(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) **1-0036805**

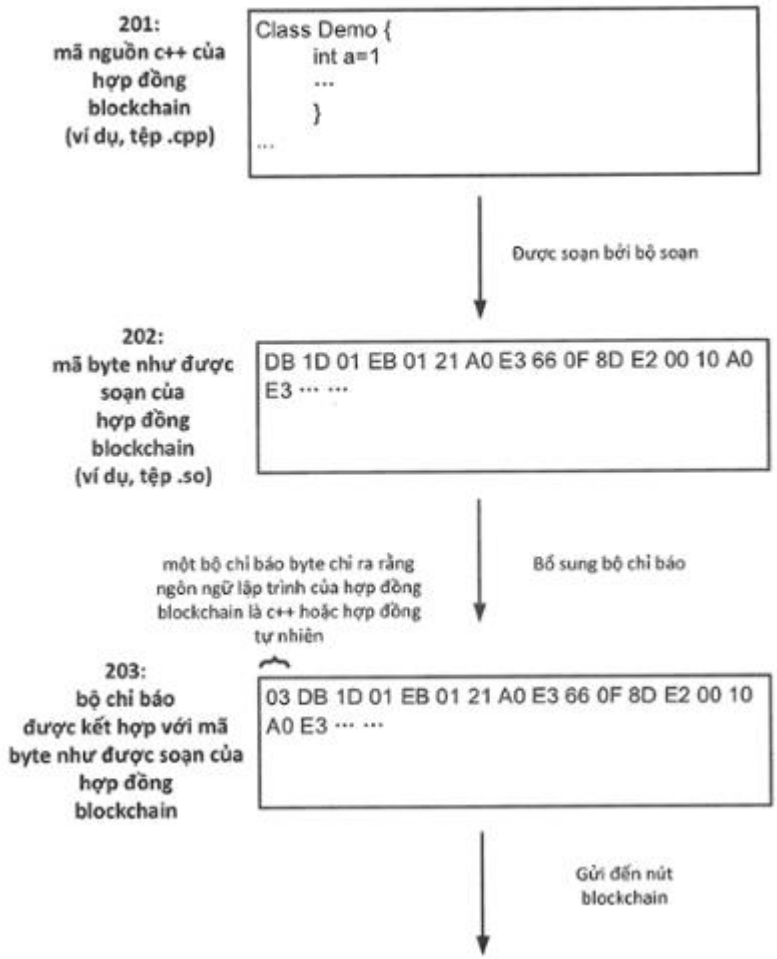
(51)[8] **G06Q 10/10**; H04L 9/32; H04L 9/06; G06Q 20/10; G06Q 30/00

(13) **B**

(21) 1-2019-02691
(22) 29/12/2018
(86) PCT/CN2018/125623 29/12/2018
(87) WO/2019/072310 18/04/2019
(45) 25/09/2023 426
(43) 26/08/2019 377A
(73) ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) SUN, He (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG ĐƯỢC THỰC HIỆN BỞI MÁY TÍNH ĐỂ THỰC HIỆN CÁC HỢP ĐỒNG BLOCKCHAIN, VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BỞI MÁY TÍNH KHÔNG CHUYỂN TIẾP

(57) Phương pháp được thực hiện bởi máy tính để thực hiện hợp đồng tự nhiên trên blockchain bao gồm các bước: thu nhận mã byte được kết hợp mà được liên kết với hợp đồng blockchain, trong đó mã byte được kết hợp bao gồm bộ chỉ báo biểu diễn kiểu hợp đồng blockchain; xác định kiểu hợp đồng blockchain ít nhất là dựa trên bộ chỉ báo; và thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định.


201:
mã nguồn c++ của hợp đồng blockchain (ví dụ, tệp .cpp)
Class Demo {
int a=1
...
}
...
Được soạn bởi bộ soạn
202:
mã byte như được soạn của hợp đồng blockchain (ví dụ, tệp .so)
DB 1D 01 EB 01 21 A0 E3 66 0F 8D E2 00 10 A0 E3 ··· ···
một bộ chỉ báo byte chỉ ra rằng ngôn ngữ lập trình của hợp đồng blockchain là c++ hoặc hợp đồng tự nhiên
Bổ sung bộ chỉ báo
203:
bộ chỉ báo được kết hợp với mã byte như được soạn của hợp đồng blockchain
03 DB 1D 01 EB 01 21 A0 E3 66 0F 8D E2 00 10 A0 E3 ··· ···
Gửi đến nút blockchain

Lĩnh vực kỹ thuật được đề cập

Nói chung, sáng chế đề cập đến các phương pháp và các thiết bị để thực hiện hợp đồng tự nhiên trên blockchain.

Tình trạng kỹ thuật của sáng chế

Công nghệ blockchain hứa hẹn sự lưu trữ dữ liệu theo kiểu phân tán. Dữ liệu có thể được lưu trữ theo chuỗi của các khối dữ liệu mà có mối quan hệ ưu tiên với nhau, mà tạo nên chuỗi các khối. Chuỗi các khối được duy trì bởi mạng gồm các nút, mà cũng có tác dụng phê chuẩn dữ liệu trước khi lưu trữ vào các khối. Với các công nghệ mật mã và đồng thuận được sử dụng bởi các nút, dữ liệu lưu trữ trong blockchain hầu như không thể thay đổi. Mạng gồm các nút còn được gọi là mạng đồng thuận blockchain. Hiện nay, công nghệ blockchain đã mở rộng để tạo ra khung cơ cấu để thực thi các hợp đồng blockchain (hoặc được gọi là các hợp đồng thông minh). Một hợp đồng blockchain là giao thức máy tính nhằm tạo điều kiện thuận lợi, xác minh hoặc đòi hỏi theo cách kỹ thuật số đàm phán hoặc thực hiện hợp đồng. Ví dụ, các hợp đồng blockchain cho phép thực hiện các giao dịch đáng tin mà không cần các bên thứ ba.

Các hợp đồng thông minh hiện tại hầu hết là các hợp đồng vững chắc chạy trên máy ảo Ethereum (Ethereum Virtual Machine, EVM), do chúng được yêu cầu được viết bằng ngôn ngữ chắc chắn. Các hợp đồng vững chắc là tập hợp của mã (các chức năng hợp đồng) và dữ liệu (trạng thái hợp đồng) mà khu trú ở địa chỉ cụ thể trên blockchain Ethereum. Một số các hợp đồng thông minh khác là các hợp đồng tự nhiên. Các hợp đồng tự nhiên có thể được viết bằng ngôn ngữ khác với ngôn ngữ vững chắc. Các hợp đồng tự nhiên không nên bị làm lẫn lộn với hợp đồng được soạn trước. Các hợp đồng được soạn trước là các chức năng có thể sử dụng lại mà chạy bên ngoài EVM mà có thể được loại bỏ khỏi EVM. Ví dụ, SHA256, RIPEMD160, và ECRECOVER được thực hiện là các hợp đồng được soạn trước. Các hợp đồng tự

nhiên cho phép nhà lập trình viết không xác định, thực thi không giới hạn, và viết mã thoát hộp cát. Đối với các hợp đồng tự nhiên, nhà phát triển không bị giới hạn bởi khí (phí thực thi cho mỗi hoạt động được tạo ra trên Ethereum) và sự giới hạn khí, và mã chạy nhanh hơn đáng kể so với trên EVM. Tuy nhiên, các hệ thống blockchain hiện tại yêu cầu các hợp đồng được viết chặt chẽ và thiếu hỗ trợ thích hợp để thực thi các hợp đồng tự nhiên.

Bản chất kỹ thuật của sáng chế

Các phương án của sáng chế đề cập đến các hệ thống, phương pháp và phương tiện đọc được bởi máy tính không chuyển tiếp để thực hiện hợp đồng tự nhiên trên blockchain.

Theo một khía cạnh, phương pháp được thực hiện bởi máy tính để thực hiện hợp đồng tự nhiên trên blockchain bao gồm các bước: thu nhận mã byte được kết hợp mà được liên kết với hợp đồng blockchain, trong đó mã byte được kết hợp bao gồm bộ chỉ báo biểu diễn kiểu hợp đồng blockchain; xác định kiểu hợp đồng blockchain ít nhất là dựa trên bộ chỉ báo; và thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định.

Theo một số phương án, mã byte được kết hợp bao gồm mã byte của tệp thư viện động được soạn từ mã nguồn của hợp đồng blockchain. Theo một ví dụ, mã nguồn là c++.

Theo một số phương án, bước xác định kiểu hợp đồng blockchain ít nhất là dựa trên bộ chỉ báo bao gồm việc: xác định nếu kiểu hợp đồng blockchain là hợp đồng tự nhiên.

Theo một số phương án, bước thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định bao gồm việc: để đáp lại việc xác định hợp đồng blockchain là hợp đồng tự nhiên, thì kích hoạt máy ảo blockchain để thực thi hợp đồng blockchain. Việc kích hoạt máy ảo để thực thi hợp đồng blockchain bao gồm việc: xác định máy ảo tương ứng với kiểu ít nhất là dựa trên bộ chỉ báo; và kích hoạt máy ảo được xác định để thực thi tệp thư viện động.

Theo một số phương án, bước thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định bao gồm việc: để đáp lại việc xác định hợp đồng

blockchain là hợp đồng tự nhiên, thì tạo ra quy trình con để thực thi hợp đồng blockchain. Việc tạo ra quy trình con để thực thi hợp đồng blockchain bao gồm các việc: tạo ra tệp có thể thực thi được; và sinh ra quy trình con để khởi chạy tệp có thể thực thi được để thực thi tệp thư viện động. Quy trình con và máy ảo blockchain truyền thông qua bộ nhớ cắm hoặc bộ nhớ dùng chung.

Theo một số phương án, bước thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định bao gồm việc: để đáp lại việc xác định hợp đồng blockchain là hợp đồng tự nhiên, thì khởi chạy bộ phận chứa biên bản lưu để thực thi hợp đồng blockchain. Việc khởi chạy bộ phận chứa biên bản lưu để thực thi hợp đồng blockchain bao gồm các việc: tạo ra bộ phận chứa biên bản lưu; và khởi chạy bộ phận chứa biên bản lưu để thực thi tệp thư viện động. Bộ phận chứa biên bản lưu và máy ảo blockchain truyền thông qua ổ cắm.

Theo khía cạnh khác, phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp được tạo cấu hình bởi các lệnh có thể thực thi được bởi một hoặc nhiều bộ xử lý để làm cho một hoặc nhiều bộ xử lý thi hành các hoạt động bao gồm các việc: thu nhận mã byte được kết hợp mà được liên kết với hợp đồng blockchain, trong đó mã byte được kết hợp bao gồm bộ chỉ báo biểu diễn kiểu hợp đồng blockchain; xác định kiểu hợp đồng blockchain ít nhất là dựa trên bộ chỉ báo; và thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định.

Theo khía cạnh khác, hệ thống để thực hiện hợp đồng tự nhiên trên blockchain bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ đọc được bởi máy tính không chuyển tiếp mà được ghép nối với một hoặc nhiều bộ xử lý và được tạo cấu hình bởi các lệnh có thể thực thi được bởi một hoặc nhiều bộ xử lý để làm cho hệ thống thi hành các hoạt động bao gồm các việc: thu nhận mã byte được kết hợp mà được liên kết với hợp đồng blockchain, trong đó mã byte được kết hợp bao gồm bộ chỉ báo biểu diễn kiểu hợp đồng blockchain; xác định kiểu hợp đồng blockchain ít nhất là dựa trên bộ chỉ báo; và thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định.

Các dấu hiệu này và các dấu hiệu khác của các hệ thống, phương pháp và phương tiện đọc được bởi máy tính không chuyển tiếp đã được mô tả ở đây, cũng như các phương pháp vận hành và các chức năng của các phần tử cấu trúc liên quan

và sự kết hợp của các phần, và tính kinh tế sản xuất, sẽ trở nên rõ ràng hơn khi xem xét phần mô tả sau đây và các điểm yêu cầu bảo hộ kèm theo với sự tham khảo đến các hình kèm theo, tất cả tạo thành một phần của bản mô tả, trong đó các số tham chiếu giống nhau chỉ các phần tương ứng trên các hình khác nhau. Tuy nhiên, cần hiểu rằng các hình đó chỉ nhằm mục đích minh hoạ và mô tả chứ không nhằm giới hạn sáng chế.

Mô tả vắn tắt các hình

Các dấu hiệu cụ thể của các phương án thực hiện khác nhau của công nghệ này được chỉ ra một cách cụ thể trong các yêu cầu bảo hộ kèm theo. Để hiểu rõ hơn, các dấu hiệu và các ưu điểm sẽ thu nhận nhờ việc tham khảo tới phần mô tả chi tiết các phương án thực hiện, trong đó các nguyên lý của sáng chế sẽ được sử dụng, và các hình kèm theo, trong đó:

Fig.1A là hình minh họa hệ thống làm ví dụ để thực hiện hợp đồng tự nhiên trên blockchain, theo các phương án thực hiện khác nhau;

Fig.1B là hình minh họa khung cơ sở làm ví dụ để thực hiện hợp đồng blockchain, theo các phương án thực hiện khác nhau;

Fig.2 là hình minh họa phương pháp làm ví dụ để bổ sung bộ chỉ báo, theo các phương án thực hiện khác nhau;

Fig.3A là hình minh họa phương pháp làm ví dụ để thực hiện hợp đồng tự nhiên trên blockchain, theo các phương án thực hiện khác nhau;

Fig.3B là hình minh họa phương pháp làm ví dụ để thực hiện hợp đồng tự nhiên trên blockchain, theo các phương án thực hiện khác nhau;

Fig.3C là hình minh họa phương pháp làm ví dụ để thực hiện hợp đồng tự nhiên trên blockchain, theo các phương án thực hiện khác nhau;

Fig.4 là hình minh họa lưu đồ của phương pháp làm ví dụ để thực hiện hợp đồng tự nhiên trên blockchain, theo các phương án thực hiện khác nhau;

Fig.5 là hình minh họa sơ đồ khối của hệ thống máy tính làm ví dụ để thực hiện hợp đồng tự nhiên trên blockchain, theo các phương án thực hiện khác nhau; và

Fig.6 là hình minh họa sơ đồ khối của hệ thống máy tính làm ví dụ trong đó phương án thực hiện bất kỳ trong số các phương án thực hiện đã được mô tả ở đây có thể được thực hiện.

