



(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)



1-0033417

(51)⁷ G06F 21/64; H04L 29/06; G06Q 20/06 (13) B

(21) 1-2019-04034

(22) 26/07/2018

(86) PCT/US2018/043919 26/07/2018

(87) WO 2019/023470 31/01/2019

(30) 201710617599.7 26/07/2017 CN

(45) 26/09/2022 414

(43) 27/04/2020 385ASC

(73) Advanced New Technologies Co., Ltd. (KY)

Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands

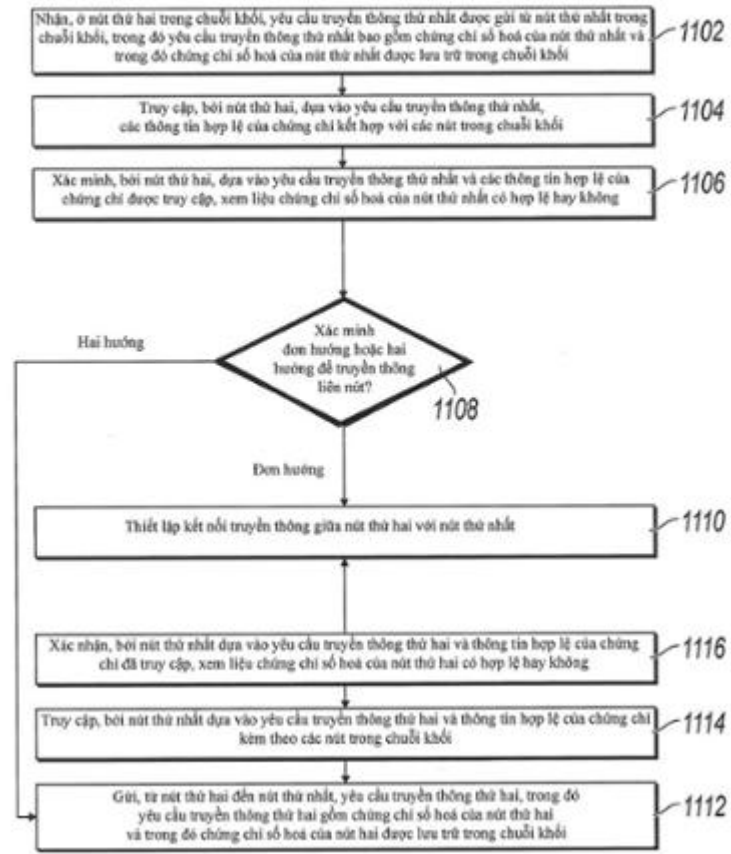
(72) QIU, Honglin (CN).

(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ ĐIỆN TỬ ĐỂ TRUYỀN THÔNG GIỮA CÁC NÚT CHUỖI KHỐI VÀ QUẢN LÝ CHỨNG CHỈ TRÊN CƠ SỞ CHUỖI KHỐI

(57) Sáng chế đề cập đến phương pháp truyền thông giữa các nút chuỗi khối, trong đó yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất thu được bởi nút thứ hai, ở đó yêu cầu truyền thông thứ nhất gồm chứng chỉ số hóa của nút thứ nhất và chứng chỉ số hóa của nút thứ nhất được lưu trữ trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai. Xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không được xác minh bằng nút thứ hai dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, ở đó thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa của nút. Khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không được xác định bởi nút thứ hai. Ngoài ra, sáng chế còn đề cập đến thiết bị điện tử để truyền thông giữa các nút chuỗi khối và để quản lý chứng chỉ số hóa trên cơ sở chuỗi khối.

1100



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ máy tính và cụ thể là phương pháp, thiết bị và thiết bị điện tử để truyền thông giữa các nút chuỗi khối và phương pháp, thiết bị và thiết bị điện tử để quản lý chứng chỉ số hóa trên cơ sở chuỗi khối.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển của các công nghệ máy tính, công nghệ chuỗi khối (cũng được gọi là công nghệ sổ cái phân tán) được ưa chuộng nhờ các ưu điểm như sự phi tập trung, công khai và minh bạch, chống làm giả và tin cậy và do đó, được áp dụng rộng rãi cho nhiều lĩnh vực, ví dụ, giao kết thông minh, giao dịch an toàn, thương mại điện tử, internet kết nối vạn vật, truyền thông xã hội, lưu trữ tệp tin, chứng minh sự tồn tại, xác thực nhận dạng và gọi vốn cộng đồng theo hình thức góp cổ phần.

Hiện nay, các hệ thống chuỗi khối chủ yếu rơi vào ba loại: chuỗi khối công khai, chuỗi khối bí mật và chuỗi khối tập đoàn. Ba loại chuỗi khối này khác biệt chủ yếu về các đối tượng mở. Chuỗi khối công khai được mở cho mọi người. Chuỗi khối bí mật mở cho một cá thể, thực thể hoặc tổ chức. Chuỗi khối tập đoàn được mở cho cá thể cụ thể, thực thể hoặc tổ chức và không mở cho các cá nhân, các thực thể hoặc các tổ chức khác.

Trong chuỗi khối, đặc biệt trong chuỗi khối tập đoàn cho tổ chức cụ thể, để nâng cao tính bảo mật truyền thông, trung tâm cấp phép chứng chỉ (trung tâm CA) thường được thiết kế để cấp chứng chỉ nút tới mỗi nút mà tham gia vào quá trình truyền thông chuỗi khối, sao cho chỉ các nút giữ các chứng chỉ hợp lệ mới có thể truyền thông với nhau. Theo một số phương án thực hiện, chứng chỉ nút được cấp và thông tin liên quan đến tính hợp lệ của chứng chỉ, ví dụ, danh sách thu hồi chứng chỉ, được lưu trữ trong máy chủ ở trung tâm CA. Khi các nút trong chuỗi khối cần truyền thông với nhau, thì thông tin được lưu trữ ở trung tâm CA và liên quan đến tính hợp lệ của chứng chỉ được gọi và truy vấn, để khẳng định tính hợp lệ của chứng chỉ và hoàn thành việc xác minh

quy trình truyền thông. Các hạn chế chính của phương pháp này là như sau:

Việc truyền thông bảo mật trong số các nút chuỗi khối phụ thuộc vào việc xác minh tính hợp lệ của chứng chỉ nút khi thiết lập kết nối truyền thông. Khi trung tâm CA bị tấn công, tin tặc có thể thay đổi tùy ý thông tin liên quan đến tính hợp lệ của chứng chỉ. Ví dụ, tin tặc có thể làm giả danh sách thu hồi chứng chỉ và khôi phục chứng chỉ đã hủy trở thành chứng chỉ bình thường. Tin tặc có thể còn sử dụng các chứng chỉ đã hủy trước đây để tham gia vào chuỗi khối mà không cần cho phép và nút trong chuỗi khối khẳng định tính hợp lệ của chứng chỉ dựa vào thông tin bị làm giả, gây đe dọa đối với tính bảo mật của chuỗi khối.

Bản chất kỹ thuật của sáng chế

Theo phương án thực hiện, sáng chế đề xuất phương pháp, thiết bị và thiết bị điện tử để truyền thông giữa các nút chuỗi khối và phương pháp, thiết bị và thiết bị điện tử để quản lý chứng chỉ số hóa trên cơ sở chuỗi khối, để nâng cao tính bảo mật truyền thông giữa các nút chuỗi khối và còn nâng cao độ an toàn của mạng chuỗi khối.

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

Theo khía cạnh thứ nhất của phương án thực hiện, sáng chế đề xuất phương pháp truyền thông giữa các nút chuỗi khối, bao gồm các bước: nhận, bởi nút thứ hai, yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, ở đó yêu cầu truyền thông thứ nhất gồm chứng chỉ số hóa của nút thứ nhất và chứng chỉ số hóa của nút thứ nhất được lưu trữ trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai; xác minh, bởi nút thứ hai dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không, ở đó thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa của nút; và khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, thì xác định, bởi nút thứ hai, xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không.

Tốt hơn nếu phương pháp truyền thông giữa các nút chuỗi khối được đề xuất theo khía cạnh thứ nhất còn bao gồm các bước: gửi, bởi nút thứ hai, yêu cầu truyền thông thứ hai tới nút thứ nhất, ở đó yêu cầu truyền thông thứ hai bao gồm chứng chỉ số hóa của

nút thứ hai, để nút thứ nhất xác minh, dựa vào yêu cầu truyền thông thứ hai và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ hai là hợp lệ hay không; và khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, thì bước xác định, bởi nút thứ hai, xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không bao gồm: khi chứng chỉ số hóa của nút thứ nhất là hợp lệ và nút thứ nhất xác minh rằng chứng chỉ số hóa của nút thứ hai là hợp lệ, thiết lập, bởi nút thứ hai, kết nối truyền thông với nút thứ nhất.

Tốt hơn nếu trong phương pháp truyền thông giữa các nút chuỗi khối được đề xuất theo khía cạnh thứ nhất, thông tin hợp lệ của chứng chỉ ghi lại chứng chỉ số hóa không hợp lệ được hủy và bước xác minh, bởi nút thứ hai dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không bao gồm: xác định, bởi nút thứ hai, chứng chỉ số hóa của nút thứ nhất dựa vào yêu cầu truyền thông thứ nhất; xác minh, bởi nút thứ hai dựa vào thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối, xem liệu chứng chỉ số hóa của nút thứ nhất có được ghi lại trong thông tin hợp lệ của chứng chỉ hay không; và xác minh rằng chứng chỉ số hóa của nút thứ nhất là không hợp lệ, nếu chứng chỉ số hóa của nút thứ nhất được ghi lại trong thông tin hợp lệ của chứng chỉ.

Tốt hơn nếu trong phương pháp truyền thông giữa các nút chuỗi khối được đề xuất theo khía cạnh thứ nhất, thông tin hợp lệ của chứng chỉ ghi lại chứng chỉ số hóa hợp lệ và bước xác minh, bởi nút thứ hai dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không bao gồm: xác định, bởi nút thứ hai, chứng chỉ số hóa của nút thứ nhất dựa vào yêu cầu truyền thông thứ nhất; xác minh, bởi nút thứ hai dựa vào thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối, xem liệu chứng chỉ số hóa của nút thứ nhất có được ghi lại trong thông tin hợp lệ của chứng chỉ hay không; và xác minh rằng chứng chỉ số hóa của nút thứ nhất là hợp lệ, nếu chứng chỉ số hóa của nút thứ nhất được ghi lại trong thông tin hợp lệ của chứng chỉ.

Tốt hơn nếu trước khi nhận, bởi nút thứ hai, yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, phương pháp truyền thông giữa các nút chuỗi khối được đề xuất theo khía cạnh thứ nhất còn bao gồm các bước: lưu trữ, bằng cách ghi chứng chỉ số hóa của nút thứ nhất vào chuỗi khối, chứng chỉ số hóa của nút thứ nhất trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai.

Tốt hơn nếu trong phương pháp truyền thông giữa các nút chuỗi khối được đề xuất theo khía cạnh thứ nhất, thông tin hợp lệ của chứng chỉ được xác định dựa vào chứng chỉ số hóa không hợp lệ đã hủy và/hoặc chứng chỉ số hóa hợp lệ nhận được bởi chuỗi khối.

Tốt hơn nếu trong phương pháp truyền thông giữa các nút chuỗi khối được đề xuất theo khía cạnh thứ nhất, yêu cầu truyền thông thứ nhất thu được bởi nút thứ hai được gửi bởi nút thứ nhất dựa vào giao thức lớp cổng bảo mật (Secure Sockets Layer - SSL) hoặc giao thức bảo mật lớp vận chuyển (Transport Layer Security (TLS).

Theo khía cạnh thứ hai của một phương án thực hiện, sáng chế đề xuất phương pháp quản lý chứng chỉ số hóa trên cơ sở chuỗi khối, bao gồm các bước: nhận chứng chỉ số hóa của nút và thông tin tình trạng hợp lệ của chứng chỉ số hóa được gửi bởi trung tâm CA; xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá; và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ trong chuỗi khối, ở đó chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ được sử dụng để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Tốt hơn nếu phương pháp quản lý chứng chỉ số hóa dựa vào chuỗi khối được đề xuất theo khía cạnh thứ hai còn bao gồm các bước: gửi, bởi nút thứ nhất trong chuỗi khối, yêu cầu áp dụng chứng chỉ cho trung tâm CA, ở đó yêu cầu áp dụng chứng chỉ bao gồm thông tin áp dụng của nút thứ nhất và được sử dụng để áp dụng cho trung tâm CA đối với chứng chỉ số hóa của nút thứ nhất.

Theo khía cạnh thứ ba của một phương án thực hiện, sáng chế đề xuất phương pháp quản lý chứng chỉ số hóa trên cơ sở chuỗi khối, phương pháp này bao gồm các bước: gửi chứng chỉ số hóa của nút trong chuỗi khối và thông tin tình trạng hợp lệ của chứng chỉ số hóa tới chuỗi khối, để chuỗi khối xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ, để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu

truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Tốt hơn nếu phương pháp quản lý chứng chỉ số hóa dựa vào chuỗi khối được đề xuất theo khía cạnh thứ ba còn bao gồm các bước: nhận yêu cầu áp dụng chứng chỉ được gửi bởi nút trong chuỗi khối, ở đó yêu cầu áp dụng chứng chỉ bao gồm thông tin áp dụng của nút thứ nhất và được sử dụng để áp dụng cho trung tâm CA đối với chứng chỉ số hóa của nút thứ nhất; nhận và xem lại thông tin áp dụng của nút thứ nhất; và khi thông tin áp dụng của nút thứ nhất đã được xem lại, thì cấp chứng chỉ số hóa tới nút thứ nhất, ở đó thông tin tình trạng hợp lệ của chứng chỉ số hóa là hợp lệ.

Theo khía cạnh thứ tư của một phương án thực hiện, sáng chế đề xuất thiết bị truyền thông giữa các nút chuỗi khối. Thiết bị này được áp dụng cho nút thứ hai trong chuỗi khối và bao gồm: môđun thu yêu cầu truyền thông, được tạo cấu hình để thu yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, ở đó yêu cầu truyền thông thứ nhất gồm chứng chỉ số hóa của nút thứ nhất và chứng chỉ số hóa của nút thứ nhất được lưu trữ trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai; môđun xác minh hợp lệ, được tạo cấu hình để xác minh, dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không, ở đó thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa của nút; và môđun thiết lập kết nối truyền thông, được tạo cấu hình để: khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, thì xác định xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không.

Tốt hơn nếu thiết bị truyền thông giữa các nút chuỗi khối được đề xuất theo khía cạnh thứ tư còn bao gồm: môđun gửi yêu cầu truyền thông, được tạo cấu hình để gửi yêu cầu truyền thông thứ hai tới nút thứ nhất, ở đó yêu cầu truyền thông thứ hai bao gồm chứng chỉ số hóa của nút thứ hai, để nút thứ nhất xác minh, dựa vào yêu cầu truyền thông thứ hai và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ hai là hợp lệ hay không; và môđun thiết lập kết nối truyền thông đặc biệt được tạo cấu hình để: khi chứng chỉ số hóa của nút thứ nhất là hợp lệ và nút thứ nhất xác minh rằng chứng chỉ số hóa của nút thứ hai là hợp lệ, thì thiết lập kết nối truyền thông với nút thứ nhất.

Theo khía cạnh thứ năm của một phương án thực hiện, sáng chế đề xuất thiết bị điện tử. Thiết bị điện tử này được áp dụng cho nút thứ hai trong chuỗi khối và bao gồm: bộ xử lý; và bộ nhớ, được tạo cấu hình để lưu trữ lệnh thực thi được bằng máy tính, ở đó lệnh thực thi được thực thi bởi bộ xử lý để thực hiện các thao tác sau đây: nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, ở đó yêu cầu truyền thông thứ nhất gồm chứng chỉ số hóa của nút thứ nhất và chứng chỉ số hóa của nút thứ nhất được lưu trữ trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai; xác minh, dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không, ở đó thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa của nút; và khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, thì xác định xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không.

Tốt hơn nếu trong thiết bị điện tử được đề xuất theo khía cạnh thứ năm, lệnh thực thi được thực thi bởi bộ xử lý để còn thực hiện các thao tác sau đây: gửi yêu cầu truyền thông thứ hai tới nút thứ nhất, ở đó yêu cầu truyền thông thứ hai bao gồm chứng chỉ số hóa của nút thứ hai, để nút thứ nhất xác minh, dựa vào yêu cầu truyền thông thứ hai và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ hai là hợp lệ hay không; và khi chứng chỉ số hóa của nút thứ nhất là hợp lệ và nút thứ nhất xác minh rằng chứng chỉ số hóa của nút thứ hai là hợp lệ, thiết lập, bởi nút thứ hai, kết nối truyền thông với nút thứ nhất.

Theo khía cạnh thứ sáu của một phương án thực hiện, sáng chế đề xuất thiết bị quản lý chứng chỉ số hóa trên cơ sở chuỗi khối. Thiết bị này được áp dụng cho chuỗi khối và bao gồm: môđun nhận thông tin chứng chỉ, được tạo cấu hình để thu chứng chỉ số hóa của nút và thông tin tình trạng hợp lệ của chứng chỉ số hóa được gửi bởi trung tâm CA; thông tin hợp lệ của môđun xác định chứng chỉ, được tạo cấu hình để xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá; và môđun lưu trữ, được tạo cấu hình để lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ trong chuỗi khối, ở đó chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ được sử dụng để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu

truyền thông thứ nhất là hợp lệ hay không.

Theo khía cạnh thứ bảy của một phương án thực hiện, sáng chế đề xuất thiết bị điện tử. Thiết bị điện tử này được áp dụng cho chuỗi khối và bao gồm: bộ xử lý; và bộ nhớ, được tạo cấu hình để lưu trữ lệnh thực thi được bằng máy tính, ở đó lệnh thực thi được thực thi bởi bộ xử lý để thực hiện các thao tác sau đây: nhận chứng chỉ số hóa của nút và thông tin tình trạng hợp lệ của chứng chỉ số hóa được gửi bởi trung tâm CA; xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá; và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ trong chuỗi khối, ở đó chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ được sử dụng để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Theo khía cạnh thứ tám của một phương án thực hiện, sáng chế đề xuất thiết bị quản lý chứng chỉ số hóa trên cơ sở chuỗi khối. Thiết bị này được áp dụng cho trung tâm CA và bao gồm: môđun gửi, được tạo cấu hình để gửi chứng chỉ số hóa của nút trong chuỗi khối và thông tin tình trạng hợp lệ của chứng chỉ số hóa tới chuỗi khối, để chuỗi khối xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ, để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Tốt hơn nếu thiết bị quản lý chứng chỉ số hóa dựa vào chuỗi khối được đề xuất theo khía cạnh thứ tám còn bao gồm: mô đun nhận yêu cầu áp dụng, được tạo cấu hình để thu yêu cầu áp dụng chứng chỉ được gửi bởi nút trong chuỗi khối, ở đó yêu cầu áp dụng chứng chỉ bao gồm thông tin áp dụng của nút thứ nhất và được sử dụng để áp dụng cho trung tâm CA đối với chứng chỉ số hóa của nút thứ nhất; mô đun nhận và xem lại, được tạo cấu hình để thu và xem lại thông tin áp dụng của nút thứ nhất; và mô đun cấp và gửi, được tạo cấu hình để: khi thông tin áp dụng của nút thứ nhất đã được xem lại, thì cấp chứng chỉ số hóa tới nút thứ nhất, ở đó thông tin tình trạng hợp lệ của chứng chỉ

số hóa là hợp lệ.

