(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) **1-0036055**

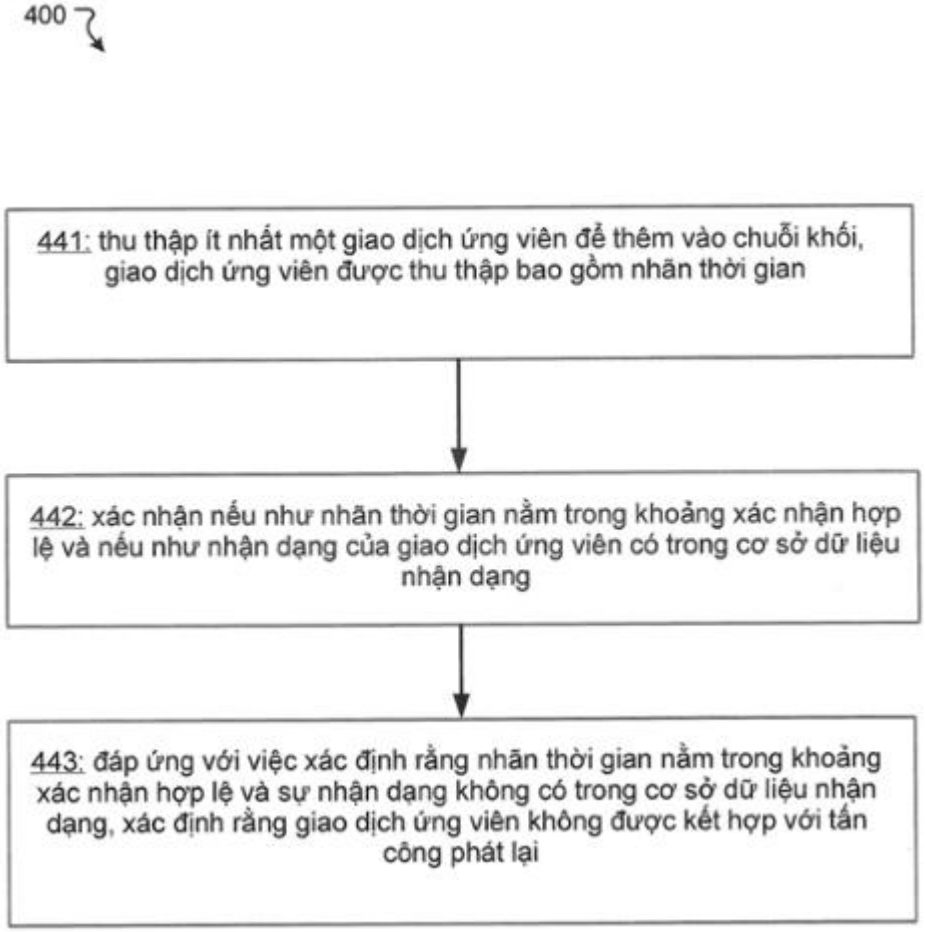
(51)[7] **H04L 9/00**; G06F 21/00

(13) **B**

(21) 1-2019-02694
(22) 29/12/2018
(86) PCT/CN2018/125782 29/12/2018
(87) WO2019/072314 18/04/2019
(45) 26/06/2023 423
(43) 25/12/2019 381A
(73) ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) XIE, Guilu (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP ĐƯỢC THI HÀNH BỞI MÁY TÍNH VÀ HỆ THỐNG ĐỂ DÒ TẤN CÔNG PHÁT LẠI, VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BỞI MÁY TÍNH KHÔNG CHUYỂN TIẾP

(57) Sáng chế đề cập tới phương pháp được thi hành bởi máy tính để dò tấn công phát lại bao gồm các bước: thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối; xác nhận nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, cơ sở dữ liệu nhận dạng bao gồm nhiều nhận dạng trong khoảng xác nhận hợp lệ; và đáp ứng với việc xác định rằng nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.


400
441: thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối, giao dịch ứng viên được thu thập bao gồm nhãn thời gian
442: xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ và nếu như nhận dạng của giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng
443: đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại

Lĩnh vực kỹ thuật được đề cập

Nói chung, sáng chế đề cập tới các phương pháp và các thiết bị để dò tấn công phát lại.

Tình trạng kỹ thuật của sáng chế

Một tấn công phát lại (cũng được biết như tấn công quay lại, tấn công tính chất mới, tấn công xen giữa) là dạng tấn công mạng trong đó việc truyền dữ liệu hợp lệ bị lặp lại hoặc bị chậm một cách cố tình hoặc gian lận. Điều này có thể được thực hiện bởi người bắt đầu truyền tới một nút (node) (chẳng hạn máy chủ) hoặc bởi đối phương người chặn dữ liệu và truyền lại nó tới nút. Chẳng hạn, sự tấn công phát lại có thể được thực hiện như một phần của tấn công giả mạo bằng cách thay thế gói giao thức internet (Internet Protocol, IP). Cách khác mô tả tấn công phát lại là: tấn công vào giao thức an toàn bằng cách sử dụng phát lại các thông báo từ một thuộc tính khác thành thuộc tính được dự tính (hoặc ban đầu và được chờ đợi), nhờ vậy lừa (các) nút trung thực có ý tưởng là các nút này đã thực hiện thành công tiến trình giao thức. Chẳng hạn, giao thức có thể là một giao thức giao dịch chuỗi khối (blockchain). Chuỗi khối có thể phân nhánh thành hai hoặc nhiều chuỗi con mà đi theo cùng địa chỉ, khóa mã hóa, và hệ thống giao dịch. Một giao dịch hợp pháp trên một chuỗi con có thể bị cố tình lặp lại trên chuỗi con khác bởi một tấn công phát lại, gây tổn thất cho người gửi.

Mặc dù chuỗi khối có ưu điểm với các lợi thế khác nhau hơn các mạng truyền thống, nhưng dù sao nó cũng nhạy cảm với các tấn công phát lại. Chẳng hạn, một giao dịch gửi 20 tiền mã hóa (ether) từ A đến B thông qua chuỗi khối có thể là được lặp lại bởi B trong các tấn công phát lại để bòn rút liên tục số dư của A. Vì vậy, việc dò tấn công phát lại là giải pháp cấp thiết để tránh các hoạt động của chuỗi khối độc hại và đảm bảo an toàn cho các tài sản cá nhân.

Bản chất kỹ thuật của sáng chế

Các phương án thực hiện sáng chế khác nhau bao gồm các hệ thống, các phương pháp, và các phương tiện đọc được bởi máy tính không chuyển tiếp để dò tấn công phát lại.

Theo một khía cạnh của sáng chế, phương pháp được thi hành bởi máy tính để dò tấn công phát lại bao gồm các bước: thu thập ít nhất một giao dịch ứng viên (candidate) để thêm vào chuỗi khối; xác nhận nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, cơ sở dữ liệu nhận dạng bao gồm nhiều nhận dạng trong khoảng xác nhận hợp lệ; và đáp ứng với việc xác định rằng nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

Theo một số phương án, giao dịch ứng viên đã thu thập bao gồm nhãn thời gian (timestamp); xác nhận nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng bao gồm: xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ và nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng; và đáp ứng với việc xác định rằng nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại bao gồm, đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

Theo một số phương án, giao dịch ứng viên bao gồm nhãn thời gian và thông tin giao dịch. Sau khi thu thập ít nhất một giao dịch ứng viên và trước khi xác nhận nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, phương pháp còn bao gồm bước: xác định giá trị băm (hash) ít nhất dựa trên nhãn thời gian và thông tin giao dịch, giá trị băm có tác dụng như nhận dạng.

Theo một số phương án, giao dịch ứng viên bao gồm nhãn thời gian, thông tin giao dịch, và giá trị băm được xác định ít nhất dựa trên nhãn thời gian và thông tin giao dịch, giá trị băm có tác dụng như nhận dạng. Sau khi thu thập ít nhất một giao dịch ứng viên và trước khi xác nhận nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, phương pháp còn bao gồm bước: xác nhận nhận dạng bằng cách xác nhận giá trị băm ít nhất dựa trên nhãn thời gian và thông tin giao dịch.

Theo một số phương án, nhãn thời gian được tạo cấu hình bởi thiết bị đầu cuối người dùng đã khởi đầu ít nhất một giao dịch ứng viên; và thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối bao gồm tiếp nhận giao dịch ứng viên từ thiết bị đầu cuối người dùng.

Theo một số phương án, nhãn thời gian được tạo cấu hình bởi nút chuỗi khối; và thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối bao gồm: tiếp nhận ít nhất một giao dịch được khởi đầu từ thiết bị đầu cuối người dùng; và thêm nhãn thời gian vào giao dịch được khởi đầu để thu thập ít nhất một giao dịch ứng viên.

Theo một số phương án, phương pháp còn bao gồm bước: đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, thêm nhận dạng vào cơ sở dữ liệu nhận dạng.

Theo một số phương án, phương pháp còn bao gồm bước: đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, thêm giao dịch ứng viên vào vùng nhớ đệm để lưu trữ các giao dịch ứng viên.

Theo một số phương án, phương pháp còn bao gồm bước: đáp ứng với việc xác định rằng nhãn thời gian không nằm trong khoảng xác nhận hợp lệ, trả lại thông báo lỗi tới thiết bị tính toán đã đệ trình giao dịch ứng viên.

Theo một số phương án, phương pháp còn bao gồm bước: đáp ứng với việc xác định rằng nhận dạng có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên được kết hợp với tấn công phát lại.

Theo một số phương án, phương pháp còn bao gồm bước: thực hiện sự xác nhận đồng thuận, trong đó giao dịch ứng viên được bao gồm trong sự xác nhận đồng thuận nếu như giao dịch ứng viên được xác định là không được kết hợp với tấn công phát lại.

Theo một số phương án, phương pháp còn bao gồm các bước: đồng bộ hóa cơ sở dữ liệu nhận dạng với một hoặc nhiều nút chuỗi khối khác; xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ và nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng được đồng bộ hóa; đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có

trong cơ sở dữ liệu nhận dạng được đồng bộ hóa, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại; và đáp ứng với việc xác định rằng nhận dạng có trong cơ sở dữ liệu nhận dạng được đồng bộ hóa, xác định rằng giao dịch ứng viên được kết hợp với tấn công phát lại.

Theo một số phương án, trước khi thu thập ít nhất một giao dịch ứng viên, phương pháp còn bao gồm bước: đồng bộ hóa cơ sở dữ liệu nhận dạng với một hoặc nhiều nút chuỗi khối khác.

Theo một số phương án, cơ sở dữ liệu nhận dạng bao gồm thông tin của các giao dịch với các nhãn thời gian trong khoảng thời gian gần đây tương ứng với khoảng xác nhận hợp lệ.

Theo một số phương án, khoảng xác nhận hợp lệ được dựa trên nhãn thời gian khác của khối (block) muộn nhất của chuỗi khối; và khoảng xác nhận hợp lệ được bao gồm trong khối nguồn gốc của chuỗi khối.

Theo một số phương án, khoảng xác nhận hợp lệ được dựa trên đồng hồ nội tại của nút chuỗi khối mà thực hiện xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ.

Theo khía cạnh khác, hệ thống dò tấn công phát lại bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ đọc được bởi máy tính không chuyển tiếp được kết nối với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để khiến hệ thống thực hiện các hoạt động bao gồm: thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối; xác nhận nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, cơ sở dữ liệu nhận dạng bao gồm nhiều nhận dạng trong khoảng xác nhận hợp lệ; và đáp ứng với việc xác định rằng nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

Theo khía cạnh khác, phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp được tạo cấu hình với các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để khiến một hoặc nhiều bộ xử lý thực hiện các hoạt động bao gồm: thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối; xác nhận nếu như sự nhận dạng giao dịch

ứng viên có trong cơ sở dữ liệu nhận dạng, cơ sở dữ liệu nhận dạng bao gồm nhiều nhận dạng trong khoảng xác nhận hợp lệ; và đáp ứng với việc xác định rằng nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

Các dấu hiệu này và khác nữa của các hệ thống, các phương pháp, và các phương tiện đọc được bởi máy tính không chuyển tiếp đã bộc lộ ở đây, cũng như các phương pháp hoạt động và các chức năng của các bộ phận kết cấu liên quan và sự kết hợp các bộ phận và tính kinh tế của sản phẩm, sẽ trở nên rõ ràng hơn khi xem xét phần mô tả dưới đây và các điểm yêu cầu bảo hộ kèm theo với tham chiếu đến các hình vẽ kèm theo, toàn bộ chúng tạo ra phần mô tả này, trong đó các số chỉ dẫn giống nhau biểu thị các bộ phận tương ứng trên các hình vẽ khác nhau. Tuy nhiên, cần hiểu rằng các hình vẽ chỉ nhằm mục đích minh họa và mô tả và không được dự tính tạo ra sự giới hạn sáng chế.

Mô tả vắn tắt các hình vẽ

Các dấu hiệu nhất định của các phương án thực hiện khác nhau của sáng chế được nêu cụ thể trong các điểm yêu cầu bảo hộ kèm theo. Việc hiểu rõ nhất các dấu hiệu và ưu điểm của giải pháp sẽ đạt được với tham chiếu đến phần mô tả chi tiết dưới đây trình bày các phương án minh họa sáng chế, trong đó các nguyên lý của sáng chế được sử dụng, và các hình vẽ kèm theo, trong đó:

Fig.1 là hình vẽ minh họa hệ thống dò tấn công phát lại để làm ví dụ sáng chế theo các phương án thực hiện khác nhau.

Fig.2 là hình vẽ minh họa giao dịch mà với nó việc dò tấn công phát lại được thực hiện theo các phương án thực hiện khác nhau để làm ví dụ sáng chế.

Fig.3 minh họa lưu đồ thể hiện phương pháp dò tấn công phát lại để làm ví dụ sáng chế theo các phương án thực hiện khác nhau.

Fig.4A minh họa lưu đồ thể hiện phương pháp dò tấn công phát lại để làm ví dụ sáng chế theo các phương án thực hiện khác nhau.

Fig.4B minh họa lưu đồ thể hiện phương pháp dò tấn công phát lại để làm ví dụ sáng chế theo các phương án thực hiện khác nhau.

Fig.5 minh họa sơ đồ khối của hệ thống máy tính dò tấn công phát lại để làm ví dụ sáng chế theo các phương án thực hiện khác nhau.

Fig.6 minh họa sơ đồ khối của hệ thống máy tính dò tấn công phát lại để làm ví dụ sáng chế theo các phương án thực hiện khác nhau.

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

Mô tả chi tiết sáng chế

Chuỗi khối (blockchain) có thể được xem như cơ sở dữ liệu phi tập trung, được gọi chung là sổ cái phân phối do hoạt động được thực hiện bởi các nút (node) khác nhau (chẳng hạn các thiết bị tính toán) trong mạng. Thông tin bất kỳ có thể được ghi cho chuỗi khối và được lưu hoặc đọc từ đó. Các nút, chẳng hạn, là các thiết bị tính toán hoặc các hệ thống máy tính lớn mà hỗ trợ mạng chuỗi khối và duy trì chúng chạy êm. Mỗi nút có thể tạo ra một phần hoặc toàn bộ các chức năng của chuỗi khối. Chẳng hạn, nút mà tạo ra sự xác nhận đồng thuận có thể được gọi là nút tham gia đồng thuận (hoặc nút đồng thuận).

