(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) **1-0037790**

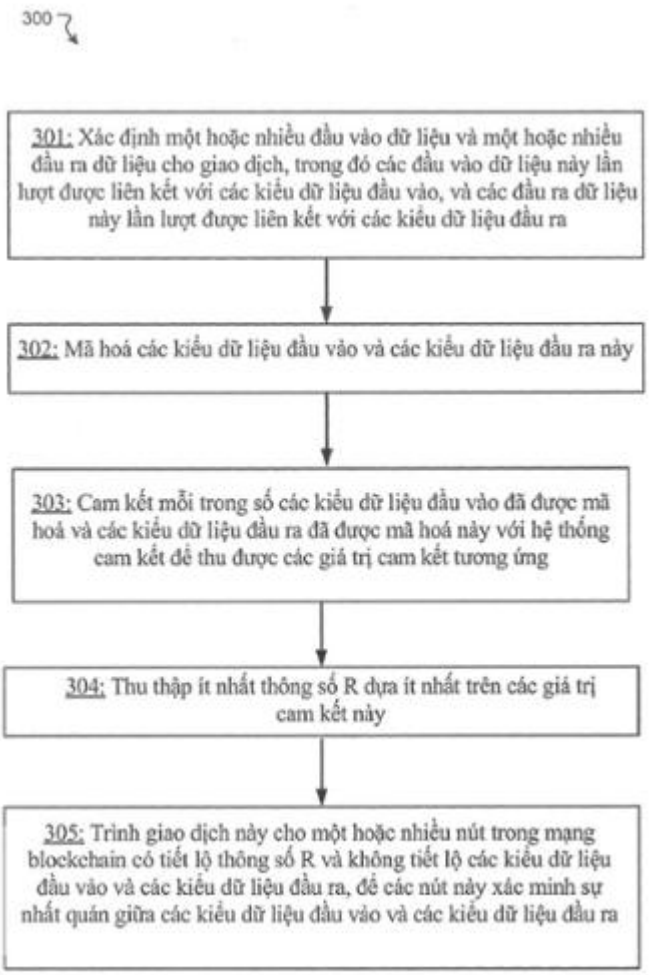
(51)[7] **G06Q 40/04**; H04L 9/32; H04L 29/08; G06Q 20/38; H04L 29/06

(13) **B**

(21) 1-2019-01911
(22) 27/11/2018
(86) PCT/CN2018/117548 27/11/2018
(87) WO 2019/072275 14/08/2019
(45) 25/12/2023 429
(43) 25/11/2019 380A
(73) ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) MA, Baoli (CN); ZHANG, Wenbin (CN); LI, Lichun (CN); LIU, Zheng (CN); YIN, Shan (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 xuất phương pháp được thực hiện bằng máy tính để bảo vệ thông tin, phương pháp này bao gồm các bước: xác định một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu cho giao dịch, trong đó các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra; mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này; cam kết mỗi trong số các kiểu dữ liệu đầu vào đã được mã hóa và các kiểu dữ liệu đầu ra đã được mã hóa này với hệ thống cam kết để thu được các giá trị cam kết tương ứng; thu thập ít nhất thông số R dựa ít nhất trên các giá trị cam kết này; và trình giao dịch này cho một hoặc nhiều nút trong mạng blockchain (chuỗi khối) có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra để các nút này xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra.


300
301: Xác định một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu cho giao dịch, trong đó các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra
302: Mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này
303: Cam kết mỗi trong số các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá này với hệ thống cam kết để thu được các giá trị cam kết tương ứng
304: Thu thập ít nhất thông số R dựa ít nhất trên các giá trị cam kết này
305: Trình giao dịch này cho một hoặc nhiều nút trong mạng blockchain có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra, để các nút này xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập chung đến các phương pháp và các thiết bị để bảo vệ thông tin.

Tình trạng kỹ thuật của sáng chế

Sự bí mật là yếu tố quan trọng đối với các hoạt động liên lạc và truyền tải dữ liệu giữa những người dùng khác nhau. Không có sự bảo vệ, thì người dùng có nguy cơ bị đánh cắp danh tính, chuyển tiền bất hợp pháp, hoặc những thiệt hại tiềm tàng khác. Nguy cơ này trở nên càng lớn khi các hoạt động liên lạc và chuyển tiền được thực hiện trực tuyến, vì khả năng tiếp cận tự do đến các thông tin trực tuyến.

Bản chất kỹ thuật của sáng chế

Theo các phương án khác nhau, sáng chế bao gồm các hệ thống, các phương pháp, và phương tiện bất biến đọc được bằng máy tính để bảo vệ thông tin.

Theo một khía cạnh, phương pháp được thực hiện bằng máy tính để bảo vệ thông tin bao gồm các bước: xác định một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu cho giao dịch, trong đó các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra; mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này; cam kết mỗi trong số các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá này với hệ thống cam kết để thu được các giá trị cam kết tương ứng; thu thập ít nhất thông số R dựa ít nhất trên các giá trị cam kết này; và trình giao dịch này cho một hoặc nhiều nút trong mạng blockchain (chuỗi khối) có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra để các nút này xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra.

Theo một số phương án, bước mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bao gồm bước mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bằng hàm băm.

Theo một số phương án, hệ thống cam kết nêu trên bao gồm cơ chế cam kết Pedersen.

Theo một số phương án, hệ thống cam kết này bao gồm ít nhất là nhân tố mù; và nhân tố mù này thay đổi theo thời gian cam kết các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá.

Theo một số phương án, các nút nêu trên được làm cho xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra mà không biết gì về các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này.

Theo một số phương án, giao dịch nêu trên là dựa ít nhất trên mô hình đầu ra giao dịch chưa tiêu dùng (Unspent Transaction Output - UTXO); và các đầu vào dữ liệu và các đầu ra dữ liệu bao gồm các kiểu của một hoặc nhiều tài sản của quá trình giao dịch.

Theo một số phương án, hệ thống cam kết nêu trên bao gồm các nhân tố mù lần lượt tương ứng với các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra; và bước thu thập ít nhất thông số R dựa ít nhất trên các giá trị cam kết bao gồm các bước: thu thập các hiệu số giữa các cặp giá trị cam kết; móc nối các hiệu số thu được; mã hoá các hiệu số đã được móc nối đó bằng hàm băm để thu được giá trị mã hoá x; và thu thập thông số R dựa ít nhất trên giá trị mã hoá x này và các hiệu số giữa các cặp nhân tố mù.

Theo một số phương án, bước trình giao dịch cho một hoặc nhiều nút trong mạng blockchain có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra để các nút đó xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bao gồm bước trình giao dịch cho một hoặc nhiều nút trong mạng blockchain có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra để khiến các nút đó: thu thập thông số R và điểm cơ sở G; thu thập các hiệu số giữa các cặp giá trị cam kết; móc nối các hiệu số thu được; mã hoá các hiệu số đã được móc nối đó bằng hàm băm để thu được giá trị mã hoá x; thu thập tổng C của các đa thức dựa ít nhất trên các hiệu số thu được và giá trị mã hoá x; đáp lại

việc xác định được rằng tổng C là bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán; và đáp lại việc xác định được rằng tổng C không bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán.

Theo khía cạnh khác, phương tiện lưu trữ bất biến đọc được bằng máy tính có lưu giữ các lệnh để được thực thi bằng bộ xử lý để khiến bộ xử lý đó thực hiện các thao tác bao gồm các bước: xác định một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu cho giao dịch, trong đó các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra; mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này; cam kết mỗi trong số các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá này với hệ thống cam kết để thu được các giá trị cam kết tương ứng; thu thập ít nhất thông số R dựa ít nhất trên các giá trị cam kết này; và trình giao dịch này cho một hoặc nhiều nút trong mạng blockchain (chuỗi khối) có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra để các nút này xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra.

Theo khía cạnh khác, hệ thống để bảo vệ thông tin bao gồm bộ xử lý và phương tiện lưu trữ bất biến đọc được bằng máy tính được ghép nối với bộ xử lý này, phương tiện lưu trữ này lưu giữ các lệnh để được thực thi bằng bộ xử lý này để khiến hệ thống này thực hiện các thao tác bao gồm các bước: xác định một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu cho giao dịch, trong đó các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra; mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này; cam kết mỗi trong số các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá này với hệ thống cam kết để thu được các giá trị cam kết tương ứng; thu thập ít nhất thông số R dựa ít nhất trên các giá trị cam kết này; và trình giao dịch này cho một hoặc nhiều nút trong mạng blockchain (chuỗi khối) có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra để các nút này xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra.

Theo khía cạnh khác, phương pháp được thực hiện bằng máy tính để bảo vệ thông tin bao gồm bước: thu thập, bởi một hoặc nhiều nút trong mạng blockchain, giao dịch được khởi tạo bởi nút khởi tạo. Giao dịch này được liên kết với một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu. Các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra. Các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này được mã hoá và được cam kết với hệ thống cam kết để thu được các giá trị cam kết tương ứng. Các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này không được tiết lộ cho một hoặc nhiều nút đó. Phương pháp bảo vệ thông tin nêu trên còn bao gồm các bước: xác minh, bởi một hoặc nhiều nút nêu trên, sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra; đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán, thì bổ sung, bởi một hoặc nhiều nút này, giao dịch nêu trên vào mạng blockchain này; và đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán, thì từ chối, bởi một hoặc nhiều nút này, không cho bổ sung giao dịch này vào mạng blockchain này.

Theo một số phương án, bước xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bao gồm các bước: thu thập thông số R và điểm cơ sở G; thu thập các hiệu số giữa các cặp giá trị cam kết; móc nối các hiệu số thu được; mã hoá các hiệu số đã được móc nối đó bằng hàm băm để thu được giá trị mã hoá x; thu thập tổng C của các đa thức dựa ít nhất trên các hiệu số thu được và giá trị mã hoá x; và xác định xem tổng C có bằng tích của thông số R và điểm cơ sở G hay không.

Theo một số phương án, phương pháp này còn bao gồm các bước: đáp lại việc xác định được rằng tổng C là bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán; và đáp lại việc xác định được rằng tổng C không bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán.

Theo một số phương án, một hoặc nhiều nút nêu trên bao gồm các nút đồng thuận.

Theo khía cạnh khác, phương tiện lưu trữ bất biến đọc được bằng máy tính có lưu giữ các lệnh để được thực thi bằng bộ xử lý để khiến bộ xử lý đó thực hiện các

thao tác bao gồm các bước: thu thập, bởi một hoặc nhiều nút trong mạng blockchain, giao dịch được khởi tạo bởi nút khởi tạo. Giao dịch này được liên kết với một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu. Các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra. Các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này được mã hoá và được cam kết với hệ thống cam kết để thu được các giá trị cam kết tương ứng. Các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này không được tiết lộ cho một hoặc nhiều nút đó. Các thao tác này còn bao gồm các bước: xác minh, bởi một hoặc nhiều nút này, sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra; đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán, thì bổ sung, bởi một hoặc nhiều nút này, giao dịch này vào mạng blockchain này; và đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán, thì từ chối, bởi một hoặc nhiều nút này, không cho bổ sung giao dịch này vào mạng blockchain này.

Theo khía cạnh khác, hệ thống để bảo vệ thông tin bao gồm bộ xử lý và phương tiện lưu trữ bất biến đọc được bằng máy tính được ghép nối với bộ xử lý này, phương tiện lưu trữ này lưu giữ các lệnh để được thực thi bằng bộ xử lý này để khiến hệ thống này thực hiện các thao tác bao gồm các bước: thu thập, bởi một hoặc nhiều nút trong mạng blockchain, giao dịch được khởi tạo bởi nút khởi tạo. Giao dịch này được liên kết với một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu. Các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra. Các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này được mã hoá và được cam kết với hệ thống cam kết để thu được các giá trị cam kết tương ứng. Các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này không được tiết lộ cho một hoặc nhiều nút đó. Các thao tác này còn bao gồm các bước: xác minh, bởi một hoặc nhiều nút này, sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra; đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán, thì bổ sung, bởi một hoặc nhiều nút này, giao dịch này vào mạng blockchain này; và đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán, thì

từ chối, bởi một hoặc nhiều nút này, không cho bổ sung giao dịch này vào mạng blockchain này.

Các dấu hiệu này và các dấu hiệu khác của các hệ thống, các phương pháp, và phương tiện bất biến đọc được bằng máy tính được bộc lộ ở đây, cũng như các phương pháp vận hành và các chức năng của các phần tử liên quan của cấu trúc và sự kết hợp của các bộ phận và tính kinh tế của quá trình sản xuất, sẽ được làm rõ hơn nhờ phần mô tả sau đây và các điểm yêu cầu bảo hộ kèm theo dựa vào các hình vẽ kèm theo, tất cả trong số chúng tạo thành một phần của bản mô tả này, trong đó các số chỉ dẫn giống nhau thì thể hiện các bộ phận tương ứng trên các hình vẽ khác nhau. Tuy nhiên, cần hiểu rằng các hình vẽ đó là chỉ nhằm mục đích minh hoạ và mô tả chứ 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 thể hiện hệ thống ví dụ để bảo vệ thông tin, theo các phương án khác nhau.

Fig.2 là hình vẽ thể hiện các bước ví dụ để khởi tạo và xác minh giao dịch, theo các phương án khác nhau.

