快閃記憶體、或者其他非揮發性固態記憶體。在一些實例中，記憶體104可進一步包括相對於處理器102遠端設置的記憶體，這些遠端存放器可以通過網路連接至電腦終端10。上述網路的實例包括但不限於網際網路、企業內部網、局域網、移動通訊網及其組合。

傳輸模組106用於經由一個網路接收或者發送資料。上述的網路具體實例可包括電腦終端10的通訊供應商提供的無線網路。在一個實例中，傳輸模組106包括一個網路介面卡(Network Interface Controller，NIC)，其可通過基站與其他網路設備相連從而可與網際網路進行通訊。在一個實例中，傳輸模組106可以為射頻(Radio Frequency，RF)模組，其用於通過無線方式與網際網路進行通訊。

基於上述所述的區塊鏈資料處理的方法，本說明書還提供一種區塊鏈資料處理裝置。所述的裝置可以包括使用了本說明書實施例所述方法的系統(包括分散式系統)、軟體(應用)、模組、元件、伺服器、使用者端等並結合必要的實施硬體的設備裝置。基於同一創新構思，本說明書提供的一種實施例中的處理裝置如下面的實施例所述。由於裝置解決問題的實現方案與方法相似，因此本說明書實施例具體的處理裝置的實施可以參見前述方法的實施，重複之處不再贅述。儘管以下實施例所描述的裝置較佳地以軟體來實現，但是硬體，或者軟體和硬體的組合的實現也是

可能並被構想的。具體的，如圖6所示，一種可以用於區塊鏈節點的區塊鏈資料處理裝置的實施例中，可以包括：

消息接收模組201，可以用於接收合約的狀態轉換消息，所述狀態轉換消息包括所述合約的狀態參與方的簽名資料；

簽名驗證模組202，可以用於利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證；

狀態確認模組203，可以用於在K個狀態參與方的簽名資料驗證通過時，對所述狀態轉換消息中的合約狀態進行確認，K≥1，所述合約中預先約定K的取值。

需要說明的是，本說明書實施例上述所述的處理裝置，根據相關方法實施例的描述還可以包括其他的實施方式。具體的實現方式可以參照方法實施例的描述，在此不作一一贅述。

本說明書實施例提供的設備型號識別方法可以在電腦中由處理器執行相應的程式指令來實現，如使用windows/Linux作業系統的c++/java語言在PC端/伺服器端實現，或其他例如android、iOS系統相對應的應用設計語言集合必要的硬體實現，或者基於量子電腦的處理邏輯實現等。具體的，本說明書提供的一種處理設備實現上述方法的實施例中，所述處理設備可以包括處理器以及用於儲存處理器可執行指令的記憶體，所述處理器執行所述指令時實現：

接收合約的狀態轉換消息，所述狀態轉換消息包括所

述合約的狀態參與方的簽名資料；

利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證；

若K個狀態參與方的簽名資料驗證通過，則對所述狀態轉換消息中的合約狀態進行確認，K≥1，所述合約中預先約定K的取值。

基於前述方法實施例描述，所述設備的另一個實施例中，所述對所述狀態轉換消息中的合約狀態進行確認包括：

在判定各個狀態參與方的多重簽名通過後，執行合約狀態的轉換，所述多重簽名包括預先在合約中約定的合約狀態轉換所需要的狀態參與方的簽名資料。

基於前述方法實施例描述，所述設備的另一個實施例中，所述狀態轉換消息由所述狀態參與方加密處理產生，以及所述狀態參與方所在的區塊鏈節點儲存有所述加密處理對應的解密金鑰。

