



(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)



1-0033987

(51)⁷ G06F 21/62

(13) B

(21) 1-2019-03489

(22) 26/04/2018

(86) PCT/CN2018/084624 26/04/2018

(87) WO 2018/196813 01/11/2018

(30) 201710292517.6 28/04/2017 CN

(45) 25/11/2022 416

(43) 30/01/2020 382A

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

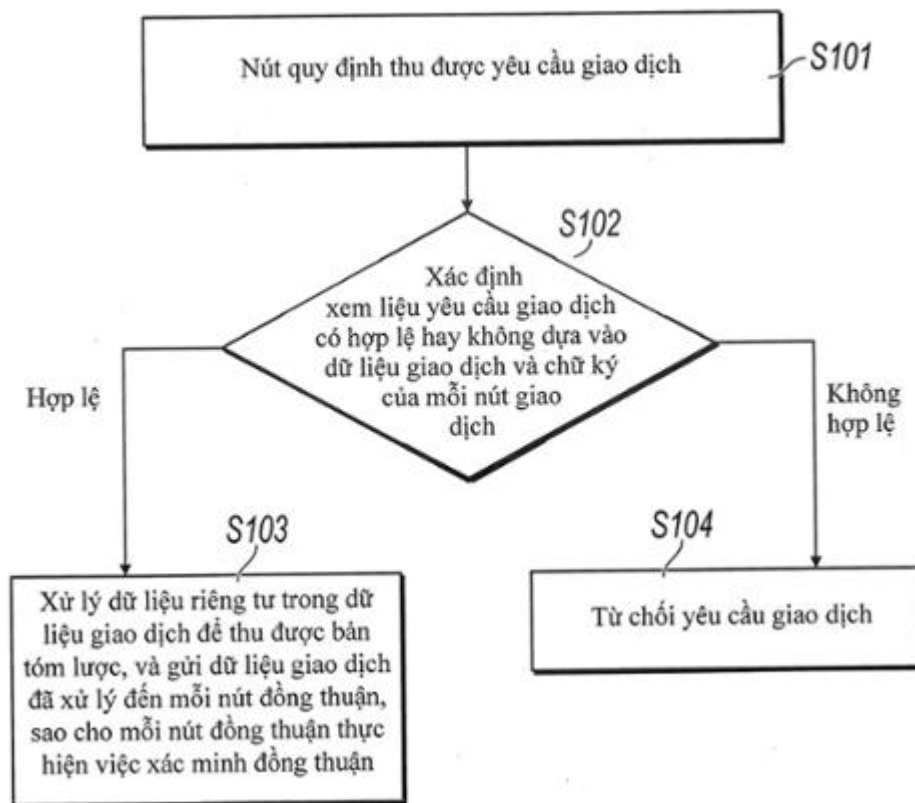
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands

(72) TANG, Qiang (CN).

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

(54) PHƯƠNG PHÁP ĐƯỢC THỰC THI BẰNG MÁY TÍNH VÀ THIẾT BỊ XÁC MINH ĐỒNG THUẬN

(57) Sáng chế đề xuất phương pháp và thiết bị xác minh đồng thuận. Nút quy định có trách nhiệm xác minh xem liệu yêu cầu giao dịch có hợp lệ hay không. Nếu yêu cầu giao dịch là hợp lệ, thì nút quy định tạo ra bản tóm lược dựa vào dữ liệu được chỉ định trong dữ liệu giao dịch và gửi bản tóm lược và dữ liệu không được chỉ định có trong dữ liệu giao dịch tới mỗi nút đồng thuận để xác minh đồng thuận. Mỗi nút đồng thuận lưu trữ bản tóm lược và dữ liệu không được chỉ định trong chuỗi khối sau khi xác minh đồng thuận thành công. Như vậy, nút đồng thuận không nhận dữ liệu được chỉ định và do đó không lưu giữ dữ liệu được chỉ định trong chuỗi khối. Kết quả là, dữ liệu được chỉ định không bị lộ. Thêm nữa, bản tóm lược có thể được sử dụng để xác minh xem liệu dữ liệu được chỉ định không được lưu trữ trong chuỗi khối có bị làm giả hay không.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ chuỗi khối (blockchain) và cụ thể là đề cập đến phương pháp và thiết bị xác minh đồng thuận.

Tình trạng kỹ thuật của sáng chế

Mạng chuỗi khối còn được gọi là mạng sổ cái phân tán và được đặc trưng bởi sự phi tập trung, tính công khai và tính minh bạch. Mỗi nút chuỗi khối đồng bộ hóa với chuỗi khối. Mạng chuỗi khối gồm các nút chuỗi khối. Mỗi nút chuỗi khối có thể khởi tạo yêu cầu giao dịch và tham gia vào việc xác minh đồng thuận về yêu cầu giao dịch.

Phương pháp xác minh đồng thuận hiện nay là như sau: nút chuỗi khối tham gia vào giao dịch sẽ phát đi yêu cầu giao dịch cho giao dịch tới mỗi nút đồng thuận trong mạng chuỗi khối. Nút đồng thuận là nút chuỗi khối chịu trách nhiệm xác minh đồng thuận và yêu cầu giao dịch gồm dữ liệu giao dịch của giao dịch. Mỗi nút đồng thuận lưu trữ dữ liệu giao dịch trong chuỗi khối sau khi xác minh đồng thuận được thực hiện bởi mỗi nút đồng thuận về yêu cầu giao dịch thành công.

Tuy nhiên, mỗi nút chuỗi khối có thể đồng bộ với chuỗi khối để thu được dữ liệu giao dịch của mỗi giao dịch được lưu trữ trong chuỗi khối. Do đó, tính riêng tư có trong dữ liệu giao dịch của nút chuỗi khối tham gia vào giao dịch dễ dàng bị lộ.

Bản chất kỹ thuật của sáng chế

Theo các phương án thực hiện, sáng chế đề xuất phương pháp và thiết bị xác minh đồng thuận, để khắc phục nhược điểm mà khi sử dụng phương pháp xác minh đồng thuận, tính riêng tư của nút chuỗi khối tham gia vào giao dịch dễ dàng bị bộc lộ.

Để khắc phục các nhược điểm kỹ thuật đã biết, theo các phương án thực hiện, sáng chế được thực hiện như sau:

Theo phương án thực hiện, sáng chế đề xuất phương pháp xác minh đồng thuận, trong đó phương pháp này bao gồm các bước sau: thu được yêu cầu giao dịch, trong đó yêu cầu giao dịch gồm dữ liệu giao dịch và chữ ký của ít nhất một nút giao dịch, bởi một nút quy định; xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa vào dữ

liệu giao dịch và chữ ký của mỗi nút giao dịch; và nếu yêu cầu giao dịch là hợp lệ, thì tạo ra bản tóm lược dựa vào dữ liệu được chỉ định có trong dữ liệu giao dịch và gửi bản tóm lược và dữ liệu không được chỉ định có trong dữ liệu giao dịch tới mỗi nút đồng thuận, sao cho mỗi nút đồng thuận thực hiện xác minh đồng thuận.

Theo phương án thực hiện, sáng chế đề xuất thiết bị xác minh đồng thuận, trong đó thiết bị này bao gồm: môđun thu nhận thứ nhất, được tạo cấu hình để thu được yêu cầu giao dịch, trong đó yêu cầu giao dịch gồm dữ liệu giao dịch và chữ ký của ít nhất một nút giao dịch; và môđun xác định và xử lý, được tạo cấu hình để xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa vào dữ liệu giao dịch và chữ ký của mỗi nút giao dịch; và nếu yêu cầu giao dịch là hợp lệ, thì tạo ra bản tóm lược dựa vào dữ liệu được chỉ định có trong dữ liệu giao dịch và gửi bản tóm lược và dữ liệu không được chỉ định có trong dữ liệu giao dịch tới mỗi nút đồng thuận, sao cho mỗi nút đồng thuận thực hiện xác minh đồng thuận.

Có thể thấy từ các giải pháp kỹ thuật được đề xuất theo các phương án thực hiện của sáng chế mà, trong các phương án thực hiện của sáng chế, nút quy định có trách nhiệm xác minh xem liệu yêu cầu giao dịch có hợp lệ hay không. Nếu yêu cầu giao dịch là hợp lệ, thì nút quy định tạo ra bản tóm lược dựa vào dữ liệu được chỉ định trong dữ liệu giao dịch và gửi bản tóm lược và dữ liệu không được chỉ định có trong dữ liệu giao dịch tới mỗi nút đồng thuận để xác minh đồng thuận. Mỗi nút đồng thuận lưu trữ bản tóm lược và dữ liệu không được chỉ định trong chuỗi khối sau khi xác minh đồng thuận thành công. Như vậy, nút đồng thuận không nhận dữ liệu được chỉ định và do đó không lưu giữ dữ liệu được chỉ định trong chuỗi khối. Kết quả là, dữ liệu được chỉ định không bị lộ. Thêm nữa, bản tóm lược có thể được dùng để xác minh xem liệu dữ liệu được chỉ định không được lưu trữ trong chuỗi khối có bị làm giả hay không.

