ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO NGHIÊN CỨU KHOA HỌC SINH VIÊN

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

Enhancing Blockchain Interoperability through Sidechain Integration and Valid-Time-Key Data Access Control

Giáo viên hướng dẫn: **Th.S Trần Tuấn Dũng**

Sinh viên thực hiện: **Võ Anh Kiệt – 20520605**

Nguyễn Bùi Kim Ngân – 20520648

Nguyễn Bình Thục Trâm – 20520815

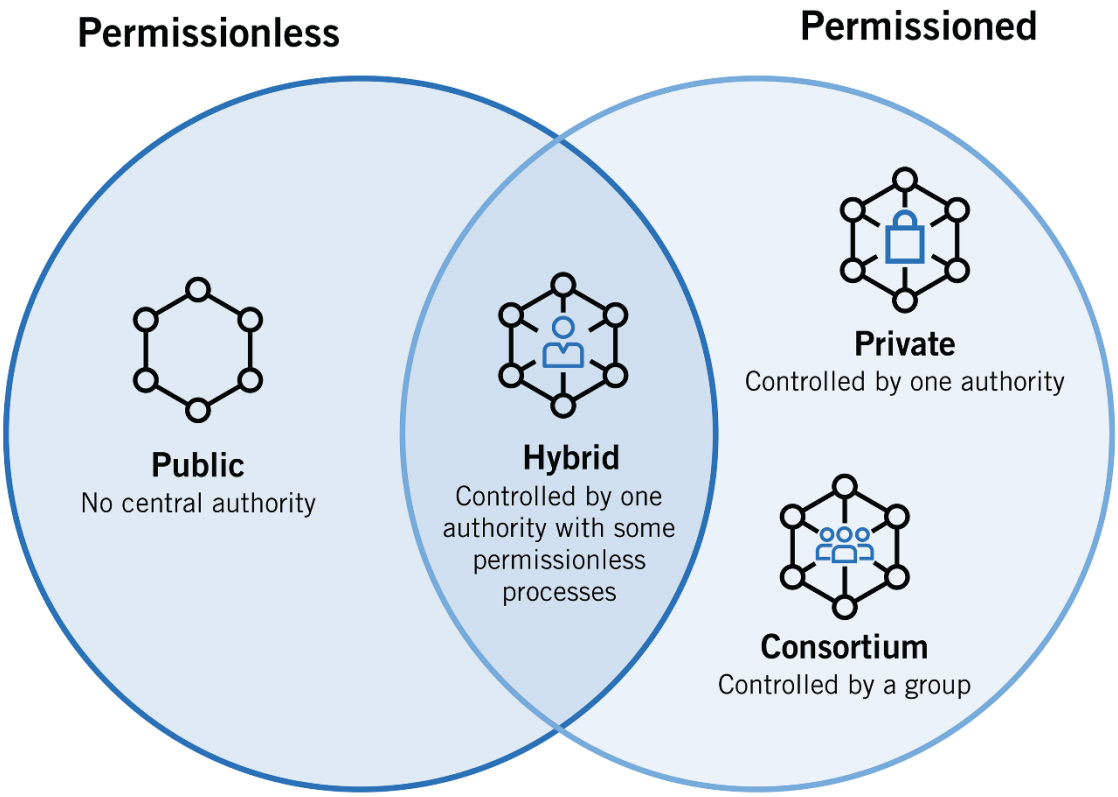
Lớp: **ATTN.2020**

Thành phố Hồ Chí Minh, tháng 6 năm 2023

MỤC LỤC

CHƯƠNG 1: TÓM TẮT ĐỀ TÀI

Chuỗi khối đã được ứng dụng rộng rãi trong nhiều ngành như tài chính, bảo hiểm, chăm sóc sức khỏe, hỗ trợ xã hội và giáo dục. 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. Do đó để công nghệ chuỗi khối có thể phát triển mạnh mẽ và có khả năng áp dụng được với nhiều ngữ cảnh hơn, việc thúc đẩy sự phát triển trong các mối liên kết giữa các chuỗi khối khác kiến trúc là một khía cạnh vô cùng quan trọng.



Hình 1. Sự khác biệt giữa các kiến trúc chuỗi khối

Đặc biệt là trong lĩnh vực chăm sóc sức khỏe 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. 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

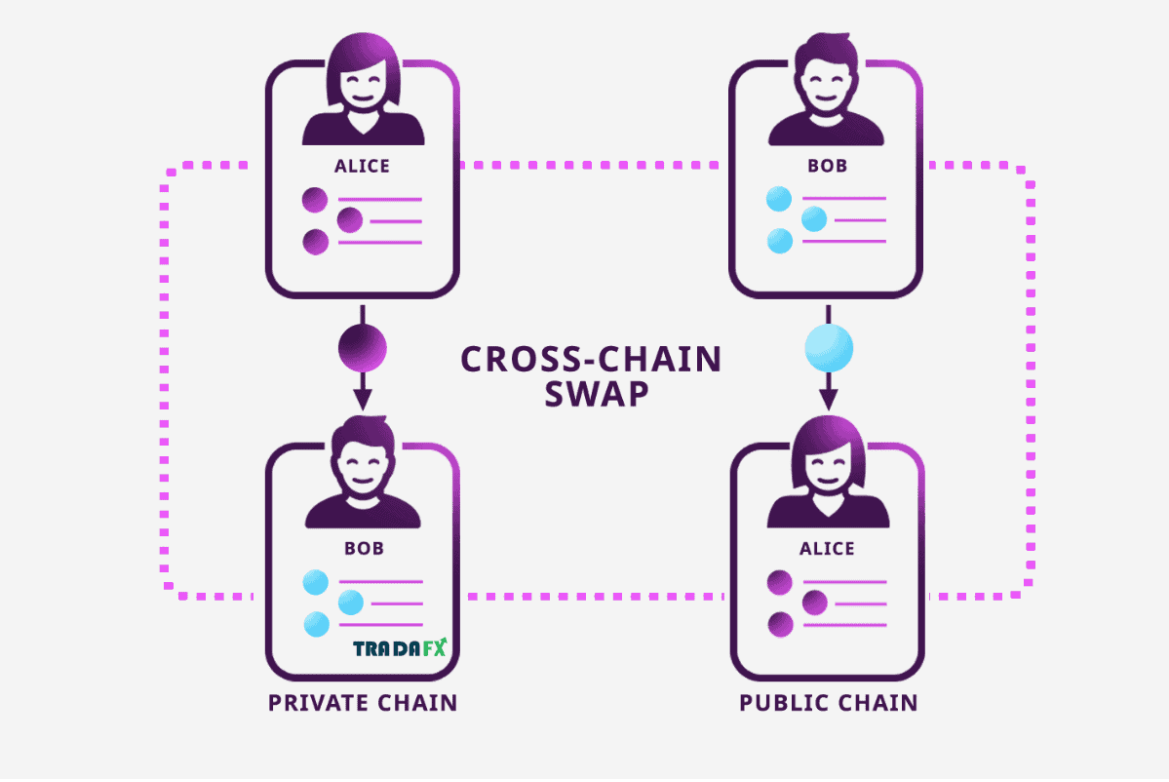
cấp dữ liệu có độ chính xác cao để đáp ứng kịp thời cho quá trình chăm sóc và điều trị bệnh nhân một cách tốt nhất.

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. Chúng tôi đề xuất hướng giải quyết bằng cách xây dựng một hệ thống chuỗi khối ngoài (Sidechain) gồm các nút Oracle bên trong. Bên cạnh đó chúng tôi cũng giới thiệu cơ chế thực thi kiểm soát truy cập dữ liệu và thực hiện cấp quyền tương tác liên chuỗi thông qua khóa có thời hạn (Valid time key – VTK). Qua đó, mô hình được đề xuất hoạt động một cách tối ưu, liền mạch, đáp ứng yêu cầu trao đổi dữ liệu liên chuỗi, đồng thời có thể tăng cường bảo mật dữ liệu của hệ thống mạng nội bộ.

