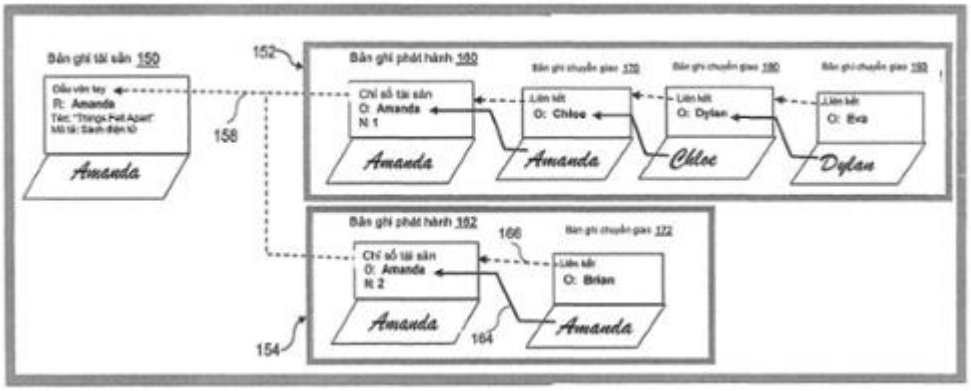
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0032692**
(51)[8] **G06Q 50/00** (13) **B**

(21) 1-2017-04347 (22) 06/04/2016
(86) PCT/US2016/026266 06/04/2016 (87) WO 2016/164496 13/10/2016
(30) 62/143,771 06/04/2015 US; 62/195,238 21/07/2015 US
(45) 25/07/2022 412 (43) 26/03/2018 360A
(73) 1. BITMARK, INC. (TW)
IF No. 489-1, Taipei City, TAI 115, Taiwan
2. MOSS-PULTZ, Sean (US)
1338 Rubenstein Avenue, Cardiff-by-the-Sea, California 92007, United States of America
(72) MOSS-PULTZ, Sean (US); ALT, Casey (US); HALL, Christopher (GB); CUONG, Le Quy Quoc (VN); WANG, Yu-Chiang Frank (TW); LIN, Tzu-Yun Eddie (TW).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG GHI NHẬN QUYỀN SỞ HỮU ĐỐI VỚI TÀI SẢN

(57) Sáng chế đề cập đến phương pháp và hệ thống ghi nhận quyền sở hữu đối với tài sản, cụ thể là đề cập đến phương pháp và hệ thống tài sản phân cấp cho phép quyền sở hữu được chuyển giao trực tiếp từ một bên sang bên khác mà không đòi hỏi một trung tâm có thẩm quyền trung gian để vận hành hoặc đảm bảo hệ thống. Chữ ký số đưa ra phương pháp để phát hành và chuyển giao quyền ("bitmark") trong hệ thống. Bằng cách sử dụng thuật toán chuỗi khối, có thể đạt được thỏa thuận phân tán về quyền sở hữu tài sản.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống và phương pháp ghi nhận và chuyển giao quyền sở hữu tài sản và cụ thể hơn là hệ thống phi tập trung không cần có quyền tập trung.

Tình trạng kỹ thuật của sáng chế

Một trong những điều quan trọng nhất mà hệ thống tài sản dạng hình thức thực hiện là biến đổi tài sản từ trạng thái khó tiếp cận sang trạng thái dễ tiếp cận hơn, sao cho quyền sở hữu có thể được truyền thông và tập hợp dễ dàng trong mạng rộng hơn. Việc chuyển đổi từ tài sản nói chung sang tài sản sở hữu cần có hệ thống phức tạp để ghi nhận và tổ chức các thuộc tính hữu ích về mặt xã hội và kinh tế của quyền sở hữu. Hành động cụ thể hoá tài sản dưới dạng chứng thư tài sản và ghi nhận nó vào sổ cái công cộng tạo điều kiện thuận lợi cho thỏa thuận giữa những người thực thi về cách thức mà tài sản nên được nắm giữ, sử dụng và trao đổi. Ngoại trừ các khoảng thời gian bất ổn chính trị, các hệ thống tài sản vận hành bởi chính phủ và cơ quan chính phủ cung cấp niềm tin và tạo ra giá trị đáng kể. Việc số hóa các bản ghi hứa hẹn sẽ làm tăng hiệu quả và giảm chi phí, nhưng lại khiến cho hệ thống rất dễ bị gian lận và mất mát dữ liệu.

Đối với tài sản hiện vật, quyền sở hữu và chuyển giao tài sản đã được thiết lập trước đây thông qua quyền trung tâm. Ví dụ, đăng ký quyền đối với bất động sản được ghi nhận tại văn phòng chính phủ, đăng ký quyền đối với phương tiện cơ giới được xử lý thông qua Cục quản lý xe cơ giới. Ngay cả quyền sở hữu tài sản không hữu hình ví dụ như sáng chế, nhãn hiệu và bản quyền cũng có thể được ghi nhận tại văn phòng chính phủ.

Giả mạo là vấn đề nghiêm trọng trong tiếp thị kinh doanh. Việc làm giả các

hàng hóa được sản xuất là vấn đề trên toàn thế giới, các nghiên cứu gần đây ước tính rằng 8% tổng GDP của thế giới đang được tạo ra từ việc sản xuất và kinh doanh các sản phẩm giả mạo. Nhiều loại hàng hóa giả mạo gây ra các nguy cơ lớn cho sức khỏe cộng đồng bao gồm dược phẩm, phụ tùng ô tô, thuốc trừ sâu và đồ chơi trẻ em giả mạo. Ngoài ra, chip máy tính, phụ tùng máy bay và các tài liệu nhận dạng giả mạo gây ra các mối nguy lớn cho an ninh quốc gia. Các đồ vật có giá trị như công trình nghệ thuật, văn bản chính thức và hàng hóa xa xỉ thường cần có các thủ tục nhất định và thậm chí có sự xác minh của chuyên gia về tính xác thực của đồ vật. Nhiều phương pháp khác nhau đã được thử nghiệm để nhận dạng và xác thực các đồ vật một cách độc nhất, bao gồm các chiến lược tạo nhãn và gắn thẻ sử dụng các số seri, mã vạch, nhãn ba chiều, thẻ RFID và các mẫu hình chìm sử dụng mực bảo mật hoặc các sợi đặc biệt. Tất cả các phương pháp này đều có thể bị sao chép hoặc làm giả, và nhiều nơi cộng thêm chi phí thêm đáng kể vào việc sản xuất các hàng hóa cần được bảo vệ. Các nhãn và thẻ vật lý cũng có thể dễ dàng bị mất, chỉnh sửa hoặc lấy cắp. Do đó, việc thực hiện xác thực chất liệu đối với các ứng dụng thực tế có thể là vấn đề thách thức lớn.

Cơ quan FBI Mỹ đã gọi vấn đề giả mạo là "Tội phạm của thế kỷ 21". Nói chung, trên 650 tỷ USD doanh thu toàn cầu bị mất cho hàng giả mỗi năm. Vấn đề giả mạo gây tốn kém cho các doanh nghiệp Mỹ từ 200 đến 250 tỷ USD mỗi năm. 92% công ty trong danh sách Fortune 500 bị ảnh hưởng bởi vấn đề giả mạo. Tổ chức Thuế quan Quốc tế và Phòng Thương mại Quốc tế ước tính rằng khoảng 7-8% nền mậu dịch thế giới trong mỗi năm là dành cho hàng giả. Vấn đề giả mạo ảnh hưởng đến hầu như mọi thị trường và gần như mọi người tiêu dùng, không kể độ tuổi, nơi ở hay mức của cải. Các sản phẩm giả mạo bao gồm dược phẩm, trong đó thuốc giả đã gây ra thương vong, các đồ điện tử và công nghệ thông tin (information technology, IT) bao gồm pin giả, các bộ phận phương tiện cơ giới – gồm cả ô tô và máy bay, thức ăn, đồ uống và các sản phẩm tiêu dùng khác, ví dụ như thuốc lá và các sản phẩm nông nghiệp khác, hàng tiêu dùng bao gồm đồ chơi, quần áo và phụ kiện, đồ đạc, vải vóc, vật liệu xây dựng chẳng hạn. Ngay cả các công nghệ quốc phòng cũng đã bị ảnh hưởng bởi các vi mạch giả mạo.

Việc xác thực độc lập là không đủ để ngăn chặn vấn đề giả mạo. Những kẻ làm giả sử dụng nhiều kỹ thuật khác nhau, bao gồm việc tuồn ra các sản phẩm chưa hoàn thiện từ nhà máy chế tạo sản phẩm chính hãng và thêm các dấu hiệu nhận dạng thương

hiệu giả của họ ví dụ như nhãn và thẻ. Các mặt hàng giả mạo có thể đi vào chuỗi cung ứng tại bất kỳ điểm nào, bao gồm tại cơ sở sản xuất ban đầu, tại nhà vận chuyển, tại nơi phân phối hoặc tại các cửa hàng bán lẻ. Trừ khi nhà sản xuất hoặc nhà cung cấp có thể xác định chính xác ở đâu và khi nào mặt hàng đó đi vào chuỗi cung ứng, nếu không thì việc nhận dạng hàng giả gần như là không thể.

Giải pháp mong muốn chính là phương pháp mà giống với các phương pháp sinh trắc dùng để nhận dạng và xác minh con người. Quy trình này sẽ nhận dạng được các mẫu hình riêng biệt hoặc các đặc trưng chính có thể được sử dụng để xác thực vật một cách duy nhất. Khi các mẫu hình này được trích xuất, cùng với các kỹ thuật băm và mã hóa thích hợp, thì các đặc trưng thu được có thể nhỏ gọn và không sao chép được, do đó đảm bảo quy trình xác thực mà không cần có sự xác minh con người khác.

Một số giải pháp để lấy dấu vân tay đối tượng đã được đề xuất. Xem, ví dụ, J.D. Buchanan, et al., "Forgery: "Fingerprinting" documents and packaging", *Nature* 436, 475 (28/7/2005); W. Clarkson, et al., "Fingerprinting Blank Paper Using Commodity Scanners", *Proc. IEEE Symposium on Security and Privacy*, Tháng 5/2009, pp. 301-314; A. Sharma, et al., "Paperspeckle: microscopic fingerprinting of paper", Proc. 18th ACM Conf. Comput. Comm. Secur., pp. 99-110, 2011. Công trình nghiên cứu được mô tả trong các tài liệu này nói chung đề cập đến việc trích xuất và mã hóa cấu trúc bề mặt của các đối tượng. Ngoài ra, các đặc tính vật lý như tính ngẫu nhiên của kết cấu còn được xem xét khi mã hóa các đặc trưng đã được trích xuất của chúng. Tuy nhiên, các giải pháp trên thường phụ thuộc vào các sự thiết lập máy móc phức tạp hoặc cần có sự căn chỉnh chính xác, khiến cho nó không thực tế để áp dụng rộng rãi. Do đó, vẫn có nhu cầu đối với hệ thống và phương pháp thực hiện xác thực đối tượng mà mọi người, từ các nhà môi giới tác phẩm nghệ thuật phức tạp đến người tiêu dùng phổ thông, có thể chi trả được và tiếp cận được.

Các phương pháp tiếp cận khác nhau đã được thực hiện để đưa ra các giải pháp xử lý tình trạng gia tăng của hàng giả. Một ví dụ đó là dự án RF-DNA của Microsoft, dự án này sử dụng Chứng nhận xác thực (certificate of authenticity, COA) có công nghệ phức tạp, thiết bị chống hàng giả có "chữ ký" khó sao chép nhưng lại dễ dàng và thuận tiện để xác thực. COA được đề xuất là đối tượng vật lý được ký số có các kích thước cố định có cấu trúc duy nhất ngẫu nhiên. Điều cốt lõi trong các yêu cầu của nó đó là COA không đắt để làm ra được và xác thực, nhưng rất đắt để có thể sao chép. Sử

dụng "dấu vân tay" điện từ tần số vô tuyến của các bộ cộng hưởng điện môi và dẫn điện trong trường gần là cơ sở công nghệ của COA đề xuất. DuPont™ đề xuất công nghệ chống hàng giả Izon®, công nghệ này sử dụng hệ thống bảo mật dựa trên ảnh ba chiều 3D trực quan có hình ảnh được nhúng để tạo nhãn sản phẩm.

Các hệ thống hiện có cần có sự quản trị tập trung và sự cung ứng các thiết bị bảo mật, điều này có thể giới hạn khả năng truy cập để tạo ra các bản ghi cũng như để thu được thông tin về bản ghi. Hơn nữa, khi có nhiều thực thể quản trị khả dụng, và nhiều chuẩn được sử dụng để tạo ra và lưu giữ bản ghi, bất kỳ ai tìm kiếm thông tin về mặt hàng cụ thể sẽ cần phải biết chuẩn nào đang được sử dụng và sẽ cần có khả năng giải mã đối với mỗi chuẩn khả dụng.

Các nỗ lực để giải quyết các thách thức đối với việc ghi lại quyền sở hữu các tài sản số, và việc chuyển giao các bản quyền số, nghĩa là quản lý các bản quyền số hoặc "DRM", đã thực hiện nhiều phương pháp tiếp cận khác nhau. Như được mô tả trong Bằng sáng chế Mỹ số 9,064,276, Amazon Technologies, Inc. mô tả hệ thống tạo ra các kho lưu số cho ứng dụng cụ thể để cho phép người dùng cuối thực hiện giao dịch với các bên khác để mua, bán hoặc giao dịch các mục nội dung (trò chơi, âm nhạc, sách điện tử, phim, v.v.) được kết hợp với ứng dụng. Hệ thống này phụ thuộc vào hệ thống quản lý nội dung tập trung mà qua đó các dấu hiệu xác thực giới hạn thời gian được kết hợp với các mục cần được chuyển giao. Nếu các dấu hiệu không được mua lại trong khoảng thời gian xác định, thì không có bản ghi chuyển giao nào được tạo ra trong cơ sở dữ liệu trung tâm.

Các hệ thống chuỗi khối là các hệ thống trạng thái toàn cầu trong đó trạng thái toàn cầu được lưu trữ trên một số thiết bị phân tán. Ví dụ là các mạng như Bitcoin, Ripple, Namecoin và các mạng khác. Sự kết hợp của mã hóa khóa công khai/bí mật và các chuỗi băm cung cấp cơ chế để lưu trữ các trạng thái bảo mật tùy ý dưới dạng một sổ cái - chuỗi khối - được đặt tại tất cả các nút phân tán. Các nút cập nhật trạng thái cục bộ của chúng dựa trên các thuật toán băm "bằng chứng công việc" được áp dụng cho toàn bộ hệ thống. Các hệ thống này cung cấp cơ chế bảo mật để thiết lập nền tảng chung trên nhiều thiết bị.

Ascribe dựa trên Berlin cung cấp hệ thống xác minh và bản quyền kỹ thuật số sử dụng giá trị băm mật mã của tác phẩm nghệ thuật kỹ thuật số được ghi trong chuỗi

khối bitcoin. Phương pháp của Ascribe, được mô tả trong Công số Sáng chế Quốc tế số WO 2015/024129, sử dụng giá trị băm của tác phẩm nghệ thuật để tạo ra ký hiệu nhận dạng là địa chỉ Bitcoin. Các sự chuyển giao của tác phẩm nghệ thuật được thể hiện bằng các giao dịch Bitcoin. Do đó, hệ thống phụ thuộc vào chuẩn tiền điện tử cụ thể và sẽ không tương thích với các loại tiền điện tử khác. Hơn nữa, sự phụ thuộc vào mã hóa đường cong elip của Bitcoin tạo thành giá trị băm chỉ là 160 bit (giá trị băm thứ nhất: SHA256; giá trị băm thứ hai: RIPEMD-160), mà đã được dự báo là sẽ dễ bị tấn công bởi các tin tặc khi máy tính lượng tử khả dụng. Các công ty khác, gồm có Proof of Existence và Blocksign, trong số nhiều công ty khác, cung cấp các hệ thống để băm các tài liệu thành chuỗi khối bitcoin, tạo ra chứng nhận sự tồn tại của tài liệu, giống với dịch vụ công chứng, cho phép nó được xác minh sau. Đối với Ascribe, việc sử dụng chuỗi khối bitcoin giới hạn hệ thống ở chuẩn tiền điện tử duy nhất.

EverLedger ghi lại hàng nghìn viên kim cương và các đặc điểm duy nhất của chúng vào chuỗi khối bitcoin nhằm nỗ lực ngăn chặn gian lận. Dự định sẽ ứng dụng vào các mặt hàng xa xỉ có giá trị cao khác mà nguồn gốc của chúng phụ thuộc vào các chứng nhận trên giấy. Ít nhất là đối với các viên kim cương, việc kiểm tra bởi phòng thí nghiệm được ủy quyền là cần thiết để đảm bảo tính thống nhất về "dấu vân tay" đối với mỗi viên. Các phương pháp này sử dụng mã op bản thảo bitcoin OP_RETURN. Nhà phát triển có mối quan tâm tương đối lớn liên quan đến các phương pháp này - việc lưu trữ dữ liệu tùy ý trong chuỗi khối thường được xem là "ý tưởng tồi". Việc lưu trữ dữ liệu không phải tiền vào chỗ khác sẽ tiết kiệm chi phí hơn và hiệu quả hơn.

Nhu cầu cần có hệ thống khả dụng rộng rãi cho hầu hết tất cả các người dùng tiềm năng và không phụ thuộc vào hệ thống tiền điện tử hoặc phương pháp băm cụ thể bất kỳ.

Bản chất kỹ thuật của sáng chế

Theo một phương án làm ví dụ, phương pháp và hệ thống tài sản phi tập trung được đưa ra để cho phép quyền sở hữu được chuyển giao trực tiếp từ một bên sang bên khác mà không cần có trung tâm có thẩm quyền trung gian để vận hành hoặc bảo mật hệ thống. Các chữ ký số đưa ra phương pháp để phát hành và chuyển giao quyền ("bitmark") trong hệ thống. Bằng cách sử dụng thuật toán chuỗi khối, có thể đạt được thỏa thuận phân tán về việc ai sở hữu cái gì. Các tài sản số có thể được nhận dạng duy

nhất bởi các dấu vân tay số nhờ sử dụng các hàm băm mã hóa an toàn. Các dấu vân tay được tính toán từ các hình ảnh của tài sản có thể được sử dụng trong phương pháp nhận dạng duy nhất các tài sản hiện vật. Theo một số phương án, ký hiệu nhận dạng duy nhất được sử dụng cho tài sản hiện vật có thể là hàm không thể nhân bản vật lý, hay "PUF". Các sự chuyển giao quyền là có thể xác minh và tạo ra chuỗi quyền sở hữu không làm giả được ("nguồn gốc").

Chữ ký số và các phương pháp khác như dấu vân tay đưa ra phương pháp để phát hành và chuyển giao các quyền ("bitmark") bằng cách sử dụng thuật toán chuỗi khối tương tự nhưng có các sự khác biệt lớn với thuật toán được sử dụng đối với Bitcoin (tham khảo, Satoshi Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System", có trên trang web bitcoin.org, được kết hợp trong bản mô tả này bằng cách tham chiếu. Một sổ cái thống nhất độc lập với đồng tiền điện tử bất kỳ được tạo ra. Bản ghi tài sản bao gồm các thuộc tính cụ thể mô tả tài sản được tạo ra để biểu diễn số tài sản. Bản ghi phát hành sau đó được tạo ra để biểu diễn các phiên bản của tài sản liên kết với một bản ghi tài sản cụ thể. Bản ghi chuyển giao được tạo ra để ghi nhận mỗi sự thay đổi quyền sở hữu. Các bản ghi chuyển giao được liên kết với nhau và gốc bản ghi được liên kết với bản ghi phát hành mà được liên kết với bản ghi tài sản. Bitmark là chuỗi gồm tất cả các bản ghi, mà được lưu trữ trong chuỗi khối bitmark. Không có tiền điện tử nào được tạo ra trong quá trình xây dựng chuỗi khối, và cũng không có tiền điện tử nào được sử dụng để biểu diễn sự chuyển giao quyền sở hữu. Bởi vì chuỗi khối bitmark độc lập với hệ thống tiền điện tử cụ thể bất kỳ, các hàm băm từ họ thuật toán băm bảo mật bất kỳ đều có thể được sử dụng, bao gồm SHA-2 và SHA-3.

Mỗi người dùng hệ thống bitmark có một tài khoản gắn với một số duy nhất, ví dụ, cặp khóa công khai ("pubkey") Ed25519, hoặc hệ thống pubkey thích hợp khác cho phép người dùng ký các bản ghi phát hành và bản ghi chuyển giao. Chủ sở hữu bitmark được nhận dạng bởi pubkey của họ. Điều này khác với Bitcoin, Bitcoin chỉ có một loại địa chỉ và chữ ký bởi vì tài khoản bitmark có thể hỗ trợ nhiều loại chữ ký bao gồm các thuật toán tính toán hậu lượng tử ví dụ như SPHINCS.