Mô tả chi tiết sáng chế

Blockchain có thể được xem là cơ sở dữ liệu phân tán, thường được gọi là sổ cái phân bố (trong kế toán) do sự hoạt động được thi hành bởi các nút khác nhau (ví dụ, các thiết bị điện toán) trong mạng ngang hàng (Peer-to-Peer, P2P). Thông tin bất kỳ có thể được ghi vào blockchain và được lưu hoặc đọc từ đó. Các nút là, ví dụ, các thiết bị điện toán hoặc các hệ thống máy tính lớn để hỗ trợ mạng blockchain và giữ nó hoạt động trơn tru. Mỗi nút có thể tạo ra một phần hoặc tất cả các chức năng của blockchain. Ví dụ, nút mà cung cấp sự xác minh đồng thuận có thể được gọi là nút tham gia đồng thuận (hoặc nút đồng thuận).

Fig.1A thể hiện hệ thống làm ví dụ 100 để thi hành các bước và các phương pháp đã được bộc lộ khác nhau, theo các phương án thực hiện khác nhau. Như được thể hiện trên hình, mạng blockchain có thể bao gồm các nút blockchain (ví dụ, nút 1, nút 2, nút 3, nút 4, nút i, v.v.). Các nút blockchain có thể tạo ra mạng (ví dụ, mạng ngang hàng) với một nút blockchain truyền thông với nhau. Thứ tự và số lượng của các nút blockchain được thể hiện trên hình chỉ để làm ví dụ và để đơn giản hóa sự minh họa. Các nút blockchain có thể được thực hiện trên các máy chủ, các máy tính, v.v. Mỗi nút blockchain có thể tương ứng với một hoặc nhiều linh kiện phần cứng vật lý hoặc các thiết bị ảo ghép nối với nhau thông qua các kiểu phương pháp truyền thông khác nhau như TCP/IP. Tùy thuộc vào các phân loại, các nút blockchain có thể bao gồm các nút đầy đủ, các nút Geth, các nút đồng thuận, v.v.

Theo các phương án thực hiện khác nhau, người dùng A và người dùng B có thể sử dụng các thiết bị tương ứng như các máy tính xách tay và điện thoại di động để kích hoạt các nút blockchain để thực thi các giao dịch, mà có thể được tiến hành bởi các hợp đồng blockchain (ví dụ, các hợp đồng thông minh). Ví dụ, người dùng A có thể muốn giao dịch với người dùng B bằng cách chuyển một số tài sản trong tài khoản của người dùng A cho tài khoản của người dùng B. Người dùng A và người dùng B có thể sử dụng các thiết bị tương ứng được cài đặt bởi phần mềm blockchain

thích hợp (ví dụ, ví tiền điện tử) cho giao dịch. Thiết bị của người dùng A có thể được gọi là nút khởi tạo A để khởi tạo giao dịch với thiết bị của người dùng B được gọi là nút tiếp nhận B. Nút A có thể truy cập blockchain nhờ truyền thông với nút 1, và nút B có thể truy cập blockchain nhờ truyền thông với nút 2. Ví dụ, nút A và nút B có thể gửi các giao dịch cho blockchain thông qua nút 1 và nút 2 để yêu cầu bổ sung các giao dịch cho blockchain. Ngoài blockchain, nút A và nút B có thể có các kênh truyền thông khác (ví dụ, truyền thông Internet thông thường mà không đi qua các nút 1 và 2). Theo một số phương án, phần mềm blockchain trên nút A có thể được xem là đầu trước của nút blockchain 1, và nút blockchain 1 chạy đầu sau của phần mềm blockchain.

Mỗi nút trong số các nút trên Fig.1A có thể bao gồm bộ xử lý và phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp được tạo cấu hình bởi các lệnh có thể thực thi được bởi bộ xử lý khiến cho nút thi hành các bước khác nhau để thực hiện hợp đồng tự nhiên trên blockchain đã được mô tả ở đây. Mỗi nút có thể được cài đặt bởi phần mềm (ví dụ, chương trình giao dịch) và/hoặc phần cứng (ví dụ, các kết nối có dây, không dây) để truyền thông với các nút và/hoặc thiết bị khác. Ví dụ, các thiết bị người dùng như nút A và nút B có thể được cài đặt bởi phần mềm đầu cuối người dùng như ví tiền điện tử, và các nút blockchain có thể được cài đặt bởi phần mềm xử lý giao dịch blockchain. Các chi tiết khác của nút phần cứng và phần mềm được mô tả sau với sự tham khảo đến Fig.5 và Fig.6.

Các nút blockchain mỗi nút có thể bao gồm hoặc được ghép nối với bộ nhớ. Theo một số phương án, bộ nhớ có thể lưu trữ cơ sở dữ liệu vùng. Cơ sở dữ liệu vùng có thể được truy nhập vào các nút blockchain theo cách được phân bố. Ví dụ, cơ sở dữ liệu vùng có thể được lưu trữ một cách tương ứng trong các bộ nhớ của các nút blockchain. Cơ sở dữ liệu vùng có thể lưu trữ các giao dịch mà được gửi bởi một hoặc nhiều thiết bị người dùng như nút A mà được vận hành bởi người dùng. Theo một số phương án đối với hệ thống Ethereum, sau khi nhận yêu cầu giao dịch của giao dịch chưa xác nhận, thì nút blockchain tiếp nhận có thể thi hành một số xác minh sơ bộ của giao dịch. Ví dụ, với sự tham khảo đến Fig.1A, nút 1 có thể thi hành việc xác minh sơ bộ sau khi nhận giao dịch từ nút A. Ngay khi được xác minh, giao dịch có thể được lưu trữ trong cơ sở dữ liệu vùng của nút blockchain tiếp nhận, và

cũng có thể gửi giao dịch đến một hoặc nhiều nút blockchain khác (ví dụ, nút 3, nút 4) mà lặp lại quy trình được thực hiện bởi tiếp nhận. Ngay khi giao dịch trong cơ sở dữ liệu vùng tương ứng đạt đến mức nhất định, thì các nút blockchain trong đó mỗi nút có thể xác minh đợt của các giao dịch trong cơ sở dữ liệu vùng tương ứng theo các quy tắc đồng thuận hoặc phương pháp khác. Nếu giao dịch tham gia hợp đồng blockchain, thì nút blockchain có thể thực thi được hợp đồng blockchain một cách cục bộ. Nút blockchain cụ thể mà xác minh thành công đợt của các giao dịch của nó (ví dụ, theo các quy tắc đồng thuận) có thể được đóng gói các giao dịch để bổ sung các bản sao cục bộ blockchain của nó và gửi các kết quả đến các nút blockchain khác. Nút blockchain cụ thể có thể là nút mà trước tiên hoàn thành sự xác minh thành công, mà thu nhận đặc quyền xác minh, hoặc được xác định dựa trên quy tắc đồng thuận khác. Các nút blockchain khác có thể thực thi được các giao dịch một cách cục bộ, xác minh các kết quả thực thi với nhau (ví dụ, bằng cách thi hành tính toán băm), và đồng bộ các bản sao của blockchain với các bản sao của nút blockchain cụ thể. Bằng cách cập nhật các bản sao cục bộ của blockchain, thì các nút blockchain có thể ghi thông tin này vào các bộ nhớ cục bộ. Nếu sự xác minh lỗi ở điểm nào đó, thì các giao dịch bị hủy bỏ.

Fig.1B là hình minh họa khung cơ sở làm ví dụ để thực hiện hợp đồng blockchain, theo các phương án thực hiện khác nhau. Các hoạt động mà được thể hiện dưới đây là nhằm mục đích minh họa. Tùy theo phương án thực hiện, các bước làm ví dụ có thể bao gồm các bước bổ sung, loại bỏ hoặc thay thế được thi hành theo các thứ tự khác nhau hoặc song song.

Theo các phương án thực hiện khác nhau, để triển khai hợp đồng blockchain, nút A có thể soạn mã nguồn hợp đồng blockchain bởi bộ soạn, mà trả lại mã byte. Nút A có thể xây dựng và ký giao dịch gồm mã byte. Ví dụ, giao dịch có thể bao gồm thông tin như thực hiện một lần, gasPrice, gasLimit, đến (ví dụ, hợp đồng blockchain cần được gọi hoặc địa chỉ của tài khoản của người nhận), giá trị, dữ liệu (ví dụ, mã byte), và thông tin tương tự. Nút A có thể gửi giao dịch đến nút blockchain 1 thông qua giao diện cuộc gọi thủ tục từ xa (Remote Procedure Call, RPC). RPC là khi chương trình máy tính làm cho thủ tục (ví dụ, trình con) thực thi trong không gian địa chỉ khác nhau (ví dụ, trên máy tính khác như nút 1 trên mạng

dùng chung), mà được viết mã như thể nó là cuộc gọi thủ tục thông thường (cục bộ), mà không cần người lập trình viết mã một cách rõ ràng các chi tiết cho tương tác từ xa. Nút 1 có thể xác minh nếu giao dịch là hợp lệ bằng cách xác minh chữ ký. Ngay khi được xác minh, nút 1 có thể gửi giao dịch đến mạng blockchain gồm nhiều nút blockchain khác. Các nút blockchain có thể xác minh giao dịch thông qua sự tính toán trên các máy ảo (Virtual Machine, VM) cục bộ và đóng gói giao dịch đã xác minh thành khối mới của blockchain. Khối mới sẽ được đồng bộ với tất cả các nút blockchain.

Các nền tảng blockchain hiện nay như hệ thống Ethereum chỉ hỗ trợ các hợp đồng vững chắc. Sự vững chắc là ngôn ngữ lập trình định hướng hợp đồng để viết các hợp đồng blockchain được thực hiện bởi EVM. Các hệ thống blockchain này không hỗ trợ các ngôn ngữ hợp đồng trong các ngôn ngữ lập trình khác như c++, java, python, v.v. Kết quả là, các hệ thống blockchain không hỗ trợ hoặc thực thi các hợp đồng tự nhiên (ví dụ, các hợp đồng blockchain được viết trong ngôn ngữ c++ hoặc các ngôn ngữ không vững chắc khác). Sự thiếu sót này trong các công nghệ hiện có kìm hãm sự phát triển và hạn chế sự ứng dụng của các hệ thống blockchain.

Để ít nhất là giảm bớt các thiếu sót trong các công nghệ hiện có, thì sáng chế đề xuất giải pháp kỹ thuật đối với vấn đề kỹ thuật trên đây, và cải thiện các chức năng máy tính, các hệ thống và phương pháp để thực hiện các hợp đồng tự nhiên trên blockchain được đề xuất. Sự hỗ trợ đối với các hợp đồng tự nhiên có thể đạt được nhờ sử dụng thư viện động để mở rộng các ứng dụng của các hợp đồng thông minh. Theo một ví dụ, các hệ thống và phương pháp dưới đây được mô tả dựa trên hệ thống c++. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ hiểu rõ rằng ứng dụng của các hệ thống và phương pháp đã được bộc lộ trên các hệ thống ngôn ngữ máy tính khác nhau.

Fig.2 là hình minh họa phương pháp làm ví dụ để bổ sung bộ chỉ báo, theo các phương án thực hiện khác nhau. Các hoạt động mà được thể hiện dưới đây là nhằm mục đích minh họa. Tùy theo phương án thực hiện, các bước làm ví dụ có thể bao gồm các bước bổ sung, loại bỏ hoặc thay thế được thi hành theo các thứ tự khác nhau hoặc song song. Mặc dù ví dụ trên Fig.2 sử dụng c++ là ngôn ngữ lập trình làm

ví dụ, nhưng các ngôn ngữ lập trình khác nhau có thể được sử dụng để viết hợp đồng blockchain.

Ở bước 201, người dùng có thể viết chương trình hợp đồng blockchain trong c++ trên thiết bị người dùng. Một phần của mã nguồn c++ làm ví dụ được thể hiện. Mã nguồn có thể được gửi đến bộ soạn (ví dụ, bộ soạn c++). Bộ soạn có thể ở trên thiết bị người dùng hoặc thiết bị khác mà được ghép nối với thiết bị người dùng.

Ở bước 202, bộ soạn có thể soạn mã nguồn (ví dụ, trong tệp .cpp) thành mã byte (ví dụ, trong tệp .so) của hợp đồng blockchain. Theo một số phương án, người dùng có thể xây dựng hợp đồng blockchain ở đầu trước trong các ngôn ngữ lập trình khác nhau (ví dụ, java, c++, python). Phần mềm đầu trước có thể được nạp vào thiết bị người dùng. Sau đó, bộ soạn được liên kết với đầu trước có thể soạn hợp đồng blockchain thành mã byte. Bộ soạn có thể là phần mềm máy tính mà biến đổi mã máy tính được viết trong một ngôn ngữ lập trình (ngôn ngữ nguồn) thành ngôn ngữ lập trình khác (ngôn ngữ đích). Các bộ soạn có thể dịch mã nguồn từ ngôn ngữ lập trình cấp cao thành ngôn ngữ cấp thấp hơn (ví dụ, hợp ngữ, mã đối tượng, hoặc mã máy) để tạo ra chương trình có thể thực thi được. Mã byte, cũng được gọi là mã di động hoặc p-code, là dạng tập lệnh được thiết kế để thực thi một cách hiệu quả bởi bộ thông dịch phần mềm. Hợp đồng blockchain có thể được viết mã nguồn có thể đọc được bởi người trong các ngôn ngữ lập trình khác nhau, trong khi đó mã byte có thể được gọi là mã máy hoặc nút đối tượng. Không giống mã nguồn mà người có thể đọc, mà các mã byte là các mã bởi số nhỏ gọn, các hằng số, và số tham chiếu (ví dụ, các địa chỉ số) mà mã hóa kết quả của bộ soạn phân tích cú pháp và thi hành việc phân tích ngữ nghĩa của các loại như kiểu, phạm vi, và độ sâu lồng vào nhau của các đối tượng lập trình. Trong trường hợp này, mã byte có thể được đọc bởi nút blockchain để thực thi hợp đồng blockchain.

