(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0033277**

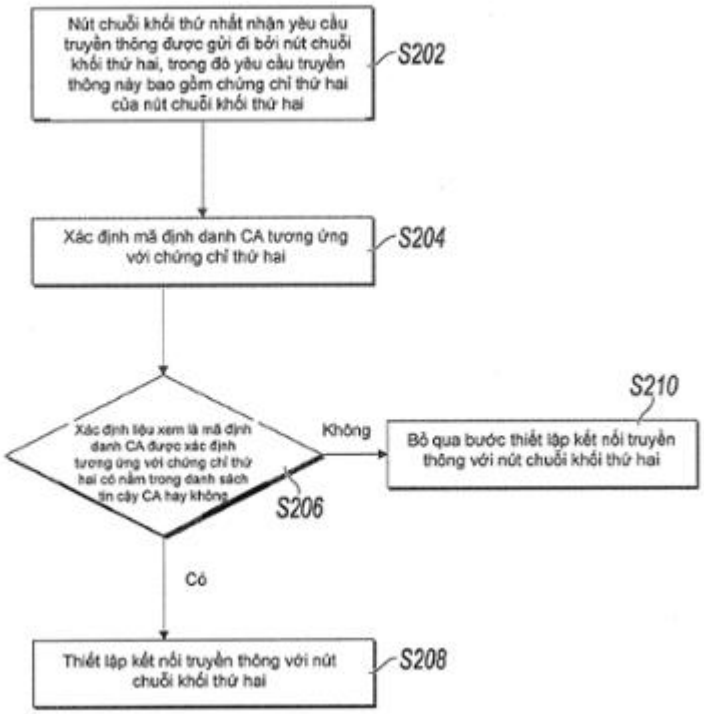
(51)[7] **G06F 21/64**; H04W 12/02; H04L 29/06; G06F 21/62; G06Q 20/06

(13) **B**

(21) 1-2019-04105
(22) 26/07/2018
(86) PCT/US2018/043927 26/07/2018
(87) WO 2019/023475 31/01/2019
(30) 201710617463.6 26/07/2017 CN
(45) 25/09/2022 414
(43) 25/05/2020 386ASC
(73) Advanced New Technologies Co., Ltd. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) QIU, Honglin (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP, PHƯƠNG TIỆN VÀ THIẾT BỊ TRUYỀN THÔNG NÚT CHUỖI KHỐI

(57) Sáng chế đề cập đến phương pháp, phương tiện và thiết bị truyền thông nút chuỗi khối. Yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai được nhận bởi nút chuỗi khối thứ nhất của mạng chuỗi khối, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai, và trong đó mạng chuỗi khối này bao gồm nút dịch vụ để lưu chứng chỉ được gửi bởi bên cung cấp chứng chỉ (Certificate Authority, CA) và được tạo cấu hình trước bởi danh sách tin cậy CA. Mã định danh CA tương ứng với chứng chỉ thứ hai được xác định. Việc xem liệu mã định danh CA được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không được xác định. Nếu có, thì kết nối truyền thông với nút chuỗi khối thứ hai được thiết lập. Nếu không, thì bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai được bỏ qua.


Nút chuỗi khối thứ nhất nhận yêu cầu truyền thông được gửi đi bởi nút chuỗi khối thứ hai, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai
S202
Xác định mã định danh CA tương ứng với chứng chỉ thứ hai
S204
Xác định liệu xem là mã định danh CA được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không
S206
Không
S210
Bỏ qua bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai
Có
Thiết lập kết nối truyền thông với nút chuỗi khối thứ hai
S208

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ thông tin, và cụ thể là phương pháp, phương tiện và thiết bị truyền thông nút chuỗi khối.

Tình trạng kỹ thuật của sáng chế

Là một nhánh của công nghệ chuỗi khối, công nghệ chuỗi khối tập đoàn ngày càng được sử dụng rộng rãi. Các nút chuỗi khối trong mạng chuỗi khối tập đoàn bao gồm các nút dịch vụ và các nút đồng thuận. Nút dịch vụ này tham gia vào trong dịch vụ, và nút đồng thuận này chịu trách nhiệm đối với việc nhận dữ liệu dịch vụ được gửi bởi nút dịch vụ và thực hiện việc xác minh đồng thuận đối với dữ liệu dịch vụ.

Nút dịch vụ được mô tả ở trên là máy chủ dịch vụ của mỗi tổ chức tham gia mạng chuỗi khối tập đoàn, và phần mềm được cài đặt trên máy chủ để truyền thông với nút khác trong mạng chuỗi khối tập đoàn (trong bản mô tả này, phần mềm được gọi là "chương trình truyền thông").

Fig.1 là sơ đồ kiến trúc minh họa mạng chuỗi khối tập đoàn. Như được thể hiện trên Fig.1, các vòng tròn đặc là các nút đồng thuận, và các vòng tròn rỗng là các nút dịch vụ. Các nút dịch vụ khác nhau cung cấp các dịch vụ cho các ứng dụng khác nhau (Application, APP). Nút dịch vụ này gửi dữ liệu dịch vụ được tạo ra bởi APP đến nút đồng thuận để xác minh đồng thuận. Giả sử là nút dịch vụ là một máy chủ tương ứng với ứng dụng dịch vụ ăn uống, nút dịch vụ khác là máy chủ tương ứng với ứng dụng thanh toán. Người dùng có thể thực hiện thanh toán thông qua ứng dụng thanh toán sau khi thực hiện đặt món thông qua ứng dụng dịch vụ ăn uống, như vậy, hai nút dịch vụ này có thể tham gia vào cùng một dịch vụ, và có thể đăng ký mối tương quan dịch vụ như được thể hiện trên Fig.1 với mạng chuỗi khối tập đoàn.

Trong mạng chuỗi khối tập đoàn, mỗi nút dịch vụ lưu trữ dữ liệu dịch vụ của dịch vụ mà nút dịch vụ này tham gia, và dữ liệu dịch vụ này thường bao gồm dữ liệu riêng tư của người dùng. Dựa vào công nghệ hiện có, cần có phương pháp truyền

thông bảo mật hơn.

Bản chất kỹ thuật của sáng chế

Một hoặc nhiều phương án thực hiện của sáng chế đề xuất phương pháp truyền thông nút chuỗi khối, để giải quyết vấn đề, trong công nghệ hiện có, lộ dữ liệu cá nhân có thể bị xảy ra khi các nút dịch vụ trong mạng chuỗi khối thực hiện việc truyền thông.

Một hoặc nhiều phương án thực hiện của sáng chế đề xuất phương tiện truyền thông nút chuỗi khối, để giải quyết vấn đề, trong công nghệ hiện có, lộ dữ liệu cá nhân có thể bị xảy ra khi các nút dịch vụ trong mạng chuỗi khối thực hiện việc truyền thông.

Các giải pháp kỹ thuật dưới đây được sử dụng theo các phương án thực hiện của sáng chế:

Phương pháp truyền thông nút chuỗi khối được đề xuất. Các nút chuỗi khối trong mạng chuỗi khối bao gồm nút dịch vụ. Nút dịch vụ này lưu trữchứng chỉ được gửi bởi bên cung cấp chứng chỉ (Certificate Authority, CA), và được tạo cấu hình trước bởi danh sách tin cậy CA. Phương pháp này bao gồm các bước: nhận, bởi nút chuỗi khối thứ nhất, yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai; xác định mã định danh CA tương ứng với chứng chỉ thứ hai này; xác định xem liệu mã định danh CA đã được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không; và nếu có, thì thiết lập kết nối truyền thông với nút chuỗi khối thứ hai; hoặc nếu không, thì bỏ qua bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai.

Phương tiện truyền thông nút chuỗi khối được đề xuất, và phương tiện này bao gồm: môđun nhận, được tạo cấu hình để nhận yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai; môđun xác định, được tạo cấu hình để xác định mã định danh CA tương ứng với chứng chỉ thứ hai này; và môđun xác định và thực thi, được tạo cấu hình để xác định xem liệu mã định danh CA đã được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không; và nếu có, thì thiết lập kết nối truyền thông với nút chuỗi khối thứ hai; hoặc nếu không, thì bỏ qua bước thiết lập

kết nối truyền thông với nút chuỗi khối thứ hai; trong đó các nút chuỗi khối trong mạng chuỗi khối bao gồm nút dịch vụ, và nút dịch vụ này lưu chứng chỉ được gửi bởi CA, và được tạo cấu hình trước bởi danh sách tin cậy CA.

Thiết bị truyền thông nút chuỗi khối được đề xuất. Thiết bị truyền thông này bao gồm một hoặc nhiều bộ xử lý và bộ nhớ. Bộ nhớ này lưu chương trình, và chương trình này được thực thi bởi một hoặc nhiều bộ xử lý để thực hiện các bước sau: nhận, ở nút chuỗi khối thứ nhất, yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai; xác định mã định danh CA tương ứng với chứng chỉ thứ hai này; xác định xem liệu mã định danh CA đã được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không; và nếu có, thì thiết lập kết nối truyền thông với nút chuỗi khối thứ hai; hoặc nếu không, thì bỏ qua bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai; trong đó các nút chuỗi khối trong mạng chuỗi khối bao gồm nút dịch vụ, và nút dịch vụ này lưu chứng chỉ được gửi bởi CA, và được tạo cấu hình trước bởi danh sách tin cậy CA.

Một hoặc nhiều giải pháp kỹ thuật được sử dụng theo một hoặc nhiều phương án thực hiện của sáng chế có thể đạt được các hiệu quả có lợi sau đây:

Nút dịch vụ trong mạng chuỗi khối lưu chứng chỉ được gửi bởi CA, và được tạo cấu hình trước bởi danh sách tin cậy CA. Khi nhận yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, thì trước tiên nút chuỗi khối thứ nhất có thể xác định, dựa vào chứng chỉ thứ hai của nút chuỗi khối thứ hai nằm trong yêu cầu truyền thông, mã định danh CA tương ứng với chứng chỉ thứ hai, và sau đó xác định xem liệu mã định danh CA tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không. Nếu có, thì nút chuỗi khối thứ nhất thiết lập kết nối truyền thông với nút chuỗi khối thứ hai; hoặc nếu không, thì nút chuỗi khối thứ nhất không thiết lập kết nối truyền thông với nút chuỗi khối thứ hai. Theo phương pháp được đề xuất theo các phương án thực hiện của sáng chế, trước khi thiết lập kết nối truyền thông, nút dịch vụ trong mạng chuỗi khối có thể xác định xem liệu có thiết lập kết nối truyền thông hay không dựa vào danh sách tin cậy CA được tạo cấu hình trước và chứng chỉ có nằm trong yêu cầu truyền thông hay không, sao cho khả năng lộ dữ liệu cá nhân bởi nút dịch vụ có thể được giảm xuống bằng cách giới hạn đối tượng (ví dụ, nút dịch vụ khác) mà nút

dịch vụ này có thể thiết lập kết nối truyền thông, và việc bảo mật dữ liệu được lưu trong mạng chuỗi khối có thể được cải thiện.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo được mô tả ở đây nhằm hiểu hơn về sáng chế, và cấu thành một phần của sáng chế. Các phương án thực hiện minh họa của sáng chế và các phần mô tả các phương án thực hiện này nhằm mô tả sáng chế, và không cấu thành giới hạn đối với sáng chế. Trên các hình vẽ kèm theo:

Fig.1 là sơ đồ kiến trúc giản lược minh họa mạng chuỗi khối tập đoàn.

Fig.2 là lưu đồ minh họa quy trình truyền thông nút chuỗi khối, theo một phương án thực hiện của sáng chế.

Fig.3 là sơ đồ kiến trúc giản lược minh họa mạng chuỗi khối tập đoàn, theo một phương án thực hiện của sáng chế.

Fig.4 là sơ đồ giản lược minh họa mối tương quan CA theo một phương án thực hiện của sáng chế.

Fig.5 là sơ đồ cấu trúc giản lược minh họa phương tiện truyền thông nút chuỗi khối, theo một phương án thực hiện của sáng chế.

Fig.6 là sơ đồ cấu trúc giản lược minh họa thiết bị truyền thông nút chuỗi khối, theo một phương án thực hiện của sáng chế.

Fig.7 là lưu đồ minh họa ví dụ về phương pháp được thực hiện bằng máy tính để làm cải thiện tính bảo mật của mạng chuỗi khối, theo một phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Trong mạng chuỗi khối tập đoàn, dữ liệu dịch vụ được tạo ra bởi nút dịch vụ do sự tham gia của nút dịch vụ này vào dịch vụ bao gồm dữ liệu riêng tư của người dùng. Do đó, để ngăn dữ liệu riêng tư của người dùng không bị lộ do nút dịch vụ không tham tham gia vào dịch vụ này, trong mạng chuỗi khối tập đoàn, mỗi nút dịch vụ chỉ lưu dữ

liệu dịch vụ của dịch vụ mà nút dịch vụ này tham gia.

Tuy nhiên, trong các ứng dụng thực tế, ví dụ, đối với dịch vụ, nút dịch vụ A không tham tham gia vào dịch vụ này có thể thiết lập, thông qua chương trình truyền thông, kết nối truyền thông với nút dịch vụ B tham gia vào dich vụ này, và sử dụng các phương tiện kỹ thuật (như bẻ khóa cơ sở dữ liệu) để đánh cắp dữ liệu dịch vụ được lưu trong nút dịch vụ B. Tức là, mỗi nút dịch vụ thiết lập kết nối truyền thông thông qua chương trình truyền thông có thể sử dụng các phương tiện kỹ thuật để thu được dữ liệu dịch vụ được lưu trong nút dịch vụ khác nếu truyền thông có thể được thiết lập giữa hai nút dịch vụ này. Vì dữ liệu dịch vụ có thể bao gồm dữ liệu cá nhân của người dùng, nên sáng chế đề xuất giải pháp công nghệ truyền thông bảo mật hơn.

Để làm cho các mục đích, các giải pháp kỹ thuật, và các ưu điểm của các phương án thực hiện của sáng chế rõ ràng hơn, phần tiếp theo mô tả một cách rõ ràng các giải pháp kỹ thuật của sáng chế với tham chiếu đến các hình vẽ kèm theo tương ứng và một hoặc nhiều phương án thực hiện cụ thể của sáng chế. Rõ ràng là, các phương án thực hiện được mô tả chỉ là một số phương án thực hiện chứ không phải tất cả các phương án thực hiện của sáng chế. Tất cả các phương án thực hiện khác thu được bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật dựa vào theo một hoặc nhiều phương án thực hiện của sáng chế mà không có nỗ lực sáng tạo nào sẽ nằm trong phạm vi bảo hộ của sáng chế. Các giải pháp kỹ thuật được đề xuất theo các phương án thực hiện của sáng chế được mô tả chi tiết dưới đây với tham chiếu đến các hình vẽ kèm theo.