Theo một khía cạnh của sáng chế, dữ liệu mã hóa được suy ra từ các hình ảnh của các vùng cục bộ của đối tượng vật lý được sử dụng để tham chiếu bảo mật ("lấy dấu vân tay") các tài sản hiện vật dựa trên các mẫu hình cấu trúc mức bề mặt duy nhất,

kết xuất tài sản hiện vật truy nguyên được dưới dạng mục kỹ thuật số. Hàm băm mã hóa an toàn được sử dụng để lấy dấu vân tay các tài sản số. Sáng chế đề xuất bộ khung để xác thực các đối tượng hoặc vật thể khác nhau thông qua việc trích xuất và so khớp các dấu vân tay của chúng. Không giống như các quy trình lấy dấu vân tay sinh trắc sử dụng các mẫu hình như các điểm kết thúc và các điểm rẽ nhánh làm "các điểm quan tâm", một phương án theo sáng chế áp dụng các kỹ thuật quang trắc lập thể để khôi phục các vùng hình ảnh cục bộ của các đối tượng chứa thông tin cấu trúc bề mặt. Các điểm quan tâm của các vùng hình ảnh được khôi phục có thể được phát hiện và mô tả bằng các thuật toán thị giác máy tính tiên tiến. Cùng với các kỹ thuật băm và giảm kích thước, phương pháp theo sáng chế có thể thực hiện việc xác minh đối tượng nhờ sử dụng các đặc trưng hình ảnh nén cho đối tượng bất kỳ, bao gồm cả tài liệu, cho các tác vụ xác thực đối tượng vật lý thực tế.

Cần lưu ý rằng các kỹ thuật được mô tả ở đây khác biệt với "Quản lý bản quyền số (Digital Rights Management, DRM)". Việc khiến cho những người thực thi tôn trọng quyền sở hữu trí tuệ được ghi nhận của người khác phụ thuộc vào bản chất cụ thể của tài sản và quyền hạn pháp lý. Hệ thống và phương pháp theo sáng chế cung cấp phương tiện để đồng thuận bảo mật về việc ai sở hữu cái gì.

Theo một khía cạnh của sáng chế, phương pháp ghi nhận quyền sở hữu đối với tài sản bao gồm các bước: sử dụng thiết bị tính toán, tạo ra bản ghi tài sản có dấu vân tay bao gồm giá trị băm của phép biểu diễn số của tài sản, khóa công khai của khách hàng tạo ra bản ghi tài sản, và chữ ký số bao gồm khóa bí mật của khách hàng tạo ra; sử dụng thiết bị tính toán, truyền thông với một hoặc nhiều nút của mạng ngang hàng để tạo ra mục nhập trong sổ cái công cộng bằng cách thực hiện các bước: tạo ra ít nhất một bản ghi phát hành bao gồm giá trị băm kép của dấu vân tay, khóa công khai của khách hàng tạo ra, và chữ ký chủ sở hữu bao gồm giá trị băm của chữ ký số của khách hàng tạo ra với dấu vân tay băm kép và khóa công khai của khách hàng tạo ra; và hiển thị ít nhất một bản ghi phát hành trên sổ cái công cộng. Theo một số phương án, tài sản là tài sản số được chọn từ nhóm gồm có âm nhạc, video, sách điện tử, ảnh chụp kỹ thuật số, hình ảnh kỹ thuật số và dữ liệu cá nhân. Theo một phương án khác, tài sản là tài sản hiện vật, và phương pháp này còn bao gồm bước tạo ra dấu vân tay số tương ứng với tài sản hiện vật bằng cách sử dụng hình ảnh cục bộ của vùng quan tâm trên bề mặt của tài sản hiện vật. Hình ảnh cục bộ có thể là hình ảnh quang trắc lập thể mà từ

đó thiết bị tính toán nhận dạng các điểm quan tâm cục bộ trong hình hình ảnh quang trắc lập thể bằng cách sử dụng bộ dò điểm chính; và mã hóa các điểm quan tâm cục bộ dưới dạng chuỗi nhị phân bằng cách sử dụng bộ mô tả nhị phân; trong đó chuỗi nhị phân bao gồm phép biểu diễn số của tài sản.

Phương pháp này còn bao gồm bước tạo ra bản ghi chuyển giao thứ nhất để ghi nhận chuyển giao tài sản cho chủ sở hữu mới, trong đó bản ghi chuyển giao này bao gồm giá trị băm kép của bản ghi phát hành hoàn chỉnh cho tài sản và khóa công khai của chủ sở hữu mới, trong đó bản ghi chuyển giao được ký tên số bằng chữ ký chủ sở hữu; sử dụng thuật toán chuỗi khối để tạo ra thỏa thuận phân tán về quyền sở hữu tài sản được kết hợp với chữ ký chủ sở hữu để xác thực bản ghi chuyển giao thứ nhất; và nếu bản ghi chuyển giao thứ nhất được xác thực, thì hiển thị bản ghi chuyển giao này trên sổ cái công cộng; và nếu bản ghi chuyển giao thứ nhất không được xác thực, thì loại bỏ bản ghi chuyển giao này. Theo một số phương án, phương pháp này có thể còn bao gồm, sau bước tạo ra bản ghi chuyển giao thứ nhất: bước hiển thị yêu cầu thanh toán trên giao diện người dùng; và bước xác định xem khoản thanh toán của người dùng đã được chuyển hay chưa trước khi tiếp tục với bước thực thi.

Phương pháp này có thể còn bao gồm bước tạo ra bản ghi chuyển giao tiếp theo để ghi nhận chuyển giao từ chủ sở hữu trước đó sang chủ sở hữu mới tiếp theo, trong đó bản ghi chuyển giao tiếp theo bao gồm giá trị băm kép của bản ghi chuyển giao trước đó, và khóa công khai của chủ sở hữu mới tiếp theo, trong đó bản ghi chuyển giao tiếp theo được ký tên số bởi chủ sở hữu trước đó. Theo một số phương án, phương pháp có thể còn bao gồm, sau bước tạo ra bản ghi chuyển giao tiếp theo: bước hiển thị yêu cầu thanh toán trên giao diện người dùng; và bước xác định xem khoản thanh toán của người dùng đã được chuyển hay chưa trước khi tiếp tục với bước thực thi. Theo các phương án trong đó ít nhất một bản ghi phát hành bao gồm nhiều bản ghi phát hành, mỗi bản ghi phát hành bao gồm một số dùng một lần khác nhau và được kết hợp với chuỗi khối riêng.

Theo một khía cạnh khác của sáng chế, hệ thống ghi nhận quyền sở hữu đối với tài sản bao gồm: thiết bị tính toán khách được tạo cấu hình để tạo ra bản ghi tài sản có dấu vân tay bao gồm giá trị băm của phép biểu diễn số của tài sản, khóa công khai của khách hàng tạo ra bản ghi tài sản, và chữ ký số bao gồm khóa bí mật của khách hàng tạo ra; mạng ngang hàng truyền thông với thiết bị tính toán khách để tạo ra mục nhập

trong sổ cái công cộng bằng cách thực hiện các bước: tạo ra ít nhất một bản ghi phát hành bao gồm giá trị băm kép của dấu vân tay, khóa công khai của khách hàng tạo ra, và chữ ký chủ sở hữu bao gồm giá trị băm của chữ ký số của khách hàng tạo ra với dấu vân tay băm kép và khóa công khai của khách hàng tạo ra; và hiển thị ít nhất một bản ghi phát hành trên sổ cái công cộng. Tài sản có thể là tài sản số được chọn từ nhóm gồm có âm nhạc, video, sách điện tử, ảnh chụp kỹ thuật số, hình ảnh kỹ thuật số và dữ liệu cá nhân. Theo cách khác, tài sản có thể là tài sản hiện vật, trong đó thiết bị tính toán khách còn truyền thông với thiết bị quang trắc lập thể được tạo cấu hình để tạo ra dấu vân tay số tương ứng với tài sản hiện vật nhờ sử dụng ảnh cục bộ của vùng quan tâm trên bề mặt của tài sản hiện vật. Thiết bị quang trắc lập thể được tạo cấu hình để nhận dạng các điểm quan tâm cục bộ trong hình ảnh quang trắc lập thể bằng cách sử dụng bộ dò điểm chính; và mã hóa các điểm quan tâm cục bộ dưới dạng chuỗi nhị phân bằng cách sử dụng bộ mô tả nhị phân; trong đó chuỗi nhị phân bao gồm phép biểu diễn số của tài sản. Thiết bị tính toán khách và ít nhất một nút trong mạng ngang hàng có thể còn được tạo cấu hình để truyền thông để tạo ra bản ghi chuyển giao thứ nhất để ghi nhận chuyển giao tài sản cho chủ sở hữu mới, trong đó bản ghi chuyển giao này bao gồm giá trị băm kép của bản ghi phát hành hoàn chỉnh cho tài sản và khóa công khai của chủ sở hữu mới, trong đó bản ghi chuyển giao được ký tên số bằng chữ ký chủ sở hữu; sử dụng thuật toán chuỗi khối để tạo ra thỏa thuận phân tán về quyền sở hữu tài sản được kết hợp với chữ ký chủ sở hữu để xác thực bản ghi chuyển giao thứ nhất; và nếu bản ghi chuyển giao thứ nhất được xác thực, thì hiển thị bản ghi chuyển giao này trên sổ cái công cộng; và nếu bản ghi chuyển giao thứ nhất không được xác thực, thì loại bỏ bản ghi chuyển giao này. Theo một số phương án, hệ thống còn bao gồm việc khiến ít nhất một thiết bị tính toán khách và ít nhất một nút truyền thông, sau bước tạo ra bản ghi chuyển giao tiếp theo, để hiển thị yêu cầu thanh toán trên giao diện người dùng; và xác định xem khoản thanh toán của người dùng đã được chuyển hay chưa trước khi tiếp tục với bước thực thi.

Hệ thống này có thể còn bao gồm ít nhất một thiết bị tính toán khách thứ hai truyền thông với mạng ngang hàng để tạo ra bản ghi chuyển giao tiếp theo để ghi nhận chuyển giao từ chủ sở hữu trước đó sang chủ sở hữu mới tiếp theo, trong đó bản ghi chuyển giao tiếp theo bao gồm giá trị băm kép của bản ghi chuyển giao trước đó, và khóa công khai của chủ sở hữu mới tiếp theo, trong đó hệ thống có thể còn bao gồm

việc khiến ít nhất một thiết bị tính toán khách thứ hai, sau khi tạo ra bản ghi chuyển giao tiếp theo, hiển thị yêu cầu thanh toán trên giao diện người dùng; và xác định xem khoản thanh toán của người dùng đã được chuyển hay chưa trước khi tiếp tục với bước thực thi.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ khối của hệ thống theo sáng chế.

Fig.2 là sơ đồ khối của một phương án của hệ thống thể hiện nhiều bản ghi chuyển giao.

Fig.3A là sơ đồ khối thể hiện giao dịch ban đầu để tạo ra bản ghi tài sản.

Fig.3B là sơ đồ khối thể hiện các giao dịch trong đó các bitmark được tạo ra dựa trên bản ghi tài sản của Fig.3A.

Fig.3C là sơ đồ khối thể hiện các giao dịch trong hai bitmark.

Fig.3D là sơ đồ khối thể hiện việc phát hành bitmark bổ sung dựa trên bản ghi tài sản gốc trên Fig.3A.

Fig.4 là sơ đồ thể hiện giao diện người dùng (user interface, UI) làm ví dụ cho bản ghi bitmark mẫu.

Fig.5 là sơ đồ thể hiện UI làm ví dụ để chuyển giao bitmark.

Fig.6 là sơ đồ thể hiện UI làm ví dụ sau khi hoàn tất sự chuyển giao của Fig.5.

Fig.7A là hình vẽ dạng sơ đồ của một phương án của thiết bị dùng để tạo ra các dấu vân tay được mã hóa cho các tài sản hiện vật; Fig.7B minh họa việc sử dụng mẫu của thiết bị.

Fig.8 là sơ đồ khối thể hiện các bước để tạo ra dấu vân tay được mã hóa cho tài sản hiện vật.

Các hình vẽ từ Fig.9A đến Fig.9C thể hiện sự so sánh của các sự phân bố điểm số đạt được nhờ sử dụng một phương án của phương pháp quang trắc lập thể so với lấy dấu vân tay đối tượng vật lý (Fig.9A) và phương pháp đường cơ sở (Fig.9B); Fig.9C so sánh các đường cong ROC đối với mỗi phương pháp.

Fig.10 là sơ đồ của môi trường mạng làm ví dụ để thực hiện phương án của hệ thống theo sáng chế.

Mô tả chi tiết sáng chế

Nhằm mục đích mô tả các phương án theo sáng chế, các định nghĩa sau đây sẽ áp dụng:

"Tài khoản" là cặp khóa công khai-bí mật được sử dụng để nhận dạng đăng ký và quyền sở hữu tài sản trong hệ thống bitmark. Ký hiệu nhận dạng (identifier, ID) tài khoản, còn được gọi là "số tài khoản công khai" hoặc "tài khoản bitmark", là khóa công khai. Một người dùng có thể có nhiều tài khoản trong hệ thống bitmark. Tài khoản là dạng mã hóa cho khóa công khai, nghĩa là, "tài khoản" trong hệ thống bitmark. Tài khoản chứa các thông tin khác nhau về khóa. Theo một phương án làm ví dụ, dạng mã hóa này là dạng mã hóa base58.

"Bản ghi tài sản" là cấu trúc dữ liệu chuỗi khối ghi nhận một cách bất biến việc đăng ký tài sản mới trong trong hệ thống bitmark.

"Bitmark" là quyền số đảm bảo quyền sở hữu đối với tài sản hiện vật hoặc tài sản số cụ thể trong hệ thống bitmark. Việc chuyển giao bitmark từ một chủ sở hữu sang chủ sở hữu khác là chuyển giao quyền sở hữu tài sản được định rõ. Bitmark được biểu diễn trong chuỗi khối qua chuỗi bản ghi chuyển giao bitmark và bản ghi phát hành gốc.

"Bản ghi chuyển giao bitmark" hoặc "BTR" là cấu trúc dữ liệu chuỗi khối biểu diễn quyền bitmark.

"Phát hành" là quy trình tạo ra các bitmark mới cho tài sản số. Phát hành chỉ có thể áp dụng với các tài sản số và tạo ra một cách hiệu quả nhiều bản sao hơn mà có thể được sở hữu trong hệ thống bitmark. Việc phát hành bitmark mới chỉ có thể được thực hiện bởi chủ sở hữu bản ghi chuyển giao đăng ký gần đây nhất.

"Định dạng nhập khóa" hoặc "KIF" là việc mã hóa (base-58 hoặc khác) của khóa bí mật và một số đối tượng thuật toán và kiểm tra tổng. KIF có thể được sử dụng để nhập tài khoản bitmark trở lại cho khách hàng.

"Chủ sở hữu" là người dùng bất kỳ của hệ thống bitmark, người này giữ khóa bí mật cho ít nhất một tài khoản. Người dùng hệ thống bitmark được gọi là "sở hữu bitmark" nghĩa là anh ấy/cô ấy giữ khóa bí mật tương ứng với trường khóa công khai của chủ sở hữu trong bản ghi chuyển giao bitmark mới nhất trong chuỗi bitmark của

chủ sở hữu.

"Cụm mật khẩu" là mật khẩu phức tạp được sử dụng để truy cập vào kho khóa của người dùng. Trong khi tài khoản bitmark nhận dạng kho khóa được đồng bộ nào thuộc về người dùng để tải về cục bộ, cụm mật khẩu cho phép người dùng giải mã kho khóa cục bộ và truy cập các khóa bí mật cho mỗi tài khoản của họ. Cả ID tài khoản bitmark và cụm mật khẩu đều cần thiết để đăng nhập vào ứng dụng khách hàng bitmark. Cụm mật khẩu cũng cần thiết bất kỳ khi nào giao dịch bảo mật được khởi tạo trong máy khách.

"Tài sản" là phép trình diễn số duy nhất (giá trị băm) của tài sản hiện vật hoặc tài sản số. Giá trị băm của tài sản được tạo ra trong khi đăng ký định giá cho tài sản mới. Trong quá trình ghi nhận đăng ký, giá trị băm của tài sản là vĩnh viễn và bất biến.

"Người đăng ký" là tài khoản bitmark được sử dụng để tạo ra đăng ký cho tài sản mới, bản ghi tài sản, trong hệ thống bitmark. Cụ thể hơn là, khóa công khai của tài khoản được ghi nhận bất biến trong trường "người đăng ký" của bản ghi tài sản, và khóa bí mật của tài khoản được sử dụng để ký bản ghi tài sản. Đối với tài sản hiện vật, người đăng ký đồng thời là chủ sở hữu của bản ghi chuyển giao bitmark ban đầu. Đối với tài sản số, người đăng ký là chủ sở hữu của bản ghi chuyển giao đăng ký ban đầu.

"Đăng ký" là quy trình thêm tài sản hiện vật hoặc tài sản số mới vào chuỗi khối bitmark. Việc đăng ký ràng buộc vĩnh viễn một tài sản với bản ghi đăng ký trong chuỗi khối. Việc đăng ký được tạo ra bởi người đăng ký và được ghi nhận trong chuỗi khối dưới dạng bản ghi đăng ký. Bản ghi đăng ký đóng vai trò làm phần tử cơ sở cho toàn bộ chuỗi bitmark của tài sản.

"Bản ghi chuyển giao đăng ký" hay "RTR" là cấu trúc dữ liệu chuỗi khối biểu diễn chủ sở hữu hiện thời của hoạt động đăng ký tài sản. Các RTR chỉ tồn tại đối với tài sản số. Quyền sở hữu bản ghi chuyển giao đăng ký cấp quyền khả năng phát hành bitmark cho chủ sở hữu. Sự khác nhau duy nhất về mặt kỹ thuật giữa bản ghi chuyển giao đăng ký và bản ghi chuyển giao bitmark là loại tài sản.

"Giao dịch" là quy trình bất kỳ trong số ba quy trình bitmark chính: đăng ký, chuyển giao và phát hành.

"Chuyển giao" là sự thay đổi quyền sở hữu từ một tài khoản bitmark sang tài

khoản khác. Sự chuyển giao có thể áp dụng vào BTR hoặc RTR. Giao dịch chuyển giao tạo ra một BTR hoặc RTR mới được ký bởi khóa bí mật của chủ sở hữu cũ và được chỉ định cho khóa công khai của người dùng mới. Chuỗi bản ghi chuyển giao cấu thành đăng ký hoặc chuỗi quyền sở hữu bitmark, trong chuỗi khối bitmark.

Theo các phương án của sáng chế, hệ thống và phương pháp tài sản phi tập trung cho phép quyền sở hữu được chuyển giao trực tiếp từ một bên cho bên khác mà không cần có trung tâm có thẩm quyền trung gian để vận hành hoặc bảo mật hệ thống, và không phụ thuộc vào hệ thống tiền điện tử hiện có. Các chữ ký số đưa ra phương pháp để phát hành và chuyển giao quyền ("bitmark") trong hệ thống. Bằng cách sử dụng thuật toán chuỗi khối, có thể đạt được thỏa thuận phân tán về việc ai sở hữu tài sản, theo cách tương tự như cách dùng cho Bitcoin và các loại tiền điện tử khác. Tài sản số có thể được nhận dạng duy nhất bằng cách sử dụng các hàm băm mã hóa an toàn. Các dấu vân tay được suy ra từ các hình ảnh cục bộ của tài sản hiện vật có thể được sử dụng để nhận dạng duy nhất tài sản hiện vật. Việc chuyển giao quyền là có thể xác minh và tạo ra chuỗi quyền sở hữu không thể làm giả ("nguồn gốc").

Theo một khía cạnh của sáng chế, dữ liệu mã hóa được suy ra từ các hình ảnh của các vùng cục bộ của bề mặt của đối tượng vật lý được sử dụng để tham chiếu bảo mật ("lấy dấu vân tay") các tài sản hiện vật dựa trên các mẫu hình cấu trúc mức bề mặt duy nhất. Hàm băm mã hóa an toàn được sử dụng để lấy dấu vân tay các tài sản số. Sự khan hiếm tài sản số là có thể xảy ra và có thể thích nghi với các bộ khung khái niệm và pháp lý của thế giới thực.

Để bắt đầu sử dụng hệ thống bitmark, người dùng hoặc "khách hàng", trước tiên cần tạo tài khoản. Khách hàng có thể đăng nhập vào hệ thống bitmark bằng cách sử dụng ứng dụng dựa trên web được lưu trữ hoặc truy cập nhờ sử dụng máy tính để bàn hoặc thiết bị tính toán cá nhân khác, hoặc sử dụng thiết bị di động có "ứng dụng bitmark". Nhằm mục đích mô tả hệ thống bitmark, các thiết bị này sẽ được gọi chung là "các thiết bị tính toán". Trình hướng dẫn cài đặt hướng dẫn người dùng thực hiện các bước tạo tài khoản mới. Trước tiên một số tài khoản được chỉ định. Theo một phương án làm ví dụ, số tài khoản bitmark 50 ký tự duy nhất được sử dụng để nhận dạng người dùng và các tài sản của anh ấy/cô ấy trong hệ thống bitmark. Số tài khoản là ký hiệu nhận dạng mà khách hàng đưa cho người dùng bitmark khác để chuyển giao các bitmark sang tài khoản của khách hàng. Số tài khoản sẽ vẫn có thể truy cập trên

thiết bị tính toán từ trang thiết lập của khách hàng.

