



(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)



1-0037134

(51)⁷ H04L 9/00

(13) B

(21) 1-2019-03550

(22) 01/02/2019

(86) PCT/CN2019/074436 01/02/2019

(87) WO2019/072318 18/04/2019

(45) 25/10/2023 427

(43) 25/09/2019 378A

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

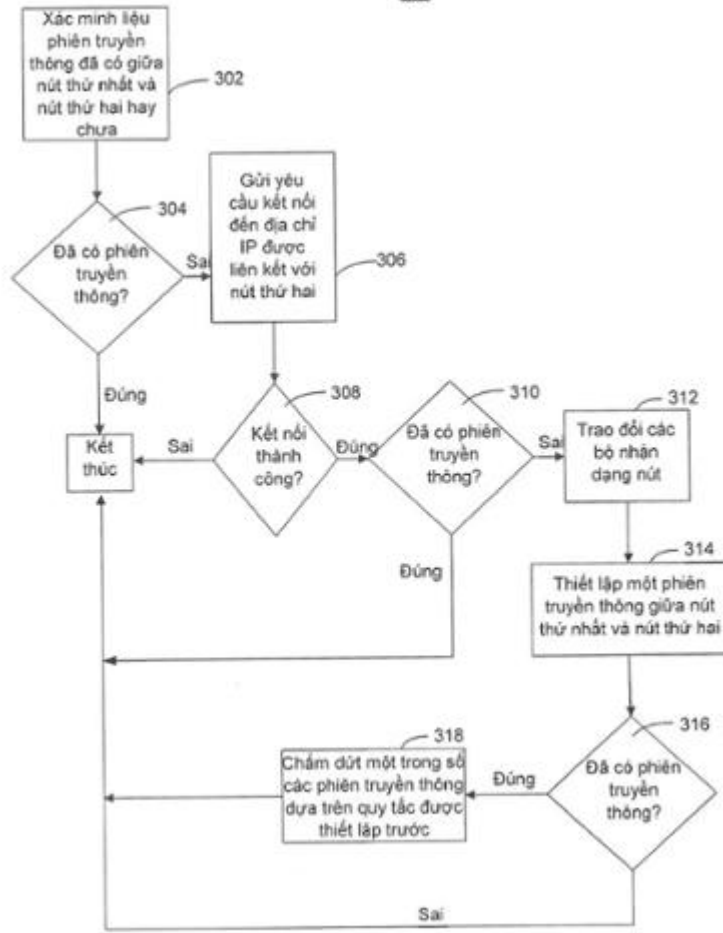
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands

(72) QI, Yitong (CN); WANG, Jiang (CN).

(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ ĐỂ THIẾT LẬP VIỆC TRUYỀN THÔNG GIỮA CÁC NÚT TRONG HỆ THỐNG CHUỖI KHỐI

(57) Sáng chế đề cập đến các phương pháp, thiết bị, và máy, bao gồm các chương trình máy tính được lưu trữ trên phương tiện đọc được bằng máy tính, để thiết lập việc truyền thông giữa nút thứ nhất và nút thứ hai trong hệ thống chuỗi khối (blockchain). Một trong số các phương pháp này bao gồm các bước: nút thứ nhất cung cấp bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận bộ nhận dạng nút của nút thứ hai từ nút thứ hai, để khiến cho phiên truyền thông thứ nhất được thiết lập giữa nút thứ nhất và nút thứ hai; nút thứ nhất xác định liệu có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai hay không; và đáp lại việc xác định rằng có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai, chấm dứt một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai dựa trên bộ nhận dạng nút của nút thứ nhất và bộ nhận dạng nút của nút thứ hai.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập chung đến các công nghệ máy tính, và cụ thể hơn, sáng chế đề cập đến các phương pháp và thiết bị để thiết lập truyền thông giữa các nút trong hệ thống chuỗi khối (blockchain).

Tình trạng kỹ thuật của sáng chế

Các hệ thống chuỗi khối, cũng được biết đến là các hệ thống sổ cái phân tán (distributed ledger system, DLS) hoặc các hệ thống đồng thuận, có thể cho phép các thực thể tham gia lưu trữ dữ liệu theo cách bảo mật và bất biến. Các hệ thống chuỗi khối có thể bao gồm các DLS bất kỳ, mà không tham chiếu trường hợp sử dụng cụ thể bất kỳ, và có thể được sử dụng cho các mạng chuỗi khối chung, riêng, và liên doanh. Mạng chuỗi khối chung để mở cho tất cả các thực thể sử dụng hệ thống và tham gia vào quy trình đồng thuận. Mạng chuỗi khối riêng được cung cấp cho thực thể cụ thể, mà nó điều khiển tập trung việc cho phép đọc và ghi. Mạng chuỗi khối liên doanh được cung cấp cho một nhóm thực thể có lựa chọn, mà chúng điều khiển quy trình đồng thuận, và bao gồm lớp điều khiển truy cập.

Hệ thống chuỗi khối duy trì một hoặc nhiều chuỗi khối. Chuỗi khối là cấu trúc dữ liệu để lưu trữ dữ liệu, chẳng hạn như các giao dịch, mà nó có thể ngăn chặn sự can thiệp và thao túng dữ liệu bởi các bên có ác ý.

Hệ thống chuỗi khối được thi hành nhờ sử dụng mạng đồng cấp (peer-to-peer, P2P), trong đó các nút truyền thông trực tiếp với nhau, ví dụ, không cần máy chủ trung tâm, cố định. Mỗi nút trong mạng P2P có thể khởi tạo việc truyền thông với một nút khác trong mạng P2P.

Trong một hệ thống như vậy, hai nút, nút A và nút B, trong mạng P2P đều có thể gửi các yêu cầu kết nối đến nhau để khởi tạo việc truyền thông. Nếu cả hai yêu cầu kết nối đều được xử lý, mạng tạo thành sẽ chứa hai kết nối thừa được thiết lập giữa nút A và nút B. Trong một hệ thống khác kiểu như vậy, chỉ nút với bộ nhận dạng nút lớn hơn giữa hai nút được phép gửi yêu cầu kết nối. Nếu nút với bộ nhận dạng nút nhỏ hơn không

được phép chấp nhận yêu cầu kết nối bất kỳ, ví dụ, vì các lý do bảo mật, thì không có hoạt động truyền thông nào có thể được thiết lập giữa hai nút này.

Bản chất kỹ thuật của sáng chế

Theo một khía cạnh, phương pháp được thi hành bằng máy tính để thiết lập việc truyền thông giữa nút thứ nhất và nút thứ hai trong hệ thống chuỗi khối bao gồm các bước: cung cấp, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ hai từ nút thứ hai, để khiến cho phiên truyền thông thứ nhất được thiết lập giữa nút thứ nhất và nút thứ hai; xác định, bởi nút thứ nhất, liệu có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai hay không; và đáp lại việc xác định rằng có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai, chấm dứt, bởi nút thứ nhất, một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai dựa trên bộ nhận dạng nút của nút thứ nhất và bộ nhận dạng nút của nút thứ hai.

Theo một khía cạnh khác, thiết bị tính toán để thi hành nút thứ nhất trong hệ thống chuỗi khối bao gồm: một hoặc nhiều bộ xử lý; và một hoặc nhiều bộ nhớ đọc được bằng máy tính được ghép nối với một hoặc nhiều bộ xử lý này và có các lệnh được lưu trữ trên đó. Các lệnh này có thể thực thi được bởi một hoặc nhiều bộ xử lý này để: cung cấp bộ nhận dạng nút của nút thứ nhất cho nút thứ hai trong hệ thống chuỗi khối và nhận bộ nhận dạng nút của nút thứ hai từ nút thứ hai, để khiến cho phiên truyền thông thứ nhất được thiết lập giữa nút thứ nhất và nút thứ hai; xác định liệu có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai hay không; và đáp lại việc xác định rằng có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai, chấm dứt một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai dựa trên bộ nhận dạng nút của nút thứ nhất và bộ nhận dạng nút của nút thứ hai.

Theo một khía cạnh khác nữa, phương tiện phi chuyên tiếp đọc được bằng máy tính lưu trữ trong đó các lệnh để, khi được thực thi bởi bộ xử lý của thiết bị tính toán, khiến cho thiết bị tính toán này thực hiện phương pháp để thiết lập việc truyền thông giữa nút thứ nhất và nút thứ hai trong hệ thống chuỗi khối. Phương pháp này bao gồm các bước: cung cấp, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ hai từ nút thứ hai, để khiến cho phiên truyền thông thứ nhất được thiết lập giữa nút thứ nhất và nút thứ hai; xác định,

bởi nút thứ nhất, liệu có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai hay không; và đáp lại việc xác định rằng có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai, chấm dứt, bởi nút thứ nhất, một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai dựa trên bộ nhận dạng nút của nút thứ nhất và bộ nhận dạng nút của nút thứ hai.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo, mà chúng kết hợp và cấu thành nên một phần của bản mô tả này, minh họa các phương án. Trong phần mô tả sau đây, mà nó sẽ tham chiếu đến các hình vẽ, các số chỉ dẫn giống nhau trong các hình vẽ khác nhau thể hiện các thành phần giống hoặc tương tự nhau trừ khi được thể hiện khác.

Fig.1 là sơ đồ giản lược của hệ thống chuỗi khối, theo một phương án.

Fig.2 là sơ đồ giản lược của thiết bị tính toán để thi hành nút trong hệ thống chuỗi khối, theo một phương án.

Fig.3 là lưu đồ của phương pháp để thiết lập việc truyền thông giữa các nút thứ nhất và thứ hai trong hệ thống chuỗi khối, theo một phương án.

Fig.4 là lưu đồ của phương pháp để thiết lập việc truyền thông giữa các nút thứ nhất và thứ hai trong hệ thống chuỗi khối, theo một phương án.

Fig.5 là sơ đồ giản lược của hệ thống chuỗi khối, theo một phương án.

