



(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)



1-0047878

(51)^{2020.01} G06F 21/64; H04L 9/32

(13) B

(21) 1-2022-01583

(22) 21/10/2019

(86) PCT/JP2019/041396 21/10/2019

(87) WO 2021/079416 29/04/2021

(45) 25/06/2025 447

(43) 25/07/2022 412A

(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) ENDO, Kotaro (JP).

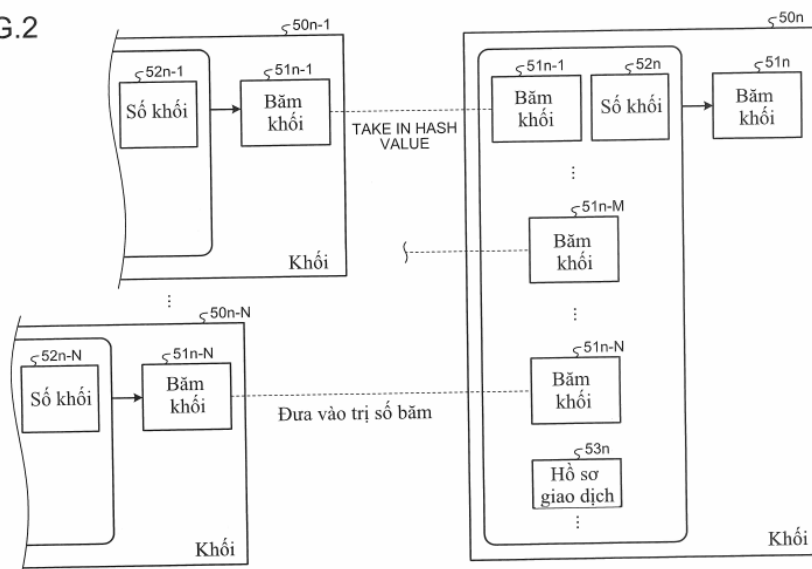
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP XÁC THỰC GIẢ MẠO VÀ HỆ THỐNG XÁC THỰC GIẢ MẠO

(21) 1-2022-01583

(57) Sáng chế đề cập đến phương pháp xác thực giả mạo bao gồm: bước tính băm khối dựa vào các băm khối khác của các khối khác và thông tin duy nhất và tạo ra chuỗi khối trong đó khối chứa băm khối được tính được kết nối; bước, đáp lại việc thu yêu cầu xác thực cho khối xác thực được chứa trong chuỗi khối, tạo ra chứng nhận được sử dụng cho phép tính lại của các khối tính lại chứa các băm khối mà phụ thuộc vào băm khối của khối xác thực, cho các băm khối khác; và bước, đáp lại việc thu chứng nhận, xác thực khối xác thực bằng cách tính lại các băm khối của các khối tính lại nhờ sử dụng chứng nhận.

FIG.2



Lĩnh vực kỹ thuật được đề cập

Các phương án của sáng chế đề cập đến phương pháp xác thực giả mạo và hệ thống xác thực giả mạo.

Tình trạng kỹ thuật của sáng chế

Các tiền mã hóa được biểu diễn bởi các bitcoin đã được đưa vào sử dụng thực tế. Các hồ sơ chuyển khoản tiền mã hóa được lưu trữ trong sổ cái điện tử được gọi là chuỗi khối. Trong trường hợp các bitcoin, việc chấp nhận phương pháp được gọi là bằng chứng công việc khiến việc giả mạo chuỗi khối trở nên khó khăn. Bằng chứng công việc là cơ sở của việc bảo mật bitcoin. Trong khi đó việc ghi các giao dịch chung, không giới hạn ở việc chuyển khoản, trong sổ cái điện tử đã bắt đầu, như ứng dụng của chuỗi khối. Ngoài ra, với chuỗi khối, công nghệ hợp đồng điện tử được gọi là hợp đồng thông minh cũng được đưa vào sử dụng thực tế. Trong việc ứng dụng của chuỗi khối, phương pháp duy trì tính nhất quán chuỗi khối giữa các thiết bị ngang hàng cũng được đưa vào sử dụng thực tế nhờ sử dụng thuật toán đồng thuận chung mà không sử dụng bằng chứng công việc. Chuỗi khối như vậy được gọi là chuỗi khối được cho phép.

Danh mục tài liệu trích dẫn

Tài liệu sáng chế

Tài liệu sáng chế 1: JP 2017-207979 A

Bản chất kỹ thuật của sáng chế

Vấn đề cần được giải quyết bởi sáng chế

Tuy nhiên, theo công nghệ thông thường, khó làm giảm thời gian xác thực chuỗi khối.

Phương tiện giải quyết vấn đề

Phương pháp xác thực giả mạo theo phương án bao gồm: bước tính băm

khối dựa vào các băm khối khác của các khối khác và thông tin duy nhất và tạo ra chuỗi khối trong đó khối chứa băm khối được tính được kết nối; bước, đáp lại việc thu yêu cầu xác thực cho khối xác thực được chứa trong chuỗi khối, tạo ra chứng nhận được sử dụng cho phép tính lại của các khối tính lại chứa các băm khối mà phụ thuộc vào băm khối của khối xác thực, cho các băm khối khác; và bước, đáp lại việc thu chứng nhận, xác thực khối xác thực bằng cách tính lại các băm khối của các khối tính lại nhờ sử dụng chứng nhận.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ minh họa ví dụ về cấu hình của hệ thống xác thực giả mạo theo phương án thứ nhất.

Fig.2 là hình vẽ minh họa ví dụ về cấu trúc dữ liệu chuỗi khối theo phương án thứ nhất.

Fig.3 là hình vẽ minh họa ví dụ về khối #24 theo phương án thứ nhất.

Fig.4 là hình vẽ minh họa ví dụ về việc kết nối của chuỗi khối theo phương án thứ nhất.

Fig.5 là hình vẽ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ nhất.

Fig.6A là lưu đồ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ nhất.

Fig.6B là lưu đồ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ nhất.

Fig.7 là hình vẽ minh họa ví dụ về việc kết nối của chuỗi khối theo phương án thứ hai.

Fig.8A là lưu đồ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ hai.

Fig.8B là lưu đồ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ hai.

Fig.9A là lưu đồ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ năm.

Fig.9B là lưu đồ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ năm.

Fig.10 là hình vẽ minh họa ví dụ về cấu hình phần cứng của thiết bị ngang hàng và thiết bị xác thực theo các phương án từ thứ nhất đến thứ năm.

Mô tả chi tiết sáng chế

Các phương án của phương pháp xác thực giả mạo và hệ thống xác thực giả mạo sẽ được mô tả chi tiết dưới đây dựa vào các hình vẽ kèm theo.

Trong chuỗi khối, trong phép tính băm khối cho khối nhất định, băm khối của khối trước đó được đưa vào cho việc tính toán. Vì vậy, các phép tính băm được liên kết thành chuỗi, và toàn bộ khả năng chống giả mạo có thể được thu nhận. Ví dụ, nếu nội dung của khối quá khứ đã bị giả mạo, thì các trị số băm khối được tính lặp lại theo thứ tự từ khối, việc thực hiện các phép so sánh để xác định xem các trị số trùng khớp các trị số được lưu trữ trong chuỗi khối hay không, việc tìm thấy sự không nhất quán khi phép tính đạt đến khối không bị giả mạo, và việc giả mạo có thể được phát hiện.

Một cách ngẫu nhiên, chuỗi khối được cho phép yêu cầu thời gian tương đối ngắn để tính lại các băm khối khi được so với chuỗi khối bằng chứng công việc, vì vậy làm cho việc giả mạo với băm khối trong chuỗi khối rất dài tương đối dễ dàng.

Việc phát hiện việc giả mạo quy mô lớn như vậy với các băm khối yêu cầu phép tính lại của các trị số băm trong khi theo dõi chuỗi khối dài, gây ra vấn đề là việc xác thực mất thời gian dài.

Ngoài ra, để cấp bên ngoài chứng nhận chống giả mạo của khối quá khứ, cần lưu hàng loạt các trị số băm khối như chứng nhận, nhưng cũng có vấn đề là kích thước dữ liệu của chứng nhận trở nên lớn.

(Phương án thứ nhất)

Thứ nhất, ví dụ về cấu hình của hệ thống xác thực giả mạo theo phương án thứ nhất sẽ được mô tả.

[Ví dụ về cấu hình]

Fig.1 là hình vẽ minh họa ví dụ về cấu hình của hệ thống xác thực giả mạo 100 theo phương án thứ nhất. Hệ thống xác thực giả mạo 100 theo phương án thứ nhất bao gồm thiết bị ngang hàng 10 và thiết bị xác thực 20. Thiết bị ngang hàng 10 bao gồm bộ phận tạo ra 11, bộ phận lưu trữ 12, và bộ phận xác thực thứ nhất 13. Thiết bị xác thực 20 bao gồm bộ phận xác thực thứ hai 21.

Thiết bị ngang hàng 10 là thiết bị máy chủ mà lưu trữ chuỗi khối. Nói chung, các thiết bị ngang hàng 10 được đề xuất, và tất cả các thiết bị ngang hàng 10 lưu trữ cùng chuỗi khối.

Bộ phận tạo ra 11 tạo ra chuỗi khối. Chuỗi khối là sổ cái điện tử mà chứa một hoặc nhiều hồ sơ giao dịch. Theo phương án thứ nhất, chuỗi khối loại bitcoin điển hình được giả sử là cấu hình của chuỗi khối. Nói cách khác, các (có thể là 0) hồ sơ giao dịch được thu thập theo chuỗi thời gian để tạo nên các khối. Các khối được gán với các số khối theo thứ tự tăng dần theo chuỗi thời gian.

