



(21)申請案號：106138732

(22)申請日：中華民國 106 (2017) 年 11 月 09 日

(51)Int. Cl. :

G06Q10/00 (2012.01)

H04L9/00 (2006.01)

H04L29/06 (2006.01)

H04L12/58 (2006.01)

G06F3/06 (2006.01)

(30)優先權：2017/02/24 中國大陸 201710102824.3

(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：李奕 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW 200635317A

CN 106022917A

US 2007/0005962A1

WO 2017/027438A1

審查人員：林育弘

申請專利範圍項數：12 項 圖式數：4 共 41 頁

(54)名稱

資料發送方法及裝置

(57)摘要

本案公開了一種資料發送方法，用以解決現有的資料交換過程中資料的安全性較低的問題。該方法包括：資料交易平台將第一用戶與第二用戶達成的資料交易的合約寫入區塊鏈中並儲存；資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；所述第一終端將加密後的第一資料發送至第二終端，所述第二終端為第二用戶對應的終端；資料交換平台將第一密鑰發送至所述第二終端；第二終端根據第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料。本案還公開了一種資料發送裝置。

指定代表圖：

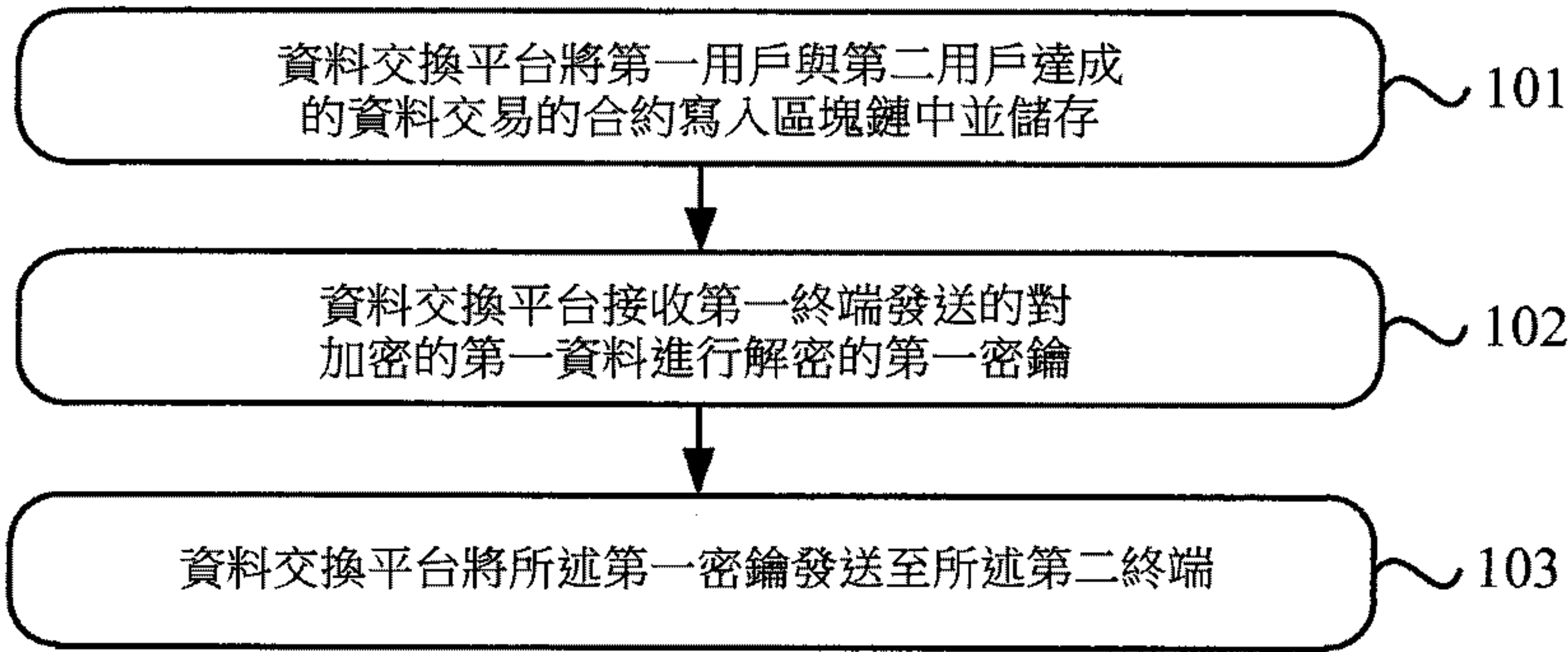


圖 1



I727114

【發明摘要】

【中文發明名稱】

資料發送方法及裝置

【中文】

本案公開了一種資料發送方法，用以解決現有的資料交換過程中資料的安全性較低的問題。該方法包括：資料交易平台將第一用戶與第二用戶達成的資料交易的合約寫入區塊鏈中並儲存；資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；所述第一終端將加密後的第一資料發送至第二終端，所述第二終端為第二用戶對應的終端；資料交換平台將第一密鑰發送至所述第二終端；第二終端根據第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料。本案還公開了一種資料發送裝置。

【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

【發明說明書】

【中文發明名稱】

資料發送方法及裝置

【技術領域】

本案係關於電腦技術領域，尤其關於一種資料發送方法及裝置。

【先前技術】

隨著信息技術的發展，信息技術極大地方便了人們的工作和生活，在信息技術領域中，信息是以資料為載體進行儲存和傳播的，資料可以以二進位制的形式儲存於計算設備的儲存媒體中，這裏所說的資料可以是文字、符號、視頻或音頻等所有能被計算設備識別的元素。

資料作為信息的載體，往往會有一定的價值，尤其在大數據時代，各單位自身在運營、服務過程中往往會積累大量的資料，這些資料對某些業務的開展會有一定的利用價值。為了極大地利用資料的價值，持有資料的雙方可以互相交換資料，各取自身所需的資料。

為了方便交換資料的雙方能夠尋找合適的交換資料的對象，資料交換平台應運而生，資料交換平台可以展示資料持有方發布的資料交換信息，以便能被資料需求方發現。同時，在資料交換過程中，資料交換平台作為中介，會接收資料持有方的資料，然後再將資料發送給資料需求

