201926111

(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 201926111 A

(43)公開日： 中華民國 108 (2019) 年 07 月 01 日

(21)申請案號：107132970 (22)申請日： 中華民國 107 (2018) 年 09 月 19 日

(51)Int. Cl.： *G06F21/62 (2013.01)*

(30)優先權：2017/11/23 中國大陸 201711183121.4

(71)申請人：香港商阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED (HK)
香港

(72)發明人：王虎森 (CN)

(74)代理人：林志剛

申請實體審查：有 申請專利範圍項數：42 項 圖式數：16 共 80 頁

(54)名稱

產品信息的加密、解密方法及裝置

(57)摘要

本說明書公開一種基於區塊鏈的產品信息加密、解密方法及裝置，可以由生產方以產品唯一暗碼為基礎，對生產信息進行加密，當存在流通方時可以根據唯一暗碼單向產生流通密鑰，而流通方可以繼續根據流通密鑰產生流通信息加密密鑰，對流通信息進行加密，根據流通信息加密密鑰再產生下一個流通密鑰。也就是以鏈式連環單向產生密鑰的方式，對產品信息進行加密，利用產品唯一暗碼除生產方和購買方以外無法獲知的特性，以及區塊鏈不可篡改不可偽造的特性，對生產信息進行加密和儲存，使得生產信息有很高的保密性。

指定代表圖：

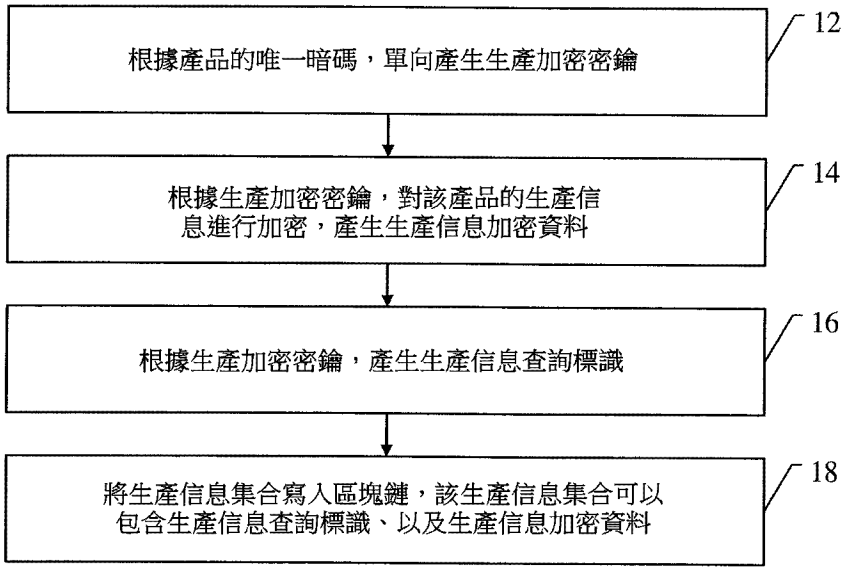

圖 1

【發明說明書】

【中文發明名稱】

產品信息的加密、解密方法及裝置

【技術領域】

本說明書涉及電腦技術領域，尤其涉及一種產品信息的加密方法及裝置、以及一種產品信息的解密方法及裝置。

【先前技術】

目前，隨著各行各業的發展，包括線上線下各種產品的交易、流通已經非常普遍，這裡所說的產品可以是實體產品，比如工業製品、工藝品等；也可以是電腦產品，比如軟體、網路儲存空間等。

對於一個產品，通常存在一個生產方和一個購買方，即生產產品的一方和購買產品的一方，且多數情況下還存在流通方，即流通產品的一方或多方。比如，對於一批飲料產品，可以有一個生產方（飲料的生產廠商），以及一個購買方（消費者），或者在生產方和購買方之間存在至少一個流通方（代理商、零售商等），在整個流通的過程中，除購買方的每一方均會為產品產生一個產品信息（生產方可以產生生產信息，而流通方可以產生流通信息），這些信息串聯到一起，就可以是由生產方到購買方的全過程，即的產品信息就是對產品進行溯源的依據。

而通常情況下，需要對各產品信息進行保密，即每一方的產品信息只能由生產方和購買方獲取到，而需要對流通方或竊取者保密。所以需要提供一種為各方產生的產品信息進行保密的方案，並確保購買方能夠對產品進行溯源。

【發明內容】

本說明書實施例提供一種基於區塊鏈的產品信息加密、解密方法，用於在產品流通過程中，對產品信息進行保密，且確保購買方能夠獲得產品信息。

本說明書實施例提供一種基於區塊鏈的產品信息加密、解密裝置，用於在產品流通過程中，對產品信息進行保密，且確保購買方能夠獲得產品信息。

為解決上述技術問題，本說明書實施例是這樣實現的：

本說明書實施例採用下述技術方案：

一種基於區塊鏈的產品信息加密方法，所述方法應用於生產方，包括：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

根據所述生產加密密鑰，產生生產信息查詢標識；

將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

一種基於區塊鏈的產品信息加密方法，所述方法應用於流通方，包括：

根據第n公鑰，單向產生第n流通密鑰查詢標識；

根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

根據所述第n流通密鑰，單向產生第n加密密鑰；

根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

一種基於區塊鏈的產品信息解密方法，所述方法應用於購買方，包括：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，產生生產信息查詢標識；

根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

一種基於區塊鏈的產品信息加密裝置，應用於生產方，包括：密鑰產生單元、資料產生單元、標識產生單

元、資料寫入單元，其中，

所述密鑰產生單元，根據產品的唯一暗碼，單向產生生產加密密鑰；

所述資料產生單元，根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

所述標識產生單元，根據所述生產加密密鑰，產生生產信息查詢標識；

所述資料傳輸單元，將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

一種基於區塊鏈的產品信息加密裝置，應用於流通方，包括：標識產生單元、資料讀取單元、資料解析單元、密鑰產生單元、資料加密單元、資料傳輸單元，其中，

所述標識產生單元，根據第n公鑰，單向產生第n流通密鑰查詢標識；

所述資料讀取單元，根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

所述資料解析單元，根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

所述密鑰產生單元，根據所述第n流通密鑰，單向產生第n加密密鑰；

所述資料加密單元，根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

所述資料傳輸單元，將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

一種基於區塊鏈的產品信息解密裝置，所述方法應用於購買方，包括：密鑰產生單元、標識產生單元、資料讀取單元、以及資料解析單元，其中，

所述密鑰產生單元，根據產品的唯一暗碼，單向產生生產加密密鑰；

所述標識產生單元，根據所述生產加密密鑰，產生生產信息查詢標識；

所述資料讀取單元，根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

所述資料解析單元，根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

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：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

根據所述生產加密密鑰，產生生產信息查詢標識；

將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

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：

根據第n公鑰，單向產生第n流通密鑰查詢標識；

根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

根據所述第n流通密鑰，單向產生第n加密密鑰；

根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

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：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，產生生產信息查詢標識；

根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

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當被包括多個應用程式的電子設備執行時，使得所述電子設備執行以下操作：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

根據所述生產加密密鑰，產生生產信息查詢標識；

將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

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當被包括多個應用程式的電子設備執行時，使得所述電子設備執行以下操作：

根據第n公鑰，單向產生第n流通密鑰查詢標識；

根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

根據所述第n流通密鑰，單向產生第n加密密鑰；

根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

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當被包括多個應用程式的電子設備執行時，使得所述電子設備執行以下操作：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，產生生產信息查詢標識；

根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

由以上實施例提供的技術方案可見，本說明書提供的實施例生產方可以利用產品的唯一暗碼，單向產生生產加密密鑰，再根據生產加密密鑰，對產品的生產信息進行加密，產生生產信息加密資料，根據生產加密密鑰，產生生產信息查詢標識，將包含生產信息查詢標識、以及生產信息加密資料的生產信息集合寫入區塊鏈。購買方可以利用產品的唯一暗碼，單向產生生產加密密鑰，再根據生產加密密鑰產生生產信息查詢標識，對從區塊鏈讀取到的生產

信息加密資料進行解密，獲得生產信息。而在產品流通過程中出現流通方的情況，可以根據生產加密密鑰，單向產生用於流通至第1次序流通方的第1流通密鑰，再單向產生生產信息查詢標識，根據第1公鑰，對第1流通密鑰進行加密，產生第1流通密鑰加密資料，根據第1公鑰，單向產生第1流通密鑰查詢標識，將包含所述第1接收密鑰查詢標識、生產信息查詢標識、第1接收密鑰加密資料以及生產信息加密資料生產信息集合寫入區塊鏈。利用產品唯一暗碼在購買方破壞產品完整性後才能獲知的特性，以及區塊鏈不可篡改不可偽造的特性，對生產信息進行加密解密，使得生產信息有很高的保密性，且將生產信息寫入區塊鏈，使得下個流通方能夠透過鏈式連續加密的方式，將產品信息寫入區塊鏈。

【圖式簡單說明】

為了更清楚地說明本說明書實施例或現有的技術方案，下面將對實施例或現有技術描述中所需要使用的附圖作簡單地介紹，顯而易見地，下面描述中的附圖僅僅是本說明書中記載的一些實施例，對於本領域普通技術人員來講，在不付出創造性勞動性的前提下，還可以根據這些附圖獲得其他的附圖。

圖1為實施例1提供的基於區塊鏈的產品信息加密方法的流程示意圖；

圖2為實施例1提供的基於區塊鏈的產品信息加密方法

的示意圖；

圖3為實施例1提供的基於區塊鏈的產品信息加密方法的示意圖；

圖4為實施例2提供的基於區塊鏈的產品信息解密方法的流程示意圖；

圖5為實施例2提供的基於區塊鏈的產品信息解密方法的示意圖；

圖6為實施例2提供的基於區塊鏈的產品信息解密方法的示意圖；

圖7為實施例3提供的基於區塊鏈的產品信息加密方法的流程示意圖；

圖8為實施例3提供的基於區塊鏈的產品信息加密方法的示意圖；

圖9為實施例4提供的基於區塊鏈的產品信息加密方法的流程示意圖；

圖10為實施例4提供的基於區塊鏈的產品信息加密方法的示意圖；

圖11為實施例5提供的基於區塊鏈的產品信息解密方法的流程示意圖；

圖12為實施例5提供的基於區塊鏈的產品信息解密方法的示意圖；

圖13為實施例6提供的基於區塊鏈的產品信息加密裝置的結構示意圖；

圖14為實施例7提供的基於區塊鏈的產品信息加密裝

置的結構示意圖；

圖15為實施例8提供的基於區塊鏈的產品信息解密裝置的結構示意圖；

圖16為本說明書實施例提供的一種電子設備的結構示意圖。

【實施方式】

為使本說明書的目的、技術方案和優點更加清楚，下面將結合具體實施例及相應的附圖對本說明書的技術方案進行清楚、完整地描述。顯然，所描述的實施例僅是本說明書一部分實施例，而不是全部的實施例。基於本說明書中的實施例，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其他實施例，都屬本說明書保護的範圍。

以下結合附圖，詳細說明本說明書中各實施例提供的技術方案。

實施例1

如前所述，在產品的整個流通過程中，除購買方的任一方均會為產品產生一個產品信息，比如生產方（產品廠商）可以在生產過程中，為產品產生一個生產信息（可以包含該產品、廠商等特徵信息），而流通方可以在接收到產品後，產生一個流通信息（可以包含流通方的時間、價格、地址等特徵信息），這些信息串聯到一起，可以是對產品進行溯源的依據，溯源可以是指跟踪特定產品從生

產、經過流通等中間環節，到購買方的整個流通過程。而對於非購買方和生產方而言（流通方和竊取者），都需要對產品信息進行保密，並確保購買方可以查看產品信息，所以需要提供一種為各方產生的產品信息進行保密的方案，並確保購買方能夠對產品進行溯源。

本說明書提供一種基於區塊鏈的產品信息加密、解密方法，用於在產品流通過程中，對產品信息進行保密，且確保購買方能夠獲得產品信息。該方法可以適用於流通過程中，存在生產方和購買方的情況，也可以適用於流通過程中，存在購買方、一個或多個流通方，以及購買方的情況。

而本實施例1以流通過程中，可以是存在生產方和購買方的情況為例，介紹產品信息的加密方法。具體地，先介紹一種基於區塊鏈的產品信息加密方法，應用於存在生產方和購買方中的生產方。該方法的流程如圖1所示，包括下述步驟：

步驟12：根據產品的唯一暗碼，單向產生生產加密密鑰；

產品的唯一暗碼，可以是指暗藏在產品內部的識別碼，只有購買方在破壞產品完整性，開始使用產品後，才能夠找到唯一暗碼，產品唯一暗碼的意義在於除了生產方和購買方以外，均無法獲取產品的唯一暗碼。比如，對於瓶裝飲料而言，只有開啓瓶蓋，即破壞了產品的完整後，才可以從瓶蓋內側找到產品的唯一暗碼。所以作為生產

方，可以以唯一暗碼作為依據，對產品信息進行加密，以致只有購買方在破壞產品完整性開始使用後，才可以找到唯一暗碼。

具體地，可以透過單向函數的方式，對產品的唯一暗碼產生生產加密密鑰，其中，單向函數可以是指對於任何輸入計算輸出，但已知輸出却無法確定輸入，也可以透過單向散列函數的方式，對產品的唯一暗碼產生生產加密密鑰，單向散列函數，又稱單向Hash函數、雜湊函數，就是把任意長的輸入消息串變化成固定長的輸出串且由輸出串難以得到輸入串的一種函數。所以，在無法獲取到唯一暗碼的情況下，無法確定出生產加密密鑰。這裡唯一暗碼可以由pincode表示，而單向函數可以由hash表示，則根據產品唯一暗碼單向產生的生產加密密鑰可以由$key_{生產加密}$表示，則可以有$key_{生產加密}$=hash（pincode）的表達方式。

在實際應用中，為了進一步加强的$key_{生產加密}$的安全性，在一種實施方式中，本步驟可以包括：接收生產方在生產該產品時產生的生產隨機數；根據唯一暗碼與生產隨機數的組合，單向產生生產加密密鑰。具體地，生產方在生產產品時可以產生一個生產隨機數，該生產隨機數可以用於對pincode進行單向計算，產生隨機數可以用$nonce_{生產}$表示。唯一暗碼與生產隨機數的組合可以以（pincode||$nonce_{生產}$）表示，也就是可以有$key_{生產加密}$=hash（pincode||$nonce_{生產}$），需要說明的是，這裡所指的pincode與$nonce_{生產}$的組合，可以是簡單的字元串先後串

聯，即pincode字元串在前、nonce生產字元串在後，也可以是預設的字元串穿插串聯的方式，比如pincode可以有6位字元串，而nonce生產可以有4位字元串，預設的字元串穿插串聯的方式可以是pincode前3位+ nonce生產前2位+pincode後3位+ nonce生產後2位，等。

步驟14：根據生產加密密鑰，對該產品的生產信息進行加密，產生生產信息加密資料。

由於在前一步驟中，產生的生產加密密鑰key生產加密需要pincode的支持，而除購買方以外均無法得到pincode，所以本步驟就可以根據key生產加密對產品的生產信息進行加密，產生生產信息加密資料。具體地，生產信息可以是指生產方在生產產品時產生的產品信息，其中，產品信息可以透過m表示，則生產信息可以透過m生產表示。在實際應用中，通常需要保護m生產的隱私，也可以理解為保護生產方的隱私，所以根據除購買方以外無法獲知的pincode對生產信息進行加密，安全性很高。