Theo các phương án thực hiện khác nhau, đồng thuận có thể là thuật toán gồm các quy tắc cho mạng các nút chuỗi khối để đạt được chấp nhận chung các kết quả xử lý. Chẳng hạn, các nút chuỗi khối có thể tiếp nhận các giao dịch theo thứ tự khác nhau do sự trễ mạng, việc cấp chúng có thể được giải quyết bởi sự đồng thuận. Theo một ví dụ, ở hệ thống đồng thuận "bằng chứng công việc", các nút chuỗi khối có thể bao gồm các thiết bị đào tác động vào phần cứng của chúng hoặc công suất tính toán để kiểm tra các khối của chuỗi khối và nhận thù lao. Việc đưa ra bằng chứng công việc có thể là quá trình ngẫu nhiên với xác suất thấp khiến cho một loạt kiểm tra và xác định lỗi nói chung là cần thiết trước khi bằng chứng công việc hợp lệ được tạo ra. Đồng tiền điện tử (Bitcoin) sử dụng hệ thống bằng chứng công việc dạng tem điện tử (Hashcash). Theo ví dụ khác, ở hệ thống đồng thuận "bằng chứng cổ phần/dịch vụ", các nút chuỗi khối với mức nhất định của quyền biểu quyết có thể được viện dẫn đến các nút đồng thuận/chủ/chính, mà đảm nhận xác nhận giao dịch, khi đối lập với các nút không đồng thuận. Các nút đồng thuận có thể tạo các khối mới cho chuỗi khối và đưa ra các quyết định cho chuỗi khối, chẳng hạn, thanh toán các phí dịch vụ cho chuỗi khối. Các nút

đồng thuận có thể được kết hợp với một lượng lớn các đồng tiền mã hóa và xác nhận các giao dịch mới dựa trên các quy tắc đồng thuận nhất định được đồng ý lẫn nhau. Dựa trên quy tắc xác định các nút đồng thuận, hệ thống đồng thuận bằng chứng cổ phần/dịch vụ có thể được thi hành như một bằng chứng dựa trên chuỗi của hệ thống đồng thuận bằng chứng cổ phần/dịch vụ, hệ thống đồng thuận bằng chứng cổ phần/dịch vụ thuật toán Dung sai lỗi Byzantin (Byzantine Fault Tolerance - BFT), v.v. Trong phần mô tả này, các nút đầy đủ, các nút đồng thuận, hoặc các nút tương đương khác trong hệ thống chuỗi khối đã bộc lộ hoặc hệ thống chuỗi khối khác có thể xác nhận các giao dịch như các nút chuỗi khối. Chẳng hạn, hệ thống chuỗi khối có thể bao gồm chuỗi khối dùng chung, chuỗi khối cho phép, chuỗi khối riêng tư, v.v.

Khác với kiểu đầu ra giao dịch chưa được dùng (unspent transaction output, UTXO), ethereum được dựa trên kiểu Số dư/Tài khoản (hoặc được gọi là kiểu giao dịch dựa trên tài khoản), mà duy trì sự kiểm tra số dư của mỗi tài khoản như trạng thái toàn cầu. Trong giao dịch, số dư của tài khoản được kiểm tra để đảm bảo rằng nó lớn hơn hoặc bằng lượng giao dịch đang dùng. Một ví dụ về cách mà kiểu Số dư/Tài khoản làm việc trong ethereum được thực hiện:

1. Alice thu được 5 ether thông qua việc đào. Nó được ghi trong hệ thống là Alice có 5 ether.

2. Alice muốn chuyển cho Bob 1 ether, vậy hệ thống trước hết sẽ trừ đi 1 ether từ tài khoản của Alice, khiến lúc này Alice có 4 ether.

3. Hệ thống sau đó tăng tài khoản của Bob thêm 1 ether. Hệ thống biết rằng Bob có 2 ether để bắt đầu, do vậy số dư Bob được tăng tới 3 ether.

Với kiểu Tài khoản/Số dư, các nút chuỗi khối lưu trữ trạng thái gần đây nhất của mỗi hợp đồng thông minh, bổ sung cho toàn bộ các giao dịch ether. Với mỗi ứng dụng ethereum, mạng có thể duy trì sự theo dõi "trạng thái" hoặc thông tin hiện thời, bao gồm nonce (số chỉ dùng một lần) tài khoản, số dư của mỗi người dùng, toàn bộ mã hợp đồng thông minh (chẳng hạn mã nhị phân), dung lượng lưu trữ (chẳng hạn để lưu trữ các băm).

Khác với kiểu UTXO vốn ngăn ngừa các tấn công phát lại hoặc dùng hai lần bằng cách xác định số dư khả dụng như lượng chưa dùng từ giao dịch trước đó, kiểu Số dư/Tài khoản truyền thống sử dụng nonce tài khoản khi như một cơ chế để lọc các tấn công phát lại. Nonce tài khoản là bộ đếm giao dịch trong mỗi tài khoản để ngăn ngừa các tấn công phát lại. Mặc dù cả hai đều có thể có mặt trong kiểu Số dư/Tài khoản, nonce tài khoản có thể được phân biệt với nonce bằng chứng công việc trong các hệ thống đồng thuận bằng chứng công việc, vốn là giá trị vô nghĩa trong khối mà có thể được điều chỉnh để cố đáp ứng điều kiện bằng chứng công việc với kiểu UTXO. Mặc dù được mô tả hầu hết với tham chiếu đến kiểu Số dư/Tài khoản (hệ thống bằng chứng cổ phần/dịch vụ), các hệ thống và các phương pháp đã bộc lộ không bị hạn chế bởi các ứng dụng với kiểu Tài khoản/Số dư (chẳng hạn hệ thống ethereum).

Tấn công phát lại thường được sử dụng để nhận được một cách bất hợp pháp các lợi ích bằng cách dùng hai lần một tài sản nhất định. Để việc dùng hai lần trở nên "thành công", người dùng có dụng ý xấu thường: gửi một giao dịch tới một bên, chờ nó đăng ký, đến lượt thu thập gì đó từ giao dịch thứ nhất nay, gửi nhanh giao dịch khác với giá năng lượng cao (giá tính toán trên ethereum), và có giao dịch thứ hai được bắt đầu đào do vậy làm mất tính hợp lệ giao dịch thứ nhất. Giao dịch thứ hai thường là bản sao của giao dịch thứ nhất với một số thay đổi (chẳng hạn thời gian, giá năng lượng, đối tượng nhận, hoặc thông số khác được tạo cấu hình bởi người gửi). Giao dịch thứ hai có thể sử dụng cùng nhận dạng (chẳng hạn băm) của giao dịch thứ nhất. Do giá năng lượng cao hơn có thể thu hút các thợ đào để bắt đầu đào giao dịch thứ hai, có giao dịch thứ hai được đào trước khi giao dịch thứ nhất có thể cho phép người dùng dụng ý xấu duy trì sự trả lại từ giao dịch thứ nhất trong khi giao dịch thứ hai được thực thi, vì vậy đạt được việc dùng hai lần. Việc sử dụng nonce tài khoản dự tính loại trừ vấn đề này.

Khi thực hiện giao dịch trong ethereum, số liên tiếp được gán vào mỗi giao dịch ở cùng tài khoản như số nonce tài khoản. Vì vậy, nonce tài khoản cũng có thể biểu thị số lượng các giao dịch đã gửi từ một địa chỉ tài khoản xác định. Nonce tài khoản được duy trì bởi mạng chuỗi khối, gồm các nút của nó. Mỗi nút sẽ xử lý các giao dịch từ một tài khoản cụ thể với trình tự nghiêm ngặt theo giá trị nonce tài khoản của nó. Do vậy, việc thất bại để gia tăng giá trị nonce tài khoản một cách chính xác có thể dẫn

đến các loại lỗi khác nhau. Chẳng hạn, giả thiết nonce tài khoản cuối cùng là 121, nếu như chủ tài khoản gửi một giao dịch mới cho cùng tài với nonce tài khoản bằng 121 hoặc nhỏ hơn (cố gắng sử dụng lại nonce tài khoản), nút sẽ từ chối nó. Với cùng giả thiết, nếu như chủ tài khoản gửi một giao dịch mới với nonce tài khoản bằng 123 hoặc lớn hơn, giao dịch sẽ không được xử lý cho đến khi khoảng hở này được đóng lại, nghĩa là cho đến khi giao dịch với nonce tài khoản 122 được xử lý.

Như được mô tả trong phần tình trạng kỹ thuật của sáng chế, việc dò tấn công phát lại là cấp thiết để tránh các hoạt động chuỗi khối độc hại và đảm bảo an toàn các tài sản cá nhân. Mặc dù chuỗi khối có ưu điểm với xác nhận đồng thuận phi tập trung, nhưng dù sao có thể nhạy cảm với các tấn công phát lại. Cụ thể là, cơ chế nonce tài khoản có các thiếu sót hoặc các nhược điểm nhất định. Chẳng hạn, để khởi đầu giao dịch, thiết bị đầu cuối người dùng trước hết có thể cần thu thập nonce tài khoản từ nút chuỗi khối, thêm tải truyền tới nút chuỗi khối. Với ví dụ khác, cơ chế nonce tài khoản là không tin cậy với một số trạng thái như sau. Ở trạng thái (1), tài khoản gửi giao dịch thứ nhất và giao dịch thứ hai kế tiếp cả với cùng phí giao dịch tới cùng nút chuỗi khối. Tuy nhiên, nếu như nút chuỗi khối tiếp nhận giao dịch thứ hai trước khi giao dịch thứ nhất do không theo thứ tự sự truyền gói dữ liệu mạng, nút chuỗi khối sẽ thực thi giao dịch thứ hai và sau đó là giao dịch thứ nhất, gây ra các thất bại thực thi cho cả hai giao dịch do không phù hợp với cơ chế nonce tài khoản. Ở trạng thái (2), tài khoản gửi giao dịch thứ nhất và giao dịch thứ hai kế tiếp tới cùng nút chuỗi khối, với giao dịch thứ hai có phí giao dịch cao hơn. Để tăng tối đa lợi nhuận, các nút chuỗi khối có thể được lập trình để ưu tiên thực thi giao dịch thứ hai và sau đó là giao dịch thứ nhất, gây ra các thất bại thực thi cho cả hai giao dịch do không phù hợp với cơ chế nonce tài khoản. Ở trạng thái (3), tài khoản gửi song song các giao dịch khác nhau từ các thiết bị đầu cuối người dùng khác nhau, nhưng các giao dịch này sẽ có cùng giá trị nonce tài khoản. Kết quả là, tối đa một trong số các giao dịch sẽ được xử lý thành công.

Để giảm ít nhất các nhược điểm của các công nghệ hiện tại, tạo ra giải pháp kỹ thuật để khắc phục vấn đề kỹ thuật được mô tả ở trên, và cải thiện các chức năng máy tính, các hệ thống và các phương pháp để dò tấn công phát lại được bộc lộ. Như được mô tả dưới đây, theo các phương án thực hiện khác nhau, sự kết hợp xác nhận nhãn thời gian và xác nhận nhận dạng giao dịch có thể được sử dụng thay cho sử dụng

nonce tài khoản để đạt được việc dò tấn công phát lại mạnh mẽ. Do đó, các giao dịch độc hại có thể được nhận biết kịp thời từ các giao dịch trung thực và được hủy bỏ.

Fig.1 thể hiện hệ thống làm ví dụ 100 để thực hiện các bước và các phương pháp được bộc lộ khác nhau, theo các phương án thực hiện khác nhau. Như được thể hiện trên hình vẽ, mạng chuỗi khối có thể bao gồm nhiều nút chuỗi khối (chẳng hạn nút 1, nút 2, nút 3, nút 4, nút i, v.v.). Các nút chuỗi khối có thể tạo mạng (chẳng hạn mạng ngang hàng) có một nút chuỗi khối truyền thông với một nút khác. Thứ tự và số lượng các nút chuỗi khối như được thể hiện trên hình vẽ chỉ để làm ví dụ minh họa và đơn giản hóa việc mô tả. Các nút chuỗi khối có thể được thi hành trong các máy chủ, 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 kết nối với nhau qua các loại phương pháp truyền thông khác nhau như TCP/IP. Tùy thuộc vào các phân loại, các nút chuỗi khối có thể bao gồm các nút đầy đủ, các nút Geth, các nút đồng thuận, v.v.

Theo các phương án thực hiện khác nhau, người dùng A và người dùng B có thể sử dụng các thiết bị tương ứng như máy tính xách tay và điện thoại di động để kích hoạt các nút chuỗi khối nhằm thực thi các giao dịch, mà có thể hoặc có thể không bao gồm các hợp đồng chuỗi khối (chẳng hạn các hợp đồng thông minh). Theo một ví dụ, người dùng A muốn giao dịch với người dùng B bằng cách truyền một tài sản nào đó trong tài khoản của người dùng A đến tài khoản người dùng B. Người dùng A và người dùng B có thể sử dụng các nút A và nút B của thiết bị tương ứng (còn gọi là các thiết bị đầu cuối người dùng) được cài đặt phần mềm chuỗi khối thích hợp (chẳng hạn ví tiền mã hóa) để khởi đầu, chuyển tiếp, hoặc truy nhập giao dịch. Nút A thiết bị người dùng A có thể được gọi là nút người khởi đầu mà khởi đầu giao dịch với nút B thiết bị người dùng B được gọi là nút người nhận. Nút A có thể truy nhập chuỗi khối thông qua sự truyền thông với nút 1, và nút B có thể truy nhập chuỗi khối thông qua sự truyền thông với nút 2. Nút A, nút B, hoặc các nút tương tự có thể đệ trình các giao dịch với chuỗi khối thông qua nút 1, nút 2, hoặc các nút tương tự để yêu cầu thêm các giao dịch vào chuỗi khối. Ngoài chuỗi khối, nút A và nút B có thể có các kênh truyền thông khác (chẳng hạn truyền thông internet chính tắc mà không đi qua các nút 1 và 2). Theo một số phương án, phần mềm chuỗi khối với nút có thể được xem như bắt đầu nút chuỗi khối 1, và nút chuỗi khối 1 vận hành kết thúc phần mềm chuỗi khối.

