ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO THỰC TẬP DOANH NGHIỆP

NGHIÊN CỨU VỀ CÔNG NGHỆ BLOCKCHAIN VÀ MÔ HÌNH CROSSCHAIN

Công ty: Phòng thí nghiệm An Toàn Thông Tin ĐHCNTT – ĐHQGHCM

Người hướng dẫn tại công ty:	**Nghi Hoàng Khoa**
Giáo viên hướng dẫn:	**Th.S Trần Tuấn Dũng**
Sinh viên thực hiện:	**Võ Anh Kiệt**
	Nguyễn Bùi Kim Ngân
	Nguyễn Bình Thục Trâm
Mã số sinh viên:	**20520605**
	20520648
	20520815
Lớp:	**ATTN.2020**

Thành phố Hồ Chí Minh, tháng 12 năm 2022

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO THỰC TẬP DOANH NGHIỆP

NGHIÊN CỨU VỀ CÔNG NGHỆ BLOCKCHAIN VÀ MÔ HÌNH CROSSCHAIN

Công ty: Phòng thí nghiệm An Toàn Thông Tin ĐHCNTT – ĐHQGHCM

Người hướng dẫn tại công ty:	**Nghi Hoàng Khoa**
Giáo viên hướng dẫn:	**Th.S Trần Tuấn Dũng**
Sinh viên thực hiện:	**Võ Anh Kiệt**
	Nguyễn Bùi Kim Ngân
	Nguyễn Bình Thục Trâm
Mã số sinh viên:	**20520605**
	20520648
	20520815
Lớp:	**ATTN.2020**

Thành phố Hồ Chí Minh, tháng 12 năm 2022

LỜI CẢM ƠN

Trân trọng gửi lời cảm ơn đến Phòng thí nghiệm An Toàn Thông Tin ĐHCNTT – ĐHQGHCM và thầy cô ở phòng E8.1đã tạo điều kiện cho nhóm chúng em có một mùa thực tập thành công.

Hơn thế nữa, nhóm chúng em xin trân thành cảm ơn đến quý thầy cô trường Đại Học Công Nghệ Thông Tin, đặc biệt là quý thầy cô khoa Mạng Máy Tính và Truyền Thông, trong đó chúng em xin gửi lời cảm ơn sâu sắc đến thầy Trần Tuấn Dũng – người hướng dẫn hết sức tận tâm, nhiệt tình và luôn động viên, tạo mọi điều kiện tốt nhất cho chúng em khi thực tập tại Phòng thí nghiệm An Toàn Thông Tin ĐHCNTT – ĐHQGHCM. Những ý kiến đóng góp, hướng dẫn của thầy luôn là nguồn cảm hứng và định hướng cho chúng em ngày càng hoàn thiện, phát triển ứng dụng ngày một tốt hơn và ngày càng hoàn thiện bản thân hơn trong giai đoạn hội nhập và phát triển của đất nước.

Trong quá trình thục hiện nhiệm vụ thực tập, cũng như là trong quá trình làm bài báo cáo thực tập, do kiến thức của chúng em còn hạn chế nên khó có thể tránh khỏi những sai sót không mong muốn, chúng em rất mong quý thầy cô chỉ bảo, đóng góp ý kiến để chúng em ngày càng hoàn thiện hơn về mặt kiến thức. Đồng thời do trình độ lý luận cũng như kinh nghiệm thực tiễn còn hạn chế nên bài báo cáo không thể tránh khỏi những thiếu sót, chúng em rất mong nhận được ý kiến đóng góp của quý thầy cô, để em học thêm được nhiều kinh nghiệm giúp chúng em trong quá trình tương lai sắp tới.

Cuối cùng, chúng em xin chúc Phòng thí nghiệm An Toàn Thông Tin ngày càng phát triển, đạt được nhiều thành công trong tương lai để có thể tiếp tục dẫn dắt thế hệ trẻ trên con đường An Toàn Thông Tin. Chúng em xin chúc quý thầy cô của trường Đại Học Công Nghệ Thông Tin, đặc biệt là quý thầy cô khoa Mạng Máy Tính và Truyền Thông, và đặc biệt hơn hết đó là thầy Dũng có được nhiều sức khỏe để có thể dốc lòng trong sự nghiệp "trồng người".

Thành phố Hồ Chí Minh, tháng 12 năm 2022

Võ Anh Kiệt – 20520605 – ATTN.2020

Nguyễn Bùi Kim Ngân – 20520648 – ATTN.2020

Nguyễn Bình Thục Trâm – 20520815 – ATTN.2020

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

MỤC LỤC

DANH MỤC HÌNH ẢNH

PHẦN MỞ ĐẦU

Quá trình thực tập tại Phòng thí nghiệm An toàn thông tin ĐHCNTT – ĐHQGHCM cung cấp cho sinh viên cũng như thực tập sinh kỹ năng nghiên cứu và thực nghiệm giúp cho việc nắm vững về một vấn đề cụ thể trở nên gần gũi và trực quan hơn từ đó có thể mở rộng vấn đề cũng như phát hiện được những hạn chế, những vấn đề để có thể cải thiện vấn đề đó. Từ đó thấy được công việc đòi hỏi không chỉ về kiến thức, hiểu biết, kinh nghiệm của bản thân mà còn là về việc rèn luyện tiếp thu và xây dựng mô hình, giải pháp được đề xuất trong bài báo khoa học, qua đó chuẩn bị cho việc thực hiện Đồ Án Chuyên Ngành và Khóa Luận Tốt Nghiệp trong thời gian sắp tới.

Không chỉ các lợi ích trên, việc thực hiện nghiên cứu, thực tập tại Phòng thí nghiệm An toàn thông tin ĐHCNTT – ĐHQGHCM giúp chúng em hiểu hơn về những kiến thực liên quan đến Blockchain và mô hình CrossChain trong BlockChain, ngôn ngữ lập trình Rust và Solidity hỗ trợ tốt cho Blockchain, ngôn ngữ lập trình Python và framework Django,… Thông qua đó, có thể hiểu được mục đích của bài báo AppXChain mà nhóm đang nghiên cứu và cải tiến mô hình đề xuất trong bài báo.

Nội dung đề tài gồm 3 phần sau:

Phần mở đầu

Phần nội dung

- Chương 1: Giới thiệu về công ty
- Chương 2: Giới thiệu chương trình thực tập
- Chương 3: Nội dung thực tập

Phần kết luận

PHẦN NỘI DUNG

Chương 1: Giới thiệu về công ty

1.1. Giới thiệu chung

Hình 1 - Logo Phòng thí nghiệm An Toàn Thông Tin

Phòng thí nghiệm An Toàn Thông Tin (InSec Lab) thuộc Trường Đại học Công nghệ Thông tin – ĐHQG TP.HCM được thành lập theo quyết định số 19/QĐ-ĐHCNTT-TCHC ngày 19/01/2016, hướng đến việc xây dựng một phòng thí nghiệm chuyên sâu về an toàn thông tin, có chức năng nghiên cứu khoa học trong lĩnh vực an toàn thông tin, giải quyết các nhu cầu đặt ra bởi thực tiễn cũng như các giải pháp cho tương lai, tham gia đào tạo đại học, sau đại học, hợp tác quốc tế, chuyển giao công nghệ trong lĩnh vực an toàn thông tin.

Phòng Thí nghiệm An toàn thông tin (UIT InSec Lab) là một môi trường nghiên cứu, thực nghiệm chuyên dụng dành cho các nghiên cứu về an toàn thông tin, hỗ trợ sinh viên, nghiên cứu viên tham gia vào các hoạt động liên quan đến an toàn thông tin trên các hệ thống mạng với các tài nguyên máy tính, môi trường thực nghiệm, cũng như các dịch vụ ứng dụng được kiểm soát, mà không ảnh hưởng đến các môi trường mạng khác.

Cơ sở hạ tầng phục vụ nghiên cứu của Phòng Thí nghiệm bao gồm hệ thống server mạnh mẽ với nhiều cơ chế phân phối, xử lý dữ liệu đa dạng và các dịch vụ về an toàn thông tin.

UIT InSec Lab hướng đến việc cung cấp một nền tảng hỗ trợ và thúc đẩy sự hợp tác giữa các nghiên cứu viên trong môi trường học thuật, chính phủ điện tử và doanh nghiệp. Hệ thống phần mềm quản lý cơ sở hạ tầng của Phòng Thí nghiệm An toàn thông tin được đặt lại Phòng E8.1 (tòa nhà E) và Data Center (tòa nhà A) - UIT.

1.2. Lĩnh vực hoạt động

1.2.1. Nghiên cứu khoa học liên quan đến An Toàn Thông Tin

Triển khai các đề án nghiên cứu khoa học và công nghệ có tính cấp thiết, tính đi trước trên cơ sở bám sát định hướng phát triển, mục tiêu kinh tế, xã hội Quốc gia và tiến bộ khoa học hiện đại trên thế giới.

Tập hợp và phát triển đội ngũ cán bộ khoa học công nghệ có trình độ cao, ưu tiên các nghiên cứu, hợp tác quốc tế, tạo điều kiện thuận lợi triển khai các nghiên cứu theo định hướng về An toàn thông tin.

1.2.2. Tư vấn, nghiên cứu giải pháp và chuyển giao công nghệ

Thực hiện tư vấn, nghiên cứu giải pháp và chuyển giao công nghệ nhằm giải quyết vấn đề kĩ thuật, công nghệ cụ thể có liên quan đến an toàn thông tin do địa phương, doanh nghiệp đặt hàng.

