202139667

(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 202139667 A

(43)公開日： 中華民國 110 (2021) 年 10 月 16 日

(21)申請案號：110105827 (22)申請日： 中華民國 110 (2021) 年 02 月 19 日

(51)Int. Cl.： *H04L29/06 (2006.01)* *H04L9/32 (2006.01)*

(30)優先權：2020/02/19 英國 2002285.1

2020/12/21 英國 2020279.2

2021/02/18 英國 2102314.8

(71)申請人：安地卡及巴布達商區塊鏈控股有限公司 (安地卡及巴布達) NCHAIN HOLDINGS LIMITED (AG)

安地卡及巴布達

(72)發明人：美伊 安德魯 J MEE, ANDREW JAMES (GB)；蘭德 理查 C RAND, RICKY CHARLES (GB)；戴維斯 傑克 O DAVIES, JACK OWEN (GB)

(74)代理人：劉法正；尹重君

申請實體審查：無 申請專利範圍項數：98 項 圖式數：18 共 124 頁

(54)名稱

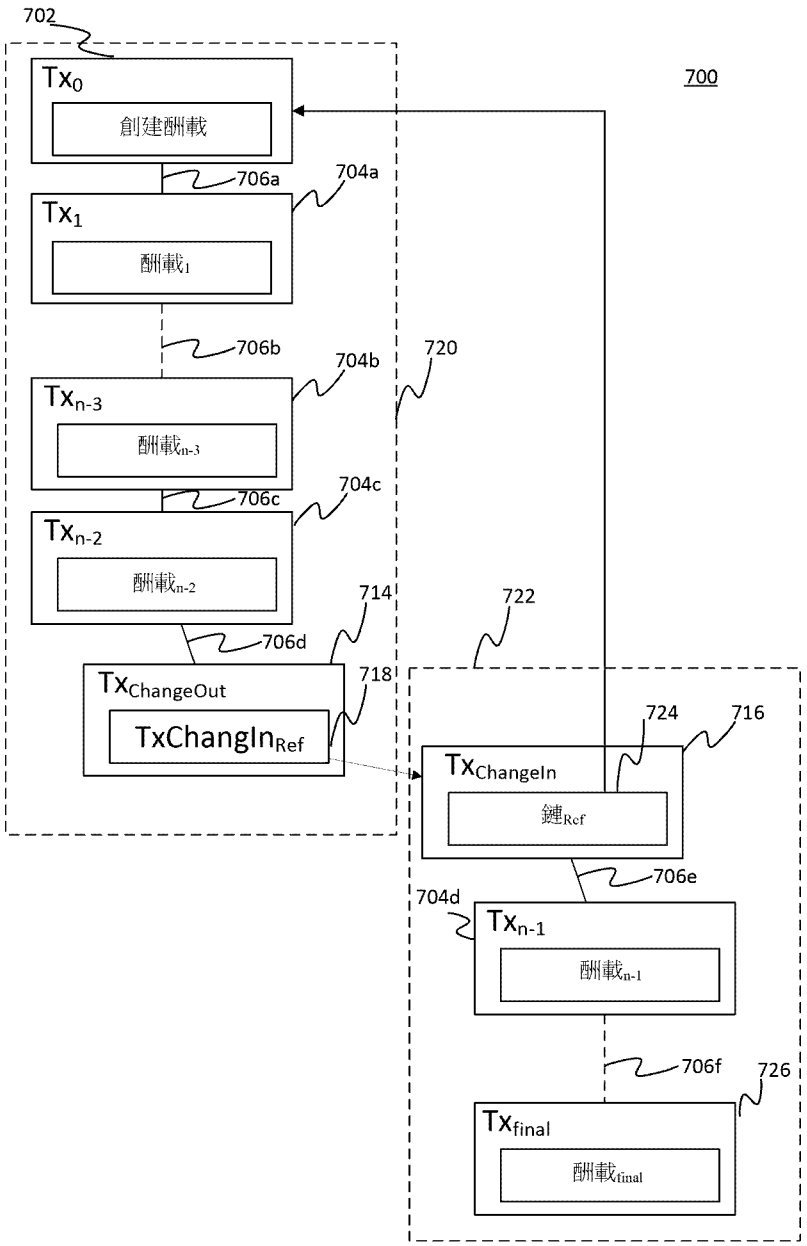
電腦實施系統及方法

(57)摘要

在一個態樣中，本揭露內容提議用於實施一有序唯加資料登錄系統之方法、裝置、系統及資料結構。詳言之，一種方法包含創建一第一類型之一交易，該交易包含與來自一組交易中之一最新交易的一交易輸出相關聯之一輸入。接著創建一第二類型之一交易。最終，將該第二類型之該交易及該第一類型之該交易二者提交至區塊鏈。

In one aspect, the present disclosure proposes methods, devices, systems, and data structures for implementing an ordered, append-only data logging system. In particular a method comprises creating a transaction of a first type comprising an input associated with a transaction output from a latest transaction in the set of transactions. Then creating a transaction of a second type. Finally submitting both the transaction of the second type and the transaction of the first type to the blockchain.

指定代表圖：



【圖7A】

符號簡單說明：

700:資料結構

702:第一交易

704a,704b,704c,704d:附加交易

706a,706b,706c,706d,706e,706f:引用

714,716:資料結構

718:正向引用

720,722:塵埃鏈

724:鏈引用

726:最終交易

202139667

【發明摘要】

【中文發明名稱】

電腦實施系統及方法

【英文發明名稱】

COMPUTER IMPLEMENTED SYSTEM AND METHOD

【中文】

在一個態樣中，本揭露內容提議用於實施一有序唯加資料登錄系統之方法、裝置、系統及資料結構。詳言之，一種方法包含創建一第一類型之一交易，該交易包含與來自一組交易中之一最新交易的一交易輸出相關聯之一輸入。接著創建一第二類型之一交易。最終，將該第二類型之該交易及該第一類型之該交易二者提交至區塊鏈。

【英文】

In one aspect, the present disclosure proposes methods, devices, systems, and data structures for implementing an ordered, append-only data logging system. In particular a method comprises creating a transaction of a first type comprising an input associated with a transaction output from a latest transaction in the set of transactions. Then creating a transaction of a second type. Finally submitting both the transaction of the second type and the transaction of the first type to the blockchain.

【指定代表圖】　圖7A

【代表圖之符號簡單說明】

700:資料結構
702:第一交易
704a,704b,704c,704d:附加交易
706a,706b,706c,706d,706e,706f:引用
714,716:資料結構
718:正向引用
720,722:塵埃鏈
724:鏈引用
726:最終交易

【特徵化學式】

無

【發明說明書】

【中文發明名稱】

電腦實施系統及方法

【英文發明名稱】

COMPUTER IMPLEMENTED SYSTEM AND METHOD

【技術領域】

發明領域

【0001】 本揭露內容係關於用於使用分散式分類帳(亦即區塊鏈)儲存資料之方法、裝置、系統及資料結構。更具體言之，本揭露內容提供用於有序、唯加資料項目之儲存。

【先前技術】

發明背景

【0002】 區塊鏈係指分散式資料結構之形式，其中區塊鏈之複本被維護在分散式同級間(P2P)網路(在下文稱作「區塊鏈網路」)之多個節點中之每一者處並被廣泛公佈。該區塊鏈包含一系列資料區塊，其中每一區塊包含一或多個交易。除了所謂的「創幣交易」以外，每一交易亦按一序列指向先前的交易，該序列可能跨越一或多個區塊，直至一或多個創幣交易為止。下文論述創幣交易。經提交至區塊鏈網路之交易包括於新區塊中。新區塊係藉由常常被稱作「挖掘」之程序而創建，其涉及多個節點中之每一者競爭以執行「工作量證明」，亦即基於等待包括於區塊鏈的新區塊中之有序及經驗證未決交易之經界定集合的表示而解決密碼謎題。應注意，可在節點處修剪區塊鏈，並且可藉由僅公佈區塊標頭來實現區塊的公佈。

【0003】 區塊鏈中之交易用以執行以下各者中之一或多者：傳達數位資產(亦即，數個數位符記)，以在虛擬化分類帳或登記表中排序一組日誌條目，以接

收及處理時戳條目，及/或按時間次序索引指標。亦可利用區塊鏈以便對區塊鏈之頂部上的額外功能性分層。區塊鏈協定可允許將額外使用者資料或資料之索引儲存在交易中。對於可儲存於單個交易內之最大資料容量不存在預先指定之限制，且因此可併入愈來愈複雜之資料。舉例而言，此可用於將電子文件、或音訊或視訊資料儲存在區塊鏈中。

【0004】 區塊鏈網路的節點(其常常被稱作「挖掘者」)執行將在下文詳細描述之分散式交易登記及認證程序。總之，在此程序期間，節點驗證交易且將其插入至區塊範本中，針對該區塊範本，其試圖識別有效的工作量證明解決方案。一旦發現了有效的解決方案，即將新區塊傳播至網路之其他節點，因此使得每一節點能夠在區塊鏈上記錄新區塊。為了使交易記錄於區塊鏈中，使用者(例如，區塊鏈用戶端應用程式)將交易發送至網路節點中之一者以供傳播。接收交易之節點可快速找到將經驗證交易併入至新區塊中的工作量證明解決方案。每一節點經組配以推行相同節點協定，其將包括用於待有效之交易的一或多個條件。無效交易將不被傳播或併入至區塊中。假設交易經驗證且藉此經接受至區塊鏈上，則交易(包括任何使用者資料)將因此在區塊鏈網路中之節點中之每一者處保持被登記及索引化為不可變公用記錄。

【0005】 成功地解決工作量證明難題以創建最新區塊之節點通常係以被稱作「創幣交易」之新交易被獎勵，該新交易分配一定金額之數位資產，亦即數個符記。無效交易之偵測及拒絕係藉由競爭節點的動作而被推行，該等競爭節點充當網路之代理並且被激勵以報告且阻止非法行為。資訊之廣泛公佈允許使用者連續地審核節點之效能。純粹區塊標頭之公佈允許參與者確保區塊鏈之持續完整性。

【0006】 在「基於輸出」之模型(有時被稱作基於 UTXO 之模型)中，給定交易之資料結構包含一或多個輸入及一或多個輸出。任何可支出輸出都包含一

元素，該元素指定可自交易之進行序列中得出的一定金額之數位資產。可支出輸出有時被稱作 UTXO (「未支出交易輸出」)。該輸出可進一步包含鎖定指令碼，其指定用於未來兌換該輸出之條件。鎖定指令碼為述詞，其定義驗證及轉移數位符記或資產所必需的條件。交易(除了創幣交易以外)的每一輸入包含指向先前交易中之此輸出的指標(亦即，參考)，並且可進一步包含用於解鎖所指向的輸出的鎖定指令碼之解鎖指令碼。因此，考慮一對交易，將其稱為第一交易及第二交易(或「目標」交易)。該第一交易包含至少一個輸出，其指定一定金額之數位資產且包含定義解鎖該輸出之一或多個條件的鎖定指令碼。第二目標交易包含至少一個輸入，其包含指向第一交易之輸出的指標，及用於解鎖第一交易之輸出的解鎖指令碼。

【0007】 在此模型中，當第二目標交易經發送至區塊鏈網路以在區塊鏈中傳播及記錄時，在每一節點處應用之有效性準則中之一者將係解鎖指令碼滿足定義於第一交易之鎖定指令碼中的所有一或多個條件。另一準則將為第一交易之輸出尚未由另一較早有效的交易兌換。發現根據此等條件中之任一者目標交易為無效的任何節點將不會傳播該目標交易(作為有效交易，但可能登記無效交易)，亦不將該目標交易包括在新區塊中以記錄在區塊鏈中。

【0008】 交易模型之替代類型係基於帳戶之模型。在此狀況下，每一交易都不會藉由返回參考一系列過去交易中的先前交易之 UTXO 來定義要轉移的金額，而是參考絕對帳戶餘額。所有帳戶的當前狀態由獨立於區塊鏈的節點儲存，並不斷更新。

【0009】 儘管區塊鏈技術由於密碼貨幣實施之使用而為最廣泛已知的，但數位企業家正在探索比特幣所基於之密碼安全系統及可儲存於區塊鏈上以實施新系統之資料二者的使用。區塊鏈技術在區塊鏈可用於不限於密碼貨幣範圍之自動任務及程序時將非常有利。此類解決方案將能夠利用區塊鏈之益處(例如，

事件之永久性防篡改記錄、分散式處理等)，同時在其應用中變得更通用。

【0010】 當前研究之一個領域係使用區塊鏈用於實施「智慧型合約」。此等智慧型合約係經設計以使機器可讀合約或協定之條款之執行自動化的電腦程式。不同於將以自然語言撰寫之傳統合約，智慧型合約係包含可處理輸入以產生結果之規則的機器可執行程式，該等規則接著可取決於彼等結果而使得執行動作。區塊鏈相關關注之另一領域係使用「符記」(或「彩色幣」)以經由區塊鏈表示及轉移真實世界實體。潛在地敏感或秘密之項目可由符記表示，符記不具有可辨別之含義或值。符記因此充當允許自區塊鏈引用真實世界項目之識別符。

【0011】 在利用區塊鏈的優點以提供事件之永久性防篡改記錄的同時，上文提及的實例或情境需要用戶端包括或實施軟體及/或硬體以用於實施管理數位資產、用於橢圓曲線數位簽章演算法(ECDSA)之密碼密鑰的功能性，能夠實施區塊鏈交易構造及可存取區塊鏈庫。英國專利申請案第 2002285.1 號(以 nChain Holdings Limited 之名稱在 2020 年 2 月 19 日提交)描述用於與區塊鏈相關聯之一或多個服務的平台，其中與用戶端相關聯之資料或資訊可藉由以下方法、裝置及系統簡單地、安全地且立即經寫入至區塊鏈中或自區塊鏈獲得，而無需此類用戶端實施用於使用區塊鏈之任何處理或功能性，同時仍能夠利用與區塊鏈相關聯之所有優點，該等方法、裝置及系統提供用於與區塊鏈相關聯之一或多個服務的應用程式設計介面(API)。對於此類平台，亦需要確保資料在使用或經由平台進入區塊鏈中後不被篡改或修改，且可獨立地被審核。因此，本揭露內容描述一或多種技術，其確保基於與平台相關聯或經由平台提供之資料及/或自任意用戶端提供之任意序列之資料項目的一連串事件係防篡改的，且可獨立地被遍歷及認證。

【發明內容】

發明概要

【0012】在一第一態樣中，本揭露內容提議用於實施一有序唯加資料儲存之方法、裝置、資料結構及系統。根據此態樣之一資料結構包含：一第一交易及一第二交易。該第一交易包含：一第一輸出及一第一資料項目之一表示。該第二交易包含：該第一資料項目之另一表示、一第二資料項目之一表示、與該第一輸出相關聯之一第一輸入，及一第二輸出。

【0013】一種與根據該第一態樣之一區塊鏈系統中之一組交易相關聯的方法，其包含以下步驟：接收一請求，該請求觸發待儲存在該區塊鏈上之一資料項目之一表示；獲得該組交易中之一最新交易；創建一新區塊鏈交易，該新區塊鏈交易包含：與來自該最新交易之一輸出相關聯的一輸入；一輸出；待儲存在該區塊鏈上之該資料項目之該表示；及對該最新交易之一引用；將該交易提交至該區塊鏈。

【0014】在一第二態樣中，本揭露內容提議用於實施一有序唯加資料儲存之方法、裝置、資料結構及系統。一種根據該第二態樣之方法包含以下步驟：創建一第一類型之一交易，該交易包含與來自該組交易中之一最新交易之一交易輸出相關聯的一輸入；創建一第二類型之一交易；將該第二類型之該交易提交至該區塊鏈；及將該第一類型之該交易提交至該區塊鏈。

【0015】一種根據該第二態樣之資料結構，該資料結構包含：一第一類型之一交易，其包含一輸出，該輸出包含對一第二類型之一交易之一第一引用；及該第二類型之該交易。

【0016】一種根據該第二態樣之用於正向遍歷一組交易之方法，其包含以下步驟：(a)獲得該交易鏈中之一當前交易；(b)判定該當前交易為一第一類型之一交易且基於該判定，進行以下步驟(i)、(ii)及(iii)：i.基於該第一類型之該交易獲得對一第二類型之一交易之一引用；ii.基於對該第二類型之該交易之該引用獲得該第二類型之該交易；及 iii.繼續至步驟(c)，其中將該第二類型之該交易作為

該當前交易；(c)獲得一當前交易識別符；(d)獲得引用該當前交易識別符之另一交易；及(e)自該另一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【0017】 該第二態樣任擇地包括該第一態樣之特徵。

【0018】 在一第三態樣中，本揭露內容提議用於實施一有序唯加資料儲存之方法、裝置、資料結構及系統。一種根據該第三態樣之方法包含以下步驟：創建一第二類型之一交易；將該第二類型之該交易提交至該區塊鏈；創建一第一類型之一交易，該交易包含與來自該組交易中之一最新交易之一交易輸出相關聯的一輸入及對該第二類型之該交易之一引用；在於該區塊鏈上確認該第二類型之該交易之後將該第一類型之該交易提交至該區塊鏈。

【0019】 該第三態樣任擇地包括第一及第二態樣之特徵。

【0020】 在一第四態樣中，本揭露內容提議用於實施一有序唯加資料儲存之方法、裝置、資料結構及系統。一種資料結構包含該第一類型之一交易及一第二類型之一交易，該第二類型之該交易包含至少一個輸入。該第一類型之該交易包含對該第二類型之該交易之一引用，其中該引用係基於該至少一個輸入中之至少一者。

【0021】 該第四態樣任擇地包括第一、第二及第三態樣之特徵。

【0022】 在一第五態樣中，本揭露內容提議用於實施一有序唯加資料儲存之方法、裝置、資料結構及系統。一種根據該第五態樣之資料結構包含：一第一類型之一交易，其包含對一第二類型之一交易之一第一引用；及該第二類型之該交易，其包含對該第一類型之該交易之一第二引用及至少一個輸入。較佳地，該第一引用係基於至該第二類型之該交易之該至少一個輸入。較佳地，該第二引用為該第一類型之該交易之交易 id。

【0023】 一種根據該第五態樣之用於反向遍歷根據該第五態樣之一資料結

構的方法包含以下步驟：(a)獲得該交易鏈中之一當前交易；(b)判定該當前交易為一第二類型之一交易且基於該判定，進行以下步驟(i)、(ii)、(iii)：i.基於該第二類型之該交易獲得對一第一類型之一交易之一引用；ii.基於對該第一類型之該交易之該引用獲得該第一類型之該交易；iii.繼續至步驟(c)，其中將該第一類型之該交易作為該當前交易；(c)自該當前交易獲得前一交易之一交易識別符；(d)基於前一交易之該交易識別符獲得該前一交易；(e)自該前一交易作為該當前交易開始進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【0024】 該第五態樣任擇地包括第一、第二、第三及第四態樣之特徵。

【0025】 在一第六態樣中，本揭露內容提議用於實施一有序唯加資料儲存之方法、裝置、資料結構及系統。一種根據該第六態樣之資料結構包含：一第一類型之一交易，其包含對一轉入交易之一第一引用；及該第二類型之該交易，其包含對該第一類型之該交易之一第二引用。該第一引用係基於該第二類型之該交易的該至少一個輸入中之至少一者。該第二引用係基於該第一類型之該交易的該至少一個輸入中之至少一者。

【0026】 該第六態樣任擇地包括第一、第二、第三、第四及/或第五態樣之特徵。

【0027】 在一第七態樣中，本揭露內容提議用於實施有序唯加資料儲存之方法，該有序唯加資料儲存包含一第三類型之交易。該第三類型任擇地為一交會交易。

【0028】 一種用於正向遍歷一組區塊鏈交易之方法，其包含以下步驟：(a)獲得該組交易中之一當前交易；(b)判定該當前交易為一第三類型之一交易且基於該判定，進行以下步驟(i)、(ii)、(iii)及(iv)：(i)獲得包含對前一交易之一引用之輸入的一索引；(ii)獲得與包含對該前一交易之一引用之該輸入相關聯之輸出；(iii)基於經獲得輸出獲得下一交易；及(iv)繼續至步驟(c)，其中將該下一交易作為

該當前交易；(c)獲得一當前交易識別符；(d)獲得引用該當前交易識別符之另一交易；及(e)自該另一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【0029】 一一種用於反向遍歷一組區塊鏈交易之方法，其包含以下步驟：(a)獲得該組交易中之一當前交易；(b)判定該當前交易為一第三類型之一交易且基於該判定，進行以下步驟(i)、(ii)、(iii)及(iv)：(i)獲得該當前交易之一輸入之一索引；(ii)基於該當前交易之經獲得輸入獲得對前一交易之一引用；(iii)基於引用獲得該前一交易；及(iv)繼續至步驟(c)，其中將該前一交易作為該當前交易；(c)自該當前交易獲得該前一交易之一交易識別符；(d)基於前一交易之該交易識別符獲得該前一交易；(e)自該前一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【0030】 該第七態樣任擇地包括第一、第二、第三、第四、第五及第六態樣之特徵。較佳地，該第七態樣亦包含與正向及反向遍歷方法相關的實施例，該等正向及反向遍歷方法與態樣二、三、四、五及六相關聯。

【圖式簡單說明】

現將僅作為實例且參考附圖描述本揭露內容之態樣及實施例，在附圖中：

【0031】 圖 1 為描繪用於實施區塊鏈之實例系統的示意圖。

【0032】 圖 2 為描繪用於區塊鏈系統中之實例交易的示意圖。

【0033】 圖 3A 及圖 3B 為描繪實例電子錢包系統及使用者介面之圖。

【0034】 圖 4 為描繪包含軟體模組之實例區塊鏈節點之示意圖。

【0035】 圖 5 為根據第一態樣之描繪儲存日誌條目及對應的日誌條目之一系列交易的概述之示意圖。

【0036】 圖 6A、圖 6B 及圖 6C 為根據第一態樣之描繪資料結構之示意圖。

【0037】 圖 6D 為根據第一態樣的描繪用於實施有序唯加資料儲存系統之

方法之流程圖。

【0038】 圖 7A 及圖 7B 為根據第二態樣之描繪資料結構之示意圖。

【0039】 圖 8 為根據第二態樣的描繪用於實施有序唯加資料儲存系統之方法之流程圖。

【0040】 圖 9 為根據第二態樣的用於遍歷有序唯加資料儲存結構之方法的流程圖。

【0041】 圖 10 為根據第三態樣的描繪用於有序唯加資料儲存之資料結構之示意圖。

【0042】 圖 11 為根據第四態樣的描繪用於有序唯加資料儲存之資料結構之示意圖。

【0043】 圖 12 為根據第五態樣的描繪用於有序唯加資料儲存之資料結構之示意圖。

【0044】 圖 13 為根據第五態樣的用於遍歷有序唯加資料儲存結構之方法的流程圖。

【0045】 圖 14 為根據第六態樣的描繪用於有序唯加資料儲存之資料結構之示意圖。

【0046】 圖 15 為根據一態樣之描繪用於與區塊鏈相關聯的多個服務之平台的概述之示意圖。

【0047】 圖 16 為根據一態樣之描繪與區塊鏈相關聯的多個服務之平台的組件之示意圖。

【0048】 圖 17 為說明其中可實施本揭露內容之各種態樣及實施例的計算環境之示意圖。

【0049】 圖 18 為根據第八態樣的描繪用於有序唯加資料儲存之資料結構之示意圖。

【實施方式】

較佳實施例之詳細說明

【0050】 現在作為說明參考附圖描述經揭示方法之一些特定組件及實施例，在該等附圖中，相同附圖標記指代相同特徵。

實例系統概述

【0051】 圖 1 展示用於實施區塊鏈 150 之實例系統 100。系統 100 可包含封包交換式網路 101，通常為諸如網際網路之廣域網際網路。封包交換式網路 101 包含多個區塊鏈節點 104，該等區塊鏈節點可經配置以在封包交換式網路 101 內形成同級間(P2P)網路 106。雖然未說明，但區塊鏈節點 104 可經配置為接近完整的圖。每一區塊鏈節點 104 因此高度連接至其他區塊鏈節點 104。

【0052】 每一區塊鏈節點 104 包含同級者之電腦設備，其中節點 104 中之不同節點屬不同同級者。每一區塊鏈節點 104 包含：處理設備，其包含一或多個處理器，例如一或多個中央處理單元(CPU)、加速器處理器、特殊應用處理器及/或場可規劃閘陣列(FPGA)；及其他設備，諸如特殊應用積體電路(ASIC)。每一節點亦包含記憶體，亦即呈非暫時性電腦可讀媒體之形式之電腦可讀儲存裝置。該記憶體可包含一或多個記憶體單元，其使用一或多個記憶體媒體，例如，諸如硬碟之磁性媒體；諸如固態驅動機(SSD)、快閃記憶體或 EEPROM 之電子媒體；及/或諸如光碟驅動機之光學媒體。

【0053】 區塊鏈 150 包含一系列資料區塊 151，其中在分散式或區塊鏈網路 101 中之多個區塊鏈節點 104 中之每一者處維護區塊鏈 150 之各別複本。如上文所提及，維護區塊鏈 150 之複本不一定意謂完整地儲存區塊鏈 150。實情為，只要每一區塊鏈節點 150 儲存每一區塊 151 之(下文論述的)區塊標頭，即可修剪區塊鏈 150 之資料。該鏈中之每一區塊 151 包含一或多個交易 152，其中此上下文中之交易係指一種資料結構。資料結構之性質將取決於用作交易模型或

方案之一部分的交易協定之類型。給定區塊鏈將始終使用一個特定交易協定。在一個常見類型之交易協定中，每一交易 152 之資料結構包含至少一個輸入及至少一個輸出。每一輸出指定表示如財產之數位資產之數量的金額，其實例為使用者 103，該輸出以密碼方式鎖定至該使用者(需要彼使用者之簽名或其他解決方案以便解鎖且藉此兌換或支出)。每一輸入均指向先前交易 152 之輸出，藉此鏈接交易。

【0054】 每一區塊 151 亦包含區塊指標 155，其指向該鏈中之先前創建之區塊 151 以便界定區塊 151 之依序次序。每一交易 152 (除了創幣交易以外)包含指正向述交易之指標，以便界定交易序列之次序(注意：允許交易 152 之序列形成分支)。區塊 151 之鏈一直返回至起源區塊(Gb) 153，該起源區塊為該鏈中之第一區塊。鏈 150 中較早的一或多個原始交易 152 指向起源區塊 153，而非先前交易。

【0055】 區塊鏈節點 104 中之每一者經組配以將交易 152 轉遞至其他區塊鏈節點 104，且藉此使得交易 152 在整個網路 106 中傳播。每一區塊鏈節點 104 經組配以創建區塊 151，且將相同區塊鏈 150 之各別複本儲存在其各別記憶體中。每一區塊鏈節點 104 亦維護等待併入至區塊 151 中之交易 152 的有序集合 154。有序集合 154 常常被稱作「記憶體池」。本文中之此術語不意欲限於任何特定區塊鏈、協定或模型。該術語係指交易之有序集合，節點 104 將交易之有序集合接受為有效的且用於交易之有序集合之節點 104 必須不接受嘗試支出相同輸出之任何其他交易。

【0056】 在給定的目前的交易 152j 中，該(或每一)輸入包含引用交易序列中之先前交易 152i 之輸出之指標，指定此輸出將在目前的交易 152j 中被兌換或「支出」。一般而言，先前交易可為有序集合 154 或任何區塊 151 中之任何交易。當目前的交易 152j 經創建或甚至發送至網路 106 時無需必定存在先前交易 152i，

但先前交易 152i 將需要存在且被驗證以便使目前的交易為有效的。因此，本文中之「先前」係指藉由指標鏈接之邏輯序列中的前置者，未必在時間序列中創建或發送的時間，且因此，其不一定排除無序地創建或發送交易 152i、152j (參見下文關於孤立交易之論述)。先前交易 152i 可同樣地被稱作前期或前置交易。

【0057】 目前的交易 152j 之輸入亦包含輸入授權，例如先前交易 152i 之輸出鎖定至的使用者 103a 之簽名。繼而，目前的交易 152j 之輸出可以密碼方式鎖定至新使用者或實體 103b。目前的交易 152j 因此可將先前交易 152i 之輸入中所定義之金額轉移至如目前的交易 152j 之輸出中定義的新使用者或實體 103b。在一些狀況下，交易 152 可具有多個輸出以在多個使用者或實體(多個使用者或實體中之一者可為原始使用者或實體 103a 以便給出改變)之間劃分輸入金額。在一些狀況下，交易亦可具有多個輸入以將來自一或多個先前交易之多個輸出的金額聚集在一起，且重新分配至當前交易之一或多個輸出。

【0058】 根據基於輸出之交易協定，諸如比特幣，當諸如使用者或機器 103 之實體希望實行新交易 152j 時，實體接著將新交易自其電腦終端 102 發送至接收者。該實體或接收者將最終將此交易發送至網路 106 之區塊鏈節點 104 中之一或多者(該等區塊鏈節點如今通常為伺服器或資料中心，但原則上可為其他使用者終端)。亦不排除實行新交易 152j 之實體 103 可將交易發送至區塊鏈節點 104 中之一或多者，且在一些實例中不發送至接收者。接收交易之區塊鏈節點 104 檢查根據應用於區塊鏈節點 104 中之每一者處之區塊鏈節點協定，該交易是否為有效的。區塊鏈節點協定通常需要區塊鏈節點 104 檢查新交易 152j 中之密碼簽名是否與預期簽名匹配，此取決於交易 152 之有序序列中之前述交易 152i。在此基於輸出之交易協定中，此可包含檢查包括於新交易 152j 之輸入中之實體 103 的密碼簽名或其他授權是否與先前交易 152i 之輸出中所定義之新交易指派之條件匹配，其中此條件通常包含至少檢查新交易 152j 之輸入中之密碼簽名或

其他授權是否解鎖新交易之輸入鏈接至之前述交易 152i 的輸出。該條件可至少部分地由包括於先前交易 152i 之輸出中的指令碼界定。替代地，該條件可簡單地由單獨的區塊鏈節點協定固定，或其可歸因於指令碼及區塊鏈節點協定之組合。無論如何，若新交易 152j 係有效的，則區塊鏈節點 104 將其轉遞至區塊鏈網路 106 中之一或多個其他區塊鏈節點 104。此等其他區塊鏈節點 104 根據相同區塊鏈節點協定應用相同測試，且因此將新交易 152j 轉遞至一或多個其他節點 104 上，等等。以此方式，新交易在區塊鏈節點 104 之整個網路中傳播。

【0059】 在基於輸出之模型中，是否指派給定輸出(例如，UTXO)之定義係其是否已根據區塊鏈節點協定而由另一正向交易 152j 的輸入有效地兌換。用於交易係有效的另一條件為該交易嘗試指派或兌換之先前交易 152i 之輸出尚未由另一交易指派/兌換。再次，若並非有效的，則不在區塊鏈 150 中傳播或記錄交易 152j (除非經標記為無效的，且經傳播以用於警告)。此防止雙重支出，其中交易者嘗試多於一次地指派相同交易之輸出。基於帳戶之模型另一方面藉由維護帳戶餘額來防止雙重支出。因為再次存在經界定的交易次序，所以帳戶餘額在任一個時間均具有單個經界定狀態。

【0060】 除了驗證交易之外，區塊鏈節點 104 亦快速率先在通常被稱作挖掘之程序中創建交易區塊，該程序係由「工作量證明」支援。在區塊鏈節點 104 處，新交易經添加至有效交易的有序集合 154，該等有效交易尚未出現在經記錄在區塊鏈 150 上之區塊 151 中。區塊鏈節點接著快速藉由嘗試解決密碼謎題而組合來自交易 154 之有序集合的交易 152 之新有效區塊 151。通常，此包含搜索「隨機數」值，使得當隨機數與交易 154 之有序集合的表示串接且經散列時，散列之輸出接著符合預定條件。例如，預定條件可為散列之輸出具有某一預定數量的前置零。應注意，此恰好為一個特定類型之工作量證明謎題，且不排除其他類型。散列函數的屬性為散列函數具有相對於其輸入的不可預測的輸出。因此，此

搜索可僅藉由蠻力執行，因此在正嘗試解決謎題之每一區塊鏈節點 104 處消耗了大量的處理資源。

【0061】 解決該謎題之第一區塊鏈節點 104 將此宣佈給網路 106，從而提供該解決方案作為證明，其接著可由網路中之其他區塊鏈節點 104 容易地檢查(一旦給定散列之解決方案，即直接檢查其是否使得散列之輸出滿足該條件)。第一區塊鏈節點 104 將區塊傳播至接受該區塊且因此推行協定規則之其他節點的臨限共識。交易之有序集合 154 接著藉由區塊鏈節點 104 中之每一者而在區塊鏈 150 中經記錄為新區塊 151。區塊指標 155 亦經指派至指向鏈中之先前創建的區塊 151n-1 之新區塊 151n。創建工作量證明解決方案所需的例如呈散列形式之大量工作傳信第一節點 104 之意圖以遵循區塊鏈協定之規則。此類規則包括在交易將相同輸出指派為先前驗證之交易之情況下，不接受該交易為有效的，除非該交易已知為雙重支出。一旦被創建，則區塊 151 無法被修改，此係由於在區塊鏈網路 106 中之區塊鏈節點 104 中之每一者處辨識且維護該區塊。區塊指標 155 亦將依序次序強加至區塊 151。由於交易 152 在網路 106 中之每一區塊鏈節點 104 處經記錄在有序區塊中，因此此提供交易的不可變公用分類帳。

