ĐẠI HỌC QUỐC GIA TP. HCM
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

BÁO CÁO TỔNG KẾT
ĐỀ TÀI KHOA HỌC VÀ CÔNG NGHỆ SINH VIÊN NĂM 2023

Tên đề tài tiếng Việt: HƯỚNG TỚI KHẢ NĂNG TƯƠNG TÁC LIÊN CHUỖI SỬ DỤNG CHUỖI KHỐI NGOÀI VÀ KIỂM SOÁT TRUY CẬP DỮ LIỆU BẰNG KHOÁ CÓ THỜI HẠN

.....

Tên đề tài tiếng Anh: ENHANCING BLOCKCHAIN INTEROPERABILITY THROUGH SIDECHAIN INTEGRATION AND VALID-TIME-KEY DATA ACCESS CONTROL

.....

Khoa/ Bộ môn: Mạng máy tính và truyền thông

Thời gian thực hiện: 6 tháng

Cán bộ hướng dẫn: Th.S Trần Tuấn Dũng

Tham gia thực hiện

TT	Họ và tên, MSSV	Chịu trách nhiệm	Điện thoại	Email
1.	Võ Anh Kiệt, 20520605	Chủ nhiệm	0365642317	20520605@gm.uit.edu.vn
2.	Nguyễn Bùi Kim Ngân, 20520648	Tham gia	0964763638	20520648@gm.uit.edu.vn
3.	Nguyễn Bình Thục Trâm, 20520815	Tham gia	0934010902	20520815@gm.uit.edu.vn

Thành phố Hồ Chí Minh – Tháng 12 /2023

ĐẠI HỌC QUỐC GIA TP. HCM
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

Ngày nhận hồ sơ	
Mã số đề tài	
(Do CQ quản lý ghi)	

BÁO CÁO TỔNG KẾT

Tên đề tài tiếng Việt: HƯỚNG TỚI KHẢ NĂNG TƯƠNG TÁC LIÊN CHUỖI SỬ DỤNG CHUỖI KHỐI NGOÀI VÀ KIỂM SOÁT TRUY CẬP DỮ LIỆU BẰNG KHOÁ CÓ THỜI HẠN

.....

Tên đề tài tiếng Anh: ENHANCING BLOCKCHAIN INTEROPERABILITY THROUGH SIDECHAIN INTEGRATION AND VALID-TIME-KEY DATA ACCESS CONTROL

.....

Ngày ... tháng ..... năm ....
Cán bộ hướng dẫn
(Họ tên và chữ ký)

Ngày ... tháng ..... năm ....
Sinh viên chủ nhiệm đề tài
(Họ tên và chữ ký)

THÔNG TIN KẾT QUẢ NGHIÊN CỨU

1. Thông tin chung:

- Tên đề tài: HƯỚNG TỚI KHẢ NĂNG TƯƠNG TÁC LIÊN CHUỖI SỬ DỤNG CHUỖI KHỐI NGOÀI VÀ KIỂM SOÁT TRUY CẬP DỮ LIỆU BẰNG KHOÁ CÓ THỜI HẠN

- Chủ nhiệm: Võ Anh Kiệt - 20520605

- Thành viên tham gia: Nguyễn Bùi Kim Ngân – 20520648, Nguyễn Bình Thục Trâm – 20520815

- Cơ quan chủ trì: Trường Đại học Công nghệ Thông tin.

- Thời gian thực hiện: 6 tháng

2. Mục tiêu:

- Xây dựng hệ thống liên chuỗi để vận chuyển dữ liệu liền mạch và hiệu quả qua lại giữa nhiều mạng blockchain khác nhau thông qua phương pháp sidechain, với kiến trúc là mạng phi tập trung của các oracles tương tự như một blockchain trung gian thứ ba.

- Triển khai kiểm soát truy cập dữ liệu dựa trên vai trò bằng khóa có thời gian (VTK), giúp thuận tiện, tối ưu hơn và tăng cường bảo mật cho dữ liệu được yêu cầu truy suất.

- Hệ thống được xây dựng không gây ảnh hưởng tới hiệu suất và bảo mật của những blockchain mẹ.

- Giải pháp có thể triển khai lên nhiều kiến trúc blockchain khác nhau như Ethereum, Quorum, Hyperledger Fabric,…

- Kiểm tra hiệu suất thực tế và đo lường chi phí tiêu tốn để thực hiện mỗi giao dịch, đồng thời đánh giá tổng thể về hoạt động, chức năng và an toàn của hệ thống đề suất.

3. Tính mới và sáng tạo:

Hệ thống sidechain được xây dựng gồm các nút oracle bên trong. Sidechain đóng vai trò là một cầu nối giao tiếp giữa hai chuỗi khối, đồng thời đảm bảo tính hợp lệ của dữ liệu bằng cách sử dụng các nút oracle còn lại xác minh khi có một nút oracle thực hiện giao dịch liên chuỗi. Đồng thời, việc triển khai kiểm soát truy cập dữ liệu bằng khóa có thời hạn giúp bảo vệ dữ liệu an toàn trước những truy cập trái phép.

4. Tóm tắt kết quả nghiên cứu:

Hệ thống được triển khai hoạt động liền mạch trên nhiều mạng blockchain khác nhau, quy trình diễn ra một cách tự động, giảm thiểu tối đa sự can thiệp của người dùng cuối. Về kết quả thực nghiệm cho thấy hệ thống có hiệu suất tốt về mặt thời gian và chi phí tiêu tốn.

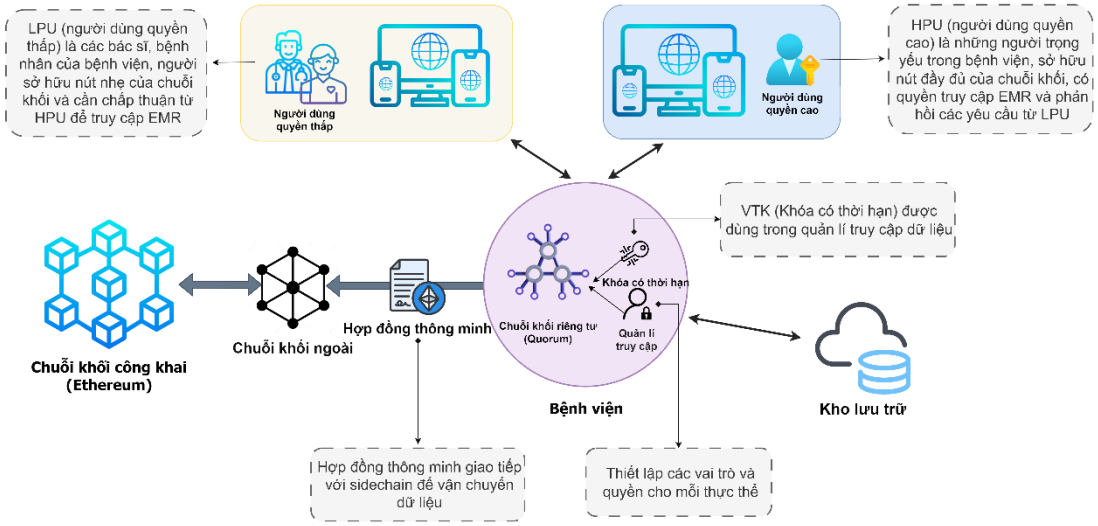
5. Tên sản phẩm:

Hướng tới khả năng tương tác liên chuỗi sử dụng chuỗi khối ngoài và kiểm soát truy cập dữ liệu bằng khoá có thời hạn

6. Hiệu quả, phương thức chuyển giao kết quả nghiên cứu và khả năng áp dụng:

Nhóm tác giả đã tiến hành thử nghiệm hệ thống sidechain với 2 mạng blockchain riêng biệt là Ethereum và Quorum trong bối cảnh chăm sóc sức khỏe y tế. Nhằm bảo đảm cho tính toàn vẹn cho Hồ sơ y tế được quản lý trong bệnh viện xây dựng Quorum, hệ thống sidechain đã làm trung gian vận chuyển bằng chứng toàn vẹn của dữ liệu lên mạng blockchain công khai là Ethereum. Qua đó khi cần kiểm tra Hồ sơ, sidechain cũng sẽ làm nhiệm vụ vận chuyển bằng chứng về mạng của bệnh viện. Kết quả cho thấy khả năng hoạt động và tính khả thi của hệ thống sidechain trong việc vận chuyển dữ liệu liên chuỗi, cũng như tiềm năng mở rộng khả năng ứng dụng cho các lĩnh vực khác.

7. Hình ảnh, sơ đồ minh họa chính



Cơ quan Chủ trì (*ký, họ và tên, đóng dấu*)	Chủ nhiệm đề tài *(ký, họ và tên)*

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC BẢNG VÀ THUẬT TOÁN

Danh mục bảng

Danh mục thuật toán

TÓM TẮT

Hiện nay, một trong những rào cản lớn nhất đối với sự phát triển của công nghệ blockchain là thiếu khả năng tương tác giữa các chuỗi khối riêng biệt. Điều này hạn chế đáng kể tiềm năng mở rộng và phát triển của hệ sinh thái đa chuỗi. Để giải quyết vấn đề này, nhóm nghiên cứu đề xuất một kiến trúc tương tác mới cho phép chia sẻ dữ liệu an toàn giữa các chuỗi blockchain.

Hệ thống đề xuất sẽ sử dụng sidechain kết hợp với hệ thống kiểm soát truy cập dữ liệu bằng valid-time key (VTK) để cho phép truyền dữ liệu an toàn và xác thực thông tin trên nhiều mạng blockchain khác nhau. Kiến trúc này đã được chứng minh là hiệu quả trong việc trao đổi dữ liệu hồ sơ sức khỏe điện tử (EMR), đảm bảo giao tiếp liền mạch, bảo mật và xác thực thông tin.

Hệ thống kiểm soát truy cập VTK giúp chống truy cập trái phép và gian lận, chỉ cấp quyền truy cập cho các bên được ủy quyền trong thời hạn nhất định. Nhờ vậy, kiến trúc đề xuất có tiềm năng giải quyết thách thức tương tác blockchain và thúc đẩy phát triển hệ sinh thái đa chuỗi khối trong tương lai.