Theo khía cạnh thứ chín của một phương án thực hiện, sáng chế đề xuất thiết bị điện tử. Thiết bị điện tử này được áp dụng cho trung tâm CA và bao gồm: bộ xử lý; và bộ nhớ, được tạo cấu hình để lưu trữ lệnh thực thi được bằng máy tính, ở đó lệnh thực thi được thực thi bởi bộ xử lý để thực hiện các thao tác sau đây: gửi chứng chỉ số hóa của nút trong chuỗi khối và thông tin tình trạng hợp lệ của chứng chỉ số hóa tới chuỗi khối, để chuỗi khối xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hóa, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ, để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Tốt hơn nếu trong thiết bị điện tử được đề xuất theo khía cạnh thứ chín, lệnh thực thi được thực thi bởi bộ xử lý để còn thực hiện các thao tác sau đây: nhận yêu cầu áp dụng chứng chỉ được gửi bởi nút trong chuỗi khối, ở đó yêu cầu áp dụng chứng chỉ bao gồm thông tin áp dụng của nút thứ nhất và được sử dụng để áp dụng cho trung tâm CA đối với chứng chỉ số hóa của nút thứ nhất; nhận và xem lại thông tin áp dụng của nút thứ nhất; và khi thông tin áp dụng của nút thứ nhất đã được xem lại, cấp chứng chỉ số hóa tới nút thứ nhất, ở đó thông tin tình trạng hợp lệ của chứng chỉ số hóa là hợp lệ.

Các phương án thực hiện của sáng chế có thể sử dụng ít nhất một trong các giải pháp kỹ thuật nêu trên để đạt được các tác dụng có lợi sau đây.

Nhờ việc sử dụng các giải pháp kỹ thuật của sáng chế, chứng chỉ số hóa được yêu cầu khi nút thứ nhất gửi yêu cầu truyền thông được lưu trữ trong chuỗi khối và thông tin hợp lệ của chứng chỉ được sử dụng làm nền tảng khi nút thứ hai xác minh xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không cũng được lưu trữ trong chuỗi khối. Bởi vì các ưu điểm như sự phi tập trung, công khai và minh bạch và chống làm giả của chuỗi khối, thậm chí nếu trung tâm CA bị tấn công, thì tin tặc không thể làm giả chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và do đó, không thể sử dụng chứng chỉ số hóa không hợp lệ để tham gia vào chuỗi khối. Thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và có thể phản ánh đúng thông

tin tình trạng hợp lệ của chứng chỉ nút. Do đó, nhờ việc sử dụng thông tin hợp lệ của chứng chỉ để xác minh xem liệu chứng chỉ nút có hợp lệ hay không, nút chưa được phép có thể được ngăn không cho tham gia vào chuỗi khối, để đảm bảo tính bảo mật truyền thông giữa các nút chuỗi khối và còn gia tăng tính bảo mật của mạng chuỗi khối.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo được mô tả ở đây được dự tính làm rõ hơn về sáng chế và tạo thành một phần của sáng chế. Các phương án thực hiện minh họa của sáng chế và phần mô tả của các phương án thực hiện được dự định để mô tả sáng chế và không làm giới hạn sáng chế. Trên các hình vẽ kèm theo:

Fig.1 là lưu đồ giản lược minh họa phương pháp truyền thông giữa các nút chuỗi khối theo phương án thực hiện của sáng chế.

Fig.2 là sơ đồ giản lược minh họa kịch bản có thể áp dụng đơn giản của phương pháp truyền thông giữa các nút chuỗi khối theo phương án thực hiện của sáng chế.

Fig.3 là lưu đồ giản lược minh họa phương pháp quản lý chứng chỉ số hóa trên cơ sở chuỗi khối theo phương án thực hiện của sáng chế.

Fig.4 là sơ đồ giản lược minh họa kịch bản có thể áp dụng, trong đó chuỗi khối và trung tâm CA tương tác để quản lý chứng chỉ số hóa theo phương án thực hiện của sáng chế.

Fig.5 là sơ đồ kết cấu giản lược minh họa thiết bị truyền thông giữa các nút chuỗi khối được áp dụng cho chuỗi khối theo phương án thực hiện của sáng chế.

Fig.6 là sơ đồ kết cấu giản lược minh họa thiết bị khác để truyền thông giữa các nút chuỗi khối được áp dụng cho chuỗi khối theo phương án thực hiện của sáng chế.

Fig.7 là sơ đồ kết cấu giản lược minh họa thiết bị điện tử được áp dụng cho nút trong chuỗi khối theo phương án thực hiện của sáng chế.

Fig.8 là sơ đồ kết cấu giản lược minh họa thiết bị quản lý chứng chỉ số hóa được áp dụng cho chuỗi khối theo phương án thực hiện của sáng chế.

Fig.9 là sơ đồ kết cấu giản lược minh họa thiết bị điện tử để quản lý chứng chỉ số hóa được áp dụng cho chuỗi khối theo phương án thực hiện của sáng chế.

Fig.10 là sơ đồ kết cấu giản lược minh họa thiết bị điện tử để quản lý chứng chỉ số hóa ở trung tâm CA, theo phương án thực hiện của sáng chế.

Fig.11 là lưu đồ minh họa ví dụ về phương pháp được thực hiện bằng máy tính để truyền thông giữa các nút chuỗi khối theo phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Để làm cho các mục đích, giải pháp kỹ thuật và các lợi ích của sáng chế rõ ràng hơn, phần sau đây mô tả các giải pháp kỹ thuật của sáng chế dựa vào các phương án cụ thể của sáng chế và các hình vẽ kèm theo tương ứng. Rõ ràng là các phương án thực hiện đã mô tả chỉ là một số hơn mà không phải là tất cả các phương án thực hiện của sáng chế. Các phương án thực hiện khác thu được bởi người có hiểu biết trung bình về lĩnh vực dựa vào các phương án thực hiện của sáng chế mà không cần nỗ lực sáng tạo sẽ nằm trong phạm vi bảo hộ của sáng chế.

Hiện nay, các hệ thống chuỗi khối chủ yếu rơi vào ba loại: chuỗi khối công khai, chuỗi khối bí mật và chuỗi khối tập đoàn. Ba loại chuỗi khối này chủ yếu khác biệt về các đối tượng công khai. Chuỗi khối công khai được mở cho mọi người. Bất kỳ ai cũng có thể đọc và gửi giao dịch và giao dịch có thể được xác nhận một cách hiệu quả. Bất kỳ ai đều có thể tham gia vào quá trình đồng thuận. Các ứng dụng điển hình bao gồm bitcoin, Ethereum, siêu sổ cái, v.v.. Chuỗi khối bí mật được mở cho một cá thể, thực thể hoặc tổ chức. Sự cho phép bằng văn bản chỉ được kiểm soát bởi một tổ chức. Sự cho phép đọc có thể được mở cho bên ngoài hoặc có thể bị hạn chế một cách ngẫu nhiên. Các ứng dụng điển hình bao gồm các dự án siêu sổ cái, v.v., của Linux Foundation, nền tảng R3CEVCorda và mạng Gem Health. Chuỗi khối tập đoàn nằm giữa chuỗi khối công khai và chuỗi khối bí mật, được mở cho cá thể cụ thể, thực thể hoặc tổ chức và các cá nhân, các thực thể hoặc các tổ chức khác bị hạn chế.

Trong chuỗi khối, đặc biệt trong chuỗi khối tập đoàn dùng cho các tổ chức cụ thể, để nâng cao tính bảo mật truyền thông, trung tâm cấp phép chứng chỉ (trung tâm CA) thường được thiết kế. Trung tâm CA, cũng được gọi là tổ chức CA, đóng vai trò làm bên thứ ba tin cậy trong giao dịch thương mại điện tử và có trách nhiệm xác minh tính hợp lệ của khóa công khai trong hệ thống khóa công khai. Trung tâm CA cấp chứng chỉ số hóa tới mỗi người dùng nút sử dụng khóa công khai. Chức năng của chứng chỉ số hóa

là để chứng minh rằng, người dùng được liệt kê trong chứng chỉ sở hữu hợp lệ của khóa công khai được liệt kê trong chứng chỉ. Để ngăn không cho kẻ tấn công làm giả hoặc thay đổi chứng chỉ, trung tâm CA ký số mỗi chứng chỉ số hóa.

Trong ứng dụng chuỗi khối, trung tâm CA của chuỗi khối có thể thực thi việc liên xác thực trong số các nút trong chuỗi khối và nâng cao tính bảo mật truyền thông giữa các nút chuỗi khối. Chuỗi khối duy trì một trung tâm CA và cấp chứng chỉ số hóa (cũng được gọi là chứng chỉ nút) của nút tới mỗi nút mà tham gia vào quá trình truyền thông chuỗi khối, sao cho chỉ các nút giữ các chứng chỉ hợp lệ mới có thể truyền thông với nhau.

Theo một số phương án thực hiện, cả chứng chỉ nút cấp và thông tin liên quan đến tính hợp lệ của chứng chỉ (phản ánh xem liệu nút có tương ứng với chứng chỉ được phép tham gia vào chuỗi khối hay không) đều được lưu trữ trong máy chủ của trung tâm CA và có thể được gọi và truy vấn bởi các nút trong chuỗi khối trong suốt quá trình truyền thông để hoàn tất việc xác minh quy trình truyền thông. Có rủi ro an toàn tương đối lớn trong phương pháp do việc truyền thông an toàn giữa các nút chuỗi khối phụ thuộc vào việc xác minh tính hợp lệ của nút của chứng chỉ khi thiết lập kết nối truyền thông. Theo phương án thực hiện giải pháp trên, chứng chỉ nút được cấp bởi trung tâm CA và thông tin liên quan đến tính hợp lệ của chứng chỉ cả hai được lưu trữ trong máy chủ của trung tâm CA. Khi trung tâm CA bị tấn công, tin tặc có thể thay đổi tùy ý thông tin liên quan đến tính hợp lệ của chứng chỉ. Ví dụ, tin tặc có thể thay đổi danh sách thu hồi chứng chỉ và khôi phục cứng thư đã hủy thành bình thường. Tin tặc có thể sử dụng các chứng chỉ bị hủy trước đó để tham gia vào chuỗi khối mà không cần cho phép, do đó gây đe dọa tính bảo mật của chuỗi khối.

Ngoài ra, trong giải pháp theo phương án thực hiện ở trên, để xác minh tính hợp lệ nút của chứng chỉ, chuỗi khối cần gọi từ xa thông tin được lưu trữ ở trung tâm CA và liên quan đến tính hợp lệ của chứng chỉ. Cuối cùng, tốc độ phản hồi có thể là thấp, thông tin bị chặn trong quá trình truyền, rủi ro liên quan đến tốc độ gọi thông tin và sự an toàn có thể xuất hiện và do đó, việc xác minh tính hợp lệ của nút của chứng chỉ sẽ bị ảnh hưởng.

Do đó, các phương án thực hiện của sáng chế đề xuất phương pháp, thiết bị và

thiết bị điện tử để truyền thông giữa các nút chuỗi khối và phương pháp, thiết bị và thiết bị điện tử để quản lý chứng chỉ số hóa trên cơ sở chuỗi khối, để nâng cao tính bảo mật truyền thông giữa các nút chuỗi khối và còn nâng cao độ an toàn của mạng chuỗi khối.

Các giải pháp kỹ thuật được đề xuất theo các phương án thực hiện của sáng chế được mô tả chi tiết dưới đây dựa vào các hình vẽ kèm theo.

Như được thể hiện trên Fig.1, theo phương án thực hiện, sáng chế đề xuất phương pháp truyền thông giữa các nút chuỗi khối. Phương pháp này cụ thể là có thể bao gồm các bước sau:

Bước S101. Nút thứ hai nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, ở đó yêu cầu truyền thông thứ nhất gồm chứng chỉ số hóa của nút thứ nhất và chứng chỉ số hóa của nút thứ nhất được lưu trữ trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai.

Bước S103. Nút thứ hai xác minh, dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không, ở đó thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa của nút.

Bước S105. Khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, xác định xem liệu nút thứ hai có thiết lập kết nối truyền thông với nút thứ nhất hay không.

Có thể hiểu rằng, nút thứ nhất và nút thứ hai theo phương án thực hiện ở trên có thể là hai nút khác nhau bất kỳ trong chuỗi khối. Khi nút thứ nhất (nút này có thể là nút bất kỳ trong chuỗi khối) trong chuỗi khối mong muốn truyền thông với nút thứ hai (nút này có thể là nút bất kỳ khác với nút thứ nhất trong chuỗi khối), nút thứ nhất có thể thêm chứng chỉ số hóa của nút thứ nhất tới yêu cầu truyền thông và gửi yêu cầu truyền thông tới nút thứ hai, để chứng minh, tới nút thứ hai, nhận dạng hợp lệ của nút thứ nhất được xác thực bởi trung tâm CA. Kịch bản có thể áp dụng của quy trình tương tác có thể là: nút thứ nhất mong muốn truyền thông với nút thứ hai và trước khi thiết lập kết nối truyền thông, nút thứ hai trước tiên xác minh xem liệu nút thứ nhất có yêu cầu truyền thông là nút xác thực hay không, để xác định xem liệu có đồng ý với yêu cầu truyền thông của nút thứ nhất hay không. Trong kịch bản này, nút thứ nhất tương ứng với nút thứ hai gửi yêu cầu truyền thông thứ nhất trước đó tới nút thứ hai và gửi chứng chỉ số hóa của nút

thứ nhất tới nút thứ hai để xác minh; và nút thứ nhất sau đó chờ để nhận phản hồi hoặc hồi tiếp từ nút thứ hai. Ví dụ, sự phản hồi hoặc hồi tiếp có thể là kết quả xác minh chứng chỉ số hóa: tính hợp lệ hoặc không hợp lệ hoặc có thể là thông tin chỉ báo việc xác định để thiết lập kết nối truyền thông sau khi nút thứ hai xác minh rằng chứng chỉ số hóa của nút thứ nhất là hợp lệ hoặc có thể là chứng chỉ số hóa của nút thứ hai được gửi bởi nút thứ hai tới nút thứ nhất để xác minh bởi nút thứ nhất.

Có thể hiểu thêm rằng, khi nút thứ hai (nút này có thể là nút bất kỳ trong chuỗi khối) trong chuỗi khối mong muốn truyền thông với nút thứ nhất (nút này có thể là nút bất kỳ khác với nút thứ hai trong chuỗi khối), trước khi bước S101, các bước trước có thể được bao gồm: nút thứ hai gửi yêu cầu bắt tay (handshake request) với nút thứ nhất, để yêu cầu thiết lập với nút thứ nhất và yêu cầu nút thứ nhất để gửi chứng chỉ số hóa của nút thứ nhất để xác minh; phản hồi, nút thứ nhất sau đó có thể gửi yêu cầu truyền thông thứ nhất trước đó tới nút thứ hai và gửi chứng chỉ số hóa của nút thứ nhất tới nút thứ hai để xác minh. Kịch bản có thể áp dụng của quy trình tương tác có thể là: nút thứ hai mong muốn truyền thông với nút thứ nhất và khi thiết lập kết nối truyền thông, nút thứ hai mong muốn trước tiên xác minh xem liệu nút thứ nhất trong chuỗi khối có phải là nút xác thực hay không, để xác định xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không. Tương tự với kịch bản trước đó, nút thứ hai có thể hồi tiếp thông tin bao gồm các loại nội dung khác nhau và ở các dạng khác nhau tới nút thứ nhất và các chi tiết không được mô tả ở đây.

Có thể hiểu rằng, để đảm bảo tính bảo mật truyền thông, nút thứ hai nhận yêu cầu truyền thông cần để xác minh xem liệu nút thứ nhất thiết lập kết nối truyền thông với nút thứ hai có mã nhận dạng hợp lệ hay không và cụ thể, nút thứ hai có thể xác minh xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông được gửi bởi nút thứ nhất là chứng chỉ số hóa hợp lệ hay không. Theo các phương án cụ thể, sáng chế sử dụng thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối để xác minh chứng chỉ số hóa của nút thứ nhất.

Theo các phương án thực hiện của sáng chế, chứng chỉ số hóa của mỗi nút trong chuỗi khối và thông tin hợp lệ từ trước của chứng chỉ được lưu trữ trong chuỗi khối chứa nút và chứng chỉ số hóa có thể được lưu trữ trong chuỗi khối bằng cách viết chứng chỉ số hóa vào chuỗi khối. Do đó, theo các phương án thực hiện của sáng chế, các tính chất

của chuỗi khối, như sự phi tập trung và chống làm giả, có thể được sử dụng để ngăn không cho tin tặc làm giả chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá, để đảm bảo rằng kết quả xác minh tính hợp lệ của chứng chỉ là đúng và chính xác và đảm bảo tính bảo mật và tính ổn định của mạng chuỗi khối. Ngoài ra, theo phương án thực hiện này của sáng chế, khi xác minh tính hợp lệ của chứng chỉ số hoá, nút thứ hai có thể đọc trực tiếp thông tin hợp lệ của chứng chỉ được lưu trữ cục bộ trong nút, không cần đọc từ xa thông tin hợp lệ của chứng chỉ được lưu trữ ở trung tâm CA và cuối cùng, tốc độ và tính bảo mật của việc xác minh hợp lệ được nâng cao. Ngoài ra, nhờ việc gọi cục bộ thông tin như thông tin hợp lệ của chứng chỉ, sự phụ thuộc vào một điểm của chuỗi khối ở trung tâm CA có thể được loại trừ và độ tin cậy của mạng chuỗi khối còn gia tăng tiếp.