方。這樣資料交換平台便有可能將雙方交換的資料挪作他用，或在發送給接收方前私自更改資料，損害資料交換雙方的利益，即現有的資料交換過程中，資料的安全性較低。

【發明內容】

本案實施例提供一種資料發送方法，用以解決現有的資料交換過程中資料的安全性較低的問題。

本案實施例採用下述技術方案：

一種資料發送方法，包括：

資料交換平台將第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中並儲存；

資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；

所述第一終端將加密後的第一資料發送至第二終端，所述第二終端為第二用戶對應的終端；

資料交換平台將第一密鑰發送至所述第二終端；

所述第二終端根據第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料。

本案實施例還提供一種資料發送方法，用以解決現有的資料交換過程中資料的安全性較低的問題。

本案實施例採用下述技術方案：

一種資料發送方法，包括：

資料交換平台將第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中並儲存；

資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；

資料交換平台將所述第一密鑰發送至所述第二終端，以便所述第二終端在接收到第一終端發送的第一資料後，根據所述第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料，所述第二終端為第二用戶對應的終端。

本案實施例還提供一種資料發送方法，用以解決現有的資料交換過程中資料的安全性較低的問題。

本案實施例採用下述技術方案：

一種資料發送方法，包括：

資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；

資料交換平台將所述第一密鑰發送至所述第二終端，以便所述第二終端在接收到第一終端發送的第一資料後，根據所述第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料，所述第二終端為第二用戶對應的終端。

本案實施例還提供一種資料發送裝置，用以解決現有的資料交換過程中資料的安全性較低的問題。

本案實施例採用下述技術方案：

一種資料發送裝置，包括：

寫入單元，將第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中並儲存；

第一接收單元，接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；

第一發送單元，將所述第一密鑰發送至所述第二終端，以便所述第二終端在接收到第一終端發送的第一資料後，根據所述第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料，所述第二終端為第二用戶對應的終端。

本案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：

在進行資料交換時，資料交換平台會將交換資料的第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中，然後資料交換平台接收第一用戶對應的第一終端發送的對加密的第一資料進行解密的第一密鑰，第一終端將加密後的第一資料發送至第二用戶對應的第二終端，資料交換平台將第一密鑰發送至第二終端，第二終端根據第一密鑰對接收到的經加密的第一資料進行解密，即可得到第一資料。顯然，在資料交換的過程中，資料交換平台不接觸交換的第一資料，這就避免了第一資料可能被資料交換平台挪作他用的風險，提高了資料交換過程中資料的安全性，

同時資料交換平台。

【圖式簡單說明】

此處所說明的附圖用來提供對本案的進一步理解，構成本案的一部分，本案的示意性實施例及其說明用於解釋本案，並不構成對本案的不當限定。在附圖中：

圖1為本案實施例提供的一種資料發送方法的實現流程示意圖；

圖2為本案實施例提供的一種資料發送方法的實現場景示意圖；

圖3為本案實施例提供的一種資料交易方法的實現流程示意圖；

圖4為本案實施例提供的一種資料發送裝置的具體結構示意圖。

【實施方式】

為使本案的目的、技術方案和優點更加清楚，下面將結合本案具體實施例及相應的附圖對本案技術方案進行清楚、完整地描述。顯然，所描述的實施例僅是本案一部分實施例，而不是全部的實施例。基於本案中的實施例，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，都屬於本案保護的範圍。

如背景技術中所描述的，資料作為信息的載體，往往會有一定的價值，尤其在大數據時代，大數據對政府和企

業各項工作的開展更是具有巨大的價值，從大數據中提取出來的信息，能夠幫助政府和企業做出更好的決策。比如，大型的社交網站往往都積累了大量的用戶資料，這些用戶資料不僅記錄有用戶的個人身份信息，還能從一定程度上反映出用戶的個人愛好、生活習慣以及人脈關係等信息，資料中包含的這些信息對後續業務的開展都有很大的利用價值，其利用價值比如可以是幫助營銷公司向用戶進行精準的廣告推送。

為了極大地利用資料的價值，持有資料的各方可以互相交換資料，以期從交換得來的資料中挖掘出對自身有價值的信息，從而促進自身業務的發展。這樣，為了方便資料需求方尋找對自己有用的資料，資料交換的雙方可以透過資料交換平台來交換資料。

然而，由於資料可以被複製，這就決定了資料的歸屬權不像實物的歸屬權那樣明確，實物在從甲方轉至乙方後，甲方便喪失了對該實物的擁有權，但是資料在從一方轉至另一方時，如果這個過程中資料經過了第三方，那麼第三方便可能會複製資料，從而擁有資料，這就有可能損害資料交換雙方的利益。

資料交換平台不僅可以起到撮合雙方交換資料的作用，還可以起擔保的作用，即在資料交換過程中保障雙方權益的作用。現有的資料交換流程中，為了防止交換資料的一方在發送資料後，另一方不發送自己的資料，資料交換平台會先獲取到資料交換雙方的資料，然後再分別發送

給資料交換的雙方，以防止一方抵賴。這樣，資料交換平台便會有將資料挪作他用的機會，這便會導致資料在交換時的安全性較低。為了解決該問題，本案提供了一種資料發送方法。本案提供的資料發送方法的執行主體可以是資料交換平台，資料交換平台可以是實現本方法的軟體、硬體或者軟體與硬體的結合。

以下結合附圖，詳細說明本案各實施例提供的技術方案。

實施例 1

為解決現有的資料交換過程中資料的安全性較低的問題，本案實施例 1 提供一種資料發送方法。本案實施例中，為便於描述，將資料交換雙方稱為第一用戶和第二用戶，第一用戶和第二用戶可以是任何單位或個人，這裏的第一用戶和第二用戶用於區分資料交易的雙方，而不應理解為對本案例中資料交易雙方的限定。

資料交換雙方在進行資料交換時，會透過終端設備來執行某些操作，為便於描述，將第一用戶執行操作所對應的終端稱為第一終端，將第二用戶執行操作所對應的終端稱為第二終端。需要說明的是，同一用戶在整個資料交換過程中，可以使用同一終端，也可以使用不同的終端，即本案實施例中各過程中所提到的第一終端可以是不同的終端，第二終端也可以是不同的終端。這裏所說的終端比如可以是個人電腦、伺服器、移動終端等電腦設備，本案對

此不做限定。

在進行資料交換時，資料交換雙方在交換資料之前往往會約定一份資料交換合約，這裏所說的資料交換合約是資料交換的雙方在進行資料交換前，就資料交換的細節達成的合約，資料交換合約是資料交換雙方為了確定各自的權利和義務而訂立的共同遵守的條文。

在達成資料交換合約時，第一用戶可以透過第一終端在資料交換平台發布資料信息，那麼資料交換平台在接收到第一終端發布的資料信息後，便可將該資料信息公布，這樣對該資料信息感興趣的第二用戶在看到該資料信息後，便可以透過第二終端向資料交換平台發送對該資料信息的下單請求，資料交換平台接收第二終端對公布的該資料信息的下單請求，並將該請求發送至第一終端，第一終端在確認後，資料交換平台會接收到第一終端發送的對該下單請求的確認信息，以達成資料交換的合約。