Mô tả vắn tắt các hình vẽ

Để mô tả các giải pháp kỹ thuật theo phương án thực hiện của sáng chế hoặc trong công nghệ hiện tại rõ ràng hơn, sau đây sẽ mô tả vắn tắt các hình vẽ kèm theo cần để mô tả các phương án thực hiện hoặc công nghệ này. Rõ ràng là, các hình vẽ kèm theo trong phần mô tả sau đây chỉ thể hiện một số phương án thực hiện của sáng chế và người có hiểu biết trung bình về lĩnh vực kỹ thuật vẫn có thể dẫn chiếu đến các hình vẽ khác từ các hình vẽ kèm theo này mà không cần nỗ lực sáng tạo.

Fig.1 là lưu đồ minh họa phương pháp xác minh đồng thuận, theo phương án thực hiện của sáng chế;

Fig.2 là giản đồ minh họa mạng chuỗi khối, theo phương án thực hiện của sáng chế;

Fig.3 là giản đồ minh họa mạng chuỗi khối, theo phương án thực hiện của sáng chế; và

Fig.4 là giản đồ minh họa thiết bị xác minh đồng thuận, theo phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Theo các phương án thực hiện, sáng chế đề xuất phương pháp và thiết bị xác minh đồng thuận.

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

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

Fig.1 là lưu đồ minh họa phương pháp xác minh đồng thuận, theo phương án thực hiện của sáng chế. Phương pháp này gồm các bước sau đây.

Bước S101. Nút quy định thu được yêu cầu giao dịch.

Phương pháp được thực hiện bởi nút quy định. Nút quy định là nút chuỗi khối có trách nhiệm điều chỉnh các giao dịch. Nút quy định có sự tin cậy công khai và các mục được xác minh bởi nút quy định được báo nhận bởi các nút chuỗi khối trong toàn bộ mạng.

Trong mạng chuỗi khối, nút chuỗi khối tham gia vào giao dịch là nút giao dịch và nút chuỗi khối tham gia vào đồng thuận là nút đồng thuận. Rất đáng nhấn mạnh rằng,

nút chuỗi khối có thể vừa là nút giao dịch và vừa là nút đồng thuận và có thể không chỉ tham gia vào giao dịch mà cũng tham gia vào xác minh đồng thuận về giao dịch.

Fig.2 là giản đồ minh họa mạng chuỗi khối, theo phương án thực hiện của sáng chế. Như được thể hiện trên Fig.2, nút chuỗi khối đen là nút quy định. Nút chuỗi khối trắng là nút đồng thuận. Nút bóng là nút giao dịch và có thể cũng tham gia vào xác minh đồng thuận.

Theo phương án thực hiện này của sáng chế, yêu cầu giao dịch gồm dữ liệu giao dịch và chữ ký của ít nhất một nút giao dịch. Nút giao dịch có thể là nút chuỗi khối thanh toán cho tài sản trong giao dịch. Nút chuỗi khối chấp nhận tài sản trong giao dịch có thể cũng là nút giao dịch được mô tả trong sáng chế. Để dễ dàng mô tả, các mô tả được nêu ra bên dưới bằng cách sử dụng ví dụ nút giao dịch là nút chuỗi khối mà thanh toán cho tài sản trong giao dịch. Thêm nữa, sáng chế thiết lập không giới hạn ở việc xem liệu nút giao dịch cũng là nút đồng thuận tại cùng thời điểm hay không.

Dữ liệu giao dịch là dữ liệu chi tiết của giao dịch, như nhận dạng của nút giao dịch, nội dung chi tiết của tài sản liên quan trong giao dịch, số tài sản của tài sản liên quan trong giao dịch và địa chỉ tài khoản của nút giao dịch.

Theo phương án thực hiện này của sáng chế, chữ ký của nút giao dịch được tạo bởi nút giao dịch cho dữ liệu giao dịch và được sử dụng làm bằng chứng và ghi nhận rằng nút giao dịch phê duyệt dữ liệu giao dịch. Nếu nút giao dịch phê duyệt dữ liệu giao dịch của giao dịch rằng nút giao dịch tham gia vào, để bảo lưu bằng chứng và bản ghi giao dịch sau đó, nút giao dịch trước tiên có thể xây dựng bản tóm lược của dữ liệu giao dịch dựa vào thuật toán tạo bản tóm lược và còn xử lý bản tóm lược của dữ liệu giao dịch nhờ thuật toán chữ ký và khóa riêng tư để tạo ra chữ ký của nút giao dịch.

Rất đáng lưu ý là, đây có thể là các thuật toán tạo bản tóm lược, nhưng đặc điểm chung của thuật toán tạo bản tóm lược là văn bản gốc trước không thể được dẫn xuất ngược từ bản tóm lược thu được bằng cách tính toán văn bản gốc. Nếu có bất kỳ sửa đổi nào đến văn bản gốc, bản tóm lược thu được bằng cách tính toán văn bản gốc cải biến cũng có thể khác nhau. Có thể thấy rằng, bản tóm lược của dữ liệu giao dịch có thể được sử dụng làm mã nhận dạng duy nhất của dữ liệu giao dịch để nhận dạng mỗi giao dịch. Do đó, nếu nút giao dịch ký dữ liệu giao dịch, nó có thể chỉ ra rằng nút giao dịch phê duyệt dữ liệu giao dịch và theo đó nút giao dịch sau đó có thể được ngăn không cho từ

chối dữ liệu giao dịch.

Theo phương án thực hiện này của sáng chế, trong yêu cầu giao dịch, chữ ký của nút giao dịch tương ứng với số tài sản của tài sản được sử dụng bởi nút giao dịch trong dữ liệu giao dịch. Nút giao dịch sử dụng chữ ký để kê khai số tài sản của tài sản được sử dụng bởi nút giao dịch. Nút giao dịch cho phép chữ ký của nút giao dịch và số tài sản được sử dụng bởi nút giao dịch tạo ra cấu trúc dữ liệu cụ thể, ví dụ, “số tài sản 001 (chữ ký A)”; hoặc có thể sử dụng phương pháp khác để xác lập tương quan ánh xạ giữa chữ ký và số tài sản được sử dụng bởi nút giao dịch. Chắc chắn, số tài sản tương ứng với chữ ký của nút giao dịch không nhất thiết là số tài sản thực tế do nút giao dịch sở hữu. Nói cách khác, nút giao dịch có thể sử dụng với mục đích xấu và lừa đảo số tài sản do nút kia sở hữu. Cách thức tránh rủi ro là một phần của phần mô tả sau đây về việc xác minh tính hợp lệ của yêu cầu giao dịch.

Theo phương án thực hiện này của sáng chế, một yêu cầu giao dịch có thể bao gồm các chữ ký của các nút giao dịch. Tức là, bất kỳ một giao dịch nút có thể thu thập các chữ ký của các nút giao dịch, tạo ra yêu cầu giao dịch và gửi yêu cầu giao dịch tới nút quy định. Phương pháp thu thập các chữ ký có thể là như sau: Dữ liệu giao dịch được truyền trong số các nút giao dịch theo thứ tự, mỗi nút giao dịch gán chữ ký của nút giao dịch cho dữ liệu giao dịch và giao dịch nút cuối cùng mà dữ liệu giao dịch được truyền để tạo ra yêu cầu giao dịch. Theo cách khác, nút giao dịch có thể nhận chữ ký được gửi bởi mỗi nút giao dịch khác và sau đó tạo ra yêu cầu giao dịch. Để dễ dàng mô tả, các mô tả được nêu ra bên dưới bằng cách sử dụng ví dụ yêu cầu giao dịch gồm các chữ ký của các nút giao dịch.

Bước S102. Xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa vào dữ liệu giao dịch và chữ ký của mỗi nút giao dịch và thực hiện bước S103 nếu yêu cầu giao dịch là hợp lệ, hoặc thực hiện bước S104 nếu yêu cầu giao dịch là không hợp lệ.

