

BLOCKCHAIN - ỨNG DỤNG TRONG VIỆC KHAI THÁC DỊCH VỤ CHUYỂN VÙNG VIỄN THÔNG

Võ Minh Đức^{1*}, Nguyễn Mậu Hân²

¹ VNPT Phú Yên, Tập đoàn Bưu chính Viễn thông Việt Nam

² Trường Đại học Khoa học, Đại học Huế

*Email: duc.pyn@gmail.com

Ngày nhận bài: 6/4/2020; ngày hoàn thành phản biện: 20/4/2020; ngày duyệt đăng: 14/7/2020

TÓM TẮT

Blockchain là một công nghệ cho phép truyền tải dữ liệu một cách an toàn dựa vào hệ thống mã hoá vô cùng phức tạp, tương tự như cuốn sổ cái kế toán của một công ty, nơi mà mọi hoạt động liên quan đến tiền bạc của công ty được giám sát một cách chặt chẽ. Vài năm gần đây, công nghệ blockchain 3.0 đã vượt khỏi biên giới của lĩnh vực tài chính – tiền tệ và thâm nhập đa dạng vào các lĩnh vực khác. Blockchain mở ra cơ hội cho ngành viễn thông nâng cao hiệu quả quản lý khai thác mạng lưới, kinh doanh và giao dịch các loại tài sản số như các dịch vụ nội dung, quản lý chuỗi cung ứng bằng hợp đồng thông minh, đặc biệt là an ninh mạng và ngăn chặn gian lận. Trên cơ sở đó, bài báo này đề xuất phương pháp giải quyết vấn nạn gian lận chuyển vùng quốc tế trong lĩnh vực thông tin truyền thông bằng công nghệ blockchain nhằm tăng cường hiệu quả trong việc quản lý, khai thác dịch vụ chuyển vùng viễn thông.

Từ khóa: blockchain, chuyển vùng, viễn thông.

1. MỞ ĐẦU

Công nghệ blockchain không phải là một phát minh mới lạ mà là sự kết hợp giữa 3 loại công nghệ đã tồn tại qua nhiều năm: mạng ngang hàng [1], lý thuyết mật mã [2] và lý thuyết trò chơi [3]. Blockchain được sử dụng trong việc lưu trữ thông tin trong các khối thông tin được liên kết với nhau và được quản lý bởi tất cả mọi người tham gia hệ thống. Blockchain được tạo ra để chống lại sự thay đổi dữ liệu trong hệ thống, không thể làm giả, không thể phá hủy sự liên kết giữa các khối thông tin. Thông tin khi được nhập vào trong chuỗi khối blockchain thì sẽ không thể thay đổi và chỉ được bổ sung thêm thông tin khi có sự đồng thuận của tất cả các bên trong hệ thống. Các loại công nghệ được sử dụng trong blockchain là:

Mật mã học: Sử dụng public key trong chữ ký số và giá trị băm của hash function để đảm bảo tính minh bạch, toàn vẹn và riêng tư.

Mạng ngang hàng: Một hệ thống mạng mà mỗi nút trong mạng có vai trò như nhau, tự quản lý tài nguyên của mình. Một nút được xem như một client và cũng là server để lưu trữ bản sao dữ liệu.

Lý thuyết trò chơi: Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (PoW, PoS...) và được thúc đẩy bởi động lực xác định trước [4].

Công nghệ blockchain đóng vai trò giống như một cuốn sổ cái ghi lại tất cả các giao dịch xảy ra trong hệ thống và có các đặc điểm chính có thể kể đến như:

Tính bất biến: Blockchain hoạt động theo nguyên tắc không thoái thác và không thể đảo ngược giao dịch. Blockchain là bất biến bởi vì một khi dữ liệu đã được ghi vào sổ cái, không ai có thể bí mật thay đổi dữ liệu cũ mà không bị mạng phát hiện [5] (tức là, blockchain có khả năng chống giả mạo). Tính bất biến được bảo đảm nhờ sử dụng các thuật toán băm.

Bảo mật: Người dùng chỉ có thể chuyển dữ liệu nếu họ sở hữu khóa riêng. Khóa riêng được sử dụng để tạo chữ ký cho mỗi giao dịch blockchain mà người dùng gửi đi. Chữ ký này xác nhận rằng giao dịch đã đến từ người dùng và cũng để giữ cho giao dịch không bị thay đổi bởi bất cứ ai một khi nó đã được phát hành [5].

Tính minh bạch: Các bản ghi trên blockchain có thể được kiểm tra bởi các bên tham gia được xác định trước [5]. Ví dụ, trong các blockchain công khai, tất cả mọi người có kết nối Internet đều có quyền truy cập vào sổ cái và kiểm tra mọi giao dịch.

Hợp đồng thông minh: Là các hợp đồng được viết thành mã máy tính hoạt động trên blockchain, nó bảo đảm tất cả các bên tham gia đều biết được chi tiết hợp đồng và các điều khoản sẽ được tự động thực hiện một khi các điều kiện được bảo đảm mà không cần bên thứ ba can thiệp [6].

