(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) **1-0037592**

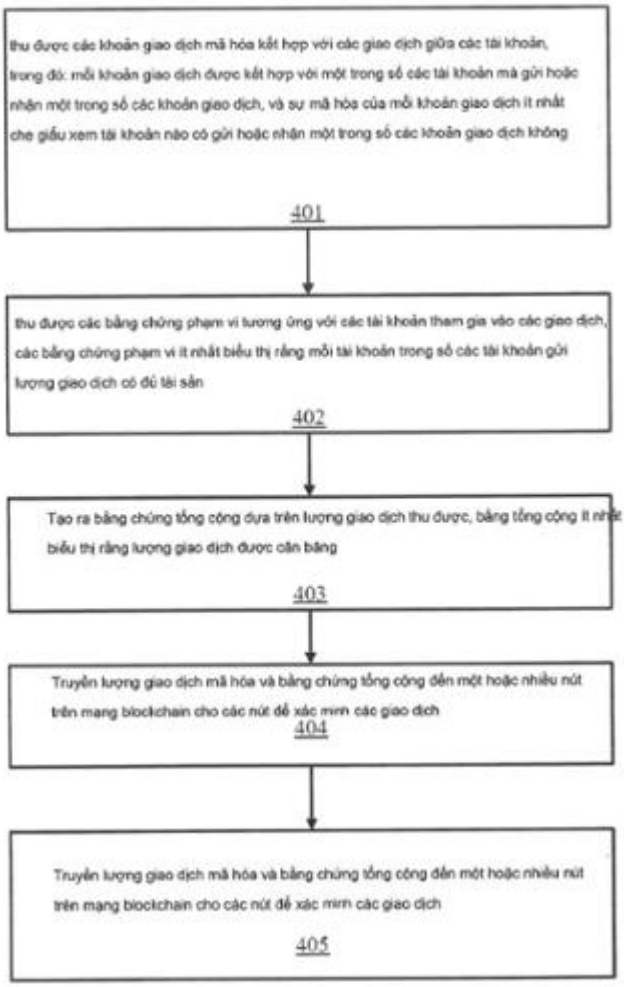
(51)[7] **G06Q 40/04**; H04L 9/32; H04L 29/08; G06Q 20/38; H04L 29/06

(13) **B**

(21) 1-2019-02632
(22) 29/12/2018
(86) PCT/CN2018/125749 29/12/2018
(87) WO/2019/072313 18/04/2019
(45) 27/11/2023 428
(43) 25/07/2019 376A
(73) ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) ZHANG, Wenbin (CN); LI, Lichun (CN); MA, Baoli (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) HỆ THỐNG VÀ PHƯƠNG PHÁP BẢO VỆ THÔNG TIN, VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(57) Sáng chế đề cập đến phương pháp bảo vệ thông tin thực hiện bằng máy tính bao gồm: thu được các khoản giao dịch đã được mã hóa kết hợp với các giao dịch trong số các tài khoản, trong đó mỗi lượng trong số các khoản giao dịch đã được mã hóa được kết hợp với một trong số các tài khoản mà gửi hoặc nhận một trong số các khoản giao dịch, và sự mã hóa của mỗi khoản trong số các khoản giao dịch ít nhất che giấu một tài khoản gửi hoặc nhận một trong số các khoản giao dịch chưa; tạo ra bằng chứng tổng hợp dựa trên các khoản giao dịch đã được mã hóa thu được, bằng chứng tổng hợp ít nhất biểu thị rằng các khoản giao dịch được cân bằng; và truyền các khoản giao dịch đã được mã hóa và bằng chứng tổng hợp đến một hoặc nhiều nút trong mạng blockchain (chuỗi khối) để các nút xác minh các giao dịch.


thu được các khoản giao dịch mã hóa kết hợp với các giao dịch giữa các tài khoản, trong đó, mỗi khoản giao dịch được kết hợp với một trong số các tài khoản mà gửi hoặc nhận một trong số các khoản giao dịch, và sự mã hóa của mỗi khoản giao dịch ít nhất che giấu xem tài khoản nào có gửi hoặc nhận một trong số các khoản giao dịch không
401
thu được các bằng chứng phạm vi tương ứng với các tài khoản tham gia vào các giao dịch, các bằng chứng phạm vi ít nhất biểu thị rằng mỗi tài khoản trong số các tài khoản gửi lượng giao dịch có đủ tài sản
402
Tạo ra bằng chứng tổng cộng dựa trên lượng giao dịch thu được, bằng tổng cộng ít nhất biểu thị rằng lượng giao dịch được cân bằng
403
Truyền lượng giao dịch mã hóa và bằng chứng tổng cộng đến một hoặc nhiều nút trên mạng blockchain cho các nút để xác minh các giao dịch
404
Truyền lượng giao dịch mã hóa và bằng chứng tổng cộng đến một hoặc nhiều nút trên mạng blockchain cho các nút để xác minh các giao dịch
405

Lĩnh vực kỹ thuật được đề cập

Nói chung sáng chế đề cập đến các công nghệ máy tính, và cụ thể là, đến các hệ thống và phương pháp để bảo vệ thông tin.

Tình trạng kỹ thuật của sáng chế

Quyền riêng tư là điều quan trọng đối với các truyền thông và truyền dữ liệu giữa các người dùng khác nhau. Ví dụ, thông tin về bên gửi, bên nhận, và khoản giao dịch giữa các bên là phần quan trọng của bảo vệ quyền riêng tư. Nếu không được bảo mật, người dùng có thể gặp rủi ro là bị đánh cắp thông tin nhận dạng, truyền dữ liệu trái phép, hoặc các nguy cơ bị đánh cắp thông tin khác. Rủi ro càng lớn hơn khi truyền thông và truyền dữ liệu được thực hiện trực tuyến, do khả năng truy cập không giới hạn của thông tin trực tuyến.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất các khía cạnh khác nhau bao gồm hệ thống, phương pháp, và phương tiện đọc được bằng máy tính bất chuyển tiếp để bảo vệ thông tin.

Theo một khía cạnh, phương pháp thực hiện bằng máy tính để bảo vệ thông tin bao gồm các bước: thu được các khoản giao dịch đã được mã hóa kết hợp với các giao dịch trong số các tài khoản, trong đó mỗi khoản trong số các khoản giao dịch đã được mã hóa được kết hợp với một trong số các tài khoản mà gửi hoặc nhận một trong số các khoản giao dịch, và sự mã hóa của mỗi khoản trong số các khoản giao dịch ít nhất che giấu một tài khoản gửi hoặc nhận một trong số các khoản giao dịch chưa; tạo ra bằng chứng tổng hợp dựa trên các khoản giao dịch đã được mã hóa thu được, bằng chứng tổng hợp ít nhất biểu thị rằng các khoản giao dịch được cân bằng; và truyền các khoản giao dịch đã được mã hóa và bằng chứng tổng hợp đến một hoặc nhiều nút trong mạng blockchain (chuỗi khối) để các nút xác minh các giao dịch.

Theo một số phương án, sự mã hóa của mỗi khoản giao dịch trong số các khoản giao dịch ít nhất che giấu một tài khoản gửi hoặc nhận một trong số các khoản giao dịch

chưa bằng cách ẩn đi xem mỗi khoản giao dịch trong số các khoản giao dịch đi vào hoặc đi ra một tài khoản hay chưa.

Theo một số phương án, trước khi tạo ra bằng chứng tổng hợp, phương pháp còn bao gồm: thu được các bằng chứng phạm vi tương ứng cho các tài khoản liên quan đến các giao dịch, các bằng chứng phạm vi ít nhất biểu thị rằng mỗi tài khoảng trong số các tài khoản mà gửi các khoản giao dịch có đủ tài sản.

Theo một số phương án, trước khi truyền các khoản giao dịch đã được mã hóa và bằng chứng tổng hợp tới một hoặc nhiều nút, phương pháp còn bao gồm: thu được các chữ ký tương ứng từ các tài khoản. Bước truyền các khoản giao dịch đã được mã hóa và bằng chứng tổng hợp tới một hoặc nhiều nhút trong mạng blockchain để các nút xác minh các giao dịch bao gồm truyền các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký tới một hoặc nhiều nhút trong mạng blockchain để các nút xác minh các giao dịch dựa trên các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký.

Theo một số phương án, truyền các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký tới một hoặc nhiều nút trong mạng blockchain để các nút xác minh các giao dịch dựa trên các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký bao gồm: truyền các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký tới một hoặc nhiều nút trong mạng blockchain; và khiến các nút: thẩm định các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký, thực thi các giao dịch đáp lại với việc xác minh các giao dịch thành công, và bổ sung các giao dịch vào khối dữ liệu mới của blockchain mà được duy trì bởi mạng blockchain.

Theo một số phương án, khiến các nút thực thi các giao dịch đáp lại với việc xác minh các giao dịch thành công bao gồm: khiến các nút trừ đi các khoản giao dịch đã được mã hóa một cách tương ứng từ số dư tài khoản đã được mã hóa của các tài khoản đáp lại với việc xác minh các giao dịch thành công.

Theo một số phương án, sự mã hóa của mỗi khoản giao dịch trong số các khoản giao dịch bao gồm sự mã hóa đồng hình.

Theo một số phương án, sự mã hóa của mỗi khoản giao dịch trong số các khoản giao dịch bao gồm lược đồ cam kết Pedersen.

Theo khía cạnh khác, hệ thống bảo vệ thông tin bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ đọc được bằng máy tính bất chuyển tiếp mà được nối với một\ hoặc nhiều bộ xử lý và được cấu hình bằng các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để làm cho hệ thống thực hiện các hoạt động bao gồm: thu được các khoản giao dịch đã được mã hóa kết hợp với các giao dịch trong số các tài khoản, trong đó mỗi lượng trong số các khoản giao dịch đã được mã hóa được kết hợp với một trong số các tài khoản mà gửi hoặc nhận một trong số các khoản giao dịch, và sự mã hóa của mỗi khoản trong số các khoản giao dịch ít nhất che giấu một tài khoản gửi hoặc nhận một trong số các khoản giao dịch chưa; tạo ra bằng chứng tổng hợp dựa trên các khoản giao dịch đã được mã hóa thu được, bằng chứng tổng hợp ít nhất biểu thị rằng các khoản giao dịch được cân bằng; và truyền các khoản giao dịch đã được mã hóa và bằng chứng tổng hợp đến một hoặc nhiều nút trong mạng blockchain để các nút xác minh các giao dịch.

Theo khía cạnh khác, phương tiện lưu trữ đọc được bằng máy tính bất chuyển tiếp được cấu hình bằng các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để làm cho một hoặc nhiều bộ xử lý thực hiện các hoạt động bao gồm: thu được các khoản giao dịch đã được mã hóa kết hợp với các giao dịch trong số các tài khoản, trong đó mỗi lượng trong số các khoản giao dịch đã được mã hóa được kết hợp với một trong số các tài khoản mà gửi hoặc nhận một trong số các khoản giao dịch, và sự mã hóa của mỗi khoản trong số các khoản giao dịch ít nhất che giấu một tài khoản gửi hoặc nhận một trong số các khoản giao dịch chưa; tạo ra bằng chứng tổng hợp dựa trên các khoản giao dịch đã được mã hóa thu được, bằng chứng tổng hợp ít nhất biểu thị rằng các khoản giao dịch được cân bằng; và truyền các khoản giao dịch đã được mã hóa và bằng chứng tổng hợp đến một hoặc nhiều nút trong mạng blockchain để các nút xác minh các giao dịch.

Các dấu hiệu này và các dấu hiệu khác của các hệ thống, phương pháp và phương tiện đọc được bằng máy tính bất chuyển tiếp, đã được bộc lộ trong sáng chế này, cũng như các phương pháp hoạt động và các chức năng của các thành phần cấu trúc liên quan và sự kết hợp của các phần và các yếu tố hài hòa trong sản xuất, sẽ trở nên rõ ràng hơn

khi xem xét phần mô tả dưới đây và các yêu cầu bảo hộ kèm theo có tham chiếu đến các hình vẽ đi kèm, tất cả tạo nên một phần của phần mô tả, trong đó các số chỉ dẫn là để chỉ các bộ phận tương ứng trong các hình vẽ. Tuy nhiên, cần hiểu rằng các hình vẽ chỉ nhằm mục đích minh hoạ và mô tả mà không nhằm giới hạn sáng chế.

Mô tả vắn tắt các hình vẽ

Các dấu hiệu nhất định của các phương án khác nhau của sáng chế được nêu ở các điểm yêu cầu bảo hộ kèm theo. Các dấu hiệu và các ưu điểm của sáng chế sẽ được hiểu rõ hơn dựa vào phần mô tả chi tiết sau đây mà mô tả các phương án minh hoạ, trong đó các nguyên lý theo sáng chế được sử dụng, và các hình vẽ kèm theo, trong đó:

FIG. 1 là hình vẽ minh họa blockchain làm ví dụ, kết hợp với các phương án thực hiện khác nhau;

FIG. 2 là hình vẽ minh họa mạng blockchain làm ví dụ để bảo vệ thông tin, kết hợp với các phương án thực hiện khác nhau;

FIG. 3 là hình vẽ minh họa luồng thực thi giao dịch làm ví dụ với các người gửi và người nhận hòa lẫn, kết hợp với các phương án thực hiện khác nhau;

FIG. 4 là hình vẽ minh họa lưu đồ của phương pháp làm ví dụ để bảo vệ thông tin, kết hợp với các phương án thực hiện khác nhau;

FIG. 5 là hình vẽ minh họa lưu đồ của phương pháp làm ví dụ khác để bảo vệ thông tin, kết hợp với các phương án thực hiện khác nhau;

FIG. 6 là hình vẽ minh họa lưu đồ của phương pháp làm ví dụ để bảo vệ thông tin, kết hợp với các phương án thực hiện khác nhau; và

FIG. 7 là hình vẽ minh họa sơ đồ khối của hệ thống máy tính làm ví dụ trong đó phương án thực hiện bất kỳ trong số các phương án thực hiện đã được mô tả ở đây có thể được thực hiện.

