(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) **1-0033608**

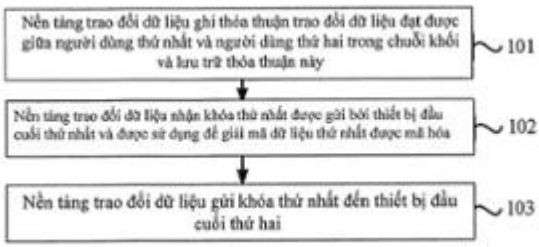
(51)[7] **G06F 21/64**; H04W 12/04; H04L 9/32; H04L 29/06; H04L 9/08

(13) **B**

(21) 1-2019-03872
(22) 23/02/2018
(86) PCT/US2018/019464 23/02/2018
(87) WO 2018/156924 30/08/2018
(30) 201710102824.3 24/02/2017 CN
(45) 25/10/2022 415
(43) 25/12/2019 381A
(73) Advanced New Technologies Co., Ltd. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) LI, Yi (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ GỬI DỮ LIỆU

(57) Sáng chế đề cập đến phương pháp gửi dữ liệu để giải quyết vấn đề an ninh dữ liệu thấp trong quy trình trao đổi dữ liệu hiện có. Phương pháp này bao gồm các bước: ghi, bởi nền tảng giao dịch dữ liệu, thỏa thuận giao dịch dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối và lưu trữ thỏa thuận này; nhận, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa, thiết bị đầu cuối thứ nhất là thiết bị đầu cuối tương ứng với người dùng thứ nhất; gửi, bởi thiết bị đầu cuối thứ nhất, dữ liệu thứ nhất được mã hóa đến thiết bị đầu cuối thứ hai, thiết bị đầu cuối thứ hai là thiết bị đầu cuối tương ứng với người dùng thứ hai; gửi, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất đến thiết bị đầu cuối thứ hai; và giải mã, bởi thiết bị đầu cuối thứ hai, dữ liệu thứ nhất được mã hóa nhận được dựa trên khóa thứ nhất để thu dữ liệu thứ nhất. Sáng chế còn đề cập đến thiết bị gửi dữ liệu.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ máy tính, và cụ thể là phương pháp và thiết bị gửi dữ liệu.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển của công nghệ thông tin, công nghệ thông tin mang lại lợi ích to lớn cho công việc và cuộc sống của mọi người. Trong lĩnh vực công nghệ thông tin, thông tin được lưu trữ và được truyền bằng cách sử dụng dữ liệu dưới dạng sóng mang, và dữ liệu có thể được lưu trữ là số nhị phân trong vật ghi lưu trữ của thiết bị điện toán. Dữ liệu được đề cập ở đây có thể là văn bản, ký hiệu, viđeo hoặc auđio, và tất cả các phần tử khác có thể được nhận dạng bởi thiết bị điện toán.

Dữ liệu, dưới dạng sóng mang của thông tin, luôn có giá trị nhất định. Đặc biệt trong thời đại dữ liệu lớn, mỗi đơn vị tiến tới tích lũy lượng lớn dữ liệu trong việc vận hành hoặc xử lý dịch vụ, và dữ liệu có thể có giá trị sử dụng nhất định để tiến hành một số công việc. Để tận dụng hết giá trị của dữ liệu, chính hai bên giữ dữ liệu có thể trao đổi dữ liệu với nhau để lấy dữ liệu được yêu cầu.

Để tạo thuận lợi cho cả hai bên trao đổi dữ liệu để tìm kiếm đối tượng trao đổi dữ liệu thích hợp, nền tảng trao đổi dữ liệu được đưa vào đó. Nền tảng trao đổi dữ liệu có thể thể hiện thông tin trao đổi dữ liệu được đưa ra bởi bên giữ dữ liệu, để thông tin có thể được tìm thấy dễ dàng bởi bên yêu cầu dữ liệu. Tại cùng một thời điểm trong quy trình trao đổi dữ liệu, nền tảng trao đổi dữ liệu, đóng vai trò trung gian, có thể nhận dữ liệu từ bên giữ dữ liệu, và sau đó gửi dữ liệu đến bên yêu cầu dữ liệu. Theo cách này, nền tảng trao đổi dữ liệu có thể sử dụng dữ liệu được trao đổi giữa cả hai bên cho các mục đích khác, hoặc thay đổi dữ liệu mà không cần ủy quyền trước khi gửi dữ liệu đến bên nhận, gây tổn hại đến lợi ích của các bên trao đổi dữ liệu. Tức là, trong quy trình trao đổi dữ liệu hiện có, an ninh dữ liệu tương đối thấp.

Bản chất kỹ thuật của sáng chế

Các phương án của sáng chế đề xuất phương pháp gửi dữ liệu để giải quyết vấn đề an ninh dữ liệu thấp trong quy trình trao đổi dữ liệu hiện có.

Các phương án của sáng chế chấp nhận giải pháp kỹ thuật sau đây:

Phương pháp gửi dữ liệu được đề xuất, bao gồm các bước:

ghi, bởi nền tảng trao đổi dữ liệu, thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối và lưu trữ thỏa thuận này;

nhận, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa, thiết bị đầu cuối thứ nhất là thiết bị đầu cuối tương ứng với người dùng thứ nhất; và

gửi, bởi thiết bị đầu cuối thứ nhất, dữ liệu thứ nhất được mã hóa đến thiết bị đầu cuối thứ hai, thiết bị đầu cuối thứ hai là thiết bị đầu cuối tương ứng với người dùng thứ hai;

gửi, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất đến thiết bị đầu cuối thứ hai; và

giải mã, bởi thiết bị đầu cuối thứ hai, dữ liệu thứ nhất được mã hóa thu được dựa trên khóa thứ nhất để thu dữ liệu thứ nhất.

Các phương án của sáng chế còn đề xuất phương pháp gửi dữ liệu để giải quyết vấn đề an ninh dữ liệu thấp trong quy trình trao đổi dữ liệu hiện có.

Các phương án của sáng chế chấp nhận giải pháp kỹ thuật sau đây:

Phương pháp gửi dữ liệu được đề xuất, bao gồm các bước:

ghi, bởi nền tảng trao đổi dữ liệu, thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối và lưu trữ thỏa thuận này;

nhận, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa, thiết bị đầu cuối thứ nhất là thiết bị đầu cuối tương ứng với người dùng thứ nhất; và

gửi, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất đến thiết bị đầu cuối thứ hai, sao cho thiết bị đầu cuối thứ hai, sau khi nhận dữ liệu thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất, giải mã dữ liệu thứ nhất được mã hóa thu được dựa trên khóa thứ nhất để thu dữ liệu thứ nhất, thiết bị đầu cuối thứ hai là thiết bị đầu cuối tương ứng với người dùng thứ hai.

Các phương án của sáng chế còn đề xuất phương pháp gửi dữ liệu để giải quyết vấn đề an ninh dữ liệu thấp trong quy trình trao đổi dữ liệu hiện có.

Các phương án của sáng chế chấp nhận giải pháp kỹ thuật sau đây:

Phương pháp gửi dữ liệu được đề xuất, bao gồm:

nhận, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa, thiết bị đầu cuối thứ nhất là thiết bị đầu cuối tương ứng với người dùng thứ nhất; và

gửi, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất đến thiết bị đầu cuối thứ hai, sao cho thiết bị đầu cuối thứ hai, sau khi nhận dữ liệu thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất, giải mã dữ liệu thứ nhất được mã hóa thu được dựa trên khóa thứ nhất để thu dữ liệu thứ nhất, thiết bị đầu cuối thứ hai là thiết bị đầu cuối tương ứng với người dùng thứ hai.

Các phương án của sáng chế còn đề xuất thiết bị gửi dữ liệu để giải quyết vấn đề an ninh dữ liệu thấp trong quy trình trao đổi dữ liệu hiện có.

Các phương án của sáng chế chấp nhận giải pháp kỹ thuật sau đây:

Thiết bị gửi dữ liệu được đề xuất, bao gồm:

bộ ghi được tạo cấu hình để ghi thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối và lưu trữ thỏa thuận này;

bộ nhận thứ nhất được tạo cấu hình để nhận khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa, thiết bị đầu cuối thứ nhất là thiết bị đầu cuối tương ứng với người dùng thứ nhất; và

bộ gửi thứ nhất được tạo cấu hình để gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, sao cho thiết bị đầu cuối thứ hai, sau khi nhận dữ liệu thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất, giải mã dữ liệu thứ nhất được mã hóa thu được dựa trên khóa thứ nhất để thu dữ liệu thứ nhất, thiết bị đầu cuối thứ hai là thiết bị đầu cuối tương ứng với người dùng thứ hai.

Ít nhất một trong số các giải pháp kỹ thuật nêu trên được chấp nhận bởi các phương án của sáng chế có thể đạt được các hiệu quả có lợi sau đây:

Trong khi trao đổi dữ liệu, nền tảng trao đổi dữ liệu ghi thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai mà trao đổi dữ liệu trong chuỗi khối. Nền tảng trao đổi dữ liệu sau đó nhận khóa thứ nhất, được gửi bởi thiết bị đầu cuối thứ nhất tương ứng với người dùng thứ nhất, để giải mã dữ liệu thứ nhất được mã hóa. Thiết bị đầu cuối thứ nhất gửi dữ liệu thứ nhất được mã hóa đến thiết bị đầu cuối thứ hai tương ứng với người dùng thứ hai. Nền tảng trao đổi dữ liệu gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, và thiết bị đầu cuối thứ hai giải mã dữ liệu thứ nhất được mã hóa thu được dựa trên khóa thứ nhất, để thu dữ liệu thứ nhất. Rõ ràng là nền tảng trao đổi dữ liệu giữ sạch cho dữ liệu thứ nhất được trao đổi trong quy trình trao đổi dữ liệu, nhờ đó tránh nguy cơ mà dữ liệu thứ nhất có thể được sử dụng bởi nền tảng trao đổi dữ liệu cho các mục đích khác, tăng cường an ninh dữ liệu trong quy trình trao đổi dữ liệu, và cùng lúc với nền tảng trao đổi dữ liệu.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo được mô tả trong bản mô tả này được sử dụng để hiểu thêm về sáng chế, và cấu thành một phần của sáng chế. Các phương án làm ví dụ của sáng chế và các minh họa của các phương án này được sử dụng để giải thích sáng chế, và không tạo thành giới hạn không thích hợp đối với sáng chế. Trong các hình vẽ:

FIG.1 là lưu đồ giản lược thực hiện phương pháp gửi dữ liệu theo một phương án của sáng chế;

FIG.2 là sơ đồ giản lược của kịch bản thực hiện của phương pháp gửi dữ liệu theo một phương án của sáng chế;

FIG.3 là lưu đồ giản lược thực hiện phương pháp giao dịch dữ liệu theo một phương án của sáng chế; và

FIG.4 là sơ đồ cấu trúc giản lược cụ thể của thiết bị gửi dữ liệu theo một phương án của sáng chế.

FIG.5 là lưu đồ minh họa ví dụ khác về phương pháp được thực hiện bằng máy tính cho các giao dịch dữ liệu an toàn, theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

Để làm cho các mục tiêu, các giải pháp kỹ thuật và các ưu điểm theo sáng chế dễ hiểu hơn, các giải pháp kỹ thuật theo sáng chế được mô tả rõ ràng và toàn diện thông qua các phương án cụ thể của sáng chế và các hình vẽ kèm theo tương ứng. Hiển nhiên, các phương án được mô tả chỉ là một số phương án tốt hơn là tất cả các phương án của sáng chế. Dựa trên các phương án của sáng chế, tất cả các phương án khác được suy ra bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật này mà không cần bất kỳ nỗ lực sáng tạo nào sẽ nằm trong phạm vi bảo hộ theo sáng chế.

Như được mô tả trong phần tình trạng kỹ thuật của sáng chế, dữ liệu, dưới dạng sóng mang thông tin, luôn có giá trị nhất định. Cụ thể, trong thời đại dữ liệu lớn, dữ liệu lớn có giá trị to lớn cho chính phủ và các doanh nghiệp để tiến hành các công việc khác nhau. Thông tin được trích xuất từ dữ liệu lớn có thể giúp đỡ chính phủ và các doanh nghiệp đưa ra các quyết định tốt hơn. Ví dụ, các vị trí kết nối mạng xã hội lớn luôn tích lũy lượng lớn dữ liệu người dùng, không những ghi thông tin nhận dạng cá nhân của người dùng mà còn phản ánh sở thích cá nhân, thói quen sống, mối quan hệ cá nhân của người dùng, và thông tin khác đối với phạm vi nhất định. Thông tin được chứa trong dữ liệu có giá trị sử dụng lớn để tiến hành các công việc tiếp theo, và giá trị sử dụng của nó, ví dụ, có thể hỗ trợ các công ty tiếp thị để đẩy quảng cáo đến người dùng một cách chính xác.

Để tận dụng hết giá trị dữ liệu, các bên giữ dữ liệu có thể trao đổi dữ liệu với nhau để đào sâu thông tin có giá trị từ dữ liệu được trao đổi, nhờ đó đẩy mạnh sự phát triển của các doanh nghiệp. Do đó, để tạo thuận lợi cho các bên yêu cầu dữ liệu để tìm kiếm dữ liệu hữu ích cho họ, cả hai bên trao đổi dữ liệu có thể trao đổi dữ liệu thông qua nền tảng trao đổi dữ liệu.

Tuy nhiên, vì dữ liệu có thể tái sản xuất, quyền sở hữu dữ liệu không rõ ràng như đối tượng thực. Khi đối tượng thực được chuyển từ bên A đến bên B, bên A mất quyền sở hữu của đối tượng thực. Tuy nhiên, khi dữ liệu được chuyển từ một bên đến bên khác, nếu dữ liệu truyền qua bên thứ ba trong quy trình này, bên thứ ba có thể sao chép dữ liệu, nhờ đó sở hữu dữ liệu. Điều này có thể làm tổn hại đến các lợi ích của cả hai bên trao đổi dữ liệu.

Nền tảng trao đổi dữ liệu có thể không những đóng vai trò làm tương thích trao đổi dữ liệu giữa cả hai bên, mà còn đóng vai trò là bên bảo lãnh, tức là, đảm bảo các lợi ích của cả hai bên trong quy trình trao đổi dữ liệu. Trong quy trình trao đổi dữ liệu hiện có, để ngăn ngừa trường hợp là, sau khi một bên trao đổi dữ liệu gửi dữ liệu, bên khác không gửi chính dữ liệu của nó, nền tảng trao đổi dữ liệu có thể thu thập dữ liệu của cả hai bên trao đổi dữ liệu trước, và sau đó gửi tách biệt dữ liệu cho cả hai bên trao đổi dữ liệu, nhờ đó ngăn ngừa một trong hai bên hủy lời cam kết. Theo cách này, nền tảng trao đổi dữ liệu có thể có cơ hội sử dụng dữ liệu cho các mục đích khác. Điều này sẽ dẫn đến an ninh dữ liệu thấp trong khi trao đổi. Để giải quyết vấn đề này, sáng chế đề xuất phương pháp gửi dữ liệu. Phương pháp gửi dữ liệu được đề xuất theo sáng chế có thể được thực hiện bởi nền tảng trao đổi dữ liệu, và nền tảng trao đổi dữ liệu có thể là phần mềm, phần cứng, hoặc kết hợp của phần mềm và phần cứng để thực hiện phương pháp này.

Sau đây, giải pháp kỹ thuật được đề xuất trong mỗi phương án của sáng chế được mô tả chi tiết với tham chiếu đến các hình vẽ kèm theo.

Phương án 1

Để giải quyết vấn đề an ninh dữ liệu thấp trong quy trình trao đổi dữ liệu hiện có, Phương án 1 theo sáng chế đề xuất phương pháp gửi dữ liệu. Theo phương án này của sáng chế, để dễ mô tả, cả hai bên trao đổi dữ liệu được gọi là người dùng thứ nhất

và người dùng thứ hai. Người dùng thứ nhất và người dùng thứ hai có thể là tổ chức hoặc cá nhân bất kỳ. Người dùng thứ nhất và người dùng thứ hai trong bản mô tả này được sử dụng để phân biệt cả hai bên giao dịch dữ liệu, và không được hiểu là giới hạn với cả hai bên giao dịch dữ liệu theo sáng chế.

