



(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)



1-0045016

(51)⁷ H04L 9/32

(13) B

(21) 1-2019-04061

(22) 26/07/2018

(86) PCT/US2018/043897 26/07/2018

(87) WO 2019/023452 31/01/2019

(30) 201710617598.2 26/07/2017 CN

(45) 25/04/2025 445

(43) 27/04/2020 385A

(71) 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 QUẢN LÝ CHỨNG CHỈ SỐ

(21) 1-2019-04061

(57) Sáng chế đề cập đến phương pháp và thiết bị quản lý chứng chỉ số. Theo phương pháp này, yêu cầu giao dịch thứ nhất được gửi bởi cơ quan chứng nhận (CA) được nhận, trong đó yêu cầu giao dịch thứ nhất được sử dụng để yêu cầu viết chứng chỉ số được cấp bởi CA cho nút trong chuỗi khối vào chuỗi khối. Kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số được xác định. Yêu cầu giao dịch thứ nhất được đáp ứng hoặc từ chối dựa trên kết quả đồng thuận.

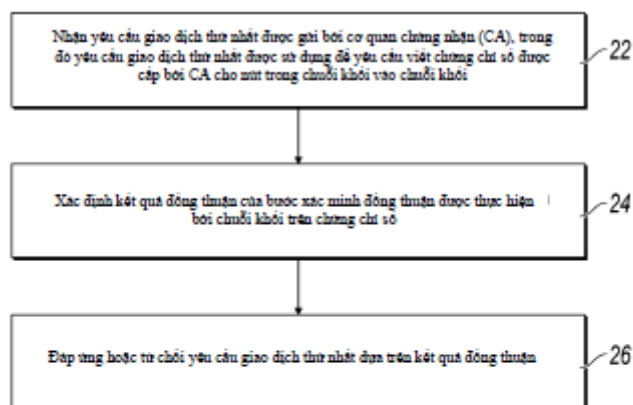


FIG. 2

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến công nghệ chuỗi khối, và cụ thể là phương pháp, thiết bị và hệ thống quản lý chứng chỉ số.

Tình trạng kỹ thuật của sáng chế

Công nghệ chuỗi khối còn được gọi là công nghệ sổ cái phân tán và là công nghệ cơ sở dữ liệu phân tán phi tập trung. Công nghệ chuỗi khối được đặc trưng bởi tính phi tập trung, tính minh bạch, chống giả mạo và tính tin cậy. Mỗi phần dữ liệu trong chuỗi khối có thể được phát đến các nút chuỗi khối trong toàn bộ mạng. Như vậy, mỗi nút có dữ liệu đầy đủ, nhất quán.

Trên cơ sở tính phi tập trung, mỗi nút trong chuỗi khối có một cặp khóa tương ứng. Tính hợp lệ của khóa công khai trong cặp khóa được xác minh bởi cơ quan chứng nhận (CA). Theo Fig.1, CA cấp chứng chỉ số cho nút 2, để chứng tỏ rằng nút 2 có khóa công khai được liệt kê trong chứng chỉ số một cách hợp pháp. Ngoài ra, khi nút 2 khởi tạo giao dịch, CA có thể xác minh từ xa xem chứng chỉ số của nút 2 có hợp lệ hay không.

Tuy nhiên, quyền của chứng chỉ số của nút dễ bị thay đổi ngẫu nhiên khi CA bị xâm nhập hoặc khi CA hoạt động với ý đồ xấu. Do đó, tính bảo mật của toàn bộ chuỗi khối bị ảnh hưởng.

Bản chất kỹ thuật của sáng chế

Các phương án thực hiện của sáng chế đề xuất phương pháp, thiết bị và hệ thống quản lý chứng chỉ số để giải quyết vấn đề trong công nghệ đã có, trong đó quyền của chứng chỉ số của nút thường bị thay đổi ngẫu nhiên khi CA bị xâm nhập hoặc khi CA hoạt động với ý đồ xấu.

Một phương án thực hiện của sáng chế đề xuất phương pháp quản lý chứng chỉ số, bao gồm các bước sau đây: nhận yêu cầu giao dịch thứ nhất được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ nhất được sử dụng để yêu cầu viết chứng chỉ số được cấp bởi CA cho nút trong chuỗi khối vào chuỗi khối; xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ nhất dựa trên kết quả

đồng thuận này.

Tùy ý, bước xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số bao gồm các bước sau đây: xác định các kết quả xác minh của các nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số; xác định số lượng nút thứ nhất và/hoặc số lượng nút thứ hai trong các nút tham gia xác minh đồng thuận, trong đó nút thứ nhất là nút có kết quả xác minh là “xác minh đồng thuận thành công” và nút thứ hai là nút có kết quả xác minh là “xác minh đồng thuận thất bại”; và xác định kết quả đồng thuận dựa trên số lượng nút thứ nhất và/hoặc số lượng nút thứ hai.

Tùy ý, bước xác định các kết quả xác minh của các nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số bao gồm các bước sau đây: xác định thông báo được công bố bởi nút sau khi nút thực hiện xác minh đồng thuận trên chứng chỉ số, trong đó thông báo được sử dụng để phát yêu cầu giao dịch và kết quả xác minh của nút đến một nút khác; và xác định các kết quả xác minh của các nút tham gia xác minh đồng thuận dựa trên thông báo của mỗi nút.

Tùy ý, bước xác định kết quả đồng thuận dựa trên số lượng nút thứ nhất bao gồm việc xác định rằng xác minh đồng thuận trên chứng chỉ số thành công khi số lượng nút thứ nhất đạt đến ngưỡng định trước thứ nhất hoặc khi tỷ lệ của các nút thứ nhất trong các nút tham gia xác minh đồng thuận đạt đến ngưỡng định trước thứ hai.

Tùy ý, bước đáp ứng hoặc từ chối yêu cầu giao dịch thứ nhất dựa trên kết quả đồng thuận bao gồm các bước sau đây: đáp ứng yêu cầu giao dịch thứ nhất để viết chứng chỉ số vào chuỗi khối nếu kết quả đồng thuận là “xác minh đồng thuận thành công”; hoặc từ chối yêu cầu giao dịch thứ nhất nếu kết quả đồng thuận là “xác minh đồng thuận thất bại”.

Một phương án thực hiện của sáng chế đề xuất phương pháp quản lý chứng chỉ số, bao gồm các bước sau đây: nhận yêu cầu giao dịch thứ hai được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ hai được sử dụng để yêu cầu viết danh mục hủy bỏ chứng chỉ vào chuỗi khối, và danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ; xác định kết quả đồng thuận của bước xác

minh đồng thuận được thực hiện bởi chuỗi khối trên danh mục hủy bỏ chứng chỉ; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ hai dựa trên kết quả đồng thuận này.

Tùy ý, phương pháp còn bao gồm các bước sau đây: xác minh yêu cầu giao dịch thứ ba trong chuỗi khối dựa trên danh mục hủy bỏ chứng chỉ, trong đó yêu cầu giao dịch thứ ba được sử dụng để yêu cầu hoàn thành giao dịch giữa nhóm nút thứ nhất và nhóm nút thứ hai; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ ba dựa trên kết quả xác minh.

Tùy ý, bước xác minh yêu cầu giao dịch thứ ba trong chuỗi khối dựa trên danh mục hủy bỏ chứng chỉ bao gồm các bước sau đây: so sánh chứng chỉ số của nút trong nhóm nút thứ nhất và nhóm nút thứ hai với chứng chỉ số đã bị hủy bỏ được ghi trong danh mục hủy bỏ chứng chỉ; và xác định kết quả xác minh dựa trên kết quả so sánh tham chiếu đến quy tắc giao dịch định trước của giao dịch.

Tùy ý, phương pháp còn bao gồm các bước sau đây: nhận yêu cầu giao dịch thứ tư được gửi bởi CA, trong đó yêu cầu giao dịch thứ tư được sử dụng để yêu cầu viết thông tin cập nhật của danh mục hủy bỏ chứng chỉ vào chuỗi khối; xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên thông tin cập nhật; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ tư dựa trên kết quả đồng thuận này.

Một phương án thực hiện của sáng chế đề xuất phương pháp quản lý chứng chỉ số, bao gồm các bước sau đây: nhận yêu cầu giao dịch thứ năm được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ năm được sử dụng để yêu cầu viết bản ghi của chứng chỉ số đã bị hủy bỏ bởi CA vào chuỗi khối; xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên bản ghi của chứng chỉ số đã bị hủy bỏ; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ năm dựa trên kết quả đồng thuận này.

Tùy ý, phương pháp còn bao gồm bước xây dựng danh mục hủy bỏ chứng chỉ dựa trên bản ghi của chứng chỉ số đã bị hủy bỏ được ghi vào chuỗi khối, trong đó danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ.

Một phương án thực hiện của sáng chế đề xuất phương pháp quản lý chứng chỉ

số, bao gồm các bước sau đây: nhận yêu cầu cấp được gửi bởi nút trong chuỗi khối, trong đó yêu cầu cấp được sử dụng để yêu cầu cơ quan chứng nhận (CA) cấp chứng chỉ số cho nút; cấp chứng chỉ số cho nút để phản hồi yêu cầu cấp; và gửi yêu cầu giao dịch thứ sáu đến chuỗi khối, trong đó yêu cầu giao dịch thứ sáu được sử dụng để yêu cầu viết chứng chỉ số vào chuỗi khối. Do đó, chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số và đáp ứng hoặc từ chối yêu cầu giao dịch thứ sáu dựa trên kết quả đồng thuận.

Một phương án thực hiện của sáng chế đề xuất thiết bị quản lý chứng chỉ số, bao gồm các bộ phận sau đây: bộ phận nhận, được tạo cấu hình để nhận yêu cầu giao dịch thứ nhất được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ nhất được sử dụng để yêu cầu viết chứng chỉ số được cấp bởi CA cho nút trong chuỗi khối vào chuỗi khối; bộ phận xác định, được tạo cấu hình để xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số; và bộ phận phản hồi, được tạo cấu hình để đáp ứng hoặc từ chối yêu cầu giao dịch thứ nhất dựa trên kết quả đồng thuận này.

Tùy ý, bộ phận xác định được tạo cấu hình để xác định các kết quả xác minh của các nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số; xác định số lượng nút thứ nhất và/hoặc số lượng nút thứ hai trong các nút tham gia xác minh đồng thuận, trong đó nút thứ nhất là nút có kết quả xác minh là “xác minh đồng thuận thành công” và nút thứ hai là nút có kết quả xác minh là “xác minh đồng thuận thất bại”; và xác định kết quả đồng thuận dựa trên số lượng nút thứ nhất và/hoặc số lượng nút thứ hai.

Một phương án thực hiện của sáng chế đề xuất thiết bị quản lý chứng chỉ số, bao gồm bộ nhớ và bộ xử lý, trong đó bộ nhớ được tạo cấu hình để lưu chương trình; và bộ xử lý được tạo cấu hình để thực thi chương trình được lưu trong bộ nhớ, và cụ thể là thực hiện các hoạt động sau đây: nhận yêu cầu giao dịch thứ nhất được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ nhất được sử dụng để yêu cầu viết chứng chỉ số được cấp bởi CA cho nút trong chuỗi khối vào chuỗi khối; xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ nhất dựa trên kết quả

đồng thuận này.

Một phương án thực hiện của sáng chế đề xuất thiết bị quản lý chứng chỉ số, bao gồm các bộ phận sau đây: bộ phận nhận, được tạo cấu hình để nhận yêu cầu giao dịch thứ hai được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ hai được sử dụng để yêu cầu viết danh mục hủy bỏ chứng chỉ vào chuỗi khối, và danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ; bộ phận xác định, được tạo cấu hình để xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên danh mục hủy bỏ chứng chỉ; và bộ phận phản hồi, được tạo cấu hình để đáp ứng hoặc từ chối yêu cầu giao dịch thứ hai dựa trên kết quả đồng thuận này.

Tùy ý, bộ phận phản hồi còn được tạo cấu hình để xác minh yêu cầu giao dịch thứ ba trong chuỗi khối dựa trên danh mục hủy bỏ chứng chỉ, trong đó yêu cầu giao dịch thứ ba được sử dụng để yêu cầu hoàn thành giao dịch giữa nhóm nút thứ nhất và nhóm nút thứ hai; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ ba dựa trên kết quả xác minh.

Tùy ý, bộ phận phản hồi còn được tạo cấu hình để so sánh chứng chỉ số của nút trong nhóm nút thứ nhất và nhóm nút thứ hai với chứng chỉ số đã bị hủy bỏ được ghi trong danh mục hủy bỏ chứng chỉ; và xác định kết quả xác minh dựa trên kết quả so sánh tham chiếu đến quy tắc giao dịch định trước của giao dịch.

Một phương án thực hiện của sáng chế đề xuất thiết bị quản lý chứng chỉ số, bao gồm các bộ phận sau đây: bộ phận nhận, được tạo cấu hình để nhận yêu cầu giao dịch thứ năm được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ năm được sử dụng để yêu cầu viết bản ghi của chứng chỉ số đã bị hủy bỏ bởi CA vào chuỗi khối; bộ phận xác định, được tạo cấu hình để xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên bản ghi của chứng chỉ số đã bị hủy bỏ; và bộ phận phản hồi, được tạo cấu hình để đáp ứng hoặc từ chối yêu cầu giao dịch thứ năm dựa trên kết quả đồng thuận.

Tùy ý, bộ phận phản hồi còn được tạo cấu hình để xây dựng danh mục hủy bỏ chứng chỉ dựa trên bản ghi của chứng chỉ số đã bị hủy bỏ được viết vào chuỗi khối,

trong đó danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ.

Một phương án thực hiện của sáng chế đề xuất thiết bị quản lý chứng chỉ số, bao gồm các bộ phận sau đây: bộ phận nhận, được tạo cấu hình để nhận yêu cầu cấp được gửi bởi nút trong chuỗi khối, trong đó yêu cầu cấp được sử dụng để yêu cầu cơ quan chứng nhận (CA) cấp chứng chỉ số cho nút; bộ phận phản hồi, được tạo cấu hình để cấp chứng chỉ số cho nút để phản hồi yêu cầu cấp; và bộ phận giao dịch, được tạo cấu hình để gửi yêu cầu giao dịch thứ sáu đến chuỗi khối, trong đó yêu cầu giao dịch thứ sáu được sử dụng để yêu cầu viết chứng chỉ số vào chuỗi khối. Do đó, chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số và đáp ứng hoặc từ chối yêu cầu giao dịch thứ sáu dựa trên kết quả đồng thuận.

Một phương án thực hiện của sáng chế đề xuất hệ thống quản lý chứng chỉ số, bao gồm ít nhất một thiết bị quản lý chứng chỉ số nêu trên.

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

Sau khi CA cấp chứng chỉ số và trước khi chứng chỉ số được xâu chuỗi, chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số, xác định tính hợp lệ của chứng chỉ số dựa trên kết quả xác minh, và cho phép/từ chối chứng chỉ số sẽ được xâu chuỗi. So với giải pháp trong công nghệ đã có sử dụng CA tập trung để cấp chứng chỉ và xâu chuỗi trực tiếp chứng chỉ, CA phi tập trung chỉ có thể cấp chứng chỉ và yêu cầu viết chứng chỉ số đã cấp vào chuỗi khối theo các phương án thực hiện của sáng chế. Nói cách khác, chứng chỉ số được cấp bởi CA là không hợp lệ trước khi được xâu chuỗi. Do đó, ngay cả khi CA bị lỗi (ví dụ, bị xâm nhập) và được sử dụng với ý đồ xấu để cấp ngẫu nhiên chứng chỉ số, tính bảo mật của chuỗi khối không bị ảnh hưởng do chứng chỉ số được cấp là không hợp lệ. Như vậy, theo các phương án thực hiện của sáng chế, khi CA bị lỗi, toàn bộ chuỗi khối có thể được ngăn chặn một cách hiệu quả khỏi rủi ro bảo mật lớn để cải thiện tính bảo mật của chuỗi khối.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo được mô tả sau đây nhằm mục đích cung cấp hiểu biết sâu hơn về sáng chế và cấu thành một phần của sáng chế. Các phương án minh họa

của sáng chế và phần mô tả các phương án này nhằm mục đích mô tả sáng chế và không tạo thành các giới hạn đối với sáng chế. Trên các hình vẽ kèm theo:

Fig.1 là sơ đồ giản lược minh họa quy trình hệ thống CA viết chứng chỉ số vào chuỗi khối trong công nghệ đã có;

Fig.2 là lưu đồ giản lược minh họa phương pháp quản lý chứng chỉ số, theo phương án thực hiện 1 của sáng chế;

Fig.3 là sơ đồ giản lược minh họa nguyên lý hệ thống CA viết chứng chỉ số vào chuỗi khối, theo một phương án thực hiện của sáng chế;

Fig.4 là lưu đồ giản lược minh họa bước xác minh đồng thuận trong phương pháp quản lý chứng chỉ số, theo phương án thực hiện 2 của sáng chế;

Fig.5 là lưu đồ giản lược minh họa phương pháp quản lý chứng chỉ số, theo phương án thực hiện 3 của sáng chế;

Fig.6 là sơ đồ giản lược minh họa nguyên lý hệ thống CA viết chứng chỉ số vào chuỗi khối, theo một phương án thực hiện của sáng chế;

Fig.7 là lưu đồ giản lược minh họa phương pháp quản lý chứng chỉ số, theo phương án thực hiện 4 của sáng chế;

Fig.8 là lưu đồ giản lược minh họa phương pháp quản lý chứng chỉ số, theo phương án thực hiện 5 của sáng chế;

Fig.9 là sơ đồ cấu trúc giản lược minh họa thiết bị quản lý chứng chỉ số, theo phương án thực hiện 6 của sáng chế;

Fig.10 là sơ đồ cấu trúc giản lược minh họa thiết bị điện tử, theo phương án thực hiện 7 của sáng chế;

Fig.11 là sơ đồ cấu trúc giản lược minh họa thiết bị quản lý chứng chỉ số, theo phương án thực hiện 8 của sáng chế;

Fig.12 là sơ đồ cấu trúc giản lược minh họa thiết bị điện tử, theo phương án thực hiện 9 của sáng chế;

Fig.13 là sơ đồ cấu trúc giản lược minh họa thiết bị quản lý chứng chỉ số, theo

phương án thực hiện 10 của sáng chế;

Fig.14 là sơ đồ cấu trúc giản lược minh họa thiết bị điện tử, theo phương án thực hiện 11 của sáng chế;

Fig.15 là sơ đồ cấu trúc giản lược minh họa thiết bị quản lý chứng chỉ số, theo phương án thực hiện 12 của sáng chế;

Fig.16 là sơ đồ cấu trúc giản lược minh họa thiết bị điện tử, theo phương án thực hiện 13 của sáng chế; và

Fig.17 là lưu đồ minh họa một ví dụ về phương pháp được thực hiện bằng máy tính để bảo đảm chứng chỉ số trong hệ thống quản lý chứng chỉ số, theo một phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Để làm rõ hơn các mục đích, các giải pháp kỹ thuật và các ưu điểm của sáng chế, phần dưới đây mô tả các giải pháp kỹ thuật của sáng chế dựa vào các phương án thực hiện của sáng chế và các hình vẽ đi kèm tương ứng. Rõ ràng, các phương án thực hiện được mô tả chỉ là một số chứ 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 trong lĩnh vực kỹ thuật này dựa trên các phương án thực hiện của sáng chế mà không cần đến nỗ lực sáng tạo sẽ nằm trong phạm vi bảo hộ của sáng chế.

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

Phương án thực hiện 1

Fig.2 là lưu đồ giản lược minh họa phương pháp quản lý chứng chỉ số, theo phương án thực hiện này của sáng chế. Theo Fig.2, phương pháp cụ thể bao gồm các bước sau đây.

