(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) **1-0031105**

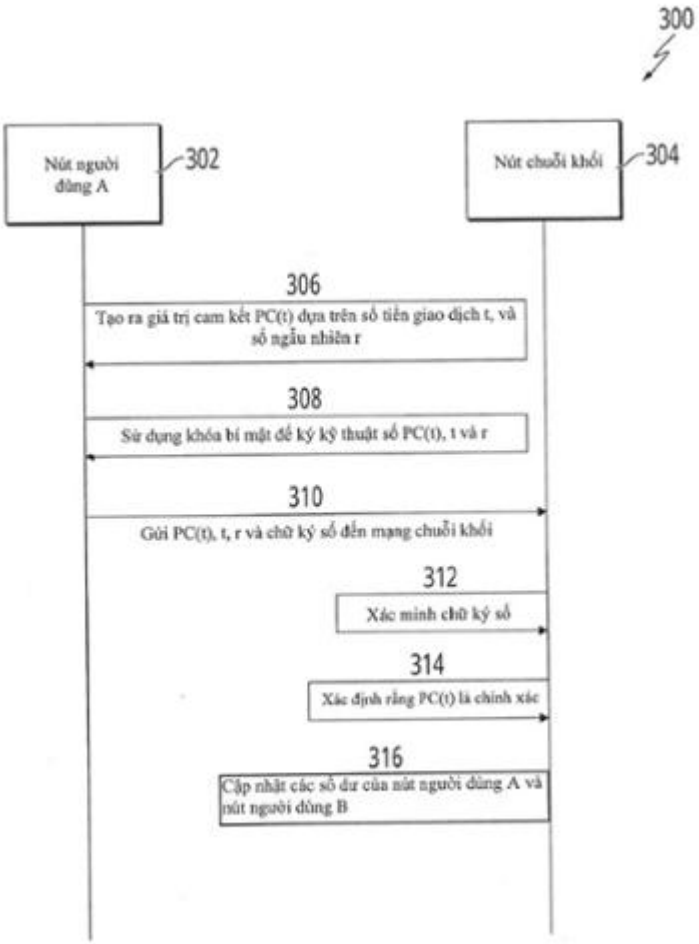
(51)[2020.01] G06Q 20/10

(13) **B**

(21) 1-2019-02018
(22) 07/11/2018
(86) PCT/CN2018/114401 07/11/2018
(87) WO 2019/072265 18/04/2019
(45) 25/02/2022 407
(43) 25/05/2020 386ASC
(73) Advanced New Technologies Co., Ltd. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) MA, Baoli (CN); ZHANG, Wenbin (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG ĐỂ XÁC NHẬN CÁC GIAO DỊCH CHUỖI KHỐI DỰA TRÊN CÁC MÔ HÌNH TÀI KHOẢN VÀ VẬT GHI ĐỌC ĐƯỢC BẰNG MÁY TÍNH LÂU DÀI

(57) Sáng chế đề cập đến phương pháp được thực hiện bằng máy tính bao gồm bước nhận dữ liệu giao dịch và chữ ký số của dữ liệu giao dịch bởi nút đồng thuận của chuỗi khối. Sáng chế đề cập đến vật ghi đọc được bằng máy tính lâu dài được ghép nối với một hoặc nhiều bộ xử lý và có các lệnh được lưu trữ trên đó, khi được thực hiện bởi một hoặc nhiều bộ xử lý, thì khiến cho một hoặc nhiều bộ xử lý thực hiện các hoạt động theo phương pháp nêu trên. Sáng chế còn đề cập đến hệ thống bao gồm thiết bị tính toán; và thiết bị lưu trữ đọc được bằng máy tính được ghép nối với thiết bị tính toán và có các lệnh được lưu trữ trên đó, khi được thực hiện bởi thiết bị tính toán, thì khiến cho thiết bị tính toán này thực hiện các hoạt động theo phương pháp nêu trên.


300
Nút người dùng A
302
Nút chuỗi khối
304
306
Tạo ra giá trị cam kết PC(t) dựa trên số tiền giao dịch t, và số ngẫu nhiên r
308
Sử dụng khóa bí mật để ký kỹ thuật số PC(t), t và r
310
Gửi PC(t), t, r và chữ ký số đến mạng chuỗi khối
312
Xác minh chữ ký số
314
Xác định rằng PC(t) là chính xác
316
Cập nhật các số dư của nút người dùng A và nút người dùng B

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp và hệ thống để xác nhận các giao dịch chuỗi khối dựa trên các mô hình tài khoản. Sáng chế còn đề cập đến vật ghi lưu trữ đọc được bằng máy tính lâu dài được ghép nối với một hoặc nhiều bộ xử lý và có các lệnh được lưu trữ trên đó, khi được thực hiện bởi một hoặc nhiều bộ xử lý, thì khiến cho một hoặc nhiều bộ xử lý này thực hiện các hoạt động theo phương pháp nêu trên.

Tình trạng kỹ thuật của sáng chế

Các mạng chuỗi khối, có thể còn được gọi là các hệ thống chuỗi khối, mạng đồng thuận, mạng hệ thống sổ cái phân tán (distributed ledger system - DLS), hoặc chuỗi khối, cho phép các thực thể tham gia lưu trữ dữ liệu một cách an toàn và bất biến. Chuỗi khối có thể được mô tả dưới dạng sổ cái của các giao dịch, và nhiều bản sao của chuỗi khối được lưu trữ qua mạng chuỗi khối. Các kiểu chuỗi khối làm ví dụ có thể bao gồm các chuỗi khối công khai và chuỗi khối bí mật. Chuỗi khối công khai được mở cho tất cả các thực thể sử dụng chuỗi khối, và tham gia vào quá trình đồng thuận. Chuỗi khối bí mật được tạo ra cho thực thể cụ thể, kiểm soát một cách tập trung các quyền đọc và ghi.

Các chuỗi khối được sử dụng trong các mạng tiền mã hóa, mà cho phép các bên tham gia thực hiện các giao dịch mua/bán hàng hóa và/hoặc dịch vụ sử dụng tiền mã hóa. Tiền mã hóa chung bao gồm Bitcoin. Trong các mạng tiền mã hóa, các mẫu giữ bản ghi được sử dụng để ghi các giao dịch giữa những người dùng. Các mô hình giữ bản ghi làm ví dụ bao gồm mô hình đầu ra giao dịch chưa chi tiêu (unspent transaction output - UTXO) và mô hình số dư tài khoản. Trong mô hình UTXO, mỗi giao dịch chi tiêu đầu ra từ các giao dịch trước và tạo ra các đầu ra mới mà có thể được chi tiêu trong các giao dịch tiếp theo. Các giao dịch chưa chi tiêu của người dùng được theo dõi, và số dư mà người dùng phải chi tiêu được tính toán dưới dạng tổng giao dịch chưa chi tiêu. Trong mô hình số dư tài khoản, mỗi số dư tài khoản của người dùng được theo dõi dưới dạng trạng thái chung. Đối với mỗi giao dịch, số dư của tài khoản chi tiêu được kiểm tra để

đảm bảo số dư này lớn hơn hoặc bằng số tiền giao dịch. Điều này so sánh được với ngân hàng truyền thống.

Chuỗi khối bao gồm một loạt khối, mỗi trong số các khối này chứa một hoặc nhiều giao dịch được thực hiện trong mạng. Mỗi khối có thể được tương tự hóa với trang của sổ cái, trong đó chính chuỗi khối là bản sao đầy đủ của sổ cái. Các giao dịch riêng biệt được xác nhận và thêm vào khối, các giao dịch này được thêm vào chuỗi khối. Các bản sao của chuỗi khối được sao chép qua tất cả các nút của mạng. Theo cách này, có sự đồng thuận chung về trạng thái của chuỗi khối. Hơn nữa, chuỗi khối được mở cho tất cả các nút để xem, ít nhất là trong trường hợp các mạng công khai. Để bảo vệ tính riêng tư của người dùng chuỗi khối, các công nghệ mã hóa được thực hiện.

Bản chất kỹ thuật của sáng chế

Các phương án thực hiện của sáng chế bao gồm các phương pháp được thực hiện bằng máy tính để bảo vệ tính riêng tư của dữ liệu giao dịch công khai và bí mật theo mô hình số dư tài khoản của mạng chuỗi khối. Cụ thể hơn, các phương án thực hiện của sáng chế được đề xuất trực tiếp để cho phép các giao dịch bí mật và giao dịch công khai theo mô hình số dư tài khoản trong mạng chuỗi khối. Theo cách này, và như được mô tả một cách chi tiết hơn ở đây, những người dùng có thể tự do lựa chọn xem mỗi giao dịch là giao dịch công khai, hay giao dịch bí mật trong mạng chuỗi khối.

Theo một số phương án thực hiện, các hoạt động bao gồm bước nhận dữ liệu giao dịch và chữ ký số của dữ liệu giao dịch bằng nút đồng thuận của mạng chuỗi khối, trong đó dữ liệu giao dịch này bao gồm giá trị cam kết, số ngẫu nhiên và số tiền giao dịch cần được chuyển từ một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ nhất sang một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ hai, và trong đó chữ ký số được tạo ra bằng cách ký kỹ thuật số dữ liệu giao dịch sử dụng khóa bí mật của nút người dùng thứ nhất và giá trị cam kết được tạo ra dựa trên số ngẫu nhiên và số tiền giao dịch sử dụng sơ đồ cam kết; xác minh chữ ký số của dữ liệu giao dịch sử dụng khóa công khai của nút người dùng thứ nhất; và xác định rằng số tiền giao dịch này là hợp lệ, nếu giá trị cam kết là chính xác dựa trên số ngẫu nhiên và sơ đồ cam kết, và số tiền giao dịch này nhỏ hơn hoặc bằng số dư của một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ nhất trước khi chuyển số tiền giao dịch. Các phương án thực hiện khác bao gồm các hệ thống, thiết bị và chương trình máy

tính tương ứng, được tạo cấu hình để thực hiện các hoạt động của phương pháp, được mã hóa trên các thiết bị lưu trữ của máy tính.

Mỗi trong số các phương án thực hiện này và các phương án thực hiện khác có thể tùy ý bao gồm một hoặc nhiều dấu hiệu trong số các dấu hiệu sau:

Dấu hiệu thứ nhất, kết hợp được với dấu hiệu bất kỳ trong số các dấu hiệu sau, trong đó tài khoản công có số dư công khai xem được bởi nút đồng thuận, và tài khoản riêng có số dư riêng xem được sử dụng khóa bí mật của nút người dùng tương ứng.

Dấu hiệu thứ hai, kết hợp được với dấu hiệu bất kỳ trong số các dấu hiệu trước đó dấu hiệu sau, trong đó số tiền giao dịch là từ tài khoản công được kết hợp với nút người dùng thứ nhất sang tài khoản riêng được kết hợp với nút người dùng thứ hai.