Băm khối biểu diễn trị số băm mà được tính từ chuỗi dữ liệu chứa các hồ sơ giao dịch được chứa trong khối. Trị số băm là trị số được tính bởi hàm băm mà khiến cho việc thực hiện phép tính ngược trở nên khó khăn và có xác suất xung đột băm thấp. Băm khối được ghi trên chuỗi khối cùng với khối. Băm khối được tính đệ quy, và do đó, các hồ sơ giao dịch là đích tính cho băm khối được xét đến là tất cả các hồ sơ giao dịch trước khối. Do đó, ví dụ, khi hồ sơ giao dịch quá khứ bị giả mạo, tất cả các băm khối tiếp theo khối thay đổi.

Băm khối về mặt lý thuyết có thể được tính lại từ các hồ sơ giao dịch, nhưng đối với hiệu quả xử lý thêm, băm khối được lưu trữ trong bộ phận lưu trữ 12 cùng với các hồ sơ giao dịch cho mỗi khối.

Chuỗi khối theo phương án thứ nhất có thể là chuỗi khối bằng chứng công việc hoặc chuỗi khối được cho phép.

Fig.2 là hình vẽ minh họa ví dụ về cấu trúc dữ liệu chuỗi khối theo phương án thứ nhất. Cấu trúc dữ liệu chuỗi khối theo phương án thứ nhất khác với cấu trúc dữ liệu chuỗi khối thông thường. Đối với phép tính của băm khối $51n$ của khối $50n$ được chứa trong chuỗi khối theo phương án thứ nhất, không những băm khối $51n-1$ của khối trước đó $50n-1$ mà còn các băm khối (các băm khối khác) của các khối khác không giới hạn ở khối trước đó được sử dụng. Theo ví dụ trên Fig.2, phép tính của băm khối $51n$ sử dụng các các băm khối khác (băm khối trước đó $51n-1, \dots$, băm khối $51n-M$ được bố trí trước M băm khối cuối cùng, $\dots$, băm khối $51n-N$ được bố trí trước N băm khối cuối cùng), số khối $52n$ và hồ sơ giao dịch $53n$.

Các băm khối khác được nhận dạng bởi tập hợp của các số khối khác được xác định trên cơ sở của các số khối của các khối được kết nối. Ví dụ, các băm khối khác được nhận dạng bởi các số khối được chứa trong tập hợp $S(BN)$ được định rõ như sau.

Khi BN là số lẻ, $S(BN) = \{BN - 1\} \cap N$.

Khi BN là số mà có thể chia được cho 2 nhưng không thể chia được cho 4,

$S(BN) = \{BN - 1, BN - 2\} \cap N$.

Khi BN là số mà có thể chia được cho 4 nhưng không thể chia được cho 8,

$S(BN) = \{BN - 1, BN - 2, BN - 4\} \cap N$.

Nói chung, khi BN là số chẵn và BN là số mà có thể chia được cho 2^n nhưng không thể chia được cho $2^{(n+1)}$,

$S(BN) = \{BN - 2^m | m \text{ là số nguyên thỏa mãn } 0 \leq m \leq n\} \cap N$.

Ở đây, BN biểu diễn số khối, và N biểu diễn tập hợp của tất cả các số tự nhiên. Băm khối của khối có số khối BN được tính trên cơ sở của các băm khối khác được nhận dạng bởi các số khối $b \in S(BN)$ và thông tin duy nhất được chứa trong khối có số khối BN .

Quay lại Fig.1, bộ phận tạo ra 11 tính băm khối trên cơ sở của các băm khối

còn lại của các khối khác và thông tin duy nhất, và tạo ra chuỗi khối trong đó khối chứa băm khối được tính được kết nối.

Thông tin duy nhất bao gồm ít nhất một trong số thông tin dựa vào các hồ sơ giao dịch, và số khối BN. Lưu ý rằng thông tin duy nhất còn có thể bao gồm chuỗi ký tự ngẫu nhiên hoặc tương tự, nhằm mục đích tăng cường khả năng chống giả mạo.

Thông tin dựa vào các hồ sơ giao dịch có thể chính là các hồ sơ giao dịch hoặc trị số băm của các hồ sơ giao dịch. Phép tính cho băm khối nhờ sử dụng trị số băm của các hồ sơ giao dịch loại bỏ nhu cầu tham chiếu tới các nội dung giao dịch thô (các hồ sơ giao dịch) trong phép tính lại cho băm khối, và mang lại hiệu quả có lợi của việc nâng cao bảo mật thông tin. Phép tính cho băm khối nhờ sử dụng trị số băm của các hồ sơ giao dịch sẽ được mô tả theo phương án thứ tự được mô tả dưới đây.

Bộ phận lưu trữ 12 lưu trữ chuỗi khối được tạo ra (được cập nhật) bởi bộ phận tạo ra 11.

Khi thu yêu cầu xác thực cho khối xác thực được chứa trong chuỗi khối, bộ phận xác thực thứ nhất 13 tạo ra chứng nhận được sử dụng cho phép tính lại của các khối tính lại chứa các băm khối mà tùy thuộc vào băm khối của khối xác thực, cho các băm khối khác được sử dụng cho phép tính băm. Lưu ý rằng thiết bị bất kỳ có thể được sử dụng để truyền yêu cầu xác thực tới thiết bị ngang hàng 10. Bộ phận xác thực thứ nhất 13 truyền chứng nhận tới thiết bị xác thực 20.

Chứng nhận chứa, ví dụ, thông tin duy nhất về các khối tính lại, các băm khối của các khối tính lại, và các băm khối khác được sử dụng cho phép tính của các băm khối của các khối tính lại.

Khi thu chứng nhận từ thiết bị ngang hàng 10, bộ phận xác thực thứ hai 21 của thiết bị xác thực 20 tính lại các băm khối của các khối tính lại nhờ sử dụng chứng nhận để xác thực khối xác thực.

[Ví dụ về khối]

Fig.3 là hình vẽ minh họa ví dụ về khối #24 theo phương án thứ nhất. Khối #24 biểu diễn khối có số khối BN 24. Số khối BN = 24 có thể chia được cho 2^3 nhưng không thể chia được cho 2^4 , và $S(BN = 24) = \{16, 20, 22, 23\}$. Do đó, phép tính của băm khối 51a của khối #24 sử dụng, như các băm khối khác, băm khối trước đó 51b (BN = 23), băm khối 51c (BN = 22) được bố trí trước băm khối cuối cùng, băm khối 51d (BN = 20) được bố trí trước bốn băm khối cuối cùng, và băm khối 51e (BN = 16) được bố trí trước tám băm khối cuối cùng.

Fig.4 là hình vẽ minh họa ví dụ về việc kết nối của chuỗi khối theo phương án thứ nhất. Ví dụ, khối #24 $S(BN = 24) = \{16, 20, 22, 23\}$, và khối #24 được kết nối với khối #16, khối #20, khối #22, và khối #23.

[Ví dụ về phương pháp xác thực giả mạo]

Fig.5 là hình vẽ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ nhất. Ví dụ trên Fig.5 thể hiện việc lựa chọn khối #5 là khối xác thực trong chuỗi khối lên tới khối #24. Theo ví dụ trên Fig.5, đối với việc xác thực không xáo trộn của khối #5, bốn lần tính lại băm khối (các băm khối #6, #8, #16, và #24) và tham chiếu tới 12 băm khối khác được thực hiện bởi bộ phận xác thực thứ nhất 13 và bộ phận xác thực thứ hai 21.

Hơn nữa, theo ví dụ trên Fig.5, chứng nhận được tạo ra bởi bộ phận xác thực thứ nhất 13 chứa thông tin duy nhất về các khối tính lại (các khối #6, #8, #16, và #24), các băm khối (các băm khối #6, #8, #16, và #24) của các khối tính lại, và 12 băm khối khác được sử dụng cho phép tính của các băm khối của các khối tính lại.

Fig.6A và Fig.6B là các lưu đồ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ nhất. Lưu đồ trên Fig.6A và Fig.6B minh họa ví dụ về lưu đồ để thực hiện phương pháp xác thực giả mạo trên Fig.5 nêu trên. Quy trình xử lý của các lưu đồ trên Fig.6A và Fig.6B được thực hiện bởi bộ phận xác thực thứ nhất 13.

Thứ nhất, bộ phận xác thực thứ nhất 13 thiết đặt số khối của khối xác thực tới BN0 và thiết đặt băm khối của khối xác thực tới BH0 (bước S1).

Tiếp theo, bộ phận xác thực thứ nhất 13 thiết đặt số khối mới nhất tới BN và thiết đặt băm khối của số khối mới nhất được lưu trữ trên chuỗi khối (thiết bị ngang hàng 10) tới BH (bước S2).

Tiếp theo, bộ phận xác thực thứ nhất 13 xác định xem $BN = BN0$ hay không (bước S3).

Khi $BN = BN0$ (bước S3, đúng), được xác định xem $BH = BH0$ hay không (bước S4). Khi $BH = BH0$ (bước S4, đúng), bộ phận xác thực thứ nhất 13 xác định thành công xác thực và hoàn tất quy trình xử lý. Khi $BH \neq BH0$ (bước S4, sai), bộ phận xác thực thứ nhất 13 xác định lỗi xác thực và hoàn tất quy trình xử lý.

Khi $BN \neq BN0$ (bước S3, sai), bộ phận xác thực thứ nhất 13 thiết đặt danh mục trống tới L, và thiết đặt 1 tới K (bước S5). Tiếp theo, bộ phận xác thực thứ nhất 13 thiết đặt băm khối của số khối BN-K được lưu trữ trên chuỗi khối (thiết bị ngang hàng 10) tới H (bước S6). Tiếp theo, bộ phận xác thực thứ nhất 13 bổ sung H tới danh mục L (bước S7).

Tiếp theo, bộ phận xác thực thứ nhất 13 xác định xem $BN - K \geq BN0$ hay không (bước S8). Trong trường hợp $BN - K \geq BN0$ (bước S8, đúng), bộ phận xác thực thứ nhất 13 thiết đặt BN-K tới BN1, thiết đặt H tới BH1 (bước S9), và đến bước S10. Trong trường hợp không là $BN - K \geq BN0$ (bước S8, sai), quy trình xử lý đến bước S10 mà không thực hiện việc xử lý của bước S9.

