I753367

(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 I753367 B**

(45)公告日： 中華民國 111 (2022) 年 01 月 21 日

(21)申請案號：109106120 (22)申請日： 中華民國 109 (2020) 年 02 月 25 日

(51)Int. Cl.： *G06Q50/30 (2012.01)* *G06Q50/28 (2012.01)*
H04L29/08 (2006.01) *H04L9/32 (2006.01)*
G11B20/00 (2006.01)

(30)優先權：2019/02/25 美國 62/919,097
2019/04/06 美國 16/501,399

(71)申請人：英屬維爾京群島商東方海外（信息科技）控股有限公司 (英屬維爾京群島) OOCL (INFOTECH) HOLDINGS LIMITED (VG)
英屬維爾京群島

(72)發明人：黃 信鶴 WONG, SHUN HOK (US) ；蘇 慧明 SO, WEI MING BELINDA (US)

(74)代理人：陳長文

(56)參考文獻：

TW	201812674A	JP	4005619B2
US	2010/0031021A1	US	2018/0005186A1
US	2019/0012637A1		

審查人員：黃彥豪

申請專利範圍項數：20 項 圖式數：37 共 143 頁

(54)名稱

貨物運輸組織之零信任通信系統及其使用方法

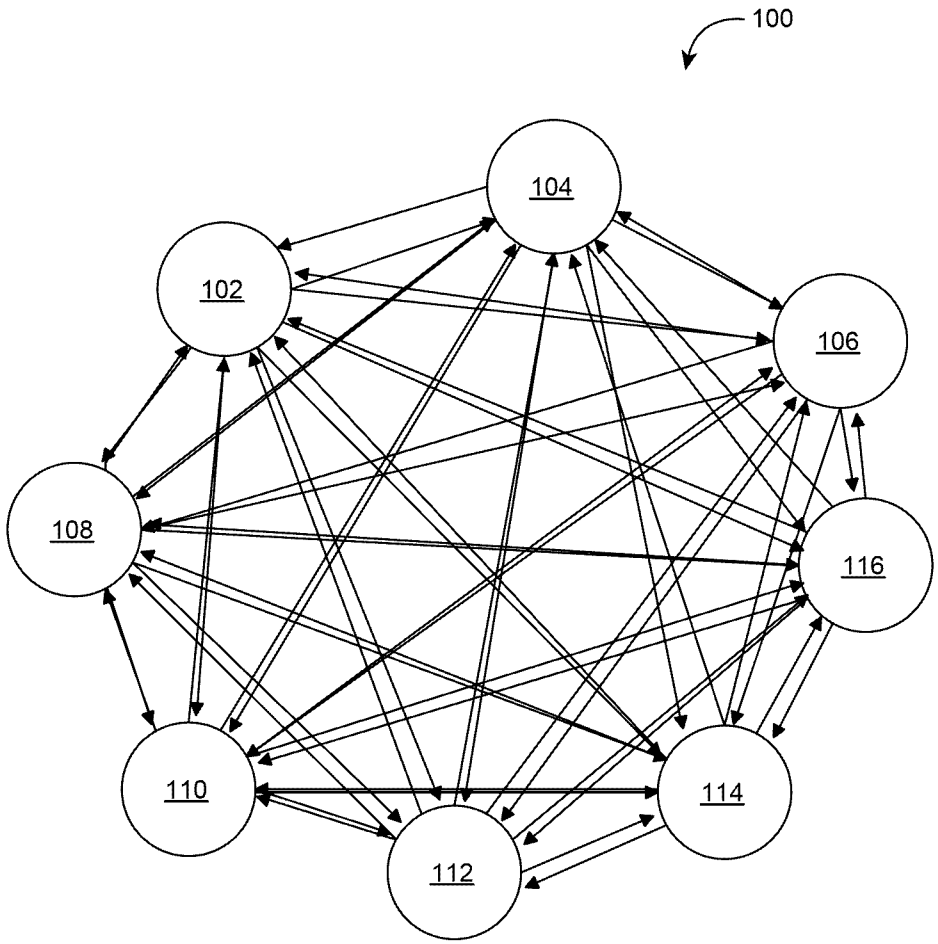
(57)摘要

本文中呈現與不同用戶端終端機安全地共用來自多個源之資料的系統及方法。一伺服器可建立用於定義一交易之一電子文件。該電子文件可具有資料欄位。每一資料欄位可係來自一用戶端終端機。該伺服器可識別用以將經包含於該電子文件中之該等對應資料欄位加密的加密金鑰。該伺服器可根據一存取控制原則來跨越該等用戶端終端機分佈該等加密金鑰。該存取控制原則可基於一用戶端終端機在該交易中之一角色而規定該用戶端終端機對該複數個資料欄位中之每一者的存取權限。該伺服器可經由根據該存取控制原則分佈之該等加密金鑰，向每一用戶端終端機提供對該電子文件中之該等資料欄位的存取。

Presented herein are systems and methods of securely sharing data from multiple sources with different client terminals. A server may establish an electronic document for defining a transaction. The electronic document may have data fields. Each data field may be from a client terminal. The server may identify encryption keys to encrypt the corresponding data fields included in the electronic document. The server may distribute the encryption keys across the client terminals in accordance with an access control policy. The access control policy may specify access permissions for a client terminal to each of the plurality of data fields based on a role of the client terminal in the transaction. The server may provide, to each client terminal with access to the data fields in the electronic document via the encryption keys distributed in accordance with the access control policy.

TW I753367 B

指定代表圖：



【圖1】

符號簡單說明：

102:托運人

104:代運人

106:承運人

108:碼頭

110:海關

112:港務局

114:收貨人

116:金融機構

專利案號：109106120

公告本

I753367

【發明摘要】

【中文發明名稱】

貨物運輸組織之零信任通信系統及其使用方法

【英文發明名稱】

ZERO TRUST COMMUNICATION SYSTEM FOR FREIGHT SHIPPING ORGANIZATIONS, AND METHODS OF USE

【中文】

本文中呈現與不同用戶端終端機安全地共用來自多個源之資料的系統及方法。一伺服器可建立用於定義一交易之一電子文件。該電子文件可具有資料欄位。每一資料欄位可係來自一用戶端終端機。該伺服器可識別用以將經包含於該電子文件中之該等對應資料欄位加密的加密金鑰。該伺服器可根據一存取控制原則來跨越該等用戶端終端機分佈該等加密金鑰。該存取控制原則可基於一用戶端終端機在該交易中之一角色而規定該用戶端終端機對該複數個資料欄位中之每一者的存取權限。該伺服器可經由根據該存取控制原則分佈之該等加密金鑰，向每一用戶端終端機提供對該電子文件中之該等資料欄位的存取。

【英文】

Presented herein are systems and methods of securely sharing data from multiple sources with different client terminals. A server may establish an electronic document for defining a transaction. The electronic document may have data fields. Each data field may be from a client terminal. The server may identify encryption keys to encrypt the corresponding data fields included in the electronic document. The

server may distribute the encryption keys across the client terminals in accordance with an access control policy. The access control policy may specify access permissions for a client terminal to each of the plurality of data fields based on a role of the client terminal in the transaction. The server may provide, to each client terminal with access to the data fields in the electronic document via the encryption keys distributed in accordance with the access control policy.

【指定代表圖】

圖1

【代表圖之符號簡單說明】

102:托運人

104:代運人

106:承運人

108:碼頭

110:海關

112:港務局

114:收貨人

116:金融機構

【發明說明書】

【中文發明名稱】

貨物運輸組織之零信任通信系統及其使用方法

【英文發明名稱】

ZERO TRUST COMMUNICATION SYSTEM FOR FREIGHT SHIPPING ORGANIZATIONS, AND METHODS OF USE

【技術領域】

【0001】 本發明係關於用於交換經加密資料之系統及方法，包含但不限於用於在零信任通信環境中交換經加密資料之系統及方法。

【先前技術】

【0002】 使用貨櫃長距離運送商品係一標準運輸形式。聯運貨櫃用於藉由汽車、火車及船來運送商品。單元係可堆疊的且經設計以在不打開貨櫃之情況下自一種形式之運送移動至另一種形式之運送。可涉及運送一或多個貨櫃之一運輸係一運輸承運人承諾使用聯運貨櫃或作為項目貨品(總稱為「貨品」或「貨物」)遞送商品。為了成功完成一運輸，需要在運輸中所涉及之不同當事方當中共用相關資料。此等當事方包含但不限於運輸承運人、運輸程序中之船舶經營者、港口/碼頭、政府機關以及運輸中之運輸方(包含托運人、收貨人，且有時包含代運人及通知方)。一貨物運輸中亦可涉及其他當事方。

【發明內容】

【0003】 在本文中闡述用於使用其中涉及零信任之一通信系統之系統及方法。該通信系統可經設計以與使用者一起工作，該等使用者可係彼此之直接競爭者或輔助競爭者，但有時期望或可需要在同一空間中工作以

便達成其業務目標。

【0004】 在運輸貨櫃(有時稱為聯運貨櫃)之裝載、卸載及移動中涉及之企業使用企業間(B2B)通信、電子資料互換(EDI)及應用程式設計介面(API)調用來彼此通信。此等通信頻道係點對點的，要求一個當事方與另一當事方通信。此通信之個體對個體性質一般不允許多個當事方同時「保持在循環中」。不同當事方在其如何處置通信方面採取之協定亦存在變化，因此通信可經延遲或受製於降低此類通信之及時性之企業原則定時。在移動貨物中當事方之地理分佈導致通信延遲。貨物可起源於亞洲且去往美洲、歐洲或非洲中之位置。嘗試一個當事方之通信之方便時間可係在另一當事方之營業時間之後，從而導致進一步延遲。

【0005】 彼此直接競爭之組織有時可共用資源以完成其企業職責。諸如兩個或兩個以上運輸公司共用其船舶來運送商品，使得可達成更佳服務覆蓋範圍以及規模經濟。另一實例係其中使用同一代運人之多個托運人可共用一單個聯運貨櫃以避免每一者必須付費且運輸單獨的部分地裝滿之聯運貨櫃。當公司可協調其活動時，實現其他經濟及更佳服務履行。然而，協調通常需要揭露機密資料，公司不願意這樣做。亦存在禁止與特定當事方共用特定類型之資料之法規要求。更一般而言，每一當事方皆具有機密資訊。保護機密資訊(諸如業務聯繫、客戶清單、定價資訊等)之需要對於在市場中維持一競爭優勢及法規遵從性係至關重要的。因此，彼此競爭或需要使用彼此之服務之當事方不會共用其機密資訊。

【0006】 處理聯運貨櫃且追蹤其位置之方法趨於聚焦於貨櫃之內容，或在小位置中而非在一全域意義上進行追蹤。因此，仍需要允許為一共同任務而一起工作之當事方共用呈一格式之機密資訊的一通信與資料控

制系統，該格式允許各個當事方僅看到他們執行其任務之部分所需要之資訊，同時使任何其他資訊對(資訊之)源保持機密。進一步需要可減少在運輸程序之路徑中之任何地方追蹤貨物所需要之時間且提供聯運貨櫃及項目貨品兩者之位置之及時更新的一系統。

【0007】 進一步需要為與聯運貨櫃及項目貨品之運送、交貨裝載及卸載相關聯之各個當事方提供此等運輸之一及時狀態及運輸更新，同時保護資料私密性及商業機密性。可藉由以下揭示內容滿足此等及其他目標。

【0008】 闡述一種用於產生一運輸文件之系統。該系統可具有一運輸文件控制中樞及一或多個使用者節點。該運輸文件控制中樞可具有一電腦，該電腦具有一邏輯、一記憶體及一通信裝置。該中樞亦可具有能夠發送及接收事件訊息之一訊息代理者。可存在儲存全域成員清單、存取原則文件清單及角色清單清單之一存取原則儲存庫。亦可存在儲存於該記憶體上之一公開金鑰儲存庫。亦可存在一識別碼(ID)儲存庫，該識別碼(ID)儲存庫具有一或多個使用者、一或多個使用者登入認證及一或多個使用者參數之一清單。亦可存在一區塊鏈資料庫，該區塊鏈資料庫包含儲存經加密運輸文件、經加密資料加密金鑰及文件發起者之簽章之一或多個區塊鏈節點。該等使用者節點可具有一電腦、一訊息代理者、用於將運輸文件解密之一金鑰儲存區、具有用於將運輸文件加密之一密碼層之一API介面及用於存取該運輸文件控制中樞之一入口網站中之一或多者。該API介面可在使用者電腦之邏輯上執行且與運輸文件控制中樞訊息代理者通信。

【0009】 亦闡述供在產生一單個共用運輸文件交易中使用之一獨立使用者節點。該使用者節點可具有一電腦，該電腦具有用於執行程式指令之一邏輯、一記憶體裝置、一使用者介面及用於存取一運輸文件控制中樞

之一通信裝置。該使用者節點可具有能夠發送及接收事件訊息之一訊息代理者。一API介面可具有一密碼存取層，該API介面協調該共用運輸文件交易與該運輸文件控制中樞之對應性。該使用者節點亦可具有儲存於該記憶體裝置上之一區塊鏈資料庫。該記憶體裝置可係區域的、遠端的、基於雲的或可抽換的。該區塊鏈資料庫可具有與單個共用運輸文件交易中之使用者角色有關之運輸文件。

【0010】 亦闡述用於在一共用運輸(電子)文件之分佈中協調一第一使用者節點與第二使用者節點之間的通信的一獨立運輸文件控制中樞。該共用運輸文件可具有經加密資料屬性、經加密資料加密金鑰及/或一文件發起者之數位簽章。該運輸文件控制中樞可使用一電腦，該電腦具有用於執行程式指令之一邏輯、一記憶體裝置及用於與該等使用者節點通信之一通信裝置。可存在一通信路由控制器，該控制器可使用一路由邏輯來將自該第一使用者節點接收之一共用運輸文件路由至該第二使用者節點。該第二使用者節點可係由該第一使用者節點提供之運輸文件之運輸方中之一者。可存在儲存於該記憶體上之一分散式分類帳。該分散式分類帳可係用於儲存經加密共用運輸文件(或選擇一共用運輸文件之資料屬性)之一區塊鏈資料庫。亦可儲存經加密資料加密金鑰及經加密共用運輸文件之一雜湊以及該共用運輸文件的一文件發起者之數位簽章。

【0011】 亦存在產生一共用運輸文件之一方法。該方法可涉及：產生一共用運輸文件且藉由API介面中之密碼存取層將該共用運輸文件加密；將該經加密共用運輸文件、經加密資料加密金鑰及文件發起者之數位簽章提交給一運輸文件控制中樞(中樞)；識別一或多個使用者，且每一使用者可根據一存取控制原則具有至少一個所指派角色；將該經加密共用運

輸文件、該等經加密資料加密金鑰及該文件發起者之數位簽章轉發給該一或多個使用者，其中該一或多個使用者可基於如由該存取控制原則提供之該一或多個使用者所指派角色而履行該經加密運輸文件之一角色。

【0012】 亦可存在用於識別對該共用運輸文件之使用者存取權之一方法。該方法可涉及接收待被至少一個使用者共用之一運輸文件，該文件具有一發起者、一角色清單及一識別碼。然後識別該發起者，基於一全域使用者清單(或全域成員清單)而判定該發起者之角色，驗證該共用運輸文件之該角色清單，藉由資料加密金鑰將該共用運輸文件之至少一個資料屬性加密，根據存取原則藉由相關運輸方之公開金鑰將該等資料加密金鑰加密，且將彼至少一個資料屬性分佈至至少一個經驗證使用者。

【0013】 亦闡述額外態樣。

【0014】 本文中所闡述之貨物追蹤系統及方法可幫助公司及個體透過運輸程序追蹤諸如聯運貨櫃之貨物貨櫃之進度。此可藉由在各個當事方向系統提供運輸文件時給每一當事方指派一角色而達成。該系統可組織該等運輸文件且根據一邏輯方案將該等運輸文件加密。該等運輸文件可經歷其中可與邏輯上彼此相關之其他當事方共用該等經加密運輸文件(例如，當其全部與一共同承運人或代理有關聯時)之一程序。可在將貨物自起始點運送至目的地點期間在各個時間及事件處更新與經運輸之貨物對應之資料。每一更新產生新的經加密運輸文件，可與共用一邏輯、業務或財務關係之所有當事方共用該等新的經加密運輸文件。

【0015】 表示貨運之運輸文件可含有關於貨物運輸之資訊，諸如可運輸哪種產品、其重量為多少及其是否需要任何特殊處置(僅舉幾個例子)。該運輸文件亦可包含關於所涉及之當事方(例如托運人、收貨人、運

輸承運人)之資訊及運輸之路線資訊。另外，該運輸文件可包含儲存運輸中發生之對於其狀態可有意義之事情的一或多個事件記錄。總之，該運輸文件可涵蓋可與任何運輸有關之各種其他細節。該運輸文件之存取原則亦可含有關於誰可擔任一運輸角色之資訊。可在該系統中添加、編輯或讀取一運輸文件。在某些實施例中，該運輸文件可含有關於一使用者之資訊。在某些實施例中，該運輸文件可係一貨物運輸之一虛擬文件。在某些實施例中，該運輸文件可含有關於一用戶之資訊。

【0016】 在某些實施例中，存取該系統之當事方可係該系統之使用者。此等使用者可具有對系統之各種存取級別及特權。在某些實施例中，該等使用者可能夠讀取在該系統中呈現之資料。在某些實施例中，使用者可能夠在該系統中創建資料。在又某些實施例中，使用者可能夠更新該系統中之現有資訊。在某些實施例中，使用者可能夠進行以下操作中之一或多者：在該系統中創建該資料；讀取該系統中之該資料；及更新該系統中之該資料。

【0017】 在某些實施例中，該系統中可存在一或多個成員級別。此等不同成員級別可伴隨著不同存取權或授權。在某些實施例中，該等不同存取權可伴隨著不同費用。

【0018】 在某些實施例中，可存在接收使用者資訊且即時儲存與貨櫃之運輸及追蹤有關之資訊的一系統。該系統可包含一電腦，該電腦具有一處理器、一記憶體裝置及用於存取網際網路之一通信介面。該電腦系統可經由該通信介面自一或多個使用者接收資料。可處理該資料且收集該資料且將該資料分類為該記憶體裝置中之一有組織資料結構。該電腦可具有使得該電腦能夠將來自一或多個使用者之該資料轉變成一經加密記錄之一

邏輯。該電腦可使用各種加密方法來將該資料加密以產生該經加密運輸文件。亦可產生一系列資料加密金鑰，其中為該運輸文件中之每一屬性提供一個資料加密金鑰。可藉由使用者之公開金鑰基於相關運輸方之使用者之角色而將相關個別資料加密金鑰加密。該使用者之該公開金鑰稱為金鑰加密金鑰。可透過可由系統用於每一使用者之區塊鏈節點將此等經加密資料加密金鑰及經加密資料封裝提供給該等使用者。節點可經共用或專用於一運輸方。一使用者可使用一私密金鑰將經加密資料加密金鑰解密，且然後使用該等經解密加密金鑰來將節點中之相關資料解密。

【0019】 在某些實施例中，可存在保護在一分佈式使用者群組中共用之一運輸文件之資料私密性之一方法。該方法包括經由一通信網路自一使用者接收該運輸文件，該使用者可具有一所指派角色，其中該運輸文件包括複數個資料屬性。亦可存在經由一第一加密邏輯將該複數個資料屬性加密成相似數目個經加密資料屬性，該第一加密邏輯產生對應於每一經加密資料屬性之一資料加密金鑰。該方法亦可涉及經由一程式化邏輯將該複數個經加密資料屬性組織至一分散式資料分類帳中，該分散式資料分類帳含有來自一使用者之至少一個經加密運輸文件。該方法進一步涉及經由一第二加密邏輯將對應於該複數個資料屬性之該等加密金鑰加密，該第二加密邏輯可使用基於使用者之所指派角色而為該分散式資料分類帳之一或多個使用者提供權限的一查找表。該方法亦可具有：經由該通信網路以一更高效方式將該等經加密資料屬性、該經加密資料加密金鑰分佈至該等區塊鏈節點，使得整個解決方案可係可擴縮的。每一使用者可存取一節點，該節點可提供對該等分散式資料分類帳中之一者之存取。每一使用者可僅將與其所指派角色有關之資料解密。

【0020】 第一加密及第二加密可利用各種加密技術。使用者所指派角色可與一使用者存取控制原則相關聯。

【0021】 系統及/或方法之使用可提供內容脈絡敏感資料隔離、加密及存取控制原則之一組合以達成一分散式分類帳技術之資料私密性。

【0022】 本發明之至少一個態樣係針對與不同用戶端終端機安全地共用來自多個源之資料之一方法。具有一或多個處理器之至少一個伺服器可建立用於定義一單個交易之一電子文件。該電子文件可具有複數個資料欄位。該複數個資料欄位中之每一者可與複數個用戶端終端機中之一者相關聯。該至少一個伺服器可識別複數個加密金鑰以將包含於該電子文件中之該對應複數個資料欄位加密。該至少一個伺服器可根據一存取控制原則跨越該複數個用戶端終端機分佈該複數個加密金鑰。該存取控制原則可基於該複數個用戶端終端機中之一對應用戶端終端機在該單個交易中之一角色而規定該對應用戶端終端機對該複數個資料欄位中之每一者之存取權限。該至少一個伺服器可經由根據該存取控制原則分佈之該複數個加密金鑰向該複數個用戶端終端機中之每一者提供對該電子文件中之該複數個資料欄位中之至少一者之存取。

【0023】 在某些實施例中，建立該電子文件可包含自該複數個用戶端終端機中之一第一用戶端終端機接收更新該電子文件中之該複數個該等資料欄位中之一第一資料欄位之一屬性的一請求。在某些實施例中，建立該電子文件可包含根據該存取控制原則基於該第一用戶端終端機在該單個交易中之一角色而判定該第一用戶端終端機具有修改該第一資料欄位之權限。在某些實施例中，建立該電子文件可包含回應於判定該第一用戶端終端機具有該權限而准許該用戶端終端機更新該電子文件中之該第一資料欄

位之該屬性。

【0024】在某些實施例中，該至少一個伺服器可回應於自該複數個用戶端終端機中之一第一用戶端終端機接收到更新該電子文件中之該複數個該等資料欄位中之一第一資料欄位之一屬性的一請求而自該單個交易中之一角色清單識別該第一用戶端終端機之一角色。在某些實施例中，該至少一個伺服器可根據該存取控制原則基於該第一用戶端終端機之該所識別角色而判定該第一用戶端終端機缺乏修改該第一資料欄位之權限。在某些實施例中，該至少一個伺服器可回應於判定該第一用戶端終端機缺乏該權限而阻止由該第一用戶端終端機更新該電子文件中之該資料欄位之該屬性。

【0025】在某些實施例中，識別該複數個加密金鑰可包含針對該對應複數個用戶端終端機識別複數個私密加密金鑰及複數個公開加密金鑰。在某些實施例中，分佈該複數個加密金鑰可包含將該複數個私密加密金鑰中之一私密加密金鑰提供至該複數個用戶端終端機中之一對應用戶端終端機。在某些實施例中，分佈該複數個加密金鑰可包含根據該存取控制原則將該複數個公開加密金鑰中之一公開加密金鑰提供至該複數個用戶端終端機中之至少一者。該電子文件中之該複數個資料欄位中之至少一者可由該複數個用戶端終端機中之至少兩者使用該私密加密金鑰及該公開加密金鑰中之至少一者來存取。

【0026】在某些實施例中，該至少一個伺服器可根據該存取控制原則基於一第一用戶端終端機之一第一角色及一第二用戶端終端機之一第二角色而自該複數個用戶端終端機識別該第一用戶端終端機及該第二用戶端終端機。在某些實施例中，該至少一個伺服器可回應於識別該第一用戶端

終端機及該第二用戶端終端機而使用該第二用戶端終端機之一公開加密金鑰將該第一用戶端終端機之一第一加密金鑰加密。在某些實施例中，分佈該複數個加密金鑰可包含將藉助該第二用戶端終端機之該公開加密金鑰加密的該第一用戶端終端機之該第一加密金鑰提供至該第二用戶端終端機。

【0027】 在某些實施例中，該至少一個伺服器可識別自該電子文件之該複數個資料欄位中之對應複數個屬性導出之複數個雜湊值。該複數個雜湊值中之每一雜湊值可確保該複數個屬性中之一者之資料完整性。在某些實施例中，該至少一個伺服器可針對該複數個用戶端終端機中之一第一用戶端終端機使用該複數個雜湊值中之一第一雜湊值及該複數個加密金鑰中之一第一加密金鑰產生一第一簽章。該第一雜湊值可自該複數個屬性中之一第一屬性導出。該第一加密金鑰可係針對該複數個資料欄位中對應於該第一屬性之一第一資料欄位。該第一簽章可確保該第一屬性及該第一資料欄位之資料完整性。

【0028】 在某些實施例中，該至少一個伺服器可根據該存取控制原則基於一第一用戶端終端機之一第一角色及一第二用戶端終端機之一第二角色而自該複數個用戶端終端機識別該第一用戶端終端機及該第二用戶端終端機。在某些實施例中，提供存取可包含經由自該資料欄位之一屬性導出之一雜湊值及該第一用戶端終端機之一簽章向該第二用戶端終端機提供對該第一用戶端終端機之該複數個資料欄位中之一資料欄位之存取。該第二用戶端終端機可使用該雜湊值及該簽章獲得該第一用戶端終端機之該複數個加密金鑰中之一加密金鑰。

【0029】 在某些實施例中，該至少一個伺服器可判定該複數個加密金鑰跨越該複數個用戶端終端機之一分佈是否成功。在某些實施例中，該

至少一個伺服器可基於該複數個加密金鑰之該分佈是否成功之一判定而將一事件通知提供至該複數個用戶端終端機中之至少一者。

【0030】 在某些實施例中，識別該複數個加密金鑰可包含自該複數個用戶端終端機中之每一用戶端終端機聚合該複數個加密金鑰之一對應加密金鑰。該對應加密金鑰可由該用戶端終端機產生以將該複數個資料欄位中之一資料欄位加密。在某些實施例中，建立該電子文件可包含在一運輸文件控制中樞之一資料庫上建立該電子文件以在該複數個用戶端終端機當中協調通信，該電子文件之該複數個資料欄位對應於該資料庫上之對應複數個資料庫項目。

【0031】 在某些實施例中，該單個交易可涉及一實體商品且可包含該實體商品之一系列子交易。該複數個資料欄位中之每一者可映射至該等子交易中之一者。在某些實施例中，該實體商品之該等子交易中之每一者可由至少一個服務提供者處置。

【0032】 本發明之至少一個態樣係針對用於與不同用戶端終端機安全地共用來自多個源之資料之一系統。該系統可包含具有一或多個處理器之至少一個伺服器。該至少一個伺服器可建立用於定義一單個交易之一電子文件。該電子文件可具有複數個資料欄位。該複數個資料欄位中之每一者可與複數個用戶端終端機中之一者相關聯。該至少一個伺服器可識別複數個加密金鑰以將包含於該電子文件中之該對應複數個資料欄位加密。該至少一個伺服器可根據一存取控制原則跨越該複數個用戶端終端機分佈該複數個加密金鑰。該存取控制原則可基於該複數個用戶端終端機中之一對應用戶端終端機在該單個交易中之一角色而規定該對應用戶端終端機對該複數個資料欄位中之每一者之存取權限。該至少一個伺服器可經由根據該

存取控制原則分佈之該複數個加密金鑰向該複數個用戶端終端機中之每一者提供對該電子文件中之該複數個資料欄位中之至少一者之存取。

【0033】 在某些實施例中，該至少一個伺服器可自該複數個用戶端終端機中之一第一用戶端終端機接收更新該電子文件中之該複數個該等資料欄位中之一第一資料欄位之一屬性的一請求。在某些實施例中，該至少一個伺服器可根據該存取控制原則基於該第一用戶端終端機在該單個交易中之一角色而判定該第一用戶端終端機具有修改該第一資料欄位之權限。在某些實施例中，該至少一個伺服器可回應於判定該第一用戶端終端機具有該權限而准許該用戶端終端機更新該電子文件中之該第一資料欄位之該屬性。

【0034】 在某些實施例中，該至少一個伺服器可回應於自該複數個用戶端終端機中之一第一用戶端終端機接收到更新該電子文件中之該複數個該等資料欄位中之一第一資料欄位之一屬性的一請求而自該單個交易中之一角色清單識別該第一用戶端終端機之一角色。在某些實施例中，該至少一個伺服器可根據該存取控制原則基於該第一用戶端終端機之該所識別角色而判定該第一用戶端終端機缺乏修改該第一資料欄位之權限。在某些實施例中，該至少一個伺服器可回應於判定該第一用戶端終端機缺乏該權限而阻止由該第一用戶端終端機更新該電子文件中之該資料欄位之該屬性。

【0035】 在某些實施例中，該至少一個伺服器可針對該對應複數個用戶端終端機識別複數個私密加密金鑰及複數個公開加密金鑰。在某些實施例中，該至少一個伺服器可將該複數個私密加密金鑰中之一私密加密金鑰提供至該複數個用戶端終端機中之一對應用戶端終端機。在某些實施例

中，該至少一個伺服器可根據該存取控制原則將該複數個公開加密金鑰中之一公開加密金鑰提供至該複數個用戶端終端機中之至少一者。該電子文件中之該複數個資料欄位中之至少一者可由該複數個用戶端終端機中之至少兩者使用該私密加密金鑰及該公開加密金鑰中之至少一者來存取。

【0036】 在某些實施例中，該至少一個伺服器可根據該存取控制原則基於一第一用戶端終端機之一第一角色及一第二用戶端終端機之一第二角色而自該複數個用戶端終端機識別該第一用戶端終端機及該第二用戶端終端機。在某些實施例中，該至少一個伺服器可回應於識別該第一用戶端終端機及該第二用戶端終端機而使用該第二用戶端終端機之一公開加密金鑰將該第一用戶端終端機之一第一加密金鑰加密。在某些實施例中，該至少一個伺服器可將藉助該第二用戶端終端機之該公開加密金鑰加密的該第一用戶端終端機之該第一加密金鑰提供至該第二用戶端終端機。

【0037】 在某些實施例中，該至少一個伺服器可識別自該電子文件之該複數個資料欄位中之對應複數個屬性導出之複數個雜湊值。該複數個雜湊值中之每一雜湊值可確保該複數個屬性中之一者之資料完整性。在某些實施例中，該至少一個伺服器可針對該複數個用戶端終端機中之一第一用戶端終端機使用該複數個雜湊值中之一第一雜湊值及該複數個加密金鑰中之一第一加密金鑰產生一第一簽章。該第一雜湊值可自該複數個屬性中之一第一屬性導出。該第一加密金鑰可係針對該複數個資料欄位中對應於該第一屬性之一第一資料欄位。該第一簽章可確保該第一屬性及該第一資料欄位之資料完整性。

【0038】 在某些實施例中，該至少一個伺服器可根據該存取控制原則基於一第一用戶端終端機之一第一角色及一第二用戶端終端機之一第二

角色而自該複數個用戶端終端機識別該第一用戶端終端機及該第二用戶端終端機。在某些實施例中，該至少一個伺服器可經由自該資料欄位之一屬性導出之一雜湊值及該第一用戶端終端機之一簽章向該第二用戶端終端機提供對該第一用戶端終端機之該複數個資料欄位中之一資料欄位之存取。該第二用戶端終端機可使用該雜湊值及該簽章獲得該第一用戶端終端機之該複數個加密金鑰中之一加密金鑰。

【0039】 在某些實施例中，該至少一個伺服器可判定該複數個加密金鑰跨越該複數個用戶端終端機之一分佈是否成功。在某些實施例中，該至少一個伺服器可基於該複數個加密金鑰之該分佈是否成功之一判定而將一事件通知提供至該複數個用戶端終端機中之至少一者。

【0040】 在某些實施例中，該至少一個伺服器可自該複數個用戶端終端機中之每一用戶端終端機聚合該複數個加密金鑰之一對應加密金鑰。該對應加密金鑰可由該用戶端終端機產生以將該複數個資料欄位中之一資料欄位加密。在某些實施例中，該至少一個伺服器可在一運輸文件控制中樞之一資料庫上建立該電子文件以在該複數個用戶端終端機當中協調通信，該電子文件之該複數個資料欄位對應於該資料庫上之對應複數個資料庫項目。

【0041】 在某些實施例中，該單個交易可涉及一實體商品且可包含該實體商品之一系列子交易。該複數個資料欄位中之每一者可映射至該等子交易中之一者。在某些實施例中，該實體商品之該等子交易中之每一者可由至少一個服務提供者(例如，托運人、承運人、船舶經營者、碼頭經營者)處置。一服務提供者亦可稱為一促進者或交易成員/使用者。

【0042】 熟習此項技術者可基於本發明之研究而明白系統及方法之

替代實施例。出於本文中所附加之申請專利範圍之目的，此等替代實施例意欲作為等效內容。

【圖式簡單說明】

【0043】 為容易地識別對任何特定元件或動作之論述，一元件符號中之一或若干最高有效數位係指其中首次引入彼元件之圖編號。

【0044】 圖1圖解說明一通信系統。

【0045】 圖2圖解說明根據一實施例之一實例性運輸路線200。

【0046】 圖3圖解說明根據一實施例之一金鑰保存庫程序300。

【0047】 圖4圖解說明根據一實施例之一不對稱金鑰位置400。

【0048】 圖5圖解說明根據一實施例之一鑑認程序500。

【0049】 圖6圖解說明根據一實施例之一API介面600。

【0050】 圖7圖解說明根據一實施例之一API管理程序700。

【0051】 圖8圖解說明根據一實施例之一運輸文件資料分佈800。

【0052】 圖9圖解說明根據一實施例之一運輸文件創建模型900。

【0053】 圖10圖解說明根據一實施例之一樣本預訂清單1000。

【0054】 圖11圖解說明根據一實施例之一擷取運輸文件1100。

【0055】 圖12圖解說明根據一實施例之一創建運輸文件1200。

【0056】 圖13圖解說明根據一項實施例之一實例性系統1300。

【0057】 圖14圖解說明根據一項實施例之一實例性存取原則1400。

【0058】 圖15根據一項實施例圖解說明產生金鑰且使彼等金鑰和一使用者之所指派角色與存取原則1500匹配。

【0059】 圖16圖解說明根據一項實施例之用於基於角色與存取控制原則1600而將資料屬性加密之一程序。

【0060】 圖17圖解說明根據一項實施例之一組件關係實例1700。

【0061】 圖18圖解說明根據一項實施例之一實例性角色清單與存取控制原則1800。

【0062】 圖19圖解說明根據一項實施例之一實例性運輸文件與存取控制原則1900。

【0063】 圖20圖解說明根據一項實施例之一實例性運輸文件原則2000。

【0064】 圖21圖解說明根據一項實施例之一系統佈局(邏輯) 2100。

【0065】 圖22圖解說明根據一項實施例之一角色清單提交詳細流程2200。

【0066】 圖23圖解說明根據一項實施例之一角色清單讀取詳細流程2300。

【0067】 圖24圖解說明根據一項實施例之一運輸文件創建2400。

【0068】 圖25圖解說明根據一項實施例之一運輸文件更新2500。

【0069】 圖26圖解說明根據一項實施例之一運輸文件讀取2600。

【0070】 圖27圖解說明根據一實施例之一預訂配置2700。

【0071】 圖28圖解說明根據一實施例之一局部預訂視圖2800。

【0072】 圖29圖解說明根據一實施例之關於一第三方非使用者之一可能活動2900。

【0073】 圖30圖解說明根據一實施例之一使用者將資訊自系統提供至一第三方。

【0074】 圖31圖解說明根據一實施例之一可能貸款申請程序。

【0075】 圖32圖解說明根據一實施例之用以支援建立一貸款帳戶之

文件化交換。

【0076】 圖33圖解說明根據一實施例之用以支援申請融資之文件化交換。

【0077】 圖34圖解說明根據一實施例之一實例性發票。

【0078】 圖35圖解說明根據一實施例之一實例性支付選項。

【0079】 圖36係根據一實施例之與不同用戶端終端機安全地共用來自多個源之資料之一方法之一流程圖。

【0080】 圖37係一計算裝置之實施例之一方塊圖。

【實施方式】

相關申請案之交叉參考

【0081】 本申請案主張2019年2月25日提出申請之標題為「Encrypted Distributed Ledger for Use with Freight Shipping Organizations, and methods of use」之美國臨時申請案62/919,097的優先權，該美國臨時申請案之內容係以其全文引用的方式併入。本申請案係2019年4月5日提出申請之標題為「Zero Trust Communication System for Freight Shipping Organizations, and Methods of Use」之US 16/501,399之一部分接續案，該申請案係以其全文引用的方式併入本文中。

【0082】 多個當事方共用資料可產生協同作用及效率。然而，當進行一單個交易(例如，多級交易、多方交易、一子交易系列/序列)所需要或利用之資料對單個交易中所涉及之當事方中之一或多者可為機密的時，資料共用可係一問題。在運輸貨物領域中，此問題可係尤其嚴峻的。其他業務亦可具有此問題。一可能解決方案可係利用加密技術來保護資料私密性同時在一分散式分類帳系統中允許適當當事方共用相關資料的一系統及程

序，如本文中所闡述。所闡述之系統及方法在運輸貨品及貨物中可係有用的。本文中所闡述之系統及方法亦可應用於其他行業中。

【0083】 本文中所闡述之貨物追蹤系統及方法可幫助公司及個體追蹤貨物在運輸程序中之進度。此可藉由使各個使用者將運輸文件提供給系統來達成。系統可含有提供角色之一清單及每一角色之權利的一查找表。當一使用者將一運輸文件提交給系統時，運輸文件可含有使用者之識別碼，及個別運輸方之一角色清單。系統可使來自運輸文件的使用者之所列出角色與一查找表中的角色之權利相關。系統可處理運輸文件，因此使用者及相關運輸方可能夠在將資料加密之後存取資料。系統中之每一使用者可具有一或多個所定義角色。對一運輸文件中之每一資料屬性之存取可由使用者之角色定義。一使用者可根據使用者在存取控制原則中之角色僅存取與其有關之資料。

【0084】 系統可辨識由一使用者提交之一運輸文件且可將該運輸文件之每一資料屬性加密。第一加密程序可針對每一資料屬性創建一個別加密金鑰。

【0085】 作為一實例，一運輸文件可具有五個標頭及五個資料屬性。第一加密程序可將該五個資料屬性加密，而不將該五個標頭欄位加密。分散式分類帳亦可具有與每一經加密資料屬性中之至少一者對應之標頭欄位。分散式分類帳之標頭欄位對應於該運輸文件之標頭欄位中之至少一者。在某些實施例中，分散式分類帳之標頭欄位在一對一基礎上與運輸文件之標頭欄位對應。可不將分散式分類帳標頭欄位加密，但可將與分散式分類帳之每一標頭欄位對應之資料屬性加密。一第二級別之加密可用於將分散式分類帳之資料屬性中之加密金鑰中之每一者加密。可藉由使用在

運輸程序中具有已知角色之一或多個使用者之公開金鑰而進行該第二級別之加密。第二加密程序可藉由使來自運輸文件之使用者角色與查找表相關而識別使用者在運輸中之角色。然後，使用者之公開金鑰可用於基於使用者所指派角色及存取原則而將對應於與使用者有關之資料屬性之加密金鑰加密。可將各種屬性(經加密資料屬性、基於不同角色之經加密加密金鑰、雜湊(由經加密資料屬性產生)及文件發起者之簽章)放置至一基於權限之區塊鏈分散式分類帳區塊鏈節點中。某些使用者可具有其自身之區塊鏈節點。為在使用區塊鏈分散式分類帳時改良可擴縮性及效能，可將資料放置至屬運輸中所涉及之使用者之節點中。

【0086】 系統中之每一使用者可具有一或多個所指派角色。每一運輸文件角色清單可識別提交運輸文件角色清單之使用者之角色，且運輸文件角色清單可識別運輸中可涉及之使用者之角色。在某些實施例中，角色清單可追蹤誰創建了其、使用者之角色及對應使用者之一清單以及一定位子金鑰(創建者之識別碼及運輸文件之預訂號)。