Bước 22: Nhận yêu cầu giao dịch thứ nhất được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ nhất được sử dụng để yêu cầu viết chứng chỉ số được cấp bởi CA cho nút trong chuỗi khối vào chuỗi khối.

Ví dụ, theo Fig.3, nút 2 trong chuỗi khối xin CA chứng chỉ số. CA cấp chứng

chỉ số cho nút 2 và yêu cầu viết chứng chỉ số của nút 2 vào chuỗi khối bằng cách khởi tạo yêu cầu giao dịch thứ nhất.

Chứng chỉ số có thể bao gồm phiên bản, số seri, kiểu thuật toán chữ ký, thông tin bên cấp, thời hạn hiệu lực, bên cấp, khóa công khai được cấp, chữ ký số của CA, thông tin khác, v.v.

Bước 24: Xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số.

Theo Fig.3, sau khi nhận yêu cầu giao dịch, chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số của nút 2. Tiêu chuẩn xác minh có thể liên quan đến thông tin trong chứng chỉ số, ví dụ, thời hạn hiệu lực kết thúc hay chưa hoặc số seri có thỏa mãn yêu cầu hay không. Theo cách khác, bước xác minh có thể được thực hiện dựa trên tiêu chuẩn tùy chỉnh. Ví dụ, chuỗi ký tự tùy chỉnh A có thể được thêm vào chứng chỉ số. Bước xác minh thành công nếu nút phát hiện ra rằng chuỗi ký tự A tồn tại trong chứng chỉ số. Bước xác minh thất bại nếu chuỗi ký tự A không tồn tại trong chứng chỉ số.

Bước 26: Đáp ứng hoặc từ chối yêu cầu giao dịch thứ nhất dựa trên kết quả đồng thuận.

Không khó để hiểu rằng chuỗi khối đáp ứng yêu cầu giao dịch thứ nhất nếu kết quả đồng thuận là “xác minh đồng thuận thành công”, nói cách khác là xác định rằng chứng chỉ số là hợp lệ, và cho phép chứng chỉ số được viết vào chuỗi khối. Khi nút (ví dụ, nút 2 trên Fig.3) xin chứng chỉ khởi tạo giao dịch, chứng chỉ số của nút có thể được sử dụng bình thường. Chuỗi khối từ chối yêu cầu giao dịch thứ nhất nếu kết quả đồng thuận là “xác minh đồng thuận thất bại”, nói cách khác là coi chứng chỉ số được cấp bởi CA là không hợp lệ và từ chối chứng chỉ số sẽ được xâu chuỗi.

Có thể thấy rằng, theo phương án thực hiện này của sáng chế, sau khi CA cấp chứng chỉ số và trước khi chứng chỉ số được xâu chuỗi, chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số, xác định tính hợp lệ của chứng chỉ số dựa trên kết quả xác minh, và cho phép/từ chối chứng chỉ số sẽ được xâu chuỗi. So với giải pháp trong công nghệ đã có sử dụng CA tập trung để cấp chứng chỉ và xâu chuỗi trực tiếp chứng

chỉ, CA phi tập trung chỉ có thể cấp chứng chỉ và yêu cầu viết chứng chỉ số được cấp vào chuỗi khối theo phương án thực hiện này của sáng chế. Nói cách khác, chứng chỉ số được cấp bởi CA là không hợp lệ trước khi được xâu chuỗi. Do đó, ngay cả khi CA bị lỗi (ví dụ, bị xâm nhập) và được sử dụng với ý đồ xấu để cấp ngẫu nhiên chứng chỉ số, tính bảo mật của chuỗi khối không bị ảnh hưởng do chứng chỉ số được cấp là không hợp lệ. Như vậy, theo phương án này của sáng chế, khi CA bị lỗi, toàn bộ chuỗi khối có thể được ngăn chặn một cách hiệu quả khỏi rủi ro bảo mật lớn để cải thiện tính bảo mật của chuỗi khối.

Phương án thực hiện 2

Sự khác nhau giữa phương án thực hiện này và phương án thực hiện 1 là ở chỗ bước 24 bị giới hạn hơn nữa theo phương án này. Theo Fig.4, bước xác minh đồng thuận trong bước 24 cụ thể bao gồm các bước sau đây.

Bước 42: Xác định các kết quả xác minh của các nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số.

Ví dụ, theo Fig.4, sau khi CA gửi chứng chỉ số được cấp cho nút 2 đến chuỗi khối bằng cách sử dụng yêu cầu giao dịch thứ nhất, nút trong chuỗi khối xác minh chứng chỉ số này.

Có độ trễ mạng tương đối lớn trong mạng kết nối điểm-điểm và chuỗi các giao dịch được quan sát bởi các nút không thể nhất quán. Do đó, cơ chế đồng thuận cần phải được xác định trước để đạt được sự đồng thuận trên chuỗi các giao dịch xảy ra trên các nút.

Dựa trên cơ chế đồng thuận định trước, các nút trong chuỗi khối thực hiện xác minh đồng thuận liên tục trên chứng chỉ số. Mỗi nút phát một thông báo sau khi hoàn thành việc xác minh đồng thuận để thông báo cho một nút khác về kết quả xác minh của nút và yêu cầu giao dịch của CA. Sau đó, các kết quả xác minh của các nút tham gia xác minh đồng thuận được xác định dựa trên thông báo phát bởi mỗi nút. Ngoài ra, mỗi nút có thể ký chứng chỉ số khi xác minh chứng chỉ số để hoàn thành nhiều chữ ký và quy trình xác thực.

Cơ chế đồng thuận định trước có thể là bằng chứng về cơ chế làm việc, bằng

chứng về cơ chế cổ phần, v.v.

Bước 44: Xác định số lượng nút thứ nhất và/hoặc số lượng nút thứ hai trong các nút tham gia xác minh đồng thuận, trong đó nút thứ nhất là nút có kết quả xác minh là “xác minh đồng thuận thành công” và nút thứ hai là nút có kết quả xác minh là “xác minh đồng thuận thất bại”.

Không khó để hiểu rằng các nút tham gia xác minh đồng thuận được phân loại dựa trên các kết quả xác minh của các nút tham gia xác minh đồng thuận, để đếm số lượng nút thứ nhất và số lượng nút thứ hai.

Bước 46: Xác định kết quả đồng thuận dựa trên số lượng nút thứ nhất và/hoặc số lượng nút thứ hai.

Cần lưu ý rằng có nhiều phương pháp để xác định kết quả đồng thuận. Các ví dụ như sau:

Phương pháp 1: Xác định được rằng bước xác minh đồng thuận trên chứng chỉ số thành công khi số lượng nút thứ nhất đạt đến ngưỡng định trước thứ nhất.

Ngưỡng định trước thứ nhất có thể bằng tổng các nút trong chuỗi khối hoặc nhỏ hơn tổng các nút trong chuỗi khối và có thể được xác định cụ thể theo tình huống. Nếu ngưỡng định trước thứ nhất bằng tổng các nút, thì xác định được rằng bước xác minh đồng thuận trên chứng chỉ số thất bại khi số lượng nút thứ hai không bằng 0.

Phương pháp 2: Trước tiên, số lượng nút tham gia xác minh đồng thuận được đặt, ví dụ, là 600, nói cách khác, 600 nút trong chuỗi khối là các nút đầu tiên hoàn thành việc xác minh đồng thuận. Sau đó, tỷ lệ của các nút thứ nhất trong 600 nút được xác định trong thời gian thực. Xác định được rằng bước xác minh đồng thuận trên chứng chỉ số thành công khi tỷ lệ này đạt đến ngưỡng định trước thứ hai.

Phương pháp 3: Trước tiên, khoảng thời gian xác minh đồng thuận được đặt, ví dụ, là 2 giây. Sau đó, số lượng nút thứ nhất và các nút thứ hai hoàn thành việc xác minh đồng thuận trong vòng 2 giây được đếm, và sau đó tỷ lệ của các nút thứ nhất/các nút thứ hai được tính. Việc xác minh đồng thuận trên chứng chỉ số thành công hay không được xác định dựa trên tỷ lệ hoặc số lượng nút thứ nhất/các nút thứ hai.

Có thể thấy rằng, theo phương án thực hiện này của sáng chế, kết quả xác minh của mỗi nút được xác định dựa trên kết quả xác minh phát bởi nút sau khi hoàn thành việc xác minh đồng thuận để xác định kết quả đồng thuận đạt được. Hơn một nửa hoặc thậm chí tất cả các nút trong chuỗi khối tham gia vào và hoàn thành quá trình xác minh đồng thuận. Do đó, kết quả đồng thuận không bị ảnh hưởng trừ khi đa số hoặc thậm chí tất cả các nút bị xâm nhập cùng một lúc. Như vậy, tính bảo mật của chuỗi khối có thể được cải thiện hơn nữa theo phương án thực hiện này của sáng chế.

Phương án thực hiện 3

Fig.5 là lưu đồ giản lược minh họa phương pháp quản lý chứng chỉ số, theo phương án thực hiện 3 của sáng chế. Theo Fig.5, phương pháp cụ thể bao gồm các bước sau đây.

Bước 52: Nhận yêu cầu giao dịch thứ hai được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ hai được sử dụng để yêu cầu viết danh mục hủy bỏ chứng chỉ vào chuỗi khối và danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ.

Bước 54: Xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên danh mục hủy bỏ chứng chỉ.

Cần lưu ý rằng, theo Fig.6, trước khi danh mục hủy bỏ chứng chỉ được xâu chuỗi, chuỗi khối cần thực hiện bước xác minh đồng thuận trên danh mục hủy bỏ để ngăn việc danh mục hủy bỏ chứng chỉ được gửi từ CA là danh mục hủy bỏ chứng chỉ không chính xác được gửi bởi CA sau khi CA bị xâm nhập. Đối với phương pháp xác minh, tham khảo nội dung liên quan được ghi trong phương án thực hiện 1. Không khó để hiểu rằng tiêu chuẩn xác minh của chứng chỉ số có thể giống hoặc khác với tiêu chuẩn xác minh của danh mục hủy bỏ chứng chỉ. Phương pháp xác minh tùy chỉnh được sử dụng làm ví dụ. Hai tiêu chuẩn xác minh tương ứng có thể là chuỗi ký tự A mỗi chuỗi, hoặc có thể lần lượt là chuỗi ký tự A và chuỗi ký tự B. Điều này không bị giới hạn cụ thể ở đây.

Bước 56: Đáp ứng hoặc từ chối yêu cầu giao dịch thứ hai dựa trên kết quả đồng thuận.

Cần lưu ý rằng sau khi bước xác minh đồng thuận thành công, chuỗi khối có thể đồng bộ danh mục hủy bỏ chứng chỉ cho mỗi nút trong chuỗi khối bằng cách sử dụng mạng ngang hàng của chuỗi khối và thuật toán đồng thuận. Nói cách khác, chuỗi khối phát danh mục hủy bỏ chứng chỉ đến mỗi nút. Sau đó, nút có thể lưu danh mục hủy bỏ chứng chỉ trong sổ cái cục bộ.

Sau đó, khi yêu cầu giao dịch thứ ba xuất hiện trong chuỗi khối, chuỗi khối có thể xác minh yêu cầu giao dịch thứ ba trong chuỗi khối dựa trên danh mục hủy bỏ chứng chỉ trong sổ cái cục bộ để kiểm tra quyền của các chứng chỉ số của cả hai bên giao dịch, trong đó yêu cầu giao dịch thứ ba được sử dụng để yêu cầu hoàn thành giao dịch giữa nhóm nút thứ nhất và nhóm nút thứ hai; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ ba dựa trên kết quả xác minh.

Nhóm nút thứ nhất và nhóm nút thứ hai bao gồm ít nhất một nút mỗi nhóm. Ngoài ra, một nhóm nút là nhóm nút khởi tạo giao dịch và nhóm nút còn lại là nhóm nút nhận giao dịch.

Theo Fig.6, các sơ đồ xác minh dưới đây được mô tả bằng cách sử dụng ví dụ mà nút 2 là nút khởi tạo giao dịch và nút 1 là nút nhận giao dịch.

Sơ đồ 1: Khi nút 1 nhận giao dịch được khởi tạo bởi nút 2, nút 1 phân tích giao dịch để thu được chứng chỉ số của nút 2, sau đó tách danh mục hủy bỏ chứng chỉ ra từ sổ cái cục bộ và so sánh chứng chỉ số của nút 2 với mỗi chứng chỉ số đã bị hủy bỏ được ghi trong danh mục hủy bỏ chứng chỉ. Nếu chứng chỉ số của nút 2 thuộc danh mục hủy bỏ chứng chỉ, thì nút 1 xác định rằng chứng chỉ số của nút 2 không có quyền giao dịch liên quan và từ chối yêu cầu giao dịch được khởi tạo bởi nút 2. Nếu chứng chỉ số của nút 2 có quyền giao dịch liên quan, thì nút 1 đáp ứng yêu cầu giao dịch được khởi tạo bởi nút 2, để hoàn thành giao dịch giữa hai nút và xâu chuỗi giao dịch.

Sơ đồ 2: Nút 1 nhận giao dịch được khởi tạo bởi nút 2 và đáp ứng giao dịch sau khi học, thông qua so sánh, rằng bước xác minh trên chứng chỉ số của nút 2 thành công để phản hồi lại dữ liệu giao dịch. Nút 2 xác minh chứng chỉ số của nút 1 được mang trong dữ liệu giao dịch được phản hồi bởi nút 1; từ chối giao dịch nếu bước xác minh thất bại; hoặc hoàn thành giao dịch và xâu chuỗi giao dịch nếu bước xác minh thành

công.

Ngoài ra, trước khi khởi tạo giao dịch, nút 2 và nút 1 trước tiên có thể “bắt tay” để thu được các chứng chỉ số của mỗi nút, sau đó tách các danh mục hủy bỏ chứng chỉ ra từ các sổ cái cục bộ tương ứng của chúng và xác minh các chứng chỉ số của nhau. Nút 2 khởi tạo giao dịch nếu cả hai bước xác minh đều thành công.

Không khó để hiểu rằng các quy tắc giao dịch thay đổi theo các đặc điểm giao dịch. Do đó, có thể có nhiều loại xác minh tương ứng với các kết quả so sánh giữa chứng chỉ số trong danh mục hủy bỏ chứng chỉ và chứng chỉ số trong nhóm nút khởi tạo và nhóm nút nhận giao dịch. Ví dụ, loại giao dịch thứ nhất là như sau: Bộ khởi tạo giao dịch chỉ bao gồm nút A và bộ nhận giao dịch bao gồm nhiều nút. Quy tắc giao dịch có thể là tất cả các chứng chỉ số của các nút ở cả hai bên giao dịch cần phải có quyền giao dịch. Giao dịch có thể được thực hiện miễn là chứng chỉ số của nút A và chứng chỉ số của ít nhất một nút trong bộ nhận giao dịch có quyền giao dịch. Nút A có thể thực hiện giao dịch với nút có quyền giao dịch trong bộ nhận giao dịch.

Quy tắc giao dịch có thể được xác định dựa trên nhu cầu của người dùng và không bị giới hạn ở đây.

Giao dịch có thể bao gồm thông tin chuyển tài sản. Thông tin này bao gồm danh tính của người bán (người chuyển), danh tính của người mua (người nhận), các tài sản hoặc giá trị giao dịch, thời gian giao dịch và (hoặc) điều khoản hợp đồng tiềm năng.

Theo phương án thực hiện này, chứng chỉ đã bị hủy bỏ có thể thay đổi. Ví dụ, nếu một hoặc nhiều chứng chỉ số được thêm vào, CA sử dụng thông tin liên quan của chứng chỉ số đã bị hủy bỏ được thêm vào làm thông tin cập nhật và công bố thông tin cập nhật cho chuỗi khối ở dạng yêu cầu giao dịch thứ tư, để yêu cầu viết thông tin cập nhật cho danh mục hủy bỏ chứng chỉ vào chuỗi khối. Sau đó, nút trong chuỗi khối thực hiện xác minh đồng thuận trên thông tin cập nhật cho kết quả đồng thuận. Sau đó, nút đáp ứng yêu cầu giao dịch thứ tư dựa trên kết quả đồng thuận và viết thông tin cập nhật vào chuỗi khối; hoặc từ chối yêu cầu giao dịch thứ tư dựa trên kết quả đồng thuận.

Ngoài ra, đối với quy trình xác minh, tham khảo nội dung liên quan được ghi

trong phương án thực hiện trước đó. Chi tiết không được mô tả lại ở đây.

Nút trong chuỗi khối thêm chứng chỉ số đã bị hủy bỏ mới được thêm vào trong danh mục hủy bỏ chứng chỉ.

Có thể thấy rằng, theo phương án thực hiện này, danh mục hủy bỏ chứng chỉ được công bố cho chuỗi khối, để khi nhận yêu cầu giao dịch, nút đọc trực tiếp danh mục hủy bỏ chứng chỉ từ sổ cái cục bộ và xác minh xem chứng chỉ số của nút khởi tạo giao dịch có phải là chứng chỉ số đã bị hủy bỏ không. So với giải pháp kỹ thuật trong công nghệ đã có mà nút gửi chứng chỉ số của nút khởi tạo giao dịch đến CA, và CA xác minh quyền của chứng chỉ số dựa trên danh mục hủy bỏ đã lưu, và gửi lại kết quả xác minh cho nút, không cần phải yêu cầu từ xa dịch vụ xác minh của CA theo phương án này của sáng chế. Như vậy, chi phí xác minh chứng chỉ số có thể được giảm một cách hiệu quả và hiệu quả giao dịch có thể được cải thiện.

Ngoài ra, theo phương án thực hiện này của sáng chế, nút trong chuỗi khối thực hiện xác minh đồng thuận và ký danh mục hủy bỏ chứng chỉ trước khi danh mục hủy bỏ chứng chỉ được xâu chuỗi, để xác minh tính hợp lệ của danh mục hủy bỏ chứng chỉ, do đó tránh được việc danh mục hủy bỏ chứng chỉ không chính xác được gửi bởi CA sau khi CA bị xâm nhập. Ngoài ra, danh mục hủy bỏ chứng chỉ được lưu trong sổ cái cục bộ. Do đó, ngay cả khi CA bị xâm nhập, vấn đề sau đây trong giải pháp kỹ thuật đã có sẽ không xảy ra: Danh mục hủy bỏ chứng chỉ được sửa đổi ngẫu nhiên do CA bị xâm nhập; do đó, quyền của chứng chỉ số của nút bị hủy bỏ ngẫu nhiên, và theo đó, các giao dịch không thể được thực hiện bình thường hoặc thậm chí tính bảo mật của toàn bộ chuỗi khối bị ảnh hưởng.

Phương án thực hiện 4

Fig.7 là lưu đồ giản lược minh họa phương pháp quản lý chứng chỉ số, theo phương án thực hiện 4 của sáng chế. Theo Fig.7, phương pháp bao gồm các bước sau đây:

72. Nhận yêu cầu giao dịch thứ năm được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ năm được sử dụng để yêu cầu viết bản ghi của chứng chỉ số đã bị hủy bỏ bởi CA vào chuỗi khối.

74. Xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên bản ghi của chứng chỉ số đã bị hủy bỏ.

76. Đáp ứng hoặc từ chối yêu cầu giao dịch thứ năm dựa trên kết quả đồng thuận.

Chuỗi khối từ chối yêu cầu giao dịch thứ năm nếu bước xác minh đồng thuận trên bản ghi thất bại. Chuỗi khối đáp ứng yêu cầu giao dịch thứ năm nếu bước xác minh đồng thuận trên bản ghi thành công và xây dựng danh mục hủy bỏ chứng chỉ dựa trên bản ghi của chứng chỉ số đã bị hủy bỏ được viết vào chuỗi khối. Danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ.

Sau đó, bản ghi được viết liên tục vào chuỗi khối được sử dụng làm dữ liệu cập nhật để cập nhật danh mục hủy bỏ chứng chỉ.