Cả hai bên trao đổi dữ liệu, trong khi trao đổi dữ liệu, có thể thực hiện một số hoạt động bằng cách sử dụng các thiết bị đầu cuối. Để dễ mô tả, thiết bị đầu cuối tương ứng với hoạt động được thực hiện bởi người dùng thứ nhất được gọi là thiết bị đầu cuối thứ nhất, và thiết bị đầu cuối tương ứng với hoạt động được thực hiện bởi người dùng thứ hai được gọi là thiết bị đầu cuối thứ hai. Cần lưu ý rằng, trong toàn bộ quy trình trao đổi dữ liệu, cùng một người dùng có thể sử dụng cùng một thiết bị đầu cuối, và cũng có thể sử dụng các thiết bị đầu cuối khác nhau. Tức là, thiết bị đầu cuối thứ nhất được đề cập trong mỗi quy trình theo phương án của sáng chế có thể là các thiết bị đầu cuối khác nhau, và thiết bị đầu cuối thứ hai cũng có thể là các thiết bị đầu cuối khác nhau. Thiết bị đầu cuối ở đây, ví dụ, có thể là máy tính cá nhân, máy chủ, thiết bị đầu cuối di động, hoặc các thiết bị điện toán khác, không bị giới hạn theo sáng chế.

Trong khi trao đổi dữ liệu, cả hai bên trao đổi dữ liệu thường đạt được thỏa thuận trao đổi dữ liệu trước khi trao đổi dữ liệu. Thỏa thuận trao đổi dữ liệu ở đây đề cập đến thỏa thuận về chi tiết của trao đổi dữ liệu đạt được bởi cả hai bên trao đổi dữ liệu trước khi dữ liệu được trao đổi. Thỏa thuận trao đổi dữ liệu bao gồm các điều khoản được quy định bởi cả hai bên trao đổi dữ liệu để xác định các quyền lợi và nghĩa vụ tương ứng của họ, và các điều khoản được tuân thủ bởi cả hai bên.

Khi thỏa thuận trao đổi dữ liệu đạt được, người dùng thứ nhất có thể đưa ra thông tin dữ liệu về nền tảng trao đổi dữ liệu thông qua thiết bị đầu cuối thứ nhất. Sau khi nhận thông tin dữ liệu được đưa ra bởi thiết bị đầu cuối thứ nhất, nền tảng trao đổi dữ liệu sau đó có thể công bố thông tin dữ liệu. Do đó, người dùng thứ hai quan tâm đến thông tin dữ liệu, sau khi thấy thông tin dữ liệu, có thể gửi yêu cầu lệnh đối với thông tin dữ liệu đến nền tảng trao đổi dữ liệu thông qua thiết bị đầu cuối thứ hai. Nền tảng trao đổi dữ liệu nhận yêu cầu lệnh của thiết bị đầu cuối thứ hai đối với thông tin dữ liệu được công bố, và gửi yêu cầu đến thiết bị đầu cuối thứ nhất. Sau khi thiết bị

đầu cuối thứ nhất thực hiện xác nhận, nền tảng trao đổi dữ liệu có thể nhận thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ nhất đối với yêu cầu lệnh, nhờ đó đạt được thỏa thuận trao đổi dữ liệu.

Trên đây mô tả vắn tắt quy trình đạt được thỏa thuận. Trong các ứng dụng thực, cả hai bên trao đổi dữ liệu có thể quyết định các chi tiết của thỏa thuận thông qua các đàm phán lặp lại. Thỏa thuận trao đổi dữ liệu có thể bao gồm cụ thể thông tin nhận dạng của cả hai bên trao đổi dữ liệu, thông tin dấu hiệu về dữ liệu được trao đổi, các đặc tả sử dụng dữ liệu và các biện pháp trừng phạt đối với sự vi phạm của thỏa thuận được tuân theo bởi các hai bên, và thông tin khác. Theo cách này, sau khi nhận dữ liệu, bộ nhận có thể đưa ra các biện pháp tương ứng trên cơ sở của thỏa thuận nếu tìm thấy rằng dữ liệu không phù hợp với mô tả trong thỏa thuận.

Trong thỏa thuận này, thông tin dấu hiệu của dữ liệu được trao đổi giữa cả hai bên có thể bao gồm ít nhất một trong số sau: tóm lược tin báo để xác minh tính toàn vẹn của dữ liệu, và thông tin đường cơ sở để tóm lược nội dung cụ thể của dữ liệu. Đối với dữ liệu thứ nhất, sau đó thông tin dấu hiệu về dữ liệu thứ nhất bao gồm ít nhất một trong số sau: tóm lược tin báo để xác minh tính toàn vẹn của dữ liệu thứ nhất, và thông tin đường cơ sở để tóm lược nội dung cụ thể của dữ liệu thứ nhất.

Tóm lược tin báo là giá trị độ dài cố định tương ứng duy nhất với tin báo hoặc tài liệu, giá trị này được xác định dựa trên thuật toán băm một chiều. Do đó, khi dữ liệu cần được trao đổi được sửa đổi, tóm lược tin báo của dữ liệu cũng có thể được thay đổi. Các thuật toán băm một chiều được sử dụng phổ biến bao gồm: thuật toán tóm lược tin báo 5 (Message Digest Algorithm 5 - MD5), thuật toán băm bảo mật (Secure Hash Algorithm - SHA), mã xác thực tin báo (Message Authentication Code - MAC), và v.v.

Dựa trên tóm lược tin báo về dữ liệu thứ nhất được chứa trong thỏa thuận, sau khi nhận dữ liệu được mã hóa, người dùng thứ hai có thể tiến hành kiểm tra tính toàn vẹn đối với dữ liệu được mã hóa để đánh giá liệu dữ liệu nhận được có được sửa đổi hay không. Trong lúc đó, giá trị kiểm tra tính toàn vẹn cũng có thể trở thành cơ sở để sử dụng trong các cuộc tranh chấp trong tương lai giữa cả hai bên trao đổi dữ liệu.

Thông tin đường cơ sở để tóm lược nội dung cụ thể của dữ liệu thứ nhất có thể là, ví dụ, kiểu dữ liệu được bao gồm trong dữ liệu thứ nhất, hoặc một số điều kiện cụ thể mà dữ liệu trong dữ liệu thứ nhất cần thỏa mãn, hoặc các hiệu quả có thể đạt được bởi dữ liệu trong dữ liệu thứ nhất theo sáng chế, và v.v. Dựa trên thông tin này, thiết bị đầu cuối thứ hai có thể kiểm tra nội dung cụ thể của dữ liệu thứ nhất, do đó ngăn ngừa người dùng thứ hai khỏi bị đánh lừa, và tránh làm tổn thất lợi ích riêng.

Trên đây mô tả quy trình đạt được thỏa thuận trao đổi dữ liệu bởi cả hai bên trao đổi dữ liệu trước khi gửi dữ liệu. Quy trình gửi dữ liệu bởi cả hai bên trao đổi dữ liệu theo sáng chế, tức là, phương pháp gửi dữ liệu được đề xuất theo sáng chế, sau đó sẽ được đưa vào chi tiết sau đây. Lưu đồ giản lược thực hiện phương pháp được thể hiện trên FIG.1. Phương pháp này bao gồm các bước sau đây:

Bước 101: Nền tảng trao đổi dữ liệu ghi thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối và lưu trữ thỏa thuận này.

Trong kỷ nguyên công nghệ thông tin, thỏa thuận cũng có thể được lưu trữ trong vật ghi lưu trữ của thiết bị điện toán trong dạng dữ liệu, và dữ liệu được lưu trữ trong vật ghi lưu trữ, dữ liệu có thể có nguy cơ bị sửa đổi. Để ngăn ngừa cả hai bên trao đổi dữ liệu khỏi việc sửa đổi thỏa thuận không có ủy quyền, và tăng cường an ninh của dữ liệu thỏa thuận, nền tảng trao đổi dữ liệu có thể được sử dụng là bên thứ ba để lưu thỏa thuận này.

Tuy nhiên, nếu thỏa thuận được lưu trữ bởi nền tảng trao đổi dữ liệu, sẽ có nguy cơ rằng nền tảng trao đổi dữ liệu có thể sửa đổi thỏa thuận. Nếu nền tảng trao đổi dữ liệu thông đồng với một bên trao đổi dữ liệu để sửa đổi thỏa thuận, các lợi ích của bên khác sẽ bị tổn hại. Để tăng cường thêm an ninh của dữ liệu thỏa thuận và tăng cường độ đáng tin của nền tảng trao đổi dữ liệu, trong khi lưu trữ thỏa thuận, công nghệ chuỗi khối có thể được sử dụng để lưu trữ thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai.

Công nghệ chuỗi khối là công nghệ lưu trữ dữ liệu được phân tán không tập trung, không đáng tin cậy, chống giả mạo. Cấu trúc dữ liệu được lưu trữ bằng cách sử dụng công nghệ chuỗi khối là cấu trúc dữ liệu được móc nối. Dữ liệu trong cấu trúc dữ

liệu được móc nối có thể được thay đổi chỉ theo cách gia tăng. Dữ liệu được ghi sẵn sẽ giữ trạng thái khởi động, và sẽ không bị che đi.

Trong lúc đó, chuỗi khối tuân theo cơ chế đồng thuận khi ghi dữ liệu. Khi nút ghi dữ liệu, dữ liệu được ghi có thể được ghi trong mỗi nút của chuỗi khối chỉ sau khi đạt được sự đồng thuận của hầu hết các nút trong chuỗi khối. Điều này làm giảm đáng kể khả năng là dữ liệu được lưu trữ là dữ liệu bất hợp pháp, do đó làm giảm đáng kể khả năng thỏa thuận bị làm giả mạo.

Cơ chế đồng thuận được sử dụng trong công nghệ chuỗi khối có thể là, ví dụ, cơ chế bằng chứng công việc, cơ chế bằng chứng cổ phần, cơ chế bằng chứng cổ phần được ủy nhiệm, cơ chế vùng trữ xác minh, và v.v. Nếu được dự định để thay đổi dữ liệu hiện có trong chuỗi khối, lựa chọn duy nhất là thay thế dữ liệu ban đầu bằng cách giả mạo chuỗi bên. Giá thành cho việc giả mạo là quá lớn đối với sự khó khăn về kỹ thuật, tốn thời gian, và việc sử dụng lao động. Hầu như không thể hoàn thành việc này dưới cơ chế đồng thuận của chuỗi khối.

Có thể kết luận thông qua phân tích nêu trên rằng phương án theo sáng chế lưu trữ thỏa thuận trao đổi dữ liệu bằng các phương thức của công nghệ chuỗi khối, có thể ngăn ngừa hiệu quả khả năng thỏa thuận bị làm giả mạo, và làm tăng cường đáng kể an ninh của thỏa thuận trao đổi dữ liệu.

Bước 102: Nền tảng trao đổi dữ liệu nhận khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa.

Dữ liệu thứ nhất được đề cập ở đây là dữ liệu mà người dùng thứ nhất mong đợi gửi đến người dùng thứ hai. Do đó, người dùng thứ nhất ở đây là người gửi dữ liệu thứ nhất, và người dùng thứ hai là người nhận dữ liệu thứ nhất. Tất nhiên, trong lĩnh vực máy tính, người có hiểu biết trung bình trong lĩnh vực kỹ thuật này hiểu được việc gửi dữ liệu giữa người dùng, trong các hoạt động thực, có thể là người dùng gửi dữ liệu đến thiết bị đầu cuối của người dùng khác thông qua thiết bị đầu cuối của chúng.

Để ngăn ngừa dữ liệu khỏi bị mất bởi bên thứ ba ngoài cả hai bên trao đổi, dữ liệu thứ nhất có thể được mã hóa, và sau đó được gửi đến thiết bị đầu cuối thứ hai.

Trong việc mã hóa, việc mã hóa được sử dụng để ẩn thông tin văn bản gốc, để thông tin không đọc được khi không có khóa giải mã, nhờ đó tăng cường an ninh trong việc truyền dữ liệu.

Dữ liệu được truyền qua nền tảng tương tác dữ liệu sau khi được mã hóa, nhưng vẫn không thể ngăn ngừa hoàn toàn dữ liệu thứ nhất được mã hóa được sử dụng bởi nền tảng trao đổi dữ liệu. Ví dụ, dữ liệu có thể bị tổn hại bởi nền tảng trao đổi dữ liệu. Sau đó dữ liệu thứ nhất được mã hóa có thể được gửi trực tiếp bởi thiết bị đầu cuối thứ nhất đến thiết bị đầu cuối thứ hai, và nền tảng trao đổi dữ liệu giữ sạch dữ liệu được trao đổi, do đó tăng cường hơn nữa an ninh trong việc truyền dữ liệu.

Dữ liệu có thể được mã hóa bởi thiết bị đầu cuối thứ nhất sử dụng các phương pháp mã hóa khác nhau. Ví dụ, dữ liệu thứ nhất có thể được mã hóa bằng cách sử dụng thuật toán mã hóa đối xứng. Trong trường hợp này, khóa thứ nhất ở đây là khóa được sử dụng để mã hóa dữ liệu thứ nhất. Theo cách này, nền tảng trao đổi dữ liệu xác định khóa để giải mã dữ liệu thứ nhất được mã hóa bằng cách nhận khóa được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để mã hóa dữ liệu thứ nhất. Hoặc, thiết bị đầu cuối thứ nhất cũng có thể mã hóa dữ liệu thứ nhất bằng cách sử dụng thuật toán mã hóa không đối xứng, và mã hóa dữ liệu thứ nhất với khóa công khai được gửi bởi nền tảng trao đổi dữ liệu. Theo cách này, nền tảng trao đổi dữ liệu chỉ cần xác định khóa riêng tư để giải mã dữ liệu được mã hóa.

Để hạn chế cả hai bên trao đổi dữ liệu, tốt hơn là khóa thứ nhất được gửi bởi nền tảng trao đổi dữ liệu tại thời điểm đúng thay vì được gửi trực tiếp bởi thiết bị đầu cuối thứ nhất đến thiết bị đầu cuối thứ hai. Tức là, sau khi thiết bị đầu cuối thứ nhất mã hóa dữ liệu thứ nhất bằng cách sử dụng thuật toán mã hóa đối xứng, khóa thứ nhất được sử dụng trong việc mã hóa có thể được gửi đến nền tảng trao đổi dữ liệu. Sau khi nhận khóa được gửi bởi thiết bị đầu cuối thứ nhất, nền tảng trao đổi dữ liệu có thể gửi khóa đến thiết bị đầu cuối thứ hai bằng cách thực hiện bước 103.

Bước 103: Nền tảng trao đổi dữ liệu gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai.

Theo cách này, thiết bị đầu cuối thứ hai, sau khi nhận dữ liệu thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất, có thể giải mã dữ liệu thứ nhất được mã hóa thu được

dựa trên khóa thứ nhất để thu dữ liệu thứ nhất. Thiết bị đầu cuối thứ hai là thiết bị đầu cuối tương ứng với người dùng thứ hai.

Tương tự, khi gửi dữ liệu đến thiết bị đầu cuối thứ nhất, thiết bị đầu cuối thứ hai cũng có thể mã hóa dữ liệu bằng cách sử dụng khóa. Ở đây, dữ liệu cần được trao đổi được giữ bởi người dùng thứ hai được gọi là dữ liệu thứ hai. Sau khi mã hóa dữ liệu thứ hai, thiết bị đầu cuối thứ hai gửi dữ liệu thứ hai được mã hóa đến thiết bị đầu cuối thứ nhất, và sau đó gửi khóa thứ hai để giải mã dữ liệu được mã hóa đến nền tảng trao đổi dữ liệu. Sau đó nền tảng gửi khóa đến thiết bị đầu cuối thứ nhất, sao cho thiết bị đầu cuối thứ nhất có thể giải mã dữ liệu thứ hai được mã hóa bằng cách sử dụng khóa để thu dữ liệu thứ hai, do đó thực hiện trao đổi dữ liệu giữa cả hai bên. Trong quy trình này, dữ liệu được trao đổi giữa cả hai bên không đi qua nền tảng trao đổi dữ liệu, nhờ đó tăng cường an ninh cho dữ liệu được trao đổi.

Cần lưu ý rằng, theo phương án của sáng chế, để dễ mô tả, dữ liệu được giữ bởi người dùng thứ nhất được gọi là dữ liệu thứ nhất, dữ liệu được giữ bởi người dùng thứ hai được gọi là là dữ liệu thứ hai, và quy trình trao đổi dữ liệu bởi cả hai bên là quy trình trao đổi dữ liệu thứ nhất và dữ liệu thứ hai với nhau. Có thể hiểu rằng các thuật ngữ "thứ nhất" và "thứ hai" được sử dụng theo phương án của sáng chế được sử dụng để phân biệt các đối tượng được mô tả khác nhau, và không đề cập đến các đối tượng cụ thể.

