(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) **1-0045149**

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

(13) **B**

(21) 1-2019-01944
(22) 27/11/2018
(86) PCT/CN2018/117571 27/11/2018
(87) WO2019/072279 18/04/2019
(45) 25/04/2025 445
(43) 25/07/2019 376A
(71) ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) CUI, Jiahui (CN); MA, Baoli (CN); LIU, Zheng (CN); ZHANG, Wenbin (CN); MA, Huanyu (CN).
(74) Công ty Luật TNHH T&G (TGVN)

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

(21) 1-2019-01944

(57) Phương pháp được thực hiện bởi máy tính bao gồm các bước: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; mã hoá tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch; và truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch.

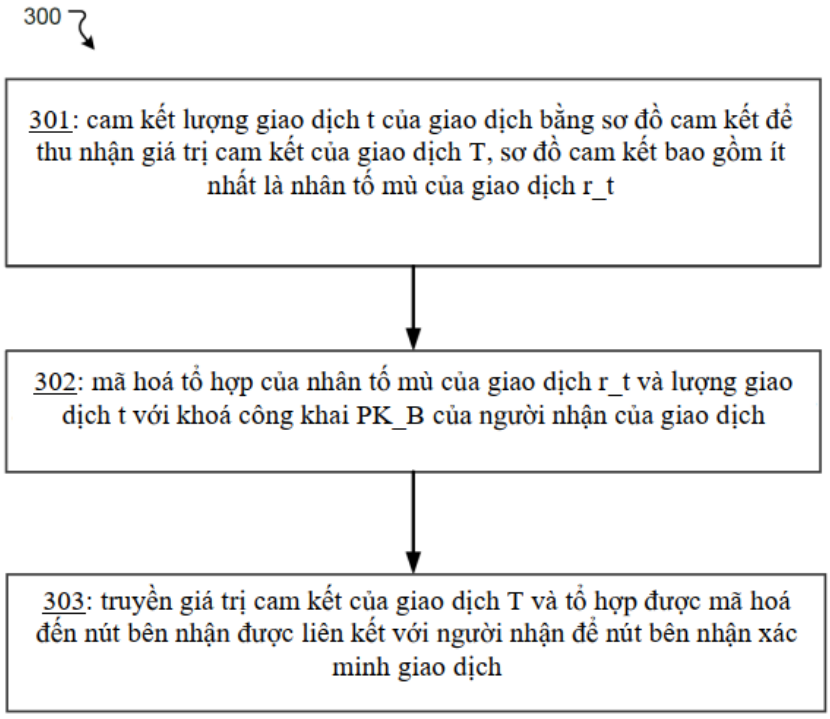


FIG. 3A

**Lĩnh vực kỹ thuật**

Sáng chế đề xuất phương pháp và thiết bị để bảo vệ thông tin.

**Tình trạng kỹ thuật của sáng chế**

Việc bảo vệ là rất quan trọng trong truyền thông và truyền dữ liệu giữa các người dùng khác nhau. Nếu không được bảo vệ, thì 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 phương án bao gồm hệ thống, phương pháp, và phương tiện có thể đọc được bởi máy tính không chuyển tiếp để bảo vệ thông tin.

Theo một khía cạnh, phương pháp thực hiện bởi máy tính để bảo vệ thông tin bao gồm các bước: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; mã hoá tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch; và truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch.

Trong một số phương án, khoá công khai PK_B là khoá mã hóa bất đối xứng.

Trong một số phương án, sơ đồ cam kết bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù của giao dịch r_t và với lượng giao dịch t là giá trị được cam kết.

Trong một số phương án, tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bao gồm sự móc nối của nhân tố mù của giao dịch r_t và lượng giao dịch t.

Trong một số phương án, bước truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch bao gồm bước truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá

đến nút bên nhận được liên kết với người nhận, làm cho nút bên nhận: giải mã tổ hợp được mã hoá bằng khoá bí mật SK_B của người nhận để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t; và xác minh giao dịch dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t.

Trong một số phương án, bước làm cho nút bên nhận xác minh giao dịch dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t bao gồm bước làm cho nút bên nhận: để đáp lại việc xác định rằng giá trị cam kết T không khớp với sơ đồ cam kết của lượng giao dịch t dựa trên nhân tố mù của giao dịch r_t, thì từ chối giao dịch; và để đáp lại việc xác định rằng giá trị cam kết của giao dịch T khớp bằng sơ đồ cam kết của lượng giao dịch t dựa trên nhân tố mù của giao dịch r_t, thì phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_B của người nhận để tạo ra chữ ký của người nhận SIGB.

Trong một số phương án, trước bước truyền tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận, thì phương pháp còn bao gồm bước: cam kết tiền trả lại y của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết tiền trả lại Y, sơ đồ cam kết bao gồm ít nhất là nhân tố mù của tiền trả lại r_y , trong đó tiền trả lại y là một hoặc nhiều tài sản của người gửi của giao dịch mà được trích cho giao dịch nhỏ hơn lượng giao dịch t ; và mã hoá tổ hợp khác của nhân tố mù của tiền trả lại r_y và tiền trả lại y bằng khoá công khai PK_A của người gửi.

Trong một số phương án, phương pháp còn bao gồm bước: để đáp lại việc nhận được chữ ký của người nhận SIGN, thì phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_A của người gửi để tạo ra chữ ký của người gửi SIGA; và trình giao dịch bao gồm tổ hợp được mã hoá, một tổ hợp khác được mã hoá, giá trị cam kết của giao dịch T, giá trị cam kết tiền trả lại Y, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB đến một hoặc nhiều nút trong mạng blockchain (chuỗi khối) để một hoặc nhiều nút đó xác minh giao dịch.

Trong một số phương án, bước trình giao dịch bao gồm tổ hợp được mã hoá, một tổ hợp khác được mã hoá, giá trị cam kết của giao dịch T, giá trị cam kết tiền trả lại Y, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch bao gồm: bước trình giao dịch bao gồm tổ hợp được mã hoá, một tổ hợp khác được mã hoá, giá trị cam

kết của giao dịch T, giá trị cam kết tiền trả lại Y, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB đến một hoặc nhiều nút trong mạng blockchain, làm cho một hoặc nhiều nút, để đáp lại việc xác minh thành công giao dịch, xuất ra lượng giao dịch t cho người nhận, loại trừ một hoặc nhiều tài sản được trích cho giao dịch, và phát hành tiền trả lại y đến người gửi.

Theo một khía cạnh khác, phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp lưu trữ các lệnh để được thực hiện bởi bộ xử lý làm cho bộ xử lý thực hiện các hoạt động bao gồm: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; mã hoá tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch; và truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch.

Theo một khía cạnh khác, hệ thống bảo vệ thông tin bao gồm bộ xử lý và phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp được kết nối với bộ xử lý, phương tiện lưu trữ này lưu các lệnh được thực hiện bởi bộ xử lý làm cho hệ thống thực hiện các hoạt động bao gồm: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; mã hoá tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch; và truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch.

Theo một khía cạnh khác, phương pháp thực hiện bởi máy tính để bảo vệ thông tin bao gồm các bước: thu nhận tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t được mã hoá bằng khoá công khai PK_B của người nhận của giao dịch, và thu nhận giá trị cam kết của giao dịch T, trong đó: lượng giao dịch t được cam kết bằng sơ đồ cam kết bởi nút bên nhận được liên kết với người nhận của giao dịch để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; giải mã tổ hợp được thu nhận bằng khoá bí mật SK_B của người nhận của giao dịch để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t; và xác minh giao dịch

dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t.

Trong một số phương án, khoá công khai PK_B của người nhận và khoá bí mật SK_B của người nhận là các khoá mã hóa bất đối xứng.

Theo một khía cạnh khác, phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp lưu trữ các lệnh để được thực hiện bởi bộ xử lý làm cho bộ xử lý thực hiện các hoạt động bao gồm: thu nhận tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t được mã hoá bằng khoá công khai PK_B của người nhận của giao dịch, và thu nhận giá trị cam kết của giao dịch T, trong đó: lượng giao dịch t được cam kết bằng sơ đồ cam kết bởi nút bên nhận được liên kết với người nhận của giao dịch để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; giải mã tổ hợp được thu nhận bằng khoá bí mật SK_B của người nhận của giao dịch để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t; và xác minh giao dịch dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t.

Theo một khía cạnh khác, hệ thống bảo vệ thông tin bao gồm bộ xử lý và phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp được kết nối với bộ xử lý, phương tiện lưu trữ này lưu các lệnh được thực hiện bởi bộ xử lý làm cho hệ thống thực hiện các hoạt động bao gồm: thu nhận tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t được mã hoá bằng khoá công khai PK_B của người nhận của giao dịch, và thu nhận giá trị cam kết của giao dịch T, trong đó: lượng giao dịch t được cam kết bằng sơ đồ cam kết bởi nút bên nhận được liên kết với người nhận của giao dịch để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; giải mã tổ hợp được thu nhận bằng khoá bí mật SK_B của người nhận của giao dịch để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t; và xác minh giao dịch dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t.

Theo một khía cạnh khác, phương pháp thực hiện bởi máy tính để bảo vệ thông tin bao gồm các bước: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; gửi lượng giao dịch t, nhân tố mù của giao dịch r_t, và giá trị

cam kết của giao dịch T đến nút bên nhận được liên kết với người nhận của giao dịch để nút bên nhận xác minh giao dịch và mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận; thu nhận tổ hợp được mã hoá của nhân tố mù của giao dịch r_t và lượng giao dịch t từ nút bên nhận; và truyền tổ hợp được mã hoá và giá trị cam kết của giao dịch T đến các nút trong blockchain để các nút này xác minh giao dịch.

Theo một khía cạnh khác, phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp lưu trữ các lệnh để được thực hiện bởi bộ xử lý làm cho bộ xử lý thực hiện các hoạt động bao gồm: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; gửi lượng giao dịch t, nhân tố mù của giao dịch r_t, và giá trị cam kết của giao dịch T đến nút bên nhận được liên kết với người nhận của giao dịch để nút bên nhận xác minh giao dịch và mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận; thu nhận tổ hợp được mã hoá của nhân tố mù của giao dịch r_t và lượng giao dịch t từ nút bên nhận; và truyền tổ hợp được mã hoá và giá trị cam kết của giao dịch T đến các nút trong blockchain để các nút này xác minh giao dịch.

Theo một khía cạnh khác, hệ thống bảo vệ thông tin bao gồm bộ xử lý và phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp được kết nối với bộ xử lý, phương tiện lưu trữ này lưu các lệnh được thực hiện bởi bộ xử lý làm cho hệ thống thực hiện các hoạt động bao gồm: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t; gửi lượng giao dịch t, nhân tố mù của giao dịch r_t, và giá trị cam kết của giao dịch T đến nút bên nhận được liên kết với người nhận của giao dịch để nút bên nhận xác minh giao dịch và mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận; thu nhận tổ hợp được mã hoá của nhân tố mù của giao dịch r_t và lượng giao dịch t từ nút bên nhận; và truyền tổ hợp được mã hoá và giá trị cam kết của giao dịch T đến các nút trong blockchain để các nút này xác minh giao dịch.

Theo một khía cạnh khác, phương pháp thực hiện bởi máy tính để bảo vệ thông tin bao gồm các bước: thu nhận lượng giao dịch t của giao dịch, nhân tố mù của giao

dịch r_t, và giá trị cam kết của giao dịch T; xác minh giao dịch dựa trên lượng giao dịch được thu nhận t, nhân tố mù của giao dịch được thu nhận r_t, và giá trị cam kết của giao dịch được thu nhận T; để đáp lại việc xác minh thành công giao dịch, thì mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch để thu nhận tổ hợp được mã hoá; và truyền tổ hợp được mã hoá đến nút bên gửi được liên kết với người gửi của giao dịch.

Theo một khía cạnh khác, phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp lưu trữ các lệnh để được thực hiện bởi bộ xử lý làm cho bộ xử lý thực hiện các hoạt động bao gồm: thu nhận lượng giao dịch t của giao dịch, nhân tố mù của giao dịch r_t, và giá trị cam kết của giao dịch T; xác minh giao dịch dựa trên lượng giao dịch được thu nhận t, nhân tố mù của giao dịch được thu nhận r_t, và giá trị cam kết của giao dịch được thu nhận T; để đáp lại việc xác minh thành công giao dịch, thì mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch để thu nhận tổ hợp được mã hoá; và truyền tổ hợp được mã hoá đến nút bên gửi được liên kết với người gửi của giao dịch.

Theo một khía cạnh khác, hệ thống bảo vệ thông tin bao gồm bộ xử lý và phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp được kết nối với bộ xử lý, phương tiện lưu trữ này lưu các lệnh được thực hiện bởi bộ xử lý làm cho hệ thống thực hiện các hoạt động bao gồm: thu nhận lượng giao dịch t của giao dịch, nhân tố mù của giao dịch r_t, và giá trị cam kết của giao dịch T; xác minh giao dịch dựa trên lượng giao dịch được thu nhận t, nhân tố mù của giao dịch được thu nhận r_t, và giá trị cam kết của giao dịch được thu nhận T; để đáp lại việc xác minh thành công giao dịch, thì mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch để thu nhận tổ hợp được mã hoá; và truyền tổ hợp được mã hoá đến nút bên gửi được liên kết với người gửi của giao dịch.

Những đặc điểm kỹ thuật này và đặc điểm kỹ thuật khác của hệ thống, phương pháp, và phương tiện có thể đọc được bởi máy tính không chuyển tiếp được bộc lộ trong sáng chế này, cũng như phương pháp hoạt động và các chức năng của các thành phần liên quan của cấu trúc và sự kết hợp của các phần và các bộ phận được chế tạo, sẽ trở nên rõ ràng hơn khi xem xét phần mô tả dưới đây và các yêu cầu bảo hộ tiếp theo với sự tham khảo đến các hình vẽ đi kèm, tất cả tạo nên một phần của phần mô tả, trong đó

các số lệnh là để chỉ các bộ phận tương ứng trong các hình vẽ. Các hình vẽ này để làm cho sáng chế trở nên dễ hiểu hơn, tuy nhiên, các hình vẽ này chỉ mang tính chất minh hoạ và mô tả và không phải là giới hạn của sáng chế.

**Mô tả vắn tắt các hình vẽ**

Những đặc điểm nhất định của các phương án của kỹ thuật này được định ra trong các yêu cầu bảo hộ dưới đây. Kỹ thuật này có thể được hiểu rõ hơn về những đặc điểm và ưu điểm mà kỹ thuật này mang lại bằng cách tham khảo đến phần mô tả chi tiết dưới đây mà được biểu diễn theo các phương án minh hoạ, trong đó các nguyên lý của sáng chế được vận dụng, và các hình vẽ đi kèm:

Fig.1 minh hoạ một ví dụ về hệ thống bảo vệ thông tin, phù hợp với các phương án khác nhau của sáng chế.

Fig.2 minh hoạ ví dụ về các bước khởi tạo và xác minh giao dịch, phù hợp với các phương án khác nhau của sáng chế.

Fig.3A minh hoạ một ví dụ về lưu đồ của phương pháp bảo vệ thông tin, phù hợp với các phương án khác nhau của sáng chế.

Fig.3B minh hoạ một ví dụ về lưu đồ của phương pháp bảo vệ thông tin, phù hợp với các phương án khác nhau của sáng chế.

Fig.4A minh hoạ một ví dụ về lưu đồ của phương pháp bảo vệ thông tin, phù hợp với các phương án khác nhau của sáng chế.

Fig.4B minh hoạ một ví dụ về lưu đồ của phương pháp bảo vệ thông tin, phù hợp với các phương án khác nhau của sáng chế.

Fig.5 minh hoạ sơ đồ khối của hệ thống máy tính làm ví dụ mà trong đó có thể thực hiện một phương án bất kỳ được mô tả ở đấy của sáng chế.

**Mô tả chi tiết sáng chế**

Blockchain có thể được coi là một cơ sở dữ liệu phi tập trung, thường được gọi là sổ cái (ledger) phân tán vì hoạt động được thực hiện bởi các nút khác nhau (ví dụ, các thiết bị máy tính) trong mạng. Bất kỳ thông tin nào cũng có thể được ghi vào blockchain và được lưu hoặc đọc từ nó. Bất cứ ai cũng có thể thiết lập một máy chủ và tham gia mạng blockchain để trở thành một nút. Bất kỳ nút nào cũng có thể đóng góp

sức mạnh tính toán để duy trì blockchain bằng cách thực hiện các tính toán phức tạp, chẳng hạn như tính toán hàm băm để bổ sung một khối vào blockchain hiện tại và khối được bổ sung vào có thể chứa nhiều loại dữ liệu hoặc thông tin. Nút đóng góp sức mạnh tính toán cho khối được bổ sung vào có thể được thưởng bằng mã thông báo (token) (ví dụ, đơn vị tiền tệ kỹ thuật số). Vì blockchain không có nút trung tâm, mỗi nút là như nhau và giữ toàn bộ cơ sở dữ liệu blockchain.

Các nút, ví dụ, các thiết bị máy tính hoặc các hệ thống máy tính lớn hỗ trợ mạng blockchain và giữ cho nó hoạt động trơn tru. Có hai loại nút, nút đầy đủ (full node) và nút nhẹ (lightweight node). Các nút đầy đủ giữ một bản sao hoàn chỉnh của blockchain. Các nút đầy đủ trên mạng blockchain phê duyệt các giao dịch và các khối nhận được và chuyển tiếp chúng đến nút ngang hàng (peers) được kết nối để cung cấp xác minh đồng thuận về các giao dịch. Các nút nhẹ, mặt khác, chỉ tải xuống một phần của blockchain. Ví dụ, các nút nhẹ được sử dụng cho các giao dịch tiền kỹ thuật số. Một nút nhẹ sẽ giao tiếp với một nút đầy đủ khi nút nhẹ này muốn giao dịch.