Theo phương án thực hiện này của sáng chế, có nhiều phương pháp để xác minh tính hợp lệ của yêu cầu giao dịch. Ví dụ, trong trường hợp 1, nút quy định có thể điểm điểm khả năng tín dụng của mỗi nút giao dịch ký dựa vào bản ghi tín dụng mỗi nút giao dịch được lưu trữ bởi nút quy định và xác định rằng yêu cầu giao dịch là không hợp lệ nếu số điểm khả năng tín dụng của mỗi nút giao dịch nhỏ hơn số điểm định trước, hoặc xác định rằng yêu cầu giao dịch là hợp lệ nếu số điểm khả năng tín dụng của mỗi nút

giao dịch không nhỏ hơn số điểm định trước. Đối với ví dụ khác, trong trường hợp 2, theo cách khác nút quy định có thể sử dụng dữ liệu giao dịch, chữ ký của mỗi nút giao dịch và khóa công khai của mỗi nút giao dịch để xác minh xem liệu nút giao dịch làm giả dữ liệu giao dịch hoặc sử dụng với mục đích lừa đảo tài sản của người khác hay không. Chắc chắn, có thể có các trường hợp khác để xác minh tính hợp lệ của yêu cầu giao dịch. Các chi tiết ở đây được bỏ qua để đơn giản.

Trong trường hợp 2, nút quy định trước tiên có thể giữ khóa công khai của mỗi nút giao dịch, hoặc yêu cầu giao dịch có thể bao gồm khóa công khai của mỗi nút giao dịch. Khóa công khai của mỗi nút giao dịch có thể được sử dụng để giải mã chữ ký của nút giao dịch để thu được bản tóm lược của dữ liệu giao dịch, nhờ vậy xác minh xem liệu người ký có làm giả dữ liệu giao dịch hay không. Nếu kết quả giải mã thu được bởi nút quy định bằng cách giải mã chữ ký của nút giao dịch nhờ sử dụng khóa công khai được cung cấp bởi nút giao dịch không phù hợp với bản tóm lược của dữ liệu giao dịch, điều này chỉ ra rằng nút giao dịch tạo ra chữ ký do lừa đảo sử dụng khóa riêng tư của nút chuỗi khối khác hoặc nút giao dịch làm giả dữ liệu giao dịch và do đó yêu cầu giao dịch là không hợp lệ. Tính hợp lệ của yêu cầu giao dịch có thể còn được xác minh sau đó nếu không có nút giao dịch làm giả dữ liệu giao dịch.

Theo phương án thực hiện này của sáng chế, việc xác minh tính hợp lệ tiếp theo có thể bao gồm các bước sau đây: xác minh xem liệu nút giao dịch lừa đảo sử dụng tài sản của người khác hay không. Trong mạng chuỗi khối thường dùng, số tài sản của tài sản do mỗi nút chuỗi khối sở hữu được kết hợp với khóa công khai của nút chuỗi khối và khóa công khai đóng vai trò làm dấu hiệu nhận dạng bộc lộ ở bên ngoài của nút chuỗi khối có thể nhận diện duy nhất nhận dạng của nút chuỗi khối. Nói cách khác, số tài sản kết hợp với khóa công khai của nút chuỗi khối là số tài sản thực tế do nút chuỗi khối sở hữu.

Do đó, theo phương án thực hiện này của sáng chế, nút quy định xác định số tài sản của tài sản thực tế do mỗi nút giao dịch sở hữu dựa vào khóa công khai của mỗi nút giao dịch và sau đó so sánh số tài sản (số tài sản được sử dụng bởi nút giao dịch) tương ứng với chữ ký của nút giao dịch trong dữ liệu giao dịch với số tài sản thực tế do nút giao dịch sở hữu để xác định xem liệu nút giao dịch sử dụng với mục đích xấu và lừa đảo số tài sản do nút chuỗi khối khác sở hữu hay không. Yêu cầu giao dịch là không hợp lệ nếu

ít nhất một nút giao dịch sử dụng với mục đích xấu và lừa đảo số tài sản do nút chuỗi khối khác sở hữu. Yêu cầu giao dịch là hợp lệ nếu số tài sản được sử dụng bởi mỗi nút giao dịch là số tài sản do nút giao dịch sở hữu.

Tóm lại, có thể thấy rằng, trong trường hợp 2 mà nút quy định xác minh tính hợp lệ của yêu cầu giao dịch, việc xác minh được thực hiện theo cách liên tiếp và hai khía cạnh sau đây cần được khẳng định liên tiếp để xác định rằng yêu cầu giao dịch là hợp lệ: 1. Dữ liệu giao dịch không bị làm giả. 2. Nút giao dịch không lừa đảo sử dụng số tài sản do nút chuỗi khối khác sở hữu.

Bước S103. Tạo ra bản tóm lược bí mật dựa vào dữ liệu riêng tư trong dữ liệu giao dịch và gửi bản tóm lược bí mật và dữ liệu không riêng tư trong dữ liệu giao dịch tới mỗi nút đồng thuận, sao cho mỗi nút đồng thuận thực hiện xác minh đồng thuận.

Theo phương án thực hiện này của sáng chế, dữ liệu được chỉ định có thể là dữ liệu riêng tư và dữ liệu không được chỉ định có thể là dữ liệu không riêng tư. Dữ liệu riêng tư gồm tính riêng tư của nút giao dịch và có thể được chỉ định bởi nút giao dịch và thông báo tới nút quy định; hoặc có thể được chỉ định bởi nút quy định. Ví dụ, dữ liệu riêng tư có thể bao gồm nhận dạng của nút giao dịch, nội dung chi tiết của tài sản và địa chỉ tài khoản, v.v., mà được coi là tính riêng tư của nút giao dịch.

Như đã mô tả ở trên, văn bản gốc không thể được dẫn xuất ngược từ bản tóm lược của văn bản gốc. Do đó, sau khi bản tóm lược được tạo ra cho dữ liệu riêng tư, bản tóm lược có thể được lưu trữ trong chuỗi khối tin cậy và dữ liệu riêng tư có thể được ẩn, sao cho bằng chứng tin cậy và bản ghi dữ liệu riêng tư có thể được bảo lưu và dữ liệu riêng tư có thể được bảo vệ.

Sau khi nhận được bản tóm lược và dữ liệu không riêng tư, mỗi nút đồng thuận có thể thực hiện xác minh đồng thuận dựa vào dữ liệu không riêng tư, ví dụ, có thể xác minh xem liệu có chi phí nhân đôi dựa vào số tài sản trong dữ liệu không riêng tư hay không. Nếu xác minh đồng thuận thành công, bản tóm lược bí mật và dữ liệu không riêng tư được lưu trữ trong chuỗi khối. Tính hợp lệ của yêu cầu giao dịch được xác minh và được chứng thực trước bởi nút quy định.

Như vậy, xác minh đồng thuận về giao dịch được hoàn thành. Bản tóm lược được lưu trữ trong chuỗi khối có thể được sử dụng để xác minh xem liệu dữ liệu riêng tư được yêu cầu bởi nút giao dịch là đúng hay không, để giải quyết tranh chấp giữa các nút giao

dịch.

Theo phương án thực hiện này của sáng chế, nút quy định có thể còn gửi chữ ký của mỗi nút giao dịch tới mỗi nút đồng thuận, sao cho sau khi xác minh đồng thuận được thực hiện bởi mỗi nút đồng thuận về giao dịch thành công, nút đồng thuận cũng lưu trữ chữ ký của mỗi nút giao dịch trong chuỗi khối để ngăn không cho mỗi nút giao dịch sau đó từ chối chữ ký.

Thêm nữa, theo phương án thực hiện này của sáng chế, nút quy định có thể lệnh cho ít nhất một nút giao dịch lưu giữ dữ liệu giao dịch hoặc dữ liệu được chỉ định có trong dữ liệu giao dịch nếu yêu cầu giao dịch là hợp lệ. Chắc chắn, theo cách khác, nút quy định có thể lệnh cho ít nhất một nút giao dịch lưu giữ dữ liệu giao dịch hoặc dữ liệu được chỉ định trong cơ sở dữ liệu riêng tư tương ứng với nút giao dịch sau khi xác minh đồng thuận được thực hiện bởi mỗi nút đồng thuận về giao dịch thành công và sau khi bản tóm lược được lưu trữ trong chuỗi khối. Tóm lại, mỗi nút giao dịch lưu trữ dữ liệu được chỉ định hoặc chính dữ liệu giao dịch này. Các phương án thực hiện không bị giới hạn ở sáng chế.