Fig.6 là sơ đồ khối của máy để thiết lập việc truyền thông giữa các nút thứ nhất và thứ hai trong hệ thống chuỗi khối, theo một phương án.

Mô tả chi tiết sáng chế

Các phương án của sáng chế đề xuất các phương pháp và các thiết bị để thiết lập việc truyền thông giữa nút thứ nhất và nút thứ hai trong hệ thống chuỗi khối. Các phương pháp và các thiết bị này cho phép mỗi nút trong số nút thứ nhất và nút thứ hai gửi yêu cầu kết nối để thiết lập phiên truyền thông giữa nút thứ nhất và nút thứ hai. Sau đó, các phương pháp và các thiết bị này kiểm tra xem liệu có nhiều hơn một phiên truyền thông đã được thiết lập giữa nút thứ nhất và nút thứ hai hay không và, nếu đúng như vậy thì có thể chấm dứt phiên truyền thông thừa và kết nối mà phiên truyền thông thừa này được thiết lập trên đó dựa trên các bộ nhận dạng nút của các nút thứ nhất và thứ hai.

Các phương án được bộc lộ trong bản mô tả này có một hoặc nhiều hiệu quả kỹ thuật sau. Theo một số phương án, các phương pháp và các thiết bị này cung cấp cho

mọi nút trong hệ thống chuỗi khối khả năng yêu cầu kết nối. Điều này cho phép sự linh hoạt và ngăn chặn sự thiếu hụt có thể xảy ra trong các điều kiện nhất định, ví dụ, khi nút không đáp ứng quy tắc được thiết lập trước nhất định, qua đó được ngăn không cho yêu cầu kết nối với một nút khác. Theo các phương án khác, các phương pháp và các thiết bị này cung cấp các khả năng kiểm tra xem liệu có nhiều hơn một phiên truyền thông đã được thiết lập giữa một cặp nút đã cho trong hệ thống chuỗi khối hay không. Điều này cho phép hệ thống chuỗi khối tránh được việc thiết lập các kết nối dư thừa giữa các nút, qua đó tiết kiệm các tài nguyên tính toán và, đồng thời, tạo thuận lợi cho việc truyền thông giữa các nút trong môi trường bảo mật. Theo các phương án khác nữa, môi trường bảo mật như vậy thỏa mãn các yêu cầu nhất định, ví dụ, nơi mà các nút nhất định chỉ được phép yêu cầu kết nối và được đòi hỏi phải từ chối tất cả các yêu cầu kết nối nhận được vì lý do bảo mật. Theo các phương án khác nữa, các phương pháp và các thiết bị này cung cấp các khả năng để nhận dạng các nút trong hệ thống chuỗi khối mà không sử dụng các địa chỉ IP của chúng. Điều này cho phép mỗi địa chỉ IP được sử dụng để hỗ trợ nhiều hơn một nút, qua đó cải thiện sự linh hoạt của hệ thống. Trên thực tế, việc cho phép một địa chỉ IP hỗ trợ nhiều hơn một nút cho phép một thiết bị tính toán làm chủ (host) nhiều hơn một nút, qua đó làm giảm chi phí phần cứng để thi hành hệ thống chuỗi khối.

Phần mô tả sau đây cung cấp nội dung chi tiết của các phương án. Theo các phương án này, chuỗi khối là cấu trúc dữ liệu để lưu trữ dữ liệu, ví dụ, các giao dịch, theo cách mà các giao dịch này có thể không thay đổi được và sau đó có thể được xác minh. Chuỗi khối bao gồm một hoặc nhiều khối. Mỗi khối được liên kết với khối trước đó ở ngay trước nó trong chuỗi khối nhờ bao gồm việc băm mật mã khối trước đó này. Mỗi khối cũng có thể bao gồm nhãn thời gian, việc băm mật mã của chính nó, và một hoặc nhiều giao dịch. Các giao dịch, thường đã được xác minh bởi các nút của hệ thống chuỗi khối, có thể được băm và mã hóa thành cấu trúc dữ liệu, như cây Merkle. Trong cây Merkle, dữ liệu tại các nút lá (leaf) của cây được băm, và tất cả các việc băm ở mỗi cành (branch) của cây có thể được nối nhau ở gốc của cành này. Quy trình này tiếp tục trên cây đến gốc của toàn bộ cây, mà nó lưu trữ việc băm đại diện cho tất cả dữ liệu trong cây. Việc băm có nội dung là một giao dịch được lưu trữ trong cây có thể nhanh chóng được xác minh nhờ việc xác định liệu nó có nhất quán với cấu trúc của cây hay không.

Hệ thống chuỗi khối bao gồm mạng của các nút tính toán mà chúng quản lý, cập nhật, và duy trì một hoặc nhiều chuỗi khối. Mạng này có thể là mạng chuỗi khối chung, mạng chuỗi khối riêng, hoặc mạng chuỗi khối liên doanh. Ví dụ, nhiều thực thể, như hàng trăm, hàng nghìn, hoặc thậm chí là hàng triệu thực thể, có thể hoạt động trong mạng chuỗi khối chung, và mỗi thực thể trong số các thực thể này vận hành ít nhất một nút trong mạng chuỗi khối chung này. Theo đó, mạng chuỗi khối chung này có thể được coi là mạng công cộng đối với các thực thể tham gia. Đôi khi, đa số thực thể (nút) phải ký mọi khối để khối này là hợp lệ và được bổ sung vào chuỗi khối của mạng chuỗi khối. Các ví dụ về các mạng chuỗi khối chung bao gồm các mạng thanh toán đồng cấp cụ thể mà chúng tận dụng sổ cái phân tán, được gọi là chuỗi khối.

Nói chung, mạng chuỗi khối chung có thể hỗ trợ các giao dịch chung. Giao dịch chung được chia sẻ với tất cả các nút trong mạng chuỗi khối chung, và được lưu trữ trong chuỗi khối toàn cục. Chuỗi khối toàn cục là chuỗi khối được tái tạo qua tất cả các nút, và tất cả các nút đều nằm trong sự đồng thuận trạng thái hoàn hảo về chuỗi khối toàn cục. Để đạt được sự đồng thuận (ví dụ, thỏa thuận bổ sung một khối vào chuỗi khối), giao thức đồng thuận được thi hành trong mạng chuỗi khối chung. Các ví dụ về các giao thức đồng thuận bao gồm bằng chứng công việc (proof-of-work, POW) (ví dụ, được thi hành trong một số mạng tiền mã hóa), bằng chứng cổ phần (proof-of-stake, POS), và bằng chứng thẩm quyền (proof-of-authority, POA).

Nói chung, mạng chuỗi khối riêng có thể được cung cấp cho thực thể cụ thể, mà nó điều khiển tập trung việc cho phép đọc và ghi. Thực thể này điều khiển việc các nút nào có thể tham gia mạng chuỗi khối. Do đó, các mạng chuỗi khối riêng thường được gọi là các mạng được cấp phép mà nó đặt các giới hạn lên việc người nào được phép tham gia vào mạng, và giới hạn lên mức độ tham gia của họ (ví dụ, chỉ trong các giao dịch nhất định). Các loại cơ chế điều khiển truy cập khác nhau có thể được sử dụng (ví dụ, các bên tham gia sẵn có bỏ phiếu về việc bổ sung các thực thể mới, cơ quan điều hành có thể điều khiển việc kết nạp).

Nói chung, mạng chuỗi khối liên doanh có thể là riêng giữa các thực thể tham gia. Trong mạng chuỗi khối liên doanh, quy trình đồng thuận được điều khiển bởi tập hợp các nút được ủy quyền, một hoặc nhiều nút được vận hành bởi thực thể tương ứng (ví dụ, định chế tài chính, công ty bảo hiểm). Ví dụ, liên doanh của mười (10) thực thể (ví

dụ, các định chế tài chính, các công ty bảo hiểm) có thể vận hành mạng chuỗi khối liên doanh, mỗi thực thể trong số các thực thể này vận hành ít nhất một nút trong mạng chuỗi khối liên doanh này. Theo đó, mạng chuỗi khối liên doanh có thể được coi là mạng riêng đối với các thực thể tham gia. Trong một số ví dụ, mỗi thực thể (nút) phải ký mọi khối để khối là hợp lệ, và được bổ sung vào chuỗi khối. Trong một số ví dụ, ít nhất một tập con của các thực thể (các nút) (ví dụ, ít nhất 7 thực thể) phải ký mọi khối để khối là hợp lệ, và được bổ sung vào chuỗi khối.

Fig.1 minh họa sơ đồ giản lược của hệ thống chuỗi khối 100, theo một phương án. Tham chiếu đến Fig.1, hệ thống chuỗi khối 100 có thể bao gồm nhiều nút, ví dụ, các nút từ 102 đến 110, được tạo cấu hình để hoạt động trên chuỗi khối 120. Các nút từ 102 đến 110 này có thể tạo thành mạng 112, chẳng hạn như mạng đồng cấp (P2P). Mỗi nút trong số các nút từ 102 đến 110 có thể là thiết bị tính toán, chẳng hạn như máy tính hoặc hệ thống máy tính, được tạo cấu hình để lưu trữ bản sao của chuỗi khối 120, hoặc có thể là phần mềm chạy trên thiết bị tính toán này, chẳng hạn như quy trình hoặc ứng dụng. Mỗi nút trong số các nút từ 102 đến 110 có thể có bộ nhận dạng duy nhất.

Chuỗi khối 120 có thể bao gồm danh sách đang lớn dần của các bản ghi dưới dạng các khối dữ liệu, chẳng hạn như các khối từ B1 đến B5 trên Fig.1. Mỗi khối trong số các khối từ B1 đến B5 có thể bao gồm nhãn thời gian, việc băm mật mã khối trước đó, và dữ liệu của khối hiện tại, mà nó có thể là các giao dịch chẳng hạn như các giao dịch tiền tệ. Ví dụ, như được minh họa trên Fig.1, khối B5 có thể bao gồm nhãn thời gian, việc băm mật mã khối B4, và dữ liệu giao dịch của khối B5. Ngoài ra, ví dụ, phép toán băm có thể được thực hiện trên khối trước đó để tạo ra việc băm mật mã khối trước đó này. Phép toán băm có thể chuyển đổi các đầu vào có các độ dài khác nhau thành các đầu ra mật mã có độ dài cố định qua thuật toán băm, chẳng hạn như SHA-256.