2. PHƯƠNG PHÁP NGHIÊN CỨU

Trên cơ sở các khối kiến thức đã có như lý thuyết mật mã, mạng ngang hàng và lý thuyết trò chơi, phương pháp nghiên cứu được sử dụng trong bài báo là tìm hiểu dự án Hyperledger Fabric (HF) [8], một dự án của Linux Foundation khởi động vào năm 2016 nhằm mục đích thúc đẩy các công nghệ blockchain công nghiệp phát triển. HF cũng hỗ trợ việc ứng dụng blockchain để thiết lập bộ khung sổ cái phân tán cấp doanh nghiệp và dự án này đang là một trong 8 dự án được triển khai với sự góp sức của IBM và Digital Asset. Ở đây, chúng tôi sử dụng giải pháp mã nguồn mở của IBM, bằng cách sử dụng một hợp đồng chuyên vùng thông minh trên HF nhằm chi phối giao dịch giữa

thuê bao di động và các nhà mạng để phục vụ quản lý, giám sát, tính cước sử dụng dịch vụ viễn thông [9].

3. NỀN TẢNG BLOCKCHAIN HYPERLEDGER FABRIC

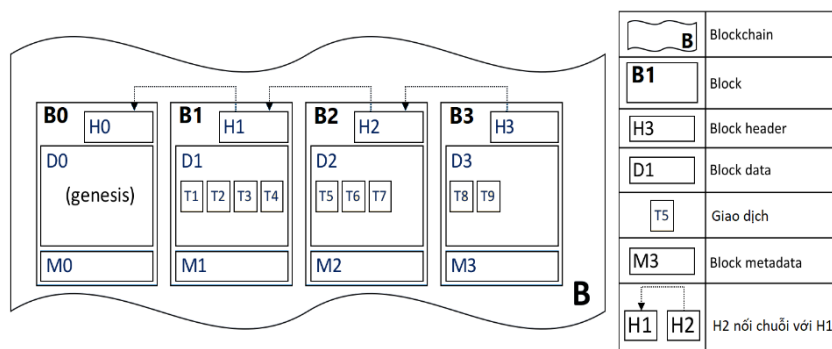
Dự án Hyperledger ra đời nhằm mục đích thúc đẩy và phát triển các công nghệ blockchain công nghiệp. Thay vì tuyên bố một chuẩn blockchain duy nhất, Hyperledger khuyến khích cách tiếp cận hợp tác để phát triển nhiều công nghệ blockchain khác nhau thông qua quy trình cộng đồng, nguồn mở. HF là một trong những dự án con trong Hyperledger và thuộc loại blockchain có cấp quyền (permissioned), nghĩa là các thành viên tham gia mạng phải đăng ký qua một nhà cung cấp dịch vụ thành viên (MSP- Membership Service Provider). Trong HF, dữ liệu sổ cái có thể được lưu ở nhiều định dạng khác nhau, các cơ chế đồng thuận có thể được hoán đổi, và các MSP khác nhau được hỗ trợ. HF cung cấp khả năng tạo kênh [8], cho phép một nhóm người tham gia kênh và chỉ những người này mới có bản sao của sổ cái trên kênh đó.

3.1 Sổ cái chia sẻ

HF có phân hệ sổ cái bao gồm hai phần: world-state và log giao dịch. Phần world-state mô tả trạng thái của sổ cái tại thời điểm hiện hành, nó là database lưu trữ các bản ghi dưới dạng key-value (hiện tại cho phép tùy chọn dùng LevelDB hoặc CouchDB). Phần log giao dịch ghi lại tất cả các giao dịch đưa đến giá trị hiện tại của world-state, nó chính là chuỗi các block liên kết nhau đang sử dụng bởi kênh (hình 1).

3.2 Cấu trúc block

Block được tạo thành từ bộ các giao dịch, mỗi giao dịch là một yêu cầu cập nhật sổ cái. Mỗi block có 3 phần chính:



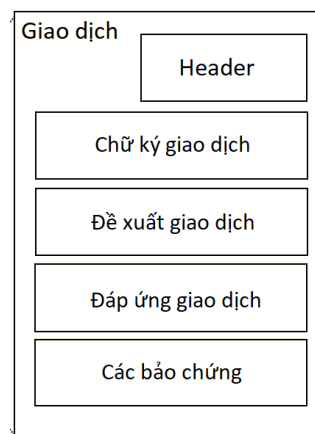
Hình 1. Ví dụ blockchain B gồm 4 block

- Header, gồm các trường: số hiệu block bắt đầu từ 0 và tăng dần; giá trị băm của block hiện tại; giá trị băm của header block kề trước.
- Data: gồm một tập danh sách các giao dịch đã được sắp xếp.
- Metadata: bao gồm các metadata như: timestamp khi block được ghi, chứng chỉ số, public-key và chữ ký số của bên ghi block.