Mặc dù nút giao dịch có thể làm giả riêng dữ liệu chỉ định được lưu trữ bởi nút giao dịch, bản tóm lược được lưu trữ trong chuỗi khối có thể được sử dụng để xác minh tính xác thực của dữ liệu được chỉ định tại thời điểm bất kỳ, nhờ vậy tránh được rủi ro do sự làm giả dữ liệu được chỉ định bởi nút giao dịch gây ra.

Fig.3 là giản đồ minh họa mạng chuỗi khối, theo phương án thực hiện của sáng chế. Như được thể hiện trên hình vẽ, trong mạng chuỗi khối, mỗi nút chuỗi khối duy trì chuỗi khối và mỗi nút chuỗi khối có cơ sở dữ liệu riêng tư của chính nó để lưu trữ dữ liệu riêng tư của giao dịch mà nút chuỗi khối tham gia vào. Đối với giao dịch A, chỉ cơ sở dữ liệu riêng tư của nút chuỗi khối (nút giao dịch) tham gia vào giao dịch A lưu trữ dữ liệu riêng tư tương ứng với giao dịch A và cơ sở dữ liệu riêng tư của nút chuỗi khối (nút không giao dịch) không tham gia vào giao dịch A không lưu trữ dữ liệu riêng tư mà tương ứng với giao dịch A.

Bước S104. Từ chối yêu cầu giao dịch.

Theo phương pháp xác minh đồng thuận được thể hiện trên Fig.1, nút quy định có trách nhiệm xác minh xem liệu yêu cầu giao dịch có hợp lệ hay không. Nếu yêu cầu giao dịch là hợp lệ, thì nút quy định tạo ra bản tóm lược dựa vào dữ liệu được chỉ định trong

dữ liệu giao dịch và gửi bản tóm lược và dữ liệu không được chỉ định có trong dữ liệu giao dịch tới mỗi nút đồng thuận để xác minh đồng thuận. Mỗi nút đồng thuận lưu trữ bản tóm lược và dữ liệu không được chỉ định trong chuỗi khối sau khi xác minh đồng thuận thành công. Như vậy, nút đồng thuận không nhận dữ liệu được chỉ định và do đó không lưu giữ dữ liệu được chỉ định trong chuỗi khối. Kết quả là, dữ liệu được chỉ định không bị lộ. Thêm nữa, bản tóm lược có thể được sử dụng để xác minh xem liệu dữ liệu được chỉ định không được lưu trữ trong chuỗi khối có bị làm giả hay không.

Thêm nữa, đối với mạng chuỗi khối cụ thể như mạng chuỗi khối liên doanh, mỗi nút chuỗi khối trong mạng chuỗi khối liên doanh có chứng chỉ số do cơ quan cấp chứng thư cấp, trong đó chứng chỉ số được sử dụng để chứng thực nhận dạng thực của nút chuỗi khối. Chứng chỉ số gồm nhận dạng (identify, ID) của nút chuỗi khối và khóa công khai. Quan trọng là, không giống như mạng chuỗi khối thường dùng, trong mạng chuỗi khối liên doanh, số tài sản do nút chuỗi khối sở hữu được kết hợp với ID của nút chuỗi khối.

Theo kịch bản ứng dụng của mạng chuỗi khối liên doanh, nút quy định có thể thu được chứng chỉ số của nút giao dịch và xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa vào chứng chỉ số của nút giao dịch, chữ ký của mỗi nút giao dịch và dữ liệu giao dịch.

Nút quy định có thể giải mã chữ ký của mỗi nút giao dịch dựa vào khóa công khai có trong chứng chỉ số của nút giao dịch; và nếu xác định kết quả giải mã tương ứng với mỗi nút giao dịch là giống như bản tóm lược của dữ liệu giao dịch, thì xác định số tài sản tương ứng với nhận dạng dựa vào nhận dạng có trong chứng chỉ số của mỗi nút giao dịch và sử dụng số tài sản là số tài sản do nút giao dịch sở hữu; và xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa vào số tài sản do mỗi nút giao dịch sở hữu, chữ ký của mỗi nút giao dịch và dữ liệu giao dịch; hoặc xác định rằng yêu cầu giao dịch là không hợp lệ nếu xác định kết quả giải mã tương ứng với ít nhất một nút giao dịch khác với bản tóm lược của dữ liệu giao dịch.

Hơn nữa, nút quy định có thể xác định số tài sản tương ứng với chữ ký của mỗi nút giao dịch trong dữ liệu giao dịch dựa vào chữ ký của nút giao dịch và sử dụng số tài sản là số tài sản được sử dụng bởi nút giao dịch; xác định rằng nút giao dịch là không hợp lệ nếu số tài sản do nút giao dịch sở hữu không bao gồm ít nhất một số tài sản được sử

dụng bởi nút giao dịch; hoặc xác định rằng nút giao dịch là hợp lệ nếu số tài sản do nút giao dịch sở hữu gồm tất cả số tài sản được sử dụng bởi nút giao dịch; và xác định rằng yêu cầu giao dịch là không hợp lệ khi ít nhất một nút giao dịch không hợp lệ; hoặc xác định rằng yêu cầu giao dịch là hợp lệ khi tất cả các nút giao dịch hợp lệ.

Nút giao dịch hợp lệ có nghĩa là nút giao dịch không thực hiện hành vi bất hợp pháp với mục đích xấu (như lừa đảo sử dụng chữ ký của người khác hoặc lừa đảo sử dụng tài sản của người khác). Khi xác định rằng ít nhất một số tài sản được sử dụng bởi nút giao dịch trong giao dịch hiện hành không phải là số tài sản do nút giao dịch sở hữu, có thể coi rằng, nút giao dịch thực hiện hành vi lừa đảo bất hợp pháp sử dụng số tài sản của người khác và theo đó là không hợp lệ.

Nói cách khác, trong kịch bản ứng dụng của mạng chuỗi khối liên doanh, nút giao dịch cung cấp chứng chỉ số của nút giao dịch thay vì khóa công khai của nút giao dịch cho nút quy định. Thêm nữa, số tài sản thực tế do nút giao dịch sở hữu cần được khẳng định dựa vào ID của nút giao dịch. Như vậy, đây có thể là khác biệt nhỏ trong hai khía cạnh mô tả ở trên mà nút quy định cần khẳng định để xác minh tính hợp lệ của yêu cầu giao dịch (1. Dữ liệu giao dịch không bị làm giả. 2. Nút giao dịch không lừa đảo sử dụng số tài sản do nút chuỗi khối khác sở hữu).

Nút quy định trước tiên cố giải mã chữ ký của mỗi nút giao dịch dựa vào khóa công khai có trong chứng chỉ số của nút giao dịch. Nếu kết quả giải mã tương thích với bản tóm lược của dữ liệu giao dịch, điều này chỉ ra rằng nút giao dịch không giả mạo dữ liệu giao dịch. Sau khi xác định rằng các nhận dạng của tất cả các nút giao dịch là đúng, nút quy định có thể tiếp tục xác định xem liệu số tài sản (cụ thể, số tài sản được sử dụng bởi mỗi nút giao dịch trong giao dịch) tương ứng với chữ ký của mỗi nút giao dịch trong dữ liệu giao dịch có phải là số tài sản của nút giao dịch hay không, dựa vào số tài sản (cụ thể, số tài sản thực tế do nút giao dịch sở hữu) tương ứng với ID có trong chứng chỉ số của nút giao dịch. Điều này chỉ ra rằng yêu cầu giao dịch là hợp lệ nếu nút giao dịch không lừa đảo sử dụng số tài sản của người khác.

Rất đáng nhấn mạnh rằng, trong kịch bản ứng dụng của mạng chuỗi khối liên doanh, ID của nút giao dịch mà có trong chứng chỉ số của nút giao dịch thực tế là tính riêng tư của nút giao dịch. Theo phương án thực hiện này của sáng chế, nút quy định không gửi chứng chỉ số của nút giao dịch đến nút đồng thuận, nhờ vậy đảm bảo rằng ID của nút

giao dịch không bị lộ.

Dựa vào phương pháp xác minh đồng thuận được thể hiện trên Fig.1, theo phương án thực hiện, sáng chế còn đề xuất tương ứng thiết bị xác minh đồng thuận. Như được thể hiện trên Fig.4, thiết bị này bao gồm: môđun thu nhận thứ nhất 401, được tạo cấu hình để thu được yêu cầu giao dịch, trong đó yêu cầu giao dịch gồm dữ liệu giao dịch và chữ ký của ít nhất một nút giao dịch; và môđun xác định và xử lý 402, được tạo cấu hình để xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa vào dữ liệu giao dịch và chữ ký của mỗi nút giao dịch; và nếu yêu cầu giao dịch là hợp lệ, tạo ra bản tóm lược dựa vào dữ liệu được chỉ định có trong dữ liệu giao dịch và gửi bản tóm lược và dữ liệu không được chỉ định có trong dữ liệu giao dịch tới mỗi nút đồng thuận, sao cho mỗi nút đồng thuận thực hiện xác minh đồng thuận.