Mô tả chi tiết sáng chế

Phần mô tả dưới đây được thực hiện cho các phương án thực hiện làm ví dụ, các ví dụ của chúng được minh họa trên các hình vẽ kèm theo. Phần mô tả sau đây tham chiếu đến các hình vẽ kèm theo trong đó các số chỉ dẫn giống nhau trên các hình vẽ khác nhau biểu thị các phần tử giống hoặc tương tự nhau trừ khi có mô tả khác. Các

phương án thực hiện đã được đưa ra trong phần mô tả sau đây của các phương án thực hiện làm ví dụ thống nhất với sáng chế không thể hiện tất cả các phương án thực hiện thống nhất với sáng chế. Thay vào đó, sáng chế chỉ thể hiện các ví dụ về các hệ thống và phương pháp thống nhất với các khía cạnh liên quan đến sáng chế.

Công nghệ blockchain có thể được xây dựng trên mạng điểm-điểm (ngang hàng), nhờ sử dụng thuật toán đồng thuận nút phân bố để thẩm định và cập nhật dữ liệu. Blockchain cũng có thể sử dụng mật mã để đảm bảo tính bảo mật của hoạt động truyền và truy nhập dữ liệu, và sử dụng các hợp đồng thông minh bao gồm mã script tự động cho chương trình và dữ liệu xử lý. Một blockchain có thể bao gồm dãy các khối dữ liệu mà mỗi thiết bị bao gồm tiêu đề mà liên kết với khối dữ liệu trước đó, do vậy tạo ra chuỗi của các khối dữ liệu. Để thành lập liên kết, tiêu đề của khối dữ liệu hiện tại có thể bao gồm băm hoặc tổng kiểm tra mật mã của tiêu đề của khối dữ liệu trước đó. mạng blockchain có thể tạo điều kiện thuận lợi cho việc thực thi các giao dịch. Giao dịch nói đến truyền thông bất kỳ giữa các người dùng (các nút người dùng như các thiết bị điện toán của họ) hoặc giữa người dùng và tổ chức tài chính. Ví dụ, giao dịch có thể nói đến mua hoặc bán hàng hóa hoặc dịch vụ, cung cấp hoặc trả lại hàng hóa hoặc dịch vụ, giao dịch trả tiền, giao dịch cho nợ, hoặc các giao dịch tương tự khác. Giao dịch cũng có thể được gọi là "thương mại" hoặc "giao dịch điện tử." Đối tượng của giao dịch có thể bao gồm, ví dụ, tiền mặt, thẻ bài, tiền kỹ thuật số, hợp đồng, chứng thư, hồ sơ bệnh án, chi tiết khách hàng, cổ phần, trái phiếu, vốn chủ sở hữu, hoặc tài sản khác bất kỳ mà có thể được thể hiện dưới dạng kỹ thuật số.

Blockchain có thể được xem là bằng chứng chống làm giả, cổ phiếu, và sổ cái kỹ thuật số để ghi lại các giao dịch trong mạng ngang hàng công khai hoặc riêng tư. Sổ cái (trong kế toán) được phân bố đến các nút thành viên trong mạng, và lịch sử của các giao dịch tài sản xảy ra trên mạng được ghi lại trong blockchain. Do sổ cái blockchain là công khai và sổ cái tự nó không có chức năng bảo vệ quyền riêng tư, thông tin giao dịch quan trọng trong sổ cái được bộc lộ công khai và có nguy cơ bị sử dụng trái phép hoặc sử dụng với mục đích xấu. Ví dụ, trong mạng lưới giao dịch blockchain đang tồn tại, các giao dịch cần biểu thị rõ ràng bên nào sẽ gửi tài sản, bên nào sẽ nhận tài sản, và lượng tài sản giao dịch, không bên nào được bảo mật. Để ít nhất làm giảm bớt các thiếu sót trong các công nghệ hiện có và cải thiện chức năng bảo vệ thông tin của các máy

tính, các hệ thống và phương pháp để bảo vệ thông tin được bộc lộ có tham chiếu đến các hình vẽ từ Fig.1 đến Fig.7.

FIG. 1 là hình vẽ minh họa blockchain làm ví dụ, kết hợp với các phương án thực hiện khác nhau. Như được thể hiện trên Fig.1, blockchain 100 có thể bao gồm nhiều khối dữ liệu 102. Mỗi khối 102 là cấu trúc dữ liệu để chứa dữ liệu 104 bao gồm, ví dụ, các giao dịch, các biên nhận thanh toán, v.v. Mỗi khối có thể liên kết với khối trước đó thông qua băm mật mã. Ví dụ, khối 2 được liên kết với khối 1 thông qua băm 106 của khối 1, khối n được liên kết với khối n-1 thông qua băm khác của khối n-1. Khi dữ liệu mới được gửi và thẩm định, các khối bổ sung chứa dữ liệu mới có thể được tạo ra và gắn với khối cuối cùng của blockchain 100 bằng cách chứa băm của khối trước đó.

FIG. 2 là hình vẽ minh họa mạng blockchain làm ví dụ 200 để thực hiện các giao dịch, kết hợp với các phương án thực hiện khác nhau. Như được thể hiện trên Fig.2, mạng blockchain 200 có thể bao gồm các nút 202 và một hoặc nhiều thiết bị điện toán người dùng 240, mà có thể truyền thông giữa chúng với nhau thông qua một hoặc nhiều con đường truyền thông. Con đường truyền thông làm ví dụ là mạng 220 (ví dụ, các kết nối có dây hoặc không dây, trên internet, v.v.) mà sử dụng một hoặc nhiều giao thức truyền thông, ví dụ, mạng tế bào, WiFi, và các giao thức truyền thông khác, để truyền và thu dữ liệu. Mạng 220 có thể dựa trên mô hình ngang hàng và/hoặc mô hình máy khách/máy chủ. Theo một số phương án, các nút 202 có thể bao gồm các thiết bị điện toán mà mỗi thiết bị bao gồm một hoặc nhiều bộ xử lý 204 và một hoặc nhiều bộ nhớ 206 (ví dụ, một hoặc nhiều phương tiện lưu trữ đọc được bằng máy tính bất chuyển tiếp để lưu trữ các lệnh) mà được nối với một\ hoặc nhiều bộ xử lý 204. Nút 202 có thể là hệ thống làm ví dụ để tăng cường tính bảo mật của hợp đồng thông minh. Một hoặc nhiều bộ nhớ có thể được cấu hình bằng các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để làm cho hệ thống (ví dụ, một hoặc nhiều bộ xử lý) thực hiện các hoạt động đã được mô tả ở đây. Theo một số phương án, bộ xử lý 204 có thể được thực hiện một phần hoặc toàn bộ như một hoặc nhiều mạch logic. Theo một số phương án, các nút 202 và các thiết bị điện toán người dùng 240 có thể bao gồm các nguồn tài nguyên điện toán khác và/hoặc có truy nhập (ví dụ, thông qua một hoặc nhiều kết nối/mạng) vào các nguồn tài nguyên điện toán khác.

Theo một số phương án, blockchain 100 được lưu trữ theo dạng phi tập trung trên các nút 202. Theo một số phương án, một số nút trong số các nút 202 có thể thẩm định các giao dịch mà chúng thu được thông qua các giao dịch đồng thuận và lan truyền đã được thẩm định đến các nút khác 202. Theo đó, các nút 202 có thể cập nhật sổ cái 208 theo các giao dịch đã được thẩm định. Các nút 202 có thể truyền thông với nhau qua mạng 220 để truyền và thu dữ liệu liên quan đến sổ cái 208. Sổ cái 208 bao gồm các khối dữ liệu 102 mà đã được thẩm định và thêm vào blockchain 100. Khi các khối dữ liệu mới được thêm vào sổ cái 208, các nút 202 có thể truyền thông hoặc chia sẻ các khối dữ liệu mới qua mạng 220. Bộ nhớ 206 của các nút 202 có thể lưu trữ ít nhất một phần của sổ cái 208 của blockchain 100.

Theo một số phương án, một hoặc nhiều người dùng có thể gửi các giao dịch tới một hoặc nhiều nhút 202 nhờ các thiết bị điện toán người dùng 240 qua các con đường truyền thông 220. Theo một số phương án, các giao dịch đã được gửi có thể được lưu trữ tạm thời trong bộ nhớ chéo vùng khu trú 206 ở các nút 202 hoặc trong cơ sở dữ liệu từ xa mà có thể truy cập qua mạng 220. Một hoặc nhiều nút trong số các nút 202 có thể lấy các giao dịch đã được gửi từ vùng và xử lý các giao dịch đã được gửi. Để cho thuận tiện và đơn giản, sáng chế có thể sử dụng dạng số ít của nút 202. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật nên hiểu rõ rằng mạng blockchain có thể có nhiều nút 202 và một hoặc nhiều nút 202 có thể được tham gia vào xử lý một giao dịch. Dạng số ít của nút 202 có thể thể hiện một hoặc nhiều nút.

Theo một số phương án, nút 202 có thể cập nhật blockchain 100 dựa trên các kết quả của các giao dịch. Theo một số phương án, giao dịch có thể liên quan đến hai hoặc nhiều người tham gia (còn được gọi là các bên hoặc người dùng như người gửi và người nhận). Giao dịch có thể là thỏa thuận giữa hai bên để trao đổi (các) tài sản. Ví dụ, giao dịch có thể bao gồm một bên sẽ chuyển hoặc thanh toán lượng tài sản cho bên kia, và lượng thanh toán có thể được đồng ý ngay bởi cả hai bên. Tài sản có thể dưới dạng tiền kỹ thuật số, ví dụ, Bitcoin, Monero, v.v. Theo cách khác tài sản có thể là tiền truyền thống, như đô la. Các bên của các giao dịch có thể được kết hợp với các tài khoản tương ứng. Mỗi tài khoản của các bên có thể có địa chỉ và số dư lưu trữ trong blockchain 100. Do vậy, sau khi giao dịch được thực hiện, nút 202 có thể cập nhật số dư của mỗi tài khoản của các bên.

Theo một số phương án, nút 202 có thể thực thi giao dịch mà không biết bên nào là người gửi gửi hoặc trả tài sản và bên nào là người nhận mà nhận tài sản. Các hệ thống và phương pháp đã được bộc lộ có thể ẩn đi thông tin liên quan đến bên nào là người gửi và bên nào là người nhận nhưng vẫn cho phép giao dịch blockchain sẽ được xử lý. Theo một số phương án, lượng tài sản sẽ được giao dịch có thể được dán nhãn là dương hoặc âm để biểu thị xem bên kết hợp với lượng tài sản là người gửi hoặc người nhận. Ví dụ, trong giao dịch giữa bên A và bên B, lượng $1,000 (dương) cho A biểu thị rằng bên A gửi $1,000 đến bên B, trong khi lượng -$1,000 (âm) cho A biểu thị rằng bên A nhận $1,000 từ bên B. Do đó, nếu khoản giao dịch của tài khoản A lớn hơn không, tài khoản A sẽ trả hoặc gửi đi khoản giao dịch đến B khác, và do vậy tài khoản A này là người gửi. Ngược lại, nếu khoản giao dịch của tài khoản A nhỏ hơn không (âm), thì tài khoản A sẽ nhận lượng giao dịch, và tài khoản A là người nhận.

Theo một số phương án, khoản giao dịch có thể được mã hóa thông qua các phương pháp mã hóa khác nhau. Theo một ví dụ, khoản giao dịch có thể được mã hóa thông qua sự mã hóa đồng hình. Lược đồ mã hóa đồng hình có thể bao gồm, nhưng không bị giới hạn ở, sự mã hóa đồng hình Elgamal,, sự mã hóa đồng hình Paillier, sự mã hóa đồng hình Benaloh, Sự mã hóa đồng hình Okamoto-Uchiyama, sự mã hóa đồng hình Naccache-Stern, sự mã hóa đồng hình Damgård-Jurik, sự mã hóa đồng hình Boneh-Goh-Nissim, v.v. Theo ví dụ khác, khoản giao dịch có thể được mã hóa thông qua lược đồ cam kết như cam kết đồng hình. Ví dụ, cam kết đồng hình có thể là cam kết Pedersen. Cam kết Pedersen "T" của khoản giao dịch "t" có thể được biểu diễn như sau.

$$T = PC(r, t) = rG + tH,$$

trong đó r là nhân tố mù ngẫu nhiên (được gọi theo cách khác là nhân tố mù) để tạo ra sự che giấu, G và H là các bộ tạo đồng ý công khai hoặc các điểm cơ sở của đường cong elip và có thể được chọn ngẫu nhiêu. Ví dụ, r có thể là số ngẫu nhiên. G và H có thể được biết là các thông số cho nút 202. Lược đồ cam kết duy trì sự bảo mật dữ liệu nhưng cam kết đối với dữ liệu sao cho nó không thể được thay đổi sau đó bởi người gửi dữ liệu. Bên nhận cam kết (ví dụ, người nhận nút của giao dịch) chỉ biết giá trị cam kết (ví dụ, PC(r, t)), bên này không thể xác định giá trị dữ liệu ưu tiên nào (ví dụ, t) được cam kết do sự có mặt của nhân tố mù ngẫu nhiên (ví dụ, r). Tuy nhiên, nút 202 nhận

cam kết có thể chạy cam kết và chứng thực rằng dữ liệu cam kết trùng khớp với dữ liệu nhận. Theo cách này, bằng cách che giấu các vai trò (ví dụ, người gửi, hoặc người nhận) của các bên cũng như bằng cách mã hóa khoản giao dịch, tổ chức bên thứ ba sẽ không biết bên nào là người gửi và bên nào là người nhận, nhờ đó bảo vệ sự riêng tư của các bên trong giao dịch.

Cam kết Pedersen có thuộc tính bổ sung là: những sự cam kết có thể được bổ sung, và tổng của tập hợp những cam kết là giống như sự cam kết đối với tổng dữ liệu (với một khoá mù được thiết đặt dưới dạng tổng các khoá mù): $\mathrm{PC}(r_1, t_1) + \mathrm{PC}(r_2, t_2) = PC(r_1 + r_2, t_1 + t_2)$. Nói cách khác, sự cam kết bảo tồn tính cộng và thuộc tính giao hoán áp dụng, tức là, cam kết Pedersen là đồng hình có tính cộng, ở chỗ dữ liệu nằm dưới có thể được vận dụng về mặt toán học như thể nó không bị mã hoá. Do đó, khi áp dụng cam kết Pedersen vào khoản giao dịch và số dư của bên giao dịch, số dư có thể được cập nhật nhờ sử dụng khoản giao dịch bằng cách bổ sung trực tiếp các cam kết Pedersen, mà không giải mã các cam kết Pedersen của khoản giao dịch và/hoặc số dư.

