(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) **1-0045917**

(51)[2006.01] **H04L 9/08**; H04L 9/32; H04L 29/06

(13) **B**

(21) 1-2019-01971

(22) 27/11/2018

(86) PCT/CN2018/117558 27/11/2018

(87) WO 2019/072277 18/04/2019

(45) 26/05/2025 446

(43) 25/07/2019 376A

(73) ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands

(72) MA, Huanyu (CN); ZHANG, Wenbin (CN); MA, Baoli (CN); LIU, Zheng (CN); CUI, Jiahui (CN).

(74) Công ty Luật TNHH T&G (TGVN)

(54) HỆ THỐNG VÀ PHƯƠNG PHÁP ĐỂ BẢO VỆ THÔNG TIN, VÀ VẬT GHI PHI CHUYỂN TIẾP, ĐỌC ĐƯỢC BỞI MÁY TÍNH

(21) 1-2019-01971

(57) Sáng chế đề cập tới phương pháp được thực hiện bởi máy tính để bảo vệ thông tin bao gồm các bước: cam kết lượng giao dịch của giao dịch với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch, cam kết thay đổi của giao dịch với sơ đồ cam kết thứ hai để thu được trị số cam kết thay đổi, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch, và sơ đồ cam kết thứ hai bao gồm nhân tố mù thay đổi; mã hóa tổ hợp thứ nhất của nhân tố mù thay đổi và thay đổi với chìa khóa thứ nhất; truyền nhân tố mù giao dịch, lượng giao dịch, và trị số cam kết giao dịch tới nút nhận được kết hợp với người nhận cho nút nhận để xác thực giao dịch; đáp ứng lại với việc người nhận xác thực thành công giao dịch, thu được tổ hợp thứ hai được mã hóa của nhân tố mù giao dịch và lượng giao dịch được mã hóa với chìa khóa thứ hai. Sáng chế còn đề cập tới hệ thống để bảo vệ thông tin, và vật ghi phi chuyển tiếp, đọc được bởi máy tính.

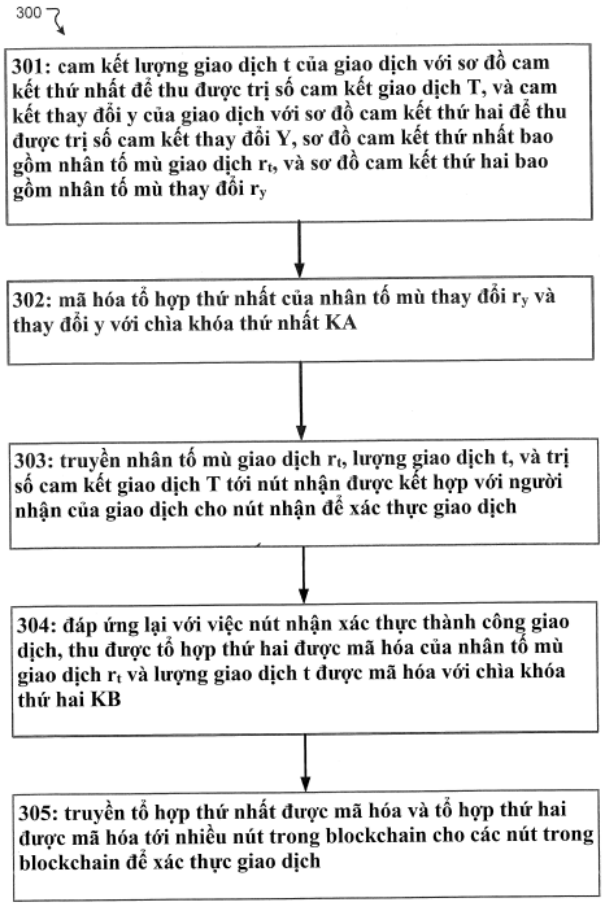

FIG. 3

Lĩnh vực kỹ thuật được đề cập

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

Tình trạng kỹ thuật của sáng chế

Sự riêng tự là quan trọng với việc liên lạc và chuyển dữ liệu giữa các người sử dụng. Nếu không có sự bảo vệ, người sử dụng sẽ phải chịu rủi ro về mất cắp danh tính, việc chuyển bất hợp pháp hoặc các tổn thất tiềm tàng khác. Rủi ro trở nên lớn hơn khi việc truyền thông và việc chuyển được thực hiện trực tiếp, do việc truy cập tự do của thông tin trực tuyến.

Bản chất kỹ thuật của sáng chế

Các phương án thực hiện khác nhau của sáng chế đề xuất các hệ thống, các phương pháp, và vật ghi phi chuyển tiếp đọc được bởi máy tính để bảo vệ thông tin.

Theo một khía cạnh, phương pháp được thực hiện bởi máy tính để bảo vệ thông tin bao gồm: cam kết lượng giao dịch t của giao dịch với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, và cam kết thay đổi y của giao dịch với sơ đồ cam kết thứ hai để thu được trị số cam kết thay đổi Y, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t, và sơ đồ cam kết thứ hai bao gồm nhân tố mù thay đổi r_y; mã hóa tổ hợp thứ nhất của nhân tố mù thay đổi r_y và thay đổi y với chìa khóa thứ nhất KA; truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch; đáp ứng lại với việc nút nhận xác thực thành công giao dịch, thu được tổ hợp thứ hai được mã hóa của nhân tố mù giao dịch r_t và lượng giao dịch t được mã hóa với chìa khóa thứ hai KB; và truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối (blockchain) cho các nút trong chuỗi khối để xác thực giao dịch.

Theo một số phương án thực hiện, sơ đồ cam kết thứ nhất bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù giao dịch r_t và với lượng giao dịch t đang là trị số được cam kết tương ứng; và sơ đồ cam kết thứ hai bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù thay đổi r_y và với thay đổi y đang là trị số được cam kết tương ứng.

Theo một số phương án thực hiện, bước truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch bao gồm: truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch, làm cho nút nhận để xác thực xem nếu trị số cam kết giao dịch T là bằng với sơ đồ cam kết thứ nhất cam kết lượng giao dịch t với nhân tố mù giao dịch r_t.

Theo một số phương án thực hiện, bước thu được tổ hợp thứ hai được mã hóa bao gồm việc nhận từ nút nhận tổ hợp thứ hai được mã hóa và chữ ký SIGB được kết hợp với tổ hợp thứ hai được mã hóa và trị số cam kết giao dịch T.

Theo một số phương án thực hiện, lượng giao dịch t được rút từ một hoặc nhiều tài sản A_1, A_2, …, A_k của người gửi của giao dịch; mỗi tài sản trong các tài sản được kết hợp với (1) cam kết Pedersen dựa ít nhất trên nhân tố mù r_{ak} và trị số của từng tài sản và (2) việc mã hóa dựa ít nhất trên nhân tố mù r_{ak} và trị số của từng tài sản; và thay đổi y là khác biệt giữa lượng giao dịch t và các tài sản được rút.

Theo một số phương án thực hiện, trước bước truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối, phương pháp còn bao gồm bước: xác thực chữ ký SIGB; và đáp ứng lại việc xác thực thành công chữ ký SIGB, sinh ra chữ ký SIGA được kết hợp với các tài sản A_1, A_2, …, A_k, tổ hợp thứ nhất, tổ hợp thứ hai, trị số cam kết giao dịch T, trị số cam kết thay đổi Y, và khác biệt giữa tổng của các nhân tố mù tương ứng với các tài sản A_1, A_2, …, A_k và tổng của nhân tố mù giao dịch r_t và nhân tố mù thay đổi r_y.

Theo một số phương án thực hiện, bước truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối bao gồm: truyền các tài sản A_1, A_2, …, A_k, tổ hợp thứ nhất, tổ hợp thứ hai, trị số cam kết giao dịch T, trị số cam kết thay đổi Y, khác biệt giữa tổng của các nhân tố mù tương ứng với các tài sản A_1,

A_2, …, A_k và tổng của nhân tố mù giao dịch r_t và nhân tố mù thay đổi r_y, chữ ký SIGA, và chữ ký SIGB tới nhiều nút trong chuỗi khối.

Theo một số phương án thực hiện, bước truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối cho các nút trong chuỗi khối để xác thực giao dịch bao gồm: truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối, làm cho các nút trong chuỗi khối, đáp ứng lại việc xác thực thành công giao dịch, đưa ra lượng giao dịch t tới người nhận, loại bỏ các tài sản A_1, A_2, …, A_k, và đưa ra thay đổi y tới người gửi.

Theo khía cạnh khác, vật ghi phi chuyển tiếp, đọc được bởi máy tính lưu các lệnh mà, khi được thực thi bởi bộ xử lý, sẽ làm cho bộ xử lý thực hiện các thao tác bao gồm: cam kết lượng giao dịch t của giao dịch với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, và cam kết thay đổi y của giao dịch với sơ đồ cam kết thứ hai để thu được trị số cam kết thay đổi Y, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t, và sơ đồ cam kết thứ hai bao gồm nhân tố mù thay đổi r_y; mã hóa tổ hợp thứ nhất của nhân tố mù thay đổi r_y và thay đổi y với chìa khóa thứ nhất KA; truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch; đáp ứng lại với việc nút nhận xác thực thành công giao dịch, thu được tổ hợp thứ hai được mã hóa của nhân tố mù giao dịch r_t và lượng giao dịch t được mã hóa với chìa khóa thứ hai KB; và truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối cho các nút trong chuỗi khối để xác thực giao dịch.

Theo khía cạnh khác, hệ thống để bảo vệ thông tin bao gồm bộ xử lý và vật ghi phi chuyển tiếp, đọc được bởi máy tính được ghép nối tới bộ xử lý, vật ghi lưu các lệnh mà, khi được thực thi bởi bộ xử lý, sẽ làm cho hệ thống thực hiện các thao tác bao gồm: cam kết lượng giao dịch t của giao dịch với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, và cam kết thay đổi y của giao dịch với sơ đồ cam kết thứ hai để thu được trị số cam kết thay đổi Y, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t, và sơ đồ cam kết thứ hai bao gồm nhân tố mù thay đổi r_y; mã hóa tổ hợp thứ nhất của nhân tố mù thay đổi r_y và thay đổi y với chìa khóa thứ nhất KA; truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận

được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch; đáp ứng lại với việc nút nhận xác thực thành công giao dịch, thu được tổ hợp thứ hai được mã hóa của nhân tố mù giao dịch r_t và lượng giao dịch t được mã hóa với chìa khóa thứ hai KB; và truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối cho các nút trong chuỗi khối để xác thực giao dịch.

Theo khía cạnh khác, phương pháp được thực hiện bởi máy tính để bảo vệ thông tin bao gồm các bước: thu được nhân tố mù giao dịch r_t, lượng giao dịch t của giao dịch, và trị số cam kết giao dịch T từ nút người gửi được kết hợp với người gửi của giao dịch, trong đó: lượng giao dịch t được cam kết với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t; xác thực giao dịch dựa trên nhân tố mù giao dịch r_t thu được, lượng giao dịch t thu được của giao dịch, và trị số cam kết giao dịch T thu được; đáp ứng lại việc xác thực thành công giao dịch, mã hóa tổ hợp thứ hai của nhân tố mù giao dịch r_t và lượng giao dịch t với chìa khóa thứ hai KB; và truyền tổ hợp thứ hai được mã hóa tới nút người gửi.

Theo một số phương án thực hiện, bước xác thực giao dịch dựa trên nhân tố mù giao dịch r_t thu được, lượng giao dịch t thu được của giao dịch, và trị số cam kết giao dịch T thu được bao gồm xác thực nếu trị số cam kết giao dịch T thu được là bằng với sơ đồ cam kết thứ nhất cam kết lượng giao dịch t thu được với nhân tố mù giao dịch r_t thu được.

Theo một số phương án thực hiện, trước bước truyền tổ hợp thứ hai được mã hóa tới nút người gửi, phương pháp còn bao gồm bước sinh ra chữ ký SIGB được kết hợp với tổ hợp thứ hai được mã hóa và trị số cam kết giao dịch T; và truyền tổ hợp thứ hai được mã hóa tới nút người gửi bao gồm việc truyền tổ hợp thứ hai được mã hóa và chữ ký SIGB tới nút người gửi.

Theo khía cạnh khác, vật ghi phi chuyển tiếp, đọc được bởi máy tính lưu các lệnh mà, khi được thực thi bởi bộ xử lý, sẽ làm cho bộ xử lý thực hiện các thao tác bao gồm: thu được nhân tố mù giao dịch r_t, lượng giao dịch t của giao dịch, và trị số cam kết giao dịch T từ nút người gửi được kết hợp với người gửi của giao dịch, trong đó: lượng giao dịch t được cam kết với sơ đồ cam kết thứ nhất để thu được trị số cam kết

giao dịch T, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t; xác thực giao dịch dựa trên nhân tố mù giao dịch r_t thu được, lượng giao dịch t thu được của giao dịch, và trị số cam kết giao dịch T thu được; đáp ứng lại việc xác thực thành công giao dịch, mã hóa tổ hợp thứ hai của nhân tố mù giao dịch r_t và lượng giao dịch t với chìa khóa thứ hai KB; và truyền tổ hợp thứ hai được mã hóa tới nút người gửi.

Theo khía cạnh khác, hệ thống để bảo vệ thông tin bao gồm bộ xử lý và vật ghi phi chuyển tiếp, đọc được bởi máy tính được ghép nối tới bộ xử lý, vật ghi lưu các lệnh mà, khi được thực thi bởi bộ xử lý, sẽ làm cho hệ thống thực hiện các thao tác bao gồm: thu được nhân tố mù giao dịch r_t, lượng giao dịch t của giao dịch, và trị số cam kết giao dịch T từ nút người gửi được kết hợp với người gửi của giao dịch, trong đó: lượng giao dịch t được cam kết với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t; xác thực giao dịch dựa trên nhân tố mù giao dịch r_t thu được, lượng giao dịch t thu được của giao dịch, và trị số cam kết giao dịch T thu được; đáp ứng lại việc xác thực thành công giao dịch, mã hóa tổ hợp thứ hai của nhân tố mù giao dịch r_t và lượng giao dịch t với chìa khóa thứ hai KB; và truyền tổ hợp thứ hai được mã hóa tới nút người gửi.

Các dấu hiệu này cũng như các dấu hiệu khác của các hệ thống, phương pháp và vật ghi phi chuyển tiếp đọc được bởi máy tính, cũng như các phương pháp vận hành, và các chức năng của các phần tử cấu trúc liên quan và sự kết hợp của các phần, và tính kinh tế sản xuất, sẽ trở nên rõ ràng hơn khi xem xét phần mô tả sau đây và các điểm yêu cầu bảo hộ kèm theo với tham chiếu đến các hình vẽ kèm theo, tất cả tạo thành một phần của bản mô tả, trong đó các số tham chiếu giống nhau chỉ các phần tương ứng trên các hình vẽ khác nhau. Tuy nhiên, cần hiểu rằng các hình vẽ đó chỉ nhằm mục đích minh hoạ và mô tả chứ không nhằm giới hạn sáng chế.

Mô tả vắn tắt các hình vẽ

Các dấu hiệu cụ thể của các phương án thực hiện khác nhau của công nghệ này được chỉ ra một cách cụ thể trong các yêu cầu bảo hộ kèm theo. Để hiểu rõ hơn các dấu hiệu và các ưu điểm sẽ thu được nhờ việc tham khảo tới phần mô tả chi tiết các phương án thực hiện, trong đó các nguyên lý của sáng chế sẽ được sử dụng, và các hình vẽ kèm theo, trong đó:

Fig.1 minh họa hệ thống làm ví dụ để bảo vệ thông tin, theo các phương án thực hiện khác nhau.

Fig.2 minh họa các bước làm ví dụ của việc khởi tạo và xác thực giao dịch, theo các phương án thực hiện khác nhau.

Fig.3 minh họa lưu đồ của phương pháp để bảo vệ thông tin làm ví dụ, theo các phương án thực hiện khác nhau.

Fig.4 minh họa lưu đồ của phương pháp để bảo vệ thông tin làm ví dụ, theo các phương án thực hiện khác nhau.

Fig.5 minh họa giản đồ khối của hệ thống máy tính làm ví dụ mà các phương án thực hiện được mô tả ở đây có thể được áp dụng vào trong đó.

Mô tả chi tiết sáng chế

Chuỗi khối có thể được coi là cơ sở dữ liệu phi tập trung, thường được gọi là sổ cái phân tán, bởi vì sự hoạt động được thực hiện bởi các nút khác nhau (ví dụ, các thiết bị điện toán) trong mạng. Bất kỳ thông tin nào cũng có thể được ghi vào chuỗi khối và được lưu vào hoặc được đọc từ nó. Bất kỳ ai cũng có thể thiết lập máy chủ và tham gia vào mạng chuỗi khối để trở thành một nút. Nút bất kỳ có thể đóng góp công suất tính toán để duy trì chuỗi khối bằng cách thực hiện các tính toán phức tạp, như việc tính toán việc băm để thêm khối vào chuỗi khối hiện có, và khối được thêm vào có thể chứa nhiều loại dữ liệu hoặc thông tin. Nút đóng góp công suất tính toán cho khối được thêm có thể được thưởng thẻ bài (ví dụ, đơn vị tiền dạng số). Do chuỗi khối không có nút trung tâm nên từng nút là bằng nhau và giữ toàn bộ cơ sở dữ liệu chuỗi khối.

