



(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)



1-0033788

(51)^{2020.01} H04L 29/06

(13) B

(21) 1-2019-04103

(22) 21/12/2018

(86) PCT/CN2018/122559 21/12/2018

(87) WO 2019/072301 18/04/2019

(45) 25/10/2022 415

(43) 25/05/2020 386ASC

(73) Advanced New Technologies Co., Ltd. (KY)

Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands

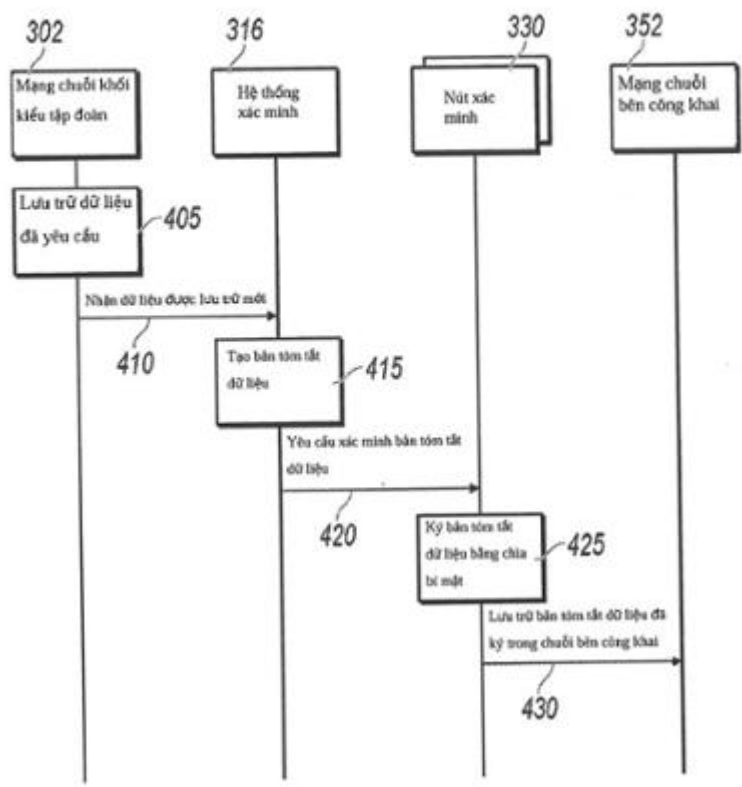
(72) CHENG, Long (CN); LI, Yanpeng (CN); FENG, Zhiyuan (CN).

(74) Công ty TNHH Tâm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG XÁC MINH TÍNH TOÀN VỆ CỦA DỮ LIỆU ĐƯỢC LƯU TRỮ TRONG CHUỖI KHỐI KIỂU TẬP ĐOÀN SỬ DỤNG CHUỖI BÊN CÔNG KHAI VÀ VẬT GHI ĐỌC ĐƯỢC BỞI MÁY TÍNH

(57) Sáng chế đề cập đến phương pháp, hệ thống xác minh tính toàn vẹn của dữ liệu được lưu trữ trong chuỗi khối kiểu tập đoàn sử dụng chuỗi bên công khai và vật ghi đọc được bởi máy tính. Phương pháp bao gồm lưu trữ mục dữ liệu trong chuỗi khối kiểu tập đoàn; tạo ra bản tóm tắt dữ liệu thứ nhất trên cơ sở mục dữ liệu được lưu trữ; gửi bản tóm tắt dữ liệu thứ nhất cho nút xác minh để ký nó theo cách mã hóa và lưu trữ bản tóm tắt dữ liệu thứ nhất đã ký trong chuỗi khối công khai; nhận yêu cầu để truy hồi mục dữ liệu được lưu trữ; truy hồi mục dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn; tạo ra bản tóm tắt dữ liệu thứ hai trên cơ sở mục dữ liệu được truy hồi; gửi bản tóm tắt dữ liệu thứ hai cho nút xác minh sao cho mỗi nút xác minh ký bản tóm tắt dữ liệu thứ hai; nhận bản tóm tắt dữ liệu thứ hai đã ký từ các nút xác minh; truy hồi bản tóm tắt dữ liệu thứ nhất đã ký từ chuỗi khối công khai; xác định rằng bản tóm tắt dữ liệu thứ nhất đã ký so khớp bản tóm tắt dữ liệu thứ hai đã ký; và gửi đáp ứng chỉ báo mục dữ liệu được lưu trữ không bị thay đổi đến yêu cầu để truy hồi mục dữ liệu được lưu trữ.

400



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp và hệ thống xác minh tính toàn vẹn của dữ liệu được lưu trữ trong chuỗi khối kiểu tập đoàn sử dụng chuỗi bên công khai. Sáng chế còn đề cập đến vật ghi đọc được bằng máy tính.

Tình trạng kỹ thuật của sáng chế

Các hệ thống sổ cái phân tán (DLS), còn được gọi là mạng đồng thuận, và/hoặc mạng chuỗi khối, cho phép các thực thể tham gia lưu trữ dữ liệu một cách an toàn, và không thay đổi. Các DLS thường được gọi là các mạng chuỗi khối mà không đề cập đến trường hợp sử dụng cụ thể bất kỳ nào. Các ví dụ về kiểu mạng chuỗi khối có thể bao gồm mạng chuỗi khối công khai, mạng chuỗi khối bí mật, và mạng chuỗi khối kiểu tập đoàn. Mạng chuỗi khối công khai được mở cho tất cả các thực thể để sử dụng DLS, và tham gia vào quy trình đồng thuận. Mạng chuỗi khối bí mật được tạo ra cho thực thể cụ thể, thực thể này điều khiển quyền hạn đọc và ghi một cách tập trung. Mạng chuỗi khối kiểu tập đoàn được tạo ra cho nhóm các thực thể được lựa chọn, mà điều khiển quy trình đồng thuận, và bao gồm tầng điều khiển truy cập.

Chuỗi khối là công nghệ lưu trữ dữ liệu phân tán phi tập trung và chống giả mạo. Dữ liệu và các hợp đồng của người sử dụng được thao tác một cách logic và được lưu trữ trên chuỗi một cách công khai. Trong nhiều kịch bản, người sử dụng cần đạt được các yêu cầu bảo mật và không muốn dữ liệu và logic của họ bị để lộ cho các bên không được cấp phép.

Mặc dù mật mã có thể được sử dụng để tăng cường bảo mật đối với một số thiết kế kịch bản cụ thể, cần có một giải pháp linh động và hiệu quả hơn để giải quyết các vấn đề riêng tư tồn đọng về các hoạt động chuỗi khối.

Bản chất kỹ thuật của sáng chế

Các phương án thực hiện của sáng chế bao gồm các phương pháp được thực hiện bằng máy tính để lưu trữ và truy hồi dữ liệu cần xác minh liên kết với các nút của mạng

chuỗi khối. Cụ thể hơn, các phương án thực hiện của sáng chế là nhằm lưu trữ bản tóm lược dữ liệu của dữ liệu cần xác minh liên kết với một hoặc nhiều nút mạng chuỗi khối kiểu tập đoàn bằng cách sử dụng một số nút xác minh, và truy hồi dữ liệu cần xác minh và các bản tóm lược dữ liệu được lưu trữ.

Theo một số phương án thực hiện, các bước bao gồm bước lưu trữ mục dữ liệu trong chuỗi khối kiểu tập đoàn được duy trì bởi mạng chuỗi khối kiểu tập đoàn; tạo ra bản tóm lược dữ liệu thứ nhất dựa trên mục dữ liệu đã lưu; gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh, sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ nhất và lưu trữ bản tóm lược dữ liệu thứ nhất đã ký của nó trong chuỗi khối công khai được duy trì bởi mạng chuỗi khối công khai; tiếp nhận yêu cầu truy hồi mục dữ liệu đã lưu; truy hồi mục dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn nhằm đáp lại bước tiếp nhận yêu cầu; tạo ra bản tóm lược dữ liệu thứ hai dựa trên mục dữ liệu đã truy hồi; gửi bản tóm lược dữ liệu thứ hai đến các nút xác minh sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ hai và trả lại bản tóm lược dữ liệu thứ hai đã ký của nó; tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký từ các nút xác minh; truy hồi các bản tóm lược dữ liệu thứ nhất đã ký từ chuỗi khối công khai; xác định rằng các bản tóm lược dữ liệu thứ nhất đã ký khớp với các bản tóm lược dữ liệu thứ hai đã ký; và gửi hồi đáp để yêu cầu truy hồi mục dữ liệu đã lưu nhằm đáp lại bước xác định, hồi đáp này chỉ báo rằng mục dữ liệu đã lưu chưa thay đổi kể từ lúc được lưu trữ. Các phương án thực hiện khác bao gồm các hệ thống, thiết bị, và chương trình máy tính tương ứng, được tạo cấu hình để thực hiện các bước của phương pháp, được mã hóa trên các thiết bị lưu trữ máy tính.

Theo một số phương án thực hiện, vật ghi lâu dài được bằng máy tính được lắp với một hoặc nhiều máy tính và được tạo cấu hình với các lệnh thực thi được bằng một hoặc nhiều máy tính để: lưu trữ mục dữ liệu trong chuỗi khối kiểu tập đoàn được duy trì bởi mạng chuỗi khối kiểu tập đoàn; tạo ra bản tóm lược dữ liệu thứ nhất dựa trên mục dữ liệu đã lưu; gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ nhất và lưu trữ bản tóm lược dữ liệu thứ nhất đã ký của nó trong chuỗi khối công khai được duy trì bởi mạng chuỗi khối công khai; tiếp nhận yêu cầu truy hồi mục dữ liệu đã lưu; truy hồi mục dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn nhằm đáp lại bước tiếp nhận yêu cầu; tạo ra bản tóm

lược dữ liệu thứ hai dựa trên mục dữ liệu đã truy hồi; gửi bản tóm lược dữ liệu thứ hai đến các nút xác minh sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ hai và trả lại bản tóm lược dữ liệu thứ hai đã ký của nó; tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký từ các nút xác minh; truy hồi các bản tóm lược dữ liệu thứ nhất đã ký từ chuỗi khối công khai; xác định rằng các bản tóm lược dữ liệu thứ nhất đã ký khớp với các bản tóm lược dữ liệu thứ hai đã ký; và gửi hồi đáp để yêu cầu truy hồi mục dữ liệu đã lưu nhằm đáp lại bước xác định, hồi đáp này chỉ báo rằng mục dữ liệu đã lưu chưa thay đổi kể từ lúc được lưu trữ.

Theo một số phương án thực hiện, hệ thống bao gồm một hoặc nhiều máy tính; và một hoặc nhiều bộ nhớ đọc được bằng máy tính được lắp với một hoặc nhiều máy tính và được tạo cấu hình với các lệnh thực thi được bằng một hoặc nhiều máy tính để: lưu trữ mục dữ liệu trong chuỗi khối kiểu tập đoàn được duy trì bởi mạng chuỗi khối kiểu tập đoàn; tạo ra bản tóm lược dữ liệu thứ nhất dựa trên mục dữ liệu đã lưu; gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ nhất và lưu trữ bản tóm lược dữ liệu thứ nhất đã ký của nó trong chuỗi khối công khai được duy trì bởi mạng chuỗi khối công khai; tiếp nhận yêu cầu truy hồi mục dữ liệu đã lưu; truy hồi mục dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn nhằm đáp lại bước tiếp nhận yêu cầu; tạo ra bản tóm lược dữ liệu thứ hai dựa trên mục dữ liệu đã truy hồi; gửi bản tóm lược dữ liệu thứ hai đến các nút xác minh sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ hai và trả lại bản tóm lược dữ liệu thứ hai đã ký của nó; tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký từ các nút xác minh; truy hồi các bản tóm lược dữ liệu thứ nhất đã ký từ chuỗi khối công khai; xác định rằng các bản tóm lược dữ liệu thứ nhất đã ký khớp với các bản tóm lược dữ liệu thứ hai đã ký đã tiếp nhận; và gửi hồi đáp để yêu cầu truy hồi mục dữ liệu đã lưu nhằm đáp lại bước xác định, hồi đáp này chỉ báo rằng mục dữ liệu đã lưu chưa thay đổi kể từ lúc được lưu trữ. Các phương án này và các phương án khác có thể tùy ý bao gồm một hoặc nhiều dấu hiệu sau đây:

Dấu hiệu thứ nhất, có thể kết hợp với bất kỳ trong số các dấu hiệu sau đây, trong đó các nút xác minh là các thiết bị điện toán tham gia vào mạng chuỗi khối công khai.

Dấu hiệu thứ hai, có thể kết hợp với bất kỳ trong số các dấu hiệu sau đây, còn bao gồm bước lưu trữ hợp đồng thông minh trong chuỗi khối công khai, trong đó hợp

đồng thông minh được tạo cấu hình để tạo phần thưởng tiền cho các nút xác minh nhằm đáp lại bước tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký được yêu cầu từ các nút xác minh.

Dấu hiệu thứ ba, có thể kết hợp với bất kỳ trong số các dấu hiệu sau đây, trong đó bước tạo ra bản tóm lược dữ liệu thứ nhất bao gồm bước tính toán giá trị băm của mục dữ liệu đã lưu.

Dấu hiệu thứ tư, có thể kết hợp với bất kỳ trong số các dấu hiệu sau đây, trong đó mỗi nút xác minh được tạo cấu hình để ký bằng mật mã bản tóm lược dữ liệu thứ nhất bằng cách sử dụng khoá bí mật liên kết với nút xác minh trên.

Dấu hiệu thứ năm, có thể kết hợp với bất kỳ trong số các dấu hiệu sau đây, trong đó bước gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh bao gồm bước phát bản tóm lược dữ liệu thứ nhất đến mạng chuỗi khối công khai.

Dấu hiệu thứ sáu, có thể kết hợp với bất kỳ trong số các dấu hiệu sau đây, trong đó bước truy hồi các bản tóm lược dữ liệu thứ nhất đã ký từ chuỗi khối công khai bao gồm bước nhận dạng các bản tóm lược dữ liệu thứ nhất đã ký dựa trên mã nhận dạng liên kết với mục dữ liệu đã lưu và được lưu trữ trong chuỗi khối công khai.

Sáng chế còn đề xuất một hoặc nhiều vật ghi lâu dài đọc được bằng máy tính được lắp với một hoặc nhiều bộ xử lý và có lưu các lệnh trên đó mà, khi được thực hiện bởi một hoặc nhiều bộ xử lý, khiến một hoặc nhiều bộ xử lý này thực hiện các thao tác theo các phương án thực hiện các phương pháp được đề xuất trong bản mô tả.