上文簡單描述了達成合約的過程，在實際應用中，資料交換雙方可能會透過多次交涉來商定合約的細節，資料交換合約中具體可以包含資料交換雙方的身份信息、交換的資料的特徵信息、雙方應遵守的資料使用規範以及違約時的懲罰措施等信息，這樣，在接收方收到資料後，如果發現資料有與合約描述不相符的地方，接收方可以依據合約採取相應的措施。

合約中雙方交換的資料的特徵信息可以包括下述至少一種，用於驗證資料完整性的消息摘要，概括資料具體內

容的基準信息。那麼，對於第一資料而言，第一資料的特徵信息包括下述至少一種：用於驗證第一資料完整性的消息摘要，概括第一資料具體內容的基準信息。

其中，消息摘要是基於單向散列算法確定出的唯一對應一個消息或文件的固定長度的值，那麼，當待交換的資料被修改時，資料的消息摘要也會發生變化。常用的單向散列算法包括：消息摘要演算法 5(Message Digest Algorithm 5，MD5)、安全哈希演算法(Secure Hash Algorithm，SHA)、消息認證代碼(Message Authentication Code，MAC)等。

基於合同中包含的第一資料的消息摘要，當第二用戶在接收到加密資料後，便可以對加密資料進行完整性校驗，以判斷接收到的資料是否被修改，同時，完整性校驗值也可以成為後期資料交換雙方發生糾紛時的依據。

概括第一資料具體內容的基準信息比如可以是第一資料中應當包含何種類型的資料，或者第一資料中的資料應當滿足某些特定的條件等，或者第一資料中的資料在應用時能達到什麼樣的效果等等。基於該些信息，第二終端便可以對第一資料的具體內容進行校驗，防止被第二用戶欺騙，對自身利益造成損失。

上文描述了發送資料前資料交換雙方達成資料交換合約的過程，那麼下文將詳細介紹本案中資料交換雙方在資料發送資料時的過程，即本案提供的一種資料發送方法，該方法的實現流程示意圖如圖1所示，包括下述步驟：

步驟 101：資料交換平台將第一用戶與第二用戶達成的資料交易的合約寫入區塊鏈中並儲存；

在信息技術時代，合約同樣可以以資料的形式保存在計算設備的儲存媒體中，而在儲存媒體中保存的資料會存在被修改的風險，為了防止資料交換的雙方私自修改合約，提高合約資料的安全性，可以由資料交換平台作為第三方來保存合約。

然而，由資料交換平台來保存合約，便會存在資料交換平台修改合約的風險，如果資料交換平台與交換資料的一方串通修改合約，便會損害另一方面的利益，為了進一步提高合約資料的安全性，提升資料交換平台的公信力，在對合約進行儲存時，可以透過區塊鏈技術將第一用戶和第二用戶達成的資料交換合約進行儲存。

區塊鏈技術是一種去中心化、去信任、防竄改的分布式資料儲存技術。透過區塊鏈技術儲存的資料結構為鏈式資料結構，鏈式資料結構中資料的變更只能透過增量的方式進行，已經記錄的資料將會一直保持最初記錄時的狀態，不會被覆蓋。

同時，區塊鏈在記錄資料時是遵循共識機制的，當某個節點在記錄資料時，其所記錄的資料需要取得區塊鏈中大部分節點的認同，才能被記錄到區塊鏈的各節點中，這就極大程度地避免了儲存的資料為非法資料的可能，也就極大程度地避免了合約被竄改的可能。

區塊鏈技術所採用的共識機制比如可以是工作量證明

機制、權益證明機制、股份授權證明機制或驗證池機制等。如果要更改區塊鏈中已經存在的資料，只能透過偽造側鏈的方式對原有的資料進行替換，竄改成本從技術難度、時間消耗以及人員使用上都是巨大的，這在區塊鏈的共識機制下幾乎是不可能做到的事情。

透過上述分析可以得出，本案實施例透過區塊鏈技術來保存資料交換合約，可以有效地避免合約被竄改的可能，極大地增強了資料交互合約的安全性。

步驟 102：資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰；

這裏所說的第一資料為第一用戶期望發送給第二用戶的資料，那麼，這裏的第一用戶便是第一資料的發送方，第二用戶即為第一資料的接收方。當然，在電腦領域，本領域技術人員應當清楚，所謂的用戶之間發送資料，在實際操作中可以是用戶透過終端向其他用戶的終端發送資料。

為了防止資料被非交換雙方的第三方竊取，可以對第一資料進行加密，然後再發送至第二終端，在密碼學中，加密是將明文信息隱匿起來，使之在缺少解密密鑰時不可讀，增強了資料傳輸時的安全性。

資料在加密後再經過資料交互平台進行傳輸，仍然不能完全保證加密的第一資料不被資料交換平台利用，比如資料交換平台有可能會對資料進行破解。那麼，可以由第一終端將加密後的第一資料直接發送至第二終端，而資料

交換平台不接觸交換的資料，這樣，便進一步增強了資料傳輸時的安全性。

第一終端在對資料進行加密時可以透過多種加密方法對資料進行加密，比如，可以使用對稱加密算法對第一資料進行加密，那麼，這裏的第一密鑰便是加密第一資料時使用的密鑰，這樣資料交換平台在確定解密加密的第一資料的密鑰時，是透過接收第一終端發送的對第一資料進行加密時的密鑰來確定的。或者第一終端還可以使用非對稱加密算法對第一資料進行加密，透過資料交換平台發送的公鑰來加密，這樣資料交換平台只要確定能解密加密資料的私鑰即可。

而為了約束資料交換雙方，第一密鑰最好不要由第一終端直接發送給第二終端，而由資料交換平台選擇合適的時機來發送。即，在第一終端透過對稱加密算法對第一資料進行加密後，可以將加密時所使用的第一密鑰發送給資料交換平台，資料交換平台接收到第一終端發送的該密鑰後，便可以透過執行步驟103來將密鑰發送給第二終端。

步驟103：資料交換平台將所述第一密鑰發送至所述第二終端。

以便所述第二終端在接收到第一終端發送的第一資料後，根據所述第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料，所述第二終端為第二用戶對應的終端。

同樣，第二終端在向第一終端發送資料時，也可以先

透過密鑰對資料進行加密，這裏將第二用戶持有的待交換的資料稱為第二資料，第二終端將第二資料進行加密後，將加密後的第二資料發送給第一終端，然後將解密該加密資料的第二密鑰發送給資料交換平台，由平台再將該密鑰發送給第一終端，這樣第一終端便可以透過密鑰對加密的第二資料進行解密，得到第二資料，至此便實現了雙方資料的交換，該過程中，雙方交換的資料均沒有經過資料交換平台，增強了交換的資料的安全性。