【0062】 應注意，快速在任何給定時間解決該謎題之不同區塊鏈節點 104 可基於尚待公佈的交易之有序集合 154 之不同快照在任何給定時間來這樣做，此取決於其何時開始搜索解決方案或接收交易之次序。不論誰首先解決其各別謎題均界定哪些交易 152 且以何種次序包括於下一新區塊 151n 中，且未公佈交易的當前集合 154 經更新。區塊鏈節點 104 接著繼續快速自未公佈交易的最新界定之未完成的有序集合 154 創建區塊，等等。亦存在用於解決可能出現的任何「分支」之協定，其係二個區塊鏈節點 104 在彼此極短的時間內解決其謎題，使得區塊鏈的衝突視圖在節點 104 之間傳播。簡言之，分支的最長的支叉變為決定性區塊鏈 150。應注意，此不應影響網路的使用者或代理，此係因為相同交易將

出現在二個分支中。

【0063】 根據比特幣區塊鏈(及大多數其他區塊鏈)，成功地建構新區塊 104 之節點被授予在新特別種類的交易中指派經接受金額的數位資產之能力，該交易分配經界定數量的數位資產(與將一定金額之數位資產自一個代理或使用者轉移至另一代理或使用者之代理間或使用者間交易相對)。此特別類型之交易通常被稱作「創幣交易」，但亦可被稱為「起始交易」。其通常形成新區塊 151n 的第一交易。工作量證明傳信建構新區塊之節點的意圖，以遵循協定規則，從而允許稍後兌換此特別交易。在可兌換此特別交易之前，區塊鏈協定規則可能需要成熟期，例如 100 個區塊。常常，常規(非生成)交易 152 亦將在其輸出中之一者中指定額外交易費用，以進一步獎勵創建了在其中公佈彼交易之區塊 151n 的區塊鏈節點 104。此費用通常被稱作「交易費用」，且在下文論述。

【0064】 歸因於交易驗證及公佈中涉及之資源，通常，至少區塊鏈節點 104 中之每一者採用伺服器之形式，該伺服器包含一或多個實體伺服器單元或甚至整個資料中心。然而，原則上，任何給定區塊鏈節點 104 可採用被網路連接在一起的使用者終端或使用者終端之群組的形式。

【0065】 每一區塊鏈節點 104 之記憶體儲存軟體，該軟體經組配以在區塊鏈節點 104 之處理設備上運行以便執行其各別角色且根據區塊鏈節點協定處置交易 152。應理解，本文中歸因於區塊鏈節點 104 之任何動作可由在各別電腦設備之處理設備上運行的軟體執行。節點軟體可實施於應用層或諸如作業系統層或協定層之下部層或應用層及下部層之任何組合處的一或多個應用程式中。

【0066】 處於消費者角色之多個當事方 103 中之每一者的電腦設備 102 亦連接至網路 101。此等使用者可與區塊鏈網路交互，但不參與驗證、建構或傳播交易及區塊。此等使用者或代理 103 中之一些可在交易中充當發送者及接收者。其他使用者可與區塊鏈 150 交互，而未必充當發送者或接收者。舉例而言，一些

當事方可充當儲存實體，其儲存區塊鏈 150 之複本(例如，已自區塊鏈節點 104 獲得區塊鏈之複本)。

【0067】 當事方 103 中之一些或全部可作為不同網路(例如在區塊鏈網路 106 的頂部上覆疊之網路)之部分連接。區塊鏈網路(常常被稱作「用戶端」)之使用者可被稱為包括區塊鏈網路之系統的一部分；然而，此等使用者並非區塊鏈節點 104，此係因為其不執行區塊鏈節點需要的角色。實情為，每一當事方 103 可與區塊鏈網路 106 交互，且藉此藉由連接至區塊鏈節點 106 (亦即，與該區塊鏈節點通訊)而利用區塊鏈 150。出於說明性目的展示二個當事方 103 及其各別設備 102：第一當事方 103a 及他的/她的各別電腦設備 102a，及第二當事方 103b 及他的/她的各別電腦設備 102b。應理解，更多此類當事方 103 及其各別電腦設備 102 可存在且參與系統 100 中，但為方便起見不對其加以說明。每一當事方 103 可為個人或組織。僅僅作為說明，第一當事方 103a 在本文中被稱作 Alice，且第二當事方 103b 被稱作 Bob，但應瞭解，此不具限制性，且在本文中對 Alice 或 Bob 之任何引用可分別用「第一當事方」及「第二當事方」替換。

【0068】 每一當事方 103 之電腦設備 102 包含各別處理設備，該處理設備包含一或多個處理器，例如一或多個 CPU、GPU、其他加速器處理器、特殊應用處理器及/或 FPGA。每一當事方 103 之電腦設備 102 進一步包含記憶體，亦即呈非暫時性電腦可讀媒體之形式之電腦可讀儲存裝置。此記憶體可包含一或多個記憶體單元，其使用一或多個記憶體媒體，例如，諸如硬碟之磁性媒體；諸如 SSD、快閃記憶體或 EEPROM 之電子媒體；及/或諸如光碟機之光學媒體。每一當事方 103 之電腦設備 102 上之記憶體儲存軟體，該軟體包含經配置以在處理設備上運行之至少一個用戶端應用程式 105 的各別例項。應理解，本文中歸因於給定當事方 103 之任何動作可使用在各別電腦設備 102 之處理設備上運行的軟體來執行。每一當事方 103 之電腦設備 102 包含至少一個使用者終端，例如桌

上型或膝上型電腦、平板電腦、智慧型電話或諸如智慧型手錶之可佩戴式裝置。給定當事方 103 之電腦設備 102 亦可包含一或多個其他網路連接資源，諸如經由使用者終端存取之雲計算資源。

【0069】 用戶端應用程式 105 最初可在合適的電腦可讀儲存媒體上經提供至任何給定當事方 103 之電腦設備 102，例如自伺服器下載，或經提供於可移除儲存裝置上，該可移除儲存裝置諸如可移除 SSD、快閃記憶體鍵、可移除 EEPROM、可移除磁碟驅動器、磁性軟碟或磁帶、諸如 CD 或 DVD ROM 之光碟或可移除光碟機等。

【0070】 用戶端應用程式 105 包含至少一「電子錢包」功能。此具有二個主要功能性。二個功能性中之一者為使得各別當事方 103 能夠創建、授權(例如，簽署)及發送交易 152 至一或多個比特幣節點 104 以接著在區塊鏈節點 104 之整個網路中傳播且藉此包括於區塊鏈 150 中。另一功能性為將他或她當前擁有之數位資產的金額報告給各別當事方。在基於輸出之系統中，此第二功能性包含核對各種散佈在整個區塊鏈 150 中之交易 152 的輸出中所定義之金額，該等金額屬於所討論的當事方。

【0071】 注意：雖然各種用戶端功能性可經描述為整合至給定的用戶端應用程式 105 中，但此未必為限制性的，且實情為，本文中所描述的任何用戶端功能性反而可實施於一套二個或多於二個不同應用程式中，例如經由 API 介接，或一個應用程式為另一應用程式之外掛程式。更一般而言，用戶端功能性可實施在應用層或諸如作業系統之下部層或應用層及下部層之任何組合處。下文將關於用戶端應用程式 105 進行描述，但應瞭解，此並非限制性的。

【0072】 每一電腦設備 102 上之用戶端應用程式或軟體 105 的例項係操作性地耦接至網路 106 之區塊鏈節點 104 中之至少一者。此使得用戶端 105 之電子錢包功能能夠將交易 152 發送至網路 106。用戶端 105 亦能夠接觸區塊鏈節點

104 以便針對各別當事方 103 為接收者之任何交易查詢區塊鏈 150 (或實際上檢測區塊鏈 150 中之其他當事方之交易，此係由於在實施例中，區塊鏈 150 為公用設施，其部分地藉由其公用可見性而在交易中提供信任)。每一電腦設備 102 上之電子錢包功能經組配以根據交易協定來制定及發送交易 152。如上文所闡述，每一區塊鏈節點 104 運行軟體，該軟體經組配以根據區塊鏈節點協定來驗證交易 152，且轉遞交易 152 以便在整個區塊鏈網路 106 中傳播該等交易。交易協定及節點協定彼此對應，且給定交易協定與給定節點協定相配，其在一起實施給定交易模型。相同的交易協定用於區塊鏈 150 中之所有交易 152。相同節點協定係由網路 106 中之所有節點 104 使用。

【0073】 當給定當事方 103，比如 Alice，希望發送待包括於區塊鏈 150 中之新交易 152j 時，她接著根據相關交易協定來制定新交易(使用她的用戶端應用程式 105 中之電子錢包功能)。她接著將交易 152 自用戶端應用程式 105 發送至她連接至的一或多個區塊鏈節點 104。例如，此可為最佳地連接至 Alice 之電腦 102 的區塊鏈節點 104。當任何給定區塊鏈節點 104 接收新交易 152j 時，該區塊鏈節點根據區塊鏈節點協定及其各別角色來處置該新交易。此包含首先檢查最新接收的交易 152j 是否符合為「有效的」某一條件，不久將較詳細地論述該條件之實例。在一些交易協定中，可藉由包括於交易 152 中之指令碼基於每一交易來組配驗證條件。替代地，該條件可簡單地為節點協定之內置特徵，或可由指令碼及節點協定之組合來界定。

【0074】 只要最新接收的交易 152j 通過被視為有效的測試(亦即，只要其「經驗證」)，則接收交易 152j 之任何區塊鏈節點 104 將會將新經驗證交易 152 添加至在彼區塊鏈節點 104 處維護的交易之有序集合 154。此外，接收交易 152j 之任何區塊鏈節點 104 將會將經驗證交易 152 正向傳播至網路 106 中之一或多個其他區塊鏈節點 104。由於每一區塊鏈節點 104 應用相同協定，因此接著假設交

易 152j 係有效的，此意謂該交易將迅速在整個網路 106 中傳播。

【0075】 一旦被接納至在給定區塊鏈節點 104 處維護之交易的有序集合 154，則彼區塊鏈節點 104 將開始競爭以解決關於包括新交易 152 之交易的其各別有序集合 154 之最新版本的工作量證明謎題(前已述及，其他區塊鏈節點 104 可嘗試基於交易之不同有序集合 154 來解決謎題，但不論誰率先完成將定義包括於最新區塊 151 中之交易之有序集合。最終，區塊鏈節點 104 將針對包括 Alice 之交易 152j 的有序集合 154 之一部分來解決謎題)。一旦針對包括新交易 152j 之有序集合 154 進行工作量證明，則其不變地變為區塊鏈 150 中之區塊 151 之一者的一部分。每一交易 152 包含指向較早的交易之指標，因此亦不變地記錄交易之次序。

【0076】 不同區塊鏈節點 104 可首先接收給定交易之不同例項，且因此具有其例項在於新區塊 151 中公佈一個例項之前係「有效的」之衝突視圖，此時，所有區塊鏈節點 104 同意經公佈例項為唯一有效的例項。若區塊鏈節點 104 將一個例項接受為有效的且接著發現第二例項已經記錄在區塊鏈 150 中，則彼區塊鏈節點 104 必須接受此情形且將丟棄其最初接受之該例項(亦即，尚未在區塊 151 中公佈之例項) (亦即，將其視為無效的)。

【0077】 作為基於帳戶之交易模型之部分，由一些區塊鏈網路操作之交易協定之替代類型可被稱作「基於帳戶」之協定。在基於帳戶之狀況下，每一交易都不會藉由返回參考一系列過去交易中的先前交易之 UTXO 來定義要轉移的金額，而是參考絕對帳戶餘額。所有帳戶的當前狀態由獨立於區塊鏈的彼網路之節點儲存，並不斷更新。在此系統中，使用帳戶之運行交易記錄(亦被稱作「位置」)來對交易進行排序。作為交易之密碼簽名之部分，此值係由發送者簽名，且作為交易參考計算之部分，經散列。另外，任擇的資料欄位亦可在交易中簽名。例如，若前述交易 ID 包括於資料欄位中，則此資料欄位可指正向述交易。

基於 UTXO 之模型

【0078】 圖 2 說明實例交易協定。此為基於 UTXO 之協定的實例。交易 152 (簡稱為「Tx」)為區塊鏈 150 之基本資料結構(每一區塊 151 包含一或多個交易 152)。下文將參考基於輸出或基於「UTXO」之協定來描述。然而，此並不限於所有可能的實施例。應注意，雖然參考比特幣描述實例基於 UTXO 之協定，但其可同樣地實施於其他實例區塊鏈網路上。

【0079】 在基於 UTXO 之模型中，每一交易(「Tx」) 152 包含資料結構，其包含一或多個輸入 202 及一或多個輸出 203。每一輸出 203 可包含未支出的交易輸出(UTXO)，其可用作另一新交易之輸入 202 之來源(若尚未兌換 UTXO)。UTXO 包括指定數位資產之金額的值。此表示分散式分類帳上之符記的經設定數量。除了其他資訊之外，UTXO 亦可含有交易之交易 ID，該交易 ID 來自該交易。交易資料結構亦可包含標頭 201，該標頭可包含輸入欄位 202 及輸出欄位 203 之大小之指示符。標頭 201 亦可包括交易之 ID。在實施例中，交易 ID 為交易資料(不包括交易 ID 自身)之散列，且儲存於經提交至節點 104 之原始交易 152 的標頭 201 中。

【0080】 比如 Alice 103a 希望創建將所討論的一定金額之數位資產轉移至 Bob 103b 之交易 152j。在圖 2 中，Alice 之新交易 152j 經標記為「Tx1」。該交易需要一定金額之數位資產且將數位資產中的至少一些轉移至 Bob，該數位資產在序列中之先前交易 152i 之輸出 203 中鎖定至 Alice。先前交易 152i 在圖 2 中經標記為「Tx0」。Tx0 及 Tx1 僅為任意標籤。其未必意謂 Tx0 為區塊鏈 151 中之第一交易，或 Tx1 為池 154 中之緊接著的下一交易。Tx1 可指向任何先前(亦即，前期)交易，其仍具有鎖定至 Alice 之未支出的輸出 203。

【0081】 當 Alice 創建她的新交易 Tx1 時，或至少在她將新交易發送至網路 106 時，先前交易 Tx0 可能已經被驗證且經包括於區塊鏈 150 之區塊 151 中。

該交易彼時可能已經包括於區塊 151 中之一者中，或其可能仍在有序集合 154 中等待，在此狀況下，該交易將迅速包括於新區塊 151 中。替代地，Tx0 及 Tx1 可在一起經創建且發送至網路 106，或若節點協定允許緩衝「孤立」交易，則 Tx0 可甚至在 Tx1 之後發送。如本文中所使用之術語「先前」及「隨後」在交易序列之上下文中係指如交易中指定之交易指標所界定的序列中之交易的次序(哪些交易指向哪些其他交易，等等)。該等術語同樣可用「前置」及「後續」或「前期」及「後期」、「父級」及「子級」等來替換。其未必暗示該等交易經創建、發送至網路 106 或到達任何給定區塊鏈節點 104 之次序。然而，直至且除非父級交易經驗證，否則將不驗證指向先前交易(前期交易或「父級」)之隨後交易(後期交易或「子級」)。在其父級之前到達區塊鏈節點 104 之子級被認為孤立的。取決於節點協定及/或節點行為，子級可被捨棄或緩衝某一時間以等待父級。

【0082】 先前交易 Tx0 的一或多個輸出 203 中之一者包含特定 UTXO，其在此處標記為 UTXO0。每一 UTXO 包含指定由 UTXO 表示之一定金額之數位資產的值，及鎖定指令碼，該鎖定指令碼定義必須由隨後交易之輸入 202 中之解鎖指令碼符合的條件，以便驗證隨後交易且因此成功地兌換 UTXO。通常，鎖定指令碼將該金額鎖定至特定當事方(其中包括鎖定指令碼之交易的受益人)。亦即，鎖定指令碼定義解鎖條件，其通常包含如下條件：隨後交易之輸入中之解鎖指令碼包含先前交易鎖定至的當事方之密碼簽名。

【0083】 鎖定指令碼(亦稱 scriptPubKey)為用節點協定辨識之域特定語言編寫的一段程式碼。此語言之特定實例被稱作「指令碼(Script)」(S 為大寫)，其係由區塊鏈網路使用。鎖定指令碼指定需要何種資訊來支出交易輸出 203，例如 Alice 的簽名之要求。解鎖指令碼出現在交易之輸出中。解鎖指令碼(亦稱 scriptSig)為用域特定語言編寫的一段程式碼，該域特定語言提供滿足鎖定指令碼準則所需之資訊。舉例而言，解鎖指令碼可含有 Bob 的簽名。解鎖指令碼出現

在交易之輸入 202 中。

【0084】 因此，在所說明之實例中，Tx0 之輸出 203 中之 UTXO0 包含鎖定指令碼[Checksig PA]，其需要 Alice 之簽名 Sig PA 以便兌換 UTXO0 (嚴格地，以便使嘗試兌換 UTXO0 之隨後交易為有效的)。[Checksig PA]含有來自 Alice 之公用-私用密鑰對之公用密鑰 PA 的表示(亦即，散列)。Tx1 之輸入 202 包含指向 Tx1 之指標(例如，藉助於其交易 ID-TxID0，其在實施例中為整個交易 Tx0 之散列)。Tx1 之輸入 202 包含識別 Tx0 內之 UTXO0 的索引，以在 Tx0 之任何其他可能的輸出中識別 UTXO0。Tx1 之輸入 202 進一步包含解鎖指令碼<Sig PA>，其包含 Alice 的密碼簽名，該密碼簽名藉由 Alice 將她的來自密鑰對之私用密鑰應用於資料之預定義部分(在密碼學中有時被稱作「訊息」)而創建。需要由 Alice 簽名以提供有效簽署之資料(或「訊息」)可由鎖定指令碼或由節點協定或由鎖定指令碼及節點協定之組合來定義。

【0085】 當新交易 Tx1 到達區塊鏈節點 104 時，該節點應用節點協定。此包含在一起運行鎖定指令碼及解鎖指令碼以檢查解鎖指令碼是否符合鎖定指令碼中所定義之條件(其中此條件可包含一或多個準則)。在實施例中，此涉及串接二個指令碼：

<Sig PA> <PA> ‖ [Checksig PA]

其中「‖」表示串接，且「<…>」」意謂將資料置放在堆疊上，且「[…]」為鎖定指令碼所包含之函數(在此實例中為基於堆疊之語言)。等效地，指令碼可一個接一個地運用共同堆疊來運行，而非串接指令碼。無論如何，當在一起運行時，指令碼使用如包括於 Tx0 之輸出中之鎖定指令碼中的 Alice 之公用密鑰 PA，以證實 Tx1 之輸入中的解鎖指令碼含有對資料之預期部分進行簽名的 Alice 之簽名。亦需要包括資料自身(「訊息」)之經預期部分，以便執行此證實。在實施例中，經簽名資料包含整個 Tx1 (因此不需要包括單獨的元素，來明確指定資料之

經簽名部分，此係因為其已經固有地存在)。

【0086】藉由公用-私用密碼學之證實的細節將為熟習此項技術者所熟悉。基本上，若 Alice 使用她的私用密鑰對訊息進行簽名，則明確給定了 Alice 的公用密鑰及訊息，諸如節點 104 之另一實體能夠證實該訊息必須由 Alice 簽名。簽名通常包含對訊息進行散列、對散列進行簽名及將此標記至訊息上作為簽名，因此使得公用密鑰之任何持有者能夠證實該簽名。因此，應注意，本文中對特定資料片段或交易之一部分或其類似者進行簽名之任何參考在實施例中可意謂對彼資料片段或交易之一部分的散列進行簽名。

【0087】若 Tx1 中之解鎖指令碼符合 Tx0 之鎖定指令碼中指定的一或多個條件(因此在所展示之實例中，若 Alice 的簽名經提供於 Tx1 中且被證實)，則區塊鏈節點 104 將 Tx1 視為有效的。此意謂區塊鏈節點 104 將會將 Tx1 添加至交易之有序集合 154。區塊鏈節點 104 亦將會將交易 Tx1 轉遞至網路 106 中之一或多個其他區塊鏈節點 104，使得該交易將在整個網路 106 中傳播。一旦 Tx1 已經驗證且包括於區塊鏈 150 中，則此將來自 Tx0 之 UTXO0 定義為已支出。應注意，Tx1 可僅在支出未支出的交易輸出 203 之情況下為有效的。若 Tx1 嘗試支出已經由另一交易 152 支出之輸出，則 Tx1 將為無效的，即使符合所有其他條件亦如此。因此，區塊鏈節點 104 亦需要檢查是否已經支出先前交易 Tx0 中之所提及 UTXO (亦即，其是否已經形成至另一有效的交易之有效輸入)。此係區塊鏈 150 將經定義次序施加在交易 152 上係重要的一個原因。在實踐中，給定區塊鏈節點 104 可維護單獨的資料庫，其標記在哪些交易 152 中支出了哪些 UTXO 203，但最終什麼定義了是否已經支出 UTXO 在於其是否已經形成至區塊鏈 150 中之另一有效的交易之有效輸入。

【0088】若給定交易 152 之所有輸出 203 中所指定的總金額大於由所有其輸入 202 指向之總金額，則此係大多數交易模型中之無效性的另一基礎。因此，

此類交易將不被傳播，亦不包括於區塊 151 中。

【0089】 應注意，在基於 UTXO 之交易模型中，需要作為整體支出給定 UTXO。其無法在 UTXO 中所定義之金額的一部分為已支出時將另一部分「遺留」為已支出。然而，來自 UTXO 之金額可在下一交易之多個輸出之間劃分。例如，Tx0 中之 UTXO0 中所定義之金額可在 Tx1 中之多個 UTXO 之間劃分。因此，若 Alice 不想將 UTXO0 中所定義之所有金額給予 Bob，則她可使用其餘部分在 Tx1 的第二輸出中給自己零錢，或付錢給另一當事方。

【0090】 在實踐中，Alice 通常亦將需要包括用於公佈她的交易 104 之比特幣節點之費用。若 Alice 不包括此費用，則區塊鏈節點 104 可拒絕 Tx0，且因此儘管技術上有效，但 Tx0 可能不會被傳播及包括於區塊鏈 150 中(若區塊鏈節點 104 不想接受交易 152，則該節點協定不會強迫區塊鏈節點接受該交易)。在一些協定中，交易費用不需要其自身單獨的輸出 203 (亦即，不需要單獨的 UTXO)。實情為，由給定交易 152 之輸入 202 指向之總金額與輸出 203 中指定之總金額之間的任何差被自動給向公佈該交易之區塊鏈節點 104。例如，比如，至 UTXO0 之指標為至 Tx1 之唯一輸入，且 Tx1 僅具有一個輸出 UTXO1。若 UTXO0 中所指定之數位資產之金額大於 UTXO1 中所指定之金額，則該差可由公佈含有 UTXO1 之區塊的節點 104 指派。然而，替代地或另外，不一定排除可在交易 152 的其自身的 UTXO 203 中之一者中明確指定交易費用。

【0091】 Alice 及 Bob 的數位資產由區塊鏈 150 中之任何位置的任何交易 152 中鎖定至 Alice 及 Bob 的 UTXO 組成。因此，通常，給定當事方 103 之資產遍及整個區塊鏈 150 中之各種交易 152 的 UTXO 散佈。區塊鏈 150 中的任何位置都未儲存定義給定當事方 103 之全部餘額的一個數字。將鎖定至各別當事方且尚未在另一正向交易中支出之所有各種 UTXO 的值在一起核對係用戶端應用程式 105 中之電子錢包功能的作用。其可藉由查詢儲存於比特幣節點 104 中之

任一者處的區塊鏈 150 的複本來進行此操作。

【0092】 應注意，常常示意性地表示指令碼程式碼(亦即，不使用確切語言)。舉例而言，可使用操作程式碼(opcode)來表示特定功能。「OP_...」係指指令碼語言的特定作業碼。作為一實例，OP_RETURN 為指令碼語言的作業碼，當在鎖定指令碼的開始處以 OP_FALSE 開頭時，會創建可在交易內儲存資料的交易之不可支出的輸出，且藉此將資料不可變地記錄在區塊鏈 150 中。例如，資料可包含希望儲存在區塊鏈中之文件。

【0093】 以此方式使用 OP_RETURN 為一特定實例，該實例使用證明不可支出的指令碼以用於基於比特幣之區塊鏈系統。熟習此項技術者將瞭解，不同區塊鏈系統將具有不同機構及資料格式以用於確保指令碼為不可支出的及/或將資料儲存在交易中。

【0094】 通常，交易之輸入含有對應於公用密鑰 PA 的數位簽名。在實施例中，此係基於使用橢圓曲線 secp256k1 之 ECDSA。數位簽名對特定資料片段進行簽名。在一些實施例中，對於給定交易，該簽名將對交易輸入之一部分及交易輸出中之一些或全部進行簽名。數位簽名進行簽名所針對的輸出之特定部分取決於 SIGHASH 旗標。SIGHASH 旗標通常為 4 位元組程式碼，其被包括在簽名之末尾，以選擇對哪些輸出進行簽名(且因此在簽名時固定)。

【0095】 鎖定指令碼有時被稱作「scriptPubKey」，其係指其通常包含各別交易鎖定至之當事方的公用密鑰之事實。解鎖指令碼有時被稱作「scriptSig」，其係指其通常供應對應的簽名之事實。然而，更一般而言，在區塊鏈 150 之所有應用程式中，不必要的是用於待兌換之 UTXO 的條件包含證實一簽名。更一般而言，指令碼處理語言可用於界定任何一或多個條件。因此，更一般術語「鎖定指令碼」及「解鎖指令碼」可為較佳的。

【0096】 如圖 1 中所展示，Alice 及 Bob 的電腦設備 102a、120b 中之每一

者上的用戶端應用程式可分別包含額外通訊功能性。此額外功能性使得 Alice 103a 能夠與 Bob 103b 建立單獨的側頻道 160 (在任一方或第三方之推動下)。側頻道 160 使得能夠與區塊鏈網路單獨地交換資料。此類通訊有時被稱作「離鏈」通訊。舉例而言，此可用於在 Alice 與 Bob 之間交換交易 152，而(尚未)將交易登記至區塊鏈網路 106 上或進入鏈 150 上，直至若干當事方中之一者選擇將其廣播至網路 106 為止。以此方式共用交易有時被稱作共用交易範本」。交易範本可能缺乏形成完整的交易所需的一或多個輸入及/或輸出。替代地或另外，側頻道 160 可用於交換任何其他交易相關資料，諸如密鑰、協商的金額或條款、資料內容等。

【0097】 可經由與區塊鏈網路 106 相同的封包交換式網路 101 建立側頻道 160。替代地或另外，可經由諸如行動蜂巢式網路之不同網路或諸如局域無線網路之區域網路或甚至 Alice 及 Bob 的裝置 102a、102b 之間的直接有線或無線鏈路來建立側頻道 160。通常，在本文中任何位置被提及之側頻道 160 可包含經由一或多個網路連接技術或通訊媒體之任一或多個鏈路，以用於「離鏈」(亦即獨立於區塊鏈網路 106)交換資料。在使用多於一個鏈路的情況下，離鏈鏈路之集束或集合可作為整體被稱作側頻道 160。因此，應注意，若據稱 Alice 及 Bob 經由側頻道 160 交換某些資訊或資料片段等等，則此未必暗示必須經由完全相同的鏈路或甚至相同類型之網路來發送所有此等資料片段。

用戶端軟體

【0098】 圖 3A 說明用於實施本發明所揭露之方案的實施例之用戶端應用程式 105 之實例實施。用戶端應用程式 105 包含交易引擎 301 及使用者介面(UI)層 302。交易引擎 301 經組配以根據上文所論述且稍後將進一步詳細論述之方案實施用戶端 105 之基礎的與交易相關的功能性，以便制定交易 152，經由側頻道 160 接收及/或發送交易及/或其他資料，及/或將交易發送至一或多個節點 104 以

經由區塊鏈網路 106 傳播。

【0099】 UI 層 302 經組配以經由各別使用者的電腦設備 102 之使用者輸入/輸出(I/O)構件來呈現使用者介面，包括將經由設備 102 之使用者輸出構件將資訊輸出至各別使用者 103，及經由設備 102 之使用者輸入構件來自各別使用者 103 接收輸入。舉例而言，使用者輸出構件可包含用於提供視覺輸出之一或多個顯示螢幕(觸摸或非觸摸螢幕)、用於提供音訊輸出之一或多個揚聲器，及/或用於提供觸覺輸出之一或多個觸覺輸出裝置等等。使用者輸入構件可包含例如以下各者之輸入陣列：一或多個觸摸螢幕(與用於輸出構件之觸摸螢幕相同或不同)；一或多個基於游標之裝置，諸如滑鼠、軌跡墊或軌跡球；一或多個麥克風及語音或話音辨識演算法，其用於接收語音或聲音輸入；一或多個基於手勢之輸入裝置，其用於接收呈手動或身體姿勢之形式之輸入；或一或多個機械按鈕、開關或操縱桿等等。

【0100】 注意：雖然本文中之各種功能性可描述為整合至相同用戶端應用程式 105 中，但此未必為限制性的，且實情為，其可實施於一套二個或多於二個不同應用程式中，例如一個應用程式為另一應用程式之外掛程式或經由應用程式設計介面(API)介接。舉例而言，交易引擎 301 之功能性可實施於與 UI 層 302 分離的應用程式中，或諸如交易引擎 301 之給定模組的功能性可在多於一個應用程式之間劃分。亦不排除可在比如作業系統層處實施經描述功能性中之一些或全部。在本文中的任何位置都提及單個或給定應用程式 105 等等的情況下，應瞭解，此僅作為實例，且更一般而言，經描述功能性可以軟體之任何形式實施。

【0101】 圖 3B 提供使用者介面(UI) 600 之實例的模型，該使用者介面可由 Alice 的設備 102a 上之用戶端應用程式 105a 的 UI 層 302 呈現。應瞭解，類似 UI 可由 Bob 的設備 102b 或任何其他當事方之設備上之用戶端 105b 呈現。

【0102】 作為說明，圖 3B 自 Alice 的視角展示 UI 350。UI 350 可包含經由

使用者輸出構件呈現為不同 UI 元件的一或多個 UI 元件 351、352、352。

【0103】 舉例而言，UI 元件可包含一或多個使用者可選擇元件 351，其可為諸如不同的螢幕上按鈕或選單中之不同選項等等。使用者輸入構件經配置以使得使用者 103 (在此狀況下為 Alice 103a)能夠選擇或以其他方式操作選項中之一者，諸如藉由點擊或觸碰螢幕上的 UI 元件，或說出所需選項的名稱(注意：如本文中所使用之術語「手動」僅意指與自動相對，且未必限於使用手)。選項使得使用者(Alice)能夠……

【0104】 替代地或另外，UI 元件可包含一或多個資料鍵入欄位 352，藉由該等資料鍵入欄位使用者可……此等資料鍵入欄位經由使用者輸出構件(例如螢幕上)呈現，且資料可藉由使用者輸入構件(例如鍵盤或觸摸螢幕)而經鍵入至欄位中。替代地，可例如基於語音辨識口頭接收資料。

【0105】 替代地或另外，UI 元件可包含一或多個資訊元件 353，其經輸出以將資訊輸出至使用者。例如，可在螢幕上或有聲地呈現此/此等元件。

【0106】 應瞭解，呈現各種 UI 元件、選擇選項及鍵入資料之特定方式並不重要。稍後將較詳細地論述此等 UI 元件之功能性。亦應瞭解，圖 3 中展示的 UI 350 僅為圖示的模型，且在實踐中，其可包含一或多個其他 UI 元件，出於簡明起見不對其加以說明。

節點軟體

【0107】 圖 4 在基於 UTXO 或輸出之模型的實例中說明在網路 106 之每一區塊鏈節點 104 上運行的節點軟體 450 之實例。應注意，另一實體可運行節點軟體 450，而不被分類為網路 106 上之節點 104，亦即不執行節點 104 所需的動作。節點軟體 450 可含有但不限於協定引擎 451、指令碼引擎 452、堆疊 453、應用程式層級決策引擎 454，及一組一或多個與區塊鏈相關的功能模組 455。每一節點 104 可運行節點軟體，該節點軟體含有但不限於以下各者中之所有三者：共識

模組 455C (例如，工作量證明)，傳播模組 455P 及儲存模組 455S (例如，資料庫)。協定引擎 401 通常經組配以認識交易 152 之不同欄位，且根據節點協定處理該等欄位。$Tx_jTx_{m-1}Tx_j$當接收具有指向另一先前交易 152i (Tx_{m-1})之輸出(例如，UTXO)之輸入的交易 152j (Tx_j)時，協定引擎 451 接著識別Tx_j中之解鎖指令碼，且將其傳遞至指令碼引擎 452。Tx_i協定引擎 451 亦基於Tx_j之輸入中的指標而識別及擷取Tx_i。可在區塊鏈 150 上公佈Tx_i，在此狀況下，協定引擎可自儲存於節點 104 處之區塊鏈 150 的區塊 151 之複本擷取Tx_i。替代地，Tx_i可能尚未在區塊鏈 150 上公佈。在彼狀況下，協定引擎 451 可自藉由節點 104 維護之未公佈的交易之有序集合 154 擷取Tx_i。無論如何，指令碼引擎 451 識別Tx_i之經提及輸出中之鎖定指令碼，且將其傳遞至指令碼引擎 452。

【0108】 Tx_iTx_j指令碼引擎 452 因此具有Tx_i之鎖定指令碼及來自Tx_j之對應的輸入之解鎖指令碼。Tx_0 and Tx_1 舉例而言，圖 2 中說明經標記為Tx_0及Tx_1之交易，但此可適用於任何一對交易。指令碼引擎 452 如先前所論述在一起運行二個指令碼，其將包括根據正使用的基於堆疊之指令碼處理語言(例如，指令碼)將資料置放至堆疊 453 上及自該堆疊擷取資料。

