I733057

(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 I733057 B**

(45)公告日： 中華民國 110 (2021) 年 07 月 11 日

(21)申請案號：107132969　(22)申請日： 中華民國 107 (2018) 年 09 月 19 日

(51)Int. Cl.：　*G06Q40/04　(2012.01)*　*G06Q20/38　(2012.01)*

(30)優先權：2017/11/23　中國大陸　201711183322.4

(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：王虎森 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW　M543413U　WO　2017145008A1

WO　2017178956A1

審查人員：林育弘

申請專利範圍項數：28 項　圖式數：11　共 75 頁

(54)名稱

資源轉移和資金轉移的方法和裝置

(57)摘要

本案公開了一種基於區塊鏈的資源轉移方法，包括：當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；根據第一資源的第一數額，確定待轉移的第二資源的第二數額，第一資源與第二資源的類型不同；資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源，其中，交易請求中包括對第二資源的第二數額進行加密處理後得到的第一加密數額信息；在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入區塊鏈。從而能夠在資源轉移過程中能夠保護資源轉移雙方的隱私信息。

指定代表圖：

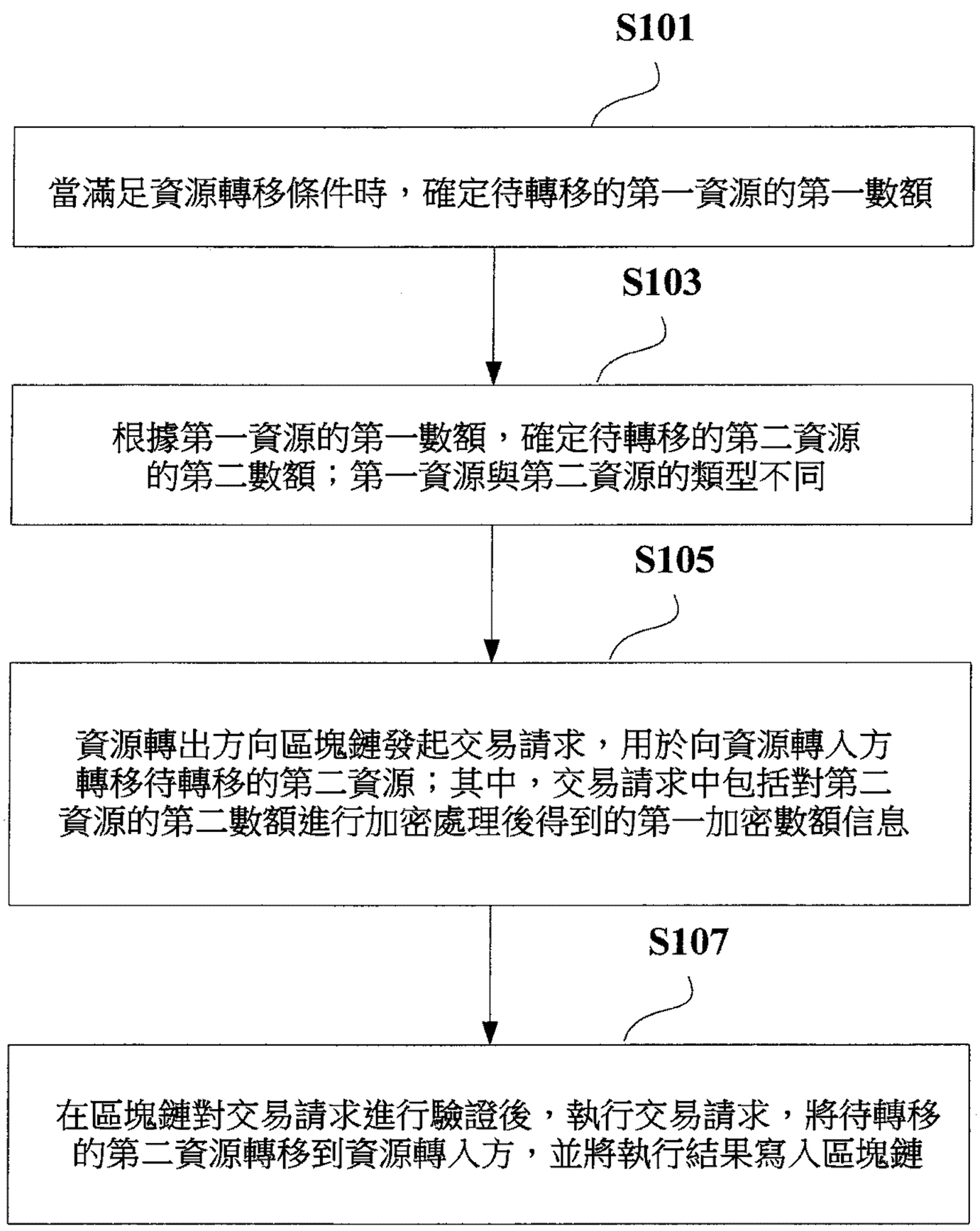
S101
當滿足資源轉移條件時，確定待轉移的第一資源的第一數額
S103
根據第一資源的第一數額，確定待轉移的第二資源的第二數額；第一資源與第二資源的類型不同
S105
資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源；其中，交易請求中包括對第二資源的第二數額進行加密處理後得到的第一加密數額信息
S107
在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入區塊鏈

圖 1

公告本

I733057

【發明摘要】

【中文發明名稱】

資源轉移和資金轉移的方法和裝置

【中文】

本案公開了一種基於區塊鏈的資源轉移方法，包括：當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；根據第一資源的第一數額，確定待轉移的第二資源的第二數額，第一資源與第二資源的類型不同；資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源，其中，交易請求中包括對第二資源的第二數額進行加密處理後得到的第一加密數額信息；在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入區塊鏈。從而能夠在資源轉移過程中能夠保護資源轉移雙方的隱私信息。

【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】

資源轉移和資金轉移的方法和裝置

【技術領域】

本案涉及電腦技術領域，尤其涉及一種資源轉移和資金轉移的方法和系統。

【先前技術】

區塊鏈技術(又稱分散式帳本技術)是一種特殊的分散式資料庫技術，適合儲存簡單的、有先後關係的、能在系統內驗證的資料，利用密碼學和共識演算法保證了資料的不可篡改和不可偽造。隨著電腦和網際網路技術的發展，區塊鏈技術以其去中心化、公開透明、不可篡改、可信任等優點，備受青睞，在智能合約、證券交易、電子商務、物聯網、社交通訊、文件儲存、存在性證明、身份驗證、股權眾籌等眾多領域得到廣泛應用。

當將區塊鏈技術應用於資源轉移這類交易場景時，由於所有交易信息均需要發送到區塊鏈系統進行驗證、實施和上鏈，參與交易的資源轉移雙方的隱私信息，例如具體交易信息，所擁有資源的總額，個體隱私信息等都將面臨洩漏給與本次交易無關的第三方的風險。以將區塊鏈技術應用於網際網路銀行的借貸業務中為例，借款方向出借方貸款的具體數額等交易信息均需要入鏈，從而對借貸雙方

的隱私信息構成威脅。

因此，亟需一種在資源轉移過程中能夠保護資源轉移雙方隱私信息的方案。

【發明內容】

本案實施例提供一種資源轉移方法、裝置及對應的電子設備和電腦可讀儲存媒體，目的在於在資源轉移過程中能夠保護資源轉移雙方的隱私信息。

本案實施例還提供一種資金轉移方法、裝置及對應的電子設備和電腦可讀儲存媒體，目的在於在資金轉移的過程中能夠保護資金借貸雙方的隱私信息。

本案實施例採用下述技術方案：

第一方面，本案實施例提供一種基於區塊鏈的資源轉移方法，包括：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括對所述第二資源的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述

交易請求，將所述待轉移的第二資源轉移到所述資源轉入方，並將執行結果寫入所述區塊鏈。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述交易請求中包括的所述第一加密數額信息，透過採用第一加密函數對所述第二資源的第二數額進行加密處理得到；

其中，所述第一加密函數的一個輸入為所述第二資源的第二數額，另一個輸入為所述資源轉入方的公鑰。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述交易請求中還包括所述資源轉入方的公鑰的標識信息。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述資源轉入方的公鑰的標識信息為所述資源轉入方的公鑰的雜湊值。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額，包括：

根據所述第一資源的第一數額，採用單向函數確定所述第二資源的第二數額。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，採用單向函數確定所述第二資源的第二數額，包括：

將所述第一資源的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述第二資源

的第二數額。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述資源轉出方向區塊鏈發起的所述交易請求中，還包括加密後的所述隨機數。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述資源轉移條件包括允許所述資源轉入方借取所述第一資源；則確定待轉移的第一資源的第一數額，包括：

將允許所述資源轉入方借取的第一資源的額度，作為所述待轉移的第一資源的第一數額。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述資源轉移條件包括所述資源轉出方已接收到所述資源轉入方歸還的第一資源；則確定待轉移的第一資源的第一數額，包括：

將所述歸還的第一資源的數額，確定為所述待轉移的第一資源的第一數額。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述資源轉移條件包括所述資源轉入方與所述資源轉出方已達成資源借取協議，所述資源借取協議中包含所述資源轉出方向所述資源轉入方申請借取的第一資源的數額；則確定待轉移的第一資源的第一數額，包括：

將所述申請借取的第一資源的數額，確定為所述待轉移的第一資源的第一數額。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方

法中，所述交易請求中還包括零知識證明，用於證明執行所述交易請求之後所述資源轉出方將要持有的第二資源的餘額與所述第二數額的和，等於所述資源轉出方在發起所述交易請求前所持有的第二資源的數額。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述零知識證明還用於證明所述第二數額大於零，所述資源轉出方在發起所述交易請求前所持有的第二資源的數額大於零，並且，執行所述交易請求之後所述資源轉出方將要持有的第二資源的餘額不小於零。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述交易請求中還包括所述資源轉出方參與的上一次資源轉移交易的標識信息。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述資源轉出方參與的上一次資源轉移交易的標識信息，具體為所述區塊鏈中記錄的、所述上一次資源轉移交易的雜湊值。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述交易請求中還包括對執行所述交易請求之後所述資源轉出方將要持有的第二資源的餘額進行加密處理後得到的第二加密數額信息。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述交易請求中包括的所述第二加密數額信息，透過採用第二加密函數對執行所述交易請求之後所述資源轉出方將要持有的第二資源的餘額進行加密處理得到；

其中，所述第二加密函數的一個輸入為所述第二資源的餘額，另一個輸入為所述資源轉出方的公鑰。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述交易請求中還包括所述資源轉出方的公鑰的標識信息。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述資源轉出方的公鑰的標識信息為所述資源轉出方的公鑰的雜湊值。

較佳地，在第一方面提供的基於區塊鏈的資源轉移方法中，所述第一資源具體為資金，所述第二資源具體為代幣。

第二方面，本案實施例還提供了一種基於區塊鏈的資金轉移方法，包括：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據所述資金的第一數額，確定待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括對所述代幣的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈。

第三方面，本案實施例提供了一種基於區塊鏈的資源轉移裝置，包括：

第一數額確定模組，當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

第二數額確定模組，根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同；

交易請求發起模組，資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括對所述第二資源的第二數額進行加密處理後得到的第一加密數額信息；

入鏈模組，在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的第二資源轉移到所述資源轉入方，並將執行結果寫入所述區塊鏈。

第四方面，本案實施例還提供一種電子設備，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：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括對所述第二資源的第二數額進行加密處理後得到的第一

加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的第二資源轉移到所述資源轉入方，並將執行結果寫入所述區塊鏈。

第五方面，本案實施例還提供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包括指令，所述指令當被包括多個應用程式的電子設備執行時，能夠使所述電子設備執行以下操作：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括對所述第二資源的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的第二資源轉移到所述資源轉入方，並將執行結果寫入所述區塊鏈。

第六方面，本案實施例提供一種基於區塊鏈的資金轉移裝置，包括：

資金數額確定模組，當滿足轉移條件時，確定待轉移的資金的第一數額；

代幣數額確定模組，根據所述資金的第一數額，確定待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

交易請求發起模組，轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括對所述代幣的第二數額進行加密處理後得到的第一加密數額信息；

入鏈模組，在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈。

第七方面，本案實施例提供一種電子設備，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：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據所述資金的第一數額，確定待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括對所述代幣的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈。

第八方面，本案實施例提供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包括指令，所述指令當被包括多個應用程式的電子設備執行時，能夠使所述電子設備執行以下操作：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據所述資金的第一數額，確定待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括對所述代幣的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈。

第九方面，本案實施例提供一種基於區塊鏈的資源轉移方法，包括：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據所述第一資源的第一數額，採用單向函數確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括與所述第二資源的第二數額相對應的信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的第二資源轉移到所述資源轉入

方，並將執行結果寫入所述區塊鏈。

較佳地，在第九方面提供的基於區塊鏈的資源轉移方法中，根據所述第一資源的第一數額，採用單向函數確定待轉移的第二資源的第二數額，包括：

將所述第一資源的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述第二資源的第二數額。

較佳地，在第九方面提供的基於區塊鏈的資源轉移方法中，所述資源轉出方向區塊鏈發起的所述交易請求中，還包括加密後的所述隨機數。

較佳地，在第九方面提供的基於區塊鏈的資源轉移方法中，所述第一資源具體為資金，所述第二資源具體為代幣。

第十方面，本案實施例提供一種基於區塊鏈的資金轉移方法，包括：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據所述資金的第一數額，採用單向函數確定待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括與所述代幣的第二數額相對應的信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈。

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：

本案實施例提供的技術方案，在滿足資源轉移條件時，確定待轉移的第一資源的第一數額，並在此基礎上，將第一資源的第一數額轉換為資源類型不同的第二資源的第二數額，進而發起用於轉移第二數額的交易請求，並透過對第二數額進行加密處理得到加密數額信息(也就是加密後的第二數額)，從而在區塊鏈針對該交易請求進行驗證、實施和上鏈時，可以透過對第二數額進行加密處理的方式隱藏資源轉出方與資源轉入方之間的具體交易信息，具體表現為待轉移的第一資源的第一數額的信息，從而能夠在資源轉移過程中保護資源轉移雙方的隱私信息。