Tiếp theo, bộ phận xác thực thứ nhất 13 gấp đôi trị số của K (bước S10). Sau đó, bộ phận xác thực thứ nhất 13 xác định xem BN có thể chia được cho K và $BN > K$ hay không (bước S11). Khi BN có thể chia được cho K và $BN > K$ (bước S11, đúng), quy trình xử lý quay lại bước S6.

Khi BN không thể chia được cho K hoặc trong trường hợp không là $BN > K$ (bước S11, sai), bộ phận xác thực thứ nhất 13 thiết đặt, tới H2, băm khối của số khối BN được tính nhờ sử dụng các trị số được chứa trong danh mục L bởi phương pháp định trước (bước S12).

Tiếp theo, bộ phận xác thực thứ nhất 13 xác định xem $BH = H2$ hay không (bước S13). Trong trường hợp $BH \neq H2$ (bước S13, sai), bộ phận xác thực thứ nhất 13 xác định lỗi xác thực và hoàn tất quy trình xử lý. Trong trường hợp $BH = H2$ (bước S13, đúng), bộ phận xác thực thứ nhất 13 thiết đặt BN1 tới BN, BH1 tới BH, và quay lại việc xử lý của bước S3.

Dựa vào thành công xác thực, bộ phận xác thực thứ nhất tạo lập chứng nhận mà bao gồm tất cả thông tin duy nhất về các khối tính lại, các băm khối của các khối tính lại, và các băm khối khác được sử dụng cho phép tính của các băm khối của các khối tính lại, mà được tham chiếu dựa vào hiệu xuất của lưu đồ.

Khi thu chứng nhận, bộ phận xác thực thứ hai thực hiện quy trình xử lý của các lưu đồ được minh họa trên Fig.6A và Fig.6B. Tại thời điểm này, băm khối được sử dụng cho phép tính được thu nhận từ chứng nhận nêu trên được truyền từ thiết bị ngang hàng 10. Nói cách khác, dựa vào thành công xác thực, bộ phận xác thực thứ nhất và bộ phận xác thực thứ hai thực hiện một cách chính xác cùng phép tính.

Như được nêu trên, trong hệ thống xác thực giả mạo 100 theo phương án thứ nhất, bộ phận tạo ra 11 tính băm khối trên cơ sở của các băm khối khác của các khối khác và thông tin duy nhất, và tạo ra chuỗi khối trong đó khối chứa băm khối được tính được kết nối. Khi thu yêu cầu xác thực cho khối xác thực được chứa trong chuỗi khối, bộ phận xác thực thứ nhất 13 tạo ra chứng nhận được sử dụng cho phép tính lại của các khối tính lại chứa các băm khối mà phụ thuộc vào băm khối của khối xác thực, cho các băm khối khác được sử dụng cho phép tính băm. Sau đó, khi thu chứng nhận, bộ phận xác thực thứ hai 21 xác thực khối xác thực bằng cách tính lại các băm khối của các khối tính lại nhờ sử dụng chứng nhận.

Do đó, theo hệ thống xác thực giả mạo 100 theo phương án thứ nhất, thời gian xác thực chuỗi khối còn có thể được làm giảm.

Trong chuỗi khối thông thường, các khối liên kế "được tạo chuỗi" bằng cách đưa vào băm khối của khối trước đó, trong phép tính của băm khối. Phép

tính lại bằng cách lần theo chuỗi của các kết nối mang lại cơ chế để cho phép không xáo trộn của băm khối được xác thực.

Theo cấu hình của phương án thứ nhất, băm khối của khối mà không cần là khối trước đó cũng được đưa vào phép tính cho băm khối, cho phép "tạo chuỗi" các khối mà không liên kết với nhau. Phép tính lại được thực hiện bằng cách theo dõi chuỗi của các khối mà cách xa nhau cho phép bỏ qua phép tính lại của các băm khối của các khối được bố trí ở giữa.

Do đó, trong chuỗi khối việc chấp nhận cấu trúc dữ liệu theo phương án thứ nhất cho phép việc xác thực tốc độ cao cho không xáo trộn. Lưu ý rằng thậm chí theo phương án thứ nhất, vẫn có thể thực hiện việc xác thực dọc theo các chuỗi liên kết, giống với chuỗi khối thông thường. Nói cách khác, phương pháp xác thực không giới hạn ở một phương pháp.

Việc lựa chọn chuỗi xác thực bởi phương pháp xác thực giả mạo theo phương án thứ nhất khiến có thể làm giảm một cách đáng kể thời gian xác thực. Hiệu quả làm giảm tăng lên khi khối được xác thực và khối không bị giả mạo đó là cơ sở của việc xác thực cách xa nhau.

Cụ thể là, thời gian xác thực có thể được đánh giá bởi số các lần tính toán cho băm khối và số các băm khối khác được tham chiếu. Trong trường hợp lĩnh vực kỹ thuật thông thường, để xác thực các khối mà cách xa nhau 100,000 khối, cần tính các băm khối 100,000 lần và tham chiếu 100,000 băm khối khác.

Mặt khác, theo phương án thứ nhất, chỉ cần tính trung bình các băm khối xấp xỉ 16,5 lần và tham chiếu trung bình xấp xỉ 154 băm khối khác. Khi các khối cách xa nhau 1 triệu khối, chỉ cần tính trung bình các băm khối xấp xỉ 20 lần và tham chiếu trung bình xấp xỉ 219 băm khối khác. Nói cách khác, số trung bình các lần tính lại của các băm khối cho việc xác thực là 20, số trung bình các băm khối khác được chuyển đổi từ thiết bị ngang hàng 10 để thực hiện việc xác thực bên ngoài (thiết bị xác thực 20) thiết bị ngang hàng 10 là 219, và số trung bình các khối tính lại được chuyển đổi cho việc xác thực bởi thiết bị xác thực 20 là 20.

(Phương án thứ hai)

Tiếp theo, phương án thứ hai sẽ được mô tả. Theo phương án thứ hai, phần mô tả giống với phần mô tả theo phương án thứ nhất sẽ được bỏ qua, và các phần khác với các phần của phương án thứ nhất sẽ được mô tả.

Theo phương án thứ hai, tập hợp $S(BN)$ nêu trên được định rõ như sau.

Khi BN là số lẻ, $S(BN) = \{BN - 1\} \cap N$.

Khi BN là số chẵn và BN là số mà có thể chia được cho 2^n nhưng không thể chia được cho $2^{(n+1)}$,

$$S(BN) = \{BN-1, BN-2^n\} \cap N.$$

Theo phương án thứ nhất nêu trên, số khối của khối càng cao, thì khối có thể được kết nối với các khối khác càng nhiều. Trong khi đó, theo phương án thứ hai, hai khối khác lớn nhất được kết nối với một khối.

Fig.7 là hình vẽ minh họa ví dụ về việc kết nối của chuỗi khối theo phương án thứ hai. Ví dụ, khối #24 được kết nối với khối #16 và khối #23 bởi vì $S(BN = 24) = \{16, 23\}$.

Fig.8A và Fig.8B là các lưu đồ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ hai. Phương pháp xác thực giả mạo của phương án thứ hai khác với phương pháp xác thực giả mạo của phương án thứ nhất ở chỗ bước S10-2 được bổ sung.

Phần mô tả của các bước từ S1 đến S10 giống với phần mô tả trên Fig.6A theo phương án thứ nhất, và vì vậy phần mô tả của chúng sẽ được bỏ qua. Tiếp theo, bộ phận xác thực thứ hai 21 xác định xem BN có thể chia được cho $K \times 2$ và $BN > K \times 2$ hay không (bước S10-2). Khi BN có thể chia được cho $K \times 2$ và trong trường hợp $BN > K \times 2$ (bước S10-2, đúng), quy trình xử lý quay lại bước S10. Khi BN không thể chia được cho $K \times 2$ hoặc trong trường hợp $BN > K \times 2$ (bước S10-2, sai), quy trình xử lý đến bước S11. Các bước từ S11 đến S14 giống như các bước trên Fig.6A và Fig.6B theo phương án thứ nhất, và phần mô tả của chúng sẽ được bỏ qua.

Theo phương án thứ hai, số lớn nhất của các băm khối (các băm khối khác)

của các khối quá khứ được đưa vào phép tính cho băm khối của khối xác thực giới hạn ở 2, thực hiện dễ dàng hơn theo phương án thứ nhất. Phương án thứ hai, để xác thực khối xác thực được bố trí trước một triệu khối cuối cùng, chỉ cần tính trung bình các băm khối xấp xỉ 114 lần và tham chiếu trung bình xấp xỉ 214 băm khối khác.

(Phương án thứ ba)

Tiếp theo, phương án thứ ba sẽ được mô tả. Theo phương án thứ ba, phần mô tả giống với phần mô tả theo phương án thứ nhất sẽ được bỏ qua, và các phần khác với các phần của phương án thứ nhất sẽ được mô tả.

Theo phương án thứ ba, tập hợp $S(BN)$ nêu trên được định rõ như sau.

Khi BN là số lẻ, $S(BN) = \{BN - 1\} \cap N$.

BN là số mà có thể chia được cho 2^n nhưng không thể chia được cho $2^{(n+1)}$

Trong trường hợp $n \leq 4$, $S(BN) = \{BN-1, BN-2^n\} \cap N$ (kết nối với khối trước đó và khối được bố trí trước 2^n khối cuối cùng)

Trong trường hợp $n \geq 5$, $S(BN) = \{BN-1, BN-2^{n-p}, BN-2^{n-q}, BN-2^n\} \cap N$ (kết nối với khối trước đó, khối được bố trí trước 2^{n-p} khối cuối cùng, khối được bố trí trước 2^{n-q} khối cuối cùng, và khối được bố trí trước 2^n khối cuối cùng)

$p = \text{ceil}(\text{sqrt}(n))$; $\text{ceil}(x)$ là số nguyên nhỏ nhất bằng hoặc lớn hơn x , và $\text{sqrt}(x)$ là căn bậc hai dương của x

$q = \text{floor}(\text{sqrt}(\text{sqrt}(n)))$; $\text{floor}(x)$ là số nguyên lớn nhất không vượt quá x

Tuy nhiên, số khối = 0 được loại trừ khỏi phép tính.