Các nút từ 102 đến 110 có thể được tạo cấu hình để thực hiện thao tác trên chuỗi khối 120. Ví dụ, khi nút, chẳng hạn như nút 102, muốn lưu trữ dữ liệu mới lên trên chuỗi khối 120, nút đó có thể tạo ra khối mới để được bổ sung vào chuỗi khối 120 và phát quảng bá khối mới này đến các nút khác, ví dụ, các nút từ 104 đến 110, trong mạng 112. Dựa trên tính hợp pháp của khối mới, ví dụ, sự hợp lệ của chữ ký và các giao dịch của nó, các nút khác này có thể xác định để chấp nhận khối mới này, sao cho nút 102 và các nút khác có thể bổ sung khối mới này vào các bản sao tương ứng của chuỗi khối 120

của chúng. Khi quy trình này lặp lại, càng ngày càng nhiều khối dữ liệu có thể được bổ sung vào chuỗi khối 120.

Fig.2 minh họa sơ đồ giản lược của thiết bị tính toán 200 để thi hành nút, ví dụ, nút 102 (Fig.1), trong hệ thống chuỗi khối, theo một phương án. Tham chiếu đến Fig.2, thiết bị tính toán 200 có thể bao gồm giao diện truyền thông 202, bộ xử lý 204, và bộ nhớ 206.

Giao diện truyền thông 202 có thể tạo thuận lợi cho những việc truyền thông giữa thiết bị tính toán 200 và các thiết bị thi hành các nút khác, ví dụ, các nút từ 104 đến 110 (Fig.1), trong mạng. Theo một số phương án, giao diện truyền thông 202 được tạo cấu hình để hỗ trợ một hoặc nhiều tiêu chuẩn truyền thông, chẳng hạn như tiêu chuẩn hoặc giao thức Internet, tiêu chuẩn mạng kỹ thuật số dịch vụ tích hợp (Integrated Services Digital Network, ISDN), v.v. Theo một số phương án, giao diện truyền thông 202 có thể bao gồm một hoặc nhiều các mạng cục bộ (Local Area Network, LAN), môđem cáp, môđem vệ tinh, bus dữ liệu, cáp, kênh truyền thông không dây, kênh truyền thông dựa trên radiô, kênh truyền thông tế bào, thiết bị truyền thông dựa trên giao thức Internet (Internet Protocol, IP) , hoặc các thiết bị truyền thông khác cho các hoạt động truyền thông có dây và/hoặc không dây. Trong một số phương án, giao diện truyền thông 202 có thể dựa trên cơ sở hạ tầng đám mây chung, cơ sở hạ tầng đám mây riêng, cơ sở hạ tầng đám mây chung/riêng lai.

Bộ xử lý 204 có thể bao gồm một hoặc nhiều đơn vị xử lý dành riêng, các mạch tích hợp chuyên dụng (application-specific integrated circuit, ASIC), các mảng cổng lập trình được dạng trường (field-programmable gate array, FPGA), hoặc các loại bộ xử lý hoặc đơn vị xử lý khác. Bộ xử lý 204 được ghép nối với bộ nhớ 206 và được tạo cấu hình để thực thi các lệnh được lưu trữ trong bộ nhớ 206.

Bộ nhớ 206 có thể được tạo cấu hình để lưu trữ các lệnh thực thi được bằng bộ xử lý và dữ liệu, chẳng hạn như bản sao của chuỗi khối 120 (Fig.1). Bộ nhớ 206 có thể bao gồm thiết bị bất kỳ trong số các thiết bị bộ nhớ khả biến hoặc bất khả biến, hoặc sự kết hợp của chúng, chẳng hạn như bộ nhớ truy cập ngẫu nhiên tĩnh (SRAM), bộ nhớ chỉ đọc lập trình được xóa được bằng điện (EEPROM), bộ nhớ chỉ đọc lập trình được xóa được (EPROM), bộ nhớ chỉ đọc lập trình được (PROM), bộ nhớ chỉ đọc (ROM), bộ nhớ từ tính, bộ nhớ tác động nhanh (flash memory), hoặc đĩa từ hoặc đĩa quang. Khi các lệnh

trong bộ nhớ 206 được thực thi bởi bộ xử lý 204, thiết bị tính toán 200 có thể thực hiện thao tác trên chuỗi khối 120.

Để tạo thuận lợi cho hoạt động của hệ thống chuỗi khối 100 (Fig.1), các nút từ 102 đến 110 trong mạng 112 có thể hoạt động theo phương pháp truyền thông liên nút. Phương pháp truyền thông liên nút này có thể chỉ rõ quy trình để thiết lập việc truyền thông giữa các nút thứ nhất và thứ hai trong mạng, sao cho có thể tránh được các kết nối thừa giữa hai nút này.

Ví dụ, các nút 102 và 104 có thể xác minh liệu kết nối đã được thiết lập hay chưa, ví dụ, dựa trên các địa chỉ IP tương ứng của chúng, trước khi gửi đi yêu cầu kết nối. Ngoài ra, khi nhận yêu cầu kết nối, nút nhận có thể xác minh liệu kết nối đã được thiết lập hay chưa. Nút nhận có thể từ chối yêu cầu kết nối nếu nút này nếu nó xác định được rằng kết nối đã được thiết lập, nên sẽ tránh được các kết nối thừa một cách hiệu quả.

Fig.3 minh họa lưu đồ của phương pháp 300 để thiết lập việc truyền thông giữa các nút thứ nhất và thứ hai trong hệ thống chuỗi khối, theo một phương án. Ví dụ, hệ thống chuỗi khối này có thể được thi hành dưới dạng mạng P2P bao gồm nhiều nút. Ngoài ra, ví dụ, phương pháp 300 có thể được thực hiện bởi nút 102 (Fig.1) là nút thứ nhất để khởi tạo việc truyền thông với nút 104 (Fig.1) là nút thứ hai.

Tham chiếu đến Fig.1 và Fig.3, ở bước 302, nút 102 có thể xác minh liệu phiên truyền thông trước đã có hoặc đã được thiết lập giữa nút 102 và nút 104 hay chưa. Ví dụ, phiên truyền thông có thể là sự trao đổi thông tin tạm thời và mang tính tương tác giữa nút 102 và nút 104. Tùy thuộc vào các cách thi hành cụ thể, phiên truyền thông có thể được thiết lập trong lớp ứng dụng hoặc lớp phiên. Trong một số phương án, nút 102 có thể sử dụng bộ nhận dạng nút của nút 104 để xác minh liệu đã có phiên truyền thông giữa nút 102 và nút 104 hay chưa.

Ở bước 304, nếu nút 102 xác định rằng đã có sẵn phiên truyền thông trước đó giữa nút 102 và nút 104 thì nút 102 có thể chấm dứt việc thực thi phương pháp 300. Mặt khác, nếu nút 102 xác định rằng không có phiên truyền thông trước đó giữa nút 102 và nút 104 thì nút 102, ở bước 306, có thể gửi yêu cầu kết nối đến địa chỉ IP được liên kết với nút 104. Ví dụ, yêu cầu kết nối này được tạo cấu hình để thiết lập kênh truyền thông vật lý giữa nút 102 và nút 104. Trong một số phương án, nút 102 có thể yêu cầu kết nối với nút 104 ở mức lớp vận chuyển, ví dụ, yêu cầu thiết lập kết nối giao thức điều khiển

truyền (Transmission Control Protocol, TCP) với nút 104. Trong một số phương án, nút 102 có thể tiến hành bước 306 bằng cách thiết lập kết nối TCP mà không tạo ra phiên truyền thông với nút 104.

Ở bước 308, nút 102 có thể xác định liệu việc kết nối với nút 104 có thành công hay không. Nếu không, ví dụ, do yêu cầu kết nối bị từ chối bởi nút 104, nút 102 có thể chấm dứt việc thực thi phương pháp 300. Mặt khác, nếu nút 102 xác định rằng việc kết nối thành công thì nút 102 có thể, ở bước 310, xác định thêm liệu có phiên truyền thông giữa nút 102 và nút 104 hay không. Ví dụ, khi nút 102 yêu cầu kết nối với nút 104, nút 104 cũng có thể yêu cầu kết nối với nút 102 và thiết lập phiên truyền thông với nút 102. Nếu nút 102 xác định rằng có phiên truyền thông giữa nút 102 và nút 104 ở bước 310 thì nút 102 có thể chấm dứt việc thực thi phương pháp 300. Nếu không, nút 102 có thể tiến hành bước 312.

Ở bước 312, nút 102 có thể trao đổi các bộ nhận dạng nút với nút 104 bằng cách cung cấp bộ nhận dạng nút của nút 102 cho nút 104 và nhận bộ nhận dạng nút của nút 104 từ nút 104. Trong một số phương án, mỗi nút trong số nút 102 và nút 104 có thể ký việc trao đổi này nhờ sử dụng các khóa riêng của chúng vì lý do bảo mật. Ví dụ, nút 102 có thể mã hóa bộ nhận dạng nút của nó nhờ sử dụng khóa riêng của nút 102, và nút 104 có thể mã hóa bộ nhận dạng nút của nó nhờ sử dụng khóa riêng của nút 104. Tuy nhiên, trong một số phương án, việc ký việc trao đổi này nhờ sử dụng các khóa riêng có thể không cần thiết, chẳng hạn như khi các nút 102 và 104 đang hoạt động trong môi trường bảo mật, ví dụ, môi trường thử nghiệm cách ly. Cần hiểu rằng, dù cho các cách thi hành cụ thể có thể thay đổi, mục đích của việc trao đổi này là giống nhau, mà chính là để tạo thuận lợi cho việc trao đổi các bộ nhận dạng nút để khiến cho phiên truyền thông được thiết lập trên đỉnh của kết nối giữa nút 102 và nút 104, ở bước 314.

