



(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)



1-0038139

(51)⁷ H04L 9/00

(13) B

(21) 1-2019-03299

(22) 28/02/2019

(86) PCT/CN2019/076485 28/02/2019

(87) WO2019/101227 31/05/2019

(45) 25/01/2024 430

(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

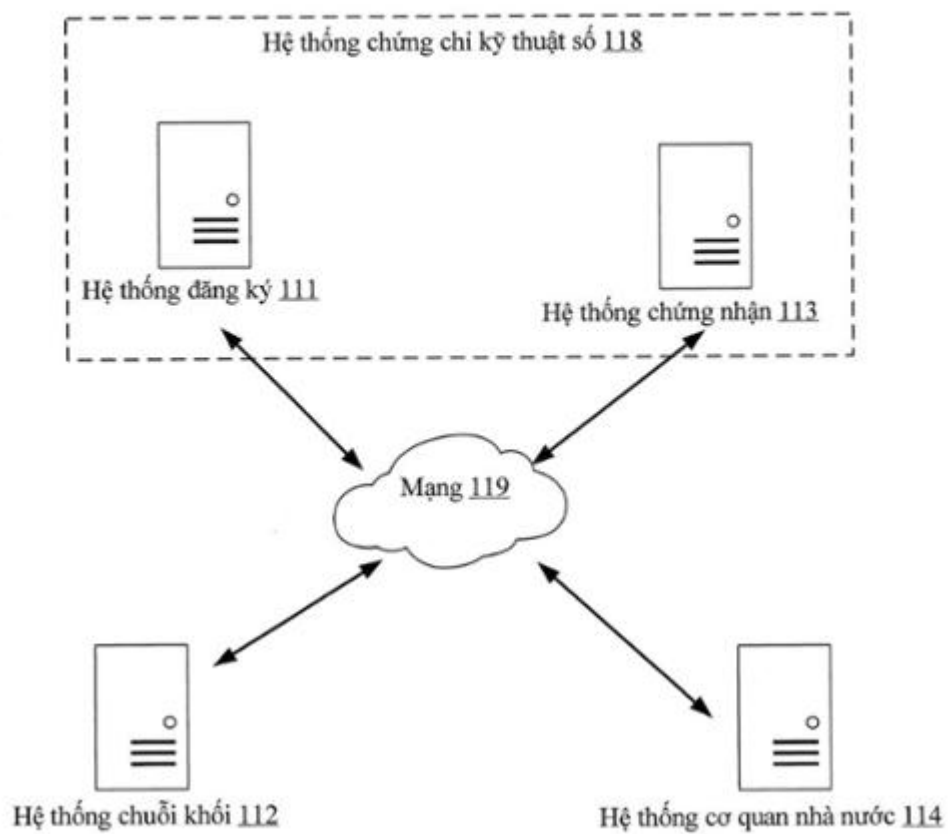
(72) CHENG, Long (CN); LI, Yanpeng (CN).

(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP ĐƯỢC THI HÀNH BỞI MÁY TÍNH ĐỂ THI HÀNH CÁC CHỨNG CHỈ KỸ THUẬT SỐ, HỆ THỐNG CHỨNG CHỈ KỸ THUẬT SỐ VÀ PHƯƠNG TIỆN LƯU TRỮ ĐƯỢC ĐƯỢC BỞI MÁY TÍNH KHÔNG CHUYÊN TIẾP

(57) Sáng chế đề cập đến các phương pháp, hệ thống, và thiết bị, bao gồm các chương trình máy tính được mã hóa trên phương tiện lưu máy tính, để thực hiện các chứng chỉ kỹ thuật số. Các phương pháp bao gồm các bước: tạo chứng chỉ kỹ thuật số; tạo bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số; truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối; thu sự nhận dạng giao dịch được kết hợp với lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số trong chuỗi khối; và kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch.

110 ↷



Lĩnh vực kỹ thuật được đề cập

Nói chung, sáng chế đề cập đến phương pháp và thiết bị để thi hành các chứng chỉ kỹ thuật số dựa vào chuỗi khối (blockchain).

Tình trạng kỹ thuật của sáng chế

Các chứng chỉ có thể cung cấp chứng cứ hoặc bằng chứng cho các giao dịch thương mại hoặc các hoạt động khác và có thể phục vụ các mục đích pháp lý nhất định. Đối với các trao đổi truyền thống, các chứng chỉ dạng giấy và được chứng thực bởi các dấu mực cao su hoặc các chữ ký. Trong một ví dụ, dấu hoặc chữ ký công ty thể hiện công ty được kết hợp được đăng ký chính thức. Tuy nhiên, các chứng chỉ giấy có thể dễ dàng bị mất hoặc hư hỏng. Đáp lại điều đó, các chứng chỉ kỹ thuật số đang dần thay thế thay thế chứng chỉ dạng giấy để khắc phục nhược điểm đó. Tuy nhiên, các chứng chỉ kỹ thuật số dễ sao chép hoặc làm sai lệch hơn các chứng chỉ giấy. Trong các công nghệ hiện tại, các chứng chỉ kỹ thuật số thường được thi hành dưới dạng hình ảnh kỹ thuật số hoặc kết xuất pdf của các chứng chỉ vật lý. Các chứng chỉ kỹ thuật số dễ bị giả mạo hoặc thay đổi trái phép khác. Kết quả là, mặc dù có các tiện ích nhất định hơn các chứng chỉ giấy, các chứng chỉ kỹ thuật số hiện nay không thể đảm bảo an ninh và thường làm giảm hoặc mất tác dụng bằng chứng pháp lý. Do đó, mong muốn có chứng chỉ kỹ thuật số an toàn và chống giả mạo.

Bản chất kỹ thuật của sáng chế

Các phương án khác nhau của sáng chế bao gồm, nhưng không bị giới hạn bởi, các hệ thống, các phương pháp, và các phương tiện đọc được bởi máy tính không chuyển tiếp để thi hành các chứng chỉ kỹ thuật số dựa vào chuỗi khối.

Theo một khía cạnh, phương pháp được thi hành bởi máy tính để thi hành các chứng chỉ kỹ thuật số bao gồm: sinh ra chứng chỉ kỹ thuật số; sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số; truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc

nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối; thu sự nhận dạng giao dịch được kết hợp với lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số trong chuỗi khối; và kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch.

Theo một số phương án, nhãn kỹ thuật số được kết hợp với thực thể. Nhãn kỹ thuật số được kết hợp với sự nhận dạng giao dịch khác được kết hợp với lưu trữ thông tin thực thể của thực thể trong chuỗi khối.

Theo các phương án khác, kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch thể hiện việc chứng thực bởi thực thể.

Theo một số phương án, nhãn kỹ thuật số bao gồm ít nhất một dấu kỹ thuật số hoặc chữ ký kỹ thuật số. Theo một phương án, nhãn kỹ thuật số bao gồm dấu kỹ thuật số. Theo phương án khác, nhãn kỹ thuật số bao gồm chữ ký kỹ thuật số. Nhãn kỹ thuật số được kết hợp với việc chứng thực bởi thực thể. khi được kết hợp với với nhãn kỹ thuật số, chứng chỉ kỹ thuật số được kết hợp với nhãn kỹ thuật số và được chứng thực bởi thực thể.

Theo các phương án khác, việc truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc nhiều nút của một hoặc nhiều nút để lưu trữ trong chuỗi khối bao gồm: viết bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số và quy trình mật mã được sử dụng để sinh ra bản tóm tắt kỹ thuật số vào trong hợp đồng chuỗi khối; và làm cho một hoặc nhiều nút để bắt đầu giao dịch chuỗi khối để triển khai liên hệ chuỗi khối.

Theo các phương án khác nữa, bản tóm tắt kỹ thuật số bao gồm giá trị băm của chứng chỉ kỹ thuật số; và sự nhận dạng giao dịch bao gồm giá trị băm của giao dịch chuỗi khối.

Theo các phương án khác nữa, việc kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch bao gồm: kết hợp nhãn kỹ thuật số, sự nhận dạng giao dịch, và bản tóm tắt kỹ thuật số.

Theo một số phương án, việc sinh ra chứng chỉ kỹ thuật số bao gồm bước: thu các nội dung của chứng chỉ kỹ thuật số từ thực thể, thực thể là công ty, và việc sinh ra chứng chỉ kỹ thuật số bao gồm nội dung.

Theo các phương án khác, phương pháp còn bao gồm bước: truyền mối quan hệ kết hợp giữa nhãn kỹ thuật số và sự nhận dạng giao dịch tới một hoặc nhiều nút để lưu trữ trong chuỗi khối.

Theo các phương án khác nữa, phương pháp còn bao gồm các bước: để đáp lại yêu cầu xác minh đối với chứng chỉ kỹ thuật số không được xác minh được chứng thực bởi nhãn kỹ thuật số không được xác minh, thu sự nhận dạng giao dịch tương ứng với chứng chỉ kỹ thuật số không được xác minh; theo sự nhận dạng giao dịch tương ứng với chứng chỉ kỹ thuật số không được xác minh, thu bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối và nhãn kỹ thuật số được lưu trữ chuỗi khối; sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số không được xác minh theo quy trình mật mã được sử dụng để sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số; xác minh nếu bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối là phù hợp với bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số không được xác minh và nếu nhãn kỹ thuật số được lưu trữ chuỗi khối là phù hợp với nhãn kỹ thuật số không được xác minh; và để đáp lại xác định rằng bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối là phù hợp với bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số không được xác minh và nhãn kỹ thuật số được lưu trữ chuỗi khối là phù hợp với nhãn kỹ thuật số không được xác minh, xác định rằng chứng chỉ kỹ thuật số không được xác minh là xác thực.

Theo một số phương án, hệ thống chứng chỉ kỹ thuật số bao gồm: một hoặc nhiều bộ xử lý; và một hoặc nhiều bộ nhớ có thể đọc được bởi máy tính được ghép với một hoặc nhiều bộ xử lý và có các lệnh được lưu trữ trên đó mà thực thi được bởi một hoặc nhiều bộ xử lý để thực hiện phương pháp của bất kỳ phương án nào trước đó.

Theo các phương án khác, thiết bị chứng chỉ kỹ thuật số bao gồm nhiều mô đun để thực hiện phương pháp của bất kỳ phương án nào trước đó.

Theo khía cạnh khác, hệ thống chứng chỉ kỹ thuật số bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ đọc được bởi máy tính không chuyển tiếp được ghép với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý làm cho hệ thống thực hiện các hoạt động bao gồm: sinh ra chứng chỉ kỹ thuật số; sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số; truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối; thu sự nhận dạng giao dịch được kết hợp với lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số trong chuỗi khối; và kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch.

Theo khía cạnh khác, phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp được tạo cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý làm cho một hoặc nhiều bộ xử lý để thực hiện các hoạt động bao gồm: sinh ra chứng chỉ kỹ thuật số; sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số; truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc nhiều nút chuỗi khối để lưu trữ trong chuỗi khối; thu sự nhận dạng giao dịch được kết hợp với lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số trong chuỗi khối; và kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch.

Theo khía cạnh khác, thiết bị chứng chỉ kỹ thuật số dựa trên chuỗi khối có thể bao gồm mô đun sinh ra thứ nhất để sinh ra chứng chỉ kỹ thuật số; mô đun sinh ra thứ hai để sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số; mô đun truyền để truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc nhiều nút chuỗi khối để lưu trữ trong chuỗi khối; mô đun thu để thu sự nhận dạng giao dịch được kết hợp với lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số trong chuỗi khối; và mô đun kết hợp để kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch.

Các phương án được bộc lộ trong bản mô tả có một hoặc nhiều hiệu quả kỹ thuật. Theo một số phương án, các phương pháp và các hệ thống có thể sinh ra nhãn kỹ thuật số vùng giả mạo để đại diện thực thể chứng thực. Sự lưu trữ trong chuỗi khối cho phép giữ bản ghi chính xác của dữ liệu gốc. Theo các phương án khác, khi thực thể đăng ký thông tin của nó (ví dụ, với người có thẩm quyền), thông tin đăng ký cũng như việc gắn của nó (sự kết hợp) với thực thể đăng ký có thể được lưu trữ vào chuỗi khối trong giao dịch chuỗi khối. Do đó, thông tin đăng ký trở nên bất biến và có thể truy xuất để xác minh. Theo các phương án khác nữa, các phương pháp và các hệ thống có thể sinh ra nhãn kỹ thuật số duy nhất được kết hợp với các thực thể đã đăng ký để chứng thực các chứng chỉ kỹ thuật số hoặc dữ liệu khác. Theo các phương án khác nữa, nhãn kỹ thuật số có thể được sinh ra dựa trên sự nhận dạng giao dịch được kết hợp với lưu trữ thông tin đăng ký trong chuỗi khối. Việc liên kết duy nhất nhãn kỹ thuật số này với thực thể đăng ký tương ứng và ngăn chặn sự giả mạo của nhận dạng. Theo một số phương án, các phương pháp và các hệ thống có thể sinh ra các chứng chỉ kỹ thuật số và lưu trữ các đại diện kỹ thuật số trong chuỗi khối. Theo các phương án khác, khi thực thể chứng thực chứng chỉ kỹ thuật số, chứng chỉ kỹ

thuật số cũng như việc gắn của nó (sự kết hợp) với nhãn kỹ thuật số của thực thể chứng thực có thể được lưu trữ vào chuỗi khối trong giao dịch chuỗi khối. Do đó, chứng chỉ kỹ thuật số và việc chứng thực của nó trở nên bất biến và có thể truy xuất để xác minh. Do đó, tính bảo mật của các chứng chỉ kỹ thuật số được nâng cao.

Các tính năng này và các tính năng khác của các hệ thống, các phương pháp, và các phương tiện đọc được bởi máy tính không chuyển tiếp được bộc lộ ở đây, cũng như các phương pháp hoạt động và chức năng của các phần tử liên quan của cấu trúc và sự kết hợp của các bộ phận và nền 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 được viết thêm vào có liên quan đến các bản vẽ kèm theo, tất cả tạo thành một phần của bản mô tả này, trong đó giống như các số tham chiếu chỉ định các phần tương ứng trong các hình khác nhau. Tuy nhiên, cần phải hiểu rõ rằng các bản vẽ chỉ nhằm mục đích minh họa và mô tả và không nhằm mục đích giới hạn.

Mô tả vắn tắt các hình vẽ

Fig.1A là hình vẽ minh họa ví dụ về hệ thống chứng chỉ kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau.

Fig.1B là hình vẽ minh họa ví dụ về mạng chuỗi khối, theo nhiều phương án khác nhau.

Fig.2 là hình vẽ minh họa ví dụ về phương pháp để sinh ra các nhãn kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau.

Fig.3 là hình vẽ minh họa ví dụ về phương pháp phát hành các chứng chỉ kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau.

Fig.4 là hình vẽ minh họa ví dụ về phương pháp xác minh các chứng chỉ kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau.

Fig.5A minh họa biểu đồ ví dụ về phương pháp để sinh ra các nhãn kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau.

Fig.5B minh họa biểu đồ ví dụ phương pháp thi hành các chứng chỉ kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau.

Fig.6A minh họa sơ đồ khối của ví dụ hệ thống máy tính sinh ra nhãn kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau.

Fig.6B minh họa sơ đồ khối của ví dụ hệ thống máy tính chứng chỉ kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau.

Fig.7 minh họa sơ đồ khối của ví dụ hệ thống máy tính trong đó bất kỳ phương án nào được mô tả ở đây có thể được thi hành.

Mô tả chi tiết sáng chế

Các phương án được bộc lộ ở đây bao gồm, nhưng không bị giới hạn bởi, các hệ thống, các phương pháp, và các phương tiện đọc được bởi máy tính không chuyển tiếp chứng chỉ kỹ thuật số dựa trên chuỗi khối. Theo nhiều phương án khác nhau, nhãn kỹ thuật số (ví dụ, dấu/chữ ký) có thể được sinh ra dựa trên thông tin xác nhận chính thức của thực thể để phục vụ như sự chứng thực bởi thực thể. Theo một số phương án, chứng chỉ kỹ thuật số có thể được phát hành dựa trên việc gắn chứng chỉ kỹ thuật số với nhãn kỹ thuật số chứng thực. Tính bất biến, tính nhất quán, và tính chính xác của chuỗi khối có thể đảm bảo tính hợp lệ và tính duy nhất của chứng chỉ kỹ thuật số và ngăn chặn giả mạo vốn thường làm cho không nhất quán hoặc không chính xác. Theo các phương án khác, việc xác nhận các chứng chỉ kỹ thuật số với các chữ ký kỹ thuật số liên kết các nội dung chứng chỉ với các thực thể xác nhận. Do đó, tính hợp lệ của các chứng chỉ kỹ thuật số có thể được xác minh một cách hiệu quả, tính bảo mật của các chứng chỉ kỹ thuật số được cải thiện, và hiệu lực pháp lý của chúng được phát huy.

Theo nhiều phương án khác nhau, các hệ thống, các phương pháp, và các phương tiện đọc được bởi máy tính không chuyển tiếp chứng chỉ kỹ thuật số được bộc lộ có thể được dựa trên các loại chuỗi khối khác nhau phụ thuộc vào thành phần được cho phép tham gia mạng lưới, thực thi giao thức đồng thuận, và duy trì sổ cái chuỗi khối được chia sẻ. Nhiều loại chuỗi khối khác nhau có thể bao gồm, ví dụ, chuỗi khối công cộng, chuỗi khối liên doanh, chuỗi khối cá nhân, v.v. Phần mô tả sau đây đề cập đến chuỗi khối liên doanh. Mặc dù vậy, các hệ thống, các phương pháp, và các phương tiện đọc được bởi máy tính không

chuyển tiếp chứng chỉ kỹ thuật số được bộc lộ cũng có thể được áp dụng đối với các loại chuỗi khối khác.

