

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

去信任確定性狀態機之電腦實施方法

TRUSTLESS DETERMINISTIC STATE MACHINE

【技術領域】

【0001】 本發明大體上係關於分散式總帳技術，包括區塊鏈交易，且更特定而言，係關於使得將來自區塊鏈交易之欄位插入至解除鎖定交易指令碼中。本發明利用密碼編譯及數學技術來加強關於經由區塊鏈網路進行之電子傳送的安全性。本發明尤其適合於但不限於用於智慧型合約及狀態機中。

【先前技術】

【0002】 在此文件中，吾人使用術語「區塊鏈」來包括所有形式的基於電腦之電子分散式總帳。此等總帳包括基於共識之區塊鏈及交易鏈技術、許可及未許可總帳、共用總帳及其變化。區塊鏈技術之最廣泛已知之應用係比特幣總帳，但已提議並開發出其他區塊鏈實施。雖然出於便利及說明的目的，「比特幣」可被稱作描述於本發明中之技術的有用應用，但比特幣僅係可應用描述於本發明中之技術的許多應用中之一者。然而應注意，本發明不限於與比特幣區塊鏈一起使用；包括非商業應用之替代區塊鏈實施及協定亦處於本發明之範圍內。舉例而言，技術對於具有類似比特幣之關於可在交易內編碼約束之限制的區塊鏈實施具有優點，而不管是否發生密碼貨幣之交換。

【0003】 區塊鏈係同級間電子總帳，其實施為由區塊組成的基於電腦的非集中式的分散式系統，區塊又由交易及其他資訊組成。在一些實例中，

「區塊鏈交易」係指編碼包含資料之欄位值之結構化彙集及條件集合的輸入訊息，該條件集合之滿足係欄位之集合待寫入至區塊鏈資料結構的前提條件。舉例而言，在比特幣之情況下，每一交易係編碼區塊鏈系統中之參與者之間的數位資產之控制傳送的資料結構，且包括至少一個輸入及至少一個輸出。在一些實施中，傳送數位資產之控制可藉由使來自第一實體之數位資產之至少一部分重新關聯至第二實體來執行。每一區塊含有先前區塊之散列，使得區塊變為鏈接在一起以產生自一開始便已寫入至區塊鏈之所有交易的永久性不可變之記錄。交易含有嵌入至其輸入及輸出中的被稱為指令碼的小型程式，其指定可如何及由誰存取交易之輸出。在比特幣平台上，此等指令碼係使用基於堆疊之指令碼處理語言來編寫。

【0004】 亦即，基於堆疊之指令碼處理語言可利用堆疊。在堆疊之情況下，值可經推入至堆疊之頂部或自堆疊之頂部彈出。對堆疊執行之各種操作可導致將該等值中之一或多者推入至堆疊之頂部或自堆疊之頂部彈出該等值中之一或多者。舉例而言，OP_EQUAL 操作將頂部兩個項目自堆疊彈出，將其進行比較且將結果(例如，若相等，則 1 或若不相等，則 0)推入至堆疊之頂部。對堆疊執行之其他操作，諸如 OP_PICK，可允許自除堆疊之頂部外的位置選擇項目。在由本發明實施例中之一些使用的一些指令碼處理語言中，可存在至少兩個堆疊：主堆疊及替代堆疊。指令碼處理語言之一些操作可將項目自一個堆疊之頂部移動至另一堆疊之頂部。舉例而言，OP_TOALTSTACK 將值自主堆疊之頂部移動至替代堆疊之頂部。

【0005】 為了將交易寫入至區塊鏈，必須「驗證」交易。網路節點(挖掘者(miner))執行工作以確保每一交易有效，其中無效交易被網路拒絕。一節點可具有不同於其他節點之有效性標準。因為區塊鏈中之有效性係基於共識的，所以若大部分節點同意交易有效，則交易被視為有效。安裝於節

點上之軟體用戶端對參考未用交易(UTXO)之交易執行此驗證工作，該驗證部分地藉由執行 UTXO 鎖定及解除鎖定指令碼來進行。若鎖定及解除鎖定指令碼之執行評估為真且其他驗證條件(若適用)滿足，則交易對該節點有效。經驗證交易被傳播至其他網路節點，因此挖掘者節點可選擇在區塊鏈中包括該交易。因此，為了將交易寫入至區塊鏈，該交易必須 i)藉由在交易經驗證之情況下接收該交易的第一節點驗證，該節點將該交易中繼傳輸至網路中之其他節點；及 ii)新增至藉由挖掘者建置之新區塊；及 iii)經挖掘，亦即，新增至過去交易之公用總帳。當足夠數目個區塊經新增至區塊鏈以使交易實際上不可逆時，該交易被視為經確認。

【0006】 本發明描述基於區塊鏈之一或多個電腦程式的技術態樣。基於區塊鏈之電腦程式係記錄於區塊鏈交易中之機器可讀且可執行程式。基於區塊鏈之電腦程式包含可處理輸入以便產生結果之規則，該等規則可接著取決於彼等結果而使得執行動作。若鎖定指令碼可存取解除鎖定交易及先前交易兩者，則區塊鏈可用以實現非常靈活且複雜的智慧型合約。當前研究之一個領域係使用基於區塊鏈之電腦程式來實施「智慧型合約」。不同於將以自然語言加以書寫之傳統合約，智慧型合約可係經設計以使機器可讀合約或協議之條款之執行自動化的電腦程式。

【0007】 在實施例中，儘管可在智慧型合約中之特定步驟處編碼與特定實體之互動，但智慧型合約可另外被自動地執行且自我強制實行。在一些實例中，自動執行係指成功地執行以實現 UTXO 之傳送之智慧型合約之執行。應注意，在此等實例中，能夠使得傳送 UTXO 之「實體」係指能夠在無需證明對某個秘密之瞭解的情況下建立解除鎖定指令碼的實體。換言之，可驗證解除鎖定交易而無需證實資料源(例如，建立解除鎖定交易之實體)可存取密碼編譯秘密(例如，私用不對稱密鑰、對稱密鑰等)。又，在此

等實例中，自我強制實行係指使得區塊鏈網路之驗證節點根據約束強制實行解除鎖定交易。在一些實例中，在技術意義上使用「解除鎖定」UTXO (亦稱為「花用」UTXO)，係指建立參考 UTXO 且有效執行之解除鎖定交易。

【0008】 區塊鏈交易輸出包括鎖定指令碼及關於諸如比特幣之數位資產之所有權的資訊。亦可被稱作負擔(encumbrance)之鎖定指令碼藉由指定需要滿足以便傳送 UTXO 之條件來「鎖定」數位資產。舉例而言，鎖定指令碼可能需要提供於解除鎖定指令碼中之某些資料來解除鎖定相關聯之數位資產。在比特幣中，鎖定指令碼亦被稱為「scriptPubKey」。需要一方提供資料來解除鎖定數位資產之技術涉及將資料之散列嵌入鎖定指令碼內部。然而，若在建立鎖定指令碼時資料未經判定(例如，未知且固定)，則此嵌入呈現問題。

【0009】 因此，需要提供在此等態樣中之一或多者中改良區塊鏈技術的改良之方法及系統。因此，根據本發明，提供一種如隨附申請專利範圍中所定義之方法及對應系統。

【發明內容】

【0010】 本發明可描述為一種證實方法、系統及或描述為一種用於控制區塊鏈交易之驗證的控制方法及系統。在一些實施例中，經驗證區塊鏈交易導致區塊鏈上之交易的記錄，其在一些應用中可導致數位資產經由區塊鏈之交換或傳送。數位資產係由區塊鏈管理之資源單位。儘管在一些實施例中，數位資產可用作密碼貨幣，但預期數位資產在實施例中另外或替代地可用於其他內容背景中。應注意，雖然適用於數位資產之控制，但本發明在本質上係技術性的且可用於利用區塊鏈資料結構而未必涉及數位資產之傳送的其他內容背景中。如下文所解釋，本發明亦可描述為一種用於經由區塊鏈網路或平台執行操作之新、經改良且有利的的安全性方法

及系統。

【0011】 如下文將更詳細地描述，在一實施例中，鎖定指令碼可藉由自解除鎖定交易之解除鎖定指令碼獲取解除鎖定交易之欄位值之集合及簽名散列(SIGHASH)類型作為輸入以及執行簽名產生及證實操作來存取解除鎖定交易之某些欄位。

【0012】 如下文將更詳細地描述，在一實施例中，鎖定指令碼可藉由約束自解除鎖定交易之某些欄位提取的交易識別符(ID)使得經序列化先前交易包括於解除鎖定交易之解除鎖定指令碼中來存取先前交易之欄位之集合。根據實施例，可提供一種藉由以下操作將經序列化先前交易插入區塊鏈交易鎖定指令碼中的方法：獲取對應於第一交易之欄位值之第一集合及對應於另一交易之欄位值之第二集合作為輸入；自欄位值之第一集合提取交易識別符；及基於欄位值之第二集合判定另一交易對應於交易識別符。

【0013】 如下文將更詳細地描述，在一實施例中，鎖定及解除鎖定指令碼可經組態以實現來自經判定或未判定源之未判定資料的安全佈建。為了使來自未判定源之資料免於更改，可將該資料嵌入於經序列化先前交易中。應注意，即使資料處於經序列化先前交易中，在鎖定指令碼並不將資料約束於某值之意義上，資料仍被視為未判定。為了使來自經判定源之資料免於更改，可將來自該經判定源之公用密鑰包括於鎖定指令碼中，在該鎖定指令碼中，資料可用以修改公用密鑰，該公用密鑰可接著用以驗證使用經修改之私用密鑰進行簽名的資料之簽名。根據實施例，可提供一種獲得未判定資料及第二值之方法，且驗證未判定資料與資料源相關聯係基於提供於解除鎖定指令碼中之資料及第二值。

【0014】 如下文將更詳細地描述，在一實施例中，經參數化之智慧型合約可藉由自先前交易提取約束參數及將約束參數應用於解除鎖定交易之

欄位來建立。經參數化之智慧型合約可經由鎖定指令碼實現，該鎖定指令碼具有藉由自經判定或未判定源提供於解除鎖定交易之解除鎖定指令碼中的安全未判定資料來參數化的約束。根據實施例，可提供一種獲得未判定資料之方法，自該未判定資料可判定應用於數位資產之重新關聯的約束之集合且根據約束之集合使數位資產與第二實體重新關聯。

【0015】 如下文將更詳細地描述，在一實施例中，智慧型合約係建立為自我複寫直至達成終止條件。根據實施例，可提供一種檢查終止條件之滿足的方法，且若終止條件未滿足，則檢查先前交易之鎖定指令碼匹配解除鎖定交易之鎖定指令碼。

【0016】 如下文將更詳細地描述，在一實施例中，經參數化之自我複寫智慧型合約可用以建立去信任確定性狀態機。根據實施例，可提供一種證實自我複寫鎖定指令碼且至少部分地基於來自經判定源之輸入及去信任確定性狀態機之當前狀態而判定去信任確定性狀態機之下一狀態的方法。

【0017】 在本發明中所描述及建議之新穎技術擴展區塊鏈之功能性而不妨礙區塊鏈的確保存儲於區塊鏈資料結構內之資料之完整性的性質。舉例而言，該等技術藉由利用區塊鏈網路來設定及強制實行用於重新關聯數位資產之準則而改良計算領域，具體而言改良數位記錄驗證領域，其中驗證條件係嵌入於記錄中之所定義智慧型合約。另外，在本發明中所描述及建議之技術可藉由使區塊鏈交易能夠充當狀態機以使電腦程式功能性能夠取決於在此等狀態機中記錄之狀態來改良區塊鏈網路之功能性。

【0018】 此外，在本發明中所描述及建議之技術可必定根植於電腦技術中，以便克服特定地由已經特定設計以出於安全性原因而限定功能性之區塊鏈技術(諸如，比特幣之指令碼)引起的問題。舉例而言，指令碼本身並不支援複雜的流程控制功能性，例如，出現迴圈。此限定之一個優點係程

式具有可預測的執行時間。將指令碼限於線性或樹狀決策任務之另一顯著優點係此避免無限迴圈，無限迴圈可用作啟動諸如阻斷服務(DoS 或 DDoS)攻擊之惡意探索(exploit)的手段。因此，區塊鏈傳送或交換之安全性經增強及保持，但需要找到實施語言自身不准許或提供之功能性的機制。本發明提供在此方面之進步，藉由實施自我複寫及自我參考區塊鏈交易鎖定指令碼來至少部分地解決區塊鏈交易之當前限制。因此，本發明提供對技術問題之技術解決方案，且供應在安全性、經由區塊鏈之數位資產交換或傳送的改良控制以及當前區塊鏈相關功能性之擴充方面的優點。

【0019】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之電腦實施方法(及對應系統)。該電腦實施方法可描述為區塊鏈資料約束方法。該電腦實施方法可包括：i)在區塊鏈網路中之節點處接收第一交易以傳送數位資產之控制，第一交易包括第一指令碼，該第一指令碼至少：包括第一交易之欄位值之集合；及作為被執行之結果，使節點獲得欄位值之集合；ii)獲得第二交易，第二交易與數位資產相關聯且包括第二指令碼，作為被執行之結果，該第二指令碼使節點至少部分地基於作為執行第一指令碼之結果而供應之欄位值之集合來至少產生簽名；及 iii)藉由執行第一指令碼及第二指令碼來驗證第一交易。

【0020】 驗證第一交易可經成功地執行而無需證實建立第一交易之實體可存取秘密資訊。

【0021】 第一指令碼可進一步包括不對稱密鑰對中之私用密碼編譯密鑰。另外或替代地，第二指令碼可進一步使節點至少部分地基於私用密碼編譯密鑰及遮罩數字來產生簽名。另外或替代地，驗證第一交易可進一步包括驗證簽名與不對稱密鑰對中之公用密碼編譯密鑰相關聯。

【0022】 第一指令碼可進一步指定簽名散列類型。另外或替代地，欄

位值之集合可至少部分地基於簽名散列類型。

【0023】 簽名散列類型可係指示第一交易之欄位值之集合中的哪些欄位值待包括於簽名中的值。

【0024】 第二指令碼可係強加用於驗證第一交易之條件之集合的鎖定指令碼。另外或替代地，鎖定指令碼之執行可使節點藉由判定條件之集合是否已滿足來驗證第一交易。

【0025】 第一指令碼可係用於符合第二指令碼之條件之集合的解除鎖定指令碼。

【0026】 數位資產可與區塊鏈網路中之未用交易輸出相關聯。

【0027】 節點可係以通信方式耦接至區塊鏈網路中之至少一個其他節點的計算裝置。

【0028】 區塊鏈網路可由運行區塊鏈協定之執行個體的分散式電子裝置組成。

【0029】 第一指令碼及第二指令碼可使用圖靈不完整指令集加以編寫。

【0030】 第一指令碼及第二指令碼係使用圖靈完整指令集加以編寫。

【0031】 藉由包括欄位之集合，作為執行第一指令碼之結果，第一指令碼可使節點可將欄位之集合用作第二指令碼之輸入。

【0032】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0033】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0034】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之電腦實施方法(及對應系統)。該電腦實施方法可描述為區塊鏈資料約束方法。該電腦實施方法可包括：i)在區塊鏈網路中之節點處接收第一交易以傳送數位資產之控制，第一交易包括第一指令碼，作為被執行之結果，該第一指令碼使節點至少：獲得對應於第一交易之欄位值之第一集合；及獲得對應於特定交易之欄位值之第二集合；ii)獲得第二交易，第二交易與數位資產相關聯且包括第二指令碼，作為被執行之結果，該第二指令碼使節點至少：獲得作為執行第一指令碼之結果而供應的欄位值之第一集合及特定交易之欄位值之第二集合；自欄位值之第一集合提取交易識別符；及至少部分地基於欄位值之第二集合而判定特定交易對應於交易識別符；及 iii)藉由執行第一指令碼及第二指令碼來驗證第一交易。

【0035】 欄位值之第二集合可呈規範化格式。

【0036】 節點可藉由產生欄位值之第二集合的散列來判定特定交易對應於交易識別符。另外或替代地，節點可藉由證實散列匹配交易識別符來判定特定交易對應於交易識別符。

【0037】 特定交易可與正在經傳送之數位資產之控制相關聯。

【0038】 特定交易可與不同於正在經傳送之數位資產的第二數位資產相關聯。

【0039】 驗證第一交易可成功而無需證實建立第一交易之實體可存取秘密資訊。

【0040】 節點可係區塊鏈網路之驗證節點。

【0041】 作為第一交易之成功驗證的結果，驗證第一交易可進一步包括將第一交易新增至區塊鏈網路中之區塊鏈。

【0042】 第二指令碼可係強加用於驗證第一交易之條件之集合的鎖

定指令碼。另外或替代地，鎖定指令碼之執行可使節點藉由判定條件之集合是否已滿足來驗證第一交易。

【0043】 第一指令碼可係用於符合第二指令碼之條件之集合的解除鎖定指令碼。

【0044】 第一指令碼可指定簽名散列類型。另外或替代地，作為被執行之結果，第二指令碼可進一步使節點獲得作為執行第一指令碼之結果而供應的簽名散列類型。

【0045】 作為被執行之結果，第二指令碼可進一步使節點至少部分地基於簽名散列類型而判定特定交易係與第一交易相關聯之交易之集合的成員。

【0046】 作為被執行之結果，第二指令碼可進一步使節點至少部分地基於簽名散列類型而判定特定交易對應於第二交易。

【0047】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0048】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0049】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之電腦實施方法(及對應系統)。該電腦實施方法可描述為區塊鏈資料約束方法。該電腦實施方法可包括：i)在區塊鏈網路中之節點處接收第一交易以傳送數位資產之控制，第一交易包括第一指令碼，該第一指令碼至少包括：第一值，該第一值之至少一部分包括不受第二指令碼約束之資料；及第二值；ii)獲得第二交易，第二交易與數位資產相關聯且包括第二指令碼，作為

被執行之結果，該第二指令碼使節點至少：獲得作為執行第一指令碼之結果的第一值及第二值；及至少部分地基於第一值及第二值而驗證資料與特定源相關聯；及 iii)藉由執行第一指令碼及第二指令碼來驗證第一交易。

【0050】 第二指令碼可係包括用於驗證第二交易之條件之集合的鎖定指令碼。另外或替代地，第一指令碼可係用於符合鎖定指令碼之條件之集合的解除鎖定指令碼。

【0051】 驗證第一交易可經執行而無需證實建立第一交易之實體可存取秘密資訊。

【0052】 資料與資料源相關聯之不成功驗證可使得驗證第一交易不成功。

【0053】 特定源之身分可不受第二指令碼約束。

【0054】 特定交易可係特定資料源。另外或替代地，第一值可係特定交易之欄位值之集合。另外或替代地，第二值可包括與特定交易相關聯之交易識別符。第二指令碼可藉由驗證特定交易對應於交易識別符來驗證資料與資料源相關聯。

【0055】 第二指令碼可藉由驗證交易識別符匹配特定交易之欄位之集合的散列來驗證特定交易對應於交易識別符。

【0056】 藉由包括特定交易之欄位之集合，作為執行第一指令碼之結果，第一指令碼可使節點可將特定交易之欄位之集合用作第二指令碼之輸入。

【0057】 特定交易可係第二交易。

【0058】 資料可編碼於特定交易之欄位中。

【0059】 第二指令碼可約束特定源之身分。

【0060】 第二值可係簽名。另外或替代地，第二指令碼可進一步使節

點獲得與資料源相關聯之公用密鑰，且另外或替代地，至少部分地基於公用密鑰及資料而產生經修改之公用密鑰。另外或替代地，第二指令碼可至少部分地基於經修改之公用密鑰而驗證資料與資料源相關聯。

【0061】 經修改之公用密鑰可藉由對公用密鑰與資料之值執行橢圓曲線點乘法來產生。

【0062】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0063】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之電腦實施方法(及對應系統)。該電腦實施方法可描述為區塊鏈資料約束方法。該電腦實施方法可包括：i) 在區塊鏈網路中之節點處接收第一交易以傳送數位資產之控制，第一交易包括第一指令碼，作為被執行之結果，該第一指令碼使節點至少獲得資料及第一交易之欄位值之第一集合；ii) 獲得第二交易，第二交易包括第二指令碼，作為被執行之結果，該第二指令碼使節點至少：至少部分地基於作為執行第一指令碼之結果而供應之資料而判定約束之集合；及至少部分地基於欄位值之第一集合而證實針對第一交易之約束之集合；及 iii) 作為執行第一指令碼及第二指令碼之結果而根據約束之集合傳送數位資產之控制。

【0064】 傳送數位資產之控制可經執行而無需證實建立第一交易之實體可存取秘密資訊。

【0065】 資料源之身分可不受第二指令碼約束。

【0066】 第二指令碼可約束資料源之身分。

【0067】 第二指令碼可包括可用以驗證資料之特定資料源的公用密鑰。

【0068】 驗證資料可包括至少部分地基於公用密鑰及資料而產生經修改之公用密鑰，及另外或替代地，至少部分地基於經修改之公用密鑰而判定資料與資料源相關聯。

【0069】 約束之集合可至少部分地自資料中之參數集導出。

【0070】 約束之集合的滿足可係用於重新關聯數位資產之至少部分的條件。

【0071】 傳送數位資產之控制可包括使來自第一實體之數位資產重新關聯至第二實體。

【0072】 第二實體之身分可至少部分地基於約束之集合而加以判定。

【0073】 資料源可係第二交易。另外或替代地，資料包括第二交易之欄位值之第二集合。另外或替代地，第二指令碼之執行可使約束之集合至少部分地自欄位值之第二集合導出。

【0074】 第二實體之身分可至少部分地基於約束之集合而加以判定。

【0075】 約束之集合可進一步使數位資產之至少一部分與第三實體重新關聯。

【0076】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0077】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0078】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定

義之電腦實施方法(及對應系統)。該電腦實施方法可描述為區塊鏈資料約束方法。該電腦實施方法可包括：i)在區塊鏈網路中之節點處接收第一交易以傳送數位資產之控制，第一交易包括第一指令碼，作為被執行之結果，該第一指令碼使節點至少：獲得第一交易之欄位值之第一集合，欄位值之第一集合包括第三指令碼；及獲得第二交易之欄位值之第二集合，欄位值之第二集合包括第二指令碼之複本；ii)獲得第二交易，第二交易包括第二指令碼，作為被執行之結果，該第二指令碼使節點作為判定終止條件未滿足之結果而至少：自欄位值之第一集合獲得第三指令碼；及判定第二指令碼之複本匹配第三指令碼；及 iii)作為執行第一指令碼及第二指令碼之結果而傳送數位資產之控制。

【0079】 第二交易可係與數位資產相關聯之交易。另外或替代地，第一交易可係使來自第一實體之數位資產之至少部分重新關聯至第二實體的交易。

【0080】 第一指令碼可係用於符合第二指令碼之條件之集合的解除鎖定指令碼。

【0081】 第二指令碼可係強加用於驗證第一交易之條件之集合的鎖定指令碼。

【0082】 第三指令碼可係強加用於驗證未來交易之條件之集合的鎖定指令碼。

【0083】 傳送數位資產之控制可包括使來自第一實體之數位資產重新關聯至第二實體。

【0084】 判定終止條件未滿足可包括判定與第二交易相關聯之數位資產的量足以重新關聯數位資產之至少部分。

【0085】 第三指令碼可嵌入於欄位值之第一集合中的欄位值中。

【0086】 區塊鏈網路可由運行區塊鏈協定之執行個體的分散式電子裝置組成。

【0087】 傳送數位資產之控制可經執行而無需證實建立第一交易之實體可存取秘密資訊。

【0088】 作為用於傳送數位資產之控制的另一條件，第二指令碼可進一步使節點證實第一交易滿足額外約束。

【0089】 第一交易及第二交易可係與數位資產相關聯之重複智慧型合約之集合的成員。

【0090】 重複智慧型合約之集合可藉由終止條件來終止。

【0091】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0092】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0093】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之電腦實施方法(及對應系統)。該電腦實施方法可描述為區塊鏈資料約束方法。該電腦實施方法可包括：一種電腦實施方法，其包含：i)在區塊鏈網路中之節點處接收第一交易以傳送數位資產之控制，第一交易包括第一指令碼，作為被執行之結果，該第一指令碼使節點至少獲得第一交易之欄位值之第一集合、第二交易之欄位值之第二集合以及輸入；ii)獲得第二交易，第二交易包括第二指令碼，該第二指令碼包括規則之集合，作為被執行之結果，該第二指令碼使節點至少：證實第二指令碼匹配嵌入於欄位值之第一集合中的第三指令碼；至少部分地基於欄位值之第二集合而判定當前狀

態；及至少部分地基於當前狀態、輸入及規則之集合而判定下一狀態；證實下一狀態包括於欄位值之第一集合中；及 iii)作為執行第一指令碼及第二指令碼之結果而傳送數位資產之控制。

【0094】 第二指令碼可約束輸入源之身分。

【0095】 如所主張之方法中之任一者可進一步包含證實輸入源之密碼編譯秘密。

【0096】 規則之集合可係狀態轉移矩陣。

【0097】 第三指令碼可係強加用於驗證未來交易之條件之集合的鎖定指令碼。

【0098】 第二指令碼可進一步使節點判定終止條件未滿足。

【0099】 輸入可嵌入於欄位值之第二集合中。

【0100】 終止條件可係與第二交易相關聯之數位資產的大小不足以被傳送。

【0101】 當前狀態可指示第二交易之狀態。

【0102】 下一狀態可指示第一交易在驗證後之狀態。

【0103】 如所主張之方法中之任一者可進一步包含接收第三交易。另外或替代地，如所主張之方法中之任一者可進一步包含自第一交易獲得第四指令碼，作為被執行之結果，該第四指令碼使節點至少部分地基於下一狀態、第二輸入及規則之集合而判定不同於下一狀態及當前狀態之另一狀態。