Fig.3 là hình vẽ thể hiện lưu đồ của phương pháp ví dụ để bảo vệ thông tin, theo các phương án khác nhau.

Fig.4 là hình vẽ thể hiện lưu đồ của phương pháp ví dụ để bảo vệ thông tin, theo các phương án khác nhau.

Fig.5 là hình vẽ thể hiện sơ đồ khối của hệ thống máy tính ví dụ mà trong đó phương án bất kỳ trong số các phương án được mô tả ở đây có thể được thực hiện.

Mô tả chi tiết các phương án thực hiện sáng chế

Blockchain có thể được coi là cơ sở dữ liệu không tập trung, thường được gọi là sổ cái phân tán, bởi vì sự hoạt động là được thực hiện bởi các nút khác nhau (ví dụ, các thiết bị điện toán) trong mạng. Bất kỳ thông tin nào cũng có thể được ghi vào blockchain và được lưu vào hoặc được đọc từ nó. Bất kỳ ai cũng có thể cài đặt máy chủ và gia nhập mạng blockchain để trở thành một nút. Bất kỳ nút nào cũng có thể góp phần vào công suất tính toán để duy trì blockchain bằng cách thực hiện các hoạt động tính toán phức tạp, chẳng hạn phép tính băm, để bổ sung một khối vào blockchain hiện tại, và khối được bổ sung đó có thể chứa các loại dữ liệu hoặc thông tin khác nhau. Nút mà góp phần vào công suất tính toán đối với khối được bổ sung vào thì có thể được thưởng thẻ bài (ví dụ, đơn vị tiền kỹ thuật số). Vì blockchain không có nút trung tâm nào, nên mọi nút là bình đẳng và giữ toàn bộ cơ sở dữ liệu blockchain.

Các nút là, ví dụ, các thiết bị điện toán hoặc các hệ thống máy tính lớn mà hỗ trợ mạng blockchain và giữ cho nó chạy trơn tru. Các nút có thể được chạy bởi những cá nhân hoặc các nhóm người góp tiền mua các hệ thống máy tính mạnh mẽ, được gọi là các giàn máy khai thác. Có hai loại nút, là các nút đầy đủ và các nút hạng nhẹ. Các nút đầy đủ thì giữ bản sao hoàn chỉnh của blockchain. Các nút đầy đủ trên mạng blockchain sẽ thẩm định các giao dịch và các khối mà chúng nhận được, và chuyển tiếp chúng đến các điểm ngang hàng được kết nối để cung cấp sự xác minh đồng thuận đối với các giao dịch. Ngược lại, các nút hạng nhẹ chỉ tải xuống một phần của blockchain. Ví dụ, các nút hạng nhẹ thì được sử dụng cho các giao dịch tiền kỹ thuật số. Nút hạng nhẹ sẽ giao tiếp với nút đầy đủ khi nó muốn giao dịch.

Thuộc tính phi tập trung hoá này có thể giúp ngăn chặn sự xuất hiện của trung tâm quản lý ở vị trí được kiểm soát. Ví dụ, việc duy trì bitcoin (một loại tiền kỹ thuật số) blockchain là được thực hiện bởi mạng gồm các nút giao tiếp của phần mềm bitcoin trong khu vực chạy. Tức là, thay vì các ngân hàng, các cơ quan, hoặc các đơn vị quản lý hành chính theo cách truyền thống, thì có nhiều trung gian tồn tại dưới dạng các máy tính chủ chạy phần mềm bitcoin. Các máy tính chủ này tạo thành mạng được kết nối qua Internet, trong đó bất kỳ ai cũng có thể gia nhập mạng. Các giao dịch trong mạng có thể có dạng: "người dùng A muốn gửi Z bitcoin đến người dùng B", trong đó

các giao dịch này được phát quảng bá đến mạng nhờ sử dụng các ứng dụng phần mềm đã sẵn có. Các máy tính chủ này có chức năng như các máy chủ bitcoin mà hoạt động được để thẩm định các giao dịch tài chính này, bổ sung bản ghi về chúng đến bản sao sổ cái của chúng, rồi sau đó phát quảng bá những sự bổ sung vào sổ cái này đến các máy chủ khác của mạng.

Việc duy trì blockchain được gọi là "khai thác", và những người làm công việc duy trì đó sẽ được thưởng những bitcoin được tạo mới và các phí giao dịch như đã nêu trên. Ví dụ, các nút có thể xác định xem các giao dịch có hợp lệ hay không, dựa trên tập hợp quy tắc mà mạng blockchain đã đồng thuận. Những máy khai thác có thể được đặt trên lục địa bất kỳ và xử lý các thanh toán bằng cách xác minh rằng mỗi giao dịch là hợp lệ và bổ sung nó vào blockchain. Việc xác minh đó được thực hiện thông qua sự đồng thuận của những máy khai thác và giả định rằng không có sự thông đồng có hệ thống nào. Cuối cùng, tất cả dữ liệu sẽ nhất quán, bởi vì việc tính toán phải thoả mãn các yêu cầu nhất định để là hợp lệ và tất cả các nút sẽ được đồng bộ để bảo đảm rằng blockchain là nhất quán.

Thông qua quá trình khai thác, thì các giao dịch, chẳng hạn các hoạt động chuyển nhượng tài sản, là được xác minh và được các nút mạng bổ sung vào chuỗi khối đang tăng trưởng của blockchain. Bằng cách duyệt toàn bộ blockchain, thì hoạt động xác minh có thể bao gồm, ví dụ, việc xem bên thanh toán có quyền tiếp cận tài sản chuyển nhượng hay không, việc xem tài sản đã được tiêu dùng trước đó chưa, việc xem lượng chuyển nhượng có đúng không, v.v.. Ví dụ, trong một giao dịch giả thiết (ví dụ, giao dịch các bitcoin dưới mô hình UTXO (Unspent Transaction Output - đầu ra giao dịch chưa tiêu dùng)) được ký số bởi người gửi, thì giao dịch được đề xuất này có thể được phát quảng bá đến mạng blockchain để khai thác. Máy khai thác cần phải kiểm tra xem giao dịch này có đủ điều kiện để thực hiện hay không, theo lịch sử blockchain. Nếu số dư trong ví tiền của người gửi có đủ ngân quỹ theo lịch sử blockchain hiện có, thì giao dịch được coi là hợp lệ và có thể được bổ sung vào khối. Khi đã được xác minh, thì các hoạt động chuyển nhượng tài sản đó có thể được bao gồm vào khối tiếp theo để bổ sung vào blockchain.

Một khối là rất giống như một bản ghi của cơ sở dữ liệu. Mỗi lần ghi dữ liệu sẽ tạo ra một khối. Các khối này được liên kết và được bảo vệ bằng mật mã để trở thành

các mạng được nối với nhau. Mỗi khối đều được nối với khối đằng trước, đó cũng là nguồn gốc của cái tên "blockchain" (chuỗi khối). Mỗi khối thường chứa mật mã băm của khối đằng trước, thời điểm sinh ra, và dữ liệu thực tế. Ví dụ, mỗi khối đều chứa hai phần: mào đầu khối để ghi giá trị đặc trưng của khối hiện tại, và thân để ghi dữ liệu thực tế (ví dụ, dữ liệu giao dịch). Chuỗi khối này được liên kết thông qua các mào đầu khối. Mỗi mào đầu khối có thể chứa các giá trị đặc trưng, chẳng hạn phiên bản, giá trị băm của khối đằng trước, gốc Merkle, mốc thời gian, độ khó mục tiêu, và số nonce (số chỉ dùng một lần). Giá trị băm của khối đằng trước không chỉ chứa địa chỉ của khối đằng trước, mà còn chứa giá trị băm của dữ liệu bên trong khối đằng trước, từ đó làm cho các blockchain không thể thay đổi được. Số nonce là số mà khi được bao gồm vào thì tạo ra giá trị băm có một số lượng cụ thể các bit số không dẫn đầu.

Để khai thác, thì giá trị băm của các nội dung của khối mới là được lấy bởi nút. Số nonce (ví dụ, chuỗi ngẫu nhiên) được thêm vào giá trị băm này để thu được chuỗi mới. Chuỗi mới này lại được băm. Sau đó, giá trị băm cuối cùng được so sánh với độ khó mục tiêu (ví dụ, mức độ), và giá trị băm cuối cùng này được xác định xem có thực sự nhỏ hơn độ khó mục tiêu hay không. Nếu không, thì số nonce này được thay đổi và tiến trình lặp lại. Nếu có, thì khối này được bổ sung vào chuỗi và sổ cái công khai được cập nhật và được báo về việc bổ sung này. Nút mà có công bổ sung thành công đó sẽ được thưởng các bitcoin, ví dụ, bằng cách bổ sung giao dịch phần thưởng đến chính nó vào khối mới (được gọi là quá trình sinh coinbase).

Tức là, đối với mỗi đầu ra "Y", nếu k được chọn từ sự phân bố có min entropy cao, thì không thể tìm được đầu vào x sao cho H(k|x) = Y, trong đó K là số nonce, x là giá trị băm của khối, Y là độ khó mục tiêu, và "|" biểu thị sự móc nối. Tính đến việc các mật mã băm về cơ bản là ngẫu nhiên, khi đầu ra của chúng là không thể được dự đoán từ những đầu vào của chúng, thì chỉ có một cách đã biết để tìm được số nonce: thử từng số nguyên một, ví dụ 1, rồi 2, rồi 3, v.v., cách này có thể được gọi là cách brute-force. Số lượng số không dẫn đầu mà càng lớn thì cần thời gian trung bình càng lâu để tìm được số nonce Y cần thiết. Theo một ví dụ, hệ thống bitcoin liên tục điều chỉnh số lượng số không dẫn đầu, nên thời gian trung bình để tìm được số nonce là khoảng mười phút. Theo cách đó, khi các năng lực xử lý của phần cứng điện toán tăng lên theo thời gian, nên qua những năm, thì giao thức bitcoin sẽ chỉ cần nhiều bit số

không dẫn đầu hơn để làm cho hoạt động khai thác luôn cần một khoảng thời gian khoảng mười phút để thực hiện.

Như đã mô tả, việc băm là nền móng quan trọng đối với blockchain. Thuật toán băm có thể được hiểu là hàm mà nén các thông điệp có chiều dài bất kỳ thành thông điệp rút gọn có chiều dài cố định. Được sử dụng phổ biến hơn là MD5 và SHA. Theo một số phương án, chiều dài băm của blockchain là 256 bit, điều này có nghĩa là cho dù nội dung gốc là gì, thì số nhị phân 256 bit cũng được tính toán cuối cùng. Và có thể bảo đảm rằng giá trị băm tương ứng là độc nhất, miễn là nội dung gốc là khác nhau. Ví dụ, giá trị băm của chuỗi "123" là a8fdc205a9f19cc1c7507a60c4f01b13d11d7fd0 (hệ thập lục phân), mà có 256 bit khi được chuyển sang nhị phân, và chỉ "123" là có giá trị băm này. Thuật toán băm trong blockchain là không thể đảo ngược, tức là, phép tính thuận thì dễ (từ "123" sang a8fdc205a9f19cc1c7507a60c4f01b1c7507a60c4f01b13d11d7fd0), còn phép tính ngược thì không thể thực hiện được ngay cả khi đã dùng hết tất cả các tài nguyên điện toán. Do đó, giá trị băm của mỗi khối của blockchain là độc nhất.

Ngoài ra, nếu nội dung của khối thay đổi, thì giá trị băm của nó sẽ thay đổi. Khối và giá trị băm có sự tương ứng một-một, và giá trị băm của mỗi khối là được tính toán cụ thể cho mào đầu khối. Tức là, các giá trị đặc trưng của các mào đầu khối là được kết nối để tạo thành chuỗi dài, và sau đó, giá trị băm được tính toán cho chuỗi này. Ví dụ, "Hash = SHA256 (mào đầu khối)" là công thức tính giá trị băm của khối, SHA256 là thuật toán băm blockchain được áp dụng cho mào đầu khối. Giá trị băm này được xác định độc nhất bởi mào đầu khối, chứ không phải thân khối. Như đã nêu trên, mào đầu khối chứa nhiều nội dung, bao gồm giá trị băm của khối hiện tại, và giá trị băm của khối đằng trước. Điều này có nghĩa là nếu các nội dung của khối hiện tại thay đổi, hoặc nếu giá trị băm của khối đằng trước thay đổi, thì điều đó sẽ gây ra sự thay đổi giá trị băm ở khối hiện tại. Nếu hacker cải biến một khối, thì giá trị băm của khối đó sẽ thay đổi. Để khối sau đó kết nối đến khối bị cải biến này, thì hacker phải lần lượt cải biến tất cả các khối đằng sau, bởi vì khối tiếp theo phải chứa giá trị băm của khối đằng trước. Nếu không thì khối bị cải biến sẽ bị tách khỏi blockchain. Vì những lý do thiết kế, nên các phép tính băm đều tốn thời gian, và gần như không thể cải biến nhiều khối trong một khoảng thời gian ngắn trừ khi hacker đã làm chủ quá

51% công suất tính toán của toàn bộ mạng. Do đó, blockchain bảo đảm độ tin cậy của riêng nó, và một khi dữ liệu đã được ghi, thì nó không thể bị can thiệp.

