(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) **1-0037593**

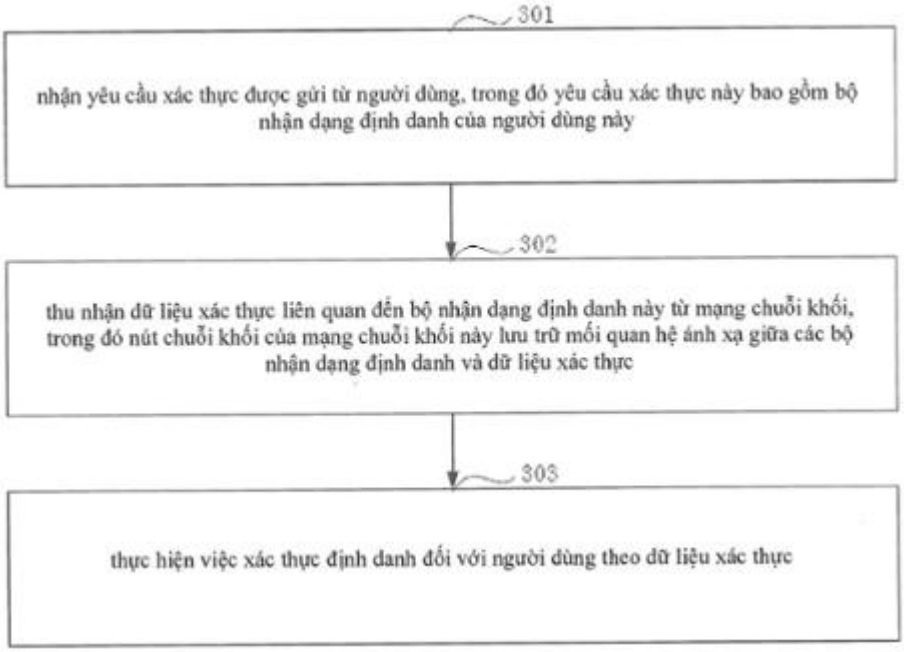
(51)[7] **H04L 29/06**; H04L 9/32

(13) **B**

(21) 1-2019-04134
(22) 14/06/2018
(86) PCT/CN2018/091198 14/06/2018
(87) WO2018/233536 27/12/2018
(30) 201710465995.2 19/06/2017 CN
(45) 27/11/2023 428
(43) 25/10/2019 379A
(73) ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) LI, Kejia (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ XÁC THỰC VÀ PHƯƠNG TIỆN PHI CHUYỂN TIẾP ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(57) Sáng chế đề cập đến phương pháp xác thực và phương pháp và thiết bị xử lý dữ liệu xác thực dựa trên chuỗi khối (blockchain). Sau khi yêu cầu xác thực được gửi từ người dùng được nhận, dữ liệu xác thực liên quan đến bộ nhận dạng định danh được thu nhận từ mạng chuỗi khối, và việc xác thực định danh được thực hiện đối với người dùng theo dữ liệu xác thực này. Dựa trên các đặc điểm chẳng hạn như việc phi tập trung hóa và chống giả mạo của mạng chuỗi khối, mối quan hệ ánh xạ giữa các bộ nhận dạng định danh của các người dùng khác nhau và dữ liệu xác thực được lưu trữ trước trong nút chuỗi khối của mạng chuỗi khối. Khi cung cấp dịch vụ cho người dùng, nền tảng dịch vụ Internet có thể thực hiện việc xác thực định danh đối với người dùng dựa trên dữ liệu xác thực được lưu trữ trong mạng chuỗi khối, do vậy cải thiện hiệu quả xử lý của việc xác thực định danh. Do dữ liệu xác thực có thể được chia sẻ giữa các nền tảng dịch vụ Internet khác nhau thông qua mạng chuỗi khối, người dùng không cần trình thông tin định danh mỗi khi đăng ký với hoặc đăng nhập vào nền tảng dịch vụ mới, và việc sử dụng không đúng thông tin định danh bởi kẻ mạo danh do sự rò rỉ thông tin định danh có thể được ngăn chặn một cách hiệu quả, do đó cải thiện một cách hiệu quả độ chính xác của việc xác thực định danh.


301
nhận yêu cầu xác thực được gửi từ người dùng, trong đó yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này
302
thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh này từ mạng chuỗi khối, trong đó nút chuỗi khối của mạng chuỗi khối này lưu trữ mối quan hệ ánh xạ giữa các bộ nhận dạng định danh và dữ liệu xác thực
303
thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập tới lĩnh vực của các công nghệ xử lý thông tin Internet và các công nghệ máy tính, và cụ thể hơn là, đề cập đến phương pháp xác thực và phương pháp và thiết bị xử lý dữ liệu xác thực dựa trên chuỗi khối (blockchain).

Tình trạng kỹ thuật của sáng chế

Với sự phát triển của công nghiệp Internet, ngày càng nhiều ngành sử dụng Internet để cung cấp các dịch vụ cho người dùng. Xác thực định danh là bước quan trọng trong quá trình cung cấp các dịch vụ qua Internet.

Máy chủ tương ứng với nền tảng dịch vụ Internet đang cung cấp các dịch vụ nhìn chung xác thực định danh của người dùng đang yêu cầu dịch vụ bằng cách sử dụng các phương pháp sau đây:

Phương pháp thứ nhất:

Liên kết dữ liệu được thiết lập từ trước giữa máy chủ (ở dưới đây được gọi là máy chủ thứ nhất) tương ứng với nền tảng dịch vụ Internet và máy chủ (sau đây được gọi là máy chủ thứ hai) tương ứng với nền tảng quản lý định danh (ví dụ, cơ quan an ninh công cộng hoặc các cơ quan nhà nước khác);

khi nhận yêu cầu dịch vụ được gửi từ người dùng, máy chủ thứ nhất tạo ra yêu cầu xác thực theo thông tin định danh của người dùng được chứa trong yêu cầu dịch vụ (trong đó thông tin định danh có thể bao gồm thông tin như bộ nhận dạng định danh), và gửi yêu cầu xác thực đến máy chủ thứ hai qua liên kết dữ liệu đã được thiết lập từ trước;

máy chủ thứ hai nhận yêu cầu xác thực được gửi từ máy chủ thứ nhất, xác thực thông tin định danh được chứa trong yêu cầu xác thực, và gửi kết quả xác thực đến máy chủ thứ nhất;

khi nhận kết quả xác thực, máy chủ thứ nhất hoàn thành việc xác thực định danh đối với người dùng theo kết quả xác thực này.

Tuy nhiên, do các nền tảng dịch vụ Internet khác nhau có thể thu nhận thông tin

định danh của người dùng, sự rò rỉ thông tin định danh của người dùng có thể xảy ra.

Phương pháp thứ hai:

Để ngăn chặn sự rò rỉ thông tin định danh, người dùng sử dụng thông tin định danh để đăng ký với máy chủ thứ hai để nhận định danh điện tử (electronic identity, eID). Theo cách này, khi yêu cầu dịch vụ, người dùng có thể gửi eID đến máy chủ thứ nhất, và máy chủ thứ nhất có thể thực thi việc xác thực định danh đối với người dùng bằng cách sử dụng phương pháp thứ nhất.

Tuy nhiên, do việc xác thực định danh được thực hiện bởi mỗi nền tảng dịch vụ Internet đối với người dùng cần có dự can dự của máy chủ thứ hai, máy chủ thứ hai cần xử lý một số lượng lớn các yêu cầu xác thực, dẫn đến hiệu quả thấp trong việc xử lý các yêu cầu xác thực và thời gian bắt buộc để nền tảng dịch vụ Internet xử lý dịch vụ được yêu cầu trở nên lâu hơn. Kết quả là, trải nghiệm người dùng về dịch vụ được cung cấp bởi nền tảng dịch vụ Internet là kém.

Bản chất kỹ thuật của sáng chế

Xem xét vấn đề này, các phương án của sáng chế đề xuất phương pháp xác thực và phương pháp và thiết bị xử lý dữ liệu xác thực dựa trên chuỗi khối, để giải quyết vấn đề hiệu suất xử lý thấp của các phương pháp xác thực định danh trong giải pháp kỹ thuật đã biết.

Các phương án của sáng chế sử dụng các giải pháp kỹ thuật sau đây.

Các phương án của sáng chế đề xuất phương pháp xác thực, bao gồm các bước:

nhận yêu cầu xác thực được gửi từ người dùng, trong đó yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này;

thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh này từ mạng chuỗi khối, trong đó nút chuỗi khối của mạng chuỗi khối này lưu trữ mối quan hệ ánh xạ giữa các bộ nhận dạng định danh và dữ liệu xác thực; và

thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực này.

Các phương án của sáng chế còn đề xuất phương pháp xử lý dữ liệu xác thực dựa trên chuỗi khối, bao gồm các bước:

nhận thông tin định danh được gửi từ người dùng, và xác thực thông tin định danh này;

tạo ra dữ liệu xác thực thứ nhất theo kết quả xác thực, trong đó dữ liệu xác thực

thứ nhất này bao gồm kết quả xác thực, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng; và

lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối.

Các phương án của sáng chế còn đề xuất thiết bị xác thực, bao gồm:

đơn vị nhận được tạo cấu hình để nhận yêu cầu xác thực được gửi từ người dùng, trong đó yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này;

đơn vị thu nhận được tạo cấu hình để thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối, trong đó nút chuỗi khối của mạng chuỗi khối này lưu trữ mối quan hệ ánh xạ giữa các bộ nhận dạng định danh và dữ liệu xác thực; và

đơn vị xác thực được tạo cấu hình để thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực này.

Các phương án của sáng chế còn đề xuất thiết bị xử lý dữ liệu xác thực dựa trên chuỗi khối, bao gồm:

đơn vị nhận được tạo cấu hình để nhận thông tin định danh được gửi từ người dùng, và xác thực thông tin định danh này;

đơn vị xử lý được tạo cấu hình để tạo ra dữ liệu xác thực thứ nhất theo kết quả xác thực, trong đó dữ liệu xác thực thứ nhất này bao gồm kết quả xác thực, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng; và

đơn vị lưu trữ được tạo cấu hình để lưu trữ dữ liệu xác thực thứ nhất này vào nút chuỗi khối của mạng chuỗi khối.

Các phương án của sáng chế còn đề xuất thiết bị xác thực, bao gồm ít nhất một bộ nhớ và ít nhất một bộ xử lý, trong đó ít nhất một bộ nhớ này lưu trữ chương trình và thiết bị này được tạo cấu hình để thực thi các bước sau đây bằng ít nhất một bộ xử lý này:

nhận yêu cầu xác thực được gửi từ người dùng, trong đó yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này;

thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh này từ mạng chuỗi khối, trong đó nút chuỗi khối của mạng chuỗi khối này lưu trữ mối quan hệ ánh xạ giữa các bộ nhận dạng định danh và dữ liệu xác thực; và

thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực này.

Các phương án của sáng chế còn đề xuất thiết bị xử lý dữ liệu xác thực dựa trên chuỗi khối, bao gồm ít nhất một bộ nhớ và ít nhất một bộ xử lý, trong đó ít nhất một bộ nhớ này lưu trữ chương trình và thiết bị này được tạo cấu hình để thực thi các bước sau đây bằng ít nhất một bộ xử lý này:

nhận thông tin định danh được gửi từ người dùng, và xác thực thông tin định danh này;

tạo ra dữ liệu xác thực thứ nhất theo kết quả xác thực, trong đó dữ liệu xác thực thứ nhất này bao gồm kết quả xác thực, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng; và

lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối.

Ít nhất một giải pháp kỹ thuật được sử dụng bởi các phương án của sáng chế có thể đạt được các hiệu quả có lợi sau đây:

Với giải pháp kỹ thuật được đề xuất bởi sáng chế, sau khi yêu cầu xác thực được gửi từ người dùng được nhận, dữ liệu xác thực liên quan đến bộ nhận dạng định danh của người dùng được thu nhận từ mạng chuỗi khối, và việc xác thực định danh được thực hiện đối với người dùng theo dữ liệu xác thực này. Theo cách này, dựa trên các đặc điểm như việc phi tập trung hóa và chống giả mạo của mạng chuỗi khối, mối quan hệ ánh xạ giữa các bộ nhận dạng định danh của các người dùng khác nhau và dữ liệu xác thực được lưu trữ trước trong nút chuỗi khối của mạng chuỗi khối. Khi cung cấp dịch vụ cho người dùng, nền tảng dịch vụ Internet có thể thực hiện việc xác thực định danh đối với người dùng dựa trên dữ liệu xác thực được lưu trữ trong mạng chuỗi khối, để tránh vấn đề hiệu quả trong việc xử lý các yêu cầu xác thực thấp do thực tế là có một số lượng lớn các yêu cầu xác thực định danh cần được xử lý bởi nền tảng quản lý định danh, nhờ đó cải thiện hiệu quả xử lý của việc xác thực định danh. Do dữ liệu xác thực có thể được chia sẻ giữa các nền tảng dịch vụ Internet khác nhau thông qua mạng chuỗi khối, người dùng không cần trình thông tin định danh mỗi khi đăng ký với hoặc đăng nhập vào nền tảng dịch vụ mới, và việc sử dụng không đúng thông tin định danh bởi kẻ mạo danh do sự rò rỉ thông tin định danh có thể được ngăn chặn một cách hiệu quả, do vậy cải thiện một cách hiệu quả độ chính xác của việc xác thực định danh.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo được mô tả ở đây được cung cấp để hiểu rõ hơn về sáng chế và cấu tạo thành nên một phần của sáng chế. Các phương án sơ đồ của sáng chế và phần mô tả của chúng được sử dụng để minh họa sáng chế, nhưng không tạo thành sự giới hạn không thích hợp bất kỳ đối với sáng chế. Trên các hình vẽ kèm theo:

Fig.1 là lưu đồ sơ lược của phương pháp xử lý dữ liệu xác thực dựa trên chuỗi khối theo một phương án của sáng chế;

Fig.2 là sơ đồ cấu trúc giản lược của dữ liệu xác thực trong mạng chuỗi khối theo một phương án của sáng chế;

Fig.3 là lưu đồ sơ lược của phương pháp xác thực theo một phương án của sáng chế;

Fig.4 là lưu đồ sơ lược của phương pháp xác thực theo một phương án của sáng chế;

Fig.5 là lưu đồ sơ lược của phương pháp xác thực theo một phương án của sáng chế;

Fig.6 là sơ đồ cấu trúc của hệ thống xác thực định danh theo một phương án của sáng chế;

Fig.7 là sơ đồ cấu trúc giản lược của thiết bị xác thực theo một phương án của sáng chế; và

Fig.8 là sơ đồ cấu trúc giản lược của thiết bị xử lý dữ liệu xác thực dựa trên chuỗi khối theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

Để đạt được các mục đích của sáng chế, các phương án của sáng chế đề xuất phương pháp xác thực và phương pháp và thiết bị xử lý dữ liệu xác thực dựa trên chuỗi khối. Sau khi yêu cầu xác thực được gửi từ người dùng được nhận, dữ liệu xác thực liên quan đến bộ nhận dạng định danh của người dùng được thu nhận từ mạng chuỗi khối, và việc xác thực định danh được thực hiện đối với người dùng theo dữ liệu xác thực này.