【0104】 當前狀態及下一狀態可係第一交易及第二交易之可能狀態之集合的成員。

【0105】 傳送數位資產之控制可包括使來自第一實體之數位資產重新關聯至第二實體。

【0106】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0107】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0108】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之方法(及對應系統)。該方法可描述為區塊鏈資料約束方法。該方法可包括：在區塊鏈網路中之節點處接收第一交易以驗證，第一交易包括第一指令碼，該第一指令碼至少：包括第一交易之欄位值之集合；及作為被執行之結果，使節點獲得欄位值之集合；ii)獲得第二交易，第二交易已經驗證且包括第二指令碼，作為被執行之結果，該第二指令碼使節點至少部分地基於作為執行第一指令碼之結果而供應之欄位值之集合來至少產生簽名；及iii)藉由執行第一指令碼及第二指令碼來驗證第一交易。

【0109】 驗證第一交易可經成功地執行而無需證實建立第一交易之實體可存取秘密資訊。

【0110】 第一指令碼可進一步包括不對稱密鑰對中之私用密碼編譯密鑰。另外或替代地，第二指令碼可進一步使節點至少部分地基於私用密碼編譯密鑰及遮罩數字來產生簽名。另外或替代地，驗證第一交易可進一步包括驗證簽名與不對稱密鑰對中之公用密碼編譯密鑰相關聯。

【0111】 第一指令碼可進一步指定簽名散列類型。另外或替代地，欄位值之集合可至少部分地基於簽名散列類型。

【0112】 簽名散列類型可係指示第一交易之欄位值之集合中的哪些欄位值待包括於簽名中的值。

【0113】 第二指令碼可係強加用於驗證第一交易之條件之集合的鎖定指令碼。另外或替代地，鎖定指令碼之執行可使節點藉由判定條件之集合是否已滿足來驗證第一交易。

【0114】 第一指令碼可係用於符合第二指令碼之條件之集合的解除鎖定指令碼。

【0115】 驗證第一交易可使得傳送未用交易輸出。

【0116】 節點可係以通信方式耦接至區塊鏈網路中之至少一個其他節點的計算裝置。

【0117】 區塊鏈網路可由運行區塊鏈協定之執行個體的分散式電子裝置組成。

【0118】 第一指令碼及第二指令碼可使用圖靈不完整指令集加以編寫。

【0119】 第一指令碼及第二指令碼係使用圖靈完整指令集加以編寫。

【0120】 藉由包括欄位之集合，作為執行第一指令碼之結果，第一指令碼可使節點可將欄位之集合用作第二指令碼之輸入。

【0121】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0122】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0123】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之方法(及對應系統)。該方法可描述為區塊鏈資料約束方法。該方法可包括：i)在區塊鏈網路中之節點處接收第一交易以驗證，第一交易包括第一指

令碼，作為被執行之結果，該第一指令碼使節點至少：獲得對應於第一交易之欄位值之第一集合；及獲得對應於特定交易之欄位值之第二集合；ii) 獲得第二交易，第二交易已經驗證且包括第二指令碼，作為被執行之結果，該第二指令碼使節點至少：獲得作為執行第一指令碼之結果而供應的欄位值之第一集合及特定交易之欄位值之第二集合；自欄位值之第一集合提取交易識別符；及至少部分地基於欄位值之第二集合而判定特定交易對應於交易識別符；及 iii) 藉由執行第一指令碼及第二指令碼來驗證第一交易。

【0124】 欄位值之第二集合可呈規範化格式。

【0125】 節點可藉由產生欄位值之第二集合的散列來判定特定交易對應於交易識別符。另外或替代地，節點可藉由證實散列匹配交易識別符來判定特定交易對應於交易識別符。

【0126】 特定交易可與作為驗證第一交易之結果而傳送的數位資產之控制相關聯。

【0127】 特定交易可與不同於作為驗證第一交易之結果而傳送的數位資產的第二數位資產相關聯。

【0128】 驗證第一交易可成功而無需證實建立第一交易之實體可存取秘密資訊。

【0129】 節點可係區塊鏈網路之驗證節點。

【0130】 作為第一交易之成功驗證的結果，驗證第一交易可進一步包括將第一交易新增至區塊鏈網路中之區塊鏈。

【0131】 第二指令碼可係強加用於驗證第一交易之條件之集合的鎖定指令碼。另外或替代地，鎖定指令碼之執行可使節點藉由判定條件之集合是否已滿足來驗證第一交易。

【0132】 第一指令碼可係用於符合第二指令碼之條件之集合的解除

鎖定指令碼。

【0133】 第一指令碼可指定簽名散列類型。另外或替代地，作為被執行之結果，第二指令碼可進一步使節點獲得作為執行第一指令碼之結果而供應的簽名散列類型。

【0134】 作為被執行之結果，第二指令碼可進一步使節點至少部分地基於簽名散列類型而判定特定交易係與第一交易相關聯之交易之集合的成員。

【0135】 作為被執行之結果，第二指令碼可進一步使節點至少部分地基於簽名散列類型而判定特定交易對應於第二交易。

【0136】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0137】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0138】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之方法(及對應系統)。該方法可描述為區塊鏈資料約束方法。該方法可包括：i)在區塊鏈網路中之節點處接收第一交易以驗證，第一交易包括第一指令碼，該第一指令碼至少包括：第一值，該第一值之至少一部分包括不受第二指令碼約束之資料；及第二值；ii)獲得第二交易，第二交易已經驗證且包括第二指令碼，作為被執行之結果，該第二指令碼使節點至少：獲得作為執行第一指令碼之結果的第一值及第二值；及至少部分地基於第一值及第二值而驗證資料與特定源相關聯；及 iii)藉由執行第一指令碼及第二指令碼來驗證第一交易。

【0139】 第二指令碼可係包括用於驗證第二交易之條件之集合的鎖定指令碼。另外或替代地，第一指令碼可係用於符合鎖定指令碼之條件之集合的解除鎖定指令碼。

【0140】 驗證第一交易可經執行而無需證實建立第一交易之實體可存取秘密資訊。

【0141】 資料與資料源相關聯之不成功驗證可使得驗證第一交易不成功。

【0142】 特定源之身分可不受第二指令碼約束。

【0143】 特定交易可係特定資料源。另外或替代地，第一值可係特定交易之欄位值之集合。另外或替代地，第二值可包括與特定交易相關聯之交易識別符。作為被執行之結果，第二指令碼可藉由驗證特定交易對應於交易識別符來驗證資料與資料源相關聯。

【0144】 作為被執行之結果，第二指令碼可藉由驗證交易識別符匹配特定交易之欄位之集合的散列來驗證資料對應於交易識別符。

【0145】 藉由包括特定交易之欄位之集合，作為執行第一指令碼之結果，第一指令碼可使節點可將特定交易之欄位之集合用作第二指令碼之輸入。

【0146】 特定交易可係第二交易。

【0147】 資料可編碼於特定交易之欄位中。

【0148】 第二指令碼可約束特定源之身分。

【0149】 第二值可係簽名。另外或替代地，第二指令碼可進一步使節點獲得與資料源相關聯之公用密鑰，且另外或替代地，至少部分地基於公用密鑰及資料而產生經修改之公用密鑰。另外或替代地，作為被執行之結果，第二指令碼可至少部分地基於經修改之公用密鑰而驗證資料與資料源

相關聯。

【0150】 經修改之公用密鑰可藉由對公用密鑰與資料之值執行橢圓曲線點乘法來產生。

【0151】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0152】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0153】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之方法(及對應系統)。該方法可描述為區塊鏈資料約束方法。該方法可包括：i)在區塊鏈網路中之節點處接收第一交易以驗證，第一交易包括第一指令碼，作為被執行之結果，該第一指令碼使節點至少獲得資料及第一交易之欄位值之第一集合；ii)獲得第二交易，第二交易包括第二指令碼，作為被執行之結果，該第二指令碼使節點至少：至少部分地基於作為執行第一指令碼之結果而供應之資料而判定約束之集合；及至少部分地基於欄位值之第一集合而證實針對第一交易之約束之集合；及 iii)作為執行第一指令碼及第二指令碼之結果而根據約束之集合驗證第一交易。

【0154】 驗證第一交易可經執行而無需證實建立第一交易之實體可存取秘密資訊。

【0155】 資料源之身分可不受第二指令碼約束。

【0156】 第二指令碼可約束資料源之身分。

【0157】 第二指令碼可包括可用以驗證資料之特定資料源的公用密鑰。

【0158】 驗證資料可包括至少部分地基於公用密鑰及資料而產生經修改之公用密鑰，及另外或替代地，至少部分地基於經修改之公用密鑰而判定資料與資料源相關聯。

【0159】 約束之集合可至少部分地自資料中之參數集導出。

【0160】 約束之集合的滿足可係用於重新關聯數位資產之至少一部分的條件。

【0161】 驗證第一交易可包括使來自第一實體之數位資產重新關聯至第二實體。

【0162】 約束之集合可進一步使數位資產之至少部分與第三實體重新關聯。

【0163】 第二實體之身分可至少部分地基於約束之集合而加以判定。

【0164】 資料源可係第二交易。另外或替代地，資料包括第二交易之欄位值之第二集合。另外或替代地，第二指令碼之執行可使約束之集合至少部分地自欄位值之第二集合導出。

【0165】 第二實體之身分可至少部分地基於約束之集合而加以判定。

【0166】 約束之集合可進一步使數位資產之至少一部分與第三實體重新關聯。

【0167】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0168】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0169】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定

義之方法(及對應系統)。該方法可描述為區塊鏈資料約束方法。該方法可包括：i)在區塊鏈網路中之節點處接收第一交易以驗證，第一交易包括第一指令碼，作為被執行之結果，該第一指令碼使節點至少：獲得第一交易之欄位值之第一集合，欄位值之第一集合包括第三指令碼；及獲得第二交易之欄位值之第二集合，欄位值之第二集合包括第二指令碼之複本；ii)獲得第二交易，第二交易包括第二指令碼，作為被執行之結果，該第二指令碼使節點作為判定終止條件未滿足之結果而至少：自欄位值之第一集合獲得第三指令碼；及判定第二指令碼之複本匹配第三指令碼；及 iii)作為執行第一指令碼及第二指令碼之結果而驗證第一交易。

【0170】 第一指令碼可係用於符合第二指令碼之條件之集合的解除鎖定指令碼。

【0171】 第二指令碼可係強加用於驗證第一交易之條件之集合的鎖定指令碼。

【0172】 第三指令碼可係強加用於驗證未來交易之條件之集合的鎖定指令碼。

【0173】 第二交易可係與數位資產相關聯之交易。另外或替代地，第一交易可係使來自第一實體之數位資產之至少部分重新關聯至第二實體的交易。

【0174】 驗證第一交易可包括使來自第一實體之數位資產重新關聯至第二實體。

【0175】 判定終止條件未滿足可包括判定與第二交易相關聯之數位資產的量足以重新關聯數位資產之至少一部分。

【0176】 第三指令碼可嵌入於欄位值之第一集合中的欄位值中。

【0177】 區塊鏈網路可由運行區塊鏈協定之執行個體的分散式電子

裝置組成。

【0178】 驗證第一交易可經執行而無需證實建立第一交易之實體可存取秘密資訊。

【0179】 作為用於驗證第一交易之另一條件，第二指令碼可進一步使節點證實第一交易滿足額外約束。

【0180】 第一交易及第二交易可係與數位資產相關聯之重複智慧型合約之集合的成員。

【0181】 重複智慧型合約之集合可藉由終止條件來終止。

【0182】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所主張之方法中之任一者。

【0183】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【0184】 因此，根據本發明，可提供一種如隨附申請專利範圍中所定義之方法(及對應系統)。該方法可描述為區塊鏈資料約束方法。該方法可包括：i)在區塊鏈網路中之節點處接收第一交易以驗證，第一交易包括第一指令碼，作為被執行之結果，該第一指令碼使節點至少獲得第一交易之欄位值之第一集合、第二交易之欄位值之第二集合以及輸入；ii)獲得第二交易，第二交易包括第二指令碼，該第二指令碼包括規則之集合，作為被執行之結果，該第二指令碼使節點至少：證實第二指令碼匹配嵌入於欄位值之第一集合中的第三指令碼；至少部分地基於欄位值之第二集合而判定當前狀態；及至少部分地基於當前狀態、輸入及規則之集合而判定下一狀態；證實下一狀態包括於欄位值之第一集合中；及 iii)作為執行第一指令碼及第二

指令碼之結果而驗證第一交易。

【0185】 第二指令碼可約束輸入源之身分。

【0186】 如所主張之方法中之任一者可進一步包含證實輸入源之密碼編譯秘密。

【0187】 規則之集合可係狀態轉移矩陣。

【0188】 第三指令碼可係強加用於驗證未來交易之條件之集合的鎖定指令碼。

【0189】 第二指令碼可進一步使節點判定終止條件未滿足。

【0190】 輸入可嵌入於欄位值之第二集合中。

【0191】 終止條件可係與第二交易相關聯之數位資產的大小不足以被傳送。

【0192】 驗證第一交易可包括使來自第一實體之數位資產重新關聯至第二實體。

【0193】 當前狀態可指示第二交易之狀態。

【0194】 下一狀態可指示第一交易在驗證後之狀態。

【0195】 如所主張之方法中之任一者可進一步包含接收第三交易。另外或替代地，如所主張之方法中之任一者可進一步包含自第一交易獲得第四指令碼，作為被執行之結果，該第四指令碼使節點至少部分地基於下一狀態、第二輸入及規則之集合而判定不同於下一狀態及當前狀態之另一狀態。

【0196】 當前狀態及下一狀態可係第一交易及第二交易之可能狀態之集合的成員。

【0197】 亦需要提供一種系統，其包含：處理器；及記憶體，其包括可執行指令，作為由處理器執行之結果，該等可執行指令使系統執行如所

主張之方法中之任一者。

【0198】 亦需要提供一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由電腦系統之處理器執行之結果，該等可執行指令使電腦系統至少執行如所主張之方法中之任一者。

【圖式簡單說明】

【0199】

圖 1 說明可實施各種實施例之區塊鏈環境；

圖 2 說明根據實施例之去信任確定性狀態機之實例；

圖 3 說明由實施例解決之與鎖定指令碼相關聯的問題之實例；

圖 4 說明根據實施例之可由解除鎖定指令碼存取的資料之實例；

圖 5 說明根據實施例之自交易欄位之經序列化集合產生簽名的實例；

圖 6 係說明根據實施例之使得插入解除鎖定交易欄位之經序列化集合的實例的流程圖；

圖 7 說明由實施例解決之與鎖定指令碼相關聯的問題之實例；

圖 8 說明根據實施例之使得插入經序列化先前交易的實例；

圖 9 說明根據實施例之取決於簽名散列類型而可用的欄位之集合的實例；

圖 10 說明根據實施例之自經序列化交易提取交易識別符的實例；

圖 11 係說明根據實施例之使得插入經序列化先前交易的實例之流程圖；

圖 12 說明根據實施例之來自未判定源之未判定資料的不安全佈建的實例；

圖 13 說明根據實施例之來自經判定源之未判定資料的安全佈建的實例；

圖 14 說明根據實施例之來自未判定源之未判定資料安全佈建至鎖定指令碼中的實例；

圖 15 係說明根據實施例之未判定資料安全佈建至鎖定指令碼中的實例之流程圖；

圖 16 說明根據實施例之經參數化智慧型合約的實例；

圖 17 係說明根據實施例之經參數化智慧型合約之執行的實例之流程圖；

圖 18 說明由實施例解決之智慧型合約複製問題的實例；

圖 19 說明根據實施例之智慧型合約複製問題之解決方案的實例；

圖 20 說明根據實施例解決之智慧型合約複製問題的另一實例；

圖 21 說明根據實施例之自我複寫智慧型合約的實例；

圖 22 係說明根據實施例之具有終止條件的自我複寫智慧型合約之實例的流程圖；

圖 23 說明根據實施例解決之下一狀態判定問題的實例；

圖 24 說明根據實施例之去信任確定性狀態機之實例；

圖 25 係說明根據實施例之去信任確定性狀態機之實例的流程圖；及

圖 26 說明可實施各種實施例之計算環境。

【實施方式】

【0200】 首先將參看圖 1，其說明根據本發明之實施例的與區塊鏈相關聯之實例區塊鏈網路 100。在該實施例中，實例區塊鏈網路 100 係由運行區塊鏈協定之執行個體的同級間分散式電子裝置組成。在一些實例中，該等分散式電子裝置被稱作節點 102。區塊鏈協定之實例係比特幣協定。

【0201】 節點 102 可由任何合適的計算裝置組成(例如，藉由資料中心中之伺服器、藉由用戶端計算裝置(例如，桌上型電腦、膝上型電腦、平

板電腦、智慧型手機等)、藉由計算資源服務提供者之分散式系統中的多個計算裝置或藉由任何合適的電子用戶端裝置,諸如圖 26 之計算裝置 2600)。

【0202】 在一實施例中,節點 102 中之一或多者係以通信方式耦接至節點 102 中之一或多個其他者。此通信耦接可包括有線或無線通信中之一或多者。在該實施例中,節點 102 各自維護區塊鏈中之所有交易的「總帳」之至少一部分。以此方式,總帳係分散式總帳。影響總帳之由節點處理的交易可藉由其他節點中之一或多者證實使得維持總帳之完整性。

【0203】 在一實施例中,節點 102 中之至少一些係執行諸如解決密碼編譯問題之複雜計算的挖掘者節點。解決密碼編譯問題之挖掘者節點建立用於區塊鏈之新區塊且將新區塊廣播至其他節點 102。其他節點 102 證實挖掘者節點之工作,且在證實後將區塊接受至區塊鏈中(例如,藉由將區塊新增至區塊鏈之分散式總帳)。在一些實例中,區塊係常常用時戳及先前區塊之「指紋」(例如,散列)進行標記的交易之群組。以此方式,每一區塊變為鏈接至先前區塊,藉此建立鏈接區塊鏈中之區塊的「鏈」。在實施例中,藉由節點 102 之共識將有效區塊新增至區塊鏈。亦在一些實例中,區塊鏈包含經驗證區塊之清單。

【0204】 在一實施例中,節點 102 中之至少一些作為驗證如本發明中所描述之交易的驗證節點而操作。在一些實例中,交易包括提供數位資產(例如,數個比特幣)之所有權之證明的資料及用於接受或傳送數位資產之所有權或控制的條件。在一些實例中,「解除鎖定交易」係指將由先前交易之未用交易輸出(UTXO)指示的數位資產之至少一部分重新關聯(例如,傳送所有權或控制)至與區塊鏈位址相關聯之實體的交易。在一些實例中,「先前交易」係指含有正由解除鎖定交易參考之 UTXO 的交易。在一些實施例中,交易包括「鎖定指令碼」,其使交易負擔有在可傳送(「解除鎖定」)所有權或控

制之前必須滿足的條件。在一些實施例中，區塊鏈位址係與實體相關聯之文數字字元串，數位資產之至少一部分的控制經傳送或重新關聯至該實體。在實施於一些實施例中之一些區塊鏈協定中，相關聯於實體之公用密鑰與區塊鏈位址之間存在一對一對應關係。交易之驗證可涉及驗證在鎖定指令碼或解除鎖定指令碼中指定之一或多個條件。在成功驗證交易 104 後，驗證節點將交易 104 新增至區塊鏈且將其分散至節點 102。

【0205】 圖 2 說明本發明之實例實施例 200。具體而言，圖 2 描繪編碼第一狀態 206 之先前區塊鏈交易 202 及編碼第二狀態 208 之解除鎖定區塊鏈交易 204。在實例實施例 200 中，在第一時間之第一狀態 206 表示為嵌入於先前區塊鏈交易 202 中之參數。關於參數化約束之其他細節見於圖 16 之描述中。解除鎖定區塊鏈交易 204 將包括表示第二狀態 208 之參數。

【0206】 在實例實施例 200 中，先前區塊鏈交易 202 及解除鎖定區塊鏈交易 204 係含有一或多個輸入及一或多個輸出之欄位值的集合。在一些實施例中，該等輸入及輸出反映將來自至少一個實體之數位資產之至少一部分重新關聯至至少另一實體的意圖。在實例實施例 200 中，先前區塊鏈交易 202 係包括於區塊鏈中之最新的經確認交易。在實例實施例 200 中，解除鎖定區塊鏈交易 204 係尚待確認且尚未包括於區塊鏈中之最接近的未來交易。解除鎖定區塊鏈交易 204 之輸入中之每一者接收先前區塊鏈交易 202 之輸出。

【0207】 如比特幣之一些區塊鏈技術將橢圓曲線數位簽名演算法 (ECDSA) 用作用於數位簽名之數學方案。在實施例中，ECDSA 係用以保證 UTXO 不被未經批准之實體獲得的密碼編譯數位簽名。比特幣中之橢圓曲線數位簽名 (ECDS) 通常呈現為具有附加至末尾之簽名散列旗標 (SIGHASH 類型)；然而，預期本發明之技術可與不實施 SIGHASH 類型之區塊鏈技術

一起使用。在此等區塊鏈技術中，預期 ECDS 符合特定區塊鏈技術之簽名產生原理。

【0208】 在實施例中，SIGHASH 類型係指在經序列化(例如，規範化)及散列之前待自交易提取的欄位之集合。舉例而言，SIGHASH 類型可影響交易之哪些欄位包括於簽名中。在一些實例中，SIGHASH 類型可係 SIGHASH_ALL 、 SIGHASH_NONE 、 SIGHASH_SINGLE 或 SIGHASH_ANYONECANPAY 中之一或多者。在一實施例中，類型 SIGHASH_ALL 指示除輸入指令碼外，交易中待散列及簽名之所有欄位。在一實施例中，類型 SIGHASH_NONE 指示輸出無需被簽名，其可允許其他者更新交易。在一實施例中，類型 SIGHASH_SINGLE 指示輸入經簽名但序號空白，因此其他者可建立交易之新版本，但僅經簽名之輸出係與輸入在相同位置處之輸出。在一實施例中，類型 SIGHASH_ANYONECANPAY 與其他類型組合且指示包括 SIGHASH_ANYONECANPAY 之輸入經簽名，但其他輸入無需被簽名。SIGHASH 類型可由指示 SIGHASH 類型之值表示。舉例而言，在一些實施中，SIGHASH_ALL 由具有值 1 之位元組表示，SIGHASH_NONE 由具有值 2 之位元組表示，SIGHASH_SINGLE 由具有值 3 之位元組表示，且 SIGHASH_ANYONECANPAY 由具有值 80 之位元組表示。在一些實施中，組合 SIGHASH 類型係藉由將位元組值加在一起來執行。

【0209】 在一些實例中，由 SIGHASH 類型判定之交易欄位之集合係指以位元組編碼之對應交易的如由 SIGHASH 類型判定之子集。舉例而言，在 SIGHASH 類型 SIGHASH_ANYONECANPAY 之情況下，僅一個交易輸入包括於簽名內。

【0210】 在一實施例中，ECDS 係由以可區別編碼規則(distinguished encoding rule ; DER)格式編碼之一對 256 位元數字(r, s)表示。然而應注意，

本發明之技術可與諸如基本編碼規則(BER)或規範編碼規則(CER)之其他編碼格式一起使用。用於 ECDSA 中之參數包括 K (具有座標 (x, y) 之橢圓曲線點)、 k (256 位元數字；通常隨機以保護私用密鑰)、 G (具有階數 n : $n \times G = 0$ 之橢圓曲線上的基點，其中 0 表示恆等橢圓曲線點)， n 係用作橢圓曲線有限域中之參數的大的質數， r (ECDS 中之 256 位元數字中之一者)、 s (簽名中之 256 位元數字中之另一者)、 k^{-1} (k 之模組化乘法逆元素；亦即， $k^{-1}k \equiv 1 \pmod n$)、 m (經簽名之訊息或資料；在實施例中，其藉由散列函數重新設定大小為 256 個位元)、 a (私用密鑰；例如 256 位元數字)。在實施例中，如下產生 ECDS。

【0211】 首先，藉由將 k 與產生器相乘來判定橢圓曲線點 K ：

$$K = k \times G$$

【0212】 接著，自 K 判定點 x ，且根據下式判定 ECDS 中之 256 位元數字中的第一者 r ：

$$r = x \pmod n$$

【0213】 接著，根據下式判定 ECDS 中之 256 位元數字中的第二者 s ：

$$s = k^{-1} (m + r \times a) \pmod n$$

【0214】 最後，以 DER 格式編碼 (r, s) 。給定簽名 (r, s) 、訊息或資料 m 及對應於私用密鑰 a 之公用密鑰 A ，可證實簽名。為證實簽名，計算 $v = s^{-1} \times (m \times G + r \times y)$ 。若 $v = r$ ，則簽名有效。

【0215】 比特幣使用被稱作「指令碼(Script)」之指令碼處理系統。在本發明中，參考各種指令碼操作碼及關鍵字以用於執行各種操作。然而，預期其他區塊鏈技術可實施不同的指令集，且因此描述於本發明中之操作碼被視為說明由操作碼而非指令碼中之特定操作碼執行的操作。在一些實施例中，指令碼處理系統係圖靈(Turing)不完整指令集(例如，不支援迴圈、

遞迴、轉到陳述式等)。在其他實施例中，指令碼處理系統係圖靈完整指令集。

【0216】 本發明之某些實施例在如下假設下操作：指令碼處理系統或用於實施所描述之指令集的其他系統允許單一指令碼中具有多於 200 個指令(例如，操作碼)。同樣地，本發明之某些實施例進一步假設：

在執行操作碼指令碼或指令集之系統中存在及啟用由在本發明中參考之操作碼所提供的功能性；

所需功能性可藉由建立經編寫以提供所要行為之自訂函式來實施。此等自訂函式可經編寫以實施 `op_codes` 之功能性，`op_codes` 存在於語言中但已被停用，或可係提供本身不在指令碼處理語言自身中提供之特定功能性的「新」`op_codes`。

