I718585

(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 I718585 B**

(45)公告日： 中華民國 110 (2021) 年 02 月 11 日

(21)申請案號：108124843　(22)申請日： 中華民國 108 (2019) 年 07 月 15 日

(51)Int. Cl.：　*H04L9/32　(2006.01)*　*H04L9/30　(2006.01)*

G06Q20/38　(2012.01)

(30)優先權：2018/11/07　世界智慧財產權組織　PCT/CN2018/114421

(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：張文彬 (CN) ；馬寶利 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW　201638798A　US　8861716B2

US　8958552B2　US　2010/0142704A1

WO　2018/115567A1

Bruno F França,"Homomorphic Mini-blockchain Scheme",公開日：2015/04/24；[https://pdfs.semanticscholar.org/ab9f/b027061fb4aa8ed8017d63002f586a18eab6.pdf]

審查人員：周官緯

申請專利範圍項數：10 項　圖式數：8　共 44 頁

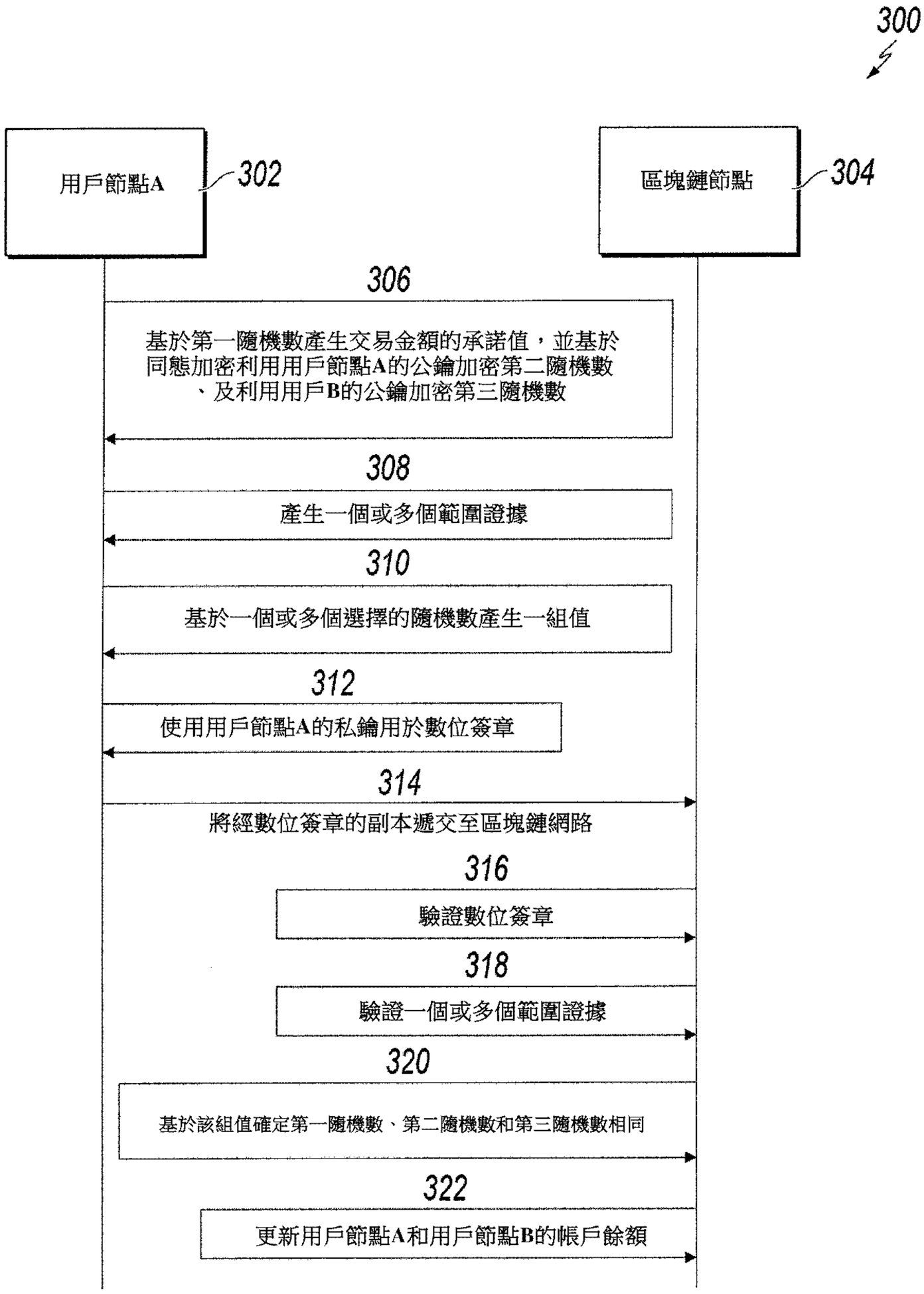
(54)名稱

使用同態加密的區塊鏈資料保護

(57)摘要

本公開的實施方式包括由共識節點從第一帳戶接收交易金額的承諾值的經數位簽章的副本、利用所述第一帳戶的公鑰加密的第二隨機數、利用第二帳戶的公鑰加密的第三隨機數、一個或多個範圍證據、和基於一個或多個選擇的隨機數產生的一組值。然後，共識節點利用所述第一帳戶的公鑰驗證對應於所述經數位簽章的副本的數位簽章，所述第一帳戶的公鑰與用於產生所述數位簽章的私鑰對應。若所述第一隨機數、所述第二隨機數和所述第三隨機數相同，所述共識節點還基於餘額轉帳金額更新所述第一帳戶的餘額和所述第二帳戶的餘額。

指定代表圖：



【圖 3】

符號簡單說明：

300:方法

302:用戶節點 A

304:區塊鏈節點

專利案號：108124843

I718585

公告本

【發明摘要】

【中文發明名稱】

使用同態加密的區塊鏈資料保護

【中文】

本公開的實施方式包括由共識節點從第一帳戶接收交易金額的承諾值的經數位簽章的副本、利用所述第一帳戶的公鑰加密的第二隨機數、利用第二帳戶的公鑰加密的第三隨機數、一個或多個範圍證據、和基於一個或多個選擇的隨機數產生的一組值。然後，共識節點利用所述第一帳戶的公鑰驗證對應於所述經數位簽章的副本的數位簽章，所述第一帳戶的公鑰與用於產生所述數位簽章的私鑰對應。若所述第一隨機數、所述第二隨機數和所述第三隨機數相同，所述共識節點還基於餘額轉帳金額更新所述第一帳戶的餘額和所述第二帳戶的餘額。

【指定代表圖】第(3)圖。

【代表圖之符號簡單說明】

300：方法

302：用戶節點A

304：區塊鏈節點

【特徵化學式】無

【發明說明書】

【中文發明名稱】

使用同態加密的區塊鏈資料保護

【技術領域】

本公開係關於使用同態加密的區塊鏈資料保護。

【先前技術】

區塊鏈網路，還可被稱為區塊鏈系統、共識網路、分散式帳本系統網路或區塊鏈，使得參與的實體能夠安全地且不可篡改地儲存資料。區塊鏈可被描述為交易的帳本系統，且帳本的多個副本被儲存於區塊鏈網路中。區塊鏈的示例類型可以包括公有區塊鏈、許可區塊鏈和私有區塊鏈。公有區塊鏈對所有實體開放使用區塊鏈，並開放參與共識過程。許可區塊鏈類似於公有區塊鏈但僅對有加入許可的實體開放。為特定實體提供私有區塊鏈，該實體集中控制讀寫權限。

區塊鏈用於加密貨幣網路，加密貨幣網路使得參與者可以使用加密貨幣進行交易以買/賣物品和/或服務。通用加密貨幣包括比特幣(Bitcoin)。在加密貨幣網路中，記帳模型用於記錄用戶之間的交易。示例記帳模型包括未被花費交易輸出(UTXO)模型和帳戶餘額模型。在UTXO模型中，每個交易花費來自先前交易的輸出並產生可以在隨後交易中被花費的新輸出。追蹤用戶的未被花費的交易，且

計算用戶的所有未被花費的交易的和作為該用戶擁有的餘額。在帳戶餘額模型中，追蹤每個用戶的帳戶餘額作為全域狀態。對於每個交易，檢查花費的帳戶的餘額以確保餘額大於或等於交易金額。這可以與傳統銀行業務對比。

區塊鏈帳本包括一系列區塊，每個區塊包含一個或多個在網路中執行的交易。每個區塊可以被類比為帳本中的一頁，而區塊鏈本身就是帳本的完整副本。各個交易被確認並被添加至區塊，該區塊被添加至區塊鏈。區塊鏈帳本的副本遍佈網路中的節點複製。以這種方式，對區塊鏈的狀態形成了全域共識。此外，至少在公有網路的情況下，區塊鏈對所有節點開放查看。為保護區塊鏈用戶的隱私可實施加密技術。

在帳戶餘額模型下，可以使用承諾方案以隱藏交易雙方當事人承諾的值。可以根據當事人對選擇或值的承諾的需求產生承諾方案，並隨後可以將該值傳達給所涉及的其他當事人。例如，在交互佩德森承諾(Pedersen Commitment，PC)中，當事人A可以透過發送基於隨機值r產生的承諾值PC(t, r)來承諾交易金額t。承諾值被產生，並且當事人B只能透過獲取隨機數r顯露交易金額t。

【發明內容】

本公開的實施方式包括用於在無需用戶確認、交互及顯露交易金額或帳戶餘額的情況下，對區塊鏈交易進行隱私保護驗證的電腦實施方法。更具體地，本公開的實施方

式涉及基於承諾方案和同態加密驗證區塊鏈用戶之間的交易，而不將交易金額、帳戶餘額或用於產生承諾的隨機數顯露給其他區塊鏈節點。

在一些實施方式中，操作包括：從第一帳戶接收要從所述第一帳戶轉帳至第二帳戶的交易金額的基於第一隨機數產生的承諾值的經數位簽章的副本、利用所述第一帳戶的公鑰加密的第二隨機數、利用所述第二帳戶的公鑰加密的第三隨機數、一個或多個範圍證據、和基於一個或多個選擇的隨機數產生的一組值；利用所述第一帳戶的公鑰，驗證對應於所述經數位簽章的副本的數位簽章，其中所述第一帳戶的公鑰與用於產生所述數位簽章的私鑰對應；確定所述一個或多個範圍證據證實所述交易金額大於零、且小於或等於所述第一帳戶的餘額；基於所述一組值確定所述第一隨機數、所述第二隨機數和所述第三隨機數是否相同；以及若所述第一隨機數、所述第二隨機數和所述第三隨機數相同，則基於所述交易金額更新所述第一帳戶的餘額和所述第二帳戶的餘額。其他實施方式包括對應的系統、裝置和電腦程式，所述電腦程式被配置為執行所述方法的操作，並編碼在電腦存放裝置上。

這些和其他實施方式可以各自可選地包括以下特徵中的一個或多個：利用同態承諾方案產生所述承諾值；所述承諾方案為佩德森承諾(Pedersen commitment)方案；基於確定性同態加密HE方案對所述第二隨機數和所述第三隨機數加密，所述HE方案具有線性特徵$\mathrm{HE}(a+b)=\mathrm{HE}(a)*$