對於加密，可以透過加密函數實現，加密函數enc可以是指對信息進行加密的函數，函數中有兩個輸入，密鑰和信息，加密後可以產生信息加密資料（在本實施例中，加密的信息即為產品信息m），可以透過enc（加密密鑰key，產品信息m）表示。而對於獲取到信息加密資料enc，但不知道key，無法解析出m；對於獲取到enc和m，也無法得知key，此處的key若是非對稱密鑰，那麼enc即為非對稱加密；若key是對稱密鑰，那麼enc即為對稱加

密。非對稱加密的情況可以存在公鑰pk和私鑰sk。在本步驟中，可以將產生生產信息加密資料表示為enc（key$_{生產加密}$，m$_{生產}$）。

在前文已經介紹，key$_{生產加密}$可以由pincode單向產生，也可以由pincode||nonce$_{生產}$單向產生，可見在加入nonce$_{生產}$的情況下，pincode與nonce$_{生產}$是得到key$_{生產加密}$的關鍵，而pincode只有購買方能夠獲得，所以為了達到保護nonce$_{生產}$的目的，本方法還可以包括：

根據唯一暗碼，單向產生隨機數查詢標識；在可信儲存庫中為該產品創建唯一標識；將隨機數查詢標識以及生產隨機數發送至可信儲存庫，並均與唯一標識關聯。

具體地，為了達到保護nonce$_{生產}$的目的，可以將該nonce$_{生產}$發送至一個可信儲存庫中，當購買方需要產生key$_{生產加密}$，並對enc（key$_{生產加密}$，m$_{生產}$）進行解密時，可以從可信儲存庫中，查找到nonce$_{生產}$。該可信儲存庫，可以是高度安全的國家機構或企業，為在可信儲存庫中，可以儲存針對不同產品的生產隨機數，所以可以為不同產品分別創建一個唯一標識，對於如何查找nonce$_{生產}$，可以根據唯一暗碼，單向產生隨機數查詢標識hash（pincode）,在將nonce$_{生產}$發送至可信儲存庫時，可以將hash（pincode）以及nonce$_{生產}$共同發送至可信儲存庫，並均與唯一標識關聯，以便購買方可以透過hash（pincode）查找到nonce$_{生產}$。而在加入nonce$_{生產}$的情況下，key$_{生產加密}$=hash（pincode||nonce$_{生產}$），對於隨機數查詢標識hash（pincode

），也不會影響的$key_{生產加密}$安全性。

根據本實施例的前提，在產品流通過程中，只存在生產方和購買方的情況下，實際應用中，可以由生產方將$enc（key_{生產加密}，m_{生產}）$發送至購買方，以便購買方解析$m_{生產}$。

步驟16：根據生產加密密鑰，產生生產信息查詢標識。

步驟18：將生產信息集合寫入區塊鏈，該生產信息集合可以包含生產信息查詢標識、以及生產信息加密資料。

區塊鏈，可以是一種按照時間順序將資料區塊以順序相連的方式組合成的一種鏈式資料結構，並以密碼學方式保證的不可篡改和不可偽造的分散式資料庫。而將$enc（key_{生產加密}，m_{生產}）$寫入區塊鏈中，可以有效地防止篡改和偽造，具有較高的安全性和隱私性。由於區塊鏈中，有大量的資料，所以為了使購買方能夠快速地查找到$enc（key_{生產加密}，m_{生產}）$，可以根據$key_{生產加密}$，產生一個生產信息查詢標識，比如，就可以透過單向函數產生，還可以根據$key_{生產加密}$中特定個字元位數產生，又或結合特定個字元位數以及單向函數產生，又或對進行二次單向計算，產生生產信息查詢標識。可以包含生產信息查詢標識以及$enc（key_{生產加密}，m_{生產}）$的生產信息集合寫入區塊鏈，以便購買方可以讀取。

如圖2所示，為本方法的一個實施方式的示意圖；如圖3所示，為本方法的另一個實施例方式的示意圖，區別

在於如圖3所示的實施方式中對$key_{生產加密}$的產生過程加入$nonce_{生產}$，更加有利於對$enc(key_{生產加密}, m_{生產})$進行保護。

需要說明的是，在本實施例以及下文的描述中，所指的“產品”均為同一產品，即生產方產生出的產品，比如，本說明書中的產品可以為“一批飲料”或“一個50GB的網路儲存空間”，圍繞產品的信息、密鑰、公鑰、私鑰等，均對應同一產品。

採用實施例1提供的方法，生產方利用產品的唯一暗碼，單向產生生產加密密鑰，再根據生產加密密鑰，對產品的生產信息進行加密，產生生產信息加密資料，根據生產加密密鑰，產生生產信息查詢標識，將包含生產信息查詢標識、以及生產信息加密資料的生產信息集合寫入區塊鏈。利用產品唯一暗碼除生產方和購買方以外無法獲知的特性，以及區塊鏈不可篡改不可偽造的特性，對生產信息進行加密和儲存，使得生產信息有很高的保密性。此外，還可以透過生產隨機數，進一步加强生產信息的保密性。

實施例2

基於與實施例1相同的發明思路，本實施例以流通過程中，存在生產方和購買方的情況為例，介紹基於區塊鏈的產品信息加密、解密方法，用於在產品流通過程中，對產品信息進行保密，且確保購買方能夠獲得產品信息。具體地，本實施例介紹一種基於區塊鏈的產品信息解密方

法，應用於存在生產方和購買方中的購買方。該方法的流程如圖4所示，包括下述步驟：

步驟22：根據產品的唯一暗碼，單向產生生產加密密鑰。

在實施例1中已經介紹，生產方可以根據pincode，單向產生$key_{生產加密}$，即有$key_{生產加密}$=hash（pincode），還介紹了pincode的特性，即購買方在破壞產品完整性，開始使用產品後，能夠找到pincode，所以，購買方也就可以根據pincode，單向產生$key_{生產加密}$。

在實施例1中還介紹了，為了進一步加强的$key_{生產加密}$的安全性，生產方在生產產品時，可以產生$nonce_{生產}$，所以在一種實施方式中，本步驟可以包括：根據產品的唯一暗碼，單向產生隨機數查詢標識；從可信儲存庫中獲取與隨機數查詢標識對應的生產隨機數；根據唯一暗碼與生產隨機數的組合，單向產生生產加密密鑰。

具體地，在加入$nonce_{生產}$的情況下，$key_{生產加密}$=hash（pincode||$nonce_{生產}$），由於生產方根據pincode產生了隨機數查詢標識hash（pincode），並將hash（pincode）以及$nonce_{生產}$共同發送至可信儲存庫，且均與為產品創建的唯一標識關聯。所以購買方也可以根據pincode，單向產生hash（pincode），可以在可信儲存庫中透過hash（pincode）查找到$nonce_{生產}$，再單向產生$key_{生產加密}$=hash（pincode||$nonce_{生產}$），在實施例1中介紹pincode的$nonce_{生產}$的組合，本步驟中可以透過相同的組合方式進行組合，以

便產生的key生產加密與生產方產生的key生產加密一致。

步驟24：根據生產加密密鑰，產生生產信息查詢標識。

在實施例1中介紹了產生生產信息查詢標識的方式，本步驟中，購買方也可以按照生產方產生生產信息查詢標識的方式進行產生，確保一致性。

步驟26：根據生產信息查詢標識，從區塊鏈中讀取產品的生產信息加密資料。

在實施例中生產方將包含生產信息查詢標識以及enc（key生產加密，m生產）的生產信息集合寫入區塊鏈，本步驟就可以根據生產信息查詢標識，讀取到enc（key生產加密，m生產）。

步驟28：根據生產加密密鑰，對生產信息加密資料進行解密，獲得生產信息。

在本步驟，根據加密函數的特性，可以根據key生產加密，對enc（key生產加密，m生產）進行解密，獲得m生產。由於購買方在破壞產品完整性，開始使用產品後，才能夠找到pincode。盜竊方即使得到enc（key生產加密，m生產），也由於無法得知pincode，無法進行解密，如果在加上nonce生產的情況，由於無法得知pincode也就無法得知hash（pincode），更無法確定出key生產加密=hash（pincode||nonce生產）。

如圖5所示，為本方法的一個實施方式的示意圖；如圖6所示，為本方法的另一個實施例方式的示意圖，區別

在於如圖6所示的實施方式中對$key_{生產加密}$的產生過程加入$nonce_{生產}$，增加了解析$m_{生產}$的難度。

採用實施例2提供的方法，購買方利用產品的唯一暗碼，單向產生生產加密密鑰，再根據生產加密密鑰產生生產信息查詢標識，對從區塊鏈讀取到的生產信息加密資料進行解密，獲得生產信息。利用產品唯一暗碼在購買方破壞產品完整性後才能獲知的特性，以及區塊鏈不可篡改不可偽造的特性，對生產信息進行解密，使得生產信息有很高的保密性。此外，還可以透過生產隨機數，進一步加强生產信息的保密性。

實施例3

在前述兩個實施例中，已經介紹了流通過程中，存在生產方和購買方的情況，而在實際應用中，也很可能存在一個或多個流通方，即可以使產品便捷地從生產方流通到購買方，比如代理商、批發商、零售商等。而流通方也會在流通過程中，為產品產生流通信息，而流通信息中可以包含流通方的隱私信息，所以也需要進行保密，即對於對其他流通方以及竊取者而言，需要對產品信息進行保密，並確保購買方可以查看產品信息，其他流通方無法獲知生產信息以及其他流通方的流通信息。

所以基於與前述兩個實施例相同的發明思路，本實施例以流通過程中存在生產方、流通方和購買方的情況為例，介紹一種基於區塊鏈的產品信息加密、解密方法，具

體地，先介紹一種基於區塊鏈的產品信息的加密方法，應用於存在生產方、流通方和購買方中的生產方。該方法的流程如圖7所示，包括下述步驟：

步驟32：根據產品的唯一暗碼，單向產生生產加密密鑰；

步驟34：根據生產加密密鑰，對該產品的生產信息進行加密，產生生產信息加密資料。

前兩步驟中，與實施例1類似，此處不再贅述，可以根據如圖2或圖3所示的實施方式產生enc（$key_{生產加密}$，$m_{生產}$）。

步驟36：根據生產加密密鑰，單向產生第1流通密鑰，再根據所述第1流通密鑰，單向產生生產信息查詢標識。

這裡所指的第1流通密鑰，可以作用於第1次序流通方進行流通，比如批發商作為生產方後的第一個流通方，那麼批發商就可以是指第1次序流通方。考慮到pincode的特性，即生產方和破壞產品完整性後的購買方才能獲知，可以以pincode作為基礎，在流通過程中進行鏈式連續產生加密密鑰。具體地，可以利用單向函數的特性，即得知結果無法逆向解析輸入的特性，根據生產加密密鑰，單向產生第1流通密鑰，該第1流通密鑰可以$key_{第1流通}$表示。

在實施例1中已經介紹，可以將信息加密資料寫入區塊鏈，購買方可以透過$key_{生產加密}$產生生產信息查詢標識，且便於從區塊鏈中讀取enc（$key_{生產加密}$，$m_{生產}$）。但針對

流通方而言，為了達到對生產信息保密的目的，可以無需流通方獲知$key_{生產加密}$，但流通方也需要在區塊鏈中讀取資料，所以可以為流通方也產生一個生產信息查詢標識，且避免由$key_{生產加密}$直接產生，即根據$key_{第1流通}$，單向產生生產信息查詢標識，可以表示為hash（$key_{第1流通}$）。

步驟38：根據第1公鑰，對第1流通密鑰進行加密，產生第1流通密鑰加密資料，所述第1公鑰為第1次序流通方的流通公鑰。

由於是$key_{第1流通}$透過$key_{生產加密}$產生的，而$key_{第1流通}$又可以作用於第1次序流通方進行流通，可以考慮讓第1次序流通方獲知$key_{第1流通}$，但無法獲知$key_{生產加密}$，所以可以透過第1公鑰對$key_{第1流通}$進行加密，第1公鑰可以表示為pk_1，可以是指第1次序流通方的流通公鑰。具體地，用第1次序流通方的pk_1對$key_{第1流通}$進行加密，可以產生第1流通密鑰加密資料enc（pk_1，$key_{第1流通}$）。從而使得第1次序流通方可以根據第1私鑰sk_1進行解密。

在實際應用中，為了進一步保護產品流通過程的隱私性，可以在產生enc（pk_1，$key_{第1流通}$）的過程中，加入產品的公開明碼，在一種實施方式中，本步驟可以包括：根據第1公鑰，對產品的公開明碼與第1流通密鑰的組合進行加密，產生第1流通密鑰加密資料。公開明碼qcode，可以在產品外部且全域唯一，任何一方在接收到產品後，均可以獲得qcode，但對於未拿到產品的任何對象不容易獲得（比如竊取者，但也可以透過非正常手段竊取），所以可

以將qcode加入到流通過程中，進一步加強流通的隱私性。具體地，可以有enc（pk_1，qcode||$key_{第1流通}$）。

步驟310：根據第1公鑰，單向產生第1流通密鑰查詢標識。

上一步驟中，產生了enc（pk_1，$key_{第1流通}$），而為了保證資料安全性，本方法也可以將信息集合寫入區塊鏈，所以為了使第1流通方便捷地找到enc（pk_1，$key_{第1流通}$），可以為流通方產生單向一個密鑰查詢標識，即第1流通密鑰查詢標識，可以表示為hash（pk_1），以便第1流通可以透過pk_1從區塊鏈中讀取到enc（pk_1，$key_{第1流通}$）。

步驟312：將生產信息集合寫入區塊鏈，該生產信息集合可以包含第1接收密鑰查詢標識、生產信息查詢標識、第1接收密鑰加密資料以及生產信息加密資料。

本步驟可以將生產信息寫入區塊鏈（上鏈），以便流通方和購買方可以獲取到enc（pk_1，$key_{第1流通}$）以及enc（$key_{生產加密}$，$m_{生產}$），對於如何查找，可以透過hash（pk_1），以及hash（$key_{第1流通}$）。

在實際應用中，為了進一步加強隱私性，本步驟可以包括：根據生產私鑰，對生產信息集合進行簽名，該生產私鑰為生產方在生產產品時產生的私鑰；將簽名後的生產信息集合寫入區塊鏈。如圖8所示，為本方法的一個實施方式的示意圖。

採用實施例3提供的方法，在實施例1的基礎上，根據生產加密密鑰，單向產生用於流通至第1次序流通方的第1

流通密鑰，再單向產生生產信息查詢標識，根據第1公鑰，對第1流通密鑰進行加密，產生第1流通密鑰加密資料，根據第1公鑰，單向產生第1流通密鑰查詢標識，將包含所述第1接收密鑰查詢標識、生產信息查詢標識、第1接收密鑰加密資料以及生產信息加密資料生產信息集合寫入區塊鏈。利用產品唯一暗碼在購買方破壞產品完整性後才能獲知的特性，以及區塊鏈不可篡改不可偽造的特性，對生產信息進行加密，使得生產信息有很高的保密性，且將生產信息寫入區塊鏈，使得下個流通方能夠透過鏈式連續加密的方式，將產品信息寫入區塊鏈。