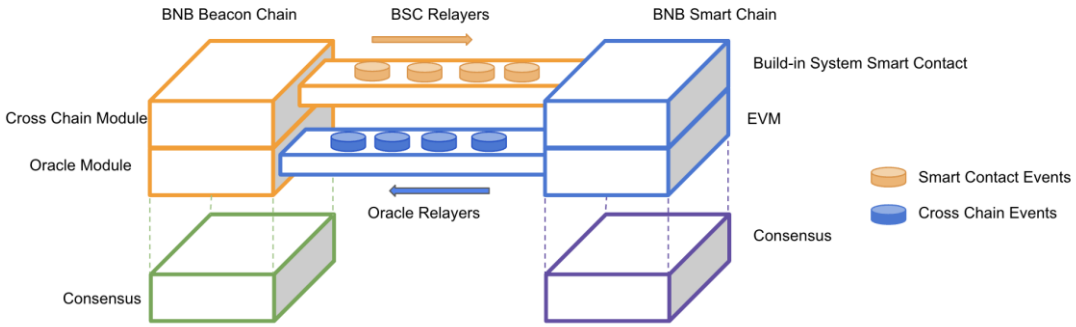
Với việc giải quyết vấn đề tương tác, hệ thống blockchain có thể tối ưu hóa hiệu suất tính toán, mở rộng khả năng lưu trữ và mở khóa tiềm năng phát triển không giới hạn.

CHƯƠNG 1: MỞ ĐẦU

Chuỗi khối (blockchain) đang ngày càng được ứng dụng rộng rãi trong nhiều ngành như tài chính, bảo hiểm, chăm sóc sức khỏe, hỗ trợ xã hội và giáo dục [1, 2]. Tuy nhiên, nhiều nghiên cứu cho thấy rằng khả năng tương tác giữa đa dạng các kiến trúc chuỗi khối khác nhau vẫn là một thách thức lớn chưa được giải quyết và yêu cầu trao đổi giữa những thực thể hoạt động cùng một lĩnh vực là rất phổ biến và thiết yếu [3]. Do đó để công nghệ chuỗi khối có thể phát triển mạnh mẽ và có khả năng áp dụng được với nhiều bối cảnh thực tế, việc thúc đẩy sự phát triển trong khả năng tương tác giữa các chuỗi khối khác kiến trúc là một khía cạnh vô cùng quan trọng. Đặc biệt là trong lĩnh vực chăm sóc sức khỏe [4] đã được ứng dụng chuỗi khối ở mức tương đối thì tính minh bạch và hiệu quả là nền tảng của sự tương tác thành công và liền mạch giữa các bên [5-7]. Tuy nhiên, vì lưu trữ dữ liệu theo cách phi tập trung, cho phép phân mảnh trong các hệ thống chuỗi khối hiện tại gây ra những hạn chế đáng kể đối với việc cung cấp dữ liệu có độ chính xác cao để đáp ứng kịp thời cho quá trình chăm sóc và điều trị bệnh nhân một cách tốt nhất [8,9]. Do vậy, việc xây dựng và tối ưu hóa hệ thống hỗ trợ tương tác liên chuỗi là vô cùng quan trọng, tuy nhiên, các giải pháp hiện tại đang gặp những trở ngại đáng kể như chi phí cao, quy trình thực hiện phức tạp.

Để đạt được khả năng tương tác liên chuỗi và thực hiện liền mạch các hợp đồng thông minh giữa các mạng chuỗi khối khác kiến trúc, việc áp dụng các giao thức được tiêu chuẩn hóa và các phương pháp mới mẻ nổi lên như những yếu tố then chốt [10]. Bằng cách nắm bắt những phát kiến đáng chú ý này, chúng ta có thể mở khóa tiềm năng vô tận của công nghệ chuỗi khối, tạo ra một hệ sinh thái chuỗi khối có khả năng tương tác và kết nối với nhau bất kể những sự khác biệt trong mặt xây dựng hệ thống nội bộ bên trong. Song, cũng đã có rất nhiều nhà nghiên cứu đã làm sáng tỏ tầm quan trọng

của khả năng tương tác chuỗi khối trong các nghiên cứu của họ, từ đó đưa ra ba loại chiến lược chính: phương pháp Notary, phương pháp khóa băm (Hash-locking) và phương pháp chuỗi chuyển tiếp (Relays)/chuỗi khối ngoài (Sidechain) và xem chúng như các khuôn khổ thiết yếu để đạt được kết nối liền mạch trên các mạng chuỗi khối đa dạng [11,12].



Hình 1: Mô hình giao tiếp liên chuỗi

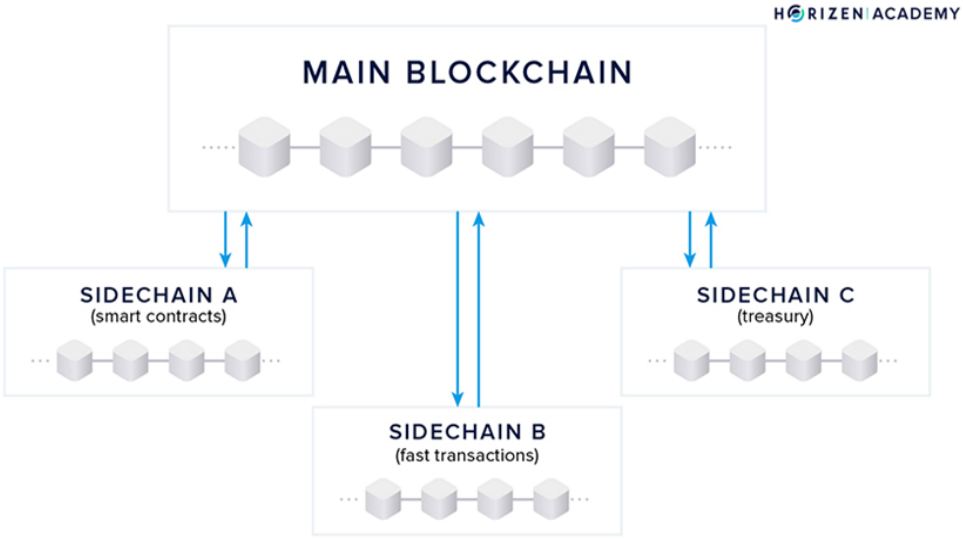
CHƯƠNG 2: CÁC CÔNG TRÌNH NGHIÊN CỨU LIÊN QUAN

2.1. Phương pháp Notary và phương pháp Hash-locking

Phương pháp Notary được xem là một trong những hướng tiếp cận cho giải pháp liên chuỗi tương đối đơn giản. Cơ chế này gồm một tập hợp các thực thể được xem là đáng tin cậy, đóng vai trò trung gian, bắt đầu các hành động trong một chuỗi khối để đáp ứng các sự kiện diễn ra trong một chuỗi khối khác [13]. Tuy nhiên, việc phụ thuộc vào một bên thứ ba có thể gây ra những lo ngại về vấn đề tập trung hóa, thắt cổ chai hoặc tin tưởng mù quáng. Ngoài ra thì phương pháp khóa băm cũng là một hướng tiếp cận vấn đề chuỗi chéo rất được quan tâm hiện nay [14,15]. Việc sử dụng khóa băm như một cơ chế giao tiếp liên chuỗi khối đã cung cấp một cách giải quyết hiệu quả để trao đổi tài sản, đồng thời loại bỏ sự phụ thuộc vào sự tham gia của bên thứ ba. Trong quá trình này, cả hai bên khóa tài sản dùng để trao đổi của họ trong hợp đồng thông minh và gửi giá trị băm của khóa bí mật đã chọn cho người nhận. Việc thực hiện thành công giao dịch phụ thuộc vào việc đáp ứng các điều kiện băm được xác định trước trong một khung thời gian cụ thể. Trong trường hợp các yêu cầu này không được đáp ứng, tài sản sẽ nhanh chóng được trả lại cho chủ sở hữu hợp pháp của chúng, nhờ vậy mà quy trình vận chuyển dữ liệu được đảm bảo tính bí mật và tính toàn vẹn của thông tin. Thế nhưng, mặc dù khóa băm có thể được xem là một giải pháp khả thi để trao đổi và chuyển giao tài sản liên chuỗi, nhưng nó đòi hỏi khả năng tương thích của cả hai chuỗi liên quan để hỗ trợ cùng một hàm băm. Hơn nữa, có một thách thức đáng kể nằm ở chi phí cao và các yêu cầu thiết kế phức tạp để việc đảm bảo sự giao tiếp và khả năng tương thích của các hợp đồng thông minh trên các chuỗi khối khác nhau.

2.2. Phương pháp Relays/Chuỗi khối ngoài

Relays/Chuỗi khối ngoài là một giải pháp chuỗi chéo đầy hứa hẹn, tập trung vào khả năng mở rộng và khả năng tương tác giữa các chuỗi khối khác kiến trúc, nhờ vậy có thể cung cấp một giải pháp phi tập trung thay thế cho phương pháp Notary. Bằng cách tận dụng cơ chế của một chuỗi khối, việc chuyển giao tài sản kỹ thuật số, bao gồm tài sản số, token và dữ liệu, trở nên dễ dàng và trôi chảy trên các mạng chuỗi khối khác nhau. Trong hệ sinh thái chuỗi khối, chuỗi khối ngoài có vai trò như một chuỗi khối thứ hai tự trị, hoạt động độc lập, chính nhờ vậy mà nó có khả năng bảo vệ hiệu suất và tính bảo mật của chuỗi khối chính mà không gặp phải bất kỳ tác động bất lợi nào.

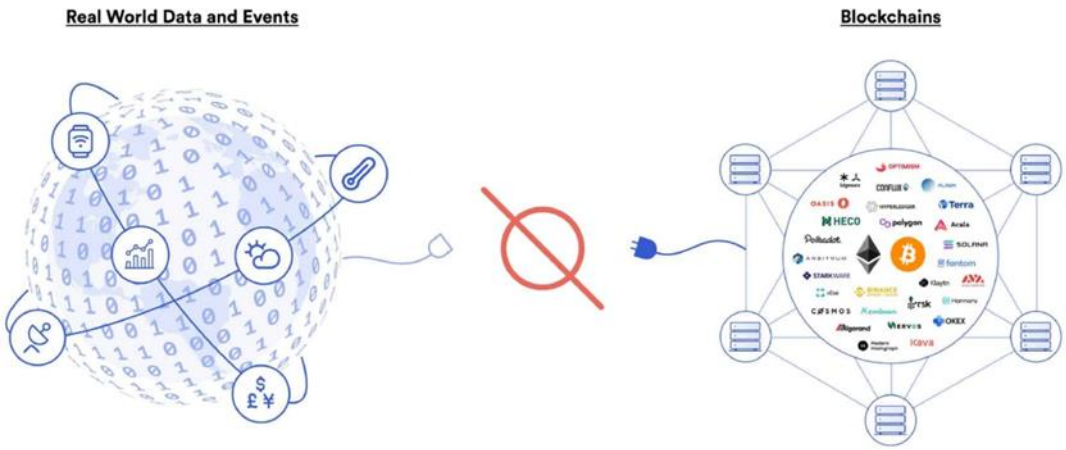


Hình 1: Mô phỏng phương pháp Relay/Sidechain

Cosmos [16] và Polkadot [17] là những nền tảng cung cấp khả năng tương tác liên chuỗi khối bằng chuỗi khối ngoài nổi bật và có kiến trúc đặc biệt giúp tương tác một cách liền mạch và hiệu quả giữa các chuỗi khối.