Fig.2 minh họa quy trình truyền thông nút chuỗi khối theo một phương án thực hiện của sáng chế. Các nút chuỗi khối trong mạng chuỗi khối bao gồm nút dịch vụ. Nút dịch vụ này lưu trữ chứng chỉ được gửi bởi bên cung cấp chứng chỉ (Certificate Authority, CA), và được tạo cấu hình trước bởi danh sách tin cậy CA. Quy trình truyền thông nút chuỗi khối này có thể bao gồm các bước sau.

S202: Nút chuỗi khối thứ nhất nhận yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai.

Theo một hoặc nhiều phương án thực hiện của sáng chế, các nút chuỗi khối trong mạng chuỗi khối tập đoàn có thể truyền thông với nhau. Các nút dịch vụ có thể

truyền thông và truyền dữ liệu để thực thi các dịch vụ. Dữ liệu dịch vụ được tạo ra trong quá trình thực thi dịch vụ được gửi đến nút đồng thuận để xác minh đồng thuận. Sau khi dữ liệu dịch vụ được xác minh bởi nút đồng thuận, dữ liệu dịch vụ này được lưu trong chuỗi khối. Do đó, nút chuỗi khối bất kỳ trong mạng chuỗi khối có thể nhận yêu cầu truyền thông được gửi bởi nút chuỗi khối khác. Để dễ dàng cho việc mô tả, theo các phương án thực hiện của sáng chế, nút chuỗi khối ví dụ nhận yêu cầu truyền thông được gọi là nút chuỗi khối thứ nhất và nút chuỗi khối gửi yêu cầu truyền thông được gọi là nút chuỗi khối thứ hai. Ngoài ra, yêu cầu truyền thông có thể là một yêu cầu thiết lập kết nối truyền thông được gửi bởi nút chuỗi khối thứ hai, và nút chuỗi khối thứ nhất có thể xác định, dựa vào các bước sau đó, xem liệu có đáp ứng yêu cầu và thiết lập kết nối truyền thông với nút chuỗi khối thứ hai hay không.

Cấu trúc của mạng chuỗi khối có thể được thể hiện trên Fig.1. Các nút chuỗi khối có thể bao gồm nút dịch vụ và nút đồng thuận. Bất kể nút đồng thuận hay nút dịch vụ, nút chuỗi khối có thể lưu trữ chứng chỉ được gửi bởi CA, và được tạo cấu hình trước bởi danh sách tin cậy CA.

Cụ thể là, sử dụng nút dịch vụ làm một ví dụ, như được thể hiện trong kiến trúc trên Fig.1, các mối tương quan dịch vụ có thể tồn tại trong mạng chuỗi khối tập đoàn, và mỗi mối tương quan dịch vụ bao gồm ít nhất hai nút dịch vụ. Như được đề cập ở trên, các nút dịch vụ này có thể là các máy chủ dịch vụ của các tổ chức mà không hoàn toàn giống nhau và tham gia vào mạng chuỗi khối tập đoàn. Các máy chủ dịch vụ trong cùng mối tương quan dịch vụ cùng nhau thực thi dịch vụ, và gửi dữ liệu dịch vụ đến nút đồng thuận để xác minh đồng thuận (ví dụ, ngân hàng của bên bán, ngân hàng của bên mua, và thậm chí là nền tảng giao dịch trung gian có thể tham gia vào dịch vụ thanh toán). Do đó, trong dịch vụ thanh toán, các máy chủ dịch vụ của ba tổ chức có thể thực hiện các bước không hoàn toàn giống nhau trong các quy trình khác nhau của cùng một dịch vụ, và cuối cùng, tạo ra dữ liệu dịch vụ để thực hiện việc xác minh đồng thuận). Để dễ dàng cho việc mô tả, tất cả các nút dịch vụ tiếp theo có thể được coi là các máy chủ dịch vụ của các tổ chức.Ngoài ra, theo một hoặc nhiều phương án thực hiện của sáng chế, mỗi mối tương quan dịch vụ tương ứng với một CA, hoặc có thể được xem là các nút dịch vụ trong cùng mối tương quan dịch vụ tương ứng với cùng CA. Đối với mỗi nút dịch vụ thực thi dịch vụ trong mối tương quan dịch vụ, để tạo cấu

hình nút dịch vụ này để thực thi dịch vụ, trước tiên yêu cầu xác minh nhận dạng có thể được gửi đến CA tương ứng với mối tương quan dịch vụ. Yêu cầu nhận dạng này bao gồm tổ chức mà nút dịch vụ này thuộc về tổ chức đó.

CA có thể xác minh mã nhận dạng của nút dịch vụ bằng cách sử dụng các phương pháp trong công nghệ hiện có, để tạo ra chứng chỉ của nút dịch vụ sau khi nút dịch vụ này được xác minh, và trả lại chứng chỉ cho nút dịch vụ này.

Do đó, theo một hoặc nhiều phương án thực hiện của sáng chế, mỗi nút dịch vụ có thể lưu chứng chỉ. Chứng chỉ này được gửi bởi CA tương ứng với nút dịch vụ này. Đối với công nghệ hiện có, chứng chỉ này có thể bao gồm mã định danh của nút dịch vụ, và khóa công khai của chứng chỉ này bao gồm chữ ký của CA cấp chứng chỉ này. Nút chuỗi khối khác cũng có thể xác định, dựa vào chứng chỉ này bằng cách sử dụng phương pháp trong công nghệ hiện có, mã nhận dạng của nút dịch vụ và mã định danh của CA cấp chứng chỉ của nút dịch vụ.

Ngoài ra, khi nút chuỗi khối thứ hai gửi yêu cầu truyền thông đến nút chuỗi khối thứ nhất, yêu cầu truyền thông này cũng có thể bao gồm chứng chỉ thứ hai được lưu trong nút chuỗi khối thứ hai. Chứng chỉ thứ hai là chứng chỉ được cấp, với nút chuỗi khối thứ hai, bởi CA tương ứng với nút chuỗi khối thứ hai. Sau khi nhận yêu cầu truyền thông, nút chuỗi khối thứ nhất có thể xác định, dựa vào chứng chỉ thứ hai, mã nhận dạng của nút chuỗi khối thứ hai, và CA tương ứng với nút chuỗi khối thứ hai.

Ngoài ra, theo một hoặc nhiều phương án thực hiện của sáng chế, các nút chuỗi khối trong mạng chuỗi khối tập đoàn có thể thiết lập kết nối truyền thông bằng cách sử dụng bảo mật lớp truyền tải (Transport Layer Security, TLS), và nút chuỗi khối thứ hai bổ sung, dựa vào giao thức bắt tay TLS (TLS Handshake), chứng chỉ thứ hai của nút chuỗi khối thứ hai cho yêu cầu truyền thông gửi đến nút chuỗi khối thứ nhất.

Cần lưu ý rằng mỗi nút chuỗi khối còn được tạo cấu hình bởi danh sách tin cậy CA. Danh sách tin cậy CA có thể được gửi bởi CA đến nút chuỗi khối, hoặc có thể được tạo cấu hình bởi nút chuỗi khối. Điều này không bị giới hạn ở bản mô tả này. Khi danh sách tin cậy CA được tạo cấu hình bởi nút chuỗi khối, thì danh sách tin cậy CA có thể được tạo cấu hình trong nút chuỗi khối dựa vào yêu cầu bởi tổ chức tương ứng với nút chuỗi khối. Nếu danh sách tin cậy CA được tạo cấu hình bởi CA, ngoài chứng

chỉ được gửi bởi CA, thì nút chuỗi khối có thể còn nhận danh sách tin cậy CA được gửi bởi CA, và lưu danh sách tin cậy CA. Danh sách tin cậy CA này bao gồm một hoặc nhiều mã định danh CA.

Theo một hoặc nhiều phương án thực hiện của sáng chế, nút chuỗi khối thứ nhất và nút chuỗi khối thứ hai có thể là các nút dịch vụ hoặc các nút đồng thuận trong mạng chuỗi khối tập đoàn. Khi các nút chuỗi khối là các nút đồng thuận, thì các nút đồng thuận này có thể là các máy chủ đồng thuận được tạo cấu hình để thực hiện việc xác minh đồng thuận, và các máy chủ đồng thuận được cung cấp bởi các tổ chức tham gia vào chuỗi khối tập đoàn. Tức là, nút đồng thuận có thể được coi là máy chủ không thuộc về bất cứ tổ chức nào và không tham gia vào dịch vụ. Chắc chắn là, mỗi máy chủ (ví dụ, mỗi máy chủ dịch vụ và mỗi máy chủ đồng thuận) có thể là thiết bị riêng biệt, hoặc có thể là hệ thống bao gồm các thiết bị. Điều này không bị giới hạn ở bản mô tả này.

S204: Xác định mã định danh CA tương ứng với chứng chỉ thứ hai.

Theo một hoặc nhiều phương án thực hiện của sáng chế, sau khi nhận yêu cầu truyền thông, nút chuỗi khối thứ nhất có thể xác định chứng chỉ thứ hai của nút chuỗi khối thứ hai nằm trong yêu cầu truyền thông, và sau đó có thể còn xác định mã định danh CA tương ứng với chứng chỉ thứ hai.

Cụ thể là, vì chứng chỉ bao gồm chữ ký của CA cấp chứng chỉ này, nên sau khi xác định chứng chỉ thứ hai nằm trong yêu cầu truyền thông, nút chuỗi khối thứ nhất có thể xác định, dựa vào chữ ký trong chứng chỉ thứ hai, mã định danh CA của CA cấp chứng chỉ này cho nút chuỗi khối thứ hai. Tức là, sau khi nhận yêu cầu truyền thông, nút dịch vụ có thể xác định mã định danh CA của chứng chỉ thứ hai nằm trong yêu cầu truyền thông.

S206: Xác định xem liệu mã định danh CA được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không. Nếu có, thì thực hiện bước S208; hoặc nếu không, thì thực hiện bước S210.

Theo một hoặc nhiều phương án thực hiện của sáng chế, mỗi nút chuỗi khối trong mạng chuỗi khối tập đoàn được tạo cấu hình bởi danh sách tin cậy CA, và danh

sách tin cậy CA này bao gồm một hoặc nhiều mã định danh CA. Do đó, nút chuỗi khối thứ nhất có thể xác định, dựa vào mã định danh CA trong danh sách tin cậy CA được tạo cấu hình trước, xem liệu mã định danh CA tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA mà được tạo cấu hình trong nút chuỗi khối thứ nhất hay không (ví dụ, phù hợp với một bất kỳ trong số các mã định danh CA trong danh sách tin cậy CA). Tức là, nút chuỗi khối thứ nhất xác định xem liệu mã định danh CA tương ứng với chứng chỉ thứ hai có đáng tin cậy hay không.

Nếu mã định danh CA tương ứng với chứng chỉ thứ hai nằm trong danh sách tin cậy CA được tạo cấu hình trước, thì nút chuỗi khối thứ nhất có thể xác định rằng mã định danh CA đáng tin cậy, và thực hiện bước S208. Nếu mã định danh CA tương ứng với chứng chỉ thứ hai không nằm trong danh sách tin cậy CA được tạo cấu hình trước, thì nút chuỗi khối thứ nhất có thể xác định rằng mã định danh CA không đáng tin cậy, và thực hiện bước S210.

S208: Thiết lập kết nối truyền thông với nút chuỗi khối thứ hai.

Theo một hoặc nhiều phương án thực hiện của sáng chế, khi xác định rằng mã định danh CA đáng tin cậy, thì nút chuỗi khối thứ nhất có thể thiết lập kết nối truyền thông với nút chuỗi khối thứ hai.

Cụ thể là, nút chuỗi khối thứ nhất có thể trực tiếp thiết lập kết nối truyền thông với nút chuỗi khối thứ hai. Để đảm bảo bảo mật truyền thông hơn nữa, nút chuỗi khối thứ nhất cũng có thể gửi chứng chỉ thứ nhất của nút chuỗi khối thứ nhất này đến nút chuỗi khối thứ hai, và sử dụng khóa riêng trong chứng chỉ thứ nhất để mã hóa dữ liệu được gửi đến nút chuỗi khối thứ hai. Tương tự, khi gửi dữ liệu đến nút chuỗi khối thứ nhất, thì nút chuỗi khối thứ hai cũng có thể mã hóa dữ liệu bằng cách sử dụng khóa riêng trong chứng chỉ thứ hai.

Ngoài ra, theo một hoặc nhiều phương án thực hiện của sáng chế, các nút chuỗi khối trong mạng chuỗi khối có thể thiết lập kết nối truyền thông dựa vào giao thức bắt tay TLS. Do đó, sau khi xác định thiết lập kết nối truyền thông với nút chuỗi khối thứ hai, nút chuỗi khối thứ nhất có thể trả lại yêu cầu xác minh cho nút chuỗi khối thứ hai.

Cụ thể là, yêu cầu xác minh này bao gồm chứng chỉ thứ nhất của nút chuỗi khối

thứ nhất này. Nút chuỗi khối thứ hai cũng có thể thực hiện bước S202 đến bước S206, để xác định xem liệu mã định danh CA tương ứng với chứng chỉ thứ nhất có nằm trong danh sách tin cậy CA được tạo cấu hình trong nút chuỗi khối thứ hai hay không. Nếu có, thì nút chuỗi khối thứ hai thiết lập kết nối truyền thông với nút chuỗi khối thứ nhất; hoặc nếu không, thì nút chuỗi khối thứ hai không thiết lập kết nối truyền thông với nút chuỗi khối thứ nhất. Tức là, nút chuỗi khối thứ hai cũng có thể xác minh xem liệu mã định danh CA tương ứng với chứng chỉ thứ nhất của nút chuỗi khối thứ nhất này có đáng in cậy hay không. Nếu có, thì nút chuỗi khối thứ hai thiết lập kết nối truyền thông với nút chuỗi khối thứ nhất; hoặc nếu không, thì nút chuỗi khối thứ hai không thiết lập kết nối truyền thông với nút chuỗi khối thứ nhất.

Khi thiết lập kết nối truyền thông, thì nút chuỗi khối thứ nhất và nút chuỗi khối thứ hai có thể xác định khóa được sử dụng trong truyền thông bằng cách sử dụng quy trình tương tự với quy trình bắt tay TLS trong công nghệ hiện có, và mã hóa dữ liệu được truyền bằng cách sử dụng khóa này. Chắc chắn là, quy trình bắt tay TLS là công nghệ tương đối hoàn thiện. Nội dung chi tiết không được mô tả trong bản mô tả này.

S210: Bỏ qua bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai.

Theo một hoặc nhiều phương án thực hiện của sáng chế, khi xác định rằng mã định danh CA tương ứng với chứng chỉ thứ hai không nằm trong danh sách tin cậy CA được tạo cấu hình trong nút chuỗi khối thứ nhất, thì nút chuỗi khối thứ nhất có thể xác định không thiết lập kết nối truyền thông với nút chuỗi khối thứ hai. Ngoài ra, nút chuỗi khối thứ nhất có thể không cần gửi yêu cầu xác minh đến nút chuỗi khối thứ hai.