【0109】 藉由在一起運行指令碼，指令碼引擎 452 判定解鎖指令碼是否符合鎖定指令碼中所定義之一或多個準則-亦即，其是否「解鎖」其中包括鎖定指令碼之輸出？指令碼引擎 452 將此判定之結果返回至協定引擎 451。若指令碼引擎 452 判定解鎖指令碼確實滿足對應的鎖定指令碼中指定之一或多個準則，則其返回結果「真」。否則，其返回結果「假」。

【0110】 在基於輸出之模型中，來自指令碼引擎 452 之結果「真」係交易之有效性的條件中之一者。通常，亦存在藉由協定引擎 451 評估之亦必須滿足的一或多個其他協定級條件；諸如Tx_j之輸出中指定之數位資產的總金額不超過由其輸入指向的總金額之條件，及Tx_i之所指向的輸出尚未由另一有效的交易支出

之條件。協定引擎 451 評估來自指令碼引擎 452 之結果連同一或多個協定級條件，且其僅在該結果及該等條件均為真之情況下驗證交易Tx_j。協定引擎 451 將交易是否有效的一指示輸出至應用程式層級決策引擎 454。僅在確實驗證了Tx_j之條件下，決策引擎 454 可選擇控制共識模組 455C 及傳播模組 455P 二者以執行其關於Tx_j之各別與區塊鏈相關的功能。此包含共識模組 455C 將Tx_j添加至節點的交易之各別有序集合 154 以用於併入區塊 151 中，及傳播模組 455P 將Tx_j轉遞至網路 106 中之另一區塊鏈節點 104。任擇地，在實施例中，應用程式層級決策引擎 454 可在觸發此等功能中之任一者或二者之前應用一或多個額外條件。例如，決策引擎可僅在交易係有效的且留下足夠的交易費用之條件下選擇公佈交易。

【0111】 亦應注意，本文中之術語「真」及「假」不一定限於返回以僅單個二進位數字(位元)之形式表示的結果，但當然為一個可能的實施。更一般而言，「真」可指指示成功或肯定結果之任何狀態，且「假」可指指示不成功或非肯定結果之任何狀態。舉例而言，在基於帳戶之模型中，結果「真」可由簽名之隱式協定級驗證及智慧型合約之額外肯定輸出之組合指示(總體結果在二個個別結果為真之情況下被視為傳信真)。

【0112】 一旦給定本文中之本揭露內容，所揭露技術之其他變型或使用狀況對於熟習此項技術者可變得顯而易見。本揭露內容之範疇不受所描述實施例而僅受隨附申請專利範圍限制。

【0113】 舉例而言，以上一些實施例已關於比特幣網路 106、比特幣區塊鏈 150 及比特幣節點 104 而加以描述。然而，應瞭解，比特幣區塊鏈為區塊鏈 150 之一個特定實例，且以上描述通常可適用於任何區塊鏈。亦即，本發明絕不限於比特幣區塊鏈。更一般而言，以上對比特幣網路 106、比特幣區塊鏈 150 及比特幣節點 104 之任何引用可分別用對區塊鏈網路 106、區塊鏈 150 及區塊鏈節點

104 之引用來替換。區塊鏈、區塊鏈網路及/或區塊鏈節點可共用如上文所描述的比特幣區塊鏈 150、比特幣網路 106 及比特幣節點 104 之經描述屬性中之一些或全部。

【0114】 在本發明之較佳實施例中，區塊鏈網路 106 為比特幣網路，且比特幣節點 104 至少執行創建、公佈、傳播及儲存區塊鏈 150 的區塊 151 之所有所描述功能。不排除可存在僅執行此等功能中之一者或一些而非所有的其他網路實體(或網路元素)。亦即，網路實體可執行傳播及/或儲存區塊而不創建及公佈區塊之功能(前已述及，此等實體不被視為較佳比特幣網路 106 的節點)。

【0115】 在本發明之非較佳實施例中，區塊鏈網路 106 可能並非比特幣網路。在此等實施例中，不排除節點可執行創建、公佈、傳播及儲存區塊鏈 150 之區塊 151 的功能中之至少一者或一些而非所有。舉例而言，在彼等其他區塊鏈網路上，「節點」可用於指代網路實體，該網路實體經組配以創建及公佈區塊 151，而非將彼等區塊 151 儲存及/或傳播至其他節點。

【0116】 甚至更一般而言，對以上術語「比特幣節點」104 之任何引用可用術語「網路實體」或「網路元件」來替換，其中此實體/元件經組配以執行創建、公佈、傳播及儲存區塊之角色中之一些或全部。此網路實體/元件之功能可以上文參考區塊鏈節點 104 所描述的相同方式實施於硬體中。

【0117】 甚至更一般而言，對以上術語「比特幣節點」104 之任何引用可用術語「網路實體」或「網路元件」來替換，其中此實體/元件經組配以執行創建、公佈、傳播及儲存區塊之角色中之一些或全部。此網路實體/元件之功能可以上文參考區塊鏈節點 104 所描述的相同方式實施於硬體中。

有序唯加資料儲存

【0118】 近年來，將區塊鏈用於大容量、針對資料之應用程式已顯著增加。隨著此增加，對用於結構化、編碼及格式化經公佈至區塊鏈之資料酬載的穩定層

-2 協定之需要亦相稱地增加。此處，層-2 意謂在現有區塊鏈系統之頂部上構建的輔助協定、框架、資料結構等。本文中所描述的態樣將被視為層-2 協定。層-1 將指代比特幣、比特幣 SV 或其他基礎的區塊鏈技術。

【0119】 對於涉及大量資料之基於區塊鏈之應用程式而言，典型的是需要一種資料方案或結構化機制，以允許許多資料載體交易彼此鏈接。此尤其與其中許多事件及/或資料可能需要以線性化序列彼此鏈接之應用程式(例如，在供應鏈中)相關。

【0120】 可藉由唯一引用來輔助對事件及/或有序資料項目之序列的維護及追蹤，由此，一個資料載體交易將明確地引用另一交易，以確保區塊鏈之觀察者可將二個交易彼此相關。

事件流及塵埃鏈

【0121】 圖 5 係關於本發明之第一態樣，且說明有序唯加資料儲存系統之基本資料結構及範例。此亦可描述為資料登錄系統。圖 5 中所展示的特定系統為用於登錄事件之事件流系統。作為實例，出於說明性目的始終使用事件流，然而，熟習此項技術者將瞭解，本文中所描述的經提議系統及態樣可通常與資料項目以及與有序唯加資料項目登錄或儲存系統一起使用。資料項目可指呈完整形式之資料，例如感測器資料或文件。替代地，資料項目係指實際資料之散列。使用散列而非資料自身有利地提供資料存在的證明，而無需資料(對於交易較大，甚至過大)儲存在交易上。

【0122】 唯加日誌中之每一事件 502 經映射至區塊鏈交易 504，且區塊鏈交易之序列使用「塵埃鏈」來排序且鏈接 506。與每一事件相關聯之資料儲存於(下文描述之)酬載中作為每一交易之一部分。資料酬載保存在交易之不可支出之 OP_RETURN 輸出中。此為指令碼作業碼，其可用以在區塊鏈上寫入任意資料且亦將交易輸出標記為無效。作為另一實例，OP_RETURN 為指令碼語言之作業

碼，其用於創建交易之不可支出輸出，該輸出可儲存交易內之資料，諸如後設資料，且藉此將後設資料不可變地記錄在區塊鏈上。

【0123】 塵埃鏈係比特幣輸入及輸出之不間斷的鏈，在此處，該等比特幣輸入及輸出用於將每一區塊鏈交易的支出相關性強加於其緊鄰的前置者之序列上。在本揭露內容之區塊鏈交易的上下文中，「塵埃」應理解為具有低或極小值之輸出的數位資產或密碼貨幣之可支出交易，亦即，該值可比用於挖掘區塊鏈中之輸出的費用小得多。

【0124】 在交易中使用塵埃輸出對於維護所有交易的不可變依序記錄係有利的且關鍵的，此係因為其針對有序唯加資料儲存系統進行，諸如事件流。此係因為，儘管藉由將交易發佈至區塊鏈，一旦交易在區塊鏈上經確認或添加至該區塊鏈，所有區塊鏈交易將被打上時戳且保持特定次序，但此不保證維護其依序次序。此係因為交易可在不同時間經挖掘至區塊中及/或即使在同一區塊內，交易亦呈不同次序。使用由該序列中之下一交易的第一輸入支出之塵埃輸出有利地確保按時間順序追蹤交易之次序，且創建事件自身及事件之依序排序二者的防篡改記錄。此係因為一旦經挖掘至區塊中，塵埃自前述交易至序列中之下一交易的支付確保了，與比特幣協定規則一致地，所嵌入資料載體元素之序列(其被稱作酬載且在下文論述)無法經重排序，且不會發生插入或刪除，此可改變序列，而不會立即明顯發現事件流已受損。在一些實施例中，比特幣協定固有的雙重支出預防機制確保密碼貨幣(例如，塵埃)在不同交易輸入及輸出之間的移動保持拓樸次序。塵埃交易的鏈結利用拓樸排序以提供區塊間及區塊內交易(且因此相關聯的事件及資料)次序維護。因此，此改良有序唯加資料項目儲存之完整性。

【0125】 以此方式，區塊鏈交易 504 形成交易之有向圖。應注意，圖之方向可被視為單向的，自該序列中之前述交易導向至下一交易，如邊緣 506 所指示。雖然圖 5 中之邊緣 506 上的箭頭指示交易指向下一交易，但比特幣交易中的

支出關係實際上係自一個交易至前一交易。此圖係由交易之間的支出關係來創建。此等支出關係可被視為一種類型的參考。

塵埃鏈中之反向引用

【0126】 圖 6A 係關於本揭露內容之第一態樣，且展示交易鏈 600。交易鏈包含彼此相關之數個交易 602、604a、604b、604c。第一交易 602 經標記為 Tx0，且包含關於鏈及種子數目之後設資料。該鏈亦包含數個附加交易 604a、604b、604c，且較佳地其包含待包括於區塊鏈中之資料項目。資料項目較佳地經儲存為下文描述之酬載的一部分。附加交易 604a、604b、604c 亦包含與來自在該等附加交易之前的交易之輸出相關聯的輸入，因此建立支付關係 606a、606b、606c、606d。此輸入支出來自前一交易之交易輸出。作為實例，參考比特幣協定，且如上文在標題「基於 UTXO 之模型」下所描述，且參考圖 2，輸出為未支出交易輸出(UTXO)，且輸入包含對 UTXO 之引用。因此，每一交易(除了第一之外)均包含經由支付關係對塵埃鏈中之前一交易的反向引用 606a、606b、606c、606d。初始交易確實包含輸入，其包含對如下文參考圖 6C 所解釋之資金 UTXO 的反向引用。然而，此資金 UTXO 並不被視為塵埃鏈之一部分，此係因為其不儲存關於塵埃鏈之資料或後設資料。

【0127】 任擇地，附加交易 604a、604b、604c 中包含二個其他的反向引用。在圖 6A 中藉由左手側的箭頭描繪了對第一交易的第二反向引用 608。此引用較佳地採用第一交易的交易 id 之形式。第三反向引用 610、612a 至 612c 採取二個形式，此取決於交易在鏈中之位置。對於鏈中之第二交易 604a，第三反向引用 610 為存在於第一交易中之種子。對於第二交易之後的所有其他交易，引用 612a 至 612c 採用前一交易內之資料的原像之散列之形式。

【0128】 第三反向引用 610、612a 至 612c 將藉由確保每一酬載取決於前一酬載之部分來保護酬載免於更改。具體而言，每一酬載包含前一酬載之串流摘

要。此亦具有創建反向引用之效應，該等反向引用允許使用者藉由遵循此等串流摘要引用來反向追蹤事件流。此等第三反向引用 610、612a 至 612c 指代與支出引用 606a 至 606d 相同的對象(相同的前一交易)，但使用不同參考對象。

【0129】 附加交易 604a、604b、604c 之酬載任擇地具有以下形式：$Payload_n = [preimage_n][streamDigest_n][...]$。此處，下標 n 用於表示當前交易，且 n-1 為前一交易。

【0130】 較佳地，酬載按以下形式儲存於交易之輸出的指令碼中：

OP_FALSE OP_RETURN OP_PUSHDATA1 <preimage> 0x20 <streamDigest> [0x20 <data digest> | OP_PUSHDATAN <data>]

【0131】 原像包含當前交易及前一交易之後設資料。該原像任擇地包含以下欄位中之任一或多者：

● txidcreate：對該鏈中之第一交易的引用 608，較佳地為該鏈中之第一交易的交易 id，

● index：資料或事件的索引，

●whenRecorded：與交易及/或資料項目之創建相關聯的時間，

●$dataDigest_n$：資料的散列，其中任擇地，資料儲存於酬載([…])的事件資料表示部分中或任擇地離鏈儲存，及

● $streamDigest_{n-1}$：前一交易之原像的散列 612a、612b、612c (亦被描述為前一交易之串流摘要，或串流摘要引用)或第一交易之種子 610 (若該交易為該鏈中之第二交易，此係因為第一交易不包含 streamDigest)。如上文所論述，此可充當前一交易之第三引用。

【0132】 串流摘要(streamDigest)為原像(preimage)的散列。

【0133】 酬載([. . .])的事件資料表示部分任擇地包含待儲存在區塊鏈上之資料項目。資料項目可為以下各者中的一者：

●待儲存在區塊鏈上之資料自身，

●資料的散列，

●待儲存於區塊鏈上之資料的子部分，或

●無及/或空的。

【0134】 若待儲存之資料項目為一些資料的散列且不存在將資料自身儲存在交易中之意圖，則酬載的事件資料表示部分可為空的。在此狀況下，資料項目(資料的散列)已經儲存於原像之 dataDigest 部分中。

【0135】 前一交易的原像之散列 612a、612b、612c 可被視為前一交易之另一引用。此散列可用於遍歷交易鏈及/或驗證前一交易。

【0136】 若待儲存在區塊鏈上之資料對於酬載過大及/或使交易對於區塊鏈系統過大，則資料可劃分成子部分。因此，橫跨多個酬載(且因此交易)儲存資料。原像任擇地包含另一欄位以追蹤子部分之總數目及存在於事件資料表示部分中之當前子部分的索引。管理劃分在多個交易上之資料之其他方法為吾人所知。第一替代方案可使用用於資料之唯一 ID，因此任何資料塊均可使用相同 ID 以表示其為相關的。第二替代方案可使用至儲存(其餘)資料之其他位置的指標，例如儲存一半資料之一個 Tx 可包括儲存另一半的另一 Tx 之 TxID，且包括其[…]中之此 TxID，且反之亦然。熟習此項技術者將瞭解，橫跨交易劃分資料之其他方法為可能的。

【0137】 參考圖 6B 及圖 6C，展示用於資料附加交易 640a、640b 及初始交易 660 以及最終交易 662 之實例區塊鏈交易格式。因為該等交易為區塊鏈交易，所以其在結構上類似於參考圖 2 所描述之交易 152i、152j，然而，包含與本發明之目前態樣相關的特定分量。輸入及輸出之確切次序並非特定的，且可使用替代排序。排序在給定鏈上較佳地為一致的。

【0138】 圖 6B 展示了二個資料附加交易 640a、640b。此等實例資料附加

交易 640a、640b 按時間順序且在塵埃鏈中一個接一個。在第二交易 640b 之塵埃輸入 646b 中引用(亦即，由該塵埃輸入支出)第一交易 640a 的塵埃輸出 644a。第二交易 640b 之塵埃輸入 646b 對第一交易 640a 之塵埃輸出 644a 之引用包含第一交易之交易 id 648a 及 UTXO 之索引二者，該索引在此實例狀況下為 0 (因為其在清單中為第一個且使用零編索引)。

【0139】 所有交易 640a、640b、660、662 包含資金輸入 648a、648b、648c、648d。此等資金輸入 648a、648b、648c、648d 由計算裝置提供，該計算裝置管理創建此等交易及將此等交易提交至區塊鏈。計算裝置任擇地為資金服務，且為如參考圖 16 所描述之服務之一部分。資金輸入之總值經選擇以涵蓋交易費用(有時被稱作挖掘者之費用)以幫助確保挖掘者將挑選交易且將其包括在區塊中。資金服務可提供一或多個輸入以確保總值為輸入係足夠的。交易費用係動態的，且將取決於網路之負載。每一位元組可以中本聰幣(或區塊鏈系統使用的任何幣/符記)量測交易費用(其中中本聰幣為單個比特幣之億分之一)。因此，若酬載較大，則該費用將亦需要較大，且將相應地調整資金輸入。由於 UTXO 模型，所支付之全部費用受在輸入中引用之 UTXO 及輸出上之 UTXO 二者來控制。來自支付交易費用的剩餘零錢任擇地經發送回至相同計算裝置，該計算裝置管理、創建此等交易及將此等交易提交至區塊鏈。資金輸入及由該等資金輸入產生的零錢作為浮動資金，並由該資金服務管理。

【0140】 初始交易 660 及最終交易 662 亦包含串流後設資料 664、666。初始串流後設資料包含如參考圖 6B 所描述之種子，以及與塵埃鏈之維護相關的其他值。最終交易 662 之後設資料 666 包含用以表示此交易為該鏈中之最後一個交易之資訊。較佳地，最終交易之後設資料 666 亦包含第一交易 660 之交易 id 648c。

【0141】 二個資料附加交易 640a、640b 分別地包含酬載 642a、642b，如上

文所描述。第二交易 640b 之酬載 642b 包含對前一交易 642a 之酬載 642a 的引用。

【0142】 在圖 5、圖 6A、圖 6B、圖 6C 及圖 6D 中之區塊鏈交易的鏈 600 中，沒有明確需要交易引用該序列中的下一交易。此係因為交易圖中之支出關係將始終足以追蹤自一個交易正向至下一交易之序列。

【0143】 替代地，交易確實包含對序列中的下一交易之正向引用。任擇地，此係藉由要求在創建當前附加交易時已知序列中的下一資料項目及/或附加交易的部分來進行的。舉例而言，若第一交易 Tx_1 需要引用序列 Tx_2 中之下一交易，則典型的機制將會將散列 $H(Tx_2)$ 包括在 Tx_1 內。此將需要在創建 Tx_1 時瞭解 Tx_2 的全部資料，而此並非始終為可能的。

【0144】 參考圖 6D，展示將附加交易添加至一組交易之方法 680。

【0145】 首先接收用於儲存至區塊鏈上之資料項目 682。資料可作為請求之部分被接收，該請求含有其他後設資料，諸如其係關於哪一鏈。替代地，應用程式已經自先前請求及/或組配已知相關鏈。資料項目可為用於儲存在事件資料表示部分中之資料。替代地，資料項目為資料的散列，且資料項目儲存於交易之 $dataDigest_n$ 部分中。

【0146】 獲得一組交易中之最新交易 684。任擇地，藉由自記憶體再調用最新交易而獲得最新交易。

【0147】 創建新交易 686。新交易包含至少一輸入，其係與來自最新交易之輸出、塵埃輸出、資料項目及對最新交易之引用相關聯。較佳地，其為來自最新交易之塵埃輸出。較佳地，對最新交易之引用包含最新交易之部分的散列。更佳地，該引用為最新交易之原像的散列。

【0148】 接著將新交易提交至區塊鏈 688。

祖先限制

【0149】 在比特幣協定的許多實施中，存在已知為祖先限制之概念。祖先限制在未確認交易之最大鏈上設置最大值，其中連續支出相關性可在單個區塊間時間間隔中處理。在寫入時，該限制在比特幣上設定為 25 個未經確認的祖先，且在比特幣 SV 上設定為 1000 (先前為 50 且在此之前為 25)。應理解，本揭露內容之態樣及實施例不限於此值。

【0150】 嘗試以高頻率創建支出相關交易的鏈之任何應用程式將遭受存在祖先限制之困擾。本文中所描述的有序唯加資料儲存系統為一個此類實例，此係因為需要在單個區塊間時段中登錄多於 25 個事件之串流將受此問題限制，因為該串流中之所有交易均為藉由設計而取決於支出。

【0151】 在一些實例中，每 10 分鐘左右(平均)，產生新比特幣區塊。因此，根據參考圖 5、圖 6A、圖 6B 及圖 6C 所描述之實施例之在比特幣網路上操作的有序唯加資料儲存系統可在遇到祖先限制之前每 10 分鐘儲存例如 25 個資料項目。

克服祖先限制

【0152】 在如參考圖 5、圖 6A、圖 6B 及圖 6C 所描述之本發明之第一態樣中，塵埃協定之鏈確保每一資料酬載經包括於鏈接交易之序列中之鏈上交易中。接著，藉由將塵埃輸出自一個交易支出至下一交易，而依序將交易彼此鏈接，從而創建鏈上交易支出圖。

【0153】 然而，考慮到祖先限制，並非每個區塊創建時段將資料添加至區塊鏈的頻率比祖先限制更頻繁(因此對想要在區塊鏈上儲存資料的資料寫入器及/或系統施加了限制)，或必須引入交易支出圖的中斷，同時仍允許有效地遍歷鏈中的交易之全部集合。

【0154】 挑戰在於確保儘管祖先限制在交易支出圖中引起了中斷，但可使用交易訊框按順序遍歷資料元素/酬載之序列。

【0155】 圖 7A、圖 7B、圖 8 及圖 9 係關於本揭露內容的第二態樣，且描述資料結構 700、714、716，用於將資料項目添加至塵埃鏈且有條件地創建新塵埃鏈之方法 800，及用於正向遍歷塵埃鏈之方法 900。除了參考圖 5 及圖 6A、圖 6B 及圖 6C 所描述之態樣之外，亦可任擇地使用此處所描述之本發明態樣。本發明態樣可與其他區塊鏈系統一起使用以建構具有支出關係之交易序列且克服祖先限制。

【0156】 參考圖 7A，展示用於第二態樣中之塵埃資料結構 700 的鏈之概述。展示包含二個交易子集的一組交易，該等子集為塵埃鏈 720、722。每一塵埃鏈包含多個附加交易 704a 至 704d。第一塵埃鏈 720 係藉由轉出交易 714 終止，且第二塵埃鏈 722 開始於轉入交易 716。轉入交易 716 與轉出交易 714 之間不存在支出關係，藉此克服祖先限制問題。此可經描述為「跳」至新塵埃鏈。

【0157】 當子集中之交易之數目接近祖先限制時，進行跳鏈。較佳地，當當前鏈中之交易之總數目比祖先限制小一個時，必須使用新鏈。因此，一對轉出交易 714 及轉入交易 716 插入在 Tx_{n-2} 交易 704c 與 Tx_{n-1} 交易 704d 之間，其中 n 係祖先限制。此係為了說明新鏈中的第一交易 702、716 (無論為初始交易 702 抑或轉入交易 716)，並為轉出交易 714 留出空間從而亦包括在塵埃鏈中。

【0158】 替代地，當鏈中之未確認交易之數目接近祖先限制時，進行跳鏈。以此方式，與跳鏈相關的交易之子集係由是否已經確認每一交易來定義。

【0159】 交易的子集並非嚴格的子集，使得若僅存在一個塵埃鏈，則子集之成員與交易集合相同。

【0160】 轉入交易 716 亦包含對前一鏈之鏈引用 724。詳言之，鏈引用 724 藉由引用前一鏈中之交易來引用鏈。較佳地，鏈引用 724 係針對第一鏈 720 中之第一交易 702。第一鏈 720 中之第一交易 702 亦可被稱作初始交易或 Tx_0。替代地，鏈引用 724 係針對前一鏈中之第一交易-亦即前一鏈中之轉入交易(圖 7 中未

展示此，因為前一鏈亦為第一鏈)。

【0161】 每一附加交易 704a 至 704d 包含對塵埃鏈中之前一交易的引用 706a 至 706f。此引用 706a 至 706f 至少包含如參考圖 5、圖 6A 及圖 6B 所描述的支出關係 606。任擇地，交易 604a 至 604d 進一步包含第三反向引用(亦經描述為 $streamDigest_{n-1}$ 引用) 610、612a 至 612c，如參考圖 6A 所描述。

【0162】 轉出交易 714 包含對轉入交易 716 之正向引用 718。在本實例中，此引用 718 係針對轉入交易 716 之交易 id。因為引用 718 為或包含交易 716 之散列，所以必須首先創建轉入交易 716。此不需要先將轉入交易 716 公佈或提交給區塊鏈。

【0163】 此正向引用 718 允許想要提取儲存於本發明資料儲存系統中之資訊的當事方正向遍歷鏈。

【0164】 雖然圖 7A 僅展示二個塵埃鏈 720、722，但熟習此項技術者將瞭解，可使用本文中所描述之相同技術將鏈添加至彼此上。

【0165】 參考圖 7B，展示用於轉出交易 714 及轉入交易 716 之實例區塊鏈交易格式。此等交易具有與參考圖 6B 及圖 6C 描述的交易 604a 至 604d 相同或類似的許多特徵。在特徵相同或類似的地方使用了相同或類似的名稱。

【0166】 轉出交易 714 之塵埃輸入 732 包含對前一塵埃鏈中之最後的附加交易之塵埃輸出的引用。作為其輸出之部分，轉出交易 714 包含對轉入交易 716 之引用。詳言之，轉出交易 714 包含轉入交易 716 之交易 id 730b。

【0167】 本發明態樣之附加交易 704a 至 704d 具有與參考圖 6B 所描述之附加交易 640a、640b 之格式極類似的格式，除了塵埃輸入 646a、646b 將不始終引用先前附加交易的塵埃輸出 644a、644b 之外。當如參考圖 8 所描述，使用轉出交易 714 及轉入交易 716 時，下一附加交易 704d 將自轉入交易繼續。亦即，下一附加交易 704d 之具有形式 646a/646b 之塵埃輸入將支出轉入交易之塵埃輸

出 734。

【0168】 參考圖 8，電腦實施方法 800 用於根據如參考圖 7 所描述之結構 700 將資料項目添加至塵埃鏈，且有條件地創建新塵埃鏈。雖然此等步驟經論述且展示為依序步驟，但其中之許多步驟可以任何次序、並行或同時進行。舉例而言，前三個步驟 802、804 及 806 可按任何次序。

【0169】 首先接收用於儲存至區塊鏈上之資料 802。資料可作為請求之部分被接收，該請求含有其他後設資料，諸如其係關於哪一鏈。替代地，應用程式已經自先前請求及/或組配已知相關鏈。

【0170】 接下來，獲得最大未確認鏈長 804。此值可經預組配，經由儲存於記憶體中之變數來存取，自儲存裝置再調用，或自第三方獲得。此最大未確認鏈長為如上文所論述的祖先限制。較佳地，只要祖先限制不改變，該步驟則執行一次，並且每次接收到儲存資料的請求時都不進行。

【0171】 獲得當前鏈中之最新交易的交易 id。交易 id 係用於將至該鏈中之下一交易的輸入與最新交易之輸出相關聯。較佳地，自最新交易經提交至區塊鏈時即保留交易 id。替代地，任擇地藉由遍歷該鏈中之最新交易而獲得最新交易。接著藉由對最新交易進行散列而判定交易 id。

【0172】 接著判定當前鏈長 806。較佳地，此值作為變數儲存在記憶體中，以用於快速重新收集。另外或替代地，若當前鏈中之最新交易係已知的，則自該等交易之酬載的原像資料讀取交易之索引。作為另一替代方案，每當運行此步驟時，都對該鏈之整個長度進行計算。任擇地，當前鏈長係表示當前鏈中之未確認交易之數目。

【0173】 作為判定當前鏈長之替代方案，替代地，判定當前鏈中之尚未包括於區塊鏈上之區塊中的交易之數目。該方法 800 藉由將此用作「當前鏈長」而照常繼續。

【0174】作為判定當前鏈長之另一替代方案，替代地，判定當前鏈中之尚未在區塊鏈上「確認」之交易之數目。「已確認」之定義取決於所討論的區塊鏈。作為實例，許多比特幣相關的應用程序都認為，當在區塊之後添加了 6 個區塊時，便被視為“已確認”。

【0175】使用超過當前鏈中之未確認交易之數目的當前鏈長之優勢在於，區塊鏈分支存在固有的回彈性，且為經挖掘區塊之部分及/或在區塊鏈中被視為「已確認」之交易不再為區塊鏈之部分。此係以可能在並非嚴格必要時使用轉入及轉出交易為代價。此等替代方案可根據經提交至區塊鏈的資料之性質及頻率進行選擇及切換。

【0176】做出關於當前鏈長係等於抑或大於臨限數目之判定 808。較佳地，選擇臨限值，使得允許在未確認交易之鏈中存在至少一個未確認交易，使得將仍允許轉入/轉出交易。較佳地，臨限數目比最大未確認鏈長小一。

【0177】若當前鏈長小於臨限值，則根據如參考圖 6A 及圖 6B 所描述之交易創建交易 810。亦即，最新創建的交易包含引用該鏈中之最新交易之輸出的輸入。

【0178】該交易經提交 812 至區塊鏈，使得其他計算裝置可挖掘該交易且將其添加至區塊鏈。

【0179】任擇地，若儲存當前鏈長，則當前鏈長遞增 814。

【0180】若當前鏈長處於或超過臨限值，則創建轉出交易及轉入交易。

【0181】首先創建 816 轉入交易，如參考圖 7A 及圖 7B 所論述。

【0182】接著創建 818 轉出交易，如參考圖 7A 及圖 7B 所論述。轉出交易包含對轉入交易之正向引用。正向引用包含或為轉入交易之交易 id。

【0183】創建 820 新交易，其包含待提交至區塊鏈之資料。新交易包含與轉入交易之輸出相關聯的輸入。新交易亦包含待提交至區塊鏈之資料。

【0184】任擇地，若儲存當前鏈長，則當前鏈長經設定為 2，此係因為當前鏈包含轉入交易及附加交易。

【0185】任擇地，新交易亦包含對當前鏈中之最新交易的引用。此引用具有如參考圖 6A 及圖 6B 所描述之第三反向引用 610、612a 至 612c 之形式。

【0186】熟習此項技術者將瞭解，關於創建轉出交易及轉入交易之步驟 816、818、820、822、824，包括檢查 808 當前鏈長是否小於臨限值，亦可在提交 812 附加交易之步驟及/或使當前鏈長遞增之步驟 814 之後執行。以此方式，已經針對下一附加交易建立新塵埃鏈。

【0187】參考圖 9，一種方法 900，其用於正向遍歷具有如參考圖 7A、圖 7B 及圖 7C 所描述之結構且運用如參考圖 8 所描述之方法來創建的塵埃鏈。正向遍歷意謂在使序列或指數增加之方向上移動。此亦可被視為自較舊的資料項目移動至較新資料項目。在附加交易中使用反向引用及在轉出交易至轉入交易中使用正向引用使得能夠進行此正向遍歷。

【0188】有利地，遍歷方法 900 不需要隱藏知識來遍歷除區塊鏈上的交易的格式之外的交易。遍歷中所使用之引用均與資料項目一起公佈在區塊鏈上。因此，第三方亦能夠遍歷塵埃鏈且獲得、儲存、認證及/或以其他方式使用儲存於區塊鏈上之資料項目，而無需任何專用或專有服務。值得注意的是，由於區塊鏈及目前的資料寫入系統及方法之性質，對儲存於區塊鏈上之資料進行之任何操作均為唯讀的。修改儲存於區塊鏈上之資料並不實際。

【0189】獲得第一交易 902。此係自子其正向遍歷之交易。

【0190】任擇地，獲得且儲存 904 種子(若其為塵埃鏈中之第一交易)或串流摘要(若其為附加交易)以供稍後認證。

【0191】接下來，對第一交易進行散列 906 以獲得其交易 id。

【0192】使用第一交易之交易 id，吾人將交易定位 908 在塵埃鏈中，該交

易在其輸入中引用此交易 id。此該塵埃鏈中之下一交易。下一交易經指派為用於下一步驟 910 之當前交易。

【0193】 定位 908 交易之步驟任擇地涉及遍歷區塊鏈中之所有區塊(自當前交易所在之區塊開始，此係因為若吾人正向遍歷，則當前交易不會位於前一區塊中-若反向遍歷，則相反情況為真)，以定位該交易。

【0194】 替代地或另外，定位交易之步驟包含查閱離鏈日誌或資料庫，其複製塵埃鏈或儲存與塵埃鏈中之每一交易相關聯的後設資料。

【0195】 在一些實施例中，離鏈日誌或資料庫將為塵埃鏈之部分的每一交易與該交易所屬之區塊標頭或至少區塊 id 相關聯。以此方式，使用交易引用(任擇地，交易 id，或在一些態樣中，PrevOut 資金輸入)，獲得包含所關注交易之區塊且接著該區塊搜尋交易。與遍歷區塊鏈中的每一區塊以定位適當的交易相比，此實施例使定位步驟的至少一部分快捷化。

【0196】 作為如參考圖 15 及圖 16 所描述之平台服務之部分操作的平台處理器任擇地維護此日誌或資料庫。

【0197】 在一些實施例中，存在頻道服務，如參考英國專利申請案第 2007597.4 號(2020 年 5 月 21 日以 nChain Holdings Limited 之名稱申請)所描述。當在區塊鏈上確認交易時，此頻道服務向第三方提供通知。該等通知包含細節，諸如在其中確認交易之區塊之區塊標頭及交易 id。訂用此等通知之第三方可使用資訊獲得之通知，以藉由直接進入正確的區塊以與上文類似的方法在區塊鏈上定位交易。

【0198】 接著，進入對當前交易進行操作的循環(在圖 9 中標記為 Tx_i)。循環中之第一步驟檢查 908 當前交易是否為最終交易。若當前交易並非最終交易，則該方法繼續到下一步驟 912。若其為最終交易，則循環及方法 900 終止。替代地，若最終交易包含對第一交易之引用，則該方法 900 可任擇地圍繞交易集合且

