



(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)



1-0053254

(51)^{2020.01} H04L 29/06; G06K 19/06

(13) B

(21) 1-2020-05743

(22) 08/03/2018

(86) PCT/US2018/021526 08/03/2018

(87) WO2019/172911 12/09/2019

(45) 25/11/2025 452

(43) 25/05/2021 398A

(73) VISA INTERNATIONAL SERVICE ASSOCIATION (US)

900 Metro Center Boulevard Foster City, California 94404, United States of America

(72) KULPATI, Ashish (IN); RAJURKAR, Pankaj (IN); SINGH, Shantnu (IN); MODI, Vikram (IN); NAYAK, Koni Uttam (IN).

(74) Văn phòng Luật sư Ân Nam (ANNAM IP & LAW)

(54) MÁY CHỦ XỬ LÝ VÀ PHƯƠNG PHÁP CUNG CẤP BẢO MẬT DỮ LIỆU
BẰNG CÁCH SỬ DỤNG MÃ XÁC THỰC MỘT CHIỀU

(21) 1-2020-05743

(57) Sáng chế đề cập đến phương pháp xử lý mới. Phương pháp xử lý bao gồm bước nhận bởi máy chủ, bản tin yêu cầu cập nhật từ máy tính ủy quyền thứ nhất cho sự tương tác giữa hai người dùng. Sự cập nhật có thể là việc chuyển giá trị tương tác từ người dùng thứ nhất đến người dùng thứ hai, và có thể bao gồm các chi tiết tương tác như thông tin và giá trị tương tác cho mã xác thực một chiều. Máy chủ có thể phân tích bản tin yêu cầu cập nhật để xác định mã xác thực một chiều, và có thể xác định tài khoản thứ hai của người dùng thứ hai từ mã xác thực. Máy chủ có thể xác định máy tính ủy quyền thứ hai gắn liền với tài khoản thứ hai, và có thể sửa đổi bản tin yêu cầu cập nhật để bao gồm mã định danh tài khoản người dùng thứ hai cũng như các sự điều chỉnh giá trị dựa trên các tốc độ tương tác được tính toán. Máy chủ có thể chuyển tiếp bản tin yêu cầu cập nhật đến máy tính ủy quyền thứ hai để cập nhật tài khoản cho phù hợp.

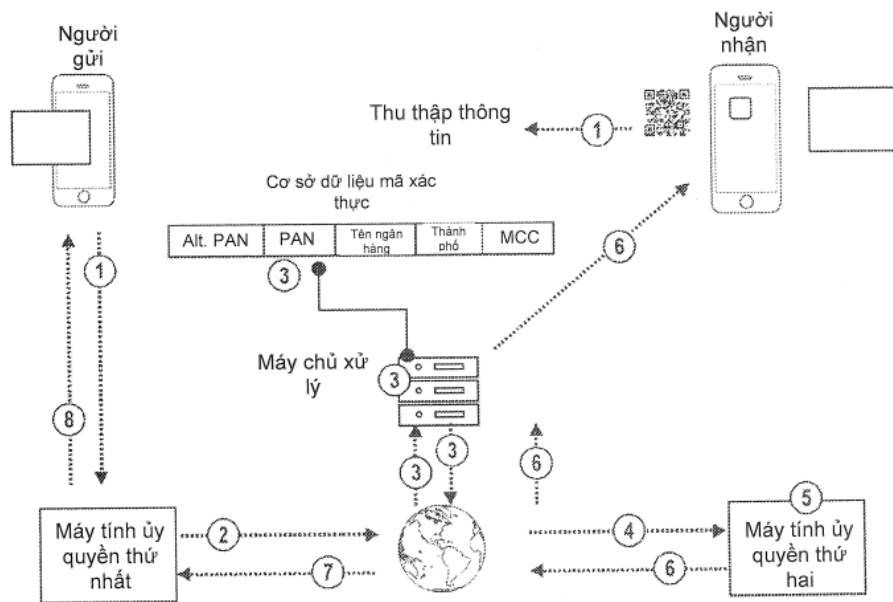


Fig.5

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến máy chủ xử lý và phương pháp cung cấp bảo mật dữ liệu bằng cách sử dụng mã xác thực một chiều.

Tình trạng kỹ thuật của sáng chế

Các hệ thống thông thường có thể chuyển giá trị từ người dùng này sang người dùng khác. Ví dụ, trong hệ thống thông thường dùng để xử lý các thanh toán, người dùng thứ nhất như chủ thẻ có thể mong muốn chuyển tiền mua hàng cho người dùng thứ hai như người bán. Tuy nhiên, trước khi điều này có thể được thực hiện, người dùng thứ hai cần phải đăng ký với bên cung cấp dịch vụ thanh toán. Bên cung cấp dịch vụ thanh toán có thể thiết lập tài khoản cho người dùng thứ hai, và có thể xác minh tính xác thực của người dùng thứ hai. Quá trình này phiền toái và phức tạp, và có thể ngăn cản một số người có khả năng chấp nhận chuyển giá trị bằng cách sử dụng các mạng thanh toán truyền thống.

Cần phải có sự cải thiện các quy trình thanh toán thông thường như quy trình được mô tả ở trên.

Các phương án sáng chế giải quyết các vấn đề này và các vấn đề khác, một cách riêng và chung.

Bản chất kỹ thuật của sáng chế

Các phương án sáng chế có thể mô tả phương pháp cập nhật các tài khoản của các người dùng đang tương tác, trong đó máy chủ có thể nhận bản tin yêu cầu cập nhật từ máy tính ủy quyền thứ nhất cho sự tương tác giữa người dùng thứ nhất và người dùng thứ hai. Yêu cầu tương tác có thể là để chuyển giá trị tương tác từ người dùng thứ nhất đến người dùng thứ hai, và có thể bao gồm các chi tiết tương tác như thông tin và giá trị tương tác cho mã xác thực một chiều. Máy chủ có thể phân tích bản tin yêu cầu cập nhật để xác định mã xác thực một chiều được chứa ở trong đó, và có thể xác định tài khoản thứ hai của người dùng thứ hai từ mã xác thực. Sau đó máy chủ có thể xác định máy tính ủy quyền thứ hai gắn liền với tài khoản thứ hai, và có thể sửa đổi bản tin yêu cầu cập nhật để bao gồm mã định danh tài khoản người dùng thứ hai. Máy chủ có thể chuyển

tiếp bản tin yêu cầu cập nhật đến máy tính ủy quyền thứ hai sao cho tài khoản người dùng thứ hai có thể được cập nhật.

Phương án khác của sáng chế có thể bao gồm máy chủ bao gồm: bộ xử lý; giao diện mạng; và phương tiện đọc được trên máy tính gồm có các chỉ lệnh có thể thực thi được bởi bộ xử lý. Các chỉ lệnh có thể ở dưới dạng mã, các chỉ lệnh mà bao gồm phương pháp bao gồm: bước nhận qua giao diện mạng, từ máy tính ủy quyền thứ nhất, bản tin yêu cầu cập nhật bao gồm yêu cầu tương tác cho sự tương tác giữa người dùng thứ nhất và người dùng thứ hai, yêu cầu tương tác bao gồm các chi tiết tương tác bao gồm mã xác thực một chiều và giá trị tương tác, sự tương tác mà chuyển giá trị tương tác từ người dùng thứ nhất đến người dùng thứ hai; bước phân tích bản tin yêu cầu cập nhật để xác định mã xác thực một chiều; bước xác định mã định danh tài khoản người dùng thứ hai cho tài khoản thứ hai của người dùng thứ hai từ mã xác thực một chiều; bước thay thế mã định danh tài khoản người dùng thứ hai cho mã xác thực một chiều trong các chi tiết tương tác để bao gồm mã định danh tài khoản người dùng thứ hai trong bản tin yêu cầu cập nhật; xác định máy tính ủy quyền thứ hai gắn liền với mã định danh tài khoản người dùng thứ hai; bước gửi đến máy tính ủy quyền thứ hai, bản tin yêu cầu cập nhật; và bước nhận bản tin phản hồi cập nhật từ máy tính ủy quyền thứ hai, trong đó máy tính ủy quyền thứ hai cập nhật tài khoản thứ hai của người dùng thứ hai dựa trên các chi tiết tương tác.

Các chi tiết khác liên quan đến các phương án sáng chế có thể được tìm thấy trong phần mô tả chi tiết sáng chế và các hình vẽ được mô tả ở trong bản mô tả này.

Mô tả vắn tắt các hình vẽ

Fig.1 thể hiện hệ thống dùng để cập nhật dữ liệu tài khoản của các người dùng đang tương tác theo các phương án sáng chế.

Fig.2 thể hiện máy chủ dùng để thuận tiện cho các cập nhật giữa các máy tính ủy quyền theo phương án sáng chế.

Fig.3 thể hiện quy trình đăng ký với hệ thống mà sử dụng thiết bị chứng thực theo phương án sáng chế.

Fig.4 thể hiện quy trình chuyển tiền đến tài khoản thẻ thanh toán mà sử dụng ứng dụng của nhà phát hành theo phương án sáng chế.

Fig.5 thể hiện quy trình chuyển tiền đến tài khoản thẻ thanh toán mà sử dụng bộ xử lý thanh toán theo phương án sáng chế.

Các thuật ngữ được sử dụng trong bản mô tả

“Người dùng” có thể là cá nhân. Người dùng thiết bị hoặc hệ thống cụ thể, có thể là cá nhân mà vận hành thiết bị và/hoặc theo sự triển khai hệ thống cụ thể. Ví dụ, người dùng điện thoại di động có thể là chủ sở hữu điện thoại. Như ví dụ khác, người dùng hệ thống thanh toán có thể là người tiêu dùng mà thực hiện các giao dịch bằng cách sử dụng hệ thống thanh toán.

“Thực thể” có thể là đối tượng hoạt động riêng biệt hoặc nhóm đối tượng hoạt động. Ví dụ, thực thể có thể là thực thể kinh doanh, như tập đoàn hoặc ngân hàng, hoặc có thể là thực thể thuộc chính phủ.

“Thiết bị điện toán” có thể là thiết bị để thực hiện các phép tính, cụ thể như phương tiện dùng để thực thi tác vụ theo các chỉ lệnh. Trong bối cảnh nối mạng máy tính, thiết bị điện toán có thể là thiết bị điện tử bất kỳ có khả năng nhận và xử lý các chỉ lệnh. Các chỉ lệnh thường ở dưới dạng “phương tiện có thể đọc được trên máy tính”, mà có thể bao gồm cả mã máy tính. Thông thường các thiết bị điện toán là các thiết bị “di động” mà người dùng có thể mang theo một cách dễ dàng và thực hiện các tác vụ hàng ngày, như thực hiện các cuộc gọi, truy cập internet, xác định vị trí của họ, và/hoặc ghi lại các sự kiện thông qua các bức ảnh, các video, và/hoặc các bản ghi âm thanh.

“Ứng dụng” hoặc “ứng dụng di động”, được gọi một cách thông tục là “áp”, có thể là chương trình máy tính dùng để thực thi các tác vụ cụ thể. Ứng dụng có thể được cài sẵn hoặc được tải lên trên thiết bị và được lưu trữ trong bộ nhớ. Khi ứng dụng được khởi chạy trên thiết bị, nó có thể cung cấp các chức năng hoặc “các tính năng” được lựa chọn cho người dùng, mà có thể làm thiết bị thực thi các mệnh lệnh khác nhau dựa trên các đầu vào của người dùng. Ví dụ, ứng dụng có thể là ứng dụng máy ảnh mà kích hoạt chức năng máy ảnh của điện thoại di động và chụp ảnh theo chỉ dẫn của người dùng. Như ví dụ khác, ứng dụng có thể là ứng dụng thanh toán mà chuyển các tài sản giữa người dùng và/hoặc các thực thể bằng cách cập nhật các sổ cái tài khoản.

“Bằng chứng chứng thực” có thể là phần tử dùng để chứng minh danh tính hoặc quyền sở hữu. Ví dụ, bằng chứng chứng thực có thể bao gồm tên người dùng và/hoặc mật khẩu. Các bằng chứng chứng thực thường được sử dụng trong các mạng máy tính

như phương tiện liên kết các nhận dạng số với các nhận dạng người. Trong bối cảnh của các mạng thanh toán, bằng chứng chứng thực có thể là mã định danh tài khoản, như số thẻ thanh toán, số định tuyến, số tài khoản ngân hàng, v.v.

“Thiết bị chứng thực” có thể là đối tượng mà chia sẻ một hoặc nhiều bằng chứng chứng thực. Ví dụ, thiết bị chứng thực có thể là đối tượng nhỏ được trang bị bộ nhớ lưu trữ các chứng thực dưới dạng số, như thẻ chứng thực chứa dải từ tính hoặc chip nhớ. Theo các ví dụ khác, thiết bị chứng thực có thể đơn giản là đối tượng với các chứng thực được in, được dập nổi, hoặc được khắc lên trên đó, mà có thể được giao tiếp bằng máy quét hoặc thiết bị quang học khác. Thiết bị chứng thực thường có tính di động, vì vậy người dùng có thể dễ dàng mang các chứng thực trong túi quần áo, ví, túi xách, hoặc tay của họ.