Đặc tính phi tập trung này có thể giúp ngăn chặn sự xuất hiện của một trung tâm quản lý ở vị trí được kiểm soát. Ví dụ, việc duy trì tiền tệ kỹ thuật số (bit coin) blockchain được thực hiện bởi mạng lưới các nút giao tiếp của phần mềm bitcoin trong khu vực đang chạy. Sáng chế này sử dụng một hoặc nhiều blockchain hoặc tiền tệ kỹ thuật số, chẳng hạn như bitcoin và Ethereum, làm ví dụ. Một người có hiểu biết trung bình trong lĩnh vực kỹ thuật cần hiểu rằng các giải pháp kỹ thuật được bộc lộ trong sáng chế này có thể sử dụng hoặc áp dụng cho các loại blockchain và tiền tệ kỹ thuật số khác. Đó là, thay vì các ngân hàng, tổ chức hoặc quản trị viên theo nghĩa truyền thống, nhiều trung gian tồn tại dưới dạng máy chủ máy tính thực thi phần mềm bitcoin. Các máy chủ này tạo thành một mạng được kết nối qua Internet, trong đó bất kỳ ai cũng có khả năng tham gia mạng. Các giao dịch được cung cấp bởi mạng có thể ở dạng: "Người dùng A muốn gửi bitcoin Z cho người dùng B," trong đó các giao dịch được phát lên mạng bằng các ứng dụng phần mềm có sẵn. Các máy tính chủ hoạt động như các máy chủ bitcoin có thể hoạt động để phê duyệt các giao dịch tài chính này, bổ sung bản ghi của các giao dịch này vào bản sao của sổ cái, sau đó phát quảng bá các bổ sung sổ cái này đến các máy chủ khác của mạng.

Việc duy trì blockchain được gọi là "khai thác trên mạng" (mining), những người thực hiện việc duy trì như vậy được thưởng bằng bitcoin mới được tạo và phí giao dịch như đã nói ở trên. Ví dụ, các nút có thể xác định xem các giao dịch có hợp lệ hay không dựa trên một bộ quy tắc mà mạng blockchain đã cam kết. Người khai thác (miner) có thể ở bất kỳ châu lục nào và xử lý các khoản thanh toán bằng cách xác minh mỗi giao dịch là hợp lệ và bổ sung nó vào blockchain. Việc xác minh như vậy đạt được thông qua sự đồng thuận được cung cấp bởi một số lượng lớn các nhà trích và giả thiết rằng không có sự thông đồng có hệ thống. Cuối cùng, tất cả dữ liệu sẽ nhất quán, vì tất cả các phép tính toán phải đáp ứng các yêu cầu nhất định để hợp lệ và tất cả các nút sẽ được đồng bộ hóa để đảm bảo rằng blockchain là đồng nhất. Do đó, dữ liệu có thể được lưu trữ nhất quán trong một hệ thống phân tán của các nút blockchain.

Thông qua quá trình khai thác, các giao dịch như chuyển giao tài sản được xác minh và bổ sung vào blockchain đang phát triển bởi các nút mạng. Bằng cách duyệt qua toàn bộ blockchain, việc xác minh có thể bao gồm, ví dụ, liệu bên thanh toán có quyền truy cập vào tài sản chuyển nhượng hay không, liệu tài sản đã được sử dụng trước đó hay chưa, liệu lượng chuyển có chính xác hay không, v.v.... Ví dụ, trong giao dịch giả định (như là giao dịch bitcoin theo mô hình UTXO (đầu ra giao dịch chưa được chi tiêu), giao dịch tiền Ethereum theo mô hình tài khoản/số dư) được ký bởi người gửi, giao dịch được đề xuất có thể được phát lên mạng blockchain để khai thác. Người khai thác cần kiểm tra xem giao dịch có đủ điều kiện để được thực hiện theo lịch sử blockchain hay không. Nếu số dư ví của người gửi có đủ tiền theo lịch sử blockchain hiện có, thì giao dịch được coi là hợp lệ và có thể được bổ sung vào khối. Sau khi được xác minh, thì việc chuyển tài sản có thể được bao gồm trong khối tiếp theo sẽ được bổ sung vào blockchain.

Khối giống như một bản ghi cơ sở dữ liệu. Mỗi lần ghi dữ liệu sẽ tạo ra một khối. Các khối này được liên kết và bảo vệ nhờ sử dụng mật mã để trở thành các mạng được kết nối với nhau. Mỗi khối được kết nối với khối trước đó, cũng là nguồn gốc của tên "blockchain". Mỗi khối thường chứa hàm băm mật mã của khối trước, thời gian tạo và dữ liệu thực tế. Chẳng hạn, mỗi khối chứa hai phần: phần đầu khối để ghi lại giá trị tính năng của khối hiện tại và phần thân để ghi dữ liệu thực tế (ví dụ, dữ liệu giao dịch). Blockchain được liên kết thông qua các phần đầu khối. Mỗi phần đầu khối có thể chứa

nhiều giá trị đặc tính, chẳng hạn như phiên bản, hàm băm khối trước, gốc merkle, nhãn thời gian, mục tiêu khó và nonce. Hàm băm của khối trước không chỉ chứa địa chỉ của khối trước mà còn băm dữ liệu bên trong khối trước đó, do đó làm cho các blockchain không thể thay đổi được. Số nonce là một số mà khi được bổ sung vào sẽ tạo ra một hàm băm với một số bit 0 hàng đầu được chỉ rõ.

Để khai thác, thì hàm băm của nội dung của khối mới được lấy bởi một nút. Số nonce (ví dụ, dãy ngẫu nhiên) được bổ sung vào hàm băm để thu nhận dãy mới. Dãy mới được băm một lần nữa. Giá trị băm cuối cùng sau đó được so sánh với mục tiêu khó khăn (ví dụ, một mức) và xác định xem giá trị băm cuối cùng có thực sự nhỏ hơn mục tiêu khó khăn hay không. Nếu không, thì nonce được thay đổi và quá trình lặp lại. Nếu có, thì khối được bổ sung vào chuỗi và sổ cái công khai được cập nhật và thông báo về việc bổ sung. Nút chịu trách nhiệm cho việc bổ sung thành công được thưởng bằng bitcoin, ví dụ, bằng cách bổ sung một giao dịch phần thưởng cho chính nút đó vào khối mới (được gọi là tạo coinbase).

Nghĩa là, với mỗi đầu ra "Y", nếu k được chọn từ sự phân bố có entropy-min cao thì không thể tìm thấy đầu vào x sao cho H(k|x) = Y, trong đó K là nonce, x là hàm băm của khối, Y là mục tiêu khó khăn, và "|" biểu thị sự ghép nối. Do các hàm băm mật mã nhất thiết là phải ngẫu nhiên, theo nghĩa là đầu ra của chúng không thể dự đoán được từ đầu vào của chúng, chỉ có một cách duy nhất để tìm ra số nonce: thử lần lượt từng số nguyên, ví dụ 1, rồi 2, sau đó 3, v.v., có thể được gọi là cưỡng bức. Số lượng số 0 đứng đầu càng lớn, sẽ càng mất nhiều thời gian hơn nói chung để tìm một số nonce Y. Trong một ví dụ, hệ thống bitcoin liên tục điều chỉnh số lượng số 0 hàng đầu, do đó thời gian trung bình để tìm một số nonce là khoảng mười phút. Theo cách đó, khi khả năng xử lý phần cứng máy tính tăng lên theo thời gian, qua nhiều năm, thì giao thức bitcoin sẽ cần nhiều bit 0 hàng đầu hơn để việc khai thác luôn mất khoảng mười phút để thực hiện.

Như được mô tả, hàm băm là một nền tảng quan trọng cho blockchain. Thuật toán băm có thể được hiểu là một hàm nén các thông điệp có độ dài bất kỳ thành một bản tóm lược thông điệp (message digest) có độ dài cố định. Các thuật toán thường được sử dụng phổ biến hơn là MD5 và SHA. Trong một số phương án, độ dài hàm băm của blockchain là 256 bit, điều đó có nghĩa là cho dù nội dung ban đầu là gì, kết quả cuối cùng được tính toán sẽ là số nhị phân 256 bit. Và có thể đảm bảo rằng giá trị hàm

băm tương ứng là duy nhất miễn là nội dung ban đầu khác nhau. Ví dụ, giá trị hàm băm của dãy "123" là a8fdc205a9f19cc1c7507a60c4f01b13d11d7fd0 (số thập lục phân), và khi được chuyển đổi thành nhị phân thì có 256 bit và chỉ có "123" mới có giá trị băm này. Thuật toán băm trong blockchain là không thể suy ngược lại, nghĩa là phép tính xuôi rất dễ dàng (từ "123" thành a8fdc205a9f19cc1c7507a60c4f01b1c7507a60c4f01b13d11d7fd0), và phép tính suy ngược lại là không thể thực hiện được ngay cả khi tất cả tài nguyên tính toán đều được tận dụng. Do đó, hàm băm của mỗi khối của blockchain là duy nhất.

Hơn nữa, nếu nội dung của khối thay đổi, thì giá trị băm của nó sẽ thay đổi. Khối và giá trị băm là sự tương ứng một-một và giá trị băm của mỗi khối được tính cụ thể cho phần đầu khối. Nghĩa là, các giá trị tính năng của các phần đầu khối được kết nối để tạo thành một dãy dài và sau đó hàm băm được tính cho dãy. Ví dụ, "Hash = SHA256 (phần đầu khối)" là một công thức tính toán giá trị băm khối, SHA256 là một thuật toán băm blockchain được áp dụng cho phần đầu khối. Hàm băm được xác định duy nhất bởi phần đầu khối chứ không phải phần thân khối. Như đã đề cập ở trên, phần đầu khối chứa rất nhiều nội dung, bao gồm hàm băm của khối hiện tại và hàm băm của khối trước đó. Điều này có nghĩa là nếu nội dung của khối hiện tại thay đổi hoặc nếu giá trị hàm băm của khối trước đó thay đổi, thì sẽ gây ra tiền trả lại về giá trị băm trong khối hiện tại. Nếu tin tặc sửa đổi một khối, thì giá trị hàm băm của khối đó sẽ thay đổi. Để khối sau kết nối với khối được sửa đổi, thì tin tặc phải sửa đổi lần lượt tất cả các khối tiếp theo, vì khối tiếp theo phải chứa giá trị hàm băm của khối trước đó. Nếu không, thì khối sửa đổi sẽ được tách ra khỏi blockchain. Vì lý do thiết kế, phép tính toán hàm băm rất tốn thời gian và gần như không thể sửa đổi nhiều khối trong một khoảng thời gian ngắn trừ khi tin tặc đã nắm giữ hơn 51% sức mạnh tính toán của toàn bộ mạng. Do đó, blockchain đảm bảo độ tin cậy của chính nó và một khi dữ liệu được ghi, nó không thể bị giả mạo.

Khi người khai thác tìm thấy hàm băm (nghĩa là chữ ký hoặc giải pháp thích hợp) cho khối mới, thì người khai thác sẽ phát rộng chữ ký này đến tất cả những người khai thác khác (các nút của blockchain). Khi đó, những người khai thác khác sẽ lần lượt xác minh liệu giải pháp đó có tương ứng với bài toán của khối của người gửi hay không (nghĩa là xác định xem liệu đầu vào băm có thực sự dẫn đến chữ ký đó không). Nếu giải

pháp là đúng, thì những người khai thác khác sẽ xác nhận giải pháp và đồng ý rằng khối mới có thể được bổ sung vào blockchain. Do đó, sự đồng thuận của khối mới đạt được. Điều này còn được gọi là "bằng chứng công việc". Các khối mà đã đạt được sự đồng thuận giờ đây có thể được bổ sung vào blockchain và được phát rộng đến tất cả các nút trên mạng cùng với chữ ký của nó. Các nút sẽ chấp nhận khối và lưu nó vào dữ liệu giao dịch của họ miễn là các giao dịch bên trong khối tương ứng chính xác với số dư ví hiện tại (lịch sử giao dịch) tại thời điểm đó. Mỗi khi một khối mới được bổ sung vào đầu khối này, thì phép cộng đó cũng được tính là một xác nhận khác cho các khối trước khối đó. Ví dụ, nếu một giao dịch được bao gồm trong khối 502 và blockchain dài 507 khối, điều đó có nghĩa là giao dịch có năm xác nhận (tương ứng với các khối 507 đến 502). Giao dịch càng có nhiều xác nhận, thì kẻ tấn công càng khó thay đổi.

Trong một số phương án, một hệ thống tài sản blockchain làm ví dụ, sử dụng mật mã khóa công khai, trong đó hai khóa mật mã, một khóa công khai và một khóa bí mật, được tạo. Khóa công khai có thể được coi là số tài khoản và khóa bí mật có thể được coi là thông tin sở hữu. Ví dụ, ví bitcoin là tập hợp các khóa công khai và khóa bí mật. Quyền sở hữu một tài sản (ví dụ, tiền kỹ thuật số, tài sản tiền mặt, cổ phiếu, vốn chủ sở hữu, trái phiếu) được liên kết với một địa chỉ tài sản nhất định có thể được xem như là một khóa bí mật thuộc về địa chỉ đó. Ví dụ, phần mềm ví bitcoin, đôi khi được gọi là "phần mềm khách bitcoin", cho phép một người dùng nhất định giao dịch bitcoin. Một chương trình ví tạo ra và lưu trữ khóa bí mật và giao tiếp với các nút ngang hàng trên mạng bitcoin. Khóa công khai và khóa bí mật có thể được gọi là các khóa mã hóa bất đối xứng (hoặc khóa mã hóa bất đối xứng).

Trong các giao dịch blockchain, người trả tiền và người được trả tiền được xác định trong blockchain bằng các khóa mật mã công khai của họ. Ví dụ, hầu hết các giao dịch chuyển bitcoin hiện đại là từ một khóa công khai này sang một khóa công khai khác. Trong thực tế hàm băm của các khóa này được sử dụng trong blockchain và được gọi là "địa chỉ bitcoin". Về nguyên tắc, nếu một kẻ tấn công giả định S có thể ăn cắp tiền của người A bằng cách bổ sung giao dịch vào sổ cái blockchain như người A trả 100 bitcoin, thì người dùng sử dụng địa chỉ bitcoin của người dùng thay vì tên của họ. Giao thức bitcoin ngăn chặn hành vi trộm cắp này bằng cách yêu cầu mọi chuyển khoản phải được ký điện tử bằng khóa bí mật của người trả tiền và chỉ có thể bổ sung các

chuyển khoản được ký vào sổ cái blockchain. Vì người S không thể giả mạo chữ ký của người A, nên người S không thể lừa đảo người A bằng cách bổ sung một mục vào blockchain tương đương với người "người A trả cho người S 200 bitcoin". Cùng lúc đó, người bất kỳ có thể xác minh chữ ký của người A sử dụng khoá công khai của người đó, và do đó người đó đã xác minh giao dịch bất kỳ trong blockchain mà người đó là người trả tiền.

Trong ngữ cảnh giao dịch bitcoin, để chuyển một số bitcoin cho người dùng B, người dùng A có thể tạo một bản ghi chứa thông tin về giao dịch thông qua một nút. Bản ghi có thể được ký bằng khóa ký tên (khóa bí mật) của người dùng A và chứa khóa xác minh công khai của người dùng A và khóa xác minh công khai của người dùng B. Chữ ký được sử dụng để xác nhận rằng giao dịch đã đến từ người dùng và cũng ngăn chặn giao dịch bị thay đổi bởi bất kỳ ai khác sau khi được phát hành. Bản ghi được đóng gói cùng với bản ghi khác diễn ra trong cùng cửa sổ thời gian trong một khối mới có thể được phát đến các nút đầy đủ. Khi nhận được các bản ghi, thì các nút đầy đủ có thể hoạt động để kết hợp các bản ghi vào sổ cái của tất cả các giao dịch đã từng diễn ra trong hệ thống blockchain, bổ sung khối mới vào blockchain được chấp nhận trước đó thông qua quy trình khai thác được mô tả ở trên và phê duyệt khối được bổ sung vào để chống lại các quy tắc đồng thuận của mạng.

Mô hình UTXO (đầu ra giao dịch chưa được chi tiêu) và mô hình tài khoản/Số dư là hai mô hình mẫu mực để thực hiện các giao dịch blockchain. UTXO là một mô hình đối tượng blockchain. Theo UTXO, tài sản được biểu diễn bằng đầu ra của các giao dịch blockchain chưa được chi tiêu, có thể được sử dụng làm đầu vào trong các giao dịch mới. Ví dụ, tài sản của người dùng được chuyển nhượng có thể ở dạng UTXO. Để chi tiêu (giao dịch) tài sản, thì người dùng A phải đăng xuất bằng khóa bí mật. Bitcoin là một ví dụ về một loại tiền kỹ thuật số sử dụng mô hình UTXO. Trong trường hợp giao dịch blockchain hợp lệ, thì các đầu ra chưa được sử dụng có thể được sử dụng để thực hiện các giao dịch tiếp theo. Trong một số ít, thì chỉ có thể sử dụng các đầu ra chưa được sử dụng trong các giao dịch tiếp theo để ngăn chặn chi tiêu và gian lận kép. Vì lý do này, nên các đầu vào trên blockchain sẽ bị xóa khi giao dịch xảy ra, đồng thời, các đầu ra được tạo ra dưới dạng UTXO. Những đầu ra giao dịch chưa được sử dụng

này có thể được sử dụng (bởi những người nắm giữ khóa bí mật, ví dụ, những người có ví tiền kỹ thuật số) cho mục đích giao dịch trong tương lai.