2.3. Chuỗi khối oracles

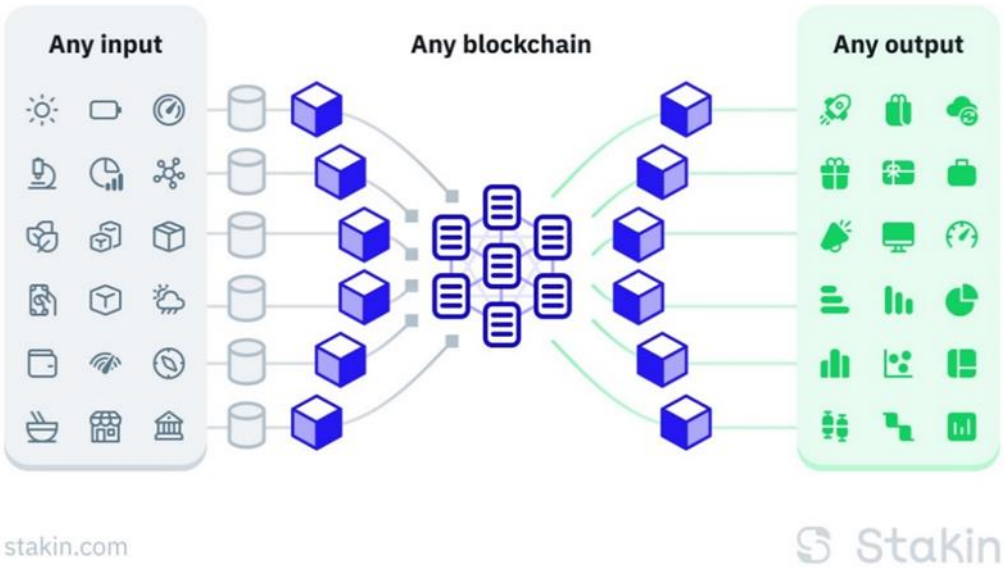
Bài toán mang đến ý tưởng xây dựng chuỗi khối oracles bắt nguồn từ một hạn chế cơ bản của các hợp đồng thông minh, đó là chúng vốn không thể tương tác với dữ liệu và hệ thống tồn tại bên ngoài môi trường chuỗi khối gốc của chúng. Các tài nguyên bên ngoài chuỗi khối được coi là tài nguyên "off-chain" (ngoài chuỗi), trong khi dữ liệu đã được lưu trữ trên chuỗi khối được coi là tài nguyên "on-chain" (trên chuỗi). Chính việc cố ý tách biệt khỏi các hệ thống bên ngoài, các chuỗi khối có được các thuộc tính có giá trị nhất của chúng như sự đồng thuận mạnh mẽ về tính hợp lệ trong các giao dịch của người dùng, ngăn chặn các cuộc tấn công double-spending và giảm thiểu thời gian ngừng hoạt động (downtime) của mạng. Thế nhưng, việc tương tác an toàn với các hệ thống và dữ liệu ngoài chuỗi từ chuỗi khối vẫn là một yêu cầu vô cùng cấp thiết để phục vụ cho những ứng dụng thực tiễn của các hệ thống chuỗi khối. Chính vì vậy, ý tưởng về chuỗi khối oracles được ra đời.



Hình 2: Sự thiếu kết nối của dữ liệu và sự kiện với Blockchains

Trong công nghệ chuỗi khối, oracle là một dịch vụ có khả năng cung cấp dữ liệu bên ngoài cho một hợp đồng thông minh hoặc một mạng chuỗi khối. oracle đóng vai trò là cầu nối giữa thế giới trong chuỗi và ngoài chuỗi, cho phép các hợp đồng thông minh truy cập và tương tác với dữ liệu hoặc sự

kiện trong thế giới thực. Bản thân các hợp đồng thông minh bị giới hạn khả năng xử lý và thực thi mã trong phạm vi mạng chuỗi khối và không thể truy cập trực tiếp dữ liệu từ các nguồn bên ngoài, chẳng hạn như tỷ giá tiền tệ, điều kiện thời tiết hoặc tỷ số thể thao. Do đó các cầu nối như oracle là rất quan trọng. Các oracles sẽ lấy và xác minh dữ liệu từ nhiều nguồn bên ngoài và chuyển dữ liệu đó tới các hợp đồng thông minh trên chuỗi khối. Chúng đóng vai trò trung gian đáng tin cậy, có thể chuyển tiếp thông tin bên ngoài một cách an toàn đến mạng chuỗi khối.



Hình 3: Cách hoạt động của chuỗi khối oracles

CHƯƠNG 3: ĐỀ XUẤT GIẢI PHÁP

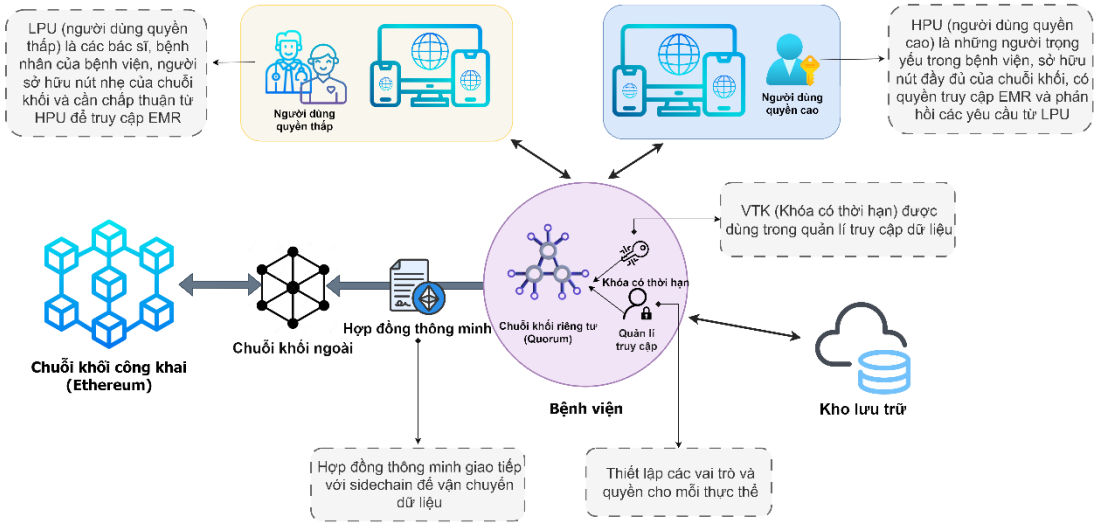
3.1. Hệ thống được triển khai

3.1.1. Ngữ cảnh đề tài

Hệ thống được đề xuất nằm trong bối cảnh bệnh viện quản lý hồ sơ sức khỏe của bệnh nhân thông qua mạng chuỗi khối riêng.

Trong mạng chuỗi khối thì nút đầy đủ (full node) là một loại nút quan trọng nhất đảm bảo hoạt động và tính nhất quán acủa hệ thống. Vai trò chính của nút đầy đủ là duy trì một bản sao đầy đủ của toàn bộ blockchain và tham gia vào quá trình xác nhận cũng như xây dựng các khối mới trong mạng. Tuy nhiên, chi phí xây dựng một mạng như vậy với nhiều nút đầy đủ là rất tốn kém. Mặt khác, một mạng chỉ có một vài full mode và nhiều nút nhẹ (light node) vốn được thiết kế để thực hiện các giao dịch nhanh và các hoạt động đơn giản hàng ngày sẽ có khả năng ảnh hưởng đến an ninh mạng. Vì như đã đề cập trước đó, chỉ có các nút đầy đủ mới có thể tham gia vào toàn bộ quá trình xác nhận giao dịch và tạo khối mới, nên với số lượng nút đầy đủ quá ít, mạng chuỗi khối sẽ gần như tương đương với một loại mạng tập trung và phải đối mặt với rất nhiều cuộc tấn công mạng. Từ đó, khi xảy ra sự cố ngoài ý muốn và cần truy xuất dữ liệu để điều tra, ta sẽ đặt ra nghi vấn về tính toàn vẹn của hồ sơ y tế điện tử (EMR) được lưu trữ.

Để giải quyết vấn đề này, cần phải có bằng chứng về tính toàn vẹn của dữ liệu và bằng chứng đó có thể được lưu trữ trên chuỗi khối công khai nhằm tăng cường bảo mật và tính minh bạch cũng như có thể truy xuất ngay khi cần. Thách thức ở đây là làm thế nào để vận chuyển dữ liệu giữa hai chuỗi khối với các kiến trúc khác nhau. Giải pháp đề xuất của nhóm tác giả sẽ giải quyết vấn đề này, với thông tin về các thành phần hệ thống được trình bày chi tiết trong các phần sau. Tổng quan hệ thống được mô tả theo hình dưới.



Hình 4: Mô hình tổng quan của hệ thống

3.1.2. Các mạng chuỗi khối và các thực thể

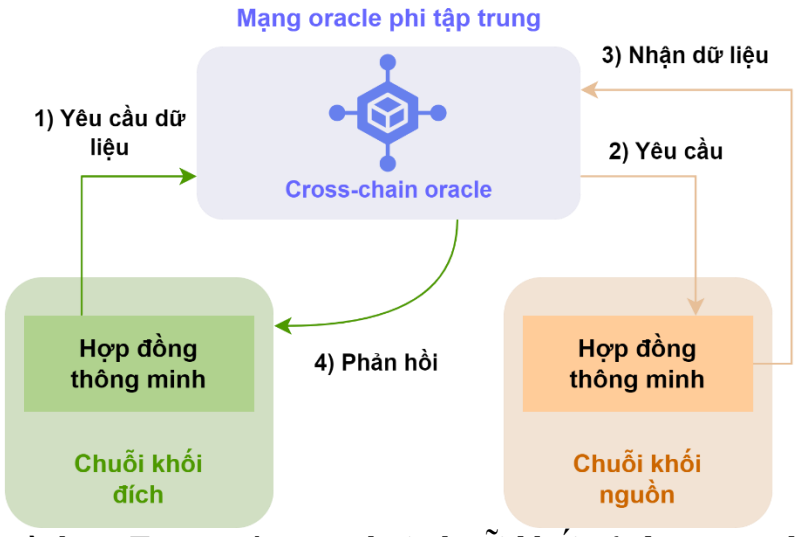
Thứ nhất, về mạng chuỗi khối riêng, nhóm tác giả triển khai xây dựng kiến trúc chuỗi khối Quorum. Để đảm bảo tính bảo mật của dữ liệu, cũng như để tối ưu hóa quy trình yêu cầu truy cập dữ liệu để sử dụng trong thực tế, nhóm đã thiết kế các biện pháp kiểm soát truy cập theo vai trò bằng cách triển khai các hợp đồng thông minh trong mạng chuỗi khối riêng tư Quorum. Có ba vai trò chính cho các thực thể trong mạng chuỗi khối riêng:

- Bác sĩ/Nhân viên y tế/Bệnh nhân có liên quan - Người dùng có quyền hạn thấp là các nút nhẹ có quyền gửi yêu cầu để đọc EMR nếu được cấp khóa có thời hạn để truy cập bởi các nút đầy đủ. Thông tin chi tiết về khóa có thời hạn sẽ được giải thích trong phần sau.
- Trưởng khoa/Người quản lý - Người dùng có quyền cao là các nút đầy đủ chịu trách nhiệm xác thực tính hợp lệ của một EMR khi nó được tạo ra, đồng thời có quyền được đọc nội dung và cấp quyền truy cập đến EMR cho nút nhẹ khi nhận được yêu cầu.