“Mã xác thực” có thể là phần tử có thể chuyển đổi được. Ví dụ, mã xác thực có thể là phần tử dữ liệu mà có thể được chuyển đổi cho một thứ gì đó có giá trị, như mã giảm giá hoặc mã truy cập một lần. Trong một số trường hợp, mã xác thực có thể đóng vai trò là đối tượng thay thế cho bằng chứng chứng thực khi được sử dụng cho mục đích chuyên biệt. Với ví dụ đơn giản, mã xác thực của trò chơi có thể đóng vai trò là chứng thực truy cập dùng để bắt đầu trò chơi. Đối với ví dụ nâng cao hơn, mã xác thực thanh toán có thể đóng vai trò là sự chuyển giá trị được giới hạn ở bối cảnh thanh toán cụ thể. Theo cách này, mã xác thực có thể được sử dụng để chứng nhận bằng chứng truy cập hoặc bằng chứng xác thực mà không cần bằng chứng danh tính hoặc bằng chứng quyền sở hữu.

Theo một số phương án, mã xác thực cũng có thể bao gồm mã định danh thay thế cho một số thông tin. Chẳng hạn, mã xác thực có thể bao gồm chuỗi ký tự số mà có thể được sử dụng như là đối tượng thay thế cho mã định danh tài khoản ban đầu. Trong một số trường hợp, mã xác thực có thể là mã xác thực thanh toán, mà có thể bao gồm mã định danh cho tài khoản thanh toán mà là đối tượng thay thế cho mã định danh tài khoản thực, như số tài khoản chính (PAN, primary account number). Ví dụ, mã xác thực “4900 0000 0000 0001” có thể được sử dụng thay cho PAN “4147 0900 0000 1234”. Theo một số phương án, mã xác thực có thể “bảo toàn định dạng” và có thể có định dạng số mà tuân theo các mã định danh tài khoản được sử dụng trong các mạng xử lý sẵn có (ví dụ, định dạng bản tin giao dịch tài chính ISO 8583). Theo một số phương án, mã xác thực có thể được sử dụng thay cho PAN để khởi tạo, ủy quyền, dàn xếp hoặc giải quyết giao

dịch thanh toán. Mã xác thực cũng có thể được sử dụng để đại diện cho chứng thực ban đầu trong các hệ thống khác nơi mà chứng thực ban đầu thường sẽ được cung cấp. Theo một số phương án, trị số mã xác thực có thể được tạo ra sao cho việc khôi phục PAN ban đầu hoặc mã định danh tài khoản khác từ trị số mã xác thực có thể không được bắt nguồn từ việc tính toán. Theo một số phương án, mã xác thực có thể là ID thư điện tử hoặc số điện thoại di động, các bí danh, hoặc “nhãn” được định vị.

“Thông tin tài khoản” có thể là thông tin bất kỳ gắn liền với tài khoản của người dùng. Thông tin như này có thể có liên quan đến trực tiếp tài khoản hoặc có thể được bắt nguồn từ thông tin có liên quan đến tài khoản. Các ví dụ về thông tin tài khoản có thể bao gồm mã định danh tài khoản, tên người dùng, mật khẩu, người dùng thông tin (ví dụ, tên, tuổi, địa chỉ thư điện tử, địa chỉ giao hàng, v.v.). Trong một số trường hợp, thông tin tài khoản cũng có thể được biết đến như thông tin tài khoản thanh toán, thông tin tài khoản thẻ, hoặc thông tin tương tự, và có thể gắn liền với thiết bị thanh toán (ví dụ, thẻ thanh toán). Ví dụ, thông tin tài khoản có thể bao gồm PAN (Số tài khoản chính, Primary Account Number hoặc “số tài khoản”), tên người dùng, ngày hết hạn, CVV (Trị số xác minh thẻ, Card Verification Value), dCVV (Trị số xác minh thẻ động, Dynamic Card Verification Value), CVV2 (Trị số xác minh thẻ 2, Card Verification Value 2), các trị số xác minh thẻ CVC3, v.v. CVV2 thường được hiểu là là giá trị xác minh tĩnh gắn liền với thiết bị thanh toán. Các giá trị CVV2 thường là nhìn thấy được đối với người dùng (ví dụ, người dùng), trong khi đó các giá trị CVV và dCVV thường được nhúng trong bộ nhớ hoặc các bản tin yêu cầu sự ủy quyền và không dễ dàng được biết đến đối với người dùng (mặc dù chúng được biết đến đối với nhà phát hành và các bộ xử lý thanh toán).

“Thực thể cung cấp tài nguyên” có thể là thực thể mà có thể làm cho các tài nguyên khả dụng đối với người dùng. Các thực thể cung cấp tài nguyên có thể còn được gọi là các nhà cung cấp tài nguyên. Các ví dụ về các thực thể cung cấp tài nguyên bao gồm các nhà cung cấp tài nguyên, các nhà bán hàng, các nhà cung ứng, các chủ sở hữu, các người bán, các nhà cung cấp ví, các nhà cung cấp dịch vụ, và thực thể tương tự. Theo một số phương án, các thực thể như này có thể là cá nhân đơn lẻ, các nhóm cá nhân cỡ nhỏ, hoặc các nhóm cá nhân cỡ lớn hơn (ví dụ, các công ty). Các thực thể cung cấp tài nguyên có thể gắn liền với một hoặc nhiều vị trí vật lý (ví dụ, siêu thị, trung tâm thương mại, cửa hàng, v.v.) và các nền tảng trực tuyến (ví dụ, các công ty thương mại

điện tử, các công ty trực tuyến, v.v.). Theo một số phương án, các thực thể cung cấp tài nguyên có thể làm tạo ra các vật phẩm vật lý khả dụng (ví dụ, hàng hóa, sản phẩm, v.v.) đối với người dùng. Theo các phương án khác, các thực thể cung cấp tài nguyên có thể tạo ra các tài nguyên số khả dụng (ví dụ, các tài liệu điện tử, các tập tin điện tử, v.v.) đối với người dùng. Theo các phương án khác, các thực thể cung cấp tài nguyên có thể quản lý việc truy cập vào các tài nguyên nhất định bởi người dùng. Theo một số phương án, các tài nguyên có thể là các dịch vụ (ví dụ, các dịch vụ ví số).

“Yêu cầu truy cập” có thể là yêu cầu dùng để truy cập vào tài nguyên. Tài nguyên có thể là tài nguyên vật lý (ví dụ, hàng hóa), các tài nguyên số (ví dụ, tài liệu điện tử, dữ liệu điện tử, v.v.), hoặc các dịch vụ. Trong một số trường hợp, yêu cầu truy cập có thể được trình nhờ sự truyền dẫn bản tin yêu cầu truy cập mà bao gồm dữ liệu yêu cầu truy cập. Thông thường thiết bị gắn liền với người yêu cầu có thể truyền bản tin yêu cầu truy cập đến thiết bị gắn liền với nhà cung cấp tài nguyên.

“Dữ liệu yêu cầu truy cập” có thể là thông tin bất kỳ xung quanh hoặc có liên quan đến yêu cầu truy cập. Dữ liệu yêu cầu truy cập có thể bao gồm thông tin hữu dụng dùng để xử lý và/hoặc xác minh yêu cầu truy cập. Ví dụ, dữ liệu yêu cầu truy cập có thể bao gồm các chi tiết gắn liền với thực thể (ví dụ, nhà cung cấp tài nguyên máy tính, máy chủ có bộ xử lý, máy tính ủy quyền, v.v.) liên quan đến việc xử lý yêu cầu truy cập, như các mã định danh thực thể (ví dụ, tên, v.v.), thông tin vị trí gắn liền với thực thể, và thông tin mà chỉ thị loại thực thể (ví dụ, mã danh mục). Dữ liệu yêu cầu truy cập ví dụ có thể bao gồm thông tin chỉ thị số lượng yêu cầu truy cập, vị trí yêu cầu truy cập, các tài nguyên đã nhận (ví dụ, sản phẩm, tài liệu, v.v.), thông tin về các tài nguyên đã nhận (ví dụ, kích cỡ, số lượng, loại, v.v.), dữ liệu về thực thể cung cấp tài nguyên (ví dụ, dữ liệu nhà cung cấp tài nguyên, dữ liệu chủ sở hữu tài liệu, v.v.), dữ liệu người dùng, ngày và thời gian yêu cầu truy cập, phương pháp được sử dụng để thực hiện yêu cầu truy cập (ví dụ, tiếp xúc, không tiếp xúc, v.v.), và thông tin liên quan khác. Dữ liệu yêu cầu truy cập có thể còn được biết đến là yêu cầu truy cập thông tin, dữ liệu giao dịch, thông tin giao dịch, hoặc dữ liệu tương tự.

“Mã xác thực một chiều” có thể là mã xác thực mà đã được gán hướng trao đổi. Ví dụ, mã xác thực trò chơi một chiều có thể là mã xác thực mà chỉ bắt đầu trò chơi cho người chơi 2 mà không phải người chơi 1. Theo ví dụ khác, trong giao dịch thanh toán, mã xác thực một chiều có thể là mã xác thực chỉ dành cho tiền gửi mà có thể đóng vai

trò là đối tượng thay thế cho các bằng chứng chứng thực tài khoản của người nhận tiền mà không phải là đối tượng thay thế cho các bằng chứng chứng thực của người trả tiền.

“Sự tương tác” có thể là hành động giữa những người dùng và/hoặc các thực thể. Ví dụ, sự tương tác có thể là cuộc gặp gỡ trực tiếp và/hoặc trao đổi thông tin, dữ liệu, hoặc giá trị.

“Yêu cầu tương tác” có thể là yêu cầu để tương tác như trong bối cảnh của các tác vụ được kiểm soát mà yêu cầu sự ủy quyền. Theo một số phương án, yêu cầu tương tác có thể là “yêu cầu truy cập”. Trong bối cảnh nổi mạng máy tính, các yêu cầu tương tác thường có liên quan đến việc ủy quyền truy cập vào cơ sở dữ liệu hoặc thao tác với dữ liệu được lưu trữ ở trong đó. Ví dụ, trên mạng xác hội, yêu cầu tương tác có thể là yêu cầu kết bạn mà, khi được ủy quyền, sẽ cấp quyền truy cập vào dữ liệu hồ sơ. Như ví dụ khác, trong mạng thanh toán, yêu cầu tương tác có thể là yêu cầu thực hiện giao dịch, và khi được ủy quyền, có thể cho phép cập nhật các sổ cái tài khoản.

“Giá trị tương tác” có thể là số lượng được gán cho sự tương tác. Ví dụ, sự tương tác trong ứng dụng dịch vụ có thể được gán cho việc đánh giá chất lượng, như “năm sao”. Theo ví dụ khác, sự tương tác ở trên mạng xác hội có thể được gán giá trị tương tác là ‘1’ cho “sự tương tác ưa thích/được thích” hoặc được gán giá trị tương tác là ‘0’ cho sự tương tác “không ưa thích/không được thích”. Theo ví dụ khác nữa, sự tương tác ở trong mạng thanh toán có thể được gán lượng tiền tệ, mà có thể là sự phản ánh về các số lượng tiền được chuyển trong khi tương tác, như số tiền giao dịch và/hoặc khoản phí giao dịch.

“Tốc độ tương tác” có thể là tỷ lệ mà tại đó người dùng hoặc thực thể tương tác. Ví dụ, tốc độ tương tác có thể là số lượng tương tác trung bình trên một ngày hoặc tổng giá trị tương tác đã nhận trên một ngày.

“Bản tin yêu cầu cập nhật” có thể là bản tin mà yêu cầu cập nhật thông tin. Trong mạng máy tính, cập nhật được yêu cầu có thể là cập nhật dữ liệu được lưu trữ trong cơ sở dữ liệu. Ví dụ, trong mạng thanh toán, cơ sở dữ liệu về số dư tài khoản có thể được yêu cầu trong giao dịch thanh toán ở trong mạng.

“Bản tin phản hồi cập nhật” có thể là bản tin mà phản hồi yêu cầu cập nhật. Ví dụ, bản tin phản hồi cập nhật có thể truyền đạt sự xác nhận hoặc từ chối cập nhật được yêu cầu.

“Máy tính ủy quyền” có thể là máy tính dùng để ủy quyền các yêu cầu. Ví dụ, máy tính ủy quyền có thể là thiết bị dùng để kiểm soát truy cập hoặc máy chủ kiểm soát truy cập. Trong mạng máy tính, máy tính ủy quyền thường là máy chủ mà ủy quyền việc truy cập vào dữ liệu thông qua sự xác minh các nhận dạng số và/hoặc các quyền hạn. Ví dụ, trong mạng thanh toán, máy tính ủy quyền có thể là máy chủ của ngân hàng mà ủy quyền các cập nhật vào các sổ cái tài khoản dựa trên sự xác minh các chứng thực thanh toán và và/hoặc các sổ dư tài khoản. Máy tính ủy quyền thường gắn liền với “nhà phát hành” hoặc “thực thể phát hành”, mà có thể là ngân hàng mà phát hành các tài khoản thanh toán và các chứng thực của chúng cho người dùng như phương tiện dùng để gửi quỹ. Ví dụ, ngân hàng phát hành có thể là ngân hàng mà phát hành thẻ ghi nợ cho người tiêu dùng sao cho chúng có thể chuyển tiền đến bên nhận trong giao dịch thanh toán.

“Máy chủ” có thể là máy tính cấu hình mạnh hoặc cụm máy tính. Ví dụ, máy chủ có thể là khung máy chính cỡ lớn, cụm máy tính cỡ nhỏ, hoặc nhóm các máy chủ mà có chức năng như khối chức năng. Theo một ví dụ, máy chủ có thể là máy chủ cơ sở dữ liệu được ghép nối vào máy chủ Web.