Để tăng cường hơn nữa an ninh dữ liệu và để ngăn ngừa tổn thất đối với các lợi ích của một trong hai bên, sau khi các khóa được gửi bởi cả hai bên đối với dữ liệu được mã hóa nhận được, cũng có thể gửi các khóa đến cả hai bên sau khi thông tin xác nhận được gửi bởi cả hai bên đối với dữ liệu nhận được, để ngăn ngừa trường hợp một bên không gửi khóa sau khi nhận dữ liệu, làm tổn hại nhiều đến các lợi ích của bên khác. Ví dụ, sau khi gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, nền tảng trao đổi dữ liệu gửi khóa thứ hai đến thiết bị đầu cuối thứ nhất sau khi nhận thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ hai đối với dữ liệu thứ nhất. Thông tin xác nhận cho dữ liệu thứ nhất chỉ báo rằng người dùng thứ hai xác định rằng dữ liệu thứ nhất phù hợp với mô tả về thỏa thuận này, do đó bảo vệ hiệu quả lợi ích của người dùng thứ hai. Tương tự, sau khi nhận thông tin xác nhận được gửi bởi người dùng thứ hai đối

với dữ liệu thứ nhất, nền tảng trao đổi dữ liệu cũng có thể nhận thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ nhất cho dữ liệu thứ hai. Thông tin xác nhận cho dữ liệu thứ hai chỉ báo rằng người dùng thứ nhất xác định rằng dữ liệu thứ hai phù hợp với mô tả về thỏa thuận này.

Một số loại dữ liệu có thể được trao đổi thông qua nền tảng. Dữ liệu có thể là, ví dụ, dữ liệu mà người dùng không quan tâm đến việc có thu được bởi bên thứ ba hay không, hoặc dữ liệu mà giá trị dữ liệu không thể đạt được thông qua sự sao chép. Các loại dữ liệu này không cần được mã hóa, do đó tiết kiệm các tài nguyên tính toán và các tài nguyên lưu trữ. Để dễ mô tả, dữ liệu mà có thể được trao đổi thông qua nền tảng được gọi là dữ liệu thứ ba.

Sau đây, phương pháp trao đổi dữ liệu được đề xuất theo sáng chế được minh họa chi tiết bằng cách sử dụng, ví dụ, trong đó là dữ liệu được trao đổi của người dùng thứ hai là dữ liệu thứ ba có thể được trao đổi thông qua nền tảng trao đổi dữ liệu, và công nghệ để mã hóa dữ liệu thứ nhất được trao đổi là công nghệ mã hóa đối xứng. Phương pháp bao gồm các bước sau:

Bước 201: Nền tảng trao đổi dữ liệu ghi thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối và lưu trữ thỏa thuận này.

Bước 202: Nền tảng trao đổi dữ liệu nhận khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa.

Bước 203: Thiết bị đầu cuối thứ nhất gửi dữ liệu thứ nhất được mã hóa đến thiết bị đầu cuối thứ hai.

Bước 204: Thiết bị đầu cuối thứ hai gửi dữ liệu thứ ba đến nền tảng trao đổi dữ liệu.

Cần lưu ý rằng sáng chế không giới hạn thứ tự thực hiện bước 202, bước 203, và bước 204.

Bước 205: Nền tảng trao đổi dữ liệu gửi khóa thứ nhất được nhận đến thiết bị đầu cuối thứ hai.

Vì người dùng thứ hai gửi dữ liệu thứ ba đến nền tảng trao đổi dữ liệu một cách trực tiếp, nền tảng trao đổi dữ liệu có thể xác minh dữ liệu thứ ba, và có thể không gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai nếu thấy rằng dữ liệu thứ ba không phù hợp với thỏa thuận đạt được bởi cả hai bên, để tránh làm tổn hại đến lợi ích của người dùng thứ nhất. Do đó, quy trình thực hiện cụ thể của bước này có thể là: gửi khóa thứ nhất được nhận đến thiết bị đầu cuối thứ hai khi được xác định rằng dữ liệu thứ ba phù hợp với thỏa thuận của cả hai bên.

Bước 206: Thiết bị đầu cuối thứ hai giải mã dữ liệu thứ nhất được mã hóa nhận được theo khóa thứ nhất được nhận để thu dữ liệu thứ nhất.

Bước 207: Nền tảng trao đổi dữ liệu gửi dữ liệu thứ ba đến thiết bị đầu cuối thứ nhất.

Đối với dữ liệu thứ nhất thu được bởi người dùng thứ hai, vì nền tảng giữ sạch cho dữ liệu thứ nhất, nền tảng này sẽ không thể xác minh tính xác thực của chúng. Trong trường hợp này, dữ liệu thứ nhất được xác minh bởi thiết bị đầu cuối thứ hai. Trong khi xác minh, thiết bị đầu cuối thứ hai có thể thu thập thông tin dấu hiệu về dữ liệu thứ nhất được đồng ý bởi cả hai bên trong thỏa thuận giao dịch. Cụ thể, thông tin dấu hiệu có thể đạt được từ thỏa thuận được lưu trữ trong chuỗi khối. Rõ ràng, khi cả hai bên đàm phán thỏa thuận này, thiết bị đầu cuối thứ hai cũng luôn lưu trữ thỏa thuận này một cách cục bộ. Do đó, thiết bị đầu cuối thứ hai cũng có thể thu thập thông tin dấu hiệu từ thỏa thuận được lưu trữ bởi thiết bị đầu cuối thứ hai. Sau khi thu thập thông tin dấu hiệu về dữ liệu thứ nhất trong thỏa thuận, thiết bị đầu cuối thứ hai có thể kiểm tra liệu dữ liệu thứ nhất thu được có phù hợp với bản ghi trong thỏa thuận theo thông tin dấu hiệu thu được.

Theo cách này, nếu người dùng thứ hai thấy rằng dữ liệu thứ nhất không phù hợp với thỏa thuận ban đầu, nền tảng không thể gửi dữ liệu thứ ba đến thiết bị đầu cuối thứ nhất, để tránh làm tổn hại đến lợi ích của người dùng thứ hai.

Do đó, dữ liệu thứ ba có thể được gửi đến thiết bị đầu cuối thứ nhất khi lệnh gửi dữ liệu được gửi bởi thiết bị đầu cuối thứ hai được nhận. Lệnh gửi dữ liệu ở đây là lệnh để lệnh cho nền tảng trao đổi dữ liệu để gửi dữ liệu thứ ba đến người dùng thứ nhất. Ví dụ, lệnh này có thể là thông tin xác nhận nêu trên cho dữ liệu thứ nhất, chỉ

báo rằng dữ liệu thứ ba được gửi đến thiết bị đầu cuối thứ nhất chỉ sau khi người dùng thứ hai gửi xác định rằng dữ liệu thứ nhất phù hợp với mô tả trong thỏa thuận này.

Tuy nhiên, nếu người dùng không gửi lệnh gửi dữ liệu đến nền tảng, người dùng thứ nhất không thể nhận dữ liệu thứ ba. Để tránh làm tổn hại đến các lợi ích của dữ liệu thứ nhất, trong một số trường hợp, dữ liệu thứ ba cũng có thể được gửi đến người dùng thứ nhất. Ví dụ, nếu người dùng thứ nhất vẫn không gửi thông tin xác nhận cho dữ liệu thứ nhất sau khoảng thời gian thiết lập trước vì khóa thứ nhất được gửi đến người dùng thứ hai, dữ liệu thứ ba có thể được gửi đến người dùng thứ nhất tại thời điểm này.

Dựa trên nội dung nêu trên, quy trình thực hiện cụ thể của bước 207 có thể là: gửi dữ liệu thứ ba đến người dùng thứ nhất khi được xác định rằng điều kiện thiết lập trước được thỏa mãn. Ở đây, thời điểm khi điều kiện thiết lập trước được thỏa mãn có thể là sau khi lệnh gửi dữ liệu được gửi bởi thiết bị đầu cuối thứ hai nhận được, hoặc sau khoảng thời gian thiết lập trước vì khóa này được gửi đến thiết bị đầu cuối thứ hai.

Trước đây, sự trao đổi của dữ liệu thứ nhất và dữ liệu thứ ba giữa những người dùng được thực hiện. Phương pháp này có thể ngăn ngừa trường hợp mà một bên không gửi dữ liệu đến bên khác sau khi thu thập dữ liệu được gửi bởi bên khác, nhờ đó bảo vệ lợi ích của cả hai bên trao đổi dữ liệu.

Sau khi hoàn thành việc trao đổi dữ liệu, nền tảng trao đổi dữ liệu cũng có thể ghi bản ghi mà sự trao đổi được hoàn thành vào kết quả của thỏa thuận thay đổi dữ liệu trong chuỗi khối và lưu trữ bản ghi này, đối với việc sử dụng tiếp theo.

Theo phương án của sáng chế, trạng thái truyền dữ liệu được mã hóa cũng có thể được xác định để ngăn ngừa người dùng thứ hai nhận dữ liệu được mã hóa nhưng yêu cầu rằng dữ liệu được mã hóa không nhận được, và để ngăn ngừa việc thiết bị đầu cuối thứ nhất không gửi dữ liệu đến thiết bị đầu cuối thứ hai nhưng người dùng thứ nhất yêu cầu phải được gửi dữ liệu đến thiết bị đầu cuối thứ hai. Dữ liệu được mã hóa ở đây là dữ liệu được trao đổi được mã hóa, ví dụ, dữ liệu thứ nhất được mã hóa và dữ liệu thứ hai được mã hóa nêu trên. Trạng thái truyền bao gồm một trong số trạng thái sau: dữ liệu được mã hóa không được truyền, dữ liệu được mã hóa được truyền, và dữ liệu được mã hóa được truyền đến thiết bị đầu cuối thứ hai.

Cách thức cụ thể để xác định trạng thái truyền của dữ liệu được mã hóa có thể như sau: nền tảng tương tác dữ liệu thu thập trạng thái truyền của dữ liệu được mã hóa thông qua chương trình giám sát định trước. Chương trình giám sát có thể là chương trình được sử dụng để truyền dữ liệu giữa cả hai bên trao đổi dữ liệu. Hoặc, cách thức cụ thể để xác định trạng thái truyền của dữ liệu được mã hóa cũng có thể là: nhận trạng thái truyền của dữ liệu được mã hóa được báo cáo chủ động bởi thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai.

Dữ liệu được mã hóa được gửi bởi thiết bị đầu cuối thứ nhất không đi qua nền tảng trao đổi dữ liệu. Do đó, nếu thiết bị đầu cuối thứ nhất cần thực hiện trao đổi dữ liệu với nhiều thiết bị đầu cuối khác nhau, vì các thiết bị đầu cuối khác nhau có thể hỗ trợ các chế độ truyền dữ liệu khác nhau, thiết bị đầu cuối thứ nhất cần phát triển các giao diện truyền dữ liệu khác nhau cho các thiết bị đầu cuối khác nhau. Điều này không những sẽ tiêu tốn nguồn nhân lực nhiều hơn, mà còn chiếm quá nhiều tài nguyên lưu trữ. Sau đó nền tảng truyền dữ liệu có thể soạn thảo đặc tả được sử dụng trong khi truyền dữ liệu, và xác định giao diện truyền tiêu chuẩn được sử dụng trong khi truyền dữ liệu. Giao diện truyền tiêu chuẩn là giao diện phổ cập được sử dụng trong khi truyền dữ liệu giữa các thiết bị đầu cuối.

Miễn là thiết bị đầu cuối của người dùng thực hiện trao đổi dữ liệu thông qua nền tảng truyền dữ liệu triển khai giao diện truyền tiêu chuẩn, thiết bị đầu cuối có thể truyền dữ liệu đến thiết bị đầu cuối bất kỳ để triển khai giao diện chuẩn. Theo giao diện truyền tiêu chuẩn được xác định bởi nền tảng truyền dữ liệu, ví dụ, thông tin như giao thức truyền dữ liệu trong khi truyền dữ liệu giữa cả hai bên trao đổi dữ liệu có thể được xác định. Các chi tiết không được mô tả trong bản mô tả.

Chức năng của giao diện chuẩn được xác định cũng có thể bao gồm chức năng gửi trạng thái truyền dữ liệu đến nền tảng trao đổi dữ liệu. Theo cách này, sau khi kết thúc việc gửi dữ liệu được mã hóa, nền tảng tương tác dữ liệu có thể xác định rằng dữ liệu được mã hóa được gửi thành công đến thiết bị đầu cuối thứ hai, và sau đó hoạt động tương ứng được thực hiện.

Dựa trên phương án theo sáng chế, FIG.2 thể hiện sơ đồ giản lược của kịch bản thực hiện của phương pháp gửi dữ liệu. Sau khi cả hai bên đạt được thỏa thuận trao

đổi dữ liệu, quy trình cụ thể để truyền dữ liệu thứ nhất đến thiết bị đầu cuối thứ hai, bởi thiết bị đầu cuối thứ nhất như sau:

Bước 301: Thiết bị đầu cuối thứ nhất mã hóa dữ liệu thứ nhất để thu dữ liệu được mã hóa.

Bước 302: Thiết bị đầu cuối thứ nhất gửi dữ liệu được mã hóa đến thiết bị đầu cuối thứ hai thông qua giao diện truyền tiêu chuẩn được triển khai.

Rõ ràng, thiết bị đầu cuối thứ hai cũng triển khai giao diện truyền tiêu chuẩn.

Bước 303: Thiết bị đầu cuối thứ nhất gửi khóa đến nền tảng trao đổi dữ liệu.

Bước 304: Nền tảng trao đổi dữ liệu gửi khóa nhận được đến thiết bị đầu cuối thứ hai.

Bước 305: Thiết bị đầu cuối thứ hai giải mã dữ liệu được mã hóa theo khóa nhận được để thu dữ liệu thứ nhất.

Trong phương pháp gửi dữ liệu được đề xuất theo Phương án 1 của sáng chế, trong khi trao đổi dữ liệu, nền tảng trao đổi dữ liệu ghi thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai mà trao đổi dữ liệu trong chuỗi khối. Nền tảng trao đổi dữ liệu sau đó nhận khóa thứ nhất, được gửi bởi thiết bị đầu cuối thứ nhất tương ứng với người dùng thứ nhất, để giải mã dữ liệu thứ nhất được mã hóa. Thiết bị đầu cuối thứ nhất gửi dữ liệu thứ nhất được mã hóa đến thiết bị đầu cuối thứ hai tương ứng với người dùng thứ hai. Nền tảng trao đổi dữ liệu gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, và thiết bị đầu cuối thứ hai giải mã dữ liệu thứ nhất được mã hóa nhận được dựa trên khóa thứ nhất để thu dữ liệu thứ nhất. Hiển nhiên là nền tảng trao đổi dữ liệu giữ sạch dữ liệu thứ nhất được trao đổi trong quy trình trao đổi dữ liệu, nhờ đó tránh được nguy cơ mà dữ liệu thứ nhất có thể được sử dụng bởi nền tảng trao đổi dữ liệu cho các mục đích khác, tăng cường an ninh dữ liệu trong quy trình trao đổi dữ liệu, và cùng lúc với nền tảng trao đổi dữ liệu.

Cần lưu ý rằng, để dễ mô tả, việc thực hiện phương pháp gửi dữ liệu được đưa vào bằng cách sử dụng ví dụ trong đó phương pháp dữ liệu được thực hiện bởi nền tảng trao đổi dữ liệu. Có thể được hiểu rằng phương pháp được thực thi bởi nền tảng trao đổi dữ liệu là minh họa làm ví dụ, và không được hiểu là giới hạn đối với phương

pháp này. Tiếp theo, các bước của phương pháp được đề xuất trong Phương án 1 có thể được thực thi bởi cùng một thiết bị, hoặc phương pháp có thể được thực thi bởi các thiết bị khác nhau. Ví dụ, bước 101 và bước 102 có thể được thực thi bởi thiết bị 1; theo ví dụ khác, bước 101 có thể được thực thi bởi thiết bị 1, và bước 102 có thể được thực thi bởi thiết bị 2; và v.v.

Phương án 2

Khái niệm sáng chế theo sáng chế được mô tả dựa trên Phương án 1 nêu trên chi tiết. Để hiểu rõ hơn về các dấu hiệu, phương tiện và hiệu quả kỹ thuật theo sáng chế, phương pháp gửi dữ liệu theo sáng chế được minh họa thêm sau đây, nhờ đó tạo ra phương án khác theo sáng chế.