Khi máy khai thác tìm thấy giá trị băm này (tức là chữ ký hoặc nghiệm thích hợp) cho khối mới, thì máy khai thác sẽ phát quảng bá chữ ký này đến tất cả các máy khai thác còn lại (là các nút của blockchain). Những máy khai thác khác sẽ lần lượt xác minh xem nghiệm đó có tương ứng với bài toán của khối của người gửi hay không (tức là, xác định xem giá trị băm được nhập vào có thực sự cho kết quả là chữ ký đó hay không). Nếu nghiệm đó là hợp lệ, thì những máy khai thác còn lại sẽ xác nhận nghiệm đó và đồng ý rằng khối mới đó có thể được bổ sung vào blockchain. Do đó, đạt được sự đồng thuận về khối mới đó. Cái này còn được gọi là "bằng chứng công việc". Lúc này, khối mà đã đạt được sự đồng thuận có thể được bổ sung vào blockchain và được phát quảng bá đến tất cả các nút trên mạng cùng với chữ ký của nó. Các nút sẽ chấp nhận khối đó và lưu nó vào dữ liệu giao dịch của chúng chừng nào mà các giao dịch bên trong khối đó tương ứng đúng với các số dư trong ví tiền hiện tại (lịch sử giao dịch) tại thời điểm đó. Mỗi lần một khối mới được bổ sung lên trên khối này, thì sự bổ sung này cũng được tính là sự "xác nhận" khác đối với các khối trước nó. Ví dụ, nếu một giao dịch được bao gồm ở khối 502, và blockchain dài 507 khối, thì điều đó có nghĩa là giao dịch này có năm lần xác nhận (tương ứng với các khối 507 đến 502). Giao dịch có càng nhiều lần xác nhận thì những kẻ tấn công càng khó thay đổi.

Theo một số phương án, hệ thống tài sản blockchain được nêu làm ví dụ sử dụng mật mã khoá công khai, trong đó có hai khoá mật mã, là một khoá công khai và một khoá bí mật, được tạo ra. Khoá công khai có thể được coi là số tài khoản, và khoá bí mật có thể được coi là chứng thư quyền sở hữu. Ví dụ, ví tiền bitcoin là tập hợp của khoá công khai và khoá bí mật. Quyền sở hữu tài sản (ví dụ, tiền kỹ thuật số, tài sản tiền mặt, cổ phiếu, vốn cổ phần, trái phiếu), mà được liên kết với địa chỉ tài sản nhất định, là có thể được biểu diễn bằng sự nhận biết về khoá bí mật thuộc về địa chỉ đó. Ví dụ, phần mềm ví tiền bitcoin, đôi khi được gọi là "phần mềm máy khách bitcoin", cho phép người dùng cụ thể giao dịch các bitcoin. Chương trình ví tiền sẽ tạo ra và lưu giữ các khoá bí mật và giao tiếp với các điểm ngang hàng trên mạng bitcoin.

Trong các giao dịch blockchain, thì những người trả tiền và những người được trả tiền là được nhận dạng trong blockchain bằng các khoá mật mã công khai của họ. Ví dụ, phần lớn các hoạt động chuyển nhượng bitcoin đương thời là từ khoá công khai này sang khoá công khai khác. Trên thực tế, các giá trị băm của các khoá này là được sử dụng trong blockchain và được gọi là "các địa chỉ bitcoin". Về nguyên lý, nếu kẻ tấn công giả thiết là người S có thể lấy cắp tiền từ người A bằng cách chỉ cần bổ sung các giao dịch vào sổ cái blockchain kiểu như "người A trả tiền cho người S là 100 bitcoin", nhờ sử dụng các địa chỉ bitcoin của những người dùng thay vì tên của họ. Giao thức bitcoin ngăn chặn loại trộm cắp này bằng cách yêu cầu mỗi lần chuyển nhượng phải được ký số bằng khoá bí mật của người trả tiền, và chỉ có các hoạt động chuyển nhượng đã được ký mới có thể được bổ sung vào sổ cái blockchain. Vì người S không thể giả mạo chữ ký của người A, nên người S không thể lừa người A bằng cách thêm mục nhập kiểu như "người A trả 200 bitcoin cho người S" vào blockchain. Đồng thời, bất kỳ ai cũng có thể xác minh chữ ký của người A nhờ sử dụng khoá công khai của người đó, và do đó, xác minh rằng người đó đã uỷ quyền giao dịch nào trong blockchain mà trong đó người đó là người trả tiền.

Trong ngữ cảnh giao dịch bitcoin, để chuyển nhượng một số bitcoin sang người dùng B, thì người dùng A có thể xây dựng bản ghi có chứa thông tin về giao dịch này thông qua một nút. Bản ghi này có thể được ký bằng khoá ký (khoá bí mật) của người dùng A và có chứa khoá xác minh công khai của người dùng A và khoá xác minh công khai của người dùng B. Chữ ký này được dùng để xác nhận rằng giao dịch là đến từ người dùng, và cũng ngăn không cho giao dịch bị thay đổi bởi bất kỳ ai một khi nó đã được ban hành. Bản ghi mà được bó buộc với bản ghi khác mà đã diễn ra trong cùng cửa sổ thời gian trong khối mới thì có thể được phát quảng bá đến các nút đầy đủ. Khi nhận được các bản ghi này, thì các nút đầy đủ có thể kết hợp các bản ghi này vào sổ cái của tất cả các giao dịch mà đã từng diễn ra trong hệ thống blockchain, bổ sung khối mới này vào blockchain đã được chấp nhận trước đó thông qua quá trình khai thác nêu trên, và thẩm định khối được bổ sung này dựa trên các quy tắc đồng thuận của mạng.

Tài sản cần được chuyển nhượng của người dùng A có thể có dạng UTXO (Unspent Transaction Output - đầu ra giao dịch chưa tiêu dùng). UTXO là mô hình

đối tượng blockchain. Trong UTXO, thì các tài sản là được biểu diễn bằng các đầu ra của các giao dịch blockchain mà chưa được tiêu dùng, mà có thể được dùng làm các đầu vào trong các giao dịch mới. Để tiêu dùng (giao dịch) tài sản, thì người dùng phải ký số bằng khoá bí mật. Bitcoin là một ví dụ về tiền kỹ thuật số mà sử dụng mô hình UTXO. Trong trường hợp giao dịch blockchain hợp lệ, thì các đầu ra chưa tiêu dùng có thể được dùng để thực hiện các giao dịch nữa. Theo một số phương án, thì chỉ những đầu ra chưa tiêu dùng mới có thể được sử dụng trong các giao dịch nữa để ngăn chặn việc tiêu dùng đúp và sự gian lận. Vì lý do này, nên các đầu vào trên blockchain sẽ được xoá khi giao dịch xuất hiện, đồng thời, các đầu ra là được tạo ra dưới dạng các UTXO. Các đầu ra giao dịch chưa tiêu dùng này có thể được sử dụng (bởi những người nắm giữ các khoá bí mật, ví dụ, những người có ví tiền kỹ thuật số) cho các giao dịch trong tương lai.

Vì blockchain và các sổ cái tương tự khác là hoàn toàn công khai, nên bản thân blockchain không có sự bảo vệ sự bí mật nào. Tính chất công khai của mạng P2P có nghĩa là, tuy những người sử dụng nó là không được nhận dạng bằng tên, nhưng việc liên kết các giao dịch với các cá nhân và các công ty vẫn khả thi. Ví dụ, trong các hoạt động chuyển tiền xuyên biên giới hoặc trong chuỗi cung ứng, thì các loại tài sản đều có giá trị bảo vệ sự bí mật ở mức độ cực kỳ cao, vì nếu có thông tin về loại tài sản, thì có thể suy ra vị trí cụ thể và danh tính của các bên giao dịch. Loại tài sản có thể bao gồm, ví dụ, tiền, tiền kỹ thuật số, hợp đồng, khế ước, hồ sơ y tế, chi tiết khách hàng, cổ phiếu, trái phiếu, vốn cổ phần, hoặc loại tài sản bất kỳ khác mà có thể được mô tả ở dạng số. Tuy mô hình UTXO có cung cấp sự ẩn danh cho các danh tính và lượng giao dịch, và đã được áp dụng cho Monero và Zcash (tiền kỹ thuật số), nhưng loại tài sản giao dịch vẫn chưa được bảo vệ. Do đó, vấn đề kỹ thuật mà sáng chế khắc phục là làm sao để bảo vệ thông tin trực tuyến, chẳng hạn sự bí mật của loại tài sản trong các giao dịch. Các hệ thống và các phương pháp được bộc lộ có thể được tích hợp vào mô hình UTXO để cung cấp sự bảo vệ sự bí mật cho nhiều nội dung giao dịch khác nhau.

Trong quá trình giao dịch, thì sự bảo vệ thông tin là yếu tố quan trọng để bảo đảm sự bí mật của người dùng, và loại tài sản giao dịch là một loại thông tin đang thiếu sự bảo vệ. Fig.1 là hình vẽ thể hiện hệ thống 100 được nêu làm ví dụ để bảo vệ thông tin, theo các phương án khác nhau. Như được thể hiện, mạng blockchain có thể

bao gồm nhiều nút (ví dụ, các nút đầy đủ được thực hiện ở các máy chủ, các máy tính, v.v.). Đối với một số nền tảng blockchain (ví dụ, NEO), thì các nút đầy đủ mà có quyền lực bầu chọn ở mức độ nhất định có thể được gọi là các nút đồng thuận, có trách nhiệm xác minh giao dịch. Theo sáng chế, thì các nút đầy đủ, các nút đồng thuận, hoặc các nút tương đương khác, đều có thể xác minh giao dịch.

Ngoài ra, như được thể hiện trên Fig.1, người dùng A và người dùng B có thể sử dụng các thiết bị tương ứng, chẳng hạn máy tính xách tay và điện thoại di động có chức năng như các nút hạng nhẹ, để thực hiện các giao dịch. Ví dụ, người dùng A có thể muốn giao dịch với người dùng B bằng cách chuyển nhượng một số tài sản trong tài khoản của người dùng A sang tài khoản của người dùng B. Người dùng A và người dùng B có thể sử dụng các thiết bị tương ứng đã được cài phần mềm blockchain thích hợp cho giao dịch. Thiết bị của người dùng A có thể được gọi là nút khởi tạo A mà khởi tạo giao dịch với thiết bị của người dùng B mà được gọi là nút bên nhận B. Nút A có thể truy cập blockchain thông qua việc giao tiếp với nút 1, và Nút B có thể truy cập blockchain thông qua việc giao tiếp với nút 2. Ví dụ, nút A và nút B có thể trình các giao dịch lên blockchain thông qua nút 1 và nút 2 để yêu cầu bổ sung các giao dịch vào blockchain. Ngoài blockchain, thì nút A và nút B có thể có các kênh giao tiếp khác. Ví dụ, nút A và nút B có thể thu thập khoá công khai của nhau thông qua đường giao tiếp Internet thông thường.

Mỗi trong số các nút trên Fig.1 có thể bao gồm bộ xử lý và phương tiện lưu trữ bất biến đọc được bằng máy tính có lưu giữ các lệnh để được thực thi bằng bộ xử lý này để khiến nút đó (ví dụ, bộ xử lý của nút đó) thực hiện các bước khác nhau để bảo vệ thông tin như được mô tả ở đây. Mỗi nút đó có thể được cài phần mềm (ví dụ, chương trình giao dịch) và/hoặc phần cứng (ví dụ, các dây dẫn, các kết nối không dây) để giao tiếp với các nút khác và/hoặc các thiết bị khác. Những chi tiết nữa về phần cứng và phần mềm của nút sẽ được mô tả sau dựa vào Fig.5.

Fig.2 là hình vẽ thể hiện các bước ví dụ để khởi tạo và xác minh giao dịch, theo các phương án khác nhau.

Việc khởi tạo giao dịch có thể được thực hiện bởi nút khởi tạo. Theo một số phương án, mỗi loại tài sản có thể được ánh xạ hoặc được gán vào một danh tính nhận

dạng độc nhất. Ví dụ, danh tính nhận dạng độc nhất đó có thể là số thứ tự sn được tính toán theo cách như sau:

Bước 1.2 sn = Hash (loại tài sản)

trong đó Hash() là hàm băm. Ngoài ra, loại tài sản có thể được mã hoá bởi hệ thống cam kết (ví dụ, cơ chế cam kết Pedersen) như sau:

Bước 1.3 $C(sn) = r \times G + sn \times H$

trong đó r là nhân tố mù ngẫu nhiên (được gọi theo cách khác là nhân tố liên kết) để cho phép che giấu, G và H là các đường sinh/các điểm cơ sở được thoả thuận công khai của đường cong elip và có thể được chọn ngẫu nhiên, sn là giá trị của sự cam kết, C(sn) là điểm gốc được dùng làm sự cam kết và được cung cấp cho đối tác, và H là điểm gốc khác. Tức là, G và H có thể là các thông số đã biết đối với các nút. Việc tạo ra theo kiểu "nothing up my sleeve" (không có gì trong tay áo tôi) đối với H là có thể được tạo ra bằng cách băm điểm cơ sở G bằng hàm băm mà ánh xạ từ điểm này đến điểm khác, với H= Hash(G). H và G là các thông số công khai của hệ thống đã cho (ví dụ, các điểm được sinh ra ngẫu nhiên trên đường cong elip). Nút gửi có thể đã công bố H và G đến tất cả các nút. Tuy phần nêu trên cung cấp ví dụ về cơ chế cam kết Pedersen dưới dạng đường cong elip, nhưng các dạng khác nhau của cơ chế cam kết Pedersen, hoặc các hệ thống cam kết khác, cũng có thể được sử dụng thay thế.