Chuỗi khối có thể được coi là cơ sở dữ liệu phi tập trung hoặc tập trung một phần, thường được gọi là sổ cái phân tán do hoạt động được thực hiện bởi nhiều nút khác nhau (ví dụ, các thiết bị tính toán) trong mạng. Thông tin bất kỳ có thể được viết cho chuỗi khối và được lưu trữ và đọc từ đó. Các nút là, ví dụ, các thiết bị tính toán hoặc các hệ thống máy tính lớn mà hỗ trợ mạng chuỗi khối và giữ cho nó chạy trơn chu. Mỗi nút có thể cung cấp một phần hoặc tất cả các chức năng của chuỗi khối. Ví dụ, nút cung cấp sự xác minh đồng thuận có thể được gọi là nút tham gia đồng thuận (hoặc nút đồng thuận). Đồng thuận có thể là một thuật toán quy tắc cho một mạng lưới các nút chuỗi khối để đạt được kết quả xử lý thường được chấp nhận. Mặc dù đồng thuận, dữ liệu liên tục được thêm vào một chuỗi các khối. Nếu các thay đổi được thực hiện cho khối, liên kết của nó với khối trước đó trong chuỗi sẽ không hợp lệ và nó sẽ hiển thị cho tất cả những người tham gia mạng, thông qua các quy tắc đồng thuận, có thể ngăn chặn các hành động trái phép bất kỳ.

Chuỗi khối liên doanh đề cập tới chuỗi khối với các thủ tục đồng thuận được điều khiển bởi các nút thiết lập trước. Chuỗi khối có thể cho phép mọi người hoặc chỉ những người tham gia được chấp thuận truy cập hoặc thông qua phương pháp truy cập lai. Ví dụ, băm gốc và API (Application Program Interface - giao diện chương trình ứng dụng) của nó có thể được mở cho công chúng; các bên ở ngoài được cho phép sử dụng API để thực hiện một số câu hỏi nhất định và thu thông tin liên quan tới trạng thái chuỗi khối.

Các chuỗi khối liên doanh có thể hiểu rõ nhất khi so sánh với đối tác phổ biến hơn của họ, chuỗi khối công cộng. Chuỗi khối công cộng không bị hạn chế truy cập, nghĩa là hoàn toàn bất kỳ ai có kết nối internet đều có thể trở thành người tham gia chuỗi khối công cộng. Cụ thể hơn, bất kỳ ai trên thế giới cũng có thể đọc dữ liệu được đưa vào chuỗi khối và bất kỳ ai trên thế giới cũng được cho phép thực thi các giao dịch trên chuỗi khối công cộng. Ngoài ra, không có giới hạn về việc ai có thể tham gia trong quá trình đồng thuận cho các chuỗi khối, đó là quá trình xác định cá nhân hoặc thực thể có thể thêm một khối vào chuỗi khối. Các chuỗi khối công cộng được coi là phi tập trung hóa hoàn toàn, với quyền điều khiển chuỗi khối không nằm trong tay của bất kỳ cá nhân hoặc tổ chức nào.

Các chuỗi khối liên doanh khác với các đối tác công khai của họ ở chỗ họ được phép, do đó, không phải bắt kỳ ai có kết nối internet cũng có thể truy cập vào một chuỗi khối của liên doanh. Những loại chuỗi khối này cũng có thể được mô tả là bán phi tập trung. Kiểm soát chuỗi khối liên doanh không được cấp cho một thực thể duy nhất, mà là nhóm các cá nhân được phê duyệt. Với chuỗi khối liên doanh, quy trình đồng thuận có thể sẽ khác với quy trình đồng thuận của chuỗi khối công cộng. Thay vì bất cứ ai có thể tham gia vào thủ tục, những người tham gia đồng thuận của chuỗi khối liên doanh có thể là một nhóm các nút được chấp thuận trước trên mạng. Các nút có thể tương ứng với các quốc gia, doanh nghiệp hoặc các thực thể khác. Do đó, các chuỗi khối liên doanh sở hữu các tính năng bảo mật vốn có trong các chuỗi khối công cộng, đồng thời cho phép mức độ kiểm soát lớn hơn đối với mạng.

Fig.1A thể hiện ví dụ về hệ thống 110 để thực hiện các bước và các phương pháp được bộc lộ khác nhau, theo nhiều phương án khác nhau. Như đã thể hiện, hệ thống 110 có thể bao gồm hệ thống đăng ký 111, hệ thống chuỗi khối 112, hệ thống chứng nhận 113, và hệ thống cơ quan nhà nước 114, mỗi hệ thống trong số đó có thể tương ứng với một hoặc nhiều thiết bị phần cứng vật lý hoặc thiết bị ảo được ghép với nhau thông qua các loại truyền thông khác nhau được đại diện bởi mạng 119.

Mỗi thành phần trong số hệ thống đăng ký 111, hệ thống chuỗi khối 112, hệ thống chứng nhận 113, và hệ thống cơ quan nhà nước 114 có thể được thi hành trong một hoặc nhiều thiết bị tính toán chẳng hạn như máy chủ, máy tính, điện thoại di động, v.v. Ví dụ, mỗi hệ thống trong số các hệ thống có thể được thi hành trong cụm máy chủ. Cụm máy chủ có thể sử dụng cân bằng tải.

Mặc dù hệ thống đăng ký 111, hệ thống chuỗi khối 112, hệ thống chứng nhận 113, và hệ thống cơ quan nhà nước 114 được hiển thị dưới dạng các thành phần duy nhất trong hình này, cần đánh giá cao các hệ thống có thể được thi hành dưới dạng một thiết bị hoặc nhiều thiết bị được ghép với nhau. Nghĩa là, hai hoặc nhiều hệ thống trong Fig.1A có thể được tích hợp vào hệ thống đơn hoặc được thi hành dưới dạng các hệ thống tách rời. Ví dụ, hệ thống đăng ký 111 và hệ thống chứng nhận 113 có thể được tích hợp vào hệ thống chứng chỉ kỹ thuật số 118 bao gồm một hoặc nhiều thiết bị tính toán. Hệ thống chứng chỉ kỹ thuật

số 118 có thể được đề cập dưới dạng hệ thống chứng chỉ kỹ thuật số dựa trên chuỗi khối. Nếu được tích hợp, hệ thống đăng ký 111 và hệ thống chứng nhận 113 có thể được thi hành như các mô đun khác nhau hoặc các thành phần tương tự của hệ thống tích hợp.

Mỗi thành phần trong số hệ thống đăng ký 111, hệ thống chuỗi khối 112, hệ thống chứng nhận 113, và hệ thống cơ quan nhà nước 114 có thể được cài đặt với phần mềm thích hợp (ví dụ, giao diện chương trình ứng dụng đăng ký, giao diện chương trình ứng dụng chuỗi khối, chương trình sinh ra chứng chỉ kỹ thuật số, giao diện ứng dụng cơ quan nhà nước) và/hoặc phần cứng (ví dụ, các kết nối có dây, không dây) để truy nhập các hệ thống hoặc các thiết bị của hệ thống 110 khác. Mỗi hệ thống trong số hệ thống đăng ký 111, hệ thống chuỗi khối 112, hệ thống chứng nhận 113, và hệ thống cơ quan nhà nước 114 có thể bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ được ghép với một hoặc nhiều bộ xử lý. Các bộ nhớ có thể là không chuyên tiếp và có thể đọc được bởi máy tính và được tạo 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 hoạt động được mô tả ở đây.

Nói chung, hệ thống đăng ký 111, hệ thống chuỗi khối 112, hệ thống chứng nhận 113, và hệ thống cơ quan nhà nước 114 có thể liên lạc với nhau qua mạng 119. Ví dụ, hệ thống đăng ký 111, hệ thống chuỗi khối 112, hệ thống chứng nhận 113, và hệ thống cơ quan nhà nước 114 có thể liên lạc với nhau thông qua một hoặc nhiều mạng có dây hoặc không dây (ví dụ, Internet) qua đó dữ liệu có thể được truyền thông. Nhiều khía cạnh khác nhau của các thành phần hệ thống được mô tả chi tiết hơn dưới đây để tham khảo Fig.1B tới Fig.7.

Fig.1B thể hiện ví dụ của mạng chuỗi khối 120, theo nhiều phương án khác nhau. Như đã 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 một mạng (ví dụ, mạng ngang hàng) với một nút chuỗi khối truyền thông với một nút khác. Thứ tự và số lượng của các nút chuỗi khối như thể hiện chỉ là ví dụ và cho sự đơn giản của minh họa. Các nút chuỗi khối có thể được thi hành 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 hoặc các thiết bị ảo được ghép với nhau qua nhiều loại của các phương pháp truyền thông như là TCP/IP. Phụ thuộc vào các

phân loại, các nút chuỗi khối có thể bao gồm các nút đầy đủ, nút Geth, các nút đồng thuận, v.v.

Theo nhiều phương án khác nhau, một hoặc nhiều nút của hệ thống chuỗi khối 112 có thể tương tác với các hệ thống và các thiết bị khác như là hệ thống đăng ký 111, hệ thống chứng nhận 113, và hệ thống cơ quan nhà nước 114 được mô tả ở trên. Các tương tác có thể liên quan việc truyền và/hoặc việc nhận của dữ liệu cho mục đích, ví dụ, các giao dịch, chứng nhận, 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 chứng chỉ kỹ thuật số 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 thực hiện thông 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 bắt đầu bởi nút 1 (hoặc một hoặc nhiều nút khác có đặc quyền như vậy dựa trên các quy tắc đồng thuận chuỗi khối) để triển khai hợp đồng tới chuỗi khối. Giống như các giao dịch chuỗi khối khác, giao dịch ở đây có thể tương ứng với băm giao dịch. Băm giao dịch có thể là đầu ra của đối tượng các thông tin giao dịch khác nhau tới hàm băm. Chuỗi khối có thể lưu trữ giá trị băm của giao dịch. Sau đó, khi thông tin cần được trích xuất (ví dụ, để xác minh), nút A/nút B (ví dụ, điện thoại di động, máy tính, v.v.) có thể ra lệnh nút 1/nút 2 (hoặc nhiều nút của hệ thống chuỗi khối 112) để bắt đầu giao dịch khác để thu thông tin từ chuỗi khối. Giao dịch khác có thể truy vấn địa chỉ để thu thông tin. Nút B có thể thuộc về hệ thống chứng chỉ kỹ thuật số 118; hệ thống cơ quan nhà nước 114, hoặc hệ thống khác (không được thể hiện) được ghép với hệ thống chuỗi khối 112.

Trong việc tương tác với hệ thống chuỗi khối 112, nút A và nút B có thể được cài đặt với phần mềm chuỗi khối thích hợp để bắt đầu, chuyển tiếp, hoặc truy nhập giao dịch. Nút A có thể truy nhập chuỗi khối thông qua truyền thông với nút 1 hoặc một hoặc nhiều nút khác của chuỗi khối, và nút B có thể truy nhập chuỗi khối thông qua truyền thông với nút 2 một hoặc nhiều nút khác của chuỗi khối. Nút A có thể gửi giao dịch tới chuỗi khối thông qua nút 1 hoặc các nút tương tự để yêu cầu bổ sung giao dịch tới chuỗi khối.

Chuỗi khối có thể được duy trì bởi nhiều nút chuỗi khối mỗi nút bao gồm hoặc được ghép với bộ nhớ. Theo một số phương án, bộ nhớ có thể lưu trữ cơ sở dữ liệu vùng. Cơ sở

dữ liệu vùng có thể truy nhập được tới nhiều nút chuỗi khối theo cách thức phân tán. Ví dụ, cơ sở dữ liệu vùng có thể được lưu trữ tương ứng trong nhiều bộ nhớ của các nút chuỗi khối. Cơ sở dữ liệu vùng có thể lưu trữ nhiều giao dịch được gửi bởi một hoặc nhiều thiết bị người dùng giống như nút A.

Theo một số phương án, sau khi nhận yêu cầu giao dịch của giao dịch không được xác nhận, nút chuỗi khối nhận có thể thực hiện một số xác minh sơ bộ của giao dịch. Ví dụ, liên quan tới Fig.1B, nút 1 có thể thực hiện xác minh sơ bộ sau khi nhận giao dịch từ nút A. Một khi được xác minh, giao dịch có thể được lưu trữ trong cơ sở dữ liệu vùng của nút chuỗi khối nhận (ví dụ, nút 1), mà có thể cũng chuyển tiếp giao dịch 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 việc xử lý được thực hiện bởi nút nhận. Một khi các giao dịch trong cơ sở dữ liệu vùng tương ứng đạt đến mức độ nhất định (ví dụ, số tiền ngưỡng), mỗi nút chuỗi khối có thể xác minh lô giao dịch trong cơ sở dữ liệu vùng tương ứng theo các quy tắc đồng thuận hoặc các quy tắc khác.

Nếu giao dịch chuỗi khối liên quan đến hợp đồng chuỗi khối (ví dụ, hợp đồng thông minh), nút chuỗi khối có thể thực thi hợp đồng chuỗi khối cục bộ. Hợp đồng chuỗi khối là giao thức máy tính nhằm mục đích tạo điều kiện, xác minh, hoặc bắt buộc theo cách kỹ thuật số đàm phán hoặc thực hiện hợp đồng. Các hợp đồng chuỗi khối cho phép hiệu suất đáng tin cậy các giao dịch chuỗi khối mà không cần các bên thứ ba. Ví dụ giao dịch chuỗi khối có thể mã hóa dữ liệu trong mã hợp đồng để lưu trữ dữ liệu (bằng cách triển khai hợp đồng) và thu hồi (bằng cách truy nhập hoặc thực thi hợp đồng). Hợp đồng chuỗi khối có thể bao gồm mã hợp đồng do người dùng viết, như là thông tin thực thể, bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số, v.v.

Nút chuỗi khối nhất định mà xác minh thành công lô các giao dịch chuỗi khối của nó phù hợp với các quy tắc đồng thuận có thể đóng gói các giao dịch chuỗi khối để thêm vào bản sao cục bộ của nó của chuỗi khối và lan truyền kết quả đến các nút chuỗi khối khác. Nút chuỗi khối nhất định có thể là nút chuỗi khối mà hoàn thành thành công thứ nhất việc xác minh, mà thu được đặc quyền xác minh, hoặc điều đó đã 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 cục bộ, xác minh các kết quả thực thi với nhau (ví dụ, bằng cách thực hiện tính toán băm), và đồng bộ hóa các bản sao của chúng của chuỗi khối với bản sao của nút chuỗi khối nhất định. Bằng cách cập nhật các bản sao cục bộ của chúng của chuỗi khối, các nút chuỗi khối khác có thể viết tương tự như vậy thông tin trong giao dịch chuỗi khối vào các bộ nhớ cục bộ tương ứng. Do đó, hợp đồng chuỗi khối được triển khai. Hợp đồng được triển khai có thể được truy nhập sau đó thông 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 trích xuất. Nếu việc xác minh sai tại một số điểm, giao dịch chuỗi khối bị từ chối. Mặc dù vậy, 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 bộc lộ.

Fig.2 là hình vẽ minh họa ví dụ về phương pháp 200 để sinh ra các nhãn kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau. Phương pháp 200 có thể được thi hành bởi một hoặc nhiều thành phần (ví dụ, hệ thống đăng ký 111, hệ thống chuỗi khối 112, hệ thống chứng nhận 113, hệ thống cơ quan nhà nước 114) của hệ thống 110 ở Fig.1A. Như được mô tả phía trên, mặc dù được thể hiện như các hệ thống tách rời, hệ thống đăng ký 111 và hệ thống chứng nhận 113 có thể được tích hợp vào hệ thống chứng chỉ kỹ thuật số 118 bao gồm một hoặc nhiều thiết bị tính toán. Các hoạt động được trình bày dưới đây được minh họa. Phụ thuộc vào việc thi hành, phương pháp 200 có thể bao gồm các bước bổ sung, ít hơn hoặc thay thế được thực hiện theo các đơn đặt hàng khác nhau hoặc song song.

Theo một số phương án, ở bước 211, thực thể thứ nhất có thể bắt đầu đăng ký thông tin thông qua hệ thống đăng ký 111. Thông tin đăng ký có thể bao gồm thông tin nhận dạng thực thể, như là số sự nhận dạng, địa chỉ, thông tin liên hệ, v.v. Thực thể có thể được kết hợp với cá nhân, công ty hoặc doanh nghiệp, tổ chức, v.v. Ví dụ, công ty có thể bắt đầu việc đăng ký thông tin công ty với hệ thống đăng ký 111 bằng cách nộp thông tin của công ty (ví dụ, tên của công ty, đăng ký của công ty, liên hệ của công ty, v.v.).

Ở bước 212, hệ thống đăng ký 111 có thể truyền yêu cầu xác minh 212 tới hệ thống chứng nhận 113. Thông tin đăng ký có thể cũng được truyền tới hệ thống chứng nhận 113.