Theo cách này, dựa trên các đặc điểm như việc phi tập trung hóa và chống giả mạo của mạng chuỗi khối, mối quan hệ ánh xạ giữa các bộ nhận dạng định danh của các người dùng khác nhau và dữ liệu xác thực được lưu trữ trước trong nút chuỗi khối của mạng chuỗi khối. Khi cung cấp dịch vụ cho người dùng, nền tảng dịch vụ Internet có thể thực hiện việc xác thực định danh đối với người dùng dựa trên dữ liệu xác thực được

lưu trữ trong mạng chuỗi khối, để tránh vấn đề hiệu quả trong việc xử lý các yêu cầu xác thực thấp do thực tế là có một số lượng lớn các yêu cầu xác thực định danh cần được xử lý bởi nền tảng quản lý định danh, nhờ đó cải thiện hiệu quả xử lý của việc xác thực định danh. Do dữ liệu xác thực có thể được chia sẻ giữa các nền tảng dịch vụ Internet khác nhau thông qua mạng chuỗi khối, người dùng không cần trình thông tin định danh mỗi khi đăng ký với hoặc đăng nhập vào nền tảng dịch vụ mới, và việc sử dụng không đúng thông tin định danh bởi kẻ mạo danh do sự rò rỉ thông tin định danh có thể được ngăn chặn một cách hiệu quả, do vậy cải thiện một cách hiệu quả độ chính xác của việc xác thực định danh.

Cần lưu ý rằng, "mối quan hệ ánh xạ giữa các bộ nhận dạng định danh của các người dùng khác nhau và dữ liệu xác thực được lưu trữ trước trong nút chuỗi khối của mạng chuỗi khối" theo các phương án của sáng chế, có thể được lưu trữ bởi máy chủ tương ứng với nền tảng quản lý định danh khi người dùng đăng ký với máy chủ tương ứng với nền tảng quản lý định danh này, hoặc có thể được lưu trữ bởi nền tảng dịch vụ Internet cung cấp các dịch vụ khi người dùng yêu cầu dịch vụ từ nền tảng dịch vụ Internet này, điều này không bị giới hạn cụ thể ở đây.

Nhằm làm rõ ràng hơn các mục đích, các giải pháp kỹ thuật, và các ưu điểm của sáng chế, các giải pháp kỹ thuật của sáng chế sẽ được mô tả một cách rõ ràng và thấu đáo dưới đây với tham chiếu đến các phương án cụ thể của sáng chế và các hình vẽ tương ứng. Rõ ràng, các phương án được mô tả chỉ là một số phương án mà không phải tất cả các phương án của sáng chế. Trên cơ sở các phương án trong sáng chế, tất cả các phương án khác thu được bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật mà không cần các nỗ lực sáng tạo sẽ thuộc về phạm vi bảo hộ của sáng chế.

Các giải pháp kỹ thuật được đề xuất bởi các phương án của sáng chế được mô tả chi tiết dưới đây với tham chiếu đến các hình vẽ kèm theo.

Fig.1 là lưu đồ sơ lược của phương pháp xử lý dữ liệu xác thực dựa trên chuỗi khối theo một phương án của sáng chế. Phương pháp này có thể được mô tả như sau. Phương án này của sáng chế có thể được thực thi bởi máy chủ tương ứng với nền tảng quản lý định danh.

Bước 101: nhận thông tin định danh được gửi từ người dùng, và xác thực thông tin định danh này.

Theo các phương án của sáng chế, máy chủ tương ứng với nền tảng quản lý định danh có thể là máy chủ quản lý đăng ký hộ khẩu của cơ quan an ninh công cộng hoặc có thể là máy chủ tương ứng với tổ chức tài chính. Điều đó có nghĩa là, việc xác thực định danh được thực hiện bởi máy chủ tương ứng với nền tảng quản lý định danh đã nêu theo các phương án của sáng chế có mức tín nhiệm cao.

Cụ thể, máy chủ tương ứng với nền tảng quản lý định danh có thể nhận thông tin định danh được gửi từ người dùng trong quá trình đăng ký của người dùng hoặc có thể nhận thông tin định danh mà được gửi từ người dùng khi người dùng khởi tạo dịch vụ (ví dụ, dịch vụ gửi tiền, dịch vụ rút tiền, dịch vụ chuyển khoản, v.v.). Trong trường hợp này, máy chủ tương ứng với nền tảng quản lý định danh cần xác thực thông tin định danh nhận được.

Ở đây, thông tin định danh bao gồm thông tin đặc điểm định danh khác nhau như tên, tuổi, số thẻ định danh, và số thẻ ngân hàng của người dùng. Máy chủ tương ứng với nền tảng quản lý định danh có thể xác thực thông tin định danh nhận được dựa trên thông tin đặc điểm định danh được lưu trữ của người dùng, để xác định liệu thông tin định danh có hợp lệ hay không.

Ví dụ, máy chủ tương ứng với nền tảng quản lý định danh là máy chủ tương ứng với tổ chức tài chính, và người dùng cung cấp thông tin định danh cho máy chủ tương ứng với tổ chức tài chính khi mở tài khoản. Trong trường hợp này, máy chủ tương ứng với tổ chức tài chính có thể xác thực thông tin định danh được cung cấp bởi người dùng. Khi xác định rằng thông tin định danh của người dùng là hợp lệ, thông tin tài khoản ngân hàng được ấn định cho người dùng, và mối quan hệ ánh xạ được thiết lập giữa thông tin tài khoản ngân hàng của người dùng (ví dụ, số thẻ ngân hàng) và thông tin định danh của người dùng.

Cần lưu ý rằng, theo các phương án của sáng chế, nếu xác định rằng thông tin định danh là hợp lệ sau khi xác thực thông tin định danh, máy chủ tương ứng với nền tảng quản lý định danh có thể còn tạo ra bộ nhận dạng định danh cho người dùng. Bộ nhận dạng định danh có thể xác dịnh duy nhất người dùng. Ở đây, bộ nhận dạng định danh có thể là eID, hoặc ở các dạng khác, điều này không bị giới hạn cụ thể ở đây.

Bước 102: tạo ra dữ liệu xác thực thứ nhất theo kết quả xác thực, trong đó dữ liệu xác thực thứ nhất bao gồm kết quả xác thực, bộ nhận dạng tổ chức của tổ chức mà nó

tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng.

Theo các phương án của sáng chế, kết quả xác thực có thể là việc xác thực thành công, chỉ ra rằng thông tin định danh của người dùng là hợp lệ; hoặc có thể là việc xác thực thất bại, chỉ ra rằng thông tin định danh của người dùng là bất thường hoặc không hợp lệ.

Bất kể kết quả xác thực, dữ liệu xác thực thứ nhất ở đây có thể được tạo ra dựa trên kết quả xác thực thu được. Ở đây, "thứ nhất", "thứ hai", và "thứ ba" trong "dữ liệu xác thực thứ nhất" và "dữ liệu xác thực thứ hai" và "dữ liệu xác thực thứ ba" sau đây không có ý nghĩa đặc biệt và chỉ được sử dụng để thể hiện dữ liệu xác thực khác nhau.

Cụ thể, khi kết quả xác minh chỉ ra rằng thông tin định danh là hợp lệ, dữ liệu xác thực thứ nhất được thu theo kết quả xác thực, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng. Điều đó có nghĩa là, nếu tiếp đó thu nhận dữ liệu xác thực thứ nhất, máy chủ tương ứng với nền tảng dịch vụ Internet có thể xác định theo dữ liệu xác thực thứ nhất này rằng thông tin định danh của người dùng là hợp lệ, do vậy cải thiện hiệu quả xử lý xác thực một cách hiệu quả.

Khi kết quả xác thực chỉ ra rằng thông tin định danh là bất thường hoặc không hợp lệ, dữ liệu xác thực thứ ba có thể được thu theo kết quả xác thực, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng.

Theo các phương án của sáng chế, mức xác thực có thể được xác định cho máy chủ tương ứng với nền tảng quản lý định danh, tức là, các kết quả xác thực được xác định bởi các máy chủ tương ứng với các nền tảng quản lý định danh có các mức xác thực khác nhau tương ứng với các mức tín nhiệm khác nhau. Mức xác thực càng cao, mức tín nhiệm tương ứng với kết quả xác thực được xác định càng cao; ngược lại, mức xác thực càng thấp, mức tín nhiệm tương ứng với kết quả xác thực được xác định càng thấp. Do dữ liệu xác thực bao gồm bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, mức tín nhiệm của kết quả xác thực được tạo ra bởi bộ nhận dạng tổ chức có thể được xác định theo mối quan hệ ánh xạ giữa bộ nhận dạng tổ chức và mức xác thực, do vậy đảm bảo một cách hiệu quả độ chính xác của việc xác thực định danh.

Bước 103: lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối.

Theo các phương án của sáng chế, máy chủ tương ứng với nền tảng quản lý định

danh có thể đóng vai trò là nút chuỗi khối trong mạng chuỗi khối hoặc có thể đóng vai trò là thiết bị độc lập của mạng chuỗi khối, điều này không bị giới hạn cụ thể ở đây.

Nếu máy chủ tương ứng với nền tảng quản lý định danh là nút chuỗi khối trong mạng chuỗi khối, máy chủ tương ứng với nền tảng quản lý định danh, sau khi thu được dữ liệu xác thực (ví dụ, dữ liệu xác thực thứ nhất hoặc dữ liệu xác thực thứ ba), có thể phát quảng bá dữ liệu xác thực này đến các nút chuỗi khối khác trong mạng chuỗi khối, sao cho các nút chuỗi khối khác thực hiện việc xử lý đồng thuận trên dữ liệu xác thực này. Khi kết quả xử lý đồng thuận chỉ ra rằng việc xác thực đồng thuận đã được vượt qua, máy chủ tương ứng với nền tảng quản lý định danh lưu trữ dữ liệu xác thực thứ nhất vào khối được tạo mới, và lưu trữ khối này vào nút chuỗi khối của mạng chuỗi khối.

Nếu máy chủ tương ứng với nền tảng quản lý định danh là thiết bị độc lập của mạng chuỗi khối, máy chủ tương ứng với nền tảng quản lý định danh, sau khi thu được dữ liệu xác thực (ví dụ, dữ liệu xác thực thứ nhất hoặc dữ liệu xác thực thứ ba), có thể gửi dữ liệu xác thực này đến nút chuỗi khối bất kỳ trong mạng chuỗi khối. Nút chuỗi khối này phát quảng bá dữ liệu xác thực này đến các nút chuỗi khối khác trong mạng chuỗi khối, sao cho các nút chuỗi khối khác thực hiện việc xử lý đồng thuận trên dữ liệu xác thực này. Khi kết quả xử lý đồng thuận chỉ ra rằng việc xác nhận đồng thuận đã được vượt qua, nút chuỗi khối đã nêu lưu trữ dữ liệu xác thực thứ nhất vào khối được tạo mới, và lưu trữ khối này vào nút chuỗi khối của mạng chuỗi khối.

Để đảm bảo sự bảo mật của thông tin định danh, theo các phương án của sáng chế, kết quả xác thực có thể được lưu trữ trong mạng chuỗi khối, và thông tin định danh có thể được lưu trữ trong cơ sở dữ liệu thông tin định danh, để ngăn chặn sự rò rỉ thông tin định danh. Ở đây, cơ sở dữ liệu thông tin định danh không được đặt trong mạng chuỗi khối và có thể được lưu trữ trong máy chủ tương ứng với nền tảng quản lý định danh.

Cụ thể, mối quan hệ ánh xạ được thiết lập giữa các bộ nhận dạng định danh của các người dùng và thông tin định danh của các người dùng; và thông tin định danh của người dùng được lưu trữ vào cơ sở dữ liệu thông tin định danh theo mối quan hệ ánh xạ.

Theo các phương án của sáng chế, do trạng thái của một số thông tin đặc điểm định danh trong thông tin định danh của người dùng có thể thay đổi do một số yếu tố bên ngoài, ví dụ, trạng thái của số thẻ định danh của người dùng thay đổi từ trạng thái bình thường thành trạng thái bị mất do do người dùng mất thẻ định danh, khi đó máy chủ

tương ứng với nền tảng quản lý định danh tạo ra dữ liệu xác thực khác phụ thuộc vào các tình huống khác nhau, để đảm bảo rằng kết quả xác thực là nhất quán với tình huống thực tế của thông tin định danh của người dùng.