Bước tiếp theo trong việc tạo tài khoản bitmark bao gồm bước tạo và lưu trữ khóa bí mật của khách hàng, việc này cũng diễn ra trên thiết bị tính toán của khách hàng, nghĩa là, không phải ở máy chủ hệ thống bitmark ("máy chủ bitmarkd"). Theo một phương án làm ví dụ, khóa bí mật là chuỗi 54 ký tự được sử dụng để truy cập tài khoản của khách hàng và kiểm soát tài sản mà các bitmark đã được tạo ra cho chúng. Tài khoản bitmark sau đó được tạo ra từ khóa bí mật của khách hàng. Ngoài việc kiểm soát tài sản của khách hàng, khóa bí mật cung cấp phương tiện cho phần mềm bitmark để khôi phục tài khoản trong trường hợp thiết bị tính toán của khách hàng bị mất hoặc bị hỏng. Bởi vì máy chủ bitmarkd không tạo ra hoặc lưu trữ khóa bí mật, trình hướng dẫn cài đặt hướng dẫn người dùng lưu khóa bí mật ở nơi an toàn, tách riêng với thiết bị tính toán, sau đó hướng dẫn người dùng nhập khóa bí mật để xác minh. Sau khi xác minh khóa bí mật, người dùng được hướng dẫn nhập mật khẩu có thể được sử dụng, khi sử dụng cùng thiết bị tính toán, dưới dạng lối tắt để nhập khóa bí mật của người dùng. Một khi mật khẩu được nhập và xác minh, phần mềm bitmark khởi tạo tài khoản mới tương ứng với số tài khoản của người dùng. Người dùng giờ đây đã sẵn sàng bắt đầu ghi nhận các tài sản của anh ấy/cô ấy trong hệ thống bitmark.

Trên Fig.1, bitmark 100 được xác định là một chuỗi được ký tên số bao gồm một bản ghi phát hành 102 và một hoặc nhiều bản ghi chuyển giao 104, mà có thể là BTR hoặc RTR. Bản ghi tài sản 106 chứa siêu dữ liệu cho tài sản hiện vật hoặc tài sản số cũng như dấu vân tay tài sản duy nhất được sử dụng để nhận dạng nó trong hệ thống bitmark. Mỗi bản ghi tài sản 106 bao gồm các trường sau: "dấu vân tay" 108, là giá trị băm của phép biểu diễn số của đối tượng vật lý hoặc tập tin số; người đăng ký 109, là khóa công khai (ED255194) của người đăng ký; (3) "tên" 110, ký hiệu nhận dạng UTF-8 ngắn; (4) "phần mô tả" 111 - nhận dạng văn bản UTF-8; và (5) "chữ ký" 112, giá trị băm của các trường từ 108-111 ký bằng khóa bí mật của người đăng ký.

Bản ghi phát hành 102 tạo ra bitmark mới từ bản ghi tài sản 106. Các bản ghi phát hành 102 bao gồm các trường sau đây: "chỉ số tài sản" 113, giá trị băm SHA-512 kép (64 byte) của giá trị dấu vân tay 108 của bản ghi tài sản 106 tương ứng. Chỉ số tài sản 113 đóng vai trò là ký hiệu nhận dạng duy nhất cho bản ghi tài sản 106 và sẽ giống nhau trên tất cả các bản ghi phát hành 102 cho cùng bản ghi tài sản 106. Dấu vân tay bản ghi tài sản 108 được băm hai lần làm phương tiện để đảm bảo kích thước nhất

quán bất kể kích thước gốc của giá trị dấu vân tay. Cũng được bao gồm trong bản ghi phát hành 102 là pubkey của chủ sở hữu 114. Theo một số phương án, pubkey của chủ sở hữu 114 là khóa công khai (ED25519) của người dùng đã tạo ra phát hành. Như đã được biết đến bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật, các khóa công khai khác, ví dụ như Ed25519+SPHINCS, có thể được sử dụng. Khi có hoạt động phát hành mới diễn ra, bản ghi phát hành 102 được sở hữu tự động bởi người phát hành. Số dùng một lần 115 là số nguyên chưa được ký tên đóng vai trò là số duy nhất để phân biệt nhiều phát hành của cùng tài sản. Bản ghi phát hành 102 cũng bao gồm chữ ký 116, là giá trị băm của các trường từ 113-115 được ký bằng khóa bí mật của người phát hành.

Về mặt kỹ thuật, bitmark chỉ cần bản ghi phát hành 102. Bản ghi chuyển giao là không cần thiết. Bitmark không có các bản ghi chuyển giao đơn giản là thuộc về người phát hành bitmark gốc. Nếu người phát hành bitmark không bao giờ chuyển giao bitmark cho chủ sở hữu khác, thì chuỗi quyền sở hữu bitmark sẽ không bao giờ phát triển vượt quá bản ghi phát hành ban đầu.

Bản ghi chuyển giao 104 chuyển giao quyền sở hữu bitmark và bao gồm các trường sau đây: liên kết 117, là giá trị băm SHA-256 kép (32 byte) của toàn bộ bản ghi trước đó (bao gồm chữ ký 116), biểu thị bản ghi trước đó trong chuỗi quyền sở hữu bitmark. Bản ghi trước đó có thể là bản ghi phát hành 102 hoặc bản ghi chuyển giao khác 104. Bản ghi trước đó được băm hai lần làm phương tiện để đảm bảo kích thước nhất quán bất kể kích thước gốc của bản ghi trước đó. Cũng được bao gồm trong bản ghi chuyển giao 104 là pubkey của chủ sở hữu 118, khóa công khai (ED25519) của người nhận chuyển giao bitmark và chữ ký của chủ sở hữu trước đó 120, giá trị băm của các trường 117 và 118, được ký nhờ sử dụng khóa bí mật của chủ sở hữu bản ghi trước đó 120.

Bản ghi chuyển giao 104 có cả kết nối chuỗi tham chiếu 107 và kết nối chuỗi chữ ký 103. Giá trị của liên kết 117 tương ứng với kết nối chuỗi tham chiếu 107, chính là giá trị băm SHA-256 kép của toàn bộ bản ghi trước. Liên kết 117 là liên kết trỏ vào bản ghi trước trong chuỗi bitmark. Kết nối chuỗi chữ ký 103 đến bản ghi trước đó (bản ghi phát hành hoặc chuyển giao) cần chủ sở hữu của bản ghi trước đó ký tên số vào bản ghi chuyển giao tiếp theo 104 bằng cách sử dụng khóa bí mật của anh ấy/cô ấy.

Phép suy ra thực tế về sự khác nhau giữa chuỗi tham chiếu 107 và chuỗi chữ ký 103 đó là không có kết nối chữ ký số giữa bản ghi tài sản 106 và các bản ghi phát hành 103 được kết nối với bản ghi tài sản đó. Chủ sở hữu khóa công khai được định rõ trong trường người đăng ký 109 của bản ghi tài sản chỉ ký mỗi bản ghi tài sản 106 và không cần phải ký các bản ghi phát hành tiếp theo. Điều này có nghĩa là người dùng bất kỳ có thể phát hành các bitmark mới cho một tài sản bởi vì bản ghi phát hành được tự ký tên bởi người dùng phát hành nó, không phải bởi người đăng ký tài sản gốc. Theo hợp đồng, các bản ghi chuyển giao phải được ký bằng cách sử dụng khóa bí mật của chủ sở hữu bản ghi trước đó. Bởi vì chủ sở hữu hiện thời của bitmark là người dùng duy nhất được ủy quyền để chuyển giao bitmark cho người dùng khác, chuỗi chữ ký đưa ra bằng chứng mã hóa của việc ủy quyền chuyển giao.

Chủ sở hữu hiện thời của bitmark (bản ghi ở ngoài cùng bên phải trong chuỗi) được xác minh bằng cách kiểm tra các chữ ký số trong chuỗi. Trong đó trường liên kết của bản ghi chuyển giao 117 thiết lập chuỗi tham chiếu 107 đến bản ghi trước đó, giá trị chữ ký của bản ghi chuyển giao xác định xem bản ghi chuyển giao 104 có thực sự hợp lệ hay không. Nếu chữ ký số của bản ghi chuyển giao khớp với khóa công khai của chủ sở hữu bản ghi trước đó, thì bản ghi chuyển giao được xem là hợp lệ và được ghi nhận trong chuỗi khối. Nếu không, bản ghi chuyển giao không hợp lệ bị loại bỏ khỏi chuỗi khối. Bản ghi tài sản gốc 106 được xác minh bằng cách xác thực dấu vân tay tham chiếu 108 của nó so với đối tượng thực. Hệ thống bảo vệ chống lại các giao dịch không hợp lệ khác (ví dụ, chuyển giao kép) thông qua máy chủ dấu thời gian phân tán.

Vẫn tham chiếu đến Fig.1, kết nối chuỗi tham chiếu 105 có nghĩa là chỉ số tài sản 113 của bản ghi phát hành trỏ lại giá trị dấu vân tay 108 của bản ghi tài sản tương ứng. Điều này khác với chuỗi chữ ký 103 mà kết nối chữ ký của chủ sở hữu trước đó 120 với pubkey của chủ sở hữu 114. Kết nối này đòi hỏi chữ ký khóa bí mật của chủ sở hữu của bản ghi ở ngay trước trong chuỗi.

Các bản ghi tài sản 106 được tự ký tên. Do đó, người dùng bất kỳ có thể phát hành các bitmark mới cho tài sản, như được thể hiện trên Fig.2. Trong trường hợp này, "Eva" và "Gina", các pubkey của chủ sở hữu được thể hiện trong các bản ghi chuyển giao ở ngoài cùng bên phải 124D và 124G, đều là các chủ sở hữu hiện thời (bởi vì họ giữ bản ghi chuyển giao cuối cùng trong chuỗi bitmark tương ứng của họ (còn được

gọi đơn giản là "các bitmark") 200A và 200B). Xung đột tuyên bố quyền sở hữu bắt nguồn từ các bitmark trỏ đến cùng tài sản nhưng có các chữ ký phát hành khác nhau phải được dàn xếp từ bên ngoài bởi các nhà thực thi quyền sở hữu tài sản. Dưới dạng lịch sử bất biến, vĩnh viễn của tất cả các giao dịch tài sản, các bitmark 200A và 200B sẽ đóng vai trò là bằng chứng.

Ví dụ 1 - Cấu trúc dữ liệu tài sản số mẫu

Ví dụ sau đây minh họa các giao dịch diễn ra theo mô hình dữ liệu cơ sở của hệ thống bitmark. Ví dụ này được đưa ra chỉ nhằm mục đích minh họa, bao gồm một tài sản, ba bitmark cho tài sản và 12 người dùng bitmark khác nhau.

Tham chiếu đến Fig.3A, ví dụ bắt đầu với giao dịch #1 trong đó người dùng #1, "Amanda", đăng ký tài sản mới trong hệ thống bitmark bằng cách tạo bản ghi tài sản mới 150. Nhằm cho mục đích của ví dụ này, tài sản này là sách điện tử mới tự xuất bản có tiêu đề "Things Fell Apart". Mặc dù Amanda có thể sử dụng toàn bộ cuốn sách điện tử để tạo ra dấu vân tay, cô ấy có thể chỉ chọn tạo ra mô tả duy nhất về cuốn sách, ví dụ, điều gì đó đơn giản như tên sách, tên cô ấy và ngày xuất bản, hoặc chọn các đoạn trích dễ nhận diện của cuốn sách, ví dụ, các trang được chọn. Bằng cách truy cập giao diện người dùng ("UI") phát hành bitmark, tập tin số được chọn của Amanda được sao chép, ví dụ, được kéo và thả, hoặc được chọn bằng cách duyệt các tập tin của người dùng và được tải qua UI vào hệ thống bitmark để băm tập tin để tính toán dấu vân tay duy nhất của tài sản. Giao diện người dùng có thể hiển thị hoạt ảnh ví dụ như đồng hồ, đồng hồ cát hoặc bánh xe đang quay trong khi dấu vân tay được tạo ra. Khi dấu vân tay đã được tính toán, thông báo đẩy có thể được gửi đi. Nếu giá trị dấu vân tay chưa tồn tại trong hệ thống bitmark, thì bản ghi tài sản mới 150 được tạo ra. Nếu giá trị dấu vân tay đã tồn tại trong hệ thống bitmark, thay vào đó Amanda sẽ được đề nghị với tùy chọn phát hành các bitmark mới cho tài sản, tuy nhiên chúng sẽ được coi là các tài sản mới, bổ sung.

Trường người đăng ký (thứ hai) của bản ghi tài sản 150 hiển thị khóa công khai của Amanda (tên cô ấy, được biểu thị bằng phông chữ in đậm). Bản ghi tài sản cũng được ký tên nhờ sử dụng khóa bí mật của Amanda. Do đó, bản ghi tài sản được "tự ký tên" bởi người đăng ký tài sản mới.

Không có bitmark nào được tạo ra thực tế trong giao dịch thứ nhất này. Các

bitmark sẽ không được tạo ra cho tới khi các hoạt động phát hành được thực hiện trong hai giao dịch (#2 và #3) được thể hiện trên Fig.3B. Trong các giao dịch #2 và #3, Amanda phát hành hai bitmark mới cho tài sản mà cô đã đăng ký trong giao dịch thứ nhất. Hai bitmark mới 152 và 154 này được tạo ra qua hai bản ghi phát hành mới 160 và 162.

Bởi vì cả hai bản ghi phát hành mới 160 và 162 tham chiếu đến cùng bản ghi tài sản 150 được tạo ra trong giao dịch #1, giá trị dấu vân tay của bản ghi tài sản được băm hai lần nhờ sử dụng thuật toán SHA-512 và được lưu trữ trong tài sản chỉ số tài sản của cả hai bản ghi phát hành mới. Giá trị cho các trường chủ sở hữu của cả hai bản ghi phát hành là khóa công khai của Amanda ("O: Amanda") bởi vì các bản ghi phát hành được sở hữu tự động bởi người dùng đã tạo ra các phát hành. Các trường số dùng một lần ("N") của các bản ghi phát hành chứa các giá trị đếm dùng một lần, ví dụ, "N: 1" và "N: 2" để đảm bảo rằng mỗi bản ghi phát hành cho cùng tài sản là duy nhất. Mỗi bản ghi phát hành 160 và 162 được ký tên ở dưới cùng nhờ sử dụng khóa bí mật của Amanda. Với các bản ghi tài sản, các bản ghi phát hành luôn được tự ký tên nhờ sử dụng khóa bí mật của người dùng đã tạo ra bản ghi phát hành. Người dùng bất kỳ có thể tạo ra các bản ghi phát hành cho tài sản. Không có chuỗi chữ ký số giữa các bản ghi tài sản và các bản ghi phát hành tương ứng của chúng. Kết nối duy nhất giữa các bản ghi phát hành 160, 162 và các bản ghi tài sản 150 tương ứng của chúng là chuỗi tham chiếu 158 được thiết lập bởi mỗi tài sản chỉ số tài sản của bản ghi phát hành. Tại thời điểm này, Amanda sở hữu các bitmark 152 và 154.

Fig.3C minh họa các giao dịch từ #4 đến #7 cho các bitmark 152 và 154. Trong giao dịch #4, Amanda chuyển giao (bán, tặng, cấp quyền, chuyển nhượng hoặc hình thức chuyển giao tài sản khác) bitmark 154 cho Brian. Bản ghi chuyển giao mới 172 liệt kê khóa công khai của Brian là chủ sở hữu ("O: Brian"), và Amanda ký tên vào bản ghi chuyển giao 172 bằng khóa bí mật của cô ấy để ủy quyền chuyển giao, như được biểu thị bằng chuỗi chữ ký 164. Chuỗi tham chiếu 166 bao gồm giá trị băm SHA-256 kép (32B) của bản ghi trước đó.

Trong giao dịch #5, Amanda chuyển giao bitmark 152 cho Chloe, tạo ra bản ghi chuyển giao mới 170 nhận dạng khóa công khai của Chloe và khóa bí mật của Amanda cùng với giá trị băm của bản ghi trước đó 160. Giao dịch #6 ghi nhận chuyển giao bitmark 152 từ Chloe sang Dylan trong bản ghi chuyển giao 180. Bởi vì Chloe

giờ đây là chủ sở hữu, khóa bí mật của cô ấy được sử dụng để ủy quyền chuyển giao qua chuỗi chữ ký giữa các bản ghi chuyển giao 170 và 180. Trong giao dịch thứ bảy, Chloe, chủ sở hữu hiện thời của bitmark 152, chuyển giao bitmark 152 cho Dylan, tạo ra bản ghi chuyển giao 190.

Các bản ghi chuyển giao luôn cần cả kết nối chuỗi tham chiếu với bản ghi trước đó và kết nối chuỗi chữ ký với bản ghi trước đó. Chuỗi tham chiếu được tạo ra bằng cách tính giá trị băm SHA-256 kép của toàn bộ bản ghi trước đó, bao gồm chữ ký, và lưu trữ giá trị băm này trong trường liên kết của bản ghi chuyển giao. Giá trị liên kết báo cho hệ thống bitmark biết bản ghi nào đứng trước bản ghi đã cho trong chuỗi bitmark. Bởi vì mỗi bản ghi chứa thông tin từ bản ghi trước, nó sẽ có thể truy nguyên về chủ sở hữu ban đầu, tạo ra nguồn gốc bất biến.

Trong khi trường liên kết của bản ghi chuyển giao thiết lập chuỗi tham chiếu đến bản ghi trước đó, giá trị chữ ký của bản ghi chuyển giao xác định xem bản ghi chuyển giao có hợp lệ không. Nếu chữ ký số của bản ghi chuyển giao khớp với trường chủ sở hữu của bản ghi trước đó (khóa công khai), bản ghi chuyển giao biểu diễn chuyển giao bitmark hợp lệ, và bản ghi chuyển giao được ghi nhận trong chuỗi khối bitmark. Tuy nhiên, nếu giá trị chữ ký của bản ghi chuyển giao không khớp với khóa công khai của chủ sở hữu bản ghi trước đó, thì các nút xác thực của hệ thống bitmark sẽ xác định Bản ghi chuyển giao là "không hợp lệ" và sẽ loại bỏ bản ghi chuyển giao khỏi bao gồm trong chuỗi khối bitmark. Tóm lại, các giá trị liên kết tạo ra chuỗi tham chiếu cho bitmark, trong khi các giá trị chữ ký bảo mật chuỗi tham chiếu.

Tham chiếu đến Fig.3D, Eddie là người cũng có các quyền nhất định đối với tài sản. Theo ví dụ này, chúng ta có thể nói rằng Eddie là người biên tập của Amanda, và Amanda đã đưa cho Freddie một số bản sao nhất định của cuốn sách điện tử vì đánh giá cao sự hỗ trợ của anh ấy. Amanda cung cấp cho Eddie dấu vân tay mà cô ấy đã tạo ra để chuẩn bị cho giao dịch thứ nhất. Việc có dấu vân tay cho phép Eddie đăng nhập vào hệ thống bitmark và sử dụng dấu vân tay để phát hành bitmark mới 156 bằng cách tạo ra bản ghi phát hành 164. Bản ghi phát hành mới được tự ký bởi Eddie và chỉ số tài sản lại là giá trị băm SHA-512 kép của giá trị dấu vân tay của bản ghi tài sản. Các trường số dùng một lần ("N") của bản ghi phát hành mới này được chỉ định một giá trị số dùng một lần (N = 3) khác với các bản ghi phát hành trước, đảm bảo rằng mỗi bản ghi phát hành cho cùng một tài sản là duy nhất. Sự phát hành mới bởi Eddie cho thấy

rằng giá trị chữ ký của bản ghi phát hành không cần phải khớp với khóa công khai của giá trị người đăng ký cho bản ghi tài sản tương ứng. Mọi người dùng có thể tạo ra bản ghi phát hành cho tài sản, tuy nhiên, người dùng sẽ cần phải truy cập vào dấu vân tay được tạo ra kết hợp với bản ghi tài sản để nó có thể được kết hợp với bản ghi tài sản gốc.

Giao diện người dùng ("UI") của hệ thống bitmark đưa ra các màn hình hiển thị và điểm truy cập khác nhau. Tài khoản bitmark của người dùng có thể truy cập được bằng cách đăng nhập vào qua máy tính cá nhân (máy tính để bàn, máy tính xách tay, máy tính bảng, v.v.) được kết nối với mạng toàn cầu bằng cách truy cập vào trang web Bitmark, hoặc ứng dụng trên máy tính để bàn hoặc trên di động, và: (1) duyệt thiết bị của người dùng (máy tính, điện thoại thông minh, máy tính bảng hoặc thiết bị khác) cho tập tin ID tài khoản bitmark; (2) quét ID tài khoản bitmark (thao tác này có thể bao gồm việc quét màn hình của thiết bị khác.) Theo một số phương án, ID tài khoản bitmark dạng in có thể được đưa ra dưới dạng mã QR có thể quét (mã phản hồi nhanh) hoặc mã có thể đọc quang học khác, bao gồm một, hai hoặc nhiều hơn hai mã vạch kích thước, mã màu và/hoặc tổ hợp của chúng, các giá trị sắc, v.v.. Theo các phương án khác, ID tài khoản bitmark có thể là ảnh chụp bằng lái xe của người dùng, hoặc có thể được mã hóa sinh trắc, ví dụ, dấu vân tay, hình học tay, mẫu võng mạc hoặc con ngươi, đặc trưng khuôn mặt, v.v., mà có thể được quét bằng cách sử dụng camera của điện thoại thông minh hoặc thiết bị quét khác, các mẫu thoại được nhập vào bằng cách sử dụng máy ghi âm của điện thoại thông minh, DNA, hoặc tổ hợp của các đặc điểm sinh trắc duy nhất khác nhau của người dùng.