Ở bước 213, hệ thống chứng nhận 113 có thể yêu cầu xác minh nhận dạng của thực thể với hệ thống cơ quan nhà nước 114. Ví dụ, hệ thống chứng nhận 113 có thể truyền thông

với giao diện chương trình ứng dụng của hệ thống cơ quan nhà nước 114 để xác minh nhận dạng. Ví dụ khác, hệ thống chứng nhận 113 có thể truyền thông tin đăng ký để yêu cầu hệ thống cơ quan nhà nước 114 để truy vấn cơ sở dữ liệu đăng ký công ty và xác minh nhận dạng của công ty.

Ở bước 214, hệ thống cơ quan nhà nước 114 có thể trả lại kết quả xác minh tới hệ thống chứng nhận 113.

Ở bước 221, nếu việc xác minh thành công, thì hệ thống chứng nhận 113 có thể truyền thông tin đăng ký tới hệ thống chuỗi khối 112 để lưu trữ trong chuỗi khối được duy trì bởi hệ thống chuỗi khối 112. Thông tin đăng ký có thể được coi là thông tin công cộng và có sẵn đối với nhiều nút khác nhau của chuỗi khối.

Theo nhiều phương án khác nhau, hệ thống chứng nhận 113 có thể bao gồm một hoặc nhiều nút nhẹ (ví dụ, nút A, nút B). Hệ thống chứng nhận 113 có thể bắt đầu giao dịch chuỗi khối (hoặc gọi tắt là giao dịch) thông qua nút của hệ thống chuỗi khối 112 (ví dụ, nút 1) được ghép với (các) nút nhẹ. Ví dụ, thông tin đăng ký có thể được viết vào trong hợp đồng chuỗi khối (ví dụ, hợp đồng thông minh), và giao dịch chuỗi khối có thể được bắt đầu để triển khai hợp đồng tới chuỗi khối. Bằng việc triển khai, hợp đồng có khả năng truy nhập từ chuỗi khối để thực thi, thu hồi, hoặc các hoạt động khác. Giao dịch chuỗi khối trong trường hợp này có thể tương ứng với sự nhận dạng giao dịch (ví dụ, băm giao dịch thứ nhất). Ví dụ, sự nhận dạng giao dịch chuỗi khối có thể là giá trị băm của giao dịch chuỗi khối. Sự nhận dạng giao dịch có thể cũng được kết hợp với thực thể. Chuỗi khối có thể lưu trữ thông tin đăng ký. Chuỗi khối có thể cũng lưu trữ sự nhận dạng giao dịch tương ứng. Do đó, sự nhận dạng giao dịch chuỗi khối và thông tin đăng ký được gắn (được kết hợp). Bằng cách truy vấn sự nhận dạng giao dịch, thông tin đăng ký được lưu trữ chuỗi khối có thể được trích xuất. Ví dụ, khi sự nhận dạng giao dịch chuỗi khối được gửi tới hệ thống chuỗi khối 112 (ví dụ, nút chuỗi khối), hệ thống chuỗi khối 112 có thể thực thi hợp đồng chuỗi khối để trích xuất thông tin đăng ký được lưu trữ chuỗi khối. Có nhiều phù hợp khác để lưu trữ và trích xuất thông tin đăng ký trên chuỗi khối. Người có hiểu biết trung bình trong lĩnh vực nên hiểu rằng các phương án của bản mô tả này không bị giới hạn trong ví

dụ trên. Giao dịch và sự nhận dạng giao dịch được đề cập trong đoạn này có thể được đề cập dưới dạng giao dịch thứ nhất và sự nhận dạng giao dịch thứ nhất.

Ở bước 222, hệ thống chuỗi khối 112 có thể trả lại sự nhận dạng giao dịch thứ nhất (ví dụ, bản tóm tắt kỹ thuật số) tới hệ thống chứng nhận 113. Sự nhận dạng giao dịch thứ nhất có thể là đại diện chống giả mạo kỹ thuật số mà đại diện duy nhất cho thực thể và tương ứng thông tin đăng ký. Ví dụ, hệ thống chuỗi khối 112 có thể trả lại giá trị băm của giao dịch thứ nhất như sự nhận dạng giao dịch thứ nhất tới hệ thống chứng nhận 113. Sự nhận dạng giao dịch thứ nhất chỉ báo rằng thực thể tồn tại trong chuỗi khối.

Ở bước 231, hệ thống chứng nhận 113 có thể sinh ra nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số) dựa ít nhất trên sự nhận dạng giao dịch thứ nhất đối với thực thể. Nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số) có thể được sự nhận dạng duy nhất dựa trên sự nhận dạng giao dịch thứ nhất (ví dụ, giá trị băm của giao dịch thứ nhất). Hệ thống chứng nhận 113 có thể duy trì mối quan hệ giữa thực thể và nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số).

Ở bước 241, hệ thống chứng nhận 113 có thể truyền mối quan hệ kết hợp giữa nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số) và thực thể tới hệ thống chuỗi khối 112 để lưu trữ trong chuỗi khối. Do đó, mối quan hệ kết hợp giữa nhãn kỹ thuật số được sinh ra (ví dụ, chữ ký/dấu kỹ thuật số) và thực thể có thể được lưu trữ bởi hệ thống chuỗi khối 112 và/hoặc hệ thống chứng nhận 113.

Theo nhiều phương án khác nhau, hệ thống chứng nhận 113 có thể bắt đầu giao dịch khác chuỗi khối thông qua nút của hệ thống chuỗi khối 112. Giao dịch được đề cập trong đoạn này có thể được đề cập tới giao dịch thứ hai và tương ứng với sự nhận dạng giao dịch thứ hai. Ví dụ, mối quan hệ kết hợp của sự kết hợp ở bước 241 giữa nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số) và thực thể có thể được viết vào trong hợp đồng chuỗi khối (ví dụ, hợp đồng thông minh). Giống như việc xử lý được mô tả ở trên có tham khảo tới bước 221 ở trên, giao dịch thứ hai chuỗi khối có thể được bắt đầu để triển khai hợp đồng tới chuỗi khối. Giao dịch thứ hai chuỗi khối có thể tương ứng với sự nhận dạng giao dịch thứ hai (ví dụ, băm giao dịch thứ hai), mà cũng được kết hợp với thực thể. Chuỗi khối có thể lưu trữ mối quan hệ kết hợp. Chuỗi khối có thể cũng lưu trữ sự nhận dạng giao dịch thứ hai tương

ứng. Bằng cách truy vấn sự nhận dạng giao dịch thứ hai, sự kết hợp được lưu trữ chuỗi khối có thể được trích xuất.

Ở bước 251, nếu các bước ở trên được thực thi thành công, hệ thống chứng nhận 113 có thể trả lại tin nhắn về việc đăng ký thành công tới hệ thống đăng ký 111.

Fig.3 là hình vẽ minh họa ví dụ về phương pháp 300 để phát hành các chứng chỉ kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau. Phương pháp 300 có thể được thi hành bởi một hoặc nhiều thành phần (ví dụ, hệ thống đăng ký 111, hệ thống chuỗi khối 112, hệ thống chứng nhận 113) của hệ thống 110 của Fig.1A. Như được mô tả phía trên, mặc dù được hiển thị như các hệ thống tách rời, hệ thống đăng ký 111 và hệ thống chứng nhận 113 có thể được tích hợp vào hệ thống chứng chỉ kỹ thuật số 118 bao gồm một hoặc nhiều thiết bị tính toán. Các hoạt động được trình bày dưới đây được minh họa. Phụ thuộc vào việc thi hành, phương pháp 300 có thể bao gồm các bước bổ sung, ít hơn hoặc thay thế được thực hiện theo các đơn đặt hàng khác nhau hoặc song song. Phương pháp 300 có thể được thực thi sau phương pháp 200.

Theo một số phương án, ở bước 311, thực thể thứ nhất có thể bắt đầu yêu cầu sinh ra chứng chỉ (ví dụ, chứng chỉ kỹ thuật số) thông qua hệ thống đăng ký 111. Trong bản mô tả này, chứng chỉ có thể bao gồm tài liệu chứng thực yếu tố nhất định hoặc thông tin khác. Chứng chỉ có thể được chứng thực bởi thực thể. Ví dụ, các thực thể như là các công ty hoặc các tổ chức có thể phát hành các biên lai giao dịch tài chính theo dạng các chứng chỉ kỹ thuật số. Ví dụ khác, công ty bảo hiểm có thể phát hành các chính sách bảo hiểm hoặc bằng chứng bảo hiểm theo dạng các chứng chỉ kỹ thuật số.

Ở bước 312, hệ thống đăng ký 111 có thể sinh ra dữ liệu chứng chỉ. Dữ liệu chứng chỉ có thể bao gồm các nội dung của chứng chỉ theo yêu cầu. Ví dụ, yêu cầu sinh ra biên lai cho giao dịch tài chính có thể tương ứng với dữ liệu chứng chỉ như là ngày giao dịch tài chính, lượng giao dịch tài chính, người trả tiền và người được trả tiền của giao dịch tài chính, v.v.

Ở bước 321, hệ thống đăng ký 111 có thể truyền chứng chỉ được yêu cầu tới hệ thống chứng nhận 113 và yêu cầu hệ thống chứng nhận 113 gắn chứng chỉ được yêu cầu với nhãn

kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số) được mô tả ở trên đối với Fig.2. Trong bản mô tả này, gần có thể có nghĩa là kết hợp hoặc thiết lập sự kết hợp. Sự kết hợp có thể được lưu trữ trong một hoặc nhiều thành phần của hệ thống chứng chỉ kỹ thuật số 118.

Ở bước 322, hệ thống chứng nhận 113 có thể gán chứng chỉ được yêu cầu với nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số). Theo một số phương án, hệ thống chứng nhận 113 có thể sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số.

Ở bước 331, hệ thống chứng nhận 113 có thể truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới hệ thống chuỗi khối 112 để yêu cầu hệ thống chuỗi khối 112 để lưu trữ bản tóm tắt kỹ thuật số trong chuỗi khối.

Theo nhiều phương án khác nhau, hệ thống chứng nhận 113 có thể bắt đầu giao dịch khác chuỗi khối thông qua nút của hệ thống chuỗi khối 112. Giao dịch được đề cập trong đoạn này có thể được đề cập tới giao dịch thứ ba và tương ứng với sự nhận dạng giao dịch thứ ba. Ví dụ, bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số có thể được viết vào trong hợp đồng chuỗi khối (ví dụ, hợp đồng thông minh). Giống như việc xử lý được mô tả ở trên có tham khảo tới bước 221 trên, giao dịch thứ ba chuỗi khối có thể được bắt đầu để triển khai hợp đồng tới chuỗi khối. Giao dịch thứ ba chuỗi khối có thể tương ứng với sự nhận dạng giao dịch thứ ba (ví dụ, băm giao dịch thứ ba). Sự nhận dạng giao dịch thứ ba có thể được kết hợp với thông tin như là bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số, nhãn thời gian của giao dịch thứ ba, người khởi xướng giao dịch thứ ba, v.v. Chuỗi khối có thể lưu trữ bản tóm tắt kỹ thuật số (ví dụ, giá trị băm của chứng chỉ kỹ thuật số), nhưng không lưu trữ các chi tiết (ví dụ, văn bản gốc) của chứng chỉ kỹ thuật số để đảm bảo tính riêng tư. Chuỗi khối có thể cũng lưu trữ sự nhận dạng giao dịch thứ ba tương ứng. Bằng cách truy vấn sự nhận dạng giao dịch thứ ba, bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối của chứng chỉ kỹ thuật số có thể được trích xuất. Các phương pháp thay thế khác tới hợp đồng thông minh có thể được sử dụng để đạt được lưu trữ của chứng chỉ trong chuỗi khối.

Ở bước 332, hệ thống chuỗi khối 112 có thể trả lại sự nhận dạng giao dịch thứ ba (ví dụ, băm giao dịch thứ ba) của giao dịch thứ ba để lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới hệ thống chứng nhận 113. Ở các bước 331 và 332, bản tóm tắt kỹ thuật

số của chứng chỉ kỹ thuật số được lưu trữ trong chuỗi khối có thể được sử dụng sau để xác minh chống lại những tóm tắt các chứng chỉ kỹ thuật số đáng ngờ.

Ở bước 341, hệ thống chứng nhận 113 có thể gắn dấu/chữ ký kỹ thuật số với sự nhận dạng giao dịch thứ ba của giao dịch thứ ba để lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ. Do ở bước 322, chứng chỉ được yêu cầu được gắn với nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số), chứng chỉ kỹ thuật số được lưu trữ trong hệ thống chứng nhận 113 được liên kết với đại diện bản tóm tắt kỹ thuật số của nó được lưu trữ trong chuỗi khối.

Ở bước 351, hệ thống chứng nhận 113 có thể truyền sự kết hợp trong số dấu/chữ ký kỹ thuật số, sự nhận dạng giao dịch thứ ba của giao dịch thứ ba để lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ, và bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới hệ thống chuỗi khối 112 để lưu trữ trong chuỗi khối. Do đó, thực thể, dấu/chữ ký kỹ thuật số, và chứng chỉ kỹ thuật số được kết hợp, và các mối quan hệ kết hợp được lưu trữ trong chuỗi khối.

Theo nhiều phương án khác nhau, hệ thống chứng nhận 113 có thể bắt đầu giao dịch khác chuỗi khối thông qua nút của hệ thống chuỗi khối 112. Giao dịch được đề cập trong đoạn này có thể được đề cập tới giao dịch thứ tư và tương ứng với sự nhận dạng giao dịch thứ tư. Ví dụ, mỗi quan hệ kết hợp của sự kết hợp ở bước 351 có thể được viết vào trong hợp đồng chuỗi khối (ví dụ, hợp đồng thông minh). Giống như xử lý được mô tả ở trên có tham khảo tới bước 221 trên, giao dịch thứ tư chuỗi khối có thể được bắt đầu để triển khai hợp đồng tới chuỗi khối. Giao dịch thứ tư chuỗi khối có thể tương ứng với sự nhận dạng giao dịch thứ tư (ví dụ, băm giao dịch thứ tư). Chuỗi khối có thể lưu trữ mỗi quan hệ kết hợp. Chuỗi khối có thể cũng lưu trữ sự nhận dạng giao dịch tương ứng. Bằng cách truy vấn sự nhận dạng giao dịch thứ tư, sự kết hợp được lưu trữ chuỗi khối có thể được trích xuất.

Ở bước 361, nếu các bước ở trên được thực thi thành công, hệ thống chứng nhận 113 có thể trả lại tin nhắn thành công tới hệ thống đăng ký 111.

Fig.4 là hình vẽ minh họa ví dụ về phương pháp 400 để xác minh các chứng chỉ kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau. Phương pháp 400 có thể được thi hành bởi một hoặc nhiều thành phần (ví dụ, hệ thống đăng ký 111, hệ thống chuỗi

khối 112, hệ thống chứng nhận 113) của hệ thống 110 theo Fig.1A. Như được mô tả phía trên, mặc dù được hiển thị như các hệ thống tách rời, hệ thống đăng ký 111 và hệ thống chứng nhận 113 có thể được tích hợp vào hệ thống chứng chỉ kỹ thuật số 118 bao gồm một hoặc nhiều thiết bị tính toán. Các hoạt động được trình bày dưới đây được minh họa. Phụ thuộc vào việc thi hành, phương pháp 400 có thể bao gồm các bước bổ sung, ít hơn hoặc thay thế được thực hiện theo các đơn đặt hàng khác nhau hoặc song song.

Theo một số phương án, ở bước 411, thực thể bên thứ ba có thể bắt đầu việc xác minh chứng chỉ thông qua hệ thống đăng ký 111. Ví dụ, bên thứ ba có thể thu được chứng chỉ kỹ thuật số và muốn xác minh nếu thu được chứng chỉ kỹ thuật số tồn tại trong chuỗi khối để mà xác thực chứng chỉ. Do đó, bên thứ ba có thể gửi chứng chỉ kỹ thuật số để xác minh.

Ở bước 412, hệ thống đăng ký 111 có thể truyền yêu cầu xác minh chứng chỉ như là việc gắn nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số) cho hệ thống chứng nhận 113.

Ở bước 413, đáp lại, hệ thống chứng nhận 113 có thể thu dữ liệu tương ứng với chứng chỉ từ chuỗi khối để xác minh chứng chỉ. Ví dụ, hệ thống chứng nhận 113 có thể truy vấn thông tin được lưu trữ chuỗi khối (ví dụ, bản tóm tắt kỹ thuật số được kết hợp với chứng chỉ, nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số) được kết hợp với chứng chỉ) thông qua nút của hệ thống chuỗi khối 112.

Ở bước 421, hệ thống chứng nhận 113 có thể thu dữ liệu tương ứng từ chuỗi khối. Nếu chứng chỉ tồn tại trong chuỗi khối, dữ liệu có thể bao gồm thông tin được lưu trữ trong chuỗi khối được mô tả ở trên có tham khảo tới Fig.3, như là bản tóm tắt kỹ thuật số được kết hợp với chứng chỉ (được gọi là bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối), nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số) được kết hợp với chứng chỉ (được gọi là nhãn kỹ thuật số được lưu trữ chuỗi khối).

Ở bước 422, hệ thống chứng nhận 113 có thể xác minh việc gắn (1) giữa nhãn kỹ thuật số (ví dụ, chữ ký/dấu kỹ thuật số) và chứng chỉ và (2) giữa tóm tắt của chứng chỉ và bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối được kết hợp với chứng chỉ. Do dữ liệu có thể bao gồm quy trình mật mã được sử dụng để sinh ra bản tóm tắt kỹ thuật số của chứng chỉ

kỹ thuật số (ví dụ, sự băm SHA-256), hệ thống chứng nhận 113 có thể sinh ra bản tóm tắt của chứng chỉ để thực hiện việc xác minh ở bước 422.