Thiết bị còn bao gồm môđun từ chối 403, được tạo cấu hình để từ chối yêu cầu giao dịch nếu yêu cầu giao dịch là không hợp lệ.

Thiết bị còn bao gồm môđun thu thập thứ hai 404, được tạo cấu hình để thu được chứng chỉ số của mỗi nút giao dịch trước khi xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa vào dữ liệu giao dịch và chữ ký của mỗi nút giao dịch.

Môđun xác định và xử lý 402 được tạo cấu hình để xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa vào dữ liệu giao dịch, chữ ký của mỗi nút giao dịch và chứng chỉ số của mỗi nút giao dịch.

Môđun xác định và xử lý 402 được tạo cấu hình để giải mã chữ ký của mỗi nút giao dịch dựa vào khóa công khai có trong chứng chỉ số của nút giao dịch; và nếu xác định kết quả giải mã tương ứng với mỗi nút giao dịch là giống như bản tóm lược của dữ liệu giao dịch, thì xác định số tài sản tương ứng với nhận dạng dựa vào nhận dạng có trong chứng chỉ số của mỗi nút giao dịch và sử dụng số tài sản là số tài sản do nút giao dịch sở hữu; và xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa vào số tài sản do mỗi nút giao dịch sở hữu, chữ ký của mỗi nút giao dịch và dữ liệu giao dịch; hoặc xác định rằng yêu cầu giao dịch là không hợp lệ nếu xác định kết quả giải mã tương ứng với ít nhất một nút giao dịch khác với bản tóm lược của dữ liệu giao dịch.

Môđun xác định và xử lý 402 được tạo cấu hình để xác định số tài sản tương ứng với chữ ký của mỗi nút giao dịch trong dữ liệu giao dịch dựa vào chữ ký của nút giao dịch và sử dụng số tài sản là số tài sản được sử dụng bởi nút giao dịch; xác định rằng

nút giao dịch là không hợp lệ nếu số tài sản do nút giao dịch sở hữu không bao gồm ít nhất một số tài sản được sử dụng bởi nút giao dịch; hoặc xác định rằng nút giao dịch là hợp lệ nếu số tài sản do nút giao dịch sở hữu gồm tất cả số tài sản được sử dụng bởi nút giao dịch; và xác định rằng yêu cầu giao dịch là không hợp lệ khi ít nhất một nút giao dịch không hợp lệ; hoặc xác định rằng yêu cầu giao dịch là hợp lệ khi tất cả các nút giao dịch hợp lệ.

Thiết bị còn bao gồm môđun thông báo 405, được tạo cấu hình để lệnh cho ít nhất một nút giao dịch lưu giữ dữ liệu giao dịch hoặc dữ liệu được chỉ định có trong dữ liệu giao dịch nếu yêu cầu giao dịch là hợp lệ.

Vào những năm 1990, liệu cải tiến kỹ thuật có phải là cải tiến phần cứng hay không (ví dụ, cải tiến đến kết cấu vi mạch, như điôt, tranzito, hoặc bộ chuyển mạch) hoặc cải thiện phần mềm (cải thiện các quy trình của phương pháp) có thể được phân biệt rõ ràng. Tuy nhiên, khi các công nghệ phát triển, các cải tiến hiện nay đến nhiều quy trình của phương pháp có thể được coi là cải tiến trực tiếp đến các kết cấu vi mạch phần cứng. Nhà thiết kế thường lập trình các quy trình của phương pháp cải tiến vào vi mạch phần cứng, để thu được kết cấu vi mạch phần cứng tương ứng. Do đó, quy trình của phương pháp có thể được cải thiện nhờ sử dụng môđun thực thể phần cứng. Ví dụ, thiết bị logic lập trình được (programmable logic device, PLD) (ví dụ, mảng công lập trình được dạng trường (field programmable gate array, FPGA)) là vi mạch tích hợp này và chức năng logic của PLD được xác định bởi người sử dụng nhờ sự lập trình bởi thiết bị. Nhà thiết kế thực hiện việc lập trình để “tích hợp” hệ thống số vào PLD mà không yêu cầu nhà sản xuất chip thiết kế và sản xuất chip mạch tích hợp ứng dụng đặc biệt. Thêm nữa, hiện tại, thay vì sản xuất một cách thủ công chip vi mạch tích hợp, sự lập trình này chủ yếu được thực hiện bằng cách sử dụng phần mềm “bộ biên dịch logic”. Phần mềm bộ biên dịch logic là tương tự với bộ biên dịch phần mềm được sử dụng để triển khai và viết chương trình. Mã gốc cần được viết theo ngôn ngữ lập trình cụ thể để biên dịch. Ngôn ngữ được gọi là ngôn ngữ mô tả phần cứng (hardware description language, HDL). Có nhiều HDL, như ngôn ngữ biểu thị Boolean tiên tiến (Advanced Boolean Expression Language, ABEL), ngôn ngữ mô tả phần cứng Altera (Altera hardware description language, AHDL), Confluence, ngôn ngữ lập trình của trường đại học Cornell (Cornell University Programming Language, CUPL), HDCal, ngôn ngữ mô tả phần cứng Java (Java hardware description language, JHDL), Lava, Lola, MyHDL, PALASM và ngôn

ngữ mô tả phần cứng Ruby (Ruby hardware description language, RHDL). Ngôn ngữ mô tả phần cứng vi mạch tích hợp tốc độ rất cao (very-high-speed intergrated circuit hardware description language, VHDL) và Verilog được sử dụng phổ biến nhất. Người có hiểu biết trung bình về lĩnh vực kỹ thuật cũng cần hiểu rằng vi mạch phần cứng thực hiện quy trình của phương pháp logic có thể sẵn sàng thu được một khi quy trình của phương pháp được lập trình logic bằng cách sử dụng một vài các ngôn ngữ mô tả phần cứng đã mô tả và được lập trình vào vi mạch tích hợp.

Bộ điều khiển có thể được thực hiện bằng cách sử dụng phương pháp thích hợp bất kỳ. Ví dụ, bộ điều khiển có thể là bộ vi xử lý hoặc bộ xử lý và vật ghi đọc được bằng máy tính lưu trữ mã chương trình đọc được bằng máy tính (như phần mềm hoặc phần sụn) có thể được thực thi bởi bộ vi xử lý hoặc bộ xử lý, cổng logic, bộ chuyển mạch, mạch tích hợp ứng dụng đặc biệt (application-specific intergrated circuit , ASIC), bộ điều khiển logic lập trình được, hoặc bộ vi điều khiển cài sẵn. Các ví dụ về bộ điều khiển bao gồm nhưng không giới hạn ở các bộ vi xử lý sau đây: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20 và Silicone Labs C8051F320. Bộ điều khiển bộ nhớ có thể cũng được thực hiện là một phần của logic điều khiển của bộ nhớ. Người có hiểu biết trung bình về lĩnh vực kỹ thuật cũng biết rằng, ngoài việc thực hiện bộ điều khiển bằng cách sử dụng mã chương trình đọc được bằng máy tính, lập trình logic có thể được thực hiện về các bước của phương pháp cho phép bộ điều khiển thực hiện cùng chức năng ở các dạng cổng logic, bộ chuyển mạch, mạch tích hợp ứng dụng đặc biệt, bộ điều khiển logic lập trình được và bộ vi điều khiển cài sẵn. Do đó, bộ điều khiển có thể được coi là thành phần phần cứng và thiết bị có trong bộ điều khiển và được tạo cấu hình thực hiện các chức năng khác nhau có thể cũng được coi là kết cấu trong thành phần phần cứng. Hoặc thiết bị được tạo cấu hình thực hiện các chức năng khác nhau thậm chí có thể được coi là cả môđun phần mềm thực thi phương pháp và kết cấu trong thành phần phần cứng.