實施例4

基於與前述兩個實施例相同的發明思路，本實施例以流通過程中存在生產方、流通方和購買方的情況為例，介紹一種基於區塊鏈的產品信息加密、解密方法，具體地，介紹一種基於區塊鏈的產品信息的加密方法，應用於存在生產方、流通方和購買方中的流通方。該方法的流程如圖9所示，包括下述步驟：

步驟42：根據第n公鑰，單向產生第n流通密鑰查詢標識。

在實施例3中，介紹了流通方公鑰的作用，本步驟可以根據pk_n，單向產生第n流通密鑰查詢標識hash（pk_n），其中，n可以是大於0的自然數，比如1、2、3、4……等。

步驟44：根據第n流通密鑰查詢標識，從區塊鏈中讀

取第n接收密鑰加密資料。

如圖8所示，在將生產信息集合寫入區塊鏈時，第1次序流通方可以根據hash（pk_1），查找到enc（pk_1，$key_{第1流通}$），類似地，第n次序流通方可以根據hash（pk_n），查找到enc（pk_n，$key_{第n流通}$）。

在實施例3中已經介紹，可以實際應用中，對生產信息集合進行簽名，而對於流通方，可以有多個流通方，每個流通方均以各自的私鑰進行簽名，所以在本步驟之後，還可以包括：根據生產公鑰，對簽名後的生產信息集合進行簽名驗證；或根據第n公鑰，對簽名後的第n信息集合進行簽名驗證。當驗證成功後，再執行下個步驟。

步驟46：根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰。

在實施例3中已經介紹，第1次序流通方可以根據第1私鑰sk_1對enc（pk_1，$key_{第1流通}$）進行解密，類似地，本步驟中，也可以根據第n私鑰sk_n對enc（pk_n，$key_{第n流通}$）進行解密。

步驟48：根據第n流通密鑰，單向產生第n加密密鑰。

在實施例3（可以參考實施例1）中介紹了根據產品的pincode，單向產生$key_{生產加密}$，而作為流通方無法獲取到pincode，而本說明書提供的加密方法，就可以對pincode進行鏈式連續產生加密密鑰作為核心，所以本步驟中，流通方，可以根據$key_{第n流通}$，單向產生$key_{第n加密}$，與生產方關聯到一起，就是可以是生產方根據pincode產生$key_{生產加密}$

，而各個流通方鏈式連續產生$key_{第1加密}$、$key_{第2加密}$、$key_{第3加密}$等，即$key_{第n加密}=hash(key_{第n流通})$。

在實際應用中，為了進一步加强隱私性，也可以與生產方類似，流通方也可以產生一個隨機數，所以在一種實施方式中，本步驟可以包括：接收第n次序流通方在接收產品時產生的第n隨機數；根據第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰。具體地，可以有$key_{第n加密}=hash(key_{第n流通}||nonce_{第n})$。

與實施例1類似的，本步驟還可以包括：將第n隨機數發送至可信儲存庫，並與產品的唯一標識關聯，以便購買方可以透過產品的唯一標識，找到各個流通方的隨機數，而其他流通方，由於無法得知pincode，也就無法獲得其他流通方的隨機數。

步驟410：根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料。

生產方可以產生一個生產信息$m_{生產}$，則流通方就可以在流通過程中產生各自的流通信息$m_{第n}$，比如，第1次序流通方可以產生$m_{第1}$，第1次序流通方可以產生$m_{第2}$，等。從而本步驟可以根據$key_{第n加密}$對$m_{第n}$進行加密，產生$enc(key_{第n加密}, m_{第n})$。

步驟412：根據第n加密密鑰，產生第n流通信息查詢標識。

在實施例1中已經介紹，產生信息查詢標識的方式，在本步驟中，也可以根據實施例1介紹的方式，由$key_{第n加密}$

產生第n流通信息查詢標識。

而在實際應用中，可以有下一個流通方，則與實施例3中步驟36類似地的，本步驟還可以包括：根據第n加密密鑰，單向產生第n+1流通密鑰，再根據第n+1流通密鑰，單向產生第n流通信息查詢標識。而第n+1流通密鑰，就可以是相對於第n次序流通方而言的下一次序的流通方。即$key_{第n+1流通}$=hash（$key_{第n流通}$），第n流通信息查詢標識可以是hash（$key_{第n+1流通}$），以便第n+1次序流通方可以根據hash（$key_{第n+1流通}$），讀取區塊鏈中的資料。

步驟414：將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料。

如圖2或3所示，本步驟可以類似地，將包含第n流通信息查詢標識以及enc（$key_{第n加密}$，$m_{第n}$）的第n信息集合寫入區塊鏈中。

在有下一個流通方的情況下，本步驟可以包括

根據第n+1公鑰，對第n+1流通密鑰進行加密，產生第n+1流通密鑰加密資料，該第n+1公鑰可以是第n+1次序流通方的流通公鑰；根據第n+1公鑰，單向產生第n+1流通密鑰查詢標識；將第n信息集合寫入區塊鏈，該第n信息集合包含第n+1接收密鑰查詢標識、第n流通信息查詢標識、第n+1接收密鑰加密資料以及第n流通信息加密資料。

具體地，可以是與前述類似地，

可以根據pk_{n+1}，對$key_{第n+1流通}$進行加密，產生enc（

pk_{n+1}，$key_{第n+1流通}$），產生hash（pk_{n+1}）作為第n+1流通密鑰查詢標識。將包含hash（pk_{n+1}）、hash（$key_{第n+1流通}$）、enc（pk_{n+1}，$key_{第n+1流通}$）、以及enc（$key_{第n加密}$，$m_{第n}$）的第n信息集合寫入區塊鏈。

而在實際應用中，根據第n+1公鑰，對第n+1流通密鑰進行加密，產生第n+1流通密鑰加密資料，可以包括：

根據第n+1公鑰，對產品的公開明碼與第n+1流通密鑰的組合進行加密，產生第n+1流通密鑰加密資料，即可以有enc（pk_{n+1}，qcode||$key_{第n+1流通}$）。

而在實際應用中，與前述類似地，可以根據第n私鑰，對所述第n信息集合進行簽名；將簽名後的第n信息集合寫入區塊鏈，以便下個流通方可以根據公鑰進行簽名驗證。如圖10所示，為本實施例的示意圖。

採用實施例4的方法，在實施例3的生產方的基礎上，根據第n私鑰，解析出第n流通密鑰，最終將包含第n+1接收密鑰查詢標識、第n流通信息查詢標識、第n+1接收密鑰加密資料以及第n流通信息加密資料的第n信息集合寫入區塊鏈。利用產品唯一暗碼在購買方破壞產品完整性後才能獲知的特性，以及區塊鏈不可篡改不可偽造的特性，對第n流通信息進行加密，使得第n流通信息有很高的保密性，且將第n流通信息寫入區塊鏈，使得下個流通方能夠透過鏈式連續加密的方式，將產品信息寫入區塊鏈。若沒有下個流通方，也可以透過將包含第n流通信息查詢標識以及第n流通信息加密資料的第n信息集合寫入區塊鏈。

實施例5

基於與前述實施例相同的發明思路，本實施例以流通過程中存在生產方、流通方和購買方的情況為例，介紹一種基於區塊鏈的產品信息加密、解密方法，具體地，介紹一種基於區塊鏈的產品信息的加密方法，應用於存在生產方、流通方和購買方中的購買方。該方法的流程如圖11所示，包括下述步驟：

步驟52：根據產品的唯一暗碼，單向產生生產加密密鑰。

步驟54：根據生產加密密鑰，產生生產信息查詢標識。

步驟56：根據生產信息查詢標識，從區塊鏈中讀取產品的生產信息加密資料。

在一種實施方式中，本步驟可以包括：

根據唯一暗碼與生產隨機數的組合，單向產生生產加密密鑰，再單向產生第1流通密鑰，再單向產生生產信息查詢標識；根據生產信息查詢標識，從區塊鏈中讀取生產信息集合中的生產信息加密資料。

具體地，本步驟可以加入隨機數的組合，即可以有$key_{生產加密}=hash(pincode||nonce_{生產})$，$key_{第1流通}=hash(key_{生產加密})$，單向產生生產信息查詢標識$hash(key_{第1流通})$，從而可以從區塊鏈中讀取生產信息集合中的$enc(key_{生產加密}, m_{生產})$。

步驟58：根據生產加密密鑰，對生產信息加密資料進行解密，獲得生產信息。

上述步驟與實施例2中介紹的實施方式類似，此處不再贅述。

步驟510：根據生產加密密鑰，單向產生第1流通密鑰，根據第n流通密鑰，單向產生第n加密密鑰，根據第n加密密鑰，單向產生第n+1流通密鑰。

購買方可以根據$key_{生產加密}$單向產生$key_{第1流通}$。即$key_{第1流通}=hash(key_{生產加密})$。根據鏈式連續產生的方式，可以根據$key_{第n流通}$產生$key_{第n加密}$，在前文已經介紹了，可以在產生加密密鑰時，加入隨機數，所以根據第n流通密鑰，單向產生第n加密密鑰，可以包括：從可信儲存庫中獲取與隨機數查詢密鑰對應的第n隨機數；根據第n流通密鑰與第n隨機數的組合，單向產生第n加密密鑰。具體地，由於購買方獲知了pincode，所以可以單向產生隨機數查詢密鑰hash（pincode），根據前述實施例的介紹，生產方和流通方，均可以將隨機數發送至可信儲存庫，且可以與產品的唯一標識關聯，也即唯一標識可以關聯hash（pincode）、生產隨機數、以及第n隨機數，此時可以將可信儲存庫設置為，只允許透過唯一標識關聯隨機數而不能讀取，而hash（pincode）可以進行讀取，就有效防止流通方透過唯一標識獲取隨機數。而購買方透過hash（pincode）獲取到對應的第n隨機數（包括第1隨機數、第2隨機數……第n隨機數）後，就可以單向產生第n加密

密鑰，可以有$key_{第n加密}$=hash（$key_{第n流通}$||$nonce_{第n}$）。而對於流通密鑰，可以根據第n加密密鑰，單向產生第n+1流通密鑰，可以有$key_{第n+1流通}$=hash（$key_{第n加密}$）。具體比如，購買方在步驟52中產生了$key_{生產加密}$，則本步驟可以有$key_{第1流通}$=hash（$key_{生產加密}$）、再可以產生$key_{第1加密}$=hash（$key_{第1流通}$||$nonce_{第1}$）、以及還可以產生$key_{第2流通}$=hash（$key_{第1加密}$），如此往復，可以得到全部的流通方的流通密鑰。

本實施例中，n可以是大於0的自然數。

步驟512：根據第n流通信息查詢標識，從區塊鏈中讀取產品的第n流通信息加密資料。

若對於最後一個流通方，可以根據第n加密密鑰，根據預設方式產生第n流通信息查詢標識，比如實施例1中步驟18介紹的方式，根據$key_{第n加密}$中特定個字元位數產生，又或結合特定個字元位數以及單向函數產生，又或對進行二次單向計算，產生第n流通信息查詢標識。

而對於非最後一個流通方而言，則本步驟可以包括：根據第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰，再單向產生第n+1流通密鑰，再單向產生第n流通信息查詢標識；根據第n流通信息查詢標識，從區塊鏈中讀取第n信息集合中的enc（$key_{第n加密}$，$m_{第n}$）。

具體地，可以有$key_{第n加密}$=hash（$key_{第n流通}$||$nonce_{第n}$），$key_{第n+1流通}$=hash（$key_{第n加密}$），此後可以產生第n流通信息查詢標識hash（$key_{第n+1流通}$）。如圖10所示，可以根據

hash（$key_{第n+1流通}$），從區塊鏈中讀取enc（$key_{第n加密}$，$m_{第n}$）。

步驟514：根據第n加密密鑰，對第n流通信息加密資料進行解密，獲得第n流通信息。

具體地，可以與實施例2的介紹類似，根據$key_{第n加密}$，對enc（$key_{第n加密}$，$m_{第n}$）進行解密，獲取$m_{第n}$。如圖12為本實施例的示意圖。

採用實施例5提供的方法，購買方利用產品的唯一暗碼，單向產生生產加密密鑰，再根據生產加密密鑰產生生產信息查詢標識，對從區塊鏈讀取到的生產信息加密資料進行解密，獲得生產信息。透過鏈式連續加密的方式，根據生產加密密鑰，產生第1流通密鑰，再產生第1加密密鑰、從而持續產生第n加密密鑰，再產生第n+1流通密鑰、第n信息查詢標識，進而根據第n加密密鑰對根據第n信息查詢標識獲取到的第n流通信息加密資料進行解密，得到第n流通信息。

實施例6

基於相同的發明構思，實施例6提供了一種基於區塊鏈的產品信息加密裝置，所述裝置可以應用於生產方，用於實現實施例1和實施例3所述的方法。該裝置的結構方塊圖如圖13所示，為該裝置的結構圖，包括：

密鑰產生單元61、資料產生單元62、標識產生單元63、資料寫入單元64，其中，

所述密鑰產生單元61，可以根據產品的唯一暗碼，單向產生生產加密密鑰；

所述資料產生單元62，可以根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

所述標識產生單元63，可以根據所述生產加密密鑰，產生生產信息查詢標識；

所述資料傳輸單元64，可以將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

在一種實施方式中，所述密鑰產生單元61，可以

接收生產方在生產所述產品時產生的生產隨機數；

根據所述唯一暗碼與所述生產隨機數的組合，單向產生生產加密密鑰。

在一種實施方式中，

所述標識產生單元63，可以根據所述唯一暗碼，單向產生隨機數查詢標識；

所述資料傳輸單元64，可以

在可信儲存庫中為所述產品創建唯一標識；

將所述隨機數查詢標識以及所述生產隨機數發送至所述可信儲存庫，並均與所述唯一標識關聯。

在一種實施方式中，所述標識產生單元63，可以

根據所述生產加密密鑰，單向產生第1流通密鑰，再根據所述第1流通密鑰，單向產生生產信息查詢標識；則

所述資料產生單元62，可以

根據第1公鑰，對第1流通密鑰進行加密，產生第1流通密鑰加密資料，所述第1公鑰為第1次序流通方的流通公鑰；

根據第1公鑰，單向產生第1流通密鑰查詢標識；

所述資料傳輸單元64，可以

將生產信息集合寫入區塊鏈，所述生產信息集合包含所述第1接收密鑰查詢標識、生產信息查詢標識、第1接收密鑰加密資料以及生產信息加密資料。

在一種實施方式中，所述資料產生單元62，

根據第1公鑰，對產品的公開明碼與第1流通密鑰的組合進行加密，產生第1流通密鑰加密資料。

在一種實施方式中，所述資料傳輸單元64，可以

根據生產私鑰，對所述生產信息集合進行簽名，所述生產私鑰為生產方在生產所述產品時產生的私鑰；

將簽名後的生產信息集合寫入區塊鏈。

實施例7

基於相同的發明構思，實施例7提供了一種基於區塊鏈的產品信息加密裝置，所述裝置可以應用於流通方，用於實現實施例4所述的方法。該裝置的結構框圖如圖14所示，為該裝置的結構圖，包括：