必要時繼續遍歷鏈。舉例而言，若該方法並不以塵埃鏈之第一交易開始且遍歷該(等)鏈之使用者想要遍歷所有交易，則此可為需要的。在此狀況下，當再次到達開始遍歷的交易時，循環終止(亦即，循環已經循環回至起點，並且遍歷了鏈中的所有交易)。

【0199】 判定 910 交易是否為最終交易之步驟係基於該交易是否包含後設資料。替代地，最終交易包含表示其為最終交易之旗標。判定最終交易是否為最終交易之另一替代方案係基於該交易是否包含未經支出之塵埃輸出，且該交易不包含對轉入交易之引用(否則，該交易將可能為轉出交易)。

【0200】 接下來，關於當前交易之類型做出判定 912。任擇地，作為檢查當前交易是否為最終交易之部分來檢查該當前交易。若該交易包含酬載，則其被視為附加交易。若該交易不包含酬載，則其被視為轉出交易。替代地，若該交易包含對下一轉入交易之引用，則其被視為轉出交易。

【0201】 若該交易為附加交易，則對酬載進行 914 任擇的操作。所進行的操作任擇地取決於由遍歷者提供之組配。

【0202】 較佳地，該操作將認證先前的交易。該認證係基於如參考圖 6A 及圖 6B 所描述之第三反向引用 610、612a 至 612c。儲存當前酬載的串流摘要以用於在下一循環反覆中認證。相較於自先前的循環反覆或獲得且儲存該值之任擇的步驟 904 儲存的先前串流摘要或種子，使用儲存於當前交易之酬載中的先前交易之串流摘要。

【0203】 另外或替代地，儲存酬載之資料項目以供稍後使用。另外或替代地，調用由遍歷者提供之回調，藉此允許藉由遍歷者對酬載進行任意操作。

【0204】 對當前交易進行散列 916 以獲得當前交易之交易 id。

【0205】 藉由發現具有引用當前交易之交易 id 的輸入之交易來定位 918 下一交易。

【0206】 該循環以指派 920 為當前交易之下一交易重複。該循環在判定 910 當前交易是否為最終交易之步驟處開始。

【0207】 返回至判定 912 交易之類型之步驟，若當前交易為轉出交易，則獲得對轉入交易之引用。藉由自儲存引用之轉出交易提取 922 該引用而較佳地獲得該引用。

【0208】 參考轉入交易，發現 924 轉入交易。在本發明態樣中，轉入交易為轉入交易之交易 id。若已確認轉入交易，則可在區塊鏈自身上發現該轉入交易，或若尚未確認該交易，則可在區塊鏈網路節點的記憶體池中發現該轉入交易。

【0209】 對轉入交易進行散列 926 以獲得轉入交易之交易 id。塵埃鏈中之下一交易將包含對呈轉入交易 id 之形式的轉入交易之反向引用。詳言之，下一交易支出與轉入交易相關聯之輸出。

【0210】 運用轉入交易之交易 id，獲得下一交易 928。

【0211】 該循環以指派 920 為當前交易之下一交易重複。該循環以判定 910 當前交易是否為最終交易之步驟開始(其亦為循環可終止之點，如上文所描述)。

【0212】 方法 900 經描述為自交易集合中之第一交易開始。然而，熟習此項技術者將瞭解，藉由自循環之起點 910 開始，此方法 900 亦可自任何交易中用作起點。

【0213】 判定交易類型之步驟 912 較佳地係基於當前交易的內容。較佳地，當前交易之輸出之大小係用於判定其係附加交易抑或轉入交易。若當前交易為轉入交易，則輸出中之一者將包含至少一個交易出點<PrevOut(s)>。替代地，如參考第一態樣所描述之原像、streamDigest 及事件資料表示部分的存在係用於判定交易是否為附加交易。替代地，如本文中所描述之<PrevOut(s)>欄位之存在係用於判定交易是否為轉入交易(或用於正向遍歷之轉出交易)。替代地，當前交易

之輸出中的欄位之數目係用於判定交易之類型，此係因為附加交易酬載中存在更多欄位。替代地，在當前交易中缺乏塵埃輸出係用於指示當前交易為轉出交易。替代地，輸出之數目係用於判定交易之類型，此係因為轉出交易比附加交易少一個輸出。替代地，當前交易可採用的所有可能結構之範本用於與當前交易進行模式匹配以判定其類型。

交易延展性

【0214】 交易延展性之概念係關於其中有效交易(例如，比特幣交易)的部分可在不使該交易無效之情況下進行修改的現象。通常，交易 id 係用於引用交易，其中交易 id 為整個交易的散列。因此，在引用交易時出現問題，此係因為對交易的任何部分之任何修改亦將改變交易之散列，此可能使對該交易的任何引用無效。

【0215】 一般而言，存在在區塊鏈交易中為可能的二種廣泛類型的延展性，二者均允許在不使提供於輸入中或經由輸入提供之簽名無效的情況下修改交易之內容。

【0216】 對於此實例，在二種狀況下，假設初始交易 Tx 具有一個輸入、彼輸入中之一個簽名及一個輸出。

類型 1：指令碼層級延展性

【0217】 此類型的延展性利用以下事實：將運用指令碼作業碼 OP_CHECKSIG 檢查之比特幣簽名不對含有簽名之交易中之任何輸入的 scriptSig 欄位進行簽名。

【0218】 此事實允許吾等生成關於交易 Tx 之簽名，修改輸入指令碼使得交易 Tx'與 Tx 不相同，且仍將 Tx 及 Tx'視為在區塊鏈共識規則下藉由相同簽名簽名之有效的交易訊息。

類型 2：輸入及輸出層級延展性

【0219】 此類型的延展性依賴於使用 SIGHASH 旗標而非在交易中使用之 SIGHASH_ALL。

【0220】 若交易 Tx 具有使用五個其他 SIGHASH 旗標組合中之任一者之輸入簽名，則輸入或輸出可經添加以創建不相同的交易 Tx'，使得根據共識將會將 Tx 及 Tx'二者視為有效的交易訊息，而無需更改簽名。

【0221】 因此，本文中所描述的態樣之每一交易較佳地使用 SIGHASH_ALL 旗標以克服此延展性。

【0222】 有利地，以下第三、第四、第五及第六態樣包含提供用於確保引用的不變性之其他及/或替代技術的資料結構及相關聯的方法。

【0223】 對交易之術語「不變引用」意謂對基於一旦交易已經公佈比特幣網路而無法修改(亦即，不變)之交易中之資料的有效交易的引用。

【0224】 對交易之「不可變引用」通常意謂已確認交易之交易 ID，其無法在較高確定性程度內改變。不變引用可為不可變引用。

【0225】 若在於轉出交易之酬載中包括轉入交易之交易 id 與在區塊鏈上包括(亦稱為確認)轉入交易之間修改轉入交易之部分，則轉入交易之交易 id 在儲存於轉出交易上之轉入交易與儲存於區塊鏈上之轉入交易之間將為不同的，藉此打破了使二個塵埃鏈橋接之引用。

【0226】 換言之，當轉出交易之正向引用應指向基於經修改交易 id 之新交易 id 時，該正向引用係針對不正確的轉入交易 id。若要進行此修改，則此將完全達不到包括引用的目的，此係因為其將不再指向正確的鏈上交易以繼續遍歷事件流。

【0227】 發生此攻擊的風險係非零的，在該攻擊中，惡意的挖掘者或竊聽者設法在將交易傳播至比特幣網路的很大一部分之前對該交易進行修改。因此，需要找到此問題的穩定解決方案。

【0228】 附加交易之延展性不因如上文在「交易可延展性」標題下所論述的不可延展的支出引用而發生。轉出及轉入交易無法具有此支出鏈路(否則，其不可用於克服祖先限制)。

確認區塊鏈上之轉入交易

【0229】 參考圖 10，展示根據第三態樣之資料結構 1000，其用於創建不可變轉入交易 1016 及對轉入交易 1014 之不變且不可變引用 1018。運用不可變轉入交易，可創建對轉入交易的不可變引用，藉此克服了在上文標題「交易延展性」下論述的轉入交易延展性問題。

【0230】 圖 10 與之前的圖以不同方式呈現資料結構，不同之處在於其按時間順序展示(較早提交之交易在頁面上顯示更高)且描述區塊鏈中之哪些區塊包含哪些交易。哪些區塊 1050、1052 包含哪些交易與此態樣相關。

【0231】 圖 10 包含與第二態樣中之特徵類似的特徵之類似附圖標記及名稱。舉例而言，每一附加交易 1004a 至 1004d 及最終交易 1026 包含對其前一交易之反向支出引用 1006a 至 1006f。此係類似於如圖 7A 中所展示之附加交易 704a 至 704d 及最終交易 726，其亦包含對其前一交易之反向支出引用 706a。

【0232】 本發明態樣任擇地包括第一態樣之第二反向引用特徵 608 及第三反向引用特徵 610、612a 至 612c。

【0233】 在本發明態樣中，在轉出交易 1014 引用轉入交易 1016 之前，在區塊鏈上之區塊 1050 中確認該轉入交易。一旦已經在區塊鏈上確認轉入交易，則惡意挖掘者幾乎不可能改變交易且因此改變交易 id。引用 1018 因此係不可變的，此係因為該引用係有效的且將始終為有效的。不能改變引用或交易。

【0234】 仍可支出轉入交易之輸出，使得下一附加交易 1004c 可引用轉入交易 1016，而無需等待在區塊中確認該轉入交易。因此，仍可提交附加交易，而無需等候確認轉入。塵埃鏈抽象層級處之所得資料結構 1000 的外觀及操作方

式將與如所參考圖 7A、圖 7B 及圖 9 所描述的外觀及操作方式相同。

【0235】 如第二態樣中所描述之用於將資料項目添加至塵埃鏈且有條件地創建新塵埃鏈之方法在此態樣中實質上相同地操作，除了延遲創建且提交轉出交易 1014 之步驟 818，直至轉入交易已經包括於區塊鏈上之區塊中為止以外。此步驟 818 可與該方法之其餘部分異步地運行，此係因為此態樣中沒有其他交易引用轉出交易 1014。一旦轉入交易 1016 已經提交至區塊鏈，則可支出其輸出，且該方法照常繼續。

【0236】 轉入交易包含對前一鏈之鏈引用 1024，其類似於如參考圖 7A 在第二態樣中所描述之鏈引用 724。

【0237】 資料結構 1000 之遍歷方法與在第二態樣中參考圖 9 所描述實質上相同。

不可延展的正向轉入引用

【0238】 參考圖 11，展示根據第四態樣之資料結構 1100，其用於創建對轉入交易 1116 之不變引用 1118。

【0239】 雖然第四態樣確實包含類似於第二及第三態樣之自轉出交易 1114 至轉入交易 1116 之正向引用 1118，而非正向引用 718 為轉入交易 1116 之交易 id，但該引用包含轉入交易 1116 之輸入中之至少一者。較佳地，對輸入中之至少一者之引用係呈交易出點之形式，其中該交易出點包含交易 id，其包含輸出及該輸出之索引。較佳地，引用 1118 包含由轉入交易 1116 消耗之先前交易輸出的集合。先前交易輸出之集合被稱作 $PrevOuts_{change\text{-}in}$。$PrevOuts_{change\text{-}in}$ 之實例格式為：

$$PrevOuts_{change-in} = \{PrevOut_1 : (TxID_{Prev,1}, vout_1), PrevOut_2 : (TxID_{Prev,2}, vout_2)\}。$$

【0240】 其中 $TxID_{Prev,n}$ 為包含支出之輸出的交易之交易 id，且 $vout_n$ 為該

交易中之該輸出之索引。元組$(TxID_{Prev,n}, vout_n)$為交易出點。用於交易之*PrevOut*之集合中的每一*PrevOut*本身均為唯一的，此係因為每一者均為區塊鏈上之交易輸出且均為唯一的。因此，*PrevOut*集合亦為唯一的。

【0241】較佳地，正向應用按以下形式儲存於轉出交易之輸出的指令碼部分中：

OP_FALSE OP_RETURN 0x20 <$TxID_{Prev1}$> <index length> <$vout_1$>

【0242】若多於一個資金輸入係用於為轉入交易提供資金，則其他輸入經附加至以上格式，如下所示：

<$TxID_{Prevn}$> <index length> <$vout_n$>

【0243】更佳地，指令碼在 OP_RETURN 之後並且在 PrevOut 引用之前包含 0x20 <$txid_{create}$>。

【0244】因此，對轉入交易之引用 1118 並非基於轉入交易 1116 之交易 id 或任何其他可延展部分或態樣。以此方式，即使在惡意挖掘者修改交易之情況下，引用 1118 仍將有效，藉此克服了如在以上標題「轉入交易延展性」下所論述的轉入交易延展性問題。

【0245】若交易已完成(亦即，有效，並且其所有簽名均使用新輸入/輸出無法添加至的適當的旗標)，吾人可假設本文中所描述的態樣中之任一者的交易中均為該狀況(任何輸入簽名都應使用如上文所論述之 SIGHASH_ALL 旗標)，則交易之可修改的僅有部分為解鎖指令碼欄位。輸出中之鎖定指令碼不可改變，此係因為輸入應含有在其上簽名之簽名。輸出之任何改變將使此等簽名失效。只要$PrevOuts_{change\text{-}in}$引用 1118 出現在轉出交易 1114 之輸出中，則無法修改引用 1118，因為其位於輸出指令碼中。即使交易之輸入指令碼被某人修改，當遍歷塵埃鏈時，*PrevOut*引用亦將不改變且亦將產生正確的交易。

【0246】圖 11 包含用於類似於第二及/或第三態樣中之特徵的特徵之類似

附圖標記及名稱。舉例而言，每一附加交易 1104a 至 1104d 及最終交易 1126 包含對其前一交易之反向支出引用 1106a 至 1106f。此係類似於如圖 7A 中所展示之附加交易 704a 至 704d 及最終交易 726，其亦包含對其前一交易之反向支出引用 706a 至 706f。

【0247】 如本發明態樣中所描述之正向遍歷資料結構 1100 之方法與第二態樣中參考圖 9 所描述之方法 900 實質上相同，除了下文所概述之差異以外。在本發明態樣中，在步驟 922 中提取之引用為 $PrevOuts_{change\text{-}in}$ 引用 1118，而非轉入交易之交易 id。基於此引用 1118 定位轉入交易 1116。藉由尋找包含 $PrevOuts_{change\text{-}in}$ 輸出之至少一子集作為輸入之交易來發現轉入交易 1116。接著對轉入交易 1116 進行散列以獲得其交易 id，且方法 900 自基於轉入交易 id 發現 928 下一附加交易而照常繼續。

【0248】 本發明態樣任擇地等待確認轉入交易 1116 以用於額外安全性。本發明態樣任擇地包括第一態樣之第二反向引用特徵 608 及/或第三反向引用特徵 610、612a 至 612c。

【0249】 如第二態樣中所描述之用於將資料項目添加至塵埃鏈且有條件地創建新塵埃鏈之方法在此態樣中實質上相同地操作，除了使用不同引用之外。

【0250】 任擇地，除了如態樣二及三中所描述之反向引用 718、1018 之外，亦使用不變正向引用 1118。

【0251】 雖然在此態樣中已經使用轉入交易之輸入的完整集合，但亦可使用 PrevOut 之子集。舉例而言，若轉入交易包含二個輸入，則如下：

$$PrevOuts_{change-in} = \{PrevOut_1 : (TxID_{Prev,1}, vout_1), PrevOut_2 : (TxID_{Prev,2}, vout_2)\}。$$

對轉入交易之引用係基於二者中之僅一者。此仍為對轉入交易之唯一引用，此係因為一旦已經將此交易公佈至比特幣網路，則先見規則及僅可在鏈上消耗

出點一次之事實確保此出點永不會被替代交易消耗。應注意，「替代」在此處係指交易之結構，亦即其輸入、輸出及價值交換，且確實阻止交易藉由延展性進行非功能性改變。

【0252】 不管是否發生任何此類延展性，交易的最終形式總是可藉由檢查哪個交易消耗了出點來唯一地識別。

【0253】 僅使用一個引用可為較佳的，此係因為僅需要單個輸出來創建基於唯一輸入(或基於 PrevOut)之引用，因為其將顯著地縮減引用之總體大小。此繼而縮減將引用包括在鏈上交易中之交易費用的成本。比特幣中基於 prevOut 之引用的最小大小可小至 36 位元組(32 位元組 TxID，及 4 位元組 vout)，且因此，引用之大小亦隨經引用交易之輸入之數目而按比例調整$O(1)$。

【0254】 因此，PrevOut 引用可包含至轉入交易之至少一個輸入中之至少一者。且較佳地，PrevOut 引用包含至轉入交易之至少一個輸入中之僅一者。

對轉出之反向引用

【0255】 雙向引用允許一對交易傳信其與另一者之關係。此外，此允許獨立於被視為起點之交易識別二者之間的鏈接，亦即在事件或資料項目之線性序列之狀況下允許正向及反向遍歷。

【0256】 然而，在實踐中，由於一般而言，每一引用應展現唯一性，因此實現此類雙向引用係困難的。由於循環引用，因此可能難以實現唯一性之屬性。散列函數之使用為將唯一識別符指派至資料之常用方式。然而，並非不可能在二個區塊鏈交易之間創建雙向基於散列之引用，此係因為此創建了循環引用。

【0257】 參考圖 12 及圖 13，展示根據第五態樣之資料結構 1200 及遍歷資料結構之方法 1300。資料結構 1200 包含自轉出交易 1214 至轉入交易 1216 之不變正向引用 1218 及自轉入交易 1216 至轉出交易 1214 之反向引用 1224。

【0258】 圖 12 包含用於類似於第二、第三及/或第四態樣中之特徵的特徵

之類似附圖標記及名稱。舉例而言，每一附加交易 1204a 至 1204d 及最終交易 1226 包含對前一交易之反向支出引用 1206a 至 1206f。此係類似於如圖 7A 中所展示之附加交易 704a 至 704d 及最終交易 726，其亦包含對其前一交易之反向支出引用 706a 至 706f。不變正向引用 1218 的構造及功能與參考圖 11 所描述的不變正向引用 1118 相同或類似。

【0259】 反向引用 1224 包含轉出交易 1224 之交易 id。此係可能的，因為正向引用 1218 不再取決於轉入交易 1216 之交易 id，藉此避免了如上文所描述之循環散列引用之問題。

【0260】 運用反向引用 1224，可在橫跨任何轉出/轉入交易反向遍歷塵埃鏈。圖 13 中所展示的遍歷之電腦實施方法 1300 開始於塵埃鏈中之最終交易 1226。熟習此項技術者將瞭解，該方法可藉由在循環開始時在步驟 1308 處起始而任擇地開始於塵埃鏈上之任何位置。

【0261】 如同反向遍歷之方法 900，有利地，此遍歷方法 1300 不需要隱藏知識來遍歷除區塊鏈上之交易的格式之外的交易。遍歷中所使用之引用均與資料項目一起公佈在區塊鏈上。因此，第三方亦能夠遍歷塵埃鏈且獲得、儲存、認證及/或以其他方式使用儲存於區塊鏈上之資料項目，而無需任何專用或專有服務。值得注意的是，由於區塊鏈及目前的資料寫入系統及方法之性質，對儲存於區塊鏈上之資料進行之任何操作均為唯讀的。修改儲存於區塊鏈上之資料並不實際。

【0262】 第一步驟 1302 將獲得最終交易，自此，該方法反向遍歷塵埃鏈。

【0263】 任擇地，塵埃鏈中之第一交易之交易 id 儲存於最終交易中。初始交易之交易 id 經儲存以供稍後引用。

【0264】 藉由對最終交易進行散列而提取 1306 最終交易之交易 id。該交易 id 經指派為當前交易 id。該方法接著進入對當前交易進行操作之循環。

【0265】 該循環中之第一步驟將判定 1308 當前交易 id 是否係指初始交易。任擇地，此係藉由比較當前交易之交易 id 與初始交易 id 來進行，其儲存於第二步驟 1304 中。替代地，在獲得 1310 交易之後進行此判定 1308。該判定 1308 接著係基於儲存於交易中之資料及/或後設資料。舉例而言，若一交易在其後設資料中包含種子，如參考圖 6C 在第二態樣中所描述，則有可能判定該交易為初始交易。

【0266】 若當前交易為初始交易，則循環終止。任擇地，基於經供應交易 id，該循環在另一交易處終止。

【0267】 基於當前交易 id 獲得 1310 當前交易(除非作為判定當前交易是否為初始交易之部分，已經獲得交易)。

【0268】 若當前交易為附加交易，如基於如第一態樣中所描述之酬載之存在所判定 1312，則任擇地對交易之酬載進行操作 1314。

【0269】 較佳地，該操作將認證當前交易。該認證係基於如參考圖 6A 及圖 6B 所描述之第三反向引用 610、612a 至 612c。當前酬載之串流摘要連同用於循環中之下一酬載之串流摘要一起經儲存以用於在下一循環反覆中進行認證。若在循環中已經存在自先前的反覆儲存的串流摘要，則將當前交易的串流摘要與該儲存的先前的串流摘要進行比較，以認證串流摘要是否為正確的。

【0270】 另外或替代地，儲存酬載之資料項目以供稍後使用。另外或替代地，調用由遍歷者提供之回調，藉此允許藉由遍歷者對酬載進行任意操作。

【0271】 自當前交易提取 1316 鏈中之下一交易的交易 id。鏈中之下一交易之交易 id 作為至當前交易之輸入加以儲存。

【0272】 下一交易 id 作為當前交易 id 加以儲存 1318，且該循環在循環之開始 1318 處重新開始。

【0273】 返回至判定 1312 交易類型之步驟，若交易為轉入交易，則獲得對

轉出交易之引用。較佳藉由自儲存引用之轉入交易提取 1320 該引用而獲得該引用。在本發明態樣中，對轉出交易之引用為轉出交易之交易 id。

【0274】 接著使用轉出交易之交易 id 來獲得 1322 轉出交易。

【0275】 自當前交易提取 1324 鏈中之下一交易的交易 id。鏈中之下一交易之交易 id 作為至轉出交易之輸入經儲存。

【0276】 下一交易 id 作為當前交易 id 經儲存 1326，且該循環在循環之開始 1318 處重新開始。

【0277】 本發明態樣之用於將資料項目添加至塵埃鏈且有條件地創建新塵埃鏈之方法與第二態樣實質上以相同方式操作，除了使用轉入與轉出之間的不同引用之外。

【0278】 本發明態樣之正向遍歷資料結構 1200 之方法與第四態樣實質上以相同方式操作，因為其包含相同的自轉出至轉入之反向引用。

【0279】 熟習此項技術者將瞭解，可反過來使用該等引用，使得轉出交易包含轉入交易之交易 id，且轉入交易包含對轉出交易之輸入的引用。

【0280】 判定交易類型之步驟 1312 (該交易係附加抑或轉入)與參考正向遍歷方法所描述相同或類似地進行，除了判定轉入交易而非轉出交易之外(因為反向遍歷首先遇到轉入遍歷)。替代地，在當前交易中缺乏塵埃輸入係用於指示當前交易為轉入交易。替代地，輸入之數目係用於判定交易之類型，此係因為轉入交易比附加交易少一個輸出。

不可延展的反向轉出參考

【0281】 參考圖 14，根據第六態樣之資料結構 1400 用於創建自轉出交易 1414 至轉入交易 1416 之不變正向引用 1418 及自轉入交易 1416 至轉出交易 1414 之不變反向引用 1424。

【0282】 圖 14 包含用於類似於第二、第三、第四及/或第五態樣中之特徵

的特徵之類似附圖標記及名稱。舉例而言，每一附加交易 1404a 至 1404d 及最終交易 1426 包含對其前一交易之反向支出引用 1406a 至 1406f。此係類似於如圖 7A 中所展示之附加交易 704a 至 704d 及最終交易 726，其亦包含對其前一交易之反向支出引用 706a 至 706f。

【0283】 自轉出交易 1414 至轉入交易 1416 之正向引用 1418 之形成及操作方式與第五態樣中所描述之正向引用 1218 實質上相同。

【0284】 自轉入交易 1416 至轉出交易 1414 之反向引用 1424 係基於 $PrevOuts_{change\text{-}out}$ 集合。$PrevOuts_{change\text{-}out}$ 集合之構造方式與如第四態樣中所描述之 $PrevOuts_{change\text{-}in}$ 集合之構造方式相同，然而，$PrevOuts_{change\text{-}out}$ 集合使用轉出交易所消耗之交易輸出。使用與第四態樣類似的引用方法具有相同的優點，尤其是在不變性方面。$PrevOuts_{change\text{-}out}$ 集合任擇地僅包含至少一個輸入中之一者。

【0285】 以下反向引用 1424 亦以相同方式進行。定位支出存在於 $PrevOuts_{change\text{-}out}$ 集合中之交易及索引的交易。此交易為轉出交易。

【0286】 因此，正向或反向遍歷之方法與如第五態樣中所描述以實質上相同的方式操作，除了當反向遍歷時，不使用轉出交易之交易 id，如上文所描述使用 $PrevOuts_{change\text{-}out}$ 引用。

【0287】 如第二態樣中所描述之用於將資料項目添加至塵埃鏈且有條件地創建新塵埃鏈之方法在此態樣中實質上相同地操作，除了使用不同引用之外。

交會交易

【0288】 根據第七態樣，塵埃鏈進一步包含交會交易。交會交易之其他細節經描述於英國專利申請案第 2020279.2 號(2020 年 12 月 21 日以 nChain Holdings Limited 之名稱提交)中且特此以引用之方式併入。

【0289】 關於附加的新資料項目(如參考圖 8 所描述)，塵埃鏈實質上相同地操作，除了將需要關於祖先限制考慮交會交易之存在之外。

【0290】 關於遍歷塵埃鏈(如參考圖 9 及圖 13 所描述)，塵埃鏈實質上相同地操作，除了進行交易類型檢查步驟 912、1312 中之額外檢查之外。此處，若當前交易經判定為交會交易，則類似於附加交易，對當前交易進行反覆，因為其與附加交易包含相同的塵埃引用。基於如參考第一態樣所描述之多個酬載的存在，當前交易經識別為交會交易。因為交會交易包含與不同鏈相關聯之多個塵埃輸入及輸出，所以選擇正確的塵埃輸出以繼續遍歷。圖 18 中提供包含交會交易 1802 的塵埃鏈之資料佈局 1800。因為存在多個酬載，所以其在交會交易中藉由「r」索引化，且在 $2r$ 及 $2r + 1$ 處提供相關輸出。

【0291】 若正向遍歷塵埃鏈且定位交會交易，則如參考圖 9 所描述之方法 900 另外包含以下步驟。

【0292】 由於判定 912 當前交易為交會交易，因此此等步驟將發生。需要交會交易之相關輸出以繼續遍歷該鏈。

【0293】 首先，藉由定位支出前一交易之塵埃出點之輸入來判定索引「r」。儲存資料之輸出接著定位於 $2r + 1$ 處，且塵埃鏈輸出定位於 $2r$ 處。

【0294】 接下來，在定位塵埃鏈輸出之情況下，定位下一交易。藉由獲得支出出點($TxID_{rendezvous}$, 2r)之交易來定位下一交易，其中 TxID 為交會交易之交易 id，且藉由隨交會交易進行散列而獲得。

【0295】 此下一交易用作方法 900 之循環 910 的開始之當前交易，且該方法繼續。

【0296】 任擇地，儲存於 $2r + 1$ 處之資料具有對其進行之操作，如參考進行圖 9 之方法 900 之操作步驟 914 所描述。

【0297】 作為實例，若正向遍歷圖 18 之鏈 L，則與 L 鏈相關之輸出位於位置 4 及 5 處且資料儲存於 5 中，且塵埃鏈儲存於 4 中，亦即 $r = 2$。r 係藉由查看 L + 2 交易(交會交易之前的交易)的塵埃輸出(第零輸出)並發現哪一輸入支出該

輸出來判定的。在此狀況下，輸入位於交會交易的索引 2 處。在判定 r = 2 之情況下，交會交易的相關輸出為 2r = 4 且 2r+1 = 5。為了繼續遍歷 L + 4 交易，對交會交易進行散列，且支出輸出($TxID_{rendezvous}$, 4)之交易將為 L+4。

【0298】 若反向遍歷塵埃鏈且定位交會交易，則如參考圖 13 所描述之方法 1300 另外包含以下步驟。此等額外步驟類似於正向步驟，但反過來除外。

【0299】 除了指派 $TxID_i = TxID_{i-1}$ 的最後步驟之外，塵埃出點之索引部分(此處被稱作「k」)亦儲存於每一循環反覆中(及初始步驟)，使得吾人另外指派 $k_i = k_{i-1}$。

【0300】 由於判定 1312 當前交易為交會交易，因此此等步驟將發生。需要交會交易之相關輸入以繼續遍歷該鏈。

【0301】 首先，「*r*」經設定為 $k_i / 2$。運用「*r*」索引，獲得交會交易之索引「r」處之輸入。該輸入包含 $TxID_{i-1}$。

【0302】 該循環在指派 $TxID_i = TxID_{i-1}$ 之後自其起始步驟 1308 繼續。

【0303】 任擇地，儲存於 $2r + 1$ 處(或替代地在 k_{i+1} 處描述)之資料具有對其進行之操作，如參考進行圖 13 之方法 1300 之操作步驟 1314 所描述。

【0304】 作為實例，再次，若反向遍歷圖 18 之鏈 L，則吾人判定當前交易為交會交易 1802。自先前反覆，已經知道且儲存索引 k_i (自前一反覆中之經消耗出點)。k_i 為 4 且除以 2 以得到 $r = 2$。因此，交會交易之相關輸入係在索引 2 處。藉由索引 2 處之輸入消耗的出點之交易 id 為 $TxID_{i-1}$。為了繼續遍歷，使用其交易 id $TxID_{i-1}$ 來定位交易 L+2。

【0305】 任擇地，與交會交易相關聯之任何資料經獲得且儲存以供遍歷者使用。

PrevOut 交易延展性

【0306】 根據第八態樣，描述克服 PrevOut 輸入之延展性的方法。如態樣

四及六中所描述之為轉入交易及轉出交易提供資金(且用作引用，對於此態樣經引用為「資金交易」)之交易易受如貫穿描述所描述之相同延展性問題影響。若在用作引用與經確認為引用之間修改資金交易，則可在至少一個方向上不可逆地打斷該鏈，藉此防止遍歷塵埃鏈。

【0307】 此外，若不在區塊鏈上確認此等資金交易，則其造成未確認的祖先計數。

【0308】 為了克服此延展性問題，調用類似於參考態樣三所描述之解決方案的解決方案。在接近祖先限制之前(且因此在在轉入交易及轉出交易中必須使用資金交易之前)，資金交易經提交至區塊鏈且經確認。藉由已經在區塊鏈上確認資金交易，其將為不可變的。

【0309】 較佳地，直至確認了用於轉入交易之資金交易才將轉出交易提交至區塊鏈。較佳地，直至確認了用於轉出交易之資金交易才將轉入交易提交至區塊鏈。

【0310】 此具有另一優點：資金交易將不會造成未確認的祖先限制。替代地或另外，臨限數目比最大的未確認的祖先限制小二個，以說明此資金交易。

【0311】 任擇地，提交轉入資金交易使得其在區塊鏈上經確認且為不可變的係藉由與參考圖 16 所描述之服務相關聯的資金服務來進行。資金服務任擇地維護多個資金交易，該等交易已在區塊鏈上確認，可供資料寫入服務使用。

資料寫入服務

【0312】 根據另一態樣，前一態樣之資料結構及方法中之任一或多者可與如下文所描述之平台處理器一起使用，該平台處理器用於至少提供如上文所描述之有序唯加資料儲存。此另一態樣可為平台即服務(PaaS)及軟體即服務(SaaS)，其使得能夠使用諸如 BSV 區塊鏈之區塊鏈網路來快速遞送有用的真實世界企業及技術應用，諸如經軟體控制的技術系統或智慧型合約之管理。

【0313】 平台服務之概述可見於圖 15 中，其展示系統之高層級示意圖。平台服務具有提供 API 1508 之平台處理器 1500，可由一或多個用戶端經由該 API 存取服務。

【0314】 如此圖中所展示之平台服務 1500 由三個服務系列構成，且旨在允許使用者及組織容易且安全地利用由區塊鏈之特有性質提供的優勢，而實際上無需在用戶端末端處實施任何基於區塊鏈之軟體、知識或庫。此等服務為：

-資料服務 1502，其旨在簡化鏈作為商品資料分類帳之使用。資料服務較佳地使用本文中提供之資料結構及方法以用於實施將資料寫入至區塊鏈及自區塊鏈讀取資料。

-計算服務 1504，其旨在提供由諸如比特幣 SV 之數位資產支援之一般化計算框架。

-商務服務 1506，其提供用於使用諸如比特幣 SV 之數位資產進行交易之企業級能力。

【0315】 可經由或使用 HTTPS 協定在 API 處自用戶端接收請求，此係因為 API 被實施為網路服務。接著由一或多個服務模組或處理資源 1502 至 1506 使用基礎軟體 1510 實施所請求服務，此基礎軟體 1510 係與區塊鏈相關聯，亦即以實施資源、庫及/或密鑰管理電子錢包實施以用於創建、處理及提交與區塊鏈相關聯之交易。一旦經處理，可將交易提交至區塊鏈網路 1512 (而非實施任何此功能性或交易庫之用戶端)。至多，用戶端可實施與密碼貨幣或某一其他數位資產相關聯之數位電子錢包等，但此並非必要的，此係因為平台服務 1500 亦可能夠提供及管理用於用戶端之數位資產。

【0316】 圖 16 提供與區塊鏈相關聯之多個服務的較細化示意圖，且該等服務可由與 API 相關聯之平台 1600 實施，經由該 API 可存取所提供服務中之任一或多者。如此圖中所見，資料服務 1602 可包括資料寫入器服務 1602a 及資料讀