Theo một ví dụ, các byte kép thứ nhất của vùng thập lục phân của mã byte như được soạn sẽ được thể hiện. Nhằm làm sáng tỏ, phần cụ thể của mã byte như vùng địa chỉ và vùng ascii không được thể hiện. Mã byte có thể theo hệ thập lục phân. Trong bản mô tả này, mã byte c++ có thể được gồm trong tệp thư viện động (ví dụ, tệp. so) mà chứa các lệnh cho máy ảo tương ứng với c++ để thực thi chương trình. Theo các phương án thực hiện khác nhau, thư viện động tồn tại bên ngoài tệp

có thể thực thi được hoặc ứng dụng. Trong thời gian chạy, thì liên kết được tạo ra giữa thư viện động và tệp có thể thực thi được hoặc ứng dụng. Thư viện động bao gồm các chức năng đặc biệt được khởi chạy trong quá trình thực thi chương trình, mà giảm thiểu kích cỡ chương trình tổng thể và tạo điều kiện thuận lợi cho hiệu suất ứng dụng được cải thiện để giảm việc tiêu thụ bộ nhớ.

Ở bước 203, thiết bị người dùng (ví dụ, phần mềm ví) có thể chèn bộ chỉ báo vào mã byte như được soạn của hợp đồng blockchain. Như một ví dụ được thể hiện ở đây, bộ chỉ báo có thể được bổ sung cho vào phần trước nhất của mã byte. Bộ chỉ báo có thể bao gồm một byte dữ liệu chỉ ra kiểu của hợp đồng blockchain (ví dụ, xem hợp đồng blockchain là hợp đồng tự nhiên, ngôn ngữ lập trình của hợp đồng blockchain, v.v.). Theo ví dụ này, bộ chỉ báo là 03 để chỉ ra hợp đồng tự nhiên và tham khảo đến c++. Bộ chỉ báo cũng có thể là các số thập lục phân. Do vậy, 03 ở đây được đổi thành 0x03. Các sự biểu diễn khác nhau có thể được sử dụng theo cách thay thế. Bộ chỉ báo cũng có thể được chèn ở vị trí khác trong mã byte.

Theo một số phương án, thiết bị người dùng (ví dụ, với ví tiền điện tử hoặc phần mềm nền tảng blockchain khác được cài đặt) có thể hỏi người dùng nhập, lựa chọn, hoặc theo cách khác nhận dạng kiểu hợp đồng của hợp đồng blockchain (ví dụ, hợp đồng tự nhiên, hợp đồng vững chắc, hợp đồng viết bằng java, hợp đồng viết bằng c++, hợp đồng viết bằng python, v.v.). Dựa trên thông tin được cung cấp bởi người dùng, thì thiết bị người dùng có thể áp dụng bộ chỉ báo để biểu diễn kiểu hợp đồng. Thiết bị người dùng có thể luân phiên tự động xác định kiểu hợp đồng và áp dụng bộ chỉ báo để biểu diễn kiểu hợp đồng đó. Ví dụ, “03” hoặc “0x03” có thể biểu diễn hợp đồng tự nhiên, và “05” hoặc “0x05” có thể biểu diễn hợp đồng vững chắc. Để làm ví dụ khác, “01” hoặc “0x01” có thể biểu diễn hợp đồng trong ngôn ngữ vững chắc, “02” hoặc “0x02” có thể biểu diễn hợp đồng trong ngôn ngữ java, “03” hoặc “0x03” có thể biểu diễn hợp đồng trong ngôn ngữ c++, “04” hoặc “0x04” có thể biểu diễn hợp đồng trong ngôn ngữ python, v.v. Bộ chỉ báo có thể ở dạng mã byte hoặc định dạng thay thế. Mặc dù biểu diễn thập lục phân thường được sử dụng, bộ chỉ báo có thể không bị giới hạn ở các ví dụ về sự biểu diễn trên đây. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể hiểu rõ rằng việc sử dụng các kiểu khác nhau của các sự biểu diễn bộ chỉ báo. Bộ chỉ báo có thể được bổ sung ở phía

trước mã byte như được soạn của hợp đồng blockchain hoặc ở vị trí khác. Theo một ví dụ, bộ chỉ báo được bổ sung ở phía trước mã byte. Bộ chỉ báo có thể chiếm một byte hoặc dung lượng khác của dữ liệu.

Sau khi bộ chỉ báo được bổ sung cho mã byte như được soạn, thì thu nhận mã byte được kết hợp. Sau bước 203, thiết bị người dùng có thể gửi mã byte được kết hợp đến nút blockchain, và nút blockchain hoặc nút blockchain khác của mạng blockchain có thể kích hoạt máy ảo dựa trên bộ chỉ báo để thực thi hợp đồng blockchain.

Theo một số phương án, với bộ chỉ báo mà được bổ sung cho mã byte, thì thiết bị người dùng có thể truyền hợp đồng blockchain đến một hoặc nhiều nút đồng thuận. Nút đồng thuận có thể nhận mã byte được kết hợp bao gồm bộ chỉ báo và mã byte đã được soạn của hợp đồng blockchain. Sau khi nhận thông điệp rằng hợp đồng được triển khai, thì nút đồng thuận có thể thu nhận một phần (ví dụ, bộ chỉ báo ở byte đầu tiên của mã byte được kết hợp) của mã byte được kết hợp và kích hoạt máy ảo tương ứng để thực thi và lưu trữ hợp đồng dựa trên phần được thu nhận của mã hợp đồng. Theo các phương án thực hiện khác nhau, máy ảo có thể biến đổi mã byte thành hợp ngữ hoặc tập lệnh khác mà có thể chạy bởi bộ xử lý. Ví dụ, nếu mã hợp đồng dựa trên c++, thì tập hợp bộ soạn GNU (GNU Compiler Collection, GCC) có thể được gọi để thực thi hợp đồng; nếu mã hợp đồng dựa trên java, thì máy ảo java (Java Virtual Machine, JVM) có thể được gọi để thực thi hợp đồng; nếu mã hợp đồng dựa trên sự vững chắc, thì máy ảo Ethereum (EVM) có thể được gọi để thực thi hợp đồng; và nếu mã hợp đồng dựa trên python, thì máy ảo python (Python Virtual Machine, PVM) có thể được gọi để thực thi hợp đồng. Các máy ảo trên đây chỉ là ví dụ và có thể được thay thế bởi các phương án khác.

Mỗi hình trong số các hình từ Fig.3A đến Fig.3C minh họa lưu đồ của phương pháp làm ví dụ để thực hiện hợp đồng tự nhiên trên blockchain, theo các phương án thực hiện khác nhau. Phương pháp có thể được thực hiện bởi hệ thống blockchain (ví dụ, hệ thống 100) bao gồm phần mềm và phần cứng khác nhau. Ví dụ, hệ thống blockchain có thể bao gồm máy khách tùy chọn là phần mềm thứ nhất và máy ảo là phần mềm thứ hai và truy nhập vào tệp áp dụng mã nguồn .cpp. Các hoạt động mà được thể hiện dưới đây là nhằm mục đích minh họa. Tùy theo phương

án thực hiện, các bước làm ví dụ có thể bao gồm các bước bổ sung, loại bỏ hoặc thay thế được thi hành theo các thứ tự khác nhau hoặc song song. Các phương pháp theo mỗi hình trong số các hình từ Fig.3A đến Fig.3C có thể chia sẻ các bước chung từ 1 đến 5 như được mô tả dưới đây.

Theo một số phương án, ở bước 1, phần mềm đầu trước có thể hỏi người dùng để nhận dạng kiểu của hợp đồng blockchain cần được thực thi. Đầu trước có thể được cung cấp thông qua nút blockchain hoặc thông qua thiết bị (ví dụ, thiết bị người dùng) được ghép nối với nút blockchain. Trong bản mô tả này, kiểu của hợp đồng blockchain có thể nói đến loại hoặc phân loại của hợp đồng blockchain. Ví dụ, loại này có thể được dựa trên ngôn ngữ lập trình của hợp đồng blockchain. Một hợp đồng blockchain có thể được viết trong java, c++, ngôn ngữ vững chắc, python, v.v. Hợp đồng blockchain được viết trong vững chắc có thể được gọi là hợp đồng vững chắc. Một hợp đồng blockchain được viết trong java, c++, python, hoặc ngôn ngữ khác giống như hệ thống blockchain có thể được gọi là hợp đồng tự nhiên. Tuy nhiên, kiểu của hợp đồng blockchain có thể nói đến loại hoặc phân loại không liên quan đến ngôn ngữ lập trình của hợp đồng blockchain.

Theo một ví dụ, người dùng có thể được yêu cầu để nhận dạng kiểu hợp đồng, mà có thể được biểu diễn bởi bộ chỉ báo. Người dùng có thể nhận dạng kiểu hợp đồng thông qua giao diện người dùng. Nếu hợp đồng tự nhiên được chỉ báo, thì bước tiếp theo của phương pháp này được thi hành.

Theo một số phương án, ở bước 2, trên nền tảng c++, giao diện (ví dụ, giao diện chung) cũng có thể được cung cấp cho người dùng để truy nhập blockchain và thực thi các hợp đồng tự nhiên. Giao diện có thể được cung cấp bằng cách nạp động. Giao diện có thể yêu cầu đầu vào định trước và các định dạng đầu ra cho các người dùng thực hiện các hợp đồng tự nhiên. Các định dạng đầu vào và đầu ra có thể bao gồm các phương pháp để gọi dữ liệu. Theo các yêu cầu này, người dùng có thể cung cấp mã nguồn cho hợp đồng tự nhiên ở giao diện.

Theo một số phương án, ở bước 3, bộ soạn có thể soạn hợp đồng tự nhiên (ví dụ, tệp mã nguồn (.cpp) trong ngôn ngữ c++) để tạo tệp thư viện động tương ứng (ví dụ, tệp .so). Tệp thư viện động có thể nằm trong mã máy như mã byte. Các chi tiết của bước này có thể được tham khảo đến Fig.2 trên đây.

Theo một số phương án, ở bước 4, hợp đồng tự nhiên có thể được triển khai trên hệ thống blockchain. Ví dụ, bộ chỉ báo có thể được bổ sung cho mã byte để thu nhận mã byte đã được kết hợp. Tức là, mã byte được kết hợp có thể bao gồm bộ chỉ báo và mã byte đã được soạn của tệp thư viện động. Mã byte được kết hợp có thể được gửi đến nút blockchain (ví dụ, phần mềm đầu cuối). Các chi tiết của bước này có thể được tham khảo đến Fig.2 trên đây.

Theo một số phương án, ở bước 5, nút blockchain có thể xác định nếu hợp đồng blockchain là hợp đồng tự nhiên ít nhất là dựa trên bộ chỉ báo. Ví dụ, nút đồng thuận có thể tách một phần của mã byte tương ứng với bộ chỉ báo để xác định nếu hợp đồng blockchain là hợp đồng tự nhiên.

Theo một số phương án, nút đồng thuận đầu cuối có thể thực thi được hợp đồng tự nhiên bởi bước bất kỳ trong số ba bước 6.1 đến 6.3. Bước 6.1 được thể hiện trên Fig.3A, bước 6.2 được thể hiện trên Fig.3B, và bước 6.3 được thể hiện trên Fig.3C.

Đối với bước 6.1, nút blockchain có thể thực thi được trực tiếp hợp đồng blockchain trên hệ thống blockchain bằng cách liên kết động và/hoặc nạp tệp thư viện động (hoặc mã byte được kết hợp) và trả lại kết quả. Ví dụ, nút blockchain có thể kích hoạt máy ảo tương ứng với hợp đồng blockchain để thực thi hợp đồng blockchain bằng cách liên kết động và/hoặc nạp tệp thư viện động và trả lại kết quả. Theo cách tùy chọn, nút blockchain có thể tạo tệp thư viện động cục bộ tương ứng để liên kết động và/hoặc nạp tệp thư viện động.

Đối với bước 6.2, nút đồng thuận có thể tạo ra quy trình con (ví dụ, nhờ hàm rẽ nhánh) để thực thi tệp thư viện động (hoặc mã byte được kết hợp). Ví dụ, nút đồng thuận có thể kích hoạt máy ảo để gọi máy khách để soạn lôgic đã được gọi vào tệp khả thi (máy khách). Tệp có thể thực thi được có thể được sử dụng thực thi tệp thư viện động bằng cách liên kết và/hoặc nạp tệp thư viện động và trả lại kết quả thực thi đến máy ảo. Quy trình con và hệ thống blockchain (ví dụ, máy ảo hoặc thành phần thay thế của hệ thống blockchain) có thể truyền thông qua bộ nhớ cắm hoặc bộ nhớ dùng chung. Sau khi nhận kết quả thực thi, thì hệ thống blockchain có thể thực hiện sự thực thi giao dịch tiếp theo.

Đối với bước 6.3, nút đồng thuận có thể lưu lôgic thực thi như một biên bản lưu. Khi người dùng gọi để thực hiện hợp đồng tự nhiên, thì biên bản lưu được kích hoạt để gọi và thực thi tệp thư viện động và trả lại kết quả thực thi đến hệ thống blockchain. Sau khi thu nhận kết quả thực thi, thì hệ thống blockchain có thể thực hiện việc thực thi giao dịch tiếp theo. Biên bản lưu và hệ thống blockchain (ví dụ, máy ảo hoặc thành phần thay thế của hệ thống blockchain) có thể truyền thông qua ổ cắm.