標識產生單元71、資料讀取單元72、資料解析單元73、密鑰產生單元74、資料加密單元75、資料傳輸單元

76，其中，

所述標識產生單元71，可以根據第n公鑰，單向產生第n流通密鑰查詢標識；

所述資料讀取單元72，可以根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

所述資料解析單元73，可以根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

所述密鑰產生單元74，可以根據所述第n流通密鑰，單向產生第n加密密鑰；

所述資料加密單元75，可以根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

所述資料傳輸單元76，可以將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

在一種實施方式中，所述密鑰產生單元74，可以

接收第n次序流通方在接收產品時產生的第n隨機數；

根據所述第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰。

在一種實施方式中，所述資料傳輸單元76，可以

將所述第n隨機數發送至可信儲存庫，並與所述產品的唯一標識關聯。

在一種實施方式中，所述標識產生單元71，可以

根據所述第n加密密鑰，單向產生第n+1流通密鑰，再根據第n+1流通密鑰，單向產生第n流通信息查詢標識；則

所述密鑰產生單元74，可以根據第n+1公鑰，對第n+1流通密鑰進行加密，產生第n+1流通密鑰加密資料，所述第n+1公鑰為第n+1次序流通方的流通公鑰；

所述標識產生單元71，可以根據第n+1公鑰，單向產生第n+1流通密鑰查詢標識；

所述資料傳輸單元76，可以將第n信息集合寫入區塊鏈，所述第n信息集合包含所述第n+1接收密鑰查詢標識、第n流通信息查詢標識、第n+1接收密鑰加密資料以及第n流通信息加密資料。

在一種實施方式中，所述資料加密單元75，可以

根據第n+1公鑰，對產品的公開明碼與第n+1流通密鑰的組合進行加密，產生第n+1流通密鑰加密資料。

在一種實施方式中，所述資料傳輸單元76，可以

根據第n私鑰，對所述第n信息集合進行簽名；

將簽名後的第n信息集合寫入區塊鏈。

在一種實施方式中，所述資料解析單元73，可以根據第n私鑰，對所述第n流通密鑰加密資料進行解密之前，

根據生產公鑰，對簽名後的生產信息集合進行簽名驗證；或

根據第n公鑰，對簽名後的第n信息集合進行簽名驗證。

實施例8

基於相同的發明構思，實施例8提供了一種基於區塊鏈的產品信息解密裝置，所述裝置可以應用於購買方，用於實現實施例3和5所述的方法。該裝置的結構方塊圖如圖15所示，為該裝置的結構圖，包括：

密鑰產生單元81、標識產生單元82、資料讀取單元83、以及資料解析單元84，其中，

所述密鑰產生單元81，可以根據產品的唯一暗碼，單向產生生產加密密鑰；

所述標識產生單元82，可以根據所述生產加密密鑰，產生生產信息查詢標識；

所述資料讀取單元83，可以根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

所述資料解析單元84，可以根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

在一種實施方式中，

所述密鑰產生單元81，可以根據所述生產加密密鑰，單向產生第1流通密鑰，根據所述第n流通密鑰，單向產生第n加密密鑰，根據第n加密密鑰，單向產生第n+1流通密鑰；

所述資料讀取單元83，可以根據所述第n流通信息查詢標識，從區塊鏈中讀取所述產品的第n流通信息加密資料；

所述資料解析單元84，可以根據所述第n加密密鑰，

對所述第n流通信息加密資料進行解密，獲得第n流通信息；

其中，n為大於0的自然數。

在一種實施方式中，

所述密鑰產生單元81，可以根據產品的唯一暗碼，單向產生隨機數查詢標識；

所述資料讀取單元83，可以從可信儲存庫中獲取與所述隨機數查詢標識對應的生產隨機數；

所述密鑰產生單元81，可以根據所述唯一暗碼與所述生產隨機數的組合，單向產生生產加密密鑰。

在一種實施方式中，

所述資料讀取單元83，從可信儲存庫中獲取與所述隨機數查詢密鑰對應的第n隨機數；

所述密鑰產生單元81，根據所述第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰，

其中，n為大於0的自然數。

在一種實施方式中，

所述密鑰產生單元81，根據所述唯一暗碼與所述生產隨機數的組合，單向產生生產加密密鑰，再單向產生第1流通密鑰，再單向產生生產信息查詢標識；

所述資料讀取單元83，根據所述生產信息查詢標識，從區塊鏈中讀取生產信息集合中的生產信息加密資料；則

所述密鑰產生單元81，根據所述第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰，再單向產生第

n+1流通密鑰，再單向產生第n流通信息查詢標識；

所述資料讀取單元83，根據所述第n流通信息查詢標識，從區塊鏈中讀取第n信息集合中的第n流通信息加密資料。

圖16是本說明書的一個實施例電子設備的結構示意圖。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16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，程式可以包括程式代碼，所述程式代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，在邏輯層面上形成會話窗口中信息對話框的描繪裝置。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：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

根據所述生產加密密鑰，產生生產信息查詢標識；

將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

還可以用於執行以下操作：

根據第n公鑰，單向產生第n流通密鑰查詢標識；

根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

根據所述第n流通密鑰，單向產生第n加密密鑰；

根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

還可以用於執行以下操作：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，產生生產信息查詢標識；

根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

上述如本說明書圖16所示實施例提供的業務反饋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說明書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見的處理器等。結合本說明書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13至圖15中的基於區塊鏈的產品信息加密、解密裝置執行的方法，並實現基於區塊鏈的產品信息加密、解密裝置在圖16所示實施例的功能，本說明書實施例在此不再贅述。

本說明書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16所示實施例中業務反饋裝置執行的方法，並具體用於執行：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

根據所述生產加密密鑰，產生生產信息查詢標識；

將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

還可以用於執行：

根據第n公鑰，單向產生第n流通密鑰查詢標識；

根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

根據所述第n流通密鑰，單向產生第n加密密鑰；

根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

還可以用於執行：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，產生生產信息查詢標識；

根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

上述實施例闡明的系統、裝置、模組或單元，具體可以由電腦晶片或實體實現，或者由具有某種功能的產品來實現。一種典型的實現設備為電腦。具體的，電腦例如可以為個人電腦、膝上型電腦、蜂巢式電話、相機電話、智慧電話、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、穿戴式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，在實施本說明書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，本說明書的實施例可提

供為方法、系統、或電腦程式產品。因此，本說明書可採用完全硬體實施例、完全軟體實施例、或結合軟體和硬體方面的實施例的形式。而且，本說明書可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體（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。

本說明書是參照根據本說明書實施例的方法、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，本說明書的實施例可提供為方法、系統或電腦程式產品。因此，本說明書可採用完全硬體實施例、完全軟體實施例或結合軟體和硬體方面的實施例的形式。而且，本說明書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。

本說明書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歷程、程式、對象、組件、資料結構等等。也可以在分散式計算環境中實踐本說明書，在這些分散式計算環境中，由透過通信網路而被連接的遠程處理設備來執行任務。在分散式計算環境中，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。

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

【符號說明】

12：步驟

14：步驟

16：步驟

18：步驟

22：步驟

24：步驟

26：步驟

28：步驟

32：步驟

34：步驟

36：步驟

38：步驟

310：步驟

312：步驟

42：步驟

44：步驟

46：步驟

48：步驟

410：步驟

412：步驟

414：步驟

52：步驟

54：步驟

56：步驟

58：步驟

510：步驟

512：步驟

514：步驟

61：密鑰產生單元

62：資料產生單元

63：標識產生單元

64：資料寫入單元

71：標識產生單元

72：資料讀取單元

73：資料解析單元

74：密鑰產生單元

75：資料加密單元

76：資料傳輸單元

81：密鑰產生單元

82：標識產生單元

83：資料讀取單元

84：資料解析單元

201926111

【發明摘要】

【中文發明名稱】

產品信息的加密、解密方法及裝置

【中文】

本說明書公開一種基於區塊鏈的產品信息加密、解密方法及裝置，可以由生產方以產品唯一暗碼為基礎，對生產信息進行加密，當存在流通方時可以根據唯一暗碼單向產生流通密鑰，而流通方可以繼續根據流通密鑰產生流通信息加密密鑰，對流通信息進行加密，根據流通信息加密密鑰再產生下一個流通密鑰。也就是以鏈式連環單向產生密鑰的方式，對產品信息進行加密，利用產品唯一暗碼除生產方和購買方以外無法獲知的特性，以及區塊鏈不可篡改不可偽造的特性，對生產信息進行加密和儲存，使得生產信息有很高的保密性。

【指定代表圖】第(1)圖。
【代表圖之符號簡單說明】無

【特徵化學式】無

【發明申請專利範圍】

【第1項】

一種基於區塊鏈的產品信息加密方法，所述方法應用於生產方，包括：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

根據所述生產加密密鑰，產生生產信息查詢標識；

將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

【第2項】

如申請專利範圍第1項所述的方法，其中根據產品的唯一暗碼，單向產生生產加密密鑰，具體包括：

接收生產方在生產所述產品時產生的生產隨機數；

根據所述唯一暗碼與所述生產隨機數的組合，單向產生生產加密密鑰。

【第3項】

如申請專利範圍第2項所述的方法，所述方法還包括：

根據所述唯一暗碼，單向產生隨機數查詢標識；

在可信儲存庫中為所述產品創建唯一標識；

將所述隨機數查詢標識以及所述生產隨機數發送至所述可信儲存庫，並均與所述唯一標識關聯。

【第4項】

如申請專利範圍第1項所述的方法，其中根據所述生產加密密鑰，產生生產信息查詢標識，具體包括：

根據所述生產加密密鑰，單向產生第1流通密鑰，再根據所述第1流通密鑰，單向產生生產信息查詢標識；則

將生產信息集合寫入區塊鏈，具體包括：

根據第1公鑰，對第1流通密鑰進行加密，產生第1流通密鑰加密資料，所述第1公鑰為第1次序流通方的流通公鑰；

根據第1公鑰，單向產生第1流通密鑰查詢標識；

將生產信息集合寫入區塊鏈，所述生產信息集合包含所述第1接收密鑰查詢標識、生產信息查詢標識、第1接收密鑰加密資料以及生產信息加密資料。

【第5項】

如申請專利範圍第4項所述的方法，其中根據第1公鑰，對第1流通密鑰進行加密，產生第1流通密鑰加密資料，具體包括：

根據第1公鑰，對產品的公開明碼與第1流通密鑰的組合進行加密，產生第1流通密鑰加密資料。

【第6項】

如申請專利範圍第4項所述的方法，其中將生產信息集合寫入區塊鏈，具體包括：

根據生產私鑰，對所述生產信息集合進行簽名，所述生產私鑰為生產方在生產所述產品時產生的私鑰；

將簽名後的生產信息集合寫入區塊鏈。

【第7項】

一種基於區塊鏈的產品信息加密方法，所述方法應用於流通方，包括：

根據第n公鑰，單向產生第n流通密鑰查詢標識；

根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

根據所述第n流通密鑰，單向產生第n加密密鑰；

根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

【第8項】

如申請專利範圍第7項所述的方法，其中根據所述第n流通密鑰，單向產生第n加密密鑰，具體包括：

接收第n次序流通方在接收產品時產生的第n隨機數；

根據所述第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰。

【第9項】

如申請專利範圍第8項所述的方法，所述方法還包括：

將所述第n隨機數發送至可信儲存庫，並與所述產品的唯一標識關聯。

【第10項】

如申請專利範圍第9項所述的方法，其中根據所述第n加密密鑰，產生第n流通信息查詢標識，具體包括：

根據所述第n加密密鑰，單向產生第n+1流通密鑰，再根據第n+1流通密鑰，單向產生第n流通信息查詢標識；則

將第n信息集合寫入區塊鏈，具體包括：

根據第n+1公鑰，對第n+1流通密鑰進行加密，產生第n+1流通密鑰加密資料，所述第n+1公鑰為第n+1次序流通方的流通公鑰；

根據第n+1公鑰，單向產生第n+1流通密鑰查詢標識；

將第n信息集合寫入區塊鏈，所述第n信息集合包含所述第n+1接收密鑰查詢標識、第n流通信息查詢標識、第n+1接收密鑰加密資料以及第n流通信息加密資料。

【第11項】

如申請專利範圍第10項所述的方法，其中根據第n+1公鑰，對第n+1流通密鑰進行加密，產生第n+1流通密鑰加密資料，具體包括：

根據第n+1公鑰，對產品的公開明碼與第n+1流通密鑰的組合進行加密，產生第n+1流通密鑰加密資料。

【第12項】

如申請專利範圍第10項所述的方法，其中將第n信息集合寫入區塊鏈，具體包括：

根據第n私鑰，對所述第n信息集合進行簽名；

將簽名後的第n信息集合寫入區塊鏈。

【第13項】

如申請專利範圍第7項所述的方法，其中根據第n私鑰，對所述第n流通密鑰加密資料進行解密之前，所述方法還包括：

根據生產公鑰，對簽名後的生產信息集合進行簽名驗證；或

根據第n公鑰，對簽名後的第n信息集合進行簽名驗證。

【第14項】

一種基於區塊鏈的產品信息解密方法，所述方法應用於購買方，包括：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，產生生產信息查詢標識；

根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

【第15項】

如申請專利範圍第14項所述的方法，所述方法還包括：

根據所述生產加密密鑰，單向產生第1流通密鑰，根據所述第n流通密鑰，單向產生第n加密密鑰，根據第n加

密密鑰，單向產生第n+1流通密鑰；

根據所述第n流通信息查詢標識，從區塊鏈中讀取所述產品的第n流通信息加密資料；

根據所述第n加密密鑰，對所述第n流通信息加密資料進行解密，獲得第n流通信息；

其中，n為大於0的自然數。

【第16項】

如申請專利範圍第14項所述的方法，其中根據產品的唯一暗碼，單向產生生產加密密鑰，具體包括：

根據產品的唯一暗碼，單向產生隨機數查詢標識；

從可信儲存庫中獲取與所述隨機數查詢標識對應的生產隨機數；

根據所述唯一暗碼與所述生產隨機數的組合，單向產生生產加密密鑰。

【第17項】

如申請專利範圍第15項所述的方法，其中根據所述第n流通密鑰，單向產生第n加密密鑰，具體包括：

從可信儲存庫中獲取與所述隨機數查詢密鑰對應的第n隨機數；

根據所述第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰，

其中，n為大於0的自然數。

【第18項】

如申請專利範圍第17項所述的方法，其中從區塊鏈中

讀取所述產品的生產信息加密資料，具體包括：

根據所述唯一暗碼與所述生產隨機數的組合，單向產生生產加密密鑰，再單向產生第1流通密鑰，再單向產生生產信息查詢標識；

根據所述生產信息查詢標識，從區塊鏈中讀取生產信息集合中的生產信息加密資料；則

從區塊鏈中讀取所述產品的第n流通信息加密資料，具體包括：

根據所述第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰，再單向產生第n+1流通密鑰，再單向產生第n流通信息查詢標識；

