



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẢNG ĐỘC QUYỀN SÁNG CHẾ

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN)
CỤC SỞ HỮU TRÍ TUỆ

(11)



1-0038662

(51)⁷ H04L 9/00

(13) B

(21) 1-2019-03237

(22) 28/02/2019

(86) PCT/CN2019/076463 28/02/2019

(87) WO2019/101224 31/05/2019

(45) 26/02/2024 431

(43) 26/08/2019 377A

(73) ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)

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

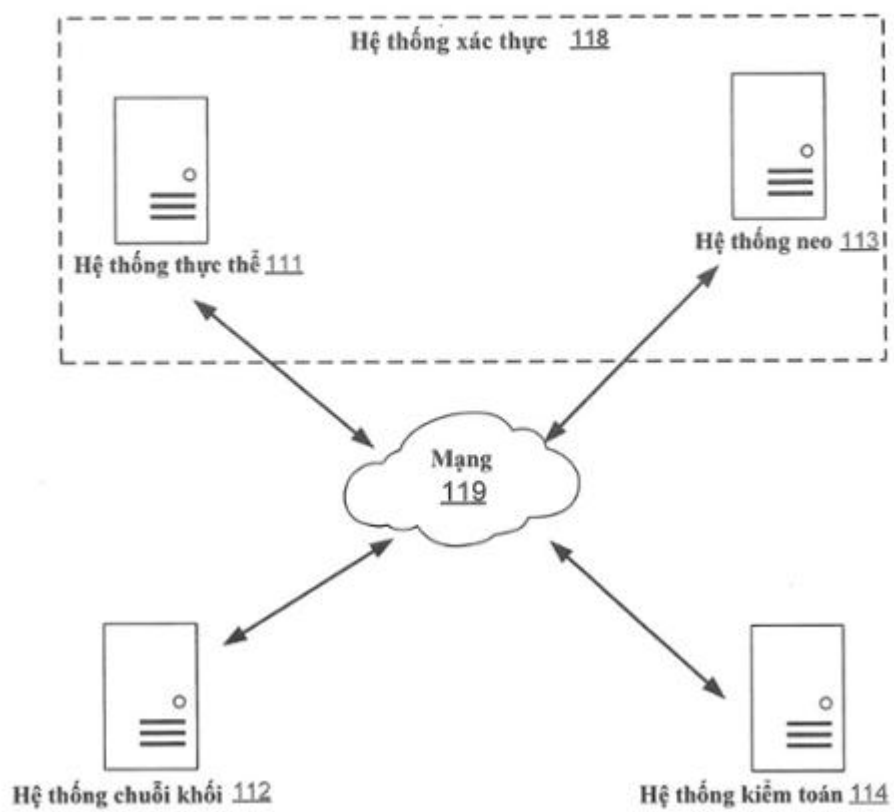
(72) CHENG, Long (CN); LI, Yanpeng (CN).

(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP, HỆ THỐNG VÀ THIẾT BỊ XÁC THỰC

(57) Sáng chế đề cập tới phương pháp, hệ thống và thiết bị chứa các chương trình máy tính được ghi mã trên vật ghi đọc được bởi máy tính, để thực hiện việc xác thực. Một trong các phương pháp chứa các bước: thu được dữ liệu kiểm toán để xác thực đối với thông tin vận hành được kết hợp với giao dịch đã được thực thi; sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán; truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối; và xác định tính xác thực của dữ liệu kiểm toán bằng cách xác minh bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành.

110 ↗



Lĩnh vực kỹ thuật được đề cập

Sáng chế này đề cập chung tới phương pháp và thiết bị cho việc xác thực dựa trên chuỗi khối.

Tình trạng kỹ thuật của sáng chế

Trong các công nghệ hiện tại, hầu hết các thực thể quản lý các tài khoản và các thao tác của riêng chúng. Dữ liệu được thu thập cho việc kiểm toán (ví dụ, bản ghi hoạt động tài khoản, thông tin người sử dụng tài khoản như nhận diện người sử dụng và mức cấp phép) thường tới từ hệ thống duy trì thực thể. Ví dụ, các thực thể tài chính thường triển khai và vận hành các hệ thống của riêng chúng, thường cấp phép điều khiển cho người sử dụng truy cập vào các hệ thống tài chính và xử lý các giao dịch. Yêu cầu làm ví dụ có thể là việc người sử dụng khởi tạo giao dịch từ phía ngân hàng không thể là cùng một người xem lại và chấp thuận giao dịch. Yêu cầu làm ví dụ khác là chỉ những người sử dụng ở các vị trí cụ thể trong thực thể mới có thể cấp phép các giao dịch trong các khung thời gian cụ thể. Tổ chức kiểm toán có thể kiểm toán các thực thể tài chính để xác nhận rằng rằng liệu các thực thể tài chính có tuân thủ các yêu cầu này hay không. Với các lý do về tính riêng tư và an ninh trong kinh doanh, các thực thể tài chính lưu trữ và quản lý dữ liệu vận hành nội bộ, hơn là tin cậy giao dữ liệu cho bên thứ ba. Với lợi ích tự thân hoặc với lý do khác, dữ liệu được thu thập cho việc kiểm toán có thể phải chịu tính không chính xác, chịu việc điều chỉnh không chân thực, hoặc thậm chí là giả mạo, vốn sẽ gây tác động xấu tới tính tin cậy của việc kiểm toán. Do đó mong muốn có hệ thống có thể làm giảm tính không chính xác, việc thao túng dữ liệu hoặc dữ liệu giả mạo.

Bản chất kỹ thuật của sáng chế

Các phương án thực hiện khác nhau của sáng chế bao gồm, nhưng không giới hạn ở, hệ thống, phương pháp và vật ghi phi chuyển tiếp đọc được bởi máy tính để nhận diện dựa trên.

Theo một khía cạnh, phương pháp xác thực được áp dụng bởi máy tính bao gồm các bước: thu được dữ liệu kiểm toán để xác thực đối với thông tin vận hành được kết

hợp với giao dịch đã được thực thi; sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán; truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối; và xác định tính xác thực của dữ liệu kiểm toán bằng cách xác minh bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành. Trước khi thu được dữ liệu kiểm toán, phương pháp có thể còn bao gồm bước: truyền bản tóm tắt dạng số của thông tin vận hành tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối.

Theo một số phương án thực hiện, bước xác định tính xác thực của dữ liệu kiểm toán bằng cách xác minh bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành bao gồm: đáp lại việc xác định rằng bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán là thống nhất với bản tóm tắt dạng số được truy hồi của thông tin vận hành, xác định rằng dữ liệu kiểm toán là xác thực; và đáp lại việc xác định rằng bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán là không thống nhất với bản tóm tắt dạng số được truy hồi của thông tin vận hành, xác định rằng dữ liệu kiểm toán là không xác thực.

Theo các phương án thực hiện khác, bước truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối bao gồm việc truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối theo nhận diện giao dịch chuỗi khối được kết hợp với bản tóm tắt dạng số của thông tin vận hành.

Theo các phương án thực hiện khác nữa, trước khi thu được dữ liệu kiểm toán, phương pháp còn bao gồm bước: đáp lại việc đăng nhập, sinh ra bản tóm tắt dạng số của thông tin nhận diện cho việc đăng nhập; truyền bản tóm tắt dạng số của thông tin nhận diện tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối; thu được nhận diện giao dịch chuỗi khối được kết hợp với bản tóm tắt dạng số của thông tin nhận diện; thực thi giao dịch; sinh ra bản tóm tắt dạng số của thông tin vận hành, trong đó thông tin vận hành chứa thông tin giao dịch của giao dịch và một hoặc nhiều thành phần trong số: bản tóm tắt dạng số của thông tin nhận diện, thông tin nhận diện, và nhận diện giao dịch chuỗi khối được kết hợp với bản tóm tắt dạng số của thông tin nhận diện; truyền bản tóm tắt dạng số của thông tin vận hành tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong

chuỗi khối; và thu được nhận diện giao dịch chuỗi khối được kết hợp với bản tóm tắt dạng số của thông tin vận hành.

Theo các phương án thực hiện khác nữa, thông tin giao dịch của giao dịch bao gồm một hoặc nhiều URL (các bộ định vị nguồn tài nguyên đồng đều - uniform resource locators) để thực thi giao dịch.

Theo một số phương án thực hiện, thông tin giao dịch của giao dịch bao gồm một hoặc nhiều thông số để gọi một hoặc nhiều URL và một hoặc nhiều kết quả được trả lại từ việc gọi một hoặc nhiều URL.

Theo các phương án thực hiện khác, thông tin nhận diện bao gồm mức cấp phép của người sử dụng cấp phép việc thực thi của giao dịch.

Theo các phương án thực hiện khác nữa, thông tin nhận diện bao gồm mức cấp phép của người sử dụng yêu cầu việc thực thi của giao dịch.

Theo các phương án thực hiện khác nữa, bước truyền bản tóm tắt dạng số của thông tin vận hành tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối bao gồm: viết bản tóm tắt dạng số của thông tin vận hành và quy trình mã hóa được sử dụng để sinh ra bản tóm tắt dạng số của thông tin vận hành thành hợp đồng chuỗi khối; và làm cho một hoặc nhiều nút khởi tạo giao dịch chuỗi khối để triển khai liên lạc chuỗi khối.

Theo một số phương án thực hiện, bước sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán bao gồm việc sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán dựa trên quy trình mã hóa được sử dụng để sinh ra bản tóm tắt dạng số của thông tin vận hành.

Theo các phương án thực hiện khác, chuỗi khối là chuỗi khối liên doanh.

Theo các phương án thực hiện khác nữa, bản tóm tắt dạng số của thông tin vận hành bao gồm trị số băm của thông tin vận hành. Việc nhận diện giao dịch chuỗi khối bao gồm giao dịch trị số băm của giao dịch chuỗi khối.

Theo một số phương án thực hiện khác, thông tin vận hành bao gồm thông tin giao dịch của giao dịch.

Theo các phương án thực hiện khác, hệ thống xác thực bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ được bởi máy tính được ghép nối tới một hoặc nhiều

bộ xử lý và có các lệnh được lưu trữ trên đó là có thể thực thi được bởi một hoặc nhiều bộ xử lý để thực hiện phương pháp theo phương án thực hiện bất kỳ trong số các phương án thực hiện nêu trên.

Theo các phương án thực hiện khác nữa, thiết bị xác thực bao gồm nhiều môđun để thực hiện phương pháp theo phương án thực hiện bất kỳ trong số các phương án thực hiện nêu trên.

Theo khía cạnh khác, sáng chế đề xuất hệ thống xác thực bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ phi chuyển tiếp đọc được bởi máy tính được ghép nối tới một hoặc nhiều bộ xử lý và được định cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý để làm cho hệ thống để thực hiện các thao tác bao gồm: thu được dữ liệu kiểm toán để xác thực đối với thông tin vận hành được kết hợp với giao dịch đã được thực thi; sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán; truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối; và xác định tính xác thực của dữ liệu kiểm toán bằng cách xác minh bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành.

Theo khía cạnh khác, sáng chế đề xuất vật ghi phi chuyển tiếp đọc được bởi máy tính được định cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý để làm cho một hoặc nhiều bộ xử lý để thực hiện các thao tác bao gồm: thu được dữ liệu kiểm toán để xác thực đối với thông tin vận hành được kết hợp với giao dịch đã được thực thi; sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán; truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối; và xác định tính xác thực của dữ liệu kiểm toán bằng cách xác minh bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành.

Theo khía cạnh khác, sáng chế đề xuất thiết bị xác thực có thể bao gồm môđun thu để thu được dữ liệu kiểm toán để xác thực đối với thông tin vận hành được kết hợp với giao dịch đã được thực thi; môđun sinh để sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán; môđun truy hồi để truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối; và môđun xác định để xác định tính xác thực của dữ liệu kiểm toán bằng cách xác minh bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành.

Các phương án thực hiện được bộc lộ trong bản mô tả này có một hoặc nhiều hiệu quả kỹ thuật sau. Theo một số phương án thực hiện, các phương pháp và hệ thống có thể tạo ra việc lưu trữ dữ liệu gốc (ví dụ, thông tin vận hành được kết hợp với giao dịch đã được thực thi) để xác thực đối với dữ liệu kiểm toán được cho là giống như dữ liệu gốc. Việc lưu trữ trong chuỗi khối cho phép giữ bản ghi chính xác của dữ liệu gốc. Theo các phương án thực hiện khác, khi giao dịch được thực thi, biểu diễn của giao dịch được đóng gói vào trong chuỗi khối và trở nên không thể thay đổi được. Theo các phương án thực hiện khác nữa, sáng chế đề xuất phương pháp và hệ thống tạo ra các khả năng để kiểm tra tính xác thực của dữ liệu kiểm toán bằng cách so sánh đối với dữ liệu gốc được lưu trữ ở chuỗi khối. Theo các phương án thực hiện khác nữa, bản tóm tắt dạng số của dữ liệu kiểm toán có thể được so sánh với bản tóm tắt dạng số của dữ liệu gốc được lưu trữ ở chuỗi khối để đảm bảo rằng dữ liệu kiểm toán không bị can thiệp. Nó ngăn chặn sự không chính xác, thiếu hụt, điều chỉnh và giả dối trong việc cung cấp dữ liệu kiểm toán. Theo một số phương án thực hiện, việc lưu trữ chuỗi khối của dữ liệu gốc như là các bản lưu trữ bản tóm tắt dạng số ghi một cách trung thực thông tin trong khi vẫn đảm bảo việc bảo vệ tính riêng tư. Theo các phương án thực hiện khác, bản tóm tắt dạng số được xác minh đồng thuận bởi nhiều nút chuỗi khối, nhưng không bộc lộ các nội dung của dữ liệu gốc. Do đó, dữ liệu gốc được giữ riêng tư. Theo các phương án thực hiện khác nữa, các phương pháp và hệ thống tạo ra các khả năng để chứa thông tin cần cho việc kiểm toán trong bản tóm tắt dạng số. Theo các phương án thực hiện khác nữa, nhận diện và mức cấp phép của người sử dụng thực hiện giao dịch gốc có thể được kết hợp với dữ liệu gốc (ví dụ, giao dịch gốc) và được chứa trong bản tóm tắt dạng số. Nó tạo thông tin đầy đủ, có thể truy hồi được cho việc xác thực dữ liệu kiểm toán đang đi tới để được kiểm toán bởi các thành phần có chức trách kiểm toán. Kết quả là, tính xác thực và chất lượng của việc kiểm toán sẽ được tăng cường.