- Quản trị viên (Admin) – Là nút đầy đủ và được cấp toàn quyền, chịu trách nhiệm quản lý toàn bộ hệ thống và xử lý các trường hợp khẩn cấp.

Thứ hai, mạng chuỗi khối công khai được triển khai xây dựng Ethereum. Chuỗi khối này có vai trò lưu trữ bằng chứng để xác minh tính toàn của các hồ sơ y tế điện tử. Cụ thể, bằng chứng gồm một mã băm là kết quả sau khi băm tài liệu tại thời điểm vừa được tạo ra, cùng với một mã ID tương ứng của tài liệu để phân biệt mã băm đó. Khi cần kiểm tra toàn vẹn của một EMR bất kì, ta có thể truy vấn và tìm mã băm được lưu trên Ethereum của tài liệu đó về. Bằng cách ứng dụng chuỗi khối công khai, thông tin lưu trữ được bảo vệ an toàn, minh bạch, không thể bị tác động sửa đổi một cách âm thầm và có thể truy vấn về dễ dàng.

Giải pháp chuỗi khối ngoài hoạt động như một người trung gian để vận chuyển dữ liệu giữa hai chuỗi khối không đồng nhất. Trong hệ thống được đề xuất, chuỗi khối ngoài của nhóm tác giả là một mạng các oracles phi tập trung, cho phép truy xuất dữ liệu từ thế giới bên ngoài vào chuỗi khối và như cũng gửi dữ liệu nội bộ ra thế giới bên ngoài. Trách nhiệm của một oracle bao gồm kích hoạt hợp đồng oracle có khả năng giao tiếp được với các hợp đồng thông minh của các chuỗi khối, gửi dữ liệu ra bên ngoài chuỗi khối và cung cấp dữ liệu cho một chuỗi khối khác. Sự tương tác giữa hai chuỗi khối không đồng nhất và oracle được mô tả trong hình dưới.



Hình 5: Tương tác giữa hai chuỗi khối sử dụng oracle

3.1.3. Ứng dụng phi tập trung

Ứng dụng phi tập trung, viết tắt là DApp, sử dụng các hợp đồng thông minh để thực hiện các giao dịch và duy trì các quy định trên mạng phi tập trung, trong trường hợp này là mạng được hỗ trợ bởi công nghệ chuỗi khối. DApps là mã nguồn mở, tự trị và có tính minh bạch, trái ngược với các ứng dụng tập trung thông thường, và đóng vai trò trung gian giữa người dùng và chuỗi khối riêng trong giải pháp đề xuất. Giao diện người dùng cho ứng dụng web là frontend của nó và phần backend kết nối với DApp được phát triển trên chuỗi khối riêng để vận chuyển các dữ liệu theo yêu cầu của người dùng đến đó.

DApp của hệ thống được tạo ra với ba phiên bản chính:

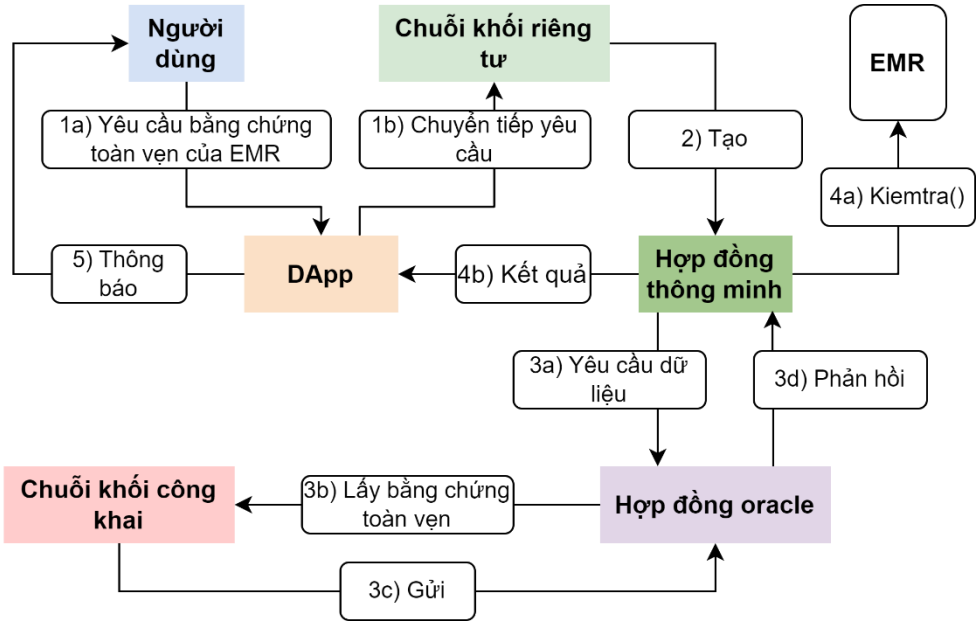
- Phiên bản dành cho bệnh nhân
- Phiên bản dành cho người dùng quyền thấp
- Phiên bản dành cho người dùng quyền cao

Mỗi vai trò người dùng sẽ có một phiên bản thích hợp riêng với những quyền sử dụng riêng trong DApp, vì vậy người dùng với các vai trò khác nhau sẽ được yêu cầu cung cấp các thông tin đăng nhập khác nhau phù hợp

với phiên bản mà mình sử dụng. Trong phiên bản chỉ dành cho bệnh nhân, người dùng chỉ có thể truy cập đến EMR của họ. Các bác sĩ và nhân viên bệnh viện cũng sử dụng phiên bản có quyền thấp, nhưng sẽ được cung cấp nhiều tính năng hơn, các tính năng này sẽ được cấp quyền sau tùy thuộc vào quá trình gửi yêu cầu để đọc và truy cập dữ liệu EMR của bệnh nhân. Phiên bản cuối cùng, phiên bản dành cho người dùng có quyền cao, cung cấp cho người lãnh đạo tùy chọn phê duyệt hoặc từ chối yêu cầu dữ liệu và cũng có thể thiết lập khóa có thời hạn và kênh kết nối để chia sẻ dữ liệu.

3.2. Hệ thống Liên chuỗi khối sử dụng Sidechain

Quá trình truyền dữ liệu băm được lưu trữ từ chuỗi khối công khai sang chuỗi khối riêng tư được trình bày trong ngữ cảnh người dùng quyền thấp gửi yêu cầu truy cập dữ liệu hoặc yêu cầu thực hiện xác minh dữ liệu cần có các dữ liệu liên chuỗi. Cụ thể hoạt động được mô tả trong hình dưới.



Hình 6: Quy trình trao đổi dữ liệu liên chuỗi

Sau khi EMR trải qua quá trình mã hóa sẽ được lưu trữ được bảo vệ bằng quyền giám hộ an toàn của khóa bí mật nằm trong tay các nút đầy đủ. Lúc này, nếu người dùng quyền cao bắt đầu gửi yêu cầu xác minh hàm băm cho

tính toàn vẹn của EMR thông qua DApp, quy trình này sẽ bảo vệ tính bảo mật tối đa của dữ liệu y tế nhạy cảm và trao quyền cho các cá nhân được ủy quyền xác thực tính xác thực của EMR. Thuật toán dưới cung cấp thông tin chi tiết về các hoạt động tuần tự liên quan đến quá trình xử lý yêu cầu kiểm tra toàn vẹn dữ liệu.

Input: ID of the requested EMR
Output: Unmodified or Modified
Perform integrity verification of the EMR request ▷ Step 1
create Oracle contract ▷ Step 2
create PriBC smart contract
if isExistsInPuBC(ID) **then** ▷ Step 3
    $AuditProof \leftarrow$ Fetch
    Oracle node transfers $AuditProof$ to PriBC
else
    The transaction is canceled
    Exit
end if
$calHash \leftarrow hashCalculation \leftarrow EMR$ ▷ Step 4
$retrievedHash \leftarrow AuditProof$
if $calHash == retrievedHash$ **then**
    return Unmodified
else
    return Modified
end if
NotifyClient ▷ Step 5

Thuật toán 1: Xác thực tính toàn vẹn dữ liệu của EMR

- Bước 1: Trong các trường hợp cần đảm bảo tính toàn vẹn của một EMR, khách hàng sử dụng DApp để yêu cầu bằng chứng cho tài liệu được chỉ định nằm trong chuỗi khối công khai. Bằng chứng kiểm tra này bao gồm mã băm và ID của EMR được đề cập. DApp sau đó chuyển tiếp yêu cầu tới chuỗi khối riêng để xử lý.
- Bước 2: Chuỗi khối riêng tạo hợp đồng thông minh của nó để liên lạc với chuỗi khối ngoài và nhận dữ liệu từ thế giới bên ngoài. Đồng thời, chuỗi khối ngoài được DApp triệu tập để tạo hợp đồng Oracle trên backend.
- Bước 3: Chuỗi khối ngoài lấy dữ liệu được yêu cầu trên chuỗi khối công khai và chuyển nó về chuỗi khối riêng.

- Bước 4: Khi nhận được bằng chứng, hợp đồng thông minh của chuỗi khối riêng tư sẽ thi hàm kiểm tra để xác minh tính toàn vẹn của EMR. Nếu hàm băm kết quả của tài liệu khớp với hàm băm được lấy từ chuỗi khối công khai, thì có thể kết luận rằng EMR không bị sửa đổi.
- Bước 5: Cuối cùng, DApp thông báo cho khách hàng về kết quả.