根據所述第n流通信息查詢標識，從區塊鏈中讀取第n信息集合中的第n流通信息加密資料。

【第19項】

一種基於區塊鏈的產品信息加密裝置，所述裝置應用於生產方，包括：密鑰產生單元、資料產生單元、標識產生單元、資料寫入單元，其中，

所述密鑰產生單元，根據產品的唯一暗碼，單向產生生產加密密鑰；

所述資料產生單元，根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

所述標識產生單元，根據所述生產加密密鑰，產生生產信息查詢標識；

所述資料傳輸單元，將生產信息集合寫入區塊鏈，所

述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

【第20項】

如申請專利範圍第19項所述的裝置，其中所述密鑰產生單元，

接收生產方在生產所述產品時產生的生產隨機數；

根據所述唯一暗碼與所述生產隨機數的組合，單向產生生產加密密鑰。

【第21項】

如申請專利範圍第20項所述的裝置，其中：

所述標識產生單元，根據所述唯一暗碼，單向產生隨機數查詢標識；

所述資料傳輸單元，

在可信儲存庫中為所述產品創建唯一標識；

將所述隨機數查詢標識以及所述生產隨機數發送至所述可信儲存庫，並均與所述唯一標識關聯。

【第22項】

如申請專利範圍第19項所述的裝置，其中所述標識產生單元，

根據所述生產加密密鑰，單向產生第1流通密鑰，再根據所述第1流通密鑰，單向產生生產信息查詢標識；則

所述資料產生單元，

根據第1公鑰，對第1流通密鑰進行加密，產生第1流通密鑰加密資料，所述第1公鑰為第1次序流通方的流通公

鑰；

根據第1公鑰，單向產生第1流通密鑰查詢標識；

所述資料傳輸單元，

將生產信息集合寫入區塊鏈，所述生產信息集合包含所述第1接收密鑰查詢標識、生產信息查詢標識、第1接收密鑰加密資料以及生產信息加密資料。

【第23項】

如申請專利範圍第22項所述的裝置，其中所述資料產生單元，

根據第1公鑰，對產品的公開明碼與第1流通密鑰的組合進行加密，產生第1流通密鑰加密資料。

【第24項】

如申請專利範圍第22項所述的裝置，其中所述資料傳輸單元，

根據生產私鑰，對所述生產信息集合進行簽名，所述生產私鑰為生產方在生產所述產品時產生的私鑰；

將簽名後的生產信息集合寫入區塊鏈。

【第25項】

一種基於區塊鏈的產品信息加密裝置，所述裝置應用於流通方，包括：標識產生單元、資料讀取單元、資料解析單元、密鑰產生單元、資料加密單元、資料傳輸單元，其中，

所述標識產生單元，根據第n公鑰，單向產生第n流通密鑰查詢標識；

所述資料讀取單元，根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

所述資料解析單元，根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

所述密鑰產生單元，根據所述第n流通密鑰，單向產生第n加密密鑰；

所述資料加密單元，根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

所述資料傳輸單元，將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

【第26項】

如申請專利範圍第25項所述的裝置，其中所述密鑰產生單元，

接收第n次序流通方在接收產品時產生的第n隨機數；

根據所述第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰。

【第27項】

如申請專利範圍第26項所述的裝置，其中所述資料傳輸單元，

將所述第n隨機數發送至可信儲存庫，並與所述產品的唯一標識關聯。

【第28項】

如申請專利範圍第27項所述的裝置，其中所述標識產生單元，

根據所述第n加密密鑰，單向產生第n+1流通密鑰，再根據第n+1流通密鑰，單向產生第n流通信息查詢標識；則

所述密鑰產生單元，根據第n+1公鑰，對第n+1流通密鑰進行加密，產生第n+1流通密鑰加密資料，所述第n+1公鑰為第n+1次序流通方的流通公鑰；

所述標識產生單元，根據第n+1公鑰，單向產生第n+1流通密鑰查詢標識；

所述資料傳輸單元，將第n信息集合寫入區塊鏈，所述第n信息集合包含所述第n+1接收密鑰查詢標識、第n流通信息查詢標識、第n+1接收密鑰加密資料以及第n流通信息加密資料。

【第29項】

如申請專利範圍第28項所述的裝置，其中所述資料加密單元，

根據第n+1公鑰，對產品的公開明碼與第n+1流通密鑰的組合進行加密，產生第n+1流通密鑰加密資料。

【第30項】

如申請專利範圍第28項所述的裝置，其中所述資料傳輸單元，

根據第n私鑰，對所述第n信息集合進行簽名；

將簽名後的第n信息集合寫入區塊鏈。

【第31項】

如申請專利範圍第25項所述的裝置，其中所述資料解析單元，根據第n私鑰，對所述第n流通密鑰加密資料進行解密之前，

根據生產公鑰，對簽名後的生產信息集合進行簽名驗證；或

根據第n公鑰，對簽名後的第n信息集合進行簽名驗證。

【第32項】

一種基於區塊鏈的產品信息解密裝置，所述裝置應用於購買方，包括：密鑰產生單元、標識產生單元、資料讀取單元、以及資料解析單元，其中，

所述密鑰產生單元，根據產品的唯一暗碼，單向產生生產加密密鑰；

所述標識產生單元，根據所述生產加密密鑰，產生生產信息查詢標識；

所述資料讀取單元，根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

所述資料解析單元，根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

【第33項】

如申請專利範圍第32項所述的裝置，其中：

所述密鑰產生單元，根據所述生產加密密鑰，單向產生第1流通密鑰，根據所述第n流通密鑰，單向產生第n加

密密鑰，根據第n加密密鑰，單向產生第n+1流通密鑰；

所述資料讀取單元，根據所述第n流通信息查詢標識，從區塊鏈中讀取所述產品的第n流通信息加密資料；

所述資料解析單元，根據所述第n加密密鑰，對所述第n流通信息加密資料進行解密，獲得第n流通信息；

其中，n為大於0的自然數。

【第34項】

如申請專利範圍第32項所述的裝置，其中：

所述密鑰產生單元，根據產品的唯一暗碼，單向產生隨機數查詢標識；

所述資料讀取單元，從可信儲存庫中獲取與所述隨機數查詢標識對應的生產隨機數；

所述密鑰產生單元，根據所述唯一暗碼與所述生產隨機數的組合，單向產生生產加密密鑰。

【第35項】

如申請專利範圍第33項所述的裝置，其中：

所述資料讀取單元，從可信儲存庫中獲取與所述隨機數查詢密鑰對應的第n隨機數；

所述密鑰產生單元，根據所述第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰，

其中，n為大於0的自然數。

【第36項】

如申請專利範圍第35項所述的裝置，其中：

所述密鑰產生單元，根據所述唯一暗碼與所述生產隨

機數的組合，單向產生生產加密密鑰，再單向產生第1流通密鑰，再單向產生生產信息查詢標識；

所述資料讀取單元，根據所述生產信息查詢標識，從區塊鏈中讀取生產信息集合中的生產信息加密資料；則

所述密鑰產生單元，根據所述第n流通密鑰與所述第n隨機數的組合，單向產生第n加密密鑰，再單向產生第n+1流通密鑰，再單向產生第n流通信息查詢標識；

所述資料讀取單元，根據所述第n流通信息查詢標識，從區塊鏈中讀取第n信息集合中的第n流通信息加密資料。

【第37項】

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：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

根據所述生產加密密鑰，產生生產信息查詢標識；

將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

【第38項】

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：

根據第n公鑰，單向產生第n流通密鑰查詢標識；

根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

根據所述第n流通密鑰，單向產生第n加密密鑰；

根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

【第39項】

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：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，產生生產信息查詢標識；

根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

根據所述生產加密密鑰，對所述生產信息加密資料進

行解密，獲得生產信息。

【第40項】

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當被包括多個應用程式的電子設備執行時，使得所述電子設備執行以下操作：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，對所述產品的生產信息進行加密，產生生產信息加密資料；

根據所述生產加密密鑰，產生生產信息查詢標識；

將生產信息集合寫入區塊鏈，所述生產信息集合包含生產信息查詢標識、以及生產信息加密資料。

【第41項】

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當被包括多個應用程式的電子設備執行時，使得所述電子設備執行以下操作：

根據第n公鑰，單向產生第n流通密鑰查詢標識；

根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料；

根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰；

根據所述第n流通密鑰，單向產生第n加密密鑰；

根據第n加密密鑰，對第n流通信息進行加密，產生第

n流通信息加密資料；

根據所述第n加密密鑰，產生第n流通信息查詢標識；

將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料；

其中，n為大於0的自然數。

【第42項】

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當被包括多個應用程式的電子設備執行時，使得所述電子設備執行以下操作：

根據產品的唯一暗碼，單向產生生產加密密鑰；

根據所述生產加密密鑰，產生生產信息查詢標識；

根據所述生產信息查詢標識，從區塊鏈中讀取所述產品的生產信息加密資料；

根據所述生產加密密鑰，對所述生產信息加密資料進行解密，獲得生產信息。

【發明圖式】

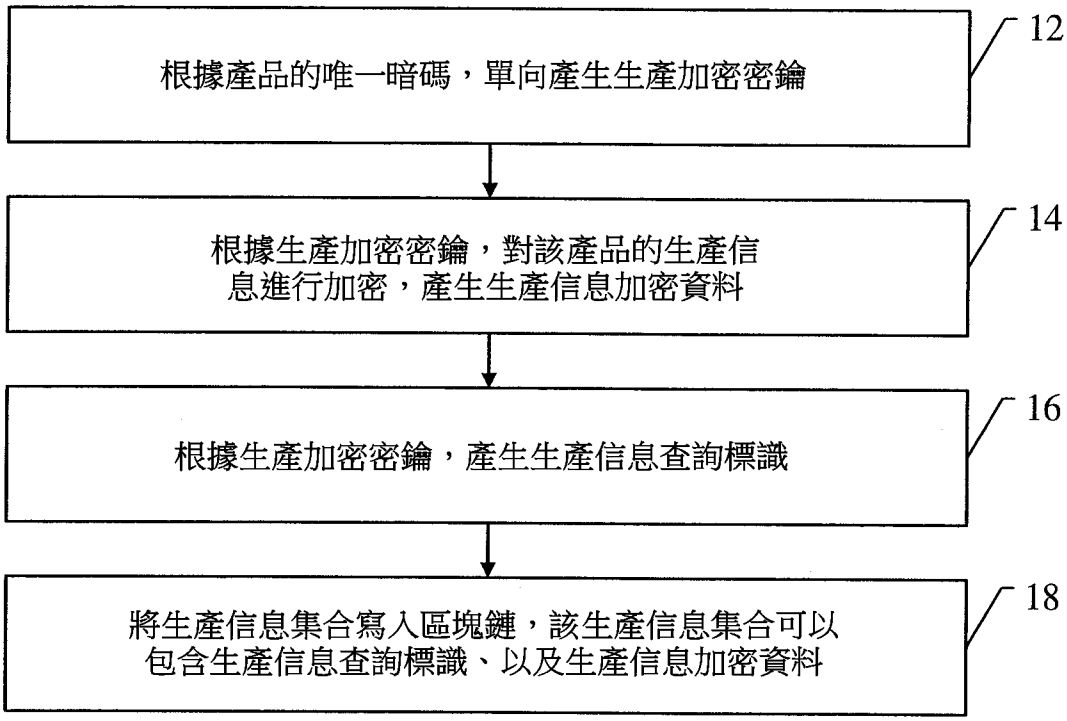
根據產品的唯一暗碼，單向產生生產加密密鑰
12
根據生產加密密鑰，對該產品的生產信息進行加密，產生生產信息加密資料
14
根據生產加密密鑰，產生生產信息查詢標識
16
將生產信息集合寫入區塊鏈，該生產信息集合可以包含生產信息查詢標識、以及生產信息加密資料
18

圖 1

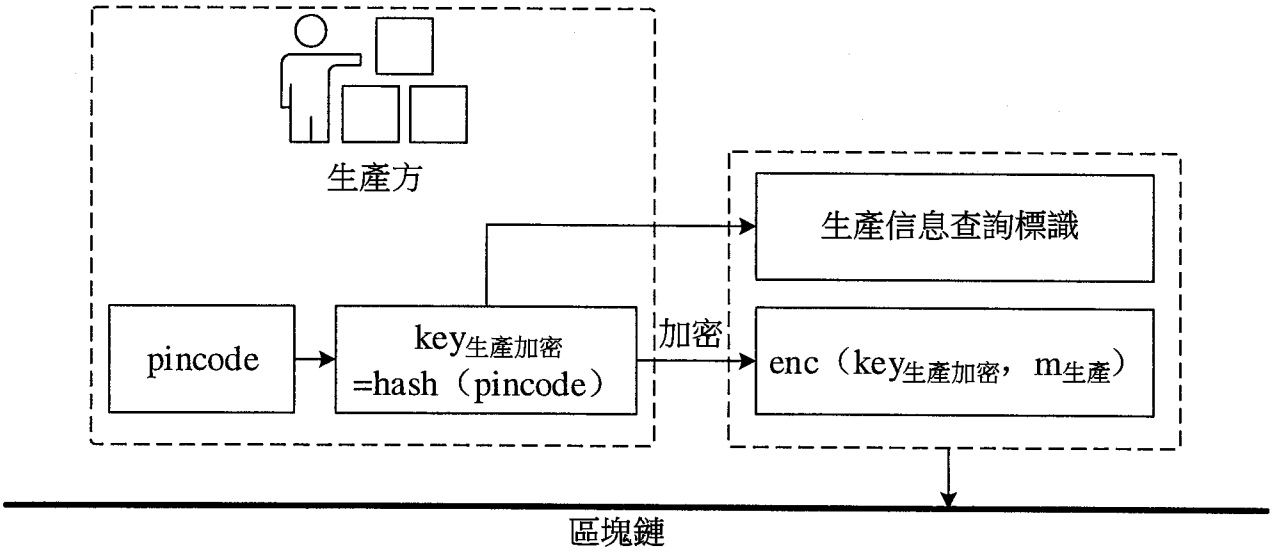
生產方
pincode
key生產加密 =hash（pincode）
加密
生產信息查詢標識
enc（key生產加密， m生產）
區塊鏈