Dấu hiệu thứ ba, kết hợp được với dấu hiệu bất kỳ trong số các dấu hiệu trước đó dấu hiệu sau, trong đó số tiền giao dịch là từ tài khoản riêng của nút người dùng thứ nhất sang tài khoản công của nút người dùng thứ hai, và phương pháp này còn bao gồm bước: nhận, từ nút người dùng thứ nhất, bằng chứng phạm vi để chứng minh rằng số tiền giao dịch nhỏ hơn hoặc bằng số dư của tài khoản riêng của nút người dùng thứ nhất; và trong đó bước chuyển được xác định là hợp lệ, nếu số tiền giao dịch này nhỏ hơn hoặc bằng số dư của tài khoản riêng của nút người dùng thứ nhất dựa trên bằng chứng phạm vi.

Dấu hiệu thứ tư, kết hợp được với dấu hiệu bất kỳ trong số các dấu hiệu trước đó dấu hiệu sau, phương pháp này còn bao gồm bước cập nhật số dư của một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ nhất, và số dư của một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ hai dựa trên số tiền giao dịch, nếu bước chuyển là hợp lệ.

Dấu hiệu thứ năm, kết hợp được với dấu hiệu bất kỳ trong số các dấu hiệu trước đó dấu hiệu sau, trong đó số dư của tài khoản riêng được cập nhật dựa trên giá trị cam kết của số tiền giao dịch và cam kết về số dư của tài khoản riêng được tạo ra bằng cách sử dụng sơ đồ cam kết.

Dấu hiệu thứ sáu, kết hợp được với dấu hiệu bất kỳ trong số các dấu hiệu trước đó dấu hiệu sau, trong đó sơ đồ cam kết là đồng cấu.

Sáng chế còn đề xuất hệ thống để thực hiện các phương pháp được đề xuất ở đây. Hệ thống này bao gồm một hoặc nhiều bộ xử lý, và vật ghi đọc được bằng máy tính được ghép nối với một hoặc nhiều bộ xử lý có các lệnh được lưu trữ trên đó, khi được thực hiện bởi một hoặc nhiều bộ xử lý, thì khiến cho một hoặc nhiều bộ xử lý thực hiện các hoạt động theo các phương án thực hiện của các phương pháp được đề xuất ở đây.

Đánh giá được rằng các phương pháp theo sáng chế có thể bao gồm sự kết hợp bất kỳ của các khía cạnh và dấu hiệu được mô tả ở đây. Nghĩa là, các phương pháp theo sáng chế không bị giới hạn ở sự kết hợp của các khía cạnh và dấu hiệu được mô tả cụ thể ở đây, mà còn bao gồm sự kết hợp bất kỳ của các khía cạnh và dấu hiệu được đề xuất.

Các chi tiết về một hoặc nhiều phương án thực hiện của sáng chế được nêu trên các hình vẽ kèm theo và phần mô tả dưới đây. Các dấu hiệu và ưu điểm khác của sáng chế sẽ là rõ ràng nhờ phần mô tả và các hình vẽ, và từ các điểm yêu cầu bảo hộ.

Mô tả vắn tắt các hình vẽ

Fig.1 mô tả môi trường làm ví dụ mà có thể được sử dụng để thực hiện các phương án thực hiện của sáng chế.

Fig.2 mô tả kiến trúc về khái niệm làm ví dụ theo các phương án thực hiện của sáng chế.

Fig.3 mô tả quy trình xác nhận làm ví dụ của giao dịch chuỗi khối theo các phương án thực hiện của sáng chế.

Fig.4 mô tả giao dịch chuỗi khối làm ví dụ từ tài khoản công sang tài khoản riêng theo các phương án thực hiện của sáng chế.

Fig.5 mô tả giao dịch chuỗi khối làm ví dụ từ tài khoản riêng sang tài khoản công theo các phương án thực hiện của sáng chế.

Fig.6 mô tả phương pháp làm ví dụ mà có thể được thực hiện theo các phương án thực hiện của sáng chế.

Các ký hiệu chỉ dẫn giống nhau trên các hình vẽ khác nhau biểu thị các bộ phận giống nhau.

Mô tả chi tiết sáng chế

Các phương án thực hiện của sáng chế bao gồm các phương pháp được thực hiện bằng máy tính để bảo vệ tính riêng tư của dữ liệu giao dịch công khai và bí mật theo mô hình số dư tài khoản (còn được gọi ở đây là mô hình tài khoản) của mạng chuỗi khối. Cụ thể hơn, các phương án thực hiện của sáng chế được đề xuất trực tiếp để cho phép các giao dịch bí mật và giao dịch công khai theo mô hình số dư tài khoản nằm trong mạng chuỗi khối. Theo cách này và như được mô tả một cách chi tiết hơn ở đây, những người dùng có thể tự do lựa chọn xem mỗi giao dịch là giao dịch công khai hay giao dịch bí mật trong mạng chuỗi khối. Theo một số phương án thực hiện, các hoạt động bao gồm các bước: nhận dữ liệu giao dịch và chữ ký số của dữ liệu giao dịch bằng nút đồng thuận của mạng chuỗi khối, trong đó dữ liệu giao dịch này bao gồm giá trị cam kết, số ngẫu nhiên và số tiền giao dịch cần chuyển từ một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ nhất sang một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ hai, và trong đó chữ ký số được tạo ra bằng cách ký kỹ thuật số dữ liệu giao dịch sử dụng khóa bí mật của nút người dùng thứ nhất và giá trị cam kết được tạo ra dựa trên số ngẫu nhiên và số tiền giao dịch sử dụng sơ đồ cam kết; xác minh chữ ký số của dữ liệu giao dịch bằng cách sử dụng khóa công khai của nút người dùng thứ nhất; và xác định rằng số tiền giao dịch này là hợp lệ, nếu giá trị cam kết là chính xác dựa trên số ngẫu nhiên và sơ đồ cam kết, và số tiền giao dịch nhỏ hơn hoặc bằng số dư của một trong số các tài khoản công hoặc tài khoản riêng của nút người dùng thứ nhất trước khi chuyển số tiền giao dịch.

Để tạo ra thêm ngữ cảnh cho các phương án thực hiện của sáng chế và như được đưa ra ở trên, các mạng chuỗi khối, có thể còn được gọi là các mạng đồng thuận (ví dụ, được tạo thành từ các nút ngang hàng), hệ thống sổ cái phân tán hoặc chuỗi khối đơn giản, cho phép các thực thể tham gia thực hiện các giao dịch và lưu trữ dữ liệu một cách an toàn và bất biến. Chuỗi khối có thể được tạo ra dưới dạng chuỗi khối công khai, chuỗi khối bí mật hoặc chuỗi khối tập đoàn. Các phương án thực hiện của sáng chế được mô tả một cách chi tiết hơn ở đây dựa trên chuỗi khối công khai, là công khai giữa các thực thể tham gia. Tuy nhiên, dự tính được rằng các phương án thực hiện của sáng chế có thể được thực hiện trong kiểu chuỗi khối thích hợp bất kỳ.

Trong chuỗi khối công khai, quy trình đồng thuận được điều khiển bởi các nút của mạng đồng thuận. Ví dụ, hàng trăm, hàng nghìn, thậm chí hàng triệu thực thể có thể

tham gia vào chuỗi khối công khai, mỗi trong số các thực thể này vận hành ít nhất một nút trong chuỗi khối công khai. Theo đó, chuỗi khối công khai có thể được xem là mạng công khai đối với các thực thể tham gia. Trong một số ví dụ, phần lớn các thực thể (các nút) phải ký vào mọi khối theo thứ tự để khối này là hợp lệ và được thêm vào chuỗi khối. Chuỗi khối công khai làm ví dụ bao gồm chuỗi khối được sử dụng trong mạng Bitcoin, là mạng thanh toán ngang hàng (mạng tiền mã hóa). Mặc dù thuật ngữ chuỗi khối thường tham chiếu cùng với mạng Bitcoin, như được sử dụng ở đây, chuỗi khối thường đề cập đến các sổ cái phân tán mà không tham chiếu cụ thể đến mạng Bitcoin.

Nói chung, chuỗi khối công khai hỗ trợ các giao dịch công khai. Giao dịch công khai được chia sẻ với tất cả các nút trong chuỗi khối vì chuỗi khối này được sao chép qua tất cả các nút. Nghĩa là, tất cả các nút ở trạng thái đồng thuận hoàn hảo đối với chuỗi khối. Để đạt được sự đồng thuận (ví dụ, đồng ý bổ sung khối vào chuỗi khối), giao thức đồng thuận được thực hiện trong mạng chuỗi khối. Giao thức đồng thuận làm ví dụ bao gồm, không làm giới hạn, bằng chứng công việc (proof-of-work - POW) được thực hiện trong mạng Bitcoin.

Các phương án thực hiện của sáng chế được mô tả một cách chi tiết hơn ở đây theo quan điểm của ngữ cảnh nêu trên. Cụ thể hơn, và như được đưa ra ở trên, các phương án thực hiện của sáng chế được đề xuất trực tiếp để cho phép các giao dịch bí mật và giao dịch công khai theo mô hình số dư tài khoản trong mạng chuỗi khối. Theo cách này và như được mô tả một cách chi tiết hơn ở đây, những người dùng có thể tự do lựa chọn xem mỗi giao dịch là giao dịch công khai hay giao dịch bí mật trong mạng chuỗi khối.

Theo các phương án thực hiện của sáng chế, các cấu trúc tài khoản dựa trên các mô hình tài khoản cho phép các giao dịch giữa các tài khoản công, các giao dịch giữa các tài khoản riêng và các giao dịch giữa các tài khoản công và bí mật. Sơ đồ bảo vệ tính riêng tư thích hợp có thể được thực hiện đối với các kiểu tài khoản khác nhau. Theo cách này, người dùng (ví dụ, nút trong mạng) có thể chọn xem thực hiện các giao dịch bằng cách sử dụng tài khoản công hay tài khoản riêng dựa trên tùy chọn quyền riêng.

Tài khoản công có thể có số dư tài khoản xem được bởi các nút đồng thuận. Tài khoản riêng có thể có số dư tài khoản xem được bằng cách sử dụng khóa bí mật của chủ sở hữu (người dùng) tài khoản. Số dư tài khoản riêng có thể được mã hóa bằng cách sử

dụng mã hóa đồng cấu, hoặc được cam kết bằng sơ đồ cam kết với tính đồng cấu. Như vậy, số dư tài khoản riêng không thể được xác định bởi các nút khác trong mạng chuỗi khối. Số tiền giao dịch được tạo ra cho hoặc từ tài khoản riêng cũng có thể được ẩn dựa trên sơ đồ cam kết để cập nhật số dư tài khoản riêng dựa trên sự mã hóa đồng cấu.