Các dấu hiệu này cũng như các dấu hiệu khác của các hệ thống, phương pháp và vật ghi phi chuyển tiếp đọc được bởi máy tính, cũng như các phương pháp vận hành, và các chức năng của các phần tử cấu trúc liên quan và sự kết hợp của các phần, và tính kinh tế sản xuất, sẽ trở nên rõ ràng hơn khi xem xét phần mô tả sau đây và các điểm yêu cầu bảo hộ kèm theo với tham chiếu đến các hình vẽ kèm theo, tất cả tạo thành một phần của bản mô tả, trong đó các số tham chiếu giống nhau chỉ các phần tương ứng trên các

hình vẽ khác nhau. Tuy nhiên, cần hiểu rằng các hình vẽ đó chỉ nhằm mục đích minh họa và mô tả chứ không nhằm giới hạn.

Mô tả vắn tắt các hình vẽ

Fig.1 minh họa ví dụ của hệ thống xác thực dựa trên chuỗi khối, theo các phương án thực hiện khác nhau.

Fig.2 minh họa ví dụ của mạng chuỗi khối, theo các phương án thực hiện khác nhau.

Fig.3 minh họa ví dụ của phương pháp lưu trữ dữ liệu vào chuỗi khối, theo các phương án thực hiện khác nhau.

Fig.4 minh họa ví dụ của phương pháp neo và xác minh dữ liệu, theo các phương án thực hiện khác nhau.

Fig.5 minh họa lưu đồ của ví dụ của phương pháp xác thực dựa trên chuỗi khối, theo các phương án thực hiện khác nhau.

Fig.6 minh họa giản đồ khối của ví dụ của hệ thống máy tính xác thực dựa trên chuỗi khối, theo các phương án thực hiện khác nhau.

Fig.7 minh họa giản đồ khối của hệ thống máy tính làm ví dụ mà phương án thực hiện bất kỳ trong các phương án thực hiện nêu trên có thể được áp dụng vào đó.

Mô tả chi tiết sáng chế

Các phương án thực hiện được bộc lộ ở đây bao gồm, nhưng không giới hạn ở, các hệ thống, các phương pháp và vật ghi phi chuyển tiếp đọc được bởi máy tính xác thực dựa trên chuỗi khối. Theo các phương án thực hiện khác nhau, bản tóm tắt dạng số của thông tin vận hành (ví dụ, dữ liệu giao dịch tài chính) được lưu trữ vào chuỗi khối bằng cách neo. Bản tóm tắt dạng số được lưu trữ có thể được truy hồi từ chuỗi khối và được sử dụng để xác minh đối với dữ liệu được cung cấp cho việc kiểm toán. Tính xác thực và tính nguyên bản của bản tóm tắt dạng số được lưu trữ có thể được đảm bảo dựa trên việc không thể thay đổi, tính thống nhất và độ chính xác của chuỗi khối. Theo một số phương án thực hiện, các cố gắng can thiệp vào dữ liệu có thể được ngăn cản. Theo các phương án thực hiện khác, việc lưu trữ tóm tắt có thể ngăn cản việc bộc lộ quá mức của

thông tin chìa khóa như trong việc lưu trữ thông tin văn bản gốc. Theo các phương án thực hiện khác, rủi ro của việc rò rỉ thông tin có thể được làm giảm, khả năng của việc dấu thông tin được làm giảm, và/hoặc độ an toàn của dữ liệu kiểm toán được tăng cường.

Theo các phương án thực hiện khác nhau, các hệ thống xác thực, các phương pháp, và vật ghi phi chuyển tiếp đọc được bởi máy tính được bộc lộ có thể là dựa trên các loại khác nhau của các chuỗi khối phụ thuộc vào người được phép tham dự vào mạng lưới, thực thi giao thức đồng thuận, và duy trì sổ cái chuỗi khối được chia sẻ. Các loại khác nhau của chuỗi khối có thể chứa, ví dụ, chuỗi khối công cộng, chuỗi khối liên doanh, chuỗi khối riêng, v.v. Phần mô tả dưới đây đề cập tới chuỗi khối liên doanh. Mặc dù vậy, các hệ thống xác thực, các phương pháp, và vật ghi phi chuyển tiếp đọc được bởi máy tính được bộc lộ cũng có thể được áp dụng so với các loại khác của chuỗi khối.

Chuỗi khối có thể được xem như là cơ sở dữ liệu phi tập trung hoặc phi tập trung một phần, nói chung được đề cập tới như là các sổ cái phân tán do việc vận hành được thực hiện bởi các nút khác nhau (ví dụ, các thiết bị tính toán) trong mạng lưới. Thông tin bất kỳ có thể được viết vào chuỗi khối và được lưu hoặc được đọc từ đó. Các nút là, ví dụ, các thiết bị tính toán hoặc các hệ thống máy tính lớn trợ giúp mạng chuỗi khối và giữ nó chạy trơn tru. Mỗi nút có thể cung cấp một phần hoặc tất cả các chức năng của chuỗi khối. Ví dụ, nút có thể cung cấp việc xác minh đồng thuận có thể được đề cập tới như là nút tham dự đồng thuận (hoặc nút đồng thuận). Việc đồng thuận có thể là thuật toán của các quy tắc để mạng các nút chuỗi khối đạt được các kết quả xử lý được chấp nhận chung. Qua việc đồng thuận, dữ liệu được thêm vào một cách liên tục vào chuỗi các khối. Nếu thay đổi được tạo ra cho khối thì liên kết của nó tới khối trước đó trong khối sẽ trở thành bất hợp lệ và nó trở nên nhìn thấy được với tất cả các thành phần tham gia mạng, mà qua các quy tắc đồng thuận, họ có thể ngăn cản các hành động không được cấp phép bất kỳ khác nữa.

Chuỗi khối liên doanh đề cập tới chuỗi khối với các thủ tục đồng thuận được điều khiển bởi các nút được đặt trước. Chuỗi khối cũng cho phép mọi người hoặc chỉ các thành phần tham dự được chấp thuận truy cập hoặc chấp thuận phương pháp truy cập lại. Ví dụ, việc băm rễ (root hash) và giao diện chương trình ứng dụng (API - Application Program Interface) của nó có thể mở ra công cộng, các bên bên ngoài được cho phép để

sử dụng API để tạo ra số lượng cụ thể các yêu cầu và thu được thông tin liên quan tới tình trạng chuỗi khối.

Các chuỗi khối liên doanh có thể được hiểu tốt nhất khi được so sánh với phần đối phổ thông hơn của chúng, các chuỗi khối công cộng. Chuỗi khối công cộng không sở hữu hạn chế truy cập, nghĩa là một cách tuyệt đối là bất cứ ai với kết nối Internet đều có thể bên tham gia của chuỗi khối công cộng. Cụ thể hơn, bất cứ hai có khả năng đọc dữ liệu có thể được chứa trong chuỗi khối, và bất cứ ai trên thế giới đều được phép thực thi các giao dịch chuỗi khối trên chuỗi khối công cộng. Cũng vậy, không có hạn chế nào về người có thể tham gia vào quy trình đồng thuận cho các chuỗi khối, vốn là quy trình xác định cá nhân hoặc thực thể có thể thêm khối vào chuỗi khối. Các chuỗi khối công cộng được xem là được phi tập trung một cách đầy đủ, với việc điều khiển qua chuỗi khối không nằm trong tay của bất cứ cá nhân hoặc thực thể nào.

Các chuỗi khối liên doanh khác với các phần đối công cộng ở chỗ chúng được cho phép, nghĩa là, không phải bất cứ ai có kết nối Internet đều cũng có thể truy cập được vào chuỗi khối liên doanh. Các loại chuỗi khối này cũng có thể được mô tả như là bán phi tập trung. Việc điều khiển qua chuỗi khối liên doanh không được cấp phép cho thực thể đơn mà là cho nhóm các cá nhân được chấp thuận. Với chuỗi khối liên doanh, quy trình đồng thuận có xu hướng là khác với quy trình của chuỗi khối công cộng. Thay cho việc bất cứ ai cũng có khả năng tham dự vào thủ tục, các thành phần tham gia đồng thuận của chuỗi khối liên doanh thường là nhóm của các nút được chấp thuận từ trước trên mạng lưới. Các nút này có thể tương ứng với các nước, các doanh nghiệp hoặc các thực thể khác nhau. Do đó, các chuỗi khối liên doanh sở hữu các đặc điểm an ninh được thừa hưởng trong các chuỗi khối công cộng, trong khi cũng cho phép có mức độ điều khiển qua mạng lưới lớn hơn.

Fig.1 thể hiện ví dụ của hệ thống 110 để thực hiện các bước và các phương pháp được bộc lộ khác nhau, theo các phương án thực hiện khác nhau. Như được thể hiện, hệ thống 110 có thể bao gồm hệ thống thực thể 111, hệ thống chuỗi khối 112, hệ thống neo 113, và hệ thống kiểm toán 114, mỗi hệ thống trong đó có thể tương ứng với một hoặc nhiều thiết bị phần cứng vật lý hoặc thiết bị ảo được ghép nối với nhau thông qua các loại khác nhau của liên lạc được thể hiện bởi mạng 119.

Mỗi hệ thống trong số hệ thống thực thể 111, hệ thống chuỗi khối 112, hệ thống neo 113, và hệ thống kiểm toán 114 có thể được áp dụng trong một hoặc nhiều thiết bị tính toán như các máy chủ, các máy tính, các điện thoại di động, v.v. ví dụ, mỗi hệ thống trong các hệ thống có thể được áp dụng trong cụm các máy chủ. Cụm các máy chủ có thể áp dụng việc làm cân bằng tải.

Mặc dù hệ thống thực thể 111, hệ thống chuỗi khối 112, hệ thống neo 113, và hệ thống kiểm toán 114 được thể hiện như là các thành phần đơn trong hình vẽ này, nhưng cần hiểu rằng các hệ thống này có thể được áp dụng như là các thiết bị đơn hoặc nhiều thiết bị được ghép nối với nhau. Nghĩa là, hai hoặc hơn hai hệ thống trong Fig.1 có thể được tích hợp vào hệ thống đơn hoặc được áp dụng như là các hệ thống tách biệt. Ví dụ, hệ thống thực thể 111 và hệ thống neo 113 có thể được tích hợp vào trong hệ thống xác thực 118 bao gồm một hoặc nhiều thiết bị tính toán. Hệ thống xác thực 118 có thể được đề cập tới như là hệ thống xác thực dựa trên chuỗi khối. Nếu được tích hợp, hệ thống thực thể 111 và hệ thống neo 113 có thể được áp dụng như là các môđun khác nhau hoặc các thành phần tương tự của hệ thống được tích hợp.

Mỗi hệ thống trong số hệ thống thực thể 111, hệ thống chuỗi khối 112, hệ thống neo 113, và hệ thống kiểm toán 114 có thể được cài đặt với phần mềm thích hợp (ví dụ, giao diện chương trình ứng dụng xác thực) và/hoặc phần cứng (ví dụ, các kết nối có dây, không dây) để truy cập các thiết bị khác của hệ thống 110. Mỗi hệ thống trong số hệ thống thực thể 111, hệ thống chuỗi khối 112, hệ thống neo 113, và hệ thống kiểm toán 114 có thể chứa một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ được ghép nối tới một hoặc nhiều bộ xử lý. Các bộ nhớ có thể là phi chuyển tiếp và đọc được bởi máy tính và được định cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý để làm cho một hoặc nhiều bộ xử lý thực hiện các thao tác được mô tả ở đây.

Nói chung, hệ thống thực thể 111, hệ thống chuỗi khối 112, hệ thống neo 113, và hệ thống kiểm toán 114 cũng có thể có khả năng liên lạc với nhau thông qua mạng 119. Ví dụ, hệ thống thực thể 111, hệ thống chuỗi khối 112, hệ thống neo 113, và hệ thống kiểm toán 114 có thể có khả năng liên lạc với nhau thông qua một hoặc nhiều mạng được nối dây hoặc không dây (ví dụ, Internet) mà dữ liệu có thể được liên lạc qua đó. Các đặc

điểm khác nhau của các thành phần hệ thống này còn được mô tả chi tiết hơn khi tham khảo tới Fig.2 tới Fig.7.

Fig.2 thể hiện ví dụ của mạng chuỗi khối 120, theo các phương án thực hiện khác nhau. Như được thể hiện, mạng chuỗi khối 120 có thể bao gồm hệ thống chuỗi khối 112 được mô tả ở trên. Hệ thống chuỗi khối 112 có thể bao gồm nhiều nút chuỗi khối (ví dụ, nút 1, nút 2, nút 3, nút 4, nút i, v.v.). Các nút chuỗi khối có thể tạo thành mạng (ví dụ, mạng ngang hàng) với một nút chuỗi khối liên lạc với nhau. Thứ tự và số các nút chuỗi khối được thể hiện chỉ đơn thuần là các ví dụ và để tạo thuận tiện cho việc minh họa. Các nút chuỗi khối có thể được áp dụng trong các máy chủ, các máy tính, v.v. Mỗi nút chuỗi khối có thể tương ứng với một hoặc nhiều thiết bị phần cứng vật lý được ghép nối với nhau qua các loại phương pháp liên lạc khác nhau như TCP/IP. Phụ thuộc vào các phân loại, các nút chuỗi khối có thể bao gồm các nút đầy đủ, các nút Geth, các nút đồng thuận, v.v.