取器服務 1602b。資料寫入器服務及資料閱讀器服務較佳地使用如第六態樣中所描述之資料結構。替代地，使用此處所描述之其他態樣中之任一或多者。資料寫入器服務 1602a 之實例使用為如上文簡單論述之事件流。參考英國專利申請案第 2002285.1 號(2020 年 2 月 19 日以 nChain Holdings Limited 之名稱提交且特此以引用之方式併入)之圖 4 至圖 8 論述事件流之其他細節。資料寫入器服務 1602a 使得用戶端能夠以簡單、安全且最佳的方式將資料寫入至區塊鏈中。資料讀取器服務 302b 使得用戶端能夠發送查詢，該查詢傳回儲存於區塊鏈中之資料。此可使用經濾波串流，其中用戶端可預定義其希望臨時或定期地(亦即，在某一時間框內)自區塊鏈讀取的資料類型，或與區塊鏈 1610 中處理的相關或不相關事件或文件之集合相關聯的彼等資料類型。資料封存特徵允許存取指定事件或合約之先前交易之日誌。

【0317】 平台 1600 之計算服務 1606 包括與智慧型合約相關聯的應用程式 1606a 及框架 1606b，其在一些實施例中可表示為區塊鏈 1610 中之狀態機。計算服務 1606 與資料服務 1602 互動，此係因為資料將需要被輸入且結果需要被提供至用戶端以用於任何此計算。

【0318】 商務服務 1604 負責經由企業電子錢包 1604a 提供企業級能力，以用於基於一流的安全實踐及技術在區塊鏈 1610 上進行交易。舉例而言，在一些實施例中，企業電子錢包可實施在多於一個人員或使用者或帳戶可能需要在滿足經定義準則，亦即與高於某一預定義限值之較大密碼貨幣值相關聯之交易上簽出時實現區塊鏈交易處理的功能性。企業電子錢包亦可包括實施臨限數目及/或類型之簽名以移動大量數位資產，諸如密碼貨幣或表示另一資源之符記的功能性。可接著基於由此類企業電子錢包實施應用之準則在處理之後在區塊鏈上表示此等資產之移動。

【0319】 SPV 服務 1608 (簡化之支付認證)為需要來自區塊鏈之資訊但並

不包括至區塊鏈之直接鏈路的應用程式，此係因為該等服務並不運行挖掘者節點。此類 SPV 服務 1608 允許輕型用戶端認證交易是否包括於區塊鏈中，而無需下載整個區塊鏈 1610。

資料寫入裝置

【0320】 現轉而參看圖 17，提供計算裝置 2600 之說明性簡化方塊圖，該計算裝置可用於實踐本揭露內容之至少一個實施例。在各種實施例中，計算裝置 2600 可用於實施上文所說明及描述之系統中之任一者。舉例而言，計算裝置 2600 可經組配以用作圖之 DBMS 之一或多個組件，或計算裝置 2600 可經組配以為與給定使用者相關聯的用戶端實體；該用戶端實體產生對於由圖 9 之 DBMS 管理之資料庫之資料庫請求。因此，計算裝置 2600 可為便攜式計算裝置、個人電腦，或任何電子計算裝置。如圖 17 中所展示，計算裝置 2600 可包括具有快取記憶體之一或多個層級的一或多個處理器以及可經組配以與包括主記憶體 2608 及持久性儲存器 2610 之儲存子系統 2606 通訊的記憶體控制器(共同地標記為 2602)。主記憶體 2608 可包括如所展示之動態隨機存取記憶體(DRAM) 2618 及唯讀記憶體(ROM) 2620。儲存子系統 2606 及快取記憶體 2602 且可用於儲存資訊，諸如與如本揭露內容中所描述之交易及區塊相關聯的細節。處理器 2602 可用以提供如本揭露內容中所描述之任何實施例的步驟或功能性。

【0321】 處理器 2602 亦可與一或多個使用者介面輸入裝置 2612、一或多個使用者介面輸出裝置 2614 及網路介面子系統 2616 通訊。

【0322】 匯流排子系統 2604 可提供用於使計算裝置 2600 之各個組件及子系統能夠按預期彼此通訊之機制。儘管匯流排子系統 2604 經示意性地展示為單一匯流排，但匯流排子系統之替代實施例可利用多個匯流排。

【0323】 網路介面子系統 2616 可提供至其他計算裝置及網路之介面。網路介面子系統 2616 可充當用於自其他系統接收資料及將資料自計算裝置 2600 傳

輸至其他系統之介面。舉例而言，網路介面子系統 2616 可使資料技術員能夠將裝置連接至網路，使得資料技術員可能夠在處於諸如資料中心之遠端位置中時將資料傳輸至裝置及自裝置接收資料。

【0324】 使用者介面輸入裝置 2612 可包括：一或多個使用者輸入裝置，諸如鍵盤；指標裝置，諸如整合式滑鼠、軌跡球、觸摸板或圖形平板電腦；掃描器；條形碼掃描器；觸摸螢幕，其併入至顯示器中；音訊輸入裝置，諸如語音辨識系統、麥克風；及其他類型之輸入裝置。一般而言，術語「輸入裝置」之使用意欲包括用於將資訊輸入至計算裝置 2600 之所有可能類型的裝置及機構。

【0325】 一或多個使用者介面輸出裝置 2614 可包括顯示子系統、印表機或諸如音訊輸出裝置之非視覺顯示器等。顯示子系統可為陰極射線管(CRT)、諸如液晶顯示器(LCD)之平板裝置、發光二極體(LED)顯示器或投影裝置或其他顯示裝置。一般而言，使用術語「輸出裝置」意欲包括用於輸出來自計算裝置 2600 之資訊的所有可能類型的裝置及機構。舉例而言，一或多個使用者介面輸出裝置 2614 可用以呈現使用者介面以在使用者與應用程式之互動可係適當的時促進此互動，該等應用程式執行所描述之程序及其中之變化。

【0326】 儲存子系統 2606 可提供電腦可讀儲存媒體，該電腦可讀儲存媒體用於儲存可提供本揭露內容之至少一個實施例之功能性的基本程式設計及資料建構。應用程式(程式、程式碼模組、指令)在由一或多個處理器執行時可提供本揭露內容之一或多個實施例的功能性，且可儲存於儲存子系統 2606 中。此等應用程式模組或指令可由一或多個處理器 2602 執行。儲存子系統 2606 可另外提供用於儲存根據本揭露內容所使用之資料的儲存庫。舉例而言，主記憶體 2608 及快取記憶體 2602 可提供用於程式及資料之依電性儲存器。持久性儲存器 2610 可提供用於程式及資料之持久性(非依電性)儲存器且可包括快閃記憶體、一或多個固態驅動機、一或多個磁性硬碟驅動機、具有相關聯可移除式媒體之一或多個

軟碟驅動機、具有相關聯可移除式媒體之一或多個光學驅動機(例如 CD-ROM 或 DVD 或 Blue-Ray)驅動機及其他類似儲存媒體。此類程式及資料可包括用於實行如本揭露內容中所描述的一或多個實施例之步驟的程式以及與如本揭露內容中所描述之交易及區塊相關聯的資料。

【0327】 計算裝置 2600 可具有各種類型，包括便攜式電腦裝置、平板電腦、工作站或下文所描述之任何其他裝置。另外，計算裝置 2600 可包括可藉由一或多個埠(例如 USB、耳機插口、閃電連接器等)連接至計算裝置 2600 之另一裝置。可連接至計算裝置 2600 之裝置可包括經組配以接受光纖連接器之多個埠。因此，此裝置可經組配以將光學信號轉換成可藉由將裝置連接至計算裝置 2600 之埠傳輸的電信號以供處理。歸因於電腦及網路不斷改變之本質，出於說明裝置之較佳實施例之目的，圖 16 中描繪之計算裝置 2600 之描述僅意欲作為一特定實例。具有比圖 16 中描繪之系統多或少之組件的許多其他組配係可能的。

【0328】 上文所述之各種方法可能由電腦程式實施。電腦程式可包括電腦程式碼，其經配置以指示電腦執行上文描述之各種方法中的一或多者的功能。電腦程式及/或用於執行此類方法之程式碼可在一或多個電腦可讀媒體上，或更一般化地，在電腦程式產品上被提供至諸如電腦的設備。電腦可讀媒體可係暫時性或非暫時性的。舉例而言，該一或多個電腦可讀媒體可能為電子、磁性、光學、電磁、紅外線或半導體系統，或用於資料傳輸，例如用於跨越網際網路下載程式碼之傳播媒體。替代地，該一或多個電腦可讀媒體可能呈一或多個實體電腦可讀媒體之形式，諸如半導體或固態記憶體、磁帶、可移除電腦磁盤、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、剛性磁碟，及光碟，諸如 CD-ROM、CD-R/W 或 DVD。

【0329】 除非另外具體陳述，否則，如自以下論述顯而易見，應瞭解，貫穿描述，利用諸如「判定」、「提供」、「運算」、「計算」、「識別」、「組

合」、「建立」、「發送」、「接收」、「儲存」、「估計」、「檢查」、「獲得」等等之術語的論述係指電腦系統或類似電子計算裝置之動作及製程，該電腦系統或類似電子計算裝置將電腦系統之暫存器及記憶體內之表示為物理(電子)量之資料操縱且變換成電腦系統記憶體或暫存器或其他此類資訊儲存、傳輸或顯示裝置內之類似地表示為物理量之其他資料。

經枚舉實例實施例

【0330】 本揭露內容特此基於與上述態樣相關之以下條項來論述，該等條項在本文中經提供作為例示性實施例以用於較佳地解釋、描述及理解態樣及實施例。

【0331】 1.一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一交易，其包含：

一第一輸出；及

一第一資料項目之一表示，

一第二交易，其包含：

該第一資料項目之另一表示；

一第二資料項目之一表示；

與該第一輸出相關聯的一第一輸入；及

一第二輸出。

【0332】 2.如條項 1 之電腦實施資料結構，其中該第一資料項目為後設資料及一種子。

【0333】 3.如條項 2 之電腦實施資料結構，其中該第一項目之該表示包含該後設資料，該後設資料包含該種子。

【0334】 4.如條項 2 或 3 之電腦實施資料結構，其中該第一項目之該另一表示包含該種子。

【0335】 5.如條項 1 之電腦實施資料結構，其中該第一資料項目之該第一表示包含該資料項目之一散列。

【0336】 6.如條項 1 之電腦實施資料結構，其中該第一資料項目之該第一表示包含該資料項目。

【0337】 7.如條項 5 或 6 之電腦實施資料結構，其中該第一交易包含一原像，該原像包含該第一資料項目之該第一表示。

【0338】 8.如條項 7 之電腦實施資料結構，其中第一資料結構之該另一表示包含該第一交易之該原像之一散列。

【0339】 9. 如條項 1 至 8 中任一或多項之電腦實施資料結構，其中該第二交易進一步包含對該第一交易之一引用。

【0340】 10.如條項 1 至 9 中任一或多項之電腦實施資料結構，其進一步包含：

一第一類型之一交易，其包含對一第二類型之一交易之一第一引用，及

該第二類型之該交易。

【0341】 11.如條項 10 之電腦實施資料結構，其中該第一引用儲存於該第一類型之該交易的一輸出中。

【0342】 12.一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一類型之一交易，其包含一輸出，該輸出包含對一第二類型之一交易之一第一引用，及

該第二類型之該交易。

【0343】 13.如條項 10 至 12 中任一或多項之電腦實施資料結構，其中該第一引用為一不變引用。

【0344】 14.如條項 13 之電腦實施資料結構，其中該第一引用係基於該第二類型之該交易的一不變特徵。

【0345】 15.如條項 10 至 14 中任一或多項之電腦實施資料結構，其中該第一引用包含該第二類型之該交易的交易 id。

【0346】 16.如條項 10 至 15 中任一或多項之電腦實施資料結構，其中該第二類型之該交易包含至少一個輸入，且該第一引用係基於至該第二類型之該交易的該至少一個輸入中之至少一者。

【0347】 17.如條項 10 至 16 中任一或多項之電腦實施資料結構，其中該第二類型之該交易包含一第二引用。

【0348】 18. 如條項 17 之電腦實施資料結構，其中該第二引用儲存於該第二類型之該交易的一輸出中。

【0349】 19.如條項 17 或 18 之電腦實施，其中該第二引用包含該第一類型之該交易的一交易 id。

【0350】 20. 如條項 17 或 18 之電腦實施資料結構，其中該第二引用為一不變引用。

【0351】 21.如條項 20 之電腦實施資料結構，其中該第二引用係基於該第一類型之該交易的一不變特徵。

【0352】 22.如條項 17、18、20 或 21 中任一或多項之電腦實施資料結構，其中該第一類型之該交易包含至少一個輸入，且該第二引用係基於至該第一類型之該交易的該至少一個輸入中之至少一者。

【0353】 23.如條項 16 或 22 之電腦實施資料結構，其中包含該至少一個輸入之該引用採用一交易出點之形式。

【0354】 24.一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一類型之一交易，其包含：

對一第二類型之一交易之一第一引用；及

至少一個輸入，

該第二類型之該交易包含：

對該第一類型之該交易之一第二引用；及

至少一個輸入，且

其中該第一引用係基於至該第二類型之該交易的該至少一個輸入中之至少一者，且該第二引用係基於至該第一類型之該交易的該至少一個輸入中之至少一者。

【0355】 25.一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一類型之一交易，其包含：

對一第二類型之一交易之一第一引用；及

至少一個輸入，

該第二類型之該交易包含：

對該第一類型之該交易之一第二引用；及

至少一個輸入，且

其中該第一引用包含該第二類型之該交易的一交易 id，且該第二引用係基於至該第一類型之該交易的該至少一個輸入中之至少一者。

【0356】 26.一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一類型之一交易，其包含：

對一第二類型之一交易之一第一引用；及

至少一個輸入，

該第二類型之該交易包含：

對一第一類型之該交易之一第二引用；及

至少一個輸入，且

其中該第一引用係基於至該第二類型之該交易的該至少一個輸入中之至少一者，且該第二引用包含該第一類型之該交易的一交易 id。

【0357】 27. 一種與一區塊鏈系統中之一組交易相關聯的電腦實施方法，該方法包含以下步驟：

接收一請求，該請求觸發待儲存在該區塊鏈上之一資料項目的一表示，

獲得該組交易中之一最新交易，

創建一新區塊鏈交易，該新區塊鏈交易包含：

與來自該最新交易之一輸出相關聯的一輸入；

一輸出；

待儲存在該區塊鏈上之該資料項目之該表示；及

對該最新交易之一引用，

將該交易提交至該區塊鏈。

【0358】 28.如條項 27 之電腦實施方法，其中對該最新交易之該引用為該最新交易之一不變特徵之一散列。

【0359】 29.如條項 28 之電腦實施方法，其中該最新交易包含一原像，且對該最新交易之該引用為該最新交易之該原像之一散列。

【0360】 30.如條項 27 至 29 中任一或多項之電腦實施方法，其中該新區塊鏈交易進一步包含對該組交易中之一初始交易之一引用。

【0361】 31. 如條項 30 之電腦實施方法，其中對該組交易中之該初始交易之該引用係基於該初始交易。

【0362】 32.如條項 30 或 31 之電腦實施方法，其中對該初始交易之該引用為該初始交易之一散列。

【0363】 33.如條項 27 至 32 中任一或多項之電腦實施方法，其進一步包含以下步驟：

創建一第二類型之一交易，

創建一第一類型之一交易，其包含與來自該組交易中之該最新交易的一交

易輸出相關聯之一輸入，

將該第二類型之該交易提交至該區塊鏈，及

將該第一類型之該交易提交至該區塊鏈。

【0364】 34.一種與一區塊鏈系統中之一組交易相關聯的電腦實施方法，該方法包含以下步驟：

創建一第二類型之一交易，

創建一第一類型之一交易，其包含與來自該組交易中之一最新交易的一輸出相關聯之至少一個輸入，

將該第二類型之該交易提交至該區塊鏈，及

將該第一類型之該交易提交至該區塊鏈。

【0365】 35.如條項 33 或 34 之電腦實施方法，其進一步包含以下步驟：

判定該組交易之一子集中的交易之一總數目，及

判定交易之該子集中的交易之該總數目係等於抑或大於一臨限值。

【0366】 36.如條項 35 之電腦實施方法，其中交易之該子集之成員係藉由是否已經在該區塊鏈上確認該交易來界定。

【0367】 37.如條項 35 或 36 之電腦實施方法，其中交易之該子集之成員係藉由與該組交易中之任何交易之一支出關係來界定。

【0368】 38.如條項 35 或 36 之電腦實施方法，其中交易之該子集之成員另外係藉由該臨限值界定。

【0369】 39.如條項 35 至 38 中任一或多項之電腦實施方法，其中交易之該子集包含一第一交易鏈。

【0370】 40.如條項 39 之電腦實施方法，其中交易之該子集為該第一交易鏈。

【0371】 41.如條項 39 或 40 之電腦實施方法，其中該第一交易鏈經建構，

使得除了該第一交易以外，該子集中之每一交易均包含對該鏈中之先前交易的一引用。

【0372】 42.如條項 41 之電腦實施方法，其中對該先前交易之該引用為與來自該先前交易之一交易輸出相關聯的一輸入。

【0373】 43. 如條項 40 至 42 中任一或多項之電腦實施方法，其中該組交易包含交易之多個子集。

【0374】 44. 如條項 43 之電腦實施方法，其中該組交易包含其他交易鏈。

【0375】 45.如條項 35 至 44 中任一或多項之電腦實施方法，其中該臨限值係基於一祖先限制。

【0376】 46.如條項 45 之電腦實施方法，其中該臨限值比該祖先限制小一。

【0377】 47.如條項 35 至 46 中任一或多項之電腦實施方法，其中創建並提交該第二類型之該交易及該第一類型之該交易的步驟係基於交易之該子集中的交易之該總數目與該臨限值之間的一比較來進行。

【0378】 48.如條項 47 之電腦實施方法，其中創建並提交該第二類型之該交易及該第一類型之該交易之步驟係基於交易之該子集中的交易之該總數目係等於抑或大於該臨限值來進行。

【0379】 49.如條項 33 至 48 中任一或多項之電腦實施方法，其中該第一類型之該交易包含對該第二類型之該交易之一第一引用。

【0380】 50 如條項 49 之電腦實施方法，其中該第一引用為一不變引用。

【0381】 51.如條項 50 之電腦實施方法，其中該第一引用係基於該第二類型之該交易的一不變特徵。

【0382】 52.如條項 49 至 51 中任一或多項之電腦實施方法，其中該第一引用包含該第二類型之該交易之一交易 id。

【0383】 53.如條項 33 至 52 中任一或多項之電腦實施方法，其中在提交該

第一類型之該交易之前在該區塊鏈上確認該第二類型之該交易。

【0384】 54.如條項 49 至 53 中任一或多項之電腦實施方法，其中該第二類型之該交易包含至少一個輸入，且該第一引用係基於該第二類型之該交易的該至少一個輸入中之至少一者。

【0385】 55. 如條項 33 至 54 中任一或多項之電腦實施方法，其中該第二類型之該交易包含對該組交易中之一交易之一第二引用。

【0386】 56.如條項 55 之電腦實施方法，其中該第二引用為對該組交易中之一初始交易之一引用。

【0387】 57.如條項 56 之電腦實施方法，其中對該初始交易之該引用包含該初始交易之一交易 id。

【0388】 58.如條項 55 至 57 中任一或多項之電腦實施方法，其中該第二引用為一不變引用。

【0389】 59.如條項 58 之電腦實施方法，其中該第二引用係基於該第一類型之該交易的一不變特徵。

【0390】 60.如條項 55 至 59 中任一或多項之電腦實施方法，其中該第二引用包含該第一類型之該交易之一交易 id。

【0391】 61.如條項 58 或 59 之電腦實施方法，該第二引用係基於該第一類型之該交易的該至少一個輸入中之至少一者。

【0392】 62.如條項 54 或 61 之電腦實施方法，其中基於該至少一個輸入中之至少一者之該引用採用一交易出點之形式。

【0393】 63.一種用於正向遍歷一組區塊鏈交易之電腦實施方法，其包含以下步驟：

(a)獲得該組交易中之一當前交易，

(b)判定該當前交易為一第一類型之一交易，且基於該判定，進行以下步驟

(i)、(ii)及(iii)：

i.基於該第一類型之該交易獲得對一第二類型之一交易之一引用；

ii.基於對該第二類型之該交易之該引用獲得該第二類型之該交易；及

iii.繼續至步驟(c)，其中將該第二類型之該交易作為該當前交易，

(c)獲得一當前交易識別符，

(d)獲得引用該當前交易識別符之另一交易，及

(e)自該另一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【0394】 64.如條項 63 之電腦實施方法，其中對該第二類型之該交易之該引用係儲存在該第一類型之該交易中，且該引用係藉由自該第一類型之該交易提取該引用而獲得。

【0395】 65.如條項 63 或 64 之電腦實施方法，其中若對該第二類型之該交易之該引用包含該第二類型之該交易之交易 id，則獲得該第二類型之該交易之步驟包含：

運用與該第二類型之該交易之該交易 id 相同之該交易 id 而在該區塊鏈中或在一區塊鏈網路節點內定位一交易。

【0396】 66. 如條項 63 或 64 之電腦實施方法，其中若對該第二類型之該交易之該引用包含至該第二類型之該交易之一組至少一個輸入，則獲得該第二類型之該交易之步驟包含：

運用如包含在對該第二類型之該交易之該引用中的輸入集合中之至少一個輸入而在一區塊鏈中或在一區塊鏈網路節點內定位一交易。

【0397】 67.如條項 63 至 66 中任一或多項之電腦實施方法，其進一步包含：

判定該當前交易並非一第二類型之該交易，且基於該判定，對與該當前交易相關聯之一資料酬載進行一操作，且繼續至步驟(c)。

【0398】 68.如條項 63 至 67 中任一或多項之電腦實施方法，其中基於該當前交易之內容將該當前交易判定為並非一第一類型之一交易。

【0399】 69.如條項 68 之電腦實施方法，基於該當前交易之一輸出之大小而將該當前交易判定為並非該第一類型之該交易。

【0400】 70.如條項 67 之電腦實施方法，其中對該資料酬載進行一操作包含：

儲存基於前一交易之一資料酬載之一散列，

自該當前交易提取對該前一交易之該資料酬載的一引用，及

證實基於該前一交易之該資料酬載之該散列及對該前一交易之該資料酬載之該引用係有效的。

【0401】 71.如條項 70 之電腦實施方法，其中對該前一交易之該引用為該前一交易之該酬載之另一散列。

【0402】 72.如條項 70 或 71 之電腦實施方法，其中認證步驟包含判定該前一交易之該資料酬載之該散列與對該前一交易之該資料酬載之該引用是否為相同的。

【0403】 73.如條項 63 至 72 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之前執行以下步驟：

獲得該組交易中之一初始交易，

證實該初始交易包含一種子值，

對該初始交易進行散列以獲得一初始交易識別符，

獲得引用該第一交易識別符之一第二交易，

證實該第二交易包含一種子值且其與該第一交易之該種子值相同，

對該第二交易進行散列以獲得一第二交易識別符，

獲得引用該第二交易識別符之一第三交易，及

移至步驟(b)，其中將該第三交易作為該當前交易。

【0404】 74.如條項 63 至 73 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之後執行以下步驟：

基於該當前交易是否為一最終交易而結束遍歷，其中判定該當前交易是否為一最終交易係基於包含於該當前交易中之資料。

【0405】 75.如條項 63 至 74 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之後執行以下步驟：

判定該當前交易為一第三類型之一交易，且基於該判定，進行以下步驟(i)、(ii)、(iii)及(iv)：

i.獲得包含對該前一交易之一引用之該輸入的一索引，

ii.獲得與包含對該前一交易之一引用的該輸入相關聯之該輸出，

iii.基於經獲得輸出獲得下一交易，及

iv.繼續至步驟(c)，其中將該下一交易作為該當前交易。

【0406】 76.一種用於反向遍歷一組區塊鏈交易之電腦實施方法，其包含以下步驟：

(a)獲得該組交易中之一當前交易，

(b)判定該當前交易為一第二類型之一交易，且基於該判定，進行以下步驟(i)、(ii)及(iii)：

i.基於該第二類型之該交易獲得對一第一類型之一交易之一引用；

ii.基於對該第一類型之該交易之該引用獲得該第一類型之該交易；及

iii.繼續至步驟(c)，其中將該第一類型之該交易作為該當前交易，

(c)自該當前交易獲得前一交易之一交易識別符，

(d)基於前一交易之該交易識別符獲得該前一交易，

(e)自該前一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創

建一循環。

【0407】77.如條項 76 之電腦實施方法，其中對該第一類型之該交易之該引用係儲存在該第二類型之該交易中，且該引用係藉由自該第二類型之該交易提取該引用而獲得。

【0408】78.如條項 76 或 77 之電腦實施方法，其中若對該第一類型之該交易之該引用包含該第一類型之該交易之該交易 id，則獲得該第一類型之該交易之步驟包含：

運用與該第一類型之該交易的該交易 id 相同的該交易 id 來在一區塊鏈中或在一區塊鏈節點內定位一交易。

【0409】79.如條項 76 或 77 之電腦實施方法，其中若對該第一類型之該交易之該引用包含至該第一類型之該交易之一組至少一個輸入，則獲得該第一類型之該交易之步驟包含：

運用如包含在對該第一類型之該交易之該引用中的輸入集合中之至少一個輸入在該區塊鏈中或在一區塊鏈網路節點內定位一交易。

【0410】80.如條項 76 至 79 中任一或多項之電腦實施方法，其進一步包含以下步驟：

判定該當前交易並非該第一類型之該交易，且基於該判定，對與該當前交易相關聯之一資料酬載進行一操作，且繼續至步驟(c)。

【0411】81.如條項 76 至 80 中任一或多項之電腦實施方法，其中接著基於該當前交易之內容將該當前交易判定為並非該第二類型之該交易。

【0412】82.如條項 81 之電腦實施方法，其中基於該當前交易是否包含一資料酬載而將該當前交易判定為並非一轉入交易，該資料酬載包含一原像。

【0413】83.如條項 76 至 82 中任一項之電腦實施方法，其中對該資料酬載進行一操作包含：

儲存基於前一交易之資料酬載之一散列，

自該當前交易提取對該前一交易之該資料酬載的一引用，及

證實基於該前一交易之該資料酬載之該散列及對該前一交易之該資料酬載之該引用係有效的。

【0414】 84.如條項 83 之電腦實施方法，其中對該前一交易之該引用為該前一交易之該酬載之另一散列。

【0415】 85.如條項 83 或 84 之電腦實施方法，其中認證步驟包含判定該前一交易之該資料酬載之該散列與對該前一交易之該資料酬載之該引用是否為相同的。

【0416】 86.如條項 76 至 85 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之前執行以下步驟：

獲得該組交易中之一最終交易，

自該最終交易獲得該組交易中之一初始交易之一交易 id，

對該最終交易進行散列以獲得一最終交易識別符，

獲得引用該最終交易識別符之一第二交易，及

移至步驟(b)，其中將該第二交易作為該當前交易。

【0417】 87.如條項 86 之電腦實施方法，其進一步包含在步驟(a)之後執行以下步驟：

基於該當前交易之該交易 id 是否等同於該初始交易 id 來結束遍歷。

【0418】 88. 如條項 76 至 87 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之後執行以下步驟：

基於該當前交易是否為一/該初始交易而結束該遍歷，其中判定該當前交易是否為該初始交易係基於包含於該當前交易之一資料酬載中之資料。

【0419】 89.如條項 76 至 88 中任一或多項之電腦實施方法，其進一步包含

在步驟(a)之後執行以下步驟：

判定該當前交易為一第三類型之一交易，且基於該判定，進行以下步驟(i)、(ii)、(iii)及(iv)：

i.獲得該當前交易之一輸入的一索引，

ii.基於該當前交易之經獲得輸入而獲得對該前一交易之一引用，

iii.基於該引用獲得該前一交易，及

iv.繼續至步驟(c)，其中將該前一交易作為該當前交易。

【0420】 90.一種用於正向遍歷一組區塊鏈交易之電腦實施方法，其包含以下步驟：

(a)獲得該組交易中之一當前交易，

(b) 判定該當前交易為一第三類型之一交易，且基於該判定，進行以下步驟(i)、(ii)、(iii)及(iv)：

i.獲得包含對該前一交易之一引用之輸入的一索引；

ii.獲得與包含對該前一交易之一引用的該輸入相關聯之輸出；

iii.基於經獲得輸出獲得下一交易；及

iv.繼續至步驟(c)，其中將該下一交易作為該當前交易，

(c)獲得一當前交易識別符，

(d)獲得引用該當前交易識別符之另一交易，及

(e)自該另一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【0421】 91.一種用於反向遍歷一組區塊鏈交易之電腦實施方法，其包含以下步驟：

(a)獲得該組交易中之一當前交易，

(b)判定該當前交易為一第三類型之一交易，且基於該判定，進行以下步驟

(i)、(ii)、(iii)、(iv)：

i.獲得該當前交易之一輸入的一索引；

ii.基於該當前交易之經獲得輸入而獲得對該前一交易之一引用；

iii.基於引用獲得該前一交易；及

iv.繼續至步驟(c)，其中將該前一交易作為該當前交易，

(c)自該當前交易獲得前一交易之一交易識別符，

(d)基於前一交易之該交易識別符獲得該前一交易，

(e)自該前一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【0422】92.一種計算裝置，其包含一處理器及記憶體，該記憶體包括可執行指令，該等可執行指令由於由該處理器執行而使得該裝置執行如條項 27 至 62 中任一或多項之電腦實施方法。

【0423】93.一種電腦系統，其包含：

一如條項 92 之資料寫入裝置，及

一計算裝置，其經組配以將包含資料之請求提交至該資料寫入裝置。

【0424】94.一種電腦可讀儲存媒體，其上儲存有可執行指令，該等可執行指令由於藉由一電腦之一處理器執行而使得該電腦執行如條項 27 至 62 中任一或多項之方法。

【0425】95.一種計算裝置，其包含一處理器及記憶體，該記憶體包括可執行指令，該等可執行指令由於由該處理器執行而使得該裝置執行如條項 63 至 75 中任一或多項之電腦實施方法。

【0426】96.一種電腦可讀儲存媒體，其上儲存有可執行指令，該等可執行指令由於藉由一電腦之一處理器執行而使得該電腦執行如條項 63 至 75 中任一或多項之方法。

【0427】 97.一種計算裝置，其包含一處理器及記憶體，該記憶體包括可執行指令，該等可執行指令由於由該處理器執行而使得該裝置執行如條項 76 至 91 中任一或多項之電腦實施方法。

【0428】 98.一種電腦可讀儲存媒體，其上儲存有可執行指令，該等可執行指令由於藉由一電腦之一處理器執行而使得該電腦執行如條項 76 至 91 中任一或多項之方法。

【0429】 如本說明書及申請專利範圍中所使用之術語「包含」意謂「至少部分地由……組成」。當解譯本說明書及申請專利範圍中之包括術語「包含」的每一語句時，亦可存在除前面有術語之彼或彼等特徵以外的特徵。諸如「包含(comprise)」及「包含(comprises)」之相關術語將以相同方式解釋。

【0430】 如本文中所使用，術語「及/或」意謂「及」或「或」或二者。如本文中所使用之名詞之後的「(多個)」意謂該名詞之複數及/或單數形式。元件之單數參考並不排除此類元件之複數參考，且反之亦然。

【0431】 應理解，上文描述意欲為說明性而非限定性的。熟習此項技術者在閱讀及理解上文描述後將明白許多其他實施。儘管本揭露內容已參考特定實例實施予以描述，但應認識到，本揭露內容不限於所描述之實施但可在係在隨附申請專利範圍之範疇內的修改及變更情況下實踐。因此，本說明書及圖式應在說明性意義上而非限制性意義上對待。因此，本揭露內容之範疇應參考隨附申請專利範圍以及此申請專利範圍所授權之等效物的完整範疇來判定。

【符號說明】

【0432】

100:系統

101:封包交換式網路

102:電腦終端

102a,102b:電腦設備

103,103a:使用者

103b:使用者或實體

104:區塊鏈節點

105,105a:用戶端應用程式

105b:用戶端

106:同級間(P2P)網路

150,1610:區塊鏈

151:資料區塊

151n:新區塊

151n-1:先前創建的區塊

152,152i,152j,602,604a,604b,604c,Tx,Tx':交易

153:起源區塊(Gb)

154:有序集合

155:區塊指標

160:側頻道

201:標頭

202:輸入

203:輸出

301:交易引擎

302:使用者介面(UI)層

350:UI

351,352:UI 元件

353 資訊元件

450:節點軟體

451:協定引擎

452:指令碼引擎

453:堆疊

454:應用程式層級決策引擎

455:與區塊鏈相關的功能模組

455C:共識模組

455P:傳播模組

455S:儲存模組

502:事件

504:區塊鏈交易

506:邊緣

600:交易鏈

606,606a,606b,606c,606d:支付關係

608:第二反向引用

610,612a,612b,612c:第三反向引用

640a,640b:資料附加交易

642a,642b:酬載

644a,644b,734:塵埃輸出

646a,646b,732:塵埃輸入

648a,648b,648c,648d:資金輸入

660:初始交易

662,726,1026,1126,1226,1426:最終交易

664,666:串流後設資料

680,800,900,1300:方法

700,714,716,1000,1100,1200,1400:資料結構

702:第一交易

718:正向引用

704a,704b,704c,704d,1004a,1004b,1004c,1004d,1104a,1104b,1104c,1104d,1204a,1204b,1204c,1204d,1404a,1404b,1404c,1404d:附加交易