HE(b)和HE(ab)=HE(b)^a，其中a和b是用於HE的明文；其中，由$r1$和$t1$表示所述選擇的隨機數，且所述選擇的隨機數用於產生$r2$和$t2$，$r2=r1+xr$、$t2=t1+xt$，$r1$和$t1$表示所述一個或多個選擇的隨機數，r是所述第一隨機數，t是所述交易金額，x是雜湊值；還基於T1、T1'和T1"產生所述一組值，其中T1=$g^{r1}h^{t1}$、T1'=HE_A($r1$)、T1"=HE_B($r1$)，g和h為橢圓曲線的生成數，HE_A($r1$)是基於利用所述第一帳戶的公鑰對$r1$進行HE產生的，以及HE_B($r1$)是基於利用所述第二帳戶的公鑰對$r1$進行HE產生的，x是基於對T1、T1'和T1"進行雜湊處理產生的；基於確定性HE的特性確定所述第一隨機數、所述第二隨機數和所述第三隨機數是否相同；若以下條件成立，則確定所述第一隨機數、所述第二隨機數和所述第三隨機數相同：$g^{r2}h^{t2}$=T^{x}T1、HE_A($r2$)=T'^{x}T1'且HE_B($r2$)=T"^{x}T1"，其中，T=g^rh^t，T'=HE_A(r)且T"=HE_B(r)，HE_A(r)和HE_A($r2$)是分別基於利用所述第一帳戶的公鑰對r和$r2$進行HE產生的，HE_B(r)和HE_B($r2$)是基於利用所述第二帳戶的公鑰對r和$r2$進行HE產生的；T、T'和T"形成所述交易金額t的密文；以及基於同態加密對所述第一帳戶的餘額和所述第二帳戶的餘額進行更新。

本公開還提供了耦接到一個或多個處理器且其上儲存有指令的一個或多個非暫態電腦可讀儲存媒體，當由所述一個或多個處理器執行所述指令時，促使所述一個或多個處理器根據本文提供的方法的實施方式執行操作。

本公開還提供了用於實現本文所提供方法的系統。該系統包括一個或多個處理器、以及耦接到所述一個或多個處理器且其上儲存有指令的一個或多個非暫態電腦可讀儲存媒體，當由所述一個或多個處理器執行所述指令時，促使所述一個或多個處理器根據本文提供的方法的實施方式執行操作。

可以理解的是根據本公開的方法可以包括本文所述的方面和特徵的任意組合。亦即，根據本公開的方法不限於本文所述的方面和特徵的組合，但也包括所提供的方面和特徵的任意組合。

本公開的一個或多個實施方式的細節將在下文結合圖式和描述進一步闡述。本公開的其他特徵或優點將從描述和圖式以及申請專利範圍中顯而易見。

【圖式簡單說明】

圖1描繪了可用於執行本公開實施方式的示例環境。

圖2描繪了根據本公開實施方式的示例概念性架構。

圖3描繪了根據本公開實施方式的基於同態加密的區塊鏈交易的隱私保護驗證的示例方法。

圖4描繪了根據本公開實施方式的基於同態加密的示例區塊鏈交易。

圖5描繪了根據本公開實施方式的基於同態加密的區塊鏈交易的隱私保護驗證的另一示例方法。

圖6描繪了根據本公開實施方式的基於同態加密的另

一示例區塊鏈交易。

圖7描繪了可根據本公開實施方式執行的示例過程。

圖8描繪了可根據本公開實施方式執行的另一示例過程。

各種圖式中的相同圖式標記指示相同元素。

【實施方式】

本公開的實施方式包括用於在無需用戶確認、交互及顯露交易金額或帳戶餘額的情況下，對區塊鏈交易進行隱私保護驗證的電腦實施方法。更具體地，本公開的實施方式涉及基於承諾方案和同態加密(HE)驗證區塊鏈用戶之間的交易而不對其他區塊鏈節點顯露交易金額、帳戶餘額或用於產生承諾的隨機數。

為本公開實施方式提供進一步的背景，如上所述的，區塊鏈網路又可被稱為共識網路(例如，由點對點節點組成)、分散式帳本系統、或簡稱為區塊鏈，使得參與的實體能夠安全地且不可篡改地進行交易並儲存資料。區塊鏈可被提供為公有區塊鏈、私有區塊鏈或聯盟區塊鏈。本文將參考在參與的實體之間公開的公有區塊鏈網路進行進一步詳述本公開的實施方式。然而，可以預測的是，可以在任何合適類型的區塊鏈中實現本公開的實施方式。

在公有區塊鏈中，共識過程由共識網路的節點控制。例如，數百、數千甚至數百萬的實體可以參與到公有區塊鏈中，每個實體操作該公有區塊鏈中的至少一個節點。因

此，就參與的實體而言，公有區塊鏈可被視為公有網路。在一些示例中，大部分實體(節點)必須對每個區塊簽名，以使區塊有效並被添加至區塊鏈中。示例公有區塊鏈包括在比特幣網路中使用的區塊鏈，該比特幣網路是點對點支付網路(加密貨幣網路)。儘管本文所用術語“區塊鏈”通常指代比特幣網路，在不特指比特幣網路的情況下，區塊鏈通常指分散式帳本。

通常來說，公有區塊鏈支援公開交易。在區塊鏈內公開交易被所有節點共用，且該區塊鏈帳本跨所有節點複製。也即，所有節點相對於區塊鏈都處於完美共識狀態。為達成共識(例如，同意將區塊添加至區塊鏈)，在區塊鏈網路內實施共識協議。示例共識協議包括但不限於，在比特幣網路中實施的工作量證明(POW)。

在這裡考慮以上背景更詳細描述本公開的實施方式。更具體地，且如上所述，本公開的實施方式涉及基於承諾方案和HE驗證區塊鏈用戶之間的交易，而不對其他區塊鏈節點顯露交易金額、帳戶餘額或用於產生承諾的隨機數。

根據本公開的實施方式，可以基於承諾驗證區塊鏈交易並將其記錄至區塊鏈(帳本)中，而不顯露交易帳戶餘額、交易金額或用於產生承諾的隨機數。例如佩德森承諾(PC)的承諾方案，可以用於利用隨機數產生交易金額的承諾。可以利用機率性HE或確定性HE對交易金額和隨機數加密。交易金額和隨機數也可以用於產生一組值，作為用

於基於HE的特性驗證交易的證據。可以在不顯露帳戶餘額、交易金額或隨機數的情況下，由區塊鏈節點利用交易的承諾、加密的交易金額、加密的隨機數和證據來驗證交易是否有效。

圖1描繪了可用於執行本公開實施方式的示例環境100。在一些示例中，示例環境100使得實體能夠參與到公有區塊鏈102中。示例環境100包括計算系統106、108以及網路110。在一些示例中，網路110包括局域網(LAN)、廣域網路(WAN)、互聯網或其組合，並連接網路網站、用戶設備(例如，計算設備)和後端系統。在一些示例中，可以透過有線和/或無線通訊鏈路訪問網路110。

在所描述的示例中，計算系統106、108可以各自包括能夠作為節點參與到公有區塊鏈102中的任何合適的計算系統。示例計算設備包括但不限於伺服器、桌上型電腦、膝上型電腦、平板計算設備和智慧型電話。在一些示例中，計算系統106、108承載一個或多個由電腦實施的服務，用於與公有區塊鏈102交互。例如，計算系統106可以承載第一實體(例如，用戶A)的由電腦實施的、例如交易管理系統的服務，第一實體使用該交易管理系統管理它與一個或多個其他實體(例如，其他用戶)的交易。計算系統108可以承載第二實體(例如，用戶B)的由電腦實施的、例如交易管理系統的服務，第二實體使用該交易管理系統管理它與一個或多個其他實體(例如，其他用戶)的交易。在圖1的示例中，公有區塊鏈102被表示為節點的點對點網

路，且計算系統106、108分別提供參與到公有區塊鏈網路102中的第一實體和第二實體的節點。

圖2描繪了根據本公開實施方式的概念性架構200的示例。示例概念性架構200包括實體層202、承載服務層204以及公有區塊鏈層206。在所描述的示例中，實體層202包括三個實體，實體1(E1)、實體2(E2)、實體3(E3)，每個實體具有對應的交易管理系統208。

在所描述的示例中，承載服務層204包括用於每個交易管理系統208的區塊鏈介面210。在一些示例中，各個交易管理系統208利用通信協議(例如，超文本傳輸協議安全(HTTPS))透過網路(例如，圖1的網路110)與各個區塊鏈介面210通信。在一些示例中，每個區塊鏈介面210提供各個交易管理系統208與區塊鏈層206之間的通信連接。更具體地，每個區塊鏈介面210使得各個實體能夠進行記錄在區塊鏈層206的區塊鏈網路212中的交易。在一些示例中，區塊鏈介面210與區塊鏈層206之間的通信是利用遠程程序呼叫(RPC)進行的。在一些示例中，區塊鏈介面210“承載”用於各個交易管理系統208的區塊鏈節點。例如，區塊鏈介面210提供用於訪問區塊鏈網路212的應用程式介面(API)。

如本文所述的，區塊鏈網路212被提供為包括多個節點214的點對點網路，所述多個節點214在區塊鏈216中不可篡改地記錄資訊。儘管示意性地描述了單個區塊鏈216，但是在區塊鏈網路212中可以提供並維護區塊鏈216

的多個副本。例如，每個節點214儲存區塊鏈216的副本。在一些實施方式中，區塊鏈216儲存與參與公有區塊鏈的兩個或更多個實體之間進行的交易相關聯的資訊。

圖3描繪了根據本公開實施方式的基於HE的區塊鏈交易的隱私保護驗證的示例方法300。在較高層面上，示例方法300由用戶節點A 302、用戶節點B(圖3中未示出)和被稱為共識節點的區塊鏈節點304執行。可以進行從用戶節點A 302至用戶節點B的例如轉帳的交易。為保護帳戶隱私，用戶節點A 302可以基於隨機數*r*利用例如PC的承諾方案產生交易金額*t*的承諾。可以將利用PC產生的承諾表達為PC(*r*, *t*)。用戶節點A 302還可以基於用戶節點B的公鑰利用HE對隨機數加密。這可以被表達為HE(*r*)。可以將交易金額*t*的表達為(PC(*r*, *t*), HE(*r*))的密文傳輸至用戶節點B。在接收到密文之後，用戶節點B可以利用私鑰對隨機數*r*解密。用戶節點B可以利用隨機數*r*對交易金額*t*解密。為證實交易的有效性，區塊鏈節點304可以將承諾中的隨機數與利用HE加密的隨機數對比。若所述隨機數匹配，則區塊鏈節點304透過交易資料的零知識確定交易有效。示例方法300的更多細節將在下文對圖3的描述中討論。

在306，用戶節點A 302基於第一隨機數產生交易金額的承諾值，並基於HE利用用戶節點A 302的公鑰對第二隨機數加密、以及利用用戶節點B的公鑰對第三隨機數加密。第一隨機數、第二隨機數和第三隨機數可以是相同的隨機數*r*，其被用於利用承諾方案產生交易金額*t*的承諾。

在一些實施方式中，承諾方案可以具有雙指數的形式，例如PC。使用PC作為非限制性示例，透過第一隨機數r產生的承諾值可以被表達為$PC(r, t)=g^r h^t$，其中g和h可以是橢圓曲線的生成數，$PC(r, t)$是曲線點的標量相乘，t是被承諾的交易金額。可以理解的是，其他基於HE的承諾方案，例如Okamoto-Uchiyama(OU) HE以及Boneh-Goh-Nissim HE也可以用於產生承諾值。

對利用用戶節點A 302的公鑰加密得到的加密第二隨機數r可以被表達為HE_A(r)。對利用用戶節點B的公鑰加密得到的加密第三隨機數r可以被表達為HE_B(r)。

在一些實施方式中，公鑰HE加密可以是確定性HE，其可根據諸如Paillier HE、Benaloh HE、OU HE、Naccache-Stern HE、Damgard-Jurik HE或Boneh-Goh-Nissim HE等的機率性HE方案透過將隨機數設置為固定值而被獲取。在一些實施方式中，滿足線性特徵$HE(a+b)=HE(a)+HE(b)$和$HE(ab)=HE(b)^a$的確定性HE方案可以用於本公開，其中a和b是用於HE的明文。