Không khó để hiểu rằng bản ghi được phát đến mỗi nút sau khi được viết vào chuỗi khối. Do đó, mỗi nút xây dựng danh mục hủy bỏ chứng chỉ trong sổ cái cục bộ.

Cần lưu ý rằng phương án thực hiện này tương tự phương án thực hiện 3. Do đó, đối với phương pháp xác minh bản ghi, việc xác minh được thực hiện theo quyền của chứng chỉ số của nút tham gia giao dịch bằng cách sử dụng danh mục hủy bỏ chứng chỉ, v.v., tham khảo các bản ghi liên quan trong phương án thực hiện 3.

Có thể thấy rằng theo phương án này, CA chỉ có thể cấp chứng chỉ, hủy bỏ chứng chỉ, v.v., và xây dựng, lưu và duy trì danh mục hủy bỏ chứng chỉ được hoàn thành bởi các nút trong chuỗi khối. Do đó, khi nhận yêu cầu giao dịch, nút có thể đọc trực tiếp danh mục hủy bỏ chứng chỉ từ sổ cái cục bộ và xác minh chứng chỉ số của nút khởi tạo giao dịch có phải là chứng chỉ số đã bị hủy bỏ hay không. So với giải pháp kỹ thuật trong công nghệ đã có mà nút gửi chứng chỉ số của nút khởi tạo giao dịch đến CA, và CA xác minh quyền của chứng chỉ số dựa trên danh mục hủy bỏ đã lưu, và gửi lại kết quả xác minh cho nút, không cần yêu cầu từ xa dịch vụ xác minh của CA theo phương án thực hiện này của sáng chế. Như vậy, chi phí xác minh chứng chỉ số có thể được giảm một cách hiệu quả và hiệu quả giao dịch có thể được cải thiện.

Phương án thực hiện 5

Fig.8 là lưu đồ giản lược minh họa phương pháp quản lý chứng chỉ số, theo phương án thực hiện 5 của sáng chế. Theo Fig.8, phương án thực hiện này được thực thi bởi CA, và phương pháp cụ thể bao gồm các bước sau đây:

82. Nhận yêu cầu cấp được gửi bởi nút trong chuỗi khối, trong đó yêu cầu cấp được sử dụng để yêu cầu cơ quan chứng nhận (CA) cấp chứng chỉ số cho nút.

84. Cấp chứng chỉ số cho nút để phản hồi yêu cầu cấp.

86. Gửi yêu cầu giao dịch thứ sáu đến chuỗi khối, trong đó yêu cầu giao dịch thứ sáu được sử dụng để yêu cầu viết chứng chỉ số vào chuỗi khối, để chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số và đáp ứng hoặc từ chối yêu cầu giao dịch thứ sáu dựa trên kết quả đồng thuận.

Theo Fig.3, ví dụ, nút 2 gửi yêu cầu cấp chứng chỉ đến CA. Yêu cầu này bao gồm thông tin liên quan của nút 2, ví dụ, ký hiệu nhận dạng của nút 2. CA sau đó xác minh thông tin liên quan của nút 2, cấp chứng chỉ số cho nút 2 nếu bước xác minh thành công và khởi tạo yêu cầu để viết chứng chỉ số của nút 2 vào chuỗi khối.

Do phương án thực hiện này và các phương án thực hiện trước đó tương ứng với nhau, nên một số bước không được mô tả chi tiết lại. Để biết chi tiết, tham khảo các phần tương ứng trong các phương án thực hiện trước đó.

Có thể thấy rằng, theo phương án thực hiện này của sáng chế, sau khi cấp chứng chỉ số cho nút, CA yêu cầu chuỗi khối xâu chuỗi chứng chỉ số. Chuỗi khối xác minh tính hợp lệ của chứng chỉ số và xác định xem có xâu chuỗi chứng chỉ số hay không. So với giải pháp trong công nghệ đã có mà CA cấp chứng chỉ số cho nút và trực tiếp viết chứng chỉ số vào chuỗi khối để xâu chuỗi, CA theo phương án thực hiện này của sáng chế không thể thực hiện quản lý chứng chỉ số tập trung, lưu chứng chỉ số và xâu chuỗi chứng chỉ số, mà chỉ có thể cấp chứng chỉ số. Như vậy, nguy cơ CA bị xâm nhập có thể được giảm xuống và độ ổn định và tính bảo mật của CA có thể được cải thiện.

Để phân mô tả ngắn gọn, các phương án thực hiện trước đó được thể hiện dưới dạng kết hợp của một loạt các hành động. Tuy nhiên, người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cần hiểu rằng các phương án thực hiện của sáng chế không

bị giới hạn ở chuỗi hành động được mô tả do một số bước có thể được thực hiện theo các trình tự khác hoặc được thực hiện đồng thời theo các phương án thực hiện của sáng chế. Ngoài ra, người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cũng cần hiểu rằng tất cả các phương án thực hiện được mô tả trong bản mô tả là các ví dụ của các phương án thực hiện, và các hành động được đề cập không nhất thiết là bắt buộc đối với các phương án thực hiện này của sáng chế.

Phương án thực hiện 6

Fig.9 là sơ đồ cấu trúc giản lược minh họa thiết bị quản lý chứng chỉ số, theo phương án thực hiện 6 của sáng chế. Theo Fig.9, thiết bị này bao gồm bộ phận nhận 91, bộ phận xác định 92 và bộ phận phản hồi 93.

Bộ phận nhận 91 được tạo cấu hình để nhận yêu cầu giao dịch thứ nhất được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ nhất được sử dụng để yêu cầu viết chứng chỉ số được cấp bởi CA cho nút trong chuỗi khối vào chuỗi khối.

Bộ phận xác định 92 được tạo cấu hình để xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số.

Bộ phận phản hồi 93 được tạo cấu hình để đáp ứng hoặc từ chối yêu cầu giao dịch thứ nhất dựa trên kết quả đồng thuận.

Theo Fig.3, ví dụ, nút 2 gửi yêu cầu cấp chứng chỉ đến CA. CA đáp ứng yêu cầu của nút 2, cấp chứng chỉ số cho nút 2, và yêu cầu, ở dạng giao dịch, xâu chuỗi chứng chỉ số đã được cấp. Bộ phận nhận 91 nhận yêu cầu giao dịch được gửi bởi CA, và chuyển tiếp yêu cầu giao dịch này đến bộ phận xác định 92. Bộ phận xác định 92 xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số, để xác định tính hợp lệ của chứng chỉ số. Sau đó, bộ phận xác định 92 gửi kết quả đồng thuận được xác định đến bộ phận phản hồi 93. Bộ phận phản hồi 93 phân tích kết quả đồng thuận; và đáp ứng yêu cầu giao dịch của CA và cho phép xâu chuỗi chứng chỉ số nếu biết rằng, thông qua sự phân tích, kết quả đồng thuận là “xác minh thành công”; hoặc từ chối yêu cầu giao dịch của CA và từ chối xâu chuỗi chứng chỉ số nếu biết rằng, thông qua sự phân tích, kết quả đồng thuận là “xác minh

thất bại”.

Theo phương án thực hiện này, quy tắc xác minh đồng thuận của bộ phận xác định 92 bao gồm:

Kết quả xác minh của các nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số được xác định. Tốt hơn là, thông báo được công bố bởi nút sau khi nút thực hiện xác minh đồng thuận trên chứng chỉ số được xác định. Thông báo được sử dụng để phát yêu cầu giao dịch và kết quả xác minh của nút đến một nút khác. Kết quả xác minh của tất cả các nút tham gia xác minh đồng thuận được xác định dựa trên thông báo của mỗi nút.

Số lượng nút thứ nhất trong tất cả các nút tham gia xác minh đồng thuận được xác định. Nút thứ nhất là nút có kết quả xác minh là “xác minh đồng thuận thành công”.

Kết quả đồng thuận được xác định dựa trên số lượng nút thứ nhất. Tốt hơn là, xác định được rằng bước xác minh đồng thuận trên chứng chỉ số thành công khi số lượng nút thứ nhất đạt đến ngưỡng định trước thứ nhất hoặc khi tỷ lệ của các nút thứ nhất trong tất cả các nút tham gia xác minh đồng thuận đạt đến ngưỡng định trước thứ hai.

Có thể thấy rằng, theo phương án thực hiện này của sáng chế, sau khi CA cấp chứng chỉ số và trước khi chứng chỉ số được xâu chuỗi, chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số, xác định tính hợp lệ của chứng chỉ số dựa trên kết quả xác minh này và cho phép/từ chối xâu chuỗi chứng chỉ số. So với giải pháp trong công nghệ đã có sử dụng CA tập trung để cấp chứng chỉ và trực tiếp xâu chuỗi chứng chỉ, CA phi tập trung chỉ có thể cấp chứng chỉ và yêu cầu viết chứng chỉ số đã được cấp vào chuỗi khối theo phương án thực hiện này của sáng chế. Nói cách khác, chứng chỉ số được cấp bởi CA là không hợp lệ trước khi được xâu chuỗi. Do đó, ngay cả khi CA bị lỗi (ví dụ, bị xâm nhập) và được sử dụng với ý đồ xấu để cấp ngẫu nhiên chứng chỉ số, thì tính bảo mật của chuỗi khối không bị ảnh hưởng vì chứng chỉ số đã được cấp là không hợp lệ. Như vậy, theo phương án thực hiện này của sáng chế, khi CA bị lỗi, toàn bộ chuỗi khối có thể được ngăn chặn một cách hiệu quả khỏi rủi ro bảo mật lớn để cải

thiện tính bảo mật của chuỗi khối.

Phương án thực hiện 7

Fig.10 là sơ đồ cấu trúc giản lược minh họa thiết bị điện tử, theo phương án thực hiện 7 của sáng chế. Theo Fig.10, từ góc độ phần cứng, thiết bị điện tử bao gồm bộ xử lý, bus nội bộ, giao diện mạng, bộ nhớ và bộ nhớ không khả biến, và chắc chắn có thể còn bao gồm phần cứng được yêu cầu bởi một dịch vụ khác. Bộ xử lý đọc chương trình máy tính tương ứng từ bộ nhớ không khả biến đến bộ nhớ, và sau đó chạy chương trình máy tính để tạo ra thiết bị quản lý chứng chỉ số ở mức logic. Chắc chắn là, ngoài phương án thực hiện về phần cứng, sáng chế không loại trừ một phương án thực hiện khác, ví dụ, thiết bị logic hoặc sự kết hợp của phần cứng và phần mềm. Nói cách khác, khối thực thi của quy trình xử lý sau đây không bị giới hạn ở các bộ phận logic và cũng có thể là phần cứng hoặc thiết bị logic.

Giao diện mạng, bộ xử lý và bộ nhớ có thể được liên kết bằng cách sử dụng hệ thống bus. Bus có thể là bus cấu trúc chuẩn công nghiệp (Industry Standard Architecture, ISA), bus liên kết thiết bị ngoại vi (Peripheral Component Interconnect, PCI), bus cấu trúc chuẩn công nghiệp mở rộng (Extended Industry Standard Architecture, EISA), v.v.. Bus có thể được phân loại thành bus địa chỉ, bus dữ liệu, bus điều khiển, v.v.. Để dễ biểu thị, trên Fig.10, bus được biểu thị bằng cách chỉ sử dụng một mũi tên hai đầu. Tuy nhiên, điều đó không có nghĩa là chỉ có một bus hoặc chỉ có một loại bus.

Bộ nhớ được tạo cấu hình để lưu chương trình. Cụ thể, chương trình có thể bao gồm mã chương trình và mã chương trình bao gồm lệnh vận hành máy tính. Bộ nhớ có thể bao gồm bộ nhớ chỉ đọc và bộ nhớ truy cập ngẫu nhiên, và cung cấp lệnh và dữ liệu cho bộ xử lý. Bộ nhớ có thể bao gồm bộ nhớ truy cập ngẫu nhiên tốc độ cao (RAM) và cũng có thể bao gồm bộ nhớ không khả biến như ít nhất một bộ nhớ đĩa từ.

Bộ xử lý được tạo cấu hình để thực thi chương trình được lưu trong bộ nhớ và cụ thể thực hiện các hoạt động sau đây: nhận yêu cầu giao dịch thứ nhất được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ nhất được sử dụng để yêu cầu viết chứng chỉ số được cấp bởi CA cho nút trong chuỗi khối vào chuỗi khối; xác

định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ nhất dựa trên kết quả đồng thuận.

Phương pháp trước đó được thực hiện bởi thiết bị quản lý chứng chỉ số hoặc nút chính (Master) và được bộc lộ trong các phương án thực hiện được thể hiện trên Fig.2, Fig.4 và Fig.9 của sáng chế có thể được áp dụng cho bộ xử lý hoặc được thực hiện bởi bộ xử lý. Bộ xử lý có thể là vi mạch tích hợp và có khả năng xử lý tín hiệu. Trong quá trình thực hiện, các bước trong các phương pháp trước đó có thể được thực hiện bằng cách sử dụng mạch logic tích hợp của phần cứng trong bộ xử lý hoặc bằng cách sử dụng các lệnh ở dạng phần mềm. Bộ xử lý có thể là bộ xử lý đa dụng, 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 một thiết bị logic lập trình được khác, cổng rời hoặc thiết bị logic tranzito, hoặc linh kiện phần cứng rời; và có thể triển khai hoặc thực hiện các phương pháp, các bước và các sơ đồ khối logic được bộc lộ trong các phương án thực hiện của sáng chế. Bộ xử lý đa dụng có thể là bộ vi xử lý hoặc bộ xử lý này có thể là bộ xử lý thông thường bất kỳ, v.v.. Các bước của các phương pháp được bộc lộ liên quan đến các phương án thực hiện của sáng chế có thể được thực thi và hoàn thành trực tiếp bằng cách sử dụng bộ xử lý giải mã phần cứng hoặc sự kết hợp của các môđun phần cứng và phần mềm trong bộ xử lý giải mã. Môđun phần mềm có thể được đặt trong vật ghi hoàn thiện trong lĩnh vực kỹ thuật, như bộ nhớ truy cập ngẫu nhiên, bộ nhớ nhanh, bộ nhớ chỉ đọc, bộ nhớ chỉ đọc lập trình được, bộ nhớ lập trình được và xóa được bằng điện hoặc thanh ghi. Vật ghi được đặt trong bộ nhớ và bộ xử lý đọc thông tin trong bộ nhớ và hoàn thành các bước của các phương pháp trước đó kết hợp với phần cứng của bộ xử lý.

Thiết bị quản lý chứng chỉ số có thể còn thực hiện phương pháp trên Fig.2 và triển khai phương pháp được thực hiện bởi nút chính.

Phương án thực hiện 8

Fig.11 là sơ đồ cấu trúc giản lược minh họa thiết bị quản lý chứng chỉ số, theo

phương án thực hiện 8 của sáng chế. Theo Fig.11, thiết bị này bao gồm bộ phận nhận 111, bộ phận xác định 112 và bộ phận phản hồi 113.

Bộ phận nhận 111 được tạo cấu hình để nhận yêu cầu giao dịch thứ hai được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ hai được sử dụng để yêu cầu viết danh mục hủy bỏ chứng chỉ vào chuỗi khối và danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ.

Bộ phận xác định 112 được tạo cấu hình để xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên danh mục hủy bỏ chứng chỉ.

Bộ phận phản hồi 113 được tạo cấu hình để đáp ứng hoặc từ chối yêu cầu giao dịch thứ hai dựa trên kết quả đồng thuận.

Cần lưu ý rằng, sau khi hệ thống chuỗi khối-CA hiện thời được nâng cấp, CA công bố danh mục hủy bỏ chứng chỉ được duy trì hiện thời cho chuỗi khối. Bước xác minh đồng thuận được thực hiện trên danh mục hủy bỏ chứng chỉ sau khi bộ phận nhận 111 nhận danh mục hủy bỏ chứng chỉ. Bộ phận xác định 112 xác định kết quả đồng thuận và gửi kết quả đồng thuận đến bộ phận phản hồi 113. Bộ phận phản hồi 113 cho phép xâu chuỗi nếu bộ phận phản hồi 113 biết được rằng bước xác minh thành công hoặc từ chối xâu chuỗi nếu bước xác minh thất bại.

Ngoài ra, việc xâu chuỗi có thể lưu cụ thể danh mục chứng chỉ số trong sổ cái cục bộ của mỗi nút. Sau đó, khi nút nhận yêu cầu giao dịch thứ ba, bộ phận phản hồi 113 xác minh yêu cầu giao dịch thứ ba trên danh mục hủy bỏ chứng chỉ được lưu trong sổ cái cục bộ, và sau đó đáp ứng hoặc từ chối yêu cầu giao dịch thứ ba dựa trên kết quả xác minh. Yêu cầu giao dịch thứ ba được sử dụng để yêu cầu hoàn thành giao dịch giữa nhóm nút thứ nhất và nhóm nút thứ hai.

Theo phương án thực hiện này, nguyên lý làm việc của bộ phận phản hồi 113 là như sau:

Chứng chỉ số của nút trong nhóm nút thứ nhất và nhóm nút thứ hai được so sánh với chứng chỉ số đã bị hủy bỏ được ghi trong danh mục hủy bỏ chứng chỉ. Kết quả xác minh được xác định dựa trên kết quả so sánh dựa vào quy tắc giao dịch định

trước của giao dịch.

Theo phương án thực hiện này, thiết bị này còn bao gồm bộ phận cập nhật, được tạo cấu hình để nhận yêu cầu giao dịch thứ tư được gửi bởi CA, trong đó yêu cầu giao dịch thứ tư được sử dụng để yêu cầu viết thông tin cập nhật của danh mục hủy bỏ chứng chỉ vào chuỗi khối; xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên thông tin cập nhật; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ tư dựa trên kết quả đồng thuận.

Có thể thấy rằng theo phương án thực hiện này, danh mục hủy bỏ chứng chỉ được công bố cho chuỗi khối, để khi nhận giao dịch được khởi tạo bởi nút khởi tạo giao dịch, nút đọc trực tiếp danh mục hủy bỏ chứng chỉ từ sổ cái cục bộ và xác minh quyền của chứng chỉ số của nút khởi tạo giao dịch. Không cần gọi từ xa dịch vụ xác minh của CA. Như vậy, các chi phí xác minh có thể được giảm một cách hiệu quả và hiệu quả xác minh có thể được cải thiện. Ngoài ra, do danh mục hủy bỏ chứng chỉ được lưu trong sổ cái cục bộ, nên không có hậu quả nghiêm trọng xảy ra ngay cả khi CA bị xâm nhập.

Phương án thực hiện 9

Fig.12 là sơ đồ cấu trúc giản lược minh họa thiết bị điện tử, theo phương án thực hiện 9 của sáng chế. Theo Fig.12, thiết bị điện tử bao gồm bộ xử lý, bus nội bộ, giao diện mạng, bộ nhớ và bộ nhớ không khả biến, và chắc chắn có thể còn bao gồm phần cứng được yêu cầu bởi một dịch vụ khác. Bộ xử lý đọc chương trình máy tính tương ứng từ bộ nhớ không khả biến đến bộ nhớ, và sau đó chạy chương trình máy tính để tạo ra thiết bị quản lý chứng chỉ số ở mức logic. Chắc chắn, ngoài phương án thực hiện về phần cứng, sáng chế không loại trừ một phương án khác, ví dụ, thiết bị logic hoặc sự kết hợp của phần cứng và phần mềm. Nói cách khác, khối thực thi của quy trình xử lý sau đây không bị giới hạn ở các bộ phận logic và cũng có thể là phần cứng hoặc thiết bị logic.