Sáng chế còn đề xuất hệ thống để thực hiện các phương pháp được đề xuất tại đây. Hệ thống này bao gồm một hoặc nhiều bộ xử lý, và vật ghi đọc được bằng máy tính được lắp với một hoặc nhiều bộ xử lý này có lưu các lệnh trên đó mà, khi được thực hiện bởi một hoặc nhiều bộ xử lý, khiến một hoặc nhiều bộ xử lý này thực hiện các thao tác theo các phương án thực hiện các phương pháp được đề xuất trong bản mô tả.

Mạng chuỗi khối đã nêu có thể được sử dụng để xác minh sự nguyên vẹn của dữ liệu được lưu trữ trong mạng chuỗi khối. Mạng này bao gồm một lượng lớn các nút có thể tham gia vào quy trình đồng thuận, nhờ đó đảm bảo sự nguyên vẹn của dữ liệu. Ngoài ra, các kỹ thuật đã nêu đề xuất cơ chế khuyến khích dựa trên các hợp đồng thông minh để tăng sự tham gia của nút vào chuỗi bên công khai.

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

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

Mô tả vắn tắt các hình vẽ

Fig. 1 là hình vẽ thể hiện một ví dụ về môi trường có thể được sử dụng để thực thi các phương án thực hiện của sáng chế.

Fig. 2 là hình vẽ thể hiện một ví dụ về kiến trúc ý tưởng theo các phương án thực hiện của sáng chế.

Fig. 3 là hình vẽ thể hiện một ví dụ về hệ thống có thể được sử dụng để thực thi các phương án thực hiện của sáng chế theo các phương án thực hiện của sáng chế.

Fig. 4 là hình vẽ thể hiện một ví dụ về giảm lược lưu trữ dữ liệu trong mạng chuỗi khối kiểu tập đoàn và mạng chuỗi bên công khai liên kết theo các khía cạnh của sáng chế.

Fig. 5 là hình vẽ thể hiện một ví dụ về quy trình truy hồi dữ liệu từ mạng chuỗi khối kiểu tập đoàn, và xác minh dữ liệu đã truy hồi dựa trên mạng chuỗi bên công khai theo các khía cạnh của sáng chế.

Fig. 6 mô tả ví dụ về quy trình có thể được thực thi theo các phương án thực hiện của sáng chế.

Fig. 7 là hình vẽ thể hiện một ví dụ về sơ đồ minh họa các môđun của thiết bị theo các phương án thực hiện của sáng chế.

Các ký hiệu chỉ dẫn giống nhau trên các hình vẽ khác nhau biểu diễn các thành phần giống nhau.

Mô tả chi tiết sáng chế

Các phương án thực hiện của sáng chế bao gồm các phương pháp được thực hiện bằng máy tính để lưu trữ và truy hồi dữ liệu cần xác minh liên kết với các nút của mạng chuỗi khối. Cụ thể hơn, các phương án thực hiện của sáng chế là nhằm lưu trữ bản tóm lược dữ liệu của dữ liệu cần xác minh liên kết với một hoặc nhiều nút mạng chuỗi khối kiểu tập đoàn bằng cách sử dụng một số nút xác minh, và truy hồi dữ liệu cần xác minh và các bản tóm lược dữ liệu được lưu trữ.

Để cung cấp ngữ cảnh khác cho các phương án thực hiện của sáng chế, và như được giới thiệu trên đây, hệ thống sổ cái phân tán (DLS), mà còn có thể được gọi là mạng đồng thuận (ví dụ, được tạo thành từ các nút ngang hàng), hoặc các mạng chuỗi khối, cho phép các thực thể tham gia thực hiện các giao dịch một cách an toàn và bất biến, và lưu trữ dữ liệu. Thuật ngữ chuỗi khối được sử dụng trong bản mô tả để đề cập chung đến DLS mà không đề cập đến bất kỳ trường hợp sử dụng nào.

Chuỗi khối là cấu trúc dữ liệu lưu các giao dịch theo cách mà các giao dịch này là bất biến, và có thể được xác minh tiếp. Chuỗi khối bao gồm một hoặc nhiều khối. Mỗi khối trong chuỗi được liên kết với khối trước ngay trước nó trong chuỗi này bằng cách bao gồm hàm băm mật mã của khối trước này. Mỗi khối cũng bao gồm dấu thời gian, hàm băm mật mã của chính nó, và một hoặc nhiều giao dịch. Các giao dịch, mà đã được xác minh bằng các nút của mạng chuỗi khối này, được băm và được mã hóa thành cây Merkle. Cây Merkle là cấu trúc dữ liệu trong đó dữ liệu ở các nút lá của cây được băm, và tất cả các giá trị băm ở mỗi nhánh của cây được nối với nhau ở gốc của nhánh này. Quy trình này tiếp tục lên phía trên cây xuống đến rễ của toàn bộ cây, lưu giá trị băm biểu diễn toàn bộ dữ liệu trong cây này. Giá trị băm có ý nghĩa là giao dịch được lưu trong cây này có thể được xác minh nhanh chóng bằng cách xác định nó có phù hợp với cấu trúc của cây này hay không.

Trong khi chuỗi khối là cấu trúc dữ liệu để lưu các giao dịch, mạng chuỗi khối là mạng chứa các nút tính toán mà quản lý, cập nhật, và duy trì một hoặc nhiều chuỗi khối. Như đã giới thiệu trên đây, mạng chuỗi khối có thể được cung cấp dưới dạng mạng chuỗi khối công khai, mạng chuỗi khối bí mật, hoặc mạng chuỗi khối kiểu tập đoàn.

Trong mạng chuỗi khối công khai, quy trình đồng thuận được điều khiển bằng các nút của mạng đồng thuận. Ví dụ, hàng trăm, hàng nghìn, thậm chí hàng triệu thực thể có thể phối hợp trong một mạng chuỗi khối công khai, mỗi thực thể này điều hành

ít nhất một nút trong mạng chuỗi khối công khai. Theo đó, mạng chuỗi khối công khai này có thể được coi là mạng công khai đối với các thực thể tham gia. Theo một số ví dụ, phần lớn các thực thể (nút) phải ký mọi khối để khối này hợp lệ, và được bổ sung vào chuỗi khối (sổ cái phân tán) của mạng chuỗi khối. Các mạng chuỗi khối công khai được lấy làm ví dụ bao gồm các mạng thanh toán ngang hàng cụ thể có thể dùng sổ cái phân tán làm đòn bẩy, được gọi là chuỗi khối. Tuy nhiên, như được lưu ý trên đây, thuật ngữ chuỗi khối thường được sử dụng để đề cập đến các sổ cái phân tán mà không đề cập cụ thể đến mạng chuỗi khối cụ thể bất kỳ.

Nói chung, mạng chuỗi khối công khai hỗ trợ các giao dịch công khai. Giao dịch công khai được chia sẻ với tất cả các nút nằm trong mạng chuỗi khối công khai, và được lưu trữ trong chuỗi khối toàn cầu. Chuỗi khối toàn cầu là chuỗi khối được sao chép qua tất cả các nút. Tức là tất cả các nút đồng thuận hoàn toàn ở cấp quốc gia đối với chuỗi khối toàn cầu. Để đạt được đồng thuận (ví dụ, đồng ý về việc bổ sung khối vào chuỗi khối), giao thức đồng thuận được thực hiện trong mạng chuỗi khối công khai. Ví dụ về các giao thức đồng thuận bao gồm, không giới hạn ở, bằng chứng công việc (POW), bằng chứng cổ phần (POS), và bằng chứng ủy quyền (POA). POW còn được đề cập thêm tại đây dưới dạng ví dụ không giới hạn.

Nói chung, mạng chuỗi khối cá nhân được cung cấp cho một thực thể cụ thể, mà kiểm soát tập trung quyền đọc và ghi. Thực thể này kiểm soát, các nút nào có thể tham gia vào mạng chuỗi khối. Do đó, mạng chuỗi khối bí mật thường được gọi là mạng đã cấp quyền đặt giới hạn lên việc ai được phép tham gia vào mạng này, và lên mức độ tham gia (ví dụ, chỉ tham gia một số giao dịch). Nhiều loại cơ chế điều khiển truy cập khác nhau có thể được sử dụng (ví dụ, người đang tham gia biểu quyết về việc bổ sung thêm thực thể mới, cơ quan quản lý có thể điều khiển việc kết nạp).

Nói chung, mạng chuỗi khối kiểu tập đoàn là bí mật giữa các thực thể tham gia. Trong mạng chuỗi khối liên hợp, quy trình đồng thuận được kiểm soát bởi tập hợp các nút được cấp phép, một hoặc nhiều nút đang được điều hành bởi thực thể tương ứng (ví dụ, cơ quan tài chính, công ty bảo hiểm). Ví dụ, tập đoàn gồm mười (10) thực thể (ví dụ, viện tài chính, công ty bảo hiểm) có thể thao tác mạng chuỗi khối kiểu tập đoàn, mỗi thực thể thao tác ít nhất một nút trong mạng chuỗi khối kiểu tập đoàn. Theo đó, mạng chuỗi khối kiểu tập đoàn có thể được coi là mạng bí mật đối với các thực thể tham gia.

Theo một số ví dụ, mỗi thực thể (nút) phải ký mọi khối để khối này hợp lệ, và được bổ sung vào chuỗi khối. Theo một số ví dụ, ít nhất một tập hợp con của các thực thể (nút) (ví dụ, ít nhất 7 thực thể) phải ký mọi khối để khối này hợp lệ, và được bổ sung vào chuỗi khối.

Chuỗi khối là sổ cái kỹ thuật số chống làm giả được dùng chung mà ghi lại các giao dịch trong mạng ngang hàng công khai hoặc bí mật. Sổ cái được phân cho tất cả các nút thành viên trong mạng, và lịch sử của giao dịch tài sản diễn ra trong mạng được ghi lại vĩnh viễn trong khối. Trước khi tham gia vào một giao dịch, nút trên chuỗi khối có thể cần phải thực thi tính toán bằng cách sử dụng các kỹ thuật khác nhau. Theo các giải pháp hiện có, do mỗi chuỗi khối là độc lập, nút của một chuỗi khối không thể giao tiếp với các chuỗi khác. Ví dụ, nút không thể đọc dữ liệu từ các chuỗi khối khác hoặc trao đổi dữ liệu với các chuỗi khối khác. Ngoài ra, ngay cả khi nếu một nút không cần dữ liệu từ các chuỗi khối khác phải thực thi tính toán, thực hiện các tính toán này toàn bộ trên chuỗi khối có thể tốn rất nhiều thời gian và các tài nguyên tính toán của chuỗi khối, nếu nó cần các logic và giao thức tính toán phức tạp.

Các phương án của sáng chế được mô tả chi tiết hơn tại đây về mạng chuỗi khối kiểu tập đoàn, là công khai giữa các thực thể tham gia. Tuy nhiên, dự kiến là các phương án thực hiện của sáng chế có thể được nhận biết về kiểu mạng chuỗi khối thích hợp bất kỳ.

Các phương án của sáng chế được mô tả chi tiết hơn tại đây trong ngữ cảnh trên đây. Cụ thể hơn, và như đã giới thiệu trên đây, các phương án thực hiện của sáng chế là nhằm cung cấp dịch vụ hợp đồng thông minh ngoài chuỗi có khả năng thao tác lên dữ liệu chuỗi chéo trong môi trường thực thi tin cậy.

Cụ thể, các kỹ thuật đã nêu giới thiệu một chuỗi khối phụ trợ công khai (cũng được gọi là “chuỗi bên”) được sử dụng để xác minh sự nguyên vẹn của dữ liệu được lưu trữ trong chuỗi khối kiểu tập đoàn. Do chuỗi bên là công khai, một lượng lớn các nút có thể tham gia vào quy trình đồng thuận, nhờ đó đảm bảo sự nguyên vẹn của dữ liệu trong chuỗi bên. Biểu diễn của mỗi giao dịch trên chuỗi khối kiểu tập đoàn được lưu trữ trong chuỗi bên. Bởi vậy, để biến đổi dữ liệu trong chuỗi khối kiểu tập đoàn, kẻ tấn công cũng phải thực hiện việc biến đổi tương tự đối với chuỗi bên công khai. Việc biến đổi trong chuỗi bên công khai này sẽ gặp khó khăn hơn nhiều so với trong chuỗi khối kiểu tập

đoàn, do số lượng nút được bao gồm trong quy trình đồng thuận cho chuỗi bên công khai. Theo cách này, sự nguyên vẹn của dữ liệu trong chuỗi khối kiểu tập đoàn có thể được đảm bảo. Ngoài ra, các kỹ thuật đã nêu đề xuất cơ chế khuyến khích dựa trên các hợp đồng thông minh để tăng sự tham gia của nút vào chuỗi bên công khai. Hợp đồng thông minh có thể là thỏa thuận máy tính được thiết kế để phổ biến, xác minh, hoặc thực thi hợp đồng theo cách mang tính thông tin. Các hợp đồng thông minh cho phép các giao dịch tin cậy được thực hiện mà không cần sự can thiệp của bên thứ ba. Các giao dịch này có thể truy vết được và có thể đảo ngược.

Các kỹ thuật đã nêu có thể có nhiều ứng dụng đa dạng. Ví dụ, trong quá trình kiện tụng về vi phạm bản quyền, nguyên đơn cần phải cung cấp cho toà án một số loại bằng chứng dạng số để thể hiện chính xác thời gian cô ấy tạo ra sản phẩm gốc. Nếu bằng chứng dạng số được trình bởi nguyên đơn ban đầu được lưu trữ ở một chuỗi khối kiểu tập đoàn, bằng chứng này có thể không có khả năng đạt yêu cầu về trách nhiệm chứng minh, do toà án không thể xác định được rằng bằng chứng dạng số là không thể giả mạo được. Để thiết lập bản ghi chứng minh mà có thể được chấp nhận bởi toà án, nguyên đơn có thể lưu trữ bằng chứng dữ liệu bằng cách sử dụng các kỹ thuật đã nêu qua một hệ thống xác minh. Tại thời điểm trình bằng chứng, nguyên đơn có thể trình bằng chứng dạng số được lưu trữ ở chuỗi khối kiểu tập đoàn, cùng với các bản sao của bằng chứng dạng số được trình bởi các nút xác minh. Bằng cách này, toà án sẽ dễ nhận ra tính xác thực của bằng chứng dạng số hơn do một lượng lớn các nút xác minh làm chứng cho tính xác thực của bằng chứng dạng số này.

Ngoài ví dụ đã nêu ở trên, các kỹ thuật đã nêu có thể có lợi cho nhiều ứng dụng khác mà tận dụng công nghệ chuỗi khối.