Cách khác, hệ thống chuỗi khối 112 có thể thực hiện việc xác minh và gửi trả các kết quả tới hệ thống chứng nhận 113.

Ở bước 431, hệ thống chứng nhận 113 có thể trả lại kết quả xác minh tới hệ thống đăng ký 111.

Fig.5A minh họa biểu đồ ví dụ phương pháp 510 để sinh ra các nhãn kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau. Phương pháp 510 có thể được thi hành bởi một hoặc nhiều thành phần (ví dụ, hệ thống chứng chỉ kỹ thuật số 118) của hệ thống 110 của Fig.1A. Phương pháp 510 có thể được thi hành bởi hệ thống bao gồm nhiều phần cứng và/hoặc phần mềm. Ví dụ, hệ thống chứng chỉ kỹ thuật số 118 có thể được thi hành bởi một hoặc nhiều hệ thống hoặc các thiết bị (ví dụ, các máy tính, các máy chủ). Hệ thống thi hành phương pháp 510 có thể bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều phương tiện lưu trữ đọc được bởi máy tính không chuyên tiếp (ví dụ, một hoặc nhiều bộ nhớ) được ghép với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý làm cho hệ thống (ví dụ, bộ xử lý) thực hiện phương pháp 510. Các hoạt động được trình bày dưới đây được minh họa. Phụ thuộc vào việc thi hành, phương pháp 510 có thể bao gồm các bước bổ sung, ít hơn hoặc thay thế được thực hiện theo các đơn đặt hàng khác nhau hoặc song song. Ví dụ về việc thi hành của phương pháp 510 được mô tả ở trên có tham khảo tới Fig.2.

Bước 511 bao gồm thu thông tin thực thể của thực thể. Theo một số phương án, thực thể là công ty, và thông tin thực thể bao gồm thông tin đăng ký công ty được xác nhận bởi cơ quan nhà nước. Ví dụ, hệ thống chứng chỉ kỹ thuật số 118 có thể thu thông tin thực thể từ thực thể dưới dạng thông tin đăng ký. Hệ thống chứng chỉ kỹ thuật số 118 có thể chuyển tiếp thông tin đăng ký tới hệ thống cơ quan nhà nước để xác minh. Một khi được xác minh, các bước sau đây có thể được thực hiện để sinh ra nhãn kỹ thuật số.

Bước 512 bao gồm truyền thông tin thực thể tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối. Theo một số phương án, truyền thông tin thực thể tới một hoặc

nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối bao gồm: viết ít nhất thông tin thực thể vào trong hợp đồng chuỗi khối; và làm cho một hoặc nhiều nút bắt đầu giao dịch chuỗi khối để triển khai liên hệ chuỗi khối. Ví dụ, các nút của chuỗi khối có thể có các đặc quyền để bắt đầu các giao dịch chuỗi khối. Hệ thống chứng chỉ kỹ thuật số 118 có thể ghép với một hoặc nhiều nút để bắt đầu giao dịch chuỗi khối. Các nút có thể xác minh và thực thi giao dịch chuỗi khối theo các quy tắc đồng thuận. Sau việc triển khai, giao dịch chuỗi khối được đóng gói thành khối mới của chuỗi khối, bản sao của chúng có sẵn tới các nút. Chi tiết có thể được đề cập đến bước 221 được mô tả ở trên. Giao dịch chuỗi khối trong trường hợp này có thể tương ứng với sự nhận dạng giao dịch (ví dụ, băm giao dịch). Chuỗi khối có thể lưu trữ thông tin thực thể. Chuỗi khối có thể cũng lưu trữ sự nhận dạng giao dịch tương ứng. Bằng cách truy vấn sự nhận dạng giao dịch, thông tin được lưu trữ chuỗi khối thực thể có thể được trích xuất.

Bước 513 bao gồm thu sự nhận dạng giao dịch (ví dụ, bản tóm tắt kỹ thuật số) được kết hợp với lưu trữ thông tin thực thể trong chuỗi khối. Sự nhận dạng giao dịch có thể được trả lại bởi một hoặc nhiều nút của chuỗi khối khi thông tin thực thể được lưu trữ thành công trong chuỗi khối. Theo một số phương án, sự nhận dạng giao dịch bao gồm giá trị băm của giao dịch chuỗi khối. Ví dụ, thuật toán băm có thể được hiểu là hàm để nén các tin nhắn với độ dài bất kỳ thành tóm tắt tin nhắn độ dài cố định. Các hàm băm thường được sử dụng bao gồm MD5 và SHA. Giá trị băm của giao dịch chuỗi khối có thể bao gồm đầu ra của hàm băm có các thông tin khác nhau của giao dịch chuỗi khối dưới dạng đầu vào. Thông tin của giao dịch chuỗi khối có thể bao gồm một hoặc nhiều tham số giao dịch như là “từ” (địa chỉ người gửi), “giá trị” (giá trị giao dịch), “gas” (chi phí hoàn thành giao dịch), “dữ liệu” (dữ liệu hợp đồng chuỗi khối), v.v. Thuật toán băm trong chuỗi khối là không thể đảo ngược, nghĩa là, việc tính toán chuyển tiếp là dễ dàng, và tính toán ngược không thể được thực hiện ngay cả khi tất cả các tài nguyên tính toán đã cạn kiệt. Do đó, giá trị băm của giao dịch chuỗi khối là duy nhất. Chi tiết có thể được đề cập đến bước 222 được mô tả ở trên.

Bước 514 bao gồm sinh ra nhãn kỹ thuật số cho thực thể được dựa trên ít nhất sự nhận dạng giao dịch. Nhãn kỹ thuật số được kết hợp với thực thể. Mỗi quan hệ kết hợp có thể được duy trì bởi hệ thống chứng chỉ kỹ thuật số 118. Theo một số phương án, nhãn kỹ thuật

số bao gồm sự nhận dạng giao dịch (ví dụ, giá trị băm của giao dịch chuỗi khối). Giá trị băm dữ liệu nhất định là kết quả số của việc áp dụng thuật toán băm tới dữ liệu như là nhiều thông tin khác nhau của giao dịch chuỗi khối được mô tả ở trên. Ví dụ, nhãn kỹ thuật số có thể là sự nhận dạng giao dịch ở bước 513. Sự nhận dạng giao dịch có thể là cách khác được đề cập tới dưới dạng tóm tắt của giao dịch tương ứng. Chi tiết có thể được đề cập đến bước 231 được mô tả ở trên.

Theo một số phương án, nhãn kỹ thuật số bao gồm ít nhất một dấu kỹ thuật số hoặc chữ ký kỹ thuật số; và nhãn kỹ thuật số có thể kết hợp với chứng chỉ kỹ thuật số để thể hiện sự chứng thực bởi thực thể. Ví dụ, bởi sự kết hợp, nhãn kỹ thuật số và chứng chỉ kỹ thuật số có thể được kết hợp thành một tệp tin. Ví dụ khác, bởi sự kết hợp, chứng chỉ kỹ thuật số có thể được liên kết với nhãn kỹ thuật số.

Theo một số phương án, phương pháp còn bao gồm truyền mối quan hệ kết hợp giữa thực thể và nhãn kỹ thuật số tới một hoặc nhiều nút để lưu trữ trong chuỗi khối. Ví dụ, các nút của chuỗi khối có thể có đặc quyền để bắt đầu các giao dịch chuỗi khối. Hệ thống chứng chỉ kỹ thuật số 118 có thể ghép với một hoặc nhiều nút để bắt đầu giao dịch chuỗi khối. Các nút có thể xác minh và thực thi giao dịch chuỗi khối theo các quy tắc đồng thuận. Sau khi triển khai, giao dịch chuỗi khối được đóng gói thành khối mới của chuỗi khối, bản sao của chúng có sẵn tới các nút. Chi tiết có thể được đề cập đến bước 241 được mô tả ở trên. Giao dịch chuỗi khối trong trường hợp này có thể tương ứng với sự nhận dạng giao dịch (ví dụ, băm giao dịch). Chuỗi khối có thể lưu trữ sự kết hợp. Chuỗi khối có thể cũng lưu trữ sự nhận dạng giao dịch tương ứng. Bằng cách truy vấn sự nhận dạng giao dịch, sự kết hợp được lưu trữ chuỗi khối có thể được trích xuất.

Theo một số phương án, phương pháp còn bao gồm các bước: sinh ra chứng chỉ kỹ thuật số; kết hợp nhãn kỹ thuật số với chứng chỉ kỹ thuật số; truyền chứng chỉ kỹ thuật số tới một hoặc nhiều nút chuỗi khối để lưu trữ trong chuỗi khối; thu bản tóm tắt kỹ thuật số khác được kết hợp với lưu trữ chứng chỉ kỹ thuật số trong chuỗi khối; kết hợp nhãn kỹ thuật số với bản tóm tắt kỹ thuật số khác; và truyền mối quan hệ kết hợp giữa nhãn kỹ thuật số và sự nhận dạng giao dịch tới một hoặc nhiều nút để lưu trữ trong chuỗi khối. Sự kết hợp của nhãn kỹ thuật số với bản tóm tắt kỹ thuật số khác cho thấy sự chứng thực bởi thực thể.

Do chứng chỉ kỹ thuật số được liên kết với bản tóm tắt kỹ thuật số khác, chứng chỉ kỹ thuật số được chứng thực bởi thực thể. Phương pháp có thể còn bao gồm bước truyền mỗi quan hệ kết hợp của nhãn kỹ thuật số với sự nhận dạng giao dịch tới một hoặc nhiều nút để lưu trữ trong chuỗi khối. Nhiều chi tiết sẽ được mô tả dưới đây có tham khảo tới Fig.5B.

Theo các phương án khác, chứng chỉ kỹ thuật số có thể được thu bởi thiết bị bất kỳ. Phương pháp còn bao gồm các bước: sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số được kết hợp với thực thể; truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối; thu sự nhận dạng giao dịch khác được kết hợp với lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số trong chuỗi khối; và kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch khác. Sự kết hợp của nhãn kỹ thuật số với sự nhận dạng giao dịch khác cho thấy sự chứng thực bởi thực thể. Do chứng chỉ kỹ thuật số được liên kết với sự nhận dạng giao dịch khác, chứng chỉ kỹ thuật số được chứng thực bởi thực thể. Phương pháp có thể còn bao gồm bước truyền mỗi quan hệ kết hợp của nhãn kỹ thuật số với sự nhận dạng giao dịch khác tới một hoặc nhiều nút để lưu trữ trong chuỗi khối.

Theo các phương án khác nữa, phương pháp còn bao gồm các bước: sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số được kết hợp với thực thể; và kết hợp nhãn kỹ thuật số với bản tóm tắt kỹ thuật số. Sự kết hợp của nhãn kỹ thuật số với bản tóm tắt kỹ thuật số cho thấy sự chứng thực bởi thực thể. Do chứng chỉ kỹ thuật số được liên kết với bản tóm tắt kỹ thuật số, chứng chỉ kỹ thuật số được chứng thực bởi thực thể. Phương pháp có thể còn bao gồm truyền mỗi quan hệ kết hợp của nhãn kỹ thuật số với bản tóm tắt kỹ thuật số tới một hoặc nhiều nút để lưu trữ trong chuỗi khối.

Theo các phương án khác nữa, phương pháp còn bao gồm bước: kết hợp nhãn kỹ thuật số với chứng chỉ kỹ thuật số được kết hợp với thực thể. Sự kết hợp của nhãn kỹ thuật số với chứng chỉ kỹ thuật số cho thấy sự chứng thực bởi thực thể. Phương pháp có thể còn bao gồm truyền mỗi quan hệ kết hợp của nhãn kỹ thuật số với chứng chỉ kỹ thuật số tới một hoặc nhiều nút để lưu trữ trong chuỗi khối.

Fig.5B minh họa biểu đồ ví dụ phương pháp 520 để thi hành các chứng chỉ kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau. Phương pháp 520 có thể được thi

hành bởi một hoặc nhiều thành phần (ví dụ, hệ thống chứng chỉ kỹ thuật số 118) của hệ thống 110 của Fig.1A. Phương pháp 520 có thể được thi hành bởi hệ thống bao gồm nhiều phần cứng và/hoặc phần mềm. Ví dụ, hệ thống chứng chỉ kỹ thuật số 118 có thể được thi hành bởi một hoặc nhiều hệ thống hoặc các thiết bị (ví dụ, các máy tính, các máy chủ). Hệ thống thi hành phương pháp 520 có thể bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp (ví dụ, một hoặc nhiều bộ nhớ) được ghép với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý làm cho hệ thống (ví dụ, bộ xử lý) thực hiện phương pháp 520. Các hoạt động được trình bày dưới đây được dự định để minh họa. Phụ thuộc vào việc thi hành, phương pháp 520 có thể bao gồm các bước bổ sung, ít hơn hoặc thay thế được thực hiện theo các thứ tự khác nhau hoặc song song. Ví dụ về việc thi hành của phương pháp 520 được mô tả ở trên có tham khảo tới Fig.3 và Fig.4.

Bước 521 bao gồm sinh ra chứng chỉ kỹ thuật số. Theo một số phương án, việc sinh ra chứng chỉ kỹ thuật số bao gồm: thu các nội dung của chứng chỉ kỹ thuật số từ thực thể, thực thể là công ty; và sinh ra chứng chỉ kỹ thuật số bao gồm các nội dung. Ví dụ, hệ thống chứng chỉ kỹ thuật số 118 có thể thu các nội dung mà cần được thể hiện ở chứng chỉ kỹ thuật số từ thực thể hoặc nguồn khác. Chi tiết có thể được đề cập đến bước 312 được mô tả ở trên.

Tùy chọn bước 522 bao gồm kết hợp nhãn kỹ thuật số với chứng chỉ kỹ thuật số. Nhãn kỹ thuật số có thể được mô tả ở trên có tham khảo tới Fig.5A. Nhãn kỹ thuật số có thể được duy trì bởi hệ thống chứng chỉ kỹ thuật số 118. Theo một số phương án, nhãn kỹ thuật số bao gồm dấu kỹ thuật số và/hoặc chữ ký kỹ thuật số; và nhãn kỹ thuật số được kết hợp với sự chứng thực bởi thực thể. Chi tiết có thể được đề cập đến bước 322 được mô tả ở trên.

Bước 523 bao gồm sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số. Ví dụ, quy trình băm như là SHA-256 có thể được sử dụng để sinh ra bản tóm tắt kỹ thuật số từ chứng chỉ kỹ thuật số. Do đó, các nội dung của chứng chỉ kỹ thuật số được chuyển đổi thành một đại diện mật mã.

Bước 524 bao gồm truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc nhiều nút chuỗi khối để lưu trữ trong chuỗi khối. Theo một số phương án, truyền bản

tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối bao gồm: viết bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số và quy trình mật mã được sử dụng để sinh ra bản tóm tắt kỹ thuật số (ví dụ, sự băm SHA-256) vào trong hợp đồng chuỗi khối; và làm cho một hoặc nhiều nút bắt đầu giao dịch chuỗi khối để triển khai liên hệ chuỗi khối. Ví dụ, các nút của chuỗi khối có thể có đặc quyền để bắt đầu các giao dịch chuỗi khối. Hệ thống chứng chỉ kỹ thuật số 118 có thể ghép với một hoặc nhiều của nút để bắt đầu giao dịch chuỗi khối. Các nút có thể xác minh và thực thi giao dịch chuỗi khối theo các quy tắc đồng thuận. Sau khi triển khai, giao dịch chuỗi khối được đóng gói thành khối mới của chuỗi khối, bản sao của chúng có sẵn tới các nút. Chi tiết có thể được đề cập đến bước 331 được mô tả ở trên. Giao dịch chuỗi khối trong trường hợp này có thể tương ứng với sự nhận dạng giao dịch (ví dụ, băm giao dịch). Chuỗi khối có thể lưu trữ bản tóm tắt kỹ thuật số (ví dụ, giá trị băm của chứng chỉ kỹ thuật số), nhưng không lưu trữ các chi tiết (ví dụ, văn bản gốc) của chứng chỉ kỹ thuật số để đảm bảo tính riêng tư. Chuỗi khối có thể cũng lưu trữ sự nhận dạng giao dịch tương ứng. Bằng cách truy vấn sự nhận dạng giao dịch, bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối của chứng chỉ kỹ thuật số có thể được trích xuất.

Bước 525 bao gồm thu sự nhận dạng giao dịch được kết hợp với lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số trong chuỗi khối. Sự nhận dạng giao dịch (ví dụ, bản tóm tắt của giao dịch) có thể được trả lại bởi một hoặc nhiều nút của chuỗi khối khi bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số được lưu trữ thành công trong chuỗi khối. Theo một số phương án, bản tóm tắt kỹ thuật số bao gồm giá trị băm của chứng chỉ kỹ thuật số; và sự nhận dạng giao dịch bao gồm giá trị băm của giao dịch chuỗi khối. Chuỗi khối có thể lưu trữ bản tóm tắt kỹ thuật số hơn là văn bản gốc của chứng chỉ kỹ thuật số để bảo vệ sự riêng tư. Chi tiết có thể được đề cập đến bước 332 được mô tả ở trên.