3.3 Cấu trúc một giao dịch

Mỗi giao dịch có cấu trúc như hình 2, bao gồm:

- Header: bao gồm một số metadata chứa tên chaincode và phiên bản
- Chữ ký: chữ ký số của ứng dụng yêu cầu thực hiện giao dịch.
- Đề xuất (Proposal): chứa danh sách các tham số đầu vào do ứng dụng đưa ra để gọi một hàm nào đó trong chaincode.
- Đáp ứng (Response): kết quả đầu ra của chaincode, là tập đọc/ghi (RW-set).
- Các bảo chứng (Endorsements): danh sách các phản hồi đề xuất giao dịch được tính toán từ các nút ngang hàng có trong chính sách chứng thực.



Hình 2. Cấu trúc một giao dịch

3.4 Hợp đồng thông minh

Hợp đồng thông minh trong HF là một tập các hàm được gọi là chaincode và được một ứng dụng bên ngoài blockchain gọi khi ứng dụng đó cần tương tác cập nhật số cái. Trong hầu hết các trường hợp, chaincode chỉ tương tác với thành phần world-state database của sổ cái chứ không phải nhật ký giao dịch. Chaincode có thể được viết bởi một trong số các ngôn ngữ lập trình như Go, Java, Node.

3.5 Quyền riêng tư

Đối với các mạng public, quyền riêng tư không phải là mối quan tâm hàng đầu mà tùy thuộc vào nhu cầu sử dụng mạng. Ngược lại, những người tham gia mạng giữa các doanh nghiệp (B2B-Business to Business) có thể cực kỳ nhạy cảm về lượng thông tin họ chia sẻ. HF hỗ trợ các mạng trong đó đảm bảo quyền riêng tư bằng cách sử dụng các kênh là một yêu cầu then chốt cùng với việc mạng chỉ mở một cách tương đối.

4. ỨNG DỤNG KHAI THÁC DỊCH VỤ CHUYỂN VÙNG QUỐC TẾ

4.1 Bài toán đặt ra

Trong lĩnh vực viễn thông di động, chuyển vùng (roaming) quốc tế là một trong những dịch vụ mang lại doanh thu rất cao. Các công ty viễn thông ở các quốc gia thường có thỏa thuận ăn chia về chuyển vùng với nhau để cung cấp dịch vụ đến khách hàng. Chuyển vùng quốc tế cho phép thuê bao của một mạng di động trong nước khi đi ra nước ngoài vẫn sử dụng được các dịch vụ một cách bình thường thông qua các

mạng di động ở nước sở tại. Tuy nhiên đây cũng là dịch vụ thường bị tấn công gian lận để chiếm đoạt doanh thu cước phí.

Gian lận chuyển vùng diễn ra khi thuê bao di động chuyển vùng và gây phát sinh cước phí lớn nhưng không có ý định thanh toán [7] cho nhà mạng thường trú HPMN (Home Public Mobile Network). Kẻ gian lận có được các SIM card bằng nhiều cách như đánh cắp, nhân bản hoặc đăng ký thuê bao giả mạo và mang ra nước ngoài chuyển vùng để sử dụng cho các giao dịch có mức cước phí cao như gọi quốc tế hoặc truy cập các dịch vụ nội dung giá cao. HPMN không thu được cước phí của thuê bao gian lận nhưng vẫn phải chi trả doanh thu kết nối cho đối tác chuyển vùng.

Hành vi gian lận chuyển vùng quốc tế lợi dụng thời gian trễ trong cơ chế trao đổi đối soát dữ liệu giữa nhà mạng thường trú và nhà mạng tạm trú. Bản ghi chi tiết (CDR-Call Detail Records) của thuê bao chuyển vùng được ghi bởi nhà mạng tạm trú VPMN (Visited Public Mobile Network) và sau một chu kỳ thời gian được tập hợp về một trung tâm thanh toán bù trừ DCH (Data Clearing House) [7]. DCH chuyển file số liệu cho HPMN để thực hiện đối soát và tính cước, quy trình này có thể mất đến một tuần. Như vậy khi HPMN phát hiện được thuê bao gian lận để ngăn chặn thì thiệt hại đã khá lớn.

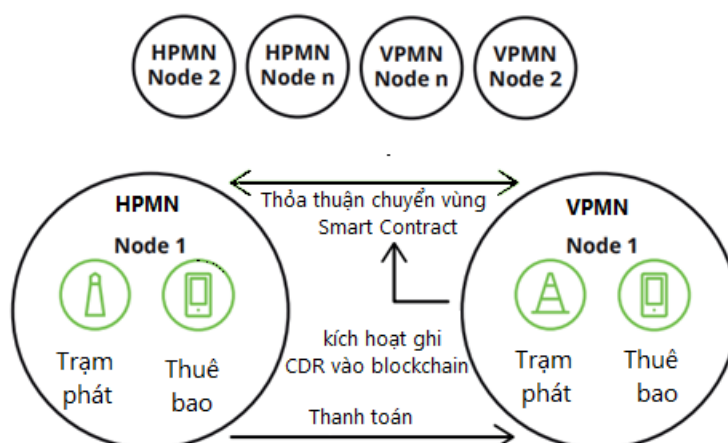
Chống gian lận dịch vụ chuyển vùng là một trong những ưu tiên trong ngành viễn thông di động và đây thực sự là một cuộc chiến chưa có hồi kết. Nhiều tổ chức đã đưa ra một số kỹ thuật và tiêu chuẩn nhằm rút ngắn khung thời gian trao đổi bản ghi chi tiết cuộc gọi xuống còn 4 giờ đã giúp hạn chế bớt nhiều vụ gian lận lớn. Tuy nhiên bất chấp sáng kiến này, nếu một nhóm gian lận dùng một cụm vài chục thẻ SIM thì chúng vẫn có thể gây ra nhiều thiệt hại trong vòng 4 giờ, với mức tổn thất dao động từ 50 đến 100 nghìn USD [10].