Mỗi một trong số các nút trên Fig.1 có thể bao gồm bộ xử lý và phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp được tạo cấu hình với các lệnh có thể thực thi bởi bộ xử lý để khiến nút (chẳng hạn bộ xử lý) thực hiện các hoạt động khác nhau để dò tấn công phát lại được mô tả ở đây. Mỗi nút có thể được cài đặt phần mềm (chẳng hạn chương trình giao dịch) và/hoặc phần cứng (chẳng hạn các kết nối có dây hoặc không dây) để truyền thông với các nút khác và/hoặc các thiết bị khác. Chẳng hạn, các thiết bị người dùng như nút A và nút B có thể được cài đặt phần mềm đầu cuối người dùng như ví tiền mã hóa, và các nút chuỗi khối có thể được cài đặt phần mềm xử lý giao dịch chuỗi khối. Các chi tiết tiếp theo của phần cứng và phần mềm nút được mô tả sau với tham chiếu đến các hình vẽ từ Fig.5 đến Fig.7.

Mỗi nút chuỗi khối có thể bao gồm hoặc kết nối với bộ nhớ. Theo một số phương án, bộ nhớ có thể lưu trữ cơ sở dữ liệu mỏ đào (pool). Cơ sở dữ liệu mỏ đào có thể truy nhập được với nhiều nút chuỗi khối theo cách được phân tán. Chẳng hạn, cơ sở dữ liệu mỏ đào có thể được lưu trữ một cách tương ứng trong các bộ nhớ của các nút chuỗi khối. Cơ sở dữ liệu mỏ đào có thể lưu trữ nhiều giao dịch được đệ trình bởi một hoặc nhiều thiết bị người dùng như các nút A và B được kích hoạt bởi các người dùng. Theo một số phương án liên quan đến hệ thống ethereum, sau khi tiếp nhận một yêu cầu giao dịch của một giao dịch chưa được xác nhận, nút chuỗi khối của người nhận có thể thực hiện sự kiểm tra sơ bộ nào đó giao dịch. Chẳng hạn, tham khảo Fig.1, nút 1 có thể thực hiện kiểm tra sơ bộ sau khi tiếp nhận giao dịch từ nút A. Ngay khi được xác nhận, giao dịch có thể được lưu trữ trong cơ sở dữ liệu mỏ đào của nút chuỗi khối của người nhận, mà cũng có thể chuyển tiếp giao dịch tới một hoặc nhiều nút chuỗi khối khác (chẳng hạn nút 3, nút 4) mà lặp lại quá trình được thực hiện bởi nút người nhận. Ngay khi các giao dịch trong cơ sở dữ liệu mỏ đào tương ứng đạt tới mức nhất định, mỗi nút chuỗi khối có thể xác nhận loạt các giao dịch trong cơ sở dữ liệu mỏ đào tương ứng theo các quy tắc đồng thuận hoặc phương pháp khác. Nếu như giao dịch bao gồm hợp đồng chuỗi khối, nút chuỗi khối có thể thực thi hợp đồng chuỗi khối một cách cục bộ. Nút chuỗi khối nhất định mà xác nhận một cách thành công loạt các giao dịch của nó (chẳng hạn, theo các quy tắc đồng thuận) có thể đóng gói các giao dịch để bổ sung vào các bản sao chép cục bộ chuỗi khối của nó và đưa các kết quả tới các nút chuỗi khối khác. Nút chuỗi khối nhất định có thể là nút mà hoàn thành xác nhận thành

công đầu tiên, mà thu thập sự ưu tiên xác nhận, hoặc được xác định dựa trên quy tắc đồng thuận khác. Các nút chuỗi khối khác có thể thực thi các giao dịch một cách cục bộ, các kết quả thực thi xác nhận với một nút khác (chẳng hạn bằng cách thực hiện tính toán băm), và đồng bộ hóa các bản sao chép chuỗi khối của chúng với các bản sao chép của nút chuỗi khối nhất định. Bằng cách cập nhật các bản sao chép cục bộ chuỗi khối, các nút chuỗi khối có thể ghi thông tin này vào trong các bộ nhớ cục bộ. Nếu như sự xác nhận thất bại tại một điểm nào đó, các giao dịch bị từ chối.

Fig.2 là hình vẽ minh họa giao dịch mà với nó việc dò tấn công phát lại được thực hiện theo các phương án thực hiện khác nhau để làm ví dụ.

Theo một số phương án, nút người khởi đầu có thể khởi đầu giao dịch X có 2 ether từ tài khoản có địa chỉ 3df53h (tài khoản A) tới tài khoản có địa chỉ 45wqr1 (tài khoản B). Tài khoản A có 10 ether, và tài khoản B có 1 ether trước khi giao dịch. Giao dịch X có thể được đệ trình bởi nút người khởi đầu (chẳng hạn máy tính, điện thoại di động) với nút chuỗi khối (chẳng hạn nút đầy đủ). Giao dịch X có thể được kết hợp với nhãn thời gian, chẳng hạn thời gian khi giao dịch X được đệ trình bởi nút người khởi đầu thông qua nút chuỗi khối, khi giao dịch X được đệ trình bởi nút chuỗi khối, hoặc khi giao dịch X được tiếp nhận bởi nút chuỗi khối khác mà thực hiện sự xác nhận đồng thuận. Giao dịch X có thể được gọi là giao dịch ứng viên trước khi nó được xác nhận và được thêm vào chuỗi khối. Nút chuỗi khối có thể lưu giao dịch ứng viên X trong cơ sở dữ liệu mỏ đào cùng với các giao dịch ứng viên khác. Nút chuỗi khối có thể lưu nhận dạng (chẳng hạn băm) của giao dịch X vào cơ sở dữ liệu nhận dạng (chẳng hạn bảng băm).

Theo một số phương án, nhiều nút chuỗi khối có thể xác nhận các giao dịch ứng viên của cơ sở dữ liệu mỏ đào theo các quy tắc đồng thuận. Chẳng hạn, các nút chuỗi khối có thể xác nhận nếu như các tài khoản gửi có đủ vốn, nếu như các bên gửi và bên nhận đã ký giao dịch, nếu như lượng giao dịch nằm trong khoảng cho phép, v.v. Nhờ xác nhận đồng thuận, các nút chuỗi khối có thể đồng bộ hóa các cơ sở dữ liệu nhận dạng của chúng để có được toàn bộ các nhận dạng của các giao dịch được lưu trữ trong các cơ sở dữ liệu nhận dạng. Chẳng hạn, mỗi cơ sở dữ liệu nhận dạng có thể lưu trữ các giao dịch trong khoảng thời gian gần đây nhất định. Với việc dò tấn công phát

lại, các nút chuỗi khối có thể xác nhận nếu như nhãn thời gian của giao dịch ứng viên nằm trong khoảng thời gian gần đây, và nếu như vậy, thì lọc giao dịch ứng viên dựa vào cơ sở dữ liệu nhận dạng đối với sự tấn công phát lại.

Nhãn thời gian và các xác nhận nhận dạng có thể được thực hiện ngay sau xác nhận đồng thuận hoặc được thực hiện hai lần: trước và sau khi xác nhận đồng thuận. Nếu như sự phù hợp được thỏa mãn, các nút chuỗi khối có thể đóng gói các giao dịch ứng viên được xác nhận vào trong khối mới để bổ sung vào chuỗi khối. Do đó, khi giao dịch X được thêm vào chuỗi khối, giao dịch X của tài khoản A chuyển 2 ether cho tài khoản B được ghi nhận.

Fig.3 minh họa các bước 300 để dò tấn công phát lại theo các phương án thực hiện khác nhau để làm ví dụ sáng chế. Các bước 300 có thể được thi hành bởi một hoặc nhiều bộ phận cấu thành (chẳng hạn nút A, nút 1, sự kết hợp nút A và nút 1, nút 2, nút i) của hệ thống 100 trên Fig.1. Các hoạt động mô tả dưới đây nhằm mục đích minh họa. Tùy thuộc vào sự thi hành, các bước 300 để làm ví dụ sáng chế có thể bao gồm các bước bổ sung, ít hơn, hoặc lựa chọn được thực hiện theo các thứ tự khác nhau hoặc song song.

Theo các phương án thực hiện khác nhau, như được mô tả trước đây, nhãn thời gian được thêm vào giao dịch, chẳng hạn, dưới dạng Tài khoản/Số dư. Theo một ví dụ, nút người khởi đầu giao dịch (chẳng hạn nút A trên Fig.1) hoặc thiết bị đầu cuối người dùng lựa chọn có thể thêm nhãn thời gian (chẳng hạn thông số nhãn thời gian) vào sự đệ trình giao dịch chưa được xác nhận cho các nút chuỗi khối để xác nhận hợp lệ. Theo cách lựa chọn khác, nút chuỗi khối tiếp nhận giao dịch chưa được xác nhận (chẳng hạn nút 1 trên Fig.1) có thể thêm nhãn thời gian. Nhãn thời gian có thể chính xác đến các mức khác nhau (chẳng hạn đến mức mili giây). Nhờ tăng độ chính xác của nhãn thời gian, các hệ thống và các phương pháp đã bộc lộ có thể hỗ trợ nhiều các giao dịch được khởi đầu bởi một tài khoản trong một đơn vị thời gian hơn. Chẳng hạn, nếu như nhãn thời gian chính xác đến 10ms, các hệ thống và các phương pháp đã bộc lộ có thể hỗ trợ tốt nhất khoảng 100 giao dịch khác nhau được khởi đầu bởi cùng tài khoản được truy nhập trên 100 thiết bị đầu cuối người dùng khác nhau, trong khi việc duy trì các thiết bị này được dự tính như các tấn công phát lại.

Theo một số phương án, khoảng xác nhận hợp lệ có thể được sử dụng để khắc phục ít nhất là các nhược điểm được mô tả ở trên của nonce (số được thêm vào khối băm) tài khoản. Khoảng xác nhận hợp lệ là cửa sổ thời gian trong đó các giao dịch gần đây được lọc với các tấn công phát lại. Khoảng xác nhận hợp lệ có thể được xác định trong mối liên hệ với chuẩn phổ dụng, chẳng hạn trong khoảng thời gian từ nhãn thời gian của khối muộn nhất của chuỗi khối do nhãn thời gian của khối muộn nhất được chấp nhận một cách phổ dụng trong chuỗi khối. Chẳng hạn, khối muộn nhất của chuỗi khối có thể được thêm vào ngày 8/6/2018 lúc 08:42:44 thời gian theo giờ Bắc Kinh, và khoảng xác nhận hợp lệ có thể là hai giờ trước và/hoặc sau thời gian đó. Trước khi xác nhận đồng thuận, thời gian địa phương của nút (chẳng hạn dựa trên đồng hồ nội tại) có thể được sử dụng đan xen. Trước và sau khi xác nhận đồng thuận, nếu như đồng hồ nội tại của nút về cơ bản nhất quán với chuẩn phổ dụng, thời gian địa phương của nút có thể được sử dụng đan xen. Khoảng xác nhận hợp lệ có thể là đủ dài để duy trì hiệu quả dò tấn công phát lại và đủ ngắn để hạn chế yêu cầu lưu trữ dữ liệu. Khoảng xác nhận hợp lệ có thể được bao gồm trong khối nguồn gốc (khối đầu tiên từ trước đến giờ) của chuỗi khối để đảm bảo rằng mỗi nút chuỗi khối chấp thuận và sử dụng cùng khoảng xác nhận hợp lệ. Với khoảng xác nhận hợp lệ, việc dò tấn công phát lại không yêu cầu sự đồng bộ hóa giữa thời gian nút người khởi đầu và thời gian của nút chuỗi khối, cũng không yêu cầu hệ thống định thời giữa các nút chuỗi khối khác nhau. Ngoài ra, các nút chuỗi khối có thể xác nhận cùng giao dịch ứng viên ở các thời điểm khác nhau và vẫn thu thập cùng kết quả.

Theo một số phương án, khi tiếp nhận giao dịch ứng viên, nút chuỗi khối có thể xác nhận hợp lệ nhãn thời gian của giao dịch ứng viên dựa trên khoảng xác nhận hợp lệ. Với sự xác nhận hợp lệ nhãn thời gian thành công và không dò thấy tấn công phát lại, nút chuỗi khối cũng có thể lưu trữ một nhận dạng của giao dịch ứng viên trong khoảng xác nhận hợp lệ. Chẳng hạn, nút chuỗi khối có thể lưu trữ băm của giao dịch đã xác nhận hợp lệ trong bảng băm giao dịch trong bộ nhớ (chẳng hạn vùng nhớ đệm) của nút chuỗi khối. Bộ lưu trữ đệm có thể cho phép truy vấn dữ liệu nhanh từ bảng băm giao dịch, vì vậy tăng hiệu quả giao dịch tổng thể (chẳng hạn tăng số lượng các giao dịch trong một giây). Bảng băm được lưu trữ có thể lưu trữ thông tin trong khoảng thời gian gần đây nhất tương ứng với khoảng xác nhận hợp lệ (chẳng

hạn hai giờ cuối cùng). Nhờ đưa vào khoảng xác nhận hợp lệ, các nút chuỗi khối không phải tìm kiếm toàn bộ chuỗi khối với các tấn công phát lại, vốn thường mất nhiều thời gian nếu tìm kiếm từ đĩa cứng và cũng tăng các khối đang được thêm liên tục vào chuỗi khối. Trái lại, việc tìm kiếm từ bộ nhớ đệm tương ứng với thông tin được thu thập từ khoảng xác nhận hợp lệ có thể cải thiện đáng kể hiệu quả dò tấn công phát lại. Chi tiết các bước được mô tả dưới đây.

Ở bước 301, nút chuỗi khối có thể thu thập giao dịch ứng viên được đệ trình bởi nút người khởi đầu để xác nhận và thêm vào chuỗi khối. Ở bước 302, nút chuỗi khối có thể xác nhận hợp lệ giao dịch nhãn thời gian. Nếu như xác nhận hợp lệ thành công, bước 303 được thực hiện, và nút chuỗi khối xác định nếu như băm giao dịch của giao dịch ứng viên có trong bảng băm. Bảng băm có thể lưu trữ các băm của toàn bộ các giao dịch trong khoảng thời gian tương ứng với khoảng xác nhận hợp lệ. Nếu như băm giao dịch của giao dịch ứng viên đã sẵn sàng trong bảng băm, nó chỉ thị rằng giao dịch ứng viên có thể liên quan đến tấn công phát lại và sự xác nhận hợp lệ thất bại. Nếu khác, xác nhận hợp lệ thành công ở bước 304, và nút chuỗi khối lưu băm giao dịch vào bảng băm ở bước 305. Nếu như việc xác nhận hợp lệ ở bước 302 thất bại, bước 306 được thực hiện, và một thông báo lỗi có thể được trả về thiết bị đầu cuối người dùng đã đệ trình giao dịch. Nếu như việc xác định ở bước 303 thất bại, bước 306 được thực hiện, và giao dịch có nhãn thời gian sớm nhất được xử lý như một giao dịch xác thực, và toàn bộ các giao dịch sau đó được xem như các tấn công phát lại tiềm tàng và được hủy bỏ. Các băm của các giao dịch sau đó cũng có thể được lọc ra khỏi bảng băm.