Theo phương án thứ ba, để xác thực khối xác thực được bố trí trước một triệu khối cuối cùng, chỉ cần tính trung bình các băm khối xấp xỉ 31 lần và tham chiếu trung bình xấp xỉ 98 băm khối khác.

(Phương án thứ tư)

Tiếp theo, phương án thứ tư sẽ được mô tả. Theo phương án thứ tư, phần mô tả giống với phần mô tả theo phương án thứ nhất sẽ được bỏ qua, và các phần

khác với các phần của phương án thứ nhất sẽ được mô tả.

Theo phương án thứ tư, bộ phận tạo ra 11 tính trị số băm của các hồ sơ giao dịch cho các nội dung giao dịch (các hồ sơ giao dịch), và tính băm khối nhờ sử dụng trị số băm.

Khi việc giả mạo với các băm khối bị nghi ngờ, có thể được xét đến rằng chính thiết bị ngang hàng 10 có thể đã bị vô hiệu hóa từ đầu, và việc xác thực ở thiết bị ngang hàng 10 có thể vô nghĩa. Do đó, mong muốn thực hiện việc xác thực cho việc không xáo trộn với máy tính (thiết bị xác thực 20 theo ví dụ trên Fig.1) độc lập với thiết bị ngang hàng 10. Phép tính lại các băm khối trên máy tính khác yêu cầu đọc các băm khối khác liên quan đến băm khối của khối xác thực từ thiết bị ngang hàng 10.

Chúng nhận lưu trữ các băm khối khác và thông tin duy nhất (ví dụ, trị số băm của các hồ sơ giao dịch, số khối chẳng hạn) được chứa trong khối tính lại cho phép tính lại băm khối, theo thứ tự định trước. Chúng nhận có thể được thu nhận bằng cách đưa ra yêu cầu tới thiết bị ngang hàng 10. Chúng nhận chứa tất cả dữ liệu được sử dụng cho việc xác thực, và phép tính lại băm khối được thực hiện bởi máy tính bên ngoài theo chúng nhận cho phép việc xác thực cho việc không xáo trộn. Chúng nhận theo phương án thứ tư không chứa các hồ sơ giao dịch thô (các nội dung giao dịch), vì vậy, ngăn ngừa một cách hữu hiệu sự rò rỉ thông tin được ghi trên chuỗi khối từ chúng nhận.

(Phương án thứ năm)

Tiếp theo, phương án thứ năm sẽ được mô tả. Theo phương án thứ năm, phần mô tả giống với phần mô tả theo phương án thứ nhất sẽ được bỏ qua, và các phần khác với các phần của phương án thứ nhất sẽ được mô tả.

Phương án thứ năm mô tả về trường hợp trong đó các phương án từ thứ nhất đến thứ năm nêu trên còn được khái quát hóa. Theo phương án thứ năm, tập hợp $S(BN)$ của các số khối khác định trước được xác định cho mỗi số khối BN . Ở đây, $b \in S(BN)$ thỏa mãn $b < BN$. $BN-1 \in S(BN)$ cần được thỏa mãn (loại trừ

BN có số ban đầu).

Băm khối của khối có số khối BN được tính bởi phương pháp định trước, dựa vào tập hợp của các băm khối của các khối đều có số khối $b \in S(BN)$, và các giao dịch và tương tự được chứa trong khối. Tại thời điểm này, phương pháp xác thực, ví dụ, như được minh họa trên Fig.9A và Fig.9B được sử dụng.

Fig.9A và Fig.9B là các lưu đồ minh họa ví dụ về phương pháp xác thực giả mạo theo phương án thứ năm. Các bước từ S21 đến S24 giống như các bước từ S1 đến S4 của phương án thứ nhất nêu trên, và phần mô tả của chúng sẽ được bỏ qua.

Bộ phận xác thực thứ hai 21 thiết đặt danh mục trống tới L, và thiết đặt số lớn nhất của $S(BN)$ tới K (bước S25). Tiếp theo, bộ phận xác thực thứ hai 21 thiết đặt băm khối của số khối K được lưu trữ trên chuỗi khối (thiết bị ngang hàng 10) tới H (bước S26). Tiếp theo, bộ phận xác thực thứ hai 21 bổ sung H vào danh mục L (bước S27).

Tiếp theo, bộ phận xác thực thứ hai 21 xác định xem $K \geq BN_0$ hay không (bước S28). Trong trường hợp $K \geq BN_0$ (bước S28, đúng), bộ phận xác thực thứ hai 21 thiết đặt K tới BN_1 , thiết đặt H tới BH_1 (bước S29), và đến bước S30. Trong trường hợp $K < BN_0$ (bước S28, sai), quy trình xử lý đến bước S30 mà không thực hiện việc xử lý của bước S29.

Tiếp theo, bộ phận xác thực thứ hai 21 xác định xem K là số nhỏ nhất của $S(BN)$ hay không (bước S30). Khi K không là số nhỏ nhất của $S(BN)$ (bước S30, đúng), bộ phận xác thực thứ hai 21 thiết đặt số mà là số cao nhất tiếp theo sau K của $S(BN)$ tới K (bước S31), và quay lại bước S26.

Khi K là số nhỏ nhất của $S(BN)$ (bước S30, đúng), quy trình xử lý đến bước S32. Các bước từ S32 đến S34 giống như các bước từ S12 đến S14 của phương án thứ nhất nêu trên, và phần mô tả của chúng sẽ được bỏ qua.

Như được nêu trên, theo phương án thứ năm, thậm chí khi tập hợp $S(BN)$ của các số khối khác được khái quát hóa, thời gian xác thực chuỗi khối còn có thể

được làm giảm như theo phương án thứ nhất.

Cuối cùng, ví dụ về cấu hình phần cứng của thiết bị ngang hàng 10 và thiết bị xác thực 20 theo các phương án từ thứ nhất đến thứ năm sẽ được mô tả.

[Ví dụ về cấu hình phần cứng]

Fig.10 là hình vẽ minh họa ví dụ về cấu hình phần cứng của thiết bị ngang hàng 10 và thiết bị xác thực 20 theo các phương án từ thứ nhất đến thứ năm. Mỗi trong số thiết bị ngang hàng 10 và thiết bị xác thực 20 bao gồm thiết bị điều khiển 401, thiết bị lưu trữ chính 402, thiết bị lưu trữ phụ 403, thiết bị hiển thị 404, thiết bị đầu vào 405, và thiết bị truyền thông 406. Thiết bị điều khiển 401, thiết bị lưu trữ chính 402, thiết bị lưu trữ phụ 403, thiết bị hiển thị 404, thiết bị đầu vào 405, và thiết bị truyền thông 406 được kết nối qua bus 410.

Thiết bị điều khiển 401 thực hiện chương trình được đọc từ thiết bị lưu trữ phụ 403 vào thiết bị lưu trữ chính 402. Thiết bị lưu trữ chính 402 là bộ nhớ chẳng hạn như bộ nhớ chỉ đọc (read only memory, viết tắt là ROM) và bộ nhớ truy cập ngẫu nhiên (random access memory, viết tắt là RAM). Thiết bị lưu trữ phụ 403 là ổ đĩa cứng (hard disk drive, viết tắt là HDD), thẻ nhớ, và tương tự.

Thiết bị hiển thị 404 hiển thị thông tin. Thiết bị hiển thị 404 là, ví dụ, màn hình tinh thể lỏng hoặc tương tự. Thiết bị đầu vào 405 là giao diện mà thu đầu vào. Thiết bị đầu vào 405 là, ví dụ, bàn phím và chuột. Thiết bị hiển thị 404 và thiết bị đầu vào 405 có thể là bảng cảm ứng và tương tự có chức năng hiển thị và chức năng đầu vào. Thiết bị truyền thông 406 là giao diện cho việc truyền thông với thiết bị khác.

Chương trình được thực hiện bởi thiết bị ngang hàng 10 và thiết bị xác thực 20 được ghi trong phương tiện lưu trữ có thể đọc được bởi máy tính, chẳng hạn như CD-ROM, thẻ nhớ, CD-R, hoặc DVD, trong tệp định dạng có thể thực hiện được hoặc có thể cài đặt được, và được cung cấp như sản phẩm chương trình máy tính.

Hơn nữa, chương trình được thực hiện bởi thiết bị ngang hàng 10 và thiết

bị xác thực 20 có thể được tạo cấu hình để được lưu trữ trên máy tính được kết nối với mạng chẳng hạn như Internet và được cung cấp bằng cách được tải xuống qua mạng. Hơn nữa, chương trình được thực hiện bởi thiết bị ngang hàng 10 và thiết bị xác thực 20 có thể được tạo cấu hình để được cung cấp qua mạng chẳng hạn như Internet mà không được tải xuống.

Hơn nữa, chương trình đối với thiết bị ngang hàng 10 và thiết bị xác thực 20 có thể được tạo cấu hình để được cung cấp bằng cách được kết hợp trước vào ROM hoặc tương tự.

Chương trình được thực hiện bởi thiết bị ngang hàng 10 và thiết bị xác thực 20 có cấu hình môđun mà bao gồm khối chức năng của các khối chức năng trên Fig.1 nêu trên, khối chức năng cũng được tạo cấu hình để được thực hiện bởi chương trình. Xét đến phần cứng thực tế, mỗi trong số các khối chức năng được tải trên thiết bị lưu trữ chính 402 đáp lại việc thực hiện của chương trình được đọc từ phương tiện ghi bởi thiết bị điều khiển 401. Nói cách khác, mỗi trong số các khối chức năng nêu trên được tạo ra trên thiết bị lưu trữ chính 402.