4.2 Hướng giải quyết dựa trên công nghệ blockchain

Blockchain có thể làm thay đổi sâu sắc ngành công nghiệp viễn thông. Tổ chức tư vấn quốc tế Deloitte đã nêu ra 4 trường hợp sử dụng có thể ứng dụng blockchain: quản lý gian lận, dịch vụ cung cấp xác định danh tính, triển khai 5G và kết nối IoT [11]. Đối với phòng chống gian lận chuyển vùng có thể sử dụng các biện pháp sau:

4.2.1 Triển khai thỏa thuận chuyển vùng bằng smart contract

Một blockchain cấp phép có thể triển khai giữa các nhà mạng. Thỏa thuận chuyển vùng giữa HPMN và VPMN được thực thi dưới dạng một hợp đồng thông minh sẽ được kích hoạt khi có một giao dịch mạng dữ liệu CDR được phát trên mạng blockchain như trong hình 3.



Hình 3. Minh họa sử dụng hợp đồng chuyển vùng thông minh

Hành vi chuyển vùng của một thuê bao trong mạng VPMN sẽ kích hoạt một hợp đồng thông minh và các điều khoản của thỏa thuận chuyển vùng sẽ được tự động thực thi. Do đó, thông tin chi tiết cuộc gọi và cước phí phải trả được ghi nhận tức thời trên blockchain. Điều này giúp xác minh cũng như giải quyết gian lận ngay trong các điều khoản của hợp đồng thông minh dựa trên blockchain. Các nhà khai thác cũng có thể loại bỏ vai trò trung gian của tổ chức DCH để tiết kiệm chi phí.

4.2.2 Nhận dạng thuê bao bằng public key

Mã hóa khóa công khai – khóa riêng được kế thừa trong blockchain có thể dùng để xác định một thiết bị và liên kết thiết bị đó với một danh tính của thuê bao. Thay vì phải phát số IMSI (International Mobile Subscriber Identity) lên mạng để xác định thiết bị, khóa công khai của điện thoại được sẽ được gửi lên mạng. Thiết bị lưu giữ bảo mật khóa riêng, bất kỳ ai khác đều không thể biết khóa riêng của thiết bị.

Giải pháp “eSIM” này có thể giúp bảo vệ thông tin riêng được mã hóa trong khóa riêng. Khóa riêng được liên kết với chỉ một thiết bị cụ thể và do đó rất khó bị đánh cắp. Khóa công khai được sử dụng để xác định thiết bị và cấp quyền cho thiết bị trên mạng. Thuê bao được định danh bằng khóa công khai này, trong khi có thể giữ bí mật thông tin khóa riêng. Bằng cách này, các dịch vụ chỉ có thể được sử dụng bởi thuê bao đã đăng ký.

4.3 Xây dựng hệ thống khai thác dịch vụ chuyển vùng

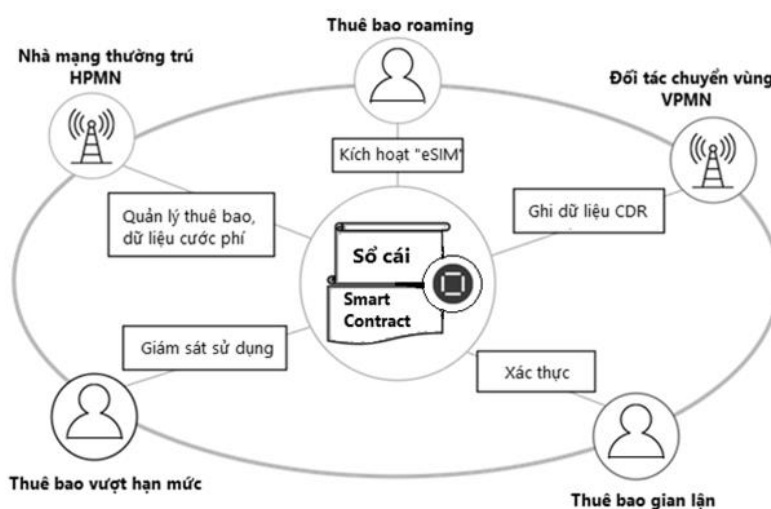
Tháng 9/2018, IBM công bố mã nguồn mở một hợp đồng thông minh mẫu trên HF dành cho chuyển vùng viễn thông [9], gồm một số hàm phục vụ các giao dịch giám sát, kết nối và tính cước dịch vụ đàm thoại cho thuê bao chuyển vùng. Dựa trên mẫu mã nguồn này, chúng tôi điều chỉnh nghiệp vụ xử lý đối với dịch vụ thoại cho phù hợp với thực tế của doanh nghiệp, đồng thời bổ sung xử lý cho các dịch vụ chuyển vùng khác gồm dịch vụ nhắn tin ngắn (SMS) và dịch vụ dữ liệu (mobile broadband).