Mô hình tài khoản/số dư (hay còn gọi là mô hình giao dịch dựa trên tài khoản), mặt khác, theo dõi số dư của từng tài khoản như một trạng thái toàn cầu. Số dư của một tài khoản được kiểm tra để đảm bảo rằng nó lớn hơn hoặc bằng lượng giao dịch chi tiêu. Một ví dụ về cách thức mô hình tài khoản/số dư hoạt động trong Ethereum được cung cấp:

1. Alice thu được 5 ether thông qua việc khai thác. Nó được ghi lại trong hệ thống rằng Alice có 5 ether.

2. Alice muốn cho Bob 1 ether, vì vậy trước tiên hệ thống sẽ khấu trừ 1 ether từ tài khoản Alice, vì vậy Alice hiện có 4 ethers.

3. Hệ thống sau đó tăng tài khoản Bob lên 1 ether. Hệ thống biết rằng Bob ban đầu có 2 ether, do đó số dư của Bob được tăng lên thành 3 ether.

Việc lưu trữ bản ghi cho Ethereum có thể giống như trong một ngân hàng. Một cách thức tương tự đang sử dụng thẻ ATM/thẻ ghi nợ. Ngân hàng theo dõi mỗi thẻ ghi nợ có bao nhiêu tiền và khi Bob cần chi tiền, thì ngân hàng kiểm tra hồ sơ của mình để đảm bảo Bob có đủ số dư trước khi phê duyệt giao dịch.

Vì blockchain và các sổ cái tương tự khác hoàn toàn công khai, nên bản thân blockchain không có sự bảo vệ quyền riêng tư. Bản chất công khai của mạng P2P có nghĩa là, trong khi những người sử dụng nó không được định danh bằng tên, việc liên kết các giao dịch với các cá nhân và công ty là khả thi. Ví dụ, trong kiều hối xuyên biên giới hoặc trong chuỗi cung ứng, thì lượng giao dịch có giá trị bảo vệ cực kỳ cao, bởi vì với thông tin về lượng giao dịch, nên có thể suy ra vị trí và danh tính cụ thể của các bên giao dịch. Đối tượng của giao dịch có thể bao gồm, ví dụ, tiền, mã thông báo, tiền kỹ thuật số, hợp đồng, chứng thư, hồ sơ y tế, thông tin khách hàng, cổ phiếu, trái phiếu, vốn chủ sở hữu hoặc bất kỳ tài sản nào khác có thể được mô tả dưới dạng kỹ thuật số. Mặc dù mô hình UTXO có thể cung cấp ẩn danh cho lượng giao dịch, ví dụ, thông qua chữ ký vòng trong Monero và mật mã không kiến thức (zero-knowledge) Zcash, nhưng các lượng giao dịch vẫn không được bảo vệ theo mô hình tài khoản/số dư. Do đó, một vấn đề kỹ thuật được giải quyết theo sáng chế này là làm thế nào để bảo vệ thông tin

trực tuyến như bảo vệ lượng giao dịch. Các giao dịch như vậy có thể theo mô hình tài khoản/số dư.

Một số kỹ thuật hiện có đề xuất sử dụng sơ đồ cam kết Pedersen để mã hóa lượng giao dịch và thay thế mô hình tài khoản/số dư. Theo sơ đồ, người gửi sẽ gửi lượng giao dịch và một số ngẫu nhiên tương ứng với cam kết Pedersen về lượng giao dịch cho người được thanh toán thông qua một kênh được bảo vệ ngoài blockchain. Người được thanh toán xác minh nếu số ngẫu nhiên khớp với cam kết giao dịch và thực hiện lưu trữ cục bộ. Ví dụ, trong mô hình tài khoản/số dư, tài khoản có thể được coi là ví (tài khoản) để giữ tài sản được tổng hợp nhưng không được hợp nhất. Mỗi tài sản có thể tương ứng với một loại tài sản (ví dụ, tiền điện tử) và số dư của tài khoản là tổng của các giá trị tài sản. Ngay cả các tài sản cùng loại cũng không được hợp nhất. Trong quá trình giao dịch, người nhận tài sản chuyển nhượng có thể được chỉ rõ và tài sản tương ứng có thể được xóa khỏi ví để cấp tiền cho giao dịch. Các nút blockchain xác minh rằng ví thanh toán có đủ tài sản để trang trải giao dịch và sau đó các nút xóa tài sản được chuyển khỏi ví thanh toán và bổ sung một tài sản tương ứng vào ví người nhận.

Tuy nhiên, những hạn chế vẫn tồn tại trong sơ đồ như vậy. Đầu tiên, sơ đồ yêu cầu người dùng duy trì việc lưu trữ liên tục cục bộ để quản lý số ngẫu nhiên và số dư ở dạng văn bản nguyên gốc (plaintext) tương ứng với số dư tài khoản được mã hóa và việc thực hiện quản lý rất phức tạp; thứ hai, việc lưu trữ các nhân tố mù (blinding factor) (ví dụ, số ngẫu nhiên) và số dư ở dạng văn bản nguyên gốc tương ứng với "tài sản Pedersen" trong một nút cục bộ dễ bị mất hoặc hỏng, trong khi lưu trữ sao lưu ở nhiều nút rất khó nhận ra do tiền trả lại thường xuyên trong số dư tài khoản.

Các hệ thống và phương pháp được trình bày trong sáng chế này có thể khắc phục các hạn chế trên và đạt được sự bảo vệ chắc chắn đối với lượng giao dịch, giá trị tài sản và các nhân tố mù trong các sơ đồ cam kết. Do đó, các khóa bí mật có thể được sử dụng để mã hóa/giải mã các số ngẫu nhiên và số dư dạng văn bản nguyên gốc, do đó cung cấp khả năng quản lý thuận tiện hơn. Hơn nữa, việc lưu trữ thông tin được mã hóa trong blockchain đảm bảo rằng lượng giao dịch, giá trị tài sản và các nhân tố mù trong các sơ đồ cam kết không dễ bị mất hoặc bị giả mạo.

Trong một số phương án, một sơ đồ cam kết (ví dụ, cam kết Pedersen) có thể mã hóa một giá trị nhất định a (ví dụ, lượng giao dịch, giá trị tài sản, tham số chính) như sau:

$$PC(a) = r \times G + a \times H$$

Trong đó r là một nhân tố mù ngẫu nhiên (còn được gọi là nhân tố ràng buộc) để tạo ra sự che giấu, G và H là các bộ tạo/các điểm cơ sở được thỏa thuận công khai của đường cong elip và có thể được chọn ngẫu nhiên, sn là giá trị của cam kết, C (sn) là điểm đường cong được sử dụng như cam kết và được trao cho đối tác và H là một điểm đường cong khác. Tức là, G và H có thể được biết đến như là các tham số cho các nút. Việc tạo ra các số "nothing up my sleeve" ("không có gì thay đổi") của H có thể được tạo ra bằng cách băm điểm cơ sở (basepoint) G với ánh xạ hàm băm từ điểm này sang điểm khác với H = Hash (G). H và G là các tham số công khai của hệ thống đã cho (ví dụ, các điểm được tạo ngẫu nhiên trên một đường cong elip). Mặc dù phần trên cung cấp một ví dụ về cam kết Pedersen ở dạng đường cong elip, nhưng các hình thức khác nhau của cam kết Pedersen hoặc các sơ đồ cam kết khác có thể được sử dụng thay thế.

Sơ đồ cam kết duy trì bảo vệ dữ liệu nhưng vẫn cam kết dữ liệu để dữ liệu không thể bị thay đổi sau đó bởi người gửi dữ liệu. Nếu một bên chỉ biết giá trị cam kết (ví dụ, PC(a)), thì họ không thể xác định giá trị dữ liệu ẩn chứa (underlying) nào (ví dụ, a) đã được cam kết. Cả dữ liệu (ví dụ, a) và nhân tố mù (ví dụ, r) có thể được tiết lộ sau (ví dụ, bởi nút khởi tạo) và người nhận (ví dụ, nút đồng thuận) của cam kết có thể chạy cam kết và xác minh rằng dữ liệu cam kết khớp với dữ liệu được tiết lộ. Nhân tố mù có mặt vì nếu không có nó, thì sẽ có ai đó có thể cố gắng đoán ra dữ liệu.

Các sơ đồ cam kết là một cách để người gửi (bên cam kết) cam kết một giá trị (ví dụ, a) sao cho giá trị được cam kết vẫn ở chế độ bảo vệ, nhưng sau đó, bên cam kết sẽ tiết lộ một tham số cần thiết của quy trình cam kết. Các sơ đồ cam kết mạnh có thể là cả ẩn giấu thông tin và ràng buộc tính toán. Ẩn giấu là khái niệm một giá trị cho trước a và cam kết của giá trị đó PC(a) sẽ không liên quan. Đó là, PC(a) sẽ không tiết lộ thông tin về a. Với PC(a), G và H đã biết, gần như không thể biết a vì số r ngẫu nhiên. Một sơ đồ cam kết là ràng buộc nếu không có cách nào hợp lý mà để hai giá trị khác nhau có thể dẫn đến cùng một cam kết. Một cam kết Pedersen hoàn toàn che giấu và ràng buộc

tính toán theo giả định logarit rời rạc. Hơn nữa, với r, G, H và PC(a) đã biết, thì có thể xác minh PC(a) bằng cách xác định xem liệu PC(a) = r × G + a × H.

Cam kết Pedersen có một thuộc tính bổ sung: có thể bổ sung các cam kết và tổng của một tập hợp các cam kết cũng giống như một cam kết đối với tổng dữ liệu (với nhân tố mù được đặt là tổng của các nhân tố mù): PC( r1, data1) + PC(r2, data2) == PC(r1 + r2, data1 + data2); PC(r1, data1) − PC(r1, data1) == 0. Nói cách khác, cam kết bảo tồn tính cộng và thuộc tính giao hoán được áp dụng, tức là, cam kết Pedersen mạng tính đồng hình phù, trong đó dữ liệu ẩn giấu có thể bị thao túng bằng toán học khi nó không được mã hóa.

Trong một phương án, một cam kết Pedersen được sử dụng để mã hóa giá trị đầu vào có thể được xây dựng bằng các điểm đường cong elip. Thông thường, khóa công khai mật mã đường cong elip (ECC) được tạo bằng cách nhân một trình tạo cho nhóm (G) với khóa bí mật (r): Pub = rG. Kết quả có thể được tuần tự hóa thành một mảng 33 byte. Các khóa công khai của ECC có thể tuân theo thuộc tính đồng hình phụ được đề cập trước đó đối với các cam kết Pedersen. Đó là: Pub1 + Pub2 = (r1 + r2 (mod n)) G. Cam kết Pedersen cho giá trị đầu vào có thể được tạo bằng cách chọn một trình tạo bổ sung cho nhóm (H, trong các phương trình bên dưới) để không ai biết logarit rời rạc cho trình tạo thứ hai H đối với trình tạo thứ nhất G (hoặc ngược lại), nghĩa là không một ai biết x sao cho rG = H. Điều này có thể được thực hiện, ví dụ, bằng cách sử dụng hàm băm mật mã của G để chọn H: H = to_point (SHA256 (ENCODE (G))).

Với hai bộ tạo G và H, một sơ đồ cam kết mẫu mực để mã hóa giá trị đầu vào có thể được định nghĩa là: cam kết = rG + aH. Ở đây, r có thể là nhân tố mù bí mật và có thể là giá trị đầu vào được cam kết. Do đó, nếu sn được cam kết, thì có thể thu nhận sơ đồ cam kết được mô tả ở trên (a) = r × G + a × H. Các cam kết của Pedersen là bảo vệ về mặt lý thuyết thông tin: đối với cam kết bất kỳ, thì luôn tồn tại một số nhân tố mù sẽ làm cho một lượng bất kỳ khớp với cam kết. Các cam kết Pedersen có thể an toàn về mặt tính toán trước các cam kết giả mạo, theo phương án ánh xạ theo cách tùy chọn không thể tính toán được.

Bên (nút) đã cam kết một giá trị có thể mở cam kết bằng cách tiết lộ giá trị ban đầu a và nhân tố r hoàn thành phương trình cam kết. Bên muốn mở giá trị PC(a) sau đó sẽ tính lại cam kết để xác minh rằng giá trị ban đầu được chia sẻ thực sự khớpvới cam

kết PC(a) ban đầu nhận được. Do đó, thông tin loại tài sản có thể được bảo vệ bằng cách ánh xạ nó thành một số liên tiếp duy nhất và sau đó mã hóa nó theo cam kết của Pedersen. Số ngẫu nhiên r được chọn khi tạo cam kết khiến mọi người gần như không thể suy ra loại tài sản được cam kết theo giá trị cam kết PC(a).

Trong quá trình giao dịch, bảo vệ thông tin rất quan trọng để bảo đảm quyền riêng tư của người dùng và số lượng giao dịch là một loại thông tin thiếu sự bảo vệ. Fig.1 thể hiện một hệ thống làm ví dụ 100 để bảo vệ thông tin, phù hợp với các phương án khác nhau của sáng chế. Như được thể hiện, mạng blockchain có thể bao gồm nhiều nút (ví dụ, các nút đầy đủ được triển khai trong máy chủ, máy tính, v.v.). Đối với một số nền tảng blockchain (ví dụ, NEO), thì các nút đầy đủ với mức độ quyền biểu quyết nhất định có thể được gọi là các nút đồng thuận, chịu trách nhiệm xác minh giao dịch. Trong sáng chế này, các nút đầy đủ, các nút đồng thuận hoặc các nút tương đương khác 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 như máy tính xách tay và điện thoại di động đóng vai trò là các nút nhẹ để thực hiện giao dịch. Ví dụ, người dùng A có thể muốn giao dịch với người dùng B bằng cách chuyển 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 được cài đặt với phần mềm blockchain phù hợp cho giao dịch. Thiết bị của người dùng A có thể được gọi là nút khởi tạo A khởi tạo giao dịch với thiết bị của người dùng B được gọi là nút bên nhận B. Nút A có thể truy cập chuỗi khối thông qua giao tiếp với nút 1 và nút B có thể truy cập blockchain thông qua giao tiếp với nút 2. Ví dụ, nút A và nút B có thể trình giao dịch đến blockchain thông qua nút 1 và nút 2 để yêu cầu bổ sung giao dịch vào blockchain. Tắt blockchain, nút A và nút B có thể có các kênh liên lạc khác (ví dụ, giao tiếp Internet thông thường mà không thông qua các nút 1 và 2).

Mỗi nút trong số các nút trên Fig.1 có thể bao gồm một bộ xử lý và phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp lưu trữ các lệnh để bộ xử lý thực thi để làm cho nút (ví dụ, bộ xử lý) thực hiện các bước khác nhau để bảo vệ thông tin được mô tả trong tài liệu này. Mỗi nút có thể được cài đặt bằng một phần mềm (ví dụ, chương trình giao dịch) và/hoặc phần cứng (ví dụ, các kết nối có dây, không dây)

để giao tiếp với các nút khác và/hoặc các thiết bị khác. Thông tin chi tiết về phần cứng và phần mềm nút được mô tả sau với sự tham khảo đến Fig.5.

Fig.2 minh họa các bước ví dụ để giao dịch và xác minh giữa một nút bên gửi A, nút bên nhận B và một hoặc nhiều nút xác minh, phù hợp với các phương án khác nhau của sáng chế. Các hoạt động được trình bày dưới đây được xem là minh họa. Tùy thuộc vào việc thực hiện, các bước ví dụ có thể bao gồm các bước bổ sung, loại trừ một số bước hoặc thay thế một số bước được thực hiện theo các trình tự khác nhau hoặc được thực hiện song song.

Trong các phương án khác nhau, tài khoản của các bên giao dịch (người dùng A và người dùng B) được cấu hình theo mô hình tài khoản/số dư. Người dùng A và người dùng B có thể thực hiện các bước sau để thực hiện giao dịch qua một hoặc nhiều thiết bị, chẳng hạn như máy tính xách tay, điện thoại di động, v.v. Các thiết bị có thể được cài đặt với phần mềm và phần cứng phù hợp để thực hiện các bước khác nhau. Mỗi tài khoản có thể được liên kết với một cặp khóa riêng mật mã (khóa bí mật) - khóa công khai. Khóa bí mật có thể được ký hiệu là SK = x và khóa công khai có thể được ký hiệu là PK = xG, trong đó G là trình tạo của nhóm. Mỗi tài khoản có thể chứa nhiều tài sản khác nhau, mỗi tài sản được ký hiệu là: (V = PC(r, v), E(K, r, v)), trong đó v biểu diễn mệnh giá của tài sản, V biểu diễn cam kết Pedersen của mệnh giá v, r là một nhân tố mù (ví dụ, số ngẫu nhiên), PC() là thuật toán cam kết Pedersen, E() là thuật toán mã hóa (ví dụ, thuật toán mã hóa khóa bất đối xứng) và K là khóa mã hóa. Trong một ví dụ, mỗi tài sản có thể được ký hiệu là (V = PC(r, v), E(K, r||v)), trong đó || biểu diễn sự ghép nối. Mỗi tài sản cũng có thể bao gồm thông tin khác với thông tin được liệt kê, chẳng hạn như thông tin nguồn của tài sản.

