(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) **1-0051888**

(51)[2020.01] **H04L 9/32**; G06F 21/64

(13) **B**

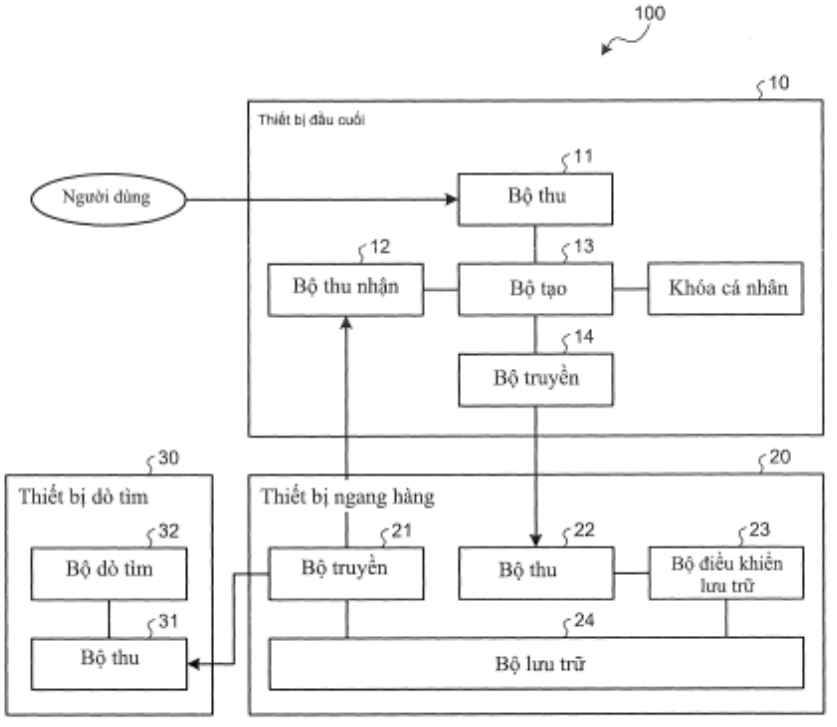
(21) 1-2020-05300
(22) 27/04/2018
(86) PCT/JP2018/017331 27/04/2018
(87) WO 2019/207804 31/10/2019
(45) 25/09/2025 450
(43) 25/03/2021 396A
(73) 1. KABUSHIKI KAISHA TOSHIBA (JP)
1-1, Shibaura 1-chome, Minato-ku, Tokyo 105-0023 Japan
2. TOSHIBA DIGITAL SOLUTIONS CORPORATION (JP)
72-34, Horikawa-cho, Saiwai-ku, Kawasaki-shi, Kanagawa 212-0013 Japan
(72) Kotaro ENDO (JP).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) HỆ THỐNG DÒ TÌM GIẢ MẠO VÀ PHƯƠNG PHÁP DÒ TÌM GIẢ MẠO

(21) 1-2020-05300

(57) Sáng chế đề cập đến hệ thống dò tìm giả mạo bao gồm một hoặc nhiều thiết bị đầu cuối thứ nhất có thể được kết nối tới bất kỳ một trong số một hoặc nhiều thiết bị ngang hàng và một hoặc nhiều thiết bị dò tìm. Thiết bị đầu cuối thứ nhất bao gồm bộ thu nhận mà thu nhận phần băm khối trong chuỗi khối từ thiết bị ngang hàng, và bộ truyền truyền bản ghi giao dịch thứ nhất mà chứa bản tin được ký số thứ nhất mà chứa phần băm khối và dữ liệu dựa trên nội dung giao dịch của thiết bị đầu cuối thứ nhất và chứa chữ ký số đối với bản tin được ký số thứ nhất, tới thiết bị ngang hàng. Thiết bị dò tìm bao gồm bộ thu thu chuỗi khối từ thiết bị ngang hàng và bộ dò tìm phát hiện sự giả mạo chuỗi khối nếu chữ ký số được chứa trong bản ghi giao dịch thứ nhất trong khối của chuỗi khối là không hợp lệ hoặc nếu chuỗi khối không chứa các phần băm khối đồng nhất với phần băm khối được chứa trong bản ghi giao dịch thứ nhất trong khối.

FIG.1



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống dò tìm giả mạo và phương pháp dò tìm giả mạo.

Tình trạng kỹ thuật của sáng chế

Tiền ảo được đại diện bởi Bitcoin đã được sử dụng trong thực tiễn. Các bản ghi của việc chuyển tiền ảo được lưu trữ trong sổ cái điện tử được gọi là chuỗi khối. Đối với Bitcoin, mô hình được gọi là bằng chức công việc (Proof of Work) làm cho sự giả mạo của chuỗi khối trở nên khó khăn. Mô hình bằng chứng công việc (Proof of Work) là nền tảng an toàn của Bitcoin. Mặt khác, đối với các ứng dụng cho chuỗi khối, việc ghi nhận mua bán (giao dịch) tới sổ cái chuỗi khối điện tử mà không bị giới hạn ở việc chuyển tiền đã bắt đầu. Kỹ thuật hợp đồng điện tử được gọi là hợp đồng thông minh trong sử dụng thực tế là ứng dụng của chuỗi khối. Ngoài ra, chuỗi khối được áp dụng thực tế đối với phương pháp duy trì sự đồng nhất của chuỗi khối trong số các thiết bị ngang hàng sử dụng thuật toán đồng thuận chung mà không sử dụng mô hình bằng chứng công việc (Proof of Work). Loại chuỗi khối này được gọi là chuỗi khối được cấp phép.

Danh sách trích dẫn:

Tài liệu sáng chế

Tài liệu sáng chế 1: Công bố đơn patent Nhật Bản số 2017-207979

Vấn đề kỹ thuật:

Tuy nhiên, các kỹ thuật thông thường có khó khăn trong việc phát hiện sự giả mạo của chuỗi khối. Cụ thể, đối với chuỗi khối được cấp phép, việc phát hiện sự giả mạo của chuỗi khối là khó khăn nếu người quản trị thiết bị ngang hàng có âm mưu xấu.

Bản chất kỹ thuật của sáng chế

Giải quyết vấn đề:

Mục đích của sáng chế là đề xuất hệ thống dò tìm giả mạo theo phương án bao gồm một hoặc nhiều thiết bị đầu cuối thứ nhất mà có thể được kết nối tới bất kỳ trong số một hoặc nhiều thiết bị ngang hàng; và một hoặc nhiều thiết bị dò tìm, trong đó mỗi thiết bị đầu cuối thứ nhất bao gồm: bộ thu nhận mà thu nhận phần băm khối được chứa trong chuỗi khối từ thiết bị ngang hàng, và bộ truyền mà truyền bản ghi giao dịch thứ

nhất mà chứa bản tin được ký số thứ nhất chứa phần băm khối và dữ liệu dựa trên nội dung giao dịch của thiết bị đầu cuối thứ nhất và chứa chữ ký số đối với bản tin được ký số thứ nhất, tới thiết bị ngang hàng, và mỗi thiết bị dò tìm bao gồm: bộ thu mà thu chuỗi khối từ thiết bị ngang hàng, và bộ dò tìm mà phát hiện sự giả mạo của chuỗi khối khi chữ ký số được chứa trong bản ghi giao dịch thứ nhất được chứa trong khối của chuỗi khối là không hợp lệ hoặc khi chuỗi khối không chứa phần băm khối mà đồng nhất với phần băm khối được chứa trong bản ghi giao dịch thứ nhất được chứa trong khối.

Mô tả vắn tắt các hình vẽ

FIG.1 là sơ đồ mà minh họa cấu trúc chức năng ví dụ của hệ thống dò tìm giả mạo theo phương án của sáng chế.

FIG.2 là sơ đồ mà minh họa cấu trúc dữ liệu ví dụ của chuỗi khối theo phương án của sáng chế.

FIG.3 là lưu đồ của hoạt động ví dụ của thiết bị đầu cuối theo phương án của sáng chế.

FIG.4 là lưu đồ của hoạt động ví dụ của thiết bị ngang hàng theo phương án của sáng chế.

FIG.5 là hình vẽ của hoạt động ví dụ của bộ dò tìm theo phương án của sáng chế.

FIG.6 là sơ đồ mà minh họa các tính toán ví dụ của phần băm khối của cải biến thứ nhất theo phương án của sáng chế.

FIG.7 là sơ đồ mà minh họa cấu trúc dữ liệu ví dụ của chuỗi khối của cải biến thứ nhất theo phương án của sáng chế.

FIG.8 là hình vẽ của hoạt động ví dụ của bộ dò tìm của cải biến thứ nhất theo phương án của sáng chế.

FIG.9 là hình vẽ mà minh họa cấu trúc phần cứng của thiết bị đầu cuối, thiết bị ngang hàng, và thiết bị dò tìm theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Các phương án của hệ thống dò tìm giả mạo và phương pháp dò tìm giả mạo sẽ được mô tả chi tiết có viện dẫn tới các hình vẽ kèm theo.

Ví dụ về cấu trúc chức năng

FIG.1 là sơ đồ mà minh họa cấu trúc chức năng ví dụ của hệ thống dò tìm giả mạo 100 theo phương án của sáng chế. Hệ thống dò tìm giả mạo 100 bao gồm thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30. Thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 được kết nối tới một thiết bị khác thông qua mạng như Internet.

Các ví dụ về thiết bị đầu cuối 10 bao gồm thiết bị thông minh và máy tính cá nhân được sử dụng bởi người dùng. Thiết bị ngang hàng 20 là máy tính để lưu trữ trong đó các chuỗi khối. Chuỗi khối là sổ cái điện tử mà chứa một hoặc nhiều bản ghi giao dịch. Thiết bị dò tìm 30 là thiết bị để dò tìm sự giả mạo của chuỗi khối được lưu trữ trong thiết bị ngang hàng 20.

Cấu trúc dữ liệu của chuỗi khối được lưu trữ trong thiết bị ngang hàng 20 theo phương án của sáng chế sẽ được mô tả.

FIG.2 là sơ đồ mà minh họa cấu trúc dữ liệu ví dụ của chuỗi khối theo phương án của sáng chế. Theo ví dụ của sáng chế, chuỗi khối theo phương án của sáng chế có cấu trúc chuỗi. Cấu trúc của chuỗi khối không bị giới hạn ở cấu trúc chuỗi. Cấu trúc ví dụ khác ngoài chuỗi sẽ được mô tả sau đây trong cải biến thứ nhất theo phương án của sáng chế.