Mô tả chi tiết sáng chế

Như đã được đề cập trước đó, việc chấp nhận các thanh toán thẻ với tư cách là người bán nhỏ lẻ (nghĩa là người bán cá nhân gắn liền với các giao dịch giá trị nhỏ) phần lớn được xem là không thực tế do bản chất của các mạng thẻ thanh toán. Các phương án sáng chế mô tả phương pháp cho phép các giao dịch buôn bán nhỏ sử dụng các cơ sở hạ tầng thẻ thanh toán sẵn có và theo cách mà thuận tiện cho người tiêu dùng. Các phương án sáng chế cho phép chủ thẻ bất kỳ trở thành người bán nhỏ lẻ và chấp nhận các thanh toán từ các chủ thẻ khác, nhờ mã xác thực chỉ dành cho tiền gửi mà có thể khởi tạo “thanh toán đẩy” như khoản bồi hoàn, hoặc đẩy tín dụng, đến tài khoản thẻ ghi nợ của người nhận tiền hoặc sự chuyển tiền tương tự khác đến tài khoản tài chính đã được phát hành của người nhận tiền.

Theo một phương án, ứng dụng thiết bị di động có thể được cung cấp cho người dùng, mà có thể cho phép người dùng đăng ký làm người bán nhỏ lẻ hoặc gửi các thanh toán đến người bán nhỏ lẻ đã đăng ký trong hệ thống. Để đăng ký làm người bán (ví dụ, người dùng thứ hai), người dùng có thể sử dụng ứng dụng thiết bị di động để cung cấp và tạo ra dữ liệu người bán của chính họ, mà có thể bao gồm thông tin thẻ, tên người

bán, danh mục người bán, và vị trí người bán, cũng như thiết lập cài đặt thông báo bất kỳ ở trong ứng dụng. Khi nhận dữ liệu người bán, máy chủ có thể tạo ra mã xác thực chỉ dành cho tiền gửi (ví dụ chuỗi duy nhất) và có thể liên kết mã xác thực chỉ dành cho tiền gửi với dữ liệu người bán trong bản ghi đăng ký. Sau đó sự xác nhận có thể được gửi đến người dùng đang đăng ký, mà trong đó người dùng được cấp mã có thể đọc được bằng máy mà truyền đạt thông tin mã xác thực chỉ dành cho tiền gửi (ví dụ mã QR). Mã QR có thể được hiển thị từ thiết bị di động của người dùng đã đăng ký, sao cho khách hàng tương lai có thể quét mã bằng cách sử dụng máy ảnh trên điện thoại thông minh của họ và khởi tạo thanh toán.

Khi người dùng đã đăng ký, mà hiện tại được thiết lập như người bán nhỏ lẻ trong hệ thống, sẵn sàng chấp nhận thanh toán từ khách hàng (ví dụ, người dùng thứ nhất) trong giao dịch dành cho hàng hóa hoặc dịch vụ, khách hàng có thể khởi chạy ứng dụng thiết bị di động trên điện thoại thông minh của họ và sử dụng giao diện máy ảnh được cung cấp để quét mã QR của người bán nhỏ lẻ. Khi quét mã QR, điện thoại thông minh của khách hàng có thể chia sẻ mã xác thực chỉ dành cho tiền gửi nằm dưới mã này cho ngân hàng phát hành của khách hàng, cùng với thông tin thanh toán và số tiền giao dịch của khách hàng. Theo một phương án, thông tin thanh toán của khách hàng có thể được truy xuất từ trong thiết bị di động của họ, như từ ứng dụng thiết bị được cung cấp hoặc ứng dụng di động khác được lưu trữ trên thiết bị của khách hàng. Ngân hàng phát hành của khách hàng có thể nhận thông tin giao dịch và khởi tạo việc chuyển tiền với máy chủ xử lý của hệ thống. Sau đó máy chủ xử lý có thể nhận mã xác thực chỉ dành cho tiền gửi và truy vấn dữ liệu người bán được liên kết (mà có thể là dữ liệu người dùng thứ hai), bao gồm thông tin thẻ được đăng ký bởi người bán nhỏ lẻ. Theo một phương án, máy chủ cũng có thể ghi mỗi giao dịch và số tiền giao dịch được liên kết, mà sau đó có thể được sử dụng để xác định các khoản phí dành cho người bán được dựa trên tốc độ (ví dụ các khoản phí gắn liền với các người bán có khối lượng giao dịch cao hơn mà đặt áp lực lớn hơn lên hệ thống). Sau đó máy chủ có thể thay mã xác thực chỉ dành cho tiền gửi với thông tin thẻ thanh toán của người bán nhỏ lẻ trong việc chuyển tiền cũng như trừ đi các khoản phí liên kết bất kỳ từ số tiền chuyển khoản. Sau đó việc chuyển tiền được chuyển tiếp đến ngân hàng phát hành của người bán nhỏ lẻ, sao cho ngân hàng phát hành có thể cập nhật các sổ cái của mình cho phù hợp.

Fig.1 thể hiện hệ thống dùng để cập nhật dữ liệu tài khoản của các người dùng đang tương tác theo các phương án. Hệ thống 100 có thể bao gồm nhiều người dùng đang tương tác bao gồm người dùng thứ nhất 101 và người dùng thứ hai 102. Hệ thống 100 có thể còn bao gồm thiết bị người dùng thứ nhất 121 của người dùng thứ nhất 101 và tương tự như vậy, thiết bị người dùng thứ hai 122 của người dùng thứ hai 102. Thiết bị người dùng thứ nhất 121 và thiết bị người dùng thứ hai 122 có thể là thiết bị điện toán bất kỳ mà có khả năng truyền và nhận dữ liệu. Ví dụ, các thiết bị người dùng có thể là điện thoại thông minh, máy tính bảng, thiết bị đeo được, các thiết bị trợ lý số cầm tay, các thiết bị chơi điện tử cầm tay, máy tính xách tay, máy tính, v.v. Hệ thống 100 có thể còn bao gồm máy tính ủy quyền thứ nhất 131 có khả năng truy cập và cập nhật cơ sở dữ liệu tài khoản thứ nhất 131A, cũng như máy tính ủy quyền thứ hai 132 có khả năng truy cập và cập nhật tài khoản thứ hai cơ sở dữ liệu 132A. Hệ thống 100 có thể còn bao gồm máy chủ xử lý 140 dùng để xử lý dữ liệu tương tác và có khả năng truy cập và cập nhật cơ sở dữ liệu mã xác thực 140A. Cần phải hiểu rằng hệ thống 100 có thể bao gồm một hoặc nhiều kênh dùng để truyền dẫn dữ liệu giữa các thiết bị điện toán, chẳng hạn như số lượng bất kỳ các mạng di động, mạng giao thức internet, và/hoặc mạng ISO 8583 phù hợp. Cần phải hiểu thêm rằng mặc dù Fig.1 chỉ thể hiện hệ thống bao gồm hai người dùng đang tương tác, hệ thống 100 có thể hỗ trợ xử lý nhiều tương tác một cách đồng thời, và các thiết bị điện toán đơn lẻ và các cơ sở dữ liệu được thể hiện có thể được triển khai như nhiều thiết bị điện toán dùng để thực hiện các chức năng giống nhau.

Theo các phương án, thiết bị người dùng thứ hai 122 có thể chứa mã xác thực một chiều. Theo một phương án, mã xác thực một chiều có thể được cung cấp đến người dùng thứ hai 102 bởi máy chủ xử lý 140 trong quy trình đăng ký, như được mô tả chi tiết hơn dưới đây. Mã xác thực một chiều có thể được sử dụng bởi người dùng thứ hai 102 để nhận các giá trị tương tác từ người dùng thứ nhất 101, và có thể được sử dụng để cung cấp chúng cho tài khoản gắn liền với các chứng thực của người dùng thứ hai này, ví dụ, các chứng thực người dùng thứ hai 112. Ví dụ, mã xác thực một chiều có thể là mã xác thực chỉ dành cho tiền gửi gắn liền với số thẻ thanh toán của người dùng, mà quỹ có thể được phân bổ vào, trong khi giao dịch. Các chứng thực người dùng thứ hai 112 có thể bao gồm mã định danh tài khoản, mà có thể là chuỗi ký tự duy nhất, như số thẻ ghi nợ hoặc số tài khoản chính (PAN). Bản thân mã xác thực một chiều có thể là chuỗi số duy nhất có định dạng dữ liệu giống như các chứng thực người dùng thứ hai

112. Ví dụ, mã xác thực một chiều có thể là số có 16 chữ số mà có thể được xử lý bởi máy tính ủy quyền thứ nhất 131 và máy tính ủy quyền 132 như thể nó là số thẻ thanh toán thông thường. Theo một phương án, thông tin mã xác thực một chiều có thể được chia sẻ thông qua mã có thể đọc được bằng máy (ví dụ mã QR hoặc nhãn quang học khác) mà có thể được lưu trữ bởi thiết bị người dùng thứ hai 122. Thiết bị người dùng thứ hai 122 sau đó có thể gửi/hiển thị mã có thể đọc được bằng máy, sao cho mã xác thực một chiều cơ sở có thể thu được bởi thiết bị của người dùng khác trong quy trình tương tác, như bằng cách sử dụng máy ảnh hoặc máy quét quang học khác.

Theo các phương án, người dùng thứ hai 102 có thể là người dùng mà mong muốn chấp nhận các giá trị tương tác từ người dùng thứ nhất 101, như trong bối cảnh việc nhận tiền được phân bổ cho việc thanh toán. Ví dụ, người dùng thứ hai 102 có thể là người bán hàng và người dùng thứ nhất 101 có thể là khách hàng tiềm năng. Để chuyển các giá trị tương tác đến người dùng thứ hai 102, người dùng thứ nhất 101 có thể sử dụng thiết bị người dùng thứ nhất 121 để trao đổi dữ liệu tương tác với thiết bị người dùng thứ hai 122 của người dùng thứ hai 102. Theo các phương án, sự tương tác có thể được khởi tạo khi người dùng thứ nhất 101 thu được mã xác thực một chiều từ thiết bị người dùng thứ hai 122 bằng cách sử dụng thiết bị người dùng thứ nhất 121. Ví dụ, giao dịch có thể được khởi tạo khi người dùng thứ nhất 101 quét mã xác thực chỉ dành cho tiền gửi thông tin từ mã QR trên thiết bị người dùng thứ hai 122 bằng cách sử dụng giao diện máy ảnh của thiết bị người dùng thứ nhất 121. Điều này có thể được thực hiện từ ứng dụng trên thiết bị người dùng thứ nhất 121, như ứng dụng dịch vụ ngân hàng di động hoặc ứng dụng thanh toán. Từ trong ứng dụng, người dùng thứ nhất cũng có thể nhập vào các chi tiết tương tác hoặc các chi tiết giao dịch bổ sung bao gồm giá trị tương tác như số tiền giao dịch gắn liền với sự tương tác. Theo một phương án, sự khởi tạo giao dịch trong ứng dụng cũng có thể tạo ra dấu thời gian và/hoặc mã định danh giao dịch (nghĩa là, ID giao dịch) mà có thể được bao gồm với các chi tiết tương tác.

Các chi tiết tương tác có thể còn bao gồm các chứng thực người dùng thứ nhất 111 dùng để xác định dữ liệu tài khoản trong cơ sở dữ liệu tài khoản thứ nhất 131A mà gắn liền với người dùng thứ nhất 101. Các chứng thực người dùng thứ nhất 111 có thể được nhập thủ công bởi người dùng thứ nhất 101 (ví dụ gõ hoặc quét thông tin thẻ thanh toán) hoặc có thể được truy xuất từ bộ nhớ của thiết bị người dùng thứ nhất 121. Theo một phương án, các chứng thực người dùng thứ nhất 111 có thể bao gồm mã định danh

tài khoản, mà có thể được sử dụng bởi máy tính ủy quyền thứ nhất 131 để truy vấn cơ sở dữ liệu tài khoản thứ nhất 131A cho dữ liệu tài khoản của người dùng thứ nhất 101. Ví dụ, mã định danh tài khoản có thể là số tài khoản chính có 16 chữ số mà được liên kết với số tiền của quỹ được phân bổ đến người dùng thứ nhất 101 cũng như lịch sử giao dịch. Theo các phương án, máy tính ủy quyền thứ nhất 131 có thể có khả năng ủy quyền các cập nhật cho cơ sở dữ liệu tài khoản thứ nhất 131A được yêu cầu bởi người dùng thứ nhất 101. Ví dụ, máy tính ủy quyền thứ nhất 131 có thể là máy chủ của ngân hàng phát hành mà có thể ủy quyền hoặc từ chối các thay đổi được yêu cầu đối với các số dư tài khoản của người dùng trong giao dịch được yêu cầu và/hoặc chuyển tiền.