Biên bản lưu cho phép dễ dàng đóng gói, vận chuyển và chạy ứng dụng dưới dạng một bộ gồm nhẹ, di động và tự túc. Các bộ phận chứa biên bản lưu chia sẻ hệ thống hoạt động khi hệ thống hoạt động máy chủ chia sẻ nhân của nó với các bộ phận chứa biên bản lưu đang chạy, trong khi đó các ứng dụng máy ảo mỗi ứng dụng có hệ thống hoạt động khách. Biên bản lưu có thể cài đặt các môi trường phát triển cục bộ mà giống như máy chủ thực, chạy các phương tiện đa phát triển từ cùng một máy chủ mà mỗi môi trường có phần mềm duy nhất, các hệ thống hoạt động, và các cấu hình, các dự án thử nghiệm trên các máy chủ mới hoặc khác nhau, và cho phép bất kỳ ai làm việc với dự án này với các cài đặt giống nhau chính xác, bất kể môi trường máy chủ cục bộ. Ở đây, biên bản lưu cung cấp môi trường ảo để thực thi hợp đồng blockchain, mà có thể giữ nút đồng thuận được bảo vệ khỏi các vấn đề gây ra bởi sự thực thi (ví dụ, khởi động lại hệ thống, vá lỗi, thực thi mã độc hại, v.v.).

Fig.4 là hình minh họa lưu đồ của phương pháp làm ví dụ 450 để thực hiện hợp đồng tự nhiên trên blockchain, theo các phương án thực hiện khác nhau. Phương pháp 450 có thể được thực hiện bởi một hoặc nhiều thành phần (ví dụ, nút 1, nút 2, …, nút i, hoặc sự kết hợp của nút 1 và nút A hoặc tương tự) của hệ thống 100 trên Fig.1A. Phương pháp 450 có thể được thực hiện bởi nút đồng thuận tương ứng với máy phần cứng (ví dụ, máy chủ) mà phần mềm (ví dụ, phần mềm blockchain). Phương pháp 450 có thể được thực hiện bởi một hoặc nhiều hệ thống hoặc thiết bị (ví dụ, máy tính, máy chủ). Hệ thống hoặc thiết bị có thể bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp (ví dụ, một hoặc nhiều bộ nhớ) mà được ghép nối với một hoặc nhiều bộ xử lý và được tạo cấu hình bởi các lệnh có thể thực thi được bởi một hoặc nhiều bộ xử lý để làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) để thi hành phương pháp 450. Các

hoạt động của phương pháp 450 mà được thể hiện dưới đây là nhằm mục đích minh họa. Tùy theo phương án thực hiện, phương pháp làm ví dụ 450 có thể bao gồm các bước bổ sung, loại bỏ hoặc thay thế được thi hành theo các thứ tự khác nhau hoặc song song.

Khối 451 bao gồm việc: thu nhận mã byte được kết hợp mà được liên kết với hợp đồng blockchain, trong đó mã byte được kết hợp bao gồm bộ chỉ báo biểu diễn kiểu hợp đồng blockchain. Theo một số phương án, mã byte được kết hợp bao gồm mã byte của tệp thư viện động được soạn từ mã nguồn của hợp đồng blockchain. Theo một ví dụ, mã nguồn là c++. Thuật ngữ "được kết hợp" có thể chỉ ra sự có mặt của bộ chỉ báo là mã byte được kết hợp có thể bao gồm (1) bộ chỉ báo và (2) mã byte như được soạn từ mã nguồn. Bộ chỉ báo có thể hoặc có thể không ở định dạng mã byte.

Khối 452 bao gồm việc: xác định kiểu hợp đồng blockchain ít nhất là dựa trên bộ chỉ báo. Theo một số phương án, bước xác định kiểu hợp đồng blockchain ít nhất là dựa trên bộ chỉ báo bao gồm việc: xác định nếu kiểu hợp đồng blockchain là hợp đồng tự nhiên.

Khối 453 bao gồm việc: thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định.

Theo một số phương án, ở khối 454, việc thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định bao gồm việc: để đáp lại việc xác định hợp đồng blockchain là hợp đồng tự nhiên, thì kích hoạt máy ảo blockchain để thực thi hợp đồng blockchain. Việc kích hoạt máy ảo để thực thi hợp đồng blockchain bao gồm việc: xác định máy ảo tương ứng với kiểu ít nhất là dựa trên bộ chỉ báo; và kích hoạt máy ảo được xác định để thực thi tệp thư viện động.

Theo một số phương án, ở khối 455, việc thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định bao gồm việc: để đáp lại việc xác định hợp đồng blockchain là hợp đồng tự nhiên, thì tạo ra quy trình con để thực thi hợp đồng blockchain. Việc tạo ra quy trình con để thực thi hợp đồng blockchain bao gồm các việc: tạo ra tệp có thể thực thi được; và sinh ra quy trình con để khởi chạy tệp có thể thực thi được để thực thi tệp thư viện động. Quy trình con và máy ảo blockchain truyền thông qua bộ nhớ cắm hoặc bộ nhớ dùng chung.

Theo một số phương án, ở khối 456, việc thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định bao gồm việc: để đáp lại việc xác định hợp đồng blockchain là hợp đồng tự nhiên, thì khởi chạy bộ phận chứa biên bản lưu để thực thi hợp đồng blockchain. Việc khởi chạy bộ phận chứa biên bản lưu để thực thi hợp đồng blockchain bao gồm các việc: tạo ra bộ phận chứa biên bản lưu; và khởi chạy bộ phận chứa biên bản lưu để thực thi tệp thư viện động. Bộ phận chứa biên bản lưu và máy ảo blockchain truyền thông qua ổ cắm.

Trong các công nghệ hiện tại, phần mềm blockchain của nút blockchain hầu như không tích hợp các kiểu khác nhau của các máy ảo, cho dù máy phần cứng của nút blockchain có thể truy cập các máy ảo này (ví dụ, từ các sự cài đặt trước đó trong máy phần cứng hoặc các cấu hình hệ thống). Với các phương pháp đã được bộc lộ, nút blockchain có thể xác định kiểu hợp đồng (ví dụ, là hợp đồng tự nhiên hay hợp đồng vững chắc, ngôn ngữ lập trình của hợp đồng) dựa trên mã byte của hợp đồng nhận được và kích hoạt phương pháp tương ứng để thực thi hợp đồng. Với việc sử dụng tệp thư viện động, các hợp đồng tự nhiên có thể được hỗ trợ bởi hệ thống blockchain cho việc thực thi mà không phải chuyển đổi thành các hợp đồng vững chắc. Do vậy, phạm vi ứng dụng và độ tương thích của hợp đồng hệ thống blockchain được mở rộng, do hợp đồng blockchain không còn cần được viết bằng ngôn ngữ chắc chắn và các hợp đồng tự nhiên có thể được thực thi như các hợp đồng vững chắc.

Các công nghệ đã được mô tả ở đây được thực hiện bởi một hoặc nhiều thiết bị điện toán có chuyên dụng. Các thiết bị điện toán có chuyên dụng có thể là các hệ thống máy tính để bàn, các hệ thống máy tính máy chủ, các hệ thống máy tính xách tay, các thiết bị cầm tay, các thiết bị mạng hoặc thiết bị khác bất kỳ của sự kết hợp của các thiết bị mà kết hợp lôgic kiểm soát bởi mạng điện tử và/hoặc lôgic chương trình để thực hiện các công nghệ. (Các) thiết bị điện toán thường được điều khiển và điều phối bằng cách vận hành phần mềm hệ thống. Sự điều khiển các hệ thống hoạt động thông thường và các quy trình lập lịch biểu máy tính để thực thi, thi hành việc quản lý bộ nhớ, cung cấp tệp hệ thống, liên kết mạng, các dịch vụ nhập/xuất, và cung cấp chức năng giao diện người dùng, như giao diện đồ họa người dùng (Graphical User Interface, GUI), ngoài các vấn đề khác.

Fig.5 là hình minh họa sơ đồ khối của hệ thống máy tính làm ví dụ 550 để thực hiện hợp đồng tự nhiên trên blockchain, theo các phương án thực hiện khác nhau. Hệ thống 550 có thể là phương án thực hiện làm ví dụ của nút 1, sự kết hợp của nút A và nút 1, nút 2, …, nút i của hệ thống 100 trên Fig.1A hoặc thiết bị tương tự. Phương pháp 450 có thể được thực hiện bởi hệ thống máy tính 550. Hệ thống máy tính 550 có thể bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp (ví dụ, một hoặc nhiều bộ nhớ) mà được ghép nối với một hoặc nhiều bộ xử lý và được tạo cấu hình bởi các lệnh có thể thực thi được bởi một hoặc nhiều bộ xử lý để làm cho hệ thống hoặc thiết bị (ví dụ, bộ xử lý) để thi hành phương pháp 450. Hệ thống máy tính 550 có thể bao gồm các đơn vị/môđun khác nhau tương ứng với các lệnh (ví dụ, các lệnh phần mềm). Theo một số phương án, hệ thống máy tính 550 có thể bao gồm môđun thu nhận 551 mà được tạo cấu hình để thu nhận mã byte đã được được kết hợp mà được liên kết với hợp đồng blockchain, trong đó mã byte được kết hợp bao gồm bộ chỉ báo biểu diễn kiểu hợp đồng blockchain; môđun xác định 552 được tạo cấu hình để xác định kiểu của hợp đồng blockchain ít nhất là dựa trên bộ chỉ báo; và môđun thực thi 553 được tạo cấu hình để thực thi hợp đồng blockchain dựa trên kiểu hợp đồng blockchain được xác định.

Fig.6 là sơ đồ khối minh họa hệ thống máy tính 600 mà phương án thực hiện bất kỳ trong số các phương án thực hiện đã được mô tả ở đây có thể được thực hiện trên đó. Hệ thống 600 có thể được thực hiện ở nút bất kỳ trong số các nút đã được mô tả ở đây và được tạo cấu hình để thi hành các bước tương ứng để thực hiện hợp đồng tự nhiên trên blockchain. Hệ thống máy tính 600 bao gồm đường bus 602 hoặc cơ chế truyền thông khác để truyền thông thông tin, một hoặc nhiều (các) bộ xử lý phần cứng 604 được ghép nối với đường bus 602 để xử lý thông tin. (Các) bộ xử lý phần cứng 604 có thể là, ví dụ, một hoặc nhiều bộ vi xử lý mục đích chung.

Hệ thống máy tính 600 còn bao gồm bộ nhớ chính 606, như bộ nhớ truy cập ngẫu nhiên (Random Access Memory, RAM), bộ nhớ đệm và/hoặc thiết bị lưu trữ thay đổi khác, được ghép nối với đường bus 602 để lưu trữ thông tin và các lệnh sẽ được thực thi bởi (các) bộ xử lý 604. Bộ nhớ chính 606 cũng có thể được sử dụng để lưu trữ các biến tạm thời hoặc thông tin trung gian khác trong quá trình thực thi các

lệnh sẽ được thực thi bởi (các) bộ xử lý 604. Các lệnh này, khi được lưu trữ trong phương tiện lưu trữ có thể truy nhập vào (các) bộ xử lý 604, thì kết xuất hệ thống máy tính 600 thành máy chuyên dụng mà được tùy biến để thi hành các hoạt động được chỉ rõ trong các lệnh. Hệ thống máy tính 600 còn bao gồm bộ nhớ chỉ đọc (Read Only Memory, ROM) 608 hoặc thiết bị lưu trữ không thay đổi khác ghép nối với đường bus 602 để lưu trữ thông tin không thay đổi và các lệnh cho (các) bộ xử lý 604. Thiết bị lưu trữ 610, như đĩa từ, đĩa quang, ổ USB (ổ đĩa tác động nha (flash)), v.v., được cung cấp và được ghép nối với đường bus 602 để lưu trữ thông tin và các lệnh.

Hệ thống máy tính 600 có thể thực hiện các công nghệ đã được mô tả ở đây nhờ sử dụng lôgic có dây, một hoặc nhiều ASIC hoặc FPGA, phần sụn và/hoặc lôgic chương trình mà kết hợp với hệ thống máy tính làm cho hoặc tạo chương trình cho hệ thống máy tính 600 để trở thành máy chuyên dụng. Theo một phương án thực hiện, các hoạt động, các phương pháp, và các quy trình đã được mô tả ở đây được thi hành bởi hệ thống máy tính 600 để đáp lại việc (các) bộ xử lý 604 thực thi một hoặc nhiều chuỗi của một hoặc nhiều lệnh gồm trong bộ nhớ chính 606. Các lệnh này có thể được đọc bên trong bộ nhớ chính 606 từ phương tiện lưu trữ khác, như thiết bị lưu trữ 610. Sự thực thi của các lệnh tuần tự gồm trong bộ nhớ chính 606 khiến cho (các) bộ xử lý 604 để thi hành các bước xử lý đã được mô tả ở đây. Theo các phương án thực hiện khác, hệ thống mạch có dây có thể được sử dụng thay thế hoặc kết hợp với các lệnh phần mềm.

Bộ nhớ chính 606, ROM 608, và/hoặc bộ lưu trữ 610 có thể bao gồm phương tiện lưu trữ không chuyển tiếp. Thuật ngữ "phương tiện không chuyển tiếp," và các thuật ngữ tương tự, như được sử dụng ở đây để nói đến phương tiện mà lưu trữ dữ liệu và/hoặc các lệnh mà làm cho máy hoạt động theo cách riêng, các tín hiệu chuyển tiếp loại trừ phương tiện. Phương tiện không chuyển tiếp này có thể bao gồm phương tiện bất khả biến và/hoặc phương tiện khả biến. Phương tiện bất khả biến bao gồm, ví dụ, đĩa quang hoặc đĩa từ, như thiết bị lưu trữ 610. Phương tiện khả biến bao gồm bộ nhớ động, như bộ nhớ chính 606. Các dạng chung của phương tiện không chuyển tiếp bao gồm, ví dụ, ổ đĩa mềm, ổ đĩa dẻo, ổ đĩa cứng, ổ đĩa trạng thái rắn, băng từ, hoặc phương tiện lưu trữ dữ liệu từ tính khác bất kỳ, CD-ROM, phương tiện lưu trữ

dữ liệu quang học khác bất kỳ, phương tiện vật lý bất kỳ có các kiểu lỗ, RAM, PROM, và EPROM, FLASH-EPROM, NVRAM, chip hoặc hộp bộ nhớ khác bất kỳ, và các phiên bản liên kết của chúng.