Giao diện mạng, bộ xử lý và bộ nhớ có thể được liên kết bằng cách sử dụng hệ thống bus. Bus có thể là bus cấu trúc chuẩn công nghiệp (ISA), bus liên kết thiết bị ngoại vi (PCI), bus cấu trúc chuẩn công nghiệp mở rộng (EISA), v.v.. Bus có thể được

phân loại thành bus địa chỉ, bus dữ liệu, bus điều khiển, v.v.. Để dễ biểu thị, trên Fig.12, bus được biểu thị bằng cách chỉ sử dụng một mũi tên hai đầu. Tuy nhiên, điều đó không có nghĩa là chỉ có một bus hoặc chỉ có một loại bus.

Bộ nhớ được tạo cấu hình để lưu chương trình. Cụ thể, chương trình có thể bao gồm mã chương trình và mã chương trình bao gồm lệnh vận hành máy tính. Bộ nhớ có thể bao gồm bộ nhớ chỉ đọc và bộ nhớ truy cập ngẫu nhiên và cung cấp lệnh và dữ liệu cho bộ xử lý. Bộ nhớ có thể bao gồm bộ nhớ truy cập ngẫu nhiên tốc độ cao (RAM) và có thể còn bao gồm bộ nhớ không khả biến như ít nhất một bộ nhớ đĩa từ.

Bộ xử lý được tạo cấu hình để thực thi chương trình được lưu trong bộ nhớ và cụ thể là thực hiện các hoạt động sau đây: nhận yêu cầu giao dịch thứ hai được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ hai được sử dụng để yêu cầu viết danh mục hủy bỏ chứng chỉ vào chuỗi khối và danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ; xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên danh mục hủy bỏ chứng chỉ; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ hai dựa trên kết quả đồng thuận.

Phương pháp trước đó được thực hiện bởi thiết bị quản lý chứng chỉ số hoặc nút chính (Master) và được bộc lộ trong các phương án thực hiện được thể hiện trên Fig.5 và Fig.11 của sáng chế có thể được áp dụng cho bộ xử lý hoặc được thực hiện bởi bộ xử lý. Bộ xử lý có thể là vi mạch tích hợp và có khả năng xử lý tín hiệu. Trong quy trình thực hiện, các bước trong các phương pháp trước đó có thể được thực hiện bằng cách sử dụng mạch logic tích hợp của phần cứng trong bộ xử lý hoặc bằng cách sử dụng các lệnh ở dạng phần mềm. Bộ xử lý có thể là bộ xử lý đa dụng, 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 công lập trình được dạng trường (FPGA) hoặc một thiết bị logic lập trình được khác, cổng rời hoặc thiết bị logic tranzito, hoặc linh kiện phần cứng rời; và có thể triển khai hoặc thực hiện các phương pháp, các bước, và các sơ đồ khối logic được bộc lộ trong các phương án thực hiện của sáng chế. Bộ xử lý đa dụng có thể là bộ vi xử lý hoặc bộ xử lý có thể là bộ xử lý thông thường bất kỳ, v.v. Các bước của các phương pháp được bộc lộ liên quan đến các phương án thực hiện của sáng chế có thể được triển khai và hoàn thành trực tiếp bằng

cách sử dụng bộ xử lý giải mã phần cứng hoặc kết hợp của môđun phần cứng và phần mềm trong bộ xử lý giải mã. Môđun phần mềm có thể được đặt trong vật ghi hoàn thiện trong lĩnh vực kỹ thuật, như bộ nhớ truy cập ngẫu nhiên, bộ nhớ nhanh, bộ nhớ chỉ đọc, bộ nhớ chỉ đọc lập trình được, bộ nhớ lập trình được và xóa được bằng điện hoặc thanh ghi. Vật ghi được đặt trong bộ nhớ và bộ xử lý đọc thông tin trong bộ nhớ và hoàn thành các bước của các phương pháp trước đó kết hợp với phần cứng của bộ xử lý.

Thiết bị quản lý chứng chỉ số có thể còn thực hiện phương pháp trên Fig.5 và triển khai phương pháp được thực hiện bởi nút chính.

Phương án thực hiện 10

Fig.13 là sơ đồ cấu trúc giản lược minh họa thiết bị quản lý chứng chỉ số, theo phương án thực hiện 10 của sáng chế. Theo Fig.13, thiết bị này bao gồm bộ phận nhận 131, bộ phận xác định 132 và bộ phận phản hồi 133.

Bộ phận nhận 131 được tạo cấu hình để nhận yêu cầu giao dịch thứ năm được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ năm được sử dụng để yêu cầu viết bản ghi của chứng chỉ số đã bị hủy bỏ bởi CA vào chuỗi khối.

Bộ phận xác định 132 được tạo cấu hình để xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên bản ghi của chứng chỉ số đã bị hủy bỏ.

Bộ phận phản hồi 133 được tạo cấu hình để đáp ứng hoặc từ chối yêu cầu giao dịch thứ năm dựa trên kết quả đồng thuận.

Cần lưu ý rằng, sự khác biệt so với phương án thực hiện 8 là phương án thực hiện này có thể áp dụng được cho hệ thống CA tái cấu trúc. Trong hệ thống tái cấu trúc này, CA yêu cầu công bố bản ghi của chứng chỉ đã bị hủy bỏ thứ nhất cho chuỗi khối. Sau khi nhận yêu cầu của CA, bộ phận nhận 131 chuyển tiếp yêu cầu này đến bộ phận xác định 132. Bộ phận xác định 132 thực hiện xác minh đồng thuận trên bản ghi và gửi kết quả đồng thuận đến bộ phận phản hồi 133. Bộ phận phản hồi 133 cho phép xây chuỗi nếu bộ phận phản hồi 113 biết được rằng bước xác minh thành công hoặc từ chối xây chuỗi nếu bước xác minh thất bại.

Ngoài ra, không khó để hiểu rằng mỗi nút trong chuỗi khối xây dựng danh mục hủy bỏ chứng chỉ trong sổ cái cục bộ dựa trên bản ghi của chứng chỉ đã bị hủy bỏ thứ nhất để lưu thông tin về chứng chỉ số đã bị hủy bỏ, như số seri. Sau đó, các danh mục hủy bỏ chứng chỉ tương ứng được cập nhật và duy trì dựa trên các bản ghi được ghi vào chuỗi khối sau đó.

Cần lưu ý rằng, các bước như bước xác minh, dựa trên danh mục hủy bỏ chứng chỉ, quyền của chứng chỉ số của nút trong chuỗi khối mà tham gia vào giao dịch tương tự như các bước theo phương án thực hiện 8 hoặc các phương án thực hiện của phương pháp tương ứng. Do đó, chi tiết không được mô tả lại ở đây. Để biết chi tiết, tham khảo các bản ghi liên quan trong các phương án thực hiện tương ứng.

Có thể thấy rằng, theo phương án thực hiện này, CA công bố bản ghi của chứng chỉ số đã bị hủy bỏ đến chuỗi khối, để nút xây dựng danh mục hủy bỏ chứng chỉ. Sau đó, khi nhận giao dịch được khởi tạo bởi nút khởi tạo giao dịch, nút đọc trực tiếp danh mục hủy bỏ chứng chỉ từ sổ cái cục bộ và xác minh quyền của chứng chỉ số của nút khởi tạo giao dịch. Không cần gọi từ xa dịch vụ xác minh của CA. Như vậy, chi phí xác minh có thể được giảm một cách hiệu quả, và hiệu quả xác minh có thể được cải thiện. Ngoài ra, vì danh mục hủy bỏ chứng chỉ được lưu trong sổ cái cục bộ, không có hậu quả nghiêm trọng xảy ra ngay cả khi CA bị xâm nhập.

Phương án thực hiện 11

Fig.14 là sơ đồ cấu trúc giản lược minh họa thiết bị điện tử, theo phương án thực hiện 11 của sáng chế. Theo Fig.14, thiết bị điện tử bao gồm bộ xử lý, bus nội bộ, giao diện mạng, bộ nhớ và bộ nhớ không khả biến, và chắc chắn có thể còn bao gồm phần cứng được yêu cầu bởi một dịch vụ khác. Bộ xử lý đọc chương trình máy tính tương ứng từ bộ nhớ không khả biến đến bộ nhớ, và sau đó chạy chương trình máy tính để tạo ra thiết bị quản lý chứng chỉ số ở mức logic. Chắc chắn, ngoài phương án thực hiện về phần cứng, sáng chế không loại trừ một phương án thực hiện khác, ví dụ, thiết bị logic hoặc sự kết hợp của phần cứng và phần mềm. Nói cách khác, khối thực thi của quy trình xử lý sau đây không bị giới hạn ở các bộ phận logic và cũng có thể là phần cứng hoặc thiết bị logic.

Giao diện mạng, bộ xử lý và bộ nhớ có thể được liên kết bằng cách sử dụng hệ thống bus. Bus có thể là bus cấu trúc chuẩn công nghiệp (ISA), bus liên kết thiết bị ngoại vi (PCI), bus cấu trúc chuẩn công nghiệp mở rộng (EISA), v.v.. Bus có thể được phân loại thành bus địa chỉ, bus dữ liệu, bus điều khiển, v.v.. Để dễ biểu thị, trên Fig.14, bus được biểu thị bằng cách chỉ sử dụng một mũi tên hai đầu. Tuy nhiên, điều đó không có nghĩa là chỉ có một bus hoặc chỉ có một loại bus.

Bộ nhớ được tạo cấu hình để lưu chương trình. Cụ thể, chương trình có thể bao gồm mã chương trình và mã chương trình bao gồm lệnh vận hành máy tính. Bộ nhớ có thể bao gồm bộ nhớ chỉ đọc và bộ nhớ truy cập ngẫu nhiên, và cung cấp lệnh và dữ liệu cho bộ xử lý. Bộ nhớ có thể bao gồm bộ nhớ truy cập ngẫu nhiên tốc độ cao (RAM) và có thể còn bao gồm bộ nhớ không khả biến như ít nhất một bộ nhớ đĩa từ.

Bộ xử lý được tạo cấu hình để thực thi chương trình được lưu trong bộ nhớ, và cụ thể là thực hiện các hoạt động sau đây: nhận yêu cầu giao dịch thứ năm được gửi bởi cơ quan chứng nhận (CA), trong đó yêu cầu giao dịch thứ năm được sử dụng để yêu cầu viết bản ghi của chứng chỉ số đã bị hủy bỏ bởi CA vào chuỗi khối; xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên bản ghi của chứng chỉ số đã bị hủy bỏ; và đáp ứng hoặc từ chối yêu cầu giao dịch thứ năm dựa trên kết quả đồng thuận.

Phương pháp trước đó được thực hiện bởi thiết bị quản lý chứng chỉ số hoặc nút chính (Master) và được bộc lộ trong các phương án thực hiện được thể hiện trên Fig.7 và Fig.13 của sáng chế có thể được áp dụng cho bộ xử lý hoặc được thực hiện bởi bộ xử lý. Bộ xử lý có thể là vi mạch tích hợp và có khả năng xử lý tín hiệu. Trong quá trình thực hiện, các bước trong các phương pháp trước đó có thể được thực hiện bằng cách sử dụng mạch logic tích hợp của phần cứng trong bộ xử lý hoặc bằng cách sử dụng các lệnh ở dạng phần mềm. Bộ xử lý có thể là bộ xử lý đa dụng, 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 một thiết bị logic lập trình được khác, cổng rời hoặc thiết bị logic tranzito, hoặc linh kiện phần cứng rời; và có thể triển khai hoặc thực hiện các phương pháp, các bước và các sơ đồ khối logic được bộc lộ trong các phương án thực hiện của

sáng chế. Bộ xử lý đa dụng có thể là bộ vi xử lý hoặc bộ xử lý có thể là bộ xử lý thông thường bất kỳ, v.v.. Các bước của các phương pháp được bộc lộ liên quan đến các phương án thực hiện của sáng chế có thể được thực thi và hoàn thành trực tiếp bằng cách sử dụng bộ xử lý giải mã phần cứng hoặc sự kết hợp của môđun phần cứng và phần mềm trong bộ xử lý giải mã. Môđun phần mềm có thể được đặt trong vật ghi hoàn thiện trong lĩnh vực kỹ thuật, như bộ nhớ truy cập ngẫu nhiên, bộ nhớ nhanh, bộ nhớ chỉ đọc, bộ nhớ chỉ đọc lập trình được, bộ nhớ lập trình được và xóa được bằng điện hoặc thanh ghi. Vật ghi được đặt trong bộ nhớ và bộ xử lý đọc thông tin trong bộ nhớ và hoàn thành các bước của các phương pháp trước đó kết hợp với phần cứng của bộ xử lý.

Thiết bị quản lý chứng chỉ số cũng có thể thực hiện phương pháp trên Fig.7 và triển khai phương pháp được thực hiện bởi nút chính.

Phương án thực hiện 12

Fig.15 là sơ đồ cấu trúc giản lược minh họa thiết bị quản lý chứng chỉ số, theo phương án thực hiện 12 của sáng chế. Theo Fig.15, thiết bị này bao gồm bộ phận nhận 151, bộ phận phản hồi 152 và bộ phận giao dịch 153.

Bộ phận nhận 151 được tạo cấu hình để nhận yêu cầu cấp được gửi bởi nút trong chuỗi khối, trong đó yêu cầu cấp được sử dụng để yêu cầu cơ quan chứng nhận (CA) cấp chứng chỉ số cho nút.

Bộ phận phản hồi 152 được tạo cấu hình để cấp chứng chỉ số cho nút để phản hồi yêu cầu cấp.

Bộ phận giao dịch 153 được tạo cấu hình để gửi yêu cầu giao dịch thứ sáu đến chuỗi khối, trong đó yêu cầu giao dịch thứ sáu được sử dụng để yêu cầu viết chứng chỉ số vào chuỗi khối. Do đó, chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số và đáp ứng hoặc từ chối yêu cầu giao dịch thứ sáu dựa trên kết quả đồng thuận.

Cần lưu ý rằng, sau khi nhận yêu cầu cấp chứng chỉ số được gửi bởi nút, bộ phận nhận 151 gửi yêu cầu đến bộ phận phản hồi 152. Bộ phận phản hồi 152 đáp ứng yêu cầu và yêu cầu xâu chuỗi chứng chỉ số đã được cấp.

Có thể thấy rằng, theo phương án thực hiện này của sáng chế, sau khi cấp chứng chỉ số cho nút, CA yêu cầu chuỗi khối xâu chuỗi chứng chỉ số. Chuỗi khối xác minh tính hợp lệ của chứng chỉ số và xác định có xâu chuỗi chứng chỉ số hay không. So với giải pháp trong công nghệ đã có mà CA cấp chứng chỉ số cho nút và trực tiếp viết chứng chỉ số vào chuỗi khối để xâu chuỗi, CA theo phương án thực hiện này của sáng chế không thể thực hiện việc quản lý chứng chỉ số tập trung, lưu chứng chỉ số và xâu chuỗi chứng chỉ số, mà chỉ có thể cấp chứng chỉ số. Như vậy, nguy cơ CA bị xâm nhập có thể được giảm xuống và sự ổn định và tính bảo mật của CA có thể được cải thiện.

Phương án thực hiện 13

Fig.16 là sơ đồ cấu trúc giản lược minh họa thiết bị điện tử, theo phương án thực hiện 13 của sáng chế. Theo Fig.16, thiết bị điện tử bao gồm bộ xử lý, bus nội bộ, giao diện mạng, bộ nhớ và bộ nhớ không khả biến, và chắc chắn có thể còn bao gồm phần cứng được yêu cầu bởi một dịch vụ khác. Bộ xử lý đọc chương trình máy tính tương ứng từ bộ nhớ không khả biến đến bộ nhớ và sau đó chạy chương trình máy tính để tạo ra thiết bị quản lý chứng chỉ số ở mức logic. Chắc chắn, ngoài phương án thực hiện về phần cứng, sáng chế không loại trừ một phương án thực hiện khác, ví dụ, thiết bị logic hoặc sự kết hợp của phần cứng và phần mềm. Nói cách khác, khối thực thi của quy trình xử lý sau đây không bị giới hạn ở các bộ phận logic và cũng có thể là phần cứng hoặc thiết bị logic.

Giao diện mạng, bộ xử lý và bộ nhớ có thể được liên kết bằng cách sử dụng hệ thống bus. Bus có thể là bus cấu trúc chuẩn công nghiệp (ISA), bus liên kết thiết bị ngoại vi (PCI), bus cấu trúc chuẩn công nghiệp mở rộng (EISA), v.v.. Bus có thể được phân loại thành bus địa chỉ, bus dữ liệu, bus điều khiển, v.v.. Để dễ biểu thị, trên Fig.16, bus được biểu thị bằng cách chỉ sử dụng một mũi tên hai đầu. Tuy nhiên, điều đó không có nghĩa là chỉ có một bus hoặc chỉ có một loại bus.

Bộ nhớ được tạo cấu hình để lưu chương trình. Cụ thể, chương trình có thể bao gồm mã chương trình và mã chương trình bao gồm lệnh vận hành máy tính. Bộ nhớ có thể bao gồm bộ nhớ chỉ đọc và bộ nhớ truy cập ngẫu nhiên, và cung cấp lệnh và dữ

liệu cho bộ xử lý. Bộ nhớ có thể bao gồm bộ nhớ truy cập ngẫu nhiên tốc độ cao (RAM) và có thể còn bao gồm bộ nhớ không khả biến như ít nhất một bộ nhớ đĩa từ.

Bộ xử lý được tạo cấu hình để thực thi chương trình được lưu trong bộ nhớ, và cụ thể thực hiện các hoạt động sau đây: nhận yêu cầu cấp được gửi bởi nút trong chuỗi khối, trong đó yêu cầu cấp được sử dụng để yêu cầu cơ quan chứng nhận (CA) cấp chứng chỉ số cho nút; cấp chứng chỉ số cho nút để phản hồi yêu cầu cấp; và gửi yêu cầu giao dịch thứ sáu đến chuỗi khối, trong đó yêu cầu giao dịch thứ sáu được sử dụng để yêu cầu viết chứng chỉ số vào chuỗi khối. Do đó, chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số và đáp ứng hoặc từ chối yêu cầu giao dịch thứ sáu dựa trên kết quả đồng thuận.

Phương pháp trước đó được thực hiện bởi thiết bị quản lý chứng chỉ số hoặc nút chính (Master) và được bộc lộ trong các phương án thực hiện được thể hiện trên Fig.8 và Fig.15 của sáng chế có thể được áp dụng cho bộ xử lý hoặc được thực hiện bởi bộ xử lý. Bộ xử lý có thể là vi mạch tích hợp và có khả năng xử lý tín hiệu. Trong quá trình thực hiện, các bước trong các phương pháp trước đó có thể được thực hiện bằng cách sử dụng mạch logic tích hợp của phần cứng trong bộ xử lý hoặc bằng cách sử dụng các lệnh ở dạng phần mềm. Bộ xử lý có thể là bộ xử lý đa dụng, 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 một thiết bị logic lập trình được khác, cổng rời hoặc thiết bị logic tranzito, hoặc linh kiện phần cứng rời; và có thể triển khai hoặc thực hiện các phương pháp, các bước và các sơ đồ khối logic được bộc lộ trong các phương án thực hiện của sáng chế. Bộ xử lý đa dụng có thể là bộ vi xử lý hoặc bộ xử lý có thể là bộ xử lý thông thường bất kỳ, v.v. Các bước của các phương pháp được bộc lộ liên quan đến các phương án thực hiện của sáng chế có thể được thực thi và hoàn thành trực tiếp bằng cách sử dụng bộ xử lý giải mã phần cứng hoặc sự kết hợp của môđun phần cứng và phần mềm trong bộ xử lý giải mã. Môđun phần mềm có thể được đặt trong vật ghi hoàn thiện trong lĩnh vực kỹ thuật, như bộ nhớ truy cập ngẫu nhiên, bộ nhớ nhanh, bộ nhớ chỉ đọc, bộ nhớ chỉ đọc lập trình được, bộ nhớ lập trình được và xóa được bằng điện hoặc thanh ghi. Vật ghi được đặt trong bộ nhớ và bộ xử lý đọc thông tin trong bộ

nhớ và hoàn thành các bước của các phương pháp trước đó kết hợp với phần cứng của bộ xử lý.