706a,706b,706c,706d,706e,706f:引用

720,722:塵埃鏈

724,1024:鏈引用

730b:交易 id

682,684,686,688,802,804,806,808,810,812,814,816,818,820,822,824,902,904,906,908,910,912,914,916,918,920,922,924,926,928,1302,1304,1306,1308,1310,1312,1314,1316,1318,1320,1322,1324,1326:步驟

1006a,1006b,1006c,1006d,1006e,1006f,1106a,1106b,1106c,1106d,1106e,1106f,1206a,1206b,1206c,1206d,1206e,1206f,1406a,1406b,1406c,1406d,1406e,1406f:反向支出引用

1014,1116,1216,1416:轉入交易

1016:不可變轉入交易

1018:不變且不可變引用

1050,1052:區塊

1114,1214,1414:轉出交易

1118:不變引用

1218,1418:不變正向引用

1224:反向引用

1300:電腦實施方法

1424:不變反向引用

1500:平台處理器

1502,1602:資料服務

1504,1606:計算服務

1506,1604:商務服務

1508:API

1510:基礎軟體

1512:區塊鏈網路

1600:平台

1602a:資料寫入器服務

1602b,302b:資料讀取器服務

1604a:企業電子錢包

1606a:應用程式

1606b:框架

1608:SPV 服務

1800:資料佈局

1802:交會交易

2600:計算裝置

2602:處理器

2604:匯流排子系統

2606:儲存子系統

2608:主記憶體

2610:持久性儲存器

2612:使用者介面輸入裝置

2614:使用者介面輸出裝置

2616:網路介面子系統

2618:動態隨機存取記憶體(DRAM)

2620:唯讀記憶體(ROM)

L:鏈

【發明申請專利範圍】

【請求項1】 一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一類型之一交易，其包含一輸出，該輸出包含對一第二類型之一交易之一第一引用，及

該第二類型之該交易。

【請求項2】 如請求項 1 之電腦實施資料結構，其中該第一引用為一不變引用。

【請求項3】 如請求項 2 之電腦實施資料結構，其中該第一引用係基於該第二類型之該交易的一不變特徵。

【請求項4】 如請求項 1 至 3 中任一或多項之電腦實施資料結構，其中該第一引用包含該第二類型之該交易之交易 id。

【請求項5】 如請求項 1 至 4 中任一或多項之電腦實施資料結構，其中該第二類型之該交易包含至少一個輸入，且該第一引用係基於至該第二類型之該交易的該至少一個輸入中之至少一者。

【請求項6】 如請求項 1 至 5 中任一或多項之電腦實施資料結構，其中該第二類型之該交易包含一第二引用。

【請求項7】 如請求項 6 之電腦實施資料結構，其中該第二引用儲存於該第二類型之該交易的一輸出中。

【請求項8】 如請求項 6 或 7 之電腦實施資料結構，其中該第二引用包含該第一類型之該交易之一交易 id。

【請求項9】 如請求項 6 至 8 中任一或多項之電腦實施資料結構，其中該第二引用為一不變引用。

【請求項10】如請求項 9 之電腦實施資料結構，其中該第二引用係基於該第一類型之該交易的一不變特徵。

【請求項11】如請求項 6、7、9 或 10 中任一或多項之電腦實施資料結構，其中該第一類型之該交易包含至少一個輸入，且該第二引用係基於該第一類型之該交易的該至少一個輸入中之至少一者。

【請求項12】如請求項 5 或 11 之電腦實施資料結構，其中包含該至少一個輸入之該引用採用一交易出點之形式。

【請求項13】一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一類型之一交易，其包含：

對一第二類型之一交易之一第一引用；及

至少一個輸入，

該第二類型之該交易包含：

對該第一類型之該交易之一第二引用；及

至少一個輸入，且

其中該第一引用係基於至該第二類型之該交易的該至少一個輸入中之至少一者，且該第二引用係基於至該第一類型之該交易的該至少一個輸入中之至少一者。

【請求項14】一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一類型之一交易，其包含：

對一第二類型之一交易之一第一引用；及

至少一個輸入，

該第二類型之該交易包含：

對該第一類型之該交易之一第二引用；及

至少一個輸入，且

其中該第一引用包含該第二類型之該交易的一交易 id，且該第二引用係基於至該第一類型之該交易的該至少一個輸入中之至少一者。

【請求項15】一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一類型之一交易，其包含：

對一第二類型之一交易之一第一引用；及

至少一個輸入，

該第二類型之該交易包含：

對該第一類型之該交易之一第二引用；及

至少一個輸入，且

其中該第一引用係基於至該第二類型之該交易的該至少一個輸入中之至少一者，且該第二引用包含該第一類型之該交易的一交易 id。

【請求項16】如請求項 1 至 15 之電腦實施資料結構，其包含：

一第一交易，其包含：

一第一輸出；及

一第一資料項目之一表示，

一第二交易，其包含：

該第一資料項目之另一表示；

一第二資料項目之一表示；

與該第一輸出相關聯的一第一輸入；及

一第二輸出。

【請求項17】一種與一區塊鏈相關聯之電腦實施資料結構，其包含：

一第一交易，其包含：

一第一輸出；及

一第一資料項目之一表示，

一第二交易，其包含：

該第一資料項目之另一表示；

一第二資料項目之一表示；

與該第一輸出相關聯的一第一輸入；及

一第二輸出。

【請求項18】如請求項 16 或 17 之電腦實施資料結構，其中該第一資料項目為後設資料及一種子。

【請求項19】如請求項 18 之電腦實施資料結構，其中該第一項目之該表示包含該後設資料，該後設資料包含該種子。

【請求項20】如請求項 18 或 19 之電腦實施資料結構，其中該第一項目之該另一表示包含該種子。

【請求項21】如請求項 16 或 17 之電腦實施資料結構，其中該第一資料項目之該第一表示包含該資料項目之一散列。

【請求項22】如請求項 16 或 17 之電腦實施資料結構，其中該第一資料項目之該第一表示包含該資料項目。

【請求項23】如請求項 21 或 22 之電腦實施資料結構，其中該第一交易包含一原像，該原像包含該第一資料項目之該第一表示。

【請求項24】如請求項 23 之電腦實施資料結構，其中第一資料結構之該另一表示包含該第一交易之該原像之一散列。

【請求項25】如請求項 16 至 24 中任一或多項之電腦實施資料結構，其中該第二交易進一步包含對該第一交易之一引用。

【請求項26】如請求項 17 至 25 中任一或多項之電腦實施資料結構，其進一步包含：

一第一類型之一交易，其包含一輸出，該輸出包含對一第二類型之一交易之一第一引用，及

該第二類型之該交易。

【請求項27】一種與一區塊鏈系統中之一組交易相關聯的電腦實施方法，該方法包含以下步驟：

接收一請求，該請求觸發待儲存在該區塊鏈上之一資料項目的一表示，

獲得該組交易中之一最新交易，

創建一新區塊鏈交易，該新區塊鏈交易包含：

與來自該最新交易之一輸出相關聯的一輸入；

一輸出；

待儲存在該區塊鏈上之該資料項目之該表示；及

對該最新交易之一引用，

將該交易提交至該區塊鏈。

【請求項28】如請求項 27 之電腦實施方法，其中對該最新交易之該引用為該最新交易之一不變特徵之一散列。

【請求項29】如請求項 28 之電腦實施方法，其中該最新交易包含一原像，且對該最新交易之該引用為該最新交易之該原像之一散列。

【請求項30】如請求項 27 至 29 中任一或多項之電腦實施方法，其中該新區塊鏈交易進一步包含對該組交易中之一初始交易之一引用。

【請求項31】如請求項 30 之電腦實施方法，其中對該組交易中之該初始交易之該引用係基於該初始交易。

【請求項32】如請求項 30 或 31 之電腦實施方法，其中對該初始交易之該引用為該初始交易之一散列。

【請求項33】如請求項 27 至 32 中任一或多項之電腦實施方法，其進一步包含以下步驟：

創建一第二類型之一交易，

創建一第一類型之一交易，其包含與來自該組交易中之該最新交易的一交

易輸出相關聯之一輸入，

將該第二類型之該交易提交至該區塊鏈，及

將該第一類型之該交易提交至該區塊鏈。

【請求項34】一種與一區塊鏈系統中之一組交易相關聯的電腦實施方法，該方法包含以下步驟：

創建一第二類型之一交易，

創建一第一類型之一交易，其包含與來自該組交易中之一最新交易的一輸出相關聯之至少一個輸入，

將該第二類型之該交易提交至該區塊鏈，及

將該第一類型之該交易提交至該區塊鏈。

【請求項35】如請求項 33 或 34 之電腦實施方法，其進一步包含以下步驟：

判定該組交易之一子集中的交易之一總數目，及

判定交易之該子集中的交易之該總數目係等於抑或大於一臨限值。

【請求項36】如請求項 35 之電腦實施方法，其中交易之該子集之成員係藉由是否已經在該區塊鏈上確認該交易來界定。

【請求項37】如請求項 35 或 36 之電腦實施方法，其中交易之該子集之成員係藉由與該組交易中之任何交易之一支出關係來界定。

【請求項38】如請求項 35 或 36 之電腦實施方法，其中交易之該子集之成員另外係藉由該臨限值界定。

【請求項39】如請求項 35 至 38 中任一或多項之電腦實施方法，其中交易之該子集包含一第一交易鏈。

【請求項40】如請求項 39 之電腦實施方法，其中交易之該子集為該第一交易鏈。

【請求項41】如請求項 39 或 40 之電腦實施方法，其中該第一交易鏈經建

構，使得除了該第一交易以外，該子集中之每一交易均包含對該鏈中之先前交易的一引用。

【請求項42】如請求項 41 之電腦實施方法，其中對該先前交易之該引用為與來自該先前交易之一交易輸出相關聯的一輸入。

【請求項43】如請求項 40 至 42 中任一或多項之電腦實施方法，其中該組交易包含交易之多個子集。

【請求項44】如請求項 43 之電腦實施方法，其中該組交易包含其他交易鏈。

【請求項45】如請求項 35 至 44 中任一或多項之電腦實施方法，其中該臨限值係基於一祖先限制。

【請求項46】如請求項 45 之電腦實施方法，其中該臨限值比該祖先限制小一。

【請求項47】如請求項 35 至 46 中任一或多項之電腦實施方法，其中創建並提交該第二類型之該交易及該第一類型之該交易的步驟係基於交易之該子集中的交易之該總數目與該臨限值之間的一比較來進行。

【請求項48】如請求項 47 之電腦實施方法，其中創建並提交該第二類型之該交易及該第一類型之該交易之步驟係基於交易之該子集中的交易之該總數目係等於抑或大於該臨限值來進行。

【請求項49】如請求項 33 至 48 中任一或多項之電腦實施方法，其中該第一類型之該交易包含對該第二類型之該交易之一第一引用。

【請求項50】如請求項 49 之電腦實施方法，其中該第一引用為一不變引用。

【請求項51】如請求項 50 之電腦實施方法，其中該第一引用係基於該第二類型之該交易的一不變特徵。

【請求項52】如請求項 49 至 51 中任一或多項之電腦實施方法，其中該第一引用包含該第二類型之該交易之一交易 id。

【請求項53】如請求項 33 至 52 中任一或多項之電腦實施方法，其中在提交該第一類型之該交易之前在該區塊鏈上確認該第二類型之該交易。

【請求項54】如請求項 49 至 53 中任一或多項之電腦實施方法，其中該第二類型之該交易包含至少一個輸入，且該第一引用係基於該第二類型之該交易的該至少一個輸入中之至少一者。

【請求項55】如請求項 33 至 54 中任一或多項之電腦實施方法，其中該第二類型之該交易包含對該組交易中之一交易之一第二引用。

【請求項56】如請求項 55 之電腦實施方法，其中該第二引用為對該組交易中之一初始交易之一引用。

【請求項57】如請求項 56 之電腦實施方法，其中對該初始交易之該引用包含該初始交易之一交易 id。

【請求項58】如請求項 55 至 57 中任一或多項之電腦實施方法，其中該第二引用為一不變引用。

【請求項59】如請求項 58 之電腦實施方法，其中該第二引用係基於該第一類型之該交易的一不變特徵。

【請求項60】如請求項 55 至 59 中任一或多項之電腦實施方法，其中該第二引用包含該第一類型之該交易之一交易 id。

【請求項61】如請求項 58 或 59 之電腦實施方法，該第二引用係基於該第一類型之該交易的該至少一個輸入中之至少一者。

【請求項62】如請求項 54 或 61 之電腦實施方法，其中基於該至少一個輸入中之至少一者之該引用採用一交易出點之形式。

【請求項63】一種用於正向遍歷一組區塊鏈交易之電腦實施方法，其包含以下步驟：

(a)獲得該組交易中之一當前交易，

(b)判定該當前交易為一第一類型之一交易，且基於該判定，進行以下步驟(i)、(ii)及(iii)：

i.基於該第一類型之該交易獲得對一第二類型之一交易之一引用；

ii.基於對該第二類型之該交易之該引用獲得該第二類型之該交易；及

iii.繼續至步驟(c)，其中將該第二類型之該交易作為該當前交易，

(c)獲得一當前交易識別符，

(d)獲得引用該當前交易識別符之另一交易，及

(e)自該另一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【請求項64】如請求項 63 之電腦實施方法，其中對該第二類型之該交易之該引用係儲存在該第一類型之該交易中，且該引用係藉由自該第一類型之該交易提取該引用而獲得。

【請求項65】如請求項 63 或 64 之電腦實施方法，其中若對該第二類型之該交易之該引用包含該第二類型之該交易之交易 id，則獲得該第二類型之該交易之該步驟包含：

運用與該第二類型之該交易之該交易 id 相同之該交易 id 而在該區塊鏈中或在一區塊鏈網路節點內定位一交易。

【請求項66】如請求項 63 或 64 之電腦實施方法，其中若對該第二類型之該交易之該引用包含至該第二類型之該交易之一組至少一個輸入，則獲得該第二類型之該交易之該步驟包含：

運用如包含在對該第二類型之該交易之該引用中的輸入集合中之至少一個輸入而在一區塊鏈中或在一區塊鏈網路節點內定位一交易。

【請求項67】如請求項 63 至 66 中任一或多項之電腦實施方法，其進一步包含：

判定該當前交易並非一第二類型之該交易，且基於該判定，對與該當前交易相關聯之一資料酬載進行一操作，且繼續至步驟(c)。

【請求項68】如請求項 63 至 67 中任一或多項之電腦實施方法，其中基於該當前交易之內容將該當前交易判定為並非一第一類型之一交易。

【請求項69】如請求項 68 之電腦實施方法，基於該當前交易之一輸出之大小而將該當前交易判定為並非該第一類型之該交易。

【請求項70】如請求項 67 之電腦實施方法，其中對該資料酬載進行一操作包含：

儲存基於前一交易之一資料酬載之一散列，

自該當前交易提取對該前一交易之該資料酬載的一引用，及

證實基於該前一交易之該資料酬載之該散列及對該前一交易之該資料酬載之該引用係有效的。

【請求項71】如請求項 70 之電腦實施方法，其中對該前一交易之該引用為該前一交易之該酬載之另一散列。

【請求項72】如請求項 70 或 71 之電腦實施方法，其中該認證步驟包含判定該前一交易之該資料酬載之該散列與對該前一交易之該資料酬載之該引用是否為相同的。

【請求項73】如請求項 63 至 72 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之前執行以下步驟：

獲得該組交易中之一初始交易，

證實該初始交易包含一種子值，

對該初始交易進行散列以獲得一初始交易識別符，

獲得引用該第一交易識別符之一第二交易，

證實該第二交易包含一種子值且其與該第一交易之該種子值相同，

對該第二交易進行散列以獲得一第二交易識別符，

獲得引用該第二交易識別符之一第三交易，及

移至步驟(b)，其中將該第三交易作為該當前交易。

【請求項74】如請求項 63 至 73 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之後執行以下步驟：

基於該當前交易是否為一最終交易而結束遍歷，其中判定該當前交易是否為一最終交易係基於包含於該當前交易中之資料。

【請求項75】如請求項 63 至 74 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之後執行以下步驟：

判定該當前交易為一第三類型之一交易，且基於該判定，進行以下步驟(i)、(ii)、(iii)及(iv)：

i.獲得包含對該前一交易之一引用之該輸入的一索引，

ii.獲得與包含對該前一交易之一引用的該輸入相關聯之該輸出，

iii.基於經獲得輸出獲得下一交易，及

iv.繼續至步驟(c)，其中將該下一交易作為該當前交易。

【請求項76】一種用於反向遍歷一組區塊鏈交易之電腦實施方法，其包含以下步驟：

(a)獲得該組交易中之一當前交易，

(b)判定該當前交易為一第二類型之一交易，且基於該判定，進行以下步驟(i)、(ii)及(iii)：

i.基於該第二類型之該交易獲得對一第一類型之一交易之一引用；

ii.基於對該第一類型之該交易之該引用獲得該第一類型之該交易；及

iii.繼續至步驟(c)，其中將該第一類型之該交易作為該當前交易，

(c)自該當前交易獲得前一交易之一交易識別符，

(d)基於前一交易之該交易識別符獲得該前一交易，

(e)自該前一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【請求項77】如請求項 76 之電腦實施方法，其中對該第一類型之該交易之該引用係儲存在該第二類型之該交易中，且該引用係藉由自該第二類型之該交易提取該引用而獲得。

【請求項78】如請求項 76 或 77 之電腦實施方法，其中若對該第一類型之該交易之該引用包含該第一類型之該交易之該交易 id，則獲得該第一類型之該交易之該步驟包含：

運用與該第一類型之該交易的該交易 id 相同的該交易 id 來在一區塊鏈中或在一區塊鏈節點內定位一交易。

【請求項79】如請求項 76 或 77 之電腦實施方法，其中若對該第一類型之該交易之該引用包含至該第一類型之該交易之一組至少一個輸入，則獲得該第一類型之該交易之該步驟包含：

運用如包含在對該第一類型之該交易之該引用中的輸入集合中之至少一個輸入在該區塊鏈中或在一區塊鏈節點內定位一交易。

【請求項80】如請求項 76 至 79 中任一或多項之電腦實施方法，其進一步包含以下步驟：

判定該當前交易並非該第一類型之該交易，且基於該判定，對與該當前交易相關聯之一資料酬載進行一操作，且繼續至步驟(c)。

【請求項81】如請求項 76 至 80 中任一或多項之電腦實施方法，其中接著基於該當前交易之內容將該當前交易判定為並非該第二類型之該交易。

【請求項82】如請求項 81 之電腦實施方法，其中基於該當前交易是否包含一資料酬載而將該當前交易判定為並非一轉入交易，該資料酬載包含一原像。

【請求項83】如請求項 76 至 82 中任一項之電腦實施方法，其中對該資料酬載進行一操作包含：

儲存基於前一交易之資料酬載之一散列，

自該當前交易提取對該前一交易之該資料酬載的一引用，及

證實基於該前一交易之該資料酬載之該散列及對該前一交易之該資料酬載之該引用係有效的。

【請求項84】如請求項 83 之電腦實施方法，其中對該前一交易之該引用為該前一交易之該酬載之另一散列。

【請求項85】如請求項 83 或 84 之電腦實施方法，其中該認證步驟包含判定該前一交易之該資料酬載之該散列與對該前一交易之該資料酬載之該引用是否為相同的。

【請求項86】如請求項 76 至 85 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之前要執行的以下步驟：

獲得該組交易中之一最終交易，

自該最終交易獲得該組交易中之一初始交易之一交易 id，

對該最終交易進行散列以獲得一最終交易識別符，

獲得引用該最終交易識別符之一第二交易，及

移至步驟(b)，其中將該第二交易作為該當前交易。

【請求項87】如請求項 86 之電腦實施方法，其進一步包含在步驟(a)之後要執行的以下步驟：

基於該當前交易之該交易 id 是否等同於該初始交易 id 來結束遍歷。

【請求項88】如請求項 76 至 87 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之後要執行的以下步驟：

基於該當前交易是否為一/該初始交易而結束該遍歷，其中判定該當前交易

是否為該初始交易係基於包含於該當前交易之一資料酬載中之資料。

【請求項89】如請求項 76 至 88 中任一或多項之電腦實施方法，其進一步包含在步驟(a)之後要執行的以下步驟：

判定該當前交易為一第三類型之一交易，且基於該判定，進行以下步驟(i)、(ii)、(iii)及(iv)：

i.獲得該當前交易之一輸入的一索引，

ii.基於該當前交易之經獲得輸入而獲得對該前一交易之一引用，

iii.基於該引用獲得該前一交易，及

iv.繼續至步驟(c)，其中將該前一交易作為該當前交易。

【請求項90】一種用於正向遍歷一組區塊鏈交易之電腦實施方法，其包含以下步驟：

(a)獲得該組交易中之一當前交易，

(b)判定該當前交易為一第三類型之一交易，且基於該判定，進行以下步驟(i)、(ii)、(iii)及(iv)：

i.獲得包含對該前一交易之一引用之輸入的一索引；

ii.獲得與包含對該前一交易之一引用的該輸入相關聯之輸出，

iii.基於經獲得輸出獲得下一交易；及

iv.繼續至步驟(c)，其中將該下一交易作為該當前交易，

(c)獲得一當前交易識別符，

(d)獲得引用該當前交易識別符之另一交易，及

(e)自該另一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【請求項91】一種用於反向遍歷一組區塊鏈交易之電腦實施方法，其包含以下步驟：

(a)獲得該組交易中之一當前交易，

(b) 判定該當前交易為一第三類型之一交易，且基於該判定，進行以下步驟(i)、(ii)、(iii)、(iv)：

i.獲得該當前交易之一輸入的一索引；

ii.基於該當前交易之經獲得輸入而獲得對前一交易之一引用；

iii.基於引用獲得該前一交易；及

iv.繼續至步驟(c)，其中將該前一交易作為該當前交易，

(c)自該當前交易獲得該前一交易之一交易識別符，

(d)基於前一交易之該交易識別符獲得該前一交易，

(e)自該前一交易作為該當前交易開始，進行步驟(b)、(c)、(d)及(e)，藉此創建一循環。

【請求項92】一種計算裝置，其包含一處理器及記憶體，該記憶體包括可執行指令，該等可執行指令由於由該處理器執行而使得該裝置執行如請求項 27 至 62 中任一或多項之電腦實施方法。

【請求項93】一種電腦系統，其包含：

一如請求項 92 之資料寫入裝置，及

一計算裝置，其經組配以將包含資料之請求提交至該資料寫入裝置。

【請求項94】一種電腦可讀儲存媒體，其上儲存有可執行指令，該等可執行指令由於藉由一電腦之一處理器執行而使得該電腦執行如請求項 27 至 62 中任一或多項之方法。

【請求項95】一種計算裝置，其包含一處理器及記憶體，該記憶體包括可執行指令，該等可執行指令由於由該處理器執行而使得該裝置執行如請求項 63 至 75 中任一或多項之電腦實施方法。

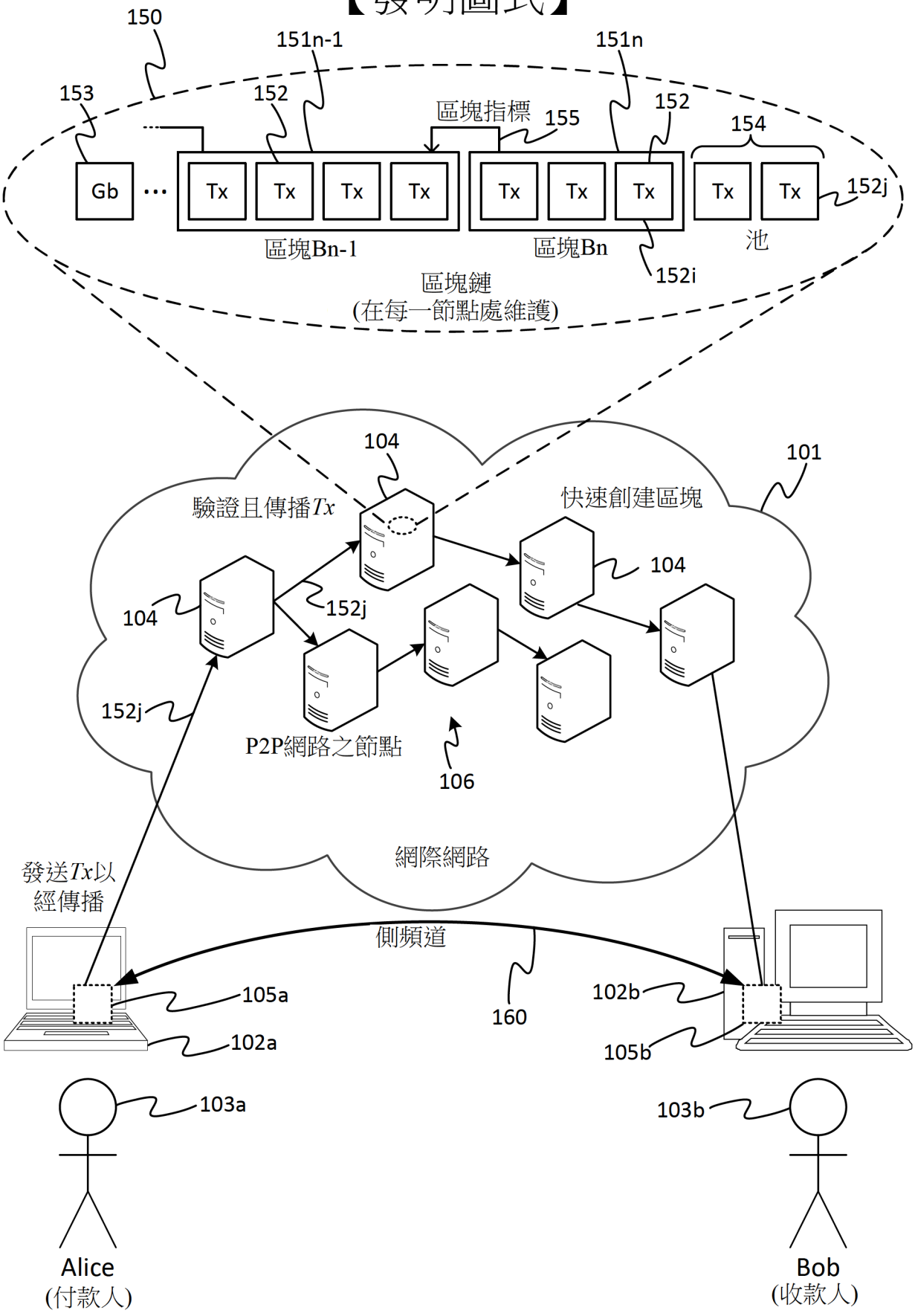
【請求項96】一種電腦可讀儲存媒體，其上儲存有可執行指令，該等可執行

指令由於藉由一電腦之一處理器執行而使得該電腦執行如請求項 63 至 75 中任一或多項之方法。

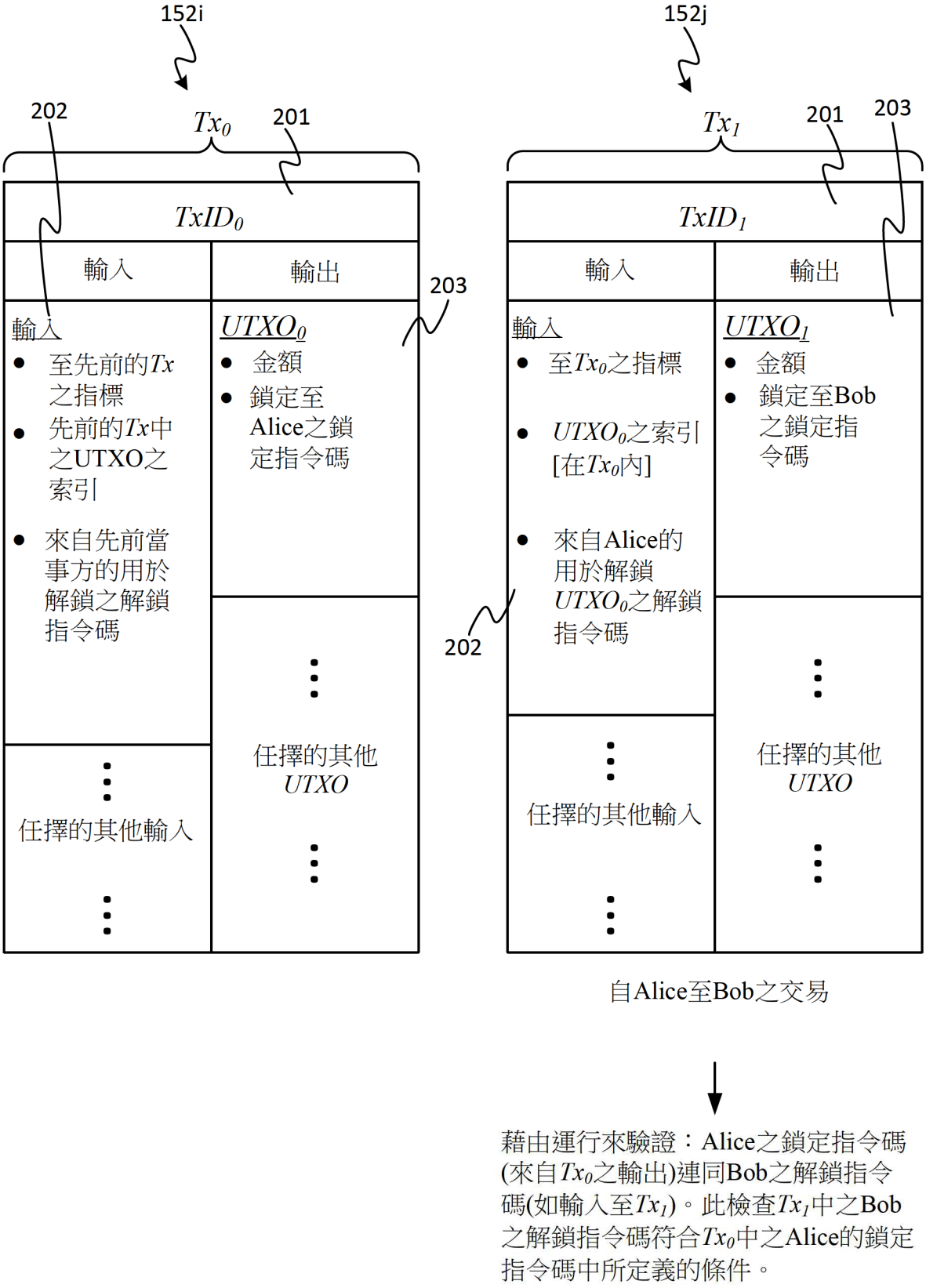
【請求項97】一種計算裝置，其包含一處理器及記憶體，該記憶體包括可執行指令，該等可執行指令由於由該處理器執行而使得該裝置執行如請求項 76 至 91 中任一或多項之電腦實施方法。

【請求項98】一種電腦可讀儲存媒體，其上儲存有可執行指令，該等可執行指令由於藉由一電腦之一處理器執行而使得該電腦執行如請求項 76 至 91 中任一或多項之方法。

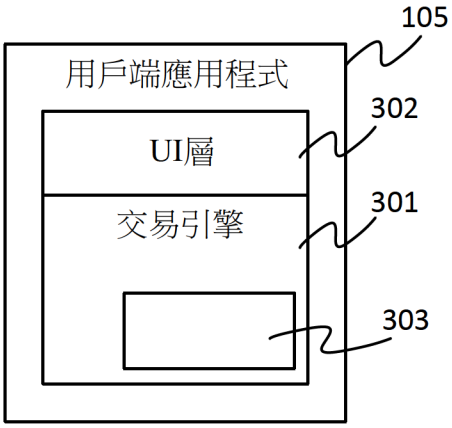
【發明圖式】


150
151n-1
151n
153
152
區塊指標
155
152
154
Gb
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
152j
區塊Bn-1
區塊Bn
池
152i
區塊鏈
(在每一節點處維護)
104
101
驗證且傳播Tx
快速創建區塊
104
104
152j
152j
P2P網路之節點
106
網際網路
發送Tx以
經傳播
側頻道
160
105a
102a
102b
105b
103a
103b
Alice
(付款人)
Bob
(收款人)

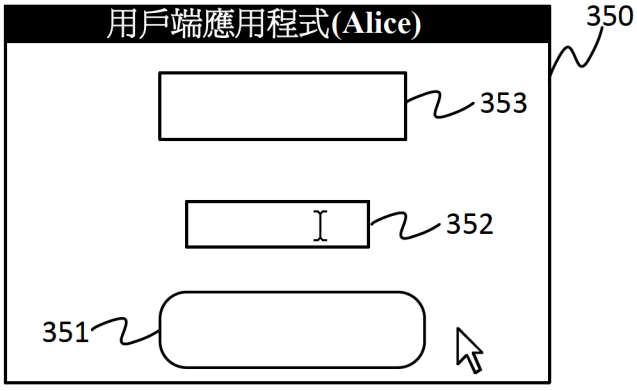
【圖1】


152i
202
Tx_0
201
$TxID_0$
輸入
輸出
203
輸入
• 至先前的*Tx*之指標
• 先前的*Tx*中之UTXO之索引
• 來自先前當事方的用於解鎖之解鎖指令碼
$UTXO_0$
• 金額
• 鎖定至Alice之鎖定指令碼
任擇的其他輸入
任擇的其他*UTXO*
152j
Tx_1
201
203
$TxID_1$
輸入
輸出
輸入
• 至Tx_0之指標
• $UTXO_0$之索引[在Tx_0內]
• 來自Alice的用於解鎖$UTXO_0$之解鎖指令碼
202
$UTXO_1$
• 金額
• 鎖定至Bob之鎖定指令碼
任擇的其他輸入
任擇的其他*UTXO*
自Alice至Bob之交易
藉由運行來驗證：Alice之鎖定指令碼(來自Tx_0之輸出)連同Bob之解鎖指令碼(如輸入至Tx_1)。此檢查Tx_1中之Bob之解鎖指令碼符合Tx_0中之Alice的鎖定指令碼中所定義的條件。