CHƯƠNG 2: NỘI DUNG ĐỀ TÀI

2.1. Tóm tắt các công trình liên quan

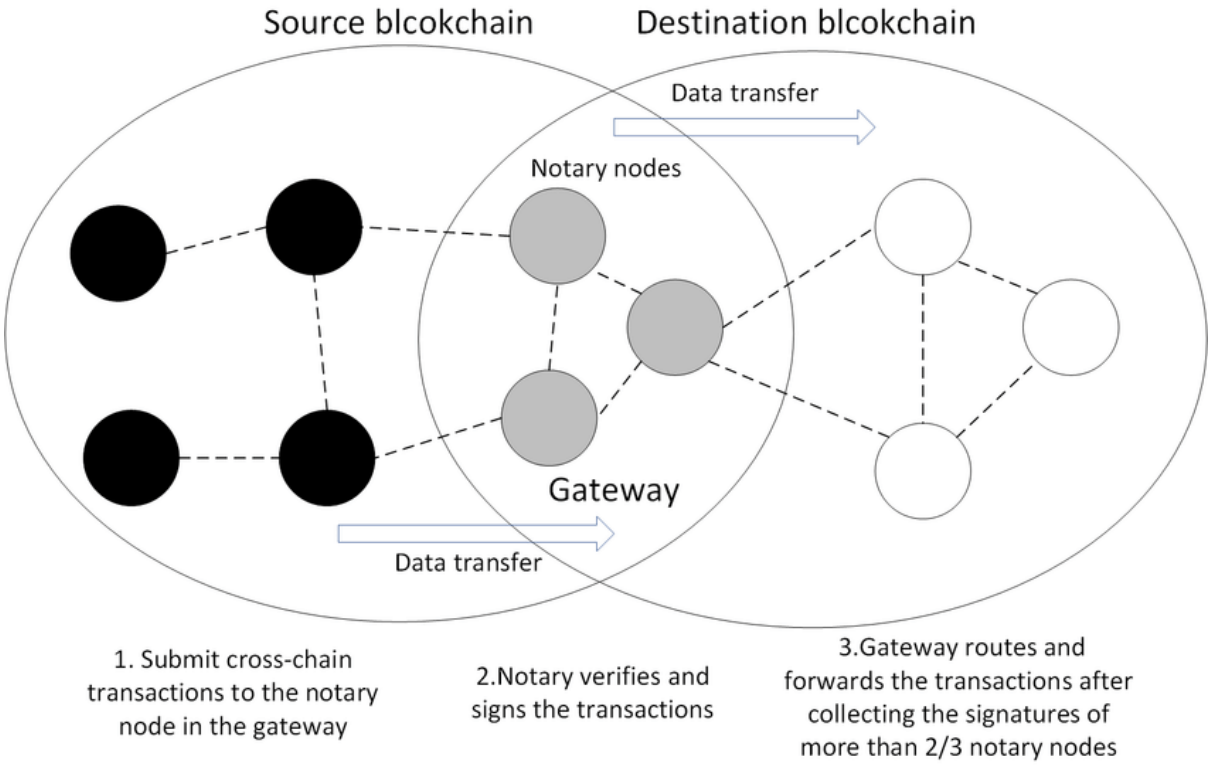
Để đạt được khả năng tương tác liên chuỗi và thực hiện liền mạch các hợp đồng thông minh giữa các mạng chuỗi khối khác kiến trúc, việc áp dụng các giao thức được tiêu chuẩn hóa và các phương pháp mới mẻ nổi lên như những yếu tố then chốt. Bằng cách nắm bắt những phát kiến đáng chú ý này, chúng ta có 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.



Hình 2. Mô phỏng chuỗi chéo

2.1.1. Phương pháp Notary

Phương pháp Notary được gợi ý là một trong những hướng tiếp cận cho giải pháp liên chuỗi tương đối đơn giản. Cơ chế này liên quan đến 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. 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 sự tin tưởng mù quáng.



Hình 3. Mô phỏng phương pháp Nontary Blockchain Interoperability

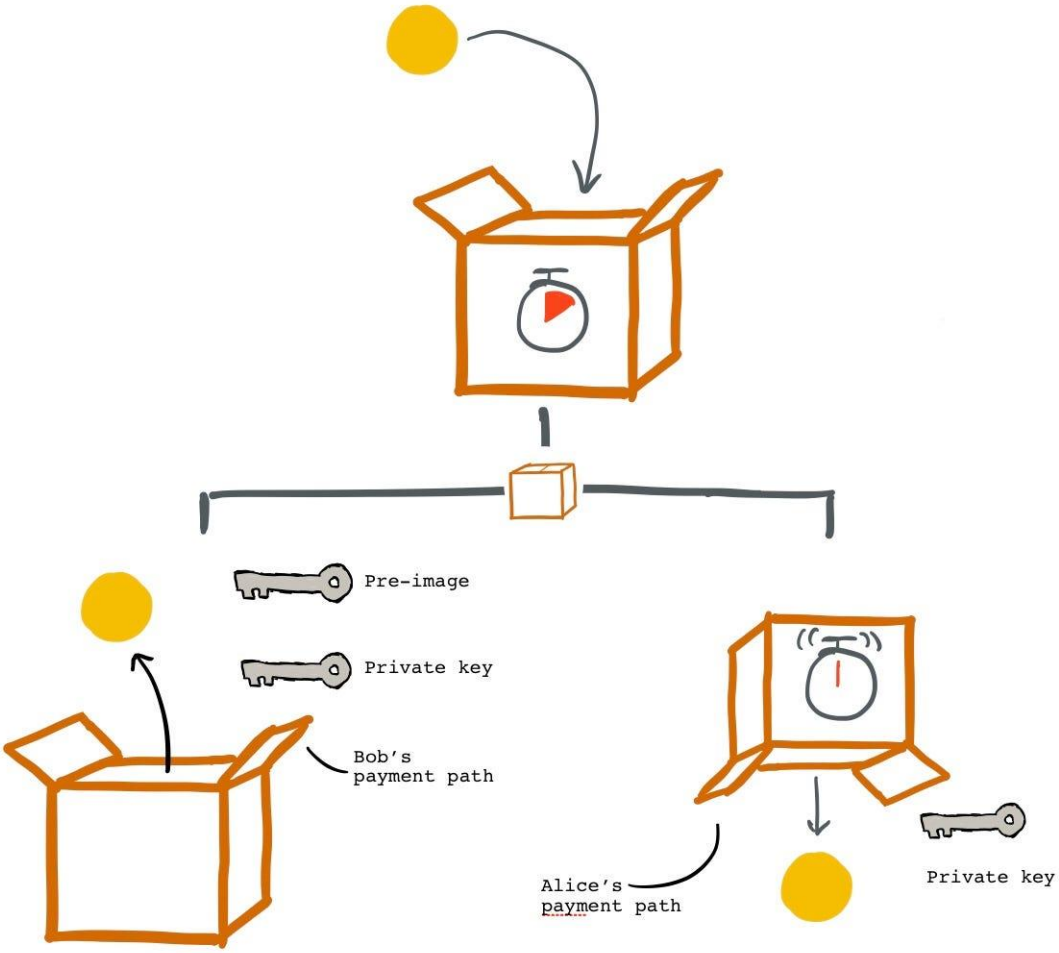
Như trên Hình 3 đã miêu tả, sẽ có 3 nút Notary đóng vai là "người xác minh" (verifier) xác minh các giao dịch và thực hiện quá trình vận chuyển dữ liệu giữa hai chuỗi khối không cùng kiến trúc theo yêu cầu của một trong hai chuỗi khối. Trong quá trình này, các nút Notary sẽ xác minh và kí vào các giao dịch được tạo ra bởi chuỗi khối nguồn. Tiếp đến, giao dịch được gửi đến sẽ được tin tưởng nếu như chuỗi khối đích có thể thu thập được ít nhất là 2/3 chữ ký xác minh từ các nút Notary ở giữa. Sau khi đã kiểm tra xong, chuỗi khối đích sẽ thu thập dữ liệu và giao dịch từ chuỗi khối nguồn, hoàn thành quá trình trao đổi dữ liệu.

Như vậy, các nút Notary đóng vai trò là bên thứ ba và trình kết nối của chúng có thể được xem như một loại "công chứng" cho các hành động chuyển đổi dữ liệu và thực hiện giao dịch liên chuỗi, cho phép chuyển giá trị giữa những người dùng từ các chuỗi khối khác kiến trúc với nhau. Nhưng đồng thời, làm thế nào để đảm bảo độ tin cậy, tính bảo mật của quá trình "công chứng" và tính toàn vẹn của giao dịch là một phần gây tranh cãi cho phương pháp này.

Mặt khác, các nút Notary này cũng có thể gây ra tình trạng "thắt nút cổ chai" trong quá trình xử lý nếu như số lượng giao dịch liên chuỗi tăng quá nhiều và số lượng nút Notary không đủ để đáp ứng. Song song với đó, việc xây dựng các nút Notary còn gặp phải vấn đề chính là gây nên tính tập trung hóa, dễ bị tấn công mạng và có thể khiến cho các thông tin được vận chuyển không thể đảm bảo. Nhưng nếu tăng số lượng nút Notary lên thì cũng đồng nghĩa với việc chi phí bỏ ra để xây dựng hệ thống sẽ tăng cao và quá trình xác minh có thể mất nhiều thời gian do số lượng chữ ký kiểm tra cũng sẽ tăng lên theo.

2.1.2. Phương pháp Hash-locking

Ngoài phương pháp Notary thì khóa băm cũng là một hướng tiếp cận vấn đề chuỗi chéo rất được quan tâm hiện nay. 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.



Hình 4. Mô phỏng phương pháp Hash – locking

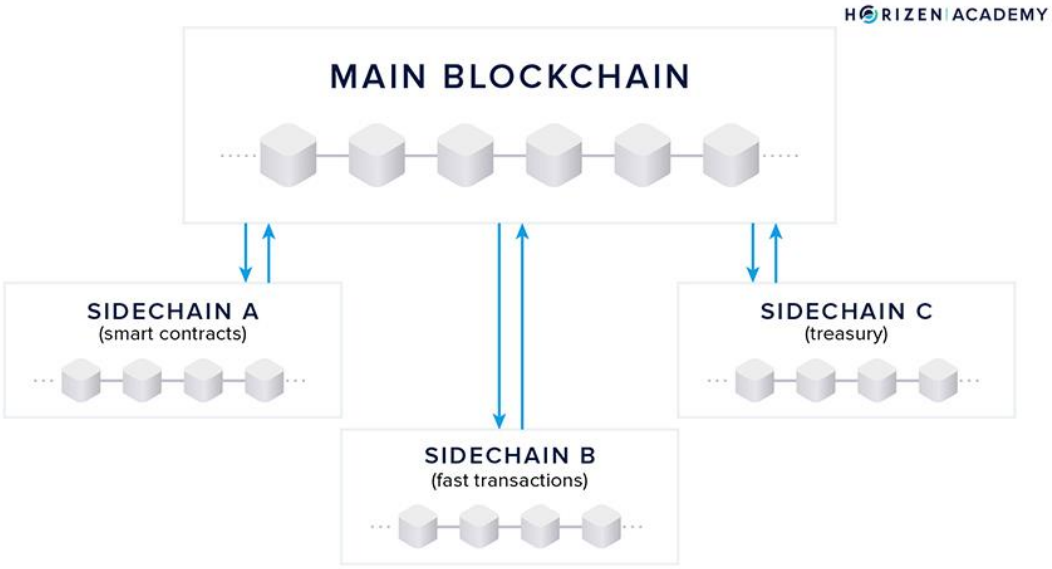
Hình 4 bên trên mô phỏng cách cụ thể hóa quá trình trao đổi dữ liệu giữa hai chuỗi khối trong một ngữ cảnh nhất định là trao đổi tiền điện tử. Ở đây, Bob muốn gửi một giá trị tiền điện tử cho Alice. Để hoàn thành mục tiêu này, Bob sẽ gửi giá trị băm của tiền điện tử cho Alice và các loại tiền điện tử tương ứng sẽ bị khóa. Nếu Alice có thể đưa ra giá trị chính xác của tiền điện tử bị khóa từ hàm băm của nó, thì tài sản bị khóa sẽ được chuyển cho người nhận. Còn ngược lại, nếu Alice không thể đưa ra giá trị chính xác trong thời gian quy định, số tiền này sẽ được hoàn trả về ví thanh toán của Bob.