Theo phương án thực hiện này của sáng chế, thông tin tình trạng hợp lệ của chứng chỉ số hóa có thể rơi vào hai loại: một loại là thông tin tình trạng hợp lệ chỉ ra rằng chứng chỉ là hợp lệ và loại kia của thông tin tình trạng hợp lệ chỉ ra rằng chứng chỉ là không hợp lệ. Chứng chỉ số hóa không hợp lệ thường được hủy bỏ bởi trung tâm CA.

Trước khi bước S103 được thực hiện, để xác minh tính hợp lệ của chứng chỉ số hóa bằng cách đọc thông tin hợp lệ của chứng chỉ từ chuỗi khối bao gồm nút thứ nhất và nút thứ hai, bản ghi của chứng chỉ số hóa và thông tin tình trạng hợp lệ của chứng chỉ số hóa mà nhận được bởi chuỗi khối có thể được cấp phát từ trước để tạo thành thông tin hợp lệ của chứng chỉ để truy hồi bởi nút thứ hai. Cụ thể hơn, thông tin hợp lệ của chứng chỉ có thể được tạo thành là cơ sở để nhận chứng chỉ số hóa hợp lệ được tập hợp từ danh sách chứng chỉ hợp lệ và cũng phản ánh cơ sở nhận các chứng chỉ số hóa không hợp lệ được tập hợp từ danh sách chứng chỉ bị hủy.

Hơn nữa, nếu chứng chỉ số hóa không hợp lệ đã hủy được ghi lại trong thông tin hợp lệ từ trước của chứng chỉ, ví dụ, thông tin hợp lệ từ trước của chứng chỉ được tạo thành dưới dạng danh sách chứng chỉ bị hủy được tạo ra dựa vào bản ghi của chứng chỉ số hóa không hợp lệ thu được, thì nút thứ hai này xác minh, dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không trong bước trước S103 cụ thể là có thể bao gồm các việc: xác định, bởi nút thứ hai, chứng chỉ số hóa của nút thứ nhất dựa vào yêu cầu truyền thông thứ nhất; xác minh, bởi nút thứ hai dựa vào thông tin hợp lệ của chứng chỉ được lưu trữ

trong chuỗi khối, xem liệu chứng chỉ số hóa của nút thứ nhất có được ghi lại trong thông tin hợp lệ từ trước của chứng chỉ hay không; và chỉ báo rằng chứng chỉ số hóa của nút thứ nhất được hủy, thì xác định rằng chứng chỉ số hóa của nút thứ nhất là không hợp lệ, nếu chứng chỉ số hóa của nút thứ nhất được ghi lại trong thông tin hợp lệ của chứng chỉ.

Tương tự, nếu thông tin hợp lệ từ trước của chứng chỉ ghi lại chứng chỉ số hóa hợp lệ, ví dụ, thông tin hợp lệ từ trước của chứng chỉ được tạo thành dưới dạng danh sách chứng chỉ hợp lệ được tạo ra dựa vào bản ghi của chứng chỉ số hóa hợp lệ thu được, thì nút thứ hai này được xác minh, dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không trong bước trước S103 cụ thể là có thể bao gồm: xác định, bởi nút thứ hai, chứng chỉ số hóa của nút thứ nhất dựa vào yêu cầu truyền thông thứ nhất; xác minh, bởi nút thứ hai dựa vào thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối, xem liệu chứng chỉ số hóa của nút thứ nhất có được ghi lại trong thông tin hợp lệ của chứng chỉ hay không; và xác minh rằng chứng chỉ số hóa của nút thứ nhất là hợp lệ, nếu chứng chỉ số hóa của nút thứ nhất được ghi lại trong thông tin hợp lệ của chứng chỉ, chỉ báo rằng chứng chỉ số hóa của nút thứ nhất được xác minh.

Theo các phương án cụ thể, nút thứ hai có thể phân tích cú pháp yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất tới xác định chứng chỉ số hóa của nút thứ nhất.

Chứng chỉ số hóa của nút được cấp bởi trung tâm CA (có thể là trung tâm CA từ trước) và được sử dụng để xác minh nhận dạng thực thể của mỗi nút tham gia vào truyền thông chuỗi khối. Trong truyền thông internet, chứng chỉ số hóa có thể được tạo thành dưới dạng chuỗi các số chỉ báo thông tin nhận dạng của các bên đang truyền thông với nhau và có thể bao gồm nội dung như số phiên bản chứng chỉ, thông tin về người giữ chứng chỉ (ví dụ, thông tin về người giữ chứng chỉ có thể được tạo thành dưới dạng thông tin nhận dạng của nút tương ứng với chứng chỉ), thông tin từ trung tâm CA, khoảng hợp lệ của chứng chỉ, số thứ tự chứng chỉ và chữ ký của trung tâm CA.

Theo phương án thực hiện ở trên, quy trình, trong đó nút thứ hai xác minh chứng chỉ số hóa của nút thứ nhất được mô tả. Khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, nút thứ hai có thể còn xác định xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không. Cụ thể hơn, có thể xác định dựa vào giao thức truyền thông giữa nút

thứ nhất và nút thứ hai ở đó chuỗi khối được bố trí. Sau đây là phần mô tả chi tiết bằng cách sử dụng ví dụ.

Ví dụ, nút thứ hai có thể thiết lập trực tiếp kết nối truyền thông với nút thứ nhất, nếu giao thức truyền thông quy định rằng chỉ xác minh đơn hướng cần được thực hiện để truyền thông liên nút, khi nút thứ hai xác minh rằng chứng chỉ số hóa của nút thứ nhất là hợp lệ.

Ví dụ, nút thứ hai cũng cần để gửi chứng chỉ số hóa của nút thứ hai tới nút thứ nhất, để nút thứ nhất xác minh tính hợp lệ của chứng chỉ số hóa của nút thứ hai, nếu giao thức truyền thông quy định xác minh hai hướng cần được thực hiện để truyền thông liên nút, theo phương án thực hiện này của sáng chế, ngoài việc xác minh tính hợp lệ của chứng chỉ của nút thứ nhất. Cụ thể, phương pháp trên phương án thực hiện này của sáng chế có thể còn bao gồm: gửi, bởi nút thứ hai, yêu cầu truyền thông thứ hai tới nút thứ nhất, ở đó yêu cầu truyền thông thứ hai bao gồm chứng chỉ số hóa của nút thứ hai. Nút thứ hai gửi chứng chỉ số hóa của nút thứ hai tới nút thứ nhất, để nút thứ nhất xác minh xem liệu chứng chỉ số hóa của nút thứ hai là hợp lệ hay không dựa vào chứng chỉ số hóa trong yêu cầu truyền thông thứ hai và thông tin hợp lệ của chứng chỉ được lưu trữ cục bộ trong nút thứ nhất. Hơn nữa, sau khi nút thứ nhất xác minh rằng chứng chỉ số hóa của nút thứ hai là hợp lệ và nút thứ hai xác minh rằng chứng chỉ số hóa của nút thứ nhất là hợp lệ, thiết lập kết nối truyền thông giữa nút thứ hai và nút thứ nhất. Đối với kịch bản có thể áp dụng truyền thông điểm tới điểm này giữa các nút chuỗi khối, phương pháp xác minh hai hướng được ưu tiên.

Theo các phương án cụ thể, nút cụ thể đóng vai trò làm bộ khởi tạo yêu cầu truyền thông và nút kia đóng vai trò làm người nhận yêu cầu truyền thông. Trình tự tương tác của cả hai nút có thể được xác định bởi giao thức truyền thông của cả hai nút, với điều kiện là chứng chỉ số hóa của nút ngang hàng có thể cuối cùng được xác minh. Giải pháp được đề xuất theo phương án thực hiện này của sáng chế không nhằm giới hạn ở các bước cụ thể và thứ tự thực hiện các bước.

Theo các phương án cụ thể, tốt hơn nếu thiết lập kết nối truyền thông giữa các nút trong chuỗi khối nhờ việc sử dụng giao thức SSL hoặc giao thức TLS. Do đó, yêu cầu truyền thông thứ nhất thu được bởi nút thứ hai được gửi bởi nút thứ nhất dựa vào

giao thức SSL hoặc giao thức TLS và cuối cùng, kênh truyền thông đã mã hóa được thiết lập giữa các nút. Kết nối mạng có thể được mã hóa ở lớp truyền nhờ việc sử dụng giao thức SSL hoặc giao thức TLS, để đảm bảo tính bảo mật truyền dữ liệu. Nhờ việc sử dụng công nghệ mã hóa dữ liệu, có thể còn đảm bảo rằng, dữ liệu không bị chặn hoặc nghe lén trong quá trình truyền qua internet.

Phương án thực hiện ở trên mô tả chi tiết các khía cạnh của phương pháp truyền thông giữa các nút chuỗi khối trong sáng chế. Fig.2 minh họa vắn tắt quá trình trao đổi thông tin của phương pháp. Ở đây, chỉ xác thực đơn hướng được sử dụng làm ví dụ.

Bước S01. Nút thứ nhất gửi yêu cầu truyền thông tới nút thứ hai.

Bước S02. Nút thứ hai đọc cục bộ thông tin hợp lệ của chứng chỉ và xác minh xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không.

Bước S03. Nút thứ hai thiết lập kết nối truyền thông với nút thứ nhất, nếu chứng chỉ số hóa của nút thứ nhất là hợp lệ.

Ý tưởng cốt lõi của phương án thực hiện này của sáng chế là như sau: chứng chỉ số hóa của chuỗi khối được lưu trữ trong chuỗi khối và thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa của nút cũng được lưu trữ trong chuỗi khối, để chứng chỉ số hóa được xác minh nhờ việc sử dụng thông tin chống giả mạo này, để đảm bảo sự đúng đắn và độ chính xác của kết quả xác minh và đảm bảo tính bảo mật truyền thông của các nút trong chuỗi khối.

Sau đây mô tả chi tiết phương án thực hiện cụ thể của việc quản lý chứng chỉ số hóa trên cơ sở chuỗi khối bởi hệ thống chuỗi khối và trung tâm CA.

Như được thể hiện trên Fig.3, theo phương án thực hiện, sáng chế đề xuất phương pháp quản lý chứng chỉ số hóa trên cơ sở chuỗi khối. Phương pháp được áp dụng cho hệ thống chuỗi khối và cụ thể là có thể bao gồm các bước sau đây:

Bước S201. Nhận chứng chỉ số hóa của nút và thông tin tình trạng hợp lệ của chứng chỉ số hóa được gửi bởi trung tâm CA.

Bước S203. Xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá.

Bước S205. Lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ trong chuỗi khối, ở đó chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ được sử dụng để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Cụ thể, khi bước S203 của xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa được thực hiện, như được mô tả theo phương án thực hiện ở trên, bản ghi của chứng chỉ số hóa và thông tin tình trạng hợp lệ của chứng chỉ số hóa mà nhận được bởi chuỗi khối có thể được cấp phát, để xác định thông tin hợp lệ của chứng chỉ cần được truy vấn bởi nút thứ hai. Cụ thể hơn, thông tin hợp lệ của chứng chỉ không chỉ có thể được tạo thành dưới dạng danh sách chứng chỉ hợp lệ được tạo ra dựa vào việc ghi lại chứng chỉ số hóa hợp lệ thu được, mà cũng có thể được tạo thành dưới dạng danh sách chứng chỉ bị hủy được tạo ra dựa vào bản ghi của chứng chỉ số hóa không hợp lệ thu được.

Theo các phương án cụ thể, chuỗi khối có thể lưu trữ chứng chỉ số hóa mới hoặc thông tin tình trạng hợp lệ mới của chứng chỉ số hóa dựa vào chứng chỉ số hóa của nút và thông tin tình trạng hợp lệ của chứng chỉ số hóa thu được trong bước S201, để thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối do đó có thể cũng được cập nhật, để đảm bảo độ chính xác của kết quả xác minh.

Trong phương pháp tương ứng với phương pháp quản lý chứng chỉ số hóa trên cơ sở chuỗi khối trước đó, trung tâm CA cũng gửi chứng chỉ số hóa của nút trong chuỗi khối và thông tin tình trạng hợp lệ của chứng chỉ số hóa tới chuỗi khối, để chuỗi khối xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ, để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Đối với chuỗi khối, ngoài việc nhận chứng chỉ số hóa và thông tin tình trạng hợp

lệ của chứng chỉ số hóa được gửi bởi trung tâm CA, nút yêu cầu tham gia vào chuỗi khối có thể còn gửi yêu cầu áp dụng chứng chỉ cho trung tâm CA. Yêu cầu áp dụng chứng chỉ bao gồm thông tin áp dụng của nút thứ nhất và được sử dụng để áp dụng cho trung tâm CA đối với chứng chỉ số hóa của nút thứ nhất.

Do đó, trung tâm CA có thể nhận yêu cầu áp dụng chứng chỉ được gửi bởi nút trong chuỗi khối. Yêu cầu áp dụng chứng chỉ bao gồm thông tin áp dụng của nút thứ nhất và được sử dụng để áp dụng cho trung tâm CA đối với chứng chỉ số hóa của nút thứ nhất. Trung tâm CA còn nhận và xem lại thông tin áp dụng của nút thứ nhất. Khi thông tin áp dụng của nút thứ nhất đã được xem lại, trung tâm CA cấp chứng chỉ số hóa tới nút thứ nhất và thông tin tình trạng hợp lệ của chứng chỉ số hóa là “hợp lệ”.

Fig.4 minh họa vắn tắt quy trình tương tác ví dụ giữa hệ thống chuỗi khối và trung tâm CA. Công đoạn, trong đó nút trong chuỗi khối áp dụng lên trung tâm CA đối với chứng chỉ số hóa cụ thể là có thể bao gồm các bước sau đây:

Bước S10. Hệ thống chuỗi khối (ví dụ, nút thứ nhất) gửi đơn yêu cầu áp dụng chứng chỉ số hoá tới trung tâm CA (bao gồm tổ chức RA chấp nhận các ứng dụng chứng chỉ và tổ chức CA cấp các chứng chỉ).

Bước S12. RA (tổ chức chấp nhận) nhận và xem lại đơn yêu cầu và sau khi đơn yêu cầu đã được xem lại, RA về phía đơn yêu cầu tới cơ quan CA (cơ quan xác minh) để xử lý.

Bước S14. Tổ chức CA cấp chứng chỉ số hoá và tổ chức CA gửi chứng chỉ số hóa đã cấp tới hệ thống chuỗi khối.

Bước S16. Sau khi nhận chứng chỉ số hóa đã cấp, hệ thống chuỗi khối viết chứng chỉ vào chuỗi khối để lưu trữ chứng chỉ vào tất cả các nút (như nút thứ nhất, nút thứ hai, nút thứ ba và nút thứ tư được thể hiện trên Fig.4) trong hệ thống chuỗi khối.

Hơn nữa, khi chứng chỉ số hóa được cấp bởi trung tâm CA được hủy, thông tin tình trạng hợp lệ của chứng chỉ số hóa được thay đổi từ “hợp lệ” tới “không hợp lệ” (hoặc “bị hủy”) và trung tâm CA thực hiện bước S20 để gửi lệnh cập nhật thông tin tình trạng hợp lệ của chứng chỉ tới hệ thống chuỗi khối. Theo các phương án cụ thể, trung tâm CA có thể gửi cả hai chứng chỉ số hóa và thông tin tình trạng hợp lệ của chứng chỉ số hóa tới chuỗi khối nhờ việc sử dụng phương pháp cấp chứng chỉ số hóa mới tương

tự. Khác nhau chỉ là thông tin tình trạng hợp lệ của chứng chỉ số hóa là “không hợp lệ” hoặc “hủy bỏ” trong trường hợp này. Sau khi nhận thông tin trước đó, chuỗi khối thực hiện bước S22, cập nhật thông tin hợp lệ của chứng chỉ dựa vào thông tin tình trạng hợp lệ mới của chứng chỉ và viết thông tin hợp lệ của chứng chỉ vào chuỗi khối, để tạo ra thông tin hợp lệ chính xác của chứng chỉ khi chứng chỉ số hóa của nút được xác minh.

Theo phương án thực hiện, sáng chế còn đề xuất thiết bị truyền thông giữa các nút chuỗi khối. Như được thể hiện trên Fig.5, thiết bị được áp dụng cho nút thứ hai trong chuỗi khối và bao gồm: môđun thu yêu cầu truyền thông 101, được tạo cấu hình để thu yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, ở đó yêu cầu truyền thông thứ nhất gồm chứng chỉ số hóa của nút thứ nhất và chứng chỉ số hóa của nút thứ nhất được lưu trữ trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai; môđun xác minh hợp lệ 103, được tạo cấu hình để xác minh, dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không, ở đó thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa của nút; và môđun thiết lập kết nối truyền thông 105, được tạo cấu hình để: khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, xác định xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không.

Như được thể hiện trên Fig.6, thiết bị trước có thể còn bao gồm: môđun gửi yêu cầu truyền thông 107, được tạo cấu hình để gửi yêu cầu truyền thông thứ hai tới nút thứ nhất, ở đó yêu cầu truyền thông thứ hai bao gồm chứng chỉ số hóa của nút thứ hai, để nút thứ nhất xác minh, dựa vào yêu cầu truyền thông thứ hai và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ hai là hợp lệ hay không; và môđun thiết lập kết nối truyền thông 105 cụ thể là có thể được tạo cấu hình để: khi chứng chỉ số hóa của nút thứ nhất là hợp lệ và nút thứ nhất xác minh rằng chứng chỉ số hóa của nút thứ hai là hợp lệ, thiết lập kết nối truyền thông với nút thứ nhất.

Fig.7 là sơ đồ kết cấu giản lược của thiết bị điện tử theo phương án thực hiện của sáng chế. Tham chiếu đến Fig.7, thiết bị điện tử bao gồm bộ xử lý và tùy ý còn bao gồm buýt nội bộ, giao diện mạng và bộ phận lưu trữ theo thuật ngữ phần cứng. Bộ phận lưu trữ có thể bao gồm bộ nhớ, ví dụ, bộ nhớ truy cập ngẫu nhiên (RAM) tốc độ cao hoặc có thể còn bao gồm bộ nhớ không khả biến, ví dụ, ít nhất một bộ nhớ dạng đĩa từ. Nhất định là thiết bị điện tử có thể còn bao gồm phần cứng được yêu cầu bởi dịch vụ khác.

Bộ xử lý, giao diện mạng và bộ phận lưu trữ có thể được liên kết nhờ việc sử dụng buýt nội bộ. Buýt nội bộ có thể là buýt kiến trúc tiêu chuẩn công nghiệp (industry standard architecture - ISA), buýt kết nối thành phần ngoại vi (peripheral component interconnect - PCI), buýt kiến trúc tiêu chuẩn công nghiệp kéo dài (EISA), v.v.. Buýt có thể được phân loại thành buýt địa chỉ, buýt dữ liệu, buýt điều khiển, v.v.. Để dễ dàng minh họa, chỉ mũi tên hai đầu được sử dụng trên Fig.7, nhưng không chỉ ra chỉ có một buýt hoặc chỉ một loại là buýt.