Theo phương pháp truyền thông nút chuỗi khối được thể hiện trên Fig.2, có thể thấy rằng nút dịch vụ trong mạng chuỗi khối lưu chứng chỉ được gửi bởi CA, và được tạo cấu hình bởi danh sách tin cậy CA được gửi bởi CA. Ngoài ra, nút đồng thuận trong mạng chuỗi khối cũng có thể lưu chứng chỉ được gửi bởi CA, và được tạo cấu hình bởi danh sách tin cậy CA được gửi bởi CA. Khi nhận yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, thì trước tiên nút chuỗi khối thứ nhất trong mạng chuỗi khối có thể xác định, dựa vào chứng chỉ thứ hai của nút chuỗi khối thứ hai nằm trong yêu cầu truyền thông, mã định danh CA tương ứng với chứng chỉ thứ hai, và sau đó xác định, dựa vào mã định danh CA trong danh sách tin cậy CA được tạo cấu hình

trước, xem liệu mã định danh CA tương ứng với chứng chỉ thứ hai có đáng tin cậy hay không. Nếu có, thì nút chuỗi khối thứ nhất thiết lập kết nối truyền thông với nút chuỗi khối thứ hai; hoặc nếu không, thì nút chuỗi khối thứ nhất không thiết lập kết nối truyền thông với nút chuỗi khối thứ hai. Theo phương pháp được đề xuất theo một hoặc nhiều phương án thực hiện của sáng chế, trước khi thiết lập kết nối truyền thông, nút dịch vụ trong mạng chuỗi khối có thể xác định xem liệu có thiết lập kết nối truyền thông hay không dựa vào danh sách tin cậy CA được tạo cấu hình trước và chứng chỉ nằm trong yêu cầu truyền thông. Do đó, khả năng lộ dữ liệu cá nhân bởi nút dịch vụ có thể được giảm đi bằng cách giới hạn đối tượng (ví dụ, nút dịch vụ khác) mà nút dịch vụ này có thể thiết lập kết nối truyền thông, tăng cường bảo mật dữ liệu được lưu trong mạng chuỗi khối.

Ngoài ra, phương pháp truyền thông nút chuỗi khối được thể hiện trên Fig.2 có thể áp dụng cho cả nút dịch vụ và nút đồng thuận, và không có sự khác biệt giữa quy trình thiết lập kết nối truyền thông cho nút dịch vụ và quy trình thiết lập kết nối truyền thông cho nút đồng thuận. Việc xem liệu có thiết lập kết nối truyền thông hay không có thể được xác định chỉ dựa vào chứng chỉ được lưu trong nút và danh sách tin cậy CA được tạo cấu hình trước. Nút chuỗi khối thứ nhất có thể là nút dịch vụ hoặc nút đồng thuận. Tương tự, nút chuỗi khối thứ hai có thể là nút dịch vụ hoặc nút đồng thuận. Chắc chắn là, vì nút đồng thuận thường chỉ được tạo cấu hình để nhận các dữ liệu được gửi bởi nút dịch vụ và trên đó việc xác minh đồng thuận sẽ được thực hiện, nên nút chuỗi khối thứ hai thường là nút dịch vụ. Điều này không bị giới hạn ở các phương án thực hiện của sáng chế.

Ngoài ra, sử dụng mạng chuỗi khối được thể hiện trên Fig.1 làm ví dụ, khi mỗi nút chuỗi khối tương ứng với một CA, và các nút chuỗi khối trong cùng mối tương quan dịch vụ có thể tương ứng với cùng CA, thì kiến trúc của mạng chuỗi khối tập đoàn có thể được thể hiện trên Fig.3. Có thể thấy rằng mỗi mối tương quan dịch vụ bao gồm CA (tức là, các vòng tròn nét đứt trên Fig.3). CA này được tạo cấu hình để cấp chứng chỉ cho mỗi nút dịch vụ trong mối tương quan. Ngoài ra, các CA có thể tồn tại trong các nút đồng thuận, và có thể cấp các chứng chỉ cho các nút đồng thuận khác nhau. Mỗi nút dịch vụ có thể gửi, đến nút đồng thuận khác nhau, dữ liệu để thực hiện việc xác minh đồng thuận. Các nút đồng thuận có các chứng chỉ được cấp bởi cùng CA

thực hiện việc xác minh đồng thuận đối với dữ liệu này. Cần lưu ý rằng một nút chuỗi khối có thể nhận các chứng chỉ được gửi bởi các CA, và nút chuỗi khối này có thể được tạo cấu hình với một hoặc nhiều danh sách tin cậy CA. Khi gửi yêu cầu truyền thông đến nút chuỗi khối khác, thì chứng chỉ bất kỳ có thể được thêm vào yêu cầu truyền thông. Điều này không bị giới hạn ở bản mô tả này.

Ngoài ra, trong chuỗi khối hiện có trong đó các nhóm nút đồng thuận thực hiện việc xác minh đồng thuận một cách riêng biệt, ví dụ, chuỗi khối dựa vào giao thức Corda, vì các chuỗi khối được lưu trong các nút đồng thuận này không hoàn toàn giống nhau, nên các kết quả thu được sau khi các nút đồng thuận này thực hiện việc xác minh đồng thuận đối với cùng dữ liệu dịch vụ để thực hiện việc xác minh đồng thuận có thể khác nhau. Do đó, có thể có phương pháp (được gọi là chuyển giao công chứng trong giao thức Corda) để chuyển giao dữ liệu trong chuỗi khối. Phương pháp tương tự có thể được sử dụng để chuyển giao dữ liệu trong các nút đồng thuận khác nhau theo một hoặc nhiều phương án thực hiện của sáng chế. Nội dung chi tiết không được mô tả trong mô tả này. Chắc chắn là, theo cách khác, theo một hoặc nhiều phương án thực hiện của sáng chế, các chứng chỉ của các nút đồng thuận có thể chỉ được cấp bởi một CA. Điều này không bị giới hạn ở bản mô tả này.

Ngoài ra, vì sự tin tưởng lẫn nhau giữa các CA trong công nghệ hiện có cần được hỗ trợ bởi CA gốc, để tạo danh sách tin cậy CA được tạo cấu hình trong mỗi nút chuỗi khối có thể được sử dụng trong giao thức bắt tay TLS để xác định xem liệu có thiết lập kết nối truyền thông hay không, có thể thực hiện tham chiếu đến Fig.4. Fig.4 là sơ đồ giản lược minh họa mối tương quan CA theo một phương án thực hiện của sáng chế. CA gốc có thể là CA bên thứ ba, và CA chuỗi khối tập đoàn có thể được tạo ra dựa vào chứng chỉ được cấp bởi CA bên thứ ba. CA chuỗi khối tập đoàn cấp các chứng chỉ cho các CA của các nút chuỗi khối (ví dụ, cấp các chứng chỉ cho CA thứ nhất, CA thứ hai, và CA thứ ba), và cuối cùng, các CA của các nút chuỗi khối gửi các chứng chỉ nút chuỗi khối đến các chuỗi khối (ví dụ, CA thứ nhất cấp chứng chỉ nút chuỗi khối 1-n, và CA thứ hai cấp chứng chỉ nút chuỗi khối m-p, trong đó các chứng chỉ nút có thể được gửi đến các nút chuỗi khối không hoàn toàn giống nhau). Chắc chắn là, một chuỗi tin cậy chứng chỉ dựa vào chứng chỉ là công nghệ tương đối hoàn thiện. Nội dung chi tiết không được mô tả theo các phương án thực hiện của sáng chế.

Cần lưu ý rằng các bước của phương pháp được đề xuất theo một hoặc nhiều phương án thực hiện của sáng chế có thể được thực hiện bằng một thiết bị, hoặc phương pháp này có thể được thực hiện bằng các thiết bị khác nhau. Ví dụ, bước S202 và bước S204 có thể được thực hiện bằng thiết bị 1, và bước S206 có thể được thực hiện bằng thiết bị 2. Ví dụ khác, bước S202 có thể được thực hiện bằng thiết bị 1, và bước S204 và bước S206 có thể được thực hiện bằng thiết bị 2. Các phương án thực hiện cụ thể của sáng chế được mô tả ở trên. Các phương án thực hiện khác nằm trong phạm vi của yêu cầu bảo hộ kèm theo. Trong một số trường hợp, các hành động hoặc các bước được mô tả trong yêu cầu bảo hộ có thể được thực hiện theo thứ tự khác với thứ tự theo một phương án thực hiện và vẫn đạt được các kết quả mong muốn. Ngoài ra, quy trình được mô tả trên các hình vẽ kèm theo không nhất thiết yêu cầu thứ tự thực thi cụ thể để đạt được các kết quả mong muốn. Theo một số phương án, xử lý đa nhiệm và xử lý song song có thể là ưu điểm.

Dựa vào quy trình truyền thông nút chuỗi khối được thể hiện trên Fig.2, một phương án thực hiện của sáng chế còn đề xuất phương tiện truyền thông nút chuỗi khối, như được thể hiện trên Fig.5.

Fig.5 là sơ đồ cấu trúc giản lược minh họa phương tiện truyền thông nút chuỗi khối, theo một phương án thực hiện của sáng chế. Phương tiện truyền thông nút chuỗi khối này bao gồm: môđun nhận 302, được tạo cấu hình để nhận yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, trong đó các nút chuỗi khối trong mạng chuỗi khối bao gồm nút dịch vụ, nút dịch vụ này lưu chứng chỉ được gửi bởi CA, và được tạo cấu hình trước bởi danh sách tin cậy CA, và phương tiện này cũng bao gồm: môđun xác định 304, được tạo cấu hình để xác định mã định danh CA tương ứng với chứng chỉ thứ hai; và môđun xác định và thực thi 306, được tạo cấu hình để xác định xem liệu mã định danh CA được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không; và nếu có, thì thiết lập kết nối truyền thông với nút chuỗi khối thứ hai; hoặc nếu không, thì bỏ qua bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai.

Các nút chuỗi khối còn bao gồm nút đồng thuận, và nút đồng thuận này lưu chứng chỉ được gửi bởi CA, và được tạo cấu hình trước bởi danh sách tin cậy CA.

Các nút chuỗi khối trong mạng chuỗi khối tương ứng với các CA và các CA này không giống nhau

Môđun nhận 302 nhận, dựa vào giao thức bắt tay TLS, yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai.

Môđun xác định và thực thi 306 trả lại yêu cầu xác minh cho nút chuỗi khối thứ hai, và yêu cầu xác minh này bao gồm chứng chỉ thứ nhất của phương tiện này, sao cho nút chuỗi khối thứ hai xác định, dựa vào chứng chỉ thứ nhất và danh sách tin cậy CA được tạo cấu hình trước trong nút chuỗi khối thứ hai, xem liệu có thiết lập kết nối truyền thông với phương tiện này hay không.

Cụ thể là, phương tiện truyền thông nút chuỗi khối có thể được đặt trong nút chuỗi khối. Nút chuỗi khối này có thể là nút dịch vụ hoặc nút đồng thuận trong mạng chuỗi khối tập đoàn. Điều này không bị giới hạn ở bản mô tả này. Ngoài ra, vì nút đồng thuận trong mạng chuỗi khối tập đoàn cũng có thể là máy chủ được cung cấp bởi một thành viên (tổ chức) của tập đoàn, nên nút chuỗi khối có thể là máy chủ đồng thuận. Chắc chắn là, theo cách khác, khi nút chuỗi khối là nút dịch vụ, thì nút dịch vụ cũng có thể là máy chủ dịch vụ của tổ chức.

Ngoài ra, máy chủ (ví dụ, máy chủ dịch vụ hoặc máy chủ đồng thuận) có thể là thiết bị riêng biệt, hoặc có thể là hệ thống bao gồm các thiết bị, chẳng hạn như máy chủ phân tán. Tuy nhiên, dù các máy chủ là một thiết bị hay nhiều hơn một thiết bị, thì máy chủ trong mạng chuỗi khối tập đoàn có thể được coi là nút chuỗi khối.

Dựa vào quy trình truyền thông nút chuỗi khối được thể hiện trên Fig.2, một phương án thực hiện của sáng chế còn đề xuất thiết bị truyền thông nút chuỗi khối, như được thể hiện trên Fig.6.

Fig.6 là sơ đồ cấu trúc giản lược minh họa thiết bị truyền thông nút chuỗi khối theo một phương án thực hiện của sáng chế. Thiết bị truyền thông này bao gồm một hoặc nhiều bộ xử lý và bộ nhớ. Bộ nhớ này lưu chương trình, và chương trình này được thực thi bằng một hoặc nhiều bộ xử lý để thực hiện các bước sau: nhận, ở nút chuỗi khối thứ nhất, yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai;

xác định mã định danh CA tương ứng với chứng chỉ thứ hai; xác định xem liệu mã định danh CA được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không; và nếu có, thì thiết lập kết nối truyền thông với nút chuỗi khối thứ hai; hoặc nếu không, thì bỏ qua bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai.

Các nút chuỗi khối trong mạng chuỗi khối bao gồm nút dịch vụ. Nút dịch vụ này lưu chứng chỉ được gửi bởi CA, và được tạo cấu hình trước bởi danh sách tin cậy CA.

Ngoài ra, nút chuỗi khối có thể là nút đồng thuận, và thực hiện các bước giống như khi thiết lập kết nối truyền thông với nút chuỗi khối khác bằng cách sử dụng nút chuỗi khối thiết bị truyền thông.

Trong những năm 1990, việc xem liệu sự cải tiến của công nghệ là sự cải tiến phần cứng (ví dụ, sự cải tiến về cấu trúc mạch chẳng hạn như điôt, tranzito, hoặc bộ chuyển mạch) hay cải tiến phần mềm (sự cải tiến về thủ tục phương pháp) có thể được phân biệt rõ ràng. Tuy nhiên, với sự phát triển của các công nghệ, sự cải tiến đối với các thủ tục phương pháp có thể được xem là sự cải tiến trực tiếp của cấu trúc mạch phần cứng. Nhà thiết kế luôn lập trình thủ tục phương pháp được cải tiến vào mạch phần cứng, để thu được cấu trúc mạch phần cứng tương ứng. Do đó, thủ tục phương pháp có thể được cải tiến bằng cách sử dụng môđun thực thể phần cứng. Ví dụ, thiết bị logic lập trình được (Programmable Logic Device, PLD) (ví dụ, mảng cổng lập trình được dạng trường (Field Programmable Gate Array, FPGA)) là mạch tích hợp, và chức năng logic của thiết bị logic lập trình được được xác định bởi người dùng thông qua việc lập trình thiết bị. Nhà thiết kế thực hiện lập trình để "tích hợp" hệ thống kỹ thuật số vào PLD mà không yêu cầu nhà sản xuất chip thiết kế và sản xuất chip mạch tích hợp chuyên dụng. Ngoài ra, hiện nay, thay cho việc sản xuất thủ công chip mạch tích hợp, việc lập trình hầu hết được thực hiện bằng cách sửa đổi phần mềm "biên dịch logic". Điều này tương tự với bộ biên dịch phần mềm được sử dụng để phát triển và biên dịch chương trình. Tuy nhiên, mã ban đầu trước khi biên dịch cũng được ghi ở dạng ngôn ngữ lập trình cụ thể, được gọi là ngôn ngữ mô tả phần cứng (Hardware Description Language, HDL). Có nhiều HDL, chẳng hạn như ngôn ngữ biểu thức Boolean nâng cao (Advanced Boolean Expression Language, ABEL), ngôn ngữ mô tả phần cứng Altera (Altera Hardware Description Language, AHDL), Confluence, ngôn

ngữ lập trình đại học Cornell (Cornell University Programming Language, CUPL), HDCal, Ngôn ngữ mô tả phần cứng Java (Java Hardware Description Language, JHDL), Lava, Lola, MyHDL, PALASM, và ngôn ngữ mô tả phần cứng Ruby (Ruby Hardware Description Language, RHDL). Hiện nay, ngôn ngữ mô tả phần cứng mạch tích hợp tốc độ rất cao (Very-High-Speed Integrated Circuit Hardware Description Language, VHDL) và Verilog được sử dụng phổ biến nhất. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cũng hiểu rằng mạch phần cứng thực hiện thủ tục phương pháp logic có thể dễ dàng đạt được ngay khi thủ tục phương pháp này được lập trình logic bằng cách sử dụng các ngôn ngữ mô tả phần cứng được mô tả và được lập trình trong mạch tích hợp.