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. Yêu cầu này gần như là rất khó để có thể được đáp ứng, đồng thời nó sẽ đặt ra những hạn chế trong các tình huống trong đó các chuỗi

tham gia sử dụng các thuật toán băm riêng biệt hoặc sở hữu các điều kiện kỹ thuật tiên quyết khác nhau. Hơn nữa, có một thách thức đáng kể nằm ở chi phí cao và các yêu cầu thiết kế phức tạp liên quan đến việc đảm bảo sự hiểu biết lẫn nhau và khả năng tương thích của các hợp đồng thông minh trên các chuỗi khối khác nhau.

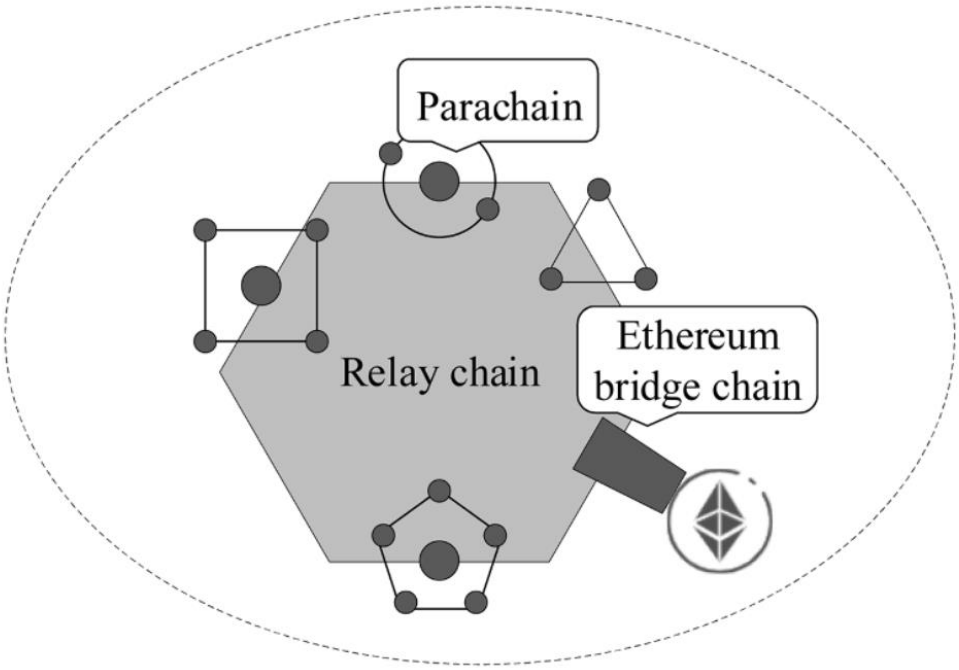
2.1.3. Phương pháp Relays/Chuỗi khối ngoài (Sidechain)

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.

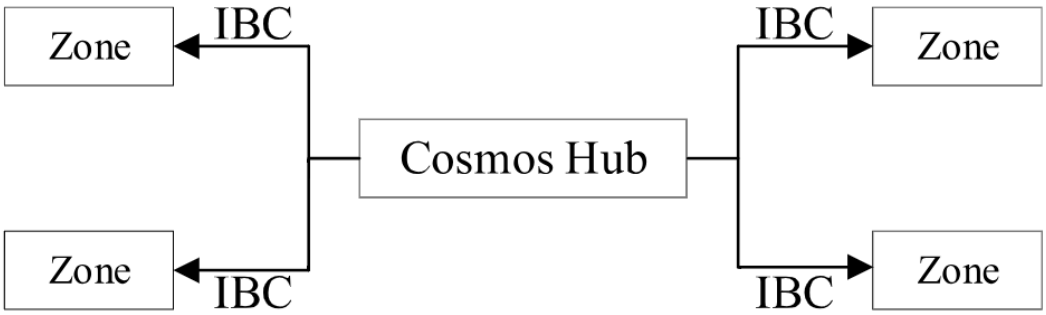


Hình 5. Mô phỏng phương pháp Relays/Sidechain

Cosmos và Polkadot là những platform 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.



Hình 6. Tổng quan về framework của Polkadot

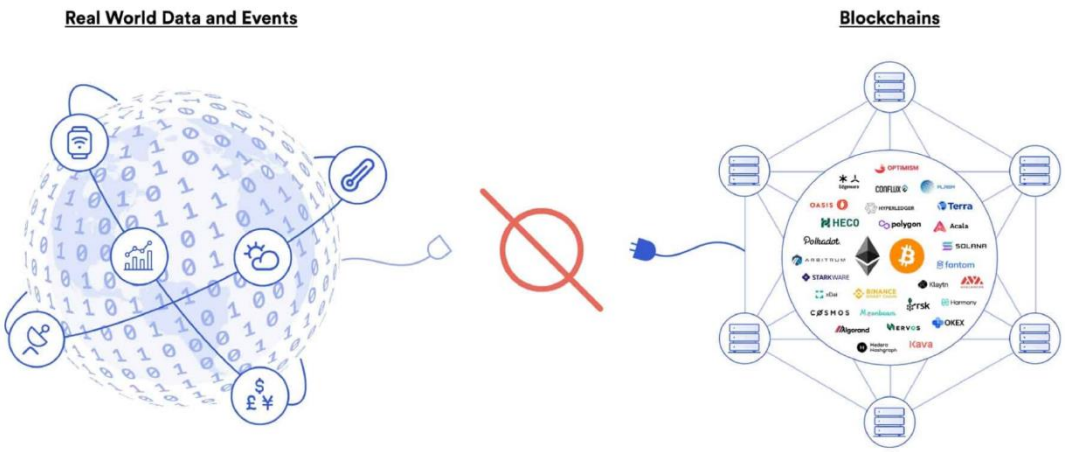


Hình 7. Triển khai Cosmos sử dụng giao thức IBC để giao tiếp liên chuỗi

2.1.4. Chuỗi khối Oracle

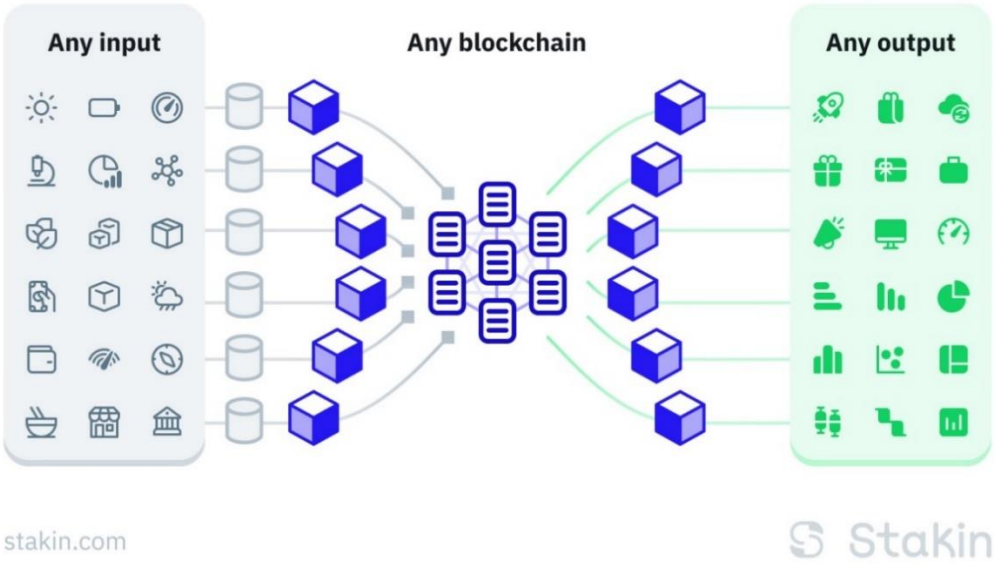
Bài toán mang đến ý tưởng xây dựng chuỗi khối Oracle bắt nguồn từ một hạn chế cơ bản của các hợp đồng thông minh, đó là chúng vốn không thể tương tác với dữ liệu và hệ thống tồn tại bên ngoài môi trường chuỗi khối gốc của chúng. Các tài nguyên bên ngoài chuỗi khối được coi là tài nguyên "off-chain" (ngoài 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 Oracle được ra đời.