1.3. Những hướng nghiên cứu chính

Phòng thí nghiệm An toàn thông tin tập trung vào các chủ đề nghiên cứu chính như sau:

- SPS: Software-defined programmable security (SDN, NFV, Cloud, Edge)
- Lập trình an toàn: Giải pháp kiểm thử xâm nhập, bảo mật thông tin và tính riêng tư cho người dùng trong các ứng dụng (end-to-end encryption, pentesting, software vulnerablity...)
- Điều tra bằng chứng số, tội phạm số (digital forensics)
- AI security and AI-based security: An toàn thông tin, tính riêng tư dữ liệu cho các mô hình AI & Ứng dụng trí tuệ nhân tạo (deep learning, Generative Adversarial Networks) cho bài toán an ninh trên không gian mạng
- Internet malware/botnet/APT detection, defense, and analysis
- Phát hiện – ngăn chặn xâm nhập/ tấn công trong các hệ thống

- Mã độc (phần mềm độc hại): trên nền tảng Android, iOs, Windows, Linux, Web...
- Intrusion detection, anomaly detection
- Blockchain (các công nghệ nền tảng, giao thức và các ứng dụng thực tế)
- Mobile and IoT security

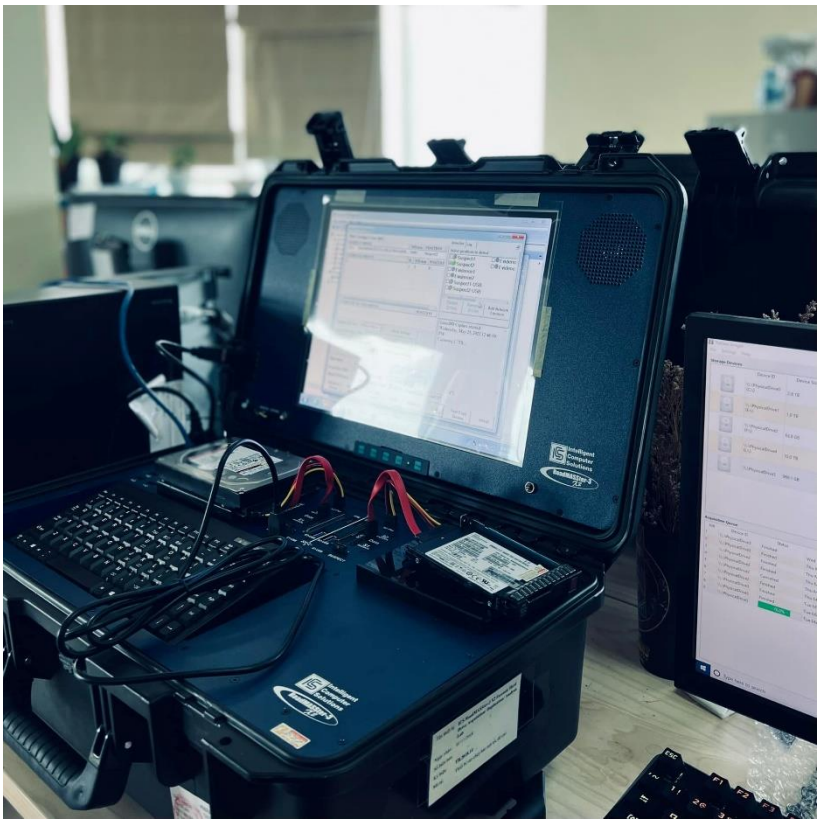
1.4. Môi trường làm việc

Môi trường làm việc đày tính sáng tạo, học thuật, là môi trường tốt để các bạn thực tập sinh cũng như là sinh viên có thể phát triển tốt trong lĩnh vực An Toàn Thông Tin.

Hình 2 - Môi trường làm việc

Hình 3 - Môi trường làm việc

Trang thiết bị hiện đại, phục vụ tốt cho việc nghiên cứu trong An Toàn Thông Tin.



Hình 4 - Trang thiết bị

Hình 5 - Trang thiết bị

Chương 2: Giới thiệu chương trình thực tập

2.1. Tổng quan chương trình thực tập

Tìm hiểu, nghiên cứu hệ thống Blockchain và mô hình CrossChain được ứng dụng trong Blockchain.

Ứng dụng mô hình CrossChain cho việc quản lý hồ sơ bệnh án của bệnh nhân thông qua AppXChain.

Cải tiến phương thức kiểm soát truy cập AppXChain thông qua webapp.

2.2. Các sản phẩm và dịch vụ

Khi thực hiện công việc nghiên cứu thì cần phải có những yêu cầu sau:

- Kiến thức cơ bản về Blockchain và mô hình CrossChain
- Hiểu biết, có thể sử dụng ngôn ngữ lập trình Rust và Solidity
- Hiểu biết về ngôn ngữ lập trình Python và các sử dụng những thư viện liên quan đến web3 trong Python
- Hiểu biết framework Django – một framework dựa trên ngôn ngữ Python dùng trong việc xây dựng web
- Tinh thần trách nhiệm cao, thái độ tốt trong công việc
- Tính đoàn kết, kỷ luật trong quá trình làm việc

2.3. Thời gian thực tập

Thời gian thực tập kéo dài từ ngày 05/09/2022 đến ngày 05/11/2022.

Hình thức làm việc áp dụng mô hình kết hợp giữa online và offline.

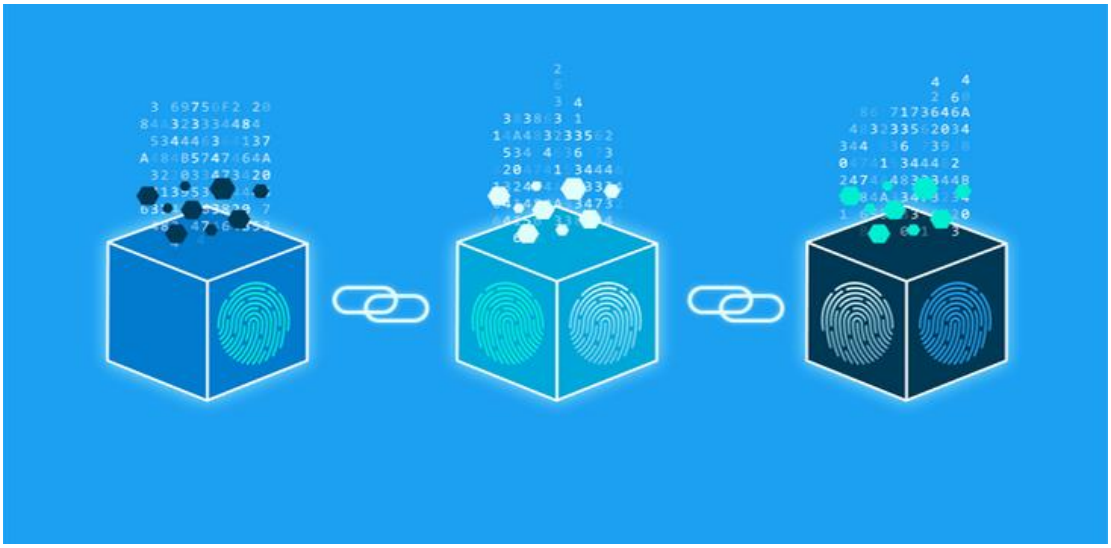
Yêu cầu thực hiện việc offline tại văn phòng 4 buổi/tuần.

Thời gian làm việc từ 8h00 đến 11h30 (sáng) và 1h đến 5h (chiều).

Chương 3: Nội dung thực tập

3.1. Các kiến thức nền tảng

3.1.1. Blockchain



Hình 6 - Blockchain

Blockchain (chuỗi khối), tên ban đầu block chain là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối thông tin được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối thông tin đều chứa thông tin về thời gian khởi tạo và được liên kết tới khối trước đó, kèm một mã thời gian và dữ liệu giao dịch. Blockchain được thiết kế để chống lại sự thay đổi của dữ liệu: Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được nó.

3.1.2. Rust

Hình 7 - Rust

Rust là một ngôn ngữ lập trình đa mô hình, có mục đích chung. Rust nhấn mạnh vào hiệu suất, an toàn kiểu và đồng thời. Rust thực thi an toàn bộ nhớ – nghĩa là tất cả các tham chiếu đều trỏ đến bộ nhớ hợp lệ – mà không yêu cầu sử dụng bộ thu gom rác hoặc đếm tham chiếu có trong các ngôn ngữ an toàn cho bộ nhớ khác.

3.1.3. Solidity

Hình 8 - Solidity

Solidity là một ngôn ngữ lập trình hướng đối tượng để thực hiện các hợp đồng thông minh trên các nền tảng blockchain khác nhau, đáng chú ý nhất là Ethereum. Nó được phát triển bởi Christian Reitwiessner, Alex Beregszaszi và một số cựu cộng tác viên cốt lõi của Ethereum.

3.1.4. Python

Hình 9 - Python

Python là một ngôn ngữ lập trình bậc cao cho các mục đích lập trình đa năng, do Guido van Rossum tạo ra và lần đầu ra mắt vào năm 1991. Python được thiết kế với ưu điểm mạnh là dễ đọc, dễ học và dễ nhớ. Python là ngôn ngữ có hình thức rất sáng sủa, cấu trúc rõ ràng, thuận tiện cho người mới học lập trình và là ngôn ngữ lập trình dễ học; được dùng rộng rãi trong phát triển trí tuệ nhân tạo. Cấu trúc của Python còn cho phép người sử dụng viết mã lệnh với số lần gõ phím tối thiểu. Vào tháng 7 năm 2018, van Rossum đã từ chức lãnh đạo trong cộng đồng ngôn ngữ Python sau 30 năm làm việc.