在一些示例中，$T=PC(r, t)$、T'=HE_A(r)和T"=HE_B(r)，並且交易金額的密文可被表達為(T, T'和T")。若滿足示例條件，則可以確定交易有效。首先，交易金額t大於或等於零且小於或等於用戶節點A 302的帳戶餘額s_A。其次，透過用戶節點A 302的私鑰對交易進行數位簽章以證實交易是由用戶節點A 302授權的。再次，承諾$PC(r, t)$中的隨機數r與密文HE_A(r)中使用用戶節點A302

的公鑰加密的*r*和密文HE_B(*r*)中使用用戶節點B的公鑰加密的*r*分別相等。

在一些實施方式中，密文也可以被分解成發送金額(*t'*)的密文和接收金額(t")的密文，其中發送金額(*t'*)的密文可被表達為(PC(*r'*, *t'*), HE_A(*r'*))，接收金額(t")的密文可被表達為(PC(*r"*, *t"*), HE_B(*r"*))。在此情況下，還需要確定發送金額t'與接收金額t''相等以驗證交易。

在308，用戶節點A 302產生一個或多個範圍證據。在一些實施方式中，範圍證據可以包括範圍證據*RP1*以表示交易金額*t*大於或等於零，以及範圍證據*RP2*以表示交易金額*t*小於或等於用戶節點A的帳戶餘額。

在310，用戶節點A 302基於一個或多個選擇的隨機數使用HE產生一組值。標記為*Pf*的該組值可以包括用於證實承諾PC(*r*, *t*)中的隨機數*r*與密文HE_A(*r*)和HE_B(*r*)中分別利用用戶節點A 302和用戶節點B的公鑰加密的*r*相等的證據。在一些實施方式中，可以選擇兩個隨機數*r1*和*t1*以計算*t1*的被標記為(T1, T1', T1")的另一組密文，其中$T1=g^{r1}h^{t1}$、T1'=HE_A(*r1*)、T1"=HE_B(*r1*)。可以計算兩個附加的證據*r2*和*t2*：*r2*=*r1*+*xr*、*t2*=*t1*+*xr*，其中*x*是T1、T1'和T1"的雜湊值。可將該組值標記為*Pf*=(T1, T1', T1", *r2*, *t2*)。

在312，用戶節點A 302利用其私鑰對密文(T', T', T")、密文(T1, T1' T1")、*r2*、*t2*、範圍證據*RP1*和*RP2*以及用戶節點A 302和用戶節點B的公鑰進行數位簽章。由用戶

節點A 302添加的數位簽章可以用於表明交易是由用戶節點A 302授權的。在314，將經數位簽章的副本遞交至區塊鏈網路。

在316，區塊鏈節點304利用用戶節點A 302的公鑰驗證數位簽章。區塊鏈節點304可以是能夠證實區塊鏈網路中的交易的有效性的共識節點。若區塊鏈節點304利用該公鑰不能驗證用戶節點A 302的數位簽章，則可以確定該數位簽章錯誤，並可以拒絕該交易。在一些實施方式中，區塊鏈節點304還可以包括反雙花機制。區塊鏈節點304可以驗證交易是否已被執行或記錄。若交易已經被執行，則可以拒絕該交易。否則，可以進行交易驗證。

在318，區塊鏈節點304驗證一個或多個範圍證據。例如，範圍證據*RP1*可以用於證實交易金額*t*大於或等於零，且範圍證據*RP2*可以用於證實交易金額*t*小於或等於用戶節點A 302的帳戶餘額。

在320，區塊鏈節點304基於該組值確定第一隨機數、第二隨機數以及第三隨機數相同。在一些實施方式中，確定過程包括基於上述確定性HE的特性確定示例條件$g^{r2}h^{t2}=T^{x}T1$、$HE_A(r2)=T'^{x}T1'$以及$HE_B(r2)=T''^{x}T1''$是否為真。若為真，則其可以表明承諾中的隨機數與利用用戶節點A 302和用戶節點B的公鑰同態加密的隨機數相同，且交易有效。

在322，區塊鏈節點304更新用戶節點A 302和用戶節點B的帳戶餘額。可以基於HE的特性執行餘額更新而不顯

露用戶節點A 302或用戶節點B的帳戶餘額。本文將參考圖4進一步描述帳戶餘額的更新。

圖4描繪了根據本公開實施方式的基於HE的示例區塊鏈交易400。如示例區塊鏈交易400所示，用戶節點A 402向用戶節點B 406轉帳交易金額t。在交易之前，用戶節點A 402的帳戶餘額為s_A，且用戶節點B 406的帳戶餘額為s_B。

使用本文參考圖3描述的加密方案和交易過程作為示例，可以基於PC利用隨機數r_A對帳戶餘額s_A加密，且基於HE對隨機數r_A加密。帳戶餘額s_A的密文可被表達為$(S_A, S'_A)=(g^{r_A}h^{s_A}, HE_A(r_A))$，其中$g$和$h$可以是橢圓曲線的生成數以用於產生帳戶餘額$s_A$的PC。類似地，可以基於PC利用隨機數$r_B$對用戶節點B 406的帳戶餘額$s_B$加密。帳戶餘額$s_B$的密文可被表達為$(S_B, S'_B)=(g^{r_B}h^{s_B}, HE_A(r_B))$。

在404，用戶節點A 402可以將數位簽章添加至用於驗證交易的一系列證據中，並將經數位簽章的副本遞交至區塊鏈網路408。參考圖3如上所述，上述證據可以包括交易金額的密文(T, T', T")、一個或多個範圍證據(*RP1*, *RP2*)以及其他證據(T1, T1', T1", *r2*, *t2*)。

在交易之後，用戶節點A 402的帳戶餘額可被表達為s_A-t'，且用戶節點B 406的帳戶餘額可被表達為s_B+t''，其中t'是由用戶節點A 402發送的金額，且t''是由用戶節點B接收的金額。用戶節點A 402在交易後的帳戶餘額的密文

可以表達為(S_A-T, S'_A-T')，用戶節點B 406在交易之後的帳戶餘額的密文可被表達為(S_B+T, S'_B+T')。因為S_A、S'_A、S_B、S'_B、T、T'、T"均是利用雙指數形式的HE加密的，因此可以在它們的加密形式下進行加減運算而無需解密成明文值。

圖5描繪了根據本公開實施方式的基於HE的區塊鏈交易的隱私保護驗證的另一示例方法500。在較高層面上，示例方法500由用戶節點A 502、用戶節點B(圖5中未示出)以及可被稱為共識節點的區塊鏈節點504執行。可以進行從用戶節點A 502至用戶節點B的例如轉帳的交易。為保護帳戶隱私，用戶節點A 502可以基於隨機數*r*利用例如PC的承諾方案產生交易金額*t*的承諾。利用PC產生的承諾可被表達為PC(*r*, *t*)。用戶節點A 502還可以利用具有雙指數形式的HE(例如OU)對交易金額*t*和隨機數*r*加密。

交易金額*t*的密文可以被遞交至區塊鏈網路。在接收到密文之後，區塊鏈節點504可以確定隱藏在PC中的隨機數*r*是否與OU中分別利用用戶節點A 502的公鑰和用戶節點B的公鑰加密的隨機數*r*匹配。此外，區塊鏈節點504可以確定隱藏在PC中的交易金額*t*是否與OU中分別利用用戶節點A 502的公鑰和用戶節點B的公鑰加密的交易金額*t*匹配。若隨機數和交易金額都匹配，則區塊鏈節點504可基於交易資料的零知識驗證該交易有效。

在506，用戶節點A 502基於第一隨機數產生第一交易金額的承諾值，且使用用戶節點A 502的公鑰對第一交易

金額和第一隨機數加密。使用用戶節點B的公鑰對第二交易金額和第二隨機數加密。第一交易金額和第二交易金額可以為相同的交易金額*t*。第一隨機數和第二隨機數可以是相同的隨機數*r*，以用於利用承諾方案產生交易金額*t*的承諾。在一些實施方式中，承諾方案可以具有雙指數形式、例如PC。使用PC作為示例，透過第一隨機數*r*產生的承諾值可以被表達為$PC(r, t)=g^r h^t$，其中*g*和*h*可以是橢圓曲線的生成數，PC(*r*, *t*)是曲線點的標量相乘，*t*是被承諾的交易金額。可以理解的是，其他基於HE的承諾方案，例如OU HE以及Boneh-Goh-Nissim HE也可以用於產生承諾值。

用戶節點A 502還可以利用用戶節點A 502的公鑰對第一隨機數和第一交易金額加密，並利用用戶節點B的公鑰對第二隨機數和第二交易金額加密。在一些實施方式中，隨機數和交易金額的加密可以基於機率性HE、例如OU。使用OU作為示例，利用用戶節點A 502的公鑰加密的第一隨機數和第一交易金額可被分別表達為$OU_A(r)=u1^r v1^{y1}$和$OU_A(t)=u1^t v1^{y2}$，其中*u1*和*v1*分別為橢圓曲線的生成數，且*y1*和*y2*為用於產生OU_A(*r*)和OU_A(*t*)的隨機數。加密的第二隨機數和第二交易金額分別表達為$OU_B(r)=u2^r v2^{z1}$和$OU_B(t)=u2^t v1^{z2}$，其中*u2*和*v2*為橢圓曲線的生成數，且*z1*和*z2*分別為用於產生OU_B(*r*)和OU_B(*t*)的隨機數。機率性OU滿足OU(*a*+*b*)=OU(*a*)*OU(*b*)的特性，其中*a*和*b*為用於OU的明文。

交易金額*t*的密文可被表達為(PC(*r*, *t*), OU_A(*r*), OU_A(*t*), OU_B(*r*), OU_B(*t*))。若符合以下示例條件，則可以確定交易有效。首先，交易金額*t*大於或等於零，且小於或等於用戶節點A 502的帳戶餘額*s*_A。其次，交易是利用用戶節點A 502的私鑰數位簽章的，以證實交易是由用戶節點A 502授權的。再次，承諾PC(*r*, *t*)中的隨機數*r*與密文OU_A(*r*)和OU_B(*r*)中分別利用用戶節點A 502和用戶節點B的公鑰加密的*r*相同。最後，承諾PC(*r*, *t*)中的交易金額*t*與密文OU_A(*r*)和OU_B(*r*)中分別利用用戶節點A 502和用戶節點B的公鑰加密的*t*相同。

在一些實施方式中，密文也可以被分解成發送金額為(*t'*)的密文和接收金額為(*t''*)的密文，發送金額為(*t'*)的密文可表達為(PC(*r'*, *t'*), OU_A(*r'*), OU_A(*t'*))，接收金額為(*t''*)的密文可表達為(PC(*r''*, *t''*), OU_B(*r''*), OU_B(*t''*))。在這種情況下，還需要確定發送金額*t'*等於接收金額*t''*以驗證交易。

在508，用戶節點A 502產生一個或多個範圍證據。在一些實施方式中，範圍證據可以包括範圍證據*RP1*以顯示交易金額*t*大於或等於零，以及範圍證據*RP2*以顯示交易金額*t*小於或等於用戶節點A的帳戶餘額。

在510，用戶節點A 502基於一個或多個選擇的隨機數利用HE產生一組值。標注為*Pf*的該組值可以包括用於證實承諾PC(*r*, *t*)中的隨機數*r*與密文OU_A(*r*)和OU_B(*r*)中加密的*r*相同的證據，以及承諾PC(*r*, *t*)中的交易金額*t*與密文