Trong FIG.2, ký tự tham chiếu n ký hiệu dữ liệu liên quan đến khối thứ n. Ví dụ, khối 50n ký hiệu khối thứ n, và khối 50n-3 ký hiệu khối thứ n-3. Phần băm khối 51n ký hiệu phần băm khối của khối thứ n 50n, phần băm khối 51n-1 ký hiệu phần băm khối của khối thứ n-1 50n-1, phần băm khối 51n-3 ký hiệu phần băm khối của khối n-3 50n-3, và phần băm khối 51n-4 ký hiệu phần băm khối của khối n-4 50n-4. Nếu n khối không được phân biệt với nhau, n sẽ được bỏ qua trong phần mô tả.

Chuỗi khối theo phương án của sáng chế được tạo ra với các khối 50, mà chứa chung nhiều bản ghi giao dịch 53, được thêm vào chuỗi khối theo trình tự thời gian. Đối với mỗi khối 50, số khối 52 được cấp phát theo thứ tự tăng dần theo trình tự thời gian. Số khối 52 được sử dụng để nhận dạng khối 50 được chứa trong chuỗi khối.

Khối 50n bao gồm phần băm khối 51n, phần băm khối 51n-1 của khối trước đó 50n-1, 0 (zero) hoặc bản ghi giao dịch 53n hoặc nhiều hơn, và số khối 52n của khối 50n.

Phần băm khối 51n là giá trị băm được tạo ra từ bản tin bao gồm phần băm khối 51n-1 của khối trước đó 50n-1, 0 (zero) bản ghi giao dịch 53n hoặc nhiều hơn, và số khối 52n của khối 50n. Giá trị băm được tính toán sử dụng hàm băm (ví dụ, SHA-256), mà làm cho việc tính toán ngược để thu nhận giá trị đầu vào từ giá trị đầu ra (giá trị băm) khó khăn và có khả năng xung đột giá trị băm hoàn toàn thấp. Phần băm khối 51n được tạo ra khi khối 50n được tạo ra.

Ở đây, bản ghi giao dịch 53n chứa bản tin được ký số, mà chứa số khối 52n-3, phần băm khối 51n-3 và nội dung giao dịch 54n, và chữ ký số 55n của bản tin được ký số. Nói cách khác, bản ghi giao dịch thứ n 53n chứa phần băm khối 51n-k (k = 3 trong ví dụ của FIG.2) của khối trước đó 50n-k.

Số khối 52n-3 không bắt buộc được chứa trong bản ghi giao dịch 53n. Việc chứa số khối 52n-3 trong bản ghi giao dịch 53n cho phép xử lý nhanh hơn để nhận dạng phần băm khối đích 51n-3 được chứa trong chuỗi khối.

Phần băm khối 51 được chứa trong khối 50 được tính toán đệ quy. Theo đó, tập hợp của các bản ghi giao dịch 53, mà là các đích của việc tính toán phần băm khối 51, được xem là tất cả các bản ghi giao dịch 53 của khối 50 mà chứa bản ghi giao dịch 53 và khối trước đó. Do đó, ví dụ, nếu việc giả mạo liên quan đến việc xóa bản ghi giao dịch trong quá khứ 53 diễn ra, tất cả các phần băm khối 51 của khối 50 mà chứa bản ghi giao dịch bị giả mạo 53 và khối sau đó được thay đổi.

Ví dụ về việc giả mạo chuỗi khối sẽ được mô tả. Cụ thể, ví dụ, sau khi bản ghi giao dịch đích 53 bị xóa, tất cả các phần băm khối 51 mà chứa bản ghi giao dịch đích 53 được tính toán lại, và sau đó chuỗi khối được ghi đè bằng các phần băm khối mới 51 như là các phần băm khối hợp lệ. Trong trường hợp của mô hình Chứng cớ công việc (Proof of Work), sẽ mất nhiều thời gian để tính toán lại tất cả các phần băm khối 51, và do đó phương pháp tính toán lại này không khả thi trong thực tế. Tuy nhiên, ngay cả với mô hình Chứng cớ công việc (Proof of Work), việc bảo mật thông tin theo lý thuyết không được thỏa mãn. Ví dụ, trong trường hợp sử dụng tiền ảo mà áp dụng mô hình Chứng cớ công việc (Proof of Work), nếu khả năng tính toán bởi người dùng có âm mưu xấu (hoặc nhóm người dùng có âm mưu xấu) vượt quá khả năng tính toán bởi các người dùng tốt khác, các kỹ thuật thông thường có khả năng khó khăn trong việc phát hiện giả mạo chuỗi khối.

Hệ thống dò tìm giả mạo 100 theo phương án của sáng chế là hệ thống cho

phép phát hiện sự giả mạo dễ dàng hơn khi chuỗi khối, mà là chuỗi khối phù hợp tại thời điểm khi được lưu trữ trong thiết bị ngang hàng 20, bị giả mạo sau đó.

Trong phương án này, mặc dù phần băm khối 51 có thể được tính toán lại về mặt lý thuyết từ tập hợp của tất cả các bản ghi giao dịch 53, phần băm khối 51 được lưu trữ trong thiết bị ngang hàng 20 cùng với bản ghi giao dịch 53 đối với mỗi khối 50 nhằm mục đích của hiệu quả xử lý.

phần băm khối 51 có thể được tính toán bởi phương pháp khả dụng bất kỳ. Mặc dù phương pháp tính toán phần băm khối 51 theo phương án của sáng chế được giả định để có ít ràng buộc hơn so với mô hình Chứng cớ công việc (Proof of Work), mô hình Chứng cớ công việc (Proof of Work) cũng có thể được sử dụng.

Viện dẫn tới FIG.1, hoạt động của thiết bị đầu cuối 10 sẽ được mô tả một cách chi tiết. Mặc dù hệ thống dò tìm giả mạo 100 trong ví dụ trên FIG.1 minh họa một thiết bị đầu cuối 10, nhiều thiết bị đầu cuối 10 có thể được sử dụng. Số lượng thiết bị đầu cuối 10 mà truyền thông với thiết bị ngang hàng 20 là tùy ý.

Thiết bị đầu cuối 10 bao gồm bộ thu 11, bộ thu nhận 12, bộ tạo 13, và bộ truyền 14. Viện dẫn tới lưu đồ của FIG.3, hoạt động của bộ thu 11, bộ thu nhận 12, bộ tạo 13, và bộ truyền 14 sẽ được mô tả một cách chi tiết.

Hoạt động ví dụ của thiết bị đầu cuối

FIG.3 là lưu đồ về hoạt động ví dụ của thiết bị đầu cuối 10 theo phương án của sáng chế.

Bộ thu 11 thu sự nhập dữ liệu mà chỉ báo nội dung giao dịch 54n từ người dùng (bước S1) và nhập dữ liệu vào bộ tạo 13. Nội dung giao dịch 54n có thể là dữ liệu bất kỳ. Ví dụ, nội dung giao dịch 54n chỉ báo sự chuyển tiền của tiền ảo.

Bộ thu nhận 12 thu nhận, từ thiết bị ngang hàng 20, phần băm khối 51n-k được chứa trong chuỗi khối và số khối 52n-k của khối 50n-k mà chứa phần băm khối 51n-k (bước S2). Trong ví dụ của FIG.2, k bằng 3. Được ưu tiên rằng k là nhỏ hơn, nhưng k không cần là mới nhất (k = 1).

Do đó, phần băm khối 51n-k và số khối 52n-k có thể được thu nhận tại thời điểm bất kỳ. Ví dụ, bộ thu nhận 12 đều đặn (ví dụ, mỗi phút, mỗi giờ, hoặc mỗi ngày) thu nhận phần băm khối 51n-k và số khối 52n-k được chứa trong chuỗi khối. Sau khi thu nhận phần băm khối mới 51n-k2 và số khối mới 52n-k2, bộ thu nhận 12 loại bỏ

phần băm khối 51n-k và số khối 52n-k thu được trước khi phần băm khối 51n-k2 và số khối 52n-k2 được thu nhận.

Ví dụ, bộ thu nhận 12 có thể thu nhận phần băm khối 51n-k và số khối 52n-k, sau khi thu được yêu cầu thu nhận từ bộ tạo 13 khi bộ tạo 13 tạo ra bản ghi giao dịch 53.

Ví dụ, bộ thu nhận 12 có thể thu nhận một cách thụ động phần băm khối 51n-k và số khối 52n-k từ thiết bị ngang hàng 20 sử dụng việc truyền của phần băm khối 51n-k và số khối 52n-k bởi thiết bị ngang hàng 20 như là kích hoạt.

Phương pháp bất kỳ có thể được sử dụng để lựa chọn phần băm khối 51n-k cần được thu nhận. Ví dụ, bộ thu nhận 12 có thể thu nhận phần băm khối mới 51n-k trong số các phần băm khối 51 được chứa trong chuỗi khối trên cơ sở của số khối 52. Trong phương án này, phần băm khối 51n-k của khối 50n-k có số khối lớn hơn là đích thu nhận.

Ví dụ, bộ thu nhận 12 có thể thu nhận phần băm khối mới 51n-k trong số các phần băm khối 51 được chứa trong chuỗi khối trên cơ sở của thời điểm khi phần băm khối 51 được tạo ra.

Ví dụ, bộ thu nhận 12 có thể thu nhận, từ trong số các phần băm khối 51 được chứa trong chuỗi khối và như là phần băm khối mới hơn 51n-k, phần băm khối 51 mà nhiều bản ghi giao hơn 53 được lưu trữ trong chuỗi khối được sử dụng cho việc tính toán giá trị băm.

Bộ thu nhận 12 nhập phần băm khối thu được 51n-k và số khối 52n-k tới bộ tạo 13.

Bộ tạo 13 thu dữ liệu mà chỉ báo nội dung giao dịch 54n từ bộ thu 11 và thu phần băm khối 51n-k và số khối 52n-k từ bộ thu nhận 12. Bộ tạo 13 sử dụng khóa cá nhân của thiết bị đầu cuối 10 để tạo ra chữ ký số 55n của bản tin bao gồm phần băm khối 51n-k và số khối 52n-k và nội dung giao dịch 54n. Bộ tạo 13 tạo ra bản ghi giao dịch 53n (bản ghi giao dịch thứ nhất) mà chứa phần băm khối 51n-k, số khối 52n-k, nội dung giao dịch 54n, và chữ ký số 55n (bước S3), và nhập bản ghi giao dịch 53n vào bộ truyền 14.

Tiếp theo, bộ truyền 14 thu bản ghi giao dịch 53n từ bộ tạo 13 và truyền bản ghi giao dịch 53n tới thiết bị ngang hàng 20 (bước S4).