Fig. 1 là hình vẽ thể hiện một ví dụ về môi trường 100 có thể được sử dụng để thực thi các phương án thực hiện của sáng chế. Theo một số ví dụ, môi trường 100 cho phép các thực thể tham gia vào mạng chuỗi khối 102. Môi trường 100 bao gồm các thiết bị điện toán 106, 108, và mạng 110. Theo một số ví dụ, mạng 110 bao gồm mạng cục bộ (LAN), mạng diện rộng (WAN), Internet hoặc sự kết hợp của chúng, và kết nối các trang web, thiết bị người sử dụng (ví dụ, thiết bị điện toán) và hệ thống đầu cuối với nhau. Theo một số ví dụ, mạng 110 có thể được truy cập qua liên kết truyền thông có dây và/hoặc không dây. Theo một số ví dụ, mạng 110 cho phép giao tiếp với, và giao

tiếp bên trong mạng chuỗi khối 102. Nói chung, mạng 110 là một hoặc nhiều mạng truyền thông. Trong một số trường hợp, các thiết bị điện toán 106, 108 có thể là các nút của hệ thống điện toán đám mây (không được thể hiện), hoặc mỗi thiết bị điện toán 106, 108 có thể là hệ thống điện toán đám mây riêng biệt bao gồm một số máy tính được liên kết bằng mạng và hoạt động như là một hệ thống xử lý phân tán.

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

Fig. 2 là hình vẽ thể hiện một ví dụ về kiến trúc ý tưởng 200 theo các phương án thực hiện của sáng chế. Ví dụ về kiến trúc ý tưởng 200 bao gồm các hệ thống tham gia 202, 204, 206 tương ứng lần lượt với Bên tham gia A, Bên tham gia B, và Bên tham gia C. Mỗi bên tham gia (ví dụ, người sử dụng, doanh nghiệp) tham gia vào mạng chuỗi khối 212 được cung cấp dưới dạng mạng ngang hàng bao gồm các nút 214, ít nhất một số trong các nút này ghi không đổi thông tin trong chuỗi khối 216. Mặc dù chuỗi khối đơn 216 được mô tả giản lược trong mạng chuỗi khối 212, các bản sao của chuỗi khối 216 được cung cấp, và được duy trì xuyên mạng chuỗi khối 212, như được mô tả tiếp tại đây.

Theo các ví dụ đã mô tả, mỗi hệ thống tham gia 202, 204, 206 được cung cấp bởi, hoặc lần lượt biểu diễn Bên tham gia A, Bên tham gia B, và Bên tham gia C, và có

chức năng như nút 214 tương ứng trong mạng chuỗi khối. Như được sử dụng tại đây, một nút thường là hệ thống cá nhân (ví dụ, máy tính, máy chủ) được kết nối với mạng chuỗi khối 212, và cho phép bên tham gia tương ứng tham gia vào mạng chuỗi khối. Theo ví dụ, trên Fig. 2, bên tham gia tương ứng với mỗi nút 214. Tuy nhiên, dự tính rằng bên tham gia có thể thao tác các nút 214 trong mạng chuỗi khối 212, và/hoặc các bên tham gia có thể dùng chung nút 214. Theo một số ví dụ, các hệ thống tham gia 202, 204, 206 giao tiếp với, hoặc qua mạng chuỗi khối 212 bằng cách sử dụng giao thức (ví dụ, bảo mật giao thức truyền tải siêu văn bản (HTTPS)), và/hoặc sử dụng các lệnh gọi quy trình từ xa (RPC).

Các nút 214 có thể có các mức độ tham gia vào mạng chuỗi khối 212 khác nhau. Ví dụ, một số nút 214 có thể tham gia vào quy trình đồng thuận (ví dụ, dưới dạng nút đào bổ sung các khối vào chuỗi khối 216), trong khi các nút 214 khác không tham gia vào quy trình đồng thuận này. Theo một ví dụ khác, một số nút 214 lưu trữ bản sao hoàn chỉnh của chuỗi khối 216, trong khi các nút 214 khác chỉ lưu trữ các bản sao một phần của chuỗi khối 216. Ví dụ, các đặc quyền truy cập dữ liệu có thể làm giới hạn dữ liệu chuỗi khối mà bên tham gia tương ứng lưu trữ trong hệ thống tương ứng của nó. Theo ví dụ, trên Fig. 2, các hệ thống tham gia 202, 204, 206 lần lượt lưu trữ các bản sao hoàn chỉnh 216', 216'', 216''' của chuỗi khối 216.

Chuỗi khối (ví dụ, chuỗi khối 216 trên Fig. 2) được tạo nên từ chuỗi các khối, với mỗi khối này lưu trữ dữ liệu. Các ví dụ về dữ liệu bao gồm biểu diễn dữ liệu giao dịch của giao dịch giữa hai hoặc nhiều bên tham gia. Trong khi giao dịch được sử dụng tại đây theo các ví dụ, không giới hạn, dự tính rằng dữ liệu thích hợp bất kỳ có thể được lưu trữ trong chuỗi khối (ví dụ, tài liệu, ảnh, video, âm thanh). Các ví dụ về giao dịch có thể bao gồm, mà không giới hạn, trao đổi thứ có giá trị (ví dụ, tài sản, vật phẩm, dịch vụ, và tiền tệ). Dữ liệu giao dịch được lưu trữ không đổi bên trong chuỗi khối. Nghĩa là không thể thay đổi dữ liệu giao dịch.

Trước khi lưu trữ trong khối, dữ liệu giao dịch được tạo băm. Việc tạo băm là quá trình biến đổi dữ liệu giao dịch (được đưa ra dưới dạng dữ liệu chuỗi) thành giá trị băm có độ dài cố định (cũng được đưa ra dưới dạng dữ liệu chuỗi). Không thể tạo băm ngược giá trị băm để thu được dữ liệu giao dịch. Việc tạo băm đảm bảo rằng ngay cả sự thay đổi nhỏ về dữ liệu giao dịch cũng sẽ cho ra giá trị băm hoàn toàn khác. Ngoài ra,

và như nêu trên, giá trị băm có độ dài cố định. Nghĩa là với bất kỳ cỡ nào của dữ liệu giao dịch, độ dài của giá trị băm là cố định. Việc tạo băm bao gồm bước xử lý dữ liệu giao dịch qua hàm băm để tạo ra giá trị băm. Ví dụ về hàm băm bao gồm, mà không giới hạn, thuật toán băm bảo mật (SHA)-256, cho đầu ra là các giá trị băm 256 bit.

Dữ liệu giao dịch của các giao dịch được tạo băm và được lưu trữ trong khối. Ví dụ, các giá trị băm của hai giao dịch được cung cấp, và bản thân các giá trị băm này được tạo băm để tạo ra một giá trị băm khác. Quy trình này được lặp lại cho đến khi giá trị băm đơn được tạo ra để tất cả các giao dịch được lưu trữ trong khối. Giá trị băm này được gọi là giá trị băm gốc Merkle, và được lưu trữ trong phần đầu khối. Thay đổi trong giao dịch bất kỳ sẽ dẫn đến thay đổi về giá trị băm của nó, và cuối cùng, thay đổi về giá trị băm gốc Merkle.

Các khối được thêm vào chuỗi khối qua giao thức đồng thuận. Các nút trong mạng chuỗi khối tham gia vào giao thức đồng thuận, và cạnh tranh để khối được thêm vào chuỗi khối. Các nút này được gọi là bên đào (hoặc nút trông coi (miner node)). POW, được giới thiệu ở trên, được sử dụng làm ví dụ, không giới hạn.

Nút đào thực thi quy trình đồng thuận để thêm giao dịch vào chuỗi khối. Mặc dù nhiều nút đào tham gia vào quy trình đồng thuận này, chỉ một nút đào có thể ghi khối vào chuỗi khối này. Nghĩa là các nút đào cạnh tranh trong quy trình đồng thuận để khối của các nút đào này được thêm vào chuỗi khối. Ngoài ra, nút đào thu thập định kỳ các giao dịch đang chờ xử lý từ nhóm giao dịch (ví dụ, lên đến giới hạn định trước về số lượng giao dịch có thể được bao gồm trong khối, nếu có). Nhóm giao dịch bao gồm tin nhắn giao dịch từ các bên tham gia trong mạng chuỗi khối. Nút đào tạo cấu trúc một khối, và thêm các giao dịch vào khối này. Trước khi thêm các giao dịch vào khối, nút đào kiểm tra xem bất kỳ trong số các giao dịch đã được bao gồm trong khối của chuỗi khối hay chưa. Nếu giao dịch đã được bao gồm trong một khối khác, giao dịch được huỷ bỏ.

Nút đào tạo ra phần đầu khối, tạo băm tất cả các giao dịch trong khối, và kết hợp các giá trị băm theo cặp để tạo ra tiếp các giá trị băm cho đến khi giá trị băm đơn được tạo ra cho tất cả các giao dịch trong khối (giá trị băm gốc Merkle). Giá trị băm này được thêm vào phần đầu khối. Bên đào cũng xác định giá trị băm của khối gần nhất trong chuỗi khối (tức là khối cuối cùng được thêm vào chuỗi khối). Nút đào cũng thêm giá trị

dùng một lần, và dấu thời gian (timestamp) vào phần đầu khối. Trong quá trình đào, nút đào thử tìm giá trị băm mà đáp ứng các thông số bắt buộc. Nút đào không ngừng thay đổi giá trị dùng một lần cho đến khi tìm ra giá trị băm mà đáp ứng các thông số bắt buộc.

Mỗi bên đào trong mạng chuỗi khối thử tìm giá trị băm mà đáp ứng các thông số bắt buộc, và, theo cách này, cạnh tranh với nhau. Kết quả là một trong số các nút đào tìm giá trị băm mà đáp ứng các thông số bắt buộc, và quảng cáo giá trị này cho tất cả các nút đào khác trong mạng chuỗi khối. Các nút đào khác xác minh giá trị băm, và nếu các nút này được xác định là đúng, xác minh mỗi giao dịch trong khối, chấp nhận khối, và bổ sung khối vào bản sao chuỗi khối của mình. Theo cách này, trạng thái toàn cục của chuỗi khối là nhất quán qua tất cả các nút đào trong mạng chuỗi khối. Quy trình nêu trên là giao thức đồng thuận POW.

Một ví dụ không giới hạn được đề xuất dựa vào Fig. 2. Theo ví dụ này, Bên tham gia A muốn gửi một lượng tiền đến Bên tham gia B. Bên tham gia A tạo ra tin nhắn giao dịch (ví dụ, bao gồm Từ, Đến, và Các trường giá trị), và gửi tin nhắn giao dịch này đến mạng chuỗi khối, từ đó thêm tin nhắn giao dịch vào nhóm giao dịch. Mỗi nút đào trong mạng chuỗi khối tạo ra một khối, và lấy tất cả các giao dịch từ nhóm giao dịch (ví dụ, lên đến giới hạn định trước về số lượng giao dịch mà có thể được thêm vào khối, nếu có), và thêm các giao dịch vào khối này. Theo cách này, giao dịch được công bố bởi Bên tham gia A được thêm vào các khối của nút đào.

Trong một số mạng chuỗi khối, mật mã được thực hiện để duy trì độ bí mật của giao dịch. Ví dụ, nếu hai nút muốn giữ bí mật một giao dịch, sao cho các nút khác trong mạng chuỗi khối không thể biết các chi tiết của giao dịch này, các nút này có thể mã hoá dữ liệu giao dịch. Các ví dụ về các phương pháp mật mã bao gồm, không giới hạn, mã hoá đối xứng, và mã hoá không đối xứng. Mã hoá đối xứng là quá trình mã hoá sử dụng khoá đơn cho cả quá trình mã hoá (tạo ra ký tự dạng mã từ ký tự đơn giản), và quá trình giải mã (tạo ra ký tự đơn giản từ ký tự dạng mã). Trong quá trình mã hoá đối xứng, có sẵn cùng một khoá cho nhiều nút, nên mỗi nút có thể mã hoá/giải mã dữ liệu giao dịch.

Quy trình mã hoá không đối xứng sử dụng các cặp khoá, mỗi khoá tổng cặp bao gồm khoá bí mật, và khoá công khai, khoá bí mật này chỉ được biết đến với nút tương ứng, và khoá công khai này chỉ được biết đến với nút bất kỳ hoặc tất cả các nút khác trong mạng chuỗi khối. Nút có thể sử dụng khoá công khai của một nút khác để mã hoá

dữ liệu, và dữ liệu đã mã hoá có thể được giải mã bằng cách sử dụng khoá bí mật của các nút khác. Ví dụ, và lại dựa vào Fig. 2, Bên tham gia A có thể sử dụng khoá công khai của Bên tham gia B để mã hoá dữ liệu, và gửi dữ liệu đã mã hoá đến Bên tham gia B. Bên tham gia B có thể sử dụng khoá bí mật của mình để giải mã dữ liệu đã mã hoá (ký tự dạng mã) và trích xuất dữ liệu ban đầu (ký tự đơn giản). Các tin nhắn được mã hoá với khoá công khai của nút có thể chỉ giải mã được bằng cách sử dụng khoá bí mật của nút.

Quy trình mã hoá không đối xứng được sử dụng để cung cấp chữ ký số hoá, cho phép các bên tham gia trong giao dịch xác nhận các bên tham gia khác trong giao dịch, cũng như tính hợp lệ của giao dịch. Ví dụ, nút có thể ký số một tin nhắn, và một nút khác có thể xác nhận rằng tin nhắn đã được gửi bởi nút dựa trên chữ ký số hoá của Bên tham gia A. Chữ ký số hoá cũng có thể được sử dụng để đảm bảo rằng tin nhắn không bị giả mạo khi chuyển tiếp. Ví dụ, và lại dựa vào Fig. 2, Bên tham gia A chuẩn bị gửi tin nhắn đến Bên tham gia B. Bên tham gia A tạo ra giá trị băm của tin nhắn, và sau đó, bằng cách sử dụng khoá bí mật của mình, mã hoá giá trị băm này để đưa ra chữ ký số hoá dưới dạng giá trị băm đã mã hoá. Bên tham gia A bổ sung chữ ký số hoá vào tin nhắn, và gửi tin nhắn có chữ ký số hoá đến Bên tham gia B. Bên tham gia B giải mã chữ ký số hoá này bằng cách sử dụng khoá công khai của Bên tham gia A, và trích xuất giá trị băm. Bên tham gia B tạo băm tin nhắn này và so sánh các giá trị băm với nhau. Nếu các giá trị băm là một, Bên tham gia B có thể xác nhận rằng tin nhắn chắc chắn là từ Bên tham gia A, và đã không bị giả mạo.

Fig. 3 là hình vẽ thể hiện một ví dụ về hệ thống có thể được sử dụng để thực thi các phương án thực hiện của sáng chế theo các phương án thực hiện của sáng chế.