Hệ thống cam kết sẽ duy trì sự bí mật của dữ liệu nhưng cam kết đối với dữ liệu để nó không thể bị thay đổi về sau bởi người gửi dữ liệu. Nếu một bên chỉ biết giá trị cam kết (ví dụ, C(sn)), thì họ không thể xác định các giá trị dữ liệu nằm dưới nào (ví dụ, sn) đã và đang được cam kết. Cả dữ liệu (ví dụ, sn) và nhân tố mù (ví dụ, r) đều có thể được tiết lộ về sau (ví dụ, bởi nút khởi tạo), và người nhận (ví dụ, nút đồng thuận) sự cam kết có thể chạy sự cam kết và xác minh rằng dữ liệu được cam kết là khớp với dữ liệu được tiết lộ. Nhân tố mù hiện diện bởi vì nếu không có, thì người ta có thể thử đoán dữ liệu.

Các hệ thống cam kết là cách để người gửi (bên cam kết) cam kết một giá trị (ví dụ, sn) sao cho giá trị được cam kết đó vẫn còn là bí mật, nhưng có thể được tiết lộ về sau, khi bên cam kết tiết lộ thông số cần thiết của tiến trình cam kết. Các hệ thống cam kết mạnh mẽ có thể vừa có tính che giấu thông tin, vừa có tính liên kết tính toán. Che giấu có nghĩa là giá trị cụ thể sn và sự cam kết của giá trị đó C(sn) là không có

tính liên quan. Tức là, C(sn) không tiết lộ thông tin gì về sn. Với C(sn), G, và H đã biết, thì gần như không thể biết sn vì số ngẫu nhiên r. Hệ thống cam kết là có tính liên kết nếu không có cách hợp lý nào mà hai giá trị khác nhau có thể gây ra cùng một sự cam kết. Cơ chế cam kết Pedersen có tính che giấu và liên kết tính toán hoàn toàn dưới giả định logarit rời rạc.

Cơ chế 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): C(BF1, data1) + C(BF2, data2) == C(BF1+BF2, data1+data2); C(BF1, data1) − C(BF1, data1) == 0. Nói cách khác, sự cam kết bảo tồn tính cộng và thuộc tính giao hoán áp dụng, tức là, cơ chế cam kết Pedersen là đồng cấu 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.

Theo một phương án, cơ chế cam kết Pedersen mà được dùng để mã hoá giá trị đầu vào là có thể được xây dựng nhờ sử dụng các điểm của đường cong elip. Theo cách thông thường, thì khoá công khai mật mã đường cong elip (Elliptic Curve Cryptography - ECC) là được tạo ra bằng cách nhân đường sinh của nhóm (G) với khoá bí mật (r): Pub=rG. Kết quả có thể được xếp thứ tự thành mảng 33 byte. Các khoá công khai ECC có thể tuân theo thuộc tính đồng cấu có tính cộng nêu trên đối với các cơ chế cam kết Pedersen. Tức là: Pub1+Pub2=(r1+r2(mod n))G.

Cơ chế cam kết Pedersen dành cho giá trị đầu vào có thể được tạo ra bằng cách chọn đường sinh bổ sung dành cho nhóm (H, trong các phương trình dưới đây) sao cho không ai biết loga rời rạc dành cho đường sinh thứ hai H so với đường sinh thứ nhất G (hoặc ngược lại), nghĩa là không ai biết x sao cho rxG=H. Điều này có thể được thực hiện, ví dụ, nhờ sử dụng mật mã băm của G để chọn H: H=to_point(SHA256(ENCODE(G))).

Tính đến hai đường sinh G và H này, thì hệ thống cam kết được nêu làm ví dụ để mã hoá giá trị đầu vào có thể được xác định dưới dạng: commitment=rG+aH. Ở đây, r có thể là nhân tố mù bí mật, và a có thể là giá trị đầu vào được cam kết. Do đó, nếu sn được cam kết, thì có thể thu được hệ thống cam kết C(sn) = r×G + sn×H được mô tả trên đây. Các cơ chế cam kết Pedersen là bí mật theo lý thuyết thông tin: đối với sự cam kết bất kỳ, thì đều tồn tại nhân tố mù nào đó mà sẽ làm cho lượng bất kỳ khớp

với sự cam kết. Các cơ chế cam kết Pedersen có thể bảo đảm về mặt tính toán chống lại sự cam kết giả, ở chỗ sự ánh xạ tuỳ ý là có thể không được tính toán.

Bên (nút) mà đã cam kết giá trị có thể để ngỏ sự cam kết bằng cách bộc lộ giá trị gốc sn và nhân tố r mà hoàn thiện phương trình cam kết. Sau đó, bên muốn mở giá trị C(sn) sẽ lại tính toán sự cam kết để xác minh rằng giá trị gốc được chia sẻ là thực sự khớp với sự cam kết C(sn) nhận được ban đầu. Do đó, thông tin về loại tài sản có thể được bảo vệ bằng cách ánh xạ nó đến số thứ tự độc nhất, và sau đó mã hoá nó bằng cơ chế cam kết Pedersen. Số ngẫu nhiên r, mà được chọn khi tạo ra sự cam kết, làm cho bất kỳ ai cũng gần như không thể suy ra được loại tài sản được cam kết theo giá trị cam kết C(sn).

Theo một số phương án, khi áp dụng phương pháp bảo vệ thông tin về loại tài sản này theo mô hình UTXO, thì sự nhất quán giữa loại tài sản của đầu vào (sn_in) và loại tài sản của đầu ra (sn_out) của giao dịch có thể được xác minh để xác định tính hợp lệ của giao dịch. Ví dụ, các nút blockchain có thể từ chối các giao dịch hoặc các khối không đạt bài kiểm tra sự nhất quán để sn_in = = sn_out. Vì loại tài sản sn được mã hoá (ví dụ, bằng cơ chế cam kết Pedersen), nên bài kiểm tra sự nhất quán là để xác minh xem C(sn_in) = = C(sn_out) hay không.

Theo một số phương án, như được thể hiện trên Fig.2, bước 1, giao dịch kiểu UTXO có thể bao gồm m đầu vào (ví dụ, các tài sản khả dụng) và n đầu ra (ví dụ, các tài sản đã được chuyển nhượng và các tài sản còn lại). Các đầu vào có thể được biểu thị dưới dạng sn_in_k, trong đó $1 \leq k \leq m$, và các đầu ra có thể được biểu thị dưới dạng sn_out_k, trong đó $1 \leq k \leq n$. Một số trong số các đầu ra này có thể được chuyển nhượng sang nút bên nhận B, trong khi các đầu ra còn lại có thể quay trở lại nút khởi tạo A. Ví dụ, trong một giao dịch giả thiết, người dùng A có thể sở hữu tổng số là 5 bitcoin và 10 cổ phiếu trong ví tiền của mình, và đối với các đầu vào giao dịch, thì sn_in_1 = Hash(bitcoin) và sn_in_2 = Hash(stock). Nếu người dùng A muốn chuyển nhượng 3 bitcoin sang người dùng B, đối với các đầu ra giao dịch, thì sn_out_1 = Hash(bitcoin), sn_out_2 = Hash(bitcoin), và sn_out_3 = Hash(stock), nhờ đó một trong số các đầu ra bitcoin (3 bitcoin) là được đánh địa chỉ đến người dùng B, và đầu ra bitcoin còn lại (2 bitcoin) và đầu ra cổ phiếu là được đánh địa chỉ trở lại người dùng A.

Do đó, theo một số phương án, thì loại tài sản tương ứng đầu vào có thể được mã hoá dưới dạng:

$C\_in\_k = r\_in\_k \times G + sn\_in\_k \times H$, trong đó $1 \leq k \leq m$

Loại tài sản đầu ra là tương ứng với dạng mã hoá:

$C\_out\_k = r\_out\_k \times G + sn\_out\_k \times H$, trong đó $1 \leq k \leq n$

Với các loại tài sản được che giấu, thì bên khởi tạo giao dịch cần phải chứng minh cho các nút (ví dụ, các nút đầy đủ, các nút đồng thuận) rằng các loại tài sản đầu vào của giao dịch là lần lượt nhất quán với các loại tài sản đầu ra. Theo đó, các nút đầy đủ có thể xác minh xem giao dịch có hợp lệ hay không.

Theo một số phương án, để khởi tạo giao dịch kiểu UTXO với loại tài sản được che giấu bởi cơ chế cam kết Pedersen, thì bên khởi tạo giao dịch có thể chọn các đầu vào và các đầu ra thích hợp để thực hiện các bước từ 2.1 đến 2.5 dưới đây (tương ứng với Fig.2, bước 2):

Bước 2.1 Tính

$C\_1 = C\_in\_1 - C\_in\_2$,

$C\_2 = C\_in\_2 - C\_in\_3$,

…

$C\_(m-1) = C\_in\_(m-1) - C\_in\_m$,

$C\_m = C\_out\_1 - C\_out\_2$,

$C\_(m+1) = C\_out\_2 - C\_out\_3$,

…

$C\_(m+n-2) = C\_out\_(n-1) - C\_out\_n$,

$C\_(m+n-1) = C\_in\_1 - C\_out\_1$;

Bước 2.2 Tính $x = Hash (C\_1 \| C\_2 \| C\_3 \| \dots \| C\_(m+n-1))$, trong đó "||" biểu diễn sự móc nối;

Bước 2.3 Tính $C = C\_1 + x \times C\_2 + x^2 \times C\_3 + \dots + x^{(m+n-2)} \times C\_(m+n-1)$. Lưu ý rằng các số hạng đa thức này có thể tương ứng với các số hạng ở Bước 2.1;

Bước 2.4 Tính $R = (r\_in\_1 - r\_in\_2) + x \times (r\_in\_2 - r\_in\_3) + x^2 \times (r\_in\_3 - r\_in\_4) + \dots + x^{(m+n-2)} \times (r\_in\_1 - r\_out\_1)$. Lưu ý rằng các số hạng đa thức này có

thể tương ứng với các số hạng ở bước 2.1, ví dụ, (r_in_1 – r_in_2) là tương ứng với C_in_1 – C_in_2;

Bước 2.5 Công bố R đến các nút, ví dụ, trong lần phát quảng bá thông tin giao dịch.

Theo một số phương án, để xác minh rằng các loại tài sản đầu vào và các loại tài sản đầu ra là nhất quán, thì phải có $C = R \times G$. Ví dụ, trong quá trình xác minh giao dịch, thì các nút thực hiện các Bước 3.1 đến 3.3 (tương ứng với Fig.2, Bước 3.1-3.3) dưới đây để xác minh xem loại tài sản giao dịch có nhất quán hay không:

Bước 3.1 Tính $x = \text{Hash}(C\_1 \,||\, C\_2 \,||\, C\_3 \,||\, \ldots \,||\, C\_(m+n-1))$;

Bước 3.2 Tính $C = C\_1 + x \times C\_2 + x^2 \times C\_3 + \ldots + x^{(m+n-2)} \times C\_(m+n-1)$;

Bước 3.3 Xác minh xem $C = R \times G$ hay không. Nếu $C = R \times G$, thì loại tài sản là nhất quán; nếu không, thì loại tài sản là không nhất quán, và giao dịch bị từ chối. Theo một số phương án, thì C(sn) có thể được công bố đến các nút, và các thuật toán của các Bước 2.1-2.3 là đã biết đối với các nút (ví dụ, bao gồm nút trình giao dịch và các nút xác minh giao dịch). Do đó, các nút xác minh giao dịch có thể thực hiện các Bước 3.1 đến 3.3 theo đó để thực hiện việc xác minh. Do đó, giao dịch bị từ chối sẽ không được bổ sung vào blockchain. Được thể hiện dưới dạng bước 4 trên Fig.2, dựa trên việc xác định sự nhất quán, thì các nút có thể xác định xem là bổ sung giao dịch vào blockchain hay là từ chối không cho bổ sung giao dịch.