Viện dẫn tới FIG.1, hoạt động của thiết bị ngang hàng 20 sẽ được mô tả một cách chi tiết. Trong ví dụ trên FIG.1, mặc dù hệ thống dò tìm giả mạo 100 bao gồm một thiết bị ngang hàng 20, nhiều thiết bị ngang hàng 20 có thể được sử dụng. Ví dụ, những người quản trị thiết bị ngang hàng có thể vận hành một hoặc nhiều thiết bị ngang hàng tương ứng 20.

Thiết bị ngang hàng 20 bao gồm bộ truyền 21, bộ thu 22, bộ điều khiển lưu trữ 23, và bộ lưu trữ 24. Hoạt động của bộ truyền 21, bộ thu 22, bộ điều khiển lưu trữ 23, và bộ lưu trữ 24 sẽ được mô tả chi tiết có viện dẫn tới lưu đồ trên FIG.4.

Hoạt động ví dụ của thiết bị ngang hàng

FIG.4 là lưu đồ về hoạt động ví dụ của thiết bị ngang hàng 20 theo phương án của sáng chế.

Bộ thu 22 thu bản ghi giao dịch 53n từ thiết bị đầu cuối 10 (bộ truyền 14) (bước S11) và nhập bản ghi giao dịch 53n vào bộ điều khiển lưu trữ 23.

Bộ điều khiển lưu trữ 23 thu bản ghi giao dịch 53n từ bộ thu 22 và xác định rằng chữ ký số 55n được chứa trong bản ghi giao dịch 53n có hợp lệ hay không (bước S12). Nếu chữ ký số 55n là không hợp lệ (Không tại bước S12), mà có nghĩa rằng bản ghi giao dịch 53n đã bị giả mạo, bộ điều khiển lưu trữ 23 loại bỏ bản ghi giao dịch 53n (bước S14).

Nếu chữ ký số là hợp lệ (Có tại bước S12), bộ điều khiển lưu trữ 23 nhận dạng phần băm khối 51n-k được lưu trữ trong chuỗi khối sử dụng số khối 52n-k được chứa trong bản ghi giao dịch 53n và xác định rằng phần băm khối được nhận dạng 51n-k là đồng nhất với phần băm khối 51n-k được chứa trong bản ghi giao dịch 53n (bước S13). Nếu các phần băm khối 51n-k không đồng nhất với nhau (Không tại bước S13), bộ điều khiển lưu trữ 23 loại bỏ bản ghi giao dịch 53n (bước S14). Các xử lý của bước S12 và bước S13 đảm bảo rằng bản ghi giao dịch 53n thu được tại xử lý của bước S11 không bị giả mạo tại thời điểm khi bản ghi giao dịch 53n được lưu trữ trong thiết bị ngang hàng 20.

Nếu các phần băm khối 51n-k đồng nhất với nhau (Có tại bước S13), bộ điều khiển lưu trữ 23 xác định rằng có tạo ra khối 50n hay không (bước S15). Số lượng bản ghi giao dịch 53n được chứa trong khối 50n không bị giới hạn ở một. Các bản ghi giao dịch 53n có thể được bao gồm. ví dụ, khi số lượng bản ghi giao dịch được xác định

trước 53n được tích lũy, bộ điều khiển lưu trữ 23 sẽ tạo ra khối 50n mà chứa số lượng bản ghi giao dịch được xác định trước 53n.

Nếu khối 50n không cần được tạo ra (Không tại bước S15), bộ điều khiển lưu trữ 23 tích lũy bản ghi giao dịch 53n thu được tại xử lý của bước S11 trong bộ đệm hoặc loại tương tự của bộ điều khiển lưu trữ 23 (bước S16).

Nếu khối 50n cần được tạo ra (Có tại bước S15), bộ điều khiển lưu trữ 23 tạo ra khối 50n mà chứa các bản ghi giao dịch 53n được tích lũy trong bộ đệm hoặc loại tương tự của bộ điều khiển lưu trữ 23 và bản ghi giao dịch 53n thu được tại xử lý của bước S11 và lưu trữ khối 50n trong chuỗi khối của bộ lưu trữ 24 (bước S17).

Bộ truyền 21 truyền số khối 52n của khối 50n được tạo ra tại xử lý của bước S17 và phần băm khối 51n được chứa trong khối 50n tới thiết bị đầu cuối 10 (bước S18). Phần băm khối 51n và số khối 52n được truyền tại bước S18 được sử dụng trong bản ghi giao dịch 53 được chứa trong khối đối với khối n+thứ nhất và khối phía sau. Xử lý của bước S18 có thể được bỏ qua. Ví dụ, xử lý của bước S18 được bỏ qua, nếu bộ thu nhận 12 của thiết bị đầu cuối 10 một cách độc lập thu nhận phần băm khối 51n+1-k và số khối 52n+1—k trong khi tạo ra bản ghi giao dịch 53 được chứa trong khối đối với khối n+thứ nhất và khối sau đó.

Viện dẫn tới FIG.1, hoạt động của thiết bị dò tìm 30 sẽ được mô tả một cách chi tiết. Trong ví dụ của FIG.1, hệ thống dò tìm giả mạo 100 bao gồm một thiết bị dò tìm 30. Thay vì đó, nhiều thiết bị dò tìm 30 có thể được bao gồm.

Thiết bị dò tìm 30 bao gồm bộ thu 31 và bộ dò tìm 32. Trong ví dụ của FIG.1, thiết bị dò tìm 30 được lắp đặt phía ngoài thiết bị ngang hàng 20. Cấu trúc này cho phép người kiểm tra độc lập với người quản trị của thiết bị ngang hàng 20 để dò tìm sự giả mạo của chuỗi khối được lưu trữ trong thiết bị ngang hàng 20.

Bộ thu 31 thu chuỗi khối từ thiết bị ngang hàng 20 (bộ truyền 21) và nhập chuỗi khối vào bộ dò tìm 32.

Bộ dò tìm 32 dò tìm rằng chuỗi khối có bị giả mạo hay không bằng cách xác nhận mỗi khối 50 trong chuỗi khối.

FIG.5 là hình vẽ của hoạt động ví dụ của bộ dò tìm 32 theo phương án của sáng chế. Ký tự tham chiếu tx trong FIG.5 chỉ báo bản ghi giao dịch 53 (giao dịch).

Bộ dò tìm 32 tính toán lại phần băm khối 51 được chứa trong mỗi khối 50 và

xác định rằng giá trị băm thu được bằng việc tính toán lại có đồng nhất với phần băm khối 51 được chứa trong khối 50 hay không (các dòng thứ nhất đến thứ năm trong FIG.5). Nếu giá trị băm thu được bằng việc tính toán lại không đồng nhất với phần băm khối 51 được chứa trong khối 50, bộ dò tìm 32 phát hiện sự giả mạo của chuỗi khối.

Bộ dò tìm 32 xác định sự hợp lệ của chữ ký số 55 được chứa trong bản ghi giao dịch 53 được chứa trong mỗi khối 50 của chuỗi khối (dòng thứ tám của FIG.5). Nếu chữ ký số 55 được chứa trong bản ghi giao dịch 53 được chứa trong khối 50 của chuỗi khối là không hợp lệ, bộ dò tìm 32 phát hiện sự giả mạo của chuỗi khối.

Nếu chuỗi khối không chứa các phần băm khối 51 đồng nhất với phần băm khối 51 được chứa trong bản ghi giao dịch 53 được chứa trong khối 50, bộ dò tìm 32 phát hiện sự giả mạo của chuỗi khối. Cụ thể, bộ dò tìm 32 xác định rằng phần băm khối 51 của khối 50, được nhận dạng từ chuỗi khối sử dụng số khối 52 được chứa trong bản ghi giao dịch 53, có đồng nhất với phần băm khối 51 được chứa trong bản ghi giao dịch hay không (các dòng thứ chín đến thứ mười hai trong FIG.5). Nếu phần băm khối 51 của khối được nhận dạng 50 không đồng nhất với phần băm khối 51 được chứa trong bản ghi giao dịch, bộ dò tìm 32 phát hiện sự giả mạo của chuỗi khối.

Thứ tự xử lý của các bước để dò tìm sự giả mạo được minh họa trong FIG.5 là ví dụ, và các bước xử lý để dò tìm sự giả mạo có thể được thực hiện trong thứ tự mong muốn bất kỳ.

Hiệu quả của phương án theo sáng chế

Như được mô tả nêu trên, hệ thống dò tìm giả mạo 100 theo phương án của sáng chế bao gồm một hoặc nhiều thiết bị đầu cuối 10 (các thiết bị đầu cuối thứ nhất) có thể được kết nối tới bất kỳ một hoặc nhiều thiết bị ngang hàng 20, và thiết bị dò tìm 30. Trong thiết bị đầu cuối 10 hoặc các thiết bị đầu cuối 10, bộ thu nhận 12 thu nhận phần băm khối 51 được chứa trong chuỗi khối từ thiết bị ngang hàng 20. Bộ truyền 14 truyền tới thiết bị ngang hàng 20 bản ghi giao dịch 53 (bản ghi giao dịch thứ nhất) mà chứa bản tin được ký số (bản tin được ký số thứ nhất) mà chứa phần băm khối 51 và dữ liệu dựa trên nội dung giao dịch 54 của thiết bị đầu cuối 10 (trong phương án này, về bản chất là nội dung giao dịch 54) và chứa chữ ký số 55 đối với bản tin được ký số. Bộ thu 31 của thiết bị dò tìm 30 thu chuỗi khối từ thiết bị ngang hàng 20. Bộ dò tìm 32 phát hiện sự giả mạo của chuỗi khối nếu chữ ký số 55 được chứa trong bản ghi giao

dịch 53 trong khối 50 của chuỗi khối là không hợp lệ, hoặc nếu chuỗi khối không chứa các phần băm khối 51 đồng nhất với phần băm khối 51 được chứa trong bản ghi giao dịch 53 trong khối 50.

Điều này cho phép hệ thống dò tìm giả mạo 100 theo phương án của sáng chế phát hiện dễ dàng hơn sự giả mạo của chuỗi khối. Cụ thể, nếu người quản trị thiết bị ngang hàng của chuỗi được cấp phép có âm mưu, sự giả mạo của chuỗi khối có thể được phát hiện dễ dàng hơn.