Ở bước 316, nút 102 có thể xác định liệu đã có sẵn một phiên truyền thông khác, ví dụ, phiên truyền thông trước đó khác với phiên truyền thông vừa mới được thiết lập ở bước 314, giữa nút 102 và nút 104 hay chưa. Ví dụ, khi nút 102 trao đổi các bộ nhận dạng nút với nút 104, nút 104 cũng có thể thiết lập phiên truyền thông với nút 102. Nếu nút 102 xác định rằng không có phiên truyền thông khác giữa nút 102 và nút 104 thì nút 102 có thể chấm dứt việc thực thi phương pháp 300. Mặt khác, nếu nút 102 xác định rằng đã có sẵn một phiên truyền thông khác giữa nút 102 và nút 104 thì nút 102 có thể

tiến hành bước 318 để chấm dứt một phiên trong số các phiên truyền thông dựa trên quy tắc được thiết lập trước. Nút 102 cũng có thể chấm dứt kết nối giữa nút 102 và nút 104 mà phiên truyền thông bị chấm dứt đã được thiết lập trên đó.

Quy tắc được thiết lập trước có thể dựa trên các bộ nhận dạng nút. Ví dụ, nút 102 có thể chọn chấm dứt phiên truyền thông mà nó đã được khởi tạo bởi nút với bộ nhận dạng nút lớn hơn (hoặc nhỏ hơn). Quy tắc được thiết lập trước cũng có thể dựa trên các yếu tố khác miễn là các yếu tố được sử dụng có khả năng phân biệt một cách có hệ thống các phiên truyền thông, sao cho một phiên truyền thông được phép giữ nguyên và tất cả các phiên truyền thông khác có thể được nhận dạng và chấm dứt. Ví dụ, quy tắc được thiết lập trước có thể đòi hỏi nút 102 chấm dứt tất cả các phiên truyền thông đã được thiết lập trước đó và giữ phiên truyền thông đã được thiết lập gần đây nhất.

Fig.4 là lưu đồ của phương pháp 400 để thiết lập việc truyền thông giữa các nút thứ nhất và thứ hai trong hệ thống chuỗi khối, theo một phương án. Ví dụ, hệ thống chuỗi khối được thi hành trong mạng P2P bao gồm nhiều nút. Ngoài ra, ví dụ, phương pháp 400 có thể được thực hiện bởi nút 104 (Fig.1) là nút thứ hai để xử lý yêu cầu kết nối được gửi bởi nút 102 (Fig.1) là nút thứ nhất.

Tham chiếu đến Fig.1 và Fig.4, ở bước 402, nút 104 có thể nhận yêu cầu kết nối được gửi bởi nút 102. Trong một số phương án, nút 102 có thể yêu cầu kết nối với nút 104 ở mức lớp vận chuyển, ví dụ, yêu cầu thiết lập kết nối giao thức điều khiển truyền (TCP) với nút 104. Nút 104 có thể xử lý yêu cầu này và thiết lập kết nối với nút 102 theo đó.

Ở bước 404, nút 104 có thể trao đổi các bộ nhận dạng nút với nút 102 bằng cách cung cấp bộ nhận dạng nút của nút 104 cho nút 102 và nhận bộ nhận dạng nút của nút 102 từ nút 102. Trong một số phương án, mỗi nút trong số nút 102 và nút 104 có thể ký việc trao đổi này nhờ sử dụng các khóa riêng của chúng vì lý do bảo mật. Tuy nhiên, trong một số phương án, việc ký việc trao đổi này nhờ sử dụng các khóa riêng có thể không cần thiết, chẳng hạn như khi các nút 102 và 104 đang hoạt động trong môi trường bảo mật, ví dụ, môi trường thử nghiệm cách ly. Cần hiểu rằng, dù cho các cách thi hành cụ thể có thể thay đổi, mục đích của việc trao đổi này là giống nhau, mà chính là để tạo thuận lợi cho việc trao đổi các bộ nhận dạng nút để khiến cho phiên truyền thông được thiết lập trên đỉnh của kết nối giữa nút 102 và nút 104, ở bước 406.

Ở bước 408, nút 104 có thể xác định liệu đã có sẵn một phiên truyền thông khác, ví dụ, phiên truyền thông trước đó khác với phiên truyền thông vừa mới được thiết lập ở bước 406, giữa nút 102 và nút 104 hay chưa. Ví dụ, khi nút 104 trao đổi các bộ nhận dạng nút với nút 102, nút 102 cũng có thể thiết lập phiên truyền thông với nút 104. Nếu nút 104 xác định không có phiên truyền thông trước đó giữa nút 102 và nút 104 thì nút 104 có thể chấm dứt việc thực thi phương pháp 400. Mặt khác, nếu nút 104 xác định rằng đã có sẵn phiên truyền thông trước đó giữa nút 102 và nút 104 thì nút 104 có thể tiến hành bước 410 để chấm dứt một phiên trong số các phiên truyền thông dựa trên quy tắc được thiết lập trước. Nút 104 cũng có thể chấm dứt kết nối giữa nút 102 và nút 104 mà phiên truyền thông bị chấm dứt đã được thiết lập trên đó.

Trong một số phương án, nút 104 được tạo cấu hình để sử dụng quy tắc được thiết lập trước giống với quy tắc được thiết lập trước được sử dụng bởi nút 102 để chọn chấm dứt phiên truyền thông nào. Ví dụ, nếu nút 102 được tạo cấu hình để chọn phiên truyền thông mà nó đã được khởi tạo bởi nút với bộ nhận dạng nút lớn hơn là phiên để chấm dứt thì nút 104 được tạo cấu hình để sử dụng quy tắc giống như vậy, điều này có thể tạo thuận lợi cho việc chấm dứt cùng phiên truyền thông bởi nút 102 và nút 104.

Cần hiểu rằng, các phương pháp được mô tả trên đây để thiết lập việc truyền thông giữa các nút thứ nhất và thứ hai được dựa trên các bộ nhận dạng nút của các nút thứ nhất và thứ hai này. Theo đó, địa chỉ IP có thể được sử dụng để hỗ trợ nhiều hơn một nút trong các phương án được minh họa. Kết quả là, một thiết bị tính toán có thể được sử dụng để thi hành nhiều hơn một nút trong các phương án được minh họa.

Fig.5 minh họa sơ đồ giản lược của hệ thống chuỗi khối 500, theo một phương án. Tham chiếu đến Fig.5, hệ thống chuỗi khối 500 có thể bao gồm nhiều nút từ 502 đến 510 được tạo cấu hình để hoạt động trên chuỗi khối 520, tương tự như các nút từ 102 đến 110 được tạo cấu hình để hoạt động trên chuỗi khối 120 (Fig.1). Hơn nữa, thiết bị tính toán 530 được tạo cấu hình để làm chủ (host) các nút từ 502 đến 506. Thiết bị tính toán 530 có thể được thi hành theo cách tương tự như thiết bị tính toán 200 (Fig.2). Tức là, thiết bị tính toán 530 có thể bao gồm giao diện truyền thông, bộ xử lý, và bộ nhớ. Trong một số phương án, thiết bị tính toán 530 có thể thi hành các bộ siêu giám sát (hypervisors) và/hoặc các máy ảo để làm chủ các nút từ 502 đến 506. Trong một số phương án, thiết bị tính toán 530 có thể làm chủ các nút từ 502 đến 506 dưới dạng các

quy trình hoặc các ứng dụng đang thực thi song song. Thiết bị tính toán 530 cũng có thể sử dụng các kỹ thuật tính toán khác để làm chủ các nút từ 502 đến 506.

Việc có khả năng sử dụng một thiết bị tính toán để làm chủ nhiều hơn một nút có thể làm giảm chi phí phần cứng đối với các hệ thống chuỗi khối. Tuy nhiên, các thiết bị tính toán này không bị bắt buộc phải làm chủ nhiều hơn một nút. Như được minh họa trên Fig.5, ví dụ, các thiết bị tính toán 540 và 550 có thể được sử dụng để lần lượt làm chủ chỉ một nút 508 và 510, và tất cả các nút từ 502 đến 510 có thể hoạt động chung để hoạt động trên chuỗi khối 520 như được mô tả trên đây. Hơn nữa, cần lưu ý rằng các phương pháp được tạo cấu hình theo các phương án của sáng chế không áp đặt các giới hạn bất kỳ về việc nút nào có thể khởi tạo yêu cầu kết nối.

Các phương án khác nhau nêu trên chỉ đơn thuần mang tính ví dụ và không phải là giới hạn. Ví dụ, tuy các nút 102 và 104 (Fig.1) được sử dụng để minh họa việc thực thi các phương pháp 300 (Fig.3) và 400 (Fig.4), nút bất kỳ trong hệ thống chuỗi khối 100 có thể sử dụng phương pháp 300 để yêu cầu việc truyền thông với một nút khác. Tương tự, nút bất kỳ trong hệ thống chuỗi khối 100 có thể sử dụng phương pháp 400 để xử lý yêu cầu kết nối nhận được.

Các phương pháp 300 và 400 có thể được sử dụng trong các loại mạng chuỗi khối khác nhau, như mạng chuỗi khối chung, mạng chuỗi khối riêng, hoặc mạng chuỗi khối liên doanh, được mô tả trên đây. Các phương pháp 300 và 400 cũng có thể được sử dụng cho các loại ứng dụng khác nhau, ví dụ, lưu giữ sổ sách, tiền mã hóa, các sổ cái phân tán dựa trên chuỗi khối hoặc dạng tương tự, mà không tách rời khỏi nguyên lý và phạm vi của sáng chế.