Hệ thống máy tính 600 còn bao gồm mạng giao diện 618 được ghép nối với đường bus 602. Mạng giao diện 618 cung cấp truyền thông dữ liệu hai chiều ghép nối với một hoặc nhiều liên kết mạng mà được kết nối với một hoặc nhiều mạng cục bộ. Ví dụ, mạng giao diện 618 có thể là các mạng kỹ thuật số dịch vụ tích hợp (Integrated Services Digital Network, ISDN), môđem cáp, môđem vệ tinh, hoặc môđem để cung cấp kết nối truyền thông dữ liệu với kiểu đường dây điện thoại tương ứng. Là một ví dụ khác, mạng giao diện 618 có thể là thẻ mạng cục bộ (Local Area Network LAN) để cung cấp kết nối truyền thông dữ liệu với mạng LAN tương thích (hoặc thành phần mạng WAN để giao tiếp với WAN). Các liên kết không dây cũng có thể được thực hiện. Theo phương án thực hiện bất kỳ này, mạng giao diện 618 gửi và nhận các tín hiệu điện, điện từ hoặc quang mà mang các luồng dữ liệu số biểu diễn các kiểu thông tin khác nhau.

Hệ thống máy tính 600 có thể gửi các thông điệp và nhận dữ liệu, bao gồm mã chương trình, thông qua (các) mạng, liên kết mạng và mạng giao diện 618. Trong ví dụ về Internet, máy chủ có thể truyền mã yêu cầu đối với chương trình ứng dụng thông qua Internet, ISP, mạng cục bộ và mạng giao diện 618.

Mã nhận được có thể được thực thi bởi (các) bộ xử lý 604 khi nó được nhận, và/hoặc lưu trữ trên thiết bị lưu trữ 610, hoặc bộ lưu trữ bất biến khác để thực thi sau.

Mỗi phần trong số các quy trình, các phương pháp, và thuật toán đã được mô tả ở các phần trên đây có thể được thực hiện trong, và tự động hoàn toàn hoặc một phần bởi, các môđun mã thực thi bởi một hoặc nhiều hệ thống máy tính hoặc các bộ xử lý máy tính bao gồm phần cứng máy tính. Các quy trình và các thuật toán có thể được thực hiện một phần hoặc toàn bộ trong hệ mạch ứng dụng chuyên dụng.

Các dấu hiệu và các quy trình khác nhau đã được mô tả trên đây có thể được sử dụng một cách độc lập với nhau, hoặc có thể được kết hợp theo nhiều. Tất cả các kết hợp và kết hợp con được dự tính nằm trong phạm vi của bản mô tả này. Ngoài ra, phương pháp hoặc các khối quy trình cụ thể có thể được bỏ qua trong một số phương

án thực hiện. Các phương pháp và các quy trình đã được mô tả ở đây cũng không bị giới hạn ở tuần tự cụ thể bất kỳ, và các khối hoặc trạng thái liên quan đến chúng có thể được thi hành theo các tuần tự khác nếu thích hợp. Ví dụ, các khối hoặc trạng thái đã được mô tả có thể được thi hành theo thứ tự khác với thứ tự đã được bộc lộ một cách cụ thể, hoặc nhiều khối hoặc trạng thái có thể được kết hợp thành một khối hoặc trạng thái. Các khối hoặc các trạng thái làm ví dụ có thể được thi hành theo kiểu nối tiếp, song song hoặc một số cách khác. Các khối hoặc các trạng thái có thể được bổ sung vào hoặc loại bỏ ra khỏi các phương án thực hiện làm ví dụ đã được bộc lộ. Các hệ thống làm ví dụ và các thành phần đã được mô tả ở đây có thể được tạo cấu hình khác với cấu hình đã được mô tả. Ví dụ, các phần tử có thể được bổ sung cho, loại bỏ ra khỏi, hoặc bố trí lại so với các phương án thực hiện làm ví dụ đã được bộc lộ.

Các hoạt động khác nhau của các phương pháp làm ví dụ đã được mô tả ở đây có thể được thi hành, ít nhất một phần, bởi một thuật toán. Thuật toán có thể được gồm trong các mã chương trình hoặc các lệnh lưu trữ trong bộ nhớ (ví dụ, phương tiện lưu trữ đọc được bởi máy tính không chuyển tiếp đã được mô tả trên đây). Thuật toán này có thể bao gồm thuật toán học máy. Theo một số phương án, thuật toán học máy có thể không lập trình một cách rõ ràng các máy tính để thi hành chức năng, mà có thể học từ dữ liệu đào tạo để tạo ra mô hình dự đoán mà thực hiện chức năng này.

Các hoạt động khác nhau của các phương pháp làm ví dụ đã được mô tả ở đây có thể được thi hành, ít nhất một phần, bởi một hoặc nhiều bộ xử lý mà được tạo cấu hình tạm thời (ví dụ, bởi phần mềm) hoặc được tạo cấu hình vĩnh viễn để thi hành các hoạt động liên quan. Cho dù là được tạo cấu hình tạm thời hay vĩnh viễn, các bộ xử lý này có thể cấu tạo nên các phương tiện thực hiện bởi bộ xử lý mà vận hành để thi hành một hoặc nhiều hoạt động hoặc chức năng đã được mô tả ở đây.

Tương tự, các phương pháp đã được mô tả ở đây có thể được thực hiện bộ xử lý ít nhất một phần, bởi bộ xử lý hoặc các bộ xử lý cụ thể là ví dụ về phần cứng. Ví dụ, ít nhất một số hoạt động trong số các hoạt động của phương pháp có thể được thi hành bởi một hoặc nhiều bộ xử lý hoặc các phương tiện thực hiện bởi bộ xử lý. Ngoài ra, một hoặc nhiều bộ xử lý cũng có thể vận hành để hỗ trợ hiệu suất của các hoạt động liên quan trong môi trường "điện toán đám mây" hoặc dưới dạng "phần

mềm như một dịch vụ" (Software as a Service, SaaS). Ví dụ, ít nhất một số hoạt động trong số các hoạt động có thể được thi hành bởi nhóm các máy tính (là các ví dụ về các máy gồm các bộ xử lý), với các hoạt động này có thể truy cập được qua mạng (ví dụ, Internet) và qua một hoặc nhiều giao diện thích hợp (ví dụ, giao diện chương trình ứng dụng (Application Program Interface, API)).

Hiệu quả của hoạt động cụ thể trong số các hoạt động có thể được phân bố giữa các bộ xử lý, không chỉ nằm trong một máy, mà có thể được triển khai trên nhiều máy. Theo một số phương án làm ví dụ, các bộ xử lý hoặc các phương tiện được thực hiện bởi bộ xử lý có thể được đặt ở một vị trí địa lý (ví dụ, trong môi trường gia đình, môi trường văn phòng, hoặc trang trại máy chủ). Theo một số phương án làm ví dụ khác, các bộ xử lý hoặc các phương tiện được thực hiện bởi bộ xử lý có thể được phân bố trên nhiều vị trí địa lý.

Trong toàn bộ bản mô tả này, nhiều ví dụ có thể áp dụng các thành phần, các hoạt động, hoặc các cấu trúc đã được mô tả như là một ví dụ. Mặc dù các hoạt động riêng rẽ của một hoặc nhiều phương pháp được minh họa và được mô tả là các hoạt động tách biệt, nhưng một hoặc nhiều hoạt động trong số các hoạt động riêng biệt có thể được thi hành đồng thời, và không yêu cầu rằng các hoạt động được theo thứ tự đã được minh họa. Các cấu trúc và chức năng mà được trình bày dưới dạng các thành phần riêng biệt trong các cấu hình ví dụ có thể được thi hành dưới dạng cấu trúc hoặc thành phần kết hợp. Tương tự, các cấu trúc và chức năng được thể hiện dưới dạng một thành phần có thể được thực hiện là các thành phần tách biệt. Các biến thể, biến đổi, bổ sung và cải tiến này cũng như các biến thể, biến đổi, bổ sung và cải tiến này khác đều nằm trong phạm vi bảo hộ của sáng chế này.

Mặc dù tổng quan về sáng chế đã được mô tả với sự tham khảo đến các phương án làm ví dụ cụ thể, nhưng các biến thể và thay đổi khác nhau có thể được thực hiện đối với các phương án này mà không nằm ngoài phạm vi rộng hơn của các phương án thực hiện sáng chế. Các phương án thực hiện này của sáng chế có thể được đề cập tới ở đây, một cách riêng rẽ hoặc chung chung, bởi thuật ngữ "sáng chế" chỉ để tạo thuận tiện và không nhằm làm cho phạm vi bảo hộ của sáng chế này giới hạn ở một phần bộc lộ hoặc khái niệm bất kỳ nếu trong thực tế có nhiều hơn một phần như vậy được bộc lộ. Phần mô tả chi tiết không được xem là trường hợp giới

hạn, và phạm vi của các phương án khác nhau chỉ được xác định bởi các điểm yêu cầu bảo hộ kèm theo, cùng với phạm vi đầy đủ của các phương án tương đương mà các điểm yêu cầu bảo hộ đó bao trùm.

YÊU CẦU BẢO HỘ

1. Phương pháp được thực hiện bởi máy tính để thực hiện các hợp đồng blockchain, bao gồm các bước:

thu nhận mã byte được kết hợp mà được liên kết với hợp đồng blockchain, trong đó:

mã nguồn của hợp đồng blockchain được viết bằng một ngôn ngữ lập trình cấp cao trong số nhiều ngôn ngữ lập trình cấp cao khác nhau,

phần thứ nhất của mã byte được kết hợp biểu diễn kiểu hợp đồng blockchain chỉ ra một ngôn ngữ lập trình cấp cao trong số các ngôn ngữ lập trình cấp cao khác nhau,

kiểu hợp đồng blockchain bao gồm kiểu hợp đồng tự nhiên hoặc kiểu hợp đồng vững chắc,

kiểu hợp đồng tự nhiên chỉ ra rằng một ngôn ngữ lập trình cấp cao là khác với vững chắc, và

kiểu hợp đồng vững chắc chỉ ra rằng một ngôn ngữ lập trình cấp cao là vững chắc;

xác định một ngôn ngữ lập trình cấp cao ít nhất là dựa trên phần thứ nhất của mã byte được kết hợp; và

thực thi hợp đồng blockchain trong máy ảo blockchain khớp với một ngôn ngữ lập trình cấp cao.

2. Phương pháp theo điểm 1, trong đó:

mã byte được kết hợp là mã máy cấp thấp; và

ít nhất một bộ phận của mã byte được kết hợp là được soạn từ mã nguồn của hợp đồng blockchain.

3. Phương pháp theo điểm 1, trong đó bước xác định một ngôn ngữ lập trình cấp cao ít nhất là dựa trên phần thứ nhất của mã byte được kết hợp bao gồm việc:

xác định nếu hợp đồng blockchain là hợp đồng vững chắc hay hợp đồng tự nhiên được viết bằng ngôn ngữ lập trình cấp cao khác với vững chắc.

4. Phương pháp theo điểm 1, trong đó:

phần thứ hai của mã byte được kết hợp bao gồm tệp thư viện động trong mã byte được soạn từ mã nguồn của hợp đồng blockchain.

5. Phương pháp theo điểm 4, trong đó bước thực thi hợp đồng blockchain trong máy ảo blockchain khớp với một ngôn ngữ lập trình cấp cao bao gồm việc:

kích hoạt máy ảo blockchain để thực thi tệp thư viện động.

6. Phương pháp theo điểm 4, trong đó bước thực thi hợp đồng blockchain trong máy ảo blockchain khớp với một ngôn ngữ lập trình cấp cao bao gồm việc:

tạo ra quy trình con để thực thi hợp đồng blockchain.

7. Phương pháp theo điểm 6, trong đó bước tạo ra quy trình con để thực thi hợp đồng blockchain bao gồm các việc:

tạo ra tệp có thể thực thi được; và

sinh ra quy trình con để khởi chạy tệp có thể thực thi được để thực thi tệp thư viện động.

8. Phương pháp theo điểm 6, trong đó:

quy trình con và máy ảo blockchain truyền thông qua bộ nhớ cắm hoặc bộ nhớ dùng chung.

9. Phương pháp theo điểm 4, trong đó bước thực thi hợp đồng blockchain trong máy ảo blockchain khớp với một ngôn ngữ lập trình cấp cao bao gồm việc:

khởi chạy bộ phận chứa biên bản lưu để thực thi hợp đồng blockchain.

10. Phương pháp theo điểm 9, trong đó bước khởi chạy bộ phận chứa biên bản lưu để thực thi hợp đồng blockchain bao gồm các việc:

tạo ra bộ phận chứa biên bản lưu; và

khởi chạy bộ phận chứa biên bản lưu để thực thi tệp thư viện động.

11. Phương pháp theo điểm 9, trong đó:

bộ phận chứa biên bản lưu và máy ảo blockchain truyền thông qua ổ cắm.