Trong trường hợp người dùng mất ID tài khoản bitmark của anh ấy hoặc cô ấy, phương pháp thứ ba để đăng nhập vào hệ thống là sử dụng mã khôi phục bitmark. Các mã này thường được cung cấp cho các người dùng hệ thống mới khi họ lần đầu kích hoạt tài khoản. Nếu chế độ khôi phục được khởi tạo bằng cách nhập mã khôi phục, thì người dùng sẽ được gợi ý nhập cụm mật khẩu bitmark mới cần được sử dụng để mã hóa dữ liệu bitmark và để ủy quyền các giao dịch bitmark mới. Hệ thống sẽ cảnh báo người dùng rằng mã khôi phục của họ không nên được lưu trữ trên thiết bị được sử dụng để truy cập hệ thống bitmark. Cụm mật khẩu tốt hơn là nên được in ra và được lưu trữ ở nơi bảo mật như hộp bảo mật tài liệu hoặc hộp ký gửi an toàn. Lựa chọn thứ tư nếu ID tài khoản bitmark của người dùng bị mất không thể cứu vãn được đó là tạo

ID mới.

Một khi người dùng bitmark có quyền truy cập vào tài khoản của anh ấy hoặc cô ấy (hoặc của nó, trong trường hợp là thực thể kinh doanh), UI có thể được truy cập bao gồm bản ghi cho bitmark cụ thể - UI bản ghi bitmark. Fig.4 thể hiện bản ghi bitmark mẫu 400 dựa trên bitmark 152 trên Fig.3C, mà có thể được truy cập bằng cách nhập mã ký tự chữ-số tương ứng với ID tài khoản bitmark, nghĩa là, khóa bí mật của người dùng như được mô tả trên đây hoặc, theo một số phương án, thao tác quét mã QR 402 cho bitmark 152. (Lưu ý rằng mã QR trên các hình vẽ chỉ là ví dụ minh họa.) UI hiển thị mã QR (nếu được sử dụng), tên của tài sản, phần mô tả 404 của tài sản dựa trên thông tin được đưa ra trong quá trình tạo ra bản ghi tài sản tương ứng 150, và ngày tháng và thời gian hiện thời. Tên và ngày tháng liệt kê trong bản ghi 400 bao gồm "nguồn gốc". Mỗi hàng 406 biểu diễn một lần chuyển giao. Các lần chuyển giao được minh họa tương ứng với các lần chuyển giao được thể hiện đối với bitmark 152 trên Fig.3C, với mỗi hàng thể hiện liên kết đến UI tài khoản tương ứng cho người dùng được nhận dạng, ví dụ, Dylan, Chloe, Amanda, có ngày tháng và dấu thời gian khi sự chuyển giao hợp lệ được hoàn tất. Nếu người dùng là chủ sở hữu hiện thời của bitmark, trong trường hợp này, Eva, nhấp chuột lên hoặc lướt chuột qua dòng đầu tiên sẽ hiện ra nút "chuyển giao" sẽ đưa Eva đến trang khác trong đó tên, số tài khoản hoặc thông tin nhận dạng khác có thể được nhập vào cho bên nhận chuyển giao, trong ví dụ này là Freddie. Fig.5 minh họa UI mẫu để khởi tạo chuyển giao.

Theo một số phương án của hệ thống, phí giao dịch có thể được tính khi ghi nhận mỗi lần chuyển giao. Phí giao dịch có thể được thanh toán bằng Bitcoin riêng hoặc tài khoản tiền điện tử khác boặc bằng tài khoản thẻ tín dụng/ghi nợ. Theo một phương án, ví bitcoin được nhúng cho mỗi tài khoản bitmark mới. Cùng khóa bí mật được sử dụng cho tài khoản bitmark có thể được sử dụng để tạo ra các tài khoản Bitcoin. Về mặt kỹ thuật, khóa bí mật được băm với một số khác (bộ đếm) để tạo ra các địa chỉ Bitcoin. Ví HD (phân cấp định hình) có thể được thực hiện cho mục đích này. Để chọn hình thức thanh toán phí giao dịch, người dùng có thể chọn nút "Bitcoin" hoặc nút "Tín dụng/Ghi nợ" trên trang, mà sẽ đưa họ đến màn hình thích hợp để nhập thông tin thanh toán của họ.

Một khi thanh toán đã được xác nhận, UI sẽ chuyển thông tin nhận dạng sang người được chuyển giao ("Freddie") đến danh sách nguồn gốc, biểu thị sự chuyển giao

là "Đang chờ" cho tới khi sự chuyển giao đã được xác thực. Sau khi xác thực chuyển giao, bản ghi bitmark 400, được thể hiện trên Fig.6, sẽ hiển thị nguồn gốc với chủ sở hữu hiện thời của bitmark, Freddie, ở trên cùng, cùng với ngày tháng và thời gian chuyển giao.

Các giao diện người dùng bổ sung có thể bao gồm lịch sử của các giao dịch bitmark, nghĩa là, UI giao dịch, với danh sách các giao dịch Bitmark đã diễn ra trong khoảng thời gian cho trước, nhận dạng các tài khoản (người dùng) đã khởi tạo giao dịch và loại giao dịch đã diễn ra, ví dụ, phát hành hoặc chuyển giao, cùng với trạng thái, ví dụ, "Đang chờ", hoặc, nếu được xác thực, ngày tháng và thời gian. UI điều hướng có thể bao gồm danh sách tìm kiếm được của các tài sản được ghi nhận trong hệ thống bitmark. Danh sách điển hình có thể bao gồm tên tài sản, người tạo ra tài sản, người đăng ký (người tạo ra bản ghi tài sản), Người phát hành (người tạo ra bản ghi phát hành) và số lượng bitmark được phát hành cho tài sản cụ thể đó. Với khả năng này, một cá nhân mong muốn mua một trong các tài sản được liệt kê có thể nhấp chuột vào tài sản để truy cập thông tin về (các) bitmark để cho phép họ chọn giữa các chủ sở hữu khác nhau nếu có nhiều bitmark, hoặc để cung cấp phương tiện để liên hệ với chủ sở hữu hiện thời để điều tra về hoạt động mua bán có thể có của tài sản. (Chủ sở hữu có thể chọn không chấp nhận các điều tra tự nguyện, trong trường hợp này người mua tiềm năng sẽ được yêu cầu tìm kiếm nguồn khác, nếu có.)

UI bản ghi tài khoản, có thể truy cập, ví dụ, bằng cách nhấp chuột vào tên người phát hành sau khi tìm kiếm tài sản cụ thể, có thể bao gồm thông tin liên hệ của người phát hành, các ID tài khoản bitmark và số lượng bitmark được kết hợp với người phát hành đó, và lịch sử giao dịch của người phát hành đó, nghĩa là, các hoạt động phát hành và các lần chuyển giao đang chờ và đã hoàn tất.

Ví dụ trên đây dựa trên tài sản số đó là cuốn sách điện tử được đưa ra chỉ nhằm mục đích minh họa. Như đã được biết đến bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật, phương pháp được mô tả ở đây có thể áp dụng được với tài sản bất kỳ, cho dù là tài sản số hay tài sản hiện vật. Tài sản số có thể bao gồm, nhưng không giới hạn ở tác phẩm văn học, ảnh, tài liệu, tác phẩm nghệ thuật, trò chơi video, phần mềm, nhạc, phim, hoặc tài sản khác được thể hiện dưới dạng số. Tài sản hiện vật sẽ được thảo luận thêm dưới đây.

Ví dụ 2 – Dữ liệu cá nhân dưới dạng các tài sản số

Vấn đề đang thu hút sự quan tâm ngày càng lớn bao gồm việc kiểm soát các tài sản số được kết hợp với dữ liệu cá nhân của một người, ví dụ, ảnh, video, âm nhạc hoặc tác phẩm văn học, mà có thể được đăng lên phương tiện truyền thông xã hội hoặc được lưu trữ trong các tập tin lưu trữ đám mây, dữ liệu được thu bởi các thiết bị giám sát đeo được ví dụ như vòng đeo tay sức khỏe, thiết bị theo dõi vận động, các thiết bị theo dõi nhịp tim, giấc ngủ và thiết bị theo dõi sức khỏe khác, thiết bị trong mạng internet kết nối vạn vật (Internet of Things, IoT), trong số nhiều thiết bị khác, được gọi chung là "dữ liệu cá nhân". Các phương pháp được bộc lộ ở đây có thể được sử dụng để tạo ra bitmark tương ứng với dữ liệu cá nhân của người dùng.

Theo một phương án kiểm soát dữ liệu cá nhân, người dùng có thể kết hợp các đặc trưng hiện đang khả dụng từ IFTTT (If This Then That) của San Francisco, CA, một dịch vụ cơ sở mạng tạo ra các chuỗi câu lệnh có điều kiện được gọi là "công thức". Các công thức này được kích hoạt dựa trên thay đổi cho các ứng dụng khác nhau, ví dụ, các trang truyền thông xã hội như Facebook, Gmail, Instagram, Twitter và Pinterest. Các công thức IFTTT kích hoạt hành động khi xảy ra một hành động kích hoạt cụ thể, ví dụ, ảnh của người dùng được gắn thẻ trong bài đăng Facebook, trong đó ảnh này tương ứng với dữ liệu cá nhân của người dùng. Việc xảy ra hành động kích hoạt đó dẫn đến hành động tạo ra bitmark cho dữ liệu cá nhân, tạo ra dấu vân tay, bản ghi tài sản và bản ghi phát hành cho dữ liệu cá nhân theo cùng cách như đã được mô tả ở trên với quản lý các tài sản số, để tạo ra bản ghi bất biến của dữ liệu, nguồn gốc và quyền sở hữu dữ liệu. Theo một phương án, hệ thống bitmark có trong một ứng dụng mà nhúng mã hóa để xóa hoặc soạn thảo dữ liệu cá nhân được sao chép hoặc được sử dụng theo cách khác mà không có sự ủy quyền. Việc mã hóa và/hoặc tạo ra bitmark cho dữ liệu cá nhân của người dùng cung cấp cho người tạo ra/người phát hành/chủ sở hữu sự kiểm soát đối với việc sử dụng tài sản của anh ấy hoặc cô ấy (dữ liệu), và cũng cung cấp một công cụ để tiền tệ hóa tài sản.

Ví dụ 3 – Nguồn gốc tài sản hiện vật

Dấu vân tay mà có thể được băm để tạo ra bản ghi tài sản có thể được tạo ra cho đối tượng vật lý bằng cách tạo ra dữ liệu số duy nhất cho tài sản hiện vật đó. Theo một số phương án, ký hiệu nhận dạng duy nhất được sử dụng cho tài sản hiện vật có thể là

hàm không thể nhân bản vật lý hay "PUF".

Nhiều phương pháp hiện có dùng để theo dõi các đối tượng vật lý bao gồm bước áp dụng mã vạch hoặc nhãn được mã hóa khác cho đối tượng, nhãn này có thể được gắn vào bằng chất kết dính hoặc đóng dấu, khắc hoặc trạm chổ lên bề mặt của đối tượng. Thông tin số tương ứng với mã vạch (hoặc mã khác) sau đó có thể được sử dụng để tạo ra bản ghi tài sản trong hệ thống bitmark để chuẩn bị cho việc tạo ra chuỗi quyền bất biến. Mặc dù điều này có thể thực tế đối với các mặt hàng tiêu dùng phổ thông, rải rộng khắp từ các sản phẩm tiêu dùng đến các thuốc kê đơn đến phương tiện cơ giới và các mặt hàng lớn hơn khác, nó lại không phù hợp với các tác phẩm nghệ thuật, các mặt hàng giá trị cao, độc đáo, bộ sưu tập hoặc các tài liệu gốc quan trọng khác có tầm quan trọng pháp lý, giá trị của chúng sẽ bị giảm bớt hoặc hủy hoại bởi việc gắn hoặc đóng dấu mã theo dõi lên đối tượng.

Theo một phương án của phương pháp bitmark, phương pháp quang trắc lập thể được sử dụng để trích xuất thông tin cấu trúc bề mặt cho một hoặc nhiều vùng quan tâm (regions of interest, ROI) của tài sản hiện vật. Một phương pháp có thể được sử dụng cho mục đích này được mô tả bởi R. J. Woodham ("Photometric method for determining surface orientation from multiple images", Optical Engineering, 1980, tài liệu này được kết hợp trong bản mô tả này bằng cách tham chiếu.) Cấu trúc bề mặt có thể là các nét cọ trong một bức tranh, các vùng được nâng lên hạ xuống trong tác phẩm điêu khắc hoặc trạm chổ, kiểu dệt hoặc thớ trên vải bạt hoặc giấy, hoặc đặc trưng vật lý khác bất kỳ mà là thành phần vĩnh viễn của tài sản hiện vật.

Theo phương án làm ví dụ được minh họa trên Fig.7A, thiết bị quang trắc lập thể 700 bao gồm các đèn LED 702 được đặt cách đều nhau xung quanh giá đỡ hình vành khuyên 704 được gắn trên thấu kính camera 706. Thấu kính có thể là thấu kính của camera chuyên dụng được dự định cho mục đích cụ thể đó là tạo ra các dấu vân tay số của đối tượng vật lý, hoặc nó có thể là thấu kính 708 của camera điện thoại thông minh như được thể hiện, ví dụ, iPhone, Android hoặc điện thoại thông minh hiện đại 710 khác có tính năng ảnh độ nét cao. Theo một phương án, bốn (4) đèn LED trắng 702 được gắn bên trong giá đỡ hình vành khuyên 704 ở các góc 0, 90, 180 và 270 độ theo cách sao cho mỗi đèn LED có thể được điều khiển độc lập để cho phép kích hoạt theo trình tự hoặc kích hoạt theo các tổ hợp khác nhau. (Lưu ý rằng chỉ ba trong bốn đèn LED 702 là có thể nhìn thấy trên hình vẽ do hình chiếu phối cảnh. Như đã biết, số

lượng đèn LED bất kỳ có thể được sử dụng miễn là có thể có nhiều góc chiếu sáng.) Dụng cụ để gắn các cấu kiện vào camera/điện thoại có thể là kẹp lò xo 716 như được thể hiện, móc, dụng cụ giữ khác, (tạm thời hoặc vĩnh viễn), hoặc có thể là vỏ máy mà điện thoại thông minh được lắp vào để tăng thêm tính ổn định. Để sử dụng, giá đỡ hình vành khuyên 704 được bố trí ổn định hướng xuống dưới về phía bề mặt đối tượng trên ROI. Giá đỡ cơ học bổ sung có thể được bố trí để đảm bảo giãn cách đều trong chuỗi chiếu sáng/chụp ảnh hoàn chỉnh trong đó đèn LED được kích hoạt lần lượt và các hình ảnh được thu cho mỗi góc chiếu sáng. Ví dụ, giá đỡ hình vành khuyên 704 có thể được tạo kết cấu để có hình dạng phẳng rộng ở trên cạnh của nó, ví dụ, cấu trúc dạng mặt bích có đường kính vài centimet, cho phép nó có thể nằm phẳng trên bề mặt để hỗ trợ tính ổn định tốt của điện thoại/camera.

Fig.7B minh họa thiết lập mẫu để tạo ra dấu vân tay cho bức tranh nổi tiếng của Van Gogh "The Starry Night" 720. ROI 750 nhỏ được tạo ảnh bằng cách sử dụng thiết bị quang trắc lập thể 700 và điện thoại thông minh 710 bằng cách kích hoạt lần lượt nhiều đèn LED để chiếu sáng ROI từ các góc khác nhau và thu nhiều ảnh, các ảnh này sau đó được kết hợp để tạo ra ảnh chuyển màu 754. Các điểm chính mẫu 756 được thể hiện trên các hình ảnh chuyển màu được mô tả dưới đây.

Các phương pháp được mô tả trong sáng chế trước đó, ví dụ, bởi Sharma, et al. ("Paperspeckle: microscopic fingerprinting of paper", *Proc. 18th ACM Conf. Comput. Comm. Secur.*, pp. 99-110, 2011) và Takahashi, et al. (FIBAR: Fingerprint Imaging by Binary Angular Reflection for Individual Identification of Metal Parts", *Proc. of Fifth International Conference on Emerging Security Technologies* (*EST '14*), 2014, pp. 46-51), chỉ chụp một ảnh từ ROI. Ngược lại, việc sử dụng các kỹ thuật quang trắc lập thể của phương pháp theo sáng chế tạo ra thông tin chi tiết về cấu trúc bề mặt, cho phép trích xuất các dấu vân tay duy nhất để xác minh.

Fig.8 minh họa bộ khung làm ví dụ để lấy dấu vân tay đối tượng theo một phương án của hệ thống và phương pháp theo sáng chế. Một khi ảnh chuyển màu tạo ra từ tổ hợp các ảnh được thu bằng cách chiếu sáng lần lượt và chụp hình ảnh ROI được suy ra, các điểm quan tâm cục bộ (nghĩa là, các điểm chính 756, các ví dụ được thể hiện trên Fig.7B) được nhận dạng và mô tả bằng cách sử dụng thuật toán thị giác máy ví dụ như FAST (E. Rosten et al. "Faster and better: a machine learning approach to corner detection", *IEEE Trans. Pattern Analysis and Machine Intelligence*

(*PAMI'10*), 32(1), 105-119, 2010, được kết hợp trong bản mô tả này bằng cách tham chiếu) hoặc FREAK (A. Alahi et al., "FREAK: Fast Retina Keypoint", In *Proc. of 2012 IEEE Conference on Computer Vision and Pattern Recognition (CVPR'12),* June 16-21, 2012, pp. 510-517, được kết hợp trong bản mô tả này bằng cách tham chiếu.)

Việc sử dụng phép chiếu ngẫu nhiên và hàm băm nhạy vị trí cho phép mã hóa các bộ mô tả được trích xuất và giảm kích thước đặc trưng. Do đó, chỉ thông tin nén sẽ cần được lưu trữ, xử lý và so khớp. Theo phương án ưu tiên cụ thể, thu được ít hơn 300 điểm chính đối với mỗi ROI, trong khi mỗi bộ mô tả chỉ cần 64 bit. Việc bổ sung vị trí của các điểm chính dẫn đến kích thước dấu vân tay cho ROI chỉ là khoảng 25K bit.

Trên Fig.8, ở bước 802, với mỗi ROI, bốn ảnh riêng biệt được chụp bằng cách sử dụng với ánh sáng từ bốn hướng ngang và dọc khác nhau (nghĩa là, 0, 90, 180 và 270 độ). Bằng cách sử dụng các kỹ thuật quang trắc lập thể, ảnh chuyển màu tạo thành có thể được suy ra để mô tả thông tin cấu trúc bề mặt. Ở bước 804, bộ dò điểm chính ví dụ như FAST được áp dụng cho hình ảnh để nhận dạng các điểm quan tâm cục bộ của ROI (ít hơn 300). Các điểm chính có thể bao gồm các đặc trưng riêng biệt ví dụ như các góc, cạnh, các vết xước và chỗ sai hỏng có thể có, v.v.. Bộ mô tả nhị phân sau đó được áp dụng cho các điểm quan tâm cục bộ để mô tả vùng quanh mỗi điểm chính dưới dạng một vectơ đặc trưng. Các bộ mô tả nhị phân, như được biết đến trong trường thị giác máy tính, được sử dụng để thu và mã hóa thông tin hình ảnh dưới dạng chuỗi nhị phân. Các bộ mô tả này có thể được tính toán rất nhanh và chuẩn bị cho việc áp dụng các số liệu ví dụ như khoảng cách Hamming với hoạt động XOR để xác minh, làm cho nó hiệu quả về mặt tính toán. Một số bộ mô tả nhị phân khác nhau được công bố công khai, bao gồm BRIEF, ORB, BRISK và FREAK. Nhằm phục vụ mục đích của phương án làm ví dụ, mỗi trong số các điểm quan tâm cục bộ được mô tả ở bước 806 bằng cách sử dụng bộ mô tả FREAK.

Ở bước 808, phép chiếu ngẫu nhiên được áp dụng trên mỗi bộ mô tả với hàm băm nhạy vị trí để giảm mỗi bộ mô tả về chuỗi nhị phân 64-bit. Việc thu các chuỗi nhị phân cho tất cả các bộ mô tả (810) và vị trí điểm chính (812) tạo thành tập hợp chi tiết nhỏ duy nhất biểu diễn dấu vân tay của đối tượng. Các dấu vân tay này có thể được lưu trong bộ sưu tập được giữ bởi chủ sở hữu của đối tượng để sử dụng cho lần xác thực sau này của đối tượng. Tốt hơn là, dấu vân tay sẽ được sử dụng để tạo ra bản ghi tài

sản cho việc tạo ra chuỗi bitmark mà qua đó nguồn gốc có thể được thiết lập. Để xác thực đối tượng tại thời điểm nào đó sau này bởi người mua tiềm năng, dấu vân tay được tạo ra cho hình ảnh đầu vào của đối tượng được thu bằng cách sử dụng thiết bị quang trắc lập thể được mô tả ở trên, ví dụ, ở bước 802, có thể được so sánh với dấu vân tay trong chuỗi bitmark.

Để đánh giá hiệu suất của quy trình xác minh, mười mẫu giấy mỹ thuật khác nhau có cùng nguyên liệu được sử dụng. Đối với mỗi loại giấy, ngoài giấy không chỉnh sửa được, hai quy trình làm giả khác nhau, chà và nhúng, được thực hiện trước khi thu được ảnh chuyển màu để làm cho tác vụ xác minh thực tế hơn nhưng khó hơn. Quy trình chà bao gồm bước chà rất mạnh giấy bằng tẩy, trong khi đó quy trình nhúng bao gồm bước nhúng giấy vào nước trong một giờ.