【0087】 可與所有類型之運輸文件一起使用本文中所闡述之各種實施例。一共同運輸文件係一「預訂」–創建一提單之一前體文件。儘管可與本發明系統一起使用諸多運輸文件，但諸多實例可使用術語「預訂」或「預訂資料」。此等術語應被視為分別與任何運輸文件或運輸文件資料相同。

【0088】 在某些實施例中，各個使用者之間可存在允許其看到彼此之資料屬性之一關係。在某些實施例中，可存在建構至查找表中之業務關係，該查找表准許一個使用者看到並非其自身之業務之一部分之資料。可透過每一當事方識別其需要之權利以及其期望之權利來導出存取權之查找

表，其中系統控制器係每一使用者具有之權利之最終仲裁者。

【0089】 在某些實施例中，分散式分類帳可表示一單個運輸文件。在某些實施例中，可存在併入至一單個分散式分類帳中之多個運輸文件。

【0090】 在某些實施例中，不對稱密碼學可用作本文中所闡述之加密方法之一部分或全部。

【0091】 特定方法中之總體程序之概略圖。

【0092】 在圖1中展示用於追蹤一運輸在貨運通道中之狀態之程序。陰影橢圓展示一單個運輸交易中之各個當事方，及其如何使用EDI(電子資料互換)彼此進行通信。當事方之實例經展示為一托運人、代運人、承運人、碼頭、海關、港務局及收貨人。

【0093】 當事方之簡要說明

【0094】 托運人－將貨品運輸至收貨人之公司或人。

【0095】 收貨人－一貨運合同中經指定已將商品運輸至或移交看護之人或公司。

【0096】 代運人(或貨物代運人)－從事於組裝、收集、鞏固、運輸及分佈零擔貨運(less-than-carload或less-than-truckload)貨物之業務的一人或企業。以及在通過海關轉運貨物中充當代理(包含充分準備文件、安排運輸、入倉、交貨及出口結關)之一人。

【0097】 承運人－經營運送旅客或商品以獲得租金之一個體或法律實體。

【0098】 船舶經營者－負責船舶之操作成本、維修及盈餘之任何企業單位。經營者可為或可並非船舶之擁有者。成本包含船員工資、港口費及船體險。海運承運人透過聯盟或船舶共用協議來共用船舶之使用，且一

承運人之一船舶擁有者(船舶經營者)可載運透過其他承運人預訂之運輸。

【0099】 碼頭經營者 – 海上碼頭經營者(MTO)為在海運對外貿易中移動貨品之海洋共同承運人提供碼頭停泊位、船塢、倉庫或其他海上碼頭設施。

【0100】 除一貨物運輸之此等當事方之外，亦可存在對一貨物運輸感興趣之其他當事方，諸如政府機關(海關、檢驗局)、金融機構、保險公司等等。

【0101】 一托運人102可產生一產品運輸且透過直接通信將資訊提供給其他當事方。此等係自托運人102至代運人104、承運人106、碼頭108、海關110、港務局112、收貨人114及(若需要)一金融機構116 (諸如一銀行、放款人、保險公司、債券持有人等)中之每一者之單向通信。如圖1中可見，與其他當事方之每一通信係與每一當事方之一單向通信，每一當事方基本上向其他當事方發送與一運輸有關之某些資訊，且然後接收當事方向原始當事方發送一回應。程序中之每一當事方可已針對此形式之通信開發了其自身之專屬技術。通信協定未經整合以共同起作用，因此每一接收當事方將接收一訊息，且然後以其自身之協定做出回應且等待其他當事方做出回應。此程序為低效的且耗時的。

【0102】 可給一運輸合同中之各個當事方指派運輸中之一或多個角色。在圖2中展示各種角色。每一所指派角色之位置在圖中由一不同陰影標記。圖2僅僅係說明性的。諸多其他角色位置係可能的且存在於實際交易中。可在圖2中所展示之圖解說明200中看到在世界範圍內創建一預訂與運輸貨運之系統。在某些實施例中，一托運人202可藉由判定商品將經收取且發送至一特定目的地而開始一運輸預訂。托運人202可創建一預訂

請求(形成一商業合同以發送貨物之一預備步驟)，且指定具有如所展示之碼頭A、B及C之一港務局204。托運人亦可選擇一船或船舶以由一船舶經營者206載運貨品。托運人202亦可指定一最終收貨人208進行運輸。亦在圖2中藉由實例方式圖解說明一運輸可採取之路線。若遵循自起點(收貨地點)至終點(最終目的地)之路徑，則可見，涉及眾多當事方。在此路線內運送商品可涉及諸多當事方，其全部具有其自身之通信模式，如先前所闡述。

【0103】 以上實例未展示一運輸中可涉及之所有當事方。每當貨物進入一港口時，一港務局204可具有在其管轄權下工作之數個代理。可存在各種檢驗員(例如，針對糧食、牲畜、水果及蔬菜)、對未經授權之危險品之檢查、用以證明任何受製裁材料之ITC檢驗、移民檢驗員等等。碼頭經營者可屬一私營公司且在數個其他港口具有在其權威下之碼頭設施。在某些情形中，一當事方可屬一更大公司，其中該公司必須沿著一上級組織之子公司鏈向上或向下進行通信。

【0104】 在本文中闡述創建一新類型之預訂合同(一類型之運輸文件)之一系統及方法之各種實施例，該新類型之預訂合同允許協議之相關當事方藉由以一單點聯繫進行檢查而追蹤貨運之進度。該單點聯繫提供對於所有相關當事方可係可用之最新資訊且避開使每一當事方一次一個地或以一順序方式與每一其他當事方通信之限定性通信。可隨著貨品移動穿過各個運送階段而連續地更新各個使用者。此等更新可包含貨品之狀態、債務、監管事項及其他問題。

【0105】 如本文中所使用，術語「使用者」可係指一個體或組織。一使用者可係可存取系統且與本文中所闡述之程序互動之任何人、當事

方、組織或程式。可存取如本文中所闡述之系統之任何個體或實體可被視為一使用者。本發明亦利用詳述各個使用者之特定權利、特權及責任之清單。一般而言，一使用者可表示一交易中之一角色，儘管不必要使每一使用者成為交易之一當事方。術語「使用者」及「當事方」可在本文中互換地使用，除非內容脈絡另有清晰指示。

【0106】 在某些實施例中，一使用者可登上系統且然後可獲得金鑰保存庫存取及各種所指派金鑰。該使用者可起始一金鑰保存庫程序300(圖3)，至系統之一初始登入或開始302。該使用者登上系統且系統可登入至一金鑰儲存區，且使金鑰儲存區為使用者產生一金鑰保存庫304。系統之一全域使用者清單(或全域成員清單)可記錄使用者之基本資訊。該基本資訊可包含使用者之姓名、使用者在任一預訂中之角色、聯繫資訊及與使用者具有之角色相關之其他資訊。系統可將使用者金鑰保存庫之映射儲存於一金鑰保存庫映射資料庫中306。然後，使用者可登入至系統以產生公開金鑰及私密金鑰。可將私密金鑰儲存於使用者之私密金鑰保存庫中308。系統可自金鑰保存庫獲得公開金鑰，且將公開金鑰儲存於一公開金鑰儲存庫中310。一旦兩個金鑰在其各別資料庫中得到保護，程序便可結束312。在某些實施例中，使用者可具有對一金鑰保存庫之預配置存取且連同如本文中所闡述之系統使用一預先存在金鑰保存庫。

【0107】 在某些實施例中，一當事方可一次追蹤一或多個金鑰。可使用金鑰位置400 (圖4)，因此一當事方可有權使用其自身之私密金鑰404，而系統可使用當事方之公開金鑰402。每一使用者可具有一金鑰保存庫，該金鑰保存庫具有一私密金鑰404及一公開金鑰402。該公開金鑰可儲存於系統服務提供者網路中。系統可藉由使用使用者組織之公開金鑰

而將一資料加密金鑰加密。此加密可發生在系統服務提供者網路中。當系統將經加密資料加密金鑰(DEK)解密時，系統經由一安全網路連接410將經加密DEK發送至金鑰儲存區網路。金鑰儲存區然後可使用使用者之私密金鑰404來將經加密DEK 406解密以在金鑰儲存區網路中產生一經解密DEK。金鑰儲存區然後可再次經由一安全網路連接412將經解密DEK 408往回發送至系統。使用者可使用DEK 408來將與彼特定金鑰有關之經加密資料解密。

【0108】 在某些實施例中，每一資料屬性加密金鑰可使用一單獨公開金鑰或一單獨加密協定來加密，但使用相同公開金鑰來將資料加密金鑰加密。在一特定使用者可具有准許彼使用者看到每一預訂記錄中之多個資料屬性之一角色之情況下，可針對使用者存取之每一欄位重複以上程序。此加密及解密程序之使用發生在各個系統之間的通信中，且對存取資料庫資訊之人可係不可見的。

【0109】 在某些實施例中，一使用者可透過一鑑認程序500 (圖5)獲得對系統之存取。該使用者可藉由提供其登入名及密碼而存取一用戶端應用程式502。用戶端應用程式502可向經授權使用者提供組織認證且可透過一安全網路連接504將登入請求發送至一授權權杖產生器506。用戶端應用程式502可提供鑑認資訊(例如，使用者姓名及密碼以及任何其他鑑認資訊)。舉例而言，鑑認資訊可係一API訂用ID及秘密(例如，密碼)。該授權權杖產生器可自用戶端應用程式接收API訂用ID及秘密且對照API訂用資料庫驗證資訊。一旦可鑑認此等項目，權杖產生器506便可產生可傳回至使用者之一權杖。使用者之用戶端應用程式502然後可使用權杖以透過安全網路連接504與預訂API 508通信。使用者可獲得對預訂API 508之存

取以輸入及/或存取資料。

【0110】 在某些實施例中，用戶端應用程式502可係授權權杖產生器506或預訂API 508之一基於網路之入口網站及部分。在某些實施例中，用戶端應用程式502可係用戶端自身之軟體，且授權權杖產生器506及預訂API 508可經調試以與用戶端軟體通信。在一些實施例中，授權權杖產生器506及預訂API 508可係相同應用程式(未展示)。在某些實施例中，授權權杖可對用戶端應用程式可存取預訂API 508多長時間具有一預定時間限制，或者用戶端應用程式502可必須在每一工作階段使其自身由授權權杖產生器506鑑認。在某些實施例中，一預定時間量可設定為一「超時」安全協定，以在一設定不活動時間之後自動注銷一使用者。

【0111】 在某些實施例中，可存在API管理程序之三個域，如圖6中所展示。在某些實施例中，展示API介面600之交握。API介面600可使用用戶端應用程式602、API管理工具604及一區塊鏈API 606。一用戶端應用程式602可係由用戶端(使用者)創建之一應用程式或經具體地創建以與API管理工具604一起工作之一應用程式。使用者可登入至用戶端應用程式602且可提交一請求(例如，創建一預訂請求)，用戶端應用程式602可將一驗證請求608 (在某些實施例中，其可包含API訂用ID及一秘密)發送至API管理工具604。驗證請求608可產生一用戶鑑認616結果，或一錯誤(未展示)。若用戶鑑認616係結果，則API管理工具604然後可產生一存取權杖且將權杖610傳回至用戶端應用程式602。用戶端應用程式602然後可將存取權杖及預訂請求有效負載612發送至API管理工具604。當API管理工具604接收權杖及有效負載612請求時，API管理工具604可提供權杖鑑認618。然後，可鑑認權杖，可基於權杖及組織之映射而將權杖解析為組織

ID。然後可將組織ID及有效負載請求發送614至區塊鏈API 606以對區塊鏈節點進行寫入。

【0112】 圖6中所展示之實例性實施例具有三個域。用戶端應用程式602可存在於用戶端應用程式網路中。API管理工具604可駐存於API管理工具網路中，且區塊鏈API 606可駐存於系統服務提供者網路中。然而，在某些實施例中，API管理工具網路及系統服務提供者網路可合併至一單個系統網路中。在又其他實施例中，可使用3個以上域。

【0113】 在某些實施例中，可存在一API管理程序700，如圖7中所展示。API管理程序700可向一使用者提供對本發明之系統之存取，且在登入時向系統鑑認使用者。一使用者可在開始方塊702處開始，其中使用者可透過鑑認一使用者之一API管理程序700存取系統，如本文中所闡述。訂用ID可由系統指派給使用者，或使用者可選擇一訂用ID (例如，自一下拉式選單，或一組系統選項)且系統記錄其。該訂用ID可基於一訂用費(基於一貨幣支付、一以物換物交換)，或其可係免費的。可將訂用ID發出給監管機構、支付客戶、系統管理者或需要對本文中所闡述之系統之存取之任何其他當事方。每一使用者亦可具有可隨登入請求或隨與系統之每一通信發出給系統之一秘密。一旦使用者與系統建立秘密，秘密便可儲存於API管理程序700或API管理程序700可視需要存取以檢查使用者秘密之一資料庫中。可採取額外步驟，或替代步驟可代替訂用ID及秘密挑戰，使得可使用任何形式之用於一使用者之鑑認之可接受安全性。

【0114】 系統可對照其自身之準則檢查鑑認認證以驗證鑑認可係正確的706。若鑑認失敗，則可報告一錯誤714且程序結束716。當鑑認成功時，可將一權杖發出708至用戶端應用程式。用戶端應用程式然後可將權

杖與一有效負載請求710一起提交給API管理工具。API管理工具可檢查權杖以查看其是否有效712。若權杖並非有效的，則可傳回一錯誤回應714。若權杖係有效的，則可基於權杖及組織之映射而將權杖解析為組織ID 718。然後可將組織ID及有效負載請求轉發至區塊鏈API且程序結束716。

【0115】有效負載請求可係用於預訂請求API (或其他運輸文件API)之預訂請求資料。當由系統確認權杖及組織ID時，可隨著做出預訂預留請求而將資料儲存至相同資料庫。資料可經加密且儲存於一區塊鏈資料庫中。如本文中所闡述，用於預訂請求之資料可含有標頭欄位。每一資料屬性可具有一對應標頭欄位。可在具有或不具有一對應標頭欄位之情況下，將資料屬性儲存至資料庫中。在其中可於不具有一標頭欄位之情況下儲存資料的情形中，每一資料屬性可含有其所來自之標頭欄位之一指標，因此當讀取資料時，可在恰當欄位中恰當地展示資料。類似地，當使用經加密資料來建構各個當事方之間的關係時(諸如當做出一提單(B/L)時)，標頭資料可係有用的。

【0116】在某些實施例中，於圖8中展示用於分佈經加密資料及經加密資料加密金鑰之程序之一概觀。該程序可於開始方塊802處開始，系統可將資料及資料加密金鑰加密804，如本文中所闡述。系統然後可藉由使用其組織ID來找到、存取或定位發送者及各種運輸方之分類帳806。系統可檢查以查看是否可找到所有運輸方之分類帳。若未找到一分類帳，則系統可傳回一錯誤810回應且該程序結束。若找到所有運輸方之分類帳，則系統可繼續將資料及資料加密金鑰發送至分類帳。

【0117】系統然後可繼續發送經加密資料及經加密資料金鑰，且可

檢查至各種適當分類帳之發送成功808 (接收驗證)。若發送係成功的，則程序可繼續進行至結束方塊812。

【0118】 在某些實施例中，一使用者可經由一獲得預訂程序900獲得預訂資訊，如圖9中所展示。該程序可以系統執行預訂之最新版本904之一尋找來開始902。系統可藉由運輸文件資料庫中之一唯一預訂ID找到一預訂之最新版本904。記錄可含有分類帳名稱。系統可藉由唯一預訂ID 904來搜索(預訂之)最新版本。在某些實施例中，系統可能未找到正確資料記錄。當發生此情況時，系統可產生且傳回一錯誤918。若找到資料記錄，則系統可檢查組織之存取原則且檢查存取原則定義906以查看組織權限可係什麼資料。若組織不具有指派給其角色之一存取原則，則系統可傳回一錯誤918，且程序結束920。若恰當地識別存取原則及定義，則系統可自預訂908之分類帳收集經加密預訂資料及經加密資料加密金鑰。預訂之分類帳可藉由其分類帳名稱來定位。系統可進行一檢查相關910步驟，其中可檢查經加密預訂資料及經加密資料加密金鑰以查看其在分散式分類帳中是否相同。若否，則可傳回一錯誤918回應且程序結束。若資料確實在不同分散式分類帳中相關，則程序可登入至金鑰儲存區912，且金鑰儲存區使用發送者組織之私密金鑰來將資料加密金鑰解密。若金鑰儲存區無法將資料解密，則可產生一錯誤918回應，且該程序結束。系統然後可將資料及金鑰914解密且為使用者公佈經解密資訊916。該程序然後可進行至結束方塊920。

【0119】 在圖10中展示一預訂樣本清單1000。在此處，可基於各種不同搜索準則而將由一托運人使用預訂API創建之每一預訂列出且分類。預訂樣本清單1000可表示預訂記錄資料庫，該等預訂記錄可經加密且儲

存於一資料庫中，如本文中所闡述。

【0120】 此處可在表I中看到資料庫之一實例。

資料庫名稱	對資料庫中之資料之一闡述
ID儲存庫	一使用者清單、使用者登入認證及使用者參數
存取原則儲存庫	全域成員清單、存取原則文件清單、角色清單清單及動態存取原則清單
公開金鑰儲存庫	使用者之公開金鑰之一清單
金鑰儲存區	使用者之私密金鑰之一清單
運輸文件資料庫	一運輸文件清單，例如預訂請求
全域使用者清單	所有使用者及每一成員之角色之一清單可呈現在各種運輸文件中
角色清單原則	定義具有存取權之使用者及角色之清單。

【0121】 圖11圖解說明已經放置於系統中之一擷取預訂程序1100。該程序在開始方塊1102處開始且可繼續進行以對針對預訂之所提交請求是否含有一唯一預訂ID及發送者之組織ID進行一屬性驗證1104。在某些實施例中，系統可使用預訂號、版本及預訂提供者之組織ID。系統可評估請求是否可具有所需要之屬性(屬性驗證1104)。若請求不具有所需要屬性，則可產生一錯誤回應1116且程序結束1118。若請求具有所需要屬性，則程序可自運輸文件資料庫獲得預訂資訊且將經加密預訂資訊解密1106。在某些實施例中，資料庫可以一區塊鏈格式經加密且儲存於一分散式分類帳或一超級分類帳中。系統可檢查以確保恰當地擷取所要預訂且將所要預訂解密1108。若否，則系統可產生一錯誤回應1116。若擷取且解密預訂，則系統可現在進行一運輸角色檢查1110，且可針對每一運輸方判定其組織之組織ID是否可與發送者之組織ID相同。若是，則系統可收集運輸方之運輸角色。

【0122】 系統可執行一運輸角色檢查1110以驗證收集至少一個運輸

角色，然後對於該等所收集運輸角色，系統可獲得可被允許由彼等角色讀取之屬性。在某些實施例中，系統進行檢查以查看每一運輸方角色，且基於運輸角色檢查1110而識別當事方可被允許查看之屬性。在某些實施例中，在一過濾屬性1112檢查中移除當事方可不被允許查看之屬性。在成功1114時，可傳回一成功回應碼。

【0123】 可仍未解決之任何錯誤可使程序在結束1116步驟處終止。

【0124】 現在在圖12中展示一預訂預留之創建。一旦自一使用者或組織接收到預訂有效負載請求，進行預訂之程序便開始(開始方塊1202)。系統可首先檢查以查看所提交請求是否含有一參考預訂號及使用者之組織ID 1204 (檢查屬性驗證)。若使用者之組織ID及/或預訂號不在所提交請求中，則系統可報告一錯誤1234且程序可結束1236。若存在組織ID及預訂號，則系統可藉由定位子金鑰找到預訂之一角色清單1206。定位子金鑰可由參考預訂號及使用者之組織ID構建。若未找到角色清單，則系統可報告一錯誤1234且程序可結束1236。若存在角色清單，則系統可檢查是否可定義預訂之存取原則1208。若未定義存取原則，則系統可傳回一錯誤1234且程序可結束1236。若定義存取原則，則系統可針對每一運輸方檢查運輸方之組織ID是否可與發送者之組織ID相同。若一或多個組織ID可係相同的，則系統可收集運輸方之運輸角色1210。

【0125】 系統然後可進行檢查以查看是否可收集至少一個運輸角色。若未收集角色，則可傳回一錯誤1234且程序可結束1236。若可識別至少一個角色，則系統可檢查所收集運輸角色是否具有存取權以創建預訂資料之所有所提交屬性1212。若角色不具有存取權，則可傳回一錯誤1234且程序可結束1236。若存取權係正確的，則系統可產生預訂之一唯

一預訂ID 1214。一旦創建預訂ID，系統便可針對每一資料屬性產生個別資料加密金鑰1216。該等金鑰可係對稱金鑰。在產生加密金鑰之後，系統可以其資料加密金鑰將每一資料屬性加密1218。在某些實施例中，針對經加密之每一資料屬性可存在一個資料加密金鑰(一1:1關係)。系統然後可擷取每一運輸方之運輸角色資訊，且亦可擷取每一運輸角色之存取控制原則1220。若一運輸方具有一存取控制原則，則系統可自公開金鑰儲存庫擷取公開金鑰1222。系統可針對指派給角色之與當事方相關聯之特定組織ID擷取恰當金鑰。對於每一運輸方，針對可被讀取之資料屬性，系統以運輸方之公開金鑰將對應資料加密金鑰一個接一個地加密1224。系統然後可將經加密資料及經加密資料加密金鑰分佈至恰當組織1226。系統可驗證成功地將資料及金鑰分佈至相關運輸方之所有分類帳1228。在某些實施例中，分類帳可傳回指示是否成功地分佈經加密資料及經加密資料金鑰之一回應。若系統無法驗證恰當分佈，則系統可產生一錯誤碼1234且程序可停止1236。若系統確實驗證經加密資料及經加密資料加密金鑰之分佈，則系統可將分類帳之名稱、唯一預訂ID及預訂版本號保存於運輸文件資料庫中1230。系統然後可產生一成功回應碼1232且程序可結束1236。

【0126】 在某些實施例中，可在圖13中看到系統1300之一運輸文件控制中樞1302。在某些實施例中，運輸文件控制中樞1302可具有一系列使用者節點(出於圖解說明目的且作為一實例而呈現，使用者節點1 1306、使用者節點2 1324及使用者節點N 1342)。每一使用者節點可連接至一對應區塊鏈邏輯(1至N)且擁有一區塊鏈節點(1至N)。區塊鏈邏輯1 1320及區塊鏈節點1 1322可係運輸文件控制中樞1302之一部分。運輸文

件控制中樞1302亦可具有一脫鏈資料庫1304。

【0127】 每一使用者節點可指派給一或多個使用者。舉例而言，一第一使用者節點1306a可指派給一承運人組織，且一第二使用者節點1306b可指派給另一承運人組織。每一使用者(諸如一船舶經營者、一碼頭經營者、一收貨人、一托運人等等)可將一使用者節點1306a至1306n指派給其。儘管在本發明圖中呈現三個節點，但應理解，此圖僅僅係說明性的，且不意欲以任何方式受限制。系統可具有之節點數目係不受限制的，如由「n」記號指定。每一節點中之每一區塊鏈邏輯亦可與一脫鏈資料庫1304通信。在某些實施例中，使用者節點1306a至1306n可存取區塊鏈邏輯1320a至1320n以將經加密資料及一經加密資料加密金鑰(DEK)寫入至一或多個區塊鏈節點1322a至1322n。密碼存取層1314a至1314n可透過一網路通信1318a至1318n與區塊鏈邏輯1320a至1320n通信。可將在密碼存取層1314a至1314n與區塊鏈邏輯1320a至1320n之間發送之任何資料加密。密碼存取層1314a至1314n可基於一存取原則而進行各種解密及加密功能。密碼存取層1314a至1314n可產生對稱資料加密金鑰(DEK)，藉由DEK將資料加密，藉由運輸方之公開金鑰將DEK加密且存取一金鑰儲存區1312a至1312n以將DEK解密。API介面1316a至1316n、密碼存取層1314a至1314n及金鑰儲存區1312a至1312n可存在於在不具有權限之情況下可係不可存取之一隔離網路或使用者節點1306a至1306n中。用戶端應用程式1308a至1308n可連接至一API介面1316a至1316n以對一區塊鏈節點1322a至1322n進行寫入，或自區塊鏈節點1322a至1322n獲得資料。用戶端應用程式1308a至1308n可係一電腦、一伺服器或具有一處理器之任何計算裝置，其存取一記憶體裝置且存取一網路連接以與區塊鏈API

1316a至1316n通信。在某些實施例中，網路連接可係安全的。區塊鏈API 1316a至1316n可將一請求自用戶端應用程式1308a至1308n傳遞至密碼存取層1314a至1314n。用戶端應用程式1308a至1308n亦可具有一用戶端應用程式資料庫1310a至1310n。用戶端應用程式資料庫1310a至1310n中之資料可呈純文字形式。用戶端應用程式1308a至1308n可直接在用戶端應用程式資料庫1310a至1310n中進行搜索。使用者可透過其自身之網路連接1318a至1318n存取用戶端應用程式1308a至1308n及然後使用者節點1306a至1306n及然後區塊鏈邏輯1320a至1320n。

【0128】 針對使用者節點1306所提供之闡述可以與針對使用者節點1324所提供之闡述類似或完全相同之一方式來操作。在某些實施例中，所闡述之區塊鏈節點組件可係分散式分類帳。在某些實施例中，區塊鏈節點組件可係超級分類帳。

【0129】 在某些實施例中，一存取控制原則可用於判定運輸文件分佈，如圖14中所展示。在某些實施例中，各個當事方可將一運輸文件自一使用者節點提供至一運輸文件控制中樞。舉例而言，兩者皆具有用戶端節點之一實例性承運人及一實例性托運人可將一運輸文件傳達至一運輸文件控制中樞。每一使用者節點可具有或可存取一API介面、一密碼存取層及一金鑰儲存區。在所展示之實例中，承運人可將運輸文件角色清單發送至運輸文件控制中樞，而托運人可將運輸文件發送至運輸文件控制中樞。可將運輸文件角色清單及運輸文件加密。

【0130】 運輸文件中樞可具有一存取控制原則(存取原則)，該存取控制原則具有一靜態部分及/或一動態部分，如圖14中所展示。該靜態部分可包含一全域成員清單及一存取原則文件清單。該全域成員清單可用於

判定一成員之一所指派角色。在某些實施例中，一成員可具有多個所指派角色。該存取原則亦可具有一存取原則文件清單。此等一般係指可在一貨物運輸中之角色之間使用之文件類型。某些實例包含但不限於；一提單、一碼頭裝載或卸載艙單、一預訂合同、一預先預訂合同等等。該存取原則可具有對應於每一運輸文件類型之一存取原則文件。存取原則文件與運輸文件類型之間的關係可係1:1，或其可係2+:1或其可係1:2+。此等各種關係及查找特徵一般可係靜態的。在某些實施例中，可更新及/或修正存取原則文件與運輸文件類型之間的關係。

【0131】 在某些實施例中，清單、資料結構、資料庫及原則中之每一者可具有一動態版本及一靜態版本。該靜態版本可係最後所保存版本，而每一所保存版本之封存可存在於區塊鏈中。一動態版本可作為使用者或系統更新而存在或者對待儲存於記憶體中或儲存於區塊鏈中之項目中之任一者做出改變。在某些實施例中，動態版本可僅存在於暫時記憶體中。在某些實施例中，可將動態版本寫入至持久記憶體或區塊鏈。

【0132】 在某些實施例中，可存在存取原則之一動態部分。存取原則可具有動態角色清單之一清單。在某些實施例中，動態角色清單可具有可定位存取原則中之一對應角色清單的一定位子金鑰。在某些實施例中，一定位子金鑰可定位一角色清單或一運輸文件。該運輸文件可係或可並非存取原則之一部分。可使用動態運輸方自一或多個運輸文件構建角色清單。動態存取原則清單可給每一運輸文件提供與一特定存取原則之一相關。在某些實施例中，可產生動態操作中之角色清單且與運輸文件一起提交該等角色清單，可將角色清單指派給靜態存取原則文件之一動態版本(從而創建一動態及靜態存取原則文件)，且可將動態存取原則指派給彼運

輸文件。在某些實施例中，可存在動態存取原則，只要存在運輸文件即可，且動態存取原則控制運輸文件及與彼特定運輸編號相關之所有文件之分佈。

【0133】在某些實施例中，一承運人將一預訂請求發送至運輸文件控制中樞。托運人實例可類似於承運人實例，但用於托運人之運輸文件之分佈之角色清單可係運輸文件控制中樞中之一現有角色清單。當承運人提交運輸文件及角色清單時，承運人可預先創建運輸文件控制中樞中之該現有角色清單。可基於角色清單而將請求發送至各個成員。文件控制中樞可將預訂請求(或其他文件)通知給每一使用者。舉例而言，可通知船舶經營者其船舶將運送指定貨櫃，可通知一碼頭經營者其將接收運送貨櫃之船舶，且可通知一收貨人在一所估計交貨日期時接取貨櫃。在某些實施例中，系統可記錄已通知各個使用者在預訂請求中之其各別責任且記錄彼通知。在某些實施例中，各個使用者可提供對預訂請求接收之一應答(手動地或自動地)。回應文件回到運輸文件控制中樞且經路由給承運人。角色清單可係動態存取原則之一部分，且動態存取原則可用於控制用於此交易之文件之分佈及共用直至完成交易為止。在某些實施例中，系統可僅僅驗證資料遞送且不需要來自接收當事方之應答。

【0134】在某些實施例中，存取原則可具有一全域成員(使用者)清單。該全域成員(使用者)清單可係系統之所有使用者及每一使用者可在各種運輸交易及文件中採用之角色之一清單。該等角色可對應於在共用運輸文件中使用之彼等角色(例如，托運人、承運人、船舶經營者、碼頭經營者等等)。存取原則亦可具有一存取原則文件清單，每一存取原則文件適用於一運輸文件類型(例如危險品(DG)憑證、提單、貨櫃入境事件、貨櫃

出境事件等等)。存取原則亦可具有角色清單之一清單，每一角色清單與具有相同定位子金鑰(例如，承運人 + 預訂(BKG)號)之任一運輸文件有關。存取原則亦可具有一動態存取原則清單，每一動態存取原則與具有相同定位子金鑰及運輸文件類型之任一運輸文件有關。動態存取原則可定義哪一特定當事方可創建、更新、讀取及/或接收共用運輸文件及可以屬性位準進行創建、更新及/或讀取。此動態存取原則可自一給定定位子金鑰之一角色清單及/或一給定共用運輸文件類型之一存取原則文件導出。

【0135】 當一使用者登入至使用者節點以存取運輸文件控制中樞時，使用者可由其登入認證識別。使用者之用戶端應用程式可將一運輸文件角色清單發送至運輸文件控制中樞。運輸文件使用者節點可依據運輸文件角色清單識別角色清單類型。運輸文件用戶端可自運輸文件控制中樞獲得來自存取原則之以下資訊中之任何一或多者：

-來自全域使用者清單(或全域成員清單)之使用者之角色。

-角色清單類型之存取原則文件

-用於每一共用運輸文件類型之一共用存取原則文件，及

-一動態存取原則清單，其中動態存取原則為一運輸文件所特有，動態存取原則定義每一角色對一運輸文件之存取權。

-連結至存取原則、使用者ID或使用者角色之任何其他資訊。

【0136】 運輸文件使用者節點可驗證是否可允許使用者之角色對照存取原則文件創建(更新)運輸文件角色清單。運輸文件使用者節點可依據運輸文件角色清單識別具有新指派之值之角色且進一步驗證使用者之角色是否可指派彼等角色。

【0137】 可將經驗證運輸文件角色清單加密且提交給運輸文件控制

中樞，且可將其添加至一特定定位子金鑰之存取原則。

【0138】 在某些實施例中，用戶端應用程式可將一運輸文件發送至運輸文件使用者節點。使用者節點可依據運輸文件識別文件類型及定位子金鑰。運輸文件使用者節點可自運輸文件控制中樞獲得來自存取原則之以下資訊：-

-運輸文件之動態存取原則(在文件中樞處，在運輸文件使用者節點請求之後自給定定位子金鑰之角色清單及給定運輸文件類型之存取原則文件導出動態存取控制原則)

-運輸文件類型之存取原則文件

-使用者可存取或對其有權限之任何其他資訊。

【0139】 運輸文件使用者節點亦可依據動態存取原則識別使用者扮演之角色。使用者節點可驗證彼等角色可對照存取原則文件創建(更新)運輸文件。使用者節點可依據運輸文件識別具有新指派之值之資料屬性且進一步驗證彼等角色是否可創建(更新)彼等資料屬性。

【0140】 在某些實施例中，可將經驗證運輸文件加密且提交給運輸文件控制中樞。

【0141】 舉例而言，一承運人可將一經加密角色清單及一經加密共用運輸文件提交給運輸文件控制中樞。承運人(或其他使用者)可首先發送角色清單，以將角色清單繫結至運輸文件之一預訂號或其他文件ID來識別。另一選擇係，運輸文件可隨著角色清單(或在角色清單之後)經發送，且運輸文件可藉助定位子金鑰與角色清單相關。可讀取角色清單，且角色清單可包含承運人將通知之角色之一清單。角色清單亦可具有發起者(發送者)之一數位簽章，從而允許角色清單與發起者相關。運輸文件可含有

表示所擬議合同之條款之資料(數量、交貨、排程等等)。此等條款可個別地經加密為資料屬性。角色清單可使特定運輸方之名稱與其相關聯。

【0142】 可自運輸文件複製角色清單且將角色清單添加至唯一於運輸文件之一存取原則。存取原則可含有關於運輸文件中可涉及之每一運輸方之資訊。存取原則之角色清單可提供可接收最初在運輸文件中提供之資料之成員之識別碼。角色清單上之每一運輸方可自運輸文件獲得對於其特定角色(功能)適當之資料。

【0143】 可藉由分開對稱金鑰將運輸文件之資料屬性一個接一個地加密。可藉助與可在運輸文件中具有一角色之每一運輸方對應之公開金鑰將對稱金鑰一個接一個地加密。每一運輸方之角色可由角色清單定義。然後可將資料屬性之對稱金鑰分割至需要或請求資料屬性之每一使用者(運輸方)，且可使用當事方之公開金鑰將去往恰當運輸方之每一資料屬性之對稱金鑰加密。然後可將經加密資料屬性、經加密資料加密金鑰、經加密資料屬性之雜湊及文件發起者之數位簽章發送至運輸方。

【0144】 在某些實施例中，運輸文件用戶端可將經加密共用運輸文件、經加密資料加密金鑰(DEK)、經加密資料屬性之雜湊及文件發起者之數位簽章角色清單發送至運輸文件控制中樞。運輸文件控制中樞可使用運輸文件之定位子金鑰來找到存取原則中之角色清單。基於角色清單，運輸文件控制中樞可查找接收方清單。在某些實施例中，運輸文件控制中樞可具有存取權以解密角色清單從而獲得接收方清單。在某些實施例中，使用者節點可提供角色清單中之運輸方之公開金鑰且運輸文件控制中樞可基於公開金鑰而查找接收方清單。在某些實施例中，使用者節點可將接收方清單之純文字與運輸文件一起提供至運輸文件控制中樞。接收方清單可係角

色清單中之當事方(使用者)。運輸文件控制中樞然後可分佈經加密運輸文件資料屬性、經加密資料加密金鑰、經加密資料屬性之雜湊及文件發起者之數位簽章以根據接收方清單對對應區塊鏈節點進行寫入。運輸文件控制中樞可檢查文件、金鑰、雜湊及簽章是否成功地寫入至區塊鏈節點。若文件、金鑰、雜湊及簽章成功地寫入，則運輸文件控制中樞可將通知發起者交易係成功的之一事件發佈給發起者之訊息代理者中樞。運輸文件控制中樞亦可將具有經加密運輸文件、經加密資料加密金鑰及文件發起者之數位簽章之事件發佈至接收方清單。

【0145】 存取原則含有關於特定運輸文件中可涉及之每一運輸方(使用者)之資訊。存取原則之角色清單可提供將接收最初在運輸文件中提供之資料之使用者之識別碼。在角色清單上之每一使用者可自運輸文件獲得對於其角色(功能)適當之資料。

【0146】 可藉助稱為資料加密金鑰(DEK)之運行時所產生對稱金鑰將運輸文件之資料屬性一個接一個地加密。可藉助與可在運輸文件中具有一角色且可具有對對應屬性之存取權之每一使用者對應之公開金鑰將DEK一個接一個地加密。每一使用者之角色可由角色清單定義。每一角色對每一屬性之存取權可由存取原則定義。然後可將經加密資料屬性、經加密DEK、經加密資料屬性之雜湊及文件發起者之數位簽章發送至適當成員。

【0147】 在某些實施例中，一使用者可將一狀態更新提交給運輸文件控制中樞。該狀態更新提供資料，諸如接收且卸載運輸文件識別碼12345之貨櫃，且某人可必須接取其。運輸文件12345之碼頭狀態更新可未找到任何角色清單。因此除將狀態更新發送至運輸文件控制中樞以外，亦可在使用者節點中緩衝更新。另一當事方可隨後將角色清單發送至使用

者節點，此角色清單可具有相同運輸文件ID (12345)。使用者節點可繼續處理碼頭狀態更新。

使用者節點可自運輸文件控制中樞獲得來自存取原則之以下資訊：

-碼頭狀態更新之動態存取原則(動態存取控制原則可自給定定位子金鑰之角色清單及給定運輸狀態更新類型之存取原則文件導出)

-運輸狀態更新類型之存取原則文件

使用者節點可依據動態存取原則識別使用者扮演之角色。使用者節點可驗證是否允許彼等角色對照存取原則文件創建運輸更新狀態。使用者節點亦可驗證彼等角色是否可創建運輸更新狀態之彼等資料屬性。

可將此經驗證運輸狀態更新加密且提交給運輸文件控制中樞。

【0148】 在某些實施例中，使用者節點可基於使用者之存取原則而自運輸文件控制中樞接收各種文件：碼頭狀態之動態存取原則(動態存取控制原則可自給定定位子金鑰之角色清單及給定運輸狀態更新類型之存取原則文件導出)，及運輸狀態更新類型之存取原則文件。運輸文件使用者節點亦可依據動態存取原則識別使用者扮演之角色。運輸文件使用者節點可驗證是否允許彼等角色對照存取原則文件創建運輸更新狀態。運輸文件使用者節點亦可驗證彼等角色是否可創建運輸更新狀態之彼等資料屬性。在驗證之後，可將此經驗證運輸狀態更新加密。可將經加密運輸狀態更新、經加密資料加密金鑰、經加密資料之雜湊及使用者之數位簽章與一接收方清單一起提交給運輸文件控制中樞。

【0149】 現在闡述操作方法之一實例。

【0150】 在本發明之一運輸操作之一實例中，涉及以下當事方：

【0151】 托運人：工廠A

【0152】 收貨人： S-Mart

【0153】 承運人：XYZ

【0154】 路線：中國至USA

【0155】 貨品：玩具

【0156】 貨櫃號：5

【0157】 在此實例中，運輸線路係XYZ，且運輸線路正在組織將5個玩具貨櫃自工廠A (位於中國)運送至USA之一港口。承運人產生用於運輸之一運輸文件。

【0158】 表II

標頭欄位	資料屬性
托運人	工廠A
收貨人	S-Mart
最後碼頭經營者	長灘，CA
…	…
船舶經營者	SS貨運者
承運人	XYZ

【0159】 承運人係組織將玩具自中國運輸至USA之當事方。承運人然後透過一安全傳輸以純文字形式將以上運輸訂單提供至使用者節點。使用者節點然後將資料屬性加密同時單獨留下標頭欄位。每一資料屬性經加密且具有一單獨資料加密金鑰。

