201812630

(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 201812630 A

(43)公開日： 中華民國 107 (2018) 年 04 月 01 日

(21)申請案號：106131301 (22)申請日： 中華民國 106 (2017) 年 09 月 12 日

(51)Int. Cl.： *G06F21/31 (2013.01)* *H04L9/32 (2006.01)*

(30)優先權：2016/09/12 中國大陸 201610815590.2

2016/09/12 中國大陸 201610818053.3

2016/09/12 中國大陸 201610818054.8

(71)申請人：大陸商上海鼎利信息科技有限公司 (中國大陸) SHANGHAI DINGLI INFORMATION TECHNOLOGY CO. LTD. (CN)

中國大陸

(72)發明人：陸揚 LU, YANG (CN)

(74)代理人：李文賢

申請實體審查：無 申請專利範圍項數：1 項 圖式數：1 共 20 頁

(54)名稱

區塊鏈身份系統

(57)摘要

一種區塊鏈身份系統，包含用戶端、雲端，所述用戶端由射頻讀取模組、計算平臺、觸控式螢幕模組、通訊模組、智慧身份卡組成，雲端由區塊鏈多節點網路組成，區塊鏈多節點網路包括資料區塊鏈以及多節點網路，多節點網路負責與用戶端之間協調完成身份的生成過程以及身份認證過程。本認證系統使用智慧身份卡保證用戶身份的安全性，將傳輸的資訊加密後再進行傳輸，保證不會在傳輸的過程中洩漏資訊，保證兩次認證的有效性，避免認證過程中遭受不必要的攻擊。

指定代表圖：

TW 201812630 A

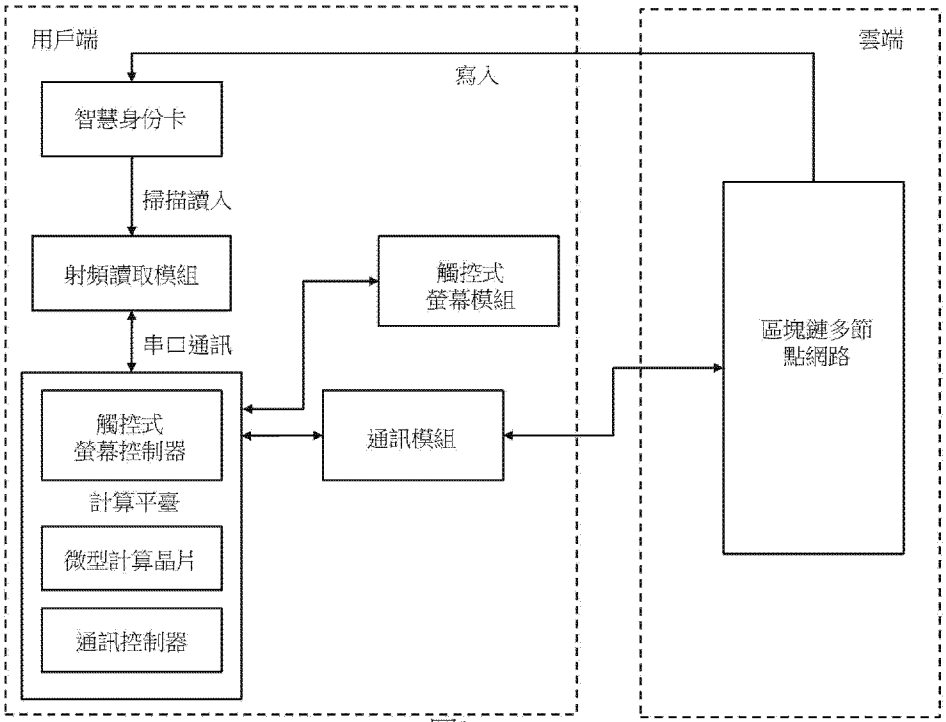

圖1

201812630

【發明摘要】

【中文發明名稱】　區塊鏈身份系統

【中文】

一種區塊鏈身份系統，包含用戶端、雲端，所述用戶端由射頻讀取模組、計算平臺、觸控式螢幕模組、通訊模組、智慧身份卡組成，雲端由區塊鏈多節點網路組成，區塊鏈多節點網路包括資料區塊鏈以及多節點網路，多節點網路負責與用戶端之間協調完成身份的生成過程以及身份認證過程。本認證系統使用智慧身份卡保證用戶身份的安全性，將傳輸的資訊加密後再進行傳輸，保證不會在傳輸的過程中洩漏資訊，保證兩次認證的有效性，避免認證過程中遭受不必要的攻擊。