Theo các phương án thực hiện khác nhau, một hoặc nhiều nút của hệ thống chuỗi khối 112 có thể tương tác với các hệ thống hoặc các thiết bị khác như hệ thống thực thể 111, hệ thống neo 113, và hệ thống kiểm toán 114 được mô tả ở trên. Các tương tác có thể bao gồm việc truyền và/hoặc nhận dữ liệu cho mục đích, ví dụ, các giao dịch, chứng thư, hợp đồng, v.v. Theo một ví dụ, nút A (ví dụ, điện thoại di động, máy tính, v.v.) có thể tương ứng với thiết bị của hệ thống xác thực 118 và có thể truyền thông tin tới nút 1 (hoặc nhiều nút của hệ thống chuỗi khối 112) để lưu trữ trong chuỗi khối. Quy trình lưu trữ có thể được hoàn thành qua giao dịch chuỗi khối. Ví dụ, thông tin có thể được viết vào trong hợp đồng chuỗi khối (ví dụ, hợp đồng thông minh), và giao dịch chuỗi khối có thể được khởi tạo bởi nút 1 (hoặc một hoặc nhiều nút khác có đặc quyền này dựa trên các quy tắc đồng thuận chuỗi khối) để triển khai hợp đồng với chuỗi khối. Tương tự như các giao dịch chuỗi khối khác, giao dịch chuỗi khối ở đây có thể tương ứng với việc băm giao dịch. Việc băm nghĩa là trị số băm và có thể là đầu ra số học của dữ liệu đưa vào (ví dụ, thông tin nhận diện, thông tin giao dịch được kết hợp với giao dịch đã được thực thi) hàm băm hoặc thuật toán băm. Chuỗi khối có thể lưu trữ trị số băm của giao dịch chuỗi khối. Sau đó, khi thông tin cần được truy hồi (ví dụ, để xác minh), nút A/nút B (ví dụ, điện thoại di động, máy tính, v.v.) có thể ra lệnh cho nút 1/nút 2 (hoặc nhiều nút của hệ thống chuỗi khối 112) để khởi tạo giao dịch chuỗi khối để thu được thông tin từ chuỗi

khối. Giao dịch chuỗi khối khác có thể truy vấn địa chỉ để thu được thông tin. Nút B có thể thuộc về hệ thống xác thực 118, hệ thống kiểm toán 114, hoặc hệ thống khác (không được thể hiện) được ghép nối tới hệ thống chuỗi khối 112.

Trong tương tác với hệ thống chuỗi khối 112, nút A và nút B có thể được cài đặt phần mềm chuỗi khối thích hợp để khởi tạo, chuyển tiếp hoặc truy cập giao dịch chuỗi khối. Nút A có thể truy cập chuỗi khối qua liên lạc với nút 1 hoặc một hoặc nhiều nút khác của chuỗi khối, và nút B có thể truy cập chuỗi khối qua liên lạc với nút 2 hoặc một hoặc nhiều nút khác của chuỗi khối. Nút A có thể nộp giao dịch chuỗi khối tới chuỗi khối qua nút 1 hoặc các nút tương tự để yêu cầu thêm giao dịch chuỗi khối vào chuỗi khối.

Chuỗi khối có thể được duy trì bởi nhiều nút chuỗi khối mà mỗi nút bao gồm hoặc ghép nối tới bộ nhớ. Theo một số phương án thực hiện, bộ nhớ có thể lưu trữ cơ sở dữ liệu bể. Cơ sở dữ liệu bể có thể là truy cập được cho nhiều nút chuỗi khối theo cách phân tán. Ví dụ, cơ sở dữ liệu bể có thể được lưu trữ một cách tương ứng trong các bộ nhớ của các nút chuỗi khối. Cơ sở dữ liệu bể có thể lưu trữ nhiều giao dịch chuỗi khối được nộp bởi một hoặc nhiều thiết bị người sử dụng tương tự như nút A.

Theo một số phương án thực hiện, sau khi nhận yêu cầu giao dịch chuỗi khối của giao dịch chuỗi khối không được xác nhận, nút chuỗi khối nhận có thể thực hiện một số việc xác minh sơ bộ của giao dịch chuỗi khối. Ví dụ, đề cập tới Fig.2, nút 1 có thể thực hiện việc xác minh sơ bộ sau khi nhận giao dịch chuỗi khối từ nút A. Khi đã được xác minh, giao dịch chuỗi khối có thể được lưu trữ trong cơ sở dữ liệu bể của nút chuỗi khối nhận (ví dụ, nút 1), cũng có thể chuyển tiếp giao dịch chuỗi khối tới một hoặc nhiều nút chuỗi khối khác (ví dụ, nút 3, nút 4). Một hoặc nhiều nút chuỗi khối khác có thể lặp lại quy trình được thực hiện bởi nút nhận. Khi các giao dịch chuỗi khối trong cơ sở dữ liệu bể tương ứng đạt tới mức cụ thể (ví dụ, lượng ngưỡng), thì các nút chuỗi khối có thể xác minh mẽ của các giao dịch chuỗi khối trong cơ sở dữ liệu bể tương ứng theo các quy tắc đồng thuận hoặc các quy tắc khác. Nếu giao dịch chuỗi khối bao gồm hợp đồng chuỗi khối (ví dụ, hợp đồng thông minh), thì nút chuỗi khối có thể thực thi hợp đồng chuỗi khối tại chỗ. Hợp đồng chuỗi khối là giao thức máy tính nhằm mục đích tạo thuận tiện, xác minh, hoặc củng cố dạng số của việc thương lượng hoặc của việc thực thi của hợp

đồng. Các hợp đồng chuỗi khối cho phép vận hành các giao dịch chuỗi khối một cách đáng tin mà không có các bên thứ ba. Ví dụ của giao dịch chuỗi khối có thể ghi mã dữ liệu trong mã hợp đồng để lưu trữ dữ liệu (bằng cách triển khai hợp đồng) và truy hồi (bằng cách truy cập hoặc thực thi hợp đồng). Hợp đồng chuỗi khối có thể chứa mã hợp đồng được viết bởi người sử dụng, như trị số băm của thông tin nhận diện, chuỗi khối thông tin giao dịch được kết hợp với giao dịch chuỗi khối được thực thi, v.v. Nút chuỗi khối cụ thể xác minh một cách thành công mẽ các giao dịch chuỗi khối của nó theo các quy tắc đồng thuận có thể đóng gói các giao dịch chuỗi khối để thêm vào bản sao tại chỗ của nó của chuỗi khối và lan truyền các kết quả tới các nút chuỗi khối khác. Nút chuỗi khối cụ thể có thể là nút chuỗi khối đầu tiên hoàn thành việc xác minh thành công, thu được quyền ưu tiên xác minh, hoặc được xác định dựa trên quy tắc đồng thuận khác, v.v. Sau đó, các nút chuỗi khối khác có thể thực thi các giao dịch chuỗi khối tại chỗ, xác minh các kết quả thực thi với nhau (ví dụ, bằng cách thực hiện việc tính toán băm), và đồng bộ các bản sao của chúng của chuỗi khối với các bản sao của nút chuỗi khối cụ thể. Bằng cách cập nhật các bản sao tại chỗ của chúng của chuỗi khối, các nút chuỗi khối khác có thể viết một cách tương tự thông tin này trong giao dịch chuỗi khối vào các bộ nhớ tại chỗ tương ứng. Do đó, hợp đồng chuỗi khối sẽ được triển khai. Hợp đồng được triển khai sau đó có thể được truy cập qua địa chỉ tương ứng của nó trên chuỗi khối để thực thi. Ví dụ, dữ liệu được lưu trữ trong hợp đồng có thể được truy hồi. Nếu việc xác minh thất bại ở điểm nào đó thì giao dịch chuỗi khối sẽ bị từ chối. Tuy nhiên, các loại khác của các hệ thống chuỗi khối và các quy tắc đồng thuận được kết hợp có thể được áp dụng cho hệ thống chuỗi khối được bọc lộ.

Fig.3 minh họa ví dụ của phương pháp 300 để lưu trữ dữ liệu vào chuỗi khối, theo các phương án thực hiện khác nhau. Phương pháp 300 có thể được áp dụng bởi một hoặc nhiều thành phần (ví dụ, hệ thống thực thể 111, hệ thống chuỗi khối 112) của hệ thống 110 trên Fig.1. Như được mô tả sớm hơn, hệ thống thực thể 111 có thể là một phần của hệ thống xác thực 118 bao gồm một hoặc nhiều thiết bị tính toán. Hệ thống thực thể 111 có thể là hệ thống tài chính, như hệ thống ngân hàng. Các thao tác được biểu diễn bên dưới là nhằm mục đích minh họa. Phụ thuộc vào ứng dụng, phương pháp 300 có thể chứa các bước bổ sung, ít bước hơn, hoặc các bước thay thế được thực hiện trong các thứ tự khác hoặc được thực hiện song song.

Theo một số phương án thực hiện, tại bước 311, thực thể có thể khởi tạo yêu cầu xác minh nhận diện (ví dụ, đăng nhập) qua hệ thống thực thể 111. Thực thể có thể được kết hợp với cá nhân, tập đoàn hoặc công ty, tổ chức, v.v. ví dụ, người có thể cố gắng đăng nhập vào hệ thống thực thể 111 hoặc hệ thống tương tự được ghép nối tới hệ thống thực thể 111 (ví dụ, hệ thống ngân hàng trực tuyến được vận hành bởi ngân hàng và được áp dụng trên nút A) bằng cách nhập thông tin nhận diện cụ thể của người sử dụng đăng nhập (ví dụ, thông tin chứng thư như tài khoản và mật mã, mức cấp phép của người sử dụng đăng nhập, v.v.) để xác minh.

Tại bước 312, hệ thống thực thể 111 có thể xác minh thông tin nhận diện và thu được bản tóm tắt dạng số thứ nhất của thông tin nhận diện cho yêu cầu xác minh nhận diện. Thông tin nhận diện cho yêu cầu xác minh nhận diện có thể bao gồm thông tin bất kỳ liên quan tới, ví dụ, nhưng không giới hạn ở, một hoặc nhiều của thành phần trong các thành phần sau: thông tin lý lịch của người sử dụng đăng nhập (ví dụ, tên, giới tính, địa chỉ, nhận diện, số liên hệ, v.v.), dấu thời gian đăng nhập và vị trí đăng nhập, thiết bị đăng nhập, xem liệu việc đăng nhập là thành công hay thất bại, v.v. bản tóm tắt dạng số thứ nhất của thông tin nhận diện có thể là việc băm (ví dụ, việc băm SHA-256) của thông tin nhận diện. Hệ thống thực thể 111 có thể thực hiện quy trình băm trên thông tin nhận diện để thu được bản tóm tắt dạng số thứ nhất. Ví dụ, bản tóm tắt dạng số thứ nhất có thể bao gồm trị số băm thu được bằng cách đưa thông tin nhận diện vào thuật toán băm. Hệ thống thực thể 111 có thể truyền bản tóm tắt dạng số thứ nhất tới hệ thống chuỗi khối 112 để lưu trữ trong chuỗi khối được duy trì bởi hệ thống chuỗi khối 112. Nhờ giao dịch chuỗi khối thứ nhất, bản tóm tắt dạng số thứ nhất được lưu trữ vào hệ thống chuỗi khối 112. Chuỗi khối có thể lưu trữ bản tóm tắt dạng số thứ nhất (ví dụ, trị số băm của thông tin nhận diện), nhưng không lưu trữ các chi tiết (ví dụ, văn bản gốc) của thông tin nhận diện để đảm bảo tính riêng tư, do dữ liệu được lưu trữ trong chuỗi khối là nhìn thấy được với các nút chuỗi khối khác.

Theo một số phương án thực hiện, hệ thống thực thể 111 có thể chứa một hoặc nhiều nút hạng nhẹ (ví dụ, nút A, nút B). Hệ thống thực thể 111 có thể khởi tạo giao dịch chuỗi khối đầu tiên qua nút của hệ thống chuỗi khối 112 (ví dụ nút 1) được ghép nối tới nút (các nút) hạng nhẹ. Ví dụ, bản tóm tắt dạng số thứ nhất có thể được viết vào trong hợp đồng chuỗi khối (ví dụ, hợp đồng thông minh), và giao dịch chuỗi khối thứ nhất có

thể được khởi tạo để triển khai hợp đồng cho chuỗi khối. Bằng cách triển khai này, hợp đồng là có thể truy cập được từ chuỗi khối để thực thi hoặc cho các thao tác khác. Giao dịch chuỗi khối thứ nhất trong trường hợp này tương ứng với nhận diện giao dịch chuỗi khối thứ nhất (ví dụ, việc băm giao dịch thứ nhất). Ví dụ, nhận diện giao dịch chuỗi khối thứ nhất có thể là trị số băm của giao dịch chuỗi khối thứ nhất. Hệ thống chuỗi khối 112 cũng có thể lưu trữ nhận diện giao dịch chuỗi khối thứ nhất. Do đó, nhận diện giao dịch chuỗi khối thứ nhất và bản tóm tắt dạng số thứ nhất được neo. Quan hệ neo có thể được lưu trữ trong hệ thống neo 113. Bằng cách truy vấn nhận diện giao dịch chuỗi khối thứ nhất, bản tóm tắt dạng số được lưu trữ ở chuỗi khối thứ nhất có thể được truy hồi. Ví dụ, khi nhận diện giao dịch chuỗi khối thứ nhất được gửi tới hệ thống chuỗi khối 112, hệ thống chuỗi khối 112 có thể thực thi hợp đồng chuỗi khối để truy hồi bản tóm tắt dạng số thứ nhất. Có nhiều cách thực hợp khác nhau để lưu trữ và truy hồi bản tóm tắt dạng số trên hệ thống chuỗi khối 112. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ hiểu rằng các phương án thực hiện của sáng chế này không bị hạn chế vào các ví dụ nêu trên.

Tại bước 313, nếu các bước nêu trên được thực thi một cách thành công thì hệ thống chuỗi khối 112 có thể trả lại kết quả chỉ thị rằng bản tóm tắt dạng số thứ nhất được lưu trữ một cách thành công vào chuỗi khối. Ví dụ, hệ thống thực thể 111 có thể thu được thông báo rằng việc đăng nhập là thành công. Hệ thống chuỗi khối 112 cũng có thể trả lại nhận diện giao dịch chuỗi khối thứ nhất được kết hợp với việc lưu trữ bản tóm tắt dạng số thứ nhất của thông tin nhận diện vào chuỗi khối.

Tại bước 321, thực thể có thể khởi tạo yêu cầu giao dịch (ví dụ, giao dịch tài chính hoặc hành động khác) qua hệ thống thực thể 111.