Lưu ý rằng một số hoặc tất cả các khối chức năng trên Fig.1 nêu trên có thể được thực hiện bởi phần cứng chẳng hạn như IC mà không được thực hiện bởi phần mềm.

Hơn nữa, khi các chức năng được thực hiện nhờ sử dụng các bộ xử lý, mỗi bộ xử lý có thể thực hiện một trong số các chức năng, hoặc có thể thực hiện hai hoặc nhiều trong số các chức năng.

Hơn nữa, chế độ thao tác bất kỳ có thể được chấp nhận đối với chế độ thao tác của thiết bị ngang hàng 10 và thiết bị xác thực 20. Thiết bị ngang hàng 10 và thiết bị xác thực 20 có thể được thao tác, ví dụ, như thiết bị cấu thành hệ thống đám mây trên mạng.

Trong khi các phương án nhất định đã được mô tả, các phương án này đã được thể hiện chỉ bằng ví dụ, và không nhằm giới hạn phạm vi của các sáng chế. Thực vậy, các phương pháp và các hệ thống mới được mô tả ở đây có thể được bao gồm dưới nhiều dạng khác, và hơn nữa, các sự bỏ qua, các sự thay thế, và các

sự thay đổi khác nhau dưới dạng của các phương pháp và các hệ thống được mô tả ở đây có thể được thực hiện mà không trệch khỏi tinh thần của các sáng chế. Các điểm yêu cầu bảo hộ kèm theo và các sự tương đương của chúng nhằm bao gồm các dạng hoặc các sự sửa đổi như vậy sẽ nằm trong phạm vi và tinh thần của các sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp xác thực giả mạo bao gồm:

bước tính băm khối dựa vào các băm khối khác của các khối khác và thông tin duy nhất, và tạo ra chuỗi khối trong đó khối chứa băm khối được tính được kết nối;

bước, đáp lại việc thu yêu cầu xác thực cho khối xác thực được chứa trong chuỗi khối, tạo ra chứng nhận được sử dụng cho phép tính lại của các khối tính lại chứa các băm khối mà phụ thuộc vào băm khối của khối xác thực, cho các băm khối khác; và

bước, đáp lại việc thu chứng nhận, xác thực khối xác thực bằng cách tính lại các băm khối của các khối tính lại nhờ sử dụng chứng nhận.

2. Phương pháp xác thực giả mạo theo điểm 1, trong đó

chứng nhận chứa thông tin duy nhất về các khối tính lại, các băm khối của các khối tính lại, và các băm khối khác được sử dụng cho phép tính của các băm khối của các khối tính lại.

3. Phương pháp xác thực giả mạo theo điểm 1, trong đó

các băm khối khác của các khối khác được nhận dạng bởi tập hợp của các số khối khác được xác định dựa vào các số khối của các khối được kết nối.

4. Phương pháp xác thực giả mạo theo điểm 3, trong đó

khi BN là số khối, N là tập hợp của tất cả các số tự nhiên, và n là số nguyên chỉ báo rằng BN có thể chia được cho 2^n nhưng không thể chia được cho $2^{(n+1)}$, tập hợp của các số khối khác được định rõ bởi:

$$S(BN) = \{BN - 1\} \cap N, \text{ khi BN là số lẻ; và}$$

$$S(BN) = \{BN - 2^m \mid m \text{ là số nguyên mà thỏa mãn } 0 \leq m \leq n\} \cap N, \text{ khi BN là số chẵn.}$$

5. Phương pháp xác thực giả mạo theo điểm 3, trong đó

khi BN là số khối, N là tập hợp của tất cả các số tự nhiên, và n là số nguyên chỉ báo rằng BN có thể chia được cho 2^n nhưng không thể chia được cho $2^{(n+1)}$, tập hợp của các số khối khác được định rõ bởi:

$$S(BN) = \{BN - 1\} \cap N, \text{ khi BN là số lẻ; và}$$

$$S(BN) = \{BN - 1, BN - 2^n\} \cap N, \text{ khi BN là số chẵn.}$$

6. Phương pháp xác thực giả mạo theo điểm 3, trong đó

khi BN là số khối, N là tập hợp của tất cả các số tự nhiên, n là số nguyên chỉ báo rằng BN có thể chia được cho 2^n nhưng không thể chia được cho $2^{(n+1)}$, $p = \text{ceil}(\text{sqrt}(n))$ ($\text{ceil}(x)$ là số nguyên nhỏ nhất bằng hoặc lớn hơn x, và $\text{sqrt}(x)$ là căn bậc hai dương của x), và $q = \text{floor}(\text{sqrt}(\text{sqrt}(n)))$ ($\text{floor}(x)$ là số nguyên lớn nhất không vượt quá x), tập hợp của các số khối khác được định rõ bởi:

$$S(BN) = \{BN - 1\} \cap N, \text{ khi BN là số lẻ;}$$

$$S(BN) = \{BN - 1, BN - 2^n\} \cap N, \text{ khi } n \leq 4; \text{ và}$$

$$S(BN) = \{BN - 1, BN - 2^{n-p}, BN - 2^{n-q}, BN - 2^n\} \cap N, \text{ khi } n \geq 5.$$

7. Phương pháp xác thực giả mạo theo điểm 1, trong đó

thông tin duy nhất bao gồm ít nhất một trong số thông tin dựa vào các hồ sơ giao dịch và số khối.

8. Phương pháp xác thực giả mạo theo điểm 7, trong đó

thông tin dựa vào các hồ sơ giao dịch biểu diễn các hồ sơ giao dịch hoặc trị số băm của các hồ sơ giao dịch.

9. Hệ thống xác thực giả mạo bao gồm:

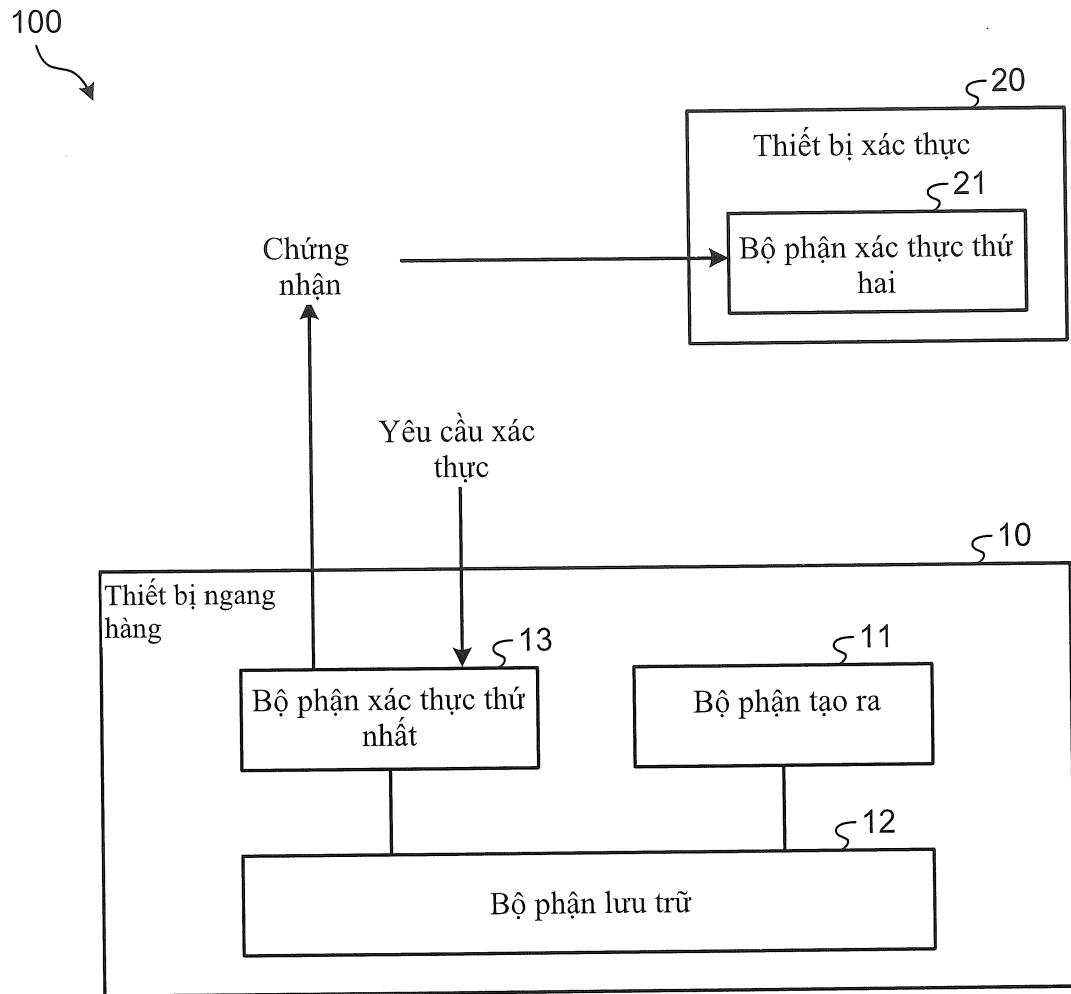
bộ phận tạo ra mã tính băm khối dựa vào các băm khối khác của các khối khác và thông tin duy nhất, và tạo ra chuỗi khối trong đó khối chứa băm khối được tính được kết nối;

bộ phận xác thực thứ nhất mà, đáp lại việc thu yêu cầu xác thực cho khối xác thực được chứa trong chuỗi khối, tạo ra chứng nhận được sử dụng cho phép tính lại của các khối tính lại chứa các băm khối mà phụ thuộc vào băm khối của