Theo một số phương án, đối với thỏa thuận đồng thuận mà cho phép mỗi nút khởi đầu khai thác giao dịch (xác nhận giao dịch theo các quy tắc đồng thuận), sự tấn công phát lại có thể nhắm vào các nút chuỗi khối khác nhau, và các nút chuỗi khối đã bị ngắm đích không thể dò được sự đe dọa trước khi thực hiện sự xác nhận giao dịch theo các quy tắc đồng thuận. Vì vậy, sau khi các nút chuỗi khối thực hiện sự xác nhận giao dịch theo các quy tắc đồng thuận, các nút chuỗi khối có thể thu thập thông tin đầy đủ của bảng băm và thực hiện các bước từ 302 đến 305 để lọc các tấn công phát lại. Vì vậy, các bước từ 302 đến 305 có thể được thực hiện sau khi nút chuỗi khối thực hiện sự xác nhận giao dịch theo các quy tắc đồng thuận. Tuy nhiên, các bước từ 302

đến 305 có thể được thực hiện bổ sung trước khi nút chuỗi khối thực hiện sự xác nhận giao dịch theo các quy tắc đồng thuận. Bằng cách thực hiện các bước từ 302 đến 305 trước khi xác nhận giao dịch, có thể loại trừ sơ bộ các tấn công phát lại tiềm tàng. Nghĩa là, các bước từ 302 đến 305 có thể được thực hiện (1) cả trước lẫn sau hoặc (2) sau khi xác nhận giao dịch theo các quy tắc đồng thuận. Nếu được thực hiện ngay khi hoặc hai lần, bước 302 và bước 303 có thể được thực hiện theo thứ tự bất kỳ mà không ảnh hưởng đến các kết quả.

Fig.4A minh họa lưu đồ thể hiện phương pháp 400 để dò tấn công phát lại để làm ví dụ sáng chế theo các phương án thực hiện khác nhau của phần mô tả này. Phương pháp 400 có thể được thi hành bởi một hoặc nhiều bộ phận cấu thành (chẳng hạn nút 1, sự kết hợp nút A và nút 1, nút 2, …, nút i) của hệ thống 100 trên Fig.1. Phương pháp 400 có thể được thi hành bởi một hoặc nhiều nút chuỗi khối. Phương pháp 400 có thể được thi hành bởi hệ thống hoặc thiết bị (chẳng hạn máy tính, máy chủ). Hệ thống hoặc thiết bị 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 (chẳng hạn một hoặc nhiều bộ nhớ) được kết nối với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để khiến hệ thống hoặc thiết bị (chẳng hạn bộ xử lý) thực hiện phương pháp 400. Các hoạt động của phương pháp 400 mô tả dưới đây chỉ nhằm mục đích minh họa. Tùy thuộc vào sự thi hành, phương pháp 400 để làm ví dụ sáng chế có thể bao gồm các bước bổ sung, ít hơn, hoặc lựa chọn được thực hiện theo các thứ tự khác nhau hoặc song song.

Khối 441 bao gồm bước: thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối, giao dịch ứng viên đã thu thập bao gồm nhãn thời gian.

Khối 442 bao gồm bước: xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ và nếu như nhận dạng (chẳng hạn giá trị băm hoặc nhận dạng lựa chọn) của giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng (chẳng hạn bảng băm).

Khối 443 bao gồm bước: đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

Các điều kiện, các phương án, và các ví dụ khác nhau của phương pháp 450 được mô tả dưới đây có thể áp dụng tương tự cho phương pháp 400.

Fig.4B minh họa lưu đồ thể hiện phương pháp làm ví dụ 450 để dò tấn công phát lại, theo các phương án thực hiện khác nhau của phần mô tả này. Phương pháp 450 có thể được thi hành bởi một hoặc nhiều bộ phận cấu thành (chẳng hạn nút 1, sự kết hợp nút A và nút 1, nút 2, …, nút i) của hệ thống 100 trên Fig.1. Phương pháp 450 có thể được thi hành bởi một hoặc nhiều nút chuỗi khối. Phương pháp 450 có thể được thi hành bởi hệ thống hoặc thiết bị (chẳng hạn máy tính, máy chủ). Hệ thống hoặc thiết bị 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 (chẳng hạn một hoặc nhiều bộ nhớ) được kết nối với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để khiến hệ thống hoặc thiết bị (chẳng hạn bộ xử lý) thực hiện phương pháp 450. Các hoạt động của phương pháp 450 mô tả dưới đây nhằm mục đích minh họa. Tùy thuộc vào sự thi hành, phương pháp 450 để làm ví dụ sáng chế có thể bao gồm các bước bổ sung, ít hơn, hoặc lựa chọn được thực hiện theo các thứ tự khác nhau hoặc song song.

Khối 451 bao gồm bước: thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối. Giao dịch ứng viên đã thu thập có thể bao gồm nhãn thời gian. Theo một số phương án, chuỗi khối có thể là dựa trên kiểu Số dư/Tài khoản (chẳng hạn hệ thống ethereum, hệ thống BFT như hệ thống Dung sai lỗi Byzantin thực tế (PBFT - Practical Byzantine Fault Tolerance), Hệ thống HoneyBadger hoặc Hashgraph), nhưng với hệ thống đã bộc lộ thay thế việc sử dụng nonce tài khoản (nếu như có) để dò tấn công phát lại.

Theo một số phương án, giao dịch ứng viên đã thu thập bao gồm nhãn thời gian. Giá trị băm được xác định ít nhất dựa trên nhãn thời gian và thông tin giao dịch, giá trị băm có tác dụng như sự nhận dạng. Sau khi thu thập ít nhất một giao dịch ứng viên và trước khi xác nhận nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, phương pháp còn bao gồm các bước: xác nhận nhận dạng bằng cách xác nhận giá trị băm ít nhất dựa trên nhãn thời gian và thông tin giao dịch. Chẳng hạn, giao dịch ứng viên có thể bao gồm một hoặc nhiều thông số như nhãn thời gian,

từ (địa chỉ người gửi giao dịch), đến (địa chỉ người nhận giao dịch), giá trị (khoản giao dịch), dữ liệu (hợp đồng chuỗi khối nếu có), thanh toán giao dịch (chẳng hạn giới hạn năng lượng Gas Limit, giá trị năng lượng Gas Value), giá trị băm (giá trị băm để sử dụng như nhận dạng đồng nhất giao dịch), và/hoặc thông tin khác (chẳng hạn chữ ký (chứng thực ký bởi người gửi)). Các thông số này có thể được gọi chung là khối cấu trúc giao dịch. Các thông số bao gồm ngoài nhãn thời gian (và chữ ký) có thể được gọi là thông tin giao dịch. Giá trị băm có thể được xác định (chẳng hạn bởi nút như nút A mà đã khởi đầu giao dịch ứng viên) dựa trên thông tin giao dịch, chẳng hạn, thông qua chức năng băm lấy nhãn thời gian và thông tin giao dịch như các giá trị đầu vào. Để xác nhận giá trị băm ít nhất dựa trên nhãn thời gian và thông tin giao dịch, nút chuỗi khối (chẳng hạn nút 1) mà thu nhận giao dịch ứng viên có thể tính toán lại chức năng băm với các giá trị đầu vào để kiểm tra dựa vào giá trị băm.

Theo một số phương án, giao dịch ứng viên bao gồm nhãn thời gian và thông tin giao dịch. Sau khi thu thập ít nhất một giao dịch ứng viên và trước khi xác nhận nếu như nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, phương pháp còn bao gồm các bước: xác định giá trị băm ít nhất dựa trên nhãn thời gian và thông tin giao dịch, giá trị băm có tác dụng như nhận dạng. Chẳng hạn, giao dịch ứng viên có thể bao gồm một hoặc nhiều thông số như nhãn thời gian, từ, đến, giá trị, dữ liệu, thanh toán giao dịch, và/hoặc thông tin khác. Thông số được bao gồm ngoài nhãn thời gian có thể được gọi là thông tin giao dịch. Giá trị băm có thể được xác định (chẳng hạn bởi nút chuỗi khối như nút 1 mà đã tiếp nhận giao dịch ứng viên) dựa trên nhãn thời gian và thông tin giao dịch, chẳng hạn, thông qua chức năng băm lấy nhãn thời gian và thông tin giao dịch như các giá trị đầu vào.

Theo một số phương án, nhãn thời gian được tạo cấu hình bởi thiết bị đầu cuối người dùng mà đã khởi đầu ít nhất một giao dịch ứng viên; và thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối bao gồm tiếp nhận giao dịch ứng viên từ thiết bị đầu cuối người dùng. Chẳng hạn, thiết bị đầu cuối người dùng có thể là nút A trên Fig.1, mà truyền giao dịch ứng viên tới nút 1. Nút A có thể thêm nhãn thời gian vào giao dịch ứng viên trước khi truyền giao dịch ứng viên tới nút 1.

Theo một số phương án, nhãn thời gian được tạo cấu hình bởi nút chuỗi khối; và thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối bao gồm: tiếp nhận ít nhất một giao dịch được khởi đầu từ thiết bị đầu cuối người dùng; và thêm nhãn thời gian vào giao dịch được khởi đầu để thu thập ít nhất một giao dịch ứng viên. Chẳng hạn, thiết bị đầu cuối người dùng có thể là nút A trên Fig.1, mà truyền giao dịch ứng viên tới nút 1. Nút A không thể thêm nhãn thời gian vào giao dịch ứng viên, và nút 1 có thể thêm nhãn thời gian vào giao dịch ứng viên được tiếp nhận. Khi nút chuỗi khối thứ nhất tiếp nhận giao dịch ứng viên, nút 1 có thể thêm nhãn thời gian dựa trên đồng hồ nội tại của nó hoặc nguồn thời gian lựa chọn. Ngay khi các nút chuỗi khối khác tiếp nhận muộn hơn giao dịch ứng viên, các nút chuỗi khối khác có thể thu thập nhãn thời gian được thêm bởi nút 1.

Khối 452 bao gồm bước: xác nhận nếu như nhận dạng (chẳng hạn giá trị băm hoặc nhận dạng lựa chọn) của giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng (chẳng hạn bảng băm của cơ sở dữ liệu mỏ đào), cơ sở dữ liệu nhận dạng bao gồm nhiều nhận dạng trong khoảng xác nhận hợp lệ.

Theo một số phương án, xác nhận nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng bao gồm: xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ và nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng. Sự xác nhận nhãn thời gian và sự xác nhận nhận dạng có thể được thực hiện theo thứ tự bất kỳ. Cơ sở dữ liệu nhận dạng có thể được lưu trữ trong phương tiện lưu trữ. Cơ sở dữ liệu nhận dạng có thể được lưu trữ trong bộ nhớ đệm.

Theo một số phương án, cơ sở dữ liệu nhận dạng bao gồm thông tin về các giao dịch với các nhãn thời gian nằm trong khoảng thời gian gần đây tương ứng với khoảng xác nhận hợp lệ. Chẳng hạn, mỗi nút chuỗi khối có thể duy trì cơ sở dữ liệu nhận dạng để lưu trữ các băm của các giao dịch ứng viên được tiếp nhận bởi nút chuỗi khối cho hai giờ từ nhãn thời gian của khối muộn nhất của chuỗi khối. Các nút chuỗi khối có thể đồng bộ hóa các cơ sở dữ liệu nhận dạng của chúng tại mỗi xác nhận đồng thuận để mỏ đào các băm được lưu trữ. Sau mỗi xác nhận đồng thuận, khối mới có thể được thêm vào chuỗi khối, và nhãn thời gian của khối muộn nhất của chuỗi khối tiến triển

theo thời gian. Chẳng hạn, khối muộn nhất của chuỗi khối có thể được thêm lúc 5 giờ sáng của ngày nhất định, và khoảng xác nhận hợp lệ có thể là từ 5 giờ sáng đến 7 giờ sáng của ngày nhất định này. Sau đó, sau khi khối mới được thêm lúc 7 giờ sáng, khoảng xác nhận hợp lệ trở thành từ 7 giờ sáng đến 9 giờ sáng của ngày nhất định. Do đó, các băm trong cơ sở dữ liệu nhận dạng có thể được cập nhật bằng cách thêm các băm trong khoảng xác nhận hợp lệ và/hoặc loại bỏ các băm ra ngoài khoảng xác nhận hợp lệ. Mỗi băm có thể được kết hợp với nhãn thời gian tương ứng để xác định nếu như băm nằm trong hoặc nằm ngoài khoảng xác nhận hợp lệ.

Theo một số phương án, khoảng xác nhận hợp lệ được dựa trên nhãn thời gian khác của khối muộn nhất của chuỗi khối (chẳng hạn nhãn thời gian khác mà được chấp thuận phổ dụng bởi mạng chuỗi khối + khoảng xác nhận hợp lệ từ nhãn thời gian khác); và khoảng xác nhận hợp lệ được bao gồm trong khối nguồn gốc của chuỗi khối.

Theo một số phương án, khoảng xác nhận hợp lệ được dựa trên đồng hồ nội tại của nút chuỗi khối mà thực hiện xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ.

Khối 453 bao gồm bước: đáp ứng với việc xác định rằng nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

Theo một số phương án, đáp ứng với việc xác định rằng nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại bao gồm đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

Theo một số phương án, phương pháp 450 còn bao gồm các bước: đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, thêm nhận dạng vào cơ sở dữ liệu nhận dạng.

Theo một số phương án, phương pháp 450 còn bao gồm các bước: đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, thêm giao dịch ứng viên vào vùng nhớ đệm

để lưu trữ các giao dịch ứng viên. Chẳng hạn, vùng nhớ đệm có thể là cơ sở dữ liệu mỏ đào. Vùng nhớ đệm cũng có thể lưu trữ cơ sở dữ liệu nhận dạng (chẳng hạn bảng băm).

Theo một số phương án, phương pháp 450 còn bao gồm các bước: đáp ứng với việc xác định rằng nhãn thời gian không nằm trong khoảng xác nhận hợp lệ, trả lại thông báo lỗi tới thiết bị tính toán đã đệ trình giao dịch ứng viên. Giao dịch ứng viên có thể hoặc không thể được kết hợp với tấn công phát lại, mà là giao dịch không hợp lệ do nó nằm ngoài khoảng xác nhận hợp lệ (chẳng hạn quá lâu từ thời điểm hiện tại). Vì vậy, giao dịch ứng viên bị từ chối thêm vào chuỗi khối.

Theo một số phương án, phương pháp 450 còn bao gồm bước: đáp ứng với việc xác định rằng nhận dạng có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên được kết hợp với tấn công phát lại. Vì vậy, giao dịch ứng viên bị từ chối thêm vào chuỗi khối.