Hình 8. Sự thiếu kết nối của dữ liệu và sự kiện với Blockchains

Các nút Oracle này là một giải pháp để hệ sinh thái Web3 phi tập trung có thể truy cập vào các nguồn dữ liệu hiện có, các hệ thống kế thừa và tính toán nâng cao ngoài chuỗi. Các mạng Oracles phi tập trung (Decentralized oracle networks - DON) cho phép tạo các hợp đồng thông minh lai, trong đó mã trên chuỗi và cơ sở hạ tầng ngoài chuỗi được kết hợp để hỗ trợ các ứng dụng phi tập trung (DApp) tiên tiến phản ứng với các sự kiện trong thế giới thực và tương tác với các hệ thống truyền thống.



Hình 9. Cách hoạt động của chuỗi khối Oracles

2.2. Tính khoa học, tính mới

Để khắc phục trở ngại trong việc truyền dữ liệu giữa các chuỗi khối riêng biệt, chúng tôi đề xuất hướng giải quyết bằng cách xây dựng một hệ thống chuỗi khối ngoài (Sidechain) gồm các nút Oracle bên trong. Chuỗi khối ngoài 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 buộc các nút Oracle còn lại xác minh khi có một nút Oracle thực hiện giao dịch liên chuỗi.

Bên cạnh đó chúng tôi cũng giới thiệu cơ chế thực thi kiểm soát truy cập dữ liệu và thực hiện cấp quyền tương tác liên chuỗi thông qua khóa có thời hạn (Valid time key – VTK). Kết hợp hai điều này, hệ thống đã cho thấy được những giới hạn rõ ràng và nghiêm ngặt, đảm bảo rằng việc trao đổi và xem dữ liệu chỉ được thực hiện bởi các bên liên quan đã được được cấp quyền. Mặt khác, chúng tôi cũng đặt nhiều sự lưu tâm vào vấn đề bảo mật dữ liệu và quyền riêng tư của người dùng hệ thống, vì vậy giải pháp của nhóm chúng em đã đưa ra một số những đóng góp đáng kể trong các khía cạnh sau:

Đề xuất được một hướng tiếp cận mới cho vấn đề trao đổi dữ liệu giữa hai chuỗi khối khác kiến trúc, cụ thể chính là sáng tạo một hệ thống liên chuỗi được xây dựng dựa trên kiến trúc chuỗi khối ngoài để vận chuyện dữ liệu giữa hai chuỗi khối khác kiến trúc,

cung cấp bằng chứng xác minh tính minh bạch của dữ liệu. Đồng thời, hệ thống kết hợp kiểm soát truy cập thông qua việc triển khai cơ chế khóa có thời hạn để đảm bảo các quy tắc về an toàn thông tin.

Hệ thống của chúng tôi đã được triển khai và thử nghiệm thành công trên mạng thử nghiệm (testnet) các nền tảng chuỗi khối của các bên liên quan, kết quả cho thấy khả năng vận chuyển và chia sẻ dữ liệu liên chuỗi mà hệ thống mang lại thật sự nhanh chóng và an toàn. Các tiêu chí về hiệu suất, chi phí và bảo mật đã được kiểm nghiệm và đánh giá, cho tới hiện tại, các kết quả cho ra đều theo hướng tích cực.

CHƯƠNG 3: MỤC TIÊU - PHƯƠNG PHÁP

3.1. Mục tiêu công trình

Chúng tôi đề xuất hệ thống liên chuỗi mới để vận chuyển dữ liệu liền mạch và hiệu quả qua lại giữa hai mạng blockchain khác nhau thông qua Sidechain – 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 đề suất không gây ảnh hưởng tới hiệu suất và bảo mật của blockchain mẹ.

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

Quy trình vận chuyển dữ liệu được diễn ra một cách tự động hóa, giảm thiểu tối đa sự can thiệp của người dùng cuối.

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.

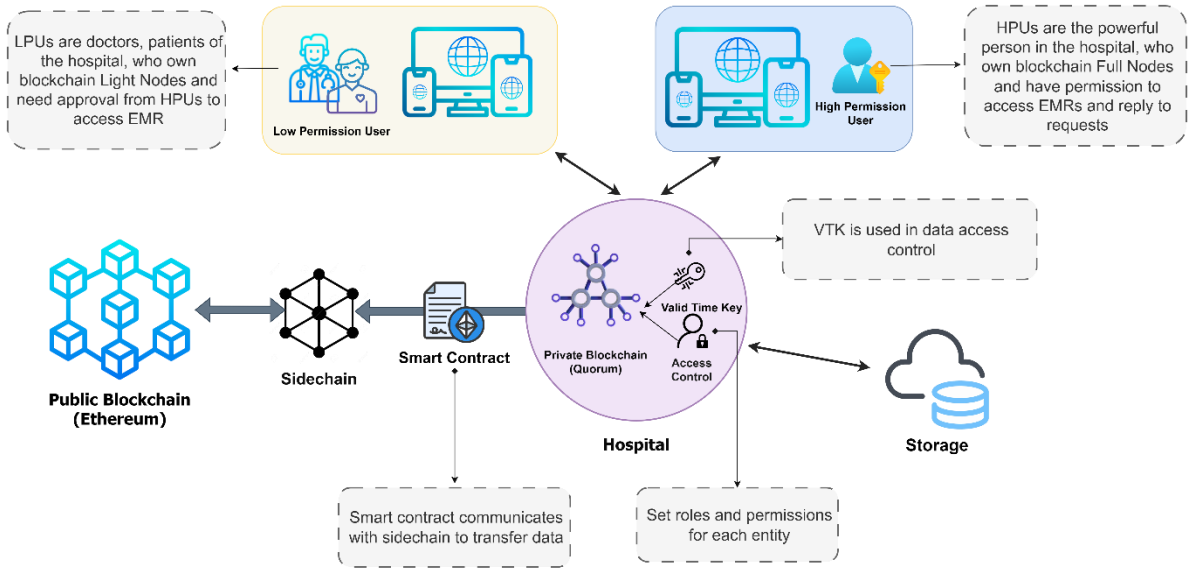
3.2. Tổng quan giải pháp

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 của 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 chúng em 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.

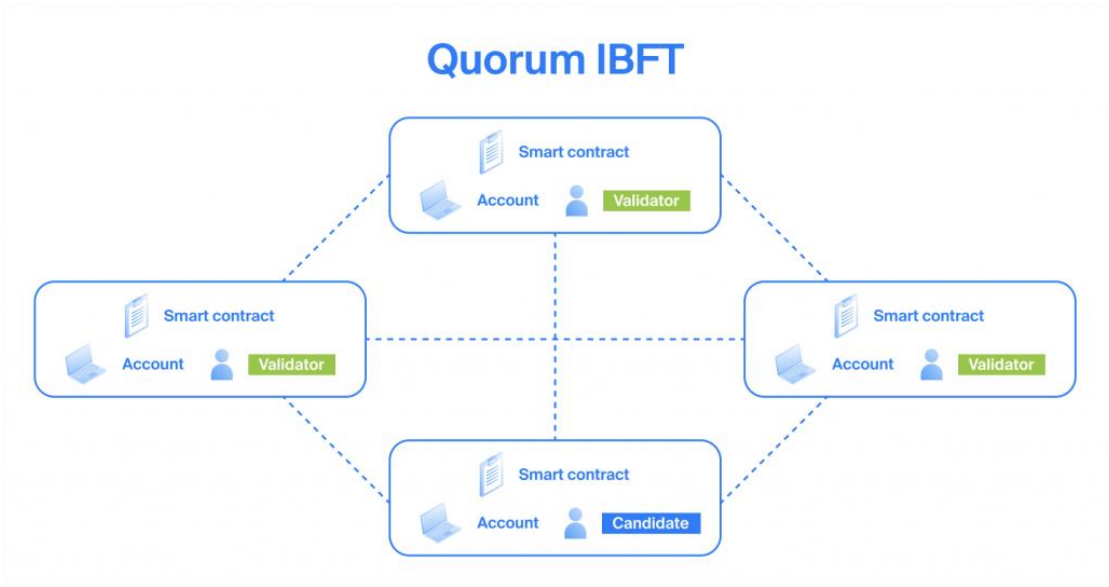


Hình 10. Mô hình tổng quan của hệ thống

3.3. Hệ thống chuỗi khối

3.3.1. Các mạng chuỗi khối

Thứ nhất, về mạng chuỗi khối riêng, chúng tôi 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, chúng tôi 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.



Hình 11. Mạng Quorum cung cấp khả năng phần quyền các nút

Có ba vai trò chính cho các thực thể trong mạng chuỗi khối riêng:

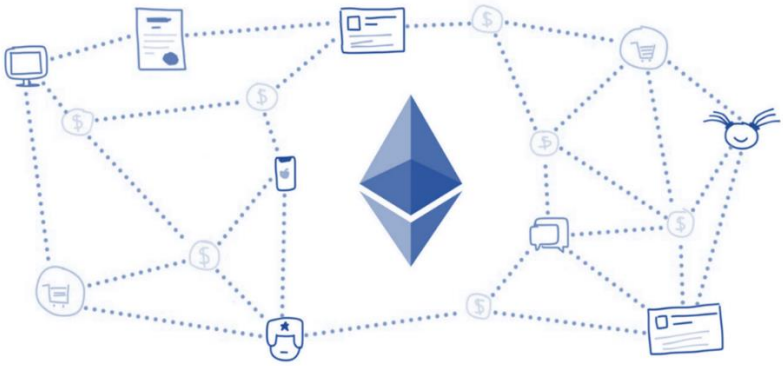
Bác sĩ/Nhân viên y tế/Bệnh nhân có liên quan - Người dùng có quyền hạn thấp là các nút nhẹ có quyền gửi yêu cầu để đọc EMR nếu được cấp khóa có thời hạn để truy cập bởi các nút đầy đủ. Thông tin chi tiết về khóa có thời hạn sẽ được giải thích trong phần sau.