需要說明的是，本案實施例中為便於描述，將第一用戶持有的資料稱為第一資料，第二用戶持有的資料為第二資料，雙方進行資料交互的過程為彼此交換第一資料和第二資料的過程。可以理解的是，本案實施例中所使用的第一和第二，是為了區分不同的描述對象，並不是指特定的某一對象。

為了進一步提高資料的安全性，防止資料交換雙方一方的利益受損，在接收到雙方發送的加密資料的密鑰後，還可以在接收到雙方發送的對資料的確認信息後，再將密鑰發送給雙方，以防止一方收到資料後不發送密鑰的情況，這會極大地損害另一方的利益。比如，資料交換平台將第一密鑰發送至第二終端之後，在收到第二終端發送的對第一資料的確認信息後，再將第二密鑰發送給第一終端，對第一資料的確認信息表示第二用戶確定第一資料與合約中的描述相符，這樣便有效地保護了第二用戶的利益。同樣資料交換平台接收第二用戶發送的對第一資料的

確認信息之後，還可以接收第一終端發送的對第二資料的確認信息，所述對第二資料的確認信息表示第一用戶確定所述第二資料與所述合約中的描述相符。

對於某些類型的資料，是可以經過平台進行交換的，該些資料比如可以是用戶不在乎是否被第三方獲取的資料，或者無法透過複製獲取資料價值的資料，對於該些類型的資料，則沒有必要再對其加密，以便節省計算資源和儲存資源，為便於描述，將可經過平台進行交互的資料稱為第三資料。

下面以第二用戶待交換的資料是可以經過資料交換平台進行交換的第三資料，以對待交換的第一資料的加密技術為對稱加密技術為例，詳細說明本案提供的一種資料交換方法，該方法包括如下步驟：

步驟 201：資料交換平台將第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中並儲存；

步驟 202：資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰；

步驟 203：第一終端將加密後的第一資料發送至第二終端；

步驟 204：第二終端將第三資料發送給資料交換平台；

需要說明的是，本案並不對步驟 202、步驟 203 和步驟 204 的執行順序做限定。

步驟 205：資料交換平台將接收到的第一密鑰發送至

第二終端；

由於第二用戶是直接將第三資料發送給資料交換平台的，那麼資料交換平台便可以對第三資料進行驗證，如果發現第三資料與雙方之前約定的不符，那麼便可以不再向第二終端發送第一密鑰，避免第一用戶的利益受損，那麼本步驟的具體執行過程可以是在確定第三資料與雙方約定相符時，將接收到的第一密鑰發送至第二終端。

步驟 206：第二終端根據接收到的第一密鑰對接收到的經加密的第一資料進行解密，即可得到第一資料；

步驟 207：資料交換平台將第三資料發送給第一終端。

對於第二用戶獲得的第一資料而言，由於平台不接觸第一資料，那麼平台也就無法對其真實性進行校驗，那麼可以由第二終端來對第一資料進行校驗，在進行校驗時，第二終端會獲取交易合約中雙方約定的第一資料的特徵信息，具體獲取時可以是從區塊鏈中保存的合約中獲取特徵信息，當然，雙方在商定合約時，第二終端本地往往也會存有合約，那麼第二終端也可以從第二終端所儲存的合約中獲取特徵信息。第二終端在獲取到合約中第一資料的特徵信息後，便可根據獲取的特徵信息，校驗獲取的第一資料是否與合約中的記錄相符。

這樣，如果第二用戶發現第一資料與當初約定不符，則平台就不能將第三資料發送給第一終端了，以避免第二用戶的利益受損。

那麼，可以在接收到所述第二終端發送的資料發送指令時，再將第三資料發送給第一終端，這裏的資料發送指令為指示資料交換平台將第三資料發送給第一用戶的指令，比如可以是上文所述的對第一資料的確認信息，這樣即表明在第二用戶確定第一資料與合約中的描述相符時，才將第三資料發送給第一終端。

然而，如果用戶不向平台發送資料發送指令，那麼第一用戶便一直無法收到第三資料，為了避免第一用戶的利益受損，在某些情況下，也可以將第三資料發送給第一用戶，比如，在向第二用戶發送第一密鑰預設時長後，如果第一用戶還未發送對第一資料的確認信息，此時便可以將第三資料發送給第一用戶。

綜上所述，步驟207的具體執行過程可以是在確定預設的條件成立時，將第三資料發送給第一用戶。這裏的預設的條件成立時，比如可以是接收到所述第二終端發送的資料發送指令後，也可以是向第二終端發送密鑰預設時長後。

至此，便實現了用戶間第一資料和第三資料的交換，透過該方法，可以防止某一方獲取了對方發送的資料後不給另一方發送資料的情況，保護了資料交換雙方的利益。

在資料交換完成後，資料交換平台還可以將達成交換的記錄寫入區塊鏈中資料交換合約結果中並儲存，以便於後續利用。

本案實施例中，還可以確定加密資料的傳輸狀態，以

防止第二用戶接收到了加密資料後卻聲稱未接收到加密資料，同時也可以防止第一終端沒有向第二終端發送資料，而第一用戶卻聲稱已經將資料發送給了第二終端，這裏的加密資料為加密後的交互的資料，比如上文所述的經加密的第一資料、經加密的第二資料。傳輸狀態包括下述至少一種：加密資料還未傳輸、加密資料正在傳輸以及加密資料已經傳輸至第二終端。

確定加密資料的傳輸狀態的具體方式，可以是資料交互平台透過預定的監控程序來獲取加密資料的傳輸狀態，該監控程序可以是資料交換雙方傳輸資料的程序。或者確定加密資料的傳輸狀態的具體方式，還可以是接收第一終端和第二終端主動上報的加密資料的傳輸狀態。

由於第一終端發送加密資料時是不經過資料交換平台的，如果第一終端需要和多個不同的終端進行資料交換的話，由於不同終端支持的資料傳輸方式可能不同，這樣，第一終端便需要為不同的終端開發不同的資料傳輸介面，這不僅會耗費較多的人力資源，還會占用過多的儲存資源。那麼，資料傳輸平台可以擬定資料傳輸時的規範，定義資料傳輸時的標準傳輸介面，該標準傳輸介面是各終端之間傳輸資料時通用的介面。

透過該資料傳輸平台進行資料交換的用戶的終端只要實現了該標準傳輸介面，便可以向任何實現了該標準介面的終端傳輸資料。資料傳輸平台定義的標準傳輸介面中，比如可以定義有交換資料的雙方在進行資料傳輸時的資料