Như vậy, bên khởi tạo giao dịch có thể trình thông tin để các nút blockchain xác minh giao dịch dựa trên sự nhất quán của các loại tài sản được nhập vào và được xuất ra từ giao dịch mà không tiết lộ các loại tài sản thực tế và không có khả năng thay đổi thông tin được trình này. Việc cấp phát các số thứ tự (ví dụ, các giá trị băm) cho mỗi loại tài sản sẽ mở rộng và ngẫu nhiên hoá sự biểu diễn mỗi loại tài sản, làm cho bên khởi tạo giao dịch khó giả mạo được loại tài sản để vượt qua quá trình xác minh. Ngoài ra, vì sự tồn tại của số ngẫu nhiên r, nên cùng một loại tài sản được mã hoá tại những thời điểm khác nhau là không giống nhau. Việc áp dụng cơ chế cam kết Pedersen để mã hoá giá trị băm của loại tài sản sẽ tăng cường sự bảo vệ sự bí mật của loại tài sản đến mức độ thậm chí còn cao hơn. Do đó, thông qua các Bước 2.1 đến 2.5, thì bên khởi tạo giao dịch có thể chứng minh cho các nút còn lại rằng các loại tài sản của giao dịch là hợp lệ mà không tiết lộ các loại tài sản. Ví dụ, các hiệu số giữa các

loại tài sản đầu vào và các loại tài sản đầu ra được thu thập, và dựa trên đó, các đa thức được xây dựng, để bên khởi tạo giao dịch có thể chuyển các loại tài sản đã được làm biến đổi đến các nút còn lại để chứng minh sự nhất quán của các loại tài sản và sự hợp lệ của giao dịch. Đồng thời, xác suất mà bên khởi tạo giao dịch hoặc nút khác có thể giả mạo loại tài sản là có thể được bỏ qua, vì x được tính toán bằng cách băm để có chức năng như cơ số của các hàm số mũ khác nhau trong các đa thức. Ngoài ra, việc tiết lộ R cho phép các nút còn lại xác minh rằng các loại tài sản trong giao dịch là nhất quán mà không biết các loại tài sản, thông qua các Bước 3.1 đến 3.3. Do đó, với các hệ thống và các phương pháp được bộc lộ này, thì thông tin về dữ liệu có thể được xác minh bởi các bên thứ ba trong khi vẫn duy trì được sự bảo vệ sự bí mật đặc biệt.

Fig.3 là hình vẽ thể hiện lưu đồ của phương pháp 300 được nêu làm ví dụ để bảo vệ thông tin, theo các phương án khác nhau của sáng chế. Phương pháp 300 này có thể được thực hiện bởi một hoặc nhiều thành phần (ví dụ, nút A) của hệ thống 100 trên Fig.1. Phương pháp 300 này có thể được thực hiện bởi hệ thống hoặc thiết bị (ví dụ, máy tính) mà bao gồm bộ xử lý và phương tiện lưu trữ bất biến đọc được bằng máy tính (ví dụ, bộ nhớ) có lưu giữ các lệnh để được thực thi bởi bộ xử lý này để khiến hệ thống hoặc thiết bị này (ví dụ, bộ xử lý này) thực hiện phương pháp 300. Các thao tác của phương pháp 300 được trình bày dưới đây là nhằm mục đích minh hoạ. Tuỳ theo cách thức thực hiện mà phương pháp 300 được nêu làm ví dụ này có thể bao gồm nhiều bước hơn, ít bước hơn, hoặc các bước thay thế mà được thực hiện theo các thứ tự khác nhau hoặc song song nhau.

Bước 301 bao gồm thao tác: xác định một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu cho giao dịch, trong đó các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra. Xem, ví dụ, Bước 1 trên Fig.2. Theo một số phương án, giao dịch nêu trên là dựa ít nhất trên mô hình đầu ra giao dịch chưa tiêu dùng (Unspent Transaction Output - UTXO); và các đầu vào dữ liệu và các đầu ra dữ liệu bao gồm các kiểu của một hoặc nhiều tài sản của quá trình giao dịch giữa người gửi (nút khởi tạo) và người nhận (nút bên nhận). Loại tài sản có thể bao gồm, ví dụ, tiền, tiền kỹ thuật số, hợp đồng, khế ước, hồ sơ y tế, chi tiết khách hàng, cổ phiếu, trái phiếu, vốn cổ phần, hoặc loại tài sản bất kỳ khác mà có thể được mô tả ở dạng số.

Bước 302 bao gồm thao tác: mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này. Xem, ví dụ, Bước 1.2 đã mô tả trên đây. Theo một số phương án, bước mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bao gồm bước mã hoá mỗi trong số các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bằng hàm băm hoặc hàm một chiều khác.

Bước 303 bao gồm thao tác: cam kết mỗi trong số các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá này với hệ thống cam kết để thu được các giá trị cam kết tương ứng. Xem, ví dụ, Bước 1.3 đã mô tả trên đây. Theo một số phương án, hệ thống cam kết nêu trên bao gồm cơ chế cam kết Pedersen. Theo một số phương án, hệ thống cam kết này bao gồm ít nhất là nhân tố mù; và nhân tố mù này thay đổi theo thời gian cam kết các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá. Tức là, ngay cả dữ liệu giống nhau (ví dụ, cùng kiểu dữ liệu) được cam kết tại các thời điểm khác nhau cũng sẽ là các giá trị cam kết khác nhau do nhân tố mù thay đổi.

Bước 304 bao gồm thao tác: thu thập ít nhất thông số R dựa ít nhất trên các giá trị cam kết này. Xem, ví dụ, các Bước 2.1 đến 2.4 đã mô tả trên đây. Theo một số phương án, hệ thống cam kết nêu trên bao gồm các nhân tố mù lần lượt tương ứng với các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra (xem, ví dụ, r_in_k và r_out_k); và bước thu thập ít nhất thông số R dựa ít nhất trên các giá trị cam kết bao gồm các bước: thu thập các hiệu số giữa các cặp giá trị cam kết (xem, ví dụ, Bước 2.1 đối với các cặp giá trị cam kết khác nhau trong số các loại tài sản đầu vào và các loại tài sản đầu ra, mà đối với chúng các hiệu số có thể được thu thập); móc nối các hiệu số thu được (xem, ví dụ, Bước 2.2); mã hoá các hiệu số đã được móc nối đó bằng hàm băm để thu được giá trị mã hoá x (xem, ví dụ, Bước 2.2); và thu thập thông số R dựa ít nhất trên giá trị mã hoá x này và các hiệu số giữa các cặp nhân tố mù (xem, ví dụ, Bước 2.4).

Bước 305 bao gồm thao tác: trình giao dịch này cho một hoặc nhiều nút trong mạng blockchain (chuỗi khối) có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra để các nút này xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra. Theo một số phương án, các nút nêu trên được làm cho xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra mà không biết gì về các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này.

Theo một số phương án, bước trình giao dịch cho một hoặc nhiều nút trong mạng blockchain có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra để các nút đó xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bao gồm bước trình giao dịch cho một hoặc nhiều nút trong mạng blockchain có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra để khiến các nút đó: thu thập thông số R và điểm cơ sở G (xem, ví dụ, G ở Bước 3.1. H và G có thể là các thông số công khai khả dụng cho tất cả các nút); thu thập các hiệu số giữa các cặp giá trị cam kết của các loại tài sản đầu vào và các loại tài sản đầu ra (xem, ví dụ, bước tương tự như Bước 2.1); móc nối các hiệu số thu được (xem, ví dụ, Bước 3.1); mã hoá các hiệu số đã được móc nối đó bằng hàm băm để thu được giá trị mã hoá x (xem, ví dụ, Bước 3.1); thu thập tổng C của các đa thức dựa ít nhất trên các hiệu số thu được và giá trị mã hoá x (xem, ví dụ, Bước 3.2); đáp lại việc xác định được rằng tổng C là bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán và bổ sung giao dịch vào blockchain (xem, ví dụ, Bước 3.3); và đáp lại việc xác định được rằng tổng C không bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán và từ chối không cho bổ sung giao dịch vào blockchain (xem, ví dụ, Bước 3.3).

Fig.4 là hình vẽ thể hiện lưu đồ của phương pháp 400 được nêu làm ví dụ để bảo vệ thông tin, theo các phương án khác nhau của sáng chế. Phương pháp 400 này có thể được thực hiện bởi một hoặc nhiều thành phần (ví dụ, nút i) của hệ thống 100 trên Fig.1. Nút i này có thể bao gồm nút đầy đủ được thực hiện trên máy chủ. Phương pháp 400 này có thể được thực hiện bởi hệ thống hoặc thiết bị (ví dụ, máy tính) mà bao gồm bộ xử lý và phương tiện lưu trữ bất biến đọc được bằng máy tính (ví dụ, bộ nhớ) có lưu giữ các lệnh để được thực thi bởi bộ xử lý này để khiến hệ thống hoặc thiết bị này (ví dụ, bộ xử lý này) thực hiện phương pháp 400. Các thao tác của phương pháp 400 được trình bày dưới đây là nhằm mục đích minh hoạ. Tuỳ theo cách thức thực hiện mà phương pháp 400 được nêu làm ví dụ này có thể bao gồm nhiều bước hơn, ít bước hơn, hoặc các bước thay thế mà được thực hiện theo các thứ tự khác nhau hoặc song song nhau.

Bước 401 bao gồm thao tác: thu thập, bởi một hoặc nhiều nút (ví dụ, các nút đồng thuận) trong mạng blockchain, giao dịch được khởi tạo bởi nút khởi tạo. Giao dịch này được liên kết với một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu. Các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra. Các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này được mã hoá và được cam kết với hệ thống cam kết để thu được các giá trị cam kết tương ứng. Các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này không được tiết lộ cho một hoặc nhiều nút đó.

Bước 402 bao gồm thao tác: xác minh, bởi một hoặc nhiều nút nêu trên, sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra. Theo một số phương án, bước xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bao gồm các bước: thu thập thông số R và điểm cơ sở G (xem, ví dụ, R ở Bước 2.4 và 2.5, G ở Bước 3.1); thu thập các hiệu số giữa các cặp giá trị cam kết của các loại tài sản đầu vào và các loại tài sản đầu ra (xem, ví dụ, bước tương tự như Bước 2.1); móc nối các hiệu số thu được (xem, ví dụ, Bước 3.1); mã hoá các hiệu số đã được móc nối đó bằng hàm băm để thu được giá trị mã hoá x (xem, ví dụ, Bước 3.1); thu thập tổng C của các đa thức dựa ít nhất trên các hiệu số thu được và giá trị mã hoá x (xem, ví dụ, Bước 3.2); và xác định xem tổng C có bằng tích của thông số R và điểm cơ sở G hay không (xem, ví dụ, Bước 3.3).

Bước 403 bao gồm thao tác: đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán, thì bổ sung, bởi một hoặc nhiều nút này, giao dịch nêu trên vào mạng blockchain này.

Bước 404 bao gồm thao tác: đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán, thì từ chối, bởi một hoặc nhiều nút này, không cho bổ sung giao dịch này vào mạng blockchain này.

Theo một số phương án, phương pháp này còn bao gồm các bước: đáp lại việc xác định được rằng tổng C là bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán; và đáp lại việc xác định được rằng tổng C không bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán.

Như vậy, bên khởi tạo giao dịch có thể trình thông tin để các nút blockchain xác minh giao dịch dựa trên sự nhất quán của các loại tài sản được nhập vào và được xuất ra từ giao dịch mà không tiết lộ các loại tài sản thực tế và không có khả năng thay đổi thông tin được trình này. Việc cấp phát các số thứ tự (ví dụ, các giá trị băm) cho mỗi loại tài sản sẽ mở rộng và ngẫu nhiên hoá sự biểu diễn mỗi loại tài sản, làm cho bên khởi tạo giao dịch khó giả mạo được loại tài sản để vượt qua quá trình xác minh. Ngoài ra, vì sự tồn tại của số ngẫu nhiên r, nên cùng một loại tài sản được mã hoá tại những thời điểm khác nhau là không giống nhau. Việc áp dụng cơ chế cam kết Pedersen để mã hoá giá trị băm của loại tài sản sẽ tăng cường sự bảo vệ sự bí mật của loại tài sản đến mức độ thậm chí còn cao hơn. Do đó, thông qua các Bước 2.1 đến 2.5, thì bên khởi tạo giao dịch có thể chứng minh cho các nút còn lại rằng các loại tài sản của giao dịch là hợp lệ mà không tiết lộ các loại tài sản. Ví dụ, các hiệu số giữa các loại tài sản đầu vào và các loại tài sản đầu ra được thu thập, và dựa trên đó, các đa thức được xây dựng, để bên khởi tạo giao dịch có thể chuyển các loại tài sản đã được làm biến đổi đến các nút còn lại để chứng minh sự nhất quán của các loại tài sản và sự hợp lệ của giao dịch. Đồng thời, xác suất mà bên khởi tạo giao dịch hoặc nút khác có thể giả mạo loại tài sản là có thể được bỏ qua, vì x được tính toán bằng cách băm để có chức năng như cơ số của các hàm số mũ khác nhau trong các đa thức. Ngoài ra, việc tiết lộ R cho phép các nút còn lại xác minh rằng các loại tài sản trong giao dịch là nhất quán mà không biết các loại tài sản, thông qua các Bước 3.1 đến 3.3. Do đó, với các hệ thống và các phương pháp được bộc lộ này, thì thông tin về dữ liệu có thể được xác minh bởi các bên thứ ba trong khi vẫn duy trì được sự bảo vệ sự bí mật đặc biệt.

Các kỹ thuật được mô tả ở đây là được thực hiện bởi một hoặc nhiều thiết bị điện toán chuyên dụng. Các thiết bị điện toán chuyên dụng này có thể là các hệ thống máy tính để bàn, các hệ thống máy tính chủ, các hệ thống máy tính mang vác được, các thiết bị cầm tay, các thiết bị nối mạng hoặc thiết bị hoặc tổ hợp thiết bị bất kỳ khác mà có mạch logic được nối cứng và/hoặc mạch logic lập trình để thực hiện các kỹ thuật này. (Các) thiết bị điện toán nói chung là được điều khiển và được điều phối bởi phần mềm hệ điều hành. Các hệ điều hành thông thường sẽ điều khiển và lập lịch các tiến trình máy tính để thực hiện, thực hiện việc quản lý bộ nhớ, cung cấp hệ thống tệp tin, các dịch vụ nối mạng, các dịch vụ I/O, và cung cấp chức năng giao diện người

dùng, chẳng hạn giao diện đồ hoạ người dùng (Graphical User Interface - "GUI"), trong số các yếu tố khác.