Các nút là, ví dụ, các thiết bị tính toán hoặc các hệ thống máy tính lớn trợ giúp mạng chuỗi khối và giữ nó chạy trơn tru. Có hai loại nút, các nút đầy đủ và các nút hạng nhẹ. Các nút đầy đủ giữ bản sao hoàn chỉnh của chuỗi khối. Các nút đầy đủ trên mạng chuỗi khối xác thực hợp lệ các giao dịch và các khối chúng nhận, và chuyển tiếp chúng tới các thành phần ngang hàng được kết nối để tạo việc xác nhận đồng thuận của các giao dịch. Mặt khác, các nút hạng nhẹ chỉ tải xuống một phần của chuỗi khối.

Ví dụ, các nút hạng nhẹ được sử dụng cho các giao dịch tiền dạng số. Nút hạng nhẹ sẽ giao tiếp với nút đầy đủ khi nó muốn giao dịch.

Thuộc tính phi tập trung hoá này có thể giúp ngăn chặn sự xuất hiện của trung tâm quản lý ở vị trí được kiểm soát. Ví dụ, việc duy trì bitcoin chuỗi khối được thực hiện bởi mạng gồm các nút giao tiếp của phần mềm bitcoin trong khu vực chạy. Phần bộc lộ này sử dụng một hoặc nhiều chuỗi khối hoặc các tiền kỹ thuật số, như bitcoin và Ethereum, làm ví dụ. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ hiểu rằng các giải pháp kỹ thuật được bộc lộ trong phần mô tả này có thể sử dụng hoặc áp dụng tới các loại chuỗi khối và tiền kỹ thuật số khác. Tức là, thay cho các ngân hàng, các cơ quan, hoặc các đơn vị quản lý hành chính theo cách truyền thống, là nhiều thành phần trung gian tồn tại dưới dạng các máy tính chủ chạy phần mềm bitcoin. Các máy tính chủ này tạo thành mạng được kết nối qua Internet, trong đó bất kỳ ai cũng có thể gia nhập mạng. Các giao dịch được chứa bởi mạng có thể ở dạng: "người sử dụng A muốn gửi Z bitcoin đến người sử dụng B", trong đó các giao dịch này được truyền quảng bá đến mạng nhờ sử dụng các ứng dụng phần mềm đã sẵn có. Các máy tính chủ này có chức năng như các máy chủ bitcoin mà hoạt động được để xác nhận hợp lệ cho các giao dịch tài chính này, bổ sung bản ghi về chúng đến bản sao sổ cái của chúng, rồi sau đó truyền quảng bá những việc bổ sung vào sổ cái này đến các máy chủ khác của mạng.

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

Thông qua quá trình đào, các giao dịch, chẳng hạn các hoạt động chuyển nhượng tài sản, được xác thực và được các nút mạng bổ sung vào chuỗi khối đang tăng trưởng của chuỗi khối. Bằng cách đi qua toàn bộ chuỗi khối, hoạt động xác thực có thể bao gồm, ví dụ, việc xem liệu bên thanh toán có quyền tiếp cận tài sản chuyển nhượng hay không, việc xem tài sản đã được tiêu dùng trước đó chưa, việc xem lượng chuyển nhượng có đúng không, v.v.. Ví dụ, trong giao dịch giả tưởng (ví dụ, giao dịch của các bitcoin dưới mô hình đầu ra giao dịch chưa được sử dụng (UTXO - unspent transaction output), giao dịch của các đồng Ethereum dưới mô hình tài khoản/số dư) được thoát ra bởi người gửi, giao dịch được đề xuất có thể truyền quảng bá tới mạng chuỗi khối thông qua việc đào. Người đào cần phải kiểm tra xem giao dịch này có đủ điều kiện để thực hiện theo lịch sử chuỗi khối hay không. Nếu số dư trong ví của người gửi có đủ ngân quỹ theo lịch sử chuỗi khối hiện có, thì giao dịch được coi là hợp lệ và có thể được bổ sung vào khối. Khi đã được xác thực, thì các hoạt động chuyển nhượng tài sản đó có thể được bao gồm trong khối tiếp theo để bổ sung vào chuỗi khối.

Một khối là rất giống như một bản ghi của cơ sở dữ liệu. Mỗi lần ghi dữ liệu sẽ tạo ra một khối. Các khối này được liên kết và được bảo vệ bằng mật mã để trở thành các mạng được nối với nhau. Mỗi khối đều được nối với khối đằng trước, đó cũng là nguồn gốc của cái tên "chuỗi khối" (blockchain). Mỗi khối thường chứa phần băm mã hóa của khối đằng trước, thời điểm sinh ra, và dữ liệu thực tế. Ví dụ, mỗi khối đều chứa hai phần: phần đầu khối để ghi giá trị đặc trưng của khối hiện tại, và thân để ghi dữ liệu thực tế (ví dụ, dữ liệu giao dịch). Chuỗi các khối được liên kết thông qua các phần đầu khối. Mỗi phần đầu khối có thể chứa các giá trị đặc trưng, chẳng hạn phiên bản, phần băm của khối trước, gốc Merkle, dấu thời gian, đích độ khó, và nonce (phần dùng một lần). Phần băm của khối trước không chỉ chứa địa chỉ của khối trước, mà còn chứa phần băm của dữ liệu bên trong khối trước, từ đó làm cho các chuỗi khối không thể thay đổi được. Nonce là số mà khi được chứa thì sẽ tạo ra phần băm có một số lượng cụ thể các bit số không dẫn đầu.

Để đào, thì phần băm của các nội dung của khối mới sẽ được lấy bởi nút. Nonce (ví dụ, chuỗi ngẫu nhiên) được thêm vào phần băm này để thu được chuỗi mới. Chuỗi

mới này lại được băm. Sau đó, phần băm cuối cùng được so sánh với đích độ khó (ví dụ, mức độ), và được xác định xem phần băm cuối cùng này có thực sự nhỏ hơn đích độ khó này hay không. Nếu không, thì nonce này được thay đổi và tiến trình lặp lại. Nếu có, thì khối này được bổ sung vào chuỗi và sổ cái công khai được cập nhật và được báo về việc bổ sung này. Nút chịu trách nhiệm cho việc bổ sung thành công đó sẽ được thưởng các bitcoin, ví dụ, bằng cách bổ sung giao dịch phần thưởng đến chính nó vào khối mới (được gọi là quá trình sinh coinbase).

Tức là, đối với mọi đầu ra "Y", nếu k được chọn từ sự phân bố có entropy min cao, thì không thể tìm được đầu vào x sao cho H(k|x) = Y, trong đó K là nonce, x là phần băm của khối, Y là đích độ khó, và "|" biểu thị sự móc nối. Tính đến các phần băm mã hóa về cơ bản là ngẫu nhiên, theo nghĩa khi đầu ra của chúng là không thể được dự đoán từ những đầu vào của chúng, thì chỉ có một cách đã biết để tìm được nonce: thử từng số nguyên một, ví dụ 1, rồi 2, rồi 3, và tiếp tục như vậy, cách này có thể được gọi là cách thử vũ phu (brute-force). Số các số không dẫn càng lớn thì thời gian trung bình cần có để tìm được nonce Y được đòi hỏi càng dài. Theo một ví dụ, hệ thống bitcoin điều chỉnh theo cách không đổi số lượng các số không dẫn, sao cho thời gian trung bình để tìm được nonce là khoảng mười phút. Theo cách đó, khi các năng lực xử lý của phần cứng điện toán tăng lên theo thời gian, qua nhiều năm, thì giao thức bitcoin sẽ chỉ cần yêu cầu nhiều bit số không dẫn hơn để làm cho hoạt động đào luôn cần một khoảng thời gian khoảng mười phút để thực hiện.

Như đã mô tả, việc băm là nền móng quan trọng đối với chuỗi khối. Thuật toán băm có thể được hiểu là hàm nén các thông điệp có chiều dài bất kỳ thành thông điệp rút gọn có chiều dài cố định. Được sử dụng phổ biến hơn là MD5 và SHA. Theo một số phương án thực hiện, chiều dài phần băm của chuỗi khối là 256 bit, nghĩa là không quan tâm tới nội dung gốc là gì, số nhị phân 256-bit cuối cùng sẽ được tính toán. Và nó có thể được đảm bảo rằng việc băm tương ứng là duy nhất miễn là nội dung gốc là khác nhau. Ví dụ, việc băm của chuỗi "123" là a8fdc205a9f19cc1c7507a60c4f01b13d11d7fd0 (thập lục phân), có 256 bit khi được biến đổi thành nhị phân, và chỉ "123" có phần băm này. Thuật toán băm trong chuỗi khối là không thể đảo ngược, nghĩa là, việc tính toán tiến là dễ (từ "123" tới

a8fdc205a9f19cc1c7507a60c4f01b1c7507a60c4f01b13d11d7fd0), và việc tính toán ngược là không thể được thực hiện thậm chí nếu tất cả các nguồn tài nguyên tính toán đều được tận dụng. Do đó, phần băm của từng khối trong chuỗi khối là duy nhất.

Ngoài ra, nếu nội dung của khối thay đổi, thì việc băm của nó cũng sẽ thay đổi. Khối và việc băm là tương ứng một-một, và việc băm của từng khối được tính toán một cách cụ thể cho từng phần đầu khối. Nghĩa là, các trị số đặc trưng của các phần đầu khối được kết nối để tạo thành chuỗi dài, và sau đó việc băm được tính toán cho chuỗi. Ví dụ, "Hash = SHA256 (phần đầu khối)" là công thức tính việc băm khối, SHA256 là thuật toán băm chuỗi khối được áp dụng cho phần đầu khối. Việc băm được xác định duy nhất bởi phần đầu khối, và không phải là thân khối. Như được đề cập ở trên, phần đầu khối chứa nhiều nội dung, bao gồm việc băm của khối hiện tại, và việc băm của khối trước đó. Nó có nghĩa là nếu các nội dung của khối hiện tại thay đổi, hoặc nếu khối trước đó thay đổi thì nó sẽ gây ra việc thay đổi việc băm trong khối hiện tại. Nếu hacker thay đổi khối, việc băm của khối đó sẽ thay đổi. Để khối sau kết nối tới khối bị thay đổi, hacker phải thay đổi tất cả các khối sau đó theo thứ tự, do khối tiếp theo phải chứa việc băm của khối trước đó. Nếu không, khối bị biến đổi sẽ bị tách khỏi chuỗi khối. Do các lý do thiết kế, nên việc tính toán việc băm là tốn thời gian, và hầu như là không khả thi để biến đổi nhiều khối trong khoảng thời gian ngắn trừ khi hacker chiếm nhiều hơn 51% công suất tính toán của toàn bộ mạng lưới. Do đó, chuỗi khối đảm bảo độ tin cậy của riêng nó, và khi dữ liệu được viết, nó sẽ không thể bị can thiệp.

Khi người đào tìm thấy việc băm (nghĩa là, chữ ký hợp lệ hoặc giải pháp hợp lệ) cho khối mới, thì người đào sẽ truyền quảng bá chữ ký này tới tất cả các người đào khác (các nút của chuỗi khối). Các người đào khác, đến lượt họ sẽ xác thực nếu giải pháp tương ứng với vấn đề của khối của người gửi (nghĩa là, xác định nếu đầu vào băm thực sự tạo thành trong chữ ký này). Nếu giải pháp là hợp lệ, thì những người đào khác sẽ xác nhận giải pháp và đồng ý rằng khối mới có thể được thêm vào chuỗi khối. Do đó, đạt được sự đồng thuận của khối mới. Điều này còn được biết tới như là "bằng chứng của công việc". Khối mà đạt được sự đồng thuận cho nó hiện sẽ được thêm vào chuỗi khối và được truyền quảng bá tới tất cả các nút trên mạng lưới cùng với chữ ký

của nó. Các nút sẽ chấp nhận khối và lưu nó vào dữ liệu giao dịch của chúng cùng với các giao dịch bên trong khối tương ứng một cách chính xác với các số dư ví hiện tại (lịch sử giao dịch) tại thời điểm này. Mọi thời điểm khi khối mới được thêm trên đỉnh của khối này, việc thêm cũng sẽ tính như là "việc xác thực" khác cho các khối trước nó. Ví dụ, nếu giao dịch được chứa trong khối 502, và chuỗi khối dài 507 khối, nghĩa là giao dịch có năm xác nhận (tương ứng với các khối từ 507 đến 502). Giao dịch có càng nhiều xác nhận thì càng khó để những người tấn công thay đổi nó.

Theo một số phương án thực hiện, hệ thống tài sản chuỗi khối làm ví dụ sử dụng việc mã hóa chìa khóa chung, trong đó hai chìa khóa mã hóa, một chìa khóa chung và một chìa khóa riêng, được sinh ra. Chìa khóa chung có thể được xem như là số tài khoản, và chìa khóa riêng có thể được xem như là các chứng thực quyền sở hữu. Ví dụ, ví bitcoin là tập hợp của các chìa khóa chung và chìa khóa riêng. Quyền sở hữu của tài sản (ví dụ, tiền dạng số, tài sản tiền mặt, chứng khoán, cổ phần, khế ước) được kết hợp với địa chỉ tài sản cụ thể có thể được minh họa với hiểu biết về chìa khóa riêng thuộc về địa chỉ. Ví dụ, phần mềm ví bitcoin, đôi khi còn được đề cập tới như là "phần mềm khách hàng bitcoin", cho phép người sử dụng đã cho giao dịch các bitcoin. Chương trình ví sinh ra và lưu các chìa khóa riêng và liên lạc với thành phần ngang hàng trên mạng lưới bitcoin.

Trong các giao dịch chuỗi khối, thì những người trả tiền và những người được trả tiền được nhận dạng trong chuỗi khối bằng các chìa khóa mật mã công khai của họ. Ví dụ, phần lớn các hoạt động chuyển nhượng bitcoin đương thời là từ một chìa khoá công khai này sang chìa khoá công khai khác. Trên thực tế, các việc băm của các chìa khoá này được sử dụng trong chuỗi khối và được gọi là "các địa chỉ bitcoin". Về nguyên lý, nếu kẻ tấn công giả thiết là người S có thể lấy cắp tiền từ người A bằng cách chỉ cần bổ sung các giao dịch vào sổ cái chuỗi khối kiểu như "người A trả tiền cho người S là 100 bitcoin", nhờ sử dụng các địa chỉ bitcoin của những người dùng thay vì tên của họ. Giao thức bitcoin ngăn chặn loại trộm cắp này bằng cách yêu cầu mỗi lần chuyển nhượng phải được ký số bằng chìa khoá bí mật của người trả tiền, và chỉ có các chuyển nhượng đã được ký mới có thể được bổ sung vào sổ cái chuỗi khối. Vì người S không thể giả mạo chữ ký của người A, nên người S không thể lừa người

A bằng cách thêm mục nhập kiểu như "người A trả 200 bitcoin cho người S" vào chuỗi khối. Đồng thời, bất kỳ ai cũng có thể xác minh chữ ký của người A nhờ sử dụng chìa khoá công khai của người đó, và do đó, xác minh rằng người đó đã uỷ quyền giao dịch nào trong chuỗi khối mà trong đó người đó là người trả tiền.

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

Mô hình đầu ra giao dịch không được sử dụng (UTXO - unspent transaction output) và mô hình tài khoản/số dư là hai mô hình làm ví dụ cho việc áp dụng các giao dịch chuỗi khối. UTXO là mô hình đối tượng chuỗi khối. Trong UTXO, thì các tài sản được biểu diễn bằng các đầu ra của các giao dịch chuỗi khối mà chưa được tiêu dùng, mà có thể được dùng làm các đầu vào trong các giao dịch mới. Ví dụ, tài sản của người sử dụng A cần được chuyển nhượng của người dùng A có thể ở dạng UTXO. Để tiêu dùng (giao dịch) tài sản, thì người dùng A phải ký sổ bằng chìa khóa riêng. Bitcoin là một ví dụ về tiền kỹ thuật số sử dụng mô hình UTXO. Trong trường hợp giao dịch chuỗi khối hợp lệ, thì các đầu ra chưa tiêu dùng có thể được dùng để thực hiện các giao dịch khác. Theo một số phương án, chỉ những đầu ra chưa tiêu dùng mới có thể được sử dụng trong các giao dịch khác nữa, để ngăn chặn việc tiêu dùng đúp và sự gian lận. Vì lý do này, nên các đầu vào trên chuỗi khối sẽ được xoá khi giao dịch xuất hiện, trong khi, đồng thời, các đầu ra được tạo ra dưới dạng các UTXO. Các đầu

ra giao dịch chưa tiêu dùng này có thể được sử dụng (bởi những người nắm giữ các chìa khoá bí mật, ví dụ, những người có ví tiền kỹ thuật số) cho các giao dịch trong tương lai.