khối xác thực, cho các băm khối khác; và

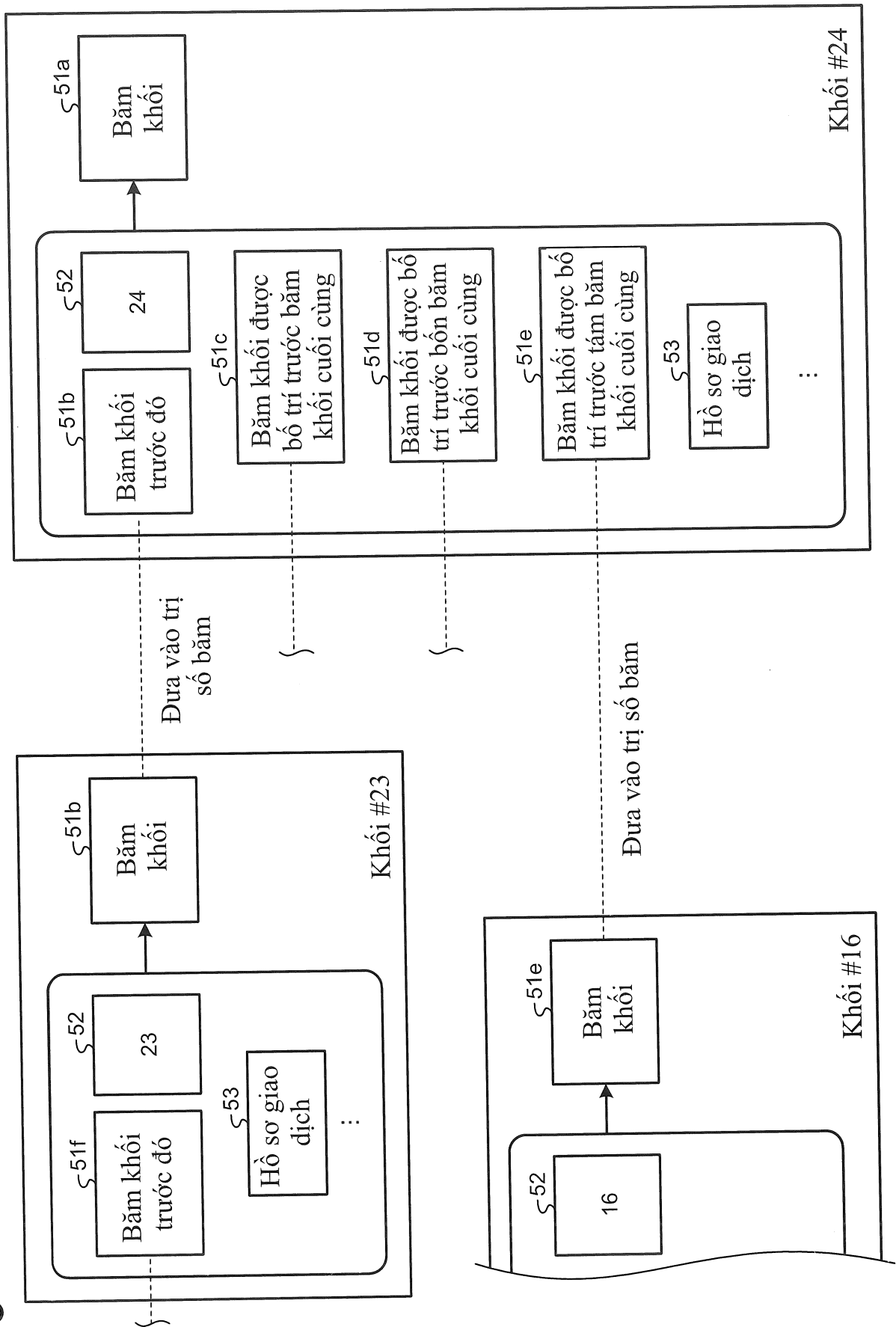
bộ phận xác thực thứ hai mà, đáp lại việc thu chứng nhận, xác thực khối xác thực bằng cách tính lại các băm khối của các khối tính lại nhờ sử dụng chứng nhận.