【指定代表圖】　圖1

【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】　區塊鏈身份系統

【技術領域】

【0001】 本發明係關於網際網路上的身份生成以及認證，一種區塊鏈身份系統。

【先前技術】

【0002】在網際網路中，區塊鏈身份需要依靠網路資料的形式進行頒發，與傳統的身份不同，網際網路上的身份對生成及認證過程的難度更大。對於目前廣泛使用的基於密碼的認證機制或基於簡訊的身份認證中，如果密碼一旦洩漏或者手機不慎丟失，其他用戶同樣可以使用該終端進行認證交易。另外近年來開始出現結合生物特徵資訊(例如指紋、虹膜等)來增加認證安全性的技術。然而就當前環境下，如果在要進行身份認證之前必須要先接受自己的指紋等生物特徵資訊被一協力廠商系統採集保存，對於一普通用戶來說尚不容易接受，用戶很可能因為擔心個人資訊洩漏。因此，現今極需一種安全性高、可操作性高、方便的區塊鏈身份系統。

【發明內容】

【0003】有鑑於此，本發明提供一種解決或部分解決上述問題的區塊鏈身份系統。

【0004】為達到上述技術方案的效果，本發明的技術方案為：一種區塊鏈身份系統，包含用戶端、雲端，用戶端由射頻讀取模組、計算平臺、觸控式螢幕模組、通訊模組、智慧身份卡組成，雲端由區塊鏈多節點網路

組成，區塊鏈多節點網路包括資料區塊鏈以及多節點網路，多節點網路負責與用戶端之間協調完成身份的生成過程以及身份認證過程；

【0005】計算平臺的內部包含觸控式螢幕控制器、通訊控制器及微型計算晶片；

【0006】觸控式螢幕控制器用於控制觸控式螢幕模組的顯示，將需要顯示的資訊發送給所述觸控式螢幕模組；

【0007】通訊控制器以串口通訊的方式調度射頻讀取模組、觸控式螢幕模組及通訊模塊之間的交互通訊；

【0008】微型計算晶片用於處理所述身份的生成過程以及身份認證過程中的資訊；

【0009】智慧身份卡內含內建積體電路的晶片，晶片包含存有用戶ID編號，每個智慧身份卡的用戶ID編號都是唯一的，用於識別用戶身份，智慧身份卡由專門的廠商通過專門的設備生產，是不可複製的硬體，智慧身份卡由註冊過的合法用戶攜帶，認證時必須將智慧身份卡經過射頻讀取模組掃描讀入其中的用戶ID編號，以驗證用戶的身份；

【0010】觸控式螢幕模組採用五線電阻屏，依靠壓力感應原理，用於顯示以及輸入在身份的生成過程以及身份認證過程中所需的資訊；

【0011】通訊模組用於接收和發送相關資訊，內含網路傳輸篩檢程式及專用編碼晶片以實現計算平臺與雲端之間的通訊，並以資料幀的方式實現網路資料的接收和發送，並且還要在接收和發送時避免背景雜訊及干擾，資料幀的編碼方式為相位編碼，並採取同步時鐘編碼技術，在傳輸資料資訊的同時，也將時鐘同步信號一起傳輸到對方；

【0012】在雲端的所述區塊鏈多節點網路中，區塊鏈多節點網路中的資料區塊鏈由一串按創建的時間順序相連的資料區塊組成，區塊鏈多節點網路中的多節點網路是由多個節點構成的P2P網路，節點之間通過網路共用及互相傳輸資訊，資料區塊鏈對多節點網路中所有所述節點都是開放的，資料區塊由區塊頭以及區塊主體組成，區塊頭包含前一資料區塊的哈希值、時間戳、當前資料區塊的哈希值，前一資料區塊的哈希值用於不同資料區塊的連接，時間戳記錄當前資料區塊連接的時間，當前資料區塊的哈希值用於確保資料區塊的內容不會被篡改，區塊主體記錄了用戶身份的帳戶資訊，其中合法的用戶身份的帳戶資訊為：用戶名、用戶身份資訊、加密後的用戶密碼、加密後的用戶ID編號、用戶公鑰；

【0013】節點中包含偽亂數產生器；

【0014】身份生成過程如下：

【0015】1）用戶在觸控式螢幕模組上輸入用戶名、用戶身份資訊、用戶密碼，並將用戶名、用戶身份資訊、用戶密碼傳輸給多節點網路，多節點網路檢驗用戶名在資料區塊鏈中是否存在，如果用戶名不存在，進行下一步，如果用戶名存在，傳送回饋資訊經由通訊模組傳送給計算平臺，計算平臺將回饋資訊處理，在觸控式螢幕模組上顯示“用戶存在，重新輸入”，用戶在觸控式螢幕模組上重新輸入用戶名，多節點網路重新檢驗用戶名在資料區塊鏈是否存在；

【0016】2）計算平臺驗證所述用戶密碼是否符合要求，如果用戶密碼符合要求，進行下一步，如果不符合要求傳輸給觸控式螢幕模組，在觸控式螢幕模組上顯示“用戶密碼不符合要求，重新輸入”，用戶在觸控式