OU_A(*r*)和OU_B(*r*)中加密的*t*相同的證據。在一些實施方式中，可以選擇四個隨機數*r**、*t**、*z1**和*z2**來計算標注為(C, D, E)的另一組密文，其中C=$g^{r*}h^{t*}$、D=$u2^{r*}v2^{z1*}$且E=$u2^{t*}v2^{z2*}$，其中*g*、*h*、*u2*和*v2*是橢圓曲線的生成數。可計算四個附加證據*a*、*b*、*c*和*d*：*a*=*r**+*xr*、*b*=*t**+*xt*、*c*=*z1**+*xz1*和*d*=*z2**+*xz2*，其中*x*是*g*、*h*、*u2*、*v2*、C、D和E的雜湊函數。該組值可被標注為*Pf*=(*C*, *D*, *E*, *a*, *b*, *c*, *d*)。

在512，用戶節點A 502使用其私鑰對密文(PC(*r*, *t*), OU_A(*r*), OU_A(*t*), PC(*r*, *t*), OU_B(*r*), OU_B(*t*))、範圍證據*RP1*和*RP2*以及該組值*Pf*進行數位簽章。由用戶節點A 502添加的數位簽章可以用於顯示交易是由用戶節點A 502授權的。在514，將經數位簽章的副本遞交至區塊鏈網路。

在516，區塊鏈節點504利用用戶節點A 502的公鑰驗證數位簽章。區塊鏈節點504可以是能夠證實在區塊鏈網路上的交易的有效性的共識節點。若區塊鏈節點504利用用戶節點A的公鑰不能驗證數位簽章，則該數位簽章可被確定為錯誤，並且交易可被拒絕。在一些實施方式中，區塊鏈節點504還可以包括反雙花機制。區塊鏈節點504可以驗證交易是否已被執行或記錄。若交易已經被執行，則交易可被拒絕。否則，可以進行交易驗證。

在518，區塊鏈節點504驗證一個或多個範圍證據。例如，範圍證據*RP1*可以用於證實交易金額*t*大於或等於零，且範圍證據*RP2*可以用於證實交易金額*t*小於或等於用戶節點A 502的帳戶餘額。

在520，區塊鏈節點504基於該組值確定第一交易金額是否與第二交易金額相同，以及第一隨機數是否與第二隨機數相同。在一些實施方式中，確定過程包括確定$g^a h^b$=CT^x、$u2^a v2^c$=DZ_B1^{x}以及$u2^b v2^d$=EZ+B2^{x}是否為真，其中T=$g^r h^t$是第一交易金額t的承諾值、Z_B1=$u2^r v2^{z1}$、Z_B2=$u2^t v2^{z2}$、且$z1$和$z2$是用於基於機率性HE方案對第二交易金額和第二隨機數加密的隨機數。若確定為真，則可以指示承諾中的隨機數和交易金額分別與利用用戶節點A 502和用戶節點B的公鑰同態加密的隨機數和交易金額相等，且交易有效。

在522，區塊鏈節點504更新用戶節點A 502和用戶節點B的帳戶餘額。可以基於HE的特性執行帳戶餘額更新而不顯露用戶節點A 502和/或用戶節點B的帳戶餘額。

圖6描繪了根據本公開實施方式的基於HE的示例區塊鏈交易600。如示例交易600所示，用戶節點A 602將交易金額t轉帳至用戶節點B 606。在交易之前，用戶節點A 602具有為s_A的帳戶餘額，且用戶節點B 606具有為s_B的帳戶餘額。

在一些示例中，可使用本文參考圖5描述的加密方案和交易過程，基於PC利用隨機數r_A隱藏帳戶餘額s_A。可基於OU對隨機數r_A和帳戶餘額加密。帳戶餘額s_A的密文可被表達為(S_A, R_A, Q_A)=($g^{r\_A} h^{s\_A}$, OU_A(r_A), OU_A(s_A))，其中g和h可以為橢圓曲線的生成數以用於產生帳戶餘額s_A的PC。類似地，可基於PC利用隨機數

r_B對用戶節點B 606的帳戶餘額s_B加密。帳戶餘額s_B的密文可被表達為(S_B, R_B, Q_B)=($g^{r\_B}h^{s\_B}$, OU_B(r_B), OU_B(s_B))。

在604，用戶節點A 602可以向用於驗證交易的證據添加數位簽章，並將經數位簽章的副本遞交至區塊鏈網路608中。這裡參考圖5所描述的，證據可以包括交易金額的密文(PC(r, t), OU_A(r), OU_A(t), OU_B(r), OU_B(t))、一個或多個範圍證據(*RP1*, *RP2*)和其他證據(C, D, E, a, b, c, d)。

在交易之後，用戶節點A 602的帳戶餘額可被表達為s_A-t，且用戶節點B 606的帳戶餘額可被表達為s_B+t。在交易之後，用戶節點A 602的帳戶餘額的密文可被表達為(S_A-T, R_A-Y_A1, Q_A-Y_A2)，其中Y_A1=OU_A(r)且Y_A2=OU_A(t)。在交易之後,用戶節點B 606的帳戶餘額的密文可被表達為(S_B+T, R_B+Z_B1, Q_B+Z_B2),其中Z_B1=OU_B(r)且Z_B2=OU_B(t)。因為S_A、S_B、R_A、R_B、Q_A、Q_B、Y_A1、Y_A2、Z_B1、Z_B2和T是利用具有雙指數形式的HE加密的，因此可以在它們的加密形式下進行加減運算而無需解密成明文值。

圖7描繪了可根據本公開實施方式執行的示例過程700。為清楚地呈現，在本說明書中以下描述在其他圖式的背景下總體地描述方法700。然而，應當理解示例過程700可以例如透過任何系統、環境、軟體和硬體或者系統、環境、軟體和硬體的組合合理來執行。在一些實施方

式中，示例過程700的步驟可以以並行、組合、迴圈或任何順序進行。

在702，共識節點從第一帳戶接收待從第一帳戶向第二帳戶轉帳的交易金額的、基於第一隨機數產生的承諾值的經數位簽章的副本。共識節點還可以從第一帳戶接收利用第一帳戶的公鑰加密的第二隨機數、利用第二帳戶的公鑰加密的第三隨機數、一個或多個範圍證據以及基於一個或多個選擇的隨機數利用HE產生的一組值。在一些實施方式中，使用基於HE的承諾方案產生承諾值。在一些實施方式中，基於確定性HE方案對第二隨機數和第三隨機數加密。

在一些實施方式中，透過(T1, T1′, T1″, *r2*, *t2*)表示該組值，其中 $r2=r1+xr$ 、 $t2=t1+xt$ ，*r1*和*t1*表示一個或多個選擇的隨機數，且*r*表示第一隨機數，*t*表示餘額轉帳金額。在一些示例中，$T1=g^{r1}h^{t1}$ 、T1′=HE_A(*r1*)、T1″=HE_B(*r1*)，其中*g*和*h*是橢圓曲線的生成數，HE_A(*r1*)是基於利用第一帳戶的公鑰對r1進行HE產生的，且HE_B(*r1*)是基於利用第二帳戶的公鑰對r1進行HE產生的。在一些示例中，*x*是基於對T1、T1′和T1″進行雜湊處理產生的。

在704，共識節點利用第一帳戶的與用於產生數位簽章的私鑰相對應的公鑰，驗證與經數位簽章的副本相對應的數位簽章。

在706，共識節點確定一個或多個範圍證據證實餘額轉帳金額是否大於零，且小於或等於第一帳戶的餘額。

在708，共識節點基於該組值確定第一隨機數、第二隨機數和第三隨機數是否相同。在一些實施方式中，若以下條件成立，則確定第一隨機數、第二隨機數和第三隨機數相同：$g^{r2}h^{t2}$=T^{x}T1、HE_A($r2$)=T$'^{x}$T1'且HE_B($r2$)=T$''^{x}$T1''，其中T=$g^{r}h^{t}$是餘額轉帳金額的承諾值，T'=HE_A(r)且T''=HE_B(r)，HE_A(r)是基於利用第一帳戶的公鑰對r進行HE產生的，HE_B(r)是基於利用第二帳戶的公鑰對r進行HE產生的，HE_A($r2$)是基於利用第一帳戶的公鑰對r2進行HE產生的，以及HE_B($r2$)是基於利用第二帳戶的公鑰對r2進行HE產生的，x是基於對g、h、T1、T1'和T1"進行雜湊處理產生的。在一些實施方式中，T、T'和T"形成交易金額t的密文。

在710，若第一隨機數、第二隨機數和第三隨機數相同，則共識節點基於交易金額更新第一帳戶的餘額和第二帳戶的餘額。在一些實施方式中，更新第一帳戶的餘額和第二帳戶的餘額是基於HE進行的。

圖8描繪了可根據本公開實施方式執行的另一示例過程800。為清楚地呈現，在本說明中以下描述在其他圖式的執行背景下總體地描述示例過程800。然而，應該理解示例過程800可以例如透過任何系統、環境、軟體和硬體或者系統、環境、軟體和硬體的組合合理進行。在一些實施方式中，示例過程800的步驟可以以並行、組合、迴圈或任何順序進行。

在802，共識節點從第一帳戶接收待從第一帳戶向第

二帳戶轉帳的第一交易金額的承諾值的經數位簽章的副本。在一些示例中，基於第一隨機數產生該承諾值的經數位簽章的副本。共識節點還接收利用第一帳戶的公鑰加密的第一交易金額和第一隨機數、利用第二帳戶的公鑰加密的第二餘額轉帳金額和第二隨機數、一個或多個範圍證據、以及基於一個或多個選擇的隨機數利用HE產生的一組值。在一些實施方式中，利用PC方案產生承諾值。在一些實施方式中，基於機率性HE演算法使用第一帳戶的公鑰對第一餘額轉帳金額和第一隨機數加密。在一些示例中，基於機率性HE演算法使用第二帳戶的公鑰對第二餘額轉帳金額和第二隨機數加密。在一些實施方式中，機率性HE演算法為Okamoto-Uchiyama HE演算法。

在一些實施方式中，透過(C, D, E, a, b, c, d)表示該組值，其中$a=r^*+xr$、$b=t^*+xt$、$c=z1^*+xz1$且$d=z2^*+xz2$，r^*、t^*、$z1^*$和$z2^*$表示一個或多個選擇的隨機數，r表示第一隨機數，t表示第一餘額轉帳金額，$C=g^{r^*}h^{t^*}$，$D=u2^{r^*}v2^{z1^*}$，$E=u2^{t^*}v2^{z2^*}$，g、h、$u2$和$v2$為橢圓曲線的生成數，且x表示對C、D和E進行雜湊處理。

在804，共識節點利用第一帳戶的與用於產生數位簽章的私鑰相對應的公鑰，驗證與經數位簽章的副本相對應的數位簽章。

在806，共識節點確定一個或多個範圍證據證實餘額轉帳金額是否大於零，且小於或等於第一帳戶的餘額。

在808，共識節點基於該組值確定第一金額是否與第

二金額相同，以及第一隨機數是否與第二隨機數相同。在一些實施方式中，若以下條件成立，則確定第一金額與第二金額相同且第一隨機數與第二隨機數相同：$g^a h^b$=CT^x、$u2^a v2^c$=DZ_B1^{x}且$u2^b v2^d$=EZ_B2^x，其中T=$g^r h^t$是餘額轉帳金額的承諾值，Z_B1=$u2^r v2^{z1}$，Z_B2=$u2^t v2^{z2}$。在一些示例中，*z1*和*z2*是用於基於機率性HE方案對第二交易金額和第二隨機數加密的隨機數。

在810，若第一金額與第二金額相同且第一隨機數與第二隨機數相同，則共識節點基於第一餘額轉帳金額更新第一帳戶的餘額和第二帳戶的餘額。在一些實施方式中，更新第一帳戶的餘額和第二帳戶的餘額是基於HE進行的。

本申請中所描述主題的實施方式可被實施以實現特定優點或技術效果。例如，本公開的實施方式允許區塊鏈節點的帳戶餘額和區塊鏈節點的交易金額在交易期間是隱私的。資金轉移的接收方不需要確認交易或使用隨機數驗證承諾，交易驗證可以是非互動性的。區塊鏈節點可以基於HE和承諾方案驗證交易以允許零知識證明。