Hệ thống khai thác dịch vụ chuyển vùng này có những lợi ích sau:

- Tự động kích hoạt và thực thi hợp đồng chuyển vùng giữa HPMN và VPMN theo hành vi của thuê bao.
- Cho phép xử lý tính cước gần như tức thời, loại bỏ các quy trình của bên thứ ba gây tổn kém (loại bỏ các tổ chức DCH).
- Cung cấp kho lưu trữ các giao dịch để dàng kiểm chứng giữa các nhà mạng.
- Quản lý định danh hiệu quả để giảm thiểu gian lận đăng ký và chuyển vùng.
- Cảnh báo theo thời gian thực về các vấn đề vượt mức sử dụng dữ liệu / cuộc gọi giữa các bên, dẫn đến sự hài lòng của khách hàng tăng lên.

4.3.1 Biểu đồ ngữ cảnh hệ thống khai thác chuyển vùng

Các nhà cung cấp dịch vụ viễn thông di động sẽ tham gia vào một mạng blockchain HF (hình 4). Trái tim của mô hình này là một hợp đồng thông minh chi phối các tương tác giữa thuê bao di động và nhà mạng viễn thông. Mỗi nhà mạng đều có các bản sao sổ cái như nhau, thông tin được trao đổi và cập nhật tức thời bằng các giao dịch không thể đảo ngược. Các tác nhân chính gồm có:



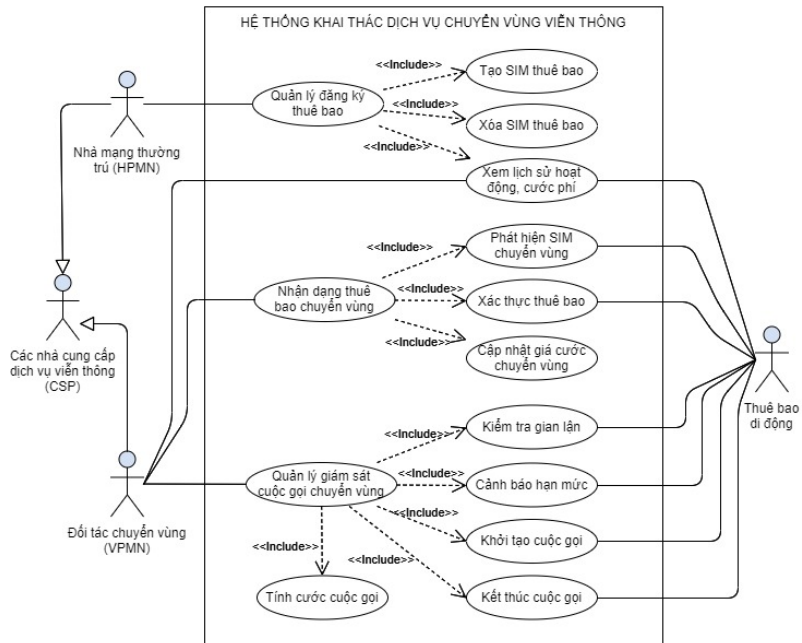
Hình 4. Biểu đồ ngữ cảnh hệ thống khai thác chuyển vùng

- Các nhà cung cấp dịch vụ viễn thông CSP (Communication Service Providers): Tùy theo ngữ cảnh đối với thuê bao di động, một CSP có thể đóng vai trò là nhà mạng thường trú hoặc là đối tác chuyển vùng.
- Các SIM thuê bao di động (SubscriberSim): Hiểu đơn giản mỗi thuê bao được đại diện bởi một khóa công khai kèm theo số điện thoại di động. Thuê bao có thể là chuyển vùng hợp pháp, thuê bao đang vượt hạn mức sử dụng hoặc là thuê bao gian lận.

4.3.2 Các chức năng của hệ thống

Các chức năng của hệ thống gồm có:

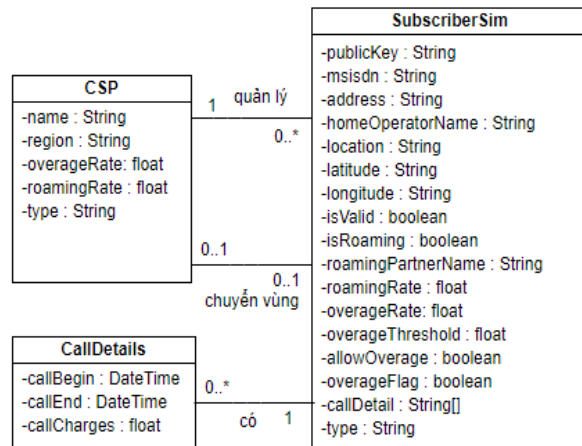
- Quản lý đăng ký thuê bao: tạo SIM thuê bao; Xóa SIM thuê bao; Xem lịch sử hoạt động cước phí.
- Nhận dạng thuê bao chuyển vùng: Phát hiện SIM chuyển vùng; Xác thực thuê bao; Cập nhật giá cước chuyển vùng.
- Quản lý giám sát cuộc gọi chuyển vùng: Kiểm tra gian lận; Cảnh báo hạn mức; Khởi tạo cuộc gọi; Tính cước cuộc gọi; Kết thúc cuộc gọi.