Python hoàn toàn tạo kiểu động và dùng cơ chế cấp phát bộ nhớ tự động; do vậy nó tương tự như Perl, Ruby, Scheme, Smalltalk, và Tcl. Python được phát triển trong một dự án mã mở, do tổ chức phi lợi nhuận Python Software Foundation quản lý.

Ban đầu, Python được phát triển để chạy trên nền Unix. Nhưng rồi theo thời gian, Python dần mở rộng sang mọi hệ điều hành từ MS-DOS đến Mac OS, OS/2, Windows, Linux và các hệ điều hành khác thuộc họ Unix. Mặc dù sự phát triển của Python có sự đóng góp của rất nhiều cá nhân, nhưng Guido van Rossum hiện nay vẫn là tác giả chủ yếu của Python. Ông giữ vai trò chủ chốt trong việc quyết định hướng phát triển của Python.

Python luôn được xếp hạng vào những ngôn ngữ lập trình phổ biến nhất.

3.1.5. Django

Hình 10 - Django

Django là một framework web dựa trên Python, mã nguồn mở, miễn phí tuân theo mô hình kiến trúc mô hình MTV. Nó được duy trì bởi Django Software Foundation (DSF), một tổ chức độc lập được thành lập ở Hoa Kỳ với tư cách là một tổ chức phi lợi nhuận.

Mục tiêu chính của Django là để dễ dàng tạo ra các trang web dựa trên cơ sở dữ liệu phức tạp. Framework hỗ trợ tốt tái sử dụng lại và khả năng tương thích của các thành phần, ít source code hơn, khớp nối ít, phát triển nhanh và không lặp lại. Python được sử dụng xuyên suốt, ngay cả đối với cài đặt, tệp và mô hình dữ liệu. Django cũng cung cấp một giao diện tạo, đọc, cập nhật và xóa quản trị tùy chọn được tạo động thông qua introspection và được định cấu hình thông qua các mô hình quản trị.

Một số trang web nổi tiếng sử dụng Django bao gồm Instagram, Mozilla, Disqus, Bitbucket, Nextdoor và Clubhouse.

3.2. Bài báo khoa học

Bài báo chính được chọn và phân tích là:

Madine, M., Salah, K., Jayaraman, R., Al-Hammadi, Y., Arshad, J., & Yaqoob, I. (2021). appxchain: Application-level interoperability for blockchain networks. IEEE Access, 9, 87777-87791.

3.2.1. Vấn đề được đề cập trong bài báo

Công nghệ blockchain ra đời chính là một cuộc cách mạng trong ngành công nghiệp về công nghệ với việc cung cấp những tính năng phi tập trung, transparent, realiable, trustworthy.

Tuy nhiên công nghệ này cũng đặt ra một thách thức đó chính là trong mô hình CrossChain thì việc kiểm soát truy cập luôn là một thách thức lớn khi trong mô hình CrossChain bao gồm một private blockchain và 1 public Blockchain. Việc này sẽ dẫn đến việc khi sử dụng private blockchain và người dùng bị mất private key thì đây chính là một vấn đề lớn về security trong mô hình CrossChain.

Phương pháp giải quyết hiện yêu cầu kết hợp tính tập trung hóa và tái tạo lại Blockchain và mô hình CrossChain để chia sẽ dữ liệu giữa các mạng trong CrossChain.

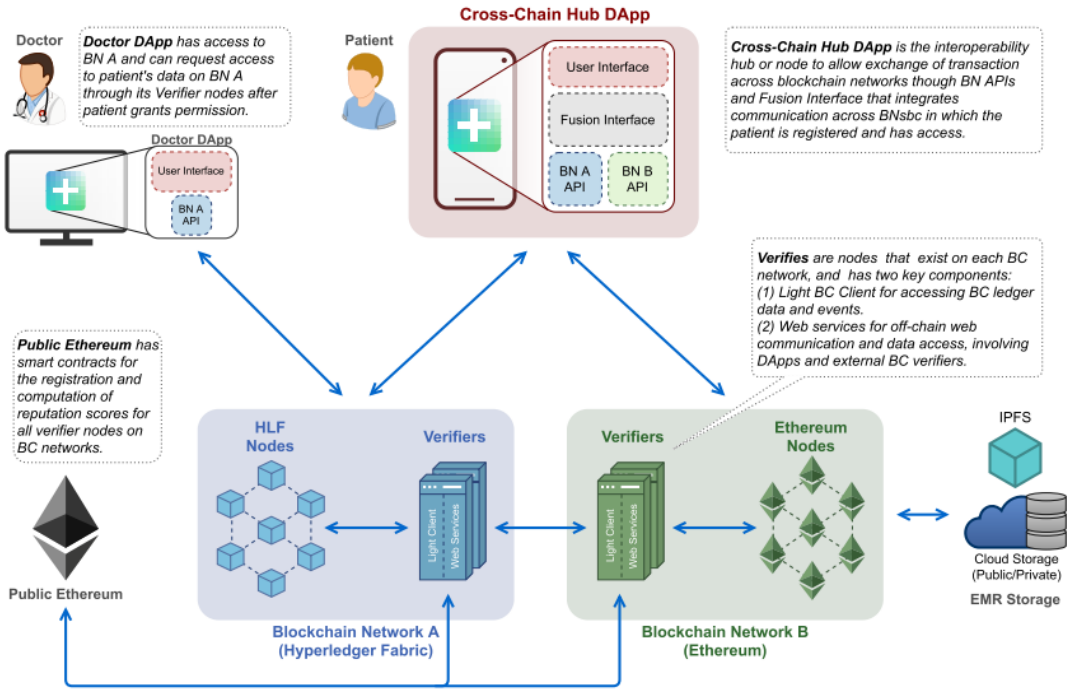
3.2.2. Tổng quan về nội dung

Bài báo đã đặt ra vấn đề trao đổi, giao tiếp, chuyển đổi tập tin dựa trên mô hình CrossChain thông qua ứng dụng AppXChain. Mô hình này cho phép các mạng Blockchain bất kỳ kết nối vào để giao tiếp và chia sẻ dữ liệu:

- Thiết kế ứng dụng trên cơ sở mạng phi tập trung có nhiều mạng Blockchain và giữa các mạng này có thể giao tiếp và trao đổi dữ liệu cùng

cho nhau, từ đó thực hiện các cơ chế ủy quyền và truy vấn được đến các giá trị thông số.

- Sử dụng các node trong mạng để thực hiện việc duy trì tính toàn vẹn của dữ liệu được chia sẻ, trao đổi khi các mạng Blockchain khi giao tiếp.
- Cụ thể hóa các vai trò và yêu cầu của các thực thể chính csở hữu mủa mô hình CrossChain trong bối cảnh giữa các bệnh viện, mỗi bệnh viện sẽ sở hữu 1 mạng Blockchain để giao tiếp.
- Giải thích về việc hồ sơ bệnh án điện tử (EMR) và những yêu cầu, phương thức giao tiếp, tương tác để thực hiện chia sẻ hồ sơ bên án điện tử giữa các mạng Blockchain trong mô hình CrossChain bằng thuật toán mang tính chất bắt buộc.
- Triển khai ứng dụng AppXChain để bệnh nhân có thẻ thực hiện việc chuyển đổi đồng thời kiểm tra chi phí và tính bảo mật của nó.



Hình 11 - Các thành phần trong mô hình ứng dụng AppXChain

3.2.3. Các thành phần được đề cập

Bệnh nhân (Patient): sử dụng CrossChain Hub Dapp cho phép trao đổi các thông tin trên các mạng blockchain thông qua Fusion Interface tích hợp giao tiếp, nơi mà bệnh nhân đăng ký và truy cập.

Bác sĩ (Doctor): sử dụng Docter DAppcó thể truy cập vào mạng blockchain A để yêu cầu xem hồ sơ bệnh nhan ở đó thông qua verifier note sau khi được bệnh nhân cho phép.

Public Ethereum sở hữu smart constract (hợp đồng thông tin) cho phép thực hiện đăng ký và tính toàn điểm uy tin cho tất cả verifier node trong blockchain.

Verifier là node tồn tại trong mạng blockchain với 2 thành phần chính:

- Blockchain client truy cập thông tin sổ cái blockchain và sự kiện.
- Dịch vụ tại Dapp cho phép giao tiếp offchain và truy cập dữ liệu liên quan đến DApp và verifier bên ngoài blockchain.