Bộ phận lưu trữ được tạo cấu hình để lưu trữ chương trình. Cụ thể, chương trình có thể bao gồm mã chương trình và mã chương trình bao gồm lệnh vận hành được bằng máy tính. Bộ phận lưu trữ có thể bao gồm bộ nhớ và bộ nhớ không khả biến và tạo ra lệnh và dữ liệu cho bộ xử lý.

Bộ xử lý đọc chương trình máy tính tương ứng từ bộ nhớ không khả biến vào bộ nhớ và sau đó chạy chương trình máy tính tương ứng, để tạo ra thiết bị truyền thông giữa các nút chuỗi khối theo thuật ngữ logic. Bộ xử lý thực thi chương trình được lưu trữ trong bộ nhớ để thực hiện các thao tác sau đây: nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, ở đó yêu cầu truyền thông thứ nhất gồm chứng chỉ số hóa của nút thứ nhất và chứng chỉ số hóa của nút thứ nhất được lưu trữ trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai; xác minh, dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không, ở đó thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa của nút; và khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, thì xác định xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không.

Phương pháp trên được thực hiện bởi thiết bị truyền thông giữa các nút chuỗi khối và được bộc lộ theo phương án thực hiện được thể hiện trên Fig.1 của sáng chế có thể được áp dụng cho bộ xử lý hoặc có thể được thực thi bởi bộ xử lý. Bộ xử lý có thể là chip mạch tích hợp và có khả năng xử lý tín hiệu. Trong quá trình thực thi, các bước của phương pháp trên có thể được hoàn tất nhờ việc sử dụng mạch logic tích hợp của phần cứng trong bộ xử lý hoặc lệnh ở dạng phần mềm. Bộ xử lý trước đó có thể là bộ xử lý mục đích chung và bao gồm bộ xử lý trung tâm (CPU), bộ xử lý mạng (NP), v.v. hoặc có thể là bộ xử lý tín hiệu số (DSP), mạch tích hợp chuyên dụng (ASIC), mảng

cổng lập trình được dạng trường (FPGA) hoặc thiết bị logic lập trình được (PLD) khác, cổng riêng biệt hoặc thiết bị logic tranzito hoặc thành phần phần cứng riêng biệt. Bộ xử lý trước đó có thể thực thi hoặc thực hiện các phương pháp, các bước và các sơ đồ khối logic được bộc lộ theo các phương án thực hiện của sáng chế. Bộ xử lý mục đích chung có thể là bộ vi xử lý hoặc bộ xử lý có thể là bộ xử lý đã biết, v.v.. Các bước của phương pháp được bộc lộ dựa vào các phương án thực hiện của sáng chế có thể được thực hiện trực tiếp và hoàn thành bởi bộ xử lý mã hóa phần cứng hoặc có thể được thực hiện và hoàn thành nhờ việc sử dụng tổ hợp của môđun phần cứng và môđun phần mềm trong bộ xử lý giải mã. Môđun phần mềm có thể được đặt trong vật ghi trường thành trong lĩnh vực, như RAM, bộ nhớ flash, bộ nhớ chỉ đọc (ROM), bộ nhớ chỉ đọc lập trình được (PROM), bộ nhớ chỉ đọc lập trình được xóa được bằng điện (EEPROM) hoặc thanh ghi. Vật ghi được bố trí trong bộ phận lưu trữ và bộ xử lý đọc thông tin từ bộ nhớ và hoàn thành các bước của phương pháp trên nhờ việc sử dụng phần cứng của bộ xử lý.

Thiết bị điện tử có thể còn thực hiện phương pháp trên Fig.1 mà được thực hiện bởi thiết bị truyền thông giữa các nút chuỗi khối và thực thi các chức năng của thiết bị truyền thông giữa các nút chuỗi khối theo phương án thực hiện được thể hiện trên Fig.1. Các chi tiết không được một cách theo phương án thực hiện này của sáng chế.

Theo phương án thực hiện, sáng chế còn đề xuất vật ghi đọc được bằng máy tính. Vật ghi đọc được bằng máy tính lưu trữ một hoặc nhiều chương trình, một hoặc nhiều chương trình chứa các lệnh. Các lệnh được thực thi bởi thiết bị điện tử bao gồm các chương trình ứng dụng để thực hiện phương pháp được thực hiện bởi thiết bị truyền thông giữa các nút chuỗi khối theo phương án thực hiện được thể hiện trên Fig.1, bao gồm các bước: nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, ở đó yêu cầu truyền thông thứ nhất gồm chứng chỉ số hóa của nút thứ nhất và chứng chỉ số hóa của nút thứ nhất được lưu trữ trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai; xác minh, dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không, ở đó thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa của nút; và khi chứng chỉ số hóa của nút thứ nhất là hợp lệ, xác định xem liệu có thiết lập kết nối truyền thông với nút thứ nhất hay không.

Hơn thế nữa, trong thiết bị điện tử được thể hiện trên Fig.7, lệnh thực thi được

thực thi bởi bộ xử lý để còn thực hiện các thao tác sau đây: gửi yêu cầu truyền thông thứ hai tới nút thứ nhất, ở đó yêu cầu truyền thông thứ hai bao gồm chứng chỉ số hóa của nút thứ hai, để nút thứ nhất xác minh, dựa vào yêu cầu truyền thông thứ hai và thông tin hợp lệ của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ hai có hợp lệ hay không; và khi chứng chỉ số hóa của nút thứ nhất là hợp lệ và nút thứ nhất xác minh rằng chứng chỉ số hóa của nút thứ hai là hợp lệ, thiết lập, bởi nút thứ hai, kết nối truyền thông với nút thứ nhất.

Theo phương án thực hiện, sáng chế còn đề xuất thiết bị quản lý chứng chỉ số hóa trên cơ sở chuỗi khối. Như được thể hiện trên Fig.8, thiết bị được áp dụng cho chuỗi khối và bao gồm: môđun nhận thông tin chứng chỉ 201, được tạo cấu hình để thu chứng chỉ số hóa của nút và thông tin tình trạng hợp lệ của chứng chỉ số hóa được gửi bởi trung tâm CA; thông tin hợp lệ của môđun xác định chứng chỉ 203, được tạo cấu hình tới xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá; và môđun lưu trữ 205, được tạo cấu hình để lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ trong chuỗi khối, ở đó chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ được sử dụng để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Fig.9 là sơ đồ kết cấu giản lược của thiết bị điện tử theo phương án thực hiện của sáng chế. Tham chiếu đến Fig.9, thiết bị điện tử bao gồm bộ xử lý và tùy ý còn bao gồm buýt nội bộ, giao diện mạng và bộ phận lưu trữ về mặt phần cứng. Bộ phận lưu trữ có thể bao gồm bộ nhớ, ví dụ, RAM tốc độ cao hoặc có thể còn bao gồm bộ nhớ không khả biến, ví dụ, ít nhất một bộ nhớ dạng đĩa từ. Nhất định là thiết bị điện tử có thể còn bao gồm phần cứng được yêu cầu bởi dịch vụ khác.

Bộ xử lý, giao diện mạng và bộ phận lưu trữ có thể được liên kết nhờ việc sử dụng buýt nội bộ. Buýt nội bộ có thể là buýt ISA, buýt PCI, buýt EISA, v.v.. Buýt có thể được phân loại thành buýt địa chỉ, buýt dữ liệu, buýt điều khiển, v.v.. Để dễ dàng minh họa, chỉ mũi tên hai đầu được sử dụng trong Fig.9, nhưng không chỉ báo rằng, chỉ có một buýt hoặc chỉ một loại là buýt.

Bộ phận lưu trữ được tạo cấu hình để lưu trữ chương trình. Cụ thể, chương trình có thể bao gồm mã chương trình và mã chương trình bao gồm lệnh vận hành được bằng máy tính. Bộ phận lưu trữ có thể bao gồm bộ nhớ và bộ nhớ không khả biến và tạo ra lệnh và dữ liệu cho bộ xử lý.

Bộ xử lý đọc chương trình máy tính tương ứng từ bộ nhớ không khả biến vào bộ nhớ và sau đó chạy chương trình máy tính tương ứng, để tạo ra thiết bị quản lý chứng chỉ số hóa dựa vào chuỗi khối theo thuật ngữ logic. Bộ xử lý thực thi chương trình được lưu trữ trong bộ nhớ để thực hiện các thao tác sau đây: nhận chứng chỉ số hóa của nút và thông tin tình trạng hợp lệ của chứng chỉ số hóa được gửi bởi trung tâm CA; xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá; và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ trong chuỗi khối, ở đó chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ được sử dụng để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Phương pháp trên được thực hiện bởi thiết bị quản lý chứng chỉ số hóa dựa vào chuỗi khối và được bộc lộ theo phương án thực hiện ở trên của sáng chế có thể được áp dụng cho bộ xử lý hoặc có thể được thực thi bởi bộ xử lý. Bộ xử lý có thể là chip mạch tích hợp và có khả năng xử lý tín hiệu. Trong quá trình thực thi, các bước của phương pháp trên có thể được hoàn tất nhờ việc sử dụng mạch logic tích hợp của phần cứng trong bộ xử lý hoặc lệnh ở dạng phần mềm. Bộ xử lý trước đó có thể là bộ xử lý mục đích chung và bao gồm CPU, NP, v.v. hoặc có thể là DSP, ASIC, FPGA hoặc PLD khác, cổng riêng biệt hoặc thiết bị logic tranzito hoặc thành phần phần cứng riêng biệt. Bộ xử lý trước đó có thể thực thi hoặc thực hiện các phương pháp, các bước và các sơ đồ khối logic được bộc lộ theo các phương án thực hiện của sáng chế. Bộ xử lý mục đích chung có thể là bộ vi xử lý hoặc bộ xử lý có thể là bộ xử lý đã biết bất kỳ, v.v.. Các bước của phương pháp được bộc lộ dựa vào các phương án thực hiện của sáng chế có thể được thực hiện trực tiếp và hoàn thành bởi bộ xử lý mã hóa phần cứng hoặc có thể được thực hiện và hoàn thành nhờ việc sử dụng tổ hợp của môđun phần cứng và môđun phần mềm trong bộ xử lý giải mã. Môđun phần mềm có thể được đặt trong vật ghi trữ thành

trong lĩnh vực, như RAM, bộ nhớ flash, ROM, PROM, EEPROM hoặc thanh ghi. Vật ghi được bố trí trong bộ nhớ và bộ xử lý đọc thông tin từ bộ nhớ và hoàn thành các bước của phương pháp trên nhờ việc sử dụng phần cứng của bộ xử lý.

Thiết bị điện tử có thể còn thực hiện phương pháp mà được thực hiện nhờ thiết bị quản lý chứng chỉ số hóa trên cơ sở chuỗi khối và thực thi các chức năng của thiết bị quản lý chứng chỉ số hóa dựa vào chuỗi khối theo phương án thực hiện ở trên. Các chi tiết không được mô tả theo phương án thực hiện này của sáng chế.

Theo phương án thực hiện, sáng chế còn đề xuất vật ghi đọc được bằng máy tính. Vật ghi đọc được bằng máy tính lưu trữ một hoặc nhiều chương trình, một hoặc nhiều chương trình bao gồm lệnh. Lệnh được thực thi bởi thiết bị điện tử bao gồm các chương trình ứng dụng để thực hiện phương pháp mà được thực hiện bởi thiết bị quản lý chứng chỉ số hóa dựa vào chuỗi khối theo phương án thực hiện ở trên, bao gồm các bước: nhận chứng chỉ số hóa của nút và thông tin tình trạng hợp lệ của chứng chỉ số hóa được gửi bởi trung tâm CA; xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá; và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ trong chuỗi khối, ở đó chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ được sử dụng để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Theo phương án thực hiện, sáng chế còn đề xuất thiết bị quản lý chứng chỉ số hóa trên cơ sở chuỗi khối. Thiết bị được áp dụng cho trung tâm CA và bao gồm: môđun gửi, được tạo cấu hình để gửi chứng chỉ số hóa của nút trong chuỗi khối và thông tin tình trạng hợp lệ của chứng chỉ số hóa tới chuỗi khối, để chuỗi khối xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ, để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Hơn nữa, thiết bị trước còn bao gồm các bước: mô đun nhận yêu cầu áp dụng,

được tạo cấu hình để thu yêu cầu áp dụng chứng chỉ được gửi bởi nút trong chuỗi khối, ở đó yêu cầu áp dụng chứng chỉ bao gồm thông tin áp dụng của nút thứ nhất và được sử dụng để áp dụng cho trung tâm CA đối với chứng chỉ số hóa của nút thứ nhất; mô đun nhận và xem lại, được tạo cấu hình để thu và xem lại thông tin áp dụng của nút thứ nhất; và mô đun cấp và gửi, được tạo cấu hình để: khi thông tin áp dụng của nút thứ nhất đã được xem lại, cấp chứng chỉ số hóa tới nút thứ nhất, ở đó thông tin tình trạng hợp lệ của chứng chỉ số hóa là hợp lệ.

Fig.10 là sơ đồ kết cấu giản lược của thiết bị điện tử theo phương án thực hiện của sáng chế. Tham chiếu đến Fig.10, thiết bị điện tử bao gồm bộ xử lý và tùy ý còn bao gồm buýt nội bộ, giao diện mạng và bộ phận lưu trữ về mặt phần cứng. Bộ phận lưu trữ có thể bao gồm bộ nhớ, ví dụ, RAM tốc độ cao hoặc có thể còn bao gồm bộ nhớ không khả biến, ví dụ, ít nhất một bộ nhớ dạng đĩa từ. Nhất định là thiết bị điện tử có thể còn bao gồm phần cứng được yêu cầu bởi dịch vụ khác.

Bộ xử lý, giao diện mạng và bộ phận lưu trữ có thể được liên kết nhờ việc sử dụng buýt nội bộ. Buýt nội bộ có thể là buýt ISA, buýt PCI, buýt EISA, v.v.. Buýt có thể được phân loại thành buýt địa chỉ, buýt dữ liệu, buýt điều khiển, v.v.. Để dễ dàng minh họa, chỉ mũi tên hai đầu được sử dụng trong Fig.10, nhưng không chỉ báo rằng, chỉ có một buýt hoặc chỉ một loại là buýt.

Bộ phận lưu trữ được tạo cấu hình để lưu trữ chương trình. Cụ thể, chương trình có thể bao gồm mã chương trình và mã chương trình bao gồm lệnh vận hành được bằng máy tính. Bộ phận lưu trữ có thể bao gồm bộ nhớ và bộ nhớ không khả biến và tạo ra lệnh và dữ liệu cho bộ xử lý.

Bộ xử lý đọc chương trình máy tính tương ứng từ bộ nhớ không khả biến vào bộ nhớ và sau đó chạy chương trình máy tính tương ứng, để tạo ra thiết bị quản lý chứng chỉ số hóa dựa vào chuỗi khối theo thuật ngữ logic. Bộ xử lý thực thi chương trình được lưu trữ trong bộ nhớ để thực hiện các thao tác sau đây: gửi chứng chỉ số hóa của nút trong chuỗi khối và thông tin tình trạng hợp lệ của chứng chỉ số hóa tới chuỗi khối, để chuỗi khối xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ, để xác minh,

sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Phương pháp trên được thực hiện bởi thiết bị quản lý chứng chỉ số hóa dựa vào chuỗi khối và được bộc lộ theo phương án thực hiện ở trên của sáng chế có thể được áp dụng cho bộ xử lý hoặc có thể được thực thi bởi bộ xử lý. Bộ xử lý có thể là chip mạch tích hợp và có khả năng xử lý tín hiệu. Trong quá trình thực thi, các bước của phương pháp trên có thể được hoàn tất nhờ việc sử dụng mạch logic tích hợp của phần cứng trong bộ xử lý hoặc lệnh ở dạng phần mềm. Bộ xử lý trước đó có thể là bộ xử lý mục đích chung và bao gồm CPU, NP, v.v. hoặc có thể là DSP, ASIC, FPGA hoặc PLD khác, cổng riêng biệt hoặc thiết bị logic tranzito hoặc thành phần phần cứng riêng biệt. Bộ xử lý trước đó có thể thực thi hoặc thực hiện các phương pháp, các bước và các sơ đồ khối logic được bộc lộ theo các phương án thực hiện của sáng chế. Bộ xử lý mục đích chung có thể là bộ vi xử lý hoặc bộ xử lý có thể là bộ xử lý đã biết bất kỳ, v.v.. Các bước của phương pháp được bộc lộ dựa vào các phương án thực hiện của sáng chế có thể được thực hiện trực tiếp và hoàn thành bởi bộ xử lý mã hóa phần cứng hoặc có thể được thực hiện và hoàn thành nhờ việc sử dụng tổ hợp của môđun phần cứng và môđun phần mềm trong bộ xử lý giải mã. Môđun phần mềm có thể được đặt trong vật ghi trường thành trong lĩnh vực, như RAM, bộ nhớ flash, ROM, PROM, EEPROM và thanh ghi. Vật ghi được bố trí trong bộ phận lưu trữ và bộ xử lý đọc thông tin từ bộ nhớ và hoàn thành các bước của phương pháp trên nhờ việc sử dụng phần cứng của bộ xử lý.

Thiết bị điện tử có thể còn thực hiện phương pháp mà được thực hiện nhờ thiết bị quản lý chứng chỉ số hóa trên cơ sở chuỗi khối và thực thi các chức năng của thiết bị quản lý chứng chỉ số hóa dựa vào chuỗi khối theo phương án thực hiện ở trên. Các chi tiết không được mô tả theo phương án thực hiện này của sáng chế.

Theo phương án thực hiện, sáng chế còn đề xuất vật ghi đọc được bằng máy tính. Vật ghi đọc được bằng máy tính lưu trữ một hoặc nhiều chương trình, một hoặc nhiều chương trình bao gồm lệnh. Lệnh được thực thi bởi thiết bị điện tử bao gồm các chương trình ứng dụng để thực hiện phương pháp mà được thực hiện nhờ thiết bị quản lý chứng chỉ số hóa dựa vào chuỗi khối theo phương án thực hiện ở trên, bao gồm các bước: gửi chứng chỉ số hóa của nút trong chuỗi khối và thông tin tình trạng hợp lệ của chứng chỉ

số hóa tới chuỗi khối, để chuỗi khối xác định, dựa vào thông tin tình trạng hợp lệ của chứng chỉ số hoá, thông tin hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hoá và lưu trữ chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ, để xác minh, sau khi nút thứ hai trong chuỗi khối nhận yêu cầu truyền thông thứ nhất được gửi bởi nút thứ nhất, xem liệu chứng chỉ số hóa của nút thứ nhất có trong yêu cầu truyền thông thứ nhất là hợp lệ hay không.