Thiết bị quản lý chứng chỉ số có thể còn thực hiện phương pháp trên Fig.8 và triển khai phương pháp được thực hiện bởi nút chính.

Phương án thực hiện về thiết bị về cơ bản là tương tự với phương án thực hiện về phương pháp, và do đó được mô tả ngắn gọn. Đối với các phần liên quan, tham khảo các phần mô tả từng phần trong phương án thực hiện về phương pháp.

Cần lưu ý rằng, trong các bộ phận của thiết bị theo sáng chế, các bộ phận được phân chia logic dựa trên các chức năng được thực hiện. Tuy nhiên, sáng chế không bị giới hạn ở điều này và các bộ phận có thể được phân chia hoặc kết hợp khi cần thiết.

Phương án thực hiện 14

Dựa trên sáng chế tương tự, phương án thực hiện này của sáng chế còn đề xuất vật ghi đọc được bằng máy tính. Vật ghi đọc được bằng máy tính lưu một hoặc nhiều chương trình. Khi một hoặc nhiều chương trình này được thực thi bởi thiết bị điện tử bao gồm nhiều chương trình ứng dụng, thiết bị điện tử này có thể thực hiện các phương pháp quản lý chứng chỉ số được đề xuất trong các phương án thực hiện 1, 3, 4 và 5.

Phương án thực hiện 15

Dựa trên sáng chế tương tự, phương án thực hiện này của sáng chế còn đề xuất hệ thống quản lý chứng chỉ số, bao gồm một hoặc nhiều thiết bị quản lý chứng chỉ số bất kỳ được đề xuất trong các ví dụ tương ứng với Fig.9, Fig.11, Fig.13 và Fig.15.

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

nhớ đĩa từ, CD-ROM, bộ nhớ quang, v.v.) bao gồm mã chương trình có thể sử dụng bằng 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 trên các phương án thực hiện của sáng chế. Cần hiểu rằng các lệnh chương trình máy tính có thể được sử dụng để thực hiện mỗi quy trình và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối và kết 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 cung cấp cho máy tính đa dụng, máy tính chuyên dụng, bộ xử lý nhúng hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được bất kỳ khác để tạo ra máy, sao cho các lệnh được thực thi bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được bất kỳ khác tạo ra thiết bị để thực hiện chức năng cụ thể theo 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 trong bộ nhớ đọc được bằng máy tính mà có thể ra lệnh cho máy tính hoặc thiết bị xử lý dữ liệu lập trình được bất kỳ khác làm việc theo cách cụ thể, sao cho các lệnh được lưu trong bộ nhớ đọc được bằng máy tính tạo ra thành phần lạ bao gồm thiết bị ra lệnh. Thiết bị ra lệnh thực hiện chức năng cụ thể theo 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 tải vào máy tính hoặc một thiết bị xử lý dữ liệu lập trình được khác, sao cho một loạt các hoạt động và các bước được thực hiện trên máy tính hoặc một thiết bị lập trình được khác, nhờ đó tạo ra quy trình xử lý được thực hiện bằng máy tính. Do đó, các lệnh được thực thi trên máy tính hoặc trên một thiết bị lập trình được khác cung cấp các bước để thực hiện chức năng cụ thể theo 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 máy tính bao gồm một hoặc nhiều bộ xử lý (CPU), giao diện đầu vào/ đầu ra, giao diện mạng và bộ nhớ.

Bộ nhớ có thể bao gồm bộ nhớ không bền vững, bộ nhớ truy cập ngẫu nhiên

(RAM), bộ nhớ không khả biến và/hoặc một dạng khác trong vật ghi đọc được bằng máy tính, ví dụ, bộ nhớ chỉ đọc (ROM) hoặc bộ nhớ nhanh (RAM nhanh). Bộ nhớ là một ví dụ của vật ghi đọc được bằng máy tính.

Vật ghi đọc được bằng máy tính bao gồm vật ghi bền vững, không bền vững, di động và không di động mà có thể lưu thông tin bằng cách sử dụng phương pháp hoặc công nghệ bất kỳ. Thông tin có thể là lệnh đọc được bằng máy tính, cấu trúc dữ liệu, mô đun chương trình hoặc dữ liệu khác. Các ví dụ của vật ghi máy tính bao gồm nhưng không giới hạn ở bộ nhớ truy cập ngẫu nhiên thông số (PRAM), bộ nhớ truy cập ngẫu nhiên tĩnh (SRAM), bộ nhớ truy cập ngẫu nhiên động (DRAM), một loại bộ nhớ truy cập ngẫu nhiên (RAM) khác, bộ nhớ chỉ đọc (ROM), bộ nhớ chỉ đọc lập trình được và xóa được bằng điện (EEPROM), bộ nhớ nhanh hoặc một công nghệ bộ nhớ khác, bộ nhớ chỉ đọc đĩa nén (CD-ROM), đĩa đa dụng kỹ thuật số (DVD) hoặc một bộ nhớ quang khác, hộp băng từ, bộ nhớ đĩa băng từ hoặc một thiết bị lưu từ khác hoặc vật ghi lâu dài bất kỳ khác, có thể được sử dụng để lưu thông tin mà có thể được truy cập bằng thiết bị máy tính. Dựa trên định nghĩa trong bản mô tả này, vật ghi đọc được bằng máy tính không bao gồm vật ghi tạm thời đọc được bằng máy tính (vật ghi tạm thời) như tín hiệu dữ liệu và sóng mang được điều biến.

Cần lưu ý rằng, thuật ngữ “bao gồm”, “chứa” hoặc biến thể bất kỳ khác của chúng nhằm bao hàm sự bao gồm không loại trừ, sao cho quy trình, phương pháp, hàng hóa hoặc thiết bị bao gồm một loạt các thành phần không chỉ bao gồm các thành phần đó mà còn bao gồm các thành phần khác không được liệt kê rõ ràng hoặc còn bao gồm các thành phần vốn có của quy trình, phương pháp, hàng hóa hoặc thiết bị đó. Thành phần được mô tả là “bao gồm...” còn bao gồm, không giới hạn thêm, thành phần tương đồng khác trong quy trình, phương pháp, hàng hóa hoặc thiết bị bao gồm thành phần đó.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cần hiểu rằng các phương án thực hiện của sáng chế có thể được đề xuất dưới dạng phương pháp, hệ thống hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng các dạng phương án thực hiện chỉ phần cứng, phương án thực hiện chỉ phần mềm hoặc các phương án thực hiện với sự kết hợp của phần mềm và phần cứng. Ngoài ra, sáng chế

có thể sử dụng dạng sản phẩm chương trình máy tính được triển khai trên một hoặc nhiều vật ghi sử dụng được bằng máy tính (bao gồm nhưng không bị giới hạn ở bộ nhớ đĩa từ, CD-ROM, bộ nhớ quang, v.v.) bao gồm mã chương trình sử dụng được bằng máy tính.

Các phương án thực hiện trước đó chỉ đơn thuần là các phương án thực hiện của sáng chế và không nhằm mục đích giới hạn sáng chế. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này có thể thực hiện các cải biến và thay đổi khác nhau đối với sáng chế. Các cải biến, thay thế tương đương hoặc sự cải tiến bất kỳ được thực hiện mà không nằm ngoài phạm vi của sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế.

Fig.17 là lưu đồ minh họa một ví dụ của phương pháp được thực hiện bằng máy tính 1700 để bảo đảm chứng chỉ số trong hệ thống quản lý chứng chỉ số, theo phương án thực hiện của sáng chế. Để trình bày rõ ràng, phần mô tả sau đây mô tả chung về phương pháp 1700 trong trường hợp của các hình vẽ khác trong phần mô tả này. Tuy nhiên, cần hiểu rằng phương pháp 1700 có thể được thực hiện, ví dụ, bằng hệ thống, môi trường, phần mềm và phần cứng bất kỳ, hoặc kết hợp của các hệ thống, môi trường, phần mềm và phần cứng, nếu phù hợp. Theo một số phương án thực hiện, các bước khác nhau của phương pháp 1700 có thể được chạy song song, kết hợp, theo vòng hoặc theo thứ tự bất kỳ.

Ở bước 1702, hệ thống quản lý chứng chỉ số nhận yêu cầu giao dịch bao gồm chứng chỉ số từ cơ quan chứng nhận tại nút trong mạng chuỗi khối, và yêu cầu giao dịch là yêu cầu viết chứng chỉ số vào chuỗi khối được liên kết với mạng chuỗi khối, và chứng chỉ số được cấp cho nút trong mạng chuỗi khối. Yêu cầu giao dịch từ cơ quan chứng nhận có thể bao gồm thông tin chuyển tài sản biểu thị yêu cầu giao dịch, như chứng chỉ số. Ví dụ, thông tin chuyển tài sản có thể bao gồm danh tính của người bán hoặc người chuyển, danh tính của người mua hoặc người nhận (ví dụ, được đặt tại nút nhận). Thông tin chuyển tài sản cũng có thể bao gồm các tài sản hoặc giá trị giao dịch biểu thị lượng thông tin giao dịch. Thời gian của giao dịch được yêu cầu và một hoặc nhiều khoản hợp đồng tiềm năng. Yêu cầu giao dịch có thể là thanh toán giữa hai bên hoặc yêu cầu thanh toán giữa hai bên, như hai tổ chức tài chính.

Theo một số phương án thực hiện, yêu cầu giao dịch có thể bao gồm chứng chỉ số. Chứng chỉ số có thể đảm bảo hai bên giao dịch là các bên đáng tin cậy. Ví dụ, chứng chỉ số có thể bao gồm số phiên bản, số seri, kiểu chữ ký, thông tin bên cấp, thời hạn hiệu lực, bên cấp, khóa công khai được cấp, chữ ký số của cơ quan chứng nhận và các thông tin khác liên quan đến yêu cầu giao dịch. Từ bước 1702, phương pháp 1700 chuyển sang bước 1704.

Ở bước 1704, hệ thống quản lý chứng chỉ số xác định kết quả xác minh đồng thuận cho yêu cầu giao dịch và kết quả xác minh đồng thuận được tạo ra bởi các nút trong mạng chuỗi khối. Theo một số phương án thực hiện, hệ thống quản lý chứng chỉ số dựa trên một hoặc nhiều tiêu chí để xác định bước xác minh đồng thuận. Ví dụ, một hoặc nhiều tiêu chí có thể bao gồm tiêu chuẩn xác minh bao gồm thông tin liên quan đến chứng chỉ số, như, ví dụ, thời hạn hiệu lực cho biết chứng chỉ số là hợp lệ trong bao lâu trước khi hết hiệu lực hoặc số seri tương ứng với chứng chỉ số có thỏa mãn yêu cầu giữa hai bên hay không.

Theo một số phương án thực hiện, mỗi nút trong mạng chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số một cách tuần tự. Ví dụ, trong mạng chuỗi khối, nút A thực hiện bước xác minh đồng thuận thứ nhất và sau đó phát thông báo tới một nút B khác về kết quả xác minh đồng thuận của nút A và yêu cầu giao dịch nhận được từ cơ quan chứng nhận. Quy trình này tiếp tục cho đến khi các nút từ B đến Z mỗi nút thực hiện xác minh đồng thuận trên yêu cầu giao dịch nhận được và mỗi nút biết mọi kết quả của các nút khác. Cuối cùng, sau khi mỗi nút thực hiện xác minh đồng thuận, mỗi nút này ký chứng chỉ số để xác minh với cơ quan chứng nhận rằng bước xác minh đồng thuận đã hoàn thành.

Theo một số phương án thực hiện, mỗi nút trong mạng chuỗi khối thực hiện xác minh đồng thuận. Cụ thể, nút, ví dụ nút A, phân tích yêu cầu giao dịch để thu được chứng chỉ số. Nếu chứng chỉ số không tồn tại, thì nút từ chối yêu cầu giao dịch từ cơ quan chứng nhận. Nếu chứng chỉ số tồn tại, thì nút tách sổ cái cục bộ từ bộ nhớ của nó. Sổ cái cục bộ duy trì bản ghi của mỗi trong số các giao dịch được thực hiện bởi nút và danh mục hủy bỏ chứng chỉ. Danh mục hủy bỏ chứng chỉ theo dõi các chứng chỉ bị từ chối truy cập bởi mỗi trong số các nút và cơ quan chứng nhận. Cụ thể, nút so sánh

chứng chỉ số đã được tách với mỗi chứng chỉ số trong danh mục hủy bỏ chứng chỉ. Nếu chứng chỉ số đã được tách khớp với chứng chỉ số trong danh mục hủy bỏ chứng chỉ, thì nút từ chối yêu cầu giao dịch. Nếu chứng chỉ số đã được tách không khớp với chứng chỉ số bất kỳ trong danh mục hủy bỏ chứng chỉ, thì nút hoàn thành giao dịch cho nút đó và phát thông báo về kết quả và yêu cầu giao dịch. Để phản hồi việc hoàn thành yêu cầu giao dịch, nút thêm yêu cầu giao dịch vào sổ cái cục bộ trong chuỗi khối. Theo các phương án thực hiện khác, giao dịch không hoàn thành cho đến khi mỗi nút trong mạng chuỗi khối thực hiện xác minh đồng thuận. Từ bước 1704, phương pháp 1700 chuyển sang bước 1706.

Ở bước 1706, hệ thống quản lý chứng chỉ số so sánh kết quả xác minh đồng thuận với giá trị ngưỡng định trước. Để phản hồi mỗi nút trong mạng chuỗi khối thực hiện xác minh đồng thuận, hệ thống quản lý chứng chỉ số so sánh kết quả của bước xác minh đồng thuận với giá trị ngưỡng định trước. Ví dụ, hệ thống quản lý chứng chỉ số phân tích số lượng nút tham gia xác minh đồng thuận có kết quả xác minh là thành công. Hệ thống quản lý chứng chỉ số cũng phân tích số lượng nút tham gia xác minh đồng thuận có kết quả xác minh là thất bại. Hệ thống quản lý chứng chỉ số so sánh số lượng nút mà kết quả xác minh đồng thuận thành công so với ngưỡng định trước. Nếu số lượng này lớn hơn ngưỡng định trước, thì hệ thống quản lý chứng chỉ số lưu chứng chỉ số này. Từ bước 1706, phương pháp 1700 chuyển sang bước 1708.

Ở bước 1708, để phản hồi việc hệ thống quản lý chứng chỉ số xác định kết quả xác minh đồng thuận lớn hơn hoặc bằng giá trị ngưỡng định trước, hệ thống quản lý chứng chỉ số lưu chứng chỉ số trong chuỗi khối được liên kết với mạng chuỗi khối. Cụ thể, hệ thống quản lý chứng chỉ số (mạng chuỗi khối của các nút) lưu chứng chỉ số và dữ liệu nhận dạng yêu cầu giao dịch từ cơ quan chứng nhận để phản hồi kết quả của bước xác minh đồng thuận từ hệ thống quản lý chứng chỉ số lớn hơn hoặc bằng với giá trị ngưỡng định trước. Hệ thống quản lý chứng chỉ số có thể lưu chứng chỉ số và dữ liệu nhận dạng yêu cầu giao dịch trong sổ cái cục bộ hoặc chuỗi khối của mạng chuỗi khối. Mỗi trong số các nút có thể truy cập nút riêng của nó để đọc và viết vào sổ cái cục bộ. Ngoài ra, mỗi nút cần có cùng sổ cái cục bộ hoặc chuỗi khối trong hệ thống quản lý cục bộ số hóa. Hệ thống quản lý chứng chỉ số ghi ngày và giờ thực thi yêu cầu

giao dịch. Hệ thống quản lý chứng chỉ số cung cấp chỉ dẫn cho cơ quan chứng nhận rằng giao dịch đã được thực thi. Sau bước 1708, phương pháp 1700 dừng lại.

Các dấu hiệu của sáng chế tìm cách loại bỏ các vấn đề với cơ quan chứng nhận bị lỗi. Ví dụ, bằng cách nhận yêu cầu giao dịch được gửi bởi cơ quan chứng nhận và yêu cầu giao dịch bao gồm dữ liệu giao dịch và chứng chỉ số để viết chứng chỉ số vào chuỗi khối trong mạng chuỗi khối; xác định bước xác minh đồng thuận được thực hiện bởi mạng chuỗi khối trên yêu cầu giao dịch và phản hồi việc xác định kết quả của bước xác minh đồng thuận lớn hơn ngưỡng định trước; viết chứng chỉ số vào chuỗi khối của mạng chuỗi khối và thực thi yêu cầu giao dịch từ cơ quan chứng nhận. Bằng cách thực hiện xác minh đồng thuận tại hệ thống quản lý chứng chỉ số, giao dịch có thể vẫn được thực thi ngay cả khi cơ quan chứng nhận bị lỗi, bị xâm nhập hoặc được sử dụng với ý đồ xấu để cấp ngẫu nhiên chứng chỉ số. Kết quả là, mạng chuỗi khối có thể loại bỏ rủi ro bảo mật lớn từ cơ quan chứng nhận bị lỗi để cải thiện tính bảo mật của chuỗi khối trong mạng chuỗi khối.

Các phương án và hoạt động được mô tả trong bản mô tả này có thể được triển khai trong mạch điện tử số hoặc trong phần mềm, phần sụn hoặc phần cứng của máy tính, bao gồm các kết cấu được bộc lộ trong bản mô tả này hoặc kết hợp của một hoặc nhiều trong số chúng. Các hoạt động có thể được triển khai dưới dạng các hoạt động được thực hiện bởi thiết bị xử lý dữ liệu trên dữ liệu được lưu 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 các thiết bị và các máy xử lý dữ liệu, gồm, ví dụ bộ xử lý lập trình được, máy tính, hệ thống trên chip hoặc nhiều thiết bị này hoặc kết hợp của các thiết bị trên. Thiết bị này 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 này cũng có thể bao gồm mã tạo ra môi trường thực thi cho chương trình máy tính được đề cập, ví dụ, mã tạo thành phần sụn của bộ xử lý, chồng giao thức, hệ thống quản lý cơ sở dữ liệu, hệ điều hành (ví dụ hệ điều hành hoặc kết hợp của các hệ điều hành), môi trường thời gian chạy đa nền tảng, máy ảo hoặc kết 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 được biết đến, ví dụ, là chương trình, phần mềm, ứng dụng phần mềm, môđun phần mềm, bộ phận phần mềm, tập lệnh hoặc mã) có thể được viết ở dạng ngôn ngữ lập trình bất kỳ, bao gồm các ngôn ngữ biên 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, đối tượng hoặc bộ phận khác phù hợp để sử dụng trong môi trường điện toán. Chương trình có thể được lưu trong một phần của tệp tin mà chứa chương trình hoặc dữ liệu khác (ví dụ, một hoặc nhiều tập lệnh được lưu trong tài liệu ngôn ngữ đánh dấu), trong một tệp tin chuyên dụng cho chương trình được đề cập hoặc trong các tệp tin nhiều tọa độ (ví dụ, các tệp tin lưu một hoặc nhiều môđun, các chương trình con hoặc các phần của mã). Chương trình máy tính có thể được thực thi trên một máy tính hoặc trên nhiều máy tính được đặt ở một vị trí hoặc được phân phối trên 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, ví dụ, cả bộ vi xử lý đa dụng và chuyên dụng và một hoặc nhiều bộ xử lý bất kỳ của loại máy tính kỹ thuật số bất kỳ. Nói chung, bộ xử lý sẽ nhận các lệnh và dữ liệu từ bộ nhớ chỉ đọc hoặc bộ nhớ truy cập ngẫu nhiên hoặc cả hai. Các thành phần chính của máy tính là bộ xử lý để thực hiện các hành động theo các lệnh và một hoặc nhiều thiết bị nhớ để lưu các lệnh và dữ liệu. Nói chung, máy tính cũng sẽ bao gồm hoặc được ghép nối theo cách hoạt động để nhận dữ liệu từ hoặc truyền dữ liệu tới, hoặc cả hai, một hoặc nhiều thiết bị lưu trữ lớn để lưu dữ liệu. Máy tính có thể được nhúng trong một 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 các lệnh chương trình máy tính và dữ liệu bao gồm bộ nhớ không khả biến, phương tiện và các thiết bị nhớ, bao gồm, ví dụ, các thiết bị nhớ bán dẫn, các đĩa từ và các đĩa quang từ. Bộ xử lý và bộ nhớ có thể được bổ sung 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), điện thoại di động (ví dụ, điện thoại thông minh), máy tính bảng, thiết bị đeo

được (ví dụ, đồng hồ thông minh và kính mắt thông minh), thiết bị cấy ghép bên trong cơ thể người (ví dụ, cảm biến sinh học, 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 không dây (ví dụ, sử dụng các tín hiệu 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 thời 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 độ ẩm, con quay hồi chuyển, la bàn, khí áp kế, cảm biến vân tay, hệ thống nhận dạng khuôn mặt, cảm biến RF (ví dụ, Wi-Fi và radio tế bào), cảm biến nhiệt hoặc các loại cảm biến khác. Ví dụ, camera có thể bao gồm camera lắp ở phía trước và phía sau với thấu kính tháo ra được hoặc cố định, đèn flash, cảm biến ảnh và bộ xử lý hình 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 thông tin xác thực được lưu 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 màn hình điốt phát quang hữu cơ (OLED)/màn hình thực tế ảo (VR)/màn hình thực tế tăng cường (AR) để hiển thị thông tin cho người dùng và màn hình chạm, bàn phím và thiết bị trở nhờ đó người dùng có thể cung cấp đầu vào cho máy tính. Các loại thiết bị khác có thể được sử dụng để tạo ra tương tác với người dùng; ví dụ, phản hồi được cung cấp cho người dùng có thể là dạng phản hồi cảm giác bất kỳ, ví dụ, phản hồi thị giác, phản hồi thính giác hoặc phản hồi xúc giác; và đầu vào từ người dùng có thể được nhận 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 khách của người dùng để phản hồi các yêu cầu nhận được từ trình duyệt web.