傳輸協議等信息，此處不再贅述。

定義的該標準介面的功能還可以包含發送資料傳輸狀態至資料交換平台的功能，這樣，當加密資料發送完畢後，資料交互平台便可以確定加密資料已經成功發送至第二終端，然後再進行相應的操作。

基於本案實施例，圖2示出了一種資料發送方法的實現場景示意圖，在雙方達成資料交換合約後，第一終端將第一資料傳輸給第二終端的具體過程如下：

步驟301：第一終端將第一資料加密，得到加密資料；

步驟302：第一終端透過實現的標準傳輸介面將加密資料發送至第二終端；

當然，第二終端也實現了該標準傳輸介面。

步驟303：第一終端將密鑰發送給資料交換平台；

步驟304：資料交換平台將收到的密鑰發送給第二終端；

步驟305：第二終端根據收到的該密鑰對加密資料進行解密，便可得到第一資料。

本案實施例1提供的資料發送方法，在進行資料交換時，資料交換平台會將交換資料的第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中，然後資料交換平台接收第一用戶對應的第一終端發送的對加密的第一資料進行解密的第一密鑰，第一終端將加密後的第一資料發送至第二用戶對應的第二終端，資料交換平台將第一密鑰發送至

第二終端，第二終端根據第一密鑰對接收到的經加密的第一資料進行解密，即可得到第一資料。顯然，在資料交換的過程中，資料交換平台不接觸交換的第一資料，這就避免了第一資料可能被資料交換平台挪作他用的風險，提高了資料交換過程中資料的安全性，同時資料交換平台。

需要說明的是，為便於描述，本案以資料方法的執行主體為資料交換平台為例，對資料發送方法的實施方式進行了介紹。可以理解，該方法的執行主體為資料交換平台只是一種示例性的說明，並不應理解為對該方法的限定。其次，實施例1所提供方法的各步驟的執行主體均可以是同一設備，或者，該方法也由不同設備作為執行主體。比如，步驟101和步驟102的執行主體可以為設備1；又比如，步驟101的執行主體可以為設備1，步驟102的執行主體可以為設備2；等等。

實施例2

基於前述實施例1詳細敘述了本案的發明構思，為了便於更好的理解本案的技術特徵、手段和效果，下面對本案的資料發送方法做進一步說明，從而形成了本案的又一個實施例。

本案實施例2中資料交換的過程與實施例1中所述資料交換的過程相似，實施例2中沒有介紹到的其他一些步驟可以參見實施例1中的相關描述，此處不再贅述。

在對該方案的實現方式進行詳細介紹前，先對該方案

的實施場景進行簡單介紹。

在互聯網中，資金也是以資料的形式存在的，那麼，表示資金的資料的價值可以是其所代表的資金的價值，在互聯網中，對表示資金的資料的轉移，在實際操作中往往是透過更改標識資金的數值來實現的。比如從賬戶A中向賬戶B轉帳100元，實際上資料的轉移是將賬戶A和賬戶B中表示資金的數值進行相應的更改。

如實施例1中所描述的，某些類型的資料是無法透過複製而獲取資料價值的，該些資料可以透過平台來傳輸，那麼實施例2以第三資料為表示資金的資料為例，詳細介紹本案提供的資料發送方法的具體實施過程，為便於描述，後續將用於表示資金的第三資料簡稱為資金，那麼資料交換過程可以理解為資料交易的過程，實施例1中的第一用戶即為資料出售方，第二用戶即為資料購買方，資料交換平台即為資料交易平台，可以為用戶提供資料交易服務。

基於上述場景，實施例2中實現資料交易的過程如圖3所示，包括下述步驟：

步驟401：資料出售方透過資料交易平台發布出售的資料的信息；

資料交易平台可以支持有資料出售需求的用戶發布出售資料的信息，這樣有資料消費需求的用戶便可以在資料交易平台尋找自己需要的信息。

步驟402：資料消費方與資料出售方達成資料交易合

約；

資料消費方可以就具體的交易細節進行溝通，然後最終達成資料交易合約，資料交易合約的作用與實施例1中所描述的資料交換合約的作用類似，此處不再贅述。

步驟403：資料交易平台將雙方達成的資料交易合約寫入區塊鏈中；

透過將資料交易合約寫入區塊鏈中，可以極大程度上避免合約被竄改的可能，增強了合約的安全性。

步驟404：資料消費方向平台支付合約中約定的金額；

在互聯網中，對資金的轉移實際上是對表示資金的資料的轉移，在實際操作中往往是透過更改賬戶中標識資金的資料的數值來實現的。

步驟405：資料出售方對出售的資料進行加密，得到加密資料，然後將加密時的密鑰發送給資料交易平台；

在對資料進行加密時，可以採用對稱加密技術，這樣加密的密鑰和解密的密鑰是相同的。

需要說明的是，本案實施例中不對步驟404和步驟405執行時的先後順序做限定。

步驟406：資料出售方透過實現了標準傳輸介面的終端將加密資料傳輸至資料消費方的終端；

如實施例1中所描述的，這裏的標準傳輸介面是由資料交換平台定義的、終端之間傳輸資料時通用的介面。資料消費方終端也應該實現了該標準傳輸介面，以便接收資

料。這樣，當資料消費方和資料出售方再與平台的其它用戶進行資料交換時，便可以不必再開發其他的傳輸介面，節省了人力資源和儲存資源。

步驟 407：資料交易平台確定加密資料已經傳輸至資料消費方終端；

具體確定加密資料已經傳輸至資料消費方終端的方法與實施例 1 中的相關描述類似，此處不再贅述。

步驟 408：資料交易平台確定資料消費方支付的金額與合同中記錄的相符後，將密鑰發送給資料消費方；

需要說明的是，本案實施例中不對步驟 407 和步驟 408 執行時的先後順序做限定。

步驟 409：資料消費方利用接收到的密鑰對加密資料進行解密，並驗證解密後的資料是否與合同中描述的相符；

步驟 410：資料消費方在確定接收到的資料與合同中描述的相符之後，透過終端向資料交易平台發送確認收貨指令；

這裏的確認收貨指令的作用與實施例 1 中描述的第二資料發送指令類似，此處不再贅述。

步驟 411：資料交易平台接收到確認收貨指令後，將資料消費方支付的金額轉移至資料發售方的賬戶中。

如果後續雙方因為交易的資料產生糾紛，可以依據區塊鏈中的合約來維護自身的權利。

本案實施例 2 提供的資料交易方法，資料交易平台接

收消費方發送的對出售的資料進行加密時的密鑰，然後在接收到資料消費方透過終端支付的資金後，將該密鑰發送至資料消費方的終端，這樣資料消費方在接收到資料出售方發送的加密資料後，便可以利用該密鑰解密加密資料得到資料出售方出售的資料。這樣，在資料交易的過程中，資料交換平台不接觸出售的資料，避免了出售的資料可能被資料交換平台挪作他用的風險，提高了資料交易過程中資料的安全性。