Hơn nữa, trong thiết bị điện tử được thể hiện trên Fig.10, lệnh thực thi được thực thi bởi bộ xử lý để còn thực hiện các thao tác sau đây: nhận yêu cầu áp dụng chứng chỉ được gửi bởi nút trong chuỗi khối, ở đó yêu cầu áp dụng chứng chỉ bao gồm thông tin áp dụng của nút thứ nhất và được sử dụng để áp dụng cho trung tâm CA đối với chứng chỉ số hóa của nút thứ nhất; nhận và xem lại thông tin áp dụng của nút thứ nhất; và khi thông tin áp dụng của nút thứ nhất đã được xem lại, cấp chứng chỉ số hóa tới nút thứ nhất, ở đó thông tin tình trạng hợp lệ của chứng chỉ số hóa là hợp lệ.

Các phương án thực hiện trong sáng chế được mô tả theo cách liên tiếp. Đối với cùng các phần hoặc các phần tương tự theo các phương án thực hiện, là các phương án thực hiện. Mỗi phương án thực hiện tập trung vào khác biệt với các phương án thực hiện khác. Cụ thể, phương án thực hiện của hệ thống tương tự với phương án thực hiện của phương pháp và do đó, được mô tả vắn tắt. Đối với các phần liên quan, là phần mô tả liên quan theo phương án thực hiện của phương pháp.

Các phương án cụ thể của sáng chế được mô tả ở trên. Các phương án thực hiện khác nằm trong phạm vi của các điểm yêu cầu bảo hộ kèm theo. Trong một số trường hợp, các thao tác hoặc các bước được mô tả trong các điểm yêu cầu bảo hộ có thể được thực hiện theo thứ tự khác với thứ tự theo phương án thực hiện và các kết quả mong muốn có thể vẫn sẽ đạt được. Ngoài ra, quy trình được minh họa trên các hình vẽ kèm theo không nhất thiết yêu cầu thứ tự thực hiện cụ thể để đạt được các kết quả mong muốn. Theo một số phương án thực hiện, việc xử lý đa nhiệm hoặc song song có thể có lợi.

Người có hiểu biết trung bình về lĩnh vực cần hiểu rằng các phương án thực hiện của sáng chế có thể được tạo ra là phương pháp, hệ thống hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dạng chỉ các phương án thực hiện của phần

cứng, chỉ các phương án thực hiện của phần mềm hoặc các phương án thực hiện với tổ hợp của 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 giới hạn ở bộ nhớ dạng đĩa từ, bộ nhớ chỉ đọc đĩa compắc (CD-ROM) và bộ nhớ quang) chứa mã chương trình sử dụng được bởi máy tính.

Sáng chế được mô tả dựa vào 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 thi mỗi quy trình và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối và tổ hợp của quy trình và/hoặc khối trong các lưu đồ và/hoặc các sơ đồ khối. Các lệnh chương trình máy tính này có thể được tạo ra cho máy tính mục đích chung, 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 thực thi bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác để tạo ra thiết bị thực hiện chức năng cụ thể trong một hoặc nhiều quy trình 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 trữ 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 trữ trong bộ nhớ đọc được bằng máy tính tạo thành phần giả tạo bao gồm thiết bị lệnh. Thiết bị lệnh thực hiện chức năng cụ thể trong một hoặc nhiều quy trình 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 nạp vào máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, để một loạt các thao tác được thực hiện trên máy tính hoặc thiết bị lập trình được khác để tạo ra việc xử lý thực thi được bằng máy tính. Do đó, các lệnh được thực thi trên máy tính hoặc thiết bị lập trình được khác tạo ra các bước để thực hiện chức năng cụ thể trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Trong cấu hình điển hình, thiết bị điện toán bao gồm một hoặc nhiều CPU, giao diện đầu vào/đầu ra, giao diện mạng và bộ nhớ.

Bộ nhớ có thể bao gồm bộ nhớ khả biến, RAM, và/hoặc bộ nhớ không khả biến,

v.v.. Trong vật ghi đọc được bằng máy tính, ví dụ, ROM hoặc bộ nhớ flash. Bộ nhớ là ví dụ về vật ghi đọc được bằng máy tính.

Vật ghi đọc được bằng máy tính bao gồm bộ nhớ liên tục, không liên tục, tháo ra được và không tháo ra được có thể lưu trữ lệnh nhờ việc 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. Vật ghi máy tính bao gồm nhưng không giới hạn ở sự thay đổi pha RAM (PRAM), RAM tĩnh (SRAM), RAM động (DRAM), loại RAM khác, ROM, EEPROM, bộ nhớ flash hoặc thiết bị lưu trữ dạng bộ nhớ khác, CD-ROM, đĩa vạn năng kỹ thuật số (DVD) hoặc bộ nhớ quang khác, catxét, đĩa từ hoặc thiết bị lưu trữ từ khác hoặc bất kỳ phương tiện không truyền khác. Vật ghi máy tính có thể được tạo cấu hình để lưu trữ lệnh có thể được truy cập bởi thiết bị điện toán. Dựa vào định nghĩa trong phần mô tả này, vật ghi đọc được bằng máy tính không bao gồm phương tiện chuyển tiếp đọc được bằng máy tính như tính hiệu dữ liệu điều biến và sóng mang.

Còn lưu ý rằng, thuật ngữ “gồm có”, “bao gồm” hoặc biến thể bất kỳ khác được dự tính bao hàm không cạn quyền, sao cho quy trình, phương pháp, hàng hóa hoặc thiết bị bao gồm hàng loạt các chi tiết không chỉ bao gồm các chi tiết này, mà còn bao gồm các chi tiết khác không được liệt kê rõ ràng hoặc còn bao gồm các chi tiết vốn có cho quy trình, phương pháp, hàng hóa hoặc thiết bị. Chi tiết, đứng tiếp sau “bao gồm ...”, không có nhiều ràng buộc, không loại trừ sự có mặt của các chi tiết giống nhau trong quy trình, phương pháp, hàng hóa hoặc thiết bị bao gồm chi tiết này.

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

Phần mô tả trên chỉ là các phương án thực hiện của sáng chế và không nhằm giới hạn sáng chế. Người có hiểu biết trung bình về lĩnh vực có thể tạo ra các cải biến và các

thay đổi khác nhau đến sáng chế. Bất kỳ các cải biến, các thay thế tương đương, các cải tiến, v.v., đều nằm trong mục đích và nguyên lý của sáng chế sẽ nằm trong phạm vi bảo hộ của các điểm yêu cầu bảo hộ của sáng chế.

Fig.11 là lưu đồ minh họa ví dụ về phương pháp được thực hiện bằng máy tính 1100 để truyền thông giữa các nút chuỗi khối theo phương án thực hiện của sáng chế. Để thể hiện rõ ràng, phần mô tả là theo phương pháp 1100 mô tả chung theo bối cảnh của các hình vẽ khác trong phần mô tả này. Tuy nhiên, sẽ hiểu rằng, phương pháp 1100 có thể được thực hiện, ví dụ, bởi bất kỳ trong số hệ thống, môi trường, phần mềm và phần cứng hoặc tổ hợp của các hệ thống, các môi trường, phần mềm và phần cứng, nếu phù hợp. Theo một số phương án thực hiện, các bước khác nhau của phương pháp 1100 có thể được chạy song song, theo cách kết hợp, thành vòng lặp hoặc theo thứ tự bất kỳ.

Ở bước 1102, yêu cầu truyền thông thứ nhất được nhận ở nút thứ hai trong chuỗi khối, ở đó yêu cầu truyền thông thứ nhất được nhận từ nút thứ nhất trong cùng chuỗi khối. Các nút thứ nhất và thứ hai được mô tả ở đây có thể là hai nút khác nhau bất kỳ trong chuỗi khối. Khi nút thứ nhất mong muốn truyền thông với nút thứ hai, nút thứ nhất có thể khởi tạo quá trình đã mô tả. Ở đây, yêu cầu truyền thông thứ nhất có thể bao gồm chứng chỉ số hóa của nút thứ nhất để được sử dụng bởi nút thứ hai trong xác minh nhận dạng của nút thứ nhất. Hơn nữa, chứng chỉ số hóa của nút thứ nhất được lưu trữ trong chuỗi khối. Phương pháp 1100 chuyển từ bước 1102 sang bước 1104.

Ở bước 1104, nút thứ hai có thể truy cập, dựa vào yêu cầu truyền thông thứ nhất, tập hợp các thông tin hợp lệ của chứng chỉ kết hợp với các nút trong chuỗi khối. Thông tin hợp lệ của chứng chỉ có thể lưu trữ hoặc viết thông tin nhận dạng các chứng chỉ số hóa cụ thể được lưu trữ trong chuỗi khối là hợp lệ hoặc không hợp lệ (ví dụ, hủy bỏ các chứng chỉ số hóa). Trong một số trường hợp, thông tin hợp lệ của chứng chỉ có thể được cập nhật qua thời gian là thông tin hợp lệ mới được nhận, như từ xác minh chứng chỉ. Trong một số trường hợp, khi chứng chỉ số hóa của nút được nhận trước các bước vận hành của 1102, chứng chỉ số hóa của nút được lưu trữ trong chuỗi khối. Hơn nữa, tập hợp các thông tin hợp lệ của chứng chỉ dựa vào chứng chỉ số hóa và được sử dụng để phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa nhận được và nút kết hợp cũng được lưu trữ trong chuỗi khối. Làm như vậy, chứng chỉ số hóa có thể được xác minh sử dụng thông tin chống hàng giả để đảm bảo sự đúng đắn và độ chính xác của kết quả xác

minh mà không yêu cầu truy vấn thêm bên ngoài chuỗi khối, do vậy đảm bảo tính bảo mật truyền thông của các nút bên trong chuỗi khối. Trong một số trường hợp, thông tin hợp lệ của chứng chỉ có thể bao gồm danh sách chứng chỉ hợp lệ và danh sách chứng chỉ bị hủy, ở đó các danh sách này có thể được sử dụng để xác định tính hợp lệ tình trạng của nút và chứng chỉ số hóa cụ thể. Phương pháp 1100 chuyển từ bước 1104 sang bước 1106.

Ở bước 1106, dựa vào yêu cầu truyền thông thứ nhất và thông tin hợp lệ được truy cập của chứng chỉ, nút thứ hai xác minh xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không. Để xác minh xem liệu chứng chỉ số hóa của nút thứ nhất là hợp lệ hay không, nút thứ hai có khả năng đọc trực tiếp thông tin hợp lệ của chứng chỉ được lưu trữ cục bộ trong nút không cần đọc từ xa thông tin hợp lệ của chứng chỉ được lưu trữ trong trung tâm xác minh chứng chỉ (CA). Việc xác minh có thể bao gồm xác định xem liệu nút thứ nhất và chứng chỉ số hóa của nó được có trong danh sách chứng chỉ hợp lệ hoặc danh sách chứng chỉ không hợp lệ như được lưu trữ trong thông tin hợp lệ cục bộ của chứng chỉ hay không. Nếu chứng chỉ số hóa của nút thứ nhất được xác định là hợp lệ, thì phương pháp 1100 có thể tiếp tục ở bước 1108. Nếu chứng chỉ số hóa của nút thứ nhất được xác định là không hợp lệ, thì phương pháp 1100 kết thúc, khi chứng chỉ số hóa của nút thứ nhất không thể được xác minh là hợp lệ.

Ở bước 1108, xác định được thực hiện để xem liệu giao thức truyền thông để truyền thông liên nút (ví dụ, giữa nút thứ nhất và thứ hai) đơn hướng hoặc hai hướng. Nếu giao thức truyền thông yêu cầu xác minh đơn hướng, thì phương pháp 1100 tiếp tục ở bước 1110. Nếu giao thức truyền thông yêu cầu xác minh hai hướng, thì phương pháp 1100 chuyển sang bước 1112. Trong việc xác minh đơn hướng, xác minh tính hợp lệ của chứng chỉ số hóa của nút thứ nhất là đủ để thiết lập kết nối truyền thông giữa nút thứ hai và nút thứ nhất. Trong xác minh hai hướng, nút thứ nhất cũng phải xác minh nút thứ hai trước khi kết nối truyền thông có thể được thiết lập.

Ở bước 1112, theo phương án thực hiện xác minh hai hướng, yêu cầu truyền thông thứ hai được gửi từ nút thứ hai tới nút thứ nhất, ở đó yêu cầu truyền thông thứ hai bao gồm chứng chỉ số hóa của nút thứ hai, trong đó chứng chỉ số hóa của nút thứ hai được lưu trữ trong cùng chuỗi khối như hai nút. Yêu cầu truyền thông thứ hai có thể được gửi phản hồi việc xác minh thành công tính hợp lệ của nút thứ nhất hoặc yêu cầu truyền

thông thứ hai có thể được gửi phản hồi tới nhận yêu cầu truyền thông thứ nhất. Trong một số trường hợp, yêu cầu truyền thông thứ hai có thể được gửi bất kể xem liệu nút thứ nhất được xác định là hợp lệ hay không. Từ bước 1112, phương pháp 1100 chuyển sang bước 1114.

Ở bước 1114, nút thứ nhất, dựa vào yêu cầu truyền thông thứ hai, có thể truy cập thông tin hợp lệ của chứng chỉ, tương tự với các thao tác được thực hiện bởi nút thứ hai ở bước 1104. Ở bước 1116, nút thứ nhất có thể xác minh, dựa vào yêu cầu truyền thông thứ hai và thông tin hợp lệ được truy cập của chứng chỉ, xem liệu chứng chỉ số hóa của nút thứ hai là hợp lệ hay không, tương tự với các thao tác được thực hiện bởi nút thứ nhất ở bước 1106. Nếu chứng chỉ số hóa của nút thứ hai là không hợp lệ, thì kết nối truyền thông không thể được thiết lập. Tuy nhiên, nếu, chứng chỉ số hóa của nút thứ hai được xác minh là hợp lệ, phương pháp 1100 có thể chuyển sang bước 1110.

Ở bước 1110, kết nối truyền thông giữa nút thứ hai và nút thứ nhất có thể được thiết lập dựa vào (các) xác minh.

Trong một số trường hợp, một hoặc nhiều chứng chỉ số hóa kết hợp với các nút cụ thể là có thể bị hủy bỏ bởi CA cơ quan cấp từ trước chứng chỉ số hóa. Trong các trường hợp này, thông tin tình trạng hợp lệ của chứng chỉ số hóa được thay đổi từ “hợp lệ” thành “không hợp lệ” (hoặc “bị hủy”). CA sau đó có thể gửi, tới chuỗi khối, lệnh cập nhật thông tin tình trạng hợp lệ của chứng chỉ số hóa cho nút cụ thể. Khi nhận các lệnh, chứng chỉ số hóa đã lưu trữ có thể được cập nhật và xác minh thông tin chứng chỉ có thể được cập nhật để phản ánh tình trạng hiện thời của chứng chỉ số hóa của nút. Thông tin này có thể được lưu trữ trong chuỗi khối và được sử dụng cho các giao dịch trong tương lai.

Trong một số trường hợp, thiết lập kết nối truyền thông giữa các nút trong chuỗi khối nhờ việc sử dụng giao thức SSL hoặc giao thức TLS. Do đó, yêu cầu truyền thông thứ nhất thu được bởi nút thứ hai được gửi bởi nút thứ nhất dựa vào giao thức SSL hoặc giao thức TLS và kênh truyền thông đã mã hóa được thiết lập giữa các nút. Kết nối mạng có thể được mã hóa ở lớp truyền nhờ việc sử dụng giao thức SSL hoặc giao thức TLS để đảm bảo tính bảo mật truyền dữ liệu. Nhờ việc sử dụng công nghệ mã hóa dữ liệu, có thể còn đảm bảo rằng, dữ liệu không bị chặn hoặc nghe lén trong quá trình truyền

qua internet. Sau bước 1110, phương pháp 1100 ngừng lại.

Các phương án thực hiện của giải pháp kỹ thuật được mô tả trong bản mô tả này có thể được thực hiện để nhận thực các lợi ích và các hiệu quả kỹ thuật cụ thể. Ví dụ, các phương án thực hiện của giải pháp kỹ thuật được mô tả sử dụng các lợi ích của chuỗi khối, như sự phi tập trung, công khai và minh bạch và chống làm giả, để đảm bảo rằng tính bảo mật được duy trì. Thậm chí nếu trung tâm CA bị tấn công, tin tặc không thể làm giả chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và do đó, không thể sử dụng chứng chỉ số hóa không hợp lệ để tham gia vào chuỗi khối. Thông tin hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối và có thể phản ánh đúng thông tin tình trạng hợp lệ của chứng chỉ nút. Do đó, nhờ việc sử dụng thông tin hợp lệ của chứng chỉ để xác minh xem liệu chứng chỉ nút là hợp lệ hay không, nút chưa được phép có thể được ngăn không cho tham gia vào chuỗi khối để đảm bảo tính bảo mật truyền thông giữa các nút chuỗi khối và còn gia tăng tính bảo mật của mạng chuỗi khối.

Theo các phương án thực hiện của sáng chế, chứng chỉ số hóa của mỗi nút trong chuỗi khối và thông tin hợp lệ từ trước của chứng chỉ được lưu trữ trong chuỗi khối chứa nút và chứng chỉ số hóa có thể được lưu trữ trong chuỗi khối bằng cách viết chứng chỉ số hóa vào chuỗi khối. Do đó, theo các phương án thực hiện của sáng chế, các tính chất của chuỗi khối, như sự phi tập trung và chống làm giả, có thể được sử dụng để ngăn không cho tin tặc làm giả chứng chỉ số hóa và thông tin hợp lệ của chứng chỉ phản ánh thông tin tình trạng hợp lệ của chứng chỉ số hóa để đảm bảo rằng kết quả xác minh tính hợp lệ của chứng chỉ là đúng và chính xác và nhờ vậy đảm bảo tính bảo mật và tính ổn định của mạng chuỗi khối. Ngoài ra, theo phương án thực hiện này của sáng chế, khi xác minh tính hợp lệ của chứng chỉ số hóa, nút thứ hai có thể đọc trực tiếp thông tin hợp lệ của chứng chỉ được lưu trữ cục bộ trong nút không cần đọc từ xa thông tin hợp lệ của chứng chỉ được lưu trữ ở trung tâm CA. Dựa vào điều này, tốc độ và tính bảo mật của xác minh hợp lệ được nâng cao. Ngoài ra, nhờ việc gọi cục bộ thông tin như thông tin hợp lệ của chứng chỉ, sự phụ thuộc vào một điểm của chuỗi khối ở trung tâm CA có thể được loại trừ và độ tin cậy của mạng chuỗi khối còn được gia tăng.