Fig.1 mô tả môi trường 100 làm ví dụ mà có thể được sử dụng để thực hiện các phương án thực hiện của sáng chế. Trong một số ví dụ, môi trường 100 làm ví dụ cho phép các thực thể tham gia vào chuỗi khối công khai 102. Môi trường 100 làm ví dụ này bao gồm các hệ thống tính toán 106, 108 và mạng 110. Trong một số ví dụ, mạng 110 bao gồm mạng vùng cục bộ (local area network - LAN), mạng diện rộng (wide area network - WAN), Internet, hoặc sự kết hợp của các mạng này, và kết nối các trang web, thiết bị người dùng (ví dụ, các thiết bị tính toán) và hệ thống nền. Trong một số ví dụ, mạng 110 có thể được truy cập qua liên kết truyền thông có dây và/hoặc không dây.

Trong ví dụ đã mô tả, mỗi trong số các hệ thống tính toán 106, 108 có thể bao gồm hệ thống tính toán thích hợp bất kỳ mà cho phép tham gia dưới dạng nút trong chuỗi khối công khai 102. Các thiết bị tính toán làm ví dụ bao gồm, không làm giới hạn, máy chủ, máy tính để bàn, máy tính xách tay, thiết bị tính toán dạng bảng và điện thoại thông minh. Trong một số ví dụ, các hệ thống tính toán 106, 108 làm chủ một hoặc nhiều dịch vụ được thực hiện bằng máy tính để tương tác với chuỗi khối công khai 102. Ví dụ, hệ thống tính toán 106 có thể làm chủ các dịch vụ được thực hiện bằng máy tính của thực thể thứ nhất (ví dụ, người dùng A), chẳng hạn như hệ thống quản lý giao dịch mà thực thể thứ nhất sử dụng để quản lý giao dịch của nó với một hoặc nhiều thực thể khác (ví dụ, những người dùng khác). Hệ thống tính toán 108 có thể làm chủ các dịch vụ được thực hiện bằng máy tính của thực thể thứ hai (ví dụ, người dùng B), chẳng hạn như hệ thống quản lý giao dịch mà thực thể thứ hai sử dụng để quản lý giao dịch của nó với một hoặc nhiều thực thể khác (ví dụ, những người dùng khác). Trong ví dụ trên Fig.1, chuỗi khối công khai 102 được thể hiện dưới dạng mạng ngang hàng của các nút, và các hệ thống tính toán 106, 108 lần lượt tạo ra các nút của thực thể thứ nhất và thực thể thứ hai, mà tham gia vào chuỗi khối công khai 102.

Fig.2 mô tả kiến trúc về khái niệm 200 làm ví dụ theo các phương án thực hiện của sáng chế. Kiến trúc về khái niệm 200 làm ví dụ này bao gồm lớp thực thể 202, lớp dịch vụ được làm chủ 204 và lớp chuỗi khối công khai 206. Trong ví dụ đã mô tả, lớp

thực thể 202 bao gồm ba thực thể, Thực thể_1 (E1), Thực thể_2 (E2) và Thực thể_3 (E3), mỗi thực thể này có hệ thống quản lý giao dịch 208 tương ứng.

Trong ví dụ đã mô tả, lớp dịch vụ được làm chủ 204 bao gồm chuỗi khối hoặc các giao diện DLS 210 cho mỗi hệ thống quản lý giao dịch 208. Trong một số ví dụ, hệ thống quản lý giao dịch 208 tương ứng truyền thông với giao diện DLS 210 tương ứng qua mạng (ví dụ, mạng 110 trên Fig.1) sử dụng giao thức truyền thông (ví dụ, giao thức bảo mật truyền tải siêu văn bản (hypertext transfer protocol secure - HTTPS)). Trong một số ví dụ, mỗi giao diện DLS 210 tạo ra sự kết nối truyền thông giữa hệ thống quản lý giao dịch 208 tương ứng và lớp chuỗi khối 206. Cụ thể hơn, mỗi giao diện DLS 210 cho phép thực thể tương ứng thực hiện các giao dịch được ghi trong mạng chuỗi khối 212 của lớp chuỗi khối 206. Trong một số ví dụ, sự truyền thông giữa giao diện DLS 210, và lớp chuỗi khối 206 được tiến hành sử dụng các cuộc gọi thủ tục từ xa (remote procedure call - RPC). Trong một số ví dụ, các giao diện DLS 210 "làm chủ" các nút chuỗi khối đối với hệ thống quản lý giao dịch 208 tương ứng. Ví dụ, các giao diện DLS 210 tạo ra giao diện lập trình ứng dụng (application programming interface - API) để truy cập vào mạng chuỗi khối 212.

Như được mô tả ở đây, mạng chuỗi khối 212 được tạo ra dưới dạng mạng ngang hàng bao gồm các nút 214 mà ghi thông tin một cách bất biến trong chuỗi khối 216. Mặc dù một chuỗi khối 216 duy nhất được mô tả sơ lược, nhiều bản sao của chuỗi khối 216 được tạo ra, và được duy trì qua chuỗi khối 212. Ví dụ, mỗi nút 214 lưu trữ bản sao của chuỗi khối 216. Theo một số phương án thực hiện, chuỗi khối 216 lưu trữ thông tin được kết hợp với các giao dịch mà được thực hiện giữa hai hoặc nhiều hơn hai thực thể tham gia vào chuỗi khối công khai.

Sáng chế bộc lộ các phương pháp mà có thể cho phép các giao dịch bí mật và các giao dịch công khai được thực hiện theo mô hình số dư tài khoản trong mạng chuỗi khối dựa trên các sơ đồ cam kết. Theo cách này, những người dùng có thể tự do lựa chọn xem mỗi giao dịch hoặc tài khoản được sử dụng cho giao dịch này là công khai hay bí mật.

Fig.3 mô tả biểu đồ phân làn minh họa quy trình xác nhận 300 làm ví dụ của giao dịch chuỗi khối theo các phương án thực hiện của sáng chế. Nhằm mục đích minh họa quy trình xác nhận 300 làm ví dụ, giao dịch chuyển tiền được giả định cần được thực

hiện bởi nút người dùng A 302 đến nút người dùng B (không được thể hiện trên Fig.3), và giao dịch này được gửi bởi nút người dùng A 302 sang nút chuỗi khối 304 để xác nhận. Mỗi trong số nút người dùng A 302, và nút người dùng B có thể bao gồm tài khoản công và tài khoản riêng. Số dư của tài khoản công có thể xem được bởi tất cả các nút trong mạng chuỗi khối. Số dư của tài khoản riêng có thể chỉ xem được bởi chủ sở hữu (người dùng) tài khoản sử dụng khóa bí mật. Theo các phương án thực hiện của sáng chế, các nút người dùng có thể chọn xem thực hiện các giao dịch công khai hoặc bí mật bằng cách sử dụng tài khoản công hoặc tài khoản riêng.

Ở bước 306, nút người dùng A 302 tạo ra giá trị cam kết dựa trên số tiền giao dịch t và số ngẫu nhiên r. Giá trị cam kết có thể được tạo ra bởi sơ đồ cam kết đồng cấu. Sơ đồ cam kết làm ví dụ bao gồm, không làm giới hạn, cam kết Pedersen (Pedersen Commitment - PC). Mặc dù các phương án thực hiện của sáng chế được mô tả một cách chi tiết hơn ở đây dựa trên PC, dự tính được rằng các phương án thực hiện của sáng chế có thể được thực hiện bằng cách sử dụng sơ đồ cam kết thích hợp bất kỳ.

Bằng cách sử dụng PC, ví dụ, giá trị cam kết là văn bản mã hóa mà có thể được biểu thị dưới dạng $PC(t) = rG + tH$, trong đó G và H có thể là bộ tạo của đường cong elip, $PC(t)$ là tích vô hướng của các điểm cong, t là giá trị được cam kết. Sơ đồ cam kết PC có tính đồng cấu, nghĩa là, $PC(t_1) + PC(t_2) = PC(t_1+t_2)$. Các bên giữ văn bản mã hóa $PC(t)$ có thể xác minh số tiền giao dịch t bằng cách sử dụng số ngẫu nhiên r. Ở bước 308, nút người dùng A 302 sử dụng khóa bí mật để ký kỹ thuật số giá trị cam kết $PC(t)$, số tiền giao dịch t và số ngẫu nhiên r. Nút người dùng A 302 gửi giá trị cam kết $PC(t)$, số tiền giao dịch t, số ngẫu nhiên r và chữ ký số đến nút chuỗi khối 304 ở bước 310.

Theo một số phương án thực hiện, số tiền giao dịch t có thể được gửi từ tài khoản riêng của nút người dùng A 302. Đối với tài khoản riêng, xem tài khoản này có số dư đủ hay không để chuyển số tiền giao dịch t không thể được xác minh trực tiếp bởi các nút khác của chuỗi khối. Trong các trường hợp này, nút người dùng A 302 có thể tạo ra một hoặc nhiều bằng chứng phạm vi để thể hiện rằng số tiền giao dịch t lớn hơn hoặc bằng không, và nhỏ hơn hoặc bằng số dư của tài khoản riêng của nút người dùng A 302.

Ở bước 312, nút chuỗi khối 304 xác minh chữ ký số của giá trị cam kết $PC(r, t)$, số tiền giao dịch t và số ngẫu nhiên r sử dụng khóa công khai của nút người dùng A 302.

Nếu chữ ký số là chính xác, thì quy trình xác nhận 300 làm ví dụ tiến hành sang bước 314.

Ở bước 314, nút chuỗi khối 304 xác minh xem giá trị cam kết *PC(t)* có chính xác và số tiền giao dịch *t* có hợp lệ hay không. Để xác minh nếu *PC(t)* là chính xác, thì số ngẫu nhiên *r* và số tiền giao dịch *t* đã nhận có thể được sử dụng để tạo ra PC được ký hiệu là *PC'(r, t)*. Nếu *PC'(r, t)* bằng cam kết *PC(r, t)* đã nhận, thì cam kết *PC(r, t)* được xác minh là cam kết chính xác của số tiền giao dịch *t*. Theo một số phương án thực hiện, nút chuỗi khối 304 có thể xác minh rằng số tiền giao dịch *t* là hợp lệ nếu lượng này lớn hơn hoặc bằng 0, và nhỏ hơn hoặc bằng số dư tài khoản của tài khoản 302 của nút người dùng A trong đó số tiền giao dịch được chuyển dựa trên một hoặc nhiều bằng chứng phạm vi.

Ở bước 316, nút chuỗi khối 304 cập nhật các số dư của nút người dùng A 302, và nút người dùng B trên chuỗi khối, và phát rộng chuỗi khối đến phần còn lại của các nút trong mạng chuỗi khối. Đối với các giao dịch tài khoản công, số tiền giao dịch có thể được trừ trực tiếp từ, hoặc được cộng vào số dư của tài khoản công dựa trên kiểu giao dịch. Đối với các giao dịch tài khoản riêng, số tiền giao dịch *t* có thể được cam kết để sử dụng PC dưới dạng *PC(t)*, và được trừ từ, hoặc được cộng vào số dư tài khoản riêng *s* cũng được cam kết để sử dụng PC dưới dạng *PC(s)*. Vì PC là đồng cấu, nên $PC(s) \pm PC(t) = PC(s \pm t)$. Các chi tiết cập nhật số dư tài khoản công và bí mật được mô tả một cách chi tiết hơn ở đây dựa trên các Fig.4 và Fig.5.