實施例3

為解決現有的資料交換過程中資料的安全性較低的問題，本案實施例1提供一種資料發送裝置。該資料發送裝置的結構示意圖如圖4所示，主要包括下述功能單元：

寫入單元501，將第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中並儲存；

第一接收單元502，接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；

第一發送單元503，將所述第一密鑰發送至所述第二終端，以便所述第二終端在接收到第一終端發送的第一資料後，根據所述第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料，所述第二終端為第二用戶對應的終端。

本案實施例中，對資料進行交換的具體實施方式還有

很多，在一種實施方式中，所述裝置還包括第三接收單元504，在第一發送單元503將第一密鑰發送至所述第二終端之前，接收第二終端發送的對加密的第二資料進行解密的第二密鑰；

第三發送單元505，在第一發送單元503將第一密鑰發送至所述第二終端之後，將所述第二密鑰發送給第一終端，以便所述第一終端接收第二終端發送的經加密的第二資料後，根據所述第二密鑰對接收到的經加密的第二資料進行解密，得到第二資料。

為了保障第二用戶的利益，在一種實施方式中，所述裝置還包括第四接收單元506，在第一發送單元503將第一密鑰發送至所述第二終端之後，第三發送單元505將所述第二密鑰發送給所述第一終端之前，接收第二終端發送的對第一資料的確認信息，所述對第一資料的確認信息表示第二用戶確定所述第一資料與所述合約中的描述相符。

在一種實施方式中，所述裝置還包括第五接收單元507，在第四接收單元506接收第二終端發送的對第一資料的確認信息之後，接收第一終端發送的對第二資料的確認信息，所述對第二資料的確認信息表示第一用戶確定所述第二資料與所述合約中的描述相符。

在一種實施方式中，所述裝置還包括寫入單元508，在第五接收單元507接收第一終端發送的對第二資料的確認信息之後，將達成交換的記錄寫入區塊鏈中所述資料交換合約結果中並儲存。

為了保障資料交換雙方的利益，在一種實施方式中，所述裝置還包括第二接收單元509，在第一發送單元503將所述第一密鑰發送至第二終端之前，接收所述第二終端發送的第三資料；第二發送單元510，在第一發送單元503將所述第一密鑰發送至所述第二終端之後，在確定預設的條件成立時，將所述第三資料發送給所述第一用戶。

在一種實施方式中，所述確定預設的條件成立，具體包括：所述資料交換平台接收到所述第二終端發送的資料發送指令，所述資料發送指令為指示所述資料交換平台將所述第三資料發送給所述第一終端的指令。

在一種實施方式中，所述資料交換合約中包含所述第一資料的特徵信息；

所述第一資料的特徵信息包括下述至少一種：用於驗證所述第一資料完整性的消息摘要；概括所述第一資料具體內容的基準信息。

為了避免介面開發時耗費較多的人力資源，在一種實施方式中，所述經加密的第一資料是透過實現了標準傳輸介面的第一終端傳輸至所述第二終端的，所述標準傳輸介面是所述資料交換平台定義的、終端之間傳輸資料時通用的介面。

本案實施例3提供的資料發送裝置，在進行資料交換時，資料交換平台會將交換資料的第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中，然後資料交換平台接收第一用戶對應的第一終端發送的對加密的第一資料進行

解密的第一密鑰，第一終端將加密後的第一資料發送至第二用戶對應的第二終端，資料交換平台將第一密鑰發送至第二終端，第二終端根據第一密鑰對接收到的經加密的第一資料進行解密，即可得到第一資料。顯然，在資料交換的過程中，資料交換平台不接觸交換的第一資料，這就避免了第一資料可能被資料交換平台挪作他用的風險，提高了資料交換過程中資料的安全性，同時資料交換平台。

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。設計人員幾乎都透過將改進的方法流程編程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塊來實現。例如，可編程邏輯器件（Programmable Logic Device, PLD）（例如現場可編程閘陣列（Field Programmable Gate Array, FPGA））就是這樣一種積體電路，其邏輯功能由用戶對器件編程來確定。由設計人員自行編程來把一個數位系統“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，這種編程也多半改用“邏輯編譯器（logic compiler）”軟體來實現，它與程序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

編程語言來撰寫，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編程並編程到積體電路中，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代碼（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）、可編程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，儲存器控制器還可以被實現為儲存器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代碼方式實現控制器以外，完全可以透過將方法步驟進行邏輯編程來使得控

制器以邏輯閘、開關、專用積體電路、可編程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塊又可以是硬體部件內的結構。

上述實施例闡明的系統、裝置、模塊或單元，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、行動電話、相機電話、智能電話、個人數位助理、媒體播放器、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。

為了描述的方便，描述以上裝置時以功能分為各種單元分別描述。當然，在實施本案時可以把各單元的功能在同一個或多個軟體和/或硬體中實現。

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、系統或電腦程序產品。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代碼的電腦可用儲存媒體（包括但不限於磁碟儲存器、**CD-ROM**、光學儲存器等）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)、和電腦程序產品的流程圖和／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編程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編程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編程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／或塊框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編程資料處理設備上，使得在電腦或其他可編程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編程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、網絡介面和記憶體。

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、程式的模塊或其他資料。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)、電可擦除可編程唯讀記憶體 (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) 或其他光學記憶體、磁盒式磁帶，磁帶磁碟記憶體或其他磁性儲存設備或任何其他非傳輸媒體，可用於儲存可以被電腦設備接達的信息。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 (transitory media)，如調制的資料信號和載波。

還需要說明的是，術語“包括”、“包含”或者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。

本案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例程、程式、對象、組件、資料結構等等。也可以在分布式計算環境中實踐本案，在這些分布式計算環境中，由透過通信網絡而被連接的遠程處理設備來執行任務。在分布式計算環境中，程式模組可以位於包括儲存設備在內的本地和遠程電腦儲存媒體中。

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。

以上所述僅為本案的實施例而已，並不用於限制本案。對於本領域技術人員來說，本案可以有各種更改和變化。凡在本案的精神和原理之內所作的任何修改、等同替換、改進等，均應包含在本案的權利要求範圍之內。