所述方法能夠提高各種行動計算裝置的帳戶/資料安全性。帳戶餘額和交易金額可以基於HE被加密並透過承諾方案被隱藏。照此，共識節點在交易之後可以基於HE的特性更新帳本中的帳戶餘額，而不顯露帳戶的真實帳戶餘額。因為不需要將隨機數發送至接收方以確認交易，所以資料洩露的風險可被降低，並且需要更少的用於管理隨

機數的計算和儲存資源。

本申請中描述的實施方式和操作可以在數位電子電路中或者在電腦軟體、韌體、包括本申請中公開的結構的硬體中或它們中一個或多個的組合中實現。這些操作可被實施為由資料處理裝置對儲存在一個或多個電腦可讀存放裝置上的、或從其他資源接收的資料執行的操作。資料處理裝置、電腦或計算設備可以包括，包括諸如可編程處理器、電腦、系統單晶片或以上一個或多個或組合的，用於處理資料的裝置、設備和機器。裝置可以包括專用邏輯電路，例如，中央處理單元(CPU)、現場可編程閘陣列(FPGA)或專用積體電路(ASIC)。裝置還可包括為所討論的電腦程式創建執行環境的程式碼，例如，構成處理器韌體、協定堆疊、資料庫管理系統、作業系統(例如一個作業系統或多個作業系統的組合)、跨平台執行時間環境、虛擬機器或者它們之中一個或多個的組合的程式碼。裝置和執行環境可以實現各種不同的計算模型基礎設施，例如網頁服務、分散式運算和網格計算基礎設施。

電腦程式(又稱，例如，程式、軟體、軟體應用、軟體模組、軟體單元、腳本或程式碼)可以以任何形式的編程語言編寫，包括編譯語言或演繹性語言、說明性語言或程式性語言，並且它可以配置為任何形式，包括作為獨立程式，或者作為模組、元件、副程式、物件或適合在計算環境中使用的其他單元。程式可儲存在：保存其他程式或資料的檔案的一部分中(例如，儲存在標記語言文檔中的

一個或多個腳本)、專用於所討論的程式的單個檔案中或者多個協調檔案中(例如，儲存一個或多個模組，副程式或部分程式碼的多個檔案)中。電腦程式可以在一台電腦或者位於一個網站或由通信網路互聯的分佈在多個網站上的多台電腦執行。

用於執行電腦程式的處理器包括，例如，通用和專用微型處理器兩者，和任意種類的數碼電腦的任意一個或多個處理器。通常，處理器將從唯讀記憶體或隨機存取記憶體或其兩者接收指令和資料。電腦的重要元件為用於根據指令進行操作的處理器和用於儲存指令和資料的一個或多個存放裝置。通常，電腦還將包括一個或多個用於儲存資料的大型存放裝置，或可操作地耦接以從所述大型存放裝置接收資料或向其轉發資料，或兩者。電腦可嵌入在另一個設備中，例如，行動電話、個人數位助理(PDA)、遊戲控制台、全球定位系統(GPS)接收器或可攜式存放裝置。適用於儲存電腦程式指令和資料的設備包括非易失性記憶體、媒體和存放裝置，包括，例如，半導體存放裝置、磁片和磁光碟。處理器和記憶體可補充有專用邏輯電路或集成在專用邏輯電路中。

移動設備可以包括手機、用戶設備(UE)、行動電話(例如，智慧型電話)、平板電腦、可穿戴設備(例如，智慧手錶和智慧眼鏡)、人體內的植入設備(例如，生物感測器、人工耳蝸植入)、或其它類型的移動設備。移動設備可以無線地(例如，使用射頻(RF)信號)與各種(下文描述

的)通信網路通信。移動設備可以包括用於確定移動設備當前環境的特徵的感測器。感測器可以包括相機、麥克風、接近感測器、GPS感測器、運動感測器、加速度測量計、環境光感測器、濕度感測器、陀螺儀、指南針、氣壓計、指紋感測器、面部識別系統、RF感測器(例如，WiFi和蜂巢式無線電)、熱量感測器或其它類型的感測器。例如，相機可以包括帶有可動或固定鏡頭的前置或後置相機、閃光燈、圖像感測器和影像處理器。相機可以是能夠捕捉用於面部和/或虹膜識別的細節的百萬像素相機。相機與資料處理器和儲存在記憶體中或可遠端存取的認證資料一起可以形成面部識別系統。面部識別系統或者一個或多個感測器，例如，麥克風、運動感測器、加速度測量計、GPS感測器或RF感測器可以用於用戶認證。

為提供用於與用戶的交互，實施方式可以在具有顯示裝置和輸入裝置的電腦上實現，例如，用於向用戶顯示資訊的液晶顯示器(LCD)或有機發光二極體(OLED)/虛擬實境(VR)/增強實境(AR)顯示器以及用戶可提供輸入至電腦的觸控式螢幕、鍵盤和指示設備。其他種類的設備也可以用於提供與用戶的交互；例如，提供給用戶的回饋可是任何形式的感官回饋，例如視覺回饋，聽覺回饋或觸覺回饋；且可以以任何形式接收來自用戶的輸入，包括聲學、語音或觸覺輸入。此外，電腦可透過向用戶使用的設備發送文檔並從用戶使用的設備接收文檔來與用戶交互；例如，透過回應於從網頁瀏覽器接收到的請求向客戶設備上

的網頁瀏覽器發送網頁。

實施方式可以使用計算設備實現，計算設備透過有線或無線數位資料通信(或其組合)的任意形式或媒介互聯，例如，通信網路。互聯設備的示例為通常彼此遠離的、通常透過通信網路交互的客戶端和伺服器。客戶端，例如，移動設備，可以自身與伺服器或透過伺服器進行交易，例如進行買、賣、支付、給予、發送或貸款交易，或認證以上交易。這種交易可以是即時的使得操作和回應在時間上接近，例如個體感覺操作和回應基本上是同時發生的，對於在個體的操作之後的響應的時間差小於一毫秒(ms)或小於一秒(s)，或在不考慮系統的處理限制的情況下，回應沒有主動延遲。

通信網路的示例包括局域網(LAN)、無線電存取網路(RAN)、都會區網路(MAN)和廣域網路(WAN)。通信網路可以包括所有或部分網際網路、其他通信網路或通信網路的組合。可以根據各種協議和標準在通信網路上傳輸資訊，包括長期演進網路(LTE)、5G、IEEE 802、網際網路協議(IP)或其他協議或協議的組合。通信網路可以在連接的計算設備之間傳輸音訊、視頻、生物特徵或認證資料或其他資訊。

作為單獨實施方式描述的特徵可以組合實施、在單個實施方式中實施，然而被描述為單個實施方式的特徵可以在多個實施方式中分別單獨實現，或在任何合適的子組合中實現。按特定順序描述的和要求保護的操作不應理解為

必須以該順序進行，也不是所有示出的操作都必須被執行(一些操作可以是可選的)。適當地，可以進行多工或並行處理(或多工和並行處理的組合)。

【符號說明】

100：環境

102：公有區塊鏈

106：計算系統

108：計算系統

110：網路

200：概念架構

202：實體層

204：承載服務層

206：公有區塊鏈層

208：交易管理系統

210：區塊鏈介面

212：區塊鏈網路

214：節點

216：區塊鏈

300：方法

302：用戶節點A

304：區塊鏈節點

306~322：方法步驟

400：區塊鏈交易

402：用戶節點A

404：方法步驟

406：用戶節點B

408：區塊鏈網路

500：方法

502：用戶節點A

504：區塊鏈節點

506~522：方法步驟

600：區塊鏈交易

602：用戶節點A

604：方法步驟

606：用戶節點B

608：區塊鏈網路

700：方法

702~710：方法步驟

800：過程

802~810：過程步驟

【發明申請專利範圍】

【第1項】

一種由區塊鏈網路的共識節點執行的電腦實施方法，包括：

從第一帳戶接收要從該第一帳戶轉帳至第二帳戶的交易金額的基於第一隨機數產生的承諾值的經數位簽章的副本、利用該第一帳戶的公鑰加密的第二隨機數、利用該第二帳戶的公鑰加密的第三隨機數、一個或多個範圍證據、和基於一個或多個選擇的隨機數產生的一組值；

利用該第一帳戶的公鑰，驗證對應於該經數位簽章的副本的數位簽章，其中該第一帳戶的公鑰與用於產生該數位簽章的私鑰對應；

確定該一個或多個範圍證據證實該交易金額大於零、且小於或等於該第一帳戶的餘額；

基於該一組值確定該第一隨機數、該第二隨機數和該第三隨機數是否相同；以及

若該第一隨機數、該第二隨機數和該第三隨機數相同，則基於該交易金額以及基於同態加密更新該第一帳戶的餘額和該第二帳戶的餘額，

其中，基於確定性同態加密HE方案加密該第二隨機數和該第三隨機數，該HE方案具有線性特徵$HE(a+b)=HE(a)*HE(b)$和$HE(ab)=HE(b)^a$，其中a和b是用於HE的明文。

【第2項】

如請求項1所述的電腦實施方法，其中，利用同態承諾方案產生該承諾值。

【第3項】

如請求項2所述的電腦實施方法，其中，該承諾方案為佩德森承諾方案。

【第4項】

如請求項1所述的電腦實施方法，其中，

由*r1*和*t1*表示該選擇的隨機數，且

該選擇的隨機數用於產生*r2*和*t2*，其中$r2=r1+xr$、$t2=t1+xt$，*r1*和*t1*表示該一個或多個選擇的隨機數，*r*是該第一隨機數，*t*是該交易金額，*x*是雜湊值。

【第5項】

如請求項4所述的電腦實施方法，其中，還基於T1、T1'和T1"產生該一組值，其中

$T1=g^{r1}h^{t1}$、T1'=HE_A(*r1*)、T1"=HE_B(*r1*)，

其中，*g*和*h*為橢圓曲線的生成數，

HE_A(*r1*)是基於利用該第一帳戶的公鑰對r1進行HE產生的，

HE_B(*r1*)是基於利用該第二帳戶的公鑰對r1進行HE產生的，

*x*是基於對T1、T1'和T1"進行雜湊處理產生的。

【第6項】

如請求項5所述的電腦實施方法，其中，基於確定性HE的特性確定該第一隨機數、該第二隨機數和該第三隨

機數是否相同。

【第7項】

如請求項5所述的電腦實施方法，其中，若以下條件成立，則確定該第一隨機數、該第二隨機數和該第三隨機數相同：

$g^{r2}h^{t2}$=T^{x}T1、HE_A(*r2*)=T'^{x}T1'且HE_B(*r2*)=T"^{x}T1"，

其中，T=$g^{r}h^{t}$，T'=HE_A(*r*)且T"=HE_B(*r*)，且

HE_A(*r*)和HE_A(*r2*)是分別基於利用該第一帳戶的公鑰對*r*和*r2*進行HE產生的，

HE_B(*r*)和HE_B(*r2*)是基於利用該第二帳戶的公鑰對*r*和*r2*進行HE產生的。

【第8項】

如請求項1所述的電腦實施方法，其中，T、T'和T"形成該交易金額*t*的密文。

【第9項】

一種耦接到一個或多個處理器且其上儲存有指令的非暫態電腦可讀儲存媒體，當由該一個或多個處理器執行該指令時，促使該一個或多個處理器根據請求項1-8中一個或多個所述的方法執行操作。