Bước 526 bao gồm kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch. Chi tiết có thể được đề cập đến gần bước 341 được mô tả ở trên. Theo một số phương án, kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch bao gồm: kết hợp nhãn kỹ thuật số, sự nhận dạng giao dịch, và bản tóm tắt kỹ thuật số. Theo một số phương án, phương pháp còn bao gồm: truyền mối quan hệ kết hợp giữa nhãn kỹ thuật số và sự nhận dạng giao dịch tới một hoặc

nhiều nút để lưu trữ trong chuỗi khối. Theo một số phương án, phương pháp còn bao gồm: truyền sự kết hợp trong số nhãn kỹ thuật số, sự nhận dạng giao dịch, và bản tóm tắt kỹ thuật số. Ví dụ, các nút của chuỗi khối có thể có đặc quyền bắt đầu các giao dịch chuỗi khối. Hệ thống chứng chỉ kỹ thuật số 118 có thể ghép với một hoặc nhiều của các nút bắt đầu giao dịch chuỗi khối. Các nút có thể xác minh và thực thi giao dịch chuỗi khối theo các quy tắc đồng thuận. Sau khi triển khai, giao dịch chuỗi khối được đóng gói thành khối mới của chuỗi khối, bản sao của chúng có sẵn tới các nút. Chi tiết có thể được đề cập đến bước 351 được mô tả ở trên. Giao dịch chuỗi khối trong trường hợp này có thể tương ứng với sự nhận dạng giao dịch (ví dụ, băm giao dịch). Chuỗi khối có thể lưu trữ sự kết hợp. Chuỗi khối có thể cũng lưu trữ sự nhận dạng giao dịch tương ứng. Bằng cách truy vấn sự nhận dạng giao dịch, sự kết hợp được lưu trữ chuỗi khối có thể được trích xuất.

Theo một số phương án, phương pháp còn bao gồm các bước: để đáp lại yêu cầu xác minh đối với chứng chỉ kỹ thuật số không được xác minh được chứng thực bởi nhãn kỹ thuật số không được xác minh, thu sự nhận dạng giao dịch tương ứng với chứng chỉ kỹ thuật số không được xác minh; theo sự nhận dạng giao dịch tương ứng với chứng chỉ kỹ thuật số không được xác minh, thu bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối và nhãn kỹ thuật số được lưu trữ chuỗi khối; sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số không được xác minh theo quy trình mật mã được sử dụng để sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số; xác minh nếu bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối là phù hợp với bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số không được xác minh và nếu nhãn kỹ thuật số được lưu trữ chuỗi khối là phù hợp với nhãn kỹ thuật số không được xác minh; để đáp lại việc xác định rằng bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối là phù hợp với bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số không được xác minh và nhãn kỹ thuật số được lưu trữ chuỗi khối là phù hợp với nhãn kỹ thuật số không được xác minh, xác định rằng chứng chỉ kỹ thuật số không được xác minh là xác thực; và để đáp lại xác định rằng bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối là không phù hợp với bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số không được xác minh hoặc nhãn kỹ thuật số được lưu trữ chuỗi khối là không phù hợp với nhãn kỹ thuật số không được xác minh, xác định rằng chứng chỉ kỹ thuật số không được xác minh là không xác thực.

Ví dụ, như được mô tả ở trên có tham khảo tới Fig.4, bên thứ ba có thể nhận được chứng chỉ kỹ thuật số không được xác minh được chứng thực bởi nhãn không được xác minh của thực thể không được xác minh và muốn xác minh tính xác thực của nó. Do chuỗi khối lưu trữ các mối quan hệ kết hợp giữa các thực thể, các bản tóm tắt cho các chứng chỉ kỹ thuật số, sự nhận dạng các giao dịch, và các nhãn kỹ thuật số tương ứng, hệ thống chứng chỉ kỹ thuật số 118 có thể thu sự nhận dạng giao dịch tương ứng với chứng chỉ kỹ thuật số không được xác minh và trích xuất thông tin được lưu trữ chuỗi khối tương ứng, ví dụ, bằng cách khởi tạo giao dịch qua một hoặc nhiều nút của chuỗi khối để thu dữ liệu (ví dụ, bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối, nhãn kỹ thuật số được lưu trữ chuỗi khối, thông tin được lưu trữ chuỗi khối thực thể) được kết hợp với chứng chỉ kỹ thuật số không được xác minh. Để xác minh, hệ thống chứng chỉ kỹ thuật số 118 có thể lấy được bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số không được xác minh. Hệ thống chứng chỉ kỹ thuật số 118 có thể xác minh nếu bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số không được xác minh là phù hợp với bản tóm tắt kỹ thuật số được lưu trữ chuỗi khối (để đảm bảo rằng các nội dung của chứng chỉ kỹ thuật số không bị làm giả mạo) và nếu nhãn kỹ thuật số không được xác minh là phù hợp với nhãn kỹ thuật số (để đảm bảo rằng việc chứng thực thực thể là chính xác). Một cách tùy chọn, hệ thống chứng chỉ kỹ thuật số 118 có thể xác minh nếu thực thể không được xác minh là phù hợp với thông tin được lưu trữ chuỗi khối thực thể được kết hợp với chứng chỉ kỹ thuật số. Nếu việc xác minh tính nhất quán thành công, hệ thống chứng chỉ kỹ thuật số 118 có thể được xác định rằng chứng chỉ kỹ thuật số không được xác minh là xác thực. Nếu dữ liệu không thể thu được hoặc nếu của việc xác minh tính nhất quán bất kỳ sai, thì hệ thống chứng chỉ kỹ thuật số 118 có thể được xác định rằng chứng chỉ kỹ thuật số không được xác minh là không xác thực.

Fig.6A minh họa sơ đồ khối của ví dụ hệ thống máy tính 610 để sinh ra nhãn kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau. Hệ thống 610 có thể là ví dụ về việc thi hành một hoặc nhiều thành phần (ví dụ, hệ thống chứng chỉ kỹ thuật số 118) của hệ thống 110 của Fig.1A. Phương pháp 510 có thể được thi hành 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 phương tiện lưu trữ đọc được bởi máy tính không chuyên tiếp (ví dụ, một hoặc nhiều bộ

nhớ) được ghép với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý 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 khối/các mô đun khác nhau tương ứng với các lệnh (ví dụ, các lệnh phần mềm). Theo một số phương án, hệ thống máy tính 610 có thể được đề cập dưới dạng thiết bị sinh ra nhãn kỹ thuật số dựa trên chuỗi khối. Thiết bị sinh ra nhãn kỹ thuật số dựa trên chuỗi khối có thể bao gồm mô đun thứ nhất 611 để thu thông tin thực thể của thực thể; mô đun truyền 612 để truyền thông tin thực thể tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối; mô đun thứ hai 613 để thu sự nhận dạng giao dịch được kết hợp với lưu trữ thông tin thực thể trong chuỗi khối; và mô đun sinh ra 614 để sinh ra nhãn kỹ thuật số cho thực thể được dựa trên ít nhất sự nhận dạng giao dịch.

Fig.6B minh họa sơ đồ khối của ví dụ hệ thống máy tính 620 để thi hành chứng chỉ kỹ thuật số dựa trên chuỗi khối, theo nhiều phương án khác nhau. Hệ thống 620 có thể là ví dụ về việc thi hành một hoặc nhiều thành phần (ví dụ, hệ thống chứng chỉ kỹ thuật số 118) của hệ thống 110 của Fig.1A. Phương pháp 520 có thể được thi hành bởi hệ thống máy tính 620. Hệ thống máy tính 620 có thể bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp (ví dụ, một hoặc nhiều bộ nhớ) được ghép với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh thực thi được bởi một hoặc nhiều bộ xử lý làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) để thực hiện phương pháp 520. Hệ thống máy tính 620 có thể bao gồm các khối/các mô đun khác nhau tương ứng với các lệnh (ví dụ, các lệnh phần mềm). Theo một số phương án, hệ thống máy tính 620 có thể được đề cập dưới dạng thiết bị chứng chỉ kỹ thuật số dựa trên chuỗi khối. Thiết bị chứng chỉ kỹ thuật số dựa trên chuỗi khối có thể bao gồm mô đun sinh ra thứ nhất 621 để sinh ra chứng chỉ kỹ thuật số; mô đun sinh ra thứ hai 622 để sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số; mô đun truyền 623 để truyền bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số tới một hoặc nhiều nút của chuỗi khối để lưu trữ trong chuỗi khối; mô đun thu 624 để thu sự nhận dạng giao dịch được kết hợp với lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số trong chuỗi khối; và mô đun kết hợp 625 để kết hợp nhãn kỹ thuật số với sự nhận dạng giao dịch.

Như đã thể hiện, bằng cách thu bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số và lưu trữ bản tóm tắt trong chuỗi khối, đại diện của chứng chỉ kỹ thuật số gốc có thể được duy trì an toàn và có thể truy nhập để xác minh. Giả mạo của chứng chỉ kỹ thuật số có thể bị cản trở được dựa trên các quy tắc đồng thuận chuỗi khối bao gồm cả sự băm. Đại diện bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số có thể cũng ẩn đi thông tin văn bản gốc để bảo vệ sự riêng tư. Thêm nữa, đại diện được lưu trữ chuỗi khối của chứng chỉ kỹ thuật số gốc được kết hợp với nhãn kỹ thuật số chứng thực tương ứng và sự nhận dạng giao dịch tương ứng lưu trữ mối quan hệ chứng thực. Thông qua việc truy vấn sự nhận dạng giao dịch, thông tin kết hợp có thể được trích xuất từ chuỗi khối để xác minh. Do đó, việc phát hành chứng chỉ kỹ thuật số và xác minh có thể được cung cấp với sự đảm bảo an ninh.

Các kỹ thuật được mô tả ở đây được thi hành bởi một hoặc nhiều thiết bị tính toán có mục đích đặc biệt. Các thiết bị tính toán có mục đích đặc biệt có thể là hệ thống máy tính để bàn, hệ thống máy chủ, hệ thống máy di động, các thiết bị cầm tay, các thiết bị mạng hoặc thiết bị bất kỳ khác hoặc kết hợp các thiết bị có dây và/hoặc chương trình logic để thi hành các kỹ thuật. Các thiết bị tính toán có mục đích đặc biệt có thể được thi hành như các máy tính cá nhân, các máy tính xách tay, các điện thoại cầm tay, camera điện thoại, điện thoại thông minh, trợ lý kỹ thuật số cá nhân, máy chơi phương tiện, thiết bị điều hướng, thiết bị email, máy chơi game, máy tính bảng, thiết bị đeo được hoặc kết hợp chúng. (Các) thiết bị tính toán thường được kiểm soát và phối hợp bởi hoạt động phần mềm hệ thống. Các hệ điều hành thông thường điều khiển và lập lịch quy trình máy tính để thực thi, thực hiện quản lý bộ nhớ, cung cấp hệ thống tập tin, kết nối mạng, các dịch vụ I/O, và cung cấp chức năng giao diện người dùng, như là giao diện người dùng đồ họa (“GUI” - graphical user interface), giữa những thứ khác. Các hệ thống, các thiết bị, các phương tiện lưu trữ, các mô đun, và các khối khác nhau được mô tả ở đây có thể được thi hành trong các thiết bị tính toán có mục đích đặc biệt, hoặc một hoặc nhiều chip tính toán của một hoặc nhiều thiết bị tính toán có mục đích đặc biệt. Theo một số phương án, các lệnh được mô tả ở đây có thể được thi hành 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 bao gồm phần mềm, phần cứng, hoặc sự

kết hợp của chúng. Ví dụ, máy ảo có thể bao gồm phần mềm máy ảo Ethereum (EVM - Ethereum Virtual Machine) mà cung cấp môi trường chạy thực cho các hợp đồng thông minh trong Ethereum.

Fig.7 là sơ đồ khối mà minh họa hệ thống máy tính 700 trên đó các phương án bất kỳ được mô tả ở đây có thể được thi hành. Hệ thống 700 có thể được thi hành trong hệ thống và thiết bị bất kỳ được mô tả ở đây và được tạo cấu hình để thực hiện các bước tương ứng để thi hành chứng chỉ kỹ thuật số dựa trên chuỗi khối. Hệ thống máy tính 700 bao gồm bus 702 hoặc cơ chế truyền thông khác để truyền thông thông tin, một hoặc nhiều phần cứng bộ xử lý 704 được ghép với bus 702 để xử lý thông tin. (Các) phần cứng bộ xử lý 704 có thể là, ví dụ, một hoặc nhiều bộ vi xử lý đa năng.

Hệ thống máy tính 700 cũng bao gồm bộ nhớ chính 706, như là bộ nhớ truy nhập ngẫu nhiên (RAM - random access memory), vùng nhớ đệm và/hoặc các thiết bị lưu trữ động khác, được ghép với bus 702 để lưu trữ thông tin và các lệnh thực thi được bởi (các) bộ xử lý 704. Bộ nhớ chính 706 cũng có thể được sử dụng để lưu trữ biến tạm thời hoặc thông tin trung gian khác trong khi thực thi các lệnh thực thi được bởi (các) bộ xử lý 704. Các lệnh, khi được lưu trữ trong các phương tiện lưu trữ có thể truy nhập tới (các) bộ xử lý 704, hệ thống máy tính kết xuất 700 vào một máy chuyên dùng được tùy chỉnh để thực hiện các hoạt động được chỉ định trong các lệnh. Hệ thống máy tính 700 còn bao gồm bộ nhớ chỉ đọc (ROM - Read-Only Memory) 708 hoặc thiết bị lưu trữ tĩnh khác được ghép với bus 702 để lưu trữ thông tin tĩnh và các lệnh cho (các) bộ xử lý 704. Thiết bị lưu trữ 710, như là đĩa từ, đĩa quang hoặc ổ USB (ổ Flash), v.v., được cung cấp và được ghép với bus 702 để lưu trữ thông tin và các lệnh.

Hệ thống máy tính 700 có thể thi hành các kỹ thuật được mô tả ở đây sử dụng logic có dây cứng tùy chỉnh, một hoặc nhiều ASIC hoặc FPGA, phần sụn và/hoặc chương trình logic mà kết hợp với hệ thống máy tính làm cho hoặc lập trình hệ thống máy tính 700 thành máy có mục đích đặc biệt. Theo một phương án, các hoạt động, các phương pháp, và các xử lý được mô tả ở đây được thực hiện bởi hệ thống máy tính 700 để đáp lại (các) bộ xử lý 704 thực thi một hoặc nhiều chuỗi của một hoặc nhiều lệnh được chứa trong bộ nhớ chính 706. Như các lệnh có thể được đọc vào bộ nhớ chính 706 từ phương tiện lưu trữ khác, như

là thiết bị lưu trữ 710. Việc thực thi của chuỗi các lệnh được chứa trong bộ nhớ chính 706 làm cho (các) bộ xử lý 704 thực hiện các bước xử lý được mô tả ở đây. Theo các phương án thay thế, mạch điện có dây cứng có thể được sử dụng thay thế hoặc kết hợp với các lệnh phần mềm.

Bộ nhớ chính 706, ROM 708, và/hoặc bộ lưu trữ 710 có thể bao gồm các phương tiện lưu trữ không chuyển tiếp. Thuật ngữ “các phương tiện không chuyển tiếp”, và các thuật ngữ tương tự, như được sử dụng ở đây đề cập đến các phương tiện lưu trữ dữ liệu và/hoặc các lệnh làm cho máy hoạt động theo kiểu cụ thể, phương tiện không bao gồm tín hiệu chuyển tiếp. Như phương tiện không chuyển tiếp có thể bao gồm phương tiện bất khả biến và/hoặc phương tiện khả biến. Phương tiện bất khả biến bao gồm, ví dụ, đĩa quang hoặc từ, như là thiết bị lưu trữ 710. Phương tiện khả biến bao gồm bộ nhớ động, như là bộ nhớ chính 706. Các dạng chung của phương tiện không chuyển tiếp bao gồm, ví dụ, một đĩa mềm, một đĩa linh hoạt, đĩa cứng, ổ đĩa trạng thái rắn, băng từ hoặc bất kỳ phương tiện lưu trữ dữ liệu từ tính nào khác, CD-ROM, bất kỳ phương tiện lưu trữ dữ liệu quang học nào khác, bất kỳ phương tiện vật lý nào có các mẫu lỗ, RAM, PROM và EPROM, FLASH-EPROM, NVRAM, bất kỳ chip nhớ hoặc hộp mực nào khác và các phiên bản nối mạng giống nhau.

Hệ thống máy tính 700 cũng bao gồm giao diện mạng 718 được ghép với bus 702. Giao diện mạng 718 cung cấp việc truyền thông dữ liệu hai chiều ghép với một hoặc nhiều liên kết mạng mà được kết nối với một hoặc nhiều mạng cục bộ. Ví dụ, giao diện mạng 718 có thể là thẻ mạng thuật số dịch vụ tích hợp (integrated services digital network - ISDN), modem cáp, modem vệ tinh hoặc modem để cung cấp kết nối truyền dữ liệu đến một loại đường dây điện thoại tương ứng. Một ví dụ khác, giao diện mạng 718 có thể là thẻ mạng cục bộ (LAN-Local Area Network) để cung cấp kết nối truyền dữ liệu đến mạng LAN tương thích (hoặc thành phần WAN (Wide area network) để được truyền thông với mạng LAN). Các liên kết không dây cũng có thể được thi hành. Trong bất kỳ việc thi hành nào như vậy, giao diện mạng 718 sẽ gửi và nhận các tín hiệu điện, điện từ hoặc quang mang các luồng dữ liệu số đại diện cho các loại thông tin khác nhau.