【0217】 本發明中所參考之操作碼之實例包括：

`OP_ECPX`，其傳回橢圓曲線點之 `x` 座標

`OP_ADD`，其將堆疊上之頂部兩個項目相加

`OP_BIGMOD`，其傳回在將堆疊上之頂部兩個項目相除之後的餘數

`OP_BIGMODADD`，其執行堆疊之頂部兩個項目模堆疊之第三項目的模數加法

`OP_BIGMODINVERSE`，其執行模數負指數運算

`OP_BIGMODMUL`，其執行堆疊之頂部兩個項目模堆疊之第三項目的模數乘法

`OP_CAT`，其串連堆疊上之頂部兩個項目

`OP_CHECKSIG`，其中公用密鑰及簽名自堆疊彈出且對照根據 `SIGHASH` 類型之交易欄位之簽名進行證實。若簽名有效，則傳回 1，否則傳回 0。

OP_CHECKSIGVERIFY，其與 OP_CHECKSIG 起相同作用，但 OP_VERIFY 在之後被執行。

OP_DERENCODE，其以 DER 格式編碼堆疊上之頂部兩個項目

OP_DUP，其複製頂部堆疊項目

OP_ECPMULT，其執行堆疊上之頂部兩個項目的橢圓曲線點乘法(亦被稱作橢圓曲線純量乘法)

OP_ELSE，若未執行先前 OP_IF 或 OP_NOTIF 或 OP_ELSE，則執行此等陳述式；否則，若已執行先前 OP_IF 或 OP_NOTIF 或 OP_ELSE，則不執行此等陳述式

OP_ENDIF，其結束 if/else 區塊

OP_EQUAL，若輸入完全相等，則傳回 1，否則傳回 0

OP_EQUALVERIFY，其與 OP_EQUAL 相同，但之後運行 OP_VERIFY

OP_FROMALTSTACK，其將輸入置於主堆疊之頂部上且將輸入自替代堆疊移除

OP_HASH256，其中輸入經散列兩次：第一次用 SHA-256 且接著用 RIPEMD-160

OP_IF，若頂部堆疊值並非假，則執行陳述式且移除頂部堆疊值

OP_MUL，其將堆疊上之頂部兩個項目相乘

OP_NOTIF，若頂部堆疊值係假，則執行陳述式且移除頂部堆疊值

OP_ROLL，其中將堆疊中深至 n 個項目之項目移動至頂部

OP_SUBSTR，其傳回字串區段

OP_SWAP，其中調換堆疊上之頂部兩個項目

OP_TOALTSTACK，其將輸入置於替代堆疊之頂部上且將輸入自主堆疊移除

OP_VERIFY，其在頂部堆疊值並非真之情況下將交易標記為無效

【0218】 在一實施例中，可使用操作碼建立 ECDS 產生指令碼，其可藉由將 SIGHASH 位元組附加至末尾而擴展以建立簽名產生指令碼 OP_GENSIG。

表 1：

類型	指令碼
輸入	<SIGHASH Byte><m><a><k>
OP_GENSIG	// $K = k \times G$ OP_DUP OP_TOALTSTACK <PubK G> OP_ECPMULT // $r = x \bmod n$ OP_ECPX <N> OP_BIGMOD OP_DUP OP_TOALTSTACK // $k^{-1}(r \times d + m) \bmod n$ <N> OP_BIGMODMUL <N> OP_BIGMODADD OP_FROMALTSTACK OP_SWAP OP_FROMALTSTACK <N> OP_BIGMODINVERSE <N> OP_BIGMODMUL //DER 編碼(r,s)且附加 SIGHASH 類型 OP_DERENCODE OP_SWAP OP_CAT

【0219】 在以上指令碼中，將<SIGHASH Byte>、訊息<m>、私用密鑰<a>及數字<k>按以上次序輸入至主(後入先出)堆疊中。執行指令碼操作「OP_DUP OP_TOALTSTACK <PubK G> OP_ECPMULT」使得將數字<k>複製至替代堆疊，且<k>與橢圓曲線產生器<PubK G>相乘以在主堆疊之頂部產生橢圓曲線點 K 。執行指令碼操作「OP_ECPX <N> OP_BIGMOD OP_DUP OP_TOALTSTACK」使得自 K 之 x 座標模 n 來計算 r 。將 r 之複本推入至替代堆疊。執行指令碼操作「<N> OP_BIGMODMUL <N> OP_BIGMODADD OP_FROMALTSTACK OP_SWAP OP_FROMALTSTACK OP_SWAP

OP_FROMALTSTACK <N> OP_BIGMODINVERSE <N>
 OP_BIGMODMUL」計算 $s = k^{-1} (m + r \times a) \bmod n$ 。最後，執行指令碼
 操作「OP_DERENCODE OP_SWAP OP_CAT」使得以 DER 格式編碼 r 及 s 且
 與<SIGHASH Byte>串連。在本發明中，此指令碼被稱作 OP_GENSIG。因
 此，在本發明之實施例中對 OP_GENSIG 的參考應被視為在以上指令碼中
 執行之操作的速記。

【0220】 圖 3 係說明由本發明之實施例解決的與區塊鏈交易相關聯
 之問題的實例 300。亦即，在圖 3 中所說明之實例 300 實施例中，先前交易
 302 中之鎖定指令碼 306 不能直接讀取解除鎖定交易 304 之欄位。如所提
 到，在一些實施例中，先前交易 302 係包括於區塊鏈中之最新的經確認交
 易。同樣地，在一些實施例中，解除鎖定交易 304 係尚待確認且尚未包括
 於區塊鏈中之未來交易，其表示試圖重新關聯由先前交易 302 控制之數位
 資產之至少一部分。

【0221】 如上文所提到，在一些實施例中，鎖定指令碼 306 係藉由指
 定需要滿足以便傳送輸出之條件來負擔交易的指令碼。更特定而言，作為
 藉由區塊鏈系統之驗證節點執行的結果，執行鎖定指令碼 306 經組態以接
 受來自經執行解除鎖定指令碼之資料，且基於該資料執行某些操作並傳回
 指示解除鎖定指令碼之執行是否成功地「解除鎖定」該鎖定指令碼(亦即，
 滿足設定於鎖定指令碼內之條件集合)的結果。在一些實施例中，鎖定指令
 碼 306 定義必須符合(例如，由經由解除鎖定指令碼提供之資料)以使交易驗
 證成功之一或多個資料約束。舉例而言，鎖定指令碼 306 可需要某些資料
 提供於解除鎖定指令碼中以解除鎖定先前交易 302 之相關聯數位資產。

【0222】 圖 4 描繪實例 400，其說明不同於先前交易 402 之鎖定指令
 碼 406，本發明之解除鎖定指令碼 408 在一實施例中可存取解除鎖定交易

404 之欄位(例如，根據 SIGHASH 類型判定之解除鎖定交易欄位之集合)。在一些實施例中，先前交易 402 類似於圖 3 之先前交易 302。在一些實施例中，解除鎖定交易 404 類似於解除鎖定交易 304。在一些實施例中，鎖定指令碼 406 具有類似於圖 3 之鎖定指令碼 306 的特性。

【0223】 在一些實施例中，解除鎖定指令碼 408 係置放於交易之輸入上的可執行指令碼，該等輸入試圖符合藉由鎖定指令碼置放於交易之輸出上的條件之集合。解除鎖定指令碼亦稱為「scriptSig」。如上文所提到，解除鎖定指令碼 408 已經設計以提供根據 SIGHASH 類型判定之解除鎖定交易欄位之集合作為鎖定指令碼之輸入，藉此使鎖定指令碼能夠存取解除鎖定交易之欄位。關於經序列化交易之內容及構造的其他細節可見於下文圖 5 之描述中。應注意，在實施例中，先前交易 402 及解除鎖定交易 404 包含額外欄位。舉例而言，在一些實施例中，「nVersion」係指區塊鏈協定版本，「#vin」係指交易之輸入數目的計數，「hash」係指實體之支付公用密鑰散列，數位資產係自該實體重新關聯，「#vout」係指交易之輸出數目的計數，「nValue」係指剩餘的未用數位資產之量，且「nLockTime」係指交易成為最終時的時戳。

【0224】 圖 5 說明交易欄位之經序列化集合如何形成的實例 500。如圖 5 中所說明，經序列化交易 510 (亦即，以特定格式之一系列位元組表示的交易)包含交易之欄位值之集合。在步驟 512 中，簽名人選擇 SIGHASH 類型及數字 k 。數字 k 通常係隨機或偽隨機數以便遮罩或保護私用密鑰且因此在本發明中有時被稱作「遮罩數字(mask number)」。交易之經修改複本 514 係經序列化交易 510 之根據指定 SIGHASH 類型(例如，在實例 500 中係 SIGHASH_NONE+ANYONECANPAY)選擇的欄位之集合的實例。簽名人將交易之經修改複本 514 進行散列(例如，執行雙 SHA-256 散列)，其產生訊

息 m 516。簽名人接著使用 SIGHASH 類型、訊息 m 、簽名人之私用密鑰及數字 k 諸如以上文結合圖 2 所描述之方式來產生簽名。

【0225】 下表說明典型的解除鎖定及解除鎖定指令碼之實例，由此使用 OP_CHECKSIG 操作碼對照實體 A 之公用密鑰檢查在解除鎖定指令碼中指定之實體 A 的所假設簽名。

表 2：

解除鎖定指令碼	鎖定指令碼
<Sig A>	<PubK A> OP_CHECKSIG

【0226】 因此，在理解圖 5 之簽名產生的情況下，下表說明在實例 500 中所說明之程序之部分移至解除鎖定指令碼內的情況下解除鎖定及鎖定指令碼之實例。

表 3：

解除鎖定指令碼	鎖定指令碼
<SIGHASH Type>< m >< a >< k > OP_GENSIG	<PubK A> OP_CHECKSIG

【0227】 可進一步修改解除鎖定指令碼以在解除鎖定指令碼中包括計算訊息 m 之步驟。

【0228】 表 4：

解除鎖定指令碼	鎖定指令碼
<SIGHASH Type>< Serialized Set of Unlocking Tx Fields> OP_HASH256 < a >< k > OP_GENSIG	<PubK A> OP_CHECKSIG

【0229】 然而應注意，除 SIGHASH 類型及根據 SIGHASH 類型判定之解除鎖定交易欄位之集合外，程序之其他操作可移至鎖定指令碼。

表 5：

解除鎖定指令碼	鎖定指令碼
<SIGHASH Type><Serialized Set of Unlocking Tx Fields>	OP_HASH256 <a><k> OP_GENSIG <PubK A> OP_CHECKSIG

【0230】 因此，藉由將操作「OP_HASH256 <a><k> OP_GENSIG」移至鎖定指令碼內部，使解除鎖定指令碼含有 SIGHASH 類型及根據 SIGHASH 類型判定之解除鎖定交易欄位之集合以便為有效的。

【0231】 以此方式，使得將經序列化先前交易插入至鎖定指令碼中。下表說明鎖定指令碼及解除鎖定指令碼如何執行實例 500 之每一步驟程序且驗證交易。

表 6：

解除鎖定指令碼	鎖定指令碼
<SIGHASH Type> <Serialized Set of Unlocking Tx Fields>	//對訊息進行雙 SHA256 OP_HASH256 //使用 SIGHASH 類型、訊息、私用密鑰及 k 產生簽名 <a><k> OP_GENSIG //執行簽名證實 <PubK A> OP_CHECKSIG

【0232】 在本發明中，以上指令碼可被稱作 OP_UNLOCKINGTXINJECTION。因此，在本發明之實施例中對 OP_UNLOCKINGTXINJECTION 之參考應被視為在以上指令碼中執行之操作的速記。然而應注意，提供 SIGHASH 類型及根據 SIGHASH 類型判定之解除鎖定交易欄位之集合的任何實體可接收交易輸出。然而，此成為如下文進一步詳細描述之有用特徵。如上文所提到，在一些實例中，接收交易

輸出係指建立解除鎖定交易，該解除鎖定交易參考交易輸出且將評估為有效，其將藉此使得接收交易輸出。

【0233】 圖 6 係說明根據各種實施例之用於根據實施例使得插入根據 SIGHASH 類型判定之解除鎖定交易欄位之集合的處理程序 600 之實例的流程圖。處理程序 600 (或所描述之任何其他處理程序，或彼等處理程序之變化或組合)中之一些或全部可在經組態有可執行指令或其他資料之一或多個電腦系統的控制下執行，且可實施為共同地在一或多個處理器上執行之可執行指令。可執行指令或其他資料可儲存於非暫時性電腦可讀儲存媒體上(例如，永久地儲存於磁性、光學或快閃記憶體媒體上之電腦程式)。

【0234】 舉例而言，處理程序 600 中之一些或全部可藉由區塊鏈網路(諸如，圖 1 之實例區塊鏈網路 100)中之驗證節點執行。此驗證節點可由任何合適的計算裝置組成(例如，藉由資料中心中之伺服器、藉由用戶端計算裝置、藉由計算資源服務提供者之分散式系統中的多個計算裝置或藉由任何合適的電子用戶端裝置，諸如圖 26 之計算裝置 2600)。處理程序 600 包括一系列步驟，其中執行處理程序 600 之系統以圖 5 中所描述之方式聯合地執行未經驗證交易之解除鎖定指令碼及鎖定指令碼，且作為結果，獲得 SIGHASH 類型及交易欄位值之集合，產生簽名並驗證簽名。

【0235】 在步驟 602 中，系統自試圖重新關聯數位資產之至少一部分的實體獲得未經驗證交易。未經驗證交易包括鎖定指令碼及解除鎖定指令碼。解除鎖定指令碼係藉由系統在執行鎖定指令碼之前執行。解除鎖定指令碼可類似於上表 5 及表 6 中所展示之解除鎖定指令碼，且指定 SIGHASH 類型並包括未經驗證交易之欄位之經序列化集合。因此，在步驟 604 及步驟 606 中，執行處理程序 600 之系統自解除鎖定指令碼獲得 SIGHASH 類型及未經驗證交易之交易欄位值之經序列化集合，且將其置放於主堆疊中。

在成功完成解除鎖定指令碼之執行後，系統使用在完成解除鎖定指令碼之執行時主堆疊之狀態(且在一些實施中，替代堆疊之狀態)開始執行鎖定指令碼。鎖定指令碼可類似於上表 5 及表 6 中所展示之鎖定指令碼。

【0236】 在步驟 608 中，根據鎖定指令碼，系統至少使用作為執行解除鎖定指令碼之結果而置放於主堆疊上之 SIGHASH 類型及交易欄位值之集合以及與公用-私用密鑰對相關聯之私用密鑰來產生簽名。在步驟 610 中，根據鎖定指令碼，系統對照密鑰對之公用密鑰成功地驗證簽名。以此方式，使得交易欄位之集合藉由解除鎖定指令碼插入至鎖定指令碼中。應注意，步驟 602 至步驟 610 可取決於實施以各種次序及組合執行，且操作中的一些可與處理程序 600 之其他操作並列地執行。

【0237】 圖 7 係說明由本發明之實施例解決的與區塊鏈交易相關聯之問題的實例 700。亦即，在圖 7 中所說明之實例 700 中，鎖定指令碼 706 不能讀取其所嵌入之交易的輸入且因此不能直接讀取先前交易之欄位。在一些實施例中，交易 704 類似於圖 3 之解除鎖定交易 304，其表示試圖重新關聯由先前交易控制之數位資產之至少一部分。如上文所提到，在一些實施例中，類似於圖 3 之鎖定指令碼 306，鎖定指令碼 706 係藉由指定需要滿足以便傳送輸出之條件來負擔交易的指令碼。

【0238】 圖 8 說明藉由提取交易 ID 及執行約束檢查使解除鎖定指令碼 808 含有經串列化先前交易之實例 800。具體而言，圖 8 描繪解除鎖定交易 804，其具有利用來自先前交易 802A 至先前交易 802B 之輸出的解除鎖定指令碼 808。如可見，解除鎖定指令碼 808 使得擷取經串列化先前交易。在一些實例中，經串列化先前交易係指先前交易之欄位值之集合的未經修改版本。

【0239】 圖 8 中所描繪之實施例可藉由觀察到交易 ID 係經串列化交

易之雙 SHA-256 且交易 ID 與交易具有一對一映射來理解。因此，可藉由施加下表 7 中所展示之約束來使得將交易插入至解除鎖定指令碼中。

表 7：

解除鎖定指令碼	鎖定指令碼
<Serialized Tx>	OP_HASH256 <Tx ID> OP_EQUAL

【0240】 本發明之實施例藉由以下操作來進一步改良此插入：不僅僅使得插入任何經序列化交易，而且使得插入在解除鎖定交易 804 之輸入中參考的一或多個經序列化先前交易(例如，先前交易 802A 至先前交易 802B)。如上文參看圖 7 所描述，可經由解除鎖定指令碼 806 使得將根據 SIGHASH 類型判定之解除鎖定交易欄位之集合插入至鎖定指令碼中，且圖 9 說明取決於所指定之 SIGHASH 類型將哪些欄位包括於經序列化交易中。

【0241】 圖 9 說明取決於所指定之 SIGHASH 類型而可用於經序列化交易中的欄位之集合的實例 900。然而應注意，圖 9 僅為舉例且在各種實施例中，存在比圖 9 中所描繪更多的 SIGHASH 類型。如圖 9 中所展示，藉由不同 SIGHASH 類型，先前交易 ID 之不同集合包括於根據 SIGHASH 類型判定之解除鎖定交易欄位之集合中(應注意，「散列」欄位表示呈大在前排列法格式之交易 ID)。在一些實施例中，嵌入鎖定指令碼之先前交易之交易 ID 始終可用而不管指定哪一 SIGHASH 類型。

【0242】 因此，可使某些欄位存在於藉由以如下方式約束 SIGHASH 類型而判定之解除鎖定交易欄位之集合中：首先，複製 SIGHASH 類型。接下來，將 SIGHASH 類型推入至堆疊中(例如，SIGHASH_ALL)。最後，呼叫 OP_EQUALVERIFY。如圖 9 中可見，SIGHASH_ALL (如藉由解除鎖定交易 904A 所展示)包括如所提到表示先前交易 y 及 z 之交易 ID 的散列。相比而言，SIGHASH_ALL + ANYONECANPAY (如藉由解除鎖定交易 904B

所展示)僅包括緊接在前之交易 y 的散列。在一些實施例中，解除鎖定交易 904A 至解除鎖定交易 904B 類似於圖 3 之解除鎖定區塊鏈交易 204，其表示試圖重新關聯由先前交易(例如，交易 y 或 x)控制之數位資產之至少一部分。提取交易 ID 可藉由使用子串操作碼剖析經序列化交易直至達到所要欄位來實現，其說明於圖 10 中。

【0243】 圖 10 說明在本發明之實施例中的提取交易 ID 的實例 1000。具體而言，圖 10 說明由呈大在前排列法格式之交易 ID 組成之散列 1020 係可藉由使用指令碼內之子串操作碼提取的經序列化交易 1010 之子串。在一些實施例中，在可提取交易 ID 之前，首先剖析經序列化交易 1010 以識別散列 1020 之位置，此係因為一些欄位(例如，#vin、scriptSigLen、scriptSig、scriptPubKeyLen 及 scriptPubKey)具有可變位元組長度。然而，預期在欄位具有固定長度之實施中，剖析可能不必要。

【0244】 因此，在一些實施例中，藉由建置使得以參看圖 6 所描述之方式插入在解除鎖定交易中參考之特定經序列化先前交易的鎖定指令碼，可使得可存取先前交易 ID。舉例而言，首先判定 SIGHASH 類型約束，提取交易 ID 且複製經序列化先前交易並對照自欄位之解除鎖定交易經序列化集合提取(根據 SIGHASH 類型)的交易 ID 檢查經序列化先前交易。應注意，可執行此處理以使得插入多個不同的經序列化先前交易。作為一實例，表 8 呈現使得插入對應於解除鎖定交易之輸入 X 的先前交易的指令碼。

表 8：

解除鎖定指令碼	鎖定指令碼
<Serialized Previous Tx (for Tx ID X)> <SIGHASH Type> <Serialized Set of Unlocking Tx Fields>	<X> //下文的 OP_PREVTXINJECTION //將<X>推入至替代堆疊 OP_TOALTSTACK

	//使得插入解除鎖定 Tx (耗用 SIGHASH 類型) OP_SWAP OP_OVER OP_UNLOCKINGTXINJECTION OP_VERIFY //自解除鎖定 Tx 提取 Tx ID <X> OP_FROMALTSTACK OP_EXTRACTTXID //自經序列化先前 Tx 產生 Tx ID OP_SWAP OP_HASH256 //檢查 Tx ID 係相同的 OP_EQUAL
--	---

【0245】 在以上指令碼中，OP_EXTRACTXID 係獲取含有交易 ID 及交易 ID 位置之資料作為輸入且輸出所提取交易 ID 之操作碼或指令碼。在本發明中，以上指令碼可被稱作 OP_PREVTXINJECTION。因此，在本發明之實施例中對 OP_PREVTXINJECTION 之參考應被視為在以上指令碼中執行之操作的速記。

【0246】 然而應注意，提供 SIGHASH 類型、根據 SIGHASH 類型判定之解除鎖定交易欄位之集合及經序列化先前交易的任何實體可獲得交易輸出。然而，此成為如下文進一步詳細描述之有用特徵。

【0247】 作為另一實例，表 9 呈現使得插入對應於經簽名之輸入的先前交易的指令碼。

表 9：

解除鎖定指令碼	鎖定指令碼
<Serialized Previous Tx (for input being signed)>	//保存 SIGHASH 類型之複本 OP_OVER OP_TOALTSTACK

<SIGHASH Type> <Serialized Set of Unlocking Tx Fields>	//僅 1 個 Tx ID，其對應於此鎖定指令碼之先前 Tx <0> OP_PREVTXINJECTION OP_VERIFY //確保 SIGHASH 類型係 SIGHASH_X ANYONECANPAY OP_FROMALTSTACK <SIGHASH_ANYONECANPAY> OP_AND
--	---

【0248】 在本發明中，如同表 8 之指令碼，表 8 中之以上指令碼亦可被稱作 OP_SELFTXINJECTION。因此，在本發明之實施例中對 OP_SELFTXINJECTION 之參考應被視為在以上指令碼中執行之操作的速記。

【0249】 亦應注意，提供 SIGHASH 類型、根據 SIGHASH 類型判定之解除鎖定交易欄位之集合及經序列化先前交易的任何實體可獲得交易輸出。然而，此成為如下文進一步詳細描述之有用特徵。如上文所提到，在一些實例中，獲得交易輸出係指建立參考交易輸出之解除鎖定交易及成功地驗證解除鎖定交易。

【0250】 圖 11 係說明根據各種實施例之用於使得插入經序列化先前交易的處理程序 1100 之實例的流程圖。用於使得插入經序列化交易之處理程序 1100 (或所描述之任何其他處理程序，或彼等處理程序之變化或組合) 中之一些或全部可在經組態有可執行指令或其他資料之一或多個電腦系統的控制下執行，且可實施為共同地在一或多個處理器上執行之可執行指令。可執行指令或其他資料可儲存於非暫時性電腦可讀儲存媒體上(例如，永久地儲存於磁性、光學或快閃記憶體媒體上之電腦程式)。

【0251】 舉例而言，用於使得插入經序列化交易之處理程序 1100 中之一些或全部可藉由區塊鏈網路(諸如，圖 1 之實例區塊鏈網路 100)中之驗

證節點執行。此驗證節點可由任何合適的計算裝置組成(例如，藉由資料中心中之伺服器、藉由用戶端計算裝置、藉由計算資源服務提供者之分散式系統中的多個計算裝置或藉由任何合適的電子用戶端裝置，諸如圖 26 之計算裝置 2600)。用於使得插入經序列化交易之處理程序 1100 包括一系列操作，其中執行用於使得插入經序列化交易之處理程序 1100 之系統聯合地執行未經驗證交易之解除鎖定指令碼及鎖定指令碼，且結果，獲得對應於自未經驗證交易提取之交易 ID 的經序列化先前交易。

【0252】 在步驟 1102 中，系統自試圖重新關聯數位資產之至少一部分的實體獲得未經驗證交易。未經驗證交易包括鎖定指令碼及解除鎖定指令碼。鎖定指令碼及解除鎖定指令碼可類似於上表 8 及表 9 中所展示之鎖定指令碼及解除鎖定指令碼。亦即，鎖定指令碼包括諸如藉由解除鎖定指令碼獲取作為儲存於主堆疊及替代堆疊中之輸入值的指令集。指令集之執行若評估為真，則成功地驗證未經驗證交易。因此，在鎖定指令碼之前執行解除鎖定指令碼，從而在主堆疊及替代堆疊中設置待由鎖定指令碼使用之值。圖 11 之實施例中的未經驗證交易之解除鎖定指令碼包括經序列化先前交易、SIGHASH 類型及解除鎖定交易欄位之經序列化集合。

【0253】 作為執行解除鎖定指令碼接著執行鎖定指令碼之結果，在步驟 1104 中，系統獲得包括於解除鎖定指令碼中的經序列化先前交易、SIGHASH 類型及解除鎖定交易之經序列化集合。在步驟 1106 中，系統基於 SIGHASH 基於未經驗證交易之欄位值之經序列化集合來產生簽名。應注意，SIGHASH 類型影響哪些欄位用於簽名產生中，且所要 SIGHASH 可取決於所搜尋之特定先前交易。舉例而言，表 8 利用 SIGHASH 類型 SIGHASH_ALL，該表說明用於提取先前交易但未必提取含有相同指令碼之先前交易的鎖定指令碼及解除鎖定指令碼。如圖 9 中所說明，

SIGHASH_ALL 類型使得能夠擷取解除鎖定交易之其他先前交易的輸入。相比而言，表 9 利用 SIGHASH 類型 SIGHASH_ALL|ANYONECANPAY，該表說明用於提取具有相同鎖定指令碼之先前交易(亦即，對應於經簽名之輸入的先前交易)的鎖定指令碼及解除鎖定指令碼。如圖 9 中所說明，SIGHASH 類型 SIGHASH_ALL|ANYONECANPAY 移除除具有經簽名之輸入之先前交易外的其他先前交易之輸入。