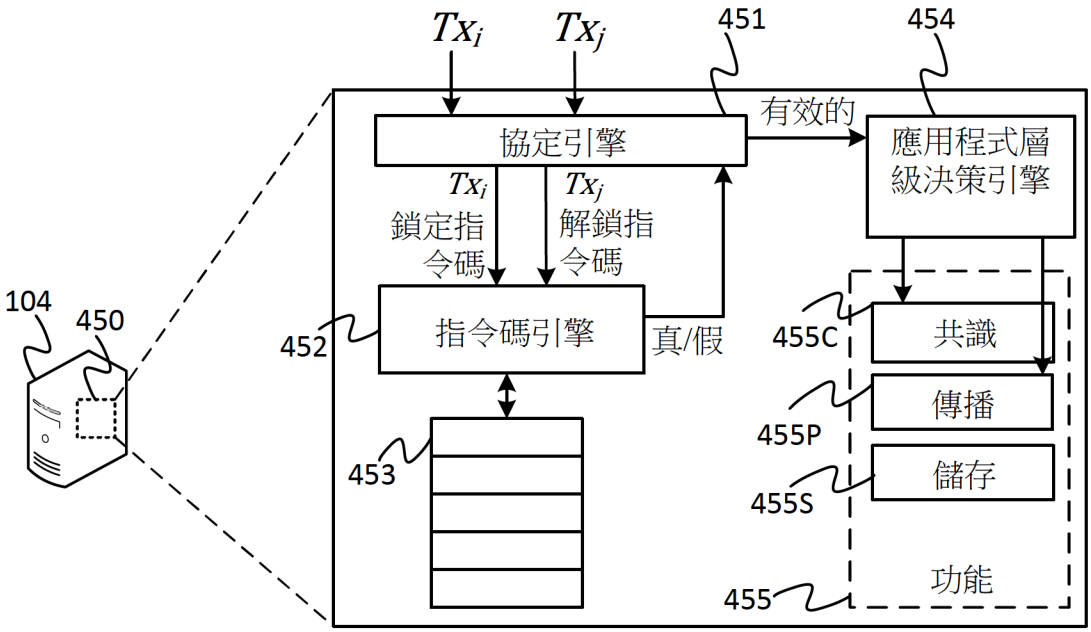
【圖2】


105
用戶端應用程式
302
UI層
301
交易引擎
303

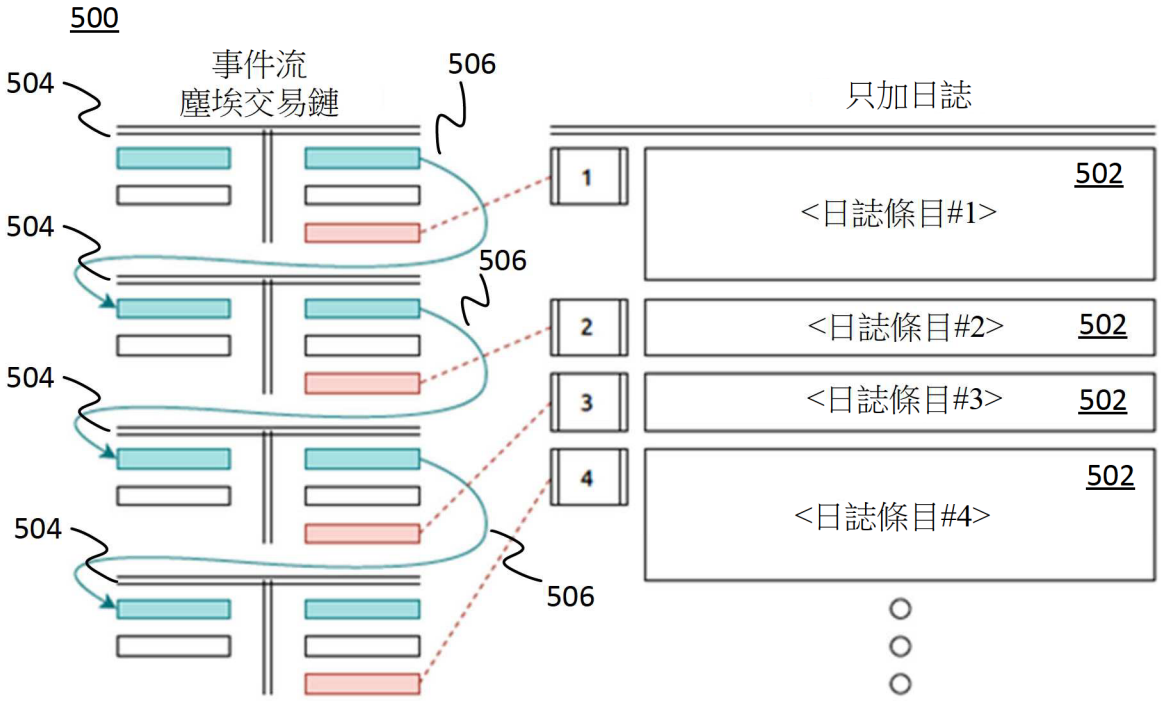
【圖3A】


用戶端應用程式(Alice)
350
353
352
351

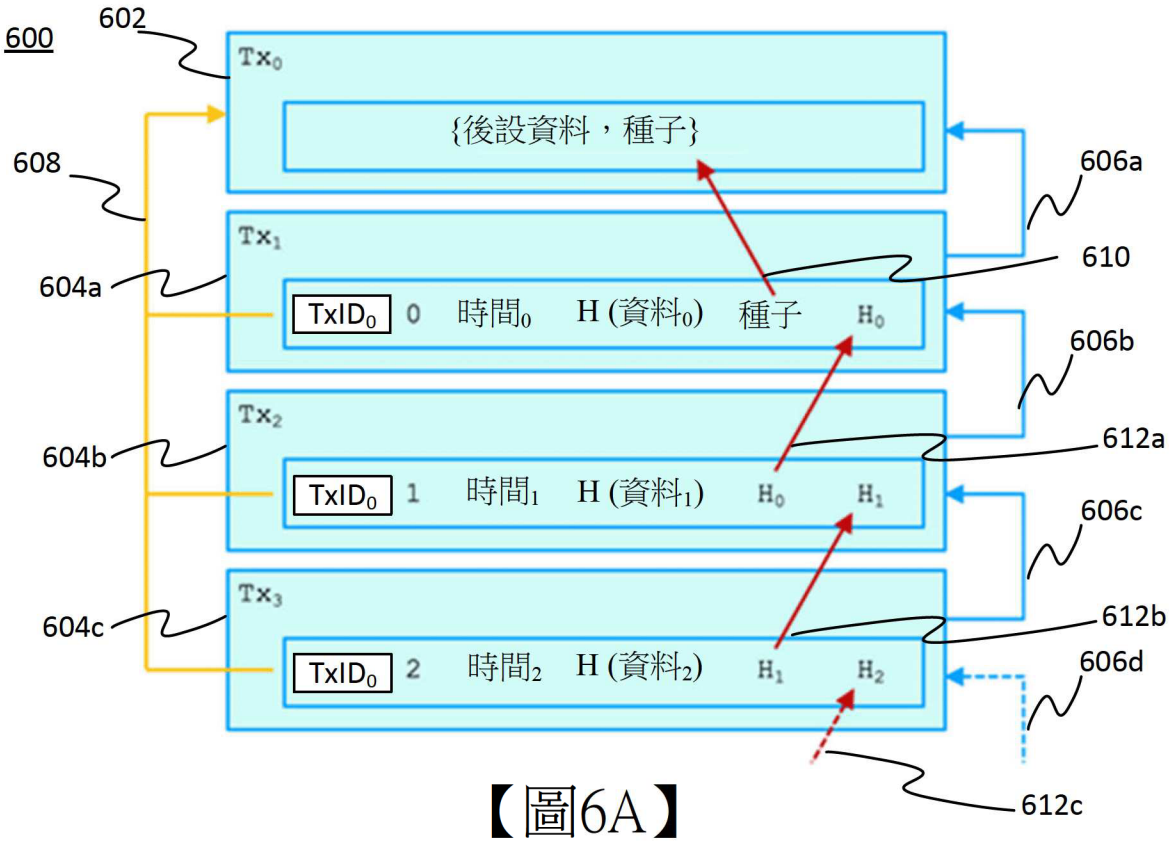
【圖3B】


Tx_i
Tx_j
451
454
協定引擎
有效的
應用程式層
級決策引擎
Tx_i
鎖定指
令碼
Tx_j
解鎖指
令碼
104
450
452
指令碼引擎
真/假
455C
共識
傳播
455P
儲存
455S
453
功能
455

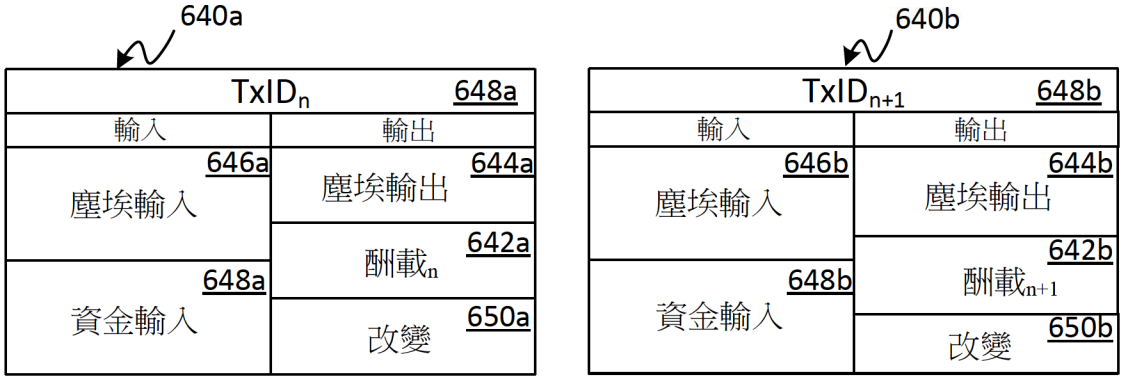
【圖4】


500
事件流
塵埃交易鏈
504
506
只加日誌
1
502
<日誌條目#1>
2
<日誌條目#2>
3
<日誌條目#3>
4
<日誌條目#4>

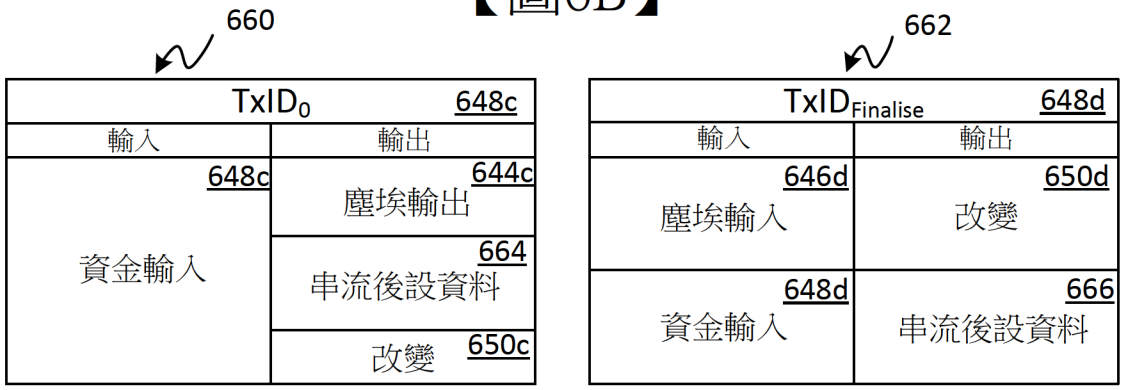
【圖5】


600
602
Tx0
{後設資料，種子}
608
606a
Tx1
610
604a
TxID0 0 時間0 H (資料0) 種子 H0
606b
Tx2
612a
604b
TxID0 1 時間1 H (資料1) H0 H1
606c
Tx3
612b
604c
TxID0 2 時間2 H (資料2) H1 H2
606d
612c

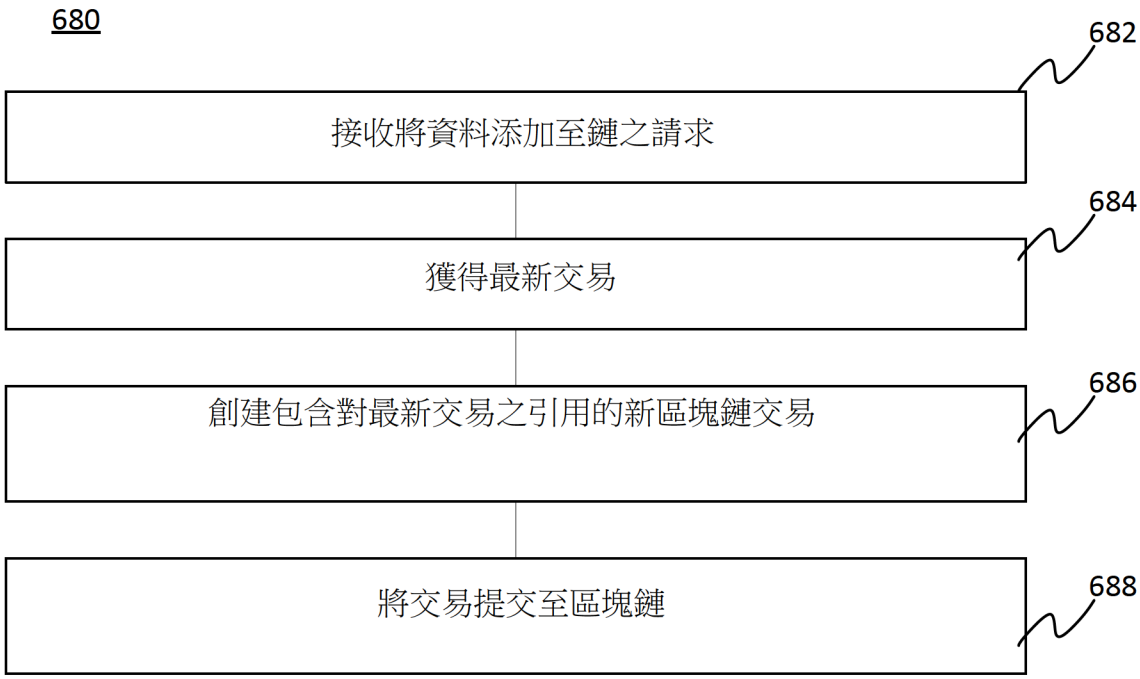
【圖6A】


640a
TxIDn 648a
輸入
輸出
646a
塵埃輸入
塵埃輸出 644a
酬載n 642a
648a
資金輸入
改變 650a
640b
TxIDn+1 648b
輸入
輸出
646b
塵埃輸入
塵埃輸出 644b
酬載n+1 642b
648b
資金輸入
改變 650b

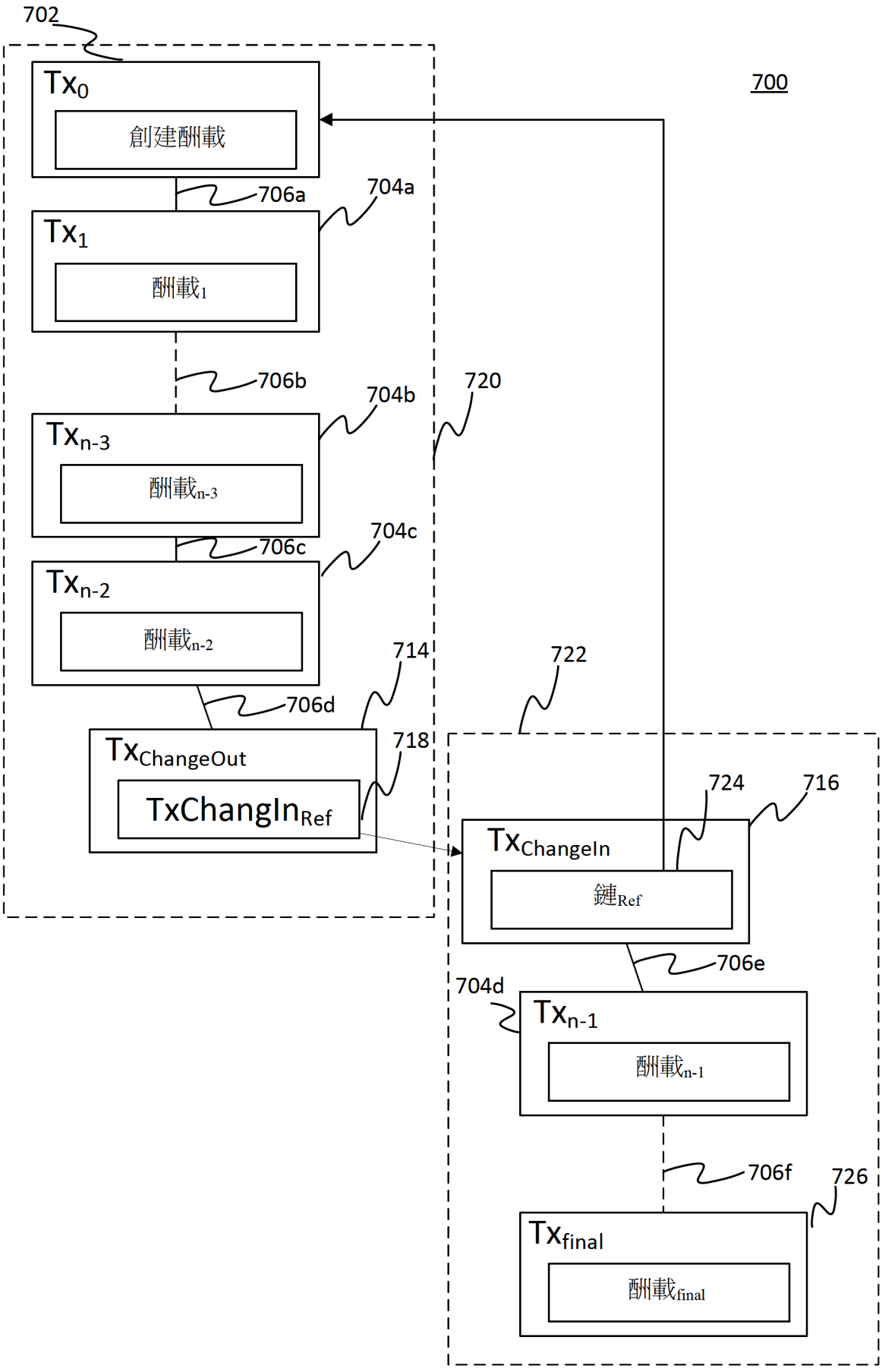
【圖6B】


660
TxID0 648c
輸入
輸出
648c
資金輸入
塵埃輸出 644c
串流後設資料 664
改變 650c
662
TxIDFinalise 648d
輸入
輸出
646d
塵埃輸入
改變 650d
648d
資金輸入
串流後設資料 666

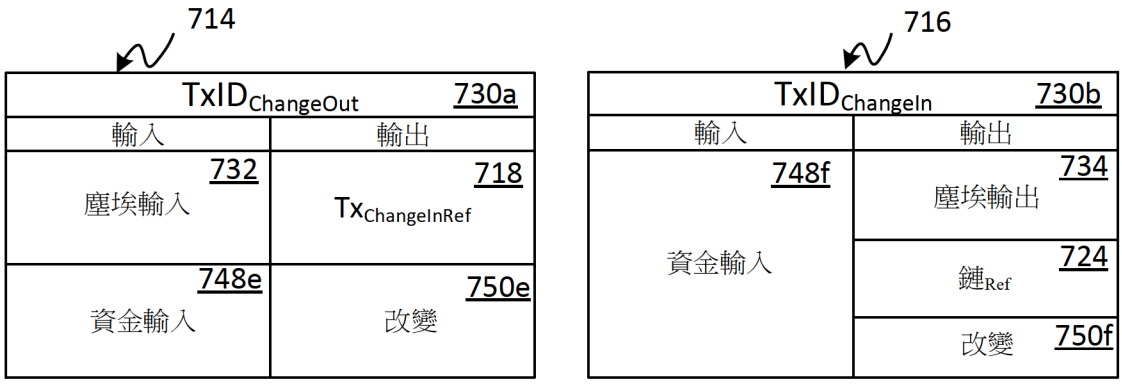
【圖6C】


680
682
接收將資料添加至鏈之請求
684
獲得最新交易
686
創建包含對最新交易之引用的新區塊鏈交易
688
將交易提交至區塊鏈

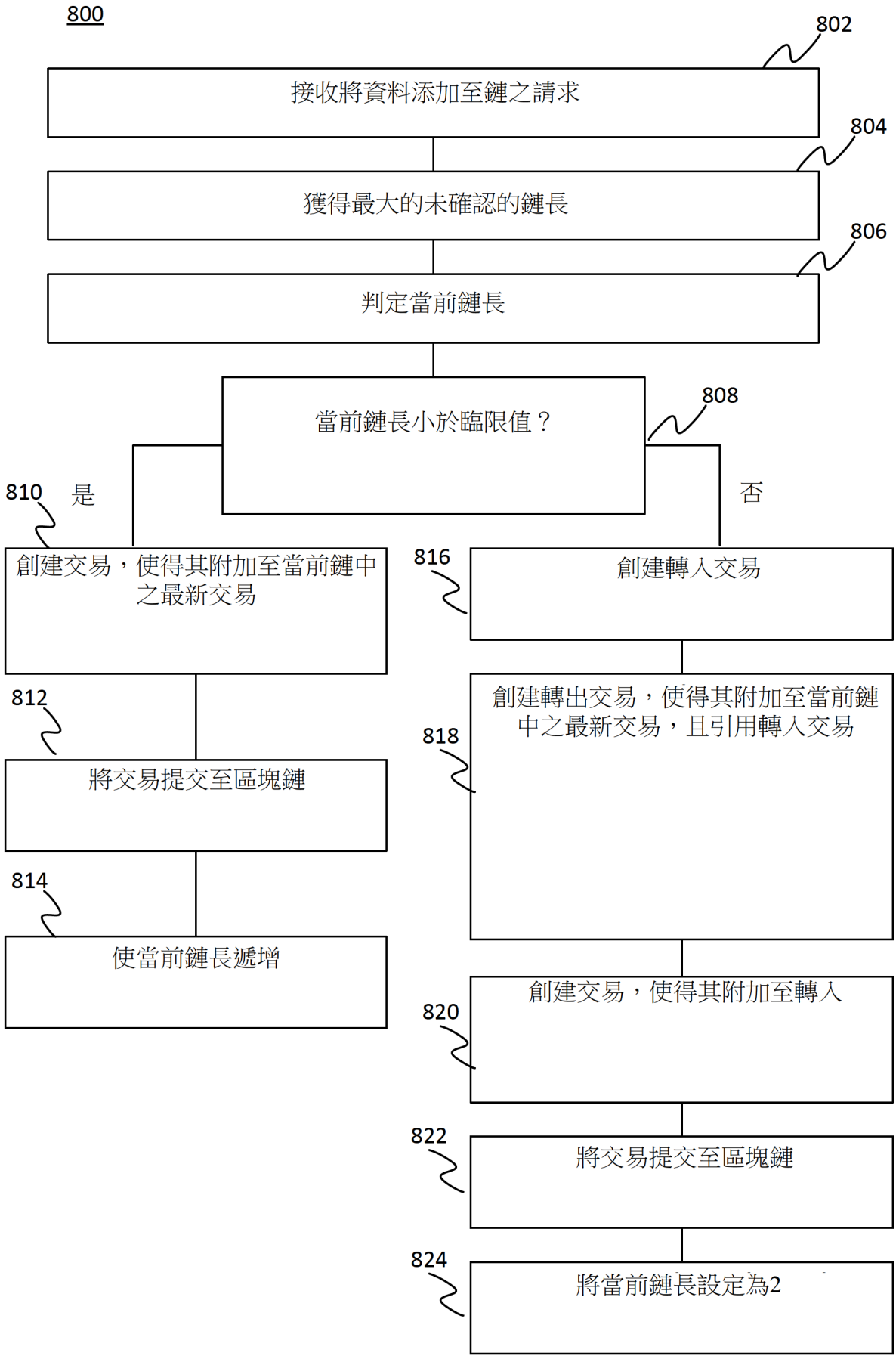
【圖6D】


702
700
Tx_0
創建酬載
706a
704a
Tx_1
酬載$_1$
706b
704b
720
Tx_{n-3}
酬載$_{n-3}$
706c
704c
Tx_{n-2}
酬載$_{n-2}$
714
722
706d
$Tx_{ChangeOut}$
718
$TxChangIn_{Ref}$
724
716
$Tx_{ChangeIn}$
鏈$_{Ref}$
706e
704d
Tx_{n-1}
酬載$_{n-1}$
706f
726
Tx_{final}
酬載$_{final}$

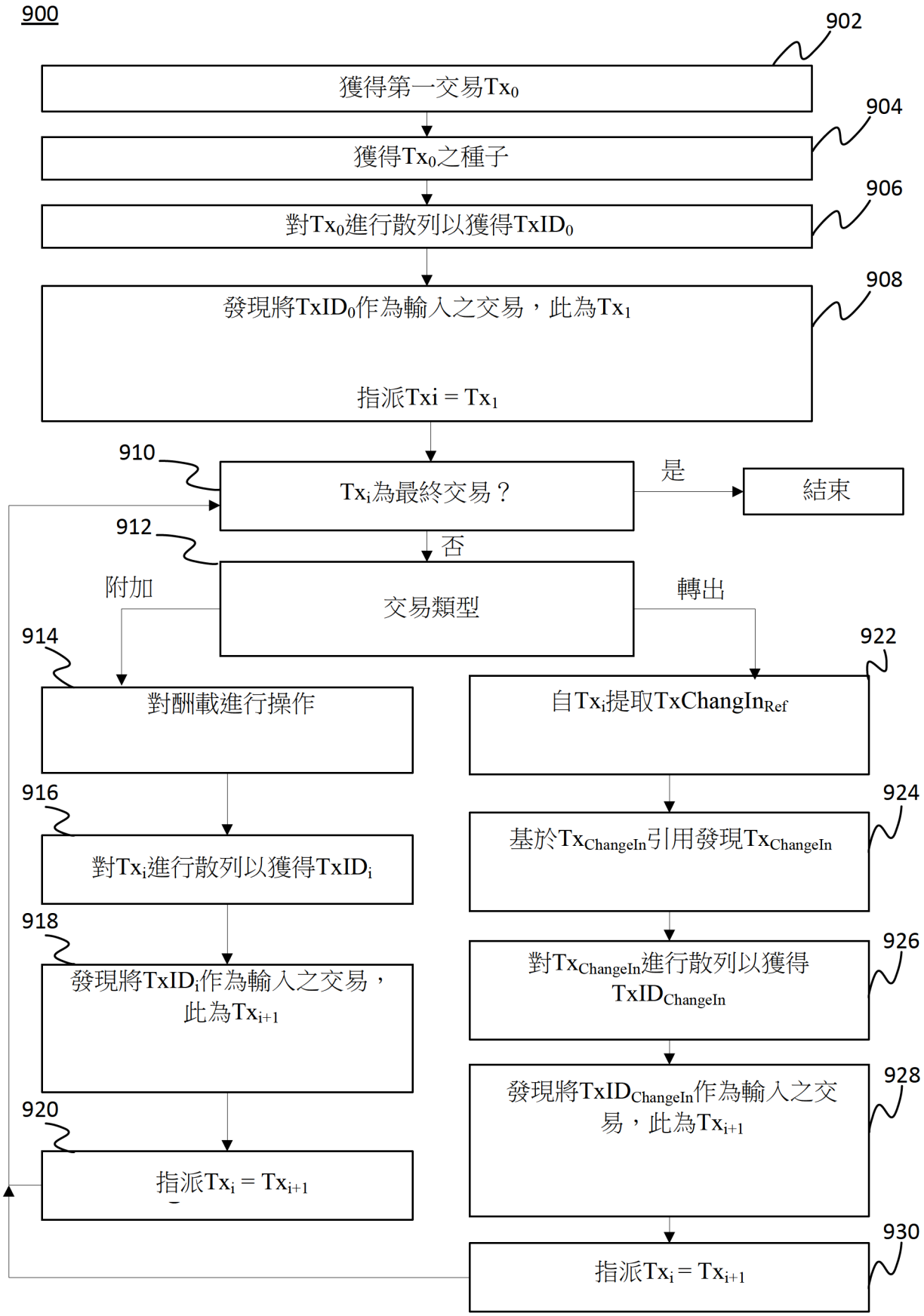
【圖7A】


714
TxID ChangeOut
730a
輸入
輸出
732
塵埃輸入
718
Tx ChangeInRef
748e
資金輸入
750e
改變
716
TxID ChangeIn
730b
輸入
輸出
748f
資金輸入
734
塵埃輸出
724
鏈Ref
750f
改變

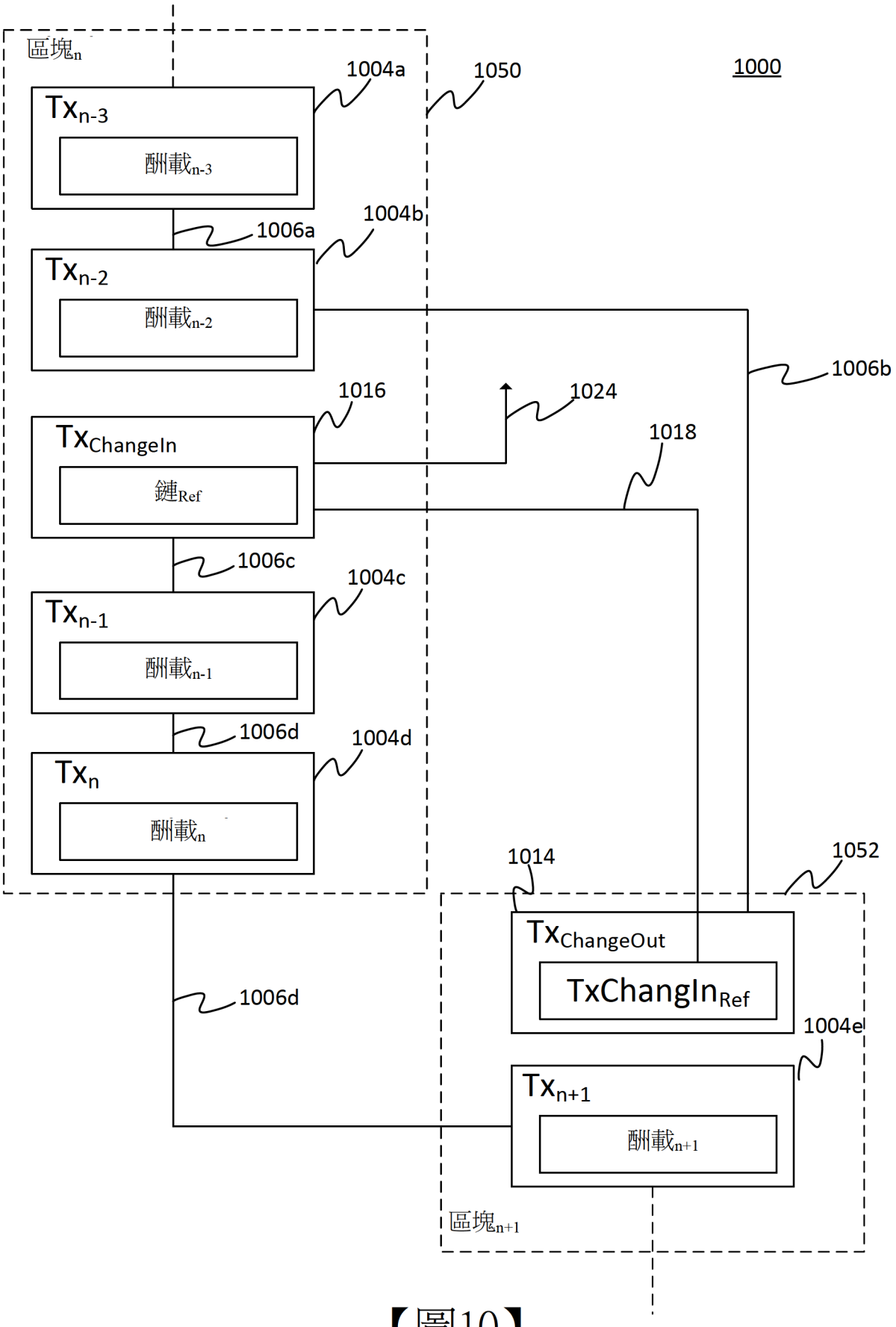
【圖7B】


800
802
接收將資料添加至鏈之請求
804
獲得最大的未確認的鏈長
806
判定當前鏈長
808
當前鏈長小於臨限值？
是
否
810
創建交易，使得其附加至當前鏈中之最新交易
812
將交易提交至區塊鏈
814
使當前鏈長遞增
816
創建轉入交易
818
創建轉出交易，使得其附加至當前鏈中之最新交易，且引用轉入交易
820
創建交易，使得其附加至轉入
822
將交易提交至區塊鏈
824
將當前鏈長設定為2