Cụ thể hơn, do việc giả mạo thông thường như bổ sung, xóa, và thay thế thứ tự của bản ghi giao dịch về bản chất không làm thay đổi bản ghi giao dịch, các việc xác thực thông thường của các chữ ký số của các bản ghi giao dịch không thể phát hiện sự giả mạo. Ngoài ra, nếu những người quản trị của tất cả thiết bị ngang hàng có âm mưu để giả mạo bản ghi giao dịch bằng cách, ví dụ, thêm, xóa, và thay thế các thứ tự của bản ghi, nội dung của chuỗi khối là đồng nhất giữa các thiết bị ngang hàng. Do đó sẽ khó để phát hiện sự giả mạo của chuỗi khối bằng cách so sánh giữa các thiết bị ngang hàng.

Phần băm khối 51 xác định duy nhất thành phần của bản ghi giao dịch 53 mà trên đó phần băm khối 51 được tính toán, tại xác suất mà được xem là gần 100%. Nói cách khác, nếu việc giả mạo như bổ sung, xóa, và thay đổi các thứ tự trong bản ghi giao dịch 53 diễn ra, phần băm khối 51 được chứa trong bản ghi giao dịch 53 theo phương án của sáng chế là không đồng nhất với phần băm khối 51 được chứa trong chuỗi khối tại xác suất mà được xem là gần 100%.

Do các người dùng tốt không có lý do để giúp việc giả mạo, các bản ghi giao dịch 53 của những người dùng tốt được kỳ vọng không bị giả mạo miễn là các chữ ký số 55 của họ được xác nhận là hợp lệ (do việc giả mạo yêu cầu rằng những người dùng tốt đưa các chữ ký số tới dữ liệu bị giả mạo và dữ liệu sau đó).

Do đó, phần băm khối 51 được chứa trong bản ghi giao dịch 53 được kỳ vọng không bị giả mạo, và theo đó, bản ghi giao dịch 53 được sử dụng cho việc tính toán được kỳ vọng không bị giả mạo (do việc tính toán ngược của hàm băm là khó và có thể được kỳ vọng rằng khả năng xảy ra ngẫu nhiên của xung đột là gần 0%).

Khi chuỗi khối được phát hiện không phải bị giả mạo bởi bộ dò tìm 32 theo phương án của sáng chế chứa nhiều bản ghi giao dịch 53 của người dùng tốt, được kỳ vọng rằng chuỗi khối không bị giả mạo bất kể sự tin cậy của những người quản trị

thiết bị ngang hàng.

Ngược lại, để những người quản trị thiết bị ngang hàng giả mạo chuỗi khối, họ cần xóa tất cả các bản ghi giao dịch 53 mà chứa phần băm khối 51 được tính toán từ bản ghi giao dịch đích giả mạo 53 hoặc cần yêu cầu những người dùng thực hiện lại các chữ ký số sử dụng phần băm khối bị giả mạo 51 (cách thức sau yêu cầu những người dùng hợp tác để giả mạo). Khi các bản ghi giao dịch 53 của những người dùng tốt tăng lên, số lượng bản ghi giao dịch 53 cần bị xóa tăng lên, và ảnh hưởng bởi sự giả mạo trở nên lớn hơn. Khả năng tìm ra sự giả mạo từ khía cạnh khác biết là cao.

Như được mô tả nêu trên, theo phương án của sáng chế, càng nhiều người dùng tốt mà sử dụng chuỗi khối, khả năng xác thực rằng chuỗi khối không bị giả mạo càng cao bất kể độ tin cậy của những người quản trị thiết bị ngang hàng. Ví dụ điển hình của người dùng tốt là người kiểm tra mà cố gắng xác minh dữ liệu. Ngay cả trong trường hợp trong đó những người dùng tốt không thể được nhận dạng, nếu có nhiều hơn người dùng không liên quan đến quyền lợi, có thể giả định một cách hợp lý rằng số lượng lớn người dùng tốt được bao gồm. Do đó, các hiệu quả của phương án theo sáng chế có thể được kỳ vọng.

Cải biến thứ nhất của phương án theo sáng chế

Cải biến thứ nhất của phương án theo sáng chế sẽ được mô tả. Trong cải biến thứ nhất, phần mô tả tương tự như phương án nêu trên sẽ được bỏ qua, và sự khác biệt giữa chúng sẽ được mô tả.

Trong cải biến thứ nhất, cấu trúc của chuỗi khối được tổng quát hóa. Ví dụ, trừ khi hệ thống sử dụng mô hình Chứng cớ công việc (Proof of Work), chuỗi khối không cần thiết được tạo thành trong các chuỗi, và số khối 52 là không cần thiết. Bản chất là phần băm khối được tính toán từ bản ghi giao dịch 53 được chứa trong chuỗi khối và bản ghi giao dịch trước đó. Việc làm thế nào tính toán phần băm khối và làm thế nào để lựa chọn bản ghi giao dịch 53 được sử dụng cho việc tính toán là linh hoạt.

Trong cải biến thứ nhất, giá trị băm (phần băm khối 51) được tính toán từ bản ghi giao dịch trước đó 53 sử dụng cấu trúc dạng cây được gọi là cây băm (cây Merkle).

FIG.6 là sơ đồ mà minh họa các tính toán ví dụ của phần băm khối 51 của cải biến thứ nhất theo phương án của sáng chế. Trong ví dụ của FIG.6, các tính toán sử dụng cây băm mà chứa các giá trị băm 101a đến 101f, 201a đến 201c, và 301a. Ví dụ,

khi tạo ra khối mới 50, bộ điều khiển lưu trữ 23 tính toán phần băm khối 51 sử dụng các giá trị băm 201c và 301a, như phần băm khối 51 dựa trên bản ghi giao dịch trước đó 53. Phần băm khối thu được 51 được thêm vào cây băm, nhờ đó cây băm được cập nhật. Nhằm mục đích xác thực chuỗi khối, bộ dò tìm 32 tìm kiếm cây băm đối với giá trị băm (phần băm khối 51) được chứa trong bản ghi giao dịch 53 của mỗi khối 50 và xác định rằng giá trị băm có được chứa trong cây băm hay không.

Bitcoin sử dụng cây băm đối với các tính toán giá trị băm bên trong khối. Các khối được kết nối tới khối khác trong các chuỗi. Trong cải biến thứ nhất, cây băm được sử dụng để kết nối giữa các khối. Ví dụ, việc sử dụng cấu trúc cây băm để kết nối giữa các khối có thể làm giảm thời gian để xác định rằng bản ghi giao dịch định trước 53 (phần băm khối định trước 51) có được chứa trong chuỗi khối hay không.

Trong ví dụ của FIG.6, bản ghi giao dịch 53 chứa nội dung giao dịch 54, chữ ký số 55, số bản ghi giao dịch 56, thời điểm 57, kết quả thực thi 58, giá trị băm 59, và giá trị băm 201a. Bản tin được ký số, mà chữ ký số 55 được đưa tới, là giá trị băm 59 và giá trị băm 201a.

Giá trị băm 101b cần được thêm vào cây băm được tính toán từ số bản ghi giao dịch 56, thời điểm 57, kết quả thực thi 58, giá trị băm 59, và giá trị băm 201a.

Số bản ghi giao dịch 56 là số để nhận dạng nội dung giao dịch 54. Thời điểm 57 là thời điểm khi việc giao dịch của nội dung giao dịch 54 được thực hiện. Kết quả thực thi 58 là kết quả của xử lý như hợp đồng thông minh. Giá trị băm 59 được tính toán từ nội dung giao dịch 54. Việc tính toán giá trị băm 101b (phần băm khối 51) sử dụng giá trị băm 59, được tính toán dựa trên nội dung giao dịch 54, thay vì sử dụng nội dung giao dịch 54. Phương pháp này cho phép việc xác thực (phát hiện giả mạo) của chuỗi khối mà không có nội dung giao dịch 54 bị bộc lộ.

FIG.7 là sơ đồ mà minh họa cấu trúc dữ liệu ví dụ của chuỗi khối của cải biến thứ nhất theo phương án của sáng chế. Trong cải biến thứ nhất, chuỗi khối có cấu trúc cây (xem FIG.6).

Trong FIG.7, các ký tự tham chiếu x và y chỉ báo dữ liệu liên quan đến khối định trước được chứa trong cây băm. Trong phần mô tả sau đây, x và y sẽ được bỏ qua nếu các khối không cần thiết được phân biệt.

Chuỗi khối của cải biến thứ nhất được tạo ra với các khối 50 trong đó các bản

ghi giao dịch 53 được tích lũy được thêm vào cây băm.

Khối 50y chứa phần băm khối 51y, giá trị băm 201z, giá trị băm 301w, và một hoặc nhiều bản ghi giao dịch 53y. Các giá trị băm 201z và 301w là các giá trị băm (phần băm khối 51 được tính toán dựa trên bản ghi giao dịch trước 53) được chứa trong cây băm.

Phần băm khối 51y là giá trị băm được tính toán dựa trên giá trị băm 201z và giá trị băm 301w và một hoặc nhiều bản ghi giao dịch 53y. Phần băm khối 51y được tạo ra khi khối 50y được tạo ra.

Bản ghi giao dịch 53y chứa phần băm khối 51x, chữ ký số 55y, số bản ghi giao dịch 56y, thời điểm 57y, kết quả thực thi 58y, và giá trị băm 59y. Giá trị băm 59y là giá trị băm được tính toán từ nội dung giao dịch 54y.

Phần băm khối 51x là phần băm khối được chứa trong khối 50x của các khối 50 được lưu trữ trong cấu trúc dạng cây. Bản tin được ký số, mà chữ ký số 55y được đưa tới, bao gồm phần băm khối 51x và giá trị băm 59y.

FIG.8 là hình vẽ về hoạt động ví dụ của bộ dò tìm 32 theo cải biến thứ nhất theo phương án của sáng chế. ký tự tham chiếu tx trong FIG.8 chỉ báo bản ghi giao dịch 53 (giao dịch).

Bộ dò tìm 32 tính toán lại phần băm khối 51 được lưu trữ trong cây băm và xác định rằng giá trị băm thu được bởi việc tính toán lại có đồng nhất với phần băm khối 51 được lưu trữ trong cây băm hay không (các dòng thứ nhất đến thứ năm trong FIG.8). Nếu giá trị băm thu được bằng việc tính toán lại không đồng nhất với phần băm khối 51 được lưu trữ trong cây băm, bộ dò tìm 32 phát hiện sự giả mạo của chuỗi khối.

Bộ dò tìm 32 xác định sự hợp lệ của chữ ký số 55 được chứa trong bản ghi giao dịch 53 của khối 50 được kết nối tới cấu trúc dạng cây (dòng thứ bảy của FIG.5). Nếu chữ ký số 55 được chứa trong bản ghi giao dịch 53 là không hợp lệ, bộ dò tìm 32 phát hiện sự giả mạo của chuỗi khối.

