



THUYẾT MINH

ĐỀ TÀI NGHIÊN CỨU KHOA HỌC SINH VIÊN 2023

A. THÔNG TIN CHUNG

A1. Tên đề tài

- Tên tiếng Việt (IN HOA): MIDAS: HỆ THỐNG QUẢN LÝ DỮ LIỆU VÀ TRUY CẬP TƯƠNG TÁC ĐA CHUỖI TRONG LĨNH VỰC CHĂM SÓC SỨC KHỎE
- Tên tiếng Anh (IN HOA): MIDAS: A MULTI-CHAIN INTEROPERABLE DATA AND ACCESS SYSTEM FOR HEALTHCARE

A2. Thời gian thực hiện

6 tháng (kể từ khi được duyệt).

A3. Tổng kinh phí

Tổng kinh phí: 6 triệu đồng, gồm:

- Kinh phí từ Trường Đại học Công nghệ Thông tin: 6 triệu đồng

A4. Chủ nhiệm

Họ và tên: Nguyễn Bình Thục Trâm

Ngày, tháng, năm sinh: 01/09/2002

Giới tính (Nam/Nữ): Nữ

Số CCCD: 079302004860

; Ngày cấp: 14/07/2022

; Nơi cấp: Cục cảnh sát

Mã số sinh viên: 20520815

Số điện thoại liên lạc: 0934010902

Khoa: Mạng máy tính và Truyền thông

Số tài khoản: 16757237

Ngân hàng: ACB

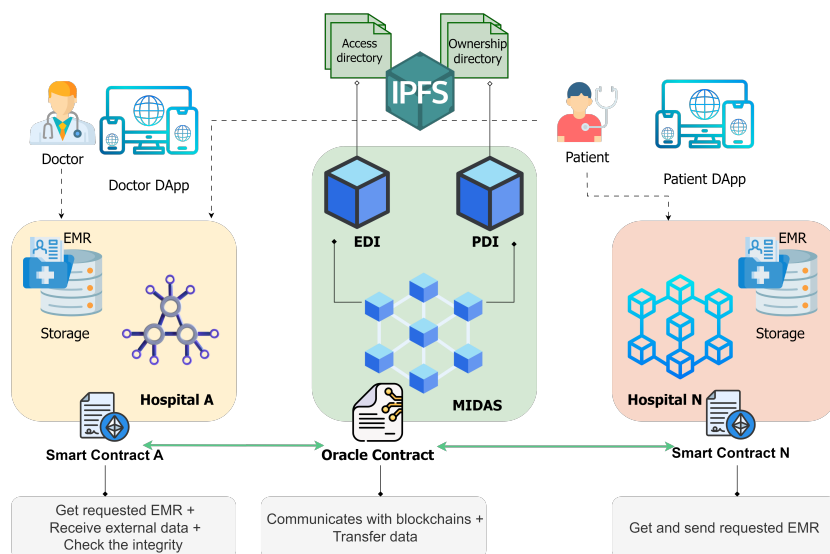
A5. Thành viên đề tài (kể cả CNĐT)

TT	Họ tên	MSSV	Khoa
1	Nguyễn Bình Thục Trâm	20520815	Mạng máy tính và Truyền thông
2	Nguyễn Bùi Kim Ngân	20520648	Mạng máy tính và Truyền thông

B. MÔ TẢ NGHIÊN CỨU

B1. Giới thiệu về đề tài

Sự xuất hiện và phát triển của công nghệ Blockchain đã mang đến những lợi thế đa diện và ứng dụng rộng rãi trên nhiều ngành công nghiệp khác nhau. Tuy nhiên, mặc dù có nhiều hứa hẹn nhưng Blockchain gặp phải thách thức đáng kể trong việc đạt được khả năng tương tác trong bối cảnh phức tạp của hệ sinh thái đa blockchain. Việc yêu cầu cấp thiết đối với trao đổi dữ liệu liên mạch và tài sản kỹ thuật số là điều hiển nhiên, tuy nhiên đi kèm với đó là sự phức tạp ngày càng tăng của việc quản lý danh tính thực thể mạng phân tán trên các hệ thống khác nhau, dẫn đến dữ liệu thiếu kết nối và tương tác linh hoạt. Do đó, để đối phó với những thách thức này, nhóm nghiên cứu giới thiệu kiến trúc 'MIDAS' nhằm thúc đẩy khả năng điều hòa tác liên mạch giữa vô số mạng blockchain. MIDAS đóng vai trò là trung gian quan trọng, tạo điều kiện thuận lợi cho các hoạt động tương tác xuyên chuỗi, nâng cao trải nghiệm người dùng và đảm bảo quyền truy cập dữ liệu an toàn. Để nâng cao khả năng của mô hình này thời tập trung vào kiểm soát dữ liệu lấy người dùng làm trung tâm, chúng tôi giới thiệu một hệ thống quản lý danh tính phi tập trung được gọi là "Mã định danh phi tập trung cho khả năng tương tác blockchain" (BIDI). BIDI cung cấp những tính năng mạnh mẽ, bao gồm quản lý thực thể nghiêm ngặt, liên kết dữ liệu và kiểm soát quyền truy cập dữ liệu tùy chỉnh cho người dùng được ủy quyền, tập trung vào quyền sở hữu dữ liệu và lấy người dùng làm trung tâm. Nói cách khác, khuôn khổ của nhóm nghiên cứu mang đến một bước quan trọng nhằm cải thiện tính hiệu quả và sự linh hoạt của công nghệ blockchain, tạo khả năng giao tiếp hài hòa giữa nhiều mạng blockchain.