Theo một số phương án, nút 202 có thể thực thi nhiều giao dịch như một phương án thực hiện đã được mô tả trên đây theo đợt. Ví dụ, bên cạnh các giao dịch giữa bên A và bên B, bên C và bên D cũng có thể yêu cầu các giao dịch giữa họ. Ngoài ra, bên E và bên F cũng có thể yêu cầu chuyển tài sản giữa mỗi bên. Các giao dịch giữa bên A và bên B có thể được hòa trộn với các giao dịch giữa bên C và bên D và giữa bên E và bên F. Nút 202 có thể thực thi các giao dịch trong số các bên A, B, C, D, E, và F ở một thời điểm mà không cần sự biểu thị rõ ràng của các người gửi và người nhận tương ứng. Trong trường hợp phức tạp hơn, nút 202 có thể thực thi nhiều giao dịch trong đó một bên (ví dụ, bên A) để đưa các khoản giao dịch khác nhau của tài sản đến các bên khác nhau (ví dụ, bên B, bên C, v.v.).

Tham chiếu đến Fig.3, luồng thực thi giao dịch làm ví dụ 300 với các người gửi và người nhận hòa lẫn được minh họa kết hợp với các phương án thực hiện khác nhau. Luồn thực thi giao dịch 300 có thể được thực hiện trong các hệ thống khác nhau bao gồm, ví dụ, mạng blockchain 200 trên Fig.2. Luồn thực thi giao dịch 300 có thể được thực hiện bằng một hoặc nhiều nút trong số các nút 202 và các thiết bị điện toán người dùng 240. Các hoạt động của luồng thực thi giao dịch 300 mà được thể hiện dưới đây

là nhằm mục đích minh họa. Tùy theo phương án thực hiện, luồng thực thi giao dịch làm ví dụ 300 có thể bao gồm các bước bổ sung, loại bỏ hoặc thay thế được thực hiện theo các thứ tự khác nhau hoặc song song.

Theo hình vẽ được minh họa trên Fig.3, những người tham gia của một hoặc nhiều giao dịch và các tài khoản liên kết của họ được thể hiện trong khối 302. Ví dụ, mỗi người tham gia trong số những người tham gia có thể được kết hợp với tài khoản "Tài khoản A_i," trong đó $1 \leq i \leq n$, và n có thể là số nguyên dương bất kỳ. Theo một số phương án, n có thể biểu thị tổng số lượng người tham gia. Theo các phương án thực hiện khác, i có thể không là các số nguyên liên tiếp, và do vậy n có thể không biểu thị tổng số lượng người tham gia. Như được thể hiện ở khối 302, mỗi tài khoản trong số các tài khoản "Tài khoản A_i" có thể bao gồm số dư "s_i," mà có thể là lượng tài sản trong tài khoản có sẵn "Tài khoản A_i." Theo một số phương án, số dư "s_1" có thể dưới dạng tiền kỹ thuật số, ví dụ, Bitcoin, v.v. Theo cách khác số dư "s_1" có thể biểu diễn tiền truyền thống. Ngoài ra, như được thể hiện ở khối 302, số dư "s_i" có thể được mã hóa để thu được số dư mã hóa "S_i" thông qua một hoặc nhiều sự mã hóa đồng hình hoặc các lược đồ cam kết đồng hình như được mô tả bên trên. Số dư mã hóa "S_i" có thể là văn bản mã hóa của số dư "s_i" và được gọi là "HE(s_i)." Do đó, S_i = HE(s_i), trong đó $1 \leq i \leq n$, và n có thể là số nguyên dương bất kỳ. Ví dụ, tài khoản "Tài khoản A_1" bao gồm văn bản mã hóa của số dư "s_1" của nó biểu diễn bởi "S_1," trong đó S_1 = HE(s_1). Theo một số phương án, số dư mã hóa "S_i" là cam kết Pedersen, và $HE(s\_i) = r\_i * G + s\_i * H$, trong đó r là nhân tố mù ngẫu nhiên.

Ở khối 304, nhiều giao dịch từ các tài khoản "Tài khoản A_i" của những người tham gia có thể được nhận bởi nút 202. Theo hình vẽ được minh họa trên Fig.3, mỗi tài khoản có thể được kết hợp với số nhận diện tài khoản (ID) như "A_i," khoản giao dịch "t_i," bằng chứng phạm vi "Pf_i," và chữ ký "Sig_i." "Chữ ký" thể hiện sự thẩm định từ danh tính thực. Thuật ngữ "chữ ký" có thể là dạng biểu thị bất kỳ của sự thẩm định. Ví dụ, chữ ký kết hợp với giao dịch từ tài khoản thể hiện rằng tài khoản thẩm định giao dịch. Theo một số phương án, các giao dịch có thể được mã hóa để che giấu ít nhất danh tính của người gửi hoặc người nhận của mỗi giao dịch trong số các các giao dịch. Ví dụ, các giao dịch có thể bao gồm văn bản mã hóa của khoản giao dịch thực của mỗi giao dịch, được biểu diễn là "T_i," trong đó $T\_i = HE(t\_i)$. Văn bản mã hóa của khoản

giao dịch có thể được tạo ra thông qua sự mã hóa đồng hình hoặc các lược đồ cam kết đồng hình nêu trên. Ví dụ, khoản giao dịch đã được mã hóa "T_i" có thể là cam kết Pedersen của khoản giao dịch thực "t_i."

Bằng chứng phạm vi có thể là giao thức bằng chứng bảo đảm được sử dụng để chứng minh rằng số lượng nằm trong phạm vi, đồng thời không để lộ thông tin khác về số lượng, như trị số số lượng thực. Ví dụ, bằng chứng phạm vi có thể được tạo ra thông qua các lược đồ bao gồm, ví dụ, lược đồ chữ ký vòng Borromean, lược đồ chống xuyên thủng, v.v. Các lược đồ khác cũng có thể được sử dụng để tạo ra bằng chứng phạm vi. Bằng chứng phạm vi "Pf_i" có thể thể hiện rằng tài khoản "A_i" có đủ số dư để thực hiện giao dịch, ví dụ, số dư của tài khoản "s_i" là lớn hơn hoặc bằng trị số tuyệt đối của khoản giao dịch "t_i." Bằng chứng phạm vi "Pf_i" của tài khoản "A_i" có thể được biểu diễn bởi $Pf\_i = Pf(s_i - t_i \geq 0)$.

Theo một số phương án, bằng chứng khác, ví dụ, $Pf\_sum = Pf(t\_1 + t\_2 + \cdots + t\_n = 0)$, có thể được tạo ra ngay trên các giao dịch. Sau đây, bằng chứng này có thể được gọi là bằng chứng tổng hợp, mà được sử dụng để thể hiện rằng tổng cộng của các khoản giao dịch được cân bằng, ví dụ, bằng không. Như được mô tả bên trên, khoản giao dịch của người gửi có thể được biểu thị là giá trị dương, trong khi khoảng giao dịch của người nhận tương ứng có thể được biểu thị là giá trị âm. Các giá trị tuyệt đối của các khoản giao dịch kết hợp với người gửi và người nhận tương ứng là bằng nhau. Theo cách này, nút 202 có thể thực thi giao dịch giữa người gửi và người nhận mà không cần sự biểu thị rõ ràng của bên nào là người gửi và bên nào là người nhận.

Theo ví dụ đã được mô tả trên đây trong đó A cần thanh toán $1,000 cho bên B, giả sử rằng A được kết hợp với ID tài khoản "A_1" trong khi bên B được kết hợp với ID tài khoản "A_2," khoản giao dịch "t_1" kết hợp với "A_1" là +$1,000, trong khi khoản giao dịch "t_2" kết hợp với "A_2" là -$1,000. bằng chứng tổng hợp "Pf_sum" có thể được tạo ra để thể hiện rằng khoản giao dịch "t_1" và khoản giao dịch "t_2" chênh lệch với nhau, và tổng cộng của các khoản giao dịch "t_1" và "t_2" bằng không.

Theo một số phương án, bằng chứng tổng hợp "Pf_sum" có thể được chứng minh dựa trên khoản giao dịch đã được mã hóa $HE(t_i)$. Ví dụ, văn bản mã hóa của khoản giao dịch $HE(t\_i)$ có thể được biểu diễn bởi $HE(t\_i) = G^{\{t\_i\}} * H^{\{r\_i\}}$, trong đó r_i là nhân tố mù ngẫu nhiên, G và H là các bộ tạo đồng ý công khai hoặc các điểm cơ

sở của đường cong elip và có thể được chọn ngẫu nhiêu. Do đó, bằng chứng tổng hợp "Pf_sum" có thể là $Pf(r = r\_1 + r\_2 + \cdots + r\_n)$. Khi thẩm định bằng chứng tổng hợp, nút 202 có thể xác thực xem $HE(t\_1) *\ldots* HE(t\_n) = H^r$ không. Nếu $HE(t\_1) *\ldots* HE(t\_n) = H^r$, thì thể hiện rằng $t\_1 + t\_2 + \cdots + t\_n = 0$, do vậy tạo ra Pf_sum và các khoản giao dịch được cân bằng. Theo cách khác, các khoản giao dịch không được cân bằng, và có thể có khoản giao dịch không chính xác bất kỳ. Theo một số phương án, các khoản giao dịch có thể được mã hóa sử dụng các lược đồ khác, và do vậy bằng chứng tổng hợp và việc xác thực bằng chứng tổng hợp có thể khác với bằng chứng tổng hợp và việc xác thực đã được mô tả ở đây.

Khi có nhiều người gửi và/hoặc người nhận, các khoản giao dịch giữa mỗi cặp người gửi người nhận được cân bằng. Theo một số phương án, khi người gửi giao dịch với nhiều người nhận, khoản giao dịch của người gửi có thể được chọn là tổng cộng của tất cả các khoản giao dịch cần gửi đến nhiều người nhận. Ví dụ, khi tài khoản "A_1" cần gửi khoản giao dịch của $1,000 đến tài khoản "A_2" và khoản giao dịch của $2,000 đến tài khoản "A_3," khoản giao dịch của tài khoản "A_1" bằng $3,000 (ví dụ, tổng cộng của $1,000 và $2,000). Khoản giao dịch của tài khoản "A_1" được cân bằng bởi khoản giao dịch của tài khoản "A_2," tức là, -$1,000, và khoản giao dịch của tài khoản "A_3," tức là, -$2,000. Tương tự, các khoản giao dịch khác trong các giao dịch được cân bằng. Bằng chứng này có thể được tạo ra và kết hợp với các giao dịch.

Như được mô tả bên trên, chữ ký từ mỗi tài khoản có thể được nhận, và chữ ký được biểu diễn bởi "Sig_i" trên Fig.3. Theo một số phương án, chữ ký có thể ký bởi mỗi tài khoản trên các giao dịch, bằng chứng phạm vi, và bằng chứng tổng hợp, biểu diễn bởi $Sig\_i = Signature\ (A\_1{:}T\_1, Pf\_1;\ \ldots;\ A\_n{:}T\_n, Pf\_n;\ Pf\_sum)$. Theo cách này, mỗi tài khoản tham gia vào (các) giao dịch đã biểu diễn thỏa thuận của nó với các thông số khác nhau trong chữ ký (). Theo một số phương án, chữ ký có thể được kết hợp với một hoặc nhiều giao dịch trong số các giao dịch, các bằng chứng phạm vi, hoặc bằng chứng tổng hợp.

Ở khối 306, nút 202 có thể nhận các giao dịch kết hợp với nhiều tài khoản nêu trên, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký kết hợp với ít nhất một trong số (các) giao dịch, bằng chứng phạm vi, hoặc bằng chứng tổng hợp, để xác thực các giao dịch đã nhận. Theo một số phương án, nút 202 có thể nhận các giao dịch

từ nút nhà tổ chức mà ngang hàng giữa những người tham gia giao dịch. Theo một số phương án, nút nhà tổ chức có thể là tổ chức bên thứ ba được thực hiện bởi thiết bị điện toán (không được thể hiện nhưng giống với nút 202). Ví dụ, mỗi người tham gia có thể gửi, thông qua thiết bị điện toán người dùng 240, ID tài khoản của nó cùng với khoản giao dịch mã hóa, bằng chứng phạm vi, và tương tự đến nút nhà tổ chức. Nút nhà tổ chức có thể tạo ra bằng chứng tổng hợp dựa trên các khoản giao dịch nhận được từ những người tham gia. Nút nhà tổ chức có thể gửi các giao dịch kết hợp với các tài khoản, bằng chứng phạm vi cho mỗi giao dịch trong số các giao dịch, bằng chứng tổng hợp trên các giao dịch, và chữ ký từ mỗi tài khoản trong số các tài khoản kết hợp với ít nhất một trong số các giao dịch, các bằng chứng phạm vi, hoặc bằng chứng tổng hợp đến mạng blockchain 200 bao gồm các nút 202. Theo một số phương án, nút nhà tổ chức có thể là một trong số những người tham gia ngang hàng những người tham gia khác. Theo cách khác nhà tổ chức có thể là nút 202 của mạng blockchain 200. Nút nhà tổ chức 202 có thể nhận các giao dịch kết hợp với nhiều ID tài khoảng, cùng với bằng chứng phạm vi cho mỗi giao dịch trong số các giao dịch, chữ ký kết hợp với ít nhất một trong số các giao dịch, các bằng chứng phạm vi, hoặc bằng chứng tổng hợp, từ những người tham gia. Nút nhà tổ chức 202 có thể thực hiện bằng chứng tổng hợp dựa trên các khoản giao dịch nhận được từ những người tham gia.