Hệ thống, thiết bị, môđun, hoặc bộ phận được minh họa trong các phương án thực hiện trước có thể được thực hiện bằng cách sử dụng chip máy tính hoặc thực thể, hoặc có thể được thực hiện bằng cách sử dụng sản phẩm có chức năng nhất định. Thiết bị thực hiện điển hình là máy tính. Máy tính có thể ví dụ là máy tính cá nhân, máy tính xách tay, điện thoại di động, điện thoại có lắp camera, điện thoại thông minh, thiết bị hỗ trợ số cá nhân, máy phát đa phương tiện, thiết bị định vị, thiết bị thư điện tử, bảng điều khiển trò chơi, máy tính bảng, thiết bị đeo được, hoặc tổ hợp của thiết bị bất kỳ trong số

các thiết bị này.

Để dễ dàng mô tả, thiết bị trên được mô tả bằng cách chia các chức năng thành các đơn vị khác nhau. Chắc chắn, khi sáng chế được thực thi, các chức năng của các bộ phận có thể được thực hiện ở một hoặc nhiều đoạn phần mềm và/hoặc phần cứng.

Người có hiểu biết trung bình về lĩnh vực kỹ thuật sẽ hiểu rằng theo phương án thực hiện, sáng chế có thể đề xuất phương pháp, hệ thống, hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể chỉ sử dụng dạng phần cứng theo các phương án thực thi, chỉ phần mềm theo các phương án thực thi, hoặc các phương án thực thi với tổ hợp của phần mềm và phần cứng. Thêm nữa, sáng chế có thể sử dụng dạng sản phẩm chương trình máy tính được thực thi trên một hoặc nhiều vật ghi lưu trữ có thể sử dụng được với máy tính (bao gồm nhưng không giới hạn ở bộ nhớ dạng đĩa, CD-ROM, bộ nhớ quang, v.v.) bao gồm mã chương trình sử dụng được 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 vào các phương án thực hiện của sáng chế. Rất đáng lưu ý là, các lệnh chương trình máy tính có thể được sử dụng thực hiện mỗi quy trình và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối và tổ hợp của quy trình và/hoặc khối trong các lưu đồ và/hoặc các sơ đồ khối. Các lệnh chương trình máy tính này có thể được tạo ra cho máy tính mục đích chung, máy tính chuyên dụng, bộ xử lý cài sẵn, hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được 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 khác tạo ra thiết bị để thực thi chức năng cụ thể trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được lưu trữ trong bộ nhớ đọc được bằng máy tính có thể lệnh cho máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác để làm việc theo cách nhất định, sao cho các lệnh được lưu trữ trong bộ nhớ đọc được bằng máy tính tạo ra thành phần lạ gồm thiết bị lệnh. Thiết bị lệnh thực hiện chức năng cụ thể trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được tải lên máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, sao cho một loạt các thao tác và các thao tác và các bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác, nhờ vậy tạo ra việc xử

lý được thực thi bằng máy tính. Do đó, các lệnh được thực thi bằng máy tính hoặc thiết bị lập trình được khác tạo ra các bước để thực thi chức năng cụ thể trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

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

Bộ nhớ có thể bao gồm bộ nhớ không bất biến, bộ nhớ truy cập ngẫu nhiên (random access memory, RAM), bộ nhớ không khả biến, và/hoặc dạng khác ở trong vật ghi đọc được bằng máy tính, ví dụ, bộ nhớ chỉ đọc (read-only memory, ROM) hoặc bộ nhớ nhanh (flash memory). Bộ nhớ là một ví dụ về vật ghi đọc được bằng máy tính.

Vật ghi đọc được bằng máy tính gồm vật ghi bất biến, không bất biến, tháo ra được và không tháo ra được có thể lưu giữ 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 về vật ghi lưu trữ được trên máy tính bao gồm nhưng không giới hạn ở bộ nhớ truy cập ngẫu nhiên tham số (parameter random access memory, PRAM), bộ nhớ truy cập ngẫu nhiên tĩnh (static random access memory, SRAM), bộ nhớ truy cập ngẫu nhiên động (dynamic random access memory, DRAM), loại bộ nhớ truy cập ngẫu nhiên (random access memory, RAM) khác, bộ nhớ chỉ đọc (read-only memory, ROM), bộ nhớ chỉ đọc lập trình được xóa được bằng điện (electrically erasable programmable read-only memory, EEPROM), bộ nhớ nhanh hoặc công nghệ bộ nhớ khác, bộ nhớ chỉ đọc đĩa compact (compact disc read-only memory, CD-ROM), đĩa đa năng kỹ thuật số (digital versatile disc, DVD) hoặc bộ lưu trữ quang khác, băng từ catxet, thiết bị lưu trữ băng từ/đĩa từ hoặc thiết bị lưu trữ từ tính khác, hoặc vật ghi không truyền khác bất kỳ. Vật ghi lưu trữ được trên máy tính có thể được sử dụng để lưu giữ thông tin truy cập được bởi thiết bị điện toán. Dựa vào định nghĩa trong phần 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 và sóng mang dữ liệu được điều biến.

Đáng để lưu ý thêm rằng, các thuật ngữ “bao gồm” hoặc các dạng biến thể khác bất kỳ của thuật ngữ này được dự định bao hàm sự bao gồm không loại trừ, nên quy trình, phương pháp, sản phẩm hoặc thiết bị gồm danh sách các chi tiết không chỉ gồm các chi

tiết này mà còn gồm các chi tiết khác không được liệt kê rõ ràng, hoặc còn gồm các chi tiết vốn có cho quy trình, phương pháp, sản phẩm hoặc thiết bị này. Không có nhiều hạn chế, chi tiết mà đứng trước là “gồm ...” không loại trừ sự xuất hiện thêm của các chi tiết giống nhau trong quy trình, phương pháp, sản phẩm hoặc thiết bị gồm chi tiết này.

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

Sáng chế có thể được mô tả theo ngữ cảnh chung của các lệnh thực thi được bằng máy tính được thực thi bằng máy tính, ví dụ, môđun chương trình. Nói chung, môđun chương trình gồm chương trình con, chương trình, vật, thành phần, cấu trúc dữ liệu, v.v. thực hiện tác vụ cụ thể hoặc thực thi loại dữ liệu ngắn cụ thể. Sáng chế có thể cũng được áp dụng trong thực tế các môi trường điện toán phân tán. Trong các môi trường điện toán phân tán, các tác vụ được thực hiện bởi thiết bị xử lý từ xa được kết nối nhờ mạng truyền thông. Trong môi trường điện toán phân tán, môđun chương trình có thể được đặt ở cả vật ghi lưu trữ trong máy tính nội bộ và từ xa bao gồm các thiết bị lưu trữ.

Các phương án thực thi trong phần mô tả này được mô tả theo cách liên tiếp. Đối với các phần giống nhau hoặc tương tự của các phương án thực thi, có thể tham chiếu đến các phương án thực thi. Mỗi phương án thực hiện tập trung vào sự khác nhau với các phương án thực thi khác. Cụ thể, phương án thực thi của hệ thống về cơ bản tương tự với phương án thực thi của phương pháp và do đó được mô tả ngắn gọn. Đối với các phần liên quan, có thể tham chiếu đến các mô tả liên quan trong phương án thực thi của phương pháp.

Các phương án thực thi trước là các phương án thực hiện của sáng chế và không được dự định giới hạn sáng chế. Người có hiểu biết trung bình về lĩnh vực kỹ thuật có thể tạo ra các cải biến và thay đổi khác nhau với sáng chế. Cải biến, thay thế tương đương hoặc cải tiến bất kỳ được tạo ra mà không tách rời khỏi mục đích và nguyên lý

của sáng chế sẽ nằm trong phạm vi của các điểm yêu cầu bảo hộ trong sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp được thực thi bằng máy tính xác minh đồng thuận, phương pháp được thực thi bằng máy tính này bao gồm các bước:

nhận, bởi nút quy định, yêu cầu giao dịch trong đó yêu cầu giao dịch này bao gồm dữ liệu giao dịch và chữ ký của ít nhất một nút giao dịch, dữ liệu giao dịch bao gồm dữ liệu được chỉ định và dữ liệu không được chỉ định, và dữ liệu được chỉ định bao gồm dữ liệu riêng tư;

xác định số tài sản tương ứng với chữ ký của ít nhất một nút giao dịch trong dữ liệu giao dịch dựa trên chữ ký;

xác định số tài sản như số tài sản được khai báo được sử dụng bởi ít nhất một nút giao dịch;

xác định xem liệu yêu cầu giao dịch có hợp lệ hay không dựa trên dữ liệu giao dịch, chữ ký, và số tài sản, trong đó bước xác định liệu yêu cầu giao dịch có hợp lệ hay không dựa trên dữ liệu giao dịch, chữ ký, và số tài sản bao gồm bước xác định liệu yêu cầu giao dịch có hợp lệ hay không dựa trên việc xác định xem liệu số tài sản được khai báo được sử dụng bởi ít nhất một nút giao dịch có thực sự được sở hữu bởi ít nhất một nút giao dịch hay không;

đáp ứng lại việc xác định rằng yêu cầu giao dịch là hợp lệ, tạo ra bản tóm lược dữ liệu được chỉ định dựa trên dữ liệu được chỉ định có trong dữ liệu giao dịch; và

gửi bản tóm lược dữ liệu được chỉ định và dữ liệu không được chỉ định và không gửi dữ liệu được chỉ định có trong dữ liệu giao dịch tới nút đồng thuận tương ứng, để việc xác minh đồng thuận dữ liệu giao dịch được thực hiện dựa trên bản tóm lược dữ liệu được chỉ định và dữ liệu không được chỉ định.