Cụ thể, báo cáo mất hoặc yêu cầu không đăng ký được gửi từ người dùng được nhận, trong đó báo cáo mất hoặc yêu cầu không đăng ký này bao gồm bộ nhận dạng định danh của người dùng;

xác định được theo báo cáo mất hoặc yêu cầu không đăng ký rằng thông tin định danh của người dùng có trạng thái bất thường;

dữ liệu xác thực thứ hai được tạo ra theo thông tin định danh của người dùng đang ở trạng thái bất thường, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng; và

dữ liệu xác thực thứ hai này được lưu trữ vào nút chuỗi khối của mạng chuỗi khối.

Nói cách khác, ngay khi nhận yêu cầu thay đổi được gửi từ người dùng (bao gồm yêu cầu báo cáo mất, yêu cầu không đăng ký, yêu cầu hồ sơ cá nhân, v.v.), máy chủ tương ứng với nền tảng quản lý định danh xác định trạng thái hiện tại của thông tin định danh của người dùng theo yêu cầu thay đổi này, và sau đó tạo ra dữ liệu xác thực thứ hai theo trạng thái hiện tại của thông tin định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng.

Tương tự, khi dữ liệu xác thực thứ hai được lưu trữ vào nút chuỗi khối của mạng chuỗi khối, việc xử lý đồng thuận trên dữ liệu xác thực thứ hai có thể được khởi tạo. Cách xử lý đồng thuận là giống hoặc tương tự với cách xử lý đồng thuận trên dữ liệu xác thực thứ nhất. Có thể tham chiếu đến các nội dung đã được mô tả trên đây, và các chi tiết sẽ không được mô tả lặp lại ở đây.

Cần lưu ý rằng các máy chủ tương ứng với các nền tảng quản lý định danh được mô tả theo các phương án của sáng chế có thể đóng vai trò là các nút chuỗi khối trong chuỗi khối liên doanh, và dữ liệu xác thực được tạo ra bởi các máy chủ có thể được sử dụng bởi các máy chủ khác mà chúng chấp nhận chuỗi khối liên doanh, do vậy cải thiện hiệu quả xử lý của việc xác thực định danh một cách hiệu quả.

Theo các phương án của sáng chế, để đảm bảo sự bảo mật của dữ liệu xác thực được lưu trữ trong chuỗi khối, dữ liệu xác thực có thể được lưu trữ theo định dạng được thiết lập trước.

Fig.2 là sơ đồ cấu trúc giản lược của dữ liệu xác thực trong mạng chuỗi khối theo một phương án của sáng chế.

Như có thể thấy từ Fig.2, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực có thể được thể hiện bằng cách sử dụng khóa công khai và chữ ký số. Tức là, cặp khóa công khai và riêng có thể được thiết lập từ trước cho các tình huống khác nhau. Theo cách này, bản tóm lược tương ứng với bộ nhận dạng tổ chức có thể được mã hóa bằng cách sử dụng khóa riêng để thu được chữ ký số, và khóa công khai và chữ ký số này được sử dụng làm thông tin tổ chức của tổ chức tạo ra kết quả xác thực trong dữ liệu xác thực.

Bộ nhận dạng định danh của người dùng cũng có thể được thể hiện bằng cách sử dụng khóa công khai và chữ ký số. Tức là, cặp khóa công khai và riêng có thể được thiết lập từ trước cho người dùng. Sau khi thông tin định danh của người dùng được xác thực, bản tóm lược tương ứng với thông tin định danh của người dùng được mã hóa bằng cách sử dụng khóa riêng để thu được chữ ký số, và khóa công khai và chữ ký số này được sử dụng làm bộ nhận dạng định danh của người dùng trong dữ liệu xác thực.

Điều đó có nghĩa là, dữ liệu xác thực được lưu trữ trong nút chuỗi khối của mạng chuỗi khối có thể được lưu trữ ở dạng được thể hiện trong bảng 1:

Bảng 1

Thời gian	Bộ nhận dạng người dùng		Bộ nhận dạng tổ chức		Kết quả xác thực
T1	Khóa công khai	Chữ ký số	Khóa công khai	Chữ ký số	Thành công/thất bại

Fig.3 là lưu đồ sơ lược của phương pháp xác thực theo một phương án của sáng chế. Phương pháp này được mô tả như sau. Phương pháp xác thực này có thể được thực thi bởi máy chủ tương ứng với nền tảng dịch vụ Internet cung cấp các dịch vụ, hoặc thiết bị đầu cuối máy khách ứng dụng đang chạy dưới dạng APP trên thiết bị đầu cuối, điều này không bị giới hạn cụ thể ở đây.

Bước 301: nhận yêu cầu xác thực được gửi từ người dùng, trong đó yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này.

Theo các phương án của sáng chế, yêu cầu xác thực được gửi từ người dùng có thể được gửi bởi người dùng khi gửi yêu cầu xử lý dịch vụ hoặc có thể được gửi bởi người dùng khi đăng nhập vào nền tảng dịch vụ Internet, điều này không bị giới hạn cụ thể ở đây.

Ở đây, bộ nhận dạng định danh có thể nhận dạng duy nhất người dùng, và có thể là tài khoản đăng nhập của người dùng, có thể là eID, hoặc có thể ở các dạng khác, điều này không bị giới hạn cụ thể ở đây.

Bước 302: thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh này từ mạng chuỗi khối, trong đó nút chuỗi khối của mạng chuỗi khối này lưu trữ mối quan hệ ánh xạ giữa các bộ nhận dạng định danh và dữ liệu xác thực.

Theo các phương án của sáng chế, do nút chuỗi khối của mạng chuỗi khối lưu trữ mối quan hệ ánh xạ giữa các bộ nhận dạng định danh và dữ liệu xác thực, khi yêu cầu xác thực được gửi từ người dùng được nhận, dữ liệu xác thực liên quan đến bộ nhận dạng định danh có thể được thu nhận từ mạng chuỗi khối dựa trên bộ nhận dạng định danh của người dùng được chứa trong yêu cầu xác thực và mối quan hệ ánh xạ được lưu trữ trong mỗi nút chuỗi khối của mạng chuỗi khối.

Ưu tiên là, trước khi dữ liệu xác thực liên quan đến bộ nhận dạng định danh được thu nhận, nếu yêu cầu xác thực còn bao gồm khóa công khai và chữ ký số, thì việc liệu chữ ký số này có hợp lệ hay không được xác minh bằng cách sử dụng khóa công khai này, trong đó chữ ký số này được thu bằng cách ký bằng khóa riêng trong cặp khóa công khai và riêng. Việc xác thực chữ ký có thể xác định xem liệu người dùng gửi yêu cầu xác thực có là người dùng mà cặp khóa công khai và riêng được thiết lập cho họ hay không, và do đó đảm bảo sự cần thiết của việc thi hành các quy trình tiếp theo.

Nếu kết quả xác minh chỉ ra rằng chữ ký số là không hợp lệ, quy trình xác thực được kết thúc.

Nếu kết quả xác minh chỉ ra rằng chữ ký số là hợp lệ, dữ liệu xác thực liên quan đến bộ nhận dạng định danh được thu nhận từ mạng chuỗi khối.

Do mỗi nút chuỗi khối của mạng chuỗi khối lưu trữ nhiều mảnh dữ liệu xác thực, phương án này của sáng chế có thể sàng lọc ra dữ liệu xác thực bao gồm bộ nhận dạng định danh từ mạng chuỗi khối dựa trên bộ nhận dạng định danh được chứa trong yêu cầu xác thực và xác định dữ liệu xác thực thu được là dữ liệu xác thực liên quan đến bộ nhận dạng định danh.

Hơn nữa, nếu nhiều hơn một mảnh dữ liệu xác thực được thu sau khi sàng lọc thì dữ liệu xác thực thỏa mãn điều kiện được thiết lập trước được xác định trong dữ liệu xác thực thu được này, và dữ liệu xác thực được xác định này được xác định là dữ liệu xác

thực liên quan đến bộ nhận dạng định danh.

Theo các phương án của sáng chế, điều kiện được thiết lập trước này bao gồm ít nhất một hoặc nhiều thành phần sau đây:

thời gian tạo ra của dữ liệu xác thực thỏa mãn điều kiện về thời gian được thiết lập trước;

bộ nhận dạng tổ chức được chứa trong dữ liệu xác thực thỏa mãn bộ nhận dạng tổ chức của tổ chức phát hành được thiết lập trước; và

loại dịch vụ được chứa trong dữ liệu xác thực là giống với loại dịch vụ của dịch vụ được khởi tạo bởi người dùng.

Cụ thể, nếu điều kiện được thiết lập trước là việc thời gian tạo ra của dữ liệu xác thực thỏa mãn điều kiện về thời gian được thiết lập trước thì các thời gian tạo ra của các mảnh dữ liệu xác thực thu được sau khi sàng lọc được xác định, dữ liệu xác thực tương ứng với thời gian tạo ra thỏa mãn điều kiện thời gian được thiết lập trước này được xác định theo các thời gian tạo ra của các mảnh dữ liệu xác thực, và dữ liệu xác thực được xác định này được xác định là dữ liệu xác thực liên quan đến bộ nhận dạng định danh.

Giả sử rằng điều kiện về thời gian được thiết lập trước là việc chênh lệch thời gian giữa thời gian tạo ra của dữ liệu xác thực và thời gian hiện tại là nhỏ nhất, sau khi các thời gian tạo ra của các mảnh dữ liệu xác thực thu được sau khi sàng lọc được xác định, các mảnh dữ liệu xác thực này được sắp xếp theo thứ tự thời gian của các thời gian tạo ra, khi đó dữ liệu xác thực tương ứng với thời gian tạo ra gần với thời gian hiện tại nhất được lựa chọn theo kết quả sắp xếp, và dữ liệu xác thực được xác định này được xác định là dữ liệu xác thực liên quan đến bộ nhận dạng định danh.

Cần lưu ý rằng thời gian tạo ra của dữ liệu xác thực có thể là thời gian mà ở đó kết quả xác thực được tạo ra, có thể là thời gian mà ở đó dữ liệu xác thực được lưu trữ vào nút chuỗi khối của mạng chuỗi khối, hoặc có thể là thời gian mà ở đó nút chuỗi khối của mạng chuỗi khối chấp nhận dữ liệu xác thực, điều này không bị giới hạn cụ thể ở đây.

Nếu điều kiện được thiết lập trước là việc bộ nhận dạng tổ chức được chứa trong dữ liệu xác thực thỏa mãn bộ nhận dạng tổ chức của tổ chức phát hành được thiết lập trước thì các bộ nhận dạng tổ chức tương ứng với các mảnh dữ liệu xác thực thu được sau khi sàng lọc được xác định, dữ liệu xác thực trong đó các bộ nhận dạng tổ chức thỏa mãn bộ nhận dạng tổ chức của tổ chức phát hành được thiết lập trước được xác định

theo các bộ nhận dạng tổ chức tương ứng với các mảnh dữ liệu xác thực này, và dữ liệu xác thực được xác định này được xác định là dữ liệu xác thực liên quan đến bộ nhận dạng định danh.

Giả sử rằng bộ nhận dạng tổ chức của tổ chức phát hành được thiết lập trước là 10000, sau khi các bộ nhận dạng tổ chức tương ứng với các mảnh dữ liệu xác thực thu được sau khi sàng lọc được xác định, dữ liệu xác thực trong đó các bộ nhận dạng tổ chức là 10000 được xác định là dữ liệu xác thực liên quan đến bộ nhận dạng định danh.

Cần lưu ý rằng bộ nhận dạng tổ chức ở đây có thể là chuỗi ký tự hoặc có thể là khóa công khai và chữ ký số. Nếu bộ nhận dạng tổ chức là khóa công khai và chữ ký số, các khóa công khai của các tổ chức tương ứng với các mảnh dữ liệu xác thực thu được sau khi sàng lọc được xác định, dữ liệu xác thực trong đó các khóa công khai thỏa mãn khóa công khai của tổ chức phát hành được thiết lập trước được xác định theo các khóa công khai của các tổ chức tương ứng với các mảnh dữ liệu xác thực này, và dữ liệu xác thực được xác định này được xác định là dữ liệu xác thực liên quan đến bộ nhận dạng định danh.

Cần lưu ý rằng, theo các phương án của sáng chế, có thể có nhiều hơn một mảnh dữ liệu xác thực trong đó các bộ nhận dạng tổ chức thỏa mãn bộ nhận dạng tổ chức của tổ chức phát hành được thiết lập trước. Nếu số lượng này là nhiều hơn một, dữ liệu xác thực bao gồm bộ nhận dạng tổ chức tương ứng với tổ chức có mức xác thực cao nhất có thể được ưu tiên thu nhận theo các mức xác thực của các tổ chức phát hành. Nếu dữ liệu xác thực bao gồm bộ nhận dạng tổ chức tương ứng với tổ chức có mức xác thực cao nhất không được tìm thấy, dữ liệu xác thực bao gồm bộ nhận dạng tổ chức tương ứng với tổ chức có mức xác thực cao nhất thứ hai được thu nhận. Theo cách này, tính xác thực và tính hợp lệ của dữ liệu xác thực có thể được đảm bảo, do vậy đảm bảo độ chính xác của kết quả xác thực.

Nếu điều kiện được thiết lập trước là việc loại dịch vụ được chứa trong dữ liệu xác thực là giống với loại dịch vụ của dịch vụ được khởi tạo bởi người dùng, loại dịch vụ của dịch vụ được khởi tạo bởi người dùng này được xác định, các loại dịch vụ được chứa trong các mảnh dữ liệu xác thực thu được sau khi sàng lọc được xác định, dữ liệu xác thực bao gồm loại dịch vụ mà nó là giống với loại dịch vụ của dịch vụ được khởi tạo bởi người dùng được xác định theo các loại dịch vụ được chứa trong các mảnh dữ

liệu xác thực, và dữ liệu xác thực được xác định này được xác định là dữ liệu xác thực liên quan đến bộ nhận dạng định danh.