Như được minh họa trên Fig. 3, hệ thống 300 bao gồm mạng chuỗi khối kiểu tập đoàn 302 bao gồm các nút 304a-304e duy trì chuỗi khối kiểu tập đoàn 306. Hệ thống 300 bao gồm hệ thống xác minh 316, hệ thống khuyến khích 320, và mạng chuỗi bên công khai 352. Mạng chuỗi bên công khai 352 bao gồm các nút xác minh 330, chuỗi khối công khai 356, và các nút chuỗi khối công khai (ví dụ, 354) duy trì chuỗi khối công khai 356.

Khi hoạt động, mạng chuỗi khối kiểu tập đoàn 302 (tức là các nút 304a-e) tiếp nhận yêu cầu lưu trữ dữ liệu (360). Các nút 304a-e lưu trữ dữ liệu trong chuỗi khối kiểu

tập đoàn 306 theo các cơ chế nêu trên. Hệ thống xác minh 316 tiếp nhận dữ liệu được lưu trữ một khi nó được thêm vào chuỗi khối 306 (tại bước 362). Ví dụ, hệ thống xác minh có thể giám sát mạng chuỗi khối kiểu tập đoàn 302 và xác định rằng dữ liệu này đã được lưu trữ một khi đạt được sự đồng thuận bởi các nút 304a-e trên chuỗi chứa dữ liệu.

Theo một số phương án thực hiện, hệ thống xác minh 316 có trách nhiệm về tương tác giữa mạng chuỗi khối kiểu tập đoàn 302 và mạng chuỗi bên công khai 352. Khi hoạt động, hệ thống xác minh 316 (tại bước 366) gửi bản tóm lược dữ liệu của dữ liệu được lưu trữ đến các nút xác minh 330. Theo một số phương án thực hiện, các nút xác minh 330 là các thiết bị điện toán tham gia vào mạng chuỗi bên công khai 352. Có thể có một lượng lớn (ví dụ, hàng nghìn) các nút xác minh 330. Trong một số trường hợp, hệ thống xác minh 316 có thể phát bản tóm lược dữ liệu đến mạng chuỗi bên công khai 352. Các nút xác minh 330, khi tiếp nhận bản tóm lược dữ liệu, ký bằng mật mã bản tóm lược dữ liệu bằng cách sử dụng khoá bí mật của chúng. Mỗi nút xác minh sau đó thử lưu trữ bản tóm lược dữ liệu đã ký của chúng trong chuỗi khối công khai 356. Theo một số phương án thực hiện, tất cả các bản tóm lược dữ liệu đã ký được tạo ra bởi các nút xác minh 330 được lưu trữ trong chuỗi khối công khai 356. Trong một số trường hợp, một số lượng nhất định các bản tóm lược dữ liệu đã ký được lưu trữ trong chuỗi khối công khai 356 và các bản tóm lược dữ liệu khác được loại bỏ. Số lượng này có thể là một hàm của các cơ chế đồng thuận được sử dụng trong mạng chuỗi bên công khai 352.

Hệ thống 300 cũng có thể bao gồm hệ thống khuyến khích 320. Theo một số phương án thực hiện, hệ thống khuyến khích 320 có thể tạo ra hợp đồng thông minh để được lưu trữ trong chuỗi khối công khai 356. Hợp đồng thông minh có thể được tạo cấu hình, khi được thực thi bởi mạng chuỗi bên công khai, để tạo phần thưởng tiền cho các nút xác minh 330 tham gia vào việc xác minh dữ liệu được lưu trữ. Ví dụ, nút xác minh 330 mà chứa bản tóm lược dữ liệu đã ký của chúng một cách thành công trong chuỗi khối công khai 356 có thể tiếp nhận phần thưởng tiền tự động thông qua việc thực thi hợp đồng thông minh. Trong một số trường hợp, nút xác minh 330 mà tham gia vào việc xác minh dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn (xem Fig. 5 dưới đây) có thể tiếp nhận phần thưởng tiền tự động thông qua việc thực thi hợp đồng thông minh.

Fig. 4 là hình vẽ mô tả quy trình 400 được lấy làm ví dụ về việc lưu trữ dữ liệu trong mạng chuỗi khối kiểu tập đoàn và mạng chuỗi bên công khai liên kết theo các khía cạnh của sáng chế.

Tại bước 405, mục dữ liệu được lưu trữ trong mạng chuỗi khối kiểu tập đoàn 302. Tại bước 410, hệ thống xác minh 316 tiếp nhận dữ liệu mới được lưu từ mạng chuỗi khối kiểu tập đoàn 302, như bằng cách giao tiếp với các nút tham gia vào mạng. Tại bước 415, hệ thống xác minh 316 tạo ra bản tóm lược dữ liệu của mục dữ liệu mới được lưu. Ví dụ, hệ thống xác minh 316 có thể tạo ra bản tóm lược dữ liệu bằng cách tạo ra giá trị băm của mục dữ liệu đã lưu bằng cách sử dụng thuật toán băm, như, ví dụ, Thuật toán băm an toàn 1 (SHA-1, Secure Hash Algorithm 1), SHA-256, Rivest–Shamir–Adleman (RSA), hoặc các thuật toán đã biết khác.

Tại bước 420, hệ thống xác minh 316 yêu cầu xác minh bản tóm lược dữ liệu bằng các nút xác minh 330. Nhằm đáp lại, tại bước 425, các nút xác minh 330 ký bằng mật mã bản tóm lược dữ liệu bằng cách sử dụng các khoá bí mật của chúng. Tại bước 430, các nút xác minh 330 lưu trữ các bản tóm lược dữ liệu đã ký riêng lẻ trong chuỗi khối công khai 356 được quản lý bởi mạng chuỗi bên công khai 352. Như đã nêu, theo một số phương án thực hiện, chỉ một số nhất định các bản tóm lược dữ liệu sẽ được lưu trữ trong chuỗi khối công khai 356 phụ thuộc vào các cơ chế đồng thuận được sử dụng bởi mạng chuỗi bên công khai 352.

Fig. 5 là hình vẽ thể hiện quy trình được lấy làm ví dụ về việc truy hồi dữ liệu từ mạng chuỗi khối kiểu tập đoàn 302, và xác minh dữ liệu đã truy hồi dựa trên mạng chuỗi bên công khai 352. Tại bước 505, yêu cầu truy hồi dữ liệu được tiếp nhận bởi mạng chuỗi khối kiểu tập đoàn 302 (tức là bởi nút tham gia vào mạng chuỗi khối kiểu tập đoàn). Theo một số phương án thực hiện, yêu cầu này có thể được tiếp nhận bởi hệ thống xác minh 316.

Tại bước 510, hệ thống xác minh 316 truy hồi dữ liệu được yêu cầu từ mạng chuỗi khối kiểu tập đoàn 302, như bằng cách thu được dữ liệu được yêu cầu từ phiên bản đồng thuận của chuỗi khối kiểu tập đoàn 306. Tại bước 515, hệ thống xác minh 316 truy hồi các bản tóm lược dữ liệu đã ký liên kết với dữ liệu được yêu cầu từ mạng chuỗi bên công khai 352. Trong một số trường hợp, các bản tóm lược đã ký có thể được truy hồi dựa trên mã nhận dạng liên kết với dữ liệu được lưu trữ, như dấu thời gian hoặc mã

nhận dạng khác được lưu trữ trong chuỗi khối công khai 356 cùng với các bản tóm lược dữ liệu đã ký bằng các nút xác minh 330.

Tại bước 520, hệ thống xác minh 316 yêu cầu bản tóm lược dữ liệu đã ký của dữ liệu đã truy hồi từ các nút xác minh 330. Hệ thống xác minh 316 có thể tạo ra bản tóm lược dữ liệu của dữ liệu đã truy hồi bằng cách sử dụng các thuật toán băm nêu trên. Tại bước 525, hệ thống xác minh 316 gửi các bản tóm lược dữ liệu đến các nút xác minh 330, sao cho mỗi nút xác minh 330 có thể ký bằng mật mã bản tóm lược dữ liệu của dữ liệu đã truy hồi, và tại bước 530 trả lại phiên bản đã ký của bản tóm lược dữ liệu của chúng cho hệ thống xác minh 316.

Tại bước 535, hệ thống xác minh 316 so sánh các bản tóm lược dữ liệu đã ký của dữ liệu đã truy hồi nhận được từ các nút xác minh 330 với các bản tóm lược dữ liệu đã ký được truy hồi từ chuỗi khối công khai 356 (được tạo ra khi dữ liệu được lưu trữ ban đầu trong mạng chuỗi khối kiểu tập đoàn, xem Fig. 4). Nếu các bản tóm lược dữ liệu đã ký của dữ liệu đã truy hồi nhận được từ các nút xác minh 330 khớp với các bản tóm lược dữ liệu đã ký được truy hồi từ chuỗi khối công khai 356, dữ liệu được lưu trữ trong mạng chuỗi khối kiểu tập đoàn 302 chưa thay đổi kể từ lúc được lưu trữ ban đầu (540).

Quy trình này xác minh rằng dữ liệu được yêu cầu chưa được thay đổi, do nếu nó chưa thay đổi, giá trị của các bản tóm lược dữ liệu đã ký của dữ liệu đã truy hồi được tạo ra bởi các nút xác minh 330 sẽ khớp với các bản tóm lược dữ liệu được lưu trữ trước mà được tạo ra khi dữ liệu được lưu trữ ban đầu. Nếu dữ liệu đã thay đổi sau khi được lưu trữ trong chuỗi khối kiểu tập đoàn, các bản tóm lược dữ liệu đã ký của dữ liệu đã truy hồi sẽ không khớp với các bản tóm lược được lưu trữ trong chuỗi khối công khai 356 khi dữ liệu được lưu trữ ban đầu.

Trong một số trường hợp, hệ thống xác minh 316 chỉ có thể yêu cầu các bản tóm lược dữ liệu đã ký tại bước 520 từ các nút xác minh đã chèn thành công các bản tóm lược dữ liệu đã ký của chúng vào chuỗi khối công khai 356. Ví dụ, mỗi nút xác minh 330 có thể thử lưu trữ mã nhận dạng đơn nhất (ví dụ, khoá công khai) nhận dạng nút cụ thể này cùng với bản tóm lược dữ liệu. Bởi vậy, chỉ các mục được bao gồm trong phiên bản đồng thuận của chuỗi khối công khai 356 sẽ được truy vấn.

Trong một số trường hợp, hệ thống xác minh 316 chỉ có thể yêu cầu việc xác minh từ một tập hợp cụ thể gồm các nút xác minh 330 khi lưu trữ dữ liệu vào chuỗi khối

kiểu tập đoàn 306. Trong một trường hợp như vậy, hệ thống xác minh 316 chỉ có thể truy vấn một tập hợp cụ thể gồm các nút cho các bản tóm lược dữ liệu đã ký khi xác minh rằng dữ liệu đã truy hồi từ chuỗi khối kiểu tập đoàn 306 chưa thay đổi.

Fig. 6 là hình vẽ mô tả quy trình 600 làm ví dụ mà có thể được thực thi theo các phương án thực hiện của sáng chế. Theo một số phương án thực hiện, quy trình 600 có thể được thực hiện bằng cách sử dụng một hoặc nhiều chương trình thực thi được bằng máy tính được thực thi bằng cách sử dụng một hoặc nhiều thiết bị điện toán. Để thể hiện một cách rõ ràng, phần mô tả sau đây mô tả quy trình 600 theo ngữ cảnh của các hình vẽ khác trong bản mô tả. Tuy nhiên, cần hiểu rằng quy trình 600 có thể được thực hiện, ví dụ, bởi bất kỳ trong số hệ thống, môi trường, phần mềm, và phần cứng thích hợp, hoặc sự kết hợp các hệ thống, môi trường, phần mềm, và phần cứng, nếu thích hợp. Theo một số phương án thực hiện, nhiều bước khác nhau của quy trình 600 có thể được thực hiện song song, theo cách kết hợp, theo vòng lặp, hoặc theo trình tự bất kỳ.

Tại bước 602, mục dữ liệu được lưu trữ trong chuỗi khối kiểu tập đoàn được duy trì bởi mạng chuỗi khối kiểu tập đoàn.

Tại bước 604, bản tóm lược dữ liệu thứ nhất được tạo ra dựa trên mục dữ liệu đã lưu.

Tại bước 606, bản tóm lược dữ liệu thứ nhất được gửi đến các nút xác minh, sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ nhất và lưu trữ bản tóm lược dữ liệu thứ nhất đã ký của nó trong chuỗi khối công khai được duy trì bởi mạng chuỗi khối công khai. Theo một số phương án thực hiện, các nút xác minh là các thiết bị điện toán tham gia vào mạng chuỗi khối công khai. Theo một số phương án thực hiện, mỗi nút xác minh được tạo cấu hình để ký bằng mật mã bản tóm lược dữ liệu thứ nhất bằng cách sử dụng khoá bí mật liên kết với nút xác minh trên. Theo một số phương án thực hiện, bước gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh bao gồm bước phát bản tóm lược dữ liệu thứ nhất đến mạng chuỗi khối công khai.

Tại bước 608, yêu cầu được tiếp nhận để truy hồi mục dữ liệu đã lưu.

Tại bước 610, mục dữ liệu được yêu cầu được truy hồi từ chuỗi khối kiểu tập đoàn nhằm đáp lại bước tiếp nhận yêu cầu.

Tại bước 612, bản tóm lược dữ liệu thứ hai được tạo ra dựa trên mục dữ liệu đã truy hồi. Theo một số phương án thực hiện, bước tạo ra bản tóm lược dữ liệu thứ nhất bao gồm bước tính toán giá trị băm của mục dữ liệu đã lưu.

Tại bước 614, bản tóm lược dữ liệu thứ hai được gửi đến các nút xác minh sao cho mỗi nút xác minh có thể ký bằng mật mã các bản tóm lược dữ liệu thứ hai và trả lại bản tóm lược dữ liệu thứ hai đã ký của nó.

Tại bước 616, các bản tóm lược dữ liệu thứ hai đã ký được tiếp nhận từ các nút xác minh.

Tại bước 618, các bản tóm lược dữ liệu thứ nhất đã ký được truy hồi từ chuỗi khối công khai. Theo một số phương án thực hiện, bước truy hồi các bản tóm lược dữ liệu thứ nhất đã ký từ chuỗi khối công khai bao gồm bước nhận dạng các bản tóm lược dữ liệu thứ nhất đã ký dựa trên mã nhận dạng liên kết với mục dữ liệu đã lưu và được lưu trữ trong chuỗi khối công khai.

Tại bước 620, xác định được rằng các bản tóm lược dữ liệu thứ nhất đã ký là khớp với các bản tóm lược dữ liệu thứ hai đã ký.

Tại bước 622, hồi đáp được gửi đến truy hồi mục dữ liệu đã lưu nhằm đáp lại bước xác định, hồi đáp này chỉ báo rằng mục dữ liệu đã lưu chưa thay đổi kể từ lúc được lưu trữ.