2. Phương pháp được thực thi bằng máy tính theo điểm 1, phương pháp này còn bao gồm bước:

từ chối yêu cầu giao dịch đáp ứng lại việc xác định rằng yêu cầu giao dịch là không hợp lệ.

3. Phương pháp được thực thi bằng máy tính theo điểm 1, trong đó trước bước xác định liệu yêu cầu giao dịch có hợp lệ hay không bao gồm bước:

thu chứng chỉ số của ít nhất một nút giao dịch.

4. Phương pháp được thực thi bằng máy tính theo điểm 3, trong đó bước xác định liệu yêu cầu giao dịch có hợp lệ hay không bao gồm bước:

xác định liệu yêu cầu giao dịch có hợp lệ hay không dựa trên dữ liệu giao dịch, chữ ký của ít nhất một nút giao dịch, và chứng chỉ số của ít nhất một nút giao dịch.

5. Phương pháp được thực thi bằng máy tính theo điểm 3, trong đó bước xác định liệu yêu cầu giao dịch có hợp lệ hay không bao gồm các bước:

giải mã chữ ký của ít nhất một nút giao dịch dựa trên khóa công khai có trong chứng chỉ số của nút giao dịch;

xác định liệu kết quả giải mã mà tương ứng với ít nhất một nút giao dịch có tương ứng với bản tóm lược của dữ liệu giao dịch hay không;

đáp ứng lại việc xác định rằng kết quả giải mã mà tương ứng với ít nhất một nút giao dịch tương ứng với bản tóm lược của dữ liệu giao dịch, xác định một hoặc nhiều số tài sản mà tương ứng với nhận dạng dựa trên nhận dạng có trong chứng chỉ số của ít nhất một nút giao dịch; và

xác định một hoặc nhiều số tài sản là một hoặc nhiều số tài sản thực sự được sở hữu bởi nút giao dịch.

6. Phương pháp được thực thi bằng máy tính theo điểm 5, phương pháp này còn bao gồm các bước:

xác định liệu yêu cầu giao dịch có hợp lệ hay không dựa trên một hoặc nhiều số tài sản do ít nhất một nút giao dịch sở hữu, chữ ký của ít nhất một nút giao dịch, và dữ liệu giao dịch; hoặc

xác định rằng yêu cầu giao dịch là không hợp lệ đáp ứng lại việc xác định rằng kết quả giải mã mà tương ứng với ít nhất một nút giao dịch là khác với bản tóm lược của dữ liệu giao dịch.

7. Phương pháp được thực thi bằng máy tính theo điểm 6, trong đó bước xác định liệu yêu cầu giao dịch có hợp lệ hay không bao gồm các bước:

xác định rằng nút giao dịch là không hợp lệ đáp ứng lại việc xác định rằng một hoặc nhiều số tài sản do nút giao dịch sở hữu không bao gồm số tài sản được khai báo được sử dụng bởi nút giao dịch; hoặc

xác định rằng nút giao dịch là hợp lệ đáp ứng lại việc xác định rằng một hoặc nhiều số tài sản do nút giao dịch sở hữu bao gồm tất cả số tài sản được khai báo được sử dụng bởi nút giao dịch.

8. Phương pháp được thực thi bằng máy tính theo điểm 1, trong đó bước xác định liệu yêu cầu giao dịch có hợp lệ hay không bao gồm các bước:

xác định rằng yêu cầu giao dịch là không hợp lệ đáp ứng lại việc xác định rằng ít nhất một nút giao dịch là không hợp lệ; hoặc

xác định rằng yêu cầu giao dịch là hợp lệ đáp ứng lại việc xác định rằng tất cả các nút giao dịch được nhận dạng trong yêu cầu giao dịch là hợp lệ.

9. Phương pháp được thực thi bằng máy tính theo điểm 1, phương pháp này còn bao gồm bước:

lệnh cho ít nhất một nút giao dịch lưu trữ dữ liệu giao dịch hoặc dữ liệu được chỉ định có trong dữ liệu giao dịch để đáp ứng lại việc xác định rằng yêu cầu giao dịch là hợp lệ.

10. Phương pháp được thực thi bằng máy tính theo điểm 1, trong đó nút quy định là nút của mạng chuỗi khối được tạo cấu hình để điều chỉnh các giao dịch bằng cách xác minh các mục, trong đó các mục này được xác minh bởi nút quy định được báo nhận bởi các nút chuỗi khối của mạng chuỗi khối.

11. Phương pháp được thực thi bằng máy tính theo điểm 10, trong đó mạng chuỗi khối bao gồm mạng chuỗi khối liên doanh.

12. Thiết bị xác minh đồng thuận, thiết bị này bao gồm các mô đun được tạo cấu hình để thực hiện phương pháp được thực thi bằng máy tính theo điểm bất kỳ trong số các điểm từ 1 đến 11.