Fig.4 mô tả sơ đồ khối minh họa giao dịch 400 làm ví dụ từ tài khoản công sang tài khoản riêng theo các phương án thực hiện của sáng chế. Như được thể hiện trong giao dịch 400 làm ví dụ, trước giao dịch này, nút người dùng A 402 có số dư tài khoản công *u*, và số dư tài khoản riêng *v* được cam kết để sử dụng PC và được biểu diễn dưới dạng *PC(v)*. Nút người dùng B 406 có số dư tài khoản công *x*, và số dư tài khoản riêng *y* được cam kết để sử dụng PC và được biểu diễn dưới dạng *PC(y)*. Nút người dùng A 402 có thể gửi giao dịch từ tài khoản công của nó sang tài khoản riêng của nút người dùng B 406 bằng cách gửi bản sao được ký số của giá trị cam kết *PC(t)*, số tiền giao dịch *t* và số ngẫu nhiên *a* tương ứng với giá trị cam kết đến mạng chuỗi khối 408. Sau khi giá trị cam kết *PC(t)* của số tiền giao dịch *t* được xác minh bằng cách sử dụng quy trình xác nhận, chẳng hạn như quy trình 300 làm ví dụ trên Fig.3, các tài khoản của nút người

dùng A 402, và nút người dùng B 406 có thể được cập nhật. Sau khi giao dịch được xác nhận bởi mạng chuỗi khối 408, số tiền giao dịch *t* được trừ từ tài khoản công của nút người dùng A 402, và được cộng vào tài khoản riêng của nút người dùng B 406. Sau khi giao dịch, nút người dùng A 400 có số dư tài khoản công *u - t*, và số dư tài khoản riêng *PC(v)*. Nút người dùng B 406 có số dư tài khoản công *x*, và số dư tài khoản riêng *PC(y + t)*.

Fig.5 mô tả sơ đồ khối minh họa giao dịch 500 làm ví dụ từ tài khoản riêng sang tài khoản công theo các phương án thực hiện của sáng chế. Như được thể hiện trong giao dịch 500 làm ví dụ, trước giao dịch này, nút người dùng A 502 có số dư tài khoản công *u* và số dư tài khoản riêng *v* được cam kết để sử dụng PC và được biểu diễn dưới dạng *PC(v)*. Nút người dùng B 506 có số dư tài khoản công *x*, và số dư tài khoản riêng *y* được cam kết để sử dụng PC và được biểu diễn dưới dạng *PC(y)*. Nút người dùng A 502 có thể gửi giao dịch từ tài khoản riêng của nó sang tài khoản công của nút người dùng B 506, bằng cách gửi bản sao được ký số của giá trị cam kết *PC(t)*, số tiền giao dịch *t*, số ngẫu nhiên *a* tương ứng với giá trị cam kết và một hoặc nhiều bằng chứng phạm vi. Một hoặc nhiều bằng chứng phạm vi này có thể được sử dụng để chứng minh rằng $0 \leq t \leq v$ đối với mạng chuỗi khối 508. Sau khi giá trị cam kết *PC(t)* của số tiền giao dịch *t* được xác minh bằng cách sử dụng quy trình xác nhận, chẳng hạn như quy trình 300 làm ví dụ trên Fig.3, các tài khoản của nút người dùng A 502, và nút người dùng B 506 có thể được cập nhật. Sau khi giao dịch được xác nhận bởi mạng chuỗi khối 508, số tiền giao dịch *t* được trừ từ tài khoản riêng của nút người dùng A, và được cộng vào tài khoản công của nút người dùng B 506. Sau khi giao dịch, nút người dùng A 502 có số dư tài khoản công *u*, và số dư tài khoản riêng *PC(v -t)*. Nút người dùng B 504 có số dư tài khoản công *x + t*, và số dư tài khoản riêng *PC(y)*.

Fig.6 mô tả phương pháp 600 làm ví dụ mà có thể được thực hiện theo các phương án thực hiện của sáng chế. Để trình bày rõ ràng, phần mô tả cho phép mô tả chung phương pháp 600 làm ví dụ theo ngữ cảnh của các hình vẽ khác trong phần mô tả này. Tuy nhiên, cần hiểu rằng phương pháp 600 làm ví dụ có thể được thực hiện, ví dụ, bằng hệ thống, môi trường, phần mềm và phần cứng bất kỳ, hoặc sự kết hợp của các hệ thống, môi trường, phần mềm và phần cứng khi thích hợp. Theo một số phương án thực

hiện, các bước khác nhau của phương pháp 600 làm ví dụ có thể chạy song song, kết hợp, trong vòng lặp hoặc theo thứ tự bất kỳ.

Ở bước 602, nút đồng thuận của mạng chuỗi khối nhận dữ liệu giao dịch và chữ ký số của dữ liệu giao dịch. Theo một số phương án thực hiện, dữ liệu giao dịch bao gồm giá trị cam kết, số ngẫu nhiên, và số tiền giao dịch cần được chuyển từ một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ nhất sang một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ hai. Chữ ký số được tạo ra bằng cách ký kỹ thuật số dữ liệu giao dịch sử dụng khóa bí mật của nút người dùng thứ nhất. Giá trị cam kết được tạo ra dựa trên số ngẫu nhiên và số tiền giao dịch sử dụng sơ đồ cam kết. Theo một số phương án thực hiện, sơ đồ cam kết là đồng cấu. Theo một số phương án thực hiện, số tiền giao dịch là từ tài khoản công được kết hợp với nút người dùng thứ nhất sang tài khoản riêng được kết hợp với nút người dùng thứ hai. Theo một số phương án thực hiện, số tiền giao dịch là từ tài khoản riêng được kết hợp với nút người dùng thứ nhất sang tài khoản công của nút người dùng thứ hai. Trong các trường hợp này, nút đồng thuận cũng có thể nhận, từ nút người dùng thứ nhất, bằng chứng phạm vi để chứng minh rằng số tiền giao dịch nhỏ hơn hoặc bằng số dư của tài khoản riêng của nút người dùng thứ nhất.

Ở bước 604, nút đồng thuận xác minh chữ ký số của dữ liệu giao dịch bằng cách sử dụng khóa công khai của nút người dùng thứ nhất.

Ở bước 606, nút đồng thuận xác định rằng số tiền giao dịch là hợp lệ, nếu giá trị cam kết là chính xác dựa trên số ngẫu nhiên và sơ đồ cam kết. Nút đồng thuận còn xác định rằng số tiền giao dịch nhỏ hơn hoặc bằng số dư của một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ nhất trước khi chuyển số tiền giao dịch. Theo một số phương án thực hiện, số tiền giao dịch là từ tài khoản riêng của nút người dùng thứ nhất sang tài khoản công của nút người dùng thứ hai. Trong các trường hợp này, xác định rằng bước chuyển số dư là hợp lệ còn bao gồm bước xác định xem số tiền giao dịch nhỏ hơn hay bằng số dư của tài khoản riêng được kết hợp với nút người dùng thứ nhất dựa trên bằng chứng phạm vi.

Theo một số phương án thực hiện, phương pháp 600 làm ví dụ có thể còn bao gồm bước cập nhật số dư của một trong số tài khoản công hoặc tài khoản riêng được kết hợp với nút người dùng thứ nhất và số dư của một trong số tài khoản công hoặc tài

khoản riêng được kết hợp với nút người dùng thứ hai. Bước cập nhật có thể được thực hiện dựa trên số tiền giao dịch, nếu số tiền giao dịch này là hợp lệ. Theo một số phương án thực hiện, số dư của tài khoản riêng được cập nhật dựa trên giá trị cam kết của số tiền giao dịch và sự cam kết của số dư của tài khoản riêng được tạo ra bằng cách sử dụng sơ đồ cam kết.

Các phương án thực hiện của đối tượng được mô tả trong bản mô tả này có thể được thực hiện để nhận ra các ưu điểm hoặc hiệu quả kỹ thuật cụ thể. Ví dụ, các phương án thực hiện của sáng chế cho phép mạng chuỗi khối hỗ trợ các giao dịch giữa các tài khoản công, các giao dịch giữa các tài khoản riêng và các giao dịch giữa các tài khoản công và bí mật. Như vậy, việc bảo vệ quyền riêng tư thích hợp có thể được thực hiện bất kể kiểu tài khoản nào, vì vậy, nút người dùng của mạng chuỗi khối có thể chọn một cách linh hoạt để gửi và nhận tiền từ tài khoản công hoặc tài khoản riêng của nó dựa trên các quyền ưu tiên riêng.

Phương pháp được mô tả cho phép tăng cường bảo mật tài khoản/dữ liệu của các thiết bị tính toán di động khác nhau. Số dư của tài khoản riêng có thể được cam kết dựa trên sơ đồ cam kết. Như vậy, số dư của tài khoản riêng có thể được xác minh dựa trên sự cam kết mà không tiết lộ số dư tài khoản thực tế của tài khoản. Số tiền giao dịch được thực hiện đến hoặc từ tài khoản riêng có thể còn được cam kết dựa trên sơ đồ cam kết để cập nhật tài khoản riêng sau khi giao dịch mà không tiết lộ số tiền thực tế được chuyển. Theo cách này, tạo ra nhiều sự kiểm soát hơn đối với tính bảo mật của các giao dịch tài khoản riêng.

Phương pháp được mô tả có thể đảm bảo sử dụng hiệu quả các tài nguyên máy tính (ví dụ, các chu trình xử lý, băng thông mạng và mức sử dụng bộ nhớ), thông qua bước cập nhật hiệu quả của chuỗi khối. Các hoạt động của tài khoản có thể được thực hiện một cách nhanh chóng và an toàn hơn thông qua các quy trình đồng thuận đơn giản hơn.