【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源轉移方法的流程示意圖；

圖2為本案實施例提供的一種資金轉移方法的流程示意圖；

圖3為本案實施例提供的資金轉移方法在資金借貸場景下發放代幣階段的業務流程示意圖；

圖4為本案實施例提供的資金轉移方法在資金借貸場

景下申請貸款階段的業務流程示意圖；

圖5為本案實施例提供的資金轉移方法在資金借貸場景下還款階段的業務流程示意圖；

圖6為本案實施例提供的另一種資源轉移方法的流程示意圖；

圖7為本案實施例提供的另一種資金轉移方法的流程示意圖；

圖8為本案實施例提供的一種資源轉移裝置的結構示意圖；

圖9為本案實施例提供的一種電子設備的結構示意圖；

圖10為本案實施例提供的一種資金轉移裝置的結構示意圖；

圖11為本案實施例提供的又一種電子設備的結構示意圖。

【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。

本案中所稱的資源，可以具體化為資料資源、資金資

源等可以在多方之間轉移的資源類型。在基於區塊鏈技術構建的資源管理平台上，資源持有者之間可以在滿足資源轉移條件時進行資源的轉移。具體的，可以在確定待轉移的資源的數額後，由資源轉出方向區塊鏈發起交易請求；區塊鏈對交易請求進行驗證、實施，資源轉出方將待轉移的資源轉移到資源轉入方後，區塊鏈將該交易請求的執行結果寫入區塊鏈。為解決交易入鏈後對資源轉移雙方的隱私信息構成威脅的問題，本案實施例提供了基於區塊鏈的資源轉移方法。以下將結合附圖，詳細說明本案各實施例提供的技術方案。

參見圖1所示，一種基於區塊鏈的資源轉移方法，適用於資源轉出方，具體包括：

S101：當滿足資源轉移條件時，確定待轉移的第一資源的第一數額。

可以理解到，當滿足資源轉移條件，需要進行資源轉移之前，資源轉出方需要確定待轉移的資源的類型及其數額，也就是待轉移的第一資源的第一數額。除此之外，資源轉出方也要確定出該次資源轉移的對象，即接收被轉移的資源的資源轉入方。

需要說明的是，在不同的應用場景下，出於不同的業務目的，資源轉移條件也會不同，具體的資源轉移條件可以根據資源轉移雙方的約定或者資源轉移所依托的業務平台的業務流程設置確定。更進一步地，在資源轉移所依托的業務平台上，根據實際業務流程的需要，可能會需要進

行多次資源轉移，以實現業務流程中不同階段的不同目的。出於不同目的進行的資源轉移，轉移的資源的類型、數額以及參與資源轉移的資源轉出方和資源轉入方也都可能不同，資源轉出方為實現資源的轉移而發起的交易請求的內容和格式也都可能不同。後文將針對多種不同的情況展開舉例說明。

S103：根據第一資源的第一數額，確定待轉移的第二資源的第二數額；第一資源與第二資源的類型不同。

需要說明的是，第一資源和第二資源的類型並不相同。執行步驟S103，將第一資源轉換為第二資源，相對應地，資源的數額也從第一資源的第一數額轉換為第二資源的第二數額。因此，在進一步進行資源轉移時，可以將對第一資源的轉移轉換為對第二資源的轉移。第一資源和第二資源的關係，可以理解為，第一資源為資源轉移雙方實質上需要轉移的資源類型(例如，在借貸場景下，第一資源可以具體化為資金，對應到真實的貨幣)，而第二資源為資源轉移時實際轉移的資源類型(例如，在借貸場景下，第二資源可以具體化為代幣，是一種虛擬的貨幣)。從保護資源轉移雙方的隱私信息的角度，也可以認為第二資源是第一資源的保護外殼，本案實施例在進行資源轉移時，將在實際業務中有實質價值的第一資源轉換為顯性的、可以沒有實質價值的第二資源進行轉換，因此，即使被實際轉移的第二資源的第二數額的相關信息被寫入區塊鏈，具有實際價值的第一資源的第一數額的信息仍然被隱

藏，從而有利於保護資源轉移這一交易的隱私。

還需要說明的是，第一資源和第二資源之間，除了類型不同之外，兩種資源的數額之間還存在對應關係，或者說數額的轉換關係，具體的轉換關係可以根據業務平台的需要進行設置。

例如，第一資源和第二資源的數額可以直接相等，即二者1:1的進行轉換。這種情況下，雖然資源轉移雙方之外的第三方可能透過第二資源的第二數額能夠推知第一資源的第一數額，但是，由於本案實施例在後續步驟發起的交易請求中，並非直接攜帶第二數額的信息，而是對第二數額進行加密處理，在交易請求中攜帶加密處理後得到的第一加密數額信息。因此，仍然可以保護資源轉移的實質數額的信息，從而保護交易隱私。

又例如，第一資源和第二資源的數額可以按照預設的轉換係數或者函數關係進行轉換，透過保護這種轉換係數或者函數關係，也能夠對資源轉移的實質數額(也就是第一資源的第一數額)進行保護。可以理解到，參與資源轉移的雙方需要知曉這種轉換係數或者函數關係，以便實現資源類型的反向轉換(即由第二類型的第二數額轉換為第一類型的第一數額)，從而達到資源轉移的最終目的。

更進一步地，第一資源和第二資源的數額較佳透過單向函數實現轉換，也就是說，根據第一資源的第一數額，採用單向函數確定第二資源的第二數額。具體地，可以將第一資源的第一數額和一隨機數作為單向函數的輸入，將

單向函數的輸出確定為第二資源的第二數額。採用這種方式，利用單向函數的特性，即使在後續發起的交易請求中不對第二數額進行加密處理，而是直接將透過單向函數轉換得到的第二數額放入交易請求中，也能在一定程度上保護資源轉移的實質數額(也就是第一資源的第一數額)。當然，在此基礎上，對第二數額進行進一步的加密處理以得到第一加密數額信息，並將第一加密數額信息攜帶在資源轉出方發起的交易請求中，能夠更好的保護資源轉移交易的隱私信息。

在採用單向函數實現第一資源與第二資源間的數額轉換時，資源轉出方還需要將進行轉換時使用的隨機數(作為單向函數的一個輸入)發送給資源轉入方，以便資源轉入方進行資源類型的反向轉換，推知第一資源的第一數額。在具體實施時，可以在資源轉出方向區塊鏈發起交易請求之前，對這一隨機數進行加密，進而發起的交易請求中攜帶的為加密後的隨機數，從而避免了隨機數的洩密，進而保護了資源轉移交易的隱私信息。具體地，可以借助資源轉入方的公鑰對隨機數進行加密，從而只有資源轉入方的私鑰才能對該隨機數進行解密，進而利用該隨機數實現資源類型的反向轉換，也就是從第二資源的第二數額推知第一資源的第一數額。

S105：資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源；其中，交易請求中包括對第二資源的第二數額進行加密處理後得到的第一加密數

額信息。

本案實施例中，執行步驟S105之前，可以還包括對第二資源的第二數額進行加密處理，得到第一加密數額信息的步驟。無論第一資源與第二資源之間的轉換關係是否能夠被資源轉移雙方以外的第三方知曉，只要對第二數額的信息進行加密處理，就能夠保護資源轉移交易的具體數額信息，從而保護資源轉移雙方的隱私。

需要說明的是，交易請求中包括的第一加密數額信息，可以透過採用第一加密函數(記為enc(x,y))對第二資源的第二數額進行加密處理得到。其中，第一加密函數的一個輸入為第二資源的第二數額(記為quota_c)，另一個輸入為資源轉入方的公鑰(記為pk_c)。可以理解到，若資源轉入方的公鑰為非對稱密鑰，則該第一加密函數為非對稱加密函數；若資源轉入方的公鑰為對稱密鑰，則該第一加密函數為對稱加密函數。

可選的，還可以將資源轉入方的公鑰的標識信息作為交易請求的一部分發送到區塊鏈系統，供區塊鏈系統在驗證、實施後上鏈。具體地，可以採用資源轉入方的公鑰的雜湊值(記為hash(pk_c))作為公鑰的標識信息。

此時，資源轉出方發起的交易請求TX的交易格式可表示為：

$$TX=(enc(pk_c, quota_c), hash(pk_c))$$

需要說明的是，在不同的應用場景下，基於不同的資源轉移條件和目的，交易請求中攜帶的信息將有所不同。

後續將詳細舉例說明。

S107：在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入區塊鏈。

需要說明的是，區塊鏈系統接收到資源轉出方發起的交易請求後，區塊鏈的各節點將對交易請求進行驗證。當達成共識，交易請求驗證通過後，資源轉出方進一步執行該交易請求，將待轉移的第二資源轉移到資源轉入方。可以理解到，被轉移的第二資源的數額為第二數額。資源轉移結束後，將該交易請求的執行結果寫入區塊鏈。

還需要說明的是，區塊鏈系統的各節點對交易請求進行驗證時，主要驗證交易請求的格式是否符合約定(例如交易請求中的欄位個數，各欄位的長度，某欄位的內容等)，而對於交易請求中攜帶的加密信息，例如第一加密數額信息，單向函數中加密後的隨機數等信息，將直接驗證通過，進而執行交易請求。

可以理解到，當區塊鏈中的節點對資源轉出方的交易請求驗證通過後，資源轉出方會將第二資源(數額為第二數額)轉移到資源轉入方。資源轉入方接收到轉移來的第二資源後，可以根據第一資源與第二資源的轉換關係，確定本次資源轉移交易實質轉移的第一資源的數額是否為第一數額。

採用本案實施例提供的技術方案，在滿足資源轉移條件時，確定待轉移的第一資源的第一數額，並在此基礎

上，將第一資源的第一數額轉換為資源類型不同的第二資源的第二數額，進而發起用於轉移第二數額的交易請求，並透過對第二數額進行加密處理得到加密數額信息(也就是加密後的第二數額)，從而在區塊鏈針對該交易請求進行驗證、實施和上鏈時，可以透過對第二數額進行加密處理的方式隱藏資源轉出方與資源轉入方之間的具體交易信息，具體表現為待轉移的第一資源的第一數額的信息，從而能夠在資源轉移過程中保護資源轉移雙方的隱私信息。

在本案實施例中，在進行資源轉移時首要保護的就是具體的交易數額信息，也就是待轉移的第一資源的第一數額。在不同的應用場景下，資源轉移條件也有所不同，確定出待轉移的第一資源的第一數額的方式、以及確定出的第一數額也不盡相同。以下將舉例說明。

(1)當資源轉移條件為允許資源轉入方借取第一資源時，可以理解為資源轉出方或業務系統中約定的其他參與方已經對資源轉入方借取第一資源的資格和能力進行了審查，並確定了允許資源轉入方借取的第一資源的額度。此時，資源轉出方向資源轉入方轉移資源的目的，可以理解為業務系統批准資源轉入方進行第一資源的借取，並向資源轉入方發放允許借取第一資源的數額的憑證。在此場景下，資源轉出方為業務系統中約定的發放額度憑證的業務參與方，資源轉入方為被允許借取第一資源的業務參與方。還可以理解到，在完成本次資源轉移之後，資源轉入方所持有的第二資源的數額，反映的就是資源轉入方能夠

借取的資源的額度。

因而，此時在確定待轉移的第一資源的第一數額時，可將允許資源轉入方借取的第一資源的額度，作為待轉移的第一資源的第一數額。在此基礎上根據第一資源的第一數額確定出的第二資源的第二數額，也能反映允許資源轉入方借取資源的額度。因此，資源轉出方發起的轉移第二資源的交易請求中，包含的第一加密數額信息(該信息透過對第二數額進行加密處理後得到)也能反映允許資源轉入方借取第一資源的數額，該第一加密數額信息也就是向資源轉入方發放的、允許借取第一資源的憑證。由於該第一加密數額信息對於資源轉移雙方之外的第三方而言是密文資料(無法知曉第二資源的第二數額)，因此，這種方式能夠保護資源轉入方被批准借取第一資源的額度這一隱私信息，達到本案實施例的技術目的。

還需要說明的是，將業務系統批准資源轉入方進行第一資源的借取後向資源轉入方發放額度憑證的這一交易請求寫入區塊鏈，有利於監管和限制資源轉入方借取第一資源的數額不超過允許的額度，進而保護借出資源的一方的利益。

(2)當資源轉移條件為資源轉出方已接收到資源轉入方歸還的第一資源時，可以理解為，在實際業務流程中，資源轉入方為第一資源的借入方，資源轉出方為第一資源的借出方。資源轉入方將需歸還的第一資源轉移到資源轉出方，以歸還向資源轉出方借取的第一資源，這一過程並

不寫入區塊鏈；當資源轉出方接收到資源轉入方在鏈下歸還的第一資源後，資源轉出方執行本案實施例的資源轉移方法，將與歸還的第一資源的數額相對應的第二資源轉移到資源轉入方。此時，進行資源轉移的目的在於，在資源轉入方將借取的資源歸還後，為其恢復額度或者補足額度。

因而，此時在確定待轉移的第一資源的第一數額時，可以將歸還的第一資源的數額，確定為待轉移的第一資源的第一數額。進行資源轉移時，將數額與第一資源的第一數額相對應的第二資源轉移到資源轉入方，以便恢復其借取資源的額度。可以理解到，在完成本次資源轉移之後，資源轉入方所持有的第二資源的數額，反映的就是資源轉入方能夠借取的資源的剩餘額度。

在資源轉出方發起交易請求時，將依據第一資源的第一數額確定出的第二資源的第二數額進行加密處理，可以保護資源轉入方實際歸還的資源的數額這一隱私資料，達到本案的技術目的。

還需要說明的是，在資源借取方歸還第一資源後，向資源借取方轉移對應數額的第二資源，並將轉移第二資源的交易寫入區塊鏈，一方面為資源借取方恢復額度或者補足額度，以便保障資源借取方的正常交易，另一方面有利於監管和限制資源借取方借取資源的數額，從而保護資源借出方的利益。

(3)當資源轉移條件為資源轉入方與資源轉出方已達

成資源借取協議時，資源借取協議中包含資源轉出方向資源轉入方申請借取的第一資源的數額。對應到實際業務流程中，該場景下的資源轉出方為第一資源的借取方，資源轉入方為第一資源的借出方。在雙方達成資源借取協議後，借取方(對應到此場景下的資源轉出方)將自己所持有的第二資源中對申請借取的第一資源的數額相對應的部分轉移到借出方(對應到此場景下的資源轉入方)，這一過程寫入區塊鏈；借出方在收到被轉移的第二資源後，進一步將資源借取協議中約定的應借給借入方的第一資源轉移給借取方，這一過程無需寫入區塊鏈，在鏈下採用常規業務手段實施即可。