Phương pháp 450 có thể được thi hành trong các hệ thống chuỗi khối khác nhau như hệ thống ethereum, hệ thống PBFT, hệ thống HoneyBadger hoặc Hashgraph, v.v. Theo một số phương án, phương pháp còn bao gồm các bước: thực hiện sự xác nhận đồng thuận, trong đó giao dịch ứng viên được bao gồm trong sự xác nhận đồng thuận nếu như giao dịch ứng viên được xác định là không được kết hợp với tấn công phát lại. Chẳng hạn, trong hệ thống ethereum, nhãn thời gian và xác nhận nhận dạng có thể được thực hiện trước khi các nút đồng thuận thực hiện một vòng tròn xác nhận đồng thuận. Trong các hệ thống chuỗi khối đã bộc lộ bất kỳ, việc thực hiện xác nhận đồng thuận có thể không có khả năng dò tấn công phát lại, và các phương pháp được bộc lộ có thể đạt được việc dò tấn công phát lại.

Theo một số phương án, phương pháp 450 còn bao gồm các bước: đồng bộ hóa cơ sở dữ liệu nhận dạng với một hoặc nhiều nút chuỗi khối khác; xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ và nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng được đồng bộ hóa; đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng được đồng bộ hóa, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại; và đáp ứng với việc xác định

rằng sự nhận dạng có trong cơ sở dữ liệu nhận dạng được đồng bộ hóa, xác định rằng giao dịch ứng viên được kết hợp với tấn công phát lại. Chẳng hạn, trong hệ thống ethereum, theo cách tùy chọn, nhãn thời gian và xác nhận nhận dạng có thể được thực hiện lại sau khi các nút đồng thuận thực hiện một vòng tròn sự xác nhận đồng thuận. Nhờ xác nhận đồng thuận, cơ sở dữ liệu nhận dạng và/hoặc cơ sở dữ liệu mỏ đào có thể được đồng bộ hóa giữa các nút chuỗi khối.

Theo một số phương án, trước khi thu thập ít nhất một giao dịch ứng viên, phương pháp 450 còn bao gồm bước: đồng bộ hóa cơ sở dữ liệu nhận dạng với một hoặc nhiều nút chuỗi khối khác. Chẳng hạn, trong hệ thống PBFT, một nút chuỗi khối (chẳng hạn nút chính) có thể đảm nhận khởi đầu xác nhận đồng thuận. Sau khi tiếp nhận các giao dịch ứng viên, các nút chuỗi khối không phải chính (chẳng hạn các nút dự phòng) có thể chuyển tiếp các giao dịch ứng viên tới nút chính. Nút chính có thể thực hiện phương pháp 450 sau khi tiếp nhận các giao dịch ứng viên và trước khi việc xác nhận đồng thuận được thực hiện. Sau khi việc xác nhận đồng thuận được thực hiện, các nút không phải chính có thể đồng bộ hóa danh sách các giao dịch ứng viên của chúng với nút chính nhằm thực thi các giao dịch ứng viên. Vì vậy, các nút không phải chính có thể hoặc không thể thực hiện phương pháp 450 sau khi xác nhận đồng thuận và trước khi thực thi các giao dịch ứng viên.

Với ví dụ khác, trong hệ thống HoneyBadger hoặc Hashgraph, mỗi nút chuỗi khối không thể chuyển tiếp giao dịch ứng viên mà nó tiếp nhận. Mỗi nút chuỗi khối có thể khởi đầu xác nhận đồng thuận cho giao dịch ứng viên được tiếp nhận. Vì vậy, nếu như giao dịch xác thực và giao dịch tấn công phát lại được gửi lần lượt tới hai nút chuỗi khối khác nhau mà mỗi nút thực hiện phương pháp 450, chúng có thể qua cả hai nút này. Để dò tấn công phát lại, sau khi sự xác nhận đồng thuận được thực hiện, các nút chuỗi khối có thể chia sẻ các giao dịch ứng viên thông qua sự xác nhận đồng thuận và sau đó thực hiện lại phương pháp 450. Nghĩa là, các nút chuỗi khối trong hệ thống HoneyBadger hoặc Hashgraph có thể đồng bộ hóa cơ sở dữ liệu nhận dạng của chúng và/hoặc các cơ sở dữ liệu mỏ đào của chúng và thực hiện phương pháp 450. Với phương pháp 450 được thực hiện sau khi xác nhận đồng thuận, các nút chuỗi khối có thể thêm các giao dịch mới vào chuỗi khối (chẳng hạn bằng cách ghi chuỗi khối đã cập nhật vào trong các bộ nhớ lưu trữ cục bộ).

Như vậy, các hệ thống và các phương pháp được bộc lộ có thể làm giảm hoặc khắc phục các nhược điểm trong công nghệ hiện có để đạt được việc dò tấn công phát lại mạnh mẽ. Bằng cách thay thế nonce tài khoản với sự kết hợp nhãn thời gian và các xác nhận nhận dạng đã bộc lộ, các thiết bị đầu cuối người dùng không cần truy vấn nút chuỗi khối cho các trị nonce. Vì vậy, các chi phí truyền thông giữa các thiết bị đầu cuối người dùng và các nút chuỗi khối được giảm.

Với trạng thái (1), tài khoản gửi cả giao dịch thứ nhất lẫn giao dịch thứ hai kế tiếp có cùng phí giao dịch tới cùng nút chuỗi khối. Tuy nhiên, nếu như nút chuỗi khối tiếp nhận giao dịch thứ hai trước giao dịch thứ nhất do sự truyền gói dữ liệu mạng không theo thứ tự, nút chuỗi khối sẽ thực thi giao dịch thứ hai và sau đó là giao dịch thứ nhất, gây ra các thất bại thực thi cho cả hai giao dịch do không phù hợp với cơ chế nonce tài khoản. Các hệ thống và các phương pháp được bộc lộ có thể thay thế cơ chế nonce tài khoản với nhãn thời gian và/hoặc xác nhận hợp lệ nhận dạng, khiến cho các giao dịch hợp lệ từ cùng tài khoản không thể phải được thực thi theo thứ tự định trước. Nghĩa là, thứ tự tiếp nhận các giao dịch hợp lệ từ cùng tài khoản sẽ không ngăn cản sự thực thi thành công các giao dịch.

Với trạng thái (2), tài khoản gửi giao dịch thứ nhất và giao dịch thứ hai kế tiếp tới cùng nút chuỗi khối, với giao dịch thứ hai có phí giao dịch cao hơn. Để tăng tối đa lợi nhuận, các nút chuỗi khối có thể được lập trình để ưu tiên thực thi giao dịch thứ hai và sau đó là giao dịch thứ nhất, gây ra các thất bại thực thi cho cả hai giao dịch do không phù hợp với cơ chế nonce tài khoản. Các hệ thống và các phương pháp được bộc lộ có thể ngăn ngừa vấn đề này do, tương tự với trạng thái (1), thứ tự tiếp nhận các giao dịch hợp lệ từ cùng tài khoản sẽ không ngăn cản sự thực thi thành công các giao dịch.

Ở trạng thái (3), tài khoản gửi song song các giao dịch khác nhau từ các thiết bị đầu cuối người dùng khác nhau, nhưng các giao dịch này sẽ có cùng giá trị nonce tài khoản. Kết quả là, tối đa một trong số các giao dịch sẽ được xử lý thành công dưới cơ chế nonce tài khoản. Các hệ thống và các phương pháp được bộc lộ có thể ngăn ngừa vấn đề này và cho phép thực thi thành công toàn bộ các giao dịch, do nonce tài khoản bị sụt giảm. Ngoài ra, như được mô tả trước đây, độ chính xác của nhãn thời gian có

thể hỗ trợ việc thực thi số lượng lớn các giao dịch được khởi đầu bởi cùng tài khoản gần như đóng trong thời gian trước khi khối mới được thêm.

Thêm vào đó, việc lọc sự tấn công phát lại trước và sau khi (hoặc ngay sau) xác nhận giao dịch ứng viên theo các quy tắc đồng thuận của chuỗi khối có thể giảm gánh nặng của xác nhận đồng thuận gốc mà bao gồm xác nhận nonce tài khoản. Việc sử dụng khoảng xác nhận hợp lệ giảm đáng kể quy mô của cơ sở dữ liệu để tìm kiếm từ đó và ngăn ngừa nhu cầu tìm kiếm toàn bộ chuỗi khối. Vì vậy, cơ sở dữ liệu nhận dạng cho phép lọc sự tấn công phát lại theo cách có hiệu quả cao và chi phí thấp. Hơn nữa, việc kết hợp nhãn thời gian với khoảng xác nhận hợp lệ cho phép đệ trình nhiều giao dịch từ cùng tài khoản theo thứ tự bất kỳ mà không gây ra việc ngắt xử lý giao dịch. Ngoài ra, khoảng xác nhận hợp lệ này ngăn ngừa yêu cầu các sự đồng bộ hóa giữa các thiết bị đầu cuối người dùng và các nút chuỗi khối, và các nút chuỗi khối có thể xác nhận cùng giao dịch ở các thời điểm khác nhau để đạt được cùng kết quả xác nhận hợp lệ.

Các công nghệ được mô tả ở đây được thi hành bởi một hoặc nhiều thiết bị tính toán chuyên dụng. Các thiết bị tính toán chuyên dụng có thể là các hệ thống máy tính để bàn, các hệ thống máy tính chủ, các hệ thống máy tính xách tay, các thiết bị cầm tay, các thiết bị nối mạng hoặc thiết bị bất kỳ khác hoặc sự kết hợp các thiết bị có đưa vào mạch logic được nối cứng và/hoặc mạch logic chương trình để thi hành các công nghệ. (Các) thiết bị tính toán nói chung được điều khiển và điều phối bởi phần mềm hệ điều hành. Các hệ điều hành thông thường điều khiển và lập lịch biểu các quá trình máy tính để thực thi, thực hiện quản lý bộ nhớ, tạo hệ thống tệp, nối mạng, các dịch vụ nhập/xuất I/O, và tạo chức năng giao diện người dùng, như giao diện đồ họa người dùng (graphical user interface, "GUI"), trong một số chức năng khác.

Fig.5 minh họa sơ đồ khối của hệ thống máy tính 550 làm ví dụ sáng chế dò tấn công phát lại, theo các phương án thực hiện khác nhau. Hệ thống 550 có thể là sự thi hành để làm ví dụ sáng chế của nút 1, sự kết hợp nút A và nút 1, nút 2, …, nút i của hệ thống 100 trên Fig.1 hoặc thiết bị tương tự. Phương pháp 400 có thể được thi hành bởi hệ thống máy tính 550. Hệ thống máy tính 550 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

(chẳng hạn một hoặc nhiều bộ nhớ) được kết nối với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để khiến hệ thống hoặc thiết bị (chẳng hạn bộ xử lý) thực hiện phương pháp 400. Hệ thống máy tính 550 có thể bao gồm các khối/các môđun khác nhau tương ứng với các lệnh (chẳng hạn các lệnh phần mềm). Theo một số phương án, hệ thống máy tính 550 có thể bao gồm môđun thu thập thứ nhất 551 được tạo cấu hình để thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối, giao dịch ứng viên đã thu thập bao gồm nhãn thời gian; môđun xác nhận thứ nhất 552 được tạo cấu hình để xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ và nếu như sự nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng; và môđun xác định thứ nhất 553 được tạo cấu hình để, đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

Fig.6 minh họa sơ đồ khối của hệ thống máy tính 560 làm ví dụ sáng chế để dò tấn công phát lại, theo các phương án thực hiện khác nhau. Hệ thống 560 có thể là sự thi hành để làm ví dụ sáng chế của nút 1, sự kết hợp nút A và nút 1, nút 2, …, nút i của hệ thống 100 trên Fig.1 hoặc thiết bị tương tự. Phương pháp 450 có thể được thi hành bởi hệ thống máy tính 560. Hệ thống máy tính 560 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 (chẳng hạn một hoặc nhiều bộ nhớ) được kết nối với một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để khiến hệ thống hoặc thiết bị (chẳng hạn bộ xử lý) thực hiện phương pháp 450. Hệ thống máy tính 560 có thể bao gồm các khối/các môđun khác nhau tương ứng với các lệnh (chẳng hạn các lệnh phần mềm). Theo một số phương án, hệ thống máy tính 560 có thể bao gồm môđun thu thập thứ hai 561 được tạo cấu hình để thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối; môđun xác nhận thứ hai 562 được tạo cấu hình để xác nhận nếu như việc nhận dạng giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, cơ sở dữ liệu nhận dạng gồm các nhận dạng trong khoảng xác nhận hợp lệ; và môđun xác nhận thứ hai 563 được tạo cấu hình để, đáp ứng với việc xác định rằng nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

Fig.7 là sơ đồ khối minh họa hệ thống máy tính 700 ngay khi các phương án bất kỳ được mô tả ở đây có thể được thi hành. Hệ thống 700 có thể được thi hành ở nút bất kỳ trong số các nút được mô tả ở đây và được tạo cấu hình để thực hiện các bước tương ứng để dò tấn công phát lại. Hệ thống máy tính 700 bao gồm buýt 702 hoặc có chế truyền thông khác để truyền thông tin, một hoặc nhiều bộ xử lý phần cứng 704 được kết nối với buýt 702 để xử lý thông tin. (Các) bộ xử lý phần cứng 704 có thể là, chẳng hạn, một hoặc nhiều bộ vi xử lý chuyên dụng.

Hệ thống máy tính 700 cũng bao gồm bộ nhớ chính 706, như bộ nhớ truy cập ngẫu nhiên (bộ nhớ truy cập ngẫu nhiên RAM), vùng nhớ đệm và/hoặc các thiết bị lưu trữ động khác, được kết nối với buýt 702 để lưu trữ thông tin và các lệnh có thể thực thi bởi (các) bộ xử lý 704. Bộ nhớ chính 706 cũng có thể được sử dụng để lưu trữ các thay đổi tạm thời hoặc thông tin trung gian khác trong quá trình thực thi các lệnh có thể thực thi bởi (các) bộ xử lý 704. Các lệnh này, khi được lưu trữ trong các phương tiện lưu trữ có thể truy cập vào (các) bộ xử lý 704, đưa hệ thống máy tính 700 thành máy chuyên dụng được tùy chỉnh để thực hiện các hoạt động được xác định trong các lệnh. Hệ thống máy tính 700 còn bao gồm bộ nhớ chỉ đọc (ROM) 708 hoặc thiết bị lưu trữ tĩnh khác được kết nối với buýt 702 để lưu trữ thông tin tĩnh và các lệnh cho (các) bộ xử lý 704. Thiết bị lưu trữ 710, như đĩa từ, đĩa quang học, hoặc ổ đĩa USB (Ổ đĩa flash), v.v., được trang bị và được kết nối với buýt 702 để lưu trữ thông tin và các lệnh.