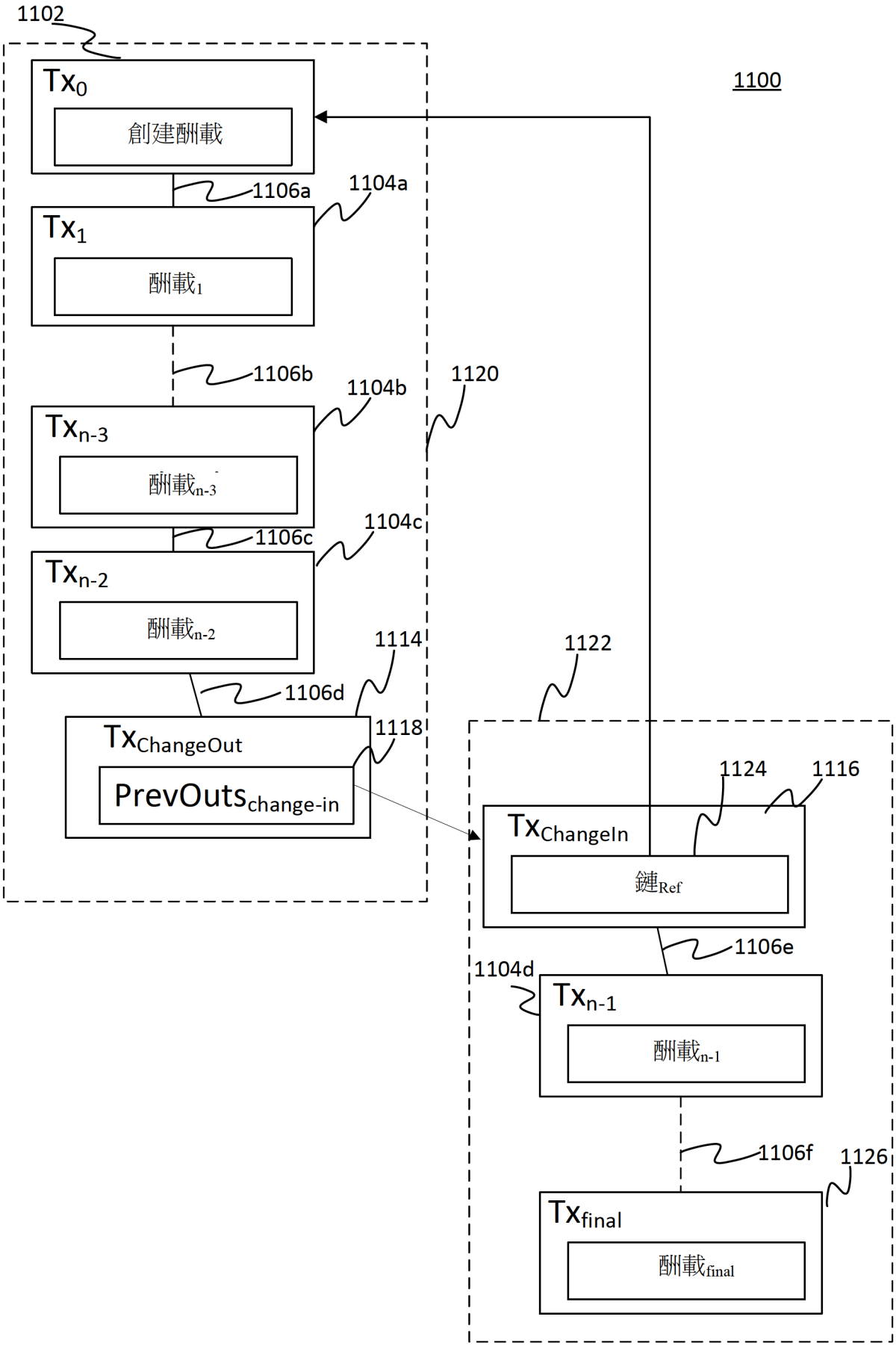
【圖8】


900
902
獲得第一交易Tx_0
904
獲得Tx_0之種子
906
對Tx_0進行散列以獲得$TxID_0$
908
發現將$TxID_0$作為輸入之交易，此為Tx_1
指派$Txi = Tx_1$
910
Tx_i為最終交易？
是
結束
912
否
附加
交易類型
轉出
914
對酬載進行操作
916
對Tx_i進行散列以獲得$TxID_i$
918
發現將$TxID_i$作為輸入之交易，此為Tx_{i+1}
920
指派$Tx_i = Tx_{i+1}$
922
自Tx_i提取$TxChangIn_{Ref}$
924
基於$Tx_{ChangeIn}$引用發現$Tx_{ChangeIn}$
926
對$Tx_{ChangeIn}$進行散列以獲得$TxID_{ChangeIn}$
928
發現將$TxID_{ChangeIn}$作為輸入之交易，此為Tx_{i+1}
930
指派$Tx_i = Tx_{i+1}$

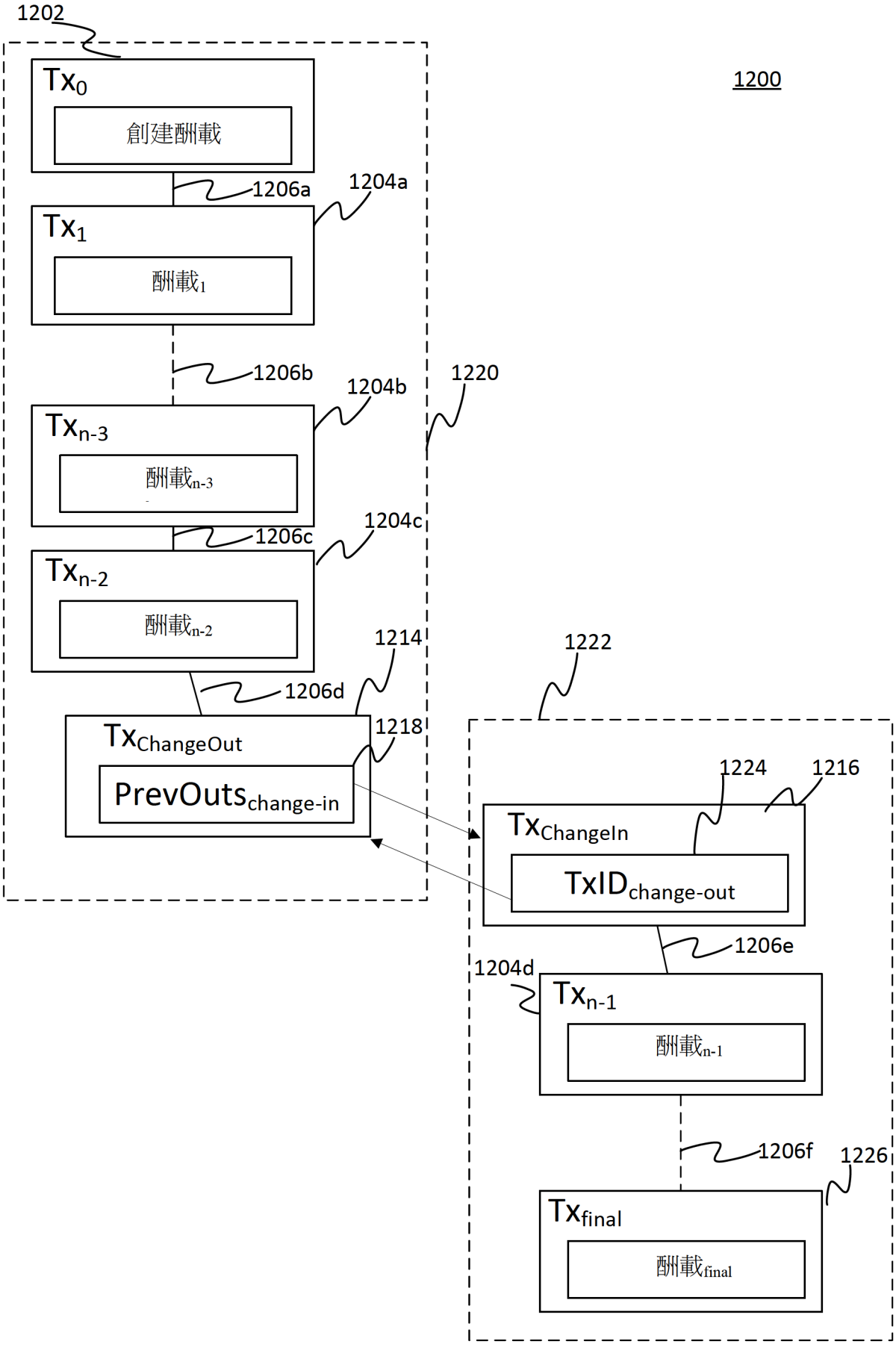
【圖9】


區塊n
1004a
1050
1000
Txn-3
酬載n-3
1004b
1006a
Txn-2
酬載n-2
1006b
1016
1024
TxChangeIn
鏈Ref
1018
1006c
1004c
Txn-1
酬載n-1
1006d
1004d
Txn
酬載n
1014
1052
TxChangeOut
TxChangInRef
1004e
Txn+1
酬載n+1
1006d
區塊n+1

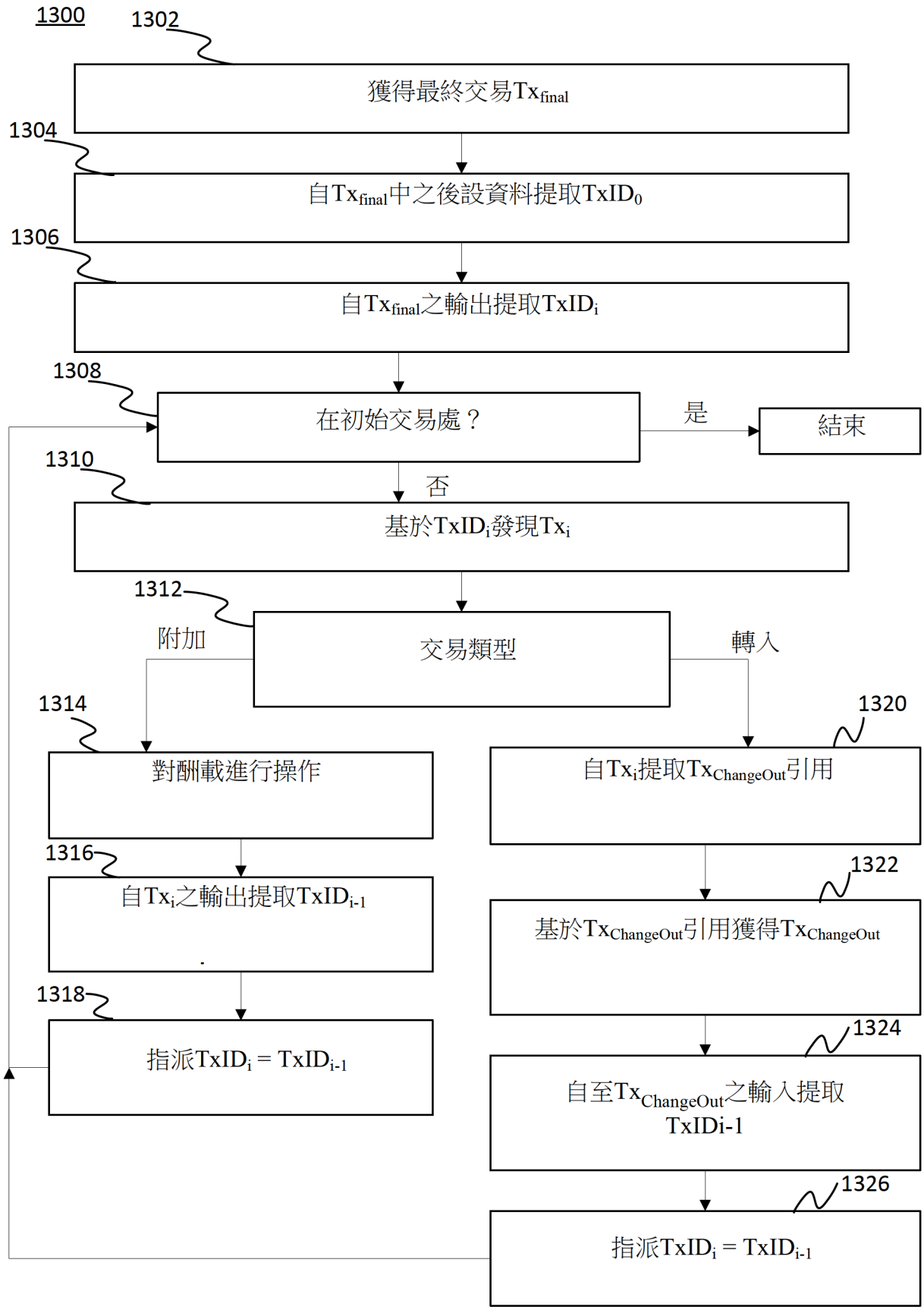
【圖10】


1102
1100
Tx0
創建酬載
1106a
1104a
Tx1
酬載1
1106b
1104b
1120
Txn-3
酬載n-3
1106c
1104c
Txn-2
酬載n-2
1114
1122
1106d
TxChangeOut
1118
PrevOutschange-in
1124
1116
TxChangeIn
鏈Ref
1106e
1104d
Txn-1
酬載n-1
1106f
1126
Txfinal
酬載final

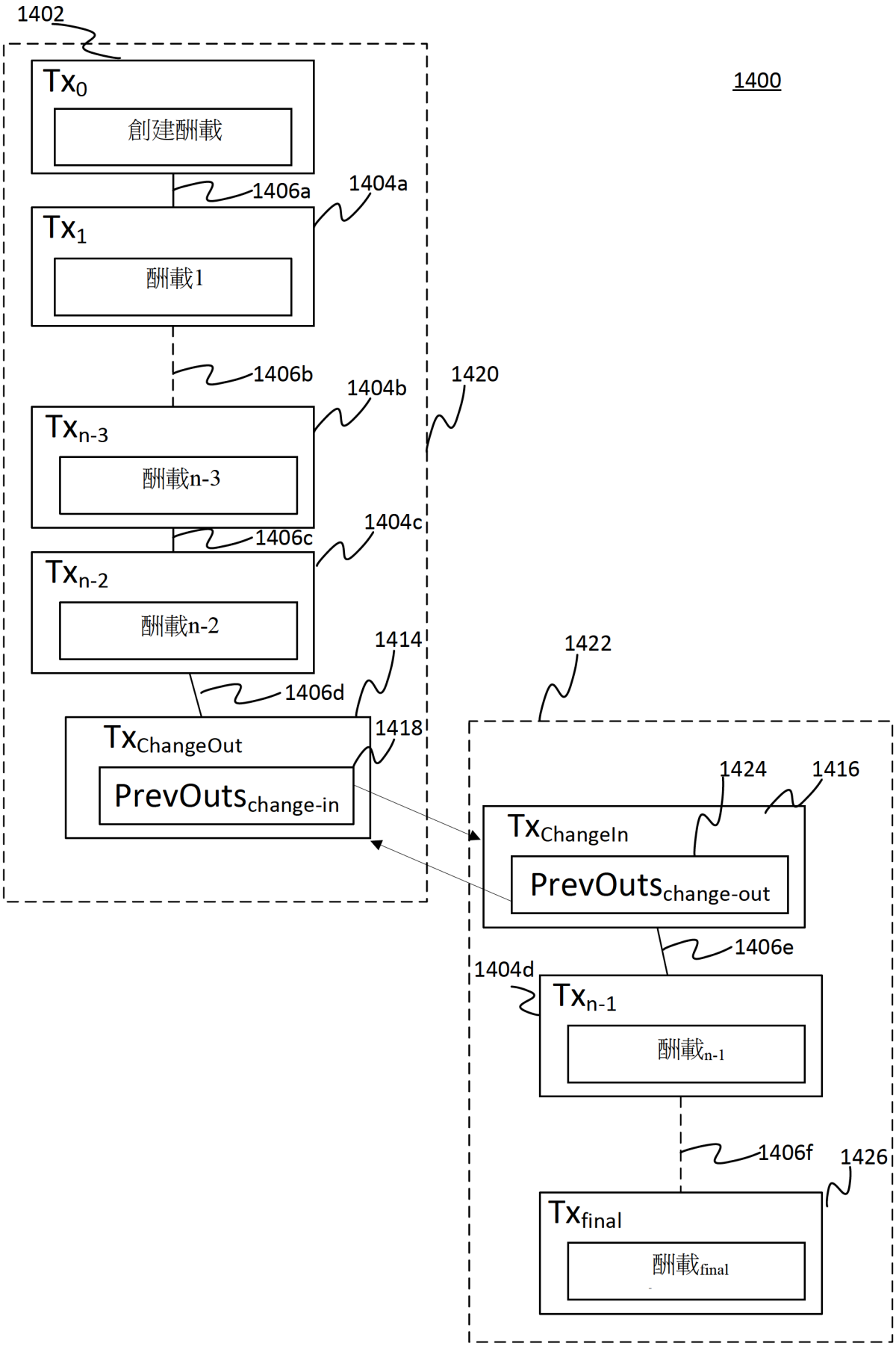
【圖11】


1202
1200
Tx0
創建酬載
1206a
1204a
Tx1
酬載1
1206b
1204b
1220
Txn-3
酬載n-3
1206c
1204c
Txn-2
酬載n-2
1214
1222
1206d
TxChangeOut
1218
PrevOutschange-in
1224
1216
TxChangeIn
TxIDchange-out
1206e
1204d
Txn-1
酬載n-1
1206f
1226
Txfinal
酬載final

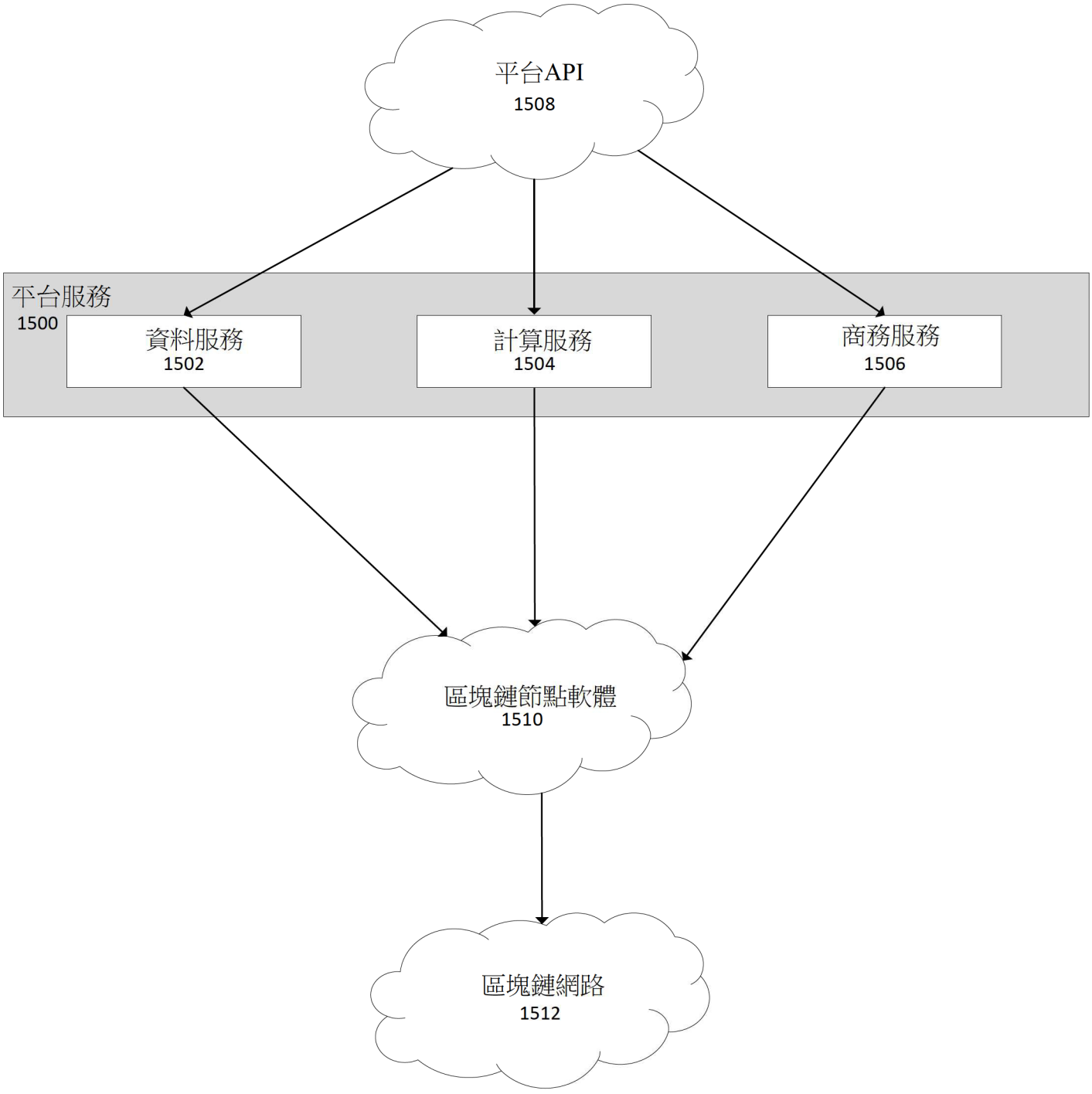
【圖12】


1300
1302
獲得最終交易Tx_{final}
1304
自Tx_{final}中之後設資料提取$TxID_0$
1306
自Tx_{final}之輸出提取$TxID_i$
1308
在初始交易處？
是
結束
否
1310
基於$TxID_i$發現Tx_i
1312
交易類型
附加
轉入
1314
對酬載進行操作
1316
自Tx_i之輸出提取$TxID_{i-1}$
1318
指派$TxID_i = TxID_{i-1}$
1320
自Tx_i提取$Tx_{ChangeOut}$引用
1322
基於$Tx_{ChangeOut}$引用獲得$Tx_{ChangeOut}$
1324
自至$Tx_{ChangeOut}$之輸入提取TxIDi-1
1326
指派$TxID_i = TxID_{i-1}$

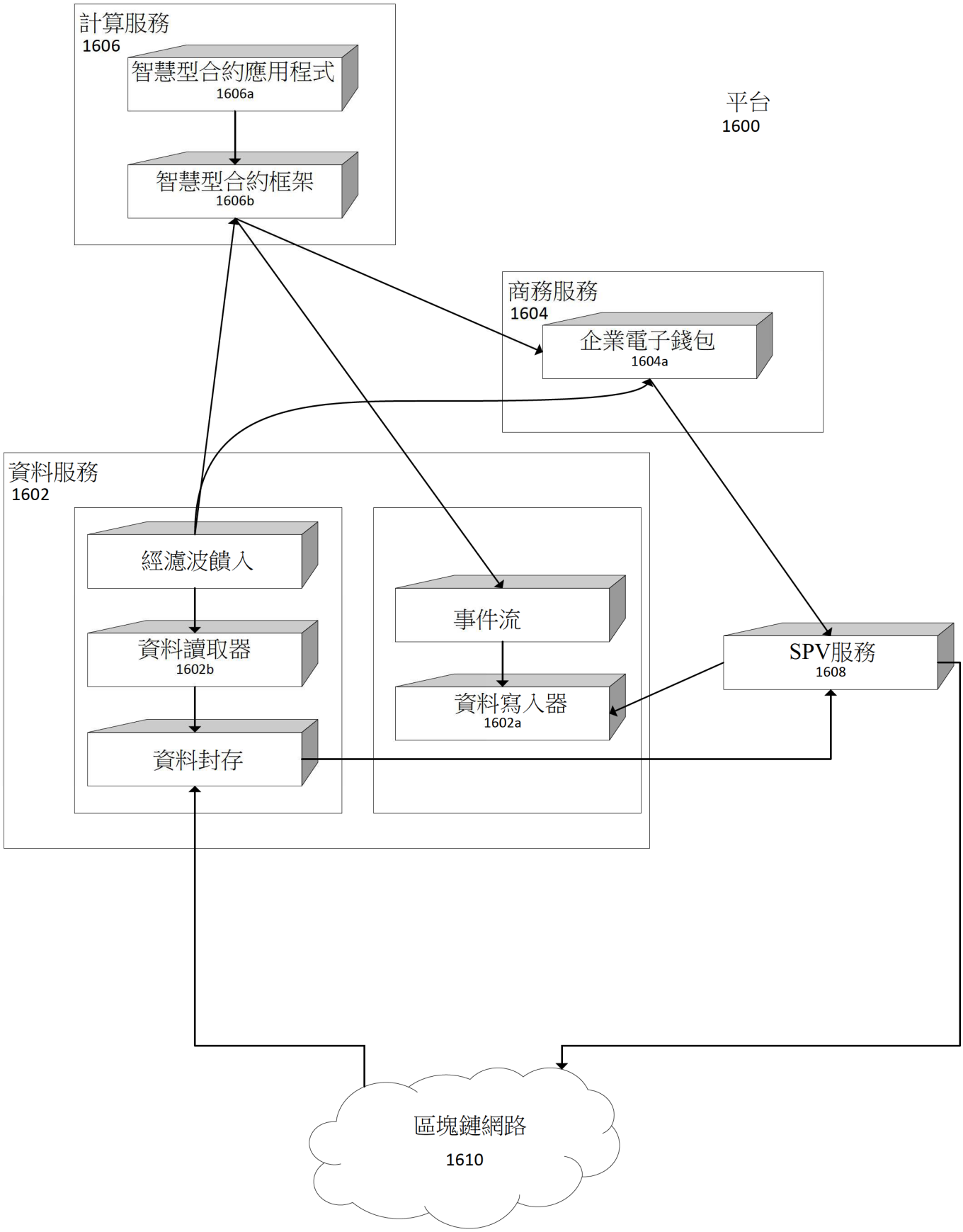
【圖13】


1402
1400
Tx0
創建酬載
1406a
1404a
Tx1
酬載1
1406b
1420
1404b
Txn-3
酬載n-3
1404c
1406c
Txn-2
酬載n-2
1414
1422
1406d
TxChangeOut
1418
PrevOutschange-in
1424
1416
TxChangeIn
PrevOutschange-out
1406e
1404d
Txn-1
酬載n-1
1406f
1426
Txfinal
酬載final

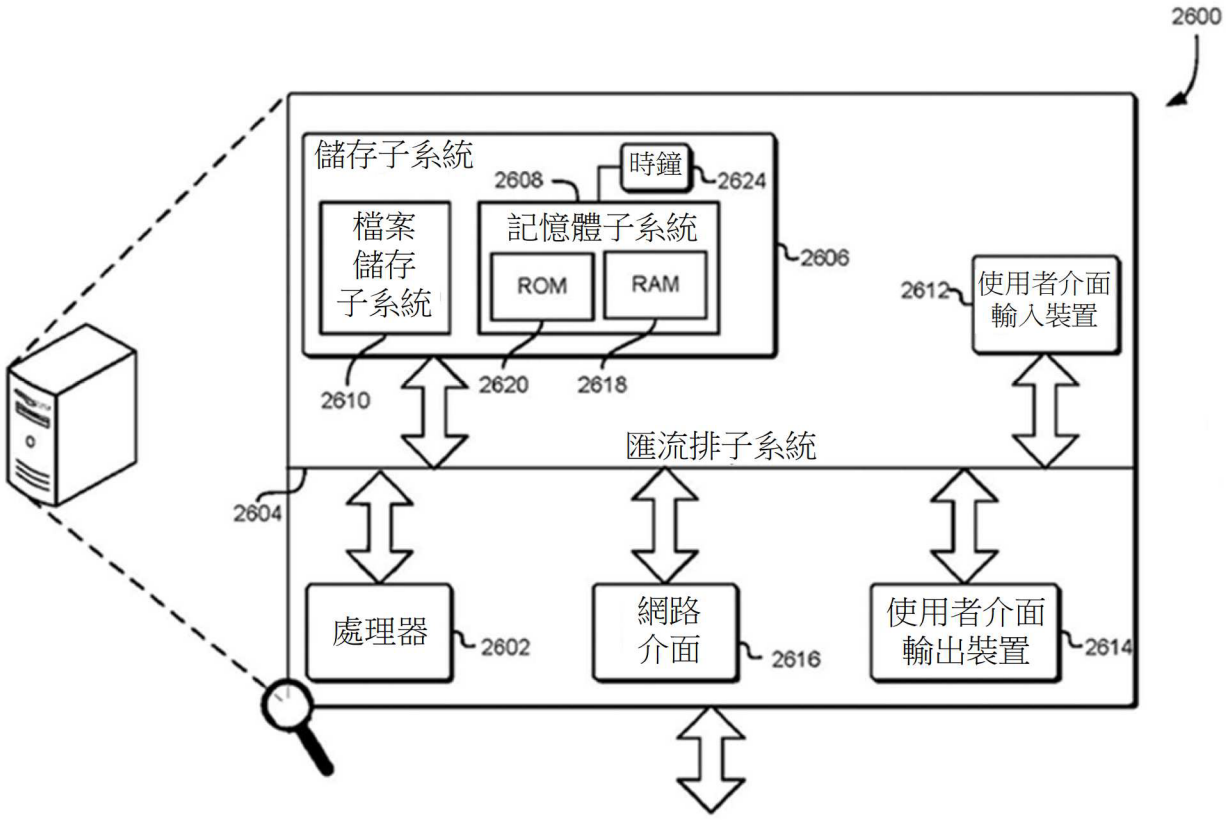
【圖14】


平台API
1508
平台服務
1500
資料服務
1502
計算服務
1504
商務服務
1506
區塊鏈節點軟體
1510
區塊鏈網路
1512

【圖15】

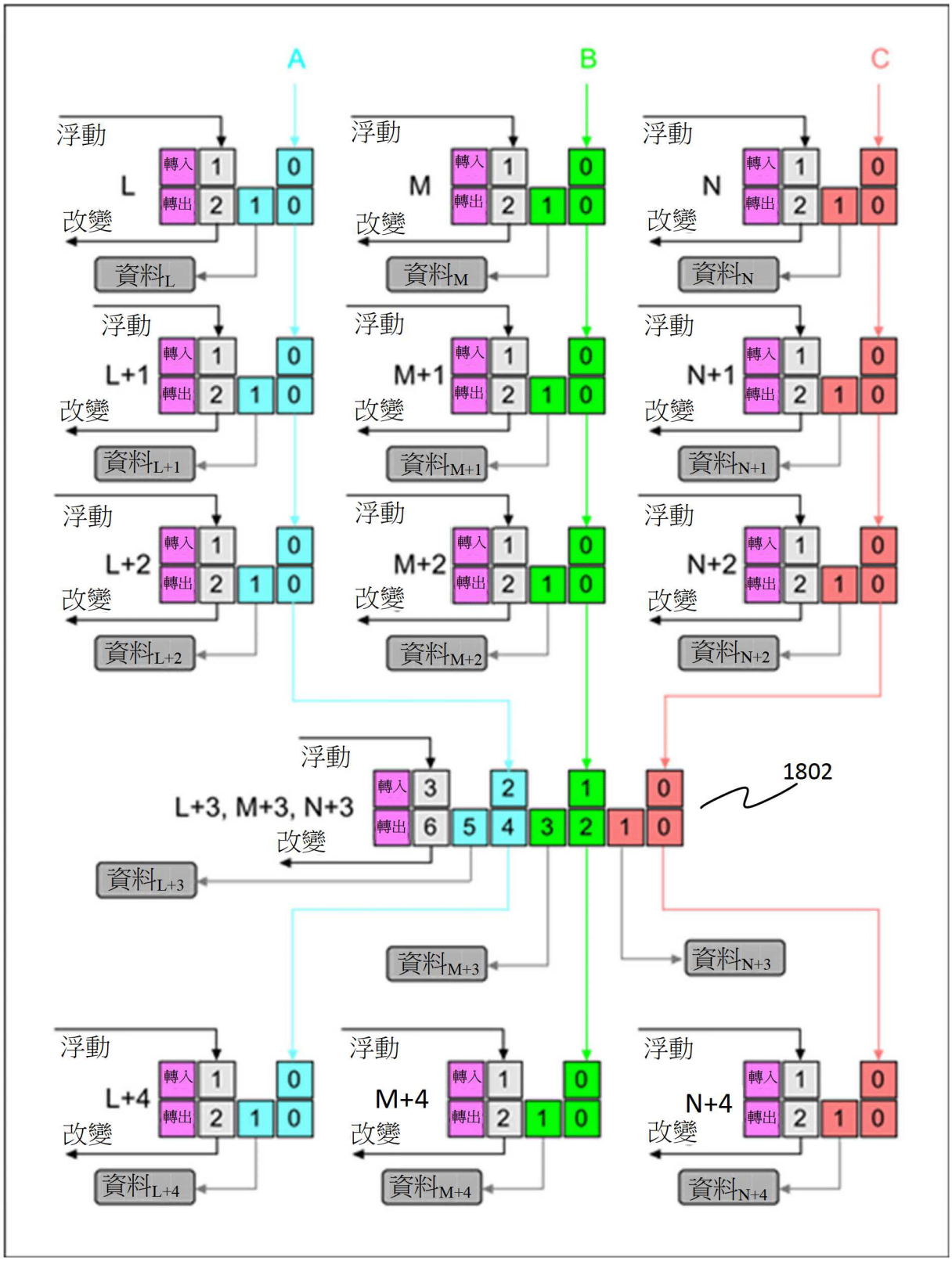

計算服務
1606
智慧型合約應用程式
1606a
智慧型合約框架
1606b
平台
1600
商務服務
1604
企業電子錢包
1604a
資料服務
1602
經濾波饋入
資料讀取器
1602b
資料封存
事件流
資料寫入器
1602a
SPV服務
1608
區塊鏈網路
1610

【圖16】


2600
儲存子系統
2608
時鐘
2624
檔案
儲存
子系統
記憶體子系統
ROM
RAM
2606
2612
使用者介面
輸入裝置
2610
2620
2618
匯流排子系統
2604
處理器
2602
網路
介面
2616
使用者介面
輸出裝置
2614

【圖17】

1800


A
B
C
浮動
L
改變
資料L
M
資料M
N
資料N
L+1
資料L+1
M+1
資料M+1
N+1
資料N+1
L+2
資料L+2
M+2
資料M+2
N+2
資料N+2
L+3, M+3, N+3
資料L+3
資料M+3
資料N+3
1802
L+4
資料L+4
M+4
資料M+4
N+4
資料N+4
轉入
轉出

【圖18】