Nếu chuỗi khối chứa không chứa các phần băm khối 51 đồng nhất với phần băm khối 51 được chứa trong bản ghi giao dịch 53 trong khối 50, bộ dò tìm 32 phát hiện sự giả mạo của chuỗi khối (các dòng thứ tám đến thứ mười trong FIG.5).

Như được mô tả nêu trên, theo cải biến thứ nhất theo phương án của sáng chế,

cấu trúc dạng cây của chuỗi khối còn hiệu quả trong trong việc phát hiện dễ dàng sự giả mạo chuỗi khối. Sử dụng giá trị băm 59, được tính toán dựa trên nội dung giao dịch 54, thay vì sử dụng nội dung giao dịch 54 cho phép xác thực chuỗi khối mà không có nội dung giao dịch 54 bị bộc lộ.

Cải biến thứ hai theo phương án của sáng chế

Cải biến thứ hai theo phương án của sáng chế sẽ được mô tả. Trong cải biến thứ hai, phần mô tả tương tự như phương án nêu trên sẽ được bỏ qua, và sự khác biệt giữa chúng sẽ được mô tả.

Phương án thứ hai liên quan đến hoạt động được thực hiện bởi kết hợp của thiết bị đầu cuối 10 (thiết bị đầu cuối thứ nhất) theo phương án của sáng chế và thiết bị đầu cuối khác (thiết bị đầu cuối thứ hai) mà tạo ra bản ghi giao dịch mà không chứa phần băm khối 51 hoặc số khối 52. Cụ thể, phương án thứ hai liên quan đến hoạt động được thực hiện, ví dụ, trong chu kỳ chuyển giao hệ thống, trong đó thiết bị đầu cuối mà tạo ra bản ghi giao dịch mà không chứa phần băm khối 51 hoặc số khối 52 di chuyển tới thiết bị đầu cuối 10 (thiết bị đầu cuối thứ nhất) theo phương án của sáng chế.

Thiết bị đầu cuối thứ nhất truyền bản ghi giao dịch thứ nhất nêu trên (bản ghi giao dịch 53n mà chứa phần băm khối 51n-k, số khối 52n-k, nội dung giao dịch 54n, và chữ ký số 55n) tới thiết bị ngang hàng 20.

Thiết bị đầu cuối thứ hai truyền bản ghi giao dịch (bản ghi giao dịch thứ hai) mà chứa bản tin được ký số (bản ghi được ký số thứ hai) mà chứa nội dung giao dịch của thiết bị đầu cuối thứ hai và chứa chữ ký số được đưa tới bản tin được ký số, tới thiết bị ngang hàng 20.

Bộ điều khiển lưu trữ 23 của thiết bị ngang hàng 20 lưu trữ khối mà chứa ít nhất một trong số bản ghi giao dịch thứ nhất và bản ghi giao dịch thứ hai trong chuỗi khối. Bộ điều khiển lưu trữ 23 thực hiện xử lý của bước S13 nêu trên trên bản ghi giao dịch thứ nhất và không thực hiện xử lý của bước S13 trên bản ghi giao dịch thứ hai.

Cấu trúc của cải biến thứ hai duy trì cùng hiệu quả như phương án của sáng chế, nếu những người dùng tốt nhập các bản ghi giao dịch thứ nhất với tần số được xác định trước hoặc cao hơn. Những người dùng tốt nêu trên có nghĩa là những người dùng mà đưa các chữ ký số tới các bản ghi giao dịch. Họ độc lập với người quản trị thiết bị ngang hàng và không có lợi nhuận từ việc giả mạo chuỗi khối.

Cải biến thứ ba theo phương án của sáng chế

Cải biến thứ ba theo phương án của sáng chế sẽ được mô tả. Trong cải biến thứ ba, phần mô tả tương tự như phương án nêu trên sẽ được bỏ qua, và sự khác biệt giữa chúng sẽ được mô tả.

Trong cải biến thứ ba, người dùng cụ thể, như người dùng tốt, đều đặn lưu trữ bản ghi giao dịch 53 trong chuỗi khối thông qua thiết bị đầu cuối 10. Người dùng cụ thể ở đây được mô tả là, ví dụ, tổ chức mà là độc lập như bên thứ ba và đang tin cậy trong xã hội. Thiết bị đầu cuối 10 được sử dụng bởi người dùng cụ thể ghi nhận, như là nội dung giao dịch 54, "sự truy nhập đều đặn của người thứ ba". Mục đích không phải là ghi nhận các giao dịch mà để lưu trữ đều đặn các bản ghi giao dịch 53 trong chuỗi khối. Bản ghi giao dịch 53 chứa phần băm khối 51, và do người dùng cụ thể là tin cậy, bản ghi giao dịch 53 mà dựa trên phần băm khối 51 được tính toán có thể được xác thực không bị giả mạo.

Bộ dò tìm 32 có thể phát hiện rằng bản ghi giao dịch 53 đã bị giả mạo, nếu bản ghi giao dịch 53 của người dùng cụ thể không được lưu trữ đều đặn trong chuỗi khối. Ví dụ, nếu người dùng có âm mưu xấu giả mạo bản ghi giao dịch 53 bằng cách xóa bản ghi, và một phần hoặc tất cả của các bản ghi giao dịch 53, mà được giả định được lưu trữ đều đặn trong chuỗi khối, không được chứa trong chuỗi khối, chuỗi khối được tìm ra là bị giả mạo.

Hệ thống dò tìm giả mạo 100 có thể được vận hành dưới dạng của cải biến thứ hai nêu trên, bằng cách cho phép người dùng cụ thể sử dụng một cách dành riêng thiết bị đầu cuối 10 theo phương án của sáng chế. Trong trường hợp này, việc phát hiện chuỗi khối chuỗi khối hoàn toàn phụ thuộc vào tính tin cậy của người dùng cụ thể.

ví dụ về cấu trúc phần cứng của thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 theo phương án của sáng chế sẽ được mô tả.

Ví dụ về cấu trúc phần cứng

FIG.9 là hình vẽ mà minh họa cấu trúc phần cứng của thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 theo phương án của sáng chế. Mỗi thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 bao gồm bộ điều khiển 401, thiết bị nhớ chính 402, thiết bị nhớ bổ trợ 403, màn hình 404, thiết bị đầu vào 405, và thiết bị truyền thông 406. Bộ điều khiển 401, thiết bị nhớ chính 402, thiết bị nhớ bổ trợ 403,

màn hình 404, thiết bị đầu vào 405, và thiết bị truyền thông 406 được kết nối tới một thiết bị khác thông qua kênh truyền 410.

Bộ điều khiển 401 thực thi chương trình máy tính được tải lên thiết bị nhớ chính 402 từ thiết bị nhớ bổ trợ 403. Thiết bị nhớ chính 402 là bộ nhớ như bộ nhớ chỉ đọc (ROM) và bộ nhớ truy nhập ngẫu nhiên (RAM). Thiết bị nhớ bổ trợ 403 là, ví dụ, ổ đĩa cứng (HDD) và thẻ nhớ.

Màn hình 404 hiển thị thông tin. Các ví dụ của màn hình 404 bao gồm màn hình tinh thể lỏng. Thiết bị đầu vào 405 là giao diện để thu dữ liệu đầu vào. Các ví dụ của thiết bị đầu vào 405 bao gồm bàn phím và chuột. Thiết bị hiển thị 404 và thiết bị đầu vào 405 có thể là, ví dụ, màn chạm có chức năng hiển thị và chức năng nhập. Thiết bị truyền thông 406 là giao diện được sử dụng cho việc truyền thông với các thiết bị khác.

Chương trình máy tính được thực thi bởi thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 theo phương án của sáng chế được lưu trữ trong phương tiện nhớ đọc được bởi máy tính như CD-ROM, thẻ nhớ, CD-R, và DVD trong tệp có thể được cài đặt hoặc thực thi, và được cung cấp như là sản phẩm chương trình máy tính.

Chương trình máy tính được thực thi bởi thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 theo phương án của sáng chế có thể được lưu trữ trong máy tính được kết nối tới mạng như Internet và được cung cấp bằng cách được tải xuống thông qua mạng. Chương trình máy tính được thực thi bởi thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 theo phương án của sáng chế có thể được cung cấp thông qua mạng như Internet mà không cần được tải xuống.

Chương trình máy tính được thực thi bởi thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 theo phương án của sáng chế có thể được cài trước trong ROM hoặc loại tương tự và được cung cấp.

Chương trình máy tính được thực thi bởi thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 theo phương án của sáng chế có cấu trúc như môđun mà bao gồm các khối chức năng được thực thi bởi chương trình máy tính, của các khối chức năng nêu trên được minh họa trong FIG.1. Đối với cấu trúc thực tế, các khối chức năng được tải lên thiết bị nhớ chính 402 với bộ điều khiển 401 mà đọc chương trình máy tính từ phương tiện nhớ và thực thi chương trình. Các khối chức năng được tạo ra

trên thiết bị nhớ chính 402.

Một vài hoặc tất cả các khối chức năng nêu trên trong FIG.1 có thể được thực hiện là phần cứng như mạch tích hợp (IC) thay vì được thực hiện là phần mềm.

Trong việc sử dụng của các bộ xử lý để thực hiện các chức năng, mỗi bộ xử lý có thể thực hiện một chức năng hoặc hai chức năng hoặc nhiều hơn.

Bất kỳ chế độ hoạt động mong muốn của thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 theo phương án của sáng chế có thể được áp dụng. Thiết bị đầu cuối 10, thiết bị ngang hàng 20, và thiết bị dò tìm 30 theo phương án của sáng chế có thể hoạt động như là các thiết bị trên nền tảng đám mây của mạng.

Trong khi một vài phương án của sáng chế đã được mô tả nêu trên, lưu ý rằng các phương án này chỉ là các ví dụ và không nhằm mục đích giới hạn phạm vi của sáng chế. các phương án mới này có thể được thực hiện trong các dạng khác nhau, và các việc bỏ qua, thay thế, và thay đổi khác nhau có thể được thực hiện mà không đi chệch khỏi bản chất của sáng chế. các phương án này và các cải biến của chúng được chứa trong phạm vi và bản chất của sáng chế, và được chứa trong phạm vi của các phần tương đương của sáng chế được bộc lộ trong yêu cầu bảo hộ đi kèm.