Với mỗi điều kiện (không bị làm giả, chà và nhúng) của mỗi mẫu giấy, hai hình ảnh chuyển màu được chụp cách nhau một khoảng thời gian. Do vậy, tổng số $10 \times 3 \times 2 = 60$ mẫu khả dụng để kiểm tra xác minh. Điều này tạo ra 360 cặp thật tương ứng với các tình trạng làm giả khác nhau của cùng mẫu giấy mỹ thuật, trong khi đó có thể thu được 3240 cặp giả. Để so với hiệu quả của các phương pháp hiện có, phương pháp đường cơ sở được xem xét bằng cách sử dụng chỉ một ảnh chụp (không chuyển màu) đối với ROI, với việc sử dụng cùng bộ mô tả để so khớp.

Fig.9A và 9B thể hiện sự phân bố tỷ lệ so khớp với các cặp thật và giả bằng cách sử dụng lần lượt phương pháp quang trắc lập thể và phương pháp đường cơ sở. Như đã nói trên, phương pháp theo sáng chế có thể phân biệt giữa các cặp thật và giả, trong khi đó phương pháp đường cơ sở không làm được như vậy. Fig.9C so sánh các đường cong ROC (nghĩa là, tỷ lệ khẳng định đúng (true positive rate, TPR) so với tỷ lệ báo động sai (false alarm rate, FAR)), xác nhận tính hiệu quả của phương pháp quang trắc lập thể. Cần lưu lý rằng, phương pháp theo sáng chế không đòi hỏi căn chỉnh chính xác khi trích xuất các dấu vân tay đối tượng. Điều này là do việc sử dụng bộ mô tả điểm chính mạnh mẽ. Một ưu điểm khác đó là, với các kỹ thuật LSH nêu trên, kích thước của các dấu vân tay được mã hóa chỉ khoảng 25K bit. Kết quả là, bộ khung theo sáng chế không chỉ có thể áp dụng cho các kiểm tra xác minh ngoại tuyến, mà còn ngăn chặn hoạt động giả mạo có thể có của đối tượng quan tâm bằng cách sử dụng các dấu vân tay được mã hóa.

Tạo ra dấu vân tay

Ví dụ 4 – Chức năng mạng

Phần thảo luận sau đây giả sử sự quen thuộc với các chuỗi khối Nakamoto. Thông tin cơ sở được công bố công khai trên mạng toàn cầu, trên Bitcoin wiki, mà được kết hợp trong bản mô tả này bằng cách tham chiếu.

Fig.10 minh họa chức năng mức cao của hệ thống bitmark, tạo ra và xử lý các giao dịch qua mạng ngang hàng (peer-to-peer, P2P) Bitmark 310. Khách hàng bitmark 200, bao gồm phần mềm để thực thi giao diện người dùng (UI) khách hàng, sử dụng giao thức cuộc gọi thủ tục từ xa (remote procedure call, RPC) 210 được sử dụng rộng rãi, ví dụ, JSON-RPC, để kết nối với máy chủ cổng của nút bitmark 304, được gọi là "bitmarkd", để khởi tạo giao dịch. Khách hàng bitmark 200 xử lý hoạt động tạo ra và lưu trữ chính, trong khi máy chủ bitmarkd đóng vai trò như người nghe JSON-RPC để đăng ký giao dịch khách hàng, tạo ra chuỗi khối và xác minh chữ ký. Hệ thống bitmark sử dụng giao thức nhị phân P2P tùy chỉnh cho chuỗi khối và phát rộng giao dịch. Nút bitmark đầy đủ 306 bao gồm người nghe JSON-RPC với các lệnh quản trị và người nghe giao thức Stratum 316 cho người khai thác 310. Dữ liệu được lưu trữ trong cơ sở dữ liệu LevelDB 312.

Khách hàng 200 kết nối với cổng RPC của bitmarkd 304 và gửi giao dịch dưới dạng yêu cầu JSON-RPC 210. Máy chủ bitmarkd xác minh chữ ký của giao dịch. Như đã được mô tả trên đây, các bản ghi tài sản và bản ghi phát hành được tự ký, trong khi đó bản ghi chuyển giao phải được ký bởi chủ sở hữu trước đó. Các chữ ký không hợp lệ và các bản ghi liên kết không chính xác bị loại bỏ. Các giao dịch hợp lệ được dồn lại dưới dạng các mục chưa thanh toán và được phát rộng đến các máy chủ khác trong mạng ngang hàng.

Đối với mỗi giao dịch chưa thanh toán, máy chủ bitmarkd sẽ trả lại ID giao dịch và mảng gồm các cặp thanh toán, ví dụ, tên đồng tiền và địa chỉ thanh toán, mà mạng sẽ chấp nhận như là khoản thanh toán để khai thác giao dịch ("phí".) Tiền dự phòng có thể được sử dụng để thanh toán cho nhiều giao dịch trong một lần thanh toán bằng cách gộp nhiều dữ liệu xuất và xác định các khoản phí cần thiết. Bằng cách sử dụng thông tin giao dịch được cung cấp bởi máy chủ bitmarkd, khách hàng hoàn tất giao dịch thanh toán và gửi nó đến bitmarkd để xác minh và chuyển tiếp. Theo một phương

án khác, khách hàng có thể thanh toán trực tiếp, và máy chủ bitmarkd sẽ giám sát tất cả tiền tệ mà nó hỗ trợ để xác định xem đã thực hiện thanh toán chưa. Máy chủ có thể chờ khoảng thời gian cố định, ví dụ, lên đến một giờ, để nhận được thanh toán trước khi làm hết hạn bản ghi. Khi thanh toán được xác nhận, thì (các) bản ghi có thể được khai thác.

Vẫn tham chiếu đến Fig.10, chuỗi khối bitmark có cấu trúc tương tự với chuỗi khối bitcoin. Theo một phương án, các chuỗi khối bitmark và bitcoin có thể dùng chung cùng thuật toán bằng chứng công việc. Theo các phương án khác, chuỗi khối bitmark có thể sử dụng thuật toán khác. Bất kể việc sử dụng công nghệ dùng chung, hệ thống bitmark thiết lập chuỗi khối của riêng nó, độc lập với bitcoin hoặc đồng tiền điện tử khác, do đó không có hạn chế rằng bitcoin được sử dụng làm tiền điện tử được kết hợp cho các giao dịch. Phần mô tả sau về sự tương tác với hệ thống bitcoin được đưa ra dưới dạng một trong các cơ chế có thể có để chuyển các khoản thanh toán và không được dự định để đề xuất rằng hệ thống bitmark phụ thuộc vào hệ thống tiền điện tử bitcoin.

Tiếp theo mô hình bitcoin, hoạt động khai thác được thực hiện để đảm bảo rằng tất cả những người tham gia có cái nhìn nhất quán về dữ liệu bitmark. Bởi vì bitmark là hệ thống ngang hàng phân tán, không có cơ sở dữ liệu trung tâm để theo dõi người sở hữu các bitmark. Thay vào đó, lược sử của tất cả các giao dịch được phân tán trên mạng ngang hàng. Các giao dịch bitmark nổi bật được khai thác thành một khối giao dịch để làm cho chúng trở nên chính thức. Các giao dịch xung đột hoặc không hợp lệ không được cho phép vào khối, do đó tránh được vấn đề chuyển giao bị trùng lặp.

Quy trình khai thác này là nằm ngoài máy chủ bitmarkd và sử dụng giao thức khai thác Stratum, như đã được biết đến trong lĩnh vực kỹ thuật này. Máy chủ bitmarkd tạo ra phần đầu bitcoin giả với giá trị băm bản ghi được nhúng cho phép phần mềm khai thác hiện tại (ví dụ, cgminer (Con Kolivas, “A multi-threaded multi-pool FPGA and ASIC miner for bitcoin”) để khai thác các khối bitmark như thể chúng là các khối bitcoin. Máy chủ tích lũy các giao dịch khả dụng thành một danh sách và tính toán cây Merkle một phần của bảng liệt kê giao dịch. (Cây Merkle một phần này thiếu bảng liệt kê ví coinbase.) Sự kiểm tra được thực hiện đối với các bản ghi phát hành để đảm bảo rằng bản ghi tài sản sẽ được bao gồm trước khi bản ghi phát hành (nghĩa là, tài sản liên quan hoặc là được khai thác trong khối trước đó hoặc được biết

đến bởi bitmarkd).

Ví coinbase một phần chứa số khối, dấu thời gian 64-bit, và địa chỉ thanh toán được tạo ra và được gửi cùng với cây Merkle một phần lên máy chủ Stratum 316. Các người khai thác 310 kết nối với các cổng Stratum để nhận dữ liệu này. Nếu người khai thác thành công, nó sẽ trả lại các giá trị số dùng một lần mà nó tìm thấy. Bitmarkd sau đó sẽ tạo ra phần đầu đầy đủ và ví coinbase cùng với cây Merkle đầy đủ và xác minh rằng bảng liệt kê ở trong độ khó hiện thời và cao hơn số khối hiện thời. Các khối đáp ứng cả hai điều kiện trên được kết hợp vào chuỗi khối hiện thời.

Ví coinbase bitmark tương thích với ví coinbase bitcoin và chứa một dữ liệu nhập và một hoặc nhiều dữ liệu xuất. Tập lệnh nhập chứa một chuỗi các thao tác dữ liệu đẩy được liệt kê dưới đây. Các tập lệnh nhập và xuất khiến cho ví coinbase không đóng vai trò như giao dịch Bitcoin thực bởi vì các tập lệnh chứa các thao tác OP_RETURN .

Dữ liệu được lưu trữ trong các giao dịch nhập và xuất được liệt kê trong bảng 1:

Bảng 1

Dữ liệu	**Mô tả**
Đầu vào	
Số khối	- 2..8 byte, đầu nhỏ (tối đa 64 bit)
Dấu thời gian	- 4..8 byte, Thanh toán đầu nhỏ (Thời gian Unix UTC tính theo giây lên đến 64 bit)
Số dùng một lần bổ sung	- 8..16 byte, để cho máy chủ Stratum và người khai thác sử dụng dữ liệu được lưu trữ trong mỗi đầu ra bao gồm tên tiền tệ và địa chỉ thanh toán
Đầu ra	
Tên đồng tiền	- 0..16 byte, tên đồng tiền ASCII chữ thường (ví dụ: “bit- coin”)
Địa chỉ thanh toán	- 0..64 byte, địa chỉ ASCII của người khai thác để nhận thanh toán (ví dụ: địa chỉ Bitcoin Base58) [mỗi đầu ra lưu trữ một cặp tên và địa chỉ để cho phép hỗ trợ nhiều loại tiền]

Khi máy chủ bitmarkd nhận được các giao dịch bổ sung, nó sẽ chỉ định một cách định kỳ công việc mới cho người khai thác và gửi lên máy chủ Stratum. Khối bitmark được giải đúng sẽ có tất cả các giao dịch được thiết lập về trạng thái được khai

thác, do đó loại bỏ chúng khỏi vùng chứa khả dụng. Máy chủ Stratum sau đó được thiết lập lại và tiếp tục làm việc với các giao dịch khả dụng còn lại.

Việc khai thác sẽ bị ngưng lại và máy chủ sẽ tiến vào chế độ khôi phục cho tới khi các vùng chứa giao dịch khả dụng đã được khôi phục hoàn toàn nếu điều kiện bất kỳ trong số các điều kiện sau đây xảy ra:

1. khối mới được tạo ra với một số cao hơn chuỗi khối hiện thời;

2. máy chủ đã ngoại tuyến trong một khoảng thời gian (hoặc vừa bỏ lỡ một số khối);

3. các nhánh chuỗi khối

Máy chủ khôi phục bằng cách xác định khối khả dụng cao nhất từ các khối lân cận và sau đó tìm nạp các khối theo thứ tự ngược, ghi đè các khối cũ hơn bất kỳ cho tới khi chuỗi khối của nó nhất quán với các chuỗi khối lân cận.

Một khi tất cả các khối đã được nhận và các giao dịch tương ứng của chúng đã được thiết lập là "được khai thác", hoạt động khai thác có thể được tiếp tục lại. Việc tìm nạp các giao dịch bị lỡ bất kỳ có thể là quy trình nền và sẽ không ảnh hưởng đến hoạt động khai thác hiện thời.

Có thể xác minh chủ sở hữu hiện thời của bitmark bất kỳ trong hệ thống mà không chạy nút mạng đầy đủ. Các máy chủ duy trì nội bộ bảng các chủ sở hữu hiện thời cho mỗi bitmark và do đó có thể xác minh các yêu cầu quyền sở hữu từ các khách hàng bằng câu hỏi tra cứu dễ dàng.

Phương pháp này có nhiều lỗ hổng. Trong số các vấn đề quan tâm, phương pháp này chỉ đáng tin cậy nếu các nút trung thực điều khiển mạng. Do đó, những người thực thi thường chuyển giao hoặc nhận bitmark nên chạy các nút đầy đủ của riêng họ. Việc chạy các nút cục bộ đầy đủ cũng tốt hơn cho bảo mật độc lập và xác minh nhanh hơn.

Sự khuyến khích khai thác được trả bằng phí giao dịch – có thể trả bằng các đồng tiền ví dụ như bitcoin hoặc tiền điện tử khác – và còn giúp ngăn chặn việc lạm dụng hệ thống. Phí giao dịch là chênh lệch giữa giá trị đầu ra của giao dịch thanh toán và giá trị đầu vào của nó.

Do thiết yếu, hệ thống công bố tất cả các giao dịch công khai. Tính riêng tư vẫn

có thể được duy trì bằng cách giữ các khóa công khai ẩn danh. Là sự phòng ngừa bổ sung, cặp khóa mới có thể được sử dụng cho mỗi giao dịch để ngăn chặn kết nối trở lại chủ sở hữu thông thường.

Các chủ sở hữu có thể mong muốn tiết lộ thông tin nhận dạng của họ trong hệ thống. Các tổ chức ví dụ như các bảo tàng thường muốn các tài sản của họ được biết đến. Hạ tầng khóa công khai (public key infrastructure, PKI) có thể được sử dụng bởi khách hàng để xác minh rằng khóa công khai cụ thể thuộc về thực thể nhất định .

Tiền giả định trước tài sản, trừ trường hợp trong đó hệ thống phi tập trung được mong muốn. Theo các phương pháp hiện tại, để tránh sự phụ thuộc vào hệ thống tập trung, một người cần tiền ngang hàng trước khi có thể chuyển giao tài sản mà không cần trung tâm có thẩm quyền trung gian. Tuy nhiên, không cần thiết được giới hạn ở việc sử dụng hệ thống tiền điện tử ngang hàng cụ thể khi cần chuyển giao tài sản. Rõ ràng là không phải tất cả các bên có thể quan tâm đến việc bán hoặc mua tài sản mong muốn bị giới hạn ở một loại hình thanh toán.

Phương pháp và hệ thống được mô tả ở đây đưa ra phương pháp miễn phí và đáng tin cậy để xây dựng hệ thống tài sản toàn cầu mà có thể được áp dụng bởi giao thức và sử dụng chuỗi khối Nakamoto để tạo ra nguồn gốc không làm giả được. Kiến trúc này dùng chung các khía cạnh kỹ thuật chính với Bitcoin để cho phép thanh toán phi tập trung và tăng cường các tài nguyên khai thác, trong khi vẫn độc lập với Bitcoin hoặc các hệ thống tiền điện tử khác.

Các Bitmark cung cấp tính minh bạch qua các chữ ký số theo cách có thể xác minh trên toàn thế giới, nhưng lại có thể thực thi cục bộ. Bởi vì hệ thống này không phân biệt giữa các tài sản (hiện vật hoặc số) hoặc các chủ sở hữu (cá nhân, tổ chức hoặc máy), quyền sở hữu có thể được mở rộng vượt xa các giới hạn của các hệ thống tài sản hiện thời.

Mặc dù phần mô tả trên đây đề cập đến nhiều chi tiết, các chi tiết này không được hiểu là các giới hạn đối với phạm vi sáng chế hoặc là những điều được yêu cầu bảo hộ, mà thay vào đó là các phần mô tả của các đặc trưng cụ thể đối với các phương án hoặc ví dụ cụ thể của sáng chế. Các đặc trưng nhất định được mô tả trong bản mô tả này trong ngữ cảnh các phương án hoặc ví dụ riêng cũng có thể được thực hiện kết hợp với nhau theo một phương án. Ngược lại, các đặc trưng khác nhau được mô tả

trong ngữ cảnh một phương án cũng có thể được thực hiện theo nhiều phương án riêng biệt hoặc theo tổ hợp con thích hợp bất kỳ. Hơn nữa, mặc dù các dấu hiệu có thể được mô tả trên đây khi đóng vai trò trong các tổ hợp nhất định và thậm chí được yêu cầu bảo hộ ban đầu như vậy, nhưng một hoặc nhiều đặc trưng từ một tổ hợp được yêu cầu bảo hộ có thể trong một số trường hợp có thể được thực hiện từ tổ hợp này và tổ hợp được yêu cầu bảo hộ có thể đề cập đến tổ hợp con hoặc biến thể của tổ hợp con.

YÊU CẦU BẢO HỘ

1. Phương pháp ghi nhận quyền sở hữu đối với tài sản, phương pháp này bao gồm các bước:

tạo ra bản ghi tài sản bằng cách sử dụng thiết bị tính toán có giao diện người dùng, bản ghi tài sản này bao gồm:

dấu vân tay bao gồm giá trị băm của phép biểu diễn số của tài sản,

khóa công khai của khách hàng tạo ra bản ghi tài sản, và

chữ ký số được tạo ra bởi khóa bí mật của khách hàng tạo ra; và

truyền thông với một hoặc nhiều nút trong mạng ngang hàng bằng cách sử dụng thiết bị tính toán và tạo ra mục nhập trong sổ cái công cộng bằng cách thực thi các bước sau:

tạo ra ít nhất một trong số bản ghi được phát hành bao gồm:

các chỉ số tài sản được thu lần lượt từ giá trị băm kép của dấu vân tay,

khóa công khai của khách hàng tạo ra, và

chữ ký của chủ sở hữu; và

ghi nhận ít nhất một bản ghi được phát hành trong sổ cái công cộng;

trong đó chữ ký của chủ sở hữu bao gồm cả các chỉ số tài sản, mà được ký bởi khóa bí mật của khách hàng tạo ra, và giá trị băm của khóa công khai của khách hàng tạo ra.

2. Phương pháp theo điểm 1, trong đó tài sản là tài sản số.

3. Phương pháp theo điểm 2, trong đó tài sản số được chọn từ nhóm bao gồm âm nhạc, video, sách điện tử, ảnh chụp kỹ thuật số, hình ảnh kỹ thuật số và dữ liệu cá nhân.

4. Phương pháp theo điểm 1, trong đó tài sản là tài sản hiện vật, phương pháp này còn bao gồm bước tạo ra dấu vân tay số tương ứng với tài sản hiện vật nhờ sử dụng ảnh cục bộ ở vùng quan tâm trên bề mặt của tài sản hiện vật.

5. Phương pháp theo điểm 4, trong đó ảnh cục bộ là hình ảnh quang trắc lập thể.

6. Phương pháp theo điểm 5, trong đó phương pháp này còn bao gồm các bước:

nhận dạng các điểm quan tâm cục bộ trong hình ảnh quang trắc lập thể bằng cách sử dụng bộ dò điểm chính, và

sử dụng thiết bị tính toán để mã hóa các điểm quan tâm cục bộ dưới dạng chuỗi nhị phân bằng cách sử dụng bộ mô tả nhị phân; trong đó chuỗi nhị phân bao gồm phép biểu diễn số của tài sản.

7. Phương pháp ghi nhận quyền sở hữu đối với tài sản, phương pháp này bao gồm các bước:

tạo ra bản ghi tài sản bằng cách sử dụng thiết bị tính toán có giao diện người dùng, bản ghi tài sản này bao gồm:

dấu vân tay bao gồm giá trị băm của phép biểu diễn số của tài sản,

khóa công khai của khách hàng tạo ra bản ghi tài sản, và

chữ ký số được tạo ra bởi khóa bí mật của khách hàng tạo ra; và

truyền thông với một hoặc nhiều nút trong mạng ngang hàng bằng cách sử dụng thiết bị tính toán và tạo ra mục nhập trong sổ cái công cộng bằng cách thực thi các bước sau:

tạo ra ít nhất một trong số bản ghi được phát hành bao gồm:

các chỉ số tài sản được thu lần lượt từ giá trị băm kép của dấu vân tay,

khóa công khai của khách hàng tạo ra, và

chữ ký của chủ sở hữu; và

ghi nhận ít nhất một bản ghi được phát hành trong sổ cái công cộng;

trong đó chữ ký của chủ sở hữu bao gồm cả các chỉ số tài sản, mà được ký bởi khóa bí mật của khách hàng tạo ra, và giá trị băm của khóa công khai của khách hàng tạo ra.

8. Phương pháp theo điểm 7, trong đó phương pháp này còn bao gồm, sau bước tạo ra bản ghi chuyển giao thứ nhất:

bước hiển thị yêu cầu thanh toán trên giao diện người dùng, và

bước xác định xem khoản thanh toán của người dùng đã được chuyển hay chưa

trước khi tiến hành bước thực thi.