Trưởng khoa/Người quản lý (Manager) - 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.

Hình 12. Vai trò các thực thể trong mạng chuỗi khối

Thứ hai, về mạng chuỗi khối công khai, chúng tôi 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 sẽ 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.

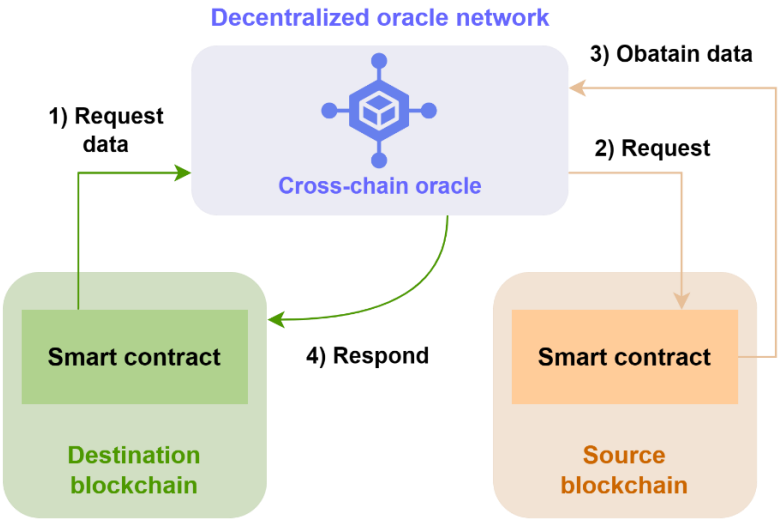


Hình 13. Mạng chuỗi khối Ethereum

3.3.2. Chuỗi khối ngoài

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.

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 chúng em 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 một Oracle được mô tả trong hình dưới.

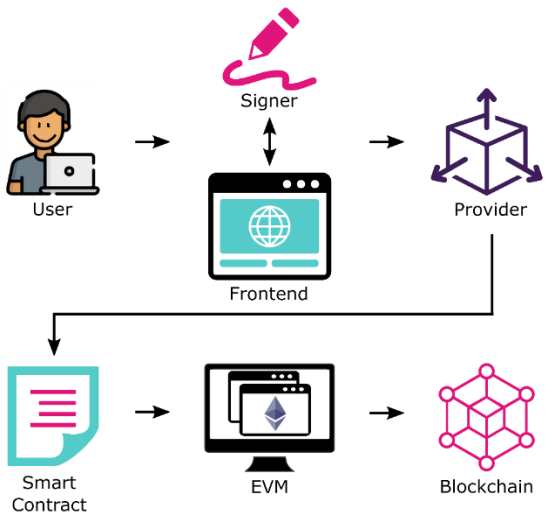


Hình 14. Tương tác giữa hai chuỗi khối sử dụng nút Oracle

Mỗi Oracle chịu trách nhiệm cho một yêu cầu về dữ liệu từ người dùng thông qua DApp và truyền dữ liệu giữa hai chuỗi khối. Bằng cách tương tác với chuỗi khối nguồn thông qua hợp đồng thông minh, nó có thể thu thập dữ liệu theo yêu cầu, có thể là hàm băm mới được tạo sau hàm băm EMR hoặc bằng chứng cho dữ liệu gồm hàm băm đã lưu và EMR ID. Nếu dữ liệu là hàm băm mới đó, nó sẽ được vận chuyển từ chuỗi khối riêng Quorum đến và lưu trữ trên Ethereum. Một hợp đồng thông minh Quorum cũng cần thiết để thực hiện hoạt động này. Quá trình truy vấn hàm băm đã lưu để kiểm tra tính toàn vẹn sẽ được giải thích chi tiết trong phần sau.

3.3.3. 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, nằm dưới sự kiểm soát của một thực thể hoặc tổ chức duy nhất. DApps có thể được sử dụng cho nhiều mục đích khác nhau, bao gồm tài chính, trò chơi, mạng xã hội, v.v. DApps đóng vai trò trung gian giữa người dùng và chuỗi khối riêng trong giải pháp đề xuất của nhóm chúng em. 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.



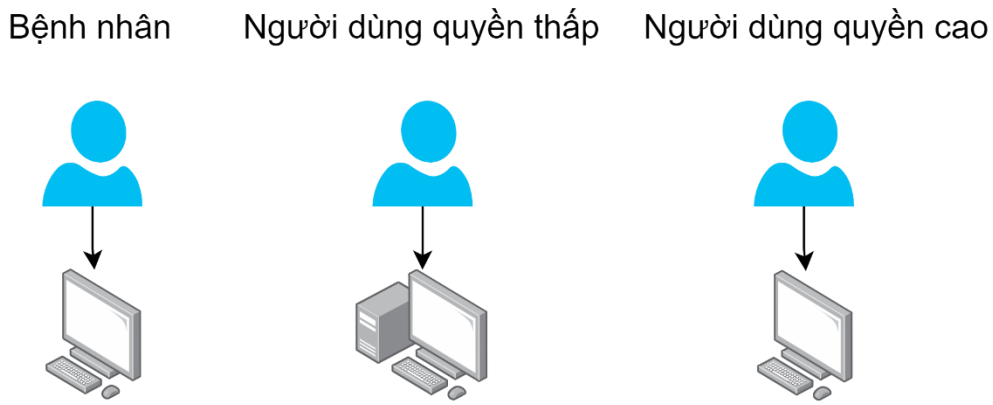
Hình 15. Ứng dụng phi tập trung cơ bản

DApp của chúng tôi 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



Hình 16. Các phiên bản DApp dành cho các thực thể

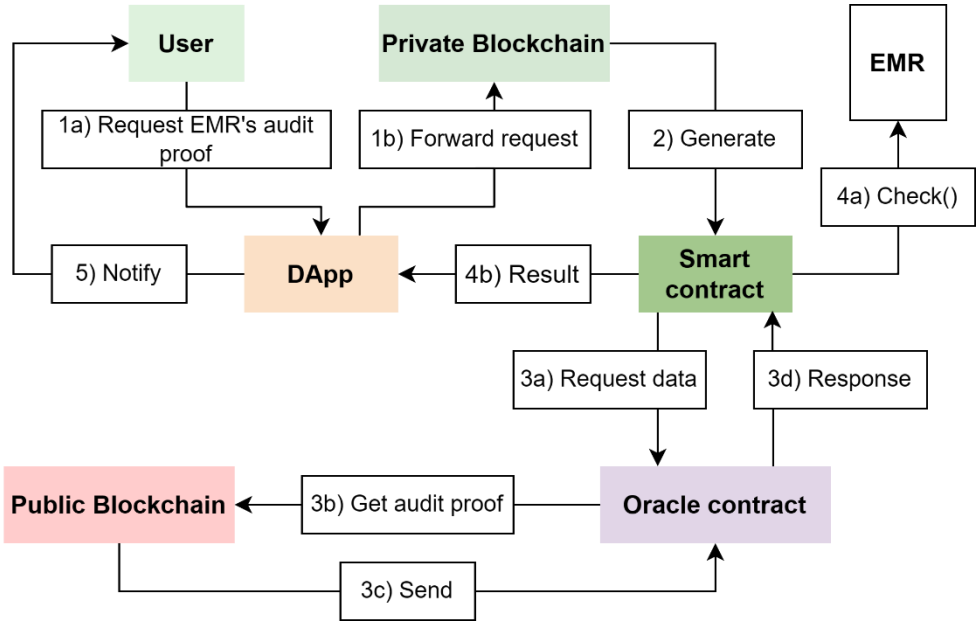
Mỗi vai trò người dùng sẽ có một phiên bản thích hợp riêng với những quyền sử dụng riêng trong DApp, vì vậy người dùng với các vai trò khác nhau sẽ được yêu cầu cung cấp các thông tin đăng nhập khác nhau phù hợp với phiên bản mà mình sử dụng.

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

3.3.4. Hệ thống liên chuỗi khối sử dụng Sidechain

Trong phần này, chúng ta đi sâu vào làm sáng tỏ quá trình truyền dữ liệu băm được lưu trữ từ chuỗi khối công khai sang chuỗi khối riêng tư. Quy trình 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 sẽ được mô tả một cách sinh động trong hình dưới.



Hình 17. 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 tỉ mỉ 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.

3.4. Hệ thống Quản lí

3.4.1. Hệ thống Quản lí hồ sơ bệnh án

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.