Hệ thống máy tính 700 có thể thi hành các công nghệ được mô tả ở đây bằng cách sử dụng mạch logic được nối cứng tùy biến, một hoặc nhiều mạch tích hợp chuyên dụng ASIC hoặc mảng cổng lập trình được dạng trường FPGA, mạch logic chương trình và/hoặc phần mềm kết hợp với hệ thống máy tính tạo ra hoặc lập trình hệ thống máy tính 700 thành máy chuyên dụng. Theo một phương án thực hiện, các hoạt động, các phương pháp, và các quá trình được mô tả ở đây được thực hiện bởi hệ thống máy tính 700 đáp ứng với (các) bộ xử lý 704 thực thi một hoặc nhiều dãy của một hoặc nhiều lệnh chứa trong bộ nhớ chính 706. Các lệnh này có thể được ghi vào trong bộ nhớ chính 706 từ phương tiện lưu trữ khác, như thiết bị lưu trữ 710. Việc thực thi các dãy lệnh chứa trong bộ nhớ chính 706 khiến (các) bộ xử lý 704 thực hiện các

bước quá trình được mô tả ở đây. Theo các phương án lựa chọn, hệ mạch điện nối cứng có thể được sử dụng thay cho hoặc kết hợp với các lệnh phần mềm.

Bộ nhớ chính 706, ROM 708, và/hoặc thiết bị 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, khi sử dụng ở đây liên quan đến các phương tiện mà lưu trữ dữ liệu và/hoặc các lệnh khiến máy vận hành theo dạng thức cụ thể, các phương tiện loại trừ các tín hiệu không chuyển tiếp. Các phương tiện không chuyển tiếp này có thể bao gồm các phương tiện bất biến và/hoặc các phương tiện khả biến. Các phương tiện bất biến bao gồm, chẳng hạn, đĩa từ hoặc đĩa quang, như thiết bị lưu trữ 710. Các phương tiện khả biến bao gồm bộ nhớ động, như bộ nhớ chính 706. Các dạng phổ biến của các phương tiện không chuyển tiếp bao gồm, chẳng hạn, đĩa mềm, đĩa lưu động, đĩa cứng, đĩa thể rắn, băng từ, hoặc phương tiện lưu trữ dữ liệu từ tính khác bất kỳ, CD-ROM, phương tiện lưu trữ dữ liệu quang học khác bất kỳ, phương tiện vật lý bất kỳ với các mẫu hình lỗ, bộ nhớ truy cập ngẫu nhiên RAM, bộ nhớ chỉ đọc lập trình được PROM, và bộ nhớ chỉ đọc có thể ghi lại được chương trình EPROM, bộ nhớ chỉ đọc nhanh có thể ghi lại được chương trình FLASH-EPROM, bộ nhớ truy cập ngẫu nhiên có khả năng lưu trữ dữ liệu khi bị mất điện NVRAM, vi mạch nhớ hoặc hộp nhớ bất kỳ khác, và các phiên bản nối mạng của chúng.

Hệ thống máy tính 700 cũng bao gồm giao diện mạng 718 được kết nối với buýt 702. Giao diện mạng 718 cung cấp sự truyền dữ liệu hai chiều kết nối với một hoặc nhiều liên kết mạng được kết nối với một hoặc nhiều mạng cục bộ. Chẳng hạn, giao diện mạng 718 có thể là thẻ mạng số với dịch vụ tích hợp (ISDN), môđem cáp, môđem vệ tinh, hoặc môđem để tạo kết nối truyền dữ liệu với kiểu đường dây điện thoại tương ứng. Như ví dụ khác, giao diện mạng 718 có thể là thẻ mạng cục bộ (local area network, LAN) để tạo kết nối truyền dữ liệu tới LAN tương hợp (hoặc linh kiện mạng diện rộng WAN truyền thông với WAN). Các liên kết không dây cũng có thể được thi hành. Theo cách thi hành bất kỳ, giao diện mạng 718 gửi và tiếp nhận các tín hiệu điện, điện từ hoặc quang mang các chuỗi dữ liệu số biểu thị các dạng thông tin khác nhau.

Hệ thống máy tính 700 có thể gửi các thông báo và nhận dữ liệu, gồm mã chương trình, thông qua (các) mạng, liên kết mạng và giao diện mạng 718. Trong ví dụ Internet, máy chủ có thể truyền mã yêu cầu cho lập trình ứng dụng thông qua Internet, nhà cung cấp dịch vụ Internet ISP, mạng cục bộ và giao diện mạng 718.

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

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

Các dấu hiệu và các quá trình khác nhau được mô tả trên đây có thể được sử dụng một cách độc lập với nhau, hoặc có thể được kết hợp theo các cách khác nhau. Tất cả các kết hợp và các kết hợp phụ có thể có được dự tính nằm trong phạm vi của phần mô tả này. Thêm vào đó, các khối phương pháp hoặc quá trình nhất định có thể được lược bỏ trong một số cách thi hành. Các phương pháp và các quá trình được mô tả ở đây cũng không bị hạn chế ở trình tự cụ thể bất kỳ, và các khối hoặc các trạng thái liên quan đến điều đó có thể được thực hiện theo các trình tự thích hợp khác. Chẳng hạn, các khối hoặc các trạng thái được mô tả có thể được thực hiện theo thứ tự khác với nội dung đã được bộc lộ cụ thể, hoặc nhiều khối hoặc trạng thái có thể được kết hợp trong một khối hoặc trạng thái. Các khối hoặc các trạng thái để làm ví dụ sáng chế có thể được thực hiện nối tiếp, song song, hoặc theo một số cách khác. Các khối hoặc các trạng thái có thể được thêm vào hoặc loại bỏ ra khỏi các phương án được bộc lộ để làm ví dụ sáng chế. Các hệ thống và bộ phận cấu thành để làm ví dụ sáng chế được mô tả ở đây có thể được tạo cấu hình khác với được mô tả. Chẳng hạn, các bộ phận có thể được thêm vào, loại bỏ ra khỏi, hoặc được bố trí lại so với các phương án được bộc lộ để làm ví dụ sáng chế.

Các hoạt động khác nhau của các phương pháp để làm ví dụ sáng chế được mô tả ở đây có thể được thực hiện, ít nhất một phần, bởi thuật toán. Thuật toán có thể được

bao gồm trong các mã chương trình hoặc các lệnh được lưu trữ trong bộ nhớ (chẳng hạn các 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 tự học của máy. Theo một số phương án, thuật toán tự học của máy không thể là chương trình chi tiết của máy tính để thực hiện chức năng, nhưng có thể học từ dữ liệu hướng dẫn để tạo kiểu tiên đoán vốn thực hiện chức năng.

Các hoạt động khác nhau của các phương pháp để làm ví dụ sáng chế được mô tả ở đây có thể được thực hiện, ít nhất một phần, bởi một hoặc nhiều bộ xử lý được tạo cấu hình tạm thời (chẳng hạn bởi phần mềm) hoặc được tạo cấu hình cố định để thực hiện các hoạt động thích hợp. Cho dù là có được tạo cấu hình tạm thời hay là cố định, các bộ xử lý này có thể tạo ra các động cơ được thi hành bởi bộ xử lý vận hành để thực hiện một hoặc nhiều hoạt động hoặc chức năng được mô tả ở đây.

Theo cách tương tự, các phương pháp được mô tả ở đây có thể được thi hành bởi bộ xử lý ít nhất một phần, với một bộ xử lý cụ thể hoặc các bộ xử lý làm ví dụ của phần cứng. Chẳng hạn, ít nhất một số hoạt động của phương pháp có thể 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 cũng có thể vận hành để hỗ trợ đặc tính của các hoạt động thích hợp trong môi trường "điện toán đám mây" hoặc dưới dạng "phần mềm như dịch vụ" (software as a service, SaaS). Chẳng hạn, ít nhất một số hoạt động có thể được thực hiện bởi nhóm máy tính (như các ví dụ về các máy có bộ xử lý), với các hoạt động nay truy cập được qua mạng (chẳng hạn Internet) và qua một hoặc nhiều giao diện thích hợp (chẳng hạn giao diện chương trình ứng dụng (Application Program Interface, API)).

Đặc tính cụ thể của các hoạt động có thể được phân phối giữa các bộ xử lý, không chỉ lưu trú trong một máy, mà được triển khai qua một số lượng máy. Theo một số phương án để làm ví dụ sáng chế, các bộ xử lý hoặc các động cơ được thi hành bởi bộ xử lý có thể nằm ở một vị trí địa lý (chẳng hạn trong môi trường nhà, môi trường cơ quan, hoặc vùng mạng). Theo các phương án khác để làm ví dụ sáng chế, các bộ xử lý hoặc các động cơ được thi hành bởi bộ xử lý có thể được phân phối qua số lượng các vị trí địa lý.

Trong toàn bộ phần mô tả này, nhiều trường hợp có thể thi hành các bộ phận, các hoạt động, hoặc các kết cấu được mô tả như cho một trường hợp. Mặc dù các hoạt động riêng biệt của một hoặc nhiều phương pháp được minh họa và được mô tả như các hoạt động tách rời, song một hoặc nhiều hoạt động riêng biệt có thể được thực hiện một cách đồng thời, và không có yêu cầu là các hoạt động phải được thực hiện theo thứ tự minh họa. Các kết cấu và chức năng biểu thị dưới dạng bộ phận cấu thành tách rời trong các kết cấu để làm ví dụ sáng chế có thể được thi hành như kết cấu hoặc bộ phận được kết hợp. Theo cách tương tự, các kết cấu và chức năng biểu thị dưới dạng một bộ phận có thể được thi hành như bộ phận tách rời. Các thay đổi, biến thể, bổ sung, và các cải tiến này và khác nữa đều nằm trong phạm vi đối tượng yêu cầu bảo hộ.

Mặc dù tổng quan về đối tượng đã được mô tả với tham chiếu đến phần mô tả các phương án để làm ví dụ sáng chế, các biến thể và thay đổi khác nhau có thể được thực hiện với các phương án này mà không nằm ngoài phạm vi rộng nhất của các phương án của phần mô tả này. Các phương án này của đối tượng có thể được viện dẫn ở đây, một cách riêng biệt hoặc thu gom, bởi thuật ngữ "sáng chế" chỉ để thuận tiện và không được xem như tự hạn chế phạm vi sáng chế bởi một phần bộc lộ hoặc khái niệm bất kỳ nếu như có nhiều hơn một được bộc lộ trên thực tế. Phần mô tả chi tiết không được xem như hạn chế sáng chế, và phạm vi của các phương án thực hiện khác nhau chỉ được xác định bởi các điểm yêu cầu bảo hộ kèm theo, cùng với toàn bộ khoảng tương đương các điểm yêu cầu được bảo hộ.

YÊU CẦU BẢO HỘ

1. Phương pháp được thi hành bởi máy tính để dò tấn công phát lại mà không sử dụng nonce tài khoản, phương pháp này bao gồm các bước:

thu thập sự nhận dạng của giao dịch ứng viên để thêm vào chuỗi khối, trong đó sự nhận dạng dựa ít nhất trên nhãn thời gian và thông tin giao dịch của giao dịch ứng viên;

xác nhận nếu nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và nếu sự nhận dạng của giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, cơ sở dữ liệu nhận dạng bao gồm nhiều sự nhận dạng của các giao dịch ứng viên với các nhãn thời gian tương ứng nằm trong khoảng xác nhận hợp lệ thời gian; và

đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

2. Phương pháp theo điểm 1, trong đó:

sự nhận dạng bao gồm giá trị băm của giao dịch ứng viên.

3. Phương pháp theo điểm 2, trong đó:

giao dịch ứng viên bao gồm nhãn thời gian và thông tin giao dịch; và

bước thu thập sự nhận dạng của giao dịch ứng viên để thêm vào chuỗi khối bao gồm tiếp nhận giao dịch ứng viên, và tạo ra giá trị băm dựa ít nhất trên nhãn thời gian và thông tin giao dịch như sự nhận dạng.

4. Phương pháp theo điểm 2, trong đó:

bước thu thập sự nhận dạng của giao dịch ứng viên để thêm vào chuỗi khối bao gồm tiếp nhận giá trị băm như sự nhận dạng; và

phương pháp còn bao gồm các bước: tiếp nhận nhãn thời gian và thông tin giao dịch, và xác nhận sự nhận dạng bằng cách xác nhận giá trị băm dựa ít nhất trên nhãn thời gian và thông tin giao dịch.

5. Phương pháp theo điểm 1, trong đó:

nhãn thời gian được tạo cấu hình bởi thiết bị đầu cuối người dùng mà đã khởi đầu giao dịch ứng viên; và

bước thu thập sự nhận dạng của giao dịch ứng viên để thêm vào chuỗi khối bao gồm tiếp nhận sự nhận dạng từ thiết bị đầu cuối người dùng.

6. Phương pháp theo điểm 1, trong đó:

nhãn thời gian được tạo cấu hình bởi nút chuỗi khối; và

bước thu thập sự nhận dạng của giao dịch ứng viên để thêm vào chuỗi khối bao gồm:

tiếp nhận, bởi nút chuỗi khối, giao dịch được khởi đầu từ thiết bị đầu cuối người dùng, giao dịch được khởi đầu bao gồm thông tin giao dịch;

thêm, bởi nút chuỗi khối, nhãn thời gian vào giao dịch được khởi đầu để thu thập giao dịch ứng viên; và

tạo ra, bởi nút chuỗi khối, sự nhận dạng dựa trên giao dịch ứng viên bao gồm thông tin giao dịch và nhãn thời gian được thêm.

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

đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, thêm sự nhận dạng vào cơ sở dữ liệu nhận dạng.

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

đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, thêm giao dịch ứng viên vào vùng nhớ đệm để lưu trữ các giao dịch ứng viên.

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

đáp ứng với việc xác định rằng nhãn thời gian không nằm trong khoảng xác nhận hợp lệ thời gian, trả lại thông báo lỗi đến thiết bị tính toán mà đã đệ trình giao dịch ứng viên hoặc sự nhận dạng.

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

đáp ứng với việc xác định rằng sự nhận dạng có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên được kết hợp với tấn công phát lại.

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

thực hiện sự xác nhận đồng thuận trên giao dịch ứng viên.

12. Phương pháp theo điểm 11, phương pháp này còn bao gồm các bước:

đồng bộ hóa cơ sở dữ liệu nhận dạng với một hoặc nhiều nút chuỗi khối khác;

xác nhận nếu nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và nếu sự nhận dạng của giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng được đồng bộ hóa; và

đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại; hoặc

đáp ứng với việc xác định rằng sự nhận dạng có trong cơ sở dữ liệu nhận dạng được đồng bộ hóa, xác định rằng giao dịch ứng viên được kết hợp với tấn công phát lại.

13. Phương pháp theo điểm 1, trước khi thu thập sự nhận dạng của giao dịch ứng viên, phương pháp này còn bao gồm bước:

đồng bộ hóa cơ sở dữ liệu nhận dạng với một hoặc nhiều nút chuỗi khối khác.

14. Phương pháp theo điểm 1, trong đó:

khoảng xác nhận hợp lệ thời gian tương ứng với khoảng thời gian bắt đầu từ thời điểm khi khối mới nhất của chuỗi khối đã được thêm vào chuỗi khối.

15. Phương pháp theo điểm 1, trong đó:

khoảng xác nhận hợp lệ thời gian được bao gồm trong khối nguồn gốc của chuỗi khối.