【0160】 表III

標頭欄位	資料屬性
托運人	加密(「工廠A」，k1金鑰)*
收貨人	加密(「S-Mart」，k2金鑰)*
最後碼頭	加密(「長灘，CA」，k3金鑰)*
船舶經營者	加密(「SS貨運者」，k4金鑰)*
承運人	加密(「XYZ」，k5金鑰)*

*在經加密欄位中提供之資料不表示實際加密資訊。文字字串僅係說明性的。「加密(「工廠A」，k1金鑰)」意味文字值「工廠A」由「k1金鑰」加密

【0161】 可將經加密資料記錄於區塊鏈節點中，可根據與所指派角色與存取原則匹配的使用者之公開金鑰將每一資料加密金鑰(在此實例中為k1至k5)加密。在此實例中，托運人工廠A可具有對所有資料屬性之存取權。工廠A之公開金鑰然後可用於將所有金鑰(k1、k2、k3、k4及k5)加密。可單獨將所有運輸文件加密。亦可個別地(串行地或並行地)將金鑰加密。可以一批次格式將金鑰加密，只要可保護每一金鑰之個性(每一經加密金鑰可獨立地經解密，且用於在金鑰不能夠將任何其他運輸文件解密之情況下存取金鑰所對應之特定運輸文件)。

【0162】 每一運輸角色讀取、創建或更新運輸文件之資料屬性之權利可取決於由系統定義之存取權。在此實例性情形中，可存在提供由系統確立之規則之一查找表，如下：

【0163】 表IV

運輸角色	D1	D2	D3	D4	D5
托運人	R	R	R	R	R
收貨人	R				R
最後碼頭經營者		R	R		
船舶經營者		R		R	
承運人	CRU	CRU	CRU	CRU	CRU

【0164】 表IV圖解說明不同運輸角色(例如托運人、收貨人、最後碼頭、船舶經營者、承運人等)之存取原則。D1至D5係由(k1至k5)加密之資料屬性。R係「讀取」,「U」係「更新」且「C」係「創建」。若收貨人具有對D1及D5之存取權(「讀取」、「更新」或「創建」)，則將藉由收貨

人之公開金鑰將k1及k5加密。

【0165】 [PC1]托運人工廠A之公開金鑰可用於將所有金鑰(k1、k2、k3、k4及k5)加密。用於碼頭經營者(USA之港口之長灘碼頭)之公開金鑰可用於將k2及k3加密。用於船舶經營者(運輸之SS貨運者)之公開金鑰可用於將k2及k4加密，且最後，用於承運人XYZ之公開金鑰可用於將所有金鑰(k1、k2、k3、k4及k5)加密。船舶經營者不需要知曉關於托運人之任何資訊。關於托運人之資訊對船舶經營者可係不可見的且可用於船舶經營者之資料屬性金鑰集可不包含用於托運人之資料屬性之金鑰。

【0166】 一旦完成及/或儲存金鑰加密，便可通知個別使用者資料係可用的。使用其自身之私密金鑰之每一使用者可將其各別金鑰解密且存取系統以查看分散式分類帳中之資料，而其他使用者之資訊保持安全地加密。

【0167】 在一更一般形式中，用於產生恰當金鑰以用於存取具有不同所有者之各種資料屬性之程序可涉及產生金鑰且使彼等金鑰與一使用者之所指派角色與存取原則匹配之一程序1500，如圖15中所展示。在開始方塊1502之後，程序可針對每一資料屬性產生一資料加密金鑰1504。在某些實施例中，該等金鑰可係對稱金鑰。可針對每一資料屬性形成加密金鑰。系統可擷取每一運輸方之運輸角色1506。如本文中所闡述，每一當事方可在預訂中具有一運輸角色。該角色可係系統中之任何所定義角色。可將額外角色添加至系統以每當需要時容納額外當事方(每一使用者可係單個運輸交易之一當事方，但一使用者並非必須係單個運輸交易之一當事方)。在某些實施例中，一單個使用者可具有一個運輸角色。在某些實施例中，一單個使用者可具有兩個或兩個以上運輸角色。在某些實施例中，

一使用者可在不具有一正式運輸角色之情況下存取系統，如本文中所闡述。程序可擷取每一運輸角色之存取控制原則1508。存取控制原則可提供資訊以通知程序每一運輸方可存取什麼資料屬性。程序然後可提供用於運輸方之公開金鑰及存取控制原則1510。在此處，可存取控制原則之每一運輸方亦可具有儲存於一公開金鑰儲存庫中之一公開金鑰。程序使運輸方之角色與存取控制原則相關以查看運輸方可存取哪些資料屬性。程序然後可擷取運輸方之適當公開金鑰。程序然後可藉助運輸方之公開金鑰將對應資料加密金鑰加密1512。可以串行方式一個接一個地進行資料加密金鑰之加密。在某些實施例中，可並行地進行資料加密金鑰之加密。在又其他實施例中，可以一批次進行資料加密金鑰之加密。每一資料加密金鑰可經加密使得每一金鑰加密金鑰對應於一或多個資料加密金鑰，且金鑰加密金鑰與經加密資料金鑰之每一一對多關系對應於一單個資料屬性。其可被視為一個一對多或一對一關系(1:m及1:1)。一旦完成程序，程序便可結束1514。

【0168】在某些實施例中，可將一當事方添加至角色清單或存取原則，但彼當事方可不具有在運輸中之一實際角色。在某些實施例中，一非運輸角色當事方可係一金融機構。在某些實施例中，該非運輸角色當事方可係一監管或政府機關。在某些實施例中，該非運輸角色當事方可係一保險公司、一保證人、一司法機關、一貿易監管者、一勞工組織或可針對本文中所闡述之系統之一文件、存取原則或其他庫之至少一個資料欄位存取或查核資料的任何其他實體。

【0169】圖16提供用於基於角色與存取控制原則而將資料屬性加密之程序之另一實例。在此實例1600中，以一托運人、收貨人、最後碼

頭、船舶經營者及一承運人之形式呈現五個角色。在某些實施例中，可存在每角色一個當事方。在某些實施例中，可存在具有一個以上角色之一個當事方。在又其他實施例中，兩個或兩個以上當事方可共用一單個角色。對於圖16中所繪示之實例，存在五個角色及每角色一個當事方。

【0170】 在某些實施例中，一資料與金鑰結構1602可含有如所展示之五個資料屬性(D1至D5)。可藉助一資料加密金鑰將每一資料屬性個別地加密1606 (k1至k5)。每一資料屬性亦可具有一標頭及資料屬性欄位。如樣本存取控制原則1604中所展示，每一角色(托運人、收貨人等)具有針對標頭所定義之存取控制及對應於每一資料屬性之一標頭(頂部列) (H1 → D1、H2 → D2、H3 → D3、H4 → D4及H5 → D5)。列(角色)與行(標頭)之間的交叉點為角色(匹配列之左邊行之當事方)提供存取原則。舉例而言，根據存取控制原則，托運人具有「R」存取。托運人可「讀取」對應於D1至D5之資料屬性。然而，托運人不可更新或修改資料，托運人亦不可創建任何資料。另一方面，根據圖16之樣本存取控制原則，承運人可具有創建(C)、讀取(R)及更新(U)權威。其他當事方(諸如收貨人)可僅讀取用於對應於D1及D5之H1及H5之資料。最後碼頭可僅讀取用於對應於D2及D3之H2及H3之資料。船舶經營者可僅讀取用於對應於D2及D4之H2及H4之資料。

【0171】 然後可藉由用於在存取控制原則中具有一角色匹配之每一當事方之公開金鑰將資料加密金鑰加密。在此實例中，托運人具有可用於將每一資料加密金鑰k1至k5個別地加密之一公開金鑰(S_{pub})，如資料加密金鑰之公開金鑰加密1608表中所展示。1604表中之托運人列意味托運人將進行存取以讀取資料屬性D1至D5，但將不能夠創建、刪除或更新彼等

欄位。收貨人具有用於將對應於H1及H5 (其係收貨人根據收貨人之存取控制原則1604存取之兩個資料屬性)之資料加密金鑰(DEK)加密之一公開金鑰(Co_{pub})。收貨人之公開金鑰用於將k1及k5加密。經加密k1及k5可稱為一DEK，且收貨人可具有用於D1及D5之DEK，吾等將其縮寫為k1及k5。收貨人可透過系統中之其使用者節點接收k1及k5。收貨人然後可使用k1及k5來存取對應於D1及D5之資料屬性。程序對於最後碼頭、船舶經營者及承運人可係相同的。具有一角色之每一當事方可透過系統中之其使用者節點存取其適當DEK，且然後可存取對應於DEK之資料屬性。

【0172】 圖17圖解說明包含具有一唯一ID 1706及一角色清單1710之一運輸文件之一實施例1700。存取原則1702可係基於角色的。其可具有兩個層級。一個層級可係用於運輸文件1706之每角色創建、更新、邏輯刪除及讀取之一文件物件層級。其亦可提供准許運輸文件1706之創建、更新及讀取屬性之一屬性層級。角色清單存取原則1704可係基於角色的。其亦可具有兩個層級。一個層級可係用於一角色清單1710之每角色創建、更新、邏輯刪除、讀取之一角色清單物件層級。其亦可具有准許角色清單1710之創建、更新及讀取之一角色屬性層級。在某些實施例中，可給一運輸文件1706指派一角色清單。角色清單1710加上運輸文件存取原則1702可提供係當事方之每一使用者對運輸文件之特權。在某些實施例中，每一運輸文件可具有其自身之角色清單及其自身之存取原則。每一使用者可具有在滾動清單上之一所定義角色及在存取原則中之一所定義存取。每一使用者之角色與每一使用者之存取之間的交叉點可定義彼使用者之特權。一角色清單可適用於諸多不同運輸文件。例如，一運輸角色清單可適用於一DG憑證、一提單、碼頭裝載或卸貨事件或任何其他形式

之運輸文件1706。此等不同形式之運輸文件亦可稱為文件類型1714及事件類型1716。文件類型1714及事件類型1716可定義所支援類型之運輸文件1706之一群組。在某些實施例中，文件類型1714之運輸文件1706具有版本化。在某些實施例中，每當編輯或修改文件時，一文件之版本號可遞增地增加。其可用於支援相同原始運輸文件之多個版本。每一運輸文件1706可具有一唯一ID。亦可存在諸多種類之角色清單1710。運輸角色清單1718、貨櫃角色清單1720係可能類型之角色清單1710中之某些。運輸文件1706及角色清單1710可分別使用定位子金鑰1708及定位子金鑰1712。在某些實施例中，可不將定位子金鑰1708、定位子金鑰1712加密。定位子金鑰1708、定位子金鑰1712對運輸文件控制中樞可係可見的且可用於支援其(中樞)功能。定位子金鑰可允許一基於金鑰之查找(例如運輸號)識別相關角色清單1710及相關運輸文件1706。運輸文件1706藉由其類型可識別存取原則1702。

【0173】 圖18圖解說明某些實例性角色清單及角色清單原則。在某些實施例中，一角色清單存取原則定位子金鑰1802可提供「角色清單類型」及「定位子金鑰欄位」之實例性標頭。「角色清單類型」下面係「運輸角色清單」且定位子金鑰欄位下方係承運人及預訂號。此圖解說明運輸角色清單之定位子金鑰欄位係承運人及預訂號。一角色清單存取原則實例1804可展示角色清單類型之類別，其中提供一運輸角色清單。角色經展示為：托運人、收貨人、承運人、船舶經營者及碼頭經營者。在此實例性表中，運輸角色清單指示承運人具有創建一角色清單之權威及系統特權。在此實例中，其他角色中無一角色可創建一角色清單。下一表展示一角色屬性層級實例1806。在此處，「角色清單類型」展示在第一行中之「運輸

角色清單」及在第二行中之「角色屬性」。現在在角色屬性行中列出來自角色清單存取原則實例1804之個別角色。表之剩餘部分展示用以創建、讀取或更新(修改)一角色清單運輸文件之一角色屬性的「角色」對「角色屬性」存取特權。粗線框展示第二行及第三行，且指示托運人可讀取運輸角色清單之所有角色，然而托運人不可創建或更新運輸角色清單中之任何角色屬性。角色清單實例具有角色清單定位子金鑰1808及角色清單內容1810。角色清單定位子金鑰1808圖解說明一承運人XYZ及一預訂號123456。運輸角色清單可包含角色清單內容1810，角色清單內容1810可圖解說明各個使用者在其角色中之識別碼(僅出於圖解說明目的，此等識別碼係虛擬的)。

【0174】 現在展示數個實例性運輸文件1900，文件可圖解說明商業相關標頭，但僅出於圖解說明目的而使用虛擬資料，如圖19中所展示。在某些實施例中，可存在一貨櫃出境事件1902之一運輸文件(來自一碼頭經營者)。實例性表展示事件ID (運輸文件之唯一識別符)、承運人及預訂號(承運人及預訂號可允許角色清單之定位)及關於碼頭處之聯運貨櫃之資訊。可將此資訊發送至運輸文件控制中樞且重新分佈至在角色清單上所識別之其他使用者，因此可將此特定出境事件同時通知給每一使用者。運輸文件存取原則可具有3個部分–「角色清單定位子」金鑰1904、「運輸文件存取原則」1906及「出境事件欄位層級之運輸文件存取原則」1910。角色清單定位子金鑰1904 (圖17之一實例，1708)指示：對於一出境事件，運輸角色清單可適用且承運人及預訂號可用於定位角色清單，承運人及預訂號可作為承運人XYZ及預訂號12345自出境實例1902經擷取。運輸文件層級原則實例1906指示：對於一出境事件，所展示之五個角色可讀取此

運輸文件類型「出境事件」運輸文件，但僅碼頭經營者(此事件之發起者)角色可創建或更新運輸文件。在某些實施例中，諸如碼頭經營者之一角色亦可執行運輸文件之一邏輯刪除。

【0175】 在某些實施例中，運輸文件架構實例1908可圖解說明左行中之一欄位名稱(「標頭欄位」)以及右邊之行中之資料屬性類型。樣本資料屬性可係任何長度，且所展示之字串長度僅僅係說明性的。如此實例1908中所圖解說明，事件ID係此運輸文件類型之唯一ID；且承運人及預訂號欄位係此運輸文件類型之角色清單定位子金鑰。運輸文件原則欄位層級實例1910提供對運輸文件類型(在此實例中為一出境事件)及一欄位行之一圖解說明，其展示來自架構實例1908及出境事件實例1902之各種標頭欄位。欄位層級實例1910之第3至第7(第三至第七)行中之欄位清單展示哪一角色針對每一欄位具有什麼權利。單個交易之所有角色可讀取資料，而承運人及碼頭經營者可更新(修改)資料。由於運輸文件出境事件係源自碼頭經營者之一資產，因此僅碼頭經營者可創建此種類之運輸文件。

【0176】 在某些實施例中，本文中所闡述之系統及方法可與危險品(DG)一起使用，如圖20中所見。危險品可需要一特殊運輸憑證，在本文中稱為一危險品憑證(DG Cert)。當所運輸之材料可係有危險的或具有可對運輸程序中所涉及之彼等造成危險之數量時出現運輸貨物中之危險品。危險品之實例可包含燃料、放射性材料、腐蝕性化學品及液體、爆炸品等等。在一實例之某些實施例2000中，展示一DG cert實例2002表之一運輸文件。標頭欄位表示左邊行且提供資訊類別。右邊行中之資料屬性展示針對每一類別之對應資料。角色清單定位子資訊可表示承運人及預訂號。亦可列出貨品闡述。角色清單定位子資訊可用於存取DG cert角色清單實

例，該DG cert角色清單實例可由運輸文件存取原則角色清單定位子金鑰2004、文件層級存取原則2006及欄位層級存取原則2008構成。角色清單定位子金鑰2004指示：對於每一出境事件，可存在一運輸角色清單，「角色清單類型」以及一承運人及預訂號用作「定位子金鑰欄位」。文件層級存取原則2006圖解說明展示處於文件層級之運輸文件類型「DG Cert」之存取原則之一表。展示與危險品之運輸相關聯之實例性當事方以及其各別讀取(R)、創建(C)、更新(U)及刪除(D)權威。DG cert架構實例2010為目前實例提供DG憑證(運輸文件)之標頭及資料屬性類型。「DG Cert之運輸文件存取原則實例– 欄位層級(欄位可係指一文件中之資料輸入欄位)」2008提供運輸文件類型之相關資訊(DG Cert)、自DG cert實例2002及DG cert架構實例2010中得到之欄位，且展示每一當事方(使用者)之各別權利。

【0177】 在一實例中，可在圖21中看到對邏輯系統佈局2100之一圖解說明。在某些實施例中，可存在用於產生一運輸文件之一系統。該系統可具有一運輸文件控制中樞2102及一第一使用者節點2104。該運輸文件控制中樞可具有一電腦，該電腦包括一邏輯、一記憶體及一通信裝置。一文件控制中樞側訊息代理者2106可透過電腦邏輯操作。訊息代理者2106可發送及接收一或多個事件訊息2108、2110。可存在可儲存於記憶體上之一存取原則儲存庫2112。在記憶體上亦可存在一公開金鑰儲存庫2114及一ID儲存庫2116。記憶體可係一或多個實體裝置且其不需要實體地含納於電腦內。只要電腦可存取所闡述之各種資料庫，可在一實體意義上分佈實體記憶體。ID儲存庫2116可具有一或多個使用者、一或多個使用者登入認證及一或多個使用者參數之一清單。記憶體可係用於儲存經加密運

輸文件之存取原則中之一或多者之一區塊鏈節點。第一使用者節點2104可具有一電腦，該電腦具有一邏輯、一記憶體及一通信裝置。類似於運輸文件控制中樞，用戶端(使用者)節點2104、2118可具有電腦之記憶體且可係可在電腦內部或外部之一個以上記憶體裝置，只要電腦可存取該(等)記憶體裝置。一金鑰儲存區2120、2122可係使用者節點之一部分，該金鑰儲存區可保存一登入ID秘密及使用者之一私密金鑰。該金鑰儲存區可係可由電腦存取的。使用者節點2104、2118亦可具有一API介面，該API介面具有用於與金鑰儲存區及一使用者訊息代理者2124、2126進行電子通信之一密碼存取層。使用者節點可具有供一使用者存取運輸文件控制中樞之一入口網站，其中API介面可在邏輯上執行，且與運輸文件控制中樞訊息代理者通信。

【0178】 在某些實施例中，使用者節點與運輸文件控制中樞之間的通信可由訊息代理者處置。系統可使用每一節點與運輸文件控制中樞(中樞)之間的一安全網路通信。該等訊息代理者可為節點及中樞提供安全網路通信以將資訊傳遞至彼此。使用者節點之應用程式設計介面(API)可係為金鑰儲存區與訊息代理者之間的密碼交換提供一存取層之一電腦實施之程式。該存取層可實施於一電腦邏輯或處理器上。用戶端應用程式可係供一使用者存取API介面及訊息代理者之任何介面。用戶端應用程式可係專屬軟體或可係現成軟體。每一節點之訊息代理者可存取中樞中之區塊鏈邏輯，且經加密運輸文件可以一區塊鏈格式來儲存，其中一或多個經加密欄位指派給每一節點。每一記憶體元件可具有任一數目個區塊鏈資料庫，此乃因針對每一運輸文件類型可存在一個區塊鏈資料庫。

【0179】 在某些實施例中，可在圖22中看到一角色清單提交之一樣

本流程圖2200。在某些實施例中，當提交一角色清單時，角色清單可具有一初始檢查屬性驗證2202。在此步驟中，程序檢查定位子金鑰(例如預訂號及發送者之組織ID (SCAC碼))及角色清單(角色清單亦包含角色清單類型)是否可在請求中。若是，則程序可執行一角色檢查2206以查看發送者之組織ID是否可係角色清單中之當事方中之一者。若是，則程序檢查以查看是否定義角色清單存取原則2208。此步驟涉及檢查彼角色清單類型之角色清單存取原則。程序然後可檢查一存取權檢查2210以藉由ID儲存庫查找發送者之組織之角色且檢查發送者之角色是否具有存取權(角色清單層級及一角色清單中之一資料欄位，有時在本文中稱為一「角色清單欄位層級」)以創建一角色清單並創建該角色清單中之角色。若在任一點處程序未能產生一有用結果，則程序可結束且可傳回一錯誤回應碼2212且然後終止(結束2234)。若所有步驟係成功的，程序可針對角色清單中之所有角色產生加密金鑰2214。使用該等加密金鑰，程序可將角色清單加密2216。程序可藉由經加密角色清單產生一雜湊且存取金鑰儲存區以藉由發送者之私密金鑰簽署雜湊從而產生發送者之簽章2218。程序可針對角色清單上之每一當事方獲得公開金鑰2220，且根據每一當事方之存取控制原則使用當事方之公開金鑰將資料加密金鑰加密2222。程序可藉由使用經加密角色清單、經加密資料加密金鑰(與當事方之公開金鑰相關聯)、雜湊及發送者之簽章而將訊息打包。程序可藉助使用者之私密金鑰以數位方式簽署訊息以產生使用者之簽章。可將訊息發送至運輸文件控制中樞2223。程序然後可藉由找出當事方之區塊鏈節點且將經加密角色清單及經加密資料加密金鑰分佈至各別區塊鏈節點而分佈資料及加密金鑰2224。程序然後可藉由檢查是否成功地分佈經加密資料、經加密資料加

密金鑰、雜湊及發送者之簽章而檢查分佈成功2226。程序然後可將具有成功碼2232之事件發佈至訊息代理者，或將具有一錯誤碼之事件發佈至訊息代理者2228。

【0180】在某些實施例中，用戶端應用程式可創建一角色清單且經由用戶端側訊息代理者及使用者節點與運輸文件控制中樞通信。使用者節點中之密碼存取層可自中樞獲得公開金鑰及存取控制原則。存取層然後可證實且加強存取控制原則，將一有效負載(角色清單)加密且將訊息放置至訊息代理者。訊息代理者(用戶端側)可與運輸文件控制中樞之訊息代理者通信，且運輸文件控制中樞側上之訊息代理者獲得去往程序之訊息以分佈經加密資料及經加密資料金鑰，且然後可發佈具有可去往用戶端側訊息代理者之一成功碼的事件2232。用戶端側可應答成功訊息及確認接收，且可創建一交易完成應答。

【0181】在某些實施例中，可存在用於讀取一運輸文件之一程序2300，如圖23中所展示。該程序可在開始方塊處以一給定文件ID (例如DG Cert ID) (在某些實施例中，可給出一版本號)、運輸號、發送者之組織ID (例如SCAC (標準承運人字母碼))及一特定角色清單類型開始。其繼續進行以檢查屬性驗證2302。在此步驟中，程序可檢查定位子金鑰(運輸號、發送者之組織ID)、文件ID及角色清單類型是否有效。若如此，則程序使用角色清單之定位子金鑰及角色清單類型(未展示)自發送者之節點獲得經加密角色清單及經加密資料加密金鑰2304。若無法找到角色清單，則程序可傳回一錯誤回應碼2316且然後可進行至結束方塊2322。若可找到角色清單，則程序可檢查角色清單之相關性2310。程序可檢查以查看所有區塊鏈節點中之角色清單資料是否彼此匹配。若任一區塊鏈節點中之

角色清單資料不與其他區塊鏈節點匹配，則程序可傳回一錯誤回應碼2316且然後可進行至結束方塊2322。若角色清單資料在所有區塊鏈節點中係相同的，則程序可存取金鑰儲存區2312以將資料加密金鑰解密2314。若無法將資料加密金鑰解密，則程序可傳回一錯誤回應碼2316且然後可進行至結束方塊2322。若可將資料加密金鑰解密，則程序可使用資料加密金鑰來將角色清單解密2318。程序然後可傳回一成功回應碼2320，或另一選擇係，若程序失敗，則程序可傳回一錯誤回應碼2316。程序然後可進行至結束方塊2322。

【0182】 現在在圖24中展示一流程圖，該流程圖展示一運輸文件創建2400。在某些實施例中，程序可藉由檢查定位子金鑰(例如預訂號及發送者之組織ID)及運輸文件內容(例如DG cert)及運輸文件類型是否可在請求中來檢查屬性驗證2402。程序可檢查是否可存在來自存取原則儲存庫之一現有角色清單2404。此步驟可涉及檢查存取原則儲存庫有無適用角色清單類型，然後檢查彼角色清單類型之一現有角色清單。一運輸角色檢查2406 (或僅僅一角色檢查)可判定發送者之組織ID是否係角色清單上之當事方中之一者。程序可檢查以查看是否可在運輸文件層級及運輸文件欄位層級處定義存取原則2408。程序可進行一存取權檢查2410以查找發送者之組織在ID儲存庫中之角色，且可檢查發送者之角色是否具有正確存取權(運輸文件層級及欄位層級)以創建彼類型之一運輸文件(例如DG cert)，且在其中創建資料。程序然後可產生遍及整個系統可係唯一之一唯一運輸文件ID 2412 (例如DG cert ID)。程序可針對運輸文件中之所有資料屬性產生資料加密金鑰2414。然後可使用資料加密金鑰在運輸文件(例如DG cert)中將資料屬性加密2416。程序可產生關於經加密資料屬性之一雜湊

且存取金鑰儲存區以藉由發送者之私密金鑰簽署雜湊來產生發送者之簽章2418。然後，可針對在運輸文件中之角色中所識別之每一當事方獲得公開金鑰2420。可針對以運輸文件中之一角色識別的每一當事方，使用適當公開金鑰來將資料加密金鑰加密2422。程序可將具有經加密資料屬性、經加密資料加密金鑰、雜湊及發送者之簽章的訊息打包2424。程序可將訊息發送2426至運輸文件控制中樞。運輸文件控制中樞可藉由以下方式來分佈經加密資料、金鑰、雜湊及發送者之簽章：找出恰當當事方之區塊鏈節點；及將經加密運輸文件、經加密資料加密金鑰(DEK)、雜湊及發送者之簽章分佈至區塊鏈節點。程序可檢查以藉由使每一使用者節點以一成功通知做出回應來查看分佈是否係成功的2428。另一選擇係，程序可分佈訊息且將分佈記錄為成功的，除非自一或多個接收方接收一錯誤訊息。可將一成功事件通知發佈給發送者2432。角色清單接收方可接收具有經加密運輸文件、經加密DEK、雜湊及發送者之簽章之一發佈事件2430。事件至任一接收方之發佈可取決於接收方是否同意一特定運輸文件類型(例如「所創建DG cert」)之更新事件。接收方使用者節點可藉由以下方式來檢查完整性2436：計算來自經加密運輸文件之雜湊；及藉由使用發送者之公開金鑰解密發送者之簽章以獲得經解密雜湊。程序可比較經解密雜湊與來自經加密運輸文件之雜湊。接收方節點然後可存取金鑰儲存區，以藉由資料解密金鑰將經加密資料加密金鑰解密2438且將運輸文件解密2440。用戶端應用程式可以純文字形式接收運輸文件2442。程序然後可進行至結束方塊2448。

【0183】 現在在圖25中展示一運輸文件更新2500之一流程圖。程序可自開始方塊2502繼續，以藉由驗證運輸文件ID/定位子金鑰(例如預訂號

及承運人之組織ID (SCAC碼))及經更新運輸文件(例如DG Cert)是否可在請求中來檢查屬性2504。程序可檢查一現有運輸文件2506。此可藉由搜索運輸文件ID及/或定位子金鑰及運輸文件類型而自區塊鏈分類帳判定。可進行一檢查以查看是否可找到現有角色清單2508。程序可藉由藉助一或多個定位子金鑰及/或一或多個角色清單類型來進行搜索而自存取原則儲存庫找到角色清單。可進行一角色檢查2510以判定發送者組織ID是否可係角色清單上之當事方中之一者。程序可檢查以查看是否定義存取原則2512。程序可存取原則藉由供應「運輸文件類型」(例如運輸文件類型=「DG Cert」)而自一部分或整個文件獲得運輸文件。可執行一存取權檢查2514以判定發送者之角色是否可具有存取權(欄位層級)以更新運輸文件中之資料值。程序可合併現有運輸文件屬性與所提交資料屬性之經加密資料(若可用) 2516。程序可使運輸文件之版本號增加一2518。程序可針對所提交運輸文件中之新資料屬性2522產生資料加密金鑰2520。舉例而言，若存在10個資料欄位，且3個資料欄位影響一使用者，則僅改變影響該使用者之三個資料欄位，因此僅3個資料欄位可需要新加密金鑰。剩餘7欄位可不具有新金鑰，且僅僅剩下已經存在之舊資訊。程序可藉由使用資料加密金鑰將運輸文件中之所提交資料屬性加密2524。程序可產生關於任何新加密之資料屬性(資料欄位)之一雜湊，且存取金鑰儲存區以藉由發送者之私密金鑰簽署雜湊來產生發送者之簽章2526。程序可獲得角色清單中之當事方的公開金鑰2528。程序可藉由使用每一當事方之公開金鑰，使用每一當事方(使用者)之存取控制原則來將經更新資料加密金鑰加密2530。程序可將具有經加密資料屬性、經加密資料加密金鑰、雜湊及發送者之簽章的訊息打包2532。程序可將訊息發送至運輸文件控制中樞

2532。程序可藉由以下方式來分佈經加密資料及金鑰：找到當事方之區塊鏈分類帳；及將經加密運輸文件、經加密資料加密金鑰、雜湊及發送者之簽章金鑰分佈至恰當區塊鏈分類帳2534。可執行是否成功地分佈經加密運輸文件、經加密資料加密金鑰、雜湊及發送者之簽章之一檢查2536。可在一成功碼發送至發送者之訊息代理者的情況下，執行具有至發送者之成功碼之一發佈事件2550。若未進行保存至交易參考資料庫，則程序可替代地將具有要發送之一錯誤碼之一事件發佈至發送者之訊息代理者2554。程序可將具有一經加密運輸文件、經加密資料加密金鑰及發送者之簽章之一事件發佈至既定接收方2538。至接收方之發佈事件取決於組織是否同意運輸文件更新事件(例如「經更新DG Cert」)。事件有效負載可含有一經加密運輸文件、經加密DEK及發送者之簽章。接收方使用者節點可藉由以下方式來檢查完整性2540：計算來自經加密運輸文件之雜湊；及藉由使用發送者之公開金鑰將發送者之簽章解密以獲得經解密雜湊。程序可比較經解密雜湊與來自經加密運輸文件之雜湊。若完整性檢查2540失敗，則程序可將錯誤回應碼傳回至接收方2548。若完整性檢查成功，則接收方節點然後可存取金鑰儲存區以將資料加密金鑰解密2542，且藉由資料解密金鑰將運輸文件解密2544。用戶端應用程式可以純文字形式接收運輸文件2546。程序然後可進行至結束方塊2556。

【0184】現在在圖26中展示用於讀取一運輸文件之一實例性程序2600。程序在一開始方塊2602處開始且可繼續進行以檢查是否可在請求中供應一運輸文件版本號，且對照一交易參考資料庫檢查該運輸文件版本號2604。程序然後可進行一屬性驗證2606以檢查運輸文件ID及/或定位子金鑰(預訂號及發送者之組織ID (SCAC碼))及運輸文件類型是否在請求

中。程序可藉由運輸文件ID自發送者之區塊鏈節點獲得經加密運輸文件及經加密資料加密金鑰2608。(在某些實施例中，可存在一相關性檢查(檢查相關性2610)以查看來自區塊鏈節點之經加密運輸文件及經加密資料加密金鑰在內容層級中是否係相同的。)

【0185】 使用者節點可存取金鑰儲存區2612以使用發送者之組織之私密金鑰將資料加密金鑰(DEK)解密且取回資料加密金鑰(DEK) 2614。使用者節點可藉由資料加密金鑰將經加密運輸文件解密2618且可將一成功回應碼傳回2620至用戶端應用程式。若程序在任一點處失敗，則程序可將一錯誤2616碼傳回至用戶端應用程式。程序可結束2622。

【0186】 在某些實施例中，在存取現有角色清單及/或現有運輸文件時之步驟中之一或多者中，可由使用者節點或運輸文件中樞檢查現有角色清單及/或現有運輸文件之資料完整性。完整性檢查程序藉由依據經加密運輸文件(或角色清單)計算雜湊且比較其與現有運輸文件(或角色清單)中之現有雜湊而開始。發送者之簽章可對照其公開金鑰經驗證。若現有雜湊與所計算雜湊匹配且成功地驗證發送者之簽章驗證，則其係一有效簽章且維持文件之完整性。

【0187】 一旦一使用者能夠存取預訂API，該使用者便可填充一預訂配置2700 (實例)。預訂配置2700可具有用於與貨物運輸有關之資料輸入之多個欄位。欄位可包含但不限於托運人、收貨人、船舶經營者、代運人、承運人及預訂方(其可係使用者)之識別碼。預訂配置2700亦可視需要具有路線資訊、貨櫃/貨品資訊及其他或雜項資訊。創建預訂之使用者可看到預訂配置中之所有資料屬性。預訂使用者可輸入至預訂配置2700中之額外資訊可包含對使用者可係機密的之資訊。當將預訂配置2700輸入

至系統中時，可單獨地處理每一欄位。舉例而言，一旦創建記錄，預訂配置2700中之托運人便可觀看記錄，但托運人可僅看到與其相關之資訊(例如，運輸處置之實際價格)。在另一實例中，收貨人可看到與其相關之資訊(例如，傳回空聯運貨櫃之位置)。預訂版本號2702表示使用者正在觀看之版本。一般而言，使用者可看到最新版本。在某些情形中，一使用者可搜索比最近記錄舊之記錄。

【0188】 現在在圖28中展示如由一船舶經營者觀看之一局部預訂視圖2800之一樣本截圖。該截圖包含承運人之識別碼，但可隱藏預訂方、托運人、代運人及收貨人之識別碼。另外，可存在路線資訊中之資訊、貨櫃/貨品資訊之一部分或自船舶經營者之視圖保持隱藏之其他資訊欄位。以此方式，製成局部預訂視圖2800之使用者(預訂方)可填充與參與貨品之運輸之每一其他當事方相關之所有資訊。運輸文件可含有每個當事方使用或進行其交易之一部分所依賴、又使預訂方可不想要共用之任何資訊隱藏之資訊。預訂方可定義其想要其他人看到什麼欄位、彼等其他當事方係誰，或預訂方可使用一組標準化保護欄位。系統可基於每一使用者之角色之存取控制原則而決定一使用者可看到哪些欄位。

【0189】 在某些實施例中，存取角色原則中之可並非系統之使用者之一當事方仍可藉由具有來自存取角色原則中之一使用者之一權限而獲得對系統中之特定材料及資訊之存取。此一非使用者當事方可係一銀行或其他金融機構、一政府實體(諸如一港口檢驗員)或對運輸交易具有一附屬興趣之其他第三方(諸如一保險公司、海關代理、維修設備或任何其他當事方)。

【0190】 在某些實施例中，一使用者可請求一第三方存取系統內之

特定資料。另一選擇係，使用者可請求在系統中具有向系統之一第三方非使用者驗證之特定資訊。使用者可向系統提出一驗證請求，且非使用者可獲得對特定資訊之存取以便驗證由使用者進行之陳述。程序可在具有或不具有來自系統之直接行動之情況下完成，且允許使用者與第三方非使用者之間的機密性。

【0191】 在圖29中可看到對系統、使用者及第三方非使用者之邏輯關係之一圖解說明。在某些實施例中，一所註冊使用者2902及一使用者節點2908可透過使用者節點2908向文件控制中樞2906提出請求。在某些實施例中，使用者可與一第三方2904通信，第三方2904可不具有對文件控制中樞2906之任何存取權，亦並非如本文中所闡述之系統之一使用者。例如，一訊息代理者可經組態以將一訊息發送至一第三方2904 (一第三方非使用者)，其中該訊息包括來自運輸文件控制中樞之經加密資料。經加密資料可限定於一使用者2902 (或一對應使用者節點2908)能夠根據一存取控制原則及一使用者角色清單存取之資料。第三方2904可係對使用者2902之運輸活動感興趣之一組織或個體，但並非運輸協議之一當事方。第三方2904可係一銀行或其他借貸機構、一保險公司、一經紀人、一維修設備、一政府機關或政府行動者或可對運輸協議感興趣之任何其他當事方，且需要存取文件控制中樞2906或由如本文中所闡述之系統支援之受控制資料庫中之任一者上之某些資料或文件。

【0192】 具體而言，出於自第三方2904獲得某物之目的，使用者2902可將文件或資訊傳達至第三方2904當事方。來自第三方2904之此物可使使用者參與運輸協議，或與系統之其他使用者進行業務。實例可係為運輸協議提供資金、為協議之一態樣提供經濟擔保、商品或承運人之保

險、檢驗資料以在到達一港口時驗證貨櫃內容等等。

【0193】 為了獲得第三方2904之輔助，使用者2902可使用經加密且安全使用者與第三方通信2912協定將第三方2904可請求之所有文件提交給第三方2904。使用者與第三方通信2912可包含自使用者2902遞送至第三方2904之經加密資料及資料加密金鑰，因此第三方2904可恰當地觀看資料。在某些實施例中，第三方2904可希望驗證由使用者2902提供之資料之真實性。第三方2904可存取一第三方節點2910以與文件控制中樞2906通信，且請求自使用者2902接收之資料之驗證。第三方節點2910可與文件控制中樞2906中之一驗證功能進行通信。在某些實施例中，第三方2904可經由第三方節點2910將經加密資料發送至文件控制中樞2906，且請求經加密資料之驗證。在某些實施例中，第三方2904可發送經加密資料及經加密資料加密金鑰以用於解密。第三方2904可發送由使用者2902提供之任何額外材料以由文件控制中樞2906驗證。文件控制中樞2906可經由第三方節點2910將驗證所需要之資訊發送回至第三方2904。

【0194】 在某些實施例中，第三方2904可將經加密資料發送至第三方節點2910，第三方節點2910可產生經加密資料之一雜湊且可提供經加密資料之該雜湊並比較其與記錄於文件控制中樞2906中之運輸文件之雜湊。匹配雜湊可揭露資料係真實的，儘管文件控制中樞2906可不實際上將任何資料發放給第三方2904。在某些實施例中，可允許使用金鑰檢查進行驗證及經加密金鑰之雜湊或現在存在或未來導出之任何其他機制，彼可適合文件控制中樞2906及使用者2902系統之使用。當第三方2904可確認來自使用者之資料之真實性時，第三方2904可繼續進行其內部操作以向使用者2902提供使用者繼續其在運輸協議中之職責所需要之任何事

物。

【0195】 在某些實施例中，可圖解說明系統側3012上之文件控制中樞3002 (DCH)、使用者3022及第三方3060之間的關係，如圖30中所展示。DCH 3002可具有一運輸文件資料庫3004_a，且可具有其他資料庫，諸如一存取原則儲存庫3004_b、一公開金鑰儲存庫3004_c、一ID儲存庫3004_d或用於系統之操作之任何其他資料庫3004_n。當使用者3022可需要一銀行貸款時，使用者3022可向DCH 3002請求特定資料及文件。可對照ID儲存庫及存取原則儲存庫或任何其他鑑認方法或要求鑑認使用者之請求。可在系統3012或DCH 3002中識別使用者。使用者可具有關於常駐於系統側上之「資料加密金鑰」之一或多個接收方庫加密3006_{a-n}。一旦鑑認使用者請求，DCH便可自一或多個資料庫提取所請求資料且將資訊提供給使用者3022。可藉助經加密資料加密金鑰將資訊捆綁至一系統產生之資料封裝3006中，然後將該資訊發送至使用者3022。

【0196】 資料封裝3006可含有經加密資料且與經加密資料加密金鑰3026一起發送資料封裝3006。使用者可經由一安全通信鏈路3020自DCH 3002或系統3012接收資料封裝3006。當資料封裝在使用者之控制區帶中時，可修改、打開或單獨留下使用者控制之資料封裝3024。在某些實施例中，資料封裝3024可含有更多或更少材料。在某些實施例中，可使用使用者之公開金鑰將資料加密金鑰3026加密。可將資料封裝3024及資料加密金鑰3026傳達至使用者3022。