基於前述方法實施例描述，所述設備的另一個實施例中，所述簽名資料以及驗證處理中使用的金鑰包括按照預設規則動態更新的臨時金鑰。

上述所述的裝置或設置具體的可以應用在區塊鏈節點的伺服器中。

上述的指令可以儲存在多種電腦可讀儲存介質中。所述電腦可讀儲存介質可以包括用於儲存資訊的物理裝置，可以將資訊數位化後再以利用電、磁或者光學等方式的媒

體加以儲存。本實施例所述的電腦可讀儲存介質有可以包括：利用電能方式儲存資訊的裝置如，各式記憶體，如RAM、ROM等；利用磁能方式儲存資訊的裝置如，硬碟、軟碟、磁帶、磁芯記憶體、磁泡記憶體、USB；利用光學方式儲存資訊的裝置如，CD或DVD。當然，還有其他方式的可讀儲存介質，例如量子記憶體、石墨烯記憶體等等。本實施例中所述的裝置或伺服器或使用者端或或處理設備或系統中的指令同上描述。

基於前述所述，本說明書實施例還提供一種區塊鏈系統，包括區塊鏈節點設備，所述區塊鏈節點設備包括至少一個處理器用於儲存處理器可執行指令的記憶體，所述處理器執行所述指令時實現：

本說明書實施例中的任意一個方法實施例所述的步驟。

需要說明的是，本說明書實施例上述所述的裝置、處理設備、系統，根據相關方法實施例的描述還可以包括其他的實施方式。具體的實現方式可以參照方法實施例的描述，在此不作一一贅述。

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，對於硬體+程式類實施例而言，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，多工處理和並行處理也是可以的或者可能是有利的。

本說明書實施例提供的一種區塊鏈資料處理方法、裝置、處理設備及系統，可以基於合約狀態參與方的多重簽名來對合約的狀態進行確認，若多重簽名認證通過則可以確認合約狀態轉換的消息有效，執行合約狀態轉換的資料處理。本說明書實施例方案，可以無需關注合約內容，可以不需要翻譯智能合約的內容，通過合約狀態參與者的多重簽名對狀態進行確認可以降低交易風險和交易成本，提高交易處理效率，提供了一種安全可靠的合約狀態轉換的輕的實現方法。

雖然本申請提供了如實施例或流程圖所述的方法操作步驟，但基於常規或者無創造性的勞動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。在實際中的裝置或使用者端產品執行時，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)。

儘管本說明書實施例內容中提到SSL的加密通訊、監

管金鑰的產生方式、包括合同建立和執行的交易定義描述、公開金鑰私密金鑰進行的加密簽名等之類的資料獲取、定義、交互、計算、判斷、加密等操作和資料描述，但是，本說明書實施例並不局限於必須是符合行業通訊標準、標準非對稱加密演算法、通訊協定和標準資料模型/範本或本說明書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，仍然可以屬於本說明書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判定。由設計人員自行程式設計來把一個數位系統「集成」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)的電腦可讀介質、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構件，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構件內的結構。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構件內的結構。

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、車載人機交互設備、蜂窩電話、相機電話、智能型電話、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。

雖然本說明書實施例提供了如實施例或流程圖所述的方法操作步驟，但基於常規或者無創造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)。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、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，在實施本說明書實施例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集成到另一個系統，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合或直接耦合或通訊連接可以是通過一些介面，裝置或單元的間接耦合或通訊連接，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構件，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構

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構件內的結構。

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／或方框、以及流程圖和／或方塊圖中的流程和／或方框的結合。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／或方塊圖一個方框或多個方框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／或方塊圖一個方框或多個方框中指定的功能。

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／或方塊圖一個方框或多個方框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介質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)。記憶體是電腦可讀介質的示例。

電腦可讀介質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。電腦的儲存介質的例子包括，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)、電可擦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介質，可用於儲存可以被計算設備訪問的資訊。按照本文中的界定，電腦可讀介質不包括暫存電腦可讀媒體(transitory media)，如調製的資料信號和載波。

本領域技術人員應明白，本說明書的實施例可提供為方法、系統或電腦程式產品。因此，本說明書實施例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，本說明書實施例可採用在一個

或多個其中包含有電腦可用程式碼的電腦可用儲存介質(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。

本說明書實施例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說明書實施例，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介質中。