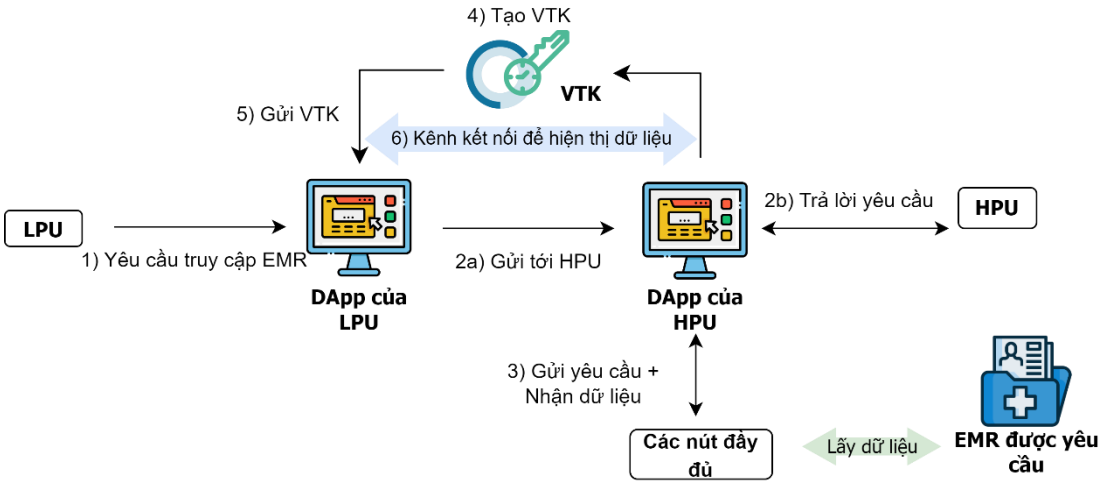
Quá trình này đảm bảo rằng các thông tin y tế nhạy cảm được bảo vệ an toàn và nguyên vẹn trong khi cung cấp cho các cá nhân được ủy quyền các phương tiện cần thiết để xác minh tính xác thực, tận dụng được tối đa tiềm lực của công nghệ chuỗi khối.

3.3. Hệ thống Quản lý truy cập bằng khóa có thời hạn

Nền tảng chuỗi khối vốn không có khả năng lưu trữ dữ liệu với kích thước lớn. Do đó để giải quyết nhược điểm này ta có thể sử dụng các giải pháp lưu trữ ngoài chuỗi như Cloud hoặc IPFS – lưu trữ phi tập trung kết hợp với việc quản lý quyền truy cập vào cơ sở dữ liệu bằng blockchain để đảm bảo an toàn thông tin cho hệ thống. Trong ngữ cảnh đưa ra, chúng tôi sử dụng lưu trữ Cloud để lưu các dữ liệu lớn như EMR. Mỗi EMR được mã hóa bằng thuật toán mã hóa đối xứng trước khi đưa vào và khóa bí mật sẽ do các fullnodes nắm giữ.

Trong các tình huống khi mà các người dùng quyền thấp tìm kiếm quyền truy cập vào EMR đã mã hóa được lưu trữ trong cơ sở dữ liệu, việc sử dụng khóa có thời gian viết tắt là khóa có thời hạn trở nên quan trọng trong việc cung cấp cho họ một quyền truy cập cần thiết. Quá trình bắt đầu khi một nút nhẹ gửi yêu cầu tới các nút đầy đủ thông qua ứng dụng phi tập trung của mình, nếu nhận được sự chấp thuận, EMR sẽ được người dùng quyền cao giải mã bằng khóa bí mật. Sau đó, một kết nối đến dữ liệu được thiết lập, đồng thời tạo ra một khóa có thời hạn và nó được gửi đến ứng dụng phi tập trung của nút nhẹ đã yêu cầu ban nãy. Sau khi được cung cấp khóa có thời

hạn hợp lệ này, ứng dụng phi tập trung dễ dàng truy cập tới kênh kết nối, người dùng có thể đọc được nội dung của dữ liệu. Khi hết thời gian được chỉ định, hiệu lực của khóa có thời hạn sẽ chấm dứt và sự chấm dứt kết nối ngay lập tức. Qua đó có thể đạt được kiểm soát truy cập dữ liệu một cách hiệu quả. Hình dưới đây giới thiệu mô hình quy trình chi tiết về giao dịch kiểm soát quyền truy cập EMR bằng khóa có thời hạn.



Hình 7: Quy trình cấp quyền cho người dùng quyền thấp

Cụ thể về từng bước trong quá trình người dùng quyền thấp yêu cầu cấp quyền để có thể truy cập hoặc lấy dữ liệu liên chuỗi được thể hiện bằng thuật toán bên dưới.

1: EMRAccessRequest ← EID ▷ Step 1
2: **if** getApprovalFromHPU ← UID **then** ▷ Step 2
3: $decryptedEMR$ ← DecryptData($PrivateKey, EID$) ▷ Step 3
4: VTK ← Generation ▷ Step 4
5: $dataConnection$ ← EstablishConnection ← $VTK, decryptedEMR$
6: Send VTK to LPU ▷ Step 5
7: **while** VTK is valid **do**
8: $dataConnection$ ← VTK ▷ Step 6
9: **end while**
10: Close $dataConnection$
11: **else**
12: NotifyClient("Don't get approval");
13: **end if**

Thuật toán 2: Kiểm soát truy cập EMR

CHƯƠNG 4: THỰC NGHIỆM VÀ ĐÁNH GIÁ

4.1. Môi trường thực nghiệm

Để kiểm tra tính khả thi và đánh giá hiệu suất của giải pháp chuỗi chéo dựa trên chuỗi khối ngoài, nhóm tác giả đã tiến hành một loạt thử nghiệm. Môi trường thực nghiệm được mô tả theo bảng sau:

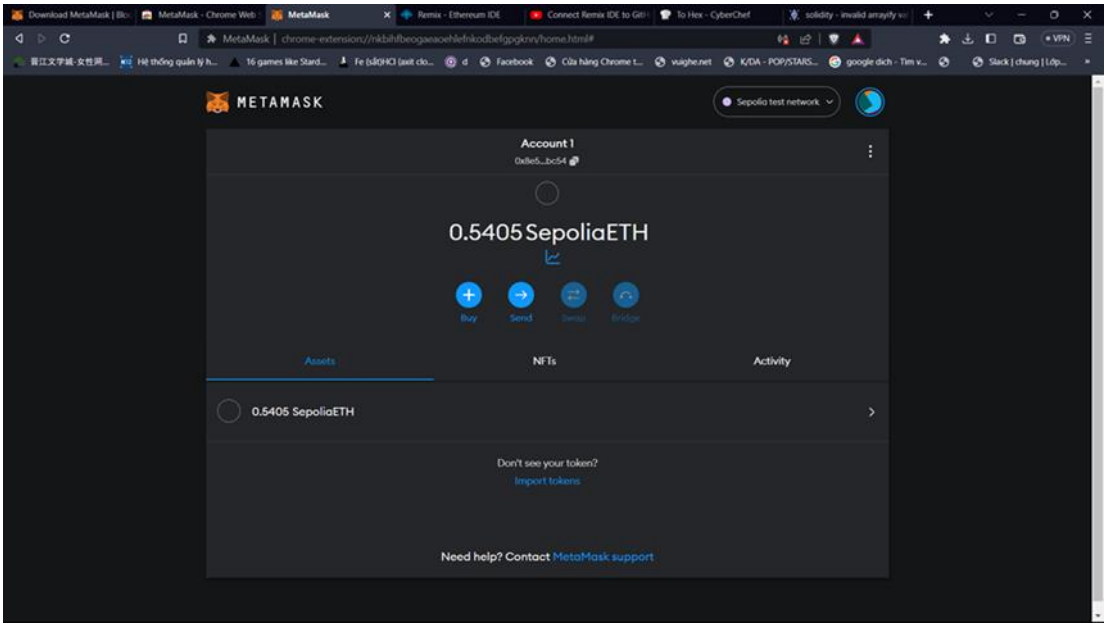
Máy ảo	**CPU**	**RAM**	**Hard drive**	**OS**	**Vai trò**
VM1	4-core	16 GB	60 GB	Ubuntu 22.04	Quorum
VM2	4-core	8 GB	60 GB	Ubuntu 22.04	Sidechain
VM3	4-core	8GB	60 GB	Ubuntu 22.04	Ethereum

Bảng 1: Môi trường thực nghiệm

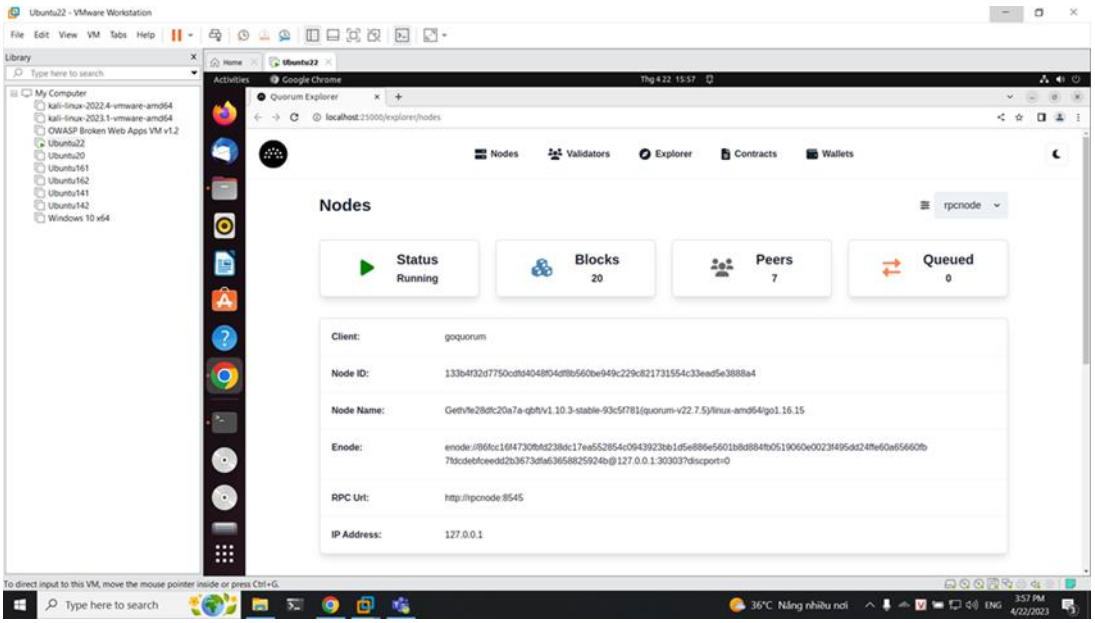
4.2. Đánh giá chức năng, hiệu suất và chi phí hệ thống

Để đánh giá chức năng của hệ thống, nhóm đã thực hiện dựng mô hình đã đề xuất bao gồm các mạng blockchain, hệ thống Sidechain và thực hiện các hoạt động bao gồm đăng ký tài khoản DApp, bắt đầu yêu cầu truy cập EMR thông qua DApp, cấp quyền truy cập EMR được yêu cầu sử dụng khóa có thời hạn và hủy kết nối sau khi kết thúc khoảng thời gian được chỉ định.