【0197】 在使用者3022側上，可使用使用者私密金鑰3028來將經加密資料加密金鑰3026解密。使用者可將資料封裝3024及經解密資料加密金鑰3026發送至第三方3060。使用者可經由一單獨安全通信鏈路3064將

資料封裝3024發送至第三方3060。由於資料之經加密性質，在某些實施例中，使用者、DCH/系統或第三方可選擇使用不安全通信。

【0198】 一旦第三方3060具有在其控制中之經加密資料、第三方受控制資料封裝3062及來自使用者3022之經解密資料加密金鑰3026，第三方3060便可透過第三方節點(未展示)存取DCH 3002。DCH 3002然後可使用DCH託管之驗證功能3010，使用第三方資料封裝3062中之經加密資料驗證第三方請求之真實性。第三方3060然後可接收由使用者3022提供之資訊可係真實的之確認，此乃因雜湊及其他資料加密元素匹配系統3012及/或DCH 3002之雜湊及其他資料加密元素。

【0199】 在某些實施例中，一使用者可將任何量之資訊提供給一第三方，就像其亦進行了存取一樣。一般而言，一使用者可僅提供可與對資訊之第三方請求相干之彼資訊。舉例而言，一第三方銀行可請求金融資訊、所完成運輸協議之記錄及來自在使用者下游之當事方之支付。一保險第三方可請求運輸一特定種類之材料(諸如一危險品)之歷史，以及使用者之歷史關於與事故數目、先前保險索賠數目等等有關之請求可係如何。舉例而言，一政府機關可充當一第三方且請求與一運輸之最終目的地、一最終購買者可係誰或貨品是否將或已經過一特定國家之領土有關之資訊。請求類型可係無限制的。使用者然後可向系統發出資料請求。系統可將資料產生至資料封裝3006中。資料封裝3006可含有經加密資料、一雜湊、一時間戳記及發送者之一簽章。取決於發送者(使用者)請求，資料封裝3006可含有額外材料或較少材料。

【0200】 在某些實施例中，可將資料封裝3006加密且發送至一使用者。在某些實施例中，使用者擁有之資料封裝3024可在所有方面完全相

同於由系統組裝之資料封裝3006。然而，由於使用者現在在資料封裝3024之控制中，因此區別資料封裝3024與由系統3006產生之資料封裝。使用者3022可打開資料封裝3024且與一第三方3060共用其。使用者可全部地共用資料封裝(在不打開其之情況下)或可打開其，且將其重新加密並發送至第三方。舉例而言，使用者3022可經由一第一用戶端節點獲得資料封裝，且可將資料封裝發送或分佈至一第三方(一第三方非使用者)。當第三方接收資料封裝時，資料封裝3062現在在第三方之控制下。其仍可完全相同於最初由系統發送之資料封裝3006，或完全相同於使用者之資料封裝3024。第三方可力圖驗證資料封裝3062之內容。第三方可使用一第三方節點(或經由該第三方節點通信)以使用或存取DCH中之驗證功能3010。舉例而言，第三方可與DCH中之一驗證功能3010 (亦稱為一驗證功能)通信，以驗證資料封裝之一完整性。在某些實施例中，第三方節點可調用DCH中之驗證功能3010，DCH可視需要自運輸文件資料庫3004a或任何其他資料庫獲得經加密資料。驗證功能3010然後可將經加密資料發送至第三方節點，因此第三方可比較來自驗證功能3010之經加密資料與由使用者3022提供之資料封裝3062中之經加密資料。在某些實施例中，第三方可將資料封裝3062之雜湊發送至DCH託管之驗證功能3010，且若用於資料封裝3062之雜湊與用於資料封裝3006之雜湊相同，第三方可具有所提供資料係正確的且未自其源變更之證明。

【0201】 現在在圖31至圖35中提供第三方功能之實例性實施例。在某些實施例中，一代運人可獲得或需要來自一銀行(一運輸交易之一非當事方)之資金支持。為使銀行借錢給代運人，銀行將實行其正常盡職調查以判定代運人是否係一可接受風險，及可能償還貸款給其之任何錢。對於

此實例，代運人可將一貸款申請3102提交給一銀行或其他借貸機構，如圖31中所展示。銀行經歷其自身之銀行活動3120，而代運人經歷其自身之代運人活動3118。在申請一貸款之程序中，代運人將要將各種文件及資料提供給銀行。此可被視為應用程式證實3104步驟。銀行然後經歷其自身之合規性檢查3106以判定代運人是否係一值得信任當事方，及一良好財務風險。若如此，則銀行可批准且發放貸款3110給代運人，且提供支付3108。

【0202】 代運人可經歷其活動且執行雇其進行之運輸事件3112，將運輸文件3114提供至感興趣之當事方，且然後為針對運輸事件簽訂合同之當事方開發票3116。然後，完成運輸事件，簽訂合同當事方可向代運人付費，且代運人可付還貸款。

【0203】 在其中代運人想要自一銀行設置一貸款帳戶之程序中，代運人可涉及輔助使用受信任儲存系統提供資料及文件化之驗證之系統。舉例而言，代運人3202可使用一安全通信3204系統與一銀行3206或其他金融機構通信以設置一帳戶3200，如圖32中所展示。代運人3202可經由安全通信3204將一貸款帳戶應用程式及其他支援文件發送至銀行。此等文件可包含關於過去運輸交易、安全記錄、支付歷史等等之歷史資料。可使用安全通信3204在代運人3202與銀行3206之間發送文件。安全通信可意味將訊息及附件加密。安全通信3204亦可涉及安全系統，如VPN、經編碼通信頻道等等。

【0204】 在此實例中，銀行3206可經由相同安全通信3204對代運人3202做出回應。在某些實施例中，可將通信加密。安全通信3204可含有歷史文件及一貸款申請(載入帳戶申請)。可將文件及帳戶應用程式加密，

如由鎖及金鑰所指示。在某些實施例中，加密機制在代運人與DCH之間可係不同的。其他當事方(諸如一承運人3208及一碼頭3212)亦可使用同一系統3210。在某些實施例中，承運人及碼頭可係運輸文件及運輸事件之源。由於運輸中可涉及代運人，因此代運人可獲得文件及事件且將該等文件及事件提供至銀行以用於貸款帳戶應用程式。

【0205】 可涉及系統3210之其他使用者以提供額外文件化。舉例而言，一承運人3208可驗證代運人3202實際上將要參與一運輸交易。承運人3208可提供關於將載運多少貨品及到達什麼目的地之此等細節。代運人3202可使用此資料來支援其需要多少錢來起始其貸款申請。

【0206】 銀行3206可請求文件之驗證且發送對系統3210之一查詢。該查詢可經加密且含有一雜湊。可識別該雜湊且比較該雜湊與用於產生該雜湊之原始資料。然後，若任何事物匹配，則系統3210可驗證由銀行3206發送之資料。

【0207】 在某些實施例中，在代運人已設置一貸款帳戶之後，代運人可將融資應用程式提交給銀行以借錢，銀行將實行其正常盡職調查以判定該應用程式是否係一可接受風險，及可能償還貸款給其之任何錢。對於此實例，代運人可將一貸款申請3304提交給一銀行或其他借貸機構，如圖33中所展示。代運人可收集來自承運人之預訂確認書文件及來自碼頭之運輸事件作為貸款申請3304之支援文件。運輸事件之完成、項目3300或貸款條件之實現可產生觸發貸款之付還之一事件。舉例而言，一碼頭3312中之一運輸或承運人車輛之到達以及運輸商品之後續卸載可觸發各種文件3314之發送。可將運輸事件報告給系統3310，然後系統可通知所有相關當事方。可將船舶已到達且已經卸載通知給承運人3308。可將貨

品已到達目的地港口且事件已觸發在一固定時間週期內向銀行支付貸款通知給代運人3302。銀行亦可接收在已完成運輸時代運人3302貸款現在到期之驗證。系統3310可具有建構至其中之各種觸發及警報，因此在一運輸之每一階段，其可接收關於運輸程序之更新，且將警報發送至其所有有關當事方。

【0208】 現在在圖34中展示一樣本發票3400。

【0209】 現在在圖35中展示一實例性支付3500。在此實例中，一代運人可自代運人可具有之諸多借貸機構選擇一或多個融資選項。交易可由系統處置，只要各個當事方能夠自系統接收資料且將資料傳輸至系統。

【0210】 在某些實施例中，當一貨櫃裝載於一碼頭上時，碼頭經營者可發出通知承運人追蹤運輸里程碑之一碼頭事件通知。碼頭事件通知含有碼頭之位置、事件類型、日期、時間、承運人及貨櫃號等。然後，承運人找到此貨櫃之相關當事方且透過經加密分散式分類帳通知當事方。

【0211】 一運輸文件之每一資料屬性之獨立加密之使用與加密欄位對加密金鑰之一對一關系組合會允許參與一共同企業之任一數目個業務(諸如聯運貨櫃或項目貨品之運輸)創建佈置一貨品預訂之所有態樣而不向參與預訂之任一其他當事方或在公眾面前大多數地洩露任何機密資訊的一單個運輸文件。

【0212】 在某些實施例中，當一貨櫃裝載於一碼頭上時，碼頭經營者可發出通知承運人追蹤運輸里程碑之一碼頭事件通知。該碼頭事件通知含有碼頭之位置、事件類型、日期、時間、承運人及貨櫃號等。然後，承運人找到此貨櫃之相關當事方且透過經加密分散式分類帳通知當事方。

【0213】 在某些實施例中，一承運人可在裝載一運輸時將發票發出

給一托運人及/或一收貨人。該托運人及/或收貨人然後可為發票付費。然後，承運人將一原始提單發出給托運人。收貨人可為貨物向托運人付費。然後，托運人可將原始提單傳遞給收貨人以獲得貨物。承運人可驗證收貨人是否為發票(若存在)付費，承運人驗證來自收貨人之原始提單及其他貨品放行程序。承運人可使用經加密分散式分類帳來將發票通知給托運人或收貨人且在托運人或收貨人已付款之後更新發票。

【0214】 現在提供非限制性態樣：

【0215】 1. 一種保護在一分佈式使用者群組中共用之一運輸文件之資料私密性之方法，該方法包括：

【0216】 經由一通信網路自一使用者接收該運輸文件，該使用者具有一所指派角色，其中高運輸文件包括複數個資料屬性；

【0217】 經由一第一加密邏輯將該複數個資料屬性加密成相似數目個經加密資料屬性，該第一加密邏輯產生對應於每一經加密資料屬性之一資料加密金鑰；

【0218】 經由一程式化邏輯將該複數個經加密資料屬性組織至一分散式資料分類帳中，該分散式資料分類帳含有來自一使用者之至少一個經加密運輸文件；

【0219】 經由一第二加密邏輯將對應於該複數個資料屬性之該等加密金鑰加密，該第二加密邏輯使用基於使用者之所指派角色而為該分散式資料分類帳之一或多個使用者提供權限的一查找表；

【0220】 及

【0221】 經由該通信網路將該分散式資料分類帳分佈至該分佈式使用者群組；

【0222】 其中每一使用者存取一節點，該節點提供對該分散式資料分類帳之存取；且

【0223】 其中每一使用者可僅將與其所指派角色有關之資料解密。

【0224】 2. 如態樣1之方法，其中使用一存取原則來判定用於寫入該經加密資料之複數個區塊鏈節點。

【0225】 3. 如態樣2之方法，其中該使用者所指派角色與一成員存取控制原則相關聯。

【0226】 4. 如態樣1之方法，其中該所指派角色進一步包括運輸方之間的一關係。

【0227】 5. 如態樣1之方法，其中該分散式資料分類帳含有來自一或多個使用者之複數個經加密運輸文件。

【0228】 6. 如態樣1之方法，其中由一使用者供應之該運輸文件包含該使用者之所指派角色。

【0229】 7. 如態樣1之方法，其中該第一或第二加密邏輯利用一不對稱密碼演算法。

【0230】 8. 如態樣1之方法，其中該通信網路進一步包括一安全網際網路存取。

【0231】 9. 一種用於向一運輸交易中之當事方提供關於交易進度之實時更新資訊之通信系統，該系統包括：

【0232】 一入口網站，其用以經由一安全網際網路存取來存取該系統；

【0233】 一資料庫，該資料庫儲存運輸交易(預訂)之系統組態資訊、公開金鑰及參考資訊；

【0234】 一分散式分類帳，該分散式分類帳具有用於一使用者之一節點，該分散式分類帳含有與相關於該運輸交易之該使用者有關之資料；及

【0235】 一程式，該程式協調欄位級別加密程序且將經加密結果分佈至該分散式分類帳；

【0236】 其中該使用者係該運輸交易之一當事方；且

【0237】 其中該入口網站、該資料庫及該分散式分類帳可透過一雲端計算環境存取。

【0238】 10. 如態樣9之通信系統，其中該入口網站係一用戶端應用程式。

【0239】 11. 如態樣9之通信系統，其中該分散式分類帳係一超級分類帳。

【0240】 現在參考圖36，繪示與不同用戶端終端機安全地共用來自多個源之資料之一方法3600之一流程圖。可使用本文中連同圖1至圖35或圖37所闡述之組件中之任一者實施或執行方法3600。在簡要概述中，方法3600可包含建立交易之一電子文件(3605)。方法3600可包含識別加密金鑰(3610)。方法3600可包含分佈加密金鑰(3615)。方法3600可包含提供存取(3620)。

【0241】 進一步詳細地，方法3600可包含建立交易之一電子文件(3605)。一伺服器(例如，一運輸文件控制中樞)可識別、創建或建立該電子文件(有時在本文中稱為一運輸文件)。該電子文件可定義、含有或包含透過多個用戶端終端機(或實體)進行之一單個交易之資訊。該單個交易可涉及一實體商品(例如，從一個點遞送到另一點)，且可包含與該實體商品

有關之一系列子交易。該實體商品之每一子交易可由至少一個服務提供者(例如，代理、中介機構)處置。該服務提供者可操作交易中所涉及之用戶端終端機中之至少一者或與交易中所涉及之用戶端終端機中之至少一者相關聯。服務提供者中之一者可係起始電子文件之建立之服務提供者，其中剩餘服務提供者在該建立之後存取及/或促成該電子文件(例如，更新該電子文件，或將資訊添加至該電子文件)。

【0242】 該電子文件可包含一組資料欄位。該電子文件之每一資料欄位可與涉及該實體商品之單個交易之子交易中之一者有關或映射至涉及該實體商品之單個交易之子交易中之一者。在該電子文件中，可給每一資料欄位指派一屬性或一值。該等資料欄位中之至少一者之該屬性可與單個交易中所涉及之用戶端終端機(例如，系統1300之使用者節點)中之一者相關聯(例如，由該等用戶端終端機中之一者提供/促成及/或更新)。該等資料欄位中之至少一者之該屬性可來自由起始或創建該電子文件之一第一實體或第一服務提供者操作之用戶端終端機及/或由該用戶端終端機更新。該等資料欄位可包含闡述交易之參數，諸如貨櫃大小、事件日期、著陸港口、貨品說明、毛重、船舶名稱及貸款帳戶以及其他。在某些實施例中，該電子文件可維持於一資料庫(例如，文件控制中樞3002)上。該資料庫可經維持或屬一運輸文件控制中樞以用於在該等用戶端終端機當中協調通信。維持於該資料庫上之該電子文件之每一資料欄位可對應於該資料庫上之一資料庫項目。

【0243】 在某些實施例中，在建立該電子文件中，該伺服器可接收設定、指派或以其他方式更新該電子文件中之一資料欄位之一屬性的一請求。該請求可繼由該第一實體進行之初始建立之後來自與促成該電子文件

之該服務提供者相關聯之該等用戶端終端機中之一者。與該請求相關聯之該服務提供者可關於該第一實體或者促成該電子文件之該等資料欄位或為該電子文件之該等資料欄位提供屬性之其他服務提供者中之任一者缺乏任何(或具有有限的)瞭解或互動。以此方式，可使用來自各種實體之資訊以一特定方式填充該電子文件之該等資料欄位。可在單個交易(例如，之子交易或部分)中引入或涉及某些或所有服務提供者，此按一特定方式(例如，視需要或者接近於產生一服務提供者在交易中之作用之時間或在該時間處)而非預定的(例如，在建立電子文件時)。交易之每一部分或子交易可由複數個可用服務提供者中之一者填充或服務，此可隨著交易發展及/或在產生需要/作用/子交易時經動態地匹配、填充及/或選擇。除作用/服務及/或一服務提供者直接與之介接以執行該服務提供者在交易中之作用/服務的(若干)服務提供者以外，該服務提供者可不具有對交易之瞭解(或具有對交易之有限瞭解)。請求可識別待更新之電子文件中之資料欄位及待設定至資料欄位之新屬性。伺服器可根據針對用戶端終端機之一角色之一存取控制原則判定用戶端終端機是否有權限修改資料欄位。該存取控制原則可規定交易中所涉及之用戶端終端機(或對應角色)有權限存取或修改哪些資料欄位。為了判定是否存在權限，用戶端終端機可識別用戶端終端機在交易中之一角色。該角色可依據交易中所涉及之子交易系列之一角色清單來識別。

【0244】 當未針對用戶端終端機識別角色(或經授權/有效角色)時，伺服器可判定用戶端終端機缺乏修改資料欄位之權限，且可維持資料欄位中之屬性。否則，當識別角色時，伺服器可識別角色之存取控制原則。伺服器可基於針對用戶端終端機所識別之角色之存取控制原則而判定用戶端

終端機是否具有權限。當存取控制原則規定用戶端終端機(或角色)缺乏權限時，伺服器可判定用戶端終端機缺乏權限。伺服器亦可阻止提交請求之用戶端終端機更新電子文件中之資料欄位之屬性。相反地，當存取控制原則規定用戶端終端機(或角色)具有權限時，伺服器可判定用戶端終端機具有存取權限。伺服器可准許用戶端終端機更新電子文件中之資料欄位之屬性。在某些實施例中，伺服器可依據請求識別屬性且將屬性指派給資料欄位。

【0245】 方法3600可包含識別加密金鑰(3610)。每一加密金鑰可用於將該電子文件中之一對應資料欄位加密。每一加密金鑰亦可與將屬性提供至電子文件中之對應資料欄位之用戶端終端機中之一者相關聯。該等加密金鑰可由伺服器或對應用戶端終端機產生。加密金鑰可根據不對稱密碼學(諸如公開金鑰密碼學、Diffie-Hellman金鑰交換、橢圓曲線函數及一RSA密碼系統以及其他)來產生。在某些實施例中，所識別之加密金鑰可包含用於對應用戶端終端機之一組私密加密金鑰及一組公開加密金鑰。每一私密加密金鑰可對應於資料欄位中之一者且可與將屬性提供至資料欄位之用戶端終端機中之一者相關聯。每一公開加密金鑰可對應於資料欄位中之一者且可與將屬性提供至資料欄位之用戶端終端機中之一者相關聯。在某些實施例中，伺服器可自單個交易中所涉及之用戶端終端機擷取、收集或聚合加密金鑰(例如，公開加密金鑰)。由伺服器聚合之每一加密金鑰可由將屬性提供至電子文件中之資料欄位之用戶端終端機中之一者產生。在某些實施例中，可針對使用來自用戶端終端機中之一者之屬性更新之一資料欄位而識別一新加密金鑰。

【0246】 方法3600可包含分佈加密金鑰(3615)。伺服器可根據存取

控制原則針對電子文件跨越單個交易中所涉及之用戶端終端機提供、遞送、分佈加密金鑰。存取控制原則可針對用戶端終端機(或對應角色)規定對電子文件中之每一資料欄位之存取權限(例如，解密、打開、寫入或編輯)。存取控制原則可基於個別用戶端終端機之一角色而規定存取權限。對於電子文件中之資料欄位中之每一者，存取控制原則可指示至少兩個用戶端終端機(或對應角色)存取資料欄位。

【0247】 在分佈中，伺服器可將一對應私密加密金鑰提供至單個交易中所涉及之用戶端終端機中之每一者。該私密加密金鑰可用於將由對應用戶端終端機提供之資料欄位加密或解密。在某些實施例中，伺服器可基於各別角色根據存取控制原則來識別單個交易中所涉及之兩個或兩個以上用戶端終端機。舉例而言，與一第一用戶端終端機相關聯之一第一角色及與一第二用戶端終端機相關聯之一第二角色可由存取控制原則規定為具有對電子文件中之資料欄位中之一者之存取。伺服器可使用第二用戶端終端機之另一加密金鑰(例如，公開加密金鑰)將第一用戶端終端機之一加密金鑰(例如，私密加密金鑰)加密。在加密時，伺服器可將第一用戶端終端機之加密金鑰提供至第二用戶端終端機。

【0248】 另外，伺服器可根據存取控制原則將一公開加密金鑰提供至用戶端終端機中之一或多者。舉例而言，存取控制原則可針對資料欄位中之一者規定：兩個用戶端終端機有權限存取資料欄位中之屬性。在此實例中，伺服器可將公開加密金鑰提供至兩個用戶端終端機。以此方式，電子文件中之資料欄位中之每一者可由用戶端終端機中之一或多者使用提供至用戶端終端機之私密加密金鑰或公開加密金鑰來存取。

【0249】 在某些實施例中，伺服器可判定加密金鑰跨越用戶端終端

機之一分佈是否係成功的。伺服器可基於該判定而將一訊息(例如，一事件通知)傳輸、發送或提供至用戶端終端機中之一或多者。當判定為分佈係成功的時，伺服器可將一成功碼發佈或提供至用戶端終端機(諸如發送更新電子文件中之資料欄位中之一者之請求之用戶端終端機)中之一或多者。相反地，當判定為分佈係不成功的時，伺服器可將一錯誤碼發佈或提供至用戶端終端機中之一或多者。

【0250】 在某些實施例中，伺服器可識別自電子文件中之資料欄位中之一者中之一對應屬性導出之一雜湊值。可使用一雜湊函數(諸如一循環冗餘檢查、一總和檢查碼、一密碼雜湊函數及一訊息鑑認碼以及其他)產生該雜湊值。可由將屬性提供至電子文件中之資料欄位之用戶端終端機產生該雜湊值。該雜湊值可係用以確保指派給電子文件中之資料欄位之屬性之資料完整性。伺服器亦可根據存取控制原則跨越用戶端終端機分佈雜湊值。

【0251】 在某些實施例中，伺服器可針對單個交易中所涉及之用戶端終端機中之每一用戶端終端機接收或識別一簽章。可藉由將對應於用戶端終端機之加密金鑰施加至自由用戶端終端機提供之資料欄位之屬性導出之雜湊值而產生該簽章。可由伺服器或提供屬性之用戶端終端機產生該簽章。該簽章可係用以確保電子文件中之資料欄位中之屬性之資料完整性。

【0252】 方法3600可包含提供存取(3620)。伺服器可使用根據存取控制原則分佈之加密金鑰將對電子文件中之資料欄位中之一或多者之存取提供至每一用戶端終端機。在某些實施例中，伺服器可輸入、提供、產生及/或維持資料欄位或電子文件之屬性。在某些實施例中，伺服器可接收使用來自用戶端終端機中之一者之一識別符(例如，一運輸文件識別符或

預訂號、承運人組織)存取電子文件之一或多個資料欄位之一請求。伺服器可判定由識別符引用之電子文件是否存在於資料庫上。當判定不存在電子文件時，伺服器可傳回一錯誤訊息。相反地，當判定存在電子文件時，伺服器可繼續驗證用戶端終端機是否存取資料欄位。每一用戶端終端機可能夠使用提供至用戶端終端機之一對應加密金鑰存取用戶端終端機將屬性提供至之資料欄位。另外，每一用戶端終端機可能夠使用提供至用戶端終端機之一對應加密金鑰存取資料欄位，如由存取控制原則所規定。

【0253】 在某些實施例中，伺服器可向基於角色根據存取控制原則而識別之兩個或兩個以上用戶端終端機提供對電子文件中之資料欄位中之一者之存取。可已向所識別用戶端中之每一者提供電子文件中之資料欄位之雜湊值及簽章。可自資料欄位中之屬性導出雜湊值且可使用提供屬性之用戶端終端機之雜湊值及加密金鑰(例如，該公開加密金鑰)產生簽章。經由雜湊值及簽章，其他用戶端終端機可獲得加密金鑰以存取資料欄位中之屬性。其他用戶端終端機可依據經加密屬性計算雜湊值，且使用雜湊值將簽章解密以獲得經解密雜湊值。用戶端終端機然後可比較經解密雜湊值與雜湊值以判定完整性。當雜湊值匹配時，用戶端終端機可判定屬性具有資料完整性。否則，當雜湊值不匹配時，用戶端終端機可判定屬性缺乏資料完整性。

【0254】 現在參考圖37，電腦3700可包含一或多個處理器3705、揮發性記憶體3710 (例如，隨機存取記憶體(RAM))、非揮發性記憶體3720 (例如，一或多個硬碟機(HDD)或其他磁性或光學儲存媒體、一或多個固態磁碟機(SSD) (諸如一快閃磁碟機或其他固態儲存媒體)、一或多個混合磁性與固態磁碟機及/或一或多個虛擬儲存容量(諸如一雲端儲存裝置)或此

等實體儲存容量與虛擬儲存容量或其陣列之一組合)、使用者介面(UI) 3725、一或多個通信介面3715及通信匯流排3730。使用者介面3725可包含圖形使用者介面(GUI) 3750 (例如，一觸控螢幕、一顯示器等)及一或多個輸入/輸出(I/O)裝置3755 (例如，一滑鼠、一鍵盤、一麥克風、一或多個揚聲器、一或多個相機、一或多個生物掃描機、一或多個環境感測器、一或多個加速度計等)。非揮發性記憶體3720儲存作業系統3735、一或多個應用程式3740及資料3745，使得(舉例而言)作業系統3735及/或應用程式3740之電腦指令由在揮發性記憶體3710以外之處理器3705執行。在某些實施例中，揮發性記憶體3710可包含一或多個類型之RAM及/或可提供比一主記憶體快之一回應時間的一快取記憶體。可使用GUI 3750之一輸入裝置輸入資料或自I/O裝置3755接收資料。電腦3700之各種元件可經由經展示為通信匯流排3730之一或多個通信匯流排通信。

【0255】 如圖37中所展示之電腦3700經展示(僅僅作為一實例)為用戶端、伺服器、中介結構及其他網路化裝置，且可由任何計算或處理環境且藉助可具有能夠如本文中所闡述而操作之適合硬體及/或軟體之任何類型之機器或機器集來實施。處理器3705可由一或多個可程式化處理器實施以執行一或多個可執行指令，諸如一電腦程式，以執行系統之功能。如本文中所使用，術語「處理器」闡述執行一功能、一操作或一操作序列之電路系統。該功能、操作或操作序列可硬編碼至該電路系統中或藉助於保存於一記憶體裝置中且由該電路系統執行之指令經軟編碼。一「處理器」可使用數位值及/或使用類比信號執行該功能、操作或操作序列。在某些實施例中，該「處理器」可體現於一或多個特殊應用積體電路(ASIC)、微處理器、數位信號處理器(DSP)、圖形處理單元(GPU)、微控制器、場

可程式化閘陣列(FPGA)、可程式化邏輯陣列(PLA)、多核心處理器或具有相關聯記憶體之一般用途電腦中。該「處理器」可係類比、數位或混合信號。在某些實施例中，該「處理器」可係一或多個實體處理器或一或多個「虛擬」(例如，遠端地定位或「雲端」)處理器。包含多個處理器核心之一處理器及/或多個處理器可提供用於一個以上資料件上之若干指令之並行同時執行或用於一個以上資料件上之一個指令之並行同時執行的功能性。

【0256】 通信介面3715可包含一或多個介面以使得電腦3700能夠透過各種有線及/或無線或蜂巢式連接存取一電腦網路，諸如一區域網(LAN)、一廣域網(WAN)、一個人區域網(PAN)或網際網路。

【0257】 本說明書中所闡述之標的物及操作之實施例可實施於數位電子電路中或電腦軟體、韌體或硬體(包含本說明書中所揭示之結構及其結構等效物)中或者其等各項中之一或多者之組合中。亦可將本說明書中所闡述之標的物之實施例實施為一或多個電腦程式，亦即，編碼於一或多個電腦儲存媒體上以供資料處理設備(諸如一處理電路)執行或用以控制資料處理設備之操作之一或多個電腦程式指令模組。一控制器或處理電路(諸如CPU)可包括經組態以執行本文中所闡述之功能之任何數位及/或類比電路組件，諸如一微處理器、微控制器、特殊應用積體電路、可程式化邏輯等。另一選擇係或另外，程式指令可編碼於一人工產生之傳播信號(例如，一機器產生之電、光學或電磁信號)上，該人工產生之傳播信號經產生以編碼用於傳輸至適合接收器設備以供一資料處理設備執行之資訊。

【0258】 一電腦儲存媒體可係以下各項或包含於以下各項中：一電腦可讀儲存裝置、一電腦可讀儲存基板、一隨機或串列存取記憶體陣列或

裝置或者其等各項中之一或多者之一組合。此外，雖然一電腦儲存媒體並非一傳播信號，但一電腦儲存媒體可係編碼於一人工產生之傳播信號中之電腦程式指令之一源或目的地。該電腦儲存媒體亦可係一或多個單獨組件或媒體(例如，多個CD、磁碟或其他儲存裝置)，或包含於一或多個單獨組件或媒體中。因此，該電腦儲存媒體既係有形的又係非暫時性的。

【0259】 本說明書中所闡述之操作可實施為由一資料處理設備對儲存於一或多個電腦可讀儲存裝置上或自其他源接收之資料執行之操作。術語「資料處理設備」或「計算裝置」囊括用於處理資料之所有種類之設備、裝置及機器，藉由實例方式包含一可程式化處理器、一電腦、一系統單芯片或者前述各項中之多者或組合。該設備可包含特殊用途邏輯電路系統，例如，一FPGA (場可程式化閘陣列)或一ASIC (特殊應用積體電路)。除硬體以外，該設備亦可包含為所討論之電腦程式創建一執行環境的程式碼，例如，構成處理器韌體、一協定堆棧、一資料庫管理系統、一作業系統、一跨平台運行時環境、一虛擬機器或其等各項中之一或多者之一組合的程式碼。該設備及執行環境可實現各種不同計算模型基礎設施，諸如web服務、分佈式計算及網格計算基礎設施。

【0260】 可以包含編譯語言或解譯語言、宣告式或程序性語言之任何形式之程式設計語言來撰寫一電腦程式(亦稱為一程式、軟體、軟體應用程式、描述性語言或程式碼)，且可將該電腦程式部署成任何形式，包含部署為一獨立程式或部署為一模組、組件、子常式、物件或適合在一計算環境中使用之其他單元。一電腦程式可但不需要對應於一檔案系統中之一檔案。一程式可儲存於保存其他程式或資料(例如，儲存於一標記語言文件中之一或多個描述性語言)之一檔案之一部分中、儲存於專用於所討

論之程式之一單個檔案中或儲存於多個經協調檔案(例如，儲存一或多個模組、子程式或程式碼之若干部分之文檔)中。一電腦程式可經部署以在一個電腦上或在多個電腦(其位於一個位點處或跨越多個位點分佈且藉由一通信網路互連)上執行。

【0261】 本說明書中所闡述之程序及邏輯流程可由執行一或多個電腦程式之一或多個可程式化處理器執行以藉由對輸入資料進行操作並產生輸出來執行動作。該等程序及邏輯流程亦可由特殊用途邏輯電路系統(例如，一FPGA(場可程式化閘陣列)或一ASIC(特殊應用積體電路))來執行，且亦可將設備實施為該專用邏輯電路系統。

【0262】 舉例而言，適於執行一電腦程式之處理器藉由實例方式包含一般用途微處理器及特殊用途微處理器兩者，以及任一種類之數位電腦之任何一或多個處理器。一般而言，一處理器將自一唯讀記憶體或一隨機存取記憶體或兩者接收指令及資料。一電腦之基本元件係用於根據指令執行動作之一處理器及用於儲存指令及資料之一或多個記憶體裝置。一般而言，一電腦亦將包含用於儲存資料之一或多個大容量儲存裝置(例如，磁碟、磁光碟或光碟)或以操作方式耦合以自該一或多個大容量儲存裝置接收資料或向其傳送資料或既接收又傳送資料。然而，一電腦不必具有此類裝置。此外，一電腦可嵌入於另一裝置中，例如，一行動電話、一個人數位助理(PDA)、一行動音訊或視訊播放器、一遊戲控制台、一全球定位系統(GPS)接收器或一可攜式儲存裝置(例如，一通用串列匯流排(USB)快閃磁碟機) (僅舉幾個例子)。適合於儲存電腦程式指令及資料之裝置包含所有形式之非揮發性記憶體、媒體及記憶體裝置，以實例方式包含：半導體記憶體裝置(例如，EPROM、EEPROM及快閃記憶體裝置)；磁碟(例如，

內部硬碟或可抽換磁碟)；磁光碟；以及CDROM及DVD-ROM碟。該處理器及該記憶體可由特殊用途邏輯電路系統補充或併入於特殊用途邏輯電路系統中。

【0263】 為提供與一使用者之互動，本說明書中所闡述之標的物之實施例可實施於一電腦上，該電腦具有：一顯示裝置，例如，一CRT (陰極射線管)或LCD (液晶顯示器)監視器、OLED (有機發光二極體)監視器或用於向使用者顯示資訊之其他形式之顯示器；及一鍵盤；及/或一指向裝置，例如，一滑鼠或一軌跡球，使用者可藉由該指向裝置將輸入提供至該電腦。亦可使用其他種類之裝置來提供與一使用者之互動；舉例而言，提供給該使用者之回饋可係任何形式之感觀回饋，例如，視覺回饋、聽覺回饋或觸覺回饋；且來自該使用者之輸入可以任何形式來接收，包含聲音、語音或觸覺輸入。另外，一電腦可藉由向由該使用者使用之一裝置發送文件及自該裝置接收文件而與一使用者交互；舉例而言，藉由回應於自一使用者之用戶端裝置上之一web瀏覽器接收之請求而向該web瀏覽器發送網頁。

【0264】 雖然此說明書含有諸多特定實施例細節，但此等細節不應解釋為對任何實施例或可主張之內容之範疇之限制，而是應解釋為特定實施例特有之特徵之說明。在單獨實施例之內容脈絡中於本說明書中闡述之特定特徵亦可以組合方式實施於一單個實施例中。相反地，在一單個實施例之內容脈絡中闡述之各種特徵亦可單獨地或以任何適合子組合形式實施於多個實施例中。此外，儘管上文可將特徵闡述為以特定組合形式起作用且甚至最初係如此主張的，但在某些情形中，可自一所主張組合去除來自該組合之一或多個特徵，且所主張組合可針對一子組合或一子組合之變化

形式。

【0265】 類似地，雖然在該等圖式中以一特定次序繪示操作，但不應將此理解為需要以所展示之特定次序或以順序次序執行此等操作或執行所有所圖解說明之操作以達成合意結果。在特定情形中，多任務及並行處理可係有利的。此外，不應將在上文所闡述之實施例中之各種系統組件之分離理解為在所有實施例中需要此分離，且應理解，一般可將所闡述程式組件及系統一起整合於一單個軟體產品中或封裝至多個軟體產品中。

【0266】 對「或」之提及可解釋為包含性的，使得使用「或」所闡述之任何術語可指示一單個、一個以上及所有所闡述術語中之任一者。

【0267】 因此，已闡述標的物之特定實施例。在所附申請專利範圍之範疇內存在其他實施例。在某些情形中，申請專利範圍中所陳述之動作可以一不同次序執行且仍達成合意結果。另外，附圖中所繪示之程序未必需要所展示之特定次序或順序次序來實現合意結果。在特定實施例中，多任務及並行處理可係有利的。

【0268】 已闡述方法及系統之特定實施例，現在熟習此項技術者將明瞭，可使用併入有概念之其他實施例。應理解，上文所闡述之系統可提供彼等組件中之任何者或每一者之多者，且此等組件可設置於一單獨機械上或在某些實施例中設置於一分佈式系統中之多個機器上。上文所闡述之系統及方法可使用程式化及/或工程設計技術實施為一方法、設備或製件以產生軟體、韌體、硬體或其任何組合。另外，上文所闡述之系統及方法可經提供為體現於一或多個製件上或中之一或多個電腦可讀程式。如本文中所使用之術語「製件」意欲囊括可自以下各項存取且嵌入於以下各項中之程式碼或邏輯：一或多個電腦可讀裝置、韌體、可程式化邏輯、記憶體

裝置(例如，EEPROM、ROM、PROM、RAM、SRAM等)、硬體(例如，積體電路晶片、場可程式化閘陣列(FPGA)、特殊應用積體電路(ASIC)等)、電子裝置、一電腦可讀非揮發性儲存單元(例如，CD-ROM、軟碟、硬碟機等)。可自一檔案伺服器存取製件，該檔案伺服器經由一網路傳輸線、無線傳輸媒體、透過空間傳播之信號、無線電波、紅外線信號等提供對電腦可讀程式之存取。製件可係一快閃記憶體卡或一磁帶。製件包含硬體邏輯以及嵌入於一電腦可讀媒體中之由一處理器執行之軟體或可程式化碼。一般而言，電腦可讀程式可以任何程式化語言(諸如LISP、PERL、C、C++、C#、PROLOG)或以任何位元組碼語言(諸如JAVA)來實施。軟體程式可作為物件程式碼儲存於一或多個製件上或中。