Tại bước 322, đáp lại việc đăng nhập thành công, hệ thống thực thể 111 có thể thực thi giao dịch theo yêu cầu giao dịch để thu được kết quả giao dịch. Ở đây, giao dịch có thể là loại bất kỳ của các hoạt động, như chuyển quỹ, rút quỹ, thay đổi thông tin tài khoản, yêu cầu thông tin, yêu cầu quỹ, chấp thuận hoặc từ chối giao dịch, v.v. giao dịch không bị hạn chế vào các ví dụ được mô tả ở đây. Trong bản mô tả này, thông tin giao dịch được sử dụng để đề cập tới thông tin liên quan tới giao dịch. Ví dụ, thông tin giao dịch có thể chứa một hoặc nhiều thành phần trong các thành phần sau, yêu cầu giao dịch,

kết quả giao dịch, thông tin người sử dụng tài khoản như nhận diện người sử dụng và mức cấp phép, các URL (các bộ định vị nguồn tài nguyên đồng đều - uniform resource locator) mà người sử dụng hoặc hệ thống thực thể 111 đã truy cập trong khi thực hiện giao dịch, các biến hoặc các hệ số liên quan để thực hiện giao dịch, cân đối tài khoản trước khi và/hoặc sau khi giao dịch, bản ghi hoạt động tài khoản, v.v. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ hiểu rằng thông tin giao dịch không bị hạn chế vào các ví dụ nêu trên.

Trong các ví dụ sau đây, thuật ngữ thông tin vận hành được sử dụng. Theo một số phương án thực hiện, thông tin vận hành có thể chứa thông tin giao dịch. Theo một số phương án thực hiện khác, thông tin vận hành có thể chứa thông tin giao dịch cộng với thông tin được kết hợp với các bước đăng nhập 311 và 313. Theo một số phương án thực hiện, thông tin được kết hợp với các bước đăng nhập 311 và 313 có thể chứa một hoặc nhiều thành phần trong số: bản tóm tắt dạng số thứ nhất, thông tin nhận diện của thực thể (người sử dụng), hoặc nhận diện giao dịch chuỗi khối thứ nhất. Ví dụ, trong một tình huống, thông tin vận hành chứa thông tin giao dịch cộng với bản tóm tắt dạng số thứ nhất. Phần chứa trong thông tin vận hành có thể là lựa chọn thiết kế của người áp dụng các phương án thực hiện được bộc lộ.

Hệ thống thực thể 111 có thể còn thu được (ví dụ, sinh ra) bản tóm tắt dạng số thứ hai của thông tin vận hành. Bản tóm tắt dạng số thứ hai của thông tin vận hành có thể là việc băm (ví dụ, việc băm SHA-256) của thông tin vận hành. Hệ thống thực thể 111 có thể thực hiện quy trình băm trên thông tin vận hành để thu được bản tóm tắt dạng số thứ hai. Ví dụ, bản tóm tắt dạng số thứ hai có thể bao gồm trị số băm thu được bằng cách đưa thông tin vận hành vào thuật toán băm. Hệ thống thực thể 111 có thể truyền bản tóm tắt dạng số thứ hai tới hệ thống chuỗi khối 112 để lưu trữ trong chuỗi khối được duy trì bởi hệ thống chuỗi khối 112.

Theo các phương án thực hiện khác nhau, hệ thống thực thể 111 có thể khởi tạo giao dịch chuỗi khối thứ hai để lưu trữ bản tóm tắt dạng số thứ hai trong chuỗi khối qua nút của hệ thống chuỗi khối 112. Ví dụ, bản tóm tắt dạng số thứ hai có thể được viết vào hợp đồng chuỗi khối (ví dụ, hợp đồng thông minh), và giao dịch chuỗi khối thứ hai có thể được khởi tạo bởi nút hoặc nút khác để triển khai hợp đồng cho chuỗi khối. Giao

dịch chuỗi khối thứ hai trong trường hợp này tương ứng với nhận diện giao dịch chuỗi khối thứ hai (ví dụ, việc băm giao dịch thứ hai), vốn cũng được kết hợp với bản tóm tắt dạng số thứ hai. Chuỗi khối có thể lưu trữ bản tóm tắt dạng số thứ hai (ví dụ, trị số băm của thông tin vận hành), nhưng không lưu trữ các chi tiết (ví dụ, văn bản gốc) của thông tin giao dịch để đảm bảo tính riêng tư, do dữ liệu được lưu trữ trong chuỗi khối là nhìn thấy được với các nút chuỗi khối khác. Chuỗi khối cũng có thể lưu trữ nhận diện giao dịch chuỗi khối thứ hai. Do đó, nhận diện giao dịch chuỗi khối thứ hai và bản tóm tắt dạng số thứ hai được neo. Quan hệ neo có thể được lưu trữ trong hệ thống neo 113. Bằng cách chất vấn nhận diện giao dịch chuỗi khối thứ hai, bản tóm tắt dạng số thứ hai được lưu trữ ở chuỗi khối có thể được truy hồi. Các phương pháp thay thế khác cho hợp đồng thông minh có thể được áp dụng để đạt được việc lưu trữ của bản tóm tắt dạng số thứ hai của thông tin vận hành trong chuỗi khối.

Tại bước 323, nếu các bước nêu trên được thực thi một cách thành công thì hệ thống chuỗi khối 112 có thể trả lại kết quả cho hệ thống thực thể 111 chỉ thị rằng bản tóm tắt dạng số thứ hai được lưu trữ một cách thành công vào chuỗi khối. Hệ thống chuỗi khối 112 cũng có thể trả lại nhận diện giao dịch chuỗi khối thứ hai được kết hợp với việc lưu trữ bản tóm tắt dạng số thứ hai của thông tin vận hành vào chuỗi khối. Nhận diện giao dịch chuỗi khối thứ hai hoặc các nhận diện giao dịch tương tự có thể được lưu trữ trong hệ thống thực thể 111 và/hoặc hệ thống khác (ví dụ, hệ thống neo 113). Do đó, hệ thống thực thể 111 có thể thu được nhận diện giao dịch được kết hợp với việc lưu trữ bản tóm tắt dạng số của thông tin vận hành vào chuỗi khối.

Theo cách khác, bước 311 có thể được kết hợp với bước 321. Nghĩa là, việc xác minh nhận diện và giao dịch có thể được yêu cầu đồng thời. Một cách tương ứng, các bước 312 có thể được kết hợp với bước 322, và bước 313 có thể được kết hợp với bước 323.

Fig.4 minh họa ví dụ của phương pháp 400 để neo và xác minh dữ liệu, theo các phương án thực hiện khác nhau. Phương pháp 400 có thể được áp dụng bởi một hoặc nhiều thành phần (ví dụ, hệ thống thực thể 111, hệ thống chuỗi khối 112, hệ thống neo 113, hệ thống kiểm toán 114) của hệ thống 110 của Fig.1. Như được mô tả sớm hơn, mặc dù được thể hiện như các hệ thống tách biệt, nhưng hệ thống thực thể 111 và hệ

thống neo 113 có thể được tích hợp thành hệ thống xác thực 118 bao gồm một hoặc nhiều thiết bị tính toán. Các thao tác được biểu diễn bên dưới là nhằm mục đích minh họa. Phụ thuộc vào ứng dụng, phương pháp 400 có thể chứa các bước bổ sung, ít bước hơn, hoặc các bước thay thế được thực hiện trong các thứ tự khác hoặc được thực hiện song song.

Theo một số phương án thực hiện, tại bước 411, hệ thống kiểm toán 114 có thể khởi tạo yêu cầu kiểm toán với hệ thống thực thể 111. Ví dụ, hệ thống của bộ phận có thẩm quyền kiểm toán có thể khởi tạo liên lạc với hệ thống thực thể 111 để yêu cầu thực thể cung cấp dữ liệu để kiểm toán. Bản mô tả này nói chung đề cập tới dữ liệu được cung cấp bởi hệ thống thực thể 111 để kiểm toán như là dữ liệu kiểm toán. Dữ liệu kiểm toán được yêu cầu có thể là một hoặc nhiều bộ hoàn chỉnh của thông tin vận hành cho một hoặc nhiều giao dịch, hoặc có thể là một phần của thông tin vận hành, ví dụ, bản ghi hoạt động tài khoản, thông tin người sử dụng tài khoản như nhận diện người sử dụng và mức cấp phép, v.v. Dữ liệu kiểm toán được cho là giống như thông tin vận hành nếu dữ liệu kiểm toán được cung cấp bởi hệ thống thực thể 111 là chân thực.

Tại bước 412, hệ thống thực thể 111 có thể truyền dữ liệu kiểm toán được yêu cầu tới hệ thống kiểm toán 114. Hệ thống kiểm toán 114 do đó có thể thu được dữ liệu kiểm toán để xác thực đối với thông tin vận hành. Ví dụ, dữ liệu kiểm toán có thể bao gồm bản ghi của một hoặc nhiều giao dịch, vốn được cho là tương ứng với một hoặc nhiều giao dịch được thực thi. Các bước sau có thể được thực hiện để xác thực nếu dữ liệu kiểm toán tương ứng một cách trung thực với các giao dịch lịch sử. Do đó, việc thao tác trên dữ liệu kiểm toán có thể được ngăn cản.

Tại bước 421, hệ thống kiểm toán 114 có thể khởi tạo việc xác minh của dữ liệu kiểm toán qua hệ thống neo 113. Hệ thống kiểm toán 114 có thể chuyển tiếp dữ liệu kiểm toán tới hệ thống neo 113. Trong bản mô tả này, neo hoặc việc neo có thể có nghĩa là việc kết hợp hoặc theo cách khác là thiết lập việc kết hợp. Hệ thống neo 113 lưu trữ các quan hệ kết hợp. Ví dụ, hệ thống neo 113 lưu trữ quan hệ kết hợp của các nhận diện giao dịch chuỗi khối và các bản tóm tắt dạng số. Hệ thống neo 113 có thể thu được các quan hệ kết hợp từ hệ thống thực thể 111.

Tại bước 422, khi phản hồi, hệ thống neo 113 có thể thu được nhận diện giao dịch chuỗi khối dựa trên dữ liệu kiểm toán. Ví dụ, dữ liệu kiểm toán có thể chứa nhận diện

của giao dịch đã được thực thi cần được kiểm toán. Giao dịch đã được thực thi có thể được kết hợp với nhận diện giao dịch chuỗi khối. Giao dịch chuỗi khối có thể là các giao dịch chuỗi khối được mô tả cùng với Fig.3 nêu trên. Như được mô tả ở trên, hệ thống neo 113 có thể có các nhận diện giao dịch chuỗi khối được lưu trữ tương ứng với các giao dịch chuỗi khối lưu trữ các bản tóm tắt dạng số tương ứng cho các giao dịch đã được thực thi vào chuỗi khối. Hệ thống neo 113 có thể thu được nhận diện giao dịch chuỗi khối một cách trực tiếp từ hệ thống kiểm toán 114 hoặc từ hệ thống thực thể 111. Nhận diện giao dịch chuỗi khối này được thu trong bước 422 có thể được đề cập tới như là nhận diện giao dịch chuỗi khối thứ ba (ví dụ, băm của giao dịch thứ ba). Tương tự như các nhận diện giao dịch chuỗi khối được mô tả ở trên cùng với Fig.3, nhận diện giao dịch chuỗi khối thứ ba được kết hợp với bản tóm tắt dạng số trên hệ thống chuỗi khối 112. Bản tóm tắt dạng số là bản tóm tắt dạng số của thông tin vận hành cần được kiểm toán được lưu trữ từ trước trong hệ thống chuỗi khối 112. Nhận diện giao dịch chuỗi khối thứ ba có thể được sử dụng để nhận diện và thu được bản tóm tắt dạng số từ hệ thống chuỗi khối 112. Trong bước này, hệ thống neo 113 có thể gửi nhận diện giao dịch chuỗi khối thứ ba tới hệ thống chuỗi khối 112 để nhận diện và thu được bản tóm tắt dạng số tương ứng.

Hệ thống neo 113 cũng có thể sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán. Bản tóm tắt dạng số này có thể được đề cập tới như là bản tóm tắt dạng số thứ ba.

Tại bước 423, hệ thống chuỗi khối 112 có thể truyền bản sao được lưu trữ ở chuỗi khối của bản tóm tắt dạng số được kết hợp với nhận diện giao dịch chuỗi khối thứ ba tới hệ thống neo 113.

Tại bước 424, hệ thống neo 113 có thể xác minh nếu bản sao được lưu trữ ở chuỗi khối của bản tóm tắt dạng số được kết hợp với nhận diện giao dịch chuỗi khối thứ ba là thống nhất với bản tóm tắt dạng số thứ ba được sinh ra.

Tại bước 431, hệ thống neo 113 có thể trả lại kết quả xác minh tới hệ thống kiểm toán 114. Nếu bản sao được lưu trữ ở chuỗi khối của bản tóm tắt dạng số được kết hợp với nhận diện giao dịch chuỗi khối thứ ba là thống nhất với bản tóm tắt dạng số thứ ba được sinh ra, thì kết quả xác minh có thể chỉ thị rằng dữ liệu kiểm toán là xác thực. Trái lại, kết quả xác minh có thể chỉ thị rằng dữ liệu kiểm toán là không xác thực.

Như được thảo luận ở trên, theo một số phương án thực hiện, hệ thống neo 113 có thể được tích hợp với hệ thống kiểm toán 114. Theo một số phương án thực hiện khác, một số hoặc tất cả các bước có thể được thực hiện bởi hệ thống kiểm toán 114, thay cho hệ thống neo 113. Ví dụ, hệ thống kiểm toán 114 có thể thu được nhận diện giao dịch chuỗi khối thứ ba từ hệ thống thực thể 111 hoặc hệ thống neo 113. Theo cách khác, hệ thống kiểm toán 114 có thể thu được nhận diện giao dịch chuỗi khối thứ ba từ cơ sở dữ liệu của riêng nó, vốn có thể lưu trữ quan hệ tương ứng giữa các giao dịch được thực thi và các nhận diện giao dịch chuỗi khối. Hệ thống kiểm toán 114 có thể truy hồi bản tóm tắt dạng số của thông tin vận hành được kết hợp với giao dịch đã được thực thi dựa trên nhận diện giao dịch chuỗi khối. Hệ thống kiểm toán 114 cũng có thể sinh ra bản tóm tắt dạng số thứ ba của dữ liệu kiểm toán. Sau đó, hệ thống kiểm toán 114 có thể so sánh bản tóm tắt dạng số thứ ba đối với bản tóm tắt dạng số được truy hồi từ chuỗi khối để xác minh dữ liệu kiểm toán.