【0254】 在步驟 1108 中，系統驗證先前產生之簽名，且接著在步驟 1110 中，藉由執行所獲得之經序列化先前交易的雙 SHA-256，產生應匹配解除鎖定交易(亦即，欄位值之經序列化集合)之交易 ID 的值。藉由使用子串操作碼，在步驟 1112 中，系統提取欄位值之經序列化集合的交易 ID，且在步驟 1114 中，系統判定藉由經序列化先前交易之雙 SHA-256 產生的交易 ID 是否匹配欄位值之經序列化集合的交易 ID。應注意，在各種實施例中，匹配未必需要相等。舉例而言，若兩個值不相等但在數學上等效，則其可匹配。作為另一實例，若兩個值對應於共同物件(例如，值)或以某預定方式互補或其符合一或多個匹配準則，則兩個值可匹配。一般而言，可使用判定是否存在匹配之任何方式。亦應注意，在步驟 1102 至步驟 1114 中執行之操作中之一或多者可按各種次序及組合(包括並列地)來執行。

【0255】 圖 12 說明實例 1200，其說明由本發明之實施例解決的與鎖定指令碼相關聯之問題。亦即，圖 12 中所描繪之實例 1200 說明由於將未判定資料提供至鎖定指令碼而呈現的問題。在一些實例中，術語「未判定資料」係指經由解除鎖定鎖定指令碼之解除鎖定指令碼提供的資料，執行鎖定指令碼之節點不具有該資料之先前指示。

【0256】 在一些實施例中，先前交易 1202 類似於圖 3 之先前交易 302。同樣地，在一些實施例中，解除鎖定交易 1204 類似於解除鎖定交易

304。在一些實施例中，區塊鏈 1224 係由同級間電子總帳中之交易的區塊之集合組成。在實施例中，區塊鏈 1224 之每一區塊包含先前區塊之散列，使得區塊變為鏈接(亦即，「鏈結」)在一起以建立區塊鏈中之所有經驗證交易的永久性不可變記錄。

【0257】 在一些實施例中，未判定源 1222A 可係試圖獲得先前交易 1202 之 UTXO 的實體。未判定源 1222B 可與未判定源 1222A 相同或可係不同於未判定源 1222A 之實體。在任一狀況下，執行鎖定指令碼之節點在執行鎖定指令碼之前不具有對未判定源 1222A 至未判定源 1222B 之先驗瞭解。

【0258】 在實例 1200 中，鎖定指令碼 1206 空白，允許其在對資料源或資料將為何資料無先驗瞭解之情況下接受資料。在建立解除鎖定交易 1204 (例如，藉由未判定源 1222A)時判定資料(「<d>」)。然而，因為解除鎖定交易 1204 在其於區塊鏈 1224 上被確認之前(此時解除鎖定交易 1204 變得不可變)易於諸如藉由未判定源 1222B 更改(換言之，其可變)，所以此鎖定指令碼呈現安全性問題。

【0259】 圖 13 說明實例 1300，其說明在本發明之實施例中來自經判定源之未判定資料可如何安全地佈建至鎖定指令碼 1306 中。亦即，圖 13 中所描繪之實例 1300 說明在如下情形中所呈現之問題：執行鎖定指令碼 1306 之節點具有對將提供資料之源(例如，經判定源 1326)的先驗瞭解，但不具有關於資料將為何資料之先驗瞭解。在一些實施例中，先前交易 1302 類似於圖 3 之先前交易 302。同樣地，在一些實施例中，解除鎖定交易 1304 類似於 304。在一些實施例中，區塊鏈 1324 類似於圖 12 之區塊鏈 1224。

【0260】 在實例 1300 中，鎖定指令碼 1306 經組態以使執行鎖定指令碼 1306 之驗證節點檢查提供於解除鎖定指令碼 1308 中之資料是否已由經

判定資料源提供。亦即，藉由以如下方式執行與資料(d)相乘，可基於資料修改私用密鑰以產生經修改之私用密鑰(a')：

$$a' = a \times d$$

【0261】 可類似地藉由以如下方式執行橢圓曲線點乘法來修改未經修改之私用密鑰的公用密鑰(A)對應物以產生經修改之公用密鑰(A')：

$$A' = d \times A$$

【0262】 因此，鎖定指令碼 1306 可經組態以使驗證節點評估使用私用密鑰進行簽名之簽名，該私用密鑰係使用資料源之公用密鑰(A)基於資料進行修改。更特定而言，簽名檢查操作碼可包括於鎖定指令碼 1306 中，該簽名檢查操作碼檢查使用經修改之私用密鑰進行簽名的簽名($\text{Sig } A'$)是否對應於經修改之公用密鑰且因此是否係有效簽名。該檢查可例如藉由使用 `OP_CHECKSIG` 操作碼執行。

【0263】 如實例 1300 中可見，鎖定指令碼 1306 之執行使節點將公用密鑰置放於堆疊上，且執行公用密鑰與藉由解除鎖定指令碼 1308 之先前執行而置放於堆疊中的資料之間的橢圓曲線點乘法運算(`OP_ECMULT`)。接著，可在藉由指定於鎖定指令碼中之源(例如，經判定源 1326)建立解除鎖定交易時判定資料。因此，鎖定指令碼瞭解提供資料之源，但不瞭解資料將為何資料。鎖定指令碼 1306 之進一步執行使得對照使用經修改之私用密鑰進行簽名的資料的亦藉由解除鎖定指令碼 1308 之先前執行置放於堆疊上的簽名而驗證結果(例如，若值匹配，則 `OP_CHECKSIG` 傳回真)。因為對解除鎖定交易 1304 之更改將使其失效，所以此方法係安全的。然而，必須指定資料源(經判定源 1326)。ECDSA 中之簽名證實演算法涉及檢查簽名、公用密鑰及訊息是否具有特定數學關係。該訊息可係任何資料。在比特幣中，證實操作碼 `OP_CHECKSIG` 藉由將訊息限於經序列化交易同時仍允許

證實訊息來自特定源來防止任何任意資料成為訊息。本發明之實施例提供此限制之替代解決方案。

【0264】 在一些實施例中，未判定源 1322 係不能更改資料之實體。在一些實施例中，經判定源 1326 係在產生鎖定指令碼 1306 時已知的實體，使得鎖定指令碼 1306 包括經判定源 1326 之公用密鑰。

【0265】 圖 14 說明實例 1400，其表明未判定資料可如何安全地自未判定源佈建至鎖定指令碼 1406 中。具體而言，圖 14 描繪執行基於結合圖 11 之處理程序 1100 所描述之鎖定指令碼的鎖定指令碼的解除鎖定交易 1404。在一些實施例中，先前交易 1402 類似於圖 3 之先前交易 302。同樣地，在一些實施例中，解除鎖定交易 1404 類似於解除鎖定交易 304。在一些實施例中，區塊鏈 1424 類似於圖 12 之區塊鏈 1224。

【0266】 實例 1400 與圖 13 之實例 1300 的不同之處在於，實例 1400 中之資料在建立鎖定指令碼 1406 時可能未判定。所討論之資料將嵌入先前交易 1402 中某處，且因此可藉由剖析如上文關於以上圖 8 至圖 11 所描述之經序列化先前交易來提取。

【0267】 以此方式，執行鎖定指令碼 1406 之節點無需對提供經序列化先前交易之實體具有先驗瞭解，節點亦無需對先前交易 1402 具有先驗瞭解。此外，正提交至區塊鏈 1424 之先前交易 1402 在建立解除鎖定交易 1404 時已不可變，且藉此在不使解除鎖定交易 1404 無效之情況下免於更改。然而，儘管執行鎖定指令碼 1406 之節點對資料不具有先驗瞭解，但在建立先前交易 1402 時資料已經判定。

【0268】 在一些實施例中，鎖定指令碼 1406 係根據關於圖 11 之用於使得插入經序列化交易之處理程序 1100 所描述之指令碼的指令碼。在一些實施例中，解除鎖定指令碼 1408 類似於結合圖 8 至圖 11 所描述之解除鎖

定指令碼。舉例而言，如實例 1400 中可見，解除鎖定指令碼 1408 包括至少一個經序列化先前交易、SIGHASH 類型及解除鎖定交易 1404 之解除鎖定交易欄位的經序列化集合。

【0269】 未判定源 1422A 係供應編碼於經序列化先前交易中之資料的實體。未判定源 1422B 係試圖攔截及更改解除鎖定交易 1404 之實體。在一些實施例中，未判定源 1422A 至未判定源 1422B 可係相同或不同實體。如實例 1400 中可見，在建立鎖定指令碼 1406 時無需知曉未判定源 1422A 之身分。此外，在建立鎖定指令碼 1406 時亦無需知曉資料。然而，仍防止未判定源 1422B 更改資料。

【0270】 在實施例中，除正由解除鎖定交易 1404 執行之鎖定指令碼外，先前交易 1402 之各種欄位可用以儲存安全的未判定資料，包括先前交易 1402 之輸出中的數位資產量或編碼於先前交易 1402 之另一輸出之鎖定指令碼中的後設資料。因此，實例 1400 之實施例實際上允許任何實體將資料嵌入先前交易中，對鎖定指令碼 1406 之某變化進行支付且保證無其他實體可修改彼資料。此特徵在下文所描述之其他實施例中係有用的。

【0271】 圖 15 係說明根據各種實施例之用於安全地佈建未判定資料的處理程序 1500 之實例的流程圖。用於安全地佈建未判定資料的處理程序 1500 (或所描述之任何其他處理程序，或彼等處理程序之變化或組合)中的一些或全部可在經組態有可執行指令或其他資料之一或多個電腦系統的控制下執行，且可實施為共同地在一或多個處理器上執行之可執行指令。可執行指令或其他資料可儲存於非暫時性電腦可讀儲存媒體上(例如，永久地儲存於磁性、光學或快閃記憶體媒體上之電腦程式)。

【0272】 舉例而言，用於安全地佈建未判定資料的處理程序 1500 中的一些或全部可藉由區塊鏈網路(諸如，圖 1 之實例區塊鏈網路 100)中之驗

證節點執行。此驗證節點可由任何合適的計算裝置組成(例如，藉由資料中心中之伺服器、藉由用戶端計算裝置、藉由計算資源服務提供者之分散式系統中的多個計算裝置或藉由任何合適的電子用戶端裝置，諸如圖 26 之計算裝置 2600)。用於安全地佈建未判定資料的處理程序 1500 包括一系列操作，其中接收未經驗證交易，作為執行解除鎖定指令碼之結果而獲得未判定資料及第二值，且將未判定資料驗證為與受信任資料源相關聯。

【0273】 在步驟 1502 中，系統自試圖重新關聯數位資產之至少一部分的實體獲得未經驗證交易。未經驗證交易包括鎖定指令碼及解除鎖定指令碼。鎖定指令碼及解除鎖定指令碼可類似於圖 13 及圖 14 中所展示之鎖定指令碼及解除鎖定指令碼。指令集之執行若評估為真，則成功地驗證未經驗證交易。因此，在鎖定指令碼之前執行解除鎖定指令碼，從而在主堆疊及替代堆疊中設置待由鎖定指令碼使用之值。

【0274】 圖 13 之實施例中的未經驗證交易之解除鎖定指令碼包括未判定資料(「<d>」)及使用經修改之私用密鑰進行簽名的未判定資料之簽名(「<SigA'>」)，該經修改之私用密鑰係藉由使用橢圓曲線點乘法將經判定資料源(例如，「鮑勃」)之私用密鑰乘以未判定資料之值來修改。因此，私用密鑰將係橢圓曲線上之點。應注意，如上文所提及，術語「未判定」在此上下文中係指資料未由鎖定指令碼自身指定或以其他方式約束。以類似方式，「未判定資料源」係身分未由鎖定指令碼指定或約束之資料源，而「經判定資料源」在鎖定指令碼內將身分約束為特定資料源(例如，藉由包括資料源之公用密鑰)。圖 14 之實施例中的未經驗證交易之解除鎖定指令碼包括經序列化先前交易之未判定資料、SIGHASH 類型及解除鎖定交易欄位之經序列化集合。以此方式，因為資料源係經序列化先前交易，所以資料源無需由鎖定指令碼自身指定或約束。

【0275】 作為執行解除鎖定指令碼接著執行鎖定指令碼之結果，在步驟 1504 中，系統獲得未判定資料及可用以驗證該資料(例如，藉由經修改之私用密鑰進行簽名的簽名或解除鎖定交易欄位之經序列化集合，自該集合可提取交易識別符)之值，該資料具有與該資料相關聯之經判定或未判定源。

【0276】 在步驟 1506 中，系統驗證資料。舉例而言，在圖 13 之實施例中，系統藉由以下操作驗證資料與包括於鎖定指令碼中之公用密鑰相關聯：使用橢圓曲線點乘法(如上文所描述)來用資料修改公用密鑰；及驗證經修改之公用密鑰與使用對應私用密鑰產生之簽名相關聯，該私用密鑰自身係使用橢圓曲線點乘法進行修改。作為另一實例，在圖 14 之實施例中，系統藉由以下操作驗證資料對應於特定先前交易：判定經序列化先前交易之散列是否匹配以圖 11 之用於使得插入經序列化交易之處理程序 1100 的方式自解除鎖定交易欄位之經序列化集合提取的交易 ID。應注意，在步驟 1502 至步驟 1506 中執行之操作中之一或多者可按各種次序及組合(包括並列地)來執行。

【0277】 圖 16 說明本發明之實施例的經參數化智慧型合約 1600 之實例。具體而言，圖 16 描繪先前交易 1602，其具有對解除鎖定交易 1604 之解除鎖定指令碼 1608 強加約束之鎖定指令碼 1606。圖 16 中所描繪之實施例可藉由回顧本發明在圖 3 至圖 6 之描述中已描述如何可使得將根據 SIGHASH 類型判定之解除鎖定交易欄位之集合插入至鎖定指令碼 1606 中來理解。進一步回顧圖 7 至圖 11 之描述，本發明描述可如何在應用約束之前使用子串操作碼剖析根據 SIGHASH 類型判定之解除鎖定交易欄位之集合以提取交易 ID，從而使得將經序列化先前交易插入至鎖定指令碼 1606 中。此處理程序可擴展以對解除鎖定交易欄位之集合中之任何欄位起作用。

【0278】 應注意，描述於圖 6 及圖 11 之上下文中的鎖定指令碼不對

建立解除鎖定交易之特定實體進行限定。舉例而言，鎖定指令碼不需要證明特定實體可存取秘密(例如，私用密鑰、產生某散列之值等)。圖 16 之實施例將此概念應用成關於建立解除鎖定交易之特定實體不進行區分，但對可如何主張 UTXO 強加某些約束。以此方式，圖 16 之實施例被自動地執行且係自我強制實行的。換言之，若智慧型合約之條件不滿足(亦即，不符合指定約束)，則合約將不執行，此係因為驗證將失敗。

【0279】 在一些實施例中，可藉由對解除鎖定交易 1604 之輸入施加約束(例如，參數)(例如，需要來自「愛麗絲」之輸入)而使鎖定指令碼中之智慧型合約交互。因為解除鎖定指令碼 1608 係用於鎖定指令碼 1606 之輸入源，所以在實施例中，鎖定指令碼 1606 中之智慧型合約可使用解除鎖定指令碼 1608 中之安全的未判定資料來參數化。在實施例中，以結合圖 13 至圖 15 所描述之方式未判定及保證安全的經參數化資料以保護智慧型合約免於更改。在實施例中，未判定經參數化資料。

【0280】 本發明描述用於將安全的未判定資料提供至鎖定指令碼(例如，智慧型合約)之二種方法。第一方法係可自如描述於圖 13 及圖 15 之上下文中之經判定源獲得安全的未判定資料。第二方法係可自如描述於圖 14 至圖 15 之上下文中之未判定源(例如，先前交易)獲得安全的未判定資料。在使用第一方法之實施例中，參數將由建立解除鎖定交易之實體判定且將在建立解除鎖定交易時設定(例如，在解除鎖定指令碼 1608 中)。在使用第二方法之實施例中，參數將由建立先前交易之實體判定且將在建立先前交易時設定(亦即，嵌入經序列化先前交易中)。亦應注意，在實施例中，可組合第一方法與第二方法使得一或多個參數可嵌入於先前交易中且一或多個其他參數可嵌入於解除鎖定交易之解除鎖定指令碼中。

【0281】 呈現以下實例以說明可如何使用此等方法建立智慧型合

約。在實例中，為愛麗絲或藉由愛麗絲建立智慧型合約以將其收入之 70% 轉遞至其儲蓄且將其收入之 30%轉遞至其投資經理鮑勃。其儲蓄帳戶與密碼編譯公用密鑰 A (PubK A)相關聯，且其與鮑勃之帳戶與密碼編譯公用密鑰 B (PubK B)相關聯。愛麗絲之雇主實施此智慧型合約，其在發薪日使得將愛麗絲之收入以上文所描述之方式進行分配。因此，愛麗絲之收入以其希望之方式自動地分離。

【0282】 在該實例中，參數係作為執行智慧型合約之結果而傳送之數位資產的量。根據以上準則，智慧型合約之執行將使得在判定對解除鎖定交易 1604 之輸出的約束之前自先前交易 1602 提取參數。表 10 呈現實例解除鎖定及鎖定指令碼以實施以上實例：

表 10：

解除鎖定指令碼	鎖定指令碼
<Serialized Previous Tx> <SIGHASH Type> <Serialized Set of Unlocking Tx Fields>	// 檢查解除鎖定 Tx 輸出 0 量係先前 Tx 輸出 0 量之 70% //處理解除鎖定 Tx OP_DUP <Script to Extract Unlocking Tx Output 0 Amount> //處理先前 Tx <3> OP_ROLL <Script to Extract Previous Tx Output 0 Amount> // 將先前 Tx 量按比例調整 70%且執行相等檢查 <70> OP_MUL <100> OP_DIV OP_EQUALVERIFY //檢查解除鎖定 Tx 輸出 0 及 1 量等於先前 Tx 輸出 0 量 //處理解除鎖定 Tx OP_DUP <Script to Extract Unlocking Tx Output 0 Amount> OP_OVER <Script to Extract Unlocking Tx Output 1 Amount>

	OP_ADD //處理先前 Tx <3> OP_ROLL <Script to Extract Previous Tx Output 0 Amount> //相等證實 OP_EQUALVERIFY //檢查輸出目的地 //檢查解除鎖定 Tx 輸出 0 鎖定指令碼 OP_DUP <Script to Extract Unlocking Tx Output 0 Locking Script> <P2PK Alice> OP_EQUALVERIFY // 檢查解除鎖定 Tx 輸出 1 鎖定指令碼 OP_DUP <Script to Extract Unlocking Tx Output 1 Locking Script> <P2PK Bob> OP_EQUALVERIFY //檢查已插入先前 Tx、SIGHASH 類型及解除鎖定 Tx OP_SELFCTXINJECTION
--	---

【0283】 圖 17 係說明根據各種實施例之用於實施經參數化智慧型合約的處理程序 1700 之實例的流程圖。用於實施經參數化智慧型合約的處理程序 1700 (或所描述之任何其他處理程序，或彼等處理程序之變化或組合)中之一些或全部可在經組態有可執行指令或其他資料之一或多個電腦系統的控制下執行，且可實施為共同地在一或多個處理器上執行之可執行指令。可執行指令或其他資料可儲存於非暫時性電腦可讀儲存媒體上(例如，永久地儲存於磁性、光學或快閃記憶體媒體上之電腦程式)。

【0284】 舉例而言，用於實施經參數化智慧型合約的處理程序 1700 中之一些或全部可藉由區塊鏈網路(諸如，圖 1 之實例區塊鏈網路 100)中之驗證節點執行。此驗證節點可由任何合適的計算裝置組成(例如，藉由資料中心中之伺服器、藉由用戶端計算裝置、藉由計算資源服務提供者之分散

式系統中的多個計算裝置或藉由任何合適的電子用戶端裝置，諸如圖 26 之計算裝置 2600)。用於實施經參數化智慧型合約的處理程序 1700 包括一系列操作，其中自嵌入於安全的未判定資料中提取約束。

【0285】 在步驟 1702 中，系統執行使得插入經序列化先前交易(例如，圖 16 之先前交易 1602 的經序列化欄位值)、SIGHASH 類型及根據 SIGHASH 類型判定之解除鎖定交易欄位(例如，解除鎖定交易 1604 之欄位值)之集合的指令碼。該指令碼可係來自表 8 或表 9 之指令碼的變化。應注意，可能不需要圖 11 之用於使得插入經序列化交易之整個處理程序 1100 用於圖 16 及圖 17 之可參數化智慧型合約，此係因為若不需要來自未判定源之參數，則可能不需要經序列化先前交易。

【0286】 在步驟 1704 中，系統以取決於參數源係未判定源抑或經判定源之方式提取參數。舉例而言，自經判定源之資料提取參數可藉由以結合圖 13 所描述之方式自解除鎖定指令碼 1608 提取參數來執行。作為另一實例，自未判定源之資料提取參數可藉由以結合圖 14 所描述之方式自經序列化先前交易提取參數來執行。作為又一實例，若一些參數嵌入於未判定源之資料中且一些參數接收自經判定源，則指令碼可經編寫以組合圖 13 及圖 14 之操作從而自來自未判定源及經判定源兩者之資料提取參數。

【0287】 在步驟 1706 中，系統自參數導出約束。舉例而言，在表 10 之實例指令碼中，參數係支付至智慧型合約之量，且導出約束包括判定向愛麗絲及鮑勃之支付公用密鑰(P2PK)位址支付的量(例如，70%及 30%)。然而，預期參數及自參數導出之約束可係眾多的且超出上文給出之實例而變化。

【0288】 在步驟 1708 中，系統對照根據 SIGHASH 類型判定之解除鎖定交易欄位值之集合證實約束。亦即，系統證實解除鎖定交易之相關子

集滿足約束。若解除鎖定交易之相關子集滿足約束，則解除鎖定交易被確認為有效，否則若解除鎖定交易之相關子集不滿足約束，則解除鎖定交易被視為無效。應注意，在步驟 1702 至步驟 1708 中執行之操作中之一或多者可按各種次序及組合(包括並列地)來執行。

【0289】 圖 18 說明由本發明之實施例解決的與重複智慧型合約相關聯之問題的實例 1800。亦即，為建立重複已知數目次(例如，五次)之交易，可預先建立已知數目個解除鎖定交易。雖然對於少數交易，此操作可管理，但對於具有許多重複交易之合約，預先產生所有解除鎖定交易 1804A 至解除鎖定交易 1804N 可變得繁瑣且指令碼 1806A 至指令碼 1806N 可變得相當大。在一實例中，愛麗絲具有一定量的數位資產(例如，比特幣)，其價值可交換商品或服務。愛麗絲已將此量分配成由其兒子鮑勃使用以支付其每日在學校的午餐。圖 18 之實例 1800 展示愛麗絲可預先針對鮑勃之個別午餐交易中之每一者建立解除鎖定交易 1804A 至解除鎖定交易 1804N。然而，如圖 19 中所展示，本發明涵蓋用於愛麗絲之替代解決方案。

【0290】 圖 19 說明本發明之實施例的自我複寫智慧型合約之實例 1900。如圖 19 中所說明，替代建立預定某數目個解除鎖定交易以達成重複合約，可建立基於結合圖 16 至圖 17 所描述之可參數化智慧型合約的具有終止條件之自我複寫智慧型合約 1904。以此方式，在以上實例中，愛麗絲僅需要建立一個解除鎖定交易以消耗先前交易 1902 中之數位資產的初始量。解除鎖定交易 1904A 包括使解除鎖定交易 1904A 將自身複寫至下一解除鎖定交易中的指令碼。該指令碼包括終止條件，該終止條件使解除鎖定交易 1904N 在終止條件滿足之後(例如，在發生 n 次之後)停止複寫。

【0291】 在一個可能實施中，為建立合約之交易鏈，預先建立未來交易且每一交易之鎖定指令碼嵌入連續交易之鎖定指令碼，如圖 20 中所展

示。然而，為使自我複寫解除鎖定交易證實解除鎖定交易之約束未經修改，每一先前交易之鎖定指令碼(例如，智慧型合約)將需要安全地證實其匹配解除鎖定交易中之鎖定指令碼。

【0292】 圖 20 說明由本發明之實施例解決的與重複交易相關聯之問題的實例 2000。亦即，先前交易 2002 之鎖定指令碼(鎖定指令碼 0)併有第一解除鎖定交易 2004A 之鎖定指令碼(鎖定指令碼 1)，其自身併有第二解除鎖定交易 2004B 之鎖定指令碼(鎖定指令碼 2)，等等，直至最終解除鎖定交易 2004N。若完全展開，則變得顯而易見的係：鎖定指令碼 0 不與鎖定指令碼 1 相同，鎖定指令碼 1 不與鎖定指令碼 2 相同，等等。因此，實例 2000 無法據稱為自我複寫的，此係因為鎖定指令碼不相同。此問題可理解為源自自我參考之問題。亦即，鎖定指令碼將需要嵌入其自身之複本，藉此變成無休止且可拆開的迴圈。因此，鎖定指令碼將係不可判定的。實例 2000 固定了迴圈可在將值指派至第 n 鎖定指令碼之前拆開的次數(n)，其接著允許第 $n-1$ 鎖定指令碼嵌入第 n 鎖定指令碼，其允許第 $n-2$ 鎖定指令碼嵌入第 $n-1$ 鎖定指令碼，等等。然而，此產生 n 個不同的鎖定指令碼。

【0293】 圖 21 說明關於自我複寫交易之缺乏經驗的(naïve)實施之問題的解決方案之實例 2100。具體而言，圖 21 描繪每次將發送至其自身之數位資產量減少一個單位以及將 1 個單位的數位資產支付給愛麗絲的複製智慧型合約。亦即，先前交易 2102 持有初始量 X 。第一解除鎖定交易 2104A 將 1 個單位的數位資產支付給屬於愛麗絲之支付公用密鑰散列(P2PKH)位址，輸出新的總量($X'=X-1$)且將其自身複寫至第二解除鎖定交易 2104B。在一些實例中，P2PK 或 P2PKH 可用作位址以將數位資產直接傳送至與各別公用密鑰相關聯之實體。第二解除鎖定交易 2104B 同樣將 1 個單位的數位資產支付給愛麗絲，輸出新的總量($X''=X'-1$)且同樣複寫其自身。