【符號說明】

【0269】

102:托運人

104:代運人

106:承運人

108:碼頭

110:海關

112:港務局

114:收貨人

116:金融機構

200:運輸路線

202:托運人

204:港務局

206:船舶經營者

208:最終收貨人

300:金鑰保存庫程序

302:開始

304:步驟

306:步驟

308:步驟

310:步驟

312:結束

400:金鑰位置

402:公開金鑰

404:私密金鑰

406:經加密資料加密金鑰

408:經解密資料加密金鑰/資料加密金鑰

410:安全網路連接

412:安全網路連接

500:鑑認程序

502:用戶端應用程式/使用者之用戶端應用程式

504:安全網路連接

506:授權權杖產生器/權杖產生器

508:預訂應用程式設計介面

600:應用程式設計介面

602:用戶端應用程式

604:應用程式設計介面管理工具

606:區塊鏈應用程式設計介面

608:驗證請求

610:權杖

612:預訂請求有效負載/有效負載

614: 將組織識別碼及有效負載請求發送至區塊鏈應用程式設計介面

616:用戶鑑認

618:提供權杖鑑認

700:應用程式設計介面管理程序

702:開始方塊

706:步驟

708:步驟

710:步驟

712:步驟

714:步驟

716:結束

718:步驟

800:運輸文件資料分佈

802:開始方塊

804:步驟

806:步驟

808:步驟

810:步驟

812:結束方塊

900:運輸文件創建模型/獲得預訂程序

902:開始

904:步驟

906:步驟

908:步驟

910:步驟

912:步驟

914:步驟

916:步驟

918:步驟

920:結束

1000:樣本預訂訂單

1100:擷取運輸文件/擷取預訂程序

1102:開始方塊

1104:屬性驗證

1106:自運輸文件資料庫獲得預訂資訊且將經加密預訂資訊解密

1108:確保恰當地擷取所要預訂且將所要預訂解密

1110:運輸角色檢查

1112:過濾屬性

1114:成功

1116:錯誤回應

1118:結束

1200:創建運輸文件

1202:開始方塊

1204:檢查屬性驗證

1206:藉由定位子金鑰找到預訂之一角色清單

1208:檢查是否可定義預訂之存取原則

1210:收集運輸方之運輸角色

1212:檢查所收集運輸角色是否具有存取權以創建預訂資料之所有所提交屬性

1214:產生預訂之一唯一預訂識別碼

1216:針對每一資料屬性產生個別資料加密金鑰

1218:將每一資料屬性加密

1220:擷取每一運輸角色之存取控制原則

1222:自公開金鑰儲存庫擷取公開金鑰

1224:以運輸方之公開金鑰將對應資料加密金鑰一個接一個地加密

1226:將經加密資料及經加密資料加密金鑰分佈至恰當組織

1228:驗證成功地將資料及金鑰分佈至相關運輸方之所有分類帳

1230:將分類帳之名稱、唯一預訂ID及預訂版本號保存於運輸文件資料庫中

1232:產生一成功回應碼

1234:傳回一錯誤

1236:結束

1300:系統

1302:運輸文件控制中樞

1304:脫鏈資料庫

1306a:第一使用者節點/使用者節點

1306b:使用者節點

1306n:使用者節點

1308a-1308n: 用戶端應用程式

1310a-1310n:用戶端應用程式資料庫

1312a-1312n:金鑰儲存區

1314a-1314n:密碼存取層

1316a-1316n:應用程式設計介面/區塊鏈應用程式設計介面

1318a-1318n: 網路通信/網路連接

1320a-1320n:區塊鏈邏輯

1322a-1322n:區塊鏈節點

1400:存取原則

1500:程序

1502:開始方塊

1504:步驟

1506:步驟

1508: 步驟

1510:步驟

1512:步驟

1514:結束

1600:角色與存取控制原則

1602:資料與金鑰結構

1604:樣本存取控制原則/收貨人之存取控制原則

1606:藉助一資料加密金鑰將每一資料屬性個別地加密

1608:資料加密金鑰之公開金鑰加密

1700:組件關係實例/實施例

1702:存取原則/運輸文件存取原則

1704:角色清單存取原則

1706:唯一識別碼/運輸文件

1708:定位子金鑰

1710:角色清單

1712:定位子金鑰

1714:文件類型

1716:事件類型

1718:運輸角色清單

1720:貨櫃角色清單

1800:角色清單與存取控制原則

1802:角色清單存取原則定位子金鑰

1804:角色清單存取原則實例

1806:角色屬性層級實例

1808:角色清單定位子金鑰

1810:角色清單內容

1900:運輸文件/運輸文件與存取控制原則

1902:貨櫃出境事件/出境實例/出境事件實例

1904:角色清單定位子金鑰

1906:運輸文件存取原則/運輸文件層級原則實例

1908:運輸文件架構實例/實例/架構實例

1910:出境事件欄位層級之運輸文件存取原則/運輸文件原則欄位層級實例/欄位層級實例

2000:實例性運輸文件原則

2002:危險品憑證實例

2004:角色清單定位子金鑰

2006:文件層級存取原則

2008:欄位層級存取原則/欄位層級

2010:危險品憑證架構實例

2100:邏輯系統佈局/系統佈局

2102:運輸文件控制中樞

2104:第一使用者節點/用戶端節點/使用者節點

2106:文件控制中樞側訊息代理者/訊息代理者

2108:事件訊息

2110:事件訊息

2112:存取原則

2114:公開金鑰儲存庫

2116:識別碼儲存庫

2118:用戶端節點/使用者節點

2124:使用者訊息代理者

2126:使用者訊息代理者

2200:樣本流程圖/角色清單提交詳細流程

2202:初始檢查屬性驗證

2206:角色檢查

2208:定義角色清單存取原則

2210:存取權檢查

2212:傳回一錯誤回應碼

2214:產生加密金鑰

2216:將角色清單加密

2218:藉由發送者之私密金鑰簽署雜湊從而產生發送者之簽章

2220:獲得公開金鑰

2222:將資料加密金鑰加密

2223:將訊息發送至運輸文件控制中樞

2224:分佈資料及加密金鑰

2226:檢查分佈成功

2228:將具有一錯誤碼之事件發佈至訊息代理者

2232:發佈具有可去往用戶端側訊息代理者之一成功碼的事件

2234:結束

2300:角色清單讀取詳細流程/用於讀取一運輸文件之一程序

2302:檢查屬性驗證

2304:獲得經加密角色清單及經加密資料加密金鑰

2310:檢查角色清單之相關性

2312:存取金鑰儲存區

2314:將資料加密金鑰解密

2316:傳回一錯誤回應碼

2318:將角色清單解密

2320:傳回一成功回應碼

2322:結束方塊

2402:檢查屬性驗證

2404:檢查是否可存在來自存取原則儲存庫之一現有角色清單

2406:運輸角色檢查

2408:查看是否可在運輸文件層級及運輸文件欄位層級處定義存取原則

2410:存取權檢查

2412:產生遍及整個系統可係唯一之一唯一運輸文件識別碼

2414:產生資料加密金鑰

2416:將資料屬性加密

2418:產生關於經加密資料屬性之一雜湊且存取金鑰儲存區以藉由發送者之私密金鑰簽署雜湊從而產生發送者之簽章

2420:獲得公開金鑰

2422:將資料加密金鑰加密

2424:將具有經加密資料屬性、經加密資料加密金鑰、雜湊及發送者之簽章之訊息打包

2426:將訊息發送至運輸文件控制中樞

2428:藉由使每一使用者節點以一成功通知做出回應而查看分佈是否係成功的

2430:接收具有經加密運輸文件、經加密DEK、雜湊及發送者之簽章之一發佈事件

2432:將一成功事件通知發佈給發送者

2436:檢查完整性

2438:將經加密資料加密金鑰解密

2440:將運輸文件解密

2442:用戶端應用程式可以純文字形式接收運輸文件

2448:結束方塊

2502:開始方塊

2504:檢查屬性

2506:檢查一現有運輸文件

2508:找到現有角色清單

2510:角色檢查

2512:是否定義存取原則

2514:存取權檢查

2516:合併現有運輸文件屬性與所提交資料屬性之經加密資料(若可用)

2518:使運輸文件之版本號增加一

2520:產生資料加密金鑰

2522:所提交運輸文件中之新資料屬性

2524:將運輸文件中之所提交資料屬性加密

2526:產生關於任何新加密之資料屬性(資料欄位)之一雜湊且存取金鑰儲存區以藉由發送者之私密金鑰簽署雜湊來產生發送者之簽章

2528:獲得角色清單中之當事方之公開金鑰

2530:將經更新資料加密金鑰加密

2532:將具有經加密資料屬性、經加密資料加密金鑰、雜湊及發送者之簽章之訊息打包

2534:將經加密運輸文件、經加密資料加密金鑰、雜湊及發送者之簽章金鑰分佈至恰當區塊鏈分類帳

2536:執行是否成功地分佈經加密運輸文件、經加密資料加密金鑰、雜湊及發送者之簽章之一檢查

2538:將具有一經加密運輸文件、經加密資料加密金鑰及發送者之簽章之一事件發佈至既定接收方

2540:檢查完整性

2542:將資料加密金鑰解密

2544:將運輸文件解密

2546:以純文字形式接收運輸文件

2548:將錯誤回應碼傳回至接收方

2550:在一成功碼發送至發送者之訊息代理者之情況下執行具有至發送者之成功碼之一發佈事件

2554:將具有要發送之一錯誤碼之一事件發佈至發送者之訊息代理者

2556:結束方塊

2600:用於讀取一運輸文件之一實例性程序

2602:開始方塊

2604:對照一交易參考資料庫檢查該運輸文件版本號

2606:屬性驗證

2608:獲得經加密運輸文件及經加密資料加密金鑰

2610:檢查相關性

2612:存取金鑰儲存區

2614:取回資料加密金鑰

2616:錯誤

2618:將經加密運輸文件解密

2620:將一成功回應碼傳回至用戶端應用程式

2622:結束

2700:預訂配置

2702:預訂版本號

2800:局部預訂視圖

2900:可能活動

2902:所註冊使用者/使用者

2904:第三方

2906:文件控制中樞

2908:使用者節點

2910:第三方節點

3002:文件控制中樞

3004a:運輸文件資料庫

3004b: 存取原則儲存庫

3004c:公開金鑰儲存庫

3004d:身份儲存庫

3004n:資料庫

3006a:接收方庫加密

3006b:接收方庫加密

3006n:接收方庫加密

3010:文件控制中樞託管之驗證功能/驗證功能

3020:安全通信鏈路

3022:使用者

3024:使用者控制之資料封裝/資料封裝

3026:資料加密金鑰/經加密資料加密金鑰/經解密資料加密金鑰

3028:使用者私密金鑰

3060:第三方

3062:第三方受控制資料封裝/第三方資料封裝/資料封裝

3064:單獨安全通信鏈路

3102:貸款申請

3104:應用程式證實

3106:合規性檢查

3108:支付

3110:批准且發放貸款

3112:運輸事件

3114:運輸文件

3116:開發票

3118:代運人經歷其自身之代運人活動

3120:銀行經歷其自身之銀行活動

3200:帳戶

3202:代運人

3204:安全通信

3206:銀行

3208:承運人

3210:系統

3212:碼頭

3300:項目

3302:代運人

3304:貸款申請

3308:承運人

3310:系統

3312:碼頭

3314:文件

3400:樣本發票

3500:實例性支付

3600:方法

3605:步驟

3610:步驟

3615:步驟

3620:步驟

3700:電腦

3705:處理器

3710:揮發性記憶體

3715:通信介面

3720:非揮發性記憶體

3725:使用者介面

3730:通信匯流排

3735:作業系統

3740:應用程式

3745:資料

3750:圖形使用者介面

3755:輸入/輸出裝置

【發明申請專利範圍】

【請求項1】

一種產生用於存取複數個資料屬性(attribute)之金鑰之方法，該複數個資料屬性具有不同所有者以作為一零信任通信系統之部分，其中該複數個資料屬性係維持於一伺服器上之貨物之一共用運輸文件之部分，該方法包括：

藉由至少一處理器產生用於該複數個資料屬性之一資料屬性之一資料加密金鑰；

藉由該至少一處理器自一記憶體擷取(retrieve)用於一運輸方之一運輸角色；

藉由該至少一處理器自該記憶體擷取對應於該運輸角色之一存取控制原則；

使用該存取控制原則擷取用於該運輸方之一或多個公開金鑰；及

藉由該至少一處理器使用該運輸方之該一或多個公開金鑰加密該資料加密金鑰以建立用於該複數個資料屬性之該資料屬性之一經加密資料加密金鑰。

【請求項2】

如請求項1之方法，其中該運輸方具有兩個或兩個以上運輸角色。

【請求項3】

如請求項1之方法，其中該存取控制原則定義該運輸方存取該複數個資料屬性之何者。

【請求項4】

如請求項1之方法，其中該公開金鑰係擷取自一公開金鑰儲存庫

(repository)。

【請求項5】

如請求項1之方法，其中存取控制原則包含關於各運輸方能夠存取之該複數個資料屬性之何者之資訊。

【請求項6】

如請求項1之方法，其中該共用運輸文件係一電子文件。

【請求項7】

如請求項1之方法，其中該共用運輸文件係一預訂(booking)。

【請求項8】

如請求項1之方法，其中該存取控制原則係動態可更新。

【請求項9】

如請求項1之方法，其進一步包括：

根據該運輸方之該運輸角色分佈該經加密資料加密金鑰及該資料屬性之一經加密版本至該運輸方。

【請求項10】

如請求項1之方法，其中該運輸方進一步包括對貨物之該共用運輸文件感興趣之一政府機關、一金融機構或貿易組織。

【請求項11】

一種與不同用戶端終端機安全地共用來自多個源之資料之方法，該方法包括：

藉由具有一或多個處理器之至少一伺服器建立定義用於複數個運輸方之複數個資料屬性之一運輸文件，該運輸文件具有複數個資料欄位，該複數個資料欄位之各者相關於各對應於該複數個運輸方之一者之複數個用

戶端終端機之一者；

藉由該至少一伺服器識別至少一加密金鑰以自包含於該運輸文件中之該複數個資料欄位加密該至少一資料欄位以形成一經加密資料欄位；

藉由該至少一伺服器根據一存取控制原則分佈該至少一加密金鑰至該複數個客戶端終端機之至少一者，該存取控制原則根據該運輸文件中之一對應運輸方之一運輸角色規定用於該複數個用戶端終端機之一對應用戶端終端機對該複數個資料欄位中之一或多者之存取權限；及

藉由該至少一伺服器根據該存取控制原則隨著該至少一加密金鑰分佈該運輸文件中之該經加密資料欄位至該複數個用戶端終端機之至少一者。

【請求項12】

如請求項11之方法，其中建立該運輸文件進一步包括：

自該複數個用戶端終端機之一第一用戶端終端機接收一請求以更新該運輸文件中之該複數個資料欄位之一第一資料欄位之一屬性；

根據該存取控制原則基於該預訂中之該第一用戶端終端機之一角色判定該第一用戶端終端機具有修改該第一資料欄位之權限；及

回應於判定該第一用戶端終端機具有該權限而准許該用戶端終端機更新該共用運輸文件中之該第一資料欄位之該屬性。

【請求項13】

如請求項11之方法，其中識別該至少一加密金鑰進一步包括針對該複數個用戶端終端機識別一私密加密金鑰及一公開加密金鑰；及

其中分佈該加密金鑰進一步包括：

提供該私密加密金鑰至該複數個用戶端終端機之一對應用戶端終

端機；及

根據該存取原則提供該公開加密金鑰至該複數個用戶端終端機之至少一者，該電子文件中之該複數個資料欄位之至少一者可藉由該複數個用戶端終端機之至少兩者使用該私密金鑰及該公開金鑰存取。

【請求項14】

如請求項11之方法，其進一步包括：

藉由該至少一伺服器識別自該電子文件之該複數個資料欄位中之對應複數個屬性導出之複數個雜湊值(hash values)，該複數個雜湊值中之各雜湊值確保該複數個屬性中之一者之資料完整性；及

藉由該至少一個伺服器針對該複數個用戶端終端機中之一第一用戶端終端機使用該複數個雜湊值中之一第一雜湊值及該複數個加密金鑰中之一第一加密金鑰產生一第一簽章，該第一雜湊值係自該複數個屬性中之一第一屬性導出，其中該第一加密金鑰係針對該複數個資料欄位中對應於該第一屬性之一第一資料欄位，該第一簽章確保該第一屬性及該第一資料欄位之資料完整性。

【請求項15】

如請求項11之方法，其進一步包括：

藉由該至少一個伺服器判定該複數個加密金鑰之至少一者及該等經加密資料欄位之至少一者跨越該複數個用戶端終端機之分佈是否成功；及

藉由該至少一個伺服器基於該加密金鑰及該經加密資料欄位之分佈是否成功之一判定來將一事件通知提供至該複數個用戶端終端機中之至少一者。

【請求項16】

如請求項11之方法，其中貨物之該運輸係一聯運貨櫃(intermodal container)。

【請求項17】

一種用於與不同用戶端終端機安全地共用來自多個源之資料之系統，其包括：

至少一伺服器，其具有一或多個處理器經組態以：

建立用於定義針對貨物之一運輸之至少一參數之一共用運輸文件，該共用運輸文件包括針對複數個運輸方之一系列資料輸入(entry)，該共用運輸文件具有複數個資料欄位，該複數個資料欄位之各者相關於各對應於該複數個運輸方之一者之複數個用戶端終端機之一者；

識別複數個加密金鑰以加密包含於該共用運輸文件中之該對應複數個資料欄位；

根據一存取控制原則跨越該複數個用戶端終端機分佈該複數個加密金鑰，該存取控制原則根據該預訂中之一對應運輸方之一運輸角色規定用於該複數個用戶端終端機之一對應用戶端終端機對該複數個資料欄位中之一或多者之存取權限；及

經由根據該存取控制原則分佈之該複數個加密金鑰提供該複數個用戶端終端機之各者至該電子文件中之該複數個資料欄位之至少一者之存取。

【請求項18】

如請求項17之　　系統，其中該至少一伺服器進一步經組態以：

自該複數個用戶端終端機之一第一用戶端終端機接收一請求以更新

該共用運輸文件中之該複數個資料欄位之一第一資料欄位之一屬性；

根據該存取控制原則基於該單獨預訂中之該第一用戶端終端機之一角色判定該第一用戶端終端機具有修改該第一資料欄位之權限；及

回應於判定該第一用戶端終端機具有該權限而准許該用戶端終端機更新該電子文件中之該第一資料欄位之該屬性。

【請求項19】

如請求項17之　　系統，其中該至少一伺服器進一步經組態以：

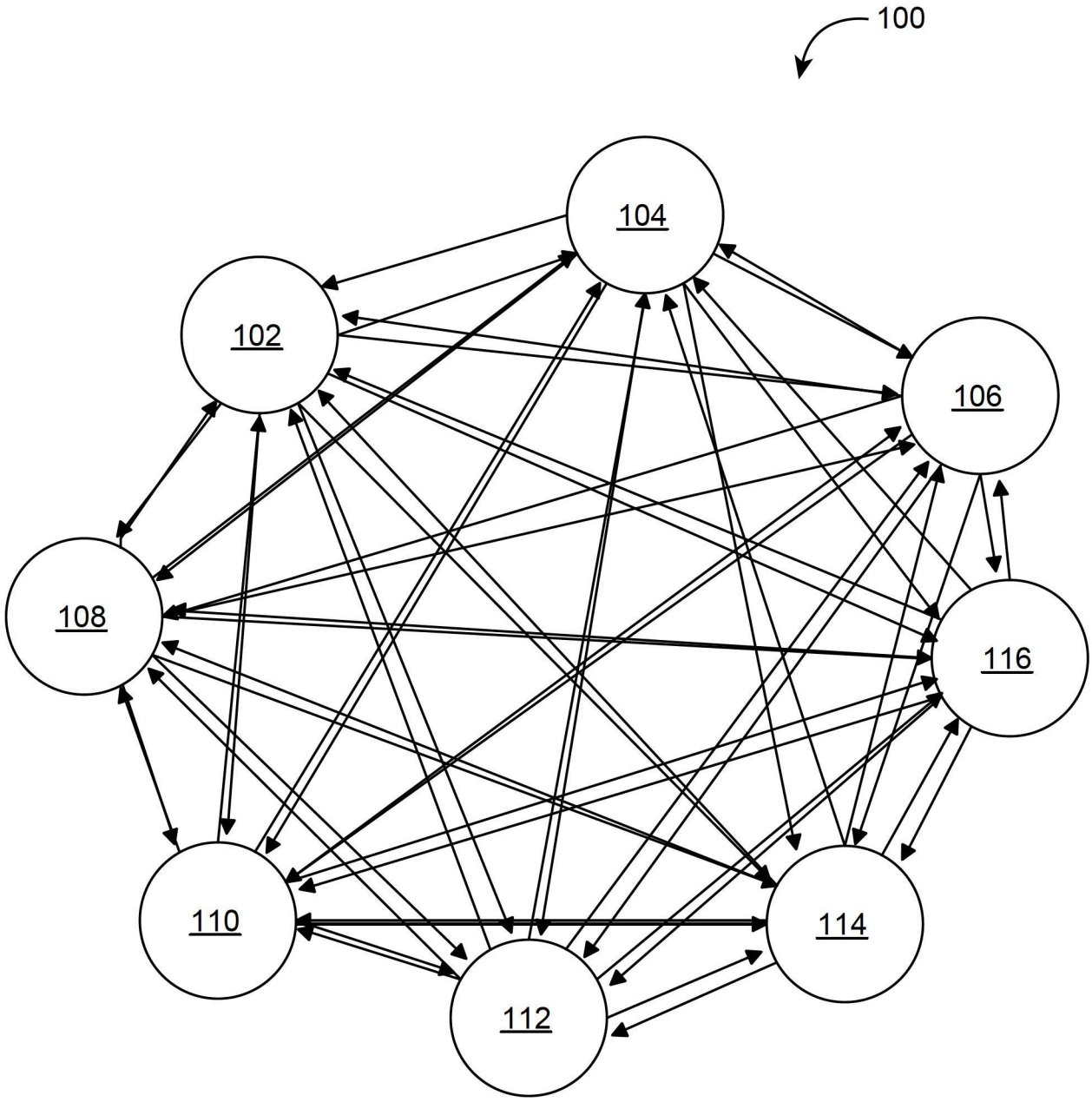
識別自該共用運輸文件之該複數個資料欄位中之對應複數個屬性導出之複數個雜湊值，該複數個雜湊值中之各雜湊值確保該複數個屬性中之一者之資料完整性；及

針對該複數個用戶端終端機中之一第一用戶端終端機使用該複數個雜湊值中之一第一雜湊值及該複數個加密金鑰中之一第一加密金鑰產生一第一簽章，該第一雜湊值係自該複數個屬性中之一第一屬性導出，其中該第一加密金鑰係針對該複數個資料欄位中對應於該第一屬性之一第一資料欄位，該第一簽章確保該第一屬性及該第一資料欄位之資料完整性。

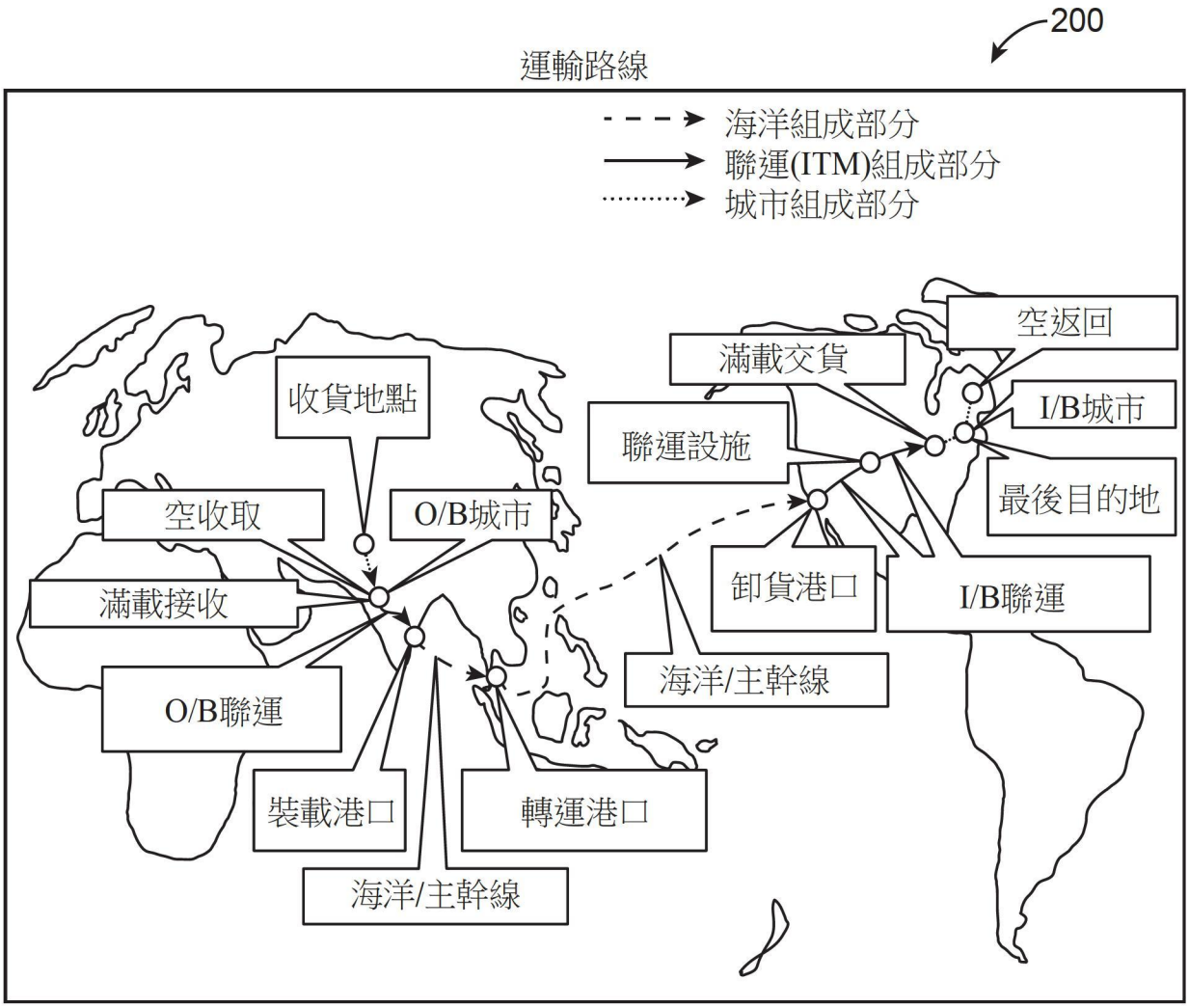
【請求項20】

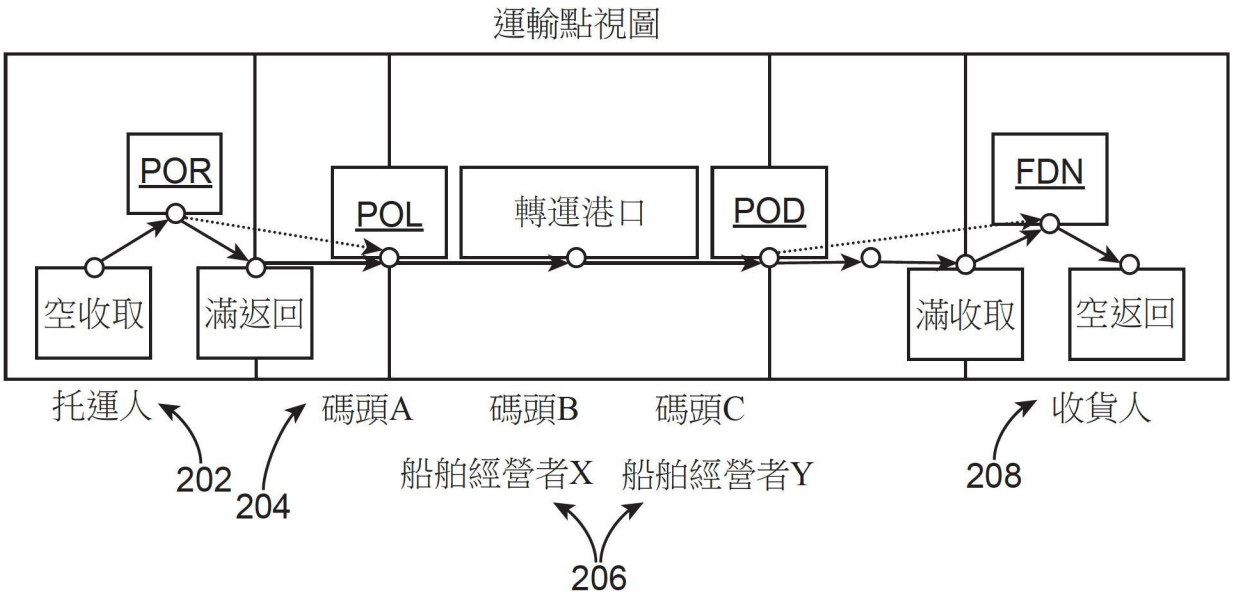
如請求項17之　　系統，其中貨物之該運輸係一聯運貨櫃。

【發明圖式】

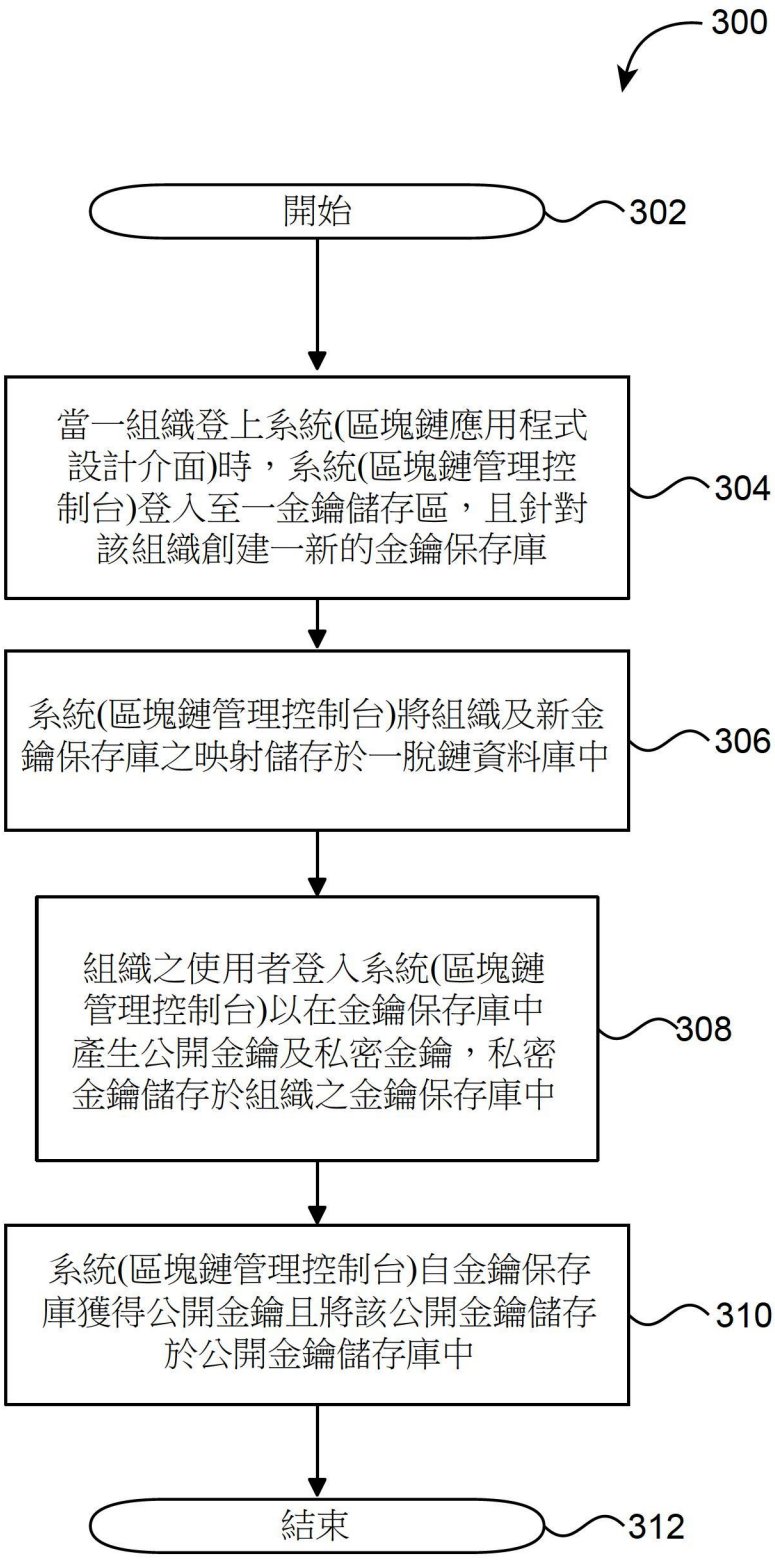


【圖1】

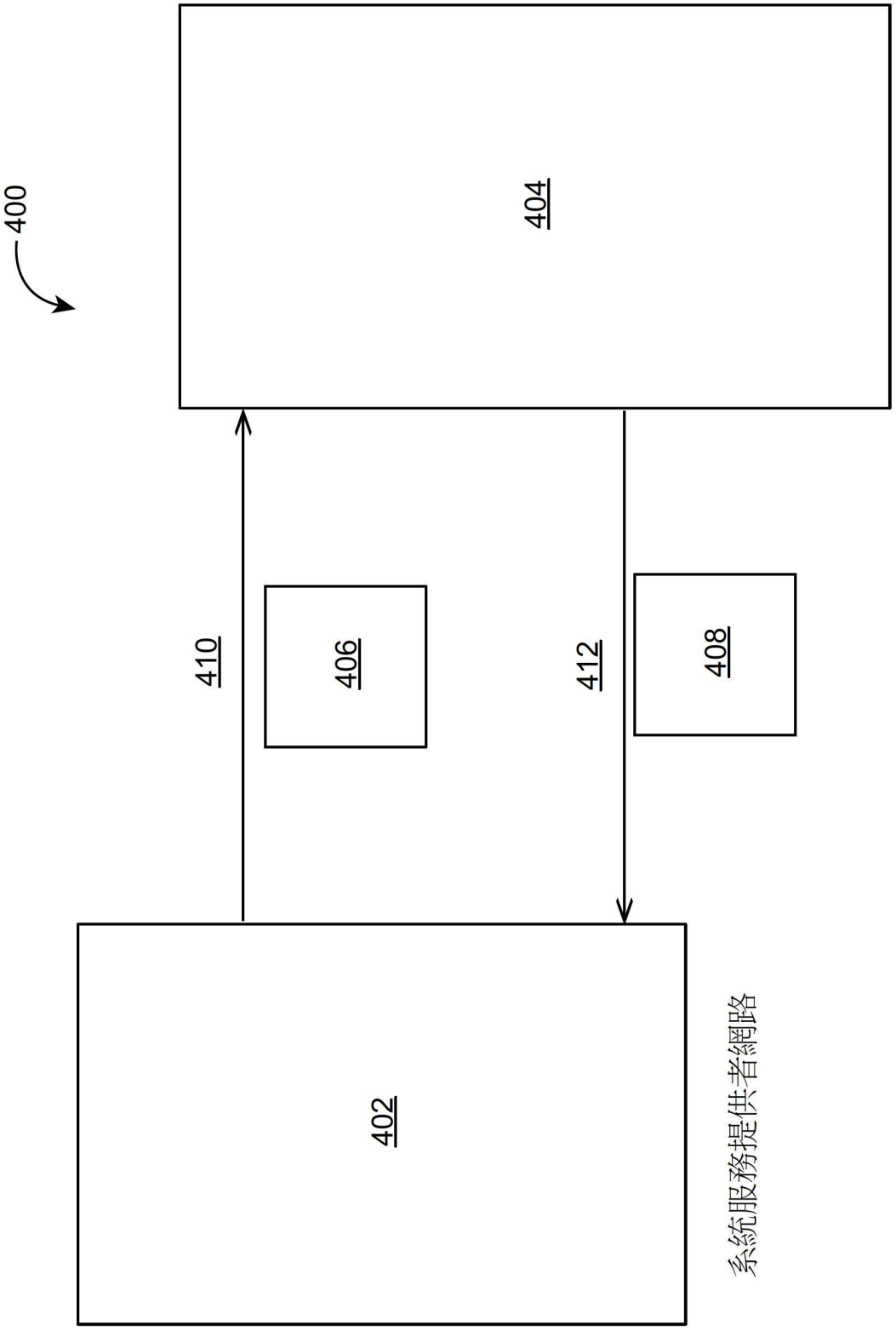

200
運輸路線
海洋組成部分
聯運(ITM)組成部分
城市組成部分
收貨地點
空收取
O/B城市
滿載接收
O/B聯運
裝載港口
轉運港口
海洋/主幹線
滿載交貨
空返回
I/B城市
聯運設施
最後目的地
卸貨港口
I/B聯運
海洋/主幹線


運輸點視圖
POR
POL
轉運港口
POD
FDN
空收取
滿返回
滿收取
空返回
托運人
碼頭A
碼頭B
碼頭C
收貨人
202
204
船舶經營者X
船舶經營者Y
206
208

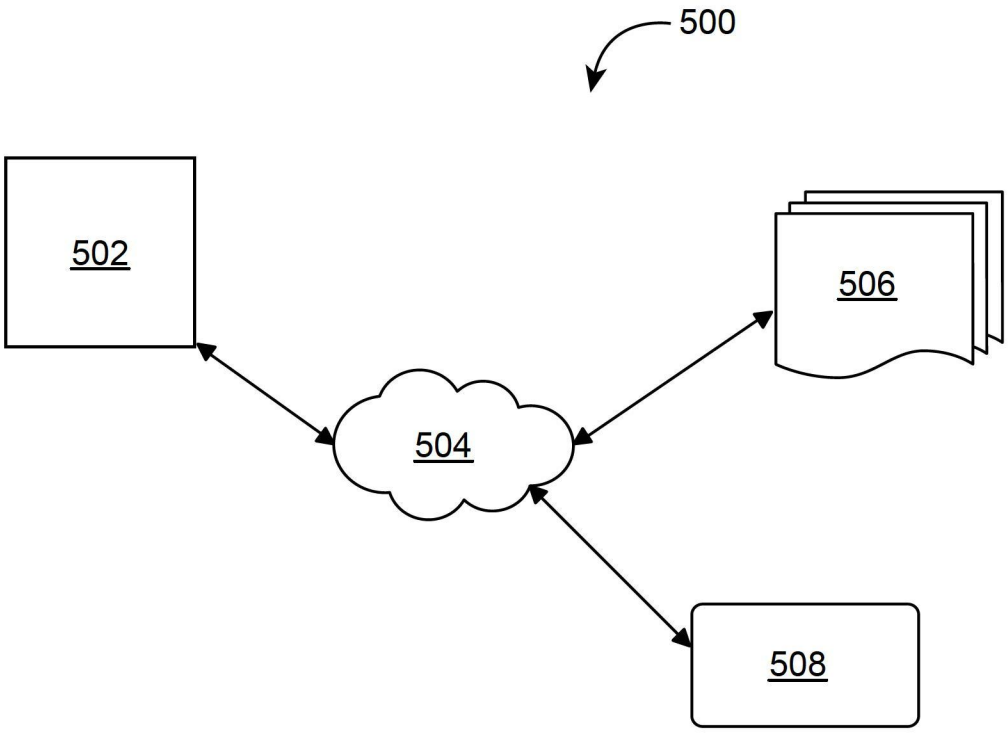
【圖2】


300
開始
302
當一組織登上系統(區塊鏈應用程式設計介面)時，系統(區塊鏈管理控制台)登入至一金鑰儲存區，且針對該組織創建一新的金鑰保存庫
304
系統(區塊鏈管理控制台)將組織及新金鑰保存庫之映射儲存於一脫鏈資料庫中
306
組織之使用者登入系統(區塊鏈管理控制台)以在金鑰保存庫中產生公開金鑰及私密金鑰，私密金鑰儲存於組織之金鑰保存庫中
308
系統(區塊鏈管理控制台)自金鑰保存庫獲得公開金鑰且將該公開金鑰儲存於公開金鑰儲存庫中
310
結束
312