Fig.5 minh họa lưu đồ của ví dụ của phương pháp 510 để áp dụng việc xác thực dựa trên chuỗi khối, theo các phương án thực hiện khác nhau. Phương pháp 510 có thể được áp dụng bởi một hoặc nhiều thành phần (ví dụ, hệ thống xác thực 118) của hệ thống 110 của Fig.1. Ví dụ, các bước 514 đến 517 có thể được thực hiện bởi hệ thống neo 113 của hệ thống xác thực 118. Ví dụ, các bước 501 đến 504 và 511 đến 513 có thể được thực hiện bởi việc kết hợp của hệ thống thực thể 111 và hệ thống neo 113 của hệ thống xác thực 118. Phương pháp 510 có thể được áp dụng bởi hệ thống bao gồm máy phần cứng và/hoặc phần mềm khác nhau. Ví dụ, hệ thống xác thực 118 có thể được áp dụng bởi một hoặc nhiều hệ thống hoặc thiết bị (ví dụ, các máy tính, máy chủ). Hệ thống áp dụng phương pháp 510 có thể bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều vật ghi phi chuyển tiếp đọc được bởi máy tính (ví dụ, một hoặc nhiều bộ nhớ) được ghép nối tới một hoặc nhiều bộ xử lý và được định cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý để làm cho hệ thống (ví dụ, bộ xử lý) để thực hiện phương pháp 510. Các thao tác được biểu diễn bên dưới là nhằm mục đích minh họa. Phụ thuộc vào ứng dụng, phương pháp 510 có thể chứa các bước bổ sung, ít bước hơn, hoặc các bước thay thế được thực hiện trong các thứ tự khác hoặc được thực hiện song song. Ví dụ của việc áp dụng của phương pháp 510 được mô tả ở trên với tham khảo tới Fig.3 tới Fig.4.

Theo một số phương án thực hiện, một số bước tùy chọn có thể được thực thi trước bước 514. Bước tùy chọn 501 chứa: đáp lại việc đăng nhập từ người sử dụng, sinh ra bản tóm tắt dạng số (ví dụ, bản tóm tắt dạng số thứ nhất) của thông tin nhận diện cho việc đăng nhập. Bước tùy chọn 502 chứa: truyền bản tóm tắt dạng số (ví dụ, bản tóm tắt dạng số thứ nhất) của thông tin nhận diện tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối. Bước tùy chọn 503 chứa: thu được nhận diện giao dịch chuỗi khối (ví dụ, nhận diện giao dịch chuỗi khối thứ nhất) được kết hợp với bản tóm tắt dạng số thứ nhất của thông tin nhận diện.

Bước tùy chọn 504 chứa: thực thi giao dịch (ví dụ, giao dịch tài chính) khi được yêu cầu bởi người sử dụng. Bước tùy chọn 511 chứa việc sinh ra bản tóm tắt dạng số (ví dụ, bản tóm tắt dạng số thứ hai) của thông tin vận hành được kết hợp với giao dịch đã được thực thi. Theo một số phương án thực hiện, bản tóm tắt dạng số thứ hai của thông tin vận hành bao gồm trị số băm của thông tin vận hành. Việc băm hoặc trị số băm của dữ liệu cụ thể có thể có ý nghĩa là trị số băm (ví dụ, kết quả số học của việc đưa dữ liệu vào thuật toán băm). Ví dụ, sinh ra bản tóm tắt dạng số của dữ liệu cụ thể (ví dụ, thông tin vận hành) có thể chứa việc đưa dữ liệu vào thuật toán băm để thu được kết quả số học. Các nội dung của thông tin vận hành có thể được định cấu hình theo yêu cầu kiểm toán. Thông tin vận hành có thể chứa thông tin giao dịch của giao dịch và một hoặc nhiều thành phần trong số: bản tóm tắt dạng số của thông tin nhận diện, thông tin nhận diện, và nhận diện giao dịch chuỗi khối được kết hợp với bản tóm tắt dạng số của thông tin nhận diện (ví dụ, nhận diện giao dịch chuỗi khối thứ nhất).

Theo một số phương án thực hiện, thông tin giao dịch của giao dịch có thể bao gồm một hoặc nhiều URL để thực thi giao dịch. Thông tin giao dịch của giao dịch có thể bao gồm một hoặc nhiều thông số (ví dụ, ID tài khoản) để gọi một hoặc nhiều URL và một hoặc nhiều kết quả được trả lại (ví dụ, các cân đối tài khoản cuối cùng) từ việc gọi một hoặc nhiều URL. Ví dụ, thông tin vận hành có thể chứa thông tin giao dịch được kết hợp với giao dịch đã được thực thi và bản tóm tắt dạng số thứ nhất. Trong ví dụ cụ thể, thông tin giao dịch trong thông tin vận hành có thể chứa yêu cầu để thực thi giao dịch, chứa URL được gọi để thực hiện giao dịch. Theo ví dụ khác, thông tin vận hành cũng có thể chứa thông tin nhận diện của người sử dụng yêu cầu hoặc cấp phép giao dịch. Với ví dụ khác, thông tin vận hành cũng có thể chứa kết quả của việc thực thi thao tác (ví dụ, truyền

các lượng hoặc các số cân đối). Theo một số phương án thực hiện, thông tin nhận diện bao gồm mức cấp phép của người sử dụng yêu cầu hoặc cấp phép việc thực thi của giao dịch, vốn có thể được sử dụng để xác minh xem nếu người sử dụng có đủ mức cấp phép để thực hiện hoặc chấp thuận giao dịch hay không.

Bước tùy chọn 512 chứa việc truyền bản tóm tắt dạng số (ví dụ, bản tóm tắt dạng số thứ hai) của thông tin vận hành tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối. Theo một số phương án thực hiện khác, bước truyền bản tóm tắt dạng số của thông tin vận hành tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối bao gồm: viết bản tóm tắt dạng số thứ hai của thông tin vận hành và quy trình mã hóa (ví dụ, việc băm SHA-256) được sử dụng để sinh ra bản tóm tắt dạng số của thông tin vận hành thành hợp đồng chuỗi khối; và làm cho một hoặc nhiều nút khởi tạo giao dịch chuỗi khối để triển khai liên lạc chuỗi khối. Các chi tiết sẽ còn được đề cập tới bước 322 được mô tả ở trên.

Bước tùy chọn 513 chứa việc thu được nhận diện giao dịch chuỗi khối (ví dụ, nhận diện giao dịch chuỗi khối thứ hai) được kết hợp với bản tóm tắt dạng số thứ hai của thông tin vận hành. Theo một số phương án thực hiện, nhận diện giao dịch bao gồm giao dịch trị số băm của giao dịch chuỗi khối triển khai liên lạc chuỗi khối. Các ví dụ của việc băm giao dịch có thể được đề cập tới việc nhận diện giao dịch chuỗi khối thứ nhất và nhận diện giao dịch chuỗi khối thứ hai được mô tả ở trên.

Bước 514 chứa việc thu được dữ liệu kiểm toán để xác thực đối với thông tin vận hành được kết hợp với giao dịch đã được thực thi (ví dụ, thông tin vận hành được kết hợp với giao dịch đã được thực thi trong các bước từ 504 đến 513). Ở đây, phần mô tả đề cập tới “giao dịch đã được thực thi”. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ hiểu rằng trong bản mô tả này, có thể chứa nhiều giao dịch được thực thi hoặc một phần của giao dịch đã được thực thi. Dữ liệu kiểm toán có thể được cung cấp bởi thực thể hoặc được thu từ chỗ khác để kiểm toán. Dữ liệu kiểm toán có thể bao gồm loại bất kỳ của dữ liệu bản ghi cần được kiểm toán hoặc được xác minh theo cách khác. Nhờ các bước sau, tính xác thực của dữ liệu kiểm toán có thể được xác minh dựa trên sự thống nhất với thông tin vận hành. Các chi tiết khác có thể được đề cập tới trong các bước 411, 412, và 421 được mô tả ở trên.

Bước 515 chứa việc sinh ra bản tóm tắt dạng số (ví dụ, bản tóm tắt dạng số thứ ba) của dữ liệu kiểm toán. Theo một số phương án thực hiện, bước sinh ra bản tóm tắt dạng số thứ ba của dữ liệu kiểm toán bao gồm việc sinh ra bản tóm tắt dạng số thứ ba của dữ liệu kiểm toán dựa trên quy trình mã hóa (ví dụ, việc băm SHA-256) được sử dụng để sinh ra bản tóm tắt dạng số thứ hai của thông tin vận hành.

Bước 516 chứa việc truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối. Ở đây, bản tóm tắt dạng số được cho là tương ứng với dữ liệu kiểm toán từ chuỗi khối có thể được truy hồi. Theo một số phương án thực hiện, bước truy hồi bản tóm tắt dạng số từ chuỗi khối bao gồm việc truy hồi bản tóm tắt dạng số theo nhận diện giao dịch chuỗi khối được kết hợp với giao dịch cần được kiểm toán. Theo một số phương án thực hiện, hệ thống kiểm toán có thể thu được nhận diện giao dịch chuỗi khối dựa trên thông tin trên giao dịch cần được kiểm toán trong dữ liệu kiểm toán. trong các tình huống mà trong đó dữ liệu kiểm toán là xác thực, việc nhận diện giao dịch chuỗi khối nên là giống như nhận diện giao dịch chuỗi khối thứ hai được kết hợp với bản tóm tắt dạng số thứ hai trong bước 513. Các chi tiết khác có thể được đề cập tới trong các bước 422, và 423 được mô tả ở trên.

Bước 517 chứa việc xác định tính xác thực của dữ liệu kiểm toán bằng cách xác minh bản tóm tắt dạng số được sinh ra (ví dụ, bản tóm tắt dạng số thứ ba) của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành. Các chi tiết sẽ còn được đề cập tới bước 424 được mô tả ở trên. Theo một số phương án thực hiện, bước 517 bao gồm việc đáp lại việc xác định rằng bản tóm tắt dạng số thứ ba được sinh ra của dữ liệu kiểm toán là thống nhất với bản tóm tắt dạng số được truy hồi, xác định rằng dữ liệu kiểm toán là xác thực; và đáp lại việc xác định rằng bản tóm tắt dạng số thứ ba được sinh ra của dữ liệu kiểm toán là không thống nhất với bản tóm tắt dạng số được truy hồi, xác định rằng dữ liệu kiểm toán là không xác thực.

Fig.6 minh họa giản đồ khối của ví dụ của hệ thống máy tính 610 để áp dụng việc xác thực dựa trên chuỗi khối, theo các phương án thực hiện khác nhau. Hệ thống 610 có thể là ví dụ của việc áp dụng của một hoặc nhiều thành phần (ví dụ, hệ thống xác thực 118) của hệ thống 110 trên Fig.1. Phương pháp 510 có thể được áp dụng bởi hệ thống máy tính 610. Hệ thống máy tính 610 có thể bao gồm một hoặc nhiều bộ xử lý và một

hoặc nhiều vật ghi phi chuyển tiếp đọc được bởi máy tính (ví dụ, một hoặc nhiều bộ nhớ) được ghép nối tới một hoặc nhiều bộ xử lý và được định cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý để làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) để thực hiện phương pháp 510. Hệ thống máy tính 610 có thể bao gồm các bộ phận/môđun khác nhau tương ứng với các lệnh (ví dụ, các lệnh phần mềm). Theo một số phương án thực hiện, hệ thống máy tính 610 có thể được đề cập tới như là thiết bị xác thực. Thiết bị xác thực có thể bao gồm môđun thu 611 để thu được dữ liệu kiểm toán để xác thực đối với thông tin vận hành được kết hợp với giao dịch đã được thực thi; môđun sinh 612 để sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán; môđun truy hồi 613 để truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối; và môđun xác định 614 để xác định tính xác thực của dữ liệu kiểm toán bằng cách xác minh bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành.

Như được thể hiện, bằng cách sinh ra bản tóm tắt dạng số của thông tin vận hành được kết hợp với giao dịch đã được thực thi và lưu trữ bản tóm tắt dạng số vào chuỗi khối, biểu diễn của thông tin vận hành có thể được duy trì một cách an toàn và là truy cập được cho việc xác minh. Bản tóm tắt dạng số được lưu trữ vào dữ liệu các bản ghi chuỗi khối để kiểm toán trong tương lai. Việc can thiệp vào dữ liệu được lưu trữ có thể bị ngăn cản dựa trên các quy tắc đồng thuận chuỗi khối bao gồm việc băm. Biểu diễn bản tóm tắt dạng số của thông tin vận hành cũng có thể giấu thông tin văn bản gốc để bảo vệ tính riêng tư. Qua việc truy vấn nhận diện giao dịch chuỗi khối, bản tóm tắt dạng số được lưu trữ ở chuỗi khối có thể được truy hồi từ chuỗi khối cho việc xác minh. Do đó, tính nguyên bản và tính xác thực của dữ liệu kiểm toán có thể được đảm bảo, vốn làm giảm cơ hội cho việc kiểm toán gian lận.

Các kỹ thuật được mô tả ở đây được áp dụng bởi một hoặc nhiều thiết bị tính toán mục đích đặc biệt. Các thiết bị tính toán mục đích đặc biệt có thể là các hệ thống máy tính để bàn, các hệ thống máy tính chủ, các hệ thống máy tính di động, các thiết bị cầm tay, các thiết bị mạng hoặc thiết bị bất kỳ khác hoặc tổ hợp của các thiết bị tích hợp phần logic được nối dây cứng và/hoặc logic chương trình để áp dụng các kỹ thuật này. Các thiết bị tính toán mục đích cụ thể có thể được áp dụng như là các máy tính cá nhân, các máy tính xách tay, các điện thoại di động, các điện thoại chụp ảnh, các điện thoại thông

minh, các thiết bị trợ giúp số cá nhân, các thiết bị chơi phương tiện, các thiết bị định vị, các thiết bị thư điện tử, các thiết bị chơi trò chơi, các máy tính bảng, các thiết bị đeo được hoặc tổ hợp của chúng. Thiết bị (các thiết bị) tính toán thường được điều khiển và được phối hợp bởi phần mềm hệ điều hành. Các hệ điều hành thông thường điều khiển và lập lịch các quy trình máy tính để thực thi, thực hiện việc quản lý bộ nhớ, tạo ra hệ thống tệp, nối mạng, các dịch vụ I/O, và tạo ra chức năng giao diện người sử dụng, như giao diện đồ họa người sử dụng (graphical user interface - GUI), bên cạnh các chức năng khác. Các hệ thống, thiết bị, môi trường lưu trữ, các mô đun, và các đơn vị khác nhau được mô tả ở đây có thể được áp dụng trong các thiết bị tính toán mục đích đặc biệt, hoặc một hoặc nhiều chip tính toán của một hoặc nhiều thiết bị tính toán mục đích đặc biệt. Theo một số phương án thực hiện, các lệnh được mô tả ở đây có thể được áp dụng trong máy ảo trên thiết bị tính toán mục đích đặc biệt. Khi được thực thi, các lệnh có thể làm cho thiết bị tính toán mục đích đặc biệt để thực hiện các phương pháp khác nhau được mô tả ở đây. Máy ảo có thể chứa phần mềm, phần cứng, hoặc tổ hợp của chúng. Ví dụ, máy ảo có thể chứa phần mềm máy ảo Ethereum (Ethereum Virtual Machine - EVM) tạo ra môi trường chạy cho các hợp đồng thông minh trong Ethereum.