Theo một số phương án thực hiện, quy trình 600 còn bao gồm bước lưu trữ hợp đồng thông minh trong chuỗi khối công khai, trong đó hợp đồng thông minh được tạo cấu hình để tạo phần thưởng tiền cho các nút xác minh nhằm đáp lại bước tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký được yêu cầu từ các nút xác minh.

Dựa vào Fig. 7, Fig. 7 là hình vẽ thể hiện một ví dụ về sơ đồ minh họa các mô đun của thiết bị theo các phương án thực hiện của sáng chế. Thiết bị 700 có thể là phương án thực hiện được lấy làm ví dụ để lưu trữ và truy hồi dữ liệu cần xác minh liên kết với các nút của mạng chuỗi khối. Thiết bị 700 có thể tương ứng với phương án thực hiện được thể hiện trên các hình vẽ từ Fig. 3 đến Fig.5, và thiết bị 700 bao gồm: bộ lưu trữ hoặc bộ phận lưu trữ 705, được tạo cấu hình để lưu trữ mục dữ liệu trong chuỗi khối kiểu tập đoàn được duy trì mạng chuỗi khối kiểu tập đoàn; bộ sinh hoặc bộ phận sinh thứ nhất 710, được tạo cấu hình để tạo ra bản tóm lược dữ liệu thứ nhất dựa trên mục dữ

liệu đã lưu; bộ truyền hoặc bộ phận truyền thứ hai 715, được tạo cấu hình để gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh, mỗi nút xác minh được tạo cấu hình để ký bằng mật mã bản tóm lược dữ liệu thứ nhất của nó và lưu trữ bản tóm lược dữ liệu thứ nhất đã ký của nó trong chuỗi khối công khai được duy trì bởi mạng chuỗi khối công khai; bộ thu hoặc bộ phận thu 720, được tạo cấu hình để tiếp nhận yêu cầu truy hồi mục dữ liệu đã lưu; bộ truy hồi thứ nhất 725, được tạo cấu hình để truy hồi mục dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn nhằm đáp lại bước tiếp nhận yêu cầu; bộ sinh hoặc bộ phận sinh thứ hai 730, được tạo cấu hình để tạo ra bản tóm lược dữ liệu thứ hai dựa trên mục dữ liệu đã truy hồi; bộ yêu cầu hoặc bộ phận yêu cầu 735, được tạo cấu hình để yêu cầu các bản tóm lược dữ liệu thứ hai được chỉ định từ các nút xác minh và đáp lại bước tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký được yêu cầu từ các nút xác minh; bộ truy hồi thứ hai 740, được tạo cấu hình để truy hồi các bản tóm lược dữ liệu thứ nhất đã ký từ chuỗi khối công khai; bộ xác định 745, được tạo cấu hình để xác định rằng các bản tóm lược dữ liệu thứ nhất đã ký từ chuỗi khối công khai khớp với các bản tóm lược dữ liệu thứ hai đã ký nhận được từ các nút xác minh; bộ truyền hoặc bộ phận truyền thứ hai 750, được tạo cấu hình để gửi hồi đáp để yêu cầu truy hồi dữ liệu được lưu trữ bao gồm mục dữ liệu đã lưu nhằm đáp lại bước xác định, hồi đáp này chỉ báo rằng mục dữ liệu đã lưu chưa thay đổi kể từ lúc được lưu trữ.

Theo một phương án thực hiện tùy ý, các nút xác minh là các thiết bị điện toán tham gia vào mạng chuỗi khối công khai.

Theo một phương án thực hiện tùy ý, thiết bị 700 còn bao gồm: bộ lưu trữ hoặc bộ lưu trữ con, được tạo cấu hình để lưu trữ hợp đồng thông minh trong chuỗi khối công khai, trong đó hợp đồng thông minh được tạo cấu hình để tạo phần thưởng tiền cho các nút xác minh nhằm đáp lại bước tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký được yêu cầu từ các nút xác minh.

Theo một phương án thực hiện tùy ý, thiết bị 700 còn bao gồm: bộ tính hoặc bộ phận tính, được tạo cấu hình để tính toán giá trị băm của mục dữ liệu đã lưu.

Theo một phương án thực hiện tùy ý, mỗi nút xác minh được tạo cấu hình để ký bằng mật mã bản tóm lược dữ liệu thứ nhất bằng cách sử dụng khoá bí mật liên kết với nút xác minh trên.

Theo một phương án thực hiện tùy ý, thiết bị 700 còn bao gồm các phần sau: bộ phát con, được tạo cấu hình để phát bản tóm lược dữ liệu thứ nhất đến mạng chuỗi khối công khai.

Theo một phương án thực hiện tùy ý, thiết bị 700 còn bao gồm: mã nhận dạng hoặc bộ nhận dạng con, được tạo cấu hình để nhận dạng các bản tóm lược dữ liệu thứ nhất đã ký dựa trên mã nhận dạng liên kết với mục dữ liệu đã lưu và được lưu trữ trong chuỗi khối công khai.

Hệ thống, thiết bị, môđun, hoặc khối được minh họa theo các phương án thực hiện trên đây có thể được thực hiện bằng cách sử dụng chip máy tính hoặc thực thể, hoặc có thể được thực hiện bằng cách sử dụng sản phẩm có chức năng nhất định. Thiết bị thực hiện điển hình là máy tính, và máy tính này có thể là máy tính cá nhân, máy tính xách tay, điện thoại di động, điện thoại camera, điện thoại thông minh, trợ lý kỹ thuật số cá nhân, trình phát đa phương tiện, thiết bị định vị, thiết bị tiếp nhận và gửi thư điện tử, bảng kiểm soát trò chơi, máy tính dạng bảng, thiết bị đeo được hoặc sự kết hợp bất kỳ của các thiết bị này.

Đối với quy trình thực hiện các chức năng và các vai trò của mỗi bộ phận khác nhau trong thiết bị, có thể tham khảo quá trình thực hiện các bước tương ứng của phương pháp trên đây. Chi tiết được lược bớt tại đây để đơn giản.

Bởi vì phương án thực hiện của thiết bị về cơ bản tương ứng với phương án thực hiện của phương pháp, nên đối với các phần liên quan, có thể tham khảo phần mô tả liên quan theo phương án thực hiện của phương pháp này. Phương án thực hiện của thiết bị được mô tả trên đây chỉ là ví dụ,. Các khối được mô tả là các phần riêng biệt có thể hoặc có thể không tách biệt về mặt vật lý, và các phần được hiển thị dưới dạng các khối có thể hoặc có thể không là các khối vật lý, có thể được bố trí ở một vị trí, hoặc có thể được phân tán trên các thiết bị mạng. Một số hoặc toàn bộ các môđun có thể được chọn dựa trên nhu cầu thực tế để đạt được các mục đích của các giải pháp theo sáng chế. Người có hiểu biết trung bình về lĩnh vực kỹ thuật có thể hiểu và thực hiện các phương án thực hiện của sáng chế mà không cần phải nỗ lực sáng tạo.

Fig. 7 là sơ đồ giản lược minh họa môđun chức năng nội bộ và cấu trúc của thiết bị mạng chuỗi khối kiểu tập đoàn. Thân thực thi về bản chất có thể là thiết bị điện tử, và thiết bị điện tử này bao gồm: một hoặc nhiều bộ xử lý; và bộ nhớ được tạo cấu hình để

lưu trữ lệnh thực thi được của một hoặc nhiều bộ xử lý.

Một hoặc nhiều bộ xử lý được tạo cấu hình để lưu trữ mục dữ liệu trong chuỗi khối kiểu tập đoàn được duy trì bởi mạng chuỗi khối kiểu tập đoàn; tạo ra bản tóm lược dữ liệu thứ nhất dựa trên mục dữ liệu đã lưu; gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh, mỗi nút xác minh được tạo cấu hình để ký bằng mật mã bản tóm lược dữ liệu thứ nhất và lưu trữ bản tóm lược dữ liệu thứ nhất đã ký của nó trong chuỗi khối công khai được duy trì bởi mạng chuỗi khối công khai; tiếp nhận yêu cầu truy hồi mục dữ liệu đã lưu; truy hồi mục dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn nhằm đáp lại bước tiếp nhận yêu cầu; tạo ra bản tóm lược dữ liệu thứ hai dựa trên mục dữ liệu đã truy hồi; yêu cầu các bản tóm lược dữ liệu thứ hai đã ký từ các nút xác minh và đáp lại bước tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký được yêu cầu từ các nút; truy hồi các bản tóm lược dữ liệu thứ nhất đã ký từ chuỗi khối công khai; xác định rằng các bản tóm lược dữ liệu thứ nhất đã ký từ chuỗi khối công khai khớp với các bản tóm lược dữ liệu thứ hai đã ký nhận được từ các nút xác minh; và gửi hồi đáp để yêu cầu truy hồi dữ liệu được lưu trữ bao gồm mục dữ liệu đã lưu nhằm đáp lại bước xác định nhằm đáp lại bước xác định, hồi đáp này chỉ báo rằng mục dữ liệu đã lưu chưa thay đổi kể từ lúc được lưu trữ.

Tuỳ ý, các nút xác minh là các thiết bị điện toán tham gia vào mạng chuỗi khối công khai.

Tuỳ ý, một hoặc nhiều bộ xử lý được tạo cấu hình để lưu trữ hợp đồng thông minh trong chuỗi khối công khai, trong đó hợp đồng thông minh này được tạo cấu hình để tạo phần thưởng tiền cho các nút xác minh nhằm đáp lại bước tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký được yêu cầu từ các nút xác minh.

Tuỳ ý, một hoặc nhiều bộ xử lý được tạo cấu hình để tính toán giá trị băm của mục dữ liệu đã lưu.

Tuỳ ý, mỗi nút xác minh được tạo cấu hình để ký bằng mật mã bản tóm lược dữ liệu thứ nhất bằng cách sử dụng khoá bí mật liên kết với nút xác minh trên.

Tuỳ ý, một hoặc nhiều bộ xử lý được tạo cấu hình để phát bản tóm lược dữ liệu thứ nhất đến mạng chuỗi khối công khai.

Tuỳ ý, một hoặc nhiều bộ xử lý được tạo cấu hình để nhận dạng các bản tóm lược

dữ liệu thứ nhất đã ký dựa trên mã nhận dạng liên kết với mục dữ liệu đã lưu và được lưu trữ trong chuỗi khối công khai.

Các phương án thực hiện của đối tượng bảo hộ và các bước và các hoạt động được mô tả trong bản mô tả này có thể được thực hiện trong các mạch điện kỹ thuật số, trong phần mềm hoặc phần sụn máy tính được bao gồm hữu hình, trong phần cứng máy tính, bao gồm các cấu trúc đã được bộc lộ trong bản mô tả này và các phương án tương đương về cấu trúc của chúng, hoặc trong các sự kết hợp của một hoặc nhiều cấu trúc này. Các phương án thực hiện của đối tượng được mô tả trong bản mô tả này có thể được thực hiện dưới dạng một hoặc nhiều chương trình máy tính, ví dụ, một hoặc nhiều môđun chứa các lệnh chương trình máy tính, các chương trình máy tính này được mã hóa trên vật mang chương trình máy tính, để thực thi bằng thiết bị xử lý dữ liệu, hoặc để điều khiển hoạt động của thiết bị xử lý dữ liệu. Vật mang này có thể là vật ghi bằng máy tính lâu dài hữu hình. Ngoài ra hoặc theo một cách khác, vật mang này có thể là tín hiệu được truyền được tạo ra theo cách nhân tạo, ví dụ, tín hiệu điện, quang, hoặc điện từ được tạo ra bằng máy mà được tạo ra để mã hóa thông tin nhằm truyền đến thiết bị thu thích hợp để thực thi bởi thiết bị xử lý dữ liệu. Vật ghi máy tính có thể là hoặc là một phần của thiết bị lưu trữ đọc được bằng máy, phương tiện lưu trữ đọc được bằng máy, thiết bị bộ nhớ truy cập ngẫu nhiên hoặc nối tiếp, hoặc sự kết hợp của một hoặc nhiều thiết bị trong số các thiết bị này. Vật ghi máy tính không phải là tín hiệu được truyền.

Thuật ngữ “thiết bị xử lý dữ liệu” bao gồm tất cả các loại thiết bị, công cụ, và máy để xử lý dữ liệu, bao gồm, ví dụ, bộ xử lý lập trình được, máy tính, hoặc nhiều bộ xử lý hoặc máy tính. Thiết bị xử lý dữ liệu có thể bao gồm mạch logic chuyên dụng, ví dụ, FPGA (mảng cổng lập trình được dạng trường), ASIC (mạch tích hợp chuyên dụng), hoặc GPU (bộ phận xử lý đồ họa). Thiết bị này cũng có thể chứa, ngoài phần cứng, mã tạo ra môi trường thực thi cho các chương trình máy tính, ví dụ, mã tạo thành phần sụn bộ xử lý, chồng giao thức, hệ thống quản lý cơ sở dữ liệu, hệ điều hành, hoặc sự kết hợp của một hoặc nhiều trong số chúng.

Chương trình máy tính, mà cũng có thể được gọi hoặc được mô tả là chương trình, phần mềm, ứng dụng phần mềm, ứng dụng, môđun, môđun phần mềm, máy, tập lệnh, hoặc mã, có thể được ghi dưới dạng ngôn ngữ lập trình bất kỳ, bao gồm các ngôn

ngữ biên dịch hoặc thông dịch, hoặc các ngôn ngữ khai báo hoặc thủ tục; và nó có thể được triển khai dưới dạng bất kỳ, bao gồm dưới dạng chương trình độc lập hoặc dưới dạng môđun, bộ phận, máy, chương trình con, hoặc bộ phận khác thích hợp để thực thi trong môi trường điện toán, môi trường này có thể bao gồm một hoặc nhiều máy tính được liên kết bởi mạng truyền thông dữ liệu ở một hoặc nhiều vị trí.

Chương trình máy tính có thể, nhưng không cần, tương ứng với một tệp tin trong hệ thống tệp tin. Chương trình máy tính 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 tập lệnh 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, các chương trình con, hoặc các đoạn mã.

Các quy trình và luồng logic được nêu trong bản mô tả có thể được thực hiện bằng một hoặc nhiều máy tính mà thực thi một hoặc nhiều chương trình máy tính để thực hiện các hoạt động bằng cách thao tác trên dữ liệu đầu vào và tạo đầu ra. Các quy trình và luồng logic cũng có thể được thực hiện bởi mạch logic chuyên dụng, ví dụ, FPGA, ASIC, hoặc GPU, hoặc bởi sự kết hợp của mạch logic chuyên dụng và một hoặc nhiều máy tính được lập trình.