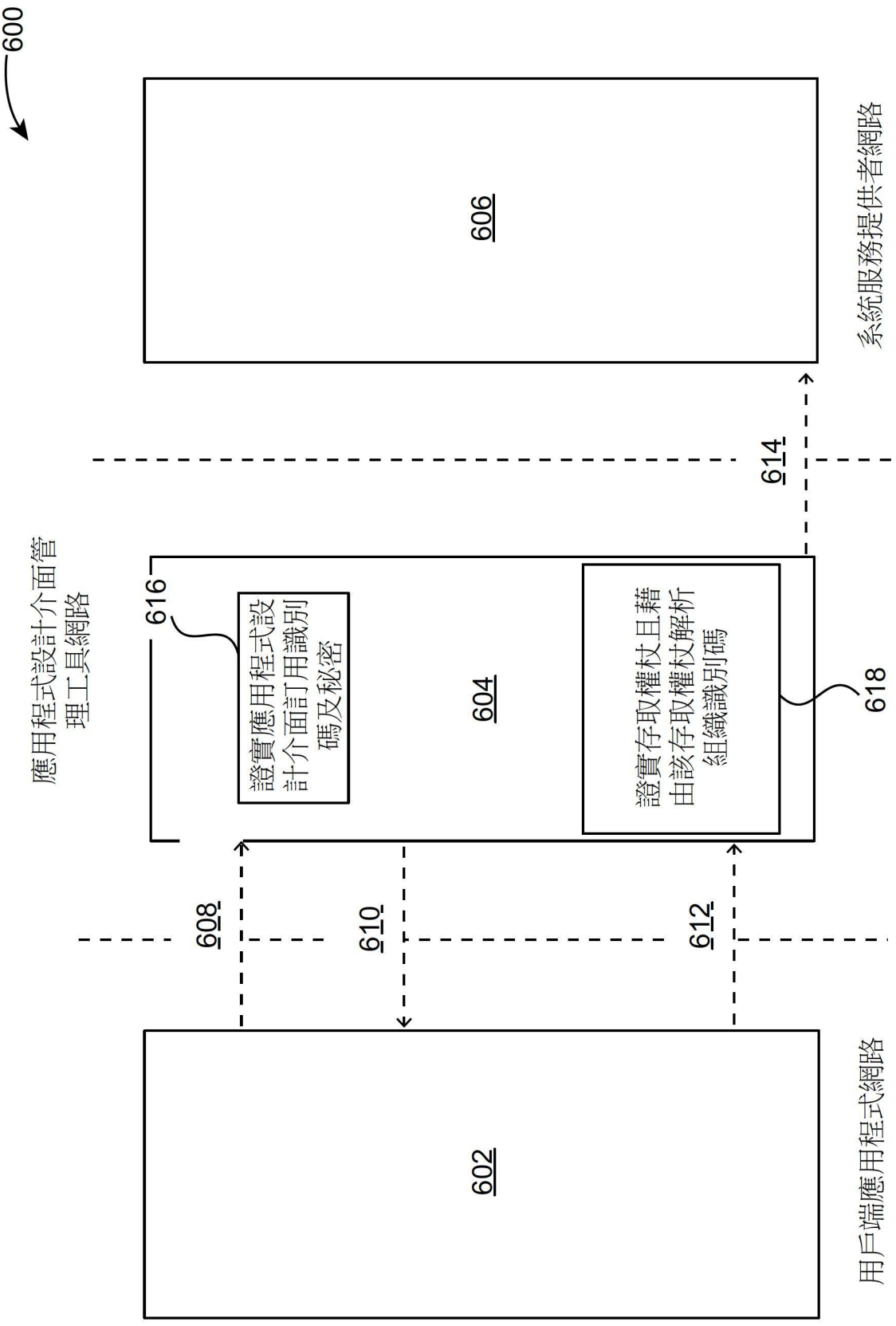
【圖3】



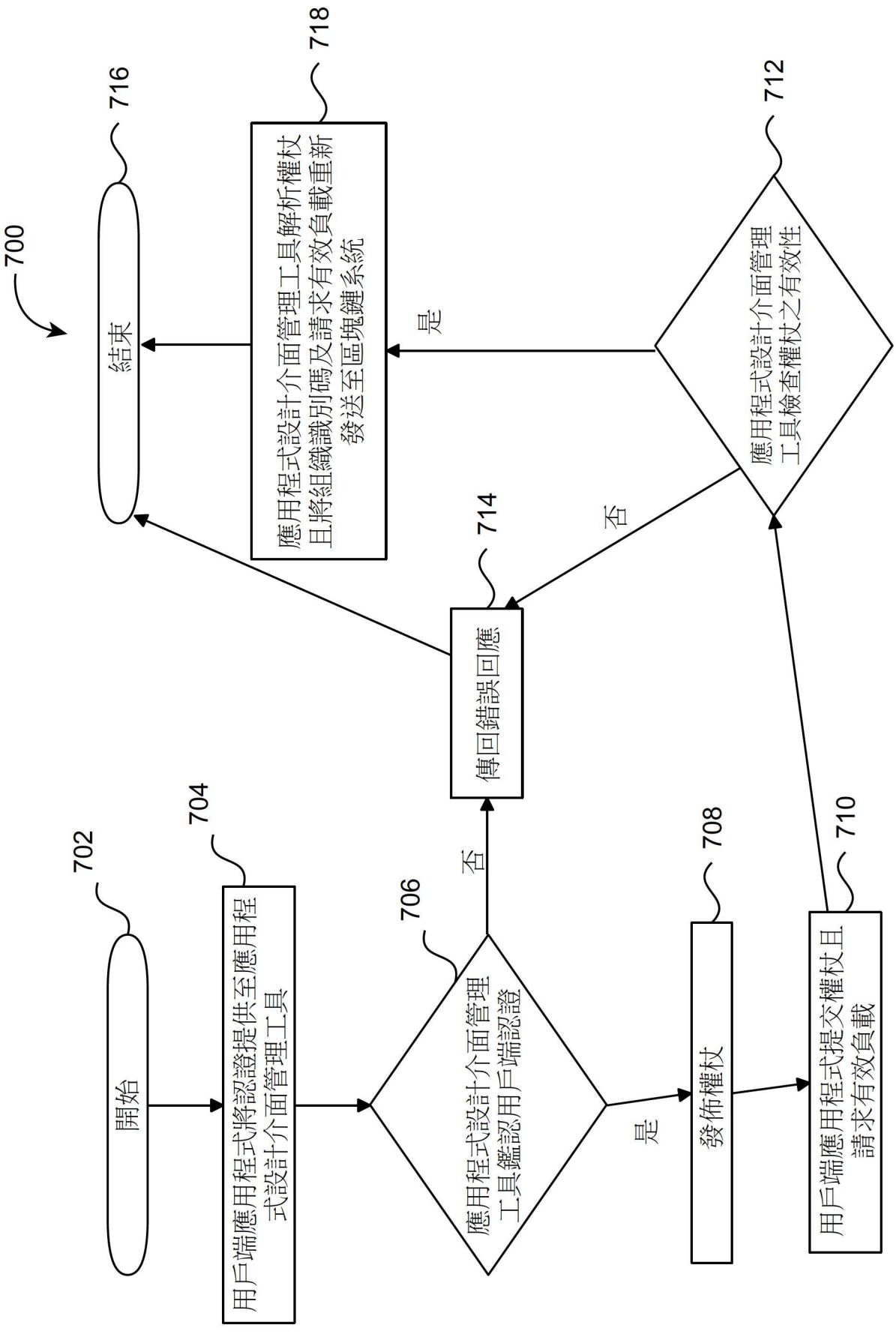
【圖4】



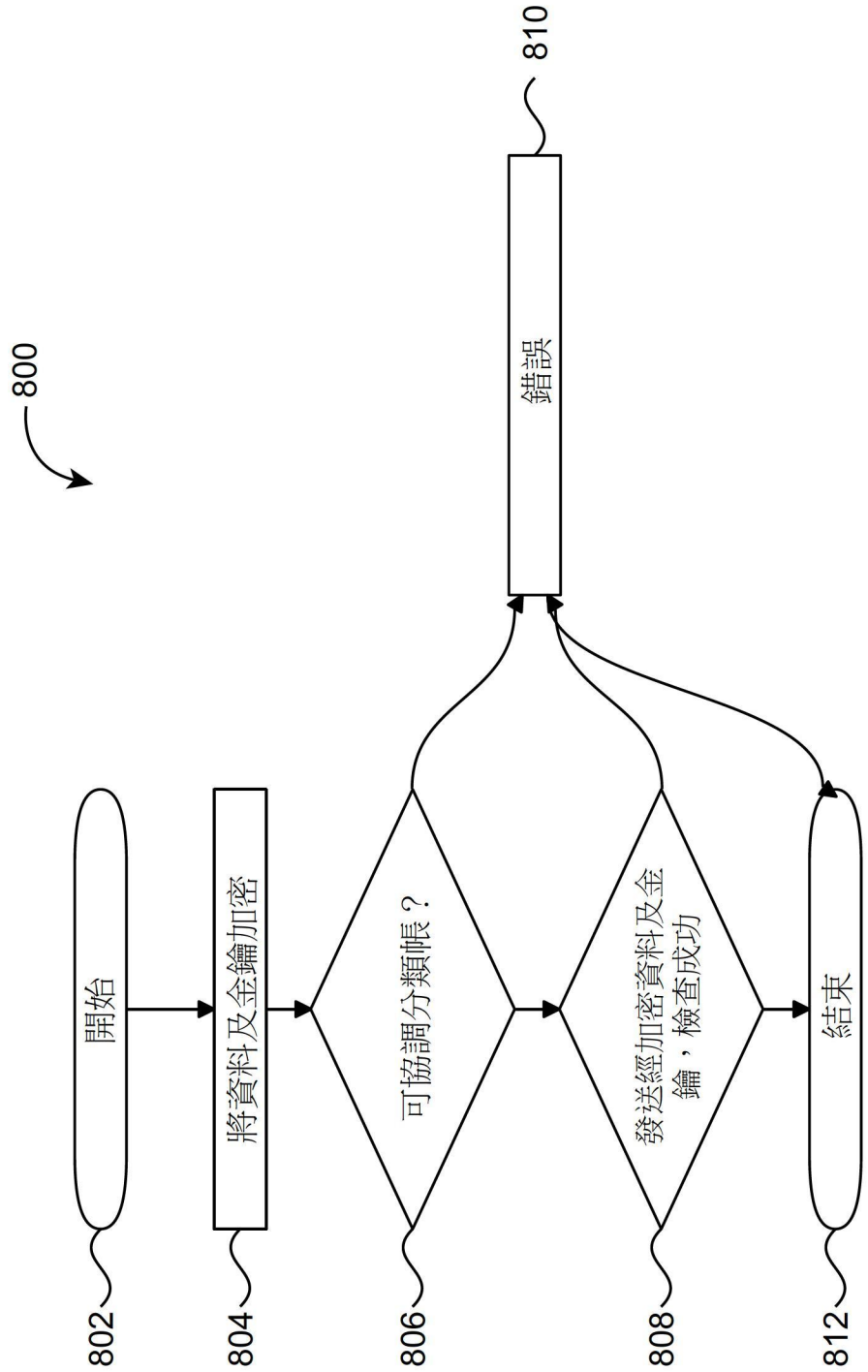
【圖5】


600
606
系統服務提供者網路
614
應用程式設計介面管理工具網路
616
證實應用程式設計介面訂用識別碼及秘密
604
證實存取權杖且藉由該存取權杖解析組織識別碼
618
608
610
612
602
用戶端應用程式網路

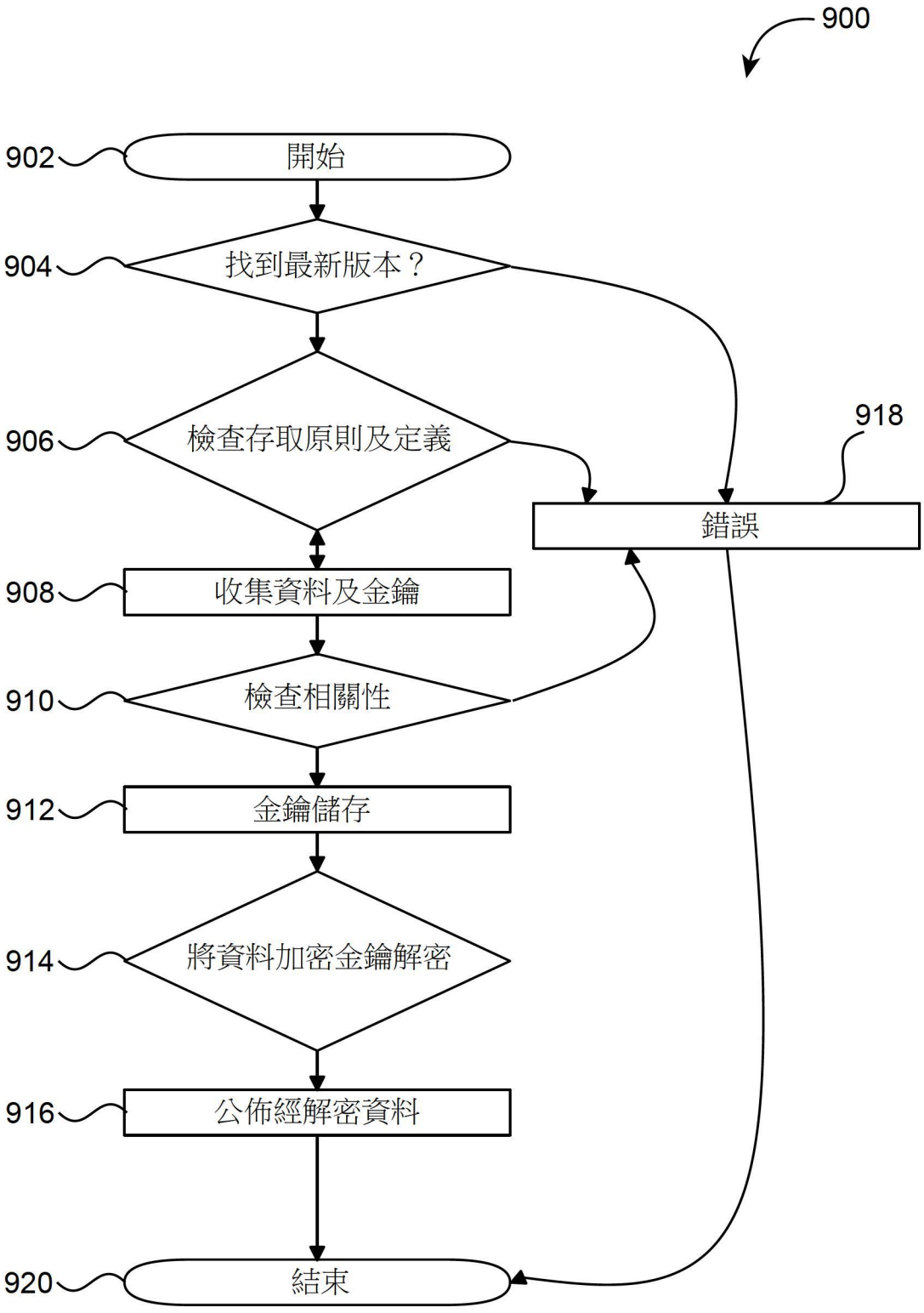
【圖6】


700
開始
702
用戶端應用程式將認證提供至應用程式設計介面管理工具
704
應用程式設計介面管理工具鑑認用戶端認證
706
否
傳回錯誤回應
714
是
發佈權杖
708
用戶端應用程式提交權杖且請求有效負載
710
應用程式設計介面管理工具檢查權杖之有效性
712
否
是
應用程式設計介面管理工具解析權杖且將組織識別碼及請求有效負載重新發送至區塊鏈系統
718
結束
716

【圖7】


800
開始
802
將資料及金鑰加密
804
可協調分類帳？
806
發送經加密資料及金鑰，檢查成功
808
結束
812
錯誤
810

【圖8】


900
902
開始
904
找到最新版本？
906
檢查存取原則及定義
908
收集資料及金鑰
910
檢查相關性
912
金鑰儲存
914
將資料加密金鑰解密
916
公佈經解密資料
918
錯誤
920
結束

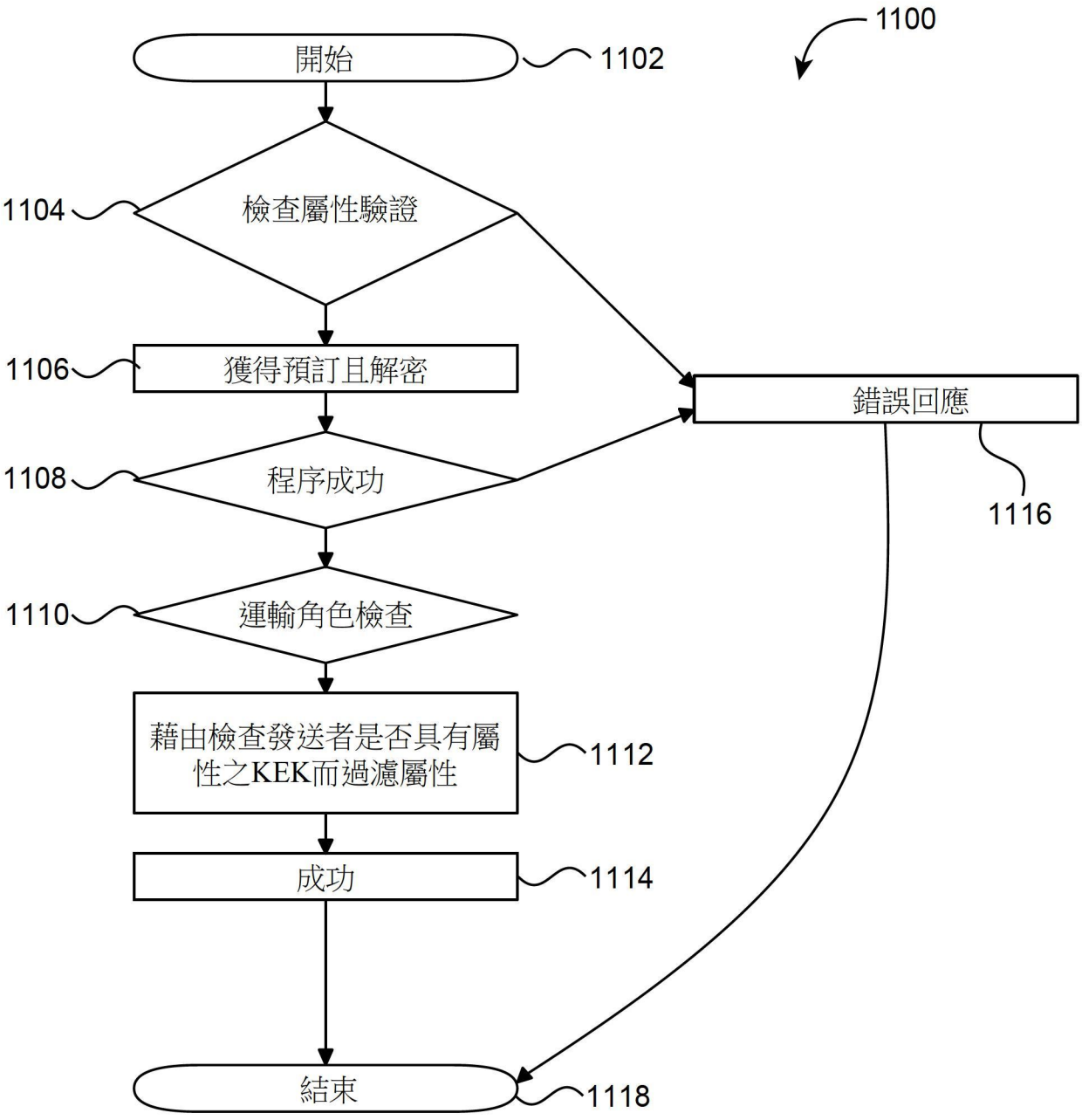
【圖9】

ms [37]　無未決行動項(4)

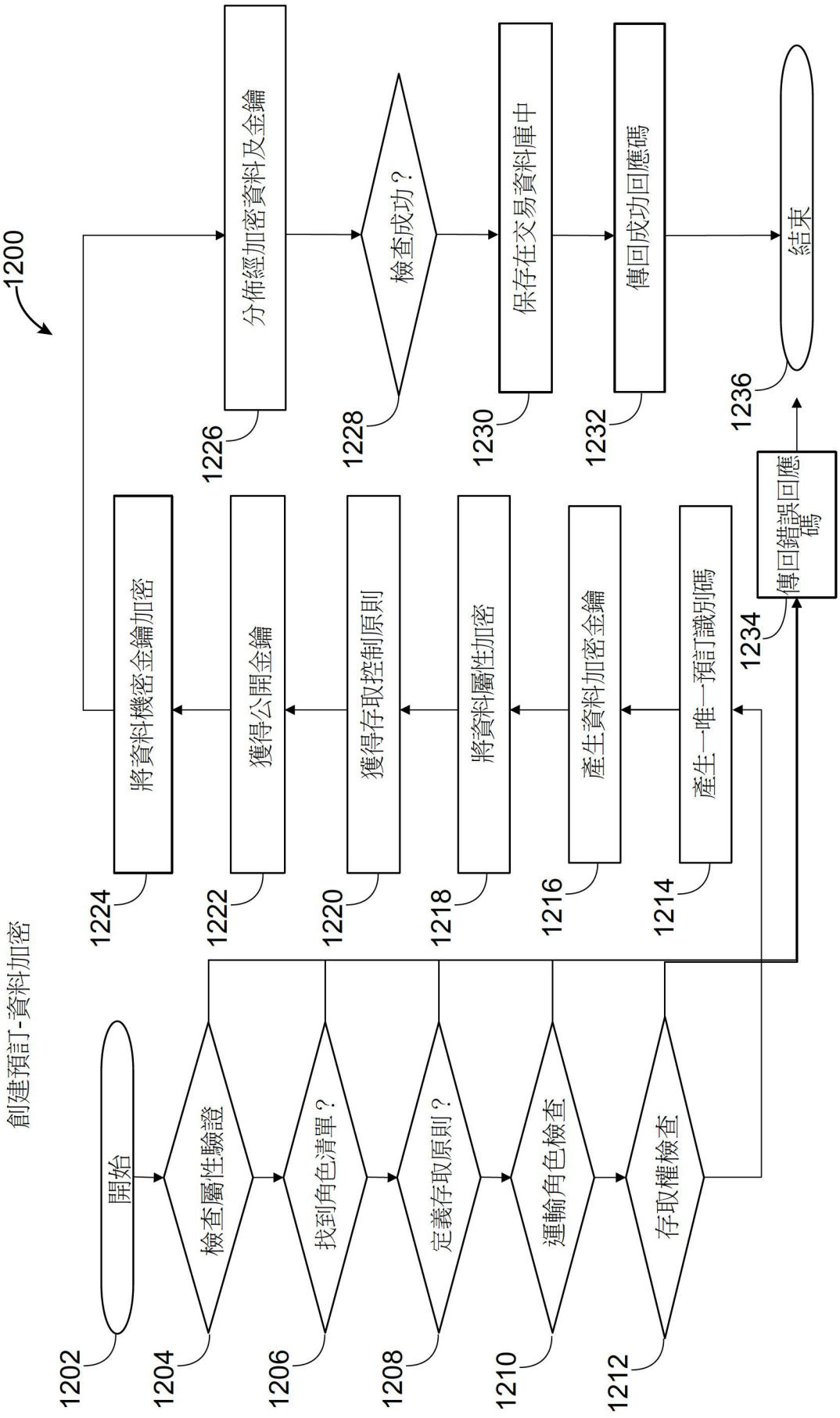
1000

資料提供者預訂號	未決行動	行動預訂版本	行動到期日期	預訂狀態	托運人	代運人
19030726781243	查核危險品應用程式	1	3d 18h 52m 之前 Mar 8 2019 3:22am	新	公司A	代運公司
19030726781243	上傳危險品憑證	1	23h 59m 剩餘 Mar 12 2019 11:15pm	新	公司A	代運公司
19030726781236	提交危險品應用程式	1	3d 9h 48m 之前 Mar 8 2019 12:26pm	新	公司B	代運公司
19030726781236	上傳危險品憑證	1	23h 59m 剩餘 Mar 12 2019 11:15pm	新	托運人99	代運公司
1903072678123	提交危險品應用程式	1	4d 4h 4m 之前 Mar 7 2019 6:11pm	新	托運人99	代運公司
1903072678123	上傳危險品憑證	1	23h 59m 剩餘 Mar 12 2019 11:15pm	新	公司B	代運公司
19030626781311	提交危險品應用程式	1	4d 8h 22m 之前 Mar 7 2019 1:52pm	新	公司A	代運公司
19030534581375	查核危險品應用程式	3	5d 18h 36m 之前 Mar 6 2019 3:38pm	經確認		
1903052678911	查核危險品應用程式	1	6d 2h 59m 之前 Mar 5 2019 7:25pm	新	托運人23	A Fore Ltd
1903052678911	上傳危險品憑證	1	23h 59m 剩餘 Mar 12 2019 11:15pm	新	托運人99	A Fore Ltd
190226267889	上傳危險品憑證	1	23h 59m 剩餘 Mar 12 2019 11:15pm	新	公司B	B Fore Ltd
190226267887	上傳危險品憑證	1	23h 59m 剩餘 Mar 12 2019 11:15pm	新	公司A	B Fore Ltd
190226267878	上傳危險品憑證	1	23h 59m 剩餘 Mar 12 2019 11:15pm	新	公司A	代運公司

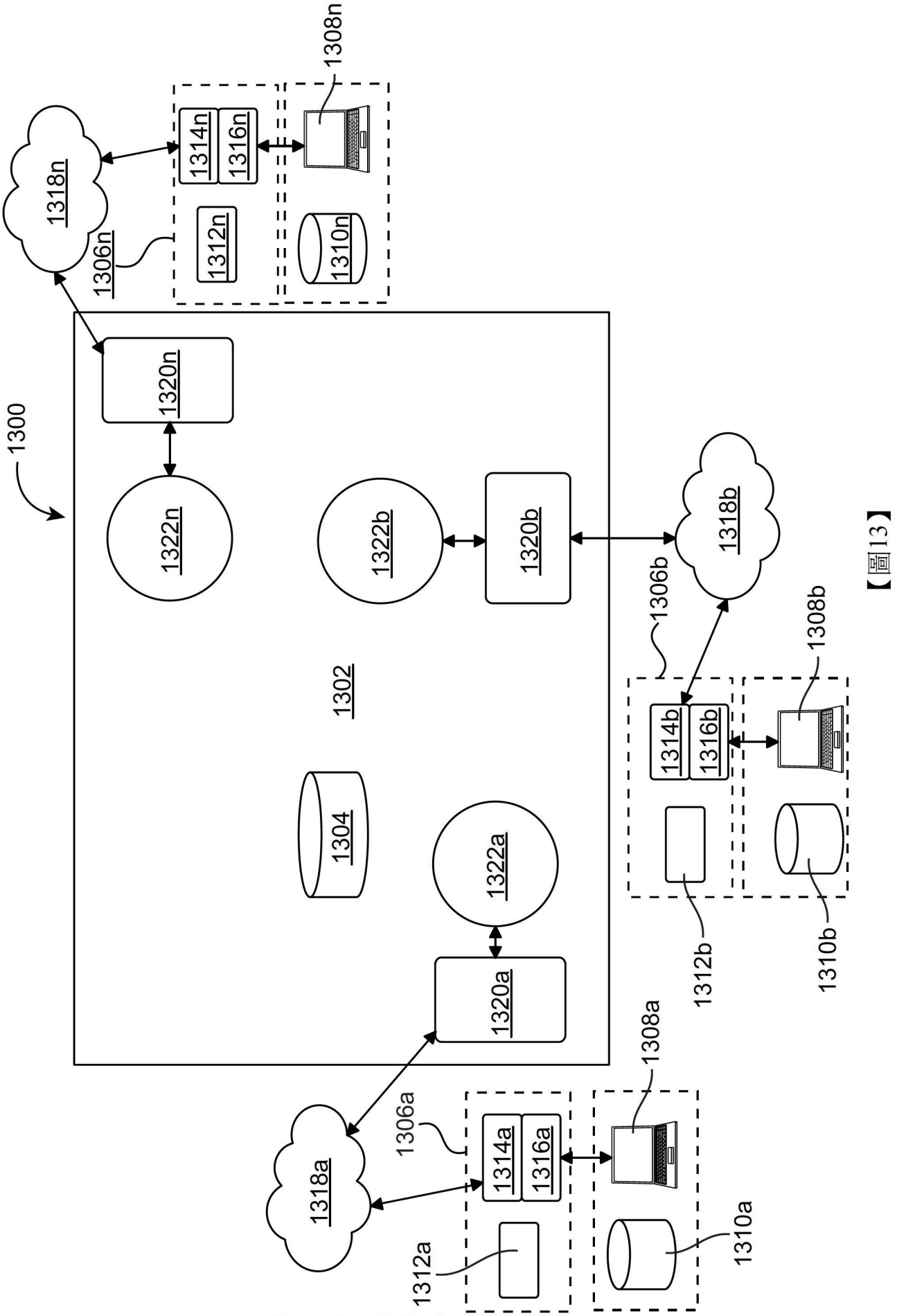
【圖10】


1100
開始
1102
檢查屬性驗證
1104
獲得預訂且解密
1106
程序成功
1108
運輸角色檢查
1110
藉由檢查發送者是否具有屬性之KEK而過濾屬性
1112
成功
1114
錯誤回應
1116
結束
1118

【圖11】


1200
創建預訂-資料加密
開始
檢查屬性驗證
找到角色清單？
定義存取原則？
運輸角色檢查
存取權檢查
產生一唯一預訂識別碼
產生資料加密金鑰
將資料屬性加密
獲得存取控制原則
獲得公開金鑰
將資料機密金鑰加密
分佈經加密資料及金鑰
檢查成功？
保存在交易資料庫中
傳回成功回應碼
結束
傳回錯誤回應碼
1202
1204
1206
1208
1210
1212
1214
1216
1218
1220
1222
1224
1226
1228
1230
1232
1234
1236

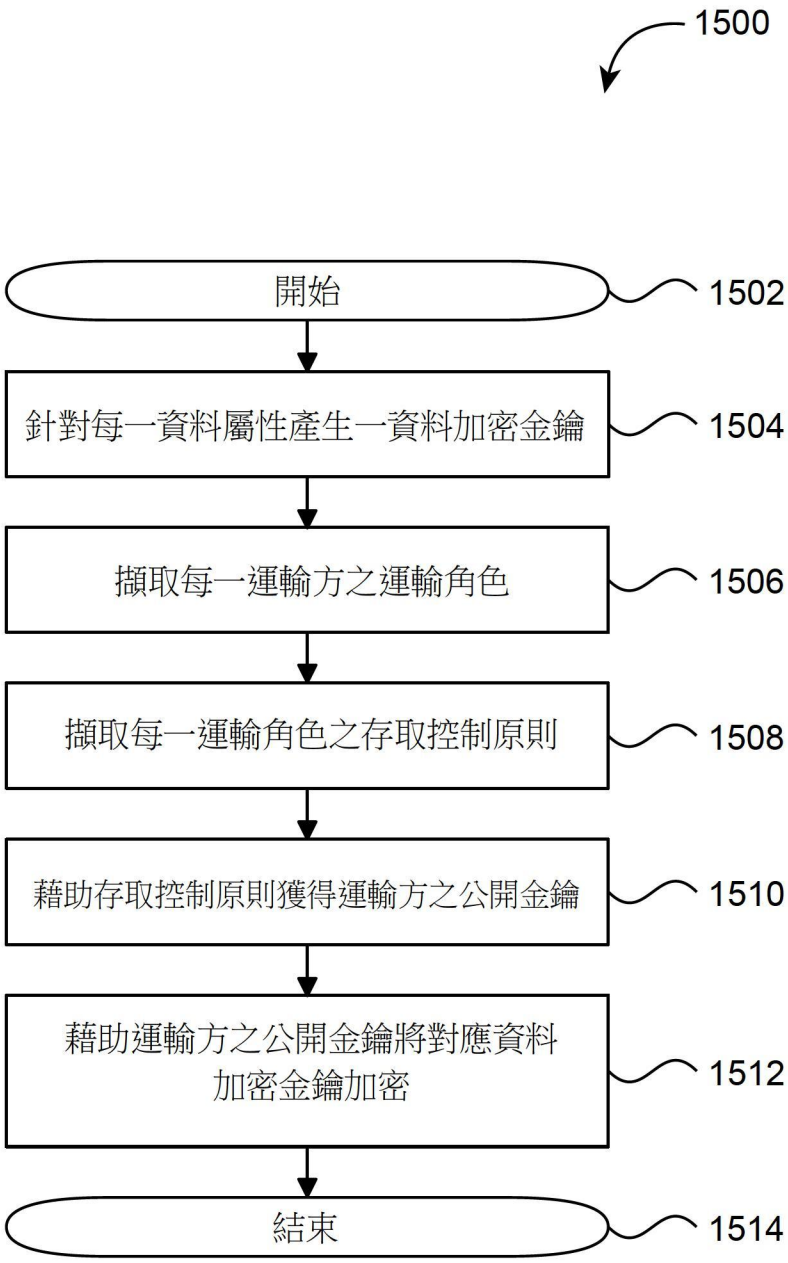
【圖12】


1300
1302
1304
1306a
1306b
1306n
1308a
1308b
1308n
1310a
1310b
1310n
1312a
1312b
1312n
1314a
1314b
1314n
1316a
1316b
1316n
1318a
1318b
1318n
1320a
1320b
1320n
1322a
1322b
1322n

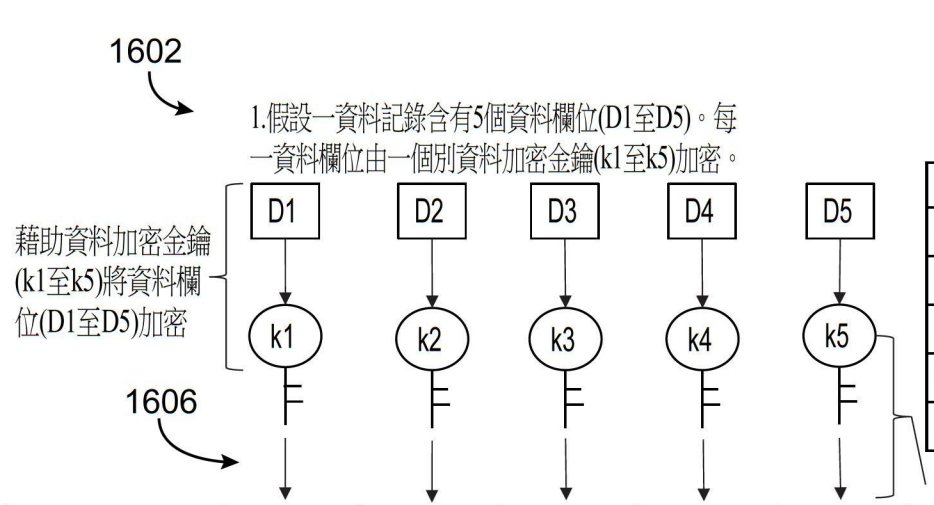
【圖13】

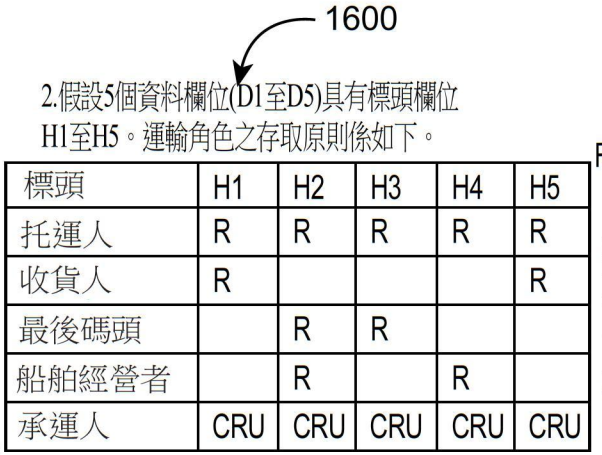
1400
運輸文件中樞
存取原則
全域成員清單
成員
*
角色
靜態的
存取原則文件清單
運輸文件類型
存取原則文件
角色清單清單
定位子金鑰
角色清單
動態的
動態存取原則清單
運輸文件
動態存取原則
運輸文件中樞
實例：承運人
用戶端應用程式
運輸文件使用者節點
發送運輸文件角色清單
實例：托運人
用戶端應用程式
運輸文件使用者節點
發送運輸文件

【圖14】


1500
開始
1502
針對每一資料屬性產生一資料加密金鑰
1504
擷取每一運輸方之運輸角色
1506
擷取每一運輸角色之存取控制原則
1508
藉助存取控制原則獲得運輸方之公開金鑰
1510
藉助運輸方之公開金鑰將對應資料加密金鑰加密
1512
結束
1514

【圖15】





標頭	H1	H2	H3	H4	H5
托運人	R	R	R	R	R
收貨人	R				R
最後碼頭		R	R		
船舶經營者		R		R	
承運人	CRU	CRU	CRU	CRU	CRU

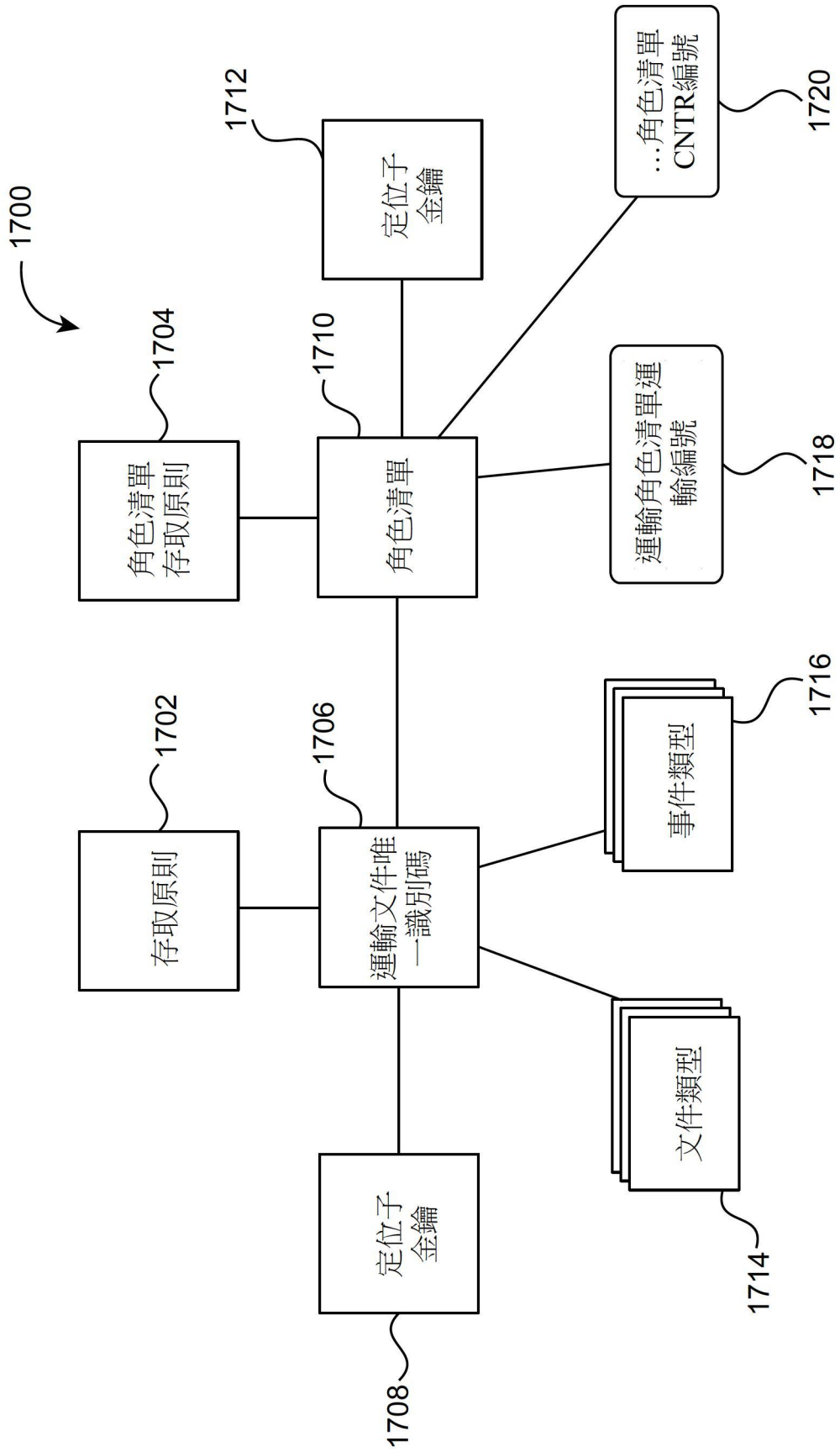
	k1	k2	k3	k4	k5
托運人	$S_{pub}(k1)$	$S_{pub}(k2)$	$S_{pub}(k3)$	$S_{pub}(k4)$	$S_{pub}(k5)$
收貨人	$Co_{pub}(k1)$				$Co_{pub}(k5)$
最後碼頭		$T_{pub}(k2)$	$T_{pub}(k3)$		
船舶經營者		$V_{pub}(k2)$		V (k4)	
承運人	$Ca_{pub}(k1)$	$Ca_{pub}(k2)$	$Ca_{pub}(k3)$	$Ca_{pub}(K4)$	$Ca_{pub}(k5)$

3.基於運輸角色之存取原則，若角色具有對特定屬性之存取權(讀取、更新或創建)，則屬性之資料加密金鑰將由角色之公開金鑰單獨地加密。舉例而言，托運人具有所有屬性(D1至D5)之存取權。D1至D5之DEK將由托運人之公開金鑰單獨地加密。對於另一實例，收貨人具有屬性(D1、D5)之存取權。D1及D5之DEK將由收貨人之公開金鑰加密。