9. Phương pháp theo điểm 7, trong đó giá trị băm kép của bản ghi được phát hành hoàn chỉnh bao gồm giá trị băm SHA-256 để tạo ra liên kết 32 byte.

10. Phương pháp theo điểm 7, trong đó phương pháp này còn bao gồm các bước:

tạo ra bản ghi chuyển giao tiếp theo để ghi nhận chuyển giao từ chủ sở hữu trước đó sang chủ sở hữu mới tiếp theo, bản ghi chuyển giao tiếp theo bao gồm cả giá trị băm kép của bản ghi chuyển giao trước đó và khóa công khai của chủ sở hữu mới tiếp theo, trong đó bản ghi chuyển giao tiếp theo được ký tên số bởi chủ sở hữu trước đó;

truyền thông bản ghi chuyển giao tiếp theo đến một hoặc nhiều nút trong mạng ngang hàng; và

bước thực thi, trong một hoặc nhiều nút, thuật toán chuỗi khối để tạo ra thỏa thuận phân tán về quyền sở hữu tài sản được kết hợp với chữ ký của chủ sở hữu, để xác nhận tính hợp lệ của bản ghi chuyển giao tiếp theo, và

nếu tính hợp lệ của bản ghi chuyển giao tiếp theo được xác nhận, thì ghi nhận bản ghi chuyển giao tiếp theo trong sổ cái công cộng, và

nếu tính hợp lệ của bản ghi chuyển giao tiếp theo không được xác nhận, thì loại bỏ bản ghi chuyển giao tiếp theo.

11. Phương pháp theo điểm 10, trong đó phương pháp này còn bao gồm, sau bước tạo ra bản ghi chuyển giao tiếp theo:

bước hiển thị yêu cầu thanh toán trên giao diện người dùng, và

bước xác định xem khoản thanh toán của người dùng đã được chuyển hay chưa trước khi tiến hành bước thực thi.

12. Phương pháp theo điểm 1, trong đó ít nhất một bản ghi được phát hành là nhiều bản ghi được phát hành, trong đó mỗi bản ghi được phát hành bao gồm một số dùng một lần khác nhau.

13. Phương pháp theo điểm 12, trong đó mỗi bản ghi được phát hành được kết hợp với chuỗi khối riêng.

14. Phương pháp theo điểm 1, trong đó giá trị băm kép của dấu vân tay bao gồm giá trị

băm SHA-512 để tạo ra bản ghi tài sản 64 byte.

15. Phương pháp theo điểm 1, trong đó thiết bị tính toán là máy tính để bàn hoặc máy tính xách tay được kết nối với mạng hoặc thiết bị di động.

16. Hệ thống ghi nhận quyền sở hữu đối với tài sản, hệ thống này bao gồm:

thiết bị tính toán khách có giao diện người dùng, thiết bị tính toán khách được tạo cấu hình để tạo ra bản ghi tài sản bao gồm:

dấu vân tay bao gồm giá trị băm của phép biểu diễn số của tài sản,

khóa công khai của khách hàng tạo ra bản ghi tài sản, và

chữ ký số được tạo ra bởi khóa bí mật của khách hàng tạo ra;

mạng ngang hàng bao gồm một hoặc nhiều nút ở trạng thái truyền thông với thiết bị tính toán khách để tạo ra mục nhập trong sổ cái công cộng bằng cách thực thi các bước sau:

tạo ra ít nhất một trong số bản ghi được phát hành bao gồm:

các chỉ số tài sản được thu lần lượt từ giá trị băm kép của dấu vân tay,

khóa công khai của khách hàng tạo ra, và

chữ ký của chủ sở hữu; và

ghi nhận ít nhất một trong số bản ghi được phát hành trong sổ cái công cộng;

trong đó chữ ký của chủ sở hữu bao gồm cả các chỉ số tài sản, mà được ký bởi khóa bí mật của khách hàng tạo ra, và giá trị băm của khóa công khai của khách hàng tạo ra.

17. Hệ thống theo điểm 16, trong đó tài sản là tài sản số.

18. Hệ thống theo điểm 17, trong đó tài sản số được chọn từ nhóm bao gồm âm nhạc, video, sách điện tử, ảnh chụp kỹ thuật số, hình ảnh kỹ thuật số và dữ liệu cá nhân.

19. Hệ thống theo điểm 16, trong đó tài sản là tài sản hiện vật, và trong đó thiết bị tính toán khách còn ở trạng thái truyền thông với thiết bị quang trắc lập thể được tạo cấu hình để tạo ra dấu vân tay số tương ứng với tài sản hiện vật nhờ sử dụng ảnh cục bộ ở

vùng quan tâm trên bề mặt của tài sản hiện vật.

20. Hệ thống theo điểm 19, trong đó thiết bị quang trắc lập thể được tạo cấu hình để:

nhận dạng các điểm quan tâm cục bộ trong hình ảnh quang trắc lập thể bằng cách sử dụng bộ dò điểm chính, và

mã hóa các điểm quan tâm cục bộ dưới dạng chuỗi nhị phân bằng cách sử dụng bộ mô tả nhị phân; trong đó chuỗi nhị phân bao gồm phép biểu diễn số của tài sản.

21. Hệ thống theo điểm 16, trong đó thiết bị tính toán khách và mạng ngang hàng còn được tạo cấu hình sao cho truyền thông để:

tạo ra bản ghi chuyển giao thứ nhất để ghi nhận chuyển giao tài sản cho chủ sở hữu mới, bản ghi chuyển giao bao gồm cả giá trị băm kép của bản ghi được phát hành hoàn chỉnh cho tài sản và khóa công khai của chủ sở hữu mới, trong đó bản ghi chuyển giao được ký tên số bằng chữ ký của chủ sở hữu,

xác nhận tính hợp lệ của bản ghi chuyển giao thứ nhất bằng cách sử dụng thuật toán chuỗi khối để tạo ra thỏa thuận phân tán về quyền sở hữu tài sản được kết hợp với chữ ký của chủ sở hữu, và

nếu tính hợp lệ của bản ghi chuyển giao thứ nhất được xác nhận, thì ghi nhận bản ghi chuyển giao trong sổ cái công cộng, và

nếu tính hợp lệ của bản ghi chuyển giao thứ nhất không được xác nhận, thì loại bỏ bản ghi chuyển giao.

22. Hệ thống theo điểm 21, trong đó thiết bị tính toán khách và mạng ngang hàng còn được tạo cấu hình để, sau khi tạo ra bản ghi chuyển giao thứ nhất:

hiển thị yêu cầu thanh toán trên giao diện người dùng, và

xác định xem khoản thanh toán của người dùng đã được chuyển hay chưa trước khi tiến hành bước thực thi.

23. Hệ thống theo điểm 21, trong đó giá trị băm kép của bản ghi được phát hành hoàn chỉnh bao gồm giá trị băm SHA-256 để tạo ra liên kết 32 byte.

24. Hệ thống theo điểm 21, trong đó hệ thống này còn bao gồm:

ít nhất một trong số thiết bị tính toán khách thứ hai ở trạng thái truyền thông với ít nhất một nút trong mạng ngang hàng để tạo ra bản ghi chuyển giao tiếp theo để ghi

nhận chuyển giao từ chủ sở hữu trước đó sang chủ sở hữu mới tiếp theo, bản ghi chuyển giao tiếp theo bao gồm cả giá trị băm kép của bản ghi chuyển giao trước đó và khóa công khai của chủ sở hữu mới tiếp theo, trong đó bản ghi chuyển giao tiếp theo được ký tên số bởi chủ sở hữu trước đó;

trong đó thiết bị tính toán đối với ít nhất một thiết bị tính toán khách thứ hai và mạng ngang hàng còn được tạo cấu hình để:

truyền thông bản ghi chuyển giao tiếp theo đến một hoặc nhiều nút trong mạng ngang hàng,

thực thi, trong một hoặc nhiều nút, thuật toán chuỗi khối để tạo ra thỏa thuận phân tán về quyền sở hữu tài sản được kết hợp với chữ ký của chủ sở hữu, để xác nhận tính hợp lệ của bản ghi chuyển giao tiếp theo, và

nếu tính hợp lệ của bản ghi chuyển giao tiếp theo được xác nhận, thì ghi nhận bản ghi chuyển giao tiếp theo trong sổ cái công cộng, và

nếu tính hợp lệ của bản ghi chuyển giao tiếp theo không được xác nhận, thì loại bỏ bản ghi chuyển giao tiếp theo.

25. Hệ thống theo điểm 24, trong đó thiết bị tính toán khách và mạng ngang hàng còn được tạo cấu hình để, sau khi tạo ra bản ghi chuyển giao tiếp theo:

hiển thị yêu cầu thanh toán trên giao diện người dùng, và

xác định xem khoản thanh toán của người dùng đã được chuyển hay chưa trước khi tiến hành bước thực thi.

26. Hệ thống theo điểm 24, trong đó ít nhất một thiết bị tính toán khách thứ hai là máy tính để bàn hoặc máy tính xách tay được kết nối với mạng hoặc thiết bị di động.

27. Hệ thống theo điểm 16, trong đó ít nhất một bản ghi được phát hành bao gồm nhiều bản ghi được phát hành, trong đó mỗi bản ghi được phát hành bao gồm một số dùng một lần khác nhau.

28. Hệ thống theo điểm 27, trong đó mỗi bản ghi được phát hành được kết hợp với chuỗi khối riêng.

29. Hệ thống theo điểm 16, trong đó giá trị băm kép của dấu vân tay bao gồm giá trị băm SHA-512 để tạo ra bản ghi tài sản 64 byte.

30. Hệ thống theo điểm 16, trong đó thiết bị tính toán khách là máy tính để bàn hoặc máy tính xách tay được kết nối với mạng hoặc thiết bị di động.

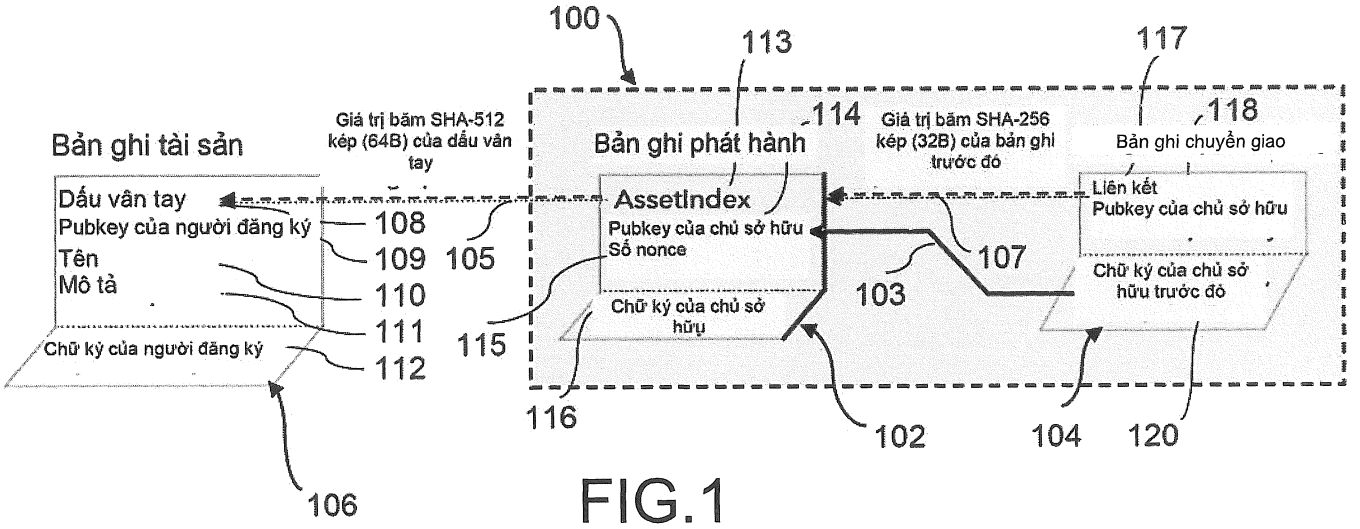

100
113
117
Bản ghi tài sản
Giá trị băm SHA-512 kép (64B) của dấu vân tay
Bản ghi phát hành
114
Giá trị băm SHA-256 kép (32B) của bản ghi trước đó
Bản ghi chuyển giao
118
Dấu vân tay
Pubkey của người đăng ký
Tên
Mô tả
Chữ ký của người đăng ký
108
109
110
111
112
105
AssetIndex
Pubkey của chủ sở hữu
Số nonce
Chữ ký của chủ sở hữu
115
116
107
103
Liên kết
Pubkey của chủ sở hữu
Chữ ký của chủ sở hữu trước đó
102
104
120
106

FIG.1

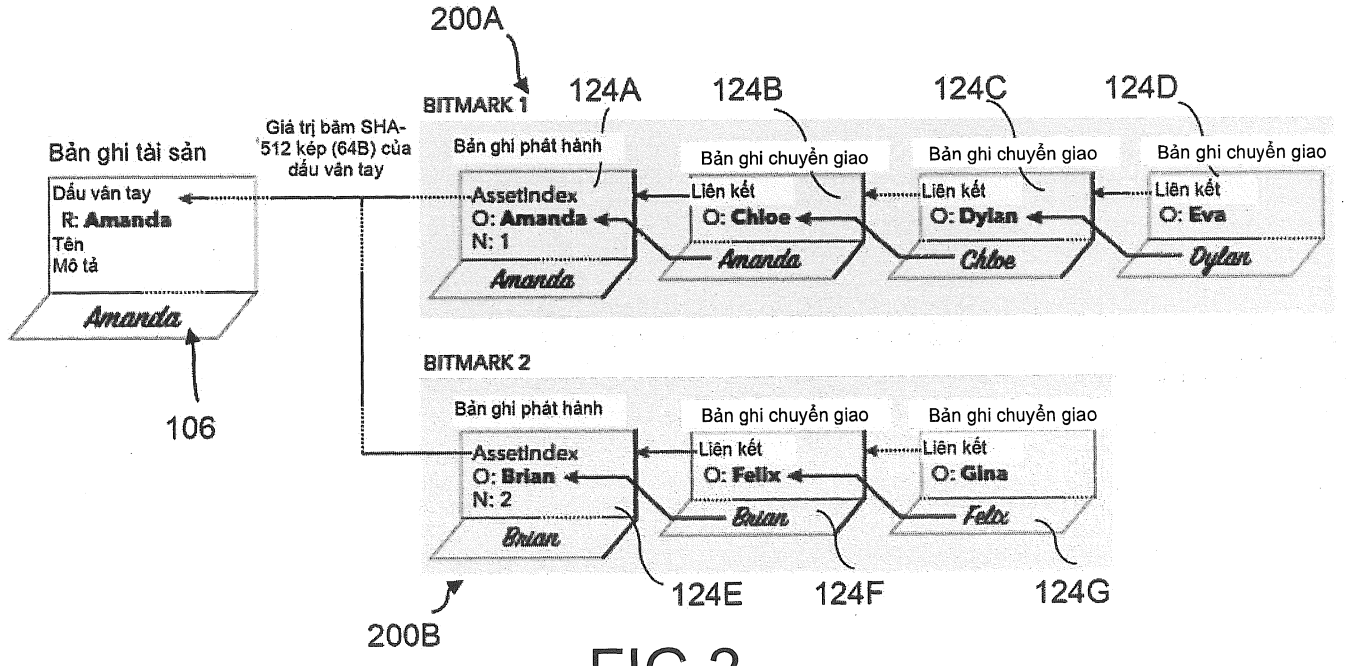

200A
BITMARK 1
124A
124B
124C
124D
Bản ghi tài sản
Giá trị băm SHA-512 kép (64B) của dấu vân tay
Bản ghi phát hành
Bản ghi chuyển giao
Bản ghi chuyển giao
Bản ghi chuyển giao
Dấu vân tay
R: Amanda
Tên
Mô tả
Amanda
AssetIndex
O: Amanda
N: 1
Liên kết
O: Chloe
Liên kết
O: Dylan
Liên kết
O: Eva
Chloe
Dylan
106
BITMARK 2
Bản ghi phát hành
Bản ghi chuyển giao
Bản ghi chuyển giao
AssetIndex
O: Brian
N: 2
Liên kết
O: Felix
Liên kết
O: Gina
Brian
Felix
200B
124E
124F
124G

FIG.2


Bản ghi tài sản 150
Dấu vân tay
R: Amanda
Tên: "Things Fell Apart"
Mô tả: Sách điện tử
Amanda

FIG.3A

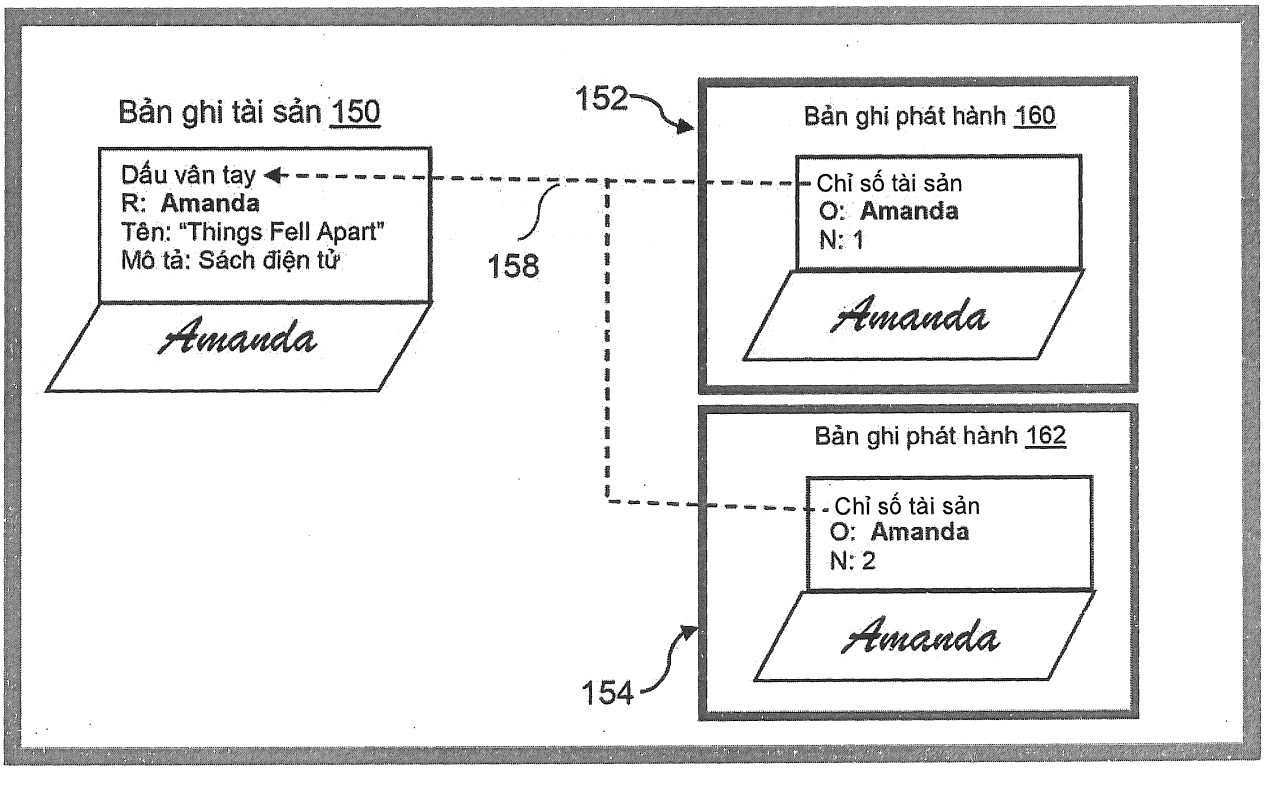

Bản ghi tài sản 150
Dấu vân tay
R: Amanda
Tên: "Things Fell Apart"
Mô tả: Sách điện tử
Amanda
158
152
Bản ghi phát hành 160
Chỉ số tài sản
O: Amanda
N: 1
Amanda
Bản ghi phát hành 162
Chỉ số tài sản
O: Amanda
N: 2
Amanda
154