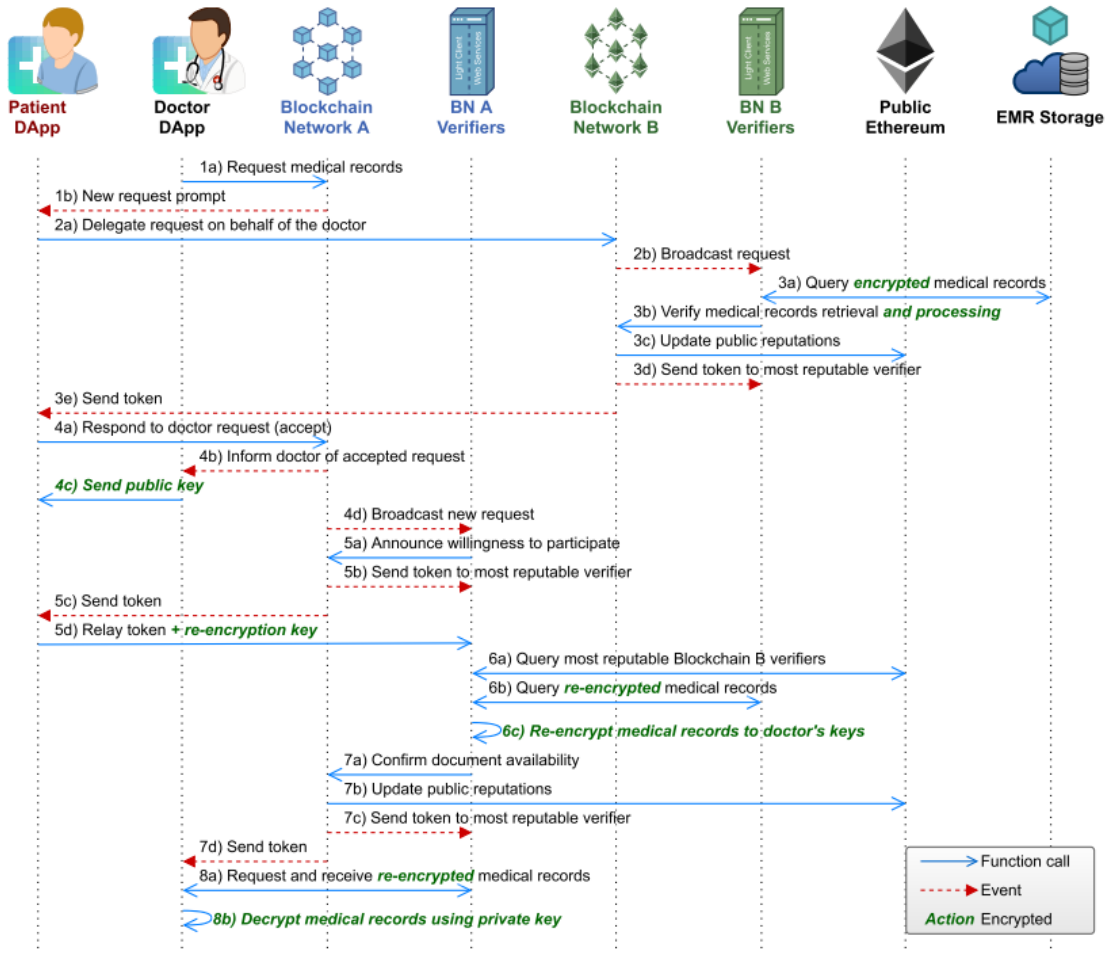
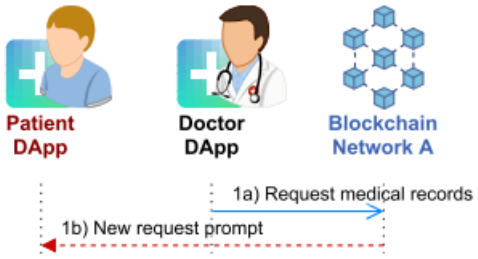


FIGURE 2. Sequence diagram of cross-chain interoperability for unencrypted and encrypted (green) EMR data sharing.

Hình 12 - Tổng quan các bước AppXChain thực hiện

3.2.4. Các bước thực hiện của bài báo

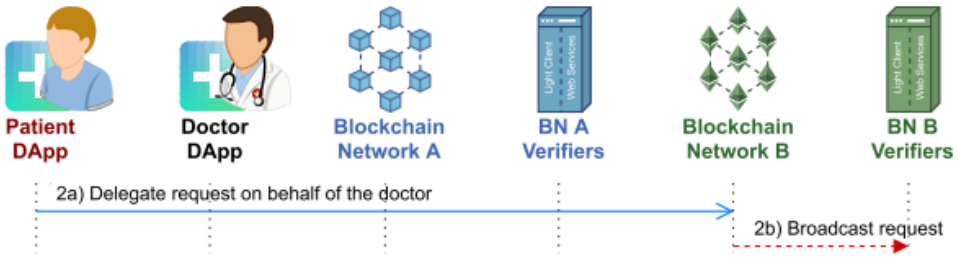
Bước 1:



Hình 13 - Bác sĩ yêu cầu hồ sơ bệnh án

- Doctor DApp tạo ra token và thực hiện gửi đến blockchain A
- Network blockchain A sẽ trả về kết quả là token identify biểu thị như một sự kiện để thực hiện việc kiểm tra, sau đó từ Doctor DApp sẽ gửi cho Patient DApp sự kiện đó và token identify theo hình thức offchain

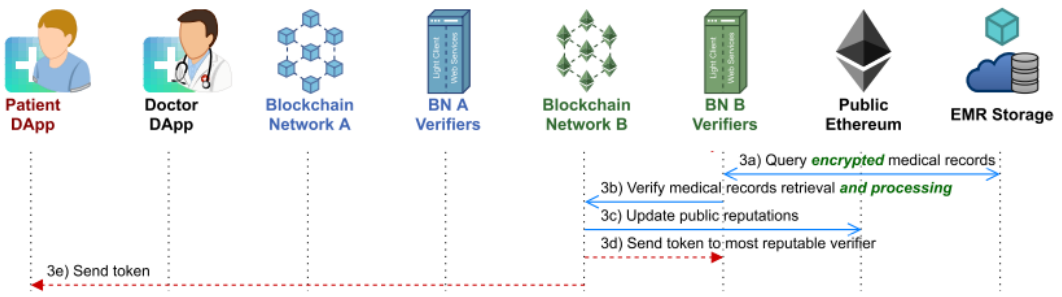
Bước 2:



Hình 14 - Bệnh nhân đồng ý cho bác sĩ gửi hồ sơ y tế

- Patient DApp thực hiện việc yêu cầu hồ sơ bệnh án điện tử (EMR) thay vì là Doctor DApp đến blockchain B. Trong đó, Patient sẽ phải xác nhận phạm vi verifiers được chấp nhận.
- Mạng blockchain B sẽ trả về cho identify yêu cầu xác nhận của Patient với biểu thị là một sự kiện để thực hiện trong tương lai. Mạng blockchain B cũng sẽ broadcast 1 identifier của bệnh nhân đến verifiers trong mạng blockchain B để thực hiện thông báo một yêu cầu mới đã sẵn sàng.

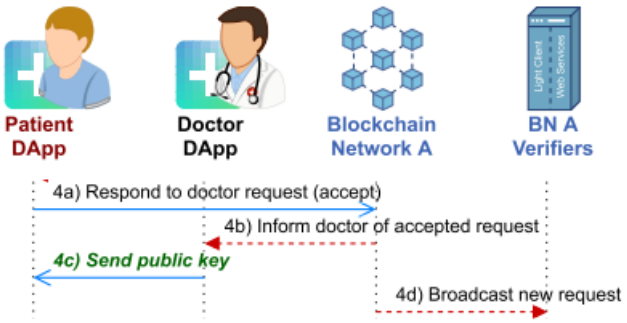
Bước 3:



Hình 15 - Blockchain Network B truy vấn hồ sơ bệnh án

- Verifier của blockchain B sẽ thực hiện việc query xuống EMR Storage để thực hiện tìm kiếm hồ sơ bệnh án và gửi proof đã được thu thập cho mạng blockchain B.
- Sẽ có 2 trường hợp xảy ra đối với proof:
    - Không mã hóa: proof là mã băm của hồ sơ bệnh án
    - Có mã hóa: proof là token có được trong bundle hồ sơ bệnh án
- Mạng blockchain sẽ xác thực proof được lưu private trên onchain và đánh giá hiệu suất của verify dựa trên sự đúng đắn và thời gian thực thi.
- Xếp hạng được sử dụng để cập nhật, đánh giá danh tiếng của network B và Public Ethereum

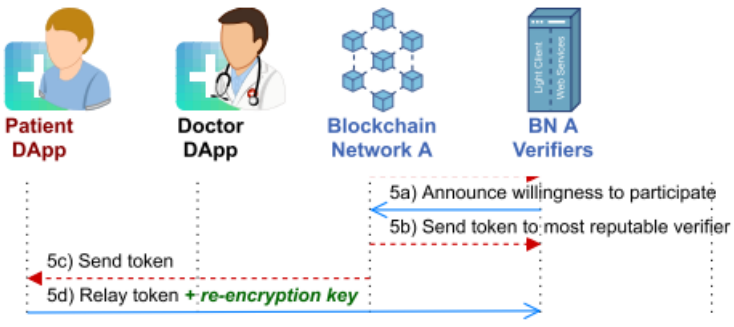
Bước 4:



Hình 16 - Bệnh nhân đồng ý yêu cầu của bác sĩ

- Bệnh nhân phản hồi bằng cách chấp nhận yêu cầu trước đó. Bệnh nhân sẽ gửi token key trong yêu cầu ban đầu của bác sĩ, tránh được người không có thẩm quyền phản hồi.
- Mạng blockchain A thông báo cho Doctor DAppviệc yêu cầu được chấp nhận, sẵn sàng để tìm và xác minh.
- Trong trường hợp sử dụng mã hóa thì Doctor DApp khi nhận được phản hồi sẽ gửi public key theo cách offchain cho bệnh nhân.

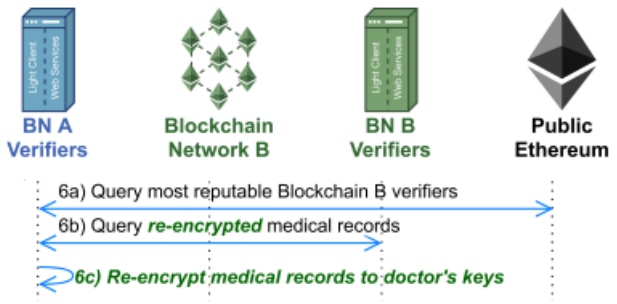
Bước 5:



Hình 17 - Chọn verifier từ Blockchain Network A

- Verify của blockchain network A thông báo sẵn sàng thực hiện việc tìm và xác minh hồ sơ bệnh án.
- Sau khi có đủ thông tin phản hồi của verify A thì blockchain network A gửi token đến verify uy tín nhất và bệnh nhân.
- Bệnh nhân sẽ giao tiếp offchain với verify nhằm chuyển token. Trong trường hợp mã hóa thì bệnh nhân sử dụng private key của họ và public key của bác sĩ để tạo re-encryptyed key và gửi đến verify tại blockchain network A.