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

thu nhận mã byte được kết hợp mà được liên kết với hợp đồng blockchain, trong đó:

mã nguồn của hợp đồng blockchain được viết bằng một ngôn ngữ lập trình cấp cao trong số nhiều ngôn ngữ lập trình cấp cao khác nhau,

phần thứ nhất của mã byte được kết hợp biểu diễn kiểu hợp đồng blockchain chỉ ra một ngôn ngữ lập trình cấp cao trong số các ngôn ngữ lập trình cấp cao khác nhau,

kiểu hợp đồng blockchain bao gồm kiểu hợp đồng tự nhiên hoặc kiểu hợp đồng vững chắc,

kiểu hợp đồng tự nhiên chỉ ra rằng một ngôn ngữ lập trình cấp cao là khác với vững chắc, và

kiểu hợp đồng vững chắc chỉ ra rằng một ngôn ngữ lập trình cấp cao là vững chắc;

xác định một ngôn ngữ lập trình cấp cao ít nhất là dựa trên phần thứ nhất của mã byte được kết hợp; và

thực thi hợp đồng blockchain trong máy ảo blockchain khớp với một ngôn ngữ lập trình cấp cao.

13. Phương tiện lưu trữ theo điểm 12, trong đó:

mã byte được kết hợp là mã máy cấp thấp; và

ít nhất một bộ phận của mã byte được kết hợp là được soạn từ mã nguồn của hợp đồng blockchain.

14. Phương tiện lưu trữ theo điểm 12, trong đó bước xác định một ngôn ngữ lập trình cấp cao ít nhất là dựa trên phần thứ nhất của mã byte được kết hợp bao gồm việc:

xác định nếu hợp đồng blockchain là hợp đồng vững chắc hay hợp đồng tự nhiên được viết bằng ngôn ngữ lập trình cấp cao khác với vững chắc.

15. Phương tiện lưu trữ theo điểm 12, trong đó:

phần thứ hai của mã byte được kết hợp bao gồm tệp thư viện động trong mã byte được soạn từ mã nguồn của hợp đồng blockchain.

16. Phương tiện lưu trữ theo điểm 15, trong đó bước thực thi hợp đồng blockchain trong máy ảo blockchain khớp với một ngôn ngữ lập trình cấp cao bao gồm việc:

kích hoạt máy ảo blockchain để thực thi tệp thư viện động.

17. Phương tiện lưu trữ theo điểm 15, trong đó bước thực thi hợp đồng blockchain trong máy ảo blockchain khớp với một ngôn ngữ lập trình cấp cao bao gồm việc:

tạo ra quy trình con để thực thi hợp đồng blockchain.

18. Phương tiện lưu trữ theo điểm 17, trong đó bước tạo ra quy trình con để thực thi hợp đồng blockchain bao gồm các việc:

tạo ra tệp có thể thực thi được; và

sinh ra quy trình con để khởi chạy tệp có thể thực thi được để thực thi tệp thư viện động.

19. Phương tiện lưu trữ theo điểm 15, trong đó bước thực thi hợp đồng blockchain trong máy ảo blockchain khớp với một ngôn ngữ lập trình cấp cao bao gồm việc:

khởi chạy bộ phận chứa biên bản lưu để thực thi hợp đồng blockchain.

20. Hệ thống được thực hiện bởi máy tính để thực hiện các hợp đồng blockchain bao gồm một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ đọc được bởi máy tính không chuyển tiếp được ghép nối với một hoặc nhiều bộ xử lý và được tạo cấu hình

với các lệnh có thể thực thi được bởi một hoặc nhiều bộ xử lý để làm cho hệ thống thi hành các hoạt động bao gồm:

thu nhận mã byte được kết hợp mà được liên kết với hợp đồng blockchain, trong đó:

mã nguồn của hợp đồng blockchain được viết bằng một ngôn ngữ lập trình cấp cao trong số nhiều ngôn ngữ lập trình cấp cao khác nhau,

phần thứ nhất của mã byte được kết hợp biểu diễn kiểu hợp đồng blockchain chỉ ra một ngôn ngữ lập trình cấp cao trong số các ngôn ngữ lập trình cấp cao khác nhau,

kiểu hợp đồng blockchain bao gồm kiểu hợp đồng tự nhiên hoặc kiểu hợp đồng vững chắc,

kiểu hợp đồng tự nhiên chỉ ra rằng một ngôn ngữ lập trình cấp cao là khác với vững chắc, và

kiểu hợp đồng vững chắc chỉ ra rằng một ngôn ngữ lập trình cấp cao là vững chắc;

xác định một ngôn ngữ lập trình cấp cao ít nhất là dựa trên phần thứ nhất của mã byte được kết hợp; và

thực thi hợp đồng blockchain trong máy ảo blockchain khớp với một ngôn ngữ lập trình cấp cao.

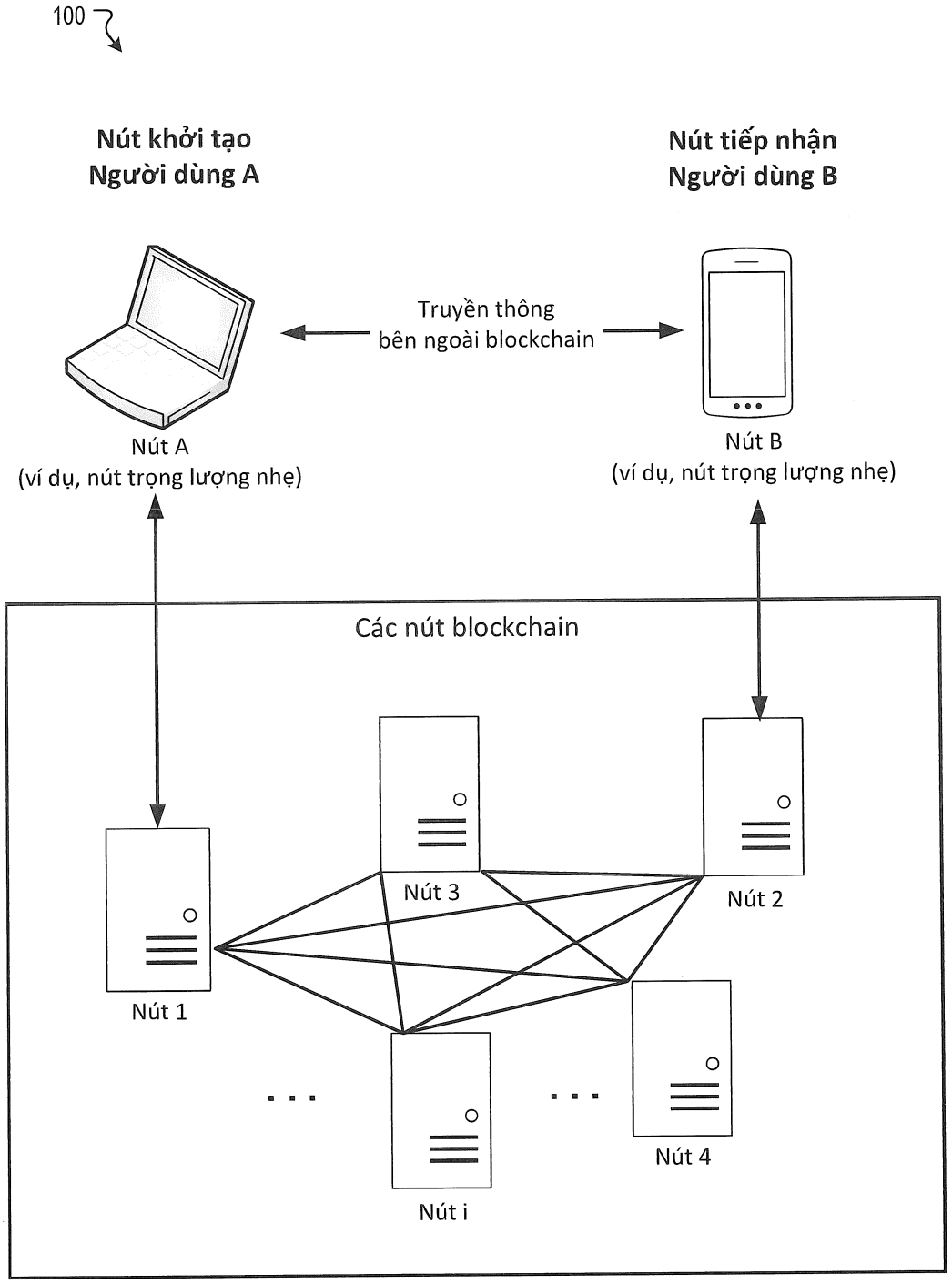

100
Nút khởi tạo
Người dùng A
Nút tiếp nhận
Người dùng B
Truyền thông
bên ngoài blockchain
Nút A
(ví dụ, nút trọng lượng nhẹ)
Nút B
(ví dụ, nút trọng lượng nhẹ)
Các nút blockchain
Nút 1
Nút 2
Nút 3
Nút 4
Nút i

FIG. 1A

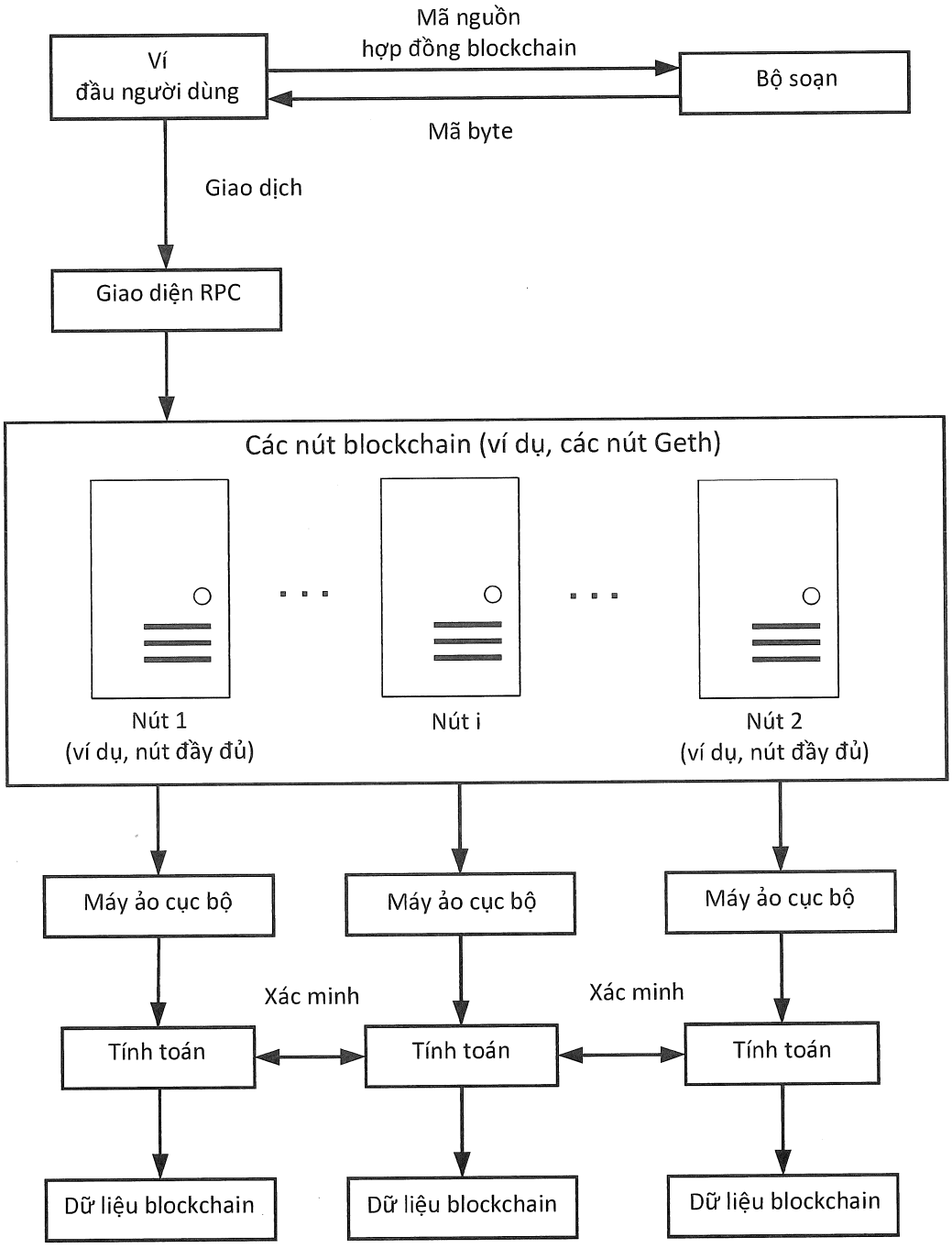

Mã nguồn
hợp đồng blockchain
Ví
đầu người dùng
Bộ soạn
Mã byte
Giao dịch
Giao diện RPC
Các nút blockchain (ví dụ, các nút Geth)
Nút 1
(ví dụ, nút đầy đủ)
Nút i
Nút 2
(ví dụ, nút đầy đủ)
Máy ảo cục bộ
Máy ảo cục bộ
Máy ảo cục bộ
Xác minh
Xác minh
Tính toán
Tính toán
Tính toán
Dữ liệu blockchain
Dữ liệu blockchain
Dữ liệu blockchain