Hình 1: Tổng quan về mô hình quản lý và truyền dữ liệu liên chuỗi thông qua MIDAS

B2. Mục tiêu, nội dung, kế hoạch nghiên cứu

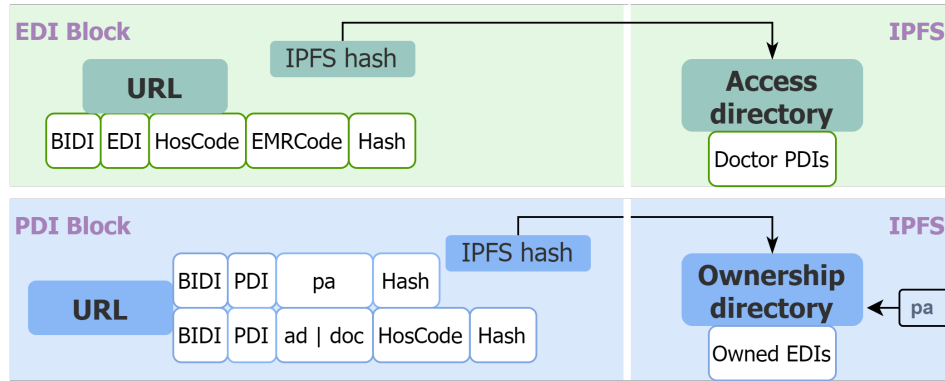
B2.1 Mục tiêu

Mục tiêu nhóm nghiên cứu hướng tới là xây dựng giải pháp mang tên MIDAS, sử dụng công nghệ danh tính phi tập trung nhằm cung cấp cơ chế định danh và quản lý các thực thể trong mạng phù hợp với bối cảnh chăm sóc sức khỏe, lấy bệnh nhân làm chủ thể trung tâm. Đồng thời tích hợp với kiến trúc Sidechain (chuỗi ngoài) có khả năng mang lại cho thế giới mạng đa chuỗi khối khả năng tương tác, giao tiếp, vận chuyển dữ liệu, và mở rộng khả năng quản lý danh tính trong bối cảnh tương tác đa chuỗi

B2.2 Nội dung và phương pháp nghiên cứu

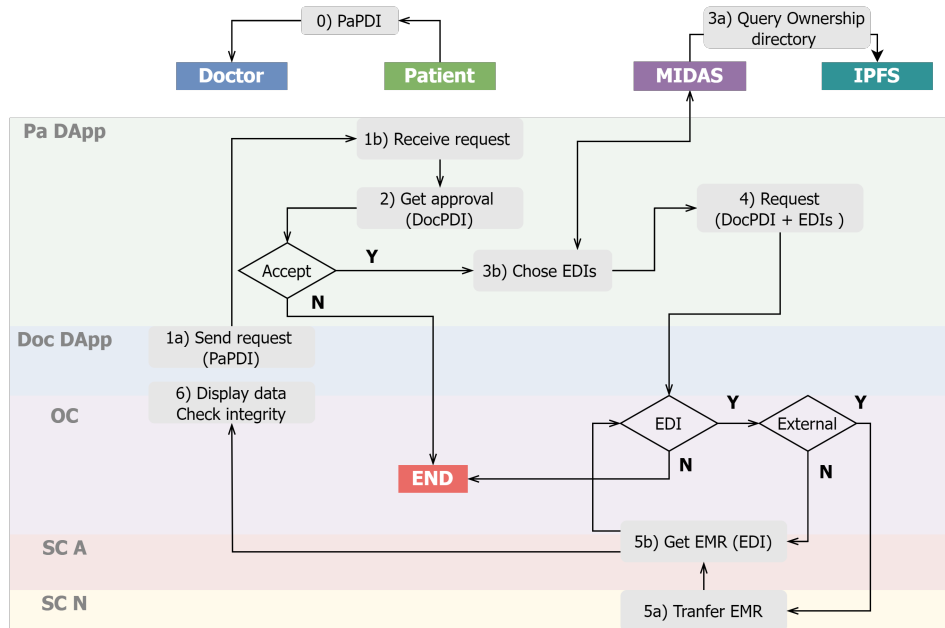
Nội dung 1: Tìm hiểu tổng quan đề tài.