圖 2

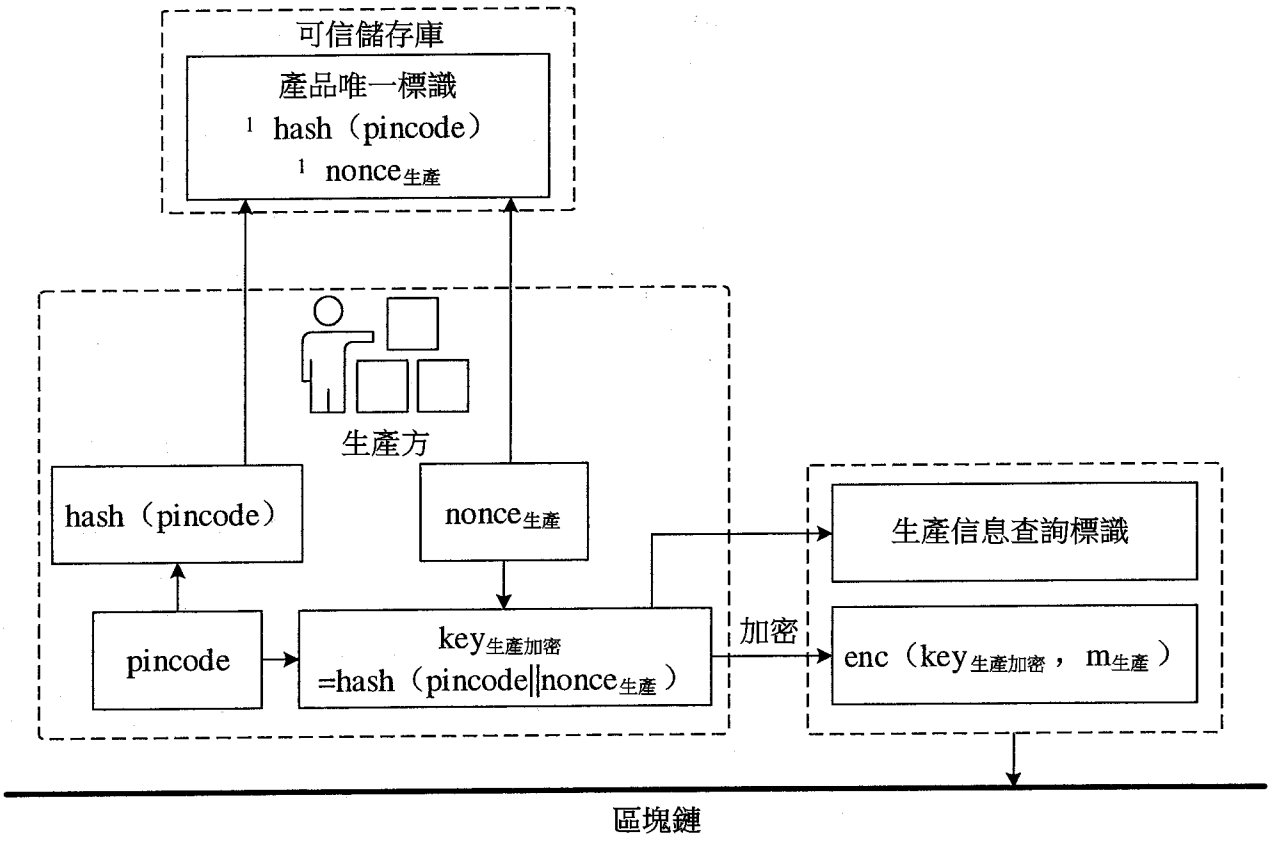
可信儲存庫
產品唯一標識
1 hash（pincode）
1 nonce生產
生產方
hash（pincode）
nonce生產
pincode
key生產加密
=hash（pincode||nonce生產）
加密
生產信息查詢標識
enc（key生產加密， m生產）
區塊鏈

圖 3

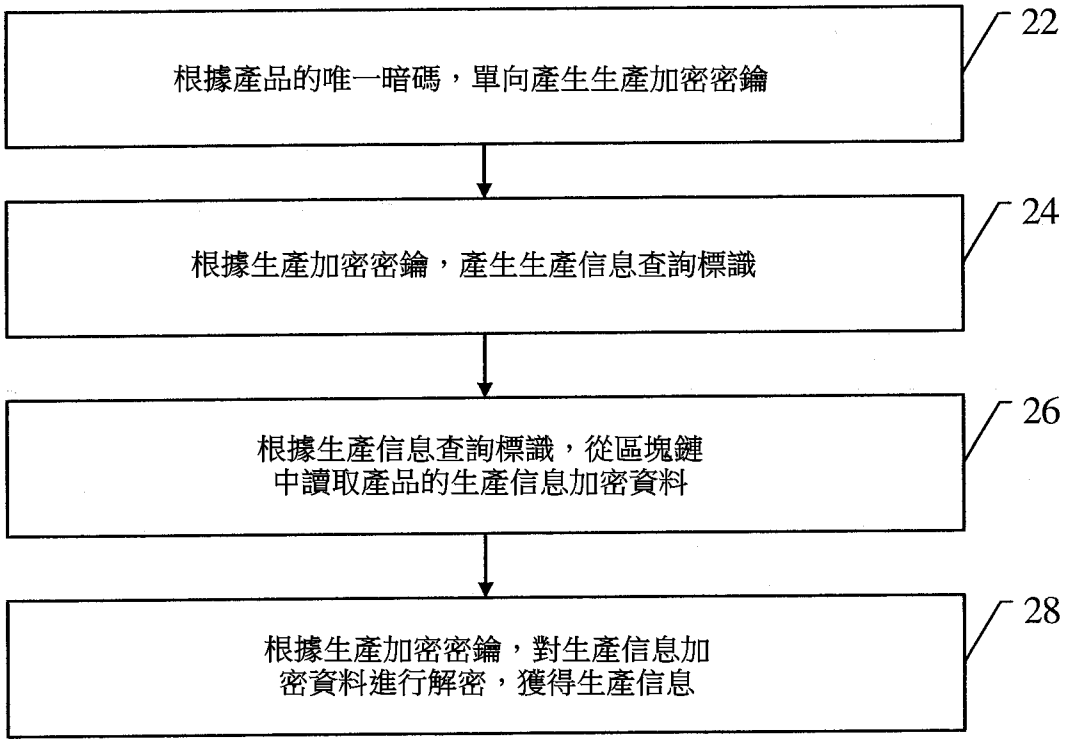
根據產品的唯一暗碼，單向產生生產加密密鑰
22
根據生產加密密鑰，產生生產信息查詢標識
24
根據生產信息查詢標識，從區塊鏈
中讀取產品的生產信息加密資料
26
根據生產加密密鑰，對生產信息加
密資料進行解密，獲得生產信息
28

圖 4

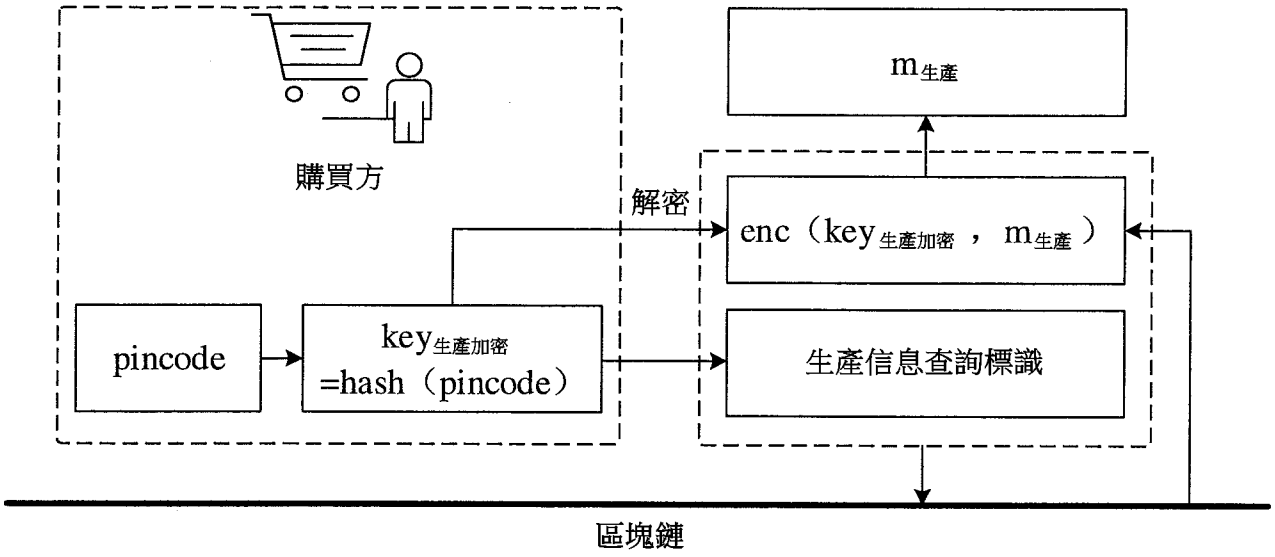
購買方
pincode
key生產加密
=hash（pincode）
解密
m生產
enc（key生產加密，m生產）
生產信息查詢標識
區塊鏈

圖 5

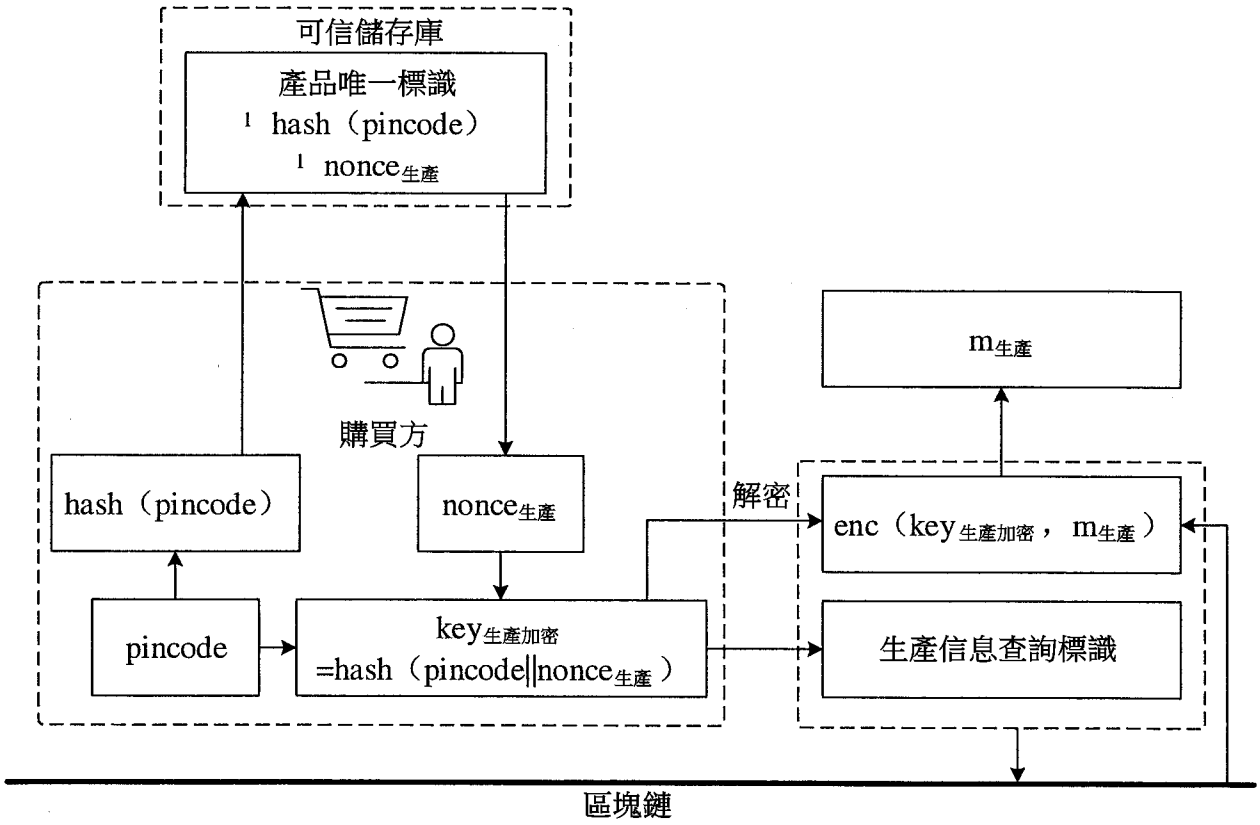
可信儲存庫
產品唯一標識
‖ hash（pincode）
‖ nonce生產
購買方
hash（pincode）
nonce生產
pincode
key生產加密
=hash（pincode‖nonce生產）
解密
m生產
enc（key生產加密，m生產）
生產信息查詢標識
區塊鏈

圖 6

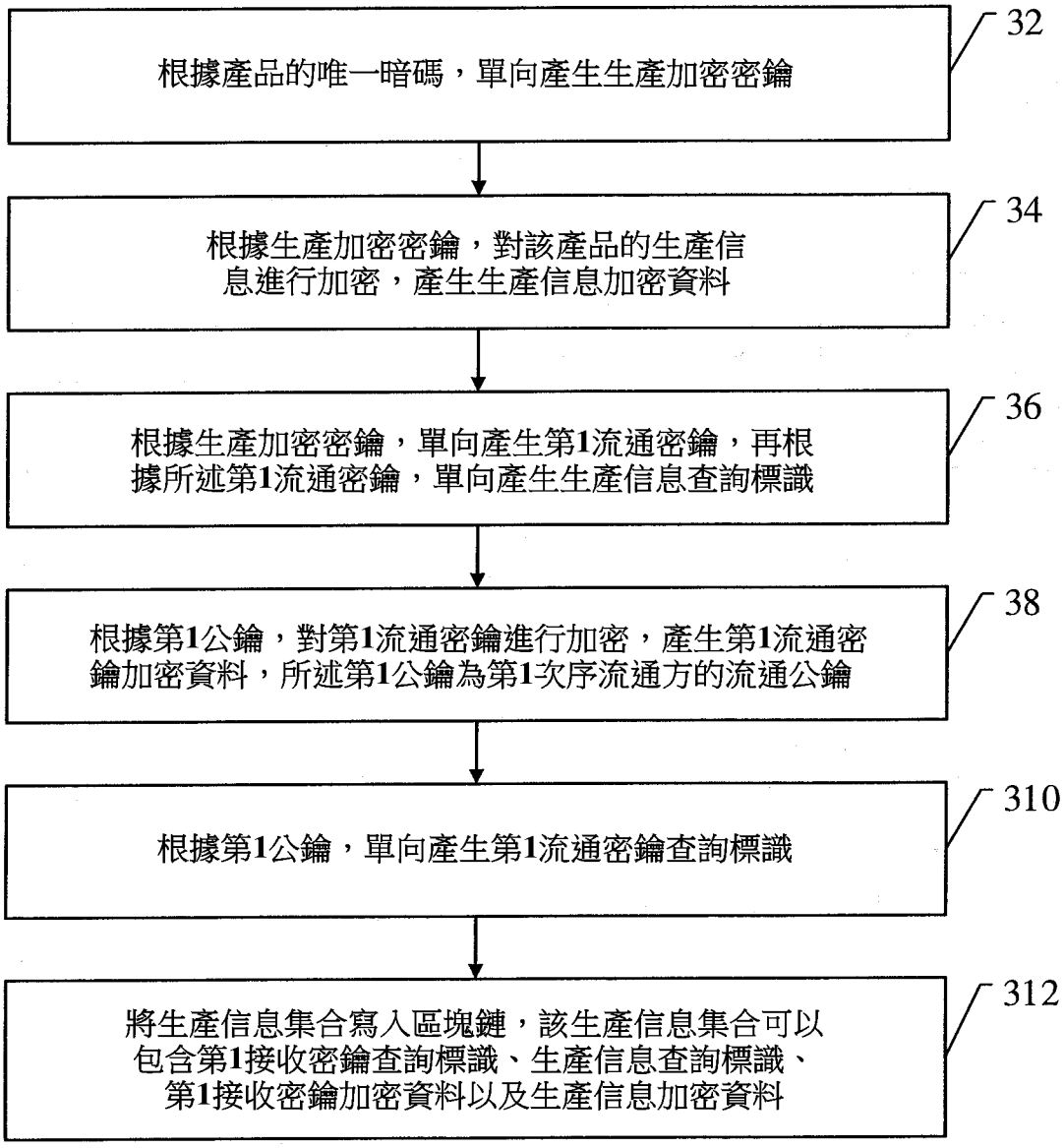
根據產品的唯一暗碼，單向產生生產加密密鑰
32
根據生產加密密鑰，對該產品的生產信息進行加密，產生生產信息加密資料
34
根據生產加密密鑰，單向產生第1流通密鑰，再根據所述第1流通密鑰，單向產生生產信息查詢標識
36
根據第1公鑰，對第1流通密鑰進行加密，產生第1流通密鑰加密資料，所述第1公鑰為第1次序流通方的流通公鑰
38
根據第1公鑰，單向產生第1流通密鑰查詢標識
310
將生產信息集合寫入區塊鏈，該生產信息集合可以包含第1接收密鑰查詢標識、生產信息查詢標識、第1接收密鑰加密資料以及生產信息加密資料
312