Bộ điều khiển có thể được thực hiện theo cách thích hợp. Ví dụ, bộ điều khiển này có thể là bộ vi xử lý, bộ xử lý, hoặc vật ghi đọc được bằng máy tính, cổng logic, bộ chuyển mạch, mạch tích hợp chuyên dụng (Application-Specific Integrated Circuit, ASIC), bộ điều khiển logic lập trình được, hoặc bộ vi điều khiển nhúng lưu mã chương trình đọc được bằng máy tính (ví dụ, phần mềm hoặc phần sụn) có thể được thực thi bởi bộ xử lý (hoặc bộ vi xử lý). Các ví dụ về bộ điều khiển bao gồm nhưng không bị giới hạn với các bộ vi điều khiển sau đây: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20, và Silicone Labs C8051F320. Bộ điều khiển của bộ nhớ cũng có thể được thực hiện là một phần của mạch logic điều khiển của bộ nhớ. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cũng cần biết rằng bộ điều khiển có thể được thực hiện theo cách của mã chương trình đọc được bằng máy tính thuần túy, và các bước theo phương pháp có thể được lập trình logic để cho phép bộ điều khiển thực hiện cùng các chức năng ở dạng cổng logic, bộ chuyển mạch, mạch tích hợp chuyên dụng, bộ điều khiển logic lập trình được, bộ vi điều khiển nhúng, v.v.. Do đó, bộ điều khiển có thể được xem là thành phần phần cứng, và phương tiện được tạo kết cấu để thực hiện các chức năng khác nhau trong bộ điều khiển này cũng có thể được xem là cấu trúc trong thành phần phần cứng. Theo cách khác, phương tiện được tạo kết cấu để thực hiện các chức năng khác nhau có thể được xem là môđun phần mềm có thể thực hiện phương pháp và cấu trúc bên trong thành phần phần cứng.

Hệ thống, phương tiện, môđun, hoặc bộ phận được minh họa theo các phương án thực hiện nêu trên có thể được thực hiện bằng cách sử dụng chip máy tính hoặc thực

thể, có thể được thực hiện bằng cách sử dụng sản phẩm có chức năng nhất định. Cụ thể là, máy tính có thể là, ví dụ, máy tính cá nhân, máy tính xách tay, điện thoại di động, điện thoại camera, điện thoại thông minh, thiết bị hỗ trợ cá nhân kỹ thuật số, máy phát đa phương tiện, thiết bị định vị, thiết bị thư điện tử, bàn giao tiếp trò chơi, máy tính dạng bảng, thiết bị đeo được, hoặc sự kết hợp của thiết bị bất kỳ trong số các thiết bị này.

Để dễ dàng cho việc mô tả, phương tiện được mô tả được mô tả bằng cách phân chia các chức năng thành các bộ phận khác nhau. Chắc chắn là, khi sáng chế được thực hiện, thì các chức năng của mỗi đơn vị có thể được thực hiện trong một hoặc nhiều đoạn của phần mềm và/hoặc phần cứng.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cần hiểu rằng các phương án thực hiện của sáng chế có thể được đề xuất ở dạng phương pháp, hệ thống, hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dạng của phương án thực hiện chỉ phần cứng, phương án thực hiện chỉ phần mềm, hoặc phương án thực hiện kết hợp phần mềm và phần cứng. Ngoài ra, sáng chế có thể sử dụng dạng sản phẩm chương trình máy tính được thực hiện trên một hoặc nhiều vật ghi lưu trữ sử dụng được bằng máy tính (bao gồm nhưng không bị giới hạn ở bộ nhớ đĩa từ, bộ nhớ chỉ đọc đĩa nén (Compact Disc Read-Only Memory, CD-ROM), và bộ nhớ quang học) bao gồm mã chương trình sử dụng được bằng máy tính.

Sáng chế được mô tả với tham chiếu đến các lưu đồ và/hoặc các sơ đồ khối của phương pháp, thiết bị (hệ thống), và sản phẩm chương trình máy tính dựa vào các phương án thực hiện của sáng chế. Cần hiểu rằng các lệnh chương trình máy tính có thể được sử dụng để thực hiện mỗi thủ tục và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối và tổ hợp của thủ tục và/hoặc khối trong các lưu đồ và/hoặc các sơ đồ khối. Các lệnh chương trình máy tính này có thể được cấp cho máy tính đa năng, máy tính chuyên dụng, bộ xử lý nhúng, hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác để tạo ra máy, để các lệnh được chạy bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác tạo ra phương tiện để thực hiện chức năng được chỉ định trong một hoặc nhiều thủ tục trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được lưu trong bộ nhớ đọc được bằng máy tính có thể lệnh cho máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác làm việc theo cách cụ thể, để các lệnh được lưu trong bộ nhớ đọc được bằng máy tính tạo ra thành phần giả tượng (artifact) bao gồm thiết bị lệnh. Thiết bị lệnh này thực hiện chức năng cụ thể trong một hoặc nhiều thủ tục trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được tải vào máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, để chuỗi các thao tác và các bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác để tạo ra quy trình xử lý được thực hiện bằng máy tính. Do đó, các lệnh được thực thi trên máy tính hoặc thiết bị lập trình được khác đề xuất các bước thực hiện chức năng được chỉ định trong một hoặc nhiều thủ tục trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Trong cấu hình điển hình, thiết bị máy tính bao gồm một hoặc nhiều bộ xử lý trung tâm (Central Processing Unit, CPU), giao diện đầu vào/đầu ra, giao diện mạng, và bộ nhớ.

Bộ nhớ có thể bao gồm bộ nhớ khả biến, bộ nhớ truy cập ngẫu nhiên (Random Access Memory, RAM) và/hoặc bộ nhớ không khả biến, v.v., trong vật ghi đọc được bằng máy tính, chẳng hạn như bộ nhớ chỉ đọc (Read-Only Memory, ROM) hoặc bộ nhớ nhanh. Bộ nhớ là một ví dụ về vật ghi đọc được bằng máy tính.

Vật ghi đọc được bằng máy tính bao gồm các vật ghi ổn định, không ổn định, di động và không di động có thể lưu thông tin bằng cách sử dụng phương pháp hoặc công nghệ bất kỳ. Thông tin có thể là lệnh đọc được bằng máy tính, cấu trúc dữ liệu, môđun chương trình, hoặc dữ liệu khác. Các ví dụ về vật ghi lưu trữ máy tính bao gồm nhưng không bị giới hạn ở bộ nhớ chuyển pha (Phase Change Memory, PRAM), bộ nhớ truy cập ngẫu nhiên tĩnh (Static Random Access Memory, SRAM), bộ nhớ truy cập ngẫu nhiên động (Dynamic Random Access Memory, DRAM), các loại RAM khác, ROM, bộ nhớ chỉ đọc lập trình được xóa được bằng tín hiệu điện (Electrically Erasable Programmable Read-Only Memory, EEPROM), bộ nhớ nhanh hoặc các công nghệ bộ nhớ khác, bộ nhớ chỉ đọc đĩa nén (Compact Disc Read-Only Memory, CD-ROM), đĩa đa năng số (Digital Versatile Disc, DVD) hoặc các thiết bị lưu trữ quang học khác,

băng từ, thiết bị lưu trữ từ tính, thiết bị lưu trữ từ tính khác, hoặc vật ghi không truyền khác bất kỳ. Vật ghi lưu trữ máy tính có thể được sử dụng để lưu thông tin có thể được truy cập bởi thiết bị máy tính. Như được mô tả trong bản mô tả này, vật ghi đọc được bằng máy tính không bao gồm các vật ghi tạm thời, tín hiệu dữ liệu điều biến và sóng mang.

Cần lưu ý rằng thuật ngữ "bao gồm", "chứa", hoặc các biến thể khác bất kỳ được dự định là bao hàm sự bao gồm không loại trừ, để quy trình, phương pháp, hàng hóa, hoặc thiết bị bao gồm chuỗi các phần tử không chỉ bao gồm phần tử đó mà còn bao gồm các phần tử khác không được liệt kê rõ ràng, hoặc còn bao gồm các phần tử vốn có của các quy trình, phương pháp, hàng hóa, hoặc thiết bị. Trong trường hợp không có giới hạn thêm, phần tử được đặt trước "bao gồm..." không loại trừ sự có mặt của các phần tử bổ sung tương tự trong quy trình, phương pháp, hàng hóa, hoặc thiết bị bao gồm phần tử này.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cần hiểu rằng các phương án thực hiện của sáng chế có thể được đề xuất ở dạng phương pháp, hệ thống hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dạng các phương án thực hiện chỉ của phần cứng, các phương án thực hiện chỉ của phần mềm hoặc các phương án thực hiện kết hợp phần cứng và phần mềm. Ngoài ra, sáng chế có thể sử dụng dạng sản phẩm chương trình máy tính được thực hiện trên một hoặc nhiều vật ghi sử dụng được bằng máy tính (bao gồm nhưng không bị giới hạn ở bộ nhớ dạng đĩa từ, CD-ROM và bộ nhớ quang học) bao gồm mã chương trình sử dụng được bằng máy tính.

Sáng chế có thể được mô tả trong các ngữ cảnh chung của các lệnh chạy được bằng máy tính thực thi được bằng máy tính, chẳng hạn như môđun chương trình. Nói chung, môđun chương trình này bao gồm thường trình, chương trình, đối tượng, thành phần, cấu trúc dữ liệu, v.v. thực thi tác vụ cụ thể hoặc thực hiện kiểu dữ liệu trừu tượng cụ thể. Sáng chế cũng có thể được thực hiện trong các môi trường máy tính phân tán. Trong các môi trường máy tính phân tán này, các tác vụ được thực thi bởi các thiết bị xử lý từ xa được kết nối bằng cách sử dụng mạng truyền thông. Trong các môi trường máy tính phân tán này, môđun chương trình có thể được định vị trong cả các vật ghi lưu trữ máy tính cục bộ và từ xa bao gồm các thiết bị lưu trữ.

Các phương án thực hiện trong bản mô tả này được mô tả theo cách lũy tiến. Đối với các phần giống hoặc tương tự theo các phương án thực hiện, có thể thực hiện tham chiếu đến các phương án thực hiện. Mỗi phương án thực hiện nhấn mạnh vào sự khác biệt với các phương án thực hiện khác. Cụ thể là, phương án thực hiện về hệ thống tương tự với phương án thực hiện về phương pháp, do đó, sẽ được mô tả ngắn gọn. Đối với các phần liên quan, có thể thực hiện tham chiếu đến các phần mô tả liên quan theo phương án thực hiện về phương pháp.

Các phần mô tả trước đó chỉ là các phương án thực hiện của sáng chế, và không nhằm giới hạn sáng chế. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này có thể thực hiện các cải biên và thay đổi khác nhau đối với sáng chế. Các cải biên, thay thế tương đương, cải tiến v.v. được thực hiện trong bản chất và nguyên lý của sáng chế cần nằm trong phạm vi yêu cầu bảo hộ của sáng chế.

Fig.7 là lưu đồ minh họa ví dụ về phương pháp được thực hiện bằng máy tính 700 để cải thiện tính bảo mật mạng chuỗi khối, theo một phương án thực hiện của sáng chế. Để trình bày rõ ràng, phần mô tả dưới đây nhìn chung mô tả phương pháp 700 khi xem xét các hình vẽ khác trong phần mô tả này. Tuy nhiên, cần hiểu rằng phương pháp 700 có thể được thực hiện, ví dụ, bởi hệ thống, môi trường, phần mềm và phần cứng bất kỳ, hoặc sự kết hợp của các hệ thống, môi trường, phần mềm và phần cứng, một cách thích hợp. Theo một số phương án thực hiện, các bước khác nhau của phương pháp 700 có thể được chạy song song, kết hợp, theo vòng lặp hoặc theo thứ tự bất kỳ.

Nói chung, sổ cái phân tán là sự đồng thuận của dữ liệu số được sao chép, chia sẻ và đồng bộ hóa trải rộng trên nhiều nút mà không cần quản trị viên trung tâm hoặc thiết bị lưu trữ dữ liệu tập trung. Các bản sao của sổ cái phân tán được sao chép và chia sẻ giữa các nút của mạng lưới sổ cái phân tán. Vệc sao chép và chia sẻ mang lại cho sổ cái phân tán khả năng phục hồi và bảo vệ đặc trưng của nó chống lại sự thay đổi trái phép. Mạng chuỗi khối là một ví dụ về sổ cái phân tán.

Mạng chuỗi khối, nói chung có thể là ‘'không được cấp phép' hoặc 'được cấp phép'. Ở mạng chuỗi khối không được cấp phép, quyền truy cập vào chuỗi khối không bị hạn chế. Tuy nhiên, do quyền truy cập không bị hạn chế, nên chuỗi khối không được cấp phép có thể có các ứng dụng hạn chế trong các giao dịch chuỗi khối chứa các

dữ liệu nhạy cảm hoặc riêng tư, chẳng hạn như dữ liệu tài chính, dữ liệu giao dịch trực tuyến, thông tin nhận dạng cá nhân, hoặc dữ liệu độc quyền. Mặt khác, chuỗi khối 'được cấp phép' có thể được sở hữu, điều khiển và quản lý bởi bên đáng tin cậy trung tâm hoặc nhóm bên tham gia ở dạng tập đoàn. Các ví dụ về chuỗi khối 'được cấp phép' bao gồm mạng chuỗi khối tập đoàn và mạng chuỗi khối riêng.

Trong mạng chuỗi khối tập đoàn, chỉ những bên tham gia hoặc nút đáng tin cậy hoặc được kiểm duyệt, là một phần của tập đoàn mới được phép tham gia vào việc kiểm soát và bảo trì của chuỗi khối. Các bản sao của chuỗi khối có thể được lưu bởi mỗi nút của mạng chuỗi khối tập đoàn, và quyền truy cập vào chuỗi khối chỉ giới hạn ở các nút tập đoàn. Việc chia sẻ có kiểm soát này của các chuỗi khối giữa các nút tập đoàn có thể được sử dụng để ghi lại các giao dịch sổ cái phân tán có chứa dữ liệu nhạy cảm hoặc riêng tư.