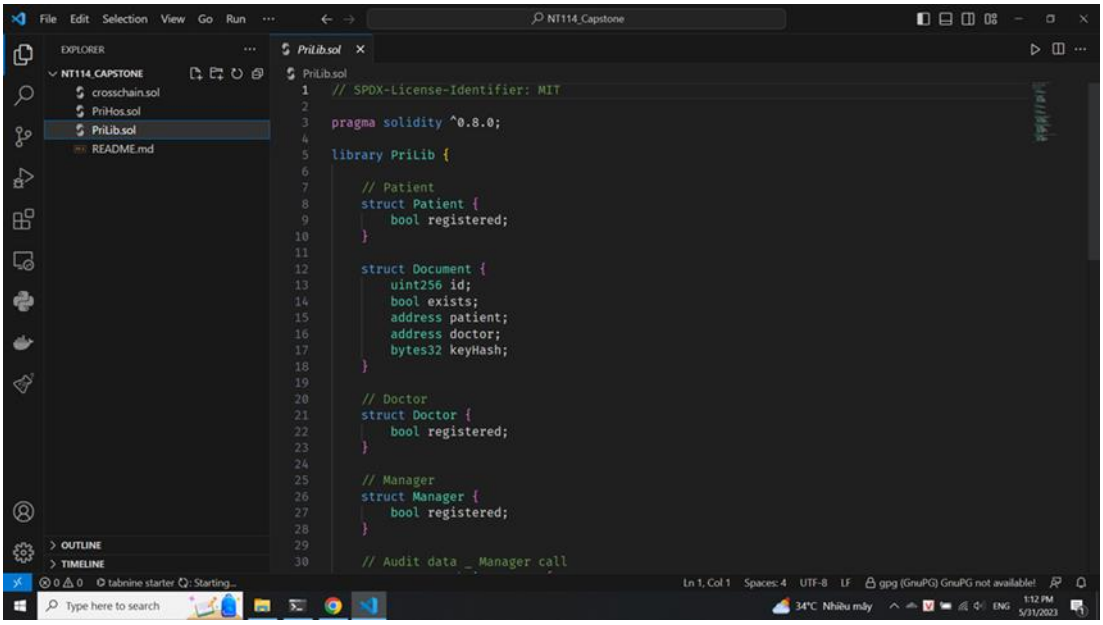
Các hình ảnh thực nghiệm khi thực hiện dựng mô hình và thực hiện các thao tác:



Hình 8: Mạng Sepolia Ethereum

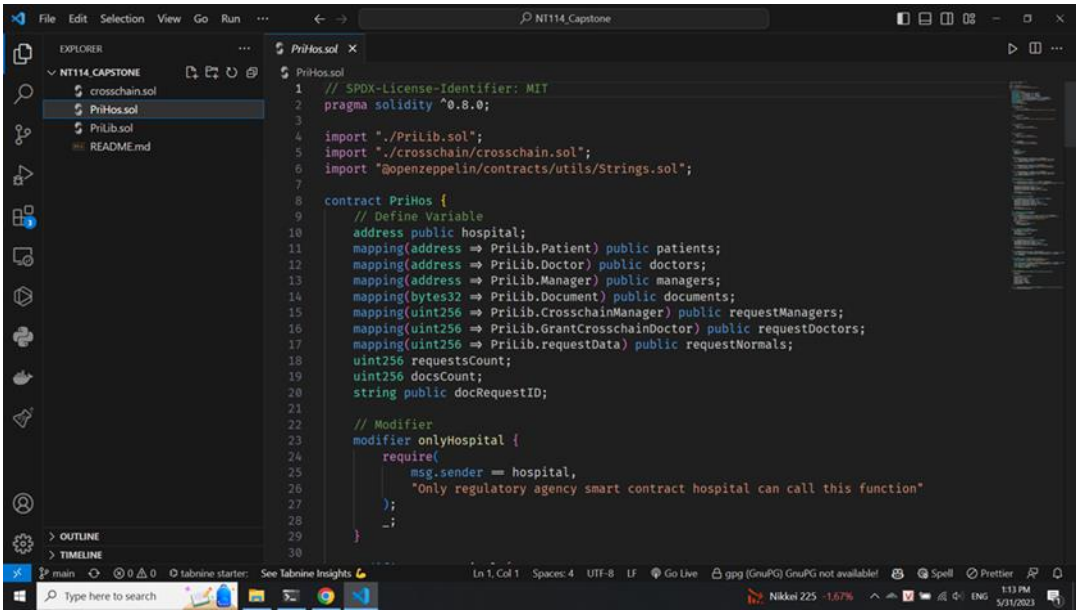


Hình 9: Mạng Quorum



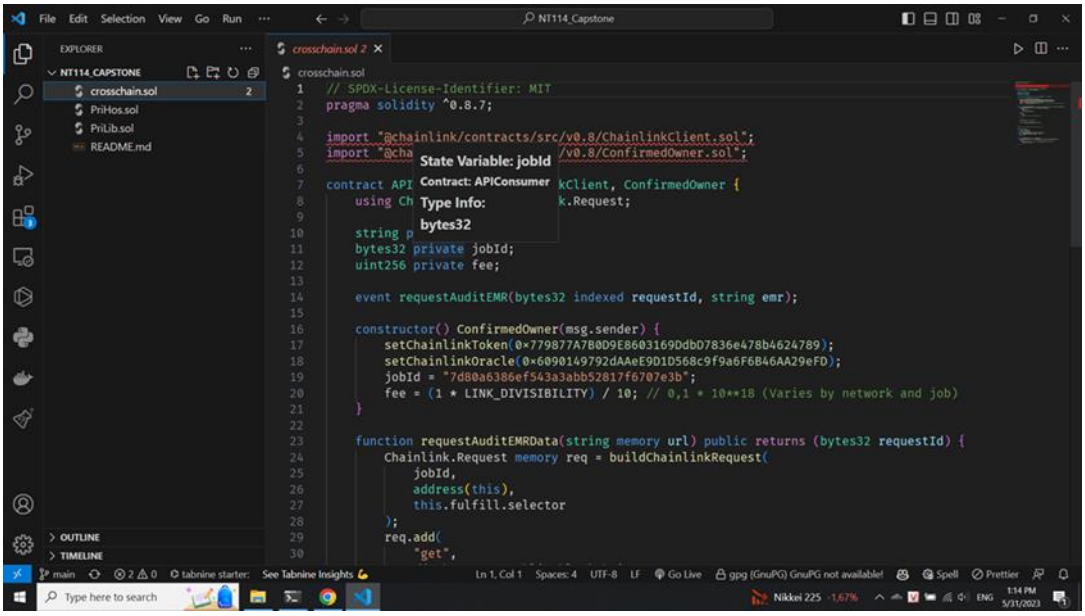
```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

library PriLib {

    // Patient
    struct Patient {
        bool registered;
    }

    struct Document {
        uint256 id;
        bool exists;
        address patient;
        address doctor;
        bytes32 keyHash;
    }

    // Doctor
    struct Doctor {
        bool registered;
    }

    // Manager
    struct Manager {
        bool registered;
    }

    // Audit data _ Manager call
```

Hình 10: Smart contract 1

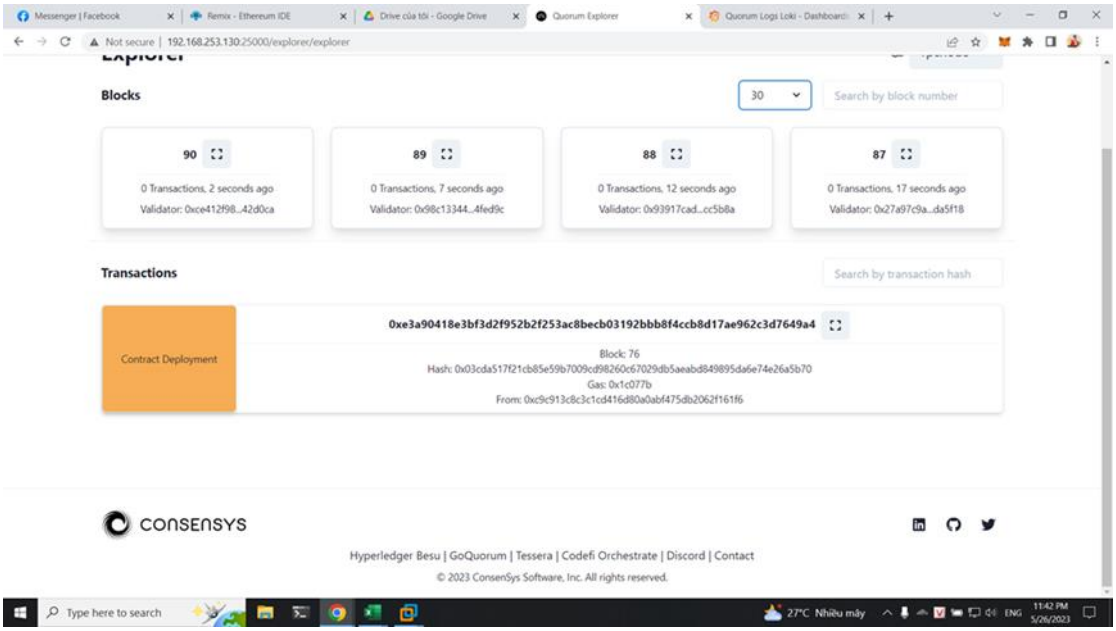


```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "./PriLib.sol";
import "./crosschain/crosschain.sol";
import "@openzeppelin/contracts/utils/Strings.sol";

contract PriHos {
    // Define Variable
    address public hospital;
    mapping(address => PriLib.Patient) public patients;
    mapping(address => PriLib.Doctor) public doctors;
    mapping(address => PriLib.Manager) public managers;
    mapping(bytes32 => PriLib.Document) public documents;
    mapping(uint256 => PriLib.CrosschainManager) public requestManagers;
    mapping(uint256 => PriLib.GrantCrosschainDoctor) public requestDoctors;
    mapping(uint256 => PriLib.requestData) public requestNormals;
    uint256 requestsCount;
    uint256 docsCount;
    string public docRequestID;

    // Modifier
    modifier onlyHospital {
        require(
            msg.sender == hospital,
            "Only regulatory agency smart contract hospital can call this function"
        );
        _;
    }
```