16. Hệ thống để dò tấn công phát lại, hệ thống này bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ đọc được bởi máy tính không chuyển tiếp được kết nối với

một hoặc nhiều bộ xử lý và được tạo cấu hình với các lệnh có thể thực thi bởi một hoặc nhiều bộ xử lý để khiến hệ thống thực hiện các hoạt động bao gồm:

thu thập sự nhận dạng của giao dịch ứng viên để thêm vào chuỗi khối, trong đó sự nhận dạng dựa ít nhất trên nhãn thời gian và thông tin giao dịch của giao dịch ứng viên;

xác nhận nếu nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và nếu sự nhận dạng của giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, cơ sở dữ liệu nhận dạng bao gồm nhiều sự nhận dạng của các giao dịch ứng viên với các nhãn thời gian tương ứng nằm trong khoảng xác nhận hợp lệ thời gian; và

đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

17. Hệ thống theo điểm 16, trong đó:

sự nhận dạng bao gồm giá trị băm của giao dịch ứng viên.

18. Hệ thống theo điểm 16, trong đó:

khoảng xác nhận hợp lệ thời gian tương ứng với khoảng thời gian bắt đầu từ thời điểm khi khối mới nhất của chuỗi khối đã được thêm vào chuỗi khối.

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

thu thập sự nhận dạng của giao dịch ứng viên để thêm vào chuỗi khối, trong đó sự nhận dạng dựa ít nhất trên nhãn thời gian và thông tin giao dịch của giao dịch ứng viên;

xác nhận nếu nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và nếu sự nhận dạng của giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, cơ sở dữ liệu nhận dạng bao gồm nhiều sự nhận dạng của các giao dịch ứng viên với các nhãn thời gian tương ứng nằm trong khoảng xác nhận hợp lệ thời gian; và

đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ thời gian và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại.

20. Phương tiện lưu trữ theo điểm 19, trong đó:

sự nhận dạng bao gồm giá trị băm của giao dịch ứng viên.

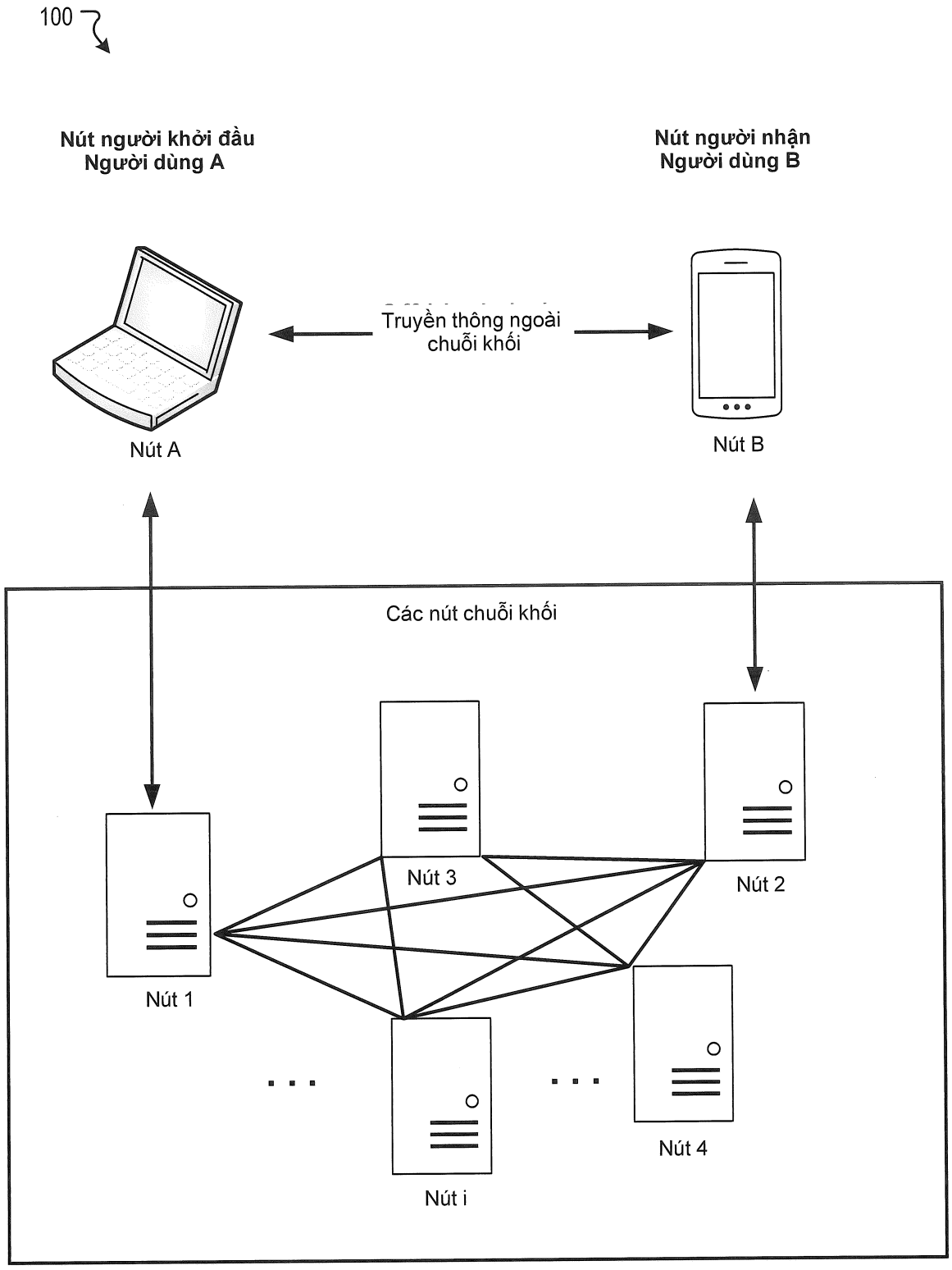

100
Nút người khởi đầu
Người dùng A
Nút người nhận
Người dùng B
Truyền thông ngoài
chuỗi khối
Nút A
Nút B
Các nút chuỗi khối
Nút 1
Nút 2
Nút 3
Nút 4
Nút i

FIG. 1

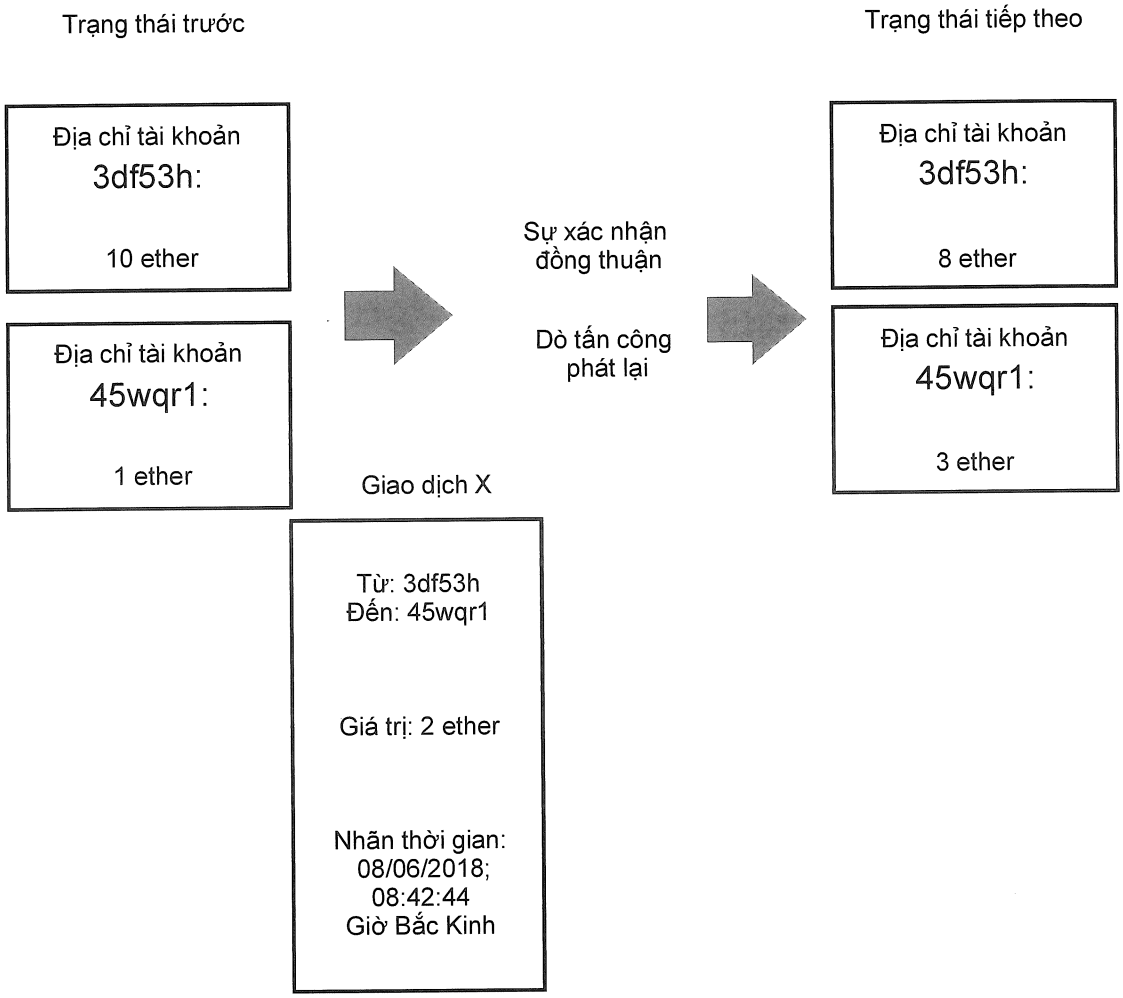

Trạng thái trước
Địa chỉ tài khoản
3df53h:
10 ether
Địa chỉ tài khoản
45wqr1:
1 ether
Giao dịch X
Từ: 3df53h
Đến: 45wqr1
Giá trị: 2 ether
Nhãn thời gian:
08/06/2018;
08:42:44
Giờ Bắc Kinh
Sự xác nhận
đồng thuận
Dò tấn công
phát lại
Trạng thái tiếp theo
Địa chỉ tài khoản
3df53h:
8 ether
Địa chỉ tài khoản
45wqr1:
3 ether

FIG. 2

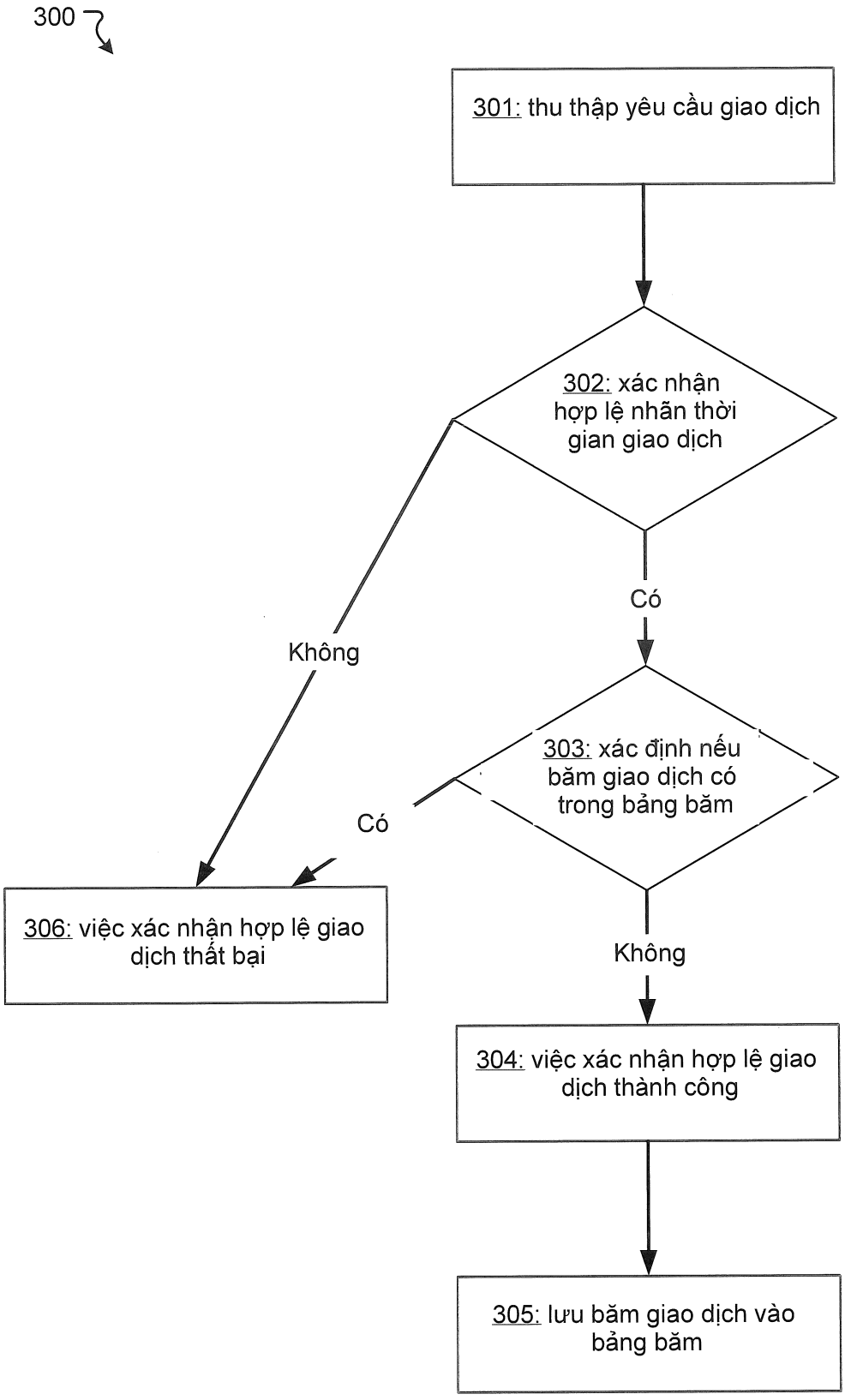

300
301: thu thập yêu cầu giao dịch
302: xác nhận hợp lệ nhãn thời gian giao dịch
Có
Không
303: xác định nếu băm giao dịch có trong bảng băm
Có
Không
306: việc xác nhận hợp lệ giao dịch thất bại
304: việc xác nhận hợp lệ giao dịch thành công
305: lưu băm giao dịch vào bảng băm