Do dữ liệu nhạy cảm và riêng tư có thể được lưu bởi mạng chuỗi khối tập đoàn, các nút của mạng chuỗi khối này có thể trở thành các mục tiêu cố gắng tấn công. Một số phương pháp tấn công có thể chỉ yêu cầu, ví dụ, phiên truyền thông được thiết lập giữa nút tin tặc và nút tập đoàn để cố gắng tấn công để có khả năng giành quyền truy cập vào chuỗi khối chứa dữ liệu riêng tư hoặc nhạy cảm. Vì mỗi nút của mạng chuỗi khối tập đoàn chứa một bản sao của chuỗi khối chứa dữ liệu nhạy cảm và riêng tư, và vì các phương pháp tấn công phát triển liên tục và các lỗ hổng ngày diễn ra sự kiện quan trọng tiếp tục bị lộ, nên cần phải kiểm soát việc thiết lập các phiên truyền thông với các nút của mạng chuỗi khối, chẳng hạn như mạng chuỗi khối tập đoàn. Có thể đạt được sự kiểm soát như vậy đối với việc thiết lập các phiên truyền thông bằng cách sử dụng các chứng chỉ khóa công khai và danh sách tin cậy.

Ở bước 702, danh sách tin cậy bên cung cấp chứng chỉ (Certificate Authority, CA) thứ nhất bao gồm các mã định danh CA được thu bởi nút thứ nhất của mạng chuỗi khối. CA là thực thể cấp các chứng chỉ khóa công khai. Chứng chỉ khóa công khai, đôi khi được gọi là chứng chỉ số hoặc chứng chỉ nhận dạng, thường được sử dụng bởi một bên của giao dịch trực tuyến để xác thực mã nhận dạng của nút này, và thường dựa vào kỹ thuật mã hóa hạ tầng khóa công khai (Public Key Infrastructure, PKI). Mỗi nút của chuỗi khối thường có chứng chỉ khóa công khai liên kết được sử dụng để xác thực mã nhận dạng của nút này và để ký mã hóa khối được thêm vào chuỗi khối. Các chứng chỉ

khóa công khai được ký số bởi CA đã cấp các chứng chỉ này, và khi đó sẽ xác nhận tính xác thực của thực thể được đặt tên của chứng chỉ khóa công khai. Như vậy, tác vụ xác thực mã nhận dạng của bên xuất trình chứng chỉ khóa công khai thuộc về CA cấp chứng chỉ khóa công khai. Theo đó, tính toàn vẹn hoặc độ tin cậy của CA cấp là rất quan trọng để duy trì tính toàn vẹn của sơ đồ xác minh mã nhận dạng số dựa vào chứng chỉ.

Nói chung, bên tin tặc có thể hoạt động như chính CA và tự ký chứng chỉ khóa công khai có ý định trở thành thực thể bất kỳ mà bên tin tặc muốn mạo danh. Như vậy, một cách để xác minh độ tin cậy của chứng chỉ khóa công khai là xác thực chuỗi tin cậy từ bên cung cấp chứng chỉ gốc tin cậy cho CA đã cấp chứng chỉ khóa công khai đang đề cập. Một ví dụ về chuỗi tin cậy được minh họa trên Fig.4, chẳng hạn như chuỗi tin cậy được thiết lập từ chứng chỉ nút chuỗi khối 1 đến CA thứ nhất cho CA chuỗi khối liên kết đến CA gốc. Trong một số trường hợp, chuỗi tin cậy này có thể tương đối dài, dẫn đến cần thời gian xử lý nhất định liên quan đến việc xác thực chuỗi tin cậy. Ngay cả trong các trường hợp chuỗi tin cậy này tương đối ngắn, nhưng mỗi lần xác nhận sẽ mất một khoảng thời gian xử lý. Trong ứng dụng chuỗi khối yêu cầu khối lượng lớn, độ trễ thấp, thông lượng cao hoặc tổ hợp của chúng, thời gian xử lý như vậy liên quan đến việc xác thực chuỗi tin cậy có thể làm giảm hiệu suất hệ thống.

Một cách để giảm thời gian xử lý liên quan đến việc xác thực chuỗi tin cậy để thu được danh sách tin cậy CA chứa danh sách mã định danh CA có thể tin cậy được. Bằng cách tin tưởng các CA nằm trong danh sách tin cậy CA, việc xác thực chuỗi tin cậy đầy đủ có thể được bỏ qua, điều này có thể làm giảm hoặc loại bỏ thời gian xử lý liên quan. Danh sách tin cậy CA có thể được thu theo các cách khác nhau. Ví dụ, nút chuỗi khối có thể được tạo cấu hình trước bởi danh sách tin cậy CA. Các ví dụ về việc tạo cấu hình trước bao gồm bản sao của danh sách tin cậy CA trong phần mềm chuỗi khối được lưu và chạy trên nút chuỗi khối, và lưu bản sao của danh sách tin cậy CA trong môđun phần cứng bảo mật được cài đặt về mặt vật lý trên nút chuỗi khối. Môđun phần cứng bảo mật này có thể là thiết bị lưu trữ chỉ đọc, có thể có lợi cho việc giảm thiểu các nỗ lực chỉnh sửa từ xa danh sách tin cậy CA theo cách cố tình. Ví dụ khác, danh sách tin cậy CA có thể được nhận từ CA đã cấp chứng chỉ khóa công khai và do đó được tin tưởng bởi nút chuỗi khối cụ thể. Việc phân phối danh sách tin cậy CA bởi CA cho các

nút mà CA đã cấp chứng chỉ có thể có lợi trong việc hợp lý hóa việc quản lý và cập nhật danh sách tin cậy CA. Theo đó, theo một số phương án, việc thu được danh sách tin cậy CA thứ nhất bao gồm các mã định danh CA có thể được thực hiện bởi một trong số: tạo cấu hình trước nút thứ nhất bởi danh sách tin cậy CA thứ nhất; hoặc nhận, từ CA được liên kết với nút thứ nhất, danh sách tin cậy CA thứ nhất. Từ bước 702, phương pháp 700 tiến hành đến bước 704.

Ở bước 704, yêu cầu truyền thông bao gồm chứng chỉ khóa công khai của nút thứ hai của mạng chuỗi khối được nhận bởi nút thứ nhất từ nút thứ hai của mạng chuỗi khối. Bước này có thể tương tự với bước S202 trên Fig.2. Yêu cầu truyền thông thường đề cập đến yêu cầu hoặc thông điệp được trao đổi qua mạng chuyển tiếp ý định của nút mạng thứ nhất để truyền thông với nút mạng thứ hai. Là một phần của biện pháp bảo mật của mạng chuỗi khối, việc truyền thông giữa các nút của mạng chuối khối thường được bảo mật bằng cách sử dụng mã hóa. Để tạo thuận lợi cho quy trình mã hóa, và để thiết lập mã nhận dạng của nút yêu cầu truyền thông, yêu cầu truyền thông bao gồm chứng chỉ khóa công khai của nút yêu cầu. Định dạng và nội dung của yêu cầu truyền thông có thể được chuẩn hóa hoặc thực hiện cụ thể.

Giao thức bảo mật lớp truyền tải (Transport Layer Security, TLS) và giao thức lớp cổng bảo mật tiền nhiệm (Predecessor Secure Socket Layer, SSL) của nó là các giao thức được sử dụng rộng rãi để thực hiện truyền thông bảo mật qua mạng giữa hai nút của mạng này. Các giao thức TLS và SSL có các thủ tục bắt tay được sử dụng để khởi tạo phiên phiên truyền thông bảo mật. Là một phần của thủ tục bắt tay, các chứng chỉ khóa công khai được trao đổi giữa hai nút mạng thông qua các thủ tục được chuẩn hóa. Như vậy, theo một số phương án thực hiện, bước nhận, bởi nút thứ nhất từ nút thứ hai của mạng chuỗi khối, yêu cầu truyền thông bao gồm chứng chỉ khóa công khai của nút thứ hai bao gồm bước: nhận, bởi nút thứ nhất từ nút thứ hai, yêu cầu truyền thông theo giao thức bắt tay bảo mật lớp truyền tải (Transport Layer Security, TLS). Từ bước 704, phương pháp 700 tiến hành đến bước 706.

Ở bước 706, mã định danh CA thứ nhất từ chứng chỉ khóa công khai nhận được được xác định. Bước này có thể tương tự với bước S204 trên Fig.2. Chứng chỉ khóa công khai thường chứa các thông tin khác nhau ở định dạng được chuẩn hóa như được quy định bởi chuẩn thích hợp, chẳng hạn như chuẩn X.509. Tên tổ chức phát hành, hoặc

tên của CA đã cấp chứng chỉ này, là một trong các lĩnh vực được chuẩn hóa của chứng chỉ khóa công khai. Như vậy, tên tổ chức phát hành có trong chứng chỉ khóa công khai có thể được sử dụng, ví dụ, làm mã định danh CA. Ví dụ khác, thông tin nhận dạng không theo thứ tự chữ cái được liên kết với CA cấp, chẳng hạn như mã định danh mã có thẩm quyền (AKI) hoặc chữ ký số của CA cấp, có thể được sử dụng làm mã định danh CA. Nói chung, thông tin bất kỳ có trong chứng chỉ khóa công khai có thể sử dụng được để nhận dạng CA đã cấp chứng chỉ khóa công khai cụ thể có thể được sử dụng làm mã định danh CA. Ngoài ra, chứng chỉ này còn bao gồm trường tên đối tượng, là tên hoặc thông tin nhận dạng của chủ sở hữu chứng chỉ khóa công khai. Từ bước 706, phương pháp 700 tiến hành đến bước 708.

Ở bước 708, quyết định được đưa ra xem liệu mã định danh CA thứ nhất có khớp với một trong số các mã định danh CA của danh sách tin cậy CA thứ nhất hay không. Bước này có thể tương tự với bước S206 trên Fig.2. Việc xác định kết quả so khớp có thể được thực hiện, ví dụ, bằng cách tìm kiếm kết quả khớp chính xác (ví dụ, thông qua việc so sánh từng bit) của mã định danh CA thứ nhất được xác định từ chứng chỉ khóa công khai nhận được với các mục nhập của danh sách tin cậy CA thứ nhất. Nếu xác định được rằng mã định danh CA thứ nhất khớp với một trong số các mã định danh CA của danh sách tin cậy CA thứ nhất, thì phương pháp 700 sẽ tiến hành đến bước 710. Ngược lại, nếu xác định được rằng mã định danh CA thứ nhất không khớp với một trong số các mã định danh CA của danh sách tin cậy CA thứ nhất, thì phương pháp 700 tiến hành đến bước 712.

Ở bước 710, yêu cầu truyền thông được phê duyệt bởi nút thứ nhất. Bước này có thể tương tự với bước S208 trên Fig.2. Khi yêu cầu truyền thông được phê duyệt bởi nút thứ nhất, thì nút thứ nhất có thể thiết lập phiên truyền thông giữa nút thứ nhất và nút thứ hai. Phiên truyền thông được thiết lập này có thể là phiên truyền thông được mã hóa, chẳng hạn như phiên truyền thông được bảo mật bằng TLS. Ngay khi phiên truyền thông được thiết lập, dữ liệu có thể chạy giữa nút thứ nhất và nút thứ hai, và các giao dịch chuỗi khối có thể được thực hiện qua phiên truyền thông được thiết lập này.

Theo một số phương án thực hiện, các bước khác có thể được thực hiện sau khi phê duyệt bởi nút thứ nhất trước khi phiên truyền thông được thiết lập. Ví dụ, nút thứ hai đã khởi tạo yêu cầu truyền thông cũng có thể muốn thực hiện việc xác minh mã

nhận dạng đối ứng của nút thứ nhất trước khi thiết lập phiên truyền thông giữa hai nút này. Việc xác minh mã nhận dạng lẫn nhau như vậy có thể cải thiện tính bảo mật tổng thể của mạng chuỗi khối. Như vậy, theo một số phương án thực hiện, nút thứ hai bao gồm danh sách tin cậy CA thứ hai bao gồm các mã định danh CA, và bước phê duyệt, bởi nút thứ nhất, yêu cầu truyền thông bao gồm bước: truyền, bởi nút thứ nhất đến nút thứ hai, yêu cầu xác minh bao gồm chứng chỉ khóa công khai của nút thứ nhất. Yêu cầu xác minh này, ví dụ, có thể được truyền theo các giao thức truyền thông hẳng hạn như giao thức TLS hoặc SSL. Theo các phương án thực hiện này, phương pháp 700 còn bao gồm các bước: xác định, bởi nút thứ hai, mã định danh CA thứ hai từ chứng chỉ khóa công khai nhận được của nút thứ nhất; xác định xem liệu mã định danh CA thứ hai có khớp với một trong số các mã định danh CA của danh sách tin cậy CA thứ hai của nút thứ hai hay không; để đáp lại việc xác định rằng mã định danh CA thứ hai khớp với một trong số các mã định danh CA của danh sách tin cậy CA thứ hai, thiết lập phiên truyền thông với nút thứ nhất; và để đáp lại việc xác định rằng mã định danh CA thứ hai không khớp với một trong số các mã định danh CA của danh sách tin cậy CA thứ hai, từ chối, bởi nút thứ hai, thiết lập phiên truyền thông với nút thứ nhất. Nội dung chi tiết của quy trình xác minh bởi nút thứ hai có thể giống với các bước 706 và 708.

Ở bước 712, yêu cầu truyền thông bị từ chối bởi nút thứ nhất. Bước này có thể tương tự với bước S210 trên Fig.2. Khi mã định danh CA thứ nhất không khớp với một trong số các mã định danh CA của danh sách tin cậy CA thứ nhất, thì nút thứ nhất từ chối yêu cầu truyền thông, vì yêu cầu truyền thông này có thể từ nút tin tặc, hoặc từ nút có mã nhận dạng của nó không thể được xác minh theo một chuẩn bởi mạng chuỗi khối. Nút thứ nhất, khi từ chối yêu cầu truyền thông, có thể thực hiện hoặc từ chối thực hiện các hành động khác nhau. Ví dụ, nút thứ nhất có thể không thực hiện thêm hành động nào liên quan đến yêu cầu truyền thông. Ví dụ khác, nút thứ nhất có thể gửi thông điệp 'yêu cầu truyền thông bị từ chối' đến nút thứ hai. Ví dụ khác nữa, nút thứ nhất có thể thêm mã định danh mạng của nút thứ hai (ví dụ: địa chỉ MAC hoặc địa chỉ IP) vào danh sách theo dõi để theo dõi các hoạt động đáng ngờ, hoặc vào danh sách đen để chặn mọi yêu cầu truyền thông khác từ nút thứ hai có yêu cầu truyền thông đã bị từ chối.