Trong một ví dụ, trước khi người dùng A giao dịch thành công lượng t cho người dùng B trong giao dịch được xác minh bằng blockchain, địa chỉ (address) và tài sản (asset) trong tài khoản của A và tài khoản của B như sau:

Đối với tài khoản của A (account A):

Địa chỉ: (SK_A=a, PK_A=aG)

Các tài sản A_1 đến A_m một cách lần lượt có các giá trị a_1 đến a_m được miêu tả như sau:

(A_1=PC(r_{a_1}, a_1), E(PK_A, r_{a_1}||a_1)),

(A_2=PC(r_{a_2}, a_2), E(PK_A, r_{a_2}||a_2)),

...

(A_m=PC(r_{a_m}, a_m), E(PK_A, r_{a_m}||a_m))

Đối với tài khoản của B (account B):

Địa chỉ: (SK_B=b, PK_B=bG)

Các tài sản B_1 đến B_n một cách lần lượt có các giá trị b_1 đến b_n được miêu tả như sau:

(B_1=PC(r_{b_1}, b_1), E(PK_B, r_{b_1}||b_1)),

(B_2=PC(r_{b_2}, b_2), E(PK_B, r_{b_2}||b_2)),

...

(B_n=PC(r_{b_n}, b_n), E(PK_B, r_{b_n}||b_n))

Trong một số phương án, việc tạo khóa có thể dựa trên đường cong elip ecp256k1 cho mỗi tài khoản theo mô hình tài khoản/số dư. Ví dụ, trên Ethereum ecp256k1, bất kỳ số nào trong khoảng từ 1 đến 2256-1 có thể là khóa bí mật SK hợp lệ. Một thư viện tốt sẽ tạo một khóa bí mật mà có xem xét đến việc có đủ tính ngẫu nhiên. Ethereum yêu cầu khóa bí mật SK phải dài 256 bit. Việc tạo khóa công khai được thực hiện nhờ sử dụng phép tạo nhóm của mật mã ECC. Để lấy khóa công khai PK, thì khóa bí mật có thể được nhân với G. Phép nhân được sử dụng để lấy khóa công khai PK là phép nhân ECC (phép nhân điểm đường cong elip), khác với phép nhân thông thường. G là điểm tạo là một trong những tham số miền của mật mã ECC. G có thể có giá trị cố định cho ecp256k1. Địa chỉ có thể là, ví dụ, 20 byte cuối cùng của hàm băm của khóa công khai PK.

Trong một số phương án, tại bước 201, nút A có thể khởi tạo giao dịch với nút B. Ví dụ, người dùng A và người dùng B có thể thương lượng lượng giao dịch t từ tài khoản A của người dùng A đến tài khoản B của người dùng B. Tài khoản A và tài khoản B có thể tương ứng với "ví" của người dùng được mô tả trong tài liệu này. Tài khoản A có thể có một hoặc nhiều tài sản. Tài sản có thể bao gồm, ví dụ, tiền, mã thông báo, tiền kỹ thuật số, hợp đồng, chứng thư, hồ sơ y tế, chi tiết khách hàng, cổ phiếu, trái phiếu, vốn chủ sở hữu hoặc bất kỳ tài sản nào khác có thể được mô tả dưới dạng kỹ thuật số. Tài khoản B có thể có một hoặc nhiều tài sản hoặc không có tài sản. Mỗi tài sản có thể được liên kết với nhiều thông tin blockchain khác nhau được lưu trữ trong các khối của

blockchain, thông tin blockchain bao gồm, ví dụ, NoteType biểu diễn loại tài sản, NoteID biểu diễn nhận dạng duy nhất của tài sản, giá trị cam kết biểu diễn giá trị cam kết (ví dụ, cam kết Pedersen) của giá trị tài sản, mã hóa của số ngẫu nhiên và giá trị tài sản, v.v.

Như được mô tả liên quan đến tài khoản A, trong một số phương án, các tài sản A_1 đến A_m tương ứng một cách lần lượt với các giá trị tài sản a_1 đến a_m và các số ngẫu nhiên r_1 đến r_m. Dựa trên các số ngẫu nhiên r_1 đến r_m, nút A có thể cam kết các giá trị tài sản trong tài khoản A bằng sơ đồ cam kết (ví dụ, cam kết Pedersen) để thu nhận các giá trị cam kết được mã hóa. Ví dụ, các giá trị cam kết được mã hóa có thể là PC_1 đến PC_m, trong đó PC_i = PC(r_{a_i}, a_i) = r_{a_i}×G + a_i×H, trong đó G và H là các tham số đã biết và i nằm trong khoảng 1 và M. Ngoài trường thứ nhất PC(…), thì mỗi tài sản cũng được liên kết với trường thứ hai E(…) như mô tả trước đó. Trường thứ hai E(…) có thể biểu diễn mã hóa số ngẫu nhiên và giá trị tài sản tương ứng được mã hóa bằng khóa PK_A. Ví dụ, mã hóa có thể là E(PK_A, r_{a_i}||a_i)). PC(…) và E(…) cho mỗi tài sản có thể được kế thừa từ các giao dịch trước đó. Cơ chế tương tự có thể áp dụng cho tài khoản B và các tài sản của nó.

Trong một số phương án, để thỏa mãn lượng giao dịch t, thì người dùng A có thể sử dụng khóa bí mật SK_A để giải mã một hoặc nhiều tài sản có giá trị tổng hợp ít nhất t từ tài khoản A. Ví dụ, nút A có thể trích tài sản A_1, A_2, …, A_k cho giao dịch này , trong đó k nhỏ hơn hoặc bằng m. Các tài sản còn lại A_k+1, A_k+2, …, A_m của tài khoản A chưa được trích. Tương ứng, nút A có thể đọc tài sản PC(r_{a_1}, a_1), PC(r_{a_2}, a_2), …, PC(r_{a_k}, a_k) từ nút 1. Với các số ngẫu nhiên r_{a_1} , r_{a_2}, …, r_{a_k} được nút A biết đến, nút A có thể giải mã các tài sản đã đọc PC(r_{a_1}, a_1), PC(r_{a_2}, a_2), …, PC(r_{ a_k}, a_k) để lấy các giá trị tài sản a_1, a_2, …, a_k để đảm bảo rằng tổng (a_1 + a_2 + … + a_k) không nhỏ hơn lượng giao dịch t. Các tài sản khác nhau có thể được trao đổi với nhau trong tài khoản dựa trên các tỷ lệ khác nhau.

Trong một số phương án, số lượng giá trị tài sản được chọn vượt quá t, nếu có, được đặt thành y như là tiền trả lại. Ví dụ, nút A có thể xác định tiền trả lại y = (a_1 + a_2 + … + a_k) - t. Nút A có thể chọn các số ngẫu nhiên r_t và r_y làm các nhân tố mù để tạo ra các cam kết Pedersen cho t và y: T = PC(r_t, t), Y = PC(r_y, y). Nghĩa là, nút

A có thể tạo ra một số ngẫu nhiên r_t cho t và một số ngẫu nhiên r_y cho y. Nút A có thể cam kết t và r_t bằng sơ đồ cam kết để thu nhận giá trị cam kết T = PC(r_t, t) và cam kết y và r_y bằng sơ đồ cam kết để thu nhận giá trị cam kết Y = PC(r_y, y).

Ngoài ra, trong một số phương án, nút A có thể sử dụng khóa công khai PK_B của người dùng B để mã hóa (r_t||t), mà mang đến sự mã hóa E(PK_B, r_t||t) và sử dụng khóa công khai PK_A của người dùng A để mã hóa (r_y||y), mà mang đến sự mã hóa E(PK_A, r_y||y). Fig.3A và Fig.3B có thể làm theo ví dụ này. Thay thế cho việc thu được mã hóa E(PK_B, r_t||t) bởi nút A, thì người dùng A có thể gửi r_t và t đến nút B cùng với thông tin giao dịch, làm cho nút B tạo khóa thứ hai để mã hóa (r_t||t) với PK_B. Nút B sẽ gửi sự mã hóa đến nút A để cho phép nút A xác minh. Fig.4A và Fig.4B có thể làm theo ví dụ này. Mặc dù sự móc nối được sử dụng trong các ví dụ khác nhau của sáng chế này, nhưng các kết hợp đầu vào, đầu ra hoặc các tham số khác có thể được sử dụng cho chức năng mã hóa hoặc hoạt động khác

Ngoài ra, trong một số phương án, nút A có thể tạo bằng chứng phạm vi RP để chứng minh cho các nút blockchain nếu giá trị của T = PC(r_t, t) và giá trị của Y = PC(r_y, y) đều nằm trong phạm vi hợp lệ. Ví dụ, để có các giá trị hợp lệ của T = PC(r_t, t), thì lượng giao dịch t có thể nằm trong phạm vi hợp lệ [0, 2n-1]; và để có các giá trị hợp lệ của Y = PC(r_y, y), thì tiền trả lại y có thể nằm trong phạm vi hợp lệ [0, 2n-1]. Trong một phương án, nút A có thể sử dụng kỹ thuật chứng minh khối để tạo bằng chứng phạm vi RP liên quan đến (r_y, y, Y, r_t, t, T) cho các nút blockchain (ví dụ, các nút đồng thuận) để xác minh tại bước sau lượng giao dịch t và tiền trả lại y nằm trong phạm vi hợp lệ dựa trên bằng chứng phạm vi. Bằng chứng phạm vi có thể bao gồm, ví dụ, chữ ký Bulletproofs, chữ ký vòng Borromean, v.v.

Tại bước 202, nút A có thể gửi thông tin giao dịch đến nút B (ví dụ, thông qua kênh được bảo vệ ngoài blockchain). Thông tin giao dịch đã gửi có thể bao gồm, ví dụ, giá trị cam kết T = PC(r_t, t), giá trị cam kết Y = PC(r_y, y), mã hóa E(PK_B, r_t||t), mã hóa E(PK_A, r_y||y), bằng chứng phạm vi RP, v.v ... Giá trị cam kết Y = PC(r_y, y), mã hóa E(PK_A, r_y| y) và bằng chứng phạm vi RP có thể là tùy chọn vì nút B có thể không quan tâm đến tiền trả lại được gửi trở lại tài khoản A. Trong một số phương án, việc truyền qua kênh liên lạc ngoài blockchain có thể ngăn thông tin giao dịch được ghi vào blockchain và ngăn các nút khác ngoài nút bên gửi A và nút bên nhận B lấy

thông tin giao dịch. E(PK_A, r_y||y) có thể không cần gửi đến nút B, nhưng có thể cần thiết trong tương lai để người dùng A sử dụng tiền trả lại y vì tiền trả lại sẽ được hoàn trả lại cho tài khoản A.

Tại bước 203, nút B có thể xác minh số ngẫu nhiên r_t, lượng giao dịch t và giá trị cam kết T. Trong khi sử dụng, nút B có thể sử dụng khóa bí mật SK_B để giải mã mã hóa E(PK_B, r_t||t ) để thu nhận r_t||t. Từ r_t||t, nút B có thể thu nhận r_t và t, sau đó xác minh xem r_t và t có khớp với T = PC(r_t, t) không. Nghĩa là, nút B có thể xác minh xem giá trị cam kết T = PC(r_t, t) có đúng hay không dựa trên số ngẫu nhiên r_t và lượng giao dịch t theo thuật toán cam kết Pedersen. Nếu việc so khớp/xác minh thất bại, thì nút B có thể từ chối giao dịch giao dịch và nếu việc so khớp/xác minh thành công, thì nút B có thể ký giao dịch để trả lời nút A tại bước 204.

Tại bước 204, nút B có thể ký giao dịch bằng khóa bí mật SK_B của người dùng B để tạo chữ ký SIGB. Việc ký có thể tuân theo thuật toán chữ ký số (Digital Signature Algorithm, DSA) như thuật toán chữ ký số Elliptic Curve (Elliptic Curve Digital Signature Algorithm, ECDSA), theo đó người nhận chữ ký có thể xác minh chữ ký bằng khóa công khai ký của người ký để xác thực dữ liệu đã ký. Chữ ký SIGB chỉ ra rằng nút bên nhận B đồng ý với giao dịch.

Tại bước 205, nút B có thể truyền giao dịch được ký trở lại nút A với chữ ký SIGB.

Tại bước 206, nếu SIGB không được xác minh thành công, thì nút A có thể sẽ từ chối giao dịch. Nếu SIGB được xác minh thành công, thì nút A có thể ký giao dịch bằng khóa bí mật SK_A của người dùng A để tạo chữ ký SIGA. Tương tự, việc ký có thể tuân theo thuật toán chữ ký số (DSA). Trong một phương án, nút A có thể ký (E(PK_B, r_t||t); E(PK_A, r_y||y); Y; T; RP) bằng khóa bí mật SK_A của người dùng A để tạo chữ ký SIGA.

Tại bước 207, nút A có thể trình giao dịch đến blockchain, làm cho các nút blockchain xác minh giao dịch và xác định có nên bổ sung giao dịch vào blockchain hay không. Trong một phương án, nút A có thể trình giao dịch (E(PK_B, r_t||t); E(PK_A, r_y||y); Y; T; r'; RP; SIGA; SIGB) cho blockchain thông qua nút 1 để thực hiện giao dịch. r' = r_1 + … + r_k - r_t - r_y. Giao dịch có thể bao gồm các tham số bổ sung hoặc có thể không bao gồm tất cả các tham số được liệt kê. Giao dịch có thể được

phát đến một hoặc nhiều nút (ví dụ, các nút đồng thuận) trong blockchain để xác minh. Nếu xác minh thành công, thì giao dịch sẽ được bổ sung vào blockchain. Nếu xác minh thất bại, thì giao dịch sẽ bị từ chối khi bổ sung vào blockchain.

Tại các bước từ 208 đến 213, thì một hoặc nhiều nút (ví dụ, các nút đồng thuận) xác minh chữ ký, bằng chứng phạm vi và thông tin khác của giao dịch được trình. Nếu xác minh thất bại, thì các nút từ chối giao dịch. Nếu xác minh thành công, thì các nút chấp nhận giao dịch, cập nhật tài khoản của người dùng A và tài khoản của người dùng B một cách riêng biệt.

Trong một số phương án, để thực hiện giao dịch, thông tin giao dịch có thể được xác minh bởi các nút blockchain khác nhau. Thông tin giao dịch có thể bao gồm địa chỉ giao dịch TXID, chữ ký, đầu vào và đầu ra. TXID có thể bao gồm hàm băm của nội dung giao dịch. Chữ ký có thể bao gồm chữ ký khóa mã hóa của người gửi và người nhận. Đầu vào có thể bao gồm một địa chỉ tài khoản của người gửi trong blockchain, một hoặc nhiều tài sản được trích từ tài khoản blockchain của người gửi để giao dịch, v.v. Đầu ra có thể bao gồm một địa chỉ tài khoản của người nhận trong blockchain, loại tài sản người nhận (các tài sản người nhận), giá trị cam kết của tài sản người nhận (các tài sản người nhận), v.v ... Đầu vào và đầu ra có thể bao gồm thông tin được lập chỉ mục dưới dạng bảng. Trong một phần mềm, giá trị của NoteID có thể là TXID + chỉ số của tài sản trong đầu ra. Mã khóa công khai PK_A của người gửi có thể đóng vai trò là địa chỉ cho tài khoản A và khóa công khai PK_B của người nhận có thể dùng làm địa chỉ cho tài khoản B.

Trong một số phương án, một hoặc nhiều nút của blockchain có thể xác minh giao dịch được trình (E(PK_B, r_t||t); E(PK_A, r_y||y); Y; T; RP; SIGA; SIGB).

Tại bước 208, các nút có thể xác minh liệu giao dịch đã được thực hiện hay chưa nhờ sử dụng cơ chế chống chi tiêu kép hay cơ chế chống tấn công lại. Nếu giao dịch đã được thực hiện, thì các nút có thể từ chối giao dịch; nếu không thì, phương pháp có thể tiến hành bước 209.

Tại bước 209, các nút có thể kiểm tra chữ ký SIGA và SIGB (ví dụ, dựa trên khóa công khai của A và khóa công khai của B một cách lần lượt). Nếu chữ ký bất kỳ không chính xác, thì các nút có thể từ chối giao dịch; nếu không thì, phương pháp có thể tiến hành bước 210.

Tại bước tùy chọn 210, các nút có thể xác minh liệu các loại tài sản có phù hợp hay không. Ví dụ, các nút có thể xác minh xem các loại tài sản trong NoteType cho A_1 đến A_k có phù hợp với loại tài sản các loại tài sản) của lượng giao dịch t hay không. Nếu bất kỳ loại tài sản nào không nhất quán, thì các nút có thể từ chối giao dịch; nếu không thì, phương pháp có thể tiến hành bước 211. Trong một số phương án, loại tài sản ban đầu trong ví có thể đã được chuyển đổi sang loại khác dựa trên tỷ giá hối đoái và bước này có thể được bỏ qua.

Tại bước 211, các nút có thể kiểm tra bằng chứng phạm vi RP để phê duyệt giá trị của PC(r_t, t) và giá trị của PC(r_y, y). Trong một phương án, các nút có thể kiểm tra bằng chứng phạm vi RP để xác minh xem lượng giao dịch t có nhỏ hơn 0 hay không và tiền trả lại y không nhỏ hơn 0. Nếu xác minh thất bại, thì các nút có thể từ chối giao dịch; nếu không thì, phương pháp có thể tiến hành bước 212.