Phương pháp thực hiện: Tìm hiểu sâu về lĩnh vực blockchain, đa blockchain. Tham khảo các nghiên cứu tiên phong cho giải pháp tương tác đa chuỗi tiêu biểu của Vitalik Buterin



Hình 2: Kiến trúc thành phần của BIDI

[1]. Lý thuyết về các hệ thống định danh hiện nay [2], những ưu nhược điểm, đặc biệt là về hệ thống định danh phi tập trung và những nghiên cứu ứng dụng trên hệ thống blockchain như [3, 4]. Tìm hiểu, xác định những vấn đề trong định danh trong hệ thống mạng liên chuỗi, bảo mật thông tin cho hệ thống và lên ý tưởng cho hướng giải quyết



Hình 3: Quá trình hoạt động cho truy vấn EMR

Kết quả dự kiến: Xác định được vấn đề về tương tác đa chuỗi và những khó khăn trong định danh cho thực thể nằm trong mạng đa blockchain. Đưa ra hướng giải quyết gồm kiến trúc chuỗi khối ngoài (sidechain) và hệ thống định danh phi tập trung mới phù hợp cho tương tác liên chuỗi. Kiến trúc tổng quan của giải pháp được mô tả trong hình 1

Nội dung 2: Thiết kế giải pháp và mô hình hoạt động.

Phương pháp thực hiện: Dựa trên nghiên cứu trước của nhóm [5], ứng dụng lại kiến trúc sidechain đã xây dựng, là một mạng oracle phi tập trung, mang lại khả năng trao đổi dữ liệu giữa các blockchain khác nhau mà cụ thể ở nghiên cứu này là trao đổi hồ sơ y tế điện tử (EMR) của bệnh nhân. Tiếp theo, xây dựng kiến trúc khuôn khổ cho hệ thống định danh phi tập trung tên BIDI, chi tiết được mô tả trong hình 2. Cách thiết kế này phù hợp với bối cảnh bệnh viện và nhu cầu trao đổi dữ liệu giữa các thực thể. Nhóm nghiên cứu cũng giới thiệu về kiến trúc BIDI document, nắm vai trò quan trọng trong xác định

quyền sở hữu dữ liệu và quản lý truy cập tự động. Hình 3 mô tả quá trình hoạt động cho truy vấn nhiều EMR từ nhiều nguồn tức các mạng blockchain khác nhau.

Kết quả dự kiến: Hoàn thiện ý tưởng, sơ đồ tổng quan và các luồng hoạt động của mô hình. Giải pháp hoàn thành các mục tiêu đề ra gồm trao đổi dữ liệu liên chuỗi, quản lý danh tính cho các thực thể.

Nội dung 3: Thực nghiệm và đánh giá hệ thống.

Phương pháp thực hiện: Từ các ý tưởng ban đầu, nhóm nghiên cứu sẽ tính toán chuẩn bị môi trường thực nghiệm phù hợp. Sau đó, thiết lập các hệ thống chuỗi khối chính của mô hình tổng quan, bao gồm: Hệ thống chuỗi khối riêng tư, hệ thống chuỗi khối công khai, hệ thống lưu trữ IPFS và hệ thống chuỗi khối ngoài để phục vụ cho quá trình quản lý dữ liệu và truy cập tương tác đa chuỗi. Sau đó, nhóm nghiên cứu sẽ thực hiện điều chỉnh và cấu hình đối với các hệ thống trên và viết các hợp đồng thông minh có khả năng giao tiếp, vận chuyển dữ liệu và quản lý danh tính phù hợp với ý tưởng đề ra trong mô hình tổng quan. Cuối cùng, nhóm nghiên cứu sẽ xây dựng các kịch bản phù hợp với ngữ cảnh để thực hiện kiểm thử và đánh giá hệ thống thông qua ba tiêu chí chính là: Chi phí, Thời gian, Hiệu năng CPU.

Kết quả dự kiến: Có được các thông số thực nghiệm chính xác của các tiêu chí: Chi phí xây dựng và vận hành hệ thống; Hiệu suất CPU khi hệ thống đang duy trì và thực hiện giao tiếp liên chuỗi; Thời gian thực thi của từng giao dịch được định nghĩa trong hợp đồng thông minh. Qua đó đánh giá được phần nào khả năng ứng dụng thực tế của hệ thống.