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。在本說明書的描述中，參考術語「一個實施例」、「一些實施例」、「示例」、「具體示例」、或「一些示例」等的描述意指結合該實施例或示例描述的具體特徵、結構、材料或者特點包含於本說明書實施例的至少一個實施例或示例中。在本說明書中，對上述術語的示意性表述不必須針對的是相同的實施例或示例。而且，描述的具體特徵、結構、材料或者特點可以在任一個或多個實施例或示例中以合適的方式結合。此外，在不相互矛盾的情況下，本領

域的技術人員可以將本說明書中描述的不同實施例或示例以及不同實施例或示例的特徵進行結合和組合。

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

【符號說明】

10：伺服器

102：處理器

104：非揮發性記憶體

106：傳輸模組

201：消息接收模組

202：簽名驗證模組

203：狀態確認模組

201947444

【發明摘要】

【中文發明名稱】

一種區塊鏈資料處理方法、裝置、處理設備及系統

【中文】

本說明書實施例公開了一種區塊鏈資料處理方法、裝置、處理設備及系統。利用本說明實施例可以基於合約狀態參與方的多重簽名來對合約的狀態進行確認，若多重簽名認證通過則可以確認合約狀態轉換的消息有效，執行合約狀態轉換的資料處理。本說明書實施例方案，可以無需關注合約內容，可以不需要翻譯智能合約的內容，通過合約狀態參與者的多重簽名對狀態進行確認可以降低交易風險和交易成本，提高交易處理效率，提供了一種安全可靠的合約狀態轉換的輕的實現方法。