Fig.6 là sơ đồ khối của máy 600 để thiết lập việc truyền thông giữa các nút thứ nhất và thứ hai trong hệ thống chuỗi khối, theo một phương án. Ví dụ, máy 600 có thể thi hành mỗi nút trong số nút thứ nhất và nút thứ hai. Ngoài ra, ví dụ, máy 600 có thể là cách thi hành một quy trình phần mềm, và có thể tương ứng với phương pháp 300 (Fig.3) hoặc phương pháp 400 (Fig.4). Tham chiếu đến Fig.6, máy 600 có thể bao gồm môđun trao đổi 602, môđun xác định 604, và môđun chấm dứt 606.

Môđun trao đổi 602 có thể cung cấp bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận bộ nhận dạng nút của nút thứ hai từ nút thứ hai, để khiến cho phiên truyền thông thứ nhất được thiết lập giữa nút thứ nhất và nút thứ hai. Môđun xác định 604 có

thể xác định liệu có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai hay không. Môđun chấm dứt 606 có thể, đáp lại việc xác định rằng có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai, chấm dứt một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai dựa trên bộ nhận dạng nút của nút thứ nhất và bộ nhận dạng nút của nút thứ hai.

Máy 600 cũng có thể bao gồm môđun truyền thông 608. Môđun truyền thông 608 có thể gửi yêu cầu kết nối đến nút thứ hai, hoặc nhận yêu cầu kết nối từ nút thứ hai, để thiết lập kết nối giữa nút thứ nhất và nút thứ hai. Môđun truyền thông 608 còn có thể thiết lập phiên truyền thông trên đỉnh của kết nối giữa nút thứ nhất và nút thứ hai.

Mỗi môđun trong số các môđun được mô tả trên đây có thể được thi hành dưới dạng phần mềm, hoặc phần cứng, hoặc sự kết hợp của phần mềm và phần cứng. Ví dụ, mỗi môđun trong số các môđun được mô tả trên đây có thể được thi hành nhờ sử dụng bộ xử lý thực thi các lệnh được lưu trữ trong bộ nhớ. Ngoài ra, ví dụ, mỗi môđun trong số các môđun được mô tả trên đây có thể được thi hành với một hoặc nhiều mạch tích hợp chuyên dụng (application specific integrated circuit, ASIC), bộ xử lý tín hiệu số (digital signal processor, DSP), thiết bị xử lý tín hiệu số (digital signal processing device, DSPD), thiết bị logic lập trình được (programmable logic device, PLD), mảng cổng lập trình được dạng trường (field programmable gate array, FPGA), bộ điều khiển, bộ vi điều khiển, bộ vi xử lý, hoặc các thành phần điện tử khác, để thực hiện các phương pháp đã được mô tả. Hơn nữa, ví dụ, mỗi môđun trong số các môđun được mô tả trên đây có thể được thi hành nhờ sử dụng chip máy tính hoặc thực thể, hoặc được thi hành nhờ sử dụng sản phẩm có chức năng nhất định. Theo một phương án, máy 600 có thể là máy tính, và máy tính này có thể là máy tính cá nhân, máy tính xách tay, điện thoại tế bào, điện thoại camera, điện thoại thông minh, thiết bị trợ giúp số cá nhân (personal digital assistant), thiết bị trình diễn phương tiện, thiết bị điều hướng, thiết bị gửi và nhận thư điện tử, bảng điều khiển trò chơi, máy tính bảng, thiết bị đeo được, hoặc sự kết hợp bất kỳ của các thiết bị này.

Đối với quy trình thi hành các chức năng và các vai trò của mỗi môđun trong máy 600, có thể tham chiếu đến các bước tương ứng trong các phương pháp được mô tả trên đây. Các nội dung chi tiết được lược bỏ để đơn giản.

Trong một số phương án, sản phẩm chương trình máy tính có thể bao gồm phương tiện lưu trữ phi chuyển tiếp đọc được bằng máy tính có các lệnh chương trình đọc được bằng máy tính trên đó để khiến cho bộ xử lý thực hiện các phương pháp được mô tả trên đây.

Phương tiện lưu trữ đọc được bằng máy tính này có thể là thiết bị hữu hình mà nó có thể lưu trữ các lệnh để sử dụng bởi thiết bị thực thi lệnh. Phương tiện lưu trữ đọc được bằng máy tính này có thể là, ví dụ, nhưng không bị giới hạn ở, thiết bị lưu trữ điện tử, thiết bị lưu trữ từ tính, thiết bị lưu trữ quang học, thiết bị lưu trữ điện tử, thiết bị lưu trữ bán dẫn, hoặc sự kết hợp thích hợp bất kỳ của các thiết bị nêu trên. Danh sách không nhằm mục đích giới hạn của các ví dụ cụ thể hơn về phương tiện lưu trữ đọc được bằng máy tính bao gồm như sau: đĩa máy tính cầm tay, đĩa cứng, bộ nhớ truy nhập ngẫu nhiên (RAM), bộ nhớ chỉ đọc (ROM), bộ nhớ chỉ đọc lập trình được xóa được (erasable programmable read-only memory, EPROM), bộ nhớ truy nhập ngẫu nhiên tĩnh (static random access memory, SRAM), bộ nhớ chỉ đọc đĩa nén (compact disc read-only memory, CD-ROM) cầm tay, đĩa đa năng kỹ thuật số (digital versatile disk, DVD), thanh nhớ (memory stick), đĩa mềm, thiết bị được mã hoá theo cách cơ học chẳng hạn như các thẻ đục lỗ hoặc các cấu trúc nổi trong rãnh có các lệnh được ghi trên đó, và sự kết hợp thích hợp bất kỳ của các loại nêu trên.

Các lệnh chương trình đọc được bằng máy tính để thực hiện các phương pháp được mô tả trên đây có thể là các lệnh hợp ngữ, các lệnh của kiến trúc tập lệnh (instruction-set-architecture, ISA), các lệnh máy, các lệnh phục thuộc máy, vi mã, các lệnh phần sụn, dữ liệu thiết lập trạng thái, hoặc mã nguồn hoặc mã đối tượng được viết theo cách kết hợp bất kỳ của một hoặc nhiều ngôn ngữ lập trình, bao gồm ngôn ngữ lập trình hướng đối tượng, và các ngôn ngữ lập trình thủ tục thông thường. Các lệnh chương trình đọc được bằng máy tính có thể thực thi toàn bộ trên thiết bị tính toán dưới dạng gói phần mềm độc lập, hoặc một phần trên thiết bị tính toán thứ nhất và một phần trên thiết bị tính toán thứ hai ở xa thiết bị tính toán thứ nhất. Trong kịch bản được nêu sau, thiết bị tính toán thứ hai, ở xa có thể được kết nối với thiết bị tính toán thứ nhất qua kiểu mạng bất kỳ, bao gồm mạng cục bộ (LAN) hoặc mạng diện rộng (wide area network, WAN).

Các lệnh chương trình đọc được bằng máy tính có thể được cung cấp cho bộ xử lý của máy tính đa năng hoặc chuyên dụng, hoặc thiết bị xử lý dữ liệu lập trình được khác

để tạo ra máy, sao cho các lệnh này, mà chúng thực thi qua bộ xử lý của máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác này, tạo ra phương tiện để thi hành các phương pháp được mô tả trên đây.

Các lưu đồ và các sơ đồ trên các hình vẽ minh họa cấu trúc, chức năng, và hoạt động của các cách thi hành khả dĩ của các thiết bị, các phương pháp, và các sản phẩm chương trình máy tính theo các phương án khác nhau của sáng chế. Về khía cạnh này, khối trong các lưu đồ hoặc sơ đồ này có thể đại diện cho phần mềm máy tính, đoạn, hoặc phần của mã, mà nó bao gồm một hoặc nhiều lệnh thực thi được để thi hành các chức năng cụ thể. Cũng cần lưu ý rằng, theo một số cách thi hành thay thế, các chức năng được ghi chú trên các khối có thể xuất hiện khác với thứ tự được ghi chú trên các hình vẽ. Ví dụ, hai khối được thể hiện nối tiếp nhau có thể, trên thực tế, được thực thi về cơ bản là đồng thời, hoặc các khối này có thể đôi khi được thực thi theo thứ tự đảo ngược, tùy thuộc vào chức năng liên quan. Cũng cần lưu ý rằng mỗi khối của các sơ đồ và/hoặc lưu đồ, và các sự kết hợp của các khối trong các sơ đồ và các lưu đồ, có thể được thi hành bởi các hệ thống dựa trên phần cứng chuyên dụng mà chúng thực hiện các chức năng hoặc hành động được chỉ rõ, hoặc các sự kết hợp của phần cứng chuyên dụng và các lệnh máy tính.

Cần hiểu rằng các dấu hiệu nhất định của sáng chế, mà chúng được mô tả, nhằm mục đích làm rõ, trong ngữ cảnh của các phương án riêng rẽ, cũng có thể được đưa ra ở dạng kết hợp trong một phương án đơn nhất. Ngược lại, các dấu hiệu khác nhau của sáng chế, mà chúng được mô tả, cho ngắn gọn, trong ngữ cảnh của một phương án đơn nhất, cũng có thể được đưa ra riêng rẽ hoặc theo sự kết hợp con thích hợp bất kỳ hoặc thích hợp trong phương án được mô tả khác bất kỳ của sáng chế. Các dấu hiệu nhất định được mô tả trong ngữ cảnh của các phương án khác nhau không phải là các dấu hiệu thiết yếu của các phương án đó, trừ khi được lưu ý như vậy.

Cần hiểu rằng, mặc dù các thuật ngữ chẳng hạn như “thứ nhất” và “thứ hai” được sử dụng ở đây để mô tả các phần tử khác nhau, các phần tử này không bị giới hạn ở các thuật ngữ này, vốn chỉ được sử dụng để phân biệt các phần tử. Ví dụ, phần tử thứ nhất (ví dụ, nút thứ nhất) cũng có thể được gọi là phần tử thứ hai (ví dụ, nút thứ hai), và tương tự, phần tử thứ hai cũng có thể được gọi là phần tử thứ nhất, mà không tách rời khỏi nguyên lý và phạm vi của sáng chế.