Các phương án thực hiện và các hoạt động được mô tả trong bản mô tả này có thể được thực hiện trong hệ mạch điện tử kỹ thuật số, hoặc trong phần mềm máy tính, phần sụn hoặc phần cứng, bao gồm các cấu trúc được bộc lộ trong bản mô tả này hoặc các kết hợp của một hoặc nhiều trong số chúng. Các hoạt động có thể được thực hiện dưới dạng các hoạt động được thực hiện bởi thiết bị xử lý dữ liệu đối với dữ liệu được lưu trữ trên

một hoặc nhiều thiết bị lưu trữ đọc được bằng máy tính hoặc nhận được từ các nguồn khác. Thiết bị xử lý dữ liệu, máy tính hoặc thiết bị tính toán có thể bao gồm thiết bị, dụng cụ và máy móc để xử lý dữ liệu, bao gồm bằng cách lấy ví dụ như bộ xử lý lập trình được, máy tính, hệ thống trên chip hoặc nhiều thiết bị, dụng cụ và máy móc hoặc sự kết hợp của các thiết bị, dụng cụ và máy móc nêu trên. Thiết bị này có thể bao gồm hệ mạch logic dùng cho mục đích cụ thể, ví dụ, bộ xử lý trung tâm (central processing unit - CPU), mảng cổng trường lập trình được dạng trường (field programmable gate array - FPGA) hoặc mạch tích hợp cho ứng dụng cụ thể (application-specific integrated circuit - ASIC). Thiết bị này có thể còn bao gồm mã mà tạo ra môi trường thực hiện cho chương trình máy tính khi đề cập, ví dụ, mã tạo thành phần sụn của bộ xử lý, chồng giao thức, hệ thống quản lý cơ sở dữ liệu, hệ điều hành (ví dụ, hệ điều hành hoặc sự kết hợp của các hệ điều hành này), môi trường thời gian chạy nền tảng chéo, máy ảo hoặc sự kết hợp của một hoặc nhiều trong số chúng. Thiết bị và môi trường thực hiện có thể nhận ra các cơ sở hạ tầng mô hình tính toán khác nhau, chẳng hạn như các dịch vụ web, cơ sở hạ tầng tính toán phân tán và tính toán dạng lưới.

Chương trình máy tính (ví dụ, còn được biết dưới dạng chương trình, phần mềm, ứng dụng phần mềm, môđun phần mềm, khối phần mềm, tập lệnh hoặc mã) có thể được viết dưới dạng ngôn ngữ lập trình bất kỳ, bao gồm các ngôn ngữ được biên dịch hoặc phiên dịch, ngôn ngữ khai báo hoặc thủ tục và có thể được triển khai dưới dạng bất kỳ, bao gồm dưới dạng chương trình độc lập hoặc dưới dạng môđun, thành phần, đoạn chương trình con, đối tượng hoặc khối khác thích hợp để sử dụng trong môi trường tính toán. Chương trình có thể được lưu trữ trong một phần tệp mà giữ các chương trình hoặc dữ liệu khác (ví dụ, một hoặc nhiều tập lệnh được lưu trữ trong tài liệu ngôn ngữ đánh dấu), trong một tệp duy nhất được dành riêng cho chương trình khi đề cập hoặc trong nhiều tệp phối hợp (ví dụ, các tệp lưu trữ một hoặc nhiều môđun, chương trình con hoặc các phần của mã). Chương trình máy tính có thể được thực hiện trên một máy tính hoặc trên nhiều máy tính được đặt ở một vị trí hoặc được phân phối ngang qua nhiều vị trí và được liên kết bởi mạng truyền thông.

Bộ xử lý để thực hiện chương trình máy tính bao gồm, bằng cách lấy ví dụ, cả bộ vi xử lý dùng cho mục đích chung và cụ thể, và một hoặc nhiều bộ xử lý bất kỳ của loại máy tính kỹ thuật số bất kỳ. Nói chung, bộ xử lý sẽ nhận các lệnh và dữ liệu từ bộ nhớ

chỉ đọc hoặc bộ nhớ truy cập ngẫu nhiên hoặc cả hai. Các bộ phận thiết yếu của máy tính là bộ xử lý để thực hiện các hành động theo các lệnh và một hoặc nhiều thiết bị bộ nhớ để lưu trữ các lệnh và dữ liệu này. Nói chung, máy tính sẽ còn bao gồm hoặc được ghép nối về mặt hoạt động để nhận dữ liệu từ hoặc truyền dữ liệu đến, hoặc cả hai, một hoặc nhiều thiết bị lưu trữ lớn để lưu trữ dữ liệu. Máy tính có thể được nhúng trong thiết bị khác, ví dụ như thiết bị di động, thiết bị kỹ thuật số hỗ trợ cá nhân (personal digital assistant - PDA), bảng điều khiển trò chơi cầm tay, bộ thu hệ thống định vị toàn cầu (global positioning system - GPS) hoặc thiết bị lưu trữ cầm tay. Các thiết bị thích hợp để lưu trữ các lệnh và dữ liệu chương trình máy tính bao gồm bộ nhớ, vật ghi và thiết bị bộ nhớ bất khả biến, bao gồm, bằng cách lấy ví dụ, các thiết bị bộ nhớ bán dẫn, đĩa từ và đĩa quang-từ. Bộ xử lý và bộ nhớ có thể được bổ sung hoặc kết hợp trong hệ mạch logic dùng cho mục đích cụ thể.

Các thiết bị di động có thể bao gồm thiết bị cầm tay, thiết bị người dùng (user equipment - UE), điện thoại di động (ví dụ, điện thoại thông minh), máy tính dạng bảng, thiết bị đeo được (ví dụ, đồng hồ thông minh và kính mắt thông minh), thiết bị cấy ghép trong cơ thể con người (ví dụ, bộ cảm biến sinh học, ốc tai điện tử) hoặc các kiểu thiết bị di động khác. Các thiết bị di động này có thể truyền thông không dây (ví dụ, sử dụng các tín hiệu tần số vô tuyến (radio frequency - RF)) với các mạng truyền thông khác nhau (được mô tả bên dưới). Các thiết bị di động có thể bao gồm các bộ cảm biến để xác định các đặc điểm của môi trường hiện tại của thiết bị di động. Các bộ cảm biến có thể bao gồm camera, micrô, bộ cảm biến tiệm cận, bộ cảm biến GPS, bộ cảm biến chuyển động, gia tốc kế, bộ cảm biến ánh sáng xung quanh, bộ cảm biến độ ẩm, con quay hồi chuyển, la bàn, khi áp kế, bộ cảm biến dấu vân tay, hệ thống nhận diện khuôn mặt, bộ cảm biến RF (ví dụ, Wi-Fi và vô tuyến di động), bộ cảm biến nhiệt hoặc các kiểu bộ cảm biến khác. Ví dụ, các camera có thể bao gồm camera phía trước hoặc phía sau với các ống kính có thể di chuyển hoặc cố định, đèn nháy, bộ cảm biến hình ảnh và bộ xử lý hình ảnh. Camera có thể là camera có độ phân giải triệu điểm ảnh có khả năng chụp các chi tiết để nhận diện khuôn mặt và/hoặc mống mắt. Camera cùng với bộ xử lý dữ liệu và thông tin xác thực được lưu trữ trong bộ nhớ hoặc được truy cập từ xa có thể tạo ra hệ thống nhận diện khuôn mặt. Hệ thống nhận diện khuôn mặt hoặc một hoặc nhiều bộ cảm

biến, ví dụ, micrô, bộ cảm biến chuyển động, gia tốc kế, bộ cảm biến GPS hoặc bộ cảm biến RF, có thể được sử dụng để xác thực người dùng.

Để tạo ra sự tương tác với người dùng, các phương án có thể được thực hiện trên máy tính có thiết bị hiển thị và thiết bị đầu vào, ví dụ, màn hiển thị tinh thể lỏng (liquid crystal display - LCD) hoặc màn hiển thị điốt phát sáng hữu cơ (organic light-emitting diode - OLED)/màn hiển thị thực tế ảo (vitual-reality - VR)/màn hiển thị thực tế tăng cường (augmented-reality - AR) để hiển thị thông tin cho người dùng và màn hình cảm ứng, bàn phím và thiết bị trỏ mà người dùng có thể cung cấp đầu vào cho máy tính. Các loại thiết bị khác cũng có thể được sử dụng để tạo ra sự tương tác với người dùng; ví dụ, phản hồi được tạo ra cho người dùng có thể là dạng phản hồi cảm giác bất kỳ, ví dụ, phản hồi thị giác, phản hồi thính giác hoặc phản hồi xúc giác; và đầu vào từ người dùng có thể được nhận ở dạng bất kỳ, bao gồm đầu vào âm thanh, lời nói hoặc xúc giác. Ngoài ra, máy tính có thể tương tác với người dùng bằng cách gửi các tài liệu đến và nhận tài liệu từ thiết bị mà được người dùng sử dụng; ví dụ, bằng cách gửi các trang web đến trình duyệt web trên thiết bị khách của người dùng để đáp ứng các yêu cầu nhận được từ trình duyệt web này.

Các phương án thực hiện của sáng chế có thể được thực hiện bằng cách sử dụng các thiết bị tính toán được liên kết bằng hình thức hoặc vật ghi truyền thông dữ liệu kỹ thuật số không dây hoặc có dây bất kỳ (hoặc sự kết hợp các hình thức hoặc vật ghi này), ví dụ, mạng truyền thông. Các ví dụ về các thiết bị liên kết là máy khách và máy chủ thường ở xa nhau mà tương tác điển hình thông qua mạng truyền thông. Máy khách, ví dụ, thiết bị di động, có thể tự thực hiện các giao dịch, với máy chủ hoặc thông qua máy chủ, ví dụ, thực hiện các giao dịch mua, bán, trả, cho, gửi hoặc cho vay hoặc ủy quyền tương tự. Các giao dịch này có thể ở thời gian thực sao cho hành động và phản hồi gần nhau về mặt thời gian; ví dụ, cá nhân nhận thấy hành động và phản hồi gần như xảy ra đồng thời, sự chênh lệch về thời gian để phản hồi theo hành động của cá nhân là dưới 1 mili giây (ms) hoặc dưới 1 giây hoặc phản hồi này không có sự chậm trễ có tính đến các giới hạn xử lý của hệ thống.

Cac ví dụ về các mạng truyền thông bao gồm mạng vùng cục bộ (LAN), mạng truy cập vô tuyến (radio access network - RAN), mạng khu vực đô thị (metropolitan area network - MAN) và mạng diện rộng (WAN). Mạng truyền thông có thể bao gồm tất

cả hoặc một phần của Internet, mạng truyền thông khác hoặc sự kết hợp của các mạng truyền thông. Thông tin có thể được truyền trên mạng truyền thông theo các giao thức và tiêu chuẩn khác nhau, bao gồm hệ thống tiến hóa dài hạn (Long Term Evolution - LTE), 5G, IEEE 802, giao thức Internet (Internet Protocol - IP) hoặc các giao thức khác hoặc các kết hợp của các giao thức này. Mạng truyền thông có thể truyền dữ liệu giọng nói, video, sinh trắc học hoặc dữ liệu xác thực hoặc thông tin khác giữa các thiết bị tính toán được kết nối.