Do các dịch vụ của cùng loại dịch vụ có các yêu cầu tương tự nhau đối với việc xác thực định danh của người dùng, việc xác thực định danh của người dùng theo dữ liệu xác thực được tạo ra bởi các nền tảng dịch vụ Internet khác nhau cung cấp các dịch vụ giống nhau có thể đảm bảo độ chính xác của kết quả xác thực.

Cần lưu ý rằng, trong quá trình sàng lọc dữ liệu xác thực, ba điều kiện được thiết lập trước được mô tả trên đây có thể được sử dụng hoặc theo cách riêng rẽ hoặc theo cách kết hợp, điều này không bị giới hạn cụ thể ở đây. Ngoài ba điều kiện được thiết lập trước nêu trên, các điều kiện được thiết lập trước khác cũng có thể được thiết lập nếu cần, mà chúng sẽ không được liệt kê ở đây.

Bước 303: thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực.

Theo các phương án của sáng chế, xác định trạng thái xác thực hiện tại của bộ nhận dạng định danh theo dữ liệu xác thực; và nếu bộ nhận dạng định danh có trạng thái bất thường và/hoặc trạng thái xác thực lỗi thì xác định rằng việc xác thực định danh đối với người dùng là không thành công; nếu không thì xác định rằng việc xác thực định danh đối với người dùng là thành công.

Trạng thái bất thường được mô tả ở đây có thể là trạng thái bị mất hoặc có thể là trạng thái không được đăng ký, điều này không bị giới hạn cụ thể ở đây.

Khi xác định trạng thái xác thực hiện tại của bộ nhận dạng định danh theo dữ liệu xác thực, ngay khi xác định được rằng dữ liệu xác thực của bộ nhận dạng định danh gặp phải trạng thái bất thường, cần xác định thêm xem liệu tình trạng xác thực của bộ nhận dạng định danh đã được phục hồi từ trạng thái bất thường hay chưa. Nếu không thì xác định được rằng bộ nhận dạng định danh đang ở trạng thái bất thường; nếu có thì xác định được rằng bộ nhận dạng định danh đang ở trạng thái bình thường.

Ví dụ, khi bộ nhận dạng định danh bị mất hoặc rò rỉ, người dùng gửi yêu cầu thay đổi đến máy chủ tương ứng với nền tảng quản lý định danh, để yêu cầu báo cáo mất bộ nhận dạng định danh hoặc cập nhật bộ nhận dạng định danh; sau đó máy chủ tương ứng với nền tảng quản lý định danh gửi thông tin báo cáo mất hoặc cập nhật đến mạng chuỗi khối thông qua nền tảng quản lý định danh, và tải thông tin báo cáo mất hoặc cập nhật

lên chuỗi khối sau khi việc xác thực đồng thuận là thành công; hoặc,

người dùng trực tiếp gửi yêu cầu không đăng ký đến tổ chức quản lý định danh, và máy chủ tương ứng với nền tảng quản lý định danh tải thông tin không đăng ký lên chuỗi khối thông qua nền tảng quản lý định danh.

Phương pháp xác thực được đề xuất theo các phương án của sáng chế tích hợp công nghệ chuỗi khối, không những tận dụng được các ưu điểm của chuỗi khối, mà còn đạt được các ưu điểm sau đây: Trước tiên, toàn bộ quy trình xác thực không liên quan đến thông tin định danh của người dùng, và quy trình xác thực được hoàn thành bằng cách chỉ sử dụng bộ nhận dạng định danh, do vậy ngăn chặn không cho thông tin định danh bị thu nhận bởi nút chuỗi khối hoặc các thực thể khác với nút chuỗi khối, và nâng cao sự bảo mật của thông tin định danh. Thứ hai, trong các ứng dụng thực tế, người dùng bất kỳ có thể tìm hiểu trạng thái xác thực của bộ nhận dạng định danh của họ bằng cách sử dụng đầu cuối máy khách người dùng hoặc bằng cách trình đơn đến tổ chức dịch vụ liên quan, để xác định liệu bộ nhận dạng định danh có bị sử dụng không đúng bởi kẻ mạo danh hay không, do vậy đạt được mục đích giám sát và thực hiện các biện pháp đối phó càng sớm càng tốt ngay khi phát hiện ra rằng bộ nhận dạng định danh bị sử dụng không đúng bởi kẻ mạo danh.

Thêm vào đó, quy trình xác thực có thể được thực thi bởi nút chuỗi khối hoặc thực thể khác không liên quan đến nút chuỗi khối. Dữ liệu xác thực được lưu trữ trong chuỗi khối có thể được viết hoặc cập nhất chỉ bởi nút chuỗi khối. Do đó, khi người dùng hoặc cơ quan quản lý phát hiện ra rằng bộ nhận dạng định danh bị sử dụng không đúng bởi kẻ mạo danh, việc theo dõi có thể được thực hiện.

Với giải pháp kỹ thuật được đề xuất theo các phương án của sáng chế, sau khi yêu cầu xác thực được gửi từ người dùng được nhận, dữ liệu xác thực liên quan đến bộ nhận dạng định danh của người dùng được thu nhận từ mạng chuỗi khối, và việc xác thực định danh được thực hiện đối với người dùng theo dữ liệu xác thực này. Theo cách này, dựa trên các đặc điểm như việc phi tập trung hóa và chống giả mạo của mạng chuỗi khối, mối quan hệ ánh xạ giữa các bộ nhận dạng định danh của các người dùng khác nhau và dữ liệu xác thực được lưu trữ trước trong nút chuỗi khối của mạng chuỗi khối. Khi cung cấp dịch vụ cho người dùng, nền tảng dịch vụ Internet có thể thực hiện việc xác thực định danh đối với người dùng dựa trên dữ liệu xác thực được lưu trữ trong mạng chuỗi

khối, để tránh vấn đề hiệu quả trong việc xử lý các yêu cầu xác thực thấp do thực tế là có một số lượng lớn các yêu cầu xác thực định danh cần được xử lý bởi nền tảng quản lý định danh, nhờ đó cải thiện hiệu quả xử lý của việc xác thực định danh. Do dữ liệu xác thực có thể được chia sẻ giữa các nền tảng dịch vụ Internet khác nhau thông qua mạng chuỗi khối, người dùng không cần trình thông tin định danh mỗi khi đăng ký với hoặc đăng nhập vào nền tảng dịch vụ mới, và việc sử dụng không đúng thông tin định danh bởi kẻ mạo danh do sự rò rỉ thông tin định danh có thể được ngăn chặn một cách hiệu quả, do vậy cải thiện một cách hiệu quả độ chính xác của việc xác thực định danh.

Fig.4 là lưu đồ sơ lược của phương pháp xác thực theo một phương án của sáng chế. Phương pháp này có thể được mô tả như sau. Phương án này của sáng chế thi hành các bước sau đây trên cơ sở của Fig.3:

Bước 404: tạo ra dữ liệu xác thực theo kết quả xác thực, trong đó dữ liệu xác thực bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và kết quả xác thực, và kết quả xác thực bao gồm việc xác thực là thành công/việc xác thực là thất bại; và

Bước 405: lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối.

Ưu tiên là, trước khi lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối, phương pháp này còn bao gồm các bước:

gửi dữ liệu xác thực đến mạng chuỗi khối, sao cho mạng chuỗi khối thực hiện việc xử lý đồng thuận trên dữ liệu xác thực này; và

nếu kết quả xử lý đồng thuận chỉ ra rằng sự đồng thuận được đạt đến thì lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối.

Fig.5 là lưu đồ sơ lược của phương pháp xác thực theo một phương án của sáng chế. Phương pháp này có thể được mô tả như sau. Phương án này của sáng chế thi hành các bước sau đây trên cơ sở của Fig.3:

Bước 504: thu nhận, theo loại dịch vụ của dịch vụ được yêu cầu bởi người dùng, thông tin đặc điểm định danh của người dùng liên quan đến loại dịch vụ này từ máy chủ quản lý thông tin định danh.

Trong các ứng dụng thực tế, một số thủ tục dịch vụ yêu cầu việc sử dụng thông tin định danh của người dùng. Ví dụ, nền tảng dịch vụ trò chơi có thể thu nhận thông tin định danh người dùng như giới tính và tuổi của người dùng, và nền tảng quản lý cộng

đồng có thể thu nhận thông tin định danh người dùng như địa chỉ, nơi đăng ký thường trú, số điện thoại, và các thành viên gia đình của người dùng.

Trong trường hợp này, máy chủ tương ứng với nền tảng dịch vụ Internet có thể thu nhận thông tin đặc điểm định danh của người dùng liên quan đến loại dịch vụ từ máy chủ quản lý thông tin định danh và xác thực thông tin đặc điểm định danh được thu nhận. Ở đây, thông tin đặc điểm định danh bao gồm giới tính, tuổi, địa chỉ của người dùng, nơi đăng ký thường trú, số điện thoại, các thành viên gia đình, và loại tương tự.

Cụ thể, trước tiên, máy chủ tương ứng với nền tảng dịch vụ Internet gửi yêu cầu thu nhận thông tin định danh người dùng đến máy chủ quản lý thông tin định danh.

Sau khi nhận yêu cầu thu nhận thông tin định danh người dùng, máy chủ quản lý thông tin định danh kiểm tra xem liệu máy chủ tương ứng với nền tảng dịch vụ Internet có được cấp phép thu nhận thông tin định danh của người dùng hay không, ví dụ, kiểm tra xem liệu máy chủ tương ứng với nền tảng dịch vụ Internet và người dùng có ký thỏa thuận xác thực hợp lệ hay không và xem liệu yêu cầu thu nhận thông tin định danh người dùng hiện tại có được ủy quyền bởi người dùng không.

Cần lưu ý rằng có thể có nhiều máy chủ quản lý thông tin định danh ở đây. Ví dụ, thông tin đặc điểm định danh "số điện thoại" và thông tin đặc điểm định danh "tuổi" có thể được lưu trữ trong các máy chủ quản lý thông tin định danh khác nhau.

Sau đó, máy chủ tương ứng với nền tảng dịch vụ Internet nhận thông tin đặc điểm định danh được trả lại từ máy chủ quản lý thông tin định danh.

Bước 505: tạo ra dữ liệu xác thực theo kết quả xác thực và thông tin đặc điểm định danh, trong đó dữ liệu xác thực bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, sự kiện xác thực của việc xác thực thông tin đặc điểm định danh, và kết quả xác thực, và kết quả xác thực bao gồm việc xác thực là thành công/việc xác thực là thất bại.

Cần lưu ý rằng "sự kiện xác thực của việc xác thực thông tin đặc điểm định danh" được nêu ở đây nhằm mục đích mô tả rằng một hoặc nhiều mảnh thông tin đặc điểm định danh (được thu nhận) của người dùng được xác thực. Cần lưu ý rằng dữ liệu xác thực không bao gồm các nội dung cụ thể của thông tin đặc điểm định danh, do vậy đảm bảo được việc bảo mật thông tin đặc điểm định danh và làm giảm nguy cơ rò rỉ.

Bước 506: lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối.

Ưu tiên là, trước khi lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối, phương pháp này còn bao gồm các bước:

gửi dữ liệu xác thực đến mạng chuỗi khối, sao cho mạng chuỗi khối thực hiện việc xử lý đồng thuận trên dữ liệu xác thực này; và

nếu kết quả xử lý đồng thuận chỉ ra rằng sự đồng thuận được đạt đến thì lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối.

Fig.6 là sơ đồ cấu trúc giản lược của hệ thống xác thực định danh theo một phương án của sáng chế.

Như có thể thấy từ Fig.6, hệ thống xác thực định danh được đề xuất theo các phương án của sáng chế bao gồm mạng chuỗi khối, máy chủ tương ứng với nền tảng quản lý định danh, máy chủ tương ứng với nền tảng dịch vụ Internet, và thiết bị người dùng.

Người dùng sử dụng thiết bị người dùng để gửi thông tin định danh đến máy chủ tương ứng với nền tảng quản lý định danh. Máy chủ tương ứng với nền tảng quản lý định danh xác thực định danh của người dùng, và lưu trữ dữ liệu xác thực bao gồm kết quả xác thực vào mạng chuỗi khối.

Khi cung cấp dịch vụ cho người dùng, máy chủ tương ứng với nền tảng dịch vụ Internet có thể thu nhận dữ liệu xác thực từ mạng chuỗi khối, và do vậy thi hành việc xác thực định danh đối với người dùng. Thêm vào đó, kết quả xác thực được tạo ra cũng có thể được lưu trữ vào mạng chuỗi khối, sao cho kết quả xác thực có thể được chia sẻ với các nền tảng dịch vụ Internet khác.

Fig.7 là sơ đồ cấu trúc giản lược của thiết bị xác thực theo một phương án của sáng chế. Như được thể hiện dưới đây, thiết bị xác thực này bao gồm đơn vị nhận 701, đơn vị thu nhận 702, và đơn vị xác thực 703, trong đó:

đơn vị nhận 701 được tạo cấu hình để nhận yêu cầu xác thực được gửi từ người dùng, trong đó yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng;

đơn vị thu nhận 702 được tạo cấu hình để thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối, trong đó nút chuỗi khối của mạng chuỗi khối này lưu trữ mối quan hệ ánh xạ giữa các bộ nhận dạng định danh và dữ liệu xác thực; và

đơn vị xác thực 703 được tạo cấu hình để thực hiện việc xác thực định danh đối

với người dùng theo dữ liệu xác thực.

Theo một phương án khác của sáng chế, thiết bị xác thực này còn bao gồm đơn vị xác minh 704, trong đó:

đơn vị xác minh 704 được tạo cấu hình để, nếu yêu cầu xác thực còn bao gồm khóa công khai và chữ ký số, xác minh xem liệu chữ ký số này có hợp lệ hay không bằng cách sử dụng khóa công khai này, trong đó chữ ký số này được thu bằng cách ký bằng khóa riêng trong cặp khóa công khai và riêng; và

việc đơn vị thu nhận 702 thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối bao gồm việc:

nếu kết quả xác minh chỉ ra rằng chữ ký số là hợp lệ, thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối.