Hình 18. Phương án lưu trữ sử dụng Cloud kết hợp với Blockchain

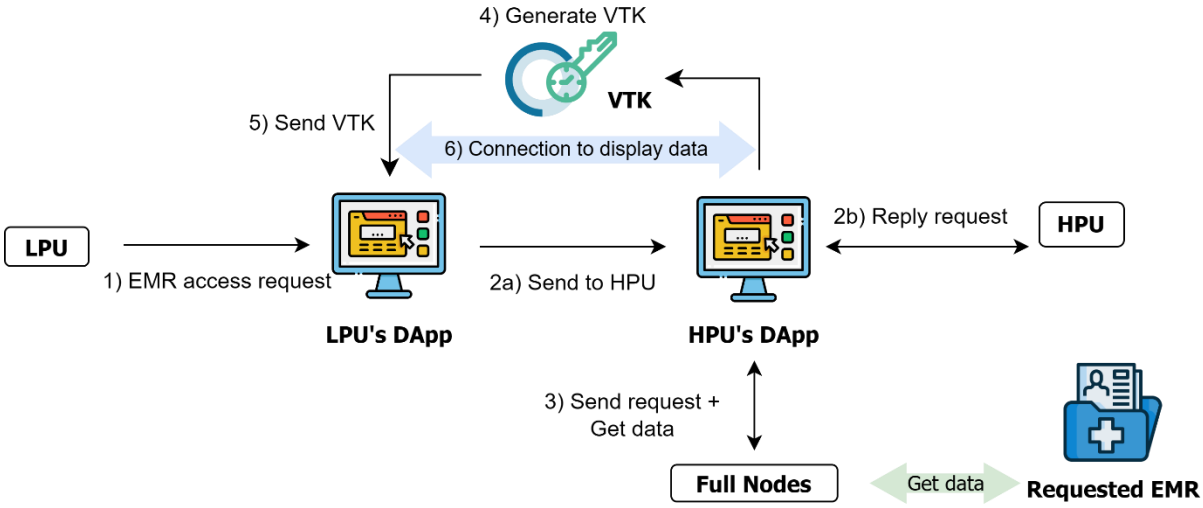
Trong ngữ cảnh đưa ra, nhóm chúng em sử dụng lưu trữ Cloud để lưu các dữ liệu lớn như EMR. Mỗi EMR được mã hóa bằng thuật toán mã hóa đối xứng trước khi đưa vào và khóa bí mật sẽ do các fullnodes nắm giữ.

3.4.2. Hệ thống Quản lí truy cập sử dụng 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 nhóm chúng em 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 và thuật toán 1 cung cấp mô tả ngắn gọn về giao dịch kiểm soát quyền truy cập EMR bằng khóa có thời hạn.



Hình 19. 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 như hình 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: KẾT QUẢ - THẢO LUẬN

4.1. Môi trường

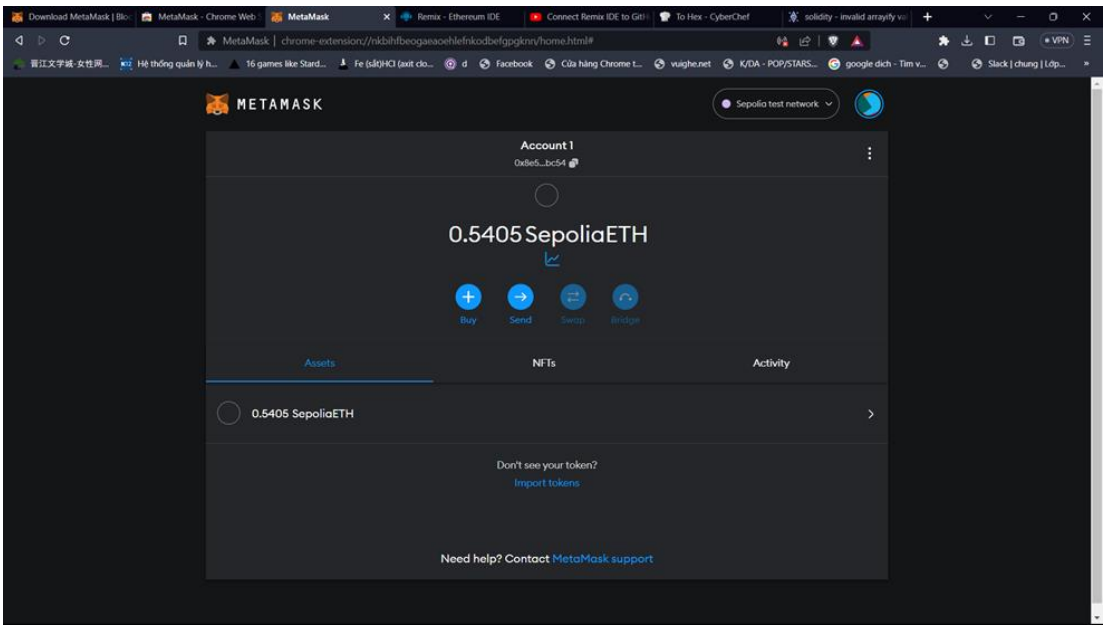
Để kiểm tra tính khả thi và đánh giá hiệu suất của giải pháp chuỗi chéo dựa trên chuỗi khối ngoài, chúng tôi tiến hành một loạt thử nghiệm. Môi trường thực nghiệm được mô tả theo bảng sau:

Máy ảo	CPU	RAM	Hard dive	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

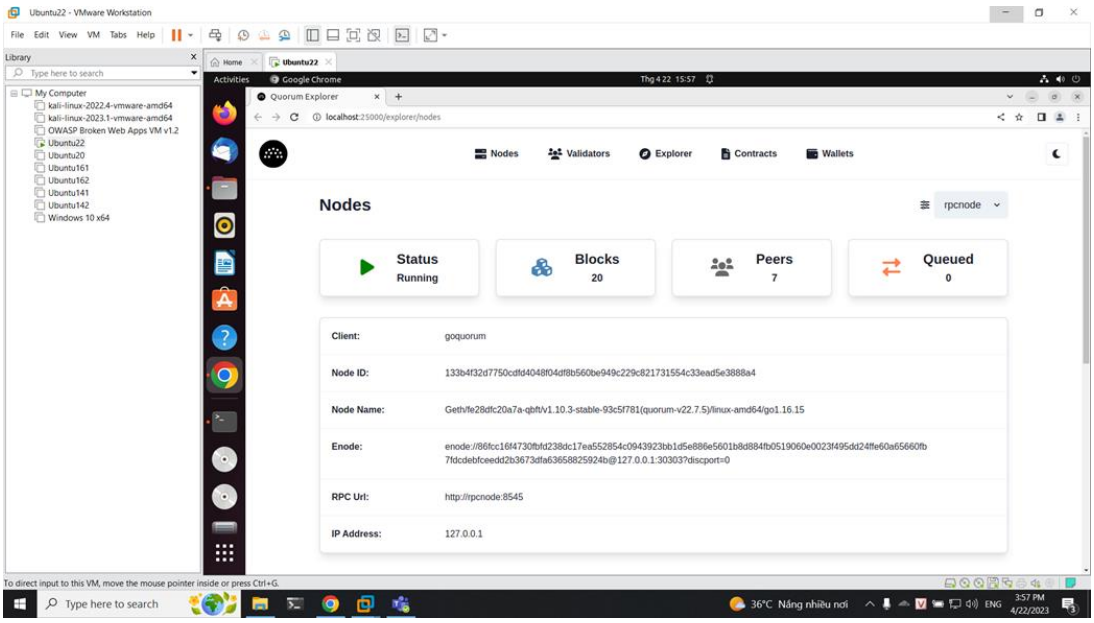
Bảng 1. Môi trường thực nghiệm

Để đánh giá chức năng của hệ thống, nhóm chúng em đã thực hiện dựng mô hình đã đề xuất bao gồm các mạng blockchain, hệ thống Sidechain và thực hiện một loạt 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.

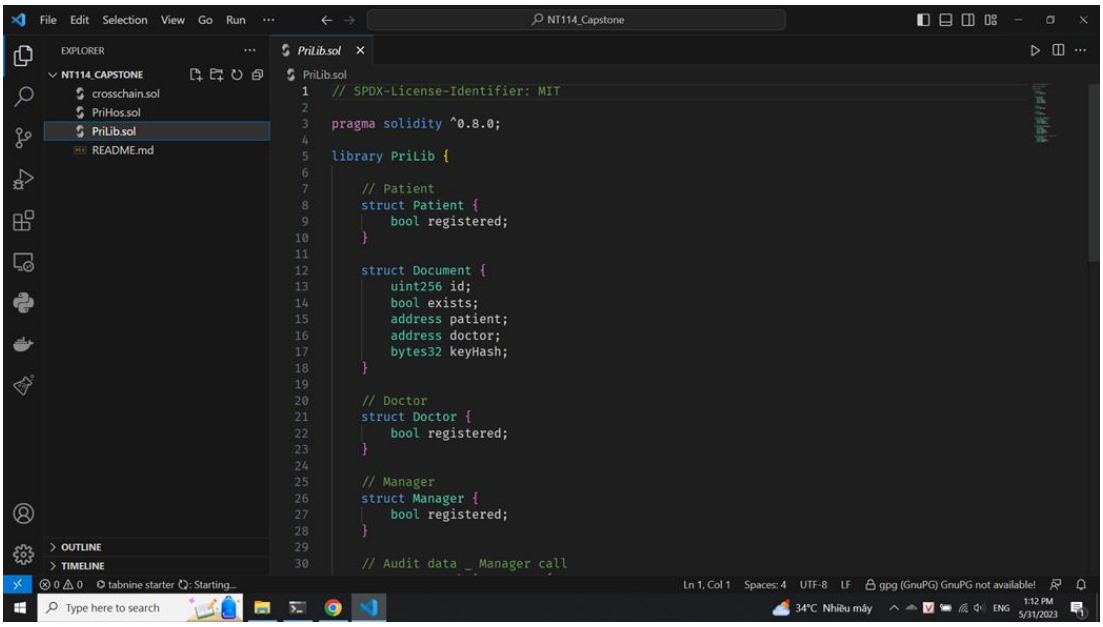
Các hình ảnh thực nghiệm khi thực hiện dựng mô hình và thực hiện các thao tác:



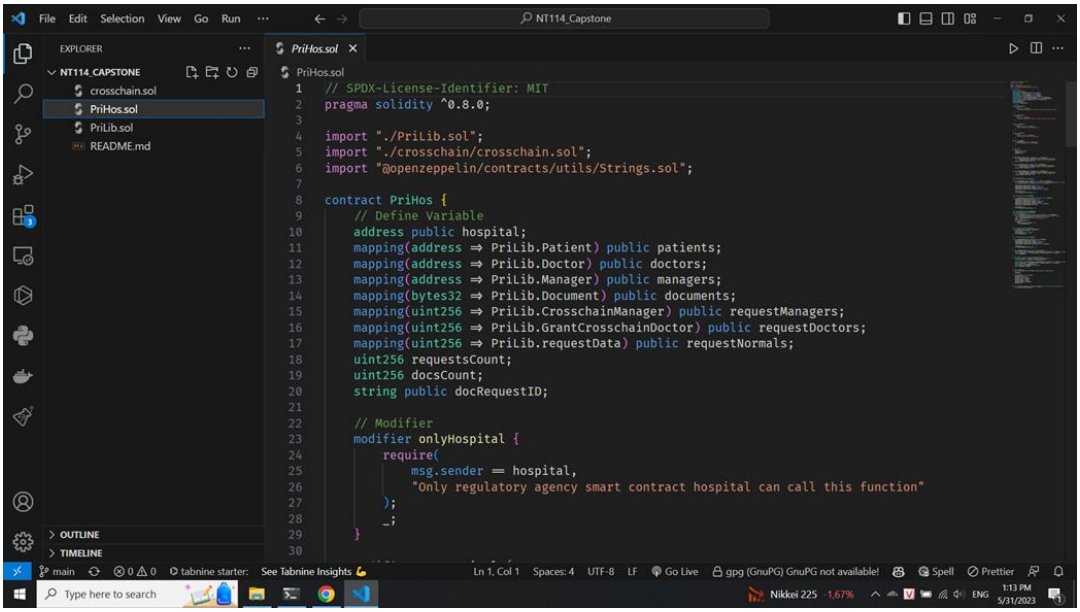
Hình 20. Mạng Sepolia Ethereum



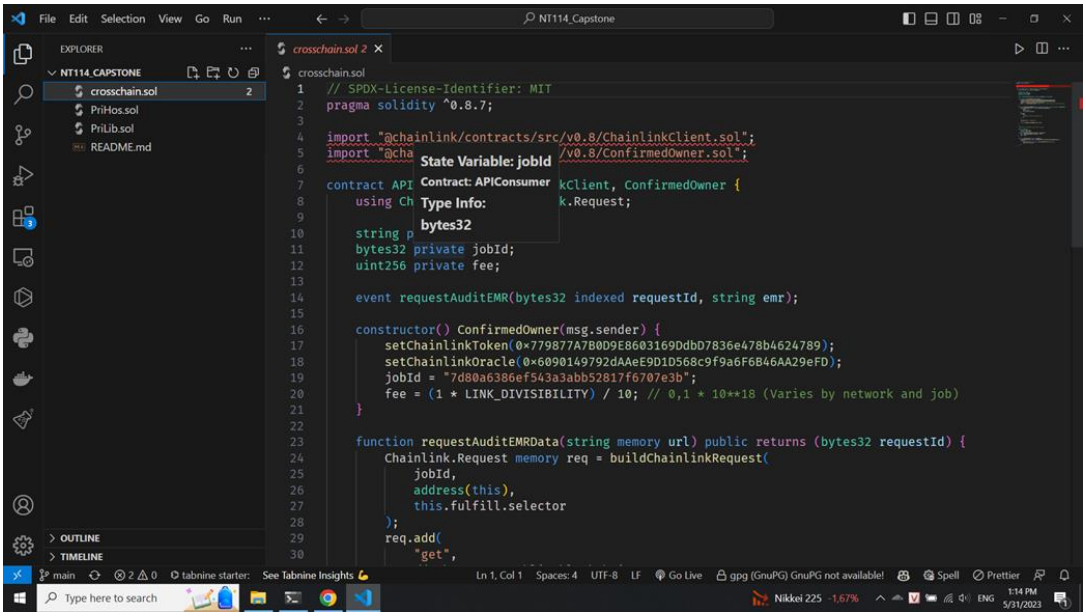
Hình 21. Mạng Quorum



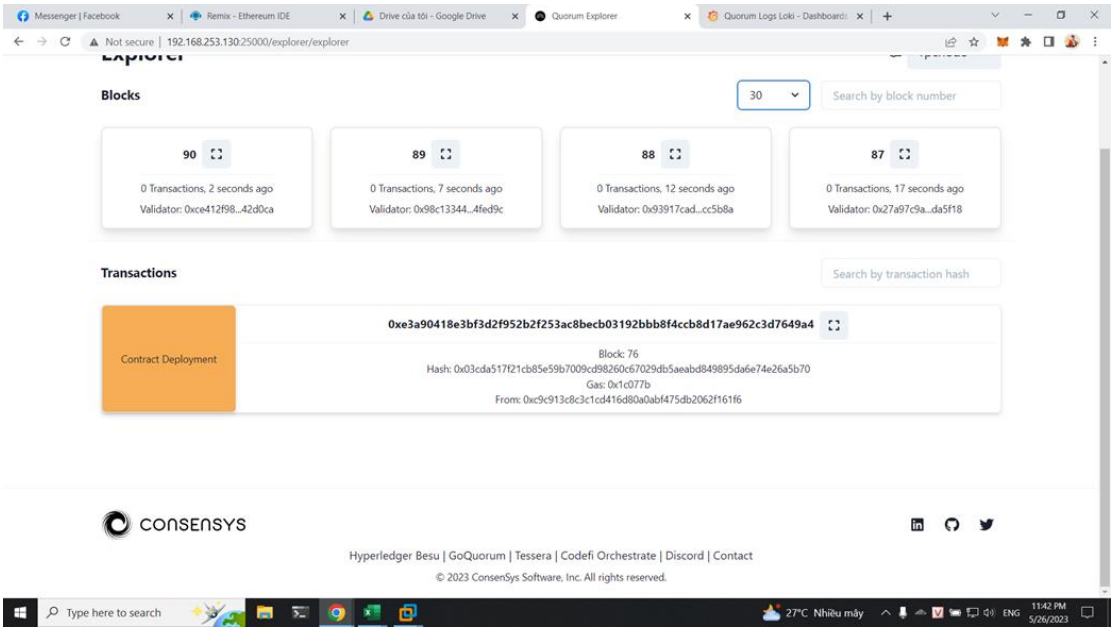
Hình 22. Smart contract 1



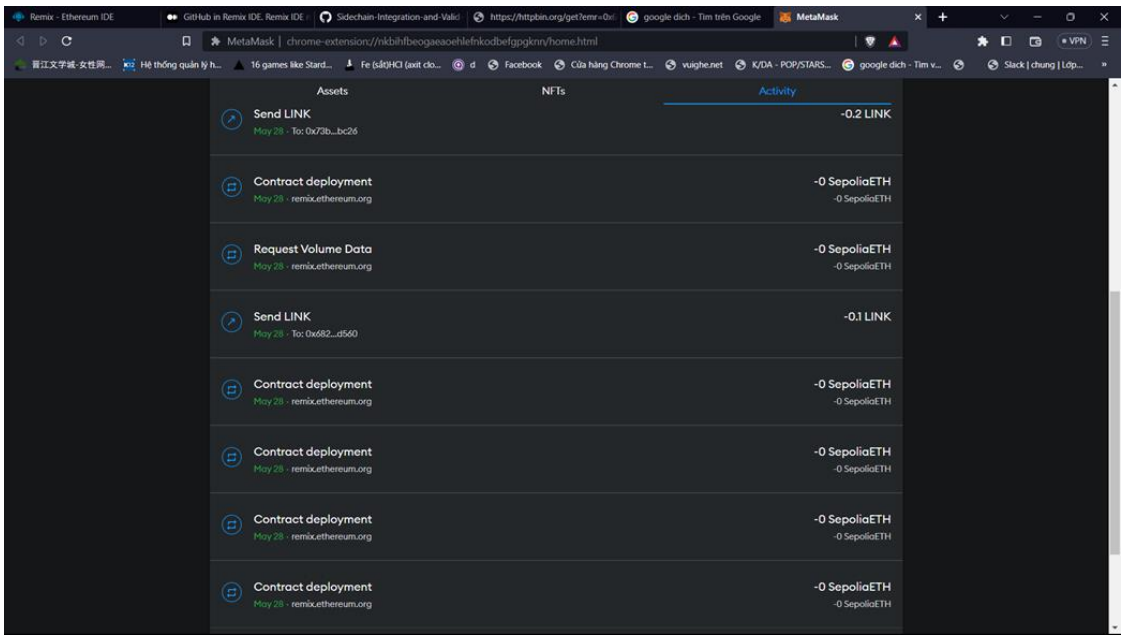
Hình 23. Smart contract 2



Hình 24. Smart contract 3



Hình 25. Deploy smart contract

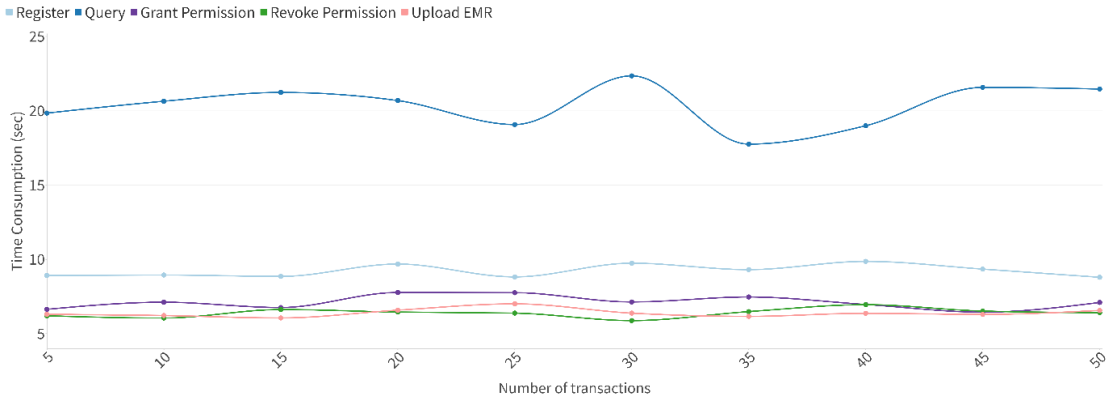


Hình 26. Thông tin các transaction

4.2. Kết quả

Để đánh giá hiệu suất, chúng tôi theo dõi tỉ mỉ thời lượng của các giao dịch này, như được minh họa trong hình 26 và tiến hành nhiều phép đo cho từng giao dịch để đảm bảo độ chính xác và độ tin cậy cao nhất. Thông qua phân tích tỉ mỉ các kết quả thử nghiệm, chúng tôi đã tiến hành đánh giá toàn diện về hiệu suất giao dịch liên quan đến việc lưu trữ và kiểm soát truy cập dữ liệu của EMR, cho phép chúng tôi có được những hiểu biết

có giá trị về hiệu suất và hiệu quả của các quy trình này. Khi nói đến 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 nói trên. Tuy nhiên, kết quả tổng thể thể hiện một triển vọng đặc biệt tích cực, củng cố khái niệm về một kết quả rất thuận lợi. Trong bối cảnh giao dịch truy vấn liên quan đến tương tác giữa các chuỗi, phép đo ghi lại toàn bộ dòng thời gian, 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. Đánh giá kỹ lưỡng của chúng tôi xác nhận rằng giải pháp đề xuất của chúng tôi đã mang lại kết quả tích cực và có tiềm năng đầy hứa hẹn cho những tiến bộ trong tương lai.



Hình 27. Kết quả thực nghiệm về mặt thời gian

Ngoài ra, chúng tôi đánh giá về 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, được đo bằng đơn vị gas. 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. Chúng tôi 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 chuyên sâu về mức sử dụng CPU liên quan đến từng giao dịch. Khi phân tích các quy trình khác nhau, rõ ràng là giao dịch truy vấn nổi bật là yêu cầu khắt khe nhất về mức sử dụng CPU cao nhất, chiếm 76,31%. Do những hạn

chế vốn có của chức năng máy ảo của chúng tôi, điều đáng chú ý là phần trăm sử dụng CPU kết quả có thể xuất hiện tương đối đáng kể. Tuy nhiên, giá trị này vẫn nằm trong giới hạn chấp nhận được, với 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. Thảo luận

Nói tóm lại, chúng tôi 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 nodes Oracle trong một chuỗi khối ngoài. Ngoài ra, chúng tôi còn thực hiện quản lí truy cập bằng cách ứng dụng khóa có thời hạn trong quá trình yêu cầu trao đổi hoặc chia sẻ dữ liệu để đảm bảo được tính riêng tư, bảo mật của các dữ liệu quan trọng. Và các thử nghiệm của chúng tôi cũng đã cho thấy tính khả thi của hệ thống trong ngữ cảnh giữa hai bệnh viện mà chúng tôi đã đưa ra.

Tuy nhiên, để đạt tới hiệu suất tối ưu và bảo mật cho các mạng chuỗi khối, chúng tôi phải chuỗi khối ngoài tương ứng với một mạng Oracle phi tập trung, nhưng cũng chính vì vậy đã dẫn đến một số hạn chế cần phải xem xét như: Khó mở rộng mạng chuỗi khối ngoài, vấn đề về bảo mật trong quá trình trao đổi liên chuỗi ở các điểm đầu cuối từ các ứng dụng phi tập trung.

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 các ứng dụng phi tập trung của các hệ thống chuỗi khối vẫn là một vấn đề cần đảm bảo tốt hơn cho các dữ liệu được trao đổi giữa hai chuỗi khối.

CHƯƠNG 5: KẾT LUẬN VÀ ĐỀ NGHỊ

5.1. Kết luận

Trong bài báo này, chúng tôi 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, chúng tôi 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.

Trong công việc trong tương lai, chúng tôi 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, chúng tôi 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.

5.2. Ý nghĩa khoa học

Công trình được triển khai góp phần đưa ra một hướng tiếp cận mới mẻ và có nhiều ưu điểm về mặt bảo mật để, góp phần giải quyết bài toán chung về trao đổi dữ liệu giữ hai chuỗi khối khác kiến trúc. Ngoài ra, chúng tôi đã trình bày một khái niệm sáng tạo được gọi là khóa có thời hạn để ứng dụng trong quản lý truy cập dữ liệu an toàn và thuận tiện. Nhờ đó phần nào đưa ra một giải pháp tham khảo cho vấn đề đảm bảo các yêu cầu về bảo mật thông tin được trao đổi liên chuỗi.