Các máy tính thích hợp để thực thi chương trình máy tính có thể dựa vào các bộ vi xử lý chung hoặc chuyên dụng, cả hai, hoặc bất kỳ loại bộ xử lý trung tâm nào khác. Nói chung, bộ xử lý trung tâm sẽ nhận lệnh và dữ liệu từ bộ nhớ chỉ đọc hoặc bộ nhớ truy cập ngẫu nhiên hoặc cả hai. Các bộ phận của máy tính có thể bao gồm bộ xử lý trung tâm để thực thi lệnh và một hoặc nhiều thiết bị nhớ để lưu trữ lệnh và dữ liệu. Bộ xử lý trung tâm và bộ nhớ này có thể được bổ sung bởi, hoặc được đưa vào trong, các mạch logic chuyên dụng.

Nói chung, máy tính sẽ được lắp vào ít nhất một vật ghi lâu dài đọc được bằng máy tính (cũng được gọi là bộ nhớ đọc được bằng máy tính). Vật ghi được lắp vào máy tính có thể là bộ phận bên trong của máy tính (ví dụ, ổ cứng tích hợp) hoặc bộ phận bên ngoài (ví dụ, ổ cứng buýt nối tiếp đa năng (USB) hoặc hệ lưu trữ được truy cập qua mạng). Các ví dụ về vật ghi có thể bao gồm, ví dụ, đĩa từ, đĩa quang từ, hoặc đĩa quang, ổ lưu trữ thể rắn (solid state drive), nguồn lưu trữ mạng như hệ lưu trữ đám mây, hoặc các loại vật ghi khác. Tuy nhiên, máy tính không cần có các thiết bị như vậy. Ngoài ra,

máy tính có thể được nhúng trong một thiết bị khác, ví dụ, điện thoại di động, thiết bị kỹ thuật số hỗ trợ cá nhân (PDA - Personal Digital Assistant), thiết bị phát video hoặc âm thanh di động, thiết bị điều khiển trò chơi, bộ thu hệ thống định vị toàn cầu (GPS - Global Positioning System), hoặc thiết bị lưu trữ di động, ví dụ, ổ bus nối tiếp đa năng (USB) chớp, và còn nhiều thiết bị khác.

Để tạo tương tác với người sử dụng, các phương án thực hiện của các đối tượng được nêu trong bản mô tả có thể được tiến hành trên, hoặc được tạo cấu hình để giao tiếp với, máy tính có thiết bị hiển thị, ví dụ, màn hình LCD (tinh thể lỏng) để hiển thị thông tin cho người sử dụng và thiết bị đầu vào mà người sử dụng có thể cung cấp đầu vào cho máy tính như bàn phím và thiết bị trỏ như chuột, bi xoay hoặc vùng chạm. Các loại thiết bị khác có thể được sử dụng để tạo ra tương tác với người sử dụng như; ví dụ, hồi đáp được tạo ra cho người sử dụng có thể ở dạng hồi đáp cảm giác bất kỳ, ví dụ, hồi đáp trực quan, hồi đáp thính giác, hoặc hồi đáp xúc giác; và được nhập vào từ người sử dụng có thể được tiếp nhận dưới dạng bất kỳ, bao gồm đầu vào âm thanh, tốc độ, hoặc xúc giác. Ngoài ra, máy tính có thể tương tác với người sử dụng bằng cách gửi các tài liệu tới thiết bị được sử dụng bởi người sử dụng và tiếp nhận các tài liệu từ thiết bị này; ví dụ, bằng cách gửi các trang web đến trình duyệt web trên thiết bị của người sử dụng để đáp ứng lại các yêu cầu được tiếp nhận từ trình duyệt web. Máy tính cũng có thể tương tác với người sử dụng bằng cách gửi tin nhắn dạng văn bản hoặc các dạng tin nhắn khác tới thiết bị cá nhân, ví dụ, điện thoại thông minh đang chạy ứng dụng nhắn tin, và nhận lại tin nhắn hồi đáp từ người sử dụng.

Bản mô tả sử dụng thuật ngữ “được tạo cấu hình để” trong kết nối với hệ thống, thiết bị, và các thành phần chương trình máy tính. Để hệ thống của một hoặc nhiều máy tính được tạo cấu hình để thực hiện các hoạt động hoặc thao tác cụ thể có nghĩa là hệ thống này đã được cài đặt phần mềm, phần sụn, phần cứng, hoặc sự kết hợp của chúng mà khi hoạt động khiến cho hệ thống thực hiện các hoạt động hoặc thao tác này. Để một hoặc nhiều chương trình máy tính được tạo cấu hình để thực hiện các hoạt động hoặc thao tác cụ thể có nghĩa là một hoặc nhiều chương trình này bao gồm các lệnh mà, khi được thực thi bằng thiết bị xử lý dữ liệu, khiến thiết bị này thực hiện các hoạt động hoặc thao tác này. Để mạch logic chuyên dụng được tạo cấu hình để thực hiện các hoạt động

hoặc thao tác cụ thể có nghĩa là mạch có logic điện tử mà thực hiện các hoạt động hoặc thao tác này.

Mặc dù bản mô tả này chứa nhiều chi tiết của phương án thực hiện cụ thể, những điều này không nên được hiểu là làm giới hạn phạm vi của sáng chế về đối tượng bảo hộ trong các điểm yêu cầu bảo hộ, mà nên được hiểu là mô tả về các dấu hiệu dành riêng cho các phương án thực hiện cụ thể. Các dấu hiệu nhất định mà được mô tả trong bản mô tả trong ngữ cảnh của các phương án thực hiện riêng biệt cũng có thể được thực hiện, theo cách kết hợp theo một phương án thực hiện. Ngược lại, các dấu hiệu khác nhau mà được mô tả trong ngữ cảnh theo một phương án thực hiện cũng có thể được thực hiện theo nhiều phương án thực hiện một cách riêng biệt, hoặc theo cách kết hợp phụ bất kỳ. Ngoài ra, mặc dù các dấu hiệu này có thể được mô tả ở trên có mặt theo các cách 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 loại bỏ khỏi kết hợp và kết hợp được yêu cầu bảo hộ có thể nhắm đến kết hợp phụ hoặc biến thể của kết hợp phụ.

Tương tự, mặc dù các hoạt động được mô tả trên các hình vẽ hoặc các điểm yêu cầu bảo hộ theo thứ tự cụ thể, nhưng điều này không nên được hiểu là yêu cầu rằng các hoạt động như vậy phải được thực hiện theo thứ tự cụ thể được thể hiện hoặc theo thứ tự lần lượt, hoặc toàn bộ các hoạt động được minh họa phải được thực hiện, để đạt được các kết quả mong muốn. Trong một số trường hợp nhất định, việc xử lý đa nhiệm và song song có thể là ưu điểm. Ngoài ra, việc tách các mô đun và các thành phần khác nhau trong các phương án thực hiện nêu trên không nên được hiểu là cần phải tách như trên theo toàn bộ các phương án thực hiện, và nên được hiểu là các hệ thống và thành phần chương trình đã nêu có thể thường được tích hợp với nhau trong một sản phẩm phần mềm hoặc được tạo gói thành nhiều sản phẩm phần mềm.

Các phương án thực hiện cụ thể của đối tượng đã được mô tả. Các phương án khác nằm trong phạm vi của các yêu cầu bảo hộ sau đây. Ví dụ, các thao tác được nêu trong các điểm yêu cầu bảo hộ có thể được thực hiện theo thứ tự khác và vẫn đạt được kết quả mong đợi. Theo một ví dụ, các quy trình được mô tả trên các hình vẽ kèm theo không nhất thiết phải theo thứ tự cụ thể được thể hiện, hoặc theo thứ tự liên tiếp, để đạt

được kết quả mong đợi. Trong một số trường hợp, việc xử lý đa nhiệm và song song có thể là ưu điểm.

YÊU CẦU BẢO HỘ

1. Phương pháp được thực hiện bằng máy tính xác minh tính toàn vẹn của dữ liệu được lưu trữ trong chuỗi khối kiểu tập đoàn, trong đó phương pháp này bao gồm các bước:

lưu trữ mục dữ liệu trong chuỗi khối kiểu tập đoàn được duy trì bởi mạng chuỗi khối kiểu tập đoàn;

tạo ra bản tóm lược dữ liệu thứ nhất dựa trên mục dữ liệu đã lưu;

gửi bản sao của bản tóm lược dữ liệu thứ nhất đến mỗi nút trong số các nút xác minh tham gia vào mạng chuỗi khối công khai sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ nhất và lưu trữ bản sao tương tự của bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất trong chuỗi khối công khai được duy trì bởi mạng chuỗi khối công khai;

tiếp nhận, bởi mạng chuỗi khối kiểu tập đoàn, yêu cầu truy hồi mục dữ liệu đã lưu;

truy hồi mục dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn nhằm đáp lại bước tiếp nhận yêu cầu;

tạo ra bản tóm lược dữ liệu thứ hai dựa trên mục dữ liệu đã truy hồi từ chuỗi khối kiểu tập đoàn;

gửi bản sao của bản tóm lược dữ liệu thứ hai đến mỗi nút trong số các nút xác minh sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ hai và trả lại bản sao tương tự của bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai;

tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai từ các nút xác minh;

truy hồi các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất từ các nút xác minh của chuỗi khối công khai bằng cách nhận dạng các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất dựa trên mã nhận dạng liên kết với mục dữ liệu được lưu trữ và được lưu trữ trong chuỗi khối công khai;

xác định rằng các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất khớp với các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai; và

gửi hồi đáp để yêu cầu truy hồi mục dữ liệu đã lưu nhằm đáp lại bước xác định là các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất khớp với các bản tóm

lược dữ liệu thứ hai đã ký bằng mật mã thứ hai, hồi đáp này chỉ báo rằng mục dữ liệu đã lưu chưa thay đổi kể từ khi được lưu trữ trong chuỗi khối kiểu tập đoàn.

2. Phương pháp được thực hiện bằng máy tính theo điểm 1, còn bao gồm bước lưu trữ hợp đồng thông minh trong chuỗi khối công khai, trong đó hợp đồng thông minh được tạo cấu hình để tạo phần thưởng tiền cho các nút xác minh nhằm đáp lại bước tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai được yêu cầu từ các nút xác minh.

3. Phương pháp được thực hiện bằng máy tính theo điểm 1, trong đó bước tạo ra bản tóm lược dữ liệu thứ nhất bao gồm bước tính toán giá trị băm của mục dữ liệu đã lưu.

4. Phương pháp được thực hiện bằng máy tính theo điểm 1, trong đó mỗi nút xác minh được tạo cấu hình để ký bằng mật mã bản tóm lược dữ liệu thứ nhất bằng cách sử dụng khoá bí mật liên kết với nút xác minh trên.

5. Phương pháp được thực hiện bằng máy tính theo điểm 1, trong đó bước gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh bao gồm bước phát bản tóm lược dữ liệu thứ nhất đến mạng chuỗi khối công khai.

6. Vật ghi lâu dài được bằng máy tính lưu trữ một hoặc nhiều lệnh thực thi được bằng hệ thống máy tính để thực hiện các thao tác bao gồm:

lưu trữ mục dữ liệu trong chuỗi khối kiểu tập đoàn được duy trì bởi mạng chuỗi khối kiểu tập đoàn;

tạo ra bản tóm lược dữ liệu thứ nhất dựa trên mục dữ liệu đã lưu;

gửi bản sao của bản tóm lược dữ liệu thứ nhất đến mỗi nút trong số các nút xác minh tham gia vào mạng chuỗi khối công khai sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ nhất và lưu trữ bản sao tương tự của bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất trong chuỗi khối công khai được duy trì bởi mạng chuỗi khối công khai;

tiếp nhận, bởi mạng chuỗi khối kiểu tập đoàn, yêu cầu truy hồi mục dữ liệu đã lưu;

truy hồi mục dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn nhằm đáp lại bước tiếp nhận yêu cầu;

tạo ra bản tóm lược dữ liệu thứ hai dựa trên mục dữ liệu đã truy hồi từ chuỗi khối kiểu tập đoàn;

gửi bản sao của bản tóm lược dữ liệu thứ hai đến mỗi nút trong số các nút xác minh sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ hai và trả lại bản sao tương tự của bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai;

tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai từ các nút xác minh;

truy hồi các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất từ các nút xác minh của chuỗi khối công khai bằng cách nhận dạng các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất dựa trên mã nhận dạng liên kết với mục dữ liệu được lưu trữ và được lưu trữ trong chuỗi khối công khai;

xác định rằng các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất khớp với các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai; và

gửi hồi đáp để yêu cầu truy hồi mục dữ liệu đã lưu nhằm đáp lại bước xác định là các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất khớp với các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai, hồi đáp này chỉ báo rằng mục dữ liệu đã lưu chưa được thay đổi kể từ khi được lưu trữ trong chuỗi khối kiểu tập đoàn.

7. Vật ghi lâu dài đọc được bằng máy tính theo điểm 6, trong đó các thao tác bao gồm:

lưu trữ hợp đồng thông minh trong chuỗi khối công khai, trong đó hợp đồng thông minh được tạo cấu hình để tạo phần thưởng tiền cho các nút xác minh nhằm đáp lại bước tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai được yêu cầu từ các nút xác minh.

8. Vật ghi lâu dài đọc được bằng máy tính theo điểm 6, trong đó bước tạo ra bản tóm lược dữ liệu thứ nhất bao gồm bước tính toán giá trị băm của mục dữ liệu đã lưu.

9. Vật ghi lâu dài đọc được bằng máy tính theo điểm 6, trong đó mỗi nút xác minh được tạo cấu hình để ký bằng mật mã bản tóm lược dữ liệu thứ nhất bằng cách sử dụng khoá bí mật liên kết với nút xác minh trên.

10. Vật ghi lâu dài đọc được bằng máy tính theo điểm 6, trong đó bước gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh bao gồm bước phát bản tóm lược dữ liệu thứ nhất đến mạng chuỗi khối công khai.