Hệ thống máy tính 700 có thể gửi các tin nhắn và dữ liệu nhận, bao gồm mã chương trình, thông qua (các) mạng, liên kết mạng và giao diện mạng 718. Trong ví dụ về Internet,

máy chủ có thể truyền mã được yêu cầu cho chương trình ứng dụng thông qua Internet, ISP, mạng cục bộ và giao diện mạng 718.

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

Mỗi thành phần trong số quy trình, phương pháp, và các thuật toán được mô tả trong các phần trước có thể được thể hiện trong, và tự động hoàn toàn hoặc một phần bởi, các mô đun mã thực thi bởi một hoặc nhiều máy tính các hệ thống hoặc các bộ xử lý máy tính bao gồm phần cứng máy tính. Các quy trình và các thuật toán có thể được thi hành một phần hoặc toàn bộ trong mạch ứng dụng cụ thể.

Các tính năng và các quy trình khác nhau được mô tả ở trên có thể được sử dụng độc lập với nhau, hoặc có thể là được kết hợp theo nhiều cách khác nhau. Tất cả các kết hợp và các kết hợp phụ có thể được dự định để nằm trong phạm vi của bản mô tả này. Ngoài ra, các khối phương pháp hoặc quy trình nhất định có thể được bỏ qua trong một số việc thi hành. Các phương pháp và các quy trình được mô tả ở đây cũng không giới hạn trong bất kỳ trình tự cụ thể, và các khối hoặc trạng thái liên quan ở đó có thể được thực hiện trong các trình tự khác phù hợp. Ví dụ, các khối và các trạng thái được mô tả có thể được thực hiện theo thứ tự khác với thứ tự được mô tả cụ thể, hoặc nhiều khối hoặc trạng thái có thể được kết hợp với khối hoặc trạng thái đơn. Các ví dụ về các khối hoặc các trạng thái có thể được thực hiện nối tiếp, song song, hoặc theo một số cách thức khác. Các khối hoặc các trạng thái có thể được bổ sung hoặc được loại bỏ khỏi các phương án của sáng chế được bộc lộ. Các ví dụ về các hệ thống và các thành phần được mô tả ở đây có thể được tạo cấu hình khác với các phương án được mô tả. Ví dụ, các thành phần có thể là được bổ sung, bị loại bỏ, hoặc được sắp xếp lại so với các phương án được bộc lộ.

Nhiều hoạt động khác nhau của các phương pháp được mô tả ở đây có thể được thực hiện, ít nhất một phần, bằng thuật toán. Thuật toán được bao gồm trong các mã chương trình hoặc các lệnh được lưu trữ trong bộ nhớ (ví dụ, phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp được mô tả ở trên). Thuật toán này có thể bao gồm thuật toán học máy. Theo một số phương án, thuật toán học máy có thể không lập trình rõ ràng các máy

tính để thực hiện chức năng, nhưng có thể học từ dữ liệu huấn luyện để tạo mô hình dự đoán thực hiện chức năng.

Nhiều hoạt động 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 mà được tạo cấu hình tạm thời (ví dụ, bởi phần mềm) hoặc được tạo cấu hình vĩnh viễn để thực hiện các hoạt động liên quan. Liệu được tạo cấu hình vĩnh viễn hoặc tạm thời, những bộ xử lý như vậy có thể tạo thành các động cơ được thi hành bởi bộ xử lý mà hoạt động để thực hiện một hoặc nhiều hoạt động hoặc chức năng được mô tả trong tài liệu này.

Tương tự, các phương pháp được mô tả ở đây có thể được thi hành ít nhất một phần bởi bộ xử lý, với bộ xử lý cụ thể hoặc các bộ xử lý là ví dụ phần cứng. Ví dụ, ít nhất một số hoạt động của phương pháp có thể là được thực hiện bởi một hoặc nhiều bộ xử lý hoặc các động cơ được thi hành bởi bộ xử lý. Hơn nữa, một hoặc nhiều bộ xử lý có thể cũng hoạt động để hỗ trợ hiệu suất của các hoạt động có liên quan trong môi trường điện toán đám mây trên nền tảng điện toán đám mây hoặc như một phần mềm trên mạng như một dịch vụ. Ví dụ, ít nhất một số hoạt động có thể được thực hiện bởi một nhóm máy tính (như ví dụ về các máy bao gồm bộ xử lý), với các hoạt động này có thể truy cập qua mạng (ví dụ, Internet) và qua một hoặc nhiều giao diện thích hợp (ví dụ, Giao diện chương trình ứng dụng (API)).

Hiệu năng của một số hoạt động có thể được phân phối giữa các bộ xử lý, không chỉ nằm trong một máy mà còn được triển khai trên một số máy. Theo một số phương án, các bộ xử lý hoặc các động cơ được thi hành bởi bộ xử lý có thể được định vị ở một vị trí địa lý (ví dụ, trong môi trường gia đình, môi trường văn phòng hoặc trang trại máy chủ). Theo các phương án khác, các bộ xử lý hoặc các động cơ được thi hành bởi bộ xử lý có thể được phân phối trên một số vị trí địa lý.

Trong toàn bộ bản mô tả này, trường hợp số nhiều có thể thi hành các thành phần, hoạt động hoặc cấu trúc được mô tả như trường hợp số ít. Mặc dù các hoạt động cá nhân của một hoặc nhiều phương pháp được minh họa và mô tả như các hoạt động riêng biệt, một hoặc nhiều hoạt động cá nhân có thể được thực hiện đồng thời, và không có gì đòi hỏi các thao tác phải được thực hiện theo thứ tự minh họa. Các cấu trúc và chức năng được

trình bày dưới dạng các thành phần riêng biệt trong cấu hình có thể được thi thành dưới dạng cấu trúc hoặc thành phần kết hợp. Tương tự, các cấu trúc và chức năng được trình bày dưới dạng một thành phần có thể được thi hành như các thành phần riêng biệt. Các biến thể, sửa đổi, bổ sung và cải tiến này và các biến thể, sửa đổi, bổ sung và cải tiến khác nằm trong phạm vi của sáng chế này.

Mặc dù tổng quan về vấn đề đã được mô tả với tham chiếu đến các phương án cụ thể, các sửa đổi và thay đổi khác nhau có thể được thực hiện cho các phương án này mà không vượt quá phạm vi của sáng chế này. Phần mô tả chi tiết không nên được thực hiện theo nghĩa hạn chế, và phạm vi của các phương án khác nhau chỉ được xác định bởi yêu cầu bảo hộ đã được sửa đổi, cùng với đầy đủ các loại tương đương mà các yêu cầu bảo hộ này được hưởng quyền. Hơn nữa, các thuật ngữ liên quan (như là “thứ nhất”, “thứ hai”, “thứ ba”, v.v.) được sử dụng ở đây không biểu thị bất kỳ thứ tự, chiều cao hoặc tầm quan trọng nào, mà được sử dụng để phân biệt một yếu tố này với yếu tố khác. Hơn nữa, các thuật ngữ “một”, “cái”, và “nhiều” không có nghĩa là giới hạn số lượng ở đây, mà biểu thị sự hiện diện của ít nhất một hạng mục được đề cập.

YÊU CẦU BẢO HỘ

1. Phương pháp được thi hành bởi máy tính để thi hành các chứng chỉ kỹ thuật số, phương pháp này bao gồm các bước:

lưu trữ thông tin thực thể của thực thể vào chuỗi khối bằng cách truyền giao dịch chuỗi khối thứ nhất bao gồm thông tin thực thể đến một hoặc nhiều nút chuỗi khối để lưu trữ giao dịch chuỗi khối thứ nhất vào chuỗi khối qua sự xác minh đồng thuận;

sinh ra nhãn kỹ thuật số dựa trên sự nhận dạng giao dịch thứ nhất của giao dịch chuỗi khối thứ nhất được lưu trữ vào chuỗi khối;

sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số bằng cách băm chứng chỉ kỹ thuật số;

lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số vào chuỗi khối bằng cách truyền giao dịch chuỗi khối thứ hai bao gồm bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số đến một hoặc nhiều nút chuỗi khối để lưu trữ giao dịch chuỗi khối thứ hai vào chuỗi khối qua sự xác minh đồng thuận;

tạo ra mối quan hệ kết hợp giữa nhãn kỹ thuật số, bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số, và sự nhận dạng giao dịch thứ hai của giao dịch chuỗi khối thứ hai được lưu trữ vào chuỗi khối;

sinh ra giao dịch chuỗi khối thứ ba bao gồm mối quan hệ kết hợp; và

thiết lập bằng chứng của sự chứng thực của thực thể của chứng chỉ kỹ thuật số bằng cách truyền giao dịch chuỗi khối thứ ba đến một hoặc nhiều nút chuỗi khối để lưu trữ giao dịch chuỗi khối thứ ba vào chuỗi khối qua sự xác minh đồng thuận, trong đó bằng chứng là truy vấn được qua sự nhận dạng giao dịch thứ ba của giao dịch chuỗi khối thứ ba được lưu trữ vào chuỗi khối, và giao dịch chuỗi khối thứ ba được lưu trữ vào chuỗi khối liên kết thực thể và chứng chỉ kỹ thuật số mà không lưu trữ văn bản gốc của chứng chỉ kỹ thuật số vào chuỗi khối.

2. Phương pháp theo điểm 1, trong đó:

nhân kỹ thuật số bao gồm ít nhất một thành phần trong số dấu kỹ thuật số hoặc chữ ký kỹ thuật số.

3. Phương pháp theo điểm 1, trong đó giao dịch chuỗi khối thứ hai còn bao gồm:

thông tin của quy trình mật mã được sử dụng để sinh ra bản tóm tắt kỹ thuật số.

4. Phương pháp theo điểm 3, trong đó:

quy trình mật mã là việc băm SHA-256.

5. Phương pháp theo điểm 1, trong đó:

bản tóm tắt kỹ thuật số bao gồm giá trị băm của chứng chỉ kỹ thuật số;

sự nhận dạng giao dịch thứ nhất bao gồm giá trị băm của giao dịch chuỗi khối thứ nhất;

sự nhận dạng giao dịch thứ hai bao gồm giá trị băm của giao dịch chuỗi khối thứ hai; và

sự nhận dạng giao dịch thứ ba bao gồm giá trị băm của giao dịch chuỗi khối thứ ba.

6. Phương pháp theo điểm 1, trước khi sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số, phương pháp này còn bao gồm các bước:

thu các nội dung của chứng chỉ kỹ thuật số từ thực thể; và

sinh ra chứng chỉ kỹ thuật số bao gồm các nội dung.

7. Phương pháp theo điểm 1, trong đó:

chuỗi khối là chuỗi khối liên doanh.

8. Hệ thống chứng chỉ kỹ thuật số bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ được đọc bởi máy tính không chuyển tiếp được ghép với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh có thể thực thi được bởi một hoặc nhiều bộ xử lý để làm cho hệ thống thực hiện các hoạt động bao gồm:

lưu trữ thông tin thực thể của thực thể vào chuỗi khối bằng cách truyền giao dịch chuỗi khối thứ nhất bao gồm thông tin thực thể đến một hoặc nhiều nút chuỗi khối để lưu trữ giao dịch chuỗi khối thứ nhất vào chuỗi khối qua sự xác minh đồng thuận;

sinh ra nhãn kỹ thuật số dựa trên sự nhận dạng giao dịch thứ nhất của giao dịch chuỗi khối thứ nhất được lưu trữ vào chuỗi khối;

sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số bằng cách băm chứng chỉ kỹ thuật số;

lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số vào chuỗi khối bằng cách truyền giao dịch chuỗi khối thứ hai bao gồm bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số đến một hoặc nhiều nút chuỗi khối để lưu trữ giao dịch chuỗi khối thứ hai vào chuỗi khối qua sự xác minh đồng thuận;

tạo ra mối quan hệ kết hợp giữa nhãn kỹ thuật số, bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số, và sự nhận dạng giao dịch thứ hai của giao dịch chuỗi khối thứ hai được lưu trữ vào chuỗi khối;

sinh ra giao dịch chuỗi khối thứ ba bao gồm mối quan hệ kết hợp; và

thiết lập bằng chứng của sự chứng thực của thực thể của chứng chỉ kỹ thuật số bằng cách truyền giao dịch chuỗi khối thứ ba đến một hoặc nhiều nút chuỗi khối để lưu trữ giao dịch chuỗi khối thứ ba vào chuỗi khối qua sự xác minh đồng thuận, trong đó bằng chứng là truy vấn được qua sự nhận dạng giao dịch thứ ba của giao dịch chuỗi khối thứ ba được lưu trữ vào chuỗi khối, và giao dịch chuỗi khối thứ ba được lưu trữ vào chuỗi khối liên kết thực thể và chứng chỉ kỹ thuật số mà không lưu trữ văn bản gốc của chứng chỉ kỹ thuật số vào chuỗi khối.

9. Hệ thống theo điểm 8, trong đó:

nhãn kỹ thuật số bao gồm ít nhất một thành phần trong số dấu kỹ thuật số hoặc chữ ký kỹ thuật số.

10. Hệ thống theo điểm 8, trong đó giao dịch chuỗi khối thứ hai còn bao gồm:

thông tin của quy trình mật mã được sử dụng để sinh ra bản tóm tắt kỹ thuật số.

11. Hệ thống theo điểm 10, trong đó:

quy trình mật mã là việc băm SHA-256.

12. Hệ thống theo điểm 8, trong đó trước khi sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số, các hoạt động còn bao gồm:

thu các nội dung của chứng chỉ kỹ thuật số từ thực thể; và

sinh ra chứng chỉ kỹ thuật số bao gồm các nội dung.

13. Hệ thống theo điểm 8, trong đó:

bản tóm tắt kỹ thuật số bao gồm giá trị băm của chứng chỉ kỹ thuật số;

sự nhận dạng giao dịch thứ nhất bao gồm giá trị băm của giao dịch chuỗi khối thứ nhất;

sự nhận dạng giao dịch thứ hai bao gồm giá trị băm của giao dịch chuỗi khối thứ hai; và

sự nhận dạng giao dịch thứ ba bao gồm giá trị băm của giao dịch chuỗi khối thứ ba.

14. Phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp được tạo cấu hình với các lệnh có thể thực thi được bởi một hoặc nhiều bộ xử lý để làm cho một hoặc nhiều bộ xử lý thực hiện các hoạt động bao gồm:

lưu trữ thông tin thực thể của thực thể vào chuỗi khối bằng cách truyền giao dịch chuỗi khối thứ nhất bao gồm thông tin thực thể đến một hoặc nhiều nút chuỗi khối để lưu trữ giao dịch chuỗi khối thứ nhất vào chuỗi khối qua sự xác minh đồng thuận;

sinh ra nhãn kỹ thuật số dựa trên sự nhận dạng giao dịch thứ nhất của giao dịch chuỗi khối thứ nhất được lưu trữ vào chuỗi khối;

sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số bằng cách băm chứng chỉ kỹ thuật số;

lưu trữ bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số vào chuỗi khối bằng cách truyền giao dịch chuỗi khối thứ hai bao gồm bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật

số đến một hoặc nhiều nút chuỗi khối để lưu trữ giao dịch chuỗi khối thứ hai vào chuỗi khối qua sự xác minh đồng thuận;

tạo ra mối quan hệ kết hợp giữa nhãn kỹ thuật số, bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số, và sự nhận dạng giao dịch thứ hai của giao dịch chuỗi khối thứ hai được lưu trữ vào chuỗi khối;

sinh ra giao dịch chuỗi khối thứ ba bao gồm mối quan hệ kết hợp; và

thiết lập bằng chứng của sự chứng thực của thực thể của chứng chỉ kỹ thuật số bằng cách truyền giao dịch chuỗi khối thứ ba đến một hoặc nhiều nút chuỗi khối để lưu trữ giao dịch chuỗi khối thứ ba vào chuỗi khối qua sự xác minh đồng thuận, trong đó bằng chứng là truy vấn được qua sự nhận dạng giao dịch thứ ba của giao dịch chuỗi khối thứ ba được lưu trữ vào chuỗi khối, và giao dịch chuỗi khối thứ ba được lưu trữ vào chuỗi khối liên kết thực thể và chứng chỉ kỹ thuật số mà không lưu trữ văn bản gốc của chứng chỉ kỹ thuật số vào chuỗi khối.

15. Phương tiện lưu trữ theo điểm 14, trong đó:

nhãn kỹ thuật số bao gồm ít nhất một thành phần trong số dấu kỹ thuật số hoặc chữ ký kỹ thuật số.

16. Phương tiện lưu trữ theo điểm 14, trong đó giao dịch chuỗi khối thứ hai còn bao gồm:

thông tin của quy trình mật mã được sử dụng để sinh ra bản tóm tắt kỹ thuật số.

17. Phương tiện lưu trữ theo điểm 16, trong đó:

quy trình mật mã là việc băm SHA-256.

18. Phương tiện lưu trữ theo điểm 14, trong đó:

bản tóm tắt kỹ thuật số bao gồm giá trị băm của chứng chỉ kỹ thuật số;

sự nhận dạng giao dịch thứ nhất bao gồm giá trị băm của giao dịch chuỗi khối thứ nhất;

sự nhận dạng giao dịch thứ hai bao gồm giá trị băm của giao dịch chuỗi khối thứ hai; và

sự nhận dạng giao dịch thứ ba bao gồm giá trị băm của giao dịch chuỗi khối thứ ba.