Ở khối 306, nút 202 có thể thẩm định các giao dịch, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký. Đáp ứng với các giao dịch và thông tin kết hợp là hợp lệ, nút 202 có thể thực hiện các giao dịch bằng cách cập nhật số dư của mỗi tài khoản liên quan đến các giao dịch. Ví dụ, nút 202 có thể xác thực mỗi chữ ký của tài khoản. Theo một số phương án, nếu chữ ký bất kỳ trong số các chữ ký là không hợp lệ, nút 202 có thể hủy bỏ các giao dịch. Sau mỗi chữ ký trong số các chữ ký được xác thực, nút 202 có thể thẩm định mỗi bằng chứng phạm vi cho mỗi giao dịch trong số các giao dịch. Theo một số phương án, nút 202 có thể lấy lại số dư mã hóa "S_i" và kiểm tra bằng chứng phạm vi "Pf_i" đối với số dư mã hóa "S_i." Theo một số phương án, nút 202 có thể xác thực tính hợp lệ của bản thân bằng chứng phạm vi "Pf_i". Đáp ứng với bằng chứng bất kỳ trong số các bằng chứng phạm vi là không hợp lệ, nút 202 có thể hủy bỏ các giao dịch.

Theo một số phương án, sau khi mỗi bằng chứng phạm vi được thẩm định, nút 202 có thể thẩm định bằng chứng tổng hợp trên các giao dịch. Ví dụ, nếu bằng chứng tổng hợp được tạo ra ngay khi các khoản giao dịch đã được mã hóa, nút 202 có thể xác thực bằng chứng tổng hợp theo lược đồ mã hóa, như được mô tả bên trên có tham chiếu đến khối 304. Đáp ứng với bằng chứng tổng hợp là không hợp lệ, nút 202 có thể hủy bỏ các giao dịch. Theo một số phương án, sau khi bằng chứng tổng hợp được thẩm định, nút 202 có thể cập nhật số dư của mỗi tài khoản. Ví dụ, nút 202 có thể cập nhật số dư "s_i" bằng cách trừ đi khoản giao dịch "t_i" từ số dư "s_i," tức là, $s\_i - t\_i$. Theo ví dụ nêu trên trong đó tài khoản "A_1" cần gửi khoản giao dịch của $1,000 đến tài khoản "A_2," nếu nút 202 có các giao dịch đã được thẩm định, sau đó nút 202 có thể trừ $1,000 từ số dư "S_1" của tài khoản "A_1," và cộng thêm $1,000 vào số dư "S_2" của tài khoản "A_2." Theo một số phương án, nút 202 có thể cập nhật trực tiếp số dư mã hóa, như được biểu diễn bởi $S\_i - T\_i$. Như được mô tả bên trên, cam kết Pedersen là đồng hình có tính cộng, và dữ liệu ưu tiên có thể được xử lý theo toán học như thể nó không được mã hóa. Ví dụ, nút 202 có thể cập nhật cam kết Pedersen của số dư bằng cách bổ sung cam kết Pedersen của khoản giao dịch vào cam kết Pedersen của số dư. Ở khối 308, có thể thu được các kết quả giao dịch. Như được thể hiện trên Fig.3, sau khi thực hiện các giao dịch, số dư của mỗi tài khoản được cập nhật là "S_i-T_i."

Phần mô tả trên đây mô tả các thẩm định của các chữ ký, các bằng chứng phạm vi, và bằng chứng tổng hợp theo thứ tự thời gian. Người có hiểu biết trung bình nên hiểu rằng các cách thẩm định có thể có thứ tự bất kỳ. Ví dụ, nút có thể thẩm định thứ tự của chữ ký, bằng chứng tổng hợp, bằng chứng phạm vi, hoặc bằng chứng phạm vi, bằng chứng tổng hợp, chữ ký, hoặc bằng chứng phạm vi, chữ ký, bằng chứng tổng hợp, hoặc bằng chứng tổng hợp, bằng chứng phạm vi, chữ ký, hoặc bằng chứng tổng hợp, chữ ký, bằng chứng phạm vi. Ngoài ra, các cách thẩm định là tùy chọn. Một số cách thẩm định trong số các cách thẩm định, ví dụ, bằng chứng phạm vi và/hoặc chữ ký có thể được bỏ qua.

Như vậy, sáng chế cho phép thực hiện nhiều giao dịch giữa các người gửi và người nhận hỗn hợp với bảo vệ quyền riêng tư tăng cường. Tức là, các nhận dạng của người gửi và người nhận được ẩn đối với công cộng. Khoản giao dịch của mỗi người tham gia có thể lớn hơn hoặc nhỏ hơn không. Khoản giao dịch dương biểu thị rằng tài

khoản của người tham gia là để sử dụng hết khoản này, trong khi âm khoản giao dịch biểu thị rằng tài khoản là để nhận khoản này. Ngoài ra, sáng chế cũng có thể sử dụng sự mã hóa đồng hình, cam kết đồng hình, hoặc các lược đồ mã hóa khác để mã hóa khoản giao dịch và số dư của mỗi tài khoản trong giao dịch, do vậy có thể làm cho người không tham gia biết được khoản giao dịch là dương hoặc âm hoặc số lượng thực của khoản giao dịch hoặc số dư, nhờ đó ngăn không cho người không tham gia nhận dạng ai là người gửi và ai là người nhận.

FIG. 4 là hình vẽ minh họa lưu đồ của phương pháp làm ví dụ 400 để thực hiện giao dịch, kết hợp với các phương án thực hiện khác nhau. Phương pháp 400 có thể được thực hiện trong các hệ thống khác nhau bao gồm, ví dụ, một hoặc nhiều thành phần của mạng blockchain 200 trên Fig.2. Phương pháp làm ví dụ 400 có thể được thực hiện bằng một hoặc nhiều nút trong số các nút 202 và/hoặc các thiết bị điện toán người dùng 240. Theo một ví dụ,, phương pháp 400 có thể được thực hiện bằng nút nhà tổ chức (ví dụ, một trong số các nút 202). Theo ví dụ khác, phương pháp 400 có thể được thực hiện bằng một hoặc nhiều nút (ví dụ, các nút 202) thực hiện các giao dịch. Các hoạt động của phương pháp 400 mà được thể hiện dưới đây là nhằm mục đích minh họa. Tùy theo phương án thực hiện, phương pháp làm ví dụ 400 có thể bao gồm các bước bổ sung, loại bỏ hoặc thay thế được thực hiện theo các thứ tự khác nhau hoặc song song.

Khối 401 bao gồm thu được các khoản giao dịch đã được mã hóa (ví dụ, $HE(t\_1), HE(t\_2), \ldots, HE(t\_n)$) kết hợp với các giao dịch trong số các tài khoản (ví dụ, A_1, A_2, … A_n), trong đó mỗi lượng trong số các khoản giao dịch đã được mã hóa được kết hợp với một trong số các tài khoản mà gửi hoặc nhận một trong số các khoản giao dịch, và sự mã hóa của mỗi khoản trong số các khoản giao dịch ít nhất che giấu một tài khoản gửi hoặc nhận một trong số các khoản giao dịch chưa.

Theo một số phương án, sự mã hóa có thể được thực hiện bằng nút tổ chức hoặc bằng các nút hoạt động như những người gửi hoặc người nhận của các giao dịch và nhận được bởi nút tổ chức. Các phương pháp mã hóa khác nhau có thể được sử dụng để mã hóa các khoản giao dịch. Sự mã hóa của mỗi khoản giao dịch trong số các khoản giao dịch bao gồm sự mã hóa đồng hình. Ví dụ, sự mã hóa của mỗi khoản giao dịch

trong số các khoản giao dịch có thể là sự mã hóa đồng hình hoặc lược đồ cam kết đồng hình (ví dụ, lược đồ cam kết Pedersen).

Theo một số phương án, sự chuyển nhượng tài sản giữa hai hoặc nhiều tài khoản có thể được tách riêng thành các giao dịch trong đó mỗi giao dịch kết hợp với một trong số tài khoản người gửi hoặc tài khoản người nhận. Mỗi tài khoản có thể được kết hợp với một nút trong số các nút 202. Ví dụ, sự chuyển nhượng tài sản của $100 từ tài khoản A sang B có thể bao gồm giao dịch thứ nhất bằng+$100 kết hợp với tài khoản A biểu thị rằng tài khoản A sử dụng $100 và bao gồm giao dịch thứ hai bằng -$100 kết hợp với tài khoản B biểu thị rằng tài khoản B nhận $100. Để làm ví dụ khác, sự chuyển nhượng tài sản của $100 từ tài khoản A sang B và sự chuyển nhượng tài sản khác của $80 từ tài khoản A sang C có thể bao gồm giao dịch thứ nhất bằng+$100 kết hợp với tài khoản A biểu thị rằng tài khoản A sử dụng $180, bao gồm giao dịch thứ hai bằng -$100 kết hợp với tài khoản B biểu thị rằng tài khoản B nhận $100, bao gồm giao dịch thứ ba bằng +$80 kết hợp với tài khoản A biểu thị rằng tài khoản A sử dụng $80, và bao gồm giao dịch thứ ba bằng -$80 kết hợp với tài khoản C biểu thị rằng tài khoản C nhận $80. Các dấu "+" và "-" có thể được hoán đổi hoặc thay đổi thành biểu diễn khác bất kỳ. Ngoài ra, như được thể hiện, hai trong số các tài khoản giống nhau, ví dụ, khi tài khoản mở rộng hoặc thu được từ nhiều tài khoản.

Ngoài ra, theo một số phương án, sự mã hóa của mỗi khoản giao dịch trong số các khoản giao dịch ít nhất che giấu một tài khoản gửi hoặc nhận một trong số các khoản giao dịch chưa bằng cách ẩn đi mỗi khoản giao dịch trong số các khoản giao dịch là đi vào (ví dụ, nhận tài sản) hay đi ra (ví dụ, gửi tài sản) đến một tài khoản. Theo ví dụ về sự chuyển nhượng tài sản của $100 từ tài khoản A sang B và của $80 từ tài khoản A sang C, bằng sự mã hóa, thông tin biểu thị nhận dạng người gửi hoặc người nhận như "+" trong khoản giao dịch "+$180" và "-" trong các khoản giao dịch "-$100" và "-$80" có thể được loại bỏ. Tức là, các khoản giao dịch đã được mã hóa sẽ không chứa thông tin mà biểu thị nhận dạng người gửi hoặc người nhận. Ngay cả nếu các khoản giao dịch đã được mã hóa có thể (nhưng không nhất thiết) bao gồm dấu "+" hoặc "-", dấu này có thể không còn biểu thị đúng nhận dạng người gửi hoặc người nhận. Do vậy, các nhận dạng của người gửi và người nhận trong các giao dịch được bảo vệ khỏi công cộng.

Khối tùy chọn 402 bao gồm: thu được các bằng chứng phạm vi (ví dụ, $Pf\_1, Pf\_2, \ldots, Pf\_n$) tương ứng cho các tài khoản liên quan đến các giao dịch, các bằng chứng phạm vi ít nhất biểu thị rằng mỗi tài khoảng trong số các tài khoản mà gửi các khoản giao dịch có đủ tài sản. Các mô tả chi tiết có thể được tham chiếu đến Pf_i đã được mô tả trên đây.

Khối 403 bao gồm: tạo ra bằng chứng tổng hợp (ví dụ, Pf_sum) dựa trên các khoản giao dịch đã được mã hóa thu được, bằng chứng tổng hợp ít nhất biểu thị rằng các khoản giao dịch được cân bằng. Các mô tả chi tiết có thể được tham chiếu đến the Pf_sum đã được mô tả trên đây. Ví dụ, nút nhà tổ chức có thể thu được các khoản giao dịch đã được mã hóa và xác định nếu $HE(t\_1) *\ldots* HE(t\_n) = H^{r\_1} * H^{r\_2} * \ldots * H^{r\_n} = H^{r}$. Nếu $HE(t\_1) *\ldots* HE(t\_n) = H^{r}$, nó thể hiện rằng $t\_1 + t\_2 + \cdots + t\_n = 0$, do vậy nút tổ chức verifies that các khoản giao dịch được cân bằng. Theo cách khác, các khoản giao dịch không được cân bằng, và nút tổ chức có thể hủy bỏ các giao dịch. Với sự mã hóa và đặc tính đồng hàm này của sự mã hóa, nút tổ chức có thể thực hiện sự xác thực này ngay cả không biết các khoản giao dịch cơ sở và liệu các khoản này là đến hay đi.

Khối tùy chọn 404 bao gồm thu được các chữ ký (ví dụ, Sig_1, Sig_2, …, Sig_n) tương ứng cho các tài khoản. Các chữ ký được kết hợp với ít nhất một trong số các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, và bằng chứng tổng hợp. Các mô tả chi tiết có thể được tham chiếu đến the Sig_i đã được mô tả trên đây. Hoạt động ký có thể tuân theo Thuật toán chữ ký điện tử (DSA: Digital Signature Algorithm) như thuật toán chữ ký điện tử đường cong elip (ECDSA: Elliptic Curve Digital Signature Algorithm), nhờ đó người nhận (ví dụ, các nút để thẩm định các giao dịch) có chữ ký có thể xác thực chữ ký bằng khóa công khai của người ký (ví dụ, các nút mà tham gia trong các giao dịch) để xác thực dữ liệu đã ký.

Khối 405 bao gồm truyền các khoản giao dịch đã được mã hóa và bằng chứng tổng hợp đến một hoặc nhiều nút (ví dụ, các nút đồng thuận) trong mạng blockchain để các nút xác minh các giao dịch. Theo một số phương án, truyền các khoản giao dịch đã được mã hóa và bằng chứng tổng hợp tới một hoặc nhiều nhút trong mạng blockchain để các nút xác minh các giao dịch bao gồm truyền các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký tới một hoặc nhiều nhút

trong mạng blockchain để các nút xác minh các giao dịch dựa trên các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký.

Theo một số phương án, truyền các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký tới một hoặc nhiều nhút trong mạng blockchain để các nút xác minh các giao dịch dựa trên các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký bao gồm: truyền các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký tới một hoặc nhiều nhút trong mạng blockchain; và khiến các nút: thẩm định các khoản giao dịch đã được mã hóa, các bằng chứng phạm vi, bằng chứng tổng hợp, và các chữ ký, thực thi các giao dịch đáp lại với việc xác minh các giao dịch thành công, và bổ sung các giao dịch vào khối dữ liệu mới của blockchain mà được duy trì bởi mạng blockchain. Với sự mã hóa và đặc tính đồng hiafnh này của sự mã hóa, các nút có thể thực hiện sự thẩm định này ngay cả khi không biết các lượng giao dịch cơ sở và liệu các khoản này là đến hay đi.