螢幕模組上重新輸入用戶密碼；

【0017】3）多節點網路產生亂數S1，並且亂數S1經過IDEA加密演算法進行加密生成加密後的亂數S1，將加密後的亂數S1廣播給多節點網路中所有節點，所有節點利用IDEA解密演算法解密加密後的亂數S1，最先解密出亂數S1的節點作為負責構建資料區塊鏈的節點；

【0018】4）負責構建資料區塊鏈的節點分配給用戶一個用戶公鑰，並通過哈希演算法將用戶身份資訊生成唯一的身份標識，負責構建資料區塊鏈的節點將生成後的唯一的身份標識進行數位簽章生成唯一的用戶ID編號，將用戶ID編號寫入智慧身份卡，由用戶公鑰進行加密生成加密後的用戶ID編號，把當前時間保存為當前資料區塊的時間戳，前一資料區塊的哈希值通過安全散列演算法生成當前資料區塊的哈希值，並且生成加密後的用戶密碼，生成加密後的用戶密碼的具體過程為：使用負責構建資料區塊鏈的節點中的偽亂數產生器生成的亂數作為鹽值，將鹽值混入用戶密碼，並使用所述加密哈希函數進行加密，生成加密後的用戶密碼；將用戶名、用戶身份資訊、加密後的用戶密碼、加密後的用戶ID編號、用戶公鑰組成用戶身份的帳戶資訊，與產生的鹽值一起寫入當前資料區塊的區塊主體中；

【0019】偽亂數產生器的工作原理如下：

【0020】偽亂數產生器基於資料加密標準，包含三重資料加密標準演算法，可以循環地產生亂數；用變數i表示第i輪亂數的產生計算，主要有3個組成部分：

【0021】1)輸入部分：輸入部分是兩個64位元的偽亂數$Date_i$及V_i，

其中，$Date_i$表示第i輪計算開始時的日期和時間，每產生一個亂數Ri後，$Date_i$需要更新一次，V_i是產生第i個亂數時需要輸入的種子，其初值可任意設定，以後每輪計算都會自動更新；

【0022】2)密鑰產生器：用於每輪的具體計算，每輪計算都使用了三重資料演算法加密，每次加密使用兩個固定的56位元的密鑰K1和密鑰K2，這兩個密鑰必須保密，由偽亂數產生器指定；

【0023】3)輸出部分：輸出為一個64位元的偽亂數Ri和一個64位元的新種子V_{i+1}；偽亂數產生器具有很高的安全強度，因為其採用了總共112位元長的密鑰和3個密鑰加密的資料演算法加密，同時還由於有兩個偽亂數輸入驅動，兩個偽亂數輸入一個是當前的日期和時間$Date_i$，另一個是上一輪產生的種子V_i，每輪都產生亂數Ri，但是每輪種子不同，產生的亂數都不相同，因此，為每個用戶產生的鹽值也不相同，所以無法通過上一輪產生的鹽值來推斷下一輪產生的鹽值；

【0024】身份認證過程如下：

【0025】第一步，用戶端向雲端發出認證請求，將智慧身份卡中所存的用戶ID編號經由射頻讀取模組讀入，多節點網路檢測在資料區塊鏈中是否存在，如果存在再進行第二步，如果不存在結束身份認證過程；

【0026】第二步，初次認證，雲端經由通訊模組回饋給計算平臺開始認證的資訊，計算平臺處理開始認證的資訊，開始認證的資訊在觸控式螢幕模組顯示提示用戶輸入，用戶在觸控式螢幕模組輸入用戶名和用戶密碼後，初步驗證用戶，根據收到的用戶名，多節點網路判斷其合法性，如果是合法用戶，再檢驗用戶密碼是否正確，從區塊鏈多節點網路中取出用

戶的鹽值，將鹽值混入用戶輸入的密碼，並且使用加密哈希函數進行加密，比較結果和對應資料區塊儲存的加密後的用戶密碼是否相同，如果相同那麼初步判斷用戶輸入的密碼正確，進入第三步，如果不相同則判斷用戶輸入的密碼不一致；

【0027】第三步，二次認證，計算平臺選取大素數p及整數a，並將這兩個數公開，即這兩個數對用戶端與多節點網路都可見，多節點網路選取隨機的大素數x，大素數x滿足x<p-1，計算$a^x \bmod p$，大素數x的值保密，只對多節點網路可見；用戶端將用戶密碼及用戶的鹽值級聯，計算散列值Z1，並生成亂數S1，將計算後的散列值Z1與計算後的$a^x \bmod p$的值、亂數S1級聯再進行一次散列運算得到散列值Z2，用戶端連同亂數S1、將計算後的$a^x \bmod p$的值和散列值Z2一起發送給多節點網路；