【符號說明】

501：寫入單元

502：第一接收單元

503：第一發送單元

【發明申請專利範圍】

【請求項1】

一種資料發送方法，包括：

資料交換平台將第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中並儲存；

資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；

所述第一終端將加密後的第一資料直接發送至第二終端，所述第二終端為第二用戶對應的終端；

所述資料交換平台接收第二終端發送的對加密的第二資料進行解密的第二密鑰；

資料交換平台將第一密鑰發送至所述第二終端；

所述資料交換平台將所述第二密鑰發送給第一終端；

所述第二終端根據第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料，

其中，所述資料交換平台將第一密鑰發送至所述第二終端之後，將所述第二密鑰發送給所述第一終端之前，還包括：

所述資料交換平台接收第二終端發送的對第一資料的確認信息，所述對第一資料的確認信息表示所述第二終端在校驗獲取的所述第一資料之後，確定所述第一資料與所述合約中的描述相符。

【請求項2】

如請求項1所述的方法，其中，所述資料交換平台將第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中並儲存之前，還包括：

所述資料交換平台接收第一終端發布的資料信息並公布；

所述資料交換平台接收第二終端對公布的所述資料信息的下單請求，並將所述請求發送至第一終端；

所述資料交換平台接收第一終端發送的對所述下單請求的確認信息，以達成資料交換的合約。

【請求項3】

一種資料發送方法，包括：

資料交換平台將第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中並儲存；

資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；

所述資料交換平台接收第二終端發送的對加密的第二資料進行解密的第二密鑰；

資料交換平台將所述第一密鑰發送至所述第二終端，以便所述第二終端在接收到第一終端所直接發送的第一資料後，根據所述第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料，所述第二終端為第二用戶對應的終端，

所述資料交換平台將所述第二密鑰發送給第一終端；

其中，所述資料交換平台將第一密鑰發送至所述第二終端之後，將所述第二密鑰發送給所述第一終端之前，還包括：

所述資料交換平台接收第二終端發送的對第一資料的確認信息，所述對第一資料的確認信息表示所述第二終端在校驗獲取的所述第一資料之後，確定所述第一資料與所述合約中的描述相符。

【請求項4】

如請求項3所述的方法，其中，

所述資料交換平台將所述第二密鑰發送給第一終端以便所述第一終端接收第二終端發送的經加密的第二資料後，根據所述第二密鑰對接收到的經加密的第二資料進行解密，得到第二資料。

【請求項5】

如請求項3所述的方法，其中，所述資料交換平台接收第二終端發送的對第一資料的確認信息之後，所述方法還包括：

所述資料交換平台接收第一終端發送的對第二資料的確認信息，所述對第二資料的確認信息表示第一用戶確定所述第二資料與所述合約中的描述相符。

【請求項6】

如請求項5所述的方法，其中，所述資料交換平台接收第一終端發送的對第二資料的確認信息之後，還包括：

所述資料交換平台將達成交換的記錄寫入區塊鏈中所

述資料交換合約結果中並儲存。

【請求項7】

如請求項3所述方法，其中，所述資料交換平台將所述第一密鑰發送至第二終端之前，所述方法還包括：

所述資料交換平台接收所述第二終端發送的第三資料；

所述資料交換平台將所述第一密鑰發送至所述第二終端之後，所述方法還包括：

所述資料交換平台在確定預設的條件成立時，將所述第三資料發送給所述第一用戶。

【請求項8】

如請求項6所述方法，其中，所述確定預設的條件成立，具體包括：

所述資料交換平台接收到所述第二終端發送的資料發送指令，所述資料發送指令為指示所述資料交換平台將所述第三資料發送給所述第一終端的指令。

【請求項9】

如請求項3至請求項8中任一項所述方法，其中：

所述資料交換合約中包含所述第一資料的特徵信息；

所述第二終端校驗獲取的所述第一資料還包括：

第二終端獲取所述特徵信息，根據所述特徵信息，校驗獲取的所述第一資料是否與所述合約中的記錄相符；

所述第一資料的特徵信息包括下述至少一種：

用於驗證所述第一資料完整性的消息摘要；

概括所述第一資料具體內容的基準信息。

【請求項10】

如請求項3至請求項8中任一項所述方法，其中，所述經加密的第一資料是透過實現了標準傳輸介面的第一終端傳輸至所述第二終端的，所述標準傳輸介面是所述資料交換平台定義的、終端之間傳輸資料時通用的介面。

【請求項11】

一種資料發送方法，包括：

資料交換平台接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；

所述資料交換平台接收第二終端發送的對加密的第二資料進行解密的第二密鑰；

資料交換平台將所述第一密鑰發送至所述第二終端，以便所述第二終端在接收到第一終端所直接發送的第一資料後，根據所述第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料，所述第二終端為第二用戶對應的終端，

所述資料交換平台將所述第二密鑰發送給第一終端；

其中，所述資料交換平台將第一密鑰發送至所述第二終端之後，將所述第二密鑰發送給所述第一終端之前，還包括：

所述資料交換平台接收第二終端發送的對第一資料的確認信息，所述對第一資料的確認信息表示所述第二終端

在校驗獲取的所述第一資料之後，確定所述第一資料與所述合約中的描述相符。

【請求項 12】

一種資料發送裝置，包括：

寫入單元，將第一用戶與第二用戶達成的資料交換的合約寫入區塊鏈中並儲存；

第一接收單元，接收第一終端發送的對加密的第一資料進行解密的第一密鑰，所述第一終端為第一用戶對應的終端；

第一發送單元，將所述第一密鑰發送至所述第二終端，以便所述第二終端在接收到第一終端所直接發送的第一資料後，根據所述第一密鑰對接收到的經加密的第一資料進行解密，得到第一資料，所述第二終端為第二用戶對應的終端，

其中，所述裝置還包括：

第二接收單元，在所述第一發送單元將所述第一密鑰發送至第二終端之前，接收所述第二終端發送的第三資料；

第二發送單元，在所述第一發送單元將所述第一密鑰發送至第二終端之後，在確定預設的條件成立時，將所述第三資料發送給所述第一用戶，

其中，所述確定預設的條件為所述資料交換平台接收第二終端發送的對第一資料的確認信息，所述對第一資料的確認信息表示所述第二終端在校驗獲取的所述第一資料之後，確定所述第一資料與所述合約中的描述相符。