Tại bước 212, các nút có thể kiểm tra xem đầu vào và đầu ra của giao dịch có nhất quán không. Trong một phương án, r' có thể tương ứng với giá trị tài sản t' = a_1 + … + a_k - t - y dựa trên tính chất đồng hình, trong đó r' = r_1 + … + r_k - r_t - r_y. Vì các tài sản đầu vào là a_1 đến a_k và đầu ra là t + y, nên t' = 0 khi đầu vào và đầu ra đều nhất quán: a_1 + … a_k = t + y. Do đó, giá trị cam kết tương ứng với r' là PC(r', t') = r'×G + t'×H = r'G. Vì r' = r_1 + … + r_k - r_t - r_y, các nút có thể xác định xem đầu vào và đầu ra có bằng nhau hay không bằng cách xác minh xem r'G có bằng PC_1 + … + PC_k - T - Y tương ứng với r_1 + … + r_k - r_t - r_y. Nếu r'G bằng với PC_1 + … + PC_k - T - Y, thì các nút có thể xác định rằng các đầu vào và đầu ra của giao dịch là nhất quán và tiến hành bước tiếp theo; nếu không thì, các nút có thể xác định rằng đầu vào và đầu ra của giao dịch không nhất quán và từ chối giao dịch.

Tại bước 213, các nút có thể xác minh nếu nút A có tài sản (các tài sản) được trích cho giao dịch. Trong một phương án, các nút có thể thực hiện xác minh này dựa trên thông tin được lưu trữ trong blockchain, chẳng hạn như thông tin tương ứng với tài khoản A. Thông tin có thể bao gồm thông tin giao dịch trước đó của tất cả các tài sản. Do đó, các nút có thể xác định xem tài khoản A có tài sản giao dịch cho giao dịch hay không. Nếu xác định là không, thì các nút có thể sẽ từ chối giao dịch; nếu không thì, phương pháp có thể tiến hành bước 214.

Tại bước 214, các nút có thể cập nhật tài khoản A và tài khoản B. Ví dụ, các nút có thể xóa tài sản giao dịch của lượng t khỏi tài khoản A và bổ sung tài sản giao dịch của lượng t vào tài khoản B. Dựa trên tính chất đồng hình, vì Y = PC(r_y, y) và nút 1 biết r_y và có thể truy cập giá trị cam kết Y từ blockchain, nút 1 có thể giải mã Y để lấy giá trị tài sản y và bổ sung lượng tương tự cho tài khoản A. Nút 2 nhận được tại bước 202 số ngẫu nhiên r_t từ nút 1 và có thể lấy từ blockchain giá trị cam kết T. Do đó, nút 2 có thể giải mã T để lấy giá trị tài sản t và bổ sung vào tài khoản B.

Trong một ví dụ, sau khi cập nhật tài khoản A và tài khoản B, tài khoản A nhận được tiền trả lại y đối với các tài sản được trích A_1, A_2, …, A_k và nhận các tài sản chưa được trích A_k + 1, …, A_m và tài khoản B nhận lượng được giao dịch t và nhận tài sản ban đầu của nó B_1, B_2, …, B_n. Các tài sản trong tài khoản A và tài khoản B như sau:

Đối với tài khoản của A (tài khoản A), các tài sản được cập nhật sẽ được miêu tả như sau:

(Y=PC(r_y, y), E(PK_A, r_y||y)),

(A_k+1=PC(r_{a_k+1}, a_k+1), E(PK_A, r_{a_k+1}||a_k+1))

(A_k+2=PC(r_{a_k+2}, a_k+2), E(PK_A, r_{a_k+2}||a_k+2))

...

(A_m=PC(r_{a_m}, a_m), E(PK_A, r_{a_m}||a_m))

Đối với tài khoản của B (tài khoản B), các tài sản được cập nhật sẽ được miêu tả như sau:

(B_1=PC(r_{b_1}, b_1), E(PK_B, r_{b_1}||b_1)),

(B_2=PC(r_{b_2}, b_2), E(PK_B, r_{b_2}||b_2)),

...

(B_n=PC(r_{b_n}, b_n), E(PK_B, r_{b_n}||b_n)),

(T=PC(r_t, t), E(PK_B, r_t||t))

Mặc dù sáng chế này sử dụng nút A người dùng A và nút B/người dùng B để minh họa cho người gửi và người nhận một cách lần lượt, nhưng người gửi và người nhận có thể là cùng một nút/người dùng. Ví dụ, tiền trả lại y của giao dịch (tổng tài sản được trích trong tài khoản A trừ đi lượng giao dịch) có thể được gửi lại cho người gửi

giao dịch. Do đó, các bước khác nhau được thực hiện bởi nút B như được mô tả ở đây có thể được thực hiện thay thế bởi nút A.

Fig.3A minh họa một sơ đồ của một phương pháp làm ví dụ 300 để bảo vệ thông tin, theo các phương án khác nhau của sáng chế. Phương pháp 300 có thể được triển khai bởi một hoặc nhiều thành phần (ví dụ, nút A, nút 1, tổ hợp của nút A và nút 1) của hệ thống 100 trên Fig.1. Phương pháp 300 có thể được thực hiện bởi một hệ thống hoặc thiết bị (ví dụ, máy tính, máy chủ) bao gồm bộ xử lý và phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp (ví dụ, bộ nhớ) lưu trữ các lệnh được thực thi bởi bộ xử lý để làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) thực hiện phương pháp 300. Các hoạt động của phương pháp 300 được trình bày dưới đây nhằm mục đích minh họa. Tùy thuộc vào việc triển khai, phương pháp ví dụ 300 có thể bao gồm các bước bổ sung, loại bỏ một số bước hoặc các bước thay thế được thực hiện theo các trình tự khác nhau hoặc song song.

Khối 301 bao gồm: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t. Ví dụ, như được mô tả ở trên, T = PC(r_t, t). Trong một số phương án, sơ đồ cam kết bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù của giao dịch r_t và với lượng giao dịch t là giá trị được cam kết.

Khối 302 bao gồm: mã hoá tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch. Ví dụ, nút A có thể sử dụng khóa PK_B để mã hóa (r_t||t), mà mang đến sự mã hóa E(PK_B, r_t||t). Trong một số phương án, khoá công khai PK_B là khoá mã hóa bất đối xứng. Trong một số phương án, tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bao gồm sự móc nối của nhân tố mù của giao dịch r_t và lượng giao dịch t.

Khối 303 bao gồm: truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch (ví dụ, làm cho nút bên nhận xác minh giao dịch). Trong một số phương án, bước truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch bao gồm bước truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận, làm cho nút bên nhận: giải mã tổ hợp được mã hoá bằng khoá bí mật SK_B của

người nhận để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t; và xác minh giao dịch dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t. Xem bổ sung bước 203.

Trong một số phương án, bước làm cho nút bên nhận xác minh giao dịch dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t bao gồm bước làm cho nút bên nhận: để đáp lại việc xác định rằng giá trị cam kết T không khớp với sơ đồ cam kết của lượng giao dịch t dựa trên nhân tố mù của giao dịch r_t, thì từ chối giao dịch; và để đáp lại việc xác định rằng giá trị cam kết của giao dịch T khớp bằng sơ đồ cam kết của lượng giao dịch t dựa trên nhân tố mù của giao dịch r_t, thì phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_B của người nhận để tạo ra chữ ký của người nhận SIGB.

Trong một số phương án, trước khi (khối 304) truyền tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận, thì phương pháp còn bao gồm bước: cam kết tiền trả lại y của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết tiền trả lại Y, sơ đồ cam kết bao gồm ít nhất là nhân tố mù của tiền trả lại r_y , trong đó tiền trả lại y là một hoặc nhiều tài sản của người gửi của giao dịch mà được trích cho giao dịch nhỏ hơn lượng giao dịch t ; và mã hoá tổ hợp khác của nhân tố mù của tiền trả lại r_y và tiền trả lại y bằng khoá công khai PK_A của người gửi. Ví dụ, nút A có thể dùng khoá PK_A để mã hoá (r_y||y), mà mang đến sự mã hoá E(PK_A, r_y||y).

Trong một số phương án, phương pháp còn bao gồm bước: để đáp lại việc nhận được chữ ký của người nhận SIGN, thì phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_A của người gửi để tạo ra chữ ký của người gửi SIGA; và trình giao dịch bao gồm tổ hợp được mã hoá, một tổ hợp khác được mã hoá, giá trị cam kết của giao dịch T, giá trị cam kết tiền trả lại Y, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch. Phần chi tiết được mô tả ở phần trên với sự tham khảo đến các bước từ 208 đến 213.

Trong một số phương án, bước trình giao dịch bao gồm tổ hợp được mã hoá, một tổ hợp khác được mã hoá, giá trị cam kết của giao dịch T, giá trị cam kết tiền trả lại Y, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch bao gồm: bước

trình giao dịch bao gồm tổ hợp được mã hoá, một tổ hợp khác được mã hoá, giá trị cam kết của giao dịch T, giá trị cam kết tiền trả lại Y, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB đến một hoặc nhiều nút trong mạng blockchain, làm cho một hoặc nhiều nút, để đáp lại việc xác minh thành công giao dịch, xuất ra lượng giao dịch t cho người nhận, loại trừ một hoặc nhiều tài sản được trích cho giao dịch, và phát hành tiền trả lại y đến người gửi. Phần chi tiết được mô tả ở phần trên với sự tham khảo đến bước 214.

Fig.3B minh hoạ sơ đồ của phương pháp lấy làm ví dụ 400 để bảo vệ thông tin, theo các phương án của sáng chế. Phương pháp 400 có thể được triển khai bởi một hoặc nhiều thành phần (ví dụ, nút B, nút 2, tổ hợp của nút B và nút 2, v.v.) của hệ thống 100 trên Fig.1. Phương pháp 400 có thể được thực hiện bởi một hệ thống hoặc thiết bị (ví dụ, máy tính, máy chủ) bao gồm bộ xử lý và phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp (ví dụ, bộ nhớ) lưu trữ các lệnh được thực thi bởi bộ xử lý để làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) thực hiện phương pháp 400. Các hoạt động của phương pháp 400 được trình bày dưới đây nhằm mục đích minh họa. Tùy thuộc vào việc triển khai, phương pháp được lấy làm ví dụ 400 có thể bao gồm các bước bổ sung, hoặc loại bỏ một số bước hoặc thay thế một số bước được thực hiện theo trình tự khác nhau hoặc song song.

Khối 401 bao gồm: thu nhận tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t được mã hoá bằng khoá công khai PK_B của người nhận của giao dịch, và thu nhận giá trị cam kết của giao dịch T, trong đó: lượng giao dịch t được cam kết bằng sơ đồ cam kết bởi nút bên nhận được liên kết với người nhận của giao dịch để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t.

Khối 402 bao gồm: giải mã tổ hợp được thu nhận bằng khoá bí mật SK_B của người nhận của giao dịch để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t. Trong một số phương án, khoá công khai PK_B của người nhận và khoá bí mật SK_B của người nhận là các khoá mã hóa bất đối xứng.

Khối 403 bao gồm: xác minh giao dịch ít nhất dựa trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t và lượng giao dịch t.

Thay thế cho việc mã hóa kết hợp (r_t, t) như (r_t||t) tại nút A, nút A có thể truyền (r_t, t) đến nút B, làm cho nút B mã hóa tổ hợp (r_t, t), như được mô tả dưới đây với sự tham khảo đến Fig.4A và Fig.4B. Các bước và mô tả khác trên Fig.1 đến Fig.3B có thể áp dụng tương tự cho Fig.4A và Fig.4B.

Fig.4A minh hoạ minh hoạ sơ đồ của phương pháp lấy làm ví dụ 440 để bảo vệ thông tin, theo các phương án của sáng chế. Phương pháp 440 có thể được triển khai bởi một hoặc nhiều thành phần (ví dụ, nút A, nút 1, tổ hợp của nút A và nút 1) của hệ thống 100 trên Fig.1. Phương pháp 440 có thể được thực hiện bởi một hệ thống hoặc thiết bị (ví dụ, máy tính, máy chủ) bao gồm bộ xử lý và phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp (ví dụ, bộ nhớ) lưu trữ các lệnh được thực thi bởi bộ xử lý để làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) thực hiện phương pháp 400. Các hoạt động của phương pháp 440 được trình bày dưới đây nhằm mục đích minh họa. Tùy thuộc vào việc triển khai, phương pháp được lấy làm ví dụ 440 có thể bao gồm các bước bổ sung, hoặc loại bỏ một số bước hoặc thay thế một số bước được thực hiện theo trình tự khác nhau hoặc song song.

Khối 441 bao gồm: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t.

Khối 442 bao gồm: gửi lượng giao dịch t, nhân tố mù của giao dịch r_t, và giá trị cam kết của giao dịch T đến nút bên nhận được liên kết với người nhận của giao dịch để nút bên nhận xác minh giao dịch và mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận (ví dụ, làm cho nút bên nhận xác minh giao dịch và mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận). Ví dụ, nút B có thể xác minh liệu T=PC(r_t, t), và nút B có thể mã hoá tổ hợp với khoá công khai PK_A để thu nhận E(PK_B, r_t||t).

Khối 443 bao gồm: thu nhận tổ hợp được mã hoá (ví dụ, E(PK_B, r_t||t)) của nhân tố mù của giao dịch r_t và lượng giao dịch t từ nút bên nhận.

Khối 444 bao gồm: truyền tổ hợp được mã hoá và giá trị cam kết của giao dịch T đến các nút trong blockchain để các nút này xác minh giao dịch (ví dụ, làm cho các nút xác minh giao dịch).

Fig.4B minh hoạ sơ đồ của phương pháp lấy làm ví dụ 440 để bảo vệ thông tin, theo các phương án của sáng chế. Phương pháp 450 có thể được triển khai bởi một hoặc nhiều thành phần (ví dụ, nút B, nút 2, tổ hợp của nút B và nút 2, v.v.) của hệ thống 100 trên Fig.1. Phương pháp 450 có thể được thực hiện bởi một hệ thống hoặc thiết bị (ví dụ, máy tính, máy chủ) bao gồm bộ xử lý và phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp (ví dụ, bộ nhớ) lưu trữ các lệnh được thực thi bởi bộ xử lý để làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) thực hiện phương pháp 450. Các hoạt động của phương pháp 450 được trình bày dưới đây nhằm mục đích minh họa. Tùy thuộc vào việc triển khai, phương pháp được lấy làm ví dụ 450 có thể bao gồm các bước bổ sung, hoặc loại bỏ một số bước hoặc thay thế một số bước được thực hiện theo trình tự khác nhau hoặc song song.

Khối 451 bao gồm: thu nhận lượng giao dịch t của giao dịch, nhân tố mù của giao dịch r_t, và giá trị cam kết của giao dịch T.

Khối 452 bao gồm: xác minh giao dịch dựa trên lượng giao dịch thu được t, nhân tố mù của giao dịch thu được r_t, và giá trị cam kết của giao dịch thu được T.

Khối 453 bao gồm: để đáp lại việc xác minh thành công giao dịch, thì mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch để thu nhận tổ hợp được mã hoá (ví dụ, E(PK_B, r_t||t)).

Khối 454 bao gồm: truyền tổ hợp được mã hoá đến nút bên gửi được liên kết với người gửi của giao dịch.

Như được thể hiện, việc bảo vệ lượng giao dịch có thể được bảo vệ thông qua các cải tiến khác nhau của công nghệ điện toán. Ví dụ, cấu trúc tài khoản bao gồm một hoặc nhiều trường, chẳng hạn như trường đầu tiên được liên kết với cam kết Pedersen của giá trị tài sản (ví dụ, trường đầu tiên là PC(r_{a_i}, a_i), với i nằm trong khoảng từ 1 đến m) và trường thứ hai được liên kết với số ngẫu nhiên cho cam kết Pedersen và giá trị tài sản (ví dụ, trường thứ hai là E(...)). Trường thứ nhất và trường thứ hai cũng được sử dụng trong các bước giao dịch và được lưu trữ trong blockchain.

Trong một ví dụ khác, hệ thống khóa công khai-bí mật (mật mã bất đối xứng) của tài khoản được sử dụng lại để mã hóa số ngẫu nhiên của mỗi cam kết Pedersen và giá trị tài sản tương ứng và lưu trữ giao dịch bao gồm số ngẫu nhiên được mã hóa và giá trị tài sản trong blockchain. Cách này cản trở việc quản lý cục bộ các số ngẫu nhiên

như vậy và tăng cường bảo vệ dựa trên lưu trữ blockchain phân tán và nhất quán. Do đó, số ngẫu nhiên cho cam kết có thể được lưu trữ hiệu quả thông qua blockchain, mà không yêu cầu hệ thống mã hóa bổ sung.

Trong một ví dụ khác nữa, bằng chứng phạm vi được sử dụng để chứng minh rằng các tài sản có sẵn của giao dịch được cân bằng với tài sản mới và giao dịch và giá trị của mỗi tài sản mới nằm trong phạm vi hợp lý. Sau đó, các bên giao dịch có thể truyền số ngẫu nhiên đã cam kết và giá trị của tài sản mới cho người nhận thông qua kênh ngoài blockchain (off-blockchain) được bảo vệ để xác minh xem giá trị cam kết có khớp với giá trị của tài sản giao dịch không.

Như vậy, các số ngẫu nhiên của cam kết Pedersen có thể được quản lý thuận tiện, không có rủi ro do bị lỗi hỏng và không phát sinh bổ sung gánh nặng quản lý khoá. Do đó, sự bí mật của giao dịch có thể được bảo vệ triệt để và lượng giao dịch có thể được giữ bí mật.