Mặc dù sáng chế đã được mô tả cùng với các phương án cụ thể, người có hiểu biết trung bình trong lĩnh vực tương ứng sẽ hiểu rõ rằng có nhiều sự thay thế, cải biến và thay đổi. Theo đó, các yêu cầu bảo hộ sau đây bao trùm tất cả các phương án thay thế, cải biến và thay đổi như vậy mà chúng nằm trong phạm vi của các yêu cầu bảo hộ này.

YÊU CẦU BẢO HỘ

1. Phương pháp được thi hành bằng máy tính để thiết lập việc truyền thông giữa nút thứ nhất và nút thứ hai trong hệ thống chuỗi khối (blockchain), phương pháp này bao gồm các bước:

cung cấp, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ hai từ nút thứ hai, để khiến cho phiên truyền thông thứ nhất được thiết lập giữa nút thứ nhất và nút thứ hai, nút thứ nhất và nút thứ hai đang tham gia trong hệ thống chuỗi khối để quản lý một hoặc nhiều chuỗi khối;

xác định, bởi nút thứ nhất, dựa trên bộ nhận dạng nút của nút thứ hai, liệu có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai hay không; và

đáp lại việc xác định rằng có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai, chấm dứt, bởi nút thứ nhất, một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai dựa trên bộ nhận dạng nút của nút thứ nhất và bộ nhận dạng nút của nút thứ hai, bước chấm dứt này bao gồm việc:

xác định một nút thông qua một bước trong số các bước: xác định một nút trong số nút thứ nhất và nút thứ hai mà nó có bộ nhận dạng nút lớn hơn, hoặc xác định một nút trong số nút thứ nhất và nút thứ hai mà nó có bộ nhận dạng nút nhỏ hơn;

xác định một phiên truyền thông trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai mà nó được thiết lập dựa trên yêu cầu kết nối được gửi từ nút được xác định; và

chọn phiên truyền thông được xác định trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai để chấm dứt.

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

chấm dứt, bởi nút thứ nhất, kết nối giữa nút thứ nhất và nút thứ hai, một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai đang được thiết lập trên kết nối này.

3. Phương pháp theo điểm 1, trước bước cung cấp, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ hai từ nút thứ hai, phương pháp này còn bao gồm một bước trong số các bước sau đây:

gửi, bởi nút thứ nhất, yêu cầu kết nối thứ nhất đến nút thứ hai để thiết lập kết nối giữa nút thứ nhất và nút thứ hai; hoặc

nhận, bởi nút thứ nhất, yêu cầu kết nối thứ hai từ nút thứ hai để thiết lập kết nối giữa nút thứ nhất và nút thứ hai.

4. Phương pháp theo điểm 3, trước khi kết nối được thiết lập giữa nút thứ nhất và nút thứ hai, phương pháp này còn bao gồm các bước:

xác định, bởi nút thứ nhất, liệu có phiên truyền thông trước đó giữa nút thứ nhất và nút thứ hai hay không; và

đáp lại việc xác định rằng không có phiên truyền thông trước đó giữa nút thứ nhất và nút thứ hai, gửi, bởi nút thứ nhất, yêu cầu kết nối thứ nhất đến địa chỉ giao thức Internet (Internet Protocol, IP) được liên kết với nút thứ hai để thiết lập kết nối giữa nút thứ nhất và nút thứ hai.

5. Phương pháp theo điểm 3, sau khi kết nối được thiết lập giữa nút thứ nhất và nút thứ hai, phương pháp này còn bao gồm các bước:

xác định, bởi nút thứ nhất, liệu có phiên truyền thông trước đó giữa nút thứ nhất và nút thứ hai hay không; và

đáp lại việc xác định rằng không có phiên truyền thông trước đó giữa nút thứ nhất và nút thứ hai, thực hiện, bởi nút thứ nhất, việc cung cấp bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và việc nhận bộ nhận dạng nút của nút thứ hai từ nút thứ hai.

6. Phương pháp theo điểm 3, trong đó kết nối giao thức điều khiển truyền (Transmission Control Protocol, TCP) được thiết lập làm kết nối giữa nút thứ nhất và nút thứ hai, phương pháp này còn bao gồm bước:

thiết lập phiên truyền thông thứ nhất dựa trên kết nối TCP này.

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

mã hóa, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ nhất nhờ sử dụng khóa riêng của nút thứ nhất, trước khi cung cấp bộ nhận dạng nút của nút thứ nhất cho nút thứ hai.

8. Thiết bị tính toán để thiết lập việc truyền thông giữa nút thứ nhất và nút thứ hai trong hệ thống chuỗi khối, thiết bị tính toán này bao gồm:

một hoặc nhiều bộ xử lý; và

một hoặc nhiều bộ nhớ đọc được bằng máy tính được ghép nối với một hoặc nhiều bộ xử lý này và có các lệnh được lưu trữ trên đó mà chúng là có thể thực thi được bởi một hoặc nhiều bộ xử lý này, trong đó một hoặc nhiều bộ xử lý này được tạo cấu hình để:

cung cấp bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận bộ nhận dạng nút của nút thứ hai từ nút thứ hai, để khiến cho phiên truyền thông thứ nhất được thiết lập giữa nút thứ nhất và nút thứ hai, nút thứ nhất và nút thứ hai đang tham gia trong hệ thống chuỗi khối để quản lý một hoặc nhiều chuỗi khối;

xác định, dựa trên bộ nhận dạng nút của nút thứ hai, liệu có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai hay không; và

đáp lại việc xác định rằng có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai, chấm dứt một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai dựa trên bộ nhận dạng nút của nút thứ nhất và bộ nhận dạng nút của nút thứ hai, trong đó trong bước chấm dứt một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai, một hoặc nhiều bộ xử lý này còn được tạo cấu hình để:

xác định một nút thông qua một bước trong số các bước: xác định một nút trong số nút thứ nhất và nút thứ hai mà nó có bộ nhận dạng nút lớn hơn, hoặc xác định một nút trong số nút thứ nhất và nút thứ hai mà nó có bộ nhận dạng nút nhỏ hơn;

xác định một phiên truyền thông trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai mà nó được thiết lập dựa trên yêu cầu kết nối được gửi từ nút được xác định; và

chọn phiên truyền thông được xác định trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai để chấm dứt.

9. Thiết bị tính toán theo điểm 8, trong đó một hoặc nhiều bộ xử lý còn được tạo cấu hình để:

chấm dứt kết nối giữa nút thứ nhất và nút thứ hai, một phiên đã nêu trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai đang được thiết lập trên kết nối này.

10. Thiết bị tính toán theo điểm 8, trong đó trước khi cung cấp bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận bộ nhận dạng nút của nút thứ hai từ nút thứ hai, một hoặc nhiều bộ xử lý còn được tạo cấu hình để:

gửi yêu cầu kết nối thứ nhất đến nút thứ hai để thiết lập kết nối giữa nút thứ nhất và nút thứ hai; hoặc

nhận yêu cầu kết nối thứ hai từ nút thứ hai để thiết lập kết nối giữa nút thứ nhất và nút thứ hai.

11. Thiết bị tính toán theo điểm 10, trong đó trước khi kết nối được thiết lập giữa nút thứ nhất và nút thứ hai, một hoặc nhiều bộ xử lý còn được tạo cấu hình để:

xác định liệu có phiên truyền thông trước đó giữa nút thứ nhất và nút thứ hai hay không; và

đáp lại việc xác định rằng không có phiên truyền thông trước đó giữa nút thứ nhất và nút thứ hai, gửi yêu cầu kết nối thứ nhất đến địa chỉ giao thức Internet (IP) được liên kết với nút thứ hai để thiết lập kết nối giữa nút thứ nhất và nút thứ hai.

12. Thiết bị tính toán theo điểm 10, trong đó sau khi kết nối được thiết lập giữa nút thứ nhất và nút thứ hai, một hoặc nhiều bộ xử lý còn được tạo cấu hình để:

xác định liệu có phiên truyền thông trước đó giữa nút thứ nhất và nút thứ hai hay không; và

đáp lại việc xác định rằng không có phiên truyền thông trước đó giữa nút thứ nhất và nút thứ hai, cung cấp bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận bộ nhận dạng nút của nút thứ hai từ nút thứ hai.

13. Thiết bị tính toán theo điểm 10, trong đó kết nối giao thức điều khiển truyền (TCP) được thiết lập làm kết nối giữa nút thứ nhất và nút thứ hai, và một hoặc nhiều bộ xử lý còn được tạo cấu hình để:

thiết lập phiên truyền thông thứ nhất dựa trên kết nối TCP này.

14. Thiết bị tính toán theo điểm 8, trong đó một hoặc nhiều bộ xử lý còn được tạo cấu hình để:

mã hóa bộ nhận dạng nút của nút thứ nhất nhờ sử dụng khóa riêng của nút thứ nhất, trước khi cung cấp bộ nhận dạng nút của nút thứ nhất cho nút thứ hai.