FIG.3B

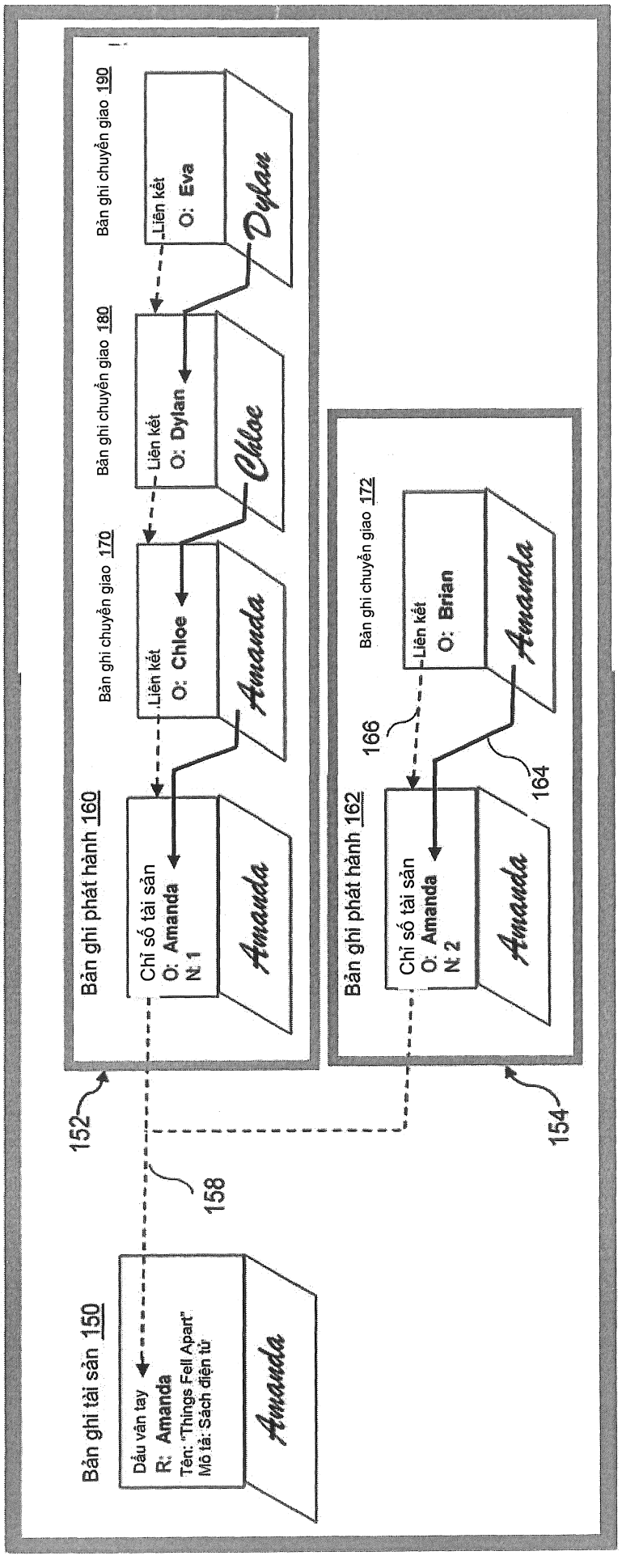

Bản ghi tài sản 150
Dấu vân tay
R: Amanda
Tên: "Things Fell Apart"
Mô tả: Sách điện tử
Amanda
158
152
Bản ghi phát hành 160
Chỉ số tài sản
O: Amanda
N: 1
Amanda
Bản ghi chuyển giao 170
Liên kết
O: Chloe
Amanda
Bản ghi chuyển giao 180
Liên kết
O: Dylan
Chloe
Bản ghi chuyển giao 190
Liên kết
O: Eva
Dylan
154
Bản ghi phát hành 162
Chỉ số tài sản
O: Amanda
N: 2
Amanda
166
164
Bản ghi chuyển giao 172
Liên kết
O: Brian
Amanda

FIG.3C

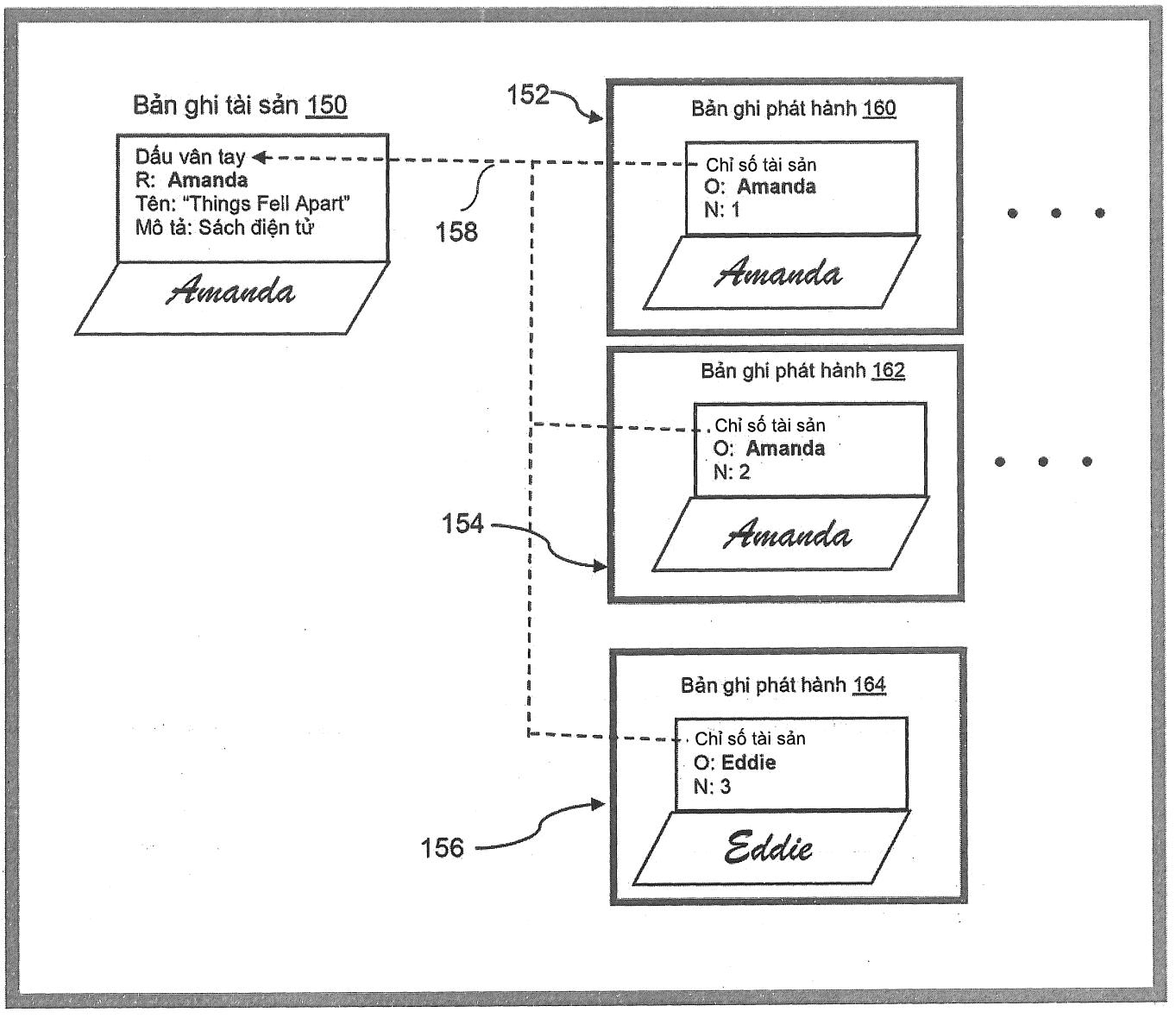

Bản ghi tài sản 150
Dấu vân tay
R: Amanda
Tên: "Things Fell Apart"
Mô tả: Sách điện tử
Amanda
158
152
Bản ghi phát hành 160
Chỉ số tài sản
O: Amanda
N: 1
Amanda
Bản ghi phát hành 162
Chỉ số tài sản
O: Amanda
N: 2
Amanda
154
Bản ghi phát hành 164
Chỉ số tài sản
O: Eddie
N: 3
Eddie
156

FIG.3D

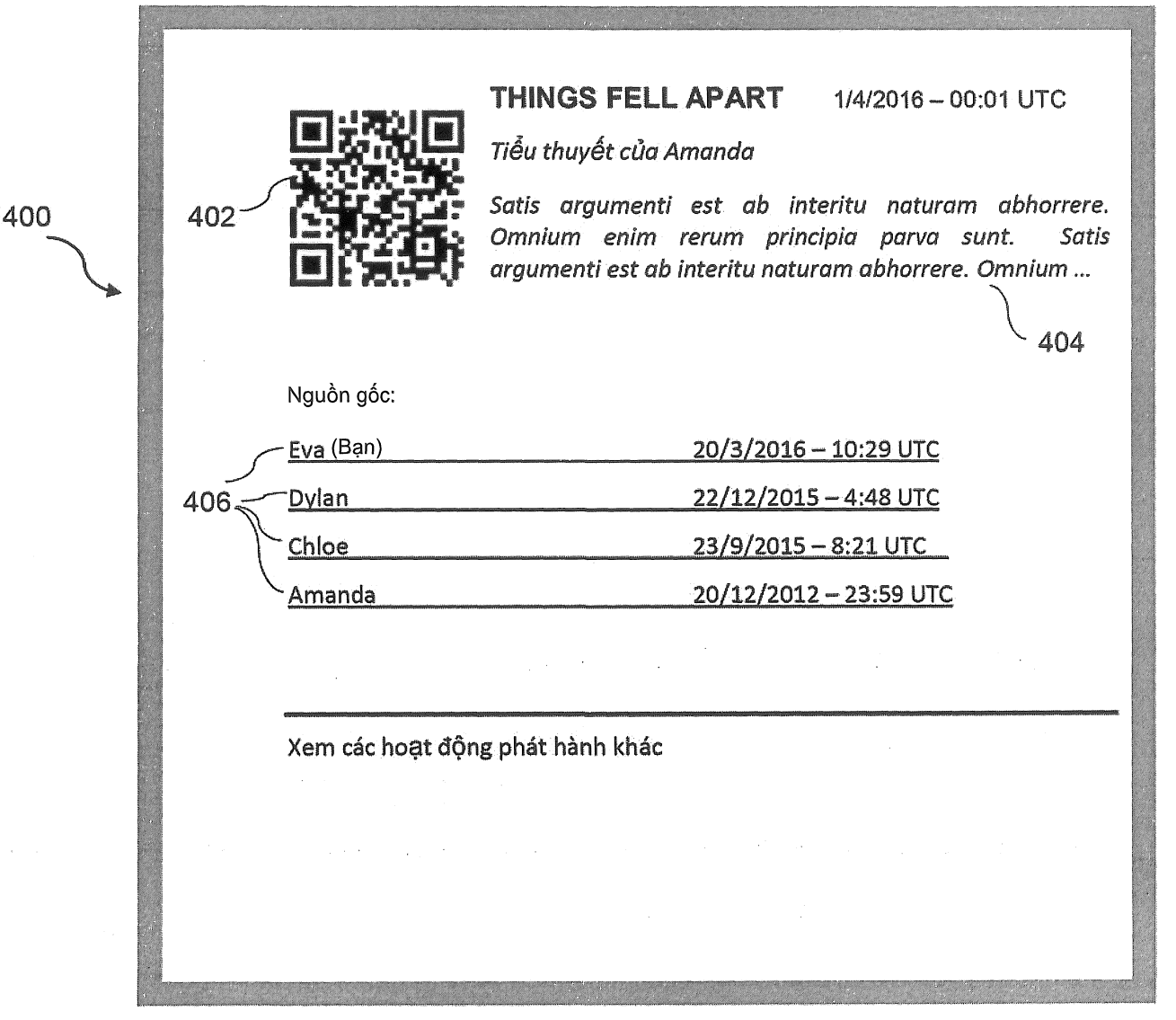

400
402
THINGS FELL APART
1/4/2016 – 00:01 UTC
Tiểu thuyết của Amanda
Satis argumenti est ab interitu naturam abhorrere. Omnium enim rerum principia parva sunt. Satis argumenti est ab interitu naturam abhorrere. Omnium ...
404
Nguồn gốc:
406
Eva (Bạn) 20/3/2016 – 10:29 UTC
Dylan 22/12/2015 – 4:48 UTC
Chloe 23/9/2015 – 8:21 UTC
Amanda 20/12/2012 – 23:59 UTC
Xem các hoạt động phát hành khác

FIG.4

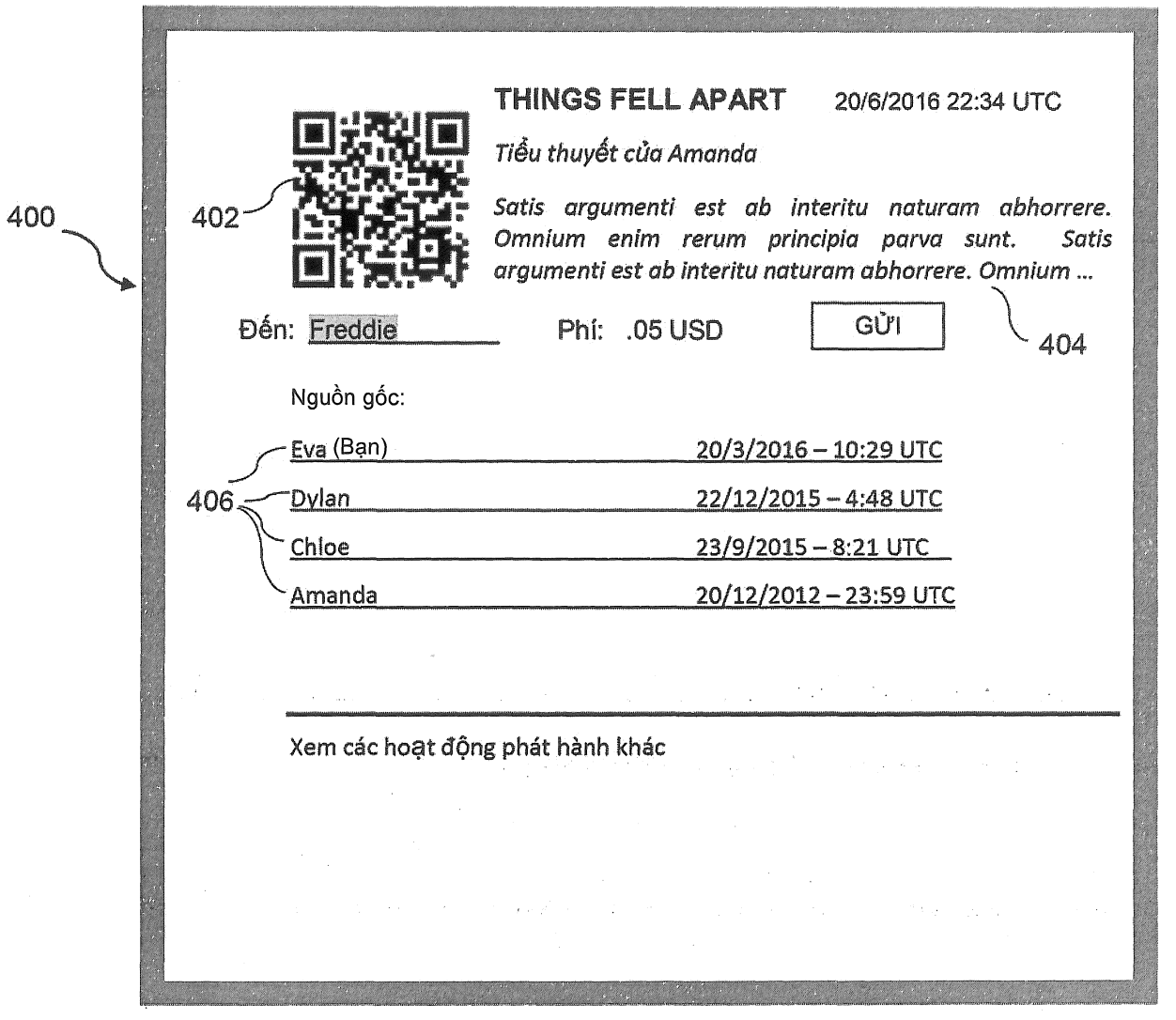

400
402
THINGS FELL APART
20/6/2016 22:34 UTC
Tiểu thuyết của Amanda
Satis argumenti est ab interitu naturam abhorrere. Omnium enim rerum principia parva sunt. Satis argumenti est ab interitu naturam abhorrere. Omnium ...
Đến: Freddie
Phí: .05 USD
GỬI
404
Nguồn gốc:
406
Eva (Bạn) 20/3/2016 – 10:29 UTC
Dylan 22/12/2015 – 4:48 UTC
Chloe 23/9/2015 – 8:21 UTC
Amanda 20/12/2012 – 23:59 UTC
Xem các hoạt động phát hành khác

FIG.5

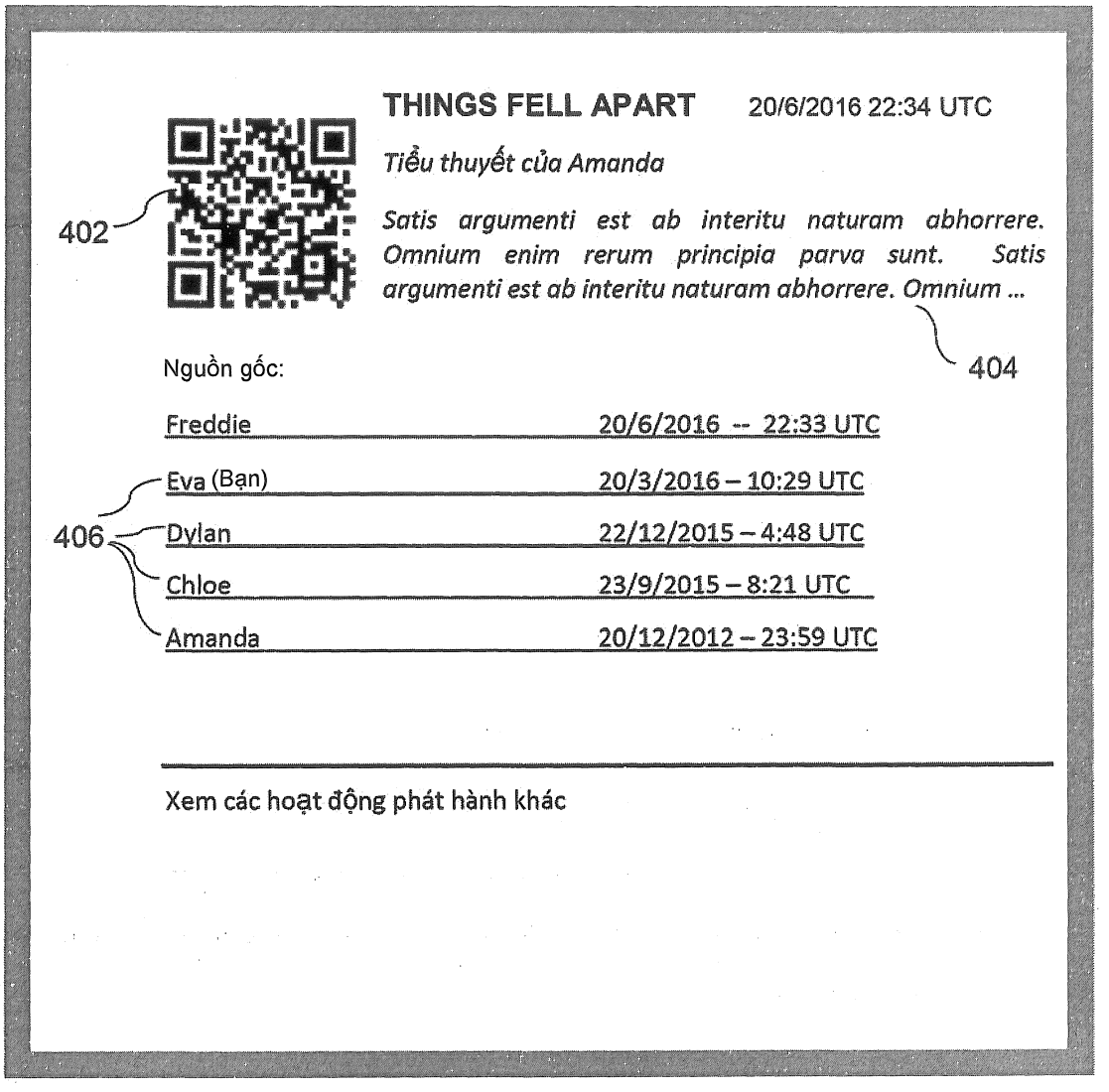

400
402
THINGS FELL APART
20/6/2016 22:34 UTC
Tiểu thuyết của Amanda
Satis argumenti est ab interitu naturam abhorrere. Omnium enim rerum principia parva sunt. Satis argumenti est ab interitu naturam abhorrere. Omnium ...
404
Nguồn gốc:
406
Freddie 20/6/2016 -- 22:33 UTC
Eva (Bạn) 20/3/2016 – 10:29 UTC
Dylan 22/12/2015 – 4:48 UTC
Chloe 23/9/2015 – 8:21 UTC
Amanda 20/12/2012 – 23:59 UTC
Xem các hoạt động phát hành khác