在此場景下，借取方(資源轉出方)將自己所持有的第二資源中與申請借取的第一資源的數額相對應的部分轉移到借出方(資源轉入方)，進行這一資源轉移並將資源轉移的交易寫入區塊鏈的目的，可以理解為，一方面，資源轉出方向資源轉入方證明自己借取資源的額度(體現為在資源轉移前，資源轉出方所持有的第二資源的數額)滿足本次申請借取的資源的數額要求，以便資源轉出方能夠向資源轉入方借取具有實際價值的第一資源；另一方面，資源轉出方在轉移出對應數額的第二資源後，自己所持有的第二資源的數額將相應減少，也就相當於扣減了允許資源轉出方借取資源的額度，將這一額度被扣減的交易寫入區塊鏈，有利於監管和限制資源借取方借取資源的數額，從而保護資源借出方的利益。

在這一場景下，可以將資源借取協議中申請借取的第一資源的數額，確定為待轉移的第一資源的第一數額，進而在此基礎上確定待轉移的第二資源的第二數額，以便進行第二資源的轉移。

可以理解到，在上述舉例的第(3)類場景下，申請借取第一資源的資源借取方(在本次資源轉移過程中充當資源轉出方)的額度需要受到限制，因此，為了實現資源轉移，資源轉出方需要向區塊鏈上除參與本次資源轉移交易的節點(資源轉出方和資源轉入方所對應的節點)之外的節點，證明本次資源轉移交易的合法性。

較佳地，可以在資源轉出方發起的交易請求中加入零知識證明，用於證明執行交易請求之後資源轉出方將要持有的第二資源的餘額與第二數額的和，等於資源轉出方在發起交易請求前所持有的第二資源的數額。利用零知識證明，資源轉出方就可以在不暴露任何具體信息(包括資源轉移的數額等)的情況下，向區塊鏈上的各節點證明相關內容的真實性，具體的，可以理解為證明上述“執行交易請求之後資源轉出方將要持有的第二資源的餘額與第二數額的和，等於資源轉出方在發起交易請求前所持有的第二資源的數額”這一論斷為真。

具體地，將資源轉出方將要持有的第二資源的餘額記為quota_c’，將待轉移的第二資源的第二數額記為quota_d，將資源轉出方在發起交易請求前所持有的第二資源的數額記為quota_c，則上述零知識證明函數proof(x)

可表達為proof(quota_c'=(quota_c-quota_d))。該零知識證明函數證明的就是：等式(quota_c'=(quota_c-quota_d))確實成立。

在此基礎上，資源轉出方向區塊鏈發起的交易請求TX，其交易格式可以表示為：

Tx=(enc(pk_d, quota_d),hash(pk_d), proof((quota_c- quota_d- quota_c' ==0)))

進一步地，資源轉出方還可以利用零知識證明向區塊鏈中的各節點證明以下事項：資源轉出方轉出的第二資源的數額，即第二數額quota_d大於零，資源轉出方在發起交易請求前所持有的第二資源的數額quota_c大於零，並且，執行交易請求之後資源轉出方將要持有的第二資源的餘額quota_c'不小於零。從而，該零知識證明函數可以表達為：

proof((quota_c- quota_d- quota_c' ==0)&& (quota_c>0) && (quota_d>0) && (quota_c' ≥0))

此時，資源轉出方向區塊鏈發起的交易請求TX，其交易格式可以表示為：

Tx=(enc(pk_d, quota_d),hash(pk_d), proof((quota_c- quota_d- quota_c' ==0)&& (quota_c>0) && (quota_d>0) && (quota_c' ≥0)))

進一步較佳地，交易請求中還可以包括資源轉出方參與的上一次資源轉移交易的標識信息(可記為Tx_in)，可具體取為區塊鏈中記錄的、上一次資源轉移交易的雜湊值。需要說明的是，資源轉出方參與的上一次資源轉移交易，可以是借取資源的交易，也可以是確認借取額度的交易，

還可以是歸還資源後增補額度的交易。將資源轉出方參與的上一次資源轉移交易的標識信息發送到區塊鏈中進行驗證，有利於保證資源轉出方(作為資源借取方)所持第二資源數額變化的連貫性。此時，資源轉出方向區塊鏈發起的交易請求TX，其交易格式可以表示為：

Tx=(Tx_in, (enc(pk_d, quota_d), hash(pk_d)), proof((quota_c-quota_d-quota_c’ ==0)&& (quota_c>0) && (quota_d>0) && (quota_c’ >0)))

進一步較佳地，交易請求中還可包括對執行交易請求之後資源轉出方將要持有的第二資源的餘額(記為quota_c’)進行加密處理後得到的第二加密數額信息。具體地，可透過採用第二加密函數(記為enc(x,y))對執行交易請求之後資源轉出方將要持有的第二資源的餘額quota_c’進行加密處理。其中，第二加密函數的一個輸入為第二資源的餘額(記為quota_c’)，另一個輸入為資源轉出方的公鑰(記為pk_c)。可以理解到，若資源轉出方的公鑰為非對稱密鑰，則該第二加密函數為非對稱加密函數；若資源轉出方的公鑰為對稱密鑰，則該第二加密函數為對稱加密函數。

可選的，還可以將資源轉出方的公鑰的標識信息作為交易請求的一部分發送到區塊鏈系統，供區塊鏈系統在驗證、實施後上鏈。具體地，可以採用資源轉出方的公鑰的雜湊值(記為hash(pk_c))作為公鑰的標識信息。則此時，資源轉出方發起的交易請求TX的交易格式可表示為：

Tx=(Tx_in, (enc(pk_d, quota_d), hash(pk_d)), (enc(pk_c, quota_c’), hash(pk_c)), proof((quota_c- quota_d- quota_c’ ==0)&& (quota_c>0) && (quota_d>0) && (quota_c’ >0)))

以上從多個角度對本案實施例提供的資源轉移方法在不同場景下、基於不同目的進行資源轉移時的具體實現進行了舉例說明。在不同的資源轉移條件下，進行資源轉移的目的不同，參與資源轉移方在業務流程中的角色不同。無論出於何種目的進行資源轉移，在向區塊鏈發起用於轉移第二數額的交易請求時，都可以透過對第二數額進行加密處理的方式隱藏資源轉出方與資源轉入方之間的具體交易信息，具體表現為待轉移的第一資源的第一數額的信息，從而能夠在資源轉移過程中保護資源轉移雙方的隱私信息。

在一種場景下，第一資源具體化為資金，第二資源具體化為代幣。這一場景下涉及到基於區塊鏈的資金轉移方法，參見圖2所示，包括：

S201：當滿足轉移條件時，確定待轉移的資金的第一數額；

S203：根據資金的第一數額，確定待轉移的代幣的第二數額；資金與代幣的類型不同；

S205：轉出方向區塊鏈發起交易請求，用於向轉入方轉移待轉移的代幣；其中，交易請求中包括對代幣的第二數額進行加密處理後得到的第一加密數額信息；

S207：在區塊鏈對交易請求進行驗證後，執行交易請

求，將待轉移的代幣轉移到轉入方，並將執行結果寫入區塊鏈。

可以理解到，上述基於區塊鏈的資金轉移方法在具體實施上的各方面，與前述實施例的基於區塊鏈的資源轉移方法相同，因此，前述實施例中關於資源轉移方法的闡釋與說明均適用於此資金借貸場景下的資源借貸方法。以下將主要以資金借貸的業務流程為例，說明本實施例的具體實施。

在資金借貸這一應用場景下，業務流程可以包括信用評估和代幣發放階段、貸款申請和發放階段、以及還款階段等。

(一)信用評估和代幣發放階段

在進行信用評估時，可以預先確定一個特定機構A，對用戶的信用等級進行評估，並就用戶的貸款發放額度給出具有公信力的結論。可以理解到，這一特定機構A的確定，可以透過資金監管部門按照相關規定審核和指定，也可以由參與放貸的機構進行推舉或約定產生。該特定機構A的職能主要在於根據用戶的相關信息對用戶進行信用評估，並確定該用戶的貸款發放額度(以真實貨幣，即資金的形式體現，也就是本案實施例中前文所述的第一資源的第一數額)。

在具體實施時，擬申請貸款的用戶C的相關信息往往涉及到用戶C的個人隱私，例如用戶的姓名、身份證號等

個人信息，以及用戶的收入資料、消費信息、還款狀況等涉及到用戶C的資金調度能力的信息。為保護用戶C的隱私，用戶C向特定機構A提供的信息並不向其他機構披露，例如發放貸款的機構等，而僅供特定機構A知曉。

在對擬申請貸款的用戶C進行信用評估後允許其貸款、並為其確定貸款發放額度的情況下，特定機構A將評估結果(包括貸款發放額度)發送到預設的特定機構B，由特定機構B向擬申請貸款的用戶C發放與貸款發放額度相對應的數額的代幣(以虛擬貨幣的形式體現，也就是本案實施例中前文所述的第二資源)。在具體實施時，特定機構A和特定機構B可以由同一實體機構兼任。

可以理解到，在信用評估和代幣發放階段，當允許擬申請貸款的用戶C貸款時(相當於滿足轉移條件)，將允許用戶C借取的貸款發放額度確定為待轉移的資金的第一數額，並在此基礎上確定出待轉移的代幣的第二數額(如前述實施例中所述，可以有多種方式實現資金的第一數額與代幣的第二數額之間的對應)。此時，轉出方具體化為上述特定機構B，轉入方具體化為擬申請貸款的用戶C，轉出方向區塊鏈發起的交易請求中，包括對代幣的第二數額(記為quota_c)進行加密處理後得到的第一加密數額信息。

具體地，可以透過採用第一加密函數(記為enc(x,y))對代幣的第二數額quota_c進行加密處理得到。其中，第一加密函數的一個輸入為代幣的第二數額quota_c，另一個輸入為轉入方(也就是用戶C)的公鑰(記為pk_c)。可以理

解到，若轉入方的公鑰為非對稱密鑰，則該第一加密函數為非對稱加密函數；若轉入方的公鑰為對稱密鑰，則該第一加密函數為對稱加密函數。

進一步地，還可以將轉入方的公鑰pk_c的標識信息作為交易請求的一部分發送到區塊鏈系統，供區塊鏈系統在驗證、實施後上鏈。具體地，可以採用轉入方的公鑰的雜湊值(記為hash(pk_c))作為公鑰的標識信息。此時，轉出方(即特定機構B)發起的交易請求TX的交易格式可表示為：

TX=(enc(pk_c, quota_c), hash(pk_c))

在本案實施例中，用戶C所持有的代幣的數額(此處體現為quota_c)能夠反映用戶C允許借取的實際資金的數額(也就是貸款發放額度)。可以理解到，當用戶C已借取了部分資金(實際借取的資金的數額應不大於上述貸款發放額度)時，用戶C所持有的代幣的數額將減少，表示用戶C能夠借取的資金的額度被扣減；而當用戶C將已借取的資金歸還時，用戶C所持有的代幣的數額將會增加，表示用戶C能夠借取的資金的額度被恢復或補足。

需要說明的是，在業務流程中，可以定時或周期性地對用戶C重新進行信用評估，從而調整用戶的貸款發放額度。當額度提高時，特定機構B可以執行上述資金轉移過程向用戶C發放額度的差值，此時，將額度的差值確定為待轉移的資金的第一數額。當額度降低時，可以要求用戶在指定時間內向特定機構B返還額度的差值，在這一資金

轉移的過程中，用戶C將作為轉出方，特定機構B將作為轉入方，將額度的差值確定為待轉移的資金的第一數額。

可以理解到，若用戶逾期未將因額度降低而需返還的額度差值返還給特定機構B，則特定機構B可以向所有的貸款發放機構發送黑名單，限制用戶C辦理貸款，而僅允許接收用戶C還款，直至用戶C返還額度的差值。

透過上述方式，將代表貸款額度的代幣發放到用戶C，並將這一發放過程寫入區塊鏈，有利於對用戶C的貸款額度進行監管，從而降低了貸款發放機構放貸的風險，維護了交易安全。

為便於理解，圖3給出了在信用評估和發放代幣階段的業務流程示意圖，具體如下：

首先，用戶C向進行信用評估的機構A提交個人資料，供機構A對本人的信用進行評估。

其次，機構A根據信用評估的結果決定是否允許用戶C貸款，確定允許的貸款額度(相當於第一資源的第一數額，資金的第一數額，體現為真實貨幣)，並向用戶C反饋信用評估的結果。

再次，機構A將允許用戶C貸款的額度的信息發送至機構B，進行代幣發放。機構B根據額度的信息確定與貸款額度相對應的代幣的數額(相當於第二資源的第二數額，代幣的第二數額，體現為虛擬貨幣)。

然後，機構B(作為資源轉出方，轉出方)向區塊鏈平台發起交易請求，該交易請求中包含代幣數額的信息。為

保護隱私，該信息為對代幣數額進行加密處理後的加密信息。區塊鏈平台對該交易請求的合法性進行驗證確認後，允許機構B實施該交易請求；並在機構B向用戶C(作為資源轉入方，轉入方)轉移對應數額的代幣後，將交易的實施結果寫入區塊鏈。

至此完成了對用戶C的信用評估和代幣發放。用戶C所持有的代幣的數額反映允許用戶C借取的貸款的額度。

(二)貸款申請和發放階段

當用戶C需要申請貸款時，可以與發貸機構D達成貸款協議(相當於資源轉移過程中的資源借取協議)，確定用戶C申請借取的資金的數額(相當於第一資源的第一數額)。在貸款協議達成後，根據協議中確定的申請借取的資金的第一數額確定相對應的代幣的第二數額(相當於第二資源的第二數額)。用戶C向發貸機構D發送所持有的代幣，代幣的數額為第二數額，記為quota_d，並可以進一步將所持有代幣的餘額(記為quota_c')返回自己的帳戶。發貸機構D接收到用戶C發送的代幣(虛擬貨幣)後，即可將資金(真實貨幣)發送給用戶C，以便用戶C取得申請借取的資金。