Khi thu được mã xác thực một chiều từ thiết bị người dùng thứ hai 122, người dùng thứ nhất 101 có thể gửi bản tin yêu cầu cập nhật đến máy tính ủy quyền thứ nhất 131 mà chứa các chi tiết tương tác đối với sự cập nhật được yêu cầu đối với dữ liệu tài khoản của người dùng thứ nhất 101. Bản tin này có thể bao gồm giá trị tương tác, các chứng thực người dùng thứ nhất 111, và mã xác thực một chiều thu được từ thiết bị người dùng thứ hai 122. Ví dụ, bản tin yêu cầu cập nhật có thể bao gồm số tiền giao dịch, thông tin thẻ thanh toán của người dùng thứ nhất 101, và mã xác thực chỉ dành cho tiền gửi của người dùng thứ hai 102. Khi nhận bản tin yêu cầu cập nhật, máy tính ủy quyền thứ nhất 131 có thể xác minh các chứng thực người dùng thứ nhất 111 bằng cách so sánh các chứng thực người dùng thứ nhất 111 với các bản ghi được lưu trữ trong cơ sở dữ liệu tài khoản thứ nhất 131A và xác định xem dữ liệu tài khoản cho các chứng thực người dùng thứ nhất 111 có tồn tại hay không dựa trên sự so khớp. Máy tính ủy quyền thứ nhất 131 còn có thể xác định xem sự cập nhật được yêu cầu có thể được ủy quyền hay không. Điều này có thể dẫn đến việc so sánh giá trị tương tác với tổng giá trị phân bổ được liên kết với tài khoản của người dùng thứ nhất 101 trong cơ sở dữ liệu tài khoản người dùng thứ nhất 131A và sau đó xác định xem tổng giá trị phân bổ có vượt quá giá trị tương tác mà sẽ được chuyển đến người dùng thứ hai 102 trong quá trình tương tác. Nói cách khác, máy tính ủy quyền thứ nhất 131 có thể xác định xem tài khoản của người dùng thứ nhất 101 đã được phân bổ đủ quỹ để trả số tiền giao dịch hay chưa. Nếu tổng giá trị phân bổ của người dùng thứ nhất 101 lớn hơn giá trị tương tác, máy tính ủy quyền 131 có thể xác định kết quả ủy quyền dương (nghĩa là ‘được chấp thuận’) và có thể tiến hành xử lý sự cập nhật được yêu cầu. Cần phải hiểu rằng số lượng quy trình đánh giá rủi ro và/hoặc xác thực bất kỳ có thể được áp dụng bởi máy tính ủy quyền

thứ nhất 131 khi xác định kết quả ủy quyền, và bản tin yêu cầu cập nhật có thể còn trải qua các quy trình đánh giá rủi ro và/hoặc xác thực bổ sung bởi máy chủ xử lý 140 và/hoặc máy tính ủy quyền thứ hai 132 sau đó trong quy trình cập nhật.

Một khi máy tính ủy quyền thứ nhất 131 đã chấp thuận sự cập nhật được yêu cầu, sau đó máy tính ủy quyền thứ nhất 131 có thể cam kết sự cập nhật của tài khoản của người dùng thứ nhất 101 trong cơ sở dữ liệu tài khoản thứ nhất 131A dựa trên giá trị tương tác và chuyển tiếp bản tin yêu cầu cập nhật đến máy chủ xử lý 140. Ví dụ, máy tính ủy quyền thứ nhất 131 có thể cam kết một phần số tiền bằng với số tiền giao dịch cho trước được quy định trong các chi tiết giao dịch. Theo một phương án, máy tính ủy quyền thứ nhất 131 có thể bao gồm kết quả ủy quyền trong bản tin yêu cầu cập nhật trước khi chuyển tiếp.

Sau đó máy chủ xử lý 140 có thể nhận bản tin yêu cầu cập nhật và có thể định danh mã xác thực một chiều được chứa ở trong đó. Sau đó máy chủ xử lý 140 có thể so sánh mã xác thực một chiều với các bản ghi được lưu trữ trong cơ sở dữ liệu mã xác thực 140A. Theo một phương án, máy chủ xử lý còn có thể sử dụng các chi tiết tương tác để cập nhật tốc độ tương tác được liên kết với mã xác thực một chiều trong cơ sở dữ liệu mã xác thực 140A, như bằng cách đánh giá các dấu thời gian tương tác, các bộ đếm tương tác, và các giá trị tương tác được liên kết với mã xác thực một chiều và tính toán số lượng tương tác hoặc tổng giá trị tương tác theo thời gian. Ví dụ, máy chủ xử lý 140 có thể tính toán tỷ lệ giao dịch hàng ngày dựa trên các giao dịch được ghi lại trước đó mà được liên kết với mã xác thực chỉ dành cho tiền gửi của người dùng thứ hai 102. Theo các ví dụ khác, các giao dịch được ghi lại có thể bao gồm số giao dịch trung bình trên một ngày, số giao dịch trung bình trên một tuần, tổng số tiền giao dịch trên một ngày, tổng số tiền giao dịch trên một tuần, một tháng, v.v.

Theo một phương án, tốc độ tương tác có thể được sử dụng bởi máy chủ xử lý 140 để thay đổi giá trị tương tác, như giảm số tiền giao dịch được chứa trong bản tin yêu cầu cập nhật. Ví dụ, máy chủ xử lý 140 có thể định danh một hoặc nhiều giới hạn tốc độ tương tác được xác định trước, mà có thể hoạt động như các ngưỡng dùng để trừ đi một hoặc nhiều khoản phí giao dịch. Sau đó các khoản phí giao dịch có thể được phân phối giữa máy tính ủy quyền thứ nhất 131, máy chủ xử lý 140, và/hoặc máy tính ủy quyền thứ hai 132 như là khoản thanh toán dùng để duy trì mạng và xử lý giao dịch. Như ví dụ, máy chủ xử lý 140 có thể khấu trừ 0,05% số tiền giao dịch cho tốc độ tương tác trên

\$50 một ngày trong khi chỉ khấu trừ 0,01% số tiền giao dịch cho tốc độ tương tác dưới \$50 một ngày. Cần phải hiểu rằng số lượng kết cấu phí bất kỳ có thể được thiết lập cho hệ thống 100, mà có thể được dựa trên tính khả dụng và/hoặc nhu cầu dùng để xử lý các tài nguyên được yêu cầu cho quy trình dữ liệu tương tác một cách an toàn. Tốc độ tương tác cũng có thể xác định xem có ngăn chặn việc hoàn thành giao dịch hay không dựa trên các giới hạn ngưỡng tốc độ trên được thiết lập trước đó.

Khi định danh mã xác thực chỉ dành cho tiền gửi trong bản tin yêu cầu cập nhật, máy chủ xử lý 140 có thể xác định người dùng tài khoản gắn liền với mã xác thực chỉ dành cho tiền gửi. Điều này có thể được dựa trên sự truy vấn cơ sở dữ liệu mã xác thực 140A, trong đó máy chủ xử lý 140 truy vấn mã định danh tài khoản mà gắn liền với mã xác thực chỉ dành cho tiền gửi. Mã định danh tài khoản gắn liền với mã xác thực chỉ dành cho tiền gửi có thể là mã định danh tài khoản mà có liên quan đến các chứng thực người dùng thứ hai 112. Ví dụ, mã định danh tài khoản có thể là số tài khoản chính có 16 chữ số của thẻ thanh toán của người dùng thứ hai 102, mà có thể đã được gán cho mã xác thực chỉ dành cho tiền gửi trong quy trình đăng ký được thực hiện bởi người dùng thứ hai 102, như được mô tả tiếp ở phần dưới.

Khi xác định mã định danh tài khoản gắn liền với mã xác thực chỉ dành cho tiền gửi, máy chủ xử lý 140 có thể định danh máy tính ủy quyền gắn liền với mã định danh tài khoản, như máy tính ủy quyền thứ hai 132. Ví dụ, 4 chữ số đầu tiên của số tài khoản chính có thể định danh thực thể ủy quyền cụ thể mà máy chủ xử lý 140 có thể chuyển tiếp bản tin yêu cầu cập nhật đến, sao cho máy tính ủy quyền thứ hai 132 có thể cập nhật sổ cái tài khoản của người dùng thứ hai 102 theo các chi tiết giao dịch.

Theo các phương án, máy chủ xử lý 140 có thể thay thế mã xác thực chỉ dành cho tiền gửi trong bản tin yêu cầu cập nhật với mã định danh tài khoản mà liên quan đến các chứng thực người dùng thứ hai 112, và có thể đệ trình bản tin yêu cầu cập nhật đến máy tính ủy quyền thứ hai được định danh 132. Máy tính ủy quyền thứ hai 132 có thể nhận bản tin yêu cầu cập nhật và, khi xác minh mã định danh tài khoản được bao gồm mà có liên quan đến các chứng thực người dùng thứ hai 112, có thể cập nhật tài khoản thứ hai cơ sở dữ liệu 132A dựa trên các chi tiết tương tác được chứa ở trong đó. Ví dụ, máy tính ủy quyền thứ hai 132 có thể truy vấn tài khoản thứ hai cơ sở dữ liệu 132A cho tài khoản được định danh bởi số tài khoản chính của người dùng thứ hai 102, và sau đó có thể cập nhật tài khoản của người dùng thứ hai này bằng cách sử dụng số tiền giao

dịch (nghĩa là bổ sung số tiền giao dịch vào số dư tài khoản của họ, trừ đi các khoản phí bất kỳ được tính toán bởi máy chủ xử lý 140).

Khi cập nhật tài khoản thứ hai cơ sở dữ liệu 132A, máy tính ủy quyền thứ hai 132 có thể gửi bản tin phản hồi cập nhật đến máy chủ xử lý 140 để xác nhận rằng những thay đổi thích hợp đã được thực hiện. Máy chủ xử lý 140 có thể nhận bản tin phản hồi cập nhật, và có thể chuyển tiếp bản tin phản hồi cập nhật với sự xác nhận đến máy tính ủy quyền thứ nhất 131. Máy chủ xử lý 140 còn có thể gửi thông báo xác nhận đến thiết bị người dùng thứ hai 122 mà việc cập nhật đã được xử lý theo các chi tiết tương tác được nhận. Theo một phương án, thông báo xác nhận có thể được gửi trực tiếp từ máy tính ủy quyền thứ hai 132 đến thiết bị người dùng thứ hai 122. Theo các phương án, máy tính ủy quyền thứ nhất 131 có thể nhận bản tin phản hồi cập nhật và cùng với sự xác nhận được cung cấp đồng thời từ máy chủ xử lý 140, và sau đó có thể thực hiện các cập nhật được cam kết trước đó cho cơ sở dữ liệu tài khoản thứ nhất 131A. Khi thực hiện việc cập nhật, máy tính ủy quyền thứ nhất 131 sau đó có thể gửi thông báo xác nhận đến thiết bị người dùng thứ nhất 121 rằng các cập nhật được yêu cầu đã được thực hiện, và do đó giao dịch được xử lý thành công.

Như có thể thấy được từ phần mô tả Fig.1 ở trên, hệ thống 100 cho phép xử lý các tương tác giữa người dùng thứ nhất và người dùng thứ hai. Điều này đạt được thông qua các cập nhật của các cơ sở dữ liệu tài khoản thứ nhất và các cơ sở dữ liệu tài khoản thứ hai bởi máy tính ủy quyền thứ nhất và máy tính ủy quyền thứ hai, một cách tương ứng. Các cập nhật được khởi tạo bởi sự truyền dẫn mã xác thực một chiều gắn liền với các bản ghi trong cơ sở dữ liệu mã xác thực. Hơn nữa, các giá trị tương tác đối với sự tương tác có thể được điều chỉnh giữa các máy tính ủy quyền bởi máy chủ xử lý dựa trên các tốc độ tương tác gắn liền với mã xác thực một chiều. Khi được áp dụng vào mạng thanh toán, có thể cho phép hạ thấp các khoản phí và làm giảm sự cản trở đối với các giao dịch giá trị nhỏ.

Fig.2 thể hiện máy chủ dùng để thuận tiện cho các cập nhật giữa các máy tính ủy quyền theo phương án sáng chế. Theo các phương án, máy chủ 200 có thể tương ứng với máy chủ xử lý 140 của Fig.1. Máy chủ 200 có thể bao gồm (các) bộ xử lý 210 dùng để thực thi các chỉ lệnh. Ví dụ, (các) bộ xử lý 210 có thể bao gồm số CPU và/hoặc GPU bất kỳ dùng để thực thi mã máy tính để thực hiện các chức năng hoặc các tác vụ. Máy chủ 200 có thể còn bao gồm giao diện mạng 220 dùng để nhận và truyền các bản tin dữ

liệu qua mạng. Ví dụ, giao diện mạng có thể bao gồm giao diện phần cứng hoặc ổ cắm mạng bất kỳ dùng để kết nối vào mạng có giao thức truyền thông cụ thể.

Máy chủ 200 có thể còn bao gồm phương tiện đọc được trên máy tính 230 mà lưu trữ các chỉ lệnh mà có thể được thực thi bởi bộ xử lý 210 để thực hiện các tác vụ. Ví dụ, phương tiện đọc được trên máy tính 230 có thể bao gồm một hoặc nhiều bộ nhớ lưu trữ dữ liệu, như bộ nhớ truy cập ngẫu nhiên (RAM), bộ nhớ truy cập ngẫu nhiên động (DRAM), và/hoặc phương tiện truy cập trực tiếp. Các chỉ lệnh của phương tiện đọc được trên máy tính 230 có thể được lưu trữ ở dưới dạng các môđun mã. Các môđun có thể bao gồm môđun xử lý bản tin cập nhật 230A, môđun xác định thực thể đang ủy quyền 230B, môđun tính toán tốc độ 230C, môđun điều chỉnh giá trị tương tác 230D, môđun truyền thông 230E, môđun xác thực 230F, môđun quản lý mã xác thực 230G, và môđun đăng ký 230H. Máy chủ 200 còn có thể truy cập vào một hoặc nhiều kho dữ liệu và/hoặc cơ sở dữ liệu ngoài, như cơ sở dữ liệu mã xác thực 200A.