Các kỹ thuật được mô tả trong sáng chế này được thực hiện bởi một hoặc nhiều thiết bị máy tính chuyên dụng. Các thiết bị máy tính chuyên dụng có thể là hệ thống máy tính để bàn, hệ thống máy chủ, hệ thống máy tính xách tay, thiết bị cầm tay, thiết bị mạng hoặc bất kỳ thiết bị hoặc tổ hợp thiết bị bất kỳ kết hợp giữa phần cứng và chương trình logic để thực hiện các kỹ thuật. Thiết bị điện toán (các thiết bị điện toán) thường được điều khiển và phối hợp bởi phần mềm hệ điều hành. Hệ điều hành thông thường kiểm soát và lên lịch các quy trình máy tính để thực thi, thực hiện quản lý bộ nhớ, cung cấp hệ thống tệp, mạng, dịch vụ I/O và cung cấp chức năng giao diện người dùng, như giao diện đồ họa người dùng (Graphical User Interface, GUI), trong số những thứ khác.

Fig.5 là sơ đồ khối minh hoạ một hệ thống máy tính 500 mà theo đó bất kỳ phương án nào được mô tả trong sáng chế này có thể được thực hiện. Hệ thống 500 có thể được triển khai trong bất kỳ nút nào được mô tả trong sáng chế này và được định cấu hình để thực hiện các bước tương ứng cho các phương pháp bảo vệ thông tin. Hệ thống máy tính 500 bao gồm bus 502 hoặc cơ chế giao tiếp khác để truyền thông tin, một hoặc nhiều bộ xử lý phần cứng 504 kết hợp với bus 502 để xử lý thông tin. Ví dụ, bộ xử lý phần cứng 504 có thể là một hoặc nhiều bộ vi xử lý thông thường.

Hệ thống máy tính 500 cũng bao gồm bộ nhớ chính 506, chẳng hạn như 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 bus 502 để lưu trữ thông tin và các lệnh được thực thi bởi bộ xử lý 504. Bộ nhớ chính 506 cũng 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 được bộ xử lý 504 thực hiện. Các lệnh này khi được lưu trữ trong phương tiện lưu trữ có thể truy cập được bởi bộ xử lý 504, làm cho hệ thống máy tính 500 trở thành máy chuyên dụng được tùy chỉnh để thực hiện các hoạt động được chỉ rõ trong các lệnh. Hệ thống máy tính 500 ngoài ra bao gồm bộ nhớ chỉ đọc (Read Only Memory, ROM) 508 hoặc thiết bị lưu trữ tĩnh khác được ghép nối với bus 502 để lưu trữ thông tin tĩnh và các lệnh cho bộ xử lý (các bộ xử lý) 504. Thiết bị lưu trữ 510, như đĩa từ, đĩa quang hoặc ổ USB (ổ Flash), v.v., được cung cấp và ghép nối với bus 502 để lưu trữ thông tin và các lệnh.

Hệ thống máy tính 500 có thể thực thi các kỹ thuật được mô tả trong sáng chế này bằng cách sử dụng mạch logic cứng được tùy chỉnh, một hoặc nhiều ASIC hoặc FPGA, phần sụn và/hoặc chương trình logic kết hợp với hệ thống máy tính hoặc hệ thống máy tính 500 là máy chuyên dụng . Theo một phương án, các hoạt động, phương pháp và quy trình được mô tả trong sáng chế này được thực hiện bởi hệ thống máy tính 500 để đáp lại với bộ xử lý 504 thực hiện một hoặc nhiều loạt của một hoặc nhiều lệnh được chứa trong bộ nhớ chính 506. Có thể đọc các lệnh như vậy vào bộ nhớ chính 506 từ một phương tiện lưu trữ khác, chẳng hạn như thiết bị lưu trữ 510. Việc thực hiện các loạt lệnh được chứa trong bộ nhớ chính 506 làm cho bộ xử lý (các bộ xử lý) 504 thực hiện các bước của quy trình được mô tả trong sáng chế này. Trong phương án thay thế, mạch có dây cứng có thể được sử dụng thay thế hoặc kết hợp với các lệnh phần mềm.

Bộ nhớ chính 506, ROM 508 và/hoặc bộ lưu trữ 510 có thể bao gồm phương tiện lưu trữ không chuyển tiếp . Thuật ngữ "phương tiện lưu trữ không chuyển tiếp ", và các thuật ngữ tương tự, như được sử dụng ở đây dùng để chỉ phương tiện lưu trữ dữ liệu và/hoặc các lệnh làm cho máy hoạt động theo kiểu cụ thể, phương tiện loại trừ tín hiệu tạm thời. Các phương tiện không chuyển tiếp như vậy có thể bao gồm các phương tiện không dễ thay đổi và/hoặc phương tiện dễ thay đổi. Ví dụ, phương tiện không dễ thay đổi bao gồm các đĩa quang hoặc từ, chẳng hạn như thiết bị lưu trữ 510. Phương tiện dễ thay đổi bao gồm bộ nhớ động, chẳng hạn như bộ nhớ chính 506. Các dạng phổ biến

của phương tiện không chuyển tiếp bao gồm, ví dụ, đĩa mềm, linh hoạt đĩa, đĩa cứng, ổ đĩa trạng thái rắn, băng từ hoặc bất kỳ phương tiện lưu trữ dữ liệu từ tính nào khác, CD-ROM, phương tiện lưu trữ dữ liệu quang học bất kỳ, phương tiện vật lý bất kỳ nào có các mẫu lỗ, RAM, PROM và EPROM, FLASH-EPROM, NVRAM, chip bộ nhớ bất kỳ hoặc hộp chứa nào khác và kết nối mạng các phiên bản của các phương tiện trên.

Hệ thống máy tính 500 cũng bao gồm giao diện mạng 518 được ghép nối với bus 502. Giao diện mạng 518 cung cấp các kết nối truyền dữ liệu hai chiều với một hoặc nhiều liên kết mạng được kết nối với một hoặc nhiều mạng cục bộ. Ví dụ, giao diện mạng 518 có thể là cạc mạng kỹ thuật số dịch vụ được tích hợp (Integrated Services Digital Network, ISDN), môđem cáp, môđem vệ tinh hoặc môđem để cung cấp kết nối giao tiếp dữ liệu với một loại đường dây điện thoại tương ứng. Một ví dụ khác, giao diện mạng 518 có thể là cạc mạng cục bộ (Local Area Network, LAN) để cung cấp kết nối giao tiếp dữ liệu với mạng LAN tương thích (hoặc thành phần WAN để giao tiếp với mạng LAN). Liên kết không dây cũng có thể được thực hiện. Trong phương án thực hiện bất kỳ, giao diện mạng 518 sẽ gửi và nhận tín hiệu điện, điện từ hoặc quang mang các luồng dữ liệu số biểu diễn các loại thông tin khác nhau.

Hệ thống máy tính 500 có thể gửi thông điệp và nhận dữ liệu, bao gồm mã chương trình, thông qua mạng, liên kết mạng và giao diện mạng 518. Trong ví dụ Internet, máy chủ có thể truyền mã được yêu cầu cho chương trình ứng dụng qua Internet, ISP, mạng cục bộ và giao diện mạng 518.

Mã nhận được có thể được thực thi bởi bộ xử lý (các bộ xử lý) 504 khi được nhận và/hoặc được lưu trữ trong thiết bị lưu trữ 510 hoặc bộ lưu trữ không chuyển tiếp khác để thực hiện sau này.

Mỗi quy trình, phương pháp và thuật toán được mô tả trong các phần trước có thể được biểu diễn và tự động hoàn toàn hoặc một phần bởi các môđun mã được thực thi bởi một hoặc nhiều hệ thống máy tính hoặc bộ xử lý máy tính bao gồm phần cứng máy tính. Các quy trình và thuật toán có thể được thực hiện một phần hoặc toàn bộ trong mạch dành riêng cho ứng dụng.

Các tính năng và quy trình khác nhau được mô tả ở trên có thể được sử dụng độc lập với nhau hoặc có thể được kết hợp theo nhiều cách khác nhau. Tất cả các kết hợp và kết hợp phụ có thể được coi là nằm trong phạm vi sáng chế này. Ngoài ra, một số

phương pháp hoặc khối quy trình nhất định có thể được bỏ qua trong một số phương án thực hiện. Các phương pháp và quy trình được mô tả trong sáng chế này cũng không giới hạn ở bất kỳ trình tự cụ thể nào và các khối hoặc trạng thái liên quan có thể được thực hiện trong các trình tự khác phù hợp. Ví dụ, các khối hoặc trạng thái được mô tả có thể được thực hiện theo thứ tự khác với các khối được bộc lộ cụ thể hoặc nhiều khối hoặc trạng thái có thể được kết hợp trong một khối hoặc trạng thái. Các khối hoặc trạng thái ví dụ có thể được thực hiện nối tiếp, song song hoặc theo một cách khác. Các khối hoặc trạng thái có thể được bổ sung vào hoặc xóa khỏi các phương án ví dụ được bộc lộ. Các hệ thống và thành phần ví dụ được mô tả trong sáng chế này có thể được cấu hình khác với mô tả. Ví dụ, các phần tử có thể được bổ sung vào, xóa khỏi hoặc sắp xếp lại so với các phương án ví dụ được bộc lộ.

Các hoạt động khác nhau của các phương pháp làm ví dụ được mô tả trong sáng chế này có thể được thực hiện, ít nhất là một phần, bằng một thuật toán. Thuật toán có thể được bao gồm trong mã chương trình hoặc lệnh được lưu trữ trong bộ nhớ (ví dụ, phương tiện lưu trữ có thể đọc được bởi máy tính không chuyển tiếp được mô tả ở trên). Thuật toán như vậy có thể bao gồm một thuật toán học máy. Trong một số phương án, một thuật toán học máy có thể không lập trình rõ ràng cho các máy tính thực hiện một chức năng, nhưng có thể học từ dữ liệu huấn luyện để tạo ra một mô hình dự đoán thực hiện chức năng đó.

Các hoạt động khác nhau của các phương pháp ví dụ được mô tả trong sáng chế này có thể được thực hiện, ít nhất là một phần, bởi một hoặc nhiều bộ xử lý được cấu hình tạm thời (ví dụ, bằng phần mềm) hoặc được định cấu hình vĩnh viễn để thực hiện các hoạt động liên quan. Dù được cấu hình tạm thời hay vĩnh viễn, các bộ xử lý như vậy có thể tạo thành các động cơ do bộ xử lý thực hiện hoạt động để thực hiện một hoặc nhiều hoạt động hoặc chức năng được mô tả trong sáng chế này.

Tương tự, các phương pháp được mô tả trong sáng chế này có thể được thực hiện ít nhất một phần bởi bộ xử lý, với một bộ xử lý hoặc bộ xử lý cụ thể là một ví dụ về phần cứng. Ví dụ, ít nhất một số hoạt động của một phương pháp có thể được thực hiện bởi một hoặc nhiều bộ xử lý hoặc thiết bị do bộ xử lý thực hiện. Ngoài ra, một hoặc nhiều bộ xử lý cũng có thể hoạt động để hỗ trợ hiệu năng của các hoạt động có liên quan trong môi trường điện toán đám mây trên nền tảng điện toán đám mây hoặc như một

phần mềm trên mạng như một dịch vụ (Software as a Service, SaaS). Ví dụ, ít nhất một số hoạt động có thể được thực hiện bởi một nhóm máy tính (như ví dụ về các máy bao gồm bộ xử lý), với các hoạt động này có thể truy cập qua mạng (ví dụ, Internet) và qua một hoặc nhiều giao diện thích hợp (ví dụ, giao diện chương trình ứng dụng (Application Program Interface, API)).

Hiệu năng của một số hoạt động có thể được phân bố giữa các bộ xử lý, không chỉ nằm trong một máy mà còn được triển khai trên một số máy. Trong một số phương án được làm ví dụ, bộ xử lý hoặc thiết bị do bộ xử lý thực hiện có thể được đặt ở một vị trí địa lý duy nhất (ví dụ, trong môi trường gia đình, môi trường văn phòng hoặc trang trại máy chủ). Trong các phương án ví dụ khác, bộ xử lý hoặc thiết bị do bộ xử lý thực hiện có thể được phân phối trên một số vị trí địa lý.

Trong toàn bộ sáng chế này, các biểu diễn số nhiều có thể thực hiện các thành phần, hoạt động hoặc cấu trúc được mô tả như một thực thể duy nhất. Mặc dù các hoạt động riêng lẻ của một hoặc nhiều phương pháp được minh họa và mô tả là các hoạt động riêng biệt, một hoặc nhiều hoạt động riêng lẻ có thể được thực hiện đồng thời và không có gì yêu cầu các hoạt động được thực hiện theo thứ tự được minh họa. Các cấu trúc và chức năng được trình bày dưới dạng các thành phần riêng biệt trong các cấu hình mẫu có thể được triển khai dưới dạng cấu trúc hoặc thành phần kết hợp. Tương tự, các cấu trúc và chức năng được trình bày dưới dạng một thành phần có thể được thực hiện như các thành phần riêng biệt. Những điều này và các biến thể, sửa đổi, bổ sung và cải tiến khác đều nằm trong phạm vi của sáng chế này.

Mặc dù tổng quan về vấn đề này đã được mô tả với sự tham khảo đến các phương án ví dụ cụ thể, các sửa đổi và thay đổi khác nhau có thể được thực hiện cho các phương án này mà không nằm ngoài phạm vi của các phương án của sáng chế này. Các phương án như vậy của vấn đề chủ đạo có thể được đề cập ở đây, dưới dạng riêng biệt hoặc kết hợp, theo thuật ngữ "sáng chế" chỉ là vì sự thuận tiện và không có ý định tự nguyện giới hạn phạm vi của sáng chế này đối với bất kỳ tiết lộ hoặc khái niệm nào nếu thực tế có nhiều hơn một tiết lộ. Mô tả chi tiết không nên được hiểu theo nghĩa hạn chế và phạm vi của các phương án khác nhau chỉ được xác định bởi các điểm yêu cầu bảo hộ, cùng với đầy đủ các tương đương mà các yêu cầu bảo hộ đó yêu cầu.

# YÊU CẦU BẢO HỘ

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

cam kết (301) lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết này bao gồm ít nhất là nhân tố mù của giao dịch r_t;

mã hoá (302) tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch;

truyền (303) giá trị cam kết của giao dịch T và tổ hợp được mã hoá này đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch;

nhận (205) chữ ký của người nhận SIGB biểu diễn rằng nút bên nhận đã phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_B của người nhận;

phê duyệt (206) giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_A của người gửi để tạo ra chữ ký của người gửi SIGA; và

trình (207) giao dịch được phê duyệt bởi người gửi và người nhận đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch này thông qua việc xác minh đồng thuận, giao dịch được phê duyệt bởi người gửi và người nhận bao gồm tổ hợp được mã hoá, giá trị cam kết của giao dịch T, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB.

2. Phương pháp theo điểm 1, trong đó khoá công khai PK_B là khoá mã hoá bất đối xứng.

3. Phương pháp theo điểm 1 hoặc 2, trong đó sơ đồ cam kết bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù của giao dịch r_t và với lượng giao dịch t là giá trị được cam kết.

4. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bao gồm sự móc nối của nhân tố mù của giao dịch r_t và lượng giao dịch t.

5. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó bước truyền (303) giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch bao gồm bước truyền (303) giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận, để làm cho nút bên nhận:

giải mã (402) tổ hợp được mã hoá này bằng khoá bí mật SK_B của người nhận để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t; và

xác minh (403) giao dịch này dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t này.

6. Phương pháp theo điểm 5, trong đó bước làm cho nút bên nhận xác minh giao dịch dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t bao gồm bước làm cho nút bên nhận:

để đáp lại việc xác định được rằng giá trị cam kết của giao dịch T không khớp với sơ đồ cam kết của lượng giao dịch t dựa trên nhân tố mù của giao dịch r_t, thì từ chối giao dịch; và

để đáp lại việc xác định được rằng giá trị cam kết của giao dịch T khớp bằng sơ đồ cam kết của lượng giao dịch t dựa trên nhân tố mù của giao dịch r_t, thì phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_B của người nhận để tạo ra chữ ký của người nhận SIGB.

7. Phương pháp theo điểm 6, trong đó trước bước truyền (304) tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận, thì phương pháp này còn bao gồm các bước:

cam kết tiền trả lại y của giao dịch với hệ thống cam kết để thu nhận giá trị cam kết tiền trả lại Y, hệ thống cam kết này bao gồm ít nhất là nhân tố mù của tiền trả lại r_y, trong đó tiền trả lại y này là một hoặc nhiều tài sản của người gửi giao dịch mà được trích cho giao dịch trừ đi lượng giao dịch t; và

mã hoá tổ hợp khác của nhân tố mù của tiền trả lại r_y và tiền trả lại y này bằng khoá công khai PK_A của người gửi.

8. Phương pháp theo điểm 7, trong đó:

bước trình (207) giao dịch được phê duyệt bởi người gửi và người nhận đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch này thông qua việc xác minh đồng thuận bao gồm bước: trình (207) giao dịch bao gồm tổ hợp được mã hoá, tổ hợp khác đã được mã hoá, giá trị cam kết của giao dịch T, giá trị cam kết tiền trả lại Y, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch này, và theo cách tùy chọn, trong đó bước trình giao dịch bao gồm tổ hợp được mã hoá, tổ hợp khác đã được mã hoá, giá trị cam kết của giao dịch T, giá trị cam kết tiền trả lại Y, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch này bao gồm bước:

trình giao dịch bao gồm tổ hợp được mã hoá, tổ hợp khác đã được mã hoá, giá trị cam kết của giao dịch T, giá trị cam kết tiền trả lại Y, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB đến một hoặc nhiều nút trong mạng blockchain, để làm cho một hoặc nhiều nút này, để đáp lại việc xác minh giao dịch thành công, thì phát hành lượng giao dịch t đến người nhận, loại trừ một hoặc nhiều tài sản được trích cho giao dịch, và phát hành tiền trả lại y đến người gửi.