Mô hình tài khoản/số dư (hoặc được đề cập tới như là mô hình giao dịch dựa trên tài khoản), mặt khác, theo dõi số dư của từng tài khoản như là trạng thái toàn cục. Số dư của tài khoản được kiểm tra để đảm bảo rằng nó lớn hơn hoặc bằng với lượng giao dịch đang sử dụng. Một ví dụ về cách mô hình tài khoản/số dư làm việc trong Ethereum được đưa ra:

1. Alice tăng 5 ether qua việc đào mỏ. Nó được ghi trong hệ thống là Alice có 5 ether.

2. Alice muốn cho Bob 1 ether, do đó hệ thống đầu tiên trừ 1 từ tài khoản của Alice, do đó Alice hiện có 4 ether.

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

Việc giữ bản ghi cho Ethereum có thể giống như vậy, như trong ngân hàng. Sự tương tự là việc sử dụng ATM/thẻ ghi nợ. Ngân hàng theo dõi xem bao nhiêu tiền mà từng thẻ ghi nợ có, và khi Bob cần sử dụng tiền thì ngân hàng kiểm tra bản ghi của nó để đảm bảo rằng Bob có đủ số dư để phê chuẩn giao dịch.

Do chuỗi khối và các sổ cái tương tự khác là hoàn toàn công khai, nên tự bản thân chuỗi khối không có bảo vệ riêng tư. Bản chất công khai của mạng P2P nghĩa là, khi người sử dụng nó không được nhận dạng bởi tên thì các giao dịch liên kết tới các cá nhân và các công ty là khả thi. Ví dụ, trong các việc chuyển khoản xuyên biên giới hoặc trong chuỗi cung ứng, lượng giao dịch có mức độ trị số bảo vệ riêng tư cực kỳ cao, do với lượng thông tin giao dịch, có thể can thiệp vào vị trí cụ thể và các nhận diện của các bên giao dịch. Đối tượng giao dịch có thể bao gồm, ví dụ, tiền, thẻ bài, tiền dạng số, hợp đồng, chứng thư, bản ghi y tế, chi tiết khách hàng, chứng khoán, khế ước, cổ phần, hoặc tài sản bất kỳ khác có thể được mô tả ở dạng số. Mặc dù mô hình UTXO có thể tạo ra sự nặc danh cho các lượng giao dịch, ví dụ, qua chữ ký vòng trong Monero và Zcash mã hóa hiểu biết không, nhưng các lượng giao dịch vẫn không được

bảo vệ dưới mô hình tài khoản/số dư. Do đó, vấn đề kỹ thuật giải quyết bởi sáng chế này là làm thế nào để bảo gệ thông tin trực tuyến như là sự riêng tư của các lượng giao dịch. Các giao dịch này có thể là dưới mô hình tài khoản/số dư.

Một số công nghệ hiện có đề xuất việc sử dụng sơ đồ cam kết Pedersen để mã hóa lượng giao dịch và thay thế mô hình tài khoản/số dư. Dưới sơ đồ này, người gửi gửi lượng giao dịch và số ngẫu nhiên tương ứng với cam kết Pedersen của lượng giao dịch tới người được trả tiền qua kênh an toàn ngoài chuỗi khối. Người được trả tiền xác thực nếu số ngẫu nhiên khớp với cam kết giao dịch và thực hiện việc lưu tại chỗ. Ví dụ, dưới mô hình tài khoản/số dư, tài khoản có thể được xử lý như là ví (tài khoản) để giữ các tài sản được tích tụ nhưng không được hợp nhất. Mỗi tài sản có thể tương ứng với loại tài sản (ví dụ, tiền mã hóa (cryptocurrency)), và số dư của tài khoản là tổng các trị số tài sản. Thậm chí các tài sản cùng một loại cũng không được hợp nhất. Trong suốt giao dịch, người nhận của việc chuyển tài sản có thể được cụ thể hóa, và tài sản tương ứng có thể được loại bỏ khỏi ví để trả cho giao dịch. Các nút chuỗi khối xác thực ví trả có đủ tài sản (các tài sản) để đảm bảo giao dịch, và sau đó các nút xóa tài sản được truyền khỏi ví trả và thêm tài sản tương ứng vào ví người nhận.

Tuy nhiên, các hạn chế vẫn tồn tại cho sơ đồ này. Lượng giao dịch và số ngẫu nhiên được sinh ra bởi cam kết Pedersen là dữ liệu nhạy cảm-riêng tư. Các bên khác với các bên có liên quan tới giao dịch sẽ không có cơ hội để biết các trị số này. Do đó, thông tin này nên được mã hóa và được lưu, và được giải mã khi được sử dụng. Trị số được cam kết và số ngẫu nhiên là các thành phần cần thiết để sử dụng tài sản được giao dịch trong tương lai, nhưng dễ mất và khó để phục hồi cho cách thiếu an toàn, ổn định, và hiệu quả để lưu các số ngẫu nhiên một cách phù hợp. Ví dụ, sơ đồ của các công nghệ hiện tại yêu cầu người sử dụng duy trì việc lưu vĩnh viễn tại chỗ để quản lý các số ngẫu nhiên và các số dư văn bản gốc tương ứng với số dư tài khoản được mã hóa, và việc áp dụng việc quản lý là phức tạp. Tiếp theo, việc lưu trữ của các nhân tố mù (ví dụ, các số ngẫu nhiên) và các số dư văn bản gốc tương ứng với "tài sản Pedersen" trong nút cục bộ đơn là thiên về phía mất mát hoặc bị hỏng, trong khi việc lưu trữ dự phòng nhiều nút là khó để nhận diện do việc thay đổi thường xuyên của số dư tài khoản.

Các hệ thống và phương pháp được thể hiện trong bản mô tả này có thể khắc phục các hạn chế nêu trên và đạt được việc bảo vệ sự riêng tư mạnh mẽ cho các lượng giao dịch, các trị số tài sản, và các nhân tố mù trong các sơ đồ cam kết. Về phía này, các giao thức trao đổi thông tin mã hóa khác nhau có thể được sử dụng để mã hóa/giải mã các số ngẫu nhiên và các số dư văn bản gốc, do đó tạo nên việc quản lý thuận tiện. Tiếp theo, việc lưu trữ thông tin đã được mã hóa trong chuỗi khối đảm bảo rằng các lượng giao dịch, các trị số tài sản, và các nhân tố mù trong cá sơ đồ cam kết không dễ dàng bị mất hoặc bị can thiệp vào.

Theo một số phương án thực hiện, sơ đồ cam kết (ví dụ, cam kết Pedersen) có thể mã hóa trị số cụ thể a (ví dụ, lượng giao dịch, trị số tài sản, thông số chìa khóa) như sau:

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

trong đó r là nhân tố mù ngẫu nhiên (còn được đề cập tới như là thông số mù) tạo ra việc giấu, G và H là các bộ sinh/điểm cơ sở được đồng thuận chung của đường cong elip và có thể được chọn một cách ngẫu nhiên, sn là trị số của cam kết, C(sn) là điểm đường cong được sử dụng như là cam kết và được đưa chon bên đối, và H là điểm đường cong khác. Nghĩa là, G và H có thể là các thông số đã biết cho các nút. Việc sinh ra "không có gì" của H có thể được sinh ra bằng cách băm điểm gốc G với việc ánh xạ hàm băm từ điểm này tới điểm khác với H= Hash(G). H và G là các thông số chung của hệ thống đã cho (ví dụ, các điểm được sinh ra ngẫu nhiên trên đường cong elip). Mặc dù phần nêu trên đưa ra ví dụ về cam kết Pedersen ở dạng đường cong elip, nhưng các dạng khác của cam kết Pedersen hoặc các sơ đồ cam kết khác cũng có thể được sử dụng thay vào đó.

Sơ đồ cam kết duy trì tính an ninh của dữ liệu nhưng cam kết với dữ liệu sao cho nó không thể được thay đổi sau này bởi người gửi của dữ liệu. Nếu một bên chỉ biết trị số cam kết (ví dụ, Pc(a)), thì họ không thể xác định các trị số dữ liệu nằm dưới nào (ví dụ, a) đã được cam kết tới. Cả dữ liệu (ví dụ, a) và nhân tố mù (ví dụ, r) có thể được bộc lộ sau (ví dụ, bởi nút bộ phận khởi tạo), và người nhận (ví dụ, nút đồng thuận) của cam kết có thể chạy cam kết và xác thực rằng dữ liệu đã được cam kết khớp với dữ liệu đã được bộc lộ. Nhân tố mù có mặt do nếu không có nó, ai đó sẽ cố đoán dữ liệu.

Các sơ đồ cam kết là cách cho người gửi (bên cam kết) để cam kết trị số (ví dụ, a) sao cho trị số được cam kết vẫn được giữ riêng tư, nhưng có thể được bộc lộ tại thời điểm sau khi bên cam kết tiết lộ thông số cần thiết cho việc xử lý cam kết. Các sơ đồ cam kết mạnh có thể là cả việc giấu thông tin và việc liên kết tính toán. Việc giấu đề cập tới ghi chú mà trị số đã cho và việc cam kết của trị số Pc(a) đó nên là không thể liên quan. Nghĩa là, PC(a) không nên bộc lộ thông tin nào về a. Với PC(a), G, và H đã biết, hầu hết là không thể biết được a do số ngẫu nhiên r. Sơ đồ cam kết là liên kết nếu không có cách hợp lý nào mà hai trị số khác nhau có thể tạo thành trong cùng một cam kết. Cam kết Pedersen là việc giấu hoàn hảo và việc liên kết theo cách có tính toán dưới giả sử của thuật toán rời rạc. Tiếp theo, với r, G, H, và PC(a) đã biết, có khả năng để xác thực PC(a) bằng cách xác định nếu PC(a) = r×G + a×H.

Cam kết Pedersen có tính chất bổ sung: các cam kết có thể được thêm vào, và tổng của bộ các cam kết là giống như cam kết với tổng của dữ liệu (với bộ nhân tố mù như là tổng của các nhân tố mù): $PC(r_1, data_1) + PC(r_2, data_2) == PC(r_1+r_2, data_1+data_2)$; $PC(r_1, data_1) - PC(r_1, data_1) == 0$. Nói cách khác, cam kết bảo toàn việc thêm vào và tính chất giao hoán áp dụng, tức là, cam kết Pedersen là đồng hình bổ sung, trong đó, dữ liệu bên dưới có thể được thao tác theo cách toán học như thể nó không bị mã hóa.

Theo một phương án thực hiện, cam kết Pedersen được sử dụng để mã hóa trị số đầu vào có thể được xây dựng sử dụng các điểm đường cong elip. Thông thường, chìa khóa chung mã hóa đường cong elip (elliptic curve cryptography - ECC) được tạo ra bằng cách nhân bộ sinh cho nhóm (G) với chìa khóa bí mật (r): Pub=rG. Kết quả có thể được đặt nối tiếp hóa như là mảng 33-byte. Các chìa khóa chung ECC có thể tuân theo thuộc tính đồng hình bổ sung được đề cập tới ở trên từ trước, liên quan tới các cam kết Pedersen. Đó là: Pub1+Pub2=(r1+r2(mod n))G.

Cam kết Pedersen cho trị số đầu vào có thể được tạo ra bởi việc nhặt bộ sinh bổ sung cho nhóm (H, trong các phương trình dưới đây) sao cho không có ai biết được bản ghi rời rạc cho bộ sinh thứ hai H liên quan tới bộ sinh thứ nhất G (hoặc ngược lại), nghĩa là không ai biết dudược x sao cho xG=H. Điều này có thể được hoàn thiện, ví

dụ, bằng cách sử dụng việc băm mã hóa của G để nhặt H: H=to_point(SHA256(ENCODE(G))).

Với hai bộ sinh G và H đã cho, sơ đồ cam kết làm ví dụ để mã hóa trị số đầu vào có thể được xác định như là: cam kết=rG+aH. Ở đây, r có thể là nhân tố mù bí mật, và a có thể là trị số đầu vào đang cam kết tới. Do đó, nếu sn được cam kết thì có thể thu được sơ đồ cam kết PC(a) = r×G + a×H nêu trên. Các cam kết Pedersen theo lý thuyết là riêng tư về mặt thông tin: với cam kết bất kỳ, có sự tồn tại của một số nhân tố mù mà nó sẽ tạo sự phù hợp về lượng với cam kết. Các cam kết Pedersen có thể là an toàn về mặt tính toán, chống lại cam kết giả mạo, trong đó việc ánh xạ ngẫu nhiên không thể được tính toán.

Bên (nút) đã cam kết trị số có thể mở việc cam kết bằng cách tiết lộ trị số gốc a và thông số r hoàn thành phương trình cam kết. Bên muốn mở trị số PC(a) sau đó sẽ tính toán việc cam kết một lần nữa để xác thực rằng trị số gốc được chia sẻ thực sự khớp với PC(a) cam kết nhận được từ đầu. Do đó, thông tin loại tài sản có thể được bảo vệ bởi việc ánh xạ nó tới số seri duy nhất, và sau đó mã hóa nó bởi cam kết Pedersen. Số ngẫu nhiên r được chọn khi sinh ra cam kết làm cho nó gần như là không thể cho bất kỳ ai để can thiệp vào loại của loại tài sản được cam kết theo trị số cam kết PC(a).

Theo một số phương án thực hiện, các giao thức trao đổi thông tin mã hóa khác nhau có thể được sử dụng, như giao thức chìa chìa khóa chung (Public-key), giao thức mã hóa đối xứng (symmetric encryption protocol), trao đổi chìa khóa Diffie-Hellman (Diffie-Hellman - DH), v.v. ví dụ, việc trao đổi chìa khóa DH có thể được sử dụng như là phương pháp trao đổi các chìa khóa mã hóa một cách an toàn thông qua kênh công cộng. Việc trao đổi chìa khóa DH, còn được gọi là trao đổi chìa khóa dạng mũ, là phương pháp mã hóa dạng số sử dụng các số được nâng lên tới các mỹ cụ thể để tạo ra các chìa khóa giải mã trên cơ sở của các thành phần không bao giờ được truyền một cách trực tiếp, làm cho nhiệm vụ của việc bẻ mã trở nên quá tải về mặt toán học.

Theo ví dụ của việc áp dụng trao đổi chìa khóa Diffie-Hellman (DH), hai người sử dụng cuối cùng Alice và Bob, trong khi liên lạc qua kênh họ biết là riêng tư, cùng nhau đồng ý trên các số nguyên vẹn dương p và q, sao cho p là số nguyên tố và q là bộ

phận sinh của p. Số sinh q là số mà, khi được nâng lên tới các bậc số toàn vẹn dương nhỏ hơn p, thì sẽ không bao giờ tạo ra cùng một kết quả cho hai số toàn vẹn dương bất kỳ này. Trị số của p có thể lớn, nhưng trị số của q thường là nhỏ. Nghĩa là, q là căn nguyên thủy mođun p.

Khi Alice và Bob đã đồng ý trên p và q trong phần riêng tư thì họ chọn các chìa khóa cá nhân số toàn vẹn dường a và b, cả hai nhỏ hơn số nguyên tố mođun p và cả hai có thể được sinh ra một cách ngẫu nhiên. Không người sử dụng nào tiết lộ chìa khóa cá nhân của họ cho bất kỳ ai, và lý tưởng là họ nhớ các số này và không viết chúng hoặc lưu chúng ở bất kỳ đâu. Tiếp theo, Alice và Bob tính toán các chìa khóa chung a* và b* dựa trên các chìa khóa cá nhân của họ dựa trên các công thức

$$a^* = q^a \bmod p$$

và

$$b^* = q^b \bmod p$$

Hai người sử dụng có thể chia sẻ các chìa khóa chung a* và b* của họ qua môi trường truyền thông được giả sử là không an toàn, như Internet hoặc mạng diện rộng của tập đoàn (wide area network - WAN). Từ các chìa khóa chung này, số k1 có thể được sinh ra bởi hoặc là người sử dụng trên cơ sở của các chìa khóa riêng của riêng họ.

Alice tính toán k1 sử dụng công thức: $k1 = (b^*)^a \bmod p$

Bob tính toán k1 sử dụng công thức: $k1 = (a^*)^b \bmod p$

Chỉ số của k1 trả về là giống như theo một trong hai công thức. Tuy nhiên, các chìa khóa riêng a và b, là thiết yếu trong tính toán của k1, không được truyền qua môi trường công cộng. Thậm chí với p, q, a* và b*, vẫn là rất khó để tính toán a và b. Do nó là lớn và rõ ràng là số ngẫu nhiên, hacker tiềm năng hầu như không có cơ sở đoán một cách chính xác k1, thậm chí với sự trợ giúp của máy tính mạnh mẽ để thực hiện hàng triệu phép thử. Do đó, theo lý thuyết, hai người sử dụng có thể liên lạc một cách riêng tư thông qua môi trường công cộng với phương pháp mã hóa theo lựa chọn của họ sử dụng chìa khóa giải mã k1.