Theo một số phương án, khiến các nút thực thi các giao dịch đáp lại với việc xác minh các giao dịch thành công bao gồm: khiến các nút trừ đi các khoản giao dịch đã được mã hóa (T_i) một cách tương ứng từ các số dư tài khoản mã hóa (ví dụ, S_i của các tài khoản đáp lại với việc xác minh các giao dịch thành công. Do đặc tính đồng hình, (S_i - T_i) có thể cập nhật số dư theo các giao dịch đồng thời duy trì số dư được mã hóa.

Như vậy, các hệ thống và phương pháp đã được bộc lộ cho phép các giao dịch được thực hiện giữa các tài khoản tham gia mà không để lộ tài khoản nào là người gửi và tài khoản nào là người nhận. Mặc dù khoản giao dịch cơ sở có thể lớn hơn hoặc nhỏ hơn không để biểu thị người gửi và người nhận, phương pháp mã hóa thích hợp có thể được sử dụng để che giấu các khoản giao dịch sao cho các khoản giao dịch không thể được sử dụng để biểu thị người gửi hoặc người nhận bởi người không tham gia. Ngoài ra, các tài khoản tham gia trong nhiều giao dịch có thể được trộn lẫn với nhau theo thứ tự bất kỳ, mà không biểu thị họ gửi hay nhận các tài sản. Và nhiều giao dịch hoặc các chuyển nhượng tài sản có thể được thực hiện theo đợt. Theo cách này, có thể đạt được sự bảo vệ quyền riêng tư của các tài khoản tham gia, điều này tăng cường chức năng của các máy tính và làm cho các giao dịch trực tuyến an toàn hơn.

FIG. 5 là hình vẽ minh họa lưu đồ của phương pháp làm ví dụ khác 500 để thực hiện giao dịch, kết hợp với các phương án thực hiện khác nhau. Phương pháp 500 có thể được thực hiện trong các hệ thống khác nhau bao gồm, ví dụ, một hoặc nhiều thành phần của mạng blockchain 200 trên Fig.2. Phương pháp làm ví dụ 500 có thể được thực hiện bằng một hoặc nhiều nút trong số các nút 202 và/hoặc các thiết bị điện toán người dùng 240. Các hoạt động của phương pháp 500 mà được thể hiện dưới đây là nhằm mục đích minh họa. Tùy theo phương án thực hiện, phương pháp làm ví dụ 500 có thể bao gồm các bước bổ sung, loại bỏ hoặc thay thế được thực hiện theo các thứ tự khác nhau hoặc song song.

Ở khối 502, các giao dịch mã hóa kết hợp với các tài khoản, bằng chứng phạm vi cho mỗi giao dịch trong số các giao dịch, bằng chứng tổng hợp trên các giao dịch, và chữ ký từ mỗi tài khoản trong số các tài khoản kết hợp với ít nhất một trong số các giao dịch, các bằng chứng phạm vi, hoặc bằng chứng tổng hợp có thể được nhận. Ở khối 504, các giao dịch mã hóa, bằng chứng phạm vi cho mỗi giao dịch trong số các giao dịch, bằng chứng tổng hợp trên các giao dịch, và chữ ký từ mỗi tài khoản trong số các tài khoản có thể được thẩm định. Ở khối 506, các giao dịch có thể được thực hiện dựa trên cách thẩm định bằng cách cập nhật số dư của mỗi tài khoản trong số các tài khoản.

FIG. 6 là hình vẽ minh họa lưu đồ của phương pháp làm ví dụ 600 để thẩm định giao dịch, kết hợp với các phương án thực hiện khác nhau. Phương pháp 600 có thể được thực hiện trong các hệ thống khác nhau bao gồm, ví dụ, một hoặc nhiều thành phần của mạng blockchain 200 trên Fig.2. Phương pháp làm ví dụ 600 có thể được thực hiện bằng một hoặc nhiều nút trong số các nút 202 và/hoặc các thiết bị điện toán người dùng 240. Ví dụ, phương pháp 600 có thể tương ứng với khối 504 của phương pháp 500. Các hoạt động của phương pháp 600 mà được thể hiện dưới đây là nhằm mục đích minh họa. Tùy theo phương án thực hiện, phương pháp làm ví dụ 600 có thể bao gồm các bước bổ sung, loại bỏ hoặc thay thế được thực hiện theo các thứ tự khác nhau hoặc song song.

Ở khối 602, có thể xác định được liệu các chữ ký là hợp lệ hay không. Nếu xác định được rằng chữ ký bất kỳ trong số các chữ ký là không hợp lệ, ở khối 604, các giao dịch có thể bị hủy bỏ. Nếu xác định được rằng mỗi chữ ký trong số các chữ ký là hợp lệ, ở khối 606, có thể xác định được liệu bằng chứng phạm vi cho mỗi giao dịch trong

số các giao dịch là hợp lệ hay không. Nếu xác định được rằng bằng chứng bất kỳ trong số các bằng chứng phạm vi là không hợp lệ, phương pháp 600 thực hiện đến khối 604 và các giao dịch có thể bị hủy bỏ. Nếu xác định được rằng mỗi bằng chứng trong số các bằng chứng phạm vi là hợp lệ, ở khối 608, có thể xác định được liệu bằng chứng tổng hợp là hợp lệ hay không. Nếu xác định được rằng bằng chứng tổng hợp là không hợp lệ, phương pháp 600 thực hiện đến khối 604 và các giao dịch có thể bị hủy bỏ. Nếu xác định được rằng bằng chứng tổng hợp là hợp lệ, phương pháp 600 thực hiện đến khối 610 và số dư của mỗi tài khoản có thể được cập nhật dựa trên khoản giao dịch kết hợp với tài khoản. Phần mô tả nêu trên mô tả các cách thẩm định theo một thứ tự. Người có hiểu biết trung bình nên hiểu rằng các cách thẩm định có thể có thứ tự bất kỳ.

Các công nghệ đã được mô tả ở đây được thực hiện bằng một hoặc nhiều thiết bị điện toán có mục đích đặc biệt. Các thiết bị điện toán có mục đích đặc biệt có thể là các hệ thống máy tính để bàn, các hệ thống máy tính máy chủ, các hệ thống máy tính xách tay, các thiết bị cầm tay, các thiết bị mạng hoặc thiết bị khác bất kỳ của sự kết hợp của các thiết bị mà kết hợp logic kiểm soát bằng mạng điện tử và/hoặc logic chương trình để thực hiện các công nghệ này.

FIG. 7 là sơ đồ khối để minh họa hệ thống máy tính làm ví dụ 700 trong đó phương án thực hiện bất kỳ trong số các phương án thực hiện đã được mô tả ở đây có thể được thực hiện. Hệ thống 700 có thể tương ứng với các nút 202 hoặc các thiết bị điện toán người dùng 240 đã được mô tả trên đây có tham chiếu đến Fig.2. Hệ thống máy tính 700 bao gồm đường bus 702 hoặc cơ chế truyền thông khác để truyền thông thông tin, một hoặc nhiều bộ xử lý phần cứng 704 ghép nối với đường bus 702 để xử lý thông tin. (Các) bộ xử lý phần cứng 704 có thể là, ví dụ, một hoặc nhiều bộ vi xử lý mục đích chung.

Hệ thống máy tính 700 còn bao gồm bộ nhớ chính 706, như bộ nhớ truy cập ngẫu nhiên (RAM), bộ nhớ cache và/hoặc thiết bị lưu trữ thay đổi khác, ghép nối với đường bus 702 để lưu trữ thông tin và các lệnh sẽ được thực thi bởi bộ xử lý 704. Bộ nhớ chính 706 also có thể được sử dụng để lưu trữ các biến tạm thời hoặc thông tin trung gian khác trong quá trình thực thi các lệnh sẽ được thực thi bởi bộ xử lý 704. Các lệnh này, khi được lưu trữ trong phương tiện lưu trữ có thể truy nhập vào bộ xử lý 704, kết xuất hệ thống máy tính 700 thành máy có mục đích đặc biệt mà được tùy biến để thực hiện

các hoạt động được biểu thị trong các lệnh. Hệ thống máy tính 700 còn bao gồm bộ nhớ chỉ đọc (ROM: read only memory) 708 hoặc thiết bị lưu trữ không thay đổi khác ghép nối với đường bus 702 để lưu trữ thông tin không thay đổi và các lệnh cho bộ xử lý 704. Thiết bị lưu trữ 710, như đĩa từ, đĩa quang, hoặc ổ USB (ổ Flash), v.v., được lắp và ghép nối với đường bus 702 để lưu trữ thông tin và các lệnh.

Hệ thống máy tính 700 có thể thực hiện các công nghệ đã được mô tả ở đây nhờ sử dụng logic có dây, một hoặc nhiều ASIC hoặc FPGA, phần sụn và/hoặc logic chương trình mà kết hợp với hệ thống máy tính làm cho hoặc tạo chương trình cho hệ thống máy tính 700 để trở thành máy mục đích đặc biệt. Theo một phương án thực hiện, các hoạt động, các phương pháp, và các quy trình đã được mô tả ở đây được thực hiện bởi hệ thống máy tính 700 đáp ứng với (các) bộ xử lý 704 thực thi một hoặc nhiều chuỗi của một hoặc nhiều lệnh chứa trong bộ nhớ chính 706. Các lệnh này có thể được đọc bên trong bộ nhớ chính 706 từ phương tiện lưu trữ khác, như thiết bị lưu trữ 710. Sự thực thi của các lệnh tuần tự chứa trong bộ nhớ chính 706 khiến cho (các) bộ xử lý 704 để thích hợp các bước xử lý đã được mô tả ở đây. Theo các phương án thực hiện khác, hệ thống mạch có dây có thể được sử dụng thay thế hoặc kết hợp với các lệnh phần mềm.

(Các) bộ xử lý 704 có thể tương ứng với bộ xử lý 204 đã được mô tả trên đây, và the bộ nhớ chính 706, ROM 708, và/hoặc bộ lưu trữ 710 có thể tương ứng với bộ nhớ 206 đã được mô tả trên đây. Bộ nhớ chính 706, ROM 708, và/hoặc bộ lưu trữ 710 có thể bao gồm phương tiện lưu trữ bất chuyển tiếp. Thuật ngữ "các phương tiện bất chuyển tiếp", và các thuật ngữ tương tự, như được sử dụng ở đây, là nói đến các phương tiện mà lưu trữ dữ liệu và/hoặc các lệnh để khiến một cỗ máy hoạt động theo cách riêng. Phương tiện bất chuyển tiếp này có thể còn bao gồm phương tiện bất biến và/hoặc phương tiện khả biến. Phương tiện bất biến bao gồm, ví dụ, các đĩa quang học hoặc đĩa từ, như thiết bị lưu trữ 710. Phương tiện khả biến chứa bộ nhớ động, như bộ nhớ chính 706. Các dạng chung của phương tiện bất chuyển tiếp bao gồm, ví dụ, ổ đĩa mềm, ổ đĩa cứng, ổ đĩa trạng thái rắn, băng từ, hoặc môi trường lưu trữ dữ liệu từ tính khác, CD-ROM, môi trường lưu trữ dữ liệu quang học bất kỳ khác, phương tiện vật lý bất kỳ khác với các mẫu lỗ, RAM, PROM, và EPROM, FLASH-EPROM, NVRAM, chip hoặc hộp nhớ bất kỳ khác, và các phiên bản được nối mạng của chúng.

Hệ thống máy tính 700 còn bao gồm giao diện truyền thông 718 ghép nối với đường bus 702. Giao diện truyền thông 718 tạo ra truyền thông dữ liệu hai chiều ghép nối với một hoặc nhiều liên kết mạng mà được nối với một hoặc nhiều mạng cục bộ. Ví dụ, giao diện truyền thông 718 có thể là cạc mạng kỹ thuật số dịch vụ tích hợp (ISDN) , modem cáp, modem vệ tinh, hoặc modem để tạo ra kết nối truyền thông dữ liệu với kiểu đường dây điện thoại tương ứng. Là một ví dụ khác, giao diện truyền thông 718 có thể là cổng nối mạng cục bộ (LAN: Local area network) để tạo ra kết nối truyền thông dữ liệu với mạng LAN tương thích (hoặc thành phần mạng WAN để giao tiếp với WAN). Các liên kết không dây cũng có thể được thực hiện. Theo phương án thực hiện bất kỳ này, giao diện truyền thông 718 gửi và nhận các tín hiệu điện, điện từ hoặc quang mà mang các luồng dữ liệu số biểu diễn các kiểu thông tin khác nhau.

Hệ thống máy tính 700 có thể gửi các thông điệp và nhận dữ liệu, bao gồm mã code chương trình, thông qua (các) mạng, liên kết mạng và giao diện truyền thông 718. Trong ví dụ về Internet, máy chủ có thể truyền mã code yêu cầu đối với chương trình ứng dụng thông qua Internet, ISP, mạng cục bộ và giao diện truyền thông 718. Mã code nhận được có thể được thực thi bởi bộ xử lý 704 khi nó được nhận, và/hoặc lưu trữ trên thiết bị lưu trữ 710, or bộ lưu trữ bất biến khác để thực thi sau.

Mỗi loại trong số các lược đồ, cơ chế, giải pháp, quy trình, các phương pháp, và thuật toán đã được mô tả ở các phần trên đây có thể được thực hiện, và được tự động hoàn toàn hoặc một phần bởi, trong các môđun mã code mà được thực thi bởi một hoặc nhiều hệ thống máy tính hoặc các bộ xử lý máy tính bao gồm phần cứng máy tính. Các quy trình và các thuật toán có thể được thực hiện một phần hoặc toàn bộ trong hệ mạch ứng dụng chuyên dụng. Theo một số phương án, (Các) bộ xử lý 704 có thể được thực hiện một phần hoặc toàn bộ như một hoặc nhiều mạch logic đã được mô tả trên đây.