19. Phương tiện lưu trữ theo điểm 14, trong đó trước khi sinh ra bản tóm tắt kỹ thuật số của chứng chỉ kỹ thuật số, các hoạt động còn bao gồm:

thu các nội dung của chứng chỉ kỹ thuật số từ thực thể; và
sinh ra chứng chỉ kỹ thuật số bao gồm các nội dung.

20. Phương tiện lưu trữ theo điểm 14, trong đó:

chuỗi khối là chuỗi khối liên doanh.

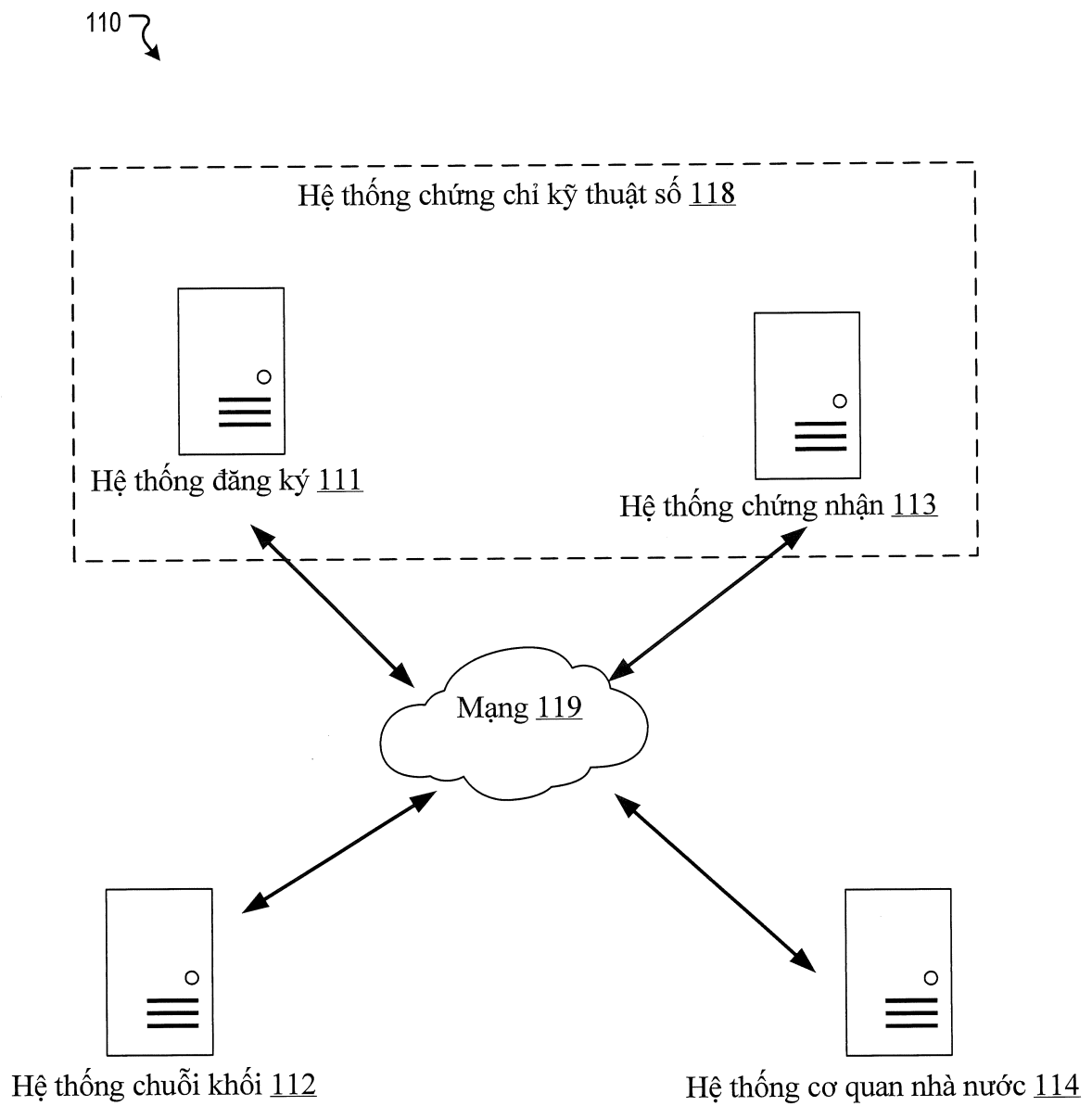


FIG. 1A

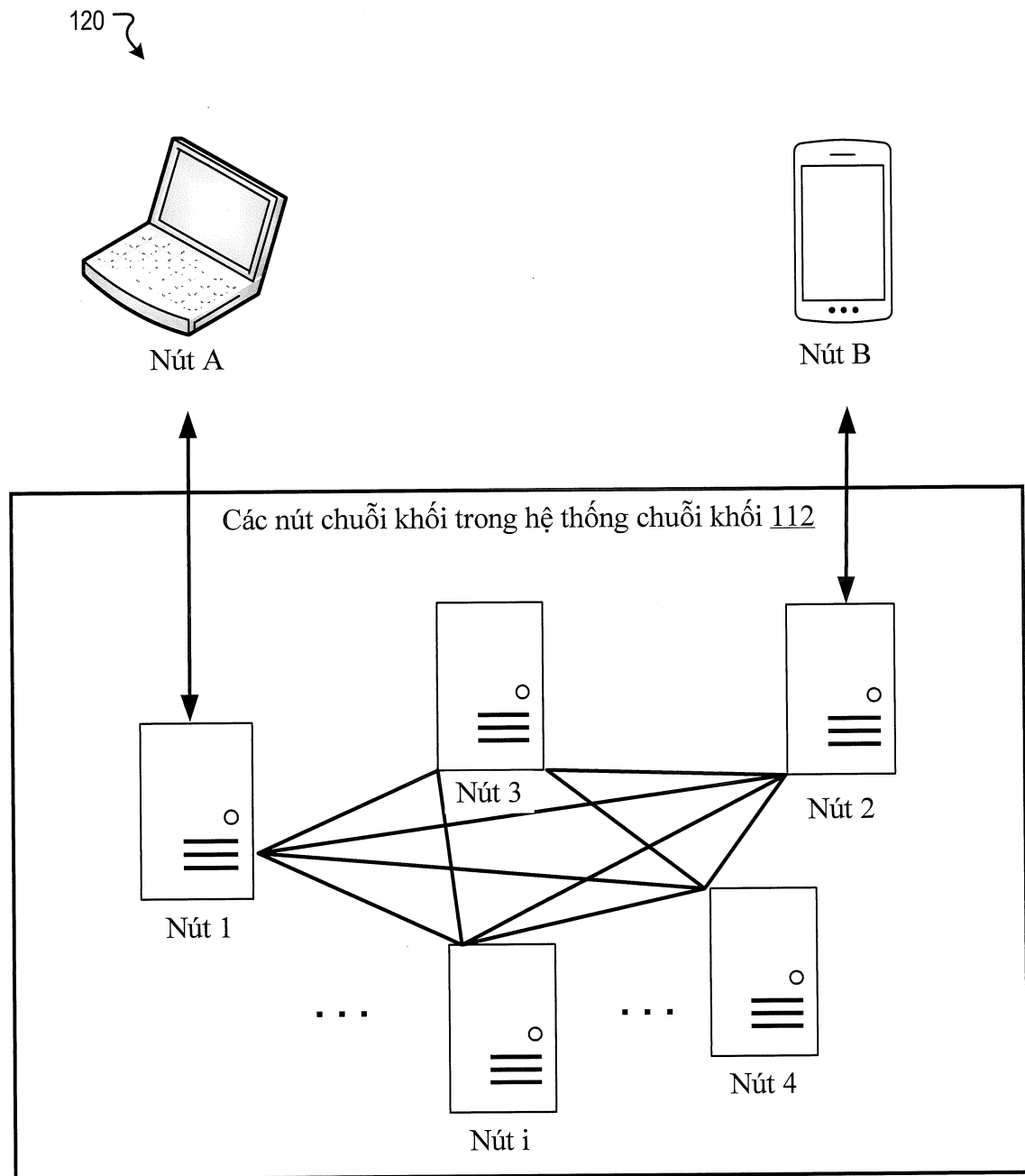