在上述過程中，用戶C向區塊鏈發送交易請求，以將數額為quota_d的代幣發送到發貸機構D。該交易請求中，可包含對quota_d進行加密處理得到的第一加密數額信息，反映將要轉移到機構D的代幣的數額；還可包含對用

戶C所持代幣的餘額quota_c’進行加密處理得到的第二加密數額信息，反映將要返回用戶C的自有帳戶的代幣的餘額；還可進一步包含用戶C參與的上一次資金轉移交易的標識信息(可記為Tx_in)，可具體取為區塊鏈中記錄的、上一次資金轉移交易的雜湊值，也可以是預設的用於區分不同交易的標識符，反映用戶C所持有代幣的數額quota_c的確定依據。

除此之外，用戶C向區塊鏈發送的交易請求中，還可以加入零知識證明，用於證明執行交易請求之後轉出方(用戶C)將要持有的代幣的餘額quota_c’與轉移的代幣數額quota_d的和，等於轉出方(用戶C)在發起交易請求前所持有的代幣的數額quota_c，也就是，利用零知識證明證明等式((quota_c-quota_d)=quota_c’)成立。進一步地，還可以利用零知識證明證明轉出方(用戶C)轉出的代幣的數額quota_d大於零，轉出方(用戶C)在發起交易請求前所持有的代幣的數額quota_c大於零，並且，執行交易請求之後轉出方(用戶C)將要持有的代幣的餘額quota_c’不小於零。

因此，用戶C向區塊鏈發起的交易請求，其交易格式可表示為：

Tx=(Tx_in, enc(pk_d, quota_d), hash(pk_d), enc(pk_c, quota_c’), hash(pk_c), proof((quota_c- quota_d- quota_c’ ==0)&& (quota_c>0) && (quota_d>0) && (quota_c’ >0)))

在上述交易請求中，Tx_in可以理解為本次交易的輸入，反映用戶C(此處為轉出方)所持有的代幣的數額的來

源。enc(pk_d, quota_d),hash(pk_d)可以理解為本次交易的第一個輸出，反映用戶C向機構D發送的代幣的數額quota_d，亦能反映機構D接收到用戶C發送的代幣的數額。enc(pk_c, quota_c’),hash(pk_c)可以理解為本次交易的第二個輸出，反映用戶C在完成代幣轉移後剩餘的代幣的數額quota_c’，相當於用戶C發送代幣後獲得的找零。零知識證明用於向區塊鏈中未參與本次交易的節點證明本次交易的合法性，同時並不洩漏本次交易的具體數額，保護了交易雙方的隱私。

透過將這一交易上鏈，可以將參與交易的雙方(用戶C和發貸機構D)所持代幣的變化狀態寫入區塊鏈，從而能夠監管交易的合法性，避免用戶C超過貸款額度申請貸款。同時，透過對轉移代幣的具體數額進行加密處理，並透過零知識證明來證明合法性，也保護了交易雙方的隱私。

為便於理解，圖4給出了貸款申請和發放階段的業務流程示意圖，具體如下：

首先，用戶C向貸款發放的機構D提出貸款申請。在與機構D達成貸款協議後，用戶C根據貸款協議的約定確定貸款的金額(相當於第一資源的第一數額，資金的第一數額，體現為真實貨幣)，再據此確定與貸款的金額相對應的代幣的數額(相當於第二資源的第二數額，代幣的第二數額，體現為虛擬貨幣)。

其次，用戶C(作為資源轉出方，轉出方)向區塊鏈平台發起交易請求，該交易請求中包含代幣數額的信息。為

保護隱私，該信息為對代幣數額進行加密處理後的加密信息。區塊鏈平台對該交易請求的合法性進行驗證確認後，允許用戶C實施該交易請求；並在用戶C向機構D(作為資源轉入方，轉入方)轉移對應數額的代幣後，將交易的實施結果寫入區塊鏈。

然後，機構D在接收到用戶C轉移的代幣後，向對應數額的貸款發放給用戶C。

至此用戶C完成了貸款的申請，機構D完成了貸款的發放。可以理解到，在交易完成後，用戶C所持有的代幣的數額將被扣減，所持有的代幣的餘額反映允許用戶C借取的貸款的剩餘額度。

(三)還款階段

當用戶C需要向發貸機構D還款時，用戶C先向發貸機構D的銀行帳戶進行匯款，用真實貨幣(相當於第一資源)歸還借款。而後發貸機構D在接收到用戶C歸還的真實貨幣後，透過向區塊鏈發起交易請求，將與用戶C歸還的真實貨幣數額相對應的代幣(相當於第二資源)轉移給用戶C，從而為用戶C恢復或者補足貸款額度。

具體地，轉出方(此處為發貸機構D)發起的交易請求TX的交易格式可表示為：

TX=(enc(pk_c, quota_d), hash(pk_c))

該交易請求可以理解為，採用加密函數對發貸機構D(資金轉出方)接收到的資金的數額相對應的代幣的數額

quota_d進行加密處理，其中，加密函數的一個輸入為代幣的數額quota_d，另一個輸入為用戶C(資金轉入方)的公鑰pk_c。除此之外，還將用戶C的公鑰的標識信息，例如公鑰pk_c的雜湊值hash(pk_c)，作為交易請求的一部分發送到區塊鏈系統。

為便於理解，圖5給出了還款階段的業務流程示意圖，具體如下：

首先，用戶C將需歸還的資金發送給發放貸款的機構D，實現真實貨幣的歸還。

其次，機構D確認接收到用戶C還款的資金的金額(相當於第一資源的第一數額，資金的第一數額，體現為真實貨幣)，並在此基礎上確定與還款的金額相對應的代幣的數額(相當於第二資源的第二數額，代幣的第二數額，體現為虛擬貨幣)。

再次，機構D(作為資源轉出方，轉出方)向區塊鏈平台發起交易請求，該交易請求中包含代幣數額的信息。為保護隱私，該信息為對代幣數額進行加密處理後的加密信息。區塊鏈平台對該交易請求的合法性進行驗證確認後，允許機構D實施該交易請求；並在機構D向用戶C(作為資源轉入方，轉入方)轉移對應數額的代幣後，將交易的實施結果寫入區塊鏈。

至此用戶C完成了貸款的歸還，機構D完成了貸款的收回。可以理解到，在交易完成後，用戶C所持有的代幣的數額將增加，所持有的代幣的數額反映允許用戶C借取

的貸款的額度。

在上述各個階段中，均採用了本案實施例提供的資金轉移方法，透過將代表真實貨幣的資金的數額轉換為代表虛擬貨幣的代幣的數額，並透過對在區塊鏈中流通的代幣數額進行加密處理的方式，保護了交易雙方的隱私。即使有多家放貸機構加入區塊鏈平台進行貸款的發放，用戶在多家發放機構申請的貸款的總數額也不會超過被允許的貸款額度，從而降低了發貸機構的放貸風險。這會因為，如以上示例中所述，反映貸款額度的代幣由特定的機構B發放，用戶所持代幣的數額也會隨著用戶的借貸、還款行為相應變化，且帶來這些變化過程的交易均被寫入區塊鏈，利用區塊鏈技術本身的公開、透明、不可篡改的特性，就能夠保證代幣數額的真實性和可靠性，進而確保用戶無法超額申請貸款。

與此同時，上述反映貸款額度的代幣的變化的交易中，轉移的代幣的數額均已進行加密處理，從而隱藏了交易雙方的具體交易信息，因此，也能夠在資金轉移過程中保護資金轉移雙方的隱私信息。

本案實施例還提供了一種基於區塊鏈的資源轉移方法，參見圖6所示，包括：

S301：當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

S303：根據第一資源的第一數額，採用單向函數確定待轉移的第二資源的第二數額；第一資源與第二資源的類

型不同；

S305：資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源；其中，交易請求中包括與第二資源的第二數額相對應的信息；

S307：在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入區塊鏈。

該實施例中，將實際需要轉移的第一資源轉換為第二資源進行轉移，透過對第二資源的轉移就能夠達到資源轉移的目的，同時，透過單向函數實現第一資源和第二資源之間的數額轉換，利用單向函數的特性，使得交易雙方之外第三方無法根據第二資源的第二數額推知第一資源的第一數額，從而可以隱藏實際轉移的第一資源的數額，起到保護交易隱私的作用。

更進一步地，根據第一資源的第一數額，採用單向函數確定第二資源的第二數額時，可以將第一資源的第一數額和一隨機數作為單向函數的輸入，將單向函數的輸出確定為第二資源的第二數額。採用這種方式，利用單向函數的特性，即使在後續發起的交易請求中不對第二數額進行加密處理，而是直接將透過單向函數轉換得到的第二數額放入交易請求中，也能在一定程度上保護資源轉移的實質數額(也就是第一資源的第一數額)。當然，在此基礎上，對第二數額進行進一步的加密處理以得到第一加密數額信息，並將第一加密數額信息攜帶在資源轉出方發起的交易

請求中，能夠更好的保護資源轉移交易的隱私信息。

在採用單向函數實現第一資源與第二資源間的數額轉換時，資源轉出方還需要將進行轉換時使用的隨機數(作為單向函數的一個輸入)發送給資源轉入方，以便資源轉入方進行資源類型的反向轉換，推知第一資源的第一數額。在具體實施時，可以在資源轉出方向區塊鏈發起交易請求之前，對這一隨機數進行加密，則發起的交易請求中攜帶的為加密後的隨機數，從而避免了隨機數的洩密，保護了資源轉移交易的隱私信息。具體地，可以借助資源轉入方的公鑰對隨機數進行加密，從而只有資源轉入方的私鑰才能對該隨機數進行解密，以便保護交易隱私。

需要說明的是，在採用單向函數進行第一資源和第二資源的數額轉換時，每一次交易所採用的隨機數應是變化的，從而避免交易數額信息的洩漏。

可以理解到，本實施例中也可應用於資金借貸這一應用場景。在該場景下，第一資源具體為資金，第二資源具體為代幣。所對應的基於區塊鏈的資金轉移方法，參見圖7所示，包括：

S401：當滿足轉移條件時，確定待轉移的資金的第一數額；

S403：根據資金的第一數額，採用單向函數確定待轉移的代幣的第二數額；資金與代幣的類型不同；

S405：轉出方向區塊鏈發起交易請求，用於向轉入方轉移待轉移的代幣；其中，交易請求中包括與代幣的第二

數額相對應的信息；

S407：在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的代幣轉移到轉入方，並將執行結果寫入區塊鏈。

需要說明的是，本實施例中採用單向函數實現第一資源與第二資源的轉換(或者資金的數額與代幣的數額的轉換)的方式，與前述多個實施例可以組合實施，也都適用於各具體的業務流程，此處不再贅述。

與圖1提供的基於區塊鏈的資源轉移方法相對應地，本案實施例還提供了一種基於區塊鏈的資源轉移裝置，參見圖8所示，包括：

第一數額確定模組101，當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

第二數額確定模組103，根據第一資源的第一數額，確定待轉移的第二資源的第二數額；第一資源與第二資源的類型不同；

交易請求發起模組105，資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源；其中，交易請求中包括對第二資源的第二數額進行加密處理後得到的第一加密數額信息；

入鏈模組107，在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入區塊鏈。

圖9是本案的一個實施例電子設備的結構示意圖。請

參考圖9，在硬體層面，該電子設備包括處理器，可選地還包括內部匯流排、網路介面、記憶體。其中，記憶體可能包含記憶體，例如高速隨機存取記憶體(Random-Access Memory，RAM)，也可能還包括非易失性記憶體(non-volatile memory)，例如至少1個磁碟記憶體等。當然，該電子設備還可能包括其他業務所需要的硬體。

處理器、網路介面和記憶體可以透過內部匯流排相互連接，該內部匯流排可以是ISA(Industry Standard Architecture，工業標準架構)匯流排、PCI(Peripheral Component Interconnect，週邊部件互連標準)匯流排或EISA(Extended Industry 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9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。記憶體可以包括記憶體和非易失性記憶體，並向處理器提供指令和資料。

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，在邏輯層面上形成基於區塊鏈的資源轉移裝置。處理器，執行記憶體所存放的程式，並具體用於執行以下操作：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據第一資源的第一數額，確定待轉移的第二資源的第二數額；第一資源與第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源；其中，交易請求中包括對第二資源的第二數額進行加密處理後得到的第一加密數額信息；

在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入區塊鏈。

上述如本案圖1所示實施例揭示的基於區塊鏈的資源轉移裝置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 Array，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案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規的處理器等。結合本案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。

該電子設備還可執行圖1中基於區塊鏈的資源轉移裝置執行的方法，並實現基於區塊鏈的資源轉移裝置在圖1所示實施例的功能，本案實施例在此不再贅述。

本案實施例還提出了一種電腦可讀儲存媒體，該電腦可讀儲存媒體儲存一個或多個程式，該一個或多個程式包括指令，該指令當被包括多個應用程式的電子設備執行時，能夠使該電子設備執行圖1所示實施例中基於區塊鏈的資源轉移裝置執行的方法，並具體用於執行：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據第一資源的第一數額，確定待轉移的第二資源的第二數額；第一資源與第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源；其中，交易請求中包括對第二資源的第二數額進行加密處理後得到的第一加密數額信息；

在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入

區塊鏈。

與圖2提供的基於區塊鏈的資金轉移方法相對應地，本案實施例還提供一種基於區塊鏈的資金轉移裝置，參見圖10所示，包括：

資金數額確定模組201，當滿足轉移條件時，確定待轉移的資金的第一數額；

代幣數額確定模組203，根據資金的第一數額，確定待轉移的代幣的第二數額；資金與代幣的類型不同；

交易請求發起模組205，轉出方向區塊鏈發起交易請求，用於向轉入方轉移待轉移的代幣；其中，交易請求中包括對代幣的第二數額進行加密處理後得到的第一加密數額信息；

入鏈模組207，在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的代幣轉移到轉入方，並將執行結果寫入區塊鏈。

圖11是本案的一個實施例電子設備的結構示意圖。請參考圖11，在硬體層面，該電子設備包括處理器，可選地還包括內部匯流排、網路介面、記憶體。其中，記憶體可能包含記憶體，例如高速隨機存取記憶體(Random-Access Memory，RAM)，也可能還包括非易失性記憶體(non-volatile memory)，例如至少1個磁碟記憶體等。當然，該電子設備還可能包括其他業務所需要的硬體。