Hình 5. Các chức năng của hệ thống được mô tả qua biểu đồ Use Case

4.3.3 Cơ sở dữ liệu (CSDL) của hệ thống

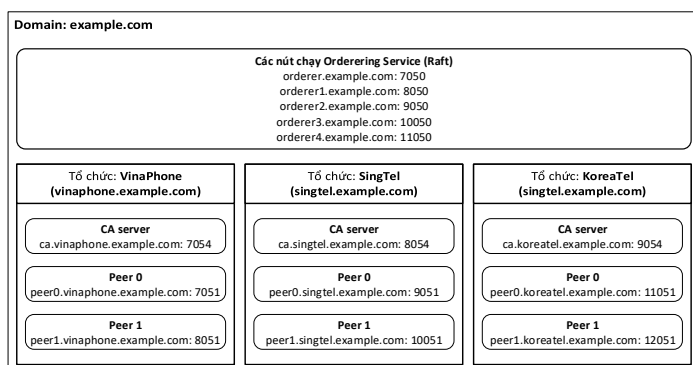
CSDL của hệ thống được mô tả qua biểu đồ lớp như hình 6. Trong đó Lớp SubscriberSim đại diện cho SIM thuê bao. Thuê bao phải đăng ký được quản lý bởi một nhà mạng thường trú (HPMN). Khi thuê bao chuyển vùng, thuê bao được phục vụ bởi một nhà mạng đối tác (VPMN). Các nhà mạng được biểu diễn chung bởi lớp các nhà cung cấp dịch vụ viễn thông (CSP). Các bản ghi chi tiết cuộc gọi đã thực hiện của thuê bao được biểu diễn bởi lớp CallDetails.



Hình 6. CSDL của hệ thống được mô tả qua biểu đồ lớp

4.4 Kết quả cài đặt thử nghiệm

Chúng tôi cài đặt mô hình mạng HF thử nghiệm với giả định 03 CSP khác nhau có thỏa ước chuyển vùng quốc tế, gồm Vinaphone (Việt Nam), SingTel (Singapore) và KoreaTel (Hàn Quốc). Mỗi CSP là một tổ chức tham gia vào kênh HF, sở hữu các nút peer ngang hàng và CA riêng để cấp chứng chỉ cho mọi nút, user, ứng dụng thuộc tổ chức mình (hình 7).



Hình 7. Mô hình cài đặt thử nghiệm

Một số kịch bản thử nghiệm kích hoạt các giao dịch quy định trong chaincode đã cài đặt trên kênh HF:

- Khởi tạo cấp phát SIM cho thuê bao: CSP gọi hàm `createSubscriberSim` của chaincode để ghi thông tin thuê bao gồm khóa công khai, số danh bạ, địa chỉ... vào sổ cái.
- Thuê bao di chuyển ra nước ngoài: Trạm phát sóng của CSP đối tác chuyển vùng sẽ kích hoạt hàm `moveSim` của chaincode để cập nhật vị trí mới của SIM. Tiếp theo, hàm `discovery` được kích hoạt để phát hiện thuê bao. Thuê bao được xác thực bằng hàm `authentication` và được cập nhật giá cước gọi chuyển vùng tương ứng bằng hàm `updateRate` của chaincode.
- Thuê bao khởi tạo cuộc gọi chuyển vùng: Tổng đài CSP đối tác gọi hàm `verifyUser` của chaincode để kiểm tra thông tin thuê bao trong sổ cái. Nếu hợp lệ, thuê bao sẽ được phép thực hiện cuộc gọi và hàm `callOut` của chaincode được kích hoạt để bắt đầu ghi cước.
- Thuê bao kết thúc cuộc gọi chuyển vùng: Tổng đài CSP đối tác sẽ gọi hàm `callEnd` của chaincode để cập nhật thời gian kết thúc cuộc gọi trong bản ghi chi tiết CDR và lưu vào sổ cái. Tiếp theo, hàm `callPay` được kích hoạt để yêu cầu chaincode tính tiền cho cuộc gọi dựa trên số liệu CDR của thuê bao.

Toàn bộ lịch sử biến động thông tin, dữ liệu liên quan đến thuê bao qua các giao dịch đều được lưu giữ trên blockchain, trong đó quan trọng nhất là các bản ghi cước chi tiết cuộc gọi CDR được ghi nhận và tính cước tức thời, có thể được truy vấn bởi tất cả các CSP tham gia hệ thống (hình 8).