Quy trình trao đổi dữ liệu theo Phương án 2 của sáng chế tương tự với quy trình trao đổi dữ liệu theo Phương án 1, và đối với một số bước không được đưa vào trong Phương án 2, tham chiếu có thể được tạo ra trong phần mô tả liên quan theo Phương án 1. Các chi tiết không được mô tả lại trong bản mô tả này.

Trước khi việc thực hiện giải pháp được đưa vào chi tiết, kịch bản thực hiện của giải pháp này được đưa vào vắn tắt trước tiên.

Trên Internet, tiền hiện có trong dạng dữ liệu. Do đó, giá trị của dữ liệu biểu diễn tiền có thể là giá trị của tiền được biểu diễn bởi dữ liệu. Trên Internet, việc chuyển dữ liệu biểu diễn tiền luôn được được thực hiện, trong hoạt động thực, bằng cách thay đổi các giá trị số nhận dạng tiền, ví dụ, nếu 100 yuan được chuyển từ tài khoản A đến tài khoản B, việc chuyển dữ liệu thực tế là các thay đổi tương ứng đối với các giá trị số biểu diễn tiền trong tài khoản A và tài khoản B.

Như được mô tả theo Phương án 1, các giá trị dữ liệu của một số kiểu dữ liệu không thể đạt được qua sự sao chép, và dữ liệu như vậy có thể được truyền thông qua nền tảng. Do đó, theo Phương án 2, quy trình thực thi cụ thể của phương pháp gửi dữ liệu được đề xuất theo sáng chế được minh họa chi tiết bằng cách sử dụng ví dụ trong đó dữ liệu thứ ba là dữ liệu biểu diễn tiền. Để dễ mô tả, dữ liệu thứ ba để biểu diễn tiền được gọi tắt là tiền sau đây. Do đó, quy trình trao đổi dữ liệu có thể được hiểu là quy trình giao dịch dữ liệu, người dùng thứ nhất theo Phương án 1 là bên bán dữ liệu,

người dùng thứ hai là người mua dữ liệu, nền tảng trao đổi dữ liệu là nền tảng giao dịch dữ liệu có thể cung cấp dịch vụ giao dịch dữ liệu cho người dùng.

Dựa trên kịch bản nêu trên, quy trình thực thi giao dịch dữ liệu theo Phương án 2 được thể hiện trên FIG.3, bao gồm các bước sau đây:

Bước 401: Bên bán dữ liệu đưa ra thông tin dữ liệu để bán thông qua nền tảng giao dịch dữ liệu.

Nền tảng giao dịch dữ liệu có thể hỗ trợ người dùng có nhu cầu bán dữ liệu để đưa ra thông tin dữ liệu để bán, sao cho người dùng có nhu cầu tiêu thụ dữ liệu có thể tìm thấy thông tin được yêu cầu tại nền tảng giao dịch dữ liệu.

Bước 402: Bên tiêu thụ dữ liệu và bên bán dữ liệu đạt được thỏa thuận giao dịch dữ liệu.

Bên tiêu thụ dữ liệu có thể truyền thông về các chi tiết giao dịch cụ thể, và sau đó cuối cùng đạt được thỏa thuận giao dịch dữ liệu. Chức năng của thỏa thuận giao dịch dữ liệu tương tự với chức năng của thỏa thuận giao dịch dữ liệu được mô tả theo Phương án 1, và do đó không được mô tả chi tiết lại ở đây.

Bước 403: Nền tảng giao dịch dữ liệu ghi thỏa thuận giao dịch dữ liệu đạt được bởi cả hai bên trong chuỗi khối.

Ngay khi thỏa thuận giao dịch dữ liệu được ghi trong chuỗi khối, khả năng làm giả mạo thỏa thuận có thể được làm giảm đáng kể, và sự an toàn của thỏa thuận do đó được tăng cường.

Bước 404: Bên tiêu thụ dữ liệu thanh toán lượng tiền được đồng ý theo thỏa thuận với nền tảng này.

Trên Internet, việc chuyển tiền thực sự là việc chuyển dữ liệu biểu diễn tiền. Trong hoạt động thực, điều này luôn được thực thi bằng cách thay đổi các giá trị dữ liệu nhận dạng tiền trong các tài khoản.

Bước 405: Bên bán dữ liệu mã hóa dữ liệu để bán để thu dữ liệu được mã hóa, và sau đó gửi khóa cho việc mã hóa đến nền tảng giao dịch dữ liệu.

Dữ liệu có thể được mã hóa bằng cách sử dụng công nghệ mã hóa đối xứng, sao cho khóa để mã hóa giống với khóa để giải mã.

Cần lưu ý rằng phương án theo sáng chế không làm giới hạn thứ tự thực hiện bước 404 và bước 405.

Bước 406: Bên bán dữ liệu truyền dữ liệu được mã hóa đến thiết bị đầu cuối của bên tiêu thụ dữ liệu thông qua thiết bị đầu cuối để triển khai giao diện truyền tiêu chuẩn.

Như được mô tả theo Phương án 1, giao diện truyền tiêu chuẩn ở đây là giao diện phổ cập được xác định bởi nền tảng trao đổi dữ liệu và được sử dụng trong khi truyền dữ liệu giữa các thiết bị đầu cuối. Thiết bị đầu cuối của bên tiêu thụ dữ liệu cũng cần triển khai giao diện truyền tiêu chuẩn, để nhận dữ liệu. Theo cách này, khi bên tiêu thụ dữ liệu và bên bán dữ liệu cũng thực hiện trao đổi dữ liệu với người dùng khác của nền tảng, không cần phát triển các giao diện truyền khác, do đó tiết kiệm các nguồn nhân lực và các tài nguyên lưu trữ.

Bước 407: Nền tảng giao dịch dữ liệu xác định rằng dữ liệu được mã hóa được truyền đến thiết bị đầu cuối của bên tiêu thụ dữ liệu.

Phương pháp cụ thể để xác định rằng dữ liệu được mã hóa được truyền đến thiết bị đầu cuối của bên tiêu thụ dữ liệu tương tự với mô tả liên quan theo Phương án 1, và do đó không được mô tả lại chi tiết ở đây.

Bước 408: Nền tảng giao dịch dữ liệu gửi khóa đến bên tiêu thụ dữ liệu sau khi xác định rằng lượng tiền được thanh toán bởi bên tiêu thụ dữ liệu phù hợp với lượng tiền được ghi trong thỏa thuận.

Cần được lưu ý rằng phương án theo sáng chế không làm giới hạn thứ tự thực hiện bước 407 và bước 408.

Bước 409: Bên tiêu thụ dữ liệu giải mã dữ liệu được mã hóa bằng cách sử dụng khóa nhận được, và xác minh xem liệu dữ liệu được giải mã có phù hợp với mô tả trong thỏa thuận này hay không.

Bước 410: Bên tiêu thụ dữ liệu gửi lệnh xác nhận được tiếp nhận đến nền tảng giao dịch dữ liệu thông qua thiết bị đầu cuối sau khi xác định rằng dữ liệu nhận được phù hợp với mô tả trong thỏa thuận này.

Chức năng của lệnh xác nhận được tiếp nhận tương tự với chức năng của lệnh gửi dữ liệu thứ hai được mô tả theo Phương án 1, và do đó không được mô tả lại chi tiết ở đây.

Bước 411: Nền tảng giao dịch dữ liệu, sau khi nhận lệnh xác nhận được tiếp nhận, chuyển một lượng tiền được thanh toán bởi bên tiêu thụ dữ liệu vào tài khoản của bên bán dữ liệu.

Nếu bên bán dữ liệu và bên tiêu thụ dữ liệu tiếp theo có sự tranh chấp đối với dữ liệu trong giao dịch, họ có thể bảo vệ quyền lợi của họ theo thỏa thuận trong chuỗi khối.

Trong phương pháp giao dịch dữ liệu được đề xuất trong Phương án 2 theo sáng chế, nền tảng giao dịch dữ liệu nhận khóa được gửi bởi bên tiêu thụ và được sử dụng để mã hóa dữ liệu để bán, và sau đó gửi khóa đến thiết bị đầu cuối của bên tiêu thụ dữ liệu sau khi nhận tiền được thanh toán bởi bên tiêu thụ dữ liệu thông qua thiết bị đầu cuối. Theo cách này, sau khi nhận dữ liệu được mã hóa được gửi bởi bên bán dữ liệu, bên tiêu thụ dữ liệu có thể giải mã dữ liệu được mã hóa bằng cách sử dụng khóa để thu được dữ liệu được bán bởi bên bán dữ liệu. Do đó, trong quy trình giao dịch dữ liệu, nền tảng trao đổi dữ liệu giữ sạch cho dữ liệu được bán, nhờ đó tránh được nguy cơ mà dữ liệu được bán có thể được sử dụng bởi nền tảng trao đổi dữ liệu cho các mục đích khác, và tăng cường an ninh dữ liệu trong quy trình giao dịch dữ liệu.

Phương án 3

Để giải quyết vấn đề về an ninh dữ liệu thấp trong quy trình trao đổi dữ liệu hiện có, Phương án 1 theo sáng chế đề xuất thiết bị gửi dữ liệu. Sơ đồ cấu trúc giản lược của thiết bị gửi dữ liệu, như được thể hiện trên FIG.4, chủ yếu bao gồm các đơn vị chức năng sau đây:

bộ ghi 501 được tạo cấu hình để ghi thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối và lưu trữ thỏa thuận này;

bộ nhận thứ nhất 502 được tạo cấu hình để nhận khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa, thiết bị đầu cuối thứ nhất là thiết bị đầu cuối tương ứng với người dùng thứ nhất;

bộ gửi thứ nhất 503 được tạo cấu hình để gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, sao cho thiết bị đầu cuối thứ hai, sau khi nhận dữ liệu thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất, giải mã dữ liệu thứ nhất được mã hóa nhận được dựa trên khóa thứ nhất để thu dữ liệu thứ nhất, thiết bị đầu cuối thứ hai là thiết bị đầu cuối tương ứng với người dùng thứ hai.

Theo phương án của sáng chế, có nhiều phương án thực hiện cụ thể khác để trao đổi dữ liệu. Theo một phương án thực hiện, thiết bị còn bao gồm bộ nhận thứ ba 504 được tạo cấu hình để, trước khi bộ gửi thứ nhất 503 gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, nhận khóa thứ hai được gửi bởi thiết bị đầu cuối thứ hai và được sử dụng để giải mã dữ liệu thứ hai được mã hóa; và

bộ gửi thứ ba 505 được tạo cấu hình để gửi khóa thứ hai đến thiết bị đầu cuối thứ nhất sau khi bộ gửi thứ nhất 503 gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, sao cho thiết bị đầu cuối thứ nhất, sau khi nhận dữ liệu thứ hai được mã hóa được gửi bởi thiết bị đầu cuối thứ hai, giải mã dữ liệu thứ hai được mã hóa nhận được dựa trên khóa thứ hai để thu dữ liệu thứ hai.

Để đảm bảo cho lợi ích của người dùng thứ hai, theo một phương án thực hiện, thiết bị này còn bao gồm bộ nhận thứ tư 506 được tạo cấu hình để, sau khi bộ gửi thứ nhất 503 gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai và trước khi bộ gửi thứ ba 505 gửi khóa thứ hai đến thiết bị đầu cuối thứ nhất, nhận thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ hai đối với dữ liệu thứ nhất, thông tin xác nhận cho dữ liệu thứ nhất chỉ báo rằng người dùng thứ hai xác định rằng dữ liệu thứ nhất phù hợp với mô tả về thỏa thuận này.

Theo một phương án thực hiện, thiết bị còn bao gồm bộ nhận thứ năm 507 được tạo cấu hình để, sau khi bộ nhận thứ tư 506 nhận thông tin xác nhận được gửi

bởi thiết bị đầu cuối thứ hai đối với dữ liệu thứ nhất, nhận thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ nhất cho dữ liệu thứ hai, thông tin xác nhận cho dữ liệu thứ hai chỉ báo rằng người dùng thứ nhất xác định rằng dữ liệu thứ hai phù hợp với mô tả về thỏa thuận này.

Theo một phương án thực hiện, thiết bị còn bao gồm bộ ghi 508 được tạo cấu hình để, sau khi bộ nhận thứ năm 507 nhận thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ nhất cho dữ liệu thứ hai, ghi bản ghi mà sự trao đổi được hoàn thành trong kết quả của thỏa thuận trao đổi dữ liệu trong chuỗi khối và lưu trữ bản ghi này.

Để đảm bảo lợi ích của cả hai bên trong việc trao đổi dữ liệu, theo một phương án thực hiện, thiết bị còn bao gồm bộ nhận thứ hai 509 được tạo cấu hình để, trước khi bộ gửi thứ nhất 503 gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, nhận dữ liệu thứ ba được gửi bởi thiết bị đầu cuối thứ hai; và bộ gửi thứ hai 510 được tạo cấu hình để, sau khi bộ gửi thứ nhất 503 gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, gửi dữ liệu thứ ba đến người dùng thứ nhất khi được xác định rằng điều kiện thiết lập trước được thỏa mãn.

Theo một phương án thực hiện, việc xác định rằng điều kiện thiết lập trước được thỏa mãn bao gồm cụ thể: nhận, bởi nền tảng trao đổi dữ liệu, lệnh gửi dữ liệu được gửi bởi thiết bị đầu cuối thứ hai, lệnh gửi dữ liệu là lệnh để lệnh cho nền tảng trao đổi dữ liệu để gửi dữ liệu thứ ba đến thiết bị đầu cuối thứ nhất.

Theo một phương án thực hiện, thỏa thuận trao đổi dữ liệu bao gồm thông tin dấu hiệu về dữ liệu thứ nhất.

Thông tin dấu hiệu của dữ liệu thứ nhất bao gồm ít nhất một trong số sau: tóm lược tin báo để xác minh tính toàn vẹn của dữ liệu thứ nhất; và thông tin đường cơ sở để tóm lược nội dung cụ thể của dữ liệu thứ nhất.

Để tránh tiêu thụ nhiều nguồn nhân lực hơn trong sự phát triển giao diện, theo một phương án thực hiện, dữ liệu thứ nhất được mã hóa được truyền đến thiết bị đầu cuối thứ hai thông qua thiết bị đầu cuối thứ nhất để triển khai giao diện truyền tiêu chuẩn. Giao diện truyền tiêu chuẩn là giao diện phổ cập được xác định bởi nền tảng trao đổi dữ liệu và được sử dụng trong khi truyền dữ liệu giữa các thiết bị đầu cuối.

Trong thiết bị gửi dữ liệu được đề xuất trong Phương án 3 theo sáng chế, trong khi trao đổi dữ liệu, nền tảng trao đổi dữ liệu ghi thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai mà trao đổi dữ liệu trong chuỗi khối. Nền tảng trao đổi dữ liệu sau đó nhận khóa thứ nhất, được gửi bởi thiết bị đầu cuối thứ nhất tương ứng với người dùng thứ nhất, để giải mã dữ liệu thứ nhất được mã hóa. Thiết bị đầu cuối thứ nhất gửi dữ liệu thứ nhất được mã hóa đến thiết bị đầu cuối thứ hai tương ứng với người dùng thứ hai. Nền tảng trao đổi dữ liệu gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, và thiết bị đầu cuối thứ hai giải mã dữ liệu thứ nhất được mã hóa thu được dựa trên khóa thứ nhất để thu dữ liệu thứ nhất. Rõ ràng là nền tảng trao đổi dữ liệu giữ sạch dữ liệu thứ nhất được trao đổi trong quy trình trao đổi dữ liệu, nhờ đó tránh nguy cơ là dữ liệu thứ nhất có thể được sử dụng bởi nền tảng trao đổi dữ liệu cho các mục đích khác, tăng cường an ninh dữ liệu trong quy trình trao đổi dữ liệu, và cùng lúc với nền tảng trao đổi dữ liệu.