【0028】第四步，多節點網路取出存儲在資料區塊鏈的加密後的用戶密碼；與收到的亂數S1、將計算後的$a^x \bmod p$級聯再進行散列運算得到散列值Z3，與散列值Z2進行比較，相等則繼續，否則判斷不一致，多節點網路隨機選取大素數y，滿足y<q，計算$a^y \bmod p$，並將大素數y的值保密；多節點網路將加密後的用戶密碼、亂數S1和計算後的$a^y \bmod p$的值再次級聯進行散列運算得到散列值Z4，並且將散列值Z4、將計算後的$a^y \bmod p$的值發送給用戶端；

【0029】第五步，用戶端將在第三步得到的散列值Z1、將計算後的$a^y \bmod p$和亂數S1級聯進行散列運算，將計算結果和第四步收到的消息中的散列值Z4進行比較，相等則回送給雲端一個認證成功的應答信號，否則返回認證失敗的消息；

【0030】經過以上五個步驟，雲端與用戶端都成功地驗證了對方的身份；

【0031】區塊鏈身份系統採用的通訊模式是一種開放系統結構的網路方式，由用戶端首先向雲端提出請求，雲端對請求做相應的處理並執行請求中包含的任務，然後將結果返回給用戶端。

【0032】本區塊鏈身份系統的優點如下：

【0033】(1)使用智慧身份卡，以保證用戶身份的安全性。

【0034】(2)將密碼資訊及智慧身份卡的ID資訊都加密，而不傳輸資訊明文，這樣即使入侵者通過網路偵聽等手段獲得通道的傳輸資訊，也無需擔心用戶密碼和身份證資訊被洩漏。

【0035】(3)身份生成過程以及身份認證過程使用了複雜的加密過程，可以有效防止重放攻擊。而且用戶端和雲端採用了二次認證，提高了認證過程中的可靠性與安全性。

【圖式簡單說明】

【0036】[圖1]為區塊鏈身份系統的結構圖。

【實施方式】

【0037】為了使本發明所要解決的技術問題、技術方案及有益效果更加清楚明白，以下結合附圖及實施例，對本發明進行詳細的說明。應當說明的是，此處所描述的具體實施例僅用以解釋本發明，並不用於限定本發明，能實現同樣功能的產品屬於等同替換和改進，均包含在本發明的保護範圍之內。具體方法如下：

【0038】實施例1：認證系統的工作流程

【0039】認證系統的工作過程如下：用戶在客戶終端的觸控式螢幕模組顯示的登入視窗上輸入用戶名密碼登入系統，進入認證系統後，觸控式螢幕模組上顯示讀卡認證介面，通過發送命令給射頻讀取模組，射頻讀取模組將用戶的智慧身份卡中的資訊讀取進來，智慧身份卡的身份讀入到計算平臺後，在處理平臺根據身份認證協議進行相應的密碼學運算，得到加密後的認證請求資訊，通訊模組通過網路通訊的方式將加密後的認證請求資訊傳送到雲端的認證伺服器，經過用戶端跟雲端的一系列的認證交互過程之後，雲端得到認證結果，並將相應的認證結果返回到用戶端進行顯示。

【0040】實施例2：身份認證協議設計

【0041】為身份認證系統安全與否的關鍵，身份認證協定的設計是整個系統的關鍵組成部分。首先介紹本文中所用符號約定：

【0042】U表示用戶；

【0043】S表示第三方認證伺服器；

【0044】ID表示射頻讀取模組讀入的身份資訊；

【0045】UserN、Password分別代表用戶名和對應登入密碼；

【0046】KuR、KuS分別代表移動用戶的公鑰和私鑰；

【0047】KsR、Kss分別代表認證伺服器的公鑰和私鑰；

【0048】EK(m)表示用密鑰k對明文m加密；

【0049】DK(C)表示用密鑰k對密文c解密；

【0050】R1、N2為系統產生的亂數；

【0051】K作為雙方身份認證成功後的會話密鑰。

【0052】首先，用戶須在第三方註冊中心進行用戶資訊註冊。註冊的時候，要求第三方註冊中心具有射頻讀取模組，以便確認用戶身份資訊，並根據從射頻裝置讀出的資訊完成用戶的註冊。註冊過程是在這樣的一個前提下進行的：整個過程都是在一個用戶完全信賴的中心完成，且註冊資訊都是通過安全通道進行的。

【0053】註冊過程如下：

【0054】(1)用戶持自己的第二代居民身份證在官方指定的場所請求註冊。註冊中心人員採用認證系統的射頻裝置掃描用戶的智慧身份卡，讀取智慧身份卡中用戶的身份ID。在認證系統讀取用戶的ID後，系統會自動查詢用戶是否已經註冊過該系統。若用戶已經註冊過此系統返回提示資訊並結束使用者註冊子協定。