處理器、網路介面和記憶體可以透過內部匯流排相互連接，該內部匯流排可以是ISA(Industry Standard

Architecture，工業標準架結構)匯流排、PCI(Peripheral Component Interconnect，週邊部件互連標準)匯流排或EISA(Extended Industry Standard Architecture，擴展工業標準架構)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11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。記憶體可以包括記憶體和非易失性記憶體，並向處理器提供指令和資料。

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，在邏輯層面上形成基於區塊鏈的資金轉移裝置。處理器，執行記憶體所存放的程式，並具體用於執行以下操作：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據資金的第一數額，確定待轉移的代幣的第二數額；資金與代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移待轉移的代幣；其中，交易請求中包括對代幣的第二數額進行加密處理後得到的第一加密數額信息；

在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的代幣轉移到轉入方，並將執行結果寫入區塊鏈。

上述如本案圖2所示實施例揭示的基於區塊鏈的資金轉移裝置執行的方法可以應用於處理器中，或者由處理器

實現。處理器可能是一種集成電路晶片，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 Array，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案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規的處理器等。結合本案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。

該電子設備還可執行圖2中基於區塊鏈的資金轉移裝置執行的方法，並實現基於區塊鏈的資金轉移裝置在圖2所示實施例的功能，本案實施例在此不再贅述。

本案實施例還提出了一種電腦可讀儲存媒體，該電腦可讀儲存媒體儲存一個或多個程式，該一個或多個程式包

括指令，該指令當被包括多個應用程式的電子設備執行時，能夠使該電子設備執行圖2所示實施例中基於區塊鏈的資金轉移裝置執行的方法，並具體用於執行：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據資金的第一數額，確定待轉移的代幣的第二數額；資金與代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移待轉移的代幣；其中，交易請求中包括對代幣的第二數額進行加密處理後得到的第一加密數額信息；

在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的代幣轉移到轉入方，並將執行結果寫入區塊鏈。

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代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、磁盒式磁帶，磁帶磁碟儲存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(transitory 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，本案的實施例可提供為方法、系統或電腦程式產品。因此，本案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，本案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，均應包含在本案的申請專利範圍之內。

【符號說明】

S101：步驟

S103：步驟

S105：步驟

S107：步驟

S201：步驟

S203：步驟

S205：步驟

S207：步驟

S301：步驟

S303：步驟

S305：步驟

S307：步驟

S401：步驟

S403：步驟

S405：步驟

S407：步驟

101：第一數額確定模組

103：第二數額確定模組

105：交易請求發起模組

107：入鏈模組

201：資金數額確定模組

203：代幣數額確定模組

205：交易請求發起模組

207：入鏈模組

【發明申請專利範圍】

【第1項】

一種基於區塊鏈的資源轉移方法，包括：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括對所述第二資源的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的第二資源轉移到所述資源轉入方，並將執行結果寫入所述區塊鏈，

其中根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額，包括：

根據所述第一資源的第一數額，採用單向函數確定所述第二資源的第二數額，及

將所述第一資源的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述第二資源的第二數額。

【第2項】

根據申請專利範圍第1項所述方法，其中所述交易請

求中包括的所述第一加密數額信息，透過採用第一加密函數對所述第二資源的第二數額進行加密處理得到；

其中，所述第一加密函數的一個輸入為所述第二資源的第二數額，另一個輸入為所述資源轉入方的公鑰。

【第3項】

根據申請專利範圍第2項所述方法，其中所述交易請求中還包括所述資源轉入方的公鑰的標識信息。

【第4項】

根據申請專利範圍第3項所述方法，其中所述資源轉入方的公鑰的標識信息為所述資源轉入方的公鑰的雜湊值。

【第5項】

根據申請專利範圍第1項所述方法，其中所述資源轉出方向區塊鏈發起的所述交易請求中，還包括加密後的所述隨機數。

【第6項】

根據申請專利範圍第1~5項之任一項所述方法，其中所述資源轉移條件包括允許所述資源轉入方借取所述第一資源；則確定待轉移的第一資源的第一數額，包括：

將允許所述資源轉入方借取的第一資源的額度，作為所述待轉移的第一資源的第一數額。

【第7項】

根據申請專利範圍第1~5項之任一項所述方法，其中所述資源轉移條件包括所述資源轉出方已接收到所述資源

轉入方歸還的第一資源；則確定待轉移的第一資源的第一數額，包括：

將所述歸還的第一資源的數額，確定為所述待轉移的第一資源的第一數額。

【第8項】

根據申請專利範圍第1~5項之任一項所述方法，其中所述資源轉移條件包括所述資源轉入方與所述資源轉出方已達成資源借取協議，所述資源借取協議中包含所述資源轉出方向所述資源轉入方申請借取的第一資源的數額；則確定待轉移的第一資源的第一數額，包括：

將所述申請借取的第一資源的數額，確定為所述待轉移的第一資源的第一數額。

【第9項】

根據申請專利範圍第8項所述方法，其中所述交易請求中還包括零知識證明，用於證明執行所述交易請求之後所述資源轉出方將要持有的第二資源的餘額與所述第二數額的和，等於所述資源轉出方在發起所述交易請求前所持有的第二資源的數額。

【第10項】

根據申請專利範圍第9項所述方法，其中所述零知識證明還用於證明所述第二數額大於零，所述資源轉出方在發起所述交易請求前所持有的第二資源的數額大於零，並且，執行所述交易請求之後所述資源轉出方將要持有的第二資源的餘額不小於零。

【第11項】

根據申請專利範圍第8項所述方法，其中所述交易請求中還包括所述資源轉出方參與的上一次資源轉移交易的標識信息。

【第12項】

根據申請專利範圍第11項所述方法，其中所述資源轉出方參與的上一次資源轉移交易的標識信息，具體為所述區塊鏈中記錄的、所述上一次資源轉移交易的雜湊值。

【第13項】

根據申請專利範圍第8項所述方法，其中所述交易請求中還包括對執行所述交易請求之後所述資源轉出方將要持有的第二資源的餘額進行加密處理後得到的第二加密數額信息。

【第14項】

根據申請專利範圍第13項所述方法，其中所述交易請求中包括的所述第二加密數額信息，透過採用第二加密函數對執行所述交易請求之後所述資源轉出方將要持有的第二資源的餘額進行加密處理得到；

其中，所述第二加密函數的一個輸入為所述第二資源的餘額，另一個輸入為所述資源轉出方的公鑰。

【第15項】

根據申請專利範圍第14項所述方法，其中所述交易請求中還包括所述資源轉出方的公鑰的標識信息。

【第16項】

根據申請專利範圍第15項所述方法，其中所述資源轉出方的公鑰的標識信息為所述資源轉出方的公鑰的雜湊值。

【第17項】

根據申請專利範圍第1~5項之任一項所述方法，其中所述第一資源具體為資金，所述第二資源具體為代幣。

【第18項】

一種基於區塊鏈的資金轉移方法，包括：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據所述資金的第一數額，確定待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括對所述代幣的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈，

其中根據所述資金的第一數額，確定待轉移的代幣的第二數額，包括：

根據所述資金的第一數額，採用單向函數確定所述代幣的第二數額，及

將所述資金的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述代幣的第二數額。

【第19項】

一種基於區塊鏈的資源轉移裝置，包括：

第一數額確定模組，當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

第二數額確定模組，根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同，其中根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額，包括：根據所述第一資源的第一數額，採用單向函數確定所述第二資源的第二數額，及將所述第一資源的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述第二資源的第二數額；

交易請求發起模組，資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括對所述第二資源的第二數額進行加密處理後得到的第一加密數額信息；

入鏈模組，在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的第二資源轉移到所述資源轉入方，並將執行結果寫入所述區塊鏈。

【第20項】

一種基於區塊鏈的資源轉移的電子設備，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：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括對所述第二資源的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的第二資源轉移到所述資源轉入方，並將執行結果寫入所述區塊鏈，

其中根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額，包括：

根據所述第一資源的第一數額，採用單向函數確定所述第二資源的第二數額，及

將所述第一資源的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述第二資源的第二數額。

【第21項】

一種基於區塊鏈的資源轉移的電腦可讀儲存媒體，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包括指令，所述指令當被包括多個應用程式的電子設備執行時，能夠使所述電子設備執行以下操作：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括對所述第二資源的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的第二資源轉移到所述資源轉入方，並將執行結果寫入所述區塊鏈，

其中根據所述第一資源的第一數額，確定待轉移的第二資源的第二數額，包括：

根據所述第一資源的第一數額，採用單向函數確定所述第二資源的第二數額，及

將所述第一資源的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述第二資源的第二數額。

【第22項】

一種基於區塊鏈的資金轉移裝置，包括：

資金數額確定模組，當滿足轉移條件時，確定待轉移的資金的第一數額；

代幣數額確定模組，根據所述資金的第一數額，確定

待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

交易請求發起模組，轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括對所述代幣的第二數額進行加密處理後得到的第一加密數額信息；

入鏈模組，在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈，

其中根據所述資金的第一數額，確定待轉移的代幣的第二數額，包括：

根據所述資金的第一數額，採用單向函數確定所述代幣的第二數額，及

將所述資金的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述代幣的第二數額。

【第23項】

一種基於區塊鏈的資金轉移的電子設備，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：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據所述資金的第一數額，確定待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括對所述代幣的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈，

其中根據所述資金的第一數額，確定待轉移的代幣的第二數額，包括：

根據所述資金的第一數額，採用單向函數確定所述代幣的第二數額，及

將所述資金的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述代幣的第二數額。

【第24項】

一種基於區塊鏈的資金轉移的電腦可讀儲存媒體，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包括指令，所述指令當被包括多個應用程式的電子設備執行時，能夠使所述電子設備執行以下操作：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據所述資金的第一數額，確定待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括對所述代幣的第二數額進行加密處理後得到的第一加密數額信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈，

其中根據所述資金的第一數額，確定待轉移的代幣的第二數額，包括：

根據所述資金的第一數額，採用單向函數確定所述代幣的第二數額，及

將所述資金的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述代幣的第二數額。

【第25項】

一種基於區塊鏈的資源轉移方法，包括：

當滿足資源轉移條件時，確定待轉移的第一資源的第一數額；

根據所述第一資源的第一數額，採用單向函數確定待轉移的第二資源的第二數額；所述第一資源與所述第二資源的類型不同；

資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移所述待轉移的第二資源；其中，所述交易請求中包括與所述第二資源的第二數額相對應的信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的第二資源轉移到所述資源轉入方，並將執行結果寫入所述區塊鏈，

其中根據所述第一資源的第一數額，採用單向函數確

定待轉移的第二資源的第二數額，包括：

將所述第一資源的第一數額和一隨機數作為所述單向函數的輸入，將所述單向函數的輸出確定為所述第二資源的第二數額。

【第26項】

根據申請專利範圍第25項所述方法，其中所述資源轉出方向區塊鏈發起的所述交易請求中，還包括加密後的所述隨機數。

【第27項】

根據申請專利範圍第25或26項所述方法，其中所述第一資源具體為資金，所述第二資源具體為代幣。

【第28項】

一種基於區塊鏈的資金轉移方法，包括：

當滿足轉移條件時，確定待轉移的資金的第一數額；

根據所述資金的第一數額，採用單向函數確定待轉移的代幣的第二數額；所述資金與所述代幣的類型不同；

轉出方向區塊鏈發起交易請求，用於向轉入方轉移所述待轉移的代幣；其中，所述交易請求中包括與所述代幣的第二數額相對應的信息；

在所述區塊鏈對所述交易請求進行驗證後，執行所述交易請求，將所述待轉移的代幣轉移到所述轉入方，並將執行結果寫入所述區塊鏈，

其中採用單向函數確定所述代幣的第二數額，包括：

將所述資金的第一數額和一隨機數作為所述單向函數

的輸入，將所述單向函數的輸出確定為所述代幣的第二數額。

【發明圖式】

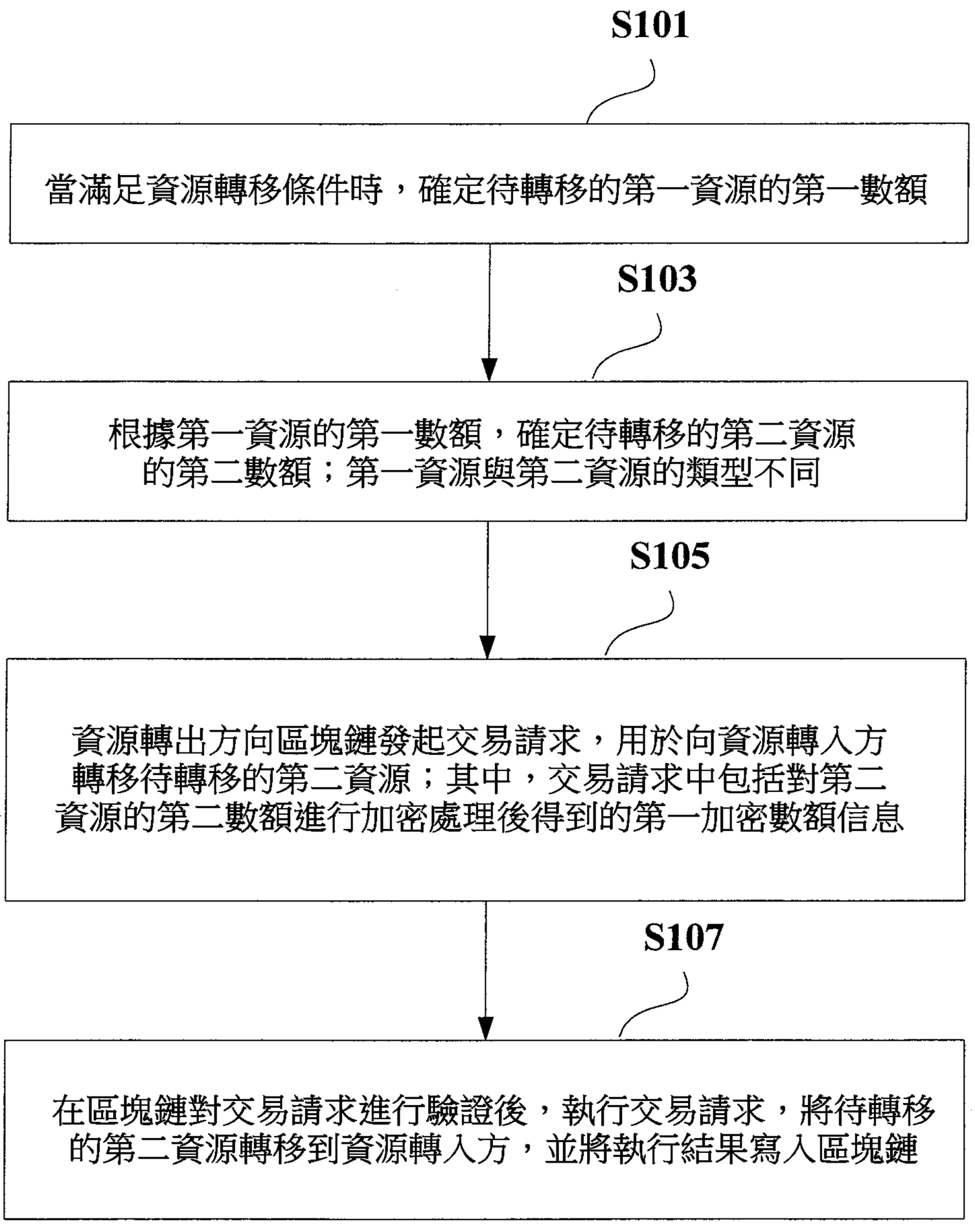
S101
當滿足資源轉移條件時，確定待轉移的第一資源的第一數額
S103
根據第一資源的第一數額，確定待轉移的第二資源的第二數額；第一資源與第二資源的類型不同
S105
資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源；其中，交易請求中包括對第二資源的第二數額進行加密處理後得到的第一加密數額信息
S107
在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入區塊鏈