FIG. 1B

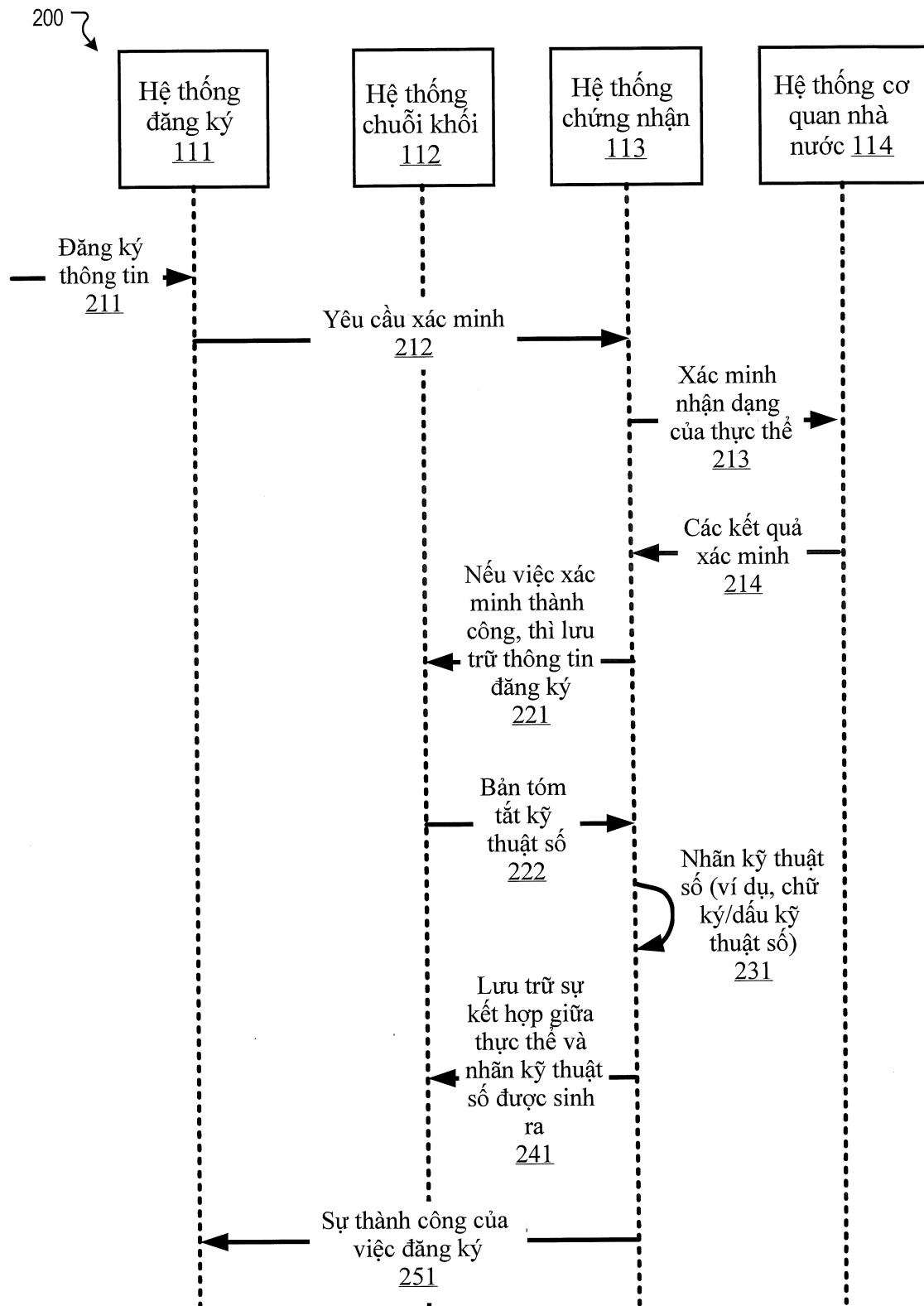


FIG. 2

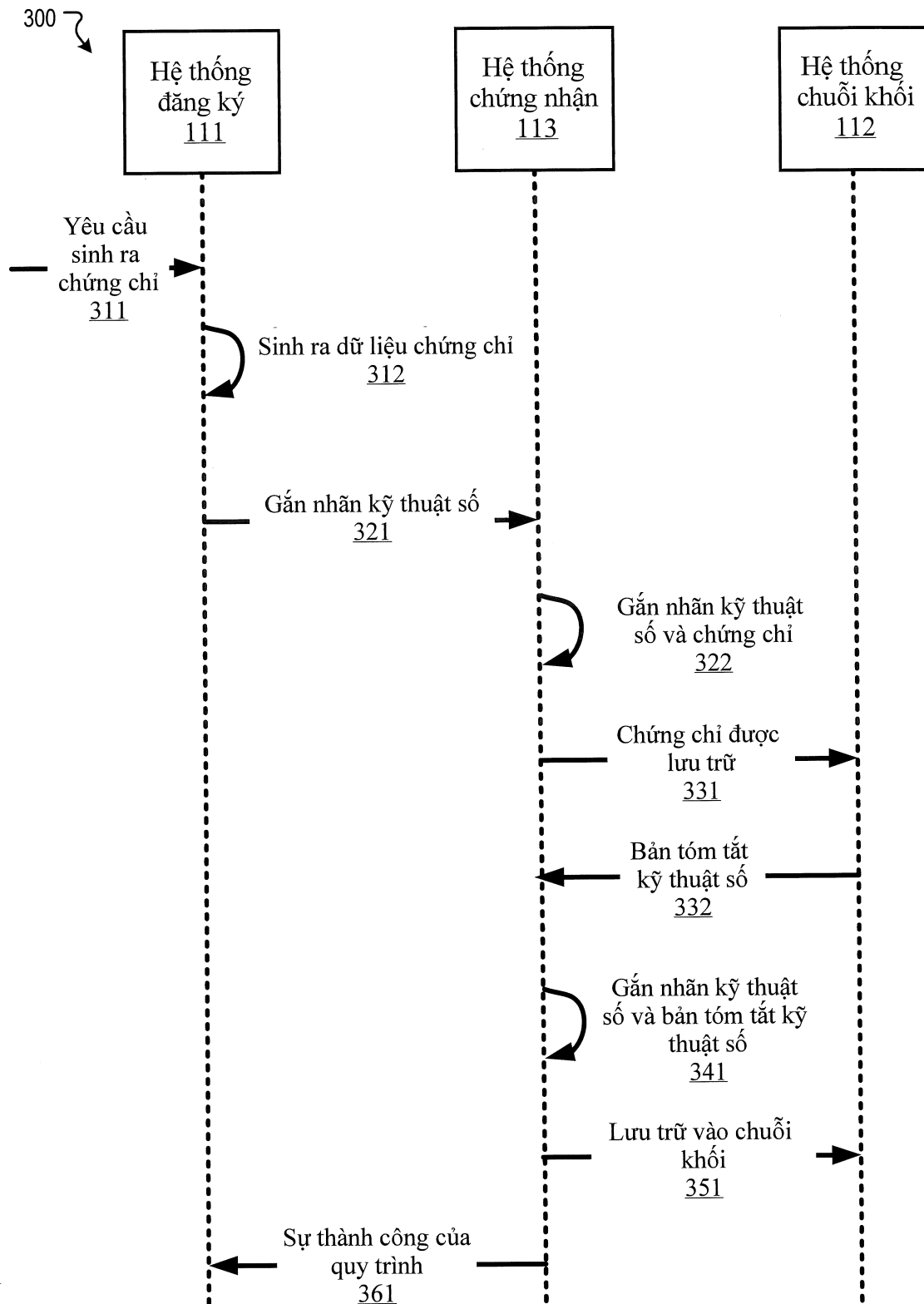


FIG. 3

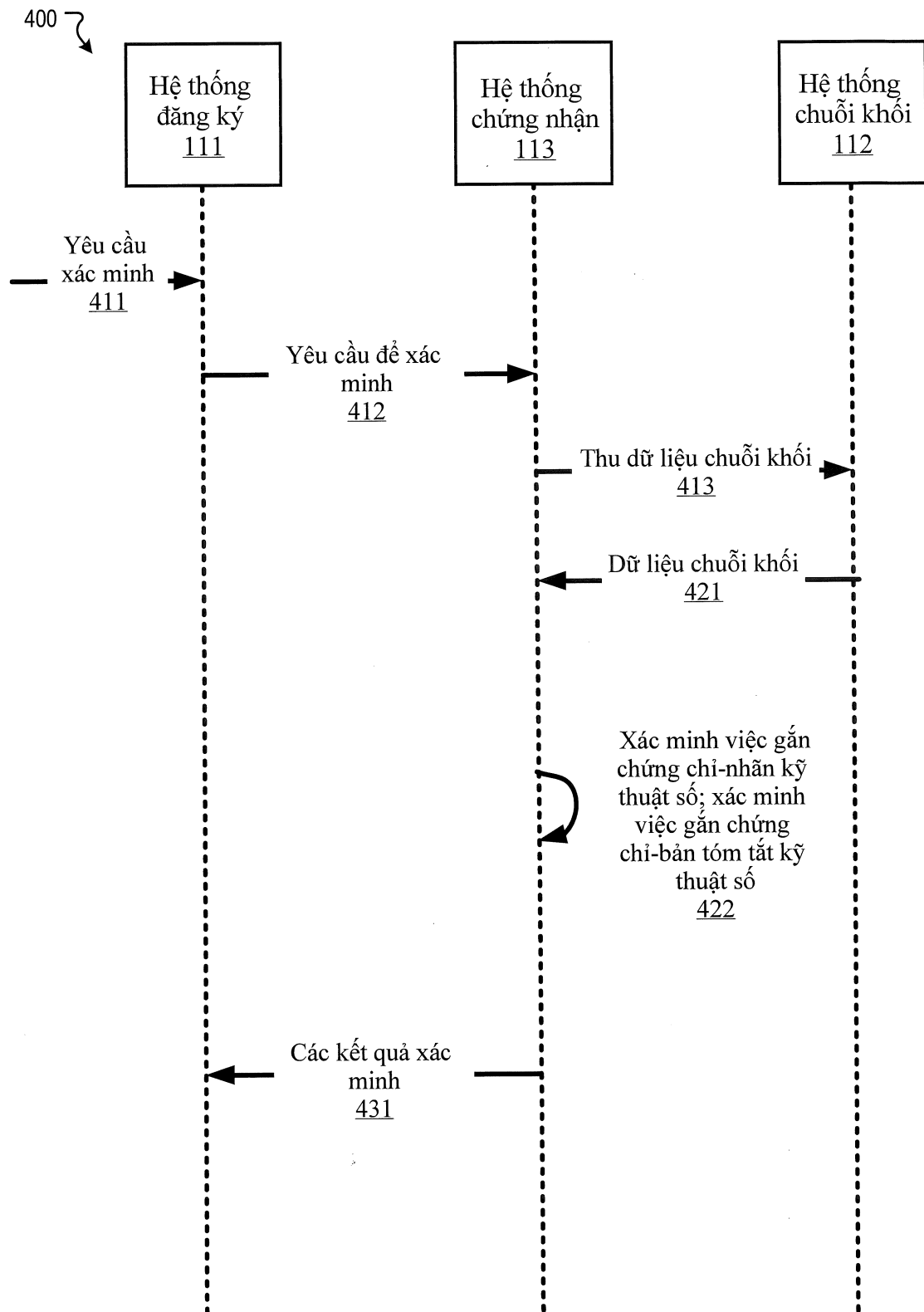


FIG. 4

510 ↘

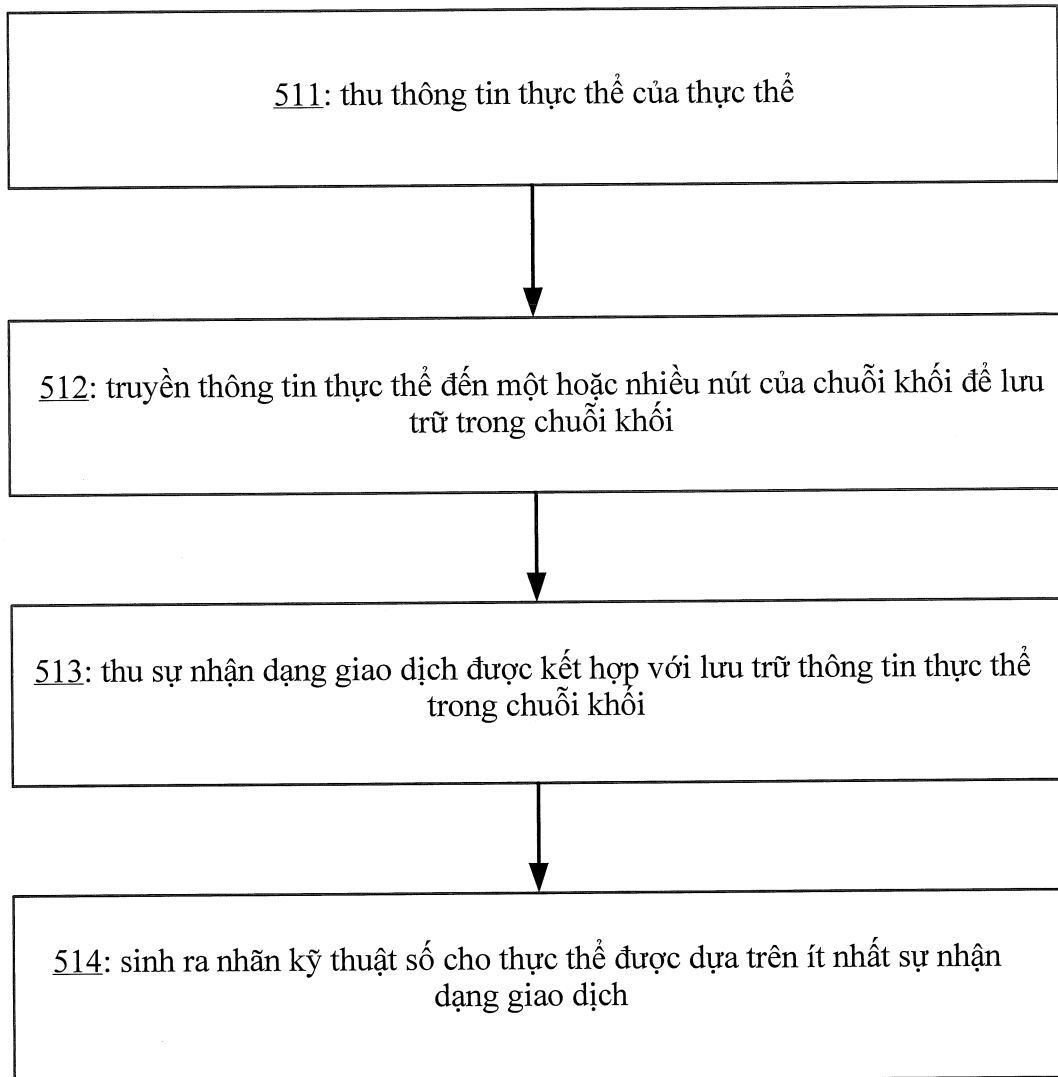


FIG. 5A

520 ↗

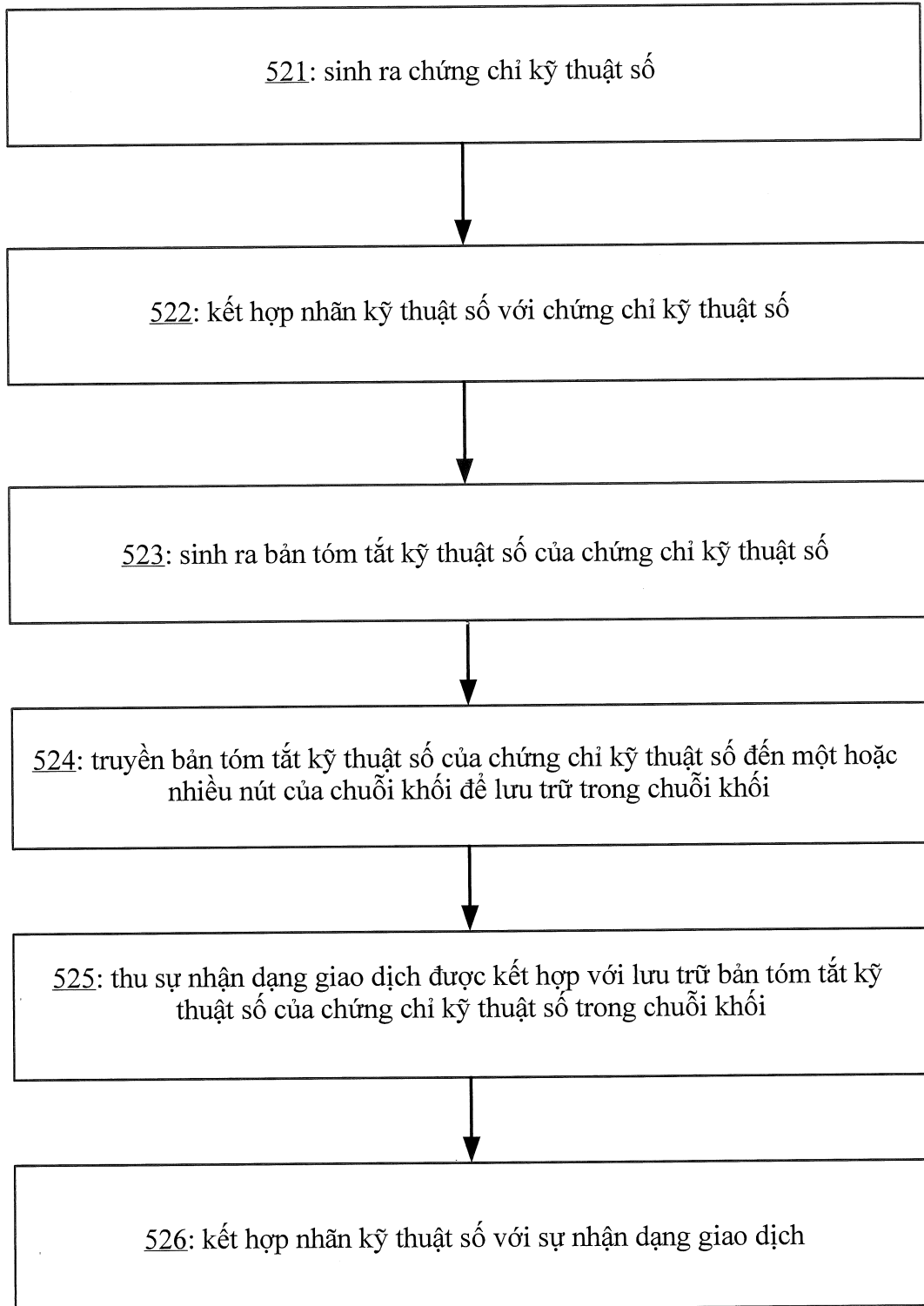


FIG. 5B

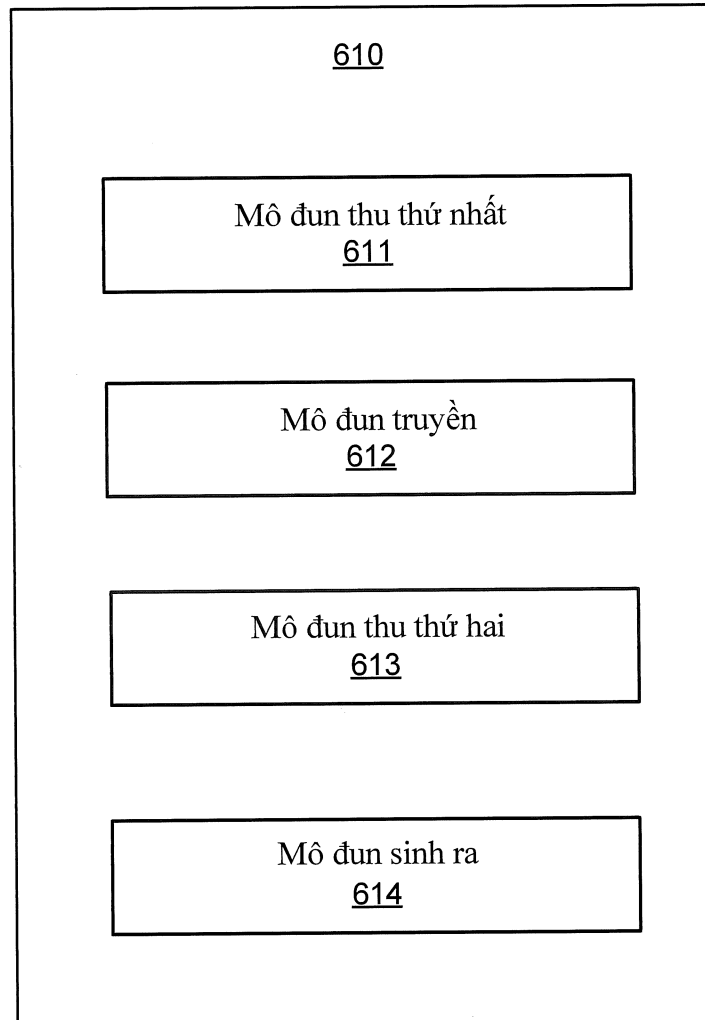
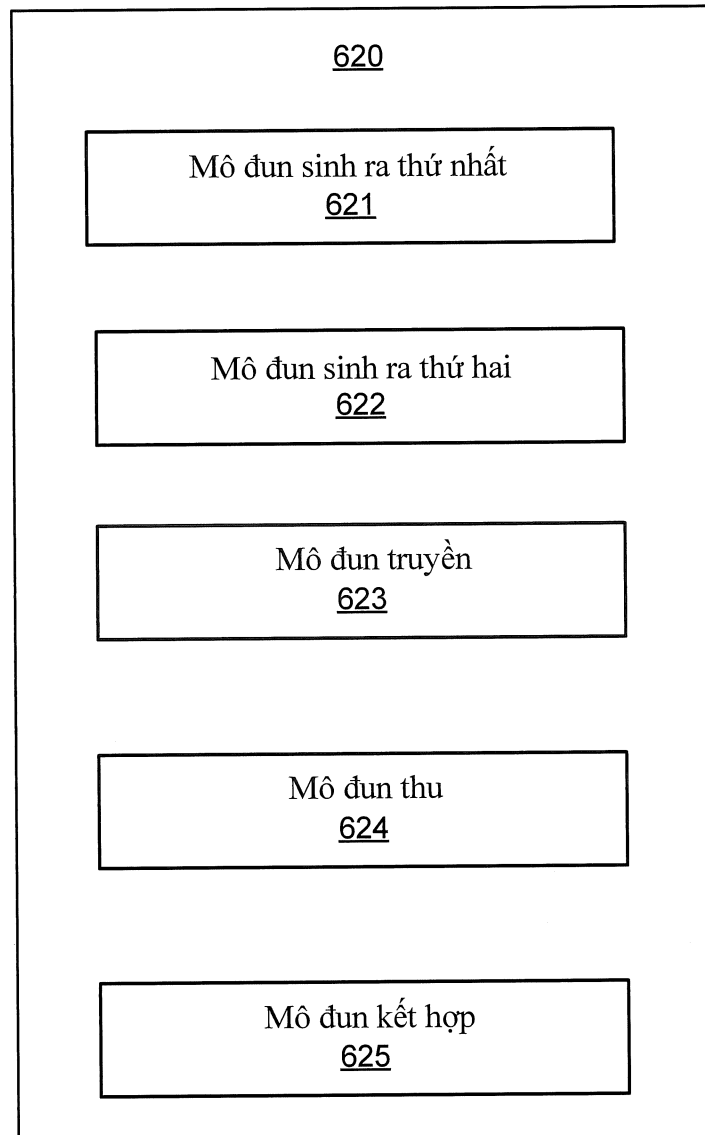


FIG. 6A

**FIG. 6B**

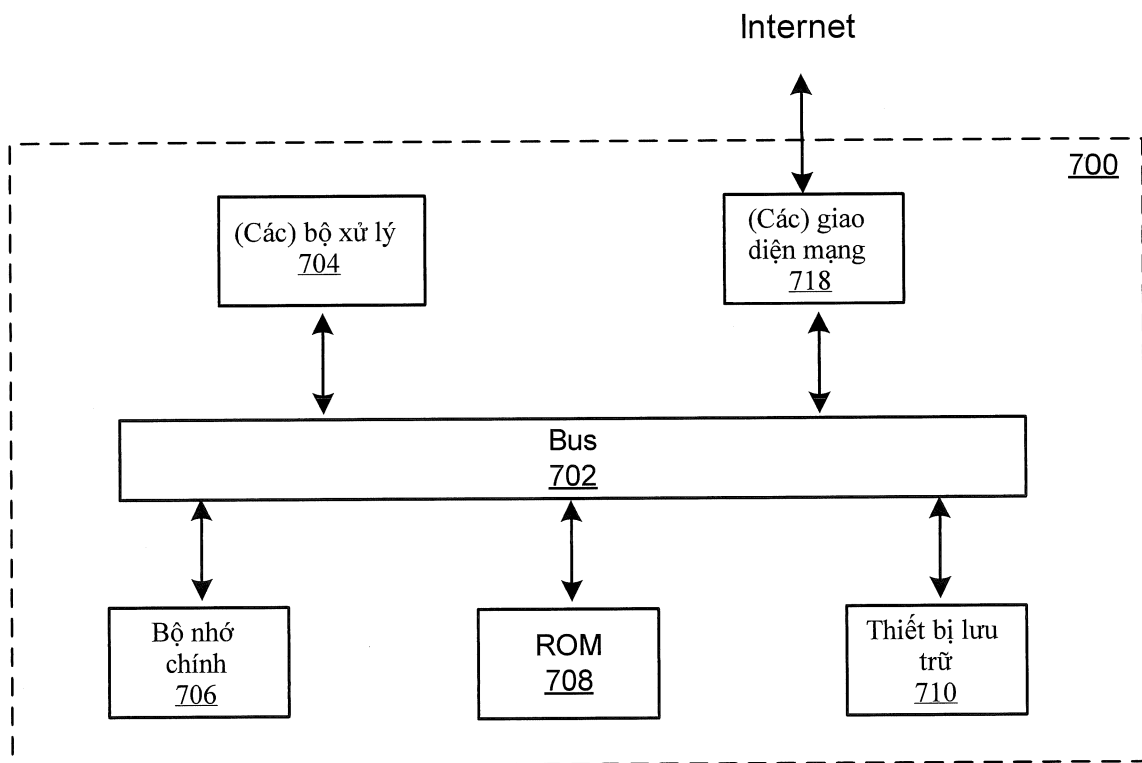


FIG. 7