Các dấu hiệu và các quy trình khác nhau đã được mô tả trên đây có thể được sử dụng một cách độc lập với nhau, hoặc có thể được kết hợp theo nhiềuh. Tất cả các kết hợp và kết hợp con được dự tính nằm trong phạm vi của sáng chế. Ngoài ra, phương pháp hoặc các khối xử lý cụ thể có thể được bỏ qua trong một số phương án thực hiện. Các phương pháp và các quy trình đã được mô tả ở đây cũng không bị giới hạn ở tuần tự cụ thể bất kỳ, và các khối hoặc trạng thái liên quan đến chúng có thể được thực hiện theo các tuần tự khác nếu thích hợp. Ví dụ, các khối hoặc trạng thái đã được mô tả có

thể được thực hiện theo thứ tự khác với thứ tự đã được bộc lộ một cách cụ thể, hoặc nhiều khối hoặc trạng thái có thể được kết hợp thành một khối hoặc trạng thái. Các khối hoặc các trạng thái làm ví dụ có thể được thực hiện theo kiểu nối tiếp, song song hoặc một số cách khác. Các khối hoặc các trạng thái có thể được bổ sung vào hoặc loại bỏ ra khỏi các phương án thực hiện làm ví dụ đã được bộc lộ. Các hệ thống và thành phần làm ví dụ đã được mô tả ở đây có thể được cấu hình khác với cấu hình đã được mô tả. Ví dụ, các phần tử có thể được bổ sung vào, loại bỏ ra khỏi, hoặc bố trí lại so với các phương án thực hiện làm ví dụ đã được bộc lộ.

Các hoạt động khác nhau của các phương pháp làm ví dụ đã được mô tả ở đây có thể được thực hiện, ít nhất một phần, bởi một thuật toán. Thuật toán này có thể được chứa trong các mã code chương trình hoặc các lệnh lưu trữ trong bộ nhớ (ví dụ, phương tiện lưu trữ đọc được bằng máy tính bất chuyển tiếp đã được mô tả trên đây). Thuật toán này có thể bao gồm thuật toán học máy. Theo một số phương án, thuật toán học máy có thể không lập trình một cách rõ ràng các máy tính để thực hiện chức năng, mà có thể học từ dữ liệu đào tạo để tạo ra mô hình dự đoán mà thực hiện chức năng này.

Các hoạt động khác nhau của các phương pháp làm ví dụ đã được mô tả ở đây có thể được thực hiện, ít nhất một phần, bởi một hoặc nhiều bộ xử lý mà được cấu hình tạm thời (ví dụ, bằng phần mềm) hoặc cấu hình vĩnh viễn để thực hiện các hoạt động liên quan. Cho dù là được cấu hình tạm thời hay vĩnh viễn, các bộ xử lý này có thể cấu tạo nên các phương tiện thực hiện bằng bộ xử lý mà vận hành để thực hiện một hoặc nhiều hoạt động hoặc chức năng đã được mô tả ở đây.

Tương tự, các phương pháp đã được mô tả ở đây có thể được thực hiện bộ xử lý ít nhất một phần, bằng bộ xử lý hoặc các bộ xử lý cụ thể là ví dụ về phần cứng. Ví dụ, ít nhất một số hoạt động trong số các hoạt động của phương pháp có thể được thực hiện bằng một hoặc nhiều bộ xử lý hoặc các phương tiện thực hiện bằng bộ xử lý. Ngoài ra, một hoặc nhiều bộ xử lý cũng có thể vận hành để hỗ trợ hiệu suất của các hoạt động liên quan trong môi trường "điện toán đám mây" hoặc dưới dạng “phầm mềm như một dịch vụ” (SaaS: software as a service). Ví dụ, ít nhất một số hoạt động trong số các hoạt động có thể được thực hiện bằng nhóm các máy tính (là các ví dụ về các máy chứa các bộ xử lý), với các hoạt động này có thể truy cập được qua mạng (ví dụ, Internet) và qua

một hoặc nhiều giao diện thích hợp (ví dụ, Giao diện chương trình ứng dụng (API: Application Program Interface)).

Hiệu quả của hoạt động cụ thể trong số các hoạt động có thể được phân bố giữa các bộ xử lý, không chỉ nằm trong một máy, mà có thể được triển khai trên nhiều máy. Theo một số phương án làm ví dụ, các bộ xử lý hoặc các phương tiện được thực hiện bằng bộ xử lý có thể được đặt ở một vị trí địa lý (ví dụ, trong môi trường gia đình, môi trường văn phòng, hoặc trang trại máy chủ). Theo một số phương án làm ví dụ khác, các bộ xử lý hoặc các phương thiện được thực hiện bằng bộ xử lý có thể được phân bố trên nhiều vị trí địa lý.

Trong toàn bộ bản mô tả này, nhiều ví dụ có thể áp dụng các thành phần, các hoạt động, hoặc các cấu trúc đã được mô tả như là một ví dụ. Mặc dù các hoạt động riêng rẽ của một hoặc nhiều phương pháp được minh họa và được mô tả là các hoạt động tách biệt, nhưng một hoặc nhiều hoạt động trong số các hoạt động riêng biệt có thể được thực hiện đồng thời, và không yêu cầu rằng các hoạt động được theo thứ tự đã được minh họa. Các cấu trúc và chức năng mà được trình bày dưới dạng các thành phần riêng biệt trong các cấu hình ví dụ có thể được thực hiện dưới dạng cấu trúc hoặc thành phần kết hợp. Tương tự, các cấu trúc và chức năng được thể hiện dưới dạng một thành phần có thể được thực hiện là các thành phần tách biệt. Các biến thể, biến đổi, bổ sung và cải tiến này cũng như các biến thể, biến đổi, bổ sung và cải tiến này khác đều nằm trong phạm vi bảo hộ của sáng chế này.

Các mô tả quy trình bất kỳ, các phần tử hoặc khối trên các lưu đồ đã được mô tả ở đây và/hoặc được minh họa trên các hình vẽ kèm theo cần được hiểu là các môđun, đoạn hoặc phần biểu diễn có thể có của mã code mà bao gồm một hoặc nhiều lệnh thực thi để thực hiện các hàm logic cụ thể hoặc các bước trong quy trình. Các phương án thực hiện thay thế được bao hàm trong phạm vi của các phương án thực hiện đã được mô tả ở đây trong đó các phần tử hoặc chức năng có thể được loại bỏ, thực hiện theo thứ tự khác với thứ tự đã được thể hiện hoặc mô tả, bao gồm thứ tự hầu như đồng thời hoặc thứ tự ngược, tùy thuộc vào chức năng liên quan, như sẽ được hiểu bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật.

Mặc dù tổng quan về sáng chế đã được mô tả có tham chiếu đến các phương án làm ví dụ cụ thể, nhưng các biến thể và thay đổi khác nhau có thể được thực hiện đối

với các phương án này mà không nằm ngoài phạm vi rộng hơn của các phương án thực hiện sáng chế. Các phương án thực hiện này của sáng chế có thể được đề cập tới ở đây, một cách riêng rẽ hoặc chung chung, bởi thuật ngữ "sáng chế" chỉ để tạo thuận tiện và không nhằm làm cho phạm vi bảo hộ của sáng chế này giới hạn ở một phần bộc lộ hoặc khái niệm bất kỳ nếu trong thực tế có nhiều hơn một phần như vậy được bộc lộ.

Các phương án thực hiện đã được minh họa trong bản mô tả này được bộc lộ chi tiết một cách thích hợp để cho phép người có hiểu biết trung bình trong lĩnh vực kỹ thuật thực hiện các dấu hiệu đã bộc lộ. Các phương án thực hiện khác có thể được sử dụng và dẫn ra từ đó, sao cho các thay thế và thay đổi về cấu trúc và logic có thể được thể hiện mà không nằm ngoài phạm vi bảo hộ của sáng chế. Do đó, phần mô tả chi tiết không được xem là trường hợp giới hạn, và phạm vi của các phương án khác nhau chỉ được xác định bởi các điểm yêu cầu bảo hộ kèm theo, cùng với phạm vi đầy đủ của các phương án tương đương mà các điểm yêu cầu bảo hộ đó bao trùm.

YÊU CẦU BẢO HỘ

1. Phương pháp bảo vệ thông tin được thực hiện bằng máy tính, trong đó phương pháp này bao gồm các bước:

thu thập các lượng giao dịch được mã hoá được liên kết với các giao dịch trong số các tài khoản, trong đó:

mỗi trong số các lượng giao dịch được mã hoá này được liên kết với một trong số các tài khoản mà gửi hoặc nhận một trong số các lượng giao dịch này, và

việc mã hoá mỗi trong số các lượng giao dịch này ít nhất là che giấu việc một tài khoản là gửi hay nhận một trong số các lượng giao dịch này;

thu thập các bằng chứng phạm vi lần lượt cho các tài khoản tham gia vào các giao dịch này, các bằng chứng phạm vi này ít nhất chỉ thị rằng mỗi trong số các tài khoản mà gửi các lượng giao dịch này là có đủ tài sản;

tạo ra bằng chứng tổng dựa trên các lượng giao dịch được mã hoá thu được, bằng chứng tổng này ít nhất chỉ thị rằng các lượng giao dịch là được làm cân bằng;

thu thập các chữ ký lần lượt từ các tài khoản này; và

truyền các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này đến một hoặc nhiều nút trên mạng blockchain (chuỗi khối) để các nút này xác minh các giao dịch dựa trên các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này.

2. Phương pháp theo điểm 1, trong đó việc mã hoá mỗi trong số các lượng giao dịch ít nhất che giấu việc một tài khoản gửi hay nhận một trong số các lượng giao dịch, bằng cách làm ẩn việc mỗi trong số các lượng giao dịch là đi vào hay đi ra đối với một tài khoản đó.

3. Phương pháp theo điểm 1, trong đó bước truyền các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này đến một hoặc nhiều nút trên mạng blockchain (chuỗi khối) để các nút này xác minh các giao dịch dựa trên các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này, là bao gồm các bước:

truyền các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này đến một hoặc nhiều nút trên mạng blockchain này; và

khiến các nút này:

thẩm định các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này,

thực thi các giao dịch đáp lại việc xác minh thành công các giao dịch, và

bổ sung các giao dịch này vào khối dữ liệu mới của blockchain (chuỗi khối) được duy trì bởi mạng blockchain này.

4. Phương pháp theo điểm 3, trong đó bước khiến các nút thực thi các giao dịch đáp lại việc xác minh thành công các giao dịch là bao gồm bước:

khiến các nút này khấu trừ tương ứng các lượng giao dịch được mã hoá từ các số dư tài khoản được mã hoá của các tài khoản đáp lại việc xác minh thành công các giao dịch này.

5. Phương pháp theo điểm 1, trong đó sự mã hoá của mỗi trong số các lượng giao dịch là bao gồm sự mã hoá đồng cấu.

6. Phương pháp theo điểm 1, trong đó sự mã hoá của mỗi trong số các lượng giao dịch là bao gồm sơ đồ cam kết Pedersen.

7. Hệ thống bảo vệ thông tin, trong đó hệ thống này bao gồm: một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ phi nhất thời đọc được bằng máy tính được ghép nối đến một hoặc nhiều bộ xử lý này và được tạo cấu hình với các chỉ dẫn thực thi được bởi một hoặc nhiều bộ xử lý này để khiến hệ thống này thực hiện các hoạt động bao gồm:

thu thập các lượng giao dịch được mã hoá được liên kết với các giao dịch trong số các tài khoản, trong đó:

mỗi trong số các lượng giao dịch được mã hoá này được liên kết với một trong số các tài khoản mà gửi hoặc nhận một trong số các lượng giao dịch này, và

việc mã hoá mỗi trong số các lượng giao dịch này ít nhất là che giấu việc một tài khoản là gửi hay nhận một trong số các lượng giao dịch này;

thu thập các bằng chứng phạm vi lần lượt cho các tài khoản tham gia vào các giao dịch này, các bằng chứng phạm vi này ít nhất chỉ thị rằng mỗi trong số các tài khoản mà gửi các lượng giao dịch này là có đủ tài sản;

tạo ra bằng chứng tổng dựa trên các lượng giao dịch được mã hoá thu được, bằng chứng tổng này ít nhất chỉ thị rằng các lượng giao dịch là được làm cân bằng;

thu thập các chữ ký lần lượt từ các tài khoản này; và

truyền các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này đến một hoặc nhiều nút trên mạng blockchain (chuỗi khối) để các nút này xác minh các giao dịch dựa trên các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này.

8. Hệ thống theo điểm 7, trong đó việc mã hoá mỗi trong số các lượng giao dịch ít nhất che giấu việc một tài khoản gửi hay nhận một trong số các lượng giao dịch, bằng cách làm ẩn việc mỗi trong số các lượng giao dịch là đi vào hay đi ra đối với một tài khoản đó.

9. Hệ thống theo điểm 7, trong đó bước truyền các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này đến một hoặc nhiều nút trên mạng blockchain (chuỗi khối) để các nút này xác minh các giao dịch dựa trên các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này, là bao gồm các bước:

truyền các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này đến một hoặc nhiều nút trên mạng blockchain này; và

khiến các nút này:

thẩm định các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này,

thực thi các giao dịch đáp lại việc xác minh thành công các giao dịch, và

bổ sung các giao dịch này vào khối dữ liệu mới của blockchain (chuỗi khối) được duy trì bởi mạng blockchain này.

10. Hệ thống theo điểm 9, trong đó bước khiến các nút thực thi các giao dịch đáp lại việc xác minh thành công các giao dịch là bao gồm bước:

khiến các nút này khấu trừ tương ứng các lượng giao dịch được mã hoá từ các số dư tài khoản được mã hoá của các tài khoản đáp lại việc xác minh thành công các giao dịch này.

11. Hệ thống theo điểm 7, trong đó sự mã hoá của mỗi trong số các lượng giao dịch là bao gồm sự mã hoá đồng cấu.

12. Hệ thống theo điểm 7, trong đó sự mã hoá của mỗi trong số các lượng giao dịch là bao gồm sơ đồ cam kết Pedersen.

13. Phương tiện lưu trữ phi nhất thời đọc được bằng máy tính được tạo cấu hình với các chỉ dẫn thực thi được bởi một hoặc nhiều bộ xử lý để khiến một hoặc nhiều bộ xử lý này thực hiện các hoạt động bao gồm:

thu thập các lượng giao dịch được mã hoá được liên kết với các giao dịch trong số các tài khoản, trong đó:

mỗi trong số các lượng giao dịch được mã hoá này được liên kết với một trong số các tài khoản mà gửi hoặc nhận một trong số các lượng giao dịch này, và

việc mã hoá mỗi trong số các lượng giao dịch này ít nhất là che giấu việc một tài khoản là gửi hay nhận một trong số các lượng giao dịch này;

thu thập các bằng chứng phạm vi lần lượt cho các tài khoản tham gia vào các giao dịch này, các bằng chứng phạm vi này ít nhất chỉ thị rằng mỗi trong số các tài khoản mà gửi các lượng giao dịch này là có đủ tài sản;

tạo ra bằng chứng tổng dựa trên các lượng giao dịch được mã hoá thu được, bằng chứng tổng này ít nhất chỉ thị rằng các lượng giao dịch là được làm cân bằng;

thu thập các chữ ký lần lượt từ các tài khoản này; và

truyền các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này đến một hoặc nhiều nút trên mạng blockchain (chuỗi khối) để các nút này xác minh các giao dịch dựa trên các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này.