Môđun xử lý bản tin cập nhật 230A có thể bao gồm mã dùng để đọc và sửa đổi dữ liệu trong các bản tin yêu cầu cập nhật và các bản tin phản hồi cập nhật. Môđun này có thể bao gồm mã dùng để nhận bản tin yêu cầu cập nhật từ máy tính ủy quyền và định danh các chi tiết tương tác được chứa ở trong đó. Theo các phương án, sự định danh các chi tiết tương tác có thể bao gồm sự xác định mã xác thực một chiều được lưu trữ trong các chi tiết tương tác. Mã có thể còn bao gồm các chỉ lệnh dùng để nhận bản tin phản hồi cập nhật từ máy tính ủy quyền và thông tin định danh được lưu trữ ở trong đó. Ví dụ, mã có thể bao gồm nhận thông báo xác nhận mà có thể được chuyển tiếp đến người dùng gắn liền với máy tính ủy quyền.

Môđun xác định máy tính ủy quyền 230B có thể bao gồm mã dùng để xác định một hoặc nhiều máy tính ủy quyền từ dữ liệu trong bản tin cập nhật. Môđun này có thể bao gồm các chỉ lệnh dùng để định danh mã định danh tài khoản và xác định máy tính ủy quyền gắn liền với mã định danh tài khoản. Ví dụ, mã định danh tài khoản có thể là số tài khoản gắn liền với nhà phát hành tài khoản cụ thể có một hoặc nhiều máy tính ủy quyền mà các bản tin cập nhật có thể được định tuyến đến.

Môđun tính toán tốc độ 230C có thể bao gồm mã dùng để tính toán tốc độ tương tác gắn liền với mã xác thực một chiều được nhận trong bản tin cập nhật. Sự tính toán tốc độ tương tác có thể được dựa trên các bản ghi được lưu trữ trong cơ sở dữ liệu mã

xác thực 200A. Ví dụ, môđun tính toán tốc độ 230C có thể bao gồm các chỉ lệnh để sử dụng lịch sử giao dịch được liên kết với mã xác thực một chiều để xác định số lượng tương tác được thực hiện bởi mã xác thực một chiều trong phân đoạn thời gian được định trước (ví dụ một ngày hoặc một tuần) và/hoặc có thể xác định tổng số tiền giao dịch được nhận bởi mã xác thực một chiều trong suốt phân đoạn thời gian đó.

Môđun điều chỉnh giá trị tương tác 230D có thể bao gồm mã dùng để xác định và thực thi các sự điều chỉnh giá trị tương tác cho các bản tin cập nhật đã nhận dữ liệu tương tác. Theo các phương án, các sự điều chỉnh giá trị tương tác có thể được xác định dựa trên các tốc độ tương tác gắn liền với mã xác thực một chiều trong tương tác. Theo một phương án, môđun điều chỉnh giá trị tương tác 230D có thể bao gồm các chỉ lệnh dùng để xác định giới hạn tốc độ được thiết lập trước, thực hiện sự điều chỉnh giá trị tương tác thứ nhất khi tốc độ tương tác thấp hơn giới hạn tốc độ, và thực hiện sự điều chỉnh giá trị tương tác thứ hai khi tốc độ tương tác cao hơn giới hạn tốc độ.

Môđun truyền thông 230E có thể bao gồm mã dùng để tạo ra, định dạng, và tái định dạng các bản tin dữ liệu được nhận qua giao diện mạng 220. Ví dụ, môđun truyền thông 230E có thể bao gồm mã dùng để tạo ra và định dạng các bản tin ISO 8583 mà truyền đạt thông tin giao dịch tài chính và các mã ủy quyền.

Môđun xác thực 230F có thể bao gồm mã dùng để thực hiện một hoặc nhiều quy trình xác thực. Ví dụ, môđun xác thực 230F có thể bao gồm mã dùng để thực thi một hoặc nhiều quy trình phân tích rủi ro và sự xác minh chứng thực.

Môđun quản lý mã xác thực 230G có thể bao gồm mã dùng để xác định và thay thế các mã xác thực được nhận trong các bản tin dữ liệu. Điều này có thể bao gồm mã dùng để định danh mã xác thực một chiều trong bản tin dữ liệu, mà truy vấn cơ sở dữ liệu mã xác thực cho thông tin tài khoản được liên kết với mã xác thực một chiều, và thay thế mã xác thực một chiều trong bản tin dữ liệu với mã định danh tài khoản mà gắn liền với mã xác thực một chiều theo thông tin tài khoản được truy vấn.

Môđun đăng ký 230H có thể bao gồm mã dùng để thực hiện quy trình đăng ký cho người dùng. Điều này có thể bao gồm mã dùng để nhận dữ liệu đăng ký, lưu trữ dữ liệu đăng ký trong cơ sở dữ liệu, tạo ra mã xác thực một chiều để liên kết với dữ liệu đăng ký, lưu trữ mã xác thực một chiều trong cơ sở dữ liệu, liên kết mã xác thực một chiều với dữ liệu đăng ký và/hoặc dữ liệu tài khoản trong cơ sở dữ liệu, và gửi bản tin

xác nhận đến người dùng và/hoặc thực thể ủy quyền gắn liền với dữ liệu tài khoản chứa dữ liệu đăng ký và mã xác thực một chiều.

Fig.3 thể hiện quy trình đăng ký với hệ thống mà sử dụng thiết bị chứng thực theo phương án sáng chế. Quá trình đăng ký 300 được thể hiện có thể là để đăng ký chấp nhận các giá trị tương tác trong hệ thống 100 của Fig.1. Ví dụ, quy trình đăng ký có thể là để đăng ký như người bán nhỏ lẻ mà chấp nhận các thanh toán đến tài khoản thẻ thanh toán của họ. Theo một phương án, quy trình đăng ký 300 có thể được thực hiện bởi người dùng thứ hai 102 của Fig.1.

Tại bước 1, người nhận (người nhận tiền) có thể nhập các chứng thực của họ và thông tin đăng ký vào thiết bị của họ. Theo một phương án, thông tin đăng ký có thể bao gồm bí danh, vị trí, và loại người dùng. Ví dụ, người nhận có thể nhập tên người bán, vị trí người bán, và mã danh mục người bán (MCC, merchant category code) mà có thể định danh người dùng như người bán nhỏ lẻ. Theo một phương án, các chứng thực của người nhận có thể bao gồm mã định danh tài khoản, như số tài khoản chính của tài khoản thẻ thanh toán của người nhận. Theo một phương án, thông tin đăng ký và các chứng thực có thể được nhập vào trong thiết bị mà sử dụng giao diện người dùng của ứng dụng di động được cung cấp bởi thực thể ủy quyền hoặc nhà cung cấp các giải pháp thanh toán. Theo phương án khác, các chứng thực có thể được truy xuất bởi ứng dụng di động từ phần được phân bổ của bộ nhớ trong thiết bị hoặc từ ứng dụng được lưu trữ khác.

Tại bước 2, người nhận gửi thông tin đăng ký đến máy tính ủy quyền gắn liền với người nhận. Theo một phương án, máy tính ủy quyền có thể được định danh dựa trên mã định danh tài khoản được nhập vào bởi người dùng. Ví dụ, ứng dụng di động có thể định tuyến bản tin dữ liệu (ví dụ bản tin yêu cầu đăng ký) đến máy tính ủy quyền của thực thể phát hành gắn liền với số tài khoản thanh toán của người nhận. Máy tính ủy quyền có thể là máy chủ mà có sự truy cập vào dữ liệu tài khoản của người nhận được lưu trữ trong cơ sở dữ liệu tài khoản. Ví dụ, máy tính ủy quyền có thể là một trong một vài máy tính của hệ thống ngân hàng của nhà phát hành mà duy trì các sổ cái tài khoản người dùng. Theo một phương án, dữ liệu đăng ký bản tin có thể bao gồm thẻ hoặc con trỏ khác mà có thể gắn liền với dữ liệu đăng ký.

Tại bước 3, máy tính ủy quyền lưu trữ bản ghi về thông tin đăng ký của người nhận và liên kết thông tin đến người nhận trong cơ sở dữ liệu tài khoản. Ví dụ, máy tính

ủy quyền có thể liên kết thẻ đăng ký của người nhận đến mã định danh tài khoản/tài khoản thẻ thanh toán của người nhận.

Tại bước 4, máy tính ủy quyền có thể tạo ra và gửi cuộc gọi API đăng ký đến máy chủ xử lý mà chứa thông tin đăng ký của người nhận và mã định danh tài khoản. Ví dụ, nhà phát hành của người nhận có thể sử dụng API được cung cấp bởi bộ xử lý các thanh toán thẻ mà cho phép nhà phát hành thực hiện sự đăng ký của người nhận vào trong hệ thống.

Tại bước 5, máy chủ xử lý có thể nhận cuộc gọi API và tạo ra mã xác thực một chiều để liên kết với thông tin đăng ký của người nhận và mã định danh tài khoản. Ví dụ, bộ xử lý các thanh toán thẻ có thể nhận cuộc gọi API đăng ký và sau đó có thể tạo ra mã xác thực chỉ dành cho tiền gửi mà được lưu trữ và được liên kết với thẻ đăng ký của người nhận, số thẻ thanh toán, và thông tin người bán trong cơ sở dữ liệu mã xác thực.

Tại bước 6, máy chủ xử lý có thể tạo ra và gửi bản tin phản hồi đăng ký bao gồm mã xác thực một chiều đến máy tính ủy quyền. Ví dụ, bộ xử lý các thanh toán thẻ có thể gửi phản hồi đến nhà phát hành của người nhận mà xác nhận sự đăng ký thành công của người nhận và chia sẻ mã xác thực chỉ dành cho tiền gửi của người nhận.

Tại bước 7, máy tính ủy quyền có thể chuyển tiếp phản hồi đăng ký đến người nhận. Ví dụ, nhà phát hành của người nhận có thể gửi phản hồi đăng ký qua kênh truyền thông được thiết lập giữa máy tính ủy quyền và thiết bị của người nhận. Sau đó thiết bị của người nhận có thể xử lý phản hồi đăng ký bằng ứng dụng di động được lưu trữ. Điều này có thể bao gồm việc truyền đạt sự xác nhận đăng ký đến người nhận (ví dụ hiển thị bản tin), việc lưu trữ mã xác thực một chiều trên thiết bị, tạo ra mã có thể đọc được bằng máy chứa thông tin mã xác thực một chiều, và việc hiển thị mã có thể đọc được bằng máy (ví dụ mã QR) đến người nhận. Sau đó người nhận có thể sử dụng mã xác thực một chiều để nhận tiền đến tài khoản thẻ thanh toán của họ, như bằng cách cho phép người gửi tiền quét mã QR để khởi tạo quy trình giao dịch. Các ví dụ về các quy trình giao dịch đã thể hiện được mô tả dưới đây.

Fig.4 thể hiện quy trình chuyển tiền đến tài khoản thẻ thanh toán mà sử dụng ứng dụng của nhà phát hành theo phương án sáng chế. Theo các phương án, các thực thể được thể hiện có thể đại diện cho hệ thống 100 của Fig.1, và các thiết bị, các máy tính,

và các máy chủ/ các máy chủ có thể tương ứng với các thiết bị, các máy tính, các máy chủ, và các cơ sở dữ liệu, được thể hiện trên Fig.1. Điều này có thể bao gồm sự tương tác được thực hiện giữa người dùng thứ nhất 101 như người trả tiền/người gửi và người dùng thứ hai 102 như người nhận tiền/người nhận. Sự tương tác có thể được xử lý như một chuỗi các cập nhật cơ sở dữ liệu giữa các thực thể phát hành của mỗi người dùng theo phân mô tả được bộc lộ ở đây.

Tham chiếu đến Fig.4, tại bước 1, sự tương tác được khởi tạo bởi người gửi mà sử dụng thiết bị của họ để thu được thông tin mã xác thực một chiều từ thiết bị của người nhận. Ví dụ, người trả tiền có thể khởi tạo giao dịch hoặc việc chuyển tiền bằng cách quét mã QR được hiển thị bởi thiết bị của người nhận tiền. Điều này có thể được thực hiện bằng cách sử dụng ứng dụng di động được cung cấp bởi nhà phát hành của người nhận tiền. Ví dụ, ứng dụng dịch vụ ngân hàng di động có thể được cài đặt lên thiết bị di động của người gửi, và có thể bao gồm giao diện dùng để kích hoạt chức năng máy ảnh của thiết bị và dùng để xử lý nhãn quang học có thể đọc được bằng máy được thu thập/được quét bởi máy ảnh khi được đặt ở chế độ xem. Nhãn quang học có thể đọc được bằng máy có thể là mã QR chứa thông tin mã xác thực chỉ dành cho tiền gửi. Khi xử lý mã QR và truy xuất mã xác thực một chiều được chứa ở trong đó, ứng dụng của nhà phát hành có thể khởi tạo yêu cầu cập nhật bằng cách sử dụng các chứng thực của người gửi và các chi tiết về sự tương tác. Ví dụ, ứng dụng của nhà phát hành có thể tạo ra bản tin yêu cầu cập nhật chứa các bit được phân bổ cho mỗi phần tử dữ liệu có liên quan đến giao dịch (ví dụ thông tin người gửi, mã xác thực người nhận, lượng, thời gian, v.v.). Các chứng thực có thể được truy cập bởi ứng dụng của nhà phát hành từ bộ nhớ và/hoặc được nhập thủ công vào bởi người gửi. Theo các phương án, các chứng thực có thể bao gồm mã định danh tài khoản cho tài khoản của người gửi mà từ đó giá trị tương tác có thể được khấu trừ. Ví dụ, các chứng thực thanh toán có thể bao gồm số tài khoản chính gắn liền với thẻ thanh toán dữ liệu tài khoản được duy trì bởi nhà phát hành, như dữ liệu giao dịch lịch sử và thông tin tương tự. Các chi tiết giao dịch có thể bao gồm số tiền giao dịch, giao dịch dấu thời gian và/hoặc ID giao dịch/mã định danh tương tác, cũng như thông tin mã xác thực một chiều thu được từ thiết bị của người nhận. Theo các phương án, một phần các chi tiết giao dịch có thể được tạo ra bởi ứng dụng của nhà phát hành, như dấu thời gian và mã định danh tương tác. Yêu cầu cập nhật sau đó có thể được

gửi bởi ứng dụng của nhà phát hành đến máy tính ủy quyền có khả năng cập nhật các bản ghi tài khoản của người gửi.