B2.3 Kế hoạch nghiên cứu

Công việc	Thời gian	Phân công
Soạn dàn ý cho ý tưởng (Bài toán, ngữ cảnh, phương pháp thực hiện)	01/09/2023 – 14/09/2023	Ngân, Trâm
Nghiên cứu các công trình có đề tài tương tự	15/09/2023 – 21/09/2023	Ngân
Thiết kế kiến trúc giải pháp, minh họa hình ảnh	22/09/2023 – 25/10/2023	Ngân
Thiết kế các kịch bản và luồng hoạt động,	26/10/2023 – 09/11/2023	Trâm
Triển khai thử nghiệm thực tế các kịch bản trên môi trường máy ảo	10/11/2023 – 06/12/2023	Trâm
Đánh giá kết quả hoạt động, phân tích độ an toàn	07/12/2023 – 13/12/2023	Ngân, Trâm
Hoàn thiện nội dung khóa luận	14/12/2023 – 30/12/2023	Ngân, Trâm

Bảng 2: Kế hoạch nghiên cứu

B3. Kết quả dự kiến

Hệ thống được kỳ vọng sẽ đạt được những kết quả bao gồm:

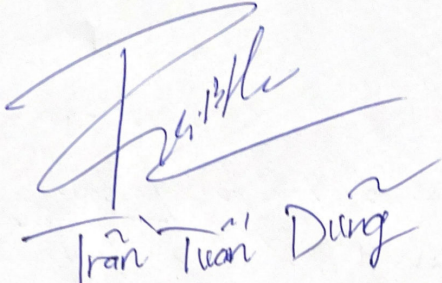
1. Giải pháp định danh liên chuỗi hiệu quả: Cung cấp khả năng vận chuyển liên chuỗi hồ sơ y tế của bệnh nhân cho bác sĩ đã yêu cầu, liên kết danh sách hồ sơ y tế đã tạo với chủ sở hữu của chúng và cơ chế tự động cấp quyền truy cập dữ liệu cho đối tượng hợp lệ.
2. Đảm bảo an toàn và bảo mật cho dữ liệu cũng như các thực thể trong mạng, đồng thời hoạt động hiệu quả về mặt thời gian, hiệu suất và chi phí tiêu tốn.
3. Đóng góp cho cộng đồng blockchain: Cung cấp kiến thức và công cụ hữu ích cho nhà phát triển hợp đồng thông minh và cộng đồng blockchain, từ đó tăng cường tính bảo mật và độ tin cậy của hệ thống.

4. Có bài báo khoa học được hội nghị chấp nhận
5. Hoàn thành Khóa luận tốt nghiệp cùng dựa trên nội dung trên

B4. Tài liệu tham khảo


- [1] Vitalik Buterin. “Chain interoperability”. In: *R3 research paper 9* (2016), pp. 1–25.
- [2] Yuan Cao and Lin Yang. “A survey of identity management technology”. In: *2010 IEEE International Conference on Information Theory and Information Security*. IEEE. 2010, pp. 287–293.
- [3] Yoshiaki Fukami, Takumi Shimizu, and Hiroyasu Matsushima. “The impact of decentralized identity architecture on data exchange”. In: *2021 IEEE International Conference on Big Data (Big Data)*. IEEE. 2021, pp. 3461–3465.
- [4] Xuehan Li, Tao Jing, Ruinian Li, Hui Li, Xiaoxuan Wang, and Dequan Shen. “Bdra: Blockchain and decentralized identifiers assisted secure registration and authentication for vanets”. In: *IEEE Internet of Things Journal* (2022).
- [5] Tuan-Dung Tran, Kiet Anh Vo, Nguyen Binh Thuc Tram, Ngan Nguyen Bui Kim, Phan The Duy, and Van-Hau Pham. “Enhancing Blockchain Interoperability Through Sidechain Integration and Valid-Time-Key Data Access Control”. In: *Intelligence of Things: Technologies and Applications*. Ed. by Nhu-Ngoc Dao, Tran Ngoc Thinh, and Ngoc Thanh Nguyen. Cham: Springer Nature Switzerland, 2023, pp. 213–224. ISBN: 978-3-031-46749-3.

Ngày 03 tháng 11 năm 2023
Giảng viên hướng dẫn
(Ký và ghi rõ họ tên)



Trần Tuấn Dũng

Ngày 03 tháng 11 năm 2023
Chủ nhiệm đề tài
(Ký và ghi rõ họ tên)



Nguyễn Bình
Thúc Trâm