【指定代表圖】第(1)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】

一種區塊鏈資料處理方法，所述方法包括：

接收合約的狀態轉換消息，所述狀態轉換消息包括所述合約的狀態參與方的簽名資料；

利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證；

若K個狀態參與方的簽名資料驗證通過，則對所述狀態轉換消息中的合約狀態進行確認，K≥1，所述合約中預先約定K的取值。

【第2項】

如申請專利範圍第1項所述的方法，所述對所述狀態轉換消息中的合約狀態進行確認包括：

在判定各個狀態參與方的多重簽名通過後，執行合約狀態的轉換，所述多重簽名包括預先在合約中約定的合約狀態轉換所需要的狀態參與方的簽名資料。

【第3項】

如申請專利範圍第1項所述的方法，所述狀態轉換消息由所述狀態參與方加密處理產生，以及所述狀態參與方所在的區塊鏈節點儲存有所述加密處理對應的解密金鑰。

【第4項】

如申請專利範圍第3項所述的方法，所述簽名資料以及驗證處理中使用的金鑰包括按照預設規則動態更新的臨時金鑰。

【第5項】

一種區塊鏈資料處理裝置，所述裝置包括：

消息接收模組，用於接收合約的狀態轉換消息，所述狀態轉換消息包括所述合約的狀態參與方的簽名資料；

簽名驗證模組，用於利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證；

狀態確認模組，用於在K個狀態參與方的簽名資料驗證通過時，對所述狀態轉換消息中的合約狀態進行確認，K≥1，所述合約中預先約定K的取值。

【第6項】

一種區塊鏈資料處理設備，所述處理設備包括處理器以及用於儲存處理器可執行指令的記憶體，所述處理器執行所述指令時實現：

接收合約的狀態轉換消息，所述狀態轉換消息包括所述合約的狀態參與方的簽名資料；

利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證；

若K個狀態參與方的簽名資料驗證通過，則對所述狀態轉換消息中的合約狀態進行確認，K≥1，所述合約中預先約定K的取值。

【第7項】

如申請專利範圍第6項所述的處理設備，所述對所述狀態轉換消息中的合約狀態進行確認包括：

在判定各個狀態參與方的多重簽名通過後，執行合約

狀態的轉換，所述多重簽名包括預先在合約中約定的合約狀態轉換所需要的狀態參與方的簽名資料。

【第8項】

如申請專利範圍第6項所述的處理設備，所述狀態轉換消息由所述狀態參與方加密處理產生，以及所述狀態參與方所在的區塊鏈節點儲存有所述加密處理對應的解密金鑰。

【第9項】

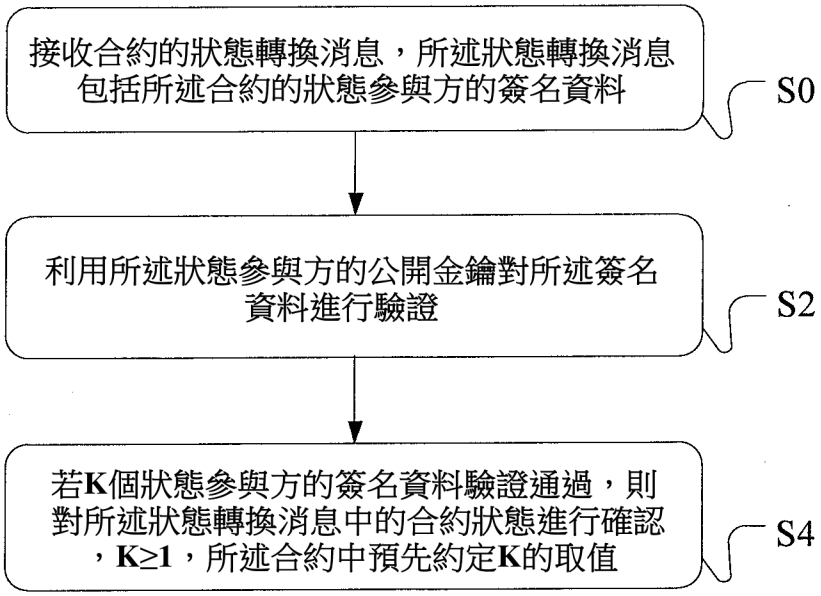
如申請專利範圍第8項所述的處理設備，所述簽名資料以及驗證處理中使用的金鑰包括按照預設規則動態更新的臨時金鑰。