Key: 0

```
Record: { publicKey: 'sim1_pkey', msisdn: '+8491.8888888', address: 'Hue',  
homeOperatorName: 'VinaPhone', roamingPartnerName: '', isRoaming: 'false', location:  
'Vietnam', latitude: '', longitude: '', roamingRate: '', overageRate: '', callDetails: [], isValid: '',  
overageThreshold: '10.0', allowOverage: '', overageFlag: 'false', type: 'SubscriberSim' }
```

Key: 1

```
Record: { address: 'Hue', allowOverage: '', callDetails: [], homeOperatorName: 'VinaPhone',  
isRoaming: 'false', isValid: '', latitude: '', location: 'Korea', longitude: '', msisdn:  
'+8491.8888888', overageFlag: 'false', overageRate: '', overageThreshold: '10.0', publicKey:  
'sim1_pkey', roamingPartnerName: '', roamingRate: '', type: 'SubscriberSim' }
```

Key: 2

```
Record: { address: 'Hue', allowOverage: '', callDetails: [], homeOperatorName: 'VinaPhone',  
isRoaming: 'false', isValid: 'Active', latitude: '', location: 'Korea', longitude: '', msisdn:  
'+8491.8888888', overageFlag: 'false', overageRate: '', overageThreshold: '10.0', publicKey:  
'sim1_pkey', roamingPartnerName: '', roamingRate: '', type: 'SubscriberSim' }
```

Key: 3

```
Record: { address: 'Hue', allowOverage: '', callDetails: [], homeOperatorName: 'VinaPhone',  
isRoaming: 'true', isValid: 'Active', latitude: '', location: 'Korea', longitude: '', msisdn:  
'+8491.8888888', overageFlag: 'false', overageRate: '1.7', overageThreshold: '10.0', publicKey:  
'sim1_pkey', roamingPartnerName: 'KoreaTel', roamingRate: '1.2', type: 'SubscriberSim' }
```

Key: 4

```
Record: { address: 'Hue', allowOverage: '', callDetails:  
[ { callBegin: '2020-04-22T04:26:23.000Z', callEnd: '', callCharges: '' } ], homeOperatorName:  
'VinaPhone', isRoaming: 'true', isValid: 'Active', latitude: '', location: 'Korea', longitude: '',  
msisdn: '+8491.8888888', overageFlag: 'false', overageRate: '1.7', overageThreshold: '10.0',  
publicKey: 'sim1_pkey', roamingPartnerName: 'KoreaTel', roamingRate: '1.2', type:  
'SubscriberSim' }
```

Key: 5

```
Record: { address: 'Hue', allowOverage: '', callDetails:  
[ { callBegin: '2020-04-22T04:26:23.000Z', callCharges: '', callEnd: '2020-04-22T06:44:56.000Z'  
} ], homeOperatorName: 'VinaPhone', isRoaming: 'true', isValid: 'Active', latitude: '', location:  
'Korea', longitude: '', msisdn: '+8491.8888888', overageFlag: 'false', overageRate: '1.7',  
overageThreshold: '10.0', publicKey: 'sim1_pkey', roamingPartnerName: 'KoreaTel',  
roamingRate: '1.2', type: 'SubscriberSim' }
```

```
Key: 6
Record: { address: 'Hue', allowOverage: '', callDetails:
[ { callBegin: '2020-04-22T04:26:23.000Z', callCharges: '166.80', callEnd: '2020-04-
22T06:44:56.000Z' } ], homeOperatorName: 'VinaPhone', isRoaming: 'true', isValid: 'Active',
latitude: '', location: 'Korea', longitude: '', msisdn: '+8491.8888888', overageFlag: 'false',
overageRate: '1.7', overageThreshold: '10.0', publicKey: 'sim1_pkey', roamingPartnerName:
'KoreaTel', roamingRate: '1.2', type: 'SubscriberSim' }
```

Hình 8. Lịch sử số liệu một thuê bao được ghi nhận trên blockchain

5. KẾT LUẬN

Trong bài báo này, bằng công nghệ blockchain và ứng dụng nền tảng HF chúng tôi đã giải quyết bài toán quản lý khai thác dịch vụ chuyển vùng di động bằng cách sử dụng hợp đồng kỹ thuật số để thực hiện thỏa ước chuyển vùng quốc tế giữa các CSP. Chúng tôi cũng đã thực hiện cài đặt mô hình mạng blockchain HF và thử nghiệm một số kịch bản khai thác. Kết quả thử nghiệm cho thấy tính khả thi trong việc phòng chống tấn công gian lận chuyển vùng, chống thất thoát doanh thu. Các CSP cũng có cơ hội cắt giảm chi phí thuê các tổ chức quốc tế trung gian để đối soát cản trở doanh thu viễn thông. Các số liệu chi tiết cuộc gọi, cước phí được ghi nhận tức thời, bất biến trên sổ cái blockchain và dễ dàng được kiểm chứng giúp tăng cường sự tin cậy giữa các đối tác và sự hài lòng của khách hàng.