Các phương án và các thao tác được mô tả trong phần mô tả này có thể được thực hiện trong mạch điện tử dạng số hoặc trong phần mềm, phần sụn hoặc phần cứng của máy tính, bằng các kết cấu được bộc lộ trong phần mô tả này hoặc tổ hợp của một hoặc

nhiều phần này. Các thao tác có thể được thực thi là các thao tác được thực hiện bởi thiết bị xử lý dữ liệu đến dữ liệu được lưu trữ trên một hoặc nhiều thiết bị lưu trữ đọc được bằng máy tính hoặc nhận được từ các nguồn khác. Thiết bị xử lý dữ liệu, máy tính hoặc thiết bị điện toán có thể bao hàm thiết bị, các thiết bị và các máy xử lý dữ liệu, 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 trên. Thiết bị có thể bao gồm mạch logic chuyên dụng, ví dụ, bộ xử lý trung tâm (CPU), mảng cổng lập trình được dạng trường (FPGA) hoặc mạch tích hợp chuyên dụng (ASIC). Thiết bị có thể cũng bao gồm mã tạo ra môi trường thực thi cho chương trình máy tính đó, ví dụ, mã tạo thành phần sun của bộ xử lý, chồng giao thức, hệ thống quản lý cơ sở dữ liệu, hệ thống điều hành (ví dụ hệ thống điều hành hoặc tổ hợp của các hệ thống điều hành), môi trường thời gian chạy đa nền tảng, máy ảo hoặc tổ hợp của một hoặc nhiều thiết bị này. Thiết bị và môi trường thực thi có thể nhận biết các cơ sở hạ tầng mô hình điện toán khác nhau, 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, kịch bản có thể áp dụng hoặc mã) có thể được viết ở dạng ngôn ngữ lập trình bất kỳ, bao gồm các ngôn ngữ biên tập hoặc biên 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, vật hoặc bộ phận khác phù hợp để sử dụng trong môi trường điện toán. Chương trình có thể được lưu trữ thành phần của tệp tin giữ chương trình khác hoặc dữ liệu (ví dụ, một hoặc nhiều kịch bản có thể áp dụng được lưu trữ trong tài liệu ngôn ngữ đánh dấu), trong một tệp tin chuyên dụng cho chương trình đó hoặc trong các tệp tin nhiều tọa độ (ví dụ, các tệp tin lưu trữ một hoặc nhiều môđun, các chương trình con hoặc các phần của mã). Chương trình máy tính có thể được thực thi trên máy tính hoặc trên nhiều máy tính được đặt ở một vị trí hoặc được phân bổ qua 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, lấy ví dụ, cả hai bộ vi xử lý mục đích chung và chuyên dụng và bất kỳ trong số một hoặc nhiều bộ xử lý 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 chi tiết 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 trữ các lệnh và dữ liệu. Nói chung, máy tính cũng sẽ bao gồm hoặc được ghép nối vận hành được để nhận dữ liệu từ hoặc truyền dữ liệu tới hoặc cả hai, một hoặc nhiều thiết bị lưu trữ lớn để lưu trữ dữ liệu. Máy tính có thể được nhúng trong thiết bị khác, ví dụ, thiết bị di động, thiết bị hỗ trợ số cá nhân (PDA), bảng điều khiển trò chơi, bộ thu của hệ thống định vị toàn cầu (GPS) hoặc thiết bị lưu trữ cầm tay. Các thiết bị phù hợp để lưu trữ các lệnh chương trình máy tính và dữ liệu bao gồm bộ nhớ không khả biến, phương tiện và thiết bị nhớ, bao gồm, 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, mạch logic chuyên dụng.

Các thiết bị di động có thể bao gồm các thiết bị cầm tay, thiết bị người dùng (UE), các điện thoại di động (ví dụ, các điện thoại thông minh), các máy tính bảng, các thiết bị đeo được (ví dụ, các đồng hồ thông minh và các kính mắt thông minh), các thiết bị cấy ghép bên trong cơ thể người (ví dụ, các cảm biến sinh học, các thiết bị cấy ghép ốc tai điện tử) hoặc các loại khác của các thiết bị di động. Các thiết bị di động có thể truyền thông vô tuyến (ví dụ, sử dụng các tính tần số radio (RF) với các mạng truyền thông khác nhau (được mô tả dưới đây). Các thiết bị di động có thể bao gồm các cảm biến để xác định các tính chất của môi trường hiện tại của thiết bị di động. Các cảm biến có thể bao gồm camera, micrô, cảm biến tiệm cận, cảm biến GPS, cảm biến chuyển động, gia tốc kế, cảm biến ánh sáng môi trường, cảm biến âm, con quay hồi chuyển, la bàn, phong vũ biểu, cảm biến vân tay, hệ thống nhận dạng khuôn mặt, cảm biến RF (ví dụ, Wi-Fi và radio dạng tế bào), cảm biến nhiệt hoặc loại cảm biến khác. Ví dụ, camera có thể bao gồm camera lắp ở phía trước và phía sau với vật kính tháo ra được hoặc cố định, đèn flash, cảm biến ảnh và bộ xử lý ảnh. Camera có thể là camera megapixel có khả năng chụp chi tiết để nhận dạng khuôn mặt và/hoặc móng mắt. Camera cùng với bộ xử lý dữ liệu và xác thực lệnh được lưu trữ trong bộ nhớ hoặc được truy cập từ xa có thể tạo thành hệ thống nhận dạng khuôn mặt. Hệ thống nhận dạng khuôn mặt hoặc một hoặc nhiều cảm biến, ví dụ, micrô, cảm biến chuyển động, gia tốc kế, cảm biến GPS hoặc 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 thi trên máy tính có thiết bị hiển thị và thiết bị nhập, ví dụ, màn hình tinh thể lỏng (LCD) hoặc điốt

phát sáng hữu cơ (OLED)/màn hình hiển thị thực tế ảo (VR)/thực tế tăng cường (AR) để hiển thị lệnh tới người dùng và màn hình chạm, bàn phím và thiết bị trợ nhờ đó người dùng có thể nhập vào máy tính. Các loại thiết bị khác có thể được sử dụng để tạo ra tương tác với người dùng; ví dụ, hồi tiếp được tạo ra cho người dùng có thể có dạng hồi tiếp cảm biến bất kỳ, ví dụ, hồi tiếp thị giác, hồi tiếp thính giác hoặc hồi tiếp xúc giác; và việc nhập từ người dùng có thể nhận được ở dạng bất kỳ, bao gồm âm thanh, giọng nói hoặc đầu vào xúc giác. Ngoài ra, máy tính có thể tương tác với người dùng bằng cách gửi các tài liệu tới và nhận các tài liệu từ thiết bị được sử dụng bởi người dùng; ví dụ, bằng cách gửi các trang web tới trình duyệt web trên thiết bị máy khách của người dùng phản hồi các yêu cầu nhận được từ trình duyệt web.

Các phương án có thể được thực thi sử dụng các thiết bị điện toán được kết nối với nhau bởi bất kỳ dạng hoặc môi trường truyền thông dữ liệu kỹ thuật số hữu tuyến hoặc vô tuyến (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 mà diễn hình tương tác qua mạng truyền thông. Máy khách, ví dụ, thiết bị di động, bản thân có thể 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 phép chúng. Các giao dịch này có thể có trong thời gian thực, để thao tác hoặc phản hồi là tạm thời; ví dụ cá nhân nhận thực thao tác hoặc phản hồi xuất hiện về cơ bản đồng thời, chênh lệch về thời gian để phản hồi sau mỗi thao tác tiêu tốn là nhỏ hơn 1 mili giây (ms) hoặc nhỏ hơn 1 giây (s) hoặc phản hồi không có thời gian trễ chủ ý tính đến các giới hạn xử lý của hệ thống.

Các ví dụ về các mạng truyền thông bao gồm mạng diện nội bộ (LAN), mạng truy cập radio (RAN), mạng diện đô thị (MAN) và mạng diện rộng (WAN). Mạng truyền thông có thể bao gồm tất cả các mạng internet hoặc một phần của các mạng internet, các mạng truyền thông khác hoặc tổ hợp của các mạng truyền thông. Lệnh có thể được truyền trên mạng truyền thông theo các giao thức và tiêu chuẩn khác nhau, bao gồm tiến hóa dài hạn (LTE), 5G, IEEE 802, giao thức internet (IP) hoặc các giao thức khác hoặc tổ hợp của các giao thức này. Mạng truyền thông có thể truyền giọng nói, video, sinh trắc hoặc dữ liệu xác thực hoặc lệnh khác giữa các thiết bị điện toán đã kết nối.

Các dấu hiệu được mô tả như các phương án thực hiện riêng biệt có thể được thực hiện, theo cách kết hợp, theo một phương án thực hiện, trong lúc 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 tổ hợp con phù hợp bất kỳ. Các thao tác được mô tả và yêu cầu bảo hộ theo thứ tự cụ thể cần được hiểu là không nhất định là yêu cầu thứ tự cụ thể này hay tất cả các thao tác minh họa (một số thao tác có thể là tùy ý) phải được thực hiện. Nếu phù 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 giữa các nút chuỗi khối, trong đó phương pháp này bao gồm các bước:

tiếp nhận, bởi nút thứ hai, yêu cầu thứ nhất để thiết lập kết nối truyền thông thứ nhất giữa nút thứ nhất và nút thứ hai trong chuỗi khối, yêu cầu thứ nhất được gửi bởi nút thứ nhất, trong đó yêu cầu thứ nhất bao gồm chứng chỉ số hoá của nút thứ nhất và chứng chỉ số hoá của nút thứ nhất được lưu trữ trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai (bước S101);

xác minh, bởi nút thứ hai dựa vào chứng chỉ số hoá được tiếp nhận cùng với yêu cầu thứ nhất và dựa vào việc truy xuất thông tin về tính hợp lệ của chứng chỉ của chứng chỉ số hoá, liệu chứng chỉ số hoá của nút thứ nhất có hợp lệ hay không, trong đó chứng chỉ số hoá của nút thứ nhất và thông tin trạng thái hợp lệ của chứng chỉ số hoá được đối chiếu trước để tạo thành thông tin về tính hợp lệ của chứng chỉ và được lưu trữ trong chuỗi khối, trong đó thông tin về tính hợp lệ của chứng chỉ được ghép dựa vào danh mục chứng chỉ hợp lệ dùng cho các chứng chỉ số hoá hợp lệ và danh mục chứng chỉ bị huỷ bỏ dùng cho các chứng chỉ số hoá không hợp lệ, và trong đó bước xác minh chứng chỉ số hoá này bao gồm:

truy vấn để truy xuất cục bộ, bởi nút thứ hai, thông tin về tính hợp lệ của chứng chỉ dùng cho chứng chỉ số hoá của nút thứ nhất từ chuỗi khối để xác minh chứng chỉ số hoá được tiếp nhận cùng với yêu cầu thứ nhất (bước S103); và

khi chứng chỉ số hoá thứ nhất của nút thứ nhất được xác định là hợp lệ dựa vào thông tin về tính hợp lệ của chứng chỉ thì xác định, bởi nút thứ hai, để thiết lập kết nối truyền thông thứ nhất với nút thứ nhất (bước S105).

2. Phương pháp theo điểm 1, trong đó phương pháp này còn bao gồm các bước:

gửi, bởi nút thứ hai, yêu cầu thứ hai để thiết lập kết nối truyền thông thứ hai giữa nút thứ hai và nút thứ nhất, trong đó yêu cầu thứ hai được gửi tới nút thứ nhất, trong đó yêu cầu thứ hai bao gồm chứng chỉ số hoá của nút thứ hai, để nút thứ nhất xác minh, dựa vào yêu cầu thứ hai và thông tin về tính hợp lệ của chứng chỉ, liệu chứng chỉ số hoá của nút thứ hai

có hợp lệ hay không (bước S01); và

khi chứng chỉ số hoá của nút thứ nhất là hợp lệ thì xác định, bởi nút thứ hai, liệu có thiết lập kết nối truyền thông thứ hai với nút thứ nhất hay không, bước này bao gồm:

khi chứng chỉ số hoá của nút thứ nhất là hợp lệ và nút thứ nhất xác minh rằng chứng chỉ số hoá của nút thứ hai là hợp lệ thì thiết lập, bởi nút thứ hai, kết nối truyền thông thứ hai với nút thứ nhất (bước S05).

3. Phương pháp theo điểm 1 hoặc 2, trong đó thông tin về tính hợp lệ của chứng chỉ ghi lại chứng chỉ số hoá không hợp lệ bị huỷ bỏ và bước xác minh, bởi nút thứ hai dựa vào yêu cầu thứ nhất và thông tin về tính hợp lệ của chứng chỉ, liệu chứng chỉ số hoá của nút thứ nhất có hợp lệ hay không, bao gồm các bước:

xác định, bởi nút thứ hai, chứng chỉ số hoá của nút thứ nhất dựa vào yêu cầu thứ nhất;

xác minh, bởi nút thứ hai dựa vào thông tin về tính hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối, liệu chứng chỉ số hoá của nút thứ nhất có được ghi lại trong thông tin về tính hợp lệ của chứng chỉ hiện thời hay không; và

nếu chứng chỉ số hoá của nút thứ nhất được ghi lại trong thông tin về tính hợp lệ của chứng chỉ thì xác định rằng chứng chỉ số hoá của nút thứ nhất là không hợp lệ.

4. Phương pháp theo điểm 1 hoặc 2, trong đó thông tin về tính hợp lệ của chứng chỉ ghi lại chứng chỉ số hoá hợp lệ và bước xác minh, bởi nút thứ hai dựa vào yêu cầu thứ nhất và thông tin về tính hợp lệ của chứng chỉ, liệu chứng chỉ số hoá của nút thứ nhất có hợp lệ hay không, bao gồm các bước:

xác định, bởi nút thứ hai, chứng chỉ số hoá của nút thứ nhất dựa vào yêu cầu thứ nhất;

xác minh, bởi nút thứ hai dựa vào thông tin về tính hợp lệ của chứng chỉ được lưu trữ trong chuỗi khối, liệu chứng chỉ số hoá của nút thứ nhất có được ghi lại trong thông tin về tính hợp lệ của chứng chỉ hay không; và

xác minh rằng chứng chỉ số hoá của nút thứ nhất là hợp lệ, nếu chứng chỉ số hoá của nút thứ nhất được ghi lại trong thông tin về tính hợp lệ của chứng chỉ.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó trước bước tiếp nhận, bởi nút thứ hai, yêu cầu thứ nhất được gửi bởi nút thứ nhất, phương pháp này còn bao gồm bước:

lưu trữ, bằng cách ghi chứng chỉ số hoá của nút thứ nhất vào chuỗi khối, chứng chỉ số hoá của nút thứ nhất trong chuỗi khối bao gồm nút thứ nhất và nút thứ hai.

6. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó thông tin về tính hợp lệ của chứng chỉ được xác định dựa vào chứng chỉ số hoá không hợp lệ bị huỷ bỏ và/hoặc chứng chỉ số hoá hợp lệ được tiếp nhận bởi chuỗi khối.

7. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó yêu cầu thứ nhất thu được bởi nút thứ hai được gửi bởi nút thứ nhất dựa vào giao thức SSL hoặc giao thức TLS.

8. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 7, phương pháp này còn bao gồm các bước:

tiếp nhận chứng chỉ số hoá của nút và thông tin trạng thái hợp lệ của chứng chỉ số hoá được gửi bởi trung tâm cấp phép chứng chỉ (bước S201);

xác định, dựa vào thông tin trạng thái hợp lệ của chứng chỉ số hoá, thông tin về tính hợp lệ của chứng chỉ được sử dụng để phản ánh thông tin trạng thái hợp lệ của chứng chỉ số hoá (bước S203); và

lưu trữ chứng chỉ số hoá và thông tin về tính hợp lệ của chứng chỉ trong chuỗi khối, trong đó chứng chỉ số hoá và thông tin về tính hợp lệ của chứng chỉ được sử dụng để xác minh, sau khi nút thứ hai trong chuỗi khối tiếp nhận yêu cầu thứ nhất được gửi bởi nút thứ nhất, liệu chứng chỉ số hoá của nút thứ nhất có trong yêu cầu thứ nhất có hợp lệ hay không (bước S205).

9. Phương pháp theo điểm 8, trong đó phương pháp này còn bao gồm bước:

gửi, bởi nút thứ nhất trong chuỗi khối, yêu cầu cấp chứng chỉ đến trung tâm cấp phép chứng chỉ, trong đó yêu cầu cấp chứng chỉ bao gồm thông tin áp dụng của nút thứ nhất và được

sử dụng để nộp vào trung tâm cấp phép chứng chỉ để xin chứng chỉ số hoá của nút thứ nhất.

10. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 9, trong đó chứng chỉ số hoá bao gồm ít nhất một trong số phiên bản, số thứ tự, thông tin về người giữ chứng chỉ, khoảng thời gian hiệu lực và chữ ký của trung tâm cấp phép chứng chỉ.

11. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 10, trong đó chứng chỉ số hoá là không hợp lệ trước khi được nối chuỗi trong nút của chuỗi khối.

12. Thiết bị điện tử, trong đó thiết bị điện tử này được áp dụng cho nút thứ hai trong chuỗi khối và bao gồm:

bộ xử lý; và

bộ nhớ, được tạo cấu hình để lưu trữ lệnh thực thi được bằng máy tính, trong đó lệnh thực thi được thực thi bởi bộ xử lý để thực hiện các bước theo điểm bất kỳ trong số các điểm từ 1 đến 11.