FIG. 3

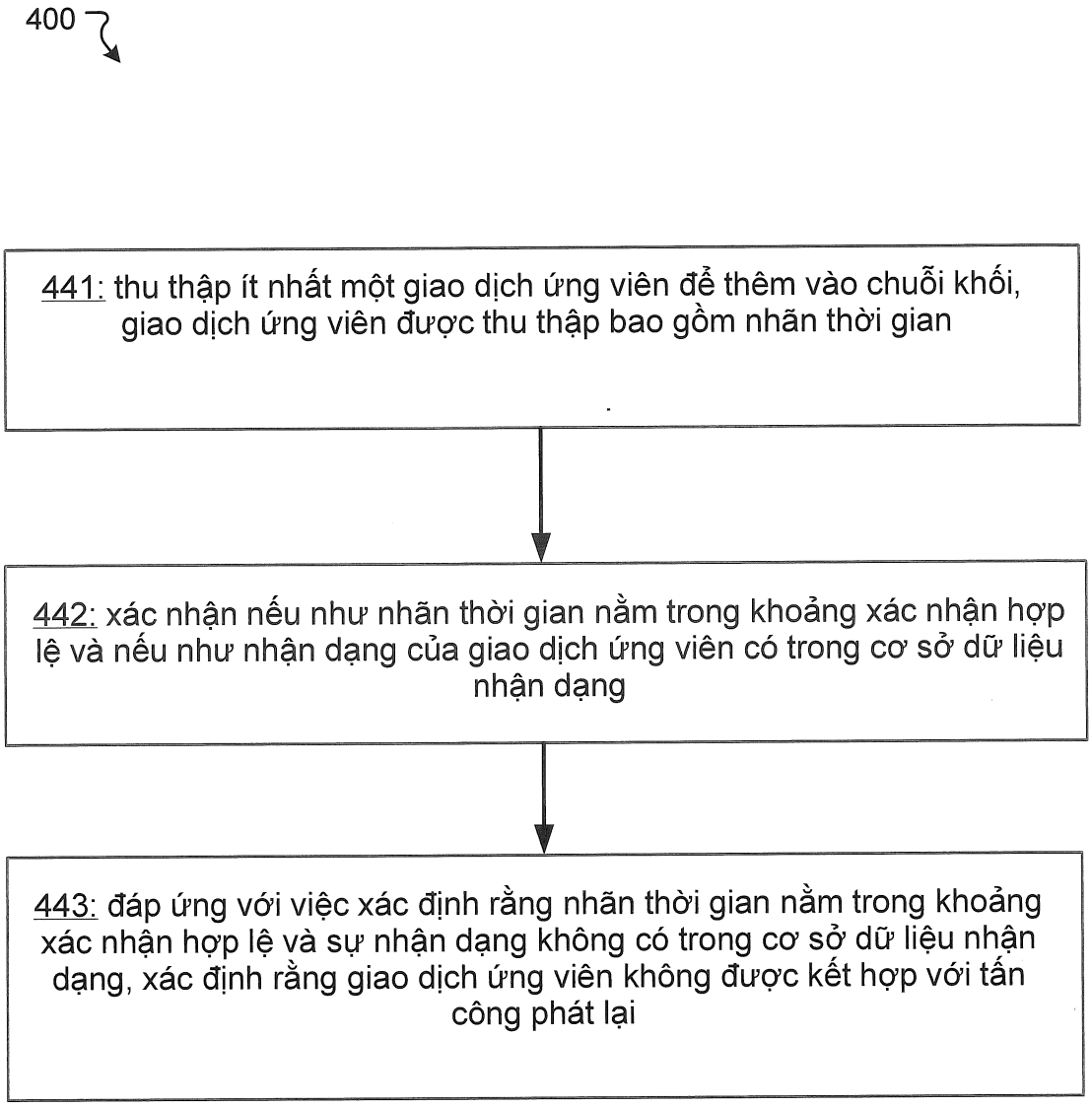

400
441: thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối, giao dịch ứng viên được thu thập bao gồm nhãn thời gian
442: xác nhận nếu như nhãn thời gian nằm trong khoảng xác nhận hợp lệ và nếu như nhận dạng của giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng
443: đáp ứng với việc xác định rằng nhãn thời gian nằm trong khoảng xác nhận hợp lệ và sự nhận dạng không có trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại

FIG. 4A

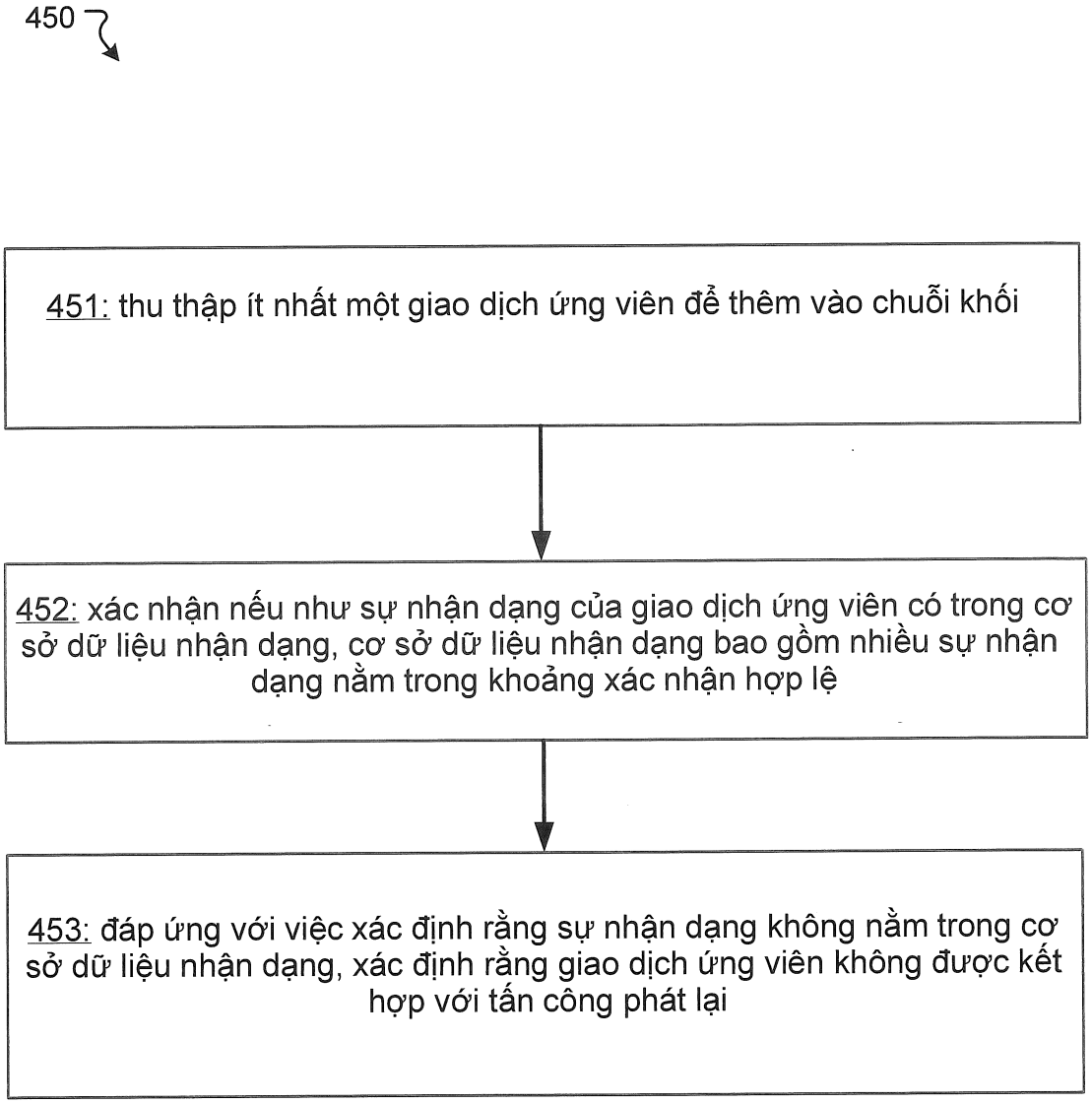

450
451: thu thập ít nhất một giao dịch ứng viên để thêm vào chuỗi khối
452: xác nhận nếu như sự nhận dạng của giao dịch ứng viên có trong cơ sở dữ liệu nhận dạng, cơ sở dữ liệu nhận dạng bao gồm nhiều sự nhận dạng nằm trong khoảng xác nhận hợp lệ
453: đáp ứng với việc xác định rằng sự nhận dạng không nằm trong cơ sở dữ liệu nhận dạng, xác định rằng giao dịch ứng viên không được kết hợp với tấn công phát lại

FIG. 4B

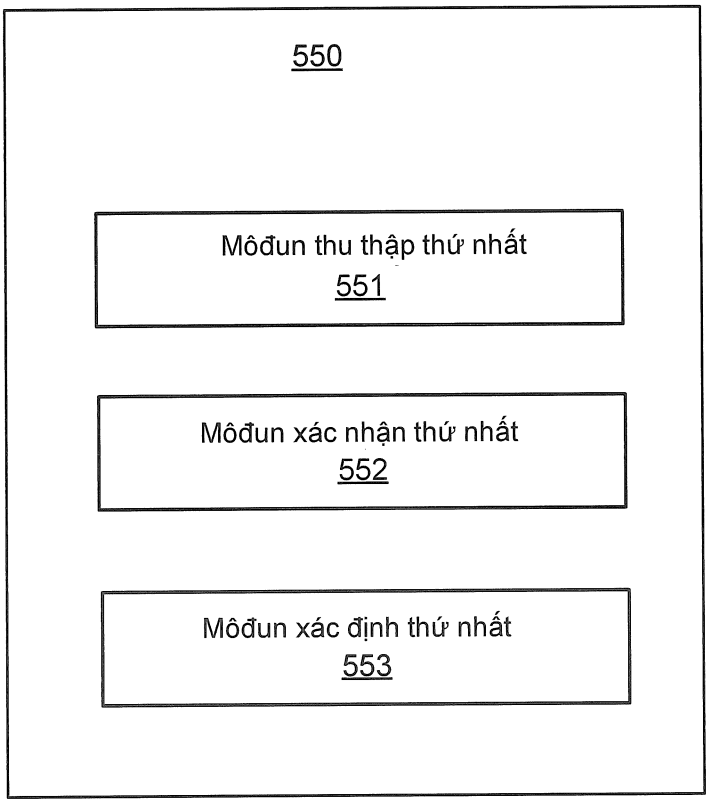

550
Môđun thu thập thứ nhất
551
Môđun xác nhận thứ nhất
552
Môđun xác định thứ nhất
553

FIG. 5

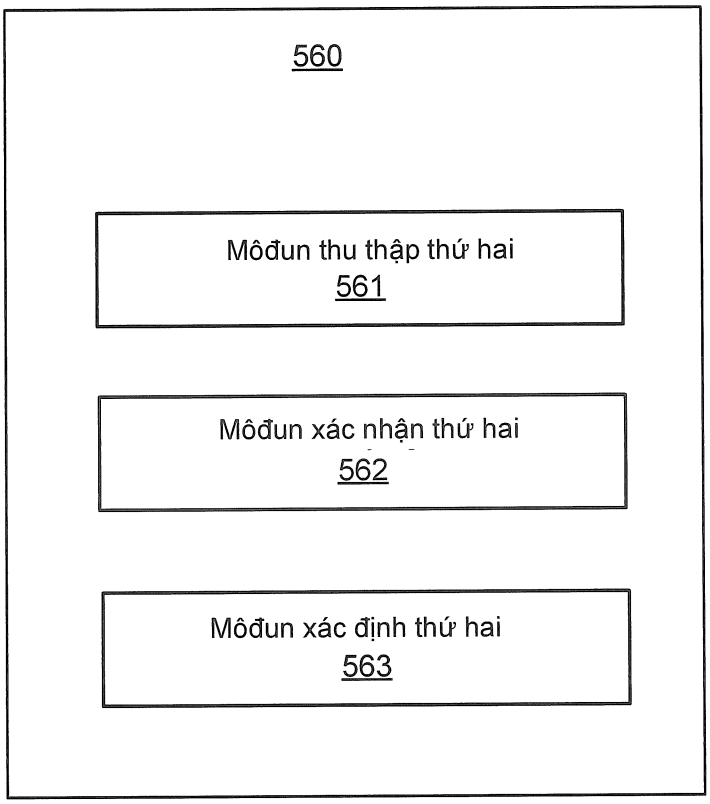

560
Môđun thu thập thứ hai
561
Môđun xác nhận thứ hai
562
Môđun xác định thứ hai
563

FIG. 6

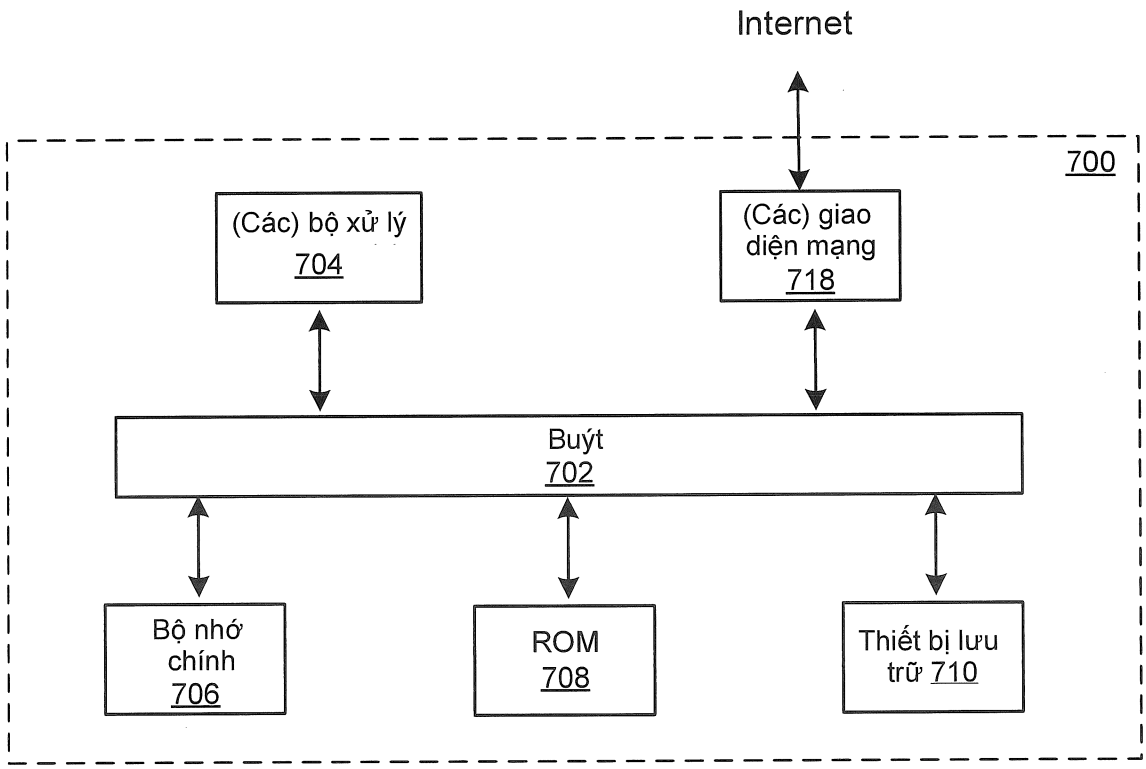

Internet
700
(Các) bộ xử lý
704
(Các) giao diện mạng
718
Buýt
702
Bộ nhớ chính
706
ROM
708
Thiết bị lưu trữ 710

FIG. 7