FIG. 1B

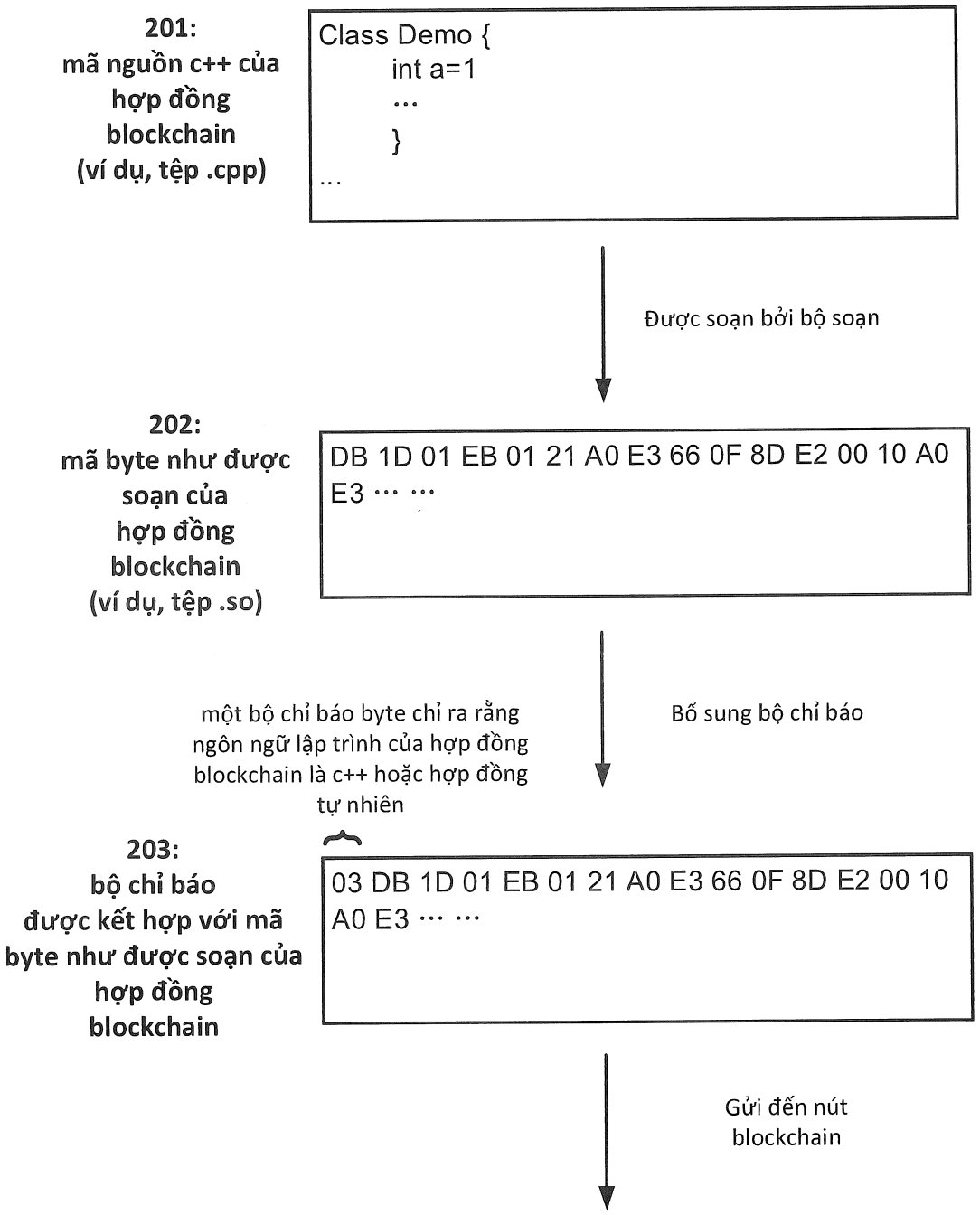

201:
mã nguồn c++ của
hợp đồng
blockchain
(ví dụ, tệp .cpp)
Class Demo {
int a=1
…
}
…
Được soạn bởi bộ soạn
202:
mã byte như được
soạn của
hợp đồng
blockchain
(ví dụ, tệp .so)
DB 1D 01 EB 01 21 A0 E3 66 0F 8D E2 00 10 A0
E3 … …
một bộ chỉ báo byte chỉ ra rằng
ngôn ngữ lập trình của hợp đồng
blockchain là c++ hoặc hợp đồng
tự nhiên
Bổ sung bộ chỉ báo
203:
bộ chỉ báo
được kết hợp với mã
byte như được soạn của
hợp đồng
blockchain
03 DB 1D 01 EB 01 21 A0 E3 66 0F 8D E2 00 10
A0 E3 … …
Gửi đến nút
blockchain

FIG. 2

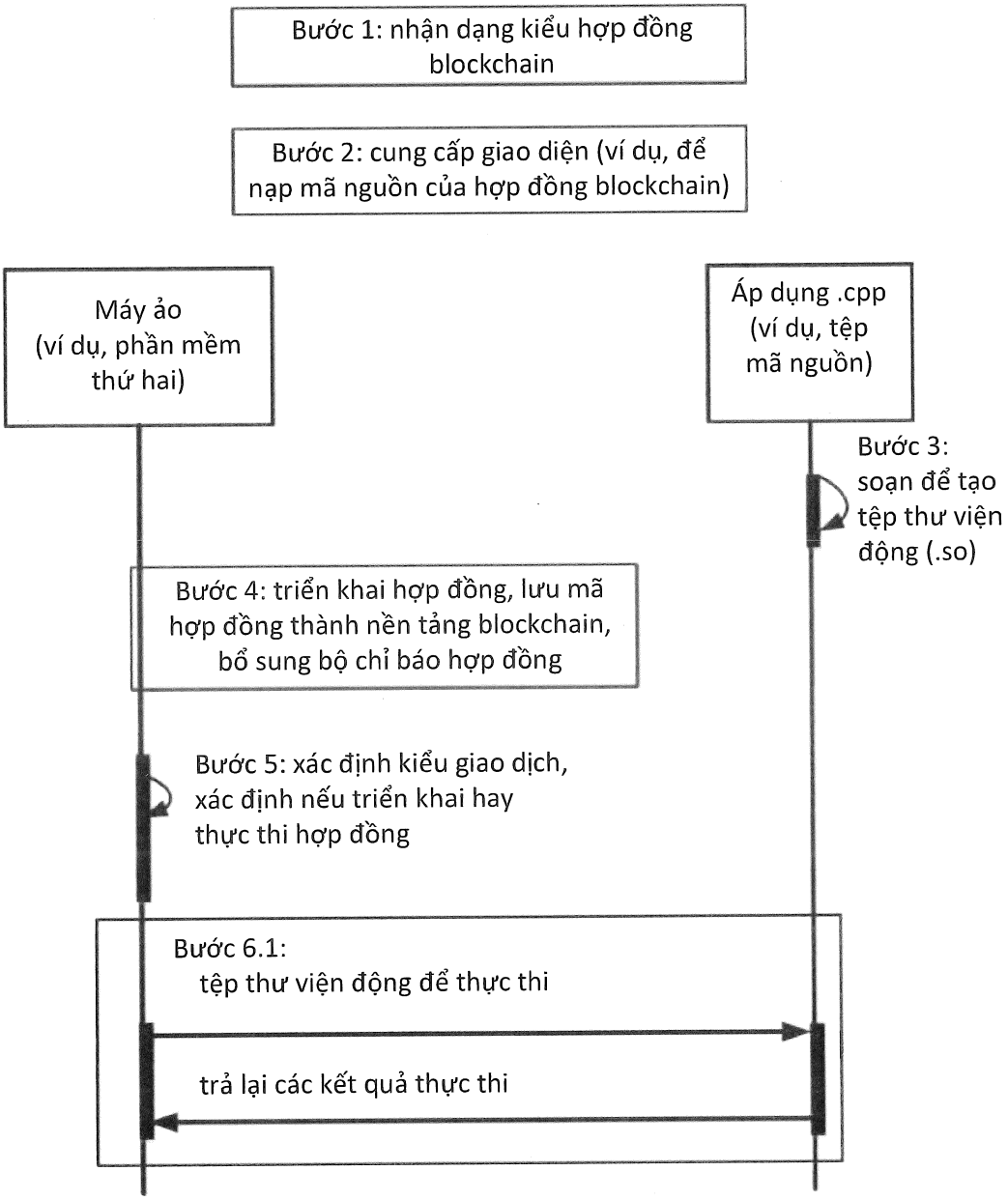

Bước 1: nhận dạng kiểu hợp đồng blockchain
Bước 2: cung cấp giao diện (ví dụ, để nạp mã nguồn của hợp đồng blockchain)
Máy ảo (ví dụ, phần mềm thứ hai)
Áp dụng .cpp (ví dụ, tệp mã nguồn)
Bước 3: soạn để tạo tệp thư viện động (.so)
Bước 4: triển khai hợp đồng, lưu mã hợp đồng thành nền tảng blockchain, bổ sung bộ chỉ báo hợp đồng
Bước 5: xác định kiểu giao dịch, xác định nếu triển khai hay thực thi hợp đồng
Bước 6.1: tệp thư viện động để thực thi
trả lại các kết quả thực thi

FIG. 3A

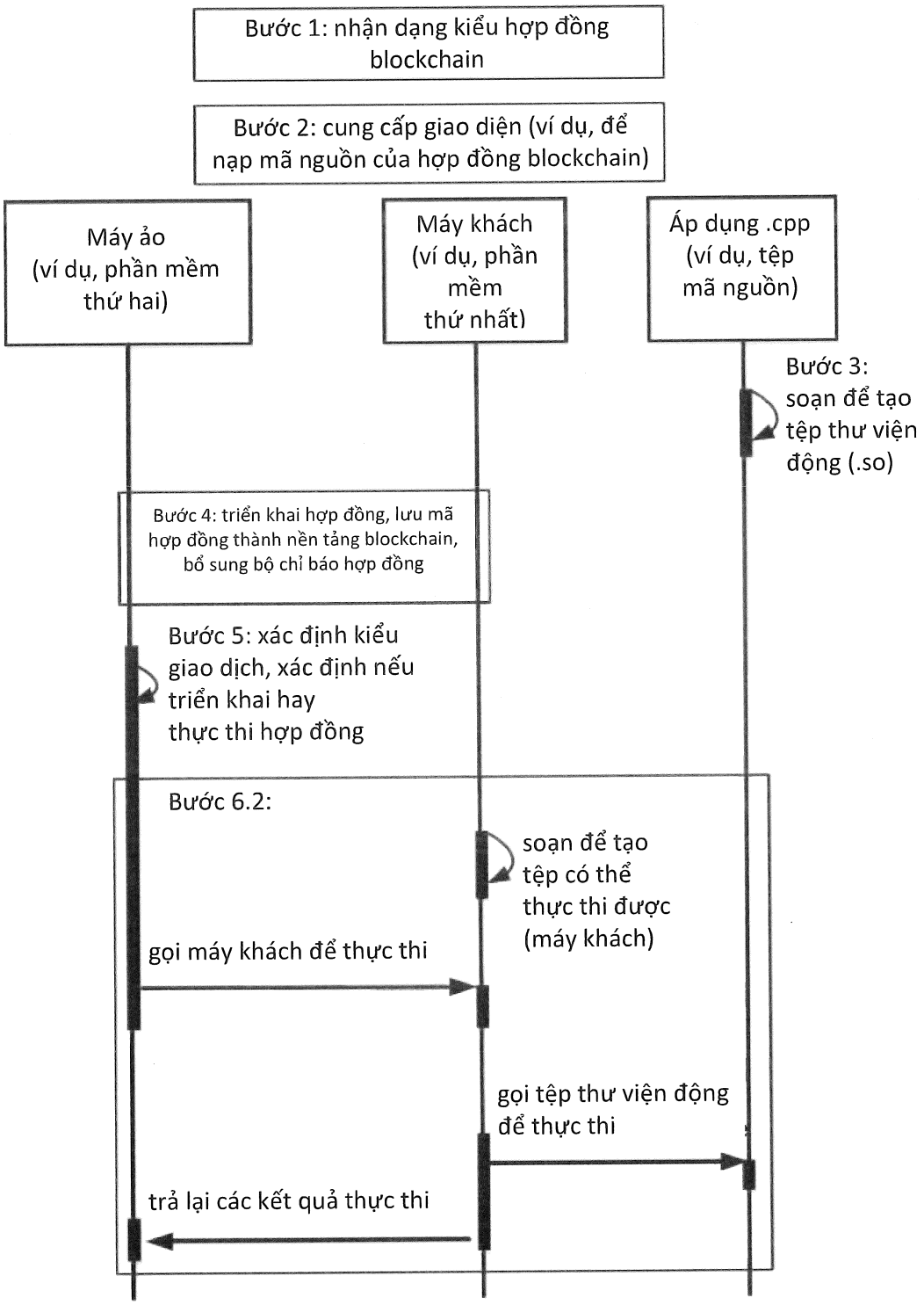

Bước 1: nhận dạng kiểu hợp đồng blockchain
Bước 2: cung cấp giao diện (ví dụ, để nạp mã nguồn của hợp đồng blockchain)
Máy ảo (ví dụ, phần mềm thứ hai)
Máy khách (ví dụ, phần mềm thứ nhất)
Áp dụng .cpp (ví dụ, tệp mã nguồn)
Bước 3: soạn để tạo tệp thư viện động (.so)
Bước 4: triển khai hợp đồng, lưu mã hợp đồng thành nền tảng blockchain, bổ sung bộ chỉ báo hợp đồng
Bước 5: xác định kiểu giao dịch, xác định nếu triển khai hay thực thi hợp đồng
Bước 6.2:
soạn để tạo tệp có thể thực thi được (máy khách)
gọi máy khách để thực thi
gọi tệp thư viện động để thực thi
trả lại các kết quả thực thi