Theo ví dụ khác của việc áp dụng việc trao đổi chìa khóa Diffie-Hellman (DH), tất cả các tính toán xảy ra trong nhóm rời rạc có kích thước đủ lớn, trong đó vấn đề Diffie-Hellman được xem là khó một cách đáng kể, thì thông thường nhóm nhân lên nhiều lần lấy modulo số nguyên tố lớn (ví dụ, với DH truyền thống) hoặc nhóm đường cong eliptic (ví dụ, với Diffie-Hellman cong Eliptic).

Hai bên mà mỗi bên chọn chìa khóa riêng a hoặc b. Mỗi bên tính toán chìa khóa chung aG hoặc bG tương ứng. Mỗi bên gửi chìa khóa chung aG hoặc bG tới bên khác. Mỗi bên sử dụng chìa khóa chung nhận được cùng với của riêng chìa khóa riêng họ để tính toán bí mật được chia sẻ mới a(bG) = b(aG), mà sau đó có thể được sử dụng với hàm dẫn ra chìa khóa để đưa ra bộ các chìa khóa cho sơ đồ mã hóa đối xứng. Theo cách khác, các phương pháp tính toán khác nhau có thể được sử dụng, ví dụ, bằng cách sinh ra các chìa khóa chung g^a và g^b và chìa khóa chia sẻ g^{ab} hoặc g^{ba}.

Trong suốt các giao dịch, việc bảo vệ thông tin là quan trọng để đảm bảo sự riêng tư của người sử dụng, và lượng giao dịch là một loại thông tin thiếu sự bảo vệ. Fig.1 thể hiện hệ thống làm ví dụ 100 để bảo vệ thông tin, theo các phương án thực hiện khác nhau. Như được thể hiện, mạng chuỗi khối có thể chứa nhiều nút (ví dụ, đầy đủ các nút được áp dụng trong các máy chủ, các máy tính, v.v.). Với một số nền tảng chuỗi khối (ví dụ, NEO), các nút đầy đủ với mức cụ thể của năng lực bỏ phiếu có thể được đề cập tới như là các nút đồng thuận, chịu trách nhiệm cho việc xác thực giao dịch. Trong phần mô tả này, các nút đầy đủ, các nút đồng thuận, hoặc các nút tương đương khác có thể xác thực giao dịch.

Cũng vậy, như được thể hiện trên Fig.1, người sử dụng A và người sử dụng B có thể sử dụng các thiết bị tương ứng, như các máy tính xách tay và các điện thoại di động có tác dụng như là các nút hạng nhẹ để thực hiện các giao dịch. Ví dụ, người sử dụng A có thể muốn giao dịch với người sử dụng B bằng cách truyền một số tài sản trong tài khoản của người sử dụng A tới tài khoản của người sử dụng B. Người sử dụng A và người sử dụng B có thể sử dụng các thiết bị tương ứng được cài đặt với phần mềm chuỗi khối thích hợp cho giao dịch. Thiết bị của người sử dụng A có thể được đề cập tới như là nút A bộ khởi tạo, khởi tạo giao dịch với thiết bị của người sử dụng B được đề cập tới như là nút nhận B. Nút A có thể truy cập chuỗi khối qua liên

lạc với nút 1, và nút B có thể truy cập chuỗi khối qua liên lạc với nút 2. Ví dụ, nút A và nút B có thể nộp các giao dịch tới chuỗi khối qua nút 1 và nút 2 để yêu cầu thêm các giao dịch vào chuỗi khối. Ngoài chuỗi khối, nút A và nút B có thể có các kênh liên lạc khác (ví dụ, liên lạc internet thông thường mà không đi qua các nút 1 và 2).

Mỗi nút trong các nút trên Fig.1 có thể chứa bộ xử lý và vật ghi phi chuyển tiếp, đọc được bởi máy tính được ghép nối tới bộ xử lý, môi trường lưu trữ lưu các lệnh mà, khi được thực thi bởi bộ xử lý, sẽ làm cho nút (ví dụ, bộ xử lý) thực hiện các bước khác nhau để bảo vệ thông tin được mô tả ở đây. Mỗi nút có thể được cài đặt với phần mềm (ví dụ, chương trình giao dịch) và/hoặc phần cứng (ví dụ, các kết nối có dây, không dây) để liên lạc với các nút khác và/hoặc các thiết bị khác. Các chi tiết khác của phần cứng và phần mềm của nút sẽ được mô tả sau với tham khảo tới Fig.5.

Fig.2 minh họa các bước làm ví dụ cho giao dịch và việc xác thực giữa nút người gửi A, nút nhận B, và một hoặc nhiều nút xác thực, theo các phương án thực hiện khác nhau. Các thao tác được biểu diễn bên dưới là nhằm mục đích minh họa. Phụ thuộc vào ứng dụng, các bước làm ví dụ có thể chứa các bước bổ sung, ít bước hơn, hoặc các bước thay thế được thực hiện trong các thứ tự khác hoặc được thực hiện song song.

Theo các phương án thực hiện khác nhau, các tài khoản của các bên giao dịch (người gửi người sử dụng A và người nhận người sử dụng B) được định cấu hình cho mô hình tài khoản/số dư (Account/Balance model). Người sử dụng A và người sử dụng B có thể thực hiện các bước sau để thực hiện giao dịch thông qua một hoặc nhiều thiết bị, như máy tính xách tay, điện thoại di động, v.v. của họ. Các thiết bị có thể được cài đặt với phần mềm thích hợp và phần cứng để thực hiện các bước khác nhau. Mỗi tài khoản có thể được kết hợp với cặp chìa khóa riêng mã hóa (chìa khóa bí mật) – chìa khóa chung. Chìa khóa riêng có thể được ghi là SK, và chìa khóa chung có thể được ghi là PK. Chìa khóa riêng có thể được sử dụng để ký thông tin được truyền (ví dụ, thông tin giao dịch). Chìa khóa chung có thể được sử dụng để xác thực thông tin được ký và sinh ra địa chỉ tài khoản. Mỗi tài khoản có thể chứa nhiều tài sản khác nhau, được ghi là: $(V=PC(r, v), E_K(r, v))$, trong đó v biểu diễn trị số mặt của tài sản, V biểu diễn cam kết Pedersen của trị số mặt v, r là 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

chìa khóa mã), và K là chìa khóa mã hóa là duy nhất cho từng tài khoản. Ví dụ, mỗi tài sản có thể được ghi là (V=PC(r, v), E_K(r||v)), trong đó || biểu diễn sự móc nối. Mặc dù sự móc nối được sử dụng trong các phương án thực hiện sau, nhưng các biểu diễn thay thế khác chứa r và v có thể được sử dụng. Chìa khóa mã hóa K (ví dụ, KA, KB) có thể được sinh ra bởi các phương pháp khác nhau như giao thức chìa khóa riêng, hàm dẫn ra chìa khóa, v.v. Mỗi tài sản có thể cúng chứa thông tin khác với thông tin đã được liệt kê, như thông tin nguồn của tài sản.

Theo một ví dụ, trước khi người sử dụng A giao dịch thành công lượng t tới người sử dụng B trong giao dịch được xác thực chuỗi khối, thì các địa chỉ của và các tài sản trong tài khoản của A và tài khoản của B là như sau:

Với tài khoản của A (account A):

Địa chỉ: AddrA

Chìa khóa chung: PK_A

Chìa khóa riêng: SK_A

Chìa khóa thứ nhất: KA

Các tài sản A_1 tới A_m tương ứng với các trị số a_1 tới a_m được ghi là:

(A_1=PC(r_{a1}, a_1), E_{KA}(r_{a1}, a_1)),

(A_2=PC(r_{a2}, a_2), E_{KA}(r_{a2}, a_2)),

...

(A_m=PC(r_{am}, a_m), E_{KA}(r_{am}, a_m))

Với tài khoản của B (account B):

Địa chỉ: AddrB

Chìa khóa chung: PK_B

Chìa khóa riêng: SK_B

Chìa khóa thứ hai: KB

Các tài sản từ B_1 đến B_n tương ứng với các trị số từ b_1 đến b_n được ghi là:

$(B_1=PC(r_{b1}, b_1), E_{KB}(r_{b1}, b_1))$,

$(B_2=PC(r_{b2}, b_2), E_{KB}(r_{b2}, b_2))$,

...

$(B_n=PC(r_{bn}, b_n), E_{KB}(r_{bn}, b_n))$

Theo một số phương án thực hiện, tại bước 201, nút A có thể khởi tạo giao dịch với nút B. Ví dụ, người sử dụng A và người sử dụng B có thể thương lượng lượng giao dịch t từ tài khoản A của người sử dụng A tới tài khoản B của người sử dụng B. Tài khoản A và tài khoản B có thể tương ứng với "các ví" được mô tả ở đây. Tài khoản A có thể có một hoặc nhiều tài sản. Tài sản có thể bao gồm, ví dụ, tiền, thẻ bài, tiền dạng số, hợp đồng, chứng thư, bản ghi y tế, chi tiết khách hàng, chứng khoán, khế ước, cổ phần, hoặc tài sản bất kỳ khác có thể được mô tả ở dạng số. Tài khoản B có thể có một hoặc nhiều tài sản hoặc không có tài khoản. Mỗi tài sản có thể được kết hợp với thông tin chuỗi khối khác nhau được lưu trong các khối của chuỗi khối, thông tin chuỗi khối bao gồm, ví dụ, NoteType thể hiện loại tài khoản, NoteID thể hiện nhận diện duy nhất của tài sản, các trị số cam kết thể hiện trị số cam kết (ví dụ, cam kết Pedersen) của trị số tài sản, việc mã hóa của số ngẫu nhiên và trị số tài sản, v.v.

Như được mô tả liên quan tới tài khoản A, theo một số phương án thực hiện, các tài sản A_1 tới A_m một cách tương ứng tương ứng vơi các trị số tài sản a_1 tới a_m và các số ngẫu nhiên từ r_{a1} đến r_{am}. Dựa trên các số ngẫu nhiên từ r_{a1} đến r_{am}, nút A có thể cam kết các trị số tài sản trong tài khoản A theo sơ đồ cam kết (ví dụ, cam kết Pedersen) để thu được các trị số cam kết được mã hóa. Ví dụ, với tài khoản A, các trị số cam kết được mã hóa có thể là từ PC_1 đến PC_m, trong đó $PC_i= PC(r_{ai}, a_i) = r_{ai}\times G + a_i\times H$, G và H là đã biết, và i là biến giữa 1 và m. Bên cạnh trường thứ nhất PC(...), mỗi tài sản cũng được kết hợp với trường thứ hai E(...) như được mô tả ở trên. Trường thứ hai E(...) có thể thể hiện việc mã hóa của số ngẫu nhiên tương ứng và trị số tài sản được mã hóa với chìa khóa KA. Ví dụ, việc mã hóa có thể là $E_{KA}(r_{ai}, a_i)$. PC(...) và E(...) cho từng tài sản có thể được thừa hưởng từ các giao dịch trước đây. Cùng một cơ chế có thể được áp dụng cho tài khoản B và và các tài sản của nó.

Theo một số phương án thực hiện, để thỏa mãn lượng giao dịch t, người sử dụng A có thể sử dụng chìa khóa thứ nhất KA (ví dụ, chìa khóa mã hóa đối xứng) để giải mã một hoặc nhiều tài sản của trị số được tích tụ ít nhất t từ tài khoản A. ví dụ, nút A có thể rút các tài sản A_1, A_2, …, A_k cho giao dịch này, trong đó k là nhỏ hơn hoặc bằng với m. Các tài sản còn lại A_{k+1}, A_{k+2}, …, A_m của tài khoản A không được rút. Một cách tương ứng, nút A có thể đọc các tài sản $PC(r_{a1}, a_1)$, $PC(r_{a2}, a_2)$, …, $PC(r_{ak}, a_k)$ từ nút 1. Với các số ngẫu nhiên r_{a1}, r_{a2}, …, r_{ak} đã biết tới nút A, nút A có thể giải mã các tài sản được đọc $PC(r_{a1}, a_1)$, $PC(r_{a2}, a_2)$, …, $PC(r_{ak}, a_k)$ để thu được các trị số tài sản a_1, a_2, …, a_k để đảm bảo rằng tổng $(a_1 + a_2 + \ldots + a_k)$ là không nhỏ hơn lượng giao dịch t. Các tài sản khác có thể được trao đổi tới một thành phần khác nằm trong tài khoản dựa trên các tỉ lệ khác nhau.

Theo một số phương án thực hiện, chìa khóa mã hóa đối xứng có thể đề cập tới cùng một chìa khóa mã được sử dụng trong thuật toán chìa khóa đối xứng mã hóa cho cả việc mã hóa của văn bản thô và việc giải mã của văn bản đã được mã hóa. Các chìa khóa có thể là trùng nhau hoặc có thể có việc biến đổi đơn giản giữa hai chìa khóa. Các chìa khóa có thể biểu diễn bí mật được chia sẻ giữa hai hoặc hơn hai bên có thể được sử dụng để duy trì liên kết thông tin riêng tư.

Theo một số phương án thực hiện, lượng của trị số tài sản được chọn vượt quá t, nếu có, sẽ được đặt là y như thay đổi. Ví dụ, nút A có thể xác định thay đổi $y = (a_1 + a_2 + \ldots + a_k) - t$. Nút A có thể chọn các số ngẫu nhiên r_t và r_y làm các nhân tố mù để sinh 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 sinh ra số ngẫu nhiên r_t cho t và số ngẫu nhiên r_y cho y. Nút A có thể cam kết t và r_t tới sơ đồ cam kết (ví dụ, việc mã hóa đồng hình) để thu được trị số cam kết $T = PC(r_t, t)$, và cam kết y và r_y tới sơ đồ cam kết (ví dụ, việc mã hóa đồng hình) để thu được trị số cam kết $Y = PC(r_y, y)$. Hơn nữa, nút A có thể xác định $r' = (r_1 + r_2 \ldots + r_k) - r_t - r_y$.

Theo một số phương án thực hiện, nút A có thể sử dụng chìa khóa thứ nhất KA để cho encrypt(r_y, y), thu được encryption $E_{KA}(r_y, y)$. Nút A có thể lưu $E_{KA}(r_y, y)$ tại chỗ.

Tại bước 202, nút A có thể gửi thông tin giao dịch tới nút B (ví dụ, qua chuỗi khối, qua kênh an ninh ngoài chuỗi khối). Thông tin giao dịch được gửi có thể bao

gồm, ví dụ, số ngẫu nhiên r_t, lượng giao dịch t, và trị số cam kết T. Thông tin giao dịch có thể được gửi ở dạng văn bản gốc.

Tại bước 203, nút B có thể xác thực số ngẫu nhiên r_t, lượng giao dịch t, và trị số cam kết T. Theo một số phương án thực hiện, nút B có thể xác thực nếu lượng t để gửi tới người sử dụng B là đúng hay không, và nếu $T=PC(r_t, t)$. Với bước 203, nếu việc so khớp/xác thực thất bại, nút B có thể từ chối giao dịch. Nếu việc so khớp/xác thực thành công thì nút B có thể trả lời nút A tại bước 204.

Tại bước 204, nút B có thể mã hóa (r_t, t) với chìa khóa thứ hai KB (ví dụ, chìa khóa mã hóa đối xứng) để thu được việc mã hóa $E_{KB}(r_t, t)$ và ký giao dịch $(E_{KB}(r_t, t), T)$ với chìa khóa riêng SK_B của người sử dụng B để sinh ra chữ ký SIGB. Việc ký có thể tuân theo thuật toán ký số (Digital Signature Algorithm - DSA) như thuật toán ký số đường cong elip (Elliptic Curve Digital Signature Algorithm - ECDSA), trong đó bộ thu của chữ ký có thể xác thực chữ ký với chìa khóa chung của người ký để xác thực dữ liệu được ký. Chữ ký SIGB chỉ thị rằng nút nhận B đồng ý với giao dịch.

Tại bước 205, nút B có thể truyền giao dịch được ký $E_{KB}(r_t, t)$ và chữ ký SIGB trở lại nút A.

Tại bước 206, nếu SIGB không được xác thực đầy đủ thì nút A có thể từ chối giao dịch. Nếu SIGB được xác thực thành công thì nút A có thể sinh ra bằng chứng khoảng giới hạn (range proof - RP) để chứng minh cho các nút chuỗi khối nếu mỗi trị số trong trị số của $PC(r_t, t)$ và trị số của $PC(r_y, y)$ nằm trong khoảng giới hạn hợp lệ. Ví dụ, để có các trị số hợp lệ của $PC(r_t, t)$, lượng giao dịch t có thể nằm trong khoảng giới hạn hợp lệ $[0, 2^n-1]$; và để có các trị số hợp lệ $PC(r_y, y)$, thay đổi y có thể nằm trong khoảng giới hạn hợp lệ $[0, 2^n-1]$. Theo một phương án thực hiện, nút A có thể sử dụng kỹ thuật bằng chứng khối (block proof) để sinh ra bằng chứng khoảng giới hạn (range proof - RP) có liên quan tới (T, r_t, t, Y, r_y, y) cho các nút chuỗi khối (ví dụ, các nút đồng thuận) để xác thực tại bước sau đó xem liệu lượng giao dịch t và thay đổi y có nằm trong khoảng giới hạn hợp lệ dựa trên bằng chứng khoảng giới hạn hay không. Bằng chứng khoảng giới hạn có thể bao gồm, ví dụ, Bulletproofs, chữ ký vòng Borromean, v.v.