【第10項】

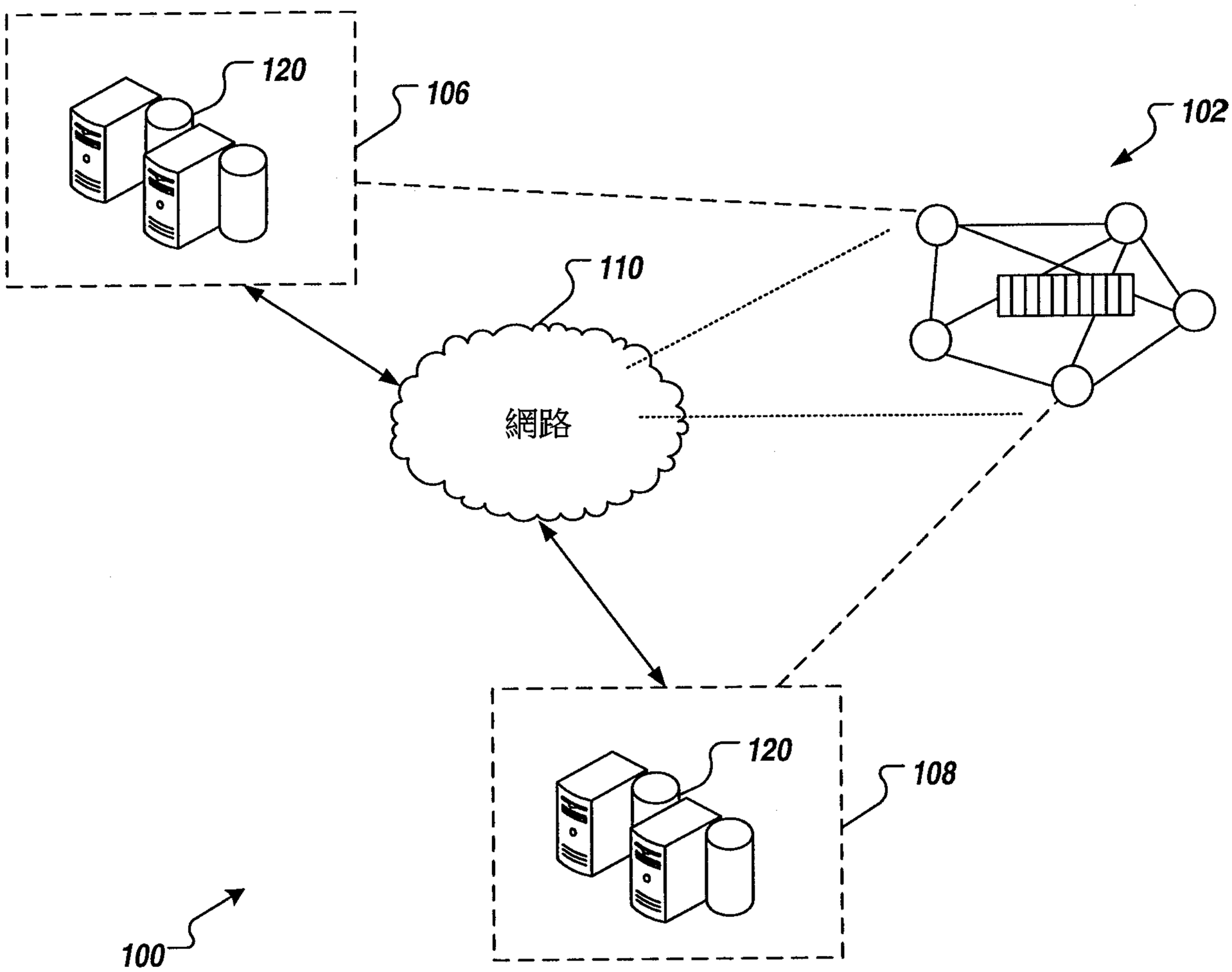
一種用於使用同態加密的區塊鏈資料保護的系統，包括：

計算設備，以及

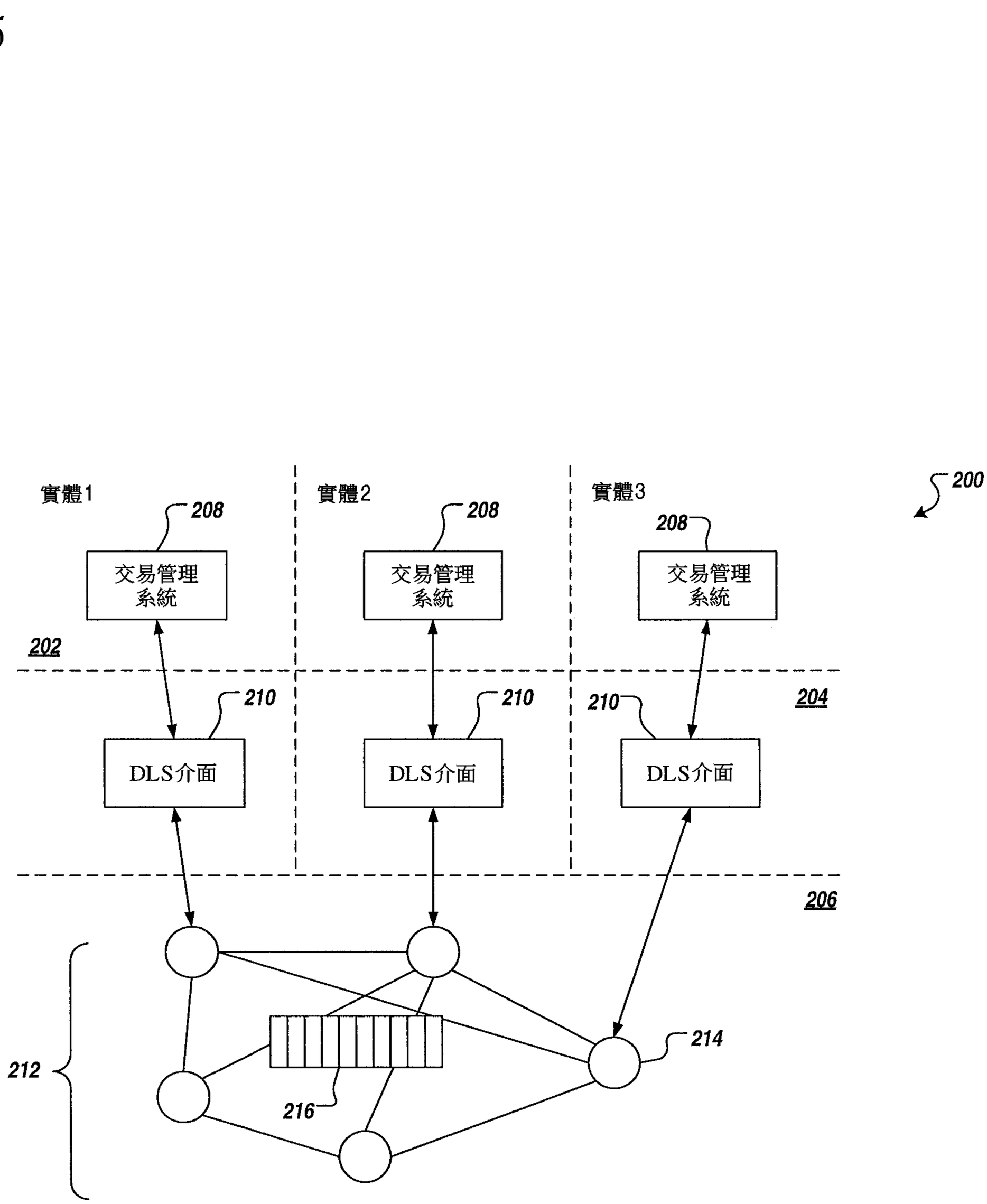
耦接到該計算設備且其上儲存有指令的電腦可讀儲存

設備，當由該計算設備執行該指令時，促使該計算設備根據請求項1-8中一個或多個所述的方法執行操作。

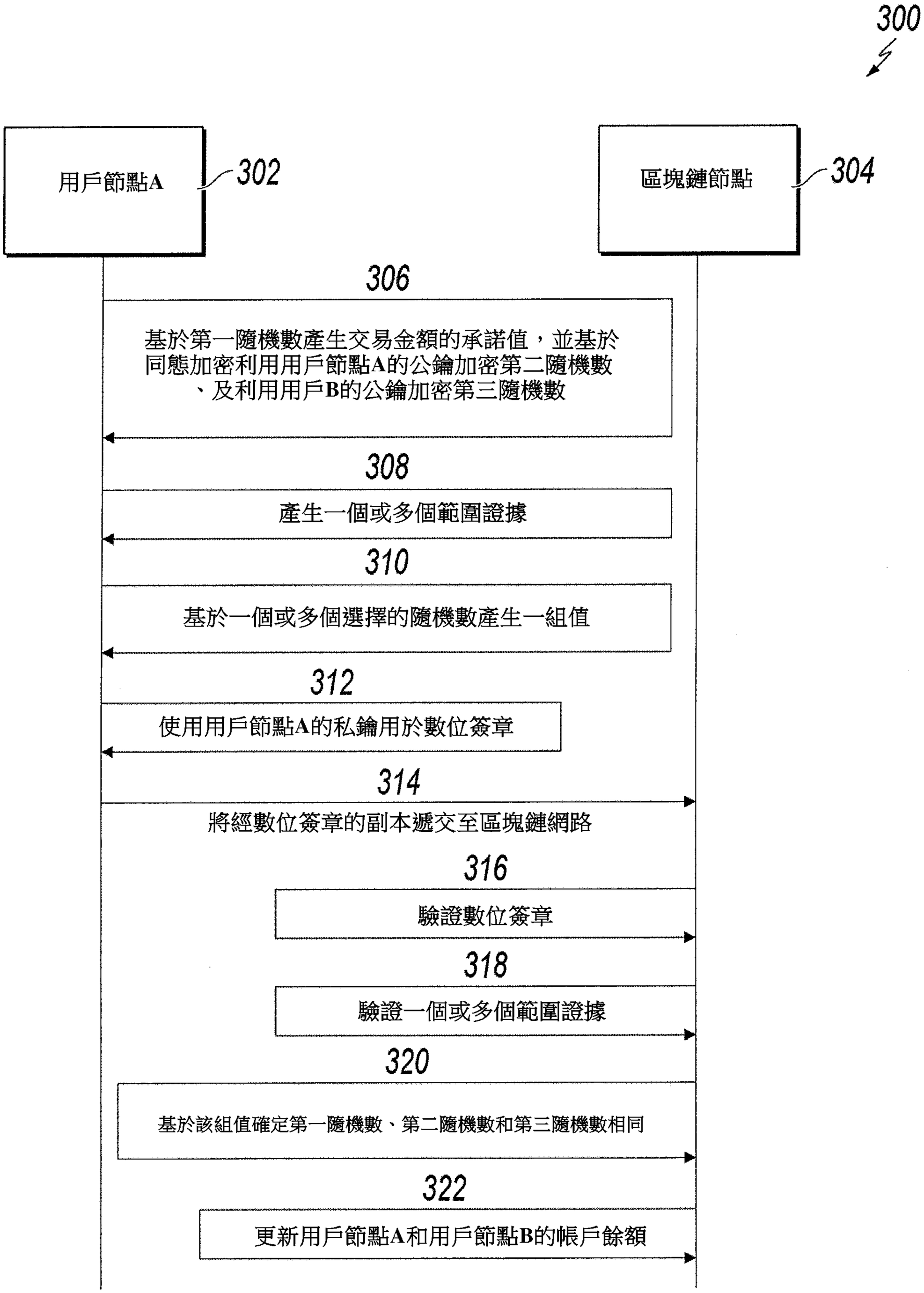
【發明圖式】



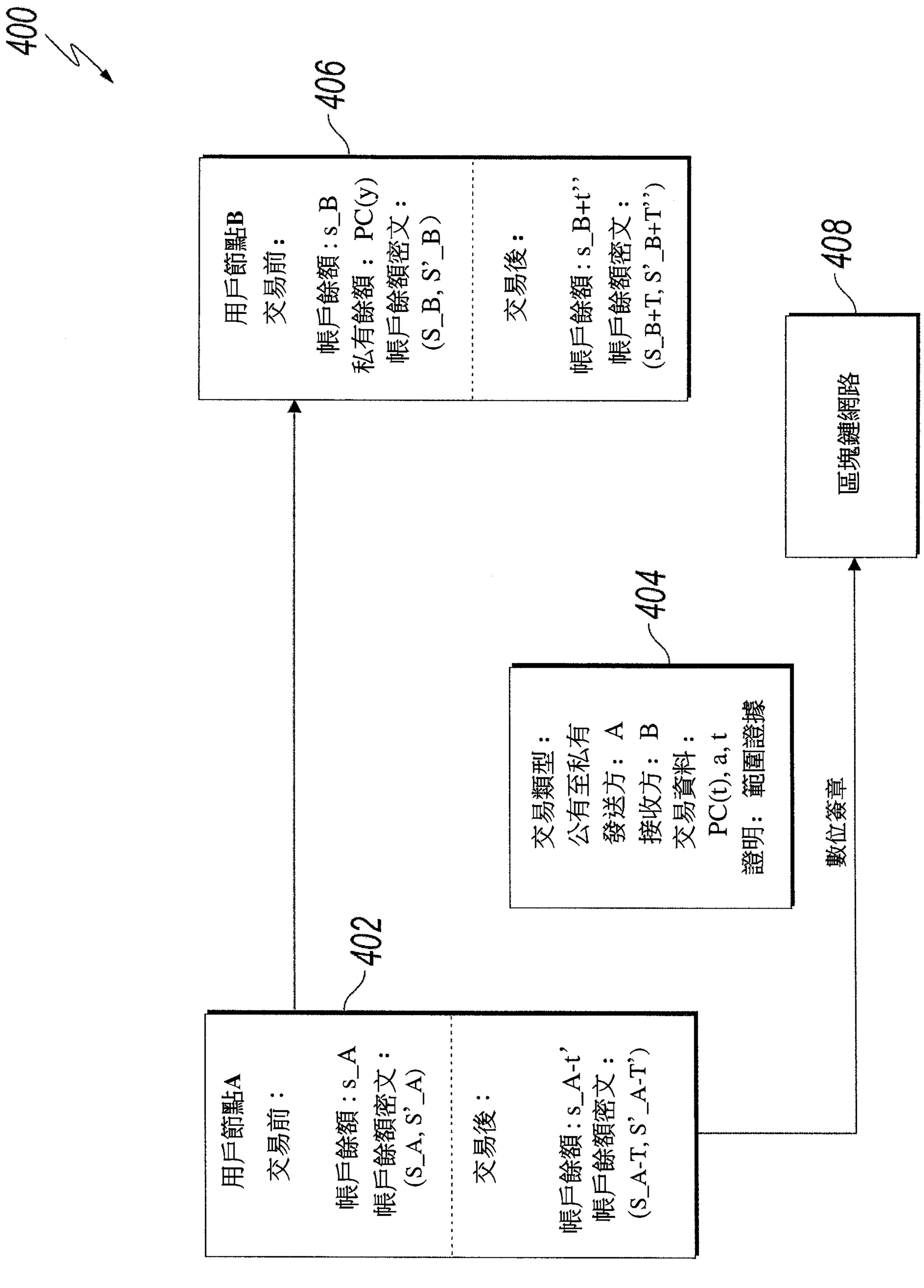
【圖 1】


實體1
實體2
實體3
200
208
208
208
交易管理系統
交易管理系統
交易管理系統
202
204
206
210
210
210
DLS介面
DLS介面
DLS介面
212
214
216

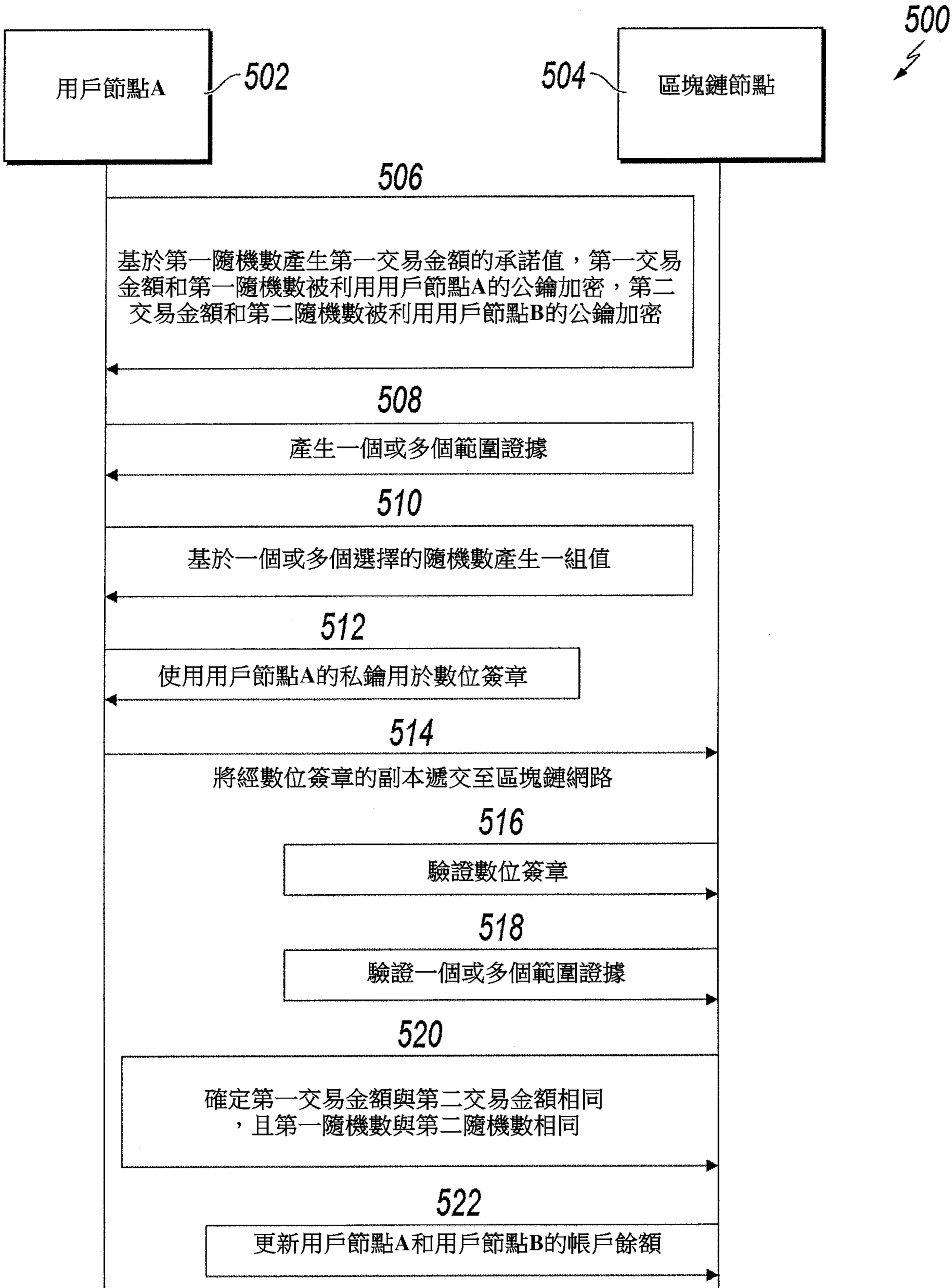
【圖 2】


300
用戶節點A
302
區塊鏈節點
304
306