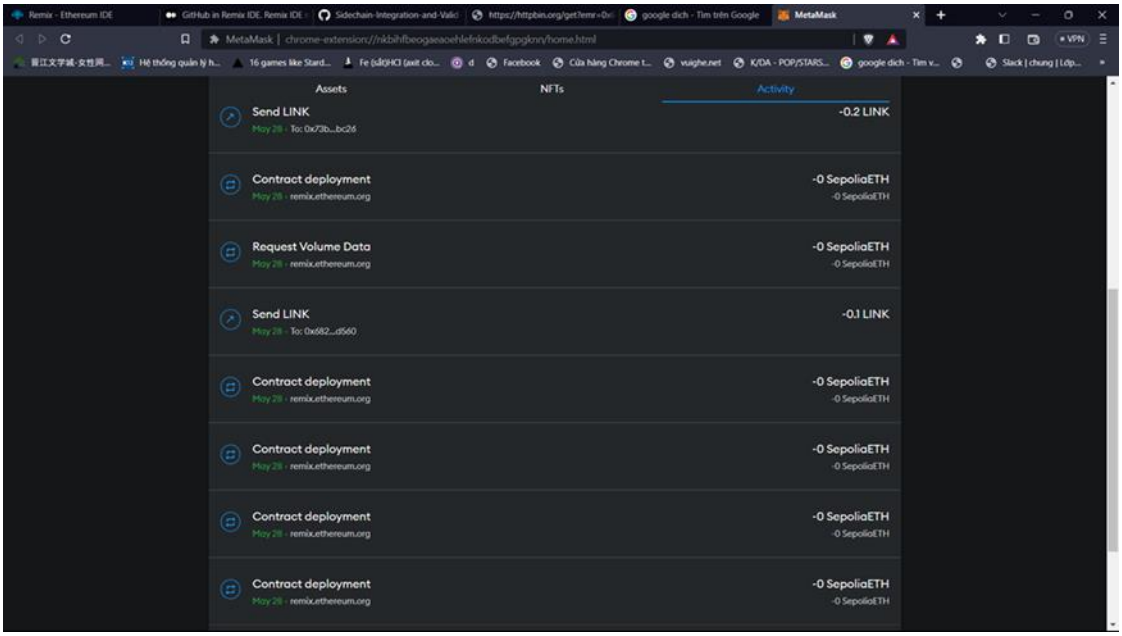
Hình 11: Smart contract 2



Hình 12: Smart contract 3

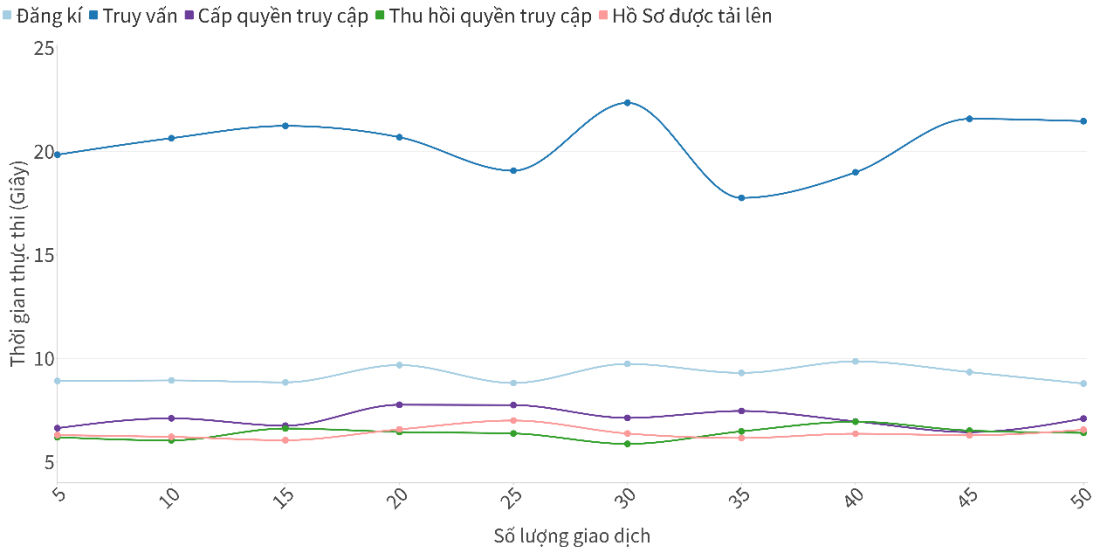


Hình 13: Deploy smart contract



Hình 14: Thông tin các transactions

Để đánh giá hiệu suất, nhóm đã theo dõi và đo lại thời lượng của các giao dịch này, như được minh họa trong hình 26 và đồng thời thực hiện nhiều lần đo cho từng giao dịch để đảm bảo độ chính xác và độ tin cậy cao nhất. Với hoạt động đăng ký tài khoản trên DApp, nó đòi hỏi một quy trình gồm nhiều bước liên quan đến việc tạo giao dịch trên PriBC, xác minh danh tính và ủy quyền, thường dẫn đến thời gian xử lý kéo dài hơn một chút so với các giao dịch khác. Tuy nhiên, kết quả về tổng thể thể hiện một triển vọng đặc biệt tích cực, củng cố cho những hứa hẹn phát triển rất thuận lợi trong tương lai. Trong bối cảnh giao dịch truy vấn liên quan đến tương tác giữa các chuỗi, phép đo ghi lại toàn bộ dòng thời gian hoạt động, bắt đầu từ thời điểm người dùng gửi yêu cầu cho đến khi nhận được kết quả kiểm tra tính toàn vẹn, cung cấp thông tin chi tiết có giá trị về hiệu quả và hiệu suất của chuỗi chéo giao tiếp. Qua đánh giá kỹ lưỡng, nhóm xác nhận rằng giải pháp đề xuất đã mang lại kết quả tích cực và có tiềm năng đầy hứa hẹn cho những tiến bộ trong tương lai.



Hình 15: Kết quả thực nghiệm về mặt thời gian

Ngoài ra, nhóm cũng đánh giá về mặt chi phí của hệ thống dựa trên giá trị trung bình của nhiều giao dịch. Bảng bên dưới trình bày kết quả tính toán và phí giao dịch cho mỗi giao dịch. Phí giao dịch cho mỗi giao dịch được đo bằng đơn vị gas và kết quả tính toán được hiển thị trong bảng. Mức tiêu thụ gas để đăng ký giao dịch cho mỗi thực thể vẫn ở mức trung bình nhất quán, và hoạt động này chỉ yêu cầu thực hiện một lần. Chi phí liên quan đến lưu trữ, truy cập dữ liệu và chuyển giao chuỗi chéo gắn liền với sự phức tạp của việc triển khai và truyền tải. Nhóm đánh giá rằng chi phí phát sinh khá hợp lý và nằm trong phạm vi có thể chấp nhận được. Ngoài ra, bảng này cũng cung cấp thông tin về mức sử dụng CPU liên quan đến từng giao dịch. Khi phân tích các quy trình khác nhau, giao dịch truy vấn có mức sử dụng CPU cao nhất, chiếm 76,31%. Do những hạn chế vốn có của thiết bị môi trường, mức sử dụng CPU có kết quả tương đối đáng kể. Tuy nhiên, giá trị này vẫn nằm trong giới hạn chấp nhận được, và có khả năng cải thiện đáng kể thông qua nâng cấp cấu hình phần cứng.

Object	**Transaction**	**CPU Usage**	**Gas**	**USD**
Blockchain Entities	Register Manager	66.29%	46407	4.46
	Register Doctor	66.17%	46378	4.45
	Register Patient	66.12%	46378	4.45
EMR	Store data	62.22%	92664	8.90
Data access control	Grant Permission	66.82%	161275	15.48
	Revoke Permission	66.60%	30261	2.91
Audit proof	Query	76.31%	229851	22.07

Bảng 2: Kết quả thực nghiệm về mặt hiệu năng và chi phí

4.3. Phân tích bảo mật

Để đạt tới hiệu suất tối ưu và bảo mật cho các mạng chuỗi khối, chuỗi khối ngoài của nhóm chúng tác giả hoạt động như một mạng Oracle phi tập trung, hoạt động độc lập để đảm bảo giải pháp được đề xuất không ảnh hưởng đến việc theo đuổi đó. Trong hệ thống này, trách nhiệm quản lý từng giao dịch thuộc về một nút Oracle, trong khi các nút khác đóng vai trò là người xác minh để duy trì tính minh bạch và ngăn chặn mọi hoạt động gian lận.

Để bảo mật tối đa thông tin được truyền trong quá trình truyền, nhóm chúng tác giả đã sử dụng các kỹ thuật mã hóa mạnh mẽ để bảo vệ quyền riêng tư và duy trì tính bảo mật, thậm chí chống lại các cuộc tấn công trung gian.

Để thiết lập một biện pháp kiểm soát truy cập mạnh mẽ, hệ thống của nhóm tác giả đã sử dụng một khung dựa trên vai trò để gán các quyền cụ thể cho các thực thể khác nhau. Bằng cách triển khai phân chia vai trò này, các yêu cầu xác minh dữ liệu chỉ được giới hạn ở người dùng quyền cao để giảm thiểu khả năng bị tấn công từ chối dịch vụ.

4.4. Hạn chế

Nhóm tác giả đã xây dựng được một hệ thống trao đổi dữ liệu cho quá trình xác minh dữ liệu giữa các chuỗi khối khác kiến trúc một cách an toàn và nhanh chóng thông qua việc sử dụng các node oracles và thực hiện quản lí truy cập bằng khóa có thời hạn khi có yêu cầu trao đổi hoặc chia sẻ dữ liệu để đảm bảo được tính riêng tư, bảo mật của các dữ liệu quan trọng. Kết quả từ các thực nghiệm cũng đã cho thấy tính khả thi của hệ thống trong ngữ cảnh bệnh viện được đưa ra.

Tuy nhiên, việc sử dụng chuỗi khối ngoài với kiến trúc là một mạng oracle phi tập trung cũng dẫn đến một số hạn chế cần phải xem xét như:

- Khó mở rộng mạng chuỗi khối ngoài: Nếu chúng ta cần phát triển hệ thống, cần yêu cầu nhiều nodes oracle để làm nhiệm vụ vận chuyển dữ liệu trao đổi hơn thì việc mở rộng chuỗi khối ngoài là một vấn đề thiết yếu cần đối mặt. Thế nhưng hiện tại, mở rộng chuỗi khối ngoài đồng nghĩa với việc sẽ cần nhiều phần cứng hơn, nhiều nodes orcale thì quá trình xác minh các giao dịch sẽ tốn nhiều thời gian và nhiều chi phí hơn, dẫn đến hiệu suất và tính thực tế của hệ thống bị giảm.
- Vấn đề về bảo mật ở các điểm đầu cuối từ các ứng dụng phi tập trung: Hiện tại, hệ thống sẽ giao tiếp với các chuỗi khối thông qua các ứng dụng phi tập trung, tuy nhiên việc kiểm soát các yêu cầu bảo mật ở ứng dụng phi tập trung của các hệ thống chuỗi khối vẫn là một vấn đề cần lưu ý nhằm đảm bảo cho các dữ liệu được trao đổi giữa hai chuỗi khối một cách an toàn.

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

5.1. Kết luận

Nhóm tác giả giới thiệu một giải pháp cho khả năng tương tác chuỗi khối, tận dụng sức mạnh của chuỗi khối ngoài và khóa thời gian hợp lệ (khóa có thời hạn). Trong đó, chuỗi khối ngoài của chúng tôi hoạt động như một mạng phi tập trung, đóng vai trò then chốt là một trung gian đáng tin cậy, tạo ra các kết nối liền mạch với vô số chuỗi khối không đồng nhất.