Ví dụ, các cải biến mà có thể dễ dàng được hiểu bởi người có hiểu biết trung bình được chứa trong phạm vi và bản chất của sáng chế, và được chứa trong phạm của các phần tương đương của sáng chế được bộc lộ trong yêu cầu bảo hộ đi kèm. Cụ thể hơn, cấu trúc dữ liệu được sử dụng cho các tính toán nêu trên của các giá trị băm không bị giới hạn ở cấu trúc chuỗi hoặc cấu trúc cây. Phương pháp tính toán các giá trị băm có thể được cải biến trong các dạng khác nhau như các tính toán trong cấu trúc liên kết, kết hợp của các tính toán, và sử dụng đệ quy của các kết quả tính toán.

YÊU CẦU BẢO HỘ

1. Hệ thống dò tìm giả mạo bao gồm:

một hoặc nhiều thiết bị đầu cuối thứ nhất mà được kết nối tới bất kỳ một trong số một hoặc nhiều thiết bị ngang hàng; và

một hoặc nhiều thiết bị dò tìm, trong đó

mỗi thiết bị đầu cuối thứ nhất bao gồm:

bộ thu nhận mà thu nhận phần băm khối được chứa trong chuỗi khối từ một trong số một hoặc nhiều thiết bị ngang hàng, và

bộ truyền mà truyền bản ghi giao dịch thứ nhất mà chứa bản tin được ký số thứ nhất chứa phần băm khối và dữ liệu dựa trên nội dung giao dịch của thiết bị đầu cuối thứ nhất và chứa chữ ký số đối với bản tin được ký số thứ nhất, tới một trong số một hoặc nhiều thiết bị ngang hàng, và

mỗi thiết bị dò tìm bao gồm:

bộ thu mà thu chuỗi khối từ thiết bị ngang hàng, và

bộ dò tìm mà phát hiện sự giả mạo của chuỗi khối khi chữ ký số được chứa trong bản ghi giao dịch thứ nhất được chứa trong khối của chuỗi khối là không hợp lệ hoặc khi chuỗi khối không chứa phần băm khối mà đồng nhất với phần băm khối được chứa trong bản ghi giao dịch thứ nhất được chứa trong khối.

2. Hệ thống dò tìm giả mạo theo điểm 1, trong đó dữ liệu dựa trên nội dung giao dịch của thiết bị đầu cuối thứ nhất là nội dung giao dịch của thiết bị đầu cuối thứ nhất hoặc giá trị băm của nội dung giao dịch của thiết bị đầu cuối thứ nhất.

3. Hệ thống dò tìm giả mạo theo điểm 1, trong đó

bản tin được ký số thứ nhất còn chứa số khối của khối tương ứng với phần băm khối, và

bộ dò tìm lưu trữ khối mà chứa bản ghi giao dịch thứ nhất trong chuỗi khối, khi chữ ký số được chứa trong bản ghi giao dịch thứ nhất là hợp lệ, và khi phần băm khối của khối được nhận dạng từ chuỗi khối sử dụng số khối được chứa trong bản ghi giao dịch thứ nhất là đồng nhất với phần băm khối được chứa trong bản ghi giao dịch thứ nhất.

4. Hệ thống dò tìm giả mạo theo điểm 3, trong đó bộ thu nhận thu nhận phần băm khối

mới hơn trong số các phần băm khối được chứa trong chuỗi khối trên cơ sở của số khối.

5. Hệ thống dò tìm giả mạo theo điểm 1, trong đó bộ thu nhận thu nhận phần băm khối mới hơn trong số các phần băm khối được chứa trong chuỗi khối, trên cơ sở của thời điểm khi phần băm khối được tạo ra.

6. Hệ thống dò tìm giả mạo theo điểm 1, trong đó bộ thu nhận thu nhận, từ trong số các phần băm khối được chứa trong chuỗi khối và như là khối mới hơn, phần băm khối mà nhiều bản ghi giao dịch thứ nhất được lưu trữ trong chuỗi khối được sử dụng cho việc tính toán giá trị băm.

7. Hệ thống dò tìm giả mạo theo điểm 1, trong đó bộ thu nhận thu nhận phần băm khối được chứa trong chuỗi khối, và sau khi thu được phần băm khối mới, loại bỏ phần băm khối thu được trước khi phần băm khối mới được thu nhận.

8. Hệ thống dò tìm giả mạo theo điểm 1, còn bao gồm một hoặc nhiều thiết bị ngang hàng, trong đó

mỗi thiết bị ngang hàng bao gồm bộ điều khiển lưu trữ mà lưu trữ khối chứa bản ghi giao dịch thứ nhất trong chuỗi khối khi chữ ký số được chứa trong bản ghi giao dịch thứ nhất là hợp lệ, và khi chuỗi khối chứa phần băm khối mà đồng nhất với phần băm khối được chứa trong bản ghi giao dịch thứ nhất.

9. Hệ thống dò tìm giả mạo theo điểm 8, còn bao gồm một hoặc nhiều thiết bị đầu cuối thứ hai, trong đó

thiết bị đầu cuối thứ hai truyền bản ghi giao dịch thứ hai mà chứa bản tin được ký số thứ hai chứa nội dung giao dịch của thiết bị đầu cuối thứ hai và chứa chữ ký số đối với bản tin được ký số thứ hai, tới một trong số một hoặc nhiều thiết bị ngang hàng, và

bộ điều khiển lưu trữ lưu trữ khối mà chứa ít nhất một trong số bản ghi giao dịch thứ nhất và bản ghi giao dịch thứ hai trong chuỗi khối.

10. Hệ thống dò tìm giả mạo theo điểm 1, trong đó

một hoặc nhiều thiết bị đầu cuối thứ nhất bao gồm thiết bị đầu cuối thứ nhất mà người dùng cụ thể truyền bản ghi giao dịch thứ nhất tới đó, và

bộ dò tìm còn xác định rằng bản ghi giao dịch thứ nhất được truyền từ người dùng cụ thể có được chứa trong chuỗi khối hay không và phát hiện sự giả mạo của

chuỗi khối khi một phần hoặc tất cả bản ghi giao dịch thứ nhất được truyền từ người dùng cụ thể không được chứa trong chuỗi khối.

11. Phương pháp dò tìm giả mạo của hệ thống dò tìm giả mạo mà bao gồm một hoặc nhiều thiết bị đầu cuối thứ nhất được kết nối tới bất kỳ một trong số một hoặc nhiều thiết bị ngang hàng và một hoặc nhiều thiết bị dò tìm, phương pháp này bao gồm:

bước thu nhận, bởi thiết bị đầu cuối thứ nhất, phần băm khối được chứa trong chuỗi khối từ một trong số một hoặc nhiều thiết bị ngang hàng;

bước truyền, bởi thiết bị đầu cuối thứ nhất, bản ghi giao dịch thứ nhất mà chứa bản tin được ký số thứ nhất chứa phần băm khối và dữ liệu dựa trên nội dung giao dịch của thiết bị đầu cuối thứ nhất và chứa chữ ký số đối với bản tin được ký số thứ nhất, tới một trong số một hoặc nhiều thiết bị ngang hàng;

bước thu, bởi thiết bị dò tìm, chuỗi khối từ thiết bị ngang hàng; và

bước dò tìm, bởi bộ dò tìm, sự giả mạo của chuỗi khối khi chữ ký số được chứa trong bản ghi giao dịch thứ nhất được chứa trong khối của chuỗi khối là không hợp lệ hoặc khi chuỗi khối không chứa phần băm khối mà đồng nhất với phần băm khối được chứa trong bản ghi giao dịch thứ nhất được chứa trong khối.

FIG.1

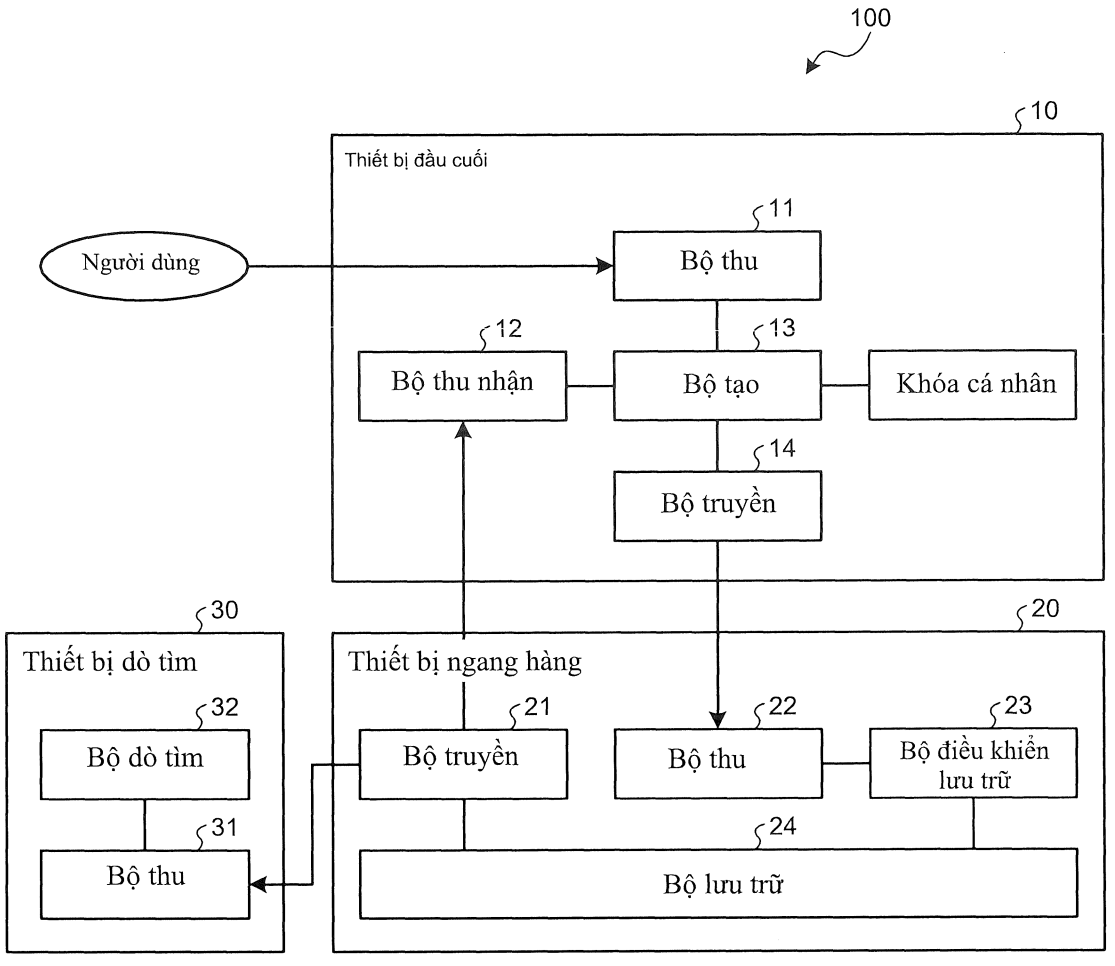

100
10
Thiết bị đầu cuối
11
Người dùng
Bộ thu
12
13
Bộ thu nhận
Bộ tạo
Khóa cá nhân
14
Bộ truyền
30
20
Thiết bị dò tìm
Thiết bị ngang hàng
32
21
22
23
Bộ dò tìm
Bộ truyền
Bộ thu
Bộ điều khiển lưu trữ
31
24
Bộ thu
Bộ lưu trữ