Tiếp theo, nút A có thể ký giao dịch với chìa khóa riêng SK_A của người sử dụng A để sinh ra chữ ký SIGA. Một cách tương tự, việc ký có thể tuân theo thuật toán ký dạng số (Digital Signature Algorithm - DSA). Theo một phương án thực hiện, nút A có thể ký ({PC(r_{a1}, a_1), E_{KA}(r_{a1}, a_1); PC(r_{a2}, a_2), E_{KA}(r_{a2}, a_2); … PC(r_{ak}, a_k), E_{KA}(r_{ak}, a_k)}; {PC(r_y, y), E_{KA}(r_y, y)}; {PC(r_t, t), E_{KB}(r_t, t)}; Y; T; r'; RP) với chìa khóa riêng của người sử dụng A để sinh ra chữ ký SIGA, trong đó {PC(r_{a1}, a_1), E_{KA}(r_{a1}, a_1); PC(r_{a2}, a_2), E_{KA}(r_{a2}, a_2); … PC(r_{ak}, a_k), E_{KA}(r_{ak}, a_k)} biểu diễn các tài sản được rút A_1, A_2, …, A_k từ tài khoản A để giao dịch. {PC(r_y, y), E_{KA}(r_y, y)} biểu diễn thay đổi mà tài khoản A sẽ nhận được từ giao dịch. {PC(r_t, t), E_{KB}(r_t, t)} biểu diễn tài sản được truyền mà tài khoản B sẽ nhận được từ giao dịch.

Tại bước 207, nút A có thể nộp giao dịch tới chuỗi khối, làm cho các nút chuỗi khối xác thực giao dịch và xác định xem liệu có thêm giao dịch vào chuỗi khối hay không. Theo một phương án thực hiện, nút A có thể nộp giao dịch ({PC(r_{a1}, a_1), E_{KA}(r_{a1}, a_1); PC(r_{a2}, a_2), E_{KA}(r_{a2}, a_2); … PC(r_{ak}, a_k), E_{KA}(r_{ak}, a_k)}; {PC(r_y, y), E_{KA}(r_y, y)}; {PC(r_t, t), E_{KB}(r_t, t)}; Y; T; r'; RP; SIGA; SIGB) vào chuỗi khối thông qua nút 1 để thực thi giao dịch. Giao dịch có thể bao gồm các thông số bổ sung hoặc có thể không bao gồm tất cả các thông số trong các thông số đã được liệt kê. Giao dịch có thể được truyền quảng bá tới một hoặc nhiều nút (ví dụ, các nút đồng lòng) trong chuỗi khối để xác thực. Nếu việc xác thực thành công thì giao dịch được thêm vào chuỗi khối. Nếu việc xác thực là thất bại thì giao dịch bị từ chối thêm vào chuỗi khối.

Tại các bước 208-213, một hoặc nhiều nút (ví dụ, các nút đồng thuận) xác thực các chữ ký, chứng cứ khoảng giới hạn, và thông tin khác của giao dịch được nộp. Nếu xác thực thất bại, các nút từ chối giao dịch. Nếu việc xác thực là thành công thì các nút chấp nhận giao dịch, cập nhật tài khoản của người sử dụng A và tài khoản của người sử dụng B một cách tách biệt.

Theo một số phương án thực hiện, để thực thi giao dịch, thông tin giao dịch có thể được xác thực bởi các nút chuỗi khối khác nhau. Thông tin giao dịch có thể chứa đại chỉ giao dịch TXID, chữ ký (các chữ ký), đầu vào, và đầu ra. TXID có thể bao gồm việc băm của nội dung giao dịch. Các chữ ký có thể chứa các chữ ký chìa khóa mã hóa bởi người gửi và người nhận. Đầu vào có thể chứa địa chỉ của tài khoản người gửi

trong chuỗi khối, một hoặc nhiều tài sản được rút từ tài khoản chuỗi khối của người gửi chi giao dịch, v.v. Đầu ra có thể bao gồm địa chỉ của tài khoản của người nhận trong chuỗi khối, loại (các loại) tài sản của tài sản (các tài sản) người nhận, trị số (các trị số) cam kết của tài sản (các tài sản) người nhận, v.v. Đầu vào và đầu ra có thể chứa thông tin được chỉ mục ở dạng bảng. Theo một số phương án thực hiện, trị số của trị số NoteID có thể là "TXID + chỉ số của tài sản trong đầu ra".

Theo một số phương án thực hiện, một hoặc nhiều nút của chuỗi khối có thể xác nhận giao dịch được nộp ({PC(r_{a1}, a_1), E_{KA}(r_{a1}, a_1); PC(r_{a2}, a_2), E_{KA}(r_{a2}, a_2); … PC(r_{ak}, a_k), E_{KA}(r_{ak}, a_k)}; {PC(r_y, y), E_{KA}(r_y, y)}; {PC(r_t, t), E_{KB}(r_t, t)}; Y; T; r'; RP; SIGA; SIGB).

Tại bước 208, các nút có thể xác thực xem liệu giao dịch có được thực thi sử dụng cơ chế sử dụng chống kép (anti-double-spending mechanism) hay cơ chế tấn công chống chơi lại (anti-replay-attack mechanism). Nếu giao dịch đã được thực thi, thì các nút có thể từ chối giao dịch; ngược lại, phương pháp có thể tiến tới bước 209.

Tại bước 209, các nút có thể kiểm tra các chữ ký SIGA và SIGB (ví dụ, dựa trên chìa khóa chung của A và chìa khóa chung của B một cách tương ứng). Nếu chữ ký bất kỳ trong các chữ ký là không đúng thì các nút có thể từ chối giao dịch; theo cách khác, phương pháp có thể tiến tới bước 210.

Tại bước tùy chọn 210, các nút có thể xác thực xem các loại tài sản có thống nhất hay không. Ví dụ, các nút có thể xác thực xem các loại tài sản trong NoteType cho A_1 tới A_k là thống nhất với loại (các loại) tài sản của lượng giao dịch t. Nếu loại bất kỳ của các loại tài sản là không thống nhất thì các nút có thể từ chối giao dịch; trái lại, phương pháp có thể tiến tới bước 211. Theo một số phương án thực hiện, loại tài sản gốc trong ví có thể được biến đổi thành loại khác dựa trên tỉ giá trao đổi, và bước này có thể được bỏ qua.

Tại bước 211, các nút có thể kiểm tra bằng chứng khoảng giới hạn (range proof - RP) để hợp lệ hóa trị số PC(r_t, t) và trị số PC(r_y, y). Theo một phương án thực hiện, các nút có thể kiểm tra bằng chứng khoảng giới hạn (range proof - RP) để xác thực xem liệu lượng giao dịch t có không nhỏ hơn không hay không và thay đổi y là không nhỏ

hơn không hay không. Nếu việc xác thực là thất bại thì các nút có thể từ chối giao dịch; theo cách khác, phương pháp có thể tiến tới bước 212.

Tại bước 212, các nút có thể kiểm tra xem liệu các đầu vào và các đầu ra của giao dịch có thống nhất hay không. Theo một phương án thực hiện, r' có thể tương ứng với trị số tài sản $t' = a_1 + a_2 \ldots + a_k - t - y$ dựa trên thuộc tính đồng hình, trong đó $r' = (r_1 + r_2 \ldots + r_k) - r_t - r_y$. Do các tài sản đầu vào là $a_1 + a_2 \ldots + a_k$ và đầu ra là $t + y$, $t' = 0$ khi đầu vào và đầu ra là thống nhất thì: $a_1 + a_2 \ldots + a_k = t + y$. Do đó, trị số cam kết tương ứng với r' là $PC(r', t') = r' \times G + t' \times H = r'G$. Do $r' = (r_1 + r_2 \ldots + r_k) - r_t - r_y$, các nút có thể xác định xem nếu các đầu vào và các đầu ra có bằng nhau hay không bằng cách xác thực xem nếu r'G có bằng với $PC_1 + \ldots + PC_k - T - Y$ tương ứng với $(r_1 + r_2 \ldots + r_k) - r_t - r_y$ hay không. Nếu r'G là bằng với $PC_1 + \ldots + PC_k - T - Y$, thì các nút có thể xác đỉnh ằng các đầu vào và các đầu ra của giao dịch là thông nhất và tiến tới bước tiếp theo; trái lại, các nút có thể xác định rằng các đầu vào và các đầu ra của giao dịch là không thống nhất và từ chối giao dịch.

Tại bước 213, các nút có thể xác thực xem nết nút A có tài sản (các tài sản) được rút cho giao dịch hay không. Theo một phương án thực hiện, các nút có thể thực hiện việc xác thực này dựa trên thông tin được lưu trong chuỗi khối, như thông tin tương ứng với tài khoản A. Thông tin có thể bao gồm thông gin giao dịch trước đây của tất cả các tài sản. Do đó, các nút có thể xác định xem nếu tài khoản A có tài sản giao dịch để giao dịch hay không. Nếu việc xác định là không thì các nút có thể từ chối giao dịch; theo cách khác, phương pháp có thể tiến tới bước 214.

Tại bước 214, các nút có thể cập nhật tài khoản A và tài khoản B. Ví dụ, các nút có thể loại bỏ tài sản giao dịch của lượng t từ tài khoản A, và thêm phần như vậy vào tài khoản B. Dựa trên thuộc tính đồng hình, do $Y = PC(r_y, y)$ và nút 1 biết r_y và có thể truy cập trị số cam kết Y từ chuỗi khối, nút 1 có thể giải mã Y để thu được trị số tài sản y và trả lại phần tương tự tới tài khoản A. Nút 2 thu được tại bước 202 số ngẫu nhiên r_t từ nút 1 và có thể thu được từ trị số cam kết chuỗi khối T. Do đó, nút 2 có thể giải mã T để thu được trị số tài sản và thêm phần tương tự vào tài khoản B.

Theo một ví dụ, sau khi cập nhật tài khoản A và tài khoản B, tài khoản A nhận thay đổi y tới các tài sản được rút $A_1, A_2, \ldots, A_k$ và nhận các tài sản không được rút

A_{ak+1}, …, A_m của nó, và tài khoản B nhận lượng giao dịch t và nhận các tài sản gốc B_1, B_2, …, B_n của nó. Các tài sản trong tài khoản của A và tài khoản của B là như sau:

Với tài khoản của A (account A), các tài sản được cập nhật được ghi là:

$(Y=PC(r_y, y), E_{KA}(r_y, y))$,

$(A_{ak+1}=PC(r_{ak+1}, a_{k+1}), E_{KA}(r_{ak+1}, a_{k+1}))$

$(A_{ak+2}=PC(r_{ak+2}, a_{k+2}), E_{KA}(r_{ak+2}, a_{k+2}))$

...

$(A_m=PC(r_{am}, a_m), E_{KA}(r_{am}, a_m))$

Với tài khoản của B (account B), các tài sản được cập nhật được ghi là:

$(B_1=PC(r_{b1}, b_1), E_{KB}(r_{b1}, b_1))$,

$(B_2=PC(r_{b2}, b_2), E_{KB}(r_{b2}, b_2))$,

...

$(B_n=PC(r_{bn}, b_n), E_{KB}(r_{bn}, b_n))$,

$(T=PC(r_t, t), E_{KB}(r_t, t))$

Mặc dù phần mô tả này sử dụng nút A/người sử dụng A và nút B/người sử dụng B để minh họa cho người gửi và người nhận một cách tương ứng, nhưng người gửi và nhgười nhận có thể là cùng một nút/người sử dụng. Ví dụ, thay đổi y của giao dịch (tổng tài sản được rút trong tài khoản A trừ đi lượng giao dịch) có thể được gửi trở lại người gửi của giao dịch. Do đó, các bước khác nhau được thực hiện bởi nút B như được mô tả ở đây theo cách khác có thể được thực hiện bởi nút A.

Fig.3 minh họa lưu đồ của phương pháp làm ví dụ 300 để bảo vệ thông tin, theo các phương án thực hiện khác nhau của sáng chế này. Phương pháp 300 có thể được áp dụng bởi một hoặc nhiều thành phần (ví dụ, nút A, nút 1, tổ hợp của nút A và nút 1) của hệ thống 100 của Fig.1. Phương pháp 300 có thể được áp dụng bởi hệ thống hoặc thiết bị (ví dụ, máy tính, máy chủ) bao gồm bộ xử lý và vật ghi phi chuyển tiếp, đọc được bởi máy tính (ví dụ, bộ nhớ) lưu các lệnh. Các lệnh, khi được thực thi bởi bộ xử lý, sẽ làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) thực hiện phương pháp 300. Các

thao tác của phương pháp 300 được biểu diễn dưới đây nhằm để minh họa. Phụ thuộc vào ứng dụng, phương pháp làm ví dụ 300 có thể chứa các bước bổ sung, ít bước hơn, hoặc các bước thay thế được thực hiện trong các thứ tự khác hoặc được thực hiện song song.

Khối 301 bao gồm bước: cam kết lượng giao dịch t của giao dịch với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, và cam kết thay đổi y của giao dịch với sơ đồ cam kết thứ hai để thu được trị số cam kết thay đổi Y, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t, và sơ đồ cam kết thứ hai bao gồm nhân tố mù thay đổi r_y. Theo một số phương án thực hiện, sơ đồ cam kết thứ nhất bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù giao dịch r_t và với lượng giao dịch t đang là trị số được cam kết tương ứng. Xem, ví dụ, $T=PC(r_t, t)$. Sơ đồ cam kết thứ hai bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù thay đổi r_y và với thay đổi y đang là trị số được cam kết tương ứng. Xem, ví dụ, $Y=PC(r_y, y)$.

Khối 302 bao gồm: mã hóa tổ hợp thứ nhất của nhân tố mù thay đổi r_y và thay đổi y với chìa khóa thứ nhất KA.

Khối 303 bao gồm: truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch; Theo một số phương án thực hiện, bước truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch bao gồm: truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch, làm cho nút nhận để xác thực xem nếu trị số cam kết giao dịch T là bằng với sơ đồ cam kết thứ nhất cam kết lượng giao dịch t với nhân tố mù giao dịch r_t.

Khối 304 bao gồm: đáp ứng lại với việc nút nhận xác thực thành công giao dịch, thu được tổ hợp thứ hai được mã hóa của nhân tố mù giao dịch r_t và lượng giao dịch t được mã hóa với chìa khóa thứ hai KB. Theo một số phương án thực hiện, bước thu được tổ hợp thứ hai được mã hóa bao gồm việc nhận từ nút nhận tổ hợp thứ hai được mã hóa và chữ ký SIGB được kết hợp với tổ hợp thứ hai được mã hóa và trị số cam kết giao dịch T.

Khối 305 bao gồm: truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối cho các nút trong chuỗi khối để xác thực giao dịch.

Theo một số phương án thực hiện, lượng giao dịch t được rút từ một hoặc nhiều tài sản A_1, A_2, …, A_k của người gửi của giao dịch; mỗi tài sản trong các tài sản được kết hợp với (1) cam kết Pedersen dựa ít nhất trên nhân tố mù r_{ak} và trị số của từng tài sản và (2) việc mã hóa dựa ít nhất trên nhân tố mù r_{ak} và trị số của từng tài sản; và thay đổi y là khác biệt giữa lượng giao dịch t và các tài sản được rút.

Theo một số phương án thực hiện, trước bước truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối, phương pháp còn bao gồm bước: xác thực chữ ký SIGB; và đáp ứng lại việc xác thực thành công chữ ký SIGB, sinh ra chữ ký SIGA được kết hợp với các tài sản A_1, A_2, …, A_k, tổ hợp thứ nhất, tổ hợp thứ hai, trị số cam kết giao dịch T, trị số cam kết thay đổi Y, và khác biệt giữa tổng của các nhân tố mù tương ứng với các tài sản A_1, A_2, …, A_k và tổng của nhân tố mù giao dịch r_t và nhân tố mù thay đổi r_y. Nghĩa là, khác biệt $r' = (r_1 + r_2 \ldots + r_k) - (r_t + r_y)$.

Theo một số phương án thực hiện, bước truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối bao gồm: truyền các tài sản A_1, A_2, …, A_k, tổ hợp thứ nhất, tổ hợp thứ hai, trị số cam kết giao dịch T, trị số cam kết thay đổi Y, khác biệt giữa tổng của các nhân tố mù tương ứng với các tài sản A_1, A_2, …, A_k và tổng của nhân tố mù giao dịch r_t và nhân tố mù thay đổi r_y, chữ ký SIGA, và chữ ký SIGB tới nhiều nút trong chuỗi khối.