14. Phương tiện lưu trữ theo điểm 13, trong đó việc mã hoá mỗi trong số các lượng giao dịch ít nhất che giấu việc một tài khoản gửi hay nhận một trong số các lượng giao dịch, bằng cách làm ẩn việc mỗi trong số các lượng giao dịch là đi vào hay đi ra đối với một tài khoản đó.

15. Phương tiện lưu trữ theo điểm 13, trong đó: bước truyền các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này đến một hoặc nhiều nút trên mạng blockchain (chuỗi khối) để các nút này xác minh các giao dịch dựa trên các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này, là bao gồm các bước:

truyền các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này đến một hoặc nhiều nút trên mạng blockchain này; và

khiến các nút này:

thẩm định các lượng giao dịch được mã hoá, các bằng chứng phạm vi, bằng chứng tổng, và các chữ ký này,

thực thi các giao dịch đáp lại việc xác minh thành công các giao dịch, và

bổ sung các giao dịch này vào khối dữ liệu mới của blockchain (chuỗi khối) được duy trì bởi mạng blockchain này.

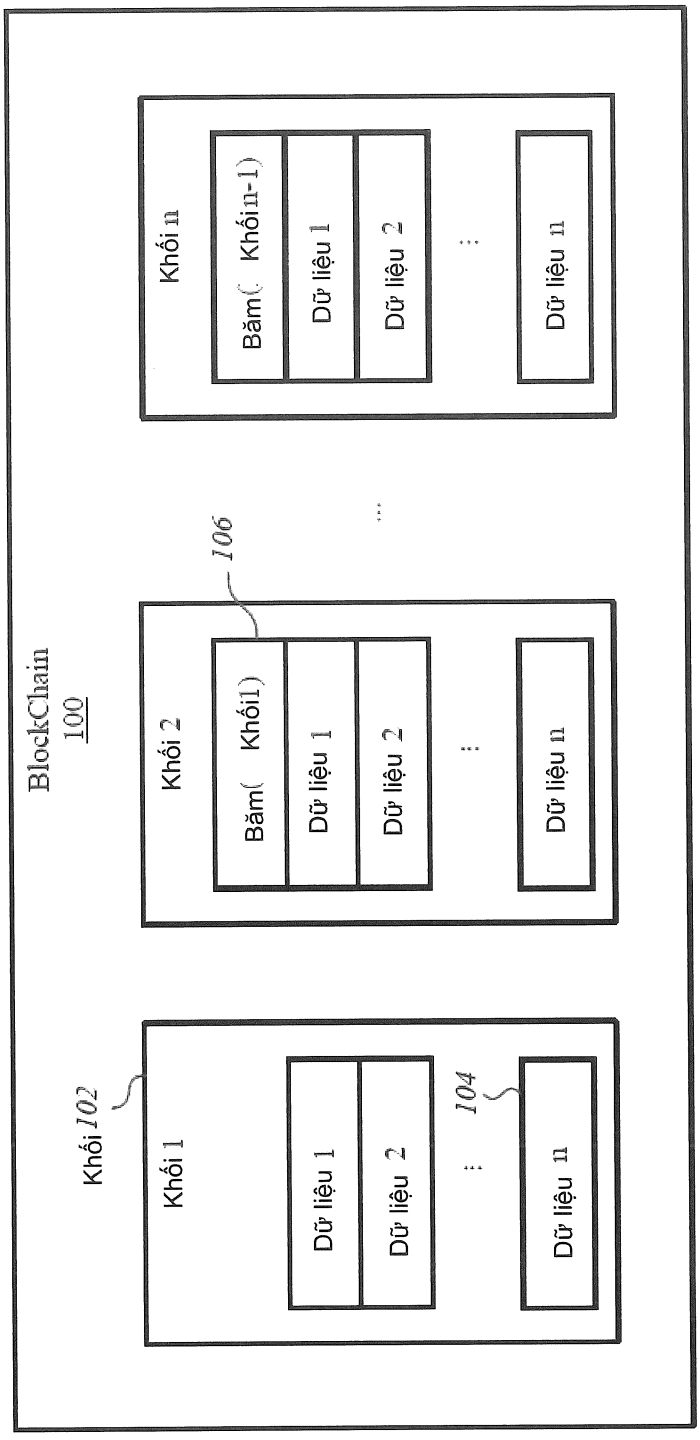

BlockChain
100
Khối 1
Khối 102
Dữ liệu 1
Dữ liệu 2
Dữ liệu n
104
Khối 2
Băm(Khối1)
Dữ liệu 1
Dữ liệu 2
Dữ liệu n
106
Khối n
Băm(Khối n-1)
Dữ liệu 1
Dữ liệu 2
Dữ liệu n

FIG. 1

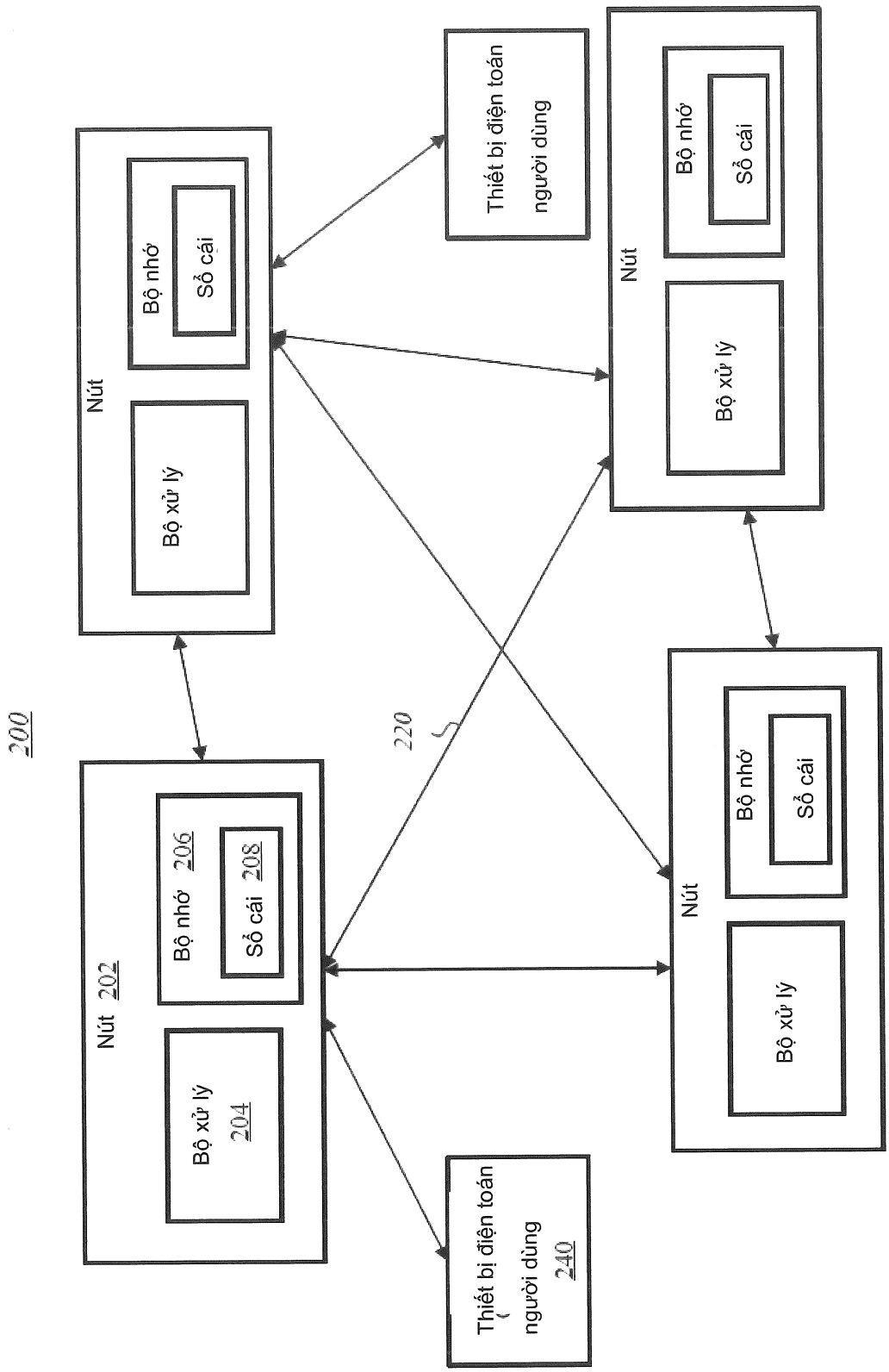

200
Nút 202
Bộ nhớ 206
Sổ cái 208
Bộ xử lý 204
220
Thiết bị điện toán người dùng 240
Nút
Bộ nhớ
Sổ cái
Bộ xử lý
Thiết bị điện toán người dùng
Nút
Bộ nhớ
Sổ cái
Bộ xử lý
Nút
Bộ nhớ
Sổ cái
Bộ xử lý

FIG. 2

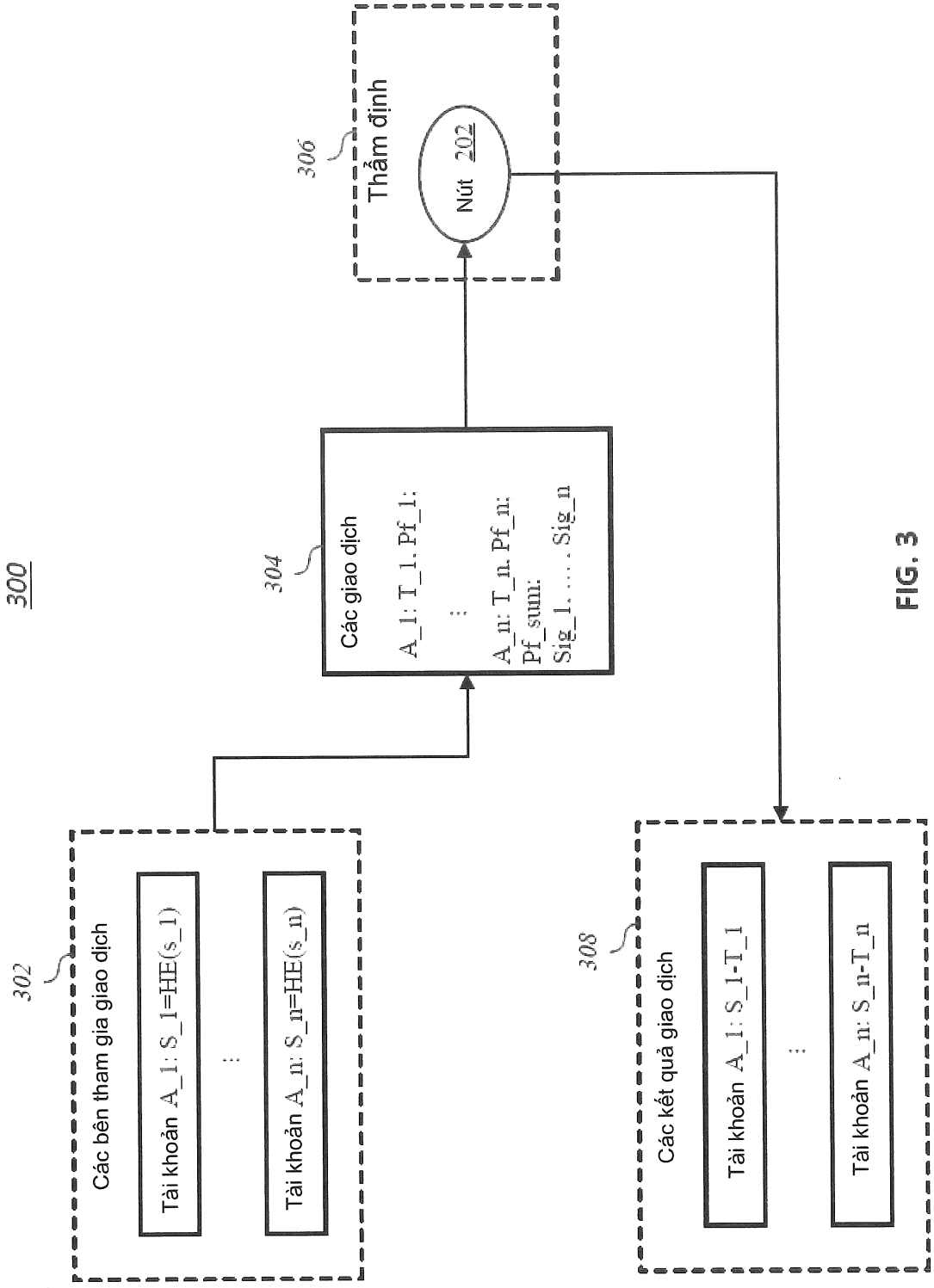

300
302
Các bên tham gia giao dịch
Tài khoản A_1: S_1=HE(s_1)
Tài khoản A_n: S_n=HE(s_n)
304
Các giao dịch
A_1: T_1, Pf_1;
A_n: T_n, Pf_n;
Pf_sum:
Sig_1, ..., Sig_n
306
Thẩm định
Nút 202
308
Các kết quả giao dịch
Tài khoản A_1: S_1-T_1
Tài khoản A_n: S_n-T_n