11. Hệ thống xác minh tính toàn vẹn của dữ liệu được lưu trữ trong chuỗi khối kiểu tập đoàn, trong đó hệ thống này bao gồm:

một hoặc nhiều máy tính; và

một hoặc nhiều thiết bị nhớ máy tính được lắp tương thích với một hoặc nhiều máy tính và có vật ghi đọc được bằng máy, lâu dài, hữu hình lưu trữ một hoặc nhiều lệnh mà, khi được thực thi bằng một hoặc nhiều máy tính, thực hiện một hoặc nhiều thao tác bao gồm:

lưu trữ mục dữ liệu trong chuỗi khối kiểu tập đoàn được duy trì bởi mạng chuỗi khối kiểu tập đoàn;

tạo ra bản tóm lược dữ liệu thứ nhất dựa trên mục dữ liệu đã lưu;

gửi bản sao của bản tóm lược dữ liệu thứ nhất đến mỗi nút trong số các nút xác minh tham gia vào mạng chuỗi khối công khai sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ nhất và lưu trữ bản sao tương tự của bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất trong chuỗi khối công khai được duy trì bởi mạng chuỗi khối công khai;

tiếp nhận, bởi mạng chuỗi khối kiểu tập đoàn, yêu cầu truy hồi mục dữ liệu đã lưu;

truy hồi mục dữ liệu được yêu cầu từ chuỗi khối kiểu tập đoàn nhằm đáp lại bước tiếp nhận yêu cầu;

tạo ra bản tóm lược dữ liệu thứ hai dựa trên mục dữ liệu đã truy hồi từ chuỗi khối kiểu tập đoàn;

gửi bản sao của bản tóm lược dữ liệu thứ hai đến mỗi nút trong số các nút xác minh sao cho mỗi nút xác minh ký bằng mật mã bản tóm lược dữ liệu thứ hai và trả lại bản sao tương tự của bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai;

tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai từ các nút xác minh;

truy hồi các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất từ các nút xác minh của chuỗi khối công khai bằng cách nhận dạng các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất dựa trên mã nhận dạng liên kết với mục dữ liệu được lưu trữ và được lưu trữ trong chuỗi khối công khai;

xác định rằng các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất khớp với các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai; và

gửi hồi đáp để yêu cầu truy hồi mục dữ liệu đã lưu nhằm đáp lại bước xác định là các bản tóm lược dữ liệu thứ nhất đã ký bằng mật mã thứ nhất khớp với các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai, hồi đáp này chỉ báo rằng mục dữ liệu đã lưu chưa được thay đổi kể từ khi được lưu trữ trong chuỗi khối kiểu tập đoàn.

12. Hệ thống theo điểm 11, trong đó các thao tác còn bao gồm:

lưu trữ hợp đồng thông minh trong chuỗi khối công khai, trong đó hợp đồng thông minh được tạo cấu hình để tạo phần thưởng tiền cho các nút xác minh nhằm đáp lại bước tiếp nhận các bản tóm lược dữ liệu thứ hai đã ký bằng mật mã thứ hai được yêu cầu từ các nút xác minh.

13. Hệ thống theo điểm 11, trong đó bước tạo ra bản tóm lược dữ liệu thứ nhất bao gồm bước tính toán giá trị băm của mục dữ liệu đã lưu.

14. Hệ thống theo điểm 11, trong đó mỗi nút xác minh được tạo cấu hình để ký bằng mật mã bản tóm lược dữ liệu thứ nhất bằng cách sử dụng khoá bí mật liên kết với nút xác minh trên.

15. Hệ thống theo điểm 11, trong đó bước gửi bản tóm lược dữ liệu thứ nhất đến các nút xác minh bao gồm bước phát bản tóm lược dữ liệu thứ nhất đến mạng chuỗi khối công khai.