9. Phương tiện lưu trữ có thể đọc được bởi máy tính tính không chuyển tiếp (506) lưu trữ các lệnh để được thực thi bởi bộ xử lý (504) để làm cho bộ xử lý (504) thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 8.

10. Hệ thống (500) để bảo vệ thông tin, trong đó hệ thống này bao gồm bộ xử lý (504) và phương tiện lưu trữ có thể đọc được bởi máy tính tính không chuyển tiếp (506) được ghép nối đến bộ xử lý này, phương tiện lưu trữ (506) này lưu trữ các lệnh để được thực thi bởi bộ xử lý (504) để làm cho hệ thống (500) này thực hiện các hoạt động bao gồm:

cam kết (301) lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết này bao gồm ít nhất là nhân tố mù của giao dịch r_t;

mã hoá (302) tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t bằng khoá công khai PK_B của người nhận của giao dịch;

truyền (303) giá trị cam kết của giao dịch T và tổ hợp được mã hoá này đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch;

nhận (205) chữ ký của người nhận SIGB biểu diễn rằng nút bên nhận đã phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_B của người nhận;

phê duyệt (206) giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_A của người gửi để tạo ra chữ ký của người gửi SIGA; và

trình (207) giao dịch được phê duyệt bởi người gửi và người nhận đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch này thông qua việc xác minh đồng thuận, giao dịch được phê duyệt bởi người gửi và người nhận bao gồm tổ hợp được mã hoá, giá trị cam kết của giao dịch T, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB.

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

thu nhận (401) tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t được mã hoá bằng khoá công khai PK_B của người nhận của giao dịch, và thu nhận giá trị cam kết của giao dịch T, trong đó: lượng giao dịch t này được cam kết bằng sơ đồ cam kết bởi nút bên gửi được liên kết với người gửi giao dịch để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết này bao gồm ít nhất là nhân tố mù của giao dịch r_t;

giải mã (402) tổ hợp được thu nhận này bằng khoá bí mật SK_B của người nhận của giao dịch để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t;

xác minh (403) giao dịch này dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t này;

để đáp lại việc xác minh thành công giao dịch, thì phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_B, và truyền, đến nút bên gửi, chữ ký của người nhận SIGB biểu diễn rằng nút bên nhận đã phê duyệt giao dịch để người gửi phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_A của người gửi để tạo ra chữ ký của người gửi SIGA và trình giao dịch được phê duyệt bởi người gửi và người nhận đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch này thông qua việc xác minh đồng thuận, giao dịch được phê duyệt bởi người gửi và người nhận bao gồm tổ hợp được thu nhận, giá trị cam kết của giao dịch T, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB.

12. Phương pháp theo điểm 11, trong đó khoá công khai PK_B của người nhận và khoá bí mật SK_B của người nhận là các khoá mã hoá bất đối xứng.

13. Phương tiện lưu trữ có thể đọc được bởi máy tính tính không chuyển tiếp (506) lưu trữ các lệnh để được thực thi bởi bộ xử lý (504) để làm cho bộ xử lý (504) thực hiện các hoạt động bao gồm:

thu nhận (401) tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t được mã hoá bằng khoá công khai PK_B của người nhận của giao dịch, và thu nhận giá trị cam kết của giao dịch T, trong đó: lượng giao dịch t này được cam kết bằng sơ đồ cam

kết bởi nút bên gửi được liên kết với người gửi giao dịch để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết này bao gồm ít nhất là nhân tố mù của giao dịch r_t;

giải mã (402) tổ hợp được thu nhận này bằng khoá bí mật SK_B của người nhận của giao dịch để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t;

xác minh (403) giao dịch này dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t này;

để đáp lại việc xác minh thành công giao dịch, thì phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_B, và truyền, đến nút bên gửi, chữ ký của người nhận SIGB biểu diễn rằng nút bên nhận đã phê duyệt giao dịch để người gửi phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_A của người gửi để tạo ra chữ ký của người gửi SIGA và trình giao dịch được phê duyệt bởi người gửi và người nhận đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch này thông qua việc xác minh đồng thuận, giao dịch được phê duyệt bởi người gửi và người nhận bao gồm tổ hợp được thu nhận, giá trị cam kết của giao dịch T, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB.

14. Hệ thống (500) để bảo vệ thông tin, trong đó hệ thống này bao gồm bộ xử lý (504) và phương tiện lưu trữ có thể đọc được bởi máy tính tính không chuyển tiếp (506) được ghép nối đến bộ xử lý (504) này, phương tiện lưu trữ (506) này lưu trữ các lệnh để được thực thi bởi bộ xử lý (504) để làm cho hệ thống (500) này thực hiện các hoạt động bao gồm:

thu nhận (401) tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t được mã hoá bằng khoá công khai PK_B của người nhận của giao dịch, và thu nhận giá trị cam kết của giao dịch T, trong đó: lượng giao dịch t này được cam kết bằng sơ đồ cam kết bởi nút bên gửi được liên kết với người gửi giao dịch để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết này bao gồm ít nhất là nhân tố mù của giao dịch r_t;

giải mã (402) tổ hợp được thu nhận này bằng khoá bí mật SK_B của người nhận của giao dịch để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t;

xác minh (403) giao dịch này dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t, và lượng giao dịch t này;

để đáp lại việc xác minh thành công giao dịch, thì phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_B, và truyền, đến nút bên gửi, chữ ký của người nhận SIGB biểu diễn rằng nút bên nhận đã phê duyệt giao dịch để người gửi phê duyệt giao dịch bằng cách ký vào giao dịch bằng khoá bí mật SK_A của người gửi để tạo ra chữ ký của người gửi SIGA và trình giao dịch được phê duyệt bởi người gửi và người nhận đến một hoặc nhiều nút trong mạng blockchain để một hoặc nhiều nút đó xác minh giao dịch này thông qua việc xác minh đồng thuận, giao dịch được phê duyệt bởi người gửi và người nhận bao gồm tổ hợp được thu nhận x, giá trị cam kết của giao dịch T, chữ ký của người gửi SIGA, và chữ ký của người nhận SIGB.

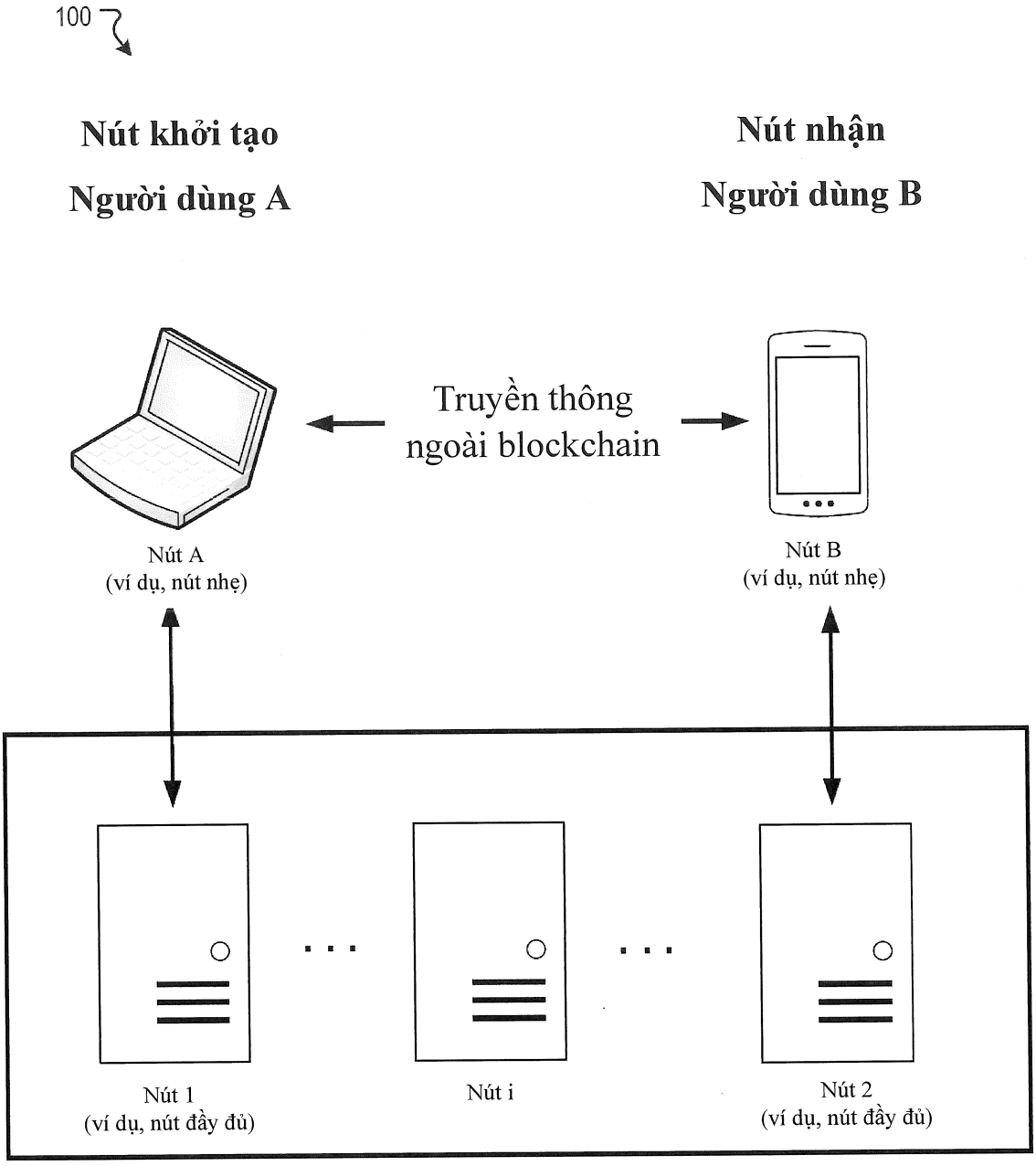
100
Nút khởi tạo
Người dùng A
Nút nhận
Người dùng B
Truyền thông
ngoài blockchain
Nút A
(ví dụ, nút nhẹ)
Nút B
(ví dụ, nút nhẹ)
Nút 1
(ví dụ, nút đầy đủ)
Nút i
Nút 2
(ví dụ, nút đầy đủ)

FIG. 1

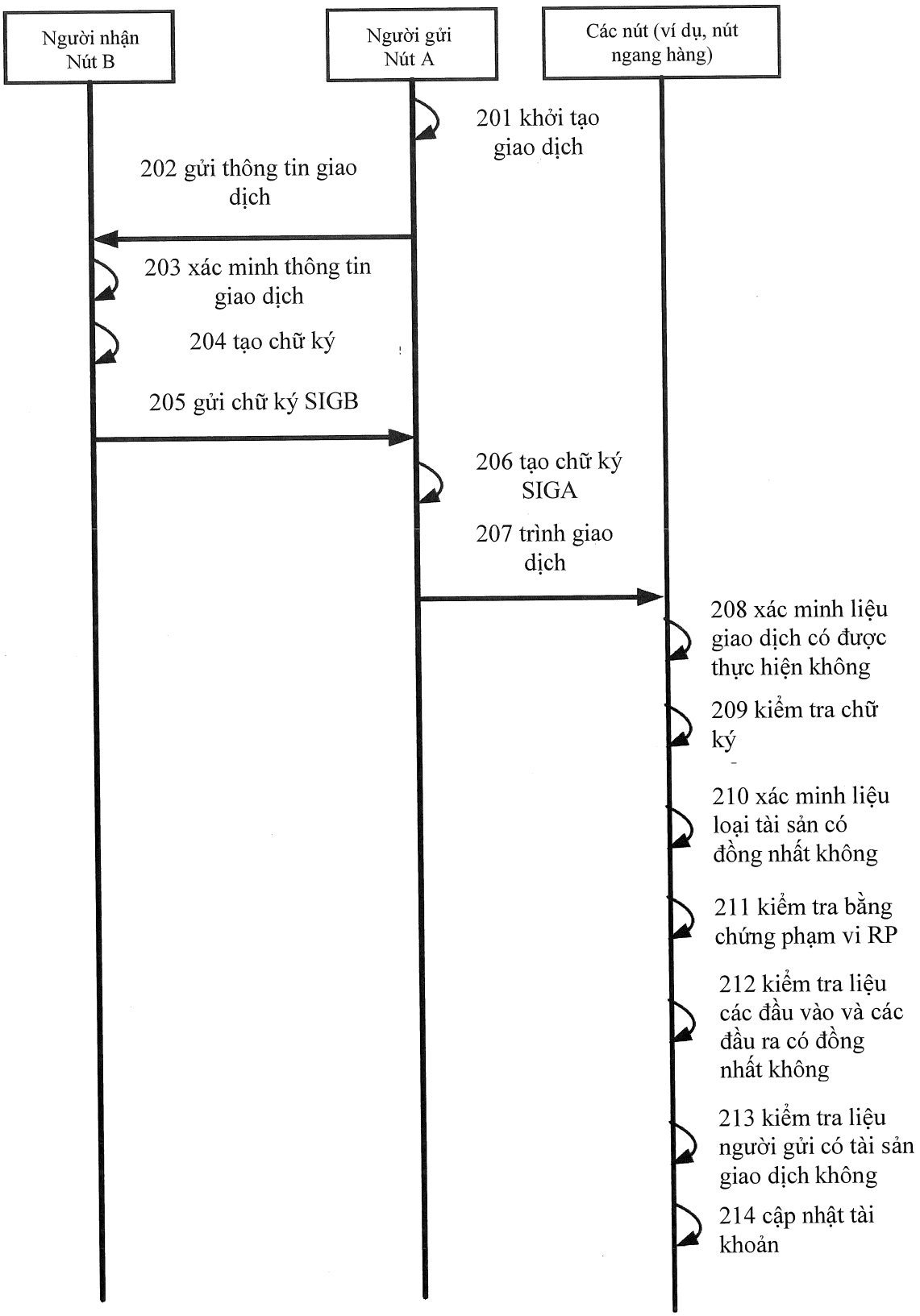
Người nhận
Nút B
Người gửi
Nút A
Các nút (ví dụ, nút ngang hàng)
201 khởi tạo giao dịch
202 gửi thông tin giao dịch
203 xác minh thông tin giao dịch
204 tạo chữ ký
205 gửi chữ ký SIGB
206 tạo chữ ký SIGA
207 trình giao dịch
208 xác minh liệu giao dịch có được thực hiện không
209 kiểm tra chữ ký
210 xác minh liệu loại tài sản có đồng nhất không
211 kiểm tra bằng chứng phạm vi RP
212 kiểm tra liệu các đầu vào và các đầu ra có đồng nhất không
213 kiểm tra liệu người gửi có tài sản giao dịch không
214 cập nhật tài khoản

FIG. 2

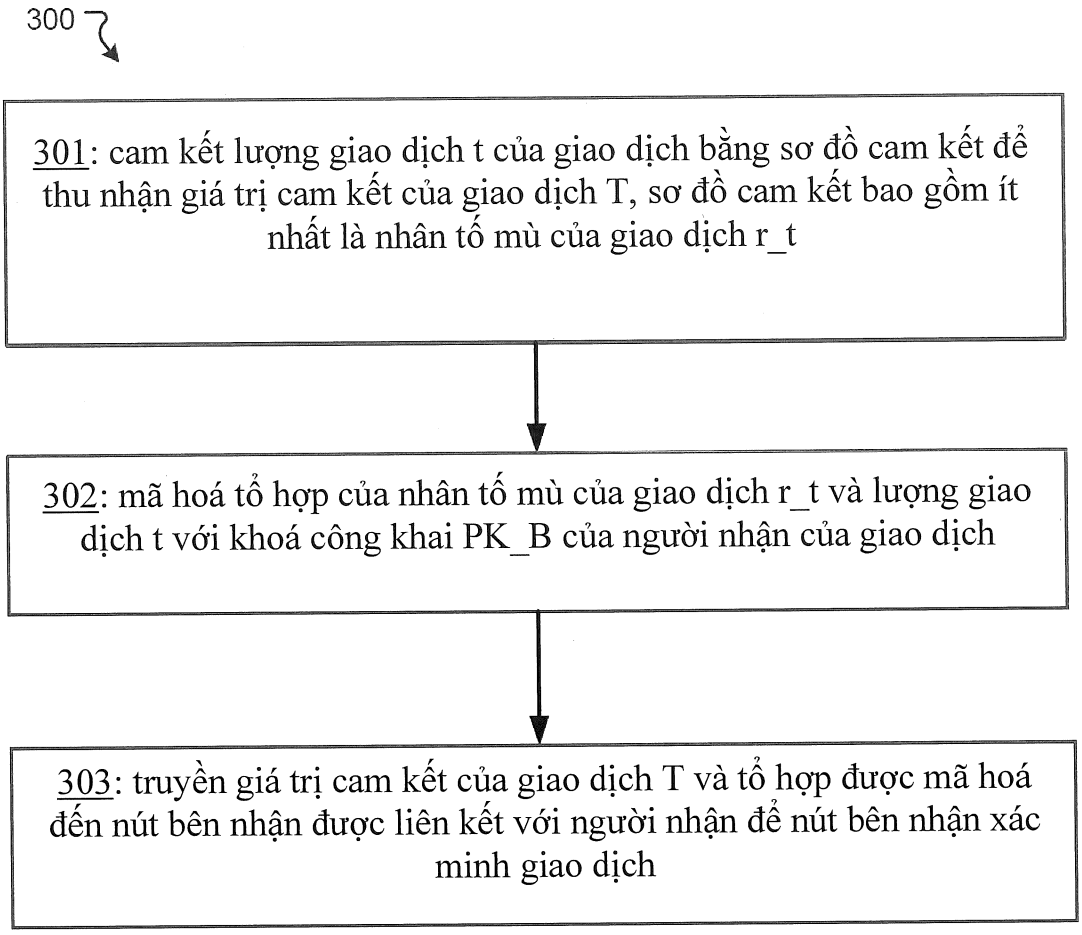
300
301: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t
302: mã hoá tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t với khoá công khai PK_B của người nhận của giao dịch
303: truyền giá trị cam kết của giao dịch T và tổ hợp được mã hoá đến nút bên nhận được liên kết với người nhận để nút bên nhận xác minh giao dịch