FIG. 3

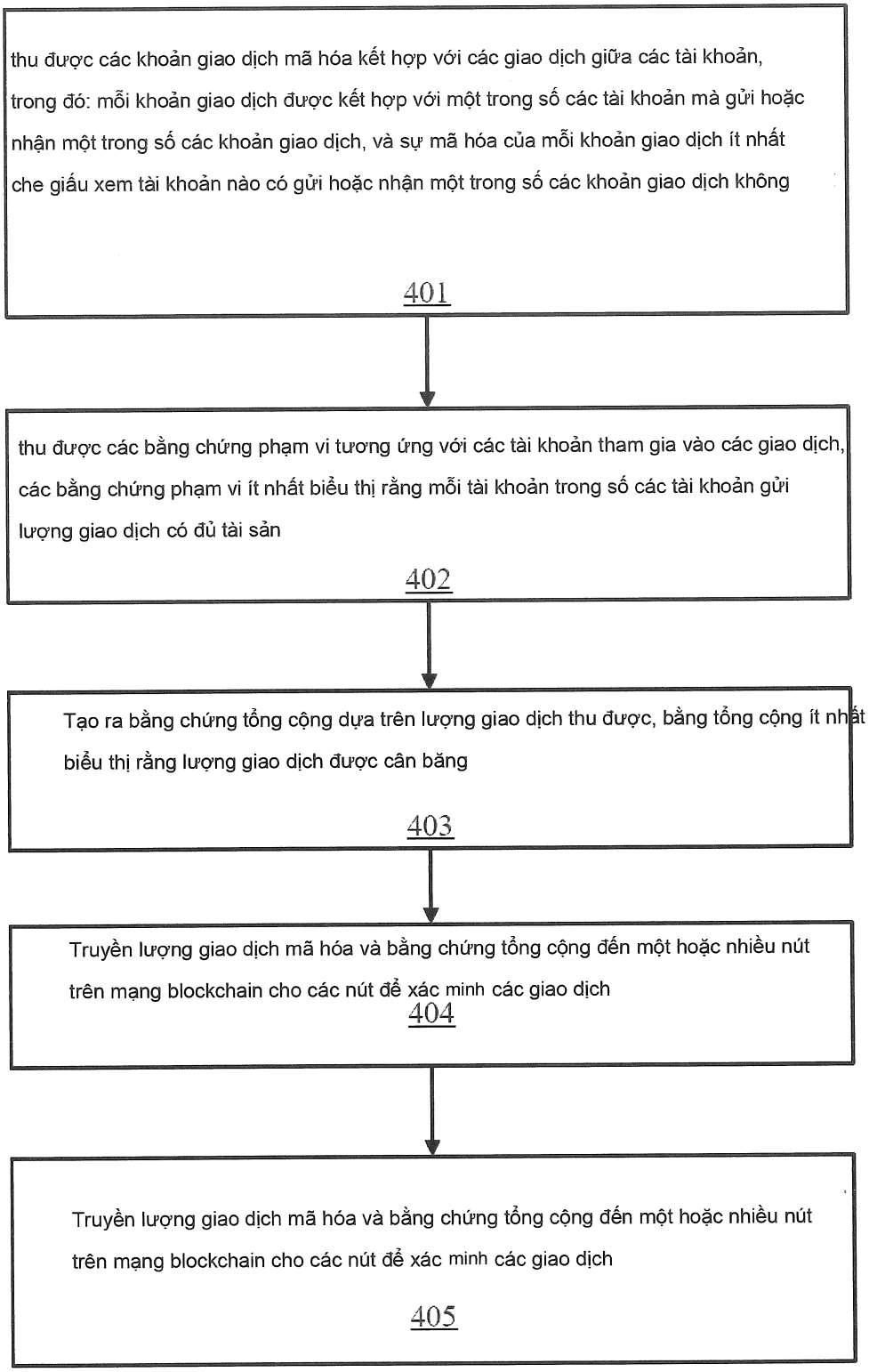

thu được các khoản giao dịch mã hóa kết hợp với các giao dịch giữa các tài khoản, trong đó: mỗi khoản giao dịch được kết hợp với một trong số các tài khoản mà gửi hoặc nhận một trong số các khoản giao dịch, và sự mã hóa của mỗi khoản giao dịch ít nhất che giấu xem tài khoản nào có gửi hoặc nhận một trong số các khoản giao dịch không
401
thu được các bằng chứng phạm vi tương ứng với các tài khoản tham gia vào các giao dịch, các bằng chứng phạm vi ít nhất biểu thị rằng mỗi tài khoản trong số các tài khoản gửi lượng giao dịch có đủ tài sản
402
Tạo ra bằng chứng tổng cộng dựa trên lượng giao dịch thu được, bằng tổng cộng ít nhất biểu thị rằng lượng giao dịch được cân bằng
403
Truyền lượng giao dịch mã hóa và bằng chứng tổng cộng đến một hoặc nhiều nút trên mạng blockchain cho các nút để xác minh các giao dịch
404
Truyền lượng giao dịch mã hóa và bằng chứng tổng cộng đến một hoặc nhiều nút trên mạng blockchain cho các nút để xác minh các giao dịch
405

FIG. 4

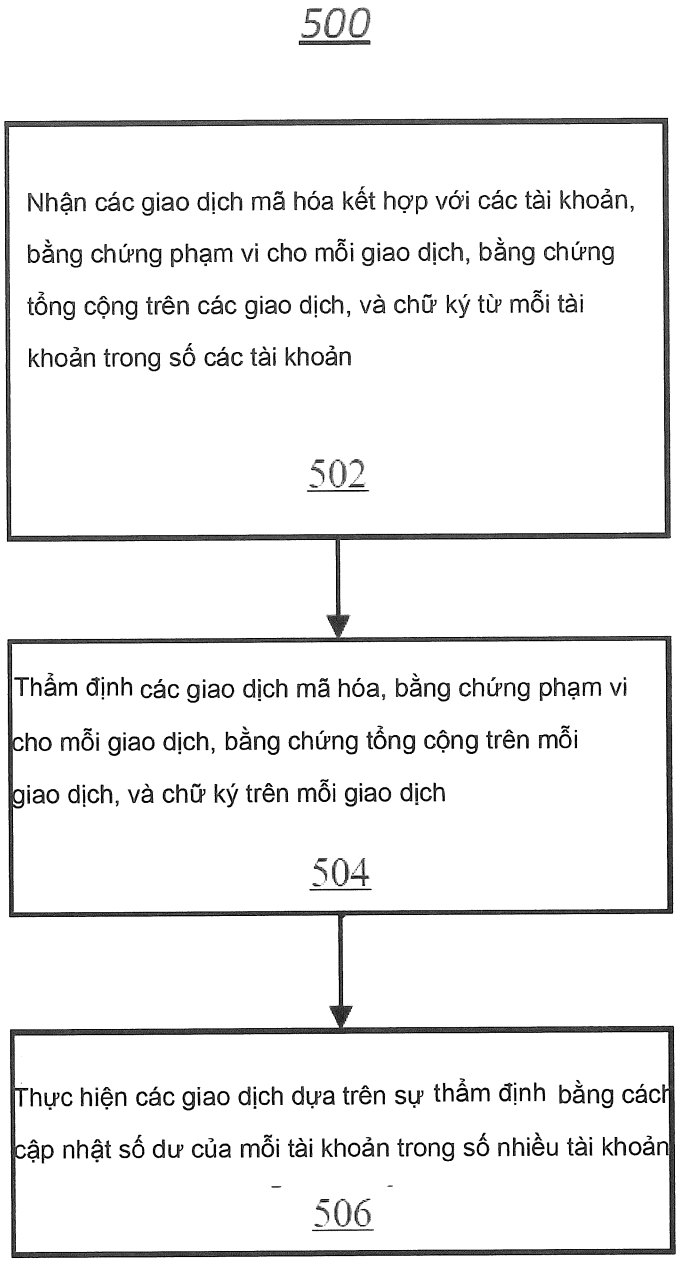

500
Nhận các giao dịch mã hóa kết hợp với các tài khoản, bằng chứng phạm vi cho mỗi giao dịch, bằng chứng tổng cộng trên các giao dịch, và chữ ký từ mỗi tài khoản trong số các tài khoản
502
Thẩm định các giao dịch mã hóa, bằng chứng phạm vi cho mỗi giao dịch, bằng chứng tổng cộng trên mỗi giao dịch, và chữ ký trên mỗi giao dịch
504
Thực hiện các giao dịch dựa trên sự thẩm định bằng cách cập nhật số dư của mỗi tài khoản trong số nhiều tài khoản
506

FIG. 5

600

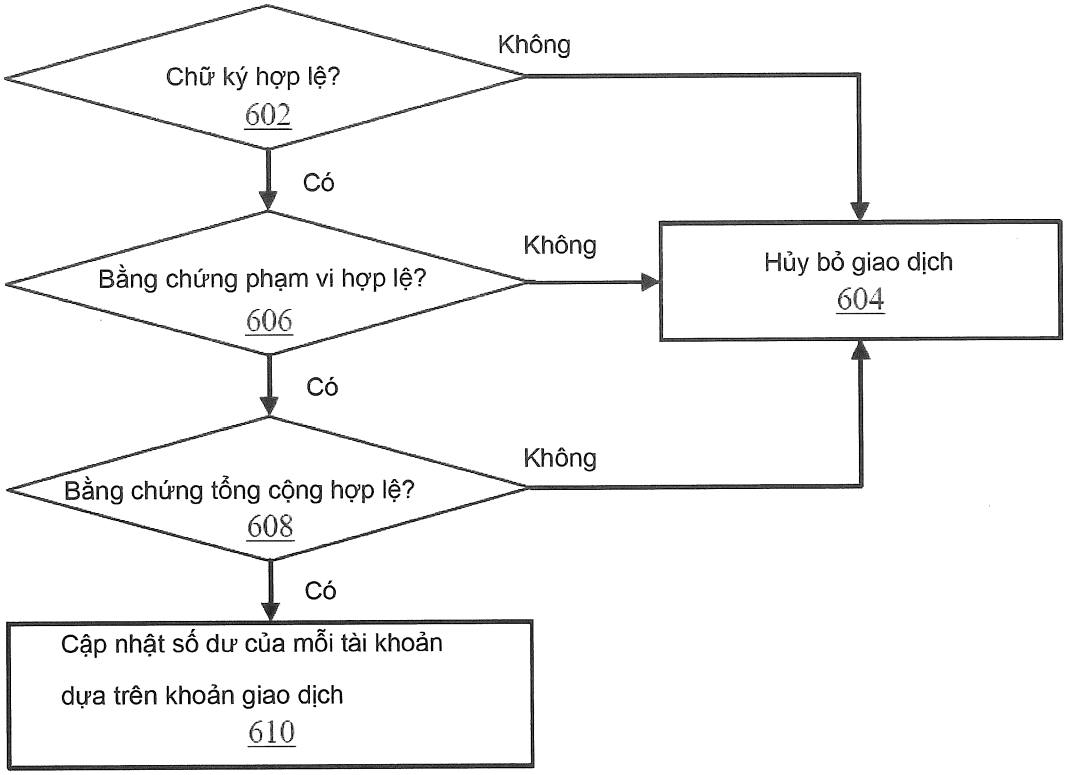

Chữ ký hợp lệ?
602
Không
Có
Bằng chứng phạm vi hợp lệ?
606
Không
Hủy bỏ giao dịch
604
Có
Bằng chứng tổng cộng hợp lệ?
608
Không
Có
Cập nhật số dư của mỗi tài khoản
dựa trên khoản giao dịch
610

FIG. 6

7/7

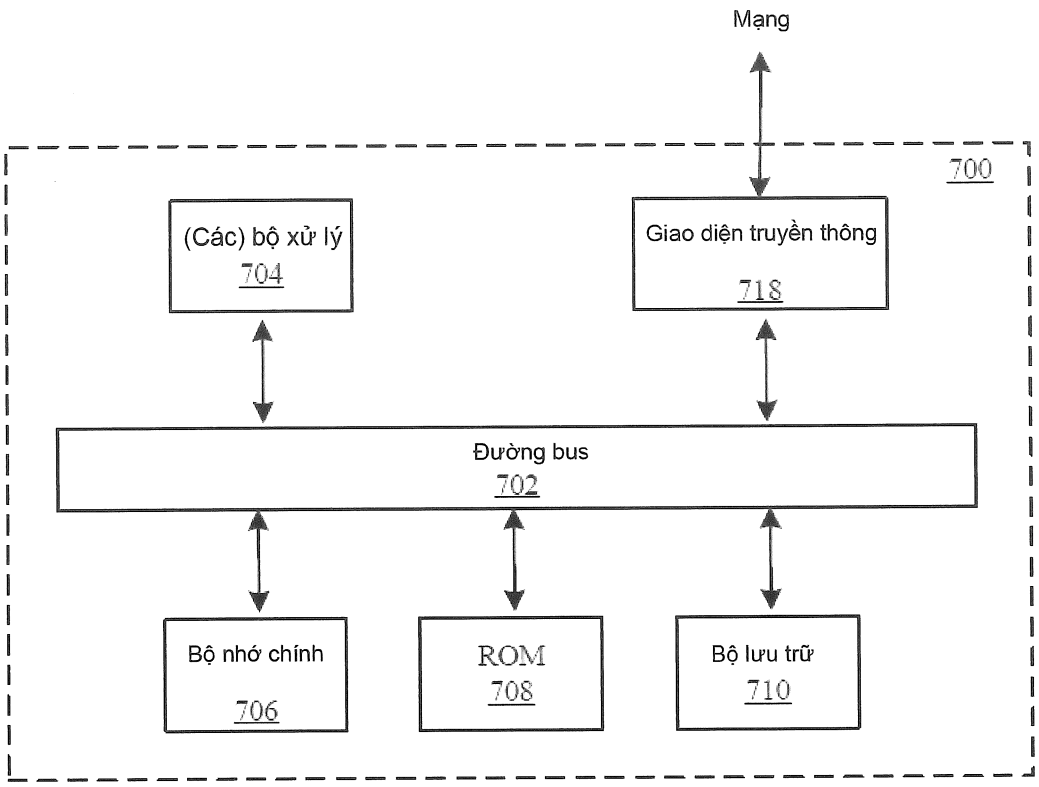

Mạng
700
(Các) bộ xử lý
704
Giao diện truyền thông
718
Đường bus
702
Bộ nhớ chính
706
ROM
708
Bộ lưu trữ
710

FIG. 7