Trong những năm 1990, sự cải tiến của công nghệ có thể được phân biệt rõ ràng dưới dạng sự cải tiến phần cứng (ví dụ, sự cải tiến về cấu trúc mạch như điôt, tranzito, hoặc bộ chuyển mạch) hoặc sự cải tiến phần mềm (sự cải tiến về thủ tục phương pháp). Tuy nhiên, với sự phát triển của các công nghệ, sự cải tiến về các thủ tục phương pháp hiện tại có thể được xét đến là sự cải tiến trực tiếp của cấu trúc mạch phần cứng. Hầu hết các nhà thiết kế đều lập trình các thủ tục phương pháp được cải tiến trong các mạch phần cứng, để thu được cấu trúc mạch phần cứng tương ứng. Do đó, không thích hợp để cho rằng sự cải tiến của thủ tục phương pháp không thể được thực thi bằng cách 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 mà chức năng logic của thiết bị logic lập trình được được xác định bởi các thiết bị được lập trình được bởi người dùng. Các nhà thiết kế tự lập trình để "tích hợp" hệ thống kỹ thuật số trong một phần của PLD mà không cần yêu cầu nhà sản xuất chip thiết kế và sản xuất chip mạch tích hợp chuyên dụng. Ngoài ra, hiện nay, thay cho việc sản xuất thủ công chip mạch tích hợp, việc lập trình hầu hết được thực thi bằng cách sử dụng phần mềm biên dịch logic. Phần mềm biên dịch logic này tương tự với bộ biên dịch phần mềm được sử dụng cho việc phát triển và ghi chương trình, và mã ban đầu trước khi biên dịch cũng

cần được ghi bằng cách 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 như ngôn ngữ biểu diễn Boolean cải tiến (Advanced Boolean Expression Language - ABEL), ngôn ngữ mô tả phần cứng Altera (Altera Hardware Description Language - AHDL), sự hợp lưu, ngôn ngữ lập trình 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 được sử dụng phổ biến nhất hiện nay. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cũng cần biết rằng mạch phần cứng thực hiện thủ tục phương pháp logic có thể dễ dàng đạt được bằng cách lập trình logic thủ tục phương pháp sử dụng các ngôn ngữ mô tả phần cứng trên và lập trình nó trong mạch tích hợp.

Bộ điều khiển có thể được lắp đặt theo cách thức 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 vật ghi đọc được bằng máy tính lưu trữ mã chương trình đọc được bằng máy tính (như phần mềm hoặc phần sụn) có thể được chạy bởi bộ vi xử lý hoặc bộ xử lý, cổng logic, bộ chuyển mạch, mạch tích hợp chuyên dụng (ASIC), bộ điều khiển logic lập trình được, hoặc bộ vi điều khiển cài sẵn. Các ví dụ về bộ điều khiển bao gồm nhưng không bị giới hạn với các bộ vi điều khiển sau đây: ARC 625D, Atmel AT91SAM, vi chip PIC18F26K20, và Silicone Labs C8051F320. Bộ điều khiển của bộ nhớ cũng có thể được vận hành với vai trò là một phần của mạch logic điều khiển của bộ nhớ. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cũng biết rằng bộ điều khiển có thể được thực hiện bằng cách sử dụng mã chương trình đọc được bằng máy tính thuần túy, và ngoài ra, các bước của phương pháp có thể được lập trình logic để cho phép bộ điều khiển thực hiện cùng một chức năng trong dạng của cổng logic, bộ chuyển mạch, mạch tích hợp chuyên dụng, bộ điều khiển logic lập trình được, bộ vi điều khiển cài sẵn, và tương tự. Do đó, loại bộ điều khiển này có thể được xét là thành phần phần cứng, và các thiết bị được bao gồm trong bộ điều khiển này để thực hiện các chức năng khác nhau cũng có thể được xét đến là các cấu trúc bên trong thành phần phần

cứng. Hoặc, các thiết bị được sử dụng để thực hiện các chức năng khác nhau có thể được xét đến dưới dạng cả môđun phần mềm để thực hiện phương pháp và các cấu trúc bên trong thành phần phần cứng.

Hệ thống, thiết bị, môđun, hoặc bộ phận được minh họa theo các phương án nêu trên có thể được thực hiện cụ thể bằng cách sử dụng chip máy tính hoặc thực thể, hoặc sản phẩm có chức năng nhất định. Thiết bị vận hành điển hình là máy tính. Cụ thể, máy tính có thể là, ví dụ, máy tính cá nhân, máy tính xách tay, điện thoại di động, điện thoại camera, điện thoại thông minh, thiết bị hỗ trợ số cá nhân, máy phát phương tiện, thiết bị định vị, thiết bị thư điện tử, bàn giao tiếp trò chơi, máy tính bảng, hoặc thiết bị đeo vào được, hoặc kết hợp của thiết bị bất kỳ trong số các thiết bị này.

Để dễ mô tả, khi thiết bị được mô tả, nó được phân chia thành các đơn vị khác nhau theo các chức năng đối với mô tả tương ứng. Hiển nhiên, khi sáng chế được thực hiện, các chức năng của các đơn vị có thể được thực hiện trong cùng một phần hoặc nhiều phần của phần mềm và/hoặc phần cứng.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cần hiểu rằng các phương án của sáng chế có thể được đề xuất dưới dạng phương pháp, hệ thống, hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể được thực hiện dưới dạng của phương án thực hiện hoàn toàn trên phần cứng, phương án thực hiện hoàn toàn trên phần mềm, hoặc phương án kết hợp của phần mềm và phần cứng. Ngoài ra, sáng chế có thể là sản phẩm chương trình máy tính được thực thi trên một hoặc nhiều vật ghi lưu trữ sử dụng được bằng máy tính (bao gồm nhưng không bị giới hạn với bộ nhớ đĩa từ, CD-ROM, bộ nhớ quang học, và tương tự) bao gồm 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 theo các phương án của sáng chế. Cần hiểu rằng lệnh chương trình máy tính có thể được sử dụng để thực hiện mỗi quy trình và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối và kết hợp của các quy trình và/hoặc các khối trong các lưu đồ và/hoặc các sơ đồ khối. Các lệnh chương trình máy tính này có thể được cung cấp cho máy tính đa dụng, máy tính chuyên dụng, bộ xử lý cài sẵn, hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình

được khác bất kỳ để tạo ra máy, để các lệnh được chạy bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác bất kỳ tạo ra thiết bị để thực hiện chức năng riêng trong một hoặc nhiều quy trình trong các lưu đồ hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này cũng có thể được lưu trữ trong bộ nhớ đọc được bằng máy tính có thể lệnh cho máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác bất kỳ để làm việc theo cách thức cụ thể, để các lệnh được lưu trữ trong bộ nhớ đọc được bằng máy tính tạo ra thành phần lạ bao gồm thiết bị lệnh. Thiết bị lệnh thực hiện chức năng riêng 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, để chuỗi của các bước thao tác được thực hiện trên máy tính hoặc thiết bị lập trình được khác, nhờ đó tạo ra xử lý được thực hiện bằng máy tính. Do đó, các lệnh được chạy trên máy tính hoặc thiết bị lập trình được khác đề xuất các bước thực hiện chức năng riêng 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 điển hình, thiết bị điện toán bao gồm một hoặc nhiều bộ xử lý trung tâm (CPU), giao diện đầu vào/đầu ra, giao diện mạng, và bộ nhớ.

Bộ nhớ có thể bao gồm các vật ghi đọc được bằng máy tính như bộ nhớ khả biến, bộ nhớ truy cập ngẫu nhiên (random access memory - RAM) và/hoặc bộ nhớ không khả biến, ví dụ, bộ nhớ chỉ đọc (read-only memory - ROM) hoặc RAM chớp. Bộ nhớ là một ví dụ về vật ghi đọc được bằng máy tính.

Vật ghi đọc được bằng máy tính bao gồm các vật ghi không khả biến và khả biến cũng như các vật ghi tháo rời được và không tháo rời được, và có thể thực hiện lưu trữ thông tin bằng phương tiện của phương pháp hoặc công nghệ bất kỳ. Thông tin có thể là lệnh đọc được bằng máy tính, cấu trúc dữ liệu, và môđun của chương trình, hoặc dữ liệu khác. Vật ghi lưu trữ của máy tính bao gồm, ví dụ, nhưng không bị giới hạn với bộ nhớ chuyển pha (PRAM), bộ nhớ truy cập ngẫu nhiên tĩnh (SRAM - Static Random Access Memory), bộ nhớ truy cập ngẫu nhiên động (DRAM - Dynamic Random Access Memory), các loại RAM khác, ROM, bộ nhớ chỉ đọc lập trình được

xóa được bằng tín hiệu điện (EEPROM - Electrically Erasable Programmable Read-Only Memory), bộ nhớ chớp hoặc các công nghệ bộ nhớ khác, bộ nhớ chỉ đọc được bằng đĩa nén (compact disc read-only memory - CD-ROM), đĩa đa năng số (digital versatile disc - DVD) hoặc các đĩa lưu quang khác, băng cassette, băng lưu trữ từ tính/đĩa lưu trữ từ tính hoặc các thiết bị lưu trữ từ tính khác, hoặc vật ghi không truyền khác bất kỳ, và có thể được sử dụng để lưu trữ thông tin được truy cập bởi thiết bị điện toán. Theo định nghĩa trong bản mô tả này, vật ghi đọc được bằng máy tính không bao gồm các vật ghi tạm thời, như tín hiệu dữ liệu điều biến và sóng mang.

Cũng lưu ý rằng thuật ngữ "bao gồm", "chứa", hoặc các biến thể khác bất kỳ được dự tính để bao hàm sự bao gồm không loại trừ, để quy trình, phương pháp, hàng hóa, hoặc thiết bị bao gồm chuỗi của các phần tử không những bao gồm các phần tử mà còn bao gồm các yếu tố khác không được liệt kê rõ ràng, hoặc còn bao gồm các yếu tố vốn có của quy trình, phương pháp, hàng hóa, hoặc thiết bị. Trong trường hợp không có giới hạn thêm bất kỳ, yếu tố được định nghĩa bởi "bao gồm ..." không loại trừ quy trình, phương pháp, hàng hóa, hoặc thiết bị bao gồm phần tử này cũng có các phần tử tương tự khác.

Sáng chế có thể được mô tả trong ngữ cảnh chung của lệnh chạy được bằng máy tính được chạy bằng máy tính, ví dụ, môđun chương trình. Nói chung, môđun chương trình bao gồm đoạn chương trình, chương trình, đối tượng, thành phần, cấu trúc dữ liệu, và tương tự được sử dụng để thực thi tác vụ cụ thể hoặc thực thi kiểu dữ liệu trừu tượng xác định. Sáng chế cũng có thể được thực thi trong các môi trường điện toán phân tán, trong các môi trường điện toán phân tán này, tác vụ được thực hiện bằng cách sử dụng các thiết bị xử lý từ xa được kết nối qua mạng truyền thông. Trong môi trường điện toán phân tán này, môđun chương trình có thể được định vị trong các vật ghi lưu trữ bằng máy tính cục bộ và từ xa bao gồm thiết bị lưu trữ.

Các phương án trong bản mô tả này được mô tả theo cách tiến triển, các phần giống hoặc tương tự của các phương án có thể đạt được với tham chiếu lẫn nhau, và mỗi phương án nhấn mạnh vào phần khác với các phương án khác. Cụ thể, phương án về hệ thống về cơ bản tương tự với phương án về phương pháp, để dễ mô tả, đối với

các phần liên quan, tham chiếu có thể được tạo ra đối với mô tả về các phần trong phương án của phương pháp.

Phần mô tả nêu trên chỉ là các phương án của sáng chế, và không nhằm giới hạn sáng chế. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này có thể tạo ra các sửa đổi và thay đổi khác nhau cho sáng chế. Bất kỳ sửa đổi, thay thế tương đương, cải tiến hoặc tương tự được tạo ra không vượt ra ngoài nguyên lý của sáng chế sẽ nằm trong phạm vi của yêu cầu bảo hộ của sáng chế.

FIG.5 là lưu đồ minh họa ví dụ khác của phương pháp được thực hiện bằng máy tính 500 đối với các giao dịch dữ liệu an toàn, theo một phương án của sáng chế. Để dễ trình bày, mô tả sau đây mô tả tổng quát phương pháp 500 trong ngữ cảnh của các hình vẽ khác trong phần mô tả này. Tuy nhiên, cần hiểu rằng phương pháp 500 có thể được thực hiện, ví dụ, bởi hệ thống, môi trường, phần mềm, và phần cứng bất kỳ, hoặc kết hợp của 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 500 có thể thực hiện song song, trong kết hợp, trong các vòng lặp hoặc theo thứ tự bất kỳ. Theo một số phương án thực hiện, phương pháp 500 có thể bao gồm các bước bổ sung hoặc khác nhau (hoặc kết hợp của cả hai) không được thể hiện trong lưu đồ. Theo một số phương án thực hiện, các bước cũng có thể được lược bỏ từ phương pháp 500.

Tại bước 510, thỏa thuận trao đổi dữ liệu giữa người dùng thứ nhất và người dùng thứ hai được ghi, bởi nền tảng trao đổi dữ liệu, trong chuỗi khối. Thỏa thuận trao đổi dữ liệu được liên kết với dữ liệu thứ nhất. Ví dụ, dữ liệu thứ nhất là dữ liệu được chuyển từ người dùng thứ nhất đến người dùng thứ hai theo thỏa thuận trao đổi dữ liệu. Theo một số phương án thực hiện, nền tảng trao đổi dữ liệu lưu trữ thỏa thuận trao đổi dữ liệu. Thỏa thuận trao đổi dữ liệu bao gồm một hoặc nhiều thông tin nhận dạng của người dùng thứ nhất và thứ hai, thông tin đặc tính của dữ liệu được trao đổi, các đặc tả sử dụng dữ liệu được tuân theo bởi người dùng thứ nhất và thứ hai, và hình phạt, được tuân theo bởi người dùng thứ nhất và thứ hai, để vi phạm thỏa thuận, và thông tin khác được liên kết với dữ liệu được trao đổi.

Theo một số phương án thực hiện, trước khi ghi thỏa thuận trao đổi dữ liệu trong chuỗi khối, thông tin dữ liệu được liên kết với dữ liệu thứ nhất được nhận, bởi

nền tảng trao đổi dữ liệu và từ thiết bị thứ nhất được liên kết với người dùng thứ nhất, để công bố trên nền tảng trao đổi dữ liệu. Sau đó thông tin dữ liệu được liên kết với dữ liệu thứ nhất được công bố bởi nền tảng trao đổi dữ liệu. Lệnh được liên kết với dữ liệu thứ nhất nhận được bởi nền tảng trao đổi dữ liệu và từ thiết bị thứ hai được liên kết với người dùng thứ hai. Lệnh được liên kết với dữ liệu thứ nhất được truyền bởi nền tảng trao đổi dữ liệu đến thiết bị thứ nhất. Thông tin xác nhận đối với lệnh được liên kết với dữ liệu thứ nhất nhận được bởi nền tảng trao đổi dữ liệu và từ thiết bị thứ nhất. Cả lệnh và thông tin xác nhận được liên kết với thỏa thuận trao đổi dữ liệu. Theo một số phương án thực hiện, thỏa thuận trao đổi dữ liệu có thể đạt được sử dụng các phương pháp thích hợp khác. Từ bước 510, phương pháp 500 tiến hành đến bước 520.

Tại bước 520, khóa thứ nhất được nhận bởi nền tảng trao đổi dữ liệu và từ thiết bị thứ nhất được liên kết với người dùng thứ nhất. Khóa thứ nhất được sử dụng để giải mã dữ liệu thứ nhất được mã hóa. Ví dụ, thiết bị thứ nhất mã hóa dữ liệu thứ nhất để thu được dữ liệu thứ nhất được mã hóa. Từ bước 520, phương pháp 500 tiến hành đến bước 530.

Tại bước 530, khóa thứ nhất được nhận được truyền bởi nền tảng trao đổi dữ liệu đến thiết bị thứ hai được liên kết với người dùng thứ hai. Theo một số phương án thực hiện, trước khi truyền khóa thứ nhất được nhận, khóa thứ hai được nhận bởi nền tảng trao đổi dữ liệu và từ thiết bị thứ hai được liên kết với người dùng thứ hai. Khóa thứ hai được sử dụng để giải mã dữ liệu thứ hai được mã hóa, và dữ liệu thứ hai được liên kết với thỏa thuận trao đổi dữ liệu. Ví dụ, dữ liệu thứ hai là dữ liệu được chuyển từ người dùng thứ hai đến người dùng thứ nhất theo thỏa thuận trao đổi dữ liệu. Sau khi truyền khóa thứ nhất được nhận, khóa thứ hai được nhận được truyền bởi nền tảng trao đổi dữ liệu đến thiết bị thứ nhất được liên kết với người dùng thứ nhất. Thiết bị thứ nhất giải mã dữ liệu thứ hai được mã hóa, nhận được từ thiết bị thứ hai, dựa trên khóa thứ hai để thu dữ liệu thứ hai. Từ bước 530, phương pháp 500 tiến hành đến bước 540.