Fig.7 là giản đồ khối minh họa hệ thống máy tính 700 mà các phương án thực hiện được mô tả ở đây có thể được áp dụng vào trong đó. Hệ thống 700 này có thể được thực hiện ở nút bất kỳ trong số các nút được mô tả ở đây, và được tạo cấu hình để thực hiện các bước áp dụng hợp đồng chuỗi khối. Hệ thống máy tính 700 chứa bus 702 hoặc cơ chế liên lạc khác để liên lạc thông tin, một hoặc nhiều bộ xử lý (các bộ xử lý) phân chứng 704 được ghép nối với bus 702 để xử lý thông tin. Bộ xử lý (các bộ xử lý) phân chứng 704 có thể, ví dụ là, một hoặc nhiều bộ vi xử lý mục đích chung.

Hệ thống máy tính 700 cũng chứa bộ nhớ chính 706, như bộ nhớ truy cập ngẫu nhiên (random access memory - RAM), bộ đệm và/hoặc các thiết bị lưu trữ động khác, được ghép nối tới bus 702 để lưu trữ thông tin và các lệnh có thể thực thi được bởi bộ xử lý (các bộ xử lý) 704. Bộ nhớ chính 706 cũng có thể được dùng để lưu trữ các biến số tạm thời hoặc thông tin trung gian khác trong quá trình thực thi các lệnh có thể thực thi được bởi (các) bộ xử lý 704. Các lệnh này, khi được lưu trữ trong môi trường lưu trữ có thể truy cập được bởi bộ xử lý (các bộ xử lý) 704, hệ thống máy tính phục hồi 700 vào máy mục đích riêng được tùy chỉnh để thực hiện các thao tác được chỉ rõ trong các

lệnh. Hệ thống máy tính 700 còn chứa bộ nhớ chỉ đọc (read only memory - ROM) 708 hoặc thiết bị lưu trữ tĩnh khác được ghép nối tới bus 702 để lưu trữ thông tin tĩnh và các lệnh cho bộ xử lý (các bộ xử lý) 704. Thiết bị lưu trữ 710, như đĩa từ, đĩa quang học, hoặc ổ đĩa USB nhỏ (ổ đĩa tác động nhanh - Flash), v.v., được tạo ra và được ghép nối tới bus 702 để lưu trữ thông tin và các lệnh.

Hệ thống máy tính 700 có thể áp dụng các kỹ thuật được mô tả ở đây sử dụng logic được nối dây cứng được tùy chỉnh, một hoặc nhiều ASIC hoặc FPGA, phần sụn và/hoặc logic chương trình trong kết hợp với hệ thống máy tính làm cho hoặc lập trình cho hệ thống máy tính 700 trở thành máy có mục đích riêng. Theo một phương án thực hiện, các thao tác, các phương pháp, và các quy trình được mô tả ở đây được thực hiện bởi hệ thống máy tính 700 đáp ứng lại bộ xử lý (các bộ xử lý) 704 thực thi một hoặc nhiều chuỗi của một hoặc nhiều lệnh được chứa trong bộ nhớ chính 706. Các lệnh này có thể được đọc vào trong bộ nhớ chính 706 từ môi trường lưu trữ khác, như thiết bị lưu trữ 710. Việc thực thi của các chuỗi của các lệnh được chứa trong bộ nhớ chính 706 làm cho bộ xử lý (các bộ xử lý) 704 thực hiện các bước xử lý được mô tả ở đây. Theo các phương án thực hiện thay thế, mạch được nối cứng có thể được sử dụng thay cho hoặc kết hợp với các lệnh phần mềm.

Bộ nhớ chính 706, ROM 708, và/hoặc bộ phận lưu trữ 710 có thể chứa môi trường lưu trữ phi chuyển tiếp. Thuật ngữ “môi trường phi chuyển tiếp”, và các thuật ngữ tương tự, như được sử dụng ở đây đề cập tới môi trường lưu trữ dữ liệu và/hoặc các lệnh làm cho máy vận hành theo cách cụ thể, môi trường ngoại trừ các tín hiệu chuyển tiếp. Môi trường phi chuyển tiếp này có thể còn bao gồm môi trường bất khả biến và/hoặc môi trường khả biến. Môi trường bất khả biến bao gồm, ví dụ, các đĩa quang học hoặc đĩa từ, như thiết bị lưu trữ 710. Môi trường khả biến chứa bộ nhớ động, như bộ nhớ chính 706. Các dạng chung của môi trường phi chuyển tiếp bao gồm, ví dụ, ổ đĩa mềm, ổ đĩa cứng, ổ đĩa trạng thái rắn, băng từ, hoặc môi trường lưu trữ dữ liệu từ tính khác, CD-ROM, môi trường lưu trữ dữ liệu quang học bất kỳ khác, môi trường vật lý bất kỳ khác với các mẫu lỗ, RAM, PROM, và EPROM, FLASH-EPROM, NVRAM, chip hoặc hộp nhớ bất kỳ khác, và các phiên bản được nối mạng của chúng.

Hệ thống máy tính 700 cũng chứa giao diện mạng 718 được ghép nối tới bus 702. Giao diện mạng 718 tạo ra ghép nối liên lạc dữ liệu hai chiều tới một hoặc nhiều liên kết mạng được kết nối tới một hoặc nhiều mạng cục bộ. Ví dụ, giao diện mạng 718 có thể là thẻ mạng dạng số dịch vụ được tích hợp (integrated services digital network - ISDN), bộ mã hóa/giải mã cấp, bộ mã hóa/giải mã vệ tinh, hoặc bộ mã hóa/giải mã để tạo ra kết nối liên lạc dữ liệu tới loại tương ứng của đường điện thoại. Như một ví dụ khác, giao diện mạng 718 có thể là thẻ mạng diện cục bộ (local area network - LAN) có thể tạo ra kết nối liên lạc dữ liệu tới LAN tương hợp (hoặc thành phần WAN để được kết nối với WAN). Các liên kết không dây cũng có thể được áp dụng. Theo áp dụng bất kỳ này, giao diện mạng 718 gửi và nhận các tín hiệu điện, điện từ hoặc quang học mang các luồng dữ liệu dạng số biểu diễn các loại thông tin.

Hệ thống máy tính 700 có thể gửi các tin nhắn và nhận dữ liệu, chứa mã chương trình, qua mạng (các mạng), liên kết mạng và giao diện mạng 718. Theo ví dụ Internet, máy chủ có thể truyền mã được yêu cầu cho chương trình ứng dụng qua Internet, ISP, mạng cục bộ và giao diện mạng 718.

Mã nhận được có thể được thực thi bởi bộ xử lý (các bộ xử lý) 704 khi nó được nhận, và/hoặc được lưu trữ trong thiết bị lưu trữ 710, hoặc bộ phận lưu trữ bất khả biến khác để thực thi sau.

Mỗi thành phần trong các quy trình, các phương pháp, và các thuật toán được mô tả trong các phần trên có thể được áp dụng trong, và được tự động hóa một cách hoàn toàn hoặc một phần bởi, các môđun mã được thực thi bởi một hoặc nhiều hệ thống máy tính hoặc các bộ xử lý máy tính chứa phần cứng máy tính. Các quy trình và các thuật toán có thể được áp dụng một phần hoặc hoàn toàn trong mạch ứng dụng riêng.

Các dấu hiệu và các quy trình được mô tả ở đây có thể được sử dụng độc lập với nhau hoặc cũng có thể được kết hợp theo nhiều cách. Các tổ hợp và các tổ hợp con khả thi được coi là nằm trong phạm vi bảo hộ của sáng chế này. Ngoài ra, phương pháp hoặc các khối xử lý cụ thể có thể được bỏ qua trong một số ứng dụng. Các phương pháp và quy trình được mô tả ở đây cũng không bị hạn chế vào trình cụ thể bất kỳ và các khối hoặc các trạng thái liên quan tới nó có thể được thực hiện theo các trình tự thích hợp khác. Ví dụ, các khối hoặc các trạng thái được mô tả có thể được thực hiện theo thứ tự

khác với thứ tự đã được bộc lộ cụ thể, hoặc nhiều khối hoặc trạng thái có thể được kết hợp thành khối hoặc trạng thái đơn. Các ví dụ của khối hoặc các trạng thái đơn có thể được thực hiện nối tiếp, song song, hoặc theo một số cách khác. Các khối hoặc các trạng thái có thể được thêm vào hoặc được loại bỏ khỏi các phương án thực hiện đã được bộc lộ. Các ví dụ của hệ thống và các thành phần được mô tả ở đây có thể được định cấu hình theo cách khác với cách được mô tả. Ví dụ, các thành phần có thể được thêm vào, được loại bỏ từ, hoặc được sắp xếp lại khi so sánh với các phương án thực hiện đã được bộc lộ.

Các thao tác khác nhau của các phương pháp được mô tả ở đây có thể được thực hiện, ít nhất một phần, bởi một hoặc nhiều bộ xử lý được định cấu hình một cách tạm thời (ví dụ, bởi phần mềm) hoặc được định cấu hình một cách vĩnh viễn để thực hiện các hoạt động liên quan. Dù được định cấu hình tạm thời hay vĩnh viễn, các bộ xử lý này có thể tạo thành các cơ chế được áp dụng bộ xử lý để vận hành để thực hiện một hoặc nhiều thao tác hoặc chức năng được mô tả ở đây.

Một cách tương tự, các phương pháp được mô tả ở đây có thể được áp dụng ít nhất một phần bởi bộ xử lý, với bộ xử lý cụ thể hoặc các bộ xử lý là ví dụ của phần cứng. Ví dụ, ít nhất một số thao tác trong các thao tác của phương pháp có thể được thực hiện bởi một hoặc nhiều bộ xử lý hoặc các máy được áp dụng bởi bộ xử lý. Hơn nữa, một hoặc nhiều bộ xử lý cũng có thể vận hành để trợ giúp hoạt động của các thao tác liên quan trong môi trường “điện toán đám mây - cloud computing” hoặc phần mềm làm dịch vụ (“software as a service” - SaaS). Ví dụ, ít nhất một số thao tác trong các thao tác có thể được thực hiện bởi nhóm các máy tính (như là các ví dụ của các máy chứa các bộ xử lý), với các thao tác này là có thể truy cập được thông qua mạng (ví dụ, Internet) và thông qua một hoặc nhiều giao diện thích hợp (ví dụ, giao diện chương trình ứng dụng (Application Program Interface - API)).

Hiệu quả hoạt động của thao tác cụ thể của các thao tác có thể được phân bố giữa các bộ xử lý, không chỉ nằm trong máy đơn, mà có thể được triển khai qua nhiều máy. Theo một số phương án thực hiện, các bộ xử lý hoặc các máy được áp dụng bộ xử lý có thể được định vị trong vị trí địa lý đơn (ví dụ, nằm trong môi trường nhà, môi trường văn

phòng, hoặc trại máy chủ). Theo các phương án thực hiện khác, các bộ xử lý hoặc các máy được áp dụng bộ xử lý có thể được phân bố qua nhiều vị trí địa lý khác nhau.

Qua suốt bản mô tả này, nhiều ví dụ có thể áp dụng các thành phần, các thao tác, hoặc các cấu trúc được mô tả như là ví dụ đơn. Mặc dù các thao tác đơn của một hoặc nhiều phương pháp được minh họa và được mô tả như là các thao tác tách biệt, nhưng một hoặc nhiều thao tác của các thao tác riêng biệt có thể được thực hiện đồng thời, và không yêu cầu các thao tác phải được theo thứ tự đã được minh họa. Các cấu trúc và chức năng đã được biểu diễn như là các thành phần tách biệt trong các cấu hình có thể được áp dụng làm cấu trúc hoặc thành phần được kết hợp. Một cách tương tự, các cấu trúc và chức năng được thể hiện như là thành phần đơn có thể được áp dụng như là các thành phần tách biệt. Các biến thể, biến đổi, bổ sung và cải tiến này cũng như các biến thể, biến đổi, bổ sung và cải tiến này khác sẽ nằm trong phạm vi bảo hộ của sáng chế này.

Mặc dù phần tổng quan của sáng chế này được mô tả với tham khảo tới các phương án thực hiện kèm theo, nhưng các biến đổi và thay thế khác có thể được tạo ra cho các phương án thực hiện này mà không tách khỏi phạm vi bảo hộ rộng hơn của các phương án thực hiện của sáng chế này. Phần mô tả chi tiết không được coi là hạn chế, và phạm vi bảo hộ của các phương án thực hiện khác nhau chỉ được xác định bởi các yêu cầu bảo hộ kèm theo, cùng với toàn bộ các dạng tương đương mà các yêu cầu bảo hộ này đề cập tới. Ngoài ra, các thuật ngữ có liên quan (như “thứ nhất”, “thứ hai”, “thứ ba”, v.v.) được sử dụng ở đây không mô tả thứ tự, độ cao, hoặc độ quan trọng bất kỳ nào mà chúng được sử dụng để phân biệt một thành phần này với thành phần khác. Hơn nữa, các thuật ngữ “một”, “cái”, và “nhiều” không mô tả hạn chế nào của số lượng, mà mô tả sự hiện diện của ít nhất một đối tượng trong các đối tượng được đề cập tới.