Tại bước 2, máy tính ủy quyền gắn liền với tài khoản của người gửi nhận yêu cầu cập nhật và khởi tạo quy trình cập nhật trong hệ thống. Ví dụ, máy tính ủy quyền có thể truy cập cơ sở dữ liệu tài khoản mà lưu trữ dữ liệu tài khoản của người gửi, và có thể cam kết cập nhật cơ sở dữ liệu mà phản ánh các chi tiết giao dịch được nhận (ví dụ khấu trừ số tiền giao dịch từ tài khoản của người dùng và liên kết sự khấu trừ với dấu thời gian và/hoặc ID giao dịch). Khi cam kết nhập mục cập nhật trong cơ sở dữ liệu, máy tính ủy quyền có thể tìm kiếm sự xác minh/xác thực cập nhật từ các bên có liên quan khác trong hệ thống xử lý tương tác. Ví dụ, thanh toán đầy OCT hoặc việc chuyển tiền phù hợp khác có thể được khởi tạo với nhà cung cấp xử lý các thanh toán trung gian/bộ xử lý các thanh toán thẻ và máy tính ủy quyền của nhà phát hành tài khoản của người nhận thanh toán. Theo các phương án, điều này có thể liên quan đến việc chuyển tiếp bản tin yêu cầu cập nhật và thông tin được chứa ở trong đó đến máy chủ xử lý của bộ xử lý thanh toán thẻ.

OCT (Giao dịch tín dụng gốc, Original Credit Transaction) thường là giao dịch tín dụng bù trừ và quyết toán mà được thiết kế để sử dụng trong các ứng dụng kinh doanh như chuyển tiền kinh doanh hoặc các sự hoàn trả giữa doanh nghiệp-với-người tiêu dùng. Khi được sử dụng trong bối cảnh của sáng chế để chuyển tiền, OCT là giao dịch được sử dụng để chuyển tiền đến tài khoản của người nhận.

Số tiền OCT là số tiền mà được thỏa thuận bởi người gửi và nhà cung cấp dịch vụ theo đơn vị tiền tệ đã thỏa thuận. Nếu đơn vị tiền tệ trong hóa đơn của người nhận khác với đơn vị tiền tệ đã thỏa thuận tại thời điểm giao dịch, việc chuyển đổi đơn vị tiền tệ có thể được thực hiện trên OCT và lượng tiền chính xác được ghi có vào tài khoản của người nhận có thể không được biết đến tại thời điểm giao dịch. Trong một số trường hợp, trong trường hợp giao dịch chéo đơn vị tiền tệ, để tránh nhầm lẫn trong việc xác định số tiền chính xác để ghi có vào trong tài khoản của người nhận, sự chuyển đổi đơn vị tiền tệ có thể được thực hiện bởi khách gửi trước khi đệ trình giao dịch đến máy tính thanh toán xử lý. Theo một số phương án, OCT chỉ mang số tài khoản của người nhận và không mang thông tin về người gửi. Chỉ báo đặc biệt định danh OCT cho ngân hàng phát hành của người nhận. Việc trao đổi có thể đi từ bên cung cấp dịch vụ thanh toán

đến nhà phát hành của người nhận, như trong giao dịch mua bán thông thường. Việc thanh toán có thể diễn ra trong vòng vài ngày.

Tại bước 3, máy chủ xử lý nhận bản tin yêu cầu cập nhật và sửa đổi nó dựa trên các bản ghi mã xác thực một chiều. Theo các phương án, sự sửa đổi có thể bao gồm: phân tích bản tin yêu cầu cập nhật để xác định mã xác thực một chiều, thay thế mã xác thực một chiều trong các chi tiết tương tác với mã định danh tài khoản người dùng thứ hai, và điều chỉnh giá trị tương tác trong bản tin yêu cầu cập nhật dựa trên tốc độ tương tác đã tính. Ví dụ, máy chủ xử lý có thể truy vấn cơ sở dữ liệu mã xác thực cho các bản ghi được liên kết với mã xác thực một chiều, mà có thể bao gồm dữ liệu người bán của người nhận và số tài khoản thẻ thanh toán (mã định danh tài khoản). Máy chủ xử lý sau đó có thể sử dụng các bản ghi lịch sử như bản ghi mã xác thực một chiều để tính toán tốc độ giao dịch được liên kết, như bằng cách sử dụng các dấu thời gian và số tiền giao dịch để tính toán số tiền giao dịch hàng ngày được nhận một ngày. Tốc độ giao dịch có liên quan có thể được so sánh với ngưỡng để thực hiện sự điều chỉnh giá trị tương tác, như các giá trị nhỏ nhất/lớn nhất để áp dụng các mức giảm giá trị giao dịch khác nhau và/hoặc phân bổ lại. Sau đó, để sửa đổi bản tin yêu cầu cập nhật, máy chủ xử lý có thể thay thế mã xác thực một chiều với số thẻ thanh toán của người nhận và điều chỉnh giá trị tương tác cho phù hợp. Máy chủ xử lý còn có thể cập nhật các bản ghi mã xác thực một chiều trong cơ sở dữ liệu mã xác thực để phản ánh giao dịch hiện tại.

Tại bước 4, máy chủ xử lý gửi bản tin yêu cầu cập nhật đã sửa đổi đến máy tính ủy quyền (máy tính ủy quyền thứ hai) gắn liền với tài khoản của người nhận, như được định danh bởi mã định danh tài khoản người dùng thứ hai được xác định ở bước 3. Ví dụ, máy chủ xử lý có thể so sánh các chi tiết giao dịch của người nhận (ví dụ số tài khoản và vị trí) đến thư mục của các địa chỉ định tuyến liên quan đến các máy tính ủy quyền mà hoạt động như các nút trong hệ thống thanh toán. Theo các phương án, máy tính ủy quyền thứ hai có thể là máy chủ của ngân hàng phát hành của người nhận, mà có thể có truy cập đến các bản ghi tài khoản thanh toán của người nhận. Máy tính ủy quyền thứ hai có thể nhận bản tin yêu cầu cập nhật, cập nhật tài khoản của người nhận theo các chi tiết tương tác được chứa ở trong đó, và có thể tạo ra bản tin phản hồi cập nhật. Ví dụ, máy tính ủy quyền thứ hai có thể cập nhật số dư tài khoản của người nhận trong cơ sở dữ liệu tài khoản và bổ sung các chi tiết giao dịch đến lịch sử giao dịch của người nhận. Theo một phương án, bản tin phản hồi cập nhật có thể bao gồm dữ liệu người bán hoặc

thông tin thẻ gắn liền với mã xác thực một chiều cho giao dịch, bao gồm tên người bán, vị trí người bán, và/hoặc mã danh mục người bán (MCC). Dữ liệu người bán và/hoặc thông tin thẻ có thể bao gồm thông tin người bán được đăng ký gắn liền với người nhận trong quy trình đăng ký, như trong quy trình được mô tả trên Fig.3.

Tại bước 5, máy tính ủy quyền thứ hai gửi người nhận thông báo rằng các cập nhật tài khoản đã được thực hiện và sự tương tác đã được xử lý. Ví dụ, máy tính ủy quyền thứ hai có thể định danh thiết bị gắn liền với tài khoản của người dùng thứ hai, như bằng cách truy vấn thiết bị hoặc ứng dụng mã định danh được liên kết với thẻ người bán của người nhận, và sau đó có thể gửi thông báo với các chi tiết giao dịch và cập nhật đến thiết bị của người nhận. Theo một phương án, thông báo có thể được nhận bởi người nhận trên thiết bị của họ từ ứng dụng của nhà phát hành, mà có thể giống hoặc tương tự như ứng dụng được sử dụng bởi người gửi, và mà cũng có thể là ứng dụng cung cấp phương tiện để hiển thị/gửi mã xác thực một chiều đến người gửi khi sự tương tác được khởi tạo. Theo phương án sáng chế, ứng dụng của nhà phát hành có thể là cùng ứng dụng mà được sử dụng bởi người nhận trong quy trình đăng ký 300 được minh họa bởi Fig.3.

Tại bước 6, máy tính ủy quyền thứ hai có thể gửi bản tin phản hồi cập nhật được tạo ra ở bước 4 đến máy chủ xử lý để chuyển tiếp đến máy tính ủy quyền của người gửi (máy tính ủy quyền thứ nhất). Máy tính ủy quyền thứ nhất có thể nhận bản tin phản hồi cập nhật và có thể thực hiện cập nhật được cam kết. Ví dụ, máy tính ủy quyền thứ nhất có thể thực thi việc giảm số dư tài khoản của người gửi theo số tiền giao dịch đang chờ xử lý ban đầu. Theo một phương án, sự cập nhật có thể bao gồm việc bổ sung dữ liệu người bán vào các chi tiết giao dịch, sao cho người gửi có thể xem và xác minh thông tin người bán trong lịch sử giao dịch họ tại thời điểm sau đó.

Tại bước 7, máy tính ủy quyền thứ nhất gửi thông báo đến người gửi rằng việc cập nhật đã được thực hiện và sự tương tác được xử lý. Ví dụ, máy tính ủy quyền thứ nhất có thể gửi thông báo xác nhận với các chi tiết giao dịch đến ứng dụng của nhà phát hành trên thiết bị của người gửi. Theo các phương án khác, quy trình tương tác tương tự có thể được thực hiện trên ứng dụng của bên thứ ba, như ứng dụng của nhà cung cấp các thanh toán thẻ hoặc nhà cung cấp ví số, như được mô tả dưới đây.

Fig.5 thể hiện quy trình chuyển tiền đến tài khoản thẻ thanh toán mà sử dụng bộ xử lý thanh toán ứng dụng theo phương án sáng chế. Theo các phương án, quy trình được thể hiện có thể tương ứng với quy trình liên quan đến các bên giống nhau như đã tham gia vào trong quy trình của Fig.4. Trong quy trình trên Fig.5, máy chủ xử lý có thể thông báo cho người nhận, thay cho máy tính ủy quyền thứ hai như theo phương án trên Fig.4.

Tại bước 1 người trả tiền/người gửi khởi tạo giao dịch sau khi quét của thông tin người bán của người nhận. Ví dụ, người trả tiền có thể quét mã QR được hiển thị trên thiết bị di động của người nhận, mà có thể báo hiệu cho thiết bị của người trả tiền để yêu cầu việc chuyển tiền theo số tiền giao dịch đã thỏa thuận.

Tại bước 2, nhà phát hành của người gửi nhận thông tin giao dịch và gửi việc chuyển tiền đến máy chủ xử lý. Ví dụ, nhà phát hành của người gửi có thể cam kết hoặc phân bổ một phần quỹ để trả số tiền giao dịch và có thể thông báo cho các bộ xử lý thanh toán trung gian đầy quỹ được phân bổ đến các sổ cái của ngân hàng phát hành khác.

Tại bước 3, máy chủ xử lý truy xuất mã định danh tài khoản được liên kết với mã xác thực một chiều được bao gồm trong thông tin giao dịch. Ví dụ, mã xác thực chỉ dành cho tiền gửi được chuyển thông qua mã QR người bán của người nhận có thể được sử dụng để truy vấn thông tin thẻ người bán. Thông tin thẻ người bán có thể gắn liền với thông tin đăng ký của người nhận trong cơ sở dữ liệu mã xác thực, như số thẻ thanh toán của người nhận (PAN), tên người bán được đăng ký, vị trí người bán, và mã danh mục người bán, và lịch sử giao dịch. Sau đó máy chủ xử lý có thể sửa đổi việc chuyển tiền theo các tính toán phí được xác định trước mà tương ứng với việc đặt các giới hạn tốc độ giao dịch được gắn liền với những người nhận có khối lượng giao dịch hàng ngày khác nhau, chuyển giá trị hàng ngày, hoặc số liệu dựa trên tần suất tương tác khác.

Tại bước 4, sau đó máy chủ xử lý có thể chuyển tiếp việc chuyển tiền với thông tin giao dịch được cập nhật đến nhà phát hành của người nhận. Việc chuyển tiền có thể bao gồm thông tin người bán người nhận (nghĩa là số thẻ thanh toán, tên người bán, vị trí, MCC, v.v.) cũng như số tiền giao dịch có tính phí.

Tại bước 5, nhà phát hành của người nhận cập nhật cơ sở dữ liệu tài khoản bao gồm việc cập nhật dữ liệu tài khoản của người nhận. Ví dụ, ngân hàng của người nhận

có thể bổ sung số tiền giao dịch đã giảm vào số dư tài khoản của họ, và có thể cập nhật tài khoản tiền gửi được phân bổ của chính nó để thu phần khoản phí đã tính của nó.

Tại bước 6, nhà phát hành của người nhận gửi bản tin phản hồi đến máy chủ xử lý, mà cũng có thể khởi tạo thông báo sẽ được gửi đến người nhận rằng giao dịch đã được xử lý thành công. Ví dụ, nhà phát hành của người nhận có thể khởi tạo cuộc gọi API đến máy chủ xử lý, mà có thể chuyển tiếp xác nhận thanh toán được xử lý đến người nhận mà sử dụng ví số đã được cung cấp hoặc ứng dụng thanh toán của bên thứ ba khác.