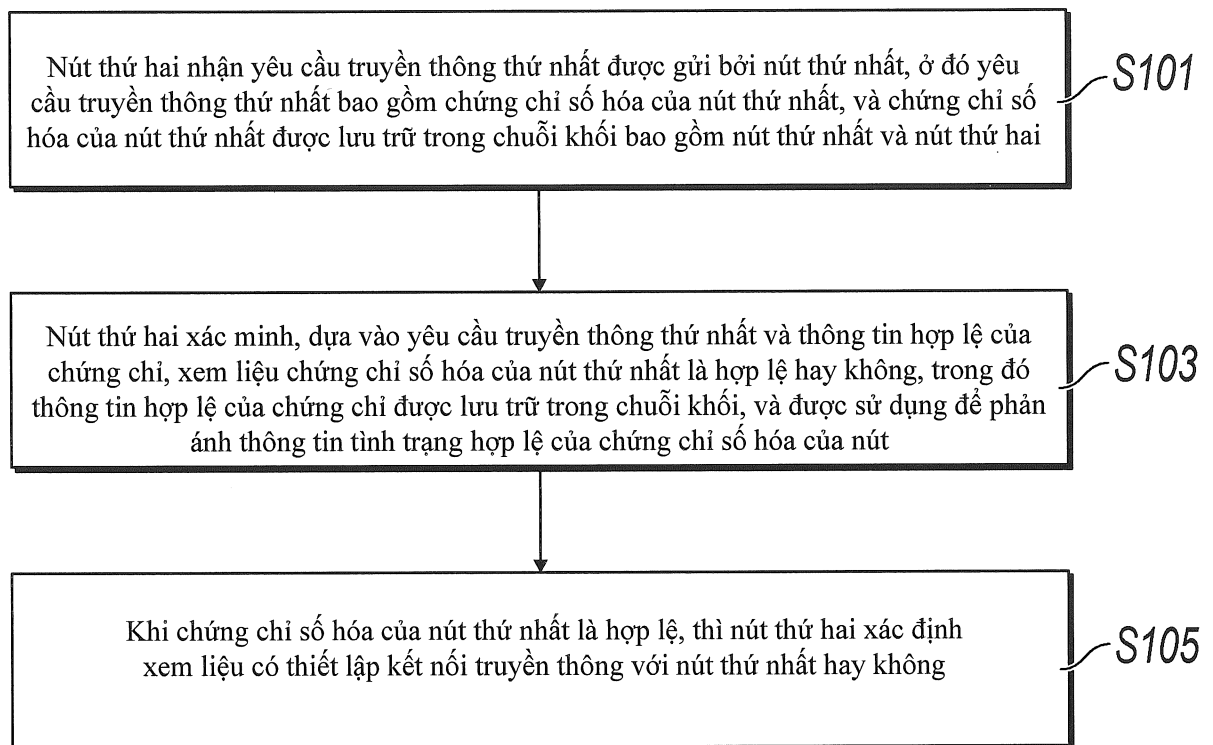


FIG. 1

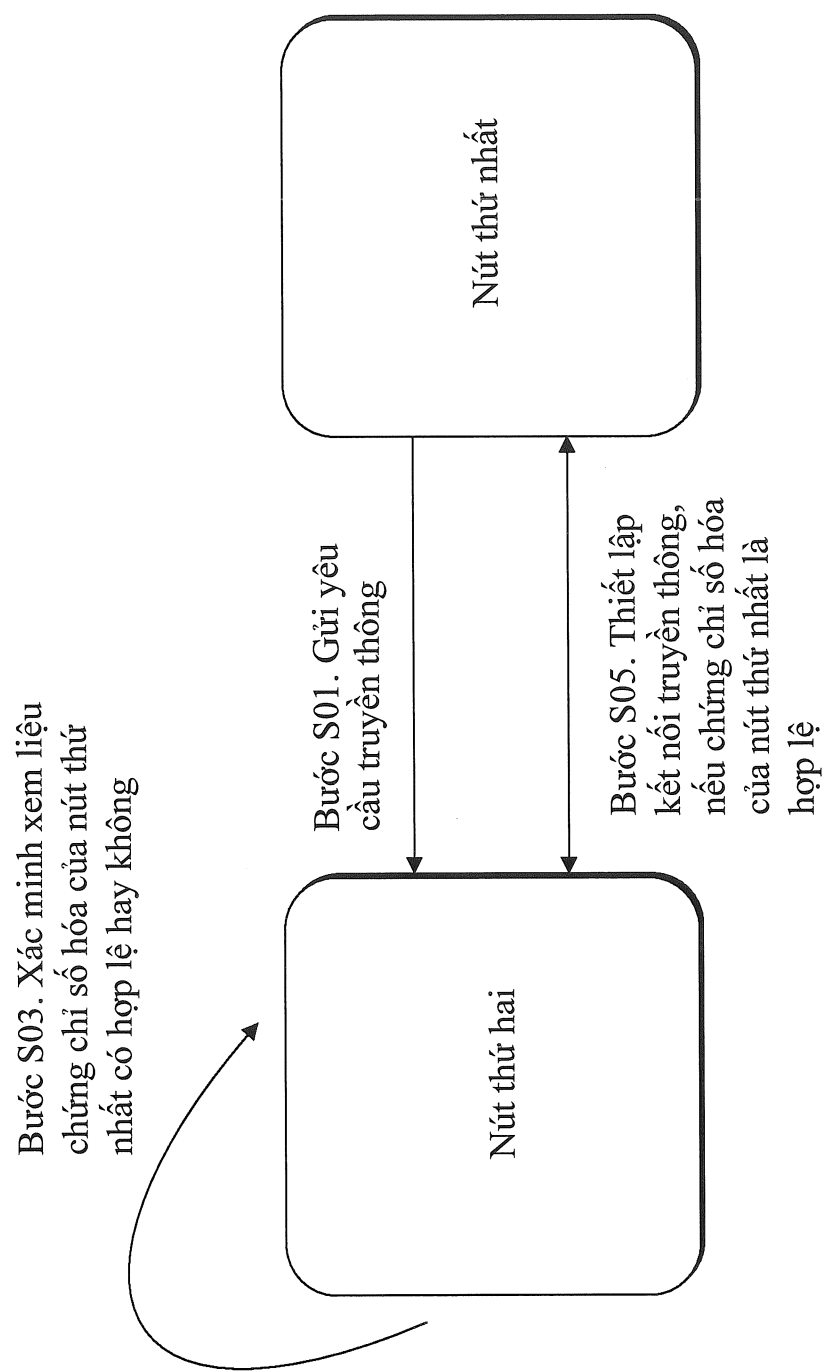


FIG. 2

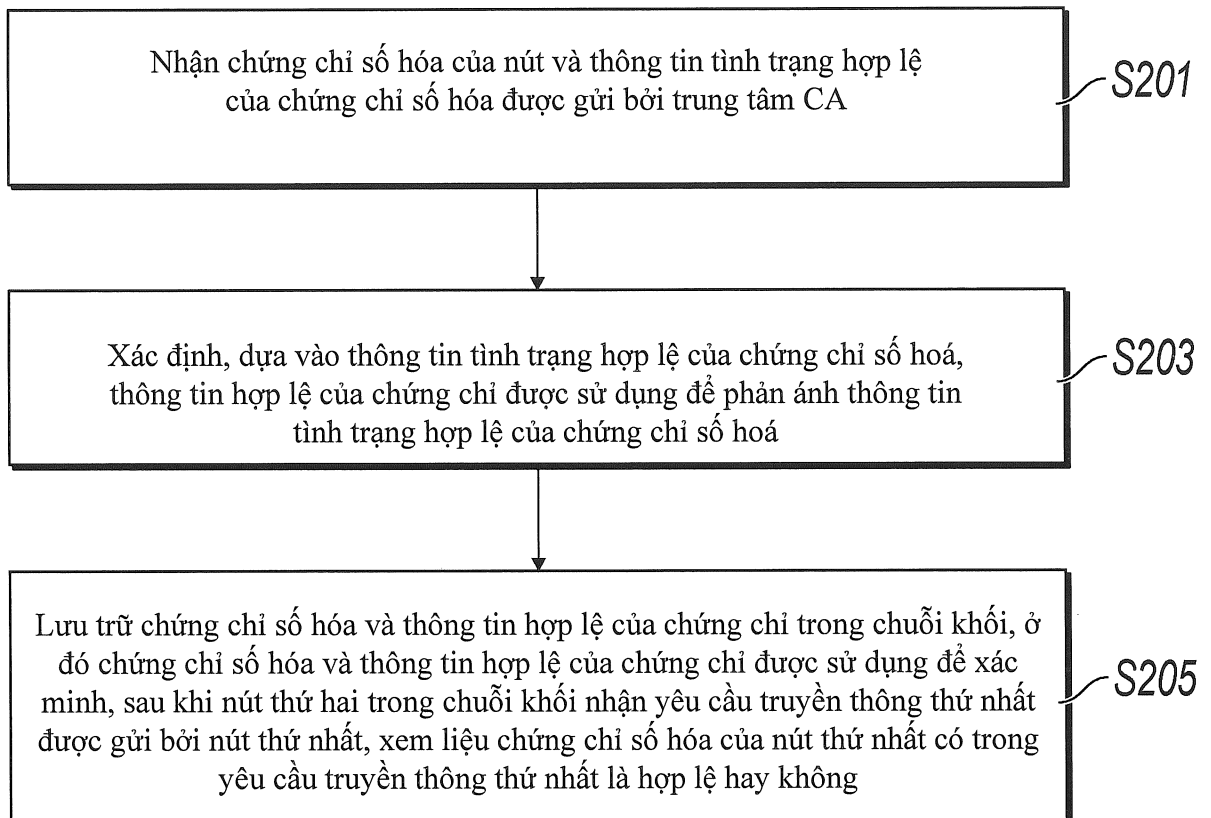
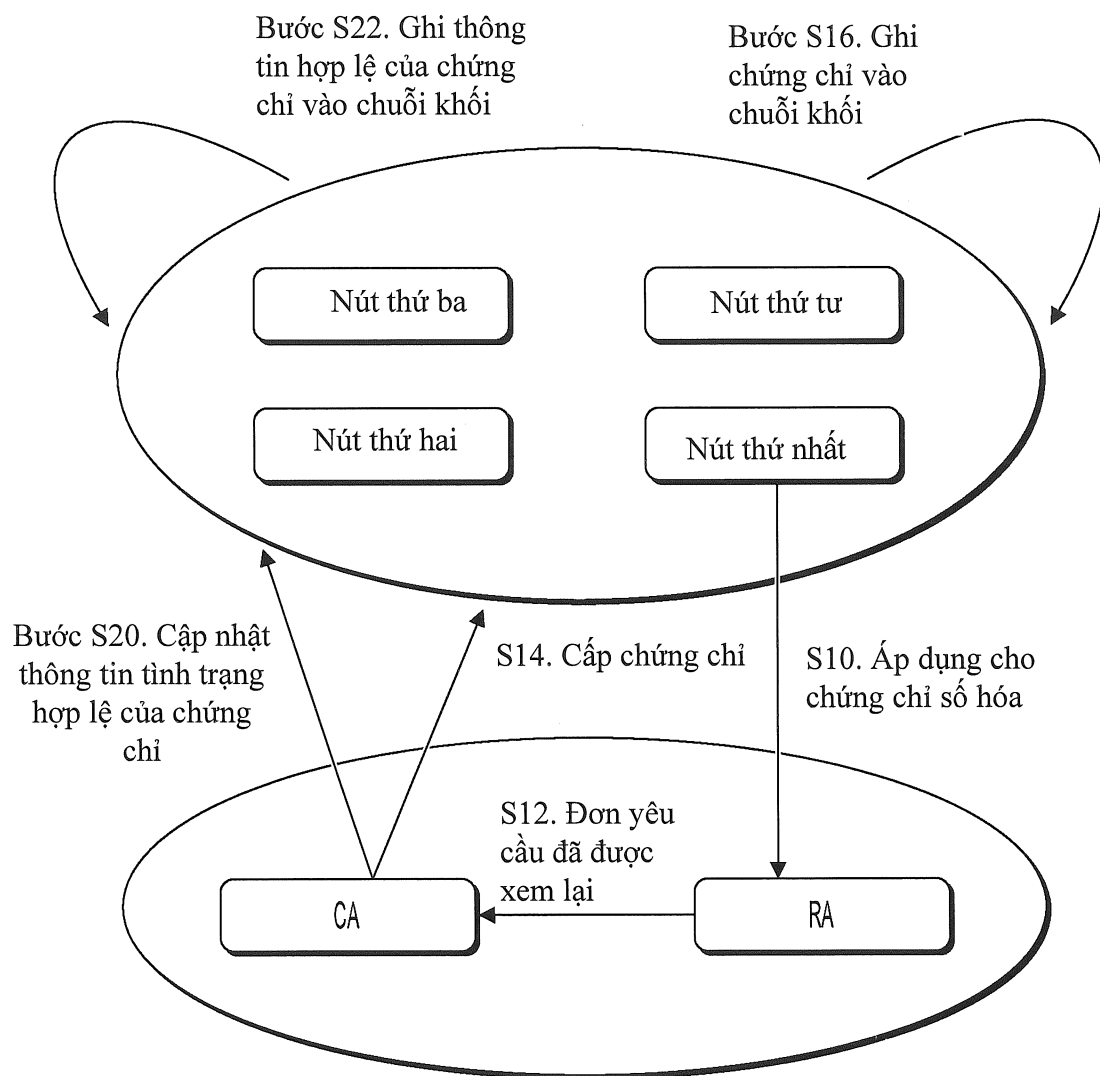
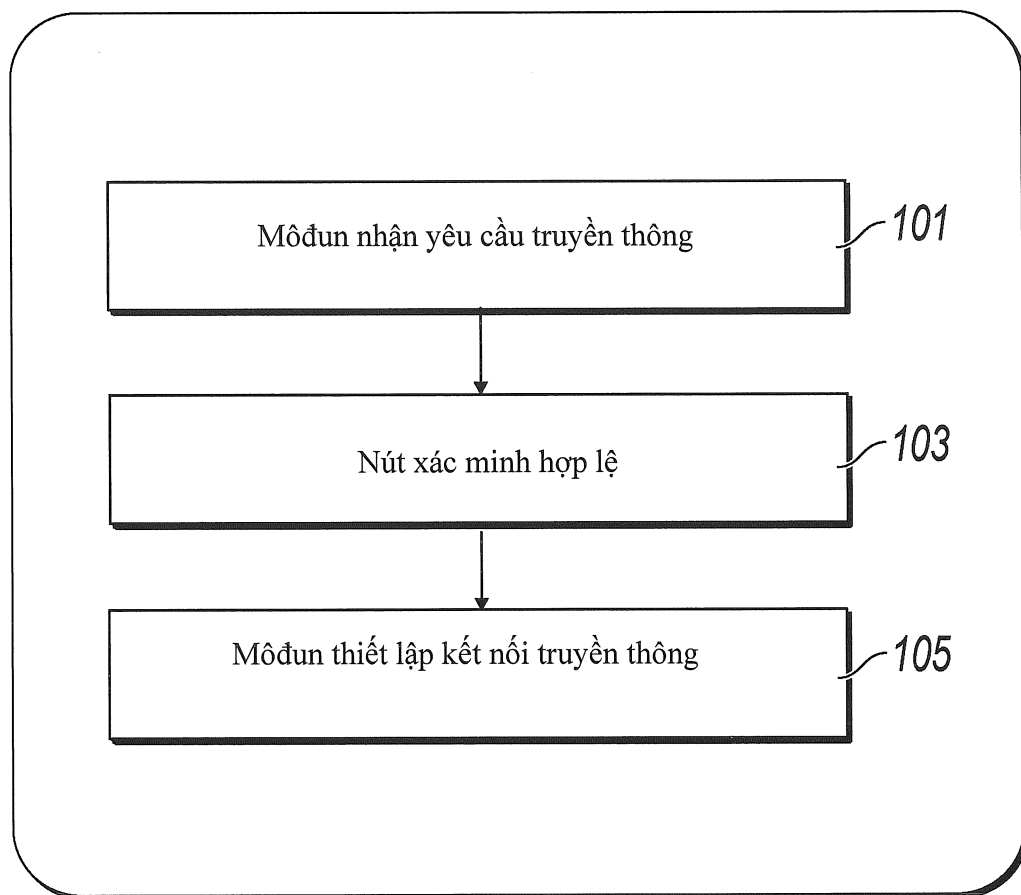
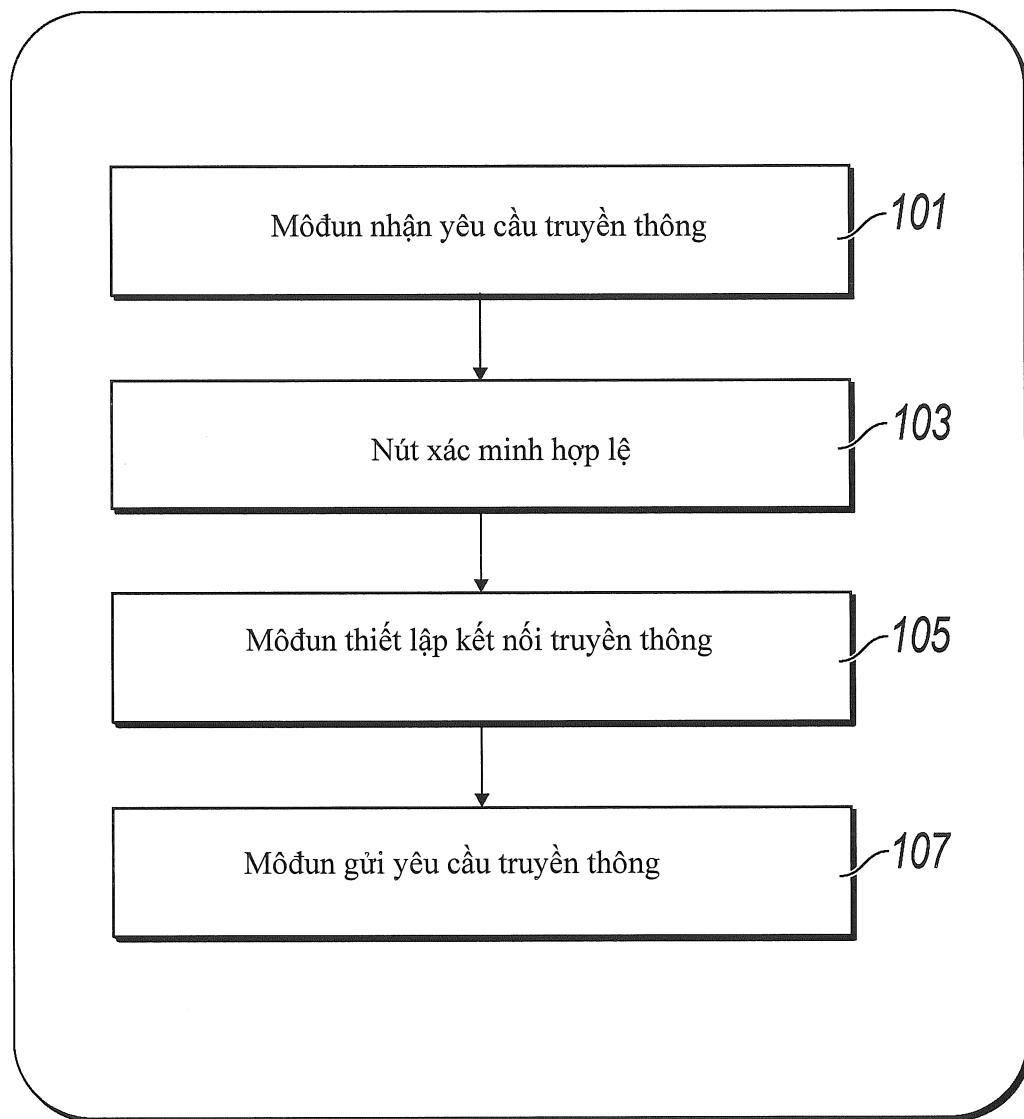