【第10項】

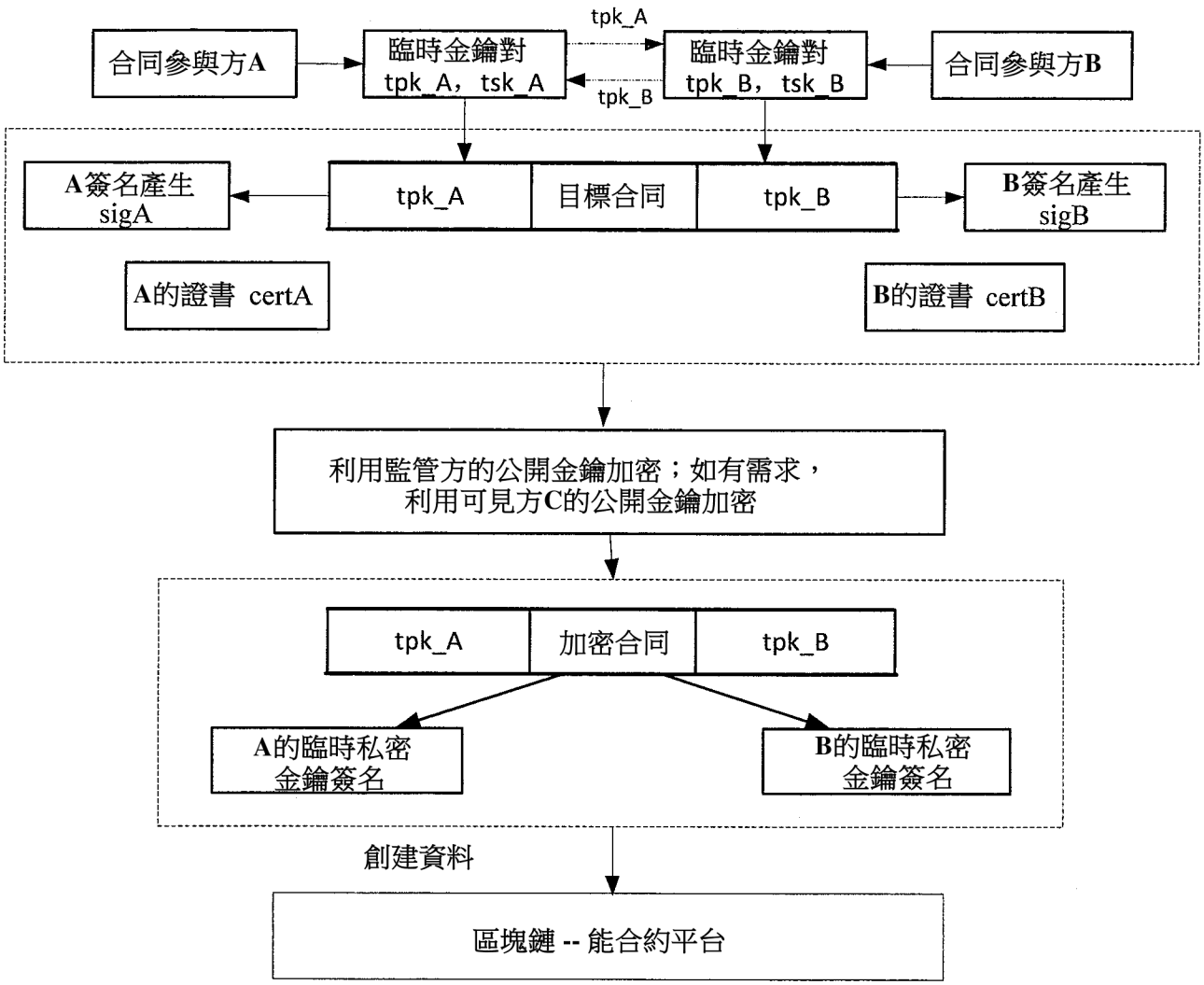
一種區塊鏈系統，包括區塊鏈節點設備，所述區塊鏈節點設備包括至少一個處理器用於儲存處理器可執行指令的記憶體，所述處理器執行所述指令時實現：

申請專利範圍第1-4項中的任意一項方法所述的步驟。

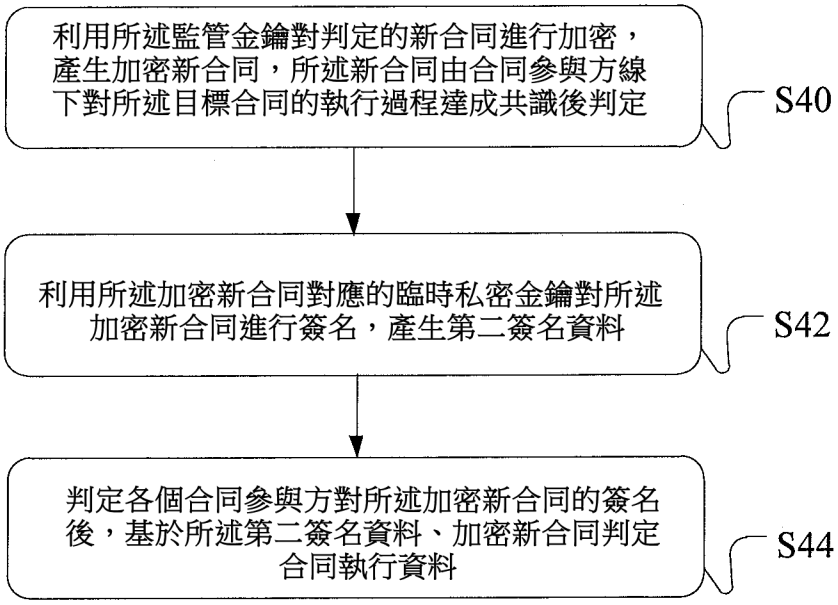
【發明圖式】


接收合約的狀態轉換消息，所述狀態轉換消息包括所述合約的狀態參與方的簽名資料
S0
利用所述狀態參與方的公開金鑰對所述簽名資料進行驗證
S2
若K個狀態參與方的簽名資料驗證通過，則對所述狀態轉換消息中的合約狀態進行確認，K≥1，所述合約中預先約定K的取值
S4