Tại bước 7, máy chủ xử lý chuyển tiếp bản tin phản hồi đến nhà phát hành của người gửi. Ví dụ, máy chủ xử lý có thể xác nhận với nhà phát hành của người gửi rằng quỹ được chuyển thành công và nhà phát hành của người gửi có thể cập nhật các số cái của họ cho phù hợp.

Tại bước 8, nhà phát hành của người gửi gửi thông báo đến người gửi rằng giao dịch đã được xử lý thành công. Ví dụ, người gửi có thể gửi thông báo xác nhận đến thiết bị của người gửi thông qua ứng dụng thanh toán được sử dụng để khởi tạo giao dịch.

Các phương án sáng chế mang lại một số hiệu quả kỹ thuật. Các phương án sáng chế cho phép các máy tính trong mạng xử lý thanh toán để đánh giá tác động của nút nhận cụ thể lên lưu lượng mạng và có thể thu phí mạng có thể thay đổi cho phù hợp, do đó cung cấp cơ hội cho các người bán nhỏ hơn và chấp nhận giá trị giao dịch nhỏ ở trong mạng. Hơn nữa, các phương án đề xuất mã xác thực một chiều (ví dụ chỉ dành cho tiền gửi) mà chỉ hợp lệ cho một hướng chuyển giá trị tương tác, do đó cho phép người dùng nhận tiền kỹ thuật số vào các tài khoản thẻ thanh toán của họ mà không tiết lộ các số thẻ thanh toán của họ hoặc cung cấp cho người khác (ví dụ các tin tặc hoặc tội phạm) với phương tiện dùng để sử dụng mã xác thực để rút tiền. Do đó, người dùng có thể dễ dàng nhận các khoản thanh toán đến các tài khoản thẻ thanh toán sẵn có của họ theo cách hiệu quả và an toàn.

Các thành phần phần mềm hoặc các chức năng bất kỳ được mô tả trong sáng chế này đều có thể được triển khai dưới dạng mã phần mềm được thực thi bởi bộ xử lý bằng cách sử dụng ngôn ngữ máy tính phù hợp bất kỳ như, ví dụ, Java, C++ hoặc Perl mà sử dụng, ví dụ, các kỹ thuật thông thường hoặc các kỹ thuật hướng đối tượng. Mã phần mềm có thể được lưu trữ như chuỗi các chỉ lệnh, hoặc các câu lệnh trên phương tiện đọc được trên máy tính, như bộ nhớ truy cập ngẫu nhiên (RAM), bộ nhớ chỉ đọc (ROM),

phương tiện từ tính như ổ cứng hoặc ổ đĩa mềm, hoặc phương tiện quang như CD-ROM. Phương tiện đọc được trên máy tính bất kỳ có thể nằm trên hoặc ở trong một thiết bị điện toán, và có thể có mặt trên hoặc ở trong các thiết bị điện toán khác nhau ở trong hệ thống hoặc mạng.

Mặc dù các phương án ví dụ nhất định đã được mô tả chi tiết và được thể hiện trong các hình vẽ kèm theo, nhưng cần phải hiểu rằng các phương án này chỉ mang tính minh họa và không nhằm giới hạn phạm vi sáng chế, và sáng chế không bị giới hạn ở các sắp xếp và cấu tạo cụ thể được thể hiện và được mô tả, vì nhiều biến thể khác có thể xuất hiện đối với người có hiểu biết trung bình trong lĩnh vực kỹ thuật này.

Như được sử dụng ở trong bản mô tả này, việc sử dụng các mạo từ số ít có ý nghĩa là "ít nhất một", trừ khi được chỉ thị cụ thể điều trái ngược lại.

YÊU CẦU BẢO HỘ

1. Phương pháp cung cấp bảo mật dữ liệu bằng cách sử dụng mã xác thực một chiều, phương pháp này bao gồm các bước:

quét bởi thiết bị người dùng thứ nhất của người dùng thứ nhất nhãn quang có thể đọc được bằng máy được hiển thị trên thiết bị người dùng thứ hai (122) của người dùng thứ hai (102), trong đó nhãn quang có thể đọc được bằng máy có chứa mã xác thực một chiều;

ứng dụng của nhà phát hành trên thiết bị người dùng thứ nhất khởi tạo bản tin yêu cầu cập nhật bao gồm mã xác thực một chiều và gửi bản tin yêu cầu cập nhật tới máy tính ủy quyền thứ nhất (131);

nhận, bởi máy chủ xử lý (140) từ máy tính ủy quyền thứ nhất (131), bản tin yêu cầu cập nhật bao gồm yêu cầu giao tiếp cho giao tiếp giữa người dùng thứ nhất (101) và người dùng thứ hai (102), yêu cầu giao tiếp bao gồm các chi tiết tương tác bao gồm mã xác thực một chiều và giá trị tương tác, sự tương tác mà chuyển giá trị tương tác từ người dùng thứ nhất (101) đến người dùng thứ hai (102);

phân tích, bởi máy chủ xử lý (140), bản tin yêu cầu cập nhật để xác định mã xác thực một chiều;

xác định, bởi máy chủ xử lý (140), mã định danh tài khoản người dùng thứ hai cho tài khoản thứ hai của người dùng thứ hai từ mã xác thực một chiều;

thay thế, bởi máy chủ xử lý (140), mã định danh tài khoản người dùng thứ hai cho mã xác thực một chiều trong các chi tiết tương tác để bao gồm mã định danh tài khoản người dùng thứ hai trong bản tin yêu cầu cập nhật;

xác định, bởi máy chủ xử lý (140), máy tính ủy quyền thứ hai (132) gắn liền với mã định danh tài khoản người dùng thứ hai;

gửi, bởi máy chủ xử lý (140), bản tin yêu cầu cập nhật đến máy tính ủy quyền thứ hai; và

nhận, bởi máy chủ xử lý (140), bản tin phản hồi cập nhật từ máy tính ủy quyền thứ hai (132), trong đó máy tính ủy quyền thứ hai cập nhật tài khoản thứ hai của người dùng thứ hai (102) dựa trên các chi tiết tương tác.

2. Phương pháp theo điểm 1, trong đó mã xác thực một chiều có định dạng dữ liệu giống như mã định danh tài khoản người dùng thứ hai.

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

xác định, bởi máy chủ xử lý (140), tốc độ tương tác của mã xác thực một chiều, trong đó tốc độ tương tác là số lượng tương tác trung bình trên một ngày hoặc tổng giá trị tương tác đã nhận trên một ngày; và

điều chỉnh, bởi máy chủ xử lý (140), giá trị tương tác trong bản tin yêu cầu cập nhật dựa trên tốc độ tương tác.

4. Phương pháp theo điểm 3, trong đó các chi tiết tương tác bao gồm dấu thời gian và mã định danh giao dịch.

5. Phương pháp theo điểm 4, còn bao gồm bước:

cập nhật cơ sở dữ liệu mã xác thực (140A) với các chi tiết tương tác, trong đó tốc độ tương tác cho mã xác thực một chiều được xác định bằng cách sử dụng các bản ghi gắn liền với mã xác thực một chiều trong cơ sở dữ liệu mã xác thực (140A) để tính toán tổng giá trị tương tác theo phân đoạn thời gian.

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

truyền bản tin phản hồi cập nhật từ máy chủ xử lý (140) đến máy tính ủy quyền thứ nhất (131).

7. Phương pháp theo điểm 1, trong đó trước khi máy chủ nhận bản tin yêu cầu cập nhật, máy tính ủy quyền thứ nhất (131) phân bổ một phần số tiền của quỹ của tài khoản thứ nhất của người dùng thứ nhất dựa trên các chi tiết tương tác, và trong đó sau khi máy chủ xử lý (140) nhận bản tin phản hồi cập nhật máy tính ủy quyền thứ nhất (131) thực hiện việc giảm trong tài khoản thứ nhất theo các chi tiết tương tác đang chờ xử lý.

8. Phương pháp theo điểm 1, còn bao gồm bước:

nhận, bởi máy chủ xử lý (140), bản tin yêu cầu đăng ký bao gồm mã định danh tài khoản người dùng thứ hai và dữ liệu người dùng thứ hai;

tạo ra, bởi máy chủ xử lý (140), mã xác thực một chiều;

liên kết, bởi máy chủ xử lý (140), mã xác thực một chiều đến mã định danh tài khoản người dùng thứ hai; và

gửi, bởi máy chủ xử lý (140), bản tin phản hồi đăng ký bao gồm mã xác thực một chiều đến thiết bị người dùng thứ hai của người dùng thứ hai.

9. Phương pháp theo điểm 8, trong đó bản tin phản hồi cập nhật bao gồm dữ liệu người dùng thứ hai.

10. Máy chủ xử lý (140) bao gồm:

nhiều thiết bị được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm nêu trên.