YÊU CẦU BẢO HỘ

1. Phương pháp xác thực được áp dụng bởi máy tính bao gồm các bước:

đáp lại việc đăng nhập, sinh ra (501) bản tóm tắt dạng số của thông tin nhận diện cho việc đăng nhập, trong đó thông tin nhận diện bao gồm nhận diện và mức cấp phép của người sử dụng yêu cầu hoặc cấp phép việc thực thi của giao dịch;

truyền (502) bản tóm tắt dạng số của thông tin nhận diện tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối;

thu được (503), từ chuỗi khối, nhận diện giao dịch chuỗi khối được kết hợp với bản tóm tắt dạng số của thông tin nhận diện;

đáp lại việc đăng nhập thành công, thực thi (504) giao dịch;

sinh ra (511) bản tóm tắt dạng số của thông tin vận hành của giao dịch được thực thi, trong đó thông tin vận hành chứa thông tin giao dịch của giao dịch và nhận diện giao dịch chuỗi khối được kết hợp với bản tóm tắt dạng số của thông tin nhận diện;

truyền (512) bản tóm tắt dạng số của thông tin vận hành tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối;

thu được (513) nhận diện giao dịch chuỗi khối được kết hợp với bản tóm tắt dạng số của thông tin vận hành;

thu được (514), từ thiết bị tính toán, dữ liệu kiểm toán để xác thực đối với thông tin vận hành của giao dịch được thực thi;

sinh ra (515) bản tóm tắt dạng số của dữ liệu kiểm toán;

truy hồi (516) bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối theo nhận diện giao dịch chuỗi khối tương ứng với bản tóm tắt dạng số của thông tin vận hành; và

xác định (517) tính xác thực của dữ liệu kiểm toán bằng cách xác minh bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành.

2. Phương pháp theo điểm 1, trong đó bước xác định tính xác thực của dữ liệu kiểm toán

bằng cách xác minh bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán đối với bản tóm tắt dạng số được truy hồi của thông tin vận hành bao gồm:

đáp lại xác định rằng bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán là thống nhất với bản tóm tắt dạng số được truy hồi của thông tin vận hành, xác định rằng dữ liệu kiểm toán là xác thực; hoặc

đáp lại xác định rằng bản tóm tắt dạng số được sinh ra của dữ liệu kiểm toán là không thống nhất với bản tóm tắt dạng số được truy hồi của thông tin vận hành, xác định rằng dữ liệu kiểm toán là không xác thực.

3. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó thông tin vận hành chứa một hoặc nhiều thành phần trong số: bản tóm tắt dạng số của thông tin nhận diện và thông tin nhận diện.

4. Phương pháp theo điểm 1, trong đó:

dữ liệu kiểm toán bao gồm nhận diện của giao dịch được thực thi; và

trước khi truy hồi bản tóm tắt dạng số của thông tin vận hành từ chuỗi khối theo nhận diện giao dịch chuỗi khối tương ứng với bản tóm tắt dạng số của thông tin vận hành, phương pháp còn bao gồm bước: từ hệ thống lưu trữ bên ngoài chuỗi khối, thu được, dựa trên nhận diện của giao dịch được thực thi, nhận diện giao dịch chuỗi khối tương ứng với bản tóm tắt dạng số của thông tin vận hành.

5. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó bước truyền bản tóm tắt dạng số của thông tin vận hành tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối bao gồm:

viết bản tóm tắt dạng số của thông tin vận hành và quy trình mã hóa được sử dụng để sinh ra bản tóm tắt dạng số của thông tin vận hành thành hợp đồng chuỗi khối; và

làm cho một hoặc nhiều nút khởi tạo giao dịch chuỗi khối để triển khai liên lạc chuỗi khối.

6. Phương pháp theo điểm 5, trong đó:

bước sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán bao gồm việc sinh ra bản tóm tắt dạng số của dữ liệu kiểm toán dựa trên quy trình mã hóa được sử dụng để sinh

ra bản tóm tắt dạng số của thông tin vận hành.

7. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó:

thông tin giao dịch của giao dịch bao gồm một hoặc nhiều URL, các bộ định vị nguồn tài nguyên đồng đều - uniform resource locators, để thực thi giao dịch.

8. Phương pháp theo điểm 7, trong đó:

thông tin giao dịch của giao dịch bao gồm một hoặc nhiều thông số để gọi một hoặc nhiều URL và một hoặc nhiều kết quả được trả lại từ việc gọi một hoặc nhiều URL.

9. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó bản tóm tắt dạng số của thông tin vận hành bao gồm trị số băm của thông tin vận hành.

10. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó:

chuỗi khối là chuỗi khối liên doanh.

11. Hệ thống xác thực (118), hệ thống này bao gồm:

một hoặc nhiều bộ xử lý; và

một hoặc nhiều bộ nhớ đọc được bằng máy tính được ghép với một hoặc nhiều bộ xử lý và có các lệnh được lưu trữ trên đó mà là có thể thực thi được bởi một hoặc nhiều bộ xử lý để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 10.