Các phương án có thể được triển khai sử dụng các thiết bị điện toán được kết nối với nhau bởi dạng hoặc môi trường bất kỳ truyền thông dữ liệu kỹ thuật số có dây hoặc không dây (hoặc kết 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 thường 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 là trong thời gian thực sao cho hành động và phản hồi gần nhau về mặt thời gian; ví dụ một cá nhân nhận thấy hành động hoặc phản hồi xảy ra về cơ bản là đồng thời, chênh lệch thời gian để phản hồi theo sau hành động của cá nhân đó là nhỏ hơn 1 mili giây (ms) hoặc nhỏ hơn 1 giây (s) hoặc phản hồi không có thời gian trễ chủ ý có tính đến các giới hạn xử lý của hệ thống.

Các ví dụ về các mạng truyền thông bao gồm mạng cục bộ (LAN), mạng truy cập radio (RAN), mạng khu vực đô thị (MAN) và mạng diện rộng (WAN). Mạng truyền thông có thể bao gồm tất cả hoặc một phần của Internet, một mạng truyền thông khác hoặc kết hợp của các mạng truyền thông. Thông tin 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 kết hợp của các giao thức này. Mạng truyền thông có thể truyền giọng nói, video, sinh trắc hoặc dữ liệu xác thực hoặc thông tin khác giữa các thiết bị điện toán đã kết nối.

Các dấu hiệu được mô tả dưới dạng các phương án thực hiện riêng biệt có thể được triển khai, ở dạng kết hợp, theo một phương án thực hiện, trong khi các dấu hiệu được mô tả là một phương án thực hiện có thể được triển khai theo nhiều phương án thực hiện, một cách riêng biệt hoặc ở dạng tổ hợp con phù hợp bất kỳ. Các hoạt động được mô tả và được bảo hộ theo thứ tự cụ thể không nên được hiểu là yêu cầu thứ tự cụ thể hoặc tất cả các hoạt động minh họa phải được thực hiện (một số hoạt động có thể là tùy ý). Khi thích hợp, có thể thực hiện xử lý đa nhiệm hoặc song song (hoặc kết hợp của xử lý đa nhiệm và song song).

YÊU CẦU BẢO HỘ

1. Phương pháp quản lý chứng chỉ số, phương pháp này bao gồm các bước:

nhận, tại chuỗi khối, yêu cầu giao dịch thứ nhất được gửi bởi cơ quan chứng nhận, trong đó yêu cầu giao dịch thứ nhất bao gồm yêu cầu viết chứng chỉ số được cấp bởi cơ quan chứng nhận cho nút trong chuỗi khối vào chuỗi khối;

xác định, bởi chuỗi khối, kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên chứng chỉ số, trong đó bước xác định kết quả đồng thuận bao gồm:

xác định kết quả xác minh của các nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số, trong đó i) nhiều hơn một nửa số nút trong chuỗi khối tham gia xác minh đồng thuận trên chứng chỉ số và ii) số lượng nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số bao gồm số lượng nút hoàn thành xác minh đồng thuận trên chứng chỉ số trong khoảng thời gian thiết lập của bước xác minh đồng thuận,

xác định số lượng nút thứ nhất và/hoặc số lượng nút thứ hai trong các nút tham gia xác minh đồng thuận, trong đó nút thứ nhất là nút có kết quả xác minh chỉ ra rằng bước xác minh đồng thuận đã thành công, và nút thứ hai là nút có kết quả xác minh chỉ ra rằng bước xác minh đồng thuận không thành công, và

xác định kết quả đồng thuận dựa trên số lượng nút thứ nhất và/hoặc số lượng nút thứ hai; và

đáp ứng hoặc từ chối, bởi chuỗi khối, yêu cầu giao dịch thứ nhất dựa trên kết quả đồng thuận.

2. Phương pháp theo điểm 1, trong đó bước xác định kết quả xác minh của các nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số bao gồm:

xác định, đối với mỗi nút, thông báo được công bố bởi nút sau khi nút này thực hiện xác minh đồng thuận trên chứng chỉ số, trong đó thông báo được sử dụng để phát yêu cầu giao dịch thứ nhất và kết quả xác minh của nút đến một nút khác; và

xác định kết quả xác minh của các nút tham gia xác minh đồng thuận dựa trên thông báo của mỗi nút.

3. Phương pháp theo điểm 1, trong đó bước xác định kết quả đồng thuận dựa trên số lượng nút thứ nhất bao gồm:

xác định rằng bước xác minh đồng thuận trên chứng chỉ số thành công khi số lượng nút thứ nhất đạt đến ngưỡng định trước thứ nhất hoặc khi tỷ lệ các nút thứ nhất trong các nút tham gia xác minh đồng thuận đạt đến ngưỡng định trước thứ hai.

4. Phương pháp theo điểm 1, trong đó bước đáp ứng hoặc từ chối yêu cầu giao dịch thứ nhất dựa trên kết quả đồng thuận bao gồm:

đáp ứng yêu cầu giao dịch thứ nhất để viết chứng chỉ số vào chuỗi khối nếu kết quả đồng thuận chỉ ra rằng bước xác minh đồng thuận đã thành công; hoặc từ chối yêu cầu giao dịch thứ nhất nếu kết quả đồng thuận chỉ ra rằng bước xác minh đồng thuận không thành công.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó phương pháp này còn bao gồm các bước:

nhận yêu cầu giao dịch thứ hai được gửi bởi cơ quan chứng nhận, trong đó yêu cầu giao dịch thứ hai bao gồm yêu cầu viết danh mục hủy bỏ chứng chỉ vào chuỗi khối và danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ;

xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên danh mục hủy bỏ chứng chỉ; và

đáp ứng hoặc từ chối yêu cầu giao dịch thứ hai dựa trên kết quả đồng thuận.

6. Phương pháp theo điểm 5, trong đó phương pháp này còn bao gồm các bước:

xác minh yêu cầu giao dịch thứ ba trong chuỗi khối dựa trên danh mục hủy bỏ chứng chỉ, trong đó yêu cầu giao dịch thứ ba được sử dụng để yêu cầu hoàn thành giao dịch giữa nhóm nút thứ nhất và nhóm nút thứ hai; và

đáp ứng hoặc từ chối yêu cầu giao dịch thứ ba dựa trên kết quả xác minh.

7. Phương pháp theo điểm 6, trong đó bước xác minh yêu cầu giao dịch thứ ba trong chuỗi khối dựa trên danh mục hủy bỏ chứng chỉ bao gồm:

so sánh chứng chỉ số của nút trong nhóm nút thứ nhất và nhóm nút thứ hai với chứng chỉ số đã bị hủy bỏ được ghi trong danh mục hủy bỏ chứng chỉ; và

xác định kết quả xác minh dựa trên kết quả so sánh có tham chiếu đến quy tắc giao dịch định trước của giao dịch.

8. Phương pháp theo điểm 5, trong đó phương pháp này còn bao gồm các bước:

nhận yêu cầu giao dịch thứ ba được gửi bởi cơ quan chứng nhận, trong đó yêu cầu giao dịch thứ ba được sử dụng để yêu cầu viết thông tin cập nhật của danh mục hủy bỏ chứng chỉ vào chuỗi khối;

xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên thông tin cập nhật; và

đáp ứng hoặc từ chối yêu cầu giao dịch thứ ba dựa trên kết quả đồng thuận.

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

nhận yêu cầu giao dịch thứ tư được gửi bởi cơ quan chứng nhận, trong đó yêu cầu giao dịch thứ tư bao gồm yêu cầu viết bản ghi của chứng chỉ số đã bị hủy bỏ bởi cơ quan chứng nhận vào chuỗi khối;

xác định kết quả đồng thuận của bước xác minh đồng thuận được thực hiện bởi chuỗi khối trên bản ghi của chứng chỉ số đã bị hủy bỏ; và

đáp ứng hoặc từ chối yêu cầu giao dịch thứ tư dựa trên kết quả đồng thuận.

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

xây dựng danh mục hủy bỏ chứng chỉ dựa trên bản ghi của chứng chỉ số đã bị hủy bỏ được viết vào chuỗi khối, trong đó danh mục hủy bỏ chứng chỉ được sử dụng để ghi chứng chỉ số đã bị hủy bỏ.

11. Phương pháp quản lý các chứng chỉ số, phương pháp này bao gồm các bước:

nhận, bởi cơ quan chứng nhận, yêu cầu cấp được gửi bởi nút trong chuỗi khối, trong đó yêu cầu cấp được sử dụng để yêu cầu cơ quan chứng nhận cấp chứng chỉ số cho nút;

cấp, bởi cơ quan chứng nhận, chứng chỉ số cho nút để phản hồi yêu cầu cấp; và gửi, từ cơ quan chứng nhận, yêu cầu giao dịch thứ nhất đến chuỗi khối, trong đó yêu cầu giao dịch thứ nhất bao gồm yêu cầu viết chứng chỉ số vào chuỗi khối, trong đó chuỗi khối thực hiện xác minh đồng thuận trên chứng chỉ số bằng cách:

xác định kết quả xác minh của các nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số, trong đó i) nhiều hơn một nửa số nút trong chuỗi khối tham gia xác minh đồng thuận trên chứng chỉ số và ii) số lượng nút trong chuỗi khối mà tham gia xác minh đồng thuận trên chứng chỉ số bao gồm số lượng nút hoàn thành xác minh đồng thuận trên chứng chỉ số trong khoảng thời gian thiết lập của bước xác minh đồng thuận,

xác định số lượng nút thứ nhất và/hoặc số lượng nút thứ hai trong các nút tham gia xác minh đồng thuận, trong đó nút thứ nhất là nút có kết quả xác minh chỉ ra rằng bước xác minh đồng thuận đã thành công và nút thứ hai là nút có kết quả xác minh chỉ ra rằng bước xác minh đồng thuận không thành công,

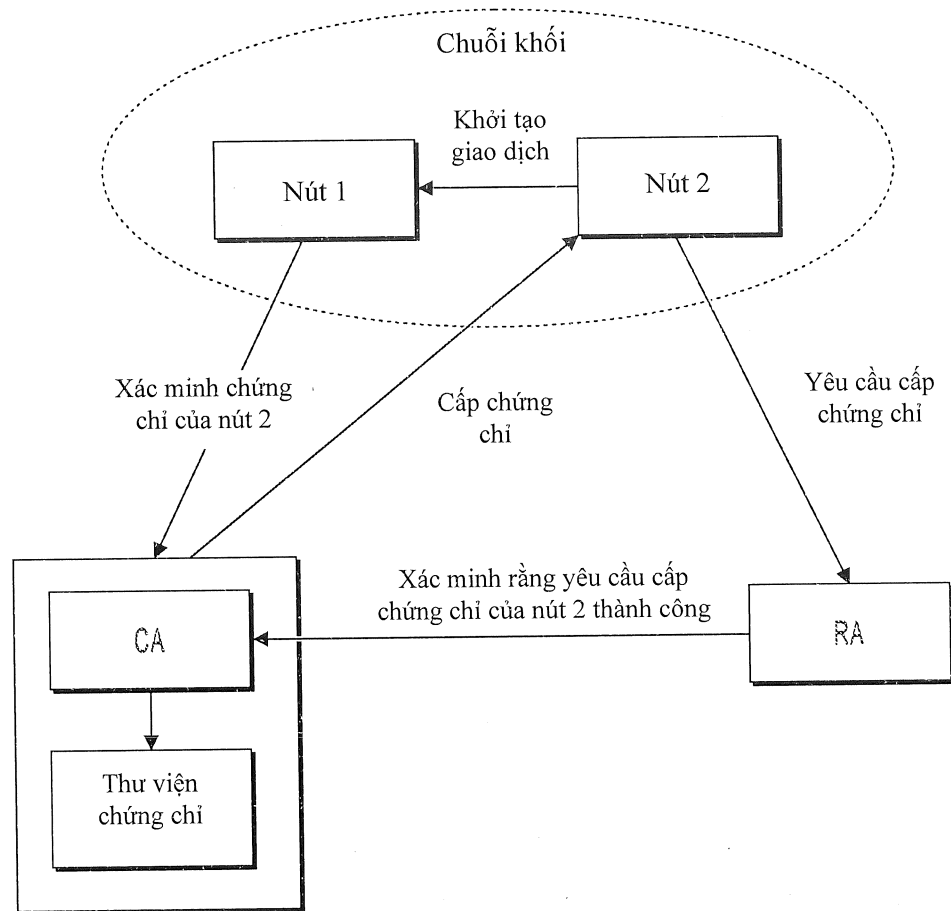
xác định kết quả đồng thuận dựa trên số lượng nút thứ nhất và/hoặc số lượng nút thứ hai; và

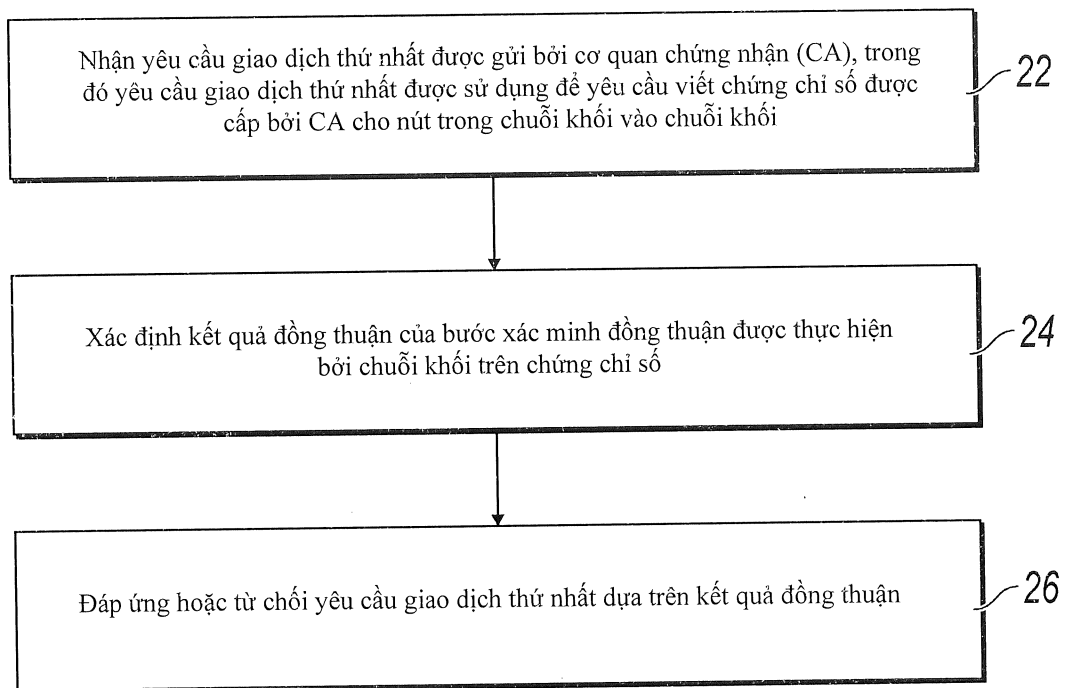
đáp ứng hoặc từ chối yêu cầu giao dịch thứ nhất dựa trên kết quả đồng thuận.

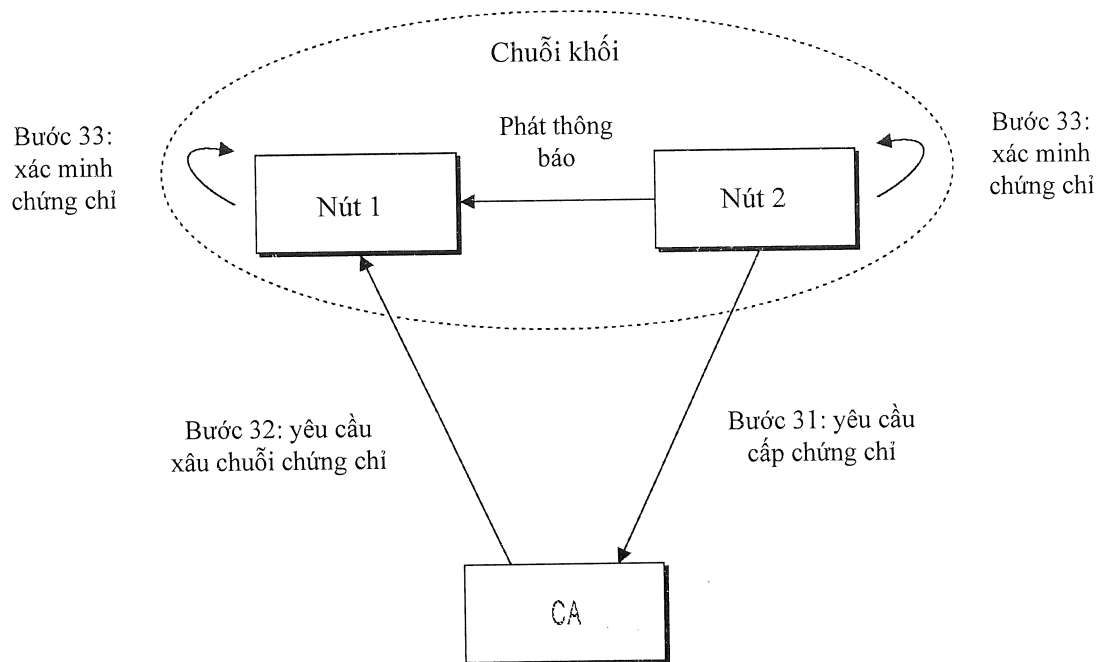
12. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 11, trong đó chứng chỉ số bao gồm ít nhất một trong số phiên bản, số seri, kiểu thuật toán chữ ký, thông tin bên cấp, thời hạn hiệu lực, bên cấp, khóa công khai được cấp và chữ ký số của cơ quan chứng nhận.