【0055】(2)在確認用戶的ID沒有註冊而且符合註冊條件後，認證系統會請求用戶輸入登入密碼。使用者輸入完密碼後，系統首先使用用戶的密碼資訊生成對應於該ID的公鑰，然後根據橢圓曲線密碼演算法使用用戶公鑰加密用戶密碼，並將用戶的公鑰和用公鑰加密後的密碼和加密後的ID資訊存儲到第三方認證伺服器上。

【0056】(3)在認證伺服器將用戶的身份資訊存儲到伺服器後。第三方註冊人員將認證系統安裝程式通過移動存放裝置或者安全通道傳送安裝到用戶的移動終端。

【0057】註冊成功之後即可使用移動終端進行身份認證，具體認證過程如下：

【0058】步驟一：認證開始，首先需要在用戶端進行登入，驗證用

戶身份和對應密碼，若雲端驗證無此用戶或者用戶名和密碼不符，則返回出錯資訊，用戶需要註冊或者重新輸入帳號和正確密碼。如用戶名和與之對應的密碼正確，則進入接下來認證過程。通訊模組中的網路通道傳輸的是驗證用戶的名稱與用戶的密碼資訊，雲端驗證從資料庫中提取這兩個資訊。

【0059】步驟二：登入成功之後，進入掃描智慧身份卡認證階段，用戶U使用移動終端設備將用戶身份證獲得身份卡ID資訊讀取到認證系統中，具體過程如下：

【0060】(1)用戶通過射頻讀卡設備讀入身份卡資訊ID後，首先在移動設備終端進行以下計算：

【0061】①使用用戶公鑰KuR加密身份ID得到加密後的用戶ID，利用隨機序列發生器產生亂數N1，並使用伺服器的公鑰計算認證請求，並暫存亂數R1。

【0062】②發送消息認證請求，認證請求中包含加密後的用戶ID資訊及亂數N1，並且需要將亂數RI暫時保存。

【0063】(2)伺服器收到用戶發送的認證請求後：

【0064】①雲端用私鑰根據橢圓曲線密碼演算法模組解密認證請求，得到用戶的ID加密後資訊和用戶發送的亂數R1，然後伺服器查找該ID加密資訊是否跟認證資料庫中userN用戶所對應的EncipherID表項相符；若不相符，則返回出錯資訊，認證失敗，即每個用戶名跟其身份ID資訊是一對應綁定的，即使入侵者竊取到用戶名密碼登入系統由於不能掃入與之相對應的ID加密資訊，亦不能通過認證。

【0065】②若①中得到的ID加密資訊驗證正確，此時伺服器保存用戶發送的亂數N1。同時伺服器利用隨機序列發生器產生亂數N2，然後利用橢圓曲線密碼演算法模組和用戶的公鑰計算應答資訊，並發送至用戶端進行驗證。

【0066】(3)用戶收到伺服器的應答資訊，會進行一下計算：

【0067】①首先用戶用自己的私鑰解密應答資訊，此時用戶將獲得的N1與以前保存R1相比較，若兩者不相等，則用戶對伺服器的認證失敗(伺服器可能被冒充)，拒絕伺服器，認證結束。

【0068】②若亂數N1相等，則用戶認證伺服器成功。同時用戶生成會話對稱密鑰K，計算伴隨著亂數N2的回應資訊，然後發送回應資訊至伺服器請求驗證。

【0069】(4)伺服器接收到用戶的回應資訊後，進行如下計算：

【0070】①首先伺服器用自己的私鑰解密得到亂數N2。

【0071】②伺服器首先比較亂數N2與保存的是否相等，若兩者不相等，則伺服器驗證用戶失敗。

【0072】本區塊鏈身份系統的優點如下：

【0073】(1)使用智慧身份卡，以保證用戶身份的安全性。

【0074】(2)將密碼資訊及智慧身份卡的ID資訊都加密，而不傳輸資訊明文，這樣即使入侵者通過網路偵聽等手段獲得通道的傳輸資訊，也無需擔心用戶密碼和身份證資訊被洩漏。

【0075】(3)身份生成過程以及身份認證過程使用了複雜的加密過程，可以有效防止重放攻擊。而且用戶端和雲端採用了二次認證，提高了

認證過程中的可靠性與安全性。

【0076】以上所述僅為本發明之較佳實施例，並非用以限定本發明的申請專利範圍保護範圍。同時以上說明，對於相關技術領域的技術人員應可以理解及實施，因此其他基於本發明所揭示內容所完成的等同改變，均應包含在本申請專利範圍的涵蓋範圍內。

【符號說明】

【0077】 無

【發明申請專利範圍】

【第1項】一種區塊鏈身份系統，其特徵在於，包含用戶端、雲端，所述用戶端由射頻讀取模組、計算平臺、觸控式螢幕模組、通訊模組、智慧身份卡組成，所述雲端由區塊鏈多節點網路組成，所述區塊鏈多節點網路包括資料區塊鏈以及多節點網路，所述多節點網路負責與所述用戶端之間協調完成身份的生成過程以及身份認證過程，並且在其中調用所述資料區塊鏈；