Fig.5 là hình vẽ thể hiện sơ đồ khối của hệ thống máy tính 500 mà phương án bất kỳ trong số các phương án được mô tả ở đây có thể được thực hiện trên đó. Hệ thống 500 này có thể được thực hiện ở nút bất kỳ trong số các nút được mô tả ở đây, và được tạo cấu hình để thực hiện các bước tương ứng của các phương pháp bảo vệ thông tin. Hệ thống máy tính 500 này bao gồm buýt 502 hoặc cơ chế giao tiếp khác để truyền thông tin, một hoặc nhiều bộ xử lý phần cứng 504 được ghép nối với buýt 502 để xử lý thông tin. (Các) bộ xử lý phần cứng 504 có thể là, ví dụ, một hoặc nhiều bộ vi xử lý thông dụng.

Hệ thống máy tính 500 cũng bao gồm bộ nhớ chính 506, chẳng hạn bộ nhớ truy cập ngẫu nhiên (Random Access Memory - RAM), bộ đệm và/hoặc các thiết bị lưu trữ động khác, được ghép nối với buýt 502 để lưu giữ thông tin và các lệnh để được thực thi bởi (các) bộ xử lý 504. Bộ nhớ chính 506 cũng có thể được dùng để lưu giữ các biến số tạm thời hoặc thông tin trung gian khác trong quá trình thực thi các lệnh cần được thực thi bởi (các) bộ xử lý 504. Các lệnh đó, khi được lưu giữ trong các phương tiện lưu trữ mà (các) bộ xử lý 504 có thể truy cập được, sẽ biến hệ thống máy tính 500 thành cỗ máy chuyên dụng mà được tuỳ biến để thực hiện các thao tác được quy định trong các lệnh này. Hệ thống máy tính 500 còn bao gồm bộ nhớ chỉ đọc (Read Only Memory - ROM) 508 hoặc thiết bị lưu trữ tĩnh khác được ghép nối với buýt 502 để lưu giữ thông tin tĩnh và các lệnh cho (các) bộ xử lý 504. Thiết bị lưu trữ 510, chẳng hạn đĩa từ, đĩa quang, hoặc ổ đĩa USB (ổ đĩa Flash), v.v., là được bố trí và được ghép nối với buýt 502 để lưu giữ thông tin và các lệnh.

Hệ thống máy tính 500 có thể thực hiện các kỹ thuật được mô tả ở đây nhờ sử dụng logic được nối cứng được tuỳ biến, một hoặc nhiều ASIC (Application Specific Integrated Circuit - mạch tích hợp chuyên dụng) hoặc FPGA (Field Programmable Gate Array - mảng cổng lập trình được dạng trường), phần sụn và/hoặc logic chương trình mà kết hợp với hệ thống máy tính này để khiến hoặc lập trình cho hệ thống máy tính 500 thành cỗ máy chuyên dụng. Theo một phương án, thì các hoạt động, các phương pháp, và các tiến trình được mô tả ở đây là được thực hiện bởi hệ thống máy tính 500 đáp lại việc (các) bộ xử lý 504 thực hiện một hoặc nhiều chuỗi gồm một hoặc

nhiều lệnh được chứa trong bộ nhớ chính 506. Các lệnh đó có thể được đọc vào bộ nhớ chính 506 từ phương tiện lưu trữ khác, chẳng hạn thiết bị lưu trữ 510. Việc thực hiện các chuỗi gồm các lệnh được chứa trong bộ nhớ chính 506 sẽ khiến (các) bộ xử lý 504 thực hiện các bước xử lý được mô tả ở đây. Theo các phương án thay thế, thì hệ mạch được nối cứng có thể được sử dụng thay cho hoặc kết hợp với các lệnh phần mềm.

Bộ nhớ chính 506, ROM 508, và/hoặc bộ lưu trữ 510 có thể bao gồm các phương tiện lưu trữ bất biến. Thuật ngữ "các phương tiện bất biến", và các thuật ngữ tương tự, như được sử dụng ở đây, là được dùng để chỉ các phương tiện mà lưu giữ dữ liệu và/hoặc các lệnh để khiến một cỗ máy hoạt động theo cách riêng, các phương tiện này không bao gồm các tín hiệu nhất thời. Các phương tiện bất biến đó có thể bao gồm các phương tiện bất biến và/hoặc các phương tiện khả biến. Các phương tiện bất biến bao gồm, ví dụ, đĩa quang hoặc đĩa từ, chẳng hạn thiết bị lưu trữ 510. Các phương tiện khả biến bao gồm bộ nhớ động, chẳng hạn bộ nhớ chính 506. Dạng phổ biến của các phương tiện bất biến bao gồm, ví dụ, đĩa mềm, đĩa dẻo, đĩa cứng, ổ đĩa thể rắn, băng từ, hoặc phương tiện lưu trữ dữ liệu từ tính bất kỳ khác, đĩa CD-ROM, phương tiện lưu trữ dữ liệu quang học bất kỳ khác, phương tiện vật lý bất kỳ với các mẫu lỗ, RAM, PROM (Programmable ROM - ROM lập trình được), và EPROM (Erasable PROM - PROM xoá được), FLASH-EPROM, NVRAM (NonVolatile Random Access Memory - bộ nhớ truy cập ngẫu nhiên bất biến), chip nhớ hoặc băng nhớ bất kỳ khác, và các phiên bản được nối mạng của chúng.

Hệ thống máy tính 500 cũng bao gồm giao diện mạng 518 được ghép nối với buýt 502. Giao diện mạng 518 cho phép truyền thông dữ liệu hai chiều để ghép nối đến một hoặc nhiều liên kết mạng mà được kết nối với một hoặc nhiều mạng cục bộ. Ví dụ, giao diện mạng 518 có thể là cạc ISDN (Integrated Services Digital Network - mạng số tích hợp các dịch vụ), môđem cáp, môđem vệ tinh, hoặc môđem để cung cấp kết nối truyền thông dữ liệu đến loại đường dây điện thoại tương ứng. Theo ví dụ khác, giao diện mạng 518 có thể là cạc LAN (Local Area Network - mạng cục bộ) để cung cấp kết nối truyền thông dữ liệu đến LAN tương thích (hoặc thành phần WAN (Wide Area Network - mạng diện rộng) để giao tiếp với WAN). Các liên kết không dây cũng có thể được thực hiện. Theo cách thức thực hiện bất kỳ đó, thì giao diện

mạng 518 đều gửi và nhận các tín hiệu điện, các tín hiệu điện từ hoặc các tín hiệu quang học mà mang các luồng dữ liệu số biểu diễn các loại thông tin khác nhau.

Hệ thống máy tính 500 có thể gửi các thông điệp và nhận dữ liệu, bao gồm mã chương trình, thông qua (các) mạng, liên kết mạng và giao diện mạng 518. Ví dụ, trên mạng Internet, thì máy chủ có thể truyền mã được yêu cầu cho chương trình ứng dụng thông qua mạng Internet, ISP (Internet Service Provider - nhà cung cấp dịch vụ Internet), mạng cục bộ và giao diện mạng 518.

Mã nhận được có thể được thực thi bởi (các) bộ xử lý 504 khi nó được nhận, và/hoặc được lưu giữ vào thiết bị lưu trữ 510, hoặc thiết bị lưu trữ bất biến khác để thực hiện về sau.

Mỗi trong số các tiến trình, các phương pháp, và các thuật toán được mô tả ở các phần nêu trên là có thể được thực hiện trong, và được tự động hoá hoàn toàn hoặc một phần bởi, các môđun mã 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 tiến trình và các thuật toán này có thể được thực hiện một phần hoặc hoàn toàn trong hệ mạch chuyên dụng.

Các dấu hiệu và các tiến trình khác nhau đã mô tả trên đây là có thể được sử dụng độc lập với nhau, hoặc có thể được kết hợp theo những cách khác nhau. Tất cả những sự kết hợp và những sự kết hợp con khả thi đều nằm trong phạm vi của sáng chế. Ngoài ra, các bước của phương pháp hoặc của tiến trình nhất định là có thể được lược bỏ theo một số cách thức thực hiện. Các phương pháp và các tiến trình được mô tả ở đây cũng không bị giới hạn ở trình tự cụ thể bất kỳ nào, và các bước hoặc các trạng thái liên quan đến chúng có thể được thực hiện theo các trình tự khác mà thích hợp. Ví dụ, các bước hoặc các trạng thái đã được mô tả có thể được thực hiện theo thứ tự khác so với thứ tự được bộc lộ cụ thể, hoặc nhiều bước hoặc nhiều trạng thái có thể được kết hợp thành một bước hoặc một trạng thái. Các bước hoặc các trạng thái được nêu làm ví dụ đó có thể được thực hiện nối tiếp, song song, hoặc theo cách nào đó khác. Các bước hoặc các trạng thái có thể được thêm vào hoặc được bớt khỏi các phương án ví dụ được bộc lộ. Các hệ thống và các thành phần ví dụ được mô tả ở đây có thể được tạo cấu hình theo cách khác so với được mô tả. Ví dụ, các phần tử có thể được thêm vào, được bớt khỏi, hoặc được sắp xếp lại so với các phương án ví dụ được bộc lộ.

Các thao tác khác nhau của các phương pháp ví dụ được mô tả ở đây có thể được thực hiện, ít nhất một phần, bằng thuật toán. Thuật toán này có thể được bao gồm trong các mã chương trình hoặc các lệnh được lưu giữ trong bộ nhớ (ví dụ, phương tiện lưu trữ bất biến đọc được bằng máy tính đã mô tả trên đây). Thuật toán đó có thể bao gồm thuật toán học máy. Theo một số phương án, thì thuật toán học máy có thể không lập trình một cách tường minh cho các máy tính để thực hiện chức năng nào đó, nhưng có thể học từ dữ liệu huấn luyện để tạo ra mô hình dự đoán để thực hiện chức năng đó.

Các thao tác khác nhau của các phương pháp ví dụ được mô tả ở đây có thể được thực hiện, ít nhất một phần, bởi một hoặc nhiều bộ xử lý mà được tạo cấu hình tạm thời (ví dụ, bằng phần mềm) hoặc được tạo cấu hình vĩnh viễn để thực hiện các thao tác liên quan. Cho dù được tạo cấu hình tạm thời hay vĩnh viễn, thì các bộ xử lý đó cũng có thể cấu thành các máy được thực hiện bằng bộ xử lý mà hoạt động để thực hiện một hoặc nhiều thao tác hoặc chức năng được mô tả ở đây.

Tương tự, các phương pháp được mô tả ở đây có thể được thực hiện ít nhất một phần bằng bộ xử lý, với bộ xử lý hoặc các bộ xử lý cụ thể được lấy làm ví dụ về phần cứng. Ví dụ, ít nhất một số trong số các thao tác của phương pháp là có thể được thực hiện bởi một hoặc nhiều bộ xử lý hoặc máy được thực hiện bằng bộ xử lý. Ngoài ra, một hoặc nhiều bộ xử lý đó cũng có thể hoạt động để hỗ trợ việc thực hiện các thao tác liên quan trong môi trường "điện toán đám mây" hoặc dưới dạng "phần mềm như một dịch vụ" (Software as a Service - SaaS). Ví dụ, ít nhất một số trong số các thao tác đó là có thể được thực hiện bởi một nhóm máy tính (dưới dạng các ví dụ về những cỗ máy bao gồm các bộ xử lý), với việc các thao tác này là có thể tiếp cận được qua mạng (ví dụ, mạng Internet) và thông qua một hoặc nhiều giao diện thích hợp (ví dụ, giao diện lập trình ứng dụng (Application Program Interface - API)).

Việc thực hiện các thao tác nhất định trong số các thao tác này là có thể được phân tán giữa các bộ xử lý, chứ không chỉ nằm trong một cỗ máy đơn lẻ, mà được triển khai giữa một số lượng máy. Theo một số phương án ví dụ, thì các bộ xử lý hoặc các máy được thực hiện bằng bộ xử lý nêu trên có thể được đặt ở một vị trí địa lý đơn lẻ (ví dụ, trong môi trường gia đình, môi trường văn phòng, hoặc trang trại máy chủ).

Theo các phương án ví dụ khác, thì các bộ xử lý hoặc các máy được thực hiện bằng bộ xử lý đó có thể được phân tán trên một số lượng vị trí địa lý.

Trong suốt bản mô tả này, thì nhiều thực thể có thể thực hiện các thành phần, các thao tác, hoặc các cấu trúc được mô tả như một thực thể đơn. Tuy các thao tác riêng lẻ của một hoặc nhiều phương pháp đã được thể hiện và được mô tả dưới dạng các thao tác riêng biệt, nhưng một hoặc nhiều trong số các thao tác riêng lẻ này có thể được thực hiện đồng thời, và không có gì yêu cầu rằng các thao tác này phải được thực hiện theo thứ tự được thể hiện. Các cấu trúc và chức năng mà được trình bày dưới dạng các thành phần riêng biệt trong các cấu hình ví dụ là có thể được thực hiện dưới dạng cấu trúc hoặc thành phần kết hợp. Tương tự, các cấu trúc và chức năng mà được trình bày dưới dạng một thành phần đơn lẻ có thể được thực hiện dưới dạng các thành phần riêng biệt. Các phương án biến thể, cải biến, bổ sung, cải tiến này và các phương án biến thể, cải biến, bổ sung, và cải tiến khác đều nằm trong phạm vi của sáng chế.