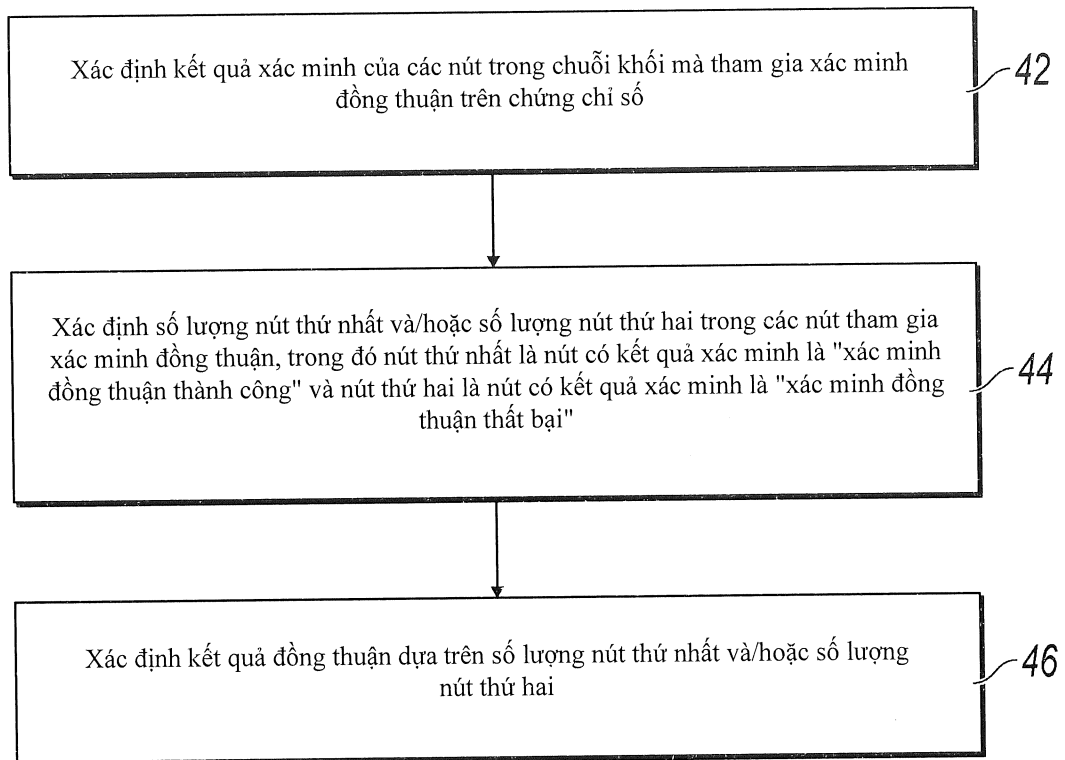
13. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 12, trong đó chứng chỉ số là không hợp lệ trước khi được xâu chuỗi trong nút của chuỗi khối.

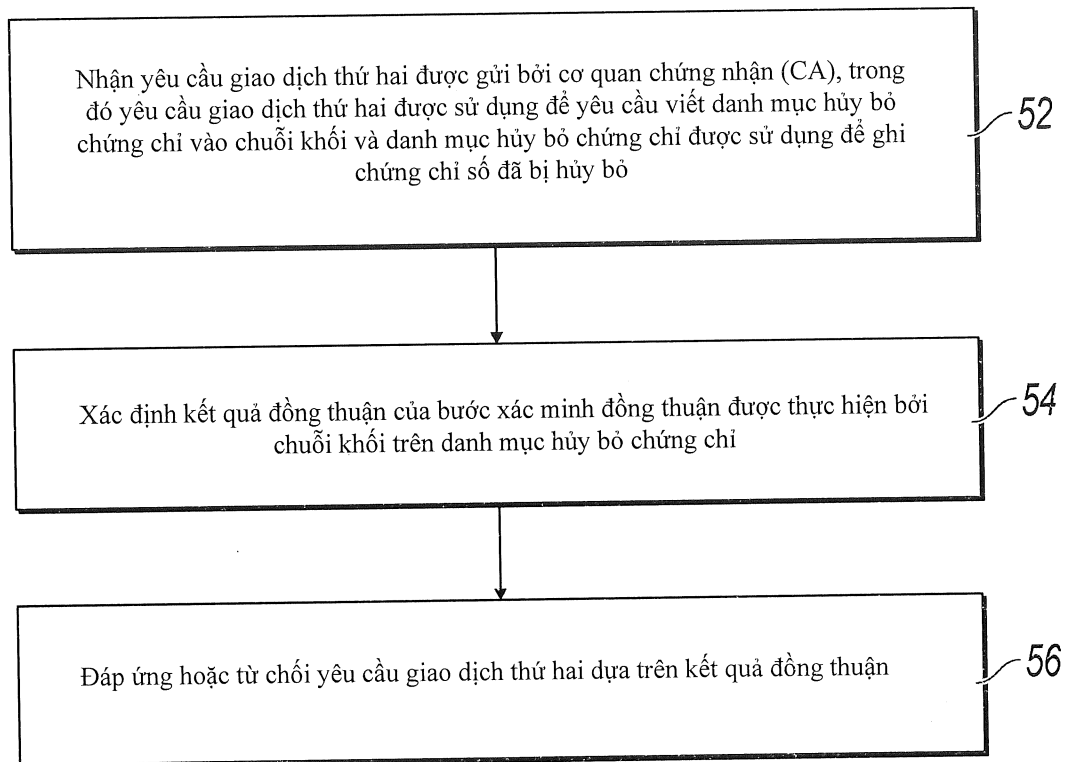
14. Thiết bị quản lý chứng chỉ số, thiết bị này bao gồm nhiều môđun được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 13.

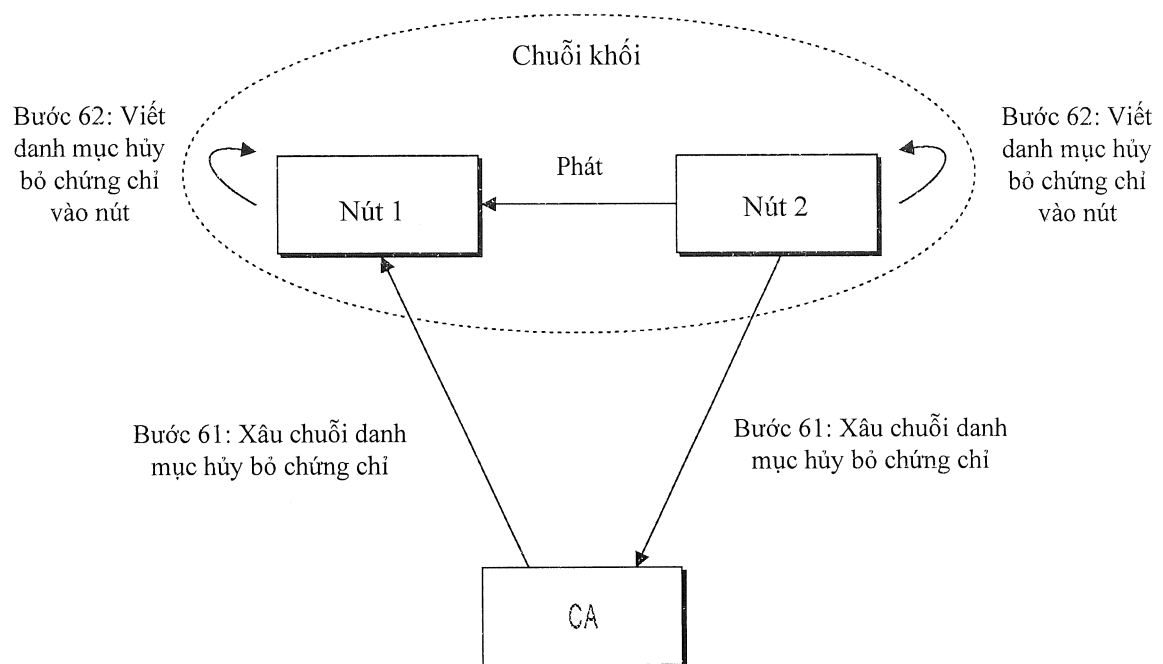
**FIG. 1**

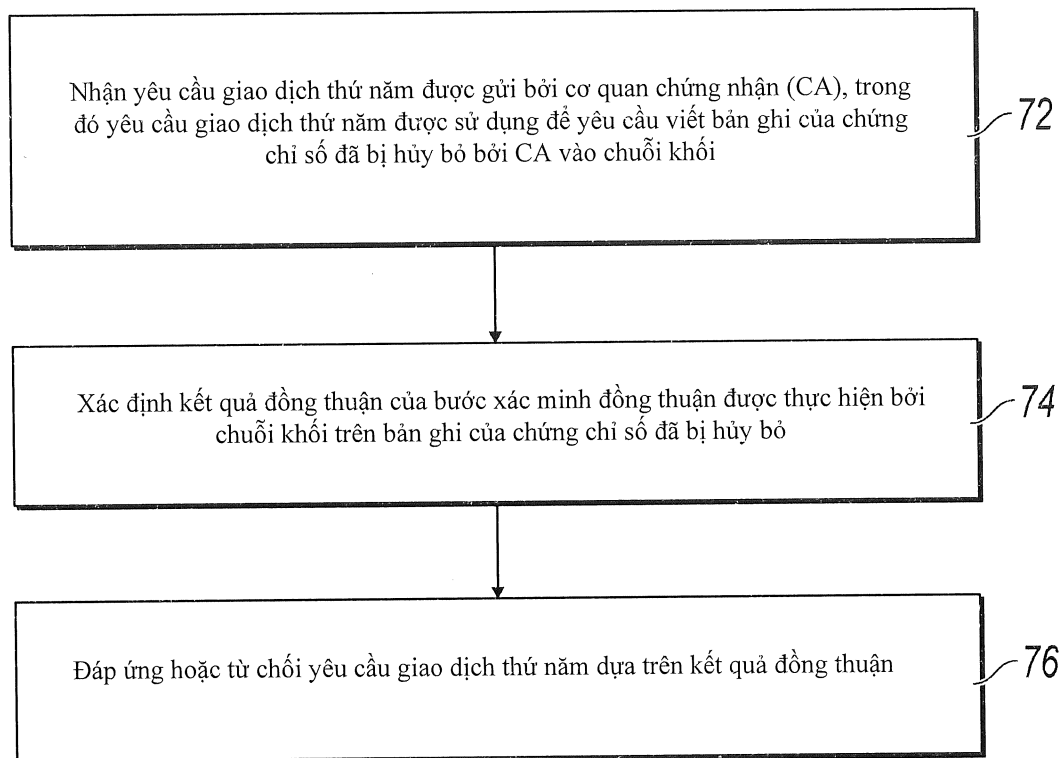
**FIG. 2**

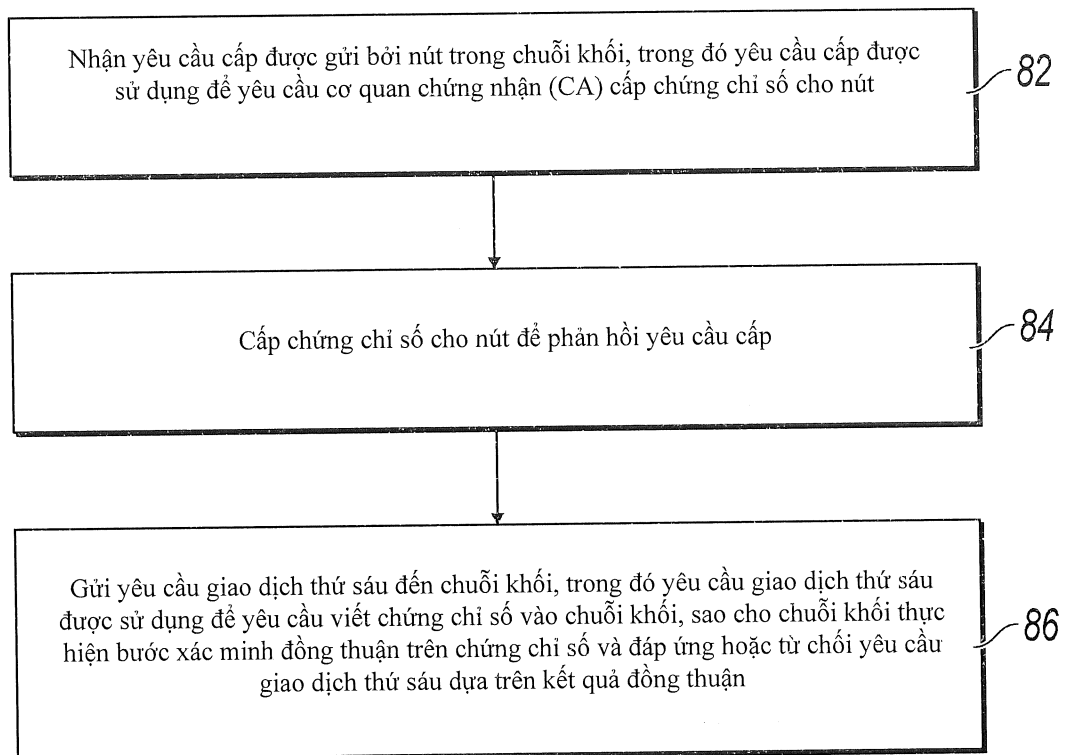
**FIG. 3**

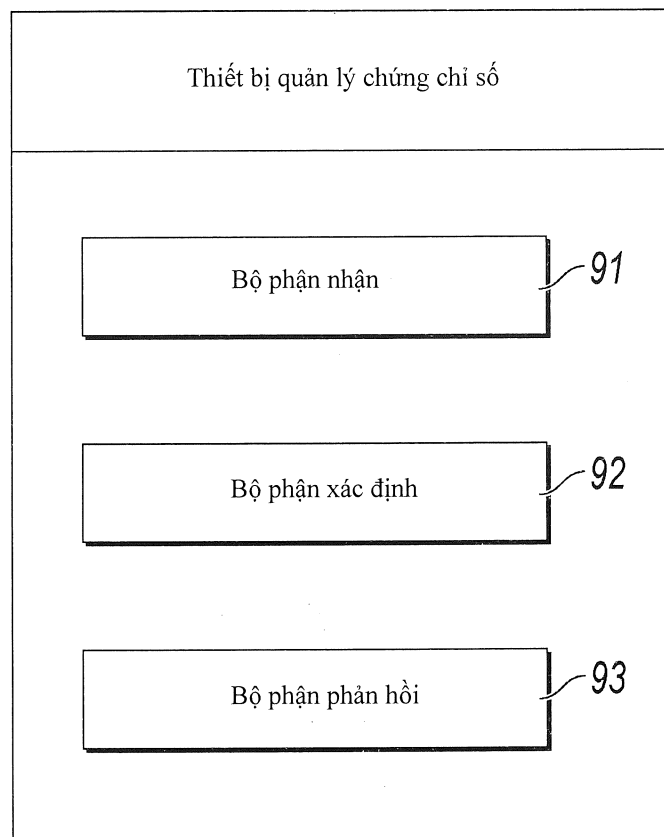
**FIG. 4**

**FIG. 5**

**FIG. 6**

**FIG. 7**

**FIG. 8**

**FIG. 9**

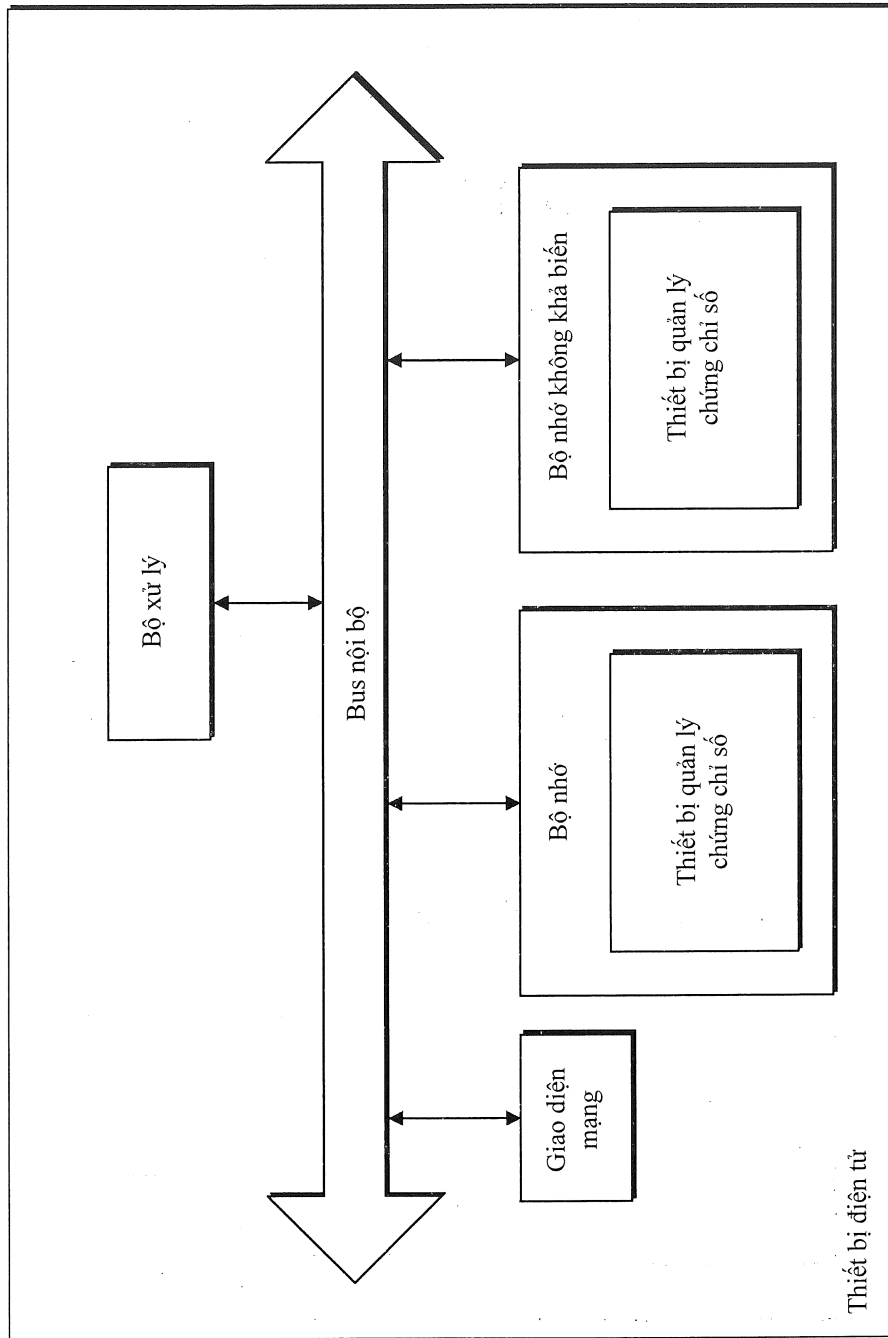
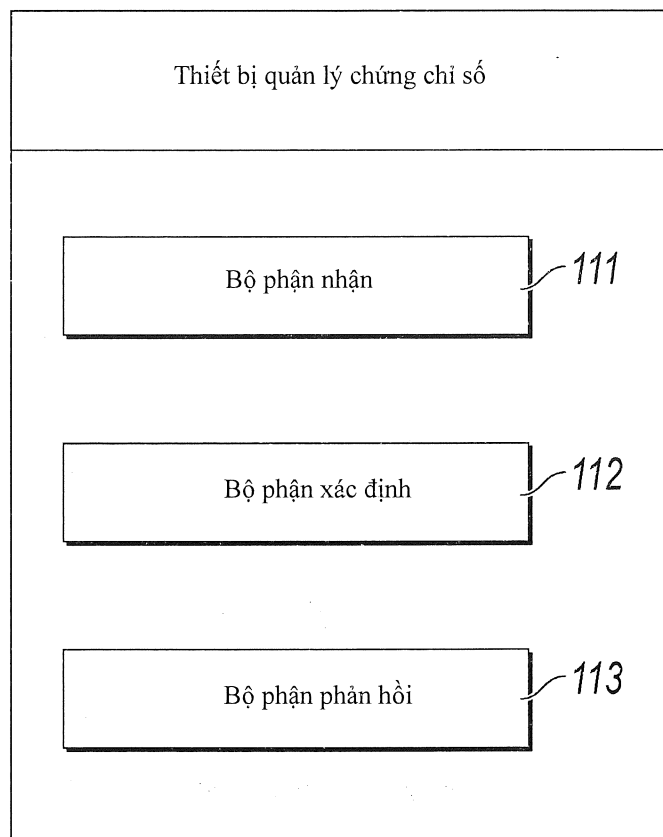