所述計算平臺的內部包含觸控式螢幕控制器、通訊控制器及微型計算晶片；

所述觸控式螢幕控制器用於控制所述觸控式螢幕模組的顯示，將需要顯示的資訊發送給所述觸控式螢幕模組；

所述通訊控制器以串口通訊的方式調度所述射頻讀取模組、所述觸控式螢幕模組及所述通訊模組之間的交互通訊；

所述微型計算晶片用於處理所述身份的生成過程以及所述身份認證過程中的資訊；

所述智慧身份卡內建積體電路的晶片，所述晶片存有用戶ID編號，每個所述智慧身份卡的所述用戶ID編號都是唯一的，用於識別用戶身份，所述智慧身份卡由專門的廠商通過專門的設備生產，是不可複製的硬體，所述智慧身份卡由註冊過的合法用戶攜帶，認證時必須將所述智慧身份卡經過所述射頻讀取模組掃描讀入其中的所述用戶ID編號，以驗證用戶的身份；

所述觸控式螢幕模組採用五線電阻屏，依靠壓力感應原理，用於顯示以及輸入在所述身份的生成過程以及所述身份認證過程中所需的資訊；

所述通訊模組用於接收和發送相關資訊，內含網路傳輸篩檢程式及專用

編碼晶片以實現所述計算平臺與所述雲端之間的通訊，並以資料幀的方式實現網路資料的接收和發送，並且還要在接收和發送時避免背景雜訊及干擾，所述資料幀的編碼方式為相位編碼，並採取同步時鐘編碼技術，在傳輸資料資訊的同時，也將時鐘同步信號一起傳輸到對方；

在所述區塊鏈多節點網路中，所述資料區塊鏈由一串按創建的時間順序相連的資料區塊組成，所述多節點網路是由多個節點構成的P2P網路，所述節點之間通過網路共用資訊及互相傳輸資訊，所述資料區塊鏈對所述多節點網路中所有所述節點都是開放的，所述資料區塊由區塊頭以及區塊主體組成，所述區塊頭包含前一資料區塊的哈希(Hash)值、時間戳、當前資料區塊的哈希值，所述前一資料區塊的哈希值用於不同所述資料區塊的連接，所述時間戳記錄當前所述資料區塊連接的時間，當前所述資料區塊的哈希值用於確保所述資料區塊的內容不會被篡改，所述區塊主體記錄了用戶身份的帳戶資訊，其中合法的所述用戶身份的帳戶資訊為：用戶名、用戶身份資訊、加密後的用戶密碼、加密後的所述用戶ID編號、用戶公鑰；

每個所述節點包含偽亂數產生器；

所述身份生成過程如下：

1）用戶在所述觸控式螢幕模組上輸入所述用戶名、所述用戶身份資訊、所述用戶密碼，並將所述用戶名、所述用戶身份資訊、所述用戶密碼傳輸給所述多節點網路，所述多節點網路檢驗所述用戶名在所述資料區塊鏈中是否存在，如果所述用戶名不存在，進行下一步，如果所述用戶名存在，傳送回饋資訊經由所述通訊模組傳送給所述計算平臺，所述計算平臺將所述回饋資訊處理，在所述觸控式螢幕模組上顯示“用戶存在，重新輸入”，用戶在所

述觸控式螢幕模組上重新輸入所述用戶名，所述多節點網路重新檢驗用戶名在所述資料區塊鏈是否存在；

2）所述計算平臺驗證所述用戶密碼是否符合要求，如果所述用戶密碼符合要求，進行下一步，如果不符合要求傳輸給所述觸控式螢幕模組，在所述觸控式螢幕模組上顯示“用戶密碼不符合要求，重新輸入”，用戶在所述觸控式螢幕模組上重新輸入所述用戶密碼；

3）所述多節點網路產生亂數S1，並且所述亂數S1經過IDEA加密演算法進行加密生成加密後的所述亂數S1，將所述加密後的所述亂數S1廣播給所述多節點網路中所有所述節點，所有所述節點利用IDEA解密演算法解密加密後的所述亂數S1，最先解密出所述亂數S1的節點作為負責構建資料區塊鏈的節點；

4）所述負責構建資料區塊鏈的節點分配給用戶一個用戶公鑰，並通過哈希演算法將所述用戶身份資訊生成唯一的身份標識，所述負責構建資料區塊鏈的節點將生成後的所述唯一的身份標識進行數位簽章生成唯一的所述用戶ID編號，將所述用戶ID編號寫入所述智慧身份卡，由所述用戶公鑰進行加密生成所述加密後的所述用戶ID編號，把當前時間保存為所述當前資料區塊的時間戳，所述前一資料區塊的哈希值通過安全散列演算法生成所述當前資料區塊的哈希值，並且生成所述加密後的用戶密碼，所述生成所述加密後的用戶密碼的具體過程為：使用所述負責構建資料區塊鏈的節點，利用其包含的所述偽亂數產生器生成亂數，所述亂數作為用戶的鹽值，將所述用戶的鹽值混入所述用戶密碼，並使用加密哈希函數進行加密，生成所述加密後的用戶密碼；將所述用戶名、所述用戶身份資訊、所述加密後的用戶密碼、所