FIG.2

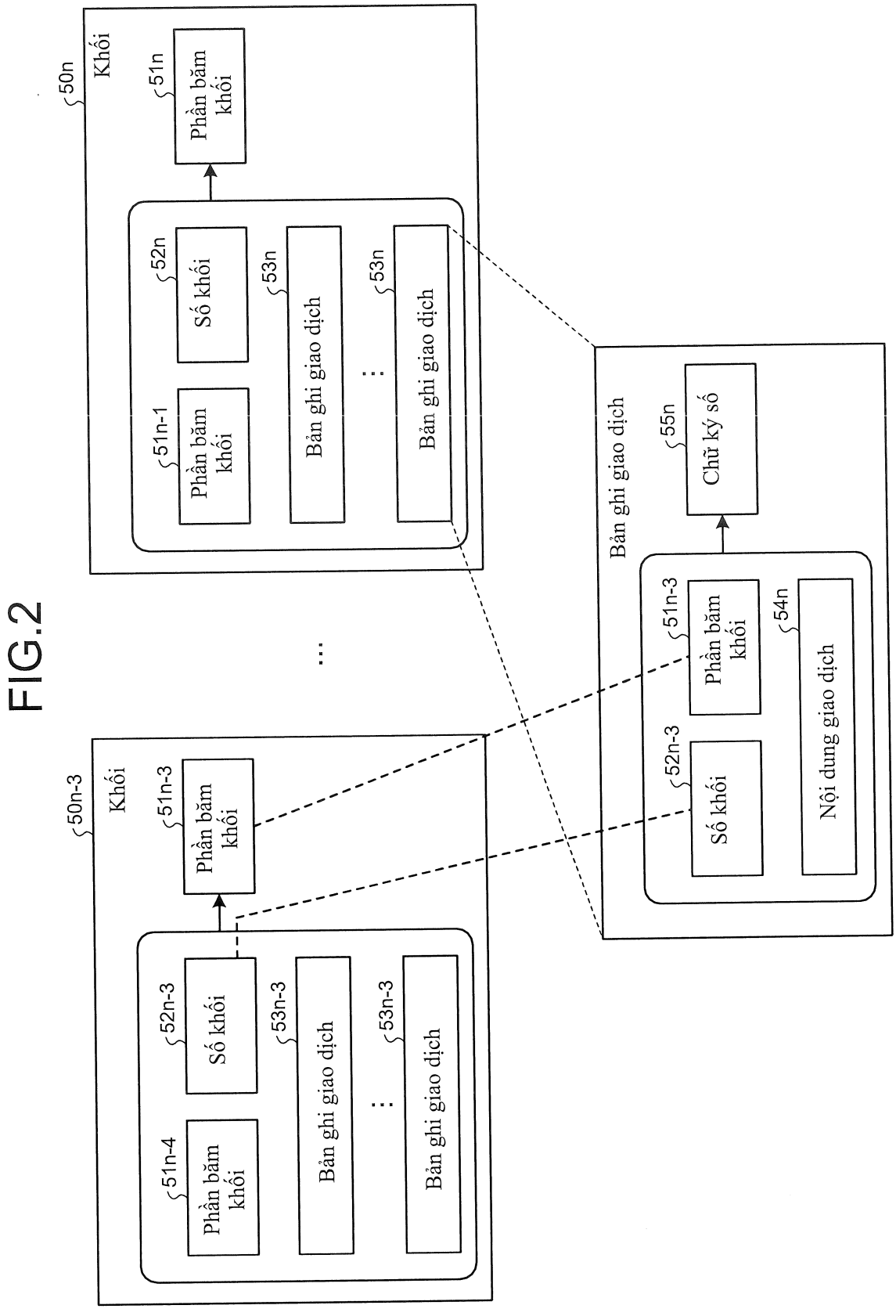

50n
Khối
51n
Phần băm khối
52n
Số khối
53n
Bản ghi giao dịch
53n
Bản ghi giao dịch
51n-1
Phần băm khối
50n-3
Khối
51n-3
Phần băm khối
52n-3
Số khối
53n-3
Bản ghi giao dịch
53n-3
Bản ghi giao dịch
51n-4
Phần băm khối
Bản ghi giao dịch
55n
Chữ ký số
51n-3
Phần băm khối
54n
Nội dung giao dịch
52n-3
Số khối

FIG.3

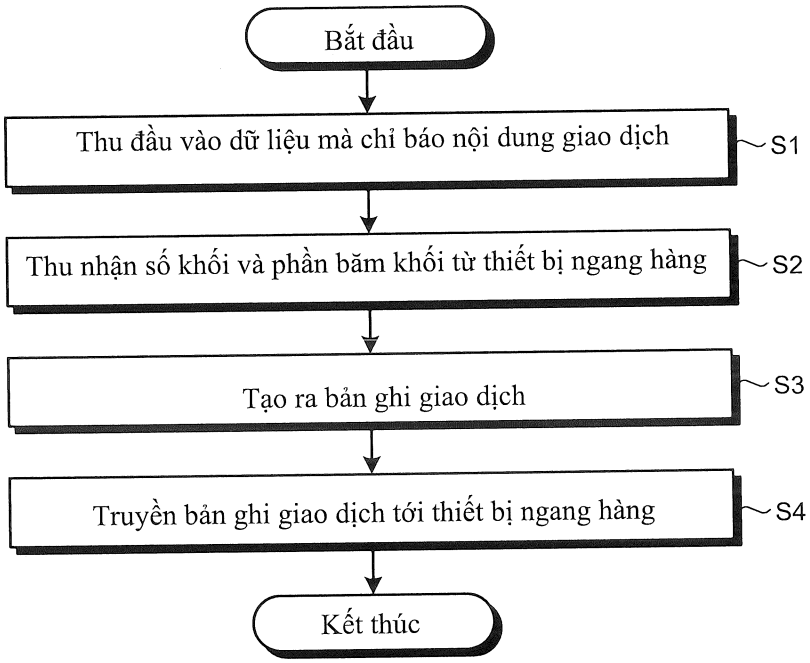

Bắt đầu
Thu đầu vào dữ liệu mà chỉ báo nội dung giao dịch
S1
Thu nhận số khối và phần băm khối từ thiết bị ngang hàng
S2
Tạo ra bản ghi giao dịch
S3
Truyền bản ghi giao dịch tới thiết bị ngang hàng
S4
Kết thúc

FIG.4

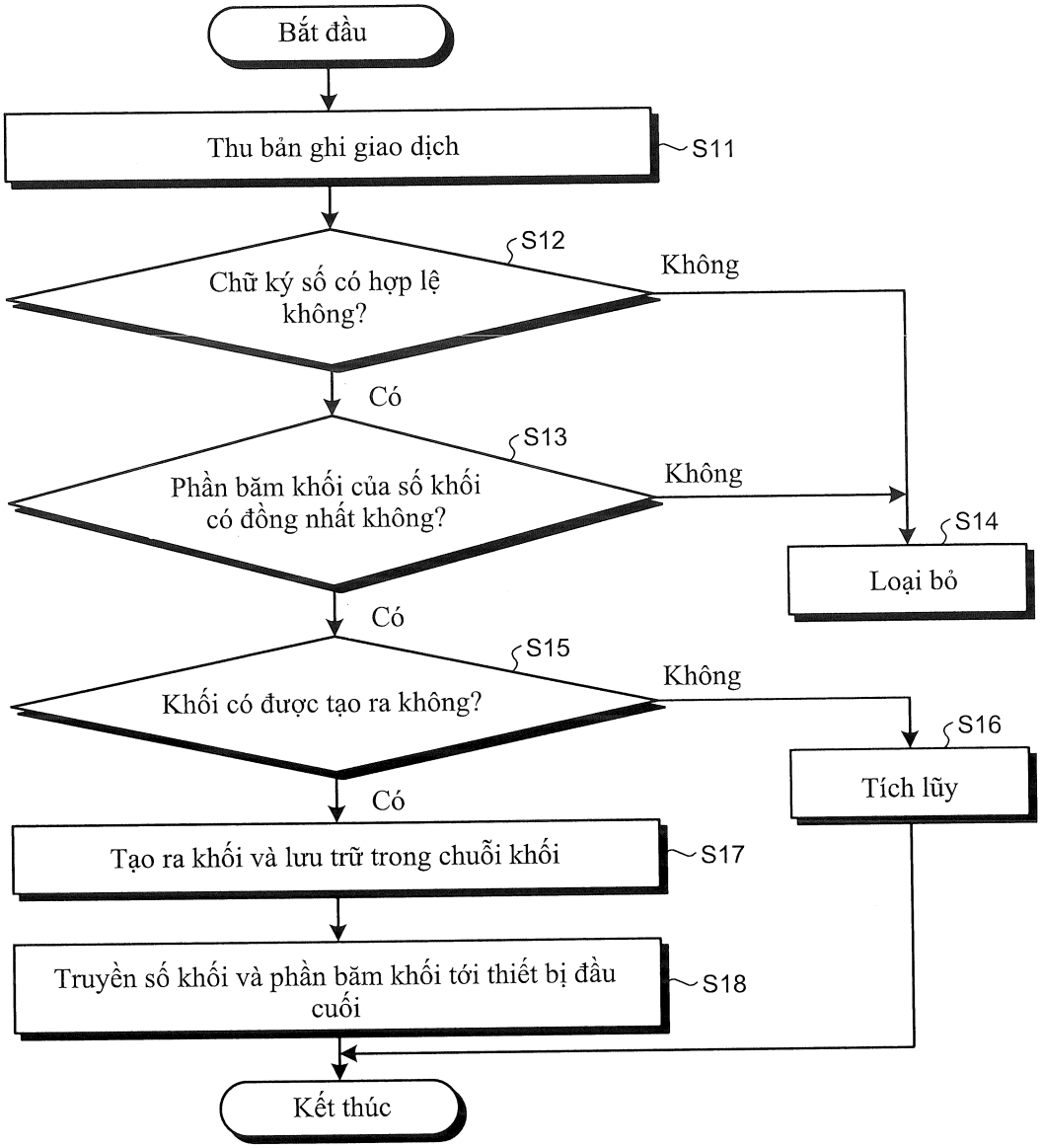

Bắt đầu
Thu bản ghi giao dịch
S11
S12
Chữ ký số có hợp lệ không?
Không
Có
S13
Phần băm khối của số khối có đồng nhất không?
Không
S14
Loại bỏ
Có
S15
Khối có được tạo ra không?
Không
S16
Tích lũy
Có
Tạo ra khối và lưu trữ trong chuỗi khối
S17
Truyền số khối và phần băm khối tới thiết bị đầu cuối
S18
Kết thúc