Nói chung, các nút khác nhau của mạng chuỗi khối có thể có chứng chỉ khóa công khai do các CA khác nhau cấp. Ví dụ, các CA có thể là một phần của mạng chuỗi khối tập đoàn, và các chứng chỉ khóa công khai cho các nút thực hiện một loại của các giao dịch chuỗi khối có thể được cấp bởi CA thứ nhất, và các chứng chỉ khóa công khai cho các nút thực hiện loại khác của các giao dịch chuỗi khối có thể được cấp bởi CA thứ hai khác với CA thứ nhất. Như vậy, theo một số phương án thực hiện, mã định danh CA thứ nhất của chứng chỉ khóa công khai của nút thứ hai là khác với mã định danh CA thứ hai của chứng chỉ khóa công khai của nút thứ nhất. Việc thực hiện CA riêng cho các loại giao dịch khác nhau có thể có lợi trong việc chứa vi phạm bảo mật bất kỳ có thể xảy ra trong một hoạt động cụ thể của mạng chuỗi khối và ngăn chặn vi phạm lây lan sang các hoạt động khác của mạng chuỗi khối.

Theo một số phương án thực hiện, mạng chuỗi khối của phương pháp 700 là mạng chuỗi khối tập đoàn.

Nói chung, mạng chuỗi khối bao gồm một hoặc nhiều nút đồng thuận được tạo cấu hình để thực hiện việc xác minh đồng thuận thông qua các bản sao của chuỗi khối được phân phối qua các nút khác nhau của mạng chuỗi khối. Như vậy, theo một số phương án thực hiện, nút thứ nhất của mạng chuỗi khối nhận yêu cầu truyền thông hoặc nút thứ hai truyền yêu cầu truyền thông là nút đồng thuận.

Sau bước 710 hoặc bước 712, phương pháp 700 dừng lại.

Các phương pháp và các thiết bị được bộc lộ trong bản mô tả này có thể cải thiện tính bảo mật của mạng chuỗi khối bằng cách giảm thiểu các mối đe dọa bảo mật do các CA đáng ngờ hoặc tin tặc gây ra. Bằng cách từ chối việc thiết lập các phiên truyền thông với các nút có mã nhận dạng không được chứng nhận bởi CA đáng tin cậy, việc bảo mật của các nút của chuỗi khối tập đoàn có thể được cải thiện có thể được cải thiện đối với các nút không sử dụng danh sách tin cậy CA. Ngoài ra, hiệu quả của mạng chuỗi khối thực hiện các phương pháp và phương tiện được bộc lộ có thể vượt trội hơn hiệu quả của các chuỗi khối thông thường do giảm thời gian xử lý liên quan đến việc xác minh chuỗi tin cậy của chứng chỉ khóa công khai.

Các phương án và các thao tác được mô tả trong bản mô tả này có thể được thực hiện trong hệ mạch điện tử số hoặc trong phần mềm, phần sụn hoặc phần cứng của

máy tính, bao gồm các kết cấu được bộc lộ trong bản mô tả này hoặc tổ hợp của một hoặc nhiều trong số chúng. Các thao tác có thể được thực hiện là các thao tác được thực hiện bởi thiết bị xử lý dữ liệu đối với dữ liệu được lưu trên một hoặc nhiều thiết bị lưu trữ đọc được bằng máy tính hoặc nhận được từ các nguồn khác. Phương tiện xử lý dữ liệu, máy tính hoặc thiết bị điện toán có thể bao gồm phương tiện, các thiết bị và các máy xử lý dữ liệu, bao gồm theo cách ví dụ bộ xử lý lập trình được, máy tính, hệ thống trên chip hoặc nhiều thiết bị này hoặc tổ hợp của các thiết bị nêu trên. Phương tiện này có thể bao gồm hệ mạch logic chuyên dụng, ví dụ, bộ xử lý trung tâm (Central Processing Unit, CPU), mảng cổng lập trình được dạng trường (Field Programmable Gate Array, FPGA) hoặc mạch tích hợp chuyên dụng (Application-Specific Integrated Circui, ASIC). Phương tiện này có thể cũng bao gồm mã tạo ra môi trường thực thi cho chương trình máy tính đang đề cập, ví dụ, mã cấu thành phần sun của bộ xử lý, chồng giao thức, hệ thống quản lý cơ sở dữ liệu, hệ điều hành (ví dụ hệ điều hành hoặc tổ hợp của các hệ điều hành), môi trường thời gian chạy đa nền tảng, máy ảo hoặc tổ hợp của một hoặc nhiều trong số các thiết bị này. Phương tiện và môi trường thực thi có thể nhận biết các cơ sở hạ tầng mô hình điện toán khác nhau, chẳng hạn như các dịch vụ web, cơ sở hạ tầng điện toán phân tán và điện toán dạng lưới.

Chương trình máy tính (cũng đã biết, ví dụ là chương trình, phần mềm, ứng dụng phần mềm, môđun phần mềm, bộ phận phần mềm, tập lệnh hoặc mã) có thể được viết ở dạng ngôn ngữ lập trình bất kỳ, bao gồm các ngôn ngữ biên dịch hoặc thông dịch, các ngôn ngữ khai báo hoặc thủ tục và có thể được triển khai ở dạng bất kỳ, bao gồm là chương trình độc lập hoặc là môđun, thành phần, thường trình con, đối tượng hoặc bộ phận khác thích hợp để sử dụng trong môi trường điện toán. Chương trình có thể được lưu trong một phần của tệp tin chứa các chương trình hoặc dữ liệu khác (ví dụ, một hoặc nhiều tập lệnh được lưu trong tài liệu ngôn ngữ đánh dấu), trong một tệp tin chuyên dụng cho chương trình đang đề cập, hoặc trong nhiều tệp tin phối hợp (ví dụ, các tệp tin lưu một hoặc nhiều môđun, các chương tình con hoặc các đoạn mã). Chương trình máy tính có thể được thực thi trên một máy tính hoặc trên nhiều máy tính được đặt ở một vị trí hoặc được phân bố ở nhiều vị trí và được kết nối với nhau bởi mạng truyền thông.

Các bộ xử lý để thực thi chương trình máy tính bao gồm, bằng cách lấy ví dụ, cả

bộ vi xử lý đa năng và chuyên dụng và một hoặc nhiều bộ xử lý bất kỳ của loại máy tính kỹ thuật số bất kỳ. Nói chung, bộ xử lý sẽ nhận các lệnh và dữ liệu từ bộ nhớ chỉ đọc hoặc bộ nhớ truy cập ngẫu nhiên hoặc cả hai. Các bộ phận chính của máy tính là bộ xử lý để thực hiện các thao tác theo các lệnh và một hoặc nhiều thiết bị nhớ để lưu các lệnh và dữ liệu. Nói chung, máy tính cũng sẽ bao gồm hoặc được ghép nối về mặt vận hành để nhận dữ liệu từ hoặc truyền dữ liệu đến hoặc cả hai, một hoặc nhiều thiết bị lưu trữ lớn để lưu dữ liệu. Máy tính có thể được nhúng trong thiết bị khác, ví dụ, thiết bị di động, thiết bị hỗ trợ cá nhân kỹ thuật số (Personal Digital Assistant, PDA), bảng điều khiển trò chơi, bộ thu của hệ thống định vị toàn cầu (Global Positioning System, GPS) hoặc thiết bị lưu trữ cầm tay. Các thiết bị thích hợp để lưu các lệnh chương trình máy tính và dữ liệu bao gồm bộ nhớ bất khả biến, phương tiện và thiết bị nhớ, bao gồm, bằng cách lấy ví dụ, thiết bị nhớ bán dẫn, các đĩa từ và các đĩa quang từ. Bộ xử lý và bộ nhớ có thể được bổ sung thêm hoặc kết hợp trong, hệ mạch logic chuyên dụng.

Các thiết bị di động có thể bao gồm các thiết bị cầm tay, thiết bị người dùng (User Equipment, UE), các điện thoại di động (ví dụ, các điện thoại thông minh), các máy tính dạng bảng, các thiết bị đeo được (ví dụ, các đồng hồ thông minh và kính mắt thông minh), các thiết bị cấy ghép bên trong cơ thể người (ví dụ, các bộ cảm biến sinh học, các thiết bị cấy ghép ốc tai điện tử) hoặc các loại thiết bị di động khác. Các thiết bị di động có thể truyền thông không dây (ví dụ, sử dụng các tín hiệu tần số vô tuyến (Radio Frequency, RF) với các mạng truyền thông khác nhau (được mô tả dưới đây). Các thiết bị di động có thể bao gồm các bộ cảm biến để xác định các đặc tính của môi trường hiện tại của thiết bị di động này. Các bộ cảm biến có thể bao gồm các camera, micrô, bộ cảm biến tiệm cận, bộ cảm biến GPS, bộ cảm biến chuyển động, gia tốc kế, bộ cảm biến ánh sáng xung quanh, bộ cảm biến độ ẩm, con quay hồi chuyển, la bàn, khí áp kế, bộ cảm biến vân tay, hệ thống nhận diện khuôn mặt, bộ cảm biến RF (ví dụ, Wi-Fi và vô tuyến dạng ô), bộ cảm biến nhiệt hoặc các loại cảm biến khác. Ví dụ, các camera có thể bao gồm camera phía trước và phía sau có thấu kính di động hoặc cố định, đèn flash, bộ cảm biến hình ảnh và bộ xử lý hình ảnh. Camera có thể là camera megapixel có khả năng chụp chi tiết để nhận diện khuôn mặt và/hoặc mống mắt. Camera cùng với bộ xử lý dữ liệu và thông tin xác thực được lưu trong bộ nhớ hoặc được truy cập từ xa có thể tạo thành hệ thống nhận diện khuôn mặt. Hệ thống nhận

diện khuôn mặt hoặc một hoặc nhiều bộ cảm biến, ví dụ, các micrô, bộ cảm biến chuyển động, gia tốc kế, bộ cảm biến GPS hoặc bộ cảm biến RF, có thể được sử dụng để xác thực người dùng.

Để tạo ra tương tác với người dùng, các phương án có thể được thực hiện trên máy tính có thiết bị hiển thị và thiết bị đầu vào, ví dụ, màn hình tinh thể lỏng (Liquid Crystal Display, LCD) hoặc điốt phát quang hữu cơ (Organic Light-Emitting Diode, OLED)/màn hình hiển thị thực tế ảo (Virtual-Reality, VR)/thực tế tăng cường (Augmented-Reality, AR) để hiển thị lệnh cho người dùng và màn hình chạm, bàn phím và thiết bị trỏ nhờ đó người dùng có thể cấp đầu vào cho máy tính. Các loại thiết bị khác có thể cũng được sử dụng để tạo ra tương tác với người dùng; ví dụ, phản hồi được tạo ra cho người dùng có thể có dạng phản hồi cảm giác bất kỳ, ví dụ, phản hồi thị giác, phản hồi thính giác hoặc phản hồi xúc giác; và đầu vào từ người dùng có thể nhận được ở dạng bất kỳ, bao gồm đầu vào âm thanh, giọng nói hoặc xúc giác. Ngoài ra, máy tính có thể tương tác với người dùng bằng cách gửi các tài liệu đến và nhận các tài liệu từ thiết bị được sử dụng bởi người dùng; ví dụ, bằng cách gửi các trang web đến trình duyệt web trên thiết bị khách của người dùng để đáp lại các yêu cầu nhận được từ trình duyệt web.

Các phương án có thể được thực hiện bằng cách sử dụng các thiết bị điện toán được kết nối với nhau bởi dạng hoặc vật ghi bất kỳ của truyền thông dữ liệu số có dây hoặc không dây (tổ hợp của chúng), ví dụ, mạng truyền thông. Các ví dụ về các thiết bị liên kết là máy khách và máy chủ thường cách xa nhau thường tương tác qua mạng truyền thông. Máy khách, ví dụ, thiết bị di động, có thể tự thực hiện các giao dịch, với máy chủ hoặc qua máy chủ, ví dụ, thực hiện các giao dịch mua, bán, thanh toán, cho, gửi hoặc vay mượn hoặc cấp quyền thực hiện cho các giao dịch này. Các giao dịch này có thể theo thời gian thực sao cho thao tác hoặc phản hồi xấp xỉ về mặt thời gian; ví dụ một cá nhân nhận thấy thao tác hoặc phản hồi xảy ra đồng thời, chênh lệch về thời gian cho phản hồi sau thao tác của cá nhân đó nhỏ hơn 1 mini giây (ms) hoặc nhỏ hơn 1 giây (s) hoặc phản hồi không có thời gian trễ có tính đến các hạn chế xử lý của hệ thống.

Các ví dụ về các mạng truyền thông bao gồm mạng cục bộ (Local Area Network, LAN), mạng truy cập vô tuyến (Radio Access Network, RAN), mạng khu vực đô thị

(Metropolitan Area Network, MAN) và mạng diện rộng (Wide Area Network, WAN). Mạng truyền thông có thể bao gồm tất cả hoặc một phần trong số Internet, các mạng truyền thông khác hoặc tổ hợp của các mạng truyền thông. Thông tin có thể được truyền trên mạng truyền thông theo các giao thức và chuẩn khác nhau, bao gồm tiến hóa dài hạn (Long Term Evolution, LTE), 5G, IEEE 802, giao thức internet (Internet Protocol, IP) hoặc các giao thức khác hoặc tổ hợp của các giao thức này. Mạng truyền thông có thể truyền dữ liệu thoại, viđeo, sinh trắc hoặc xác thực hoặc thông tin khác giữa các thiết bị điện toán đã kết nối.

Các dấu hiệu được mô tả là các phương án thực hiện riêng biệt có thể được thực hiện, theo cách kết hợp, theo một phương án thực hiện, trong khi các dấu hiệu được mô tả là một phương án thực hiện có thể được thực hiện theo nhiều phương án thực hiện, riêng biệt hoặc theo tổ hợp con thích hợp bất kỳ. Các thao tác được mô tả và yêu cầu bảo hộ theo thứ tự cụ thể cần được hiểu là không yêu cầu thứ tự cụ thể này hay tất cả các thao tác được minh họa cần được thực hiện (một số thao tác có thể là tùy chọn). Một cách thích hợp, xử lý đa nhiệm hoặc song song (hoặc theo cách kết hợp của xử lý đa nhiệm và song song) có thể được thực hiện.

YÊU CẦU BẢO HỘ

1. Phương pháp truyền thông nút chuỗi khối, trong đó các nút chuỗi khối trong mạng chuỗi khối bao gồm nút dịch vụ, nút dịch vụ này lưu chứng chỉ được gửi bởi bên cung cấp chứng chỉ (Certificate Authority, CA) và được tạo cấu hình trước bởi danh sách tin cậy CA và phương pháp này bao gồm các bước:

nhận, bởi nút chuỗi khối thứ nhất, yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai;

xác định mã định danh CA tương ứng với chứng chỉ thứ hai;

xác định xem liệu mã định danh CA được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không; và

nếu có, thì thiết lập kết nối truyền thông với nút chuỗi khối thứ hai, trong đó bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai cụ thể bao gồm bước trả lại, bởi nút chuỗi khối thứ nhất, yêu cầu xác minh cho nút chuỗi khối thứ hai, và trong đó yêu cầu xác minh này bao gồm chứng chỉ thứ nhất của nút chuỗi khối thứ nhất, để nút chuỗi khối thứ hai xác định, dựa vào chứng chỉ thứ nhất và danh sách tin cậy CA được tạo cấu hình trước trong nút chuỗi khối thứ hai, xem liệu có thiết lập kết nối truyền thông với nút chuỗi khối thứ nhất hay không; hoặc

nếu không, thì bỏ qua bước kết nối truyền thông với nút chuỗi khối thứ hai.