【0294】 因此，可見在處理程序繼續而不管初始量 X 時，將最終產生解除鎖定交易以輸出不可兌現量的數位資產(例如，零)。此可藉由觀察到以下情形來直觀地理解：每一後續解除鎖定交易將具有比其先前交易少的數位資產量，甚至在不扣除在各種區塊鏈協定中扣除之最小交易費用的情況下亦如此。因此，量輸出將趨於零，此時處理交易變得無意義。然而，本發明之實施例包括藉由實施終止條件以避免此不可兌現解除鎖定交易來解決此問題。

【0295】 此外，在實施例中，圖 20 中所說明之問題的解決方案將使鎖定指令碼 1 接收第一資料(例如，解除鎖定交易資料)及第二資料(例如，先前交易資料)，其兩者嵌入鎖定指令碼。在此等實施例中，鎖定指令碼 1 證實來自第一資料及第二資料之鎖定指令碼匹配。接著，若鎖定指令碼 1 證實第二資料(先前交易資料)嵌入鎖定指令碼 1，則其證實第一資料亦嵌入鎖定指令碼 1。

【0296】 此指令碼之基本概述見於下表 11 中：

表 11：

解除鎖定指令碼	鎖定指令碼
<Serialized Previous Tx> <SIGHASH Type> <Set of Unlocking Tx Fields >	<Script to Check Termination Condition> //若未終止 OP_NOTIF //複製及自解除鎖定 Tx 提取鎖定指令碼 OP_DUP <Script to Extract Locking Script> //複製及自先前 Tx 提取鎖定指令碼 <3> OP_ROLL <Script to Extract Locking Script> //檢查鎖定指令碼係相同的 OP_EQUALVERIFY OP_ENDIF

	//檢查對應於鎖定指令碼之先前 Tx 的插入 OP_SELFTXINJECTION
--	--

【0297】 如在以上指令碼中可見，對照第一解除鎖定交易 2104A 之鎖定指令碼來證實先前交易 2102 之鎖定指令碼，該鎖定指令碼係將解除鎖定 UTXO 之當前正運行的鎖定指令碼，該第一解除鎖定交易將在當前解除鎖定交易係另一解除鎖定交易(例如，第二解除鎖定交易 2104B)之先前交易時在未來進行兌現。因此，替代針對每一交易建立不同的解除鎖定交易，如圖 18 及圖 20 中所展示，指令碼改為強制每一鎖定指令碼必須相同。若先前交易 2102 之鎖定指令碼與第二解除鎖定交易 2104B 將試圖解除鎖定之鎖定指令碼(例如，第一解除鎖定交易 2104A)相同，則鎖定指令碼保證係真實的。

【0298】 在實施例中，終止條件避免如下情形：先前交易具有不足的資金，但鎖定指令碼仍驗證；亦即，不可兌現交易。舉例而言，可實施終止條件以證實存在足夠的數位資產來進行下一交易，否則終止驗證。作為更特定實例，若初始集區含有 365 個單位的數位資產加上每一交易費用所需的量(例如，足夠用於一年每天一個交易)，則終止條件可證實剩餘的單位數目大於完成交易所需的數目；例如，只要存在足夠資金，便可接著繼續驗證交易。否則，若資金不足，則終止條件滿足且驗證停止。因此，若在第 366 天資金不足，則驗證第 366 解除鎖定交易之鎖定指令碼係不需要的且終止條件確保其終止鎖定指令碼之自我複寫。

【0299】 圖 22 係說明根據各種實施例之用於具有終止條件之自我複寫智慧型合約的處理程序 2200 之實例的流程圖。用於具有終止條件之自我複寫智慧型合約的處理程序 2200 (或所描述之任何其他處理程序，或彼等處

理程序之變化或組合)中之一些或全部可在經組態有可執行指令或其他資料之一或多個電腦系統的控制下執行，且可實施為共同地在一或多個處理器上執行之可執行指令。可執行指令或其他資料可儲存於非暫時性電腦可讀儲存媒體上(例如，永久地儲存於磁性、光學或快閃記憶體媒體上之電腦程式)。

【0300】 舉例而言，用於具有終止條件之自我複寫智慧型合約的處理程序 2200 中之一些或全部可藉由區塊鏈網路(諸如，圖 1 之實例區塊鏈網路 100)中之驗證節點執行。此驗證節點可由任何合適的計算裝置組成(例如，藉由資料中心中之伺服器、藉由用戶端計算裝置、藉由計算資源服務提供者之分散式系統中的多個計算裝置或藉由任何合適的電子用戶端裝置，諸如圖 26 之計算裝置 2600)。用於具有終止條件之自我複寫智慧型合約的處理程序 2200 包括一系列操作，其中若終止條件未滿足，則解除鎖定交易及先前交易之鎖定指令碼經證實為相同的，且其他約束經證實。

【0301】 在步驟 2202 中，系統接收未經驗證交易。系統以運行未經驗證交易之解除鎖定指令碼開始，且接著開始執行與由未經驗證交易參考之數位資產相關聯的先前(經驗證)交易之鎖定指令碼。用於具有終止條件之自我複寫智慧型合約的處理程序 2200 描繪為執行表 11 之實例指令碼的變化。舉例而言，在步驟 2204 中，執行用於具有終止條件之自我複寫智慧型合約的處理程序 2200 之系統判定終止條件是否滿足。如上文所提到，在一實施中，若數位資產量不足以完成交易，則終止條件可滿足。然而，預期其他終止條件係可能的。舉例而言，終止條件可基於時間；若未經驗證交易在特定日期之前未得到驗證，則終止條件可滿足。

【0302】 在滿足終止條件後，在步驟 2206 中，用於具有終止條件之自我複寫智慧型合約的處理程序 2200 終止且驗證結束。否則，在步驟 2208

中，系統自未經驗證交易提取第一鎖定指令碼。應注意，第一鎖定指令碼係將在當前未經驗證交易得到驗證之後執行的鎖定指令碼，此時另一未經驗證交易試圖傳送當前交易之 UTXO。

【0303】 在步驟 2210 中，系統自經序列化先前交易提取第二鎖定指令碼。在此實施例中，第二鎖定指令碼係當前正執行之鎖定指令碼的複本。在步驟 2212 中，執行用於具有終止條件之自我複寫智慧型合約的處理程序 2200 之系統判定第一鎖定指令碼是否匹配第二鎖定指令碼(例如，兩個鎖定指令碼是否相同)。若鎖定指令碼不匹配，則在步驟 2214 中，系統判定未經驗證交易未通過驗證且保持未經驗證。

【0304】 否則，在步驟 2216 中，系統證實指令碼中之任何剩餘約束(例如，驗證數位簽名或先前交易之其他要求)。若不存在剩餘約束或若所有剩餘約束經成功驗證，則交易經成功驗證。在成功驗證之後，可將交易新增至區塊鏈。應注意，在步驟 2202 至步驟 2216 中執行之操作中之之一或多者可按各種次序及組合(包括並列地)來執行。

【0305】 圖 23 說明由本發明之實施例解決的問題之實例 2300。具體而言，圖 23 描繪使用區塊鏈交易自第一狀態轉變至第二狀態之狀態機。在一些實例中，狀態機之狀態轉變係解釋為給定當前狀態、一或多個輸入 2326 及狀態規則之集合 2306，判定下一狀態。圖 23 之實例 2300 說明先前交易 2302 與狀態規則之集合 2306 及嵌入於參數中之第一狀態 2328A。在一些實施例中，建立解除鎖定交易 2304 以接受來自經判定源之輸入 2326。輸入 2326 結合第一狀態 2328A 可用以參考狀態規則之集合 2306 判定嵌入於解除鎖定交易 2304 之參數中的第二狀態 2328B。

【0306】 在實施例中，狀態規則之集合係狀態交易矩陣，其可由以如結合圖 16 及圖 17 所描述之方式對解除鎖定交易 2304 之約束表示。在此等

實施例中，約束藉由當前狀態及輸入而參數化，自該當前狀態及該輸入判定下一狀態。約束包括確保解除鎖定交易 2304 將下一狀態值包括於特定欄位中之檢查。

【0307】 在實施例中，當前狀態表示為嵌入於交易中之參數，且解除鎖定交易 2304 將具有亦嵌入於解除鎖定交易 2304 中之下一狀態值。下一狀態值係相對於解除鎖定交易 2304 之欄位值之集合內部的智慧型合約之當前狀態，該集合如上文所提到，在建立解除鎖定交易 2304 時可存取。在一些實施例中，提供至少一個輸入作為在建立解除鎖定交易 2304 時判定之參數中的外部資料。為安全起見，此等參數來自經判定源。此提供確定性狀態轉變。最後，藉由使用上文結合圖 18 至圖 22 所描述之自我複寫智慧型合約的指令碼，建立去信任確定性狀態機之實施例。在一些實例中，「去信任」係指如下性質：只要約束滿足，任何實體便可建立有效解除鎖定交易；然而，在一些狀況下，實體可需要與經判定源互動以獲得所需輸入。應注意，儘管結合圖 23 至圖 25 所描述之各種實施例提及自經判定源獲得輸入，但預期在一些實施例中，可自未判定源，諸如自經序列化先前交易獲得一或多個輸入。

【0308】 圖 24 說明本發明之實施例的去信任確定性狀態機之實例 2400。如圖 24 中所說明，實例 2400 可包括在狀態規則之集合 2406 中的第一狀態 2428A (「S1」) 中的先前交易 2402。在實例 2400 中，狀態規則之集合 2406 提供用於下一狀態之兩個可能狀態 2430A (「S2」或「S3」)。如實例 2400 中可見，獲取解除鎖定指令碼中之輸入 2426 及嵌入於先前交易 2402 之欄位值之集合中的第一狀態 2428A (「S1」) 作為輸入的解除鎖定交易 2404 自狀態規則之集合 2406 判定適當的第二狀態 2428B (「S2」)。如實例 2400 中進一步可見，狀態轉移矩陣現提供可能用於自第二狀態 2428B 之下一狀

態轉變的新狀態 2430B (「S4」或「S5」)。應注意，狀態規則之集合 2406 可寫碼為藉由當前狀態及一或多個輸入參數化之開關陳述式或其他條件陳述式(例如，「if-then-else」)。

【0309】 在實施例中，每一可能狀態在自我複寫鎖定指令碼中表示於諸如狀態轉移矩陣之用於狀態改變的規則集合中，且特定交易表示特定狀態中之狀態機。在此等實施例中，將交易之鎖定指令碼複製至試圖將數位資產之控制傳送至必須鏈接至當前交易之下一交易的每一解除鎖定交易。此處理重複直至終止條件滿足。因為輸入不固定且可係未判定資料，所以可使狀態機之狀態基於特定外部輸入而改變。因此，未判定資料提供可影響下一狀態之輸入。

【0310】 在說明性實例中，愛麗絲借給鮑勃一些金錢且鮑勃同意還款給愛麗絲。如本發明中所描述之去信任確定性狀態機可實施為智慧型合約以表示鮑勃向愛麗絲進行之傳送。舉例而言，可建構智慧型合約使得鮑勃每月為接下來的三個月向愛麗絲進行支付，且若錯過支付，則鮑勃之債務進入債務收取階段。因此，只要鮑勃進行其每月傳送，當前狀態便保持在償還狀態。然而，外部實體提供指示鮑勃已錯過傳送之輸入，狀態接著分支至錯過傳送狀態。在錯過傳送狀態中，愛麗絲可釋放交易且將其轉向債務收取器，因此去信任確定性狀態機切換至債務收取狀態。在債務收取狀態中，債務收取器將向鮑勃收取債務。可使用圖 23 至圖 25 中所描繪之實施例的指令碼之變化來建立此智慧型合約。

【0311】 在另一實例中，愛麗絲係每月捐出 1 個單位的數位資產的非常慈善的人。其規則係任何人可主張數位資產，但每月可主張僅 1 個單位。愛麗絲以本發明中所描述之方式建立智慧型合約且將其與 3 個單位的數位資產的初始集區一起植入(seed)。愛麗絲可建構允許任何實體每月獲取 1 個

單位的數位資產的指令碼。數位資產之剩餘部分經複寫至後繼智慧型合約。下表說明實施本發明之去信任確定性狀態機之解除鎖定及鎖定指令碼的實例。

表 12：

解除鎖定指令碼	鎖定指令碼
<External Sig'><External Data> <Serialized Previous Serialized Tx> <SIGHASH Type> <Serialized Set of Unlocking Tx Fields>	<Script to Check Termination Condition> //若未終止 OP_NOTIF //檢查自我複寫智慧型合約 //自解除鎖定交易提取鎖定指令碼 <Script to Extract Locking Script> //自先前交易提取鎖定指令碼 <Script to Extract Locking Script> //檢查鎖定指令碼係相同的 OP_EQUALVERIFY //提取當前狀態 <Script to Extract Data from Serialized Previous Tx> //讀取輸入 <Script to Read Input from unlocking script> //證實狀態轉移矩陣約束 <Script to Determine State Transition> <Script to Verify Constraint on Unlocking Tx> OP_VERIFY OP_ENDIF //檢查已插入先前 Tx、SIGHASH 類型及解除鎖定 Tx OP_SELFCTXINJECTION

【0312】 圖 25 係說明根據各種實施例之用於去信任確定性狀態機之

處理程序 2500 的實例之流程圖。用於去信任確定性狀態機之處理程序 2500 (或所描述之任何其他處理程序，或彼等處理程序之變化或組合)中之一些或全部可在經組態有可執行指令或其他資料之一或多個電腦系統的控制下執行，且可實施為共同地在一或多個處理器上執行之可執行指令。可執行指令或其他資料可儲存於非暫時性電腦可讀儲存媒體上(例如，永久地儲存於磁性、光學或快閃記憶體媒體上之電腦程式)。

【0313】 舉例而言，用於去信任確定性狀態機之處理程序 2500 中的一些或全部可藉由區塊鏈網路(諸如，圖 1 之實例區塊鏈網路 100)中之驗證節點執行。此驗證節點可由任何合適的計算裝置組成(例如，藉由資料中心中之伺服器、藉由用戶端計算裝置、藉由計算資源服務提供者之分散式系統中的多個計算裝置或藉由任何合適的電子用戶端裝置，諸如圖 26 之計算裝置 2600)。用於去信任確定性狀態機之處理程序 2500 包括一系列操作，其中證實自我複寫智慧型合約之鎖定指令碼，自經串列化先前交易獲得當前狀態，自解除鎖定指令碼獲得輸入且至少部分地基於狀態規則之集合判定下一狀態。用於去信任確定性狀態機之處理程序 2500 反映表 12 中可見之實例指令碼的變化。

【0314】 在步驟 2502 中，系統接收解除鎖定交易。系統以運行解除鎖定交易之解除鎖定指令碼開始，其使得將嵌入於鎖定指令碼中之經串列化先前交易及輸入置放於堆疊中。在步驟 2512 中，取回此等輸入。在步驟 2504 中，執行用於去信任確定性狀態機之處理程序 2500 之系統判定終止條件是否滿足。終止條件可係如結合圖 19 至圖 22 所描述之終止條件。在實施例中，終止條件係在滿足後使狀態機器轉變結束之條件。若終止條件滿足，則執行用於去信任確定性狀態機之處理程序 2500 之系統繼續進行至步驟 2506，因此去信任確定性狀態機停止自我複寫。

【0315】 在步驟 2508 中，系統以描述於圖 22 之步驟 2212 中的方式證實先前交易鎖定指令碼匹配解除鎖定交易鎖定指令碼。若鎖定指令碼不匹配，則驗證未通過且解除鎖定交易未得到驗證。否則，若鎖定指令碼匹配，則在步驟 2510 中，系統自經序列化先前交易提取可能狀態集合中之當前狀態。在步驟 2512 中，系統獲得作為執行鎖定指令碼之結果而置放於堆疊上之一或多個輸入。接著，在步驟 2514 中，系統應用狀態規則之集合以基於當前狀態及一或多個輸入而判定去信任確定性狀態機之可能狀態集合中的下一狀態。在步驟 2516 中，系統證實下一狀態(例如，狀態變數及其他狀態相關資料(若適用))嵌入於解除鎖定交易中。系統亦可應用如鎖定指令碼中所指定之任何剩餘約束。在成功完成操作步驟 2502 至步驟 2516 之操作之後，用於去信任確定性狀態機之處理程序以 2500 以步驟 2518 結束，因此解除鎖定交易可被執行處理程序之系統視為有效。應注意，在步驟 2502 至步驟 2518 中執行之操作中之一或多者可按各種次序及組合(包括並列地)來執行。

【0316】 應注意，在描述所揭示實施例之上下文中，除非另外指定，否則使用關於執行「指令」通常不是獨立執行之操作(例如，傳輸資料、計算等)的可執行指令(亦被稱作程式碼、應用程式、代理程式等)之表達指示該等指令由機器執行，藉此使機器執行指定操作。

【0317】 圖 26 係可用以實踐本發明之至少一個實施例的計算裝置 2600 之說明性簡化方塊圖。在各種實施例中，計算裝置 2600 可用以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 可經組態以用作資料伺服器、網頁伺服器、攜帶型計算裝置、個人電腦或任何電子計算裝置。如圖 26 中所展示，計算裝置 2600 可包括可經組態以經由匯流排子系統 2604 與數個周邊子系統通信且以操作方式耦接至數個周邊子系統的

一或多個處理器 2602。在本發明之實施例中，處理器 2602 可用於遍歷監督模型之隨機森林中的決策樹(例如，使得評估各種搜尋項目之逆向文件頻率等)。此等周邊子系統可包括儲存子系統 2606，包含記憶體子系統 2608 及檔案或磁碟儲存子系統 2610；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。此儲存子系統 2606 可用於臨時或長期儲存資訊，諸如與本發明中所描述之交易相關聯的細節、本發明中所描述之歷史記錄的資料庫，且儲存本發明中之監督模型的決策規則。

【0318】 匯流排子系統 2604 可提供用於使計算裝置 2600 之各種組件及子系統能夠按預期相互通信之機制。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。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無線網路，使得資料技術員可能夠在處於諸如使用者資料中心之遠端位置中時傳輸及接收資料。匯流排子系統 2604 可用於將諸如細節、搜尋項目等之資料傳達至本發明之監督模型，且可用於經由網路介面子系統 2616 將監督模型之輸出傳達至一或多個處理器 2602 及商家或債權人。

【0319】 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、觸控板或圖形平板電腦；掃描器；條形碼掃描器；併入至顯示器中之觸控螢幕；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，使用術語「輸入裝置」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。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。顯示子系統可係陰極射線管(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候促進此互動，該等應用程式執行所描述之處理程序及其中之變化。

【0320】 儲存子系統 2606 可提供用於儲存可提供本發明之至少一個實施例之功能性的基本程式設計及資料建構的電腦可讀儲存媒體。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發明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發明所使用之資料的儲存庫。儲存子系統 2606 可包括記憶體子系統 2608 及檔案或磁碟儲存子系統 2610。

【0321】 記憶體子系統 2608 可包括數個記憶體，包括用於在程式執行期間儲存指令及資料之主隨機存取記憶體(RAM) 2618 及可儲存固定指令之唯讀記憶體(ROM) 2620。檔案或磁碟儲存子系統 2610 可提供用於程式及資料檔案之非暫時性永久(非揮發性)儲存，且可包括硬碟機、連同相關聯之抽取式媒體之軟碟機、緊密光碟唯讀記憶體(CD-ROM)驅動機、光碟機、抽取式媒體盒及其他相似儲存媒體。

【0322】 計算裝置 2600 可包括至少一個本端時鐘 2624。本端時鐘 2624 可係表示自特定開始日期已發生之滴答之數目的計數器，且可一體地位於計算裝置 2600 內。本端時鐘 2624 可用以使計算裝置 2600 之處理器及包括於計算裝置中之所有子系統中的資料傳送在特定時脈脈衝處同步，且

可用以協調計算裝置 2600 與資料中心中之其他系統之間的同步操作。在一個實施例中，本端時鐘 2624 係原子時鐘。在另一實施例中，本端時鐘係可程式化間隔計時器。

【0323】 計算裝置 2600 可屬於各種類型，包括攜帶型電腦裝置、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 可包括可經由一或多個埠(例如，USB、頭戴式耳機插口、Lightning 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 之裝置可包括經組態以接受光纖連接器之複數個埠。因此，此裝置可經組態以將光學信號轉換成可經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 26 中所描繪之計算裝置 2600 之描述僅意欲作為特定實例。具有比圖 26 中所描繪之系統更多或更少組件的許多其他組態係可能的。

【0324】 因此，應在說明性意義上而非限定性意義上看待說明書及圖式。然而，將顯而易見，在不脫離如申請專利範圍中所闡述之本發明之範圍的情況下，可對其進行各種修改及改變。同樣地，其他變化在本發明之範圍內。由此，雖然所揭示之技術易有各種修改及替代構造，但其某些所說明的實施例已展示於圖式中且在上文中已詳細描述。然而，應理解，不存在將本發明限於所揭示之一或多個特定形式之意圖，而相反，意圖為涵蓋屬於如隨附申請專利範圍中所定義之本發明之範圍內的所有修改、替代構造及等效物。

【0325】 除非另外指示或明顯與上下文相矛盾，否則在描述所揭示之實施例之上下文中(尤其在以下申請專利範圍之上下文中)所使用的術語「一」及「該」及類似參考物應解釋為涵蓋單數與複數兩者。除非另外提到，否則術語「包含」、「具有」、「包括」及「含有」應解釋為開放式術語(亦即，

意謂「包括但不限於」)。術語「連接」在未經修飾且指實體連接時，應解釋為部分或全部地含於……內、附接至……或接合在一起，即使存在插入之某物亦如此。除非另外指示，否則值範圍之敘述在本發明中僅意欲充當個別地提及屬於該範圍內之每一單獨值之速記方法，且每一單獨值併入本說明書中，如同其經個別地敘述一般。除非另外指出或與上下文相矛盾，否則術語「集合」(例如，「項目之集合」)或「子集」之使用應被解釋為包含一或多個成員之非空彙集。另外，除非另外指出或與上下文相矛盾，對應集合之術語「子集」未必表示對應集合之恰當子集，而是子集與對應集合可相同。

【0326】 除非另外特定陳述或另外明顯與上下文相矛盾，否則諸如形式「A、B 及 C 中之至少一者」或「A、B 及 C 中之至少一者」之片語的連接性語言另外藉由如一般用以呈現項目、術語等可係 A 或 B 或 C 或 A 及 B 及 C 之集合之任何非空子集的上下文來理解。舉例而言，在具有三個成員之集合的說明性實例中，連接性片語「A、B 及 C 中之至少一者」及「A、B 及 C 中之至少一者」係指以下集合中之任一者： $\{A\}$ 、 $\{B\}$ 、 $\{C\}$ 、 $\{A, B\}$ 、 $\{A, C\}$ 、 $\{B, C\}$ 、 $\{A, B, C\}$ 。因此，此連接性語言一般並不意欲暗示某些實施例需要 A 中的至少一者、B 中的至少一者及 C 中的至少一者各自皆存在。

【0327】 除非另外指示或另外明顯與上下文相矛盾，否則所描述之處理程序之操作可以任何合適次序執行。所描述之處理程序(或其變化或組合)可在經組態有可執行指令之一或多個電腦系統的控制下執行，且可實施為由硬體或其組合共同地在一或多個處理器上執行之程式碼(例如，可執行指令、一或多個電腦程式或一或多個應用程式)。程式碼可儲存於電腦可讀儲存媒體上，例如以包含可由一或多個處理器執行之複數個指令的電腦程式

之形式。電腦可讀儲存媒體可係非暫時性的。

【0328】 除非另外主張，否則使用所提供之任何及所有實例或例示性語言(例如，「諸如」)僅意欲較佳地闡明本發明之實施例，而不對本發明之範圍造成限制。本說明書中之語言不應解釋為指示實踐本發明所必需之任何未主張要素。

【0329】 已描述本發明之實施例，包括本發明人已知之進行本發明的最佳模式。在閱讀前述描述之後，彼等實施例之變化對於一般熟習此項技術者而言可變得顯而易見。本發明人期望熟習此項技術者在適當時使用此等變化，且本發明人意欲以不同於如特定描述之其他方式來實踐本發明之實施例。因此，本發明之範圍包括如由適用法律所准許的在隨附於此之申請專利範圍中敘述的主題之所有修改及等效物。此外，除非另外指示或明顯與上下文相矛盾，否則本發明之範圍涵蓋以上描述之要素呈其所有可能變化形式之任何組合。

【0330】 所引用之所有參考文獻(包括公開案、專利申請案及專利)在此以引用之方式併入本文中，該引用程度如同個別及特定地指示每一參考文獻以引用之方式併入且全文闡述於本文中。

【0331】 應注意，上文所提及之實施例說明而非限制本發明，且熟習此項技術者將能夠設計許多替代實施例而不背離本發明之如由隨附申請專利範圍所定義的範圍。在申請專利範圍中，置放於圓括號中之任何參考符號不應被視為限制申請專利範圍。詞「包含」(comprising/comprise)及其類似者並不排除存在除任何請求項或整個說明書中所列出之彼等元件或步驟外的元件或步驟。在本說明書中，「包含(comprises 及 comprising)」意謂「包括或由……組成」。對元件之單數參考並不排除對此類元件之複數參考，且反之亦然。本發明可藉助於包含若干相異元件之硬體且藉助於經合適程式

化之電腦實施。在列舉若干構件之裝置請求項中，此等構件中之若干構件可由硬體之同一個項目體現。在相互不同之附屬請求項中敘述某些措施之純粹實情並不指示不能有利地使用此等措施之組合。