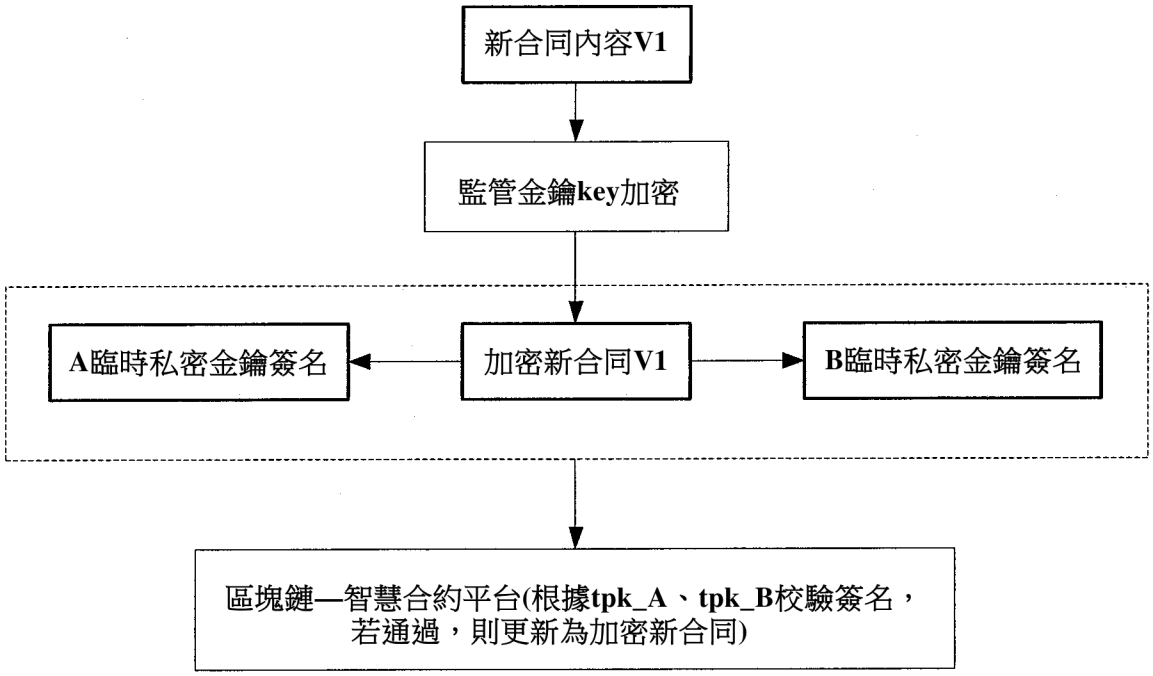
【圖 1】


合同參與方A
臨時金鑰對
tpk_A，tsk_A
tpk_A
tpk_B
臨時金鑰對
tpk_B，tsk_B
合同參與方B
A簽名產生
sigA
tpk_A
目標合同
tpk_B
B簽名產生
sigB
A的證書 certA
B的證書 certB
利用監管方的公開金鑰加密；如有需求，
利用可見方C的公開金鑰加密
tpk_A
加密合同
tpk_B
A的臨時私密
金鑰簽名
B的臨時私密
金鑰簽名
創建資料
區塊鏈 -- 能合約平台