FIG. 3B

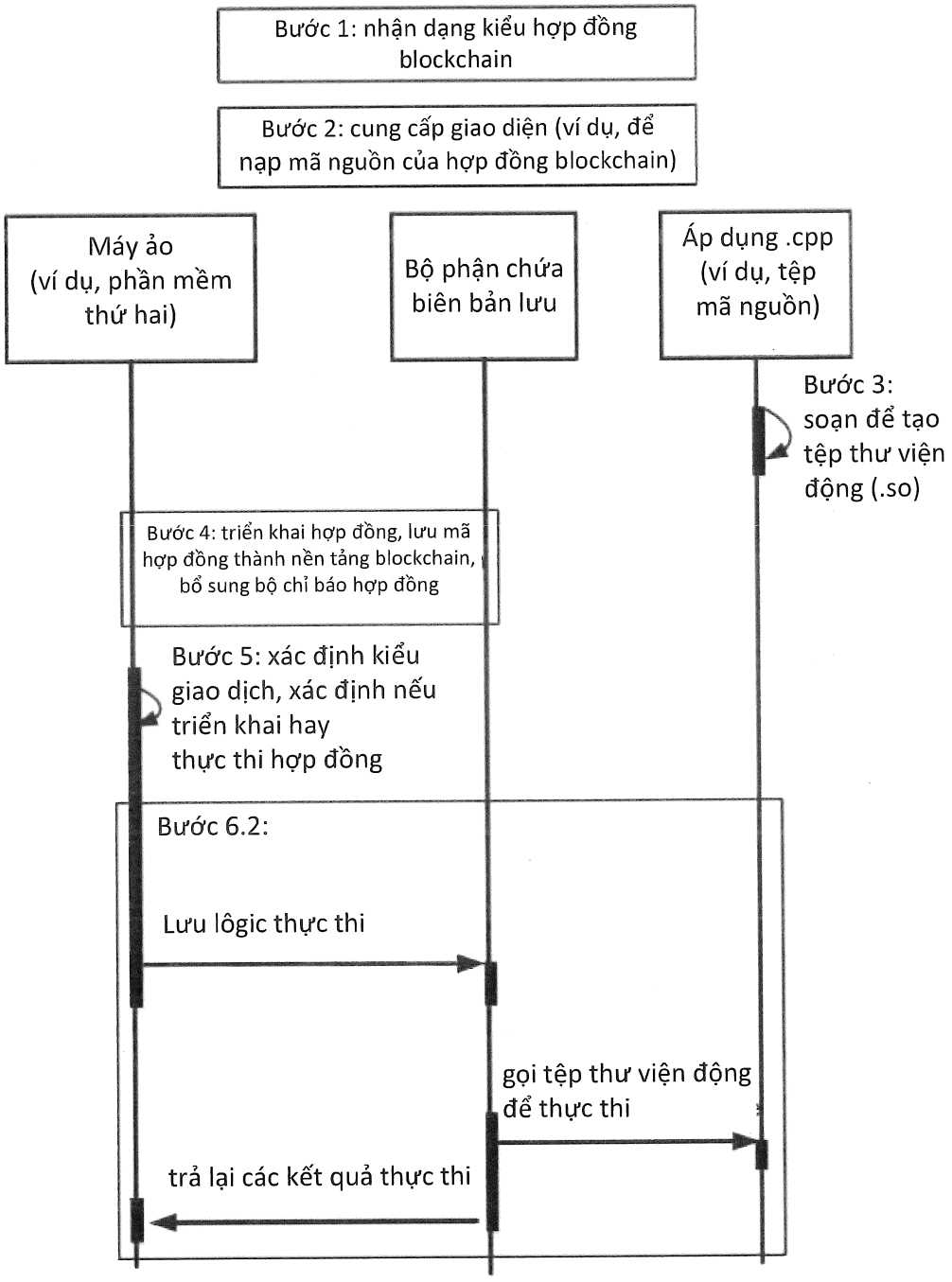

Bước 1: nhận dạng kiểu hợp đồng blockchain
Bước 2: cung cấp giao diện (ví dụ, để nạp mã nguồn của hợp đồng blockchain)
Máy ảo (ví dụ, phần mềm thứ hai)
Bộ phận chứa biên bản lưu
Áp dụng .cpp (ví dụ, tệp mã nguồn)
Bước 3: soạn để tạo tệp thư viện động (.so)
Bước 4: triển khai hợp đồng, lưu mã hợp đồng thành nền tảng blockchain, bổ sung bộ chỉ báo hợp đồng
Bước 5: xác định kiểu giao dịch, xác định nếu triển khai hay thực thi hợp đồng
Bước 6.2:
Lưu lôgic thực thi
gọi tệp thư viện động để thực thi
trả lại các kết quả thực thi

FIG. 3C

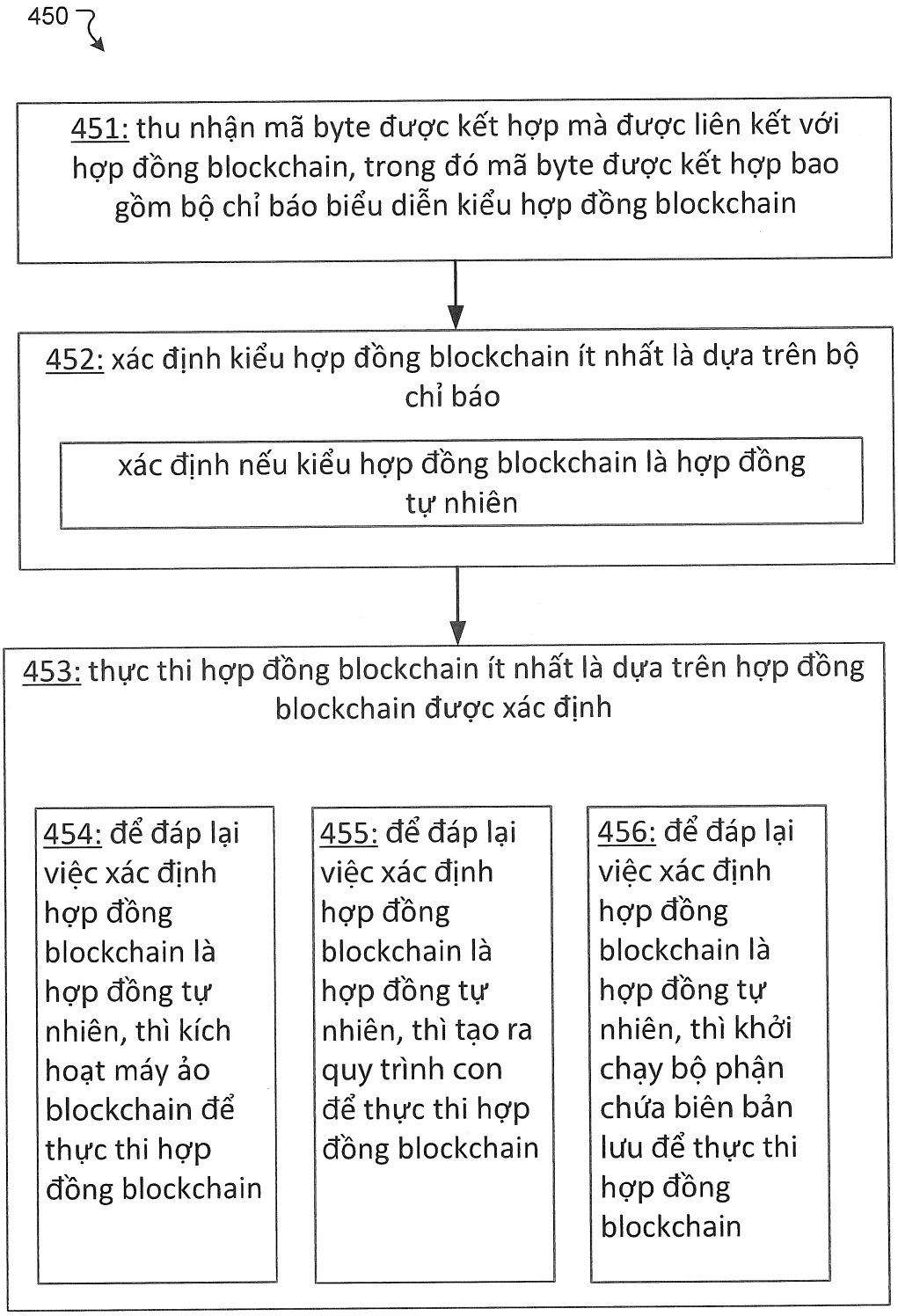

450
451: thu nhận mã byte được kết hợp mà được liên kết với hợp đồng blockchain, trong đó mã byte được kết hợp bao gồm bộ chỉ báo biểu diễn kiểu hợp đồng blockchain
452: xác định kiểu hợp đồng blockchain ít nhất là dựa trên bộ chỉ báo
xác định nếu kiểu hợp đồng blockchain là hợp đồng tự nhiên
453: thực thi hợp đồng blockchain ít nhất là dựa trên hợp đồng blockchain được xác định
454: để đáp lại việc xác định hợp đồng blockchain là hợp đồng tự nhiên, thì kích hoạt máy ảo blockchain để thực thi hợp đồng blockchain
455: để đáp lại việc xác định hợp đồng blockchain là hợp đồng tự nhiên, thì tạo ra quy trình con để thực thi hợp đồng blockchain
456: để đáp lại việc xác định hợp đồng blockchain là hợp đồng tự nhiên, thì khởi chạy bộ phận chứa biên bản lưu để thực thi hợp đồng blockchain

FIG. 4

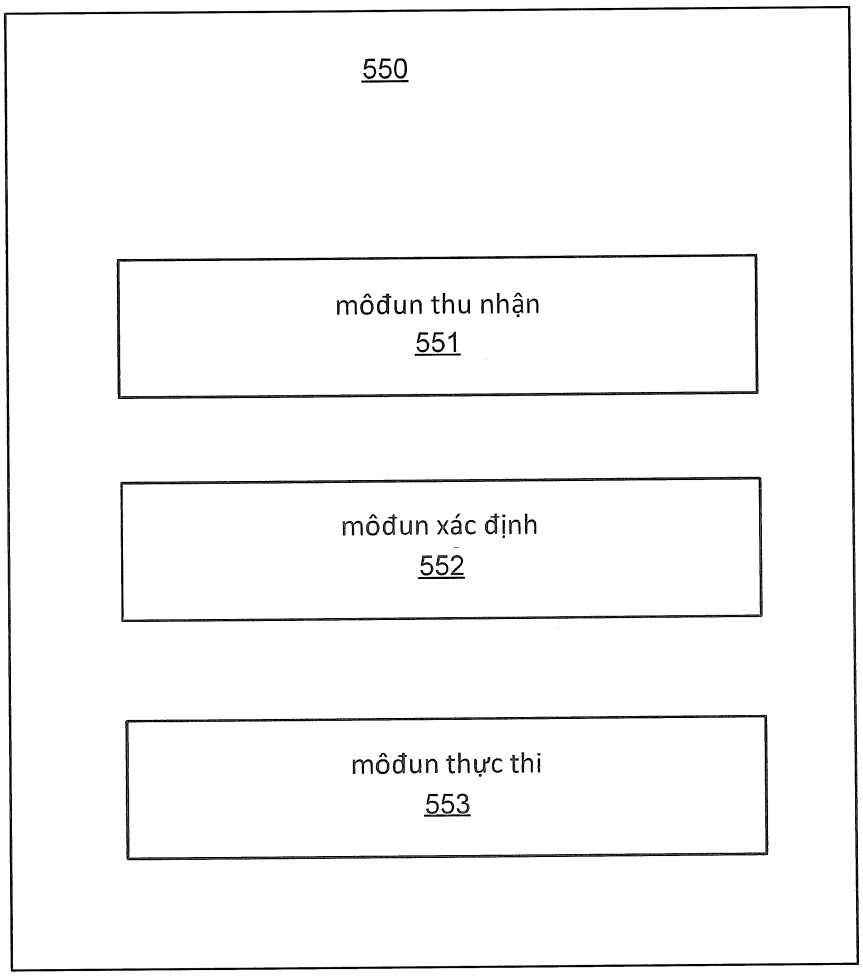


FIG. 5

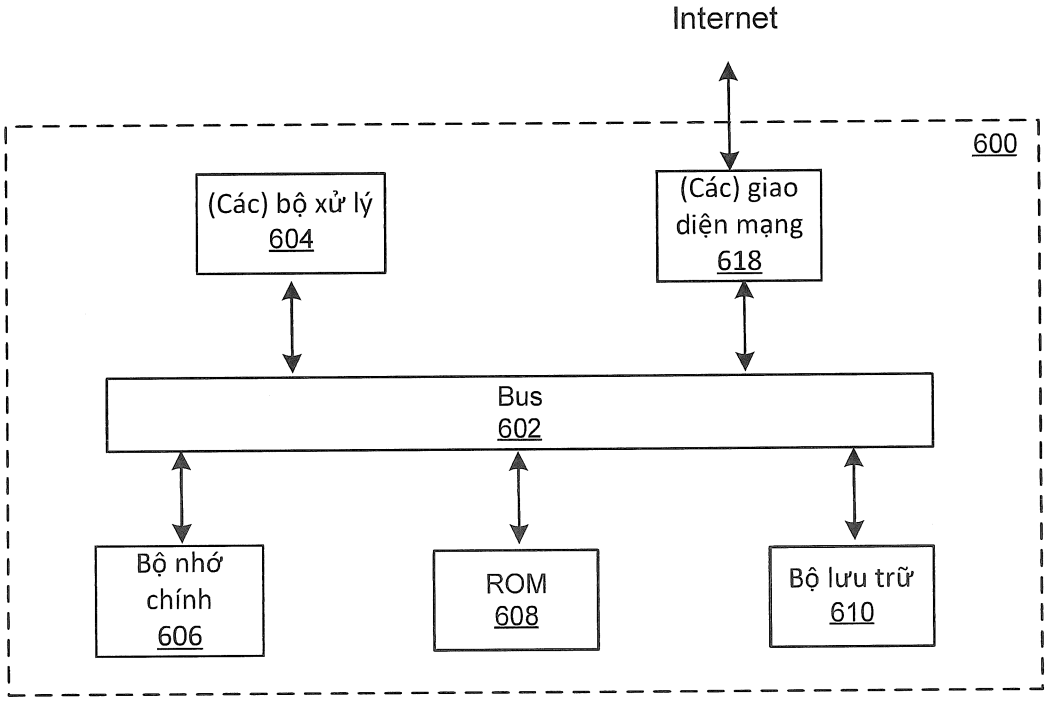

Internet
600
(Các) bộ xử lý
604
(Các) giao diện mạng
618
Bus
602
Bộ nhớ chính
606
ROM
608
Bộ lưu trữ
610

FIG. 6