15. Phương tiện phi chuyển tiếp đọc được bằng máy tính lưu trữ trong đó các lệnh để, khi được thực thi bởi bộ xử lý của thiết bị tính toán, khiến cho thiết bị tính toán này thực

hiện phương pháp để thiết lập việc truyền thông giữa nút thứ nhất và nút thứ hai trong hệ thống chuỗi khối, phương pháp này bao gồm các bước:

cung cấp, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ nhất cho nút thứ hai và nhận, bởi nút thứ nhất, bộ nhận dạng nút của nút thứ hai từ nút thứ hai, để khiến cho phiên truyền thông thứ nhất được thiết lập giữa nút thứ nhất và nút thứ hai, nút thứ nhất và nút thứ hai đang tham gia trong hệ thống chuỗi khối để quản lý một hoặc nhiều chuỗi khối;

xác định, bởi nút thứ nhất, dựa trên bộ nhận dạng nút của nút thứ hai, liệu có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai hay không; và

đáp lại việc xác định rằng có phiên truyền thông thứ hai giữa nút thứ nhất và nút thứ hai, chấm dứt, bởi nút thứ nhất, một phiên trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai dựa trên bộ nhận dạng nút của nút thứ nhất và bộ nhận dạng nút của nút thứ hai, bước chấm dứt này bao gồm việc:

xác định một nút thông qua một bước trong số các bước: xác định một nút trong số nút thứ nhất và nút thứ hai mà nó có bộ nhận dạng nút lớn hơn, hoặc xác định một nút trong số nút thứ nhất và nút thứ hai mà nó có bộ nhận dạng nút nhỏ hơn;

xác định một phiên truyền thông trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai mà nó được thiết lập dựa trên yêu cầu kết nối được gửi từ nút được xác định; và

chọn phiên truyền thông được xác định trong số phiên truyền thông thứ nhất và phiên truyền thông thứ hai để chấm dứt.

1 / 6

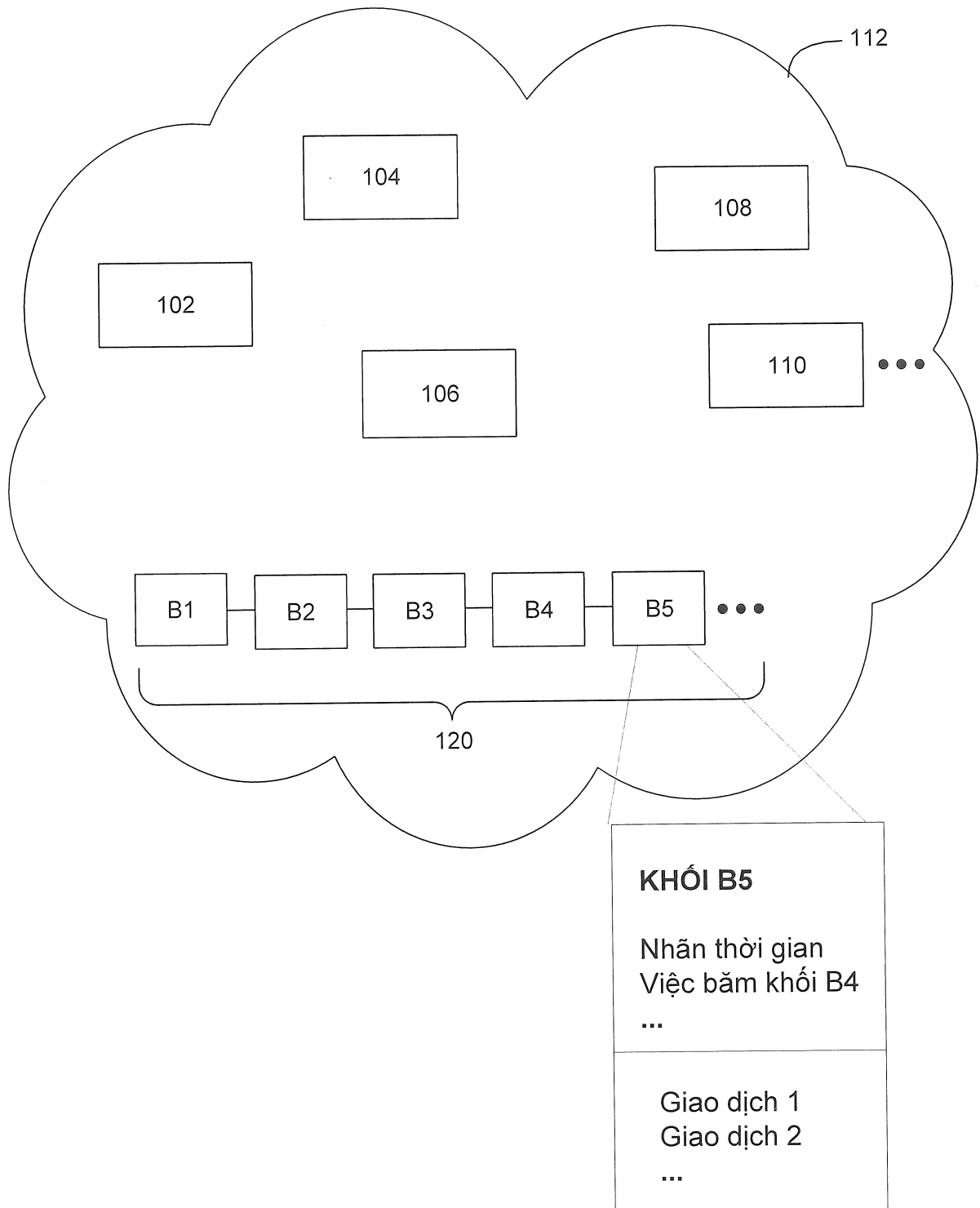
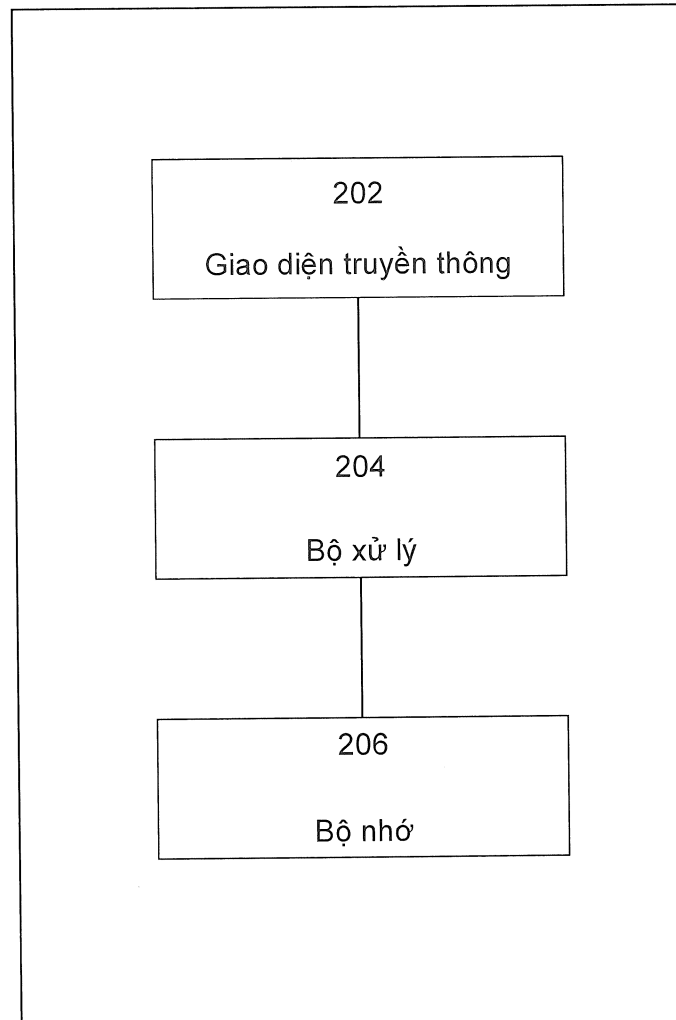
100