圖 1

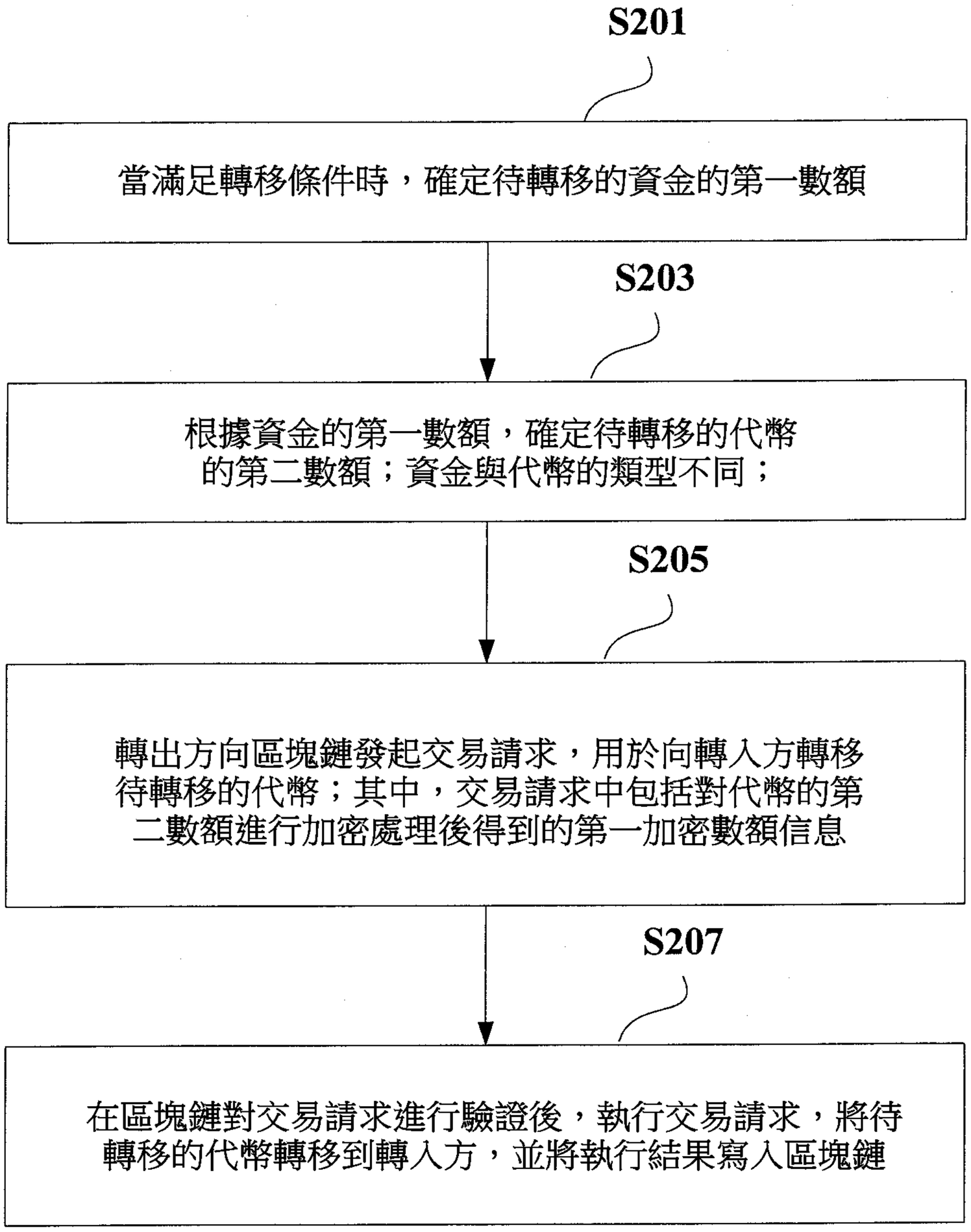
S201
當滿足轉移條件時，確定待轉移的資金的第一數額
S203
根據資金的第一數額，確定待轉移的代幣的第二數額；資金與代幣的類型不同；
S205
轉出方向區塊鏈發起交易請求，用於向轉入方轉移待轉移的代幣；其中，交易請求中包括對代幣的第二數額進行加密處理後得到的第一加密數額信息
S207
在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的代幣轉移到轉入方，並將執行結果寫入區塊鏈

圖 2

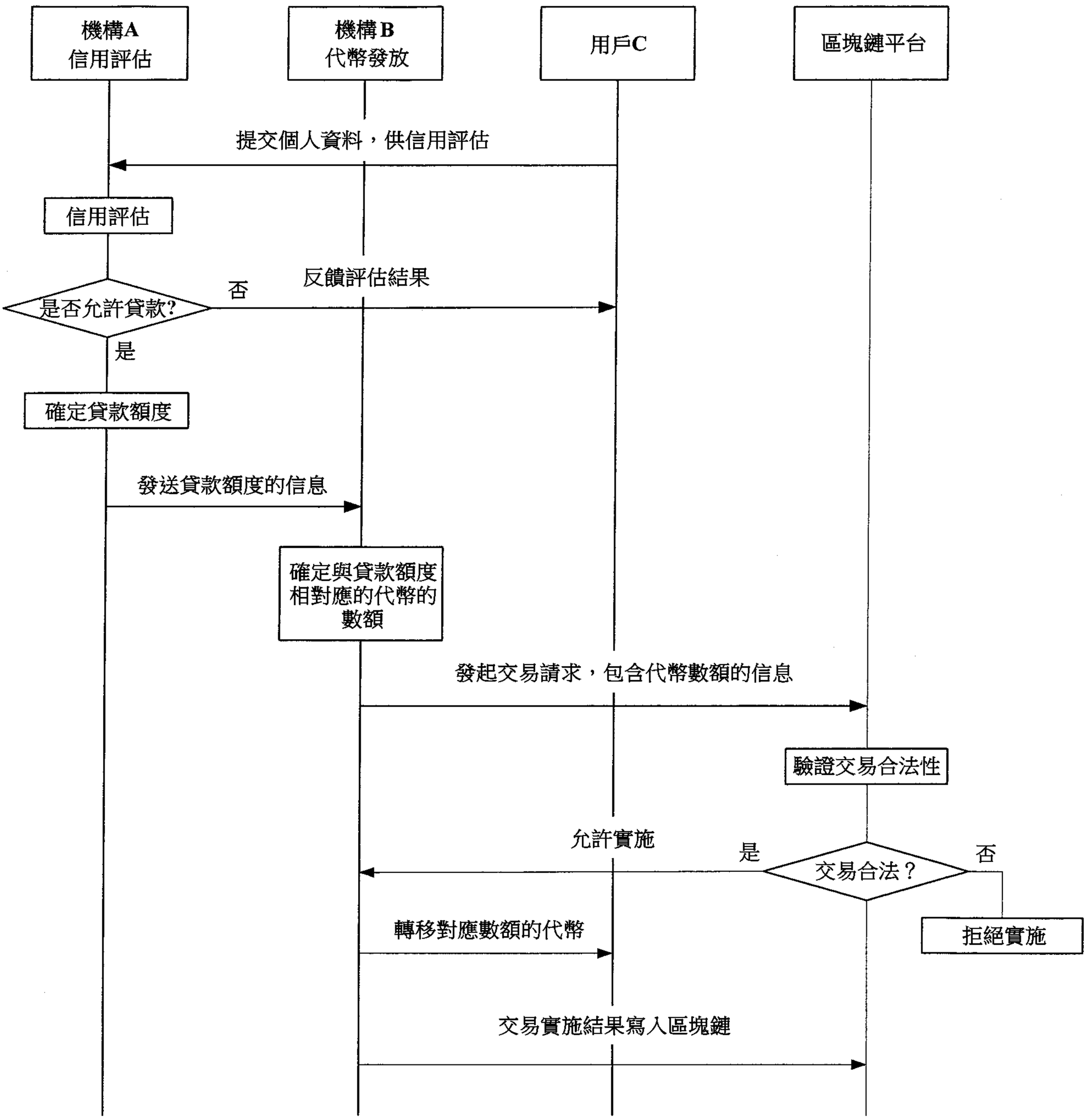
機構A
信用評估
機構B
代幣發放
用戶C
區塊鏈平台
提交個人資料，供信用評估
信用評估
反饋評估結果
是否允許貸款?
否
是
確定貸款額度
發送貸款額度的信息
確定與貸款額度相對應的代幣的數額
發起交易請求，包含代幣數額的信息
驗證交易合法性
允許實施
是
交易合法？
否
拒絕實施
轉移對應數額的代幣
交易實施結果寫入區塊鏈

圖 3

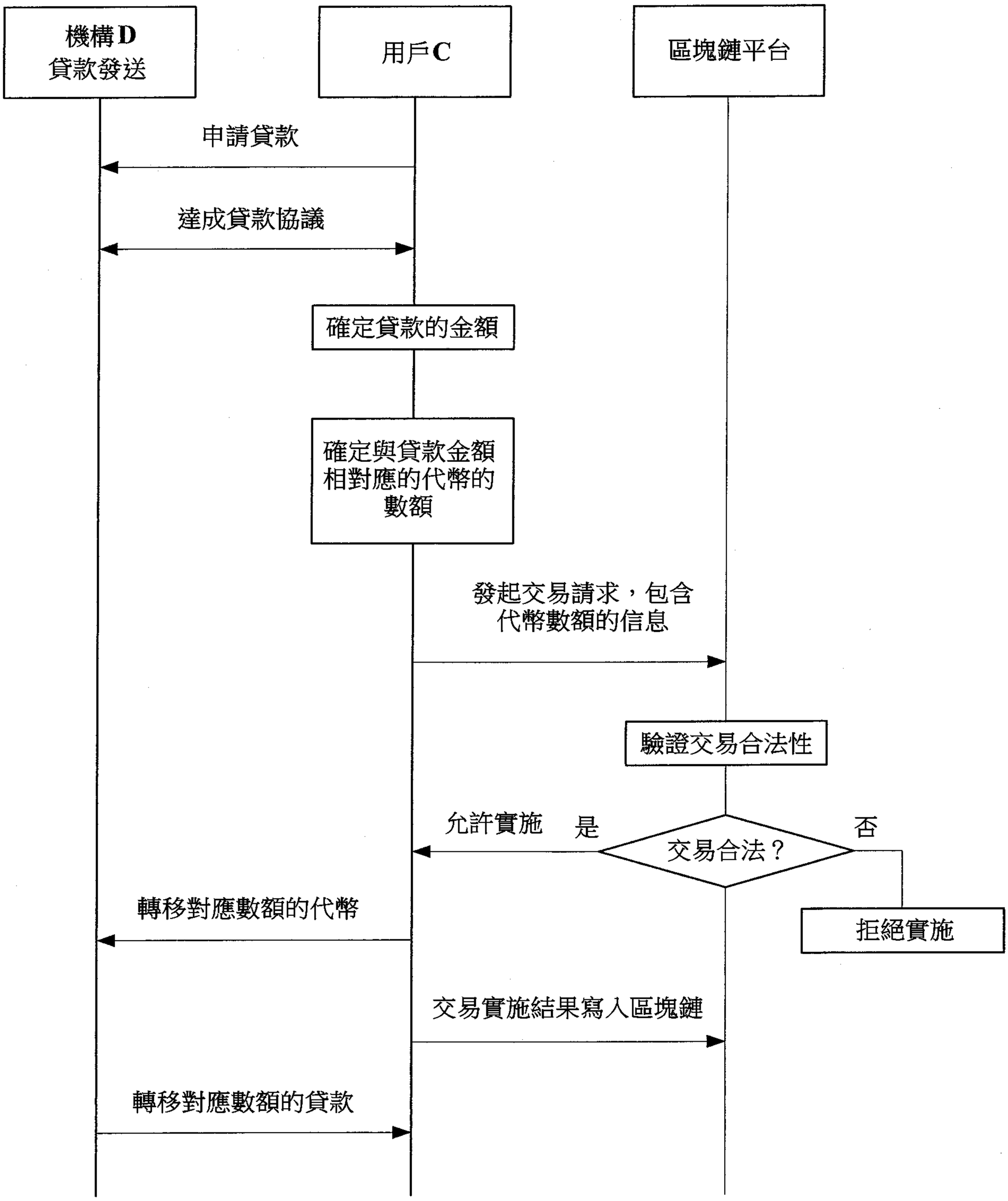
機構D
貸款發送
用戶C
區塊鏈平台
申請貸款
達成貸款協議
確定貸款的金額
確定與貸款金額相對應的代幣的數額
發起交易請求，包含代幣數額的信息
驗證交易合法性
允許實施
是
交易合法？
否
拒絕實施
轉移對應數額的代幣
交易實施結果寫入區塊鏈
轉移對應數額的貸款