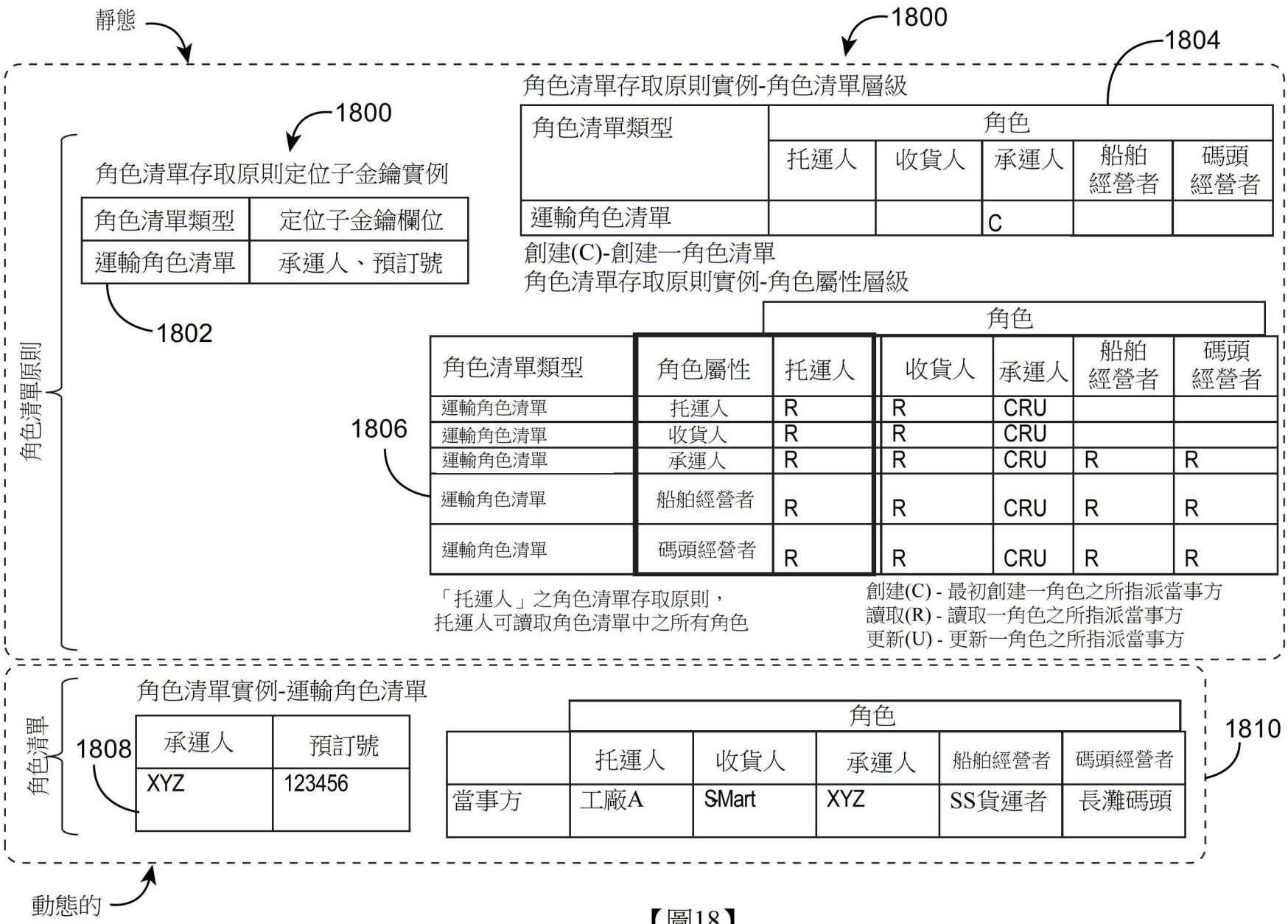
1608

S_{pub}＝托運人之公開金鑰，$S_{pub}(k1)$＝藉助托運人之公開金鑰將資料欄位D1之資料加密金鑰加密
Co_{pub}＝收貨人之公開金鑰，$Co_{pub}(k1)$＝藉助收貨人之公開金鑰將資料欄位D1之資料加密金鑰加密
T_{pub}＝最後碼頭之公開金鑰，$T_{pub}(k2)$＝藉助最後碼頭之公開金鑰將資料欄位D2之資料加密金鑰加密
V_{pub}＝船舶經營者之公開金鑰，$V_{pub}(k2)$＝藉助船舶經營者之公開金鑰將資料欄位D2之資料加密金鑰加密
Ca_{pub}＝承運人之公開金鑰，$Ca_{pub}(k1)$＝藉助承運人之公開金鑰將資料欄位D1之資料加密金鑰加密

【圖16】


1700
1702
存取原則
1704
角色清單存取原則
1706
運輸文件唯一識別碼
1708
定位子金鑰
1710
角色清單
1712
定位子金鑰
1714
文件類型
1716
事件類型
1718
運輸角色清單運輸編號
1720
...角色清單CNTR編號

【圖17】


靜態
1800
1804
角色清單存取原則實例-角色清單層級
角色清單類型
角色
托運人
收貨人
承運人
船舶經營者
碼頭經營者
運輸角色清單
C
創建(C)-創建一角色清單
1800
角色清單存取原則定位子金鑰實例
角色清單類型
定位子金鑰欄位
運輸角色清單
承運人、預訂號
1802
角色清單存取原則實例-角色屬性層級
角色清單原則
角色
角色清單類型
角色屬性
托運人
收貨人
承運人
船舶經營者
碼頭經營者
1806
運輸角色清單
托運人
R
R
CRU
運輸角色清單
收貨人
R
R
CRU
運輸角色清單
承運人
R
R
CRU
R
R
運輸角色清單
船舶經營者
R
R
CRU
R
R
運輸角色清單
碼頭經營者
R
R
CRU
R
R
「托運人」之角色清單存取原則，
托運人可讀取角色清單中之所有角色
創建(C) - 最初創建一角色之所指派當事方
讀取(R) - 讀取一角色之所指派當事方
更新(U) - 更新一角色之所指派當事方
角色清單實例-運輸角色清單
角色清單
1808
承運人
預訂號
XYZ
123456
角色
托運人
收貨人
承運人
船舶經營者
碼頭經營者
1810
當事方
工廠A
SMart
XYZ
SS貨運者
長灘碼頭
動態的

【圖18】

運輸文件　運輸文件貨櫃自碼頭出境事件

標頭欄位	資料欄位
事件識別碼	2348DI32328KU
承運人	XYZ
預訂號	12345
貨櫃號	OXLX6421234
貨櫃大小類型	40RQ
設備ISO碼	45R1
UNLocode	USLGB
事件日期時間	09/20/2015 21:58 GMT
事件時區	美國/洛杉磯

角色清單定位子

1902

唯一金鑰

運輸文件架構

標頭欄位	資料欄位類型
事件識別碼	字串 (40)
承運人	字串(4)
預訂號	字串(20)
貨櫃號	字串(20)
貨櫃大小類型	字串(4)
設備ISO碼	字串(4)
UNLocode	字串(5)
事件日期時間	日期

角色清單定位子

1908

運輸文件出境事件存取原則角色清單定位子金鑰

運輸文件類型	角色清單類型	定位子金鑰欄位
出境事件	運輸角色清單	承運人、預訂號

1904

1900 靜態的

運輸文件出境事件存取原則文件

運輸文件類型	托運人	收貨人	承運人	碼頭經營者	船舶經營者
出境事件	R	R	R	CRUD	R

1906

創建(C)-創建數位資產
讀取(R)-讀取數位資產
更新(U)-更新數位資產
刪除(D)-邏輯刪除數位資產

運輸文件出境事件存取原則-欄位層級

運輸文件類型	欄位	托運人	收貨人	承運人	碼頭經營者	船舶經營者
出境事件	貨櫃號	R	R	RU	CRU	R
出境事件	貨櫃大小類型	R	R	RU	CRU	R
出境事件	設備ISO碼	R	R	RU	CRU	R
出境事件	UNLocode	R	R	RU	CRU	R
出境事件	事件日期時間	R	R	RU	CRU	R
出境事件	事件時區	R	R	RU	CRU	R
出境事件	密封類型	R	R	RU	CRU	R
出境事件	密封號	R	R	RU	CRU	R
出境事件	參考文件類型	R	R	RU	CRU	R
出境事件	參考文件號	R	R	RU	CRU	R

1910

創建(C)-創建欄位之值
讀取(R)-讀取欄位之值
更新(U)-更新欄位之值

【圖19】

運輸文件-危險品憑證提交

2002

角色清單定位子

標頭欄位	資料欄位
危險品憑證識別碼	SDFHIO32489
版本	1
承運人	XYZ
預訂號	12345
船舶名稱	SS ASIA
航次	107E
裝載港口	HKHKG
卸載港口	USLGB
貨品描述	30230064 UN 2912, CORROSIVE SOLID, FLAMMABLE, N.O.S. (POTASSIUM-TERT BUTANOLATE), 8(4.1), PG (ERG 134)
總重	13123
總重單位	KG
批准狀態	已提交

運輸文件架構

2010

角色清單定位子

標頭欄位	資料欄位類型
危險品憑證識別碼	字串(40)
版本	整數
承運人	字串(4)
預訂號	字串(20)
船舶名稱	字串(20)
航次	字串(4)
裝載港口	字串(5)
卸載港口	字串(5)
貨品描述	字串(1000)

運輸文件危險品憑證存取原則角色清單定位子金鑰實例

2000

運輸文件類型	角色清單類型	定位子金鑰欄位
出境事件	運輸角色清單	承運者、預訂號

2004

運輸文件危險品憑證存取原則-文件層級

運輸文件類型	托運人	收貨人	承運人	碼頭經營者	船舶經營者
DG Cert	CRUD	R	RU	R	R

2006

創建(C)-創建數位資產
讀取(R)-讀取數位資產
更新(U)-更新數位資產
刪除(D)-邏輯刪除數位資產

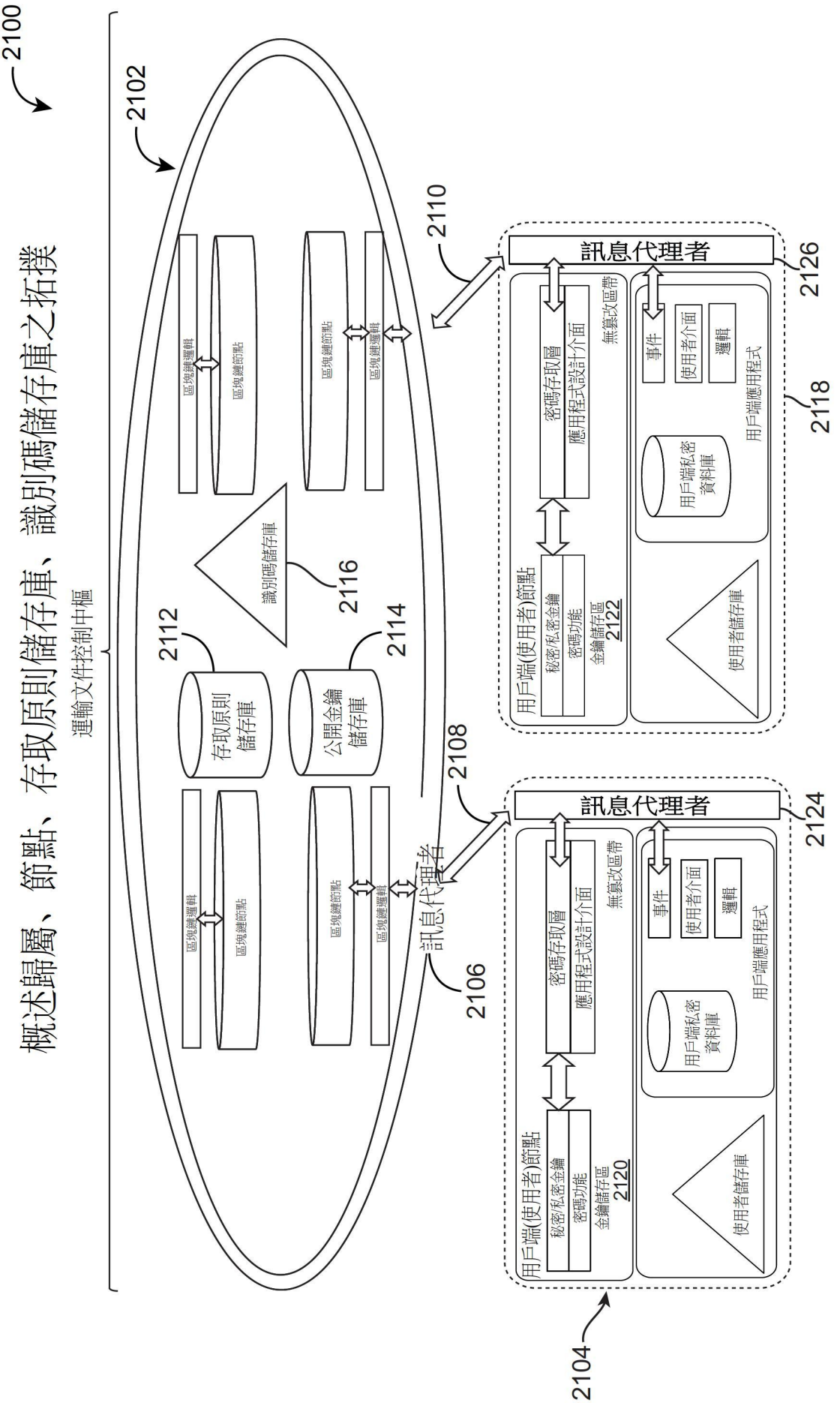
運輸文件危險品憑證存取原則-欄位層級

運輸文件類型	欄位	托運人	收貨人	承運人	碼頭經營者	船舶經營者
DG Cert	船舶名稱	CRU	R	RU	R	R
DG Cert	航次	CRU	R	RU	R	R
DG Cert	裝載港口	CRU	R	R	R	R
DG Cert	卸載港口	CRU	R	R	R	R
DG Cert	貨品描述	CRU	R	R	R	R
DG Cert	總重	CRU	R	R	R	R
DG Cert	總重單位	CRU	R	R	R	R
DG Cert	批准狀態	CRU	R	R	R	R

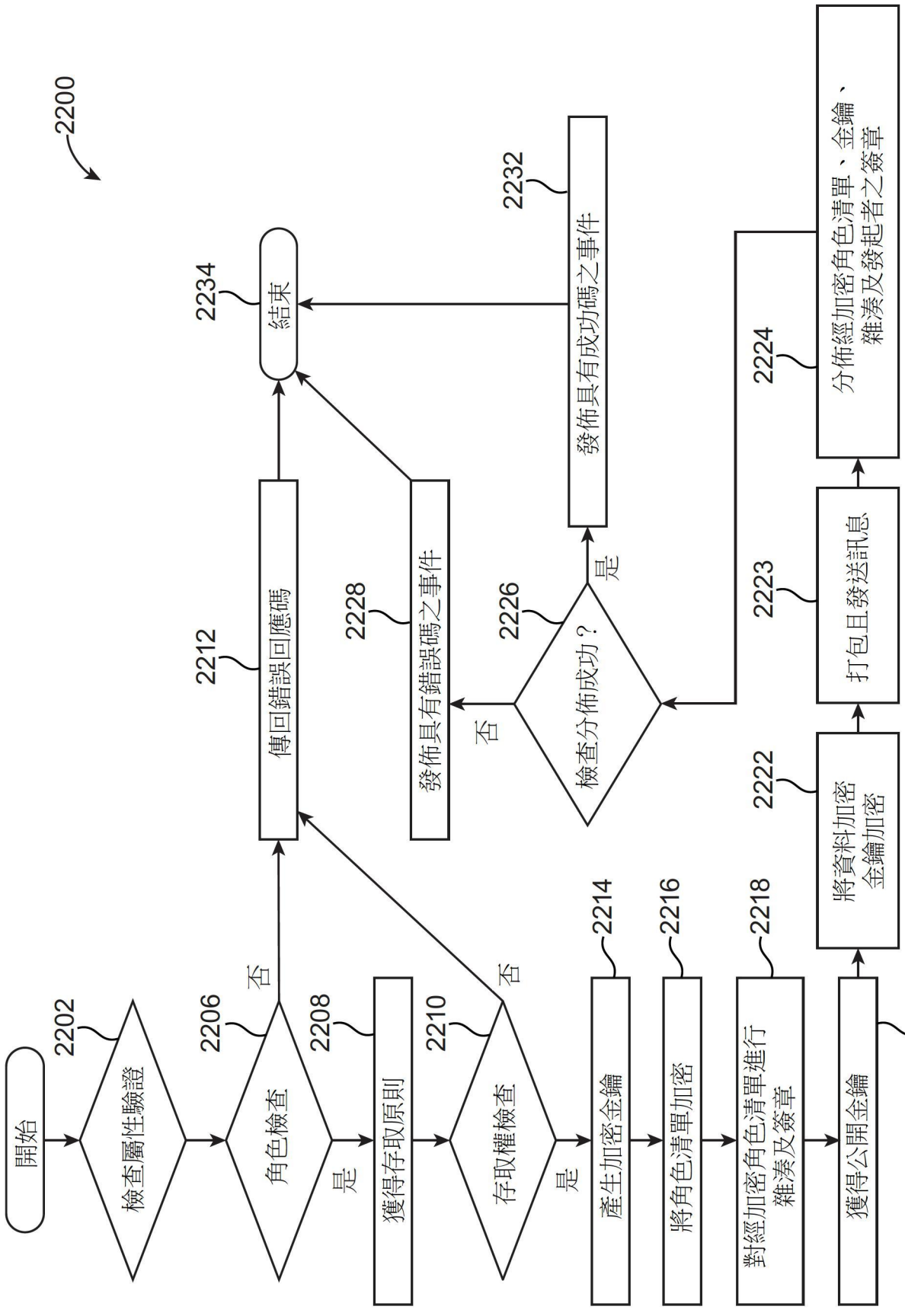
2008

創建(C)-創建欄位之值
讀取(R)-讀取欄位之值
更新(U)-更新欄位之值

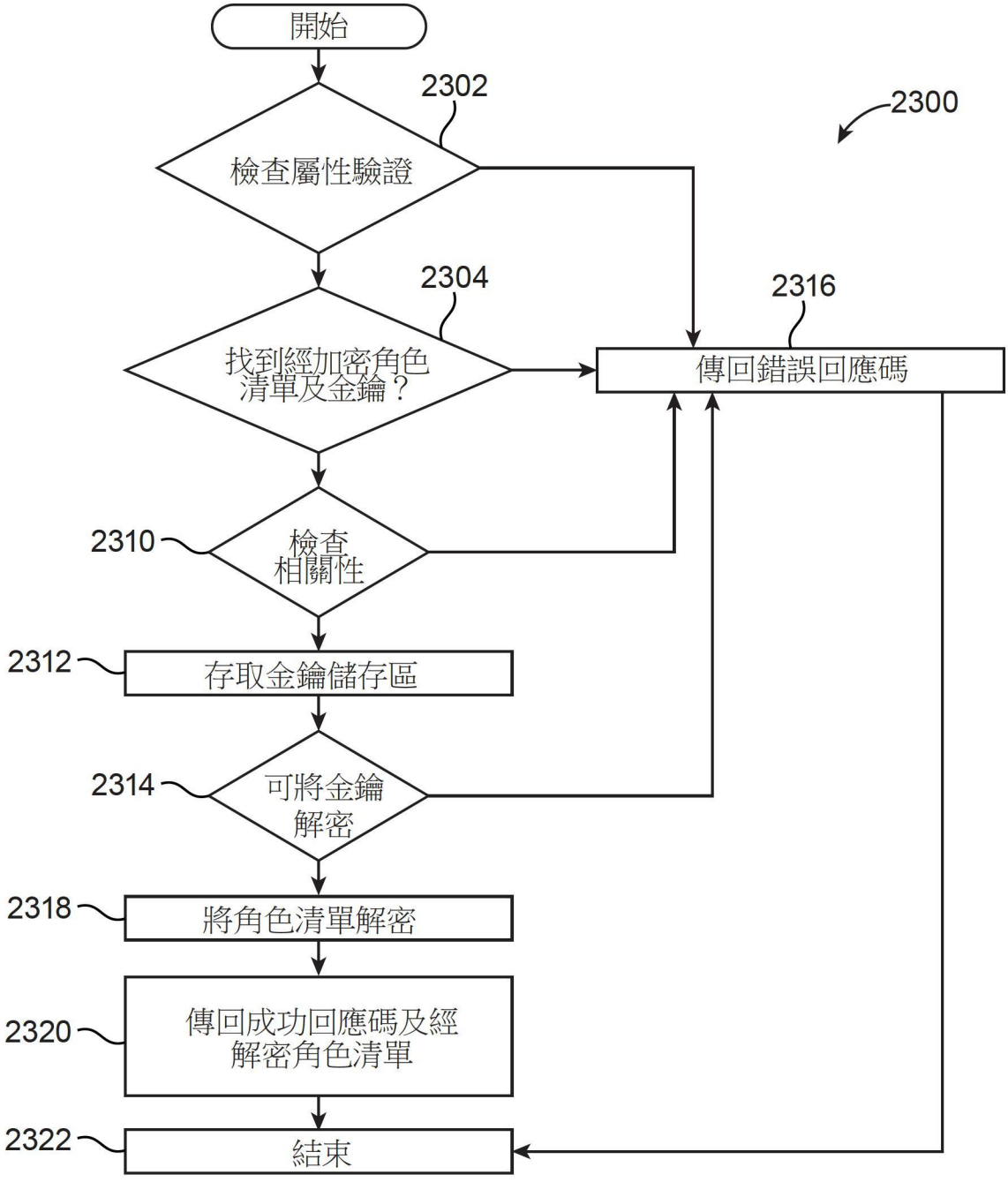
【圖20】


概述歸屬、節點、存取原則儲存庫、識別碼儲存庫之拓撲
2100
2102
運輸文件控制中樞
區塊鏈邏輯
區塊鏈節點
存取原則儲存庫
2112
識別碼儲存庫
2116
公開金鑰儲存庫
2114
訊息代理者
2106
2108
訊息代理者
2110
訊息代理者
2124
訊息代理者
2126
用戶端(使用者)節點
秘密/私密金鑰
密碼功能
金鑰儲存區
2120
密碼存取層
應用程式設計介面
無篡改區帶
用戶端私密資料庫
事件
使用者介面
邏輯
用戶端應用程式
使用者儲存庫
用戶端(使用者)節點
秘密/私密金鑰
密碼功能
金鑰儲存區
2122
密碼存取層
應用程式設計介面
無篡改區帶
用戶端私密資料庫
事件
使用者介面
邏輯
用戶端應用程式
2118
使用者儲存庫
2104

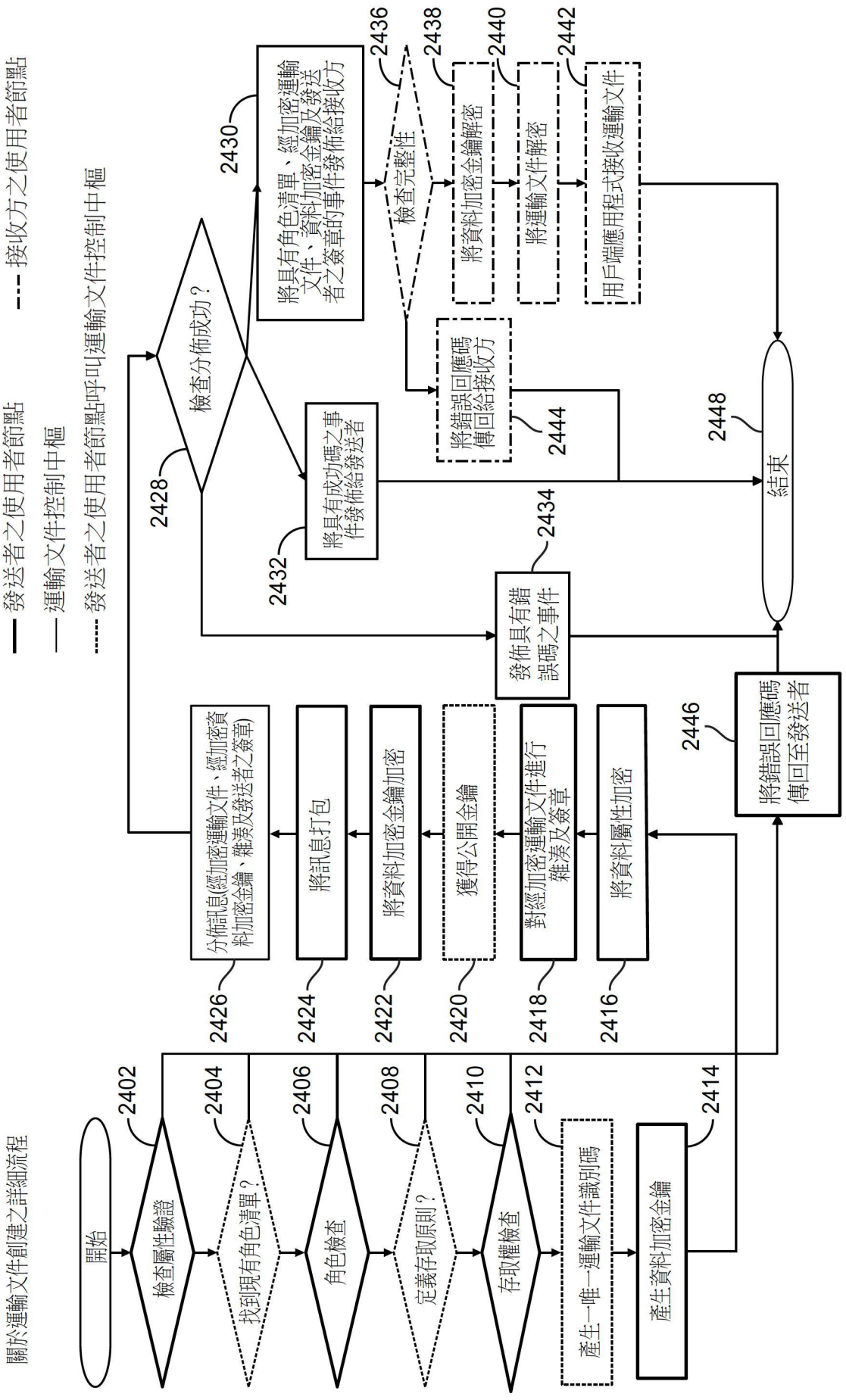
【圖21】


2200
開始
2202
檢查屬性驗證
2206
角色檢查
否
2208
是
獲得存取原則
2210
存取權檢查
否
是
2212
傳回錯誤回應碼
2214
產生加密金鑰
2216
將角色清單加密
2218
對經加密角色清單進行雜湊及簽章
2220
獲得公開金鑰
2222
將資料加密金鑰加密
2223
打包且發送訊息
2224
分佈經加密角色清單、金鑰、雜湊及發起者之簽章
2226
檢查分佈成功？
否
是
2228
發佈具有錯誤碼之事件
2232
發佈具有成功碼之事件
2234
結束

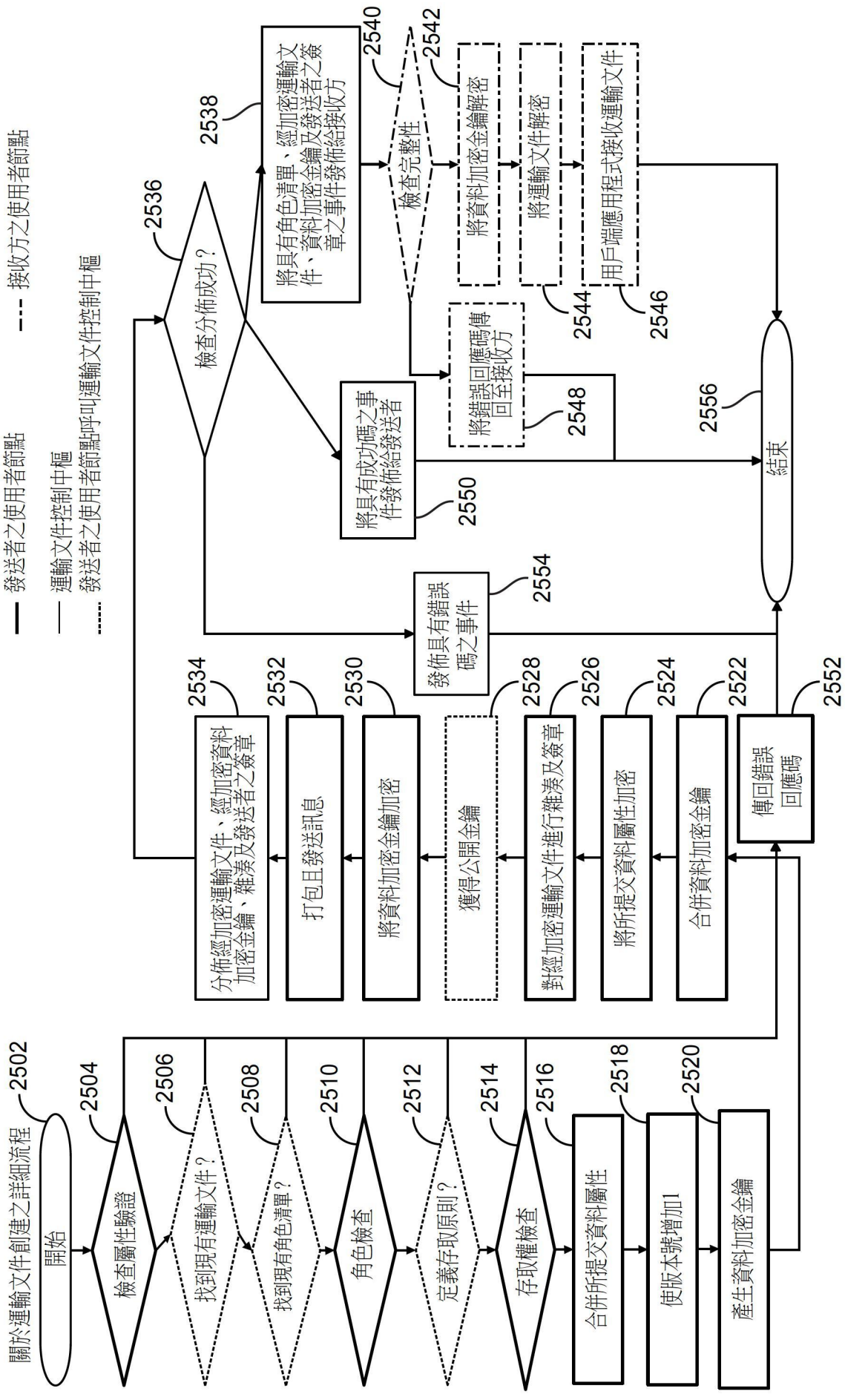
【圖22】


開始
2302
檢查屬性驗證
2300
2304
找到經加密角色清單及金鑰？
2316
傳回錯誤回應碼
2310
檢查相關性
2312
存取金鑰儲存區
2314
可將金鑰解密
2318
將角色清單解密
2320
傳回成功回應碼及經解密角色清單
2322
結束

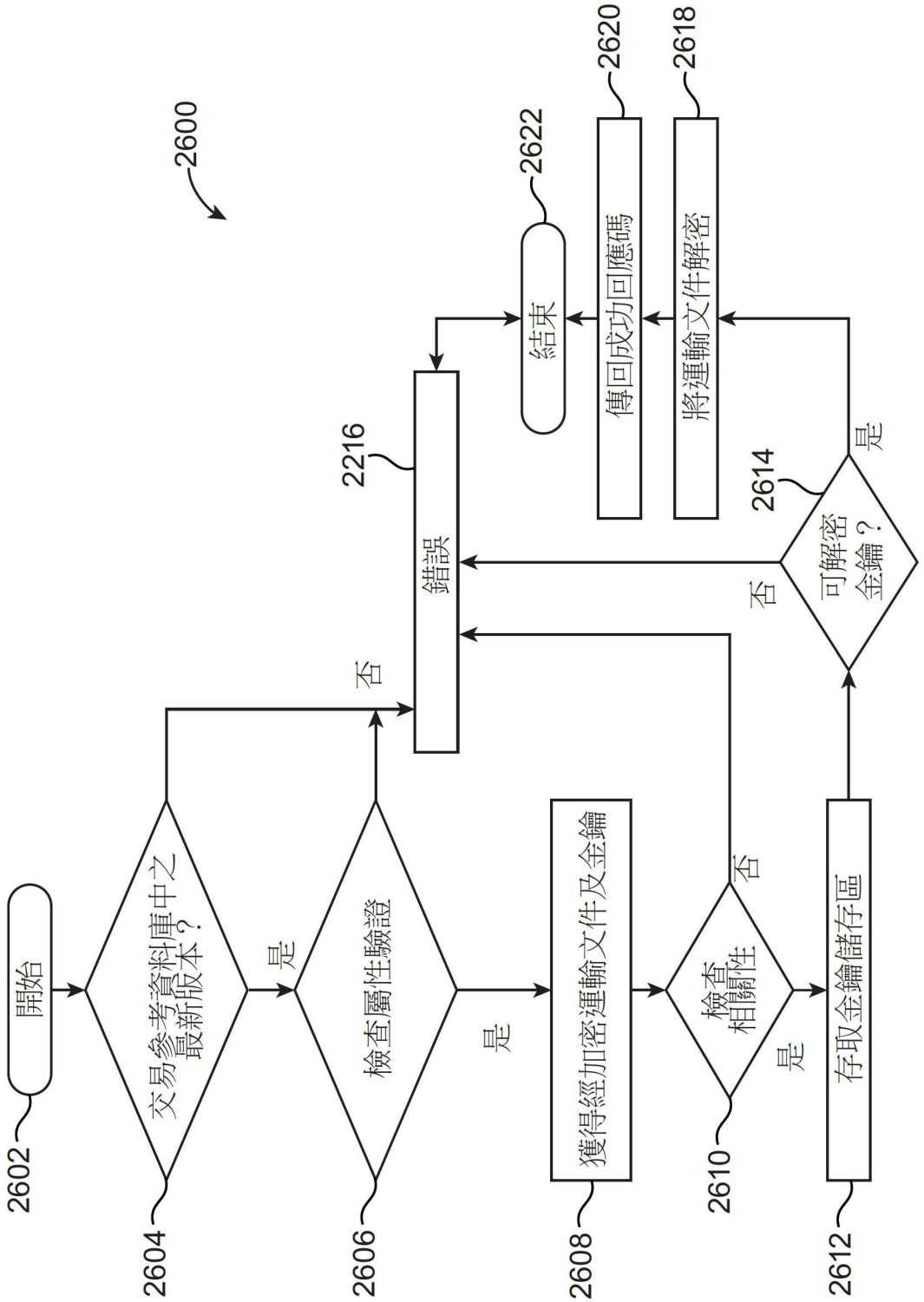
【圖23】


關於運輸文件創建之詳細流程
發送者之使用者節點
運輸文件控制中樞
發送者之使用者節點呼叫運輸文件控制中樞
接收方之使用者節點
開始
2402
檢查屬性驗證
2404
找到現有角色清單？
2406
角色檢查
2408
定義存取原則？
2410
存取權檢查
2412
產生一唯一運輸文件識別碼
2414
產生資料加密金鑰
2416
將資料屬性加密
2418
對經加密運輸文件進行雜湊及簽章
2420
獲得公開金鑰
2422
將資料加密金鑰加密
2424
將訊息打包
2426
分佈訊息(經加密運輸文件、經加密資料加密金鑰、雜湊及發送者之簽章)
2428
檢查分佈成功？
2430
將具有角色清單、經加密運輸文件、資料加密金鑰及發送者之簽章的事件發佈給接收方
2432
將具有成功碼之事件發佈給發送者
2434
發佈具有錯誤碼之事件
2436
檢查完整性
2438
將錯誤回應碼傳回給接收方
2440
將資料加密金鑰解密
2442
將運輸文件解密
2444
用戶端應用程式接收運輸文件
2446
將錯誤回應碼傳回至發送者
2448
結束

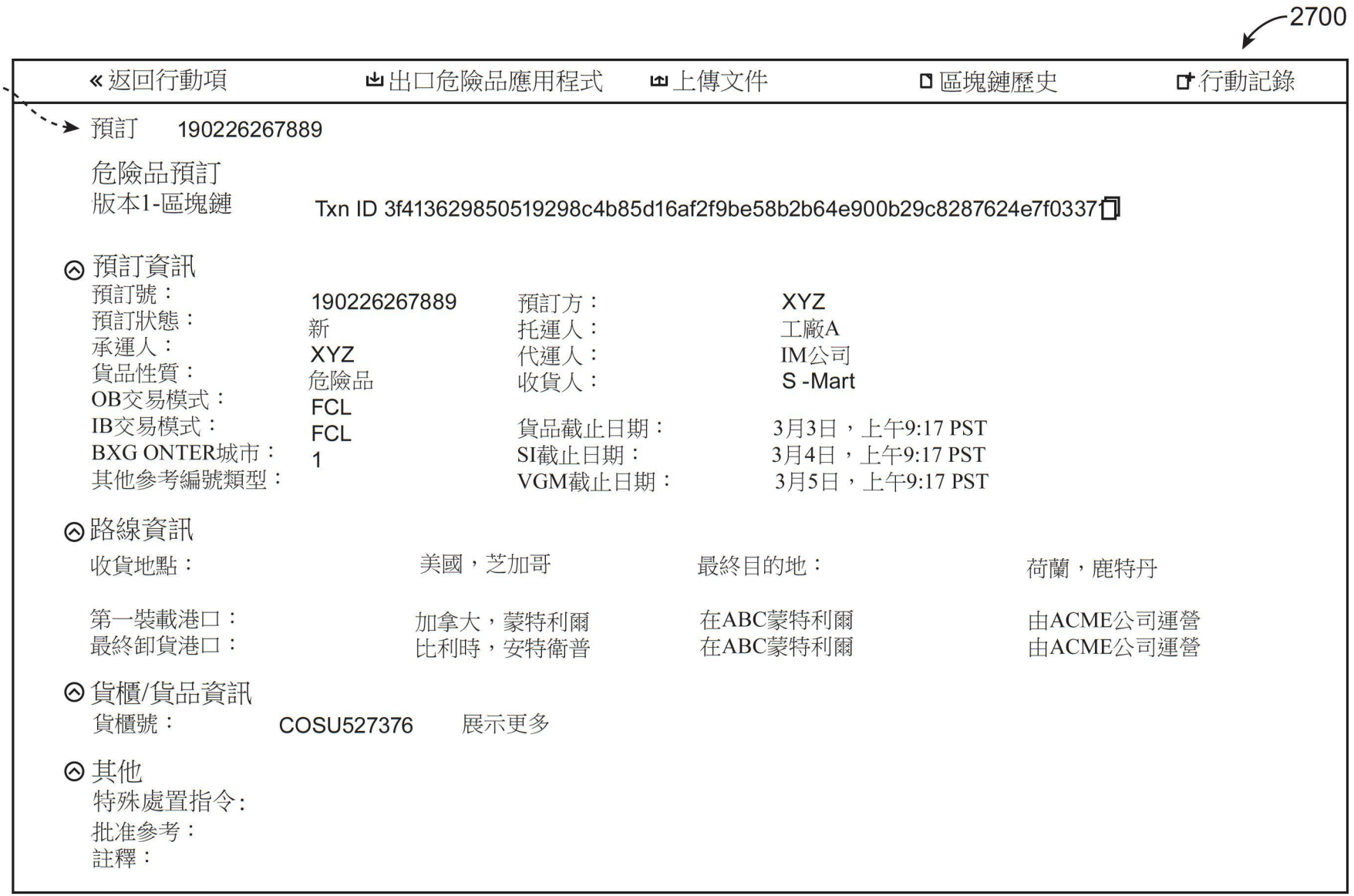
【圖24】


發送者之使用者節點
接收方之使用者節點
運輸文件控制中樞
發送者之使用者節點呼叫運輸文件控制中樞
關於運輸文件創建之詳細流程
開始
2502
檢查屬性驗證
2504
找到現有運輸文件？
2506
找到現有角色清單？
2508
角色檢查
2510
定義存取原則？
2512
存取權檢查
2514
合併所提交資料屬性
2516
使版本號增加1
2518
產生資料加密金鑰
2520
分佈經加密運輸文件、經加密資料加密金鑰、雜湊及發送者之簽章
2534
打包且發送訊息
2532
將資料加密金鑰加密
2530
獲得公開金鑰
2528
對經加密運輸文件進行雜湊及簽章
2526
將所提交資料屬性加密
2524
合併資料加密金鑰
2522
傳回錯誤回應碼
2552
發佈具有錯誤碼之事件
2554
檢查分佈成功？
2536
將具有成功碼之事件發佈給發送者
2550
將具有角色清單、經加密運輸文件、資料加密金鑰及發送者之簽章之事件發佈給接收方
2538
檢查完整性
2540
將錯誤回應碼傳回至接收方
2548
將資料加密金鑰解密
2542
將運輸文件解密
2544
用戶端應用程式接收運輸文件
2546
結束
2556