述加密後的用戶ID編號、所述用戶公鑰組成所述用戶身份的帳戶資訊，與所述用戶的鹽值一起寫入所述當前資料區塊的所述區塊主體中；

所述偽亂數產生器的工作原理如下：

所述偽亂數產生器基於資料加密標準，包含三重資料加密標準演算法，可以循環地產生亂數；i為自然數的變量；用於表示第i輪亂數的產生計算，主要有3個組成部分：

1)輸入部分：所述輸入部分是兩個64位元的偽亂數$Date_i$及V_i，其中，$Date_i$表示第i輪計算開始時的日期和時間，每產生一個亂數Ri後，$Date_i$需要更新一次，V_i是產生第i個亂數時需要輸入的種子，其初值可任意設定，以後每輪計算都會自動更新；

2)密鑰產生器：所述用於每輪的具體計算，每輪計算都使用了三重資料演算法加密，每次加密使用兩個固定的56位元的密鑰K1和密鑰K2，這兩個密鑰必須保密，由所述偽亂數產生器指定；

3)輸出部分：輸出為一個64位元的亂數Ri和一個64位元的新種子V_{i+1}；

所述偽亂數產生器具有很高的安全強度，因為其採用了總共112位元長的密鑰和3個密鑰加密的資料演算法加密，同時還由於有兩個偽亂數輸入驅動，所述兩個偽亂數輸入一個是當前的日期和時間$Date_i$，另一個是上一輪產生的種子V_i，每輪都產生亂數Ri，但是由於每輪種子不同，產生的亂數都不相同，因此，為每個用戶產生的亂數也不相同，所以無法通過上一輪產生的亂數來推斷下一輪產生的亂數；

所述身份認證過程如下：

第一步，所述用戶端向所述雲端發出認證請求，將所述智慧身份卡中所

存的所述用戶ID編號經由所述射頻讀取模組讀入，所述多節點網路檢測其在所述資料區塊鏈中是否存在，如果存在再進行第二步，如果不存在結束所述身份認證過程；

第二步，初次認證，所述雲端經由所述通訊模組回饋給所述計算平臺開始認證的資訊，所述計算平臺處理所述開始認證的資訊，所述開始認證的資訊在所述觸控式螢幕模組顯示提示用戶輸入所述用戶名以及所述用戶密碼，用戶在所述觸控式螢幕模組輸入後，初步驗證用戶，根據收到的輸入的所述用戶名，所述多節點網路判斷其合法性，如果是合法用戶，再檢驗輸入的所述用戶密碼是否正確，從所述區塊鏈多節點網路中取出所述用戶的鹽值，將所述用戶的鹽值混入所述輸入的所述用戶密碼，並且使用所述加密哈希函數進行加密，比較結果和對應資料區塊儲存的所述加密後的用戶密碼是否相同，如果相同那麼初步判斷所述輸入的所述用戶密碼正確，進入第三步，如果不相同則判斷所述輸入的所述用戶密碼不正確；

第三步，二次認證，所述計算平臺選取大素數p及整數a，並將這兩個數公開，即這兩個數對所述用戶端與所述多節點網路都可見，所述多節點網路選取隨機的大素數x，所述大素數x滿足x<p-1，計算$a^x \bmod p$，所述大素數x的值保密，只對所述多節點網路可見；所述用戶端將所述用戶密碼及所述用戶的鹽值級聯，計算散列值Z1，並生成亂數S1，將計算後的散列值Z1與計算後的所述$a^x \bmod p$的值、所述亂數S1級聯再進行一次散列運算得到散列值Z2，所述用戶端連同所述亂數S1、計算後的所述$a^x \bmod p$的值和所述散列值Z2一起發送給所述多節點網路；

第四步，所述多節點網路取出存儲在所述資料區塊鏈的所述加密後的用

戶密碼；與收到的所述亂數S1、計算後的所述a^x mod p的值級聯再進行散列運算得到散列值Z3，與所述散列值Z2進行比較，相等則繼續，否則判斷不一致，所述多節點網路隨機選取大素數y，滿足y<q，計算a^y mod p，並將所述大素數y的值保密；所述多節點網路將所述加密後的用戶密碼、所述亂數S1和計算後的所述a^y mod p的值再次級聯進行散列運算得到散列值Z4，並且將所述散列值Z4、計算後的所述a^y mod p的值發送給所述用戶端；