12. Thiết bị xác thực bao gồm nhiều môđun để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 10.

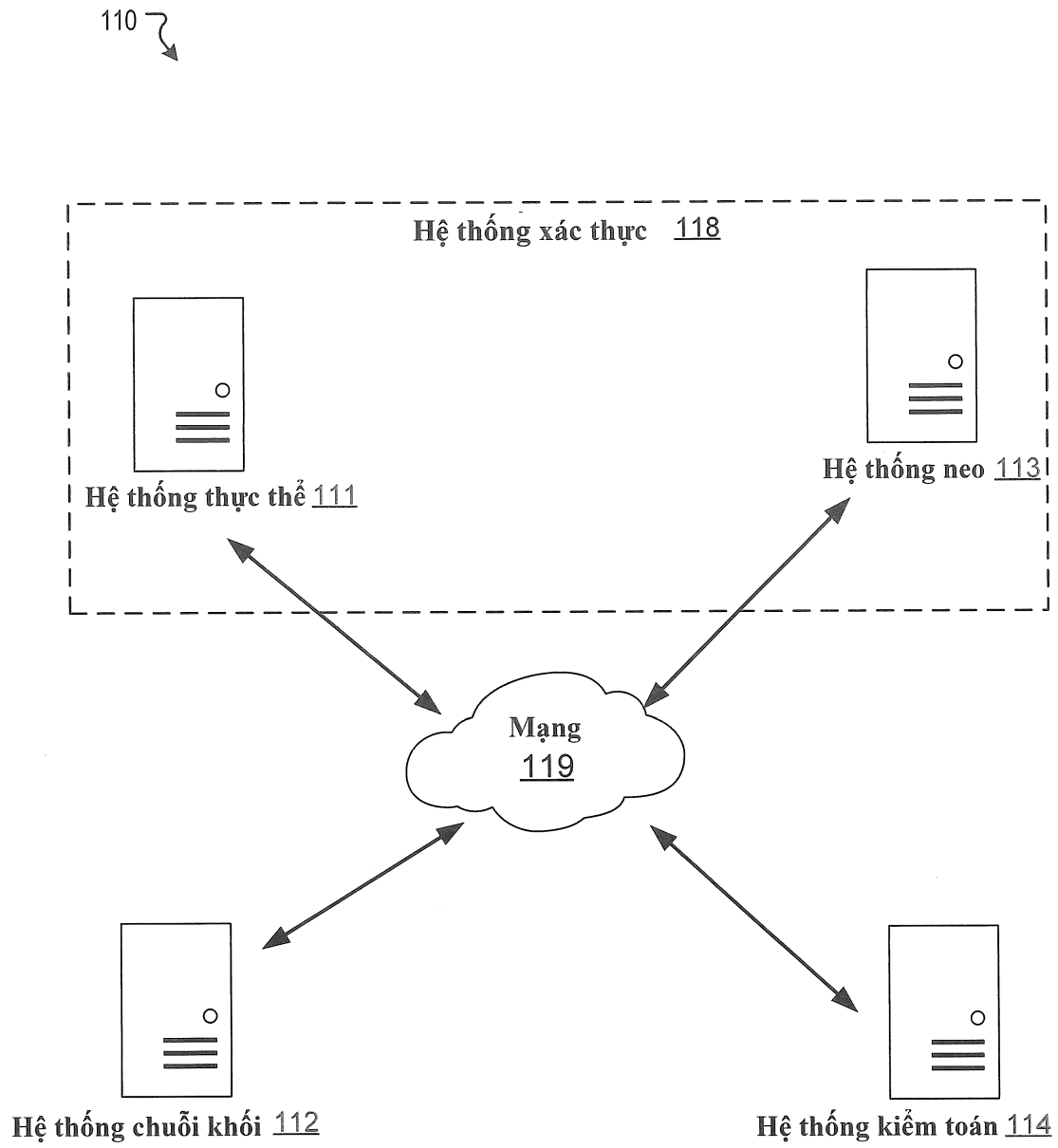


FIG. 1

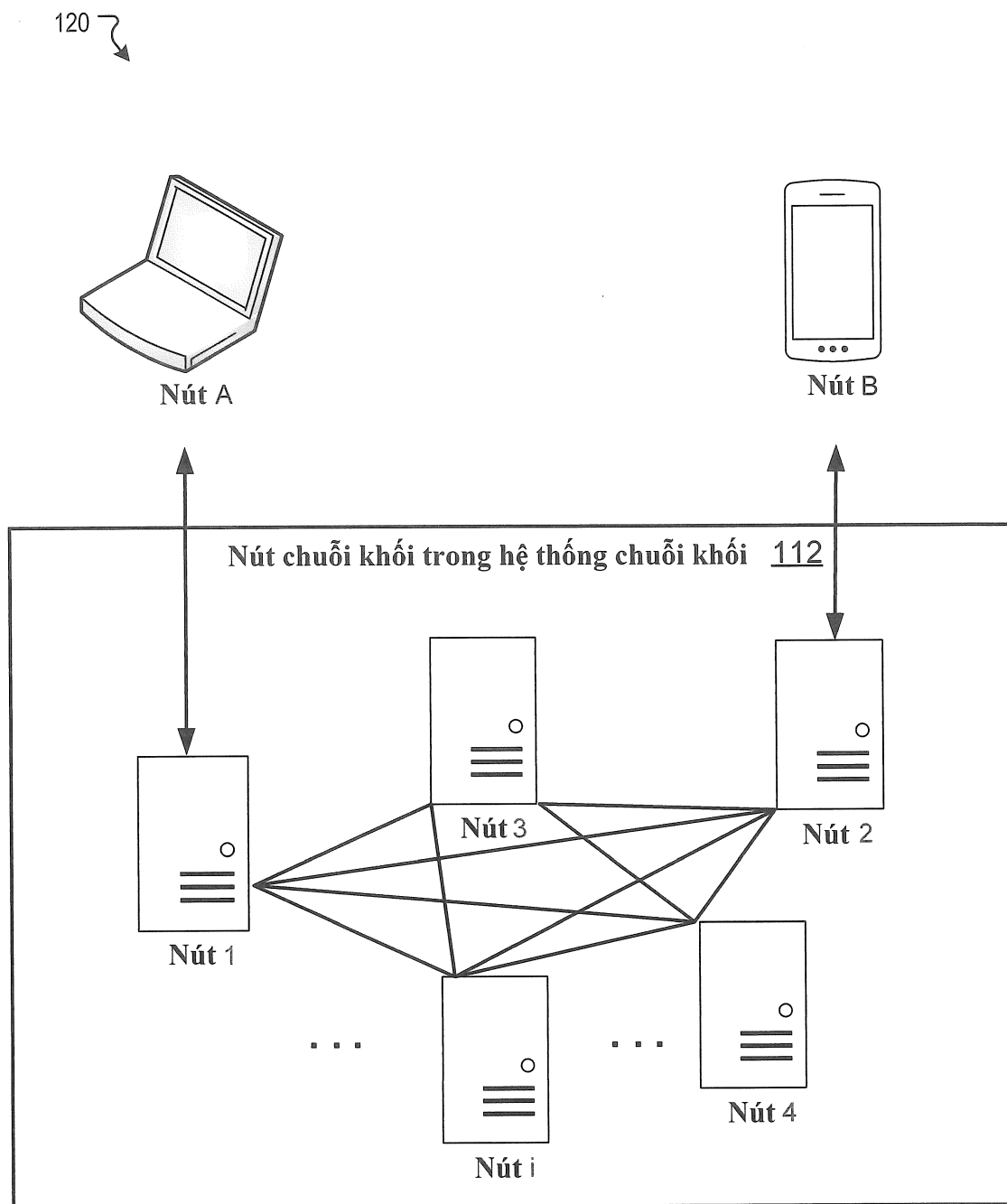


FIG. 2

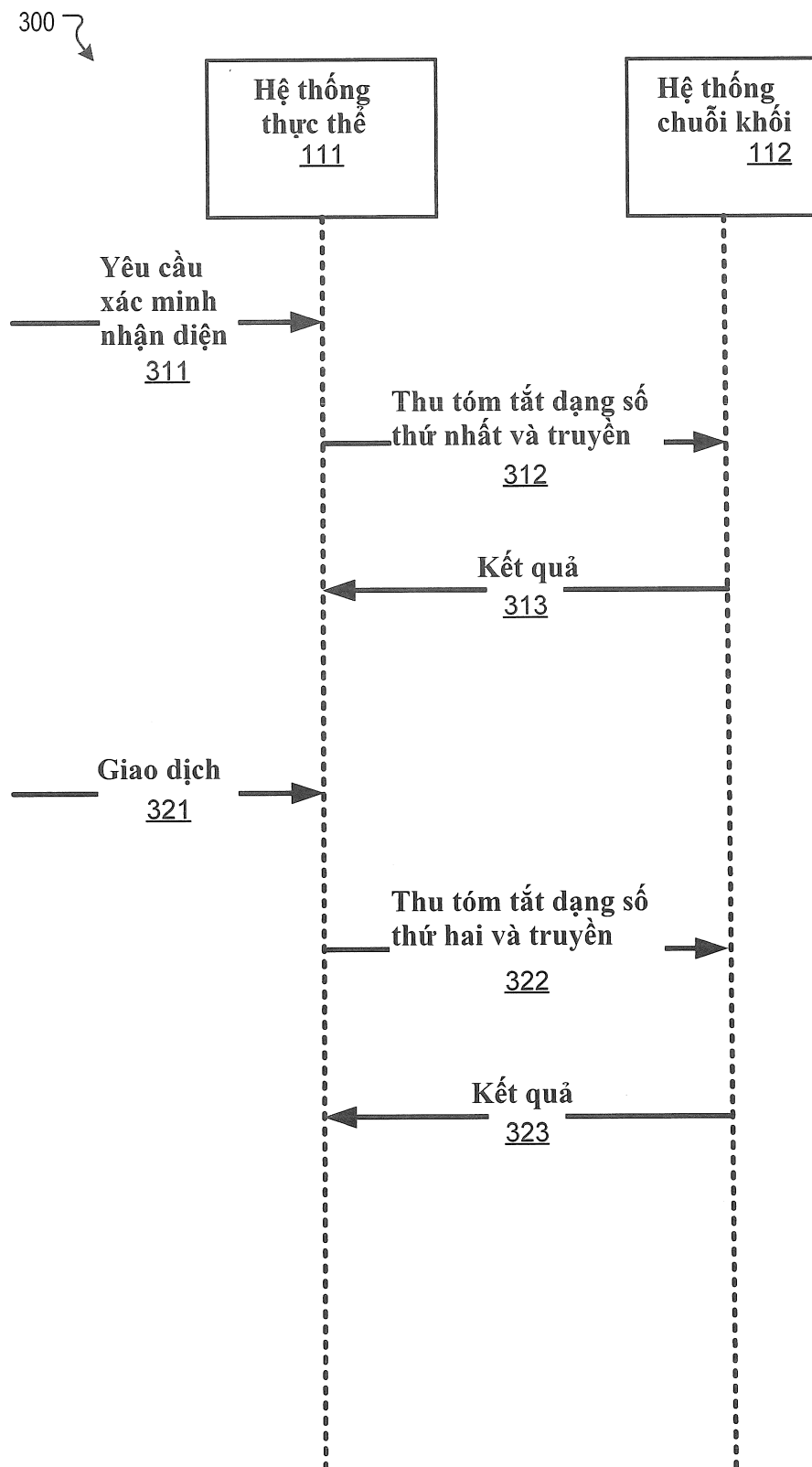


FIG. 3

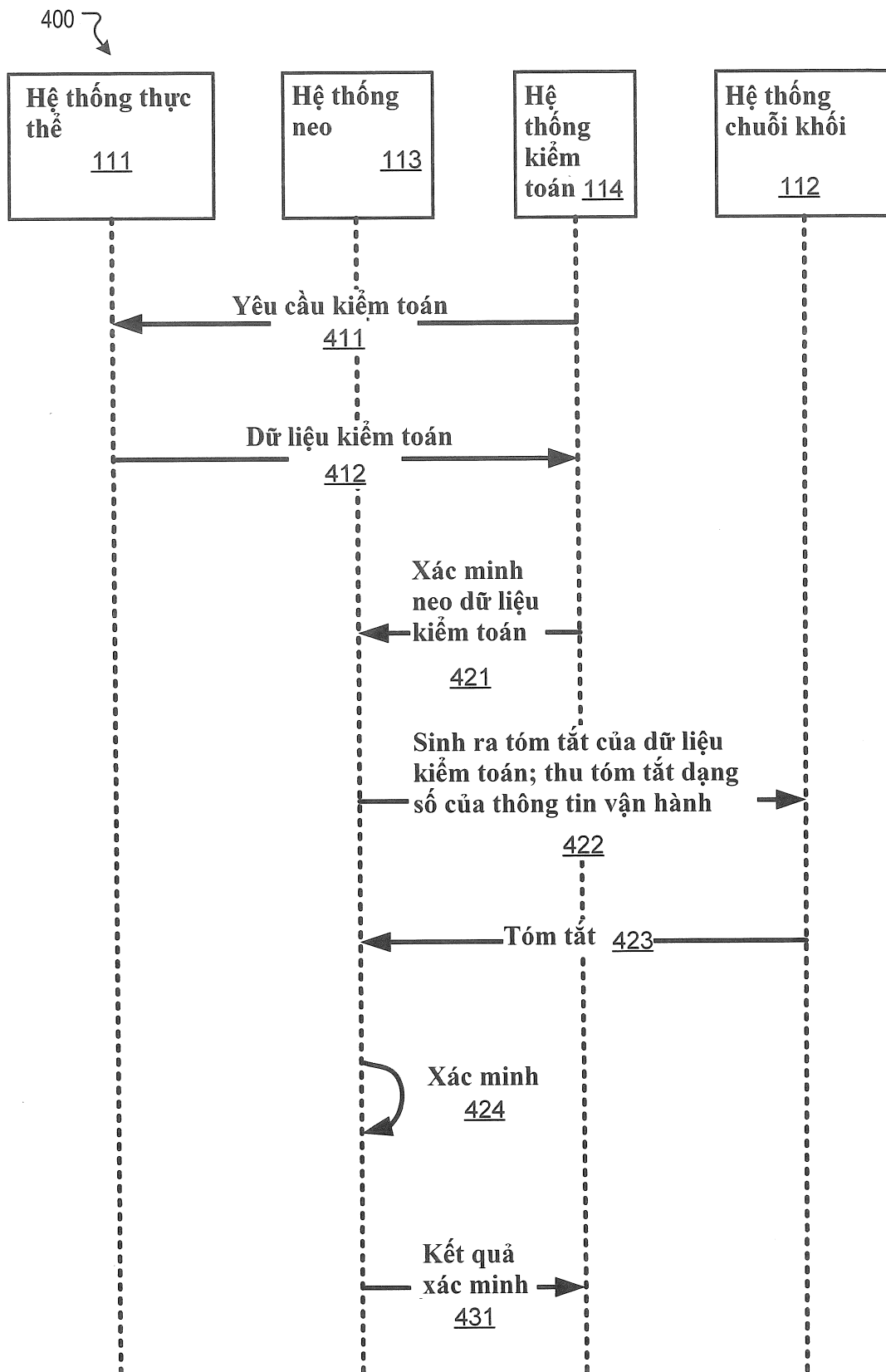


FIG. 4

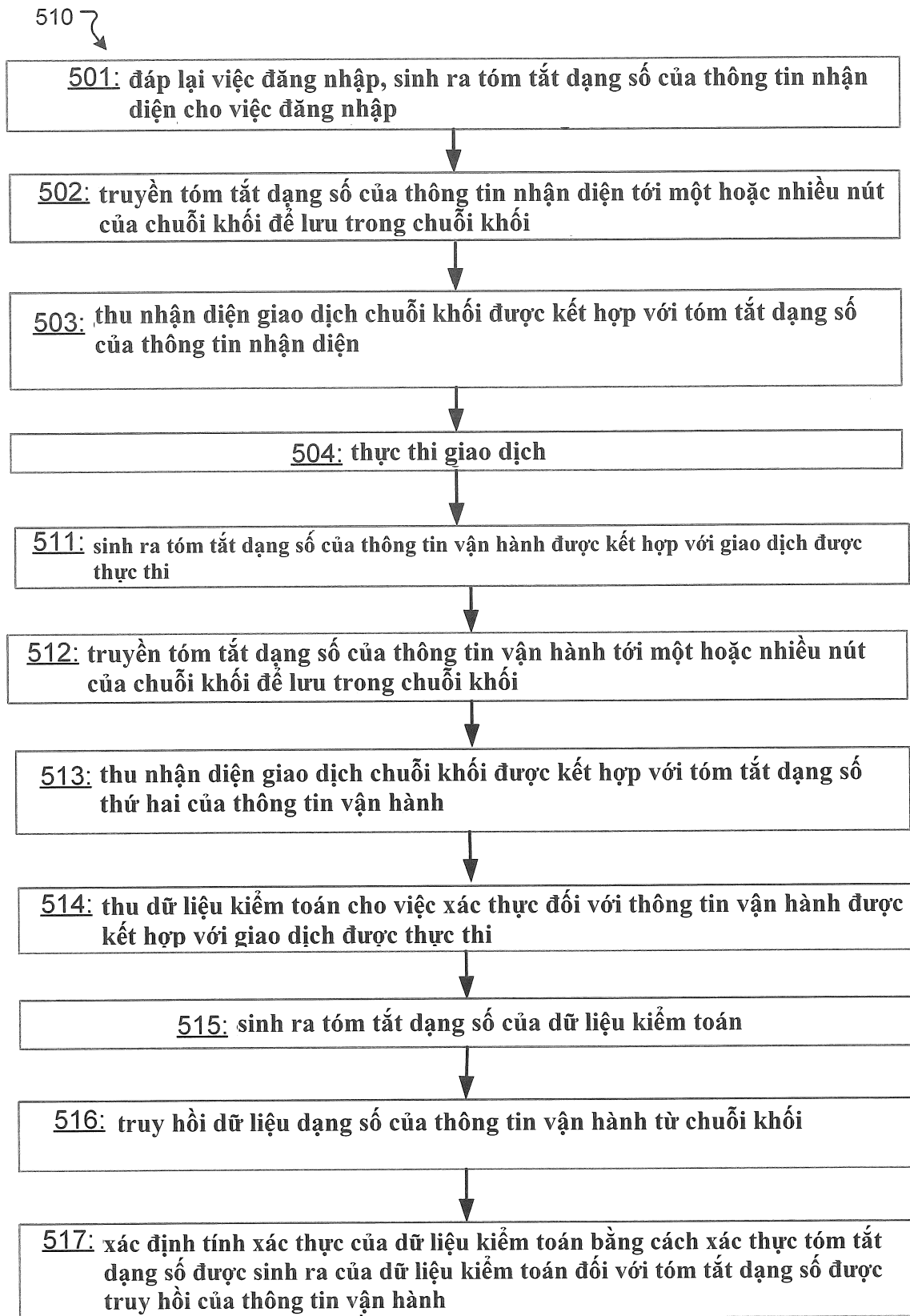
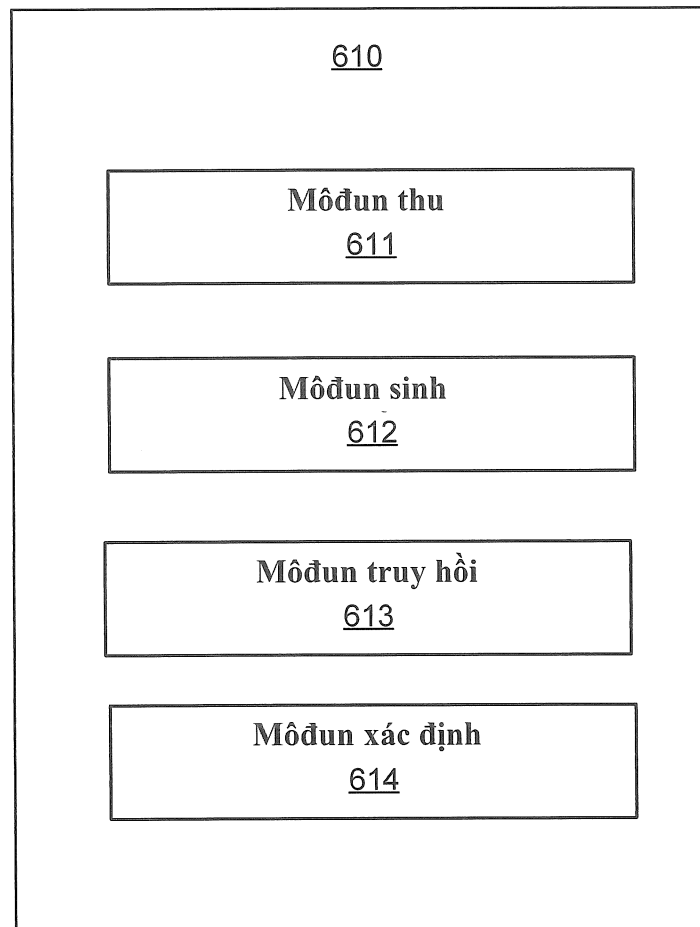


FIG. 5

**FIG. 6**

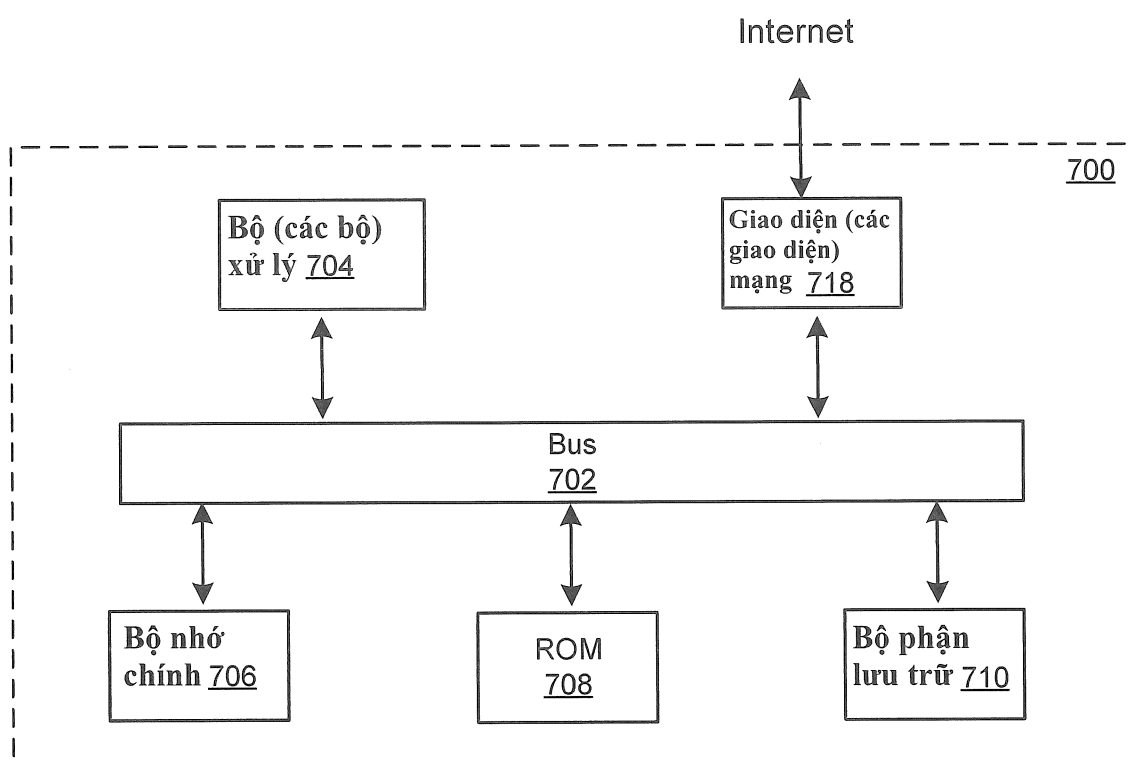


FIG. 7