FIG.1



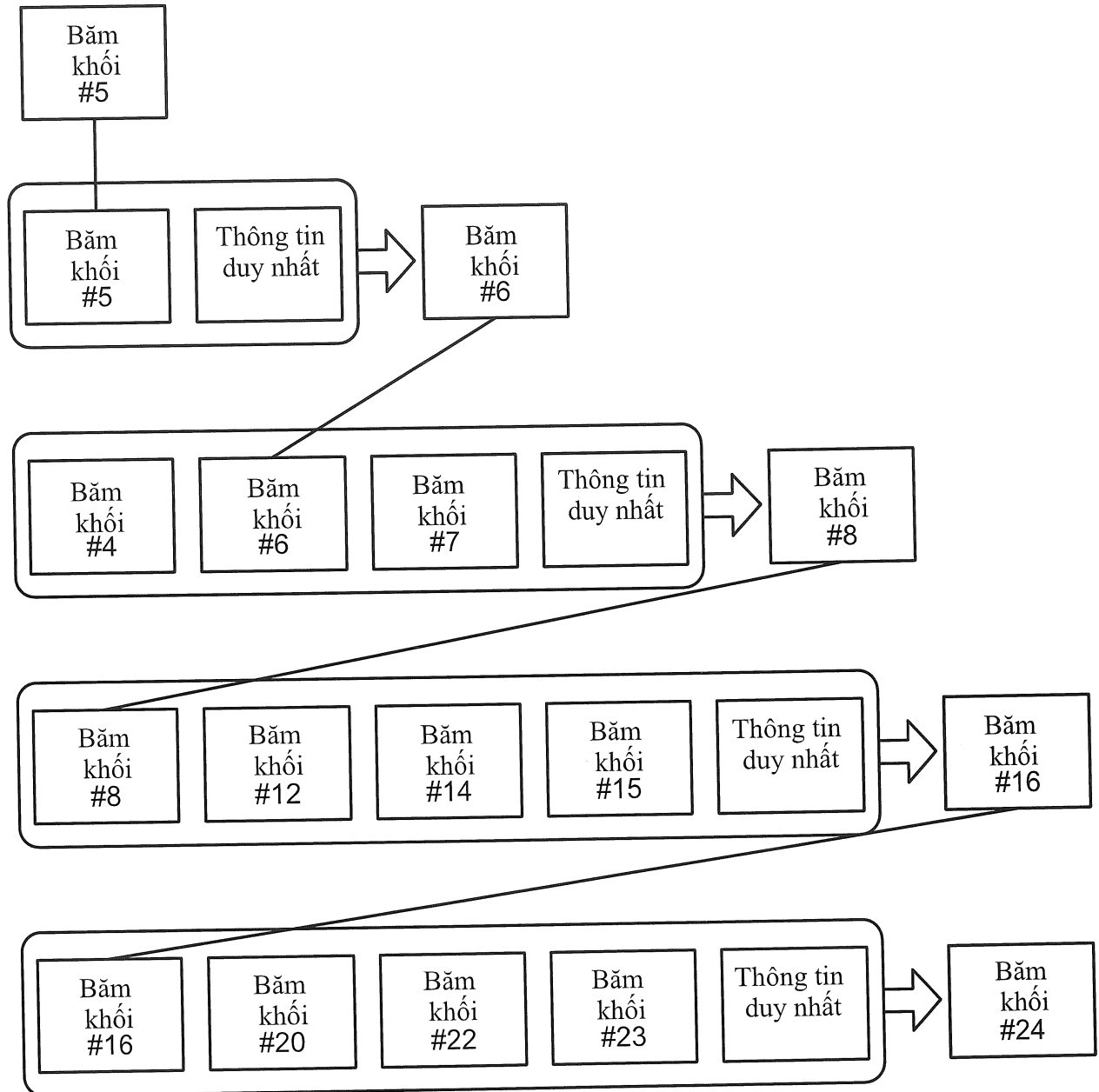
3/13

FIG.3



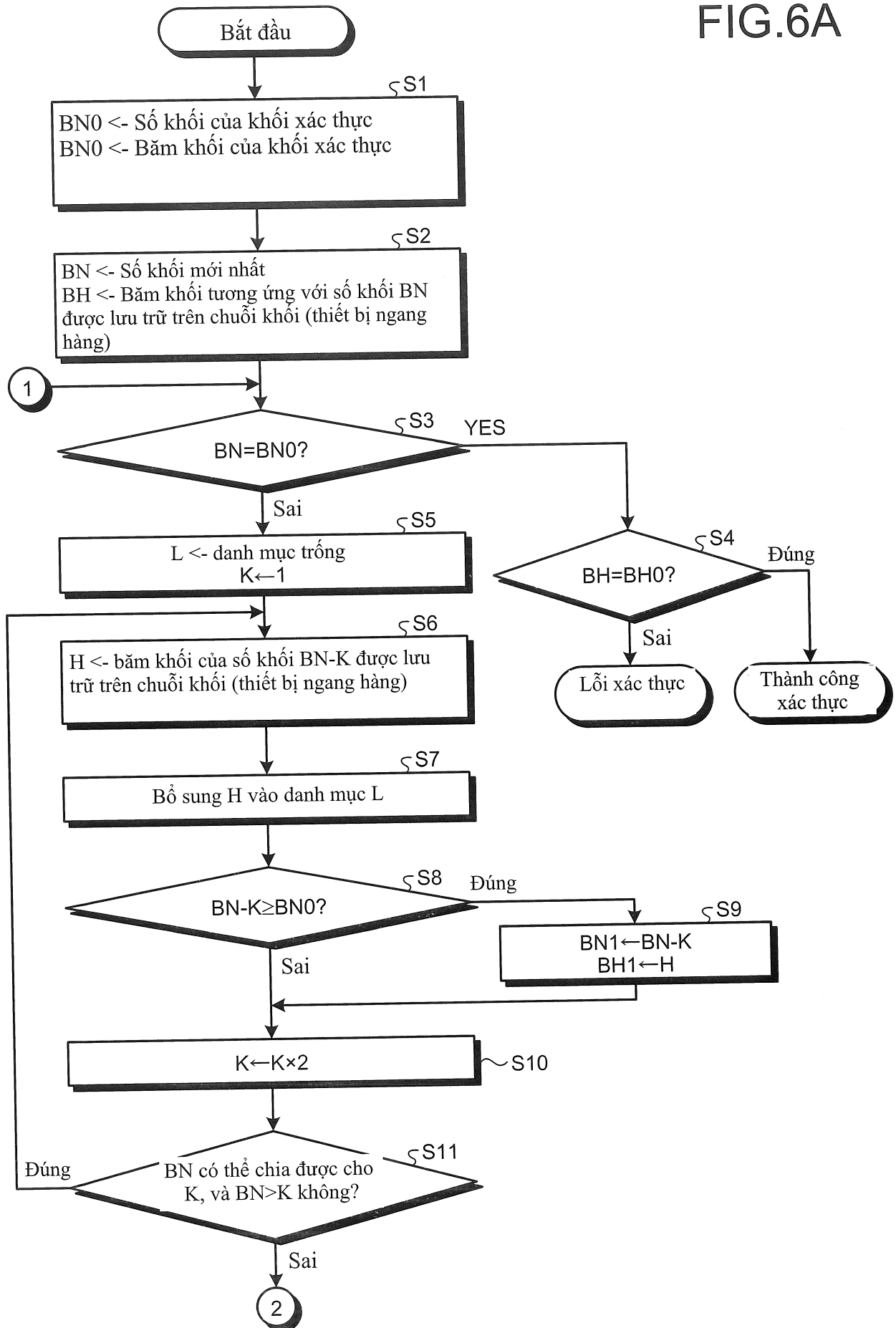
5/13

FIG.5



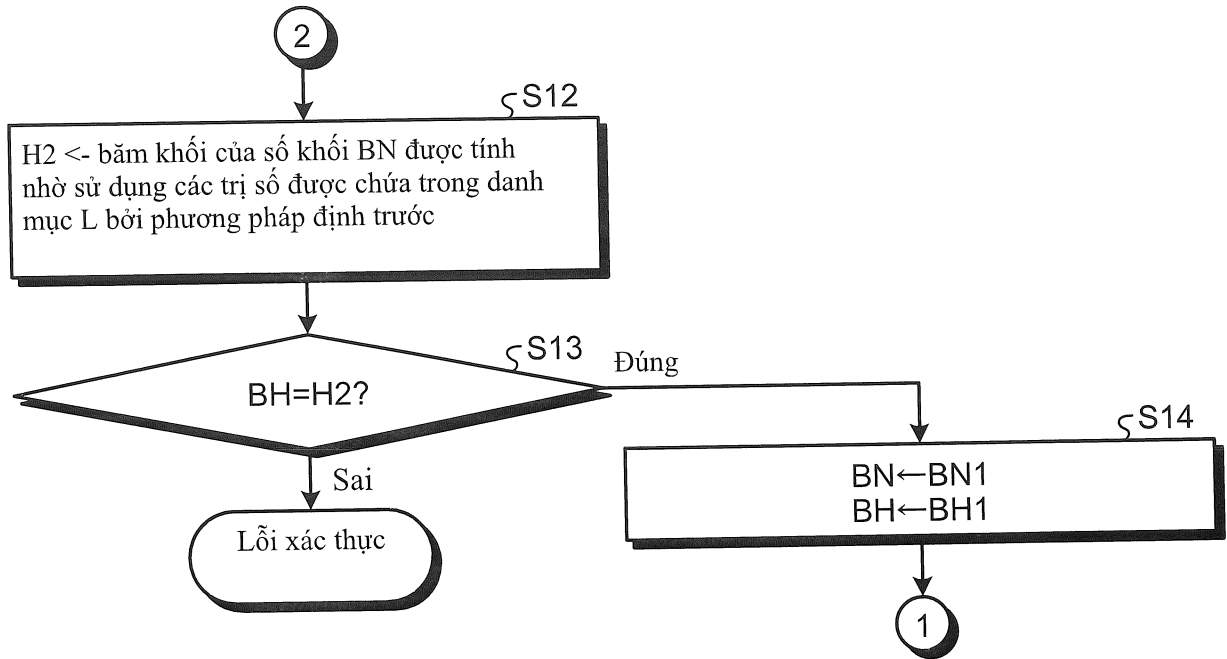
6/13

FIG.6A



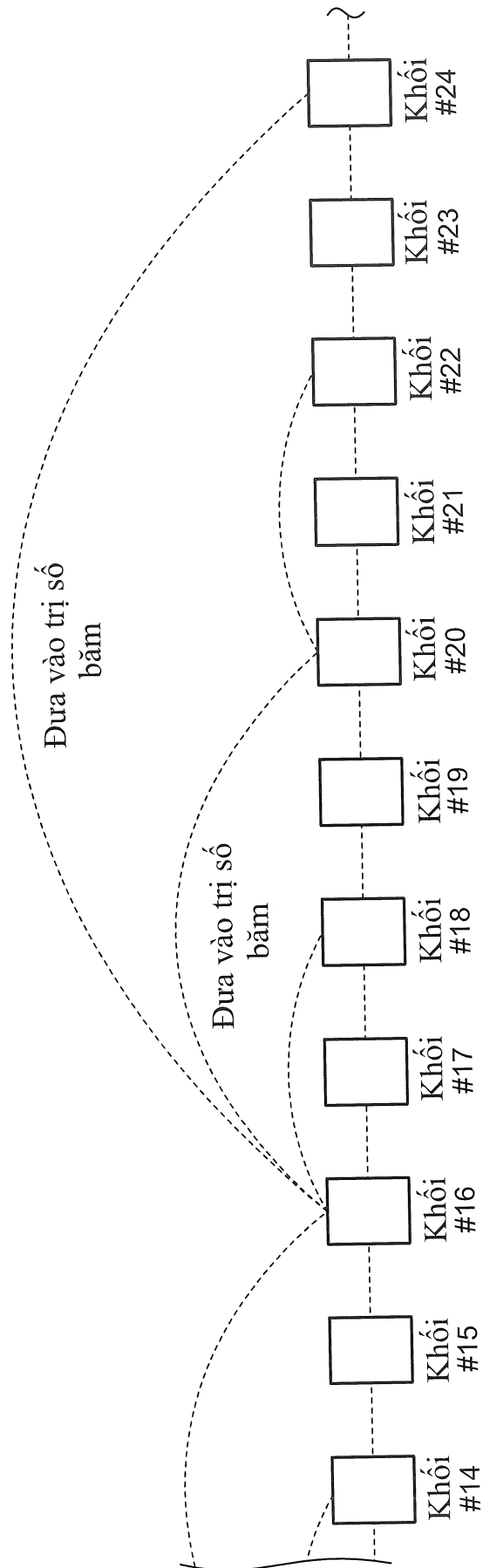
7/13

FIG.6B