Các dấu hiệu được mô tả dưới dạng các phương án thực hiện riêng biệt có thể được thực hiện, khi kết hợp, theo một phương án thực hiện duy nhất, trong khi các dấu hiệu được mô tả dưới dạng một phương án thực hiện duy nhất có thể được thực hiện theo nhiều phương án thực hiện, một cách riêng biệt hoặc khi kết hợp phụ thích hợp bất kỳ. Các hoạt động được mô tả và bảo hộ theo thứ tự cụ thể không nên được hiểu là yêu cầu thứ tự cụ thể đó, cũng không phải tất cả các hoạt động được minh họa phải được thực hiện (một số hoạt động có thể là tùy ý). Khi thích hợp, sự xử lý đa nhiệm hoặc song song (hoặc sự kết hợp của sự xử lý đa nhiệm và song song) có thể được thực hiện.

YÊU CẦU BẢO HỘ

1. Phương pháp được thực hiện bằng máy tính để xác nhận các giao dịch chuỗi khối dựa trên các mô hình tài khoản, trong đó phương pháp này bao gồm các bước:

nhận, bởi nút đồng thuận của mạng chuỗi khối, dữ liệu giao dịch và chữ ký số của dữ liệu giao dịch, trong đó dữ liệu giao dịch này bao gồm số tiền giao dịch được mã hóa, số ngẫu nhiên và số tiền giao dịch không được mã hóa cần được chuyển từ tài khoản công của nút người dùng thứ nhất sang tài khoản riêng của nút người dùng thứ hai, hoặc từ tài khoản riêng của nút người dùng thứ nhất sang tài khoản công của nút người dùng thứ hai, trong đó mỗi tài khoản công bao gồm số dư và mỗi tài khoản riêng bao gồm số dư được mã hóa, trong đó chữ ký số được tạo ra bằng cách ký kỹ thuật số dữ liệu giao dịch sử dụng khóa bí mật của nút người dùng thứ nhất, và trong đó số tiền giao dịch được mã hóa được tạo ra dựa trên số ngẫu nhiên và số tiền giao dịch không được mã hóa sử dụng sơ đồ cam kết;

xác minh chữ ký số của dữ liệu giao dịch bằng sử dụng khóa công khai của nút người dùng thứ nhất;

tạo ra số tiền giao dịch được mã hóa thứ hai dựa trên số ngẫu nhiên và số tiền giao dịch không được mã hóa sử dụng sơ đồ cam kết;

xác định rằng số tiền giao dịch được mã hóa thứ hai bằng số tiền giao dịch được mã hóa nhận được; và

xác định rằng số tiền giao dịch không được mã hóa nhỏ hơn hoặc bằng số dư của tài khoản công của nút người dùng thứ nhất trước khi chuyển khi giao dịch là từ tài khoản công của nút người dùng thứ nhất sang tài khoản riêng của nút người dùng thứ hai, hoặc số tiền giao dịch không được mã hóa nhỏ hơn hoặc bằng giá trị không được mã hóa của số dư được mã hóa của tài khoản riêng của nút người dùng thứ nhất trước khi chuyển khi giao dịch là từ tài khoản riêng của nút người dùng thứ nhất sang tài khoản công của nút người dùng thứ hai;

hoặc trừ số tiền giao dịch không được mã hóa từ số dư của tài khoản công của nút người dùng thứ nhất, và cộng số tiền giao dịch được mã hóa nhận được vào số dư được mã hóa của tài khoản riêng của nút người dùng thứ hai, khi giao dịch là từ tài khoản công của nút người dùng thứ nhất sang tài khoản riêng của nút người dùng thứ hai, hoặc

trừ số tiền giao dịch được mã hóa nhận được từ số dư được mã hóa của tài khoản riêng của nút người dùng thứ nhất, và cộng số tiền giao dịch không được mã hóa vào số dư của tài khoản công của nút người dùng thứ hai, khi giao dịch là từ tài khoản riêng của nút người dùng thứ nhất sang tài khoản công của nút người dùng thứ hai.

2. Phương pháp được thực hiện bằng máy tính theo điểm 1, trong đó số dư của tài khoản công của nút người dùng thứ nhất hoặc của nút người dùng thứ hai xem được bởi nút đồng thuận, và trong đó giá trị không được mã hóa của số dư được mã hóa của tài khoản riêng của nút người dùng thứ nhất hoặc của nút người dùng thứ hai xem được bằng cách sử dụng khóa bí mật của nút người dùng tương ứng.

3. Phương pháp được thực hiện bằng máy tính theo điểm 1, trong đó giao dịch là từ tài khoản riêng của nút người dùng thứ nhất sang tài khoản công của nút người dùng thứ hai, và phương pháp này còn bao gồm bước:

nhận, từ nút người dùng thứ nhất, bằng chứng phạm vi để chứng minh rằng số tiền giao dịch không được mã hóa nhỏ hơn hoặc bằng giá trị không được mã hóa của số dư được mã hóa của tài khoản riêng của nút người dùng thứ nhất; và

trong đó bước chuyển được xác định là hợp lệ, nếu số tiền giao dịch không được mã hóa nhỏ hơn hoặc bằng giá trị không được mã hóa của số dư được mã hóa của tài khoản riêng của nút người dùng thứ nhất dựa trên bằng chứng phạm vi.

4. Phương pháp được thực hiện bằng máy tính theo điểm 1, trong đó nút người dùng thứ nhất có cả tài khoản công của nút người dùng thứ nhất và tài khoản riêng của nút người dùng thứ nhất, và

trong đó người dùng liên quan đến nút người dùng thứ nhất chọn xem thực hiện giao dịch bằng cách sử dụng tài khoản công của nút người dùng thứ nhất hay tài khoản riêng của nút người dùng thứ nhất.

5. Phương pháp được thực hiện bằng máy tính theo điểm 1, trong đó sơ đồ cam kết là đồng cấu.

6. Vật ghi lưu trữ đọc được bằng máy tính lâu dài được ghép nối với một hoặc nhiều bộ xử lý và có các lệnh được lưu trữ trên đó, khi được thực hiện bởi một hoặc nhiều bộ xử lý, thì khiến cho một hoặc nhiều bộ xử lý thực hiện các hoạt động theo phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5.

7. Hệ thống để xác nhận các giao dịch chuỗi khối dựa trên các mô hình tài khoản, hệ thống này bao gồm:

thiết bị tính toán; và

thiết bị lưu trữ đọc được bằng máy tính được ghép nối với thiết bị tính toán và có các lệnh được lưu trữ trên đó, khi được thực hiện bởi thiết bị tính toán, thì khiến cho thiết bị tính toán thực hiện các hoạt động theo phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5.