Theo một phương án khác của sáng chế, việc đơn vị thu nhận 702 thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối bao gồm việc:

sàng lọc ra dữ liệu xác thực bao gồm bộ nhận dạng định danh từ mạng chuỗi khối, và xác định dữ liệu xác thực thu được là dữ liệu xác thực liên quan đến bộ nhận dạng định danh.

Theo một phương án khác của sáng chế, đơn vị thu nhận 702 được tạo cấu hình để, nếu nhiều hơn một mảnh dữ liệu xác thực được thu sau khi sàng lọc, xác định dữ liệu xác thực thỏa mãn điều kiện được thiết lập trước trong dữ liệu xác thực thu được, và xác định dữ liệu xác thực được xác định này là dữ liệu xác thực liên quan đến bộ nhận dạng định danh.

Theo một phương án khác của sáng chế, điều kiện được thiết lập trước bao gồm ít nhất một hoặc nhiều thành phần sau đây:

thời gian tạo ra của dữ liệu xác thực thỏa mãn điều kiện về thời gian được thiết lập trước;

bộ nhận dạng tổ chức được chứa trong dữ liệu xác thực thỏa mãn bộ nhận dạng tổ chức của tổ chức phát hành được thiết lập trước; và

loại dịch vụ được chứa trong dữ liệu xác thực là giống với loại dịch vụ của dịch vụ được khởi tạo bởi người dùng.

Theo một phương án khác của sáng chế, việc đơn vị xác thực 703 thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực bao gồm việc:

xác định trạng thái xác thực hiện tại của bộ nhận dạng định danh theo dữ liệu xác thực; và

nếu bộ nhận dạng định danh có trạng thái bất thường và/hoặc trạng thái xác thực lỗi thì xác định rằng việc xác thực định danh đối với người dùng là không thành công; nếu không thì xác định rằng việc xác thực định danh đối với người dùng là thành công.

Theo một phương án khác của sáng chế, thiết bị xác thực còn bao gồm đơn vị lưu trữ 705, trong đó:

đơn vị lưu trữ 705 được tạo cấu hình để tạo ra dữ liệu xác thực theo kết quả xác thực, trong đó dữ liệu xác thực bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và kết quả xác thực, và kết quả xác thực bao gồm việc xác thực là thành công/việc xác thực là thất bại; và

lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối.

Theo một phương án khác của sáng chế, thiết bị xác thực còn bao gồm đơn vị gửi 706, trong đó:

đơn vị gửi 706 được tạo cấu hình để, trước khi dữ liệu xác thực được lưu trữ vào nút chuỗi khối của mạng chuỗi khối, gửi dữ liệu xác thực đến mạng chuỗi khối, sao cho mạng chuỗi khối thực hiện việc xử lý đồng thuận trên dữ liệu xác thực; và

việc đơn vị lưu trữ 705 lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối bao gồm việc:

nếu kết quả xử lý đồng thuận chỉ ra rằng sự đồng thuận được đạt đến thì lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối.

Theo một phương án khác của sáng chế, đơn vị thu nhận 702 được tạo cấu hình để, sau khi xác định được rằng việc xác thực định danh đối với người dùng là thành công, thu nhận, theo loại dịch vụ của dịch vụ được yêu cầu bởi người dùng, thông tin đặc điểm định danh của người dùng liên quan đến loại dịch vụ này từ máy chủ quản lý thông tin định danh; và

đơn vị lưu trữ 705 được tạo cấu hình để tạo ra dữ liệu xác thực theo kết quả xác thực và thông tin đặc điểm định danh, trong đó dữ liệu xác thực bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, sự kiện xác thực của việc xác thực thông tin đặc điểm định danh, và kết quả xác thực, và kết quả xác thực bao gồm việc xác thực là thành công/việc xác thực là thất bại;

và

lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối.

Cần lưu ý rằng thiết bị xác thực được đề xuất theo các phương án của sáng chế có thể được thi hành thông qua phần mềm hoặc phần cứng, điều này không bị giới hạn cụ thể ở đây. Sau khi yêu cầu xác thực được gửi từ người dùng được nhận, thiết bị xác thực thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh của người dùng từ mạng chuỗi khối và thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực này. Theo cách này, dựa trên các đặc điểm như việc phi tập trung hóa và chống giả mạo của mạng chuỗi khối, mối quan hệ ánh xạ giữa các bộ nhận dạng định danh của các người dùng khác nhau và dữ liệu xác thực được lưu trữ trước trong nút chuỗi khối của mạng chuỗi khối. Khi cung cấp dịch vụ cho người dùng, nền tảng dịch vụ Internet có thể thực hiện việc xác thực định danh đối với người dùng dựa trên dữ liệu xác thực được lưu trữ trong mạng chuỗi khối, để tránh vấn đề hiệu quả trong việc xử lý các yêu cầu xác thực thấp do thực tế là có một số lượng lớn các yêu cầu xác thực định danh cần được xử lý bởi nền tảng quản lý định danh, nhờ đó cải thiện hiệu quả xử lý của việc xác thực định danh. Do dữ liệu xác thực có thể được chia sẻ giữa các nền tảng dịch vụ Internet khác nhau thông qua mạng chuỗi khối, người dùng không cần trình thông tin định danh mỗi khi đăng ký với hoặc đăng nhập vào nền tảng dịch vụ mới, và việc sử dụng không đúng thông tin định danh bởi kẻ mạo danh do sự rò rỉ thông tin định danh có thể được ngăn chặn một cách hiệu quả, do vậy cải thiện một cách hiệu quả độ chính xác của việc xác thực định danh.

Dựa trên cùng nguyên lý của sáng chế, các phương án của sáng chế còn đề xuất thiết bị xác thực, bao gồm ít nhất một bộ nhớ và ít nhất một bộ xử lý, trong đó ít nhất một bộ nhớ này lưu trữ chương trình và thiết bị này được tạo cấu hình để thực thi các bước sau đây bằng ít nhất một bộ xử lý này:

nhận yêu cầu xác thực được gửi từ người dùng, trong đó yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này;

thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh này từ mạng chuỗi khối, trong đó nút chuỗi khối của mạng chuỗi khối này lưu trữ mối quan hệ ánh xạ giữa các bộ nhận dạng định danh và dữ liệu xác thực; và

thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực này.

Đối với các cách thi hành cụ thể, có thể tham chiếu đến các nội dung được mô tả trong các phương án nêu trên, và các chi tiết sẽ không được mô tả lặp lại ở đây.

Fig.8 là sơ đồ cấu trúc giản lược của thiết bị xử lý dữ liệu xác thực dựa trên chuỗi khối theo một phương án của sáng chế. Thiết bị xử lý dữ liệu xác thực bao gồm đơn vị nhận 801, đơn vị xử lý 802, và đơn vị lưu trữ 803, trong đó:

đơn vị nhận 801 được tạo cấu hình để nhận thông tin định danh được gửi từ người dùng, và xác thực thông tin định danh này;

đơn vị xử lý 802 được tạo cấu hình để tạo ra dữ liệu xác thực thứ nhất theo kết quả xác thực, trong đó dữ liệu xác thực thứ nhất này bao gồm kết quả xác thực, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng; và

đơn vị lưu trữ 803 được tạo cấu hình để lưu trữ dữ liệu xác thực thứ nhất này vào nút chuỗi khối của mạng chuỗi khối.

Theo một phương án khác của sáng chế, thiết bị xử lý dữ liệu xác thực này còn bao gồm đơn vị thiết lập 804, trong đó:

đơn vị thiết lập 804 được tạo cấu hình để thiết lập mối quan hệ ánh xạ giữa các bộ nhận dạng định danh của các người dùng và thông tin định danh của các người dùng; và lưu trữ thông tin định danh của người dùng vào cơ sở dữ liệu thông tin định danh theo mối quan hệ ánh xạ.

Theo một phương án khác của sáng chế, việc đơn vị nhận 801 xác thực thông tin định danh bao gồm việc:

xác minh xem liệu thông tin định danh có hợp lệ hay không; và

việc đơn vị xử lý 802 tạo ra dữ liệu xác thực thứ nhất theo kết quả xác thực bao gồm việc:

khi kết quả xác minh chỉ ra rằng thông tin định danh là hợp lệ, thu dữ liệu xác thực thứ nhất theo kết quả xác thực, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng.

Theo một phương án khác của sáng chế, thiết bị xử lý dữ liệu xác thực này còn bao gồm đơn vị xác định 805, trong đó:

đơn vị nhận 801 được tạo cấu hình để nhận báo cáo mất hoặc yêu cầu hủy đăng ký được gửi từ người dùng, trong đó báo cáo mất hoặc yêu cầu hủy đăng ký này bao gồm

bộ nhận dạng định danh của người dùng;

đơn vị xác định 805 được tạo cấu hình để xác định được theo báo cáo mất hoặc yêu cầu hủy đăng ký rằng thông tin định danh của người dùng có trạng thái bất thường;

đơn vị xử lý 802 được tạo cấu hình để tạo ra dữ liệu xác thực thứ hai theo thông tin định danh của người dùng đang ở trạng thái bất thường, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng; và

đơn vị lưu trữ 803 được tạo cấu hình để lưu trữ dữ liệu xác thực thứ hai này vào nút chuỗi khối của mạng chuỗi khối.

Cần lưu ý rằng thiết bị xử lý dữ liệu xác thực được đề xuất theo các phương án của sáng chế có thể được thi hành thông qua phần mềm hoặc phần cứng, điều này không bị giới hạn cụ thể ở đây.

Dựa trên cùng nguyên lý của sáng chế, các phương án của sáng chế còn đề xuất thiết bị xử lý dữ liệu xác thực dựa trên chuỗi khối, bao gồm ít nhất một bộ nhớ và ít nhất một bộ xử lý, trong đó ít nhất một bộ nhớ này lưu trữ chương trình và thiết bị này được tạo cấu hình để thực thi các bước sau đây bằng ít nhất một bộ xử lý này:

nhận thông tin định danh được gửi từ người dùng, và xác thực thông tin định danh này;

tạo ra dữ liệu xác thực thứ nhất theo kết quả xác thực, trong đó dữ liệu xác thực thứ nhất này bao gồm kết quả xác thực, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và bộ nhận dạng định danh của người dùng; và

lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối.

Đối với các cách thi hành cụ thể, có thể tham chiếu đến các nội dung được mô tả trong các phương án nêu trên, và các chi tiết sẽ không được mô tả lặp lại ở đây.

Trong những năm 1990, sự cải thiện về công nghệ có thể được phân biệt một cách rõ ràng thành sự cải thiện trên phần cứng (ví dụ, sự cải thiện trên cấu trúc mạch chẳng hạn như điôt, tranzito, và bộ chuyển mạch) hoặc sự cải thiện trên phần mềm (sự cải thiện trên thủ tục phương pháp). Tuy nhiên, với sự phát triển của các công nghệ, những sự cải thiện về nhiều thủ tục phương pháp hiện nay có thể được xem là các cải thiện trực tiếp về các cấu trúc mạch phần cứng. Hầu hết tất cả các nhà thiết kế lập trình các thủ tục phương pháp được cải thiện vào trong các mạch phần cứng để thu được các cấu trúc mạch phần cứng tương ứng. Do đó, sẽ là không phù hợp nếu giả định rằng sự cải tiến về

thủ tục của phương pháp không thể được thi hành nhờ sử dụng môđun thực thể phần cứng. Ví dụ, thiết bị logic lập trình được (Programmable Logic Device, PLD) (ví dụ, mảng cổng lập trình được dạng trường (Field Programmable Gate Array, FPGA)) là mạch tích hợp như vậy mà các chức năng logic của nó được xác định bởi các thiết bị được lập trình bởi người dùng. Các nhà thiết kế tự lập trình để "tích hợp" hệ thống kỹ thuật số vào một phần của PLD, mà không cần yêu cầu nhà sản xuất chip thiết kế và sản xuất chip mạch tích hợp dành riêng. Hơn nữa, hiện tại, việc lập trình chủ yếu được thi hành bằng cách sử dụng phần mềm trình biên dịch logic, thay vì sản xuất thủ công một chip mạch tích hợp. Phần mềm trình biên dịch lôgic là tương tự như trình biên dịch phần mềm được sử dụng để phát triển và viết chương trình, và các mã gốc trước khi biên dịch cũng cần được viết nhờ sử dụng ngôn ngữ lập trình cụ thể, được gọi là ngôn ngữ mô tả phần cứng (Hardware Description Language, HDL). Có nhiều loại HDL, chẳng hạn như ngôn ngữ biểu thức luận lý cải tiến (Advanced Boolean Expression Language, ABEL), ngôn ngữ mô tả phần cứng của Altera (Altera Hardware Description Language, AHDL), Hợp lưu (Confluence), ngôn ngữ lập trình của đại học Cornell (Cornell University Programming Language, CUPL), HDCal, ngôn ngữ mô tả phần cứng Java (Java Hardware Description Language, JHDL), Lava, Lola, MyHDL, PALASM, và ngôn ngữ mô tả phần cứng Ruby (Ruby Hardware Description Language, RHDL), trong số đó, ngôn ngữ mô tả phần cứng mạch tích hợp tốc độ rất cao (Very-High-Speed Integrated Circuit Hardware Description Language, VHDL) và Verilog hiện đang được sử dụng phổ biến nhất. Những người có hiểu biết trung bình trong lĩnh vực kỹ thuật cũng nên biết rằng mạch phần cứng để thi hành thủ tục phương pháp logic có thể dễ dàng được thu bằng cách lập trình logic một cách hợp lý thủ tục phương pháp sử dụng một số ngôn ngữ mô tả phần cứng trên đây và lập trình thủ tục phương pháp này vào trong mạch tích hợp.