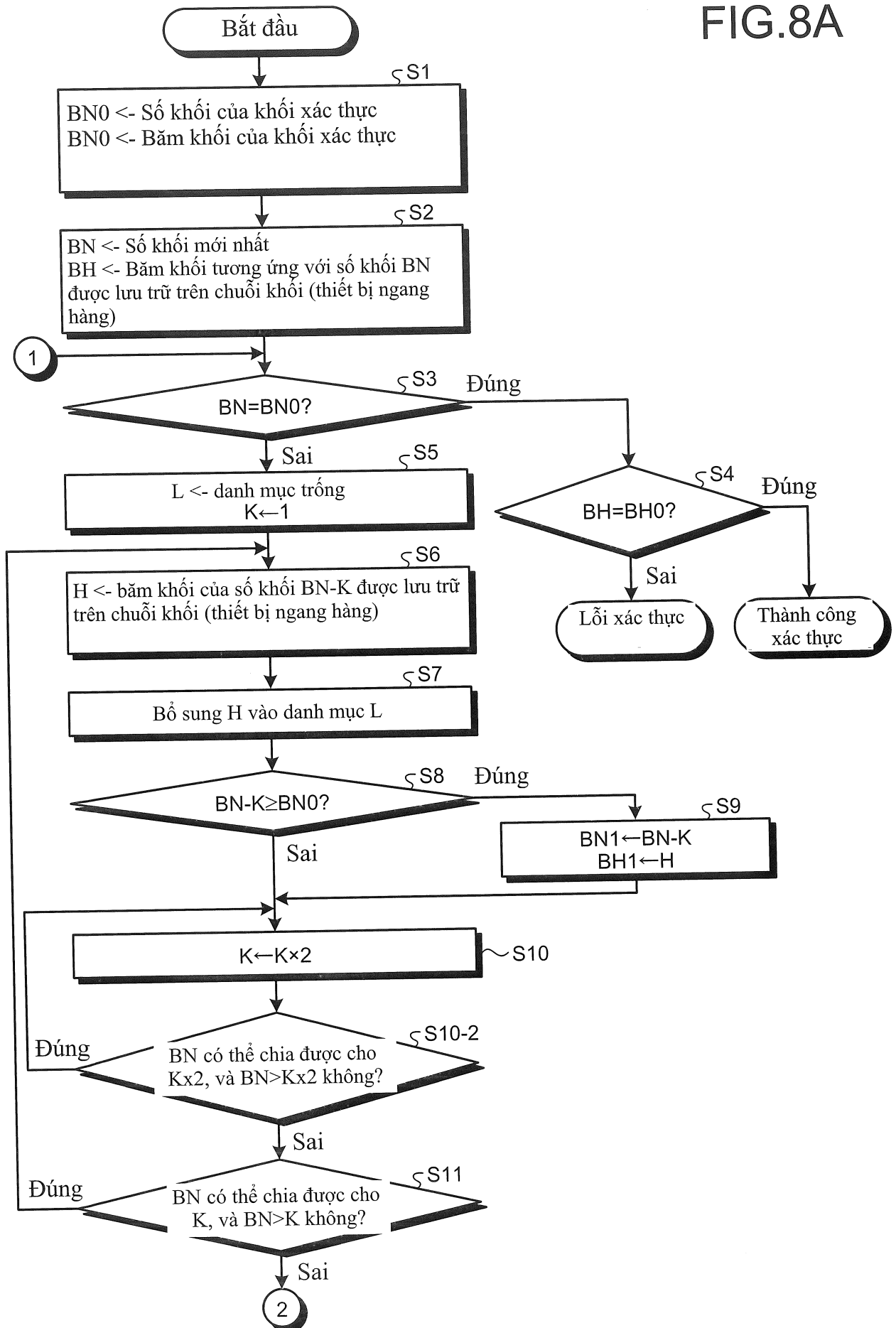
8/13

FIG.7



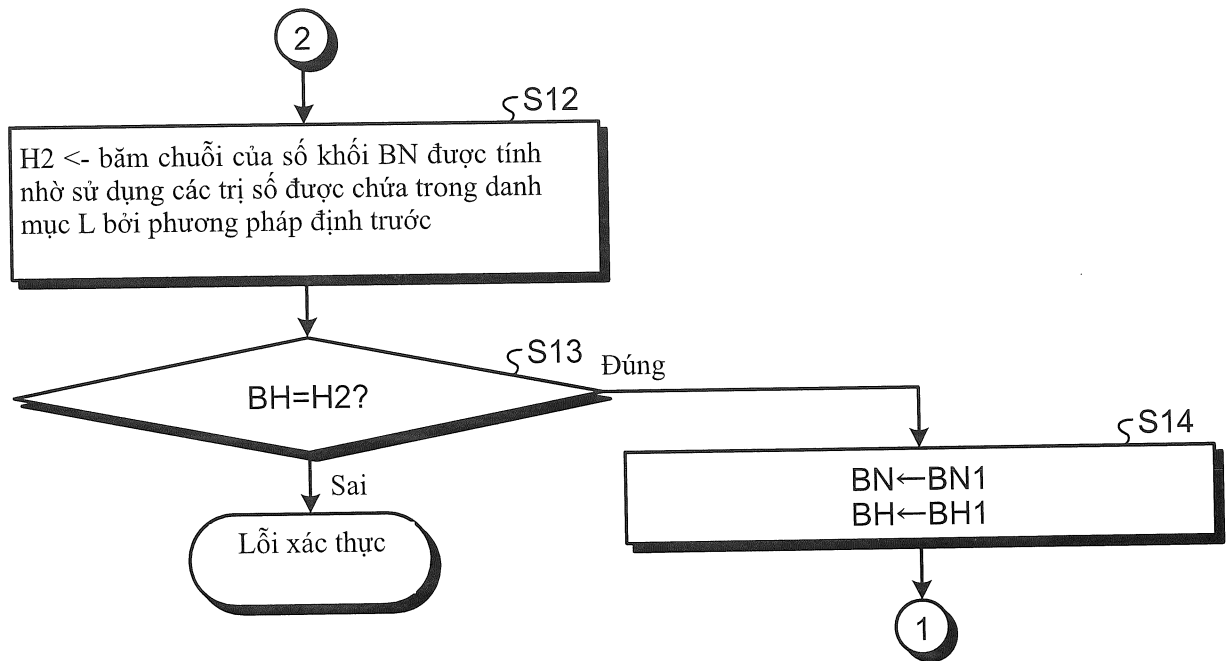
9/13

FIG.8A



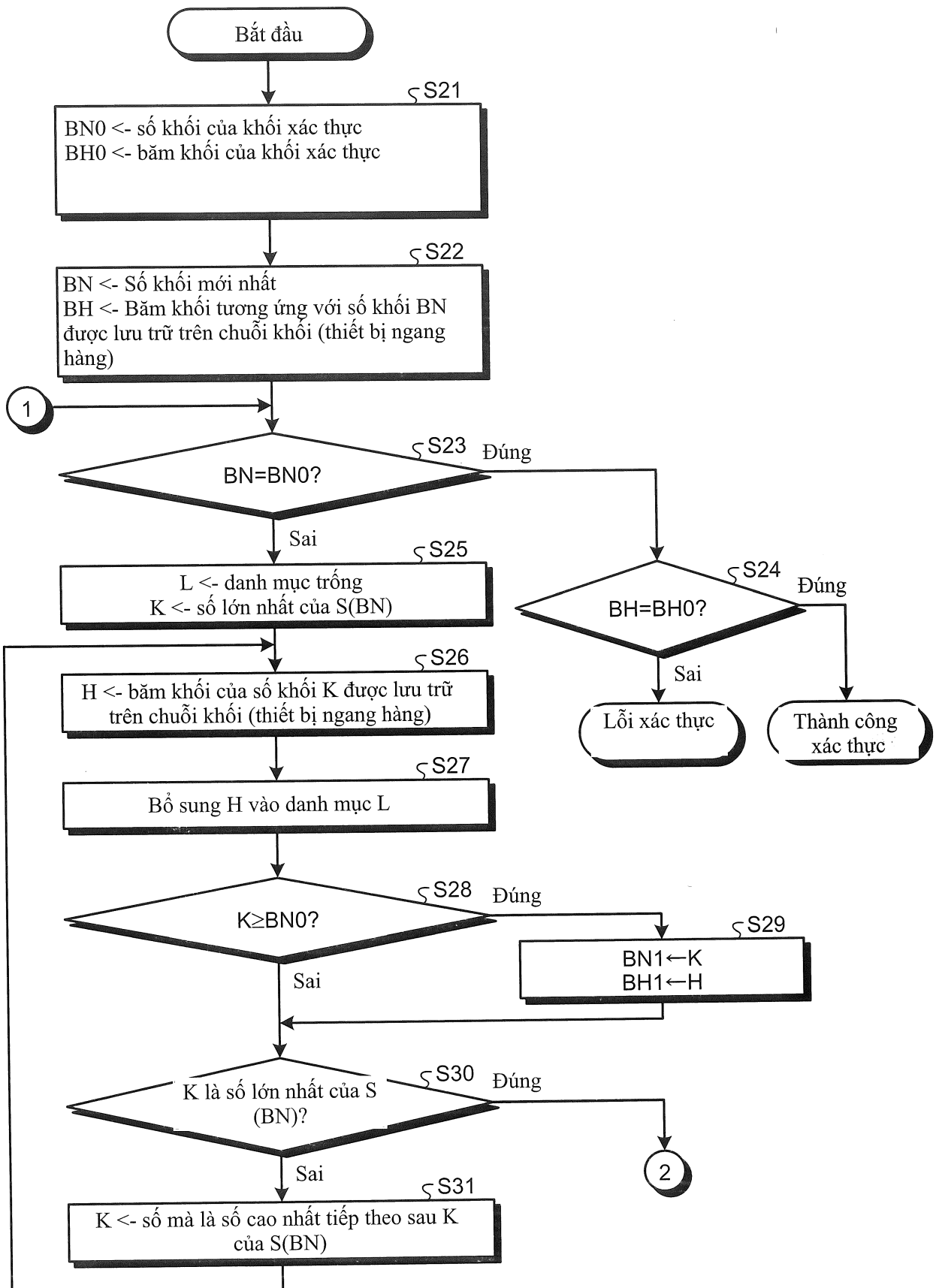
10/13

FIG.8B



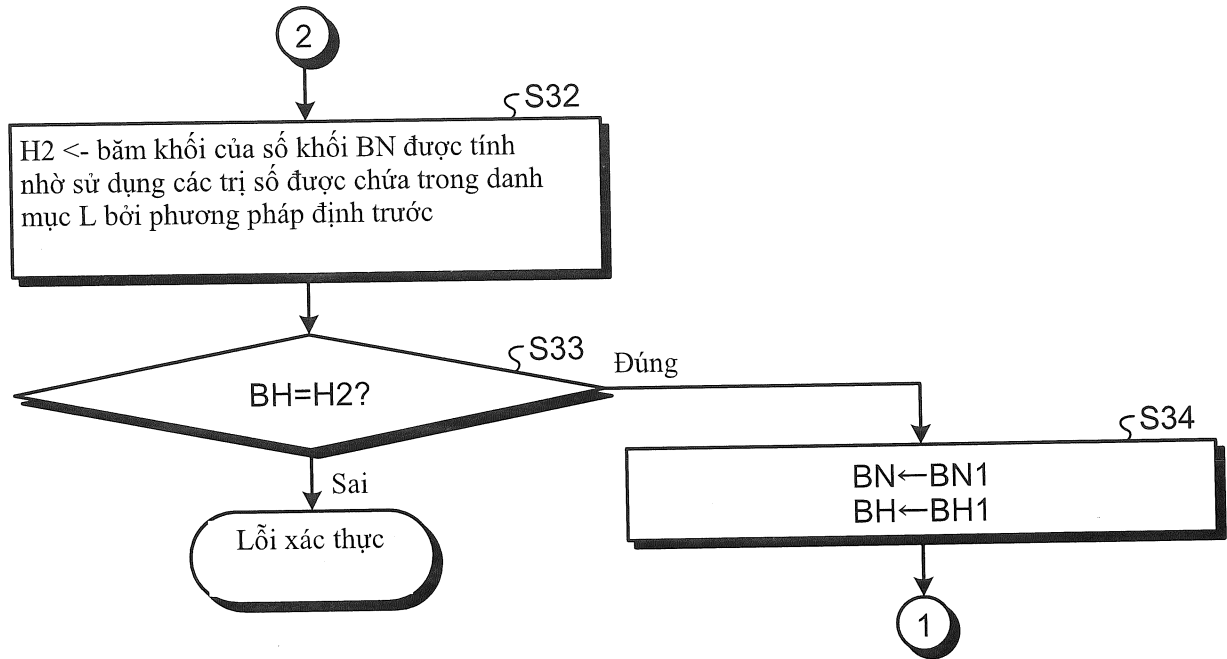
11/13

FIG.9A



12/13

FIG.9B



13/13

FIG.10