FIG. 10

**FIG. 11**

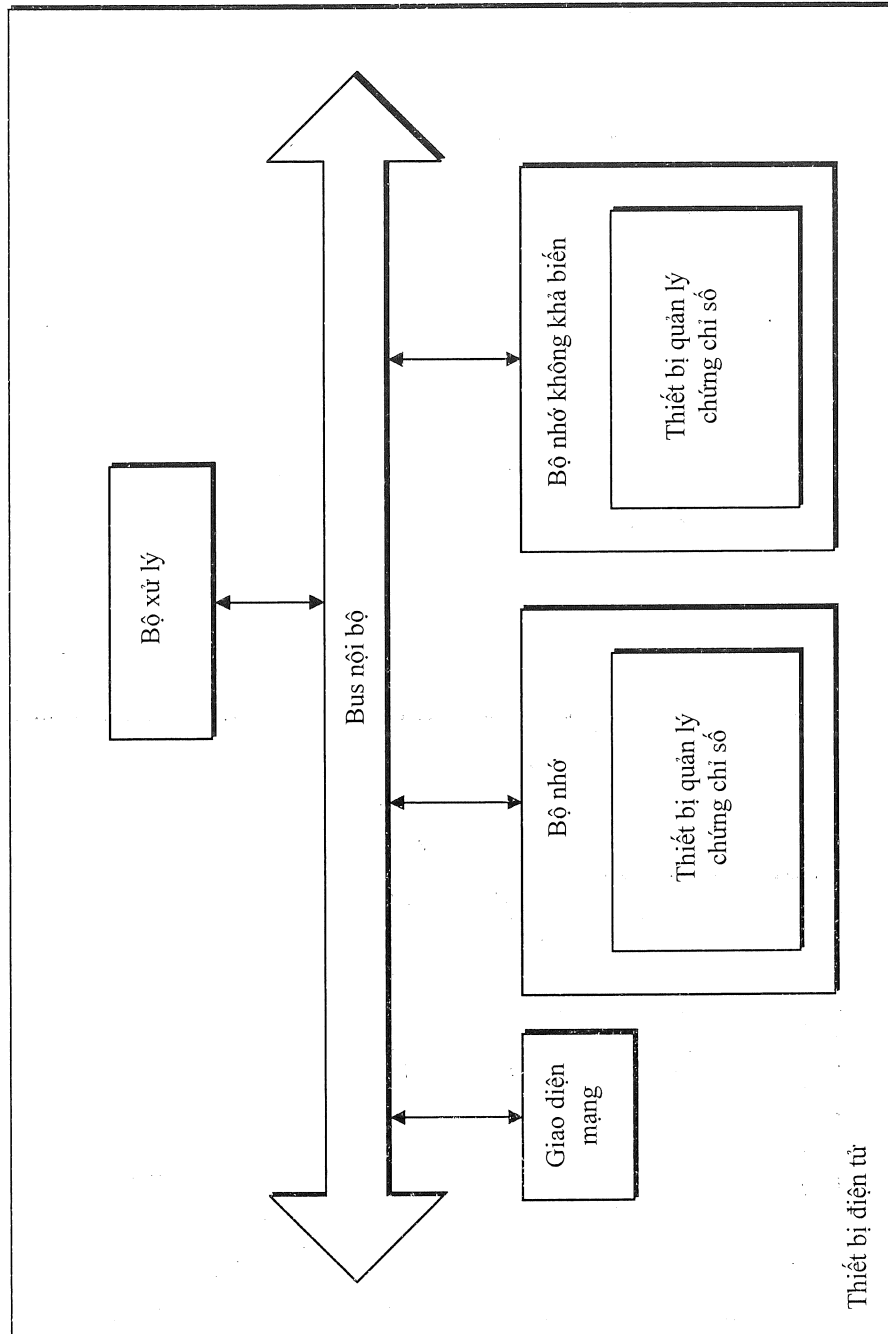
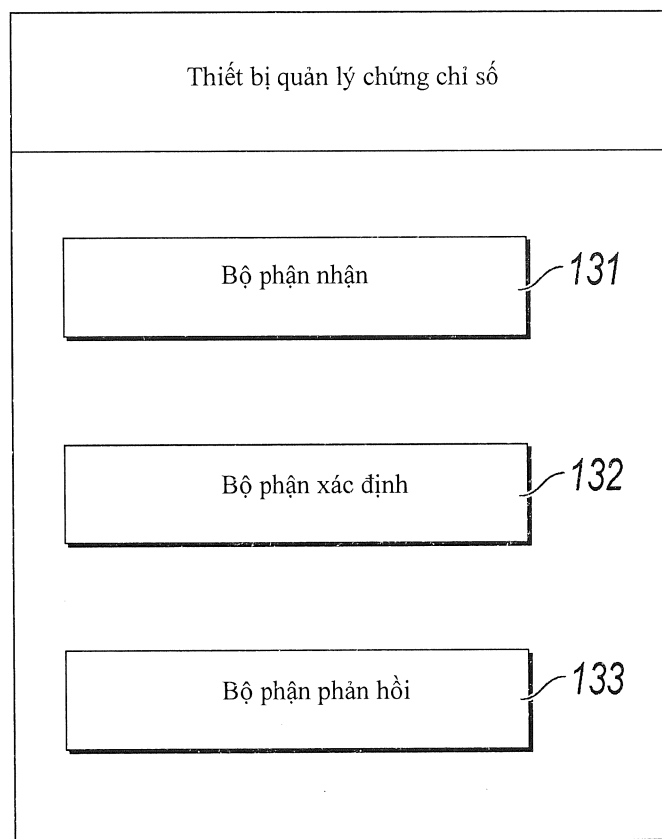


FIG. 12

**FIG. 13**

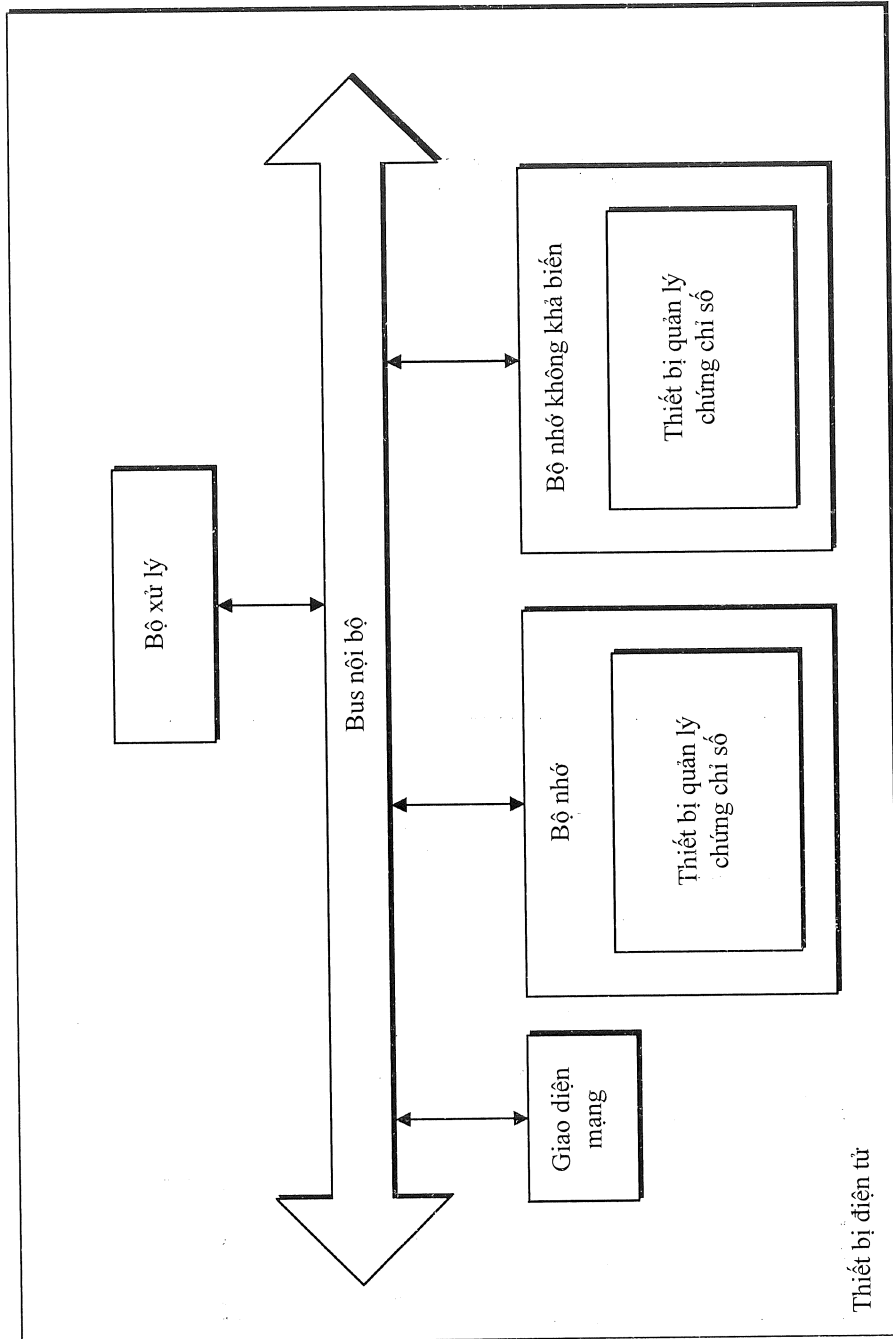
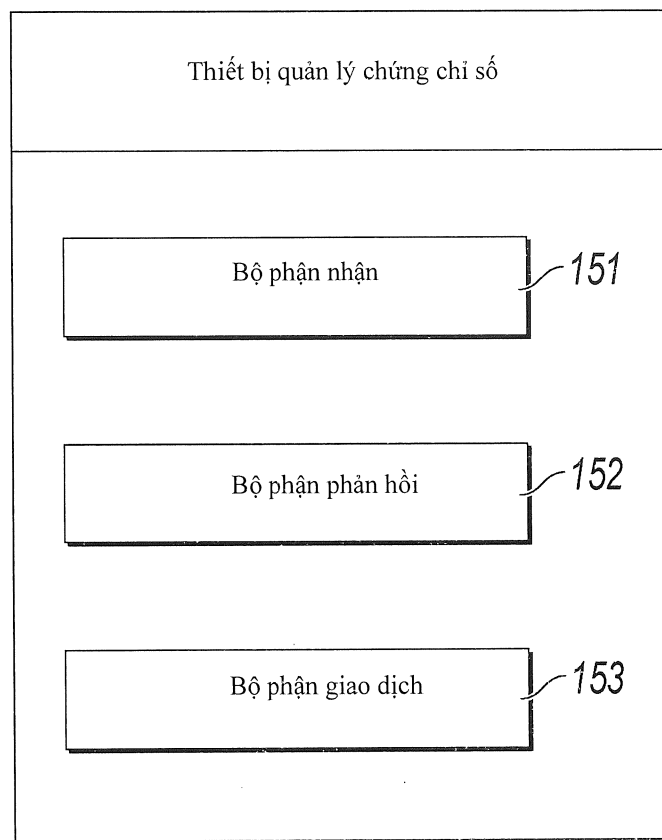


FIG. 14

**FIG. 15**

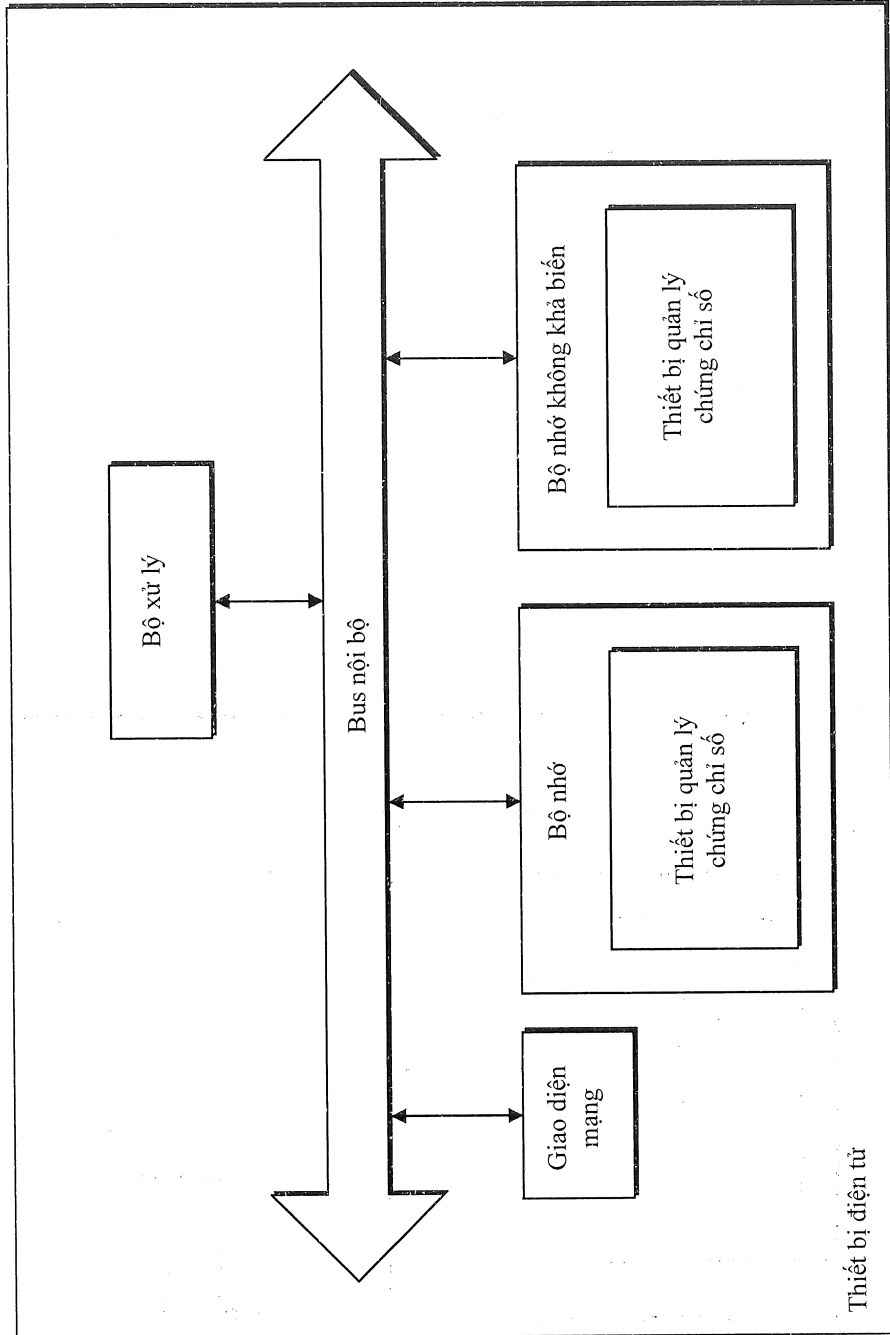


FIG. 16

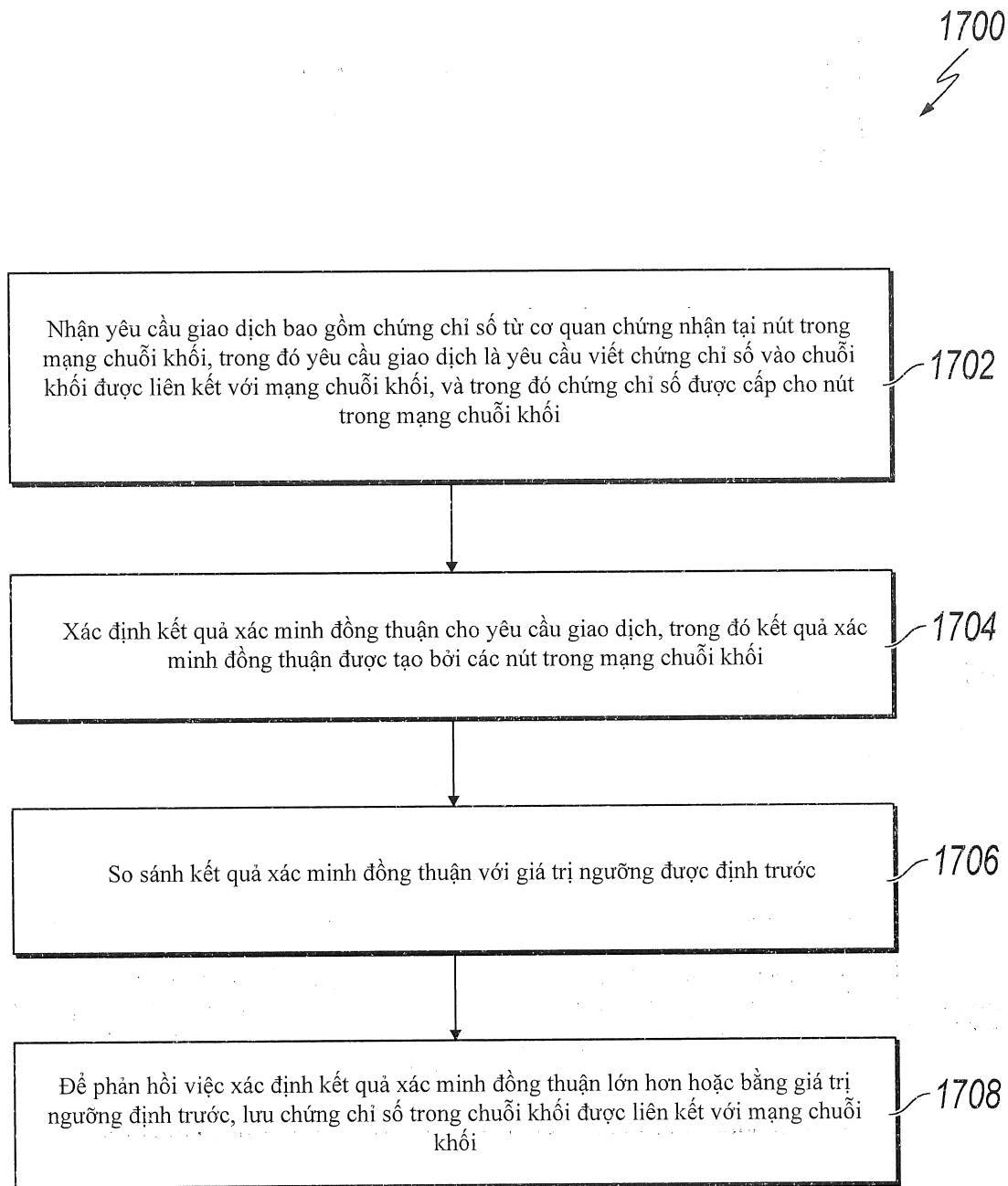


FIG. 17