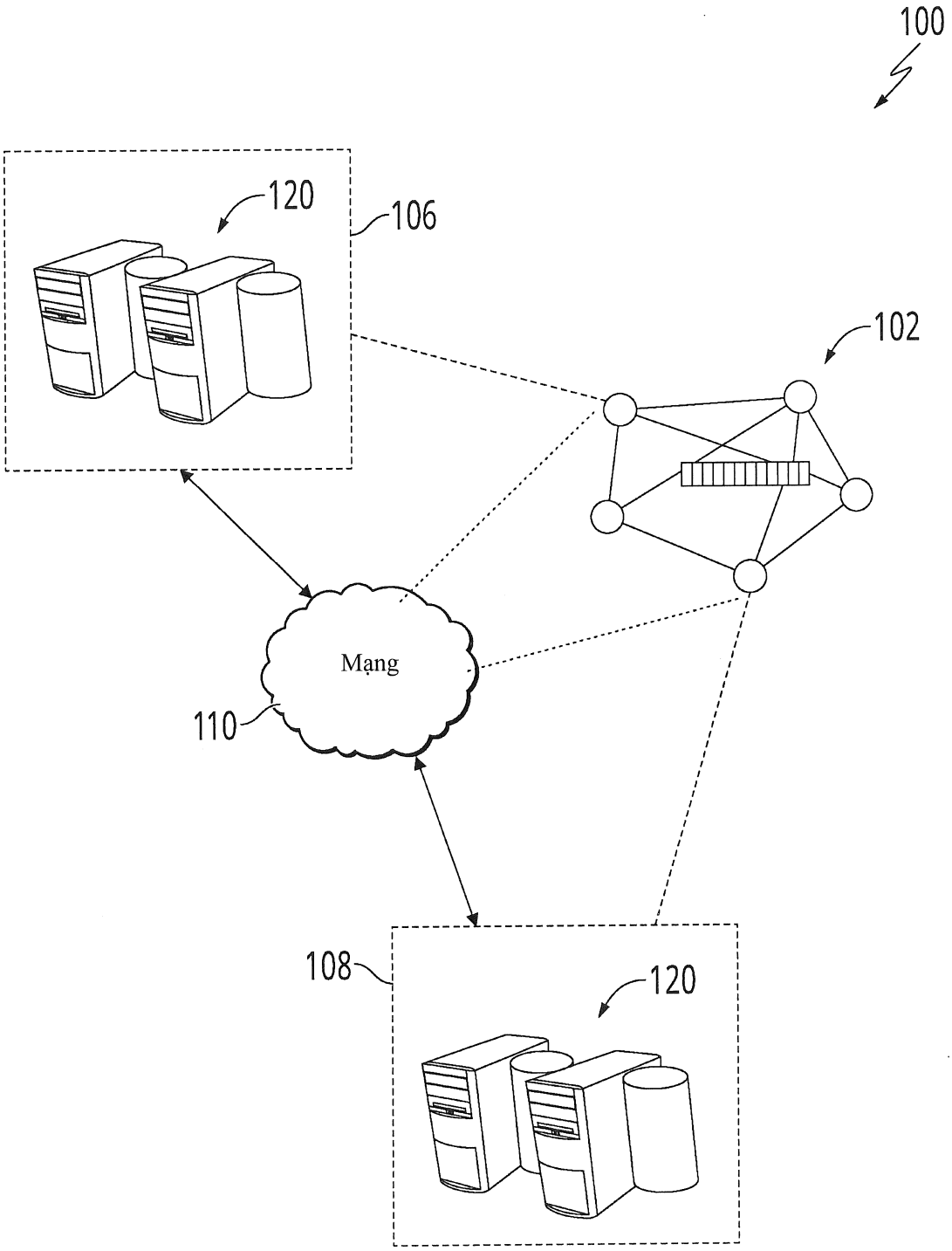


FIG. 1

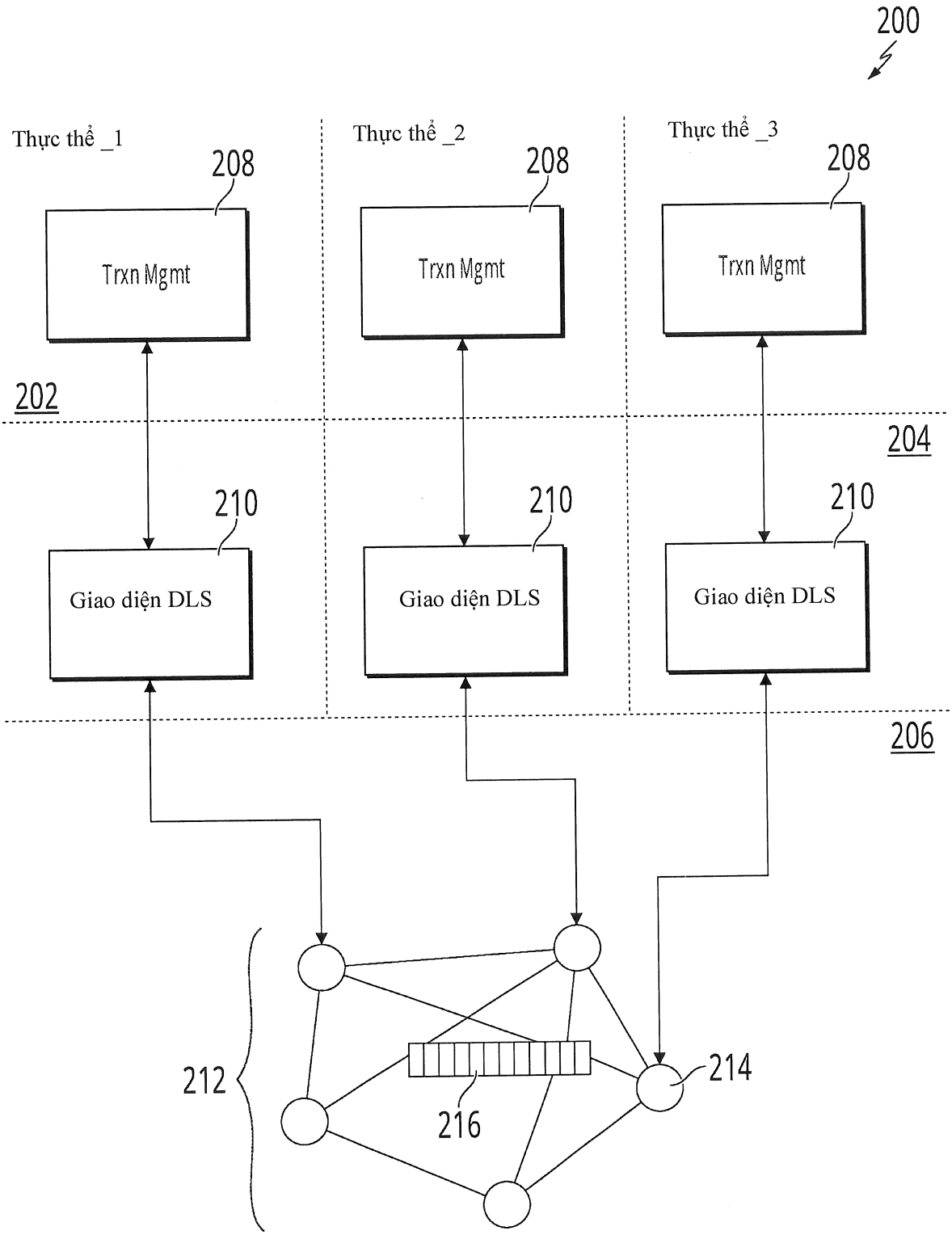

200
Thực thể _1
Thực thể _2
Thực thể _3
208
208
208
Trxn Mgmt
Trxn Mgmt
Trxn Mgmt
202
204
210
210
210
Giao diện DLS
Giao diện DLS
Giao diện DLS
206
212
214
216

FIG. 2

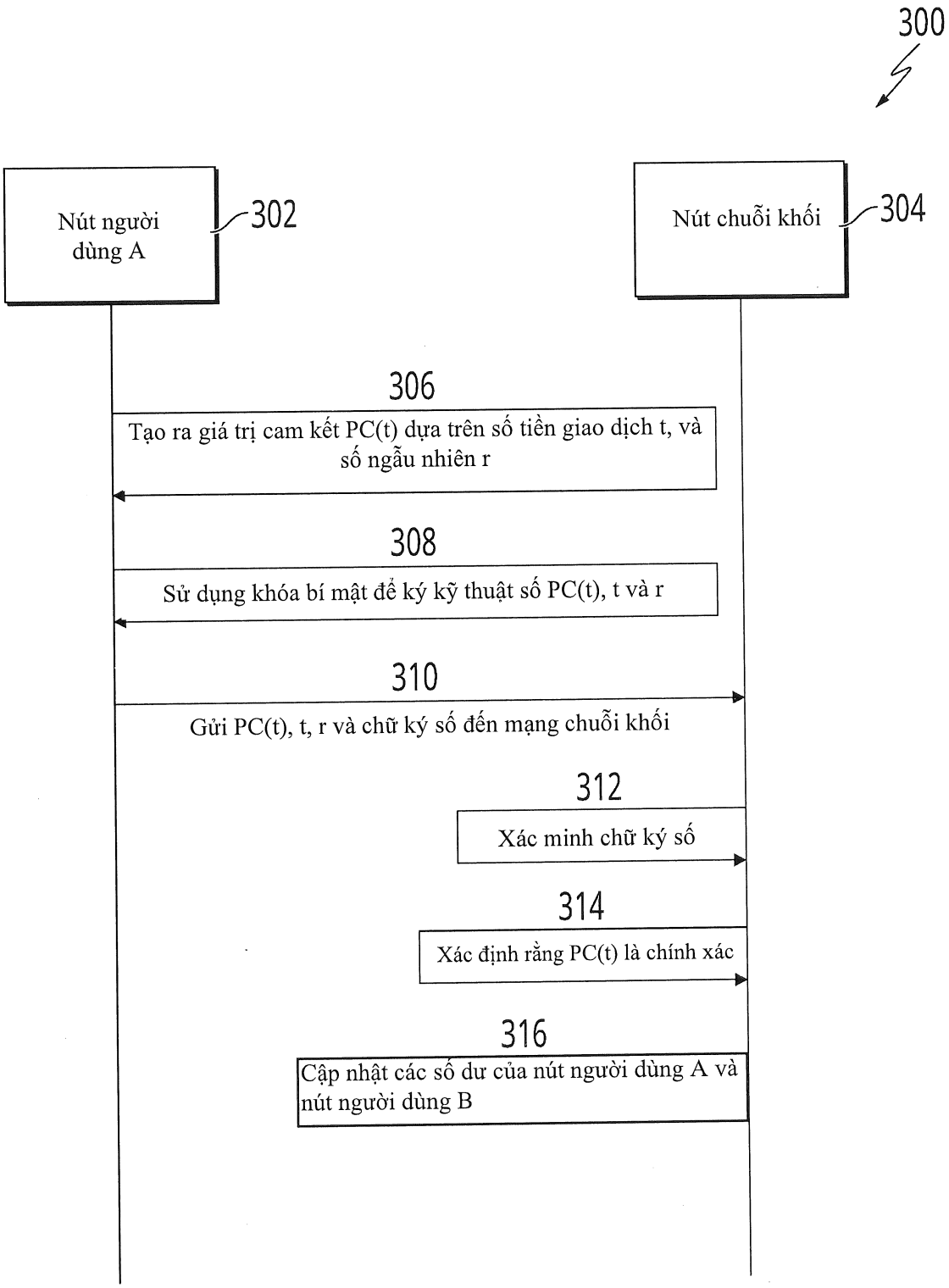

300
Nút người dùng A
302
Nút chuỗi khối
304
306
Tạo ra giá trị cam kết PC(t) dựa trên số tiền giao dịch t, và số ngẫu nhiên r
308
Sử dụng khóa bí mật để ký kỹ thuật số PC(t), t và r
310
Gửi PC(t), t, r và chữ ký số đến mạng chuỗi khối
312
Xác minh chữ ký số
314
Xác định rằng PC(t) là chính xác
316
Cập nhật các số dư của nút người dùng A và nút người dùng B

FIG. 3

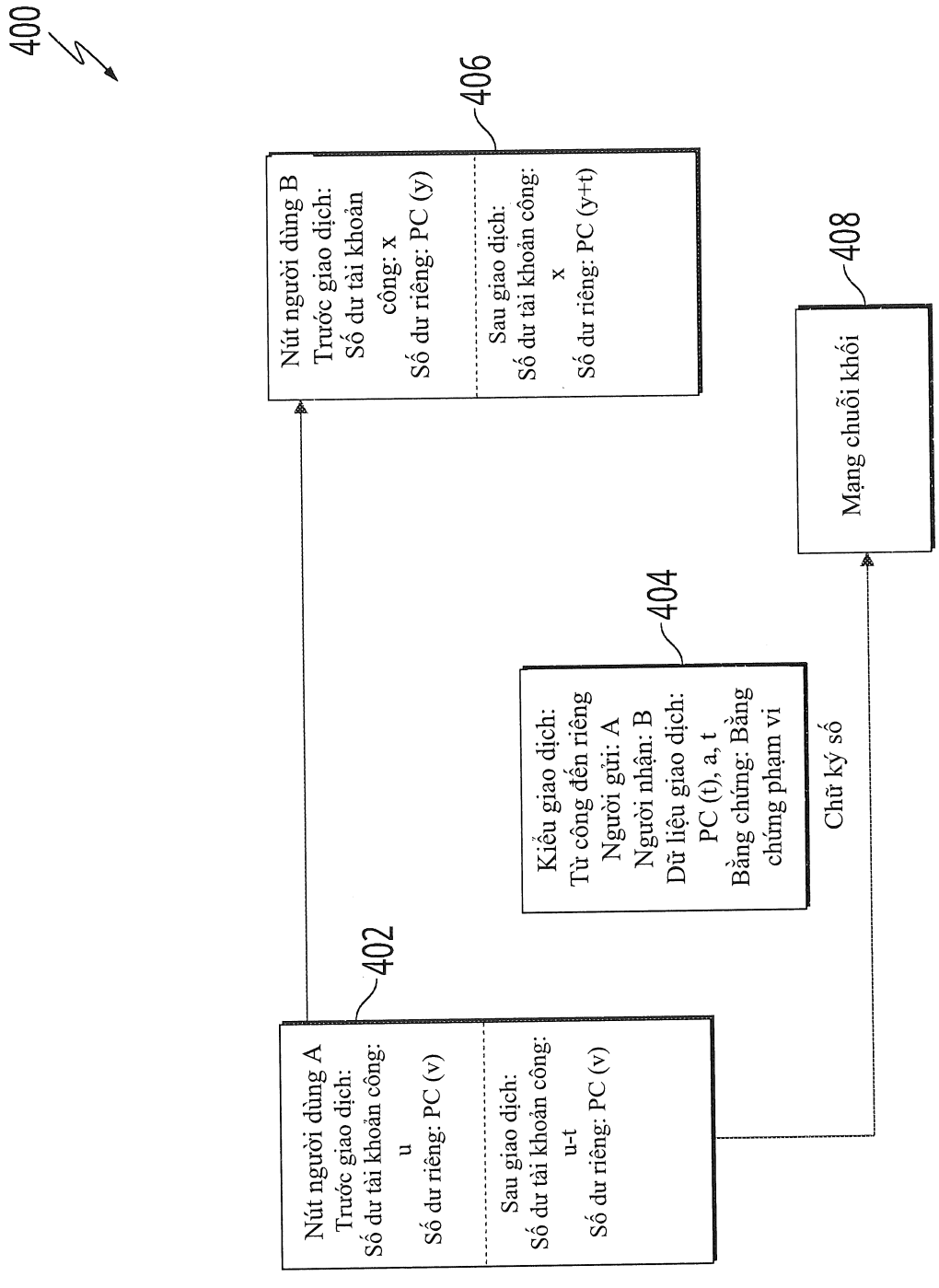

400
Nút người dùng B
Trước giao dịch:
Số dư tài khoản công: x
Số dư riêng: PC (y)
Sau giao dịch:
Số dư tài khoản công: x
Số dư riêng: PC (y+t)
406
Nút người dùng A
Trước giao dịch:
Số dư tài khoản công: u
Số dư riêng: PC (v)
Sau giao dịch:
Số dư tài khoản công: u-t
Số dư riêng: PC (v)
402
Kiểu giao dịch:
Từ công đến riêng
Người gửi: A
Người nhận: B
Dữ liệu giao dịch:
PC (t), a, t
Bằng chứng: Bằng chứng phạm vi
404
Chữ ký số
Mạng chuỗi khối
408