【符號說明】

100 區塊鏈網路

102 節點

104 交易

200 實例實施例

202 先前區塊鏈交易

204 解除鎖定區塊鏈交易

206 第一狀態

208 第二狀態

300 實例

302 先前交易

304 解除鎖定交易

306 鎖定指令碼

400 實例

402 先前交易

404 解除鎖定交易

406 鎖定指令碼

408 解除鎖定指令碼

500 實例

510 經序列化交易

512 步驟

- 514 交易之經修改複本
- 516 訊息*m*
- 600 處理程序
- 602-610 步驟
- 700 實例
- 704 交易
- 706 鎖定指令碼
- 800 實例
- 802A 先前交易
- 802B 先前交易
- 804 解除鎖定交易
- 806 解除鎖定指令碼
- 808 解除鎖定指令碼
- 900 實例
- 904A 解除鎖定交易
- 904B 解除鎖定交易
- 1000 實例
- 1010 經序列化交易
- 1020 散列
- 1100 用於使得插入經序列化交易之處理程序
- 1102-1114 步驟
- 1200 實例
- 1202 先前交易
- 1204 解除鎖定交易

1206 鎖定指令碼

1222A 未判定源

1222B 未判定源

1224 區塊鏈

1300 實例

1302 先前交易

1304 解除鎖定交易

1306 鎖定指令碼

1308 解除鎖定指令碼

1322 未判定源

1324 區塊鏈

1326 經判定源

1400 實例

1402 先前交易

1404 解除鎖定交易

1406 鎖定指令碼

1408 解除鎖定指令碼

1422A 未判定源

1422B 未判定源

1424 區塊鏈

1500 用於安全地佈建未判定資料的處理程序

1502-1506 步驟

1600 經參數化智慧型合約

1602 先前交易

- 1604 解除鎖定交易
- 1606 鎖定指令碼
- 1608 解除鎖定指令碼
- 1700 用於實施經參數化智慧型合約的處理程序
- 1702-1708 步驟
- 1800 實例
- 1804A 解除鎖定交易
- 1804N 解除鎖定交易
- 1806A 指令碼
- 1806N 指令碼
- 1900 實例
- 1902 先前交易
- 1904 自我複寫智慧型合約
- 1904A 解除鎖定交易
- 1904N 解除鎖定交易
- 2000 實例
- 2002 先前交易
- 2004A 第一解除鎖定交易
- 2004B 第二解除鎖定交易
- 2004N 最終解除鎖定交易
- 2100 實例
- 2102 先前交易
- 2104A 第一解除鎖定交易
- 2104B 第二解除鎖定交易

2200 用於具有終止條件之自我複寫智慧型合約的處理程序

2202-2216 步驟

2300 實例

2302 先前交易

2304 解除鎖定交易

2306 狀態規則之集合

2326 輸入

2328A 第一狀態

2328B 第二狀態

2400 實例

2402 先前交易

2404 解除鎖定交易

2406 狀態規則之集合

2426 輸入

2428A 第一狀態

2428B 第二狀態

2430A 狀態

2430B 新狀態

2500 用於去信任確定性狀態機之處理程序

2502-2518 步驟

2600 計算裝置

2602 處理器

2604 匯流排子系統

2606 儲存子系統

- 2608 記憶體子系統
- 2610 檔案或磁碟儲存子系統
- 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 主隨機存取記憶體(RAM)
- 2620 唯讀記憶體(ROM)
- 2624 本端時鐘

發明摘要

※ 申請案號：

※ 申請日：

※IPC 分類：

【發明名稱】(中文/英文)

去信任確定性狀態機之電腦實施方法

TRUSTLESS DETERMINISTIC STATE MACHINE

【中文】

本發明係一去信任確定性狀態機之電腦實施方法。一要驗證的第一交易係在一區塊鏈網路中之一節點處接收。該第一指令碼使該節點至少獲得該第一交易之欄位值之一第一集合、一第二交易之欄位值之一第二集合以及一輸入。獲得該第二交易。該第二指令碼使該節點至少證實該第二指令碼匹配嵌入於欄位值之該第一集合中的一第三指令碼，至少部分地基於欄位值之該第二集合而判定一當前狀態，且至少部分地基於該當前狀態、該輸入及規則之該集合而判定下一狀態。作為執行該第一指令碼及該第二指令碼之結果而驗證該第一交易。

【英文】

The invention relates computer-implemented methods for a trustless, deterministic state machine are described. A first transaction validate is received at a node in a blockchain network. The first transaction causes the node to at least obtain a first set of field values of the first transaction, a second set of field values of a second transaction, and an input. The second transaction is obtained. The second transaction causes the node to at least verify that the second script matches a third script embedded in the first set of field values, determine, based at least in part on the second set of field values, a current state,

and determine, based at least in part on the current state, the input, and the set of rules, a next state. The first transaction is validated as a result of execution of the first script and the second script.

【代表圖】

【本案指定代表圖】：圖 1

【本代表圖之符號簡單說明】：

100 區塊鏈網路

102 節點

104 交易

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

申請專利範圍

1. 一種去信任確定性狀態機之電腦實施方法，其包含：
在一區塊鏈網路中之一節點處接收一第一交易以驗證，該第一交易包括一第一指令碼，作為被執行之一結果，該第一指令碼使該節點至少獲得該第一交易之欄位值之一第一集合、一第二交易之欄位值之一第二集合以及一輸入；
獲得該第二交易，該第二交易包括一第二指令碼，該第二指令碼包括規則之一集合，作為被執行之一結果，該第二指令碼使該節點至少：
證實該第二指令碼匹配嵌入於欄位值之該第一集合中的一第三指令碼；
至少部分地基於欄位值之該第二集合而判定一當前狀態；及
至少部分地基於該當前狀態、該輸入及規則之該集合而判定下一狀態；
證實該下一狀態包括於欄位值之該第一集合中；及
作為執行該第一指令碼及該第二指令碼之結果而驗證該第一交易。
2. 如申請專利範圍第 1 項所述之去信任確定性狀態機之電腦實施方法，其中該第二指令碼約束該輸入之一源的一身分。
3. 如申請專利範圍第 1 項或第 2 項所述之去信任確定性狀態機之電腦實施方法，其進一步包含證實該輸入之一源的一密碼編譯秘密。
4. 如申請專利範圍第 1 項至第 3 項中任一項所述之去信任確定性狀態機之電腦實施方法，其中規則之該集合係一狀態轉移矩陣。
5. 如申請專利範圍第 1 項至第 4 項中任一項所述之去信任確定性狀態機之電腦實施方法，其中該第三指令碼係強加用於驗證一未來交易之條件之一集合的一鎖定指令碼。
6. 如申請專利範圍第 1 項至第 5 項中任一項所述之去信任確定性狀態機

之電腦實施方法，其中該第二指令碼進一步使該節點判定一終止條件未滿足。

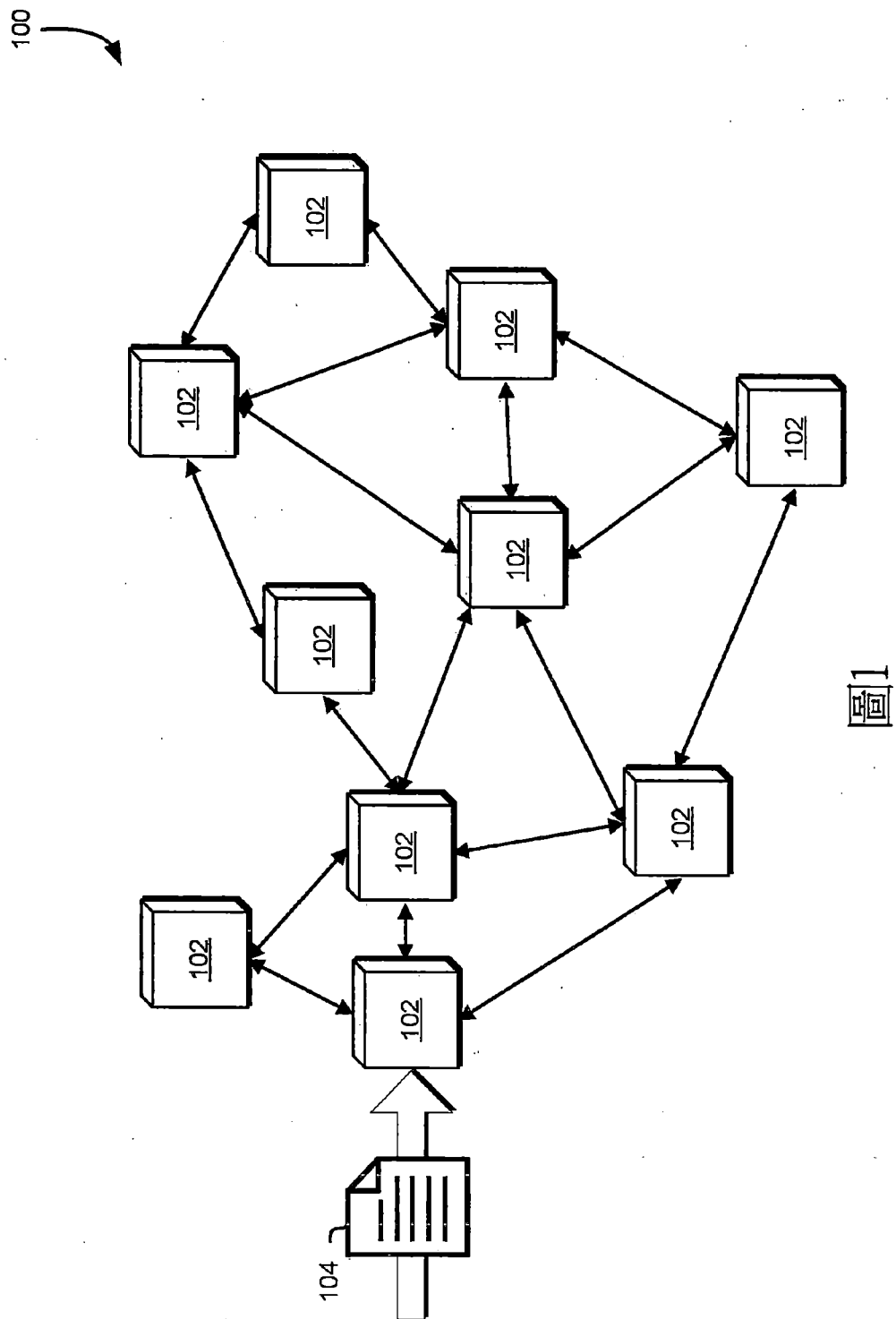
7. 如申請專利範圍第 1 項或第 3 項至第 6 項中任一項所述之去信任確定性狀態機之電腦實施方法，其中該輸入嵌入於欄位值之該第二集合中。
8. 如申請專利範圍第 6 項所述之去信任確定性狀態機之電腦實施方法，其中終止條件係與該第二交易相關聯之一數位資產的大小不足以被傳送。
9. 如申請專利範圍第 1 項至第 8 項中任一項所述之去信任確定性狀態機之電腦實施方法，其中該當前狀態指示該第二交易之一狀態。
10. 如申請專利範圍第 1 項至第 9 項中任一項所述之去信任確定性狀態機之電腦實施方法，其中該下一狀態指示該第一交易在驗證後之一狀態。
11. 如申請專利範圍第 1 項至第 10 項中任一項所述之去信任確定性狀態機之電腦實施方法，其進一步包含：
接收一第三交易；及
自該第一交易獲得一第四指令碼，作為被執行之一結果，該第四指令碼使該節點至少部分地基於該下一狀態、一第二輸入及規則之該集合而判定不同於該下一狀態及該當前狀態之另一狀態。
12. 如申請專利範圍第 1 項至第 11 項中任一項所述之去信任確定性狀態機之電腦實施方法，其中該當前狀態及該下一狀態係該第一交易及該第二交易之可能狀態之一集合的成員。
13. 如申請專利範圍第 1 項至第 12 項中任一項所述之去信任確定性狀態機之電腦實施方法，其中驗證該第一交易包括使來自一第一實體之一數位資產重新關聯至一第二實體。
14. 一種系統，其包含：

一處理器；及

記憶體，其包括可執行指令，作為由該處理器執行之一結果，該等可執行指令使該系統執行如申請專利範圍第 1 項至第 13 項中任一項所述之方法。

15. 一種非暫時性電腦可讀儲存媒體，其具有儲存於其上之可執行指令，作為由一電腦系統之一處理器執行的一結果，該等可執行指令使該電腦系統至少執行如申請專利範圍第 1 項至第 13 項中任一項所述之方法。