Tuy sáng chế đã được mô tả khái quát dựa vào các phương án ví dụ cụ thể, nhưng các phương án cải biến và thay đổi khác nhau có thể được tạo ra đối với các phương án này mà không nằm ngoài phạm vi rộng hơn của các phương án của sáng chế. Các phương án đó của sáng chế có thể được gọi một cách riêng lẻ hoặc gộp chung ở đây bằng thuật ngữ "sáng chế", chỉ để cho thuận tiện chứ không nhằm tự giới hạn phạm vi của sáng chế ở bất kỳ phần mô tả hay khái niệm đơn lẻ nào nếu có nhiều hơn một phần mô tả hoặc khái niệm được bộc lộ, mà trên thực tế là như vậy.

YÊU CẦU BẢO HỘ:

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

thu thập, bởi một hoặc nhiều nút trong mạng blockchain, giao dịch được khởi tạo bởi nút khởi tạo, trong đó:

giao dịch này được liên kết với một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu,

các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra,

các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này được mã hoá và được cam kết với hệ thống cam kết để thu được các giá trị cam kết tương ứng,

hệ thống cam kết này bao gồm ít nhất là nhân tố mù,

nhân tố mù này thay đổi theo thời gian cam kết các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá, và

các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này không được tiết lộ cho một hoặc nhiều nút đó;

xác minh, bởi một hoặc nhiều nút nêu trên, sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra; và

đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán, thì bổ sung, bởi một hoặc nhiều nút này, giao dịch nêu trên vào mạng blockchain này; hoặc đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán, thì từ chối, bởi một hoặc nhiều nút này, không cho bổ sung giao dịch này vào mạng blockchain này.

2. Phương pháp theo điểm 1, trong đó bước xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bao gồm các bước:

thu thập thông số R và điểm cơ sở G;

thu thập các hiệu số giữa các cặp giá trị cam kết;

móc nối các hiệu số thu được;

mã hoá các hiệu số đã được móc nối đó bằng hàm băm để thu được giá trị mã hoá x;

thu thập tổng C của các đa thức dựa ít nhất trên các hiệu số thu được và giá trị mã hoá x; và

xác định xem tổng C có bằng tích của thông số R và điểm cơ sở G hay không.

3. Phương pháp theo điểm 2, phương pháp này còn bao gồm các bước:

đáp lại việc xác định được rằng tổng C là bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán; và

đáp lại việc xác định được rằng tổng C không bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán.

4. Phương pháp theo điểm 1, trong đó hệ thống cam kết bao gồm cơ chế cam kết Pedersen.

5. Phương pháp theo điểm 1, trong đó: các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra được mã hóa bằng hàm băm.

6. Phương pháp theo điểm 1, trong đó:

giao dịch là dựa ít nhất trên mô hình các đầu ra giao dịch chưa tiêu dùng (Unspent Transaction Output - UTXO); và

các đầu vào dữ liệu và các đầu ra dữ liệu bao gồm các kiểu của một hoặc nhiều tài sản của quá trình giao dịch.

7. Phương tiện lưu trữ bất biến đọc được bằng máy tính có lưu giữ các lệnh để được thực thi bằng bộ xử lý để khiến bộ xử lý đó thực hiện các thao tác bao gồm các bước:

thu thập, bởi một hoặc nhiều nút trong mạng blockchain, giao dịch được khởi tạo bởi nút khởi tạo, trong đó:

giao dịch này được liên kết với một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu,

các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra,

các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này được mã hoá và được cam kết với hệ thống cam kết để thu được các giá trị cam kết tương ứng,

hệ thống cam kết này bao gồm ít nhất là nhân tố mù,

nhân tố mù này thay đổi theo thời gian cam kết các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá, và

các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này không được tiết lộ cho một hoặc nhiều nút đó;

xác minh, bởi một hoặc nhiều nút nêu trên, sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra; và

đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán, thì bổ sung, bởi một hoặc nhiều nút này, giao dịch nêu trên vào mạng blockchain này; hoặc đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán, thì từ chối, bởi một hoặc nhiều nút này, không cho bổ sung giao dịch này vào mạng blockchain này.

8. Phương tiện lưu trữ theo điểm 7, trong đó bước xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bao gồm các bước:

thu thập thông số R và điểm cơ sở G;

thu thập các hiệu số giữa các cặp giá trị cam kết;

móc nối các hiệu số thu được;

mã hoá các hiệu số đã được móc nối đó bằng hàm băm để thu được giá trị mã hoá x;

thu thập tổng C của các đa thức dựa ít nhất trên các hiệu số thu được và giá trị mã hoá x; và

xác định xem tổng C có bằng tích của thông số R và điểm cơ sở G hay không.

9. Phương tiện lưu trữ theo điểm 8, trong đó các thao tác này còn còn bao gồm các bước:

đáp lại việc xác định được rằng tổng C là bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán; và

đáp lại việc xác định được rằng tổng C không bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán.

10. Phương tiện lưu trữ theo điểm 7, trong đó hệ thống cam kết bao gồm cơ chế cam kết Pedersen.

11. Phương tiện lưu trữ theo điểm 7, trong đó: các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra được mã hóa bằng hàm băm.

12. Phương tiện lưu trữ theo điểm 7, trong đó:

giao dịch là dựa ít nhất trên mô hình các đầu ra giao dịch chưa tiêu dùng (Unspent Transaction Output - UTXO); và

các đầu vào dữ liệu và các đầu ra dữ liệu bao gồm các kiểu của một hoặc nhiều tài sản của quá trình giao dịch.

13. Hệ thống để bảo vệ thông tin, trong đó hệ thống này bao gồm bộ xử lý và phương tiện lưu trữ bất biến đọc được bằng máy tính được ghép nối với bộ xử lý này, phương tiện lưu trữ này lưu giữ các lệnh để được thực thi bằng bộ xử lý này để khiến hệ thống này thực hiện các thao tác bao gồm các bước:

thu thập, bởi một hoặc nhiều nút trong mạng blockchain, giao dịch được khởi tạo bởi nút khởi tạo, trong đó:

giao dịch này được liên kết với một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu,

các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra,

các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này được mã hoá và được cam kết với hệ thống cam kết để thu được các giá trị cam kết tương ứng,

hệ thống cam kết này bao gồm ít nhất là nhân tố mù,

nhân tố mù này thay đổi theo thời gian cam kết các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá, và

các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này không được tiết lộ cho một hoặc nhiều nút đó;

xác minh, bởi một hoặc nhiều nút nêu trên, sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra; và

đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán, thì bổ sung, bởi một hoặc nhiều nút này, giao dịch nêu trên vào mạng blockchain này; hoặc đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán, thì từ chối, bởi một hoặc nhiều nút này, không cho bổ sung giao dịch này vào mạng blockchain này.

14. Hệ thống theo điểm 13, trong đó bước xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra bao gồm các bước:

thu thập thông số R và điểm cơ sở G;

thu thập các hiệu số giữa các cặp giá trị cam kết;

móc nối các hiệu số thu được;

mã hoá các hiệu số đã được móc nối đó bằng hàm băm để thu được giá trị mã hoá x;

thu thập tổng C của các đa thức dựa ít nhất trên các hiệu số thu được và giá trị mã hoá x; và

xác định xem tổng C có bằng tích của thông số R và điểm cơ sở G hay không.

15. Hệ thống theo điểm 14, trong đó các thao tác này còn còn bao gồm các bước:

đáp lại việc xác định được rằng tổng C là bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán; và

đáp lại việc xác định được rằng tổng C không bằng tích của thông số R và điểm cơ sở G, thì xác định rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán.

16. Hệ thống theo điểm 13, trong đó hệ thống cam kết bao gồm cơ chế cam kết Pedersen.

17. Hệ thống theo điểm 13, trong đó: các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra được mã hóa bằng hàm băm.

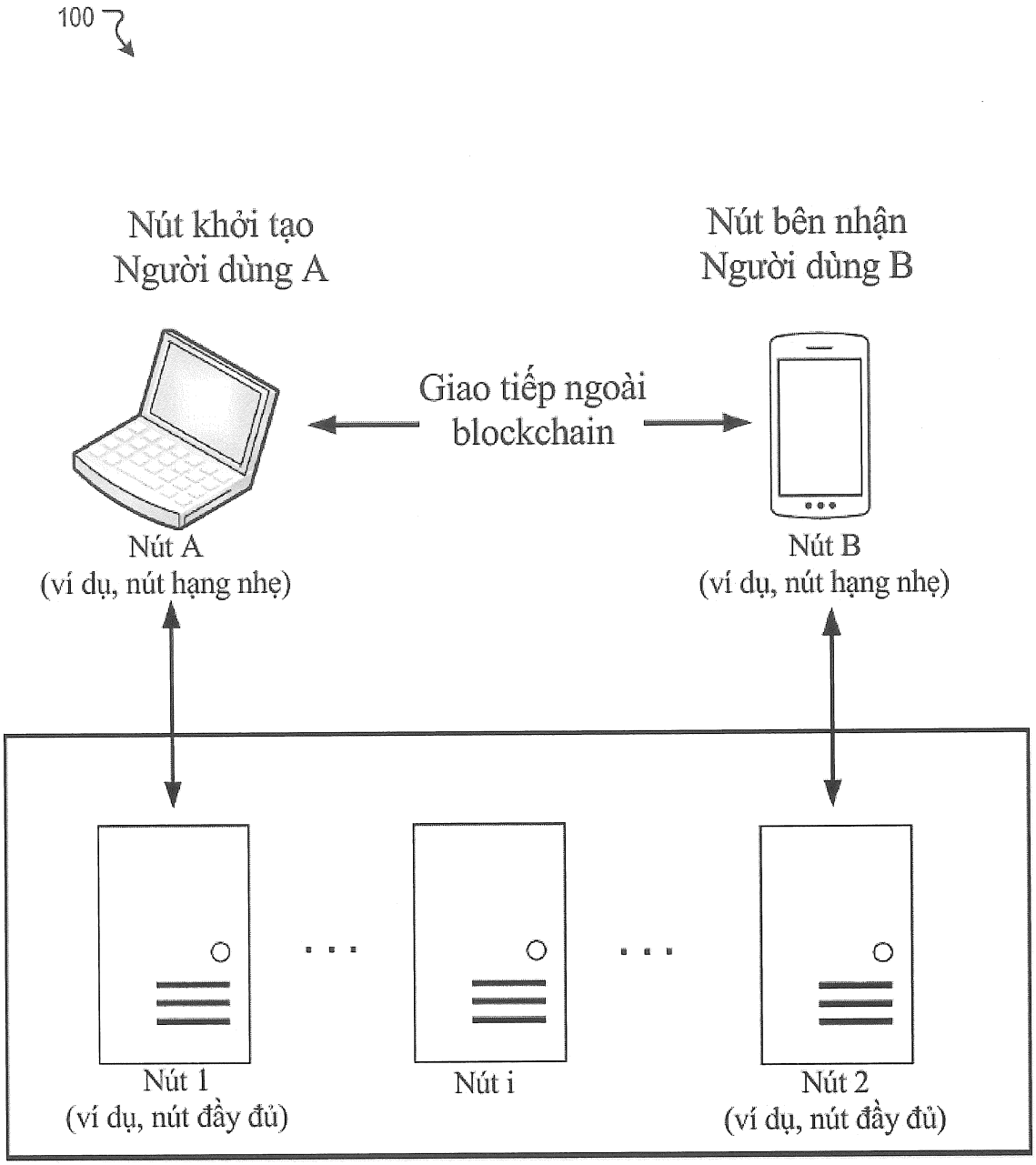
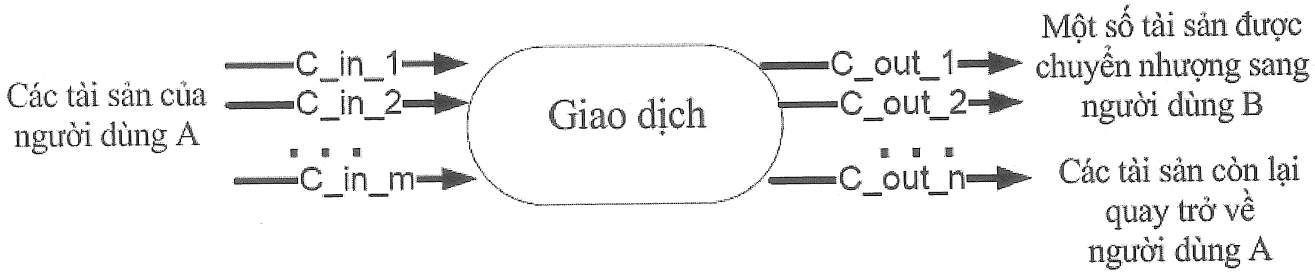

100
Nút khởi tạo
Người dùng A
Nút bên nhận
Người dùng B
Giao tiếp ngoài
blockchain
Nút A
(ví dụ, nút hạng nhẹ)
Nút B
(ví dụ, nút hạng nhẹ)
Nút 1
(ví dụ, nút đầy đủ)
Nút i
Nút 2
(ví dụ, nút đầy đủ)