圖 7

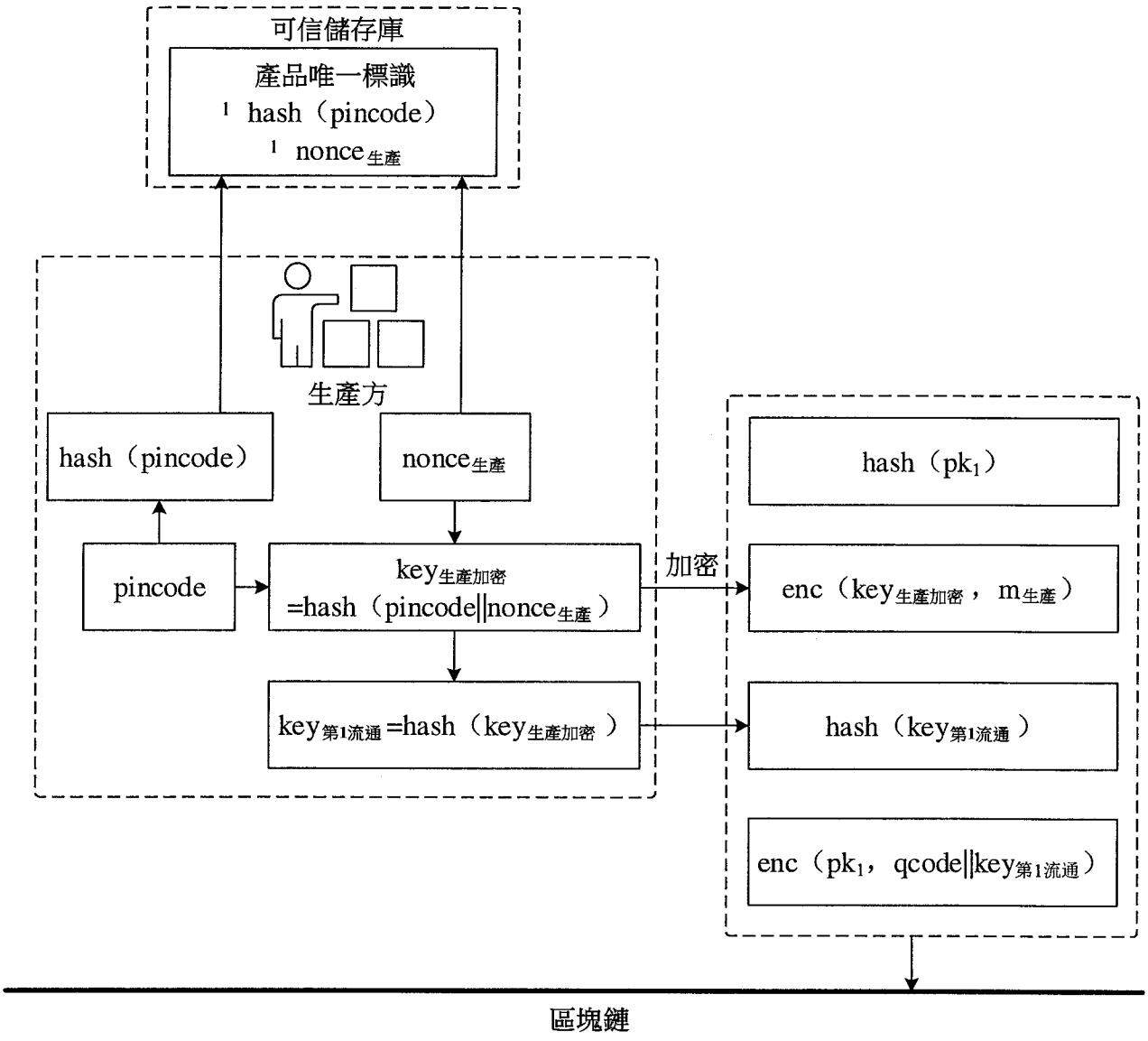
可信儲存庫
產品唯一標識
1 hash（pincode）
1 nonce生產
生產方
hash（pincode）
nonce生產
pincode
key生產加密
=hash（pincode||nonce生產）
key第1流通 =hash（key生產加密）
加密
hash（pk1）
enc（key生產加密，m生產）
hash（key第1流通）
enc（pk1，qcode||key第1流通）
區塊鏈

圖 8

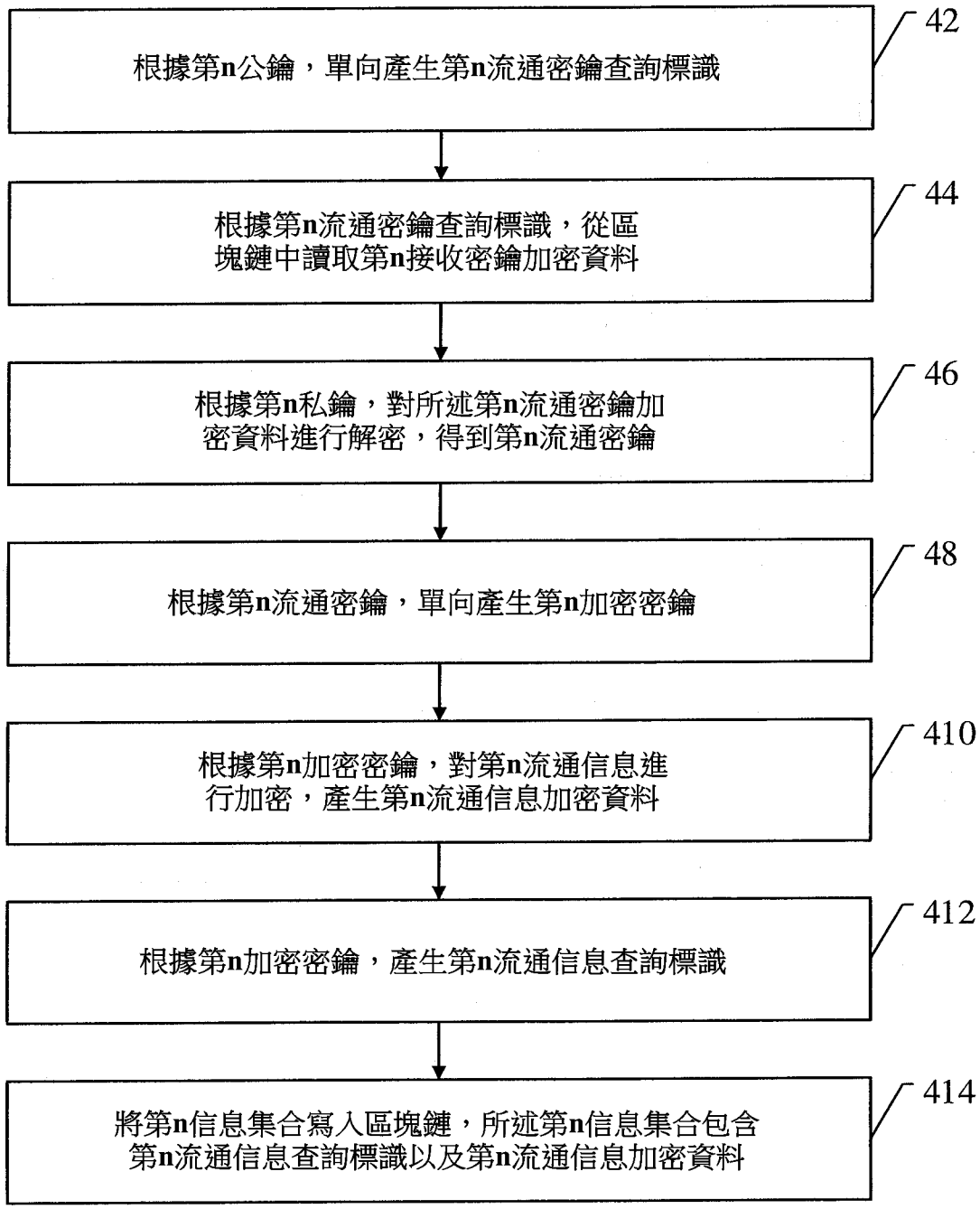
根據第n公鑰，單向產生第n流通密鑰查詢標識
42
根據第n流通密鑰查詢標識，從區塊鏈中讀取第n接收密鑰加密資料
44
根據第n私鑰，對所述第n流通密鑰加密資料進行解密，得到第n流通密鑰
46
根據第n流通密鑰，單向產生第n加密密鑰
48
根據第n加密密鑰，對第n流通信息進行加密，產生第n流通信息加密資料
410
根據第n加密密鑰，產生第n流通信息查詢標識
412
將第n信息集合寫入區塊鏈，所述第n信息集合包含第n流通信息查詢標識以及第n流通信息加密資料
414

圖 9

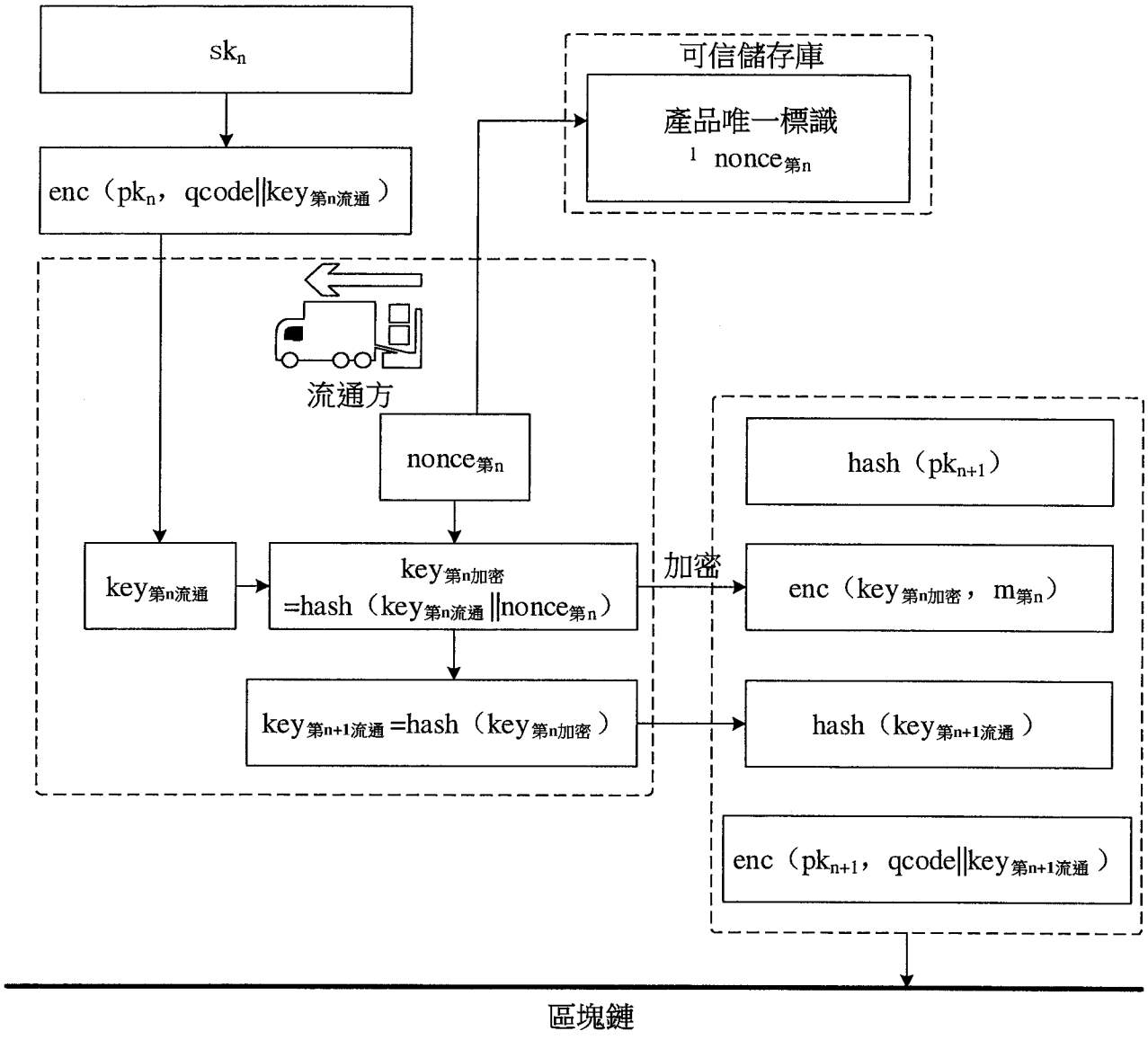
sk_n
可信儲存庫
產品唯一標識
1 $nonce_{第n}$
enc（pk_n，qcode||$key_{第n流通}$）
流通方
$nonce_{第n}$
$key_{第n流通}$
$key_{第n加密}$ =hash（$key_{第n流通}$ ||$nonce_{第n}$）
加密
hash（pk_{n+1}）
enc（$key_{第n加密}$，$m_{第n}$）
$key_{第n+1流通}$ =hash（$key_{第n加密}$）
hash（$key_{第n+1流通}$）
enc（pk_{n+1}，qcode||$key_{第n+1流通}$）
區塊鏈