基於第一隨機數產生交易金額的承諾值，並基於同態加密利用用戶節點A的公鑰加密第二隨機數、及利用用戶B的公鑰加密第三隨機數
308
產生一個或多個範圍證據
310
基於一個或多個選擇的隨機數產生一組值
312
使用用戶節點A的私鑰用於數位簽章
314
將經數位簽章的副本遞交至區塊鏈網路
316
驗證數位簽章
318
驗證一個或多個範圍證據
320
基於該組值確定第一隨機數、第二隨機數和第三隨機數相同
322
更新用戶節點A和用戶節點B的帳戶餘額

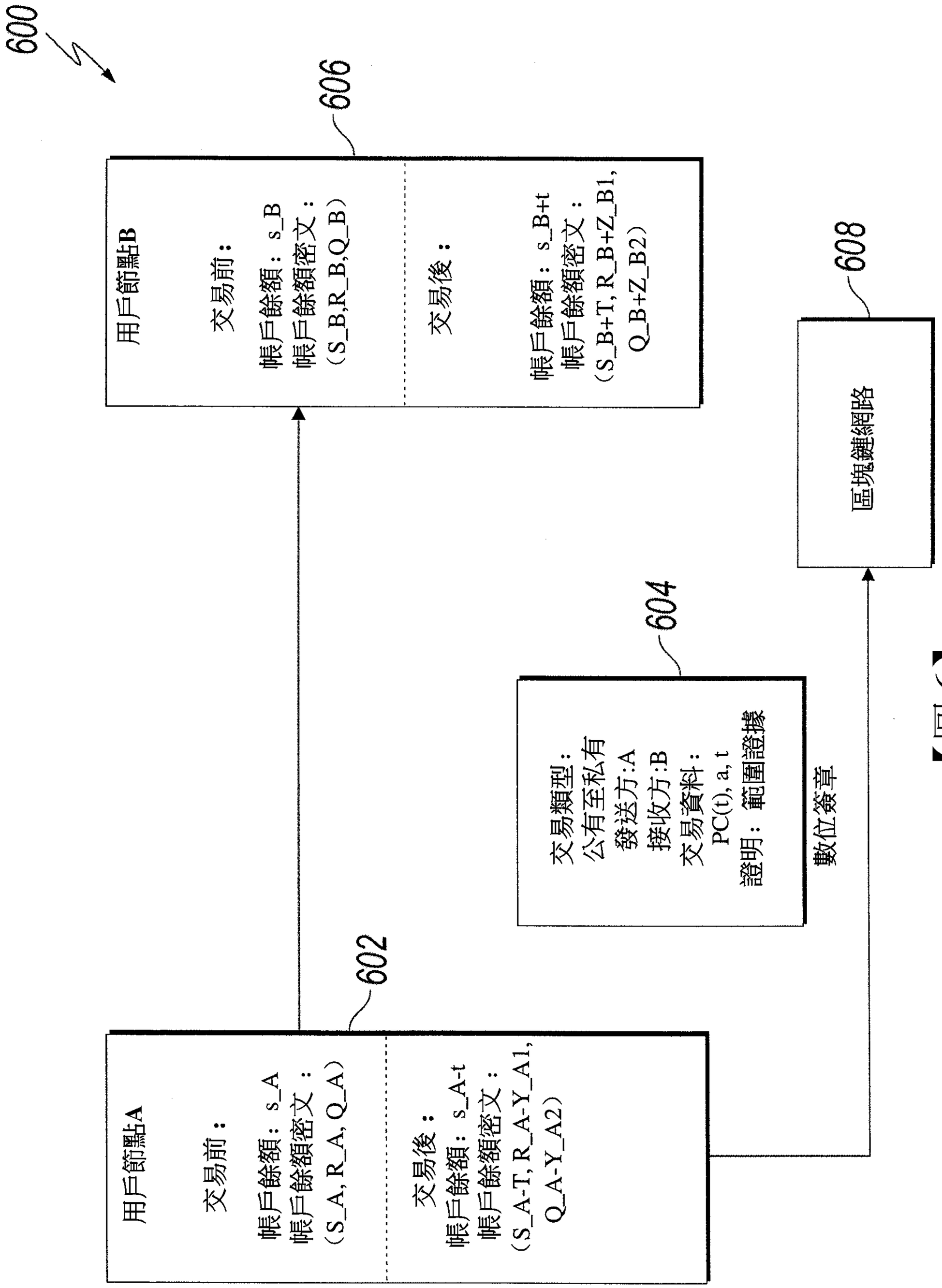
【圖 3】


400
406
用戶節點B
交易前：
帳戶餘額：s_B
私有餘額： PC(y)
帳戶餘額密文：
(S_B, S'_B)
交易後：
帳戶餘額：s_B+t''
帳戶餘額密文：
(S_B+T, S'_B+T'')
404
408
區塊鏈網路
交易類型：
公有至私有
發送方： A
接收方： B
交易資料：
PC(t), a, t
證明： 範圍證據
數位簽章
402
用戶節點A
交易前：
帳戶餘額：s_A
帳戶餘額密文：
(S_A, S'_A)
交易後：
帳戶餘額：s_A-t'
帳戶餘額密文：
(S_A-T, S'_A-T')