圖 4

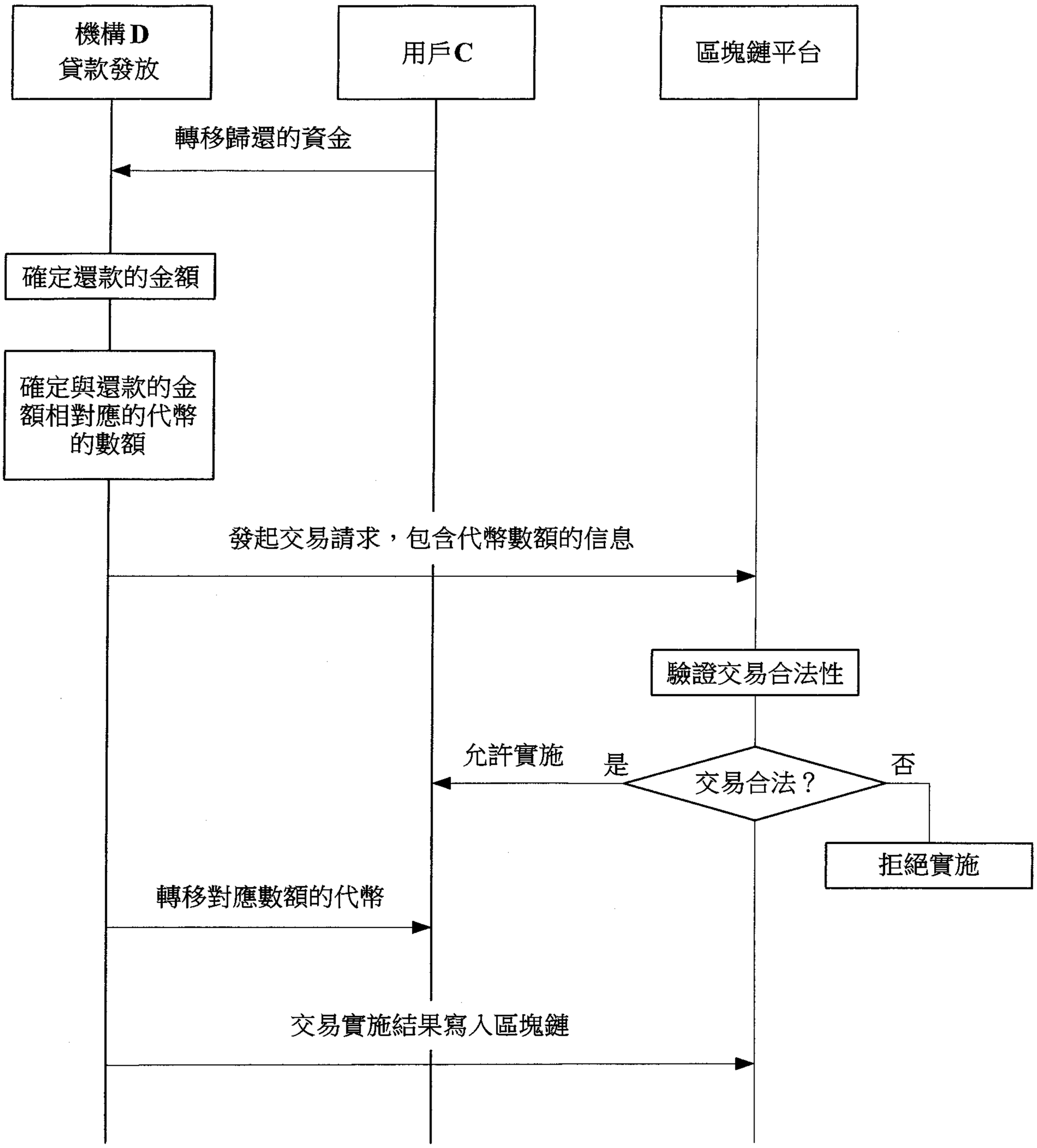
機構D
貸款發放
用戶C
區塊鏈平台
轉移歸還的資金
確定還款的金額
確定與還款的金額相對應的代幣的數額
發起交易請求，包含代幣數額的信息
驗證交易合法性
允許實施
是
交易合法？
否
拒絕實施
轉移對應數額的代幣
交易實施結果寫入區塊鏈

圖 5

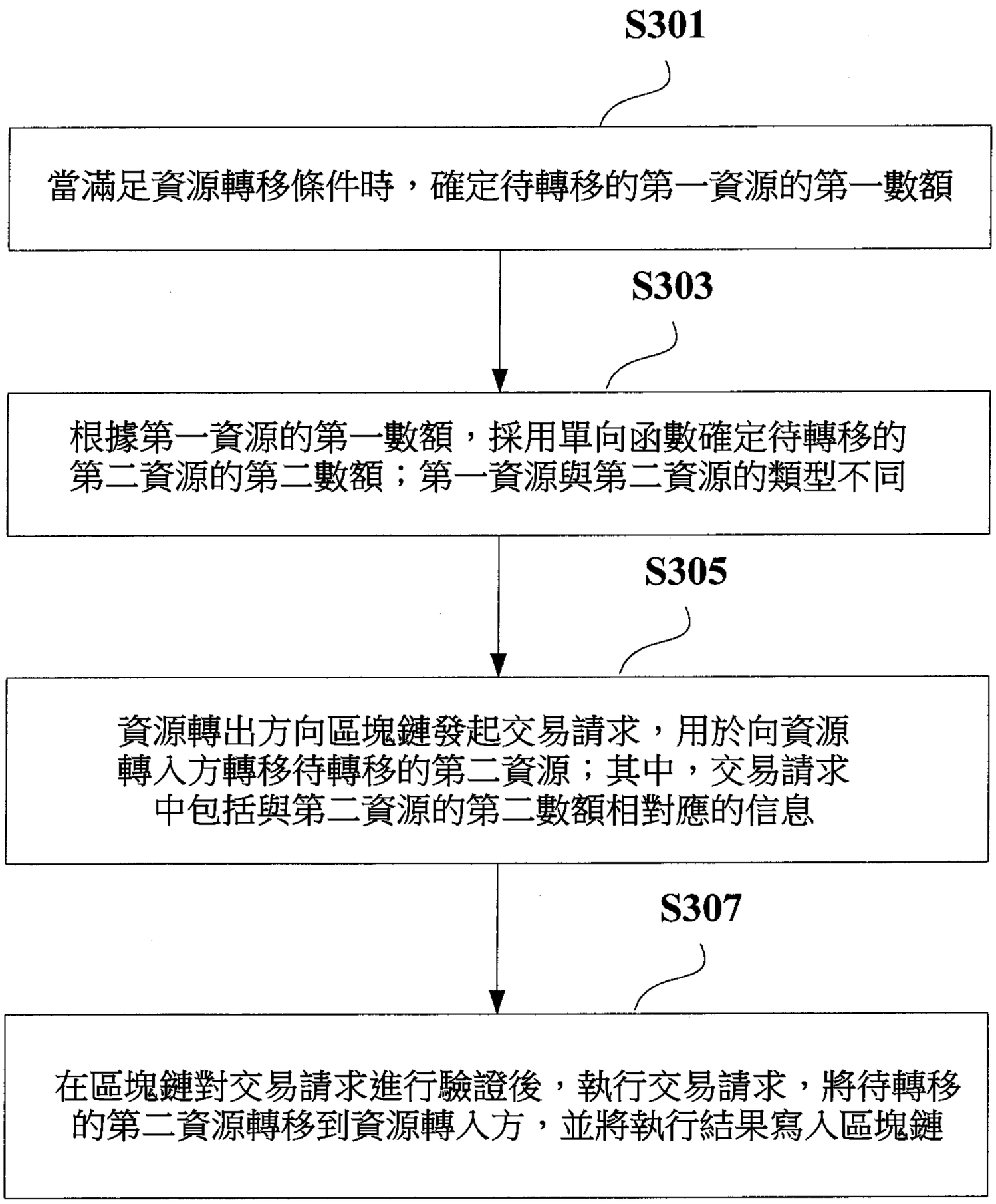
S301
當滿足資源轉移條件時，確定待轉移的第一資源的第一數額
S303
根據第一資源的第一數額，採用單向函數確定待轉移的第二資源的第二數額；第一資源與第二資源的類型不同
S305
資源轉出方向區塊鏈發起交易請求，用於向資源轉入方轉移待轉移的第二資源；其中，交易請求中包括與第二資源的第二數額相對應的信息
S307
在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的第二資源轉移到資源轉入方，並將執行結果寫入區塊鏈

圖 6

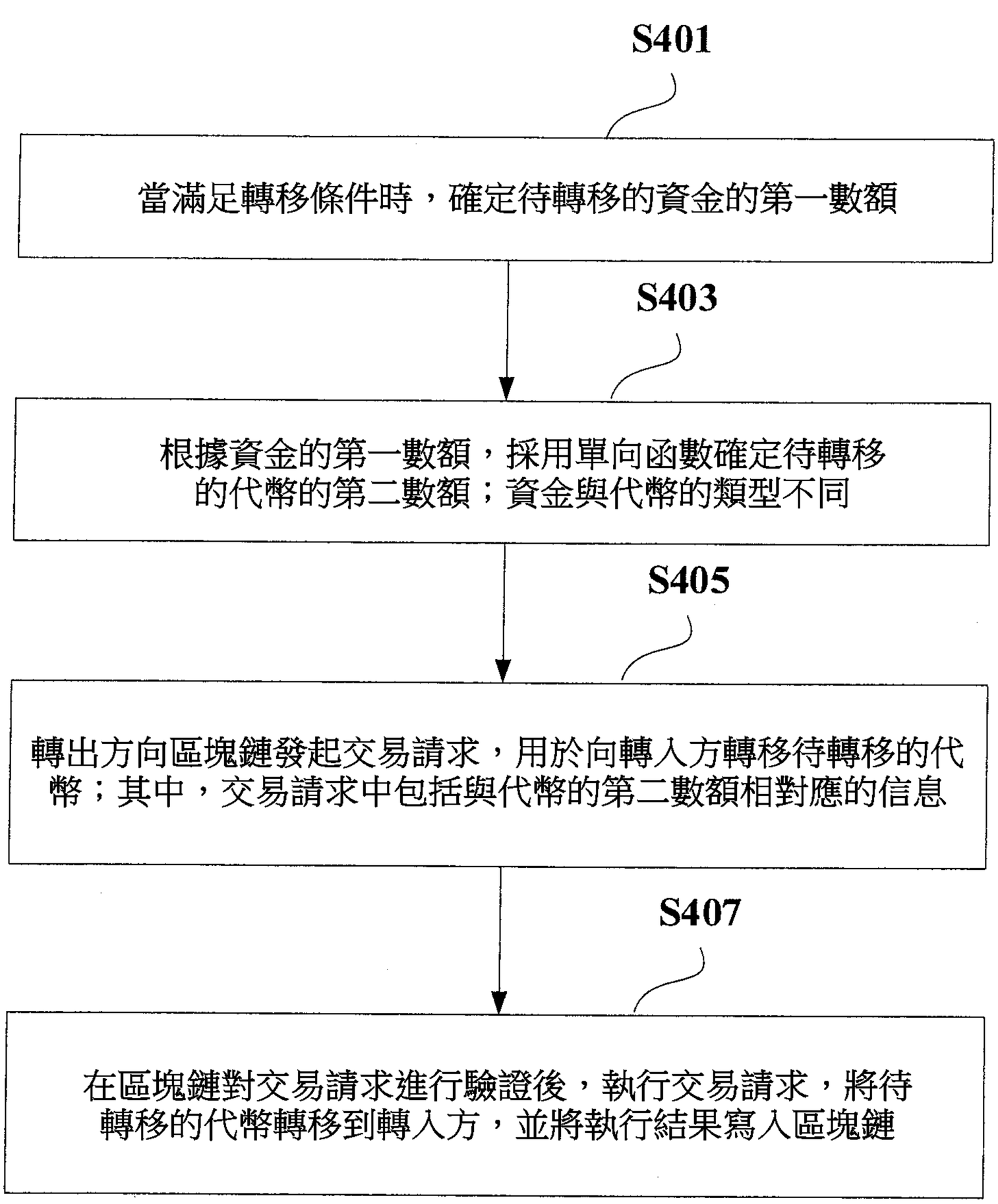
S401
當滿足轉移條件時，確定待轉移的資金的第一數額
S403
根據資金的第一數額，採用單向函數確定待轉移的代幣的第二數額；資金與代幣的類型不同
S405
轉出方向區塊鏈發起交易請求，用於向轉入方轉移待轉移的代幣；其中，交易請求中包括與代幣的第二數額相對應的信息
S407
在區塊鏈對交易請求進行驗證後，執行交易請求，將待轉移的代幣轉移到轉入方，並將執行結果寫入區塊鏈