Theo một số phương án thực hiện, bước truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối cho các nút trong chuỗi khối để xác thực giao dịch bao gồm: truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong chuỗi khối, làm cho các nút trong chuỗi khối, đáp ứng lại việc xác thực thành công giao dịch, đưa ra lượng giao dịch t tới người nhận, loại bỏ các tài sản A_1, A_2, …, A_k, và đưa ra thay đổi y tới người gửi.

Fig.4 minh họa lưu đồ của phương pháp làm ví dụ 400 để bảo vệ thông tin, theo các phương án thực hiện khác nhau của sáng chế này. Phương pháp 400 có thể được

áp dụng bởi một hoặc nhiều thành phần (ví dụ, nút B, nút 2, tổ hợp của nút B và nút 2) của hệ thống 100 của Fig.1. Phương pháp 400 có thể được áp dụng bởi hệ thống hoặc thiết bị (ví dụ, máy tính, máy chủ) bao gồm bộ xử lý và vật ghi phi chuyển tiếp, đọc được bởi máy tính (ví dụ, bộ nhớ) lưu các lệnh. Các lệnh, khi được thực thi bởi bộ xử lý, sẽ làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) thực hiện phương pháp 400. Các thao tác của phương pháp 400 được biểu diễn dưới đây nhằm để minh họa. Phụ thuộc vào ứng dụng, phương pháp làm ví dụ 400 có thể chứa các bước bổ sung, ít bước hơn, hoặc các bước thay thế được thực hiện trong các thứ tự khác hoặc được thực hiện song song.

Khối 401 bao gồm: thu được nhân tố mù giao dịch r_t, lượng giao dịch t của giao dịch, và trị số cam kết giao dịch T từ nút người gửi được kết hợp với người gửi của giao dịch, trong đó: lượng giao dịch t được cam kết với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t;

Khối 402 bao gồm: xác thực giao dịch dựa trên nhân tố mù giao dịch r_t thu được, lượng giao dịch t thu được của giao dịch, và trị số cam kết giao dịch T thu được. Theo một số phương án thực hiện, bước xác thực giao dịch dựa trên nhân tố mù giao dịch r_t thu được, lượng giao dịch t thu được của giao dịch, và trị số cam kết giao dịch T thu được bao gồm xác thực nếu trị số cam kết giao dịch T thu được là bằng với sơ đồ cam kết thứ nhất cam kết lượng giao dịch t thu được với nhân tố mù giao dịch r_t thu được.

Khối 403 bao gồm: đáp ứng lại việc xác thực thành công giao dịch, mã hóa tổ hợp thứ hai của nhân tố mù giao dịch r_t và lượng giao dịch t với chìa khóa thứ hai KB.

Khối 404 bao gồm: truyền tổ hợp thứ hai được mã hóa tới nút người gửi. Theo một số phương án thực hiện, trước bước truyền tổ hợp thứ hai được mã hóa tới nút người gửi, phương pháp còn bao gồm bước sinh ra chữ ký SIGB được kết hợp với tổ hợp thứ hai được mã hóa và trị số cam kết giao dịch T; và truyền tổ hợp thứ hai được mã hóa tới nút người gửi bao gồm việc truyền tổ hợp thứ hai được mã hóa và chữ ký SIGB tới nút người gửi.

Như được thể hiện, sự riêng tư cho lượng giao dịch có thể được bảo vệ qua nhiều cải tiến khác nhau của công nghệ máy tính. Ví dụ, cấu trúc tài khoản bao gồm một

hoặc nhiều trường, như trường thứ nhất được kết hợp với cam kết Pedersen của trị số tài sản (ví dụ, trường thứ nhất là $PC(r_{ai}, ai)$, với i là giữa 1 và m) và trường thứ hai được kết hợp với số ngẫu nhiên cho cam kết Pedersen và trị số tài sản (ví dụ, trường thứ hai là $E_{KA}(r_{ai}, ai)$, với i là giữa 1 và m). Trường thứ nhất và trường thứ hai cũng được sử dụng trong các bước giao dịch và được lưu trong chuỗi khối.

Theo ví dụ khác, chìa khóa mã hóa được sử dụng để mã hóa số ngẫu nhiên của từng cam kết Pedersen và trị số tài sản tương ứng. Chìa khóa mã hóa cho việc mã hóa/giải mã được giữ bởi người chủ tài khoản, do đó tính riêng tư của các trị số tài sản được bảo vệ khỏi người sử dụng không có chìa khóa mã hóa. Ngoài ra, giao dịch chứa các số ngẫu nhiên được mã hóa và các trị số tài sản được lưu trong chuỗi khối. Cách này tạo thuận tiện cho việc quản lý các số ngẫu nhiên, tối thiểu hóa các cơ hội tổn thất và việc thay đổi của các số ngẫu nhiên và các trị số tài sản, và thúc đẩy tính an ninh dựa trên việc lưu trữ chuỗi khối phân tán và thống nhất.

Các bước trước khi nộp giao dịch tới chuỗi khối có thể được xử lý như là thành vi ngoài chuỗi ("off-chain") hoặc trước giao dịch ("pre-transaction"), do các quy trình mã hóa và giải mã xảy ra ở các phía khách hàng, trong khi chuỗi khối lưu "asset value + corresponding random number" được mã hóa được biểu diễn bởi hàm E(). Cam kết Pedersen có thể là tương tự như két với tài sản nằm bên trong, và "asset value + corresponding random number" là tương tự như chìa khóa của két. Chìa khóa được mã hóa và két được kết hợp của nó có thể được lưu trong chuỗi khối, là chống cháy và chống mất mát. Mỗi lần người sử dụng muốn mở rộng tài sản (các tài sản), người sử dụng có thể tìm lại két và chìa khóa được mã hóa từ chuỗi khối và giải mã chìa khóa trên phía khách hàng, sao cho các bước "trước giao dịch" ("pre-transaction") có thể được thực hiện để kết hợp giao dịch mới mở rộng tài sản (các tài sản).

Như vậy, các số ngẫu nhiên của các cam kết Pedersen có thể được quản lý một cách thuận iện, mà không có rủi ro sai lệch và không tạo ra việc quá tải quản lý chìa khóa bổ sung. Do đó, sự riêng tư của giao dịch có thể được bảo vệ một cách hoàn toàn, và lượng các giao dịch có thể được giữ bí mật.

Các kỹ thuật được mô tả ở đây được áp dụng bởi một hoặc nhiều thiết bị tính toán mục đích đặc biệt. Các thiết bị tính toán mục đích đặc biệt có thể là các hệ thống

máy tính để bàn, các hệ thống máy tính chủ, các hệ thống máy tính di động, các thiết bị cầm tay, các thiết bị mạng hoặc thiết bị bất kỳ khác hoặc tổ hợp của các thiết bị tích hợp phần logic được nối dây cứng và/hoặc logic chương trình để áp dụng các ký thuật này. Thiết bị (các thiết bị) tính toán thường được điều khiển và được phối hợp bởi phần mềm hệ điều hành. Các hệ điều hành thông thường điều khiển và lập lịch các quy trình máy tính để thực thi, thực hiện việc quản lý bộ nhớ, tạo ra hệ thống tệp, nối mạng, các dịch vụ I/O, và tạo ra chức năng giao diện người sử dụng, như giao diện đồ họa người sử dụng (graphical user interface - GUI), bên cạnh các chức năng khác.

Fig.5 là giản đồ khối minh họa hệ thống máy tính 500 mà các phương án thực hiện được mô tả ở đây có thể được áp dụng vào trong đó. Hệ thống 500 có thể được áp dụng trong nút bất kỳ trong các nút được mô tả ở đây 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 chứa bus 502 hoặc cơ chế liên lạc khác để liên lạc thông tin, một hoặc nhiều bộ xử lý (các bộ xử lý) phần chứng 504 được ghép nối với bus 502 để xử lý thông tin. Bộ xử lý (các bộ xử lý) phần cứng 504 có thể, ví dụ là, một hoặc nhiều bộ vi xử lý mục đích chung.

Hệ thống máy tính 500 cũng chứa bộ nhớ chính 506, 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 tới bus 502 để lưu thông tin và các lệnh cần được thực thi bởi bộ xử lý (các bộ xử lý) 504. Bộ nhớ chính 506 cũng có thể được sử dụng để tạm thời lưu các biến hoặc thông tin trung gian khác trong quá trình thực thi các lệnh cần được thực thi bởi bộ xử lý (các bộ xử lý) 504. Các lệnh này, khi được lưu trong môi trường lưu trữ có thể truy cập được bởi bộ xử lý (các bộ xử lý) 504, hệ thống máy tính phục hồi 500 vào máy mục đích riêng được tùy chỉnh để thực thiện các thao tác được chỉ rõ trong các lệnh. Hệ thống máy tính 500 còn chứa bộ nhớ chỉ đọc (read only memory - ROM) 508 hoặc thiết bị lưu trữ tĩnh khác được ghép nối tới bus 502 để lưu 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 học, hoặc ổ đĩa USB nhỏ (ổ đĩa tác động nhanh Flash), v.v., được tạo ra và được ghép nối tới bus 502 để lưu thông tin và các lệnh.

Hệ thống máy tính 500 có thể áp dụng các kỹ thuật được mô tả ở đây sử dụng logic được nối dây cứng được tùy chỉnh, một hoặc nhiều ASIC hoặc FPGA, phần sụn và/hoặc logic chương trình trong kết hợp với hệ thống máy tính làm cho hoặc lập trình cho hệ thống máy tính 500 trờ thành máy có mục đích riêng. Theo một phương án thực hiện, các thao tác, các phương pháp, và các quy trình được mô tả ở đây được thực hiện bởi hệ thống máy tính 500 đáp ứng lại bộ xử lý (các bộ xử lý) 504 thực thi một hoặc nhiều chuỗi của một hoặc nhiều lệnh được chứa trong bộ nhớ chính 506. Các lệnh này có thể được đọc vào trong bộ nhớ chính 506 từ môi trường lưu trữ khác, như thiết bị lưu trữ 510. Việc thực thi của các chuỗi của các lệnh được chứa trong bộ nhớ chính 506 làm cho bộ xử lý (các bộ xử lý) 504 thực hiện các bước xử lý được mô tả ở đây. Theo các phương án thực hiện thay thế, mạch được nối cứng có thể được sử dụng thay cho hoặc kết hợp với các lệnh phần mềm.

Bộ nhớ chính 506, ROM 508, và/hoặc bộ phận lưu trữ 510 có thể chứa môi trường lưu trữ phi chuyển tiếp. Thuật ngữ "môi trường phi chuyển tiếp", và các thuật ngữ tương tự, như được sử dụng ở đây đề cập tới môi trường lưu dữ liệu và/hoặc các lệnh làm cho máy vận hành theo cách cụ thể, môi trường ngoại trừ các tín hiệu chuyển tiếp. Môi trường phi chuyển tiếp này có thể còn bao gồm môi trường bất khả biến và/hoặc môi trường khả biến. Môi trường bất khả biến bao gồm, ví dụ, các đĩa quang học hoặc đĩa từ, như thiết bị lưu trữ 510. Môi trường khả biến chứa bộ nhớ động, như bộ nhớ chính 506. Các dạng chung của môi trường phi chuyển tiếp bao gồm, ví dụ, ổ đĩa mềm, ổ đĩa cứng, ổ đĩa trạng thái rắn, băng từ, hoặc môi trường lưu trữ dữ liệu từ tính khác, CD-ROM, môi trường lưu trữ dữ liệu quang học bất kỳ khác, môi trường vật lý bất kỳ khác với các mẫu lỗ, RAM, PROM, và EPROM, FLASH-EPROM, NVRAM, chip hoặc hộp nhớ bất kỳ khác, và các phiên bản được nối mạng của chúng.

Hệ thống máy tính 500 cũng chứa giao diện mạng 518 được ghép nối tới bus 502. Giao diện mạng 518 tạo ra ghép nối liên lạc dữ liệu hai chiều tới một hoặc nhiều liên kết mạng được kết nối tới một hoặc nhiều mạng cục bộ. Ví dụ, giao diện mạng 518 có thể là thẻ mạng dạng số dịch vụ được tích hợp (integrated services digital network - ISDN), bộ mã hóa/giải mã cáp, bộ mã hóa/giải mã vệ tinh, hoặc bộ mã hóa/giải mã để tạo ra kết nối liên lạc dữ liệu tới loại tương ứng của đường điện thoại.

Như một ví dụ, giao diện mạng 518 có thể là thẻ mạng diện cục bộ (local area network - LAN) có thể tạo ra kết nối liên lạc dữ liệu tới LAN tương hợp (hoặc thành phần WAN để được kết nối với WAN). Các liên kết không dây cũng có thể được áp dụng. Theo áp dụng bất kỳ này, giao diện mạng 518 gửi và nhận các tín hiệu điện, điện từ hoặc quang học mang các luồng dữ liệu dạng số biểu diễn các loại thông tin.

Hệ thống máy tính 500 có thể gửi các tin nhắn và nhận dữ liệu, chứa mã chương trình, qua mạng (các mạng), liên kết mạng và giao diện mạng 518. Theo 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 nó được nhận, và/hoặc được lưu trong thiết bị lưu trữ 510, hoặc bộ phận lưu trữ bất khả biến khác để thực thi sau.

Mỗi thành phần trong các quy trình, các phương pháp, và các thuật toán được mô tả trong các phần trên có thể được áp dụng trong, và được tự động hóa một cách hoàn toàn hoặc một phần bởi, các môđun mã được thực thi bởi một hoặc nhiều hệ thống máy tính hoặc các bộ xử lý máy tính chứa phần cứng máy tính. Các quy trình và các thuật toán có thể được áp dụng một phần hoặc hoàn toàn trong mạch ứng dụng riêng.

Các dấu hiệu và các quy trình được mô tả ở đây có thể được sử dụng độc lập với nhau hoặc cũng có thể được kết hợp theo nhiều cách. Các tổ hợp và các tổ hợp con khả thi được coi là nằm trong phạm vi bảo hộ của sáng chế này. Ngoài ra, phương pháp hoặc các khối xử lý cụ thể có thể được bỏ qua trong một số ứng dụng. Các phương pháp và quy trình được mô tả ở đây cũng không bị hạn chế vào trình tự cụ thể bất kỳ và các khối hoặc các trạng thái liên quan tới nó có thể được thực hiện theo các trình tự thích hợp khác. Ví dụ, các khối hoặc các trạng thái được mô tả có thể được thực hiện theo thứ tự khác với thứ tự đã được bộc lộ cụ thể, hoặc nhiều khối hoặc trạng thái có thể được kết hợp thành khối hoặc trạng thái đơn. Các khối hoặc các trạng thái làm ví dụ có thể được thực hiện nối tiếp, song song, hoặc theo một số cách khác. Các khối hoặc các trạng thái có thể được thêm vào hoặc được loại bỏ khỏi các phương án thực hiện làm ví dụ đã được bộc lộ. Các hệ thống làm ví dụ và các thành phần được mô tả ở đây có thể được định cấu hình theo cách khác với cách được mô tả. Ví dụ, các thành

phần có thể được thêm vào, được loại bỏ khỏi, hoặc được sắp xếp lại khi so sánh với các phương án thực hiện làm ví dụ đã được bộc lộ.

Các thao tác khác nhau của các phương pháp làm ví dụ được mô tả ở đây có thể được thực hiện, ít nhất một phần bởi thuật toán. Thuật toán có thể được chứa trong các mã chương trình hoặc các lệnh được lưu trong bộ nhớ (ví dụ, vật ghi phi chuyển tiếp, đọc được bởi máy tính được mô tả ở trên). Thuật toán này có thể chứa thuật toán học máy. Theo một số phương án thực hiện, thuật toán học máy có thể không rõ ràng là lập trình cho máy tính để thực hiện chức năng, mà có thể học từ dữ liệu huấn luyện để tạo ra mô hình dự đoán để thực hiện chức năng.

Các thao tác khác nhau của các phương pháp làm ví dụ được mô tả ở đây có thể được thực hiện, ít nhất một phần, bởi một hoặc nhiều bộ xử lý được định cấu hình một cách tạm thời (ví dụ, bởi phần mềm) hoặc được định cấu hình một cách vĩnh viễn để thực hiện các hoạt động liên quan. Dù được định cấu hình tạm thời hay vĩnh viễn, các bộ xử lý này có thể tạo thành các cơ chế được áp dụng bộ xử lý để vận hành để thực hiện một hoặc nhiều thao tác hoặc chức năng được mô tả ở đây.