FIG.6

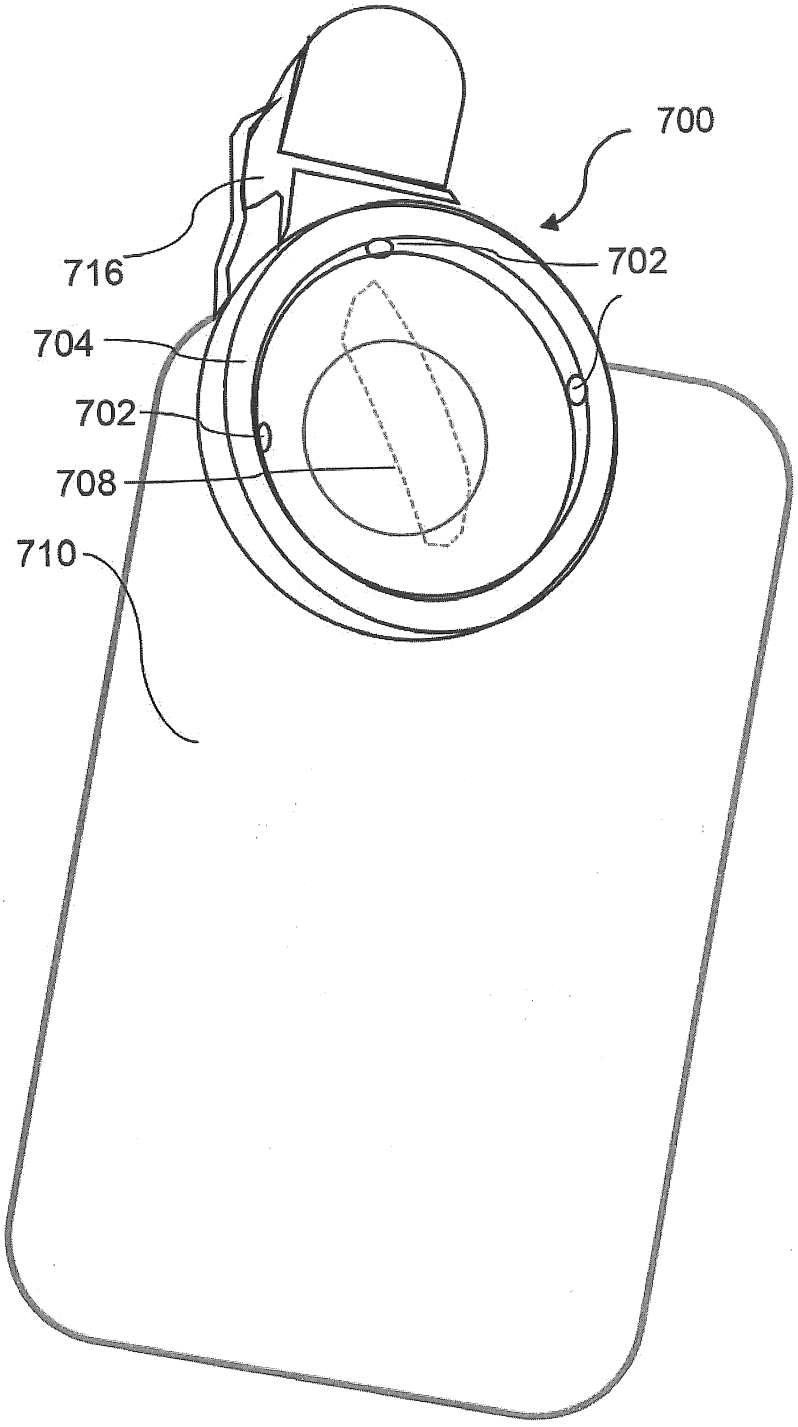


FIG.7A

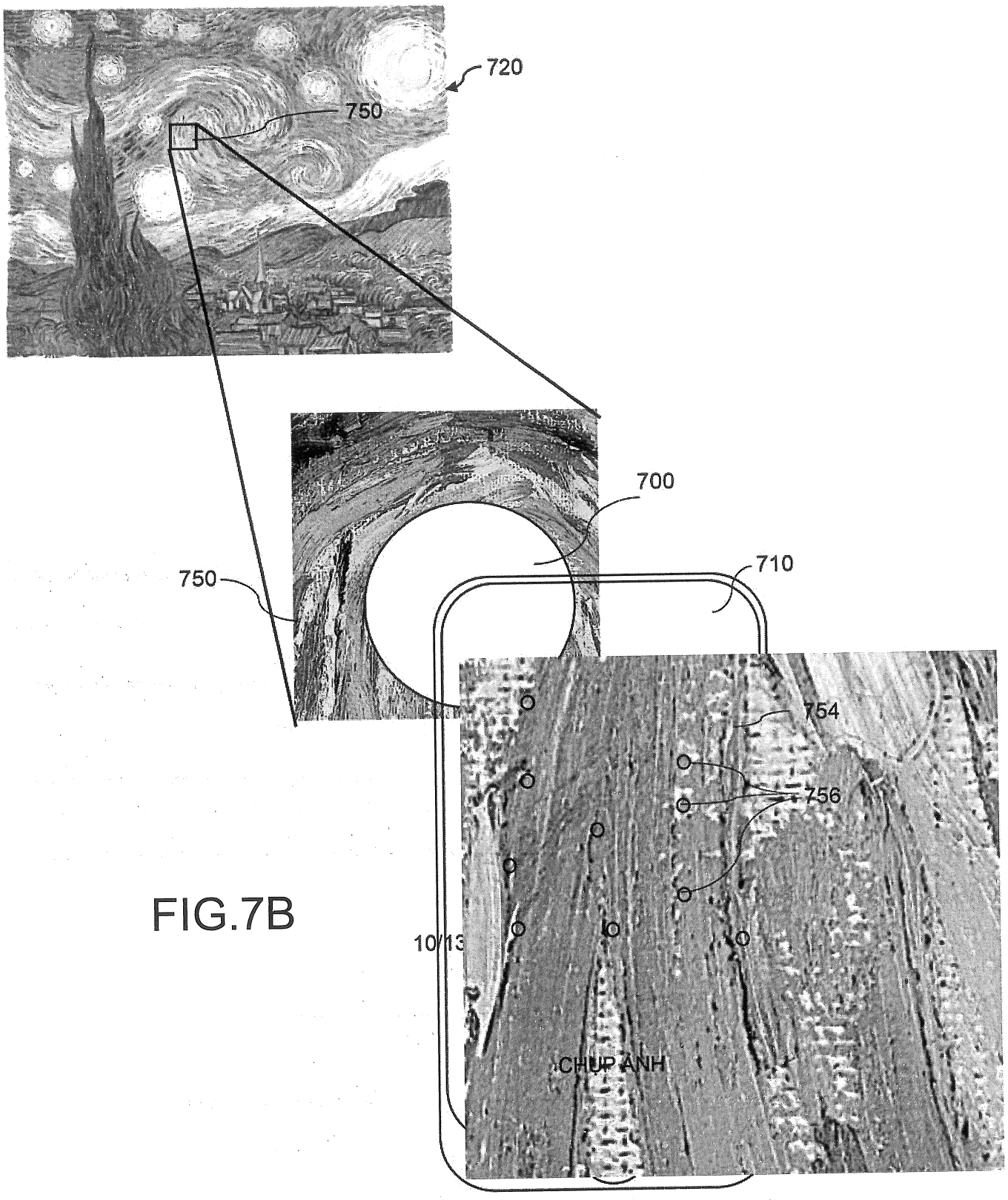


FIG.7B

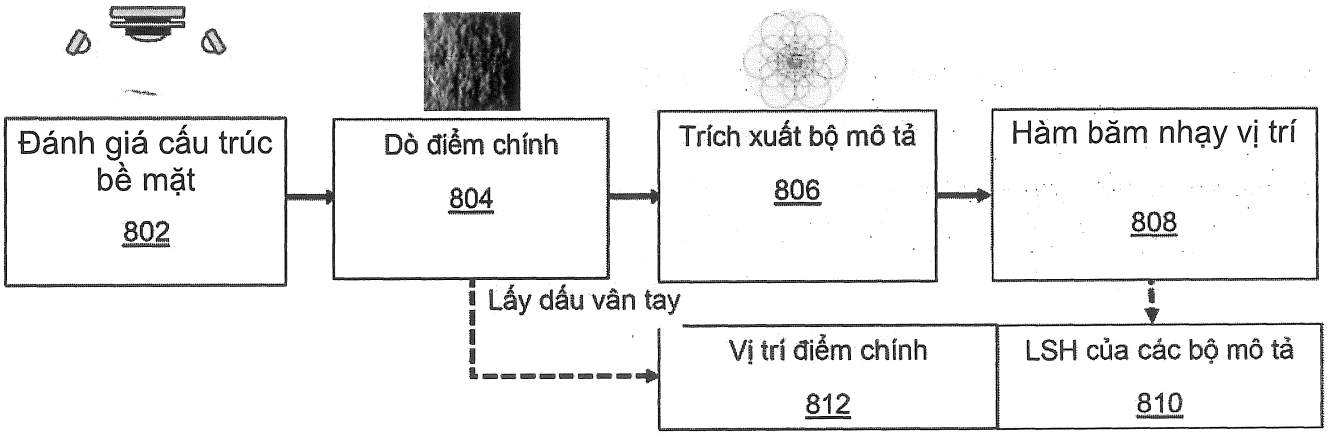

Đánh giá cấu trúc bề mặt
802
Dò điểm chính
804
Trích xuất bộ mô tả
806
Hàm băm nhạy vị trí
808
Lấy dấu vân tay
Vị trí điểm chính
812
LSH của các bộ mô tả
810

FIG.8

FIG.9A

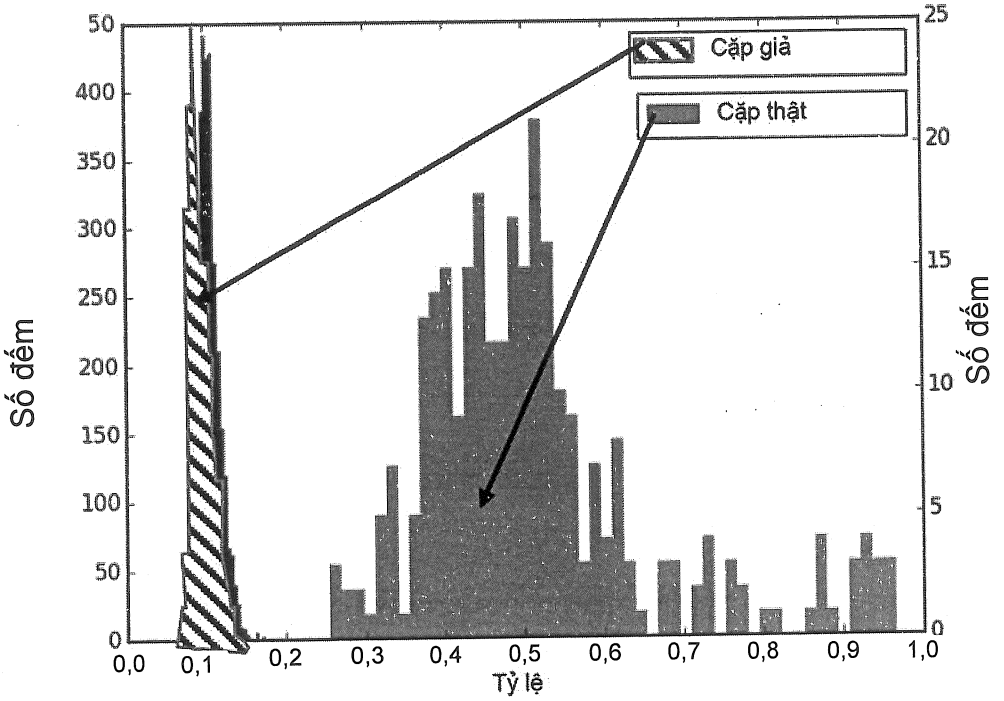


FIG.9A

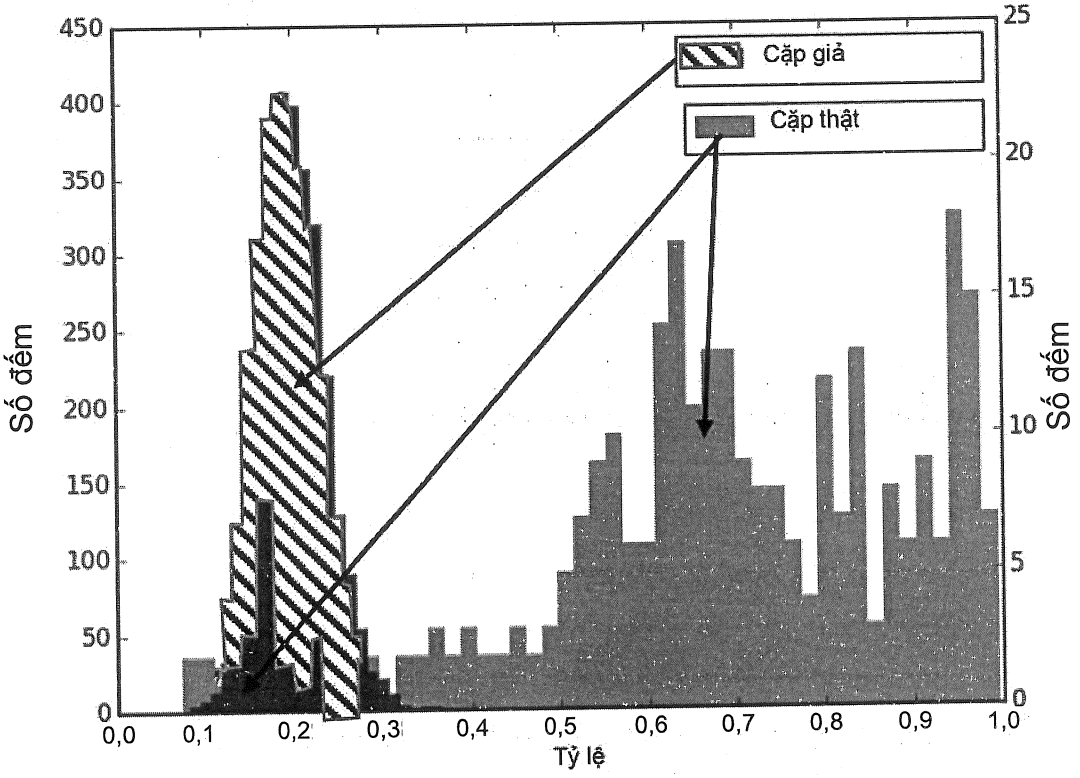


FIG.9B

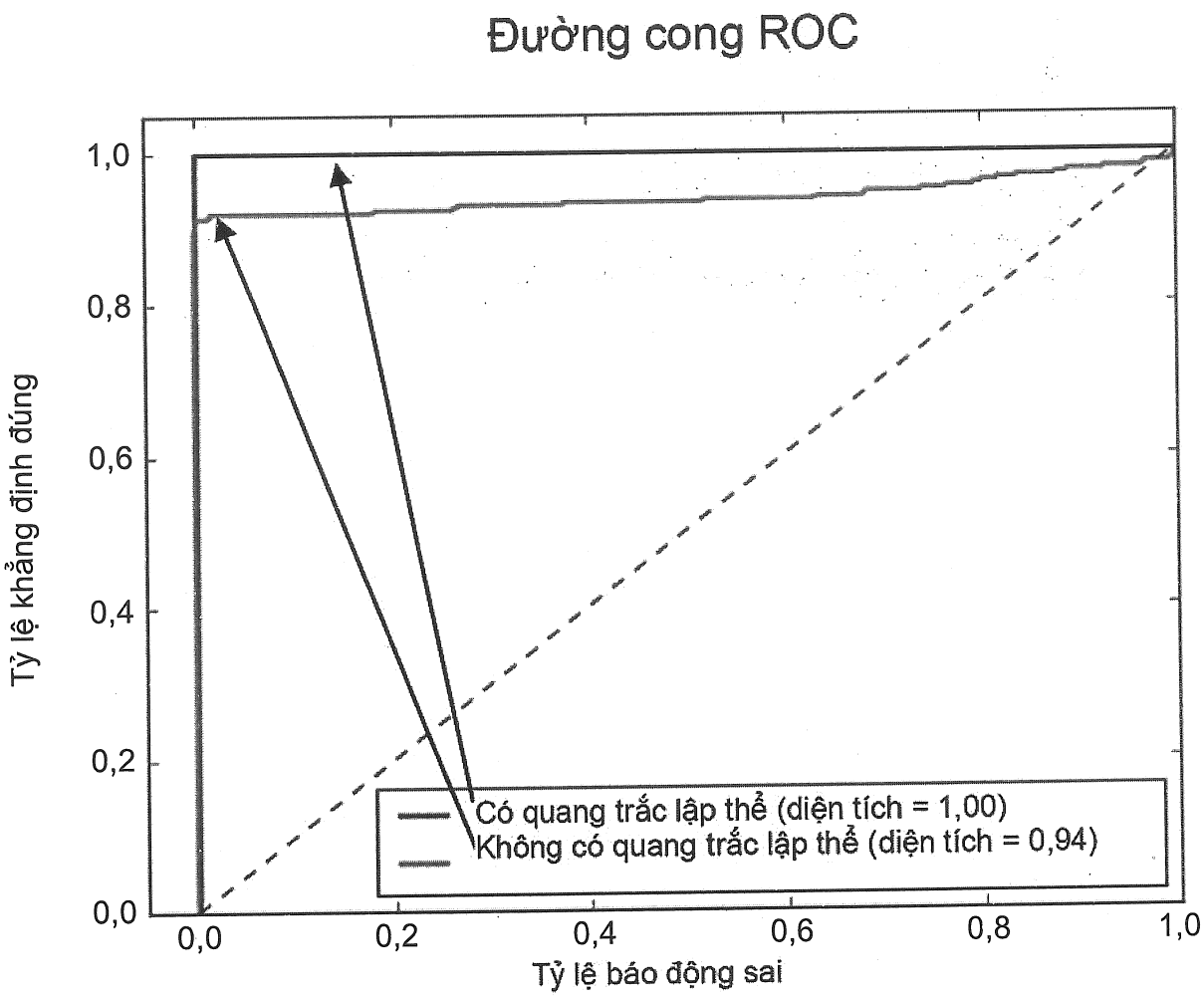

Đường cong ROC
Tỷ lệ khẳng định đúng
1,0
0,8
0,6
0,4
0,2
0,0
0,0
0,2
0,4
0,6
0,8
1,0
Tỷ lệ báo động sai
Có quang trắc lập thể (diện tích = 1,00)
Không có quang trắc lập thể (diện tích = 0,94)

FIG.9C

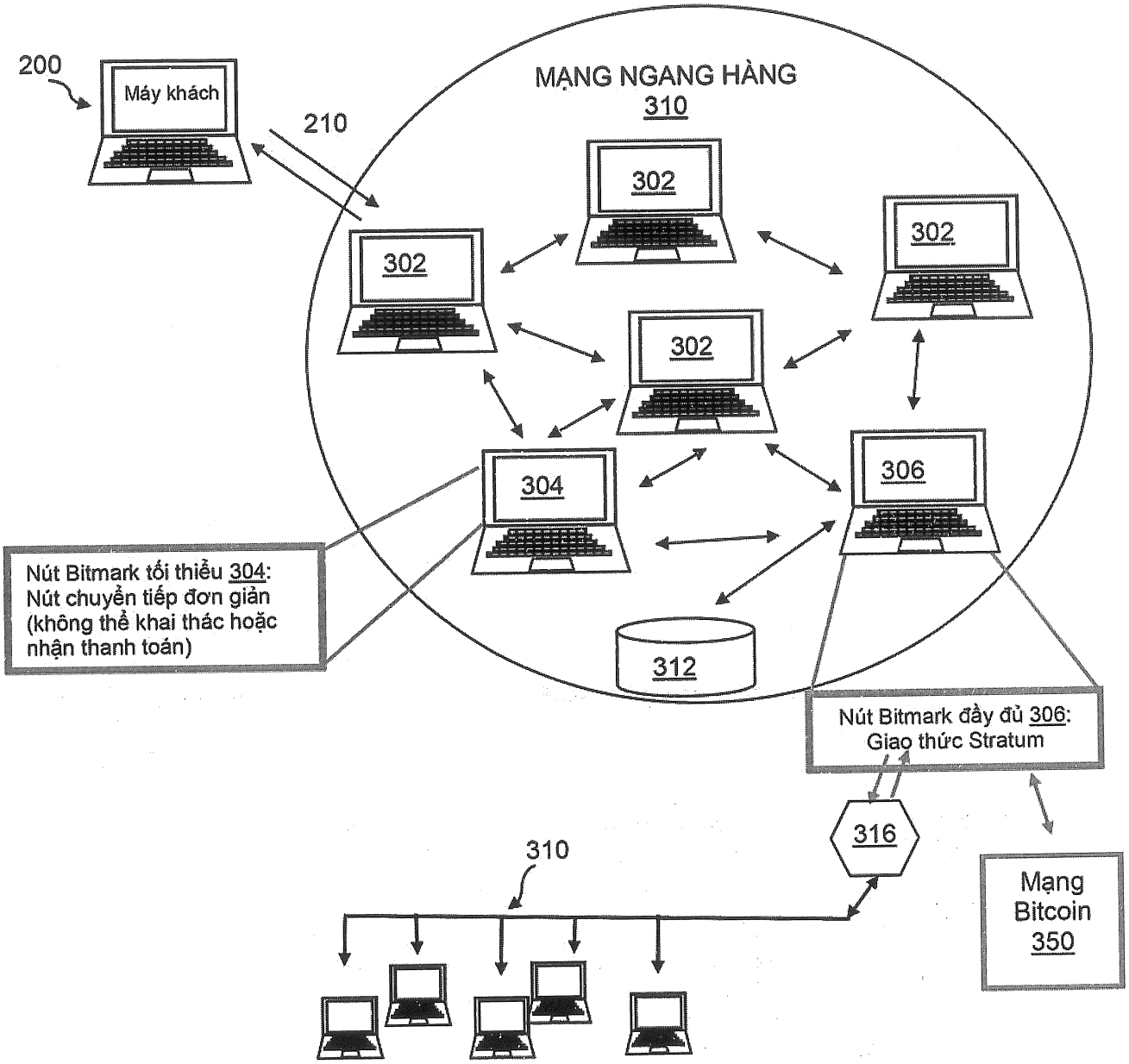

200
Máy khách
210
MẠNG NGANG HÀNG
310
302
302
302
302
304
306
312
Nút Bitmark tối thiểu 304:
Nút chuyển tiếp đơn giản
(không thể khai thác hoặc
nhận thanh toán)
Nút Bitmark đầy đủ 306:
Giao thức Stratum
316
310
Mạng
Bitcoin
350

FIG.10