FIG.5

```
1     for (khối của tất cả khối) {
2     var h1 = phần băm khối được ghi trong khối
3     var h2 = Phần băm khối được tính toán lai
4     nếu (h1 khác h2) thì phát hiện sự giả mạo
5  }
6        for (khối của tất cả khối) {
7     for (tx của tất cả bản ghi giao dịch được chứa trong khối) {
8     if (chữ ký số của tx là không hợp lệ) thì phát hiện sự giả mạo
9     var h = phần băm khối được chứa trong tx
10    var i = số khối được chứa trong tx
11    if (phần băm khối của số khối i trong chuỗi khối không đồng nhất với h) thì phát hiện sự giả mạo
12
13    }
14 }
```

FIG.6

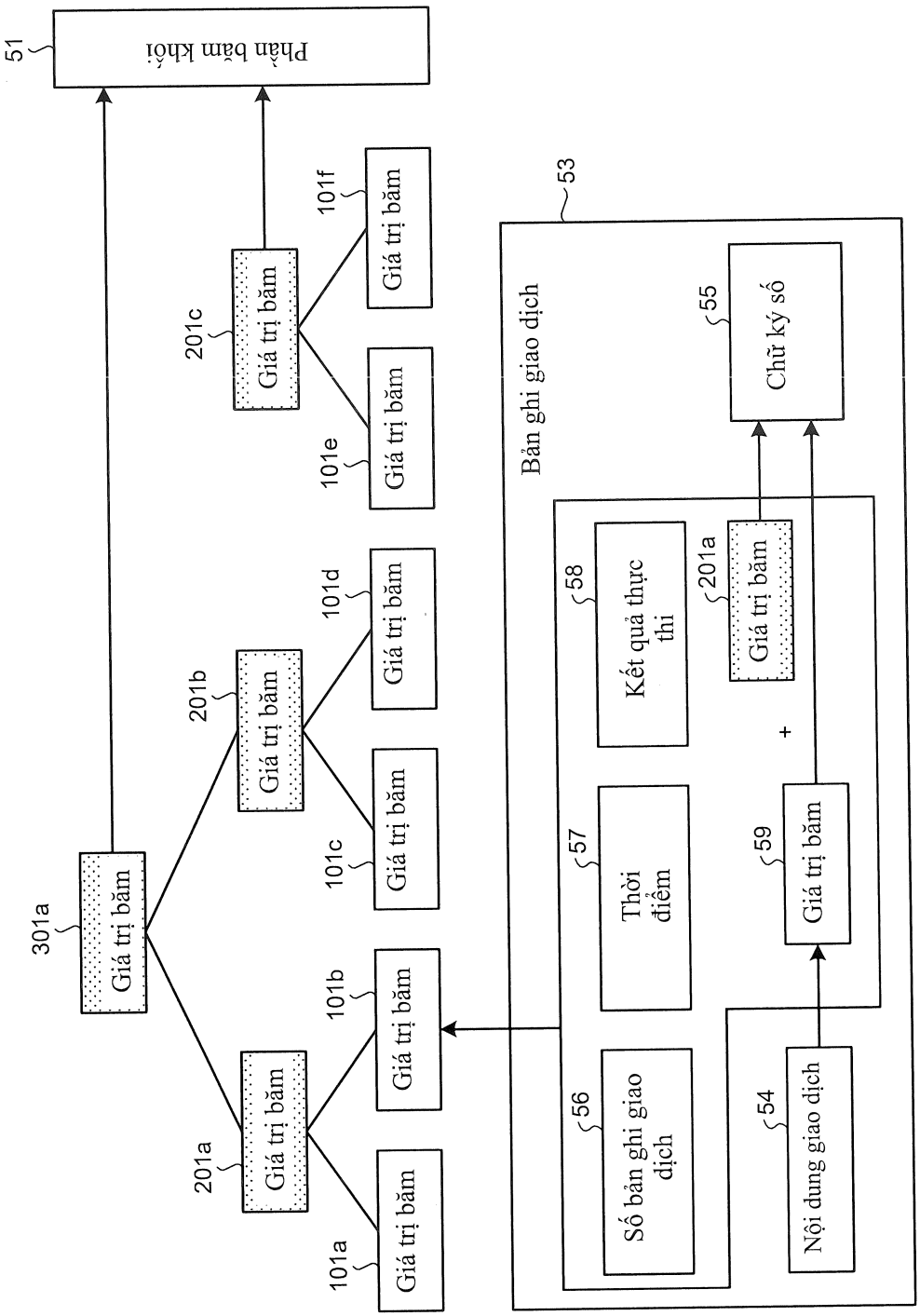

Phần băm khối
51
Bản ghi giao dịch
53
Chữ ký số
55
Kết quả thực thi
58
Thời điểm
57
Số bản ghi giao dịch
56
Nội dung giao dịch
54
Giá trị băm
59
Giá trị băm
201a
+
301a
Giá trị băm
201a
Giá trị băm
201b
Giá trị băm
201c
Giá trị băm
101a
Giá trị băm
101b
Giá trị băm
101c
Giá trị băm
101d
Giá trị băm
101e
Giá trị băm
101f

FIG.7

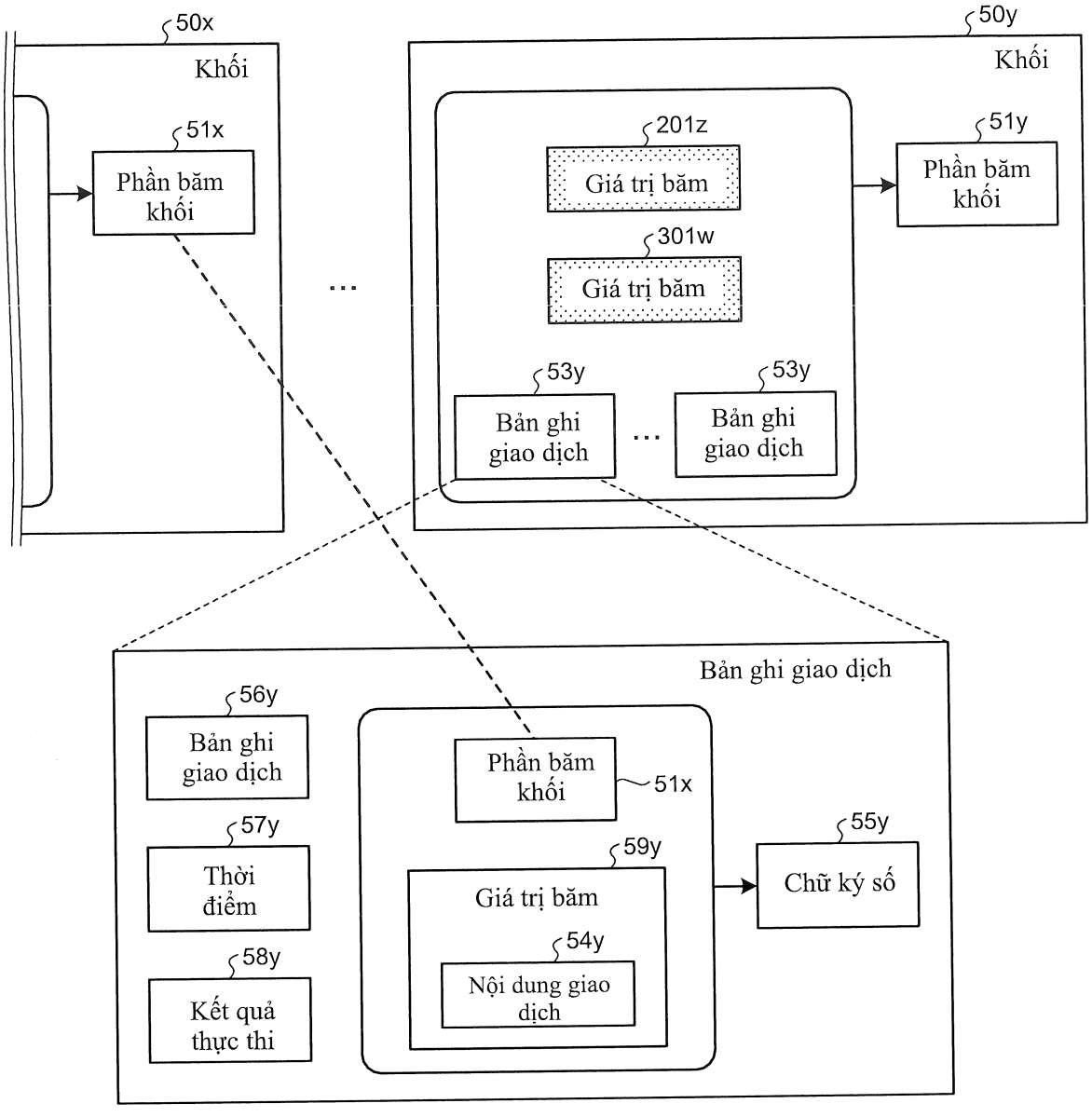

50x
Khối
51x
Phần băm khối
...
50y
Khối
201z
Giá trị băm
301w
Giá trị băm
53y
Bản ghi giao dịch
...
53y
Bản ghi giao dịch
51y
Phần băm khối
Bản ghi giao dịch
56y
Bản ghi giao dịch
57y
Thời điểm
58y
Kết quả thực thi
Phần băm khối
51x
59y
Giá trị băm
54y
Nội dung giao dịch
55y
Chữ ký số

FIG.8

```
1  for (h1 của tất cả phần băm khối được ghi) {
2      var h2 = tính toán lại phần băm khối tương ứng từ bản ghi giao dịch
3  được lưu trữ
4      if (h1 khác h2) thì phát hiện sự giả mạo
5  }
6  for (tx của tất cả bản ghi giao dịch) {
7      if (chữ ký số của tx là không hợp lệ) thì phát hiện sự giả mạo
8      var h = phần băm khối được chứa trong tx
9      if (h không được lưu trữ trong bộ nhớ như phần băm khối) thì phát hiện sự giả mạo
10
11 }
```

FIG.9