Tại bước 540, dữ liệu thứ nhất được mã hóa được truyền bởi thiết bị thứ nhất đến thiết bị thứ hai, không đi qua nền tảng trao đổi dữ liệu. Theo một số phương án thực hiện, thay cho việc truyền dữ liệu thứ nhất được mã hóa qua nền tảng trao đổi dữ

liệu, thiết bị thứ nhất truyền dữ liệu thứ nhất được mã hóa một cách trực tiếp đến thiết bị thứ hai để tránh cho nền tảng trao đổi dữ liệu sử dụng dữ liệu thứ nhất được mã hóa cho các mục đích khác (ví dụ, các hoạt động không được xác định trong thỏa thuận trao đổi dữ liệu giữa người dùng thứ nhất và người dùng thứ hai), hoặc thực hiện các thay đổi không được ủy quyền đối với dữ liệu thứ nhất được mã hóa trước khi truyền đến thiết bị thứ hai. Theo một số phương án thực hiện, dữ liệu thứ nhất được mã hóa được truyền đến thiết bị thứ hai qua giao diện truyền tiêu chuẩn của thiết bị thứ nhất. Giao diện truyền tiêu chuẩn là giao diện phổ cập được xác định bởi nền tảng trao đổi dữ liệu và được sử dụng để truyền dữ liệu giữa các thiết bị khác nhau. Từ bước 540, phương pháp 500 tiến hành đến bước 550.

Tại bước 550, dữ liệu thứ nhất được mã hóa được giải mã, bởi thiết bị thứ hai, dựa trên khóa thứ nhất để thu dữ liệu thứ nhất. Theo một số phương án thực hiện, sau khi truyền khóa thứ nhất được nhận và trước khi truyền khóa thứ hai được nhận, thông tin xác nhận cho dữ liệu thứ nhất nhận được bởi nền tảng trao đổi dữ liệu và từ thiết bị thứ hai được liên kết với người dùng thứ hai. Thông tin xác nhận cho dữ liệu thứ nhất chỉ báo rằng người dùng thứ hai xác định rằng dữ liệu thứ nhất thu được phù hợp với thỏa thuận trao đổi dữ liệu.

Theo một số phương án thực hiện, sau khi nhận thông tin xác nhận cho dữ liệu thứ nhất, thông tin xác nhận cho dữ liệu thứ hai nhận được bởi nền tảng trao đổi dữ liệu và từ thiết bị thứ nhất được liên kết với người dùng thứ nhất. Thông tin xác nhận cho dữ liệu thứ hai chỉ báo rằng người dùng thứ nhất xác định rằng dữ liệu thứ hai thu được phù hợp với thỏa thuận trao đổi dữ liệu. Bản ghi, chỉ báo rằng trao đổi dữ liệu giữa người dùng thứ nhất và người dùng thứ hai được hoàn thiện theo thỏa thuận trao đổi dữ liệu, được ghi bởi nền tảng trao đổi dữ liệu trong chuỗi khối. Bản ghi được lưu trữ bởi nền tảng trao đổi dữ liệu.

Theo một số phương án thực hiện, trước khi truyền khóa thứ nhất được nhận, dữ liệu thứ ba được nhận bởi nền tảng trao đổi dữ liệu và từ thiết bị thứ hai được liên kết với người dùng thứ hai. Dữ liệu thứ ba được liên kết với thỏa thuận trao đổi dữ liệu. Ví dụ, dữ liệu thứ ba là dữ liệu mà có thể được trao đổi qua nền tảng trao đổi dữ liệu. Sau khi truyền khóa thứ nhất được nhận, dữ liệu thứ ba được nhận được truyền

bởi nền tảng trao đổi dữ liệu đến thiết bị thứ nhất được liên kết với người dùng thứ nhất khi điều kiện định trước được thỏa mãn. Theo một số phương án thực hiện, điều kiện định trước bao gồm nền tảng trao đổi dữ liệu nhận lệnh từ thiết bị thứ hai. Lệnh này là lệnh để lệnh cho nền tảng trao đổi dữ liệu truyền dữ liệu thứ ba được nhận đến thiết bị thứ nhất.

Theo một số phương án thực hiện, thỏa thuận trao đổi dữ liệu bao gồm thông tin đặc tính của dữ liệu thứ nhất. Thông tin đặc tính của dữ liệu thứ nhất đạt được bởi thiết bị thứ hai. Thông tin đặc tính của dữ liệu thứ nhất bao gồm ít nhất một trong số tóm lược tin báo để xác thực tính toàn vẹn của dữ liệu thứ nhất, và thông tin đường cơ sở để tóm tắt nội dung cụ thể của dữ liệu thứ nhất. Việc xác định được thực hiện, bởi thiết bị thứ hai, liệu dữ liệu thứ nhất thu được có phù hợp với thỏa thuận trao đổi dữ liệu hay không dựa trên thông tin đặc tính thu được của dữ liệu thứ nhất. Nếu được xác định rằng dữ liệu thứ nhất thu được phù hợp với thỏa thuận trao đổi dữ liệu dựa trên thông tin đặc tính thu được của dữ liệu thứ nhất, thiết bị thứ hai truyền thông tin xác nhận đối với dữ liệu thứ nhất đến nền tảng trao đổi dữ liệu. Nếu được xác định rằng dữ liệu thứ nhất thu được không phù hợp với thỏa thuận trao đổi dữ liệu dựa trên thông tin đặc tính thu được của dữ liệu thứ nhất, thiết bị thứ hai sẽ không truyền thông tin xác nhận cho dữ liệu thứ nhất đến nền tảng trao đổi dữ liệu. Sau bước 550, phương pháp 500 dừng lại.

Các phương án thực hiện của đối tượng và các hoạt động chức năng được mô tả trong bản mô tả này có thể được thực thi trong hệ mạch điện tử kỹ thuật số, trong phần mềm hoặc phần sụn máy tính được biểu hiện hữu hình, trong phần cứng máy tính, bao gồm các cấu trúc được bộc lộ trong bản mô tả này và các dạng tương đương cấu trúc của chúng, hoặc trong các sự kết hợp một hoặc nhiều trong số chúng. Các phương án thực hiện trên phần mềm của đối tượng được mô tả có thể được thực thi dưới dạng một hoặc nhiều chương trình máy tính, tức là, một hoặc nhiều môđun của các lệnh chương trình máy tính được mã hóa trên vật ghi hữu hình, không khả biến, đọc được bằng máy tính lưu trữ bằng máy tính để thực thi bởi, hoặc để điều khiển hoạt động của, máy tính hoặc hệ thống được chạy bằng máy tính. Theo cách khác hoặc ngoài ra, các lệnh chương trình có thể được mã hóa trong/trên tín hiệu lan truyền được

tạo ra nhân tạo, ví dụ, tín hiệu điện từ, quang học, hoặc điện được tạo ra bằng máy mà được tạo ra để mã hóa thông tin để truyền đến thiết bị thu để thực thi bởi máy tính hoặc hệ thống được thực hiện bằng máy tính. Vật ghi lưu trữ bằng máy tính có thể là thiết bị lưu trữ đọc được bằng máy, nền lưu trữ đọc được bằng máy, thiết bị nhớ truy cập ngẫu nhiên hoặc nối tiếp, hoặc kết hợp của các vật ghi lưu trữ bằng máy tính. Việc tạo cấu hình một hoặc nhiều máy tính có nghĩa là một hoặc nhiều máy tính đã cài đặt phần cứng, phần sụn, hoặc phần mềm (hoặc các kết hợp của phần cứng, phần sụn, và phần mềm) sao cho khi phần mềm được thực thi bởi một hoặc nhiều máy tính, thì các hoạt động tính toán cụ thể được thực hiện.

Thuật ngữ "thời gian thực", ("real-time", "real time", hoặc "realtime",) "thời gian (nhanh) thực (RFT - Real (Fast) Time)", "thời gian gần như thực (NRT - Near(ly) Real-Time)", "thời gian tựa như thực", hoặc các thuật ngữ tương tự (như được hiểu bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật này), có nghĩa là thao tác và phản hồi là gần đúng theo thời gian sao cho cá nhân nhận thấy thao tác và phản hồi này xảy ra gần như đồng thời. Ví dụ, chênh lệch thời gian đối với phản hồi để hiển thị (hoặc đối với việc khởi động hiển thị) dữ liệu theo sau thao tác của cá nhân để truy cập dữ liệu có thể nhỏ hơn 1 mili giây (ms), nhỏ hơn 1 giây (s), hoặc nhỏ hơn 5s. Mặc dù dữ liệu được yêu cầu không cần được hiển thị (hoặc được khởi tạo để hiển thị) ngay lập tức, nhưng nó được hiển thị (hoặc được khởi tạo để hiển thị) mà không có bất kỳ độ trễ cố ý nào, tính đến các giới hạn xử lý của hệ thống điện toán được mô tả và thời gian được yêu cầu để, ví dụ, thu thập, đo lường chính xác, phân tích, xử lý, lưu trữ hoặc truyền dữ liệu.

Các thuật ngữ "thiết bị xử lý dữ liệu", "máy tính", hoặc "thiết bị điện toán điện tử" (hoặc thuật ngữ tương đương như được hiểu bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật này) đề cập đến phần cứng xử lý dữ liệu và bao gồm tất cả các loại của thiết bị, bộ phận, và máy để xử lý dữ liệu, bao gồm bằng cách lấy ví dụ, bộ xử lý lập trình được, máy tính, hoặc nhiều bộ xử lý hoặc máy tính. Máy tính cũng có thể là, hoặc còn bao gồm hệ mạch logic chuyên dụng, ví dụ, bộ xử lý trung tâm (CPU - Central Processing Unit), mảng cổng lập trình được dạng trường (FPGA - Field Programmable Gate Array), hoặc mạch tích hợp chuyên dụng (ASIC – Application-

Specific Integrated Circuit). Theo một số phương án thực hiện, máy tính hoặc hệ thống được thực hiện bằng máy tính hoặc hệ mạch logic chuyên dụng (hoặc kết hợp của máy tính hoặc hệ thống được thực hiện bằng máy tính và hệ mạch logic chuyên dụng) có thể là dựa trên phần cứng hoặc phần mềm (hoặc kết hợp dựa trên cả phần cứng và phần mềm). Máy tính có thể bao gồm mã một cách tùy chọn mà tạo ra môi trường thực thi cho các chương trình máy tính, ví dụ, mã cấu thành phần sụn của bộ xử lý, chồng giao thức, hệ thống quản lý cơ sở dữ liệu, hệ điều hành, hoặc kết hợp của các môi trường thực thi. Sáng chế dự tính sử dụng máy tính hoặc hệ thống được thực hiện bằng máy tính với hệ điều hành của một số loại, ví dụ, LINUX, UNIX, WINDOWS, MAC OS, ANDROID, IOS, hệ điều hành khác, hoặc kết hợp của các hệ điều hành

Chương trình máy tính, cũng có thể được gọi là hoặc được mô tả là chương trình, phần mềm, ứng dụng phần mềm, bộ phận, môđun, môđun phần mềm, bản thảo, mã, hoặc bộ phận khác có thể được ghi dưới dạng bất kỳ của ngôn ngữ lập trình, bao gồm các ngôn ngữ biên dịch hoặc thông dịch, hoặc các ngôn ngữ khai báo hoặc thủ tục, và có thể được triển khai dưới dạng bất kỳ, bao gồm, ví dụ, dưới dạng chương trình, môđun, bộ phận, hoặc chương trình con độc lập, để sử dụng trong môi trường điện toán. Chương trình máy tính có thể, nhưng không cần, tương ứng với tệp tin trong hệ thống tệp tin. Chương trình có thể được lưu trữ trong một phần của tệp tin mà chứa các chương trình hoặc dữ liệu khác, ví dụ, một hoặc nhiều bản thảo được lưu trữ trong tài liệu ngôn ngữ đánh dấu, trong tệp tin đơn dành riêng cho chương trình đang đề cập, hoặc trong nhiều tệp tin phối hợp, ví dụ, các tệp tin mà lưu trữ một hoặc nhiều môđun, chương trình con, hoặc các đoạn mã. Chương trình máy tính có thể được triển khai để được thực thi trên một máy tính hoặc trên nhiều máy tính mà được định vị trên một vị trí hoặc được phân bố trên nhiều vị trí và được kết nối bởi mạng truyền thông.

Mặc dù các phần của các chương trình được minh họa trong các hình vẽ khác nhau có thể được minh họa là các bộ phận riêng biệt, chẳng hạn như các bộ phận hoặc các môđun, mà thực hiện các dấu hiệu và chức năng được mô tả sử dụng các đối tượng khác nhau, các phương pháp, hoặc các quy trình khác, thay cho việc các chương trình có thể bao gồm số lượng các bộ phận phụ, các môđun phụ, các dịch vụ bên thứ

ba, các thành phần, các thư viện, và các bộ phận khác, khi thích hợp. Ngược lại, các dấu hiệu và chức năng của các thành phần khác nhau có thể được kết hợp thành các thành phần đơn lẻ, khi thích hợp. Các ngưỡng được sử dụng để thực hiện các phép xác định tính toán có thể được xác định tĩnh, động hoặc cả tĩnh và động.

Các phương pháp, các quy trình, hoặc các lưu đồ logic được mô tả biểu diễn một hoặc nhiều ví dụ về chức năng thích hợp với sáng chế và không nhằm để giới hạn sáng chế ở các phương án thực hiện được mô tả hoặc được minh họa, mà được quy định phạm vi rộng nhất phù hợp với các nguyên lý và các dấu hiệu được mô tả. Các phương pháp, các quy trình, hoặc các lưu đồ logic được mô tả có thể được thực hiện bởi một hoặc nhiều máy tính lập trình được thực thi một hoặc nhiều chương trình máy tính để thực hiện các chức năng bằng cách hoạt động trên dữ liệu đầu vào và tạo ra dữ liệu đầu ra. Các phương pháp, các quy trình, hoặc các lưu đồ logic cũng có thể được thực thi bởi, và máy tính cũng có thể được thực thi dưới dạng, hệ mạch logic chuyên dụng, ví dụ, CPU, FPGA, hoặc ASIC.

Các máy tính để thực thi chương trình máy tính có thể dựa trên các bộ vi xử lý đa dụng hoặc chuyên dụng, cả hai, hoặc loại CPU khác. Nói chung, CPU sẽ nhận các lệnh và dữ liệu từ và ghi vào bộ nhớ. Các phần tử cần thiết của máy tính là CPU, để thực hiện hoặc thực thi các lệnh, và một hoặc nhiều thiết bị bộ nhớ để lưu trữ các lệnh và dữ liệu. Nói chung, máy tính cũng sẽ bao gồm, hoặc được ghép nối hoạt động để, nhận dữ liệu từ hoặc chuyển dữ liệu tới, hoặc cả hai, một hoặc nhiều thiết bị lưu trữ dung lượng lớn để lưu trữ dữ liệu, ví dụ, các đĩa từ, quang từ, hoặc các đĩa quang học. Tuy nhiên, máy tính không cần có các thiết bị như vậy. Ngoài ra, máy tính có thể được cài sẵn trong thiết bị khác, ví dụ, điện thoại di động, thiết bị hỗ trợ cá nhân kỹ thuật số (PDA - Personal Digital Assistant), máy phát viđeo hoặc máy phát audio di động, bàn giao tiếp trò chơi, bộ thu hệ thống định vị toàn cầu (GPS - Global Positioning System), hoặc thiết bị lưu trữ bộ nhớ di động.