【圖25】


2600
開始
2602
交易參考資料庫中之最新版本？
2604
是
否
檢查屬性驗證
2606
是
否
獲得經加密運輸文件及金鑰
2608
檢查相關性
2610
是
否
存取金鑰儲存區
2612
可解密金鑰？
2614
是
否
錯誤
2216
結束
2622
傳回成功回應碼
2620
將運輸文件解密
2618

【圖26】



【圖27】

2800

«返回行動項　出口危險品應用程式　上傳文件　區塊鏈歷史　行動記錄

預訂　190226267889

危險品預訂

版本1-區塊鏈　Txn ID 3f413629850519298c4b85d16af2f9be58b64e900b29c8287624e7f033717

預訂資訊

預訂號：	190226267889	預訂方：	
預訂狀態：	新	托運人：	
承運人：	XYZ	代運人：	
貨品性質：	危險品	收貨人：	
OB交易模式：	FCL		
IB交易模式：	FCL	貨品截止日期：	3月3日，上午9:17 PST
BXG ONTER城市：	1	SI截止日期：	3月4日，上午9:17 PST
其他參考編號類型：	/	VGM截止日期：	3月5日，上午9:17 PST

路線資訊

收貨地點：		最終目的地：	
第一裝載港口：	加拿大，蒙特利爾	在ABC蒙特利爾	由ACME公司運營
最終卸貨港口：	比利時，安特衛普	在ABC蒙特利爾	由ACME公司運營

貨櫃/貨品資訊

貨櫃號：　COSU527376　展示更多

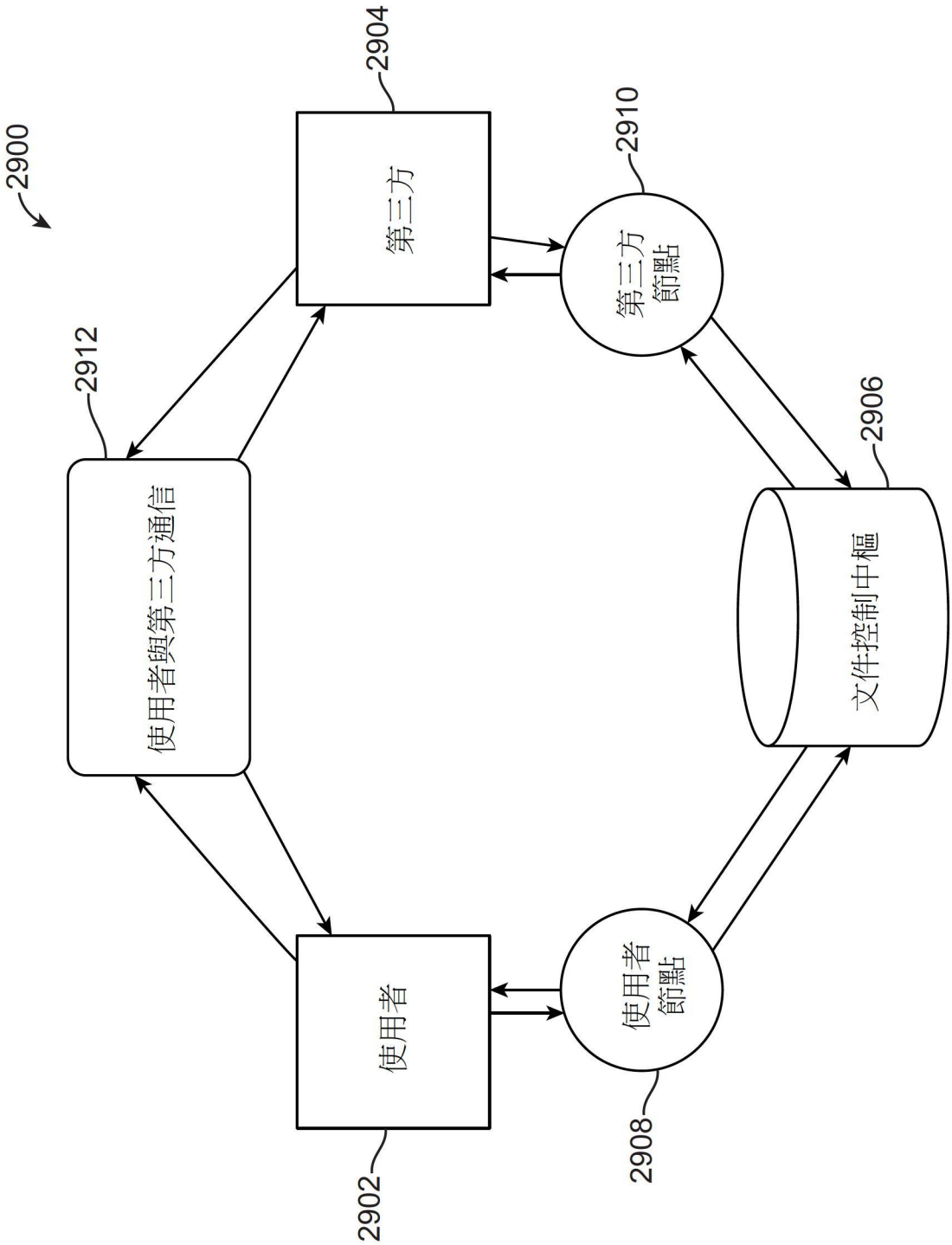
其他

特殊處置指令:

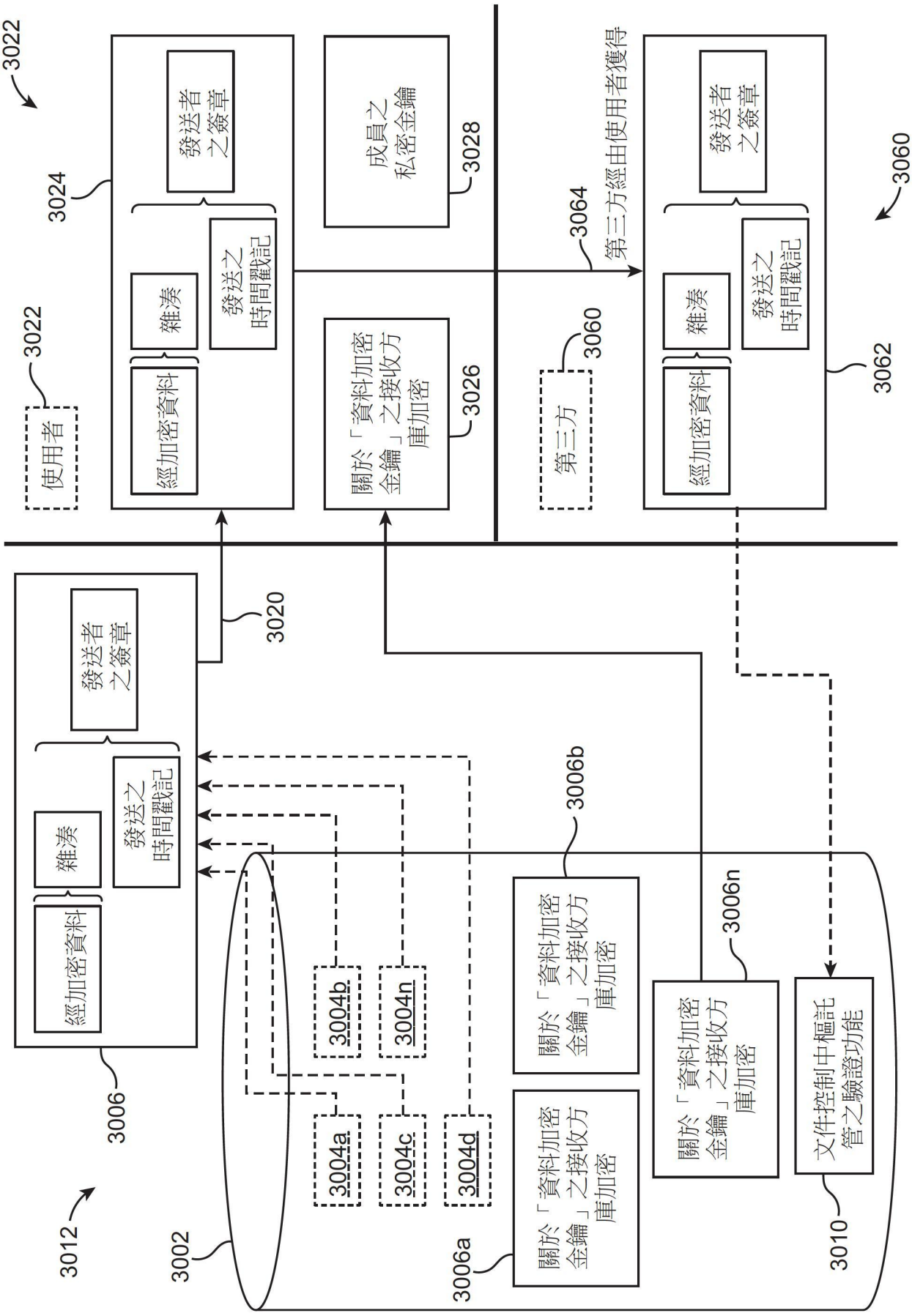
批准參考：

註釋：

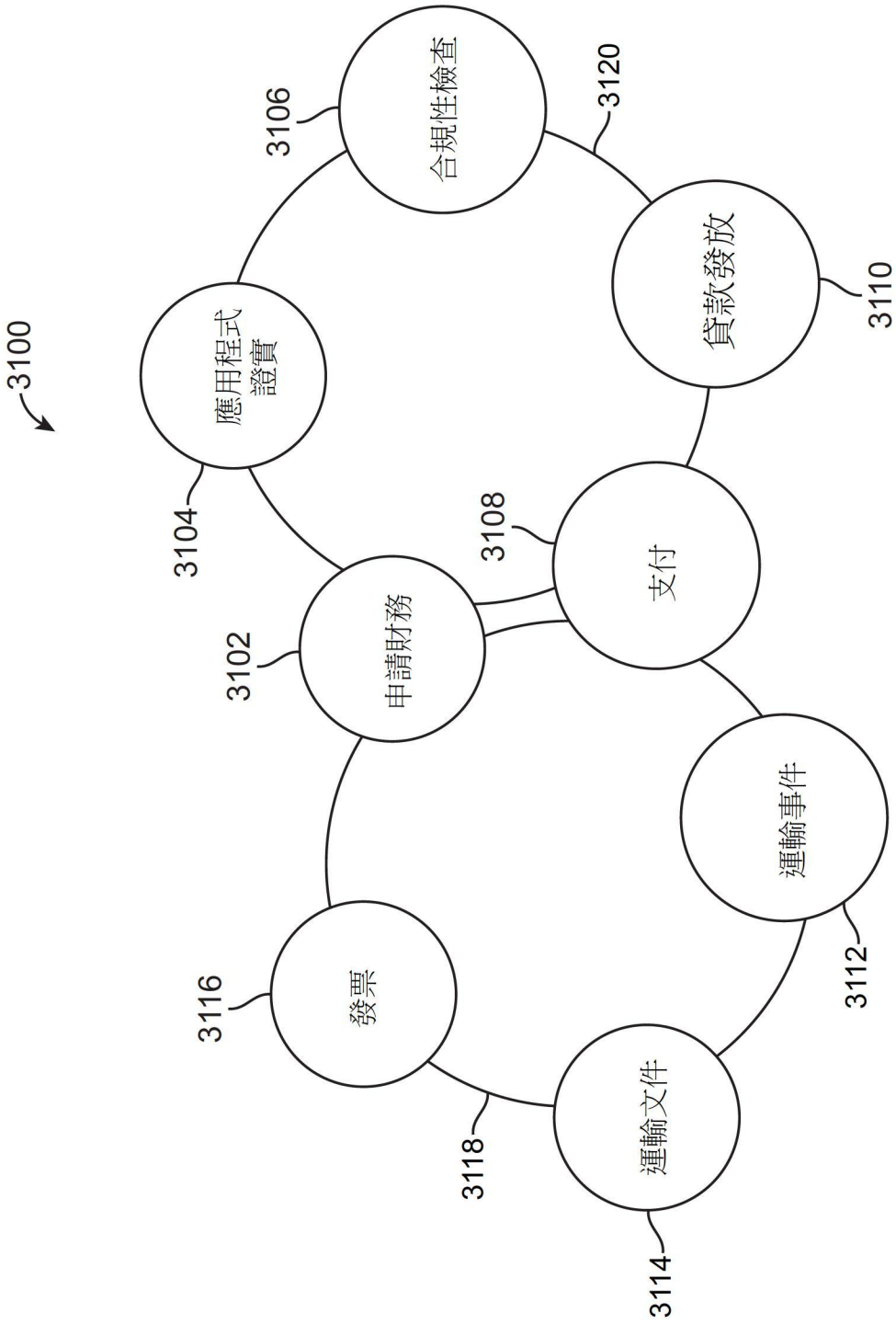
【圖28】


2900
2904
第三方
2910
第三方節點
2912
使用者與第三方通信
2906
文件控制中樞
使用者
使用者節點
2902
2908

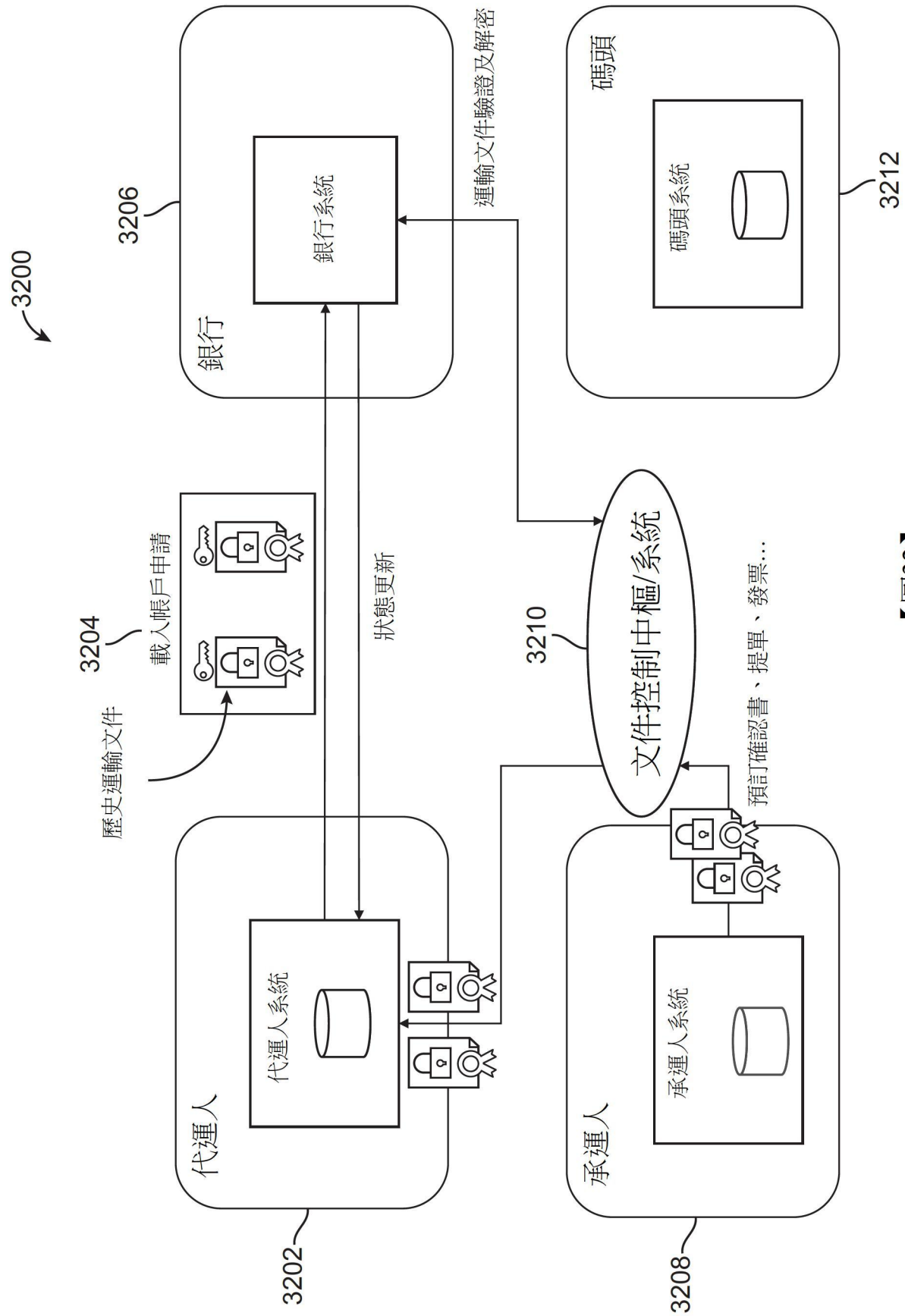
【圖29】


3022
3024
發送者之簽章
雜湊
發送之時間戳記
經加密資料
3028
成員之私密金鑰
3022
使用者
3026
關於「資料加密金鑰」之接收方庫加密
3064
第三方經由使用者獲得
3060
第三方
3060
3062
發送者之簽章
雜湊
發送之時間戳記
經加密資料
3020
發送者之簽章
雜湊
發送之時間戳記
經加密資料
3006
3004b
3004n
3004a
3004c
3004d
3006b
關於「資料加密金鑰」之接收方庫加密
3006n
關於「資料加密金鑰」之接收方庫加密
文件控制中樞託管之驗證功能
3012
3002
3006a
3010

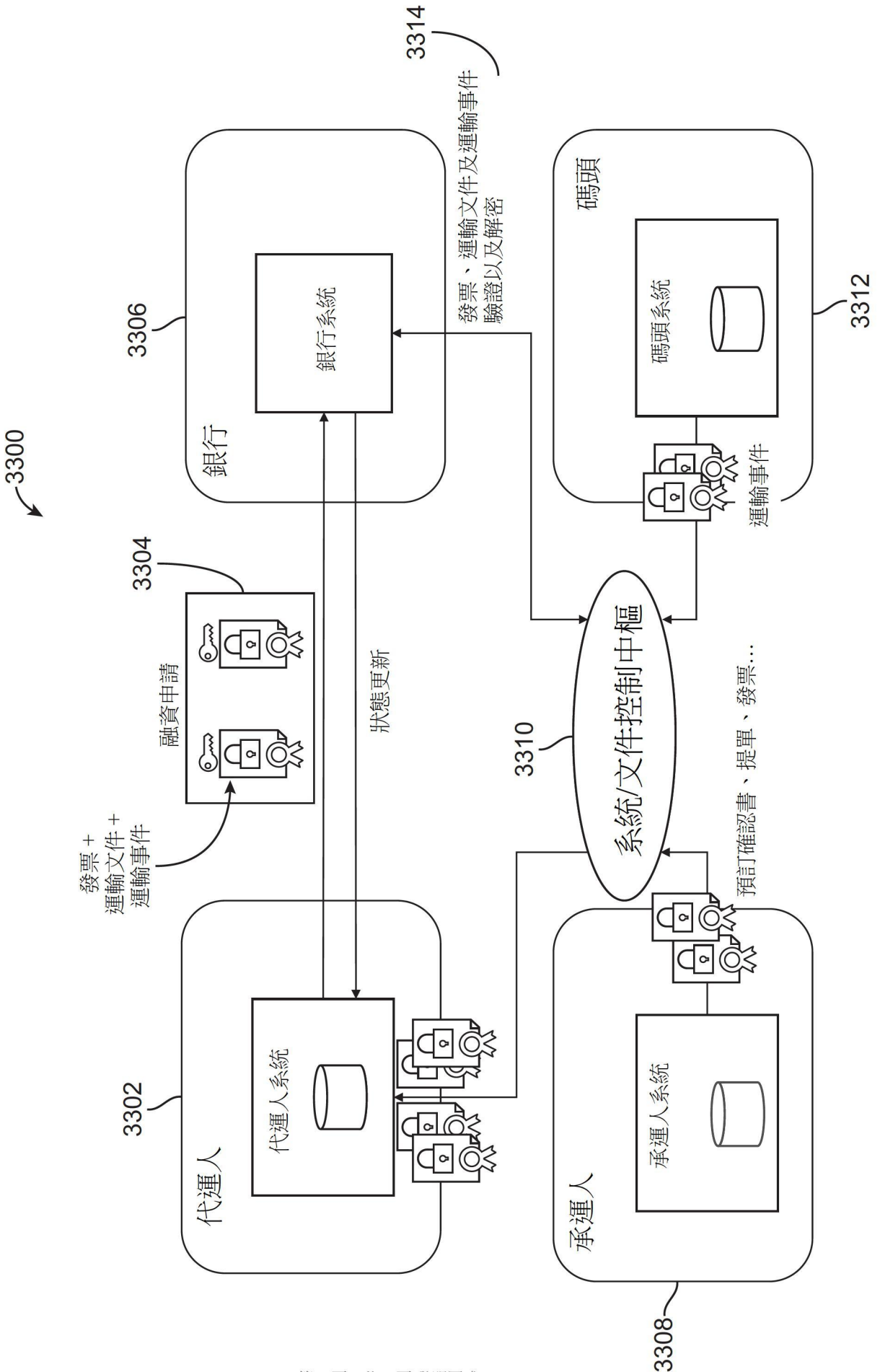
【圖30】


3100
合規性檢查
3106
3120
應用程式證實
貸款發放
3104
3110
3108
支付
申請財務
3102
運輸事件
3116
發票
3112
3118
運輸文件
3114

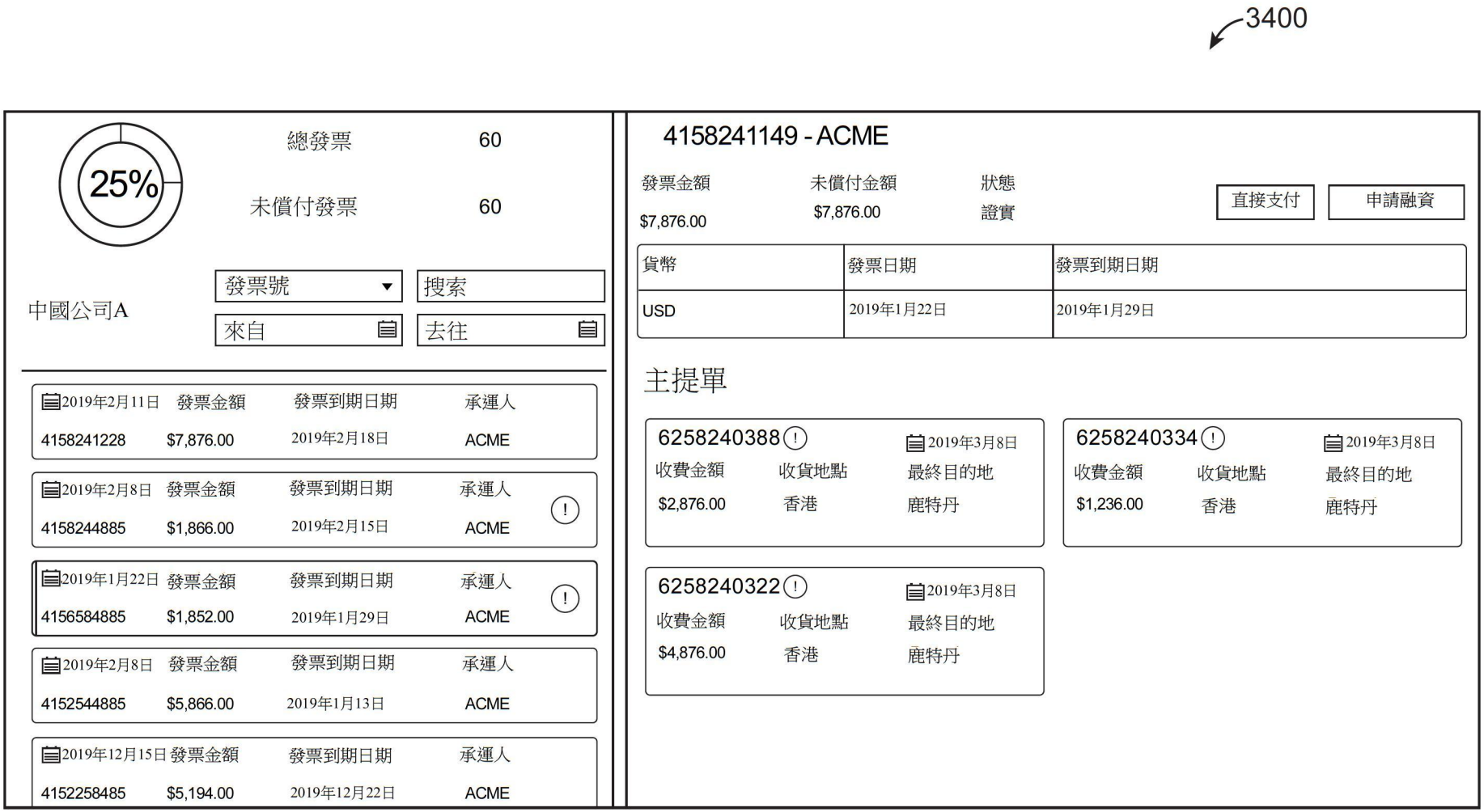
【圖31】


3200
3206
銀行
銀行系統
運輸文件驗證及解密
碼頭
碼頭系統
3212
3204
載入帳戶申請
歷史運輸文件
狀態更新
3210
文件控制中樞/系統
預訂確認書、提單、發票…
代運人
代運人系統
3202
承運人
承運人系統
3208

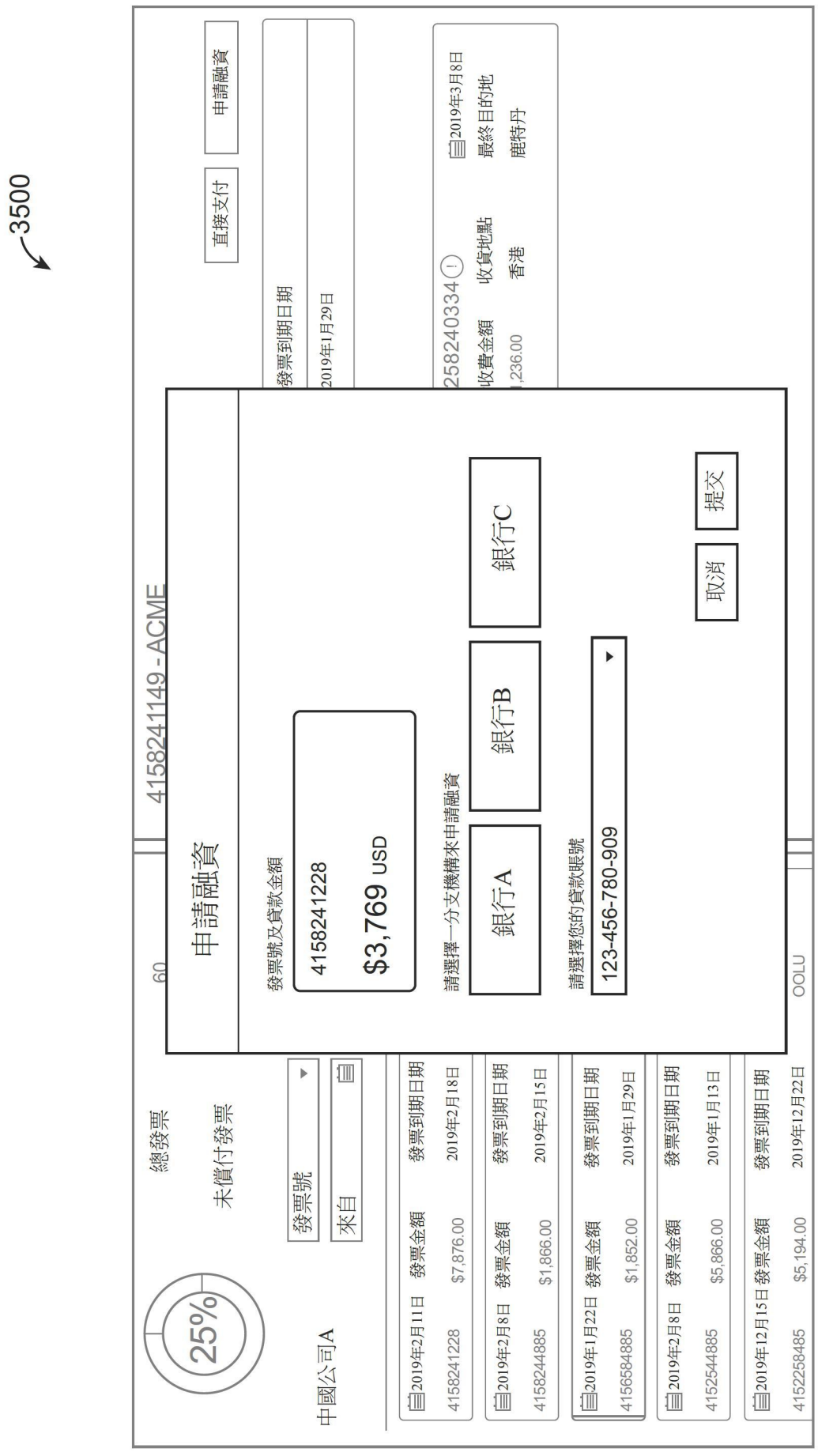
【圖32】


3300
3302
代運人
代運人系統
3304
融資申請
發票 +
運輸文件 +
運輸事件
3306
銀行
銀行系統
3308
承運人
承運人系統
3310
系統/文件控制中樞
3312
碼頭
碼頭系統
運輸事件
3314
發票、運輸文件及運輸事件
驗證以及解密
狀態更新
預訂確認書、提單、發票…

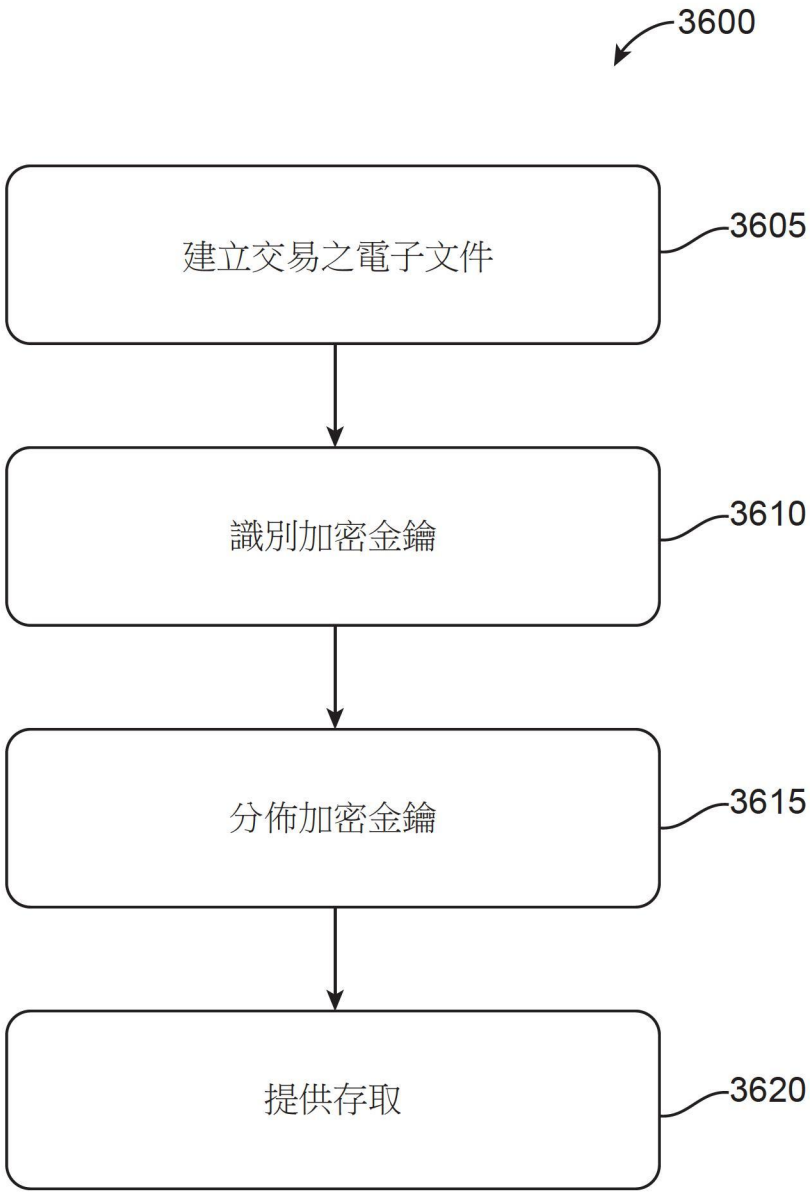
【圖33】


3400
25%
總發票 60
未償付發票 60
中國公司A
發票號
搜索
來自
去往
2019年2月11日 發票金額 發票到期日期 承運人
4158241228 $7,876.00 2019年2月18日 ACME
2019年2月8日 發票金額 發票到期日期 承運人
4158244885 $1,866.00 2019年2月15日 ACME
2019年1月22日 發票金額 發票到期日期 承運人
4156584885 $1,852.00 2019年1月29日 ACME
2019年2月8日 發票金額 發票到期日期 承運人
4152544885 $5,866.00 2019年1月13日 ACME
2019年12月15日 發票金額 發票到期日期 承運人
4152258485 $5,194.00 2019年12月22日 ACME
4158241149 - ACME
發票金額 未償付金額 狀態
$7,876.00 $7,876.00 證實
直接支付
申請融資
貨幣 發票日期 發票到期日期
USD 2019年1月22日 2019年1月29日
主提單
6258240388
2019年3月8日
收費金額 收貨地點 最終目的地
$2,876.00 香港 鹿特丹
6258240334
2019年3月8日
收費金額 收貨地點 最終目的地
$1,236.00 香港 鹿特丹
6258240322
2019年3月8日
收費金額 收貨地點 最終目的地
$4,876.00 香港 鹿特丹

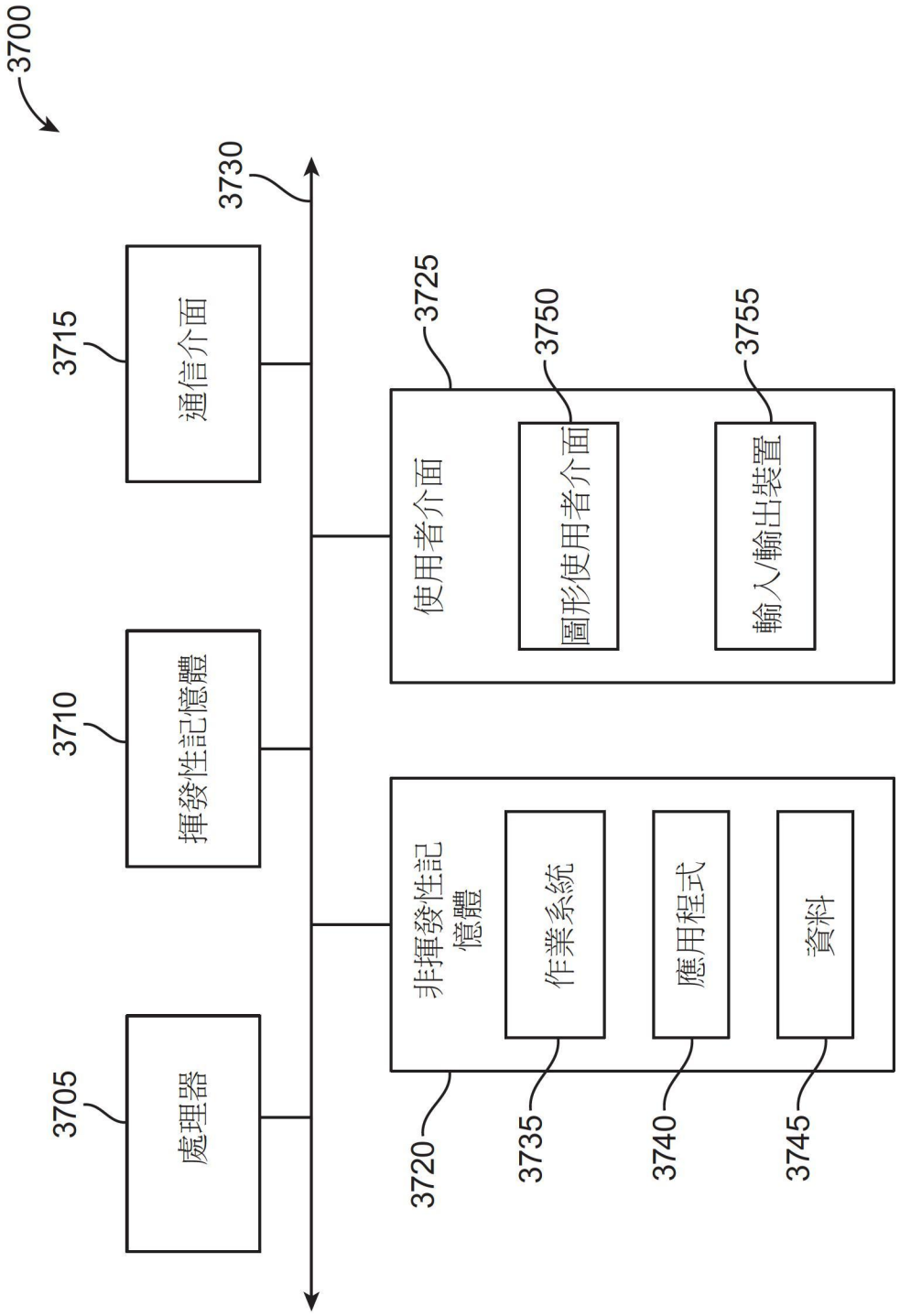
【圖34】


3500
總發票
未償付發票
25%
中國公司A
發票號
來自
自2019年2月11日 發票金額 發票到期日期
4158241228 $7,876.00 2019年2月18日
自2019年2月8日 發票金額 發票到期日期
4158244885 $1,866.00 2019年2月15日
自2019年1月22日 發票金額 發票到期日期
4156584885 $1,852.00 2019年1月29日
自2019年2月8日 發票金額 發票到期日期
4152544885 $5,866.00 2019年1月13日
自2019年12月15日 發票金額 發票到期日期
4152258485 $5,194.00 2019年12月22日
4158241149 - ACME
60
申請融資
發票號及貸款金額
4158241228
$3,769 USD
請選擇一分支機構來申請融資
銀行A
銀行B
銀行C
請選擇您的貸款賬號
123-456-780-909
取消
提交
OOLU
直接支付
申請融資
發票到期日期
2019年1月29日
258240334
收費金額
236.00
收貨地點
香港
自2019年3月8日
最終目的地
鹿特丹

【圖35】



【圖36】


3700
3730
3715
通信介面
3725
3750
3755
使用者介面
圖形使用者介面
輸入/輸出裝置
3710
揮發性記憶體
非揮發性記憶體
作業系統
應用程式
資料
3705
處理器
3720
3735
3740
3745

【圖37】