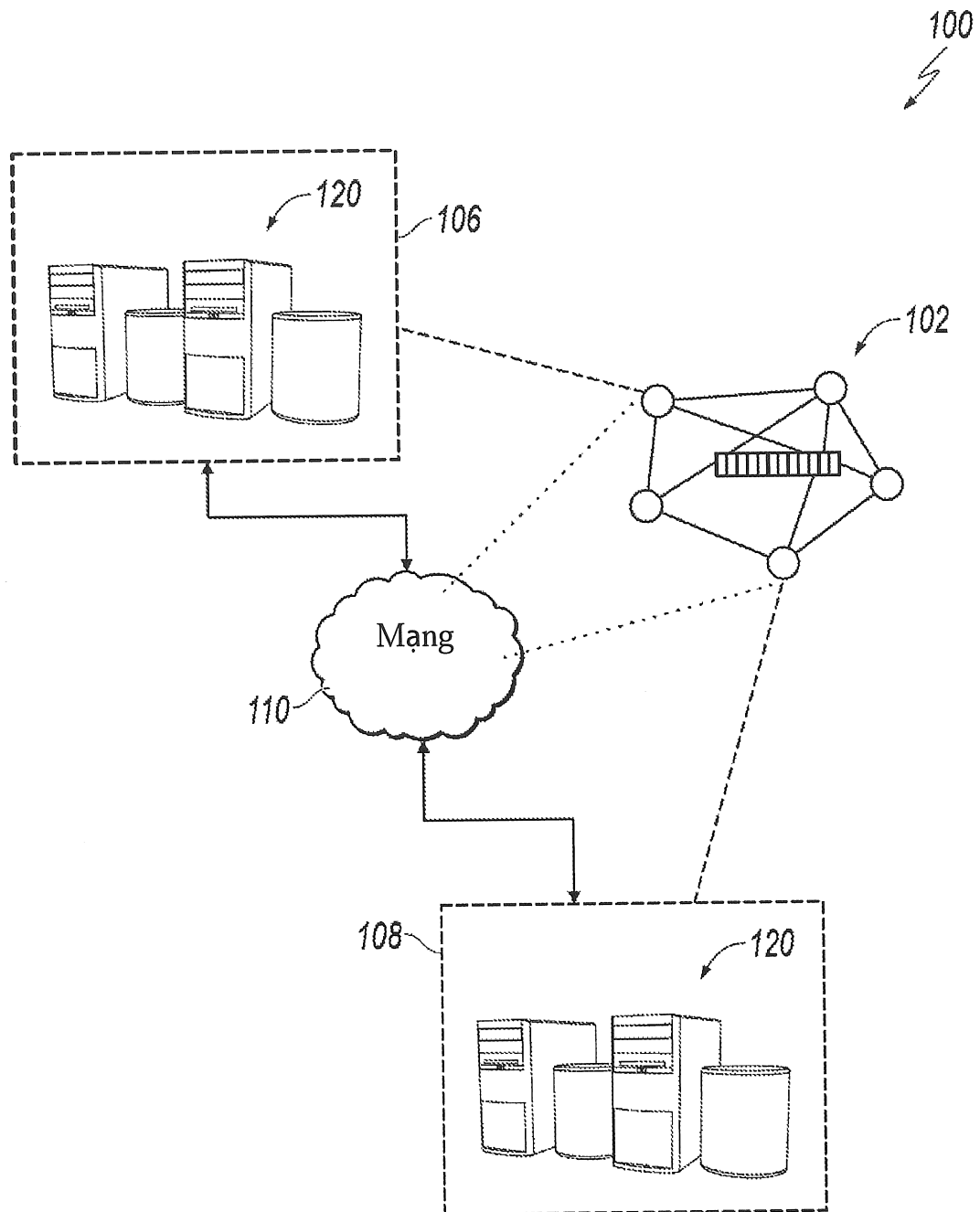


FIG. 1

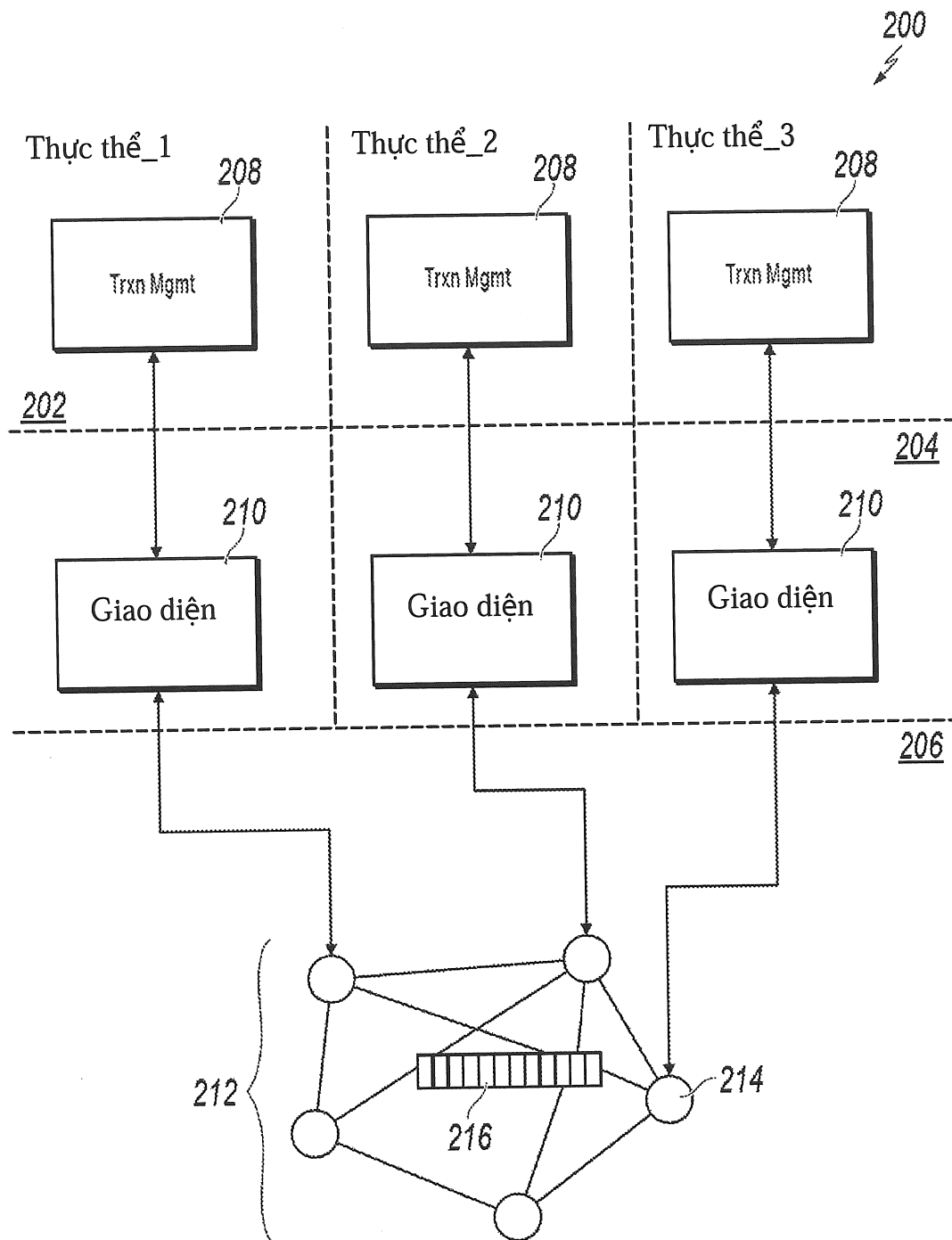


FIG. 2

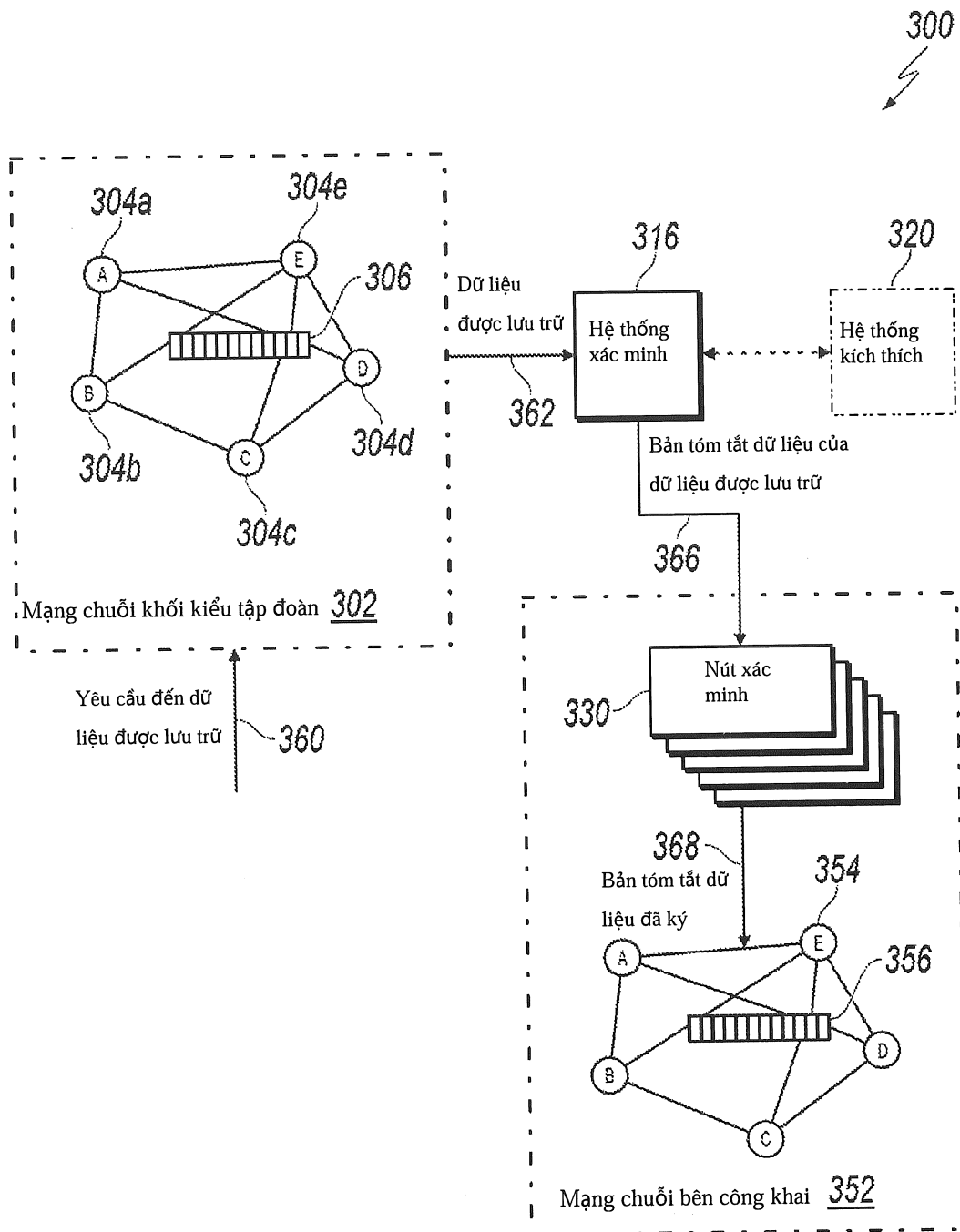


FIG. 3

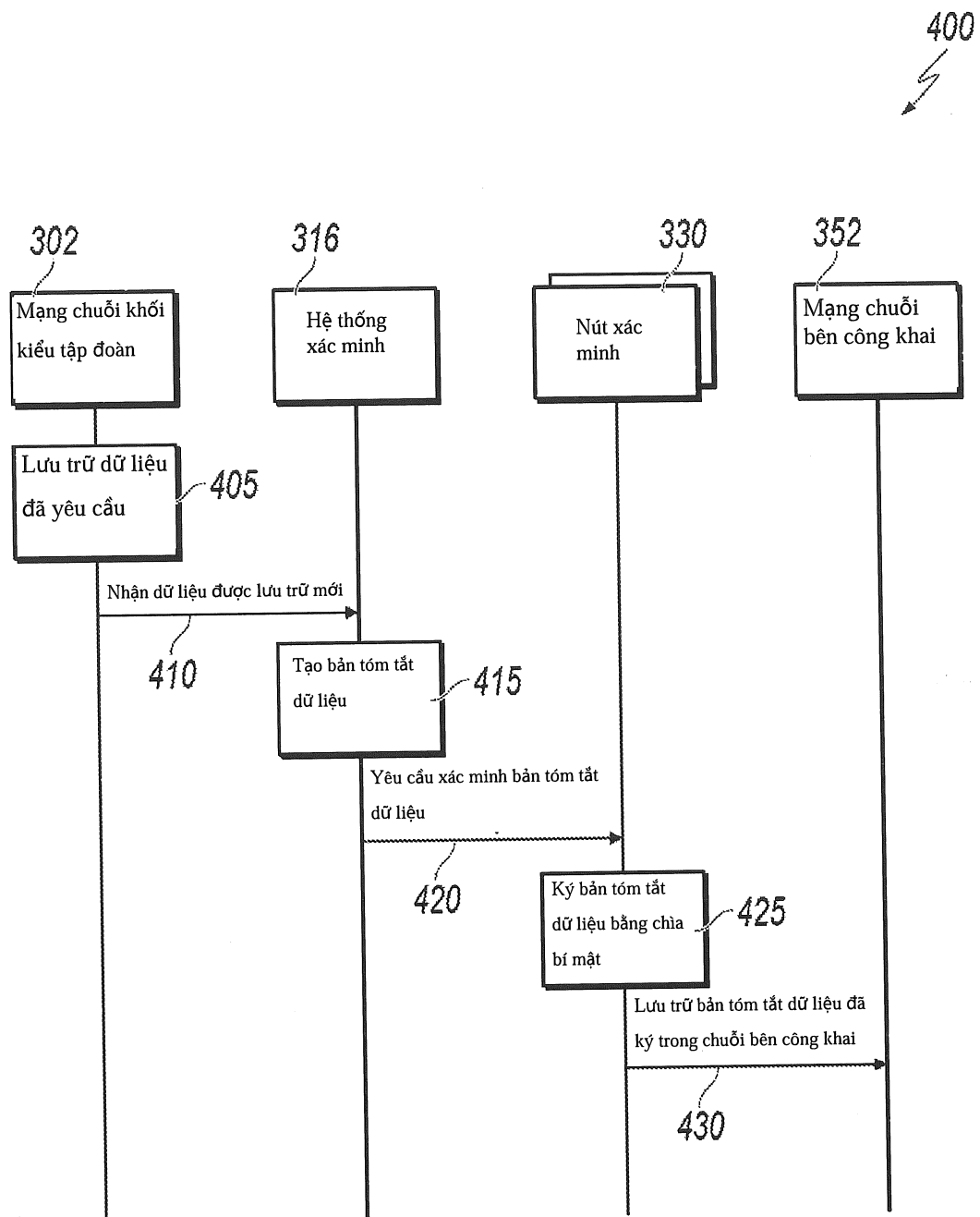


FIG. 4

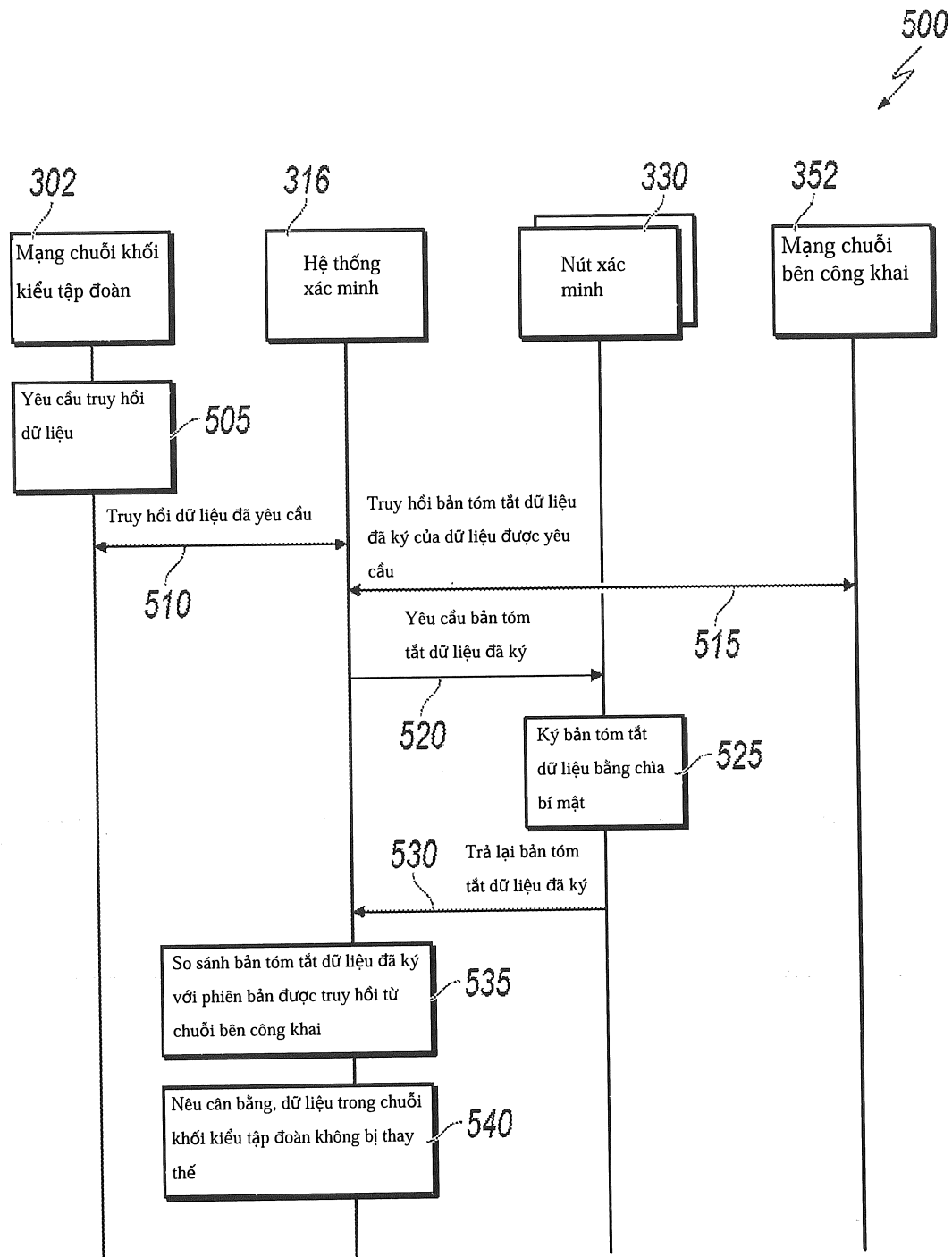


FIG. 5

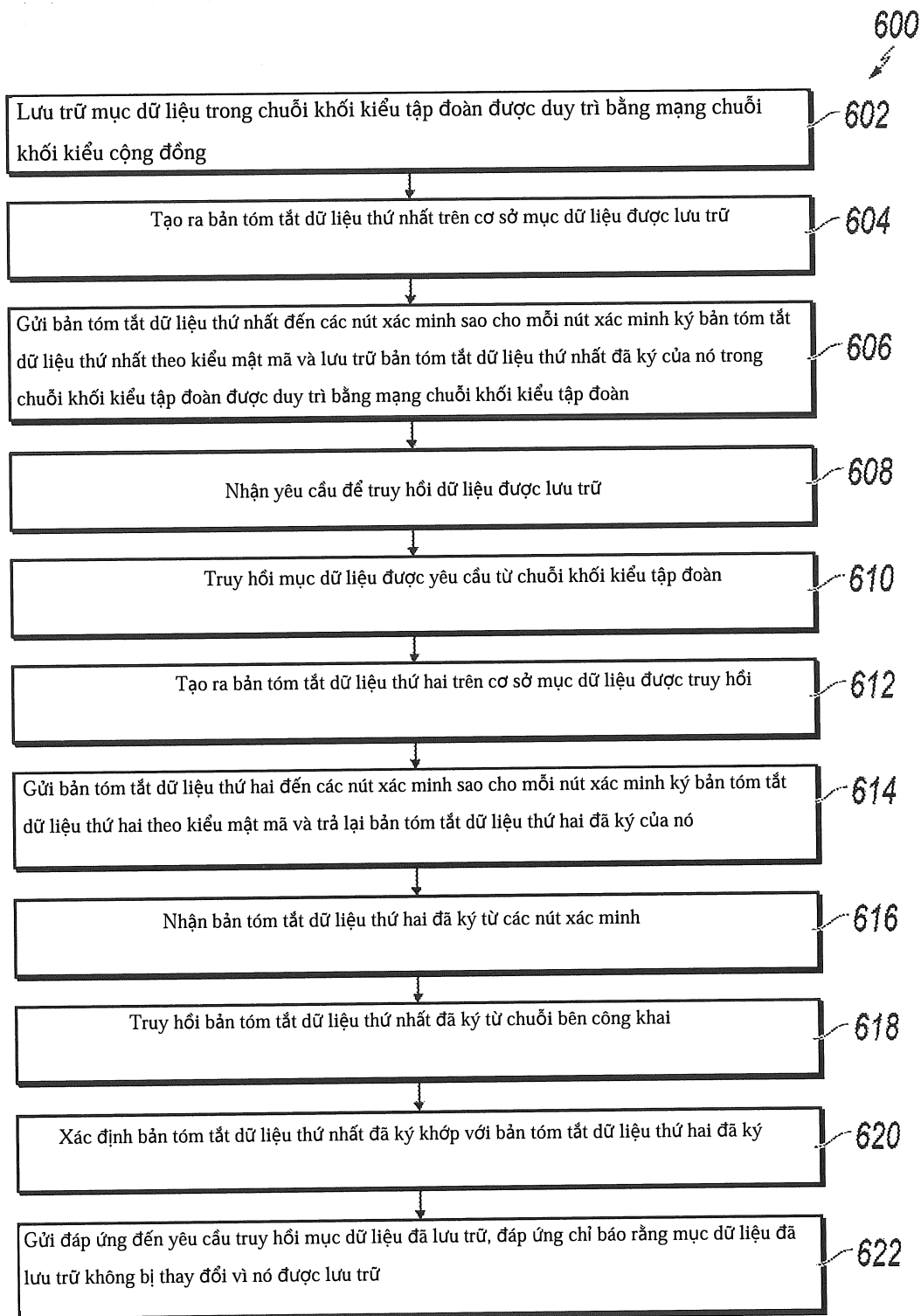


FIG. 6

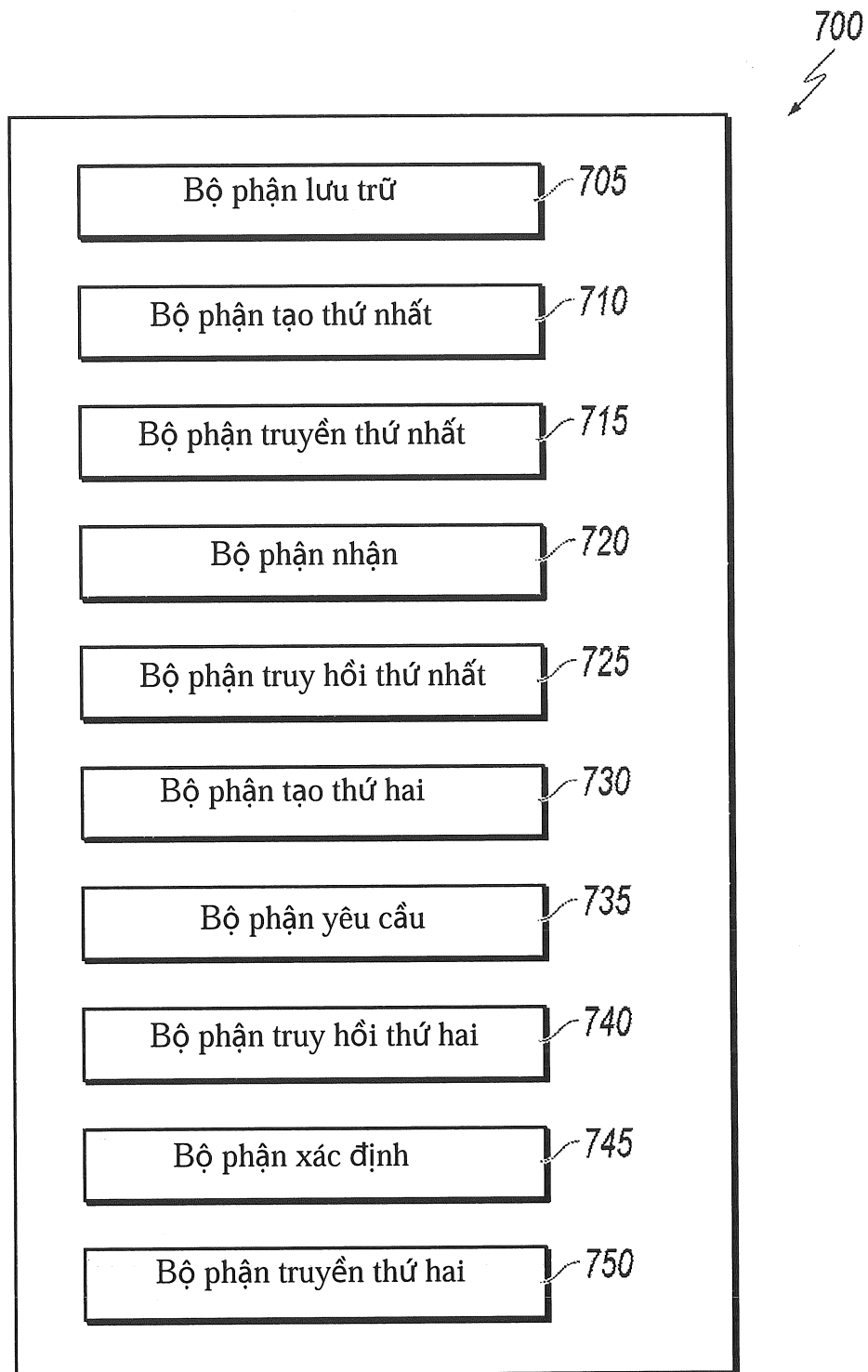


FIG. 7