圖式



200

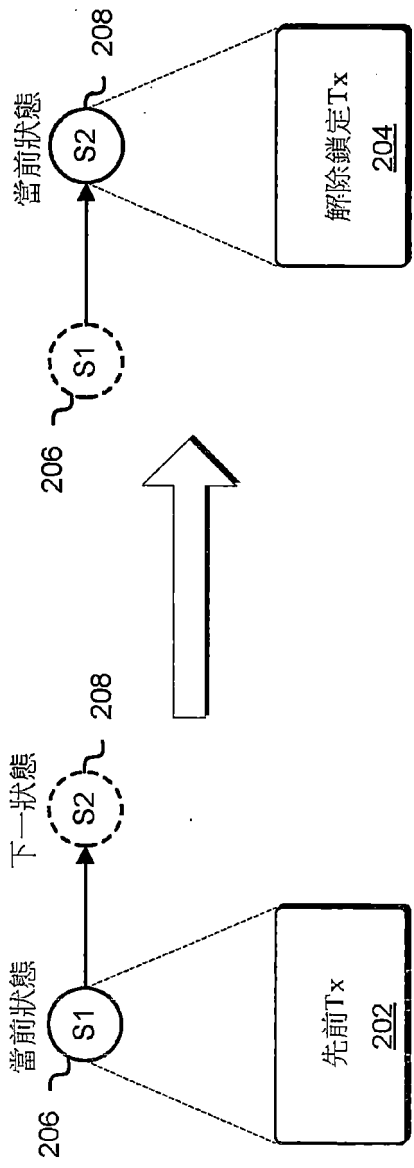


圖2

300

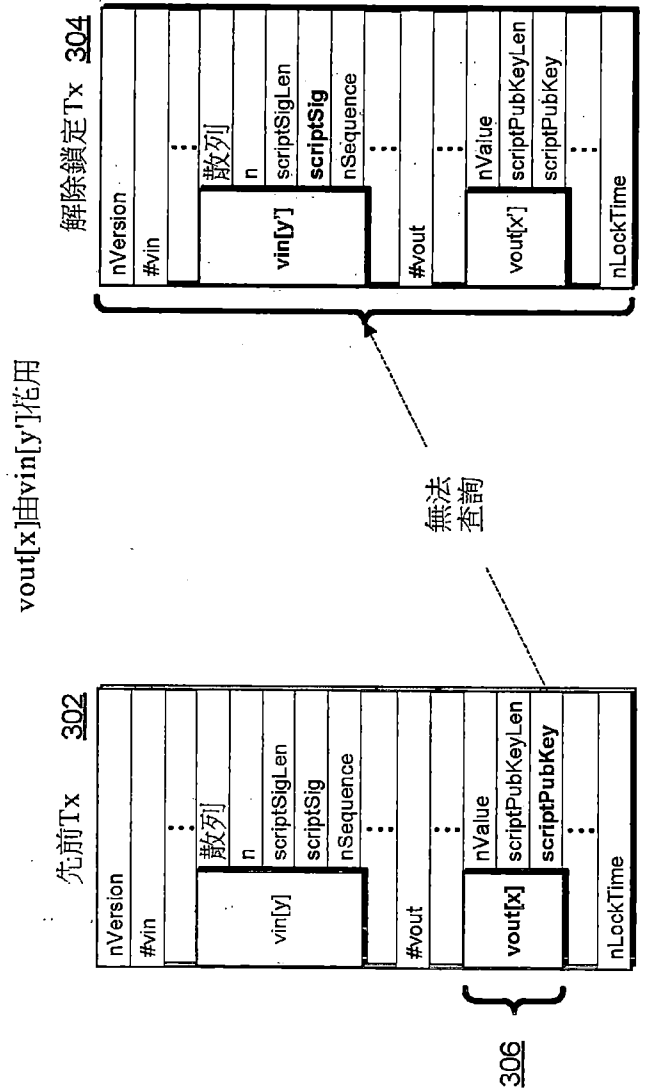


圖3

400

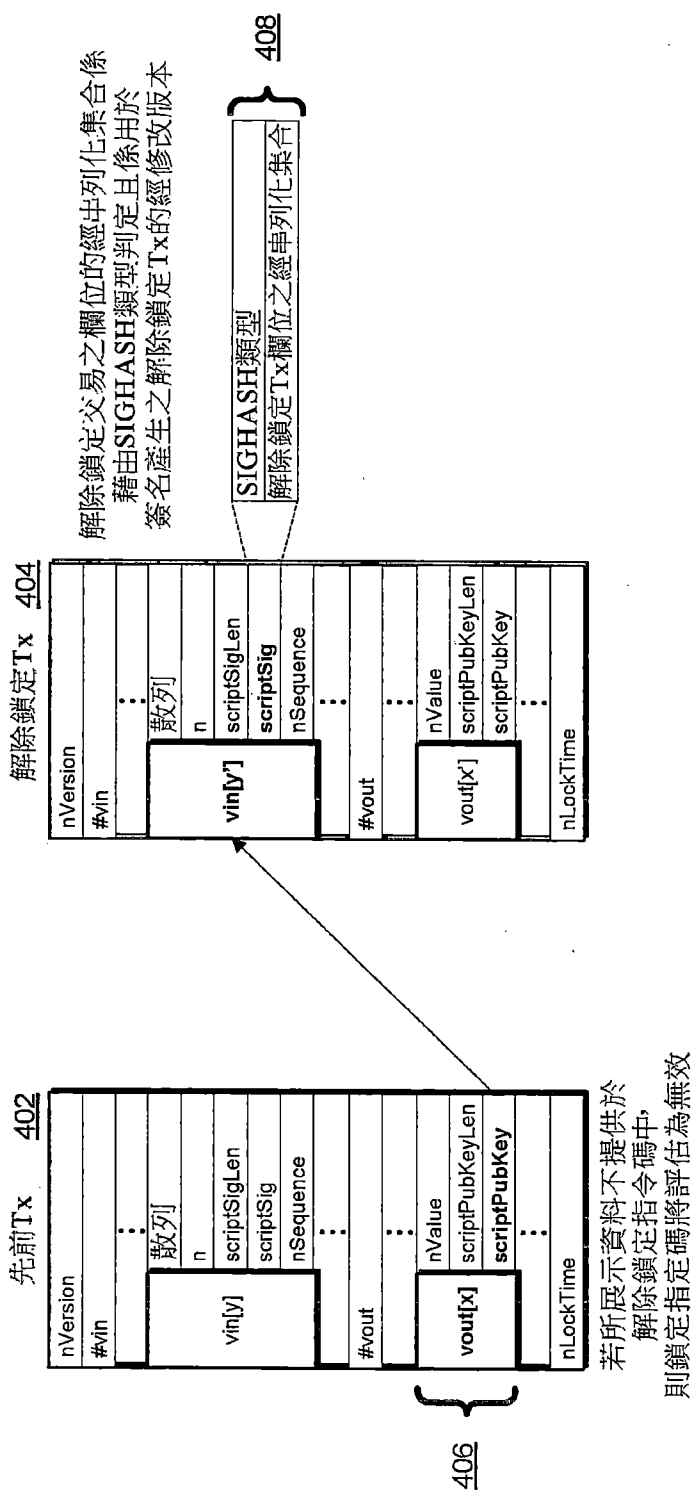


圖4

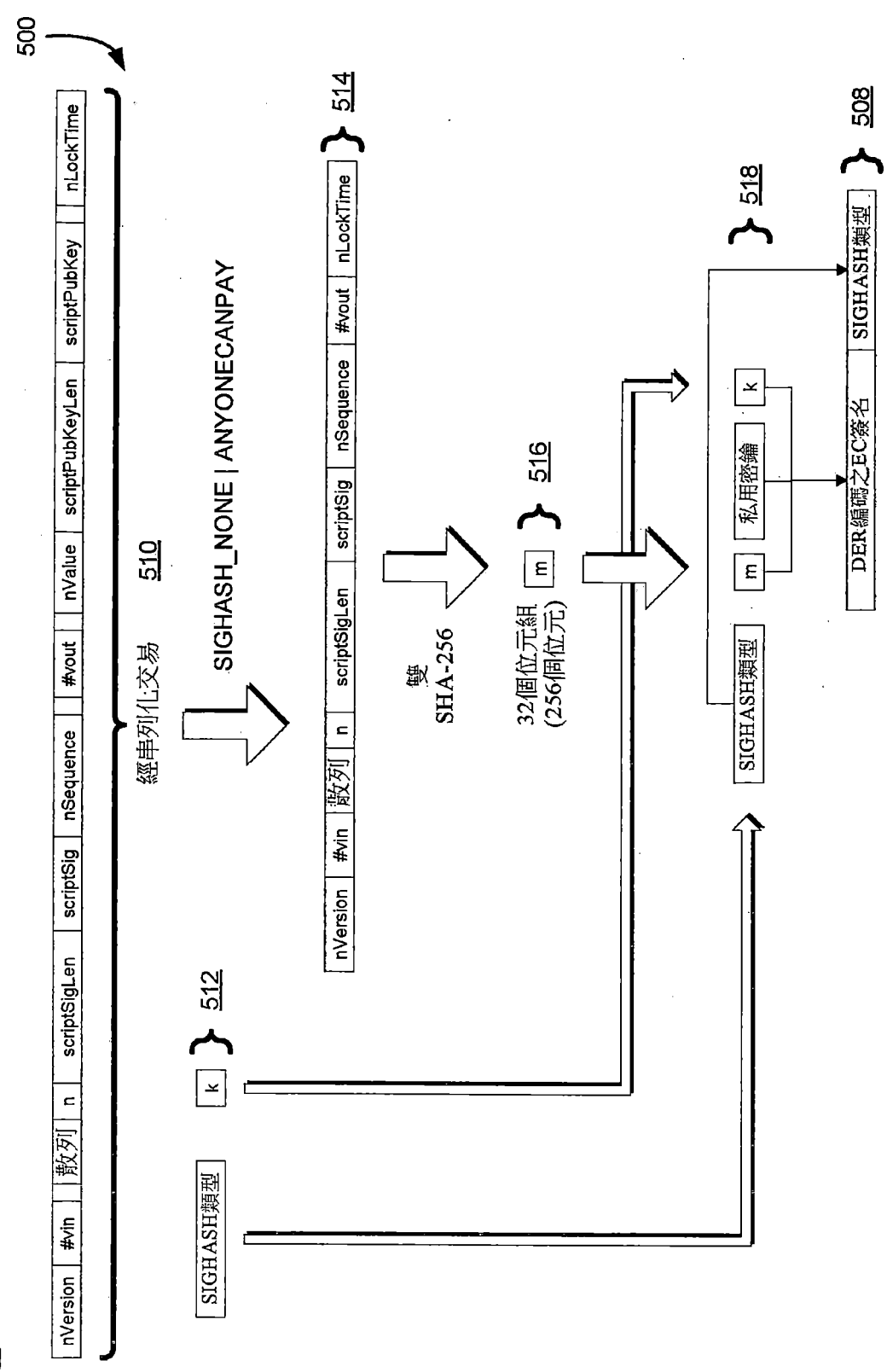


圖5

600

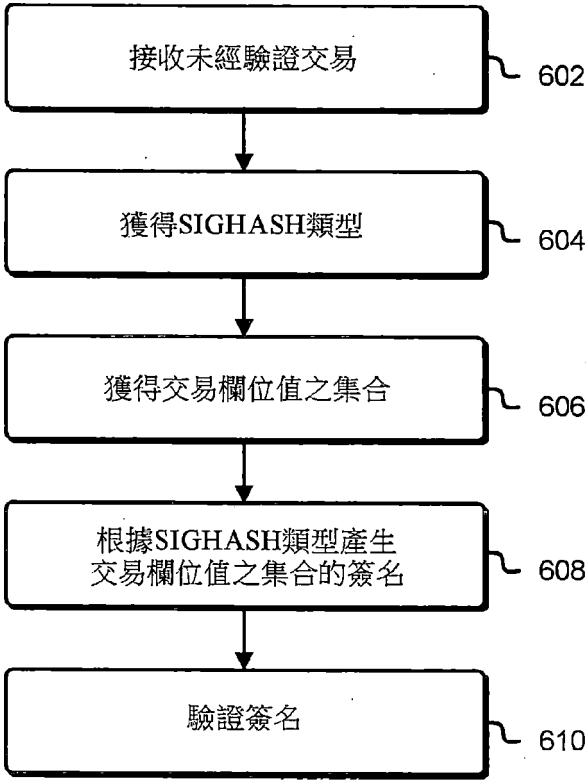


圖6

700

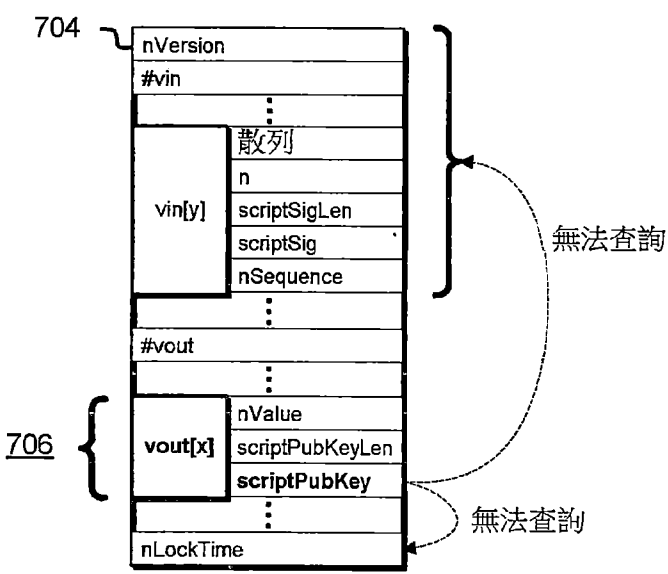


圖7

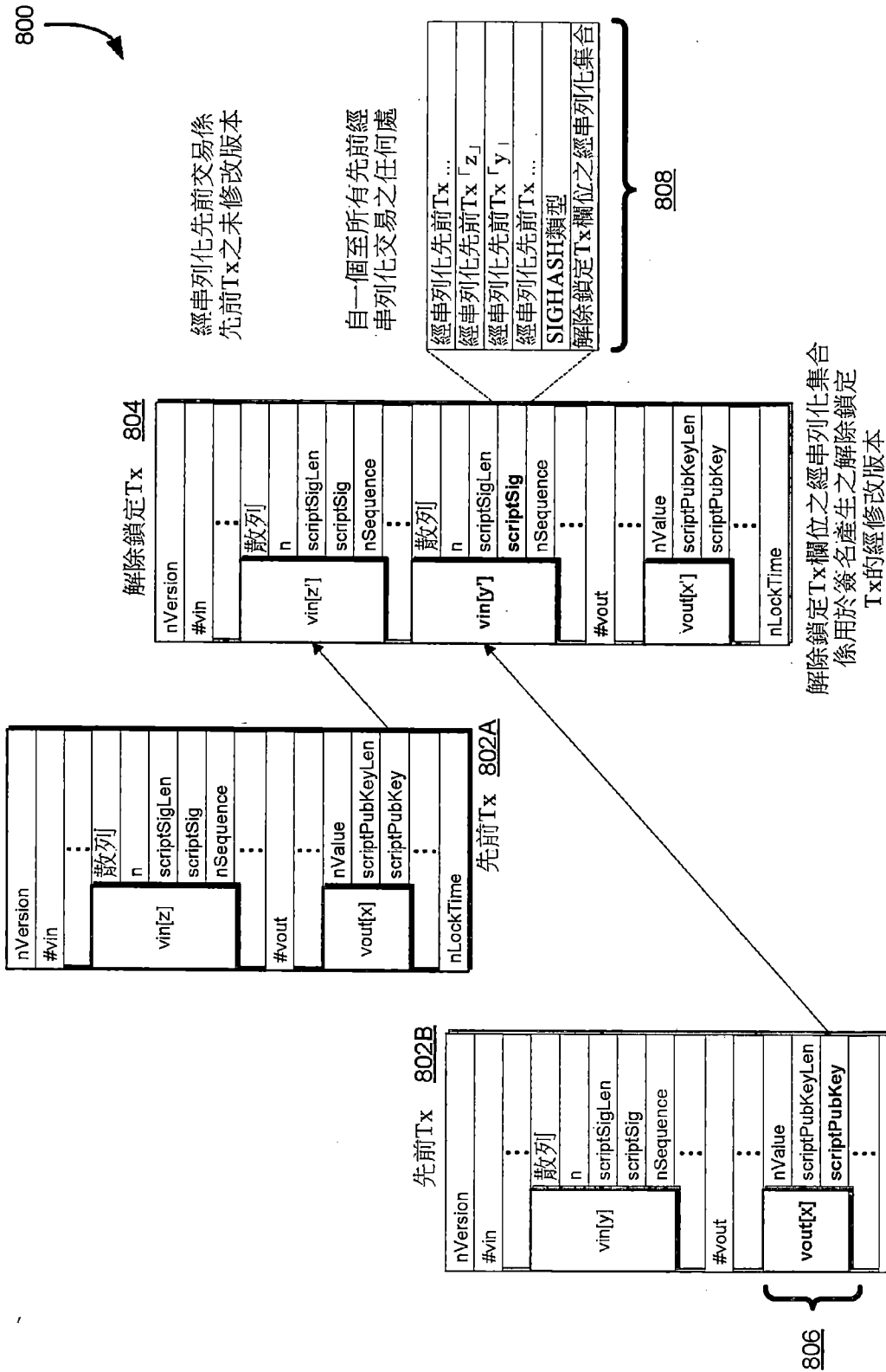
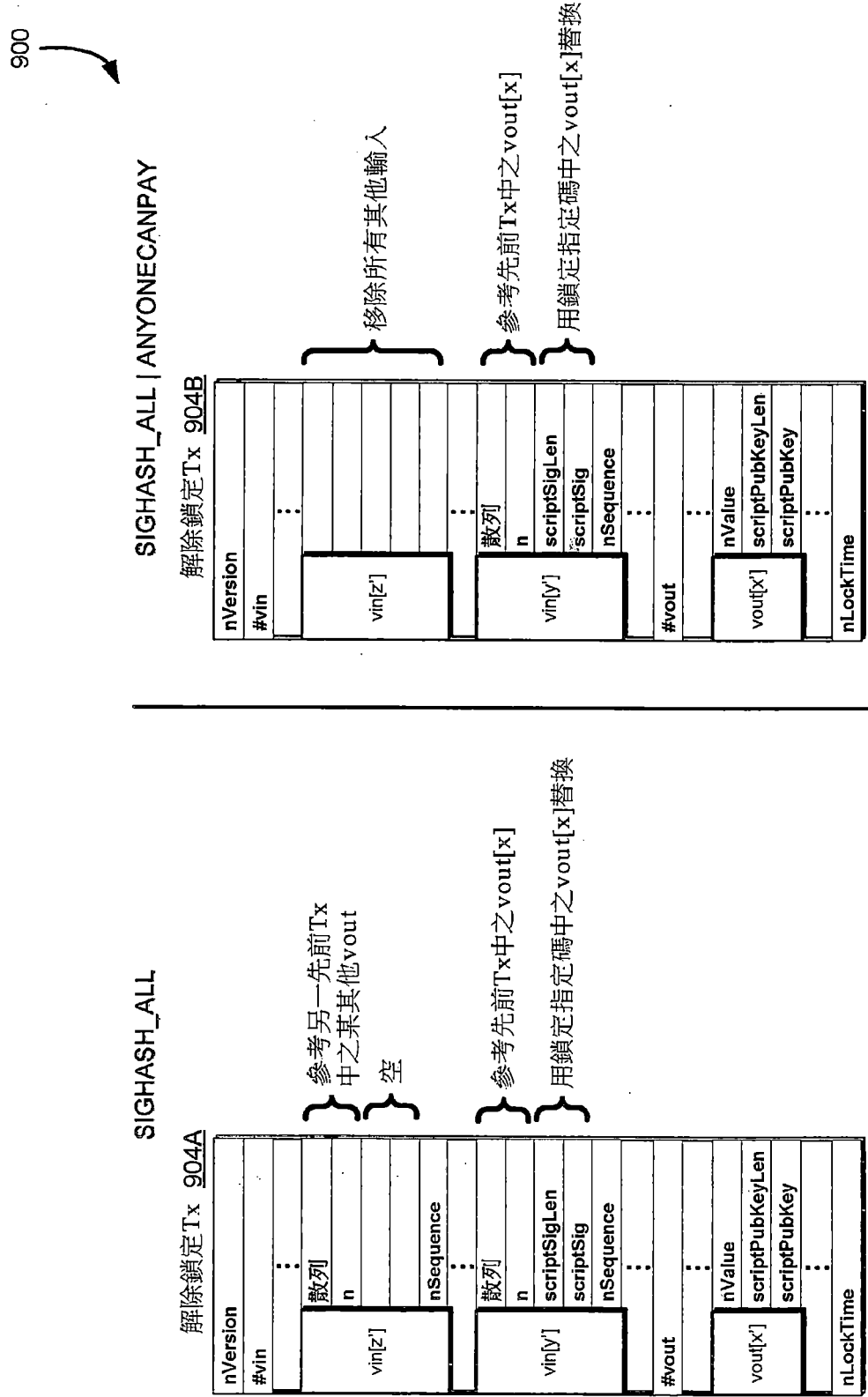


圖8



900



圖9

1000

經序列化交易 1010

nVersion	#vin	散列	n	scriptSigLen	scriptSig	nSequence	#vout	nValue	scriptPubKeyLen	scriptPubKey	nLockTime
----------	------	----	---	--------------	-----------	-----------	-------	--------	-----------------	--------------	-----------

交易欄位之集合的子串

散列

1020

圖10

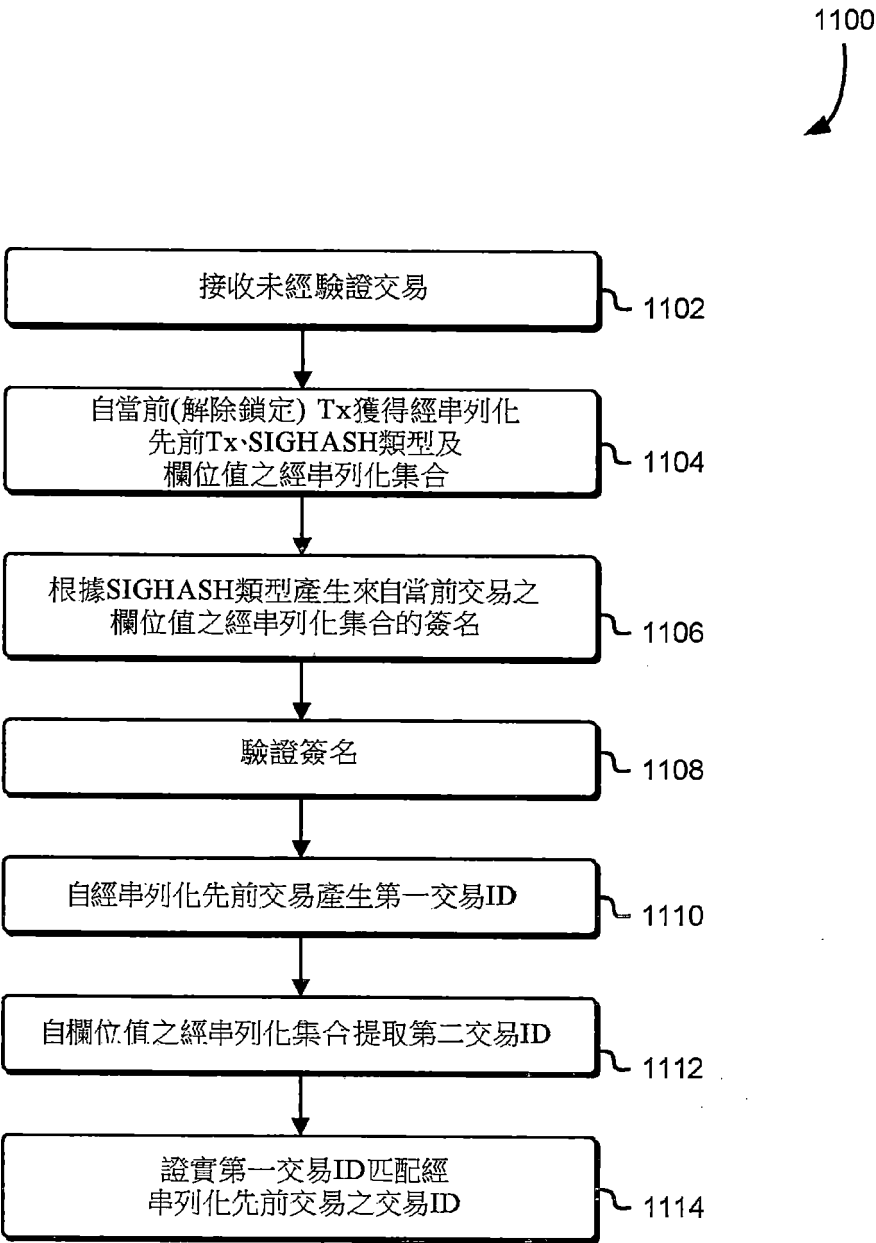


圖11

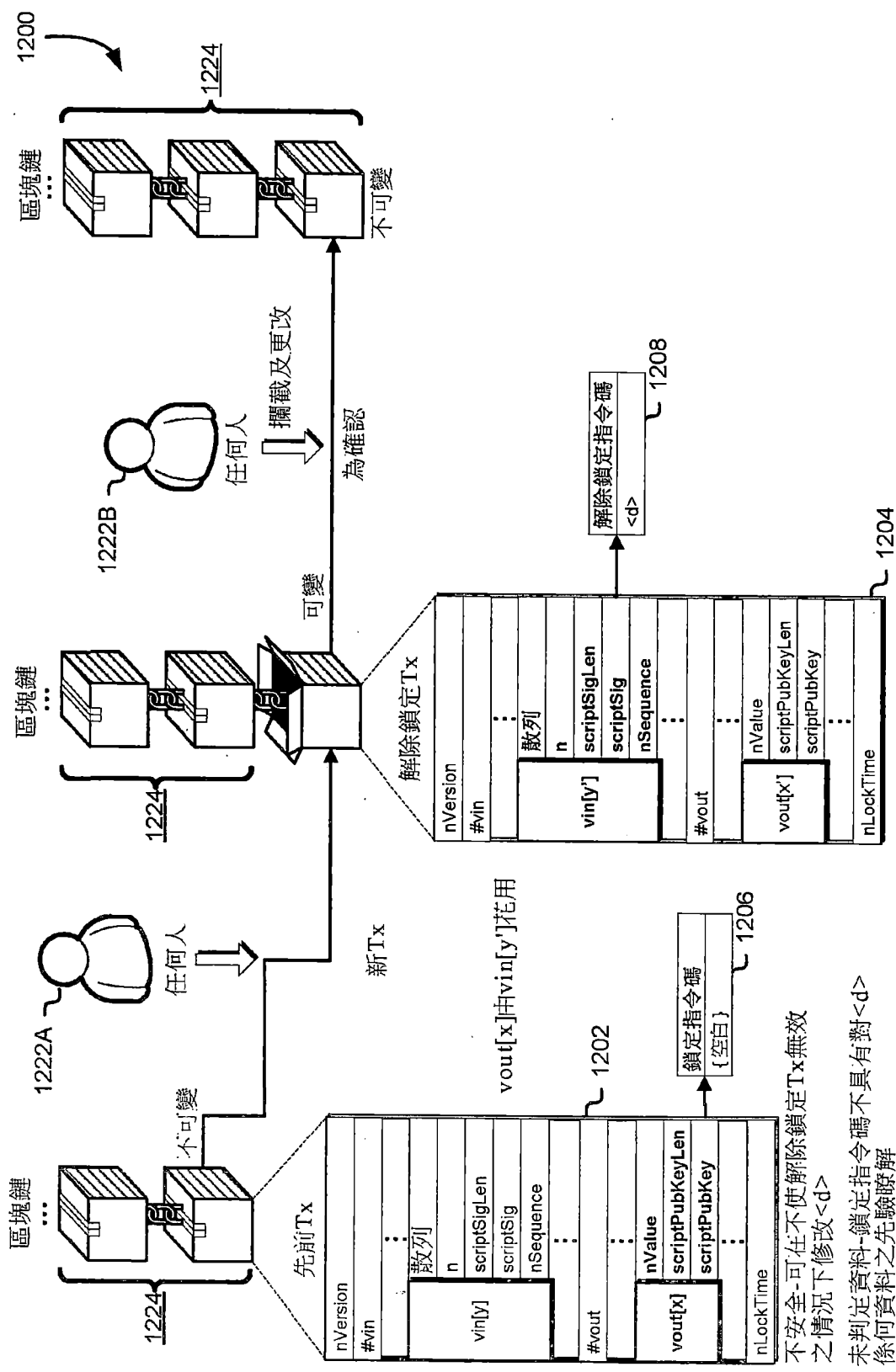


圖12

不安全-可在不使解除鎖定Tx無效之情況下修改<d>
未判定資料-鎖定指令碼不具有對<d>係何資料之先驗瞭解
未判定源-鎖定指令碼不瞭解誰將提供<d>

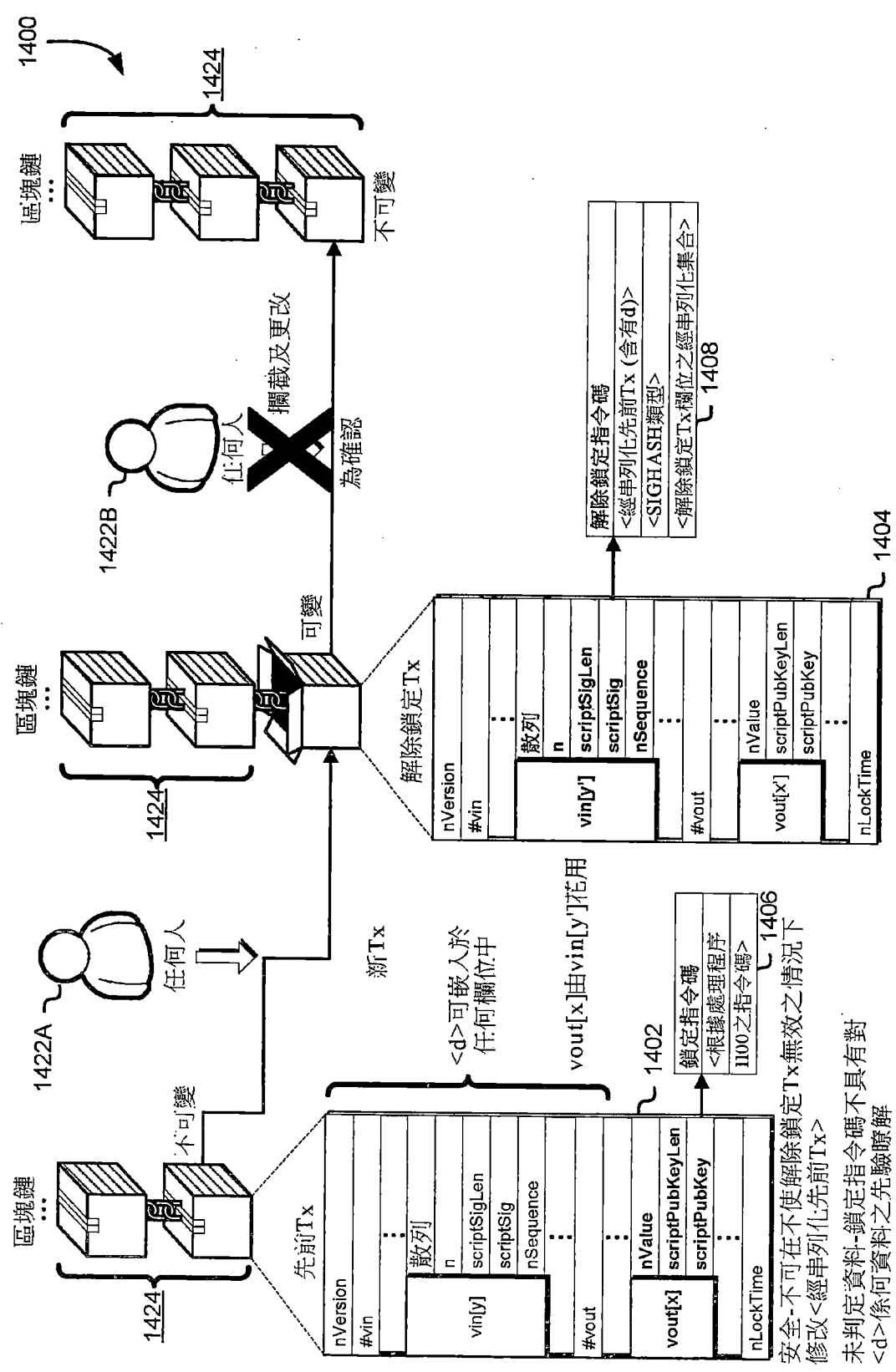


圖14

1500

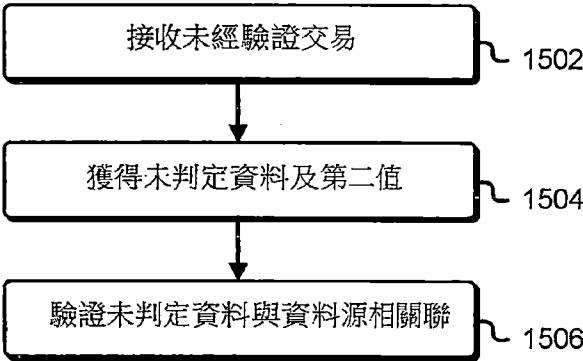


圖15

1600

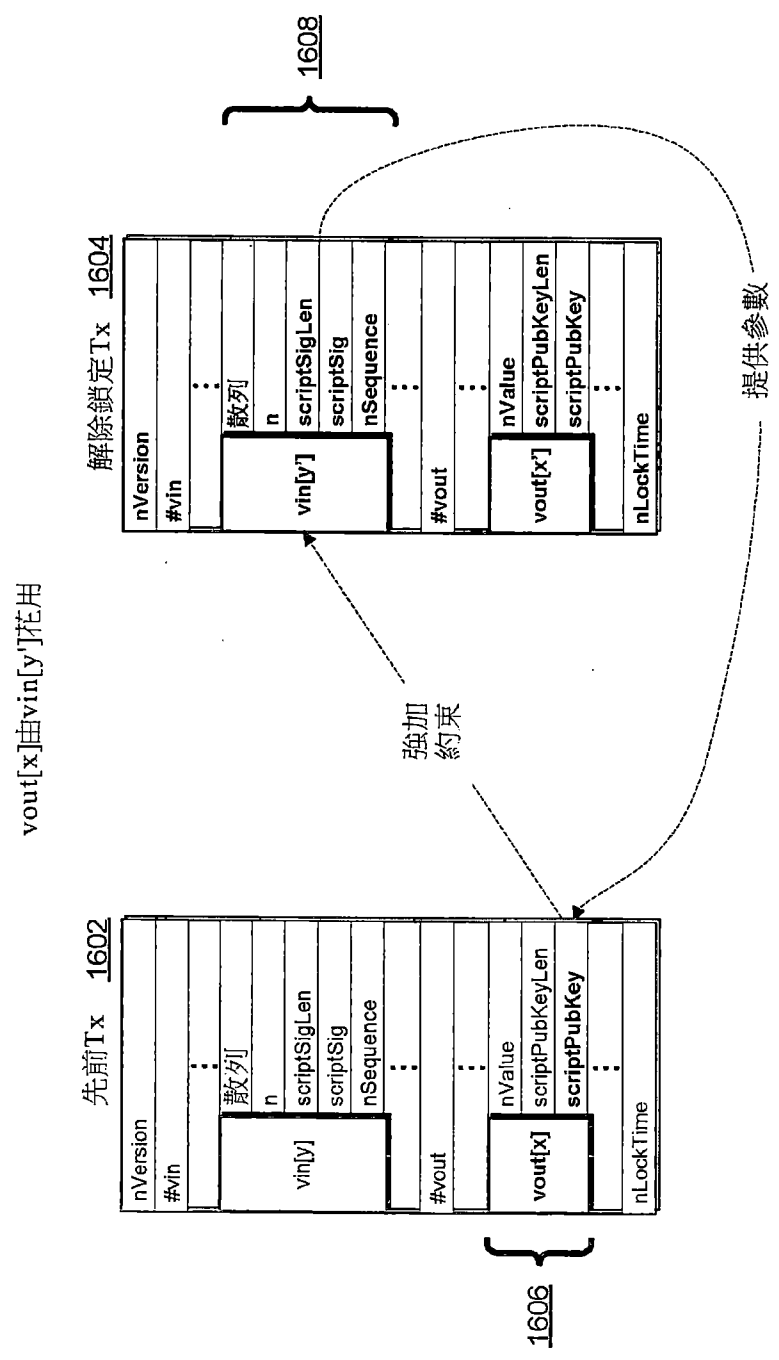


圖16

1700

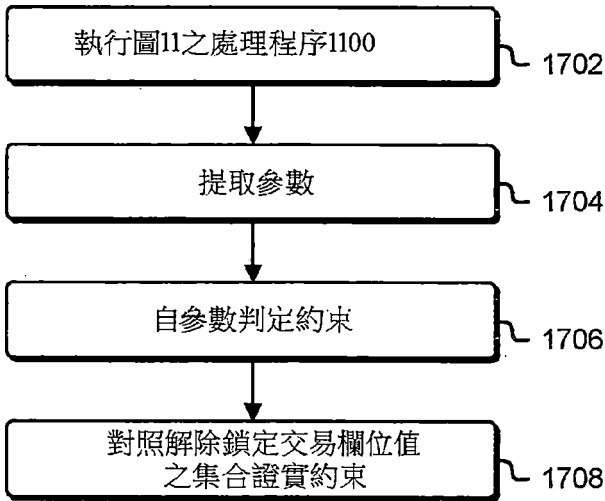
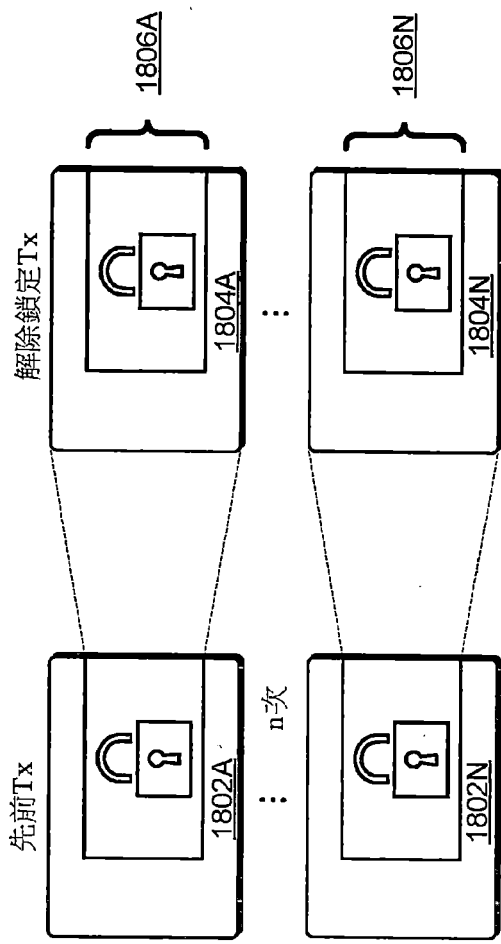