FIG. 4

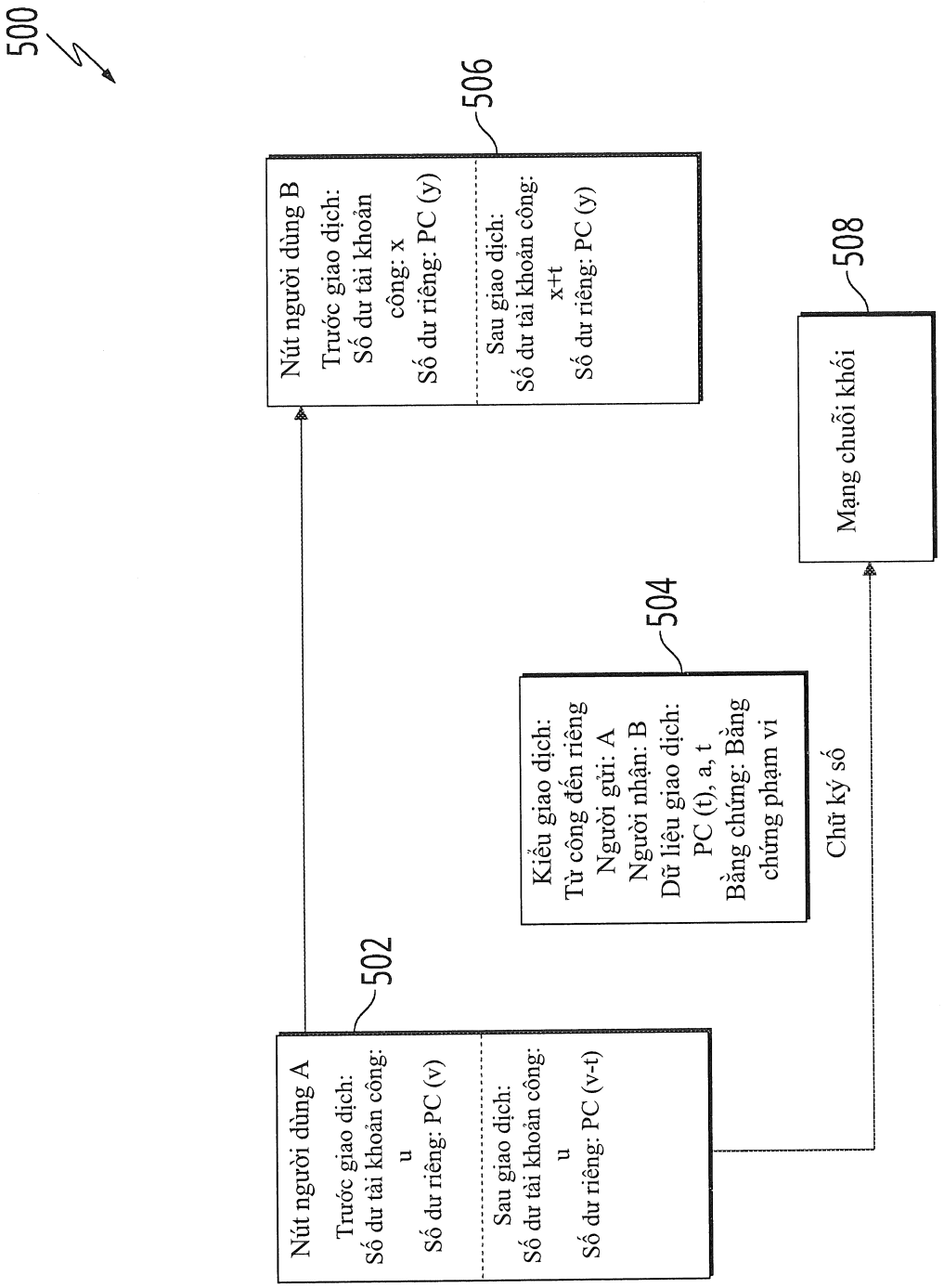

500
Nút người dùng A
Trước giao dịch:
Số dư tài khoản công: u
Số dư riêng: PC (v)
Sau giao dịch:
Số dư tài khoản công: u
Số dư riêng: PC (v-t)
502
Nút người dùng B
Trước giao dịch:
Số dư tài khoản công: x
Số dư riêng: PC (y)
Sau giao dịch:
Số dư tài khoản công: x+t
Số dư riêng: PC (y)
506
Kiểu giao dịch: Từ công đến riêng
Người gửi: A
Người nhận: B
Dữ liệu giao dịch: PC (t), a, t
Bằng chứng: Bằng chứng phạm vi
504
Chữ ký số
Mạng chuỗi khối
508

FIG. 5

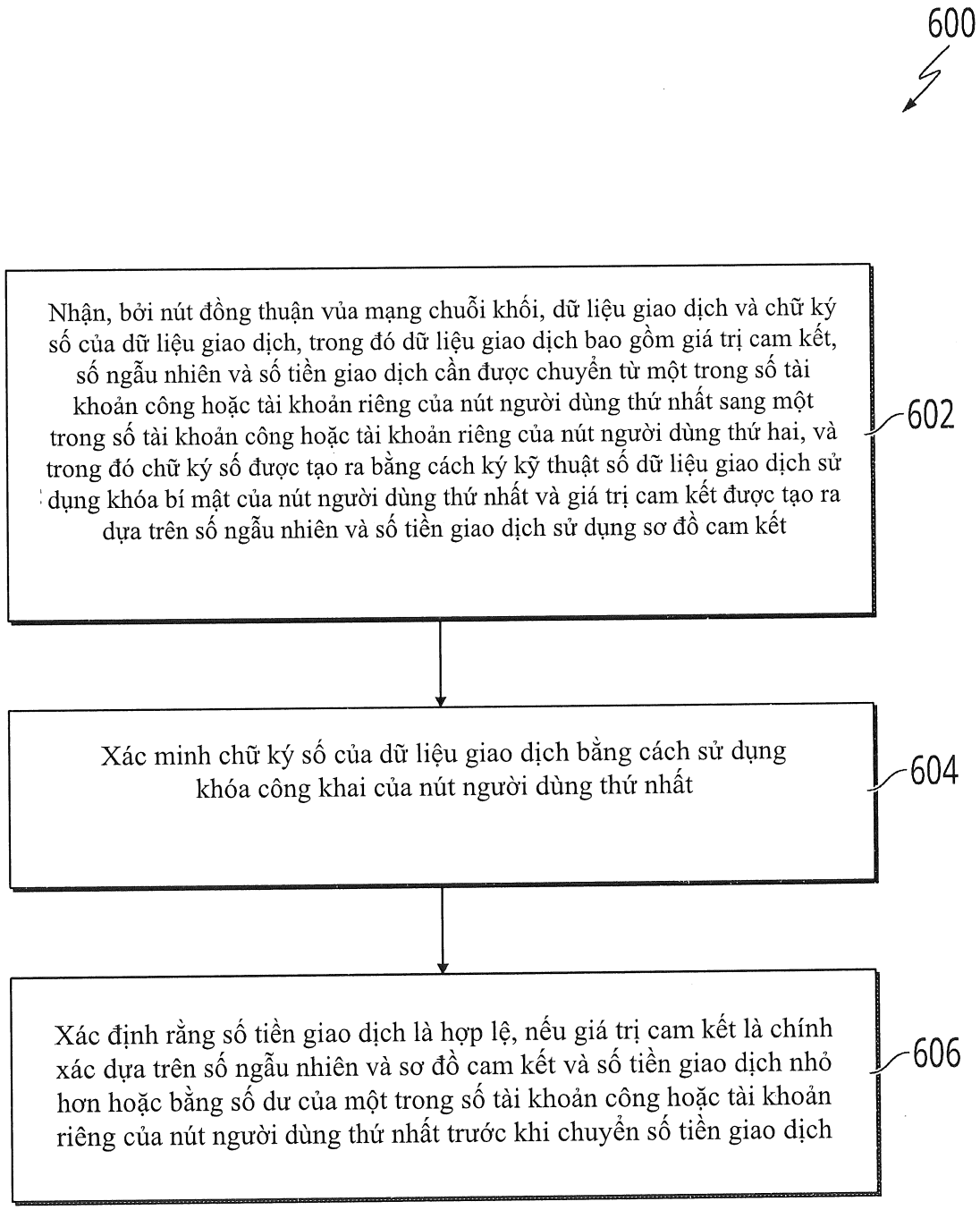

600
Nhận, bởi nút đồng thuận vủa mạng chuỗi khối, dữ liệu giao dịch và chữ ký số của dữ liệu giao dịch, trong đó dữ liệu giao dịch bao gồm giá trị cam kết, số ngẫu nhiên và số tiền giao dịch cần được chuyển từ một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ nhất sang một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ hai, và trong đó chữ ký số được tạo ra bằng cách ký kỹ thuật số dữ liệu giao dịch sử dụng khóa bí mật của nút người dùng thứ nhất và giá trị cam kết được tạo ra dựa trên số ngẫu nhiên và số tiền giao dịch sử dụng sơ đồ cam kết
602
Xác minh chữ ký số của dữ liệu giao dịch bằng cách sử dụng khóa công khai của nút người dùng thứ nhất
604
Xác định rằng số tiền giao dịch là hợp lệ, nếu giá trị cam kết là chính xác dựa trên số ngẫu nhiên và sơ đồ cam kết và số tiền giao dịch nhỏ hơn hoặc bằng số dư của một trong số tài khoản công hoặc tài khoản riêng của nút người dùng thứ nhất trước khi chuyển số tiền giao dịch
606

FIG. 6