Các vật ghi đọc được bằng máy tính không tạm thời để lưu trữ các lệnh chương trình máy tính và dữ liệu có thể bao gồm tất cả các dạng của bộ nhớ, vật ghi và thiết bị bộ nhớ vĩnh viễn/không vĩnh viễn hoặc khả biến/không khả biến, bao gồm bằng cách lấy ví dụ về các thiết bị bộ nhớ bán dẫn, ví dụ, bộ nhớ truy cập ngẫu nhiên (RAM -

Random Access Memory), bộ nhớ chỉ đọc (ROM - Read Only Memory), bộ nhớ đổi pha (PRAM), bộ nhớ truy cập ngẫu nhiên tĩnh (SRAM - Static Random Access Memory), bộ nhớ truy cập ngẫu nhiên động (DRAM - Dynamic Random Access Memory), bộ nhớ chỉ đọc lập trình được xóa được (EPROM - Erasable Programmable Read-Only Memory), bộ nhớ chỉ đọc lập trình được xóa được bằng tín hiệu điện (EEPROM - Electrically Erasable Programmable Read-Only Memory), và hoặc các thiết bị bộ nhớ chớp; các thiết bị từ, ví dụ, băng, hộp mực, băng cassette, đĩa bên trong/di động; các đĩa quang từ; và các thiết bị bộ nhớ quang học, ví dụ, đĩa đa năng/viđeo kỹ thuật số (DVD), (CD)-ROM bằng đĩa nén, DVD+/-R, DVD-RAM, DVD-ROM, DVD độ nét cao (high-definition/density - HD)-DVD, và BLU-RAY/BLU-RAY DISC (BD), và các công nghệ bộ nhớ quang khác. Bộ nhớ có thể lưu trữ các đối tượng hoặc dữ liệu khác nhau, bao gồm cạc nhớ, lớp, khung, ứng dụng, môđun, dữ liệu dự phòng, công việc, trang web, mẫu trang web, cấu trúc dữ liệu, bảng cơ sở dữ liệu, kho lưu trữ thông tin động hoặc thông tin phù hợp khác bao gồm bất kỳ tham số, biến, thuật toán, hướng dẫn, quy tắc, giới hạn hoặc tài liệu tham khảo bất kỳ. Ngoài ra, bộ nhớ có thể bao gồm dữ liệu phù hợp khác, chẳng hạn như nhật ký, chính sách, dữ liệu an ninh hoặc truy cập, hoặc tệp báo cáo. Bộ xử lý và bộ nhớ có thể được bổ sung bởi, hoặc được chứa trong, hệ mạch logic chuyên dụng.

Để mang lại tương tác với người dùng, thì các phương án thực hiện của đối tượng được mô tả trong bản mô tả này có thể được thực hiện trên máy tính có thiết bị hiển thị, ví dụ, ống tia catôt (CRT- Cathode Ray Tube), màn hình tinh thể lỏng (LCD- Liquid Crystal Display), điôt phát quang (LED- Light Emitting Diode), hoặc màn hình plasma, để hiển thị thông tin cho người dùng và bàn phím và thiết bị trỏ, ví dụ, chuột, bi xoay, hoặc bàn di chuột mà người dùng có thể tạo ra đầu vào cho máy tính. Đầu vào cũng có thể được tạo ra cho máy tính bằng cách sử dụng màn hình cảm ứng, chẳng hạn như bề mặt máy tính dạng bảng có độ nhạy áp lực, màn hình cảm ứng đa điểm sử dụng cảm biến điện dung hoặc điện hoặc loại màn hình cảm ứng khác. Các loại thiết bị khác có thể được sử dụng để tương tác với người dùng. Ví dụ, phản hồi được tạo ra cho người dùng có thể dưới dạng bất kỳ của phản hồi cảm quan (chẳng hạn như, thị giác, thính giác, xúc giác, hoặc kết hợp của các loại phản hồi). Đầu vào từ người dùng có thể được nhận dưới 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 tới và nhận các tài liệu từ thiết bị điện toán khách mà được sử dụng bởi người dùng (ví dụ, bằng cách gửi các trang web tới trình duyệt web trên thiết bị điện toán di động của người dùng để phản hồi các yêu cầu nhận được từ trình duyệt web).

Thuật ngữ "giao diện người dùng đồ họa", hoặc "GUI", có thể được sử dụng trong dạng số ít hoặc dạng số nhiều để mô tả một hoặc nhiều giao diện người dùng đồ họa và mỗi trong số các bộ hiển thị của giao diện người dùng đồ họa cụ thể. Do đó, GUI có thể biểu diễn giao diện người dùng đồ họa bất kỳ, bao gồm nhưng không bị giới hạn ở, trình duyệt web, màn hình cảm ứng, hoặc giao diện dòng lệnh (CLI - Command Line Interface) để xử lý thông tin và trình bày hiệu quả kết quả thông tin cho người dùng. Nói chung, GUI có thể bao gồm một số phần tử giao diện người dùng (UI), một số hoặc toàn bộ được liên kết với trình duyệt web, như các trường tương tác, các danh sách kéo xuống và các nút. Các phần tử UI này và khác có thể là liên quan đến hoặc biểu diễn các chức năng của trình duyệt web.

Các phương án thực hiện của đối tượng được mô tả trong bản mô tả này có thể được thực hiện trong hệ thống điện toán mà bao gồm bộ phận mặt sau (back-end), ví dụ, dưới dạng máy chủ dữ liệu, hoặc bao gồm bộ phận phần mềm trung gian, ví dụ, máy chủ ứng dụng, hoặc bao gồm bộ phận mặt trước (front-end), ví dụ, máy tính khách có giao diện người dùng đồ họa hoặc trình duyệt web qua đó người dùng có thể tương tác với phương án thực hiện của đối tượng được mô tả trong bản mô tả này, hoặc kết hợp bất kỳ của một hoặc nhiều bộ phận mặt sau, phần mềm trung gian, hoặc các bộ phận mặt trước như vậy. Các bộ phận của hệ thống có thể được kết nối với nhau bởi dạng hoặc vật ghi bất kỳ của truyền thông dữ liệu số có dây hoặc không dây (hoặc kết hợp của truyền thông dữ liệu), ví dụ, mạng truyền thông. Các ví dụ về các mạng truyền thông bao gồm mạng cục bộ (LAN - Local Area Network), mạng truy cập vô tuyến (RAN - Radio Access Network), mạng khu vực đô thị (MAN - Metropolitan Area Network), mạng diện rộng (WAN - Wide Area Network), tương thích toàn cầu để truy cập vi sóng (WIMAX - Worldwide Interoperability for Microwave Access), mạng cục bộ không dây (WLAN - Wireless Local Area Network) bằng cách sử dụng, ví dụ, 802.11 a/b/g/n hoặc 802.20 (hoặc kết hợp của

802.11x và 802.20 hoặc các giao thức khác theo sáng chế), toàn bộ hoặc một phần của Internet, mạng truyền thông khác, hoặc kết hợp của các mạng truyền thông. Mạng truyền thông có thể truyền thông với, ví dụ, các gói giao thức internet (IP - Internet Protocol), các khung chuyển tiếp khung, các ô chế độ chuyển không đồng bộ (ATM - Asynchronous Transfer Mode), âm thanh, viđeo, dữ liệu, hoặc thông tin khác giữa các nút mạng.

Hệ thống điện toán có thể bao gồm các máy khách và các máy chủ. Máy khách và máy chủ thường ở cách xa nhau và thường tương tác qua mạng truyền thông. Mối quan hệ giữa máy khách và máy chủ phát sinh nhờ các chương trình máy tính chạy trên các máy tính tương ứng và có mối quan hệ máy khách-máy chủ với nhau.

Mặc dù bản mô tả này chứa nhiều chi tiết của phương án thực hiện cụ thể, những nội dung này không nên được hiểu là các giới hạn về phạm vi của khái niệm sáng chế bất kỳ hoặc phạm vi của nội dung có thể được yêu cầu bảo hộ, nhưng tốt hơn là các mô tả về các dấu hiệu mà có thể là cụ thể cho các phương án thực hiện cụ thể của các khái niệm sáng chế cụ thể. Các dấu hiệu nhất định mà được mô tả trong bản mô tả này trong ngữ cảnh của các phương án thực hiện riêng biệt cũng có thể được thực hiện, theo kết hợp, theo một phương án. Ngược lại, các dấu hiệu khác nhau mà được mô tả trong ngữ cảnh của một phương án thực hiện cũng có thể được thực thi theo nhiều phương án thực hiện, một cách riêng biệt, hoặc theo kết hợp phụ bất kỳ. Ngoài ra, mặc dù các dấu hiệu được mô tả trước có thể được mô tả là thực hiện theo các kết hợp nhất định và thậm chí được yêu cầu bảo hộ ban đầu như vậy, một hoặc nhiều dấu hiệu từ kết hợp được yêu cầu có thể, trong một số trường hợp, được lược bỏ khỏi kết hợp, và kết hợp được yêu cầu bảo hộ có thể được hướng đến kết hợp phụ hoặc biến thể của kết hợp phụ.

Các phương án cụ thể của đối tượng đã được mô tả. Các phương án thực hiện, các thay đổi, và các hoán đổi khác của các phương án được mô tả nằm trong phạm vi của yêu cầu bảo hộ sau đây sẽ là rõ ràng đối với những người có hiểu biết trung bình trong lĩnh vực kỹ thuật này. Mặc dù các hoạt động được mô tả trên các hình vẽ hoặc yêu cầu bảo hộ theo thứ tự cụ thể, nhưng điều này không được hiểu là yêu cầu rằng các hoạt động này được thực hiện theo thứ tự cụ thể được thể hiện hoặc theo thứ tự lần

lượt, hoặc tất cả các hoạt động được minh họa được thực hiện (một số hoạt động có thể được coi là tùy chọn), để đạt được các kết quả mong muốn. Trong các trường hợp nhất định, việc xử lý song song hoặc đa nhiệm (hoặc kết hợp của xử lý song song hoặc đa nhiệm) có thể là có lợi và được thực hiện khi được coi là thích hợp.

Ngoài ra, việc tách rời hoặc tích hợp các môđun và các thành phần hệ thống khác nhau trong các phương án thực hiện được mô tả trên đây không được hiểu là yêu cầu việc tách rời hoặc tích hợp như vậy trong tất cả các phương án, và cần được hiểu rằng các hệ thống và các thành phần chương trình được mô tả nói chung có thể được tích hợp với nhau trong một sản phẩm phần mềm hoặc được đóng gói vào nhiều sản phẩm phần mềm.

Theo đó, các phương án làm ví dụ được mô tả trước không xác định hoặc làm giới hạn sáng chế. Cũng có thể có các thay đổi, thay thế, và biến đổi khác mà không nằm ngoài nguyên lý và phạm vi của sáng chế.

Hơn nữa, phương án thực hiện được yêu cầu bảo hộ bất kỳ được coi là áp dụng được vào ít nhất là phương pháp được thực hiện bằng máy tính; vật ghi đọc được bằng máy tính không tạm thời lưu trữ các lệnh đọc được bằng máy tính để thực hiện phương pháp được thực hiện bằng máy tính; và hệ thống máy tính bao gồm bộ nhớ máy tính được ghép nối tương thích với bộ xử lý phần cứng được tạo cấu hình để thực hiện phương pháp được thực hiện bằng máy tính hoặc các lệnh được lưu trữ trên vật ghi đọc được bằng máy tính không tạm thời.

YÊU CẦU BẢO HỘ

1. Phương pháp gửi dữ liệu thứ nhất từ thiết bị đầu cuối thứ nhất trực tiếp đến thiết bị đầu cuối thứ hai, bao gồm các bước:

ghi và lưu trữ, bởi nền tảng trao đổi dữ liệu, thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối, trong đó thỏa thuận trao đổi dữ liệu bao gồm thông tin dấu hiệu về dữ liệu được trao đổi, trong đó dữ liệu được trao đổi bao gồm dữ liệu thứ nhất từ người dùng thứ nhất và là dữ liệu được trao đổi từ người dùng thứ hai;

nhận, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa, thiết bị đầu cuối thứ nhất là thiết bị đầu cuối tương ứng với người dùng thứ nhất, trong đó thiết bị đầu cuối thứ nhất mã hóa dữ liệu thứ nhất để thu được dữ liệu thứ nhất được mã hóa theo công nghệ mã hóa đối xứng, thiết bị đầu cuối thứ nhất gửi khóa thứ nhất đến nền tảng trao đổi dữ liệu, và thiết bị đầu cuối thứ nhất gửi trực tiếp dữ liệu thứ nhất được mã hóa đến thiết bị đầu cuối thứ hai; và

khi được xác thực, bởi nền tảng trao đổi dữ liệu, rằng dữ liệu thứ ba được nhận bởi nền tảng trao đổi dữ liệu từ thiết bị đầu cuối thứ hai phù hợp với thỏa thuận trao đổi dữ liệu, gửi, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất đến thiết bị đầu cuối thứ hai, sao cho thiết bị đầu cuối thứ hai, sau khi nhận dữ liệu thứ nhất được mã hóa được gửi bởi thiết bị đầu cuối thứ nhất, giải mã dữ liệu thứ nhất được mã hóa nhận được dựa trên khóa thứ nhất để thu dữ liệu thứ nhất, thiết bị đầu cuối thứ hai là thiết bị đầu cuối tương ứng với người dùng thứ hai, trong đó dữ liệu thứ ba là dữ liệu cần được trao đổi từ người dùng thứ hai để nhận dữ liệu thứ nhất từ người dùng thứ nhất.

2. Phương pháp theo điểm 1, phương pháp này còn bao gồm bước:

gửi, bởi nền tảng trao đổi dữ liệu, dữ liệu thứ ba đến thiết bị đầu cuối thứ nhất khi lệnh gửi dữ liệu được gửi bởi thiết bị đầu cuối thứ hai nhận được, trong đó dữ liệu thứ ba là dữ liệu cần được trao đổi từ người dùng thứ hai được tham chiếu trong thỏa thuận trao đổi dữ liệu, trong đó dữ liệu thứ ba được trao đổi qua nền tảng trao đổi dữ liệu đến người dùng thứ nhất.

3. Phương pháp theo điểm 1, phương pháp này còn bao gồm bước:

giải mã, bởi thiết bị đầu cuối thứ hai, dữ liệu thứ nhất được mã hóa nhận được sử dụng khóa thứ nhất để thu dữ liệu thứ nhất.

4. Phương pháp theo điểm 3, trong đó trước bước ghi và lưu trữ, bởi nền tảng trao đổi dữ liệu, thỏa thuận trao đổi dữ liệu giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối, phương pháp này còn bao gồm các bước:

nhận, tại nền tảng trao đổi dữ liệu, thông tin dữ liệu được đưa ra bởi thiết bị đầu cuối thứ nhất và công bố thông tin dữ liệu;

nhận, tại nền tảng trao đổi dữ liệu, yêu cầu đặt lệnh đối với thông tin dữ liệu được công bố bởi thiết bị đầu cuối thứ hai, và gửi yêu cầu này đến thiết bị đầu cuối thứ nhất; và

nhận, bởi nền tảng trao đổi dữ liệu, thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ nhất đối với yêu cầu đặt lệnh để đạt được thỏa thuận trao đổi dữ liệu.

5. Phương pháp theo điểm 1, trong đó trước bước gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai, phương pháp này còn bao gồm các bước:

nhận, bởi nền tảng trao đổi dữ liệu, khóa thứ hai được gửi bởi thiết bị đầu cuối thứ hai và được sử dụng để giải mã dữ liệu thứ hai được mã hóa; và

sau bước gửi, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất đến thiết bị đầu cuối thứ hai, phương pháp này còn bao gồm các bước: gửi, bởi nền tảng trao đổi dữ liệu, khóa thứ hai đến thiết bị đầu cuối thứ nhất, sao cho thiết bị đầu cuối thứ nhất, sau khi nhận dữ liệu thứ hai được mã hóa được gửi bởi thiết bị đầu cuối thứ hai, giải mã dữ liệu thứ hai được mã hóa nhận được dựa trên khóa thứ hai để thu dữ liệu thứ hai.

6. Phương pháp theo điểm 5, trong đó sau bước gửi, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất đến thiết bị đầu cuối thứ hai và trước bước gửi khóa thứ hai đến thiết bị đầu cuối thứ nhất, phương pháp này còn bao gồm các bước: nhận, bởi nền tảng trao đổi dữ liệu, thông tin xác nhận cho dữ liệu thứ nhất được gửi bởi thiết bị đầu cuối thứ hai, thông tin xác nhận cho dữ liệu thứ nhất chỉ báo rằng người dùng thứ hai xác định rằng dữ liệu thứ nhất phù hợp với mô tả trong thỏa thuận trao đổi dữ liệu này.

7. Phương pháp theo điểm 6, trong đó sau bước nhận, bởi nền tảng trao đổi dữ liệu, thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ hai đối với dữ liệu thứ nhất, phương pháp này còn bao gồm các bước: nhận, bởi nền tảng trao đổi dữ liệu, thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ nhất cho dữ liệu thứ hai, thông tin xác nhận cho dữ liệu thứ hai chỉ báo rằng người dùng thứ nhất xác định rằng dữ liệu thứ hai phù hợp với mô tả trong thỏa thuận trao đổi dữ liệu này.