FIG. 1

200**FIG. 2**

300

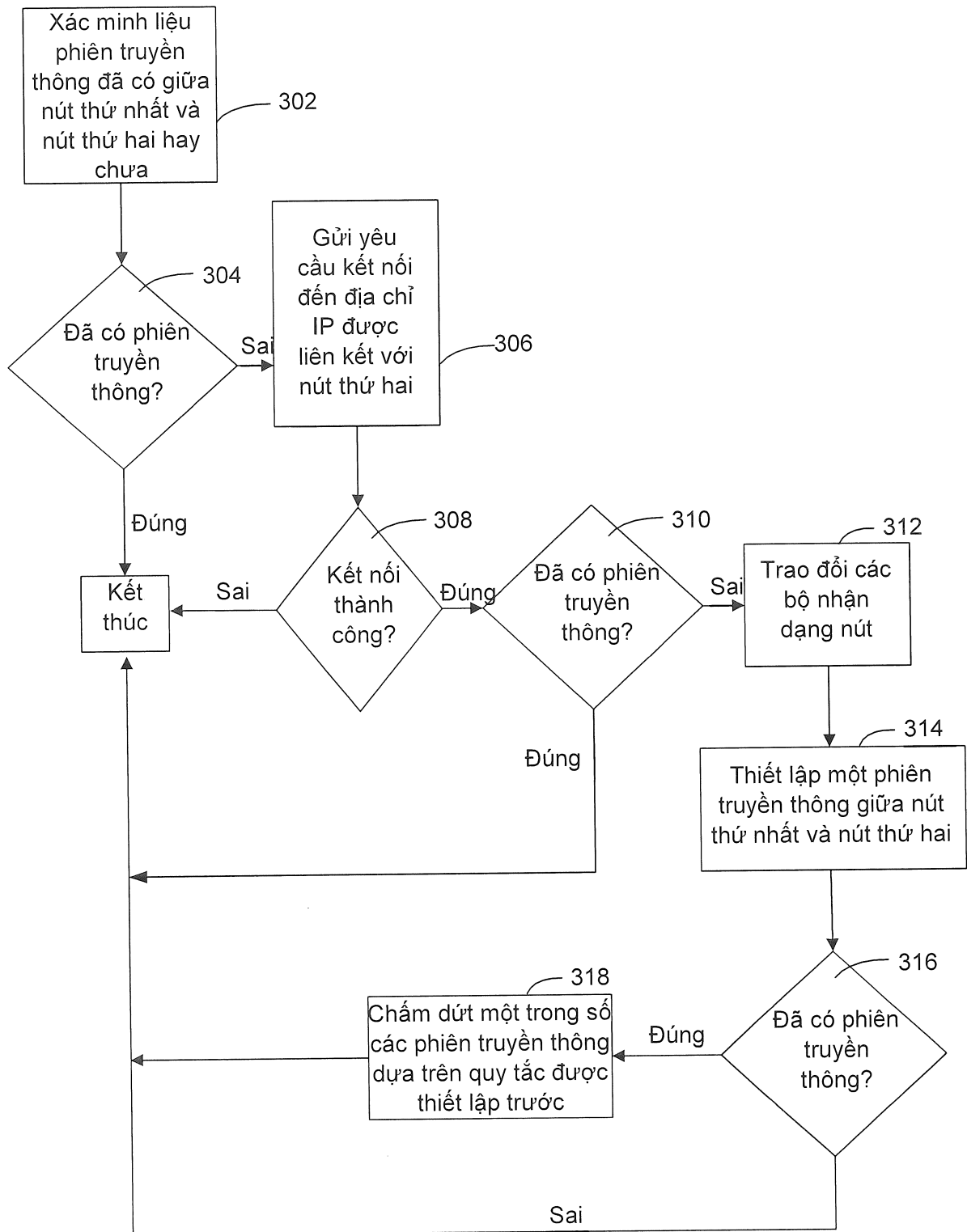


FIG. 3

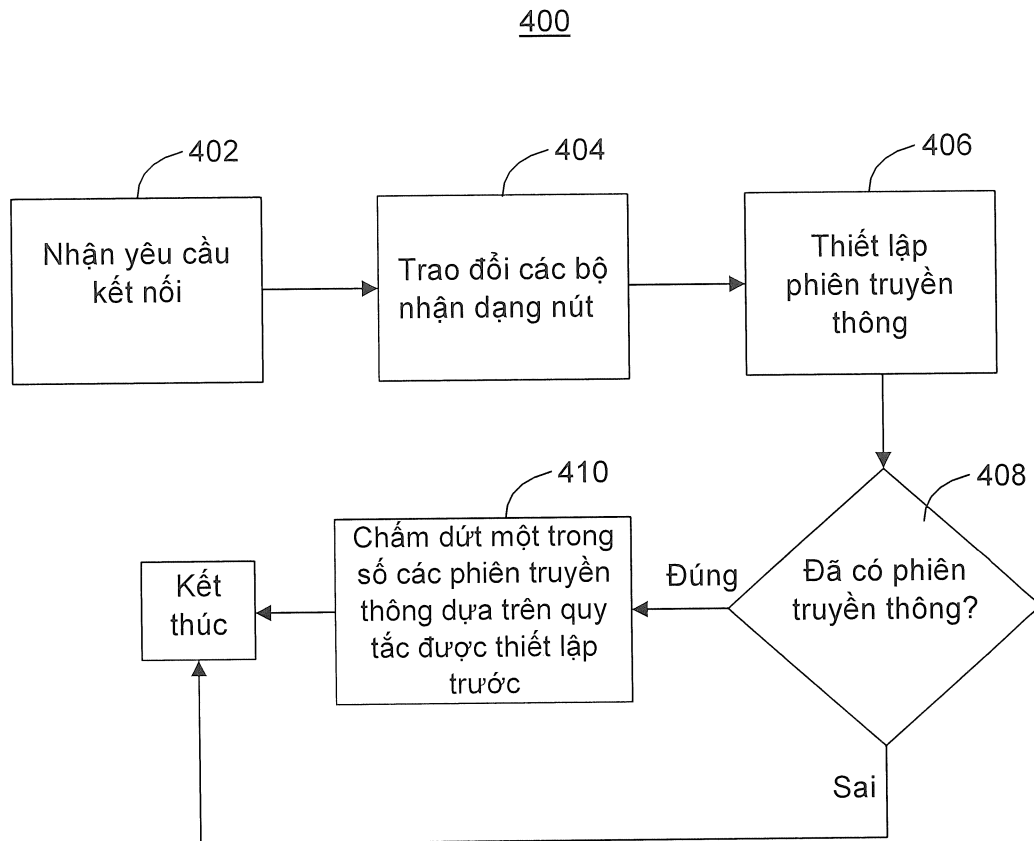


FIG. 4

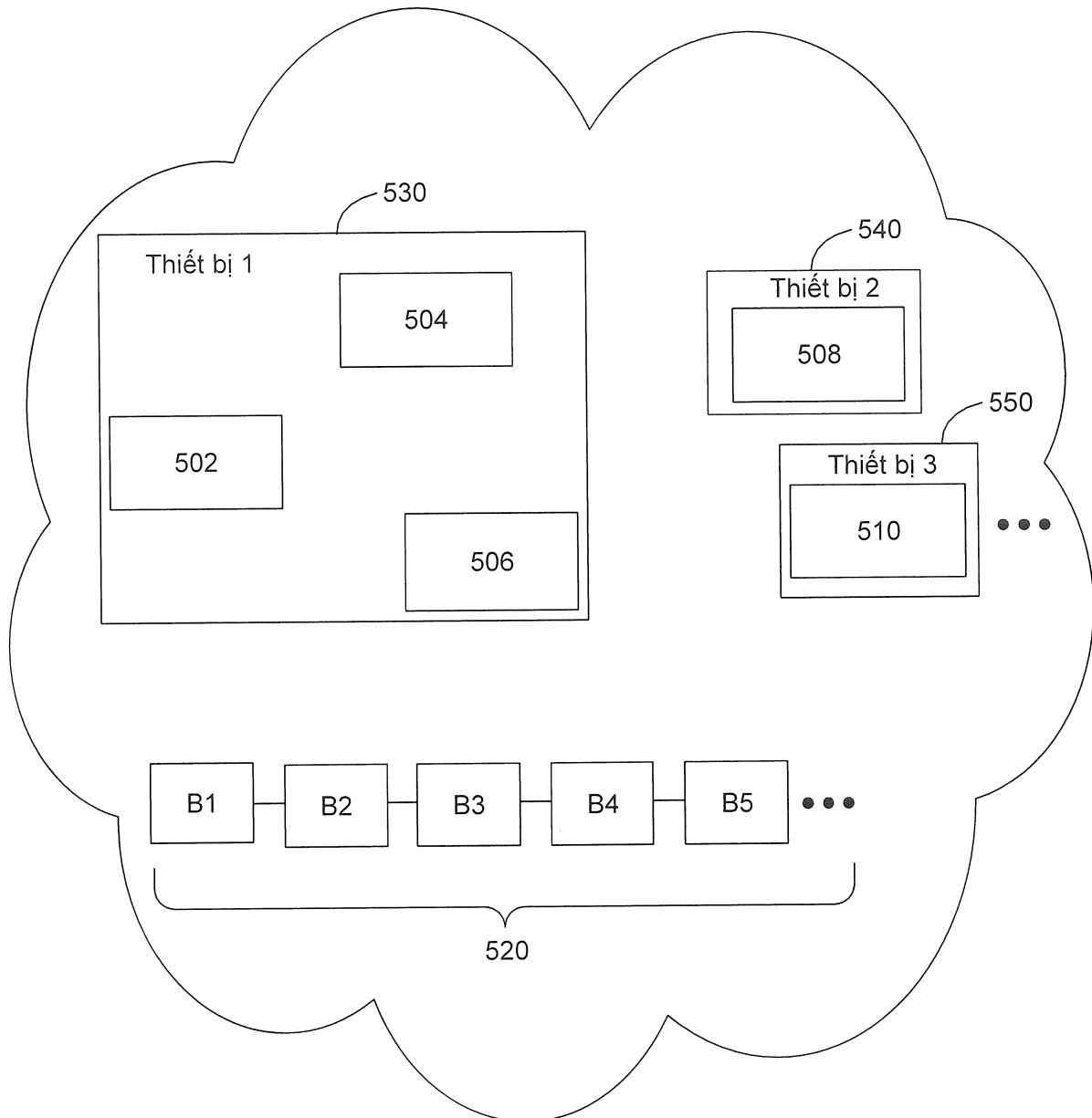
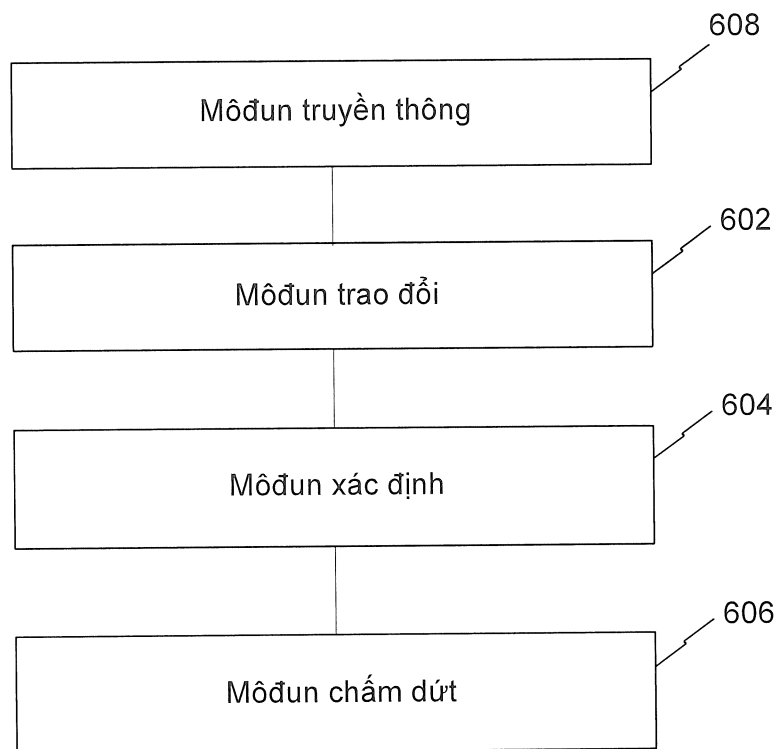
500

FIG. 5

600**FIG. 6**