第五步，所述用戶端將在第三步得到的所述散列值Z1、將計算後的所述a^y mod p的值和所述亂數S1級聯並進行散列運算，將計算結果和第四步收到的消息中的所述散列值Z4進行比較，相等則回送給所述雲端一個認證成功的應答信號，否則返回認證失敗的消息；

經過以上五個步驟，所述雲端與所述用戶端都成功地驗證了對方的身份；

所述區塊鏈身份系統採用的通訊模式是一種開放系統結構的網路方式，由所述用戶端首先向所述雲端提出請求，所述雲端對所述請求做相應的處理並執行所述請求中包含的任務，然後將結果返回給所述用戶端。

【發明圖式】

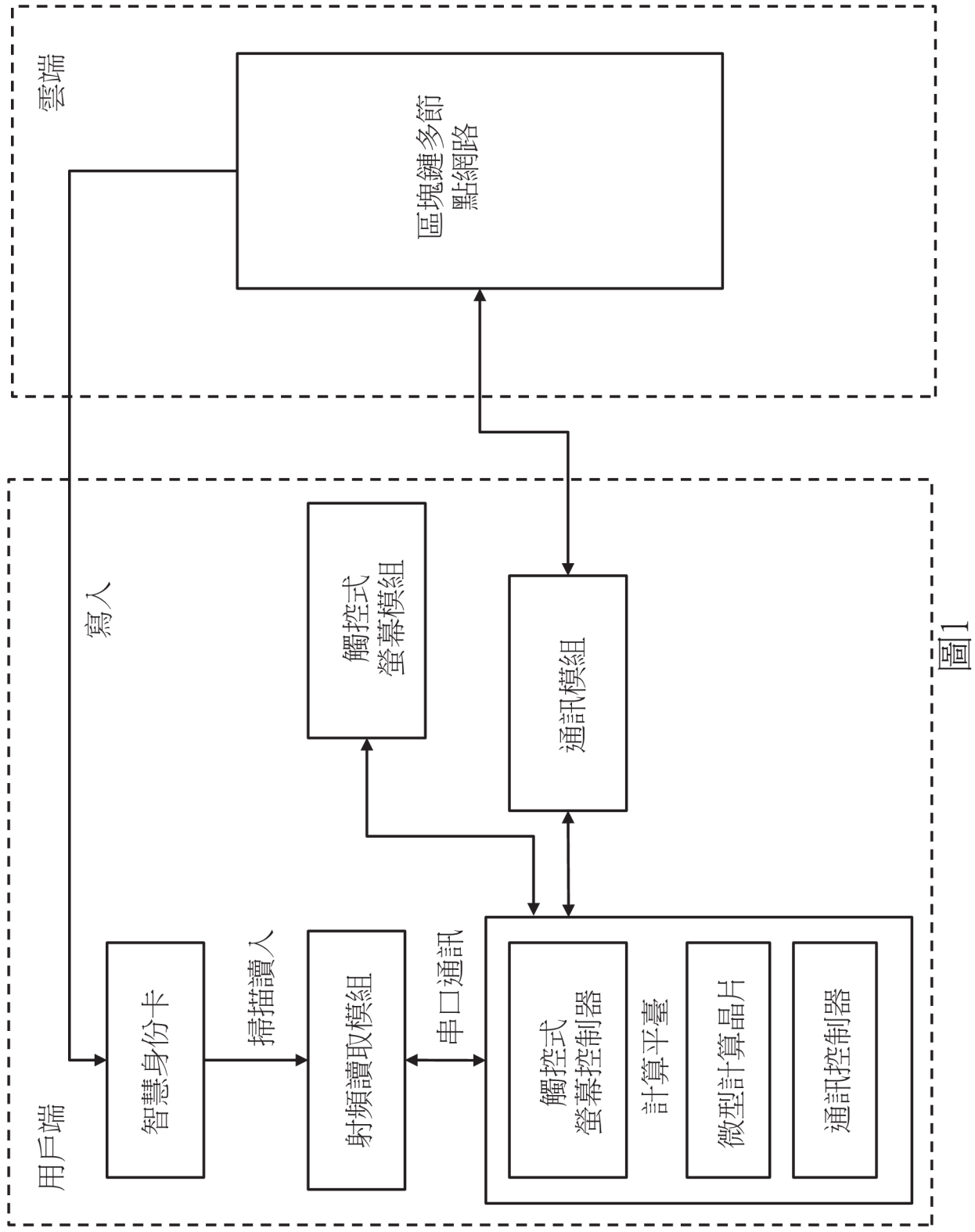
雲端
區塊鏈多節點網路
寫入
觸控式螢幕模組
通訊模組
用戶端
智慧身份卡
掃描讀入
射頻讀取模組
串口通訊
觸控式螢幕控制器
計算平臺
微型計算晶片
通訊控制器

圖1