2. Phương pháp theo điểm 1, trong đó các nút chuỗi khối còn bao gồm nút đồng thuận và nút đồng thuận này lưu chứng chỉ được gửi bởi CA và được tạo cấu hình trước bởi danh sách tin cậy CA.

3. Phương pháp theo điểm 1 hoặc 2, trong đó các nút chuỗi khối trong mạng chuỗi khối tương ứng với các CA không hoàn toàn giống nhau.

4. Phương pháp theo điểm 1, trong đó bước nhận, bởi nút chuỗi khối thứ nhất, yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai cụ thể bao gồm bước nhận, bởi nút chuỗi khối thứ nhất dựa vào giao thức bắt tay bảo mật lớp truyền tải (Transport Layer

Security, TLS), yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai.

5. Phương tiện truyền thông nút chuỗi khối, trong đó phương tiện này bao gồm:

môđun nhận, được tạo cấu hình để nhận yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai;

môđun xác định, được tạo cấu hình để xác định mã định danh CA tương ứng với chứng chỉ thứ hai; và

môđun xác định và thực thi, được tạo cấu hình để xác định xem liệu mã định danh CA được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không; và nếu có, thì thiết lập kết nối truyền thông với với nút chuỗi khối thứ hai; hoặc nếu không, thì bỏ qua bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai, trong đó

môđun xác định và thực thi trả lại yêu cầu xác minh cho nút chuỗi khối thứ hai, yêu cầu xác minh này bao gồm chứng chỉ thứ nhất của phương tiện, để nút chuỗi khối thứ hai xác định, dựa vào chứng chỉ thứ nhất và danh sách tin cậy CA được tạo cấu hình trước trong nút chuỗi khối thứ hai, xem liệu có thiết lập kết nối truyền thông với phương tiện này hay không, và

các nút chuỗi khối trong mạng chuỗi khối bao gồm nút dịch vụ, và nút dịch vụ này lưu chứng chỉ được gửi bởi CA và được tạo cấu hình trước bởi danh sách tin cậy CA.

6. Phương tiện theo điểm 5, trong đó các nút chuỗi khối còn bao gồm nút đồng thuận và nút đồng thuận này lưu chứng chỉ được gửi bởi CA và được tạo cấu hình trước bởi danh sách tin cậy CA.

7. Phương tiện theo điểm 5 hoặc 6, trong đó các nút chuỗi khối trong mạng chuỗi khối tương ứng với các CA không hoàn toàn giống nhau.

8. Phương tiện theo điểm 5, trong đó môđun nhận nhận, dựa vào giao thức bắt tay TLS, yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai.

9. Thiết bị truyền thông nút chuỗi khối, trong đó thiết bị truyền thông này bao gồm một

hoặc nhiều bộ xử lý và bộ nhớ, bộ nhớ lưu chương trình và chương trình này được thực thi bởi một hoặc nhiều bộ xử lý để thực hiện các bước sau:

nhận, ở nút chuỗi khối thứ nhất, yêu cầu truyền thông được gửi bởi nút chuỗi khối thứ hai, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai;

xác định mã định danh CA tương ứng với chứng chỉ thứ hai;

xác định xem liệu mã định danh CA được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không; và

nếu có, thì thiết lập kết nối truyền thông với nút chuỗi khối thứ hai, trong đó bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai cụ thể bao gồm bước trả lại, bởi nút chuỗi khối thứ nhất, yêu cầu xác minh cho nút chuỗi khối thứ hai, và trong đó yêu cầu xác minh này bao gồm chứng chỉ thứ nhất của nút chuỗi khối thứ nhất, để nút chuỗi khối thứ hai xác định, dựa vào chứng chỉ thứ nhất và danh sách tin cậy CA được tạo cấu hình trước trong nút chuỗi khối thứ hai, xem liệu có thiết lập kết nối truyền thông với nút chuỗi khối thứ nhất hay không; hoặc

nếu không, thì bỏ qua bước thiết lập kết nối truyền thông với với nút chuỗi khối thứ hai; trong đó

các nút chuỗi khối trong mạng chuỗi khối bao gồm nút dịch vụ, và nút dịch vụ này lưu chứng chỉ được gửi bởi CA và được tạo cấu hình trước bởi danh sách tin cậy CA.

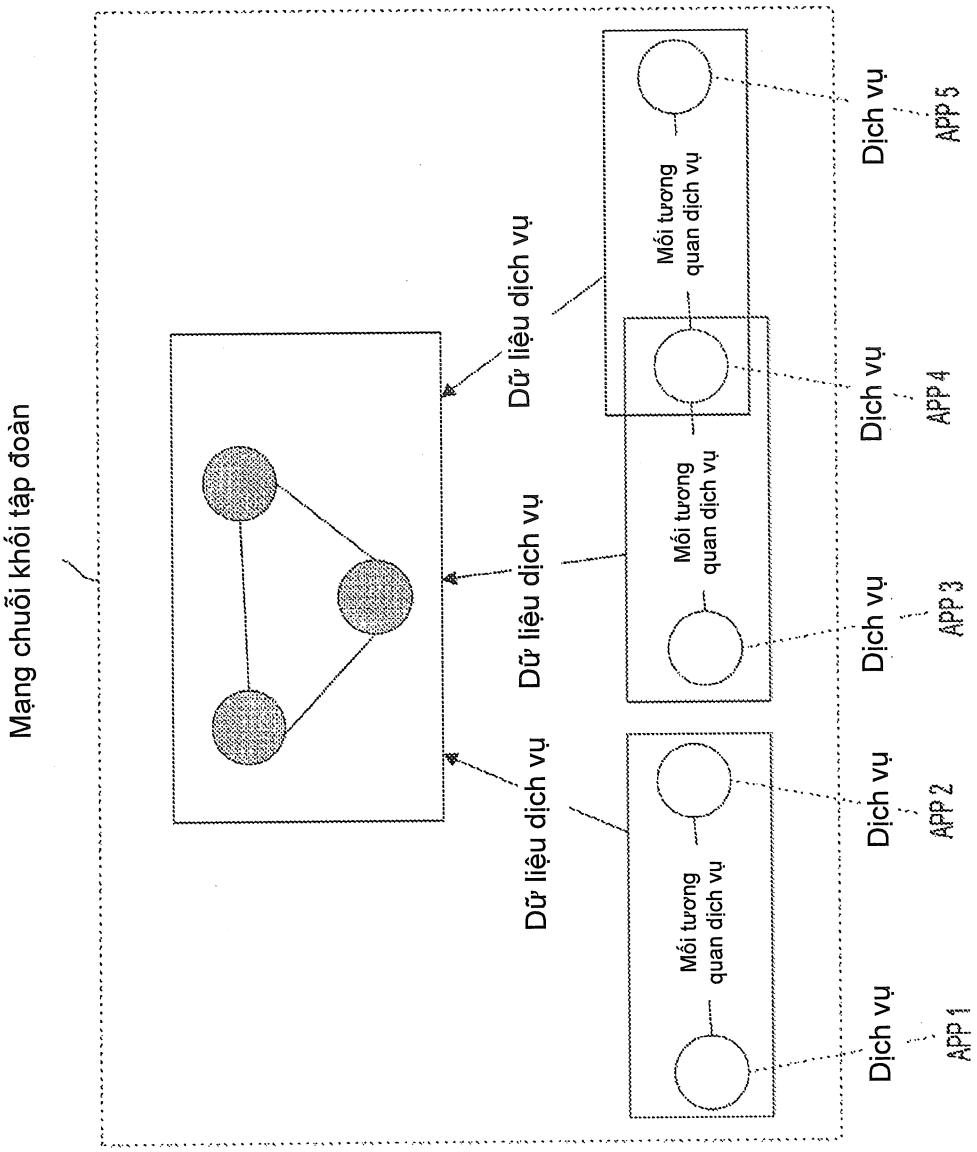

Mạng chuỗi khối tập đoàn
Dữ liệu dịch vụ
Dữ liệu dịch vụ
Dữ liệu dịch vụ
Mối tương quan dịch vụ
Mối tương quan dịch vụ
Mối tương quan dịch vụ
Dịch vụ
Dịch vụ
Dịch vụ
Dịch vụ
Dịch vụ
APP 1
APP 2
APP 3
APP 4
APP 5

FIG. 1

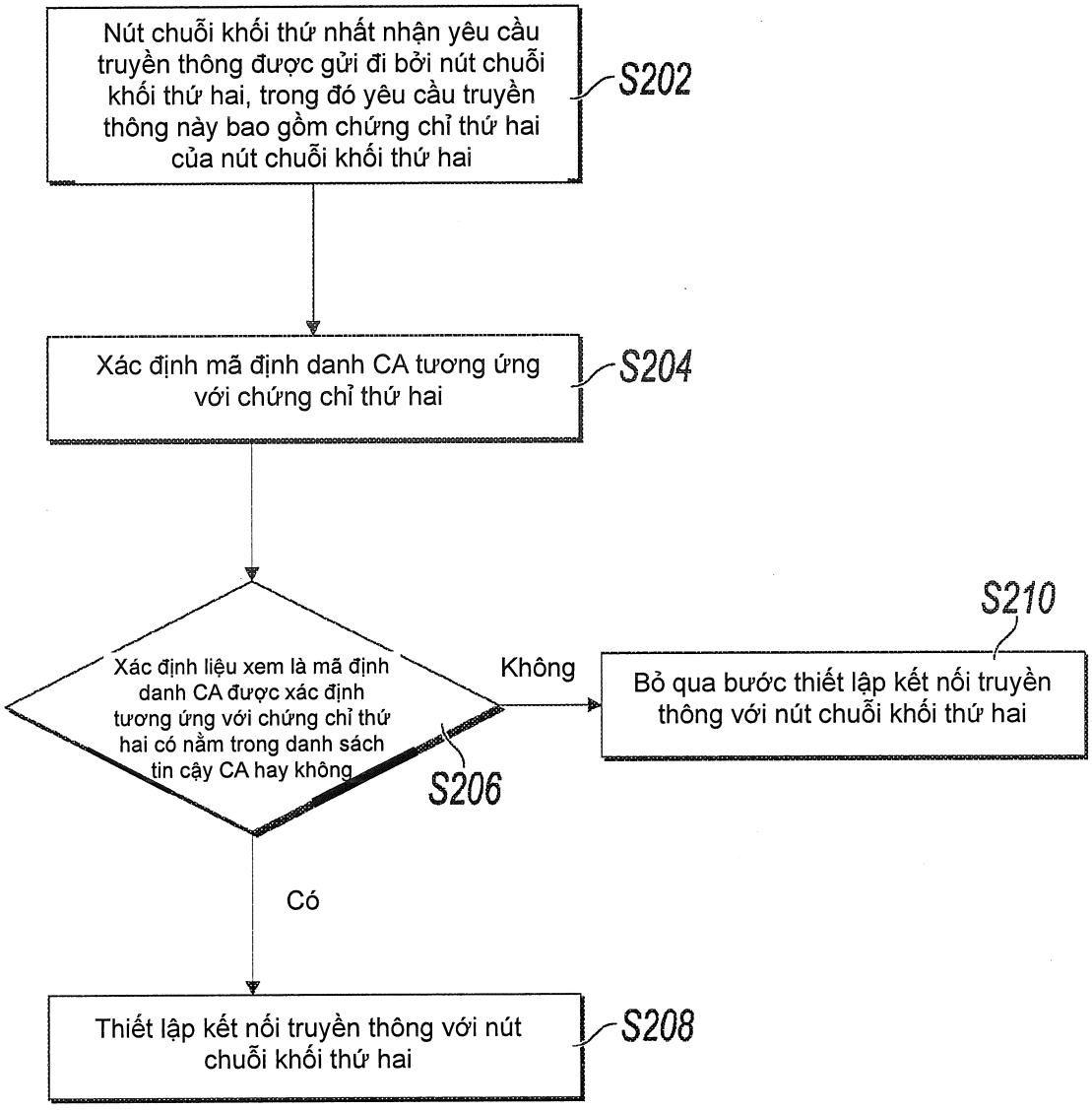

Nút chuỗi khối thứ nhất nhận yêu cầu truyền thông được gửi đi bởi nút chuỗi khối thứ hai, trong đó yêu cầu truyền thông này bao gồm chứng chỉ thứ hai của nút chuỗi khối thứ hai
S202
Xác định mã định danh CA tương ứng với chứng chỉ thứ hai
S204
Xác định liệu xem là mã định danh CA được xác định tương ứng với chứng chỉ thứ hai có nằm trong danh sách tin cậy CA hay không
S206
Không
S210
Bỏ qua bước thiết lập kết nối truyền thông với nút chuỗi khối thứ hai
Có
Thiết lập kết nối truyền thông với nút chuỗi khối thứ hai
S208