圖17

1800



註釋

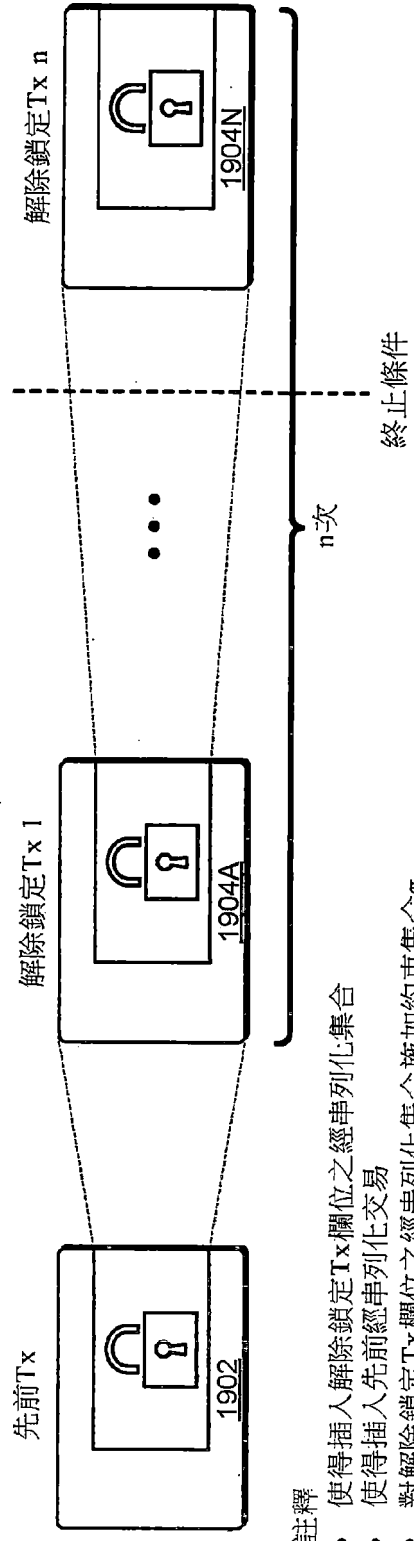
- 使得插入解除鎖定Tx欄位之經序列化集合
- 使得插入先前經序列化交易
- 對解除鎖定Tx欄位之經序列化集合施加約束集合 π

圖18

1900



解決方案



註釋

- 使得插入解除鎖定Tx欄位之經序列化集合
- 使得插入先前經序列化交易
- 對解除鎖定Tx欄位之經序列化集合施加約束集合 π
- 除非終止條件為真,否則對解除鎖定Tx欄位之經序列化集合施加約束以複製鎖定指令碼

圖19

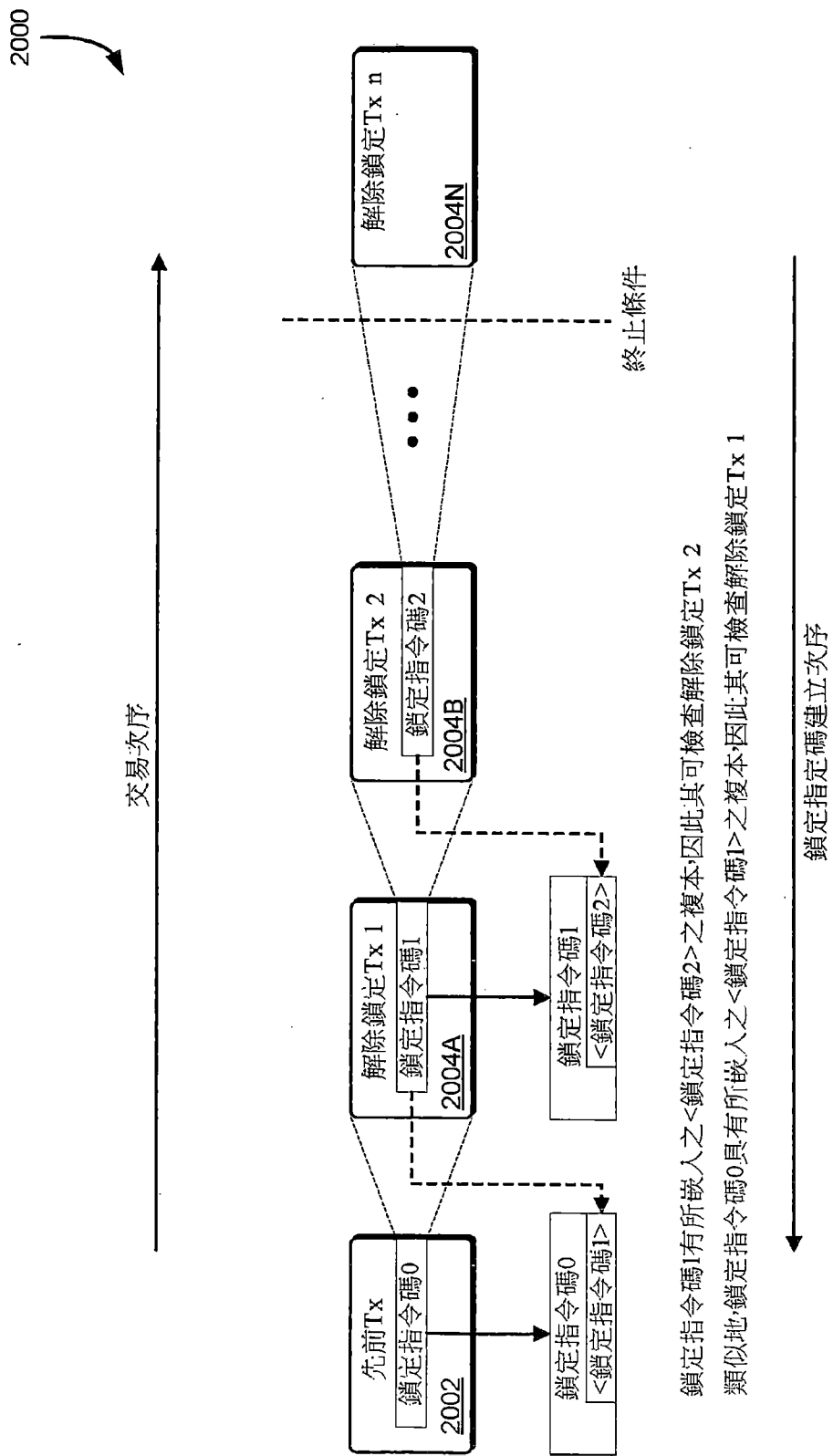


圖20

鎖定指令碼1有所嵌入之<鎖定指令碼2>之複本·因此其可檢查解除鎖定Tx 2
類似地·鎖定指令碼0具有所嵌入之<鎖定指令碼1>之複本·因此其可檢查解除鎖定Tx 1

2100

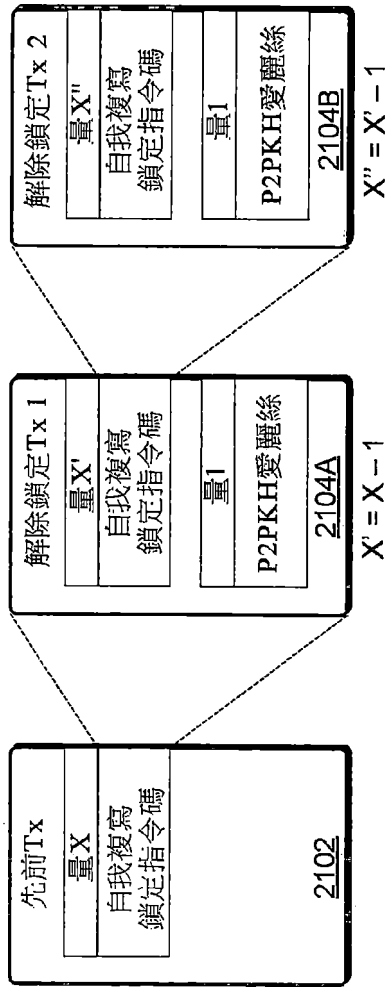


圖21

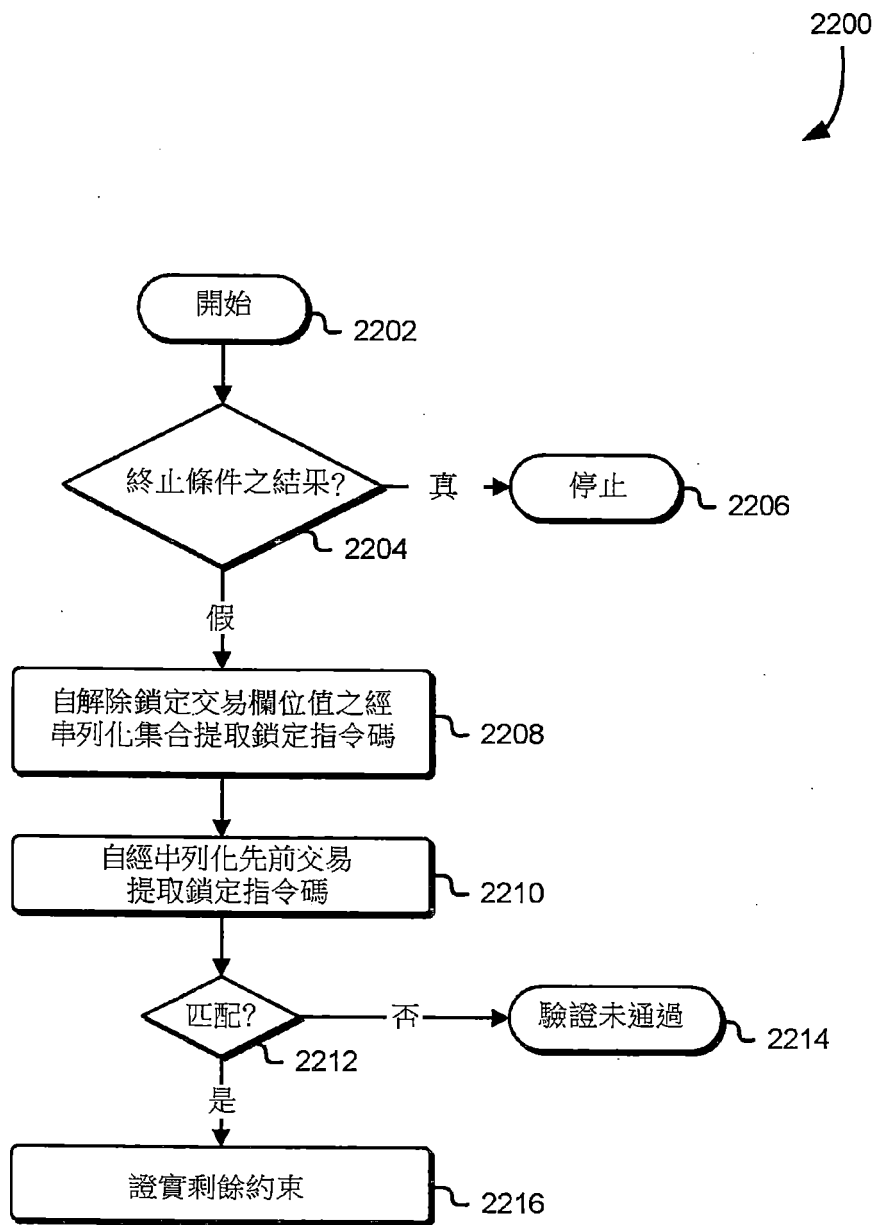


圖22

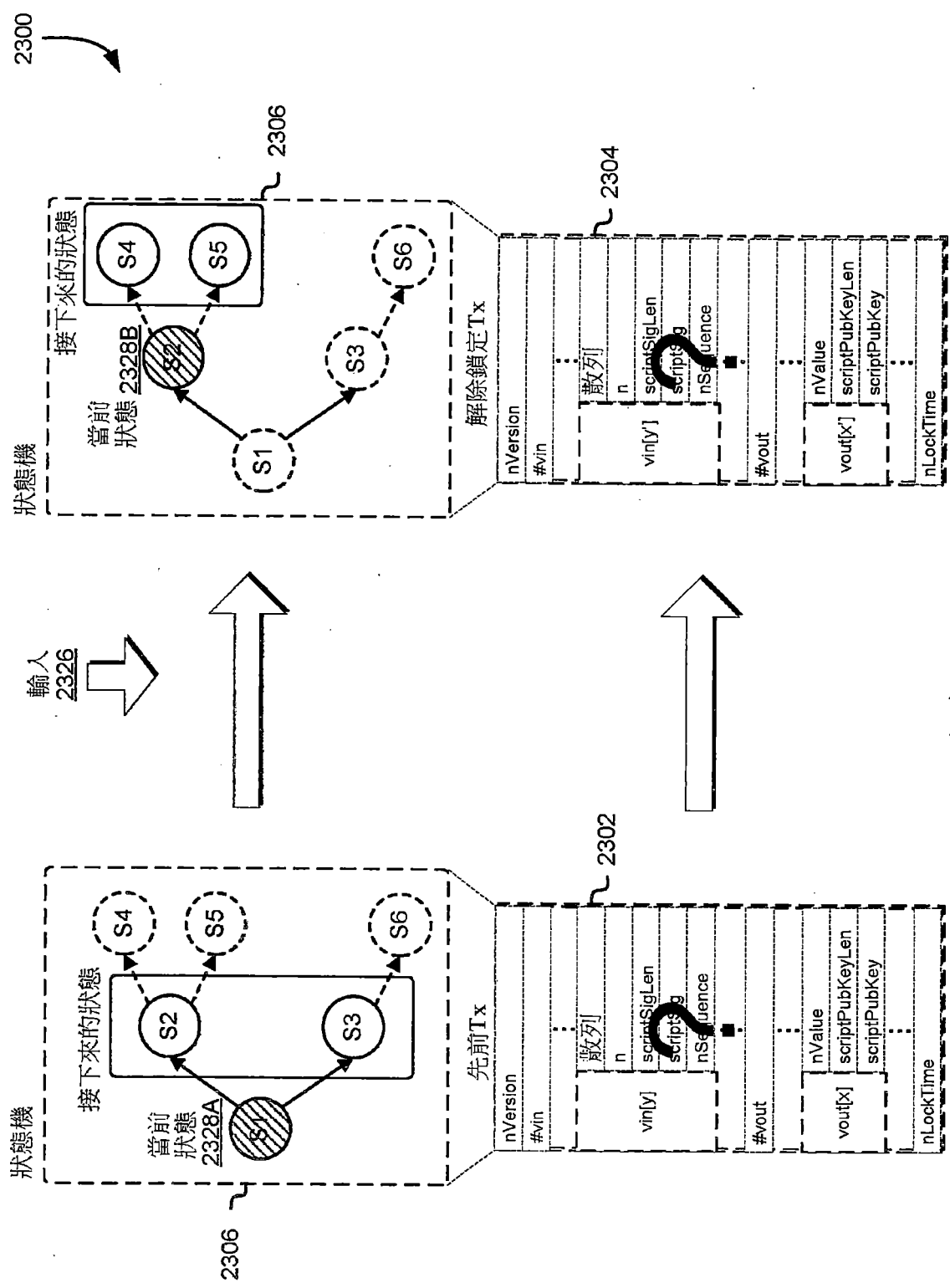
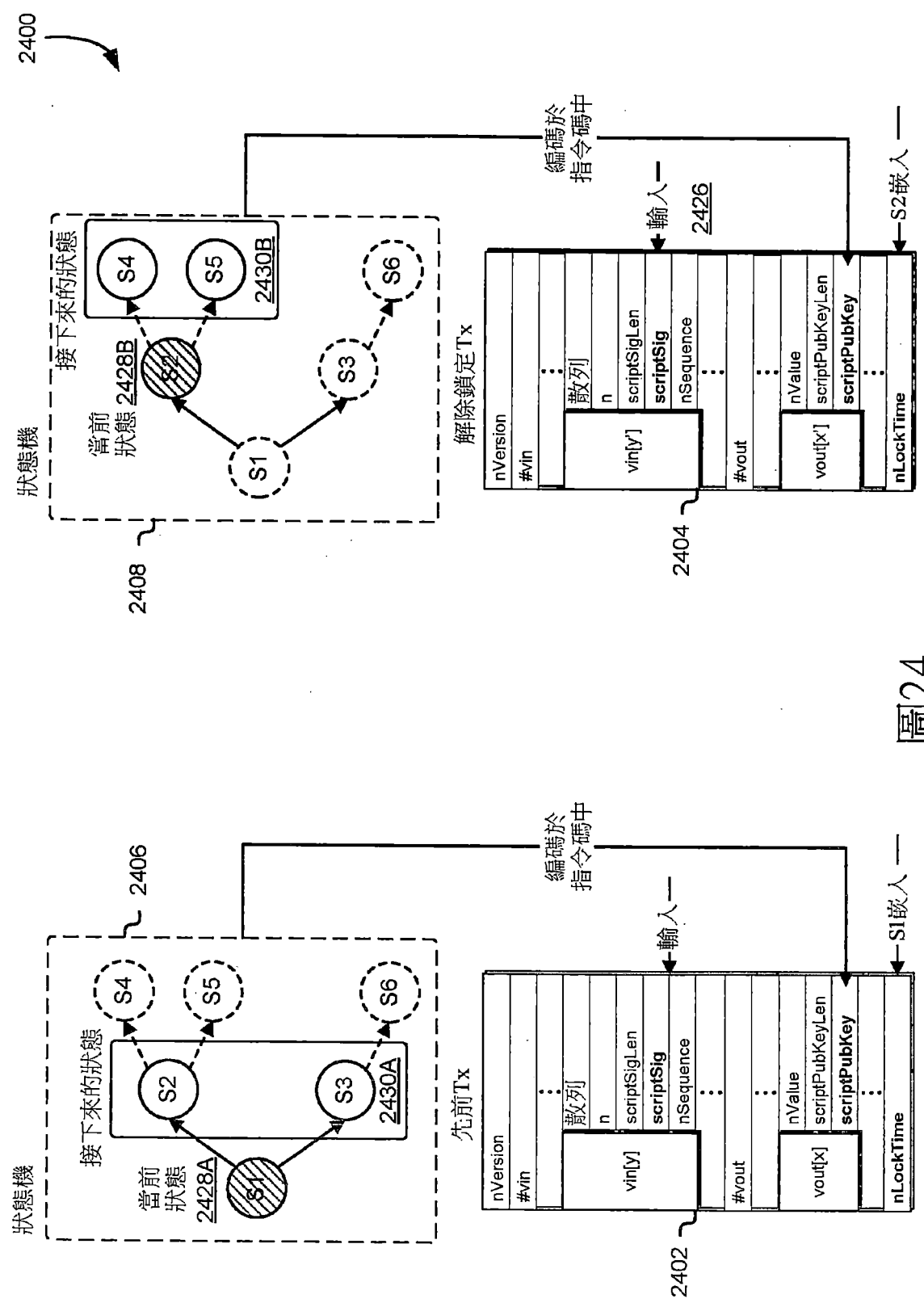


圖 23



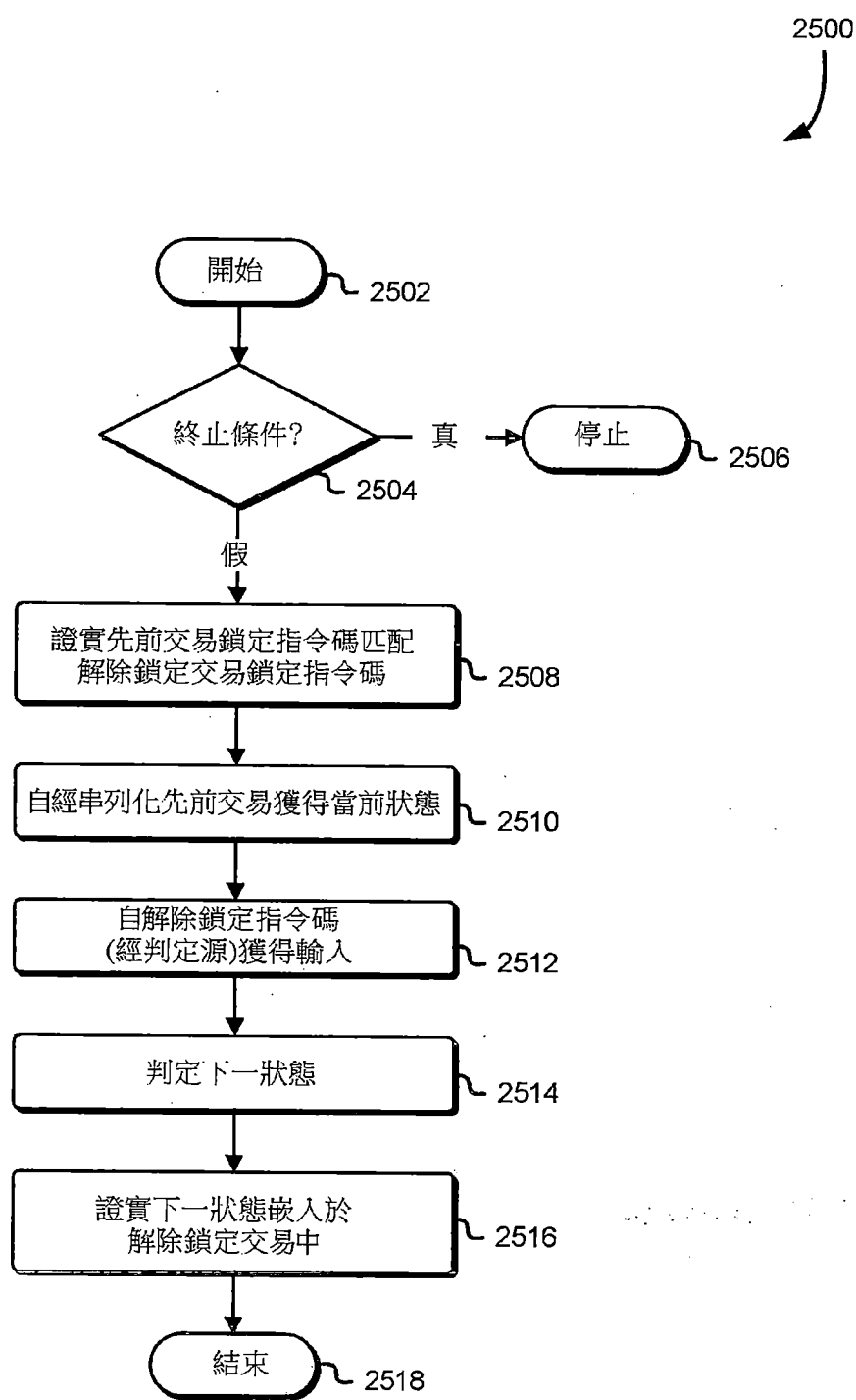


圖25

2600

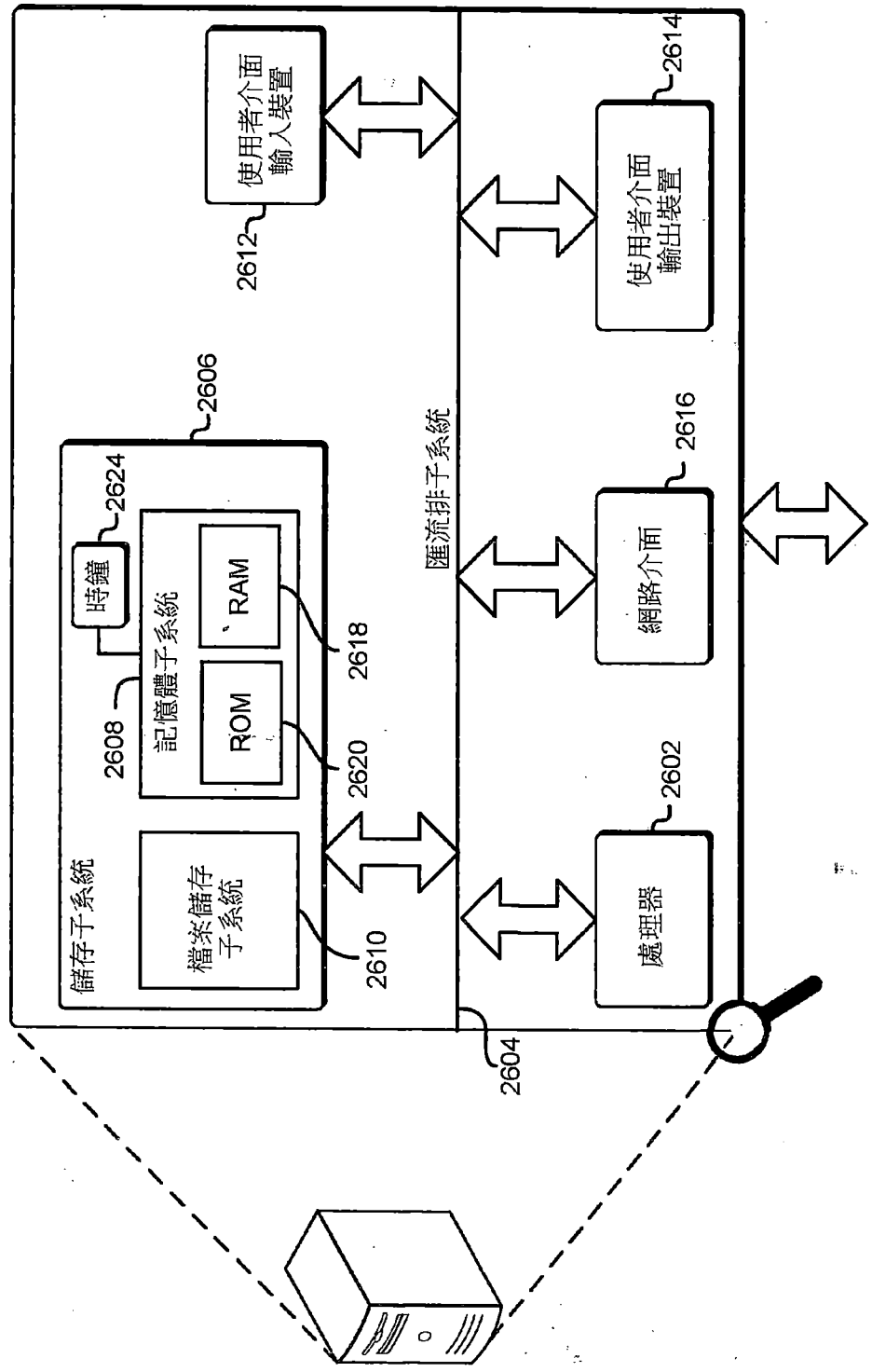


圖26