Bộ điều khiển có thể được thi hành theo cách thích hợp bất kỳ. Ví dụ, bộ điều khiển này có thể ở dạng của, ví dụ, bộ vi xử lý hoặc bộ xử lý và phương tiện có thể đọc bằng máy tính lưu trữ mã chương trình có thể đọc bằng máy tính (ví dụ, phần mềm hoặc phần sụn) có thể thực thi được bởi bộ (vi) xử lý, cổng logic, bộ chuyển mạch, mạch tích hợp chuyên dụng (Application Specific Integrated Circuit, ASIC), bộ điều khiển logic lập trình được, và bộ vi điều khiển được nhúng. Các ví dụ về bộ điều khiển bao gồm, nhưng

không bị giới hạn ở, các bộ vi điều khiển dưới đây: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20, và Silicone Labs C8051F320. Bộ điều khiển bộ nhớ có thể được thi hành thêm như là một phần của logic điều khiển của bộ nhớ. Những người có hiểu biết trung bình trong lĩnh vực kỹ thuật cũng biết rằng, bộ điều khiển có thể được thi hành bằng cách sử dụng các mã chương trình đọc được bằng máy tính thuần túy, và thêm vào đó, các bước của phương pháp có thể được lập trình logic để cho phép bộ điều khiển thi hành chức năng tương tự dưới dạng cổng logic, bộ chuyển mạch, mạch tích hợp chuyên dụng, bộ điều khiển logic lập trình được và bộ vi điều khiển được nhúng. Do đó, loại bộ điều khiển này có thể được coi là một thành phần phần cứng, và các máy được chứa trong đó để thi hành các chức năng khác nhau cũng có thể được coi là các cấu trúc bên trong thành phần phần cứng này. Hoặc, các máy được sử dụng để thi hành các chức năng khác nhau này thậm chí có thể được coi là cả các môđun phần mềm để thi hành phương pháp này và các cấu trúc bên trong thành phần phần cứng này.

Hệ thống, máy, môđun hoặc đơn vị được minh họa trong các phương án trên đây có thể được thi hành cụ thể bằng cách sử dụng chip máy tính hoặc một thực thể, hoặc một sản phẩm có chức năng cụ thể. Thiết bị thi hành điển hình là máy tính. Cụ thể, máy tính này có thể là, ví dụ, máy tính cá nhân, máy tính xách tay, điện thoại tế bào, điện thoại camera, điện thoại thông minh, thiết bị trợ giúp số cá nhân, thiết bị trình diễn phương tiện, thiết bị định vị, thiết bị thư điện tử, bảng điều khiển trò chơi, máy tính bảng, thiết bị đeo được, hoặc sự kết hợp của bất kỳ thiết bị nào trong các thiết bị này.

Để dễ mô tả, khi máy này được mô tả, nó được chia thành các đơn vị khác nhau xét về các chức năng cho các phần mô tả tương ứng. Tất nhiên, khi sáng chế được thi hành, các chức năng của các đơn vị này có thể được thi hành trong cùng một phần hoặc trong nhiều phần của phần mềm và/hoặc phần cứng.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ hiểu rằng các phương án của sáng chế có thể được thể hiện dưới dạng phương pháp, hệ thống, hoặc sản phẩm chương trình máy tính. Theo đó, sáng chế có thể sử dụng hình thức của phương án phần cứng hoàn toàn, phương án phần mềm hoàn toàn hoặc phương án kết hợp các khía cạnh phần cứng và phần mềm. Hơn nữa, sáng chế có sử dụng hình thức của sản phẩm chương trình máy tính được thi hành trên một hoặc nhiều phương tiện lưu trữ sử dụng được bằng máy tính (bao gồm, nhưng không giới hạn ở, các bộ nhớ đĩa từ, CD-ROM, bộ nhớ quang,

v.v.) bao gồm các mã chương trình sử dụng được bằng máy tính.

Sáng chế được mô tả với tham chiếu đến các lưu đồ và/hoặc các sơ đồ khối của phương pháp, thiết bị (hệ thống) và sản phẩm chương trình máy tính trong các phương án của sáng chế. Cần hiểu rằng các lệnh chương trình máy tính có thể thi hành mỗi quy trình và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối này và sự kết hợp của các quy trình và/hoặc các khối trong các lưu đồ và/hoặc các sơ đồ khối này. Các lệnh chương trình máy tính này có thể được cung cấp cho máy tính đa năng, máy tính chuyên dụng, bộ xử lý được nhúng hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác để tạo ra bộ máy, sao cho máy được tạo cấu hình để thi hành các chức năng được chỉ rõ trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc một hoặc nhiều khối trong các sơ đồ khối được tạo ra bằng cách sử dụng các lệnh được thực thi bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác.

Các lệnh chương trình máy tính này cũng có thể được lưu trữ trong bộ nhớ đọc được bằng máy tính mà nó có thể hướng dẫn máy tính hoặc các thiết bị xử lý dữ liệu lập trình được khác hoạt động theo cách được chỉ rõ, sao cho các lệnh được lưu trữ trong bộ nhớ đọc được bằng máy tính này tạo ra một sản phẩm bao gồm thiết bị ra lệnh, trong đó thiết bị ra lệnh này thi hành các chức năng được chỉ rõ trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này cũng có thể được tải vào máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, sao cho một loạt các bước hoạt động được thực hiện trên máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác này để tạo ra quá trình xử lý được thi hành bởi máy tính, và các lệnh được thực thi trên máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác này cung cấp các bước để thi hành các chức năng được chỉ rõ trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Trong cấu hình đặc trưng, thiết bị tính toán bao gồm một hoặc nhiều đơn vị xử lý trung tâm (central processing unit, CPU), các giao diện vào/ra, các giao diện mạng, và các bộ nhớ.

Bộ nhớ này có thể bao gồm các dạng phương tiện đọc được bằng máy tính sau đây: bộ nhớ khả biến, bộ nhớ truy cập ngẫu nhiên (Random Access Memory, RAM), và/hoặc bộ nhớ phi khả biến, ví dụ, bộ nhớ chỉ đọc (Read-Only Memory, ROM) hoặc bộ nhớ

RAM tác động nhanh (flash RAM). Bộ nhớ này là một ví dụ về phương tiện đọc được bằng máy tính.

Phương tiện đọc được bằng máy tính này bao gồm phương tiện khả biến và phi khả biến, di động và không di động, và có thể sử dụng phương pháp hoặc công nghệ bất kỳ để lưu trữ thông tin. Thông tin này có thể là lệnh đọc được bằng máy tính, cấu trúc dữ liệu, môđun của chương trình hoặc dữ liệu khác. Các ví dụ về phương tiện lưu trữ của máy tính bao gồm, nhưng không giới hạn với, bộ nhớ thay đổi pha (phase change memory, PRAM), bộ nhớ truy cập ngẫu nhiên tĩnh (static random access memory, SRAM), bộ nhớ truy cập ngẫu nhiên động (dynamic random access memory, DRAM), các loại RAM khác, ROM, bộ nhớ chỉ đọc lập trình được xóa được bằng điện (electrically erasable programmable read-only memory, EEPROM), bộ nhớ tác động nhanh (flash) hoặc các công nghệ nhớ khác, bộ nhớ chỉ-đọc dạng đĩa compact (CD-ROM), đĩa đa năng kỹ thuật số (digital versatile disc, DVD) hoặc các bộ nhớ quang khác, băng cát xét, bộ lưu trữ địa băng hoặc các thiết bị lưu trữ từ tính khác, hoặc phương tiện không truyền dẫn khác bất kỳ, mà chúng có thể được sử dụng để lưu trữ thông tin có thể truy cập bằng máy tính. Theo định nghĩa ở đây, phương tiện đọc được bằng máy tính không bao gồm phương tiện chuyển tiếp đọc được bằng máy tính (phương tiện chuyển tiếp), ví dụ, tín hiệu dữ liệu được điều biến và sóng mang.

Cần lưu ý thêm rằng các thuật ngữ "bao gồm", "gồm" hoặc bất kỳ biến thể nào khác được dự tính sẽ bao hàm sự bao gồm không loại trừ, do đó quy trình, phương pháp, sản phẩm hoặc thiết bị bao gồm một loạt các phần tử không chỉ bao gồm các phần tử này, mà còn bao gồm các phần tử khác không được liệt kê rõ ràng, hoặc còn bao gồm cả các phần tử cố hữu của quy trình, phương pháp, sản phẩm hoặc thiết bị này. Khi không có thêm các giới hạn, một phần tử được định ra bởi "bao gồm một ..." không loại trừ việc quy trình, phương pháp, sản phẩm hoặc thiết bị bao gồm phần tử đó còn có các phần tử giống hệt khác.

Sáng chế có thể được mô tả trong ngữ cảnh chung của lệnh có thể thực thi được bằng máy tính được thực thi bởi máy tính, ví dụ, một môđun chương trình. Nhìn chung, môđun chương trình này bao gồm một đoạn chương trình, một chương trình, một đối tượng, một tổ hợp, một cấu trúc dữ liệu, và loại tương tự được sử dụng để thực thi một tác vụ cụ thể hoặc thi hành một loại dữ liệu trừu tượng cụ thể. Sáng chế cũng có thể

được thi hành trong các môi trường điện toán phân tán, và trong các môi trường điện toán phân tán này, một tác vụ được thực thi bằng cách sử dụng các thiết bị xử lý từ xa được kết nối qua mạng truyền thông. Trong môi trường máy tính phân tán này, môđun chương trình có thể được đặt trong phương tiện lưu trữ máy tính cục bộ và từ xa bao gồm thiết bị lưu trữ.

Các phương án trong bản mô tả này được mô tả tăng dần, các phần giống hoặc tương tự của các phương án có thể được thu khi tham chiếu lẫn nhau, và mỗi phương án nhấn mạnh một phần khác với các phương án khác. Đặc biệt, phương án về hệ thống về cơ bản là tương tự với phương án về phương pháp, do vậy nó được mô tả một cách đơn giản, và đối với các phần liên quan, có thể tham chiếu đến các phần mô tả của các phần này trong phương án về phương pháp.

Phần mô tả trên đây chỉ đơn thuần là các phương án của sáng chế và không nhằm mục đích giới hạn sáng chế. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng có thể thực hiện các cải biến và biến thể khác nhau đối với sáng chế. Mọi sự cải biến, thay thế và cải tiến tương đương được thực hiện nằm trong mục đích và nguyên lý của sáng chế sẽ nằm trong phạm vi yêu cầu bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp xác thực bao gồm các bước:

nhận yêu cầu xác thực từ người dùng, yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này;

thu nhận dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh này từ mạng chuỗi khối (blockchain), nút chuỗi khối của mạng chuỗi khối này đang lưu trữ các bộ nhận dạng định danh, dữ liệu xác thực tương ứng của các bộ nhận dạng định danh này, và mối quan hệ ánh xạ giữa các bộ nhận dạng định danh này và dữ liệu xác thực tương ứng này, dữ liệu xác thực tương ứng này được lưu trữ trên nút chuỗi khối này bao gồm ít nhất một kết quả xác thực chỉ ra việc xác thực thất bại, và dữ liệu xác thực thứ nhất bao gồm kết quả xác thực chỉ ra việc xác thực thành công hoặc thất bại; và

thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực thứ nhất được thu nhận từ mạng chuỗi khối và lưu trữ dữ liệu xác thực mới trên nút chuỗi khối, trong đó bước thực hiện việc xác thực định danh bao gồm các bước:

xác định trạng thái xác thực của bộ nhận dạng định danh dựa trên dữ liệu xác thực thứ nhất được thu nhận từ mạng chuỗi khối;

đáp lại việc bộ nhận dạng định danh đang ở trạng thái bất thường hoặc trạng thái xác thực thất bại, xác định rằng việc xác thực định danh đối với người dùng là không thành công; và

đáp lại việc bộ nhận dạng định danh đang không ở trạng thái bất thường hoặc trạng thái xác thực thất bại, xác định rằng việc xác thực định danh đối với người dùng là thành công.

2. Phương pháp xác thực theo điểm 1, còn bao gồm bước:

đáp lại yêu cầu xác thực bao gồm khóa công khai và chữ ký số, xác minh xem liệu chữ ký số này có hợp lệ hay không sử dụng khóa công khai này; và

bước thu nhận dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối bao gồm bước:

đáp lại kết quả xác minh chỉ ra rằng chữ ký số là hợp lệ, thu nhận dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối này.

3. Phương pháp xác thực theo điểm 1, trong đó bước thu nhận dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối bao gồm bước:

thu dữ liệu xác thực bao gồm bộ nhận dạng định danh này từ mạng chuỗi khối; và

xác định dữ liệu xác thực thu được là dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh này.

4. Phương pháp xác thực theo điểm 3, còn bao gồm bước:

đáp lại dữ liệu xác thực thu được bao gồm nhiều mảnh dữ liệu xác thực, lựa chọn, từ dữ liệu xác thực thu được này, mảnh dữ liệu xác thực thỏa mãn điều kiện được thiết lập trước; và

xác định mảnh dữ liệu xác thực được lựa chọn này là dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh.

5. Phương pháp xác thực theo điểm 4, trong đó điều kiện được thiết lập trước bao gồm ít nhất một thành phần trong số:

thời gian tạo ra liên quan đến mảnh dữ liệu xác thực được lựa chọn thỏa mãn điều kiện về thời gian được thiết lập trước;

bộ nhận dạng tổ chức liên quan đến mảnh dữ liệu xác thực được lựa chọn thỏa mãn bộ nhận dạng tổ chức của tổ chức phát hành được thiết lập trước; hoặc

loại dịch vụ liên quan đến mảnh dữ liệu xác thực được lựa chọn khớp với loại dịch vụ của dịch vụ được khởi tạo bởi người dùng.

6. Phương pháp xác thực theo điểm 1, còn bao gồm bước:

tạo ra dữ liệu xác thực thứ nhất theo kết quả xác thực, dữ liệu xác thực thứ nhất bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và kết quả xác thực; và

lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối.