Một cách tương tự, các phương pháp được mô tả ở đây có thể được áp dụng ít nhất một phần bởi bộ xử lý, với bộ xử lý cụ thể hoặc các bộ xử lý là ví dụ của phần cứng. Ví dụ, ít nhất một số thao tác trong các thao tác của phương pháp có thể được thực hiện bởi một hoặc nhiều bộ xử lý hoặc các máy được áp dụng bởi bộ xử lý. Hơn nữa, một hoặc nhiều bộ xử lý cũng có thể vận hành để trợ giúp hoạt động của các thao tác liên quan trong môi trường "điện toán đám mây - cloud computing" hoặc phần mềm làm dịch vụ ("software as a service" - SaaS). Ví dụ, ít nhất một số thao tác trong các thao tác có thể được thực hiện bởi nhóm các máy tính (như là các ví dụ của các máy chứa các bộ xử lý), với các thao tác này là có thể truy cập được thông qua mạng (ví dụ, Internet) và thông qua một hoặc nhiều giao diện thích hợp (ví dụ, giao diện chương trình ứng dụng (Application Program Interface - API)).

Hiệu quả hoạt động của thao tác cụ thể của các thao tác có thể được phân bố giữa các bộ xử lý, không chỉ nằm trong máy đơn, mà có thể được triển khai qua nhiều máy. Theo một số phương án thực hiện làm ví dụ, các bộ xử lý hoặc các máy được áp dụng bộ xử lý có thể được định vị trong vị trí địa lý đơn (ví dụ, nằm trong môi trường nhà,

môi trường văn phòng, hoặc trại máy chủ). Theo các phương án thực hiện làm ví dụ, các bộ xử lý hoặc các máy được áp dụng bộ xử lý có thể được phân bố qua nhiều vị trí địa lý khác nhau.

Qua suốt bản mô tả này, nhiều ví dụ có thể áp dụng các thành phần, các thao tác, hoặc các cấu trúc được mô tả như là ví dụ đơn. Mặc dù các thao tác đơn của một hoặc nhiều phương pháp được minh họa và được mô tả như là các thao tác tách biệt, nhưng một hoặc nhiều thao tác của các thao tác riêng biệt có thể được thực hiện đồng thời, và không yêu cầu các thao tác phải được theo thứ tự đã được minh họa. Các cấu trúc và chức năng đã được biểu diễn như là các thành phần tách biệt trong các cấu hình làm ví dụ có thể được áp dụng làm cấu trúc hoặc thành phần được kết hợp. Một cách tương tự, các cấu trúc và chức năng được thể hiện như là thành phần đơn có thể được áp dụng như là các thành phần tách biệt. Các biến thể, biến đổi, bổ sung và cải tiến này cũng như các biến thể, biến đổi, bổ sung và cải tiến này khác sẽ nằm trong phạm vi bảo hộ của sáng chế này.

Mặc dù phần tổng quan của sáng chế này được mô tả với tham khảo tới các phương án thực hiện làm ví dụ kèm theo, nhưng các biến đổi và thay thế khác có thể được tạo ra cho các phương án thực hiện này mà không tách khỏi phạm vi bảo hộ rộng hơn của các phương án thực hiện của sáng chế này. Các phương án thực hiện này của sáng chế có thể được đề cập tới ở đây, một cách riêng rẽ hoặc cùng với nhau, bởi thuật ngữ "sáng chế" đơn thuần để tạo thuận tiện và không nhằm hạn chế phạm vi bảo hộ của sáng chế này vào phần bộc lộ hoặc khái niệm đơn nào nếu thực sự có hơn một phần như vậy được bộc lộ. Phần mô tả chi tiết không được coi là hạn chế, và phạm vi bảo hộ của các phương án thực hiện khác nhau chỉ được xác định bởi các yêu cầu bảo hộ kèm theo, cùng với toàn bộ các dạng tương đương mà các yêu cầu bảo hộ này đề cập tới.

YÊU CẦU BẢO HỘ

1. Phương pháp được thực hiện bởi máy tính để bảo vệ thông tin, được thực hiện bởi nút gửi được kết hợp với người gửi của giao dịch, phương pháp bao gồm các bước:

cam kết lượng giao dịch t của giao dịch với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, và cam kết thay đổi y của giao dịch với sơ đồ cam kết thứ hai để thu được trị số cam kết thay đổi Y, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t, và sơ đồ cam kết thứ hai bao gồm nhân tố mù thay đổi r_y;

mã hóa tổ hợp thứ nhất của nhân tố mù thay đổi r_y và thay đổi y với chìa khóa thứ nhất KA;

truyền, qua kênh an ninh ngoài chuỗi khối (blockchain), nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch;

đáp ứng lại với việc nút nhận xác thực thành công giao dịch, thu được, từ nút nhận, (1) tổ hợp thứ hai được mã hóa của nhân tố mù giao dịch r_t và lượng giao dịch t được mã hóa với chìa khóa thứ hai KB và (2) chữ ký SIGB được sinh ra bởi nút nhận ký ít nhất tổ hợp thứ hai được mã hóa và trị số cam kết giao dịch T với chìa khóa riêng của người nhận;

sinh ra chữ ký SIGA bằng cách ký ít nhất tổ hợp thứ nhất và trị số cam kết giao dịch T với chìa khóa riêng của người gửi; và

truyền thông tin giao dịch bao gồm tổ hợp thứ nhất được mã hóa, tổ hợp thứ hai được mã hóa, trị số cam kết giao dịch T, trị số cam kết thay đổi Y, chữ ký SIGA, và chữ ký SIGB tới nhiều nút trong chuỗi khối cho các nút trong chuỗi khối để xác thực thông tin giao dịch và bổ sung thông tin giao dịch vào chuỗi khối.

2. Phương pháp theo điểm 1, trong đó:

sơ đồ cam kết thứ nhất bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù giao dịch r_t và với lượng giao dịch t đang là trị số được cam kết tương ứng; và

sơ đồ cam kết thứ hai bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù thay đổi r_y và với thay đổi y đang là trị số được cam kết tương ứng.

3. Phương pháp theo điểm 1 hoặc 2, trong đó bước truyền, qua kênh an ninh ngoài chuỗi khối, nhân tố mù giao dịch rt, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch bao gồm:

truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch, làm cho nút nhận xác thực nếu trị số cam kết giao dịch T là bằng với sơ đồ cam kết thứ nhất cam kết lượng giao dịch t với nhân tố mù giao dịch r_t.

4. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó:

lượng giao dịch t được rút ra từ một hoặc nhiều tài sản A_1, A_2, ..., A_k của người gửi của giao dịch;

mỗi tài sản trong các tài sản được kết hợp với (1) cam kết Pedersen dựa ít nhất trên nhân tố mù r_{ak} và trị số của từng tài sản và (2) việc mã hóa dựa ít nhất trên nhân tố mù r_{ak} và trị số của từng tài sản; và

thay đổi y là khác biệt giữa lượng giao dịch t và các tài sản được rút ra.

5. Phương pháp theo điểm 4 mà phụ thuộc điểm 3, trong đó, bước sinh ra chữ ký SIGA bằng cách ký ít nhất tổ hợp thứ nhất và trị số cam kết giao dịch T với chìa khóa riêng của người gửi bao gồm:

xác thực chữ ký SIGB; và

đáp ứng lại với việc xác thực thành công chữ ký SIGB, ký ít nhất các tài sản A_1, A_2, ..., A_k, tổ hợp thứ nhất, tổ hợp thứ hai, trị số cam kết giao dịch T, trị số cam kết thay đổi Y, và khác biệt giữa tổng của các nhân tố mù tương ứng với các tài sản A_1, A_2, ..., A_k và tổng của nhân tố mù giao dịch r_t và nhân tố mù thay đổi r_y với chìa khóa riêng của người gửi.

6. Phương pháp theo điểm 5, trong đó thông tin giao dịch bao gồm:

các tài sản A_1, A_2, ..., A_k, tổ hợp thứ nhất được mã hóa, tổ hợp thứ hai được mã hóa, trị số cam kết giao dịch T, trị số cam kết thay đổi Y, khác biệt giữa tổng của các nhân tố mù tương ứng với các tài sản A_1, A_2, ..., A_k và tổng của nhân tố mù giao dịch r_t và nhân tố mù thay đổi r_y, chữ ký SIGA, và chữ ký SIGB.

7. Phương pháp theo điểm 6, trong đó bước truyền thông tin giao dịch tới nhiều nút trong chuỗi khối cho các nút trong chuỗi khối để xác thực thông tin giao dịch bao gồm:

truyền thông tin giao dịch tới nhiều nút trong chuỗi khối, làm cho các nút trong chuỗi khối, đáp ứng lại với việc xác thực thành công giao dịch, đưa ra lượng giao dịch t tới người nhận, loại bỏ các tài sản A_1, A_2, ..., A_k, và đưa ra thay đổi y tới người gửi.

8. Vật ghi phi chuyển tiếp, đọc được bởi máy tính lưu các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho bộ xử lý thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 7.

9. Hệ thống để bảo vệ thông tin, bao gồm bộ xử lý và vật ghi phi chuyển tiếp, đọc được bởi máy tính được ghép nối tới bộ xử lý, vật ghi lưu các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho hệ thống thực hiện, bởi nút gửi được kết hợp với người gửi của giao dịch, các thao tác bao gồm:

cam kết lượng giao dịch t của giao dịch với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, và cam kết thay đổi y của giao dịch với sơ đồ cam kết thứ hai để thu được trị số cam kết thay đổi Y, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t, và sơ đồ cam kết thứ hai bao gồm nhân tố mù thay đổi r_y;

mã hóa tổ hợp thứ nhất của nhân tố mù thay đổi r_y và thay đổi y với chìa khóa thứ nhất KA;

truyền, qua kênh an ninh ngoài chuỗi khối (blockchain), nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch;

đáp ứng lại với việc nút nhận xác thực thành công giao dịch, thu được, từ nút nhận, (1) tổ hợp thứ hai được mã hóa của nhân tố mù giao dịch r_t và lượng giao dịch t được mã hóa với chìa khóa thứ hai KB và (2) chữ ký SIGB được sinh ra bởi nút nhận

ký ít nhất tổ hợp thứ hai được mã hóa và trị số cam kết giao dịch T với chìa khóa riêng của người nhận;

sinh ra chữ ký SIGA bằng cách ký ít nhất tổ hợp thứ nhất và trị số cam kết giao dịch T với chìa khóa riêng của người gửi;

truyền thông tin giao dịch bao gồm tổ hợp thứ nhất được mã hóa, tổ hợp thứ hai được mã hóa, trị số cam kết giao dịch T, trị số cam kết thay đổi Y, chữ ký SIGA, và chữ ký SIGB tới nhiều nút trong chuỗi khối cho các nút trong chuỗi khối để xác thực thông tin giao dịch và bổ sung thông tin giao dịch vào chuỗi khối.

10. Phương pháp được thực hiện bởi máy tính để bảo vệ thông tin, được thực hiện bởi nút nhận được kết hợp với người nhận của giao dịch, phương pháp bao gồm các bước:

thu được, qua kênh an ninh ngoài chuỗi khối, nhân tố mù giao dịch r_t, lượng giao dịch t của giao dịch, và trị số cam kết giao dịch T từ nút gửi được kết hợp với người gửi của giao dịch, trong đó: lượng giao dịch t được cam kết với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t;

xác thực giao dịch dựa trên nhân tố mù giao dịch r_t thu được, lượng giao dịch t thu được của giao dịch, và trị số cam kết giao dịch T thu được;

đáp ứng lại với việc xác thực thành công giao dịch, mã hóa tổ hợp thứ hai của nhân tố mù giao dịch r_t và lượng giao dịch t với chìa khóa thứ hai KB;

sinh ra chữ ký SIGB bằng cách ký ít nhất tổ hợp thứ hai được mã hóa và trị số cam kết giao dịch T với chìa khóa riêng của người nhận, chữ ký SIGB chỉ thị rằng người nhận đồng ý với giao dịch; và

truyền tổ hợp thứ hai được mã hóa và chữ ký SIGB tới nút gửi để truyền tới chuỗi khối.

11. Phương pháp theo điểm 10, trong đó:

xác thực giao dịch dựa trên nhân tố mù giao dịch r_t thu được, lượng giao dịch t thu được của giao dịch, và trị số cam kết giao dịch T thu được bao gồm xác thực nếu trị số cam kết giao dịch T thu được là bằng với sơ đồ cam kết thứ nhất cam kết lượng giao dịch t thu được với nhân tố mù giao dịch r_t thu được.

12. Phương pháp theo điểm 10 hoặc 11, trong đó:

sơ đồ cam kết thứ nhất bao gồm cam kết Pedersen dựa ít nhất trên nhân tố mù giao dịch r_t và với lượng giao dịch t đang là trị số được cam kết tương ứng.

13. Vật ghi phi chuyển tiếp, đọc được bởi máy tính lưu các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho bộ xử lý thực hiện phương pháp theo điểm 10.

14. Hệ thống để bảo vệ thông tin, bao gồm bộ xử lý và vật ghi phi chuyển tiếp, đọc được bởi máy tính được ghép nối tới bộ xử lý, vật ghi lưu các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho hệ thống thực hiện phương pháp theo điểm 10.

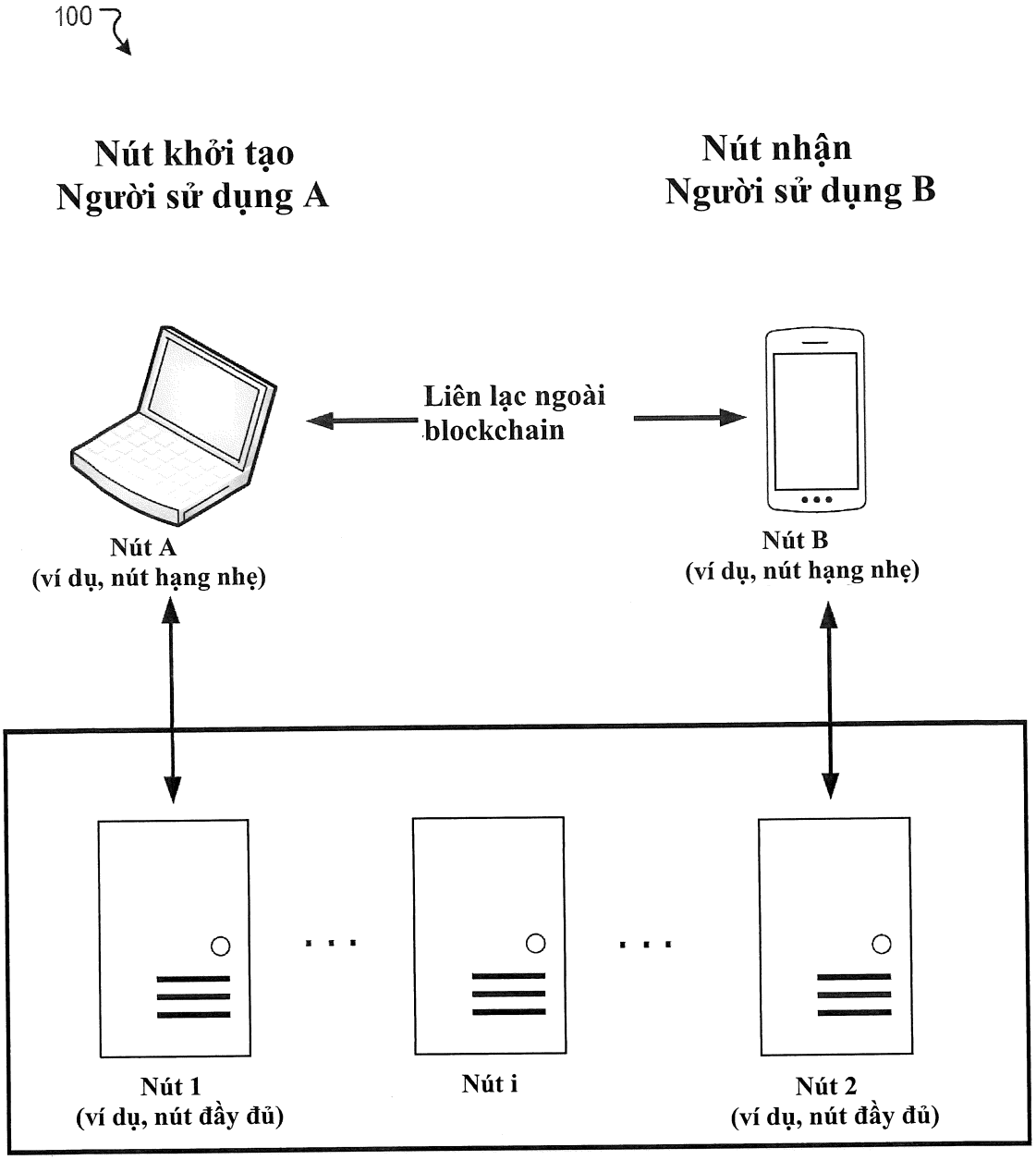
100
Nút khởi tạo
Người sử dụng A
Nút nhận
Người sử dụng B
Liên lạc ngoài blockchain
Nút A
(ví dụ, nút hạng nhẹ)
Nút B
(ví dụ, nút hạng nhẹ)
Nút 1
(ví dụ, nút đầy đủ)
Nút i
Nút 2
(ví dụ, nút đầy đủ)