圖 10

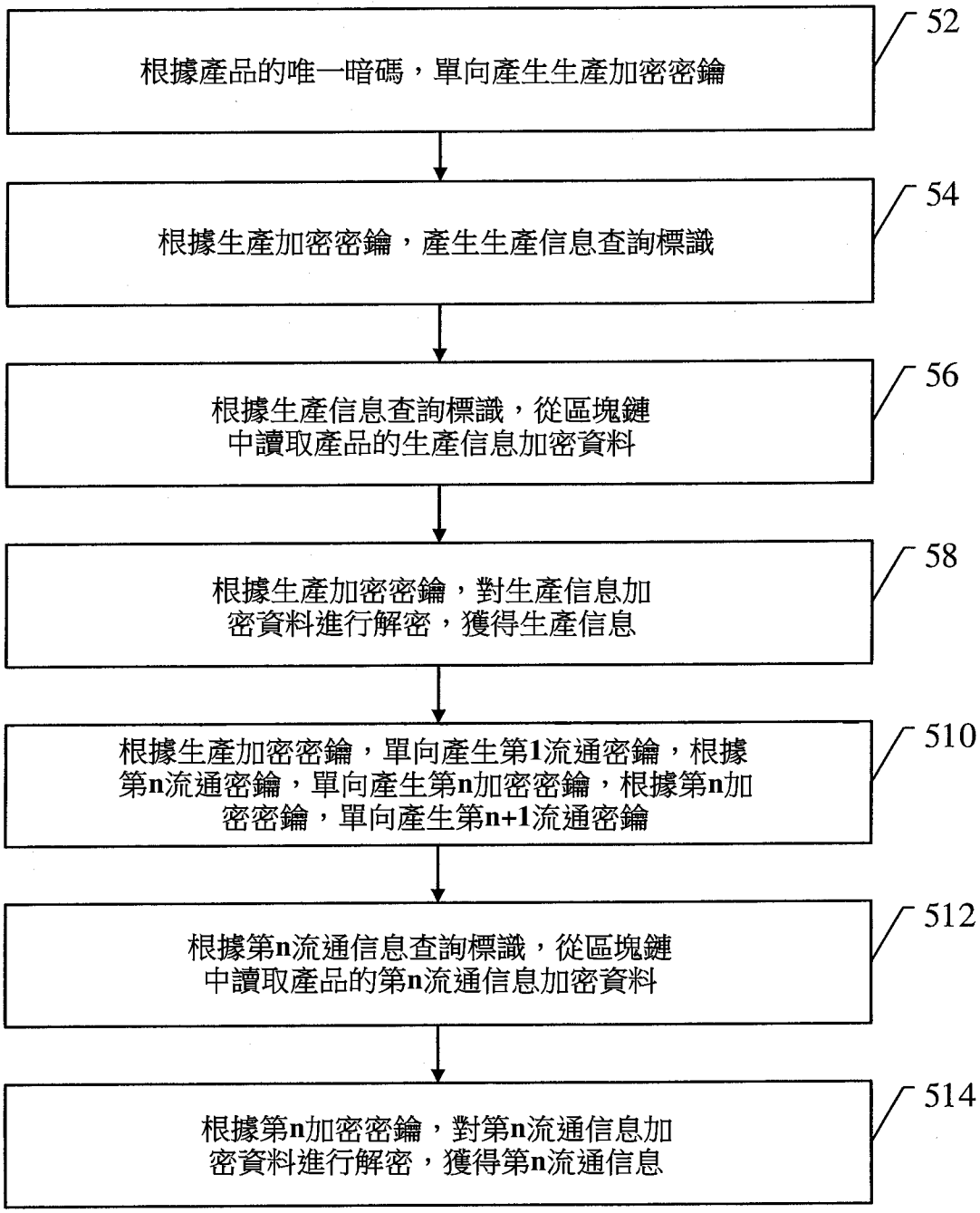
根據產品的唯一暗碼，單向產生生產加密密鑰
52
根據生產加密密鑰，產生生產信息查詢標識
54
根據生產信息查詢標識，從區塊鏈中讀取產品的生產信息加密資料
56
根據生產加密密鑰，對生產信息加密資料進行解密，獲得生產信息
58
根據生產加密密鑰，單向產生第1流通密鑰，根據第n流通密鑰，單向產生第n加密密鑰，根據第n加密密鑰，單向產生第n+1流通密鑰
510
根據第n流通信息查詢標識，從區塊鏈中讀取產品的第n流通信息加密資料
512
根據第n加密密鑰，對第n流通信息加密資料進行解密，獲得第n流通信息
514

圖 11

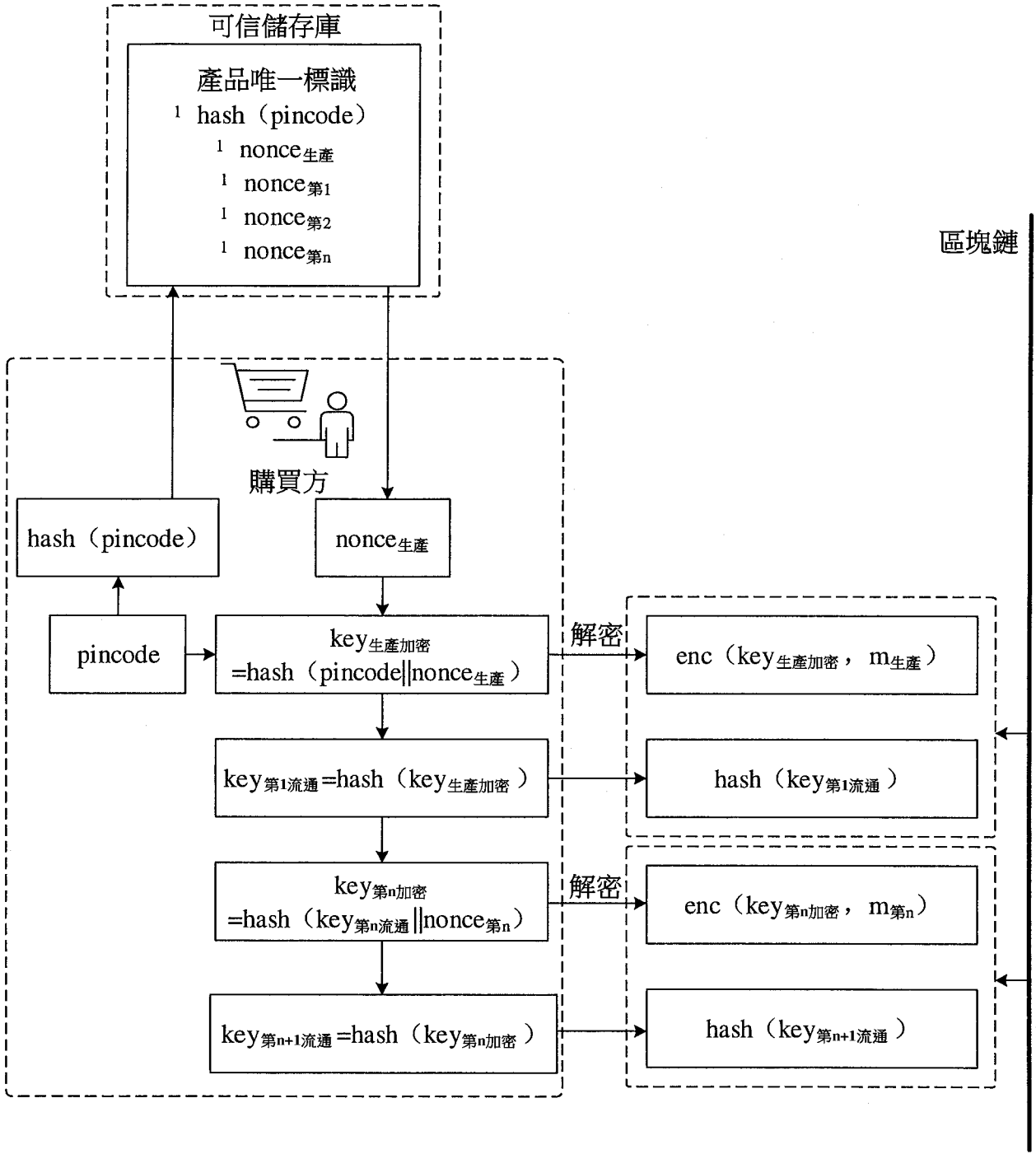
可信儲存庫
產品唯一標識
1 hash（pincode）
1 nonce生產
1 nonce第1
1 nonce第2
1 nonce第n
區塊鏈
購買方
hash（pincode）
nonce生產
pincode
key生產加密 =hash（pincode||nonce生產）
解密
enc（key生產加密， m生產）
key第1流通 =hash（key生產加密）
hash（key第1流通）
key第n加密 =hash（key第n流通||nonce第n）
解密
enc（key第n加密， m第n）
key第n+1流通 =hash（key第n加密）
hash（key第n+1流通）

圖 12

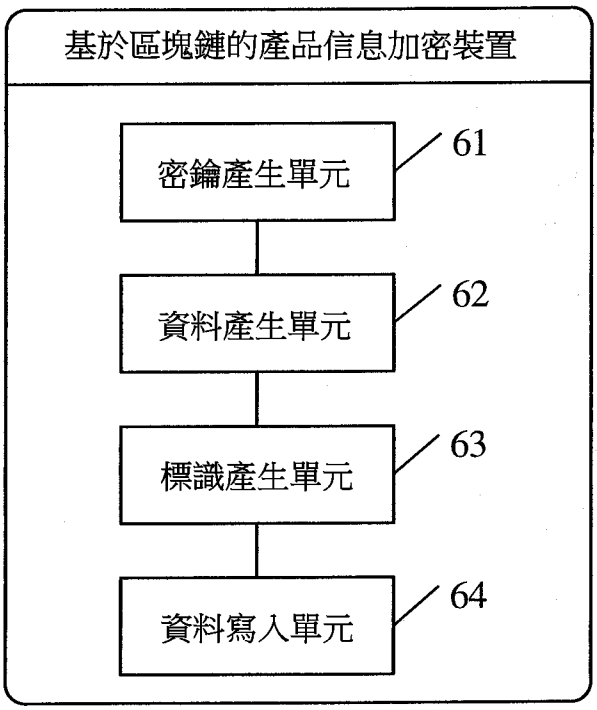

圖 13

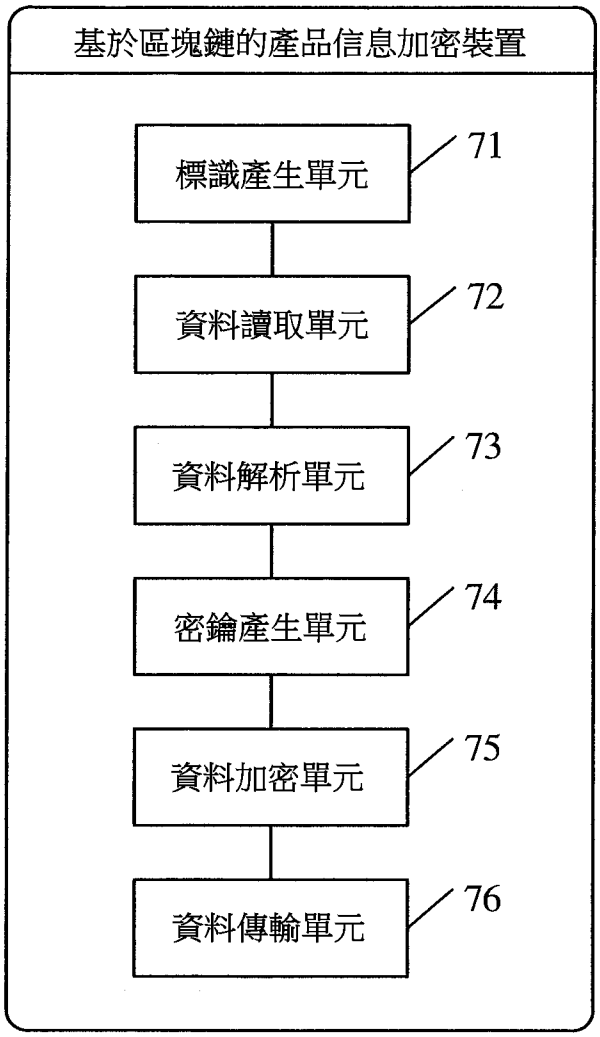
基於區塊鏈的產品信息加密裝置
標識產生單元
71
資料讀取單元
72
資料解析單元
73
密鑰產生單元
74
資料加密單元
75
資料傳輸單元
76

圖 14

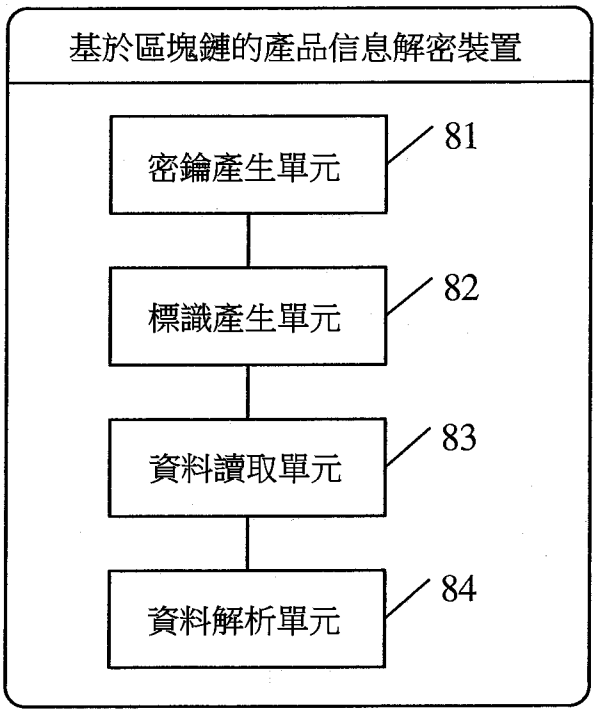
基於區塊鏈的產品信息解密裝置
密鑰產生單元
81
標識產生單元
82
資料讀取單元
83
資料解析單元
84

圖 15

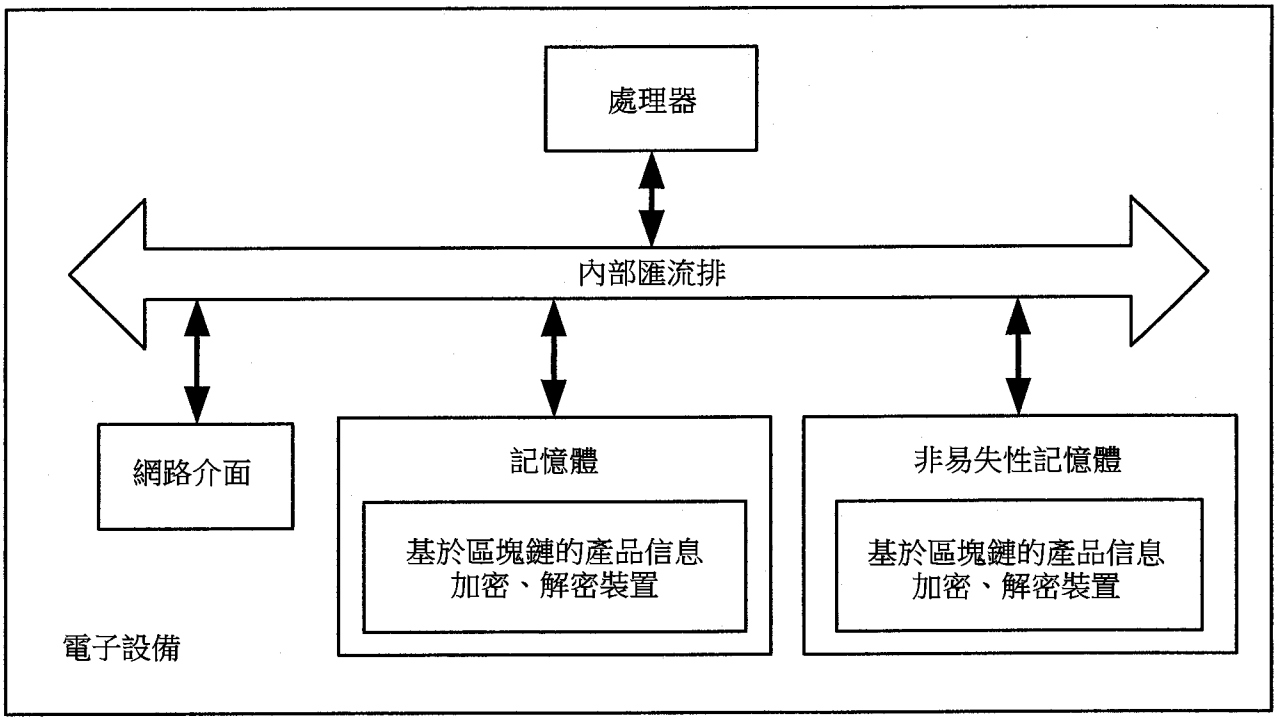
處理器
內部匯流排
網路介面
記憶體
基於區塊鏈的產品信息
加密、解密裝置
非易失性記憶體
基於區塊鏈的產品信息
加密、解密裝置
電子設備

圖 16