Ngoài ra, nhóm cũng trình bày một khái niệm đột phá được gọi là khóa có thời hạn để tăng cường quản lý truy cập dữ liệu an toàn và thuận tiện. Kết quả thử nghiệm khẳng định hiệu suất vượt trội của hệ thống của chúng tôi về chức năng và khả năng tương tác liên chuỗi khối liền mạch, hoàn toàn đảm bảo các yêu cầu về bảo mật thông tin được trao đổi liên chuỗi.

5.2. Hướng phát triển

Trong công việc trong tương lai, nhóm hướng tới việc nâng cao hiệu suất hệ thống, tối ưu hóa chi phí và thực hiện thử nghiệm rộng rãi để mở khóa toàn bộ tiềm năng của việc kết hợp dữ liệu chuỗi khối bên ngoài. Mặt khác, chúng tôi nhận thấy được vẫn còn tồn tại một số vấn đề về bảo mật trong quả trình trao đổi liên chuỗi ở các điểm đầu cuối từ các ứng dụng phi tập trung, vì vậy việc cải thiện mức độ an toàn của hệ thống cũng là một trong những hướng phát triển quan trọng mà chúng em nhắm đến. Hơn nữa, nhóm nhận ra tầm quan trọng của việc giải quyết các kịch bản dữ liệu có thể thay đổi và bắt tay vào khám phá các phương pháp thay thế cho các hàm băm có thể xác minh hiệu quả tính toàn vẹn của dữ liệu đó trong khi tương thích với chuỗi khối.

TÀI LIỆU THAM KHẢO

1. M. Rauchs, A. Blandin, K. Bear, and S. B. McKeon, “2nd global enterprise blockchain benchmarking study,” Available at SSRN 3461765, 2019.
2. M. V. Baysal, O. ¨ Ozcan-Top, and A. Betin-Can, “Blockchain technology ¨ applications in the health domain: A multivocal literature review,” The Journal of supercomputing, vol. 79, no. 3, pp. 3112–3156, 2023.
3. R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, “A survey on blockchain interoperability: Past, present, and future trends,” ACM Computing Surveys (CSUR), vol. 54, no. 8, pp. 1–41, 2021.
4. M.-H. Kuo et al., “Opportunities and challenges of cloud computing to improve health care services,” Journal of medical Internet research, vol. 13, no. 3, e1867, 2011.
5. S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, “Interoperability and synchronization management of blockchain-based decentralized e-health systems,” IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1363–1376, 2020.
6. T. Hardjono, A. Lipton and A. Pentland, "Toward an Interoperability Architecture for Blockchain Autonomous Systems," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1298-1309, Nov. 2020.
7. N. Spence, M. Niharika Bhardwaj, and D. P. Paul III, “Ransomware in healthcare facilities: A harbinger of the future?” Perspectives in Health Information Management, pp. 1–22, 2018.
8. N. Thamer and R. Alubady, “A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,” in 2021 1st BICITS, IEEE, 2021, pp. 210–216.
9. Roehrs, C. A. Da Costa, and R. da Rosa Righi, “Omniphr: A distributed architectureb model to integrate personal health records,” Journal of biomedical informatics, vol. 71, pp. 70–81, 2017.
10. Y. Pang, “A new consensus protocol for blockchain interoperability architecture,” IEEE Access, vol. 8, pp. 153 719–153 730, 2020.
11. S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, “Towards blockchain interoperability,” in Business Process Management: BPM 2019 Blockchain and CEE Forum, Vienna, Austria, Proceedings 17, Springer, 2019, pp. 3–10.
12. V. Buterin, “R3 report-chain interoperability,” R3 Res, 2016.
13. Z. Wang, J. Li, X.-B. Chen, and C. Li, “A secure cross-chain transaction model based on quantum multi-signature,” Quantum Information Processing, vol. 21, no. 8, p. 279, 2022.

14. Monika, R. Bhatia, A. Jain, and B. Singh, “Hash time locked contract based asset exchange solution for probabilistic public blockchains,” Cluster Computing, vol. 25, no. 6, pp. 4189–4201, 2022.
15. R. Bhatia, A. Jain, and B. Singh, “Hash time locked contract based asset exchange solution for probabilistic public blockchains,” Cluster Computing, vol. 25, no. 6, pp. 4189–4201, 2022.
16. J. Kwon and E. Buchman, “Cosmos whitepaper,” A Netw. Distrib. Ledgers, p. 27, 2019.
17. G. Wood, “Polkadot: Vision for a heterogeneous multi-chain framework,” White paper, vol. 21, no. 2327, p. 4662, 2016.

ĐẠI HỌC QUỐC GIA TP. HCM
TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự do - Hạnh Phúc

TP.HCM, ngày tháng năm 2023

THÔNG TIN KẾT QUẢ NGHIÊN CỨU

1. Thông tin chung:

- Tên đề tài: HƯỚNG TỚI KHẢ NĂNG TƯƠNG TÁC LIÊN CHUỖI SỬ DỤNG CHUỖI KHỐI NGOÀI VÀ KIỂM SOÁT TRUY CẬP DỮ LIỆU BẰNG KHOÁ CÓ THỜI HẠN

- Mã số:

- Chủ nhiệm: Võ Anh Kiệt - 20520605

- Thành viên tham gia: Nguyễn Bùi Kim Ngân – 20520648, Nguyễn Bình Thục Trâm - 20520815

- Cơ quan chủ trì: Trường Đại học Công nghệ Thông tin.

- Thời gian thực hiện: 6 tháng

2. Mục tiêu: Xây dựng hệ thống liên chuỗi để vận chuyển dữ liệu giữa hai mạng blockchain khác nhau thông qua chuỗi khối ngoài (sidechain) và triển khai kiểm soát truy cập dữ liệu dựa trên vai trò bằng khóa có thời gian.

3. Tính mới và sáng tạo: Hệ thống sidechain được xây dựng gồm các nút oracle bên trong. Sidechain đóng vai trò là một cầu nối giao tiếp giữa hai chuỗi khối, đồng thời đảm bảo tính hợp lệ của dữ liệu bằng cách sử dụng các nút oracle còn lại xác minh khi có một nút oracle thực hiện giao dịch liên chuỗi. Đồng thời, việc triển khai kiểm soát truy cập dữ liệu bằng khóa có thời hạn giúp bảo vệ dữ liệu an toàn trước những truy cập trái phép.

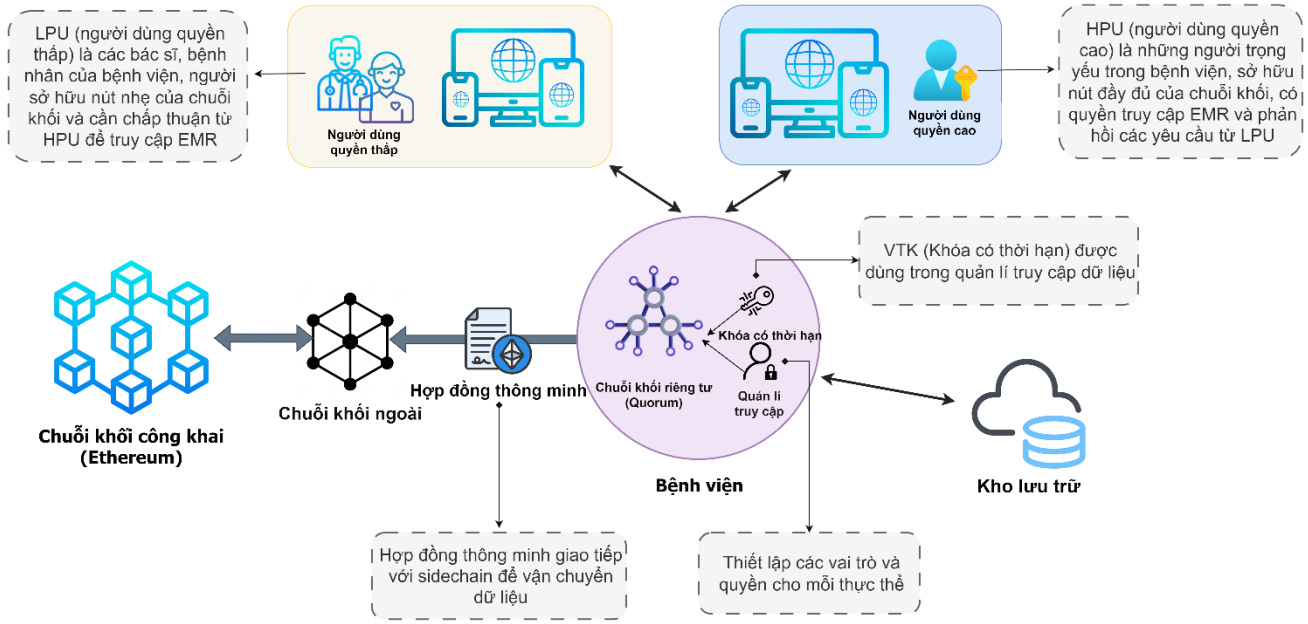
4. Tóm tắt kết quả nghiên cứu: Hệ thống được triển khai hoạt động liền mạch trên nhiều mạng blockchain khác nhau, quy trình diễn ra một cách tự động, giảm thiểu tối đa sự can thiệp của người dùng cuối. Về kết quả thực nghiệm cho thấy hệ thống có hiệu suất tốt về mặt thời gian và chi phí tiêu tốn.

5. Tên sản phẩm: Hướng tới khả năng tương tác liên chuỗi sử dụng chuỗi khối ngoài và kiểm soát truy cập dữ liệu bằng khoá có thời hạn

6. Hiệu quả, phương thức chuyển giao kết quả nghiên cứu và khả năng áp dụng: Nhóm tác giả đã tiến hành thử nghiệm hệ thống sidechain với 2 mạng blockchain riêng biệt là Ethereum và Quorum trong bối cảnh chăm sóc sức khỏe y tế. Nhằm bảo đảm cho tính toàn vẹn cho Hồ sơ y tế được quản lý trong bệnh viện xây dựng Quorum, hệ thống

sidechain đã làm trung gian vận chuyển bằng chứng toàn vẹn của dữ liệu lên mạng blockchain công khai là Ethereum. Qua đó khi cần kiểm tra Hồ sơ, sidechain cũng sẽ làm nhiệm vụ vận chuyển bằng chứng về mạng của bệnh viện. Kết quả cho thấy khả năng hoạt động và tính khả thi của hệ thống sidechain trong việc vận chuyển dữ liệu liên chuỗi, cũng như tiềm năng mở rộng khả năng ứng dụng cho các lĩnh vực khác.

7. Hình ảnh, sơ đồ minh họa chính



Cơ quan Chủ trì	**Chủ nhiệm đề tài**
(ký, họ và tên, đóng dấu)	*(ký, họ và tên)*