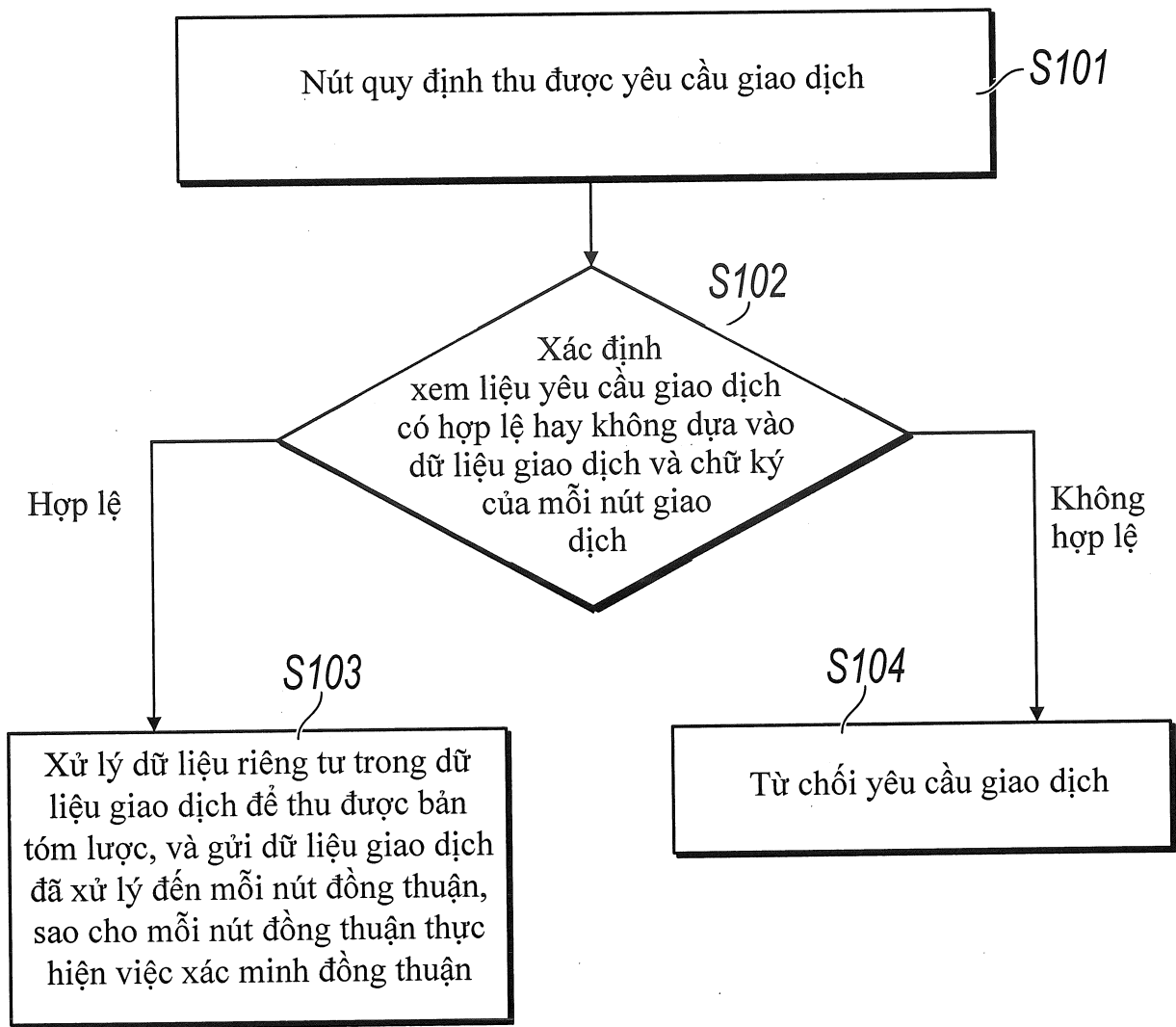
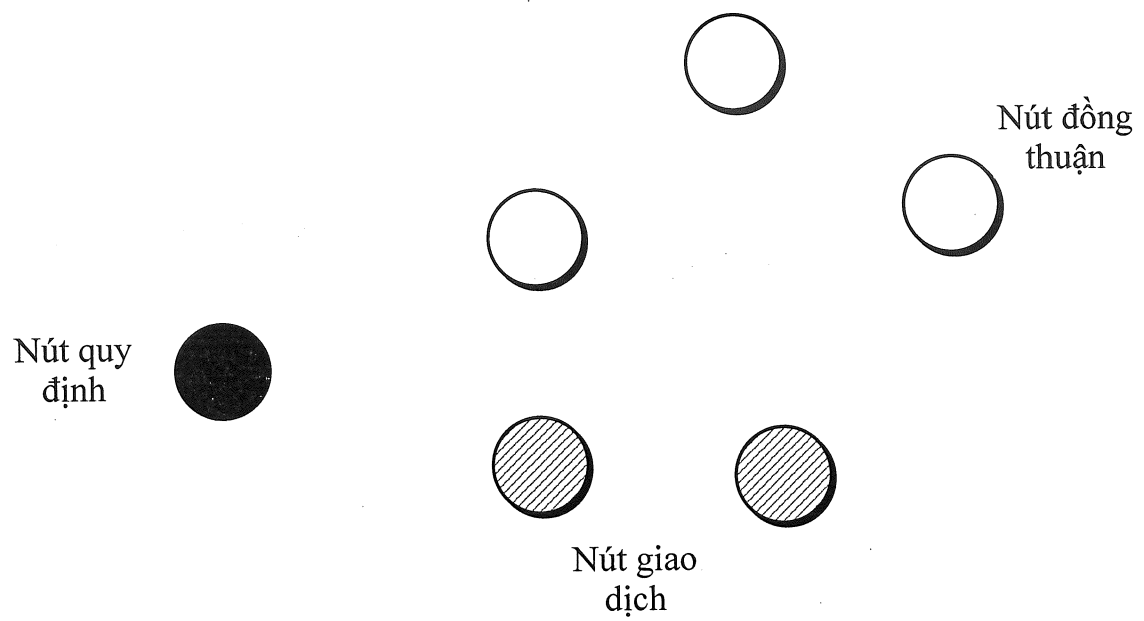


FIG. 1

2 / 4

**FIG. 2**

3 / 4

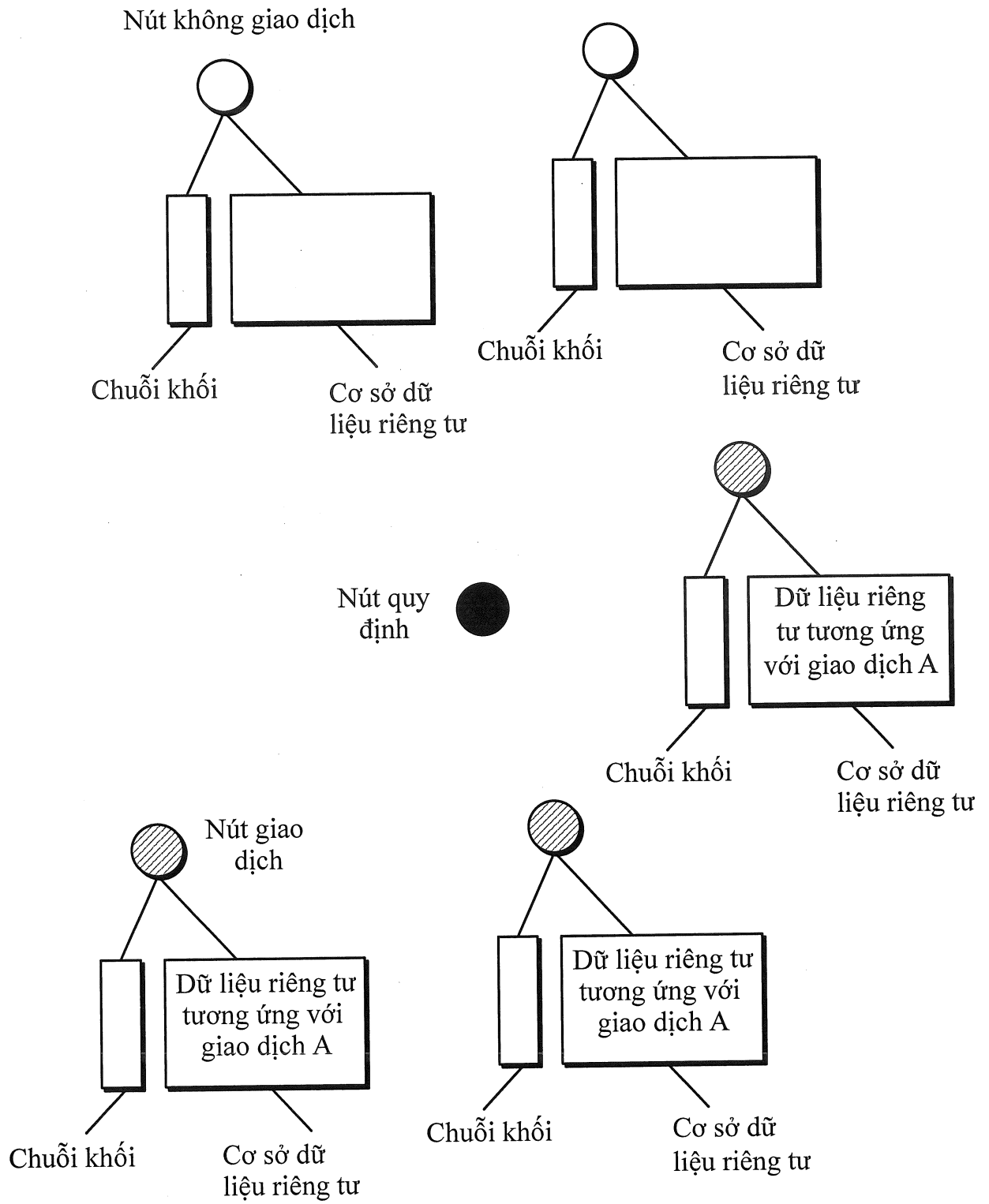
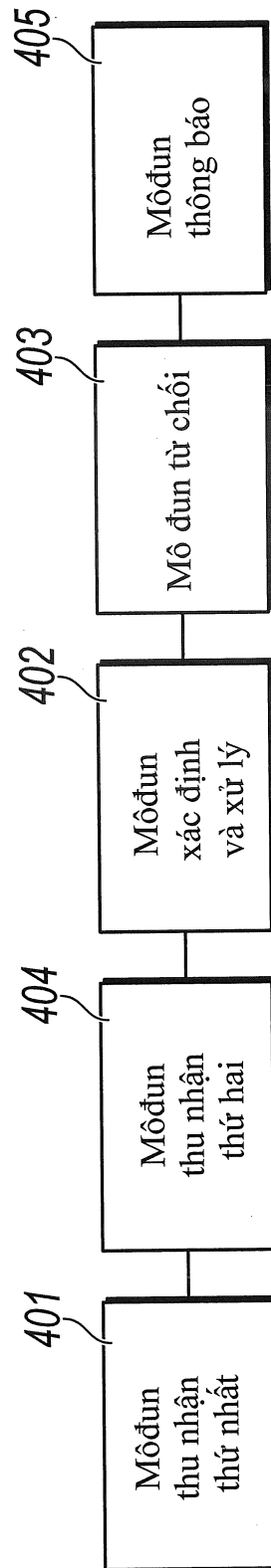


FIG. 3

**FIG. 4**