7. Phương pháp xác thực theo điểm 6, trong đó bước lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối bao gồm bước:

gửi dữ liệu xác thực thứ nhất đến mạng chuỗi khối cho việc xử lý đồng thuận; và

đáp lại việc sự đồng thuận được đạt đến, lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối.

8. Phương pháp xác thực theo điểm 1, trong đó sau bước xác định rằng việc xác thực định danh đối với người dùng là thành công, phương pháp này còn bao gồm các bước:

thu nhận, theo loại dịch vụ của dịch vụ được yêu cầu bởi người dùng, thông tin đặc điểm định danh của người dùng liên quan đến loại dịch vụ này từ máy chủ quản lý thông tin định danh;

tạo ra dữ liệu xác thực thứ hai theo kết quả xác thực và thông tin đặc điểm định danh, dữ liệu xác thực thứ hai này bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, sự kiện xác thực của việc xác thực thông tin đặc điểm định danh, và kết quả xác thực; và

lưu trữ dữ liệu xác thực thứ hai vào nút chuỗi khối của mạng chuỗi khối.

9. Thiết bị xác thực, bao gồm:

bộ nhớ lưu trữ các lệnh; và

ít nhất một bộ xử lý được tạo cấu hình để thực thi các lệnh này để:

nhận yêu cầu xác thực từ người dùng, yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này;

thu nhận dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh này từ mạng chuỗi khối, nút chuỗi khối của mạng chuỗi khối này đang lưu trữ các bộ nhận dạng định danh, dữ liệu xác thực tương ứng của các bộ nhận dạng định danh này, và mối quan hệ ánh xạ giữa các bộ nhận dạng định danh này và dữ liệu xác thực tương ứng này, dữ liệu xác thực tương ứng này được lưu trữ trên nút chuỗi khối này bao gồm ít nhất một kết quả xác thực chỉ ra việc xác thực thất bại, và dữ liệu xác thực thứ nhất bao gồm kết quả xác thực chỉ ra việc xác thực thành công hoặc thất bại; và

thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực thứ nhất được thu nhận từ mạng chuỗi khối và lưu trữ dữ liệu xác thực mới trên nút chuỗi khối, trong đó việc thực hiện việc xác thực định danh bao gồm việc:

xác định trạng thái xác thực của bộ nhận dạng định danh dựa trên dữ liệu xác thực thứ nhất được thu nhận từ mạng chuỗi khối;

đáp lại việc bộ nhận dạng định danh đang ở trạng thái bất thường hoặc trạng thái xác thực thất bại, xác định rằng việc xác thực định danh đối với người dùng là không thành công; và

đáp lại việc bộ nhận dạng định danh đang không ở trạng thái bất thường hoặc trạng thái xác thực thất bại, xác định rằng việc xác thực định danh đối với người dùng là thành công.

10. Thiết bị xác thực theo điểm 9, trong đó ít nhất một bộ xử lý đã nêu còn được tạo cấu hình để thực thi các lệnh đã nêu để:

nếu yêu cầu xác thực bao gồm khóa công khai và chữ ký số, xác minh xem liệu chữ ký số này có hợp lệ hay không sử dụng khóa công khai này; và

trong đó việc thu nhận dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối bao gồm việc:

nếu kết quả xác minh chỉ ra rằng chữ ký số là hợp lệ, thu nhận dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối này.

11. Thiết bị xác thực theo điểm 9, trong đó trong việc thu nhận dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh từ mạng chuỗi khối, ít nhất một bộ xử lý đã nêu còn được tạo cấu hình để thực thi các lệnh đã nêu để:

thu dữ liệu xác thực bao gồm bộ nhận dạng định danh này từ mạng chuỗi khối; và

xác định dữ liệu xác thực thu được là dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh này.

12. Thiết bị xác thực theo điểm 11, trong đó ít nhất một bộ xử lý đã nêu còn được tạo cấu hình để thực thi các lệnh đã nêu để:

đáp lại dữ liệu xác thực thu được bao gồm nhiều mảnh dữ liệu xác thực, lựa chọn, từ dữ liệu xác thực thu được này, mảnh dữ liệu xác thực thỏa mãn điều kiện được thiết lập trước; và

xác định mảnh dữ liệu xác thực được lựa chọn này là dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh.

13. Thiết bị xác thực theo điểm 12, trong đó điều kiện được thiết lập trước bao gồm ít nhất một thành phần trong số:

thời gian tạo ra liên quan đến mảnh dữ liệu xác thực được lựa chọn thỏa mãn điều kiện về thời gian được thiết lập trước;

bộ nhận dạng tổ chức liên quan đến mảnh dữ liệu xác thực được lựa chọn thỏa mãn bộ nhận dạng tổ chức của tổ chức phát hành được thiết lập trước; hoặc

loại dịch vụ liên quan đến mảnh dữ liệu xác thực được lựa chọn khớp với loại dịch vụ của dịch vụ được khởi tạo bởi người dùng.

14. Thiết bị xác thực theo điểm 9, trong đó ít nhất một bộ xử lý đã nêu còn được tạo cấu hình để thực thi các lệnh đã nêu để:

tạo ra dữ liệu xác thực thứ nhất theo kết quả xác thực, dữ liệu xác thực thứ nhất bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và kết quả xác thực; và

lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối.

15. Thiết bị xác thực theo điểm 14, trong đó trong việc lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối, ít nhất một bộ xử lý đã nêu còn được tạo cấu hình để thực thi các lệnh đã nêu để:

gửi dữ liệu xác thực thứ nhất đến mạng chuỗi khối cho việc xử lý đồng thuận; và

đáp lại việc sự đồng thuận được đạt đến, lưu trữ dữ liệu xác thực thứ nhất vào nút chuỗi khối của mạng chuỗi khối.

16. Thiết bị xác thực theo điểm 9, trong đó sau khi xác định rằng việc xác thực định danh đối với người dùng là thành công, ít nhất một bộ xử lý đã nêu còn được tạo cấu hình để thực thi các lệnh đã nêu để:

thu nhận, theo loại dịch vụ của dịch vụ được yêu cầu bởi người dùng, thông tin đặc điểm định danh của người dùng liên quan đến loại dịch vụ này từ máy chủ quản lý thông tin định danh;

tạo ra dữ liệu xác thực thứ hai theo kết quả xác thực và thông tin đặc điểm định danh, dữ liệu xác thực thư hai này bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, sự kiện xác thực của việc xác thực thông tin đặc điểm định danh, và kết quả xác thực; và

lưu trữ dữ liệu xác thực thứ hai vào nút chuỗi khối của mạng chuỗi khối.

17. Phương tiện phi chuyển tiếp đọc được bằng máy tính lưu trữ tập lệnh mà, khi được thực thi bởi bộ xử lý của thiết bị, khiến cho thiết bị này thực hiện phương pháp xác thực, phương pháp này bao gồm các bước:

nhận yêu cầu xác thực từ người dùng, yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này;

thu nhận dữ liệu xác thực thứ nhất liên quan đến bộ nhận dạng định danh này từ mạng chuỗi khối (blockchain), nút chuỗi khối của mạng chuỗi khối này đang lưu trữ các bộ nhận dạng định danh, dữ liệu xác thực tương ứng của các bộ nhận dạng định danh này, và mối quan hệ ánh xạ giữa các bộ nhận dạng định danh này và dữ liệu xác thực tương ứng này, dữ liệu xác thực tương ứng này được lưu trữ trên nút chuỗi khối này bao gồm ít nhất một kết quả xác thực chỉ ra việc xác thực thất bại, và dữ liệu xác thực thứ nhất bao gồm kết quả xác thực chỉ ra việc xác thực thành công hoặc thất bại; và

thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực thứ nhất được thu nhận từ mạng chuỗi khối và lưu trữ dữ liệu xác thực mới trên nút chuỗi khối, trong đó bước thực hiện việc xác thực định danh bao gồm các bước:

xác định trạng thái xác thực của bộ nhận dạng định danh dựa trên dữ liệu xác thực thứ nhất được thu nhận từ mạng chuỗi khối;

đáp lại việc bộ nhận dạng định danh đang ở trạng thái bất thường hoặc trạng thái xác thực thất bại, xác định rằng việc xác thực định danh đối với người dùng là không thành công; và

đáp lại việc bộ nhận dạng định danh đang không ở trạng thái bất thường hoặc trạng thái xác thực thất bại, xác định rằng việc xác thực định danh đối với người dùng là thành công.

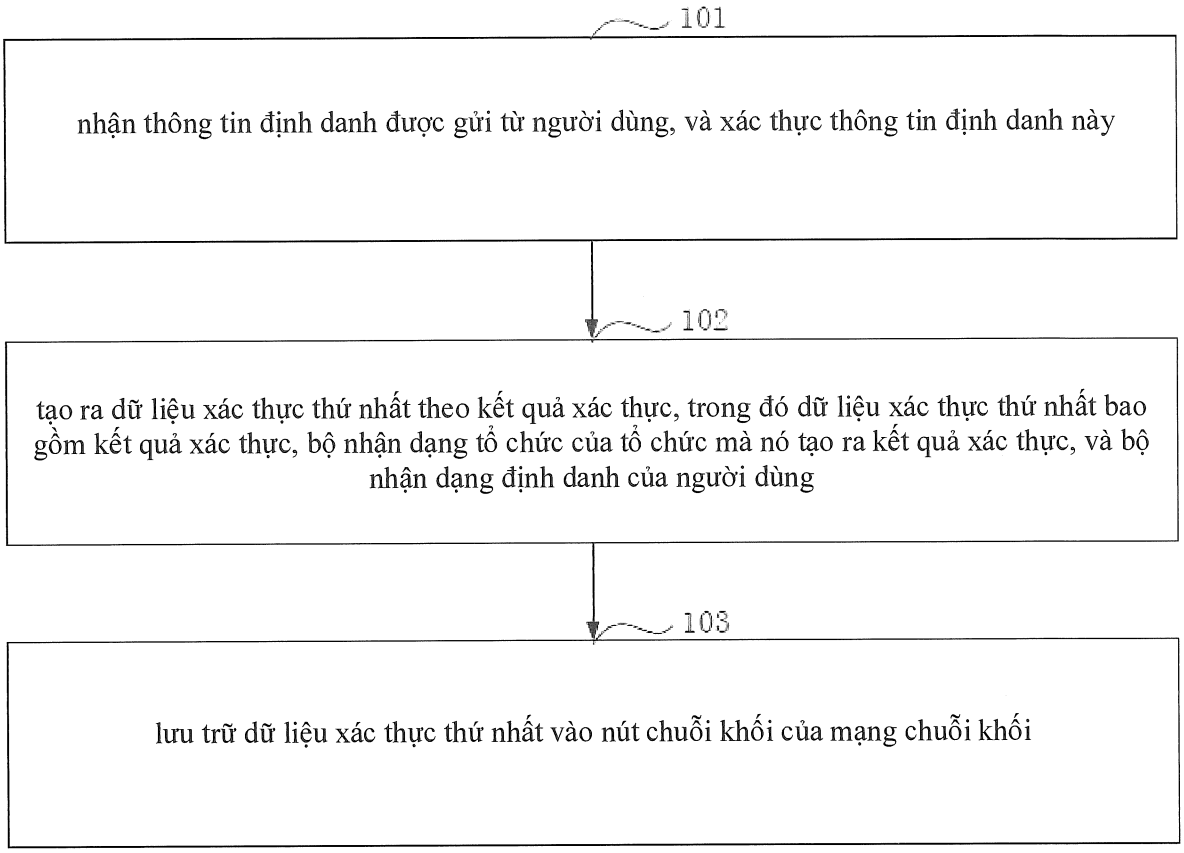


FIG. 1

cấu trúc của dữ liệu xác thực	
chữ ký số của tổ chức	chữ ký số của người dùng
khóa công khai của tổ chức	khóa công khai của người dùng
kết quả xác thực	

FIG. 2

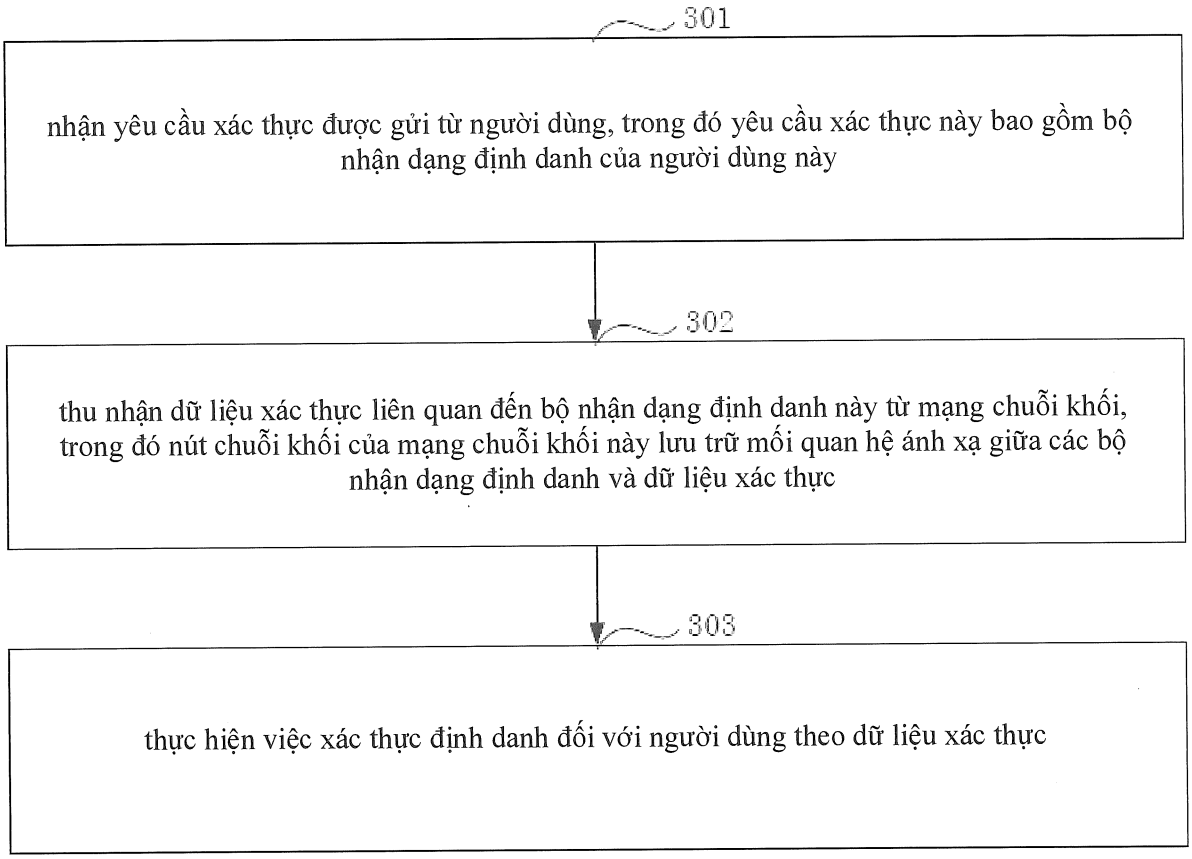

301
nhận yêu cầu xác thực được gửi từ người dùng, trong đó yêu cầu xác thực này bao gồm bộ nhận dạng định danh của người dùng này
302
thu nhận dữ liệu xác thực liên quan đến bộ nhận dạng định danh này từ mạng chuỗi khối, trong đó nút chuỗi khối của mạng chuỗi khối này lưu trữ mối quan hệ ánh xạ giữa các bộ nhận dạng định danh và dữ liệu xác thực
303
thực hiện việc xác thực định danh đối với người dùng theo dữ liệu xác thực