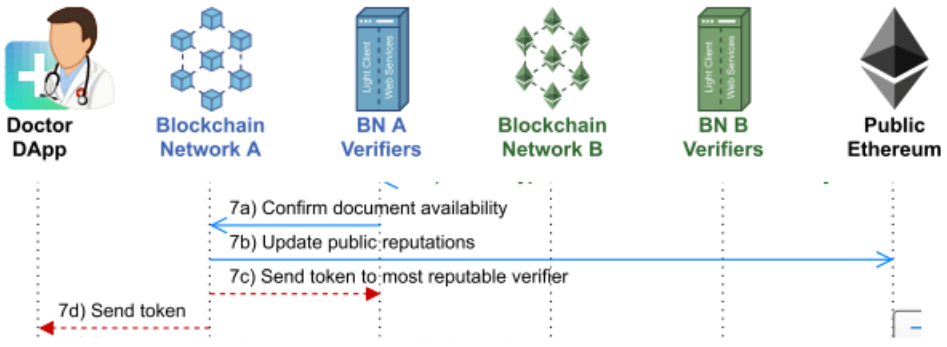
Bước 6:



Hình 18 - Verifier thực hiện truy vấn hồ sơ bệnh án

- Verify ở blockchain network A thực hiện truy vấn đến hệ thống danh tiếng Ethereum công khai để đảm bảo rằng việc chọn verify của blockchain network B uy tín được đảm bảo.
- Thiết lập kết nối giữa 2 verifier ở hai blockchain network.
- Với trường hợp có mã hóa, thì sau khi chuyển tài hồ sơ bệnh án, verify sẽ thực hiện chuyển đổi trạng thái mã hóa hồ sơ bệnh án từ Patient DApp của bệnh nhân sang Doctor DApp của bác sĩ.

Bước 7:

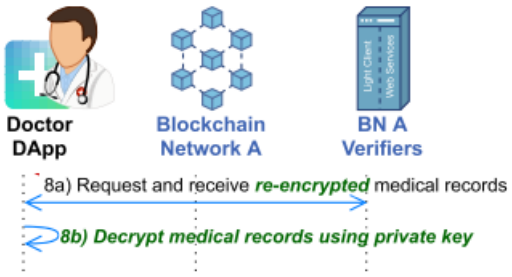


Hình 19 - Verifier xác nhận hồ sơ

- Verify của blockchain network A xác nhận tính sẵn sàng của tài liệu cùng proof.
- Sẽ có 2 trường hợp xảy ra:
    - Không mã hóa: proof ở dạng băm của hồ sơ bệnh án sẽ được tìm thấy

    - Có mã hóa: proof ở dạng token chuyển đổi tài liệu (trong bước 3)
- Mạng blockchain A sẽ cập nhật độ uy tính của verify trong hồ sơ nội bộ và hệ thống danh tiếng công khai. Mạng blockchain A gửi token đến verify và Doctor DApp cho lượt chuyển hồ sơ bệnh án lần cuối.

Bước 8:



Hình 20 - Thiết lập kết nối và chuyển tài liệu

Doctor DApp và verify sử dụng token để thiết lập kết nối để chuyển hồ sơ bệnh án từ verify của blockchain network A đến bác sĩ.

Trong trường hợp có mã hóa, Doctor DApp sẽ giải mã bằng private key của bác sĩ.

3.2.5. Bài báo khác nhằm cải thiện mô hình CrossChain

Các bài báo được chọn để nhằm tham khảo và cải thiện mô hình bài báo chính hiện tại:

- Bài 1: Zhang, Y., Jiang, J., Dong, X., Wang, L., & Xiang, Y. (2022). BeDCV: Blockchain-Enabled Decentralized Consistency Verification for Cross-Chain Calculation. IEEE Transactions on Cloud Computing.
- Bài 2: He, Y., Zhang, C., Wu, B., Yang, Y., Xiao, K., & Li, H. (2021). A cross-chain trusted reputation scheme for a shared charging platform based on blockchain. IEEE Internet of Things Journal.
- Bài 3: Jiang, J., Zhang, Y., Zhu, Y., Dong, X., Wang, L., & Xiang, Y. (2022). DCIV: Decentralized cross-chain data integrity verification with blockchain. Journal of King Saud University-Computer and Information Sciences, 34(10), 7988-7999.

Bài 1: BeDCV: Blockchain-Enabled Decentralized Consistency Verification for Cross-Chain Calculation

Ngữ cảnh:

Khi lưu trữu data quá lớn thì việc truy vấn ngày càng lâu, tốn chi phí, và nhóm tác giả đã đưa ra phương pháp lưu trữ trên nhiều blockchain và giải pháp an toàn khi thực hiện quá trình này.

Phương pháp:

- Bước 1 Initialization: Đầu tiên, SC gửi các tham số bảo mật đến C_m và C_s
- Bước 2 Task requesting: Tiếp theo, user_m get timestamp, pack chung với calculation task thành R. Sau đó tạo ra các tham số mã hóa của paillier homomorphic và gửi pub key + R tới user_s
- Bước 3 Data calculation: User_s nhận yêu cầu, get data m_i từ C_s, tính toán ra kết quả M, sau đó dùng pub key để encrypt nó thành C. Các dữ liệu được tính toán m_i được mã hóa paillier thành c_i, sau đó từ c_i tạo xác thực thành σ_i rồi được mapping vào Bloom Filter B_s
- Bước 4 Data writing: Dữ liệu được lưu vào C_s, sau đó C_s sẽ thực hiện một smart constract Ss với C để tạo audit proof, sau đó send C to C_m, Ss to SC
- Bước 5 Results Receiving: C_m nhận C, gửi C làm audit proof cho SC, user_m get result from C_m rồi decrypt bằng pri key.
- Bước 6 Verification:
  - Correctness: SC thực hiện paillier lần nữa trên data và compare kết quả với C_m.
  - Integrity Verification: C_s sends the proof (σ, ς) => SC xài bilinear pairing để verify tính toàn vẹn của dữ liệu

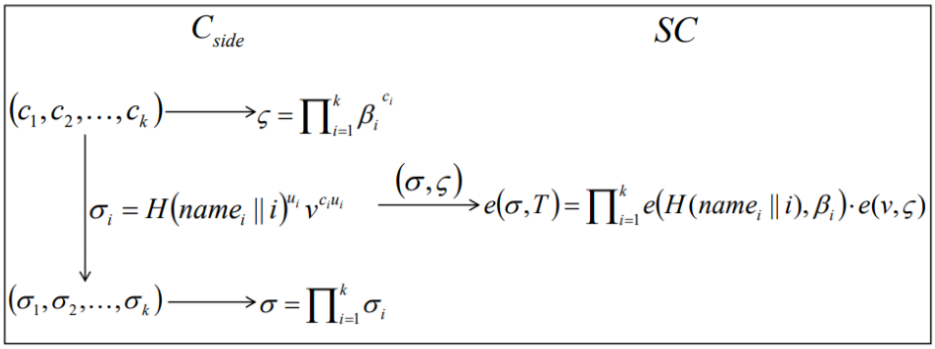


Fig. 5. The Procedure of Integrity Verification

Hình 21 - Quá trình thực hiện kiểm tra tính toàn vẹn

- Real-time Guarantee:

Algorithm 1 Real-time verification

Input: B, B_s
Output: Real-time or Non-real-time
for $i = 1; i \leq m; i++$ **do**
  if $B_s[i] != 0$ **then**
    if $B[i] == 0$ **then**
      return Non-real-time
    end if
  end if
end for
return Real-time

Hình 22 - Kiểm tra dựa trên thời gian thực

Toàn bộ quá trình thực hiện:

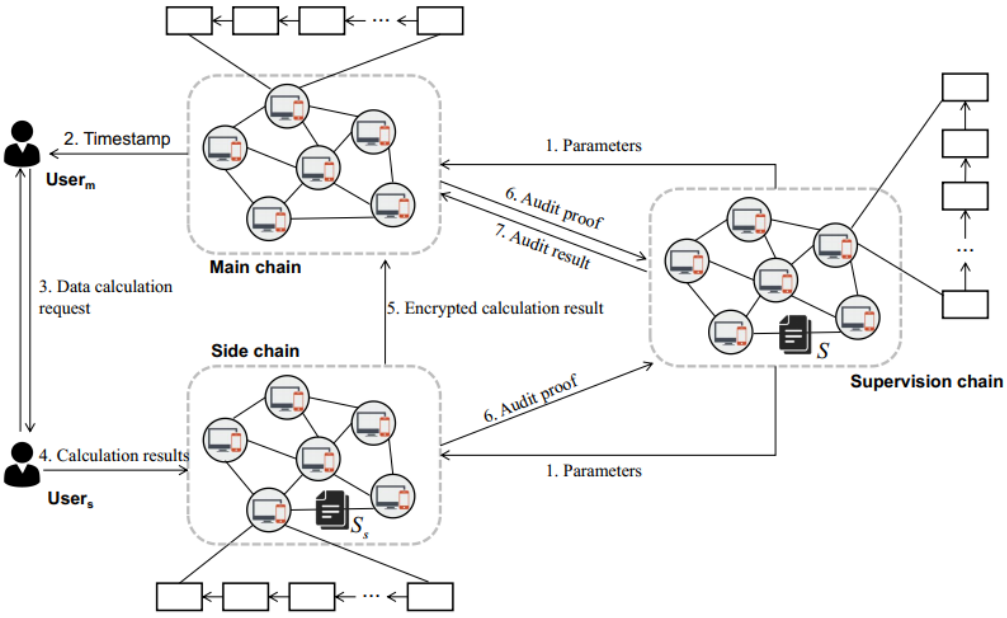


Fig. 3. Overview of the proposed scheme

Hình 23 - Toàn bộ quá trình thực hiện của bài báo số 1

Kết quả:

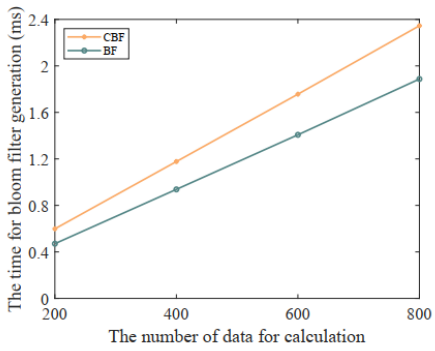
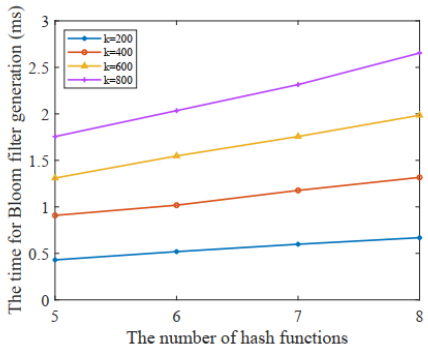


Fig. 6. The CBF Generation Time for CBF and BF



Hình 24 - Kết quả thực hiện của bài báo số 1

Bài 2: A cross-chain trusted reputation scheme for a shared charging platform based on blockchain

Ngữ cảnh:

Do thiếu hụt các charging pile (CP) nên private CP được đưa vào hệ thống sharing. Hạn chế: CPs bị hư hại, thái độ dịch vụ kém của chủ sở hữu CP.

Để nâng cao trải nghiệm người dùng, cơ chế danh tiếng được đề xuất và được tính toán dựa trên user rating. Thông tin user rating được thu thập bởi bên thứ 3 do đó dễ gặp lỗi single point và có khả năng gian dối. Do đó cơ chế danh tiếng dựa trên blockchain được ứng dụng và lưu trữ các thông tin: user authentication, charging records và rating information để tính toán chính xác nhất. Tuy nhiên như vậy lại gặp vấn đề về lưu trữ và khả năng truy xuất hiệu quả.

Phương pháp:

Quy trình 1: Hoạt động của model sạc muilt-chain

Multi-chain:

Chain C1: lưu các certificate, danh tính phương tiện, user và các CPs đã đăng ký

Chain C2: lưu thông tin các charging transactions

Chain C3: lưu rating chất lượng của mỗi CPs

- Bước 1: CPs và EVs cần đăng ký lên chain C1
- Bước 2: EV gửi request cần sạc lên platform
- Bước 3: platform xác thực danh tính EV
- Bước 4: platform chọn CP có danh tiếng tốt và xác thực danh tính của nó
- Bước 5: Sạc
- Bước 6: Upload transaction về hoạt động sạc lên C2
- Bước 7: Upload rating của user lên C3

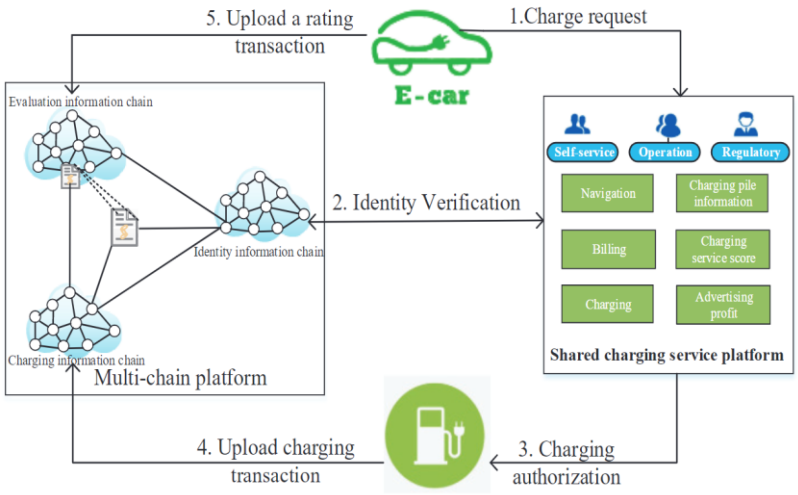


Fig. 1: Multi-chain charging model

Hình 25 - Hoạt động của model sạc muilt-chain

Quy trình 2: Sau khi sạc xong

- Bước 1: EV gửi rating request lên chain C3
- Bước 2: Kích hoạt tạo smart contract
- Bước 3: Xác thực danh tính CP và EV' trên C1
- Bước 4: Xác thực transaction trên C2
- Bước 5: Upload rating lên C3
- Bước 6: Tính điểm danh tiếng R
- Bước 7: Lưu R vào C3

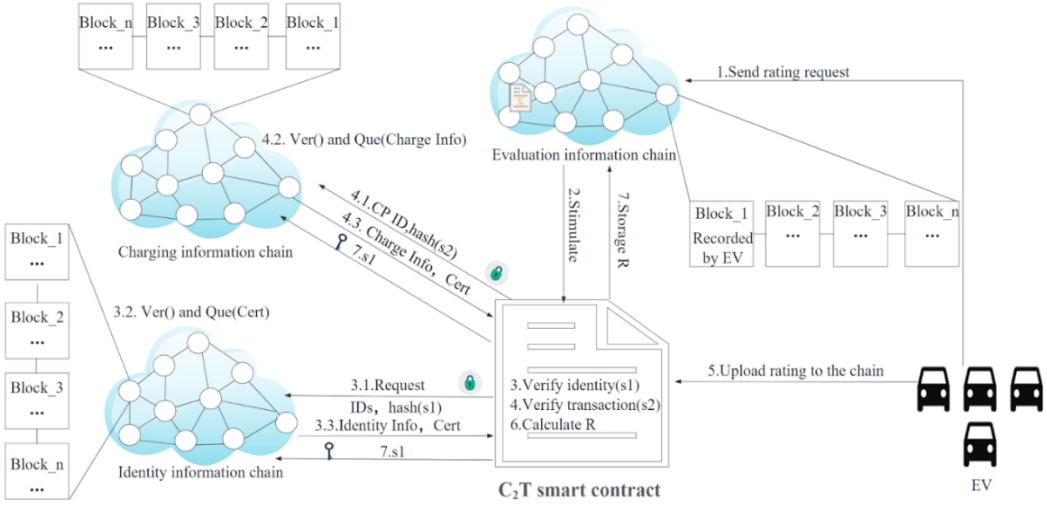


Fig. 2: The process of C_2T smart contract

Hình 26 - Hoạt động của smart contract

Kết quả:

Tiêu tốn gas cho mỗi hoạt động của C2T smart contract

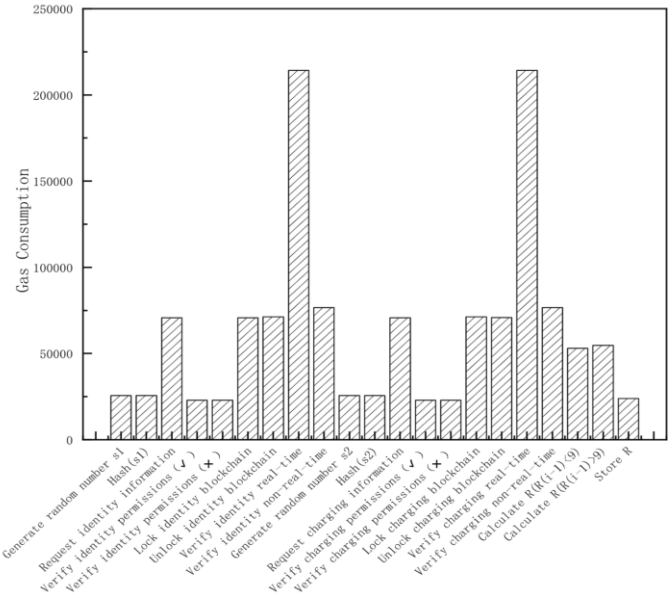


Fig. 5: The Main Gas Consumption of C_2T Smart Contract

Hình 27 - Tiêu tốn gas cho mỗi hoạt động của C2T smart contract

So sánh hiệu quả của điểm danh tiếng giữa việc kiểm tra real-time và ko kiểm tra

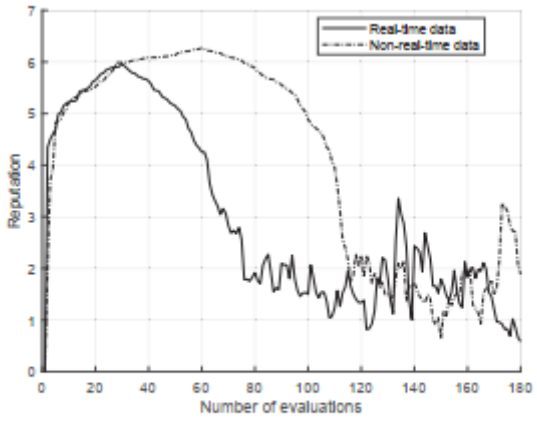


Fig. 9: Effect comparison with or without real-time verification

Hình 28 - So sánh hiệu quả của điểm danh tiếng giữa việc kiểm tra real-time và ko kiểm tra

Bài 3: DCIV: Decentralized cross-chain data integrity verification with blockchain

Ngữ cảnh:

Bài báo chỉ ra khi thực hiện chuyển đổi dữ liệu giữa các mạng blockchain sẽ xảy ra tình trạng mất tính toàn vẹn:

- Khi thực hiện gửi từ user lên AccessChain
- Khi chuyển đổi dữ liệu giữa các mạng blockchain
- Khi lưu trữ trên một mạng blockchain một dữ liệu nhưng không đầy đủ

Bài báo này nêu ra phương pháp và thực thi để khắc phục tình trạng trên

Phương pháp:

Ở bài này chúng ta sẽ thực hiện việc kiểm tra tính toàn vẹn của dữ liệu khi chuyển đổi giữa 2 mạng CrossChain khác nhau với các bước như sau:

- Bước 1: Tiền xử lý dữ liệu từ người dùng thực hiện gửi lên AccessChain
- Bước 2: Xử lý dữ liệu khi dữ liệu đang ở AccessChain
- Bước 3: Thực hiện việc chuyển đổi dữ liệu giữa hai mạng Blockchain
- Bước 4: SupervisionChain thực hiện gửi challenge cho hai mạng Blockchain
- Bước 5: Hai mạng blockchain gửi proof về SupervisionChain
- Bước 6: Kiểm tra proof và xác định tính toàn vẹn của dữ liệu sau khi chuyển đổi

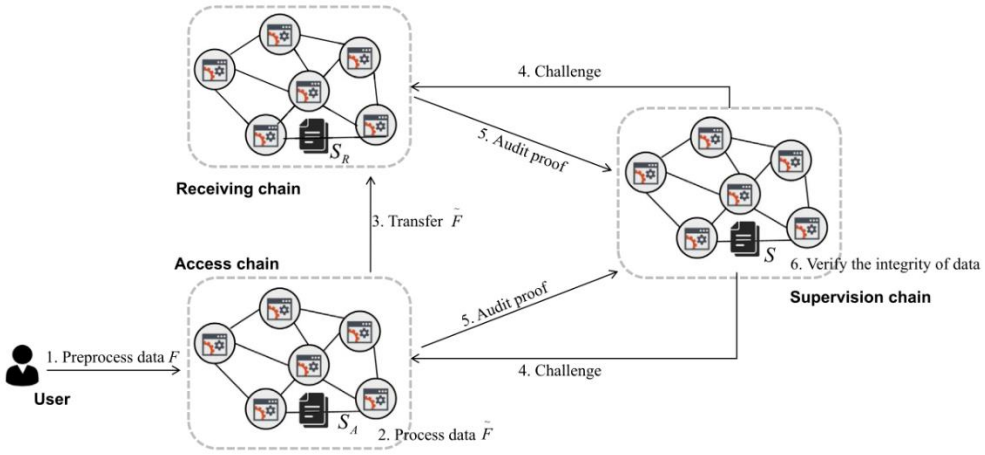


Fig. 2. Overview of the proposed scheme.

Hình 29 - Tổng quan mô hình xử lý dữ liệu và thực hiện kiểm tra tính toàn vẹn

Khi thực hiện phương pháp của hệ thống này nhằm việc xác định tính toàn vẹn của dữ liệu nhưng bên cạnh đó phải đảm bảo được tính riêng tư của dữ liệu nên tác giả đã không kiểm tra toàn bộ dữ liệu mà chỉ cần trích xuất một phần dữ liệu và tiến hành kiểm tra trên đó. Quá trình thực hiện được thể hiện bên dưới:

- Bước 1: Thực hiện xử lý để gửi lên và lưu trữu tại AccessChain: F, g1 và MT
- Bước 2: Thực hiện xử lý tại AccessChain, gửi lên và lưu trữ tại ReceiveChain: F', g2, public key và tham số phi
- Bước 3: SupervisionChain gửi challenge cho hai mạng blockchain
- Bước 4: Hai mạng blockchain gửi lại proof tương ứng là tham số Pi và Omega
- Bước 5: SupervisionChain thực hiện check proof để kiểm tra tính toàn vẹn

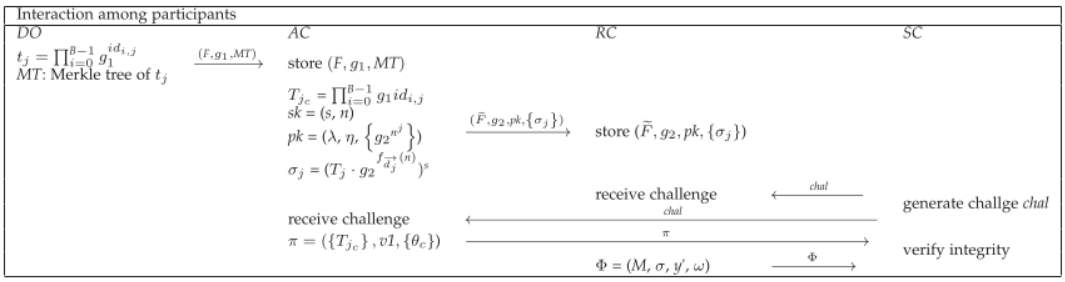


Fig. 5. The interaction among participants.

Hình 30 - Quá trình cụ thể việc thực hiện xác thực

Kết quả:

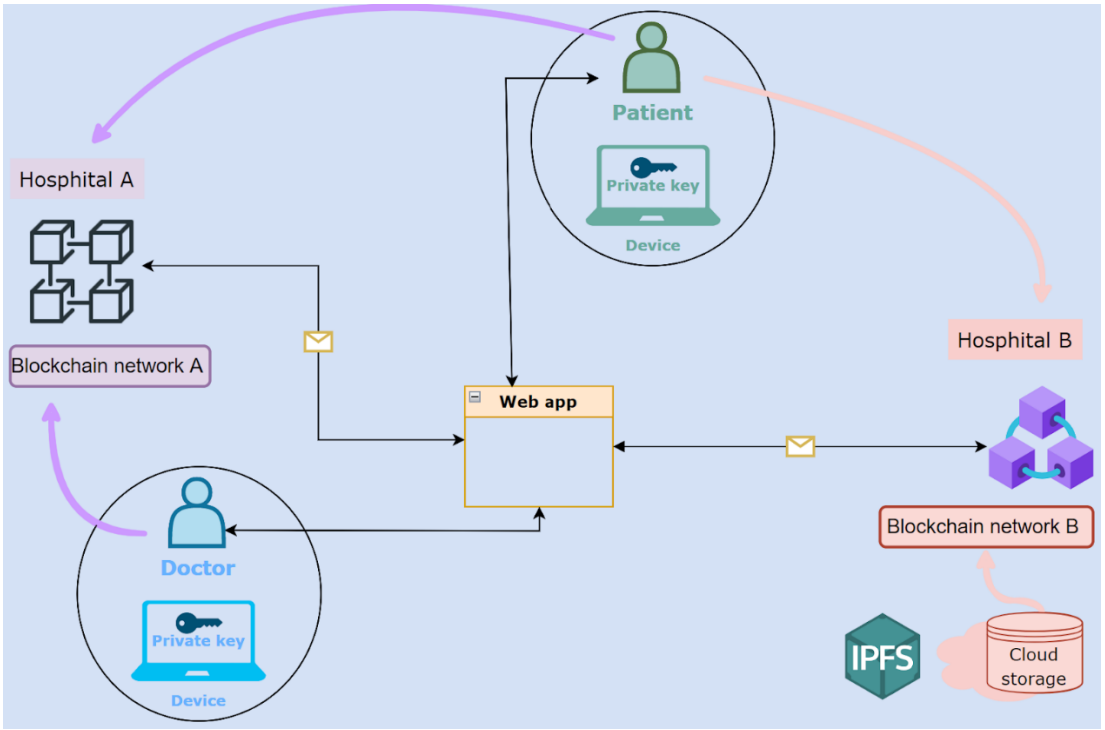
Sau khi thực hiện kiểm tra tính toàn vẹn thì sẽ có thêm phần AuditDigest

```
"action": {
        "endorsements": [ {
                "endorser": "",     "signature": ""
        } ],
        "proposal_response_payload": {
            "extension": {
                "chaincode_id": { },   "events": { },    "response": { },    "results": { }
            },
            "proposal_hash": ""
        }
        "Audit Digest": {
                "metadata": {
                    "g": " ",
                    "MT": " "
                }
        }
},
```


Fig. 11. The data structure of transaction with audit digests.

Hình 31 - Kết quả của các trường thông tin sau khi kiểm tra tính toàn vẹn

3.2.6. Đề xuất giải pháp mới



Hình 32 - Mô hình cho giải pháp mới

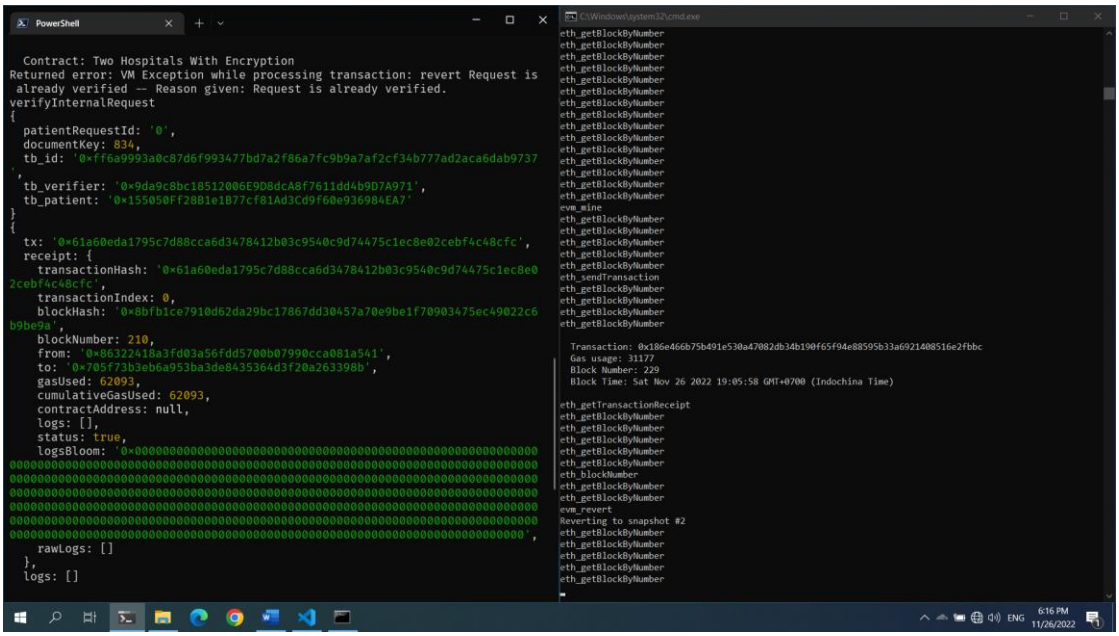
Như đã đề cập ở bài báo bên trên, do là người dùng đang trực tiếp truy cập vào Private Blockchain nên việc sẽ ảnh hưởng đến vấn đề về security của hệ thống.