【發明圖式】

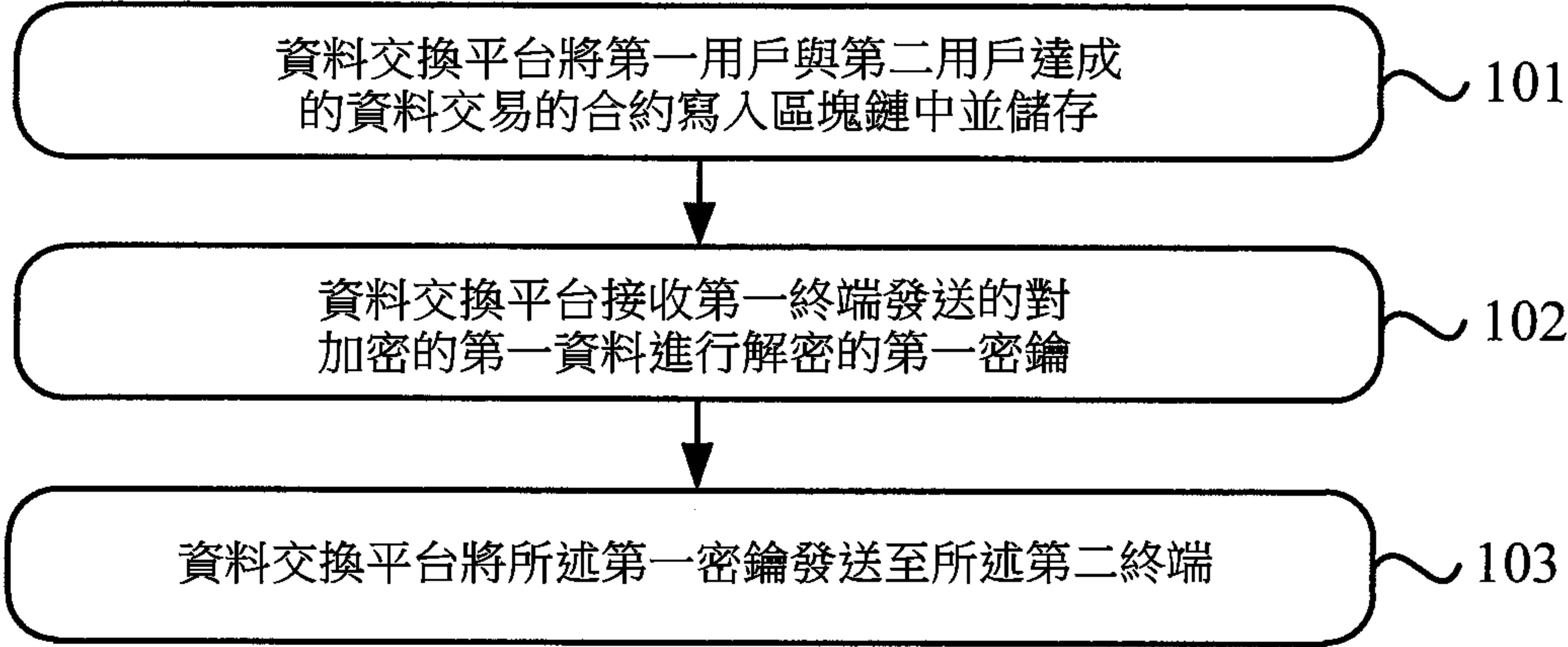


圖 1

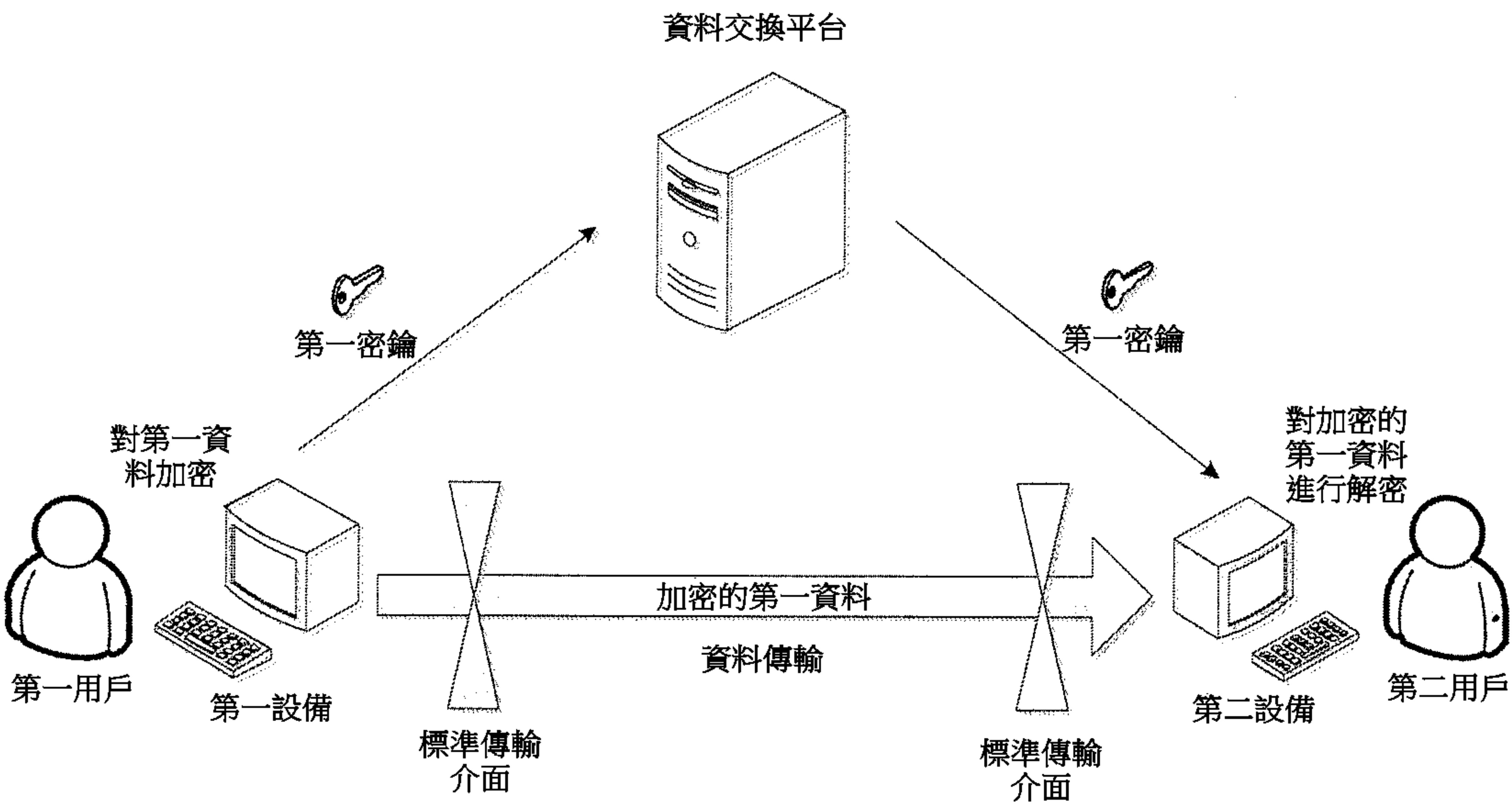


圖 2