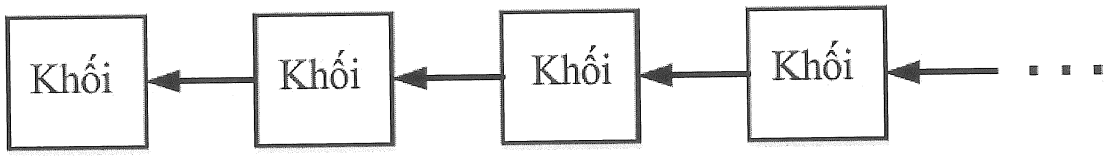
Fig.1

Nút khởi tạo khởi tạo giao dịch cần được bổ sung vào blockchain

1. Khởi tạo giao dịch



2. Tính x, C và R, và công bố R cho các nút



Nút đồng thuận xác minh xem giao dịch có hợp lệ không

3.1. Tính x

3.2. Tính C

3.3. Xác minh C=rG để thẩm định giao dịch

4. Bổ sung giao dịch vào blockchain hoặc từ chối, dựa trên tính hợp lệ

Fig.2

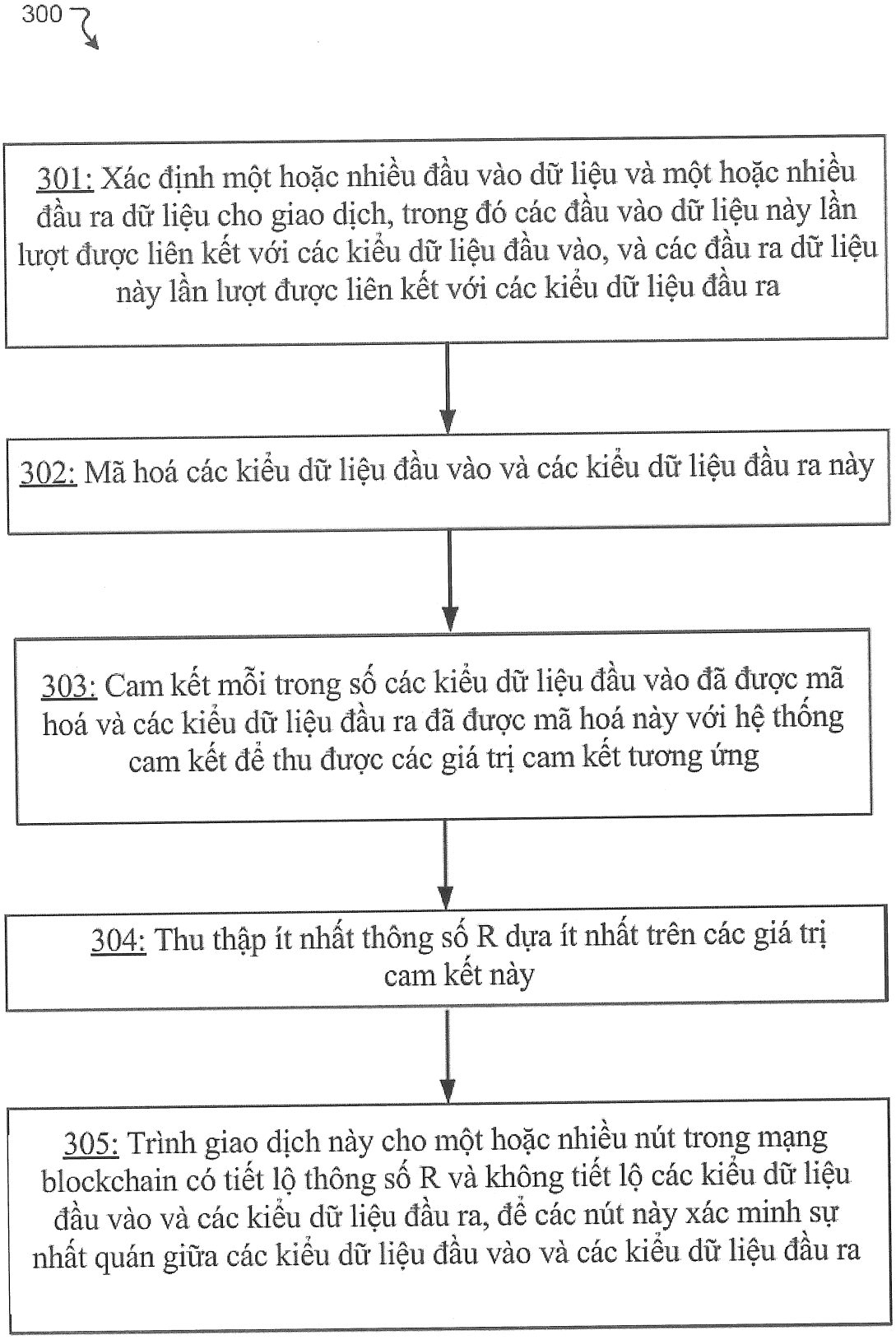

300
301: Xác định một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu cho giao dịch, trong đó các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra
302: Mã hoá các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này
303: Cam kết mỗi trong số các kiểu dữ liệu đầu vào đã được mã hoá và các kiểu dữ liệu đầu ra đã được mã hoá này với hệ thống cam kết để thu được các giá trị cam kết tương ứng
304: Thu thập ít nhất thông số R dựa ít nhất trên các giá trị cam kết này
305: Trình giao dịch này cho một hoặc nhiều nút trong mạng blockchain có tiết lộ thông số R và không tiết lộ các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra, để các nút này xác minh sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra

Fig.3

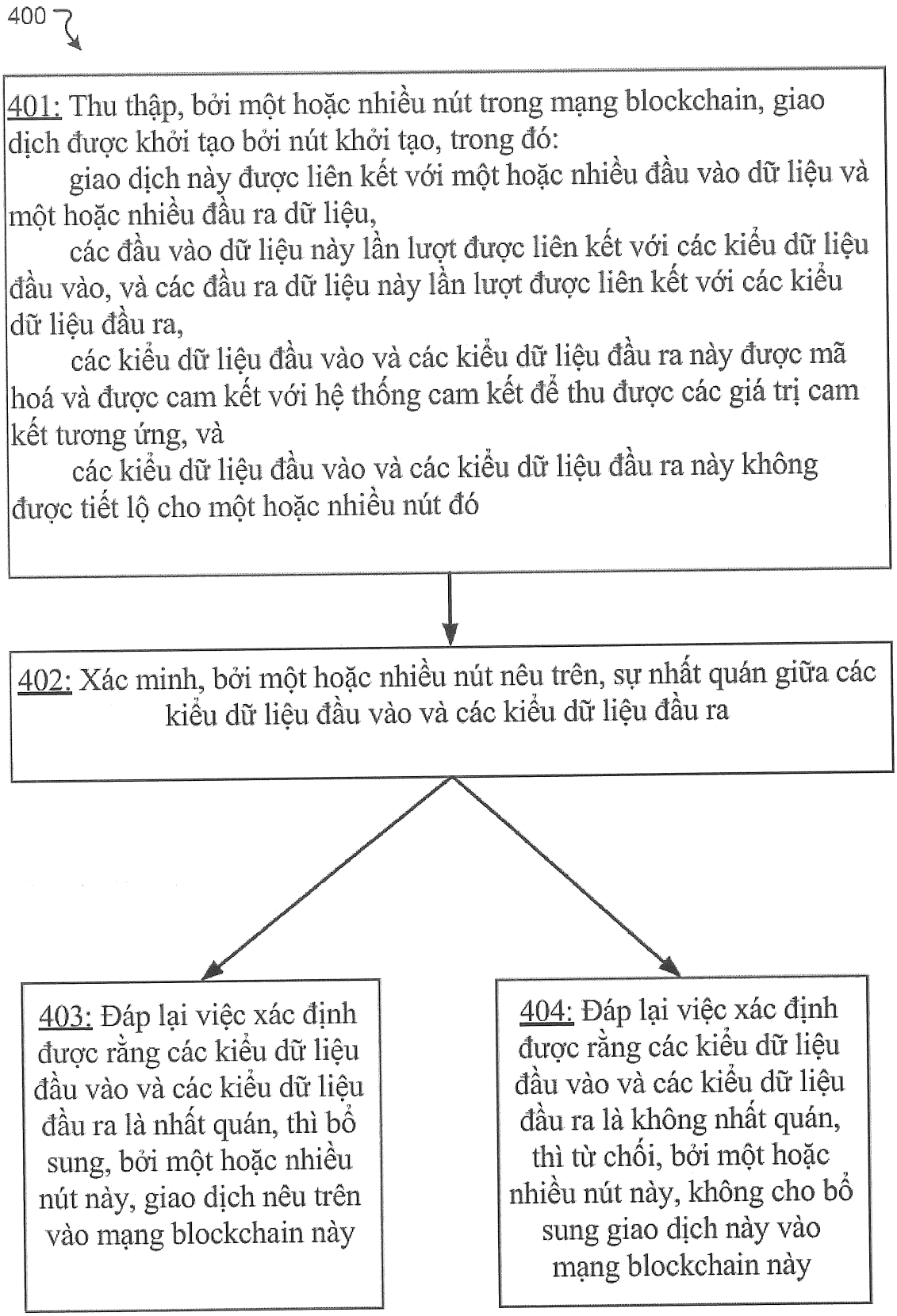

400
401: Thu thập, bởi một hoặc nhiều nút trong mạng blockchain, giao dịch được khởi tạo bởi nút khởi tạo, trong đó:
giao dịch này được liên kết với một hoặc nhiều đầu vào dữ liệu và một hoặc nhiều đầu ra dữ liệu,
các đầu vào dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu vào, và các đầu ra dữ liệu này lần lượt được liên kết với các kiểu dữ liệu đầu ra,
các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này được mã hoá và được cam kết với hệ thống cam kết để thu được các giá trị cam kết tương ứng, và
các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra này không được tiết lộ cho một hoặc nhiều nút đó
402: Xác minh, bởi một hoặc nhiều nút nêu trên, sự nhất quán giữa các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra
403: Đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là nhất quán, thì bổ sung, bởi một hoặc nhiều nút này, giao dịch nêu trên vào mạng blockchain này
404: Đáp lại việc xác định được rằng các kiểu dữ liệu đầu vào và các kiểu dữ liệu đầu ra là không nhất quán, thì từ chối, bởi một hoặc nhiều nút này, không cho bổ sung giao dịch này vào mạng blockchain này

Fig.4

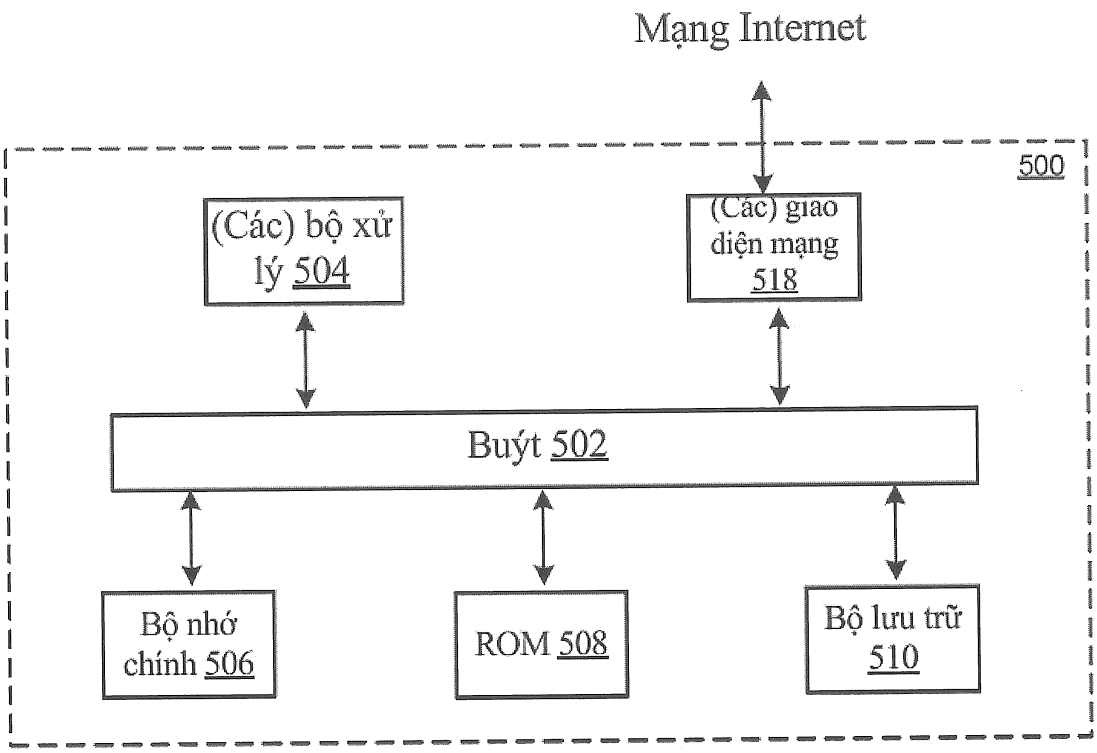

Mạng Internet
500
(Các) bộ xử lý 504
(Các) giao diện mạng 518
Buýt 502
Bộ nhớ chính 506
ROM 508
Bộ lưu trữ 510

Fig.5