圖 7

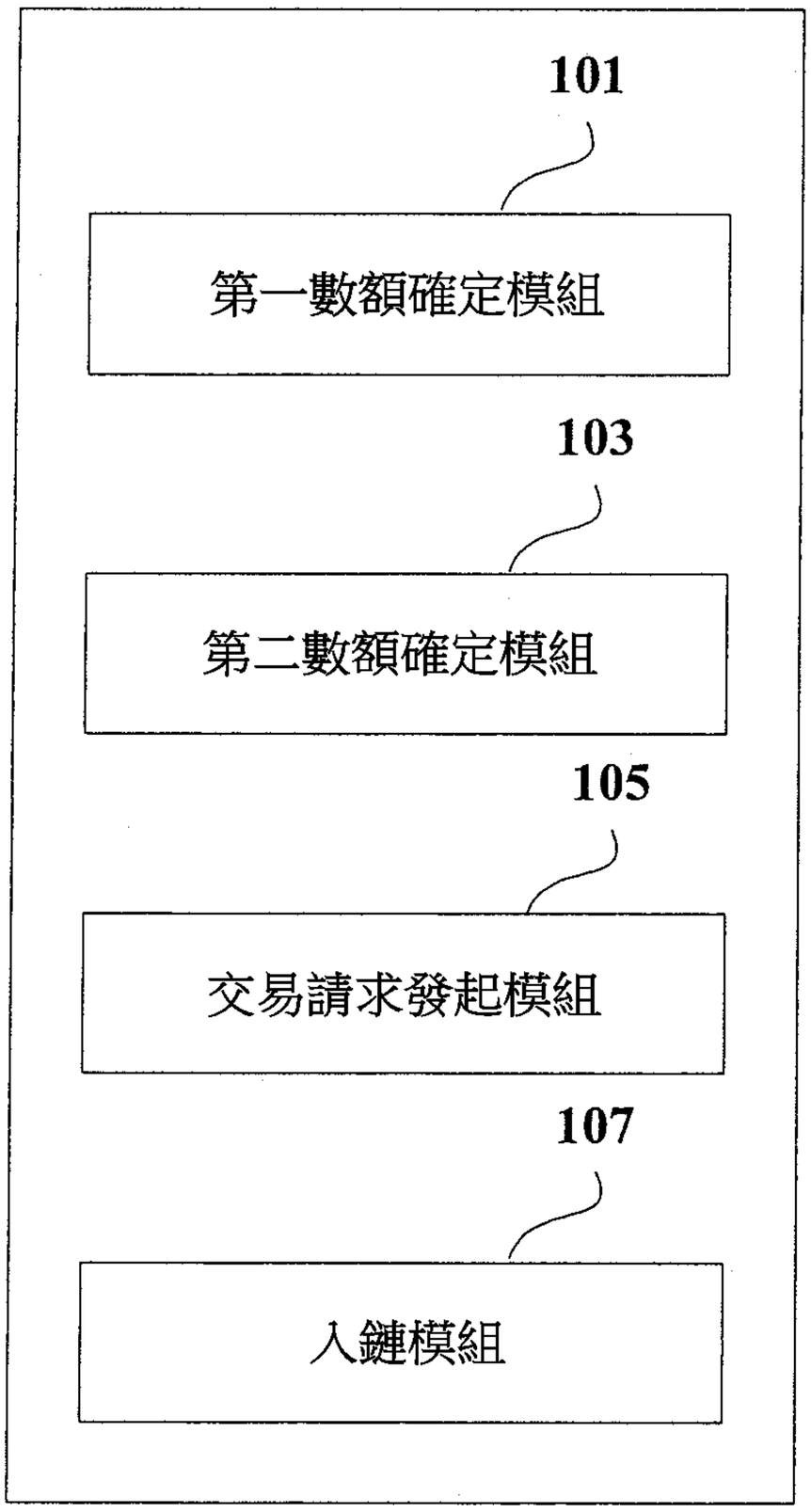
101
第一數額確定模組
103
第二數額確定模組
105
交易請求發起模組
107
入鏈模組

圖 8

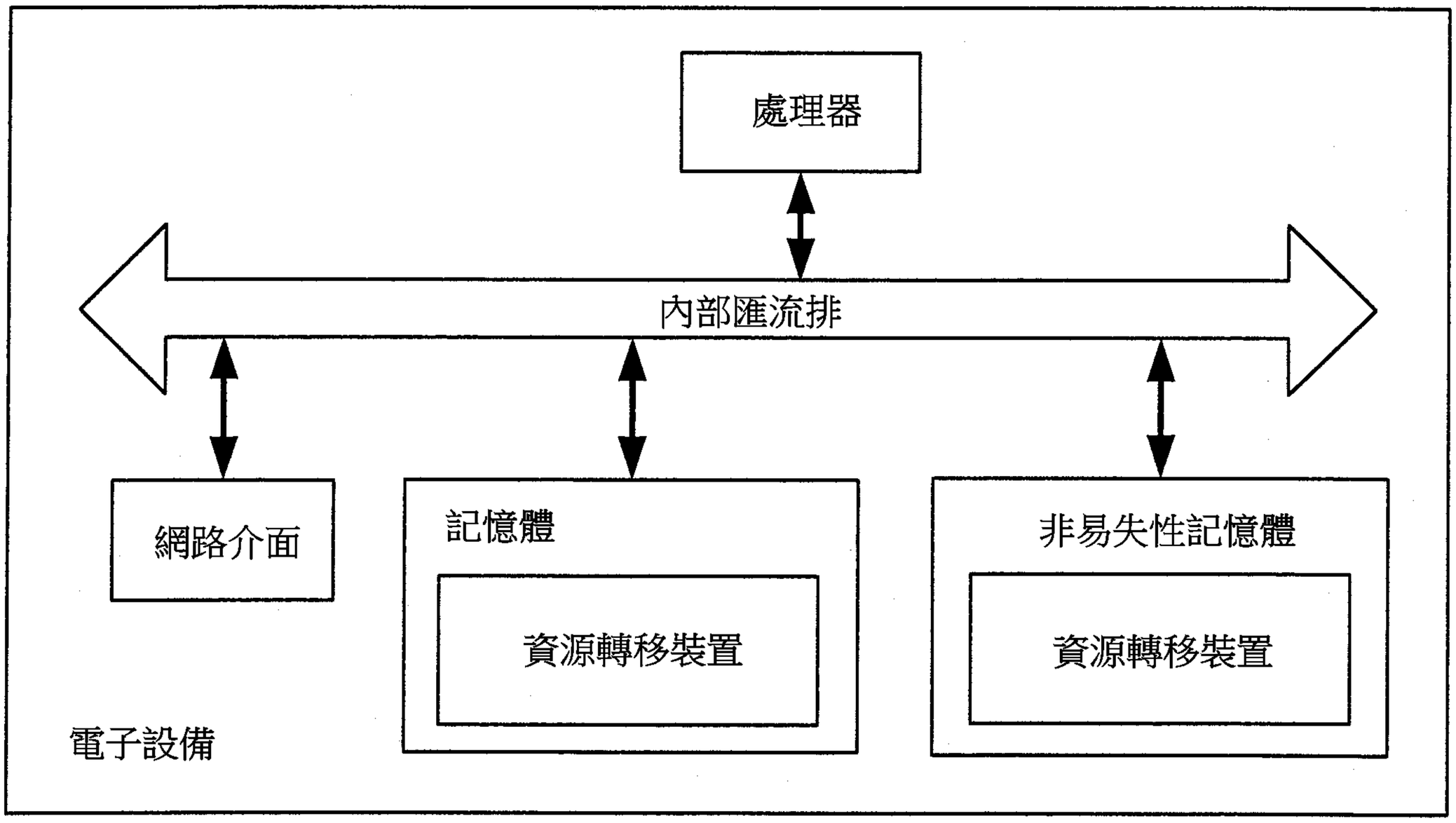
處理器
內部匯流排
網路介面
記憶體
資源轉移裝置
非易失性記憶體
資源轉移裝置
電子設備

圖 9

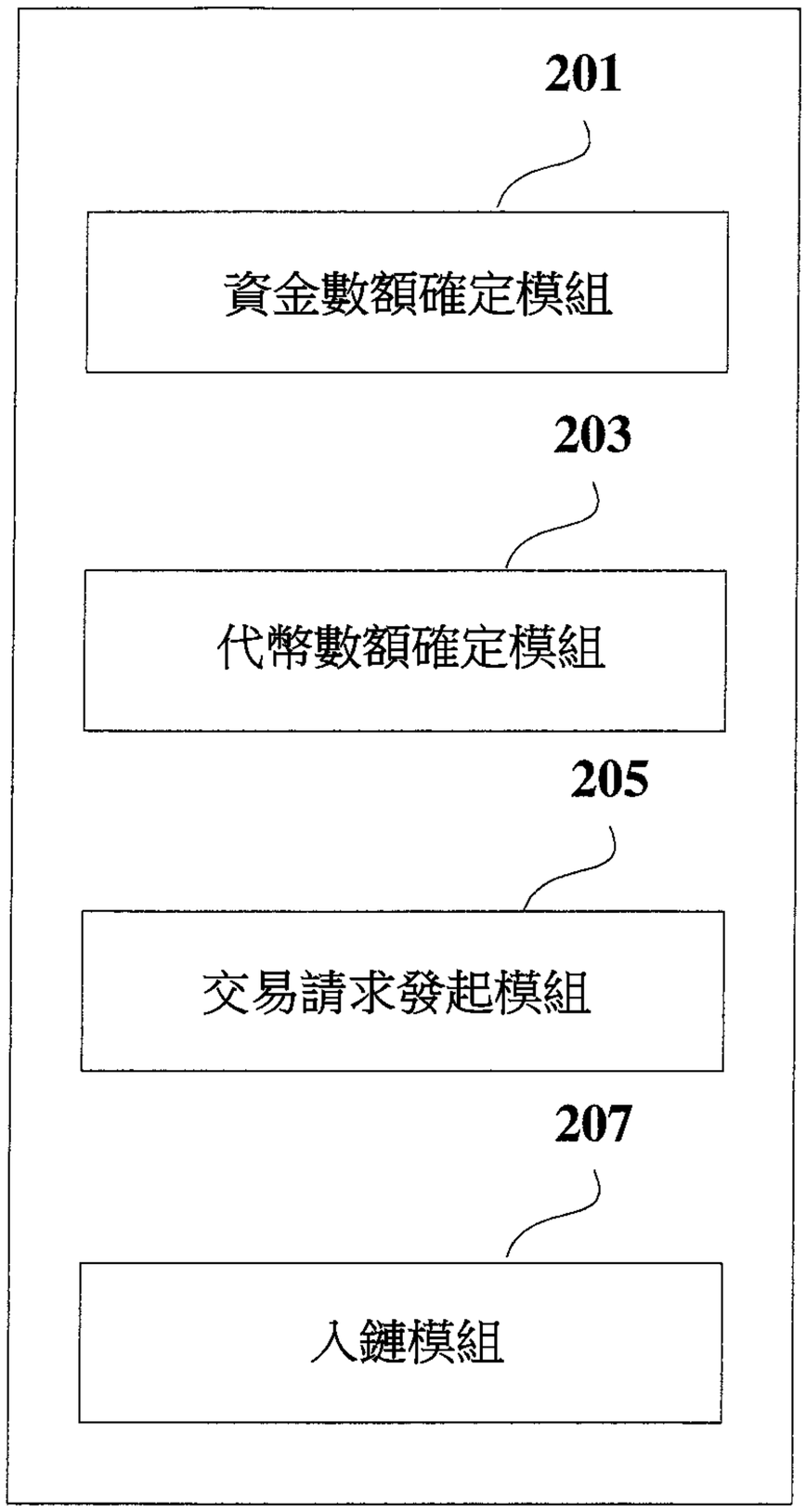
201
資金數額確定模組
203
代幣數額確定模組
205
交易請求發起模組
207
入鏈模組

圖 10

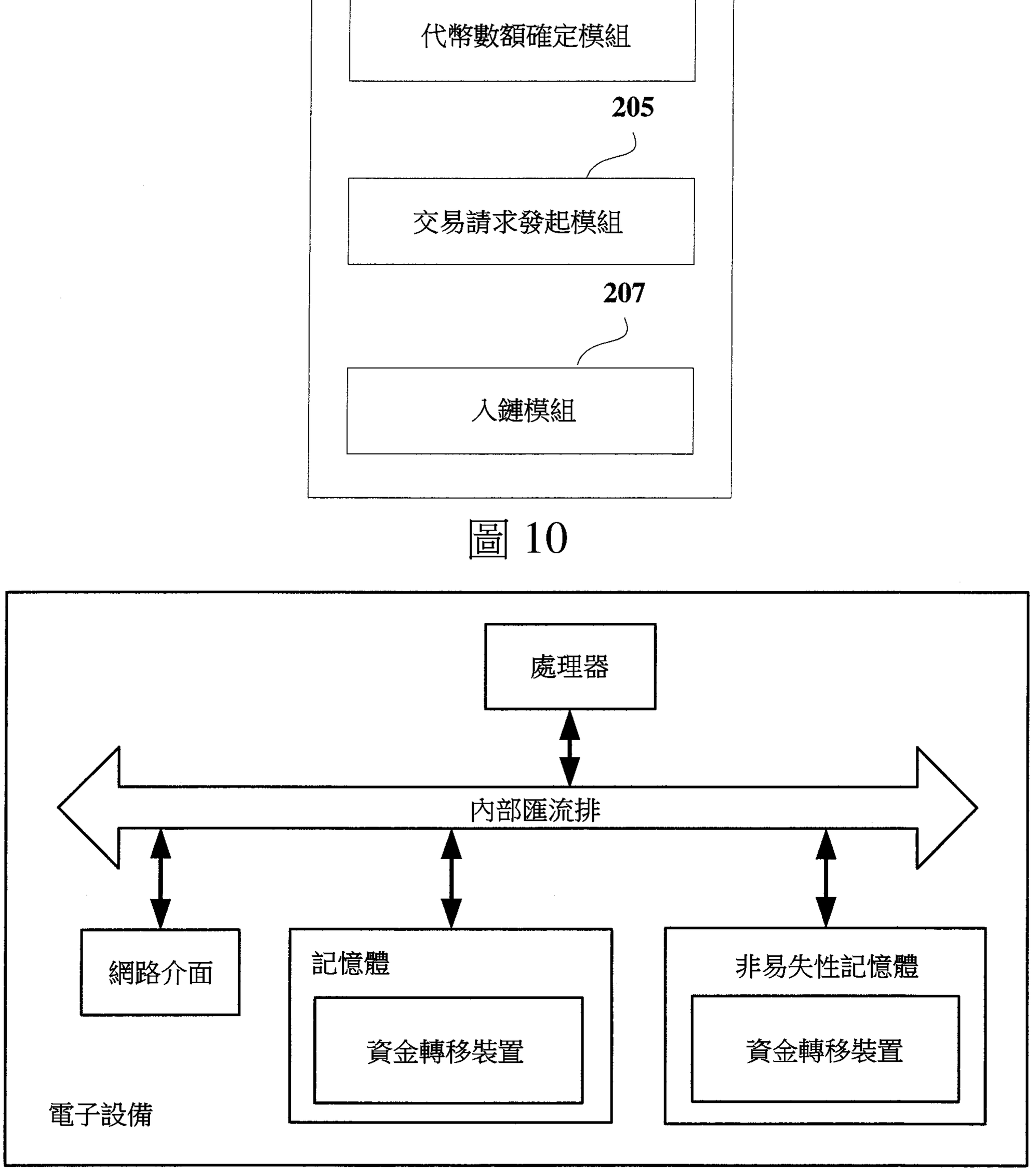
處理器
內部匯流排
網路介面
記憶體
資金轉移裝置
非易失性記憶體
資金轉移裝置
電子設備

圖 11