FIG. 3A

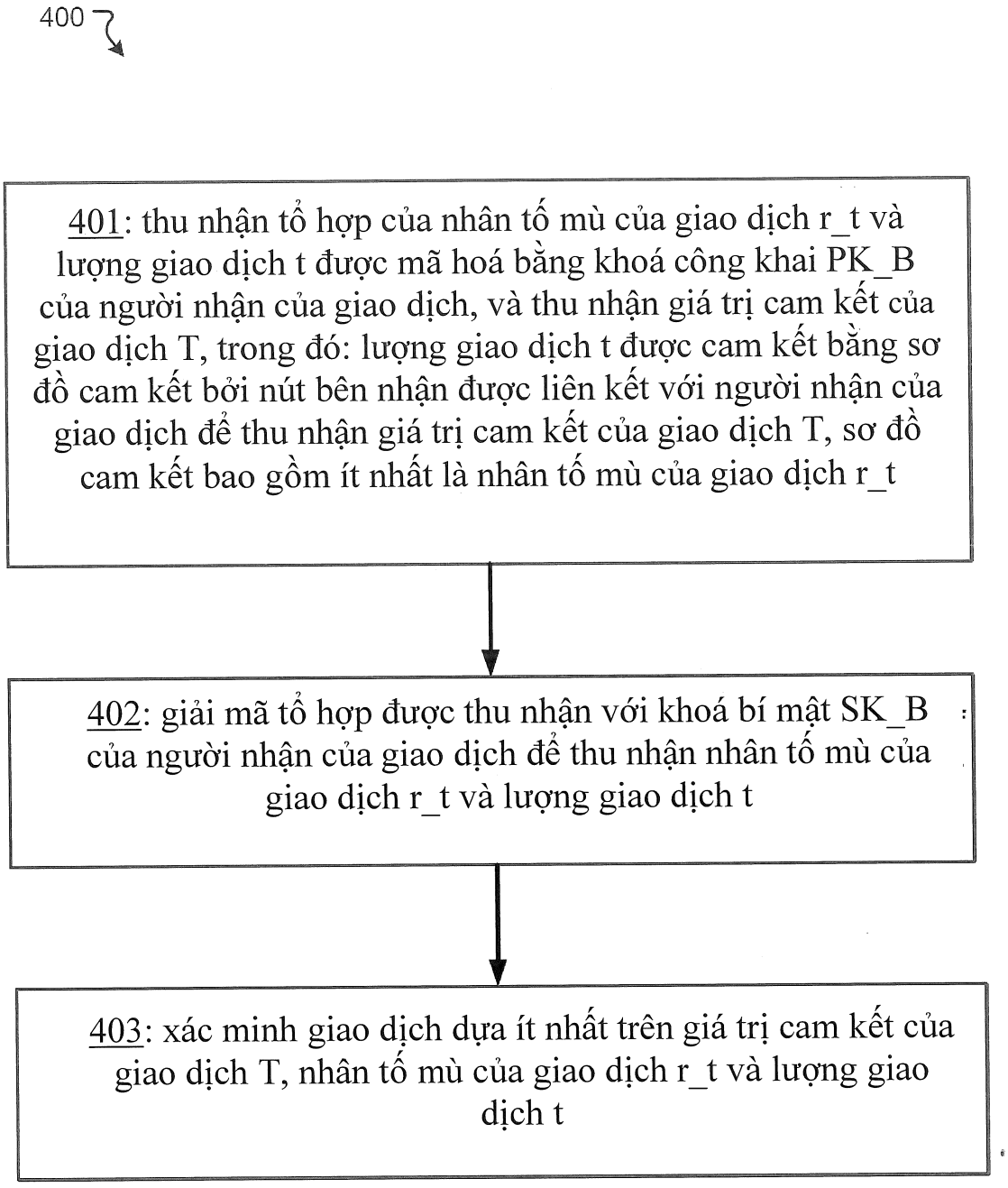
400
401: thu nhận tổ hợp của nhân tố mù của giao dịch r_t và lượng giao dịch t được mã hoá bằng khoá công khai PK_B của người nhận của giao dịch, và thu nhận giá trị cam kết của giao dịch T, trong đó: lượng giao dịch t được cam kết bằng sơ đồ cam kết bởi nút bên nhận được liên kết với người nhận của giao dịch để thu nhận giá trị cam kết của giao dịch T, sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t
402: giải mã tổ hợp được thu nhận với khoá bí mật SK_B của người nhận của giao dịch để thu nhận nhân tố mù của giao dịch r_t và lượng giao dịch t
403: xác minh giao dịch dựa ít nhất trên giá trị cam kết của giao dịch T, nhân tố mù của giao dịch r_t và lượng giao dịch t

FIG. 3B

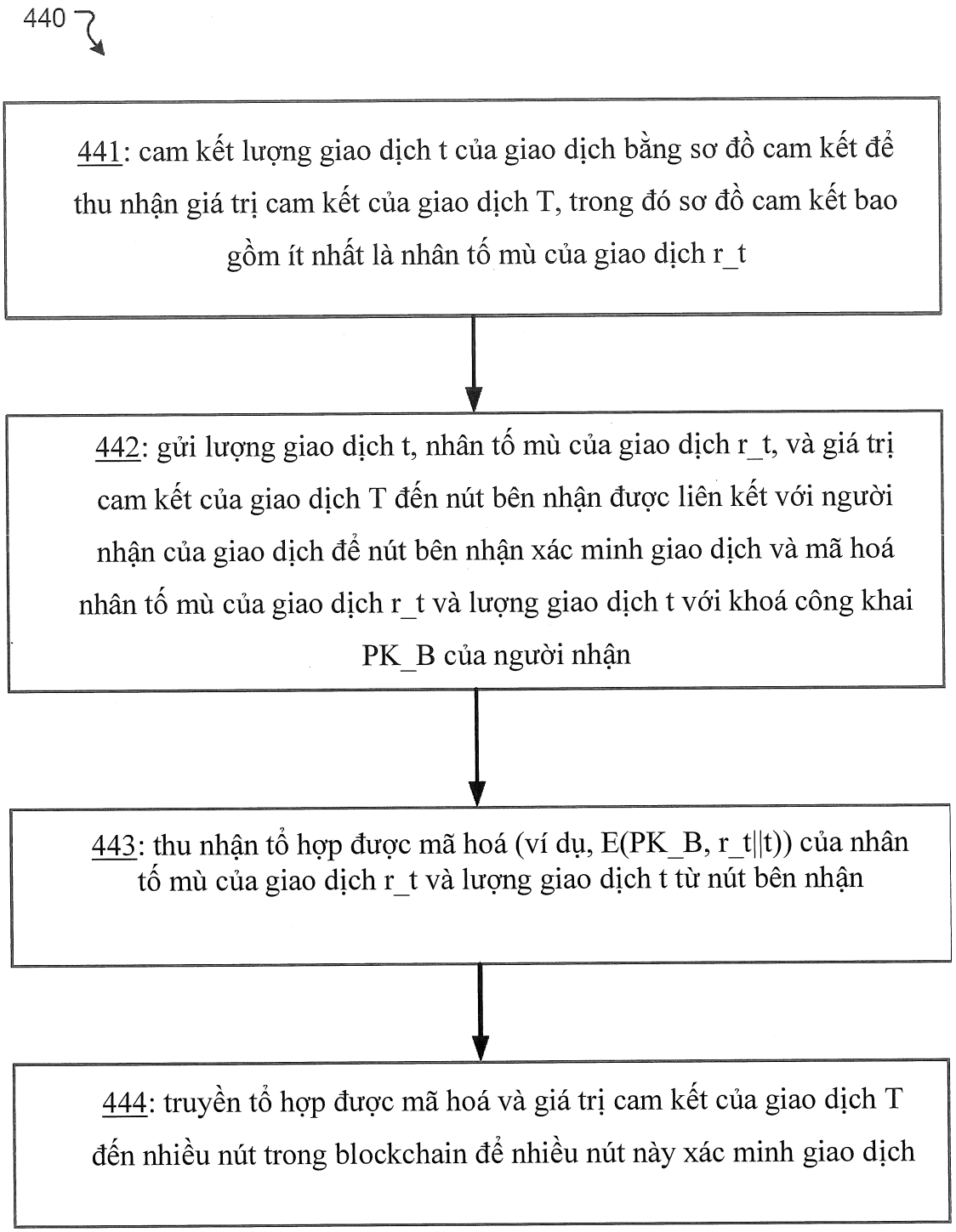
440
441: cam kết lượng giao dịch t của giao dịch bằng sơ đồ cam kết để thu nhận giá trị cam kết của giao dịch T, trong đó sơ đồ cam kết bao gồm ít nhất là nhân tố mù của giao dịch r_t
442: gửi lượng giao dịch t, nhân tố mù của giao dịch r_t, và giá trị cam kết của giao dịch T đến nút bên nhận được liên kết với người nhận của giao dịch để nút bên nhận xác minh giao dịch và mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t với khoá công khai PK_B của người nhận
443: thu nhận tổ hợp được mã hoá (ví dụ, E(PK_B, r_t||t)) của nhân tố mù của giao dịch r_t và lượng giao dịch t từ nút bên nhận
444: truyền tổ hợp được mã hoá và giá trị cam kết của giao dịch T đến nhiều nút trong blockchain để nhiều nút này xác minh giao dịch

FIG. 4A

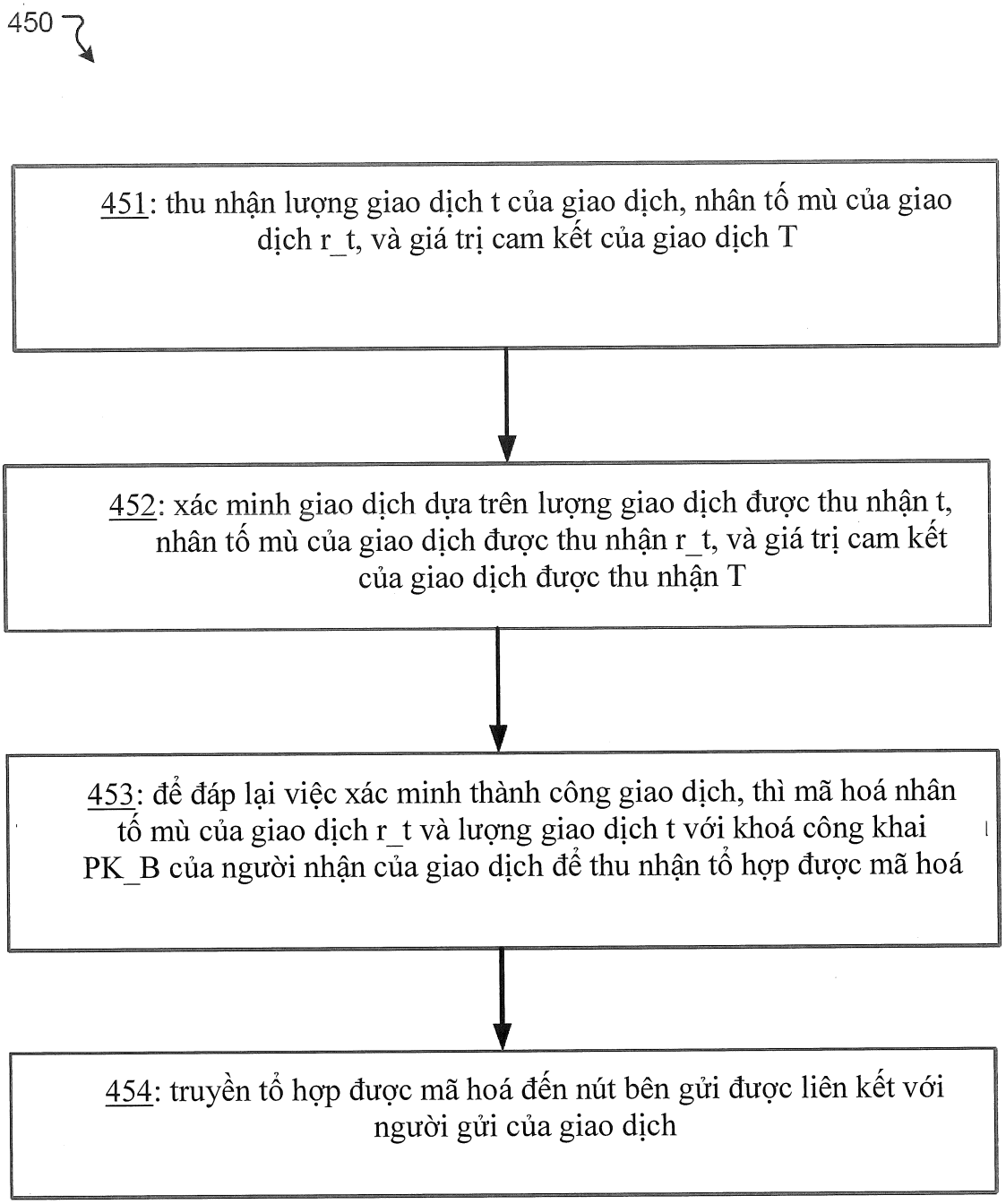
450
451: thu nhận lượng giao dịch t của giao dịch, nhân tố mù của giao dịch r_t, và giá trị cam kết của giao dịch T
452: xác minh giao dịch dựa trên lượng giao dịch được thu nhận t, nhân tố mù của giao dịch được thu nhận r_t, và giá trị cam kết của giao dịch được thu nhận T
453: để đáp lại việc xác minh thành công giao dịch, thì mã hoá nhân tố mù của giao dịch r_t và lượng giao dịch t với khoá công khai PK_B của người nhận của giao dịch để thu nhận tổ hợp được mã hoá
454: truyền tổ hợp được mã hoá đến nút bên gửi được liên kết với người gửi của giao dịch

FIG. 4B

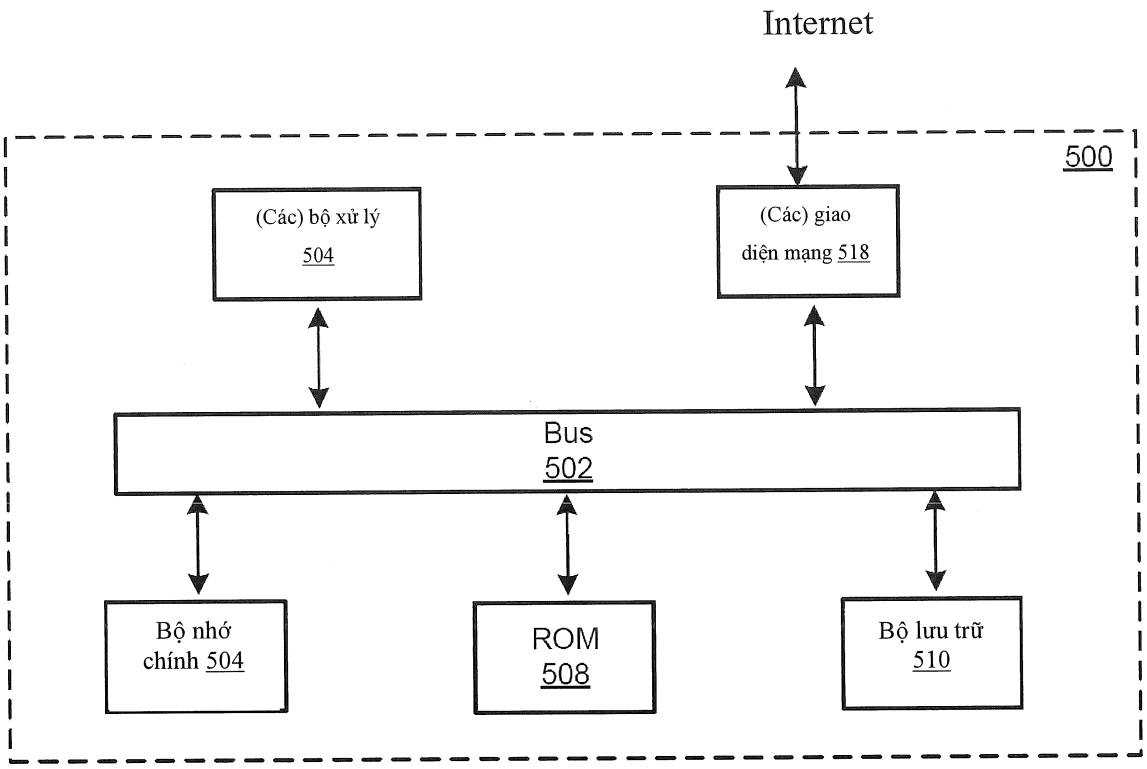
Internet
500
(Các) bộ xử lý
504
(Các) giao
diện mạng 518
Bus
502
Bộ nhớ
chính 504
ROM
508
Bộ lưu trữ
510

FIG. 5