5.3. Hiệu quả về kinh tế - xã hội

Mỗi doanh nghiệp thường sẽ có những yêu cầu riêng về hệ thống chuỗi khối, dẫn đến sự bất đồng nhất và khó khăn trong việc trao đổi dữ liệu giữa các doanh nghiệp sử dụng chuỗi khối với nhau. Việc này có thể gây bất lợi cho doanh nghiệp trong quá trình phát triển và mở rộng, dẫn đến các thiệt hại kinh tế không đáng có. Mặt khác, khi một chuỗi khối có quá nhiều khối, hiệu năng chuỗi khối sẽ giảm nhưng chi phí phần cứng bỏ ra cho lại ngày một tăng lên, vì vậy ý tưởng mở rộng chuỗi khối bằng các chuỗi khối ngoài thường được áp dụng làm tăng nhu cầu trao đổi dữ liệu giữ hai chuỗi khối với nhau. Và công trình của chúng tôi đã phần nào đóng góp một giải pháp với chi phí xây dựng và sử dụng thấp, hiệu năng cao và có thể đáp ứng được nhu cầu phát triển của doanh nghiệp sử dụng hệ thống. Đồng thời, hệ thống còn cung cấp khả năng quản lí truy cập dữ liệu, tăng tính bảo mật và riêng tư cho dữ liệu trao đổi giữa hai chuỗi khối.

5.4. Phạm vi áp dụng

Hiện nay, với việc chuỗi khối đang không ngừng được nghiên cứu và phát triển, đồng thời đã được ứng dụng rộng rãi trong nhiều ngành như pháp chứng kỹ thuật số, tài chính, bảo hiểm, chăm sóc sức khỏe, hỗ trợ xã hội và giáo dục. Giải pháp của chúng tôi hoàn toàn có thể được sử dụng trong các ngữ cảnh triển khai này với nhiều kiến trúc chuỗi khối khác nhau.

5.5. Hướng phát triển

Trong công việc trong tương lai, chúng tôi 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 cũng 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 chúng em 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.

CHƯƠNG 6: TÀI LIỆU PHỤ LỤC

6.1. Danh mục hình ảnh

6.2. Danh mục bảng

6.3. Danh mục thuật toán

6.4. Danh mục viết tắt và giải nghĩa

EMR – Electrical medical records	Hồ sơ bệnh án điện tử
Blockchain	Chuỗi khối
Public Blockchain	Chuỗi khối ngoài
Private Blockchain	Chuỗi khối riêng
Sidechain	Hệ thống chuỗi khối ngoài
VTK – Valid time key	Khoá có thời hạn
Off-chain	Ngoài chuỗi khối
On-chain	Trên chuỗi khối
DON – Decentralized oracle networks	Các mạng phi tập trung
Full Node	Nút đầy đủ
Light Node	Nút nhẹ

6.5. 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. Y. Pang, “A new consensus protocol for blockchain interoperability architecture,” IEEE Access, vol. 8, pp. 153 719–153 730, 2020.
3. 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.
4. T. Hardjono, A. Lipton, and A. Pentland, “Toward an interoperability architecture for blockchain autonomous systems,” IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1298–1309, 2019.12 T.D. Tran et al.
5. 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.
6. 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.

7. 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.
8. 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.
9. 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.
10. 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.
11. V. Buterin, “R3 report-chain interoperability,” R3 Res, 2016.
12. 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.
13. 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.
14. 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. J. Kwon and E. Buchman, “Cosmos whitepaper,” A Netw. Distrib. Ledgers, p. 27, 2019.
16. G. Wood, “Polkadot: Vision for a heterogeneous multi-chain framework,” White paper, vol. 21, no. 2327, p. 4662, 2016.
17. 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.
18. Chainlink Documents: https://docs.chain.link/
19. Foley & Lardner LLP

20. TradaFX
21. ResearchGate
22. arshbot.medium.com
23. Hyperchain Documentations: https://www.hyperchain.cn/
24. Cosmos Documentations: https://docs.cosmos.network/main
25. Polkadot Documentations: https://polkadot.network/development/docs/
26. Stakin: https://stakin.com/
27. Chainstack: https://chainstack.com/
28. Shiksha: https://www.shiksha.com/
29. Moonbeam Documentationons: https://docs.moonbeam.network/
30. Horizen Academy: https://www.horizen.io/academy/sidechains/