FIG. 2

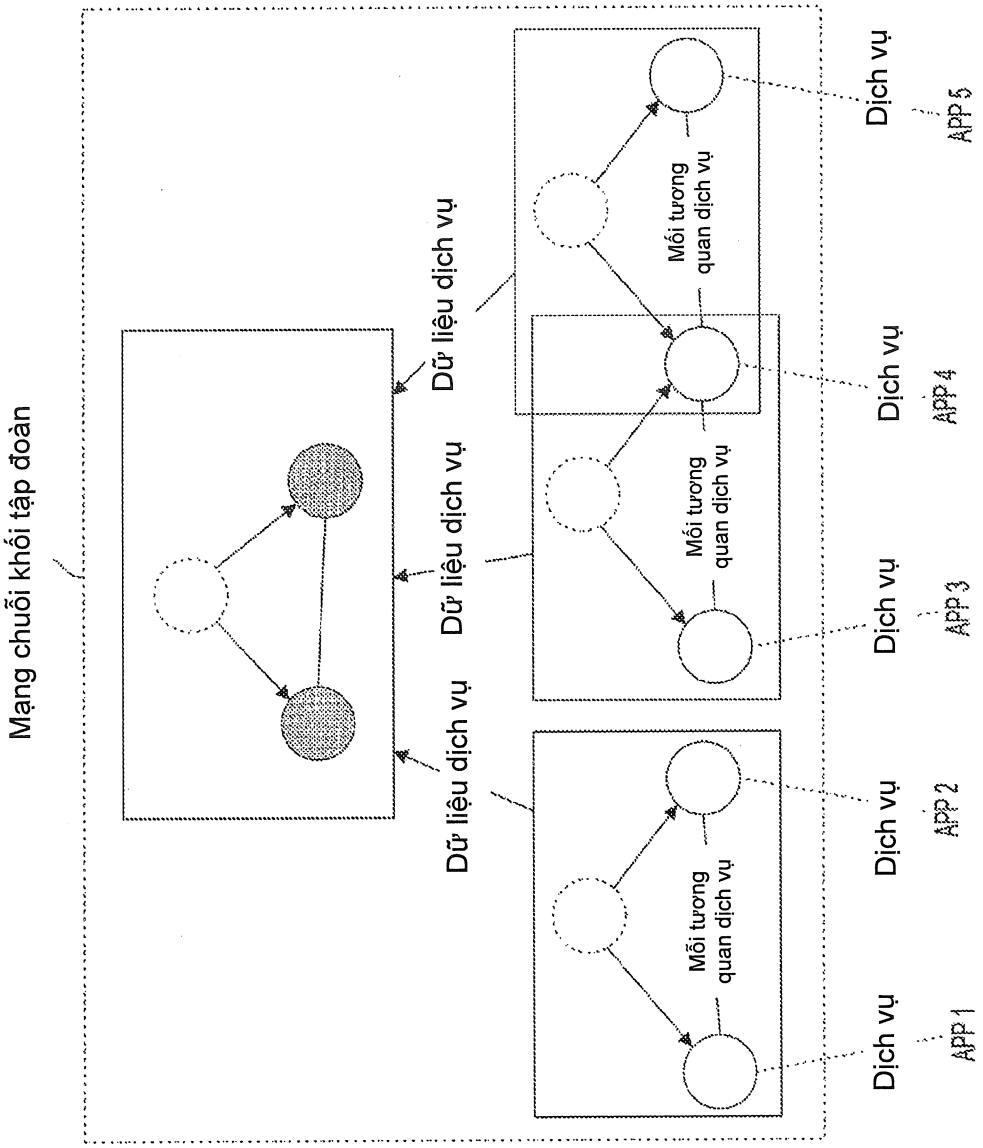

Mạng chuỗi khối tập đoàn
Dữ liệu dịch vụ
Dữ liệu dịch vụ
Dữ liệu dịch vụ
Mối tương quan dịch vụ
Mối tương quan dịch vụ
Mối tương quan dịch vụ
Dịch vụ
Dịch vụ
Dịch vụ
Dịch vụ
Dịch vụ
APP 1
APP 2
APP 3
APP 4
APP 5

FIG. 3

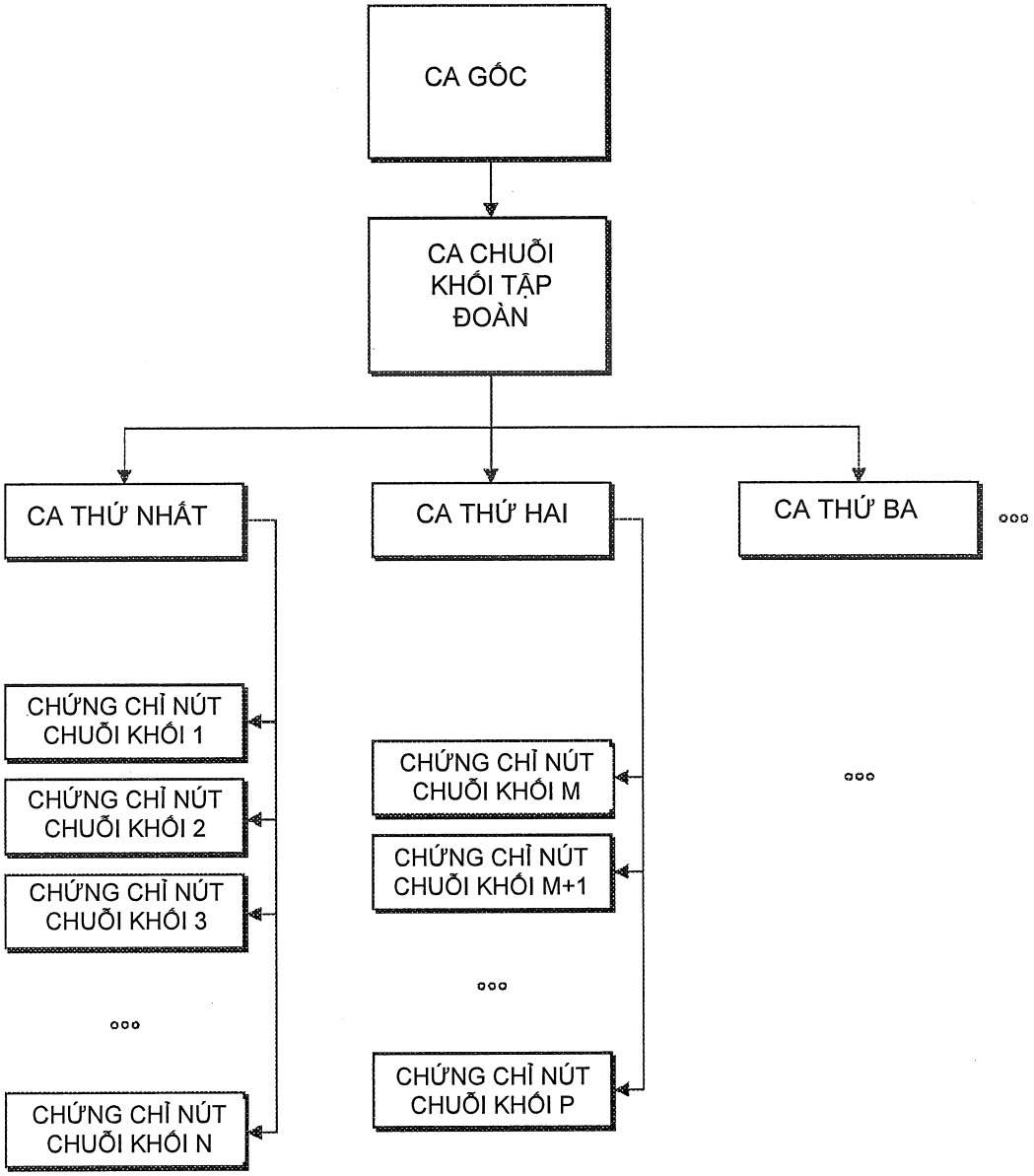

CA GỐC
CA CHUỖI KHỐI TẬP ĐOÀN
CA THỨ NHẤT
CA THỨ HAI
CA THỨ BA
CHỨNG CHỈ NÚT CHUỖI KHỐI 1
CHỨNG CHỈ NÚT CHUỖI KHỐI 2
CHỨNG CHỈ NÚT CHUỖI KHỐI 3
CHỨNG CHỈ NÚT CHUỖI KHỐI N
CHỨNG CHỈ NÚT CHUỖI KHỐI M
CHỨNG CHỈ NÚT CHUỖI KHỐI M+1
CHỨNG CHỈ NÚT CHUỖI KHỐI P

FIG. 4

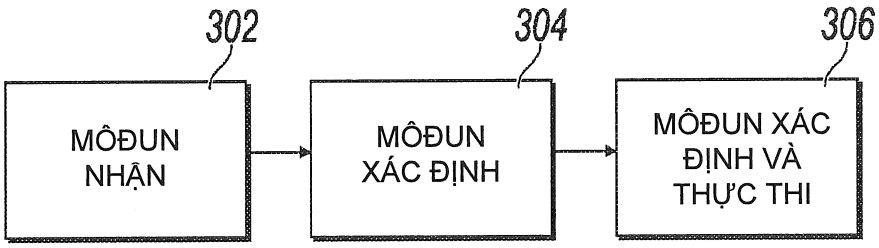

302
304
306
MÔĐUN NHẬN
MÔĐUN XÁC ĐỊNH
MÔĐUN XÁC ĐỊNH VÀ THỰC THI

FIG. 5

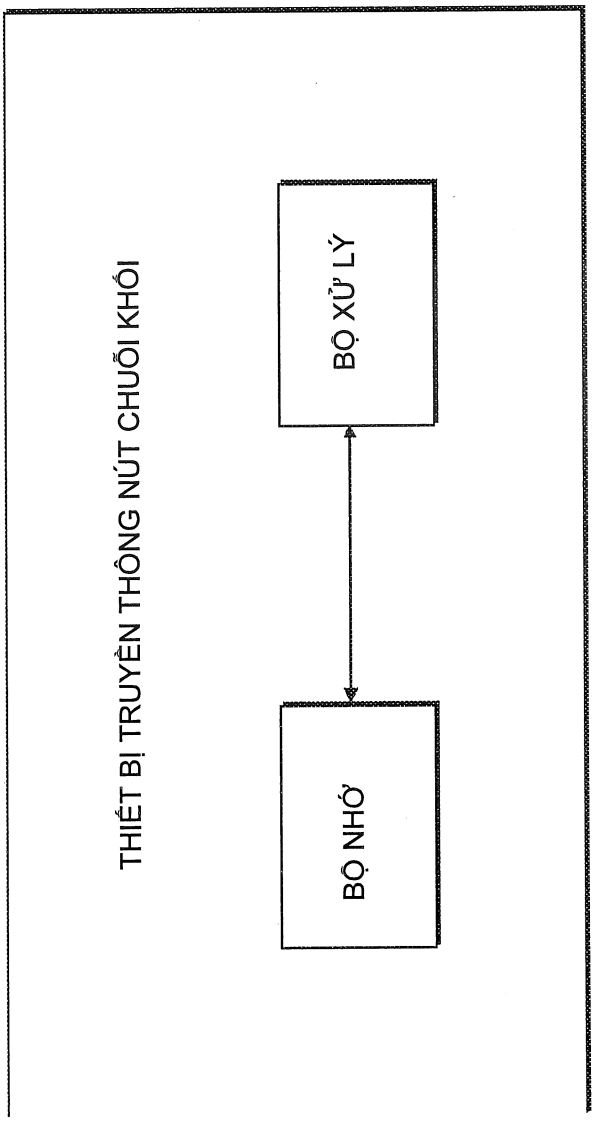


FIG. 6

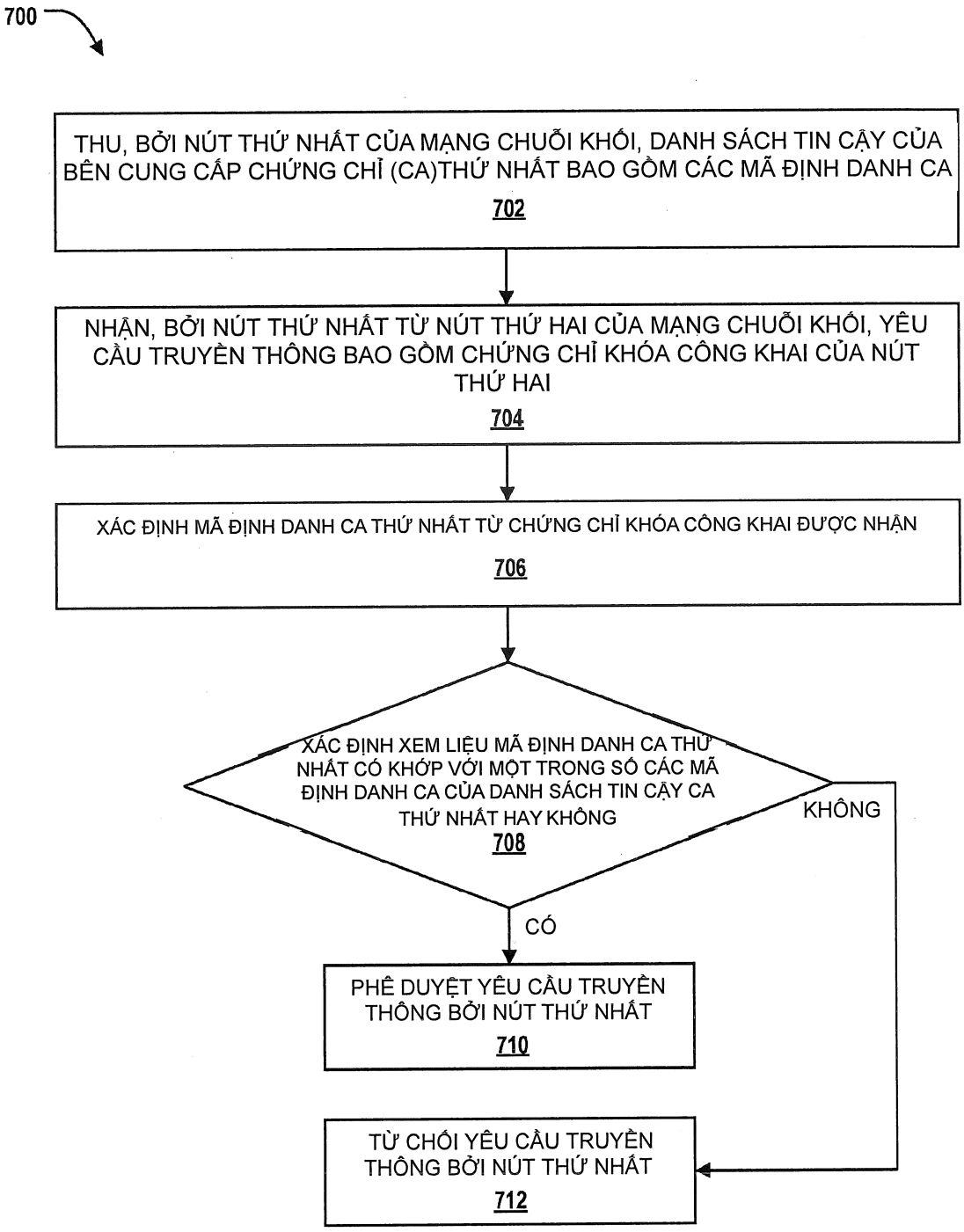

700
THU, BỞI NÚT THỨ NHẤT CỦA MẠNG CHUỖI KHỐI, DANH SÁCH TIN CẬY CỦA BÊN CUNG CẤP CHỨNG CHỈ (CA)THỨ NHẤT BAO GỒM CÁC MÃ ĐỊNH DANH CA
702
NHẬN, BỞI NÚT THỨ NHẤT TỪ NÚT THỨ HAI CỦA MẠNG CHUỖI KHỐI, YÊU CẦU TRUYỀN THÔNG BAO GỒM CHỨNG CHỈ KHÓA CÔNG KHAI CỦA NÚT THỨ HAI
704
XÁC ĐỊNH MÃ ĐỊNH DANH CA THỨ NHẤT TỪ CHỨNG CHỈ KHÓA CÔNG KHAI ĐƯỢC NHẬN
706
XÁC ĐỊNH XEM LIỆU MÃ ĐỊNH DANH CA THỨ NHẤT CÓ KHỚP VỚI MỘT TRONG SỐ CÁC MÃ ĐỊNH DANH CA CỦA DANH SÁCH TIN CẬY CA THỨ NHẤT HAY KHÔNG
708
KHÔNG
CÓ
PHÊ DUYỆT YÊU CẦU TRUYỀN THÔNG BỞI NÚT THỨ NHẤT
710
TỪ CHỐI YÊU CẦU TRUYỀN THÔNG BỞI NÚT THỨ NHẤT
712

FIG. 7