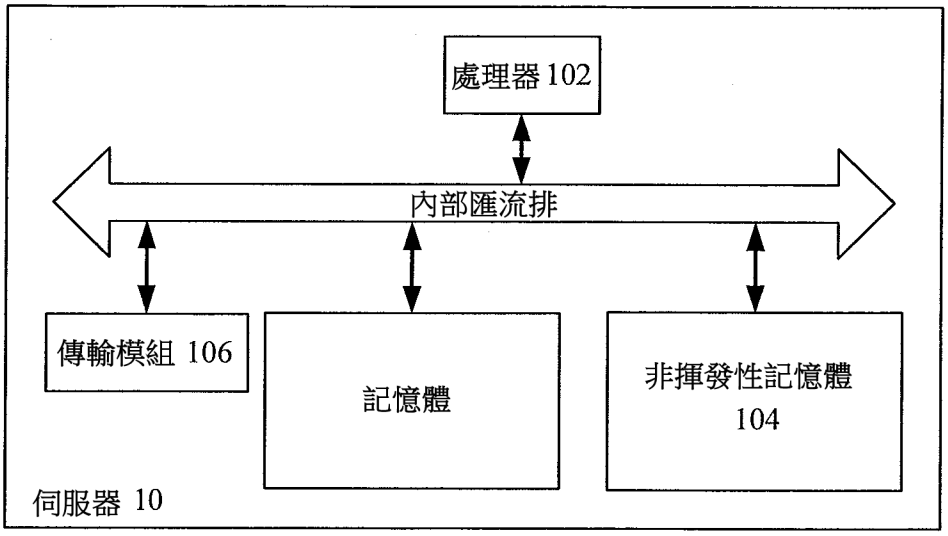
【圖 2】


利用所述監管金鑰對判定的新合同進行加密，產生加密新合同，所述新合同由合同參與方線下對所述目標合同的執行過程達成共識後判定
S40
利用所述加密新合同對應的臨時私密金鑰對所述加密新合同進行簽名，產生第二簽名資料
S42
判定各個合同參與方對所述加密新合同的簽名後，基於所述第二簽名資料、加密新合同判定合同執行資料
S44

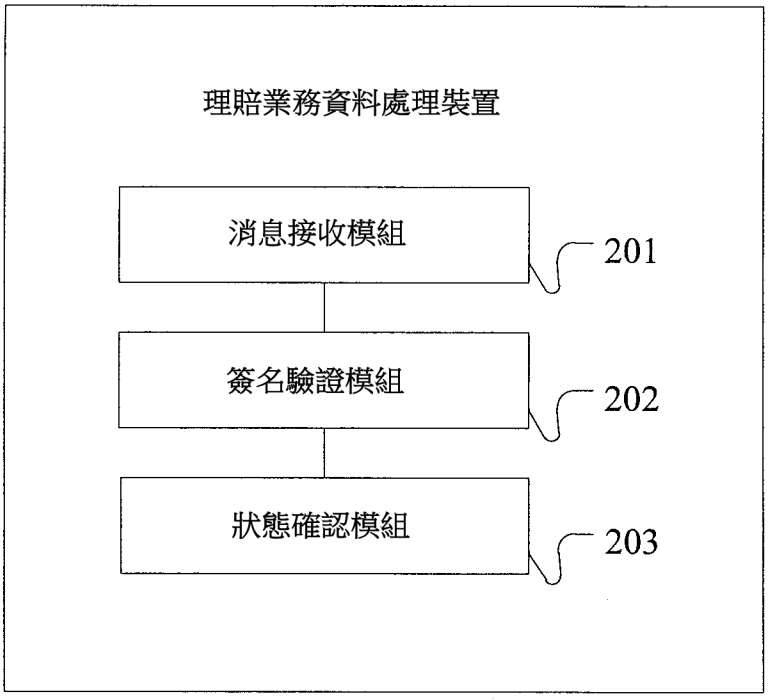
【圖 3】


新合同內容V1
監管金鑰key加密
A臨時私密金鑰簽名
加密新合同V1
B臨時私密金鑰簽名
區塊鏈—智慧合約平台(根據tpk_A、tpk_B校驗簽名，若通過，則更新為加密新合同)

【圖 4】


處理器 102
內部匯流排
傳輸模組 106
記憶體
非揮發性記憶體
104
伺服器 10

【圖 5】


理賠業務資料處理裝置
消息接收模組
201
簽名驗證模組
202
狀態確認模組
203

【圖 6】