Có thể thấy được rằng là nếu người dùng trực tiếp truy cập vào private blockchain thì attacker cũng có thể truy cập vào mạng blockchain và với số private key đủ lớn (từ 51% trở lên) thì hệ thống private blockchain sẽ gặp vấn đề.

Vậy nên ta cần phải thực hiện xây dựng một mô hình sao cho người truy cập vào webapp trước sau đó từ webapp mới giao tiếp với 2 mạng blockchain bên dưới, như vậy chúng ta sẽ tránh được tình trạng này khi sử dụng kết hợp thêm một webapp ở giữa như một cầu nối trung gian giữa người dùng và CrossChain bên dưới.

3.3. Kết quả đạt được

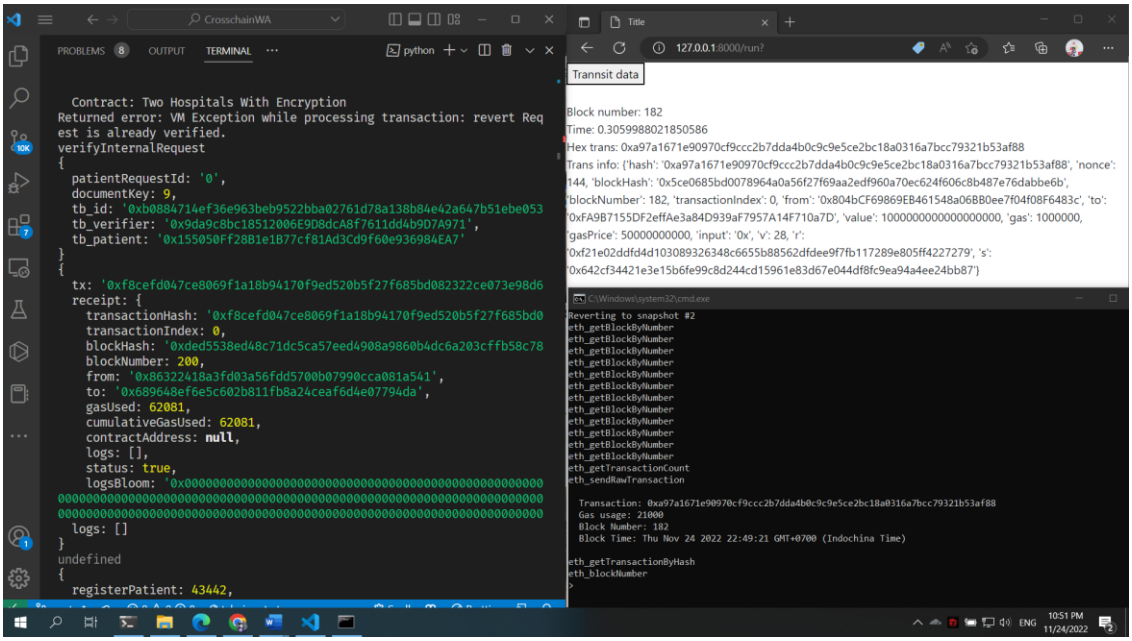
3.3.1. Kết quả demo trong bài báo



Hình 33 - Thực hiện thành công demo của bài báo

Có thể thấy ta đã thực hiện được demo code của bài báo thành công. Demo đã chỉ ra được các mà mô hình CrossChain hoạt động chính là việc trao đổi chéo thành công dữ liệu giữa 2 mạng blockchain. Tuy nhiên bài báo vẫn chưa làm rõ được chính xác bản chất và cách thức hoạt động do hiện tại bài báo chỉ đang thực hiện local trên máy tính.

3.3.2. Kết quả webapp



Hình 34 - Thực hiện thành công demo mô hình cải tiến

Nhóm đã thành công trong mô hình build thêm một webapp làm cầu nối giữa mô hình CrossChain và người dùng để có thể thực hiện thao tác trao đổi dữ liệu trên webapp và từ đó webapp sẽ gửi thông tin xuống mô hình CrossChain bên dưới để thực hiện việc trao đổi dữ liệu. Tiếp theo đó nhóm sẽ tiếp tục phát triển bài báo về xây dựng hạ tầng, cải tiến bảo mật web và cài đặt giao diện trực quan cho người dùng.

Github: https://github.com/anhkiet1227/NT215_Internship_Project

3.3.3. Hướng đi mới cho mô hình

Qua những demo bên trên nhóm đã tìm ra được hướng đi mới cho mô hình của bài báo:

- Cài đặt webapp, nâng cao cơ chế bảo mật web và cải tiến quy trình đăng nhập, đăng ký, ký xác nhận, chuyển đổi thông tin
- Xây dựng hoàn thiện hạ tầng Blockchain có thể chạy trên hai mạng blockchain thực.

Đây chính là 2 mục tiêu chính hiện tại của nhóm trong việc phát triển bài báo trong thời gian tới hướng tới việc hoàn thiện hóa mô hình và có thể ứng dụng vào nhiều hoàn cảnh hơn việc chỉ áp dụng vào hệ thống quản lý bệnh nhân, chăm sóc sức khỏe.

3.3.4. Kỹ năng mềm

- Kỹ năng thuyết trình
- Kỹ năng làm việc nhóm

- Kỹ năng giao tiếp
- Kỹ năng đọc, phân tích bài báo
- Kỹ năng quản lý thời gian
- Kỹ năng giải quyết vấn đề

PHẦN KẾT LUẬN

Lời kết đầu tiên cho chúng em gửi lời cảm ơn đến Phòng thí nghiệm An Toàn Thông Tin ĐHCNTT – ĐHQGHCM, chúng em đã được tiếp xúc với môi trường doanh nghiệp cũng như việc thực hiện nghiêm túc tác phong và thái độ đồng thời cũng trau dồi thêm nhiều kiến thức, bài học, kinh nghiệm, kỹ năng quý báu đến từ việc thực hiện nghiên cứu, phân tích bài báo khoa học, và phân tích, cải tiến mô hình của bài báo từ đó có được phương hướng thực hiện và cách xây dựng nghiên cứu khoa học. Những kinh nghiệm quý báu đó sẽ là hành trang cho chúng em có thể thực hiện Đồ Án Chuyên Ngành và Khóa Luận Tốt Nghiệp trong tương lai không xa.

Một lần nữa, chúng em xin gửi lời cảm ơn chân thành đến quý thầy cô trường Đại Học Công Nghệ Thông Tin và đặc biệt là quý thầy cô khoa Mạng Máy Tính và Truyền Thông, trong đó chúng em xin gửi lời cảm ơn sâu sắc đến thầy Trần Tuấn Dũng đã hỗ trợ chúng em trong suốt thời gian thực tập vừa qua. Do đây là lần đầu tiên chúng em thực hiện nghiên cứu khoa học cũng như làm việc trong môi trường doanh nghiệp nên nhóm chúng em khó lòng tránh khỏi những thiếu sót trong quá trình thực hiện. Chúng em cũng xin được gửi lời cảm ơn chân thành và sâu sắc đến với thầy về những lời khuyên, những lời động viên chân thành mà từ đó chúng em mới có được động lực để hoàn thành một hành trình thực tập này.

Lời cuối cùng nhóm chúng em xin gửi lời chúc sức khỏe và lời cảm ơn chân thành đến tất cả mọi người đã hỗ trợ chúng em trong suốt thời gian vừa qua.

TÀI LIỆU THAM KHẢO

1. Madine, M., Salah, K., Jayaraman, R., Al-Hammadi, Y., Arshad, J., & Yaqoob, I. (2021). appxchain: Application-level interoperability for blockchain networks. IEEE Access, 9, 87777-87791.
2. Zhang, Y., Jiang, J., Dong, X., Wang, L., & Xiang, Y. (2022). BeDCV: Blockchain-Enabled Decentralized Consistency Verification for Cross-Chain Calculation. IEEE Transactions on Cloud Computing.
3. He, Y., Zhang, C., Wu, B., Yang, Y., Xiao, K., & Li, H. (2021). A cross-chain trusted reputation scheme for a shared charging platform based on blockchain. IEEE Internet of Things Journal.
4. Jiang, J., Zhang, Y., Zhu, Y., Dong, X., Wang, L., & Xiang, Y. (2022). DCIV: Decentralized cross-chain data integrity verification with blockchain. Journal of King Saud University-Computer and Information Sciences, 34(10), 7988-7999.