Bên cạnh các ưu điểm nói trên, hệ thống này cũng có nhược điểm do tính chất bất biến của blockchain. Toàn bộ lịch sử thông tin thuê bao, dữ liệu chi tiết cuộc gọi và cước phí sẽ lưu giữ vĩnh viễn trên sổ cái. Điều này có thể là gánh nặng ảnh hưởng lớn đến hiệu năng toàn hệ thống khi vẫn phải duy trì online lượng dữ liệu khổng lồ đã hết thời hiệu xử lý. Theo quy trình thông thường, các CSP sẽ lưu trữ các dữ liệu cước chi tiết đã hết thời hiệu giải quyết khiếu nại ra các phương tiện offline để tối ưu hiệu quả sử dụng tài nguyên.

Thực tế, mỗi CSP thường phục vụ cho hàng chục triệu thuê bao hoặc nhiều hơn và họ sẽ rất thận trọng với việc thay đổi quy trình quản lý khai thác hiện tại. Vì vậy, vấn đề đánh giá hiệu năng và định cỡ hệ thống blockchain cho ngành viễn thông sẽ cần có những nghiên cứu chuyên sâu để hiện thực hóa việc triển khai.

TÀI LIỆU THAM KHẢO

- [1]. Nguyễn Mậu Hân (2012), *Cơ sở dữ liệu phân tán*, NXB Đại Học Huế.
- [2]. Phan Đình Diệu (2002), *Lý thuyết mật mã và an toàn thông tin*, NXB ĐHQG Hà Nội.
- [3]. Fiona Carmichael (2005), *A Guide to Game Theory*, Prentice Hall.
- [4]. Z. Liu, NC. Luong, W. Wang, D. Niyato, P. Wang, YC. Liang, D. Kim (2019) , *A Survey on Applications of Game Theory in Blockchain*, arXiv.
- [5]. Paolo Tasca, Claudio J. Tessone (2019), *A Taxonomy of Blockchain Technologies: Principles of Identification and Classification*, Ledger Journal.
- [6]. Gates M. (2017). *Blockchain: Ultimate guide to understanding blockchain, cryptocurrencies, smart contracts and the future of money*. Wise Fox Publishings and Mark Gates.
- [7]. Gabriel Macia-Fernandez, Pedro Garcia-Teodoro, Jesus Diaz-Verdejo (2009), *Fraud in roaming scenarios: An overview*. IEEE Wireless Communications.
- [8]. <https://hyperledger-fabric.readthedocs.io>
- [9]. <https://developer.ibm.com/patterns/blockchain-for-telecom-roaming-fraud-and-overage-management/>
- [10]. http://bswan.org/revenue_share_fraud.asp
- [11]. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf

BLOCKCHAIN-APPLICATION IN EXPLOITING TELECOMMUNICATION ROAMING SERVICE

Vo Minh Duc^{1*}, Nguyen Mau Han²

¹VNPT Phu Yen, Vietnam Posts and Telecommunications Group

²University of Sciences, Hue University

*Email: duc.pyn@gmail.com

ABSTRACT

Blockchain is a technology that allows the secure transmission of data based on an extremely complex encryption system, similar to a company's ledger, where all activities involve public money are closely monitored. In recent years, blockchain technology 3.0 has transcended the boundaries of the financial-monetary, penetrating diversely into other fields. Blockchain opens up opportunities for the telecommunications industry to improve the efficiency of network exploitation management, business transactions of digital assets such as content services, supply chain management with smart contracts, especially network security and prevent fraud. This paper proposes a method to solve international roaming fraud in the field of communication and information by blockchain technology to enhance the efficiency of the management of exploitation telecommunications roaming services.

Keywords: blockchain, roaming, telecommunications.



Võ Minh Đức sinh ngày 18/01/1975 tại Hà Nội. Năm 2008 ông tốt nghiệp kỹ sư Điện tử Viễn thông tại Học viện Công nghệ Bưu chính Viễn thông. Năm 2018 ông học thạc sĩ chuyên ngành Khoa học máy tính tại Trường Đại học Khoa học, Đại học Huế. Hiện nay ông đang công tác tại VNPT Phú Yên, chi nhánh của Tập đoàn Bưu chính Viễn thông Việt Nam.

Lĩnh vực nghiên cứu: Công nghệ phần mềm, Cơ sở dữ liệu.



Nguyễn Mậu Hân sinh năm 1957 tại Thừa thiên Huế. Năm 1981, ông tốt nghiệp cử nhân toán tại trường Đại học Tổng hợp Huế. Năm 1998 nhận bằng thạc sĩ về Khoa học máy tính tại Trường đại học Bách khoa Hà Nội. Năm 2003, nhận bằng tiến sĩ chuyên ngành Khoa học Máy tính tại Viện Công nghệ Thông tin Hà nội. Hiện ông là Phó Giáo sư, Giảng viên cao cấp tại Trường Đại học Khoa học, Đại học Huế.

Lĩnh vực nghiên cứu: Công nghệ phần mềm, Cơ sở dữ liệu, Xử lý song song và phân tán, tính toán lưới.