FIG. 1

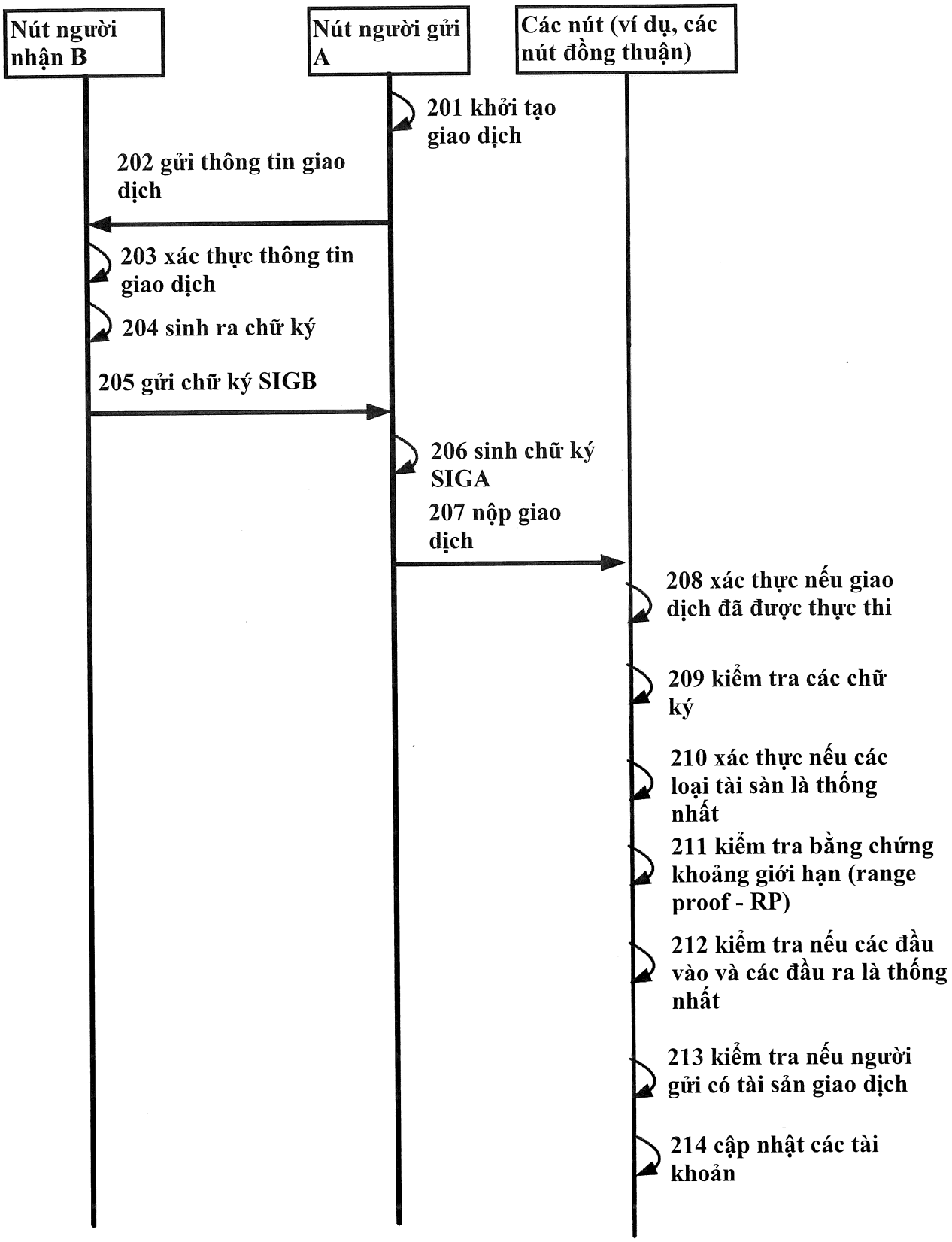
Nút người nhận B
Nút người gửi A
Các nút (ví dụ, các nút đồng thuận)
201 khởi tạo giao dịch
202 gửi thông tin giao dịch
203 xác thực thông tin giao dịch
204 sinh ra chữ ký
205 gửi chữ ký SIGB
206 sinh chữ ký SIGA
207 nộp giao dịch
208 xác thực nếu giao dịch đã được thực thi
209 kiểm tra các chữ ký
210 xác thực nếu các loại tài sàn là thống nhất
211 kiểm tra bằng chứng khoảng giới hạn (range proof - RP)
212 kiểm tra nếu các đầu vào và các đầu ra là thống nhất
213 kiểm tra nếu người gửi có tài sản giao dịch
214 cập nhật các tài khoản

FIG. 2

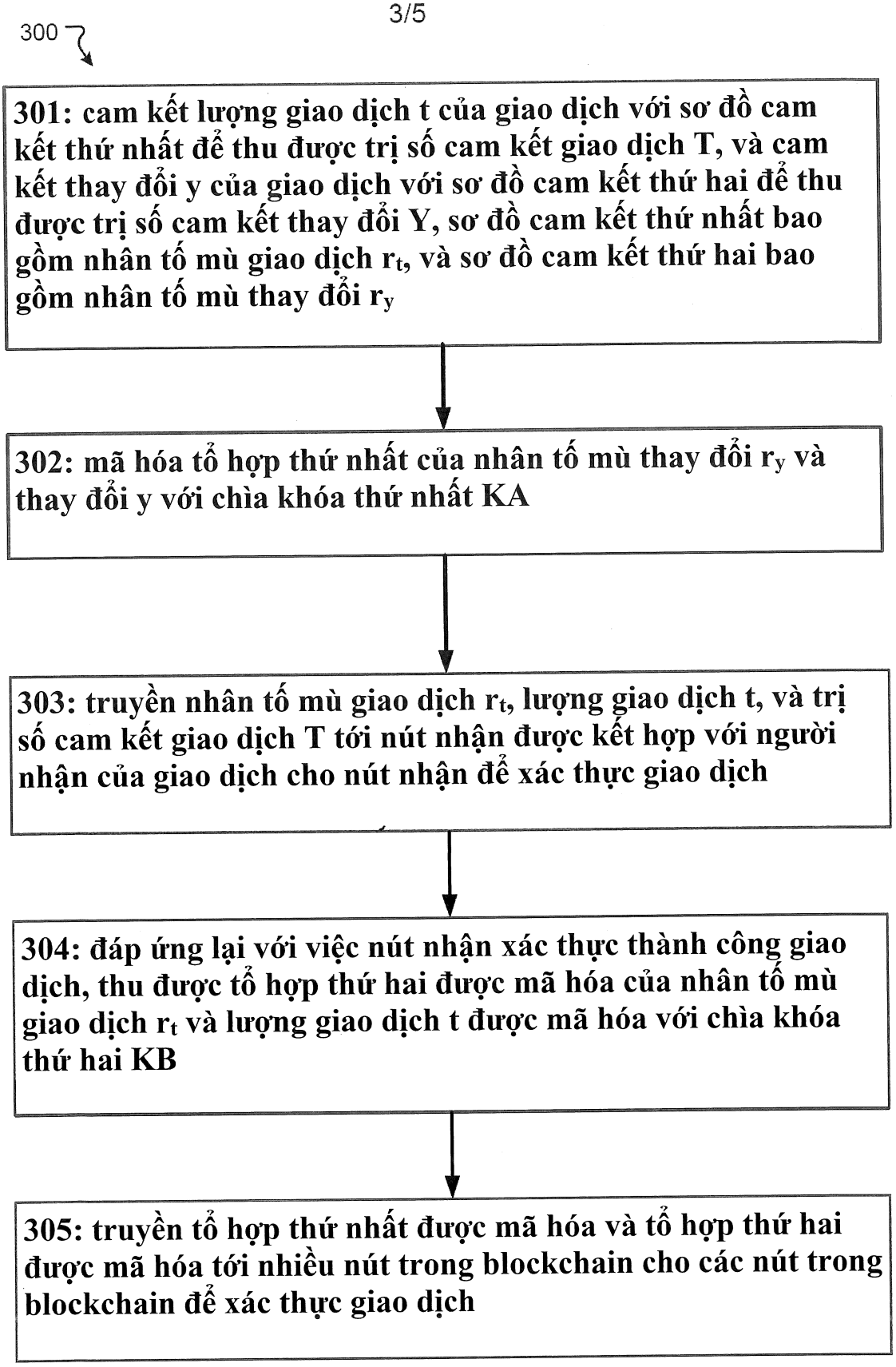
300
301: cam kết lượng giao dịch t của giao dịch với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, và cam kết thay đổi y của giao dịch với sơ đồ cam kết thứ hai để thu được trị số cam kết thay đổi Y, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t, và sơ đồ cam kết thứ hai bao gồm nhân tố mù thay đổi r_y
302: mã hóa tổ hợp thứ nhất của nhân tố mù thay đổi r_y và thay đổi y với chìa khóa thứ nhất KA
303: truyền nhân tố mù giao dịch r_t, lượng giao dịch t, và trị số cam kết giao dịch T tới nút nhận được kết hợp với người nhận của giao dịch cho nút nhận để xác thực giao dịch
304: đáp ứng lại với việc nút nhận xác thực thành công giao dịch, thu được tổ hợp thứ hai được mã hóa của nhân tố mù giao dịch r_t và lượng giao dịch t được mã hóa với chìa khóa thứ hai KB
305: truyền tổ hợp thứ nhất được mã hóa và tổ hợp thứ hai được mã hóa tới nhiều nút trong blockchain cho các nút trong blockchain để xác thực giao dịch

FIG. 3

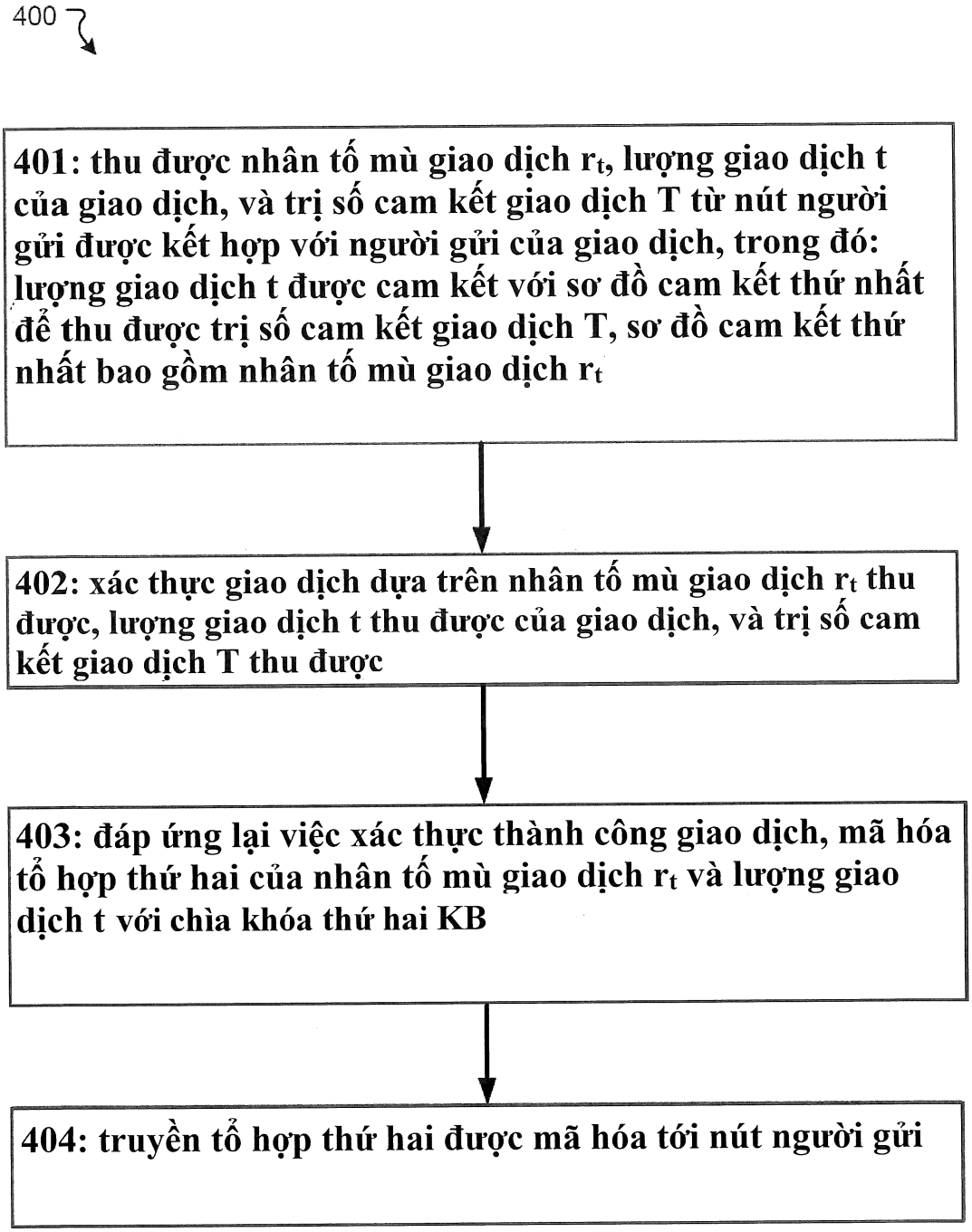
400
401: thu được nhân tố mù giao dịch r_t, lượng giao dịch t của giao dịch, và trị số cam kết giao dịch T từ nút người gửi được kết hợp với người gửi của giao dịch, trong đó: lượng giao dịch t được cam kết với sơ đồ cam kết thứ nhất để thu được trị số cam kết giao dịch T, sơ đồ cam kết thứ nhất bao gồm nhân tố mù giao dịch r_t
402: xác thực giao dịch dựa trên nhân tố mù giao dịch r_t thu được, lượng giao dịch t thu được của giao dịch, và trị số cam kết giao dịch T thu được
403: đáp ứng lại việc xác thực thành công giao dịch, mã hóa tổ hợp thứ hai của nhân tố mù giao dịch r_t và lượng giao dịch t với chìa khóa thứ hai KB
404: truyền tổ hợp thứ hai được mã hóa tới nút người gửi

FIG. 4

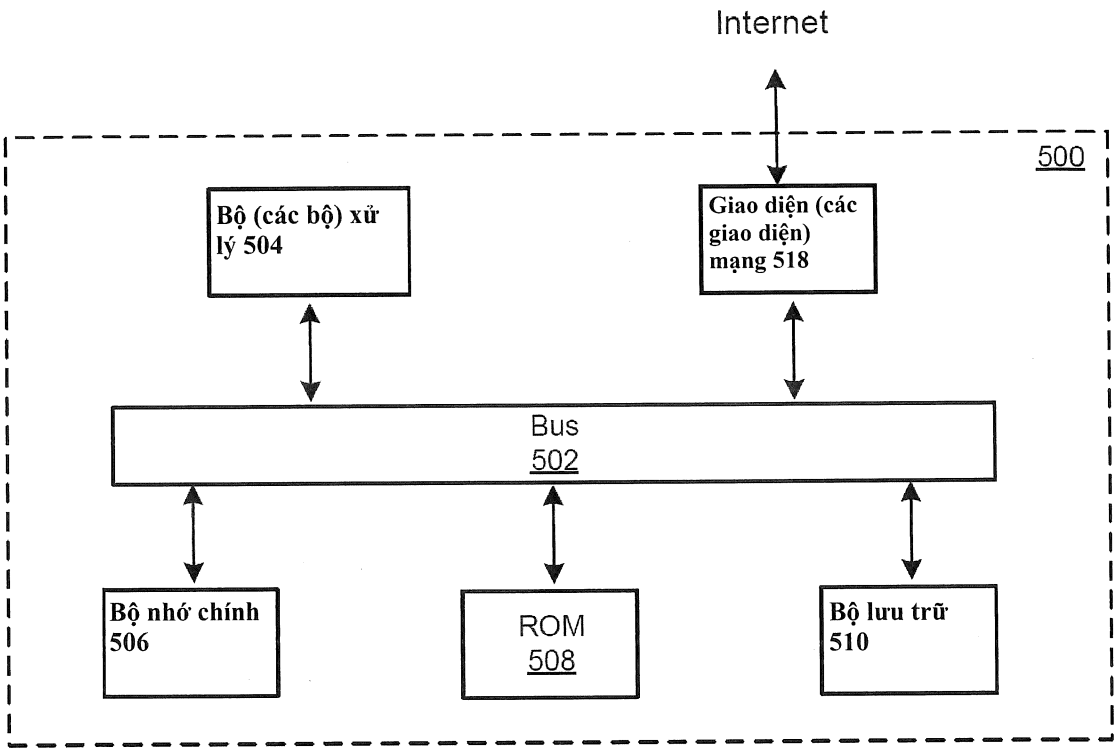
Internet
500
Bộ (các bộ) xử lý 504
Giao diện (các giao diện) mạng 518
Bus
502
Bộ nhớ chính
506
ROM
508
Bộ lưu trữ
510

FIG. 5