FIG. 3

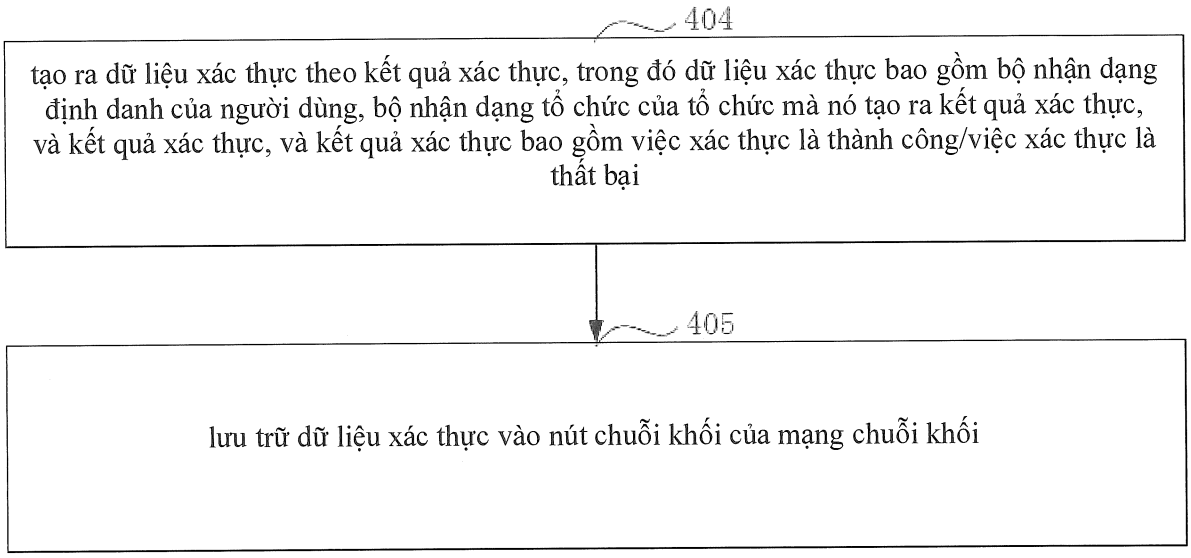

404
tạo ra dữ liệu xác thực theo kết quả xác thực, trong đó dữ liệu xác thực bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, và kết quả xác thực, và kết quả xác thực bao gồm việc xác thực là thành công/việc xác thực là thất bại
405
lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối

FIG. 4

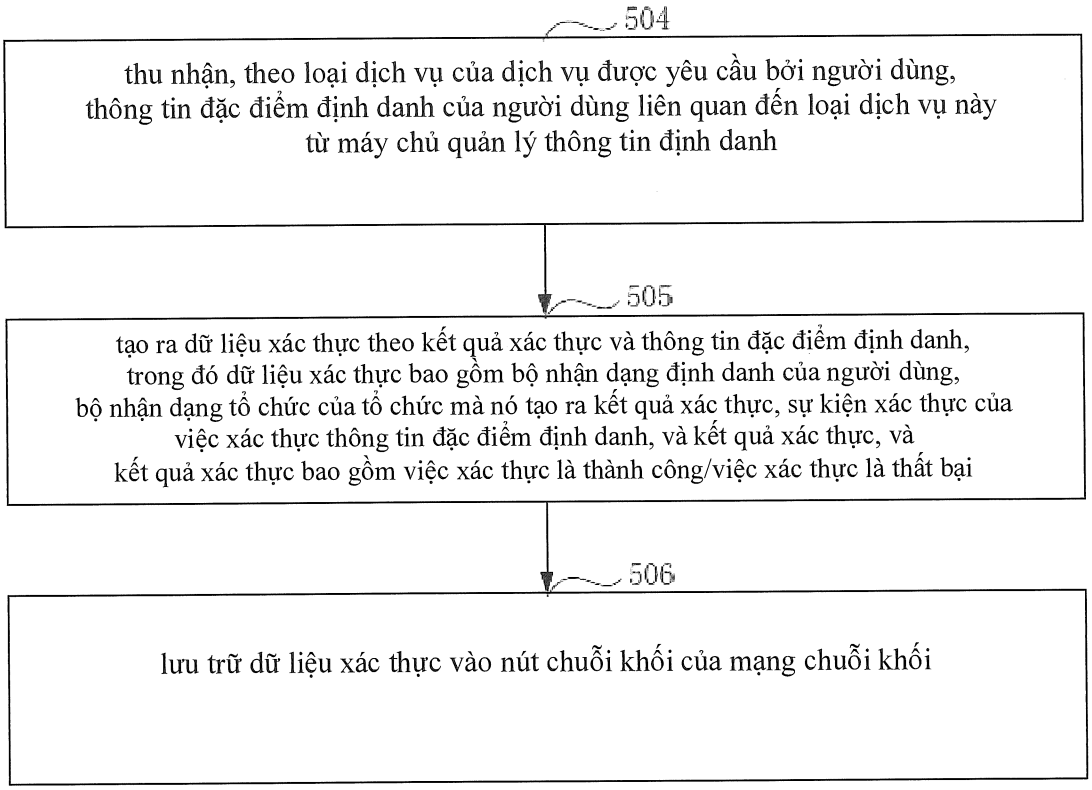

504
thu nhận, theo loại dịch vụ của dịch vụ được yêu cầu bởi người dùng, thông tin đặc điểm định danh của người dùng liên quan đến loại dịch vụ này từ máy chủ quản lý thông tin định danh
505
tạo ra dữ liệu xác thực theo kết quả xác thực và thông tin đặc điểm định danh, trong đó dữ liệu xác thực bao gồm bộ nhận dạng định danh của người dùng, bộ nhận dạng tổ chức của tổ chức mà nó tạo ra kết quả xác thực, sự kiện xác thực của việc xác thực thông tin đặc điểm định danh, và kết quả xác thực, và kết quả xác thực bao gồm việc xác thực là thành công/việc xác thực là thất bại
506
lưu trữ dữ liệu xác thực vào nút chuỗi khối của mạng chuỗi khối

FIG. 5

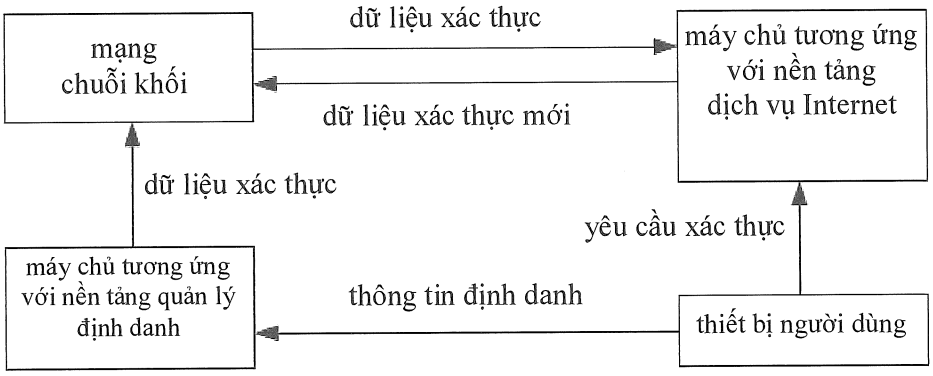

mạng
chuỗi khối
dữ liệu xác thực
dữ liệu xác thực mới
máy chủ tương ứng
với nền tảng
dịch vụ Internet
dữ liệu xác thực
yêu cầu xác thực
máy chủ tương ứng
với nền tảng quản lý
định danh
thông tin định danh
thiết bị người dùng

FIG. 6

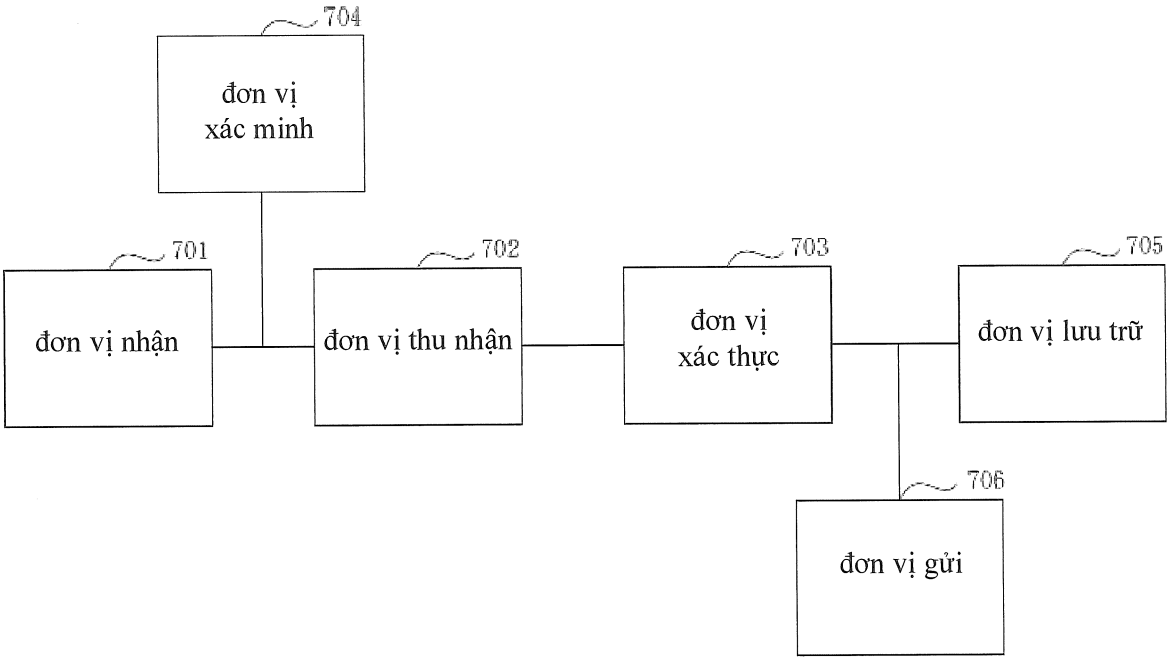

704
đơn vị
xác minh
701
đơn vị nhận
702
đơn vị thu nhận
703
đơn vị
xác thực
705
đơn vị lưu trữ
706
đơn vị gửi

FIG. 7

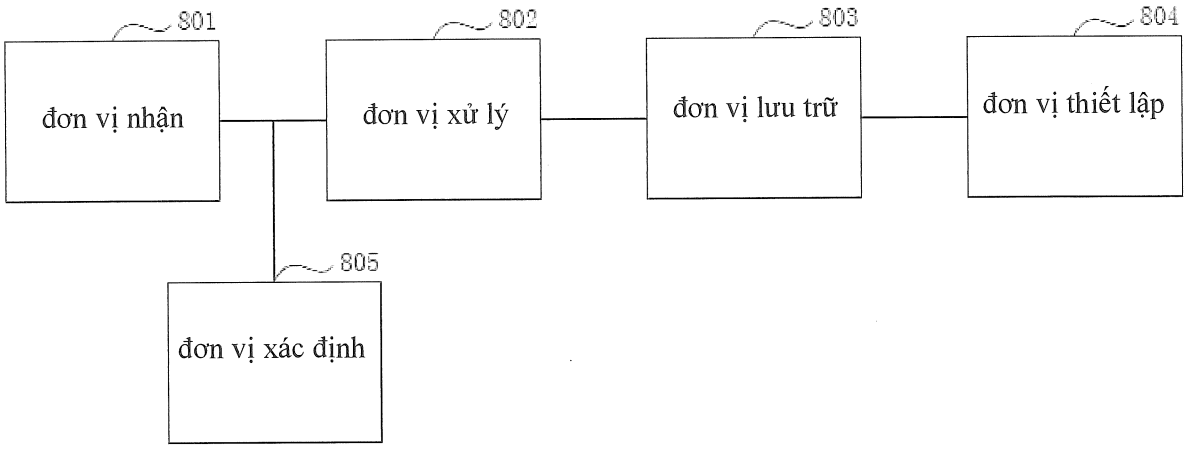

801
đơn vị nhận
802
đơn vị xử lý
803
đơn vị lưu trữ
804
đơn vị thiết lập
805
đơn vị xác định

FIG. 8