8. Phương pháp theo điểm 7, trong đó sau bước nhận, bởi nền tảng trao đổi dữ liệu, thông tin xác nhận được gửi bởi thiết bị đầu cuối thứ nhất cho dữ liệu thứ hai, phương pháp này còn bao gồm bước ghi và lưu trữ, bởi nền tảng trao đổi dữ liệu, bản ghi mà sự trao đổi được hoàn thành trong kết quả của thỏa thuận trao đổi dữ liệu trong chuỗi khối.

9. Phương pháp theo điểm 1, trong đó sau bước gửi, bởi nền tảng trao đổi dữ liệu, khóa thứ nhất đến thiết bị đầu cuối thứ hai, phương pháp này còn bao gồm bước gửi, bởi nền tảng trao đổi dữ liệu, dữ liệu thứ ba đến người dùng thứ nhất khi được xác định rằng điều kiện thiết lập trước được thỏa mãn.

10. Phương pháp theo điểm 9, trong đó bước xác định rằng điều kiện thiết lập trước được thỏa mãn cụ thể bao gồm nhận, bởi nền tảng trao đổi dữ liệu, lệnh gửi dữ liệu được gửi bởi thiết bị đầu cuối thứ hai, lệnh gửi dữ liệu là lệnh để lệnh cho nền tảng trao đổi dữ liệu gửi dữ liệu thứ ba đến thiết bị đầu cuối thứ nhất.

11. Phương pháp theo điểm bất kỳ trong số các điểm từ 2 đến 10, trong đó:

thỏa thuận trao đổi dữ liệu bao gồm thông tin dấu hiệu về dữ liệu thứ nhất;

phương pháp này còn bao gồm các bước: thu, bởi thiết bị đầu cuối thứ hai, thông tin dấu hiệu, và xác định, theo thông tin dấu hiệu, liệu dữ liệu thứ nhất thu được có phù hợp với bản ghi trong thỏa thuận trao đổi dữ liệu hay không; và

thông tin dấu hiệu về dữ liệu thứ nhất bao gồm ít nhất một trong số sau:

tóm lược tin báo để xác minh tính toàn vẹn của dữ liệu thứ nhất; và

thông tin đường cơ sở để tóm tắt nội dung cụ thể của dữ liệu thứ nhất.

12. Phương pháp theo điểm bất kỳ trong số các điểm từ 2 đến 10, trong đó dữ liệu thứ nhất được mã hóa được truyền đến thiết bị đầu cuối thứ hai bởi thiết bị đầu cuối thứ

nhất triển khai giao diện truyền tiêu chuẩn, và giao diện truyền tiêu chuẩn này bao gồm giao diện phổ cập được xác định bởi nền tảng trao đổi dữ liệu và được sử dụng để truyền dữ liệu giữa các thiết bị đầu cuối.

13. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 11, trong đó trạng thái truyền của dữ liệu được mã hóa thứ nhất được xác định để bao gồm liệu dữ liệu được mã hóa thứ nhất được truyền hoặc không được truyền đến thiết bị đầu cuối thứ hai, trong đó xác định trạng thái truyền của dữ liệu được mã hóa thứ nhất bao gồm nhận trạng thái truyền của dữ liệu được mã hóa thứ nhất được báo cáo chủ động bởi thiết bị đầu cuối thứ nhất và thiết bị đầu cuối thứ hai.

14. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó dữ liệu thứ ba biểu diễn tiền, và trong đó người dùng thứ nhất là bên bán dữ liệu, và người dùng thứ hai là bên mua dữ liệu.

15. Thiết bị gửi dữ liệu bao gồm các bộ phận được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 13.

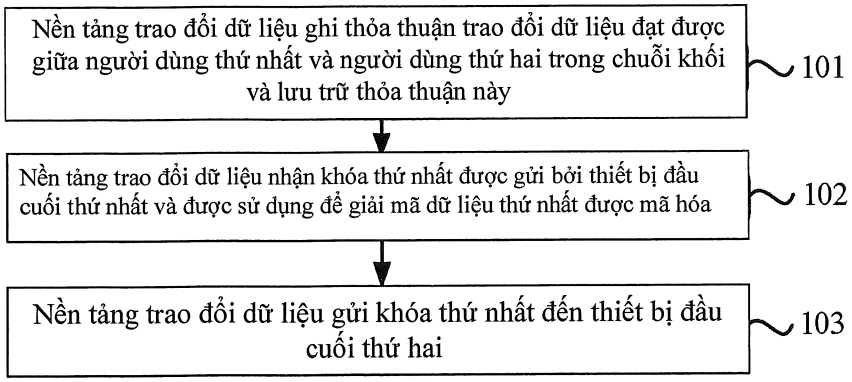

Nền tảng trao đổi dữ liệu ghi thỏa thuận trao đổi dữ liệu đạt được giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối và lưu trữ thỏa thuận này
101
Nền tảng trao đổi dữ liệu nhận khóa thứ nhất được gửi bởi thiết bị đầu cuối thứ nhất và được sử dụng để giải mã dữ liệu thứ nhất được mã hóa
102
Nền tảng trao đổi dữ liệu gửi khóa thứ nhất đến thiết bị đầu cuối thứ hai
103

FIG. 1

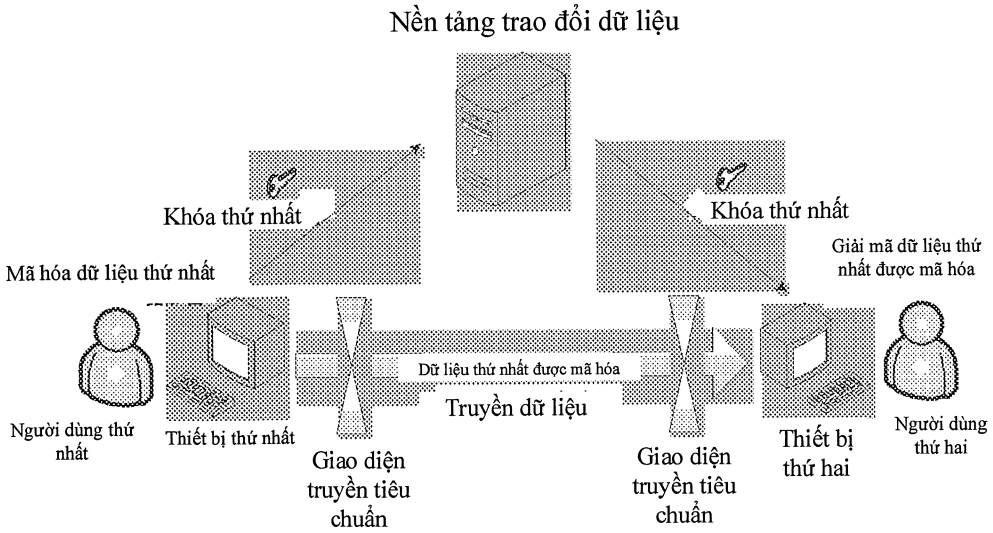

Nền tảng trao đổi dữ liệu
Khóa thứ nhất
Khóa thứ nhất
Mã hóa dữ liệu thứ nhất
Giải mã dữ liệu thứ nhất được mã hóa
Dữ liệu thứ nhất được mã hóa
Truyền dữ liệu
Người dùng thứ nhất
Thiết bị thứ nhất
Giao diện truyền tiêu chuẩn
Giao diện truyền tiêu chuẩn
Thiết bị thứ hai
Người dùng thứ hai

FIG. 2

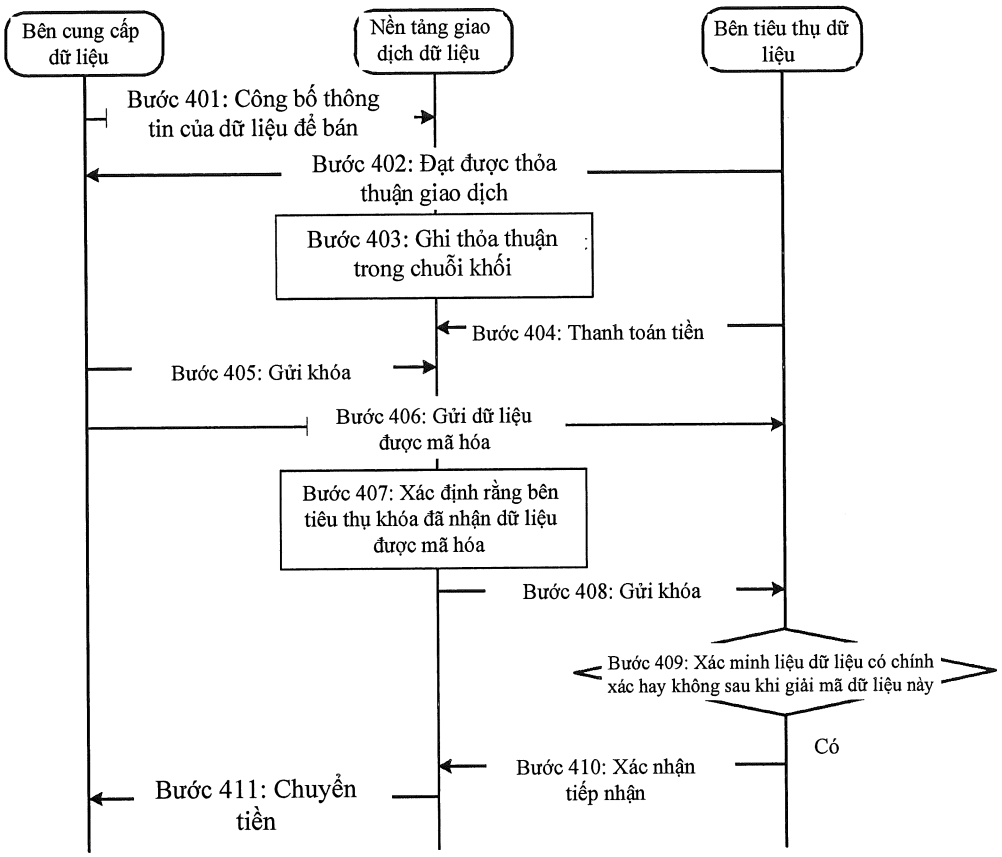

Bên cung cấp dữ liệu
Nền tảng giao dịch dữ liệu
Bên tiêu thụ dữ liệu
Bước 401: Công bố thông tin của dữ liệu để bán
Bước 402: Đạt được thỏa thuận giao dịch
Bước 403: Ghi thỏa thuận trong chuỗi khối
Bước 404: Thanh toán tiền
Bước 405: Gửi khóa
Bước 406: Gửi dữ liệu được mã hóa
Bước 407: Xác định rằng bên tiêu thụ khóa đã nhận dữ liệu được mã hóa
Bước 408: Gửi khóa
Bước 409: Xác minh liệu dữ liệu có chính xác hay không sau khi giải mã dữ liệu này
Có
Bước 410: Xác nhận tiếp nhận
Bước 411: Chuyển tiền

FIG. 3

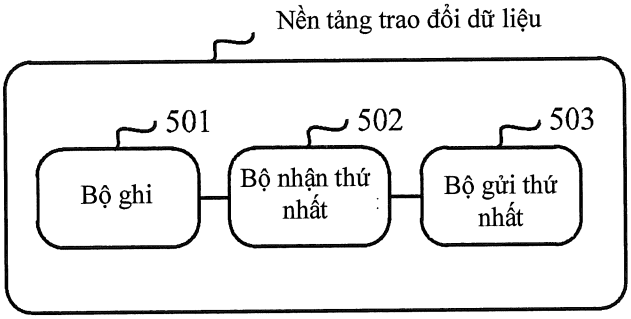

Nền tảng trao đổi dữ liệu
501
502
503
Bộ ghi
Bộ nhận thứ nhất
Bộ gửi thứ nhất

FIG. 4

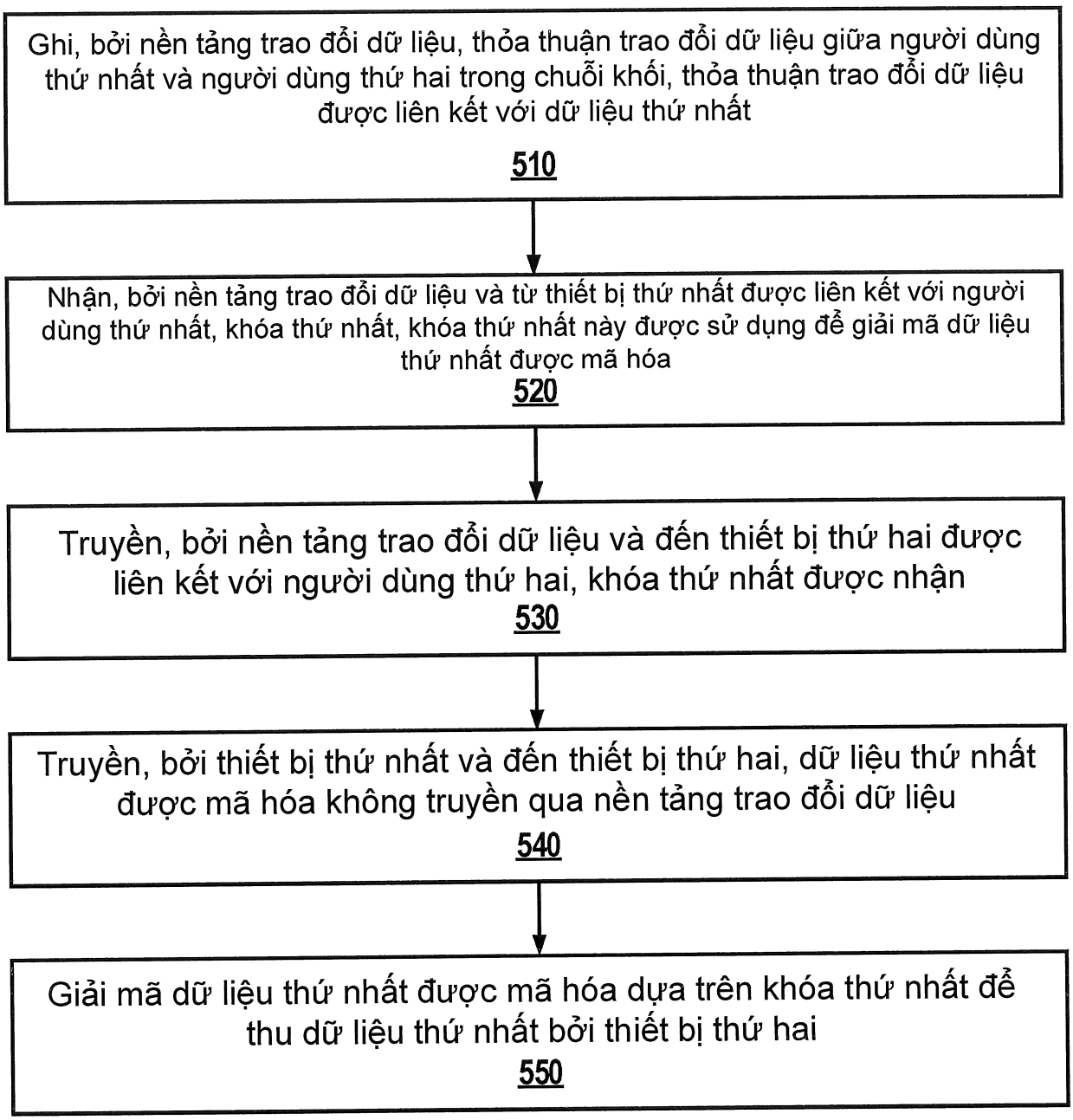

Ghi, bởi nền tảng trao đổi dữ liệu, thỏa thuận trao đổi dữ liệu giữa người dùng thứ nhất và người dùng thứ hai trong chuỗi khối, thỏa thuận trao đổi dữ liệu được liên kết với dữ liệu thứ nhất
510
Nhận, bởi nền tảng trao đổi dữ liệu và từ thiết bị thứ nhất được liên kết với người dùng thứ nhất, khóa thứ nhất, khóa thứ nhất này được sử dụng để giải mã dữ liệu thứ nhất được mã hóa
520
Truyền, bởi nền tảng trao đổi dữ liệu và đến thiết bị thứ hai được liên kết với người dùng thứ hai, khóa thứ nhất được nhận
530
Truyền, bởi thiết bị thứ nhất và đến thiết bị thứ hai, dữ liệu thứ nhất được mã hóa không truyền qua nền tảng trao đổi dữ liệu
540
Giải mã dữ liệu thứ nhất được mã hóa dựa trên khóa thứ nhất để thu dữ liệu thứ nhất bởi thiết bị thứ hai
550

FIG. 5

500