100

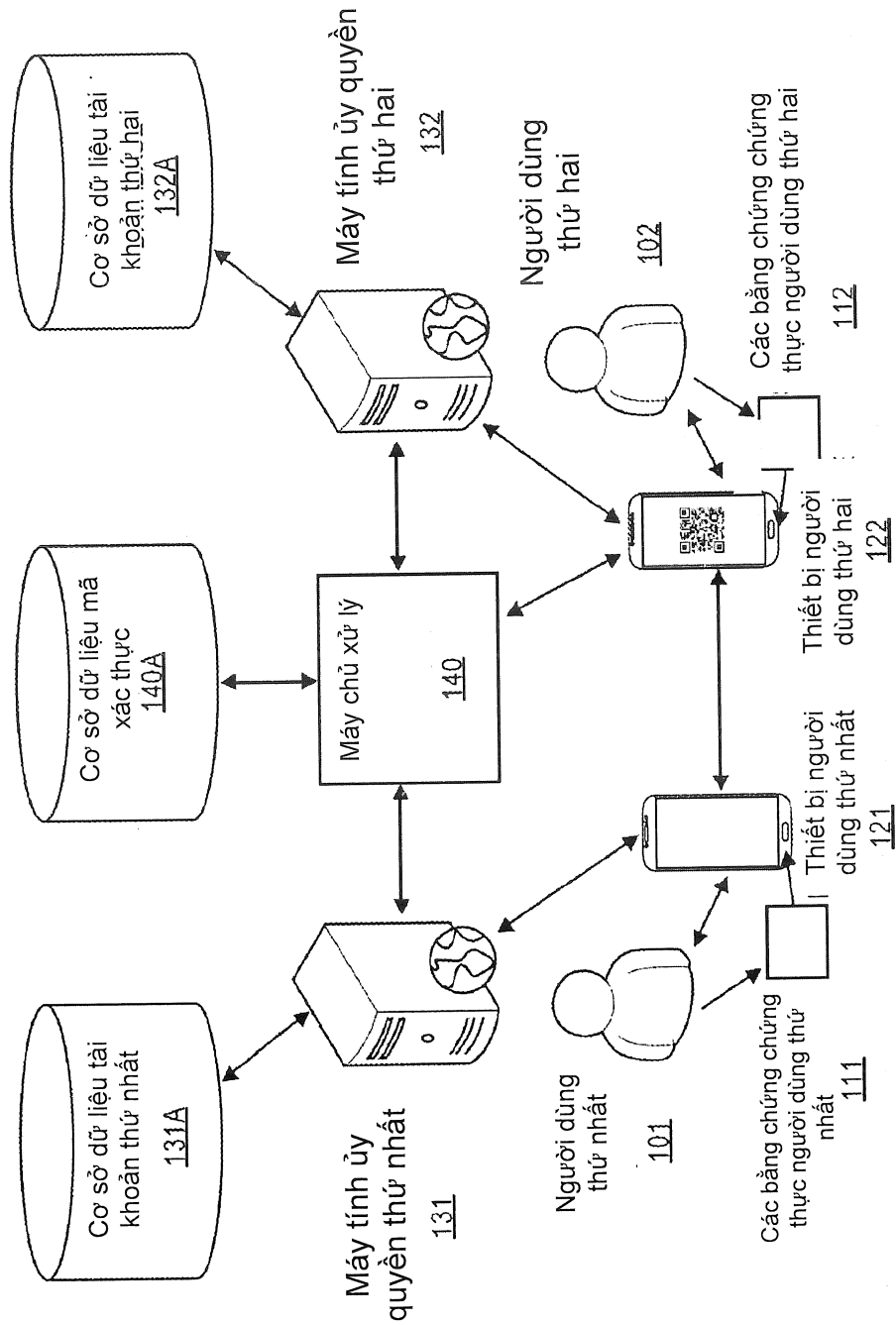


Fig.1

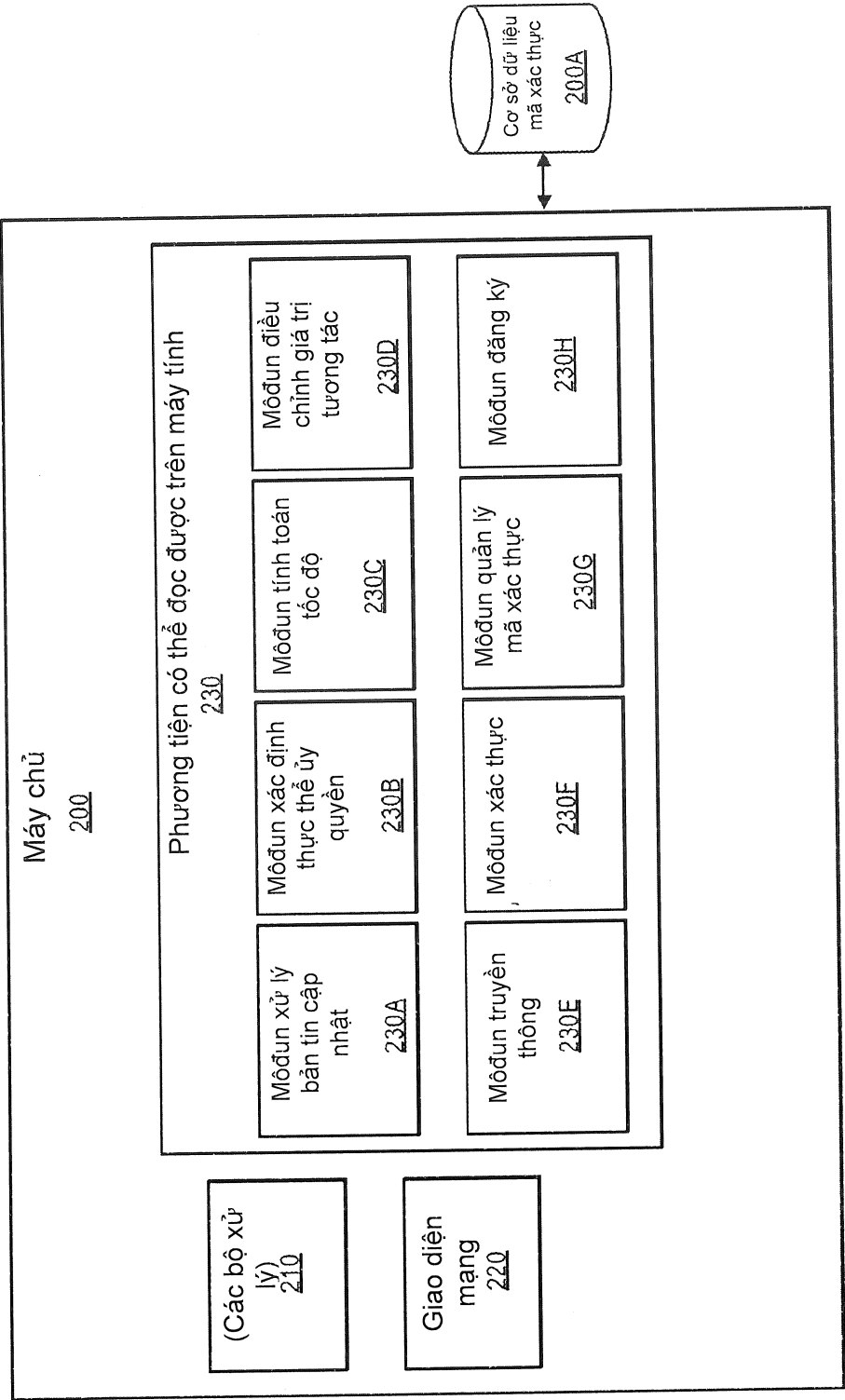


Fig.2

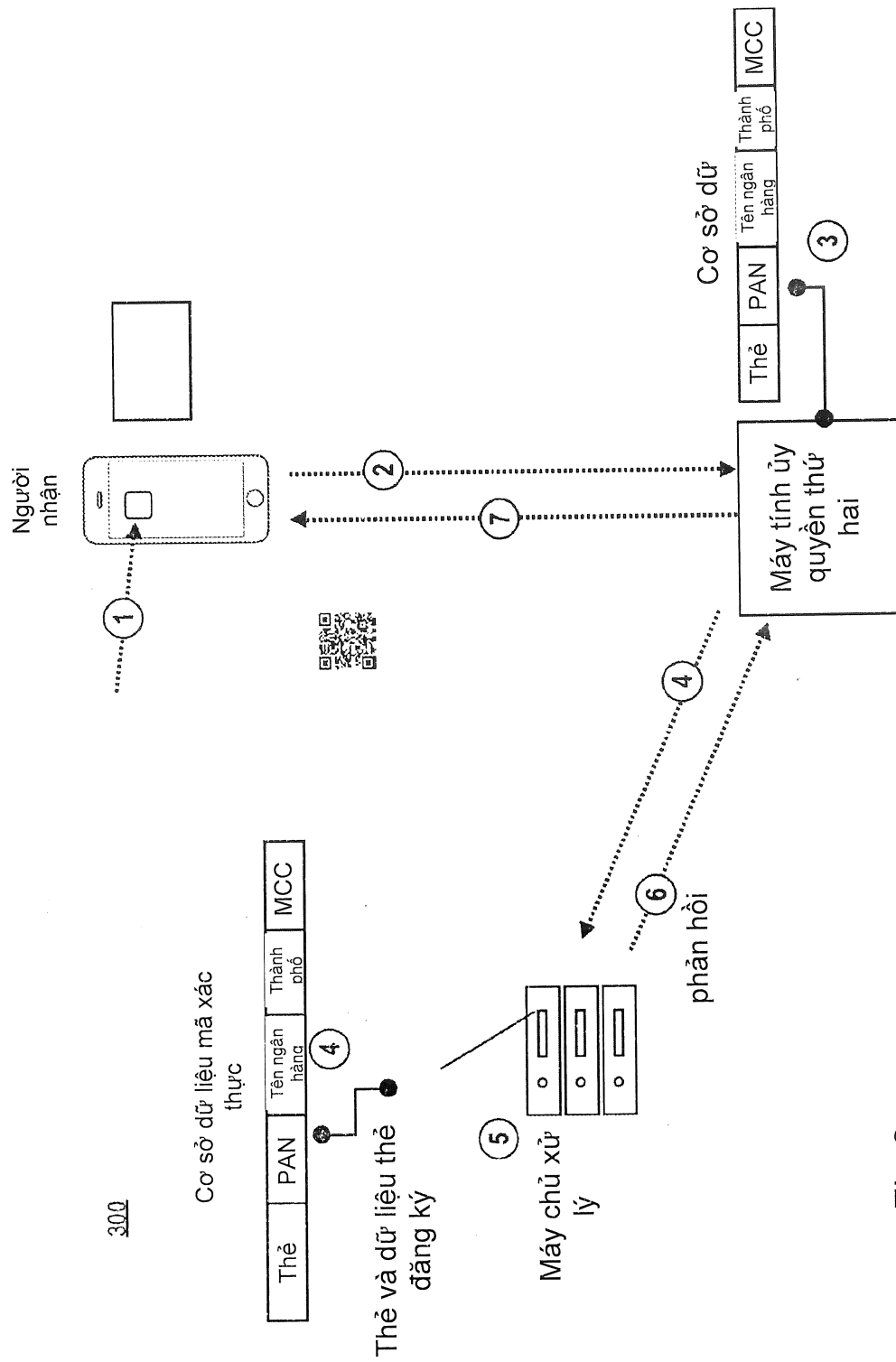


Fig.3

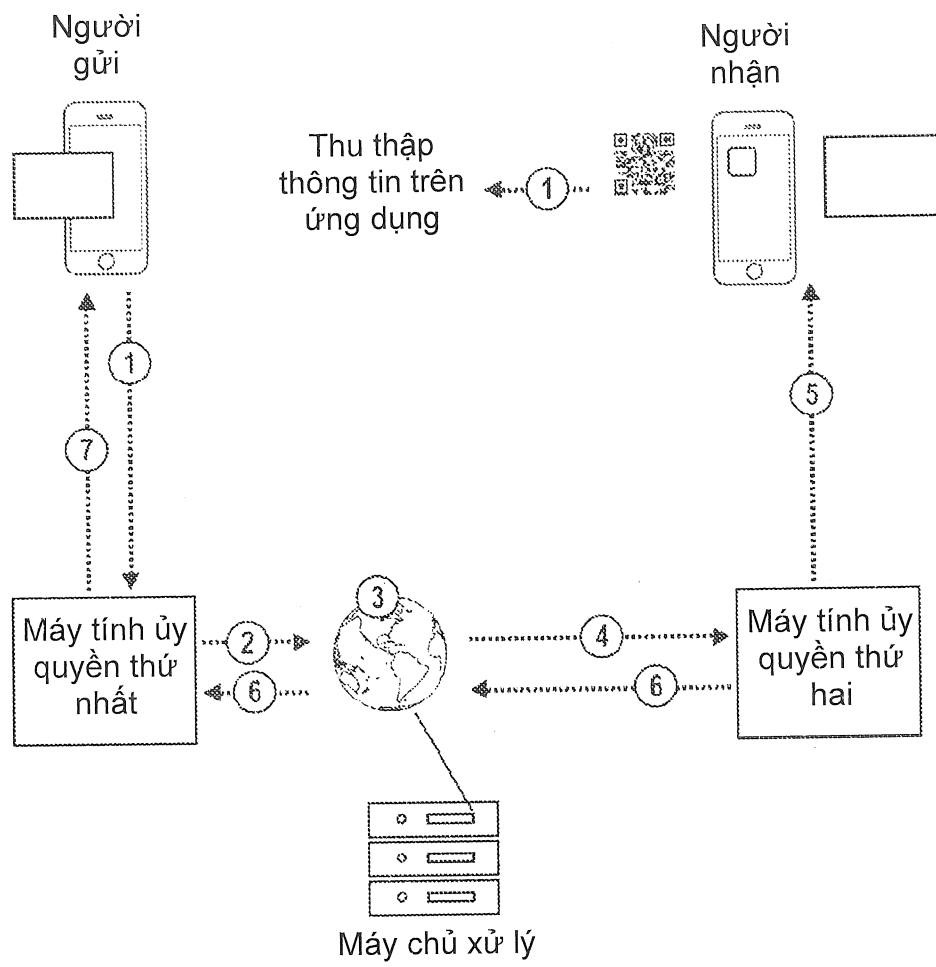


Fig.4

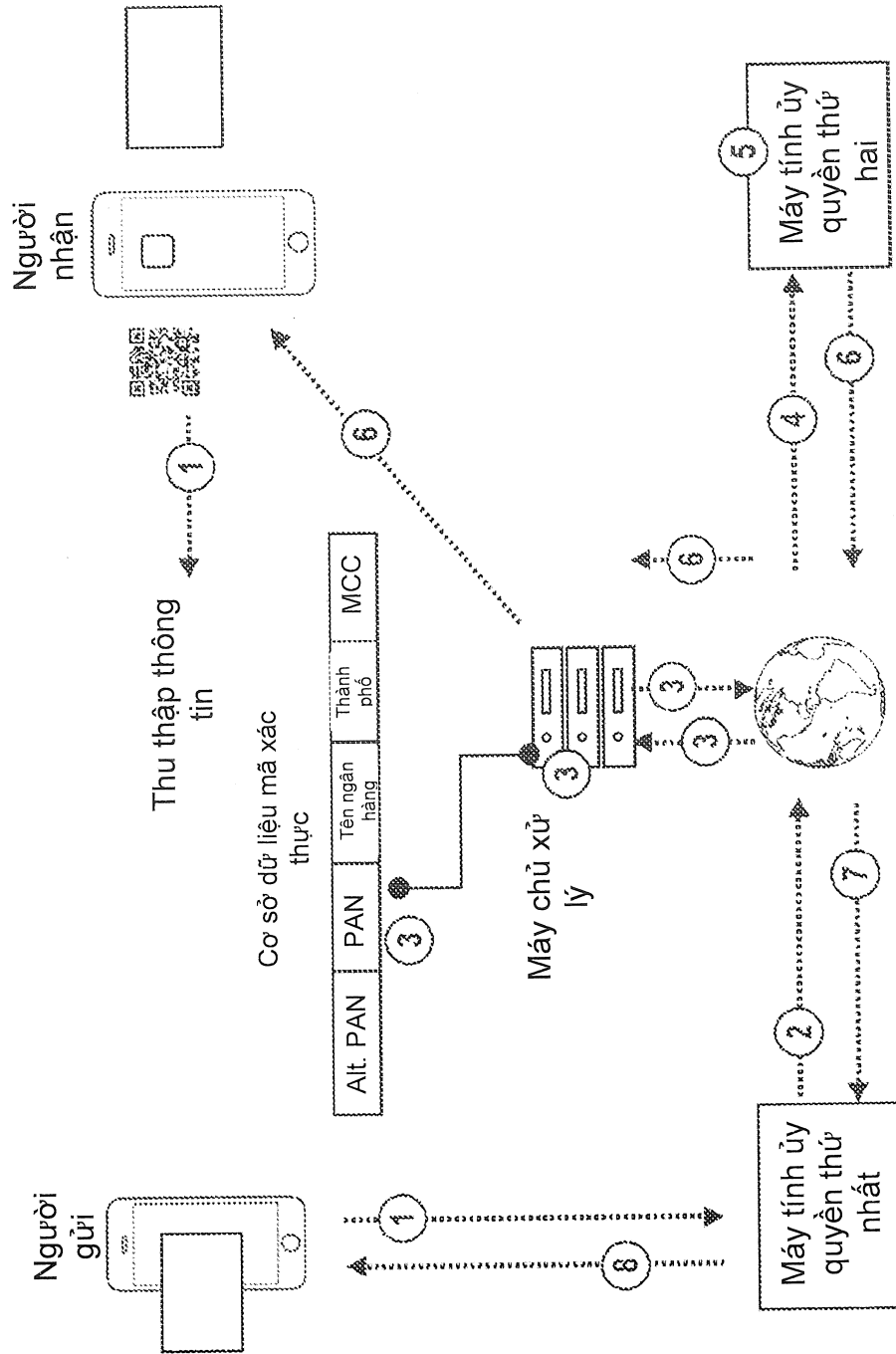


Fig.5