FIG. 3

**FIG. 4**

**FIG. 5**

**FIG. 6**

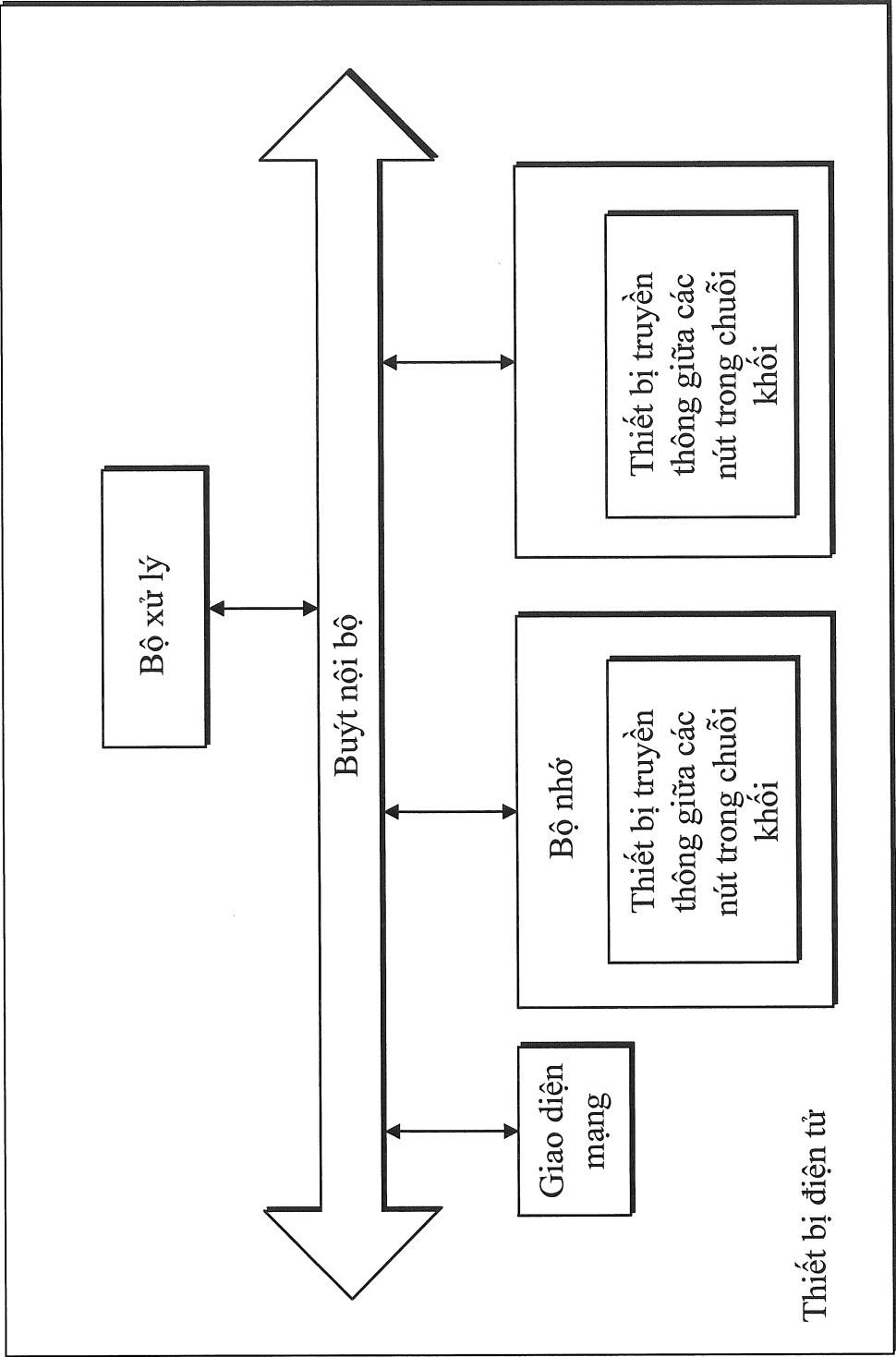
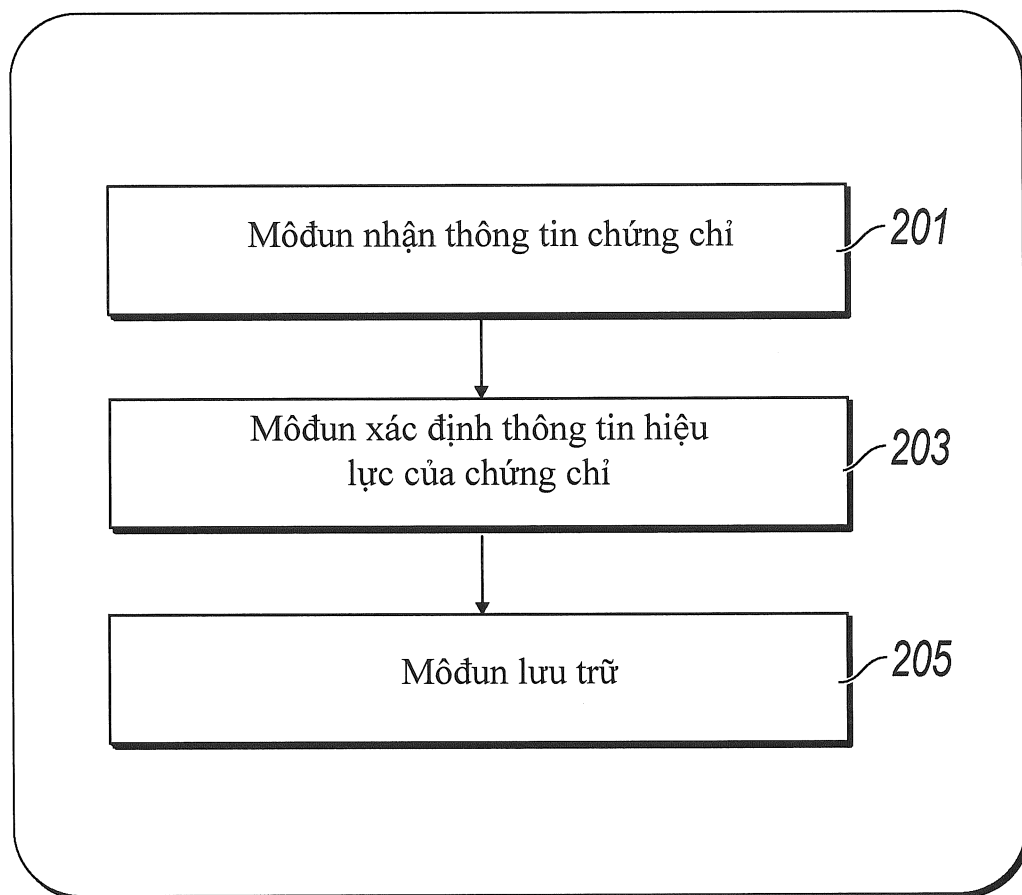


FIG. 7

**FIG. 8**

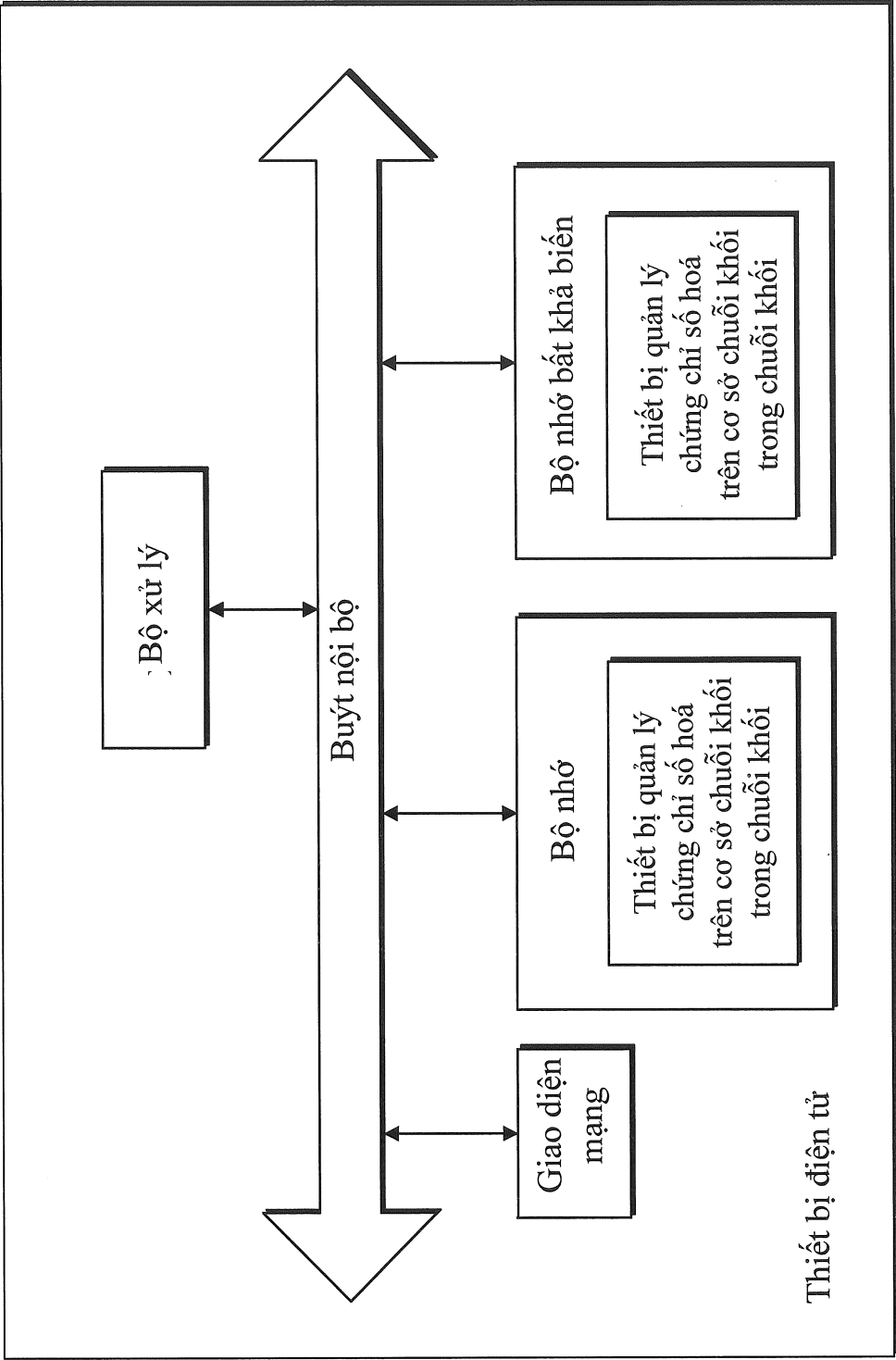


FIG. 9

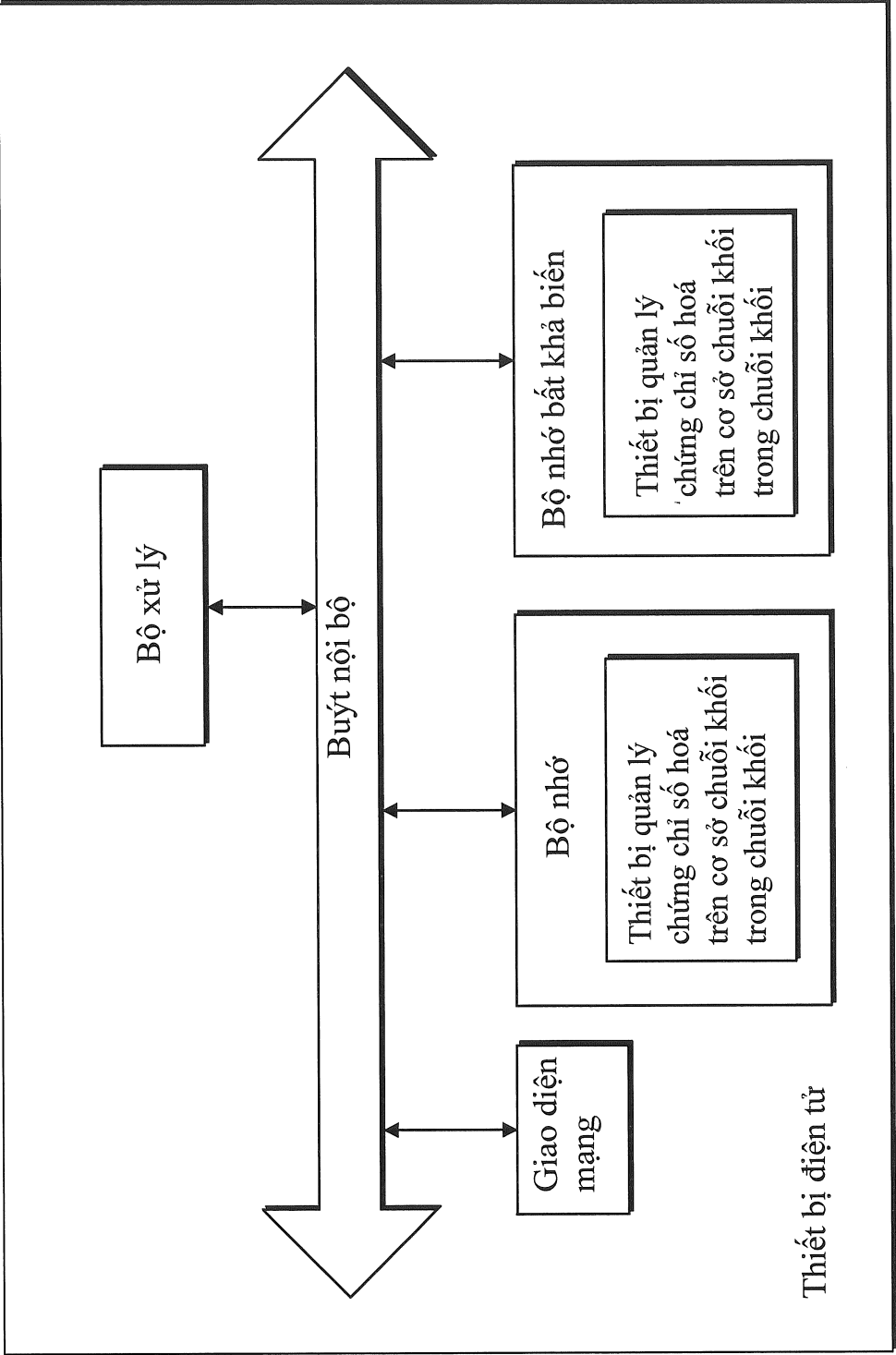


FIG. 10

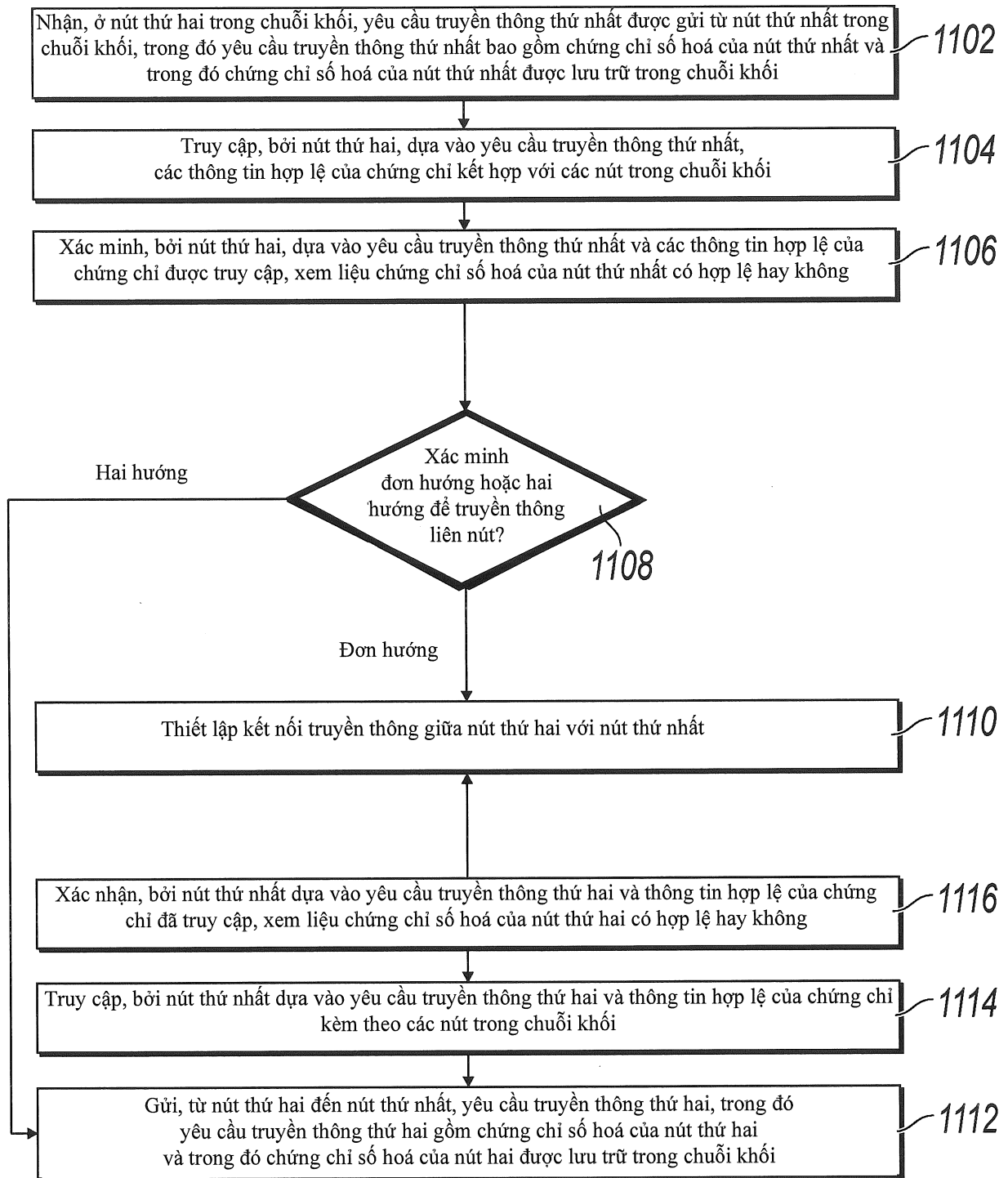


FIG. 11