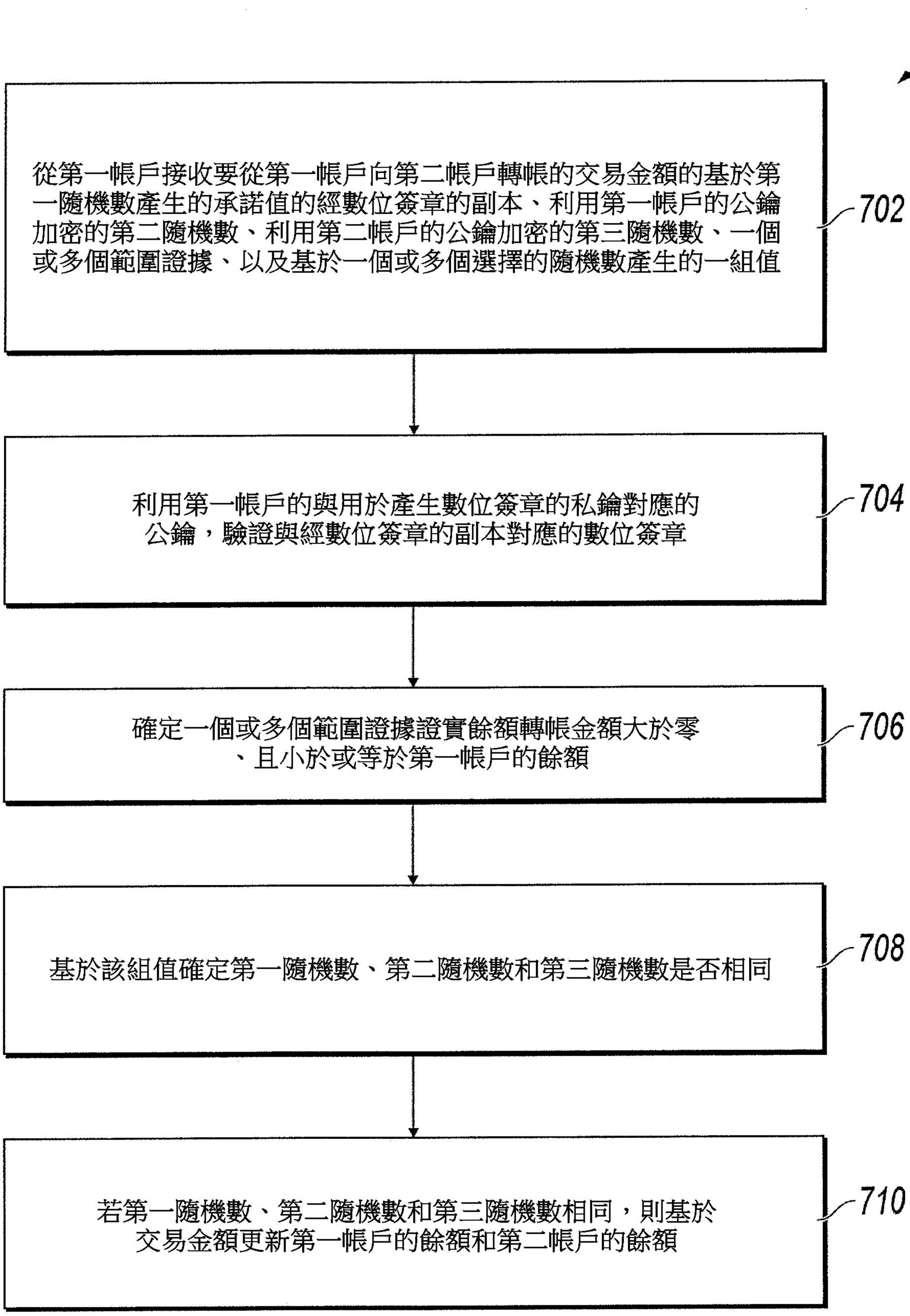
【圖 4】


500
用戶節點A
502
504
區塊鏈節點
506
基於第一隨機數產生第一交易金額的承諾值，第一交易金額和第一隨機數被利用用戶節點A的公鑰加密，第二交易金額和第二隨機數被利用用戶節點B的公鑰加密
508
產生一個或多個範圍證據
510
基於一個或多個選擇的隨機數產生一組值
512
使用用戶節點A的私鑰用於數位簽章
514
將經數位簽章的副本遞交至區塊鏈網路
516
驗證數位簽章
518
驗證一個或多個範圍證據
520
確定第一交易金額與第二交易金額相同，且第一隨機數與第二隨機數相同
522
更新用戶節點A和用戶節點B的帳戶餘額

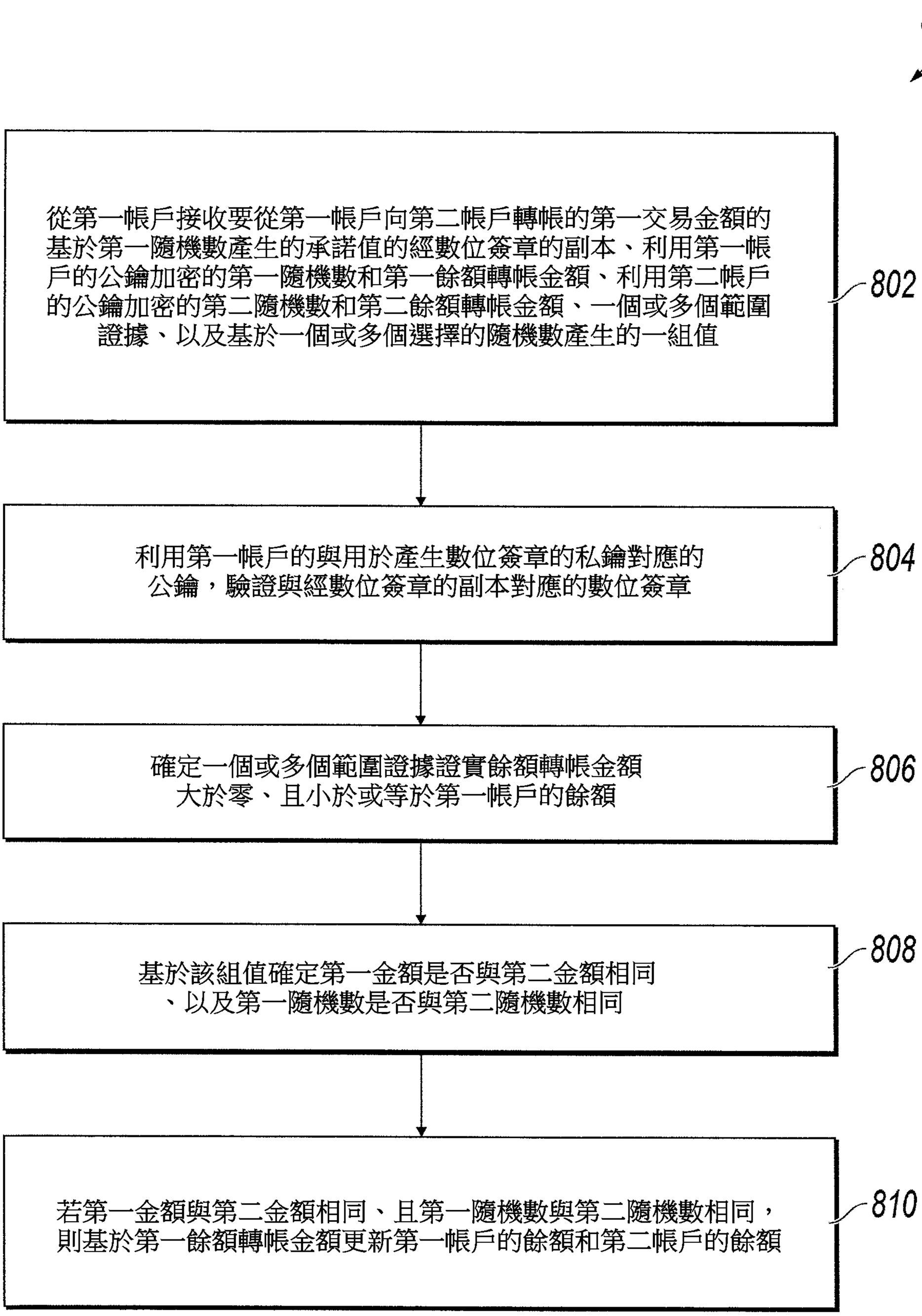
【圖 5】


600
606
用戶節點B
交易前：
帳戶餘額：s_B
帳戶餘額密文：
（S_B,R_B,Q_B）
交易後：
帳戶餘額：s_B+t
帳戶餘額密文：
（S_B+T, R_B+Z_B1,
Q_B+Z_B2）
604
608
區塊鏈網路
交易類型：
公有至私有
發送方:A
接收方:B
交易資料：
PC(t), a, t
證明：範圍證據
數位簽章
602
用戶節點A
交易前：
帳戶餘額：s_A
帳戶餘額密文：
（S_A, R_A, Q_A）
交易後：
帳戶餘額：s_A-t
帳戶餘額密文：
（S_A-T, R_A-Y_A1,
Q_A-Y_A2）

【圖6】


700
從第一帳戶接收要從第一帳戶向第二帳戶轉帳的交易金額的基於第一隨機數產生的承諾值的經數位簽章的副本、利用第一帳戶的公鑰加密的第二隨機數、利用第二帳戶的公鑰加密的第三隨機數、一個或多個範圍證據、以及基於一個或多個選擇的隨機數產生的一組值
702
利用第一帳戶的與用於產生數位簽章的私鑰對應的公鑰，驗證與經數位簽章的副本對應的數位簽章
704
確定一個或多個範圍證據證實餘額轉帳金額大於零、且小於或等於第一帳戶的餘額
706
基於該組值確定第一隨機數、第二隨機數和第三隨機數是否相同
708
若第一隨機數、第二隨機數和第三隨機數相同，則基於交易金額更新第一帳戶的餘額和第二帳戶的餘額
710

【圖 7】


800
從第一帳戶接收要從第一帳戶向第二帳戶轉帳的第一交易金額的基於第一隨機數產生的承諾值的經數位簽章的副本、利用第一帳戶的公鑰加密的第一隨機數和第一餘額轉帳金額、利用第二帳戶的公鑰加密的第二隨機數和第二餘額轉帳金額、一個或多個範圍證據、以及基於一個或多個選擇的隨機數產生的一組值
802
利用第一帳戶的與用於產生數位簽章的私鑰對應的公鑰，驗證與經數位簽章的副本對應的數位簽章
804
確定一個或多個範圍證據證實餘額轉帳金額大於零、且小於或等於第一帳戶的餘額
806
基於該組值確定第一金額是否與第二金額相同、以及第一隨機數是否與第二隨機數相同
808
若第一金額與第二金額相同、且第一隨機數與第二隨機數相同，則基於第一餘額轉帳金額更新第一帳戶的餘額和第二帳戶的餘額
810

【圖 8】